

# pharmind

## die pharmazeutische industrie

### ■ Co-Verblisterung

Alternative zur Verbesserung  
von Compliance und  
Arzneimittelsicherheit

### ■ On-going- Stabilitätsprüfungen

Praxisnahe Umsetzung der  
Vorgaben des EU-GMP-Leitfadens  
vom 1. Juni 2006

### ■ Wirkstoffproduktion

FDA-gerechte Anlagenqualifizierung

### ■ Qualitätskontrolle

Überprüfung der mikrobiologischen  
Qualität von nicht-sterilen Produkten  
gemäß international harmonisierten  
Vorschriften



online  
[www.ecv.de](http://www.ecv.de)

∞  
2006

# Protecting Pharmaceutical Products from Counterfeiting Using Digital Imaging Technologies

Dr. Martin Kutter

AlpVision Corporation, Vevey (Switzerland)

## Summary

Protecting pharmaceutical products against counterfeiting or identifying fraudulent import of donated or discounted drugs is now a major concern of the supply chain. This article describes the use of new technologies based on digital imaging supported by the continuous developments in consumer electronics, such as low cost flatbed scanners or mobile phones equipped with digital cameras and a convergence with glob-

al access to efficient, secured data communications networks and services.

## Zusammenfassung

Pharmazeutische Produkte gegen Fälschungen zu schützen sowie betrügerische Importe von gespendeten oder unter dem Marktpreis abgegebene Medikamente zu verhindern, ist mittlerweile zu einem entscheidenden Aspekt in der Produktions- und Vertriebslogistik von Pharmaunternehmen

geworden. Der nachfolgende Beitrag beschreibt neue Technologien, die auf digitaler Signal- und Bildverarbeitung basieren und einsetzbar sind für den globalen Markenschutz. Dank enormer Fortschritte in der Verbraucherelektronik, wie zum Beispiel bei Flachbettscannern und in der Mobiltelefonie, ist es möglich, kosteneffiziente Lösungen für den Produktschutz zu realisieren, die nur geringen Einfluß auf die Produktionsprozesse haben und dennoch hohe Sicherheit bieten.

## Are pharmaceutical products really targeted by counterfeiters?

Nowadays there are still a lot of pharmaceutical manufacturers and supply chain professionals who believe that drug counterfeiting is not an issue because of the very well established and controlled supply chain (manufacturer, distributors and pharmacies).

However, within its report published in 2004, the US Food and Drug Administration reported a significant rise in the number and level of sophistication, of counterfeiting operations pushing fake products into the US market<sup>1)</sup>.

A paper published in the Times Online<sup>2)</sup> (July 2005) reported that a reputable UK pharmaceutical manufacturer made a large quantity of

low-cost anti-retroviral HIV drugs available to several African countries. However, these same drugs valued at £ 18 million and desperately needed by Africans, were illicitly returned to Europe. They were then sold in new packaging at a much higher conventional price to European customers. One of the customers turned out to be the UK National Health Service.

This incident suggests that counterfeiting and fraudulent re-import of donated or discounted pharmaceutical products, delivered for example in developing countries, or after important human disasters, is only marginally due to individual criminals or corrupt civil servants. To a much larger extent such fraudulent business is due to the activities of a well organized international crime industry with sophisticated

manufacturing facilities and parallel distributions channels.

## How to differentiate authentic and authorized products from fake ones or illegally imported?

Among anti-counterfeiting specialists it is commonly admitted that it is technically very difficult to authenticate the pharmaceutical products. They also agree that it is not the responsibility of the final consumer to authenticate the product. It is the duty of the manufacturer, the pharmacists, or the legal au-

<sup>1)</sup> [http://www.fda.gov/oc/initiatives/counterfeit/report02\\_04.html](http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html)

<sup>2)</sup> <http://www.timesonline.co.uk/article/0,,8122-1684914,00.html>

thorities to ensure that only authentic products reach the consumer. For example, various pharmaceutical 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 a 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 interesting prices.

A well-known story tells of a reputable international pharmaceutical company selling high demand medicines in Russia. The product was on the market in two versions, the original and a counterfeit. Due to the fact that the counterfeit featured a hologram and the original did not, the counterfeited version sold much better than the non-counterfeited version. As a consequence the pharmaceutical company was forced to add a hologram to copy the fake product which means they were effectively counterfeiting counterfeits.

More sophisticated techniques can be found in the field of covered 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 UV ink (visible under ultra violet light) or IR ink (visible under infrared 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. They 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 "analog" because they require additional elements or special substances and they subsequently have to be managed by the manufacturer in a secured environment.

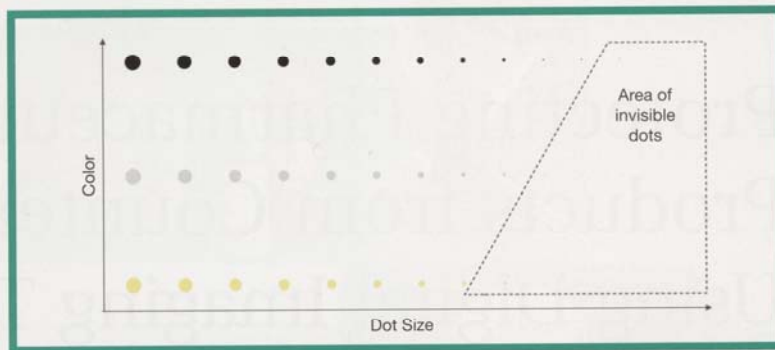


Fig. 1: Area of invisible dots depending on the size and the color of the dots as well as the printed background.

### The digital image processing breakthrough

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

The more promising new solutions are based on the same digital imaging technologies and cryptography used to protect bank notes and to secure online banking services.

A recent paper published in the Washington Post<sup>3)</sup> (October 2005) 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.

Translated into the packaging industry and security printing domain the incident described above has two important implications. First, an industrial packaging 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.

To illustrate the process of producing invisible patterns with visible ink, Fig. 1 shows the visibility of printed dots as a function of the dot size and the color used. Considering as well the nature of the paper, which always contains imperfections such as wood particles or other substances, the very small printed dots are not visible to the naked eye. And they are not identifiable with magnifying equipment because they are hidden in the imperfections of the paper.

Depending on the application, the printing process, the carton color and the ink color, the dots vary in size from about 10  $\mu\text{m}$  to 80  $\mu\text{m}$ . 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.

The two images of Fig. 2, which show a Cryptoglyph technology marking (with printed dots) and a regular printing (without printed dots), as described further, make the two images not distinguishable, even with a magnifier. The detection of the information contained in this invisible marking is based on sophisticated mathematical and statistical analysis, which is not based on the identification of the individual printed dots, but on advanced signal detection processes".

<sup>3)</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2005/10/18/AR2005101801663.html?referrer=emailarticlepg>

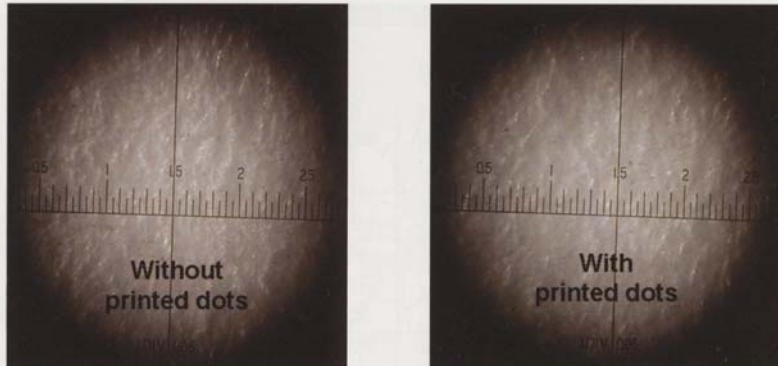


Fig. 2: Magnified images with / without invisible printed dots for a 1200 dpi black and white laser printer on white paper (one division = 0.05 mm).

When comparing “analog” processes using additional security elements or visible printed codes with the “digital” ones using invisible printed dots, we see the very big difference in cost/efficiency ratios. This also takes into account the cost of the detection process (Fig. 3).

### Track & Trace functionality

As mentioned above, simply authenticating a product is not always enough and does not necessarily represent the largest economic threat. Parallel, gray, or even black markets are as important, and under certain circumstances even not illegal. To detect such practices, the manufacturers must implement a solution which goes far beyond the simple YES or NO answer from an authentication process. In the event of unsolicited or fraudulent re-import, brand owners need to know at any point in time where a given pharmaceutical product is or should be. This functionality is often referred to as “track and trace” and ideally covers the entire life cycle of a given product.

A new solution to tackle this problem is based on electronics tagging or RFID (Radio Frequency Identification). 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 near future.

However, RFID also has significant disadvantages. The main disadvantage is that it costs too much. A target price of approximately 5 € 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.

Recently an officer from a leading global pharmaceutical manufacturer declared during a value chain conference that the bottom line with RFID is that programming errors, misread of tags, human errors and the interference of criminal counterfeiters, diverters and thieves, can or will cause great confusion.

Undoubtedly RFID will occupy a very 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, manufacturing processes. And the price of RFID must first 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 pharmaceutical brand protection and enforcement.

### 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 finger print. But because of the criminal threat, the location where to perform an authentication test must be located 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 covered 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.

### Cryptoglyph technology

A technology has been recently developed and commercialized by AlpVision SA, a Swiss supplier of di-

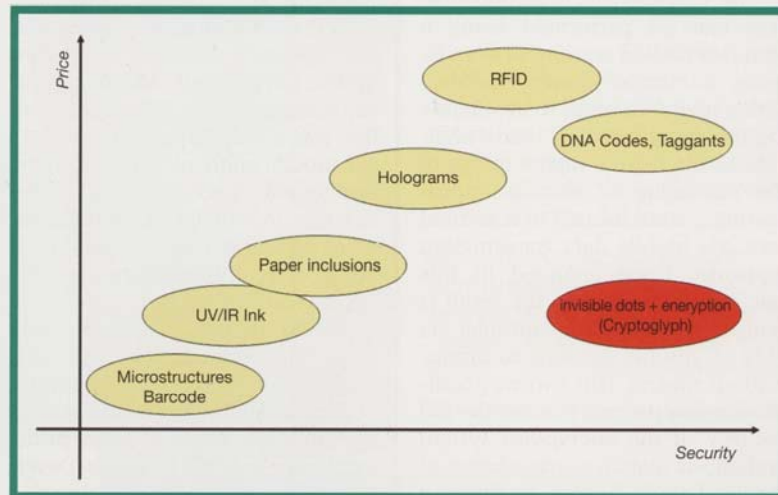


Fig. 3: Performance comparison between various security techniques.

gital security printing solutions, under the name of Cryptoglyph (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. 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 AlpVision technology. The detection software is based on advanced signal detection capabilities that have very low signal-to-noise ratios and built-in conceptual redundancies. The AlpVision technology surpasses other technologies, such as the 2D DataMatrix code bar because, by definition, the code bar requires contrasts in visible black-and-white.

The Cryptoglyph detection process can be performed using a standard flatbed scanner or even by using a mobile phone equipped with a digital camera. 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 & trace verification tests (Fig. 4).

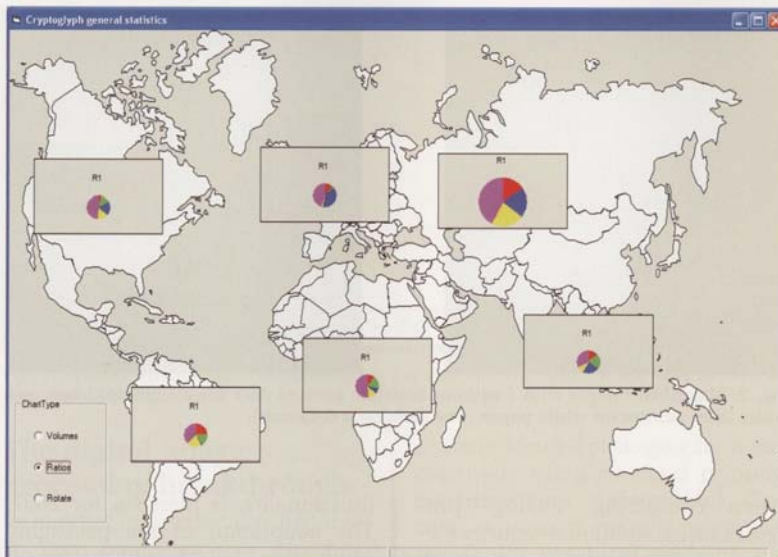


Fig. 4: Instant consolidation chart of Authentication and Track & Trace field test, showing the source of unsolicited import of products.

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

Industrial printers active in pharmaceutical packaging production have already added Cryptoglyph to their security processes.

Constantia Flexible Packaging, a leading producer of blister foils for international pharmaceutical companies, implemented the Cryptoglyph technology in their standard rotogravure printing line to produce protected blister foils. The R&D Project Manager reported that the rapid and seamless integration of the Cryptoglyph technology in the standard blister foils production line was a very important factor, as no modification of the packaging design was necessary. He added that the invisibility of Cryptoglyph is a dramatic improvement enabling easy authentication of the pharmaceutical products.

Rondo AG in Allschwil (Switzerland) another important industrial packaging printer for the pharmaceutical industry, integrated Cryptoglyph in their offset industrial printing lines. Rondo's Business Development Manager reported that due to the invisibility and the overall

distribution of the Cryptoglyph marks, it is impossible to remove the security element without visually degrading or destroying the packaging. This is not the case with conventional visible security elements.

Today millions of products are protected without the consumer's knowledge. The increase in interest in the production of counterfeit drugs or in re-importing discounted drugs, because less risky and more lucrative compared to other criminal activities, by well organized criminal industry is a real challenge for the pharmaceutical industry. Manufacturers and legal authorities will have to cooperate and define penalty processes. Manufacturers must invest in new security techniques to enable field testing and rapid and effective reaction against unfair distributors and counterfeiters.

#### Correspondence:

Dr. Martin Kutter,  
AlpVision SA,  
rue du Clos 12,  
1800 Vevey (Switzerland),  
Fax +41 (0)21 948 6465,  
e-mail: info@alpvision.com  
www.alpvision.com