Industry-suitable Technologies to Protect Pharma Products against Counterfeiting

As clearly stated in the new European directive 2011/62/EU[1] relating to medicinal products for human use, as regards the prevention of the entry into legal supply chain of falsified medicinal products, patient safety will be achieved with the combination of three components:

- verify the authenticity of the medicinal product,
- identify individual packs or batches
- verify whether the outer packaging has been tampered with.

These new measures, which improve the protection of public health, will be adopted by member states on January 2, 2013.

Because implementing labelling, tracking and tracing systems for products will likely result in additional costs to the pharmaceutical industry, this paper hopes to shed light on several cost-effective product authentication processes and features, which can be easily deployed and implemented within manufacturing plants and laboratories worldwide.

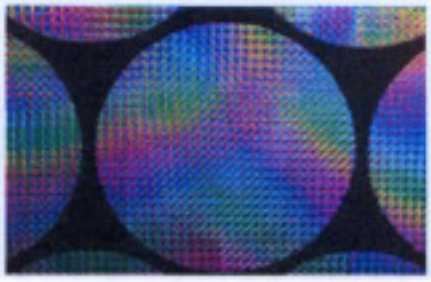
Authentication and Identification

Several organisations have reported that individual product coding can be used to identify counterfeits. However, more and more experts agree that visible product codes, batch numbers and expiry dates cannot be used reliably for product authentication because they can be copied by counterfeiters[2]. Banknotes, for example, have been serialised for decades and are still widely counterfeited. Of course, the cost invested to secure a banknote is far greater than that of medicines. However, we believe that some lessons learned in the field of high security documents can contribute to finding solutions to counterfeit pharmaceutical products.

Visible (Overt) or Invisible to the Naked Eye (Covert) Security Features

Traditionally, pharmaceutica lcompanies have added visible security features to their packaging to prevent counterfeiting. These include, for example, holograms, kinegrams, embossing, micro printing, moiré or special ink such as optical variable ink. However, these visible features only provide minimum security and require training for effective authentication Fig 1. By the same token, if a company

Figure 1 Overt security features examples (hologram)



suddenly decides to discontinue the use of visible security features, consumers might mistake a genuine product for a fake.

Today, counterfeiters have the best printing equipment and components at their disposal in order to perfectly replicate the visual aspects of a packaging, including its visible authentication features. By contrast, the use of "covert" features – security features that are invisible to the naked eye – provides a higher level of security. For example, "good" counterfeit banknotes always include a replication of the visible security features, but rarely of the invisible ones. To prevent leaks, however, covert security features should never be disclosed. These features should only be shared with a limited number of trustworthy persons of the branded manufacturing company, an approach that restricts consumer access

Anti-counterfeiting literature also suggests that a specialised scanner or a distinctive analysis is required in order to identify covert security features, making the "genuine-or-fake" verification a costly and time-consuming process. However, as in other industries, the digital or software revolution has opened up new and exciting possibilities. For example, the Cryptoglyph® on-packaging[3] (e.g. folding boxes, blister packs, labels) achieves invisible protection by using normal visible ink or varnish. Fig 2 Digital security features simply

Figure 2 Covert security (Alpidrin box)

require an off-the-shelf office flatbed scanner or an iPhone 4 smartphone device to perform a "genuine-or-fake" verification. In this case, the covert feature scanner can be purchased on the consumer electronics market anywhere, while proprietary hardware is the rule when security substances, taggant or dedicated invisible optical effect are used.

Replacing security consumables with software has also had a significant impact on the cost of implementing an anti-counterfeiting programme for multi-brand companies using multiple production plants. For example, when using security consumables, it is necessary to provide the various production plants with the right quantity of security features in relation to the number of packaging

elements to produce, plus extras for the overs. If poorly managed, this procedure can encourage theft during transportation and misuse of the overs to produce counterfeits. The use of security components can also affect the packaging printing equipment if special ink is used or if extra features such as hologram or taggant should be inserted in the production run. By contrast, digital security features using normal ink will not alter the printing process or production speed; this is an important cost-saving benefit.

Human Sensory Perception-based or Machine-based "Genuine-or-Fake" Verification

When selecting a security feature, it is not only important to assess the cost of purchase, implementation, global deployment and management, and resistance to replication, but also how a "genuine-or-fake" verification is performed.

In this case, the various anti-counterfeiting features can be placed in two main categories:

- features which use human sensory perception;
- features which are machine-readable.

When using human sensory perception-based verification (visual, tactile, oral), a person will be required to undergo adequate training to be able to distinguish a genuine security feature from a fake replication, when displayed side-by-side. By contrast, when using machine-based verification, a person will only be required to follow a step-by-step process. If properly described, the latter can be performed by anyone without any specific knowledge or training.

Some methods combine a human visual decision with a device, such as the Raman Spectroscopy analyser, which is capable of analysing the chemical components of a tablet and comparing them with the analysis result of the genuine production stored in the device. Such a device may cost dozens of thousands of dollars and require some training to properly manipulate. In addition, only a few analysers are generally available within a given company at a given time, forcing the manufacturer to send the suspected tablets to a dedicated lab.

As mentioned earlier, other visual features include the form factor packaging, that is its facial appearance, display surface, size and shape, and other printing details that counterfeiters may not have identified. A discrepancy between a genuine pack and a counterfeit can therefore also be identified with the help of a detailed description, stored in and provided by an online database. But this data can only uncover counterfeits until attempts are made to remedy these discrepancies.

So, an important question arises as to the cost of performing a machine-readable "genuine-or-fake" verification. Because some existing digital authentication processes use off-the-shelf office scanners or iPhone-like devices to verify the authenticity of the packaging components (folding box, blister pack or label) and because these supplies are often part of an office setting Fig 3, performing a machine-based verification using digital authentication processes results in virtually no added costs to the branded manufacturing company.

Figure 3 Medicine container authentication via iPhone 4

Local vs. Remote Verification Process

In order to perform a machine-based "genuine-or-fake" verification, there are two distinct methods: a local process using the appropriate hardware, or a remote identification using an online server. Local verification could be seen as advantageous as it does not require any data connection. However, in the case of covert security features, using a local verification process requires that the equipment be rid of sensitive information, which, if stolen, could fall into the hands of counterfeiters. By the same token, if the pharmaceutical manufacturing company needs to carry out verifications at multiple locations, it will need to have the appropriate equipment, provide training, and perform maintenance and calibration onsite. These added costs should not be neglected, especially when taking into account employee turnover, and equipment upgrades and refills.

Because internet and mobile connections are widely available around the world today, a security feature enabling remote "genuine-or-fake" verifications via a central secure server is a major advantage. A remote verification process not only eliminates the need to share sensitive information with the operator, but also enables consolidation of all the verifications performed worldwide, thus facilitating the detection of any correlation between various fraudulent sources within the supply chain. As for all criminal acts, the quicker you uncover them the more you are well positioned to identify the criminal source to stop it.

Security Level and Protection against Leaks

A recent FDA report[1] shows that organised crime is active in counterfeit medicine, as this industry represents a very lucrative and less risky criminal business compared to others. The use of corruption and coercion is therefore seemingly prevalent to obtain security features or programmes. An important question then arises as to the number of people and companies that should be involved in the security chain. In the case of consumable security elements, suppliers are involved in the security chain on a recurring basis, exposing the recipient company to theft or misuse of the overs necessary to produce the secure packaging. Consequently, the less suppliers are involved in critical security elements, the less leaks.

Web-based Secure Server Solutions

There are two fundamental ways web servers can be used. The first approach consists of using the server as a data repository system. This method is used to detect the different anti-counterfeiting features used in a given packaging or production batch. For example, the IPM system – Interface Public-Members of the World Customs Organisation – is a secure communication tool for the exchange of information between right holders and customs administrations. By using the IPM system, field customs officers have access to the 'genuine/fake' database to check imported goods for counterfeits.

The second approach uses the secure server to analyse different parameters of a packaging in order to automatically assess its authenticity[2] using a digital image captured with a regular office scanner, a digital camera or even a smartphone device.

In this case, the secure server is also capable of managing the deployment of anti-counterfeiting features. Because these features are digital elements, there is no need to involve additional security suppliers in the security chain. The branded pharmaceutical manufacturing company has in turn full control over the generation of digital security elements, and can allocate individual profile and password authorisations online to automate "genuine-or-fake" verifications worldwide.

This second approach appears to be the best protection against leaks, especially if very few high-level employees are authorised to access critical security elements, such as an encryption key or security patterns. The security elements are then digitally routed via encrypted and secured data networks to local markets and their related production plants.

Of course, costs related to software licenses and software customisation for the deployment of the application within an existing information technology environment, as well as royalties, have to be taken into consideration. However, if the web-based system is well conceived, access to a free internet browser should be all that is necessary to use it. This approach also frees very large organisations from having to perform complex computer validation processes while updating local PCs with new pieces of software and, in turn, from disrupting the production of medicines.

Could Smartphones be used to Uncover Fake Medicine?

Smartphones, such as iPhone-like devices, are continuously evolving with increased functionalities and computing power, as well as image and video capabilities. Smartphones can therefore benefit the development and expansion of digital authentication features based on invisible marking, allowing mobility and "on-the-fly" genuine-or-fake verification. However, these advancements do not mean that mobile verifications should be placed in the hands of patients because of many unanswered questions related to the legal responsibility of a genuine-or-fake verdict.

Given these uncertainties, we believe that mobile product authentication should stay in the hands of professionals in the pharmaceutical industry, and undergo further research before being extended to the patient level.

In summary

Covert (invisible to the naked eye) security features provide higher security compared to overt (visible) ones.

Digital solutions based on software are easier to deploy compared to security consumable-based solutions.

Machine-readable security features are less expensive and more reliable for authenticating genuine-or-fake items compared to human sensory-based features, as no specific knowledge is required, only a step-by-step process that, if well described, can be performed by anyone.

Remote online verification using a web application does not require specific software at the verification side, only a free internet browser. Moreover, this approach will reduce the risk of leaks, especially if very few people are involved in managing the sensitive security data elements.

Digital solutions for product authentication based on software are less costly compared to security consumable-based solutions, especially when considering large production volumes.

Medicinecounterfeiting is flourishing. In fact, trade in counterfeit medicines appears to be growing faster than the market for legitimate drugs[3]. Factors like global business exchanges, e-commerce, aging population and growing medicine consumption are all naturally leading counterfeiters to enter the pharmaceutical market. This growing tendency can at least be partially counteracted with technological progress. Indeed, increased computing power and the ease with which people can use handheld devices to access networks and exchange data will lead to developing effective web-based authentication solutions and fighting back.

1. *Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011*
2. *International Pharmaceutical Industry, August 2011, volume 3 issue 3, "Should we Leave it to Patients to Identify Counterfeit medicines?"*
3. *Cryptoglyph digital security solution, http://www.alpvision.com/cryptoglyph-covert-marking.htm/*
4. *FDA Conducts Preliminary Review of Agency's Diversion and Counterfeit Criminal Case Information September 2011.*
5. *Krypsos Web Application, http://www.alpvision.com/krypsos-online-authentication.htm/*
6. *United Nations Office on Drugs and Crime, http://www.unodc.org/documents/data-and-analysis/tocta/8.Counterfeit_products.pdf, June 2010.*

Dr. Fred Jordan – CEO of AlpVision SA

Dr. Jordan is co-founder of AlpVision and has served as CEO since June 2001. He is the author of numerous publications and patents and co-inventor of Cryptoglyph and Fingerprint, the core technologies currently being used by AlpVision. Dr. Jordan has work experience in the USA and France. In 1999 he obtained his PhD title from the "Ecole Polytechnique Fédérale de Lausanne (EPFL)" Signal Processing Institute (ITS).

Email: fred.jordan@alpvision.com