



Dated: July, 2008

Countering the Content Piracy Threat

by Pascal Marie, Strategic Marketing Manager, Thomson Software and Technology Solutions

The issue of content security has been a hot topic in the audio-visual market for several years. In more recent times, it has become an increasingly urgent concern. The digital revolution has led to proliferation in digital content creation while the emergence of the Internet and broadband has made it much easier to share illicit copies of content with anyone across the globe. This has increased the window of exploitation for pirates.

Today, a copy of a film which is recorded illicitly in a cinema can typically find its way onto peer-to-peer networks within a couple of hours. An increasing diversity of content sources, from movie rentals to video-on-demand and web downloads, has also led to a greater incidence of unauthorised copying and redistribution.

In addition, the migration from tape to digital workflows has made it much easier for individuals involved in production or distribution to copy content illegally onto external network drives.

According to the Motion Picture Association of America (MPAA) the worldwide motion picture industry, including foreign and domestic producers, distributors, theatres, video stores and pay-per-view operators lost US\$18.2 billion in 2005 as a result of piracy. A pirated version of one of the 'hit' movies of 2007, *Ratatouille*, for example, was trading hands online before the film's release.

In television production also, there have been some significant examples of piracy taking place prior to the first airing of content. Some of the episodes of the BBC's TV series *Doctor Who*, for example, appeared illegally on the Internet before they were officially broadcast.

The Scale of the Problem

The issue of piracy is a complex phenomenon that operates at several key levels.

- **While preparing content for release** - The content is most valuable at this point. Piracy is the result of malicious acts by a few mal-intentioned “insiders”, who are motivated by financial gain. The pirated items will typically be working or preview copies, “screeners” distributed to professional juries, promotional copies or ready-to-air copies. In the past year, French audio-visual anti-piracy body ALPA issued a “Good Practice Guide” for the industry aimed at raising awareness of the issue of piracy and advocating the introduction of anti-piracy protections based on encryption and watermarking in all technical production facilities. Thomson strongly supported this initiative, which some ALPA counterparts in other European countries are expected to replicate in the near future.
- **When content hits the screens** - In this case, piracy occurs inside the cinema theatre. The film being projected onto the big screen is recorded by camcorder from inside the theatre. While the quality of these recordings is often poor, these pirated copies are widely distributed via the internet and also give rise to illegal DVD sales. Overall, virtually all films are available on the internet soon after they are released in cinemas. In the case of American films, and because of the lag in release dates, infringements take place in most countries, prior to the cinema release date. The solutions to tackling piracy inside the cinema theatre lie either in “physical” prevention (scanning the theatre with infra-red goggles in order to locate camcorder lenses, which is possible during previews but difficult to apply during national releases), or in watermarking/tracing solutions, which will allow the date, time and cinema theatre in which the piracy took place to be conclusively identified. Use of watermarking was made mandatory by leading movie studios for all digital cinema systems.
- **When content becomes available on-demand in the home** - This scenario is even more complex. Opportunities for illegal copying and distribution increase with each new distribution window (DVD, video-on-demand (VoD), and pay-per view for example) while the quality of legitimate content has benefited from the integration of high-definition capabilities in play-back devices. Unfortunately, illicit recordings by personal camcorders are now also HD-capable.

Pirated copies tend to be of a higher quality at this level. Anti-piracy mechanisms exist but are generally easy to circumvent (e.g. Content Scrambling System (CSS) on DVDs). Watermarking, where feasible, is an excellent complement to digital rights management (DRM) in the sense that it makes consumers accountable and therefore dissuades illicit

redistribution. However, mass introduction of watermarking must obviously be implemented in total compliance with local data protection and privacy laws.

- **Upon airing** – Today’s pay-TV operators face a growing problem: the illicit redistribution of their signals. Broadband networks may inadvertently facilitate this new form of content theft, whether through global, uncontrolled peer-to-peer protocols or through personal video multicasting services. In order to successfully filter out such traffic and/or revoke subscriptions at their source, content detection techniques must be used which are capable of identifying the “rogue” decoder.

Finding a Solution

So what tools and techniques are available to the industry in order to address the increasingly pernicious problem of content piracy? Today, it is clear that the battle against piracy requires a three-pronged technological approach:

- The implementation of content protection measures (encryption-based) such as conditional access system (CAS) or DRM systems for the consumer environment, as well as professional solutions which only grant content access to authorised users or recipients;
- The deployment of content tracking solutions that deter recipients from pirating content, whether a professional receiving a preview copy or a consumer enjoying the content from a VoD service, because of the capability to identify the source of any piracy;
- The implementation of content recognition and filtering that detects and limits (or even blocks) the illegal circulation of copyrighted works.

Protective Measures

During production, post-production and advance screenings to professional audiences, it is critical that content be protected so as to strictly limit its use to sanctioned professionals, who may use or view it for purposes such as review and approval, dubbing, subtitling or duplication.

The best solutions in this area are able to secure the storage, transfer and viewing of digital content throughout the multiple tasks involved in production, post-production and distribution, combining encryption, individual rights management and watermarking.

With such types of content protection solutions, content may only have two “states” - encrypted (when stored or transferred) or individually watermarked (when accessed).

Encryption solutions combined with invisible watermarking are thus strongly recommended for professional workflows prior to cinema and/or DVD release, or first airing of TV content.

Keeping Tabs on the Situation

There is increased recognition within the industry of the important role that watermarking technology can play in keeping track of audio and visual material. Any watermarking solution must firstly ensure that a copy of any content can be reliably identified after format changes have occurred (including, in the case of content theft, changes carried out using a camcorder). Secondly, it must make certain that it never interferes with the viewer's experience while it carries out this function.

Digital watermarking solutions make audio and video content easily and precisely identifiable by embedding specific data such as the rights holder's or recipient's ID or user number. The watermark, totally invisible to the naked eye and inaudible in the case of audio watermarking, may be embedded at various points in the content preparation and distribution process.

This is the case with Thomson's NexGuard™ forensic marking solution that is integrated in the post-production process, during broadcast or in video servers depending on purpose.

This solution also becomes a key deterrent against piracy in the home when embedded in the TV decoder as a complement to a CAS/DRM system. It is expected that such an application, already successfully field-tested by Thomson, will see its first mass deployments at the same time HD VoD services are introduced to a larger audience with catalogues of premium content.

In all cases, the use of watermarking increases the responsibility of content recipients because their ID is hidden in the content, which means that their identity may be uncovered if an act of piracy takes place.

Forensic analysis of pirated video samples has already helped investigative organisations such as the FBI on several occasions to focus their inquiry on a particular copy or recipient and to successfully resolve the piracy case as a result.

Watermarking solutions are already fully operational today and are actively responding to diverse security challenges.

Filtering and new business models

One of the hottest topics affecting the audio/video market today is the issue of the proliferation of copyrighted content on video portals and user-generated content (UGC) websites.

In order to automatically filter out such content, organisations are increasingly turning to fingerprinting technology.

Given the volume of files that are traded across the internet, it seems indeed vital to install partially automated systems that filter copyrighted uploads and/or downloads in order to limit, if not block, certain traffic associated with mass downloads.

The recent development of digital fingerprinting leads to automatic recognition of copyrighted material placed online by web users. Fingerprinting technology is used to build a database of the reference digital 'fingerprints' of all copyrighted content. Illegal copies can be identified by generating the fingerprints of potential uploads and comparing them with the reference database.

The best fingerprinting systems can withstand major distortions in the original content (compression, changes in resolution, camcording, rotations, cropping, etc.) and therefore can identify content that has undergone major transformations, which is often the case with pirated copies.

Used in conjunction with such "reference databases", content recognition technologies may efficiently conduct informed content filtering that will either limit the transmission of pirated works or monetise the online circulation of works in agreement with rights holders.

Tackling the Problem

Rapid technological advances in the audio/video industry over recent years coupled with the diversity of techniques employed by content pirates have made it increasingly urgent to invest in new ways to fight the content piracy phenomenon.

Thomson leverages watermarking in combination with other technologies to deliver fully-fledged solutions tailored to each business along the content value chain and to every form of filmed and TV entertainment.

Backed by significant investment in research and development, the company's NexGuard and NexTracker™ brands provide tracking and piracy-deterrence solutions to a growing number of high-profile customers.

As new forms of entertainment continue to emerge, other challenges to copyright are in sight, but the core technologies to address them may already exist.