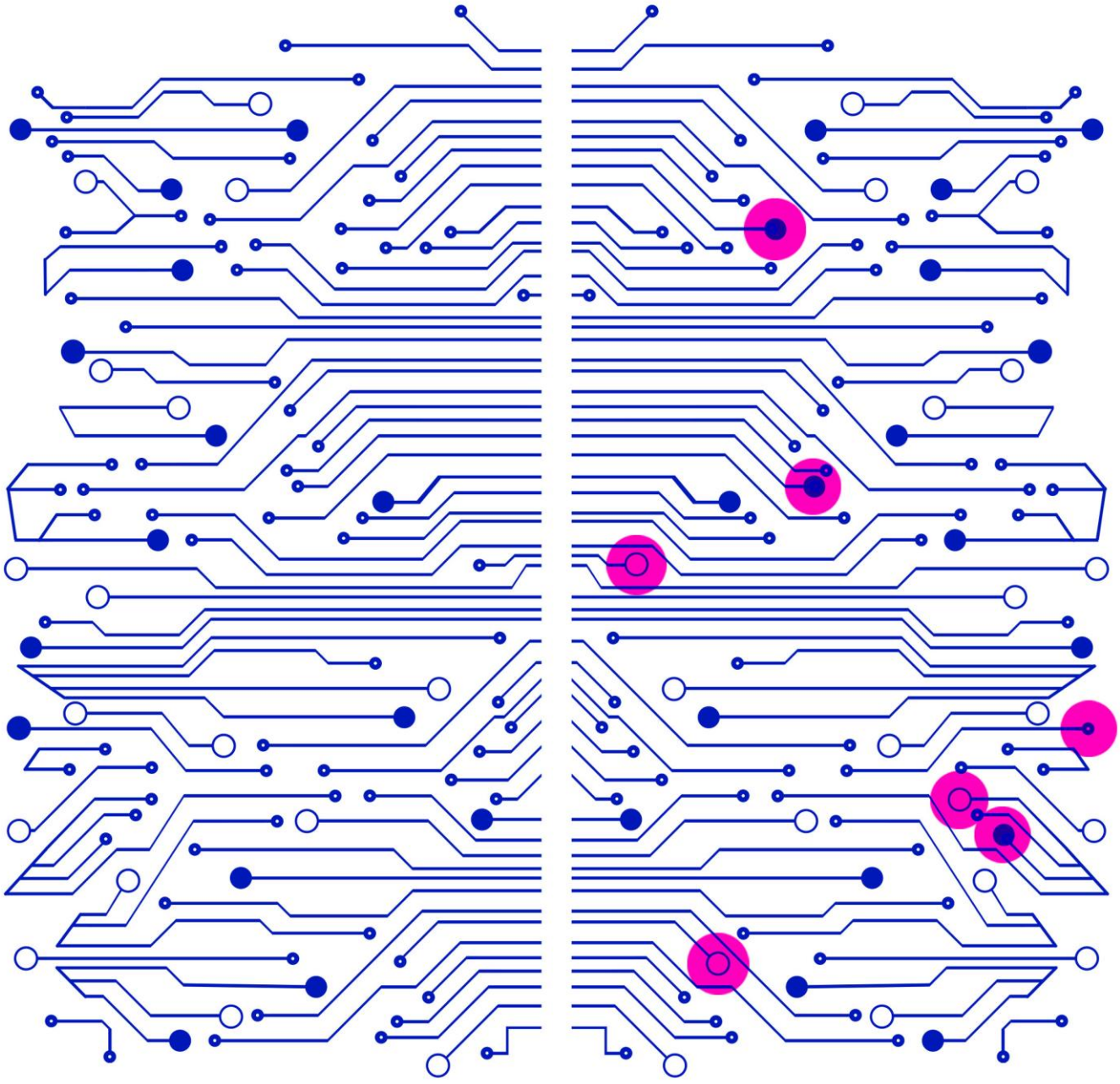
EUIPO
EUROPEAN UNION
INTELLECTUAL PROPERTY OFFICE

www.euipo.europa.eu

Automated Content Recognition: Discussion Paper – Phase 1 ‘Existing technologies and their impact on IP’



November 2020

DISCLAIMER

The views expressed in this discussion paper do not represent any official position of the EUIPO. This paper is based on initial research from the Observatory, which was complemented by contributions from individual experts of the Observatory's expert groups on the 'Impact of Technology' and 'Cooperation with Intermediaries'. The Observatory welcomes any further input or comments on this discussion paper, to keep deepening its understanding of automated content recognition technologies and their potential implications on intellectual property. This discussion paper may be subject to reviews or updates, based on any further input from experts or new developments in the field.

ISBN 978-92-9156-280-0 doi: 10.2814/52085 TB-04-20-571-EN-N

Table of Contents

EXECUTIVE SUMMARY

This first phase of the analysis on automated content recognition (ACR) technologies shows that they are deployed for a very broad range of purposes, which go far beyond the protection or management of intellectual property (IP) rights. These technologies are central to a number of business and security applications and to address major societal challenges, such as the spread of terrorist or child abuse content online. This drives major improvements and innovation in the field of ACR, with technologies that are becoming more and more effective at recognising short extracts or elements of a piece of content.

Different ACR technologies support the recognition of content at different levels, with:

- **hashing** supporting the recognition of digital files;
- **watermarking** supporting the recognition of previously marked digital copies;
- **fingerprinting** supporting the recognition of an extract of a piece of content; or
- **AI-based or enhanced solutions** supporting the recognition of specific features or elements of a piece of content.

These technologies all have their advantages and limitations, which may vary from one form of content to another. The greatest technical challenge with the development and deployment of ACR solutions lies in finding the right balance between:

- their **accuracy** to recognise content, and **robustness** to resist content alteration; and
- the **data storage and computational resources** needed to implement them.

The use of the most accurate and robust ACR technologies, such as fingerprinting or AI-based or enhanced solutions, requires significant computational power and investment. A growing number of companies are developing solutions facilitating the use of such technologies for a broad range of use cases.

A combination of different ACR technologies can contribute to optimise the resources needed to recognise content. For example, AI-based or enhanced solutions can be used to recognise illegal content. The files containing such content, and that are identified through this resource-intensive solution, are subsequently hashed for all identical files to be detected. Since hashing is a less resource-intensive method, this helps to reduce the resources. Different ACR technologies are already combined in this way, with the potential to improve content recognition while reducing the resources required.

Phase 2 of this discussion paper will explore the development and complementary uses of ACR technologies, with five use cases of such technologies to support the protection or management of IP. It should be finalised by the 2nd quarter of 2021.This should contribute to a better understanding of the current and potential impact of ACR technologies on IP.

1. INTRODUCTION

The capacity of computers to recognise content is central to some of the new developments in the fields of digital media, e-commerce or cloud computing. Computers are increasingly used to recognise and moderate illegal or harmful content online, to automatically classify content stored in the cloud, or to analyse brand awareness and sentiment by recognising pictures of products posted on social media. It is also central to the development of robotics or self-driving vehicles that depend on the capacity of computers to recognise, learn and respond to their environment. This drives major innovations in ACR technologies, with a number of technology companies developing solutions and making large-scale investments in that field.

Just like most other technological developments, ACR has an impact on IP, with different technologies already in use to better protect or manage IP. This is especially the case with ACR solutions used to identify listings for counterfeit products in e-commerce marketplaces, or to monetise the use of copyright-protected content on video-sharing platforms. The impact of these technologies on IP is likely to increase as ACR solutions keep improving and being deployed for different purposes.

1.1 Objective

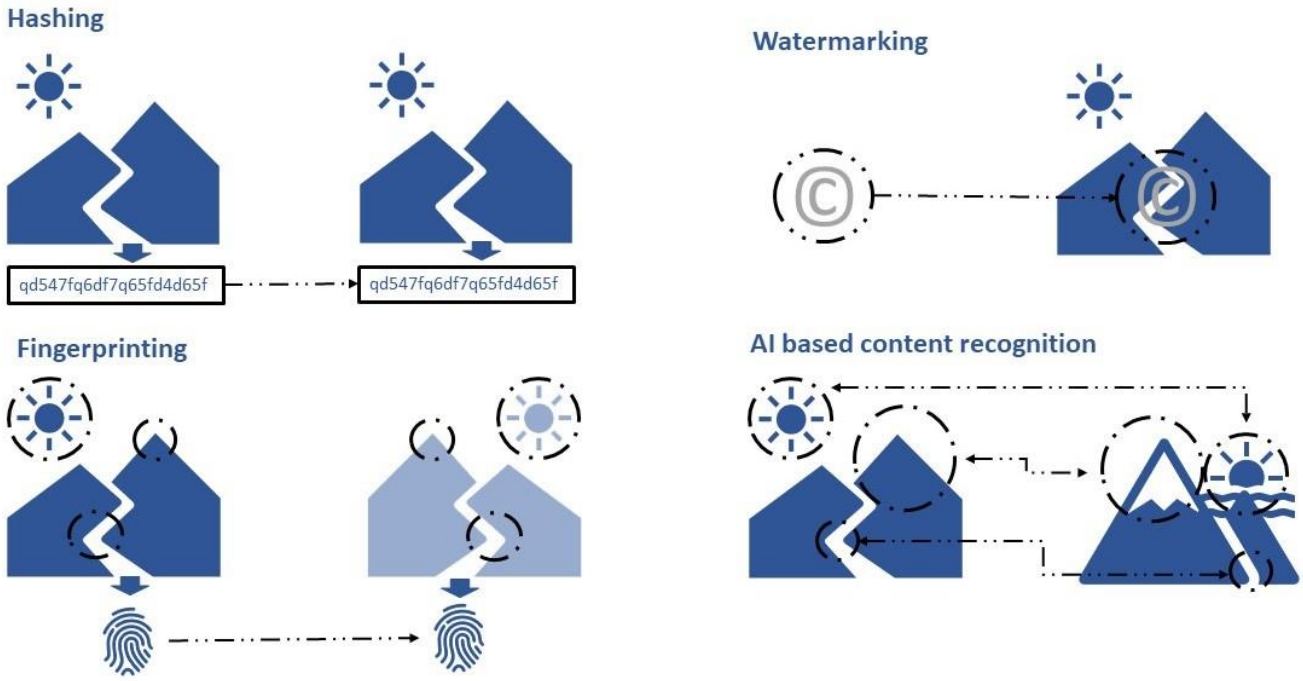
The objective of this discussion paper is to better understand ACR technology's current and potential impact on IP, following a two-step analysis:

- **Phase 1**: mapping and describing the different ACR technologies, with concrete examples of how they are currently used, and their respective advantages and limitations. The objective is to explore a broad range of use cases to get a better understanding of how ACR technologies are currently deployed and how they may develop in the future.

- **Phase 2**: will be a more focused analysis on the current and potential impact of ACR technologies to protect and manage IP rights, looking into the potential of respective technologies and their combination in that field. The phase 2 analysis is expected for the 2nd quarter of 2021.

1.2 Definition

If there is no agreed definition of ACR, technologies such as hashing, watermarking and fingerprinting are normally covered by reports looking into ACR technologies. This discussion paper also looks into artificial intelligence (AI) based or enhanced content recognition solutions. If such technologies are still developing and do not strictly fall into the scope of most definitions of ACR technology, they have a clear potential to improve content recognition directly or by complementing other ACR technologies. Hence, this first phase of the analysis explores the capacity of **Hashing (Section 1), Watermarking (Section 2), Fingerprinting (Section 3)**, but also the use of **AI-based or enhanced solutions (Section 4)** to support the recognition of different types of content.



It provides an overview of ACR technologies and of their uses, listing a series of services to provide concrete examples (1).

It also looks into the advantages and limitations of different technologies, taking into consideration a set of criteria such as:

- **Resources**: required to implement and run the technology. This includes computational, energy, network, data storage and software resources.
- **Technical implementation**: needed to integrate the ACR technology into an information system / workflow, including the need to set up a reference database or mark individually each digital copy of the content to be identified.
- **Accuracy**: describes how the technology performs in terms of matching output and performing correct identifications or false negative/positive results.
- **Robustness**: describes the capacity of a technology to resist modification of degradation of the content to be recognised.
- **Upgrade capability**: describes whether a technology can be upgraded to a more performant version and what the consequences of such an upgrade are. It especially looks into the effects of the upgrade in term or resources, technical implementation and the capability for the upgraded version to keep recognising content covered by the earlier version.

It is important to note the limitations of the analysis led in the context of this discussion paper. Information on different ACR technologies, especially with regard to resources and the costs needed to implement them, as well as their accuracy, robustness and capacity to be upgraded is very limited. In addition, most

(1) The services listed in this discussion paper are only included to provide concrete examples of ACR use to recognise different types of content. The inclusion of a specific service can in no way be construed as a form of endorsement or recognition of the quality of this service.

ACR solutions are developed to work with a specific type of content or platforms, with very different implementations of the same ACR technology. This further limits a comparison between the advantages and limitations of different categories of ACR technologies.

2. HASHING

Hashing is a generic term used to describe the process of running a digital file through a hashing function (i.e. an algorithm) to generate a unique identifier for this file in the form of a short string of characters (a 'hash'). This process cannot be reversed, therefore it is not possible to recover the original file from a hash. The newly generated string of characters is assigned to the file, as its unique identifier. If the exact same file is run through the same hash function it will return the same unique identifier.

Hashing is used for multiple purposes, including indexing content or securing passwords. In the field of content recognition, there are different types of hashing and hashing functions with different degrees of sophistication. This section only refers to cryptographic hashing, which is mainly used for indexing purposes, with the hashing function only allowing for the detection of the exact same file ([2]).

The process has two separate phases: **generation** and **comparison** of hashes.

- **Generation of a hash**: the use of a hashing function to assign a file a unique string of characters, that is much smaller than the size of the file and is stored in a reference database.

- **Comparison of hashes**: running any new or unknown file through the exact same hashing functions, and comparing the newly generated hash with the hashes stored in a reference database. If there is a match, the unknown file is considered to be exactly the same as the one in the reference database.

The added value of hashing is that it limits the amount of information that needs to be stored in the reference database and the computational power needed to compare files.

Cryptographic hashing can be used to detect all types of files, including files containing text, image, audio or video content. It appears to be well-suited when analysing hosted content rather than 'on the fly' content ([3]). It is often used by content-sharing platforms, where content is openly accessible and not individually encrypted. If it can be used in end-to-end encrypted communication environments ([4]), cryptographic hashing techniques are mostly successful in recognising content that is not encrypted. Cryptographic hashing techniques also support the recognition of compressed content, when the original format of the compressed content is known. The limitation of hashing for content recognition is that it only recognises a file as opposed to its actual content.

2.1 Use of hashing for 'content recognition'

Hashing is used for a number of 'content recognition' purposes.

- **Blocking terrorist content across different platforms**: the EU Internet Forum, initiated by the European Commission, created the 'database of hashes' of known terrorist content in December 2017 ([5]). With this database online platforms, such as Facebook, Microsoft, Twitter and YouTube, are sharing hashes of files containing images or videos they identified as

([2]) Another form of hashing is 'perceptual hashing' that can establish a match between hashes, even if they are not entirely the same, and is covered in Section 3 on Fingerprinting (see p. 14).
([3]) Content file that is transferred / in transit from one server to another.
([4]) See: 'Content Moderation for End-to-End Encrypted Messaging', Mayer, 2019, Princeton University.
([5]) See: 'Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda', European Commission, 2017.

promoting terrorism. Other platforms can use these hashes to identify and remove the exact same files from their services.

- **Detecting malicious files and viruses**: hashing is also used to detect malicious files or viruses ([6]). There are many examples and service providers in this field, such as VirusTotal ([7]) or Kaspersky Online File Reputation ([8]). Hashing is also used to prevent malicious files from being shared in the cloud with services such as OPSWAT's MetaDefender Cloud API, which provides cloud security using previously collected hash records of malware ([9]). Some services, such as cloud storage and app stores, are also using antivirus scanning to detect malicious files in software made available on their services ([10]).

- **Ensuring that a file that has been notified as infringing copyright is not shared in cloud-storage services**: some cloud-storage services are using hashing to identify and prevent the sharing of files that have been taken down for copyright infringement. This is notably the case of Dropbox ([11]) or Google Drive ([12]).

- **Ensuring that a file taken down is not re-uploaded**: YouTube is also using hashing to prevent the repeated uploading of files ([13]) that have been subject to a copyright infringement notice, and that the rights holder does not want to submit using its Content ID system (see p. 18). Dailymotion is also using cryptographic hashing technology provided by a third party ([14]).

2.2 Advantages and limitations

- **Resources**: if different hashing techniques and algorithms require different amounts of computational power, hashing requires relatively less computational and data storage capacities than other ACR technologies. A hashing reference database only stores a short string of characters as opposed to the entire file. Hashing also requires limited investment, as many open-source solutions are available.

- **Technical implementation**: hashing is relatively easy to implement. Any existing file can be hashed, with its hash included in a reference database. It can support the detection of already existing files and can be applied to legacy content / files ([15]). Running the hashing function on all the files stored in a system or server allows for the detection of any duplicates of the hashed files.

- As shown with initiatives such as the 'database of hashes' (see p. 4), the reference database can receive input and be used by different players using the same hashing function. This supports the development of collaborative initiatives in the identification of files containing illegal content, without having to share the illegal content itself.

([6]) Hashing is considered an effective technique for antivirus scanners. See, notably: 'Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey', Rad, Masrom and Ibrahim, 2011.
([7]) See: VirusTotal Hunting.
([8]) See: Kaspersky Online File Reputation.
([9]) See MetaDefender Cloud API on Opswat website.
([10]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 25.
([11]) See: How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff), Techcrunch, 2013.
([12]) See: Google contribution to U.S. Copyright Office study on Section 512, 2017, p. 15.
([13]) See: 'The Dilemma of False Positives: Making Content ID Algorithms more Conducive to Fostering Innovative Fair Use in Music Creation', Lester, T., Pachamanova, D., 2017, Chap. IV in *UCLA Entertainment Law Review*, 24(1). See also: 'Regulating disinformation with artificial intelligence', European Parliament Research Service, March 2019, p. 42.
([14]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward (January 2020), p. 26.
([15]) Unlike watermarking, which can only recognise content that has been previously marked.

- **Accuracy**: hashing can accurately identify exact duplicates of a digital file. However, as the reference database grows, so does the risk of 'hash collisions' ([16]), that is, the risk that two different files run through the same hashing function return the same unique identifier and are matched as identical, resulting in a false positive ([17]) ([18]). Another issue is the risk of 'bucket overflows', that is, the risk for the reference database to reach its limit for accepting new entries ([19]). This problem can be overcome using 'dynamic hashing' techniques ([20]), which involves dynamically inserting and redistributing hashes that share similar characteristics into the same buckets. Cryptographic hashing accuracy is also limited when content is encrypted.

- **Robustness**: the slightest edit of the hashed file makes it impossible for it to be recognised, so hashing recognition does not resist any format shifting, compression or alteration of a file. More robust hashes are able to 'resist certain type and/or number of data manipulations' ([21]). As an example, 'fuzzy hashing' allows a similarity-based comparison of hashes and is widely used in malware analysis ([22]).

- **Upgrade capability**: cryptographic hashing functions are widely used in the field of security, and a hashing function may need to be changed or upgraded if it is vulnerable to a 'hash collision attack'. This vulnerability may be used to deceive a system into accepting a malicious file as a 'benign counterpart' to bypass security measures ([23]). However, such an attack will have no purpose when the hashing function is used to identify files containing illegal content, as it will only result in a file being identified as containing illegal content.

  The challenge if a hashing function needs to be upgraded, is that the reference database that only contains hashes (as opposed to actual files) only works with a specific hash function and cannot be upgraded. If the storing of hashes (as opposed to actual files) limits the amount of data stored in the reference database, it undermines the possibility for hashing functions to be upgraded. This can be a major challenge if the files corresponding to the hashes have not been stored, or when the reference database has multiple contributors.

- **Capacity to be used in conjunction with / to complement other technologies:** Since it requires limited resources, cryptographic hashing is used to complement more resource-intensive ACR technologies and, notably:

  - **Fingerprinting**: this is the case with YouTube using Content ID fingerprinting technology to identify content stored in its fingerprint reference database (see p. 7). Once a specific file has been identified by Content ID and taken down, hashing is used to prevent the exact same file from being repeatedly uploaded. In this case cryptographic hashing is used as a 'first line of defence' to limit the use of the more resource-intensive fingerprinting technology.

  - **AI-based or enhanced content recognition**: AI can be used as an online moderation tool to detect inappropriate or illegal content (see p. **Error! Bookmark not defined.**) ([24]).

([16]) See: Hash Collision Attack on Learncryptography for an explanation.
([17]) See: 'Searchable Storage in Cloud Computing', Yu Hua and Xue Liu, 2019, in *Springer Nature Singapore Pte Ltd.* p. 108, ISBN 978-981-13-2721-6.
([18]) Hash collision has been demonstrated on several occasion for MD5 and SHA-1 algorithms. However, more complex SHA-256 and SHA-512 algorithms are still considered secure and recommended for cryptographic purposes.
([19]) See: Javapoint's explanation of static hashing.
([20]) See: Javapoint's explanation of dynamic hashing.
([21]) See: 'Robust Hashing for Models', Martinez, Gerard and Cabot, p. 2, in *MODELS '18 Proceedings of the 21th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems*, pp. 312-322.
([22]) For further information, see: Carnegie Mellon University blogs on Fuzzy Hashing Techniques in Applied Malware Analysis; technical insight on ssdeep Project.
([23]) See: Google Security Blog on Announcing the first SHA1 collision (2017).
([24]) See Cambridge Consultants' report on Use of AI in online content moderation, July 2019, p. 6 and Chap. 4.1.1.

Once inappropriate content has been identified this way, the related file can be hashed to remove other instances of the same file and prevent it being re-uploaded in the same or other systems.

3. WATERMARKING

Watermarking is adding information and embedding it directly into a product, a signal or a digital file. To some extent, '[…] it can be viewed as a communication system: the watermark is the signal carrying useful information […]' ([25]).

In the field of ACR technology, watermarking is used to identify digital media or files, with perceptible or imperceptible changes applied to the content or file. The watermarking process typically has two separate phases: **marking** and **identification** of the watermark.

- **Marking** is applying the watermark to the content. This can be a generic watermark applied to all the digital copies of a piece of content, or an individual watermark that is specific to each distributed copy.

- **Identification** of the watermark, which may be as straightforward as someone reading a visual watermark appearing on a piece of content, or requires the use of watermark detection software to identify digital watermarks that have been 'hidden' in the digital content.

Watermarking applies to text, image, video and audio content. Since the information is embedded directly into the content, there is no need for the original content, as a reference to carry out the comparison. However, watermarking can only support the detection of content that has effectively been previously marked. Inserting individual watermarks into every digital copy of a work, as well as handling the distribution of these individually marked copies, can require significant resources.

There are different types of watermarking:

- **'Visible watermarking**' as opposed to '**invisible watermarking**': in 'visible digital watermarking, the embedded information is visible […]' — for example, a TV logo embedded into the program's video — while in the latter case, '[…] information is added as digital data to audio, picture, or video, but it is not visible' ([26]).

- **'Forensic or digital watermarking'**: this type of invisible watermarking is encoding information into digital content, without distorting the content itself. An example of digital watermarking is modifying the colour intensity of selected pixels without modifying the content. This information can only be detected and decoded through specific algorithms ([27]), with watermarking technology providers offering tracking services' ([28]).

- '**Static watermarking**' as opposed to '**dynamic watermarking**': the former includes pre-determined information, usually a logo or a set of characters, fixed onto the content once published. The latter includes information in the content that is generated when it is being displayed. The information added through dynamic watermarking can be updated in real time,

([25]) For further information on watermarking of audio content, see 'Watermarking and Fingerprinting: For Which Applications?', Cano et al., 2003.
([26]) For more information on reversible watermarking in copyright protection, see, 'Copyright Protection using Digital Watermarking', Jose et al., *NCACSA* 2012, p. 24.
([27]) See: DigitalWatermarkingAlliance website.
([28]) See: White Paper: Video watermarking and fingerprinting, Dominic Milano. p. 4.

making the watermarked digital file unique and easily identifiable ([29]). Companies such as Civolution provide forensic dynamic watermarking solutions ([30]).

- '**Reversible watermarking**': a watermark is reversible when it is possible to reverse the process, by removing the watermark and re-establishing the initial state of the content ([31]). This technique is used in copyright-protected media identification to restore the quality of content when an invisible digital watermark has been applied ([32]). A service such as Digimarc provides the reversible watermarking of images for copyright purposes ([33]).

- **'Software watermarking'**: this is a technique developed to undermine software piracy by embedding a digital signal into software ([34]). For example, IBM is developing systems to verify the ownership of AI-based deep neural networks ([35]).

- **'Hardware watermarking'**: this is the process of embedding hidden marks as design features or attributes inside a hardware or IP core ([36]) and requires highly sophisticated mechanisms to implant a mark within the design without altering the functionality of the device. For example, watermarking chips can be integrated into a digital camera or any other multimedia device, so the sounds ([37]) and/or images are watermarked directly when they are captured ([38]).

3.1 Use of watermarking

Watermarking is used in multiple ways with different companies providing solutions in that field ([39]), including:

- **Adding information related to rights or rights holders**: watermarks are used to protect IP rights by including information related to the rights and their owners directly in the content (e.g. a logo, the name of the rights holder or an email address). It provides evidence of the existence of IP rights. There are a number of services in this field, such as EditionGuard ([40]), Logaster ([41]) or SnapRetail ([42]). A number of applications are also developed to watermark content on mobile devices, such as eZy Watermark ([43]) or PhotoMarks ([44]).

- **Adding information related to the content user**: watermarking can be used to embed information related to the user accessing or displaying the content. Watermarks are notably used by the music and film sectors to identify the source of pirated content. This has long been the case with individual watermarks on films displayed in theatres to identify the origin

([29]) See information on dynamic watermarking on SmartFrame website.
([30]) See information on the automated use of forensic watermarking on IBM Aspera web page.
([31]) Khan et al., A recent survey of reversible watermarking techniques in *Information Sciences* Volume 279, 2014, pp. 251-272.
([32]) For more information see: 'Copyright Protection using Digital Watermarking', Jose et al., *NCACSA* 2012, p. 24.
([33]) Lipinski, 'Watermarking software in practical applications' in *Bulletin of the Polish Academy of Sciences*, Technical Sciences, 2011, p. 23.
([34]) M. D. Preda, M. Pasqua, Software Watermarking: A Semantics-based Approach, 2017.
([35]) See 'Protecting the Intellectual Property of AI with Watermarking', 2018.
([36]) A reusable building block or integrated circuit of an electronic design which is already IP protected. The typical IP cores are hard cores, film cores and soft cores.
([37]) Jung-Hee Seo, Hung-Bog Park 'Hardware Based Real Time Audio Watermarking Using Embedded Module' in *Journal of Next Generation Information Technology* 4(5):1-8, July 2013.
([38]) Among others, see: S. P. Mohanty, A. Sengupta et. al., Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection, 2017.
([39]) This analysis focuses on digital watermarking and leaves aside analogue watermark methods consisting of embedding perceptible watermarks into products.
([40]) See EditionGuard's release on 'Watermarks for Your Digital Content: The 'How To', 2018.
([41]) See Logaster's release on 'How to create a logo and use it as a watermark', 2018.
([42]) See Snapretail's release on 'How to Watermark Your Photos for Pinterest', 2017.
([43]) See eZy Watermark web page.
([44]) See Photomarksapp web page.

of copies made with camcorders ([45]). It is also used in the pre-release distribution of music or films for promotional purposes. Each and every pre-released copy is individually watermarked, which acts as a deterrent for illegal distribution and facilitates the detection of the source if it does happen. Watermarking can also help to identify user accounts used as sources for illegal broadcasts of content, e.g. content provided by pay-TV operators offering premium video on demand (VOD) and live sports services ([46]).

- **Including information related to the content distribution network**: watermarking can be used to identify the network that distributes or broadcasts the content. A 'Network-ID' is added to the content for each broadcaster / distributor. As an example, BeIN Sports watermarks all its video streams. A watermark detector implemented on streaming platforms can help to detect potentially illegal streams of BeIN Sports programs regardless of the content or the individual recipient / source ([47]).

  Companies active in the field of detection of illegal content distribution are typically providing audio and video watermarking services, as well as investigative services to detect and identify the source of illegal copies. Examples of such services are ContentArmor ([48]), Irdeto ([49]), NAGRA ([50]) or Verimatrix ([51]).

  NAGRA is also providing conditional access systems for satellite and digital cable TV, which have put in place agreements with several access providers. It has also struck agreements with rights holders of audiovisual content ([52]) and it is leveraging its watermarking technology to perform content recognition on a large scale, including the identification and tracking of individual copies of premium content distributed through VOD services.

  Similarly, ContentArmor has an agreement with Viaccess-Orca, a provider of content-sharing solutions ([53]), to allow content filtering in conditional access systems – such as the VOD services provided by Orange France ([54]). Similar solutions have also been developed by the conditional access systems provider Irdeto, which allows content filtering on internet protocol TV (IPTV), mobile TV and digital content-sharing systems thanks to its proprietary watermarking recognition technology ([55]).

  The publishing sector is also using watermarks on individual copies of e-books and audio books through the use of services like SitMark developed by Fraunhofer ([56]) or the EU-funded Legimi service ([57]). 'Techniques used to embed invisible watermarks in e-books include things like embedding hidden data in illustrations, algorithmically altering content other than the actual substance of the book (such as text on a copyright page, index, or page header/footer), inserting non-printing characters, and using identifiers as input to kerning algorithms (for computing the spacing of characters in a line of text)' ([58]). An example of this kind of watermarking solution is Custos, whose watermark detection solutions are available

([45]) See Businesswire's release on 'Dolby Incorporates Philips Watermarking Technology for Digital Cinema', 2007.
([46]) Examples are NAGRA's watermarking technology or Viaccess-Orca's watermarking technology.
([47]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 29.
([48]) Additional information on Contentarmor watermarking solution can be found on its website.
([49]) See Piracy Control service on Irdeto's website.
([50]) See NAGRA's watermarking technology on NAGRA's website.
([51]) See Verimatrix website.
([52]) An example is the Agreement with the International Broadcaster Coalition Against Piracy.
([53]) See Viaccess-Orca website.
([54]) See 'Viaccess-Orca Secures Content for New Ultra HD STB by Orange France', 2016.
([55]) See Piracy Control service on Irdeto's website.
([56]) For more information see 'SITMark AUDIO »YOU CAN'T HEAR IT, BUT IT'S THERE!'
([57]) See Legimi website.
([58]) See 'A bounty hunting service for e-books piracy', 2017.

online for 'bounty hunters' to identify and report illegal copies of copyright-protected content ([59]).

- **Content synchronisation**: watermarks can be used to identify the content displayed on a user's device (TV set, tablet or mobile) and deliver 'complementary and fully synchronized content associated with the program, film or advertisement' ([60]). This allows for the provision of additional content-related information, targeted advertising, interactivity and audience measurement. An example of such a service is SyncNow ([61]), an audio watermarking technology provided by Kantar Media to detect audiovisual content.

- **Individual identification of 3D designs**: a key challenge in the field of 3D design is design attribution. Ensuring the origin of a 3D design and detecting infringement is possible by watermarking the STL file ([62]) – a type of file storing information about 3D models and used to transfer that information to a 3D printer. An example of a company active in this field is Treatstock with its Watermark3d ([63]). However, some 3D printing file formats do not allow the placement of watermarks ([64]).

3.2 Advantages and limitations

- **Resources**: recognising previously watermarked content requires less computational resources than fingerprinting, as it consists of recognising information embedded into the content itself with no need for a reference database. However, '[w]atermarking systems and techniques are not generic or standardised, and a watermark generated by one technology cannot be read by a system using a different technology' ([65]).

- **Technical implementation**: ACR watermark software is needed to detect the watermark, which can be implemented at network, server or device level. If there is no need for a reference database, inserting individual watermarks in every copy of a piece of work (including in copies that are livestreamed) and handling the distribution of these copies requires significant resources.

- **Accuracy**: digital watermarking technology achieves a high level of accuracy for the purposes of content identification and source tracing. However, accuracy in watermark detection – and, consequently, in content recognition – may be compromised if the watermarking protection is circumvented (by, for example, watermark removal or blurring). Video encoding can also affect accuracy in audiovisual content identification, for example, if the file is compressed to a lower bit rate ([66]) or using different methods such as discarding some of the content's data in order to reduce its size.

- **Robustness**: the robustness of watermark techniques vary from one type of content to another, as well as from one watermarking technology and / or service to another. 'Watermarks can be configured in such a way that they are robust against alterations of their carrier medium […] such [as] format changes, analogue-digital-conversion, scaling or cropping' ([67]). As for images, '[many] current digital watermarking methods embed codes so

([59]) See 'What is Forensic watermarking? Combined with blockchain it is revolutionizing DRM', Custos, 2019.
([60]) Civolution white paper on 'Automated Content Recognition: creating content aware ecosystems', 2013.
([61]) Additional information on Kantar's Synchronised Content Technology can be found on KantarMedia website.
([62]) For an explanation on STL format, 'STL File Format (3D Printing) — Simply Explained', 2019.
([63]) See Watermark3d web page.
([64]) See European Commission, Study on 'The Intellectual property implications of the development of industrial 3D printing', carried out by Bournemouth University and Technopolisj, April 2020.
([65]) *Ibid.* p. 3.
([66]) Described as the number of bits processed per second and determines the size and quality of video and audio files.
([67]) Digital Watermarking – Protecting digital media data, Fraunhofer SIT.

that image can be altered (transcoded, cropped, scaled, etc.) without losing the ability to extract the watermark. […] Many techniques are similar to those used in compression technologies. The watermark ends up as very subtle colour variations in the final image' ([68]). It is important to note that when all content is watermarked in the same way, it is becoming easier to detect the marks. Therefore, some of the systems applying watermarks on a large scale use different marks that can only be detected by the recognition tool ([69]). Another possibility is to apply multiple watermarking techniques to the same content.

Watermarks with a low degree of robustness are typically disappearing when some kind of processing of the marked file or media occurs – for example, when the content is compressed or rotated ([70]). Perceptible visual watermarks are usually more fragile and it has been demonstrated that they can be removed automatically using specific computer algorithms ([71]). With regard to audio-content protection, watermarks are normally resistant to malicious attacks. However, in some cases 'the watermark must no longer be recognised when the audio content is modified in any way' ([72]).

Several techniques to circumvent watermark protection of images or videos exist, some of them using perfectly licit software or online services:

- blurring the watermark ([73]);
- removing or replacing the watermark ([74]);
- changing the output format of a file (i.e. converting the file) ([75]);
- editing or cropping the image ([76]).

A more advanced way to circumvent watermark protection is the so-called subterfuge attack or attack by collusion ([77]). It consists of creating a new copy of the content by merging or overlaying different marked copies to make the watermark unreadable.

A number of online services and offline software solutions exist to support or facilitate the removal of watermarks from digital content. For example, Inpaint ([78]), Paint.net ([79]) Pixlr ([80]), and Watermarkremover ([81]) for online use or Erase Watermark ([82]) for mobile applications. It is also possible to detect and remove watermarks using deep learning technologies ([83]).

- **Upgrade capability**: since watermarking implies embedding data or information into a media file, a new, more robust or accurate watermark can only be applied to new content. The challenge is to maintain and run concurrently new and legacy watermark detection solutions.

([68]) *Ibid*, p. 3.
([69]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward (January 2020), p. 30.
([70]) Lian, 'Multimedia Encryption and Watermarking in Wireless Environment' in *Handbook of Research on Wireless Security*, Information Science Reference (an imprint of IGI Global), Hershey (2008), Chap. XVI, p. 239.
([71]) See Google AI Blog on 'Making Visible Watermarks More Effective' (2017).
([72]) See 'Watermarking and Fingerprinting: For Which Applications?' Cano et al., 2003, p. 4.
([73]) See '100% Working Guide of Removing Watermark from Video on Windows and Mac' (2019).
([74]) See 'How To Remove a Watermark From a Photo' (2019).
([75]) See 'How to Remove Watermark from Videos [7 Proven Solutions]' (2019).
([76]) See 'Simple Ways to Delete Watermark from Video' (2019).
([77]) For additional technical information on the topic see: 'Survey on Digital Video Watermarking Techniques and Attacks on Watermarks', Jayamalar and Radha, *in International Journal of Engineering Science and Technology*, Vol. 2(12), 2010, p. 6963.
([78]) See Theinpaint online page.
([79]) See Getpaint web page.
([80]) See Pixrl web page.
([81]) See Apowersoft website.
([82]) See Photo Eraser web page.
([83]) For more information see: Cheng, Danni & Li, Xiang & Li, Wei-Hong & Lu, Chan & Li, Fake & Zhao, Hua & Zheng, Wei-Shi, 'Large-Scale Visible Watermark Detection and Removal with Deep Convolutional Networks: First Chinese Conference', PRCV 2018, Guangzhou, China, November 23-26, 2018, Proceedings, Part III. 10.1007/978-3-030-03338-5_3.

- **Capacity to be used in conjunction with or complement other technologies**

  - **Fingerprinting**: some companies are combining watermarking and fingerprinting technologies. The first is used to embed metadata within content while the latter creates fingerprints of visual features in order to facilitate the recognition of similar content. Lamark and Imatag technologies use such a combination for image recognition purposes ([84]).

  - **AI-based or enhanced content recognition**: AI can be used as a tool to improve watermark detection and identification of copyright-protected content. This is the case with Restb technology, which uses AI to recognise watermarked content on services hosting user-generated content and to limit 'the threat of legal action by preventing photos with copyrights from ever being uploaded to [a web]site' ([85]). Restb is mainly used by real estate websites.

  - **Cryptocurrency**: some companies are making creative use of watermarking to create an incentive ('bounty hunting') system so any user can help find the source of the possible leak of a pre-released copy of a movie or e-book. This is the case of Custos, which is using forensic watermarking to include the number of a bitcoin wallet with a bit of bitcoin in copies sent to each reviewer. 'Anyone in the world that finds a copy in the wild can take this bitcoin as their reward, and through the blockchain [Custos is] informed whose copy was found somewhere it should not have been.' ([86])

4. FINGERPRINTING

Unlike watermarking, fingerprinting does not add any information to the content, but analyses it to identify some of its unique inherent properties. Fingerprinting is very similar to hashing ([87]). The main difference is that instead of generating a string of characters based on a digital file's characteristics, fingerprints are generated based on the characteristics of the actual content of that file. Just like hashing, the fingerprinting process has two separate phases: **generation** and **comparison** of fingerprints ([88]).

- **Generation of fingerprints** uses software to:
  - analyse and extract recognisable features and other information from the content;
  - generate a string of values describing the extracted features and information (the fingerprint);
  - store the generated fingerprints in a reference database.

- **Comparison of fingerprints** uses software to analyse each and every new or unknown item of content and generate a fingerprint. The generated fingerprint is compared with all the fingerprints stored in the reference database to see if there is a match. Depending on the fingerprinting technology used, if the unknown content differs slightly or strongly from the reference content, there will not be a match.

Just like hashing, fingerprinting limits the amount of data that needs to be stored in the reference database and that needs to be compared. This significantly reduces the data storage and computational power needed to compare two pieces of content.

([84]) See Lamark web page.
([85]) Information about Restb services can be found on its website.
([86]) Information on this specific service can be found on Custostech website.
([87]) The terms hash and fingerprints are used interchangeably in many articles on ACR technologies.
([88]) For an explanation on how fingerprinting works see the presentation of the INA signature technology provided by Boris Jamet-Fournier (INA) at the 2019 FIAT/IFTA World Conference in Dubrovnik.

Fingerprinting can be used to identify images, video or audio content, with a high level of accuracy, even if the content has been altered or modified (e.g. an image that has been blurred or the recording of a movie from a TV screen). 'The most advanced tools can even recognise a melody in a cover version by another performer' ([89]). Different approaches can be used for different types of content:

- with **text fingerprinting**: words are extracted from a whole text in order to generate a fingerprint; this may be achieved by selecting specific words, by using algorithms to sort words following a specific pattern or simply by assuming the raw text ([90]) as a fingerprint of the document;

- with **image fingerprinting**: the unique spatial characteristics of an image can be analysed to identify specific areas or points of that image, as these will not change even if the image is rescaled, reoriented, distorted or the brightness is changed;

- with **audio fingerprinting**: statistical samples of an audio piece can be extracted to provide a unique pattern for the fingerprint; '[f]or example, four samples [can] be taken every 10th of a second. […] If the source file is a two minute song, there would be over 4,000 samples in the fingerprint, but the actual fingerprint file would still be a thousand times smaller than the audio file. […] Any other piece of music would have a different pattern of sample' ([91]);

- with **video fingerprinting**: a statistical sample of the content is also extracted to generate a fingerprint of the whole audiovisual content or just a part of it; '[a] video fingerprint can be a global description of the video (number of scene cuts, size of the video, etc.), a set of image fingerprints of still video frames, a set of video key frames or the description of the motion vectors' ([92]).

The examples above are meant to illustrate how fingerprinting techniques may apply to different types of content, but far more complex techniques are used to randomly sample spatial and temporal features of content, and make them harder to circumvent. The more elements that are extracted, the more accurate and robust the fingerprinting solution is, but also the more data needs to be stored in the reference database, and the more computational power is needed to compare the fingerprints.

Another layer of complexity is the use of perceptual hashing ([93]). This fingerprinting technique must not be confused with cryptographic hashing ([94]). Fingerprints are typically made of a string of values (so-called hashes), and recognition occurs when the hash of the already identified content matches exactly with the hash of the unknown content. With perceptual hashing the fingerprinting algorithm is able to generate and, subsequently, recognise 'perceptually similar' content. A match will occur even if the compared strings of values are not exactly the same ([95]).

([89]) *Ibid.* p. 18.
([90]) In computing, raw or plain text indicates any group of alphanumeric characters, not their graphical representation nor other objects.
([91]) See: White Paper: Video watermarking and fingerprinting, Dominic Milano. p. 6.
([92]) See: Lefebvre, Chupeau, Massoudi and Eric Diehl 'Image and video fingerprinting: forensic applications', Proc. SPIE 7254, *Media Forensics and Security*, 725405 (February 2009), p. 2.
([93]) For more information see: R. Muthu and C. Rani, 'Perceptual hashing for efficient fingerprint based identification', *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, 2017, pp. 1-6. doi: 10.1109/ICACCS.2017.8014713.
([94]) As already explained, 'hashing' is a term used to describe the generation of a string of values assigned to a file. The main difference between cryptographic hashing and fingerprinting is that hashing allows the identification of a file, while fingerprinting allows the identification of its content.
([95]) If the content is scaled or rotated, for example, it will still be perceived as similar by the algorithm. Similarity is measured using the so-called hamming distance metric.

4.1 Use of fingerprinting

Fingerprinting is used for a broad range of purposes:

- **Data loss prevention**: some companies use text fingerprinting as a way to ensure the integrity of sensitive documents. An example of such use is provided by Microsoft 365 ([96]).

- **Second screen synchronisation and content verification**: similar to watermarking, fingerprinting solutions are used to identify content that is being played on a TV set and synchronise it with content on the same or a second screen (e.g. a tablet or a mobile phone). This enhances the television viewing experience by enabling viewers to interact or access related information, social media, advertisements or brand information. Companies such as ACRCloud ([97]) or Mufin ([98]) are providing these kinds of fingerprint-based services.

- **Audience measurement and analysis**: for broadcast media, such as television or radio, there is no direct method to know what the audience is watching or listening to. Fingerprinting solutions can address this issue. For examples, the solution of KANTAR ([99]) or Samba TV ([100]) are used to help broadcasters understand viewing habits better and how to improve audience targeting. The benefits of these kinds of solutions include accurate pricing for advertisements and measurable promotional efforts.

- **Content moderation and prevention of the distribution of child exploitation content**: fingerprinting technology is used to 'flag' and identify illicit content for content moderation purposes. An example is PhotoDNA technology, originally developed by Microsoft and now available on Microsoft's cloud service Azure, which leverages perceptual hashing technology to help stop the sharing of images of child exploitation ([101]). Such content moderation applications are made more difficult in end-to-end encrypted communication systems. Projects for advanced fingerprinting technologies are being developed to address this issue ([102]).

- **Enforcing and managing copyright**: fingerprinting is used by content-sharing platforms to detect the use of copyright-protected content. Furthermore, it is used to apply specific policies defined by content rights holders, including blocking or monetising the use of their content.

  A number of companies are providing solutions in that field, as a service for content-sharing platforms, or as a proprietary solution applying to their own content-sharing services.

  - **Audible Magic** provides its audio identification solution to different video-sharing platforms. It is based on audio fingerprinting, which allows the identification of digital soundtracks and can be used to recognise audiovisual content ([103]).

    Fingerprints can be generated for free by Audible Magic itself and integrated into its reference database together with the metadata related to the content. It also provides its AMSigGen solution ([104]), so that rights holders can generate fingerprints themselves and send them to be

([96]) See Document Fingerprinting on Microsoft 365's compliance web page.
([97]) Information about this service can be found on ACRCloud website.
([98]) Mufin provides businesses with audio fingerprinting technology; additional information on the use of its technology and uses can be found on Mufin's website.
([99]) Information about this service can be found on Kantarmedia website.
([100]) For additional information see SambaTV's website on 'Automatic Content Recognition: Overview & Methodology (Part One)' (2017).
([101]) See: PhotoDNA dedicated web page on Microsoft website.
([102]) An example is the Robust Homomorphic Image Hashing algorithm, a project developed by Singh and Farid and supported by and developed with funding from Google, Microsoft Corporation and the US Defense Advanced Research Projects Agency.
([103]) See Comment Regarding Section 512 Study, Answer no. 15 (p. 49), issued in response to the questionnaire made by the United States Copyright Office in 2016.
([104]) See Audible Magic's support web page and on the section dedicated to AMSigGen.

added to the reference database. These solutions can be integrated directly into a rights holder's digital supply chain or used by third parties acting on their behalf. Audible Magic's solutions support rights management, with rights holders having the option to block, allow or monetise the use of their content ([105]). Through its AMLive service, Audible Magic provides a solution to prevent the real-time rebroadcasting of premium content by users of live streaming platforms ([106]). Audible Magic is used by different content-sharing platforms, including Facebook ([107]), Dailymotion, Twitch, Soundcloud ([108]) or TikTok.

- **INA Signature** is the solution developed by the French national audiovisual archives. Fingerprints are generated by INA after content 'registration' into its database ([109]), albeit at a cost for rights holders. The INA solution supports rights management, with rights holders choosing to allow, block or monetise the use of their content. INA Signature is used by the video content-sharing platform Dailymotion, as well as by IP protection services such as Markmonitor ([110]). The system is constantly upgraded in order to ensure full compatibility with older fingerprints ([111]).

- **YouTube Content ID** is based on audio and video fingerprinting, which can be used to recognise the audio and/or video part of content. Content ID performs content management and monetisation on the basis of an evaluation of the match between the content that has been claimed, fingerprinted and added to its reference database, and newly uploaded content on YouTube ([112]). Following a claim of ownership by rights holders, YouTube can generate the fingerprints directly from the copyrighted content. YouTube also provides a Content ID API ([113]), allowing rights holders to create a reference file themselves and add it to the reference database ([114]). However, for such fingerprints, the system cannot provide full retro-compatibility. As YouTube fingerprints' format is updated at least once a year, older fingerprints that were generated externally and that no longer offer optimal content protection are progressively deactivated. This is not the case for fingerprints generated directly by YouTube, as the actual audio or video files that have been uploaded in the YouTube system can be used to re-generate fingerprints every time a new fingerprint update is implemented ([115]). The system supports rights management, with the possibility for rights holders to decide if they want their content to be blocked, monitored or monetised ([116]). YouTube Content ID supports the fingerprinting and identification of live broadcasted content, also via dedicated APIs ([117]).

- **Facebook Rights Manager** allows rights holders to upload and maintain references of audio and videos or live video streams in the form of fingerprints ([118]). Fingerprints are generated directly by the rights holders using Rights Manager API ([119]). The rights holder can set his/her

([105]) See Comment Regarding Section 512 Study, Answer no. 15 (p. 53), issued in response to the questionnaire made by the United States Copyright Office in 2016.
([106]) See: Audible Magic Launches AMLive™ to Protect Against Rebroadcasting Premium Content by Users of Live Streaming Platforms, 2018.
([107]) Information on the Facebook web page 'What tools does Facebook provide to help me protect my intellectual property in my videos?'
([108]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 31.
([109]) Additional information on INA Signature for Rights Holders sheet release.
([110]) See: 'Le logiciel Ina-Signature honoré par un prestigieux 'Emmy Award for Technology and Engineering'', 2018.
([111]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 37.
([112]) Additional information can be found on the YouTube online support web page related to content management.
([113]) Additional information about Content ID API can be found on YouTube's website.
([114]) Additional information on What is reference on YouTube and how to Create references can be found on YouTube Help website.
([115]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 35.
([116]) Information can be found on How Content ID works web page.
([117]) Information can be found at the web page dedicated to Life of a broadcast.
([118]) Additional information on Rights Manager tool can be found on Facebook's web page dedicated to developers.
([119]) Additional information on Rights Manager API can be found on Facebook Developers website.

own content management policy, deciding if he/she prefers to block the content, monetise it or apply attribution ([120]), so that the system can take action in case of a match ([121]).

Other companies have developed open-source solutions. This is the case with Panako ([122]) and Acoustid ([123]).

In an attempt to address the complexity arising from the use by different services of different fingerprinting solutions, some vendors offer services to manage rights holders' content protection through these different solutions. This is the case of the one-stop shop solutions provided by Blue Efficience, that allows rights holders to manage multiple recognition tools through a single portal ([124]). The system, designed for ALPA members with the support of the '*Centre national du cinema et de l'image animée*' (CNC), is another example of a one-stop shop solution for the protection of content on video-sharing platforms using fingerprinting solutions ([125]).

Some companies are also using fingerprinting to monitor the use of copyright-protected content on different media for collecting societies. This is the case of BMAT ([126]) that works for SACEM, SGAE or PRS Music.

- **Fighting piracy**: some companies are specialised in the use of fingerprinting technologies to monitor video-sharing platforms and identify pirated copies of video content ([127]), even if the content has been modified or degraded. This is the case of Vobile ([128]) that also provides services to send takedown notices as well as of Videntifier ([129]), and Friends MTS ([130]), which are providing services to identify IP infringing video in real time. As for pictures, some companies are using fingerprinting and reverse image searches to detect the use of copyright-protected pictures online, to automatically generate takedown notices or to propose legal resolution. This is the case of companies like Pixsy ([131]) and TinEye ([132]).

- **Searching content**: fingerprinting technology is also used to recognise content based on sounds and/or images captured through mobile phones. The Shazam application ([133]) (that was acquired by Apple) allows song recognition, but also real-time lyrics synchronisation, providing users with information on where to purchase the song. Echo Nest provides similar technology ([134]). Content recognition can also be used to help users recreate their content collection when moving to a new content service provider. For example, Gracenote is powering Amazon, Netflix and Hulu to automatically recognise TV programmes and films to enable users to perform content searches ([135]).

- **Text plagiarism and software theft identification**: fingerprinting technologies are also used to identify text plagiarism. An example of such use of fingerprinting is the 'Plagiarism Detection

([120]) See Facebook's Help web page.
([121]) Information on Rights Manager's solution can be found on the Facebook for media dedicated web page.
([122]) See Panako website.
([123]) See Acoustid website.
([124]) See Blue Efficience website.
([125]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 38.
([126]) See Bmat website.
([127]) In this case the fingerprinting solutions are not implemented by the video-sharing platform itself.
([128]) Vobile is working with Netflix to help it protect its original content. For further information see Vobile website.
([129]) Additional information about service provided and technology can be found on Videntifier website;
([130]) See Friends MTS website.
([131]) See Pixsy website.
([132]) See TinEye website.
([133]) See Wang's paper 'An Industrial-Strength Audio Search Algorithm' (2003) and Shazam website.
([134]) See Echo Nest website.
([135]) See Gracenote website.

Technology' by Turnitin ([136]). Plagiarism recognition systems are also developed to deal with source code plagiarism and to provide evidence of theft ([137]).

4.2 Advantages and limitations

- **Resources**: as explained, the amount of data storage and computational resources needed to generate and match fingerprints may vary greatly depending on the number of unique features that are extracted from a content piece to generate the fingerprint. In general, fingerprinting requires more resources than hashing or watermarking, and the more complex and robust the fingerprints are, the more resources are needed to generate, store and verify them. Fingerprinting technologies may not always be utilised to the full extent of their performance and recognition capabilities when used by platforms or rights holders in production environments.

- **Technical implementation**: ACR fingerprinting software is needed to generate fingerprints – so-called reference files that are stored in a reference database – and to detect the fingerprints of the monitored content ([138]). Several proprietary solutions exist with some content platforms using their own solutions, and/or solutions developed by service providers.

- **Accuracy**: generally, fingerprinting techniques offer a high level of accuracy, as they overlook (false negative identification) and misidentify (false positive identification) a limited amount of content. Accuracy depends on the number of recognisable features that are extracted to generate the fingerprint. It can be undermined by a loss in the quality of the content to be identified or if it is altered ([139]). The level of accuracy also depends on the fingerprinting solution's capability to recognise short extracts and to automatically exclude irrelevant parts of the content when performing the recognition. In general, setting a too-high quality threshold for software recognition would result in a high level of false negatives for slightly altered content. On the contrary, if the threshold set is too low, the recognition tool might over-detect, resulting in a high level of false positives ([140]).

- **Robustness**: different fingerprinting solutions have different levels of robustness and capacity to resist all forms of modifications and distortions of the content. Audio fingerprinting techniques usually present a high level of robustness ([141]). With regard to audio content, fingerprinting is more robust than watermarking since the 'fingerprint extraction procedure makes use of the full audio signal power' while 'watermark detection is based on a fraction of the watermarked signal power (the watermark, which is several times weaker than the original audio signal due to the inaudibility constraint)' ([142]).

- **Upgrade capability**: with the development of fingerprinting technologies, and the decreasing costs of both storage and computational resources, fingerprinting solutions can be upgraded to be more robust and accurate and/or reduce the level of resources they need. The real challenge lies with the reference files database, as fingerprints may not always be retro-compatible and in

([136]) See the article 'The Detection is in the Details' released by Turnitin on its online blog.
([137]) Several software identification techniques exist and among them the so-called software birthmark, which consists of extracting features of the software to produce a unique identifier of the source code. For additional information on software protection techniques see: Ibrahim et al., 'Software Manipulative Techniques Of Protection And Detection: A Review' in *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 23, December 2015, p. 17957 ISSN 1819-6608.
([138]) For a clear description of the multimedia fingerprinting procedure see: Herre, 'Content Based Identification (Fingerprinting)', Chap. II, *in Becker, Buhse, Günnewig, Rump N. (eds) Digital Rights Management (2003), Lecture Notes in Computer Science*, Vol. 2770. Springer, Berlin, Heidelberg.
([139]) Guzman-Zavaleta, Feregrino-Uribe, 'Towards a Video Passive Content Fingerprinting Method for Partial-Copy Detection Robust against Non-Simulated Attacks' (2016). PLoS ONE 11(11): e0166047, Introduction, p. 1.
([140]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward, January 2020, p. 18.
([141]) See Herre, op. cit., Chap. III.
([142]) See 'Watermarking and Fingerprinting: For Which Applications?', Cano et al., 2003, p. 20.

that case all the content to be recognised will need to be run through the new fingerprinting technology ([143]).

- **Capacity to be used in conjunction with / to complement other technologies**: it is suggested that watermarking and fingerprinting technologies can be usefully combined, especially when the former experiences issues such as scaling or blurring ([144]). For an application of such combined use, see Section 2 ([145]).

5. AI-BASED / ENHANCED CONTENT RECOGNITION

In its first technology trend report dedicated to AI, WIPO looked into computer vision, which it defines as 'an interdisciplinary field that deals with how computers see and understand digital images and videos. Computer vision spans all tasks performed by biological vision systems, including 'seeing' or sensing a visual stimulus, understanding what is being seen, and extracting complex information into a form that can be used in other processes' ([146]). Computer vision has a very broad set of applications, and notably in the fields of security, robotics or autonomous vehicles, where it can be used to allow computers to learn and respond to their environment.

This analysis is mainly focusing on image recognition whereby a computer is capable of autonomously detecting items and features present in images and videos, such as objects, faces or videos. An AI-based system, fed with a pre-labelled database of content, breaks the targeted image down into small groups of pixels and performs intensive multiple checks in order to achieve accuracy in recognising the image or the subjects contained therein.

A number of technology companies are providing AI-based recognition services to third parties. This is notably the case with Amazon Rekognition technology from AWS ([147]), Image Search provided by Alibaba Cloud ([148]), Computer Vision technology by Microsoft Azure ([149]) and Google Vision API technology provided by Google Cloud ([150]).

5.1 Use of AI-based or enhanced recognition

AI-based or enhance recognition can be used to perform different tasks or for a broad range of purposes.

Tasks - AI-based or enhanced recognition can be used to perform different tasks:

- **'Logo recognition'**: this can be considered as a specific application of image recognition. It consists of detecting, identifying (by comparing) and labelling logos placed on products. It can be used for multiple purposes, with a clear application for brand management and marketing, with brand owners tracking brand mentions and users' sentiment on social media. Companies such as Brandwatch, with their Image Insights image recognition service ([151]), or Logograb ([152]) are

([143]) French Ministry of Culture, CSPLA – Hadopi – CNC Mission Report Towards more effectiveness of copyright law on online content sharing platforms: overview of content recognition tools and possible ways forward (January 2020), p. 13.
([144]) Hsieh, Chen and Shen 'Combining Digital Watermarking and Fingerprinting Techniques to Identify Copyrights for Color Images', *ScientificWorld Journal*. 2014; 2014:454867.
([145]) Watermarking, Advantages and Limits, Capacity to be used in conjunction with / to complement other technologies.
([146]) 'WIPO Technology Trends 2019 — Artificial Intelligence, WIPO, 2019, p. 147.
([147]) Additional information related to the companies to which AWS provides this technology can be found on the Amazon AWS Customers web page.
([148])See Alibaba's Image Search tool and dedicated web page on its API.
([149]) See Computer Vision AI service on Microsoft Azure web page.
([150]) See Google Cloud website.
([151]) See Image Insights dedicated web page.
([152]) See Logograb website.

proposing these kinds of services. These services can also be used to detect trade-marked logos appearing on e-commerce listings for counterfeit products. Some major e-commerce marketplaces, such as Amazon, are developing their own solutions in that field.

- **'Facial and emotion recognition'**: in this case, a computer is able to match a face with a pre-labelled one. Computers can also understand and recognise emotions ([153]). This technology has a broad range of applications, from understanding users' engagement with content to screening a job candidate's mood. As for content recognition, it can help identify films or sports celebrities in audiovisual content. For example, Amazon Rekognition ([154]) or Microsoft Azure's Computer Vision technology ([155]) provide these kinds of services.

- **'Text recognition'**: AI-based or enhanced technologies can help overcome some typical obstacles in the fields of Optical Character Recognition (OCR) ([156]). In particular, it can help extract text present in an image or extract unstructured text from documents arranged in complex ways ([157]). The AI-based image recognition solutions proposed by Microsoft ([158]), Amazon ([159]) and Dropbox ([160]) provide such functionalities.

- **'Object detection and classification'**: through cameras and sensors, a computer can capture images and data, and detect, classify and label elements and objects of the real environment. For example, IBM's Watson technology provides such functionalities ([161]). Such technologies are developed for multiple purposes, especially in the automotive sector to allow for the detection and identification of moving objects in complex environments. Companies like Deepscale are providing these kinds of solutions for the development of 'intelligent cars' ([162]).

Purposes - AI-based or enhanced recognition is used for a broad range of purposes:

- **Content management** (automatic tagging): processing and managing large quantities of content can be facilitated by automated classification. AI-based or enhanced recognition solutions make it possible to group, categorise and tag content with a high degree of accuracy and thereby improve the level content management ([163]). Services such as 'Image Auto Tagging' are analysing pixels and extracting features to automatically assign keywords to an image ([164]). Solutions such as Canto image recognition can automatically describe backgrounds, people and text in an image ([165]). Many cloud service providers are also supporting object labelling and the categorisation of images to facilitate content management. This is, among others, the case with Google Vision API ([166]), Dropbox ([167]) or Microsoft Azure's Video Indexer ([168]). YouTube is also using machine learning to enhance the identification of videos that are targeting young audiences. The purpose is to limit data collection and use related to the viewing of such video, with the view to provide a higher level of privacy for youngsters ([169]).

([153]) For an example see Sightcorp technology web page.
([154]) See information on the Amazon Rekognition APIs can be found on Amazon AWS website.
([155]) See Microsoft Azure Computer Vision web page.
([156]) Optical Character Recognition usually refers to the capability of electronic devices to scan and digitise text.
([157]) See 'Learning to Read: Computer Vision Methods for Extracting Text from Images' (2019) on Medium.
([158]) See information on Microsoft Azure's Computer Vision tool.
([159]) Information about Amazon AWS technology is available at Amazon Textract web page.
([160]) The article 'Creating a Modern OCR Pipeline Using Computer Vision and Deep Learning' (2017) released by Dropbox.
([161]) See IBM's visual recognition service.
([162]) Information about Deepscale visual recognition tool can be found on Deepscale website.
([163]) Picturepark, for example, offers content management solutions using Clarifi's computer vision technology; See also the article 'How Computer Vision Is Impacting Content Management' (2018) released by Clarifi on its blog.
([164]) Information about this service can be found on Imagga website.
([165]) Information on Canto's Image recognition software can be found on its website.
([166]) See 'use cases' section on Google Cloud on AI and Machine Learning Products web page.
([167]) See 'Using machine learning to index text from billions of images' (2018) published on Dropbox Blogs.
([168]) Video Indexer represents a service integrated in Computer Vision API; additional information can be found on Video Indexer dedicated web page.
([169]) See YouTube's Official Blog 'An update on kids and data protection on YouTube' (September 2019).

- **Content moderation**: services are able to recognise a broad variety of concepts such as nudity, sex, violence, substance abuse, swearing and other compliance-related visual objects and sounds. This can be used to support the user-generated content moderation services, with different companies providing solutions in that field, such as Clarifi ([170]), Amazon Rekognition ([171]), Valossa ([172]) or Sightengine ([173]). Instagram recently developed a 'self-moderation' AI-based feature to address the posting of offensive content. The system automatically notifies the user of the harmfulness of the content before posting it ([174]).

- **Image detection on human trafficking websites**: AI-based or enhanced recognition technologies are also used to help law enforcement in the online detection of signs of human trafficking. This is notably the case with the collaboration between XIX – a provider of an image recognition technology ([175]) – and the NGO DeliverFund. XIX's technology allows object labelling and the analysis of images hosted on websites used by human traffickers to help law enforcement in this area ([176]).

- **Visual search and identification for e-commerce**: a mobile phone can be used to take a picture of a product and perform a visual search to obtain more information about it, or point directly to a website to buy it online. Google Images's technology allows a user to drag and drop images in order for the search engine to give back a range of similar images found on internet websites ([177]). Companies such as Visenze ([178]) are providing these kinds of services. Some other solutions can perform object description and identification in real time, which can be used to automatically generate listings for products to be sold on e-commerce marketplaces. A company like Cloudsight ([179]) is offering such solutions.

- **Anti-counterfeiting**: AI-based or enhanced image recognition technology is used to detect and identify products or logos affixed to them both online and offline. This is the case for Trademarkvision, which allows its clients to train its AI-enhanced recognition technology to enable it to automatically search for images of their trade marks or products ([180]).

  In the offline environment, image recognition can be used to recognise genuine and/or fake products. The online marketplace GOAT uses image recognition to identify and authenticate shoes in its warehouse for fraud detection purposes ([181]). Technologies are also developed to look into the microscopic characteristics of products, and detect fakes. This is the case for Entrupy ([182]), which is developing services in that field, using mobile devices for retailers to authenticate products and increase customers' trust.

- **Anti-piracy**: AI-based or enhanced technologies are used in copyright online infringement detection, with supporting services to recover money in case of infringement. Companies such as OSN (which used Amazon Rekognition technology) ([183]) or Copytrack ([184]) are using AI-based or enhanced image recognition to search and detect IP infringing use of copyright-protected images.

([170]) See Clarifi website.
([171]) See Amazon Rekognition website.
([172]) See Valossa website.
([173]) See Sightengine website.
([174]) See Instagram's Blog 'Our Commitment to Lead the Fight Against Online Bullying' (July 2019).
([175]) See XIX website.
([176]) See 'This AI can spot signs of human trafficking in online sex ads' (2019) published on Fast Company.
([177]) See How Google Search works.
([178]) See Visenze website.
([179]) See CloudSight website.
([180]) See 'Why is image recognition so critical for the future of brand protection?' (2018) published by Trademarkvision.
([181]) See 'Putting Their Foot Down: GOAT Uses AI to Stomp Out Fake Air Jordan and Adidas Yeezy Sneakers' (2018) published on Blogs Nvidia.
([182]) See Entrupy website.
([183]) See 'OSN is taking the fight against piracy a notch higher' (2019) released by Broadcastpro.
([184]) See Copytrack website.

The technology, developed by Restb, is another example of anti-piracy use with the use of AI technology to detect watermarks on copyright-protected images (see p. 12).

- **Document and source code plagiarism recognition**: technological tools to detect plagiarism are not new, but the use of AI can make these tools far more efficient. The use of neural network patterns enhances the capability to detect plagiarism based on global (entire document) and local (a sentence or paragraph) analysis of features such as the author's style ([185]) or the vocabulary used ([186]). Machine learning and natural language processing techniques are significantly improving the detection of plagiarism ([187]), with companies such as Copyleaks, and its Plagiarism Checker API technology ([188]), providing these kinds of services.

  Plagiarism recognition also applies to source code ([189]). Companies such as Codequiry ([190]) with its Code Plagiarism API are providing services in that field. Another example is the solution provided by Unicheck technology ([191]), which is able to detect both code plagiarism ([192]) and plagiarism in educational institutions ([193]).

- **Customised advertisement insertions**: AI-based image recognition technologies are used to detect the most relevant emotional contexts in audiovisual content in order to provide a brand with the opportunity to insert advertisements into them. If this is a really new application, the video platform Tencent already uses Mirriad technology ([194]) to embed advertisements in its audiovisual content ([195]). Another example is the project carried out by TF1, which tested Mirriad technology to insert SEAT advertisements into some of its programs ([196]).

5.2 Advantages and limitations

There are different advantages and limits of AI-based or enhanced recognition technologies:

- **Resources**: since AI requires the storage, processing and analysis of large amounts of data, it requires significant data storage and computational resources, especially in the field of image and video recognition ([197]). It also requires a considerable amount of work by highly skilled technical professionals in order to find the most appropriate model in relation to the purpose, develop robust characteristics and achieve the best optimisation. It is interesting to note that a number of major technology companies are making AI-based recognition solutions available as a service, for other companies to get access and use such technologies.

([185]) Machine-learning algorithms performing text mining and Natural Language Processing – including the analysis of the linguistic structure – in order to identify authorship in intellectual works have undergone a remarkable evolution in the last years. For a technical insight see 'Authors' Writing Styles Based Authorship Identification System Using the Text Representation Vector', Benzebouchi et al., in *2019 16th International Multi-Conference on Systems, Signals & Devices (SSD)*, 2019.
([186]) See Seaward and Matwin's paper on 'Intrinsic Plagiarism Detection using Complexity Analysis' (2009), University of Ottawa.
([187]) See 'How Technology is Revolutionizing Plagiarism Checking' (2019) released by Copyleaks.
([188]) See Copyleaks' API.
([189]) Among others, see: the Kilinç, Deniz and Bozyiğit, Fatma and Kut, Alp and Kaya, Muhammet 'Overview of Source Code Plagiarism' (2015) in *Programming Courses. International Journal of Soft Computing and Engineering*, 5; Yasawi, Kailash et al. on 'Unsupervised Learning Based Approach for Plagiarism.
Detection in Programming Assignments' (2017) in *ISEC '17 Proceedings of the 10th Innovations in Software Engineering Conference,* pp. 117-121.
([190]) See Code Plagiarism API on Codequiry website.
([191]) See Unicheck website.
([192]) See 'Unicheck Invites You to Test an Innovative Tool for Checking Source Code for Plagiarism' (2019) released on Unicheck Blog.
([193]) For additional information on this service see Unicheck website.
([194]) Additional information on Mirriad website.
([195]) See 'China's Tencent will seamlessly embed video ads directly into movies', 2019, Thenextweb.
([196]) See 'SEAT innove en inaugurant le placement de produit virtuel proposé par TF1 Publicité et Mirriad', 2019, published on TF1 Publicité.
([197]) See The Intelligent Transportation Society of America's report on 'Connected Vehicle Insights - Trends in Computer Vision', 2012, p. 3.

- **Technical implementation**: image or video recognition software is needed to detect and analyse digital content ([198]) and can be implemented at network, server or device level. Even if there is no need for a reference database or to embed individual watermarks, AI requires important computational resources. Furthermore, deep learning techniques require large amounts of data for the recognition technology to perform its tasks.

- **Accuracy**: there is a broad range of AI-based or enhanced recognition types of technologies and limited information on their levels of accuracy ([199]). In addition, the accuracy of a given technology largely depends on the amount of data / content provided to train it for a specific application and/or type of content. Adding new data might require models to be re-trained and/or parameters used in machine evaluation to be re-set. This might result in considerable delays when it comes to real-time detection. AI-based or enhanced solutions are still being developed and the level of accuracy is expected to increase in the coming years.

- **Robustness**: some image and video recognition technologies are already robust enough to recognise video frames subject to rotation, colour changes or compression ([200]). However, the low degree of quality, or quality distortion ([201]) of the analysed content negatively affects their performance compared to human beings. In particular, issues may arise in recognising blurred or transformed images ([202]). Machine learning techniques are constantly improved to address such issues and bridge the gap between machine and human recognition ability ([203]).

- **Upgrade capability**: AI-based or enhanced content recognition techniques are constantly evolving and since they do not rely on a reference database of content (but rather on the amount of data / content provided to be trained), they can be more easily upgraded, compared to other ACR technologies.

- **Capacity to be used in conjunction with or complement other technologies**: AI-based or enhanced solutions are already used to detect watermarks and identify copyright-protected content, notably with solutions developed by Restb (See p. 14).

6. CONCLUSION

This first phase of the analysis on ACR technologies shows that they are deployed for a very broad range of purposes. The use cases go far beyond the protection or management of IP rights, as these technologies are central to a number of business and security applications, as well as address major societal challenges, such as the spread of terrorist or child abuse content online. This drives major improvements and innovation, with technologies that are becoming ever more effective at recognising short extracts or elements of a piece of content.

The different ACR technologies all have their advantages and limitations, which may vary from one form of content to another. The greatest challenge with the development and deployment of ACR solutions lies in finding the right balance between:

- their **accuracy** to recognise content, and **robustness** to resist content alteration; and

([198]) This can be digital files in a computer system, or real-world content captured by digital cameras or sensors.
([199]) Among works carrying out an evaluation of neural network-based algorithms see 'Large-scale Video Classification with Convolutional Neural Networks', Karpathy et al., 2014, with respect to video classification and labelling.
([200]) Information about Videntifier technology is available on its website.
([201]) See: Dodge and Karam 'A Study and Comparison of Human and Deep Learning Recognition, Performance Under Visual Distortions', 2017.
([202]) Such as recognising non-distorted images and images presenting the same grade of quality.
([203]) Among the research works on improving robustness see: Hendrycks and Dietterich 'Benchmarking Neural Network Robustness to Common Corruptions and Surface Variations', 2019.

- the **data storage and computational resources** needed to implement them.

The use of the most accurate and robust ACR technologies, such as fingerprinting or AI-based or enhanced solutions, requires significant computational power and investment. A growing number of companies are developing solutions facilitating the use of such technologies for the broad range of use cases identified.

The combination of different ACR technologies can contribute to optimise the resources needed to recognise content. For example, AI-based or enhanced solutions can be used to recognise illegal content. The files containing such content, and that are identified through such resource-intensive solutions, are subsequently hashed for all identical files to be detected. Since hashing is a less resource-intensive method, this helps reduce the resources. Different ACR technologies are already combined in this way and it would be interesting to explore the potential for such combinations further, to improve content recognition while reducing the resources needed.

Phase 2 of this discussion paper will explore the development and complementary uses of ACR technologies, looking into the following five IP-focused use cases:

- Detection of IP infringing listings on e-commerce marketplaces
- Smartphone solutions to detect genuine or counterfeit products
- Solutions to recognise 3D printing files and 3D printed products
- Solutions to protect and manage IP rights on content-sharing services
- Solutions to identify live streams of IP-protected content

This 2nd phase of the analysis should be finalised by the 2nd quarter of 2021 and contribute to further the understanding of the current and potential impact of ACR technologies on IP.