Challenges in Security Printing

Alan Hodgson; 3M Chadderton; Oldham, United Kingdom, Steven J Simske; HP Labs, Fort Collins Colorado USA

Abstract

This work examines the technical challenges facing the security print business sector. This sector includes a wide variety of printed marks along with print-as-fabrication, covering a wide gamut from barcodes to interactive holograms. As a result, this work also highlights opportunities for printing and fabrication technologies.

This conference is an ideal opportunity to explore specific opportunities in the physics, chemistry and material science of security printing and to consider new hardware and software applications for print inspection and verification.

The security print application space is very much wider than the obvious ones of identification verification documents, such as passports and identity cards. It now covers brand and asset protection plus a host of emerging actionable printing applications.

Security printing can be a part of every printed item. The very printing process itself results in the unpredictable deposition of marks which can be used for forensic identification. Complex color images can be used to identify the print shop which printed an item, due to nuances of color, variable and customized printing. Intentional data can be printed in the form of barcodes, graphical alphanumerics (such as guilloches), and a host of fabrication processes – such as lenticular, adhesive and stereolithographic processes – can be used to create difficult to mimic content that can be used for overt, covert and/or forensic security features.

Introduction

This work examines the technical challenges facing the security print business sector. Naturally, this is concerned with the opportunities for printing and fabrication as well as printing-as-fabrication. There are specific opportunities for the technologies of physics, chemistry and material science in this print business and an ongoing market for new hardware and software applications for print inspection and verification.

Security Printing as a specific printing application

One key point for those coming at security printing from a background in consumer and/or industrial printing is that many aspects of this sector seem counter-intuitive. Here are a few examples where the approach to the technology differs. It also gives some hints as to the opportunities that exist in security printing that are further explored in this work.

Ink penetration into the printing substrate.

In commercial printing applications, ink/media combinations are often formulated to discourage ink penetration. This is because it increases the amount of ink used and hence increases the cost per page. In some sectors of security printing, penetration is positively encouraged as it makes it more difficult to fraudulently alter the print.

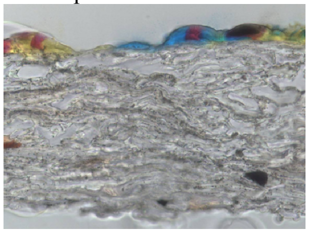

Figure 1 Color toner on paper

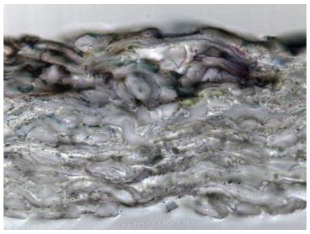

Figure 2 Dye based aqueous inkjet on paper

This effect is best illustrated using microscope cross sections. Figure 1 shows color toner on the surface and Figure 2 the penetration of dye based inkjet into the paper. The paper in both cases is approximately 120µm thick.

Ink / substrate interaction effects.

At the most basic level, ink/substrate interactions can be considered simply in terms of adhesion of the colorant to the substrate. For example, toner on paper as illustrated in Figure 1 is commonly used for documents destined for a limited lifespan. In the case of secure documents, which may require extended lifetimes, long term adhesion can be a critical issue. In that respect, the needs of security print applications can be considered to be much more like that of the archiving and conservation communities.[1]

Although it would be wrong to suggest that cost is not an issue in this application sector, it is a much weaker driver for the overall print proposition than it is in sectors such as commercial print. A much wider spectrum of price / novelty mixtures exist in this sector, resulting in niche to high volume opportunities across the security printing space.

The above points all cover opportunities in "conventional" graphics printing; that is, print that is interrogated in the visible (or near visible) spectrum. As this applications area moves into the printed electronics / fabrication space, analogous opportunities for counter-intuitive technologies will be required.

There is an opportunity for technologies that differentiate security from conventional print. Enhancement to print adhesion and colorant penetration are specific examples.

Substrates

Paper

One of the most common substrates in security printing is also the oldest – paper. The paper substrate can be engineered to produce additional security features that are also counter-intuitive to those more versed in photo quality reproduction.

One example of this is illustrated in Figure 3. Here the paper surface has a non-uniform porosity. As a result, the penetration of an aqueous pigmented ink is variable across the surface. While this produces some element of mottle to a uniform print area, it enhances the security of the product by making the print more difficult to accurately remove. This is an example where trade-off exists between parameters such as print quality and security functionality.

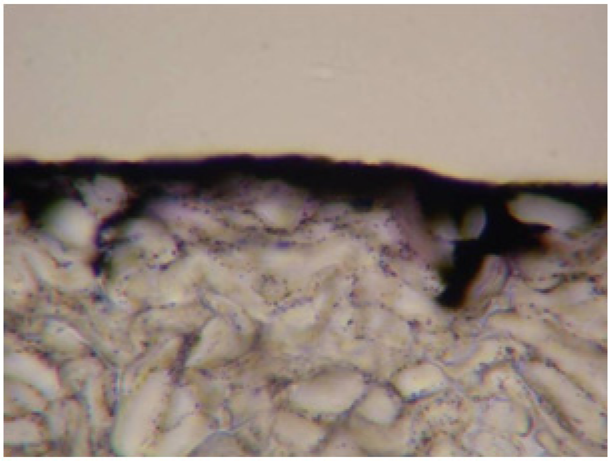

Figure 3 Ink penetration into paper "sink holes"

High security papers also include a number of other interesting features. They typically contain no fluorescent brighteners, which makes the use of any substitute paper immediately evident under UV light. They also usually contain security watermarks; however, these can now be to a certain extent mimicked by digital printing technologies.[2]

The use of coated products

Inkjet printing for photo applications will most commonly use a coated product to optimise print quality and drying time. However, in the field of security printing coatings can compromise the print security. This is because coatings such as that illustrated in Figure 4 are prone to removal by abrasion.[3]

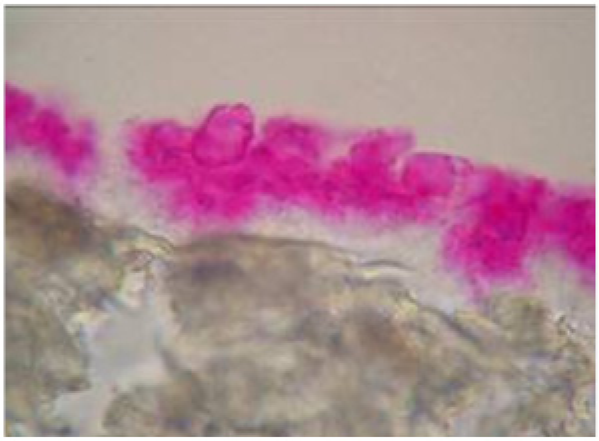

Figure 4 Dye based inkjet ink in mineral coating

The whole issue of colorant adhesion is a key one for security printing. Again, it can be considered counter-intuitive. In some industries, there is a drive towards technologies to promote deinking of print. However, in security printing there is a strong driver to promote the permanent bonding to the substrate. This is more akin to fine art than industrial printing.

Synthetic papers

Although paper is still a popular medium, there is a significant market for paper-like materials (such as non-woven polymers). These materials can produce enhanced physical properties such as tear resistance, and appear in some identity cards. Like paper, they can be manufactured to be compatible with various print processes and have some interesting and individual characteristics.

These materials can exhibit some interesting challenges when it comes to suitable printing technologies. Choosing an incorrect ink/media combination can result in some serious tamper and permanence issues.[4]

Polymer substrates

There is a growing market for polymer-based identity cards, commonly PVC or polycarbonate. The latter material is also used for the manufacture of passport pages containing personal data.

A common method of adding personal data to PVC cards is the use of thermal transfer printing.[5] For more secure applications it is common to protect this print through some form of lamination step.[6]

Polycarbonate printing is more commonly conducted with UV cure technology.

There is an opportunity for substrates engineered with features that enhance product security. Highly secure print for paper and polymer substrates is of specific interest here.

Laminates

It is common practice to shield sensitive personal data behind laminates in secure documents. Other methods have also been considered.[7] Lamination is performed to protect the print from both accidental damage and tampering. In common with conventional print, one of the key attributes of these laminates is the extent (or lack of) adhesion to both the substrate and the underlying print. Once again, each printing method has specific issues in terms of lamination performance.[8]

It is also common for these laminates to contain security features such as holograms, digital variable print and UV fluorescent features. Alternative optical features that do not obscure the underlying print are of significant interest here. As an example, periodic microlens arrays can produce a number of interesting optical effects.[9]

There is an opportunity in security printing for clear polymers that contain eye catching optical features. There is also a need for compact printers that can print onto laminate adhesive.

Printing technologies

It is noted above that a wide variety of printing techniques are used for secure documents. Some printing techniques such as offset lithography are noted for their fine detail at resolutions that were once unattainable using digital printing techniques.[10] This fine detail is commonly used as a feature in security printing as many digital printing techniques cannot match this.[11] Recently some of these techniques have come to approach lithographic printing for edge detail, notably liquid toner printing.[12] Digital presses such as the HP Indigo for example, are capable of producing 1/2400 of an inch features using liquid toner and extremely well-aligned color planes.[13] This is achieved using 1/800 of an inch dot size with 0, 1/3 and 2/3 pixel offset.

One interesting aspect of security printing is the use of multiple printing technologies overlaid in precise registration on the same document. It is common to see intaglio, lithographic, flexographic and digital printing technologies overlaid in some combination. The science of the interaction of these combinations is of interest in security printing, and aspects of this have been explored by some workers.[14] However, digital fabrication is making the same move to using multiple printing (or print-like stereolithographic) techniques for device manufacture.[15] Some of the knowledge gained here may also be applicable to secure document fabrication.

Inkjet printing has some very interesting characteristics for use in the field of security printing. As illustrated in Figure 2, aqueous dye based inks can penetrate some distance into paper and are thus difficult to remove physically. It has been shown that the ease of chemical removal is a function of a dye ink / media combination.[16] Pigmented inks however sit more on the surface as illustrated in Figure 3 and are therefore easier to physically remove.

There are opportunities in Security Printing for technologies that can enhance the durability of print to tampering. Pigmented inks with high durability are of particular interest.

Unusual inks

Security printing is an interesting market for unusual inks as this is a strong barrier to copying. Spot colours and unusual colour transitions are often employed and full photo quality printing is most often not needed.

One interesting aspect of this market is the use of IR and UV illuminants. Seemingly identical colorants can have different characteristics when viewed under IR illuminants.[17] Similarly UV fluorescence is often used to produce security artifacts.[10]

Secure documents also use optically variable printing. Examples of this are print that changes colour with viewing angle. These features are most commonly fabricated by conventional print such as silk screen. The challenge here is to introduce such inks with digital printing.

Multispectral illumination and angular variation of color offer particular challenges in colour and image science. Features and knowledge in this area are of particular interest.

Hardware for inspection & authentication

There is a significant market for print inspection hardware in security printing. For the very high end documents such as identity cards and passports bespoke readers exist.[10] These contain multispectral illuminants together with RFID subsystems. The integration of printed features, specific substrates and reader hardware allows for a high level of specificity in authentification.

Another example of this genre is the Dr. CID device that can be used to authenticate secure documents.[18] Paper has an interesting surface consisting of non-woven fibers. This surface can be characterized and used to uniquely distinguish individual prints using devices such as this.

Mobile readers

However it is in the field of mobile imaging where most interest lies. The capability of using consumer mobile imaging devices such as camera phones has great potential.[19] Solutions that can use such devices have great potential across this application area.

There is a potential need in this market for devices that can interrogate ink / media combinations to define secure features.

Axes of deterrence

Deterrence provided by security printing can be considered along at least six different axes:

1. Nature of encoded information
2. Level of image analysis
3. Role of person performing the authenticating
4. Utility of the encoded information
5. Extent of print variability
6. Complexity of the encoding

By the nature of encoded information, we mean whether the information is encoded in overt, covert, steganographic or forensic functionality. Overt objects are both visible and understood to contain readable information by the average person. Barcodes are perhaps the most obvious example of this. Covert printed objects contain information that is hidden in plain sight, and the means of decoding the content is not conveyed to at least some of the people having access to the physical item. Digital watermarks and UV/IR features are specific example. Steganographic security printing objects are marks that contain hidden information, even if the marks themselves are overt and well-understood to contain decodable information. Steganographic information can be contained by subtle text or logo manipulations, within the halftoning patterns themselves, or by the tacit addition of hue, intensity and/or saturation variation to printed areas. Forensic security printed information is used to identify with a certain degree of statistical confidence that a document, label, package or other surface is authentic. If properly protected and/or difficult to reproduce, forensic patterns will be re-used by fraudulent agents, rather than reproduced. In this case, the forensic mark must be re-use or tamper evident, as discussed below. Forensic materials – such as security substrates, security ink or substrate additives, and secure finishing coatings, laminates or procedures – must be protected from theft, and so constitute controlled substances/procedures.

The level of image analysis is important in security printing, as it defines the type of applications that can be initiated by the security printed object. Forensic image analysis is the most difficult to reproduce, with other forms of image authentication providing acceptable accuracy at the item level and forensic confidence at the cluster level. The level of image analysis required for authentication is therefore dependent on the density of information contained in the security printing object, the entropy in the information, and the inter-cluster specificity of the measurement. The greater the density of information, all other factors being equal, the greater the statistical confidence and the greater the chance a printed object can be used for true forensic confidence.

The role of person authenticating the security printed object is another means of defining the downstream applications and services that are initiated by decoding the object. Security printing is associated with a supply chain, value chain or other logistics-managed movement of content between different actors. The seven primary actors, generalized across most domains, are the manufacturer, the warehouse, the distributor, the retailer, the consumer, the inspector, and the forensic analyst.

The utility of the encoded information is an important factor when a hybridized security printing design is used. This is preferable when using variable data printing (VDP) because the amount of effort to craft multiple variable data regions is only marginally more than the effort required to implement one VDP feature. For this modest upfront effort, a wide variety of downstream advantages are garnered. In order to produce a truly secure printed feature, all three of the following utilities must be provided: (1) unique identifier, (2) copy prevention, and (3) tamper-evidence. A unique identifier (ID) is readily produced using variable data printing. The simplest unique ID is a serial number. Copy prevention is important for a minimum of one decodable object. Otherwise, a direct copy of the image can be made and falsely "authenticated". Clearly, the forensic character descriptors associated with the use of high-resolution imagers cannot be copied. However, if the complexity of an image is high, it will be very difficult to copy the image for forensic confidence at the individual object level; and certainly not at the cluster level. Tamper-evident objects are compromised when they are authenticated, making them single use. Associating a security feature with the tear strip means that it will be bisected when the package is opened. Scratch-off surfaces that must be rubbed away to access the unique ID underneath are another rational form of tamper-evidence.

The extent of print variability is used to craft the analytics for a security printing campaign. The analytics are, of course, the collection and digestion of information associated with the use of the security printing objects. Static printing, which is generally cheaper, does not provide a unique ID, and so mass serialization is usually provided by a low-cost thermal or other in-line printer. VDP opens the door for hybridization; that is, using different types of variable regions for different tasks. These include inspection, point of sale, authentication, unique ID/mass serialization, forensic authentication and URL embedding. From a security standpoint, VDP is very powerful: hybridization means that the relationship between multiple VDP objects can be varied from one security printing campaign to the next without requiring a change in the VDP objects used. This is an excellent way to make the counterfeiters spend more in reverse engineering the system. The logical extension of VDP is full customization. In full customization, everything printed can be made variable from one object to the next. This includes the layout, the relative spacing between text characters, and the amount of steganographic information added, among others. While full customization requires extensive processing overhead, modern printers boast massive – and massively parallel – processing capabilities, making this approach far less daunting than in years past.

The final factor considered is the complexity of the encoding. Here, the changing nature of printing plays a huge role. With 3D printing promising to replace many manufacturing processes in the years to come, it is obvious that many aspects of printing – both on the substrate and finishing ends – may eventually become absorbed into the printing process itself. From lamination of the substrate to textured finishing, 3D printing technologies stand on the brink of reducing the length and the complexity of the printing line. The simplest printing will continue to be "flat"; that is, a matter of printing one type of ink onto one type of surface. The security of this approach depends entirely on the degree of VDP implemented. Further complexity is accommodated by security printing when a thorough understanding of the printing and downstream imaging processes is applied to optimizing the information originally printed. Here, the printing is "pre-compensated" for the expected downstream effects. The two most effective forms of pre-compensation are structural and spectral. Structural pre-compensation is largely concerned with anticipating the manner in which ink will spread on a given substrate. For example, inkjetted inks will generally spread out more on a plastic or coated substrate than they will on a porous, cellulose-based substrate unless rapid drying or curing is implemented.

Printed electronics

One area where Printed Electronics is likely to see early adoption in Security Printing is the fabrication of antennae for RFID. Many identity documents now contain information stored electronically on silicon electronics that communicate with the outside world through a RF interface. This means that the document needs to contain a RF coil to receive a signal. At present many of these coils are made by traditional fabrication processes used for RFID manufacture. There are opportunities here for fabrication by printing processes and screen printing is already established in this field.[20] However, the field is widening and inkjet systems are now starting to emerge.[21] This widening choice of printing methods gives the potential for integration with other printed features such as bar codes.[22]

In common with packaging there is substantial market "pull" to incorporate some form of display into secure documents. There are examples of electrochromic displays being powered by remote RF activation.[23] This is a combination that could be particularly powerful in secure documents. The key technology innovations needed to bring this to fruition will be getting the right combination of flexibility, lifetime and functionality for this market.

Security printing is ready for printed electronic features with activation through RF coupling. Interesting combinations of overt, covert and forensic features are of interest.

3D printing

To a certain extent 3D printing already exists in the security sector, but not specifically from the digital domain. Intaglio printing is used in passports and banknotes to produce tactile features.[10] Microlens arrays also produce a characteristic "feel" to a document.[9] However, there are opportunities here for digitally printable features giving haptic modulation to give overt features to a document

The fabrication of optics is an area that has great potential within security printing. One area that has significant potential in this application is the ability to print both the visible content and the optics to view a 3D image.[24]

Conclusions

There are specific market and technical opportunities in the physics, chemistry and material science of security printing. The field of print inspection and verification has openings for new hardware and software applications too.

The evolving field of digital fabrication and 3D printing also has the potential to contribute to the future of secure documents.

The community present at this conference can make significant contributions to this field.

References

[1] M. A. Hopper, "Permanence of Dry Toner Based Documents", Proc. IS&T's Archiving conference, pp 49 – 52 (2004).

[2] D Tyagi, M Zoretsky, T Tombs, P Lambert, "Use of Clear Toner in Electrophotography for Security Applications", Proc. IS&T's NIP24, pp773 – 776 (2008).

[3] T. Eguchi, Y. Ueda, H. Takahashi, "Abrasion Resistance of Aqueous Pigmented Inkjet Inks on Coated Paper", Proc. IS&T's NIP 27 conference, pp201 – 204, (2011).

[4] A. L. Fricker, P Green, A. Hodgson, "An Evaluation of the Humidity Test Method ISO 18946", Proc. IS&T's NIP 27 conference, pp267 – 270, (2011).

[5] D. Kato, H. Akamatsu, Y. Moto, N. Matsukubo, A. Fukami, K. Nakada, "Development of High Quality True Edge Printhead for Card Printer", Proc. IS&T's NIP 27 conference, pp670 – 673, (2011).

[6] H. Taniguchi, S. Sunada, J. Oi , "Novel Approach to Plastic Card Overcoating Process", Proc. IS&T's NIP 28 conference, pp84 – 87, (2012).

[7] S Muke, P Fox, W Jackson, "Improvements in Document Security – The Next Generation", Proc. International Congress of Imaging Science, pp 424 – 427, (2006).

[8] G. Song, G. Sisler, S. Yang, K. Halfyard, E. Zwartz "Understanding Post Finishing Performance of Xerographic Prints", Proc. IS&T's NIP 28 conference, pp120 – 123, (2012).

[9] D S Dunn, T L Potts, L E Lorimor, J M Jonza, R M Smithson, S P Maki, "Three-dimensional floating images as overt security features", Proc. SPIE, Vol. 6075, 60750G (2006); doi:10.1117/12.640539.

[10] A. Hodgson "Technologies for Identity Document Verification", Proc. IS&T's NIP 26 conference, pp587-590 (2010).

[11] X. Rong, "Print Quality Comparison Between Kodak Prosper and Offset Lithography", Proc. IS&T's NIP 26 conference, pp256-259 (2010).

[12] B. M. Gamm, F. Frey, S. Farnand , "An Analysis of the Factors Influencing Paper Selection for Books of Reproduced Fine Art Printed on Digital Presses", Proc. IS&T's NIP 27 conference, pp791 – 796, (2011).

[13] http://h10010.www1.hp.com/wwpc/nz/en/ga/WF06b/18972-18972-236257-3638783-3638783-3382246-3382249.html?dnr=1.

[14] V. Alecrim, M. Andersson, "Flexographic ink film's resistance to inkjet ink's solvent flow in Hybrid Printing", Proc. IS&T's NIP 27 conference, pp79 – 85, (2011).

[15] R.R. Baumann, "Industrial Printing Beyond Color", Proc. IS&T's NIP 23 conference, pp759 – 761, (2007).

[16] A. Schiller, W. Rauh, T. Kuen, Fogra Research Report 45.001 (2012).

[17] V. Žiljak, K. Pap, I. Žiljak, "CMYKIR security graphics separation in the infrared area", Infrared Physics & Technology 52, 62–69, (2009).

[18] Adams G, Pollard S, Simske S: High-Resolution Imaging for Forensics and Security. NIP26: 26th International Conference on Digital Printing Technologies and Digital Fabrication 2010, 582-586, 2010.

[19] M. Gaubatz, S. Pollard, R. Ulichney, S. Simske , "Mobile Capture of High-Resolution Data-Bearing Markings", Proc. IS&T's NIP 28 conference, pp371 – 374, (2012).

[20] S. Farnsworth; K. Schroder, B. Wenz, D. Pope, I. Rawson ,"The Photonic Curing Process for Printed Electronics with Applications to Printed RFID Tags and Thin Film Transistors", Proc. IS&T's NIP 28 conference, pp440 – 443, (2012).

[21] V. Sanchez-Romaguera, S. G. Yeates, M. A. Ziai, J. C. Batchelor, E. A. Parker, "Enabling Low Cost UHF RFID Transfer Tattoo Tags by Inkjet Printing Means", Proc. IS&T's NIP 28 conference, pp568 – 570, (2012).

[22] S. J. Simske, J. S. Aronoff, B, Duncan, "Printed Antennas for Combined RFID and 2D Barcodes", Proc. IS&T's NIP 27 conference, pp544 – 547, (2011).

[23] D. Zipperer, "Printed Electronics for Flexible Applications", Proc. IS&T's NIP 27 conference, pp452 – 453, (2011).

[24] K. Yanaka, N. Kira, H. Kasuga " Integral Photography Using 2D Printer Output and Fly's Eye Lens Made with 3D Printer", Proc. IS&T's NIP 28 conference, pp273 – 276, (2012).

Author Biography

Alan has 30 years experience in printed hard copy and a background in photography and image science. Alan previously managed R&D and Technical Services groups active in inkjet application development. For 4 years he worked on printing and optics consultancy projects that often crossed over into security applications. In November 2008 he joined the Technology & Innovations group of 3M Security Printing and Systems Limited (now 3M Chadderton) in the UK as Technical Development Manager, specialising in print solutions for high security documents such as passports and identity cards.

Alan is active in Printed Electronics, both as a practitioner and Chair of IEC TC119 (Printed Electronics).

Alan has a BSc in colorant chemistry and a PhD in instrumentation, both from the Department of Chemistry at the University of Manchester. He has served as session chair, short course instructor, and presenter at a number of IS&T conferences such as NIP, DF, Archiving, and ICIS; he was Short Course Chair for Archiving 2008. He is President of the IS&T