



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
Transmission Verification
using
Media FingerPrinting

By **Andy Harrison**
© 2003 IdeasUnlimited.tv

MEDIA FINGERPRINTING – Transmission Verification

By *Andy Harrison* | *technical director, IdeasUnlimited.tv*

1.1 INTRODUCTION

IN today's sophisticated, multi-channel environment, there's a vast number of separate processes and switching stages through which a television signal will pass ... any one of which may fail or detrimentally affect the picture integrity.

And, of course, the number of channels beamed into homes - as well as the number of potential signal paths to the consumer - has also multiplied.

This means that the opportunity for faults, failures and problems occurring between the broadcaster and the consumer is significantly increased.

As a result, it has now become virtually impossible for a human being to monitor a signal through all these separate processes and transmission paths and verify that the consumer is receiving the correct picture and audio, in the correct format.

1.2 WHY PERFORM VERIFICATION?

There are, of course, sound commercial reasons why broadcasters need to know that a correctly-formatted signal is reaching its intended audience.

But very few broadcasters now own or manage their means of transmission. This is contracted out to telcos and specialized transmission organisations.

The transmission carrier enters into a service level agreement with the broadcaster where the minimum level of service performance is guaranteed. More often than not, the carrier is obliged to pay compensation to the broadcaster if the number or duration of transmission outages and failures exceeds that stated in the performance guarantee.

But if you are a broadcaster, transmitting over several regions, how do you verify the level of performance?

The transmission carrier may, after all, have a vested interest in not disclosing failures. Your own engineering staff may be unaware of brief failures in a region that is remote from the broadcast centre unless your customers ring your call centre to complain.

And by that time, of course, your reputation could easily have been damaged.

The protection of brand image and on-screen style is important, particularly to large broadcasters competing against the proliferation of smaller channels working to different – and less rigid – agendas.

And it's also essential that commercial networks can verify that the advertisements sent out to their affiliates are broadcast successfully - and in the correct aspect ratio - and that scheduled local opt-outs are being executed correctly.

We are aware that there are certain parts of the world where 'commercial blocking' is commonplace. (Usually performed on a live program feed at a cable head-end or satellite facility, this is the practice of an unscrupulous cable operator illegally replacing a channel's commercials with other, locally-sold spots).

Until now, the only way to verify the transmission chain was to provide a return reception path to the transmission suite that could be seen by the transmission operators. If they saw an unexpected discrepancy between the outgoing and incoming signals, they could raise the alarm.

Unfortunately, in some cases it is either impossible – or, indeed, too expensive - to provide a return signal path from a remote region. Also, as the number of channels being transmitted from a typical facility is increasing, it becomes impractical for the operators to visually confirm that the network is operating as expected.

ContentProbe Verification can solve this problem.

1.3 HOW CONTENTPROBE VERIFICATION WORKS

ContentProbe uses Media FingerPrinting technology, which uses the principles of video image and audio waveform recognition. By analyzing the colour, brightness and motion of the video signal and both the frequency and amplitude characteristics of the audio waveform, the FingerPrint Analysis Engine builds and stores a mathematical ‘map’ of the transmitted signal.

Media FingerPrinting technology is completely non-invasive as the FingerPrint is not encoded into the original signal ... nor does it travel with the signal. This means that it can never degrade the signal, image or audio soundtrack and can never be degraded itself.

Media FingerPrinting is immune to standards conversion, re-colouring, re-branding with logos or subtitles, compression, or severe bandwidth reduction. It will even detect when a signal has been relayed in the wrong aspect ratio or with a transposing of audio channels.

ContentProbe Verification uses Media FingerPrinting technology to perform a direct comparison between the original reference signal and a signal at any point of the processing chain or transmission path. This provides the broadcaster the capability to verify local and remote transmissions, with both local and remote alarms and a full logging facility for audit purposes.

1.4 THE HARDWARE & INFRASTRUCTURE

The hardware is very straightforward. A simple, small, dedicated 1U network device is installed in each location at which the signal is to be monitored.

These Contentprobe boxes have one or two video inputs, each with a pair of associated audio channels. The inputs may be analogue or digital.

In addition, a TCP/IP network connection is required to each device and a permanent Internet or Intranet connection capable of carrying from as little as 15kb/s per channel monitored is supplied to each appliance.

This allows data about the monitored channels to be returned to a central aggregation point.

In order to reduce the complexity (and therefore cost) of the signal monitoring appliance, the signal comparison is performed not at the point of signal capture but by a central server. This Central Comparison Server (CCS) can match and report on several hundred channels simultaneously, with remarkably low latency.

The monitoring server makes widespread use of Microsoft’s Dot Net (.Net) internet-based infrastructure to provide secure Internet communication and distributed server architecture. This also enables a high degree of redundancy to be deployed.

1.5 STATUS AND ALARMS

The status of the broadcaster’s transmission network may be accessed on any PC via a standard Internet browser. This makes the system very flexible because no special client software is required, allowing monitoring to be performed from a variety of locations (including the Chief Engineer’s home!).

One, or multiple browsers are pointed at a secure server. The status display contains the real-time status of the local and remote transmission network. Parameters monitored include:

- video path verification
- video present
- video frozen
- colour bars/VTR clocks on output
- aspect ratio
- audio present
- confidence audio level indication
- tone on output
- data communications confirmation

Also, postage-stamp sized, or 'thumbnail' images are returned from each of the monitoring points within the network, and these are updated on the status displays every few seconds. These pictures have proved to be very useful in identifying the exact nature of a transmission fault, and they can provide incontrovertible proof to the transmission carrier or cable network in the case of a dispute.

Error log files are created that include details of any detected transmission or system error (e.g. loss of communications), and reports may be generated from these files. The thumbnail images returned from each of the monitoring points during a detected error condition are also written to the log files along with timecode, and these may be included in the reports.

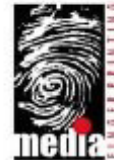


Fig 1. Status display

External alarm triggering is provided by General Purpose Interface (GPI) tallies which can be fitted to each ContentProbe box or any PC running a status display. These tallies are triggered by network messages from the CCS and may be connected to an existing alarms system or a simple external indicator.

In addition, SNMP, email and SMS notification may also be provided by the monitoring service to designated recipients. PDF format reports can be generated and emailed automatically.

Media Fingerprinting VMC Report



Fault Details

Name	ID	Start Time	Duration	Original	Video	Audio	View
Lost Video Input	0001	09:55:00	00:00:20				

09:54:12	09:54:17	09:54:22	09:54:27	09:54:32
09:54:37	09:54:42	09:54:47	09:54:52	09:54:57
09:55:02	09:55:07	09:55:12	09:55:17	09:55:22
09:55:27	09:55:32	09:55:37	09:55:42	09:55:47
09:55:52	09:55:57	09:56:02	09:56:07	09:56:12

Fig 2. Fault Report

1.6 SIGNAL VERIFICATION – HOW IT WORKS

When the integrity of a particular signal processing stage is to be verified, the signal is FingerPrinted at both the input and output of the process and these FingerPrints are compared. The Media FingerPrinting system will then alert an operator if there is a problem.

When the integrity of a transmission path is to be verified, and the monitoring point is some distance from the transmission center, a remote monitoring station - connected via the Internet - will allow comparison of the Media FingerPrints from both the transmission center and the monitoring station.

Where several transmission paths are to be verified for the same signal, multiple remote monitoring stations may be deployed.

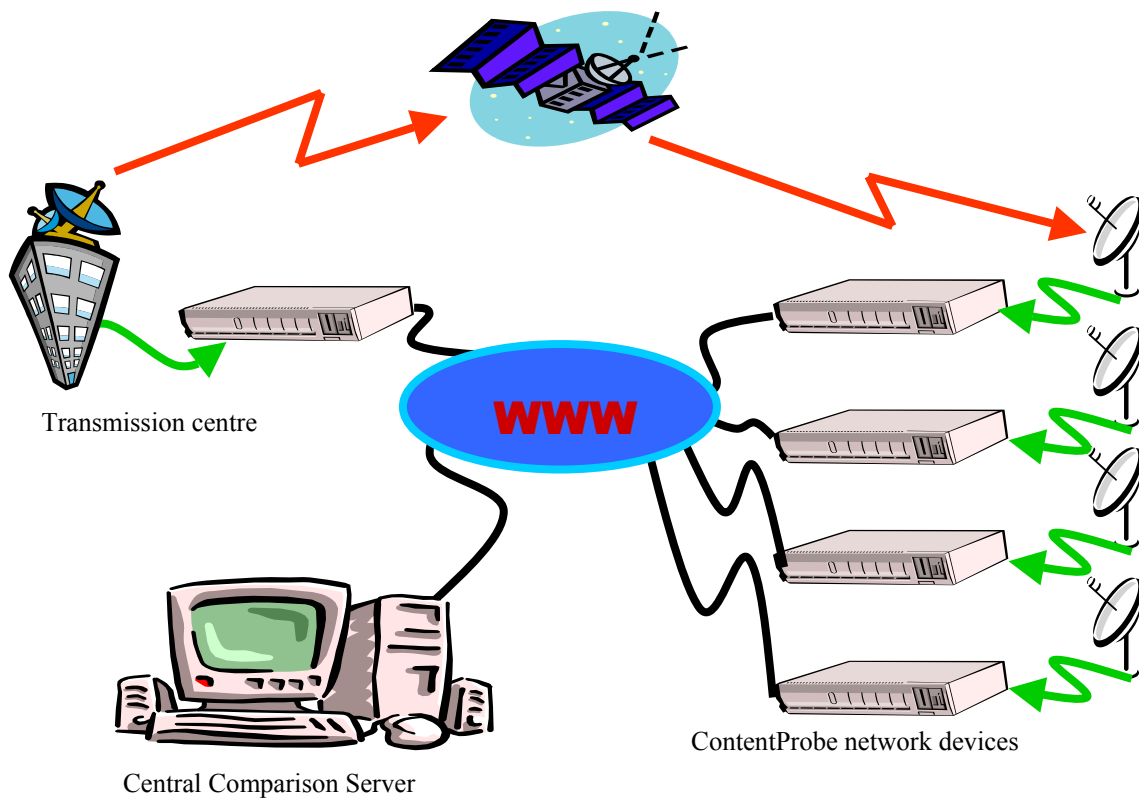


Fig 3. System overview

- ENDS -