

Scanning Electron Microscope helps ID fake dental items



Source: <http://www.buffalo.edu/>

historic composite resins used in dental components.

A German dental products brand is testing the system to check and verify if any of its products had been copied. Dental components are cheaper in China and India but it is very difficult to confirm if they were real or fake as the packaging and products looked identical to the genuine product.

Early results indicate that cheap composite resins on sale in China and India are mainly counterfeit. They contained silicon but were missing the aluminium and barium that the genuine product included.

'It's a red flag for everybody involved in dentistry who is purchasing the dental material, for the distributors and the dentists who are buying from them,' says Dhruvika Patel, a student who tested the suspected items. 'Everybody is tempted to buy the cheaper material, but you always have to find out why that is cheaper – it could be fake.'

Peter Bush, director of the South Campus Instrumentation Centre at UB, scanned the components using a Scanning Electron Microscope (SEM) with Energy Dispersive x-ray elemental analysis (EDS).

Although this was a one off service Bush is keen to forge more links with industry. 'My lab is a full-service analytical facility and we work with many companies providing services. The dental materials database is just one area of our expertise; it has also been used to help in identification of victims, for example recently in the case of the crash of Continental Flight 3407 in Buffalo, New York.'

Italian fashion adopts RFID

Leading Italian clothing designer and manufacturer G&P Net has reported a return on investment following the deployment of an RFID inventory and logistics management

system last year.

G&P Net, which designs high-end jackets for the GeoSpirit and Peuterey brands, first began discussing an RFID solution to a distribution problem it was experiencing with supply chain management provider Aton in 2007.

G&P Net says RFID has provided considerable operational efficiencies for both in-coming and outgoing goods, as well as warehouse inventory management.

G&P has applied a simple RFID solution. An RFID tag is embedded in each garment/jacket with a serial number. Retailers can then verify the quality and product origin of the garment on receipt. The solution included a comprehensive middleware software solution which provides G&P Net complete traceability from production to retail inventory control.

The tags are scanned using a handheld reader. This can help identify any retailers or distribution firms that breach the distribution contract. If an original dealer is selling products illegally to unauthorised shops, it effects both brand image and distribution margins.

The company offers a complete solution for tracking garments through supply chains. Alien Technology provided the RFID UHF reader and tag equipment that works with the company's own logistics software (onLog) integrated with its RFID Middleware solution (onID), integration services and

consultancy.

Stephen Crocker, Alien Technology sales/channels director, says: 'G&P Net chose our high performance readers, and Higgs3-based inlays to tag each garment. This combination resulted in superior system performance, providing virtually instantaneous reads of more than 300 garments packed in a shipping box as they leave the production site, translating to huge labour and time savings.'

G&P Net has four distribution centres in Italy and from those it ships clothing to retailers around Europe, but mainly in Italy. Owing to the ability to pinpoint unauthorised sales of its garments the company claims to have not only seen a return on investment thanks to legal cost savings, but also because of the improved inventory and logistics management the system provides.

Alien reveals increased RFID security

Alien Technology, in the US, is adding a new layer of challenge/response algorithm security to its Higgs-3 RFID IC, called Dynamic Authentication, as an extra solution to prevent it from being copied.

Although no Higgs tags have been cloned Alien Technology marketing director Victor Vega says that because EPC Gen 2 (Electronic Product Code Class-1 Generation-2 UHF RFID) is an open protocol, programming an EPC number into a tag makes it vulnerable to duplication.

Each Higgs-3 tag has a 32-bit unalterable TID (tag identifier) masked in the silicone; additionally, they have a 64-bit unalterable Unique TID (UTID) for counterfeit and authentication purposes.

'It's possible, but not likely, to copy, if you had \$10 million (€6.8 million) to duplicate the UTID,' explains Vega.

The Dynamic Authentication, however, requires the sending of a unique, signature challenge and only if this is correct will a challenge response arrive to validate the tag.

Since customers have asked to use the Higgs-3 RFID IC for things other than mandate requirements, such as anti-counterfeiting, adds Vega, assurance the tags are impossible

to clone becomes more important.

Aton, a mobile and wireless solutions provider in the US, is now using Higgs-3 tags to help Italian fashion manufacturer G&P Net to combat a grey market problem. They will soon be utilising all 96-bits of code to respond to the tag serial number and size and style details on individual items to provide greater anti-counterfeit protection.

Vega reveals there are 512 memory bits in total from almost 800, which can be designated into chunks of 64-bit blocks. 'Customers can lock information for downstream partners,' he explains, saying that G&P could send viewing permission for each of the eight blocks, which could only be viewed by someone in possession of the 32-bit password.

'It is built upon layers and is the way security industry works,' adds Vega. 'Although it's not encryption nor a smart card, it gives layers of security when used with open protocol at a fraction of the price.' In fact the price will remain static as Alien hopes it will foster Higgs-3 in the industry.

The new 135ft long-range RFID tags produced by Omni ID contain Higgs-3 chips and Vega says this will make them more secure. 'If you spend a lot of money on a hard tag, you want security on top on performance,' he insists.

Civolution unveils significant Pay-TV watermarking plans

Civolution, the Dutch watermarking and fingerprinting technology solutions provider for forensic tracking of media equipment, has just announced it will become the first company to deploy Pay TV watermarking in 2010.

Alex Terpstra, CEO at Civolution, says: 'This is a significant landmark for digital watermarking technology, for content owners and the Pay TV industry.'

As recordings from a television screen are of sufficient quality to make bootleg recordings Terpstra says it is up to the Pay TV and hospitality industries to convince content owners that they can minimise the risk of camcorder attack.

'Conditional Access and Digital Rights Management alone are not enough to prevent

copying as they are designed to protect against signal theft rather than content theft. So the solution is digital watermarking, which works alongside encryption and provides a additional layer of protection.

'This market for watermarking will be driven by the high margins available on premium content – early-release HD movies – and we believe the economics will prove impossible to ignore for any Pay TV operator interested in the premium content market,' continues Terpstra.

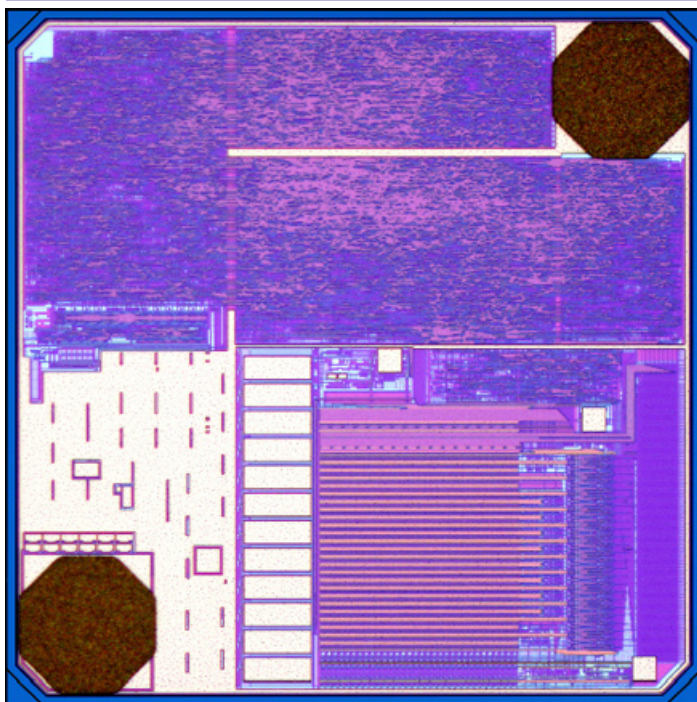
Although declining to reveal names, Terpstra says Civolution will be providing a hybrid solution, with technology at both the encoder and set-top box, allowing piracy to be detected as it is received and redistributed.

The content industry constantly monitors movie and television distribution worldwide and if a movie has been illegally copied, a digital watermark detector will reveal the source.

For the Pay TV market, Civolution's NexGuard Pay TV solution enables a hierarchical approach to digital watermarking. This means platform operators can embed unique operator IDs into movies when they are broadcast or streamed from the video server, then add unique user IDs within the settop box.

'Content owners are only able to detect the operator ID and can inform their distribution partners about unauthorised copying, leaving the Pay TV operators to identify the individual household responsible by detecting the user ID,' Terpstra explains.

Higgs-3 RFID cloning protection



Source: <http://www.alientechnology.com/>