Variable Data Security Printing and the "Layered" Deterrent

Steven Simske, Hewlett-Packard, Fort Collins, Colorado, USA; Roberto Falcon, Hewlett-Packard, Palo Alto, California, USA

Abstract

Printed documents and packages, even for high value goods like pharmaceuticals, are generally susceptible to counterfeiting. This is due in part to the use of "static" elements for most of the printed elements. Even when "variable" data features—such as bar codes, lot numbers, and expiry dates—are used, they are typically identical for pallets or larger lot sizes. This aids the would-be counterfeiter. With variable data printing (VDP) technology, every printed element on a package is, potentially, part of a multi-feature authenticating design. VDP, in combination with liquid electrophotographic (LEP) technologies, provides an opportunity to change the nature of security printing. VDP provides precision control over the individual dots, while LEP technology provides precision registration of more than a dozen layers of ink. This allows a novel "layered" deterrent, with an innately shifting deterrence strategy, to be created using variable print strategies on each of the multiple layers. This shifts the need for specialized printing techniques to the need to accommodate variable ink approaches. In our talk, we will overview the astonishing variability that can be provided in a single, modestly-sized security print feature through the use of infrared/ultraviolet fluorescent inks, infrared opaque and transparent black inks, inks containing taggants, magnetic ink, and inks with differential adhesive properties to enable sandwich printing. This variability provides covert and forensic protection to complement the overt protection of such known techniques as guilloche and microtext. Finally, when overprinting (metallic inks, lenticular printing, etc.) is considered, an extraordinary number of possible encryptions are available on very little package "real estate". We consider the permutations available in our presentation.

Introduction

Variable data printing (VDP) can be readily incorporated into existing industrial lines in which marking, or printing, occurs (such as packaging lines) allows every printed region to become a potential means for track and trace and/or authentication. Since printing—on the packaging if not part of the product itself—is required for nearly all branded products, it can be argued that *not using VDP* is an oversight in the reality of a counterfeit market that equals 10% of world trade.[1] Such oversights leave the brand owners of products such as pharmaceuticals, foodstuffs, transportation vehicles, etc., liable for the potentially lethal consequences of counterfeiting.

We introduce herein the concept of a "layered deterrent". This is a printed deterrent than contains two or more layers of information in a single printed area. We begin with a discussion of the concept of layered printing, then discuss a simple layered security printing feature that takes advantage of the liquid electrophotographic (LEP) digital press technologies underlying layered printing. We then discuss the use of inks, links and finishing to provide additional complexity to layered deterrents, before summing up our findings. In this last section, we provide metrics for comparing among different security printing features.

Layered Printing

Layered printing is possible with any multi-pass printing process, whether this involves the use of multiple layers of inks or finishing processes (e.g. lamination, lacquering, glossing). On the HP Indigo digital press,[2] sandwich printing[3] is used for a variety of applications, one of which (peel-off label) is shown in Figure 1.

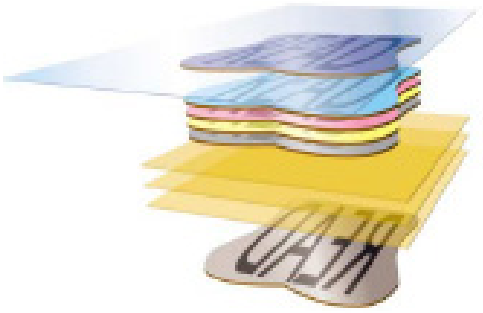

Figure 1.The use of sandwich printing on the HP Indigo Press for creating a peel-off label. A CMYK print can be seen through the transparent substrate (light layer, top), while three spot color layers (the minimum number of layers to create an opaque barrier) are used to hide the underlying message (in black spot color) until the substrate is peeled off.

Sandwich printing is possible due to the HP Indigo industrial press' ability to print as many as 16 layers of ink on a substrate in a single pass (or "shot") with perfect registration. The "sandwich" refers to the "front" design, the "back" design, and the opaque layer (the "cheese" of the sandwich) between them. When a transparent substrate is used for this layered design, there are two images created, each one visible from one side of the substrate. The opaque layer separates these two images.

The layers of (usually white) ink between the ink layers for the two images serve two purposes: they provide the side that is currently viewed with a white underground and they hide the layer (against the substrate) that is behind. While the HP LEP ink (ElectroInk) is not opaque, it has roughly the transparency of an intentionally transparent screen printing ink. Thus, for it to block light between the two images in the layers of the sandwich, it must be applied in multiple layers. This is achieved through providing a separation in the print job for the opaque ink (usually white ink). In the "Job" properties, all that need be done is multi-hit the separation. The ideal number of hits, or layers, for white ink to provide sufficient opacity is three or four. The difference between three and four hits of white is slight, and the visual difference (as well as the opacity difference) between four and five hits is negligible.

Color Tiles and Microtext

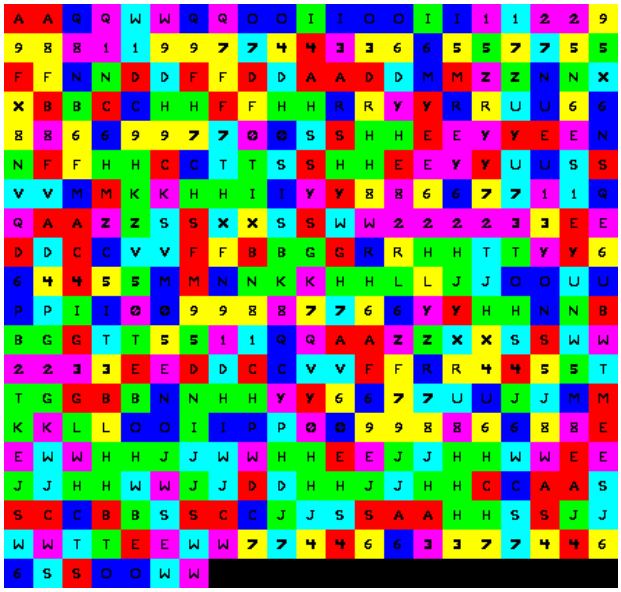

Figure 2. Simple layered deterrent example. There are two primary features in this deterrent: a 7x7 pixel (219 x 219 microns) font printed in a black spot color; and a set of color tiles that in this example are linked to the microtext via a direct 6-color, 2-tile mapping to the 10 digits and 26 English language capital letters.

Microtext is a frequently-adopted security printing technique, used for example on currency and checks. Using the HP Indigo press, microtext is variable and can be printed with unique information on each printed item. Microtext is printed on the Indigo presses using a spot color, and so can be the last layer registered over a color pattern below it. In Figure 2, we show a layered feature whereby the lower layers are the color tiles (printed at 21 x 21 pixels, or 1498 tiles/square inch), and the upper layers are the microtext. There are many ways to relate the microtext characters to the color tile; in Figure 2 we have simple mapping of two consecutive tiles (in CMYRGB colors) to the 26 English capital letters and the ten digits. For example, two consecutive R(ed) tiles indicate the "A" character that is printed over them. We discuss more methods to relate the microtext to the color tiles below.

Inks as Layers

The ability to print up to 16 layers of ink in one "shot" on the Indigo enables other ink-based layering possibilities.[3] One such possibility is to print what appears to be a static deterrent out of two black inks, one of which is opaque to infrared light, and the other of which is transparent to infrared light, such as Anoto black ink[4] (Figure 3).

Figure 3 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 are used to simply choose where on a specific target to print each of the two inks—thus, for example, 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 4).

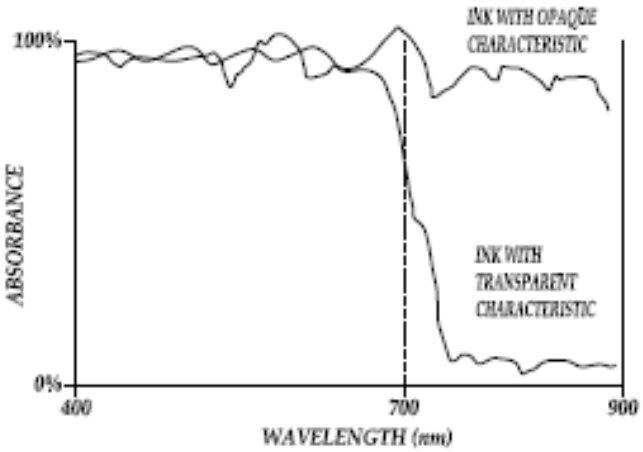

Figure 3. Idealized representation of process black ("Ink with Opaque Characteristic") and infrared transparent

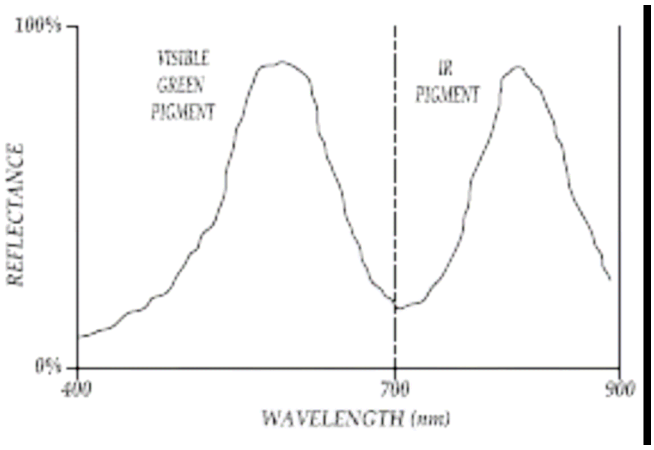

Figure 4. Sample ink with both green and infrared absorbance characteristics.

Given ink combinations such as these, a number of possible deterrent strategies are evident. One is to simply vary the sections of an ostensibly static target (such as a bar code) that are printed in process black or "infrared transparent" black. Another is to simultaneously vary the infrared patterns, creating variability in both the upper and lower layers. In addition , the emission frequency of the infrared ink can be varied. With these strategies in place, a security print target covering only 0.25 square inches of area can provide more than 10^{1000} different permutations. A unique identifier for each unit can be provided with essentially no chance of counterfeiting or spoofing, and no repeated identifiers. Because the two black inks appear identical to the human eye, an apparently static pattern, such as an SKU-specific bar code, can be used to create enough variability for product authentication.

In addition to this approach, the use of inks offers the possibility to differentiate brand while simultaneously raising the bar for counterfeiters. Because Pantone certified ElectroInk spot colors can be mixed on-location, brand owners can target hard-to-reproduce color combinations, forcing the counterfeiter into

printing (away from copying). An example of a color line security print feature is shown in Figure 5.

Figure 5. Color line security printing feature.

Additionally, the inks themselves offer forensic protection from counterfeiting. From the incorporation of DNA/RNA taggants to the use of tightly controlled pigment mixtures, inks are essentially "secret formulas" that allow investigators to prove when counterfeiting has occurred. Moreover, inks are an excellent place to plant "decoys"—untracked and print quality unaffecting ingredients to keep the counterfeiters guessing.

Links Between Layers

One of the most powerful methods for providing security in printing is to have associations between printed layers. These links can be explicit (overt linking) or obfuscated, e.g. by encryption (covert linking). However, this linking can turn otherwise low-security features into powerful anti-counterfeiting features. Consider four simple features that each provide 8 bits of information (256 possible instantiations). Linking the four together, however, provides 32 bits of information, increasing the number of instantiations to more than 4×10^9. This is difficult for a would-be counterfeiter to spoof, but offers pragmatic ease of recall, stocking, and track and trace by simply using one of the four features for routine product identification.

Returning to the color tiles/microtext combination described above, the possibilities for linking between these two security features is astronomical. Among the elements that can be varied are:

1. The number of characters (set size) in the microtext font
2. The number of tiles used to encode the font (as well as the choice of whether to let the two features vary independently to create a higher overall number of possible sequences in the combination)
3. The number and types of colors to use in the tiles
4. The possible use of infrared transparent black for some of the microtext, and the possible overprinting of ultra-violet and/or infrared inks on the tiles

It is clear that the more independent features that are linked, the greater protection can be offered by a single feature.

A different type of linking can be garnered through the use of the color line feature shown in Figure 5. Here, a set of variable colored lines can be used to improve security during shelving of the products while simultaneously linking the end units all the way back to their pallets. Shelving can be aided by "islands of stasis" within a variable feature. That is, for a given lot, a certain set of the color lines will be static (for example, lines 6-8 are always green, yellow and cyan for a given lot). This allows a shelf stocker to instantly determine that the packages are in the same lot as they are being shelved.

Next, a large set of color lines can be used on the pallet and carton packages, and a smaller subset printed on the individual packages or end units. In the case of pills, a small length of color lines can be printed directly on the tablet. A cue (such as the number in the longer line to align the shorter line with) can be used to verify that the end unit belongs with the larger carton or pallet.

Finishing as a Source of Layers

After primary printing has occurred, finishing techniques can be used to extend the security and/or further raise the bar for would-be counterfeiters. Inexpensive techniques like metallic ink printing and lenticular printing can be used to provide high-end overt security, while the incorporation of nanotaggants (DNA and RNA strands, for example) in the lacquer, gloss, or other finishing material. If precision allows, finishing can also be used to differentially inactivate parts of the printed material (e.g. through cutting, laser ablation, etc.). This adds the type of variability that counterfeiters are likely to miss (or even correct—such as the commonplace "correcting" of intentionally misspelled words on packages).

Discussion

Security printing is often viewed as an arcane field because there are few guidelines, comparative studies, or explanations of overall strategies for providing counterfeiting protection. However, in considering the layered approach outlined here, there are some possible pathways toward a quantitative approach to security printing.

First, security printing features can be characterized by their "numeric density"; that is, by the number of unique identifiers (usually but not always sequences of bits) per given area. This allows the user of a variable data printing campaign the possibility to choose which features to incorporate in the campaign based on available printing real estate, in addition to the printing technologies, inks, finishing technologies, etc.

Numeric density needs to be reported based on individual layers and on the combined set of layers, since the different layers may be used for different types of security (overt, covert and/or forensic). Suppose, for example, there are three layers, offering 10^{50}, 10^{10} and 10^{20} different permutations, respectively, in a 1 square cm feature. Suppose the first layer offers overt and forensic protection, the other two layers covert protection. Then the overall feature provides 10^{50} permutations of overt, 10^{30} of covert and 10^{50} of forensic protection.

Alternatively, a security printing feature can be qualified by the size it must be to provide a certain numeric range. Suppose, for example, that the feature above needs to provide 10^{50} unique identifiers of covert and overt protection. The feature above thus needs to be 1.67 cm^2 or more to provide the requisite protection.

Conclusion

Variable data printing, combined with the ability of LEP printing to provide 16 layers of registered ink, affords a plethora of security options. The combination of color, ink, finishing and multi-layered linking allows the security printing provider, moreover, to fabricate a digital solution to anti-counterfeiting with the same

technology used to provide branding, product information and product identification.

References

1. "The Extent of Counterfeiting", http://www.a-cg.com/info.html.
2. HP Indigo Digital Printing Presses, http://h30011.www3.hp.com/.
3. Steven Simske, Philippe Mücher, and Carlos Martinez, "Using Variable Data Security Printing to Provide Customized Package Protection", Proc. DPP 2005, pp. 112-113.
4. Anoto substitute black ink, SunChemical AB, P.O. Box 70, Bromstensvagen 152, SE-163 91 SPANGA Sweden.

Author Biography

Steven Simske (Steven.Simske@hp.com) is a senior researcher at Hewlett-Packard Labs in Fort Collins, Colorado, USA. He is the technology lead for HP Labs in security printing. Steven has worked in medical imaging, image analysis and recognition, and content understanding for the past 20 years. He is a senior research associate in Aerospace Engineering at the University of Colorado, and an adjunct professor in Physics at the Colorado School of Mines. Steven is a member of IEEE, ACM, W3C and IBMS.