OLD EQUIPMENT CAN HARNESS NEW SECURITY TECHNOLOGIES

IT and digital imaging software enable regular packaging printers to produce high level covert security packaging for brand protection and grey market detection. Roland Meylan, co-founder and corporate communications manager of AlpVision SA, a company at the forefront of security printing technologies, shares his latest white paper with Packaging Europe.

IN this day and age the billions of branded fast moving consumer goods (FMCG) and pharmaceuticals which are produced every year have become the target of counterfeiters and fraudulent importers worldwide. To ensure their protection, invisible security features can be incorporated in primary and secondary packaging using normal packaging printers. The regular equipment of packaging suppliers is sufficient. Software and computer science can help brand owners protect their products against counterfeiting and grey market activity by means of standard image capture devices and transmission via the Internet or mobile networks. A secured server and an open IT platform managing the security elements of the various products enable multinational firms to secure their products worldwide, even when the packaging is produced on numerous printers in different locations.

Covert and overt security features

Many features can be considered as security elements on packaging, such as for example tear-off detection labels, holograms, kinegrams, two dimensional barcodes, embossing or optically variable inks. The basic problem attached to overt security features is that they are visible to the naked eye and are consequently an easy target to attack. If the goal is to successfully protect products against organised crime rather than against individual defrauders in their kitchens, then we need to assume that the fraudulent producers have the financial means to replicate at will the original manufacturing processes. It follows that in these circumstances it is extremely difficult to detect the genuine product from fake ones through only visual inspection, given that overt security features can be replicated as well. These visible markings can also be erased or modified with the intention of fraudulently importing genuine products (grey market activity), for example through use of remarking techniques.

As opposed to overt security features, covert security features are not visible to the naked eye and therefore not distinguishable as present or not, on a packaging, for example. However, the security features must take into account the risk of leaks in a multiperson environment. One of the basic drawbacks of covert security is that it usually requires special scanners or investigative means operated by specialists. In this case, the authentication process cannot usually be performed without the product being sent to a dedicated forensic laboratory. However, new technologies for covert security are now available, based on software and digital imaging. They offer the significant advantage that special scanners are not required for authentication, nor any other device or specific knowledge.

Digital imaging and software breakthrough

As in other industries, the digital revolution opens exciting new possibilities. Digital technologies can now be used to combat counterfeiting and to track and trace consumer products. The chemical, micro or nanotechnology experts have been replaced by software engineers and digital imaging specialists. The more promising new solutions are based on the same digital imaging technologies and cryptography as used to protect bank notes and to secure online banking services.

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

The above has two important implications for the packaging industry and security printing domain:

• First, an industrial printer of packaging, using standard printing machines and standard ink, can produce secured packaging for manufacturers of branded products using high security covert marking

• Second, a manufacturer can secure its products without informing the printer that the packaging contains an invisible security feature. This reduces the number of parties involved in a product security process and offers a real advantage.
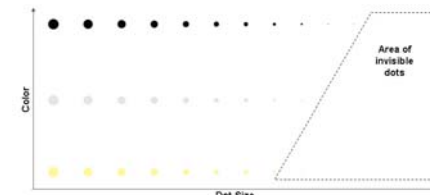
Cryptoglyph invisible marking

Cryptoglyph is the combination of two technologies:

• Cryptography using digital ciphering and deciphering with a 128-bit key, big enough to offer billions of combinations of dots, each one constituting a unique pattern.

• Glyph or marks, with appropriate colour and pattern so that they are camouflaged within the printed material which can be white or coloured.

Cryptoglyph is the only security process in the world providing invisible marking with standard ink and standard printing processes (offset, rotogravure, flexo, laser, inkjet, etc). Accordingly, Cryptoglyph can be easily integrated into any current packaging production line. Simply embed the invisible Cryptoglyph file in the prepress digital packaging image file before printing, without any modification of the packaging design.

How can invisible marking be detected without dedicated scanners or processes?

The constant progress in microelectronics and home computing has led to affordable, off-the-shelf and very powerful imaging devices such as flatbed scanners, webcams and PDA camera phones. These devices can capture an image on a mouse or button click and send it to a secured server for analysis, the same way as people are sending family photographs to their relatives.

The authentication is then automatically performed by special software installed on the server located in a safe area. A verdict 'genuine or fake' is returned to the person who asked for the authentication process, either on the mobile phone or PC screen.

Brand protection with innovative technology

A technological solution is not in itself sufficient for the delivery of a suitable and industry-compatible application which is compliant with the industrial process realities. Here again, there have been many project failures on the introduction of new systems based on very high-tech processes, without consideration for the reality of high volume production (in billions) of consumer goods or pharmaceutical products worldwide.

To manage the many products and SKUs (stock keeping units) which are produced daily and managed by large multinational branded product producers, it is necessary to embed the brand protection technology into a safe system which is fully compliant with the severe rules established by such large multinational firms and the relevant health authorities.

In parallel with the recent completion of a major deployment of a Cryptoglyph brand protection solution for a very large pharmaceutical producer operating worldwide, the Swiss company AlpVision announced that it fully complies with the US FDA 21 CFR Part 11 requirements for Electronic Records and Electronic Signatures (ERES).

An IT (information technology) open platform was developed to enable the brand owner to produce the Cryptoglyph patterns to be associated with each product or SKU and to be applied by various packaging printers. A simple quality control (QC) procedure was also developed to enable the brand owner to validate the packaging before mass printing and to ensure the presence of the invisible marking.

Conclusion

Digital technology and computer science have achieved breakthroughs in the brand protection and grey market detection domains. Constantly improved devices and services are now in use daily for business activities, eCommerce, mobile commerce or entertainment by billions of people worldwide. They open up new possibilities for brand manufacturers to provide a single point of contact for the authentication and identification of products along the whole supply chain worldwide, up to and including the end-consumer. Deployment can be extremely rapid, given that only standard software such as an Internet or mobile browser is required to get access to a secured authentication point from anywhere in the world. Standard printing processes and standard ink used by traditional industrial packaging manufacturers can produce a high level of covert security using technologies fully under the control of the brand owner. □

Visit: www.alpvision.com