Inkjet Printing for Secure Documents

Alan Hodgson, Alan Hodgson Consulting Ltd, Bollington, Cheshire, United Kingdom; Matt Hensman, Sale, Greater Manchester, United Kingdom; David Westgate, National Document Fraud Unit, Hayes, United Kingdom.

Abstract

This paper presents some of the specific challenges and opportunities for inkjet in the security printing sector. It follows on from a paper at this conference last year that examined the place of toner based printing.[1] Both papers examine the technical problems that are specific to this market sector and the opportunities that arise from these, particularly in the area of the physics and chemistry of the materials in the digital printing process. In this paper particular emphasis will be given to the challenge inkjet faces in security paper printing as market requirements diverge from typical office based inkjet.

This work examines the wetting and penetration of inkjet ink on security printing substrates. Inkjet engines used in this market sector from a number of manufacturers and generations are discussed and results presented. The implications of practical variables such as print driver settings are also included.

The challenges of Security Printing

Security printing is in itself a broad applications space. It has the broad aims of deterring forgery and counterfeiting of documents and goods. The level of this deterrence depends on the technologies deployed and is in turn determined by the perceived need.

Paper is a common substrate in security document applications both in passports and visas but also in a variety of other documents that are deemed to have security applications, such as birth certificates. As such this work concentrates on the inkjet printing of paper substrates for secure document applications. At the top end of these needs are national identity documents for border protection such as passports and entry visas.[2]

At this time passports utilise a number of material types in their production. The pages that hold the key identification data such as portrait, personal text and machine readable (optical) information may be printed onto paper or polycarbonate and protected by an over laminate. Even in passports with a polycarbonate page component there are other printable areas that are made of a secure paper substrate. The entry visas, stuck into the passport book are exclusively paper based. As such paper printing remains a substantial requirement in secure document production.

Secure document production, even on paper substrates is a rather specific application with challenges that may well be unique in the digital printing space. As a result the technical requirements differ somewhat from mainstream applications and are evolving in different directions. A number of these challenges can be considered as counter intuitive to those more used to mainstream applications.[3] Two major areas will be covered in detail in this work.

- Substrate surface physics. Secure documents in general use substrates many in the printing world would class as unusual and challenging. They are pre-printed with a security design so the digital print often has to wet and adhere to both print and paper. A typical example would be the use of print processes and UV cured inks that alter the wetting characteristics of the paper surface.
- Penetration into the substrate. Office and commercial printing technologies have evolved to retain the colorants on the surface of the substrate, maximising print quality in both the colour and spatial dimensions. This also has an impact on the deinking characteristics of the resultant print.[4] However, a somewhat different driver exists in secure document printing. The printed document must be resistant to the removal of the colorant as this would compromise both the identity of the bearer and border security. Colorant penetration is a key enabler for print security in this application space.

Desktop inkjet print engines are typically used in this market on paper substrates. For visa applications these are commonly unmodified consumer desktop printers while for passports these are inkjet engines placed within bespoke hardware. However, market forces in the wider print applications space are pulling printer development on a path that in general diverges from secure document production. The increased reliance on pigment based inksets reduces colorant penetration into the substrate and can increase drying time on these particular papers. Visibility in the Near IR (NIR) is a common need in this application and the majority of dye based inks (and coloured pigments) have little or no optical density here.

Substrate assemblies used in Security Printing

The base papers used in security document applications are manufactured by suppliers who specialise in papers for this sector. Such materials are used across the range of secure credentials including certificates, passports and entry visas and hence their use is restricted to such applications.

Security papers are typically characterised as being largely chemical wood pulp based. Weight varies according to the application but can be anything from 50 to 100gsm or so, comprising a mix of different hard and softwood fibres to meet the required performance of the paper. They can where necessary also contain other cellulose materials to provide additional physical characteristics such as paper strength and durability. The papers are usually uncoated, and omit any optical brightening agent content. This is in order to facilitate the inclusion of covert UV fluorescent security features within the overall design and construction of the document. In many cases the paper will also contain a bespoke watermark image within the paper, a further security feature to enhance the overall security of the base material and the document.

Passport applications

In passport applications, the biographical variable data is printed on to an inner leaf of the book, referred to as the bio-data page. Paper based bio-data pages include a secure watermark within the base paper construction and are printed with a secure design theme containing numerous security features. A standard passport will usually have a validity of between 5 and 10 years; hence materials used must be both durable for the lifetime of the book and secure, with features that counter attempts from tampering, alteration and counterfeiting.

For passport applications the paper bio-data page security is enhanced by the inclusion of a protective laminate, applied across the page after personalisation, which helps to protect the biographical details. These laminates, or overlays as they can also be known, carry additional and different security features to that of the bio-data page, to further enhance security and are often a combination of both printed and holographic security techniques. As a result the passport holder's data is protected by both the page construction and the multiplicity of security features layered therein.

Visa applications

In the case of entry visas, these documents are printed with design themes and numerous security features, using specialised printing techniques and are personalised with variable data prior to being applied to an inner page of a passport booklet. Their construction can be described as being similar to that of a pressure sensitive label, with the security paper forming the "label" element of the construction and suitably coated on the reverse with an adhesive layer that is then supported on a silicone coated carrier base material.

Print processes used in Security Printing

Documents such as passports and entry visas have as a requirement highly complex designs that contain a wide range of security features combined with an aesthetic appeal. To achieve this it is common for these documents to use a range of secure printing techniques, printed in close register to achieve the desired levels of security. The main print technologies include offset lithography, letterpress (frequently in offset form) and intaglio printing.[5] Others print process may also be used where appropriate, to achieve a desired feature or effect.

Offset lithography is used widely across secure credentials. It is a planographic print technique, i.e. that plate is in a flat plane and it uses a blanket to "offset" the image from the plate on to the paper. It is used in conjunction with security inks, to print the complex multi-colour designs with fine levels of detail within them. In similar fashion Dry Offset (letterpress) is a relief printing technique that is also used in conjunction with lithographic printing to create the complex multi-colour designs.

Some of the print processes used can calendar the paper surface, making the absorption and adhesion of liquid inks more difficult. A good example of this commonly used in high security documents is Intaglio printing. Intaglio is a specialised process that is the preserve of high security documents and currency. It is characterised by high ink weights that when printed on to the sheet create a tactile effect to the print. It can also be used to apply security inks which have large pigment sizes, for specific effects. Another feature of the Intaglio process are the high pressures used to effect image transfer from plate to substrate. The pressure is such that it acts as a smoothing process to the surface of the paper. In doing so the surface characteristics of the paper are altered, reducing porosity and increasing the gloss and thus impacting upon the personalisation interactions. Where a document is to include intaglio print, the calendaring effect of this process should be factored in to the overall document solution.

Inkjet printing for secure documents

As described above, paper is a common and interesting substrate for security documents. The document design is printed using the impact printing techniques also described above. However the personal details of the bearer must then be added by digital techniques and inkjet technology is commonly used in this personalisation step. Probably the most demanding application here is the personalisation of the entry visa so this work concentrates on this area. However, the lessons learnt are applicable in many cases to other security document applications.

The market for visa personalisation printing is substantial for desktop inkjet. The United Kingdom issues over 3 million visas a year in various formats and the European Union nearly 30 million. And Europe is not alone in using this technology.

Toner based printers had a traditional speed advantages over inkjet systems and the prints do not emerge wet from the printer. However, they do suffer from poor adhesion and colorant penetration.[1]

User requirements for inkjet personalisation

The biggest problem faced in this market sector is the integrity of the system from beginning to end. As intimated above this is a very different application area than standard office or photo desktop inkjet.

- The substrates themselves are secure and must all be accounted for. An unpersonalised visa is of significant value to a criminal and significant risk to a nation state. All spoilages must be accounted for. It should be noted here that self adhesive visas are not the easiest media to transport and some desktop printers do not cope with these at all well. They are analogous to thick label stock and often come in unusual formats.
- The surface of these substrates can be difficult to print. Any calendaring of the surface inhibits ink absorption and the inks used to produce the security preprint may render areas of the substrate somewhat impermeable and hydrophobic.
- When dry the inkjet inks they must resist tampering (physical and chemical). The permanence of the personalisation data is a critical consideration in this application – deinking in this case is not an acceptable attribute.[4]
- Coated substrates are used extensively in desktop inkjet applications to improve image quality and print permanence. However these are not used on security substrates as it provides another avenue for forgery.
- Machine readable text data under IR illumination is a critical requirement.

From these flow a number of specific user requirements for an inkjet printer to be used in visa printing applications:

1. Quick drying. Visas come out of the printer and are immediately placed into the passport or travel document. The back of the visa normally incorporates a permanent pressure sensitive adhesive coating. As a result the visa is pressed down onto the page to stick it in. This is usually done by rubbing across the freshly printed surface with the side of the fist to ensure that the visa is properly stuck in place. This is

not so good if the ink is not suitably dry as the ink smudges resulting in poor image quality and machine reading.

2. Adhesion of the ink to the visa substrate. Although pigmented inkjet inks give higher resistance to chemical tampering methods they do result in the ink sitting mainly on the surface of the substrate, rather than protectively adsorbed within the paper. As a result they are more prone to be removed through physical abrasion. This has proved to be the case with the highly calendared surface of visa documents but has also been recognised on more common printing substrates.[6]
3. IR readability is now vitally important these identity documents. Passport reader devices of the type used at border control contain IR LED illumination at around 850 - 950nm. This is used to interrogate machine readable text within the document.[2]

Desktop inkjet history and Security Print

It is instructive to examine how the evolution of desktop inkjet systems has impacted this area of Security Printing as this may give guidance to the applicability of future systems.

Early desktop inkjet systems majored on dye based inks that had significant penetration into paper substrates. As these systems developed the drying time onto paper became good and these gave high physical security but with low resistance to chemical attack. In photo applications this manifests itself as poor image permanence. These systems also showed poor IR visibility.

From a security printing perspective the widespread move to pigmented inks gave new opportunities and challenges.

- Desktop photo applications combined innovative coated substrates with pigmented inks to give outstanding environmental permanence. However coated substrates are less acceptable in security printing for a number of reasons, particularly in that they produce another access route to document alteration.
- New ink formulations appeared that were optimized for plain paper. However, on the highly calendared surface of security printing substrates these produce much extended drying times compared with dye based inks.

All these pigmented ink systems raise new benefits and challenges for security printing. In terms of opportunities they have much increased resistance to chemical attack and pigment black formulations have excellent visibility in the IR. However the challenges that counter these are that because the colorants are now on the surface of the substrate they are much more accessible to abrasion and physical tampering.

Printer evaluation for secure paper substrates

Following on from the above analysis the evaluation work concentrated on 2 main areas. First of all, aspects of the ink / paper interaction that in this application manifest mainly in smudge resistance. Second, a demonstration of IR visibility issues as these are not normally considered in this conference community. This will also include the implications of practical variables such as print driver settings. It will be shown that inkjet systems of different generations and manufacturers produce markedly different results when used in this security printing market, a difference not apparent on traditional plain paper substrates.

Printers and document readers used

An informal study of the desktop inkjet printers in use for paper visas within the European Union was conducted. It yielded a list of printers that are or have been used across this community that guided this research. The prints were all made on a single international entry visa substrate that is currently in use within the European Union and is indicative of the characteristics of paper used within this application area.

The document reader was typical of those used internationally to read and verify identity documents. These systems combine an RGB color camera with white, UV and IR light illumination options to reveal any security features. They can illuminate and capture optical data taking in a full passport page. They are designed to read passports, visas, national ID cards and many other travel documents.[2] As they can also save the images to file these are used to illustrate this section.

Ink / paper interactions – smudge resistance

As described above, the usage method employed in this application can be very different to that of mainstream desktop applications. Like a self adhesive label, visas are first printed and then applied to a passport page. As a result they are prone to image smear, particularly if there are time pressures on the user.

The potential extent of this problem is illustrated in Figure 1.

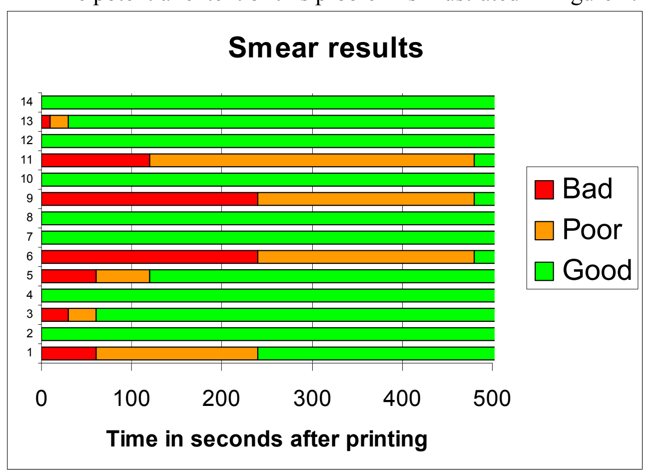

Figure 1 Smear results from printer / ink / driver combinations on a visa

Figure 1 was constructed by taking 14 different desktop printer / ink / print driver settings and printing a black square approximately $1cm^2$. These were then tested for smear resistance using a dry thumb using a constant method across the sample set. The test was done at a number of different times after the ink hit the surface and the results assessed subjectively and placed into 3 different categories (Bad, Poor and Good). Although this is a very subjective methodology it will be seen from Figure 1 that it is perfectly adequate to separate the systems under test. The following points should be noted from this sample set.

- Some samples were rated as good as they were dry straight from the printer. These were predominantly (although not exclusively) dye based blacks.
- Amongst the pigment black inks tested there was a wide variety of smear results. Some were rated as poor even after a 480 second (8 minutes) drying time. This makes the system unacceptable in a practical usage situation.

By way of comparison the test was repeated on standard plain copier paper. Only those desktop printer / ink / print driver settings that caused significant smear on the calendared visa material (Figure 1) were included in this case. The results are illustrated in Figure 2.

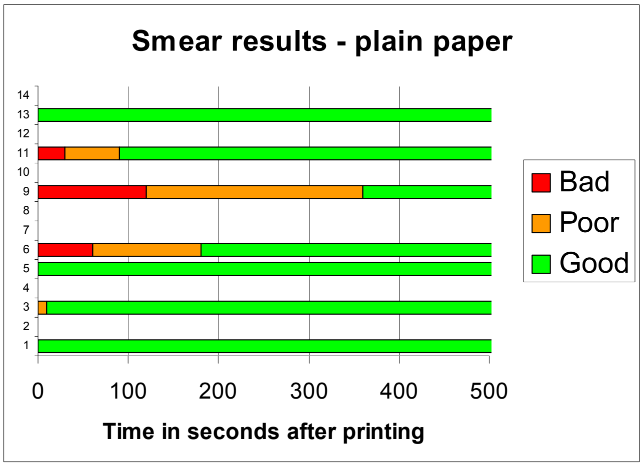

Figure 2 Smear results from printer / ink / driver combinations on plain paper

It can be seen from a comparison of Figure 1 Figure 2 that visa stock is much more of a challenge as a printing substrate than plain paper. Combinations such as 1, 5 and 13 that show significant smear on the visa substrate are completely free from this on plain paper. This shows the extent of the challenge faced by the selection of desktop inkjet solutions for visa printing.

Ink / paper interactions – colorant penetration

As noted above there is a market need in security document printing to promote penetration into the document surface to deter tampering. Examples of this are illustrated in Figure 3, taken from previous work shown at this conference.[3]

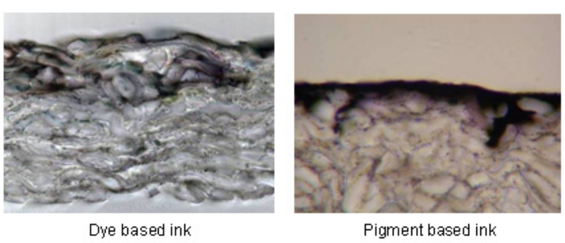

Figure 3 Penetration of dye and pigment inks

Figure 3 shows cross sections cut into a security paper substrate printed with dye and pigment based inkjet inks. The dye based ink penetrates into the substrate so is difficult to remove by abrasion. In contrast to this a pigment ink is predominantly on the surface, making it more accessible to physical tampering. A toner based print has the same problem with colorants accessible on the surface of the print.[4]

Other ink / paper interaction issues

Another ink / paper interaction effect that is visible on these samples is coalescence.[7] As the paper samples used in this work had all been calendared by the intaglio printing step they were also subject to coalescence artefacts. Whilst coalescence was observed on these samples it was insignificant compared to the practical effects of low drying speed and the consequent issues of image smear. As a result, apart from noting the effect this was not quantified further, even though measurement methodologies exist.[8] It should however be noted that poor results for coalescence did not correlate with poor results for smear in this sample set.

Security document printing is also unusual as an inkjet printing application in that the ink is in some cases required to be applied on previously applied offset litho printed designs. The offset litho printing often uses UV cured inks which would be expected to render the surface hydrophobic and therefore difficult to print. In the case of the visa stock this effect was found to be insignificant compared to the calendaring process of intaglio printing. However, for applications such as passport page printing where an intaglio step is not used, this is much more an issue.

Visibility under IR light

Various groups have explored the option of hiding information in prints that are invisible by eye but rendered readable in the IR.[9] For this evaluation our concern was simply the visibility of black text to enable Optical Character Recognition (OCR) for the purpose of machine readability. The visibility of black text is a key criterion for the applicability of a desktop printer / ink / print driver setting combination for visa printing. As a result this was assessed as part of this work on the samples illustrated in Figure 1.

Experimental method

CMYK swatches were printed at approximately 1cm^2 dimensions with the relevant desktop printer / ink / print driver settings onto intaglio pressed visa paper in an area that was free from intaglio ink. This gave a print swatch free from other ink but with identical surface to a real visa.

The samples were visualised by placing them on the platen of an industry standard passport reader.[2] These systems allow a user to illuminate the samples with white, UV and IR light and collect the image using a RGB colour camera. These images were used to generate Figure 4 and Figure 5.

Figure 4 illustrates the case of a desktop printer / ink / print driver system that utilises a pigment black and dye based colours.

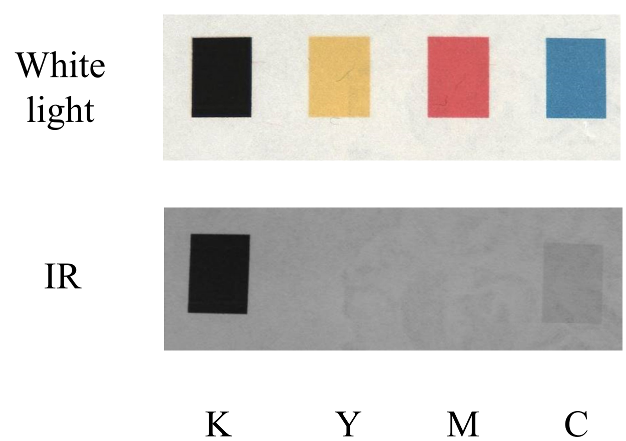

Figure 4 Pigment K and dye CMY visualised in a passport reader

As expected all the colorants are brightly visible under white light illumination. Under IR illumination the pigment black ink has good optical density but the CMY colorants are almost invisible. This high optical density of the pigment black results in good contrast from black text on any coloured printed background, making for highly effective machine reading of text information.

However, a different situation exists if a desktop printer / ink / print driver system is used that only utilises a dye based black ink. This is illustrated in Figure 5.

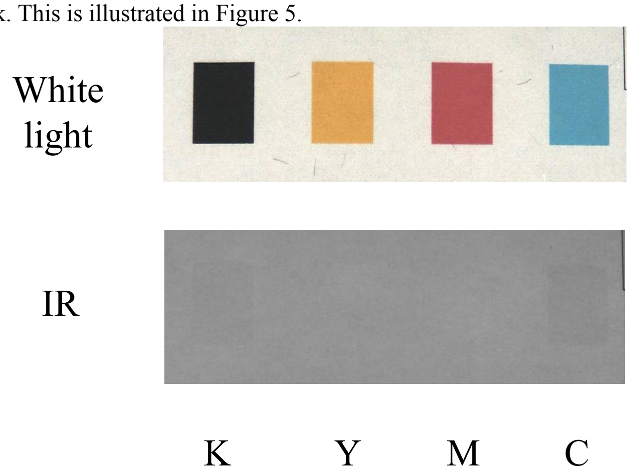

Figure 5 Dye based CMYK visualised in a passport reader

In this case the use of the dye black ink manifests in almost zero visibility in the IR image. As a result machine reading of text information will fail. This desktop printer / ink / print driver combination is wholly unsuited to visa personalisation.

There is a potential trap for an unwary user in this application space. A number of the desktop printers used in this evaluation have options in the printer driver settings that disable the pigment black. Selection of this option can render an otherwise acceptable print unreadable in the IR without this change being apparent to a user inspecting by eye.

It should be noted that in the case of Figure 4 and Figure 5 dye based CMY inks were used. Similar low optical densities in the IR are produced by pigmented CMY inks.

Discussion and conclusions

This work has highlighted two major criteria for acceptability of a desktop printer / ink / print driver combination for use in the inkjet printing of secure documents on a paper substrate. It has used as an example the printing of personal details on entry visas but the work is applicable to a wider application space, particularly the personalisation of passport bio-data pages. The two major criteria are smudge resistance and IR visibility of black text. A perceptive reader will by now have realised that these are to some extent mutually exclusive.

IR visibility in these desktop printer / ink / print driver systems is the preserve of a pigment black ink. However, pigment black inks are prone to substantially greater image smear and drying times than dye based inks.

While dye based inks are more prone to attack by chemical means pigmented inks tend to reside on the surface of substrates. This makes them more accessible to abrasive attacks. And the levels of pigment black are in some cases a function of printer driver settings.

These issues are in many ways mirrored for the use of desktop toner based engines in this application. Toner is good for IR visibility and image smear but has very poor resistance to abrasive attacks due to minimal colorant penetration into the substrate. The adhesion is often poor and can be a strong function of the printer driver settings.[1]

Opportunities for the digital printing community

There are a number of opportunities for desktop printer manufacturers to contribute in this area of Security Printing. Here are a few examples.

1. Some specialist manufactures supply bespoke inkjet systems to personalise both passports and visas. These incorporate OEM engines from the desktop inkjet space. Adding creativity within these could produce substantial benefits in terms of product security and competitive advantage.
2. Inks that combine both pigments and dyes could be particularly strong in this market, as would be IR absorbing dyes.
3. The divergence of mainstream desktop inkjet applications from security printing is a difficulty. There is the potential for page wide inkjet printing to bridge this with high throughput and rapid drying, but only if the other characteristics can be made to fit.
4. From a software perspective the capability to lock the driver and / or produce bespoke colorant combinations could confer market advantage.
5. This may be an area that is appropriate for a future International Standard, setting out the minimum features that must be present in a personalisation system for entry visas.

The route forward is for the inkjet and security print communities to work together to produce more suitable solutions for these needs. And a safer world.

References

[1] A. Hodgson and L. A. Williams, “Toner printing for secure documents”, IS&T’s 30th International Conference on Digital Printing Technologies”, 2014, 249 – 253.

[2] A. Hodgson, “Technologies for Identity Document Verification”, IS&T’s 26th International Conference on Digital Printing Technologies and Digital Fabrication, 2010, 587 – 590.

[3] A. Hodgson and S. Simske, “Challenges in Security Printing”, IS&T’s 29th International Conference on Digital Printing Technologies and Digital Fabrication, 2013**,** 148-152.

[4] A. Fisher, “What makes a digital print recyclable? Results of a European Survey”, IS&T’s 22^{nd} International Conference on Digital Printing Technologies and Digital Fabrication, 2009, 514-516.

[5] H Kipphan, “Handbook of Print Media”, ISBN 978-3-540-67326-2, 2001.

[6] D. Nishimura, G. Salesin, P. Adelstein, and D. Burge, “Abrasion of Digital Reflection Prints: The Abrasiveness of Common Surfaces and

the Vulnerability of Print Processes", 2009, http://www.dp3project.org/.
[7] N. Jones, S. J. Sargeant, K. Sargeant, J. C. Briggs, and M-K. Tse, "Characterizing and Modeling Coalescence in Inkjet Printing", IS&T's 14th International Conference on Digital Printing Technologies and Digital Fabrication, 1998.
[8] ISO/IEC 13660, "Information technology — Office equipment — Measurement of image quality attributes for hardcopy output — Binary monochrome text and graphic images", 2001.
[9] V Žilak, K Pap, I Žilak, "CMYKIR security graphics separation in the infrared area", Infrared Physics & Technology 52, 2009, 62-69.

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. He has also spent 7 years at 3M, specialising in print solutions for high security documents such as passports and identity cards. He has recently returned to his consultancy business, working on printing consultancy projects that include security applications.

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; he is Short Course Instructor for a Security Print short course at this conference. He was President of the IS&T 2013 to 2015.