Inspection and authentication of color security deterrents with multiple imaging devices

Jason S. Aronoff, Steven J. Simske

HP Laboratories
HPL-2010-8

Keyword(s):
Payload density, grayscale pre-compensation, authentication

Abstract:
The use of 2D color barcodes is quickly becoming commonplace on printed packaging and labels. The color barcode allows for a higher data density in comparison to its 1D or 2D black and white counterparts. However, with the introduction of color, a new set of imaging problems is introduced in reading the color symbol. Color requires the use of higher quality image capture devices as well as the associated bandwidth when the captured image is analyzed or sent to a central repository for authentication. In this paper we introduce a novel approach to color manipulation which enables two modalities of reading; color and grayscale. This approach adjusts the printed color set such that it is visually distinct in grayscale while still retaining a reasonable resemblance to the original colors. We examine the robustness of this approach using the color tile deterrent and printing and authenticating samples using several printers and a range of deterrent sizes. In cases where symbol size negatively impacts read accuracy we propose an alternate approach which allows for improved reading while still retaining a reasonable payload density. When properly deployed, our approach can complement any color barcode technology by allowing for dual authentication.

External Posting Date: January 21, 2010 [Fulltext] Approved for External Publication
Internal Posting Date: January 21, 2010 [Fulltext]

Published and presented at Optical Document Security 2010, San Francisco. January 20-22, 2010

Inspection and authentication of color security deterrents with multiple imaging devices

Jason S. Aronoff[a] and Steven J. Simske[a]

[a]Hewlett Packard Labs, 3404 E. Harmony Road, Fort Collins, CO, USA 80528

ABSTRACT

The use of 2D color barcodes is quickly becoming commonplace on printed packaging and labels. The color barcode allows for a higher data density in comparison to its 1D or 2D black and white counterparts. However, with the introduction of color, a new set of imaging problems is introduced in reading the color symbol. Color requires the use of higher quality image capture devices as well as the associated bandwidth when the captured image is analyzed or sent to a central repository for authentication. In this paper we introduce a novel approach to color manipulation which enables two modalities of reading; color and grayscale. This approach adjusts the printed color set such that it is visually distinct in grayscale while still retaining a reasonable resemblance to the original colors. We examine the robustness of this approach using the color tile deterrent and printing and authenticating samples using several printers and a range of deterrent sizes. In cases where symbol size negatively impacts read accuracy we propose an alternate approach which allows for improved reading while still retaining a reasonable payload density. When properly deployed, our approach can complement any color barcode technology by allowing for dual authentication.

Keywords: Payload density, grayscale pre-compensation, authentication

1. INTRODUCTION

Printed security regions, or deterrents, on packaging and labels provide an end user, inspector, or forensic analyst the ability to validate the authenticity of an object under inspection. Advances in printing and imaging have greatly increased payload density in a printed deterrent. However, reading of many high density color deterrents requires a higher resolution and/or color camera or scanner. Mobile devices may not have high-enough quality imaging devices, and manufacturing lines may not have color readers installed (due to speed and/or cost concerns).

In previous works [1, 2], we introduced the concept of spectral pre-compensation (SPC). In this approach, we examined the effect of the print/scan cycle and how it changed the hue of a color from what its intended value was supposed to be. By adjusting or pre-compensating the hues of individual colors in the digital raster such that once printed and scanned the colors correctly read as the intended hue, we were able to apply SPC towards color values of the color tile deterrent to increase authentication accuracy at smaller deterrent sizes.

In this paper we examine a different approach to pre-compensation which we term grayscale pre-compensation (GPC). This method allows for multiple types of authentication through the design of a printed security deterrent which can be authenticated with both color and grayscale imaging devices. The use of this approach has several advantages. First, for print shops using inline scanners that are grayscale only, quality assurance or QA, which includes determining that ink has been printed and that the printed regions are the right size, shape and color density, can be performed in grayscale and be correlated to color QA. Secondly, the use of grayscale over color allows for a decrease in processing time and data storage. If, for example, a security deterrent is printed in 24-bit RGB color but scanned and analyzed in 8-bit grayscale, computations are reduced to 8-bit numbers and storage space is reduced by two-thirds compared to the original color deterrent. The efficacy of this approach lies in calibrating the color palette of a specific printer model and substrate such that each printed color is distinct and separable in grayscale.

This approach, in providing dual authentication, adds an additional layer of security which can be used for forensic analysis. Since a color palette must be adjusted to a specific printer model and substrate, if a color security deterrent is counterfeited, the would-be counterfeiters would need to use the specific printer model, substrate and printer settings in order to have the deterrent pass authentication in both color and grayscale. The choice of which colors to deploy and where in the grayscale range each color is targeted can be application specific, further increasing the complexity and variability of a print job.

This paper is structured in the following manner. First, we briefly review other approaches used for printed security deterrents in the remainder of this section. We then follow by detailing out our approach in Section 2. Section 3 discusses the experiments performed to validate our approach and examine its effectiveness when deployed in a security deterrent. Section 4 reviews the results of the experiments and is followed by discussion in Section 5. We wrap up our work with concluding remarks and mention of future work in Section 6.

1.1 Related Work

Color security deterrents have been deployed by multiple research groups in an effort to provide a low cost and effective data storage symbol which can be easily deployed on a printed package or label. Within the past two years Microsoft released its version of a color security deterrent named the *High Capacity Color Barcode* (HCCB) [3, 4]. In this implementation, the security deterrent embeds data using triangles which can be implemented in either a 4 or 8 color schema allowing for either 2 or 3 bits of data storage per triangle respectively. Authentication of the HCCB deterrent relies on having a fixed point within the image be known to allow for localization and segmentation of the deterrent from the overall image (i.e. a capture device must be centered on a barcode rather than scanning the entire package and executing an inspection algorithm to locate the barcode). In the bottom right corner of each HCCB, the last 8 color triangles represent the color palette used in deployment. In the 4-color schema, each color is repeated twice. Classification of the data bearing triangles is then made by comparison to the color palette triangles.

In a completely different approach, researchers in [5] embedded data by using halftone dot orientation. This approach allowed for 4 dot orientations, or 2 bits per dot. However, authentication of this deterrent required scanning the printed deterrent at 1200 or 2400 dpi. Even with this high resolution approach and error-correcting code, symbol read errors still occurred during the authentication process. Additionally, the high resolution approach utilized for reading makes it less than desirable for use in low bandwidth applications and infeasible for use with low end point and shoot or cell phone cameras.

2. METHODOLOGY

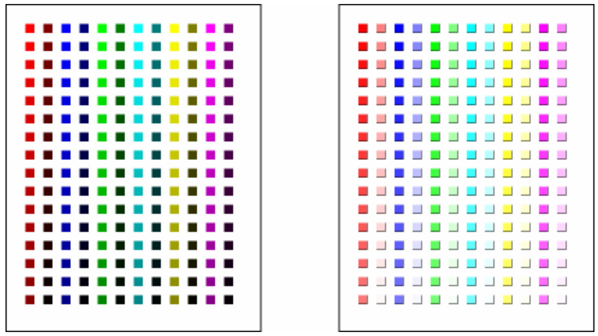
The underlying concept behind our approach is to identify a target color palette such that when scanned in grayscale the resulting grayscale intensities are distinctly separable to a machine vision/image processing application. We list out the steps to our approach below then follow in detail.

1. Identify the desired base color selections
2. Generate calibration sheets that correspond to the base color selections
3. Print calibration sheets on target printer/ink/substrate combination
4. Scan the printed calibration sheets on the target scanner
5. Extract corresponding grayscale intensities from calibration sheets
6. Analyze grayscale intensity mappings and perform color assignments
7. Validate color/grayscale assignments on a security deterrent test vehicle

We provide here a quick review of the terminology which applies to our approach. For the purposes of our research, we store all color values as a red, green, blue (RGB) triplet. For each of the three color channels, we utilize 8-bit color so each value within the triplet can have a range of 0 to 255, where 0 denotes no color or black for that channel and 255 indicates full saturation. For grayscale intensities, we also use an 8-bit channel which is represented by a single number ranging from 0 (black) to 255 (pure white).

The color palette selected for use can be comprised of a number of colors. From empirical analysis we have found that a range of three to six is most effective (reasons why are detailed in Section 5). For our tests we selected red (R), green (G), blue (B), cyan (C), magenta (M), and yellow (Y) since they comprise the standard color set which is used in our security deterrent, the color tile deterrent (Figure 4a). The main constraint in the selection of colors is that they be distinctly separable once scanned in grayscale. We have found that with this selection, {RGBCMY}, separation can be obtained.

Once the color set has been defined, calibration sheets are generated. Figure 1 depicts examples of two calibration sheets which we use. Each of the calibration sheets is comprised of half inch squares which are of a uniform color. The first calibration sheet (Figure 1a) takes each color selected from the first step and starting with full saturation decrements the saturation towards black in steps of eight. For example, beginning with red (255,0,0) in the upper leftmost corner of the sheet the second square is then (247,0,0) followed by (239,0,0) for the third square, etc. A total of 32 tiles are generated for each target color and are placed in adjacent columns. The second calibration sheet (Figure 1b) is generated in the opposite direction and each fully saturated color is traversed towards white in steps of 8.



(a) (b)

Figure 1: Calibration test sheets (scaled to 20% of actual size); (a) full saturation to black and (b) full saturation to white.

Once the digital images of the calibration sheets have been generated they are ready for printing. Five copies of each sheet are printed in color and scanned in grayscale using the exact same printer/ink/substrate and scanner combination. To ensure that all image information is retained in the scanning process, images are saved in a lossless image format (either bitmap or PNG). Using custom in-house image processing software, the images from the scanned calibration sheets are then analyzed to extract each color square. Since the RGB value of each color square is known by its location, the grayscale value of each square is tied to its corresponding RGB value to generate a lookup table (LUT). After all five sheets from each type of calibration sheet have been run, the grayscale intensity is averaged for the squares at each position and the master LUT is generated.

Using the master LUT, the intensity mappings can be analyzed to identify the color assignments. The simplest approach to performing color assignments can be executed by performing a linear discretization of the grayscale space in the following manner. First, inspecting the full saturation colors, we identify the colors which have the respective highest and lowest grayscale values. Looking at example results in Table 1, one will notice that blue corresponds to the lowest intensity with a value of 111 and yellow corresponds to the highest intensity with a value of 243. Using 111 and 243 as the end points for the range, the grayscale intensity space can be discretized uniformly by the following equation:

$$stepsize = \frac{(\max - \min)}{(n-1)} \tag{1}$$

where *n* represents the number of colors in the selected color palette. In this example the step size is 26.4. Using

Color	RGB Value	Grayscale Intensity
R	(255,0,0)	161
G	(0,255,0)	163
B	(0,0,255)	111
C	(0,255,255)	158
M	(255,0,255)	148
Y	(255,255,0)	243

Table 1: Mean grayscale intensities of baseline colors

the master LUT, the color–grayscale allocation table is constructed by inspecting the color-grayscale pairings. The RGB value for each color is selected by finding the corresponding mean grayscale intensity value which is closest to the target intensity generated from discretization. Since 4 colors remain to be allocated, a 4 by 4 allocation matrix can be generated as shown in Table 2. As can be seen in the table, there are a number of ways to allocate a color to a grayscale value. In the simplest approach the lower left to upper right diagonal is taken as the assignment list for the remaining four colors. This is graphically depicted in Figure 2.

	Target Intensity			
Color	137.4	163.8	190.2	216.6
R	138.0 (159,0,0)	162.7 (255,16,16)	191.5 (255,128,128)	217.9 (255,176,176)
G	136.3 (0,159,0)	163.0 (0,255,0)	189.2 (80,255,80)	217.7 (160,255,160)
C	138.6 (0,135,135)	161.6 (8,255,255)	191.8 (64,255,255)	216.6 (136,255,255)
M	137.7 (223,0,223)	164.4 (255,48,255)	190.4 (255,120,255)	215.5 (255,176,255)

Table 2: Color–grayscale allocation table. Values in the cells represent the closest grayscale intensity to the target intensity and the corresponding RGB values.

In addition to selecting the color–grayscale allocation from the table in a different manner, other approaches can be taken to allocate colors to specific grayscale values. One alternate approach is to expand the endpoints to increase the grayscale range. For example, blue could be pushed to a lower intensity by using a darker shade of the color.

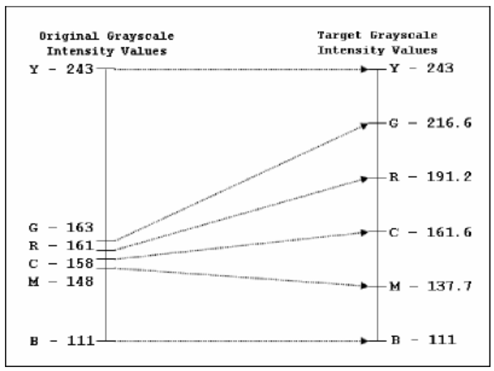


Figure 2: Grayscale Intensity Mapping utilizing uniform discretization of the grayscale intensity space.

The final step in our methodology is to test the effectiveness of the color–grayscale allocation. We perform this step using the color tile deterrent, examples of which are seen in Figures 4 and 5. The color tile deterrent is comprised of 64 square tiles laid out in a 10 by 10 grid. Eight of the tiles are used for registration and calibration and the remaining 56 store the information payload. The overall width and height of the deterrent are specified by the size of the color tiles which can range in size from 5 by 5 pixels to 20 by 20 pixels or more depending on application. The center of the deterrent is left as white space to store a 2D Data Matrix; however, in other implementations it can be filled in with additional tiles.

As can be seen in Figure 4a, the upper left and lower right corners of the deterrent contain a single black tile. These two black tiles are utilized for registration and orientation of the overall deterrent. Adjacent to each of the black tiles are three color tiles which represent the non-payload indicia (NPI) of the deterrent. These six tiles provide the color set which is used in the overall deterrent. For our purposes, the upper left corner of the deterrent contains C, M, and Y NPI tiles. The lower right contains the R, G, and B NPI tiles. Using the color assignments made during the allocation step, a digital image of the tile deterrent is generated using the GPC color values. This digital deterrent image is then replicated across an entire test sheet, spaced apart by a half inch of white space horizontally and vertically. The overall number of deterrents on a test sheet is then dependent on the size of the deterrent being rendered. For our experiments we utilized tile sizes of 10 through 15. Table 3 lists the deterrent tile size and the corresponding number of deterrents per test sheet.

Tile Size	Deterrents per sheet
10	117
11	117
12	108
13	108
14	96
15	96

Table 3: Tile size and corresponding deterrents per test sheet

Once the test sheet digital masters have been rendered, they are printed in color on the target printer and subsequently scanned in 8-bit grayscale at 600 ppi on a flatbed scanner using default settings. Figure 3 gives an example of a deterrent test sheet.

To read the color tile deterrent, the overall deterrent is segmented from the scanned image and orientation of the deterrent is determined from the black tiles. Individual tiles are then segmented, cropped in from all sides by 15%, and the representative grayscale value of each tile is then calculated. Determination of each payload tile is then performed by comparing to the six NPI tiles. This is performed in one of two ways. In the first method, the mean tile intensity is calculated from the remaining cropped area of the tile. The distance from a payload tile to each NPI tile is then calculated as the absolute difference, and the candidate tile is assigned the color of the NPI tile with the shortest distance.

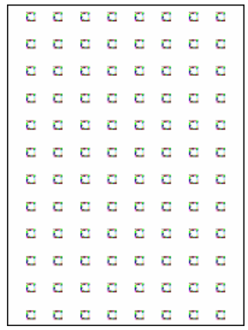


Figure 3: Color Tile Deterrent test sheet with GPC colors.

Formally, the distance calculation can be defined as

$$d = \left|\mu_{npi} - \mu_c\right| \tag{2}$$

where μ_{npi} represents the mean grayscale intensity of an NPI tile, and μ_c represents the mean grayscale intensity of a candidate tile.

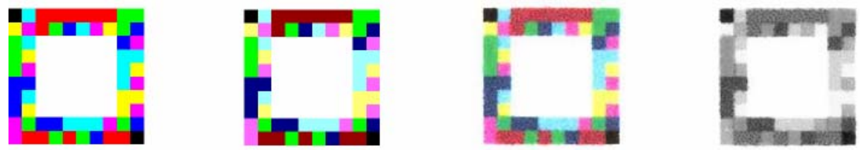
The second approach to finding a tile assignment is performed by histogram intersection. This method, implemented in [6] and [7] for image classification, performs classification by finding the largest histogram shared area between a test image and a set of training images. In our approach, pixels from the candidate tile are binned into a grayscale intensity histogram and the shared area between the candidate tile histogram and each of the NPI tile histograms are found. Since the possibility exists that the pixel counts between tiles in a deterrent may vary due to the segmentation algorithm, each histogram is normalized such that the area under the curve sums to 1.0. The candidate tile is then assigned to the color of the NPI tile with the largest histogram shared area. Formally this can be defined as

$$A = \sum_{i=0}^{255}\left[\min(H_{npi}(i), H_c(i))\right] \tag{3}$$

where H_{npi} represents the intensity histogram of an NPI tile and H_c represents a candidate tile.

The overall sequence of tile assignments is then compared to what was originally encoded to the deterrent. In order for a deterrent to pass authentication, all 56 payload tiles must be correctly read. In the event that a deterrent does not pass authentication, the number of incorrectly read tiles is stored for failure analysis.

Figure 4 shows examples of the tile deterrent and the effects that occur from GPC. In Figure 4a, the uncompensated digital image of a tile deterrent is shown. All colors for this deterrent are at full saturation. In Figure 4b, the digital image of a tile deterrent with GPC is depicted. Figures 4c and 4d show the tile deterrent after it has been printed in color, and scanned in color or grayscale, respectively. Note that the color–grayscale mapping used in Figure 4 differs from that of the example given in this section.



(a) (b) (c) (d)

Figure 4: Example color tile deterrent with 64 tiles (enlarged for legibility). The upper left and lower right corners each contain four non-payload indicia tiles used as part of the authentication algorithm. The remaining 56 tiles store the payload. (a) Digital with no compensation, (b) Digital with GPC, (c) Color scan of the printed GPC digital, and (d) Grayscale scan of the printed GPC digital.

3. EXPERIMENTS

Several types of experiments were performed to assess the viability of our approach. Since we had several objectives when developing this methodology, it was necessary to examine efficacy in several ways. First, proof of concept needed to be evaluated. This was performed by reading and authenticating two sets of color tile deterrents in grayscale. The first set was the control group, which had no GPC. The digital master of the color tile deterrent was generated at full saturation for each of the six colors. The second set of tile deterrents was generated using a GPC digital master where the color–grayscale mappings were determined by utilizing the approach described in Section 2. The tile size of the color tile deterrent was 15 by 15 pixels at 600 ppi for both test sets. Both sets of prints were run on an HP 6940 thermal inkjet (TIJ) printer. The HP 6940 is a 4-ink CMYK printer. For both tests the same printer settings were used when printing the deterrent test sheets. HP Office Paper was used for all prints and an HP Scanjet 8350 was used to scan the test prints in 8-bit grayscale.

The second set of experiments looked at the robustness of the approach across a range of tile deterrent sizes. For these experiments we used tile sizes of 10 through 15 which give an overall deterrent size of 100 x 100 to 150 x 150 pixels in width and height. For all experiments the resolution was held constant at 600 ppi or dpi for the raster, test prints, and grayscale scans. Tests were performed on three printers each with the same substrate; HP Office Paper. The printer models used were the HP 6127 (4-ink TIJ), HP 6280 (6-ink TIJ) and HP 6940 (4-ink TIJ). Calibration sheets were printed for each printer model and scanned to determine the corresponding color–grayscale intensity mappings. All scans were performed on the HP Scanjet 8350 with identical settings. All deterrents were authenticated in grayscale twice, once using the absolute difference of mean intensity and again using histogram intersection.

The third set of experiments examined the effect of GPC on color authentication. For this test all of the printed GPC test sheets from the second set of experiments were scanned in 24-bit RGB color. Authentication of the 24-bit color tile deterrent was performed by finding the L1 distance of a candidate tile to each NPI tile in RGB space. Similarly to the grayscale approach, the candidate tile was classified as the color of the NPI tile to which it had the smallest distance. Formally, the L1 distance calculation in color space can be defined as

$$d = \left(\left| \mu_{npi}^{(r)} - \mu_{c}^{(r)} \right| + \left| \mu_{npi}^{(g)} - \mu_{c}^{(g)} \right| + \left| \mu_{npi}^{(b)} - \mu_{c}^{(b)} \right| \right) \tag{4}$$

where $\mu_{npi}^{(x)}$ refers to the mean value of color x in an NPI tile and $\mu_{c}^{(x)}$ refers to the mean value of color x in a candidate tile.

The fourth set of experiments looked at the results of deterrent authentication accuracy with respect to the number of colors in the deterrent for the HP 6127. This was performed by generating two separate deterrent test sheets; one with 5 colors and one with 4 colors. Using {RGBCMY} as the set of possible colors to select from, the color to eliminate for the 5-color print was selected by looking at the tile classification results from the 6-color deterrent tests. The tile color with the largest misclassification rate was eliminated from the set and the grayscale intensity space was re-discretized to increase the separation distance between the remaining colors. Deterrent test sheets were generated with this color set and then printed on the HP 6127 and scanned in grayscale. The scans of the test sheets were then run with the absolute difference of mean grayscale intensity authentication algorithm and again using the grayscale histogram intersection algorithm. This entire process was then repeated for a 4-color tile deterrent by inspecting the tile misclassification rates for the 5-color deterrents and again eliminating the tile color with the largest misclassification rate.

4. RESULTS

For the first set of experiments, in which we tested the proof of concept for GPC, we utilized the HP 6940 TIJ printer. Two sheets of deterrents were printed, one with GPC the other without. For the GPC tile deterrents, the color–

grayscale mappings are listed in Table 7. In this experiment, the histogram intersection authentication routine was used for tile classification. Using GPC, an authentication rate of 98.958% was achieved (95 out of 96 deterrents correctly authenticated). When GPC was not utilized, all of the deterrents failed to correctly authenticate. Recalling that for each deterrent there are 56 tiles, the mean tile read errors per failed deterrent were 21.00 for the non-GPC deterrent test sheet. Table 4 shows the confusion matrix of tile classifications for all 96 deterrents from this test sheet. As can be seen from the table, significant misclassification exists for R, G, C, and M when GPC is not utilized. Comparatively, for the lone GPC tile deterrent which failed authentication, only 1 of the 56 tiles failed to read correctly. It is important to point out that error-correcting code (ECC) was not used for this experiment nor any of the other experiments in this body of work.

		Predicted					
		R	G	B	C	M	Y
Actual	R	222	224	0	346	264	0
	G	208	394	0	103	255	0
	B	6	18	927	0	9	0
	C	0	44	0	916	0	0
	M	194	191	1	153	229	0
	Y	0	0	0	0	0	672

Table 4: Confusion matrix of tile classifications for uncompensated grayscale authentication of the size 15 tile deterrent printed on the HP 6940. Result values represent the grand total of all 96 tile deterrents tested.

For the second set of experiments, which examined robustness of the GPC approach, the color–grayscale mappings obtained from the calibration test sheets are listed in Tables 5, 6, and 7. Determination of the color–grayscale mappings was performed first by expanding the overall range of the intensity. This was performed by inspecting the colors blue and yellow and selecting a darker and lighter color intensity respectively to increase the range. For example, looking at Table 5, the original mean grayscale intensity of blue at full saturation (0,0,255) was 111.0. To allow for increased intensity separation, blue was adjusted to (0,0,135) to reduce its mean intensity to 89.7. The same process was performed for yellow to increase (lighten) its intensity from 243.1 to 249.0.

The intensity space was then uniformly spaced using the step size calculated from Equation 1, to provide an equal amount of separation in grayscale space similar to the depiction on the right hand side of Figure 2. The uniform spacing is then used as the target grayscale values, listed in the "Target Intensity" column in Tables 5, 6, and 7. Selection of the desired color to target intensity was made by inspecting the color calibration sheets. The color squares with the smallest difference from the target value were selected for use. Tables 8, 9, and 10 summarize the authentication results of the tile deterrent test sheets. For all test sheets, authentication was performed once using the grayscale histogram intersection approach, and once using the absolute difference of grayscale mean intensity distance calculation. Note that in all three tables the column labeled "Mean Tile Errors" is short for mean tile errors per failed deterrent.

Color	RGB Value	Mean Intensity	Target Intensity	Actual Intensity	Adjusted RGB Value
R	(255, 0, 0)	161.0	121.5	126.0	(127, 0, 0)
G	(0, 255, 0)	162.7	185.2	185.0	(0, 255, 0)
B	(0, 0, 255)	111.0	89.7	89.7	(0, 0, 135)
C	(0, 255, 255)	158.0	217.1	216.6	(136, 255, 255)
M	(255, 0, 255)	147.9	153.4	154.0	(255, 24, 255)
Y	(255, 255 ,0)	243.1	249.0	249.0	(255, 255, 120)

Table 5: 6127 Color–Grayscale mapping.

Color	RGB Value	Mean Intensity	Target Intensity	Actual Intensity	Adjusted RGB Value
R	(255, 0, 0)	156.2	121.2	124.2	(127, 0, 0)
G	(0, 255, 0)	155.1	152.7	155.1	(0, 255, 0)
B	(0, 0, 255)	105.4	89.8	89.8	(0, 0, 135)
C	(0, 255, 255)	159.2	215.5	217.9	(168, 255, 255)
M	(255, 0, 255)	147.7	184.1	183.8	(255, 120, 255)
Y	(255, 255, 0)	240.7	246.9	246.9	(255, 255, 120)

Table 6: 6280 Color–Grayscale mapping.

In Table 11, the GPC deterrent test sheets are re-scanned and authenticated in color using L1 distance in 3-dimensional RGB space. For this test, 100% authentication is obtained for all printers and all tile sizes.

Color	RGB Value	Mean Intensity	Target Intensity	Actual Intensity	Adjusted RGB Value
R	(255, 0, 0)	154.2	120.0	123.1	(151, 0, 0)
G	(0, 255, 0)	152.3	152.1	152.3	(0, 255, 0)
B	(0, 0, 255)	119.9	88.0	88.0	(0, 0, 135)
C	(0, 255, 255)	157.4	216.1	215.2	(160, 255, 255)
M	(255, 0, 255)	146.2	184.1	182.1	(255, 104, 255)
Y	(255, 255, 0)	240.9	248.2	248.2	(255, 255, 120)

Table 7: 6940 Color–Grayscale mapping.

	Histogram Intersection			Mean Intensity Absolute Difference		
Tile Size	Passed/Total	Accuracy	Mean Tile Errors	Passed/Total	Accuracy	Mean Tile Errors
10	3/117	2.564%	4.447	1/117	0.855%	5.509
11	7/117	5.983%	2.836	1/117	0.855%	3.819
12	23/108	21.963%	1.671	12/108	10.256%	2.104
13	67/108	62.037%	1.439	38/108	35.185%	1.900
14	96/96	100.000%	0	93/96	96.875%	1.000
15	96/96	100.000%	0	95/96	98.958%	1.000

Table 8: 6127 Grayscale Tile Authentication Results

For the fourth experiment set, green was identified as the color with the highest tile misclassification rate. This color was eliminated from the set of 6 colors, and the grayscale intensity space was divided into equally spaced target intensities. Deterrent test sheets were then generated by selecting the appropriate color values from the HP 6127 color–grayscale LUT. The authentication results of the 5-color deterrents are summarized in Table 12.

Based on the tile misclassification rates of the 5-color deterrents, the color red was eliminated from the color set. The colors {BCMY} were used for the 4-color deterrent test sheets. Table 13 summarizes the authentication results for the 4 color deterrent test sheets.

5. DISCUSSION

As can be seen from the results of the first experiment, implementing GPC can significantly improve grayscale authentication accuracy. Looking at the confusion matrix of Table 4, which contains the aggregate tile classification results, it is clear that significant misclassification occurs between R, G, C, and M. These findings are supported by the mean intensity values obtained from the color calibration sheets for each of the colors at full saturation. Column 3 in Table 7 lists the mean intensities for the colors. While B and Y are distinctly separable at full saturation, {RGCM} are all clustered within a range of 8 for grayscale intensity values. By increasing the separation, the authentication accuracy jumped from 0% to 98.958%. Figure 5 gives examples of two tile deterrents; one without GPC and the other with GPC. As can be seen in Figures 5a and 5b, when the color tile deterrent has no GPC, the colors {RGCM} are visually indistinct from each other in grayscale. When GPC is implemented, as seen in Figures 5c and 5d, the individual tiles are considerably more distinct in grayscale.

The results from the second experiment, in which GPC is tested over three printers and tile sizes ranging from 10 to 15 pixels, is a bit more complex than the results of our first experiment. Clearly, the results in Tables 8, 9, and 10, indicate a downward trend for authentication accuracy with respect to tile size regardless of which authentication algorithm is used. Even so, the mean tile errors per failed deterrent is still quite low. Even at size 10 for the HP 6127, which based on the results is the worst performing of the three printers evaluated, the mean tile error is only 5.509 when mean grayscale intensity absolute difference is used for authentication. Recalling that the tile deterrent feature has 56 payload tiles, this means that on average 90.2% of the individual tiles were read correctly in a deterrent which failed overall authentication. Since in our approach ECC was not implemented, we required 100% read accuracy for an overall deterrent to pass authentication. However, it is clear that with the addition of a suitable ECC rate, even the smallest tile-sizes could be used to create a readable deterrent.

	Histogram Intersection			Mean Intensity Absolute Difference		
Tile Size	Passed/Total	Accuracy	Mean Tile Errors	Passed/Total	Accuracy	Mean Tile Errors
10	56/117	47.863%	1.541	6/117	5.128%	5.171
11	79/117	67.521%	1.263	16/117	13.675%	3.624
12	98/108	90.741%	1.000	34/108	31.481%	3.027
13	105/108	97.222%	1.000	58/108	53.704%	2.760
14	95/96	98.958%	1.000	45/96	46.875%	2.118
15	95/96	98.958%	1.000	54/96	56.250%	1.881

Table 9: 6280 Grayscale Tile Authentication Results

	Histogram Intersection			Mean Intensity Absolute Difference		
Tile Size	Passed/Total	Accuracy	Mean Tile Errors	Passed/Total	Accuracy	Mean Tile Errors
10	81/117	69.231%	1.417	48/117	41.026%	1.536
11	100/117	85.470%	1.353	72/117	61.538%	1.333
12	98/108	90.741%	1.400	82/108	75.926%	1.385
13	104/108	96.296%	2.000	90/108	83.333%	1.278
14	94/96	97.917%	1.500	80/96	83.333%	1.250
15	95/96	98.958%	1.000	87/96	90.625%	1.000

Table 10: 6940 Grayscale Tile Authentication Results

	Authentication Accuracy		
Tile Size	6127	6280	6940
10	100%	100%	100%
11	100%	100%	100%
12	100%	100%	100%
13	100%	100%	100%
14	100%	100%	100%
15	100%	100%	100%

Table 11: Authentication results for all three printers when the GPC tile deterrent test sheets are scanned and authenticated in color RGB space.

Based on inspection of the misclassified tiles from the failed deterrents, we were able to identify several trends which we believe cause failures:

- Ink bleed from one neighboring tile into another tile
- Pen misfire - no ink
- Pen drool/spatter
- Color plane mis-registration
- Halftone non-uniformity

Of the four items listed, problems with halftoning were the worst. We believe the reason for this is that when a small size image such as a 10 by 10 pixel color tile is printed, the printer is unable to correctly implement the required halftoning pattern in a limited area. Our approach to GPC involved taking fully saturated colors and modifying the intensity of the colors to increase the separation in grayscale intensity. The way this shift in intensity is obtained by the printer is to either withhold ink in the case of lighter intensities, or to add black dots to darken the overall intensity. When this is combined with ink bleed from neighboring tiles, tile classification becomes less accurate regardless of which authentication algorithm is used. Figures 6 and 7 give example tiles in which the above mentioned problems occur. Larger tile sizes are able to get around these problems since, after cropping, a large enough amount of tile area remains such that a representative sample size of pixels can still be obtained.

As indicated in the results of experiment 3, when GPC tile deterrents are authenticated in RGB color space we are still able to obtain 100% authentication across all tile sizes. These results show that GPC does not interfere with authentication in color RGB space. Additionally, the results support the objective of being able to authenticate the color tile deterrent in two modes; color and grayscale.

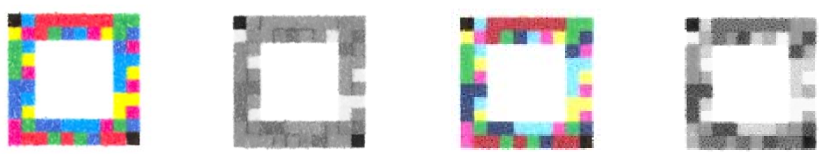
It is of interest that authentication rates are fully accurate in color but not in grayscale, especially since the same prints, with the above mentioned problems are used in both experiments. However, when taking the approach into account this discrepancy in authentication accuracy can be explained. In color space, each (r,g,b) triplet value maps to exactly one color representation and authentication takes place in this 3-dimensional space. In grayscale however, we are working with a 1-dimensional representation which is the resulting value of a remapping from 3-dimensional space down to 1-dimensional space. As can be seen in Tables 5, 6, and 7, the mean grayscale intensities of different colors can remap to approximately the same grayscale intensity. Indeed, when a larger color set is explored numerous color values can and will map to the same grayscale intensity value. This loss of information in reducing the dimensionality therefore is a contributing factor to the differences in classification between color and grayscale.

	Histogram Intersection			Mean Intensity Absolute Difference		
Tile Size	Passed/Total	Accuracy	Mean Tile Errors	Passed/Total	Accuracy	Mean Tile Errors
10	67/117	57.3%	1.780	56/117	47.9%	1.689
11	93/117	79.5%	1.167	78/117	66.7%	1.231
12	95/108	87.6%	1.462	94/108	87.0%	1.214
13	105/108	97.2%	1.000	101/108	93.5%	1.000
14	96/96	100%	0	96/96	100%	0
15	96/96	100%	0	96/96	100%	0

Table 12: 6127 Five Color Grayscale Tile Authentication Results

	Histogram Intersection			Mean Intensity Absolute Difference		
Tile Size	Passed/Total	Accuracy	Mean Tile Errors	Passed/Total	Accuracy	Mean Tile Errors
10	110/117	94.0%	1.571	99/117	84.6%	1.222
11	117/117	100%	0	104/117	88.9%	1.154
12	108/108	100%	0	102/108	94.4%	1.000
13	108/108	100%	0	108/108	100%	0
14	96/96	100%	0	96/96	100%	0
15	96/96	100%	0	94/96	97.9%	1.000

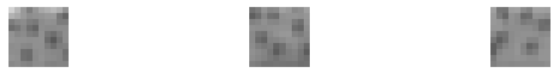
Table 13: 6127 Four Color Grayscale Tile Authentication Results



(a) (b) (c) (d)

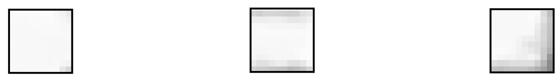
Figure 5: Non-GPC and GPC color tile deterrents (enlarged for legibility). Individual tiles are significantly more visually separable in grayscale when GPC is utilized. (a) color scan non-GPC deterrent, (b) grayscale scan non-GPC deterrent, (c) color scan of GPC deterrent, and (d) grayscale scan of GPC deterrent.

When the number of colors used in the tile deterrent is reduced, this issue of misclassification is reduced as well. The results of experiment 4 support these findings. As seen in Table 12, when 5 colors are used in the tile deterrent the overall authentication accuracy increases for both grayscale authentication approaches. When the color set is again reduced, as seen with the 4-color tile deterrent results in Table 13, 100% grayscale authentication accuracy is obtained at tile size 11 using histogram intersection. Comparatively, for the 6-color tile deterrent, the grayscale authentication accuracy using histogram intersection for tile size 11 was only 5.983%. This is a significant improvement which can be attributed to the increase in separation between a grayscale value and the next nearest value. The tradeoff, however, is the reduction in payload from 144.8 bits ($56*\log_2(6)$) to 112 bits ($56*\log_2(4)$). But if bandwidth is a limiting factor for image capture, then this approach clearly has its advantages.



(a) (b) (c)

Figure 6: Grayscale images of red color tiles (magnified 20x). Note the differences in pixel placement from the halftoning algorithm. Original tile size is 10 pixels by 10 pixels at 600 ppi.



(a) (b) (c)

Figure 7: Grayscale images of yellow color tiles (magnified 20x). Note the differences in bleed that have occurred from different neighboring tiles. Original tile size is 10 pixels by 10 pixels at 600 ppi.

6. CONCLUSION

Implementation of GPC can be an effective strategy to allow for deterrent authentication in reduced bandwidth applications. In scenarios in which package or label real estate is not a limiting factor, deploying the color tile deterrent at a tile size of 15 allows for a full set of 6 colors to be utilized in the deterrent. In scenarios in which the amount of available area is limited on a package or label, a reduced color set can be used with the color tile deterrent to allow for authentication in grayscale at smaller tile deterrent sizes. The deployment of GPC can also be seen as a complimentary strategy which can be used in parallel with color authentication thereby enabling two modalities of authentication for the same deterrent.

In our implementation of GPC, our authentication mechanism focused on utilizing one of two possible approaches; mean intensity absolute difference or intensity histogram intersection. Overall, histogram intersection outperformed absolute difference since the histogram retained more detailed information about a tile rather than a single scalar value as used with mean intensity. Future work will focus on identifying other methods for representing a grayscale tile so that more information can be retained and utilized to increase classification accuracy. Other research groups [8 -10], have used texture metrics as a means of classifying an image patch. In [8], Gabor filters were used to extract texture descriptors from images ranging in size from 8 x 8 pixels to 256 x 256 pixels. However, the classification error for the 8 x 8 pixel image samples exceeded 40% and the error for 16 x 16 pixel images was above 30%. In [9], local binary patterns (LBP) were utilized as a method for obtaining grayscale texture descriptors which were combined with histogram information to fully describe an image. While the sample sizes used were as small as 16 x 16 pixels, histograms used for training data were comprised of multiple samples rather than a single sample per class as used in our approach with NPI tiles. In [10], LBP was also utilized and the classification accuracy was as high as 98.6%. However, the smallest image sizes used for classification were 128 x 128 pixels. Neither [8], [9], nor [10] dealt with samples which had problems with ink bleed from neighboring samples.

As stated earlier, when the size of the tile deterrent is reduced the accuracy drops. This is due in part to the reduced area available for classification, which after cropping can become quite small. In the case of a 10 x 10 pixel tile, the remaining area after cropping is 7 x 7 pixels. Whether this provides enough information for texture is, to the best of our knowledge, still an open research question. Since a contributing factor to the misclassification of tiles was due to halftoning, extracting the texture of halftone patterns might provide additional data points that could aid in improved tile classification. If these additional texture metrics can be extracted to provide additional features for representation of a tile, we may be able to further reduce the tile size while maintaining full authentication accuracy.

REFERENCES

[1] Simske, S.J., Aronoff, J.S., and Sturgill, M. "Spectral Pre-Compensation of Printed Security Deterrents." In *Optical Document Security*. Reconnaissance International, January 2008.

[2] Simske, S.J., Sturgill, M., and Aronoff, J.S. "Spectral Pre-Compensation and Security Print Deterrent Authentication." In *NIP24: International Conference on Digital Printing Technologies and Digital Fabrication* 2008, pp. 792–795. IS&T, September 2008.

[3] Parikh, D. and Jancke, G. "Localization and Segmentation of A 2D High Capacity Color Barcode." In *Proceedings of the 2008 IEEE Workshop on Applications of Computer Vision*, pp. 1-6. IEEE Computer Society, January 2008.

[4] High Capacity Color Barcodes – Microsoft Research. http://research.microsoft.com/en-us/projects/hccb/default.aspx (last visited November 2009).

[5] Bulan, O., Monga, V., and Sharma, G. "High capacity color barcodes using dot orientation and color separability." In *Proc. SPIE-IS&T Electronic Imaging: Media Forensics and Security*, vol. 7254, p. 725417(7). SPIE, 2009.

[6] Swain, M.J. and Ballard, D.H. "Color indexing." *International Journal of Computer Vision*, vol. 7, no. 1, pp. 11–32, November 1991.

[7] Pietikainen, M., Nieminen, S., Marszalec, E., and Ojala, T. "Accurate Color Discrimination with Classification Based on Feature Distributions." In *13th International Conference on Pattern Recognition*, vol. 3, pp. 833-838. IEEE Computer Society, 1996.

[8] Puzicha, J., Buhmann, J.M., Rubner, Y., and Tomasi, C. "Empirical Evaluation of Dissimilarity Measures for Color and Texture." *IEEE International Conference on Computer Vision*, vol. 2, pp. 1165-1173. IEEE Computer Society, September 1999.

[9] Ojala, T., Pietikainen, M., and Maenpaa, T. "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, num. 7, pp. 971-987. IEEE, July 2002.

[10] Maenpaa, T., and Pietikainen, M. "Classification with color and texture: jointly or separately?" *Pattern Recognition*, vol. 37, num. 8, pp. 1629-1640. Elsevier Ltd, August 2004.