Towards a paperless society

Albeit with a growing number of printed documents

by Dr Fred Jordan

According to a study entitled 'How much information 2003'[1], which was conducted by the UC Berkeley School of Information, the volume of printed office documents increased by 43% between 1999 and 2002. A trend that does not appear to have abated[2], lending weight to the conclusion that printed information volumes have increased in line with computer use. This is particularly true of contracts, certificates and licenses, which are used in growing numbers and on a much broader scale than ever before. In turn, this places considerable emphasis on document security. This article looks into Variable Cryptoglyph®, a cost-effective means of preventing document tampering and counterfeiting.

Although solutions that make online transactions and the transfer of information more secure are regularly announced, the same cannot be said of solutions that improve the security of printed documents. A growing number of companies and organisations nevertheless face problems as a result of leaks, tampering, and counterfeiting, primarily on the part of insiders. The problem is exacerbated by the availability of high performance, low-cost office printers, scanners and image processing software.

Various requirements

A survey published by PricewaterhouseCoopers in 2005[3] reported that 45% of all businesses fall victims to crime involving forged or counterfeit legal and financial documents. As the (perceived) anonymity of employees that work for larger companies is greater, these companies are more at risk than smaller companies.

Document-related crime can take on any number of forms, including:

- leaking confidential documents;
- tampering with printed documents;
- counterfeiting printed documents.

In order to assess how printed office documents may be protected adequately, the following aspects must be taken into consideration:

- the visibility or invisibility of security features included in/on the document (if any);
- the document's resistance to photocopying or transmission by fax;
- the ability to eradicate or alter the security feature;
- the distinction between originals and copies;
- the ability to detect the security feature on a fragment of the document;
- the (useful) life of the security feature (for archived printed documents);
- the ability to integrate the existing document into the overall processing stream;
- the machine-readable verification process for industrial document processing, etc.

If all the above criteria are taken into consideration, it may be concluded that there is no single, universal document security process that meets all document security requirements. As is the case with banknotes, which include several distinct security features, a combination of techniques is called for.

Overview of security techniques

One way to sort the different security techniques is to distinguish between visible (overt) and invisible (covert) features. A visible or overt feature is easier to identify, and, in a sense, indicates that the document has been 'secured'. On the downside, visible features can also be identified - and subsequently reproduced - by potential criminals.

A covert (invisible) feature must first be identified. As the presence and location of such features may be disclosed by insiders, the document security process should be multifaceted. Needless to say, secrecy and confidentiality are key considerations. Well-known overt security features include two-dimensional bar codes, printed microstructures or additional elements such as holograms or kinegrams. The information contained in these data storage devices can also be encoded. However, their visibility does constitute a weakness.

The use of invisible (covert) techniques is growing all the time, largely as a result of the widespread availability of high-quality digital printers. According to a recent article in The Washington Post[4], some manufacturers of home and office printers have

Dr Fred Jordan *is co-founder of AlpVision and has been its CEO since June 2001. He has authored numerous publications, holds several patents and co-invented Cryptoglyph®, one of the core technologies used by AlpVision. Fred has worked in the United States and France. In 1999, he obtained his PhD from the Signal Processing Laboratory (LTS) at the Swiss Federal Institute of Technology (EPFL), based in Lausanne, Switzerland.*

developed products that add an invisible marking to each printed page, apparently without the user's knowledge. The purpose of hidden markings is to identify the printer, in the event that it is used to perpetrate fraud. Apart from the obvious political and legal implications, the article shows that modern technologies and equipment allow invisible information to be printed in normal ink, using standard equipment. Figure 1 shows how dots can be rendered invisible by changing their size and colour.

Other encoding techniques change the shape of the font in order to embed information, a practice known as 'text watermarking'. Here too, the nature of the document and the security specification may necessitate a dedicated security feature, or a combination of several security techniques.

There are also other techniques that require special security features such as DNA taggants or bespoke inks that react to light of a specific wavelength. The figure below shows some of these processes, ranked on the basis of cost effectiveness. The diagram not only takes account of the cost of (i) generating the security mark or (ii) buying and implementing the security feature, it also reflects the cost of detecting the feature.

Another important aspect of any security solution is that it should be machine readable. Banks, corporates and government bodies process millions of printed documents each day. This requires the detection process to be automated. In addition, the security process must dovetail with existing IT document processing systems.

Embedding encrypted information in invisible dots is currently the most cost effective means of achieving a high degree of security, albeit for very specific applications. Text watermarking also has considerable potential on account of its resistance to photocopying. A digital technology that combines the functionality5 listed below was recently developed and commercialised. The technology is capable of:

1. Printing invisible micro-points across the entire surface of a document. As the dots are both invisible and spread across the document surface, they cannot be replicated or erased.
2. The invisible micro-points can contain encrypted information that can only be deciphered using an encryption key (128 bit). If detection takes place in a unique and secure environment, the key is never compromised. It would be impossible for the information to be deciphered without the key.

Figure 3 shows how difficult it is to distinguish printed dots from natural imperfections in the paper.

The camouflage feature, whereby imperfections in the paper are used to 'conceal' the dots, is one of the unique aspects of this technology. The detection

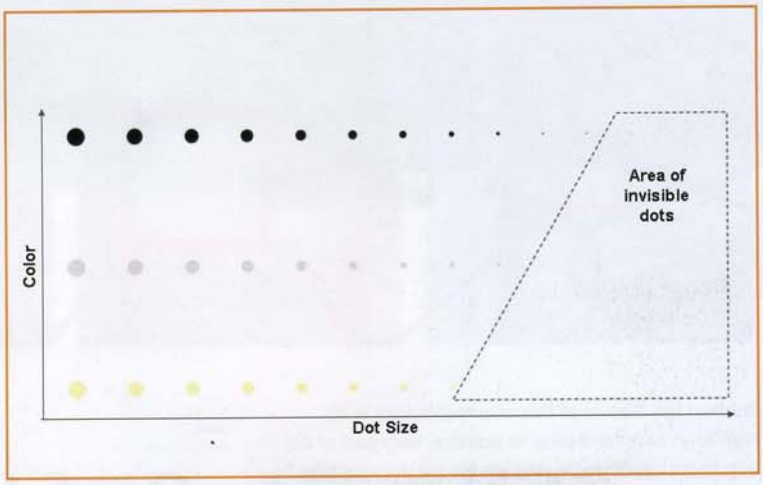
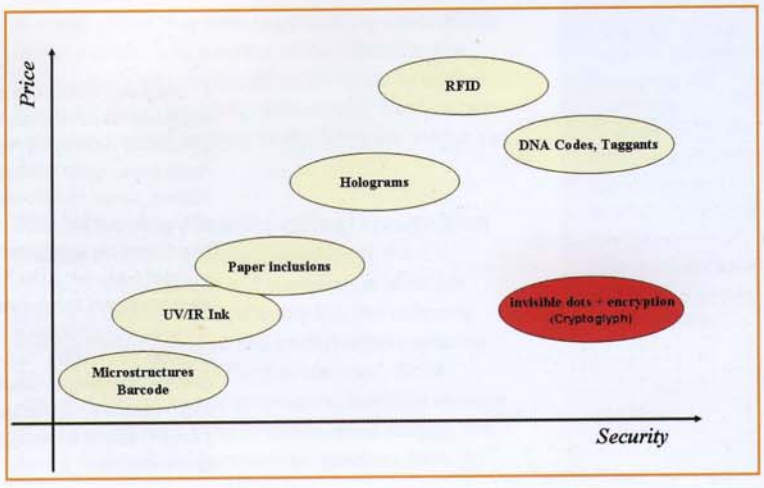


Figure 1
If and when dots become invisible depends on (i) the size and the colour of the dots and (ii) the colour of the printed background.

software processes data from an advanced signal detector (combining very low signal-to-noise ratios with built-in conceptual redundancies). The micro-points are integrated in the document before printing. They are also fully integrated with word processing packaged from any software manufacturer.

The micro-points are integrated in the electronic form of the document, via the office automation software. The electronic document can then be printed seamlessly either on offset or on digital printers (laser, inkjet). The micro-points invisible marking can also be fully integrated with word processing packages, such as MS Office Word or other brands. An additional icon will then appear in the software menu bar; clicking on it will allow to securing individual document at individual level. While very small and invisible to the naked eye, the dots can be used to distinguish between the original document and a copy. The ability to encrypt critical text fragments in the invisible dots provides additional anti-tampering protection. If the document needs to be resistant to photocopying, the micro-points can be rendered visible (larger), thus creating a light grey background (figure 4).

Figure 2
Covert and overt technologies ranked on the basis of price/ performance.



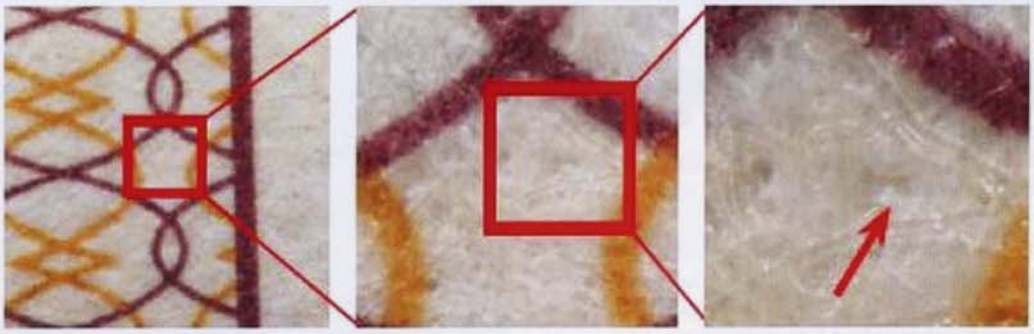


Figure 3
Invisible dots printed at 1200 dpi (offset) using regular visible ink.

Another key feature of this new technology is its high level of redundancy. In practice, only part of the document needs to be present for the document to be authenticated. In other words, torn or partly destroyed documents can also be detected, even years after the document was printed. This feature can help to detect internal leaks, for example (assuming the encrypted information contained details of the original recipient's name).

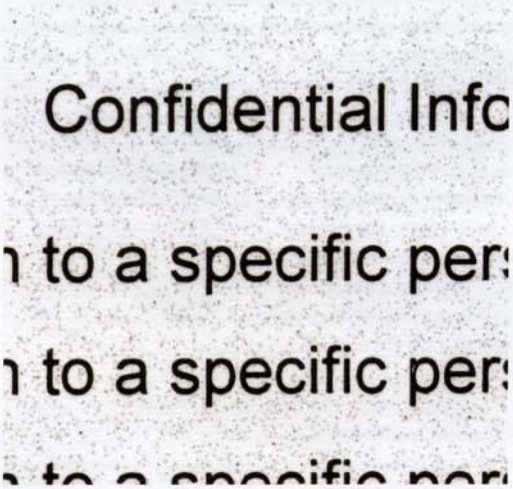


Figure 4
Visible micro points spread across the entire surface of a black & white document containing encrypted anti-photocopying data.

Conclusions

There is no single, universal solution to secure a printed document. Instead, a combination of covert and overt techniques is required. The solution adopted must reflect prevailing user requirements and system specifications, and take account of the balance between security and costs.

As indicated, the scope of the cost analysis should cover the cost of printing as well as the cost of detection and authentication. Or, to be more specific, the cost of integrating the solution into (i) existing IT processes and (ii) specific hardware/software detection systems. Where large number of documents are processed, a machine readable feature is essential.

1 ' How much information 2003?' - http://www.sims.berkeley.edu:8000/research/projects/how-much-info-2003/
2 'A Society Addicted to Paper - The Effect of Computer Use on Paper Consumption', Geoffrey Peters, School of Computing Science, Simon Fraser University, Vancouver, B.C., Canada V5A 1S6, gpeters at sfu dot ca, March 12, 2003. http://www.sfu.ca/~gpeters/essays/paper.htm
3 Global Economic Crime Survey 2005, PriceWaterhouseCoopers www.pwcglobal.com/extweb/insights.nsf/docid/D1A0A606149F2806852570C0006716C0
4 Online Washington Post - http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg
5 Covert security technology - http://www.alpvision.com/cgoverview.html