Extended Packaging through Addition of Readable Information to the Printing

Steven J. Simske, Margaret; Sturgill

HP Laboratories
HPL-2009-316

Keyword(s):
layout, VDP, printing, packaging, mobile camera

Abstract:

Packaging is the interface between your product and your customer. To enhance the customer experience, the packaging should provide brand identification and allow the user to readily obtain information that is customized to their interests. Variable data printing (VDP) provides the label converter with the tools to highlight important brand and product related information, either directly or through interpretation of tacitly designed marks on the label. If branding concerns preclude the implementation of specific information-bearing marks (e.g. barcodes and/or security deterrents), the branding information itself can be made variable without impacting the perceived aesthetics of the package design. This is possible because VDP allows each label's layout - not just content - to be unique. Several layout variances can be added to the packaging in a semi-covert manner; that is, they are not noticed until they are known to be present. These include variances in the size, x- or y-position, metameric pairs, placement over the background, and rotation of non-rectangular elements. The VDP layout differences from a template encode information. Variability humans are particular sensitive to - text kerning, misalignment, absolute color differences - are poor candidates for the layout VDP. Our work illustrates how to put in place an overall VDP layout system.

External Posting Date: September 21, 2009 [Fulltext] Approved for External Publication
Internal Posting Date: September 21, 2009 [Fulltext]

© Copyright 2009 Hewlett-Packard Development Company, L.P.

Extended Packaging through Addition of Readable Information to the Printing

Steven J Simske, Margaret Sturgill; Hewlett-Packard Labs; Fort Collins, CO, USA

Abstract

Packaging is the interface between your product and your customer. To enhance the customer experience, the packaging should provide brand identification and allow the user to readily obtain information that is customized to their interests. Variable data printing (VDP) provides the label converter with the tools to highlight important brand and product related information, either directly or through interpretation of tacitly designed marks on the label. If branding concerns preclude the implementation of specific information-bearing marks (e.g. barcodes and/or security deterrents), the branding information itself can be made variable without impacting the perceived aesthetics of the package design. This is possible because VDP allows each label's layout—not just content—to be unique. Several layout variances can be added to the packaging in a semi-covert manner; that is, they are not noticed until they are known to be present. These include variances in the size, x- or y-position, metameric pairs, placement over the background, and rotation of non-rectangular elements. The VDP layout differences from a template encode information. Variability humans are particular sensitive to—text kerning, misalignment, absolute color differences—are poor candidates for the layout VDP. Our work illustrates how to put in place an overall VDP layout system.

Introduction

Package printing, including label printing, is an important part of the aesthetics and appeal of a product. The package printer has many options among substrates, inks and finishing, along with the choice of the printing technology. In many cases, the printing on the package is the main link between the product and the customer. It conveys the brand, the product information, and often pricing and promotional information. Although marketing collateral and retail displays complement the role of packaging and labels in customer/product interaction, differentiating the packaging may be the readiest opportunity available for incremental branding of products. Additionally, packaging can be used to extend customer/brand interaction to the increasingly mobile world. Packaging can also be integrated into the overall product security strategy.

The majority of package printing is non-variable, or static in nature. While this is cost-efficient and supports large print runs for popular products, it can also result in inventory overstock and waste. Using variable data printing (VDP), customized short runs and just-in-time printing are enabled. VDP leads to reduced inventory, often improved sustainability, and an "adaptable" brand/customer interface. Time from printing to point-of-sale is reduced, and the brand owner can more readily adapt to changing conditions in the supply chain.

Figure 1 provides an example of VDP applied to a simple package label. The upper image is the static (non-variable) part of the label, designated the template, and the information conveyed by the image include the lot number, expiration date, brand name and logo, product information, country (and place) of origin, and other product-specific information—in this case, dosage, storage requirements, SKU-specific barcode, and other information. The lower image shows the template after it has been filled in with variable data elements. In this instance, the variable elements are used for security, as discussed next.

Figure 1*.Label template (top) and label template with variable copy holes filled with explicit security and point of sale marks (bottom).*

VDP for Branding and Security

In addition to sales and marketing related brand differentiation, VDP can be used for brand protection, security and product anti-counterfeiting. Security "deterrents" [1] are printed areas, overt and/or covert, that contain authenticable data ("payload" information). Deterrents compete with branding, sales and other product information for printed "real estate", so it is advantageous for the deterrent to provide, where possible, multiple levels of protection and functionality simultaneously. The deterrence is ideally integrated into the printing process in such a way that the branding, product information, etc., contains a payload that is "hidden in plain sight", or semi-covert. An example of an explicit security deterrent is shown in Figure 2. Explicit security deterrents are "known" to contain information that can be read. A 2D bar code is a simple example of such a data-containing element, as is a color tile deterrent and microtext—all visible as part of Figure 2.

***Figure 2**. Example of an explicit security deterrent.*

Printing that has as its primary function a non-security role, but can contain a (steganographic) payload, is termed "security pre-adapted" printing. Packaging is security pre-adapted, as various aspects of the printing can be variable, and so contain "readable data". At the lowest level, this data is encoded in the printing primitives—the very dots printed. At the highest level, this data is encoded in the layout

Layout Variability Methods

Using layout variability, data is added through a means not associated with the printed elements themselves, but rather the relative position of these elements. Described herein is a simple means to automatically add and verify information added to the layout.

Certain layout parameters can be varied without harming the brand identification, brand differentiation, product identification, product safety, or other intents of the printing. This variance is then quantified from a digitally captured image of the printed region, and from this the steganographic payload is extracted and authenticated. Therefore, the physical layout of a label, packaging, etc., is used to add security information. This information is data in the form that can be inspected, authenticated or otherwise "read".

A layout-based security system for packaging involves a training and a deployment phase, as described here.

Training: During training, we obtain a layout template for the printed region to which we wish to add the security information. This layout template is usually provided by a brand owner, label converter, etc. and as such specifies the size, shape, colors, location, fonts, and variable copy holes of a "printed region".

Next, we are given the constraints for any of the layout-variations, as listed here, we may wish to perform.

1. Size
2. x-positional spacing
3. y-positional spacing
4. Background centering
5. Rotation (generally applicable to non-rectangular regions only)
6. Metamerisms

Constraints can come from a variety of sources, including branding, aesthetics, variation within variable "copy holes" precluding accurate measurement, etc.

Given the set of regions (static and variable "copy holes") we can alter their absolute and relative positions, using either the largest region or an explicit fiducial (often a "+") as an anchor, and then vary the positions of non-constrained elements accordingly. For example, Figure 1 above shows an original label template (top) and then a label with three variable data explicit security deterrents added (bottom). In this label, we are free to vary several elements relative to one another without disturbing the branding message and without creating an aesthetic dilemma. For example, all three of the explicit security deterrents added (note the lowermost one is actually a set of four parallel line patterns, and so constitutes one "element") may be scaled slightly differently and located with x- and y-positional variance without offending the branding message, or becoming unreadable and/or creating visual dissonance.

Other elements can also be varied in position, size and centering over background. For example, the jelly bean image can be moved relatively in the x- and y- directions and scaled by <5% without changing the visual appeal greatly. The "10 mg" can be differently background centered. The blue line segment in the center right can be moved relative and/or with the two lines of text above/below it. Many other options from the list above are possible on this relatively complex label.

Next, for training, we vary each of the variable layout elements and then print and scan to see which of those we can reliably detect, or "read", with the devices—such as mobile cameras—that will be used to read the packaging by the customers. The number of bits that survive a print-scan (PS) cycle are considered "robust" and so suitable for encoding security information [2]. For example, if, within the constraints of aesthetics (usually set by the brand owner), we can vary the relative x-offset of "10 mg" from 30-60 pixels right of the left edge of the blue background, and our image capture devices can distinguish differences of 2 pixels or more, then we can encode data as 30, 32, 34, …, 60 pixels from the left edge. This gives us 16 different possible locations, which is 4 bits of information.

In a similar fashion, each allowable variation is printed and digitally captured, and then the total number of bits computed. This final training process is referred to as the "sensitivity analysis". In

our testing to date, we have been able to add 20-60 bits to a typical label using phone cameras for image capture. The label shown in Figure 1 has 96 bits (sufficient for EPC global use) added.

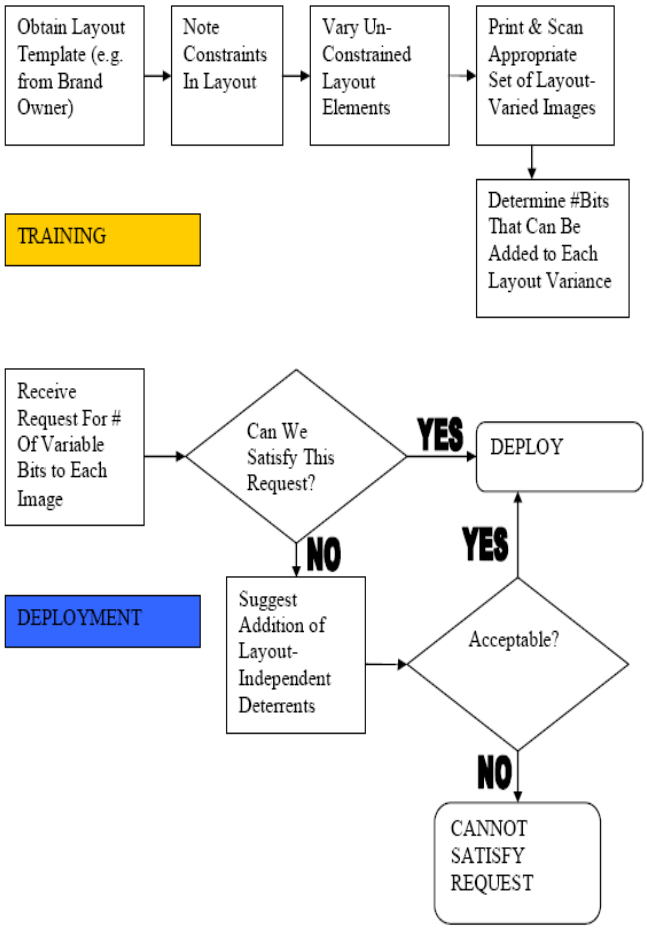

***Figure 3**.Block diagram of the system (training at top, deployment at bottom).*

Deployment: After the sensitivity analysis is performed, a deployment recommendation is made (and as necessary reviewed with the brand owner). Thence, the number of total bits that can be accommodated is encoded into the layout variations actually made. For example, if the relative location of "10 mg" as above is encoded as 0000 when at 30, 0001 when at 32, …, 1111 when at 60, then if the security bit stream (to be mass serialized, etc.) corresponding to this layout variation is 0101, for example, we place "10 mg" at 40 pixels from the left boundary of the blue background. Of course, this data can be encrypted or scrambled first, in keeping with the characteristics and deployment realities of security printing.

The block diagram of the system (Figure 3) addresses where the rest of the required security bit stream comes, if necessary. Suppose the layout variation for Figure 1 can accommodate 96 bits with brand owner acceptance. Then, if our overall security needs are 320 bits, say, we need to ensure that the remaining 224 bits can be accommodated by the explicit security deterrents such as the one shown in Figure 2.

Conclusions

Current security printing approaches focus on the information in variable-data instruments (regions with "payloads", or embedded information). More sophisticated approaches include layering (multiple levels and/or modalities of payloads in the same location). Here, we make the relative layout of the information variable, and since the manifestation of this approach is visible, it is straightforward to see the information embedded, once the method of encoding is made available. This approach also allows security information to be captured at low resolution and with poor image quality, lighting conditions, etc.

The approach described also provides ease of inspection. Since many of the differences are easy to see/verify (once you know what they are and where they are!), they can be used as part of an inspection program, e.g. by field inspectors. Since we can impose specific constraints into the variable layout (albeit at some cost of bit stream density), we can make the inspection of the varying layout images easier.

Layout variance tends to be on a massive scale—i.e. by lot or SKU—and so can accommodate large runs as well as short runs. The methods described here, while suitable to the inclusion of security information, are applicable to the printing of any readable information, and thus can underpin applications from mobile commerce to product recall.

Acknowledgements

We gratefully acknowledge our numerous security printing colleagues who have participated in research in this area. Specifically, we thank Jorge Badillo and Juan Carlos Villa for work on label templates.

References

[1] S. J. Simske, J. S. Aronoff, M. M. Sturgill, and G. Golodetz, "Security Printing Deterrents: A Comparison of Thermal Ink Jet, Dry Electrophotographic, and Liquid Electrophotographic Printing," Jour. Imaging. Sci. and Technol., 52(5), pg. 50201 (2008).

[2] S.J. Simske, M. Sturgill, and J.S. Aronoff, "Effect of Copying and Restoration on Color Barcode Payload Density," *Submitted to* ACM DocEng 2009.

Author Biography

Steven Simske is a distinguished technologist and the director for security printing and imaging in Hewlett-Packard laboratories. He has worked in a wide range of image processing, signal processing, content understanding, medical imaging and biometric technologies for the past 2 decades. Steve holds 29 US patents, and is a member of IEEE, ACM, IST and SPIE.