FORENSIC WATERMARKING FOR UHD VIDEO

Gwenaël Doërr

Technicolor R&D France

Security & Content Protection Lab

VSF
VIDEO SERVICES FORUM

technicolor
FEEL THE WONDER

Agenda

Forensic watermarking

- Essentials
- MovieLabs specification
- Baseband vs. bit stream

System considerations

- Trust management
- Physical media
- OTT
- Broadcast

UHD-specific Challenges

- High resolution and high frame rate
- High dynamic range
- Scalable encoding

Take-away Lessons

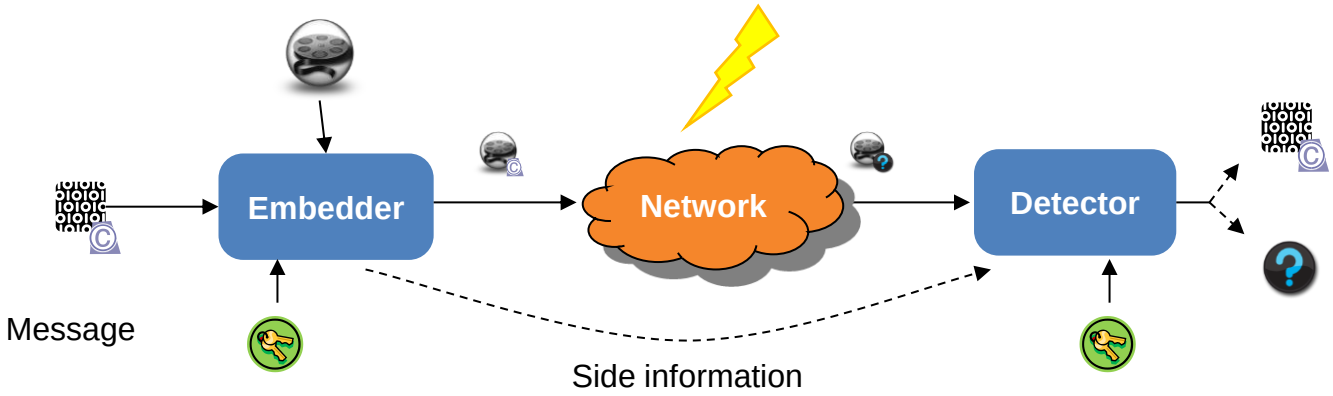
Forensic Watermarking

Digital Watermarking

Digital watermarking is a technique which imperceptibly alter digital content to hide a message in a robust manner. It is in some sense similar to invisible ink and paper watermarks.

- The watermark is inherently bound to the content
  - Cannot be removed without damaging content
  - Survive format conversion i.e. close the analog hole
- The hidden message can (a priori) be anything
  - Application use case dependent
  - Copy/playback control information, identifier, metadata, etc.

Watermarking in a Nutshell



Watermarking = communications channel

Blind vs. non-blind detection ⇒ impact on supported use cases

Performance metrics: fidelity, robustness, security, embedding rate, complexity

- Application-dependent trade-off

Forensic Watermarking a.k.a. Traitor Tracing

Goal: identify the source of a leak

- Complementary to conventional content protection
  - Cryptography (CAS/DRM) = piracy prevention
  - Watermarking = piracy deterrence

Strategy: serialize content using watermarking at rendering or distribution time

Payload: user identity, device identity, software version, …, *anti-collusion codes*

Example deployments

- Pre-theatrical release screeners
- Digital cinema
- Premium content VOD & hospitality market

MovieLabs Specification

Specification for enhanced content protection

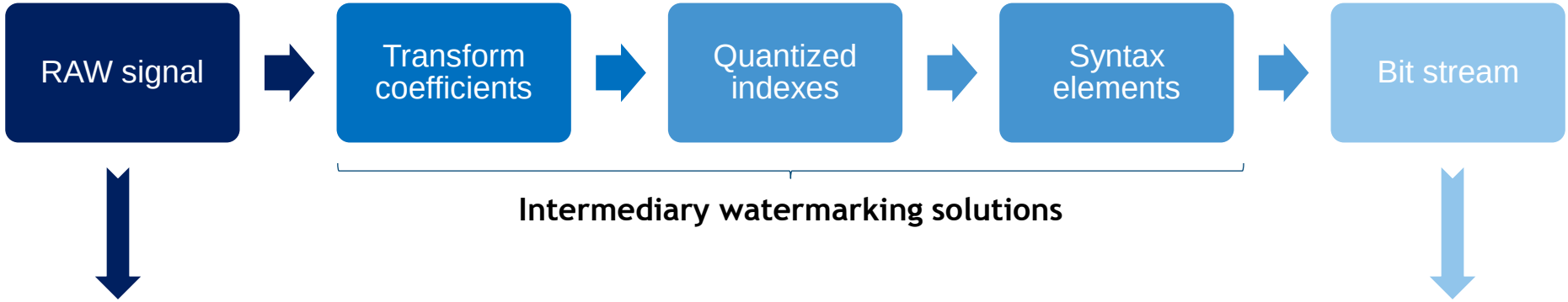
- Released Fall 2013; updated February 2015

Mandates forensic watermarking for premium content

- *The system shall have the ability to securely forensically mark video at the server and/or client to recover information necessary to address breaches*
- *The watermarking shall be robust against corruption of the forensic information*
- *The watermark shall be inserted on the server or on the client such that the valid insertion is guaranteed during playback even if the device and its secrets are compromised*

Opens business perspective for mass market deployment

From Baseband to Bit Stream Watermarking



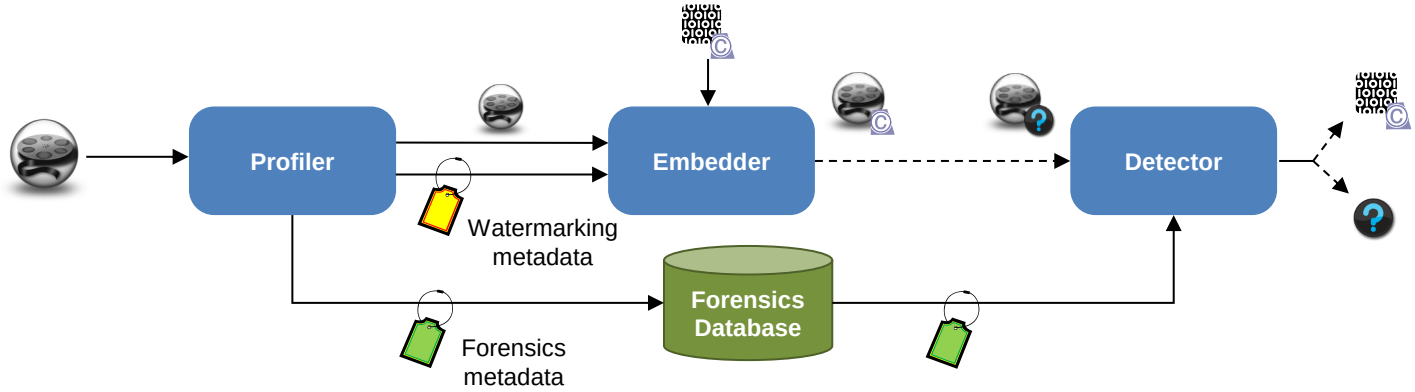
Baseband (a.k.a. raw) watermarking

~30% of the proposed watermarking algorithms
Majority of commercially deployed systems
☺ Direct access to the signal
☹ Computational complexity
☹ Full decompression-recompression loop in transit
☹ Integration to encoder/player introduces dependencies

Bit stream watermarking

<<1% of the proposed watermarking algorithms
Novel paradigm with marginal deployment
Smooth integration in existing workflows ☺
Codec-dependent solutions ☹
Non-blind detection ☹
Container and signaling management ☹

2-Step Bit Stream Watermarking



- Computational cost shifted to a preprocessing step
- Blitz-fast embedding engine with minimal memory footprint
- Controllable bandwidth overhead to forward watermarking metadata
- Non blind detection

System Considerations

A Matter of Trust

Bypassing the watermarking module = content available in clear

- Strategy used by pirates to bypass BD playback control watermarks

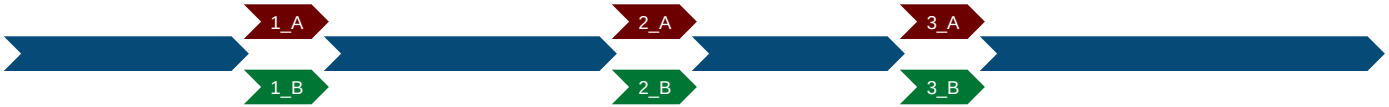
Where and when placing the watermark?

- On the distribution side
  - Not applicable in some application use cases e.g. broadcast environment
  - Avoiding leaks from the content distributor: watermarking in the encrypted domain, corruption of the bit stream
- On the reception side
  - Hardware implementations: secure… but costly
  - Software implementations: unsecure ⚠

Physical Media

Variants proposal (for Blu-ray discs)

- Alternate versions (2× or more) of small segments of the movie
- Rendered segments selected depending on the keys of the BD player



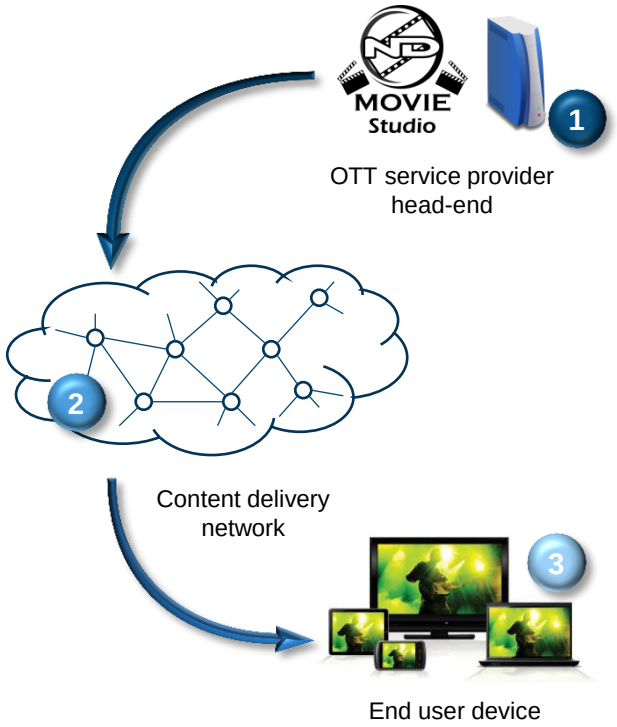
- ☺ Virtually no footprint of the watermarking process in the device
- ☺ Enables emulating bit stream watermarking with baseband systems
- ☺ Security inherited from cryptographic primitives
- ☹ Sub-optimal robustness ↔ embedding rate trade-off
- ☹ Sub-optimal storage overhead
- ☹ Complex mastering process during production

Physical Media

Watermarking engine embedded in the rendering device

- ☺ Marginal to no impact for content mastering
- ☺ Full control over the watermarking engine to optimize performances
- ☹ Tedious/costly integration depending on the watermarking technology
- ☹ Lack of standardization for device manufacturers
- ☹ Legal issues ?

OTT Distribution



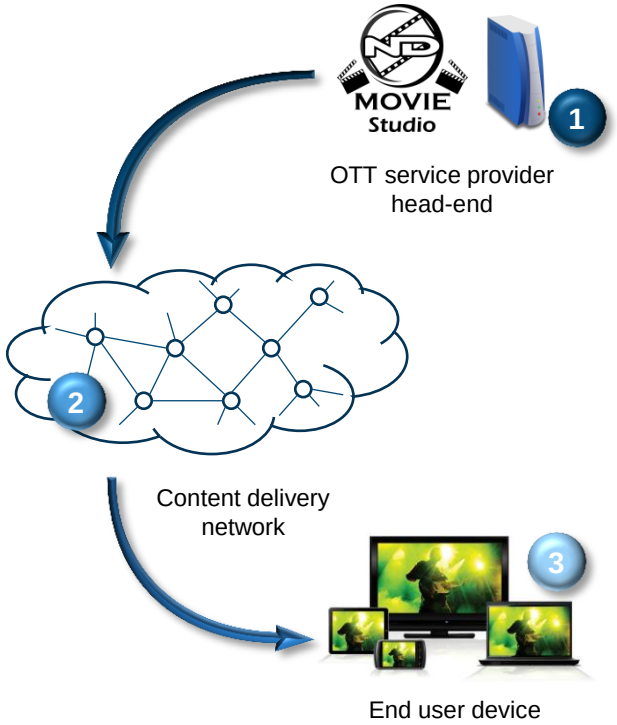
Three alternate places for watermark embedding

1. OTT service provider head-end
2. Nodes of the content delivery network
3. End user device

Watermarking and (adaptive) streaming

- On-demand delivery of pre-watermarked segments
  - Extension of the variants strategy e.g. using different manifest files
- On-demand watermarking of delivered segments
  - Harmonization of the watermarking throughput across qualities
  - CDN trust/liability issue except if watermarking encrypted content

OTT Distribution



Technical trade-off

- Storage overhead
- Cache-cancellation side effect
- Computational overhead
- Battery consumption
- Integration cost
- Scalability
- …

No solution fits all application use cases

Broadcast Delivery

By design, watermark serialization occurs on receiver side

- Dedicated proprietary hardware ⇒ increased cost and lower renewability
- Generic standard hardware (OpenPlatform, TrustZone)

Mitigating rebroadcast of live performances

- Sport, concerts, etc
- Pipe/consumer tracing granularity
- Live watermark embedding (and detection)
- Complex integration for bit stream solutions
  - Broadcast delay vs. profiling time

UHD-specific Challenges

More and Deeper Pixels

Ultra high definition (UHD)

- Resolution: 1080p → 4k / 8k
- Frame rate: 25/60 fps → 100+ fps
- Pixel coding: 8 bits → 10+ bits

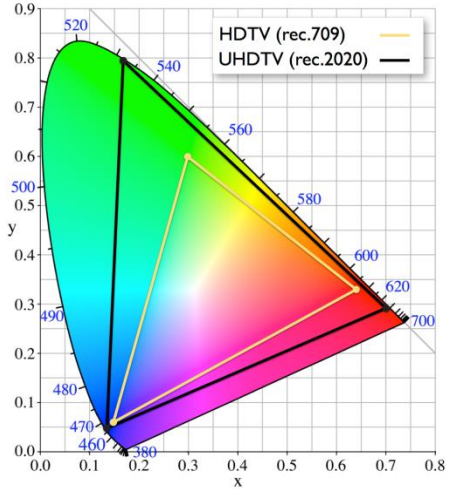
⇒ More (complex) samples to process per second

Baseband solution = increased computational burden

Dealing with a New Playground

HDR/WCG ruled by new pixel coding laws

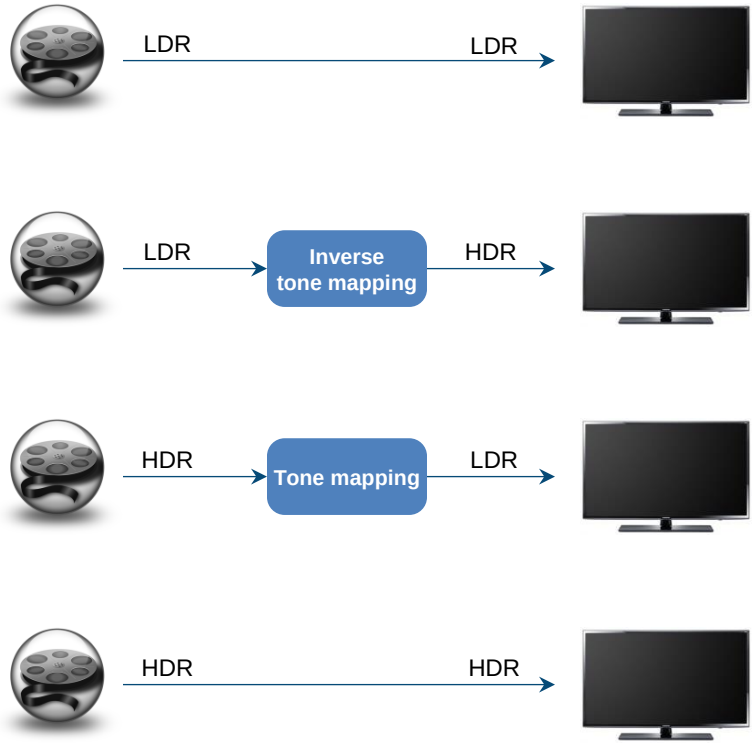
- Watermark fidelity ⇒ embedding distortion just below the human perceptibility threshold
- Perceptual models for lossy compression only marginally relevant for watermarking
  - Revise existing recipes ⇒ tedious evaluation campaigns
  - Re-use non-optimized strategies



Unclear adversary = challenging robustness

- Uncertainty about the piracy workflow

Supporting Legacy Equipment



Gradual transition to HDR

- Co-existence of two ecosystems
- Conversion mechanisms

Typical requirements

- Watermark invisible in HDR and LDR
- Watermark detectable in HDR and LDR

Technical challenges for watermarking

Video Delivery to Heterogeneous Devices

Rendering screens: TV, computers, tablets, smartphones

- Adaptive streaming (broadband)
- Scalable video encoding (broadcast)

Integration cost of baseband solutions for multiple platforms

Smooth extension for baseband solutions

- More challenging for bit stream solutions due to codec dependency
  - Watermarking throughput harmonization through qualities

Take-away Lessons

Conclusions

Forensic watermarking will be mandatory for (UHD) content delivery

- Provides a tracing mechanism to deter piracy
- Offers a competitive advantage to provide premium content

Two main watermarking paradigms

- Pros and cons for integration in existing platforms
- Technical challenges to support some UHD features

Both strategies can be adapted to support all scenarios

- Integration cost advantage may differ depending on the particular use case

Thank you

Contact details

Gwenaël Doërr – Principal Scientist
gwenael.doerr@technicolor.com

Alain Durand – Business Development
alain.durand@technicolor.com