Staggered and Dual-Channel Barcodes

Steven J. Simske, Hewlett-Packard Labs, 3404 E. Harmony Rd., MS 36, Fort Collins CO 80528, USA
Guy Adams, Hewlett-Packard Labs, 3404 E. Harmony Rd., MS 36, Fort Collins CO 80528, USA
Jason S. Aronoff, Margaret Sturgill, Marie Vans, Hewlett-Packard Labs, 3404 E. Harmony Rd., MS 36, Fort Collins CO 80528, USA

Abstract

We have previously described the printing of information in 2D color (or "3D") barcodes for subsequent reading with scanners and/or mobile cameras. In this paper, we describe how color tiles can be used in different aggregations (single tiles, 2x2 pairings of tiles, 3x3 pairings of tiles, etc.) to provide data that is readable by a wide array of imaging devices. High-end devices such as scanners and line cameras will accurately read each individual (small) module, or tile, in the barcode, while less expensive cameras, such as cameras in mobile phones, will only be able to accurately read clusters of the tiles (e.g. 2x2 module "aggregations") at a time. We address this by using a novel type of error-correcting code, the CET (chroma-enhancing tile), which reduces the payload density by 25% for a 2x2 pairing, but allows 2x2 pairings to reliably map to the same set of colors—usually {RGBCMY}—as the original (single) modules. This makes the color barcodes readable to a wide array of imaging devices.

In addition, we describe in this paper how the use of three or more colors—optimally the six colors {RGBCMY}—enables a "dual-channel" authentication approach, with a second novel type of error-correcting code—the color-multiplicity-to-color-axis mapping (CMCAM)—enabling a different interpretation of the colors in the barcodes to suit the color capabilities of the imaging device. Our data show that, in some cases, authentication with a CMCAM-reduced palette can actually increase payload density for some imaging devices.

Keywords: Color Barcodes, Mobile Imaging, Track and Trace, Authentication

Introduction

Variable data security printing is used to simultaneously provide unique serialized data and authentication information. Authentication is the reading by a sensor and the embedded information is decoded—serving purposes in product identification, track and trace, and/or brand protection. However, authentication is a complicated process, dependent on print quality (and thus substrate and ink), sensitivity/resolution of the sensor—and in the case of image-based authentication, the optics of the reader, the distance between the reader and the deterrent, the lighting conditions, etc. [1][2].

As such, many visual security printing deterrents are designed for authentication with a specific reader (bar code readers are an example of this). When not, they may instead rely on the human observer to authenticate them (e.g. OVDs, or optically-varying devices, such as holograms use this approach). Finally, deterrents may be verified with a reader that is capable of authenticating it under most conditions—this may result in either high reader cost (if "extra" reading capability is targeted) or the inability to authenticate deterrents under various conditions (if a less expensive reader is used).

Thus, what is needed is a deterrent that can be authenticated irrespective of the quality of the image obtained. The information density of such an authentication scales to the quality of the image. Higher quality images are authenticated at full "deterrent density", while lower quality images are authenticated with a correlated, staggered reduction of "deterrent density". Through this method, a diverse population of authentication customers and devices can be used to provide point-to-point location record, or provenance, of an item. Lower deterrent densities can be directly linked to higher deterrent densities in the supply chain or other point-to-point transmission path.

To accommodate this need, we use color barcodes because of the increased density of information – and thus increased density of reading options – in comparison to binary barcodes of color based marks [3][4]. The color tile deterrent uses a multiplicity, M, of colors, to provide $ln(M)/ln(2)$ bits of information per data tile (ignoring error-correcting and/or calibration tiles). Color information can be encoded in a wide variety of set sizes. The standard color tile uses M=6, and the color set is {CMYRBG}, or cyan, magenta, yellow, red, blue and green.

As an additional advantage of color based barcodes, we herein show that a printed deterrent can be simultaneously read assuming different values for M. In some cases, assuming a lower value for M can increase payload density; in addition, this "dual channel" approach can provide the means to convey security information for a (potentially large) plurality of reading (scanning) devices which themselves have different imaging capabilities – in terms of resolving power, actual bits of contrast, color integrity/consistency, etc. This provides some level of security irrespective of the presence of high-quality reading devices. Additionally, since each M-channel (channel defined by the number, M, of different colors identified per tile) has a different error rate (and in most cases, error type), each M-channel can use its own error-correcting code (ECC) strategy. This allows the same set of tiles to encode two or more distinct security strategies simultaneously in the same "deterrent", or printed region.

Methods and Materials

Staggered Color Tiles

As noted, color tiles [4] consist of six data-carrying colors: red (R), green (G), blue (B), cyan (C), magenta (M) and yellow (Y). A common implementation of color tiles, which leaves white space in the middle for printing a 2D barcode or other secondary marks, is shown in Figure 1. In this implementation, two black (K) tiles and one of each of the six color squares are placed in the upper left and lower right corners to aid in registration (these are

called non-payload indicia). White (W) also surrounds the color tile deterrent and is used for segmentation purposes.

Figure 1*. Color tile deterrent with 56 payload indicia and 8 non-payload indicia (KCYM in upper left corner and GBRK in lower right corner).*

The color tile mark therefore uses non-payload indicia (NPI) rather than error-correcting code (ECC) to provide authentication robustness (Figure 1) while providing high payload density (PD), in units of bytes/inch^2. When there are six color possibilities for each payload indicia (PI), the PD is equal to ($ln(6)/ln(2)$)*n(PI)/8, where n(PI) is the number of payload indicia in 1.0 inch^2. In the deterrent of Figure 1, eight tiles are used to provide orientation and color calibration. Two K tiles provide "Northwest-Southeast" calibration, and the neighboring CMY ("Northwest") and RGB ("Southeast") color calibration tiles are used for 180 degree disambiguation. Note that the color opponency pairings (R-C, B-Y and G-M) are 180 degrees apart (circles in Fig. 1, right), providing the greatest possible color differences for the NPI for robustness of orientation detection. Since 8 NPI are used for the 10x10 (or 100 total) tile area, PI/(PI+NPI) = 0.92 for this deterrent—that is, 92% of the area of the deterrent is used for payload (if we filled in the white space with more PI tiles).

The PD description above is based on two assumptions: (1) all individual tiles can be read, and (2) the colors are consistent across the deterrent. The former is aided by using pre-determined tile dimensions, while the latter is aided by uniform lighting and relatively compact deterrent size (or high quality capture, such as with a scanner or vision system). However, these assumptions often fail in the mobile world.

Here we provide a few definitions:

1. A **tile** is a uniformly colored glyph, nominally a square, from which the overall deterrent is constructed.

2. A **cell** is the largest set of tiles that can be individually authenticated by any reading device. As an exemplar (Figure 2), we define herein a 4 x 4 set of tiles to be this cell.

3. A **deterrent**, or mark, is the complete set of cells, combined to form the color tile security feature. For purposes of illustration, we define the deterrent to be an NxN array of cells. For further illustration, we make N an integral multiple of 4, so that the deterrent can be entirely tiled by 4x4, 2x2 and 1x1 sized clusters of tiles.

4. A **cluster** is any PxP set of tiles from the size of an individual tile (1x1 cluster) to the size of a cell (e.g. 4x4 cluster). Power-of-two cluster sets like the ones illustrated here will line up with the cells such that no clusters overlap more than one cell.

In terms of size,

Tile <= Cluster <= Cell <= Deterrent

Figure 2 shows a 16 x 16 tile deterrent, with 1x1, 2x2 and 4x4 clusters organized such that there is repeated structure in 8x8 blocks, as described next.

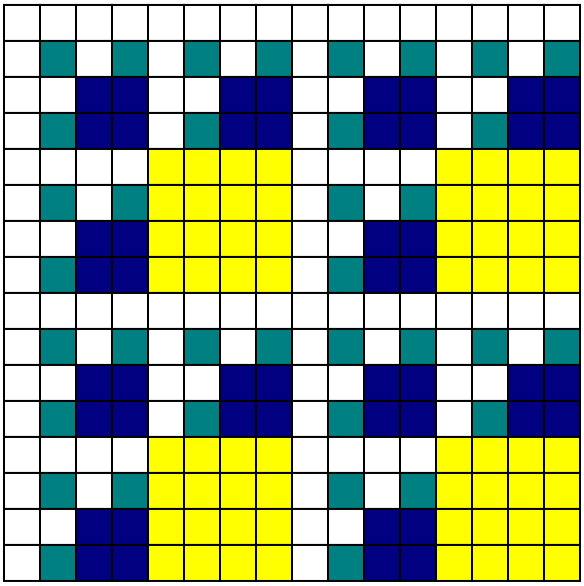

Figure 2*. Example of "staggered" color barcodes deterrent, where the white tiles are the PI tiles and the colored (non-white) tiles are used for chroma-enhancement to allow multiple-reader or "staggered" reading.*

In Figure 2, the white tiles are the payload indicia (PI). These PI tiles, when deployed, would contain one of the allowed set of colors that convey information, e.g. {RGBCMY}. The teal-colored tiles (1x1 non-white clusters) in the following deterrent examples represent what we term the chroma-enhancing tiles, or CETs. Chroma-enhancing tiles are used to direct what hue the successively larger clusters will be authenticated as. The 2x2 tile cluster in the upper left, for example, consists of three PI tiles and one CET. Suppose the three PI tiles, for example, are red, magenta and green (R,M,G). In terms of the red, green and blue channels, R={255,0,0}, M={255,0,255} and G={0,255,0}, so the sum is {510,255,255}. To enhance the chroma of the 2x2 cluster, therefore, we set the CET to R={255,0,0} and so the 2x2 cluster comes to {765,255,255} which is overwhelmingly red. The same approach is used for the larger 4x4 and 8x8 clusters (the 2x2 and 4x4, respectively, CETs, are also a single color).

In general, when the final deterrent is an NxN deterrent, and N=2M for some integer M, then the following are true:

1. The final number of independent tiles when the deterrent has been specified at every power of 2 from 0 to M is $(¾)^M * 2^{2M}$.

2. All remaining CETs are the final authority for the cells they monitor. Thus, remaining teal, blue and yellow CETs in Figure 2 enhance the chroma for their respective 2x2, 4x4 and 8x8 cells, irrespective of the presence of the larger CETs added to the deterrent.

Dual Channel Color Tiles

The color tile-based deterrent (Figure 1) uses six colors {RGBCMY}, reserving white and black for background and NPI,

respectively. This is because these colors are the furthest apart in 3D {r,g,b} color space, as shown in Figure 3.

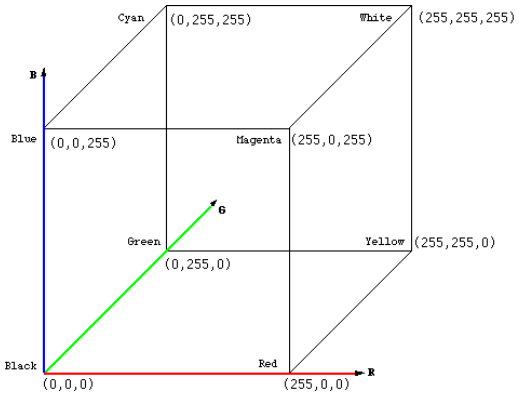

***Figure 3**. Location of the six color tile colors (RGBCMY) along with white and black on the 3D color space.*

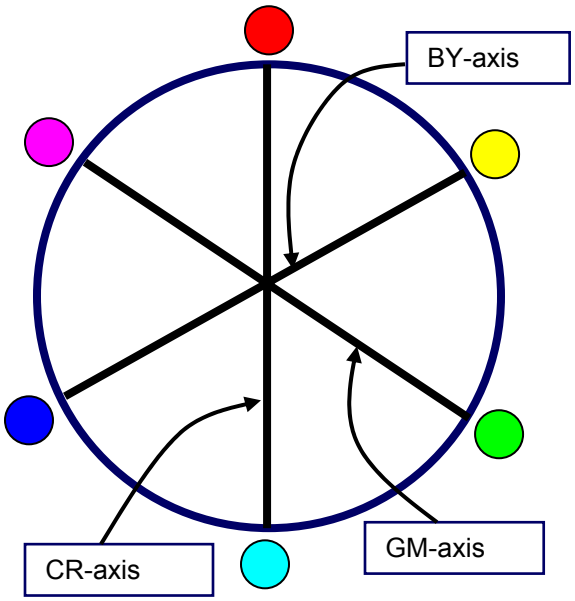

***Figure 4**.Color axes obtained by representing the 3D color space in 2D.*

The three color axes (Figure 3) comprise the following color-opponency pairs: red-cyan (RC), blue-yellow (BY) and green-magenta (GM) when we map the 3D color space to a circular color space representation (Figure 4). Using this approach, each color tile can be authenticated along one of the three color-opponency pair axes, and so the color tiles provide 3N possible device signatures, where N=number of tiles, with a reduction in payload from 2.6 bits/tile to 1.0 bits/tile.

This "surfeit" of colors in each tile can be used for another purpose—that of providing additional robustness to read-error through higher allowed color-distance error. If, for example, a R tile is being authenticated using the R-C axis, then any color read as M, Y or R will be classified as R. Thus, using a color-opponency axis allows ≤ 90º error in hue (see Figure 4) as opposed to a limit of ≤ 30º error in hue for six-color authentication (a three-fold increase in color error sensitivity for a 2.6-fold reduction in payload density). Table 1 describes the mapping between 6 colors and the three different approaches to color-axis authentication.

Table 1. Representation of color tiles when authentication of each of the six colors (CMYRGB) is along one of the three color axes

Tile Color	BY axis	CR axis	GM axis
R	Y	R	M
G	Y	C	G
B	B	C	M
C	B	C	G
M	B	R	M
Y	Y	R	G

This increased insensitivity to color error, of course, results in increased authentication accuracy for smaller tiles. To show this, we use the piecewise linear fit to the measured authentication data to estimate 100% authentication accuracy as shown in Figure 5 [4]. The size of tile for 100% accuracy is designated X2. The security payload density (SPD) at full Authentication (fA)—that is, at X2—for the piecewise linear (PL) fit, is designated SPD-fA-PL, and generally corresponds to 99.9% tile accuracy.

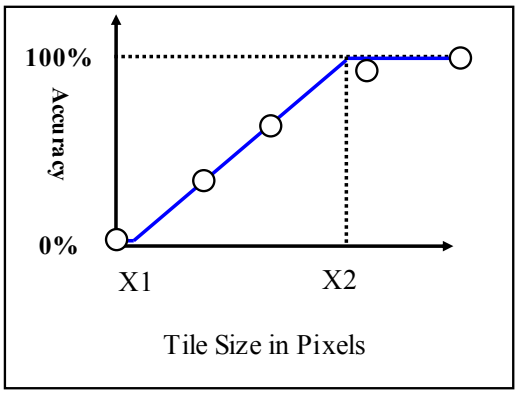

***Figure 5**. General piecewise-linear model for authentication accuracy (blue line segments) and actual data (circles). Originally described in [4].*

For 6-color authentication

$$SPD - fA - PL = \frac{\ln(6)}{\ln(2)} * \frac{PI}{(PI + NPI)} * \frac{byte}{bits} * \frac{DPI^2}{X2^2}$$

$= 2.585*(56/(56+8))*(1/8)*600^2/(X2)^2 = 101782.9/(X2)^2$. For the 2-color authentication,

$$SPD - fA - PL = \frac{PI}{(PI + NPI)} * \frac{byte}{bits} * \frac{DPI^2}{X2^2}$$

$= (56/(56+8))*(1/8)*600^2/(X2)^2 = 39375/(X2)^2$.

Results

Staggered Color Tiles

Spectral pre-compensation [4], or SPC, has been introduced as a means to improve PD. The strategy involves printing an appropriate set of target colors, scanning them and selecting the colors from this set that, *after printing and scanning*, result in the intended color set, {RGBCMY} (e.g. 60 degrees apart depicted by the circles in Figure 4). The selected colors are then used as a replacement for the original {RGBCMY} set. The authentication approach used herein assigns the color of each tile based on the minimum of the angular distance of the hue of the tile sub-segment and the hues of the six color NPI. That is, the minimum absolute hue difference between the tile sub-segment's mean {r,g,b} value and the hue of the NPIs' {**r,g,b**} values assigned that NPI's color to the tile. Hue angle of {R,Y,G,C,B, and M} is {0,60,120,180,240, and 300}, although the actual colors after scanning are somewhat different (note, though, that spectral pre-compensation preserves the 60 degree separation between the 6 colors). Spectral pre-compensation is important for staggered (multi-imaging device based) authentication, as it allows the CETs to be more effectively targeted. Regardless, a 216 element look-up table is used to map each CET to each triad of PI tiles, as described for R+M+G above.

Dual Channel Color Tiles

We tested the values for X2 and the corresponding SPD-fA-PL in bytes/in^2 using the HP 6280 thermal inkjet all-in-one for printing and scanning. Table 2 shows the X2 values for the original prints and after 1 or 2 copies. We have previously [5] found robustness to copying to significantly increase with spectral pre-compensation. Our results here support this.

Table 2. SPD-fA-PL values (bytes/in2), 99.9% per-tile accuracy

Test	No Spectral Pre-Compensation	Spectral Pre-Compensation
6-color, Original	1200	1910
2-color, Original	1300	2460
6-color, Copy #1	610	1020
2-color, Copy #1	590	830
6-color, Copy #2	200	580
2-color, Copy #2	340	470

Table 2 shows the results for SPD-fA-PL in bytes/in^2 when there is no image restoration, nearest-hue authentication is used, and with and without spectral pre-compensation.

Discussion and Conclusions

Staggered Color Tiles

Staggered color tiles as illustrated herein provide the means to read, simultaneously, 1x1 tile clusters with high-resolution, high-quality imaging devices, and 2x2, 4x4 and 8x8 clusters with progressively lower quality imaging devices. Devices acceptable for each of these sizes may be, for example, a scanner (1x1), an in-line inspection camera (2x2), a digital camera (4x4) and a mobile phone camera (8x8). Our tests have shown desktop scanners capable of reading tiles 250 microns on a side, while some phone cameras require tiles 2500 microns on a side.

Dual Channel Color Tiles

Table 2 shows the broad effectiveness of spectral pre-compensation for improving payload density (PD). For both 6-color and 2-color authentication, and even after one or two copy cycles, spectral pre-compensation greatly increases PD. Also interestingly, authentication along 2-color axes often increases the payload density. This illustrates the fact that the multiple channels, in this example 2-color and 6-color, can be encoded independently, and use different ECC approaches/amounts. For the color tile deterrent illustrated in Figure 1, such ECC could be implemented in a plurality of ways, including:

(1) Using some of the payload tiles to encode ECC for the 6-color implementation, and using some of the payload tiles to encode ECC for the more accurate 2-color implementation.

(2) Vice versa of (1).

(3) Using some of the whitespace within the deterrent to encode ECC for the 6-color implementation, and using some of the whitespace within the deterrent to encode ECC for the more accurate 2-color implementation.

(4) Vice versa of (3).

Conclusion

The staggered and dual channel approaches outlined in this paper illustrate how color bar codes can be useful in enabling an ecosystem of imaging devices to participate in product authentication and thus supply chain integrity. The staggered approach enables most imaging devices to provide some level of authentication, with a modest loss in payload density – generally less than error-correction coding (ECC). Thus, staggered approaches provide an "alternative" error-correcting approach. Dual channel approaches, on the other hand, allow for alternative means of optimizing payload density while offering further options for ECC.

References

[1] S.J. Simske and J.S. Aronoff, "Qualification of a layered security print deterrent," JIST, 51(1):86-95 (2007).

[2] 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," JIST, 52(5):50201:1-7 (2008).

[3] R. Villán, S. Voloshynovskiy, O. Koval and T. Pun, "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).

[4] S.J. Simske, J.S. Aronoff, M.M. Sturgill and J.C. Villa, "Spectral pre-compensation and security deterrent authentication," Proc. NIP24, 24:792-795 (2008).

[5] S.J. Simske, M. Sturgill and J.S. Aronoff, "Effect of copying and restoration on color barcode payload density," Proc. ACM DocEng 2009 127-130 (2009).

Author Biography

Steve Simske is an HP Fellow and the Director and Chief Technologist of the Document Lifecycle & Security Printing & Imaging portfolio in Hewlett-Packard Labs. Steve is currently on the IS&T Board. He is also an IS&T Fellow and a member of the World Economic Forum's Global Agenda Council on Illicit Trade. He holds more than 40 US patents and has more than 250 peer-reviewed publications. He holds advanced degrees in Biomedical, Electrical and Aerospace Engineering