



# Image & Video Fingerprinting Software

## Product White Paper

September 2008

### *Overview*

Similis fingerprinting technology provides the ability to ingest image and video files into a fingerprint database and then reliably match images and videos that are the same or similar. Similis ingests and processes files at high speed – up to 40 times faster than real time. Accuracy levels are high and Similis software can be provided as an API for integration into existing work flows or as a plug-in into Fortium's own Harvester scanning software for detection on networked servers and internet web sites.

### *Similis Image*

The Similis image software provides a reliable method of fingerprinting image content wherever it resides. Although other fingerprinting systems do exist such as MD5# matching, Similis is in a different league, providing several distinct advantages that will substantially increase effectiveness especially where there is a need for forensic analysis and ongoing monitoring. When an image is fingerprinted by Similis not only will the original image be detected but so also will variations of the same image. Images are commonly altered either unintentionally in transmission or intentionally to escape detection for example if edited or resaved in different image file formats.

#### **Altered Images**

Images are commonly altered in a number of ways to escape detection and such methods include resizing, file format change, color changing, flipping, mirroring, rotation, cropping addition of text, turning to monochrome, turning to negative. Depending on the degree of change, Similis is successfully able to detect fingerprinted images altered in these ways.



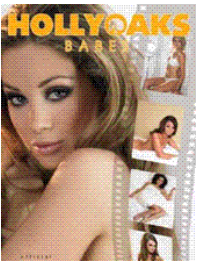
#### **Accuracy**

Independent testing confirms high levels of accuracy for matching altered images details of which can be supplied upon request.

#### **Similis Image Use Case**

In the digital world in which we now live the sheer volume of content circulated across the internet limits us from effectively monitoring where content resides and whether the content is correctly licensed or authorized to reside where it is. Professional copyright photography is a good example where widespread abuse occurs. For certain audiences images containing adult, terror, hate, bullying, defamatory, libelous or other controversial content need to be monitored. For example in the Middle East defamatory images transmitted across MMS networks can contravene local law and technological measures are required to overcome these problems. Similis provides an effective tool to enable you to match exact and similar images to a fingerprint.

## Similis - Altered Image Detection Examples

<p><b>Original</b></p> 	<p><b>Cropped</b></p> 	<p><b>Resized</b></p> 	<p><b>Changed to JPEG</b></p> 
<p><b>Colour Change</b></p> 	<p><b>Flipped</b></p> 	<p><b>Text Added</b></p> 	<p><b>Changed to Bitmap</b></p> 
<p><b>Black &amp; White</b></p> 	<p><b>Mirrored</b></p> 	<p><b>Rotated</b></p> 	<p><b>Changed to GIFF</b></p> 

### **Similis Video**

The Similis Video plug-in to Harvester Compliance software provides a similar solution to the Similis image software but is designed to handle a wide range of video formats which involve different file handling protocols. Similis video ingests video frames at a speed of up to 40 times faster than real time to create a fingerprint for subsequent matching of scanned files. This means a one hour video could be ingested in just over one minute. The size of the fingerprint depends on the size of the file but on average this would be 24KBs which avoids latency in look ups that can occur when matching to large databases. The matching of video files against the Similis fingerprint is fast - averaging at speeds of 20 times faster than real time.

### **Accuracy**

Accuracy in correctly identifying video content can be higher than image fingerprinting as there are more images and more frames to match against the fingerprint. Typically snippets of a video lasting only 20 seconds can be successfully matched against original files. Independent testing confirms high accuracy levels, details of which can be provided upon request.

**Similis Video Usage Case**

Similar to the need to detect images, videos shared on User Generated Content websites are now prolific. Much of the video content shared on web sites like You Tube is done so without authorization of the content owners and in ways that are not immediately obvious for example camcorder shots from cinemas or frames taken from commercial videos and inserted into home videos. Similis provides an effective tool to enable you to match exact and similar videos to an original fingerprint.

**Ad Monitoring**

Similis also provides a method to track content on the internet showing how far and wide content is being transmitted and where it is appearing. This information can provide critical information to monetize these digital assets attracting advertisement revenue.

*Further Technical documentation is available upon request.*

**For more information please contact us:**

**[info@fortiumtech.com](mailto:info@fortiumtech.com)**

Tel: + 44 (0) 1656 663 725

**Fortium Technologies Ltd,**  
6 Bridgend Business Centre,  
Bridgend,  
CF31 3SH,  
Wales, UK.

**[www.fortiumtech.com](http://www.fortiumtech.com)**

