



IdeasUnlimited.tv
5 Mead Lane
Farnham
Surrey
GU9 7DY

Tel +44 (0) 870 162 7200
Fax: +44 (0) 870 162 7201
Web: www.ideasunlimited.tv

white paper

An Introduction to Media FingerPrinting

By **Glyn Powell-Evans**
© 2003 IdeasUnlimited.tv

Just over 100 years ago, Scotland Yard introduced a brand new development in its fight against the pickpockets, petty criminals and pilferers that plagued Victorian London.

A report in a British scientific journal describing the uniqueness and permanence of individual fingerprints led to the introduction of a system that quickly became the most widely-used method of criminal identification in the world.

A century on, a similarly keen eye for detail is set to revolutionise the monitoring of video and still images on television and the Internet. This new technique, Media FingerPrinting, has been designed to allow broadcasters to ensure their media is correctly delivered to the TV set and desktop while helping them fight a typically 21st-Century crime ... copyright theft.

Media FingerPrinting is a core technology that analyses, categorises and records information about video, audio and still images in a very storage-efficient manner. Should that material ever receive another airing, it can be instantly recognised and matched to its original source or the time and place at which it was logged.

And while the police and security services base their identification procedures on arches, loops and whorls, Media FingerPrinting analyses an image by selecting a number of its key features.

If a felon, for example, has 'battle scars' from all his breaking and entering pursuits, his fingerprint will still incriminate him because its unique characteristics will still be intact. Media FingerPrinting can also look beyond the blemishes and will detect a picture even it has been compressed to within an inch of its life or tampered with in any way.

It's an extremely storage-efficient system, too. Each individual fingerprint – typically captured five or six times a second in a moving stream - occupies less than 30 bytes of data

This means that in a 24-hour stream of moving video, less than 20 megabytes of FingerPrint data is created and stored to represent an entire day's worth of material. Compressing video at the highest limit that will allow some sort of watchable picture would require many hundreds of megabytes' worth of storage to achieve the same task.

Although the FingerPrints cannot be seen by the naked eye, they speak volumes to a computer - this technology does not attempt to recreate a picture, it is merely looking for a FingerPrint match.

The original material is catalogued and a FingerPrint is captured – for example, a 30-second commercial will have 100 to 200 FingerPrints selected automatically and logged during the cataloguing process.

These are stored alongside the additional metadata– title, file ID, copyright ownership etc – and, by the monitoring of broadcast streams, that same image can be detected via a simple database match.

The logging and monitoring process takes place in real-time but the database matching process can be many times faster depending on the size of the catalogue which is important when someone is, for example, trying to compile data from multiple monitoring stations simultaneously.

Media FingerPrinting is particularly useful for the monitoring of transmission carried out by third parties.

To track usage of material in other broadcast streams, operators would first catalogue that material using the Media FingerPrinting ContentProbe product and then capture the FingerPrints in real time and transmit them back via an intranet or the Internet to a central database.

The amount of data collected centrally is relatively small even if there are hundreds of ContentProbe stations used.

This database matching process can either happen in real time or retrospectively.

Of course, there are other technologies available for the identification of images within third-party transmissions, such as Watermarking. This process, however, relies on an image being modified and the watermark is inserted into the video stream; this is then retrieved from the stream at a later time and compared with the database entry.

This requires the watermark to travel with the video material. It's quite likely, however, that the watermark may not survive any modification process such as compression, standards conversion or encoding for transmission on the Internet. A Media FingerPrint is stored centrally and, as it does not travel with the material, it cannot be corrupted even if the material undergoes many changes.

Indeed, Media FingerPrinting can still identify material after it has been transmitted on the web.

It is also possible to use Media FingerPrinting retrospectively.

For example, if a broadcaster takes a piece of material from its archive and wants to know if it has been used by any of its clients over the previous three months, a check through the database logging the FingerPrints of the monitoring stations will reveal the answer. This is not possible with Watermarking.

A key application for Media FingerPrinting is transmission verification. Many broadcasters are no longer in complete control of their transmission chain. They rely on third-party telecommunications companies and carriers to distribute their signal to remote locations or even around the world.

It's difficult, if not impossible, to verify that what is being transmitted in, say, Singapore is actually the same programming leaving the broadcast centre.

You could have a return video path and monitor at the transmission centre with somebody watching it or, alternatively, someone watching the signal remotely to ensure viewers are tuning into the programmes they were promised in the listings magazines.

Alternatively, Media FingerPrinting allows real time direct comparison between the transmission feed from the broadcast centre and, by using a monitoring station connected via the Internet from the remote location, it will compare the FingerPrints from both sites and alert you to a mismatch.

This process is made more complex by the fact that the system is required to deal with significant broadcast delays from satellites and encoders and also needs to be able to deal with multiple aspect ratios.

How can you make sure the transmission is being converted correctly? It's sometimes difficult for the human eye to tell if the ratio is wrong. Media FingerPrinting can tell you in what aspect the picture is being shown.

The technology is robust in that it will not be fooled by separate logos, IDs or captions laid over the picture.

And there are, of course, sound commercial reasons why broadcasters need to know the correct signal is reaching its intended audience. The protection of a brand image and on-screen style is particularly important to national broadcasters competing against the proliferation of smaller channels working to different – and less rigid – agendas.

And it's essential that commercial networks are confident that the advertisements sent out to their affiliates are broadcast correctly.

In the US, 'barter spots' are paid for nationally and are released as part of a syndicated broadcast. Affiliates have to keep a close eye on the spots to make sure they are not accidentally replaced when they carry out the insertion of their own, local commercials.

Not only will it ensure that the programming is transmitted correctly, Media FingerPrinting also guarantees that commercials are not blocked either accidentally or – in the case of less-than-scrupulous cable operators – deliberately when they secretly try to sell their own commercial space during a networked programme.

In some parts of the world, commercial blocking is a real problem. How can international broadcasters know when entire chunks of their satellite feeds are being illegally transmitted during the night on a channel in an obscure East European backwater?

Media FingerPrinting is on their case.

It is, however, the field of copyright protection – and, of course, the correct payment of licence fees – that threatens to be the largest broadcasting headache, particularly in the news environment where the pressure of chasing deadlines can often lead to misunderstandings and memory lapses.

News organisations often take in feeds from agencies on a pay-per-view basis or on the understanding that a limited usage agreement will not incur additional fees. While the agencies attempt to monitor their clients' output, the logistics can often defeat them.

Although the vast majority of broadcasters are inherently honest and return the correct fees, it's very difficult to police, even within the news organisation itself, just how – and when - the material is being used.

An editor, for example, who doesn't know the source material he is cutting into a bulletin package is copyright-protected could find himself infringing an agency's copyright without actually knowing it.

That material could be re-used in subsequent packages and, although a copyright fee is due for every transmission, it may well be that the information does not get passed to the appropriate parties.

Media FingerPrinting allows the customers of the agencies themselves to monitor what is being used from their own facilities, thereby avoiding any accidental copyright infringement.

Similarly, the agencies would know almost instantly which elements of its material is being used by its clients, thereby potentially allowing them to tailor their output better to meet their clients' requirements.

And in this truly multi-media age, broadcasters also need to protect their copyright from unscrupulous individuals.

For example, a major sports channel with exclusive pay-per-view rights to a boxing match would not be pleased should just one viewer encode the signal and make it available across the world on the Internet, charging surfers a very reasonable \$1 for a ringside seat.

Using web crawling technology, Media FingerPrinting would be able to detect such subterfuge and ensure that the webcaster would very soon be out for the count.

In the same way that forensic fingerprinting has revolutionised the field of crime detection, Media FingerPrinting is set to transform the way in which the copyright of programme material is policed.

- ENDS -