Value Protection

Roland Meylan at AlpVision investigates low-cost digital security solutions to protect pharmaceutical products against counterfeiting

Anti-counterfeiting and traceability features are often confused, especially with the current serialisation and e-Pedigree programmes under discussion in some countries, and the various claims to be able to uncover counterfeits. Anti-counterfeiting and traceability are different issues, requiring different solutions. On the one hand, traceability demands standardisation and interoperability amongst the various manufacturers and the intervening third parties within the supply chain up to the dispensing point; on the other, anti-counterfeiting features, especially covert ones, need secrecy and confidentiality. They should be constantly kept in step with the technological advances of the counterfeiters. They are the sole responsibility of each individual branded product's manufacturer, and they cannot be standardised.

WHAT SHOULD BE PROTECTED?

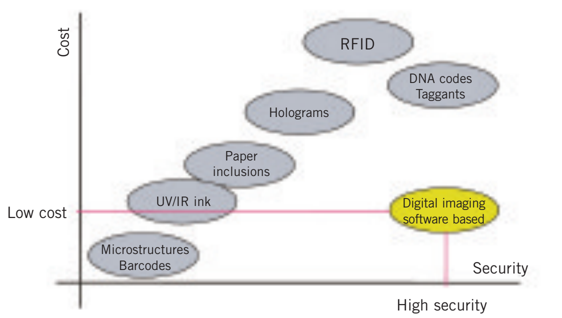
If fraudulent business is generated through sales of a mix of genuine and fake medicines in a reprocessed genuine secondary packaging, marking the secondary packaging with visible security features or visible coding does not offer sufficient protection. Moreover, at the end of the day, patients will consume the medicine, not the packaging. That is why many pharmaceutical manufacturers are now looking for solutions to authenticate the tablets, for example, and thereby complement the security features in the packaging and labelling.

SECURITY FEATURES VISIBLE OR INVISIBLE TO THE NAKED EYE?

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. However, these visible features not only provide minimal security, but they also require training for effective authentication when faced with fraudulent reproductions of such visible security features (1).

The use of 'covert' features invisible to the naked eye produces a higher level of protection, due to the inability of counterfeiters to identify the presence of such features, and their consequent inability to attack them. Covert security should never be disclosed and, to prevent leaks, they should only be known to a limited number of trustworthy persons.

Figure 1: Various security features, visible or invisible to the naked eye



The best known covert security solution is invisible ink, such as UV ink (visible under ultraviolet light) or IR ink (visible under infrared light). To authenticate these inks, a lamp which emits light in the required wavelength range will suffice. The drawback of these inks is that they are readily available to anyone. There are other chemical tracers or ink additives providing security against counterfeiting, such as DNA or magnetic tracers which provide higher security by relying on uncommon dedicated verification devices.

The problem with such special inks, ink additives or taggants resides in 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. All these techniques based on a security additive can be qualified as 'analogue or hardware based', because they require additional security elements or special substances.

Pharmaceutical packaging is produced by thousands of different printers and converters; it follows that one of the most important criteria in the selection of a security feature is its capability to be industrialised and deployed to all subcontractors. Efficient solutions should not entrain a change in the production processes, a need to acquire new machinery or to manage extra consumables which are difficult to integrate into the production process; in other words, efficient solutions should have only a minor impact on the speed and cost of production.

DIGITAL IMAGING AND SOFTWARE BREAKTHROUGH

As in other industries, the digital revolution has opened exciting new possibilities. Digital technologies can now be used to combat counterfeiting of pharmaceutical products at low cost, while providing a high level of security (2). These digital technologies are breakthroughs compared to former methods. The chemical, micro- or nanotechnology experts have been replaced by software engineers and digital imaging specialists.

An article in the online version of the *Washington Post* revealed that some

Figure 2: Example of a microscopic detail of a totally invisible security pattern incorporated in the varnish layer of the packaging.

The patented invisible marking is achieved by the creation of thickness variations in the lacquer layer, thus generating a unique pattern that identifies the product as genuine.

manufacturers of home and office printers deliver printing equipment that adds invisible marks on each printed page, without the user's knowledge (3). The purpose of this hidden marking is to identify printers used for fraudulent printing. Aside from the political or legal implications, this incident shows that, with today's technology and equipment, it is possible to print invisible information with normal ink and standard printing machines.

For the packaging industry, the incident described above has an important implication: an industrial packaging printer using standard printing machines and standard ink can produce secured packaging for manufacturers of branded products using high security covert marking without additional production cost, and without reducing production speed. This latter consideration is of high importance when large volumes of items are considered.

DIGITAL SECURITY AND INVISIBLE MARKING

However, the printing of invisible information using normal visible ink is insufficient for the protection of a document or packaging against fraudulent replication or counterfeiting. The tracking code mentioned in the *Washington Post* article has been cracked (3). But if the constant increase of computing power makes it possible to crack codes, it also opens the door to the development of new coding which is much more resistant against replication or hacking.

For example, a patented protective packaging has been designed which features variations of the thickness of the lacquer layer, thus generating a unique pattern which identifies the product as genuine and which can be applied by regular varnish printers (offset, flexography, rotogravure) without incurring additional production cost (4). Such a security feature is notably very effective on aluminium foil blister packs.

In this case, a colour filter or special light will not reveal the presence of the security feature. Replication of the invisible pattern is not possible, given that it is camouflaged within the imperfections of the varnish layer. The pattern is made of random micro-holes (10 to 80 microns) which produce the variation in the thickness of the coating, and are invisible to the naked eye. The pattern is generated by a 128-bit software key, big enough to offer many billions of different patterns, each one constituting a unique identity.

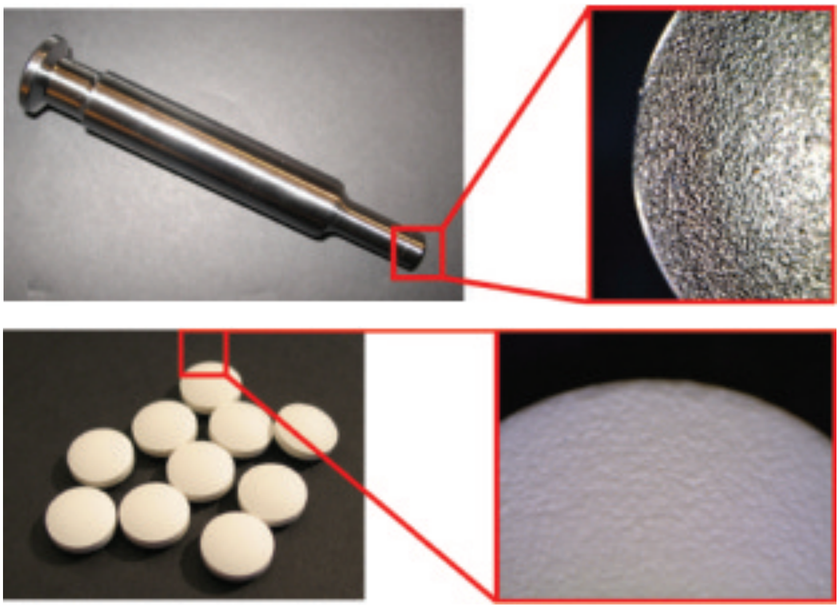


Figure 3: Microscopic details of a punch die set used in the production of tablets, together with a sample of tablets produced with the punch die set, all of which contain its 'signature'. The signature serves as a security feature even when coated

Accordingly, the invisible pattern can be easily integrated into any current packaging production line. The digital file of the security pattern is simply embedded in the prepress packaging artwork. It requires no modification of the packaging design and it is incorporated as usual before creation of the printing cylinder.

COULD VISIBLE OR INVISIBLE MARKING BE ADDED TO THE TABLET ITSELF?

As mentioned above, protection of pharmaceutical packaging may not be enough. Solutions have been proposed based on embossing of the tablet or use of a chemical taggant; but such solutions require modification of the manufacturing process. In particular, the use of a security taggant requires proper management of this type of security feature. In addition, nothing would prevent counterfeiters from finding a way to replicate this marking, whether it is visible or invisible.

A new patented solution recently disclosed is based on the unique and intrinsic characteristics of the tooling used in the tablet presses (5). With this solution, additional marking is unnecessary. The natural micro-imperfections of the punch die sets are enough to serve as security features. The process only requires the storage of a digital reference image or 'template' of each punch die set used in the production of the tablets. It follows that only a limited number of templates are necessary to authenticate the entire production of tablets. High-tech digital imaging software is used for comparing the templates with the digital image of the surface of a suspicious tablet which is produced by standard low cost office flatbed scanners or simple digital cameras.

The same process can also apply to identification of the closures of moulded plastic jars serving to contain powder or liquids. The closures are moulded parts which bear an exact replication of the

Figure 4: Plastic closure of a jar of baby food which can be identified with a reference template of the mould used to produce it

features of the mould used to produce them, giving them all a unique identity.

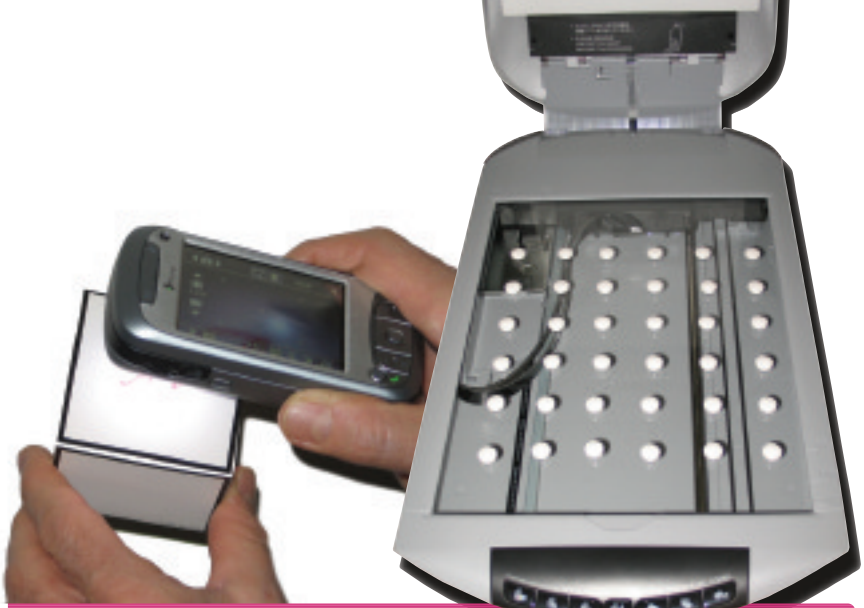


Figure 5: Example of 'genuine-or-fake' verifications using standard consumer electronics equipment which can be offline or online

'GENUINE-OR-FAKE' VERIFICATION

On selection of a security feature, it is not enough just to evaluate the purchase cost, the robustness against fraudulent replication, the cost of implementation in the production process, the cost of global management and any impact on the production process. A crucial part of the problem is how a 'genuine-or-fake' verification is performed.

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

- The features which use human sensory perception
- The 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 to hand. But, with a machine-readable feature, only a step-by-step process is required which, if it is well documented, can be performed by anyone without any specific knowledge or training.

ONLINE AND OFFLINE MACHINE-READABLE VERIFICATION PROCESSES

A machine readable security feature verification process may be performed online or offline depending on the nature of the process itself.

For chemical or other ink additive security features, offline security processes are mainly carried out with specific scanners. In this case, achievement of verification programmes at multiple sites requires the branded product manufacturer to purchase multiple scanners. The alternative would be that any suspected item be sent to a central location for verification. Such a procedure would be quite costly, and would considerably delay the desired 'genuine-or-fake' verdict.

Internet and mobile connections are today widely available around the world, including in developing countries. A security feature enabling 'genuine-or-fake' verifications to be carried out online 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, thus avoiding the risk that retro-engineering be carried out on the equipment with a view to counterfeiting. The sensitive security elements are instead located in a secured server in just one location in the world. Another major benefit of an online verdict is the consolidation of all the verdicts performed worldwide, thus facilitating the detection of any correlation between various fraudulent sources within the supply chain. As with all criminal acts, the quicker you uncover them, the more you are well positioned to identify the criminal source and can act to stop it.

CONCLUSION

The combination of security features on packaging and labelling, together with tablet and jar authentication, allows a very high degree of protection against counterfeiting, and has to be considered separately from serialisation and track and trace features. Software and digital imaging technology serving to produce covert security features enables protection of pharmaceutical products against counterfeiting without extra production cost, nor degradation of the production speed, nor any visible impact on the packaging and labelling. Machine-readable security features enable any authorised person to carry out instant online 'genuine-or-fake' verifications worldwide, with almost no prior training nor any specific security knowledge. If online verifications are feasible, it allows instant consolidation of all 'genuine-or-fake' verification results performed anytime anywhere, thus maximising the chances of uncovering fraudulent sources and putting a stop to them.

References

1. Covert and Overt Protection for Valuable Documents, *Information System Security Association Journal* pp32-34, November 2006
2. Protecting Pharmaceutical Products from Counterfeiting Using Digital Imaging Technologies, *Pharmind* pp1,005-1,008, August 2006
3. Sleuths Crack Tracking Code Discovered in Color Printers, www.washingtonpost.com, 18th October 2005
4. www.alpvision.com/cryptoglyph-covert-marking.html
5. www.alpvision.com/solid-parts-authentication.html

About the author

Roland Meylan is the co-founder of AlpVision, and currently serves as Corporate Communications Manager. He holds an MS degree in Signal Processing and Digital Communication from the Swiss Federal Institute of technology of Lausanne (EPFL), as well as a postgraduate degree in Business Administration from IMD Lausanne International Business School. Roland started his career at the graphic division of Bobst SA. He also worked in electronic communication over international data transmission networks, the forerunners of the internet. Email: avinfo@alpvision.com