Virtual perfection: the art of counterfeiting and the science of prevention

Sandy Morrison BSc

This material was originally published in 2007 on the business website SpecialChem4Coatings.com in the form of an editorial plus a more detailed technology review. I have retained that format, with the editorial first. As will become clear, the editorial looks at the broad issue of counterfeiting while the longer review focuses on print-related matters.

As with the other material reproduced here I have not updated the text. The latest plastic banknotes issued by the Bank of England incorporate additional security features which cannot be provided on a paper note. However, the older technologies have not disappeared, and I felt that information on them might be of some general interest. Some of these technologies are meant to be obvious; others are not, and many people will be unaware that they exist.

Editorial: Virtual perfection: the art of counterfeiting and the science of prevention

Counterfeiting today extends far beyond its original field of currency and documents, to pharmaceuticals and cosmetics, branded clothes and watches, software and electronic documents.

In some cases, the quality of counterfeits may match that of the originals while in others the customer may be perfectly well aware that the product is fake and likely to be of inferior quality. But in either case, product counterfeiting can damage the reputation of a company, and in the case of drugs or alcoholic drinks it can be positively dangerous.

Security printing has an important role to play in protecting consumers and businesses against all these forms of fraud. [A more contentious use of security printing is to protect against product diversion or the 'grey market'. Many companies sell products with minor differences in specification and major differences in price in different markets. Products may be diverted from the low-cost market to the higher cost one. Should this division of the market be considered a reasonable business or an unethical practice? Opinions are divided, and tend to be based on what is in one's own financial interests.]

Key aspects of current security printing technology are reviewed in this month's 'Frontiers of coatings technology'. This editorial takes a closer look at how protection against counterfeiting has evolved over the centuries, with particular reference to currency.

A short history of forgery

Counterfeiting or forgery cannot be called the 'oldest profession' since its existence depends on there being original items to counterfeit*, but the term is rather appropriate in other ways. In the days when all currency was based on precious metals, striking a coin similar to the original from cheap metal and then plating it with the correct metal was recognised as a profitable crime as long ago as the seventh century BC.

Debasement of the official coinage from pure silver or gold to various alloys reduced the profitability of the enterprise at some times. Today, silver and gold are rarely used and many official coins are produced with a core of base metal and an outer cladding of a more costly alloy. But today the face value of a coin is far greater than its metal value (with some specialised exceptions) and counterfeiting of high-value coins still occurs.

In passing, a curious kind of 'reverse counterfeiting' has been found recently on the India/Bangladesh border. Legitimate Indian currency is disappearing from the streets as fast as it is minted - apparently because it is profitable to melt down the coins and forge them into... no, not higher value coins, not Bangladeshi currency, but razor blades.

The introduction of paper currency required both a printing process and a stable banking system, neither of which was available for many centuries after the use of minted coins. Its introduction produced not only 'normal' criminal counterfeiting but a number

* For the benefit of non-Brits: 'the oldest profession' is a term applied to prostitution.

of attempts to use counterfeit notes as a form of warfare, by flooding the enemy country with enough fake currency to force devaluation, or allow large quantities of goods to be purchased for near-zero cost.

An early major example was in the American War of Independence, where the 'Continental dollar' issued by the US Congress was found to be easily counterfeited. The British authorities at one point went so far as to advertise the availability of high quality counterfeit currency, which could be purchased for the cost of paper and printing.

A state-backed scheme to produce counterfeit French currency in Hungary was uncovered in 1926, and today a significant number of US dollar bills are in circulation that are referred to as 'superdollars' because the quality of the printing is actually higher than that of the genuine notes. North Korea is usually claimed to be the source of these counterfeits, but this is disputed.

Currency technology

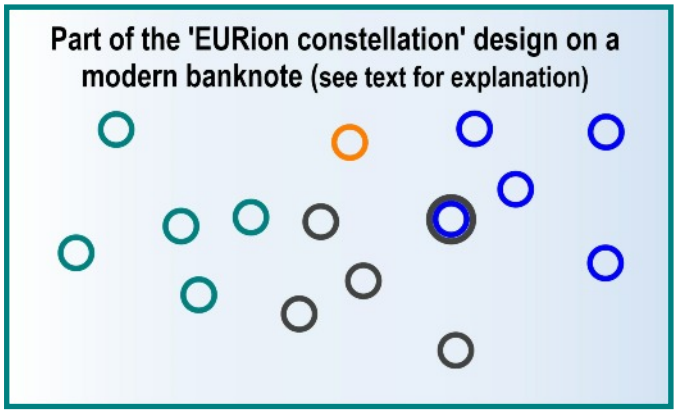
Printing technology has moved on a long way since the introduction of the Continental dollar, and modern banknotes normally incorporate a wide range of anti-counterfeiting technologies. Some are applied at the paper manufacturing stage, but far more can be used in printing.

The table below shows the main security features which may be found in a modern banknote. Exactly which ones will be found varies not only from country to country but also with the value of the note, since some features are more difficult and expensive to implement than others.

Although the European Central Bank (ECB) publishes information on the security features of Euro notes, one interesting issue is not mentioned. Banknotes of many countries now carry a patch of what appears to be a random array of circles. On Euro notes, the ECB states these are printed in fluorescent inks but does not comment on the pattern.

Sometimes the circles are just overprinted on an area of the note, but they have also been made to appear part of the overall design, in one case even appearing as musical notes where a composer's face was featured on the note, in another being incorporated into a representation of a bees' honeycomb.

Part of the 'EURion constellation' design on a modern banknote (see text for explanation)



What the ECB does not state is that the pattern is not random. On inspection, it can be found to contain arrays of five circles in different orientations. As the figure shows, a further complication in this example is that one circle does not form part of such a set while another forms part of two.

This arrangement, nicknamed the 'EURion constellation', can cause some photocopiers to refuse to copy the notes. A different arrangement, a digital watermark, causes some software to refuse to operate on images of the notes. 'Security' features of this type are something of an oddity, in that they only become effective where suppliers of software or hardware agree voluntarily to implement them.

Security features found in modern banknotes (not all are present in any specific note)

Overt	Semi-overt/covert
Guilloché patterns (interlacing curves)	Microprinting
Metal strip through paper (may carry microprinting)	Micro-embossing
Complex watermark	EURion constellation (see text)
Holograms (may also carry microprinting and microperforation)	Printing in register between back and front sides
Fine colour shade differences	Mixture of lines and dots to create halftones
Pearlescent pigments	Paper does not fluoresce under UV (all normal papers do)
Colour-travel printing (eg, on high value Euro notes, value numerals on reverse side change from purple to brown)	Coloured fibres in paper (visible under normal light and/or only under UV)
Barcode	Fluorescent pigments in part of printing
Intaglio printing gives ink a slightly raised relief and does not use halftone screening	Serial number (may incorporate a checksum)
	Magnetic ink
	Digital watermark

Future technologies

What of the future? Despite the best efforts of banks and printers, forgery will remain a profitable activity for so long as we continue to use 'hard copy' currency.

There are already a number of security technologies under development and recently introduced (as described in the technology review) which do not yet appear to have found their way into banknote production.

The limitation is, however, that these are essentially covert technologies requiring special equipment for detection. The general user does not subject every banknote to close examination on receiving it, and so copies which lack some of the more sophisticated security features may still find their way into circulation, only to be rejected when they reach a bank.

That problem, though, looks different from the forgers' viewpoint: the more detailed and perfect the forgery, the longer it will take to be discovered, and the longer that detection takes, the larger the volume of notes which can be passed off as genuine.

The ideal security technology - simple to implement, easy to see yet impossible to counterfeit - will probably never be devised, and the balance between security and forgery will continue to swing as security companies devise new technologies while others develop techniques which may unintentionally make the forgers' task easier. The main end result visible to the consumer is merely that our banknotes become more and more colourful and decorative as time goes by.

Technology review: Accept no (l)imitations: the evolving technologies of security printing

One of the unfortunate consequences of the digital revolution has been the greater ease with which all kinds of printed matter and manufactured goods can be counterfeited, and the greater speed with which international criminal activities can be organised. Globalisation, too, has increased the availability of counterfeit goods and improved their distribution.

The forging of banknotes at one time required a highly skilled engraver to imitate complex printing patterns; today, high quality scanners and printers can be and have been used to produce low quality imitations - which may pass undetected in hasty transactions - with little skill. [The specific issue of banknote forgery is discussed in greater detail in this month's editorial; here the broad range of technologies and applications is considered.]

In response to these threats, the printing industry (in particular) is engaged on an endless spiral of developing ever more sophisticated methods to protect against theft, tampering and counterfeiting, while at the same time developing advances in general printing technology which quite accidentally devalue some of what were originally high-security features.

The range of materials which is likely to be protected by some form of printed security is vast. It ranges from obvious applications such as currency, cheques, passports and credit cards, through lottery and event tickets to items which are not themselves printed, but for which securely identifiable packaging is essential.

Many of these last items are high-value consumer items, but in the case of pharmaceuticals, functional spare parts, cigarettes and alcoholic drinks, counterfeit goods can have serious health and safety implications as well as damaging the reputation of the genuine producer if the purchaser does not recognise the fraud, and his profits even when they do.

Levels of security in documents and labelling

Maximum security	High security	Consumer security
Banknotes and similar 'open' currency documents	Credit cards	Pharmaceuticals, perfumes
	Cheques, deeds and securities	CDs, DVDs, software etc
Passports, visas, ID cards	Admission tickets, lottery vouchers	Various 'designer goods' and high-value products
		Spare parts for vehicles etc

Counterfeiting can (as reported while this article was being written) extend as far down the value chain as premium toothpaste. Fake *Sensodyne* toothpaste was found on sale in street markets in the UK and attracted concern because it contained toxic diethylene glycol. In this case, the fact that the packaging carried bilingual text whereas the real article carries only text in English does not seem to have attracted general notice. It is, after all, now a common practice to have labelling in more than one language. The use of a more distinctive printing style on the genuine article might have drawn more attention to the fakes.

For convenience, a distinction has been drawn in this article between overt technologies (visible to a keen but unskilled observer without special equipment) and covert systems which require anything from a low-powered magnifier to proprietary computer-controlled equipment for their detection. However, this distinction is not a sharp one. The same technology may be used to carry both overt and covert features, as can be seen from the table below and as discussed later in this review.

One interesting case in point is the printing of an

apparently random pattern of small circles on many banknotes. These may use fluorescent or colour-shifting inks, adding to the complexity of forgery. A less obvious feature emerged after one investigator found that some photocopiers would not copy banknotes bearing these circles.

The arrangement is not in fact random, but contains a pattern of five circles repeated in different orientations, which has been nicknamed the 'EURion constellation'. Unless it has some other undisclosed mode of operation, this is a rather curious security feature, because it is ineffective on equipment which does not carry appropriate software.

Overt technologies

Where only a moderate level of security is required and high volumes are involved, the use of additional ink colours outside the normal CMYK ink set used in full-colour printing provides a first line of defence. Ordinary 'spot' colours are less useful than they used to be, since a number of printing systems have been devised in recent years specifically to avoid the need for spot colours*.

Pearlescent pigments are particularly useful, as they are fine enough to be printed by offset, gravure and flexo processes (intaglio and screen printing can accept larger particle sizes) and a vast number of different effects can be produced. Optically variable pigments are currently used by more than 90 countries in security inks for printing banknotes.

Within a certain range of coating thickness on the pigments themselves, interference effects are produced which can only be

For the non-technical: Ordinary colour printing creates a reasonable illusion of the full colour range seen by the human eye by overlaying three coloured inks plus translucent black; spot colours are widely used in packaging, for example to create very bright colours outside this 'CMYK' range or to allow simple printing of block colours in situations where it is hard to keep the colours aligned exactly with each other.

Main security features in use on documents, cards etc

Paper manufacture	Printed - overt	Printed - covert
Non-standard (rag content) paper has a distinctive feel	Thermochromic inks	Water-resoluble inks
No fluorescent brighteners added	Photochromic inks	Infrared-sensitive inks
Complex watermark	Metameric matching	Phosphorescent and UV-fluorescent inks
Coloured (overt) and/or fluorescent (covert) fibres added during manufacture ('Silurian fibres')	Simulated watermark inks	Magnetic and other machine-readable inks
Metal or textile thread embedded in paper	Metallic/pearlescent inks including colour-shift types	Microtaggants (several technologies)
Pen reactive surface	Hologram (foils)	Shaped flake pigments (visible under optical microscope)
Coin reactive surface	Diffractive pigments	Micro or nanoprinting (details visible only under magnification)
	MetalFX process	Latent images, specifically shaped pixels or scannable codes hidden within holograms
	Spot colours outside CMYK colour gamut	'EURion constellation' (see text)
	Complex printing such as guilloché patterns (interlacing curves) on banknotes	Photoactive inks used to produce 'void' messages when photocopying.
	Use of specific printing processes (intaglio, screen) to produce features not available on other processes	Labels which break up or mark substrate when removed
	Serial numbers	Checksums incorporated into serial numbers

imitated by pigments having a similar construction, and the appearance is also strongly affected by substrate colour. For example, over a dark background, a red interference pigment will appear brilliant red at all angles, but over a lighter background, scattered light of other frequencies is also visible, modifying the appearance at anything other than the spectral reflectance angle.

Multilayer interference pigments with more complex colour-shifting behaviour are used in high-security applications. Some, indeed, have been developed specifically for the security market and are sold only to approved customers.

Pigments of this type have been used recently by tobacco supplier Karelia in Greece. Simply by changing the tear strips already used on its cigarette packs to ones containing colour shift pigments, the company has made life harder for counterfeiters.

Photochromic materials (familiar in sunglasses) have a limited durability, making them unsatisfactory as security indicators in most applications. However, photochromic azo dyes have been reported which have much better lightfastness. Their colour shift is relatively small, but sufficient to act as a security feature.

Fluorescent pigments can be combined with other types in different ways to produce an extended range of effects - some of which have even been patented. For example:

- Combining fluorescent pigments with reflective types produces a colour dominated by the reflective pigment on facing view, with the fluorescent colour being more pronounced on flop.
- Coating fluorescent pigments over a light-absorbing layer can lead to the colour being dominated by the absorbing pigments at low light intensities but the fluorescent tone at higher intensities.
- A number of patents have been taken out on pigments which incorporate luminescent colours within the multiple layers of an interference-effect pigment.

Thermochromic inks have been used for several years to verify the authenticity of documents. However, the usual arrangement in which a single colour change occurs at a set temperature can make the inks difficult to use on documents that may be used anywhere from Alaska in winter to summer in Zanzibar.

At least one company offers a range of 'tri-thermochromic' inks which (for example) change from brown to orange at 25°C and change again to yellow at 35°C. Adding other materials such as luminescent pigments to the ink changes their appearance but not the actuating temperatures. The inks are available for most print processes in conventional or UV curable forms.

Package identification and protection

UK company Datalase has developed and patented the so far unique Packmark coding system in which an initially white pigment changes colour permanently to black on exposure to a low-powered CO_2 laser. The system is used both for standard variable data in packaging (barcodes and use-by dates) and for security purposes.

Either blocks of Datalase ink are applied by the package printer, or a tape ('Casemark') is used which incorporates Datalase pigment. The final laser printing is carried out in the packaging operation. In the tape, the pigment is coated onto the back surface and the laser exposure is applied through the transparent tape film, making it impossible to remove the image once it has been created - and if the tape is stripped off, some of the print remains permanently transferred to the packaging below.

A further advantage of Datalase is that the pigment can be integrated into moulded plastics. It is extremely difficult to produce durable markings on polyolefin plastics by inkjet printing and so the main alternative to Datalase requires a high-powered laser to produce coding by ablating the plastic.

Datalase has extended its system into a microprinting technology which provides a resolution of up to 10,000 dpi on a surface or within the layers of a laminate. This can provide more or less covert marking, in the form of images and text visible only under magnification, in addition to encrypted data which can only be detected and decoded with appropriate scanners.

Holographic developments

Printed holograms were once promoted as the 'final solution' to protection against forgery. Today, the cost of reproducing holograms has fallen to the point at which they are no longer regarded as a fully secure technology, but merely one way among many to make the counterfeiters' task more difficult.

The type of hologram normally used in security applications has to be produced with a very finely embossed or grooved surface, and so they are applied in the form of foils rather than by in-line printing. Very complex images which seem to move or change completely as the viewing angle is changed may be employed.

Special diffractive pigments can be used to produce simple 'holographic' images by incorporating a

ferromagnetic layer in the pigment particles and applying a magnetic field at the time of printing to orient the particles. When the printed object is rotated in front of the viewer, the brilliance of the diffractive effect will vary, and if two different pigments are printed separately, a more obvious feature can be produced in which the appearance varies from dark image/light background to light image/dark background.

Identification codes which are intended to be covert and unreadable by eye or with simple equipment are used on documents such as prepaid phonecards. But fraudsters quickly cracked the first attempts at hiding the code, simply by using laser readers. Rendering the code opaque by applying several distinct ink layers solved the problem, but was time-consuming and expensive.

A solution adopted in Italy has been to overprint the security code with a cold-foiled holographic 'wallpaper' which made the cards both impossible to read and also to copy visually, at a lower cost than applying conventional holograms.

The process used, 'HolographINK' employs a cold-applied foil with an overall multicoloured pattern whose appearance is modified by the colour of the ink beneath it. UV curable inks are printed, the foil is applied and then the ink is cured through the foil. The ink acts as an adhesive, so the design is selectively bonded only to the printed areas. The foil is available in standard or customised patterns and the same foil can be used to create many different colours and patterns by varying the background printing.

The MetalFX printing process uses special high-tack metallic inks beneath 'full-colour' CMYK inks to produce brilliant metallic effects with all the fine detail that is found in normal colour printing. It is primarily a system for producing dramatic graphics and packaging, but has some potential in security applications, since its effects can only be reproduced by a press running MetalFX. A pseudo-holographic effect can be produced by reducing the level of base silver in specific areas or eliminating it completely, while maintaining the CMYK colours unchanged.

Ironically, one of the things that are now considered worth security protection are printing inks themselves. At the end of 2006, industrial inkjet supplier Xaar introduced a hologram-based authentication scheme for solventborne inks that were approved for use with its printheads. While this does not prevent the use of non-approved inks, it does at least ensure that the customer knows whether the ink has been approved or not, and is guaranteed to perform well.

Magnetic attractions

The use of a metallic strip inserted in papermaking is a well-established technology in banknote production, and some now carry microprinting. TSSI systems has taken this approach a step further by using a magnetic thread which carries coded information that (the company claims) cannot be copied, altered or erased, and allows individual documents or batches to carry a unique code.

QMark secure paper, which incorporates this strip, is suggested as being useful for vehicle identity certificates, tickets, bond certificates and similar high security documents. The same company offers machine-readable magnetic patches which are applied as hot foils and will fracture if any attempt is made to remove them.

Undercover agents

'Invisible inks' which are rendered visible by various simple means have been in existence for a long time. Besides being useful to writers of crime and espionage stories, they can be applied for security purposes.

One patent claims the use of an invisible ink system which has the advantage of being compatible with standard inkjet technology. A colourless hydroquinone sulfonic acid salt is mixed with water and a humectant such as polyethylene glycol, then printed at the required density. Additional visible printing can be applied to make the image impossible to read under any form of illumination.

Applying a solution of a ferric salt in water will permanently colour the printed image. The patent claims that the paper can then be sent to a user with no possibility that the information on it can be intercepted without the fact becoming evident. In addition to its use for sending spy-like messages, the system can also be used to provide authentication of the source of documents.

There is an increasing interest in the use of various types of 'taggants' which are claimed to be almost impossible to replicate in inks. DNA technology is one form of taggant, though there are a number of complex issues concerned with its general use. DNA and various nanoparticles including quantum dots can be applied by inkjet. Invisible inks containing taggants can produce text readable with appropriate devices.

Other systems include optical microtaggant particles, which are coloured stable plastic particles about 50μm in diameter. By manufacturing each of these with a closely controlled size distribution and mixing sizes and colours in different proportions, millions of unique colour mixtures can be supplied, so that each

customer has a unique signature which can be identified microscopically, though the taggants are almost undetectable to the naked eye.

IR-sensitive microtaggants can provide a simple identification of their presence or absence using a hand-held reader which detects them through packaging materials. At the other end of the scale, microtaggants having unique spectral characteristics can be identified by using a spectrophotometer, and those containing specific heavy metals by X-ray analysis.

Creo is collaborating with Kodak in introducing another taggant system which is said to be 'forensically invisible' unless the special reader devices are used. Kodak's 'Traceless' taggant particles are distributed randomly by the printing process, and the reader is able to detect either simply the presence of the particles or the position of each one, providing a 'fingerprint' which is unique to each package. (The taggants can similarly be used in sprays, paints, copier toners, paper, woven fibres and even in explosives, plastics and materials exposed to very high temperatures. Addition levels are only in the region of 2 ppm.).

Tamper-evident tape seals can be designed with printed adhesive or pigment layers, or weak spots in the tape itself, that will leave a distinctive pattern on the substrate if the tape is removed.

Smart labels and RFID

Radio-frequency identification devices (RFIDs) are already in use for tracking and identifying high-value goods, but one of the great promises held out by this technology is that it will be much more widely used if its cost can be reduced - and the best way to do that is to make as much as possible of the electronic circuitry printable on conventional or near-conventional presses.

Current applications for RFID labels include library books, maintaining tracing in archives, real-time progress monitoring (and theft detection) in logistics, identification of airline baggage, logging visitor numbers to different parts of large exhibitions, monitoring use of prescription drugs, passports and various tickets and payment cards. If costs can be reduced to a sufficiently low level, RFID labelling would be more widely used to prevent theft from shops.

Electronic tamper devices using printed inks have been used to catch a thief who was stealing mobile phones from the Swedish postal service and replacing them with potatoes. The packaging recorded the time at which the boxes were opened, making it possible to identify where the thefts were taking place.

A market report from IDTechEx predicts rapid growth in this market. Some key findings from the report, which covers the period 2006-2016, are:

- Total sales of RFID for all years up to and including 2005 were 2.4 billion units, with a quarter being sold in 2005 alone. Sales value of tags alone in 2005 was $1.2 BN, but if tag readers and services are included, the total rises to $1.85 BN.
- This figure was expected to more than double to 1.3 BN tags in 2006 and to rise to more than 400 times that number by 2016 - though falling costs mean that their value may increase by only a factor of about ten, to reach a total of $26 BN.

Currently, dedicated equipment is available for continuous production and in-line testing of RFID labels, tags and tickets such as the Bielomatic machine illustrated, but the ideal would be to have a similar machine capable of printing the circuits, antenna and batteries continuously.

One step towards this direct printing of circuits is Qinetiq's patented process, in which the required patterns are printed conventionally, and the metal circuitry is then plated onto the printed areas. This is said to cut the cost and pollution of production considerably, but falls short of the goal of direct printing. Another company is working on a process in which the printed layer contains catalysts and the metal plating operation is carried out inline.

In the last few weeks, Ciba has announced the introduction of a range of printable conductive inks under the Xymara Electra brand. Currently, these inks are only available for rotary and flatbed screen printing (which can lay down thicker ink layers than other processes, apart from multi-pass inkjet).

Inkjet is thus a promising candidate for printing of circuits, especially if minor variations in the design are requested to further increase security. However, inkjet requires a very fine particle size, and so far conductive inks based on nanoparticles only become conductive after high-temperature curing is used to drive off other components of the ink.

Anti-copying systems

A number of techniques are employed specifically to prevent photocopying or scanning of documents, or to identify the fact that the copies are illicit. Thermochromic inks can be used to provide a hidden message which becomes visible when the coating is subjected to heat from thumb pressure. The same technique can also make colour copying impossible.

The heat generated when an image is exposed on the copier causes a hidden 'counterfeit' message or an overall camouflaging pattern to appear on the copies, which fades back to invisibility on the original when it is removed from the copier.

A variation on this is to apply photochromic inks to the original, so that a hidden message is generated by the light rather than the heat of the copying device. Both these approaches require latent colour systems which react very rapidly.

A more reliable method which ensures that any copies cannot reproduce colours accurately is to incorporate aluminium or optically variable ('colour travel') pigments. The specular reflections from these confuse the colour measurement systems of copiers, which can in any case only reproduce a fixed colour.

Another anti-copying proposal involves printing a form of black diffraction grating over a metallised substrate by stochastic screening. Whether the copier uses specular or diffuse illumination, random interference patterns are generated by the screening, which renders the text illegible. This is not a practical solution for general use, but can readily be applied to security numbers and similar localised areas.

Self-destruction technologies

Although it is not a solution with wide application, the best way to protect against currency theft is to ensure that the stolen currency is unusable. Solutions have included devices that cover the currency with ink if an attempt is made at theft, but a system developed by Velleman Switch and IQ Sec goes one better.

The currency is packaged in boxes covered in a security film which carries a printed silver ink circuit. Any unauthorised attempt to open the container damages the circuit and triggers high-performance pyrotechnics which burn out the box and its contents within seconds. The system had to be designed to maintain safe and stable operation over a wide temperature range, to allow printed currency to be transported worldwide.

Other smart coatings and labels

Fraud can include supplying good which are no longer fit for purpose, such as drugs and foodstuffs which are outside their shelf life or have not been stored at an appropriately low temperature. Thermochromic inkjet inks have been developed which can be used to print barcodes via normal inkjet labelling systems. If the product has been stored at too high a temperature at any time, the ink changes colour, making it impossible for the barcode to be scanned and providing the customer and vendor with a clearly visible indication of the problem.

Domino has developed a laser-based recognition system which is capable of reading barcodes through a normal paper envelope, and instantaneously processing the barcode to print an address on the envelope. This improves the confidentiality of individual mailings by avoiding the use of window envelopes (which are also more expensive and difficult to recycle than plain envelopes).

A near-future system whose potential security value has still to be established is Microsoft's coloured barcode identification system, which allows more information about products to be provided than the current standardised monochrome barcode.

The International Standard Audiovisual Number International Agency (ISAN-IA), which co-ordinates the use of barcodes, has licensed Microsoft's High Capacity Colour Barcode (HCCB) technology, initially to assist in the identification of commercial audiovisual programmes such as motion pictures, video games, broadcasts and digital video recordings.

The new barcodes will (it is claimed) assist in tracking products and collecting royalty payments. For consumers, the barcodes can be combined with Web services to offer enhanced information such as product versions, ratings identification, parental control, product availability, special releases, contests, pricing and promotions.

Other possible applications are envisaged, as improvements in the quality of mobile phone cameras should ultimately allow them to capture the barcodes. In addition to the visible part of the barcodes, DatatraceDNA plans to provide technology for anti-counterfeiting security protection features through nanotechnology that is invisibly embedded within the material and ink of the bar code and product packaging. Once again, this is an example of a technology which combines overt and covert security technologies.

It can be seen that there is and probably always will be a demand for newer and more sophisticated security printing technologies to keep business one step ahead of counterfeiters and thieves.

The most interesting developments are, as usual, the unexpected ones which it would have been almost impossible to predict in advance of their appearance. Who, for example, could have predicted the arrival of DataLase technology, Kodak's traceless taggants or even Microsoft's colour barcode?