Why Isn't Digital Printing Secure?

Glenn P. Wood, Reconnaissance International

Abstract

Digital printing is becoming very popular for the printing of personal data in government issued identification documents. This presentation will review the types of abuse that passports and other identification documents are prone to and explains why, until now, the lack of security in digital printing has had a direct impact on the way in which these documents are manufactured and issued.

The title of this paper is provocative, deliberately so because my hope is that if even one of its readers can offer a constructive suggestion for the improvement of digital print, it will have served a useful purpose. First some explanation of terms.

By 'Digital Print' we mean any printing technology using inks or toners and capable of producing printed materials directly from a computer file.

Digital printing eliminates the mechanical steps used in conventional printing and does not require an intermediary medium such as film, or an intermediary machine, such as a plate maker. In particular, we refer to the print technologies used to print the variable data on government issued identification documents such as passports, NIDs, driver's licenses etc. We are not including laser engraving in this discussion.

By 'Secure' we are referring to resistance to a number of threats which compromise the value and integrity of the print.

In general, there are six threats to the secure printing:

1. Counterfeit/Simulation - copies simulations of the print in an entirely new document
2. Theft of components copies made from stolen genuine materials and printed on a commercial printer.
3. Counterfeit from cannibalized docs - copies made from genuine pieces
4. Alteration of the print by changes to the personalization of genuine document.
5. Photo/sig substitution - replacement of photo and/or signature with another

By far the greatest threat comes from the use of commercial scanners which can record the data from a (stolen) genuine document, alter it then print it again in a fake document.

The problem is critical owing to the rapid growth in digital personalization. Although it was introduced in 1993, by 2001, only 80 million passports a year were issued of which only 25% contained digital print. Today, that figure has risen to 120 million per year and the number containing digital printing has risen to 75%. As recently as 1998, my own British passport contained a photograph of me printed on photographic paper and stuck onto the personal data page with glue. It was then covered with holographic laminate to prove it had not been tampered with. Today, my photograph in my new passport is digitally printed directly onto the paper passport page BUT IT IS STILL COVERED WITH A HOLOGRAPHIC OVERLAY.

The secure printing of personalized data today is a table supported on three legs. These are:

1. The print technology
2. The substrate onto which the print is written
3. The laminate which protects the print against tampering.

If any one of these three legs is removed or marginalised, the table becomes unstable and topples. The document is unfit for purpose.

Today, there are three types of digital personalization technology using inks, pigments or toners:

Electro-photographic (laser toner) 3%)
Dye/pigment transfer (21%)
inkjet (51% or world total)

The winner here is inkjet printing. There are more than 200 passport issuing authorities in the world and nearly half of them use inkjet printing technology.

It is true that giants like Xerox, Xiekon, Agfa and Kodak have introduced elements to increase the security of their digital print, either through software or the use of covert markers in toners, inks or pigments. None-the-less, the issuers of government IDs still feel the need to 'protect' the variable print with overlays which are usually optically variable.

An entire industry has grown up with the sole purpose of protecting this digitally printed data through the use of security overlays. Companies such as Fasver and Toppan cater for this need by offering heat activated laminates less than ten microns thick. Recognising that pressure sensitive laminates can often be removed by heat or cold, the adhesive of these polymeric membranes sinks into the paper thus sealing the print and protecting it from illegal alteration.

So severe has the problem become at many jurisdictions are favoring the use of subsurface laser engraving instead of inks, pigments or toners. In this case, the paper substrate must be replaced by expensive polycarbonate and the variable data burned into it with a laser. The process is slow, costly and the result largely monochrome (any color possible as long as it is black!).

This is a sad commentary on a printing industry which has had centuries to hone its skills in applying ink to paper. It is possible that part of the problem lies in the meagre nature of the print itself. A relatively small surface area is covered by the application of text. The eye only recognises that it is there or not and doesn't study the detail of the appearance of the letters.

However, a photographic image is another matter and it ought to be possible to print it in a way that conveys 'genuineness' to the unaided eye.

We were recently impressed by the efforts of the Dutch company Validus which developed a technology for the digital printing of optically variable inks using liquid crystal technology. The results were extremely impressive. We have seen full color images, including alphanumeric data, printed in this way. Unfortunately, the print world has not been enthusiastic to adopt this technology which may be due, in part, to the fact that the liquid crystals do not orientate and produce the correct colors when printed onto a paper substrate.

It seems ironic that the inkjet process is preferred because of speed, cost effectiveness and convenient but then to incur the cost and inconvenience of protecting it with a laminate. While not wishing to diminish the opportunities this creates for the security laminate industry and the great contribution made by transparent, holographic overlays, one feels it must just be a matter of time before a new digital printing idea renders the overlay unnecessary.

Glenn P. Wood B.Sc., M.Sc., D.Phil (Oxon)

Glenn Wood is an Associate of Reconnaissance International – consultants and publishers of market intelligence on authentication technologies and strategies for brand protection, security print and personal identification.

After obtaining a science doctorate at Oxford University in 1978, Dr Wood worked with Ilford Ltd on the development of holographic materials and then at OpSec Security Group as VP Business Development for security products. He has written and lectured widely on all aspects of counterfeiting and piracy and the technologies that can be used to combat these crimes.

He joined Reconnaissance in 2007 and is primarily responsible for technology awareness and legislative developments with particular reference to the Americas. He is an active contributor to three monthly business-to-business newsletters, Holography News, Authentication News and Tax Stamp News.