Friend MTS
Protecting content + revenue

Attacks on Subscriber Watermarking Technologies

White Paper Quick Facts

With traditional content protection measures like conditional access (CA) and digital rights management (DRM) systems, valuable premium content is safeguarded from theft only until the point of its consumption.

As the next level of content protection subscriber watermarking is a powerful solution in the anti-piracy toolkit. It allows for pirated streams to be revoked at the source and enables legitimate content owners and distributors to fully control where their content and revenue flow.

Why is Client-Composited watermarking the most widely used type of technology today?

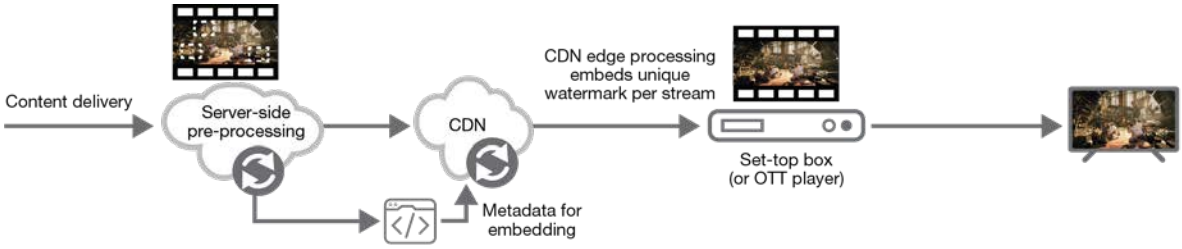
	Bitstream Modification	A/B Variant	Client-Composited
Deployment	Less widely used	Least used	**Most widely used**
Cost Implications	Higher delivery infrastructure and support costs	Higher delivery infrastructure and support costs Storage increase	**No additional delivery infrastructure and support costs** **No storage increase**
Optimised for	On-demand content (VOD)	On-demand content (VOD) Live content*	**On-demand content (VOD)** **Live content**
Primary Applications	Broadcast STB Hybrid Broadcast/IP STB IPTV STB OTT-enabled STB	Hybrid Broadcast/IP STB OTT-enabled STB OTT apps (e.g. iOS/tvOS, Android, Fire TV) OTT web-browser based	**Broadcast STB** **Hybrid Broadcast/IP STB** **IPTV STB** **OTT-enabled STB** **OTT apps (e.g. iOS/tvOS, Android, Fire TV)** **OTT web-browser based**
Multi-CDN ready	No	No**	**Yes**
Robustness and Attack Complexity	Less robust to collusion attacks Low complexity attacks entice pirates	Less robust to collusion attacks Low complexity attacks entice pirates	**More robust to collusion attacks** **High complexity attacks deter pirates, plus watermarking technique more adaptable**
Key Takeaways	Increased costs due to significant and often non-standard changes in the delivery pipeline; Increased costs for multi-CDN solutions; Less robust to collusion and, in the case of workflow option 2, request monitoring attacks.	Increased costs due to significant and often non-standard changes in the delivery pipeline; Increased costs for multi-CDN solutions; Less robust to collusion and request monitoring attacks.	Lightweight, doesn't require any changes in the delivery pipeline; No additional costs for multi-CDN solutions; More robust and adaptable to collusion and request monitoring attacks.

**Less effective for protecting live material (e.g. PPV, events) due to the potential issues with watermark extraction: it can be negatively impacted by low latency streaming protocols plus delay in extraction because of the nature of the watermark's temporal sequence. **In the case of many existing A/B Variant solutions.*

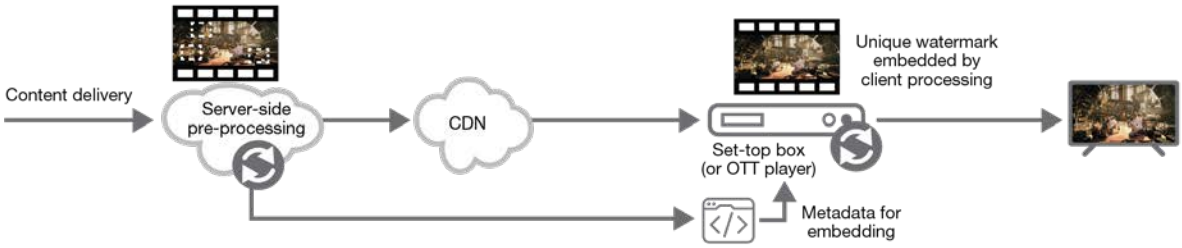
Friend MTS' ASiD is the world's most widely deployed subscriber watermarking counting millions of extractions per month. From client-only and mixed client/server-side Client-Composited solutions to server-only A/B variant watermarking, ASiD provides equally robust protection across broadcast, managed and unmanaged OTT devices and clients. Offering a breadth of watermarking and monitoring solutions for all content protection scenarios, ASiD ensures the security of high-value sports and entertainment content from illegal for-profit redistribution.

SEE OUR WHITE PAPER ATTACKS ON SUBSCRIBER WATERMARKING TECHNOLOGIES FOR FULL DETAILS

Bitstream Modification Watermarking



Bitstream Modification watermarking combining server-side pre-processing and CDN edge watermark embedding (workflow option 1)

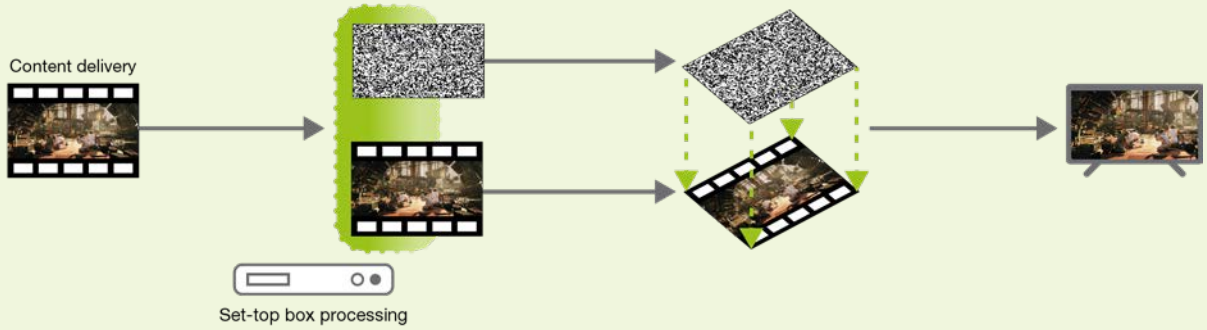


Bitstream Modification watermarking combining server-side pre-processing and client-side watermark embedding (workflow option 2)

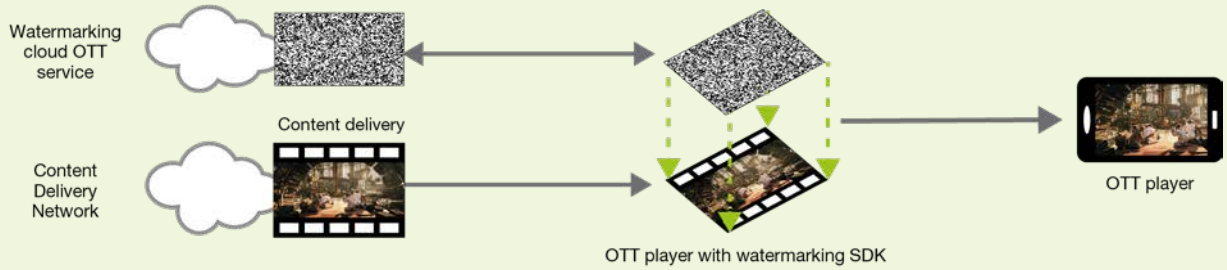
A/B Variant Watermarking

A/B Variant watermarking interleaves video segments from two copies of a stream to create a unique watermark pattern

Client-Composited Watermarking



Client-composited watermarking for set-top boxes with a watermark provided by a set-top box (workflow option 1)



Client-composited watermarking for OTT players with a watermark provided by a cloud service (workflow option 2)

SEE OUR WHITE PAPER ATTACKS ON SUBSCRIBER WATERMARKING TECHNOLOGIES FOR FULL DETAILS

Image source: frames from (CC) Blender Foundation | mango.blender.org

This image is fictional: subscriber watermark should never contain any private information related to the subscriber. This unique identifier is anonymous to any third party and can only be used by video service provider when piracy is confirmed.

© 2021 Friend MTS Ltd. | March 2021 revision v1.2

www.friendmts.com