Covert and Overt Protection for Valuable Documents

By Fred Jordan

There is no obvious trend of reduced paper consumption due to computer use. On the contrary, it seems that the volume of printed documents increases with computer use.

According to the UC Berkeley study "How Much Information" (2003), the amount of new information printed as office documents increased about 43 percent between 1999 and 2002[1]. As individuals continue to produce original information – the vast majority of it in office documents – the amount of information printed on paper increases[2]. This is evidence that there is no obvious trend of reduced paper consumption due to computer use. On the contrary, it seems that the volume of printed documents increases with computer use. Documents such as contracts, certificates and licenses of all kinds are multiplying all over the world.

Toward a paperless society: with more printed documents!

Technology screening shows that every day new solutions appear for securing online transactions and electronic document transfers, but very few reports are made public about securing printed documents. Leaks, tampering issues and counterfeiting are multiplying inside companies and other organizations, mainly due to insider misbehavior. This is explained by the relatively easy access to high-performance, low-cost office printers, scanners and image-processing software, which are all continually in development.

Various requirements

A survey published by PricewaterhouseCoopers in 2005 reported that 45 percent of companies worldwide are victims of criminal acts such as breaches of confidentiality and tampering with or counterfeiting legal or financial documents[3]. The bigger the company, the higher the risk of internal fraud. Employees of large companies feel more anonymous than employees of smaller companies.

Criminal acts related to documents take many forms, such as:

- Leaking confidential documents
- Tampering with printed documents
- Counterfeiting printed documents

How can printed documents in offices be adequately protected? For an answer, the following aspects should be taken into account:

- Visibility or non-visibility of security features
- Resistance to photocopying or fax transmission
- Resistance to eradication or alteration of security features
- Distinguishing a true original from a copied version
- Detecting the security element on a fragment of the document
- Duration of the security element for archived printed documents
- Easy integration into the existing document-processing stream
- Machine-readable verification processes for industrial document processing

There clearly is no single, universal document security process. There is also a need for continuous development to counter new forms of fraud. A combination of various techniques is necessary to meet all the security needs combined on a single document – as, for example, with banknotes that contain many security elements.

[1] Lyman, Peter and Hal R. Varian, "How Much Information," 2003. http://www.sims.berkeley.edu/how-much-info-2003

[2] Peters, Geoffrey, "A Society Addicted to Paper: The Effect of Computer Use on Paper Consumption." School of Computing Science, Simon Fraser University, Vancouver, BC, Canada. March 12, 2003. http://www.sfu.ca/~gpeters/essays/paper.htm

[3] PricewaterhouseCoopers Global Economic Crime Survey 2005. http://www.pwcglobal.com/extweb/insights.nsf/docid/D1A0A606149F2806852570C0006716C0

Security techniques for printed documents

One way to sort through the techniques in document security is to distinguish between the visible (overt) ones and the invisible (covert) ones. A visible or overt technique is in some way easily identifiable and, in a sense, labels the document as "secured." By definition, however, a visible security feature is also identifiable to criminals who may then develop a passable, fraudulent replication of the visible element.

A covert or invisible technique must first be identified in order to be subverted. Employee indiscretion could provide such information to criminals. Therefore, a document security process is always a chain of elements where secrecy and confidentiality are key.

Well-known visible techniques include two-dimensional bar codes, printed microstructures, and additional elements such as holograms or kinegrams. The information contained in such graphical data-storage elements can also be encrypted. Their major weakness, however, is the visibility that enables their simple eradication.

Non-visible or covert techniques are exploding nowadays due to the ubiquity of high-quality office digital printers. It was revealed recently that manufacturers of home and office printers produced printing equipment that added invisible marks on each printed page without the knowledge of users of the printers[4]. This hidden marking was done in order to identify a printer that has been used in fraudulent printing. Aside from the obvious political and legal implications, this incident shows that with today's technologies and equipment, it is possible to print invisible information with normal ink and standard printing machines. That the code used to encrypt the identifying information was cracked shows that the battle between frauds and counter-techniques is a never-ending process.

The figure below shows how dots can be invisible depending on their size and color.

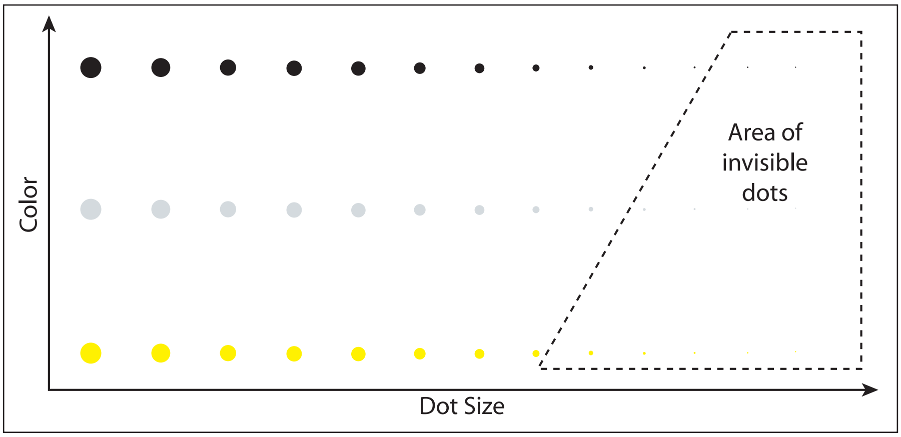


Figure 1. The area of invisible dots depends on the dots' size and color and the printed background.

Other text-alteration methods invisibly alter the form of the letters (font) in order to encode information. In the security jargon these techniques are known as "text watermarking." Here again, the nature of the document and the security specification may lead to a dedicated security feature or a combination of security techniques. There are other techniques that require special security features, such as DNA taggants and special inks that react to specific light wavelengths.

The figure below shows some of these processes ranked by cost-effectiveness. It takes into account not only the cost of generating the security mark or buying and implementing the security feature, but also of detecting the security element.

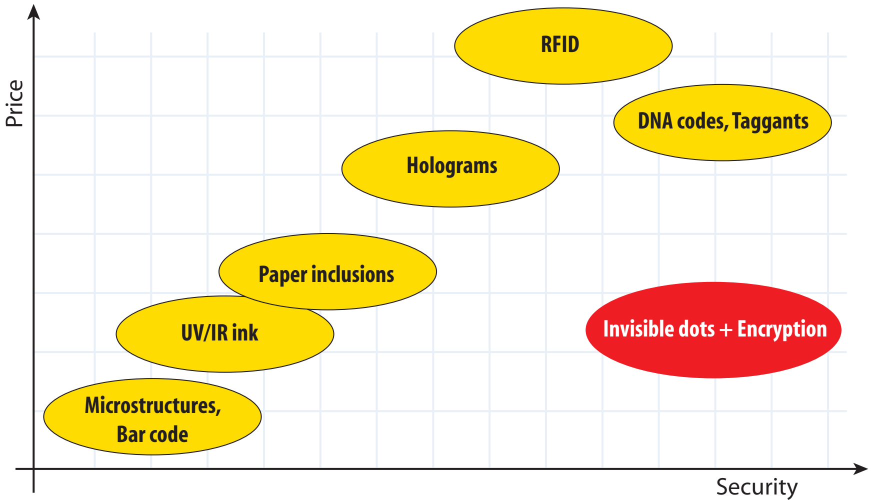


Figure 2. Covert and overt technologies ranked by price/performance ratio

Another important element in a security solution is that it should be machine-readable. Banks, large companies and government administrations process millions of printed documents. The security-generation process must be automated and also integrate smoothly into existing IT document-processing systems.

Encrypting information using invisible dots is currently the most cost-effective way to achieve a high degree of security, though for very specific applications. Text watermarking is also very promising because it resists photocopying.

One recently developed digital technology combines two elements:

1. Printing of invisible micro-points over the entire surface of the document. As these dots are invisible and spread over the surface of the document, it is impossible to replicate or erase them.
2. The micro-points contain encrypted information that can only be decrypted with a 128-bit key. If detection is performed in a unique and secured place, the key is never endangered. Fraudulent decrypting of the information is simply impossible[5].

[4] "Sleuths Crack Tracking Code Discovered in Color Printers." October 19, 2005. http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg

[5] http://www.alpvision.com/cgoverview.html

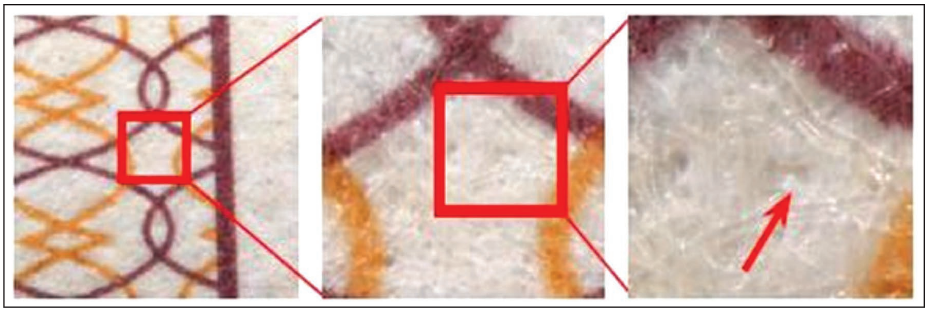


Figure 3. Magnified images with invisible 1200-dpi offset dots printed with regular visible ink.

The image above shows how difficult it is to distinguish printed dots from natural imperfections of the paper.

The camouflage feature, using the imperfections of the printed material, is one of the unique aspects of this technology. The detection software is based on advanced signal-detection capabilities that have very low signal-to-noise ratios and built-in conceptual redundancies.

These micro-points are integrated into the document before printing and fully integrated with word-processing software or pre-press tools. Though very small and invisible to the naked eye, they will still authenticate the original document against a fraudulent copy. Further, the dots enable tamper-evident detection because critical printed text can also be redundantly encrypted into them.

If the secured document must be photocopy-resistant, the micro-points will be made visible (bigger) and will generate a light gray background.

Another key feature is the high level of redundancy of the security element (visible or invisible dots), so that just a part of the document is enough for detection, in case it is torn or partly destroyed. This is even possible many years after the document was printed. This feature can detect internal leaks, for example if the encrypted information contained in the micro-points were to contain the original recipient's name.

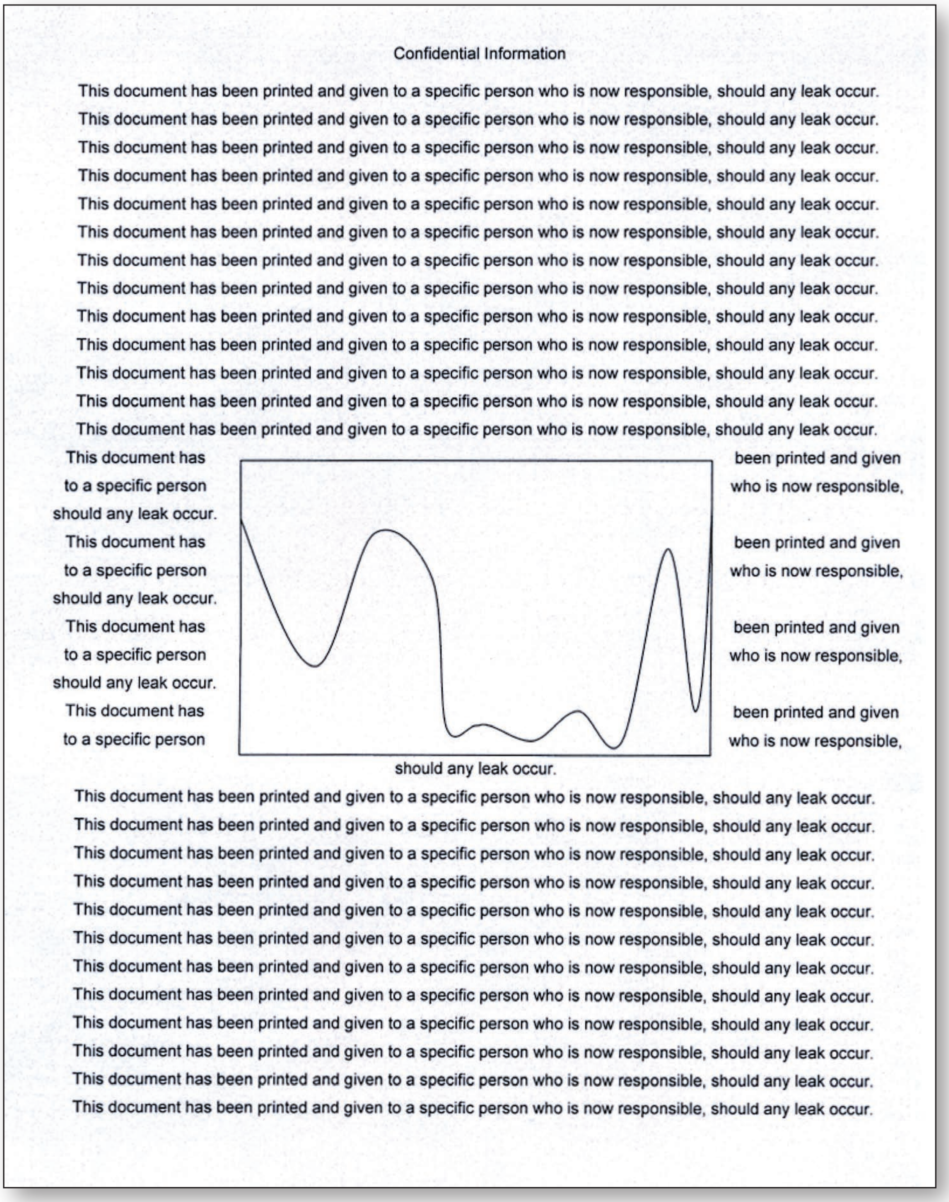
Conclusions

There is no single, universal solution to secure a printed document. A combination of covert and overt techniques is required. Any solution will have to be adapted to specifications and various needs, and take into consideration the needed level of protection measured against the cost.

Cost must take into account the generation of the secured printed document in addition to the cost of detection and authentication. This includes in particular the cost of integrating the solution into existing IT processes, as well as specific hardware/software detection systems and their deployment. Further, a machine-readable feature is required when large batches of documents have to be processed.

About the Author

Dr. Fred Jordan is co-founder of AlpVision and has served as CEO since June 2001. He is the author of numerous scientific publications in the digital watermarking domain. He is the co-inventor of Cryptoglyph®, the core technology currently being used by AlpVision.



Confidential Information

This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.

This document has been printed and given
to a specific person who is now responsible,
should any leak occur.
This document has been printed and given
to a specific person who is now responsible,
should any leak occur.
This document has been printed and given
to a specific person who is now responsible,
should any leak occur.
This document has been printed and given
to a specific person who is now responsible,
should any leak occur.

This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.
This document has been printed and given to a specific person who is now responsible, should any leak occur.

Figure 4. Word-processing printout from a 1200-dpi black-and-white laser printer. Photocopy-resistant information ciphered in visible gray dots