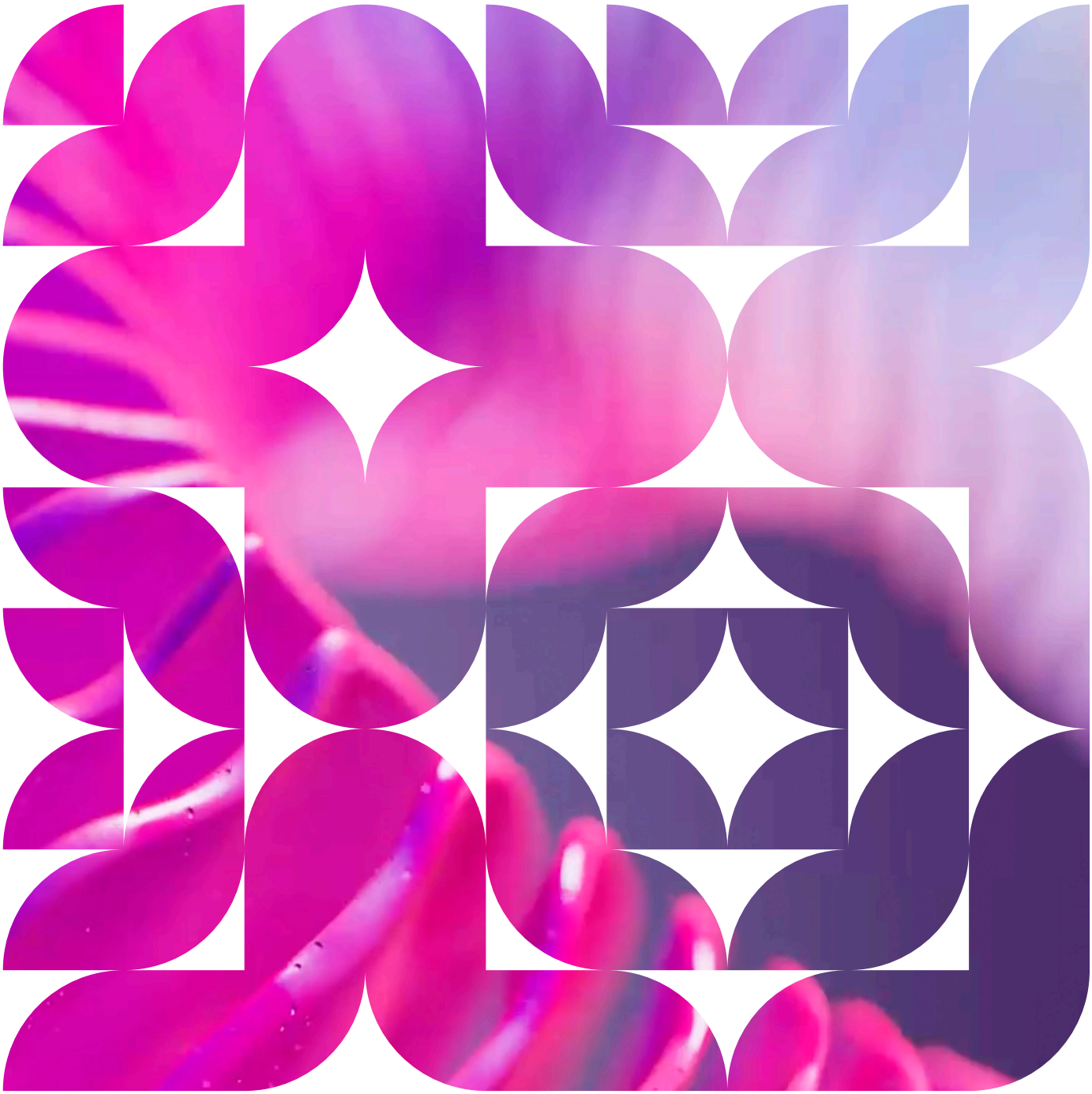


Watermarking

Choosing the Right Watermarking Solution: How to Secure Video Content Without Compromising Performance

White Paper

Contents

Introduction

Piracy is prevalent across the world. Some studies put annual revenue losses to the global TV and movie industry at $50bn. Other examples include 4M homes in the UK accessing shadowy streaming businesses, Nordic countries losing 193,000 jobs, $25B in value-creation and over $6B tax revenue to piracy and piracy penetration in Spain reaching 30% of households, or over 5 million homes and 40% in LATAM, equivalent to nearly 24 million homes. With this scale of illegal content redistribution, valuable premium content needs to be safeguarded both until the point of its consumption and beyond.

Stealing content is relatively simple. With a legitimate subscription and either free screen-scraping software or a $10 device that circumvents HDCP protection, pirates can easily capture video output and then re-encode and redistribute the video using their own infrastructure to profit from stolen streams.

As the next level of content protection aimed at securing premium sports and entertainment content from the point of its consumption, subscriber watermarking is a powerful solution in the anti-piracy toolkit. It enables identification of compromised or fraudulent accounts, which means that access to pirated streams can be revoked at the source, permitting legitimate content owners and distributors to fully control where their content and revenue flow.

There are different types of watermarking solutions, so when making an implementation choice for new or additional watermarking deployments, it is important to understand which solution is right for you. This white paper aims to help broadcasters, content owners and operators understand how different watermarking technologies work – from structure to deployment – so they can choose the best solution to protect live, linear, pay-per-view and on-demand video from illegal pirate redistribution.

Before we delve into examining watermarking technologies, here are short definitions of the types of watermarking reviewed in this white paper.

A/B variant. A technology that involves preparation of two differently watermarked media segments (“A” and “B” segments) at the server-side that are then interleaved in a specific sequence of “A” and “B” segments at the server-side or at the edge to generate a watermark pattern unique for each subscriber.

Bitstream modification. A technology that creates a watermark by modifying a specific area or areas of the video (invisibly to the user). The watermark is applied either at the CDN edge or on the client side. In either case, server-side pre-processing of the content is required.

Client-side. A technology that generates and applies a watermark (an imperceptible graphic overlay, agnostic to the video) at the point that the content is delivered to the end device (a set-top-box / an OTT player) or generates a watermark in the cloud and applies it at the point of delivery of content, to the end user’s application or device (the client). In this case, watermarks can be delivered securely via a cloud-based service usually along with other security technology, such as DRM, code obfuscation or app hardening.

Server-side. In content security terms, server-side watermarking is the generation and embedding of any type of watermark at the server or CDN edge.

Structure of Different Watermarking Technologies

Server-side watermarking

Bitstream Modification watermarking

Bitstream Modification watermarking involves modifying specific areas of the video to uniquely identify the viewer/session without impacting the video experience.

This is a two step technique: the first step is server-side pre-processing to identify areas of the video for modification, and then computing the substitutions that will be made to encode the payload.

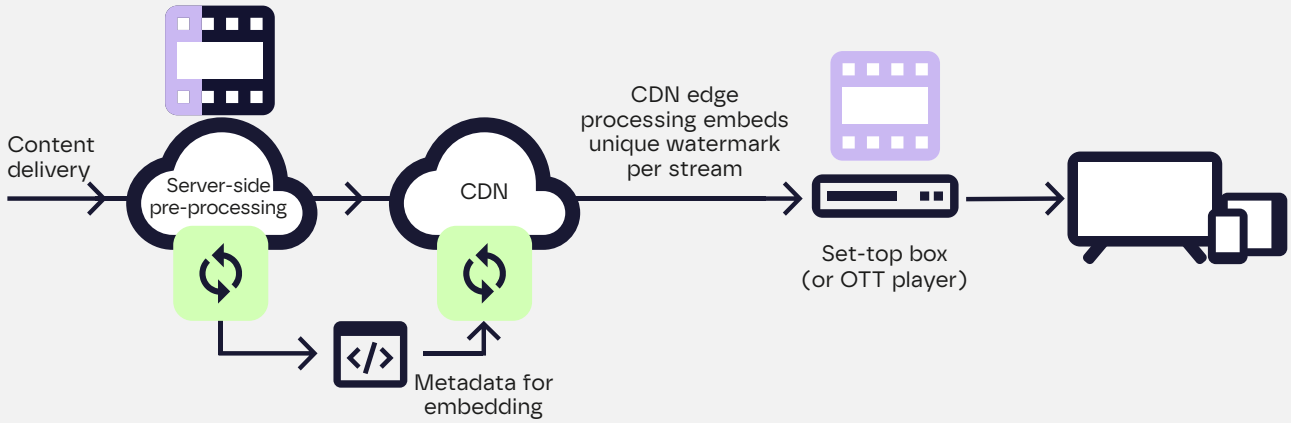
The second step is either CDN edge processing (workflow option 1) or client processing (workflow option 2) for embedding the payload. Hence, this is a hybrid technology that combines server-side and edge-side or server-side and client-side processing.

Technology Type

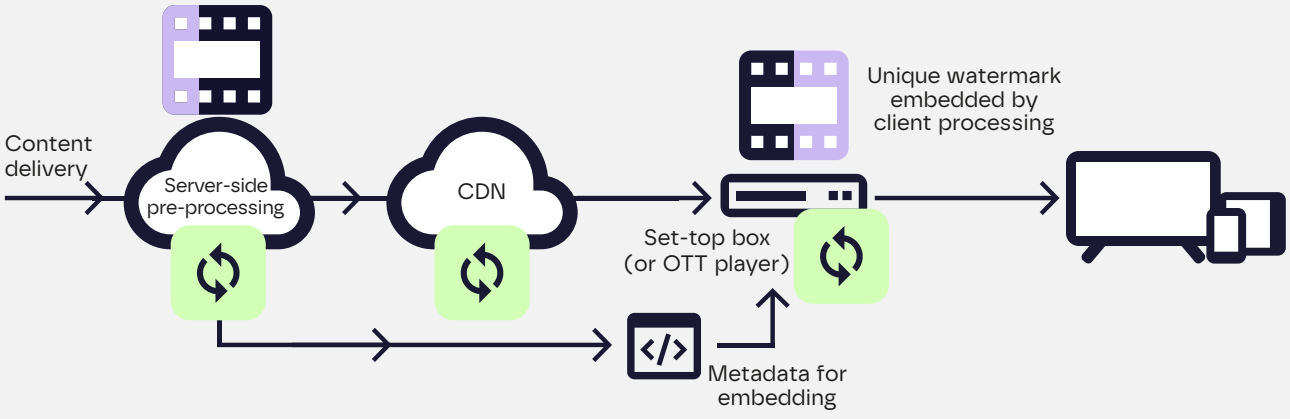
- Server-side + Edge-side (workflow option 1)
- Server-side + Client-side (workflow option 2)

Technology Summary

Watermark is applied either at the CDN edge (workflow option 1) or at the client-side (workflow option 2). In both cases pre-processing of the video at the server-side is required, resulting in data transmitted 'out of band' for the watermark embedding.



Workflow option 1: *Bitstream Modification watermarking combining server-side pre-processing and CDN edge watermark embedding*



Workflow option 2: *Bitstream Modification watermarking combining server-side pre-processing and client-side watermark embedding*

A/B Variant watermarking

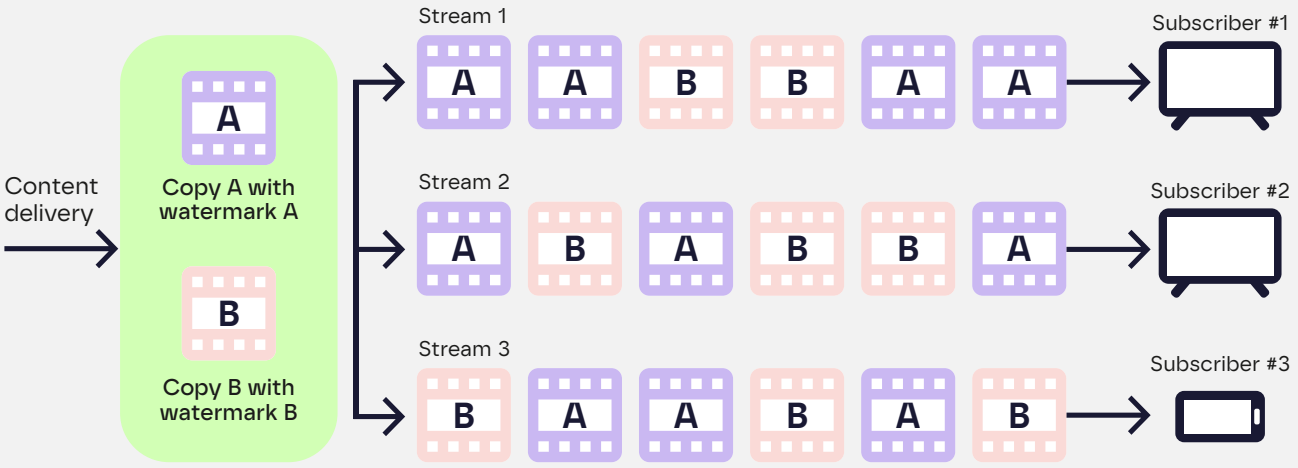
A/B Variant watermarking is a two step server-side technology. The first step is the preparation of two differently watermarked, complete media segments within an adaptive stream ('A' and 'B' segments). These segments must be absolutely identical in every way, other than the watermark, so that the player can swap between them without impacting the video playback. The second step is performed either at the server-side (manifest-switched) or at the CDN (edge-switched), for example, in edge-side scripting. Video segments are interleaved in a client-specific sequence of 'A' and 'B' segments to generate a unique watermark pattern for each subscriber.

Technology Type

- Server-side (manifest-switched) – where Uniform Resource Identifiers (URIs) for segments are predictable*
- Server-side + Edge-side (edge-switched) – where URIs for segments are not predictable

Technology Summary

Watermark is applied at the server side in a single step with two watermarked copies of each stream made available on CDN. Subscriber-specific watermark information is then created from a unique pattern of adaptive video segments either via a personalised manifest of the streaming technology used for delivery (manifest-switched) or via CDN edge segment selection (edge-switched).



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

* Segment URIs can be obfuscated to avoid detection and circumvention of the watermarking technique. However, this is not likely to make manifest-switched implementations as robust as edge-switched ones.

Client-side watermarking

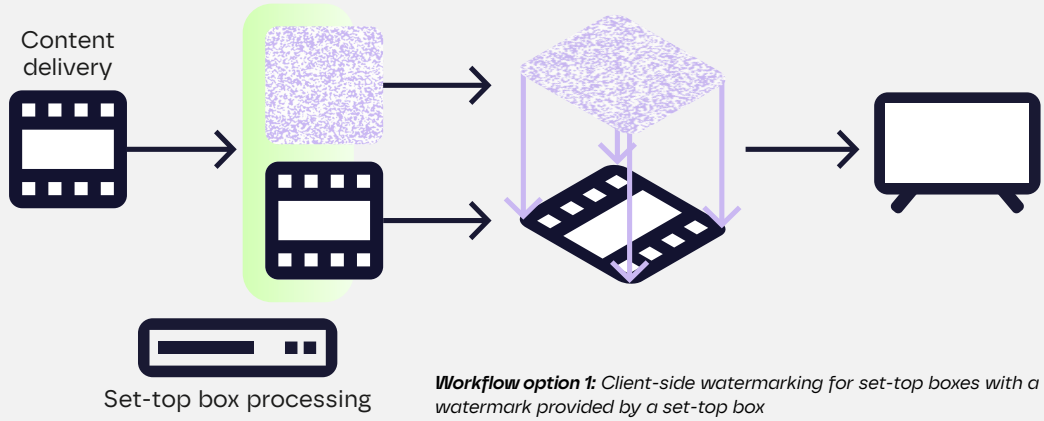
Client-side watermarking uses an imperceptible overlay added to the video within the client device. With managed and secure devices which do not require a network connection (broadcast set-top boxes), the watermark generation and embedding are typically fully contained within the client device (workflow option 1).

Technology Type

- Client-side (workflow option 1)
- Server-side + Client-side (workflow option 2)

Technology Summary

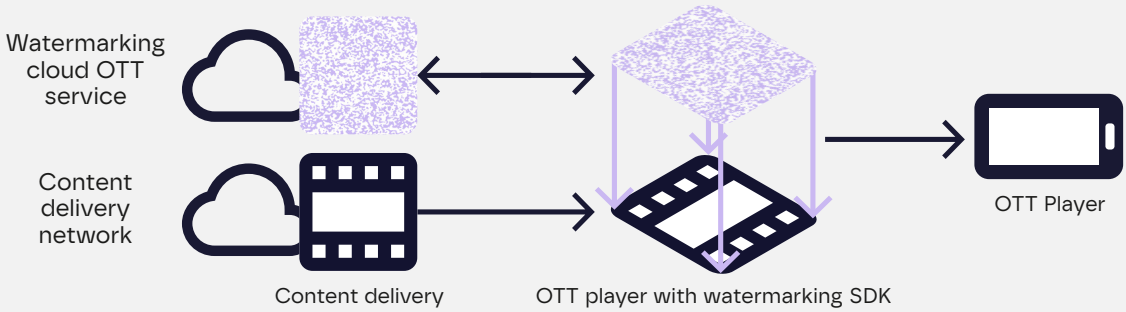
Watermark (an imperceptible overlay, agnostic to the video) is either generated at the client-side (workflow option 1) or at the server-side (workflow option 2) prior to being composited on top of the video at the client-side.



Workflow option 1: *Client-side watermarking for set-top boxes with a watermark provided by a set-top box*

With devices that require a network connection, such as unmanaged OTT devices or IPTV STBs (set-top boxes) it is not possible to fully trust the security of any code running on the client device. Therefore, additional system components are included in order to enhance the overall security of the solution and protect the integrity of the watermark payload. The generation of the watermark is provided by a hosted watermarking service for the device to embed (workflow option 2).

In either scenario, these components operate entirely independently of the existing content preparation and delivery pipeline, with the primary integration point being only in the client device/player app.



Workflow option 2: *Client-side watermarking for OTT players with a watermark provided by a secure cloud service*

Application of Different Watermarking Technologies

Regardless of their type, watermarking technologies can be used to identify both the distribution path and an end subscriber behind illicitly redistributed content. With the client-side technology, a multi-layering approach is possible where video can carry both distributor and subscriber-level payload.

In terms of devices and delivery methods, both Server-side and Client-side watermarking support broadcast and streaming. Bitstream Modification is primarily designed for STBs supporting all types of video delivery. In contrast the A/B Variant solution is designed for streaming environments. Bitstream Modification can only support unicast delivery, while A/B Variant as well as client-side support both multicast and unicast streamed delivery.

Primary applications at a glance

Primary Applications	Server-side		Client-side
	Bitstream Modification	A/B Variant	
Broadcast STB	✓		✓
Hybrid Broadcast/IP STB	✓	✓	✓
IPTV STB	✓		✓
OTT-enabled STB	✓	✓	✓
OTT apps (e.g. iOS/tvOS, Android, Fire TV)*		✓	✓
OTT web-browser based*		✓	✓

Broadcast STB is a set-top box that enables viewers to access the broadcast TV delivery method.

Hybrid Broadcast/IP STB is a set-top box that enables viewers to access both broadcast and over-the-top / over the web TV delivery methods.

IPTV STB is a set-top box that enables viewers to access the IP (e.g. multicast) TV delivery method.

OTT-enabled STB is a set-top box that enables viewers to access over-the-top / over the web TV delivery method.

OTT apps are apps that enable viewers to access over-the-top/over the web TV delivery method.

OTT web-browser based are web-browser based solutions that enable viewers to access over-the-top/over the web TV delivery method.

* While it is technically feasible to implement Bitstream Modification watermarking (workflow option 1) for OTT apps and web-browser based solutions, this watermarking solution is not designed for this environment which is reflected in the primary applications of this technology.

Deployment of Different Watermarking Technologies

Server-side watermarking

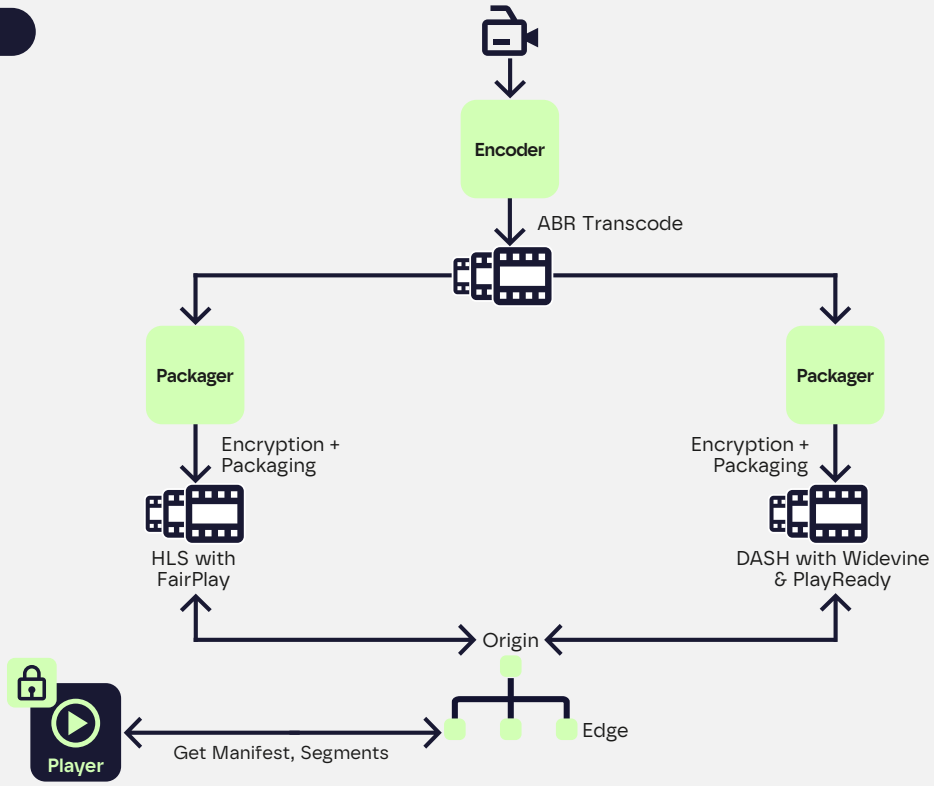
Bitstream Modification watermarking

For workflows of Bitstream Monification where the watermark is embedded by the client device, interaction occurs with the video decode pipeline, which increases processing demands compared to lighter Client-side watermarking that doesn't require this interaction. This client processing overhead is eliminated with CDN edge processing workflow option. However, this approach is not widely supported by CDN providers. With this workflow option, streaming solutions using a multi-CDN architecture become more complex and non-standard due to the lack of parity across CDN and edge-compute offerings. In general, Bitstream Modification watermarking is challenging to use for live content because it requires heavy pre-processing which adds latency. This added delay is not suitable for today's low-latency delivery platforms, so the method is typically limited to on-demand content.

A/B Variant watermarking

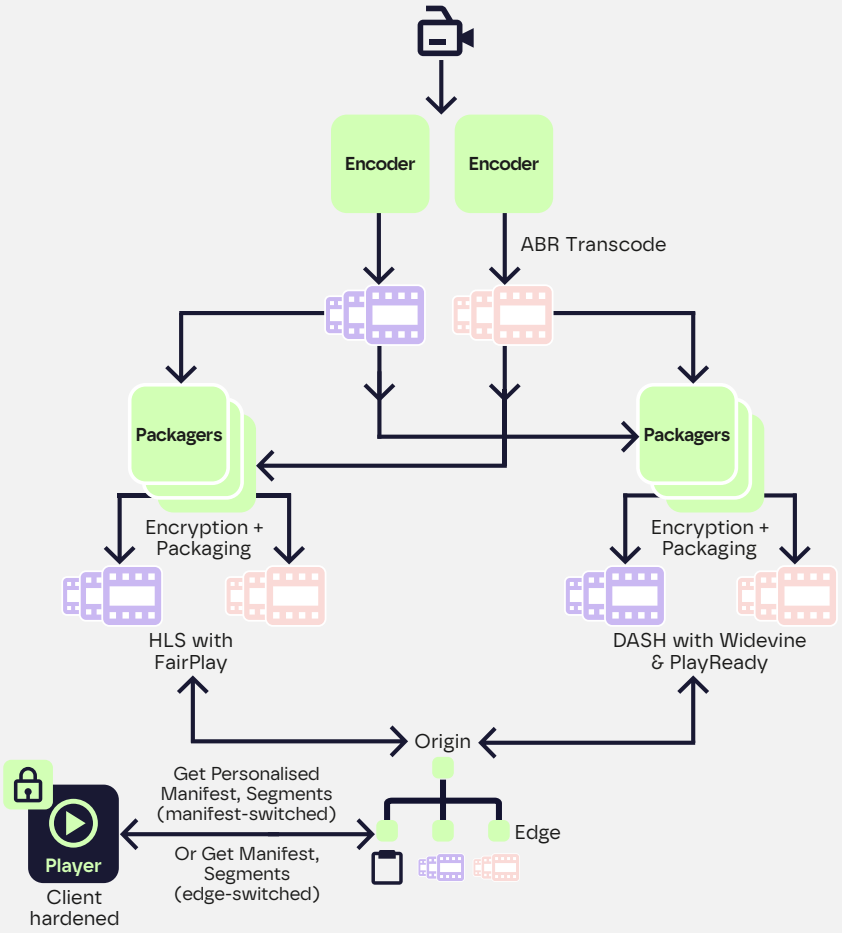
A/B Variant watermarking also requires changes in the delivery pipeline. This technology can allow ultra-fast extraction if the media segments are small, typically 2 seconds in duration, which reduces the duration of the video that needs to be captured for extraction to below 4 minutes. However, where media segments are longer, the watermark extraction time increases. Faster extraction is not always necessary for on-demand content but it's often required for live content, especially if it's shorter duration content, such as a boxing match. The reason for this delay with extraction lies in its temporal sequential structure (see the Structure of Different Watermarking Technologies section).

Before



A traditional streaming set-up for the delivery of live and on-demand content

After



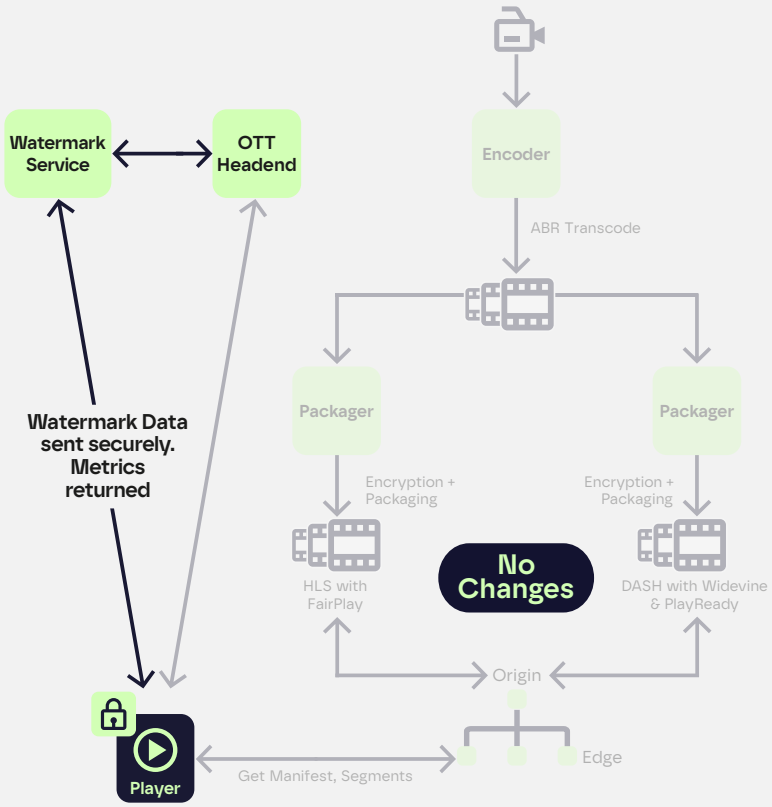
A traditional streaming set-up for the delivery of live and on-demand content after A/B variant watermarking deployment

Just like Bitstream Modification watermarking, the A/B Variant technique also faces challenges in multi-CDNs environment where the lack of parity across CDN and edge-compute offerings makes streaming solutions more complex. Since many current A/B variant solutions don't work effectively in multi-CDN environments, using this approach can increase the technical complexity – unless a CDN-agnostic solution is used. In addition, the use of Dynamic Ad Insertion (DAI), which is typically orchestrated at the server side, can further complicate the architecture. Since the ads are not A/B watermarked, any gap in the A/B sequence would increase the duration of the video needed to be captured for the watermark extraction. This may add a layer of complexity in the overall process.

Client-side watermarking

As a video agnostic technology, Client-side watermarking does not require any headend pre-processing of the video, and it also requires minimal client processing.

After



A traditional streaming set-up for the delivery of live and on-demand content after Client-side watermarking deployment

In streaming solutions with a multi-CDN architecture, Client-side watermarking requires no changes to the delivery workflows. Additionally, Dynamic Ad Insertion has no impact on watermarking method as it operates downstream of the DAI process. Unlike server-side watermarking, Client-side watermarking has no non-standard deployment requirements. It is lightweight and doesn't require changes to the delivery pipeline. However, implementing client-side watermarking does require some changes at the client level, such as integrating an SDK to manage watermark sessions and obfuscating and hardening of sensitive areas of the client code, to prevent attacks from circumventing the use of watermarking. These requirements need to be taken into account if the delivery network includes a large variety of device types as extra costs are incurred in this case.

With all three types of watermarking, there is a clear need to fully secure video delivery in-flight to the client device with a digital rights management (DRM) system. If the content is not adequately protected, any watermarking technology will not deliver effective security due to the potential to intercept and manipulate the unprotected signal.

In addition, all types of watermarking typically rely on client-side code even though server-side technology was originally devised as independent of the client device (though for A/B variant watermarking this is applicable only to secure the manifest-switched implementations).

Bitstream Modification watermarking can be highly reliant on the client device to inject the modifications/substitutions from the pre-processed information, unless proprietary CDN edge processing is deployed.

With A/B Variant watermarking, manifest-switched approach requires client-side modifications to secure the payload. This is because standard players do not secure the stream manifest (which defines the sequence of A/B segments) and none of the DRM schemes offer native security for the sequencing of variant segments.

All three watermarking solutions require client environments to be obfuscated and hardened to resist tampering. However, hardening OTT clients is also necessary to support other key functionalities, such as scalable concurrency management and any features relying on client-side anchoring. Enterprise obfuscation and hardening technologies are readily available and should be implemented as a core component of a secure content distribution platform, as recommended by the Open Web Application Security Project/OWASP guidelines. So, all delivery environments should be protected by obfuscation, app hardening etc., regardless of whether watermarking is used or not.

Deployment at a glance

	Server-side		Client-side
	Bitstream Modification	A/B Variant	
Optimised for	On-demand content (VOD)	On-demand content (VOD) Live content	On-demand content (VOD) Live content
Multi-CDN ready	No	No (for many existing A/B Variant solutions.)	Yes
Technical implementation notes	Changes in delivery pipeline - changes to the infrastructure to accommodate the required pre-processing and compute - significant changes to delivery workflow - changes for multi-CDN solutions Negatively impacts live broadcast latency	Changes in delivery pipeline - changes to the infrastructure to accommodate the required dual encoding and packaging - changes to delivery workflow to accommodate delivery of manifests (edge compute) - changes for multi-CDN solutions	No delivery pipeline changes - no changes to the infrastructure as no pre-processing, encoding or packaging required - no changes to delivery workflow - out of the box support for multi-CDN solutions
	Requires effective CA or DRM to secure content to client	Requires effective CA or DRM to secure content to client	Requires effective CA or DRM to secure content to client
	Requires software modifications at the client side (client processing workflow 2)	Requires software modifications at the client side (manifest-switched)	Requires software modifications at the client side
	Requires client hardening (client processing workflow 2)	Requires client hardening	Requires client hardening

Performance of Different Watermarking Technologies

Server-side watermarking

Bitstream Modification watermarking

With Bitstream Modification watermarking the speed of extraction is slow as with this watermarking solution the payload is spread across multiple GOPs (groups of pictures) of video. Hence, video of longer duration needs to be captured and subsequently analysed.

While not as important for VOD content, speed of watermark extraction is crucial for live events where the value of premium sports and entertainment content rapidly diminishes and fast takedown action is of paramount importance.

A/B Variant watermarking

Depending on the segment size and ad-insertion requirements, A/B Variant watermarking will require a longer duration of the payload sequence due to its dual stream temporal approach. This means that video of longer duration needs to be captured and subsequently analysed, making the speed of watermark extraction slower compared to client-side. The length of the payload sequence, and hence the duration of video captured for extraction, increase as the user population increases: which needs to be taken into account with certain A/B variant deployments.

Client-side watermarking

Client-side watermarking allows ultra-fast watermark extraction, performed via the capture and analysis of a shorter duration of video. The fast speed of extraction along with the simpler architecture makes this type of watermarking highly suitable for taking down pirated live sports in real time as well as for protecting short duration content.

In addition, to enhance watermarking performance and tackle certain attack vectors such as CDN leeching and machine-in-the-middle attacks, different watermarking technologies can be used in concert. Adding server-side watermarking to the client-side deployment allows the leeched CDN session to be identified and potentially terminated; while existing A/B watermarking deployment can be hardened by client-side technology where the client SDK provides identification of the creation of client-side sessions, which can be tracked to ensure that attacks such as machine-in-the-middle are detected, and concurrency is managed, giving enhanced telemetrics for client devices receiving watermarked streams.

Performance at a glance

Server-side		Client-side
Bitstream Modification	A/B Variant	
Watermark extraction in minutes - capture and analysis requires longer duration of video for extraction	Watermark extraction in minutes - capture and analysis requires longer duration of video for extraction	Watermark extraction in seconds - capture and analysis requires shorter duration of video for extraction

Conclusion

Watermarking is crucial in the overall content protection stack for preserving the value of live, on-demand and linear content along distribution paths and beyond. It needs to be implemented alongside other content protection technologies, such as DRM, content monitoring to detect piracy, fingerprint identification solutions, code obfuscation, etc. Working at both distributor and subscriber levels, watermarking technologies ensure a robust distribution strategy, safe from any illicit restreaming from legitimate subscription accounts.

Choosing the right watermarking technology to complete your content protection stack requires an informed review of various solutions available in the market. This white paper reviewed the most used technologies in terms of their structure, application, deployment and performance and provided some practical guidance for the broadcasters, content owners and streamers that need to make an informed decision when choosing a suitable technology to implement.

In general, both sever- and client-side solutions can protect broadcast and OTT delivery, both live and on-demand content though Bitstream Modiifcation (a server-side solution) is not suitable for protecting live content as it adds latency and therefore affects viewer experience.

Server-side watermarking is arguably more resource-intensive in deployment as it requires changes in the delivery workflow; Bitsream Modification watermarking requires more significant changes than A/B Variant technology. While all watermarking solutions require distribution security and client hardening, client-side requires software modifications at the client side which needs to be taken into account if these changes present a challenge across the existing population of devices in the field.

On the other hand, if speed of watermark extraction and swift takedown is a requirement, client-side technology will bring the best result with A/B variant yielding the next fastest extraction.

We stop piracy.

Nobody does it better

Transforming content security from cost centre to revenue source.

Friend MTS is the world leader in content security and anti-piracy. Our solutions are deployed in tens of millions of devices and apps, and we protect content whose collected media rights value is well in excess of $60 billion. We provide the world's biggest brands with the best anti-piracy services and solutions available, including monitoring & enforcement, watermarking, business intelligence and server blocking.

Our partners trust us to help them detect, deter and disable piracy, using game-changing tools that enable engagement with potential customers, converting pirate audiences into legitimate subscribers, thereby increasing revenue.

Our solutions are unrivalled. But don't take our word for it. FMTS works with the largest brands in media and entertainment to safeguard their content. Delve into our latest case studies to learn more at friendmts.com/case-studies.

Contact us today to discover more.