EDITORIAL

Intrinsic Characteristics for Authentication

In the early days of **Authentication News** we identified *intrinsic* and *extrinsic* methods of authentication. *Intrinsic* refers to the authentication and anti-counterfeiting features contained in materials that are essential to an item, such as the paper and ink used to produce a banknote, or the board or plastic used in packaging. *Extrinsic* refers to devices or features which are produced offline and added to the document, product or packaging to make it more difficult to counterfeit. Examples include holograms, labels and now RFID chips.

The advantage of intrinsic features, such as the watermarks in security paper or the use of fluorescent inks, is that they do not require additional application equipment. Despite this, the trend of the last two decades in document and product authentication has been to use both intrinsic and extrinsic features, combining them to strengthen the anti-counterfeit protection of an item.

In this and recent issues we have reported several new techniques to capture the unique characteristics of any one piece or batch of 'stuff,' such as paper, ink or colour, which could provide an added factor in the use of the authentication of intrinsic materials.

Creating a unique code from a particular characteristic of an intrinsic component is an elegant way to be able to identify that component

Wheel Turns Full Circle

Perhaps the authentication wheel is now turning full circle. In 1991 Teunis Tel applied for a patent (WO91/19614) on the *Three Dimensional-Structure Authentication System* (3DAS), later licensed to Unicate (now Orbid Corporation). 3DAS used a laser to project a shadow image of the fibres in paper onto a CCD, recording this pattern as the unique identifier of that paper. The technique was further developed by Rudolf van Renesse, who was awarded a US patent for 'a device for scanning the geometrical pattern of a mark or object' (US 5621 219).

3DAS, and now these new techniques, depend on the impossibility of producing any item so that it has exactly the same microscopic structure throughout. Recently we reported Ingenia Technology's method of using laser speckle to detect the nanometre-sized imperfections in paper or similar substrates (see AN Vol 11, No 9), invented at Imperial College London. Similarly, Rogue Digital Alarm Network was supported by the National Research Council of Canada in developing a process to sense the unique three-dimensional surface profile of documents (see AN Vol 12, No 8).

In this issue, meanwhile, we report that Visualant Inc has developed a process to read and record the unique spectral pattern of colours and textures on a given item. And AlpVision, creators of the *Cryptoglyph* marking system that embeds hidden codes in materials, has taken its technology a step further by using the random characteristics of the material itself, in this case metals, to generate the code.

Unique Characteristics

What these – and other – emerging techniques have in common is the ability to scan the material, each using a different scanning tool to 'see' and record the unique set of chosen characteristics of a given area or patch of the material. Every small area of a long reel of paper, for example, or the ink pattern on it when it has been printed, has different characteristics at the microscopic level. These given characteristics can be digitised, as a picture, or more usefully, through the use of an algorithm as a number. This information can then be stored in a database, with information about the item, so that any single manufactured or printed item has a unique number, which can be checked in the distribution chain using the appropriate reader.

This information has been referred to as the *fingerprint* of the item, and like a human fingerprint it should be unique (or at least, have such an infinitesimal a chance of duplication as to be unique). It is truly intrinsic to the item, in a way that a number or other code generated independently and then applied to the item is not. A particular feature of these 'fingerprints' is that they cannot be seen by a naked eye, nor by using a tool to enhance or reveal the feature to the human eye; this presumably makes them difficult to copy – if you can't easily see it, you can't easily copy it, but the corollary is their dependence on a reading, telecoms and data storage infrastructure.

Creating a unique code from a particular characteristic of an intrinsic component is an elegant way to be able to identify that component (as part of an item) later, and this could become a new aspect of anti-counterfeiting strategies, alongside the visual, or overt, elements designed for public examination and the hidden features used for expert examination.

New Industry Alliance... cont'd

DVDs used in the MPAA Academy Award Screening program; and preventing digital counterfeiting and color copying of banknotes. In addition, digital watermarks are being used to identify and manage image copyrights, and as a method to deter counterfeits of, and to authenticate, ID documents.

Areas addressed by the DWA will include communication and promotion of the technology to content providers, legislators and other concerned industry groups. The alliance will also address issues including privacy and technology through the development of best practices, support the development of industry standards that utilize watermarking and serve as the liaison between the industry and other related industry organizations where the technology has relevance.

The DWA is now seeking further members, with rates ranging from $500 for academic members up to $10,000 for voting members with turnover above $10m per year.

More information can be found at www.digitalwatermarkingalliance.org.

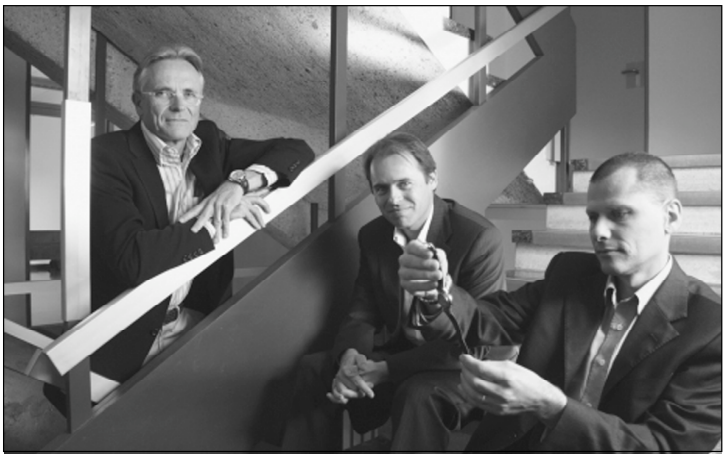
COMPANY PROFILE

AlpVision Advances Security Through Digital Technology

The emergence of digital technology has been cited as a key driver in the exponential rise of counterfeits of documents and products. But it has also provided a vehicle for the development by some companies of a new breed of authentication features that, unlike add-on or extrinsic devices, can be embedded into documents and products as part and parcel of the production process, utilising digital technology both for the application of such features and for their verification.

One such company is AlpVision of Switzerland, founded in 2001 by three entrepreneurs with a background in the emerging science of digital print technology, backed by funding from private investors (and start-up tax exemptions from the Swiss government).

Roland Meylan was the senior founder, along with Frederic Jordan and Martin Kutter of the Swiss Federal Institute of Technology (or EPFL), part of the Technical University in Lausanne. Kutter and Jordan were both studying for PhDs in digital imaging in the late 1990s, with an emphasis on digital watermarking – and in particular the protection of artwork by embedding a hidden image of the artist's signatures into this artwork. Through their work in signal processing, and the extraction of 'noise' from embedded digital images, they took this principal one step further by creating a hidden image that did not need to be camouflaged within existing graphics, but could be applied to plain paper instead.



Senior founder Roland Meylan (left) with Fred Jordan and Martin Kutter (right) (photo provided by Stéphanie Meylan)

Cryptoglyph

This, according to Meylan, is the genius behind *Cryptoglyph*®, the technology used to launch the company. Cryptoglyph is a 128-bit (minimum) encrypted mark or 'glyph' that can be added to blank paper or an overprint, to cover the whole or a chosen part of the printed document. It is decoded by using an off-the-shelf scanner and AlpVision's proprietary software suite, and can incorporate unique or batch data, such as individual bio-data or production information. Unlike other 'hidden' image technologies on the market, according to AlpVision, theirs is the only one that does not require pre-existing images behind or in which Cryptoglyph must hide.

Cryptoglyph can be printed digitally or by offset, rotogravure or flexo, and is applied as very small dots (20-80 micron) which are invisible to the naked eye. In digital printing, integration and use of the glyph is straightforward. It is introduced into the computer-generated artwork and is compatible with standard computer graphics packages (such as Adobe Acrobat and Illustrator).

For offset processes, the glyphs are either integrated into an existing plate or a separate plate is made. They can be printed onto blank paper or as an overprint on the printed item; the latter is particularly suitable for product packaging, because it can be laid over the whole surface of a box without detriment to the graphics. Printing takes place as normal and the glyph is invisible to the naked eye, camouflaging itself in the paper grain.

Whatever the form of printing, to authenticate the document or product, or to extract the coded data, the document is scanned and interrogated by the proprietary detection software program, with AlpVision providing OEM scanning and reading resources.

Office Products

A further development of Cryptoglyph is *SafePaper*, a document security solution in which the glyphs are added to documents generated and printed in office environments. The solution is delivered via a security software package that can be used on ordinary PCs, replacing the usual printer drivers. Documents sent to inkjet or laser printers are embedded with hidden marks comprising encrypted data on the person printing the document, the date of printing and the serial number of the computer. This data can be hidden anywhere in the document and can be detected and verified months, even years later, by off-the-shelf image capture devices (such as scanners or digital cameras) connected to PCs equipped with the corresponding detection software. According to AlpVision, by using SafePaper companies can track and identify the source of all printed documents, enabling them to prevent unauthorised leaks of printed material, document duplication or alteration.

Intrinsic Features

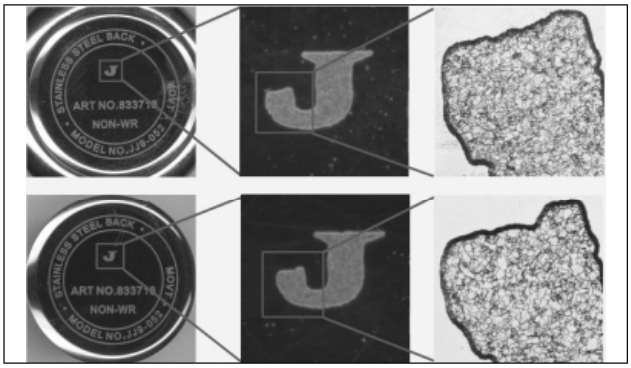
Another development, just announced by the company, is *Fingerprint*™ which, in a departure from the markings applied via Cryptoglyph, identifies objects based on a digital image of the original. According to the company, the technology capitalises on the fact that every manufactured object contains unique characteristics that come directly from its manufacturing process, with the machining or moulding leaving unique prints relating to the tooling and

Continued on page 8

COMPANY PROFILE

AlpVision... cont'd

raw materials used (eg plastics, metal or leather). These unique prints are used by AlpVision's technology to identify the object via a patent-pending process in which a standard scanner captures an image of the object to be identified. This image is sent over the internet to a secured server for later comparison when needed. The server contains the digital prints of genuine objects as well as any previously identified as counterfeits in the markets.



Two objects that were evaluated as identical, but with visible differences seen under magnification and identifiable with the AlpVision Fingerprint™ procedure

The images are converted into digital codes using sophisticated mathematical algorithms that allow comparison with millions of stored reference images in a matter of seconds, returning a verdict of genuine, counterfeit, or unknown.

The first customer for application for AlpVision's Fingerprint technology is the Swiss watch-making industry, with the technology being used to track and trace every watch model during its lifetime. Other sectors earmarked as targets for the technology including food, cosmetics, medical instruments, luxury products, automotive and aeronautical components.

AlpVision is based in Vevey, on the outskirts of Lausanne and now employs ten people, almost all of whom are computer scientists and software developers. The company has two divisions – for security print and brand protection – and turnover for the technology, which is sold worldwide, now exceeds CHF 2m (€1.26m). AlpVision does not disclose as a principal its customers for confidentiality reasons, although it does cite the international certification company SGS, which applies Cryptoglyph to official government documents, as one, and the pharmaceutical packaging giant Rondo as another (pharmaceuticals are seen as a major market for the technology).

AlpVision's technology is sold under licence, with royalties payable on the number of documents or products protected, along with development fees. According to Meylan, this business model marks a departure from traditional (or as he calls them, 'analogue') authentication technologies which are based on physical materials, describing Cryptoglyph (and now Fingerprint) as the 'dematerialisation' of authentication, much in the same way as the music industry is dematerialising through the replacement of CDs with internet downloads.

Self-Sufficiency

'Our technology involves no materials, no specialised equipment, no adjustment or alteration to existing production processes' he comments. 'Customers want to be self-sufficient and don't want to rely on third parties. Although we will work in the early phases of a contract with our customers' production staff to ensure the smooth integration of the technology, other than that we are not involved in their security supply chain.'

He also commented that technologies sold under licences can prove challenging to those with a 'material mindset', noting that some people have difficulty understanding that they have to pay for something that they cannot measure by the kilo or litre!

The Future for Authentication

According to Meylan, the future of authentication will be in the use of technologies such as AlpVision's, which work on the unique characteristics of documents and products (such characteristics being either inherent or through application), utilising readily-available equipment for verification.

He cites one example as the growth in internet sales and the removal of retailers as the interface between consumers and the products they are buying. 'Consumers need to know that what they are buying is real' he says. 'Without retailers providing this assurance, we need to put the tools for authentication into their hands. Our technology, allied to camera phones for example, will enable these consumers to check the products for themselves'.

Contact: Alpvision SA, Rue du Clos 12, 1800 Vevey, Switzerland. Tel: +41 21 948 6464; info@alpvision.com; www.alpvision.com

CACP Survey... cont'd

movements of our products in the distribution chain – 30%;

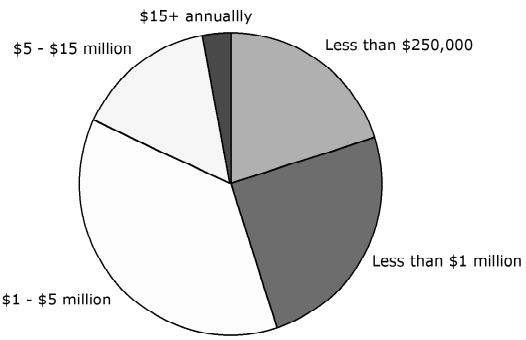
• we comply with government regulations – 8%;

• we are uncertain of the benefits we receive through using technology – 35%.

Expenditure

While the companies responding indicated that the use of technology for authentication is an important issue, their response to the question of how much they spend per year belies the true importance they place on the issue, or perhaps the level of competition among authentication suppliers. Figure 3 shows their level of expenditure.

Fig. 3 - Expenditure on Authentication Review



Continuing Research

The CACP Technology Task Force is continuing and extending its work into both the current usage of authentication technology, as well as research on emerging technologies for authentication and tracking. Its next release will be a white paper on the potential for the use of RFID in anti-counterfeiting applications in fall 2006.

More information is available at www.thecacp.com.

(See page 12 for a review of the US Chamber of Commerce summit on anti-counterfeiting)