Industry-Suitable Technologies for Protection of Pharma Products against Counterfeiting

With the new European directive 2011/62/EU[1] concerning prevention of the entry of falsified medicinal products into the legal supply chain, it appears clear that patient safety will be achieved with the combination of three components:

- Verification of the authenticity of the medicinal product,
- Identification of individual packs,
- Verification of the outer packaging to uncover any tampering.

This series of measures to increase patient safety shall come into force by January 2013 in the member states.

There are several estimations as to how much these measures will cost the pharmaceutical industry to comply with this directive. This paper concentrates on the authentication features and the way they can be implemented within the manufacturing plants of the pharmaceutical laboratories.

Authentication and Identification

Some papers and conferences have reported that identification of individual packs can be used to show up counterfeiting. More and more experts, however, have doubts, because a serial number which is visible can be copied by counterfeiters[2]. Banknotes have been an example of serialised items for decades but are still heavily counterfeited. Even if the packaging or dose of a medicine will never be comparable to a banknote from the cost of authentication features point of view, there is some banknote expertise that can be used in authentication of medicine.

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

Many pharmaceutical companies have added visible security features to their packaging to prevent counterfeiting (Fig. 1). These include, for example, holograms, kinegrams, embossing, micro-printing, moiré or special ink such as optical variable ink. However, these visible features provide not only minimal security; they also require training for effective authentication. A side-effect is that if a visible security feature is introduced, it is difficult to later abandon it because consumers may consider the genuine production to be a fake, through not seeing the overt security feature anymore.

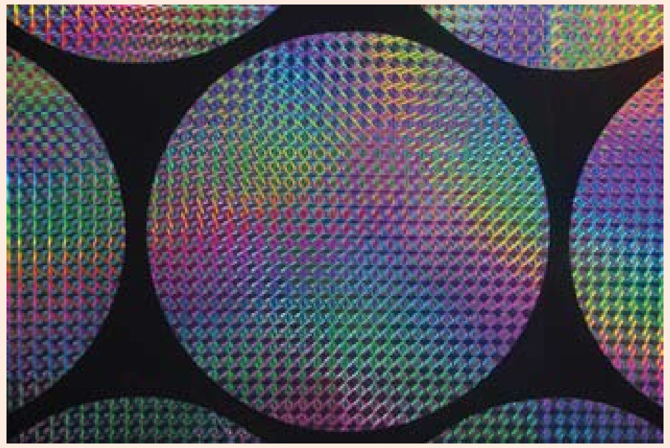


Figure 1: overt security features: examples of holographic marking

Counterfeiters today have availability of the best printing equipment and components to replicate perfectly the visible aspect of a packaging, including visible authentication features. The use of "covert" features - invisible to the naked eye – will produce a higher level of protection, due to the inability of counterfeiters to identify the presence of such features. In the case of "good" banknote counterfeits, they always show a replication of the visible security features, but not the invisible ones which are difficult to counterfeit. Covert security should never be disclosed; to prevent leaks it should only be known to a limited number of trustworthy persons.

It is generally admitted in anti-counterfeiting literature that covert features need a dedicated scanner or analysis process to show up the presence of these features, making a "genuine-or-fake" verification a quite expensive and time-consuming process. However, as in other industries, the digital or software revolution opens up exciting new possibilities, such as, for example, the Cryptoglyph® on-packaging[3] (folding boxes, blister packs, labels) invisible protection achieved with application of normal visible ink or varnish (Fig. 2). This security feature only requires a simple off-the-shelf office flatbed scanner 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, taggants or dedicated invisible optical effects are used.

Replacing security consumables with software also has considerable impact on the cost of implementing an anti-counterfeiting programme worldwide for multiple brands and production plants. For example, when using security consumables it is necessary to dispatch these features to the various production plants in proportion to the quantity of packaging elements to be produced, plus an extra percentage for overproduction. This requires careful management of the shipment of these security features in order to prevent theft during transportation and misuse of the overproduction, which otherwise could be used for production of counterfeits containing genuine security elements. 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 are included in the production run. On the contrary, digital security features using normal ink will not alter any printing processes or their production speed; this is an important cost-saving factor.

Figure 2: covert security: example Cryptoglyph® invisible marking on the entire surface of a packaging including in the blank areas

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

On selection of a security feature, it is not enough to just evaluate the purchase cost, the robustness against fraudulent replication, the cost of implementation in the production process, the cost of global management or any impact on the production process. An important part of the evaluation is 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.

If human sensory perception is used (visual, tactile, oral), adequate training is required for a person to be able to distinguish a genuine security feature from a fake replication when both are in hand. Meanwhile, in the case of a machine-readable feature, only a step-by-step process is required. When well documented, it can be performed by anyone without any specific knowledge or training.

There are some solutions which combine a human visual decision and a device such as the Raman spectroscopy analyser capable of analysing the chemical components of a tablet and comparing it with the results of analysis of genuine production stored in the device. Such an analyser may cost thousands of Euros, and specific knowledge will be required for its correct operation. Generally only a few analysers are available in the company, requiring shipment of the suspected tablets to a specialised laboratory.

Other visual inspection may be directed to details of the packaging related to its shape or details in the printing that counterfeiters may not have identified. It follows that a discrepancy between a genuine pack and a counterfeit, identified with the help of a detailed description, which might be provided by an online database, can lead to discovery of counterfeits until the counterfeiters find the remedy for such discrepancies.

However, an important question is the cost related to the whole process carried out to perform the machine-readable "genuine-or-fake" verification. Again here the Cryptoglyph® on-packaging digital solution requires only off-the-shelf office scanners to take a picture of part of the packaging component (folding box, blister pack or label). This device could already be in place for other purposes; if not, its purchase would cost about 100 US dollars on the open consumer electronics market anywhere in the world (Fig. 3).

Local or Remote Verification Processes

In order to carry out a "genuine-or-fake" verification, we have to consider either a local process with everything available locally, or remote identification via an online server. Local verification could be seen as a plus through not requiring any data connection. However, for covert security it is important to ensure that the equipment in hand does not contain sensitive security elements which could fall into the hands of counterfeiters who have been able to acquire or steal such equipment. If the pharmaceutical products manufacturer needs to carry out verification in multiple locations, it will have a need for a corresponding number of pieces of equipment as well as provision of training, maintenance and calibration on site. This cost should not be neglected, taking into account the turnover of employees and possible updates or renewal of the equipment.

Figure 3: Genuine-or-Fake" verification using a simple office scanner

Internet and mobile connections are today widely available around the world, developing countries included. A security feature enabling "genuine-or-fake" verifications to be carried out remotely via a central secured server results in an almost instant verdict. This constitutes a major benefit, eliminating the need for sensitive security elements to be in the hands of an operator. Another major benefit of remote verification is the 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 and to stop it.

Security Level and Protection against Leaks

A recent report[4] shows that organised crime is active in counterfeit medicine, as this represents a very lucrative and a less risky criminal business compared to others. One can therefore estimate that corruption and coercion could be used to benefit from leaks related to security elements or programmes. An important criterion is to see how many people and companies are necessary to be involved in the security chain. It is easy to understand that the fewer people involved in critical security elements and the lower the number of suppliers, the better the possibility of limiting leaks. When consumable security elements are used, the suppliers of these elements are part of the security chain on a recurrent basis. Delivery of these elements will also expose the recipient company to theft or misuse of the overproduction necessary in the manufacture of the security packaging, as mentioned earlier in this paper.

Web-based Secured Server Solutions

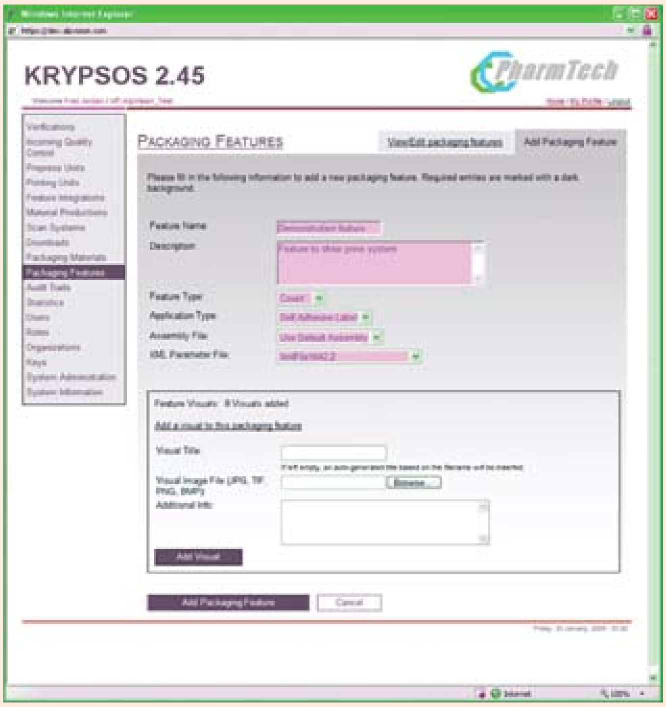
There are two fundamental ways in which web servers can be used. The first approach consists of using the server as a data repository system in order to know what different anti-counterfeiting features are deployed for a given packaging or production batch. For example, the IPM system (Interface Public-Members of the World Customs Organization system) contains such information delivered and maintained by the branded product manufacturers. This information is available for use by customs officers to detect counterfeits at customs clearance of imported goods.

The second approach uses the secured server to analyse different parameters of a packaging in order to assess its authenticity automatically. For instance the AlpVision Krypsos5 server is able to process a picture of a packaging component (folding box, blister pack, label, flip-off top, part of a vial, etc.) and detect if it is authentic (Fig. 4).

If the secured server is able to also manage the anti-counterfeiting features deployment, and if these features are digital elements, there is no additional security supplier involved in the security chain. The branded pharmaceutical products manufacturer has full control over the generation of the digital security elements and can allocate individual authorisation via password and profile for online automated "genuine-or-fake" verification worldwide.

Such a centralised secured server could be the best solution for protection against leaks, especially if very few high-level employees are entitled to access critical security elements such as encryption key or generation of security patterns. The digital security elements are then digitally routed via encrypted and secured data networks to local markets and the corresponding production plants.

Figure 4: Web application (example Krypsos) snapshot showing the various functionalities available depending on the password and the profile of each authorised user



Please fill in the following information to add a new packaging feature. Required entries are marked with a dark background.

Feature Name: Demonstration feature
Description: Feature to show [illegible] system
Feature Type: Covert
Application Type: Self Adhesive Label
Assembly File: Use Default Assembly
XML Parameter File: [illegible]

Feature Visuals: 8 Visuals added
Add a visual to this packaging feature
Visual Title:
If left empty, an auto-generated title based on the filename will be inserted
Visual Image File (JPG, TIF, PNG, BMP):
Additional Info:

The cost of such a solution is related to software licenses and software customisation for the deployment of the application within an existing Information technology environment. Royalties for use of the digital security feature have also to be considered. If the web-based system is well conceived, no software beyond a free internet browser should be necessary at the user level. This also avoids a complex computer validation process in place in every large organisation when new pieces of software are to be implemented on each local PC, and affecting medicinal products.

In Résumé

Covert (invisible to the naked eye) security is providing higher security compared to overt (visible) security. Digital solutions based on software are easier to deploy compared to solutions based on security consumables. Machine-readable security features are more reliable for authentication of genuine or fake items compared to human sensory-based features; because no specific knowledge is required beyond the capability to follow a step-by-step process that, if well described, could be performed by anyone. Remote online verification using an internet web application needs only a free internet browser at the user level; it does not require specific coding at the verification side. It will limit 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 large production volumes are considered.

References

1 *Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 (54 –o)*

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, www.alpvision.com/cryptoglyph-covert-marking.html*

4 *FDA Conducts Preliminary Review of Agency's Diversion and Counterfeit Criminal Case Information September 2011.*

5 *Krypsos Web Application, www.alpvision.com/krypsos-online-authentication.html*

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**