RECONNAISSANCE
AUTHENTICATION NEWS®

VOLUME 23 – NO 3 / MARCH 2017

Authentix Launches Vigilant to Combat Illicit Trade in Refined Fuels

Global authentication and information services company Authentix Inc – headquartered in Texas, US – has launched *Vigilant*™, an end-to-end authentication offering for national governments who want to combat the problems of smuggling, diversion and adulteration of refined fuels in their country.

Vigilant is an integrated system of chemical markers and analysers, a powerful information system and service, that in combination creates a solution to fuel fraud problems.

According to Authentix, it is the result of more than 20 years of experience in developing, implementing and supporting fuel marking programs.

Kevin McKenna, President of Authentix's Oil and Gas Division said 'a Vigilant fuel marking program helps government ministers improve fuel quality for their citizens and protect the environment by removing low quality fuel substitutes from the marketplace.

When legitimate fuel replaces illicit fuel in the supply chain, excise and other tax revenue collection increases without raising tax rates, readily paying for the program and funding other government activities.'

Authentix has partnered with governments all over the globe deploying fuel marking programs, protecting over 1.5 trillion litres of refined fuels.

The Vigilant offering also embraces the company's historical core capabilities into an Internet of Things (IoT) framework, aggregating the fuel marking program operations information along with external data into the Authentix Information System (*AXIS*®). AXIS includes analytical applications and reporting tools to present data-driven, actionable insights in support of the government's enforcement protocols.

Vigilant also includes services to advise government personnel on the design of the fuel marking program, implementation services to streamline deployment and ongoing operational support to ensure success.

www.authentix.com

YPB Group to Provide Anti-Counterfeit Technology

Australian based companies YPB Group Ltd – a provider of brand protection solutions – and Le Mac Australia – a packaging and labelling solutions producer – have entered into a Memorandum of Understanding (MOU) with a view to formalising a supply contract for YPB's *PROTECT* anti-counterfeiting technologies.

Le Mac Australia (Le Mac) was established in 1984 and is recognised in the industry as an innovator and market leader in shrink sleeve technology, winning numerous awards to confirm this position. Its 'Mutiny' parchment-like shrink sleeve won two gold and 'Best of Show' at the last Australian Packaging Awards.

YPB will provide its covert (invisible) tracer to Le Mac who will then offer this unique anti-counterfeit technology to its clients. Le Mac's clients will benefit from their end customers having increased confidence that they are purchasing authentic products. The agreement has already guaranteed five million items for the remainder of 2017; however, Le Mac produce hundreds of millions of sleeves annually.

Mike Cowan – Managing Director of Le Mac Australia – said, 'we are really excited to be partnering with YPB Group. We constantly strive to improve our service offering to our clients and product authenticity is an area where we wish to lead the way. For two Australian companies to be able to bring our technology to the world market is a really exciting for both parties.'

IC Optix Printed Magnifier Technology Focuses on Scale-Up

***Authentication News*® reported in June 2015 on a novel printed thin film patented magnifier technology, developed by IC Optix based in Philadelphia, US, for use and integration into product labels (for authentication) and everyday items such as pens, as convenient vision aids for consumers. We caught up with Jim Rittenburg CEO for an update on this new exciting technology.**

Background

Many people over the age of 40 years old have trouble reading important small print information on labels for medicines, foods, use instructions and other products.

The reasons for this are twofold. The first is the effects of aging eyes due to presbyopia, and the second is the trend in packaging including sustainability initiatives, multi-lingual and increasing regulatory requirements for warnings and product information, have resulted in smaller pack sizes carrying increasing amounts of information.

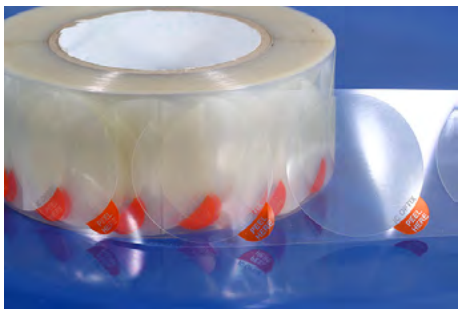
Medicines and other healthcare and personal care products are often packaging in relatively small bottles, blister packs, and boxes that have limited real estate for printed information.

The inevitable result is that text is printed in small font sizes, appearing crowded and therefore difficult to read. This can lead to errors resulting from people miss-reading or not bothering to read important information such as warnings and instructions for use.

Unique magnifier solves problem

In response, IC Optix have developed a low cost, highly scalable, unique magnifier label technology solution that tackles the problem of label legibility, thereby improving consumer/patience compliance and safety by reducing the chance of medical error.

Large format magnifier lens labels on reels.



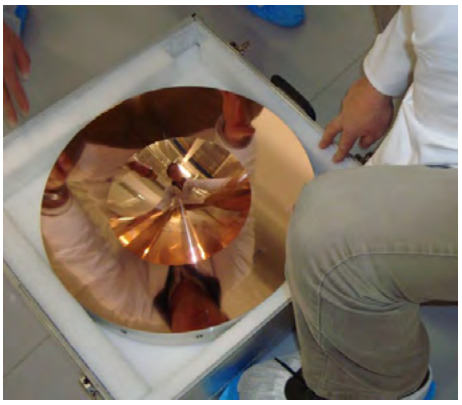
Transparent large format magnifier labels (can be integrated as an over-label).

Magnifier lens on a bottle.

Magnifier lens in use on a bottle.

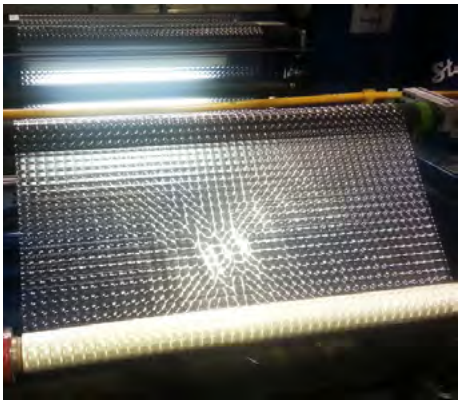
The technology begins with the design, using computer modeling, of an ultra-thin film magnifier lens of a micro-structured lens, providing the desired optical lens prescription.

The design is then transferred from the digital world into the physical world using a high precision diamond engraving process. A master tool with exact facet angles, depths, and spacing is created for the manufacture of a high quality optical lens.



An engraved master tool.

To achieve high volume, low cost production of the lens, the master tool engraving is replicated and repeated across a cylinder. This produces the lens array that can be subsequently used in a reel to reel UV casting manufacturing process and further finished into fully customisable magnifier labels or scrolling magnifier devices.



Lens array.

Inside this Issue

Latest developments:

IC Optix have worked closely with Securikett – the Austrian company that specialises in brand protection solutions, product protection and the development and production of security labels.

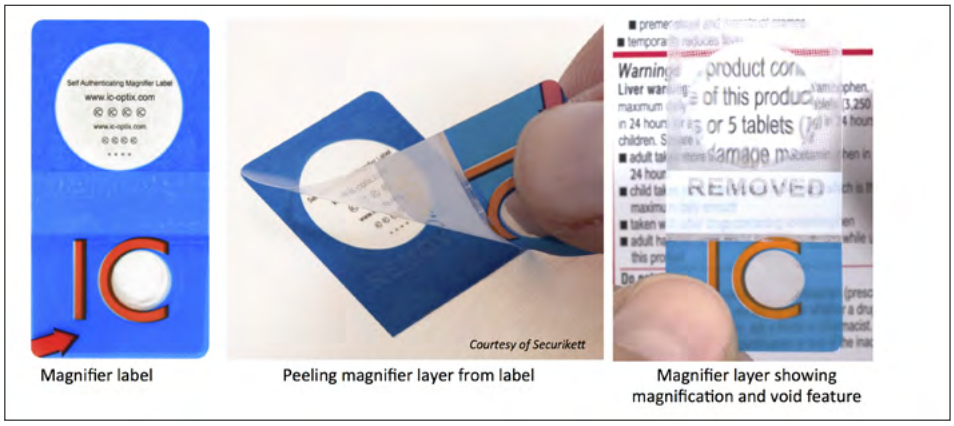
The collaborative work involved optimising the integration of the lens film into finished label constructions, scaling-up label production, and combining the magnifier functionality with various tamper evident label structures and optically variable micro-structures to improve security – as highlighted in the following sections.

Enhanced label security

Not only is the thin magnifier lens label difficult to copy due to its depth and radial structure, but it also has the 'value added' function of being able to help confirm the authenticity of the package.

To further enhance the security aspect of the magnifier film, striking overt and covert features produced from optically variable microstructures (including holographic micro-text), and diffractive watermarks can also be integrated into the magnifier film as part of the same proprietary manufacturing process used to produce the lens.

Example of IC Optix magnifier labels incorporating holographic diffractive elements.

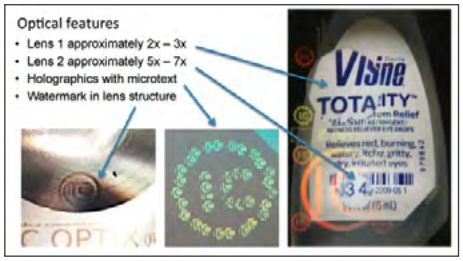


Magnifier label | Peeling magnifier layer from label | Magnifier layer showing magnification and void feature

Examples of IC Optix magnifier labels incorporating tamper evidence.

Enhanced magnification labels

Multiple thin film magnifier lens' that have different powers of magnification and that are capable of reading micro-text can also be combined within a single label structure.



Examples of IC Optix magnifier labels incorporating holographic micro-text and different lens magnifications within the label.

Tamper evidence

In addition to producing labels containing a magnifying layer that can be peeled away to read the label information and then re-adhered for multiple use, the magnifier lens labels can also incorporate functional high security tamper evidence with visual void effects.

The company also confirms that the technology is readily integrated into a manufacturer's standard packaging and labelling processes with a low impact on operations.

Applications

Primary markets for this product technology include brand owners with products in:

- Healthcare (over-the-counter and pharmaceutical);
- Personal care;
- Crop protection
- Consumer packaged goods;
- Direct to consumer applications;
- The broader packaging industry: for example, the magnifier lens technology could be incorporated into hang tags and magnifier windows in cartons.

Other applications include winding the ultra-thin and flexible magnifying lens film so that it can be scrolled onto and off a spindle in the same way as roller blind, thereby providing a larger magnifier film area to be used.

The film can also be integrated into everyday portable objects such as pens, flashlights or key fobs, enabling the magnifier device to be close at hand.

Scrolling magnifier unopened.

Scrolling magnifier opened.

www.ic-optix.com

Xerox Printed Memory: Product Protection & Consumables Monitoring

As Xerox is a well-known global brand for digital printing equipment and copying machines, the reader must understand that typical office, industrial digital printers, or graphic art printers from Xerox are not used to manufacture their printed memory devices. Today Xerox produces printed memory devices in one of their plants in Rochester, New York, US.

The deeply entrenched expectations associated with their brand testify to its strength, and naturally, when a reader thinks Xerox, they think they can print or produce something themselves. For printed memory, this is not the case.

A new concept – even internally

Patrick De Jong, Global Marketing Manager for Xerox Printed Memory (XPM), based in Spain, combats these entrenched expectations frequently within even in his own company when he presents the concept to internal executives and sales people. *Authentication News*® spoke to De Jong for this article.

Xerox prints memory devices/labels onto a thin, flexible substrate. Users of XPM (pre-programed by Xerox and post-programed by the customer) write to and read from them with a contact reader.

These devices are available in standard storage capacity sizes of 4, 10, 25, and 36 bits. A 36 bit device can store over 68 billion unique combinations. Xerox will consider custom capacities as well.

From concept to deliverable formats

Thinfilm, a Norwegian company and Xerox's partner in the development of XPM, specialises in innovation, research and development of printed electronics and smart systems. 'Because Thinfilm needed help in manufacturing expertise and in bringing printed memory to market, they reached out to Xerox's Palo Alto research center in California,' according to De Jong.

He added, 'having such a worldwide commercial coverage, a recognised brand, and being able to set up a manufacturing plant within an existing facility, made it a perfect match.'

Xerox licensed the technology from Thinfilm in December 2014. The plant for rewritable non-volatile XPM began production scale manufacturing in early 2016.

Each XPM is printed with an adhesive backing, making the most basic format an XPM label. Customers may choose from a variety of formats: web, converted single track rolls, rolls of extended size adhesive labels, or memory on cards. Optional tamper-evident adhesives are also available.

The importance of understanding manufacturing processes

As a mature manufacturing company, Xerox researched and planned to deliver products in the manner in which most users would use the products.

Many start-up and conceptual companies developing authentication technologies fail to comprehend the necessary industrial engineering steps when pitching their ideas.

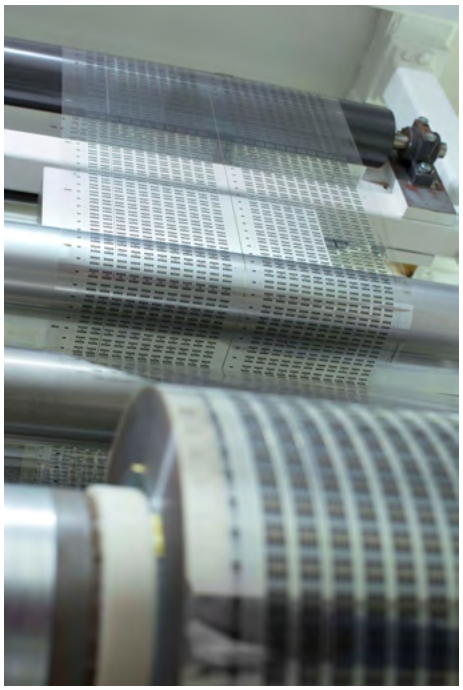
Beyond the characteristics and cost of an authentication technology, a company launching these technologies must understand the processes and associated costs required to integrate the product and deliver it into an existing manufacturing stream.

Most companies strongly resist changes to their finely tuned manufacturing processes. Anything that changes a process, slows line speed, or brings additional manufacturing complexity/risk faces a long, slow, complex selling cycle.

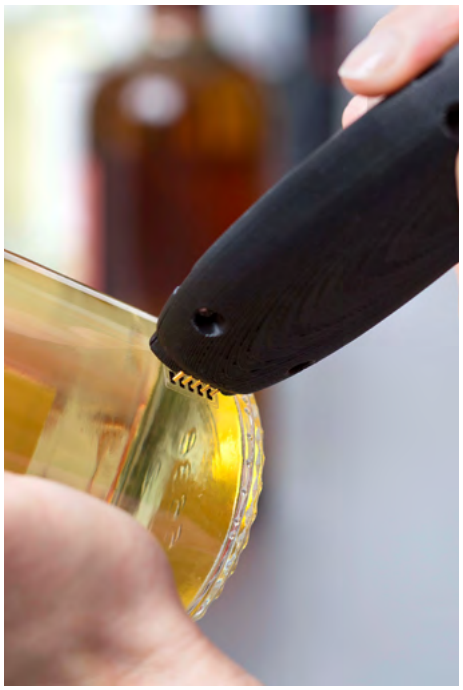
Xerox has worked to make implementation easier for their customers by delivering XPM in recognisable, industry standard formats. Xerox will also develop custom formats for customers as needed.

Reading and writing of data

'The data that is stored is written and read off line with a contact device. Data can also be accessed and uploaded as needed, but to write and read data, the memory device must make contact with the reader,' De Jong said. 'With it, you have 10 year data retention and non-volatile memory.'



Xerox printed memory in web format (left) and in single track rolls (right).



An example of Xerox printed memory being read with a device.

A user reads XPM with a contact reader attached to a smart phone that detects the unique analog signal. The inexpensive reader works offline but uses a smart phone as a display.

Devices can store production codes, channel information, manufacturing data, and other information as well as conform to GS-1 Standards. According to De Jong, Xerox will customise readers as well as XPM. For example, a wine customer may want a reader design very different from a logistics or customs agency.

Further encryption available

For further security, when needed, Xerox adds encryption with a lock and key encryption system using a proprietary algorithm linking a QR code with XPM.

'A combination within the same label could be produced by us or it [XPM] could be added to existing label configuration,' said DeJong. The Xerox reader would read the memory and a smart phone would read the QR code.

XPM is at a price point comparable to some lower cost radio frequency identification (RFID) devices at .09 to .10 USD, with higher volumes meaning potentially lower prices with lower storage capacity devices of course being lower in cost than higher storage ones. What sets XPM apart from RFID is: the higher security for authentication, the low cost of readers and an infrastructure that can be largely developed from smart phones.

Consumables monitoring and remote calibration

Further, because of the low cost of readers, XPM, becomes appropriate and cost effective for use on smart consumables.

'This is for when a consumable interacts with the device. When you stick a label with memory on an item it becomes an intelligent consumable. It is able to interact with a dispensing device with a reader installed.

The reader can read as well as transmit. It can authenticate, count usages, count dates, and collect data. It can even carry calibration data because there are certain devices that need to be calibrated after each use or after ten uses.

Some of them could be diabetes syringes or blood sugar readers which need calibration from time to time,' said De Jong.

An example of Xerox printed memory on a printer cartridge.

From printer ink cartridges and coffee pods to shampoo and paper towels, machines and dispensers can be designed to detect genuine and certified refills giving and original manufacture more control over their consumable product elements.

'With printer cartridges which is close to home for us, the XPM label would make contact and authenticate the cartridge,' said De Jong. A good application identified by De Jong for XPM is as a smart reminder for air or water filters which -whether they be industrial or for home – are usually not changed as frequently as necessary for optimal performance.

With coffee pods, for example, 'in Europe we would not want to discourage competition, but perhaps it [XPM] could trigger some information that could be shown on the tiny display to say 'thank you for using the genuine pods' or other information.'

A flexible platform to build on

Xerox appears to be taking a good approach with their dual path marketing strategy and has poised XPM to be an enabler to make consumables a small but important piece of the 'Internet of Things' as well as creating a very flexible enabler for a product security program.

Xerox leaves the design and development of backend analytics to their customers as the needs between the consumables path — albeit some intersection points exist — and product protection vary greatly.

www.xerox.com

Covert Ink for Fruit and Vegetables

At the recent AUSPACK 2017 event, Digital Ink Technologies Pty based in Melbourne unveiled its *POLYtrust*® UV invisible ink, the world's first edible covert ink for fruit and vegetables.

The technology offers the ability to provide a cost effective anti-counterfeiting solution to print text and barcodes.

POLYtrust is a complete anti counterfeit solution for direct printing onto food, packaging and luxury items. The technology encompasses thermal inkjet technology *Polytij*® and hazardous analysis and critical control points (HACCP) certified edible visible and invisible inks. A fully customisable app is also available that links to a real-time website.

An example of a code printed on an apple using Polytrust UV inks.

Using UV invisible ink and Digital Ink's POLYtij printer, growers apply a code or logo, which the wholesaler or retailer can use to identify when the fruit was picked.

CEO and Managing Director Michael Mahoney said 'the solution gives growers a means to prove freshness, removing the potential need to replace fruit, and lose profit, when freshness could not be proven.'

www.digitalinktechnologies.com.au

Printing Beyond Colour – Clear 'Inks'

By Alan Hodgson

This series of articles that examines technologies for 'printing beyond colour' now moves to consider the threats and opportunities raised by the use of clear inks. We use this term loosely here as these are also available as clear toners.

The purpose of this article is to outline some of the opportunities that may come from these technologies, but also to make you aware of their capabilities in the wrong hands.

The aim of this article is to give an overview of the relevant print technologies that can be used in secure documents with a particular emphasis on raised features, identifying both the printing and authentication aspects of these.

Clear inks – an overview

In the early days of digital colour printing almost all available printers had 4 colours; cyan, magenta, yellow and black (CMYK). This was later extended in some specialist printers to 6 or more channels to encompass spot colours or to increase the printable colour gamut. These options also enabled the incorporation of security features like fluorescent inks in some passport printers.

Around 10 years ago this concept became further extended by the provision of clear inks. To those people more versed in desktop printing, the concept of using an ink with no visible colorants may be a difficult concept to grasp.

But they do find general use in commercial printing as an overcoat to a printed image to provide a better tactile impression, resistance to abrasion and uniform gloss. A good example of this would be in the printing of high quality magazine pages or covers.

These clear inks facilitated a further print capability – the ability to print a surface texture to enhance the decorative qualities of the print. While this capability has been used to some extent in advertising and packaging, there are two areas we should consider from the perspective of security printing.

The first of these is the capability to mimic existing security features and the second is to generate new digitally printed features.

From a security printing perspective many covert fluorescent inks could be considered as clear. Under many lighting conditions they are designed to be invisible and only reveal their presence under selective illumination.

These inks are not covered here but were the subject of a previous article in this series (AN December 2016).

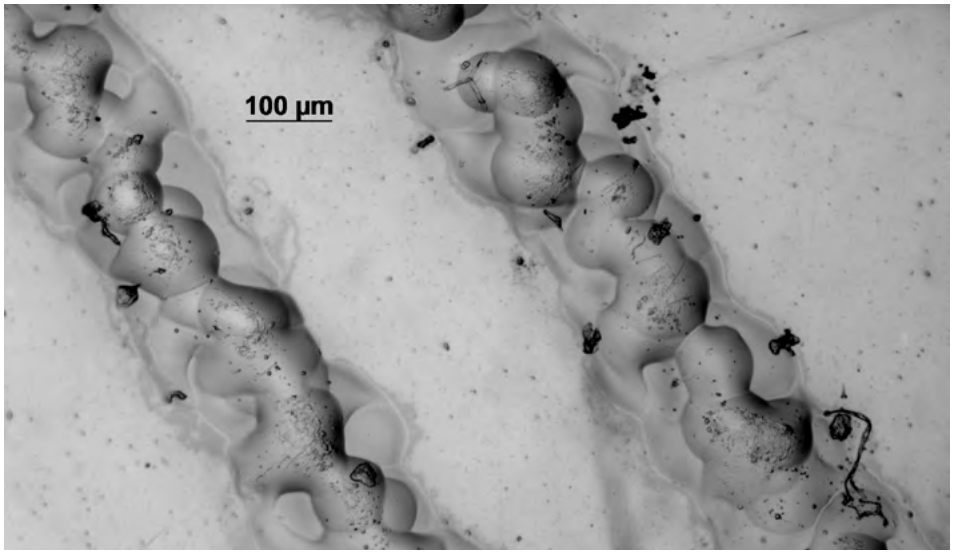


Figure 1 Inkjet printed tactile lines.

An example using clear toner

A good example of this clear ink capability is given by the *Kodak NexPress 2100* colour production printer. The original engine was introduced in 2001, but at the DRUPA printing show in 2004 a 5th printing channel was implemented with the capability of clear toners.

This unit was promoted as having security printing capability for features such as digital watermarking and raised letter printing.

The digital watermarking capability was effectively using the clear toner to modulate the gloss of the print. The use of gloss difference as a security feature is a topic that still has some interesting potential and is planned to be the subject of a future article. The point of interest here is that this advertised 'watermarking' capability has the potential to print a passable facsimile of a true watermark in a paper.

Printing raised features

Although this is somewhat counterintuitive, printing of raised tactile features was something that the older toner printers were much more suited to than more modern units.

This was because early toner formulations contained larger particles, on the order of 10-15 microns. This gave more of a raised tactile feature than more modern toners with particle sizes usually below 8 microns.

The clear toner in the Kodak NexPress 2100 was said to utilise particles around 20 microns for the clear toner and was thus capable of tactile print that is closer to thermography than typical toners.

However, the key difference here is that the image was printed directly from a digital source, giving extra capability for both the origination and copying of raised features.

One further interesting innovation with the NexPress series toner printers was the introduction of 'index based digital texture printing work flow'. This option was being featured in conference papers by 2013 and allowed users of the later generation presses to effectively digitally select a texture as a part of the print job.

This capability utilised the Kodak NexPress Dimensional Clear Dry Ink which can be programmed to produce variable texture heights on a print.

This capability was originally introduced as a decorative enhancement to a print but it has potential implications for security printing too. Texture patterns of up to 28 microns height can be realised in a single pass using this system.

This is an important metric when considering the capabilities of these systems for security printing. Samples of embossed polycarbonate cards and intaglio printed visas were measured for feature height and the results presented at the *High Security Printing™ Europe* conference in 2016. The feature heights were in the region of 15 to 25 microns, so well within the capabilities of these printers to duplicate.

Other printing options

The printing of surface relief is a rapidly evolving field. Additive manufacturing is exploring this and attracting significant research and industrial interest (see AN January 2016). This is leading to a number of print solutions that can produce tactile features that could potentially be used to originate or copy security features.

One important consideration on this is the fact that these additive manufacturing solutions are becoming widespread across university departments. This in turn leads to a steady flow of graduates leaving these groups each year who are trained in their use and capability. The implications of this were considered in an article on tactile features in AN April 2016.

One strong contender to originate and duplicate these tactile features is UV cured inkjet printing. The work the author is conducting with the University of Manchester in this area was mentioned initially in this series of 'Printing Beyond Colour' articles in October 2016 but is illustrated in a wider context here. It was presented at both the *High Security Printing™ Europe* and the IS&T Printing for Fabrication conferences in 2016.

Figure 1 on the previous page shows a microscope image of two lines printed with clear UV cure inkjet ink as a collaboration with Axzyra of Cambridge UK. The lines produce tactile features of around 18 microns in height by progressively building up the feature height from multiple passes. By varying the printing conditions the tactile nature of the surface could also be changed.

This illustration also reveals a significant point with the present generation of inkjet systems. Under moderate magnification, such as the use of a hand lens, the true droplet nature of these prints is revealed. This differentiation will probably not last, driven by the needs of printed electronics (AN February 2016).

This type of work is being conducted across multiple groups and from different directions. The connection with additive manufacturing was highlighted above. But the author also noted similar systems being shown at a Material Appearance conference within the Electronic Imaging symposium earlier this year.

In summary

Clear 'inks', formulated as either toners or inkjet inks, have significant potential within security printing for the fabrication of tactile features. While these formulations could be used to produce a new generation of features, they also have the potential to produce illicit copies of existing features.

It is important to recognise that business drivers external to our industry are facilitating both threats and opportunities in this area. The growing interest in additive manufacturing is resulting in an expanding range of print solutions and expertise that could be used to originate and copy tactile features.

From the Archives

10 years ago

Holospot Provides Multi-Level Solution for Product and Supply Chain Security

Authentication News® reported that Tesa scribos of Germany had launched its new multi-level holographic anti-counterfeiting and track and trace technology to the UK market called *Holospot*®. The new product enabled brand owners to identify and trace their products through a series of authentication levels containing both overt and covert information. According to the company, the technology was already delivering benefits to the cosmetics and auto-motive sectors.

Holospot was based on the principle of marking each product or the packaging with a miniaturised self-adhesive label incorporating a holographically-generated structure that contained four levels of information.

Four security levels

Level 1 comprised up to four numerals of diffractive text that changed colour according to the viewing angle and was viewable to the naked eye.

Level 2 comprised diffractive variable micro-text or micro-images that could be viewed under a magnifier.

Level 3 was a projection hologram containing analogue information and could only be read within the viewfinder of a laser-magnifier.

Finally, Level 4 contained encrypted digital data that was readable only with a digital reading device.

The first level was intended for consumers, the second and third levels for retailers and administrative authorities (such as customs, trading standards offices and investigators), whilst the fourth level was reserved for use by brand owners themselves.

Unique signature

Each product was given its own signature to enable authentication and identification of each product at every stage of the supply chain – from manufacturer through customs to stock control.

Data was written to Holospot in a real-time production environment using tesa's proprietary laser-lithographic system linked to a database of production information. Tesa also provided the labelling machines, the laser/viewing device so that users could have immediate access to the lower levels of data, and the digital in-line reader that linked to the manufacturer's database. According to the company, the residual cost of each Holospot label was €0.02-0.05.

The origins of Holospot technology were founded on the ability of PET adhesive tape produced by tesa scribos' parent company tesa AG both to store a large amount of information in holographic form – up to 1 Kb per Holospot – and to adhere to most materials including textiles, cardboard, glass, metal and plastics. Data and graphics could be placed on surfaces as small as 5mm in diameter. The information was then recorded into the depth of the polymeric material as opposed to the surface to prevent damage and contact copying. Once recorded, the data was irreversible and stable over time in a variety of environmental conditions.

Tesa scribos was founded in 2001 to commercialise the Holospot technology, following a €10 million investment by tesa AG, one of the world's largest manufacturers of self-adhesive products. Sales in 2005 were €5 million. Today Tesa Scribos has grown and developed a suite of products that includes *tesa® connect & check, tesa PrioSpot®, tesa VeoMark, tesa® SecurityPrint, tesa® SecuritySealing* and *tesa® trust & trace.*

Tesa Holospot.

Nexus Launches User Authentication with Swedish BankID as a Cloud Service

Swedish-owned Nexus Group, the product company developing identity and security solutions, recently announced the launch of user authentication with *Swedish BankID* as a cloud service which will eliminate passwords.

Swedish BankID is an electronic identity (eID) that is comparable to a driver's licence, passport and other physical identification documents, enabling organisations to identify individuals in web services, mobile web services and mobile applications.

7.2 million Swedes use BankID, and it is by far the most popular eID in Sweden. Previously it has been difficult and expensive to integrate authentication with BankID in user portals, but with the new cloud service from Nexus it's incredibly easy and cost effective, says Malin Ridelius, product specialist at Nexus.

Nexus acts as the so-called relying party for BankID, which means that Nexus handles all costs and contracts towards the BankID selling bank.

The system uses *Nexus GO*, which is an online portal and self-service platform that makes it easy, fast and cost efficient for all kinds of organisations to deploy advanced solutions for authentication, digital signing, identity management, Internet of Things (IoT) security and physical access control products. This is then integrated for users to then log in with Swedish BankID.

Nexus GO Authentication with Swedish BankID suits organisations that currently allow their users to identify themselves with a username and password, and also organisations that do not yet have any citizen or client portal.

Nexus GO Authentication with Swedish BankID fits organisations of all sizes, but for small organisations, this service is completely revolutionary.

A small online shop could previously only dream of offering their customers login using BankID, because it was too difficult and cost too much to install a solution on-site,' says Ridelius.

'We will soon make it possible to integrate authentication with other countries' electronic identities, and we will also release a range of other services for digital signing, IoT security and access control products,' says Gustaf Broman, Product Manager for Nexus GO.

Nexus GO Authentication with Swedish BankID is the first service to be launched in Nexus GO, where Nexus technology will be made available as a service.

www.nexusgroup.com

RECONNAISSANCE AUTHENTICATION NEWS®

Publisher: Reconnaissance International Ltd.
Editor: Mark Deakes (right).
Contributors: Alan Hodgson, Astrid Mitchell, Randall Burgess.

Annual subscription rate: £575 *plus £25 per year for postage*
Subscribers to Holography News, Tax Stamp News or ID & Secure Document News (20% discount).
Ask about multiple/corporate subscriptions.

The editorial team welcomes your news, contributions and comments.
Please send these to **publications@reconnaissance-intl.com**

10 Windmill Business Village, Brooklands Close, Sunbury, TW16 7DY, UK
Tel: +44 (0)1932 785 680; Fax: +44 (0)1932 780 790

www.authentication-news.com

Events

26–28 APRIL 2017
ID4AFRICA 2017
Windhoek, Namibia
www.id4africa.com

1–3 MAY 2017
ID:CONNECT
Washington DC, US
www.connectidexpo.com

19–21 JUNE 2017
HIGH SECURITY PRINTING LATIN AMERICA
Guatemala City, Guatemala
www.hsp-latinamerica.com

26–28 JUNE 2017
SDW 2017
London, UK
www.sdwexpo.com

04–06 JULY 2017
WATERMARK CONFERENCE
Ekaterinburg, Russia
www.watermark-conference.com