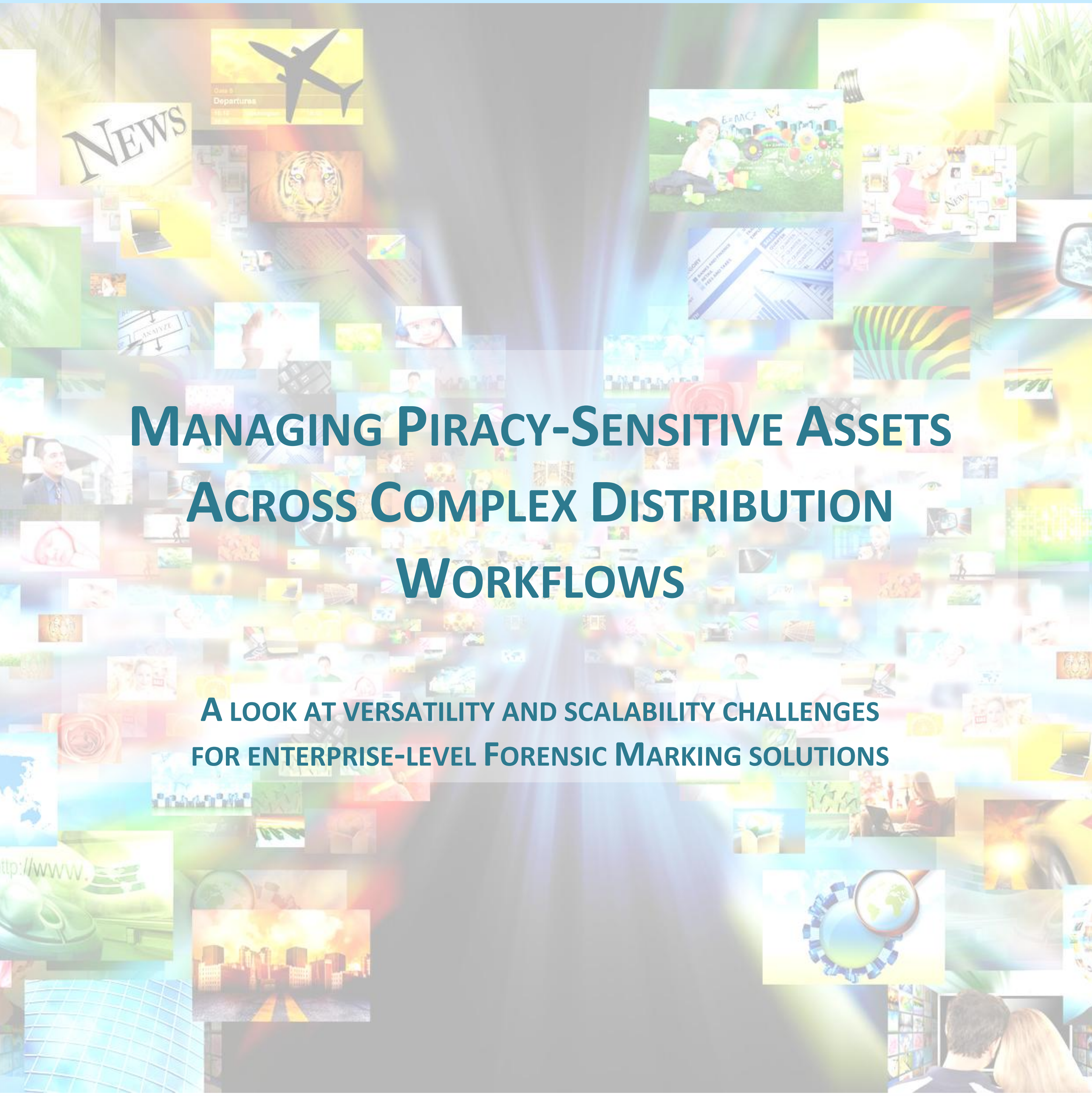
civolution

Identify | Manage | Monetize



Managing Piracy-Sensitive Assets Across Complex Distribution Workflows

A look at versatility and scalability challenges for enterprise-level Forensic Marking solutions

NexGuard - Pre-Release use cases | JAN 2013

TABLE OF CONTENT

The need for efficient duplication and distribution

Circulating content copies

During or post content production, a given piece of video content needs to be circulated throughout its lifecycle. A number of copies will therefore need to be distributed. These can include dailies for review and approval; preview proxies for screenings; master copies for VoD or TV airing; and repurposed versions for Internet and mobile portals.

Whether in-house or outsourced, duplication and circulation of content should be organized with rapid turn-around. The various content copies are distributed in a range of diverse formats, mostly as tapes, DVDs or digital files. In the specific case of content repurposing for Internet and mobile portals, each instance of the content might even have to be generated in a specific encoding format to meet the requirements of each individual content portal or distributor.

	Post-production	MarCom	Distribution	Repurposing
Content	Dailies, semi-finished content	Screeners for feature films and TV series	Preview proxies, Master copies	Live content, TV shows, TV episodic
Source	Production group	Marketing and communication group	Home entertainment group	Networks, TV stations, Broadcasters
Destination	Internal for review and approval	Journalists, Awards jury members	DVD replication plants, Broadcasters, VoD operators	Internet portals, Mobile portals

FACT #1: **Release and monetization of content necessitate appropriate duplication and distribution of copies in a variety of formats.**

NEED #1: **A complete management-of–assets solution to track the dissemination of copies.**

Content owners require accountability with regards to their assets. Solutions are needed wherever the location and whatever number of people involved are in the post-production, repurposing or distribution processes.

Impact of potential piracy from copies in the field

Content theft in professional environments is a major issue for Movie Studios and TV Content Producers. Pre-release content leakage may occur from preview and master copies circulated to broadcasters and VoD operators; screeners for the press and awards jury members; or repurposed TV programs for Internet and mobile portals.

The TV and film industries continue to heavily suffer from the illicit re-distribution of high-quality pirate copies, which are either sold as DVDs on the black market or circulated on cyberlockers and peer-to-peer web sharing sites.

The most impactful content theft is definitely the one occurring at the earliest stage of the content lifecycle. According to a survey by technologist Andy Baio **[1]**, many blockbusters are illegally available online ahead of the Oscar season, sometime ahead of the theatrical release. Likewise, often episodes of TV series appear on the Internet prior to their first broadcast.

FACT #2: **Access to content and distribution of copies must be constrained to authorized recipients only.**

NEED #2: **A strong and reliable deterrent to counter the risk of potential content theft.**

Serial numbering of content – whatever its format – to identify copies one by one may be used by rights owners to answer three critical needs through a single process:

1. Tracking the dissemination of copies and organizing audits when needed
2. Introducing a strong deterrent against content theft and curbing piracy
3. Conducting forensic analysis in case of actual illicit circulation

MPAA recommendations

For more than three decades, the Motion Picture Association of America, Inc. (MPAA) has managed site security surveys on behalf of its member companies, namely the six top Hollywood studios. The MPAA has defined content security best practices organized according to the MPAA Content Security Model. MPAA recommends use of watermarking as part of digital security and content management, especially for entities that provide digital transfer services for any type of screener **[2]**:
''*SCR-3.14: Apply invisible forensic watermarking to digitally streamed and/or downloaded screener content.*''

Workflow Challenges

Diversity of formats

Depending on the content format and on the purpose of a given instance, the audiovisual material may have to be delivered via:

- Tape or DVD-R duplication and shipment,
- Content formatting, possibly repurposing and transcoding, and file transfer or streaming.

For cost and efficiency reasons, most workflows tend to be digitized and based on files:

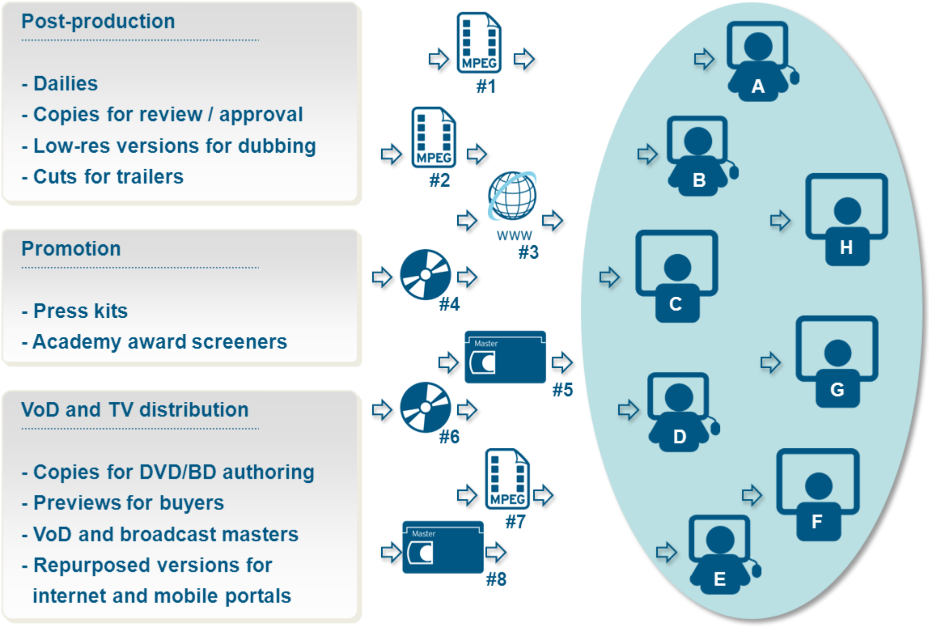
- Circulation of review and preview copies – respectively internal and to buyers – is commonly organized based on proxy file delivery or online streaming,
- Delivery of master tapes is being progressively replaced by transfer of mezzanine files,
- DVD-R duplication and shipment for screeners could be replaced by online screening,
- Content (re)formatting, possibly repurposing for different types of screens, is then delivered via file transfer to OTT VOD service providers.

File-based circulation of content relies on storage servers, transfer servers and content transcoding to deliver the expected formats. However, HD CAM SR tapes provide the utmost quality to deliver broadcast copies; and DVD is an easy way for occasional delivery to a large group of people and ensuring playability on regular computer and home-theater systems.

Multi-site operations

Movie studios or TV content producers usually work partly in-house and partly with contracted post-production facilities for content processing and delivery of content instances as tapes, DVDs or files.

Whether circulating content internally for review and approval, or externally for monetization, the challenge is to avoid having any genuine copy turn into a tidal wave of pirated versions. The risk of piracy arises from the broad circulation of content both internally and externally as illustrated in Figure *1* hereafter.



Post-production

- Dailies
- Copies for review / approval
- Low-res versions for dubbing
- Cuts for trailers

Promotion

- Press kits
- Academy award screeners

VoD and TV distribution

- Copies for DVD/BD authoring
- Previews for buyers
- VoD and broadcast masters
- Repurposed versions for internet and mobile portals

Figure 1: Content circulation and risk of piracy

The successful circulation of content requires managing multiple recipients and diverse formats through efficient and secure workflows. The sheer number of teams involved in this process makes it challenging to get an exhaustive and clear view of produced copies in their respective source, format, and destination. For each and every situation, organized serial numbering of content is required; either as part of in-house operations or when outsourcing formatting and duplication to third-party post facilities.

MANAGING PIRACY-SENSITIVE ASSETS ACROSS DECENTRALIZED DISTRIBUTION WORKFLOWS

Deterrent against content theft

In order to enforce the liability of the individuals and/or organizations receiving an instance of a piece of content – or simply make those parties more aware of their responsibility – it is essential to introduce an efficient deterrent against content theft.

→ The content preparation and delivery solution should provide the content with and identity, i.e. insert imperceptible forensic marks, and – for certain copies – add a visible identifier such as the recipient's initials, logo or other unique personalization features.

Efficient integration in distribution workflows

Such content security should integrate seamlessly with existing streamlined processes. It should introduce minimal overhead into the respective workflows, from delivery of tapes or DVDs and to specific file formatting and transfer for Internet and mobile portals.

→ The forensic marking solution should be versatile and aggregate dedicated file, tape or DVD processing units along with combined transcoding/watermarking stations for any video file formats used in digital workflows.

Multi-site and inter-organization operations

Efficiently addressing the risk of content theft requires organizing a comprehensive and systematic process, including such cases as multi-site operations within an organization or inter-organization processes.

→ The duplication and serial numbering system must be scalable and centralize content tracking information in a consolidated database in order to monitor the dissemination of assets.
→ Several layers of watermark can be applied on the same piece of content.

Forensic analysis in case of piracy

The forensic mark may be used in case of actual content theft to facilitate investigations by identifying the source of the leak.

→ The forensic marking technology should provide robust identification and easy analysis of any video sample (eg. retrieved from user generated content (UGC) sites such as YouTube or Daily Motion).

The diagram hereafter illustrates how a serial numbering process based on imperceptible audio or video watermarking can help to identify the source of a leak. Watermark detection from any illicit copy allows investigators to ascertain which occurrence of the genuine content was illegitimately redistributed.

Forensic watermarking benefits include both a deterrent against content theft, and a means to support investigations in order to identify the source of the leak when piracy does occur.

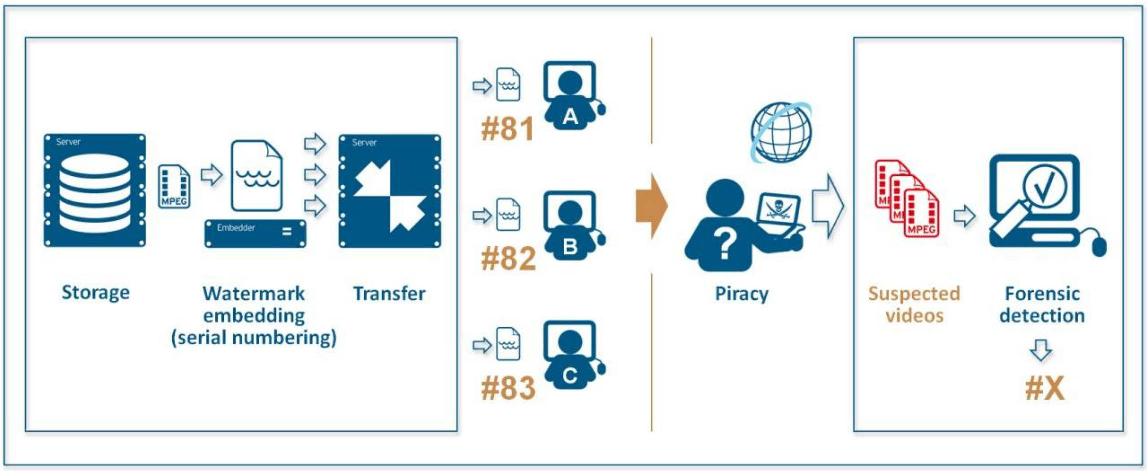


Figure 2: Imperceptible audio/video watermarking for forensic tracking

Advanced Solution – NexGuard forensic watermarking solution for Pre-Release content

Digital watermarking technology for reliable serial numbering of content instances

NexGuard® forensic watermarking solution for Pre-Release content ensures unique identification of each content copy as tape or DVD, or of each content instance as a file. It can combine inaudible audio watermarks and imperceptible video watermarks, as well as visible marking such as explicit warning messages or recipient initials.

The digital watermarks are robust to video format changes. The embedded watermark identifier represents a virtual serial number which can be recovered from collected video samples.

The use of digital watermarking technology enables the serial numbering of a given piece of content, regardless of its format, without hindering the viewer experience.

The main digital watermarking principles are depicted hereafter, in Figure 3

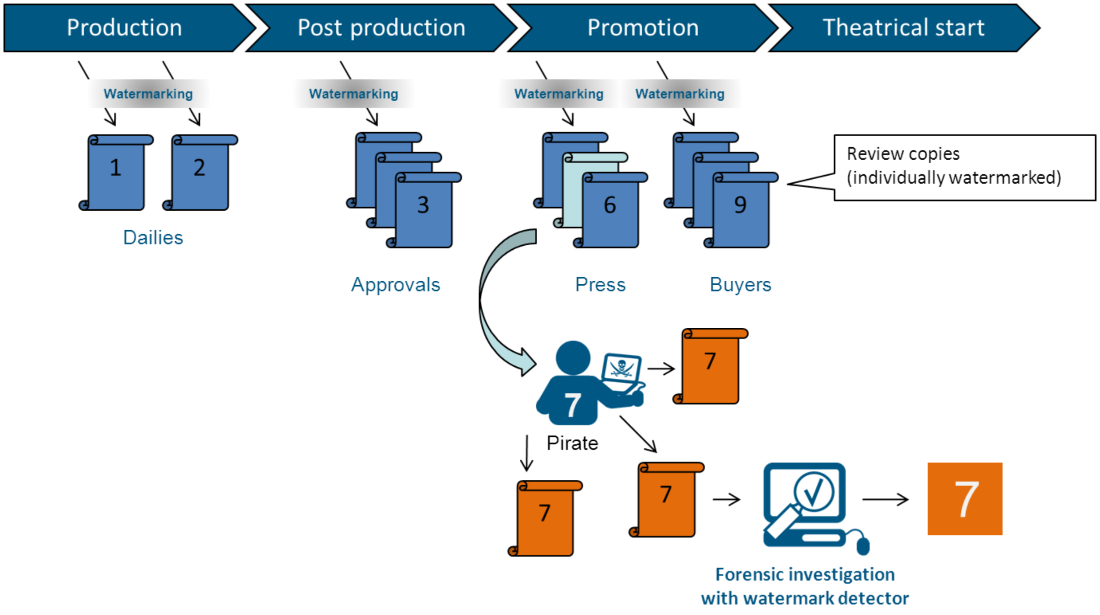


Figure 3: Video Watermarking principles for forensic marking applications

NexGuard forensic watermarking technology is also in operation in theaters equipped with digital cinema (d-cinema) systems and has been ported to set-top-box-type consumer devices used for pay-TV and premium VoD services.

Decentralized duplication and forensic marking system

The NexGuard - Pre-Release leading-edge digital forensic watermarking system offers content owners and post-production facilities a scalable and versatile solution for various workflows, including content reviewing, master or screener delivery, or content monetization through repurposing of TV programs for online services.

The system relies on a central server, dedicated watermarking devices for watermark embedding in tapes, DVDs and files, and plug-ins for third-party transcoder stations. The content-tracking related information is consolidated in a global database for access (when necessary) by the anti-piracy group.

NexGuard components are available for all teams and process types of the global workflow as illustrated in Figure 3.

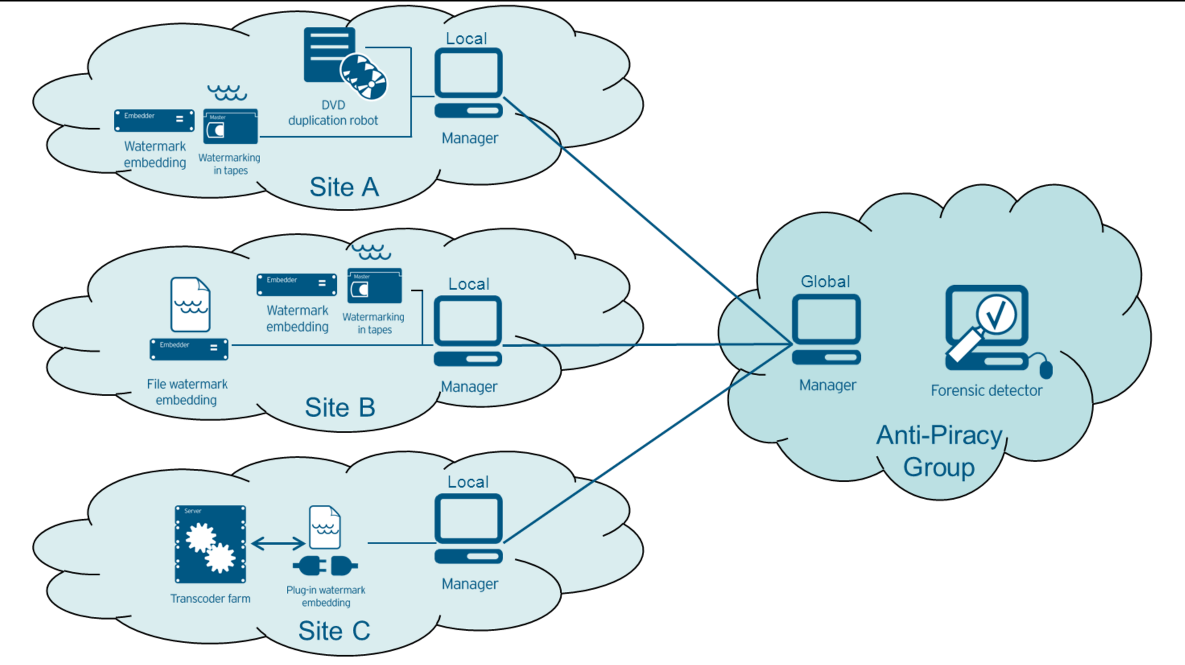


Figure 4: NexGuard - Pre-Release forensic watermarking solutions

A scalable and versatile solution

The NexGuard - Pre-Release solution consists of Local Manager servers for regional operations, a Global Manager to centralize information in a single database, and a series of embedders or screener devices and/or third-party transcoder stations with watermarking plug-in.

The solution enables the seamless integration of content serial numbering in most distribution workflows and for:

- In-house and/or outsourced operations in one or several locations,
- Content distributed via file formatting and transfer/streaming,
- Content delivered after physical media duplication.

NexGuard - Pre-Release system-level elements

The NexGuard solution is designed from the ground up to organize a complete enterprise-level content distribution and tracking system. Tracking information includes each content copy and their respective virtual serial number as well as recipient details. The global database centralizes operation information from all facilities, including database abstracts from third-party facilities whenever duplication is delegated to external post-production entities.

Each system-level component of the NexGuard - Pre-Release forensic watermarking solution is further described in the below table.

Local Manager product element Manager	System-level server to operate the devices, configure tasks, automate operations, organize load balancing, monitor progress with a dashboard and query information from the SQL database. A single local manager can drive multiple devices in multiple locations. Its database logs every single operation from Screener and Embedder elements, and can be used to export activity reports. The system can be operated in three different ways: i/ by operators using a web-based GUI, ii/ automated with pre-configured watch-folders, iii/ driven by a third-party application.
Global Manager product element Manager	Global system and inter-organization operations can consolidate information in a Global Manager database acting as a central information repository related to circulation of assets. For intra-organization operations, the Global Manager automatically collects information from the Local Manager servers in the various sites or regions. The Global Manager can also import data from third-party facilities to which some of the duplication tasks have been outsourced.
Detector product element Forensic detector	Forensic analysis of a pirate video sample can be performed using the NexGuard Detector station or through on-line investigation-as-a-service. The watermark payload is a serial number or unique identifier of a given instance for a given content. Once the video analysis has unveiled the forensic mark, the person in charge of anti-piracy operations can query the Manager database to retrieve all the details related to this specific content copy, including details of the original intended recipient.

Integration to file-based digital workflows

a/ For serial numbering of multiple file instances in a given format

The NexGuard File Embedder is designed for fast watermark insertion in selected video file formats.

The solution ensures efficient operation when delivering content in a given format to multiple recipients.

File Embedder product element File watermark embedding	The Embedder product element offers high-speed file processing for most commonly used video formats such as MPEG-2 and WMV9. The Embedder product element supports additional high-quality formats, including YUV (.avi), XD-CAM (.mxf), DPX Log (.dpx), ProRes 422 (.mov), MPEG2 Intra (.mpg), DV25 (.dv) files. File processing can be defined by the operator on a per-job basis, and can be automated using pre-configured watch-folders, or driven by a third-party application on top of NexGuard Manager API.

The Figure 4 hereafter illustrates the specific case of watermarking by the NexGuard system of master and preview versions of a given piece of content. The operations are driven based on pre-defined watch folders. A watch folder is defined on a per recipient basis.

In this example, content is encoded once as an MPEG file and then delivered to multiple recipients, each receiving a uniquely watermarked copy. The NexGuard system can consecutively perform both the file watermarking and then file transfer based on secure FTP.

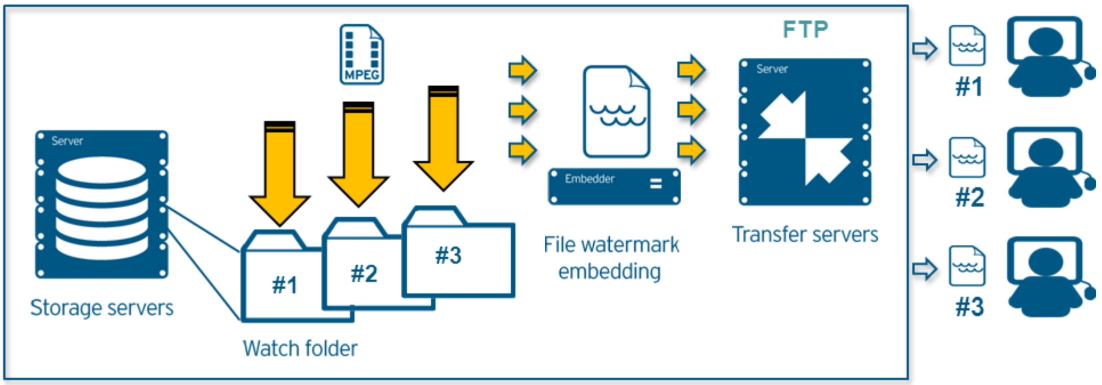


Figure 5: NexGuard file embedder solution with watch-folders

At the system level, the NexGuard Local Manager server may interface with various third-party media asset management (MAM) systems or workflow management solutions (please contact Civolution to obtain the updated list of integrated solutions).

b/ For serial numbering of content instances upon transcoding to custom format per recipient

Watermark embedding can be integrated as an image filter or audio filter during a content transcoding process. The NexGuard Embedder is then delivered as a watermarking plug-in for transcoder devices.

The solution ensures content watermarking whatever the source and destination file format.

Embedder
transcoder plug-in

Plug-in watermark embedding

NexGuard Embedder software can be integrated as part of a transcoding station in order to perform transcoding and watermarking in a single pass and for any output format.

Audio and video watermarking plug-ins are available. Both watermark types can be embedded in a given content.

The plug-in can be interfaced with NexGuard Manager for recipient definition, allocation of a unique watermark identifier per copy, and logging of operations.

The NexGuard Embedder plug-in can be integrated into various third-party ingest, encoding and transcoding systems as listed in the table hereafter.

Transcoding partners

Transcoder farm

Watermarking plug-ins can be made available for a variety of encoding and transcoding solutions including:

- iCR by **AmberFin**
- Compressor (Final Cut Pro) by **Apple** (*for ProRes 422 only*)
- StreamZ and Kayak by **Digital Rapids**
- Elemental Server by **Elemental Technologies**
- Grid Transcoding by **RadiantGrid**
- Carbon Coder and Carbon Server by **Rhozet / Harmonic**
- Agility (formerly Anystream) and Vantage by **Telestream**

c/ For serial numbering per session upon H.264 streaming or file downloading

With the increasing use of smart devices connected to the Internet, on-line screening established itself as an alternative to the disk. The OMD[1] solution is designed to avoid decoding and re-encoding each individual stream or file delivered to the end user. The content is transcoded only once at the "Pre-Processing" stage and it is then watermarked on the fly through a "Smart Embedder" upon on-line delivery. The concept of the OMD solution is illustrated in the Figure 5 below.

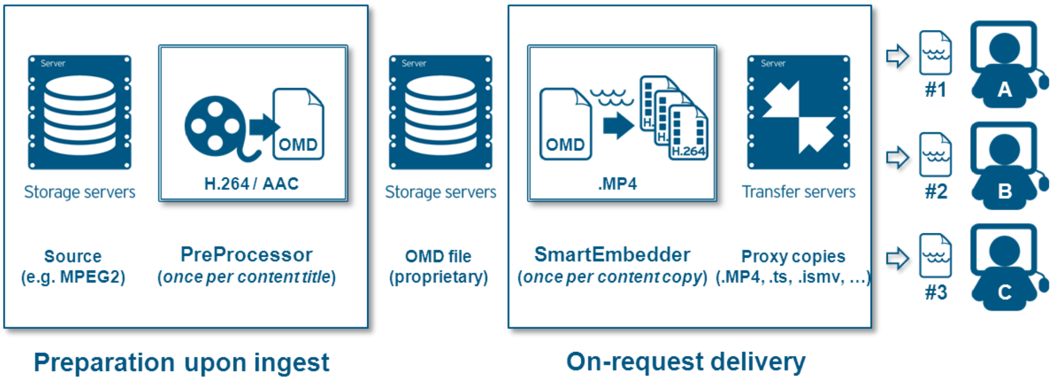


Figure 6: NexGuard OMD solution for download or streaming

[1] OMD stands for « On-line Media Delivery »

Integration to physical media duplication workflows

Content serial numbering based on digital watermarking technology can be organized upon duplication of physical media. Each duplication component – for DVDs or tapes – of the NexGuard Pre-Release forensic marking system is further described in the tables hereafter.

a/ For serial numbering of content on master tapes

Live Embedder product element Watermark embedding	Master live embedding devices offer real-time processing of audio/video signal over SDI input/output interfaces, for use upon tape duplication or during ingest of content. The solutions range from SD-SDI to dual-link HD-SDI for 444 RGB format as used on HDCAM SR video tape recorders (VTR). The solution can encompass video watermarking as well a sophisticated visible marking for logo overlay and text keying.

The Figure 6 hereafter illustrates the watermark embedding upon tape duplication. It is possible to perform a QC detection of the watermark during quality control of the tape.

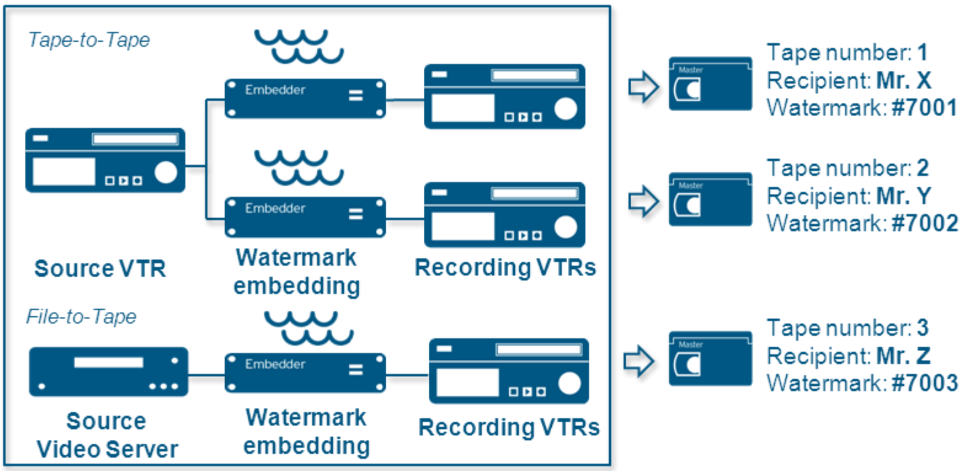


Figure 7: NexGuard Master solution for tape duplication

b/ For serial numbering of video content as DVD screeners

Screener product element Watermarking in DVDs	The Screener solution is a turnkey system which combines watermark embedding, DVD burning and label printing. The system is scalable and can typically produce 100 DVD5 copies in less than 5 hours. The DVD content may also be protected against copying by using third-party anti-rip and controlled playback technology. Video processing for individual copies can combine invisible watermarking and visible marking with either serial number or recipient initials as video overlay.

The NexGuard Screener component integrates with third-party duplication robot and anti-rip technology as listed in the table hereafter.

DVD duplication partners DVD duplication robot	The Screener solution is a turnkey system which interfaces with third-party DVD duplication robots: • 5400N, 5410N and 8100N by Rimage The DVD content may also be protected using third-party technology: • Patronus anti-rip protection by Fortium • PIN-Play playback protection by Fortium

The NexGuard Screener solution produces DVD5 or DVD9 type DVDs which can be played on a regular computer or home-theater system.

Key benefits of NexGuard – Pre-Release solution

NexGuard - Pre-Release forensic watermarking solution offers the critical benefits of organizing content copy identification, with minimum impact on operations, through a combination of leading-edge digital watermarking technology and workflow-driven system application.

Deterrent against piracy

The watermarking solution fulfills the following anti-piracy objectives:

- Unaltered viewer experience and identical playability on targeted devices,
- Compatible with further video processing (eg. use of DRM to secure file delivery),
- Survivability of the watermark in case of conversion, compression, etc.
- Blind watermark detection to identify the source of leakage in case of actual piracy.

Enterprise-level system for decentralized operations

The NexGuard - Pre-Release solution can be rolled out throughout an organization:

- Scalable multi-site multi-user system with web-based graphical user interface,
- Forensic marking system integrated to existing workflows,
- Consolidation of watermarking-related data into a global database,
- Aggregation of data from outsourced operations for inter-organization workflows.

Versatile solution for multiple workflow types

The processing elements for identifying individual content copies can handle all workflow situations:

- Duplication of tape or DVD media (e.g. masters and screeners),
- Copying and transfer of formatted files (e.g. dailies and preview proxies),
- Watermarking upon transcoding for delivery in a custom format for each recipient (e.g. repurposing for Internet portals).
- Watermarking upon on-line delivery with a unique identifier per session without the need to decode and re-encode each individual file or stream.

Automated production operations

The file-based digital workflows can be pre-defined:

- Standalone watermarking systems can be based on watch folder per recipient,
- Systems with watermarking upon transcoding can be based on watch folder per recipient and per format,
- Operations can be monitored with a control dashboard,
- Both audio and video tracks can be watermarked
- Combined systems (eg. transcoding, watermarking, transfer) can be supervised and driven by a third-party MAM or workflow management application.

The screener duplication can output ready-to-ship DVDs:

- Import or definition of the recipient list from the database,
- Automatic watermark embedding and initial overlay in the MPEG2 video,
- Printing of a label with recipient name or serial number on the DVD.

For more information

Contact

Civolution NexGuard - Pre-Release forensic watermarking solutions are widely deployed and successfully used by movie studios, TV content producers and post-production facilities worldwide.

For more information please contact us: info@civolution.com

or visit our web site:
http://www.civolution.com/applications/media-protection/nexguard-pre-release/

Follow us on Twitter: @Civolution

References

[1]: Andy Baio
Pirating the 2011 Oscars – Waxy – January 2011.
http://waxy.org/2011/01/pirating_the_2011_oscars/

Pirating the Oscars 2012: Ten Years of Data – Waxy – January 2012
http://waxy.org/2012/01/mpaa_wins_the_oscar_screener_battle_but_loses_the_war/

[2]: MPAA
Best Practice re. Screener Digital Transfer Services – December 2011
http://www.fightfilmtheft.org/best-practice.html