INA Signature

for video-sharing platforms

The content distribution monitoring solution
to optimize the value of copyrighted videos

The main reasons to implement our content management solution

Why should you set-up means to manage the distribution of contents on your platform?

➔ **Increase drastically** your capacity to **monetize audience** on contents published on your platform and protected by copyright.

➔ **Grow the audience and the value of your platform** by empowering partnerships with publishers while providing them with reliable means to control the distribution of their copyrighted contents:

- ✓ Encouraging publishers to distribute on your platform **valuable and audience-driving contents**
- ✓ Developing **long term relationship** with publishers
- ✓ **Differentiating** from others platforms to **attract valuable publishers**, cautious with their contents and the value they get

➔ **Secure legally your activity** by preventing legal issues and conflicts with rights holders, their associations or administrations

➔ **Simplify your moderation tasks** on your platform by automating rejection of contents which have already been moderated

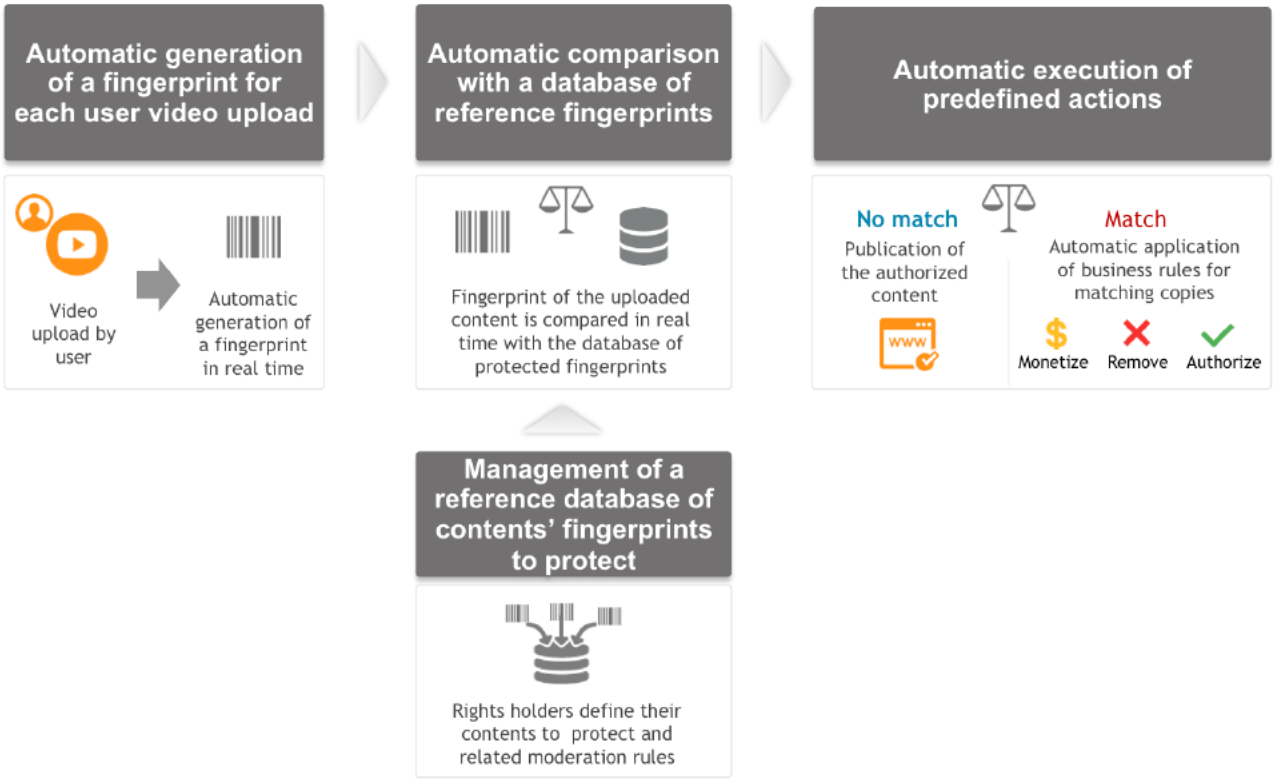
What scenarios to set-up reliable means to control the distribution of contents on your platform?

	For whom?	Protection scope
Integrate a **market solution** ina Signature	Platforms willing a market standard solution with - Proven technology - Limited development and maintenance cost - Quick time to market	Protection of partner content registered on your platform + Protection of contents from all publishers using the solution and registering their content centrally
Develop your **own solution**	Platforms willing to master entirely their own ecosystem, with major R&D budgets focused on protection, and low issue (=years) on time to market **Time consuming** in R&D **High expenses** in R&D	Protection only of partner content registered on your platform

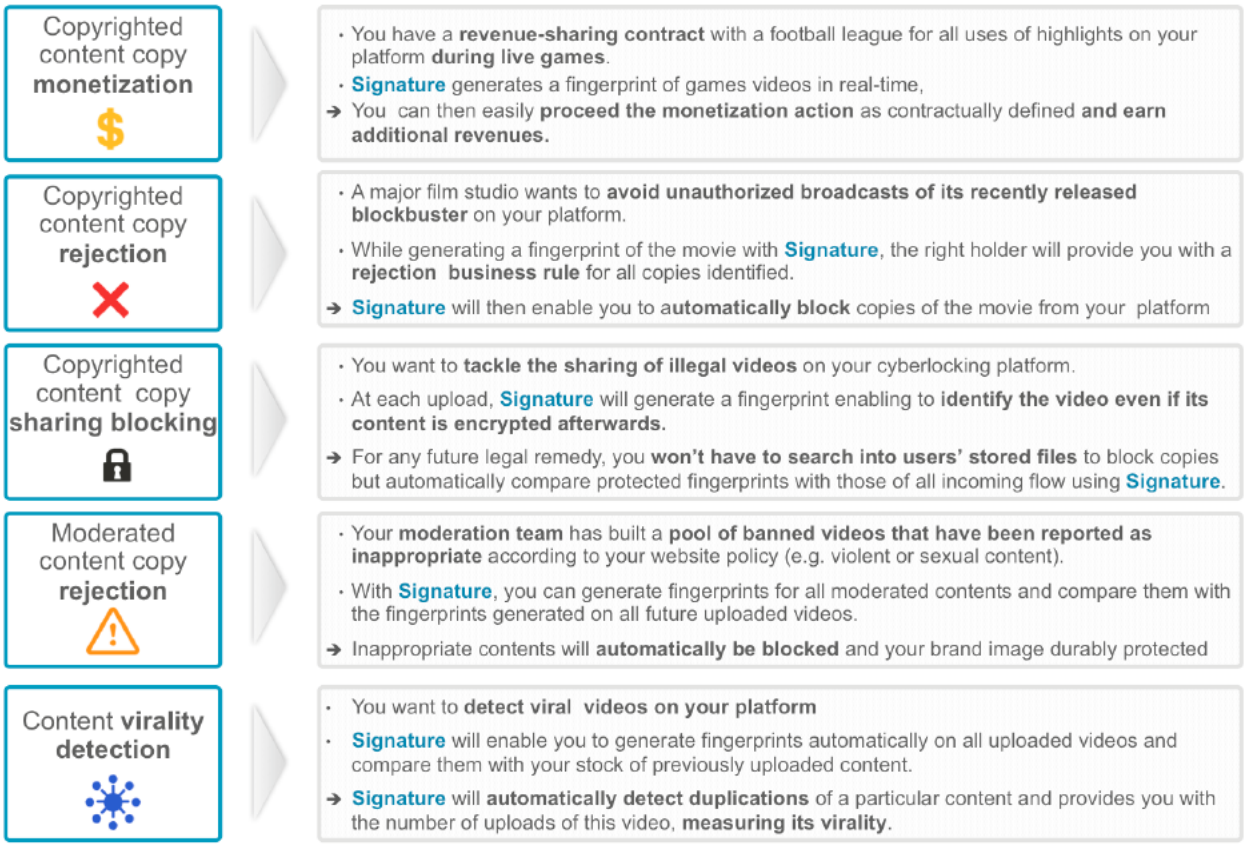
The benefits of using the INA Signature solution

What features does INA Signature include ?

- ➔ INA Signature offers features at each step of the monitoring process to ensure a complete protection of contents.
- ➔ **Video sharing websites can set-up features** to detect potential copies uploaded on their platform, a priori (during upload) or a posteriori (once videos are uploaded), compare copies to protected contents and take measures towards identified copies according to business rules defined by rights holders.



Examples of value-added monitoring use cases on video-sharing platforms:



How does INA Signature fingerprinting process compare to other identification technologies?

What is a fingerprint?

➔ Video fingerprints are small digital genetic codes, computed from the digitized images of a video sequence, and designed to represent its content.

➔ A set of fingerprints computed from a video sequence is a very condensed piece of information representing the essence of the sequence.

➔ In practice, computing fingerprints from digitized video files is a very simple process: a software program allows to quickly compute one fingerprint file per video file. Technically, the fingerprints are computed from the luminance of various areas of the images and from the motion information in the sequence. The video file is neither modified nor copied in any database.

Signature differentiates from watermarking

Watermarking is an invisible tattooing operation, that only allows to identify tattooed copies. On the contrary, a fingerprinting process analyzes very closely a content copy and then deduces a genetic code without modifying the content. The fingerprint is then valid to identify any past and future copy of the video.

What are the key benefits of using INA Signature on your platform?

Simple to implement and run

- **Automatic** fingerprint generation for all user generated video contents
- **Easy to plug**: comparison is available in SaaS
- Benefits form 5 years of R&D and avoids development **and maintenance** expenditures linked to the development of a owned solution
- Automation of business rules application avoiding a costly and tedious manual **moderation**

Super efficient

- **Robustness** of the software: detection even with modifications on content enabling a reliable moderation
- Virtually **no technical false detection**: alert only in case of an actual copy → enable to automate detection on high volumes
- **Speed of execution** of the comparison enabling to take a decision at the uploading process
- The solution has been successfully tested and implemented for years with Dailymotion on a large scale of contents
- Possibility to share **monetization revenues** with rights holders

ina Signature

Scalable

- **Scalable**: capacity to manage high volumes
- Platforms can use INA Signature in **other usages** than copyright protection → constitution of a specific database for all contents to moderate
- Get additional info on success of content ex : detect buzz (virality index)

Standard

- Fingerprints stored in the INA reference database are related **to valuable and audience-driving contents** with a high business potential from major rights holders, already including key US movie studios and international sports leagues

[redacted]

Frequently Asked Questions

To which extent can Signature detect transformed video copies?

➔ **INA Signature detects copies even with significant modifications between the protected content and the distributed copy**

- INA-Signature has regularly been benchmarked in **tier 1** of rights holders and expert tests
- The samples below illustrate a **variety of transformations types** that Signature has successfully detected on actual use cases; Signature robustness includes support of those transformations in real-world cases: text and graphic overlays, color / B&W changes, crops, camcords, video compression, video format changes, audio track changes.
- INA-Signature is **available for further tests** as needed to check it satisfies your needs

On the left the original content and on the right the broadcast content that was properly identified by Signature. This illustrates the reliability of the technology.

How reliable is the Signature comparison process?

- Signature avoids **false negatives** (non-detection of a copy whereas it is one) and **false positives** (false detection of a copy whereas it is not one) with ***zero technical false detection identified over several years*** of operation for a large UGC use case.

How fast is the Signature fingerprint generation process?

- Fingerprints are generated **up to 20 times faster than real-time**, depending on the source video format
- *e.g for a 3 minute standard video, fingerprint can be generated in less than 10 seconds*

How fast is the Signature fingerprints comparison process?

- The technical setup is scaled depending on the detection time requirements per use case
- For example, video sharing platforms integrate the comparison feature during the video upload and initial processing (time **below 2 min**), so that the user experience remains smooth
- *Actual daily operations compares* **in live** *sport matches streams or uploads during the events*

How much content can Signature compare?

- INA Signature offer to its clients the ability to **process high volumes of requests simultaneously**
- *e.g. with Signature, INA monitors automatically about 100 TV channels in real-time to identify copies of its distributed archives*

Get started with INA Signature

INA enables you to set up a free Proof Of Concept to quickly and easily discover Signature's key features

Free discovery test (1 day)

- **Upload** of the videos to be compared onto INA server (reference videos & potential copies)
- **Fingerprint generation and matching process** performed by INA
- **Manual restitution** of the results

Advanced test (1 month)

- **Fingerprint generation test** made on your own
- **Fingerprint matching process** performed by INA
- **Manual restitution of the results**

Contact us

Direct contact

[redacted]

signature@ina.fr

[redacted]

INA - Institut National de l'Audiovisuel
4, avenue de l'Europe
94366 Bry-sur-Marne Cedex - France

[redacted]

Personal data

INA Signature

for rights holders

The content distribution monitoring solution
to optimize the value of copyrighted videos

Maximize the value of your video assets by monitoring their distribution

Why should you monitor the distribution of your videos?

Three key facts make the monitoring of contents' distribution essential to **secure the financial sustainability of rights holders.**

1) The **evolution of video consumption:** expansion of access points to video content (TV, smartphones, tablets, games console…); increasing non-linear, interactive and social usages; multiplication of free access to contents.

2) The **diversification of monetization sources:** fragmentation of rights distribution between various territories/zones, broadcast medias (TV, mobile, web) and distribution chronologies (live, replay, recorded, VoD…), makes its control more difficult.

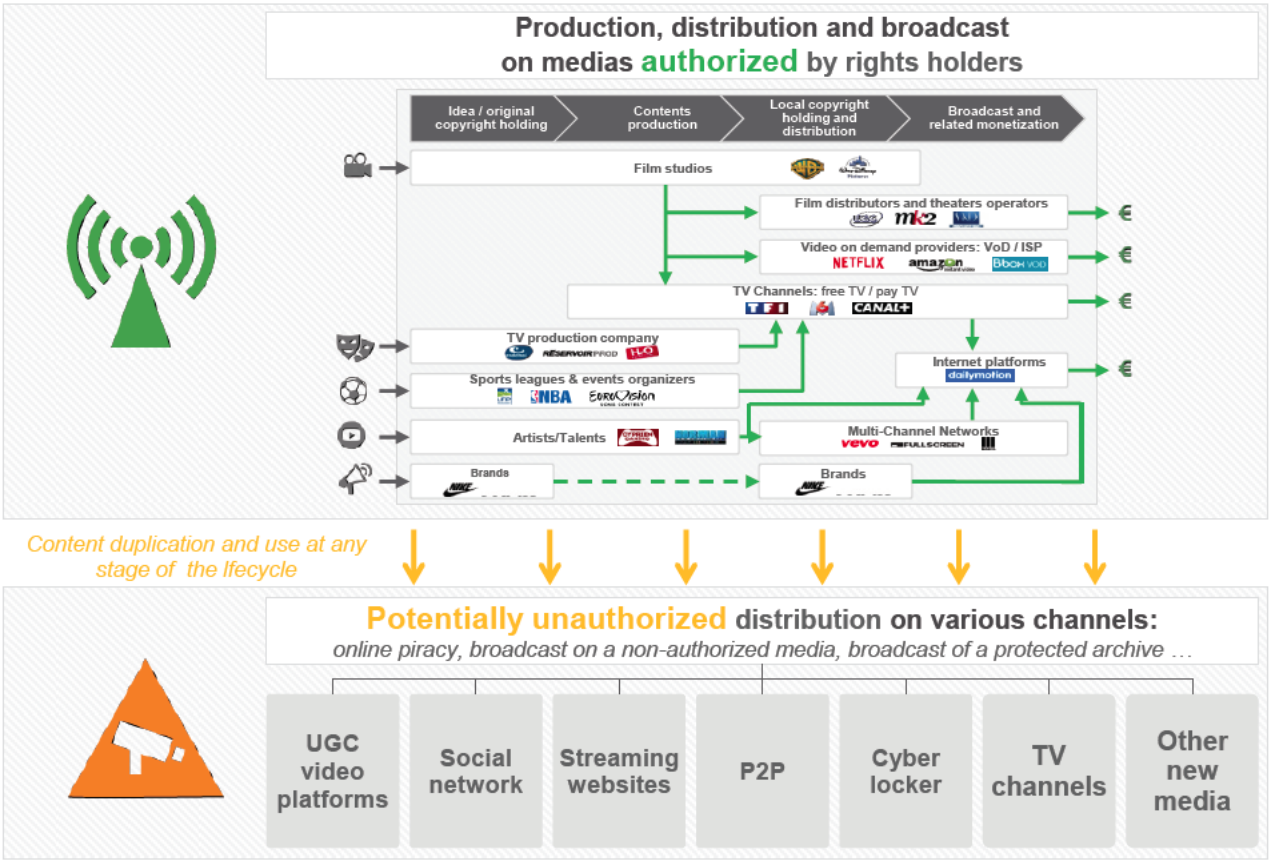
3) **Illegal content viewing,** with continuously evolving broadcasting and sharing technologies, toughen the need to track and control contents, in order to prevent rights holders revenues endanger.

Examples of use cases where video distribution monitoring brings value:

- For a TV show, maximize its replay audience on the channel's branded platforms.
- During an event (sports, music…), maximize the live audience on TV/Internet platforms used by the brand.
- For original content produced firstly for digital, maximize the audience and monetization on all Internet distribution channels.
- For a blockbuster movie, maximize cinema ticket sales, tracking and avoiding unauthorized distributions on the internet during its early life, while still taking advantage of the buzz created on Internet platforms.
- Maximize Internet revenues and identify TV broadcasts for long tail catalogs and re-use of archives.

What contents and medias should you monitor?

➔ Unauthorized and/or non-monetized distribution of copyrighted videos can occur all allong the contents' distribution chain, on a multitude of platforms and chronologies:

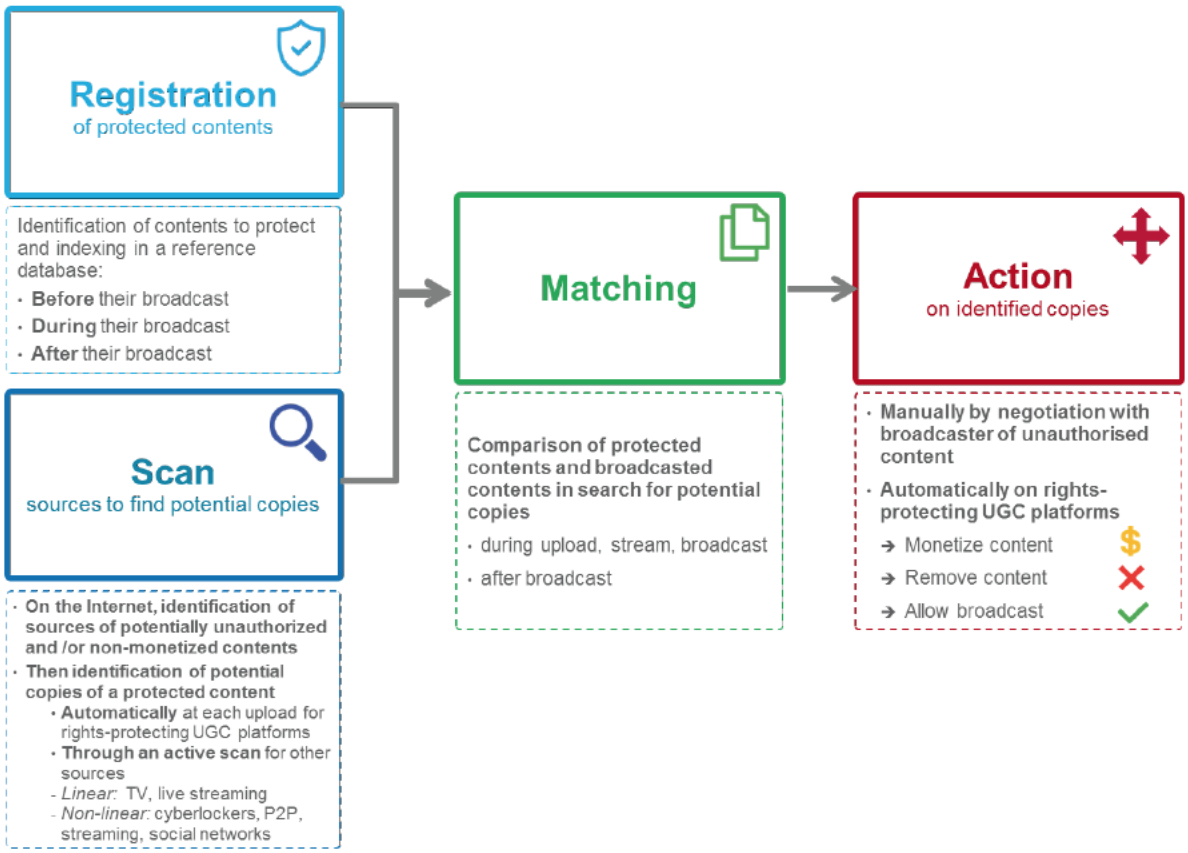


➔ It is key for your business to extend the monitoring scope to a wide technological, functional and chronological field to ensure maximization of the revenues from content distribution.

➔ Maximizing revenues related to your copyrighted contents implies to control the distribution and monetization of your videos on all accessible medias, especially at key moments of their lifecycle. Whatever their nature, video contents should be protected as early as possible.

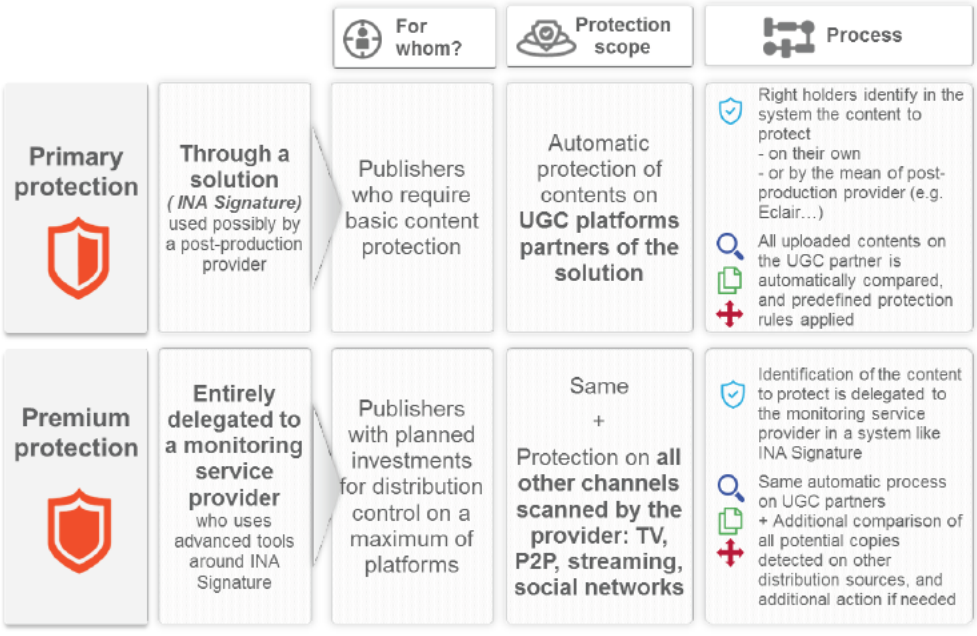
What key steps should you follow for an effective monitoring?

➔ Monitoring aims at finding existing broadcasted copies on TV or on the Internet of your copyrighted contents and taking actions towards distributors of these copies. In order apply this process, depending on your budget and priorities, you will have to define: the contents you want to protect, the sources to monitor (automatically verified platforms and other sources), and the types of actions to take per content.



[redacted]

[redacted]

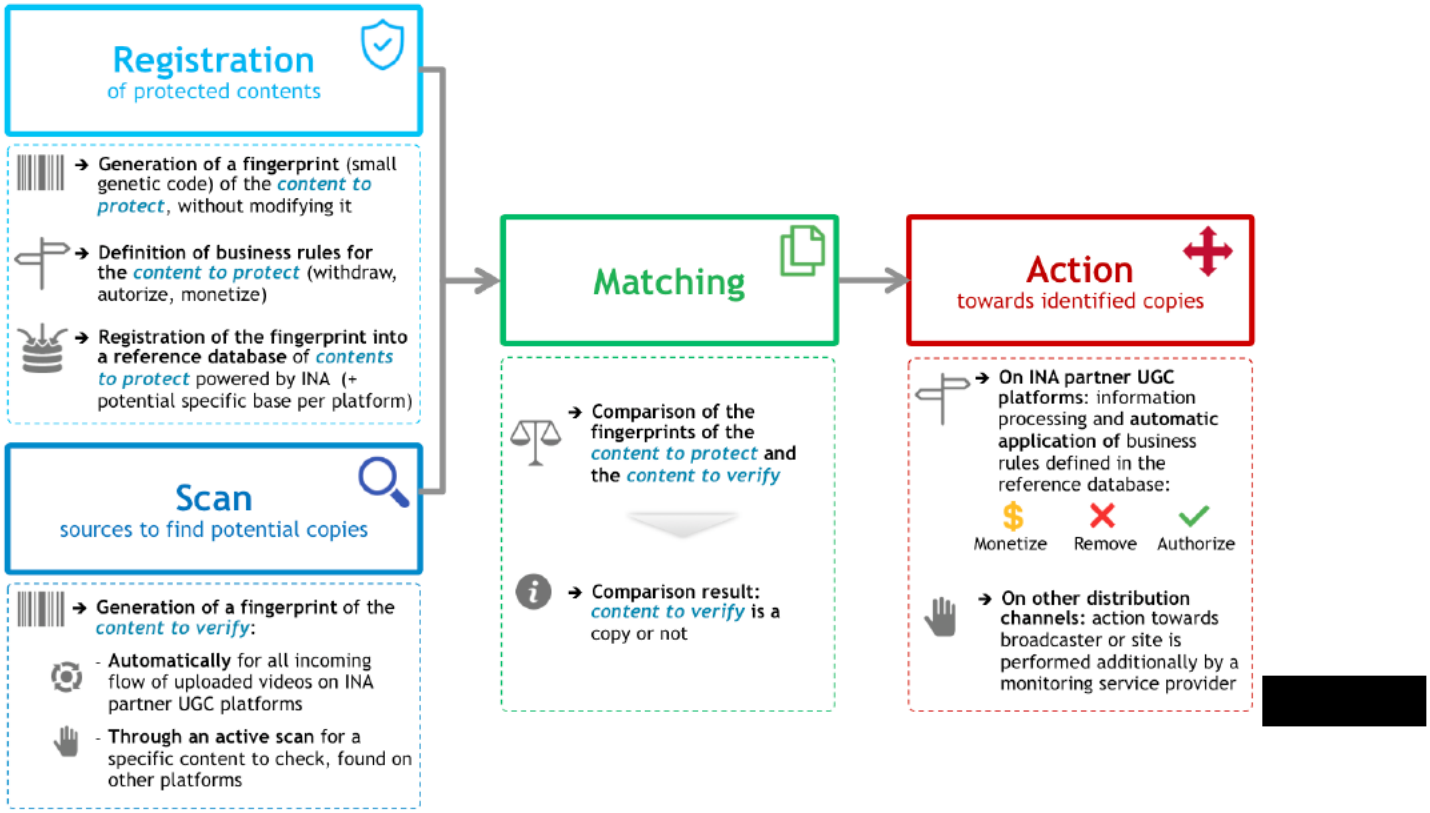


Commercial Information

Benefits of using the INA Signature solution

What features does INA Signature provide to monitor content distribution?

➔ INA Signature offers features at each step of the monitoring process to ensure a complete protection of contents:



How does INA Signature fingerprinting process compare to other identification technologies?

What is a fingerprint?

➔ Video fingerprints are small digital genetic codes, computed from the digitized images of a video sequence, and designed to represent its content.

➔ A set of fingerprints computed from a video sequence is a very condensed piece of information representing the essence of the sequence.

➔ In practice, computing fingerprints from digitized video files is a very simple process: a software program or device allows to quickly compute one fingerprint file per video file. Technically, the fingerprints are computed from the luminance of various areas of the images and from the motion information in the sequence. The video file is not modified or either copied in any database.

Signature is neither watermarking nor Digital Rights Management

Watermarking is an invisible tattooing operation, that only allows identifying tattooed copies. On the contrary, a fingerprinting process analyzes very closely a content copy and then deduces a genetic code without modifying the content. The fingerprint is then valid to potentially identify any past and future copy of the video.

DRM technologies are a set of technical measures intended to control what users can and can't do with the media and hardware they have purchased. DRM implies the set-up of encryption and conditional access technologies. While offering a good level of protection in a closed network, copies can always happen and monitoring is necessary.

What are the key benefits of using INA Signature for monitoring service providers and rights holders willing to protect on their own?

Safe

- **No need to store** the content / registration can be done without keeping any copy of the content
- **No modification** of the content
- **Master** fingerprint use and lifespan
- Right holders' monitoring service providers have access to their clients' fingerprints bank

Standard

- Centralisation of all the right holder's fingerprints into a **reference database**, including already key US movies studios and international sports leagues
- Automatic identification and comparison of all incoming flow on partner UGC platforms, including Dailymotion, representing 110 M UV per year (2014), ensuring **de facto protection on these platforms**

ina Signature

Simple to use

- **Speed of execution** of the generation process enabling to protect live contents
- Only **one fingerprint for all** international versions
- Efficient in **all technological** (web, TV) and **functional** (live, replay) distribution fields
- **Automation** of business rules application on partner UGC Websites. Can also be run **manually** to match contents from all other sources.

Super efficient

- **Robustness** of the software: detection even with modifications on content enabling to guarantee a reliable moderation
- Virtually **no false detection**: alert only in case of an actual copy → enable to automate detection
- **Revenue-oriented**: enables to monetize right holders' contents even on non-owned medias

Frequently Asked Questions

To which extent can Signature detect transformed video copies?

➔ **INA Signature detects copies even with significant modifications between the protected content and the distributed copy**

- INA-Signature has regularly been benchmarked in **tier 1** of rights holders and expert tests
- The samples below illustrate a **variety of transformations types** that Signature has successfully detected on actual use cases; Signature robustness includes support of those transformations in real-world cases: text and graphic overlays, color / B&W changes, crops, camcords, video compression, video format changes, audio track changes.
- INA-Signature is **available for further tests** as needed to check it satisfies your needs

On the left the original content and on the right the broadcast content that was properly identified by Signature. This illustrates the reliability of the technology.

How reliable is the Signature comparison process?

➔ Signature avoids **false negatives** (non-detection of a copy whereas it is one) and **false positives** (false detection of a copy whereas it is not one) with ***zero*** **technical false detection identified over several years** of operation for a major UGC platform.

How fast is the Signature fingerprint generation process?

➔ Fingerprints are generated **up to 20 times faster than real-time**, depending on the source video format

➔ *e.g. for a 3 minutes standard video, fingerprint can be generated in less than 10 seconds*

How fast is the Signature fingerprints comparison process?

➔ The technical setup is scaled depending on the detection time requirements per use case

➔ For example, video sharing platforms integrate the comparison feature during the video upload and initial processing (time **below 2 min**), so that the user experience remains smooth

➔ *Actual daily operations compare* **in live** *sport matches streams or uploads during the events*

How much content can Signature compare?

➔ INA Signature offer to its clients the ability to **process high volumes of requests simultaneously**

➔ *e.g. with Signature, INA monitors automatically about 100 TV channels in real-time to identify copies of its distributed archives*

Get started with INA Signature

INA enables you to set up a free Proof Of Concept to quickly and easily discover Signature's key features

Free discovery test (1 day)

- **Upload** of the videos to be compared onto INA server (reference videos & potential copies)
- **Fingerprint generation and matching process** performed by INA
- **Manual restitution** of the results

Advanced test (1 month)

- **Fingerprint generation test** made on your own
- **Fingerprint matching process** performed by INA
- **Manual restitution of the results**

Contact us

Direct contact

signature@ina.fr

INA - Institut National de l'Audiovisuel
4, avenue de l'Europe
94366 Bry-sur-Marne Cedex - France

Note

EMETTEUR : Service Développement & Missions / Signature
DESTINATAIRE : Sarah JACQUIER, Commission Européenne / DG Communications Networks, Content and Technology (CONNECT)
DATE : 28 juin 2016

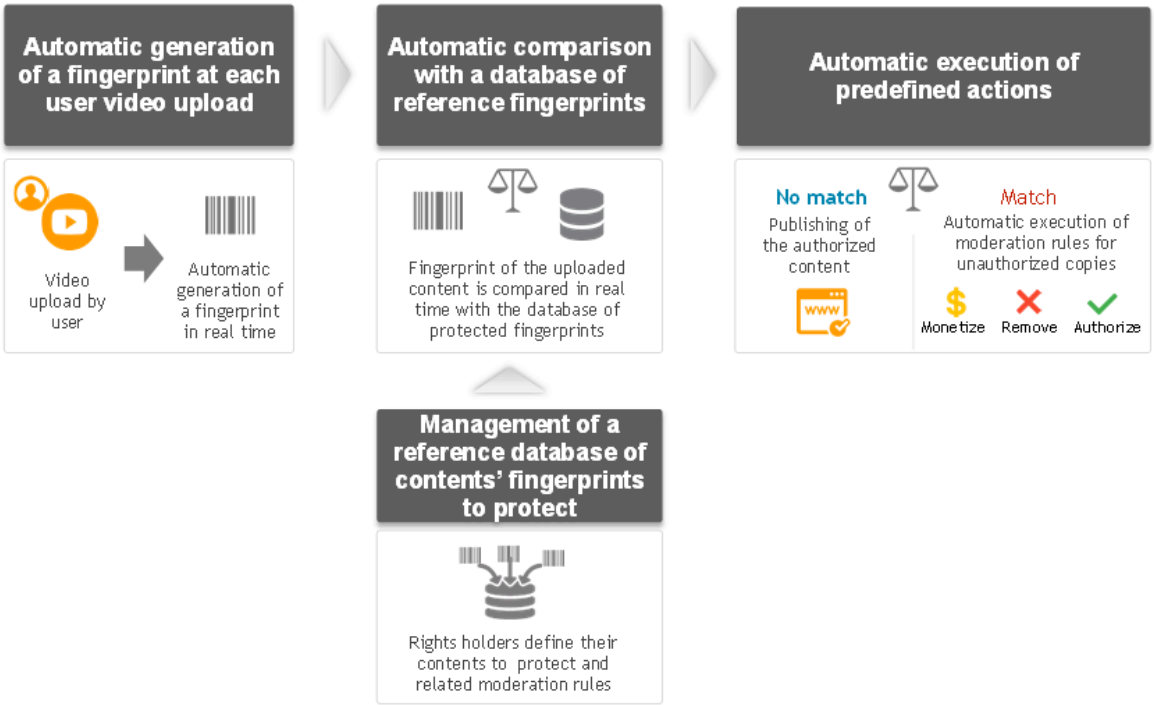
SUJET : Questions / Réponses sur la technologie Signature

I. Illustration du fonctionnement de Signature

La technologie Signature, issue de la recherche et développement de l'Ina, est opérationnelle depuis 2008. Cette technologie est construite autour de deux composants :

- Le premier génère une empreinte à partir d'une œuvre de référence ou d'une vidéo candidate
- Le second compare un flux d'empreintes issues de vidéos candidates avec une base d'empreintes de référence.

L'Ina endosse le rôle de tiers de confiance, en opérant sa solution telle une zone « neutre » qui réunit les détenteurs de droits et les sites de partage.



II. Questions / Réponses

Quel est le mode de fonctionnement pour un ayant droit ?
Pour générer les empreintes et les métadonnées, les ayants droit ont accès à 3 solutions :

- Une solution logicielle, lorsqu'ils disposent des compétences et justifient de volumes importants.
- Un réseau de partenaires (laboratoires et prestataires « antipiracy »), lorsqu'ils délèguent cette gestion.
- Une solution de type « Box », pour les ayants-droit qui souhaitent protéger un flux « live ».
- (en chantier) Un service en ligne, adapté à de petits volumes, doit être prochainement proposé.

A l'exception du dernier service, l'Ina n'a pas besoin d'avoir accès au contenu. Cette condition est d'ailleurs une exigence de certains studios, qui génèrent des empreintes pour des contenus jamais diffusés.

Quel est le coût du service pour les ayants droit ?
L'ayant-droit paye un loyer pour les empreintes « actives » (celles prises en considération lors des analyses).

Il a la possibilité de générer et de stocker gratuitement un nombre illimité d'empreintes. S'il fait appel à un partenaire, alors ce dernier facture les coûts liés à la génération.

Commercial Information

Pourquoi ce service est-il payant, à l'inverse de solutions concurrentes qui sont proposées gratuitement ?
Les principales solutions déployées sur le marché s'appuient sur une reconnaissance audio. Cette dernière est peu coûteuse, mais elle ne permet pas d'identifier des contenus transformés (par exemple l'utilisation d'extraits dans une vidéo dont la bande son a été modifiée).

Google propose une solution intégrant la vidéo (« CONTENT ID ») sur son site Youtube. Il dispose des ressources techniques et financières pour proposer cette solution gratuitement, et l'utilise par ailleurs pour son programme de monétisation.

Le cadre légal actuel n'étant actuellement pas contraignant pour les sites de partage, ces derniers privilégient la mise en œuvre de solutions « économiques », sans nécessairement prendre en compte leur efficacité.

La solution Signature ne sacrifie pas la qualité : elle permet de détecter des intégrales et des extraits, est robuste aux transformations des contenus, est utilisée pour des applications « live », est automatisée en raison de l'absence de faux positifs.

Depuis 2008 l'Ina a notamment travaillé à rendre cette solution plus compétitive, dans un contexte où le « CLOUD » rend la puissance de calcul plus facilement accessible.

La structure de coût de la solution Signature - principalement liée à la puissance de calcul nécessaire, beaucoup plus importante en vidéo qu'en audio - est donc corrélée au flux à analyser quotidiennement (sites de partage) et à la taille de la base de référence (ayants-droit).

Si la génération et le stockage des empreintes représentent un coût marginal, maintenir ces empreintes actives génère des coûts à chaque comparaison. C'est pourquoi le modèle actuel prévoit une contribution des ayants-droit.

Quelle le nombre de contenus protégés actuellement ?
La base de référence contient plus de 650 000 références de contenus vidéo. Elle comprend des contenus de stock (catalogues) et de flux (évènements sportifs).

Chaque ayant-droit signe une lettre accord avec l'Ina, dans laquelle il prend plusieurs engagements pour le bon fonctionnement de la base de référence.

Quel est le mode de fonctionnement pour un site de partage ?
Le site (UGC, réseau social, cloud privé…) calcule les empreintes des vidéos uploadées par les internautes. Ces empreintes sont envoyées à l'Ina qui les compare avec les empreintes de la base des contenus de référence. L'Ina retourne les actions à appliquer à ces vidéos (bloquer, autoriser, monétiser).

A l'inverse d'un mécanisme de « Notice and takedown », le système filtre le contenu avant sa publication. Le système permet ainsi d'éviter la réapparition du contenu (« staydown »).

Quel est le tarif pour un site de partage ?
Le tarif appliqué dépend notamment du mode d'exploitation de la solution : en mode service ou en mode logiciel.

A titre indicatif, l'analyse de 500 000 requêtes (~83 000 heures de vidéo) est proposé au tarif de 2 600€ HT (juin 2016), dans le cadre de notre service premium (en mode service 24/7, avec un temps de réponse pour chaque requête inférieur à 2 min, afin de ne pas dégrader l'expérience de l'internaute).

Le tarif est calculé en fonction du volume (nombre de requêtes et durée moyenne des requêtes) et du niveau de service requis (délai de réponse, flux instantané à analyser, disponibilité 24/7).

[redacted]

Commercial
Information

III. ANNEXES

- Document de présentation du service à l'attention des sites de partage
- Document de présentation du service à l'attention des ayants droit