

Protecting Intellectual Property in Digital Multimedia Networks



Digital content providers can choose from a range of new technologies to reproduce, store, and distribute their intellectual property. Protecting their IP from piracy, however, remains a major issue.

Ahmet M. Eskicioglu
Brooklyn College of
the City University
of New York

Recent advances in digital communications and storage technologies have brought major changes for consumers. Magnetic and optical storage capacity, for example, is much higher today than it was a few years ago. Today's basic personal computer system has 40 Gbytes of magnetic hard disk storage, and, although a DVD (digital versatile disk) is the same physical size as a CD, it's faster and can store much more audiovisual data in optical form—from 4 to 17 Gbytes (two to eight hours of video).

Moreover, Internet connection speeds are much faster. Cable modems and asymmetric digital subscriber lines dominate the industry. The emerging very high bit-rate DSL (VDSL) connection, with speeds of up to 52 Mbps, will provide sufficient bandwidth for entertainment networks.

These improvements in computers and communications networks are radically changing the economics of intellectual property reproduction and distribution. IP owners can exploit new ways to reproduce, distribute, and market their IP. A major problem with current digital distribution and storage technologies, however, is the formidable threat of piracy.

UNIVERSE OF SYSTEMS

The “universe” of digital content distribution systems offers five primary means of delivery to con-

sumers: satellite, cable, terrestrial, the Internet, and prerecorded media (optical and magnetic). Content providers use these systems to distribute and store copyright-protected entertainment content.

To ensure end-to-end security, a distribution system must provide

- secure content distribution,
- secure access key distribution,
- authentication of source and sink consumer devices in home networks, and
- renewability of content protection systems.

The “Key Players in Content Protection” sidebar lists the organizations behind the efforts to identify and implement secure solutions.

In the past two decades, collaborative projects have resulted in protection systems in commonly used digital networks. However, many problems pertaining to the security of multimedia content distribution and storage continue to challenge the motion picture, consumer electronics, and information technology industries.

IP-BASED INDUSTRIES IN THE US ECONOMY

IP's growing importance has led some countries to evaluate the role of IP-based industries in their economies. The International Intellectual Property Alliance (www.iipa.com), a private-sector coalition

Key Players in Content Protection

- Advanced Television Systems Committee (ATSC), www.atsc.org
- CableLabs, www.cablelabs.com
- Copy Protection Technical Working Group (CPTWG), www.cptwg.org
- Digital Video Broadcasting Project (DVB), www.dvb.org
- DVD Forum, www.dvdforum.org
- Electronics Industries Alliance (EIA), www.eia.org
- Internet Engineering Task Force (IETF), www.ietf.org
- Motion Picture Association of America (MPAA), www.mpa.org
- North American Broadcasters Association (NABA), www.nabanet.com
- Recording Industry Association of America (RIAA), www.riaa.org
- Society of Cable Telecommunications Engineers (SCTE), www.scte.org

formed in 1984, represents US copyright-based industries in bilateral and multilateral efforts to improve international protection of copyrighted materials. Each of the six IIPA trade associations represents a significant segment of the US copyright community. These member associations represent more than 1,100 US companies producing and distributing copyright-protected materials throughout the world.

In 1990, the IIPA commissioned Economists Incorporated (www.ei.com) to measure the economic impact and trade role of a collection of industries related through their reliance on copyright protection. The EI report defined and classified US copyright-based industries and provided statistics on their contribution to the country's gross domestic product, employment, and trade.

The US copyright industries are divided into four groups:

- *Core* industries generate, produce, and disseminate new copyrighted material as their primary function.
- *Partial* industries offer copyrighted material as only part of their product range.
- *Distribution* industries supply copyrighted materials to businesses and consumers.
- *Copyright-related* industries produce and distribute products used wholly or principally in conjunction with copyrighted materials.

Core copyright industry products include

- all types of computer software, including business applications and entertainment software;
- theatrical films, television programs, home videos, and digital representations of audiovisual works;
- music recordings, including records, CDs, and audiocassettes; and
- textbooks, trade books, reference and profes-

sional publications, and journals (both electronic and print media).

“Copyright Industries in the US Economy: The 2002 Report,”¹ an update of eight prior reports, details the importance of copyright industries to the US economy based on three economic indicators:

- *Value added to GDP.* In 2001, US core copyright industries accounted for 5.24 percent (\$535.1 billion) of the country's GDP. Between 1977 and 2001, the industries' share of the GDP grew more than twice as fast as the rest of the US economy (7 percent versus 3 percent).
- *Share of national employment.* Between 1977 and 2001, employment in the US core copyright industries grew from 1.6 percent (1.5 million workers) to 3.5 percent (4.7 million workers) of the US workforce. Average annual employment grew more than three times as fast as the rest of the US economy (5 percent versus 1.5 percent).
- *Revenues generated from non-US sales and exports.* In 2001, the US core copyright industries estimated their non-US sales and exports at \$88.97 billion, more than all other major industry sectors—chemical and allied products; motor vehicles, equipment, and parts; aircraft and aircraft parts; electronic components and accessories; and computers and peripherals.

These figures indicate the significance of copyright industries to the US economy.

COPYRIGHT PIRACY AND PROTECTION

Despite the fast growth of copyright-based industries, annual losses due to piracy (not including Internet piracy) of copyrighted materials are estimated to be as high as \$22 billion (www.iipa.com/aboutiipa.html). Inexpensive and accessible reproduction technologies make it easy for individuals in other countries to pirate copyrighted materials.

IIPA works with the US and other governments as well as private sector representatives to track copyright legislative and enforcement developments in more than 80 countries. In addition to discouraging piracy through legislation and enforcement, IIPA promotes technological and cultural development in these countries and encourages local investment and employment.

Special 301, an IIPA annual review, requires US trade representatives to identify countries that deny

adequate and effective IP protection or deny fair and equitable market access to persons relying on IP protection. Congressional passage of the Omnibus Trade and Competitive Act of 1988, which amended the Trade Act of 1974, created the review. IIPA's 2003 *Special 301 Report on Global Copyright Protection and Enforcement* states that in 2002, deficiencies in the copyright regimes of 56 countries caused US copyright industries to lose more than \$9.2 billion in trade due to piracy. Table 1 lists the 2002 trade losses for five copyright-based industry sectors.

A 14 February 2003 letter from IIPA to the US Trade Commission argued that “copyright gives creators the basic property rights that enable them to authorize and control the copying, distribution, performance, and display of the works they create.” According to the letter, copyright protection also

- develops local economies,
- creates local jobs and income,
- promotes non-US investment,
- generates tax revenue,
- establishes a structure for commercial practices, and
- supports integration with the world trading system.

As we transition from analog to digital technologies, robust copyright and content protection technologies and their enforcement become indispensable to the growth of the economy in the US and abroad.

The Computer Science and Telecommunications Board's “Digital Dilemma—Intellectual Property in the Information Age”² is a major study that assesses issues related to the nature, evolution, and use of the Internet and other networks and to the generation, distribution, and protection of network-accessed content. Experts from industry, academia, and the library and information science community formed the study committee. In addition to its expert deliberations, the committee solicited input and discussion from a wide range of institutions and individuals.

After carefully analyzing the technical tools and business models for protecting IP, the committee concluded:

There is great diversity in the kinds of digital intellectual property, business models, legal mechanisms, and technical protection services possible, making a one-size-fits-all solution too rigid. Currently, a wide variety of new models and mechanisms is being created, tried out, and in some

Table 1. 2002 estimated US trade losses due to copyright piracy in 56 countries.

Industry	Estimated losses (in billions)
Motion pictures	\$ 1,322.3
Music	2,142.3
Business software	3,539.0
Entertainment software	1,690.0
Books	514.5
Total	9,208.1

cases discarded, at a furious pace. This process should be supported and encouraged to allow all parties to find models and mechanisms well suited to their needs.

MULTIMEDIA CONTENT PROTECTION

Three of the most important objectives of information security are

- *confidentiality*, to protect information from unauthorized disclosure;
- *data integrity*, to ensure that information has not been manipulated in an unauthorized way; and
- *authentication*, to determine both the identity of the sender and the sender's active participation in a protocol (entity authentication) and to determine the identity of the sender (message authentication).

Message authentication also includes evidence of data integrity: If information is modified during transmission, the sender can't be the originator. Multimedia communications or storage systems should meet some or all of these objectives.

Table 2 lists the architectures for protecting multimedia content in popular digital domains. Content providers provide full feedback—criticism, suggestions, and so on—to the developers of private security systems in these architectures. There are two primary reasons for this privacy:

- unpublished cryptographic algorithms and systems may provide additional security, and
- privately defined systems with IP require licensing.

The Internet Engineering Task Force (IETF) Multicast Security (MSEC) Working Group, with support from many research institutions, addresses secure multicast communication.

Table 3 summarizes the major developments in protecting copyrighted content. These systems can be categorized as secure distribution networks or secure digital home networks.

Content owners approach the IP-protection problem from three avenues: law, technology, and business models.²

Table 2. Multimedia content protection architectures for different digital domains.

Type of network	Protection system	Description
Digital home network	Content protection system architecture	CPSA is a collection of content protection technologies that includes two groups of systems for DVD and digital interface protection (www.4centity.com).
Satellite, cable, and terrestrial	Conditional access	A CA system allows access to services based on payment or other requirements such as identification, authorization, authentication, registration, or a combination of these. ³
Internet	Digital rights management: unicast-based	A DRM system protects, distributes, modifies, and enforces the rights associated with the use of digital content. Currently, DRM is used for Internet distribution, but the functional difference between CA and DRM is lessening. Unicasting refers to a point-to-point communication between a server and a client device. ³
	Digital rights management: multicast-based	Multicasting is an efficient distribution mechanism from a source to a large group of clients. In secure multicast communication, all members of a group share a group key. ⁴

While changing public understanding of consumer rights, the new copyright legislation has generated a substantial amount of discussion about the limitations on copying digital content.

Given sufficient resources, professional hackers can defeat technical protection, made possible by encryption and watermark technologies. The primary purpose of such protection, however, is to deter ordinary customers who might engage in illegal activity intentionally or through ignorance.

Because of the potential difficulties associated with technical measures and legal enforcement, content owners can follow a third avenue to minimize piracy-related losses. By carefully considering the nature of new digital products, market trends, and consumer needs, content owners can develop creative business models for IP distribution.

These three complementary tools should help resolve the complex web of legal, social, cultural, and economic issues surrounding IP, IP owners, and consumers.

OPEN ISSUES

In recent years, the motion picture, consumer electronics, and information technology industries have achieved considerable success in understanding the complexity of the IP protection problem. Despite the many efforts to protect copyrighted material, an array of legal and technical issues remains.

Legal issues

The World Intellectual Property Organization is an intergovernmental United Nations organization with 179 current member states. Headquartered in Geneva, WIPO administers 23 international treaties dealing with different aspects of IP protection. The WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT), which update international copyright standards for the Internet era, went into effect in 2002. To fully implement these treaties, countries

must upgrade their copyright laws. Some laws require only minor changes, but upgrading others will involve substantial revisions.

The 1998 Digital Millennium Copyright Act, a comprehensive reform of US copyright law, implements WCT and WPPT and contains additional provisions addressing related matters. Two key DMCA topics are circumvention of copyright protection systems and fair use in a digital environment. The act has received strong criticism, particularly for its vague or inaccurate language regarding anticircumvention provisions.²

Senator Fritz Hollings of South Carolina introduced the Consumer Broadband and Digital Television Promotion Act to the US Congress in March 2002. CBDTPA seeks “to regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes.”

The Home Recording Rights Coalition (HRRC) criticized CBDTPA for inviting undefined and unlimited regulation of digital consumer devices. Jack Valenti, president and chief executive officer of the Motion Picture Association of America (MPAA), supported the bill, claiming it would serve consumers’ long-term interests by calling on the information technology, consumer electronics, and copyright industries to negotiate solutions to digital piracy. Hilary Rosen, president and CEO of the Recording Industry Association of America (RIAA), noted that the bill sent an unmistakable signal about the importance of protecting digital music and other content from piracy.

Technical issues

The technical solutions listed in Table 3 provide protection in content distribution to and within home networks. A complete solution set must address a number of problems, including the following.

Table 3. Major developments in IP protection.

Solution	Media protected	Protection technology	Authentication	Renewability
<i>Content protection system architecture (CPSA)</i>				
Content scramble system (CSS; www.dvdcca.org)	Video on DVD-ROM	Encryption	Mutual authentication between the DVD drive and the PC	Yes
Content protection for prerecorded media (CPPM; www.4centity.com)	Audio on DVD-ROM	Encryption	Mutual authentication between the DVD drive and the PC	Yes
Content protection for recordable media (CPRM; www.4centity.com)	Video or audio on DVD-R/RW/RAM	Encryption	Mutual authentication between the DVD drive and the PC	Yes
4C/Verance watermark (www.verance.com)	Audio on DVD-ROM	Watermark	None	No
Video watermark	Video on DVD-ROM/R/RW/RAM	Watermark	None	No
Digital transmission content protection (DTCP; www.dtcp.com)	IEEE 1394 serial bus	Encryption	Sender and receiver	Yes
High-bandwidth digital content protection (HDCP; www.digital-CP.com)	Digital visual interface (DVI) and high-definition multimedia interface (HDMI)	Encryption	Receiver	Yes
<i>Satellite</i>				
Privately defined by service providers and CA vendors, such as DirecTV and Dish Network	Broadcast content	Encryption; watermarking could monitor broadcast advertisements	None	Yes
	Interface between the NRSS security module and the CE host device		Sender and receiver	Yes
	Interface between the CE host device and the display unit		Sender and receiver	Yes
<i>Cable</i>				
Privately defined by OpenCable (www.opencable.com)	Transmitted content	Encryption; watermarking could monitor broadcast advertisements	None	Yes
	Interface between the POD module (NRSS B based) and the CE host device		Sender and receiver	Yes
	Interface between the CE host device and the display unit		Sender and receiver	Yes
<i>Terrestrial</i>				
ATSC framework for conditional access (www.atsc.org)	Broadcast content	Encryption; watermarking could monitor broadcast advertisements	None	Yes
	Interface between the NRSS security module and the CE host device		Sender and receiver	Yes
	Interface between the CE host device and the display unit		Sender and receiver	Yes
<i>Internet</i>				
Unicast-based DRM systems are privately defined (Microsoft and RealNetworks, for example, provide DRM for entertainment content)	Unicast content	Encryption	Receiver	Yes
The MSEC WG's Internet draft presents a common architecture for MSEC group key management protocols supporting a variety of application, transport, and internetwork security protocols (www.securemulticast.org); multicast-based DRM systems are yet to appear in the market	Multicast content	Encryption; researchers have proposed several multicast watermarking algorithms	Sender and receiver	Yes

Secure storage units. Some consumer electronics devices, such as set-top boxes for satellite or cable television, have permanent storage units. A hard

disk with multigigabyte capacity is the most common form of permanent storage.

Protecting content on local hard disks is diffi-

Content providers have achieved success in IP protection, but they need to address additional legal and technical issues.

cult. Should the system protect the encrypted data as it's received or should users require a local key to access data on their hard disks? Some service providers have been working on privately defined solutions and may not make their design publicly available.

Digital broadcast television. The broadcast flag is a sequence of digital bits sent with a television program that signals the program's need for protection from unauthorized redistribution (www.mpaa.org/Press/broadcast_flag_qa.htm). The MPAA and some broadcasters argue that implementing this flag will let digital TV stations obtain high-value content and assure consumers a continued

source of attractive, free, over-the-air programming without limiting the consumer's ability to make personal copies.

In its 3 June 2002 "BPDG Final Report," the Broadcast Protection Discussion Group—comprising content providers, television broadcasters, consumer electronics manufacturers, information technology companies, interested individuals, and consumer activists—evaluated the broadcast flag's suitability for protecting DTV content.⁵

Once suppliers of computer and electronics systems that receive broadcast television signals incorporate the broadcast flag's technical requirements into their products, television broadcasters can successfully implement the flag. Undoubtedly, full implementation will require a legislative or regulatory mandate.

In August 2002, the Federal Communications Commission (FCC) released a Notice of Proposed Rulemaking (NPRM) seeking comments about the need for regulatory copy protection legislation to protect digital broadcast television. In response to a request from several institutions, including some library associations, the deadline to submit comments was extended to 18 February 2003. The FCC received more than 6,000 comments, mostly from individuals.

The Media Bureau is in the process of preparing a recommendation for the Commission's consideration. In a 6 March 2003 written statement, W. Ken Ferree, chief of the Media Bureau, said it was difficult to predict when the Commission would complete its inquiry of this critical DTV issue.

Electronic publishing. The Open eBook Forum (www.openebook.org) is an international trade and standards organization dedicated to developing and promoting electronic publishing. Its members include hardware and software companies, publishers, accessibility advocates, authors, electronic book users, and

related organizations that seek to establish specifications and standards and to advance competitiveness in the electronic publishing industry.

OeBF working groups produce official documents such as specifications and process documents (for example, policies and procedures). The Rights and Rules Working Group's mission is to create an open and commercially viable standard for interoperability of DRM systems, providing trusted exchange of electronic publications among rights holders, intermediaries, and users. The working group gathers, analyzes, prioritizes, and coordinates requirements toward the development of an OeBF DRM specification.

Digital music. The Secure Digital Music Initiative (www.sdmi.org) forum is supported by companies and organizations representing information technology, consumer electronics, security technology, the worldwide recording industry, and Internet service providers. It aims to develop open technology specifications that protect the playing, storage, and distribution of digital music.

SDMI evaluated how well technologies for digital music protection met consumer and industry requirements, including performance, efficiency, audio quality, and survivability to attack. In May 2001, the SDMI plenary determined that no consensus existed for adopting any combination of the proposed technologies. This determination, however, does not affect the prior adoption of SDMI's portable device specification and Phase I watermark.

Interoperability of DRM systems. Many existing standards ensure consumer electronics device interoperability: A consumer can buy a Sony television and connect it to an RCA DVD player, expecting them to work together. Interoperability is also essential for content protection systems. Both the sending and receiving devices must support the protection system for a particular media.

Manufacturers can license systems like the CSS for implementation in consumer electronics devices. Unfortunately, this is not the case for DRM systems for Internet distribution. A client device supporting DRM system A can only download content protected by the same system. Current DRM systems aren't interoperable because

- DRM vendors are reluctant to share secret keys or algorithms, and
- there is no consensus on a rights expression language.

An alternative would be to implement several DRM systems on a client device, but this may not be feasi-

ble if the number of DRM systems exceeds a threshold. Ideally, the DRM system protecting the requested content should be transparent to the customer.

System renewability. Because encryption and watermark-based protection systems provide conditional security, they can be broken in time. Hackers can exploit flaws in a protection system's logical design or physical implementation. For example, in 1999, hackers broke a software implementation of the DVD CSS. As a result, injunctions banned Web sites from publishing the DeCSS code, which hackers can use to unscramble and play DVDs on unlicensed software DVD players.

DVD and digital interface protection systems have not been tested in the consumer market, so their performance is unknown. In these systems, *renewability* is defined as device revocation. If a hacker discloses and uses a device's secret keys in a pirated device, the system adds the hacked device's ID to the revocation list and distributes updated revocation lists to all licensed devices using new pre-recorded media or external connections (Internet, cable, satellite, and terrestrial). Once the ID appears on the revocation list, the pirated device can't receive protected content.

Selective encryption. Efficient data compression techniques can reduce the huge storage and communication requirements of new multimedia products and services. However, the additional need for protecting copyrighted digital content can aggravate the cost of this reduction. Encryption algorithms, which were originally developed for text data, might not be suitable for securing the large amounts of data in real-time multimedia applications.

Software cipher implementations are usually too slow for processing image and video data in commercial systems. Hardware implementations, on the other hand, increase the costs incurred by service providers and consumer electronics device manufacturers.

A recent trend is to minimize the computational requirements for secure multimedia distribution by *selective encryption*, in which only parts of the audio/visual stream are encrypted.⁶⁻⁸ Researchers have proposed many approaches for securing images, audio, and video, including integrating compression and encryption processes. Selective encryption is currently an important research area, and some of the proposed schemes have been found to provide insufficient security.

As individuals living in an information society, we need to understand the opportunities provided by an ever-expanding information infra-

structure and its impact on digital IP. Proponents and opponents of the technical measures for IP protection have presented strong arguments in discussion forums. Hopefully, these discussions will soon subside, leading to a general consensus regarding protection technologies and a common interpretation of consumers' rights in the digital age. ■

References

1. S.E. Siwek, "Copyright Industries in the US Economy: The 2002 Report," IIPA, 2000; http://www.iipa.com/copyright_us_economy.html.
2. Committee on Intellectual Property Rights and the Emerging Information Infrastructure, "The Digital Dilemma: Intellectual Property in the Information Age," US Nat'l Research Council, Nat'l Academy Press, 2000; http://www.nap.edu/html/digital_dilemma/.
3. A.M. Eskicioglu, J. Town, and E.J. Delp, "Security of Digital Entertainment Content from Creation to Consumption," *Signal Processing: Image Comm.* (special issue on image security), Apr. 2003, pp. 237-262.
4. A.M. Eskicioglu, "Multimedia Security in Group Communications: Recent Progress in Key Management, Authentication, and Watermarking," to appear in *ACM Multimedia Systems J.* (special issue on multimedia security), 2003.
5. Broadcast Protection Discussion Group, "BPDG Final Report," 3 June 2002; <http://www.cptwg.org/Assets/BPDG/home%20page.htm>.
6. I. Agi and L. Gong, "An Empirical Study of Secure MPEG Video Transmission," *Proc. Internet Society Symp. Network and Distributed System Security*, Internet Society, 1996, pp. 137-144.
7. L. Qiao and K. Nahrstedt, "Comparison of MPEG Encryption Algorithms," *Int'l J. Computer and Graphics* (special issue on data security in image comm. and network), vol. 22, no. 4, 1998, pp. 437-448.
8. C-P. Wu and C-C. Jay Kuo, "Efficient Multimedia Encryption via Entropy Codec Design," *Proc. SPIE Security and Watermarking of Multimedia Content III*, SPIE, vol. 4314, 2001, pp. 128-138.

Abmet M. Eskicioglu is a professor in the Department of Computer and Information Science, Brooklyn College of the City University of New York. His research interests are multimedia security, conditional access, digital rights management, and network security. He received a PhD in automatic control from the University of Manchester Institute of Science and Technology, Manchester, UK. Contact him at eskicioglu@sci.brooklyn.cuny.edu.