RECONNAISSANCE
AUTHENTICATION NEWS®

VOLUME 22 – NO 6 / JUNE 2016

Smartphone Authentication for Banknotes and Tax Stamps

Spectra Systems – the US-based manufacturer and developer of secure taggant materials, hardware and software to authenticate and process banknotes and other secure products – has developed *TruNote*™ and *TruStamp*™. These two solutions consist of a smartphone-based physical authentication feature for banknotes and tax stamps respectively, that requires no special phone attachments.

TruNote enables smartphone-based authentication of banknotes by utilising covert signature materials embedded in either the paper substrate or print of paper and polymer banknotes. The materials are analysed and 'read' on a smartphone, using an Android- or iOS-based app.

The app can be voice-controlled for the visually-impaired to check whether the note is authentic, and the denomination of the note can also be read out. In addition, the app can be configured to report GPS locations of suspect banknotes to the central bank.

The authentication process is ideally performed in real-time through a wireless link to a secure server, in order to prevent criminals from analysing the smartphone-embedded program and discovering the authentication algorithms used.

On personally testing this feature, several times whilst blindfolded – using banknotes both with and without the embedded covert material – the author found that the feature worked perfectly every time. In each case, the feature either read out the correct denomination or indicated that the note could be suspect.

TruStamp for tax stamps

As a similar technology to TruNote, Spectra Systems has also developed TruStamp, to provide smartphone-based authentication of tax stamps for tobacco, spirits and other taxable items. The secure covert materials can be embedded into paper substrate, print, or added during the construction of holographic tamper-proof labels.

Continued on page 2 >

Micro-Tracers: Ingestible Taggants for Pharmaceuticals

Micro-Tracers Inc has extended its range of analytical tracers to include ingestible, on-product solutions for pharmaceuticals, in response to a growing need to protect the products themselves, and not just their packaging.

The WHO has estimated worldwide sales of counterfeit drugs at over $75 billion per year. Not only has this resulted in lost revenue for proprietary drug manufacturers but also caused adverse health effects for end consumers, including as many as 1 million preventable deaths per year.

The pharmaceutical industry has responded by utilising enhanced packaging – RFID tags, holographic labels, track-and-trace systems – to differentiate authentic from counterfeit products. However, counterfeiters can replicate, mimic, or reuse packaging, rendering these security features meaningless.

Also, in many parts of the world, drugs are commonly sold outside of their original packaging. Hence the need for a security solution that can be applied directly to pharmaceuticals themselves.

Tracers, also known as taggants, have been utilised by the formula feed and other industries and remain the most viable solution for on-product pharmaceutical security.

Tracers are micro-sized particles that can be added directly into the formulation of proprietary products to differentiate those products from counterfeits. To be successfully used in pharmaceuticals they must be difficult to replicate, affordable to produce, detectable at low levels, easy to identify, safe to consume, and non-reactive with active components.

Continued on page 2 >

Inside this Issue

Smartphone Authentication *(Continued)*

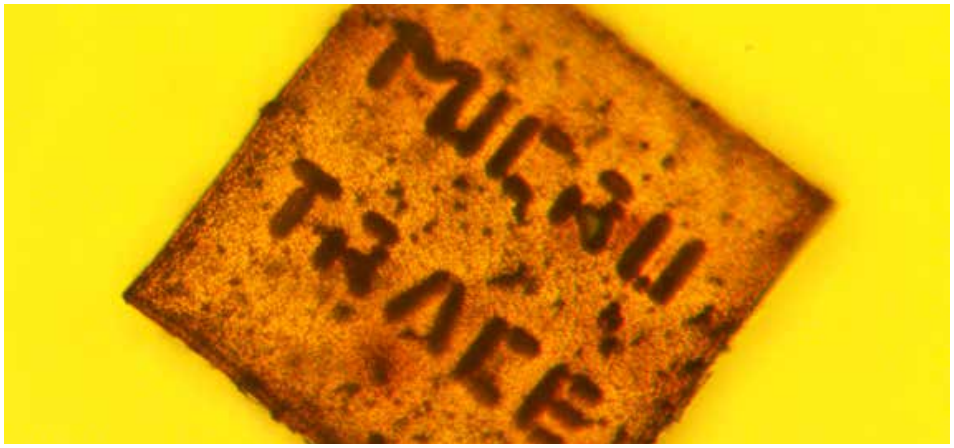
The TruStamp app has QR-capture capability to support track and trace GPS software. Products and individual items can thereby be followed along the legal supply chain in order to identify at which point they are diverted into the illicit distribution chain, as well as to aid in the investigative process.

Other characteristics of the covert material utilised in both TruNote and TruStamp include its robust physical and chemical durability, its ease of integration into existing production processes and, of course, its ease of authentication by way of a smartphone – as opposed to a separate bespoke device or special smartphone attachment.

Enquiries may be emailed to: **info@spsy.com**.

www.spsy.com

Micro-Tracers *(Continued)*



SECUR micro-engraved tracers

Micro-Tracers Inc, located in San Francisco, US, was founded in 1961 by Dr Sylvan Eisenberg, a PhD graduate from Stanford University. The company claims to be unique in that its primary focus is on manufacturing analytical tracers for quality assurance for the formula feed industry. Now the company has extended its product range to cover pharmaceuticals and other edible products such as branded foods.

SECUR micro-engraved tracers are extremely small particles that have been micro-engraved with lettering, or other data such as a batch number or date of production, to act as a tracing and anti-counterfeiting mechanism. They are magnetically attractable and fluorescent, making them easy to isolate and identify.

The particles are comprised entirely of food and pharma-grade GRAS (generally regarded as safe) materials. They are chemically inert, non-digestible and added at an extremely low rate (recommended level 20ppm). The particles can be included in pills, coatings, and labels, depending on the most appropriate method for the product.

Now that the FDA has issued a guidance document for 'physical-chemical identifiers', tracers can be included in drug products in the United States, in some cases without prior approval (as was the law in the past).

Identification and authentication

A very small and inexpensive kit (ie. $15) is available from Micro-Tracers to identify the tracer. If formulated into the coating of a pill or capsule, identification – without the need to destroy the product – is possible. Shining a black light over the pill or capsule will cause the embedded food dye within the tracer to fluoresce. The lettering on these particles can then be read using a small, hand-held microscope.

If included covertly within a drug, the pill or capsule should be ground to powder first, with the tracer isolated from the powder using a magnet.

The black light and microscope can then be used to authenticate the particles and thus the drug they were contained in.

The process takes roughly 30 seconds if included in the coating of a pill/capsule, or 3 minutes if formulated into the pill/capsule itself.

A brand name with meaning

The brand name for the product – SECUR – has meaning. SECUR is derived from:

S – Safe for human/animal consumption

E – Easy to identify

C – Customisable message

U – Useful variety of purpose, eg. authentication, track and trace and returned product validation

R – Reliable

Key differences compared to other solutions

According to the company there are several key differences between SECUR micro-engraved tracers and other taggant solutions. The most important difference is that SECUR tracers are affordable, with the tracer being added in such low quantities that the cost is trivial compared to the value of the drug.

In addition, although the tracers are derived from patented proprietary processes, the company's detection apparatus is not proprietary. Indeed most drug enforcement officials are likely to already be in possession of a microscope and a black light adequate for this purpose, which makes the solution easy to use, affordable, and usable in regions of the world with limited access to internet.

Micro-Tracers is part of a group that includes Anresco, Inc, a commercial analytical laboratory providing analytical, consulting and research services to the food industry.

www.microtracers.com

www.securtracers.com

Global Trade in Fakes Approaching Half a Trillion – What Can be Done?

By Sven Bergmann, Venture Global Consulting

In April, the Organisation for Economic Cooperation and Development (OECD) released an updated report that puts the value of imported fake goods worldwide in 2013 at $461 billion (see AN May 2016). This marks a significant increase compared to the OECD's 2008 study, which estimated the illicit trade in fake goods at approximately $250 billion. Fake goods now make up 2.5% of the $17.9 trillion overall world trade.

The OECD is a non-partisan, non-governmental organisation, which provides a forum for 34 members and more than 70 non-member economies to promote economic growth, prosperity, and sustainable development. OECD provides a setting where governments can compare policy experiences, seek answers, identify best practices and coordinate policies.

OECD started to study the economic impact of the importation of counterfeit and pirated goods in 2008 to help provide a measure of the activity, as well as provide data for policy and solution developments for governments.

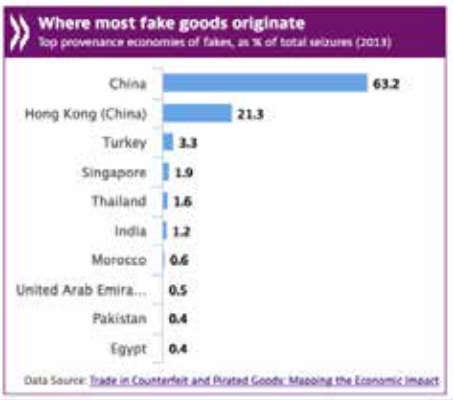
In this article we will examine the key findings of the latest OECD report on the implications of a counterfeit trade worth nearly half a trillion dollars. This number is truly staggering. It is the equivalent of the GDP of Austria, or the combined GDP of Ireland and the Czech Republic, as the authors of the report point out.

We will also examine key changes, trends and the drivers behind the increase, as well as implications for the authentication industry.

Key findings

The report analyses nearly half a million customs seizures around the world – from 2011 to 2013 – which have allowed the OECD to build a robust quantitative estimate of the counterfeit trade. The report covers physical counterfeit goods, which infringe trademarks, design rights or patents, as well as tangible pirated products. It does not cover online piracy, which further negatively impacts businesses and world economies.

The United States, Italy, France, Switzerland, Japan and Germany are the hardest hit countries, with the majority (83%) of fake goods originating (not surprisingly) from China and Hong Kong.



Source: www.OECD.org

European brands are among the most impacted, with an estimated 5% of all goods imported into the European Union (EU) being fake. This represents as much as $118 billion.

The OECD found fake products permeating virtually all categories, from luxury goods – like watches, leather goods and perfume – to industrials such as machines, spare parts and chemicals. The OECD also identified fake goods among common consumer products, including Consumer Packaged Goods (CPGs), toys, pharmaceuticals, cosmetics and even the trademark infringement of fruit producers.

Even more concerning, many counterfeit products classified as consumer safety and critical technology products – such as pharmaceuticals, spare automotive parts and toys – are often of low quality and endanger consumers' health and safety. Some fakes can even cost lives.

The OECD report also affirms that the five most counterfeited items continue to be footwear, followed by apparel, leather goods (which includes handbags), electronics and watches. The proceeds from counterfeits continue to fuel other illegal activities of criminal networks such as money laundering, drug and human trafficking and even acts of terror.

Key trends and drivers

The irony of the OECD report is that it is based on seizures as a percentage of legal exports. The report uses seizures as a proxy to 'see' into the hidden and clandestine world of illicit trade. And increased seizures point to increased counterfeits. But increased seizures also point to increased enforcement (or at least constant enforcement) against a growing issue.

Some might ask whether there is not enough being done to address counterfeit goods? But the better question is: Are the right things being done? The OECD report highlights some key aspects that are fuelling this increase:

- An expansion of counterfeit goods beyond big-name brands across virtually all industrial sectors, shipped across complex global networks;
- Increased counterfeit sales in primary and secondary markets;
- The shift of counterfeit distribution to small parcels.

As OECD Deputy Secretary-General Doug Frantz stated, 'this report contradict(s) the image that counterfeiters only hurt big companies and luxury goods manufacturers'. Instead, counterfeit goods are affecting manufacturers big or small.

Advances in cheap manufacturing and excess manufacturing capacity in countries such as China have led to almost unlimited potential to counterfeit any item or product. If the product has consumer demand, it will be counterfeited.

The OECD report also points out that counterfeit goods have penetrated primary and secondary markets. In secondary markets, also known as aftermarkets – which can include flea markets, online platforms and street sales – sellers expect, or even willingly search out, counterfeit goods. In primary markets, on the other hand, consumers are normally deceived and defrauded to believe the goods are genuine.

While the OECD report does not identify how much of the counterfeit trade flows through primary versus secondary markets, this has significant impact on how the security and authentication industry, and the brands it serves, attack this issue.

The illegal trade in counterfeit goods has become an intricate global network and a menace of historic proportions. While most fakes originate from China or Hong Kong, they use complex shipping and trading routes, which trans-ship freight through the Middle East, Eastern Europe,

Continued on page 4 >

Global Trade in Fakes – What Can be Done? *(Continued)*

Africa and free-trade zones in the United Arab Emirates, to disguise the origin of merchandise and minimise suspicions.

Even more concerning, transit points now include countries with weak governance and a strong presence of organised crime or even terrorist networks, such as Afghanistan or Syria. The criminals trafficking counterfeit goods change their shipping routes often to avoid detection and swiftly exploit weak spots in global distribution chains.

The most important change and development however, has been the migration of shipments to small parcel shipments. These include express consignments, postal parcels and international mail, and are now the primary method for shipping fake goods.

During 2011–2013, 62% of all seizures were small parcel shipments, reflecting the growing importance of online commerce in international trade, and the shrinking costs of shipping counterfeit goods globally in small parcels. This trend decreases the risk of detection, detention and seizure for the criminal distributors of counterfeit goods, while simultaneously complicating and frustrating enforcement efforts.

Implications for the authentication industry

The authentication and security marking industry has a great opportunity to capitalise on these trends by developing and deploying more standardised solutions to brand owners, law enforcement and investigative firms, to better combat changes in the illicit trade of counterfeit goods.

When counterfeit goods enter the primary market, anti-counterfeit and authentication tools are needed that enable consumers to simply, easily and reliably verify the authenticity of the goods.

Today's approach for such anti-counterfeit authentication has two major faults. It relies too heavily on overt security features, and technology approaches are so divergent that it is hard for a consumer, law enforcement and investigative firms to be educated and proficient on all these technologies.

Unfortunately, all overt technologies can be imitated to look like the real thing, even if it is only for a short time. But that's all the counterfeit authentication device needs to do – survive a cursory inspection by unsuspecting consumers.

Seized overt counterfeit authentication technologies run the range across all overt features. Counterfeiters will imitate holograms, cut-lines, colour-shift inks, intricate print patterns and others. If it can be seen as an overt feature it will be imitated or counterfeited.

While industry experts will recognise the imitated features as a counterfeit, they are good enough to pass the 'inspection' of consumers. Some authentication features are replicated so well that even law enforcement has a hard time authenticating them.

Online sales of counterfeit goods make these anti-counterfeit authentication features completely ineffective, since the consumer will not be able to inspect until the shipment is received.

What additionally is complicating authentication is the plethora, breadth and inconsistency of authentication features. Because there are so many potential features, how are law enforcement, investigators and consumers supposed to know which feature to look for? Overt or covert? Is it a hologram or colour-shift ink? Is the ink supposed to shift from green to red or blue? What is the correct placement of the security cut-lines? What covert feature do I scan for? Which scanner do I use and where on the item is it?

There is a great opportunity to provide simple, consistent, consumer-centric authentication features, which allow consumers, through broadly available non-custom technology, to verify the authenticity of items, such as the verification of encrypted product serial numbers via smartphone scan, text message or phone call. Smartphone apps, texting and calling are commonly known technologies and the consumer learning curve is very short. While not perfect, it is one example of a simple consumer-focused authentication method.

Consistent standards would also help law enforcement and investigators. During my many tours of US ports, enforcement officers often reported having a hard time to stay on top of the various covert technologies and the proprietary scanners, readers and sensors required. As a result, law enforcement is not utilising many covert features, but rather relying on other determination factors, such as packaging or shipment methods.

For example, during a recent visit to the JFK international mail port, officials highlighted the seizure of dozens of high-quality counterfeit luxury hand watches, which were identified by the fact that ten of them were shipped in a simple cardboard box. Considering the watches have a retail price of over $20,000 each, the customs officer rightfully concluded that genuine watches of that value would probably not be shipped that way and seized the shipment as counterfeit. Many overt security features had been replicated and the customs officer was unsure of the covert features.

The industry has an opportunity to rally around a select, consistent and uniform number of covert features, which allow simple authentication for law enforcement. Taggants and IR inks are two examples of covert features, which are rarely imitated. These agreed upon features should be unified by common ISO standards, which would then enable law enforcement and investigators to authenticate a variety of technologies with ideally one reader, scanner or sensor.

These issues become worse for counterfeit sales in the secondary market. In those markets, consumers are accepting counterfeit goods or are potentially even seeking them out. Overt features are, unfortunately, a waste of money and effort here.

Living in a college town, I have seen first hand the many counterfeit jerseys worn by college students, who swap information on the best websites for good counterfeit. Well-replicated overt features are used as a sign of high-quality counterfeit goods and advertised on the online sites themselves. Here also, the key to making progress against secondary counterfeit markets are standardised covert features, to help aid law enforcement and investigators, before these goods ever reach the consumer.

In summary, there are too many different authentication technologies in use today. Law enforcement, customs officers and even investigators are unlikely to be familiar with (and possess all the necessary tools to validate) every type of authentication device that comes their way. In addition, much effort is spent on 'flashy', exciting or complicated overt features. However, all features, if visible, can be counterfeited or imitated.

While many authentication technologies try to out-compete each other with complexity and novelty, I wonder if the key to better anti-counterfeit enforcement isn't the standardisation of a few key covert features and to focus our efforts on making those as good as possible, with universal readers, smartphone apps and other verification tools.

The future of anti-counterfeit technology or authentication technology, in this author's mind, is simplicity, focus and standardisation, to enable rapid and quick enforcement against increasingly small shipments. This can be achieved through voluntary industry standards, ISO standards, or mandatory technology requirements by governments or the World Customs Organisation.

Sven Bergmann is a Managing Partner at Venture Global and advises brand owners, technology providers and governments on anti-counterfeit strategies, programmes and technologies. Send your comments to **SBergmann@VentureGlobalCo.com**

Today's Authentication Methods for Documents and Products

Part 6: Offset Security Printing

Last December, *Authentication News*® began a series of articles on the characteristics and functions of the different groups of authentication features used to protect today's documents and products.

So far, we have covered four groups of authentication devices that are carried in the document substrate: watermarks, threads, embedded particles (such as fibres), and windows.

We now move away from substrate-borne features, to focus our attention on security printing processes, where we examine the role such processes play in the authentication of documents and products.

The majority of high-volume printing technologies are also used in security printing, to some extent, with only gravure being the exception. However, the two most commonly used and most important technologies are offset and intaglio, with the latter being more exclusive and mainly reserved for banknotes and other high-security documents.

Other printing technologies (that will also be covered in this series) are letterpress, silkscreen, flexography, inkjet and sublimation. These are traditional methods in that they all use ink in one form or another. Another technology is laser 'printing', which is increasingly being used for security features, especially those on polycarbonate cards for passports and IDs.

It should be noted here that some printed security features depend not so much on the printing process as on the inks used for printing. Perhaps the best-known example of this is optically variable inks, which can be printed in silkscreen or intaglio. In this case, as well as in other similar cases, such features will be dealt with in their own separate chapter, although they will also be mentioned in the relevant chapters on printing technologies.

Offset printing

Undoubtedly the most universal form of security printing is offset (or – as it is sometimes called – offset lithography, offset litho or just litho printing).

However, offset printing is also a commonly used printing method for general printing as well as security printing, so it is, in effect, a non-exclusive process. But just as Formula 1 racing cars and family saloon cars both possess wheels and an internal combustion engine – yet have very different capabilities – so too do commercial offset machines and machines designed for very high-resolution security printing.

There is another factor, however, that allows some commercial offset machines to produce security documents, and that is the use of special design and prepress techniques.

But before getting into the sophisticated aspects and techniques of offset printing, it is useful to take a quick look at its history and how it got to where it is today.

The first offset presses

Lithography was initially developed as a cost-effective method for reproducing artwork. The original process used flat, porous surfaces, given that the printing plates were produced from limestone (the word 'lithograph' historically means 'an image from stone' or 'printed from stone').

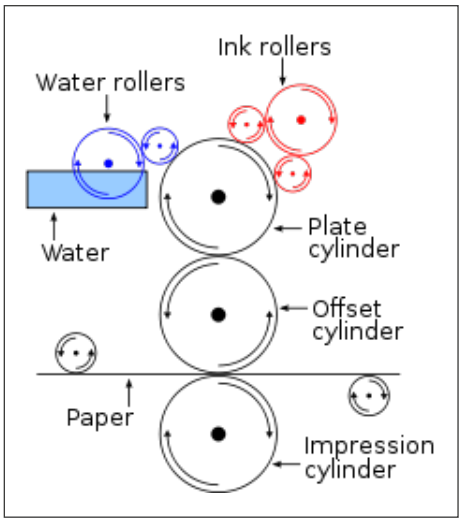
In 1875, Robert Barclay in England developed and patented a machine that used a transfer technology and also incorporated the principle of Richard Hoe's rotary printing press of 1843, which used a metal cylinder instead of a flat stone. The 'offset' cylinder was originally covered with specially treated cardboard that transferred the printed image from the stone to the surface of the metal cylinder. This process was used in England to print tin.

Then in 1901, Ira Rubel in New Jersey, US, who along with many others was using the litho process to print books, photographs etc., discovered that printing from a rubber roller, instead of the metal cylinder, produced a print that was clearer and sharper. It was this discovery that led to the establishment of the basic technology for offset lithographic printing, and machines incorporating this technology quickly became available.

Modern offset printing

Offset printing machines today are either sheet-fed or web presses. Web presses are used for very high volumes of commercial print such as newspapers and promotional brochures, whereas sheet-fed presses are used for lower volumes – and security printing.

Whereas web presses print both sides of the substrate in one pass, sheet-fed presses can either print one side only or they can perform what is called 'perfecting'. Perfecting occurs when both sides of the sheet are printed in one pass, but not simultaneously.



Security printing with offset.

There exists, however, an exception to this 'rule', in the shape of the *Super Simultan* high-resolution security printing press manufactured by KBA-NotaSys. Although a sheet-fed press, the Super Simultan is able to print both sides of the sheet simultaneously, thereby avoiding any distortion of the paper between printing first one side and then the other.

The other high-resolution offset press – the *LC32* from Komori – conventionally prints both sides of the sheet without turning it, but by using precisely engineered, double-sized transfer cylinders and grippers to transport the sheet, using the same grip edge of the paper, very accurate register is achieved.

Offset is usually based on the printing of four colours per side to enable full-colour images or specific colours. In addition, high-registration security offset presses, such as those produced by KBA-NotaSys and Komori, offer extra cylinders for special inks or features. The Super Simultan can print six colours on one side and four on the reverse, and the LC32 can print up to six colours on both sides.

Both web and sheet-fed offset machines use the same basic technology for the application of the print to paper or other substrates (see diagram above).

The plates used for the image can be produced by two different methods.

The first method consists of the photo offset process, which uses light-sensitive chemicals and photographic techniques to transfer images and indicia from original materials to the printing plate.

Continued on page 6 >

Part 6: Offset Security Printing *(Continued)*

The second method consists of the direct transfer of data in digital form from a computer to the plate (CTP systems). The latter method is much more common today.

The offset printing process consists of the inking system (ink fountain and rollers), the damping system (water fountain and water rollers), the plate cylinder, the offset or blanket cylinder and the impression cylinder.

Ink is transferred to the substrate in a series of steps. First, the inking and damping systems deliver ink and water to the offset plate covering the offset cylinder. Then the ink (image) on the offset plate is transferred to the blanket covering the offset cylinder. Finally, the ink (image) is transferred from the blanket on the offset cylinder to the substrate, which is pressed against the blanket by the impression cylinder.

High-quality offset presses are equipped with a sophisticated inking system able to deliver ink in a very precise and uniform manner that is controlled electronically from a console.

The principle of the offset process is that the lithographic plate, as in the original process of the 19th century, has both water- and ink-receptive areas. A layer of moisture is applied to the non-image areas so that the ink only adheres to the image areas on the plate.

However, in addition to the standard, or wet, offset print process, there is a dry offset process that is used frequently in security printing. This process uses a photopolymer relief plate instead of the wet offset plate, with the ink being transferred from this plate to the rubber blanket on the offset cylinder and from there to the substrate, through the action of the impression cylinder.

Waterless printing is a new development that is becoming more popular as this method can give the quality of wet offset but eliminates the use of fountain solution and alcohol, which results in sharper print and fine line reproduction.

Whether the offset press being used to produce a security feature is a good commercial press or a very high-resolution press designed for printing banknotes, passports or other high-security documents, it is important to understand that the security feature will only be as good as its design and origination, which requires specialised knowledge and design and pre-press equipment. The press can only produce what is provided on the printing plates, and only then if it can achieve the quality of print and resolution required by the security designs.

Some security documents only feature what are obviously security designs with no obvious features or images (some bank cheques would be a good example).

On the other hand, documents such as banknotes are designed to carry obvious images such as portraits, buildings, and landscapes, and security can be built into these images, as an accompaniment to other security features placed elsewhere in the design.

Security features

The following are examples of common security features created by the offset printing process:

- **Microprinting** – this is the most common security feature in the offset process. Microprinting consists of recognisable patterns or characters on a printed medium, which cannot be distinguished by the human eye and which require magnification to be read.

  The higher the resolution of the offset press, the greater the security offered by the microprint. To the unaided eye, the text may appear as a solid line. Attempts to reproduce microprint using generally available methods and equipment, such as photocopiers and scanners, will result in a dotted or solid line, as such methods cannot identify and recreate patterns to such scale;
- **Deliberate error** – this is a method of enhancing the security of offset features, such as microprint. Deliberate errors have been used to great effect in many secure documents, in particular cheques, where repeat patterns of microtext are used as the background.

  If the method used to create a counterfeit involves origination, it is highly unlikely that the deliberate error will be spotted and incorporated in the counterfeit document, as it may be as simple as one missed letter or a misspelt word in a repeated name, such as ‘Banclays’ instead of ‘Barclays’. Those involved in authenticating the document would be aware of this security feature.

  Deliberate errors are not just confined to microprint: the ‘mistake’ or fault can be incorporated into any graphic design;
- **Rainbow printing** (sometimes called split-duct printing) involves using a technique in which two or more inks are subtly applied on one printing plate, to create a gradual colour change where the inks merge into one another. This effect cannot be reproduced accurately by digital printing. The feature can be composed of fine lines, text or microtext, or a graphic design.

Example of rainbow printing as a background print.

- **Guilloche** – this is a graphic element in the form of a complex geometrical pattern of repeated thin curved lines (often composed of microprint), formed according to certain mathematical rules. Guilloche elements form rosettes, frames, borders, vignettes and elements of a security pattern. Guilloche lines can be both positive and negative and can be printed in a specific colour or using rainbow printing.

  The design of guilloches should be such that they are difficult to copy, and is therefore best achieved with specially designed software and pre-press techniques for security printing. When copied by digital means, guilloche patterns can become blurred as the lines lose their straight edges, and moiré patterns can appear – the copy will not be clean and clear like the original. The higher the resolution of the printing machine, the greater the security of the guilloche patterns, as they become much more difficult to copy by any printing method.

Example of complex guilloche pattern.

- **See-through** – this feature is printed partly on one side of a sheet and partly on the other side. When the sheet is viewed in transmitted light, both parts match up and create a complete image without overlapping and gaps. As with other offset security features, the greater the design and pre-press capabilities, and the greater the resolution of the printing press, the finer and more complex the individual parts of the design.

See-through feature on euro banknote – only achievable on very high-resolution offset press.

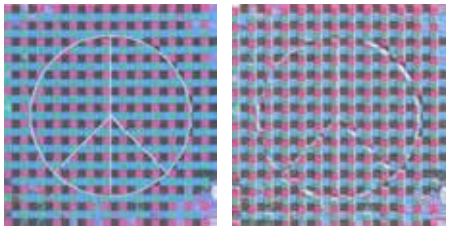
- **Precise registration** – some security features for banknotes and passports are deliberately designed to require precise registration so that they can only be produced on very high-resolution machines.

  There exist two such offset machines for banknote and passport production – one produced by Komori of Japan – the *LC32* – and the other by KBA-NotaSys – the Super Simultan. As indicated above, both print the sheet in one pass.

  These high-security presses have a resolution of around 10,000 dpi, compared with around 6,000 dpi for the best commercial machine.

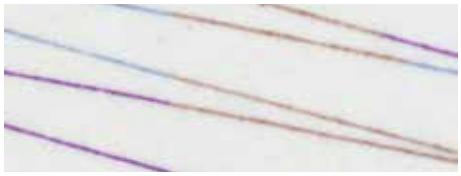
- **Negative white line feature** – this involves producing a white negative image by excluding ink from the substrate. Only a very high-resolution press can produce such a feature in negative fine lines. The below images compare the high-resolution version with the same plates used on a commercial offset press.

  It is commonly known that the eye can immediately pick up the slightest inaccuracy of a circle, or multiple circles within a circle – and this type of feature has been produced in negative white lines to demonstrate the registration ability of the KBA-NotaSys Simultan press.



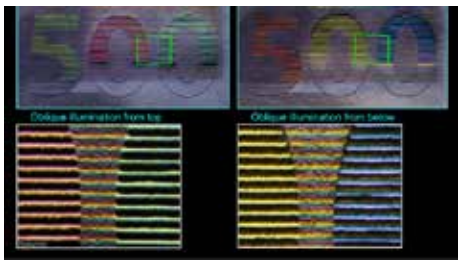
Negative white lines produced on Super Simultan high-resolution (left) and same feature produced on commercial offset press.

- **Adjacent line alignment** – this involves the precise registration of different coloured thin lines – preferably in a line structure where it is immediately obvious that the multi-coloured lines should be continuous.



Adjacent coloured lines in perfect register.

- **Latent image** – this feature combines offset and intaglio processes in precise registration with one another. The latent image is only viewable at the angle where the blind embossed intaglio allows the offset printing to be seen. This is a low-cost but easily seen authentication feature.



Example of latent image.

- **Precise registration with visible/ fluorescent inks** – this involves a development called *SUSI Flip*™ by KBA-NotaSys, where a range of inks involving both daylight and fluorescent colours are used in precise register, so that an image in daylight can appear as a different image in UV.

  An example of this is shown below where a bi-colour design in daylight switches to a three-colour design under UV – an effect which requires the use of four plates.

SUSI Flip: a bi-colour image in daylight switches to a three-colour image in UV.

Conclusion

Offset printing continues to play a major role in both general security printing – for items such as cheques, vouchers, tax stamps and licences – as well as in documents requiring a very high level of security, such as banknotes and passports.

Certain aspects of the offset process, as illustrated above, have been developed to provide security against digital copying.

However, as digital printing continues to progress, commercial offset printing, on its own, will not provide sufficient security to prevent counterfeiting.

Even the high-security offset presses are currently being challenged as some offset print features can be closely simulated – although this is not yet the case for those features, mentioned above, which are reinforced with additional technologies such as intaglio printing (in the case of latent images) and UV inks (in the case of the SUSI Flip solution).

These reinforced technologies, as well as other technologies that combine offset printing with features such as micro-optics holography, micro-mirrors, and magnetic colour-shift inks (to name but a few) will continue to play a very important role in the authentication of documents and products for many years to come.

From the Archives

10 years ago...

Interactive Security from G&D

Authentication News® reported that Giesecke & Devrient (G&D) had launched a new security feature – *FEEL*®. According to the company, FEEL's combination of optically variable effects with colour change by touch offered the banknote industry the first truly interactive feature of its kind.

FEEL utilised thermochromic inks that underwent a clearly visible colour shift when exposed to heat. Although the basic technology was not new, its use for high-security documents had been prevented because of insufficient durability and widespread commercial availability.

G&D overcame the issue of durability by developing a new series of pigments that could be printed by intaglio. The issue of security was also overcome by combining the ink's thermochromic properties with G&D's *STEP*® feature to create a multi-layered optically variable device that changed colour by touch.

Two variants of FEEL were developed – *FEEL Classic* and *FEEL Rainbow*.

In FEEL Classic, covert information was printed with litho, over which a layer of thermochromic ink was then applied via intaglio, which also embossed a design or image. This was then coated, via silkscreen, with G&D's STEP optically variable ink.

Tilting the note resulted in a distinct colour change, while rubbing the rear of the feature revealed the hidden information printed in litho.

In FEEL Rainbow, a specific mixture of liquid-crystal thermochromic ink and G&D's STEP ink was applied by silkscreen on a dark background, with subsequent individualised information added via laser printing.

When tilting the note, again a distinct colour change was visible. When the reverse of the note was touched, the hidden information was revealed in a rainbow-like appearance.

Later, G&D extended the FEEL product portfolio to the identity market with *FEEL-ID*.This product was developed for use in all kinds of ID documents, including national ID cards, driver's licences and passports with a polycarbonate or *PECSEC*® datapage (PECSEC was G&D's laser-engravable passport data page).

2016 Anti-Counterfeit Award Winners Announced

Seven winners have been recognised in this year's Global Anti-Counterfeiting Awards (GAC), which were announced on 8 June, on the occasion of *World Anti-Counterfeiting Day 2016*.

The competition – now in its 18th year – reflects 'the continuing development of the campaign to combat the international trade in fakes,' said the Global Anti-Counterfeiting Group (GACG), which runs the event.

The awards were judged by delegates from *Managing Intellectual Property* magazine, GACG network members and representatives of previous winners.

The list of winners – announced at the Museé de Contrefaçon which is housed at the Union des Fabricants headquarters in Paris – is as follows:

Individual Achievement

Lorne Lipkus of the law firm Kestenberg Siegal Lipkus – for his work at the forefront of the Canadian Anti-Counterfeiting Network campaign.

National Public Body

Enforcement and Supervision Department of China's General Administration of Quality Supervision, Inspection, and Quarantine – for various activities including the Sharp Sword operation in 2015.

International Public Body

World Intellectual Property Organisation – and specifically its Building Respect for IP unit.

Company

IP team at luxury leather goods company Longchamp – for success in seizures and deterrence that went beyond the resources available.

Association

Ukraine Alliance against Counterfeiting and Piracy – for 'great commitment in the fight against counterfeiting in Ukraine and beyond'.

Media

Kathy Chu of the Wall Street Journal – for 'clever and courageous articles on the subject of counterfeiting and piracy'.

New Category, Technology

Custodian Solutions – for its anti-counterfeiting evidence capture, management and enforcement platform, deployed by Unilever. This cloud-based platform aims to help large enterprises to secure, track, trace, authenticate and analyse evidence and data as part of their brand protection and product security strategy

The GACG commented that the spread of winners 'shows the worldwide importance of working together to build respect for the value of creativity, innovation and enterprise, and to improve best practices for enforcement'.

RECONNAISSANCE AUTHENTICATION NEWS®

Publisher: Reconnaissance International Ltd.
Editors: Nicola Sudan (right), Mark Deakes.
Contributors: Sven Bergmann, David Tidmarsh.

Annual subscription rate: £575 / €776 / $949.
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

12–16 SEPTEMBER 2016
PRINTING FOR FABRICATION 2016
Manchester, United Kingdom
www.imaging.org/manchester

13–15 SEPTEMBER 2016
LABELEXPO AMERICAS
Illinois, USA
www.labelexpo-americas.com

05–07 OCTOBER 2016
INTERGRAF
Seville, Spain
www.securityprinters.org

12–13 OCTOBER 2016
ACG CONFERENCE
London, UK
www.a-cg.org

29–30 NOVEMBER 2016
THE HOLOGRAPHY CONFERENCE
Warsaw, Poland
www.theholographyconference.com