Using Variable Data Security Printing to Provide Customized Package Protection

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

Abstract

Variable data printing (VDP) provides an opportunity to improve the security of packages. Currently packages, even for high value goods like pharmaceuticals, are often highly susceptible to counterfeiting. This is due in part to the fact that most of the printed material on packages is "static" in nature. Even "variable" data features—such as bar codes, lot numbers, and expiry dates—are typically identical for entire pallets or even larger production runs. This makes "spoofing" far easier than it should be. With VDP technology, every copy hole on a package is, potentially, part of a multi-feature authenticating design. This is advantageous, because when multiple features are involved, verification accuracy degrades with package damage; the counterfeiter has to determine how each copy hole has been used to encode both overt and covert information; and a combination of end user, investigator and machine authenticable features can be deployed. Variable linking of different variable print features furthers the package protection. In this paper, we address how fully variable package printing is implemented to provide security while still addressing branding considerations.

Introduction

All branded products are accompanied by printed material of some form—labels, packaging, inserts, cartons, boxes, etc. Therefore, printing should not be overlooked as a means of fulfilling FDA recommendations for overt, covert and forensic anti-counterfeit technologies.[1] Visible inks, from bar codes to specialty inks, provide overt anti-counterfeiting protection. Invisible inks, layered inks, and imperceptible variation in any printed feature on the package provide covert protection. Embedded reagents in the inks—from DNA and RNA to bubbles and magnetic orientations—can be used to provide forensic protection.

Variable data printing (VDP) is an important means of extending the anti-counterfeiting protection offered by printing. First, VDP is not feasible on high-quality offset and other presses, limiting the technology options for the would-be counterfeiter. Second, VDP provides the anti-counterfeiter with multiple means for integrating a specific identifier, encrypted or otherwise. Third, and most important, VDP allows any printed region to become a potentially variable region, thus contributing to the overall level of anti-counterfeiting protection *and providing an innate moving target for the would-be counterfeiter*. This is because, with VDP, the nature of the security feature in each printed region can be varied at any level—lot, pallet or even individual end unit.

Security Print Example

For example we next consider a simple 1-D bar code that can be made to contain many layers of variability through the use of VDP. Specifically, we make use of inks that have different properties in visible and infrared light, such as shown in Figure 1 for process black ("Ink with opaque characteristic") and Anoto black[2] ("Ink with transparent characteristic").

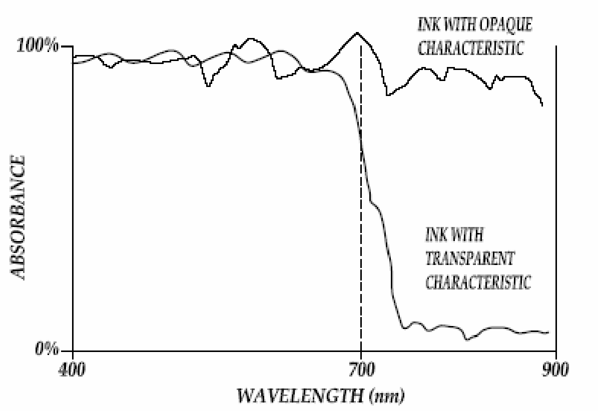

Figure 1. Infrared opaque and transparent black inks

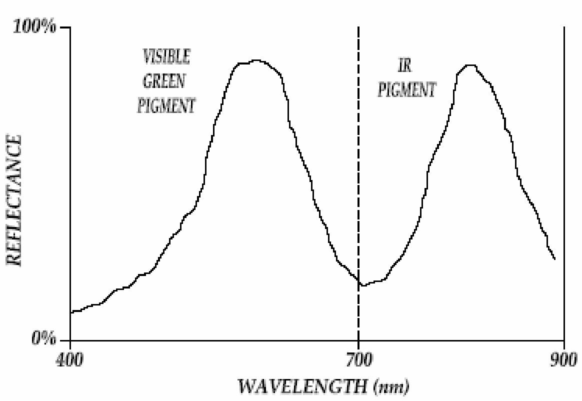

Figure 2. Ink with green visible and infrared pigments

Figure 1 shows two inks that appear black to a human observer. The "opaque" ink, however, also absorbs infrared light, while the "transparent" ink does not. VDP techniques can be used for simply selecting between these two black inks, and deciding what sections of under-printed infrared inks to reveal.[3] A similar pair of custom inks can be created with green and infrared pigments (Figure 2). Thus, separately or in combination the following are possible deterrent strategies: (A) vary which sections of the black ink are opaque and transparent (see 14 in Figure 3); (B) vary the infrared patterns (see 12 in Figure 3); and (C) vary the emission frequency of the infrared ink. With these strategies in place, a security print target half an inch on a side can provide more than 10^{1000} different permutations. A unique identifier for each unit can be provided with virtually no chance of counterfeiting or spoofing, and no repeated identifiers. Additionally, the over-pattern can be printed to exactly match the desired product branding, while the details of the identifier are literally hidden.

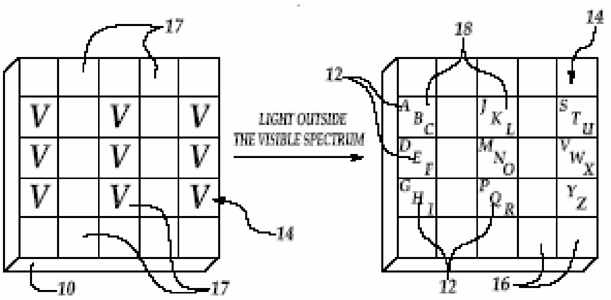

Figure 3. Security print pattern with many permutations

Innate Variability

Figure 4. This photo can be tied to printing elsewhere on the product (e.g. "Balanced Rock" printed on the insert), along with myriad photo-specific security print features (watermarks, under-printed uv/infrared, specialty inks, etc.)

Any printed region can be used to provide a unique identifier to a package. In Figures 1-3 are demonstrated possibilities around a "dedicated" security print feature, which can be matched with a brand identifier (logo, etc.) or another deterrent such as a bar code, copy-detection pattern,[4] or other overt feature. In Figure 4, a variable photo is shown. This photo can appear on one piece of printed material (box, carton, insert, etc.) and a matching (linked) allusion to it (e.g. "Balanced Rock") can be printed on the individual units (the text can also be color matched to the principal color of the photo). Watermarks, under-printed (uv, infrared) inks, specialty inks and the strategies mentioned for Figures 1-3 can be merged with the photo in a "moving target" deterrence.

Conclusion

Security print features are given additional power through the use of VDP. Variable data presses, such as the HP Indigo Presses,[5] allow brand owners to craft their campaigns featuring the types and extent of variability they see fit, which will usually depend on branding, pricing, and package complexity.

We believe that security print features will continue to outperform all other security features for density of encrypted data for the next several years. Astronomical numbers of permutations can be packed in small security print features, and with the use of microprinting, reasonable data densities (more than 1 kB/cm^2) can also be achieved.

References

1. FDA Counterfeit Drug Task Force Interim Report, U.S. Department of Health and Human Services, Food and Drug Administration, October 2003, 46 pp. On-line at: http://www.fda.gov/oc/initiatives/counterfeit/report/interim_report.pdf.
2. Anoto substitute black ink, SunChemical AB, P.O. Box 70, Bromstensvagen 152, SE-163 91 SPANGA Sweden.
3. Steven Simske, et al., Ink Coatings for Identifying Objects, HP Docket No. 200405356, filed with USPTO 12 October 2005.
4. Copy Detection Patterns, http://www.mediasec.com.
5. 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.