IGI PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-pub.com
ITJ3879

This paper appears in the publication, International Journal of E-Business Research ,Volume 3, Issue 4
edited by **In Lee © 2007, IGI Global**

IPR Protection for Digital Media Distribution: Trends and Solutions in the E-Business Domain

Bill Vassiliadis, Hellenic Open University, Greece

Vassilis Fotopoulos, Hellenic Open University, Greece

ABSTRACT

Copyright protection is becoming an important issue for organizations that create, use, and distribute digital content through e-commerce channels. As online corruption increases, new technical and business requirements are posed for protecting intellectual property rights such as watermarking, use of metadata, self-protection, and self-authentication. This work is a review of the most important of these methods and analyzes their potential use in digital rights management systems. We focus especially on watermarking and argue that it has a true potential in e-business because it is possible to embed and detect multiple watermarks to a single digital artifact without decreasing its quality. In conjunction with parallel linking of content to metadata, there is true potential for real life copyright-protection systems.

Keywords: *business model; digital rights management; digital watermark; e-commerce; intellectual property rights; legal issues; metadata; security standards*

INTRODUCTION

The wealth of information provided by digitization devices and sensors has grown dramatically while the available communication channels for faithfully transmitting that data face serious security threats. Digital media in the form of still images, video, sound, and multimedia (digital artifacts) offer many advantages in their use since they enhance human-machine interaction in numerous areas. E-commerce (B2C and B2B) channels are becoming a primary distribution channel for the digital media market, which in turn has seen a dramatic growth in the last few years (Eskicioglu, 2003). However, where there is profit there is also a big chance for corruption. The ease with which perfect digital copies are produced by virtually any user creates great concern to content providers and online resellers.

The discussion behind copyright violation in e-commerce (especially B2C) is of course justified by the considerable financial losses

of content providers and legal distributors. The international intellectual property alliance estimated the annual loss of revenue in the U.S. motion picture industry due to piracy at US$1.5 billion, and in the record and music industries at US$2.3 billion for the financial year of 2003 (IPR, 2005). It is also worth noting that a large portion of Internet bandwidth (approximately 30%) is consumed by users exchanging illegal copies of digital media (mainly video). The recent legal battle between U.S. filmmakers and companies that support free distribution technologies such as peer to peer, has resulted in a crisis for the software industry: software developers are directly deemed responsible for the use of their products (McCalman, 2005). The recent ruling of the U.S. supreme court in favor of content developers in the case of MGM vs. Grokster somewhat shook the so-called "Sony Safe Harbor" (a 1984 court ruling in the case of Sony vs. Universal according to which h/w and s/w developers are immune from liability for the infringing acts of their users) (Samuelson, 2005). It is certain that there will always be people with enough motivation to illegally use copyright material by bypassing protection mechanisms.

Although IPR protection was and is still considered a strategic goal for many organizations, vendors are not yet convinced to invest the needed, and in many cases substantial resources to achieve it (Schneider, 2005). Cost effectiveness is emerging as a major requirement for protecting IPR (Cohen, 2003). Many solutions have been proposed for addressing the problem of copyright protection and in the recent years, the community has witnessed some huge security failures and partial successes. The initial movement for the development of advanced and cost-effective techniques for IPR (intellectual property rights) management and protection of digital media was accompanied by great enthusiasm. Soon, as efforts were advancing, several technological, economic, and cultural shortcomings were identified. Some efforts for producing security standards failed, others merged (Felten, 2005). A perfect IPR protection solution still eludes us, partly because the industry cannot or will not agree in common standards. This does not mean, however, that copyright protection is impossible, it just emphasizes the need for coordinated actions.

From a technological point of view, two major categories of IPR protection techniques can be identified: a-priori (copy prevention) and a-posteriori protection (copy detection). Copy prevention methods include software techniques such as cryptography, password authentication, and physical media protection techniques such as CD/DVD copy prevention systems. Software techniques are more successful but experience has shown that these methods alone are still not as effective as predicted. Copy detection methods, such as digital watermarking are becoming extremely popular (Memon & Wong, 1998). They do not directly avert theft but rather discourage it by supporting detection of stolen copyrighted material. New methods also enable tracking of the source that provided the media and, in many cases identification of the distribution path. Copy detection provides proof that stands as evidence in legal courts. The popular anti-piracy motto of the U.S. film industry "steel it and we will catch you" is based on this concept. Other methods include futuristic ideas such as self-protecting content (Rosenblatt, 2004) or utopic proposals such as a small-scale Internet for hackers to tangle with; they have only demonstrated the urgency to find efficient solutions.

Complete solutions to IPR protection and management in e-business such as digital rights management (DRM) systems have been proposed for the persistent protection of digital content and management of licenses throughout its lifecycle (Memon et al., 1998). Technologically, the area of DRM is unique in the sense that it involves many diverse sub-areas: cryptography, signal processing and information theory, e-commerce, business modeling, and legal and social aspects just to mention a few. Current DRM systems are complicated, expensive, and inherit many of the shortcomings of the methods they use. They are considered however by many, a solution of great prospect.

In this work, we review standards, business, and technological solutions for IPR protection and management for digital media, namely watermarking and metadata with a special focus on digital rights management systems and new standards such as MPEG-7, MPEG21, and JPEG2000. We argue that watermarking combined with metadata is essential to the e-business domain, especially when multiple watermarks are used. Although DRM encompasses a wide range of security, workflow, and authentication technologies, we focus especially on security as the most important of the three. The first section of this work describes current and future technologies for IPR protection while the second presents DRM systems and discusses technological, architectural, and business issues. Subsequently an insight on watermarking (and in particular multiple watermarking) as an efficient technique for managing IPR online. Furthermore, a discussion on the advantages and disadvantages of current technologies used in DRM systems with a special focus on security is provided. Future prospects are also discussed with a focus on standardization and new computing models such as mobile and peer to peer computing. Finally, the conclusions are drawn.

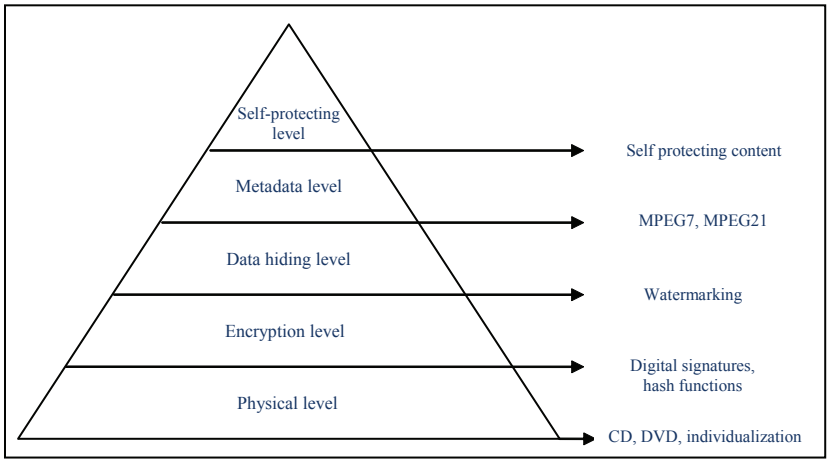
TECHNOLOGIES FOR IPR PROTECTION

IPR protection technologies provide persistent or non-persistent content protection without managing directly digital licenses to authorized users. Restrictions of content usage rights have to be maintained after the content is delivered to the end-user including data protection to protect against unauthorized interception and modification, unique identification of recipients to enable access control for the digital content and effective tamper-resistant mechanisms to process protected data and enforce content usage rights (Koenen, Lacy, MacKay, & Mitchell, 2004). There is a large number of security methods used for IPR protection in e-commerce applications that can be categorized in five levels: the physical, the encryption, the data hiding, the metadata, and the self-protecting level (Figure 1).

The physical level involves IPR protection techniques that are associated with the storage medium or the user device that accesses the content. The DVD copyright protection mechanism and individualization (the unique identification of user devices) are two such examples. This category of techniques suffers from two drawbacks. The first is the high possibility of circumventing the protection mechanism (as in the case of DVD) and the second is the "analogue hole." The latter refers to the process of making illegal copies of digital content by legally accessing the content and copying the analogue output of the player. For example, a user buys a MP3 coded song, accesses it through a player and records the analogue output of the sound card (although internally), re-digitizes it, and produces an illegal copy for distribution.

Symmetric and asymmetric encryption techniques comprise the next level as we move up the pyramid of IPR protection techniques: the content is encrypted using a symmetric key algorithm (digital signatures, one-way hash functions, or both). These techniques are persistent since they are directly and permanently associated with content. Their use is focused mainly on access control and piracy prevention. Encryption scrambles data into a form that can only be decrypted using a specific key. Encryption is also a key technology for any DRM system since it is used to ensure that public-key certificates owned by the buyer and the distributor are digitally signed by an authority. A handshake protocol makes sure that both sides have the secret keys that correspond to the public keys described in the license to use the digital media. Newer approaches such as broadcast encryption avoid the costly, in terms of data transmitted, two-way handshake with single way broadcast of public keys (Lotspiech, Nusser, & Pestoni, 2004). An interesting variation of DRM systems uses special plug-ins to decode digital information and communicate with the creator or the content provider. Nevertheless, this model suffers from the obvious lack of interoperability since there is no common

Figure 1. Five main technology categories of IPR protection



framework for encoding the information prior to its use. This situation has led to a number of different plug-ins, which are used with specific systems only and thus are inflexible. Plug-ins are usually content viewers or players. Although strong encryption techniques are successfully used in a variety of applications, encryption for IPR protection of digital media has some drawbacks. First of all, this kind of applications uses weaker encryption schemes because they require less calculations (and thus CPU power) for the user machine to decrypt digital information. This means that there is an increased possibility to break encryption keys. E-commerce applications also make use of previewing of audio or visual content. Encrypted media files are hard to preview or decrypted when used in large numbers.

Data hiding techniques are used for binding (embedding) information to digital content such as information about content owners, the buyer of the content, and payment information. The most popular and promising method in this category is watermarking. Digital watermarking subtly alters parts of the information that forms a digital work by inserting a weak signal. Usually, watermarks are not visible to humans, they can only be traced and linked to copyright information by special software. Watermarking does not preclude copying but may preclude playback on compliant devices (Wayner, 2002). This technique will be analyzed in detail in the following section.

The use of metadata is a relatively new method to overcome interoperability problems posed by different media formats and devices, the lack of structure and efficient modeling techniques for distributing, exploiting, and protecting digital content. The MPEG (moving pictures expert group) working group of ISO (international organization for standardization) has initiated a set of metadata standardization efforts in order to increase interoperability through the MPEG21 multimedia framework initiative and MPEG7 (Manjunath, Salembier, & Sikora, 2002).

MPEG-7 (multimedia content description interface) provides a common interface for describing multimedia content. MPEG-7's objective is to provide additional functionality to other MPEG standards by providing a set of description tools for multimedia artifacts that is, complex audio-visual units. It addresses interoperability, globalization of metadata resources and flexibility in data management. MPEG-7 can be classified into the group of standardized description schemes, but in contrast to many implementation schemes, it has not been

developed for a restricted application domain. It has rather been intended to be applicable to a wide range of application domains. Complex and customized metadata structures can be defined using the XML-based description definition language (DDL). Using XML, MPEG-7 provides descriptions about both static/spatial (text, drawings, images, etc.) and time-based media (such as video, audio, animation). Further content organization is possible into three major structures: hierarchical, hyperlinked, and temporal/spatial.

MPEG21 provides a framework for delivery and consumption of multimedia content to work together. It supports the whole content delivery chain from content creation to consumption by a wide range of devices and through a plethora of networks. Some of the key elements used include digital item declaration, identification, description, content handling, intellectual property management, digital item rights management, and others. Metadata enable rights management, a basic requirements for advanced IPR protection. For example, the MPEG21 REL (rights expression language), XrML (initially named DPRL by Xerox), has been chosen for wider adoption in DRM systems (Rosenblatt, Trippe, & Mooney, 2002). These standards in conjunction with new media coding standards such as JPEG2000 (for still images) and MPEG4 (for sound, video) bear great promise for IPR protection.

On the top of the pyramid, a new proposal for IPR protection, self protecting content (Rosenblatt, 2004) is placed. It was recently suggested as a solution to the ever-increasing problem of DRM interoperability and immature economics. This type of content includes special logic, which can decide by itself how it will be used by the client machine, which provides only basic functionality (Koenen et al., 2004). For example, an image encoded with a self-protecting standard is loaded in a palmtop. The logic is loaded into the palmtop, reads the appropriate information (ID, user acquired licenses etc.) and decides whether it will be viewed in full or reduced resolution, whether it will be copied or reproduced etc. It is obvious that apart from the logic encapsulated into the content, appropriate mechanisms need to be available to the user machine. These mechanisms should at least include a virtual machine for the code to run and a ROM for storing keys and licenses. If the end-user machine is a personal computer there is no obvious disadvantage but what happens when it is a CD-player or a home DVD device? Although the notion of self-protecting content is extremely innovative and attractive in many aspects, several shortcomings of technological, cultural and economic nature exist: there are no standards for encoding logic into content, what happens to the size of the media artifact when code is added to it, are the manufacturers of player devices willing to add new hardware to their products, are content creators willing to pay for new content creation tools? The self protecting content idea has already attracted criticism and it remains to be seen if it will be adopted in the future.

The previously mentioned technologies offer either a-posteriori or a-priori protection, their efficiency however cannot be estimated accurately. Current practices entail their combined use for stronger IPR protection, an approach used in systems designed for managing a wide range of functionalities: DRM systems.

DIGITAL RIGHTS MANAGEMENT SYSTEMS

Digital rights management is a set of technologies that enable the management of licenses for media artifacts throughout their lifecycle, in other words it provides a complete set of functionalities for managing IPR (Koenen et al., 2004). DRMs can either be stand-alone systems or part of a larger online selling system. They rely on licenses, which specify the content usage rules. Content is distributed with or without licenses but it cannot be used without them. Rules can be either attached or embedded to content or delivered independently (Cohen, 2003). It is important to note that DRM is about both digitally managing rights and managing digital rights (Rumb, 2003); modern DRM systems cover the full range of IPR management including the description, identification, trading,

protection, monitoring, and tracking of all forms of rights' usage. They are applied over both tangible and intangible assets including rights workflow, modeling, and owner relationships management (Iannella, 2001; Hwang, Yoon, Jun, & Lee, 2004).

Recent attempts to deploy DRM systems have shown that their success depends not only on technology but business issues as well. The underlying business model, actually the mechanism by which a business intends to generate revenue and profits, is of paramount importance. The business model defines the plans to serve customers involving both strategy and implementation. It greatly affects, and is affected, by the technology used. In the typical business model of a DRM system, the creator produces the digital content and provides the usage rules to a third party (authority) which is responsible for supervising its proper use. Distributors receive the content from the creators and distribute it through the appropriate channels (e.g., e-shops) to the end-users (buyers). In order for the buyer to use the content, the appropriate license must be obtained by the authority. This happens after the appropriate request is sent to the authority by the buyer. The transaction is concluded when the authority pays royalties to the creator. There is a plethora of DRM payment models: pay as you use, try-first buy-later, pay-per-view etc. Payment rules are closely connected to the way the content is supposed to be used.

Rosenblatt et al. (2002) discusses two definitions for DRM systems, the narrow and the broad. The narrow definition refers to systems that persistently protect content using mainly encryption techniques. 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. The broad definition includes the previously mentioned functionalities and further extends rights management. It includes definition, management, and tracking of rights (business rights, licensing, access tracking, etc.). A DRM system is defined by two kinds of architectures, the functional and the information architecture. The first one describes the basic functions of the system while the latter and most important, the modeling and flow of information inside the system (Rosenblatt et al., 2002). There are several variations of the functional architecture for DRM systems. In this work, we distinguish two as the most important: the create/manage/use model or CMU and the create/distribute/authorize or CDU. Although these two models have many functionalities in common, CDU functions are better mapped to the basic DRM business model used in practice (discussed in detail later in this section). A typical CDU functional architecture is, in general, comprised of three modules: creation/provision, distribution, and authorization (Figure 2). The creation/provision module organizes functions such as initial packaging of content and royalty distribution before initial provision. These functions define, create, and record the IPR of a digital artifact during its development. The distribution module is used for delivering content through e-distribution channels. This includes recording user rights, distribution paths, and managing transactions. Finally, authorization functions manage licensing (who is the owner of what information, use restrictions), monitoring of use and reporting to the IPR owners.

The information architecture models the flow of information between the modules of the functional architecture of the DRM system. In general, such an architecture must address three main problems: what are the main information taxonomies, how they are modeled and described and how IPR are defined and expressed. The information architecture of a classic DRM system is depicted in Figure 3.

The literature provides a relatively small but significant amount of works that deal with DRM architectures and systems. This implies that DRM systems are a new and difficult research problem. The most significant references include Park, Sandhu, and Schifalacqua's (2000) eight mechanism functional framework, Pucella and Wessman's (2002) rights definition

Figure 2. The functional architecture of a classic DRM system with three main components

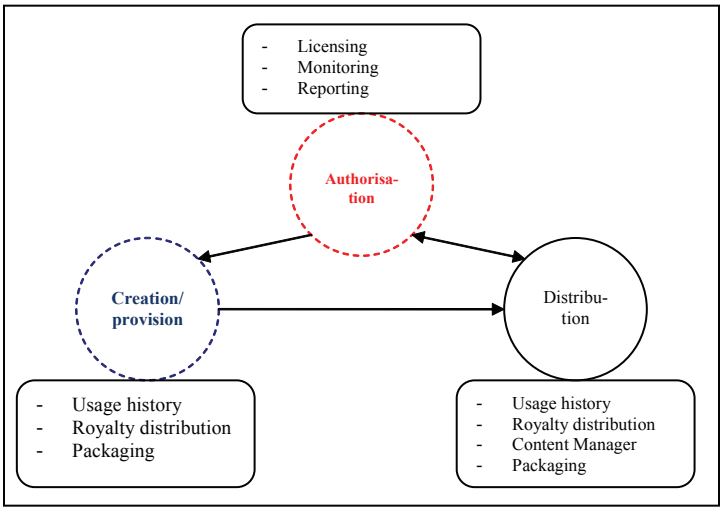
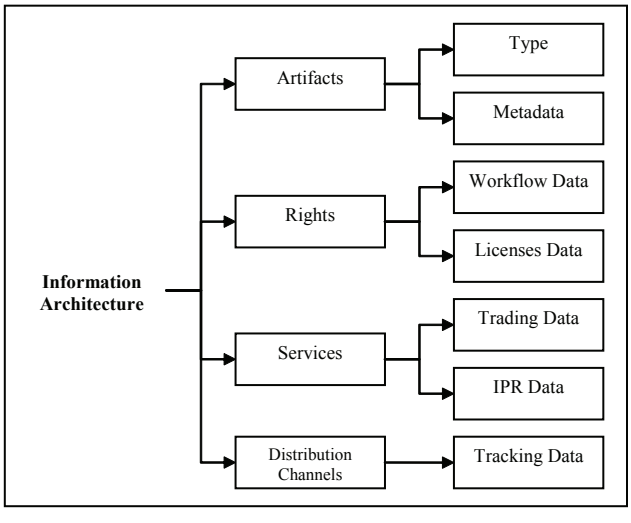


Figure 3. Information architecture of a classic DRM system (Modified from Iannella, 2001)



framework, Ianella's DRM architectures (2001), the balanced user-owner approach (federated DRM) of Martin et al. (2002) and the Imprimatur (1999) results. Commercial solutions include Adobe's e-book for pdf documents, IBM's EMMS, Real Network's RMCS, Microsoft's WMRM for audio/video, and Digimarc's family of products for video/audio and still images. A useful analysis of DRM business models, standards, and core technologies can be found in Koenen et al. (2004), Hwang et al. (2004), Rosenblatt et al. (2002). The increasing use of mobile devices has also initiated research efforts for mobile DRMs (MDRMs); technological

challenges in this area differ from classic DRM including mobile device limitations, bandwidth, usability, and other (Beute, 2005).

IPR protection using DRM systems has posed many non-technological questions. The universal request to raise standards of protection does not necessarily contribute to faster diffusion of new products and services (McCalman, 2005). Economists have raised questions mainly on two subjects, funding for developing common and viable solutions and fair use (Schneider, 2005). The first is about the willingness of large content and software providers to generously fund DRM standardization efforts and overcome interoperability issues. The second, concerns the increase in creation and transaction costs when IPR protection is too strong. Law experts have also pointed out the need for a balance of interests between private rights (the rights of the creators/owners) and the public interest (Maillard, 2004). Public policy should also ease the strong emotions posed to both content owners and end user; the first see DRM systems as a barrier to innovation and a threat to their use rights while the latter as their last defense against piracy. According to many, U.S. and EU legislation needs to be more consistent on this contentious topic (Felten, 2005; Towse, 2005).

DIGITAL WATERMARKING: A PROMISING SOLUTION FOR IPR PROTECTION

What is Watermarking?

Watermarking and authentication for digital media are relatively new technologies, descendants of research in the field of image processing of the previous decade. Digital watermarking has been proposed as a valid solution to the problem of copyright protection for multimedia data in a networked environment (Fotopoulos & Skodras, 2003). The two most important characteristics a watermarking scheme should provide are imperceptibility and robustness. A digital watermark is usually a short piece of information, which is difficult to remove, intentionally or not. In principle, an invisible mark is inserted in digital content such as digital images, video, and audio so that it can be detected at a later stage as evidence of copyright or it can generally be used against any illegal attempt to either reproduce or manipulate the content. The watermarking process includes two procedures, embedding and detection (Figure 4). In the embedding process, the original file is slightly altered by inserting a weak signal, producing a watermarked version. The detection process analyses the watermarked file in order to detect a watermark. Depending on the type of the watermark, the original file or a key may be needed to conclude the detection.

The main reason for the introduction of watermarking in IPR protection was the fact that digital artifacts are quite easy to duplicate, forge, or misuse in general. Watermarking is mainly focused toward the protection of the content's copyright while detection (authentication) aims at the verification of content, investigate if an image is tampered or not and if it is, to identify the locations that the alterations have occurred. For both technologies to succeed, side information needs to be embedded and/or linked with the original media file. This is obviously the reason why lossy compression schemes are often difficult to be used. Part of the watermarking or authentication information is unintentionally discarded along with insignificant parts of the original image information to achieve better compression.

Watermarking has been extensively researched in the past few years as far as common image formats are concerned. By identifying the rightful creator/owner, watermarks may be used to prevent illegal use, copy, or manipulation of digital content, as proof of ownership or tampering (Koenen et al., 2004). The problem that these techniques have to encounter is the robustness of the watermark against common processing tasks. Any attempt to remove the ownership information from the original image is called an "attack." For example, some common attacks for still images include filtering, compression, histogram modification, cropping, rotation, and downscaling. Recent studies

Figure 4. The watermarking process (embedding and detection) for a still image

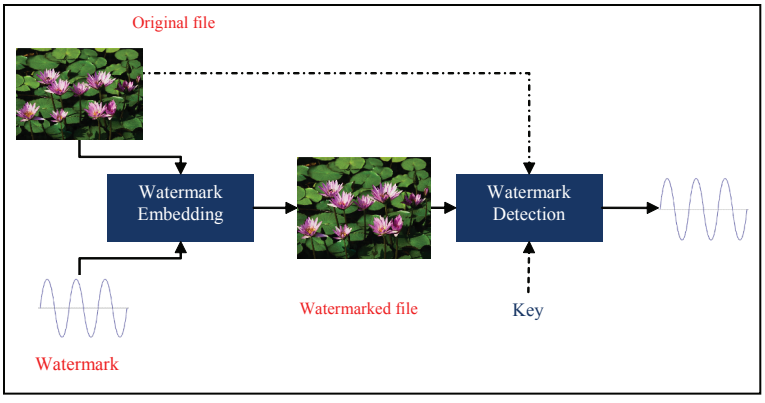


Table 1. Categorization of watermarking techniques

Watermark characteristic	Categories
Visibility	Visible, Invisible
Detection output	Readable, Detectable
Type	Logos, Serials, Pseudorandom noise sequences
Need for initial image for detection	Blind/public, Private
Embedding area	Spatial, Frequency
Taking advantage of special image characteristics	1st, 2nd generation

(Fetscherin & Schmid, 2003; Maillard, 2004) have shown that, apart from standard security technologies such as password protection and encryption, most recent DRM implementations use watermarking as well. Several commercial systems offer special crawling functions that scan the Internet for instances of the protected (watermarked) artifacts and produce usage reports. This method works only for online content and it might be successful in preventing piracy (Hwang et al., 2004). Several, sometimes overlapping, categorizations of watermarking techniques can be produced according to a set of characteristics (Fotopoulos et al., 2003) (Table 1).

Visibility categorization refers to whether a watermark is visible to humans (e.g., like a logo in an image) or invisible and as such, detectable only after analysis. The detection output characteristic refers to whether an invisible watermark can be read without the need for any additional information. For example, a visible watermark in the form of a logo or a text message is a readable watermark. These schemes are also encountered in the literature as public watermarks because they can be read without having a secret key. Detectable watermarks on the other hand, can be read only by authorized users (i.e., users that have a key that helps read the invisible mark inserted in digital media). These are called private watermarking schemes.

Watermark types are also used as a distinction characteristic. They include logos, serial numbers, and pseudorandom noise sequences. The first two categories are visible watermarks and the third one is invisible and detectable. Pseudorandom noise sequences are produced

by generators that are initialized using a specific key; without this key these sequences cannot be detected. Under certain conditions however, logos and serial numbers can also be detectable provided that they have been coded prior to the embedding procedure.

Categorization depending on the detection process includes watermarking schemes that need the original file to identify the watermark (private) and those that do not (blind or public). Blind watermarks are more interesting for researchers but not so robust to attacks. Hybrid schemes have also been proposed. Blind watermarks are best suited for resolving the rightful ownership in open environments such as the Internet because their use is not restricted to authorized users or content owners, who have the access to the original media. Moreover, requiring the original digital artifact to detect the watermark needs extra storage at the detector's side or extra bandwidth to transmit it from the embedder to the detector.

In the case of visual content, a most common categorization depends on the processing domain of the host image/ video-frame that the watermark is embedded in. One such category is the spatial domain group of techniques, according to which the intensity values of a selected group of pixels are modified. The other is the frequency domain group, where a group of the transform coefficients of the image/video frame are altered. Frequency domain approaches have been proved more successful for image watermarking. The transforms usually employed are the discrete versions of the Fourier, Cosine and Wavelet transform (DCT, DFT, and DWT) (Arnold, Wolthusen, & Schmucker, 2003; Fotopoulos et al., 2003; Voyatzis & Pitas, 2000). In these schemes, information is being transformed via one of the aforementioned frequency transforms and watermarking is performed by altering the resulting transform coefficients of the image.

In spatial watermarking a weak signal is embedded, usually in the lesser significant bits of multimedia data. For example, in a color image, the lesser significant bits of the information that codes every pixel are altered in one (usually the blue) or all color channels. In this case the watermark slightly alters the luminosity of each pixel. This category of techniques are quite fast to perform and do not seriously affect the quality of the original file. They are not however widely used because they are generally not robust to attacks; simple alterations to the original file result in great difficulties in detecting the watermark.

The Watermarking Process Detailed

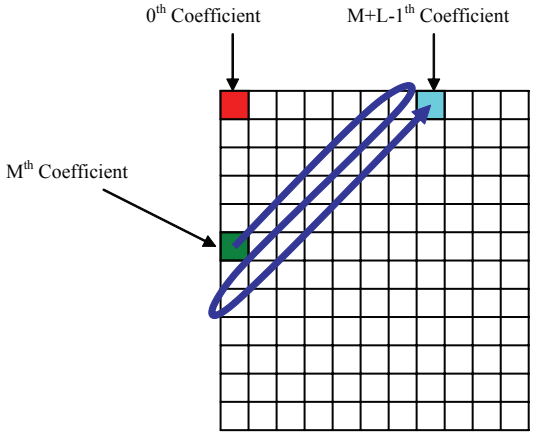
Watermarking in the frequency domain is considered quite robust by the scientific community and hence those methods are more popular. In these schemes digital information is first transformed to its equivalent representation in the frequency domain. For this purpose, a reversible transformation like FFT (forward fourier transform), DCT (discrete cosine transform), or DWT (discrete wavelet transform) is used. The output is a set of coefficients that describe the frequency content of the image data. A subset of the coefficients is chosen and altered using a simple mathematical equation with the following being one of the most commonly used:

$$C_{M+i}' = C_{M+i}(1 + ax_i) \text{ where i=1,2,3,...L}$$

with C being one of the selected image coefficients, M being the position of the first altered coefficient (assuming coefficients are reordered in a 1D-vector basis), L stands for the watermark length, a is the embedding strength and x_i is one of the watermark vector elements. The watermark is a pseudo-random noise sequence. Usually middle frequency coefficients are used, as shown in the following figure, which describes the selection strategy over a full frame image transform.

In such methods, the watermark is detectable. This means that the detector's calculates a number; if this number is above a specific threshold, then the image is marked, otherwise it is not. To obtain the output, the watermark-suspected test image is transformed with the same transform, the coefficient selection strategy is

Figure 5. Selection of middle frequency coefficients after image transform has been applied (for embedding)



applied and the detector's output is given by the following equation:

$$S(X,C)=\frac{1}{L}\sum_{i=1}^{L}x_i C_{i+M}$$

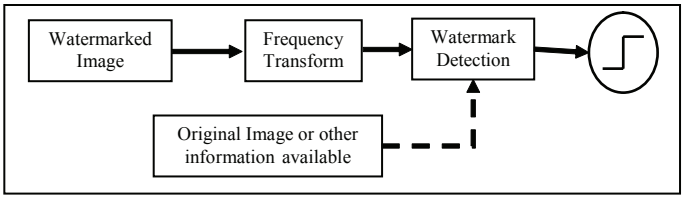
This procedure is described in Figure 6. The dashed line from the original image implies that in some methods, the original image is available and can be used (non-blind method) or that some other knowledge of the original image is given (informed method). If none is available, then the scheme is blind.

A significant question that occurs in such approaches is the number and the position of the altered coefficients set in the frequency representation of the image. Many different ideas have been proposed, however methods that process the image as a whole are more popular. In such cases the number of coefficients altered is in the order of a few thousands (e.g., 3000-15000 in the case of a 512×512 pixel image). The altered series is back-transformed to a digital representation of the initial object by applying a reverse transformation (e.g., the reverse FFT). The watermarked object is slightly different from the original. In any case, the differences should not be detectable by human vision.

Digital watermarking can be CPU demanding especially when large images, video or large numbers of artifacts are processed. Time is critical in online applications were delays increase costs and user drop-out rates. The complexity of frequency domain watermarking techniques is large. For example, for a square image of size N, the complexity of the discrete fourier and the cosine transform is O(N log N) while for the wavelet transform it is O(N). For large values of N, these transformations are becoming extremely demanding in terms of CPU cycles; however respective algorithms are suitable for distributed processing or parallelization. A common method is to partition the original object to pieces (e.g., an image to 16×16 tiles) and apply the previously mentioned procedure to these pieces.

Recently, a new approach for watermarking has been proposed, the so-called 2nd generation. First generation watermarking was either frequency or spatial and did not take into account any special characteristics of the original digital object. Second generation watermarking firstly analyses the digital artifact into smaller components (e.g., an image to the distinct objects it depicts) and then hybrid techniques appropriate for each situation are applied. These schemes are more complex but also more effective in

Figure 6. Detection procedure for a classical frequency based watermarking scheme



terms of robustness, visibility, and quality. Second generation watermarking also includes adaptive embedding and coding, asymmetric watermarking, detection with limited or zero previous knowledge and genetic programming schemes. They are not however suitable yet for commercial use.

Multiple Watermarking

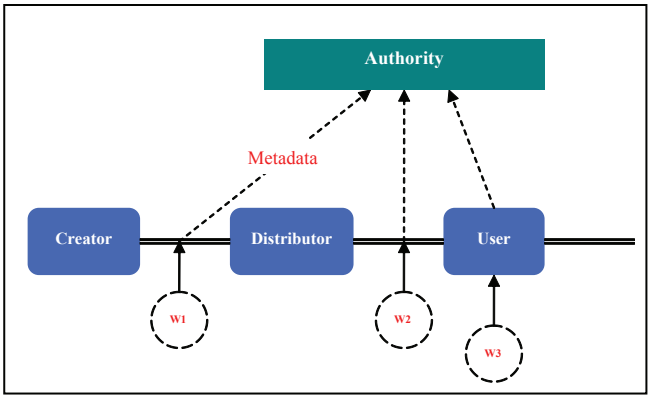
An interesting application of watermarking in e-commerce is multiple embedding/detection. A digital artifact can be marked more than once with different watermarks that can be efficiently and individually detected later. Multiple watermarks can be used to monitor distribution of digital content in e-commerce channels. A digital artifact may be marked with a watermark each time it is tunneled through a different distribution channel. Watermarks can be also associated with metadata (like keys corresponding to specific records in a database) which describe rights, owners, use, alterations to content, distribution channel characteristics etc. Figure 7 depicts a distribution monitoring example using multiple watermarking. The digital object is marked before distribution (*W1*); the initial watermark is associated with author and owner metadata and usage rules. Next, the object is tunneled through distribution channel *C1* (e.g., an e-shop), which inserts a second watermark *W2*, associated with its characteristics. A user acquires the object and, at this point, a third watermark *W3*, is embedded associated with new owner metadata. This procedure may be repeated for a finite number of steps. The distribution path from the developer to a user, along with usage, owner, and alteration information can be traced by retrieving watermarks and accessing the appropriate metadata. This metadata must be located in a central authority. Watermarking embedding should also follow the same standards in all steps of the above-mentioned procedure.

It must be noted that there is an upper limit for the number of watermarks that can be embedded in a digital object, before the quality of reproduction is significantly altered. In order to maintain a high quality of service, a consensus must be found between multiple watermarking and its perceptibility in the digital object. Multiple watermarks have already been proposed for the identification of the distribution path and/or to identify the end-user path of digital television broadcasts (Cheveau, 2002).

In the years to come, digital watermarking will be used even more as an IPR protection technique, combined with metadata methods. Metadata may be linked and not directly inserted into an image. For this purpose, a special kind of watermarking is used: annotation watermarking. Watermarks, combined with digital signature methods, may contain information about proprietary, copyright, the author, the user, the number of copies and/ or other important information.

Watermarking combined with new coding and metadata standards such as JPEG2000 creates new possibilities for the IPR protection industry and have already attracted much attention by the scientific community (Vassiliadis, Fotopoulos, Ilias, & Skodras, 2005). The JPEG2000 coding standard for still images offers features such as region of interest coding, scalability, error resilience, and visual frequency

Figure 7. Embedding of multiple watermarks for monitoring distribution channels in an e-business environment



weighting (Taubman & Marcellin, 2002). Although all of the previously mentioned features of this compression standard are very important, the application of watermarking in JPEG2000 compressed images is closely related with its IPR capabilities. These capabilities include the embedding of XML-formatted information into the image file in order to annotate/link image data with metadata. These metadata are associated with the image vendor, the image properties, the existence of IPR information in the image data etc. The new format (JP2) gives the opportunity to accompany the data that correspond to the image with extra metadata but it doesn't replace the watermarking mechanisms that are used today for copyright protection and authentication. It rather complements them.

In order to address the increasing need for security, the international community is already researching the incorporation of IPR protection characteristics within the JPEG2000 standard. This initiative will produce JPEG 2000 Secured (JPSEC) also known as Part 8 of JPEG2000 (JPEG, 2000). Applications addressed by JPSEC include, among others, encryption, source authentication, data integrity, conditional access, ownership protection, etc. It is expected that the new standard will be available by 2007.

DISCUSSION: TECHNOLOGY COMPARISON AND FUTURE TRENDS

DRM systems inherit the advantages and weaknesses of the technologies they use. The complexity of a DRM system is greater than the sum of the complexities of its parts: the complexity of the individual system components that use different technologies. Such complex systems have more pressing requirements for higher levels of security, interoperability, and usability than any simple system (i.e., a system that uses one or more technologies that are highly compatible with each other).

Security is naturally one of the main concerns in DRM system adoption. Perfect security cannot be offered by any DRM system, partly because "perfection" requires the adoption of costly methods. Furthermore, the mosaic of technologies comprising a DRM system deteriorate security; connection points between different system components are often security holes in the whole system. However, not all methods are used in a DRM system since they are usually linked to specific functionality. For example, some technologies either prevent the illegal use and other the re-use of digital content. A DRM implementation may use only one of them.

Technologies that prevent illegal re-use of content include watermarking and fingerprinting techniques. Their functionality within a DRM system is different; watermarking is used for the assertion of rights while fingerprinting for content identification during searching in large corpora. The advantage of watermarking is the fact that it persistently marks content, possibly more than once (multiple watermarks). However, watermarks are not always persistent to content changes such as compression, cropping, rotation and other content processing functions. Durability depends on the specific watermarking technique and is often connected to increased CPU costs. Another weakness is the so-called deadlock problem where a false watermark is inserted into the content and ownership is difficult to assert (Kwok, 2003). The good thing in such a situation is that no illegal watermark can stand up legally as ownership evidence.

Technologies that prevent illegal use of content include encryption, cryptography and metadata use. The later is usually combined with some other technique. Encryption of content uses symmetric key algorithms such as AES, RC4, or RSA. It is used to encrypt licenses and identities and has significant value to ensure content integrity. Portability is major concern when using encryption. Encrypted content may be compatible only with a single computer/device (e.g., the computer that downloaded it from the Internet). This content is not portable and thus cannot be used in other devices decrease its value to the users. Encryption methods that prevent cross-device or cross- media copying (e.g., from a hard disk drive to a CD) have resulted in hardware incompatibilities. Table 2 summarizes the pros and cons of the main technologies used in DRM systems.

Agreeing on industry-wide standards is a major issue in DRM that is not yet resolved. Common standards are especially important for metadata, since their use enables application-to-application interaction and thus task automation. Besides ISO, other standardization bodies continue to work on media standards in order to provide a common approach to enable interoperability, better quality, and efficiency under specific constraints. W3C's standardization effort is wider known as the semantic web. The "semantic Web" aims to make A2A (application to application) interaction possible through metadata. XML, RDF, RDF(S), and ontologies are some of the technologies that will possibly make the semantic Web a reality. Somewhat similarly to MPEG's standards, the semantic Web is based on XML/RDF. The schema language adopted by W3C is RDF

Table 2. A comparison of the main security technologies/methods used in DRM systems

Enabling Technology	Relation to content	DRM task	Advantage	Weakness
Watermarking	Prevention of illegal re-use	Assertion of rights	Persistence, multiplicity	Deadlock
Cryptography	Prevention of illegal use	Containers	Ensures content integrity	Flexibility, portability
Fingerprinting	Prevention of illegal re-use	Content identification	Alternative search mechanism	High false reject rates
Metadata	Content identification/ description	Rights expression	Flexibility	Lack of common standards

schema and OWL. A popular misconception is that both efforts are compatible or supplement each other, since they use XML as a basis. This is not true yet. Although the general goals of W3C are the same with MPEG group's the approach is different. First of all, W3C works on the Web context and does not pay so much attention to the content of the multimedia itself. For example, low level, visual feature descriptions are not explicitly taken into account in the sense that there are no explicit descriptors for them as in MPEG-7. Another obstacle is the fact that the conversion from the schema language to XML is "lossy." This means that the reverse conversion (from XML to the schema language) is possible but the description may differ significantly. Parsing is also difficult. Metadata descriptions in XML derived from MPEG-7 DDL may not be parsable by semantic Web tools. MPEG's effort is more concentrated in the digital media domain, and as such it can be considered as a subset of the semantic Web effort, although this is not entirely true. For example, MPEG-7 can be considered as an ontology and an ontology language at the same time. These differences affect IPR management in the e-business domain as well. Depending on the type of metadata used, different functionalities are supported. In general, when dealing with digital media, the MPEG's approach is more appropriate because it is focused on the specific domain.

Standardization is a difficult process and in the IPR field many attempts started with enthusiasm only to run out of steam (actually support by large vendors) a couple of years later. Current efforts seem to be more stable as they rely on advances on complementary research fields such as multimedia and computer/network security (Table 3). Standards should be used as a framework and not a panacea to technology problems (Cheng & Rambhia, 2003). Especially for DRM systems, fair use, interoperability, and usability are key requirements. The viability of a standard strongly depends by the support provided by large DRM market players from the first steps of its specification to its final deployment.

DRM has to deal with not only technical problems, but with the increased expectations of the market as well. Increased bandwidth has enabled the exchange of digital content through the WWW and peer to peer networks. Large DRM implementations (i.e., systems with a full set of functionalities) are not used extensively yet, especially from small-size users such as small and medium companies or individuals. However, subsets of DRM functionalities have begun to penetrate the market as lightweight content protection systems. The partial failure of large DRM solutions' adoption has not eliminated the need of the market for content protection. Besides the move towards more lightweight and cost-effective solutions, new trends involve the seamless embedding of DRM functions into operation systems, mobile DRM solutions, and technologies/business models for peer to peer networks.

The inclusion of DRM functions as standard operation system functions will probably start with Microsoft's Vista (formally Longhorn) operating system, the next version of Windows OS that will hit the market probably in 2007. DRM support for multimedia will be heavier than ever and already some features have already drawn heavy criticism: HD-DVD and Blu-ray videos will appear in low resolution if no licenses

Table 3. Standards currently used in main DRM mechanisms

DRM mechanism	Standard
Transmission and storage	MPEG-4, JPEG2000, OpenEBook
Rights Expression	XrML, XMCL, ODRL
Authentication	X.509, PGP, S/MIME
Metadata description	XML, RDFS, OWL

for this content are acquired. Similar DRM features are expected to be added to operating systems such as OS X in the near future.

3G mobile networks is another recent advance that opened the way for digital content distribution to mobile users. Cell phones and PDAs pose new requirements in the IPR/DRM area and architectures, business models and standards need to be reconsidered in order to be applied successfully. One consideration is the fact that mobile hardware and software architectures are more closed than their Internet counterparts and quite different for each manufacturer. Thus, the impact of an attack to a specific mobile device or software is significantly reduced by diversity. In contrast, the personal computer market enjoys a well known software and hardware architecture, not necessarily an advantage when dealing with content security. However, diversity prohibits the adoption of 'one-size-fits-most' solutions. Another consideration is hardware capabilities of mobile devices, although greatly enhanced in the past few years, they do not permit the use of sophisticated DRM software. Costly watermarking and cryptographic algorithms cannot be applied in these devices so less CPU-intensive techniques need to be applied. A significant advantage for mobile-DRM solutions is the actual lack of user anonymity in mobile networks. The large majority of users in mobile cell phone networks is known by name (and not by IP as in the case of the Internet), and this is a significant prohibitor for illegal acts. Additionally, owners, users and licenses can be more easily recognized and managed. The area of mobile-DRM is fairly new and standardization efforts have only recently begun to take place.

Besides the WWW and mobile networks, another computing paradigm will inevitably integrate DRM: peer to peer (P2P) (Rosenblatt, 2003). P2P is a relatively new, highly distributed computing paradigm that enables sharing of resources and services through direct communication between peers (Androutsellis-Theotokis & Spinellis, 2004). Extending the traditional model where most computers on a network act as clients, P2P introduces the concept of the simultaneous client/server mode: peers act both as clients and as servers. P2P networks are responsible for the distribution of huge volumes of pirated digital content especially damaging the music and film industry. The main difference between the P2P and the client-server model (used in the WWW) is its distributed business model while basic technologies remain the same. A social factor that prohibits the adoption of content protection technologies in P2P networks is the unwillingness of the users to perform transactions that are controlled or monitored in any way.

CONCLUSION

The extensive use of digital media in networked applications increases security requirements. The protection of IPR of digital media is increasingly gaining attention as a prominent research area. Increased concern by companies and academia has led to the development of numerous methods and techniques that manage and protect IPR. DRM will probably stand on the forefront of technology debates for the years to come.

In this work, we surveyed recent developments in the area of IPR protection of digital content distributed through e-commerce channels. DRM is one of the most important and complete frameworks that enable end-to-end management of digital rights through the media lifecycle. Enabling technologies for DRM systems include, among other, watermarking, an information hiding technique. Watermarking can be used for embedding or connecting usage rules in/with the content itself. The true value of watermarking lies in its multiplicity, that is its ability to embed and detect more than one watermark to a single digital artifact without decreasing its quality. Watermarks travel with content through the distribution channels and they are resistant to its altering. Combined with metadata stored in central or distributed repositories, watermarks enable tracking and managing of legal rights online. A relatively small number of software vendors has already formed an initial group for exploiting digital watermarking for IPR protection. Some of

these companies are spin-offs coming from Universities or research institutions and others are venture capital efforts. Large companies such as NEC and IBM have also expressed their intension to use this technology.

New standards offer new possibilities for IPR protection and DRM systems that involve watermarking, and may lead to the development of more advanced security services. The popularity of mobile devices and P2P networks increases the pressure for the development of new DRM business models and concrete standards. Standardization efforts, both in content representation and metadata, will hopefully contribute towards more secure transactions and media use.

In conclusion, it seems that in the next years the field of IPR protection in e-business will attract even more interest from the research community. The increasing adoption of watermarking as a main protection mechanism by important vendors denotes its strategic role in IPR protection.

ACKNOWLEDGMENT

This work was funded by the European Social Fund, Operational Programme for Educational and Vocational Training II (EPEAEK II), programme Pythagoras (contract no. 89188).

REFERENCES

Arnold, M., Wolthusen, S. D., & Schmucker, M. (2003). *Techniques and applications of digital watermarking and content protection*. Artech House Publishers.

Androutsellis-Theotokis, S., & Spinellis, D. (2004). A survey of peer-to-peer content distribution technologies. *ACM Computing Surveys*, *36*(4), 335-371.

Beute, B. (2005). Mobile DRM-usability out of the door? *Telematics and Informatics*, *22*(1/2), 83-96.

Cheng, S., & Rambhia, A. (2003). DRM and standardization--Can DRM be standardized? In E. Becker et al. (Eds.), *Digital rights management* (pp. 163-177). Springer-Verlag Lecture Notes in Computer Science 2770.

Cheveau, L. (2002). *Choosing a watermarking system for digital television--the technology and the compromises*. European Broadcasting Union, Switzerland IBC Report. Retrieved July 2005 from http://www.broadcastpapers.com/asset/IBCEBUWatermarking.pdf

Cohen, J. E. (2003). DRM and privacy. *Communications of the ACM*, *46*(4), 46-49.

Eskicioglu, E. M. (2003). Protecting intellectual property in digital multimedia networks. *Computer*, *36*, 39-45.

Felten, E. W. (2005). DRM and public policy. *Communications of the ACM*, *48*(7), 112.

Fetscherin, M., & Schmid, M. (2003). Comparing the usage of digital rights management systems in the music, film, and print industry. Proceedings from the 5th *International Conference on Electronic Commerce* (pp. 316-325). Pittsburgh, PA: ACM.

Fotopoulos, V., & Skodras, A. N. (2003). Digital image watermarking: An overview. *EURASIP Newsletter*, *14*(4), 10-19.

Hwang, S. O., Yoon, K. S., Jun, K. P., & Lee, K. H. (2004). Modelling and implementation of digital rights. *Journal of Systems and Software*, *73*(3), 533-549.

Iannella, R. (2001). Digital rights management (DRM) Architectures. *D-Lib Magazine*, *7*(6). Retrieved July 2005, from http://www.dlib.org/dlib/june01/iannella/06iannella.html

Imprimatur. (1999). Imprimatur business model, Version 2.1. Retrieved July 2005. from http://www.imprimatur.net

International IPR Alliance. (2005). Special 301 recommendations. Retrieved July 2005, from http://www.iipa.com/pdf/2005SPEC301LOSS.pdf

JPEG 2000 Secured. (JPSEC) (2000). Retrieved July 2005 from http://www.jpeg.org/jpeg2000/j2kpart8.html

Koenen, R. H., Lacy, J., MacKay, M., & Mitchell, S. (2004). The long march to interoperable digital rights management. *Proceedings of the IEEE*, *92*(6), 883-897.

Kwok, S. H. (2003). Watermark-based copyright protection system security. *Communications of the ACM*, *46*(10), 98-101.

Lotspiech, J., Nusser, S., & Pestoni, F. (2004). Anonymous trust: Digital rights management using broadcast encryption. *Proceedings of the IEEE*, *92*(6), 898-909.

Maillard, T. (2004). Towards digital rights and exemptions management systems. *Computer Law and Security Report*, *20*(4), 281- 287.

Manjunath, B. S., Salembier, P., & Sikora, T. (2002). *Introduction to MPEG-7: Multimedia content description interface*. Wiley Press.

Martin, M., Agnew, G., Kuhlman, D. L., McNair, J. H., Rhodes, W. A., & Tipton, R. (2002). Federated digital rights management–a proposed DRM solution for research and education. *D-Lib Magazine*, *8*(7-8). Retrieved July 2005, from http://www.dlib.org/dlib/july02/martin/07martin.html

McCalman, P. (2005). International diffusion and intellectual property rights: An empirical analysis. *Journal of International Economics*, *67*, 353-372.

Memon, N., & Wong, P. W. (1998). Protecting digital media content. *Communications of the ACM*, *41*(7), 34-43.

Park, J., Sandhu, R., & Schifalacqua, J. (2000). Security architectures for controlled digital information dissemination. *Proceedings from ACSAC 2000: The Annual Computer Security Applications Conference*, 224, New Orleans, Louisiana: IEEE Computer Society.

Pucella, R., & Weissman, V. (2002). A logic for reasoning about digital rights. *Proceedings from CSFW'15: The 15th IEEE Computer Security Foundations Workshop* (pp. 282-294), Cape Breton, Canada: IEEE Computer Society.

Rosenblatt, B. (2003). Integrating DRM with P2P networks: Enabling the future of online content business models. Retrieved March 2006, from http://www.drmwatch.com/special/article.php/3112631

Rosenblatt, B. (2004). Analysis of CRI's self protecting digital content. Retrieved July 2005, from http:// www.drmwatch.com/special/article.php/3095031

Rosenblatt, B., Trippe, B., & Mooney, S. (2002). *digital rights management—Business and technology*. M&T books.

Rumb, N. (2003). Digital rights management: Technological aspects. In E. Becker et al. (Eds.), *Digital rights management* (pp. 3-15). Springer-Verlag Lecture Notes in Computer Science 2770.

Samuelson, P. (2005). The Supreme Court revisits the Sony Safe Harbor. *Communications of the ACM*, *48*(6), 21- 25.

Schneider, P. H. (2005). International trade, economic growth, and intellectual property rights: A panel data study of developed and developing countries. *Journal of Development Economics*, *78*(2), 529-547.

Taubman, D. S., & Marcellin, M. W. (2002). *JPEG2000: Image compression fundamentals, standards, and practice*. Kluwer Academic Publishers.

Towse, R. (2005). Economics and copyright reform: Aspects of the EC directive. *Telematics and Informatics*, *22*, 11-24.

Vassiliadis, B., Fotopoulos, V., Ilias, A., & Skodras, A. N. (2005). protecting intellectual property rights and the JPEG2000 coding standard. In P. Bozanis & E. N. Houstis (Eds.), *Advances in informatics:10th Panhellenic Conference on Informatics* (pp. 705-715). Springer-Verlag Lecture Notes in Computer Science, 3746.

Voyatzis, G., & Pitas I. (2000). Image watermarking for copyright protection and authentication. In Bovik, A. (Ed.), *Handbook of image & video processing* (pp.733-745). Academic Press.

Wayner, P. (2002). *Disappearing cryptography*, *(2nd ed.). Information hiding: Steganography and watermarking*. Morgan Kaufmann.

Bill Vassiliadis obtained his diploma and PhD from the Department of Computer Engineering and Informatics of the University of Patras (1995 and 2004, respectively). He is currently working as a post-doctoral research fellow at the Digital Systems and Media Computing Lab of the Hellenic Open University. His current research interests include information systems design and information management. He has published more than 50 papers in international conferences and journals.

Vassilis Fotopoulos was born in Patras, Greece, in 1972. He received his BSc in physics, MSc in electronics and PhD in digital image watermarking (1995, 1998, and 2003, respectively), all of them from the Physics Department of Patras University, Greece. Currently, he is a tutor of the Hellenic Open University. His research interests include digital watermarking, DRM systems and image compression algorithms. He is a member of SPIE and IEEE's CAS, SP and Computer societies and reviewer for IEE's Electronic Letters, SPIE's Journal of Optical Engineering, Journal of Electronic Imaging, *and for the ICIP and EUSIPCO conferences.*