Reprinted from PHARMACEUTICAL ENGINEERING
The Official Magazine of ISPE
May/June 2012, Vol. 32 No. 3
www.PharmaceuticalEngineering.org

Identifying Counterfeit Medicines with Industry-Suitable Technologies

by Dr. Fred Jordan and Dr. Martin Kutter

This article presents the latest pharmaceutical anti-counterfeit technology developments and describes different criteria which will help readers select those that best safeguard patient safety and the integrity of valuable pharmaceutical brands and products.

Introduction

This article investigates the latest security technologies available to branded pharmaceutical manufacturing companies to verify the authenticity of medicines. The authors argue that while serialization in pharmaceutical and medical device packaging may be appropriate to identify or recall medicines with manufacturing or distribution problems, it cannot prevent the introduction of falsified medicine into the legal supply chain. By contrast, the authors contend that, in order to increase reliability in the supply chain, digital authentication technologies that incorporate covert (invisible) security features provide a higher level of security than those with overt (visible) features; are easier and more cost-effective to deploy than those based on consumables; do not require any specific training, only a step-by-step process; and are more reliable than human sensory perception-based verifications. The article finally forecasts that while the newly adopted European directive 2011/62/EU calls on pharmaceutical companies and any actors involved in the manufacturing or distribution of medicinal products to verify the authenticity of medicines,[1] innovations in smartphone technology, including better image capabilities and increased computing power, will accelerate the need to develop a suitable, easy-to-use, and reliable product authentication process at the patient level.

When looking at the product security market, there are more than 100 security technologies (holograms, digital watermarks, DNA taggants, serialization, etc.) used to combat counterfeiting of primary or secondary packaging and of solid or flexible components, such as liquids, powders, and tablets. For a branded pharmaceutical manufacturing company, however, it is challenging to understand the scope and role of each of these technologies, especially when considering the cost of the technology feature itself and its nationwide or worldwide deployment. This article presents the latest pharmaceutical anti-counterfeit technology developments and describes different criteria which will help readers select those that best safeguard public safety and the integrity of valuable pharmaceutical brands and products.

Answering a Basic Question: Should We Leave it to Patients to Identify Counterfeit Medicines?

This question is a very topical issue both in developing and in industrialized countries, because consumer goods, including medicines – notably those not reimbursed by health insurance companies and those issued without a prescription, e.g., Over The Counter (OTC), are increasingly purchased via the internet. However, a study carried out by the European Alliance for Access to Safe Medicines found that 62% of medicines ordered on the internet were substandard or counterfeit. Of these, 68% were unlicensed imitations and the rest were counterfeit branded medicines.[2]

The question therefore arises as to the patient's responsibility in determining the authenticity of medicines. Today, a number of track and trace applications (e.g., serialization, bar codes, RFID Tagging, etc.) are used in the pharmaceutical industry to prevent falsified medicinal products from entering the legal supply chain. According to the World Health Organization, "These involve assigning a unique identity to each stock unit during manufacture, which then remains with it through the supply chain until its consumption."[3] Using any cell phone, a patient can identify and send the unique serial number printed on secondary packaging via SMS text message to a central database. The serial number is then automatically confronted with a free or already used position. The diagnostic

will be "authentic" if the number was never sent before or possibly "fake" if already checked. If the outcome is "fake," the secondary packaging is either a counterfeit or a second use of the original packaging, filled with highly probable fake medicine.

With this technology, the patient is given full responsibility for verifying the authenticity or not of the medicine. The success of this procedure must first rely on access to and utilization of mobile authentication devices, which could be problematic for elderly patients, people with motor restrictions, or who are visually impaired, and patients affected by socio-cultural and economic inequalities, for example. It is then based on the impossibility of transferring the verification process to a pseudo-server in the hands of counterfeiters. In other words, Man-In-The-Middle (MITM) attacks. Finally, it depends on the reliability and accuracy of the written code sent by the patient via text message, provided that patients systematically check the serial number position. If not, genuine positions remain unchecked and vulnerable to counterfeiting. Given these risks, patients should not bear the responsibility for uncovering fake medicine.

What is the Drug Manufacturer's Role in Verifying the Authenticity of Medicinal Products?

The next question arises as to the drug manufacturer's liability in the event of a "false positive." A false positive occurs when a counterfeit medicine is authenticated as genuine by the verification process, an outcome that might in turn affect a patient's health. It is quite easy to imagine how such a false positive could be generated with this serial number verification: a batch of genuine medicine is hijacked somewhere in the supply chain and while the genuine tablets are removed and sold in bulk, the genuine packaging is filled with fake medicine. Or imagine the following scenario: leaks, corrupt or coerced players in the supply chain create fake replications of medicine. In these cases, fake medicine will be authenticated as genuine and inadvertently reach the patient.

Claims that tracing the secondary packaging of medicine all along the supply chain – in other words, creating its e-pedigree – would prevent counterfeited medicine from entering the legitimate supply chain, are once again highly unrealistic. No major European pharmaceutical industry player today would vote for such a complex tracking and tracing solution, because it would require "…major packaging line changes and investments"[4] and true interoperability between medicine manufacturers, wholesalers, and prescription deliverers. Although creating an e-pedigree does provide valuable data on the history of a particular batch of drugs, it does not prevent fraudulent players in the supply chain from substituting genuine products with fakes and patients from purchasing them in turn.

One possible solution to combating counterfeit medicines lies in the newly adopted European directive 2011/62/EU, relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products. This directive clearly states that, for the purposes of patient safety, the "manufacturing authorization holder" shall:

- verify the authenticity of the medicinal product
- identify individual packs
- verify whether the outer packaging has been tampered with[5]

To this end, the European Parliament and the Council are calling for new measures, including the introduction of safety features on individual packs (these features will be decided at a later stage by the Commission, via delegated acts) and stricter rules on inspections and controls of all actors involved in the manufacturing and supply of medicinal products, among others. Per the Directive, focusing on authentication features rather than identification means could be the right industry-affordable answer to detecting counterfeit medicines, without having to rely on the hypothetical interoperability of non-compatible automated processes and ways of producing medicine by the various pharmaceutical industry players.

Identification and Authentication: Two Problems that Require Adapted Solutions

The original goal of batch or individual serialization was a means to identify and recall medicines with manufacturing or distribution problems. Although integral to patient safety, trying to change the primary purpose of serialization into an authentication process is problematic. Logistically speaking, this technology forces pharmaceutical companies to print a visible linear bar code on the packaging or label, which can sometimes be difficult given the variable size of the printable area and the code/substrate contrast. In addition, inspections and controls must be in place to ensure that a unique code is applied on each individual pack or label. Moreover, serialization requires adaptive hardware, software, and skills.

In the case of authentication, there are many security features available to brand owners and manufacturers capable of detecting counterfeits, not only with primary and secondary packaging, but also with dosage forms. The most efficient features are covert or invisible to the naked eye. According to the World Health Organization, "The purpose of a covert feature is to enable the brand owner to identify a counterfeited product. The general public will not be aware of its presence nor have the means to verify it."[6] These secret or covert procedures are widely available today and include invisible printing, embedded images, and digital watermarks, to name a few. These methods can help detect counterfeits by means of regular sample controls carried out at different points in the supply chain, even in the case of consumed or recovered packaging waste.

Some methods combine a human visual inspection with a device, such as the Raman Spectroscopy analyzer, which is capable of analyzing raw materials in medicinal and finished products, then comparing them with the analysis result of the correct chemical combination stored in the device. However, this device may cost dozens of thousands of dollars and require some training to properly manipulate. In addition, only a few

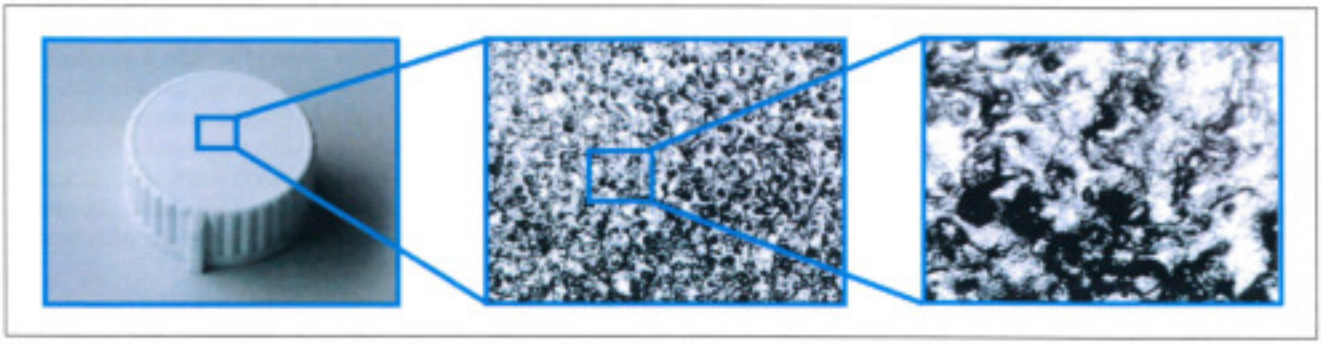

Figure 1. Details of a molded closure of a medicine jar showing microscopic differences, irregularities generated by the die cavity used to produce the part.

analyzers are generally available within a given company at a given time, forcing the manufacturer to send the suspected product to a dedicated lab.

Other more cost-effective, yet reliable technologies involve embedding an invisible marking on primary and secondary packaging using regular visible ink and standard printing processes, without having to change the packaging design or flow of production.[7] Another option involves using the intrinsic micro-differences present in a cavity mold[8] commonly used to create vials or medicine containers, capturing an image of the random pattern, and then storing it in a database - *Figure 1*.[9] In either case, the brand owner or manufacturer simply scans the item using a flatbed office scanner or an iPhone4 smartphone to receive a "genuine-or-fake" outcome.

As a consequence, while serialization may be appropriate to identify basic fraudulent actions, such as extension of the expiration date or market diversion, it is not suitable to determine the authenticity of a medicine. As we can see, checking a batch of drugs not equipped with reliable authentication features could prove costly, sometimes requiring a chemical analysis of the substance in question. Using industry-suitable invisible authentication security technologies instead can therefore help increase the number of controls at a very low cost and prevent the introduction of falsified medicine into the legal supply chain.

Can a Visual Inspection of Packaging by the Human Eye Help Identify a Well-Made Counterfeit?

Nothing looks more like a real medicine than a "well-made" counterfeit, which is sometimes virtually indistinguishable from the original.

This fact is particularly problematic for customs employees and other players in the supply chain, whose job consists in reading or visually inspecting a packaging, whose different elements may or may not be correctly replicated by counterfeiters. Some of these systems convert the object into a 3D representation displayed on a computer screen. Understandably, it would be challenging for anybody, even for customs or logistics employees to detect a real medicine from a fake. It is an either-or situation: either the replica is so poorly done (fake brand name, spelling mistakes, or other omissions) that there is no need to access the packaging information to determine that it is a counterfeit, or the replica is so well done that the visual inspection will lead to think that the packaging contains real medicine. A visual inspection of packaging by the human eye is unreliable in identifying counterfeits.

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

Many pharmaceutical companies have added visible security features to their packaging to prevent counterfeiting. These include holograms, kinegrams, embossing, micro printing, moiré, or special ink, such as optical variable ink, to name a few. However, these visible features only provide minimum security and require training for effective authentication. By the same token, if a company suddenly decides to discontinue the use of visible security features, consumers might mistake a genuine product with 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, because counterfeiters will be unable to identify the presence of such features. For example, "good" counterfeit banknotes always include a replication of the visible security features, but not of the invisible ones. However, to prevent leaks, 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.

Anti-counterfeiting literature also suggests that a specialized 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. As we have seen, it is now possible to print digital security features using normal visible ink or varnish on primary or secondary packaging (e.g., folding boxes, blister packs, labels) to achieve invisible protection. In addition, these digital security features can be verified by means of an off-the-shelf office flatbed scanner or an iPhone4 smartphone device. While covert (hidden) features have traditionally required specialized knowledge, features, and means to verify them, drug manufacturers can now have

their printers or suppliers print invisible markings on primary and secondary packaging without using special inks, as well as perform product authentication using readily available consumer electronics - *Figure 2*.

Digital solutions for product authentication also have had a significant impact on the cost and wait time of implementing an anti-counterfeiting program for multi-brand companies using multiple production plants. For example, when deploying an anti-counterfeiting program, it is necessary to provide the various production plants with the right quantity of items 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 also can affect the packaging printing equipment if special ink is used or if extra features such as holograms or taggants are 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.

As mentioned earlier, other visual features include the shape of the packaging and other printing details that counterfeiters may not have identified. A discrepancy between a genuine pack and a counterfeit can 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, performing a machine-readable verification using digital authentication processes result in virtually no added costs to the branded manufacturing company.

Local vs. Remote Verification Process

In order to perform a "genuine-or-fake" verification, there are two distinct methods: a local process using the appropriate hardware or a remote identification using an online server.

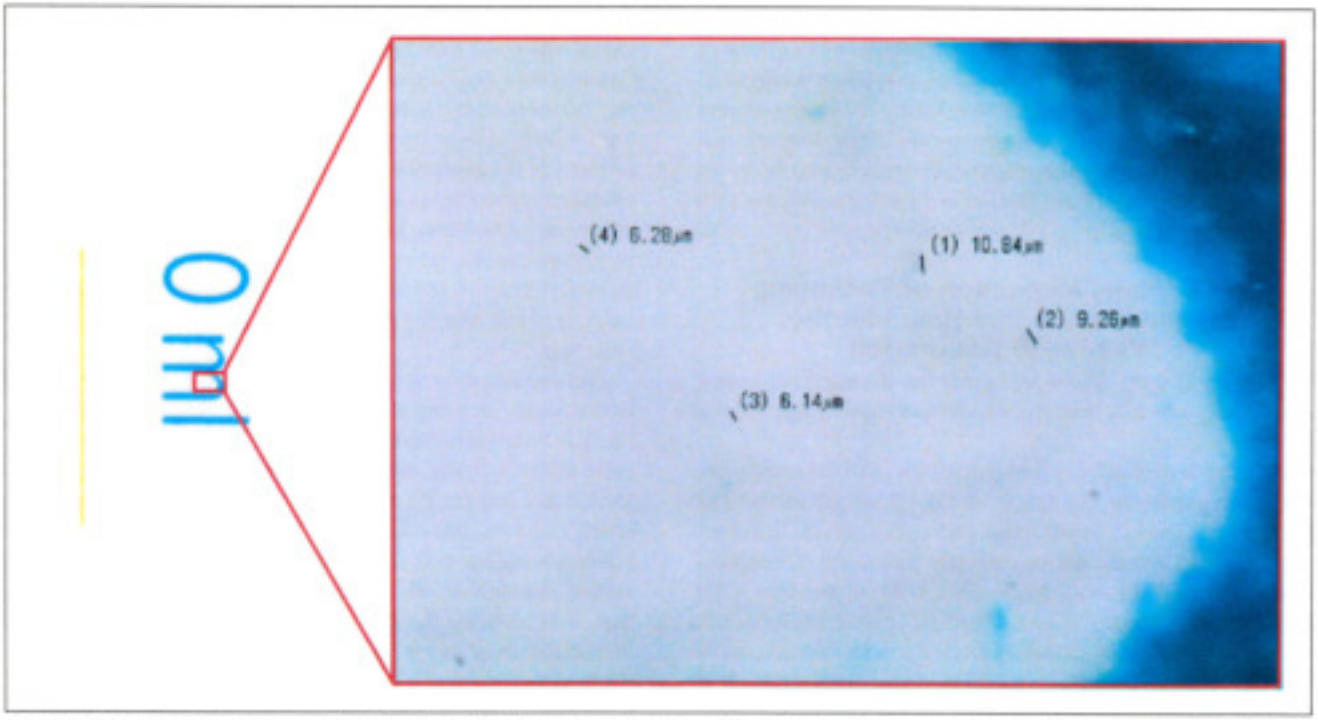

Figure 2. Example of a microscopic detail of invisible micro dots printed on the packaging thus generating a unique pattern that identifies the product as genuine.

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 in 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[10] shows that organized 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 programs. 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 in 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 Organization[11] – 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 analyze different parameters of a packaging in order to automatically assess its authenticity[12] 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 authorizations 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 authorized 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 customization 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 only be necessary to use it. This approach also frees very large organizations 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 at Various Stages of the Supply Chain, Including at the Patient Level?

Smartphones 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 - *Figure 3*. However, these advancements do not mean that mobile verifications should be placed in the hands of patients, because of various unanswered questions raised at the beginning of this article.

First, it is totally different to equip an employee of the branded manufacturing company with an iPhone4 and the appropriate application than to make this application readily available online. Indeed, consumer equipment is often in very poor condition: dusty camera optic, partly damaged screen, or poor connectivity. By the same token, if an anti-counterfeiting

Figure 3. Smartphone genuine-or-fake verification example.

solution goes public, it is necessary to understand that it also will be available to the counterfeiters themselves. In this case, strict verification processes should be in place to detect attempts to tamper with the supply chain.

Today, the internet suffers from the fact that security elements were not considered at the early stages of its development. Indeed, the internet's original users were educated scientists whose minds were simply not attuned to its possible fraudulent uses. This mistake should not be repeated if patients or consumers are one day given the opportunity to perform product authentication.

In the interim, it might be interesting to invite frequent medicine consumers, who might not get reimbursed or might adopt a consumer-like attitude toward purchasing drugs, to test mobile verification, provided they are monitored and equipped with devices in good working condition. This study would allow a select number of consumers to perform and possibly legitimize the use of mobile verification in combating counterfeiting. The results from this first study also would allow to fine tune the service and extend it to a larger pool of users.

Several factors, such as the increasing use of smartphones; changing medication refund policies; the aging of the world population; the development of online commercial sites; and the reduction of door to door shipping costs will all accelerate the need to develop a suitable, easy-to-use, and reliable product authentication process at the patient level.

Summary

The following summarizes the key points made in this article:

- Patients should not bear the responsibility for uncovering fake medicine.
- Pharmaceutical companies and any actors involved in the manufacturing or distribution of medicinal products should oversee and manage the authentication process of medicinal products.
- Serialization and e-pedigree cannot prevent the introduction of falsified medicine into the legal supply chain.
- Identification and authentication are two different problems that require adapted solutions.
- Covert (invisible to the naked eye) security features provide higher security compared to overt (visible) ones.
- Digital solutions for product authentication are easier, faster, and more cost-effective to deploy compared to security consumable-based solutions, especially when considering large production volumes.
- Machine-readable security features are 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. This approach will reduce the risk of leaks, especially if very few people are involved in managing the sensitive security data elements.
- Future developments in the smartphone industry, including better image capabilities and increased computing power, might accelerate the need to develop a suitable, easy-to-use, and reliable product authentication process at the patient level.

References

1. Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011, Official Journal of the European Union, 01.07.2011, L 174/78-8.

2. "The Counterfeiting Superhighway," *European Alliance for Access to Safe Medicines*, p. 27, http://v35.pixelcms.com/ams/assets/312296678531/455_EAASM_counterfeiting%20report_020608.pdf, 2008.

3. "Anti-Counterfeit Technologies for the Protection of Medicines," World Health Organization's International Medical Products Anti-Counterfeiting Taskforce (IMPACT), p. 8, May 2008, http://www.who.int/impact/events/IMPACTACTechnologiesv3LIS.pdf.

4. Barlas, S., "FDA Changes to Drug Bar Code Rule Could Have Significant Impact on Packaging Lines," *Healthcare Packaging*, February 23, 2012, http://www.healthcarepackaging.com/archives/2012/02/fda_changes_to_drug_bar_code_r.php.

5. Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011, Official Journal of the European Union, 01.07.2011, L 174/80.

6. "Anti-Counterfeit Technologies for the Protection of Medicines," World Health Organization's International Medical Products Anti-Counterfeiting Taskforce (IMPACT), p. 5, May 2008, http://www.who.int/impact/events/IMPACTACTechnologiesv3LIS.pdf

7. Cryptoglyph®, AlpVision website, http://www.alpvision.com/cryptoglyph-covert-marking.html.

8. Meylan, R., *Handbook of Nutraceuticals Volume II*, "Protection of Molded Nutraceutical Container and Vial Closures against Counterfeiting," p. 545-546, CRC Press, ISBN 9781439823682, 2011.

9. Fingerprint™, AlpVision website, http://www.alpvision.com/solid-parts-authentication.html.

10. FDA Conducts Preliminary Review of Agency's Diversion and Counterfeit Criminal Case Information, September 2011, http://www.fda.gov/downloads/Drugs/DrugSafety/DrugIntegrityandSupplyChainSecurity/UCM272150.pdf.

11. IPM: A WCO initiative to combat counterfeiting, June 2010, World Customs Organization website, http://ipmpromo.wcoomdpublications.org.

12. Krypsos Web Application, AlpVision website, http://www.alpvision.com/krypsos-online-authentication.html.

About the Authors

Dr. Fred 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, Switzerland (EPFL)" Signal Processing Institute (ITS). He can be contacted by telephone: +4121-922-6121 or by email: fred.jordan@alpvision.com.

AlpVision, Rue Du Clos 12, 1800 Vevey, Switzerland.

Dr. Martin Kutter is co-founder of AlpVision and today serves as President and Chairman of the Board. He holds a PhD from the "Ecole Polytechnique Fédérale de Lausanne, Switzerland (EPFL)" and an MS from the University of Rhode Island, Kingston, USA. For his PhD, Dr. Kutter received the "Best Thesis Award" in 2000. Since 1996, Dr. Kutter has published more than 25 publications, including various books and has filed numerous patents. Dr. Kutter has built on solid industrial experience and has earned an impressive scientific reputation. He is the co-inventor of Cryptoglyph and Fingerprint, the core technologies currently being used by AlpVision. He can be reached by telephone: +4121-948-9766 or by email: martin.kutter@alpvision.com.

AlpVision, Rue Du Clos 12, 1800 Vevey, Switzerland.