Friend MTS

10

Questions to Ask Your Prospective Video Watermarking Vendor

Choosing a content security solution
to best protect your revenue

So you need to implement a video watermarking solution. How do you decide which solution, and which vendor, are the right ones for you?

When choosing a content protection company that offers video watermarking, as a broadcaster or service operator you need to determine which solution is most suitable for your content protection needs. Of course, there are a large number of factors that affect this decision, but here are some questions that you should ask all of your prospective vendors to determine whether their watermarking solution:

- Is viewer-friendly and pirate-unfriendly;
- Offers a universal and cost-efficient solution;
- And actually works!

Viewer-friendly and pirate-unfriendly watermarking

Question 1:

Is the watermark completely imperceptible to the viewer?

First of all, video watermarking absolutely must be imperceptible to the viewer. Security is highly important but it cannot (and need not) compromise the viewer experience. A good watermarking solution is entirely imperceptible, which also has the benefit of making it harder for a pirate to discover and circumvent.

With live sports being the most lucrative target, deploying a watermarking technology that adapts in response to attacks in real-time is crucial for protecting this content.

Question 2:

Is the watermark robust against real-world pirate attacks?

Real-world pirate attacks are increasingly technically sophisticated, with professional pirates motivated by high-margin income from selling stolen content. Pirates are constantly investing in new techniques to circumvent security, with live sports being the most lucrative target, deploying a watermarking technology that adapts in response to attacks in real-time is crucial for protecting this content. This, therefore, requires the watermarking solution to be offered as a managed and supported service rather than an off-the-shelf product or set of tools.

A data-driven approach is essential for the watermarking vendor. A capability to gather and analyse large data sets and develop intelligence from monitoring content globally at scale will allow the vendor to make accurate predictions of pirate countermeasures and develop solutions that will remain ahead of anything the pirates are attempting.

Universal and cost-efficient watermarking

Question 3:

Is the watermark always on during playback of all content types?

If the watermark is displayed throughout the duration of the protected content playback, be it a live linear channel or VoD asset, then any capture of pirated content from that source should include the watermark and therefore deliver a result.

Conversely, if the watermark is only displayed intermittently during the playback, this will result in increased complexity of the capture process with the content monitoring system needing to align video capture with the display time of the watermarking. Accordingly, the number of instances of failed captures will inevitably be higher, and also the extraction/ identification process will likely require frequent manual intervention, resulting in higher costs.

Question 4:

Can the watermark be extracted from a short pirate video capture?

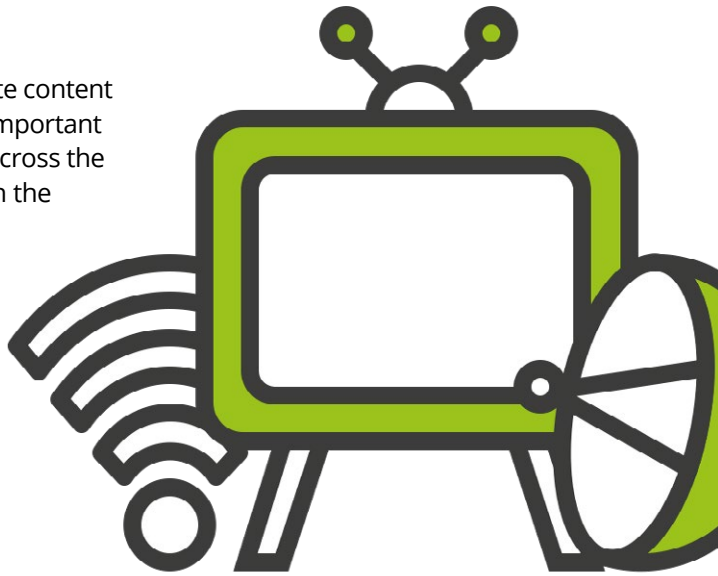
This question is especially important to ask when you are considering protecting live content. Some watermarking solutions, notably those that use A/B variant sequencing to create a unique temporal pattern to identify the infringing subscriber, can require video captures of longer duration (30 minutes or even longer) for successful extraction. This renders them ineffective for the protection of live content – remedial action, such as service suspension, usually has to happen in real-time – it's of little benefit after the event is over!

In addition, the need for extended video captures can lead to reduced reliability of the capture process, and larger video files will always mean higher storage costs. And finally, solutions that support watermark extraction from just a few minutes (or even seconds) of captured pirate video will be equally proficient at protecting both live and on-demand video.

Universal and cost-efficient watermarking

Question 5:

Is the watermark deployable on all device categories, including legacy STBs and OTT apps?



For those broadcasters and service operators that distribute content through different channels (both broadcast and OTT) it is important to make sure that valuable exclusive content is protected across the entire client device estate. Protecting an exclusive movie on the OTT players will be of limited benefit if a pirate can still easily capture or restream from an older broadcast device without fear of detection. Pirates will always identify the easiest way to steal content and exploit those distribution channels and devices. A universal watermarking solution deployable on all key device categories will cover all the bases.

Question 6:

Can the watermarking solution protect broadcaster content across multiple operators?

Broadcasters need to be able to work closely with their various distribution partners to avoid premium content being leaked to pirate networks. A single leaking source impacts the entire distribution ecosystem and makes exclusive content... well, non-exclusive. A universal watermarking solution should allow the same technology to be deployed across a number of distribution partners/operator platforms with a joined-up approach to content monitoring, watermark extraction, and subsequent notification of successful extraction.

Question 7:

Can the watermarking solution work with any monitoring provider?

Often service providers have existing relationships with anti-piracy companies whose services they use to monitor and detect instances of piracy. On deployment of a watermarking solution, they may wish to maintain this relationship, therefore the watermarking vendor must offer an easy integration for the monitoring partner to submit pirate content captures (or links) for watermark extraction.

Pirates will always identify the easiest way to steal content and exploit distribution channels and devices. A universal watermarking solution deployable on all key device categories will cover all the bases.

Watermarking that actually works

Question 8:
Has the watermarking solution actually been deployed?

Of course, this is the ultimate question that needs to be asked. If the watermarking solution has only ever existed in a lab environment (or even worse, in a slide deck) or has never been deployed to a significant subscriber population, then it will most likely not offer the same level of real-world performance and robustness as offered by a genuinely battle-hardened solution. Check that a watermarking vendor has a significantly deployed solution in environments that match your own, and can verify this with reference implementations.

Question 9:
Is the watermarking solution deployed at scale?

Many watermarking solutions simply do not scale, therefore it is important that the watermarking vendor can offer evidence of large-scale deployments.

Note that the requirements for subscriber-level watermarking are very different to those for distributor-level (network-level) or pre-production watermarking where only a limited number of streams or playback sessions are watermarked.

When a watermarking vendor talks of their existing deployments, ask the simple question: "How many concurrent client devices/apps?"

The requirements for subscriber-level watermarking are very different to those for distributor-level (network-level) or pre-production watermarking where only a limited number of streams or playback sessions are watermarked.

Question 10:
Has the watermarking solution achieved real results?

The ultimate goal when deploying a watermarking technology is to be able to identify individual subscription accounts used by pirates to feed their extensive illegal distribution networks and consequently shut down these accounts (subscriber-level identification), or in the case of distribution watermarking, to identify a distribution partner with security issues and work together to tighten up protection.

Embedding watermarks with no subsequent monitoring and extraction function will offer little value beyond compliance with the requirements published by some content owners, and in truth, it doesn't add any significant long-term value.

Bonus question 11:

Are you making an 'apples to apples' comparison?

Watermarking is just one component of a comprehensive content security system, and some vendors offer multiple components alongside watermarking. Make sure that when considering pricing you are comparing like for like, and that vendors are being transparent regarding how much they are discounting particular components.

In addition, make sure that pricing is aligned correctly across vendors: a primary expense with watermarking should be around the extraction process, and to be an effective implementation the appropriate number of extractions per month should be quoted. This will vary depending on the type of content – content such as pre-air movies will require relatively few watermark extraction attempts, whereas a broadcaster of major sports leagues may potentially require millions each month. Make sure your vendor is quoting for the appropriate level of extraction attempts for your content.

Summary

The content protection goals of marking valuable content can only be achieved by actually detecting the stolen content, extracting watermarks, and consequently taking action against infringing subscribers.

When exploring the watermarking solutions available in the market, broadcasters and service providers need to make sure they are looking at joined-up end-to-end solutions, deployed at scale in the real world, that can deliver actual business benefits.