The impact of digital print on the security market as seen from the substrate supplier.

Fiona E Davidson; Tullis Russell Coaters Ltd.; Bollington, United Kingdom

Abstract

The challenges to the traditional security market have never been greater nor in a period of greater diversity and flux. The impact of the internet, mobile phone and the SOHO printer have changed not only the way security documents are printed and examined but also the relationship between the user and the issuer. So while some security documents have been devalued by these changes; the levels of security, complexity and functionality of others have increased significantly. The incorporation of chips, RFID and displays draws the secure document into the world of printed electronics. Both worlds are being transformed by digital printing and are increasingly technically demanding on the substrate.

Introduction

Over the last 30 years electronic and mobile technology has had a major impact on financial transactions as ATMs, credit cards and debit cards have replaced cheques and cash transactions. The demise of the chequebook is in sight, it has been announced in the UK that banks will not support cheque transactions after 2018. There is a 'pull' to cashless transactions through the attraction of such things as internet shopping, and a 'push' from governments who encouraged the public to use the internet or telephone to pay car tax, TV licence fees etc as it is significantly cheaper for governments to collect revenue this way. The paper ' licence', once a secure piece of paper of financial value, has become a receipt and the proof of payment lies on a computer database.

Passports, Visas and ID cards

As government databases are increasingly linked together – changing one's information in one automatically updates the others. This is important, as often, what are seen by the public as minor documents, all help form one's footprint in a country and provide supporting feeder documents to the important ones like the passport and ID card. A passport or ID card in the wrong hands not only opens up illegal immigration, but illegal working and financial fraud.

Passports and ID cards verify the identity of an individual and hence each is a uniquely printed item. The level of personalisation in a passport makes them an ideal subject for discussion in a digital printing forum.

A passport contains all number of security features - they appear in: the cover, the pages, the printing, the hologram, the overlays, the sewing thread, the chip, and in the visas. Of the many security features only 2-3 are checked on most transits [1]. Only when something suspicious strikes the examiner will some of the others be checked. Even then it is difficult for a border guard to know what the genuine document is supposed to look like. This is a common problem with any authentication system - what is 'genuine'. The e-passport has encrypted biometric information held in a chip which self-authenticates the passport. The security lies in the sophisticated encryption routine. By necessity of the security of the encryption the chip is a write-once- read- many times (WORM) device. This means that travel history or Visa permissions are not currently held in the chip. Visas range from an ink stamp, to a security label with nearly as many security features as the passport itself. The minimum requirement set by the International Civil Aviation Organisation (ICAO) is a frangible, optical brightener free (OBA free) paper with visible and invisible fibres, planchettes, chemical sensitisation and a permanent adhesive [2]. An OBA free paper is a fundamental requirement of security papers as optical brighteners interfere with covert UV security features, and also degrade the paper on aging. Passports have a 10 year life after issue and any security feature or print process must be supported over that period.

Countries such as Australia are replacing the printed visa by an Electronic Travel Authority (ETA) ie the Visa application details are linked to the passport number, which is verified automatically on check-in to Australia and/or by an Australian Immigration officer on arrival. However printed visas do have the added benefit that the global travel history of the passport holder is easier and quicker to see by the border guard via the visa stamps in the passport [3].

Biometric Information

The basic biometric information in the 1st generation e-passport is a digital photograph and signature. The photograph is now printed digitally directly onto the passport paper to prevent removal and substitution. Some protective polymer overlays include a digital holographic facial image alongside the printed digital image. A higher level of biometric validation was introduced with the 2nd generation of e-passports by including digitised fingerprint and iris data.

Fingerprint scanners are increasing available for various uses. Not only to unlock access to doors and computers but also to act as shortcut keys on computers. A self-authenticating ID card includes a fingerprint sensor for authenticating the identity of a user. The fingerprint sensor works on pressure variations and requires contact with the sensor.

Fujitsu have developed a palm vein print reader which is contactless and seen as more hygienic in some societies [4]. Iris readers are also a non-contact biometric device. A key advantage of iris recognition is its stability, or template longevity, as, barring trauma, a single enrolment can last a lifetime. The iris is less likely to suffer scarring than a fingerprint.

An alternative method of storing the biometric information the Biometrigram ® was developed by Ver-tec (IP now owned by TSSI Systems Ltd). The Biometrigram® can incorporate multiple digital biometrics (fingerprint, palm print, iris) as well as other analogue images and encrypted digital information within the single physical space of a hologram [5]. The hologram has higher information densities than electronic chips and is verifiable against electronic chips for document authentication.

With increased security built into passports the problem is moving towards impersonation at the time of issue. People are even prepared to undergo cosmetic surgery to look like the genuine article.

Authentication by unique item signature

There are a number of technologies on the market where a 'biometric' of the item is encrypted into a unique code. Ingenia Technology's LSA™ system [6] works on the surface imperfections and irregularities of the surface of paper and plastics. The speckle pattern from a reflected laser forms the basis of a signature, which is unique to any given sheet of paper or plastic. Our own technology, Fibreloc™, uses the 3D pattern of UV fibres in security paper to create the unique signature. The papermaking process lays down fibres in a random pattern, and any random pattern that incorporates a 3D element can not be replicated by printing.

Systems, like Prooftag™ (which utilises bubbles created in a plastic film), and Univocal Sign™ (randomly distributed black bumps) are designed to be seen by the end user - the user can authenticate the item on the internet or mobile phone. The covert systems, such as Fibreloc™ and Ingenia's LSA™, require proprietary readers with specialised lighting sources to interrogate the substrate.

The passport and ID card industry is used to covert viewing systems because the passport is normally viewed in a controlled environment and hence controlled methods of lighting the item can be provided. Many technologies find it difficult to be adopted, not because of the cost of the feature but the cost of providing specialised readers. For Brand protection mobile phone based authentication offers the advantage to the customer in that they can authenticate the item before purchase.

All biometric systems (either person or item biometric) are faced with the issue of one-to-one or one-to-many verification. One-to-one is quicker and has a higher success rate. One-to-one requires a printed code or cross verification on the document itself. eg the encrypted digital photo can be checked against the digitally printed image. The printed code is usually an alphanumeric code, linear barcode or increasingly common a 2D barcode. One advantage of one-to-one verification is that it does not require access to the master database. This can be important if the inspector is out in the field away from reliable telecommunications. Digital printing; inkjet, laser or thermal will be used to print the verification code at time of item enrolment. One-to-many systems however have the advantage where the available print area is limited eg protection of electronic components. Today, speed of authentication is not an issue with one-to-many systems, with 10 million plus matches per second possible. [7]

Barcode Verification

Linear barcodes may seem dated these days. Linear barcodes on supermarket purchases are scanned for simultaneous pricing, stock control and also to monitor our shopping habits. In the pharmaceutical industry it can also be used to deliver up to date information to the customer about the medication - any new alerts, changes to the appearance of the tablet etc. The pan European project to introduce a 2D barcode containing information on product, country producer and batch as a track&trace system for pharmaceuticals has been delayed owing to issues of standardisation and cross country repacking. Belgium decided to introduce its own simpler linear barcode system and has already shown many benefits to the customer and pharmacist and does not require the investment in new scanners by the pharmacists.[8]

The 2D barcodes pack a higher density of information in to a smaller area and are used for marking small items. A 2-3mm square Datamatrix code can hold 50 characters of data. The micro printed features require higher resolution printing and greater smoothness in the substrate. The finer the detail, the higher the level of redundancy has to be built in to the code to ensure correct reading and reduced susceptibility to printing defects.

2D barcodes are used globally for tracking letters and packages by postal services. For business mail Datamatrix-type codes are placing pictorial postage stamps, and there is a trend for postage stamps to be downgraded to a sticky white label with 2D barcode.

There are two forms of bar code commonly referred to as 3D barcodes. The first is a linear or 2D barcode engraved, embossed or applied to the item itself as part of the manufacturing process. The time it takes for the laser scanner to bounce back from the surface determines the height of the structure as a function of distance and time. Thus the character represented by the code can be interpreted. The code can be used where printed labels will not adhere, or will be otherwise destroyed by a hostile or abrasive environment [9]. The challenge for printing 3D barcodes is to build up the height of the ink a fine array. A more suitable use of the printing process is to create the second type of so called 3D barcode – a 2D barcode with combined colour code.

One of the newest covert code systems on the market is Océ's Phantom code™ . A microfine pattern of dots is printed with 13 linked pairs within the target area. Each configuration of linkages defines a unique item or range of items. The reader system is comparatively cheap but the software is restricted to Océ printers. It is through the restriction of software coding that the intellectual property, and the security of the item, is protected

Security of Printing

Intaglio printing has always been seen as the most secure printing method. Partly because the process of engraving an intaglio plate was complex and laborious, taking up to 3 months of craftsmanship. Partly because intaglio printing is the printing method of banknotes and the hence the control of intaglio plates and printing machines is rigorously controlled and restricted. Through digital design and computer controlled engraving the plate can now be prepared in 48hours which eases one restriction but the access to intaglio printing machines is as tight as ever. One of the biggest concerns about digital printing is the free access to digital printing equipment. London's Metropolitan Police is running a project to establish a voluntary code of practice- Project

Genesius [10]. This is starting with thermal ID card printers and aims to capture information about the purchasers of equipment. Just the presence of a statement on one website saying that information is shared with the police cut questionable enquiries by 90%.

Project Genesius aims to build a joint working relationship between Law Enforcement and the Printing Industry for:

- The prevention of supply of specialist printing equipment for unlawful activity
- Sharing of intelligence
- Increasing the understanding of the scale of identity document abuse
- Enabling the Printing Industry to identify good practice in customer profiling
- Prevent potential loss to unregulated customers
- Maintain the industries reputation

The high security printer supply chain is secured and self regulated by associations such as Intergraf and Naspo. If the customer is unknown and not validated they are not sold the paper, film, ink, hologram, the print equipment etc. Reputation is paramount and a restricted customer base necessitates higher costs. The number of producers of security papers and films is small. Security substrates are produced in relatively small, bespoke quantities which is in conflict with the economics of paper or film making which is driving most producers to higher volume, commodity production.

Digital printing will play and increasingly important role in security. At the recent IPEX exhibition in the UK, digital printing occupied a greater floor area than traditional printing for the first time. Digital printing has been used in security applications to print the variable information – a serial number or barcode using non-secure black inks. Security inks and toners are being formulated for digital print processes but at the moment they are have not surpassed the performance of security of inks for intaglio, gravure and litho printing. To produce an optically variable effect the ink particles tend to be flake-like and thus unsuitable for inkjet processes. [11]. Inkjet systems need to be smaller than ~200nm in particle size, have a restricted particle size distribution, formulated into non-agglomerating, non-settling, low viscosity inks. The physical properties of security pigments can be detrimentally affected eg the luminescence of phosphor particles is highly dependent on particle size. The processes required to make effective, small particle size security pigments are complex and expensive and can create a barrier to unauthorised production.[11].

Printed Electronics.

Where the digital printing processes can bring benefits in the future to the security market is in the ability to print simple electrical circuits direct onto the substrate. Advances in the development of sub-micron conductive inks and print heads mean that RFID components, displays etc will be printed as part of the document rather than laminated into the document. One benefit is that it is more difficult to remove or tamper with the component when printed onto the substrate without destroying the conductive lines. The requirements on the substrate increase – in terms of smoothness, dimensional stability and porosity.

Conclusion

Security is about a multiplicity of security features and the security of the supply chain. Digital technologies enhance security by enabling late stage personalisation, and itemisation but are a threat to the security market when they become indistinguishable from intaglio printing, watermarking and holograms. However digital technologies in combination with secure materials (inks and substrates) offer an increasing variety of methods to use variable information to protect, authenticate, and track the movement of people and property.

References

[1] B. Minihane., The role of INTERPOL in the field of Document Security., Security Document World (2010)

[2] ICAO Doc 9303 Machine Readable Documents Vol.3 (2008)

[3] R Chalmers., The Shape of Things to Come., Security Document World (2010)

[4] Fujitsu PalmSecure™ Palm Vein Authentication System Technical brochure.

[5] Ver-tec Security Systems Biometrigram ® Technical brochure

[6] Ingenia Technology Limited., www. Ingeniatechnology.com

[7] LG Iris. www.lgiris.com/ps/technology

[8] G Hoogewijs., Fighting Counterfeit Medicines through online authentication in Belgium Public Pharmacies., 2nd Annual Conf. Anticounterfeiting Pharma (2009).

[9] Specifications for Popular 2D Bar Codes, Adams Communications (2009)

[10] N Downing., Preventing identity document abuse through partnerships., Security Document World (2010)

[11] M.Hampden-Smith, S. Haubrich, R. Kornbrekke, J. Shah, R.Bhatia, E. Hardman, R.Einhorn Cabot Corporation ., Overt Security Features Through Digital Printing., Proceedings of the SPIE, Volume 6075, pp. 230-239 (2006).

Author Biography

*Fiona has 28 years experience in product and process development for the photographic, holographic and security coatings industries. She has also specialised in the area of innovation & creativity. Fiona joined Tullis Russell Coaters in 2004 as Technical Manager before leading the **tru**security project. Her focus is now Market & Technology development.*

Fiona has a BSc in Chemistry & Physics and a PhD in Molecular Beam Reaction Dynamics, both from the University of Manchester. She has an MBA from Heriot Watt Universit,y Edinburgh..