DVD COPY PROTECTION FOR ON-DEMAND DISC PUBLISHING

Ensuring digital content security and preventing unauthorized duplication

RIMAGE™
ON DEMAND DIGITAL PUBLISHING™

I. Executive Summary

Unauthorized copying prevents digital content owners and distributors from capturing all of the revenue to which they are entitled. Protecting discs from unlawful duplication can mean the difference between profitability and loss for content owners.

Several key factors must be understood in order to maximize protection without creating technical compromises, workflow delays or financial risks.

Traditional protection methods do not sufficiently address the most pressing issues facing this ever-evolving industry: workflow efficiency, protection strength, and most importantly, playback compatibility. Nor do they meet the protection needs of on-demand disc burning environments. However, the technology for on-demand DVD publishing, combined with on-the-fly anti-rip copy protection and superior playback compatibility, is now possible thanks to an innovative software solution that offers content protection for publishers using recordable DVDs.

This white paper reviews and explains the protection choices and optimal configurations, and discusses the new technology.

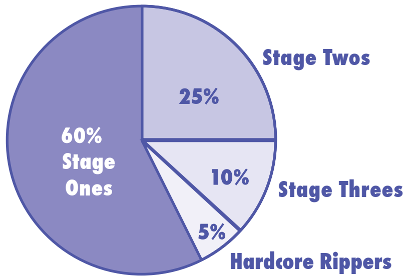
II. Background, Challenges, Opportunities

Of all the emerging threats to the television and movie industry, unauthorized duplication tops the list because of the enormous and on-going economic damage it does. In a recent In-Stat survey, half of television and movie industry professionals said they considered piracy as a threat to their bottom lines; over a quarter of those surveyed said they had suffered revenue losses due to the illegal theft or reproduction of their intellectual property.

People who choose to make illegal copies come in several levels of sophistication and dedication. They range from rippers with a primarily opportunistic mindset, to those who have, in essence, made content theft their life's focus.

Stage Ones are the least technically sophisticated rippers. They make up the majority of the pirate population. While they tend to rip low to medium volumes of content, their success level is disturbingly high.

Illegal DVD Copying –



Stage Ones: The least technical and often least successful rippers.

Stage Twos: Spends time looking for ripping tools online.

Stage Threes: Uses multiple ripping tools.

Hardcore Rippers: The most techincal and most successful rippers.

Stage Twos comprise about a quarter of all pirates. They are more likely than Stage Ones to participate in ripping forums, and they spend a lot more time trying to copy. They may also search the Internet for ripping solutions to special titles.

Stage Threes are distinguished by their use of multiple ripping tools, which they deploy in combination. They have heavier involvement in multiple ripping forums than do Stage Twos, and thus more acquired knowledge. They represent about 10 percent of the pirate universe.

Hardcore Rippers are the most technically sophisticated and focused of all content copiers. Though they make up only five percent of all pirates, Hardcore rippers are of particular concern to the industry, because they post frequently to online forums, and even mentor Stage Ones and Stage Twos. They also beta test new ripping programs, and provide their testing feedback to these forums.

If there is any good news emanating from the ripper universe, it is the fact that most rippers are on the lower end of the sophistication/dedication scale, and are not making a business out of stealing and selling content.

While movie and TV piracy garners most of the publicity, piracy plagues the digital content production and distribution marketplace as a whole.

Whether the concerned party is a large legal publishing enterprise, a healthcare organization or a motivational speaker, they face the same needs for content protection and control as the marketplace's more prominent entities.

Until recently, however, the creation of protected DVDs was tied to large production runs of stamped or silk-screened discs in response to specific quantity orders. With the advent of market activities such as download-to-burn and movies-on-demand, a completely new technology and consumer paradigm has evolved, necessitating solutions that keep the market ahead of copyright abuse, protect its sizable investments in original content and meet immediate customer demand.

Whatever the size or nature of the user, all have the same needs for a protection solution that is efficient, strong and provides optimal playback compatibility.

III. Traditional DVD Anti-Piracy Technology

The digital content industry utilizes several copy protection and pirate-tracking tactics. Regarding copy protection for recordable DVDs, there are three basic techniques:

1. CSS encryption/decryption (built into every DVD player)
2. "Bad sector" schemes, which purposely create and burn bad sectors into the DVD itself
3. Content Alteration, wherein the structure of the DVD is changed to fool ripping programs, but does not impact the playability of the discs

Type One: Content Scramble System (CSS) Encryption

This is the standard method of protecting digital content for Video DVDs. CSS works by encrypting the content, which is then distributed on read-only media. The security scheme is defined in the player, typically as software, and enforces a set of fixed security rules. In order to allow off-line playback, players are pre-loaded with media decryption keys.

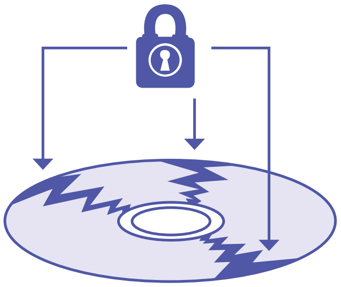
Authentication requires verification by a drive and a downstream device or a host DVD player (such as a PC software application or decoder board) that are both legally licensed to use the copy-protection system.

Despite the fact that CSS was cracked ten years ago, it continues to enjoy widespread industry use, due largely to the fact that it is still a legally recognized form of protection.

Type Two: Bad Sector Insertion

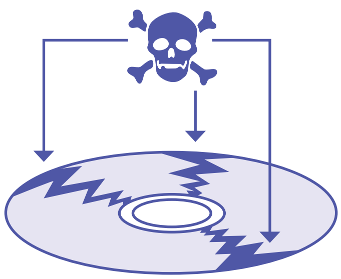
This protection method involves the deliberate creation of a number of corrupted data sectors on the DVD that cause DVD copying software to correct these errors. Standard DVD players usually can ignore these sectors and write them out to the new disc. In the process, the "bad" sectors are automatically corrected by the software and the recorder. The special playback software actually looks for the original "bad" sectors and will inhibit playback if it sees corrected sectors.

Inserting bad sectors on recordable DVDs requires a special DVD recorder with software-specific firmware modifications that allow the writing of bad sectors.



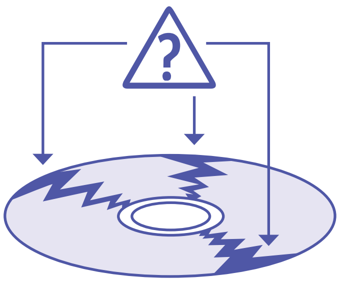
Content Scramble System (CSS) Encryption

"Locks" content and makes it inaccessible to ripping software



Bad Sector Insertion

Intentionally corrupts content and confuses ripping software



Content Alteration

Places bad data in unused portions of the disc, confusing ripping software but preserving playback compatibility

The major drawback to the use of bad sectors is their potential for negatively impacting broad playback compatibility. In effect, adding purposely bad sector reduces the quality of the discs themselves.

Examples of Bad Sector Copy Protection Solutions

ARccOS is a copy-protection system developed by Sony that deliberately creates a number of corrupted data sectors on the DVD, causing DVD copying software to produce errors. Though ARccOS was reportedly discontinued, several recent high-profile releases have used it. Like CSS, this protection method has major vulnerability issues; pirates can apparently overcome it by utilizing any number of ripping programs.

DVD-R-Movie PROTECT (by X-protect) also inserts forced errors on DVDs, making clean playback trickier. Pirates try to overcome this protection by employing ripping programs that are designed to identify and "fix" the forced errors.

FluxDVD (by ACE GmbH) is used by CinemaNow, an internet-based, on-demand movie download and burn company, to prevent copyright violations. FluxDVD's protection process creates discs with errors, which can pose playback compatibility issues.

Type Three: Content Alteration

The third form of protection attempts to disable ripping programming without negatively impacting playback compatibility.

Examples of Content Alteration

RipGuard (by Macrovision) is designed to prevent or reduce digital DVD piracy by altering the format of DVD content, thereby disrupting ripping software. It also thwarts pirates by rendering the formatted section of DVDs unwatchable on some players.

Rimage Video Protect (by Rimage Corporation) is the latest entrant into this promising category, providing protection against ripping tools without sacrificing playback compatibility. More informatioin on Rimage Video Protect follows at the end of this document.

IV. Technology Considerations

As with any technology solution, digital content protection raises several key considerations, briefly addressed below. The ideal protection solution would address all of these.

Playback Compatibility

The first and foremost objective for any protection method is provision of superior playback compatibility on the maximum number of DVD players and set-top-boxes. The best way to attain this objective – and to leave original media content unaltered – is to encapsulate smart code on unused disc areas, as opposed to coding weak sectors on disk content. However, the latter method has been the industry standard, due in large part to the fact that encapsulation solutions have not been widely available.

A Plague on All Pirates

Any given protection type needs to be effective not only against garden-variety rippers, but to provide moderate resistance to the most dedicated and prolific of pirates as well. The conundrum for digital content providers and distributors has been that they can have either excellent protection or great playback compatibility, but not both, because the more robust the protection is, the more it impairs playback compatibility.

Space Invaders

Even the least space-invasive protection will eat up some territory; the questions are: "How much territory?" and "What's an acceptable level?" Ideally, less than one percent of disc real estate should be taken up by protection elements. Solutions vary from 5% to 10% capacity lost due to protect.

Passive = Good

It is a safe bet that no content owner or distributor wants active code loaded on their system. No computer owner wants special or secret tracking software installed on their computers in an effort to protect against unauthorized copying. The way to avoid this is by utilizing a protection solution with a passive software presence.

Overhead

Because of their significant impact on the rate of disc production, prep time and burn time are major contributors to overhead costs. These factors should therefore have as minimal an impact on the protection process as possible, regardless of whether the application is one-time in nature, or involves a multiple disk burn.

Integration

Seamless workflow integration is vital; the addition of the copy protection option into the DVD creation process should be unobtrusive and minimally time invasive. The acquisition of protection licenses should likewise be seamless, with options for corporate and site licensing.

Keeping Current

Much like the Borg colonies on Star Trek: Generations, pirates are constantly adapting and finding new ways to get around protections. Software currency is one of the best tactics for keeping pirates at bay; vendors' products must therefore be flexible and updatable.

Application Compatibility

Protection must integrate smoothly with other applications, especially watermarking. The result of effective integration is a DVD that has both copy protection and origin tracking security (also known as "double-dipping").

Getting Focused

A key protection question is: Where should the protection be? There are two self-evident options; on the recordable media, or on the replicated media. What may be less self-evident is that the protection techniques that can be brought to bear on recordable media are much more powerful than those for replicated media. One reason is that recordable protection techniques provide for traceability to an actual offender. Another equally compelling reason is that the recordable-focused techniques enable alteration of protection protocols for each disc produced; such techniques make a universal crack less likely.

Why Be Blu?

Copy protection has to be compatible not just with DVD technology (including DVD9), but with whatever is next on the horizon, be it Blu-ray, HD-DVD or any other format.

V. Tackling Transparency

To be considered successful, an anti-piracy scheme must be effective, difficult to defeat and — perhaps most important — transparent to users. Most digital content protection solutions readily meet one or two of these criteria, but not all three. Where most of them trip up is in regard to transparency, because, as noted above, the better the protection, the lousier playback will be.

VI. Digital Watermarking

No matter how ingenious a protection solution is, it will be cracked eventually. That is why best practices include use of digital watermarking. Whereas protection methods are designed to prevent or hamper piracy, watermarking is forensic in nature.

As the name suggests, digital watermarking is akin to a currency watermark, in that it verifies the authenticity of the content. In addition to providing authentication, digital watermarking enables the tracking of pirates, thereby making their identification — and perhaps more to the point, their apprehension — more likely.

Watermarking is a very robust solution that involves weaving minute bits of data through the entire stream of a movie, or any other type of digital content. These watermarks, which are invisible and inaudible, are embedded into and retrieved from digital content using a proprietary algorithm. It is estimated that in a one-second stream of video from a DVD, which has an average size of five Mbps, a watermark would be about two bits of data. Watermarks are retained and detectable after the digital content is edited, compressed or converted.

These data embeds, which typically include date, time and place elements, also enable the tracing of illegal copies back to their distribution source.

In addition to its various functional anti-piracy elements, the interwoven nature of watermarking makes it hard for pirates to find and isolate the watermarking data bits. Even if the bits' whereabouts could be ascertained, pirates would not be able to remove them without damaging the DVD's content.

Among the watermarking solutions are **RUNNING MARKS™**, **VTrack**, **VideoMark** and **NexGuard**.

RUNNING MARKS™ (by Cinea) is a watermarking system designed for the consumer electronics market. It claims to offer unique, replacement-based watermarking rather than the more typical single-ended solution. The manufacturer says that this system simplifies the current complex watermark insertion process by separating the image of where to place marks, from the task of insertion. Content undergoes a one-time analysis, followed by creation of a small set of metadata that provides information on how to insert the watermark.

Replitrack (by Philips) a turnkey watermarking solution for forensic tracking purposes and currently only available for video content. The product comes as ready-to-install software and works in conjunction with Rimage DVD-R duplication equipment. It embeds an imperceptible, indelible identifier into the video signal. Replitrack digital watermarks are claimed to be extremely robust and inseparable from content, making them impossible to alter. The manufacturer says that even after severe degradation due to scaling, cropping, compression or even camcorder copying, the pirated content can still be traced.

Videomark software casts and detects invisible watermarks on digital content. The watermarks correspond to specific ID numbers, known as watermark keys, which are given to and used by the copyright owners to make exclusive watermarks.

NexGuard (from Thomson) is a watermarking solution that embeds the date, time and place of projection into a digital motion picture's image and soundtrack during play-out in movie theatres. When the information is extracted from pirated materials with NexGuard's detection and recovery system, it pinpoints the exact source of the "leakage."

VII. Rimage Video Protect

Rimage Corporation has just announced a passive, encapsulation software solution known as Rimage Video Protect. This technology is a completely integrated, turnkey pay-as-you-go application that represents the most state-of-the-art capability available for ensuring digital content security and preventing profit-killing unauthorized copying.

Rimage Video Protect guards against inappropriate copying of DVD content by encapsulating data files in areas of the DVD disk that are not read during playback. This solution not only leaves playback compatibility uncompromised, it leaves original media content unmodified.

While no digital content protection solution is totally impregnable, Rimage Video Protect stops all known ripping tools, providing on-the-fly protection to pre-release content, screeners and on-demand production DVDs. The solution is directly built into Rimage's software suite, ensuring seamless execution and streamlined workflow.

Rimage Video Protect applications include distribution centers, pre-release video (dailies), Oscar screeners, web fulfillment for content owners, pre-sales distribution, pre-release audio, service bureaus and content publishers.

Rimage Video Protect is the first downloadable pay-per-burn protection system, ensuring ease of use for small- and medium-sized media service companies. Video Protect enables users to meet customers' disk demands without unnecessary waste, which can make the difference between order profit and loss.
When combined with a proven watermarking method, Rimage Video Protect represents the best strategy available for ensuring digital content security and preventing pirate-related profit diversions.

VIII. Third-party Endorsements and Evaluations

Rimage Video Protect's high playback compatibility has been verified in two independent tests, which also confirmed the company's claim that Rimage Video Protect is a passive solution that does not install software or modify users' computers. The tests were conducted by Intellikey Labs, Los Angeles, and Next Generation Security Consulting (NGS), Surrey, U.K. Intellikey Labs is recognized by the world's top entertainment, media, manufacturing and software companies as the market leader in quality assurance testing for optical and digital media content. NGS is regarded as the world leader in the discovery and publication of computer security vulnerabilities.

Intellikey Labs Test Results

In a nutshell, Intellikey concluded that any desktop player that can play a DVD can play a Rimage-protected disk.

Intellikey Labs tested Rimage Video Protect embeds on +R and –R DVDs. Both versions were tested for compatibility on a 103-DVD player subset of Matrix 5.10; this subset represents more than 83 percent of all DVD players sold in the U.S. between 2003 and 2005.

The +R embed loaded successfully on all but two of the 103 DVD players. The no-loads occurred on the Microsoft Xbox 360 and Panasonic DVD-RV32 players, which represent a mere .39 percent of all DVD players sold in the U.S. between 2003 and 2005.

The –R embed loaded successfully on all but one of the 103 DVD players; Microsoft's Xbox 360 was the only player on which the disk failed to load.

NGS Test Results

99.61%

Rimage Video Protect Playback Compatability
Based on independent research analysis

After testing protected DVDs on three different operating systems, NGS concluded that "…(Rimage's) DVD protection technologies behave in a safe and secure manner when introduced to a user's computer system, and behave as described by Rimage."

NGS performed an assessment aimed at verifying the company's claim that Rimage Copy Protect's copy protection mechanisms did not insert software onto operating systems; NGS' self-described role was "to determine conclusively whether the technology would take any unexpected, undesirable or malicious actions when a DVD protected with the technology is played on operating systems platforms supported by" Rimage Copy Protect. The three operating systems on which the solution was tested were Windows, Intel Mac and PowerPC Mac.

NGS tested six DVD videos, three of which contained material protected using Video Protect, and three which had not. NGS also tested two Audio CDs that had been protected with Rimage Copy Protect audio copy control software. NGS determined that there were no unexpected, undesirable or malicious actions taken on any of the three systems on which the protected DVDs were played.

IX: Conclusion

Efficiency, vigorous protection and superior playback compatibility are the three biggest needs facing digital content producers and distributors. Until now, it has been virtually impossible to attain all three. Rimage Video Protect overcomes this problem with an on-the-fly, encapsulation-based passive software solution that inhibits ripping and disk copying software, while leaving original media content unmodified.

When combined with a quality watermarking method, Rimage Video Protect represents the best way for users in the digital content production and distribution marketplace to protect their profits and keep pirates at bay.

Sources

"Digital Content Protection: How Anti-Piracy Technologies are Transforming Digital Media." by Don Labriola (5/16/02). From ExtremeTech www.extremetech.com, 7/06/07.

"Survey: movie, TV execs see piracy as threat." *Austin Business Journal*, 1/04/05.

"Universal adds anti-piracy watermark," by Carlos Martinez, *San Fernando Valley Business Journal*, 10/03.

"Forensic Watermarking Technology Incorporated into On-Going 4,000-Screen Digital Cinema Rollout," 2/23/06. From TECHNEWS, www.technologynews-daily.com, 7/03/07.

"Digital Watermarking Alliance Reports Industry Demand for Anti-Piracy, Imagery, Broadcast Monitoring and ID Security Solutions Continues," 6/11/07. From yahoo! Finance, biz.yahoo.com, 7/03/07.

"Top D-Cinema Manufacturers Choose NexGuard™ to Combat Piracy," 8/16/06. From DCinema Today, www.dcinematoday.com, 7/03/07.

"Self-Protecting Digital Content: A Technical Report From the CRI Content Security Research Initiative." Kocher, Jaffe, Jun, et al, 2002-2003. From Cryptography Research, www.cryptography.com, 7/18/07.

"General information about digital watermarks." From EWATERMARK.com www.ewatermark.com, 7/20/07.

www.philips.com

www.cinea.com

RIMAGE™

ON DEMAND DIGITAL PUBLISHING

Rimage Corporation
7725 Washington Avenue South
Minneapolis, Minnesota 55439 USA
Toll Free: 800.445.8288
Fax: 952.944.7808
www.rimage.com

Rimage Europe
Rimage Europe GmbH
Albert-Einstein-Strasse 26
63128 Dietzenbach, Germany
Tel: (49) (0) 6074 8521 0
Fax: (49) (0) 6074 8521 100
www.rimage.de

Rimage Asia/Pacific
Rimage Japan Co., Ltd.
3-15 Kanda Nishikicho Chiyody-Ku
Tokyo 101-0054 Japan
Tel: +81.3.5238.8465
Fax: +81.3.5238.8463
www.rimage.co.jp