Gwenaël Doërr

Technicolor R&D France
Security & Content Protection Labs
gwenael.doerr@technicolor.com

Watermarking-based Traitor Tracing to Deter Piracy of Entertainment Content

technicolor
Security Laboratories

Technicolor at a Glance

Who We Are

Technicolor, a worldwide technology leader in the media and entertainment sector, is at the forefront of digital innovation.

Our world class research and innovation laboratories and our creative talent pool enable us to lead the market in delivering advanced services to content creators and distributors.

We also benefit from an extensive intellectual property portfolio focused on imaging and sound technologies, supporting our thriving licensing business.

Our Mission

Developing, creating and delivering immersive augmented digital life experiences that ignite our imagination.

c.350
RESEARCHERS AND EXPERTS

OSCAR® NOMINATIONS
FOR 25 FILMS SERVED BY TECHNICOLOR

6,000+
FILM & ADVERTISING VISUAL EFFECTS SHOTS

3
RESEARCH CENTERS:
RENNES
HANOVER
LOS ALTOS

300
MILLION DIGITAL HOME DEVICES SHIPPED TO DATE

80 %
OF CONSUMER ELECTRONICS MANUFACTURERS INTEGRATE OUR IP

7+%
OF PATENT PORTFOLIO RENEWED EVERY YEAR

TOUCHING 75 %
OF BLOCKBUSTERS WORLDWIDE IN 2013

1.47 BILLION
DVD AND BLU-RAY™ SHIPPED TO 40,000 DESTINATIONS IN 2013

265,000+
DIGITAL CINEMA DELIVERIES

#1 IN GATEWAYS

#2 IN SET-TOP BOXES

WORLDWIDE IN TERMS OF SHIPMENTS

technicolor
Security Laboratories

Agenda

Piracy of Entertainment Content

Robust Watermarking

Flicker Forensics

Research Outlook

Questions and Answers

Acknowledgements: Séverine Baudry, Bertrand Chupeau, Antoine Robert, Mario de Vito, *Xavier Rolland-Nevière*, *Adi Hajj-Ahmad*, *Omar Alvarez*, *Cherif Ben Zid*

Piracy of Entertainment Content

technicolor

Security Laboratories

The Challenging Transition to Digital

Key specificities of digital content

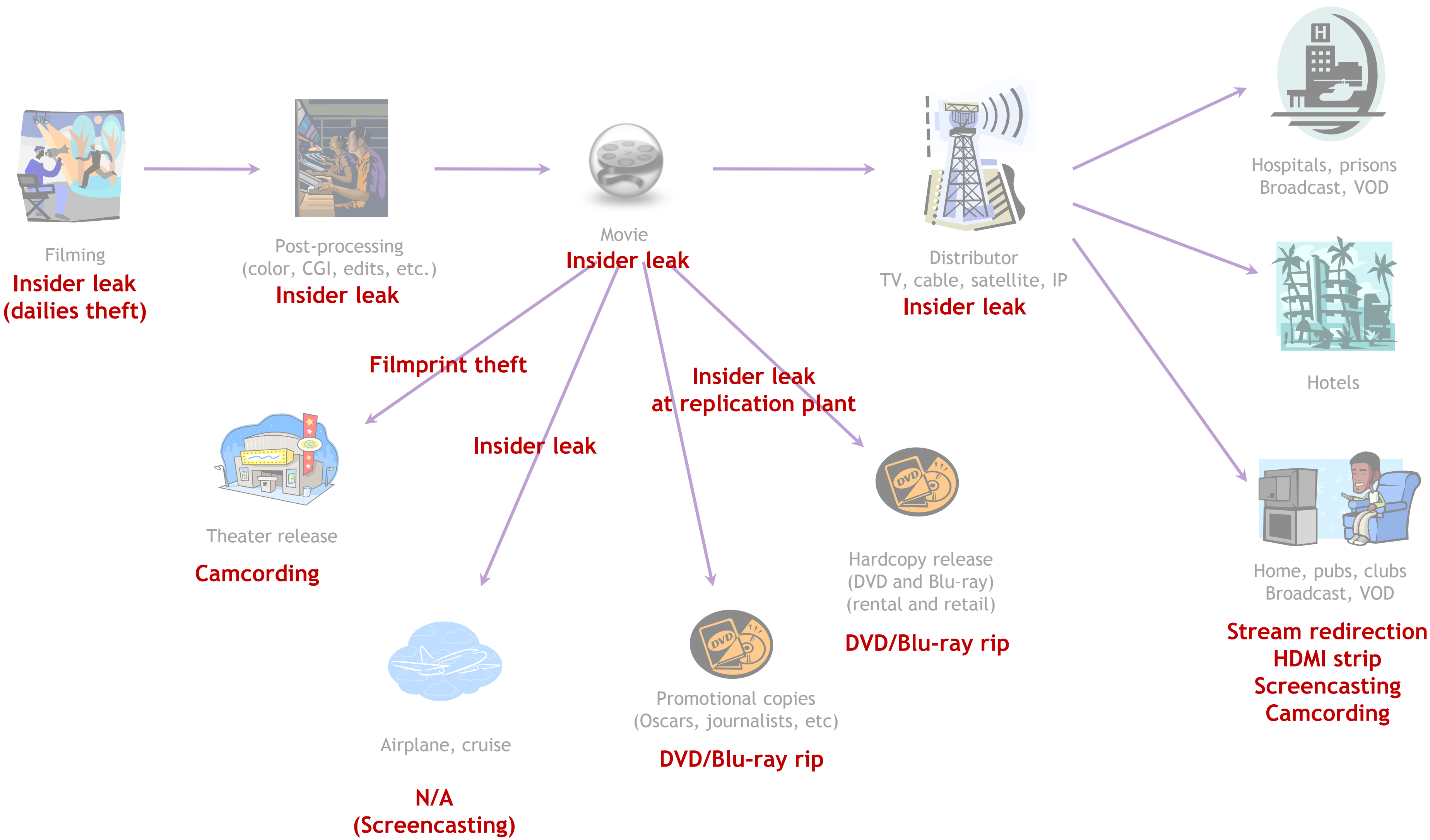
- Clones rather than copies i.e. no more generational degradation
- Assets can be tangible or intangible
- Ease of dissemination i.e. the world is at your doorstep

Apparition of a bestiary of pirates (Courtesy: Irdeto)

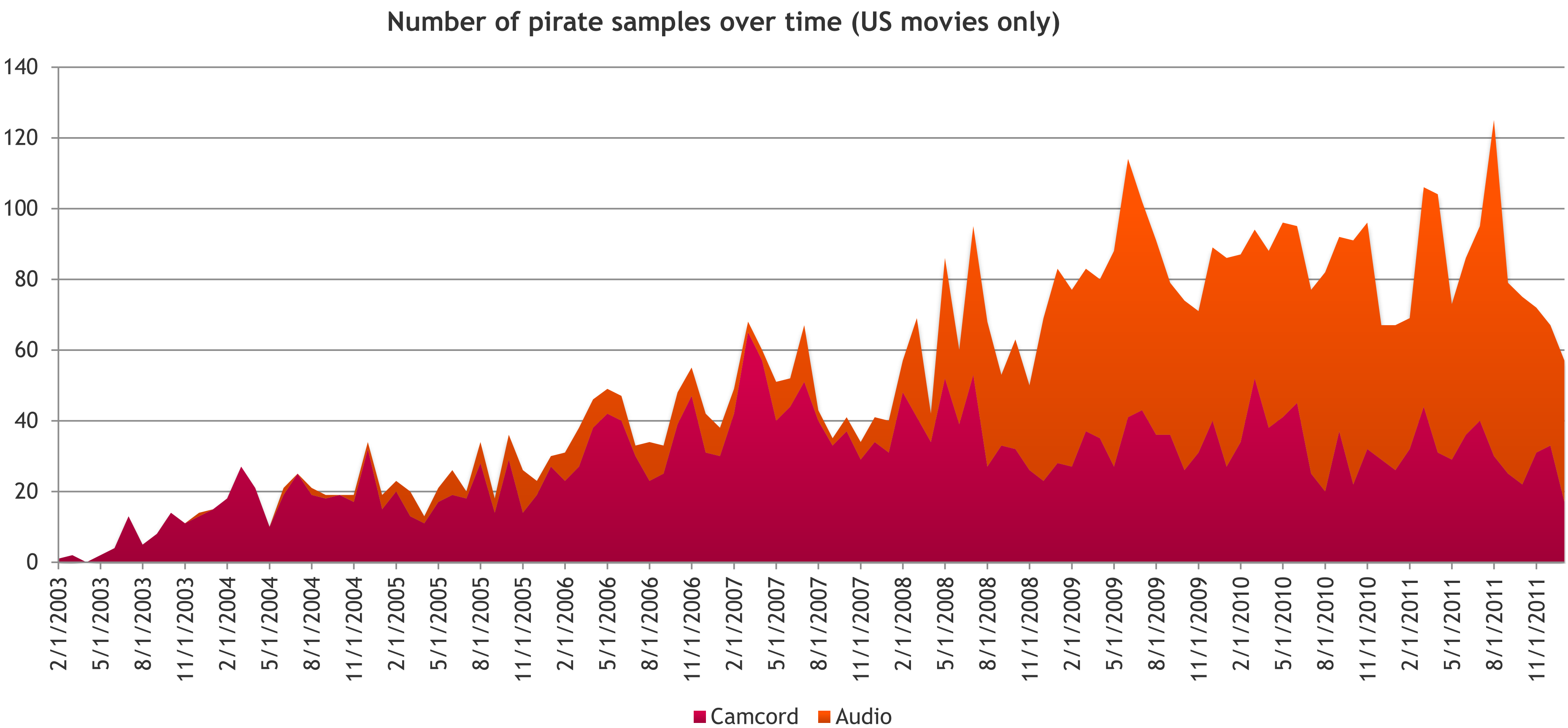
On the cost of piracy…

CNBC's Crime Inc #10: Hollywood Robbery (August 2012)

Threat Analysis

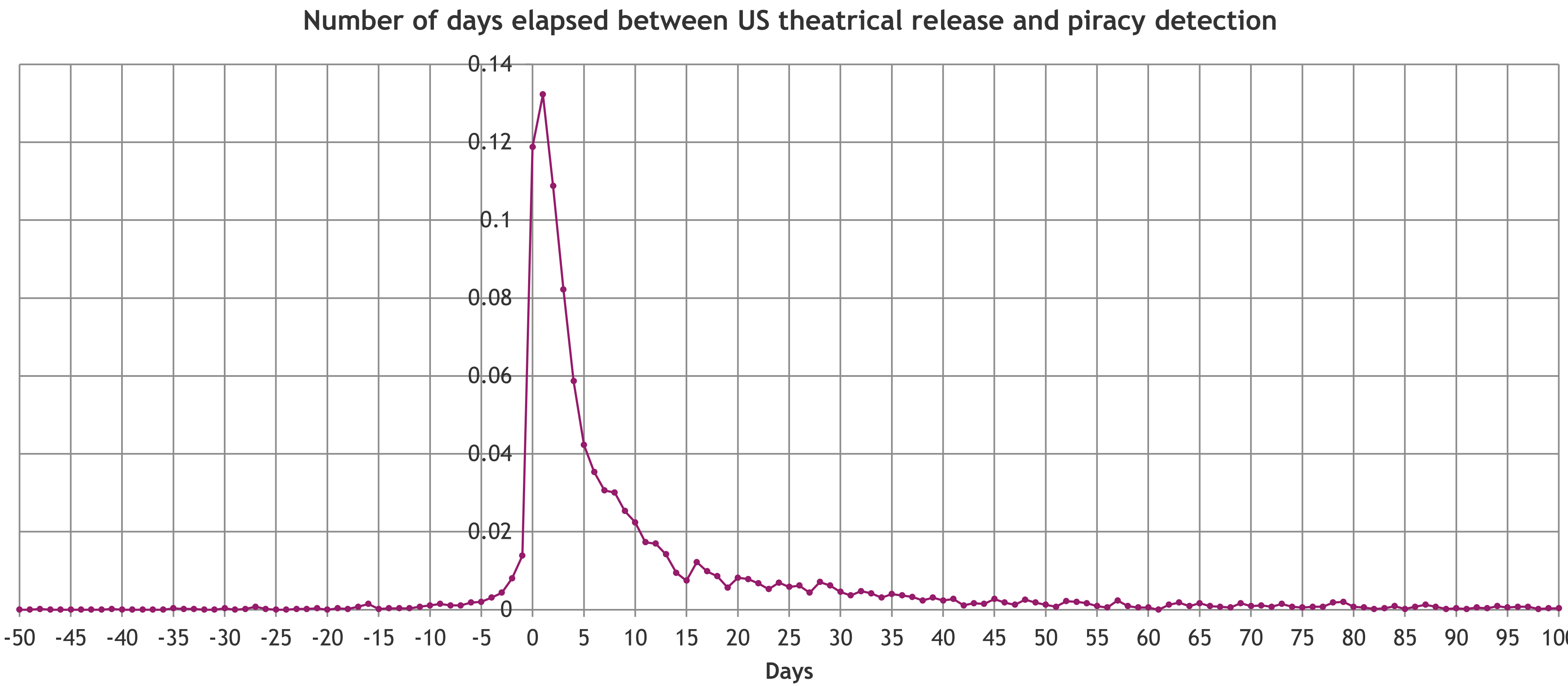


In-Theater Camcording over the Years



technicolor
Security Laboratories

Time-to-Black-Market



technicolor
Security Laboratories

Anti-Piracy Arsenal

Regulate
- WIPO 1996 (DMCA, EUCD, Hadopi, etc.)
- SOPA/PIPA

Inform / Educate
- FA©T anti-piracy information campaigns
- Hard-to-counterfeit security features
  - Intaglio, color-shifting inks, holograms, CDIs

Prevent
- Content encryption aka. CAS and DRM
- Anti rip
- Playback/record control

Interfere / Jam
- Anti-recording e.g. Macrovision
- Anti-camcording

Monitor / Scout
- Data loss prevention systems
- Content fingerprinting

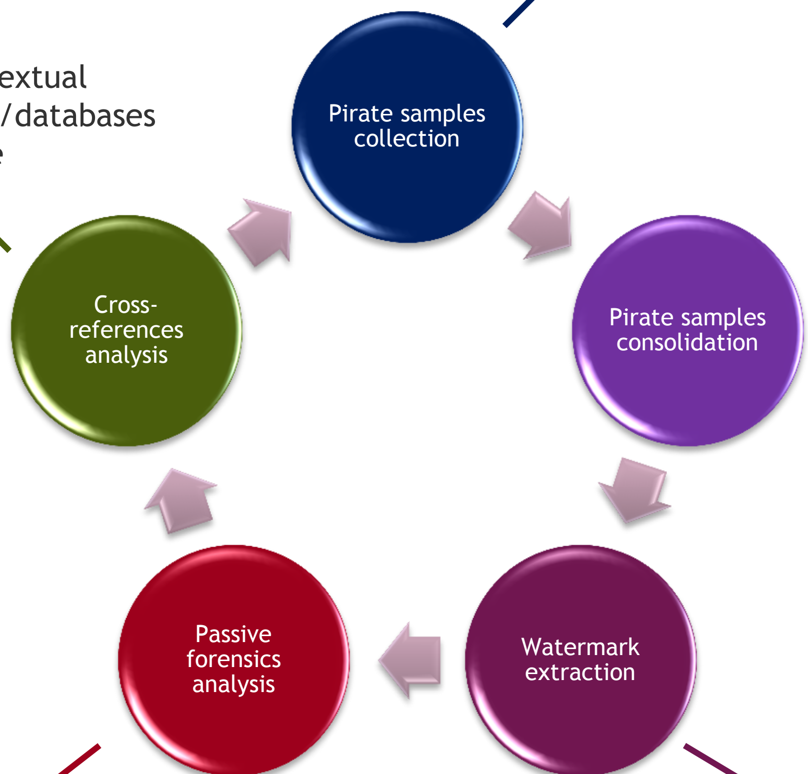
Trace
- Digital watermarking
- Passive forensics

technicolor
Security Laboratories

The Forensics Landscape

Outsourced
Internet Crimes Group, Deluxe (WEBWatch), Irdeto (Bay TSP), private investigators, blueSpike

Operated by MPAA
Manual process mostly relying on textual metadata collated in spreadsheets/databases e.g. the pirate release group name



Outsourced
Manual Process?

Mostly operated by Deluxe/Technicolor
Manual process typically involving tedious audio-visual inspection

Mostly operated by Deluxe/Technicolor
with detectors bought/licensed from WM vendors e.g. Civolution, Verimatrix, Irdeto, Verance, (Technicolor) or through web portals

Robust Watermarking

technicolor
Security Laboratories

Digital Watermarking

Digital watermarking is a technique which imperceptibly alters digital content to hide a secret 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 e.g. close the analog hole
  - The hidden message can (a priori) be anything
  - Copyright information, rights, customer ID, traitor tracing code, etc
- It is an active process
- Watermarking ≠ visual overlay

Performances Metrics

Fidelity: perceptual impact of the watermark embedding process

- Difficulty to accurately predict human perception

Robustness: ability to survive common signal processing primitives

- Filtering, lossy compression, resampling, valuemetric scaling, etc

Security: ability to withstand hostile attacks from malicious adversaries

- Protocol attacks, statistical attacks

Embedding rate: amount of data which can be reliably transmitted through the watermarking channel

Computational complexity at embedder / at detector

The trade-off between these conflicting parameters needs to be adjusted depending on the targeted application.

Watermarking Applications

Copyright protection

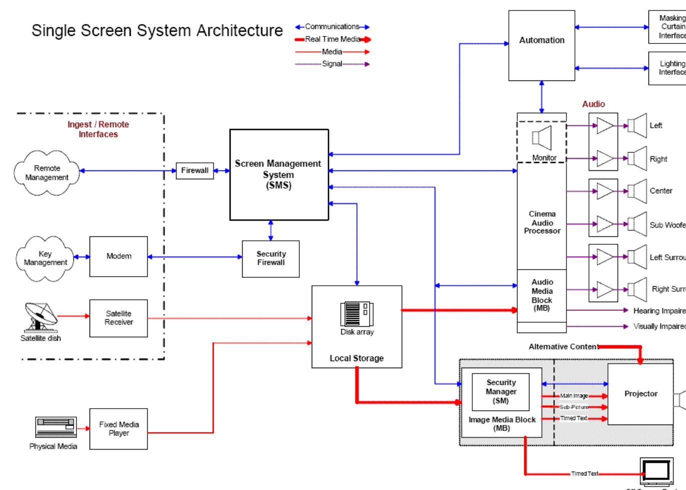
- Copy/Playback protection
- Broadcast monitoring / Audience measurement
- Content serialization for traitor tracing
  - Pre-release content distribution
  - Digital cinema
  - Premium VoD content
  - Next generation video (4k/HDR)

B2B (Pre-release content distribution, Digital cinema, Premium VoD content)

B2C (Next generation video)

Media enrichment

- Second screen applications
- Metadata binding



Traitor Tracing

Goal: identify the source of a leak

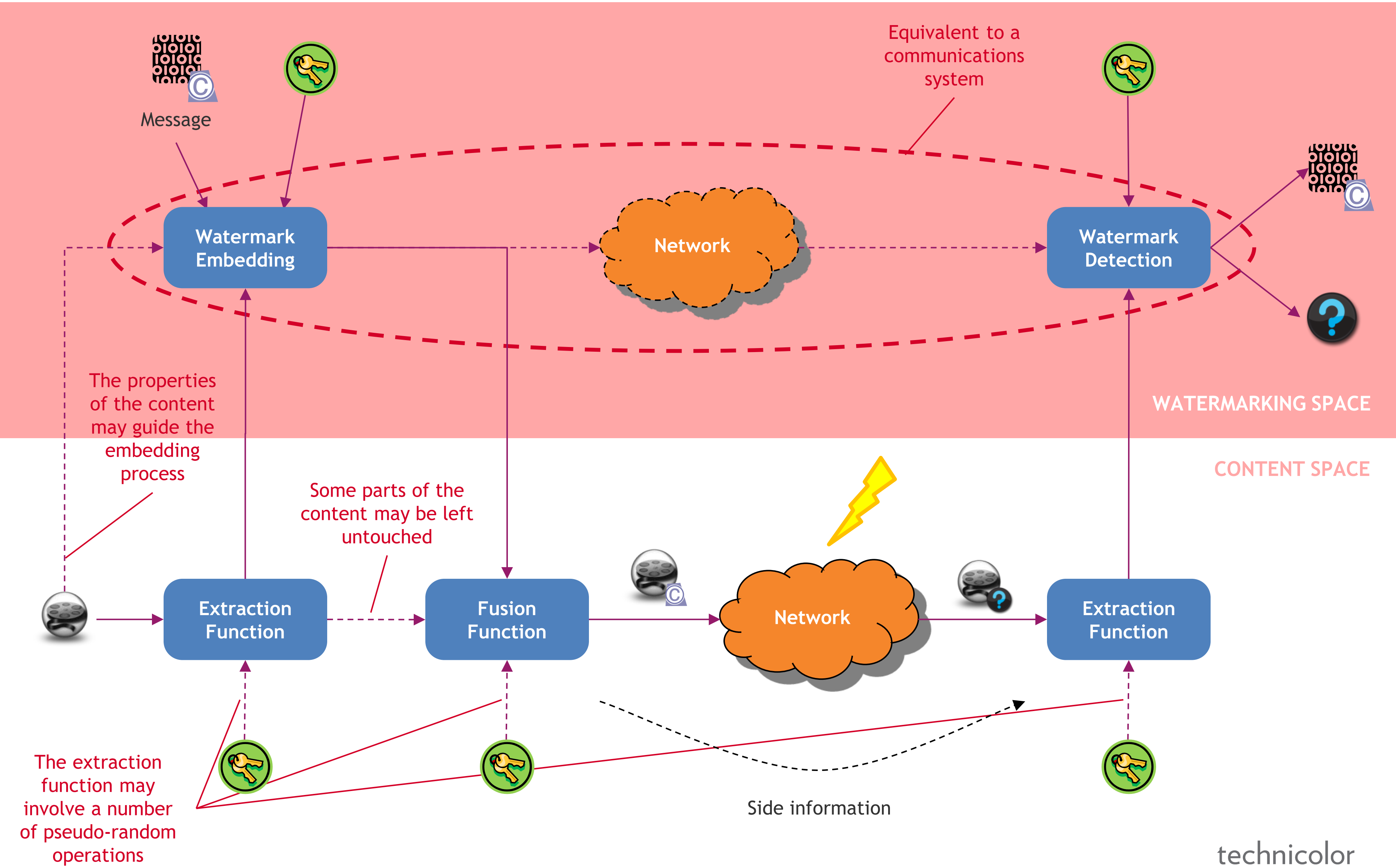
Strategy: serialize content using individual watermarks at distribution/presentation time or in transit

- On the fly, before distribution (e.g. for VOD)
- At presentation time (e.g. STB, BD player)
- At end-user home entry point (e.g. ISP gateway)

Payload: user identity, device identity, software version, [anti-collusion codes]

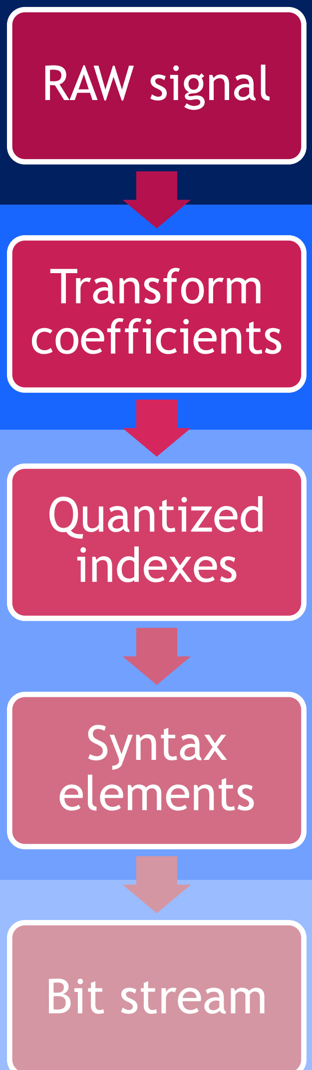
technicolor
Security Laboratories

Generic Watermarking Framework



technicolor
Security Laboratories

From the RAW Signal to the Compressed Bit Stream



RAW domain

~30% of the proposed watermarking algorithms
Easiness of implementation and understanding
Requires full decompression-recompression loop to support compression

Signal transform

Transform domain

~50% of the proposed watermarking algorithms
Better control over the placement of the watermark energy
Avoid forward/backward transform to support compression

Quantization

Compressed domain

~20% of the proposed watermarking algorithms
Only entropy coding to support compression

Predictive encoding
(DPCM, run-level, zig-zag scan, etc)

Entropy coding
(Huffman, arithmetic)

Bit stream domain

<<1% of the proposed watermarking algorithms
Difficulty of tampering directly the bit stream (usually catastrophic)
Readily support for compression with no overhead guarantee

Technicolor's Video Watermarking

Requirement: smooth integration in existing workflows

- Avoid decompression/recompression at embedder

Solution: watermark process directly in the compressed bit-stream

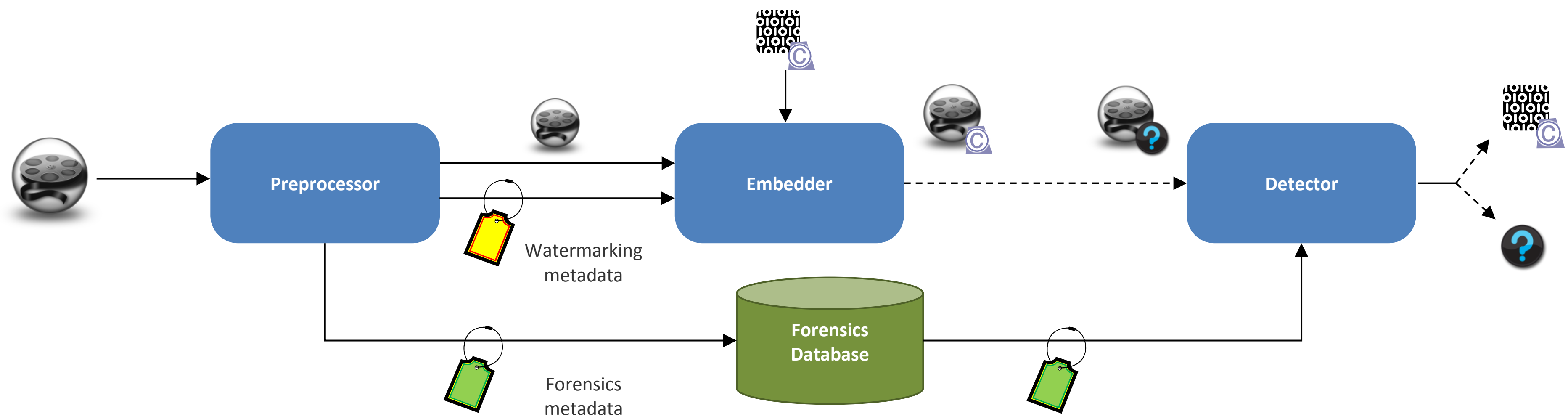
Two steps embedding process

- Computationally intensive pre-processing
- Blitz-fast switch-based embedding

Semi-blind detection process

- Registration of the tested sample using content fingerprints
- Detection of the watermark signal using reference metadata

Two-steps Watermarking



Watermark embedding metadata

- Out of band transmission
- In-band transmission $\Rightarrow$ 1% overhead in average

technicolor
Security Laboratories

A Watermarked Frame

technicolor
Security Laboratories

Fact Sheet

Watermark embedding in the compressed domain

- Watermarking while in transit i.e. without decompression / recompression
- Supported format: H.264 AVC CABAC (main and high profile) ~ BD+ standard
  - Extension to HEVC in progress

Two-step embedding procedure

- Computational cost shifted to a pre-processing step
  - Computationally intense operations are performed only once
  - Identify embedding locations in the bit-stream and corresponding alternate values
  - Embedding metadata is forwarded to the embedder through an auxiliary channel
- Embedding ≈ byte-switching in the bit stream ⇒ blitz fast
  - Low-memory RAM and ROM footprint
  - Can operate on encrypted bit streams

Fingerprint-aided resynchronization process

- Robustness to severe distortion e.g. camcording, screencast, crude compression, etc

Application Use Case: e-Screener

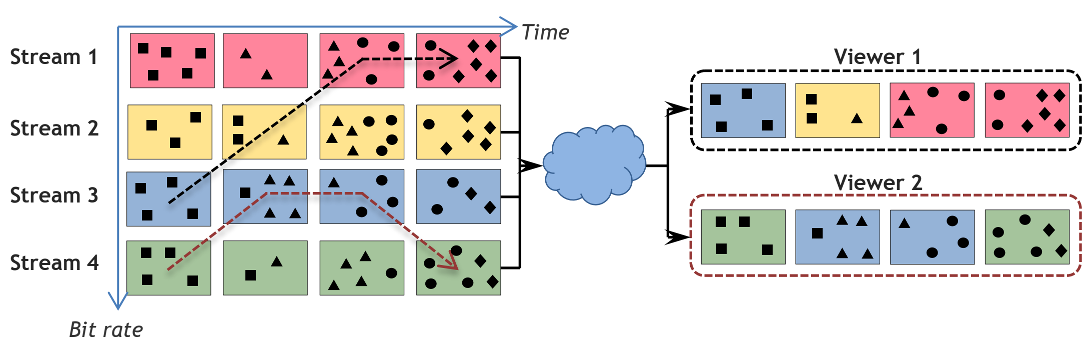
From TV-only to content everywhere

- Hard to secure all consumption devices
- Serialization watermarks to deter piracy

<u>Market:</u> dailies, screeners, premium content

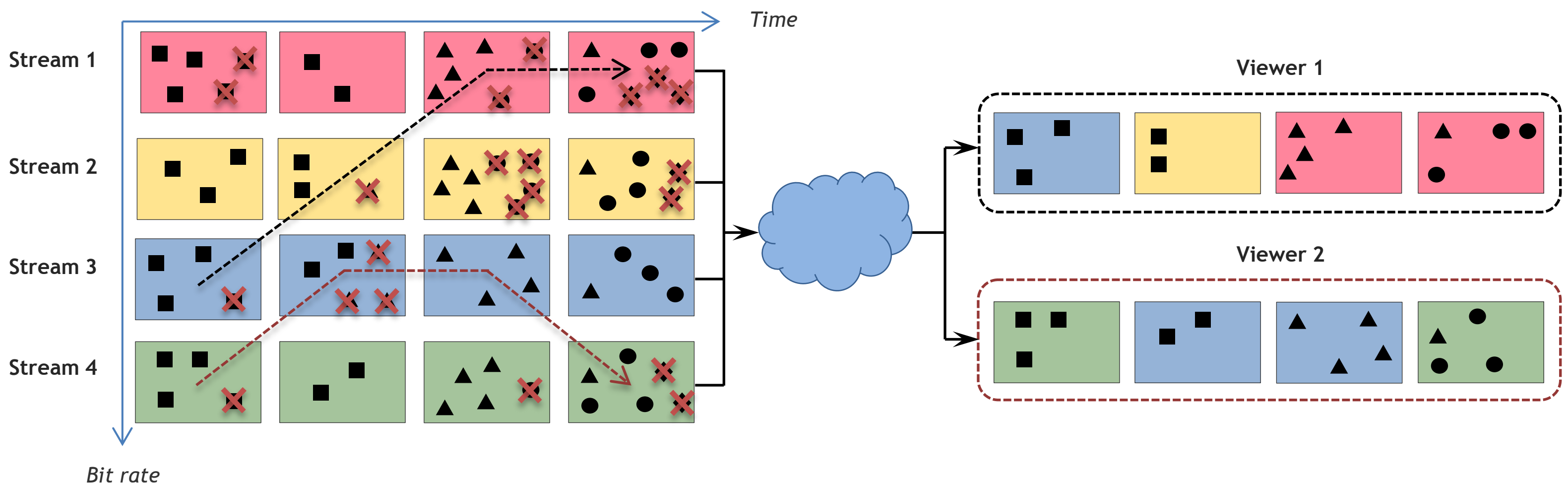
Technical challenges

- Constrained computing resources incl. battery life ⇒ bit-stream watermarking
- HTTP adaptive streaming ⇒ watermark modulation disruption



technicolor
Security Laboratories

Watermark Throughput Harmonization

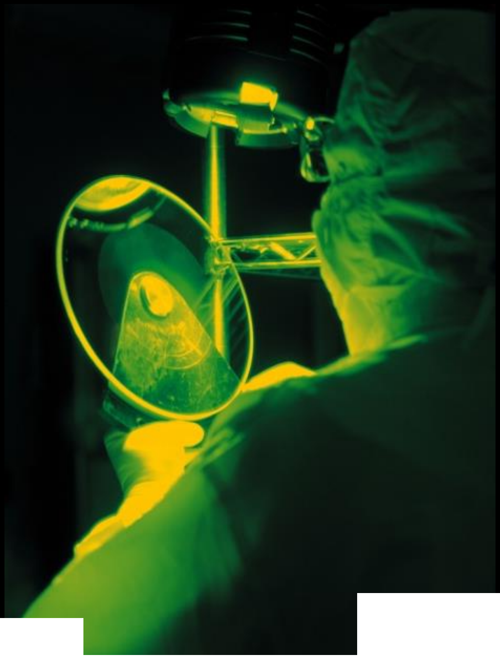


Briddle the embedding rate in line with the critical path

Demo video: forensic investigation after HAS & camcord

technicolor
Security Laboratories

Flicker Forensics



technicolor

Security Laboratories

Piracy Path Analysis

Motivation: model distortion introduced during piracy

- Fine tune watermark (tracing) settings
- Avoid unnecessary watermark detection trials
- Compensate for distortion prior to detection
- Metadata for cross-referencing pirate samples

Luminance flicker with camcorder recapture of LCD screens

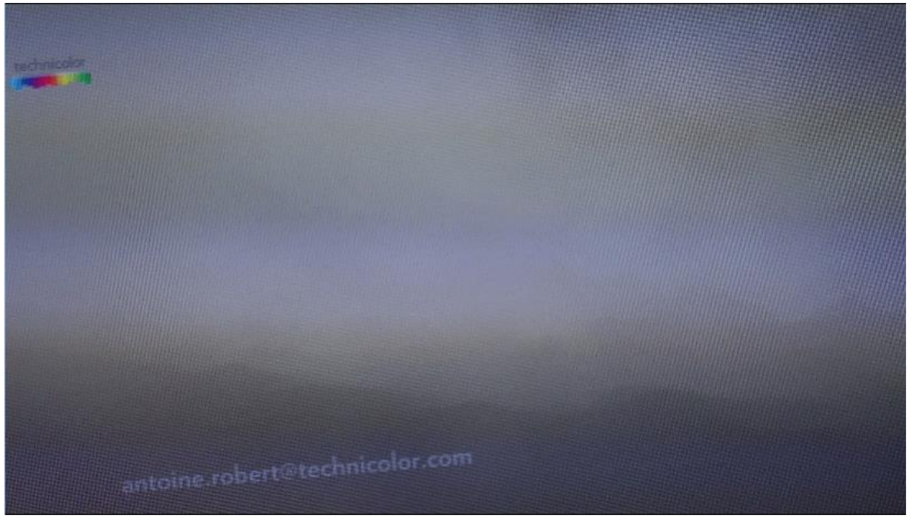
- Interplay between the screen frequency and the camera rolling shutter

technicolor Security Laboratories

Flicker Illustrated

Tell-tale visual artifacts

- Periodic spatio-temporal luminance variation
- Bright/dark stripes rolling down the screen



Video 1: visible flicker

Video 2: less visible flicker

technicolor
Security Laboratories

Flicker Model

Working assumptions

- Spatio-temporal misalignment has been compensated for
- Constant exposure (shutter speed)

Output luminance (camcorded)

Input luminance (displayed)

Periodic function

Phase

$$\mathbf{i}'(x, y, t) = \mathbf{i}(x, y, t) + (\alpha \mathbf{i}(x, y, t) + \beta).\Pi_{2\pi}(\omega_t t + \omega_y y + \varphi)$$

Flicker amplitude parameters

Flicker temporal frequency

Flicker vertical frequency

Connection with pirate devices parameters

Aliased backlight frequency

$$\omega_y = 2\pi \frac{f_t}{f_c}$$

Camcorder Frame rate

Frame read-out time (10-35 ms)

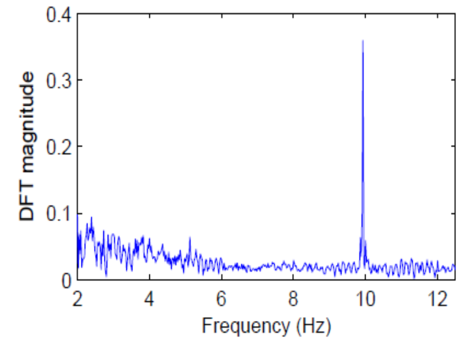
$$\omega_y = \frac{2\pi}{H} f_{\mathrm{BL}} T_{\mathrm{ro}}$$

Number of lines per frame (500-1000)

Backlight frequency (120-1000 Hz)

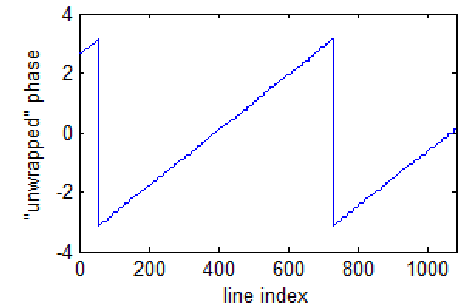
Pirate Device Identification

Scenario: candidates devices are seized at the home of a suspect and the objective is to want to check whether the recovered pirate samples could have been produced using them



ω_y estimation procedure

- Video frames ≈ 1D vector with row average luminance
- Temporal frequency analysis for one row ⇒ ω_t
- Phase at this frequency is linear by segment
  - Slope estimation ⇒ ω_y



Fallback estimation technique for corner cases

Camcord piracy identity

$$\underbrace{\frac{\omega_y H}{2\pi}}_{\text{Estimated using pirate video sample}} = \underbrace{f_{\mathrm{BL}} T_{\mathrm{ro}}}_{\text{Measured using suspect devices}}$$

Estimated using pirate video sample

Measured using suspect devices

technicolor
Security Laboratories

Experimental Results

Screens	Camcorders / T_{ro} (ms) / f_{BL} (Hz)	JVC 50fps	Panasonic 50fps	Sony 25fps	Toshiba 29.97fps
		13.5	16	15	32.65
Screen 1	240.06	(1, 1) ✓	(4, 2) ✗	(1, 3) ✓	(1, 4) ✓
Screen 2	180.43	(2, 1) ✓	(2, 2) ✓	(2, 3) ✓	(2, 4) ✓
Screen 3	159.98	(3, 1) ✓	(3, 2) ✓	(2, 1) ✗	(3, 4) ✓
Screen 4	120.00	(4, 1) ✓	(5, 1) ✗	(4, 3) ✓	(4, 4) ✓
Screen 5	146.61	(5, 1) ✓	(7, 1) ✗	(5, 3) ✓	(5, 4) ✓
Screen 6	226.70	(6, 1) ✓	(6, 2) ✓	(6, 3) ✓	(6, 4) ✓
Screen 7	172.80	(7, 1) ✓	(7, 2) ✓	(7, 3) ✓	(7, 4) ✓

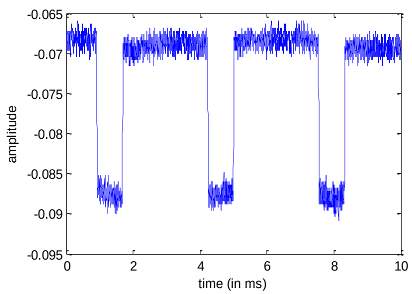
✗ Inaccuracies can result in classification errors,
e.g. (3, 3) is mistaken for (2, 1)
Expected LHS for (3, 3): $180.43 \times 15 = 2436$
Expected LHS for (2, 1): $240.06 \times 13.5 = 2400$

✓ 24/28 = 86%
Identified correctly

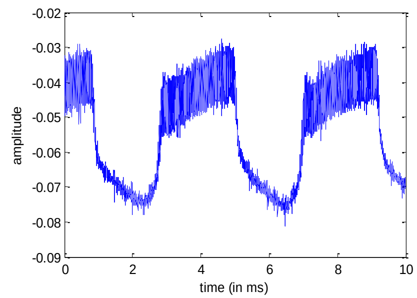
technicolor
Security Laboratories

Backlight Technology: CCFL vs. LED

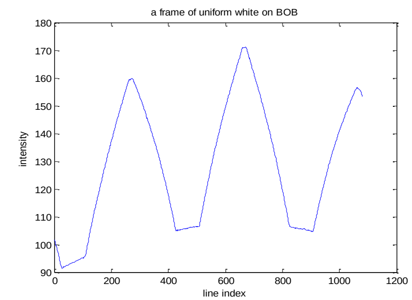
LED backlight



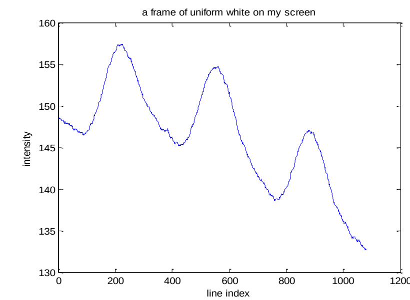
CCFL backlight



LED flicker



CCFL flicker



LED backlight signal has more discontinuities than CCFL

- Property inherited by the flicker signal present in the pirate video

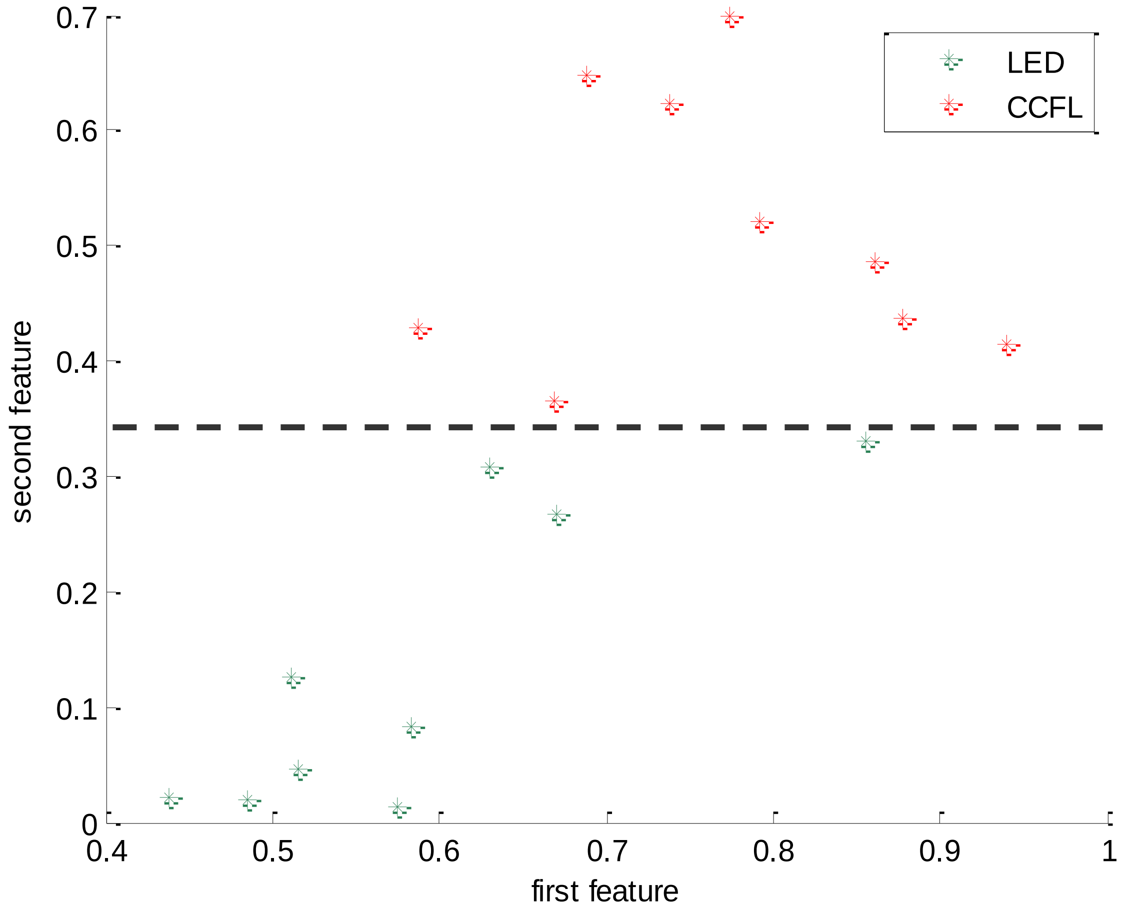
Flicker shape estimation

- High pass filtering (using least varying frames) ⇒ flicker signal estimate
- Alignment of individual flicker signal estimates
- Aggregation to improve SNR

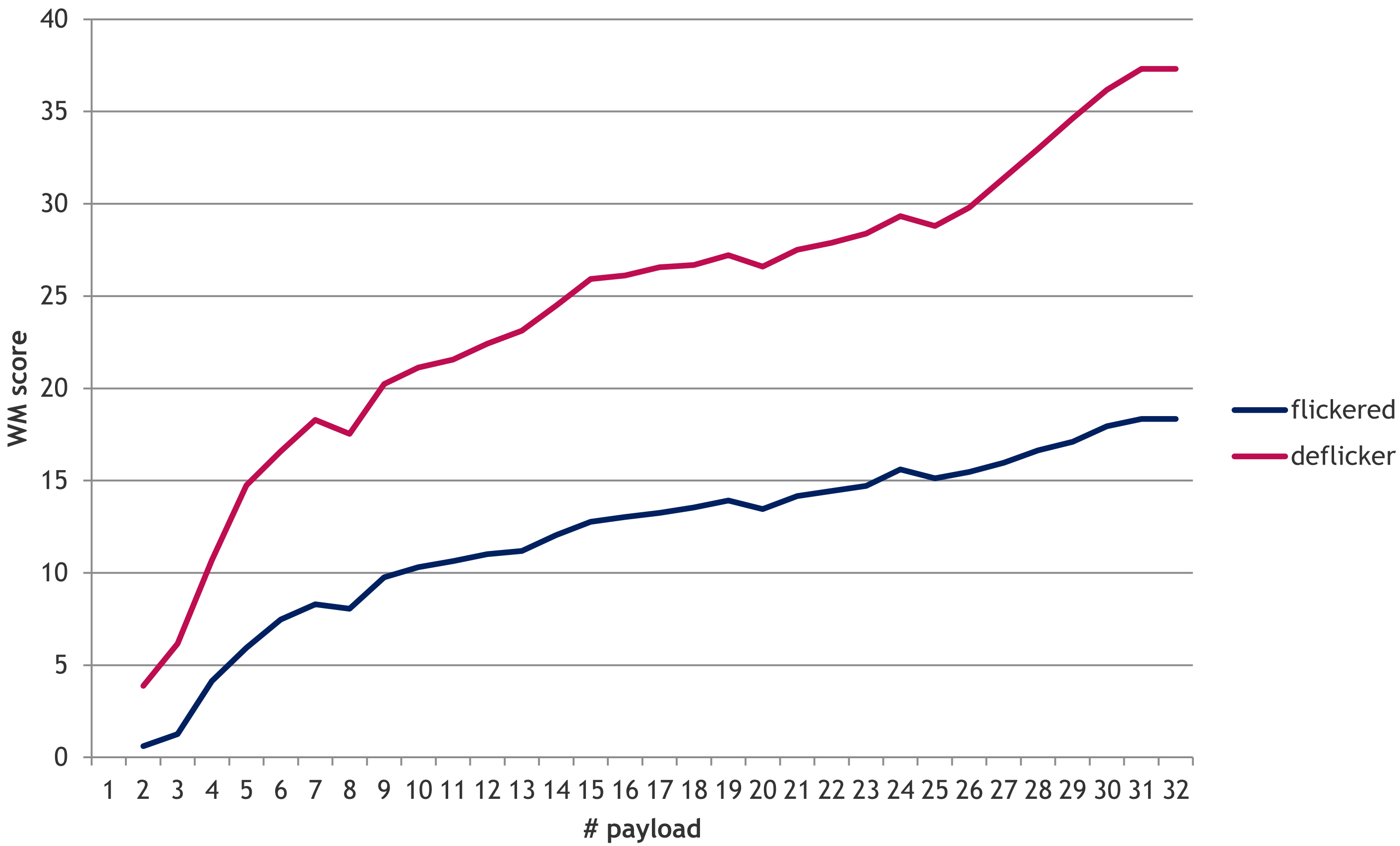
Shape of the flicker characterized by some *sharpness* features

technicolor
Security Laboratories

Experimental Results



Flicker Removal for Watermark Detection



technicolor

Security Laboratories

Research Outlook

Bad news: most low-hanging fruits have already been picked up

- Dealing with correlated samples & content-dependent transforms
- Perceptual models for stereo, HDR, UWG, HOA, …
- Real multi-dimensional watermark modulation
- Explaining the discrepancy between theory and practice
- Registration mechanisms incl. non-blind
- Piracy path analysis

Beware of common pitfalls

- False sense of security by invoking crypto argument
- Inclination to fall in a cats and mouse loop
- Find a solution to a non-existing problem
- Overlooking the impact of security on performances
- Search for perfect security

technicolor
Security Laboratories

Questions

technicolor
Security Laboratories