Digital Fingerprinting

White Paper

MEDIAHEDGE

a service of Civolution and Gracenote

Digital Fingerprinting

The need for content identification and monetization

The volume of online audio and video content is growing exponentially. An August 2009 survey conducted by the Diffusion Group for Digitalsmiths found that more than 70% of US Internet users surveyed had watched online video in the past week, and more than one-half had watched online TV programs.

Intel's chief of technology, Justin Rattner, predicted, back in September 2009 at the Intel's Developer Forum (IDF) in San Francisco, that by 2015 more than 12 billion devices will be capable of connecting to 500 billion hours of TV and video content.

These forecasts emphasize the growing need of content and rights holders to identify copyrighted content as it moves across computers and mobile phones around the world. Media owners are today looking for ways to track and control the distribution of their content on the broadcast television and the internet. They are also looking at new ways to develop business models with digital publishing platforms such as UGC or social network sites, in order to monetize their content, including through advertising revenue sharing. Content publishing companies, in turn, are looking for means to expand their business in advertising and to offer additional services that generate real revenues. There is a clear need for technology that enables flexible business rules to be applied to online content and which fits seamlessly into the established content-to-consumer delivery chain. Digital fingerprinting meets this need.

Digital Fingerprinting gives content owners and publishers more options to control the distribution of their content and enables monetization models.

This white paper provides a high level overview of digital fingerprinting and examines how this technology can be integrated into workflows for automatic and consistent content identification and monetization.

Digital Fingerprinting

Fingerprinting analyses the unique features of an audio or video asset and compares these against 'reference' fingerprints stored in a database. One of the key characteristic of fingerprinting is that it does not modify the content. Similar to a human fingerprint that uniquely identifies a human being, a digital fingerprint uniquely identifies a piece of video/audio content. The analogy can be extended to the process of fingerprint matching : first, known fingerprints ('reference' fingerprints) must be stored in a database; then, a 'candidate's' fingerprint is queried against the fingerprint database for a match.
Sometimes fingerprinting technology is referred to as robust video hashing. Conventional cryptographic hashing (e.g. MD5) is fragile; an error in a single bit is sufficient for the hash to completely change. These fragile hashing technologies are not considered to be content-based identification technologies since they do not consider the content, understood as information, just the bits.

What is a fingerprint ?

A fingerprint is a set of features that uniquely identify a segment of audio or video content (fig.1). The creation of a video or audio fingerprint involves the use of specialized software that decodes the video/audio data and then applies several feature extraction algorithms. Digital fingerprints are highly compressed when compared to the original source file (one fingerprint can be as small as 1 KB) and can therefore be easily stored in databases for later comparison. Fingerprints cannot be used to reconstruct the original video or audio content.

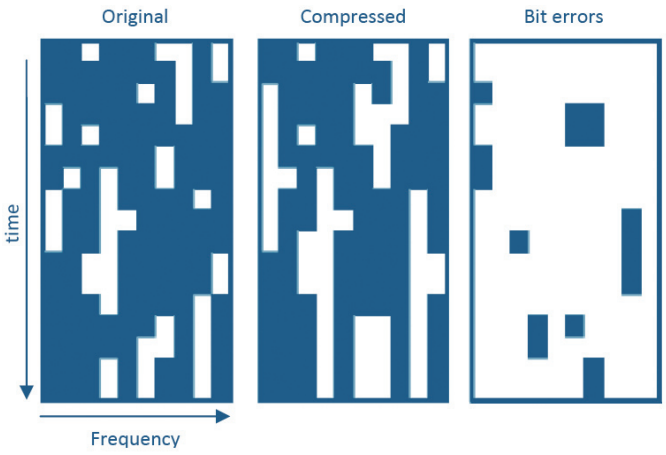


Figure 1 : Graphical depiction of fingerprint

Fingerprint parameters

An ideal fingerprinting system should fulfill several requirements. It should be able to accurately identify a media asset, regardless of the level of compression, distortion or interference in a transmission channel. For many other applications it should identify the title from excerpts as short as just a few seconds (a property known as granularity), this requires support for shifting - the lack of synchronization between the extracted fingerprint and those stored in the database. It should also be able to deal with other sources of degradation, such as :

- Audio : pitching (playing audio faster or slower), equalization, background noise, D/A-A/D conversion, speech and audio coders (such as GSM or MP3).

- Video : heavy compression (e.g. 'youtube' quality and much less), insertion or removal of subtitles or logos, scaling, aspect ration change, speed change, 16:9 to 4:3, camcorder, black bars, conversion to black and white , flipping etc.

A fingerprinting system should be computationally efficient and fully scalable. All this is related to the size of the fingerprints, the complexity of the search algorithm and the complexity of the fingerprint extraction.

Fingerprint parameters

1-2KB, is the size of single fingerprint block

4.65 seconds, is the length of a video fingerprint block

3 seconds, is the length of an audio fingerprint block

Fingerprint system

The general setup of a fingerprinting system is depicted in Figure 2. The two key components of a fingerprinting system are the fingerprint server and one or more fingerprint clients. There are two types of fingerprint clients :

- Ingestion clients : to ingest 'reference' fingerprints and associated metadata in the fingerprint database. Typically used by a content owner who wants to ingest reference fingerprints of their assets.

- Identification clients : to identify unknown content. An identification fingerprint client extracts fingerprints from audio and/or video sends them to the fingerprint server for identification. Typically used by websites who want to identify uploaded content.

Both fingerprint identification and ingestion clients require a TCP/IP connection with the server and can be located at any location from where a TCP/IP connection can be made to the server.

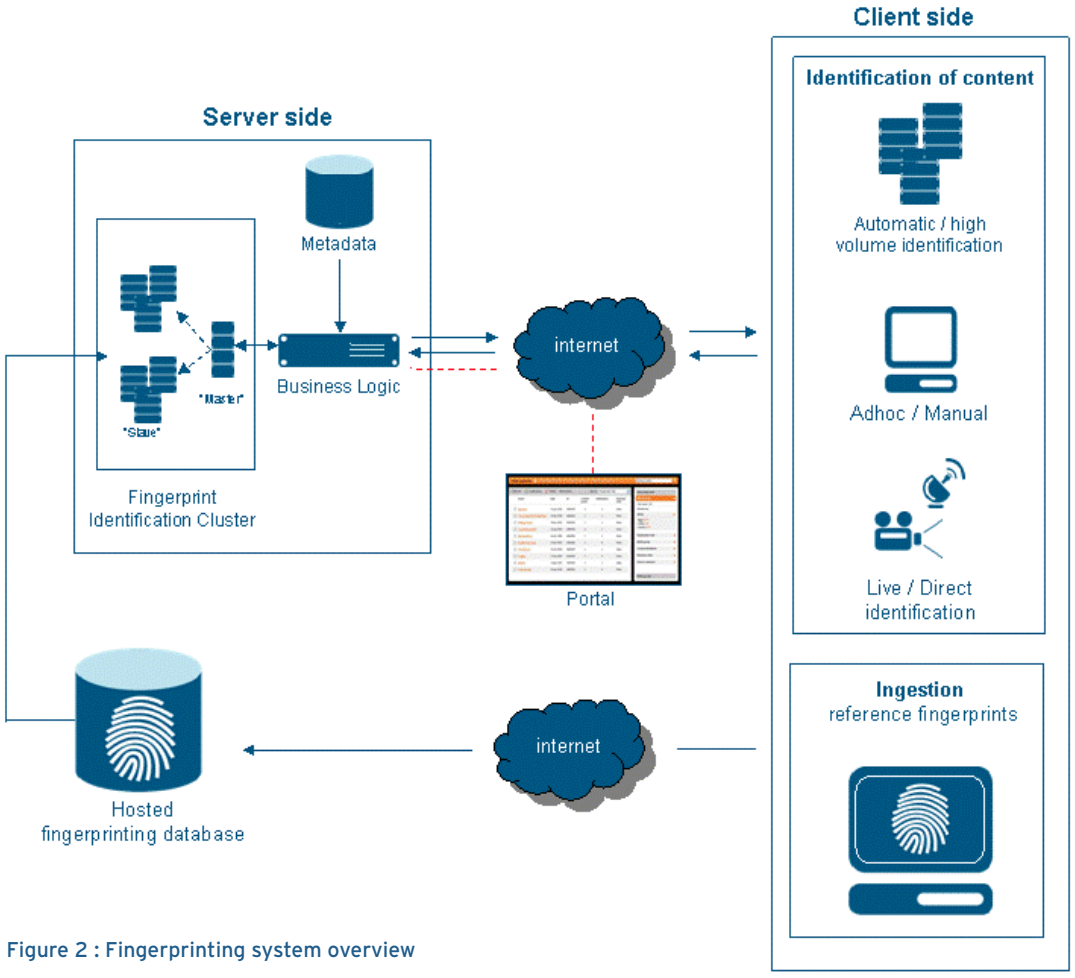


Figure 2 : Fingerprinting system overview

A high-level description of the activities that take place in a fingerprint system is as follows :

The fingerprint server (“server side”) provides the following functionalities :

- Fingerprint identification by searching and matching fingerprints generated by the identification fingerprint clients (‘candidate’ fingerprints) against the fingerprints in the reference database.

- Applying business logic to the identification results based on Movielabs content recognition rules (www.movielabs.com) and sending this information back to the identification fingerprint client.

- Asset management via Business Portal (see figure 3). Content owners can manage their assets via a business portal. They can dynamically assign business rules to their assets and create identification projects.

The fingerprint clients (“client side”) :

Ingestion fingerprint clients provide the following functionalities :
- Extracting fingerprints from audio and/or video.
- Sending them, including associated metadata such as title, assets ID, copyright holder etc. to the fingerprint server to be stored as ‘reference’ fingerprint in the hosted fingerprint database.

Identification fingerprint clients provide the following functionalities :
- Extracting fingerprints from unknown audio and/or video.
- Sending them to the fingerprint server for identification.
- Displaying the identification result. This can vary from displaying only an aggregated business rule such as ‘take down/block’ or showing detailed identification results.

The software clients for fingerprint ingestion and fingerprint identification allow for different levels of workflow integration : from simple scripting level to deep SDK integration. All software includes easy to use sample code, both for ingestion and identification). Media/Format typessuch as the following codecs are supported : MPEG2, MPEG4, WMV, flash, Quicktime, AVI, Divx, MPG, H264, Vc-1, MP3, AAC, etc.

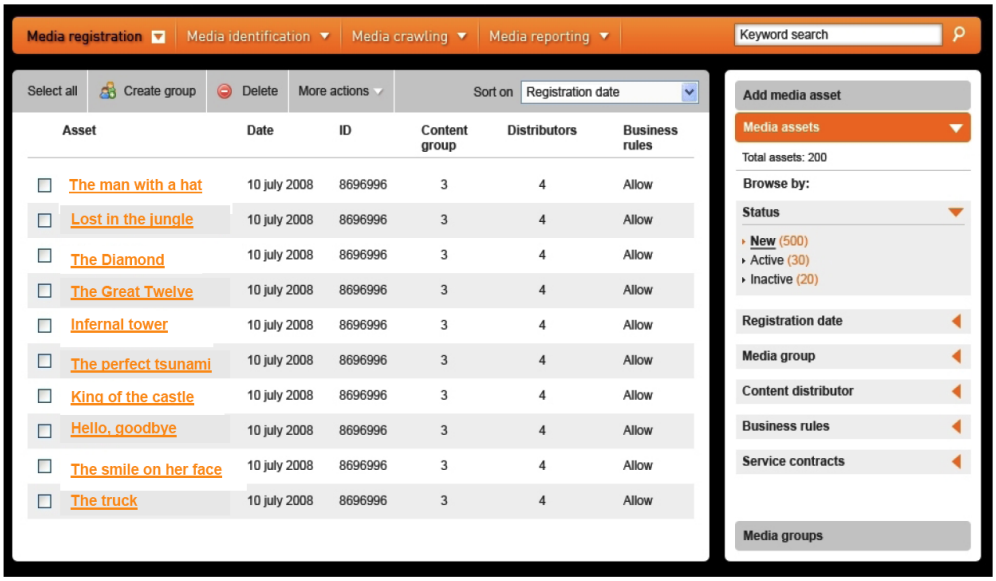


Figure 3 : Business portal for assets and business rules management

Fingerprinting vs. Watermarking

Both fingerprinting and watermarking are content identification technologies. If they are both used to identify a specific piece a video or audio asset, they are two very distinct technologies with unique applications.

Watermarking

Digital watermarking is the subtle modification of content by which an ID tag or payload (bits of information) is inserted within the media asset before distribution, making such asset unique and allowing its automatic identification. Being part of the content itself, digital watermarks survive cropping, morphing, degradation, conversion and standard processing such as conversion to MP3s/AAC, degradation to YouTube quality video and even camcorder capturing. The digital payload - which can be inserted down to every half second of content - is generally a unique identifier which is stored in a database. The content identification is mostly obtained by reference to this database. Watermarking can be used for various types of applications such as :

- Monitoring of assets
- Identification of the source of a media asset confirming its ownership
- Protecting copies of media assets by associating each copy to an individual 'owner'
- Triggering specific information or applications upon detection of a watermark
- Tagging of clips that are likely to be re-used in future programmes

Fingerprinting Applications

Broadcast monitoring

Broadcast monitoring is an application which enables content owners to automatically verify where, when and how long their content was broadcast via terrestrial, cable or satellite television (figure 4). The output of the broadcast monitoring service is a comprehensive reporting via a secure client website or automated data interchange reports which provide detailed insight into when and where content is broadcast.
The reported information can be used for contractual compliance monitoring, media intelligence, management decisions, client renewals or competitive analysis.

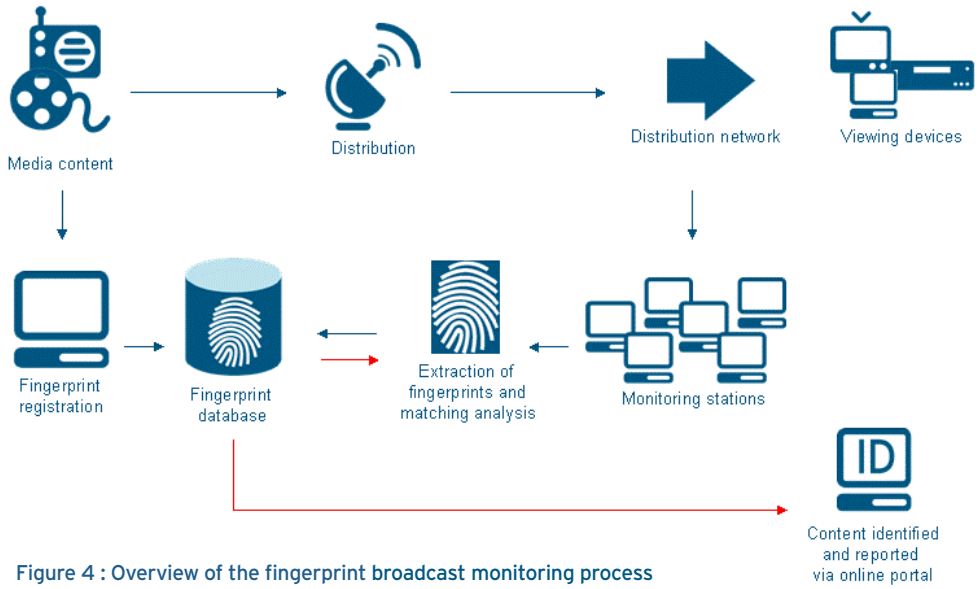


Figure 4 : Overview of the fingerprint broadcast monitoring process

Internet monitoring

Similar to the broadcast monitoring system, with a fingerprinting database in the background, web-crawling technology can be used specifically to monitor the internet (figure 5). The process uses a set of keywords to monitor internet sites. All found multimedia content is weighted on basis of various criteria - keyword usage, context, date/time of upload, popularity etc. – and content with the highest weight are categorized as "suspected media". These media files are downloaded and checked against the reference fingerprinting database. In case of a positive identification a take down notice can be issued : the website will be notified that they are hosting copyrighted content. In some cases – by having direct access to the content management system (CMS) of a website – the copyrighted content can be removed immediately.

The output of the internet monitoring service is dashboard type of reporting which provides detailed insight into when and where content is used on the internet.

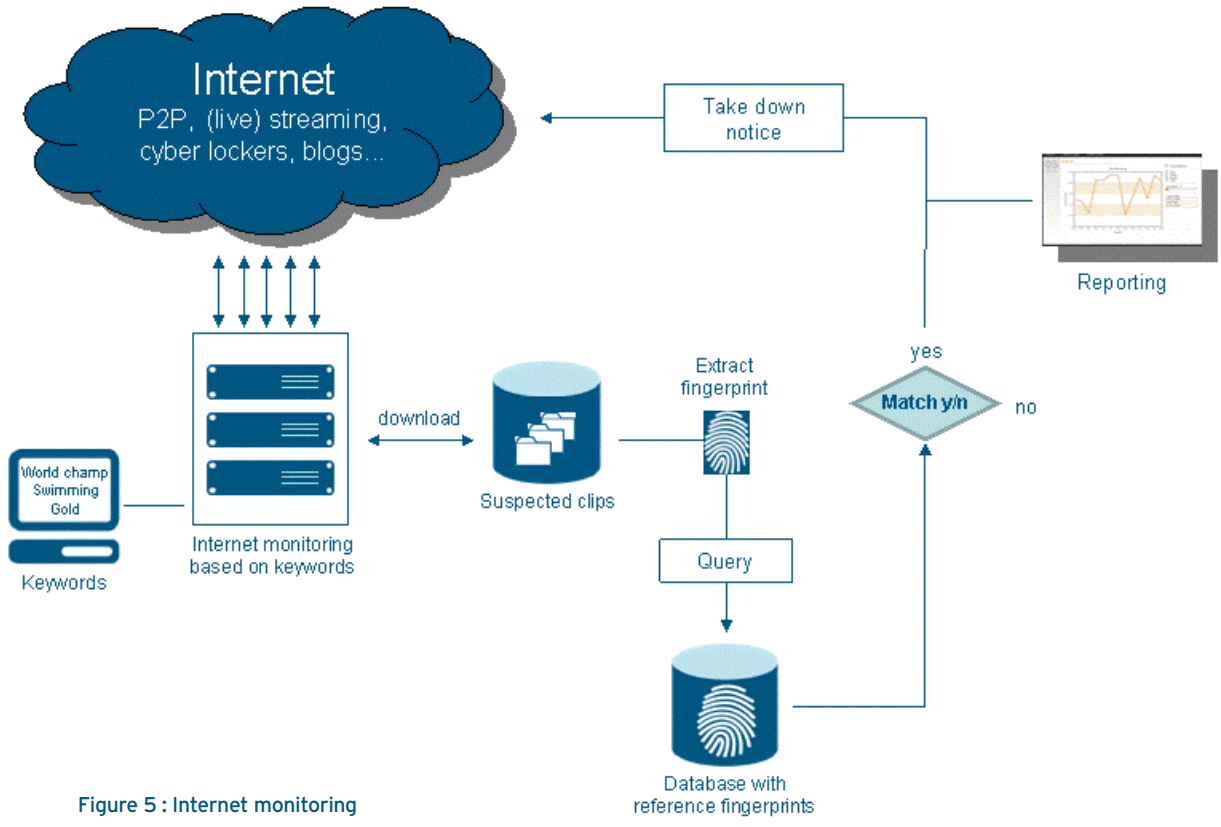


Figure 5 : Internet monitoring

Copyright control / Content filtering

Integrated in a content distributors back end, fingerprint technology allows content distributors or aggregators such as social networking sites and UGC websites to automatically recognize large volumes of content at the moment of upload and allow or block its full upload, depending upon pre-set criteria. If video fingerprint extraction and identification process is an integral part of the distributor's internal workflow; the fingerprint process doesn't delay the internal publishing process, nor does it require expensive additional hardware investments.

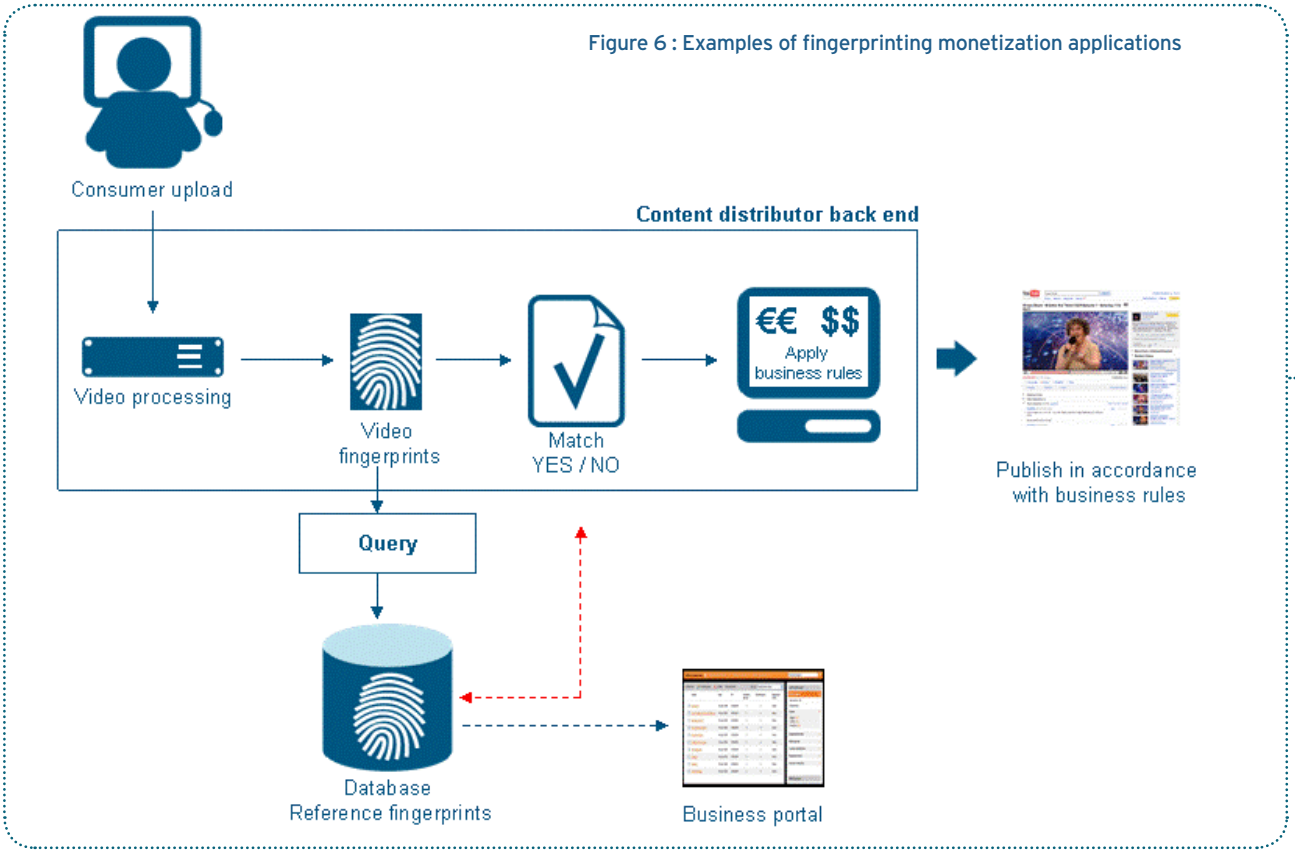
Monetization

In addition to filtering and blocking, content owners and distributors are working with social networks and UGC companies to develop new business models in order to monetize their content and turn potential piracy into profit. New models such as advertisement linking or website re-directing are now emerging. Fingerprint technology is an effective enabler of such monetization applications. Upon identification of content and based on specific 'business rules' the system, integrated in the website backend, will trigger the inclusion of a weblink, a specific discount coupon or an advertisement, see figure 6.

Metadata association

Enhanced metadata association and service linking based on metadata e.g. Content Identification services on mobile, subtitle services, movie/TV-series background info service, parental control services, trailer services, content discovery services, product purchase services, for consumer electronic devices based on video/audio recognition creates a richer viewing experience for the consumer. Scalable fingerprinting system enables such applications.

Figure 6 : Examples of fingerprinting monetization applications



Fingerprinting in the Digital Workflow

Fingerprint extraction / ingest

In order to be able to identify unknown content, content owners first need to ingest the 'reference' fingerprints of their assets, including the associated metadata in the fingerprint database. The process of fingerprint ingest includes the following steps **(see fig.7)** :

1. Extract fingerprints from the media file using fingerprint ingestion client software.
2. Combine the associated metadata with the extracted fingerprints.
3. Ingest the fingerprints and metadata into the reference fingerprint database.

The extraction and ingest process of existing content libraries can be done at the content owners so that the assets can stay in the safe environment at their premises.
There are three different types of ingest; live, large archives and manual/ad hoc ingests. Each type of ingest has its own impact on the fingerprint system :

- Live ingest : system processes real-time updates in an operational system.
- Large archive ingest : system automatically ingest large amounts of files (including metadata).
- Ad hoc/Manual : system does simple desktop file ingest.

After ingest a content owner should be able to verify if all the ingested assets are available in the system and if the assets are linked to the correct associated metadata.

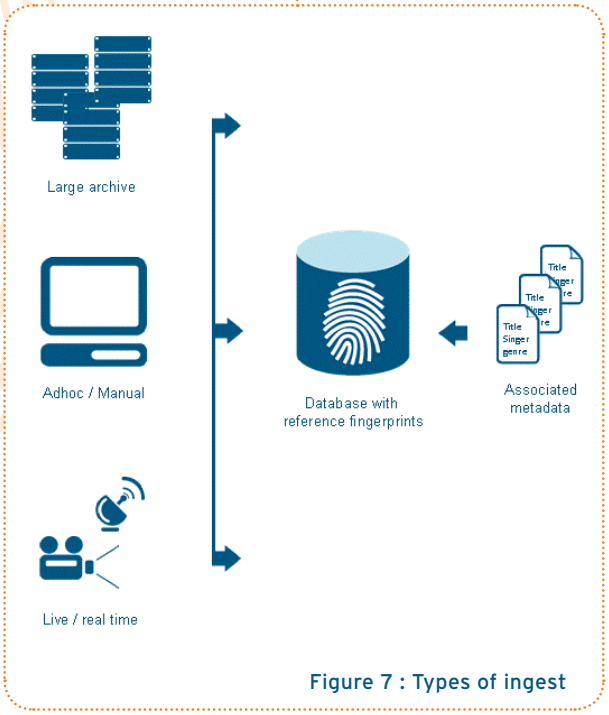


Figure 7 : Types of ingest

Fingerprint identification

Fingerprint identification is the process of identifying unknown content (aka "candidate" content). It consists of the following steps **(see fig.8)** :

1. Extract fingerprints from the media asset ("candidate") using the fingerprint identification client software.
2. Send the fingerprint to the fingerprint server. The fingerprint server queries the fingerprint database with reference fingerprints. The fingerprint server then sends the identification results back to the fingerprint identification client software.
3. Process the identification results in a customer specific application.

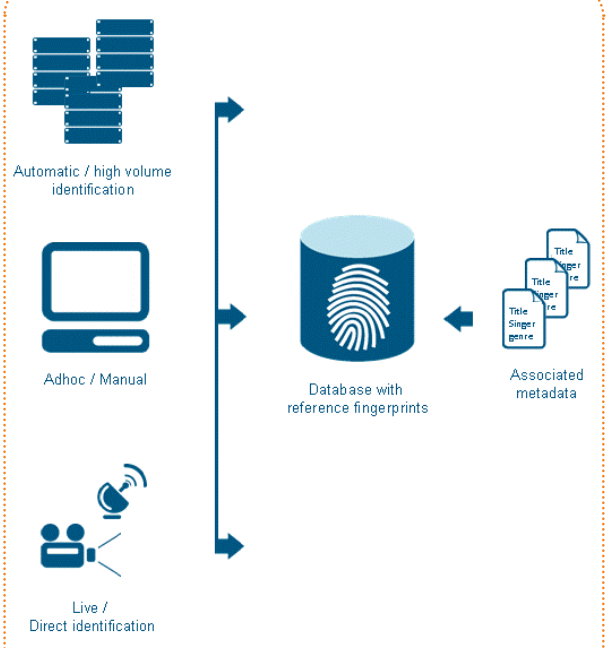


Figure 8 : Types of identification

Fingerprinting and Transcoding

The integration of a fingerprint generation plug-in into a transcoding system enables users to generate reference fingerprints immediately from the content during the encoding or transcoding process. These digital fingerprints are then uploaded to the fingerprint server. The creation of reference fingerprints directly within existing encoding and transcoding workflows increases productivity and reduces operational costs by eliminating the need for separate process steps to create the fingerprints. By generating the reference fingerprint during production, content owners only need to upload the reference fingerprint to the reference database. Such data files are much smaller than the actual media files **(see fig.9).**

Similar workflow efficiencies can be realized when generating 'candidate' fingerprints for matching against the reference database; for example when the fingerprint plug-in is tightly integrated with the transcoding process of a UGC website, the fingerprint is generated immediately during the transcoding process.

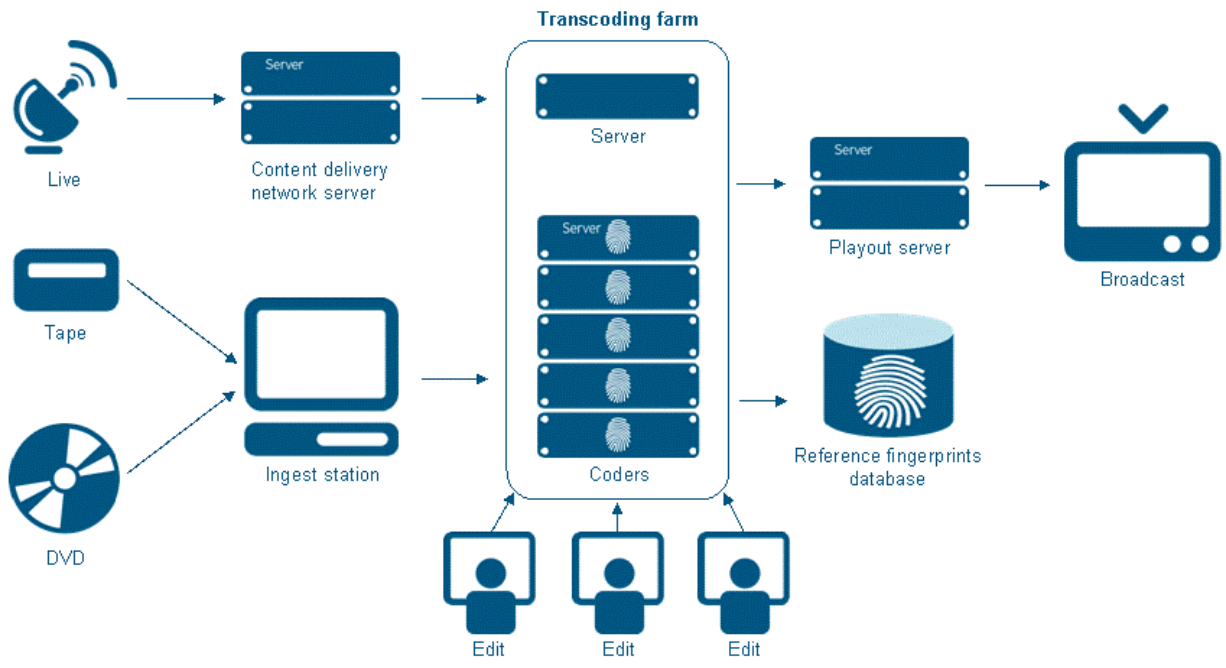


Figure 9 : Transcoding process

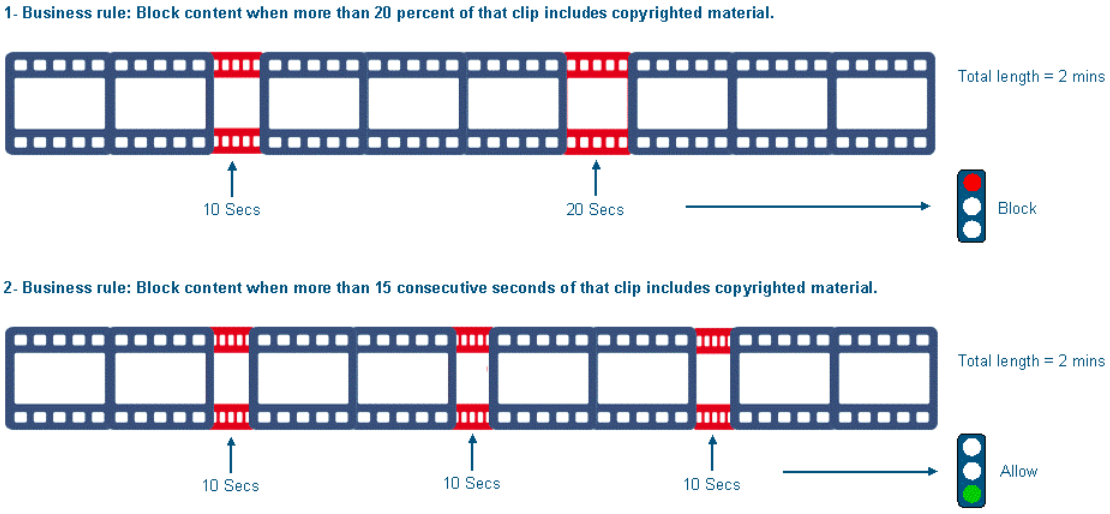
Fingerprinting and MovieLabs Content Recognition Rules

Movielabs has devised a specific scheme, known as Movielabs Content Recognition Rules which describes the various methods of applying more complex and sophisticated ways of interpreting preliminary identification results. Some examples (figure 10) of such business rules and associated actions are as follows :

a. On recognition of at least 60 seconds of an asset, remove it from use.
b. This asset is playable but only in the US.
c. This asset is not playable in the UK until July 4, 2010.
d. In case of a mash-up of multiple assets from the same television series, if the aggregate time of all assets from the series totals 3 minutes or more, then remove it from use.
e. On appearance of an asset on a UGC site, send an email notification to the rights holder.
f. When delivering an uploaded copy of an asset, some ads are associated with it and should be shown.
g. If an uploaded video contains over 60 seconds from a movie, and that represents over 50% of the video's total length, quarantine it, pending investigation.

An asset can have multiple rules associated with it, which can vary with the location of the uploader, the publishing platform that is being used or the location of an individual attempting to access the copy. A content owner may also want to deploy different rules for different sites or ISPs, in which case each such entity would receive a different set of rules.

Figure 10 : Examples of business rules



Summary

Fingerprinting is not only an identification technology, it enables monetization. For example, it can be used for broadcast monitoring to confirm contractual compliance and provide media and business intelligence. It allows automatic and continuous global internet monitoring to help content owners control the distribution of their content and supports a wide variety of business rules from take-down instructions to advertising revenue shares. Fingerprinting enable enhanced metadata applications that create a richer viewing or listening experience for consumers. These applications help social networking sites and user generated content websites to create economically sustainable businesses by making it easy to cooperate with content owners.

Fingerprint generation and identification forms an integral part of the content distributor's internal workflow: it does not delay publication. By providing practical and cost-effective ways for content owners and publishers to identify, monitor and monetize their content, fingerprinting (and its applications) should now be viewed as a key enabler in the protection of existing revenues and for the development of new business opportunities.

Gracenote and Civolution combine their respective content fingerprinting and identification technologies and databases to provide "best-in-class" advanced solutions for audio and video content detection, identification, and content monetization across multiple platforms. Both Gracenote and Civolution customers can benefit from the combined audio and video fingerprinting technologies and databases to power digital media services and protect and monetize all forms of digital content.