Digital Security Printing: Enabling Product Tracking and Authentication Using Existing Product Lines

Steven Simske, Philippe Mücher and Carlos Martinez
Hewlett-Packard Company
Fort Collins, Colorado; Maastricht, Netherlands; Aguadilla, Puerto Rico

Abstract

Many pharmaceutical and other high-value consumer goods are prepared for shipping using relatively simplistic packaging lines. However, their simplicity helps contain overall product costs and provides an excellent opportunity for digital security printing. Digital printing brings variability to pre-printed targets. Authenticating these print targets during the packaging process associates them with a large database, or registry, maintained by the packager. In this way, any desired amount of security can be added to the packages, depending on the number and quality of authenticating devices (optical, electromagnetic, chemical, etc.) added to the packaging line. Importantly, the security print features can be pre-printed with variability, thus reducing their impact on the packaging line. In this paper, we provide examples of how pre-printed variability, combined with in-line authentication and association with a registry, greatly increase product security with a minimal impact on the industrial production line itself.

Introduction

Adding variable data printing (VDP) to existing pharmaceutical production lines makes every printed region a potential means for track and trace and/or authentication of a package or other end unit. Since printing is ubiquitous for all branded products, it can be argued that *not using VDP* is a feckless oversight in the reality of a counterfeit market that equals 10% of world trade.[1] The addition of VDP print features to printed packaging/product branding/instructional material will logically take on one of the following strategies:

1. Pre-print the packages in their entirety and associate them with the registry beforehand.
2. (1.) but with association with the registry as they move through the packaging line.
3. Pre-print security print features beforehand and affix them to the packages in-line. Associated with the other printed elements beforehand.
4. (3.), but associated with other printed elements as the packages in-line (not beforehand). Like (3.), involves on-line registry association.
5. Apply security print features directly on the packaging line (during finishing).

Pre-Printing Packages in Their Entirety

Options (1.) and (2.) above are compared here to introduce the concepts involved in "on-line registry association". In option (1.), all of the printing occurs before the package is loaded onto the production line, and all the unique package identifiers are entered into the product database (or registry) before the packaging occurs. The advantage of such a strategy is that the package line can be extremely simplified—no printing, no scanning, no intelligent monitoring need occur. The reality of this situation, however, is that things go wrong in the line, and packages will occasionally need to be "knocked out", with concomitant notification to the registry. This means that in-line tracking (automatic scanning and monitoring) is required, regardless of strategy, and so the only advantage to this strategy is to remove printing from the production/ packaging line altogether. This, in turn, imposes a high degree of security on the printing and transportation of the packages, and requires that printing facilities be co-located with the product packaging lines.

Option (2.), on the other hand, assumes that packages will be tracked, and thus takes advantage of the in-line monitoring and scanning that are required for quality control and tracking. The onus of this option is the need for a real-time connection to the registry, but such a connection is *de rigueur* for packaging lines, and so imposes no overhaul. This option also potentially lessens the security required during printing and shipping—if the security print features meet the following two requirements: (1) there are an overwhelmingly larger number of possible identifiers for the feature than the number of packages that will boast the feature; and (2) the printing of the features can be randomized (a process we call random VDP). Under this scenario, a random set of security print identifiers are printed, and then the identifiers on the features are scanned and recorded as the packages progress through the line. Since combination security print features exist that can provide more than 10^{1000} unique identifiers in a square cm, this means that, if the security print features can be accurately and consistently read (e.g. with scanners as simple to use as today's 1-D and 2-D bar codes), there is virtually no chance a counterfeiter will guess a legitimate identifier (for example, if 10 million packages are shipped, only 1 in 10^{993} of the possible identifiers will be legitimate). Instead,

the counterfeiter will have to make copies of a single (or handful) of legitimate identifiers, and hope that end users do not check their product against the registry. This is where deterrence ends and track and trace begin for all security features, and so poses no new challenge for security printing.

Pre-Printing Security Features Only

Options (3.) and (4.) rely on the pre-print strategy described above for the overall package, but instead confine their variability to specific security print features on the package. This is a useful approach because it takes into account the fact that most high-quality presses (offset presses, dry electrophotography presses, etc.) do not handle variable data, and so allows a VDP press, such as the HP Indigo Press,[2] to provide VDP for parts of the overall packaging (labels, inserts, stickers, etc.). This saves costs, since large press runs can be used to print the majority of the package in a "static" format, and then shorter runs can be made for the labels and other variable print elements. The VDP strategy can be changed from one lot, pallet, etc. to the next, providing an "innate moving target" for counterfeit deterrence.

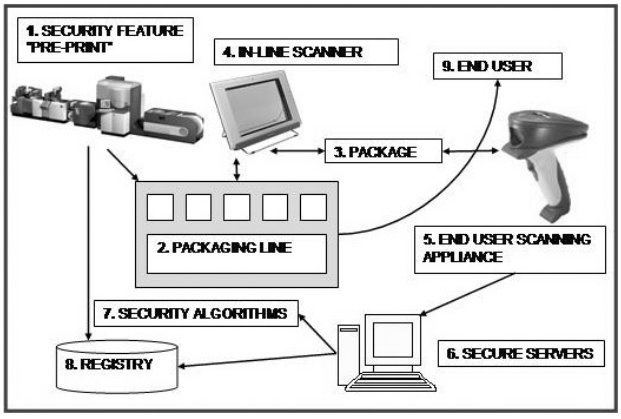

Figure 1. Schematic of Option (4.)

In addition, these approaches provide a means to add security printing without disrupting existing packaging lines. Static, branded package designs can be outsourced from an offset print shop. VDP security features can then be printed by another specialized press. The printing of labels, inserts, tags, etc., can thus be provided separately from the (static) packaging, affording an integration control point for the manufacturer while simultaneously giving the manufacturer greater flexibility in the value chain (the manufacturer can use a different press for the packages and the VDP printed elements, for example). From this standpoint, options (3.) and (4.) begin to look much like options (1.) and (2.). However, it should be noted that on-line printing, such as with traditional thermal label printers (ubiquitously used for bar codes), is an addition distinction of these options.

The key integration issue for options (3.) and (4.) is associating the security print features with the other printed elements. Figure 1 shows a schematic for option (4.), in which security print features [Block 1] are pre-printed on a VDP press and their identifiers entered into the registry [Block 8]. Next, these features are merged with the package as they enter the packaging line [Block 2]—this is distinguished from option (3.), in which the security features are merged with the packages before they enter the packaging line. The package [Block 3] is authenticated in-line [Block 4] and at this point correlated with the previous registry entries. Once in the hand of end users [Block 9], a scanning appliance can be used to authenticate the package [Block 5], provided they or a trusted third part (pharmacist, physician's office, etc.) are allowed to connect to the secure servers [Block 6] hosted by the manufacturer to verify the scan. Importantly, in this scenario the manufacturer (or its trusted partners) controls the packaging line, in-line scanners, security algorithms, registry and access to the secure servers [Blocks 2, 4, 6, 7 and 8].

Adding Security Features During Finishing

With option (5), the entire package is pre-printed with identical, static content. No in-line authentication need take place, since every package is identical. Then, security print features are added in the finishing stages (e.g. as attached features, not printing). While possible, this requires the addition of on-line finishing, a complicated alteration to the existing packaging line.

Conclusion

We herein review ways to add security printing to packaging lines. Option (4.), "pre-print and authenticate in-line", will provide the greatest product protection. It also requires only modest change to most existing package lines.

References

1. "The Extent of Counterfeiting", http://www.a-cg.com/info.html.
2. HP Indigo Digital Printing Presses, http://h30011.www3.hp.com/.

Biography

Steven Simske is a senior researcher at Hewlett-Packard Labs in Fort Collins, Colorado, USA. He is the system program manager for HP's security printing architecture, algorithms and authentication team. Steven has worked in medical imaging, image analysis and recognition, and content understanding for the past 20 years. Steven is also a senior research associate in Aerospace Engineering at the University of Colorado, and an adjunct professor in Physics at the Colorado School of Mines.