PAPER, FILM & FOIL CONVERTER®
PFFC

Brand Protection with Micro-Dots

Dr. Martin Kutter, AlpVision Corp.

Jan 1, 2007 4:24 PM

Web Exclusive

Protecting products against counterfeiting or identifying fraudulent import is a major concern of the supply chain. It is certain to be a constant and sustained battle.

Now brand owners have a new weapon based on digital imaging, supported by continuous development in consumer electronics and global access to efficient, secured data communications networks and services.

Today almost every branded product is targeted by counterfeiters. The multiplication of supply sources in this global economy is a key factor in the multiplication of counterfeiting attacks, including domains with a well-established and regulated supply chain, such as pharmaceutical products[1].

The Intl. Chamber of Commerce[2] recently launched a Web-based information service reporting daily counterfeiting infringements. It shows evidence this criminal business is increasing and concerns all kind of goods, including food and alcohol, cigarettes, automotive parts, and obviously luxury goods such as perfumes and cosmetics.

Differentiating Authentic Products
Among specialists it is commonly agreed that anti-counterfeiting processes can be sorted into two main categories:

- The visible or overt processes.
- The invisible to the naked eye or covert processes.

Various companies have added visible security features, such as holograms, embossing, special ink, and two-dimensional bar codes, onto their packaging. However, these visible elements feature not only very low security but also require training for effective authentication. It is interesting to note that various Asian companies offer hologram duplication services at very low prices.

More sophisticated techniques can be found in the field of covert security elements, that is, features not visible to the naked eye and requiring dedicated detection means. The most popular solution is invisible ink, such as ultraviolet (UV) ink (visible under UV light) or infrared (IR) ink (visible under IR light). To authenticate these inks, a lamp emitting light in the required wavelength range is sufficient. The drawback of these inks is that they can be bought very easily on the market by anyone. There are other chemical tracers or ink additives providing counterfeiting security, such as DNA or magnetic tracers.

The problem with such special inks or ink additives is the related logistics and manufacturing procedures, such as press cleaning, temperature and pressure sensitivity, as well as interaction with other chemicals. Although very efficient and effective, their implementation and deployment are quite costly. Authentication on the fly, in the retail space for example, is also difficult. These techniques can be qualified as “analogue or hardware based” because they require additional elements or special substances, and they subsequently have to be managed by the manufacturer in a secured environment.

The Digital Breakthrough
As in other industries, the digital revolution opens exciting new possibilities. Digital technologies now can be used to fight counterfeiting and to track and trace products. These digital technologies are breakthroughs compared to former “analog or hardware” ones. Instead of being issued by optical, chemical, or biology experts, they are developed by computer software and digital imaging scientists.

A recent paper published in the *Washington Post* Online[3] mentioned that some manufacturers of home and office printers delivered printing equipment in such a way that it added invisible marks on each printed page. This of course happened without informing the users. The purpose of this hidden marking is to identify the printer when used in fraudulent printing matters. Aside from the political or 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.

This paper shows also that the secret code used to cipher the printer identification has been cracked. This means it is necessary to develop new techniques continuously to cope with the continuous development of the computing power, which is used by both defrauders and anti-counterfeiters.

Translated into the packaging/converting industry and security printing domains, the incident described above has two important implications. First, an industrial package printer could produce secured packaging for manufacturers using standard printing machines and standard ink. Second, a product manufacturer can secure its products without informing the printer that the packaging contains an invisible security feature. This will reduce the number of parties involved in a product security process and make a real advantage because secrecy and privacy are the two pillars of an efficient security policy.

Figure 1: Area of invisible dots depending on the size and the color of the dots as well as the printed background.

Depending on the application, the printing process, the carton color, and the ink color, the dots vary in size from about 20–80 µm. It is important to note that the security is also a function of the dot color and the dot size. Security levels increase as lower contrasts are used and as the dots get smaller.

As these techniques do not require special features or equipment, they are extremely efficient in term of implementation cost and security management.

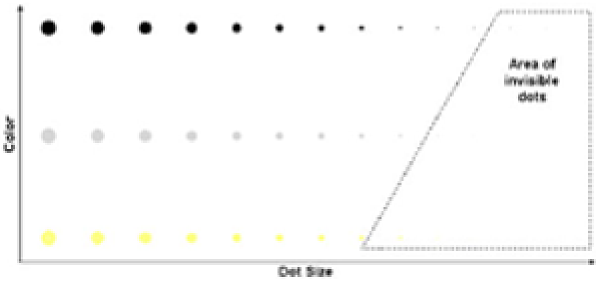

Figure 1.

Figure 2: Performance comparison between various security techniques,

Track & Trace Functionality
Today a big noise is made around Radio Frequency Identification (RFID). The addition of an electronic chip with an antenna for communication and external or internal power supply is considered a promising hope to protect and track and trace products in the future.

However, RFID also has significant disadvantages. The main disadvantage is that it costs too much. A target price of approximately seven cents, depending on complexity and functionality, is foreseen for 2007. The adaptation of the packaging production chain to add the tag on the packaging and to program and manage the information to write in the chips has to be considered as well.

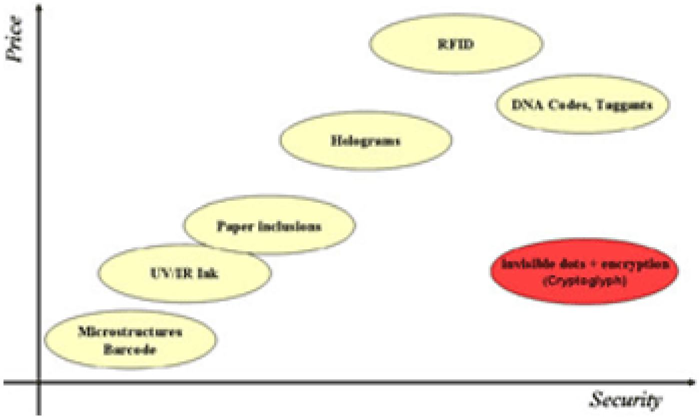

Figure 2.

Undoubtedly RFID will occupy an important position in track and trace applications as well as in counterfeit protection. However, the technology still needs to evolve as well as adapt to the various logistics and manufacturing processes. And the price of RFID first must go down. Until then, proven security printing technologies currently being used for the protection of printed media, such as banknotes, or even electronic business, such as online banking services, will provide the most efficient and cost effective means to solve the problems of brand protection.

Data Encryption and Single Authentication Detection Location
A basic idea to safely authenticate and track and trace a product is to make this product as unique as a fingerprint. But because of the criminal threat, the location to perform an authentication test must be in a secured area, controlled either by the manufacturer or by a fully trusted authority. To render the counterfeiting much more difficult and almost impossible, it is a clear advantage if the marking process is invisible and contains encrypted information. The advantage of a covert element is that counterfeiters must know there is a security element before they can attack it. If the feature is visible, the point of attack is evident.

It is also important to note that if a security element requires a specific, dedicated detection system, then this is a clear security threat since it facilitates counterfeiting due to reverse engineering methods.

Recently a technology has been developed and commercialized under the name of Cryptoglyph[4] (Crypto = encryption, glyph = marks), which combines two elements:

1. Printing of invisible micro-points over the entire surface of the primary or secondary packaging, such as the blister foil for foods and pharmaceuticals. As these dots are invisible and spread on the whole surface of the packaging, it is impossible to replicate or to erase these dots.
2. These invisible micro-points contain encrypted information, which can only be deciphered by using the encryption key. If the detection process is performed in a unique and secured place, the key is never endangered. Deciphering the information by a fraudulent party is impossible.

These micro-points are integrated in the package design before printing and are invisible to the naked eye. They are very difficult to distinguish—even with a magnifying glass—as the dots are confused with the imperfections found in all printed material structures and thus effectively camouflaged.

This 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.

Figure 3: Invisible Cryptoglyph micro-dots camouflaged in the carton imperfections.

The Cryptoglyph detection process can be performed using a standard flatbed scanner or even by using a camera phone. To avoid having the encryption key made available in the field, a digital image of the packaging is sent to a processing system located in a secured area, via mobile data transmission networks. Once analyzed in this safe and secured area, the result is sent back to the field controller via SMS or another modern communications means. This two-way communication process ensures the full security of the encryption system and allows instant consolidation of the field track and trace verification tests.

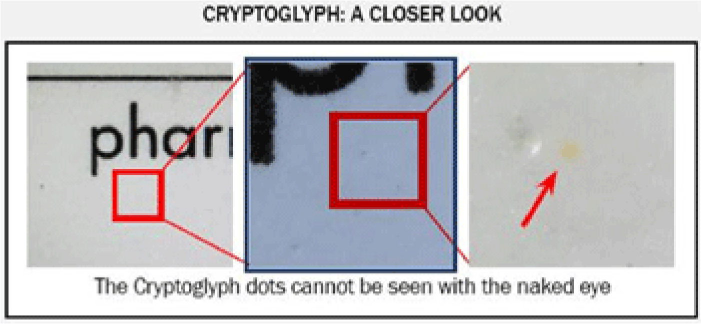
CRYPTOGLYPH: A CLOSER LOOK
phar
The Cryptoglyph dots cannot be seen with the naked eye

Figure 3.

Figure 4: Detection of the invisible Cryptoglyph marking with a camera phone or a standard flatbed scanner sent to a secured server via mobile networks or Internet connection.

For now, Cryptoglyph is the only technology in the world providing an invisible marking with visible ink on standard presses (offset, flexography, rotogravure, digital printing, etc.). This technology requires no change in the packaging graphic layout. It is easily integrated into any current industrial package printing process, without any modification.

Today millions of products are protected without the consumer's knowledge. The increase in interest in the production of counterfeits or in re-importing discounted branded products is a real challenge for the brand manufacturers, which must invest in new security techniques to enable field testing and rapid and effective reaction against unfair distributors and counterfeiters.

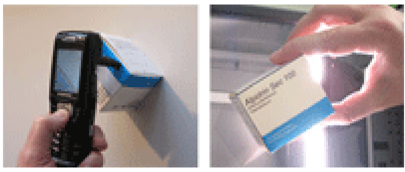

Figure 4.

[1] World Health Organization, Fact Sheet No. 275, revised February 2006: Counterfeit medicines, (**who.int/mediacentre/factsheets/fs275/en/index.html**

[2] Business Action to Stop Counterfeiting and Piracy–BASCAP, **bascap.com/incidents_via_country.asp**

[3] Washington Post Online, **washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg**

[4] Cryptoglyph technology, **alpvision.ch/cgoverview.html**

SUPPLIER INFO:
AlpVision—alpvision.ch

Dr. Martin Kutter, co-founder and current president of AlpVision SA, Vevey, Switzerland, earned his scientific Ph.D. degree at the Swiss Federal Inst. of Technology, Lausanne (EPFL), Switzerland. Earlier he earned a Master's degree from the Univ. of Rhode Island. In 2000, Dr. Kutter received the best Ph.D. dissertation award from the Swiss Technology Inst. for his contribution in Digital Watermarking domain. Since 1996 Dr. Kutter has published more than 25 publications on digital image processing, copyright protection, and data security, and has filed numerous patents. He can be reached at +41 (0) 21 948 6464.

Paper, Film & Foil CONVERTER is a monthly magazine in which recognized experts and experienced staff assist converters around the world to become more efficient and profitable in their manufacturing and business practices through newsworthy information on technology; marketing and management trends; and products and services.

- **Renew** your subscription
- **Subscribe** to the magazine
- **Sign up** for email newsletters

Want to use this article? Click here for options!

Find this article at:
http://www.pffc-online.com/mag/brand-protection-with-micro-dots/index.html

□ Check the box to include the list of links referenced in the article.