New Findings in Security Printing and Imaging

Steven Simske[1], Guy Adams[2], Jason Aronoff[1] and Margaret Sturgill[1], Hewlett-Packard Labs; Fort Collins, CO, USA[1] and Bristol, UK[2]

Abstract

In the past three NIP conferences, we have presented novel techniques for embedding security information into the variable data printing (VDP) for labels, documents and packaging. Recently, we have discovered that fundamental assumptions in other fields—error correcting code (ECC), classification and the use of color, for three examples—are not necessarily valid when functional security is the goal of the printing. It will be shown herein that the assumptions behind default ECC do not hold for 2D or color 2D barcodes with mobile image capture. Alternatives to ECC are suggested. When security-related tasks are the end goals of the printing and imaging, the deployment optimization for image classification is fundamentally altered. Tuning the classification engine to the security aim, rather than the image features as in traditional classification, provides significant improvement in both image throughput and classification accuracy for security-related tasks—such as inspection, authentication and forensic imaging. It will, finally, be shown that there are significant new security approaches either only possible or else greatly enhanced by the printing of color, rather than grayscale or binary, images. These broad results indicate that applied research in security printing requires new basic research in the related image processing fields.

Error Correcting Code

Mobile image capture devices are ubiquitous, with increasing ability of consumers, retailers, supply chain managers and manufacturers [1-4] to interrogate products [1,2], labels [1-3], and even signage [4]. Many barcode implementations, however, rely on error-correcting code (ECC), to add robustness to the barcode reading process. The robustness model, however, historically derives from the printing of 1D barcodes; mailing applications; environmental damage associated with smeared ink on low-quality paper; and abrasion or puncture damage.

For the reading of barcodes with cameras on mobile devices, localized damage is arguably a less important consideration than overall low image quality during capture. Poor or nonuniform illumination, blur due to poor focus and/or motion, and poor quality printing can cause low quality capture. And ECC is not necessarily designed to overcome these distortions. It has been argued that the selection of ECC, based on communication theory, is a largely misplaced focus, particularly for defects introduced in the process of printing or of scanning [5]. The same reference argues for "finessing the size of the spots and cells [to] minimize the effects of printing defects", and continues "by increasing the size of the data features…virtually any anticipated problem in these domains can be compensated for, so that information can be perfectly communicated" [5]. In this paper, a wide range of values for Error Correction by Percentage of Symbol Area (ECPSA) are compared to uncorrected barcodes with the same density of bits per unit area. Separately, print-scan (PS), low quality printing and blurring conditions are used to provide test cases for ECC/non-ECC comparisons.

A series of barcode readability tests were performed using Aztec symbology high-capacity 2D matrix barcodes. Aztec is able to encode both ASCII and Extended ASCII characters, and when using its full range mode of 151 modules and with 25% ECPSA, Aztec is able to encode up to 3000 characters or 3750 numeric digits (that is, its size ranges between 15 X 15 modules and 177 x 177 modules). All experiments were performed using a 27 x 27 module configuration, so that comparisons between images with the same module size were not affected by overall barcode size. For every test, module size was varied from 8 to 30 mils in 1 mil increments (1 mil = 10^{-3} in). Each module is either black or white. BCoder© Professional software (TAL Technologies, Inc., Version 4.0) allows the varying of ECPSA and payload (this is why Aztec symbology was chosen). Through iterative adjustment of these settings, we were able to obtain 27 x 27 module Aztec barcodes with 0%, 10%, 20%, 30%, 40%, and 50% ECPSA settings (Table 1). The number of payload modules (or "bits"), M_P, was equal to 648, 584, 520, 456, 392, and 328, respectively, for these ECPSA settings, so that the number of ECPSA, or non-payload modules, M_{NP}, was equal to 0, 64, 128, 192, 256 and 320 bits, respectively.

For all of the following tests, the barcodes were read using an InData Systems™ 9500LDS portable terminal with add-on optic "shroud" for 405-nm LED (light-emitting diode) Light Delivery System (LDS-V2), hereafter "IDS-LDS". This system provides uniform lighting conditions (405 nm illumination) for all barcode reading performed (so that we are sure consistent illumination was used throughout the experiments). Multiple pages (20 or more barcodes at each of the 23 module sizes) were printed under the following experimental conditions:

Fig. 1. Example of original and damaged Aztec Code 2D barcodes (ch=648 indicates maximum bits to use for encoding characters). Original size was 20 x 20 mils per module. Payload is 456 out of 648 payload bits (30% ECPSA). Images show no damage (left), 12.5% damage (center) and 25% damage (right).

(1) Print using an HP 3600 Color LaserJet (hereafter "CLJ") with grayscale-only settings.

(2) Print using the CLJ, scan and print twice using the HP 6280 inkjet all-in-one (hereafter "IJ-AIO"). This degrades the barcodes printed in (1) by two print-scan (PS) cycles, and constituted the PS-channel distortion experiment.

(3) Add damage through filling in of all white modules in increments of 1/8 of the overall payload area of the barcode, as shown in Fig. 1. This constituted the destructive damage (DD) distortion experiment.

The results for the CLJ and PS-channel distortion are shown in Table 1. Printing with the CLJ resulted in relatively high values for PD—above 1700 bytes/in^2 for 0% and 10% ECPSA. Increasing ECPSA dropped PD by a mean of nearly 20 bytes/in^2 for every 1% increase in ECPSA. After two PS cycles, the PD dropped by a mean of nearly 260 bytes/in^2. The PS distortion resulted in a more uniform drop in PD of approximately 15 bytes/in^2 for every 1% increase in ECPSA.

The Destructive Damage (DD) distortion test (Table 2) shows that reading time increases significantly with the amount of DD added. The effect of PS distortion is evident in the 50% ECPSA samples in particular, for which 37.5% DD is unreadable. This implies CLJ+PS distortion effectively removes at least ¼ of the ECPSA added; that is, at least 12.5% ECPSA is required to overcome CLJ+PS distortion. The data for 40% ECPSA, however, in which barcodes with 25% DD can still be read, implies that the CLJ+PS distortion does not exceed the equivalent of 15% ECPSA.

Target ECC (as ECPSA)	CLJ Original	CLJ + PS Distortion
0% ECPSA	1730)	8.8 (1610)
10% ECPSA	1760)	8.8 (1450)
20% ECPSA	1570)	9.1 (1210)
30% ECPSA	1370)	9.1 (1060)
40% ECPSA	1180)	9.2 (890)
50% ECPSA	990)	8.7 (840)

Table 1. Payload Density (PD) in bytes/in^2 for the original CLJ printing, and PS-distortion.

Module size (% damage)	30%	40%	50%	75%
12 mils (0%)	176	215	216	218
12 mils (12.5%)	605	862	676	230
12 mils (25%)	--	1356	680	489
12 mils (37.5%)	--	--	--	870
15 mils (0%)	126	145	114	165
15 mils (12.5%)	433	123	255	270
15 mils (25%)	--	167	297	281
15 mils (37.5%)	--	--	--	1358

Table 2. Time (mean of 10 or more successful barcode reads using the IDS-LDS, in msec) for 12 and 15 mil module Aztec 2D barcodes with ECPSA=30%, 40%, 50% and 75%. Damage is induced as shown in Fig. 1 to CLJ+PS distortion samples.

Classification

Many printed materials cannot accommodate security deterrents due to space (e.g. labels and medallions) or formatting (e.g. corporate/branded documents) concerns. As a consequence, we are interested in supporting, in some applications, a deterrent-free approach. This approach is based on different image quality or printing characteristics, which allows counterfeits based on copying and/or other facsimiles of the original image to be distinguished from the authentic original images using image classification techniques.

As mobile camera imaging capabilities continue to increase, this becomes feasible for more and more capture devices. Mobile and distributed image-based applications are often bandwidth-limited, however, and so can benefit from reducing the size of the image transmitted. Image size can be reduced in several (non-reversible) ways, including down-sampling (reducing the physical dimensions of the image through resampling) and lossy compression (reducing the information in the image without reducing its physical dimensions). Determining the optimum image size should be based, if possible, on a quantitative evaluation of the image after transmission. We considered 162 different resampling/jpeg compression combinations on 5 different sets of images which are to be used for comparing authentic and counterfeit products. Quantitative evaluation of the image transformation is measured by success in correctly classifying "authentic" and "counterfeit" images. All image transformations that maintain original image classification accuracy are accepted. We represent the overall increase in imaging bandwidth as $@\mathbf{A_{TF}}$, or at-accuracy throughput factor. This metric is the relative number of reduce-sized images (compared to the originals at 600 dpi) that can be successfully classified without reduced accuracy using the same transmission resources. For 4 of the 5 image classes, $@\mathbf{A_{TF}}$ was substantial (from 176 – 1.24 x 10^4). For barcodes, $@\mathbf{A_{TF}}$ was 1, meaning only the original images afforded high classification accuracy. These were also the only non-color images, implying that color printing is advantageous to this area of brand protection.

The Use of Color

The interesting results for ECC provided above notwithstanding, printing in color provides significant advantages for security printing. For the classification of counterfeit samples, as described above, color images are more robust to compression without loss of accuracy. Color barcodes, often termed 3D barcodes, also offer the possibility of higher density and multi-level embedded information. Color barcodes encode $\ln(N_C)/\ln(2)$ bits per tile, where N_C is the number of colors. For a 6-color barcode, then, there are 2.6 bits/tile. This surfeit of data can be used to increase payload density (PD) or provide other forms of security—for example, watermarking and copy deterrence—without compromising the tile bit stream.

Recently [8], we completed an overview of the effects of copying, spectral pre-compensation, differing authentication approaches, and image restoration prior to authentication. This research showed that copying (PS cycle) produces a consistent reduction of PD by approximately 55% under all tested conditions. Spectral pre-compensation (SPC) positively impacts PD in 12 out of 12 comparisons, though with higher variance than the PS cycle effects. SPC nearly doubled the payload density, while selecting the better authentication algorithm had half the impact of SPC in the mean—increasing PD by roughly 50% in the mean. Restoration, however, was found to increase payload density less substantially (~30%), and only when combined with the optimized settings for SPC. Interestingly, the highest PD reported in these experiments was 2210 bytes/in^2 for original (non-copied) images undergoing SPC, hue-based authentication (Hue) and saturation equalization (SE)

image restoration. It is worth noting that its non-SPC, non-Hue, non-SE counterpart (1090 bytes/in^2) has 51% less PD—a percentage comparable to an entire PS cycle. Thus, advanced printing and imaging optimizations such as combined SPC+Hue+SE can effectively "remove" an entire PS cycle. The implications of these findings are that advanced printing and imaging techniques should be deployed for security-related color barcodes. Otherwise, would-be counterfeiters are effectively given a "free pass" of one copy.

Discussion and Conclusions

2D Bar Codes: For the CLJ barcode experiment, peak PD was obtained for the 0% and 10% ECPSA barcodes. Increasing ECPSA above 10% resulted in significantly decreasing payload density. At 50% ECPSA, PD was reduced 42.8%, implying that 85.6% of the ECC added was "wasted", or at least inappropriate to the CLJ printing distortion.

When PS distortion is added to the CLJ experiment, the best results are obtained when ECC is not employed. PS distortion results in a significant decrease in PD at any setting for ECPSA; however, the 0% ECPSA barcodes suffered the least deleterious effects due to PS distortion. At 50% ECPSA, PD was reduced 47.8%, implying that 95.6% of the ECC added was inappropriate to the CLJ+PS distortion.

The addition of destructive damage (DD) distortion implies that CLJ printing + PS distortion "equals" in some sense the equivalent of between 12.5-15% ECPSA. This implies that an effective ECPSA must be at least 12.5% (note that the Aztec default ECC is approximately 23%). However, at every ECPSA above 12.5% tested herein, excepting the IJ-AIO RPQ 20% ECPSA, the significantly reduced PD contraindicated the deployment of ECC. ECC also results in increased decoding time for damaged barcodes (Table 2), which may be significant for human-to-device interaction. The results of these experiments imply that under print-scan (PS) channel distortion, ECC is contraindicated for Aztec (and related 2D) barcodes.

Classification: The results for classification are at first counterintuitive: smaller images actually classify with higher overall accuracy than the originals. This may be a consequence of the classifier used. The classifier selected [6] is designed to work best with Gaussian data, and the down-sampling operation—as well as many of the Jpeg compression settings utilized, in which considerable loss of frequency information is obvious when viewing—is an averaging operation. The image metrics of the down-sampled and/or Jpeg compressed images, therefore, are likely more Gaussian than the metrics of the original images. More on this work is available on-line [7].

Color Tiles: Color tiles have gained much attention of late for their use in security, branding, and mobile customer applications. The techniques described in our paper can be used to increase the effective payload density (PD) of color tile deterrent. The resulting improved PD matches or exceeds the PD of other barcode types and barcode research efforts. Table IX of reference [9], for example, cites the following bar code PD in bytes/in^2: Data Matrix, 1555; Aztec Code, 1888; QR Code, 1941; Multilevel 2D Bar Code (p_1 - s_1), 2211; and Multilevel 2D Bar Code (p_5 - s_1), 2397. The latter two are similar to the highest density of 2210 bytes/in^2 achieved for the "Orig+SPC+Hue+SE" case as presented here.

Other applications of color in security printing and imaging not provided by grayscale deterrents include ambiguous bit encoding (possible through the use of, for example, simultaneous blue-yellow, magenta-green and red-cyan color opponency pairs); scaled deterrents (in which 1x1, 2x2, 3x3, etc. aggregations of tiles provide different levels of authentication); and the replacement of error correction code (ECC) with calibrating non-payload indicia (NPI), affording higher PD. For example, the color bar code deterrent described in [8] uses 8% of the tiles as color calibration. These NPI effectively comprised an error-correcting code (ECC) of 8%, substantially lower than the usual ECC percentage of 25-50%.

Conclusions: Security printing is the set of technologies required to embed recoverable data in printed material. In this paper, we have focused on new results for three different types of overt printed information—2D barcodes, counterfeit detection through image classification, and color (or "3D") barcodes.

References

[1] http://www.gs1.org/productssolutions/mobile/.

[2] http://www.epcglobalinc.org/home.

[3] http://www.microsoft.com/tag/content/overview/.

[4] http://www.openmobilealliance.org/.

[5] Paperdisk, http://www.paperdisk.com/ibippap2.htm.

[6] S.J. Simske, "Low-resolution Photo/Drawing Classification: Metrics, Method and Archiving Optimization," *Proc. IEEE ICIP*, IEEE, Genoa, Italy, pp. 534-537, 2005.

[7] S.J. Simske, M. Sturgill, and J.S. Aronoff, "Comparison of Image-Based Functional Monitoring through Resampling and Compression," HP Labs Technical Report HPL-2009-145, http://www.hpl.hp.com/techreports/2009/HPL-2009-145.html.

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

[9] Villán, R., Voloshynovskiy, S., Koval, O., and Pun, T. 2006. Multilevel 2D bar codes: towards high capacity storage modules for multimedia security and management. IEEE Transactions on Information Forensics and Security, 1(4):405-420, 2006.

Author Biography

Steven Simske is a distinguished technologist and the director for security printing and imaging in Hewlett-Packard laboratories. His research focus is image and signal processing, security printing, medical imaging and biometric technologies. Steve holds 30 US patents, and is the author of more than 200 publications.