Security Printing Deterrents: A Comparison of TIJ, DEP and LEP Printing

Steven J. Simske, Jason S. Aronoff, Margaret Sturgill; Hewlett-Packard; Fort Collins, CO, USA and Galia Golodetz; Hewlett-Packard; Rehovet, Israel

Abstract

Security printing is the use of variable data printing (VDP) to add readable information to printed regions. This is used for brand identification, track and trace, product authentication and if applicable for investigation and evidentiary purposes. Well-crafted, multi-region deterrents can be powerful means to simultaneously provide readable information and deter would-be counterfeiters through the crafting of difficult-to-reproduce printing effects. This allows the brand owner to select the best printing technology for the deterrents (or for different aspects of a multi-region deterrent), and to gain insight into how the counterfeiter may attempt to reproduce their deterrent with a different printing approach. In this paper, we consider repeated line patterns (to test print quality), 2D bar code reading, and authentication of a color deterrent (color tile). We print these features using thermal inkjet (TIJ), dry electrophotography (DEP) and liquid electrophotography (LEP) digital printers. Color tiles demonstrate the printer's color fidelity and are used to show authentication accuracy on multiple printers. 2D barcodes demonstrate the printer's binary print quality, and also test different capture settings and substrates for printing. In this way, we test different printers, different inks, different substrates different reading devices and settings along with different security printing deterrent characteristics. Finally, we introduce and discuss meaningful metrics for comparison, including security payload density, deterrent reproducibility, color and spatial frequency fidelity, deterrent pre-compensation and the sensitivity of deterrent authentication to image capture settings and devices.

Introduction

Variable data printing techniques allow potentially authenticable information to be added to any printed region, or "copy hole". However, the density of information and readability of the information depends on a number of factors. These include the printing technology and settings, ink, substrate, and the reader and its settings. In order to qualify a printed deterrent, as many of these factors are fixed as possible, allowing the size of the deterrent (and concomitantly the density of information printed) to be varied [1]. In this paper, we consider the qualification of three quite different security printing deterrents. Combined, these deterrents tell us much about print quality. First, we describe the materials and methods used. Next, we present the results for the repeated line test patterns, 2D bar codes and color tile security deterrents. Finally, we discuss in terms of security payload density, reproducibility, spatial frequency and color fidelity. We introduce the concept of deterrent pre-compensation to make counterfeiting more difficult, and finish with a discussion of the impact of deterrent reader design and settings on deterrent readability.

Methods and Materials

Repeated Line Pattern Tests

The objective of the Line Feature Print (LFP) was to examine spatial frequency fidelity across TIJ (thermal inkjet) and DEP (dry electrophotography) printers. Three printers were used; the HP Deskjet 5440 (TIJ), HP Deskjet 6127 (TIJ) with two different types of print settings, and the HP Color Laserjet 4700dn. All prints were generated from the same digital image described below. For the ink jet printers the default factory settings were used except that the "Best Quality" option was chosen. For the 4700dn laser printer only factory default settings were used. For all three printers the horizontal and vertical dpi was 600.

The final uncompressed raster image master was comprised of an eight by eight layout of line features of 100 lines per inch. For testing purposes we constrained the line colors to the primary printing pigments of a color printer; cyan, magenta, yellow, and black. This decision was motivated by the goal of reducing half toning and color aliasing artifacts. For each of these colors two columns of line features were rendered, one in a vertical line orientation and the other in a horizontal orientation. Each line feature was 0.5" by 0.5" with a horizontal and vertical spacing of 0.5" between adjacent line features. Figure 1 depicts a sample of four line features.

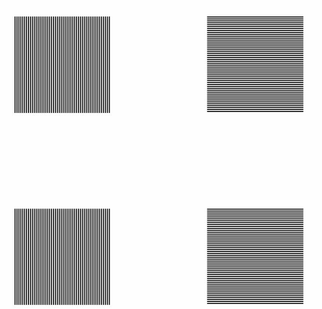

***Figure 1**. Sample of four line features. The left two features comprise 50 vertical lines 3 pixels thick each, and the right two features comprise 50 horizontal lines 3 pixels thick each.*

After the image was printed the page was scanned at 600 ppi using an HP Scanjet 8300. The scanned images were segmented and individual line features were extracted for assessment. For each line feature a *Fast Fourier Transform* (FFT) was performed on the individual R, G, and B channels, perpendicular to the direction of the printed lines, to examine how well each line feature reproduced the print raster line frequency of 100 lpi after the printing/scanning process.

2D Bar Code Reading

2D bar code test pages were created with 23 character payloads using the 2D DataMatrix symbology, with module (individual tile) sizes varied from 10 to 30 mil {10, 11, 12, … , 30 mil}. This corresponds to 254-762 micrometers (µm). 5 barcodes of each size were printed after being generated using B-Coder Bar Code Graphic Generator Version 4.0 [2], using the Symbology.DataMatrix menu, with Comment Line “xx mil” and Bar Code Message (payload) “TestPatternSet3_yyMil_x”. They were copied from the B-Coder software and pasted into Microsoft WORD using Edit.PasteSpecial.Picture(Windows Metafile). Separately, extra spacing was added between the black tiles using Edit.PasteSpecial.Picture(Enhanced Metafile) to generate an entire set of “pre-compensated” 2D barcodes (See Figure 2).

24

24

***Figure 2**. Sample “normal” 2D barcode (left) and pre-compensated 2D barcode (right). The method for generating these barcodes is described in the text.*

These “normal” and “pre-compensated” barcode pages were printed using three different printing technologies: (1) thermal inkjet, or TIJ, using the HP Deskjet 5440 and HP office paper as the substrate, (2) dry electrophotography, or DEP, using the HP Laserjet 4600, also with HP office paper as the substrate, and (3) liquid electrophotography, or LEP, using the Series 1 HP Indigo Press. Black Indigo ElectroInk was used for printing on the following substrates: White Teslin (Teslin® Synthetic Printing Sheet SP 1000 [3]), White Matte (HPIPP Coated Matte 135 gsm), White Glossy (HPIPP Coated Glossy 135 gsm).

All barcodes were read using an InData Systems LDS-4600 reader with either 365 nm w.p.e. (wavelength of peak emission) or 405 nm w.p.e. LEDs for its light source. The Data Matrix 2D bar code symbology was used to ensure that both x and y directions are factored into the authentication. Bar code test sheets containing 10 bar codes at each size were printed. Module size (size of the individual black tiles in the 2D barcode) was varied from 10-30 mils, corresponding to 254-762 µm. Successful reading of all 10 bar codes was required to consider the specified size as “readable”.

Color Tile Authentication

Color tile [1] deterrents are a form of 2D color barcode that can also be associated with microtext and other security features. For our purposes, test sheets of static (fixed sequence of color tiles) square color tile features (Figure 3) were created for testing patterns with individual tile sizes varied from 5-50 pixels at a printing resolution of 600 dpi (0.21-2.12 mm). The tiles were arranged in a 10x10 array with the middle 6x6 tiles blank (for association with another deterrent when shipped on a label). Pages containing from 24 (size=50 pixels) to 165 deterrents (size=5 pixels) were printed at 600 dpi using either the Deskjet 5440 or Laserjet 4600, and then scanned using an HP 8300 Scanjet scanner. For the 5440, “best quality” was the only non-default option used. Scanning was also performed at the same 600 pixels/inch (ppi) resolution, and 24 bit/pixel color images thus obtained.

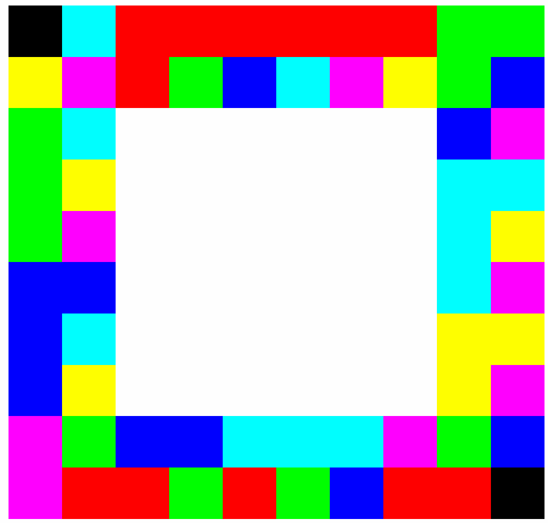

***Figure 3**. Print master of the color tile deterrent tested in this paper.*

After scanning, the scanned pages were authenticated using a modified version of the authentication algorithm described in reference [1]. Briefly, this authentication consists of:

1. Thresholding (binarization of the image)
2. Formation of regions (segmentation)
3. Identification of deterrent regions (classification)
4. Skew detection and deskew
5. Sub-segmentation to find tiles
6. Assigning color type to each tile (“decoding”)
7. Output of color type sequence
8. Comparison of “decoded” and “encoded” sequences

To aid in the task of orientation and decoding, 8 of the 64 color tiles in Figure 3 are “non-payload” indicia. Two black color tiles are located in the upper left and lower right corners. Adjacent to these orienting color tiles are six color tiles, one each of the six colors (red, green, blue, cyan, magenta and yellow) used in the deterrent. These non-payload indicia generally allow significantly greater density to be decoded successfully (authenticated).

Results

Repeated Line Pattern Tests

As the FFT was performed on each color channel, it was important to differentiate the amount of information extracted by the FFT and to determine whether one color channel provided more information than another. We defined the ratio of the magnitude of the AC component of the FFT to the sum of the magnitudes of the AC and DC components of the FFT, as written in Equation 1, as the information content ratio (ICR) of the signal. The closer the ratio is to 1 the more the (intended) AC component shows in the FFT.

$$ICR = \frac{AC}{(AC+DC)} \tag{1}$$

We also examined the distribution of the *energy spectral density* (ESD) (FFT, without the DC component, normalized to sum to 1.0) as defined in Equation 2. This metric was used not only for intra channel comparison but for inter-channel as well.

$$ESD(x) = \frac{\sqrt{(x_{real}^2 + x_{imaginary}^2)}}{\sum\sqrt{(x_{real}^2 + x_{imaginary}^2)}} \tag{2}$$

The results from Equations 1 and 2 showed a distinct trend. For the primary subtractive colors—cyan, magenta, and yellow—the FFT color channel having the highest ICR was the complementary color. However, the percent of the ESD at the line frequency was consistent (typically 30-40%) across the all channels with an ICR of 0.05 or above (we considered ICRs<0.05 to be insignificant). We refer to the channel with the highest ICR as the primary information channel (PIC). The channel with the next-highest ICR, if greater than 0.05, is termed the secondary information channel (SIC). If all three channels have a relevant ICR, then the channel with the third highest ICR is termed the tertiary information channel (TIC).

For the cyan and magenta line features, SIC was apparent (ICR > 0.05) with a peak ESD frequency matching the line frequency. The yellow channel, on the other hand, did not contain a SIC, as both the red and green channels had ICR < 0.05. The black line features demonstrated a different trend than the primary subtractive colors. For the black inks, each (RGB) channel conveys roughly the same information (0.76 ± 0.2 for the Deskjet 5440, 0.64 ± 0.2 for the Deskjet 6127 and 0.76 ± 0.2 for the Laserjet 4700dn). and the line frequency was correctly identified by all three channels as well.

The trending of the information content ratio is consistent across all three printers with one exception. For the cyan line features on the laser jet, ICR is significant across all three channels. But unlike the red (primary) and green (secondary) channels of distinction, the peak ESD frequency for the blue channel correctly identified the line frequency in only 25% of the cyan line feature samples: The remaining samples identified a frequency of 50 (half the line frequency) as the peak frequency.

Table 1: Mean ICR of vertical line features by color channel, Deskjet 5440 printer. Primary information channel (PIC) is in boldface, secondary (SIC) and tertiary (TIC) channels, if present, are italicized.

Line Feature Color	ICR (R)	ICR (G)	ICR (B)
C	**0.7294**	*0.3788*	0.0010
M	0.0045	**0.7435**	*0.4742*
Y	0.0009	0.0052	**0.7294**
K	*0.7494*	*0.7584*	**0.7794**

Table 2: Mean ICR of vertical line features by color channel, Deskjet 6127 printer. Primary information channel (PIC) is in boldface, secondary (SIC) and tertiary (TIC) channels, if present, are italicized.

Line Feature Color	ICR (R)	ICR (G)	ICR (B)
C	**0.7304**	*0.3217*	0.0009
M	0.0463	**0.7230**	*0.4338*
Y	0.0002	0.0407	**0.8841**
K	*0.6246*	*0.6404*	**0.6645**

Table 3: Mean ICR of vertical line features by color channel, LaserJet 4700dn printer. Primary information channel (PIC) is in boldface, secondary (SIC) and tertiary (TIC) channels, if present, are italicized. Note the existence of a C-colored line feature TIC (top of last column).

Line Feature Color	ICR (R)	ICR (G)	ICR (B)
C	**0.7249**	*0.4533*	*0.2685*
M	0.0009	**0.7307**	*0.5293*
Y	0.0010	0.0011	**0.7361**
K	*0.7475*	*0.7610*	**0.7785**

The differences in printer output between TIJ (Deskjet 5440) and Laserjet (4700dn) are illustrated in Figure 4.

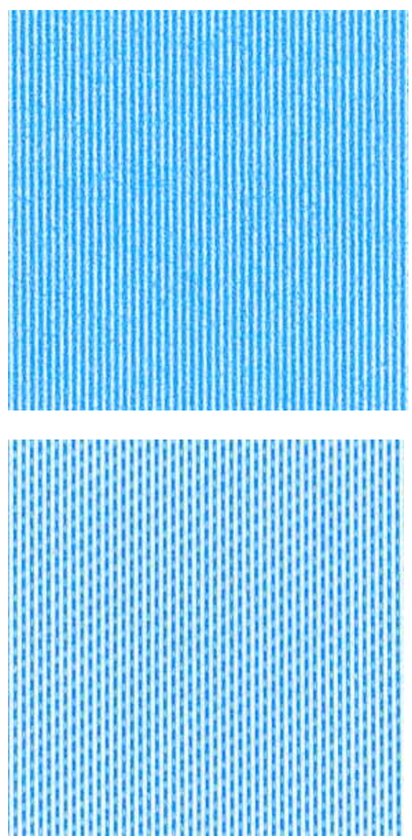

Figure 4. Sample cyan color line feature. Deskjet 5440 (top) and Laserjet 4700dn (bottom) are shown..

2D Bar Code Reading

2D barcodes printed on using LEP, TIJ and DEP printers were read with using both 365 nm and 405 nm LEDs, as described above (Table 4). For the LEP printer, the default substrate was Teslin [3], while for the TIJ and DEP printers, HP office paper was used. In all cases, the pre-compensated barcodes were readable at a smaller scale: 8% smaller for the LEP printing using either 365 nm or 405 nm LEDs for reading; 21% smaller for the DEP printing using either 365 nm or 405 nm LEDs for reading, and either 42% (365 nm LEDs) or 35% (405 nm LEDs) smaller for the TIJ (Table 1). Interestingly, with pre-compensation, all three printing technologies produced readable 2D barcodes with module size as small as 11 mils (279 µm). This was true for both far blue (405 nm) and ultraviolet (365 nm) illumination.

Table 4: Black 2D bar code reading results, default substrate (Teslin for Indigo LEP, HP Office Paper for Inkjet and Laserjet)

LEDs (nm), **=Pre-compensated barcode	Indigo LEP Min Module Size (µm)	Inkjet Min Module Size (µm)	Laserjet Min Module Size (µm)
405	305	432	356
405 **	279	279	279
365	305	483	356
365**	279	279	279

The sensitivity of bar code reading to the substrate printed on was tested for the LEP printer (Table 5). Normal (not pre-compensated) 2D barcodes were readable on all three substrates with module size as small as 12 mils (305 µm). However, the effect of pre-compensation on readability differed considerably for the three substrates. For the Teslin substrate, pre-compensation afforded 8% reduction in module size for readability. However, none of the pre-compensated barcode indicia could be read from the glossy substrate, and the "normal" barcodes could be read with a 25% smaller module size than the pre-compensated barcodes from the matte substrate.

Table 5: Black 2D bar code reading results, Differing Indigo LEP substrates (365 nm LEDs used for reading)

Substrate	Min Module Size (µm), Normal 2D Barcodes	Min Module Size (µm), Pre-compensated 2D Barcodes
Teslin	305	279
Glossy	305	**Could Not Read**
Matte	305	406

Color Tile Authentication

Color tile deterrent sheets were created for a 165 x 229 mm print sheet (affording 25 mm margins on HP Office Paper), as described above. Authentication was 100% for the TIJ deterrents at sizes of 12 pixels or above, and for DEP deterrents at sizes of 18 pixels or above. The differences in color tile appearance at 12 and 16 pixel sizes are shown in Figures 5 and 6.

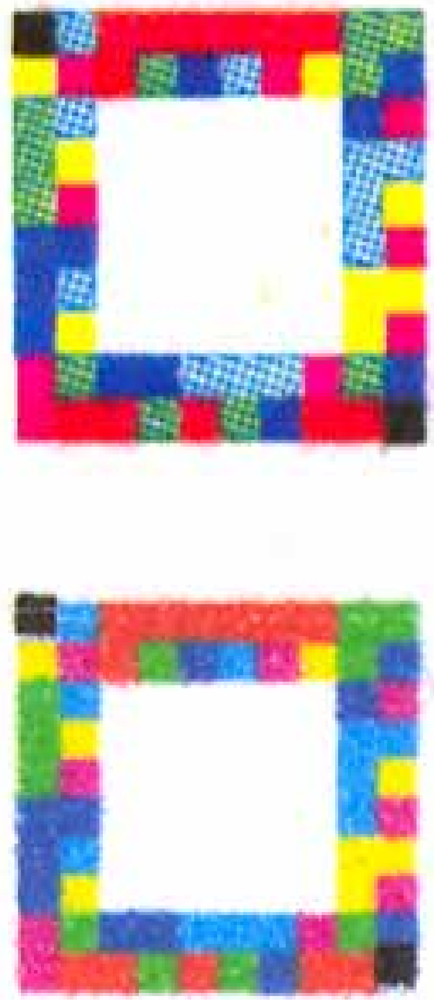

Figure 5. *Laserjet, size 12 pixels (above); TIJ, size 12 pixels (below).*

In Figure 5, the Laserjet sample shows more visible evidence of halftoning, and the inkjet sample appears to distinguish red from magenta with more clarity.

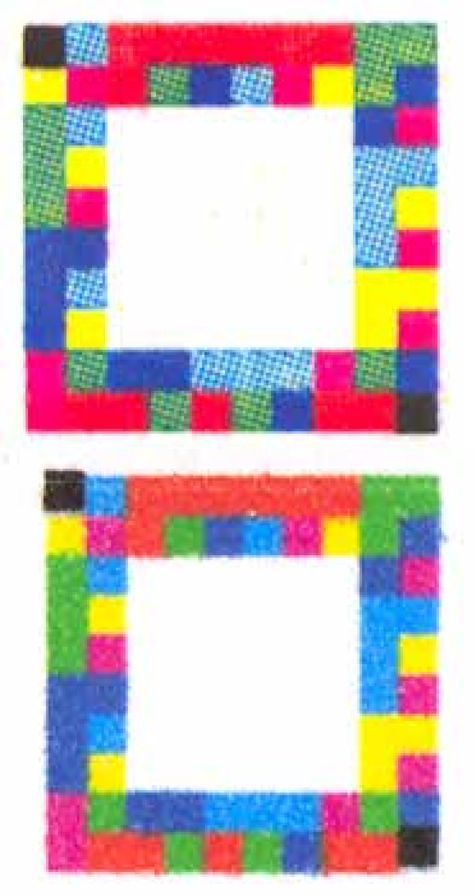

Figure 6. Laserjet, size 16 pixels (above); TIJ, size 16 pixels (below).

These trends are also observed in Figure 6, although the larger sized tiles appear more sharply defined for each printing technology.

Table 6: Authentication rate for color tile features with . Authentication rates for 18-50 pixel sizes (0.762-2.117 mm) were 100% for both printers (HP Deskjet 5440 and HP Laserjet 4600).

Color tile size (pixels at 600 ppi)	Number Tested (Single Print Sheet)	Percent Authenticated (TIJ: HP Deskjet 5440)	Percent Authenticated (DEP: HP Laserjet 4600)
5	165	0.0	0.0
6	150	0.0	0.0
7	140	0.7	0.0
8	140	0.0	0.0
9	130	46.2	47.7
10	117	88.9	76.9
12	108	100.0	71.3
14	96	100.0	94.8
16	88	100.0	98.9
18	88	100.0	100.0
20	70	100.0	100.0
25	63	100.0	100.0

Authentication results for the TIJ and DEP technologies are given in Table 6. While roughly half of the 56-tile deterrents are correctly authenticated at a size of 9 pixels (0.38 mm) for both print technologies, the TIJ printed deterrents are fully authenticable at a 50% smaller size.

Discussion and Conclusions

The security deterrent printing experiments reported here were performed to compare and contrast the quality of printing and reading for different substrates, printing approaches, and reading devices. In addition, the types of deterrents afford views of different aspects of printing and imaging quality. The repeated line deterrents, like modulation transfer function or MTF deterrents [4], can be used to simultaneously check scanner capabilities and encode information in the frequency domain. The 2D bar codes use an industry-standard reading algorithm and allow for ready assessment of ink, print, substrate and deterrent quality and the crafting of ink-specific handheld readers [5]. The experiments performed here also illustrated the potentially large impact on readability afforded by structural pre-compensation [6], as shown in Figure 1.

Security Payload Density

Briefly, the security payload density (SPD) is determined by the number of reliably readable bits that can be packed in a given area (Equation 3).

$$SPD = \#\text{authenticable bits} / \text{unit area} \qquad (3)$$

The payload density of 2D barcodes is largely determined by the error code checking (ECC) information specified by the standard. For crafted deterrents, such as the color tile deterrent described herein, wherein each tile is authenticated, the SPD trade off is between size reduction (to increase density) and the inclusion of more non-payload indicia (to increase accuracy and reduce density). The same set (8 tiles) of non-payload indicia were used for TIJ and DEP testing herein; however, the DEP deterrents had to be printed 50% larger (125% larger by area) to achieve 100% authentication, meaning the SPD was only 44% that of the TIJ deterrents. Testing the impact of adding more non-payload indicia to drive the size of the individual tile downward is a next step in the productization of these deterrents.

Deterrent Reproducibility

The deterrent reproducibility (DR) is the ability to reverse engineer the information in the deterrent, and as such is a measure of how secure a deterrent is from the counterfeiter. For the color tile deterrents as presented herein, there is no discussion of adding steganographic information (such as a microtext sequence) to the deterrents. Thus, for a covert-only deterrent, reading (or "authenticating") a deterrent and knowing the format of the non-payload indicia is all that is necessary to "reproduce" (or counterfeit) the deterrent. For such a deterrent, the security protection comes from having a much larger number of possible deterrent sequences than the number of products with the deterrents. A 56-tile 6-color deterrent contains approximately 145 bits of data, meaning more than 4 x 10^{43} different sequences are possible.

Once covert features are added, however, authentication of the color tile sequence is not enough to reproduce the deterrent, since the would-be counterfeiter may fail to reproduce the covert patterns within the tiles. For such a "copy-resistant" deterrent, DR is a combination of replicating the overt and covert nature of the deterrent.

However, a potentially more powerful mechanism to prevent casual counterfeiting is to link several deterrents on the same article through a secret chaining or association mechanism. This "hybrid" strategy generally forces a would-be counterfeiter to collect multiple reads (perhaps with different readers, e.g. ultraviolet and visible light) off each article to copy it. This drives the cost of counterfeiting up, and makes it less attractive.

The color tile deterrent, if printed using an inkjet printer at a size less than 15 pixels at 600 ppi, cannot be reliably reproduced with a color Laserjet, since a large percentage of these will fail to read, even if the codes are stolen. Thus, the TIJ printer has a higher DR than the Laserjet printer for color tiles.

Color Fidelity

Color fidelity is measured indirectly with the color tile authentication studies. As mentioned above, these results indicate better **absolute** color fidelity for the TIJ compared to DEP technology evaluated herein. One means of increasing absolute color fidelity is through spectral pre-compensation [4], in which case the printed colors are altered such that they will disambiguate better when scanned.

Note that the non-payload indicia added to the color tile deterrent greatly increase the **relative** color fidelity of the authentication algorithm, even if the absolute color fidelity is poor. So long as the color distortions are consistent, these non-payload color indicia generally greatly increase SPD. Further

Spatial Frequency Fidelity

Repeated line tests show that there are differences in the spatial frequency information contained in the scanned color channels after printing with TIJ or DEP technologies. Also, yellow color lines behave distinctively from the cyan and magenta lines, likely due to full saturation of both red and green channels by the yellow ink.

2D barcodes also test spatial frequency fidelity. The better performance of the Laserjet 4600 compared to the Deskjet 5440 is consistent with the generally better text and line quality of the Laserjet printer.

Deterrent Pre-Compensation

As described for the 2D bar code test sheets, structural pre-compensation of a deterrent is a potentially powerful means of increasing SPD, and for making counterfeiting more difficult. 2D bar codes pre-compensated to leave whitespace between the black modules read at a smaller size due to a combination of, at least, ink spread during printing and blur during reading. The efficacy of pre-compensation increased from the LEP (8% improvement) to the DEP (21% improvement) to the TIJ (35% or 42% improvement) printing, most likely as a consequence of increasing ink spread.

We briefly discussed spectral pre-compensation above related to increasing color fidelity, but did not directly test it in the experiments reported here.

Sensitivity of Deterrent Authentication to Image Capture Settings and Devices

The 2D barcodes were scanned using both 365 nm and 405 nm LEDs. The 365 nm LEDs permit reading of the Indigo UV ElectroInk, while the 405 nm LEDs do not. This sensitivity to LEDs permits the creation of ink-specific readers [5], and the combination of overt and covert inks makes the would-be counterfeiter's task more difficult.

Conclusions

The use of line features in this work was constrained to a single line frequency and fixed dimensions. While this feature alone provided information about the printer and print quality, additional tests using a range of frequencies should lead to further information about the relative print quality of different printers and print technologies. Altering the feature dimensions will allow us to understand what the minimum and maximum required sizes are to extract salient information on the fidelity of the test prints.

The experiments reported here highlight deterrent preparation, printer, substrate, modality (color, spatial frequency), and reader issues involved in qualifying and deploying a variable security deterrent. The results emphasize the power of variable data printing and merging multiple printing technologies on a single article for brand protection and anti-counterfeiting.

Acknowledgments

The authors thank David Auter, Shawn Gibson, Andrew Page, Eddie Torres and Juan Carlos Villa for collaborative work on the color tile family of deterrents.

References

[1] S. J. Simske and J. S. Aronoff, Qualification of a Layered Security Print Deterrent, J. Imaging Sci. and Technol., pp. 86-95 (2007).

[2] TAL Technologies, Inc., Philadelphia PA 19130, 800-722-6004, www.taltech.com.

[3] Teslin® Synthetic Printing Sheet SP 1000, http://corporateportal.ppg.com/NA/Silicas/Teslin/whatsteslin/.

[4] S. J. Simske, M. Sturgill, J. S. Aronoff, G. Golodetz, J.C. Villa, Method for Security Printing, HP Docket 200700131, filed with USPTO 6 June 2007.

[5] S. J. Simske, J. R. Hattersley, G. Golodetz and J. Stasiak, Ink-Specific Handheld Readers and Security Variable Data Printing, Proc. IS&T NIP22, pp.441-443 (2006).

[6] S. J. Simske, J. S. Aronoff, Target Patterns Providing Quality Assurance Verification and Security Authentication, HP Docket 200505800, filed with USPTO 18 August 2006.

Author Biography

Steven Simske is the principal scientist in security printing and imaging for Hewlett-Packard laboratories. He has worked in biomedical imaging and signal processing; image, text and speech understanding; classification and security printing over the past 20 years. He is a senior research associate in Aerospace Engineering at the University of Colorado, and an Adjunct Professor of Physics at the Colorado School of Mines. He is a member of IEEE, ACM, IST and SPIE.