# Technologies for Identity Document Verification

***Alan Hodgson; 3M Security Printing and Systems Ltd.; Oldham, United Kingdom***

## Abstract

*This paper will examine a number of key technologies used to authenticate identity documents. In the most common practical use these documents are examined by busy inspectors using the unaided eye. The paper will therefore commence with a summary of the attributes of the key printing technologies that have evolved to keep these documents secure. It will also outline the technologies used by the counterfeiter to copy these documents.*

*It will then go on to examine some of the other devices used for verification such as the hand lens, UV illumination and retro-reflective viewers. Throughout this treatment the contribution of Non-Impact Printing technologies will be highlighted, both from the perspective of the security printer and the forger/ counterfeiter. The potential for both NIP and Digital Fabrication technologies to contribute to future secure solutions is emphasized.*

## Introduction

A secure document contains a wide variety of security devices to provide verification of its provenance and to protect against forgery and counterfeiting. This is particularly true in the case of an identity document where national security concerns require increased levels of security.

Documents that are used as proof of identity such as passports, identification cards and drivers licenses are often targeted with the aim of changing or duplicating these for a range of criminal activities. Sometimes these can be used as "breeder" documents to obtain genuine legal documents to a false identity. As a result any identity document that is easy to change or duplicate can become a national security or economic threat and thus substantial effort is taken to make this as near to impossible as is practicable.

In addition these documents should include multiple levels of security that are often placed into 3 categories.

- Overt features. These are apparent to the general population who would use these documents. Examples include tactile features and watermarks. The best of these are difficult and expensive to duplicate and can be quickly examined and verified with little or no equipment.
- Covert features. These generally require some equipment to render visible. Probably the best known of these features are fluorescent artifacts that are rendered visible under a variety of UV lamps. Another similar feature considered here is microtext printing [1].
- Forensic features. These are artifacts known only to the print provider and the relevant authorities and can be used as an addition method of verification, often in a laboratory setting. An example of this would be deliberate errors in a specific placement and the use of taggants. The subject of forensic analysis of fraudulent documents has been the subject of a recent paper at this conference [2].

However, there is potentially a conflict of requirements here. Although the document should provide the utmost security to the identity of the holder it is most often necessary for the validity to be assured quickly and easily with the minimum of sophisticated and costly hardware. And given that documents such as passports, identity cards and driving licenses will be required by large segments of the population the cost of the individual documents must also be kept to an acceptable level.

Digital non impact printing technologies are both opportunity and threat in this area. They have become used extensively in the legitimate production of these documents but have also been shown to be used extensively for security document counterfeiting [3]. As the digital printing industry evolves the threats and opportunities this presents become ever more real.

Although this paper concentrates on identity documents much of the content is applicable to other secure document applications too.

## Traditional technologies

An identity document has traditionally included a mix of printing technologies and designs specifically to make copying difficult [4]. Multiple technologies, typically litho and intaglio printing made the best use of the attributes of these techniques. Unusual fonts, out of gamut colors and complicated fine line guilloche patterns were incorporated into the print design. On the media side watermarks and specialty papers have been widely used. In terms of inks unusual colors and fluorescent markers are used. However, a number of these artifacts are now under threat from digital printing technologies.

It is interesting to note that some of the technologies that have been the most difficult to copy (such as watermarks and fine intaglio print) are some of the oldest. However, even these technologies are now under threat from Non Impact Printing and Digital Fabrication technologies.

### *Tactile features*

This is traditionally a feature that has been produced by the intaglio printing process [4]. However, digital printing systems that provide some tactile features are now appearing [5]. In particular inkjet printing is now a contender against traditional tactile features for Braille printing [6]. As a result it can now be seen to be a contender to reproduce tactile features.

### *Watermarks*

Over the last few years printing technologies have appeared that can give a passable impression of a watermark by printing "clear ink" that resembles a true watermark [7]. Although others have appeared from companies such as Xerox and Canon possibly

the best documented example for security applications comes from Eastman Kodak [5].

### *Microprinting*

Traditional microprinting consisted of fine detail printed by conventional impact methods such as litho printing. As a result of this printing process it was static – the same on each personalized document. The protection lay in the fact that the intricate interlocking patterns and fine text was difficult to duplicate.

However, digital printing techniques have the potential to erode this difficulty. Microtext (fonts below 1 point size) are now within the capabilities of digital printing technologies [1]. Although this now opens up the possibility of variable data printing of fine characters it also means that the resolution advantage of traditional fine line printing is now narrowing.

### *Protecting the biometrics*

In the case of printed biometrics the portrait image and personalized markings (name, identifying number and key dates) must be kept highly secure against alteration. Any attempt to tamper with the photograph area in particular must be made particularly obvious.

The normal method is to cover these with a security laminate after printing but other methods have been considered [8]. These laminates in themselves often contain security features such as holograms and UV fluorescent features. One interesting development is the use of microlens arrays in such laminates to produce security verification functions. The combination of a periodic microlens array and underlying detail can produce a number of interesting optical effects [9].

## Verification technologies

There is a whole cascade of technologies available to verify the integrity of an identity document. This section presents these roughly in order of decreasing prevalence and increasing technology and brings us from overt to covert features. We start with an unaided observer, moving through increasing complexity of electro-technology through to complex optical artifacts that bring us full circle to unaided tactile and visual inspection.

### *Tactile and visual inspection*

This is the simplest and least costly of the verification technologies. As a result it is by far the most prevalent. However, even though it could be perceived as low technology we should not consider it as simply a "cheap option". Skilled examiners such as those found on border control are adept at distinguishing real from suspect documents using 3 basic senses.

- Touch. Intaglio print produces very a very distinctive surface topography that is easy to distinguish by touch. Embossed features in laminates and card manufacture can also be considered in this category.
  The threat here is that technologies currently under development for 3 dimensional printing could be used to undermine this security feature.
- Sight. The visual impression of fine print in register with the various features and color technologies such as spot color and "rainbow printing" [4]. This category also includes optically variable devices where the visual perception varies with illumination and visual angle to the document. Examples of these would include holograms and color shifting inks. Finally we have watermarks in paper substrates that are visible in transmitted light.
  The threat here is that increasing accuracy of digital print placement and technologies that mimic watermarks could undermine these too. Multiple and spot color inkjet engines, increasingly available in commercial printing could prejudice the security of some of the color technologies outlined here.
- Sound. Possibly the least obvious of these three senses for document verification. Some documents such as polycarbonate cards have a very distinctive "ring" when tapped or dropped. This is a common method to distinguish true polycarbonate assemblies from counterfeit copies on other substrates.

### *The hand lens*

The impact printing technologies commonly employed in security printing are capable of generating image detail too fine to be perceived by the unaided eye. As a result there is further information that can be perceived using a hand lens giving around 10x magnification. This is currently a very good way of distinguishing the resolution of desktop printing copies from true impact security print. Hand lenses are also an affordable technology available worldwide.

A hand lens will also reveal the "quantum" nature of inkjet prints on many substrates. This effect plus the usual CMYK nature of digital prints allows these to be distinguished.

The threat here is again the increasing resolution of digital printing technologies plus the proliferation of different spot color variants. However, there are opportunities here for the printing community. Digital printing techniques that can produce fine details that cannot be reproduced by readily available printing technologies could find a market in security printing.

### *The UV lamp*

This technology relies on fluorescence and has several aspects. One concerns the substrates, the other the colorants. Finally there is the location of the fluorescent feature. Judicious choice of the combination can produce some highly secure features.

- Printing substrates that exhibit no fluorescence. This is particularly powerful for paper substrates where it is most common for materials to contain some optical brightening agents (OBAs) which are also subject to degradation [10]. As a result the paper substrates in a passport book contain no OBAs, making them easy to distinguish and stable over time.
- Fluorescent colorants. These are now available in a whole variety of forms showing different fluorescent excitation and emission wavelengths. Some systems are also available with very narrow excitation wavelengths that are only revealed under very specific light sources. They can be printed using

inkjet, toner or thermal transfer [11]. The use of quantum dots in this field is of particular interest [12].

- The location of the fluorescent feature. Modern identity documents consist of multiple layers and features can be placed in various locations within this stack. Printed features as described above are of obvious interest but a further option is to place fluorescent artifacts within the security laminate layer.

The interest in the use of UV features has been increased by the development of UV Light Emitting Diode (LED) sources. Previously gas discharge lamps were used as the UV source. These had cost, bulk and power disadvantages. The ready availability of compact, low cost battery powered UV emitting LED lamps has encouraged interest in this area.

This is an area where colorant and ink suppliers can be of service to the security printing industry. There is an ongoing need for new components in this field.

### *Passport scanners*

These devices are designed for use in self-service kiosks, automated border control systems and busy immigration control desks. With more and more airline passengers using self-service kiosks to check-in for international flights, there is a growing need for easy-to-use but highly accurate passport scanners.

*Figure 1 Passport Scanner from Rochford Thompson*

These systems, illustrated in Figure 1 combine Optical Character Recognition (OCR) technology with a scanner capable of taking a full passport page. They are designed to read passports, visas, national ID cards and many other travel documents in any orientation.

The devices contain an RGB color camera with white, UV and IR light illumination options to reveal any security features. They also commonly include RF capability to enable the simultaneous acquisition of the image data from the page, the machine readable code lines through OCR and data from the contactless chip.

The incorporation of IR readability allows for some interesting printing artifacts to be produced. As an example, a carbon black ink looks very different in the IR to many CMY process colors, allowing further security features to be produced [13].

The availability of these devices further enhances the interest in UV and IR readable features. Once again, they enhance the need for materials that can form novel features revealed in the UV and IR.

### *Features utilizing optics and printing*

The features illustrated so far represent a steady increase in the technologies needed for verification. The combination of optics and printing can have the additional advantage of producing striking effects visible to the naked eye.

Retroreflectors can be used in one such system. These reflect incident light back toward the direction of the light source, regardless of the angle of incidence. They can be constructed from 90º corner cubes or from high refractive index spheres with a reflective backing [14]. Common examples of these are the reflective layers in road signs and high visibility clothing. However, this type of technology is also used in some identity documents and in combination with printing technologies. The resultant images shift with viewing angle, appearing to float above or sink below the surface as the viewing angle is changed, disappearing at large angles. Image visibility can be enhanced using a handheld collimated light source [15].

A further enhancement to this is the use of microlens arrays to provide a floating image [16]. This technology has the additional advantage of providing a tactile feature due to the topography of the microlenses.

This area provides an open field for new technologies. There are opportunities for new technologies for Non Impact Printing to write the image data, particularly as resolution and placement accuracy increase.

## Conclusion – the need for new technologies

There will always be the need for new technologies in the security printing of identity documents. Once a technology is introduced there will always be individuals and groups who will seek to copy or alter it for their own ends. As a result the legitimate designers and manufacturers of these documents require a steady stream of novel concepts to introduce into this area.

Technologies that can be validated by eye or with readily available instruments are particularly in demand. In addition covert or forensic technologies (outside the scope of this paper but very much of interest) are also required. In the future, these documents will undoubtedly incorporate printed electronics.

Border security and identity validation are essential to the workings of modern society. Printing and (increasingly) fabrication technologies have a key part to play in this.

## References

[1] T M Plutchak, “Defeating Fraud Through the Use of New Security Printing Features”, Proc. IS&T’s International Conference on Digital Production Printing and Industrial Applications, pp 110 – 111 (2005).

[2] D K Shaffer, J A Zlotnickm, “Forensic Analysis and Databasing of Toners and Inkjet Inks Used in the Production of Fraudulent Documents”, Proc. IS&T’s NIP24, pp777 – 780 (2008).
[3] S E Church, L W Pagano, “Not Your Father’s Counterfeiting”, Proc. IS&T’s International Conference on Digital Production Printing and Industrial Applications, pp 121 – 123 (2003).
[4] H Kipphan, “Handbook of Print Media”, Chapter 2.5.1 – Security Printing. ISBN 3-540-67326-1 (2001).
[5] 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).
[6] R Barcyk, L Buczynski, D Jasinska-Choromanska, D McCallum, “The Influence of Print technology on the Image Quality of Convex Braille Printouts for the Blind”, Proc. IS&T’s International Conference on Digital Production Printing and Industrial Applications, pp 65 – 66 (2005).
[7] N Limburg, “New Opportunities and Challenges with Fifth Color Units”, Proc. IS&T’s International Conference on Digital Production Printing and Industrial Applications, pp 53 – 54 (2005).
[8] S Muke, P Fox, W Jackson, “Improvements in Document Security – The Next Generation”, Proc. International Congress of Imaging Science, pp 424 – 427, (2006).
[9] R F Stevens, “Optical inspection of periodic structures using lens arrays and moiré magnification”, Imaging Science Journal Vol. 47, pp 173 – 179 (1999).
[10] J Reber, R Hofmann, M Pauchard, U Fuerholz, “Spectroscopic Investigation of IJ Layer Yellowing”, Proc. IS&T’s NIP23, pp711 – 715 (2007).
[11] F B Hazan, “Application of Thermal Printing Technology for Security Printing”, Proc. IS&T’s NIP23, pp558 – 560 (2007).
[12] J Stasiak, G Hinch, T Etheridge, T Strecker, S Simske, “Printing and Patterning of Quantum Dots Using Thermal Inkjet Techniques”, Proc. IS&T’s DF2008, pp247 – 250 (2008).
[13] V Žilak, K Pap, I Žilak, “CMYKIR security graphics separation in the infrared area”, Infrared Physics & Technology 52, 62-69 (2009).
[14] A V Arecchi, T Messadi, R J Koshel, “Field Guide to Illumination”, SPIE Press, ISBN 9780819467683 (2007).
[15] J M Florczak, R T Krasa, S P Maki, R M Osgood III, “Sheeting with composite image that floats”, US Patent 6,288,842 (2001).
[16] 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

## Author Biography

*Alan has 28 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 the next 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 and continues to be a regular conference speaker and tutor.*

*Alan has a BSc in colorant chemistry and a PhD in instrumentation, both from the Department of Chemistry at the University of Manchester. He is a Fellow of the Royal Photographic Society as an Accredited Senior Imaging Scientist. In addition to the IS&T Alan is active in the Royal Photographic Society and Institute of Physics as a speaker and session chair. He is currently IS&T Conference Vice President.*