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, allowing pirated streams to be revoked at the source and enabling legitimate content owners and distributors to fully control where their content flows and who benefits from it financially.

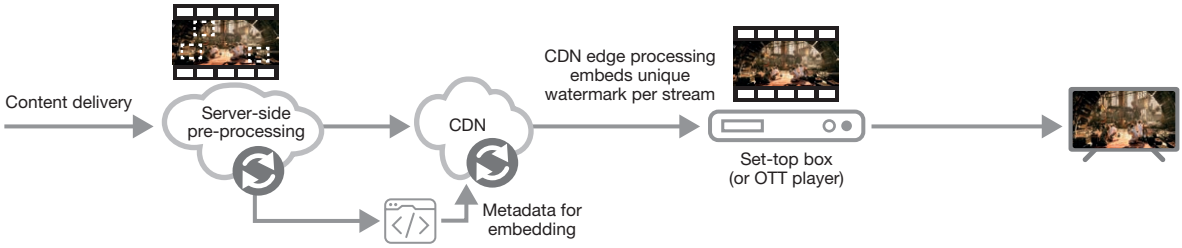
Why is Client-Composited watermarking the most widely used type of technology today?

	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	On-demand content	On-demand content Live content
Primary Applications	Broadcast STB Hybrid Broadcast/IP STB IPTV STB OTT-enabled STB	Hybrid Broadcast/IP STB OTT-enabled STB OTT apps and players	Broadcast STB Hybrid Broadcast/IP STB IPTV STB OTT-enabled STB OTT apps and players
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; Compromised by 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; Compromised by 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 attacks, request monitoring attacks are not applicable.

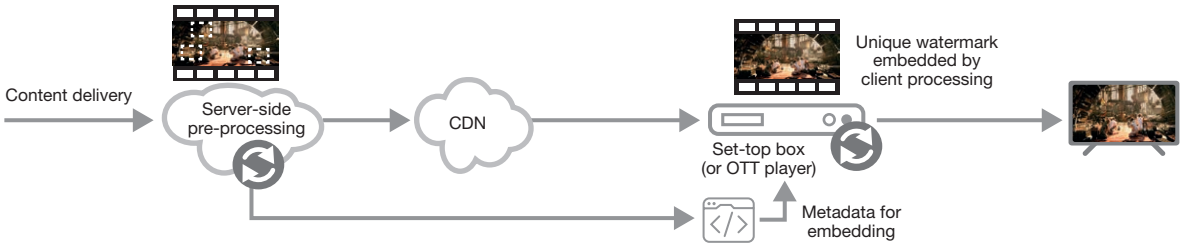
Based on Client-Composited technology, Friend MTS' **ASiD** is the world's most widely deployed subscriber watermarking securing tens of millions of set-top boxes and OTT players and is the only proven solution for premium sports and entertainment offering the fastest watermark extraction even with the largest scale operations. Highly adaptable to ever evolving pirates' attacks, ASiD has lower deployment and support costs with no additional expenses for multi-CDN solutions while offering ultra robust content protection for both broadcast and OTT.

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)

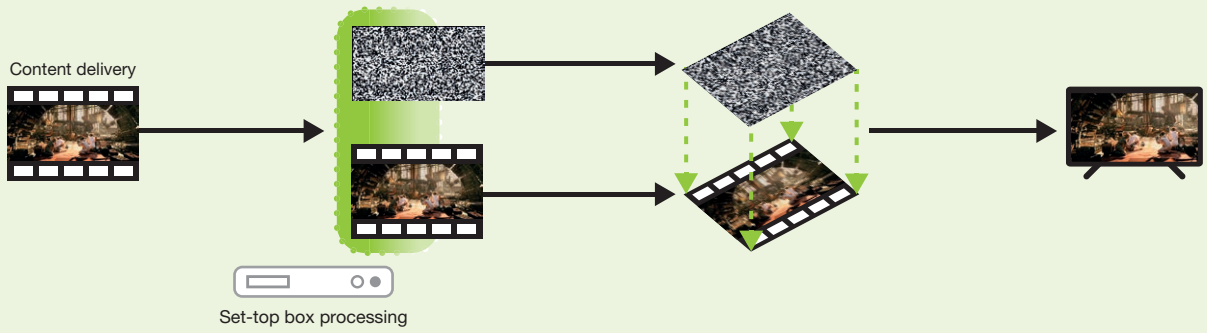


Bitstream Modification watermarking combining server-side pre-processing and client-side watermark embedding (workflow option 2)

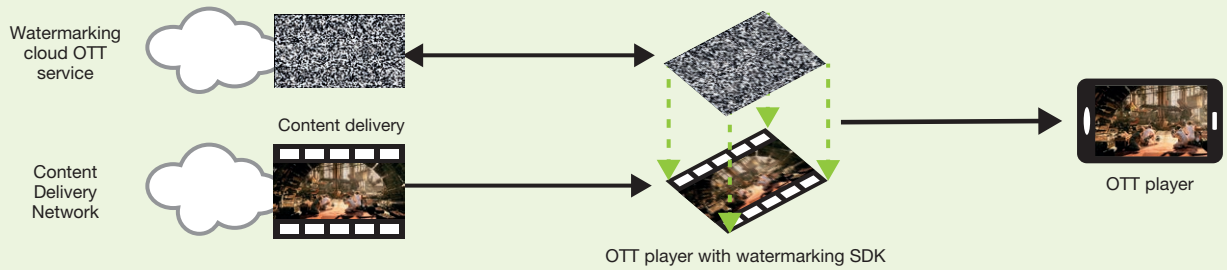
A/B Variant Watermarking

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



Client-Composited watermarking for OTT players with a watermark provided by a cloud service

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

Friend MTS
Protecting content + revenue

www.friendmts.com