Image-based Data Interfaces Revisited: Barcodes and Watermarks for the Mobile and Digital Worlds

(Invited Paper)

Gaurav Sharma
Dept. of Electrical and Computer Engineering
University of Rochester, Rochester, NY 14627-0126
Email: g.sharma@ieee.org

***Abstract*—The ubiquitous availability of image sensors in smartphones and other mobile computing devices makes feasible new applications for both barcodes that encode data as image patterns and watermarks that hide data in images. To support these new applications, a number of new methods have been developed for these long-standing image-based data communication interfaces, methods that are better suited for use with the image sensors. In this paper, we review these developments and the applications they enable, drawing upon examples from our own prior work in this area. We highlight key attributes that distinguish these image-based communications interfaces from other noncontact modes of communication and make their continued use an attractive option.**

I. Introduction

Images have long been used to communicate not only their "literal" visual content but also data encoded as visual representations. Since the invention of written language, humans have learned how to encode words, alphabets, and digits as visual patterns and to decode such encodings. It is no wonder then that several of the earliest methods for communicating over relatively longer distances were also based on visual encodings, starting out as fire, smoke, and flag signals and evolving into the relatively sophisticated semaphore signals still used by a number of railways around the world [1]. In modern times, several of the uses of such communication systems have been subsumed by electrical or electromagnetic signaling technologies operating either over connection media or, increasingly, wirelessly over free space. However, *image-based data interfaces*, which "bridge across the analog gap" by embedding digital data in rendered imagery which is captured by image sensors and utilized to recover the embedded digital data, continue to play key roles in today's world because of their advantageous attributes and because image sensors have become ubiquitous and inexpensive owing to their widespread use in smartphones.

In this paper, we review several of the techniques used for modern image-based data interfaces and the applications enabled by such interfaces. We focus particularly on the two main flavors of machine-readable image-based data interfaces: barcodes that encode data as image patterns for easy machine readability and digital image watermarks[1] that hide data within an image without impacting the primary functionality of the image. Both of these are seeing extensive use in mobile applications because of their ability to interconnect the physical and cyberworlds and the ready availability of image sensors in smartphones, already alluded to earlier.

This paper is organized as follows. In Section II, we highlight some of the common techniques used for communication with image-based data interfaces and illustrate some of their ingredients using illustrative examples from our own prior work. In Section III, we discuss applications, both existing and emerging, for these technologies, again drawing upon examples from our prior work for specific demonstrations. In Section IV, we summarize several of the attributes of image-based data interfaces and contrast these with alternative technologies that address similar applications. Section V concludes the paper with some summarizing remarks.

II. Techniques

As already indicated, we use the term *image-based data interface* to describe methods that embed digital data within imagery and decode the data from images captured from analog renditions of the imagery, in display or print. The bridge that such methods provide across the analog gap serves a useful function by connecting between the physical world in which the analog rendition resides and the cyberworld where the digital data can be understood and acted upon. We restrict our attention here primarily to image-based data interfaces for print, only peripherally mentioning display versions in the context of applications.

Barcodes have long been used as image-based data interfaces for tagging objects with machine readable digital identifiers for automation of store checkout and inventory tracking in the retail industry and for other workflow tasks. Figure 1 illustrates some of the commonly used versions of barcodes: the universal product code (UPC)1 [2] of Fig. 1(a) is extensively used for product labeling for checkout and tracking in stores; the quick response (QR) code [3] of Fig. 1(b) is a common 2D barcode used with smartphones to connect users to a website with additional information for a product, event, etc; the Aztec code [4], [5] of Fig. 1(c) is common in transportation applications for encoding air/rail ticket information on tickets or boarding passes for easy machine readability, and the the Data Matrix [6], [7] code of Fig. 1(d) is common in factory automation settings for part location and tracking. With the wide-spread availability of cameras in smartphones,

[1]Because image watermarks can also be visual patterns, we use the term *image-based data interface* instead of simply referring to these as barcodes and watermarks.

978-1-4673-9622-6/16/$31.00 ©2016 IEEE

(a) UPC (b) QR

(c) Aztec (d) Data Matrix

Fig. 1. Common barcodes: (a) UPC (b) Quick Response (QR), (c) Aztec, and (d) Data matrix. The latter three, each encode the COMSNETS URL.

there is now an increasing number of applications that read barcodes on smartphones. Driven by the widespread smartphone adoption, the cost of image sensors has also fallen dramatically and specialized scanners for 1D barcodes, such as the laser scanners traditionally used to read UPC codes, have also been largely replaced by new designs incorporating image sensors. Both the 1D and the 2D barcodes include, within their designs, elements for ready localization of the barcode within a captured image, for synchronization, and for ensuring integrity of the recorded information using error correction coding. For instance, for the QR code in Fig. 1(b), the three distinctive square blocks on three of the corners, each made up of a solid square enclosed by a hollow one, serve to readily localize the barcode region within a captured image and allow for correction of perspective geometric distortion introduced due to the capture of the barcode from a position other than the optimal fronto-parallel orientation. Combined with the additional smaller hollow square closer to the fourth corner, these squares also allow synchronization by determining the location of the individual bit-carrying "modules," which are the smaller square elements that make up the barcode and are black or white based on the bit they carry. The payload data for the barcode is protected by a Reed-Solomon code [8], [9]. The QR code standard [3] allows for various levels of redundancy based on the expected operating environment for the barcode.

Smart phone cameras are primarily designed for capturing photographs and not just barcodes, so sensing color is integral to their functionality and they typically capture images with three red (R), green (G), and blue (B) channels. Most barcodes, however, are monochrome designs and fail to exploit the capability that the color capture channels of the cameras offer. This is in part because the monochrome designs work with commonly available black and white printers. In many applications, however, the barcodes occur in color printed pages. This is invariably the case for barcodes used with product advertisements, for example. The adherence to monochrome barcodes in these situations is primarily due to the original legacy of the designs that were intended for use with specialized monochrome sensors. Color barcode designs that offer similar robustness to the monochrome designs are therefore desirable. Several recent efforts have explored the design of color barcodes for mobile and other applications [10]–[15]. Among these, in Figs. 2 and 3, we highlight our own design framework from [15], which offers not just a specific barcode design but a methodology for extending any monochrome barcode design to color. As shown in Fig. 2, the barcodes are encoded as individual layers of the cyan (C), magenta (M), and yellow (Y) layers used for printing, which are complementary to the R, G, and B, sensors, respectively. Unlike the ideal scenario, where the barcodes encoded in individual colorant layers would appear individually in the captured R, G, B channels, in the real-world, there is significant cross-channel contamination, which we are able to model and correct for as shown in Fig. 3 (details in [15]), allowing for decoding of the data in the individual barcodes. The framework is powerful because it offers a three-fold increase in the data rate (the capacity gain is slightly lower) while retaining all the features and capabilities developed via extensive research for monochrome barcodes: viz., localization, synchronization, error correction coding, etc. This re-use also ensures that these aspects of the barcode are already optimized eliminating a lot of the re-engineering required for a fresh color barcode design.

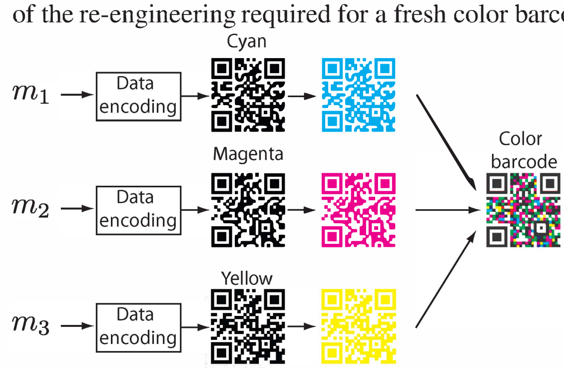


Fig. 2. Per colorant layer encoding of color barcodes (from [15]).

While barcodes have been the long-standing workhorses for image-based data interfaces, there is also a strong interest in watermarks as an alternative, where the data is embedded in an existing image via changes that are largely imperceptible to human viewers but can nonetheless be detected by appropriate processing to recover the embedded data. The requirement for image-based data interfaces to cross the analog gap limits the attention to a smaller class of watermarks designed for this purpose, examples include [16]–[22]. The key advantage that the watermarks offer over barcodes is their unobtrusiveness, which, however, also poses challenges in terms of robustness of detectability and the computational load required for detection – important considerations for mobile devices. Despite these challenges, watermarking technology has advanced to the point where there are now commercial offerings for watermark detectors as smartphone apps [23]. As with barcodes, for deployment of a watermark as an image-based data interface, the watermark must include elements for localization, synchronization, and error correction coding.

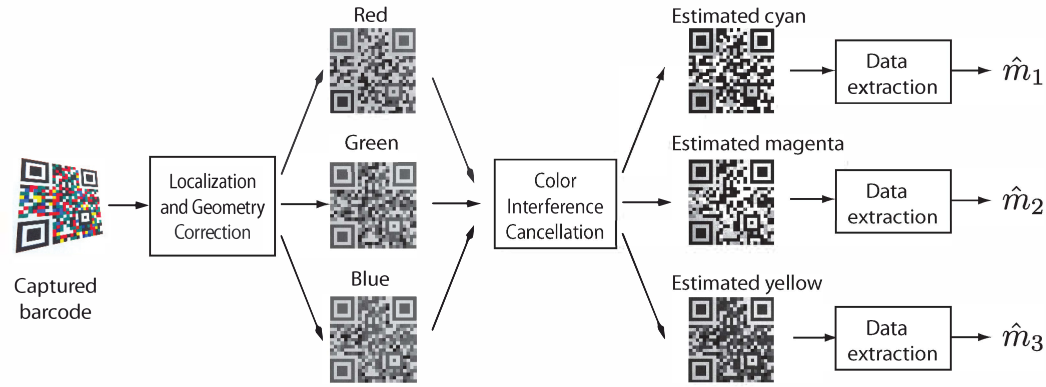


Fig. 3. Decoding of per colorant layer encoded color barcodes with color interference cancellation (from [15]).

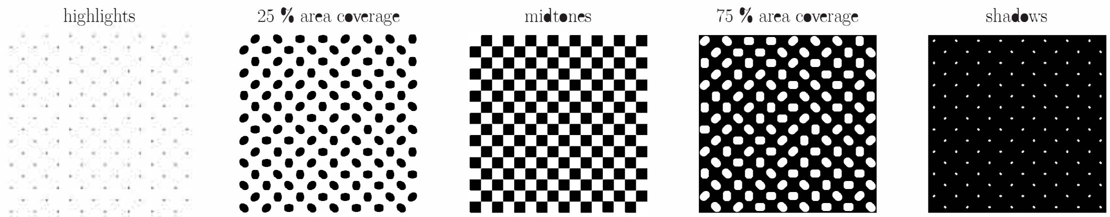


Fig. 4. Illustration for how modulation for data embedding is compromised by consideration of image quality in watermark data embedding for clustered dot halftone image watermarking by modulation of the orientation of the dots. These blocks represent highly magnified views showing regions corresponding to different gray levels in an image. Note that the orientations of the dots are discernible only in the 25% and 75% area coverage scenarios. The other regions labeled as highlights, shadows, and midtones show no discernible orientation of the dots because of the constraint imposed by the image gray level; the data in these regions is effectively erased and must be recovered by the error correction coding scheme utilized. (from [20]).

Because, unlike barcodes, watermarking systems do not have well-established open standards, these elements are typically proprietary and vary depending on the watermark design and application scenario. The data-embedding and error correction coding often need to account for the fact that the original image content needs to be preserved in the watermarked version with high quality. For a similar physical footprint, the payload is therefore usually lower with watermark based systems than with barcodes. Figure 4 illustrates this idea for a specific watermark system developed in our prior work [20] for the watermarking of documents printed with the commonly employed clustered dot halftones. We also observe that for this specific watermark, the synchronization is fortuitously accomplished by using the periodicity of the halftone structure.

Barcodes and watermarks represent two extremes of the spectrum of image-based data interfaces and there also exist techniques that explore alternatives that lie between these two extremes. In particular, a few efforts have explored image barcodes that visually approximate a desired image but allow significant distortion in order to carry data in a more robust and readily detectable manner [24]–[26]. An example from our prior work is illustrated in Fig. 5.

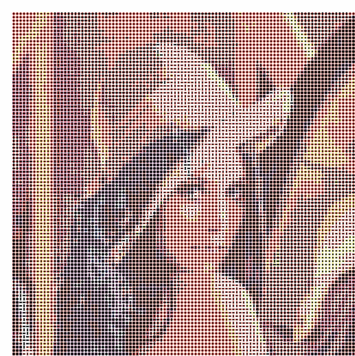


Fig. 5. An example image barcode. Significant distortion in the image is tolerated in order to increase the robustness of the data embedding compared with watermarks. (from [26]).

III. Applications

Image-based data interfaces enable a wide-array of applications. Barcodes are extremely inexpensive to produce and have long helped to automate tasks such as store checkout and inventory management, which are otherwise both labor intensive and error prone. In the mobile world, they not only provide analogous functionality in applications such as boarding pass management and tracking, but also enable new functionality by providing ready connectivity from the physical world in which the image is rendered to the digital cyberworld. A common example is the ability to easily connect to a website by using a barcode on an advertisement or poster, which is demonstrated by the barcodes in Fig. 1 (b), (c), and (d), which all encode the URL for the COMSNETS conference. A user with a smart phone app capable of reading these barcodes can use these to visit the COMSNETS website without having to type in the URL. In addition to primary advertising, the barcodes are also powerful for cross-promotion of merchandise and products, for example, through music downloads via QR codes on beverage cups. The codes are particularly powerful in providing instantaneous access at a fine granularity. Videos can be attached, for instance, to printed step-by-step instructions allowing a user to jump straight away to the step of interest instead of having to view the video from the start. A large payload to area-footprint ratio is highly desirable in a number of these applications, which makes the 2D barcodes preferable over 1D alternatives. The ability to encode additional data in such settings, enabled for instance by the use of color, can be exploited to increase the size of embedded data, reduce the physical footprint of the barcode, and/or improve the robustness of data recovery. Additional data can enhance this functionality by for instance allowing encoding of additional information for where the barcode is accessed, which can be useful for measuring effectiveness of advertisement monetization. The modular structure of the construction presented in Figs. 2 and 3 also offers the advantage of encoding independent parallel pieces of information - for example, sites for download of different (Android™, iOS™, WindowsMobile™) versions of a smartphone app can be multiplexed within a single color barcode instead of requiring separate barcodes as is often done with the monochrome versions.

Applications similar to those enabled by barcodes can also alternatively utilize watermarks. The unobtrusiveness of the watermarks makes them particularly attractive in applications where the insertion of a barcode would impair the aesthetics of the image and the overall visual presentation. This can be important, for instance, in deploying image-based data interfaces in advertisements in printed magazines, where the spatial footprint of the barcode can detract from the overall aesthetic design of the page. Watermarking has been used in such situations [18], [27]. Recently, watermarks inserted in the printing in product packaging have also been proposed to improve the efficiency of supermarket and grocery store checkouts by not requiring a specific orientation of the package while scanning it at cash registers. Such watermarks also allow consumers to access additional information regarding the product through the packaging either in the store or at home [21], [22]. In particular, the product code and other embedded information can be cross-linked and referenced via back-end databases to provide information on nutrition, recipes, related products, etc. Because the watermark data is closely coupled with the images in which the watermark is embedded it can also enable other applications for which barcodes are inapplicable or an unnatural fit. In particular piracy can be deterred through the use of watermarks. An example is the so-called forensic watermark that embeds a unique data identifier in each distributed version of multimedia content allowing for localization of the source for unauthorized redistributions. Notably, a forensic watermark [28] was utilized to identify the source of illegally redistributed copies of the screeners from the 2003, 2004, and 2005 Academy Awards (Oscars) [29]. Interestingly, one of the earliest proposed versions of such watermarks was for printed documents [16].

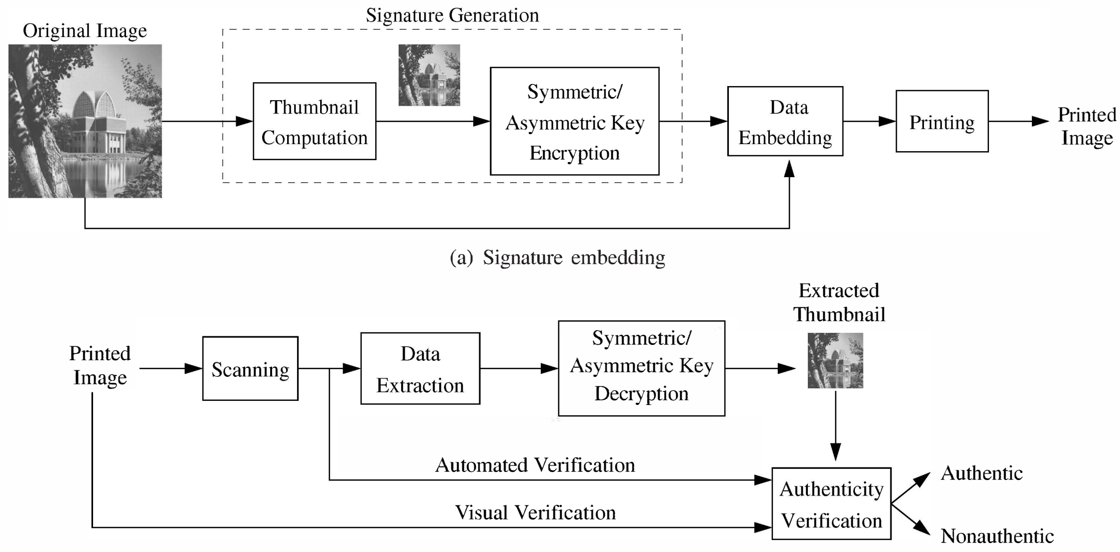
The close coupling between a printed document and any embedded data it carries has also been proposed as an effective mechanism for validating the integrity and/or authenticity of printed documents using both barcodes and watermarks [30]–[33]. In such applications, the embedding of digital data facilitates the use of cryptographic protocols and significantly enhances security over alternative methods that cannot offer similar guarantees. Validating image content poses additional challenges in such settings because of the analog nature of the printed image content which makes direct cryptographic signature based authentication infeasible and necessitates that comparison focus on verifying visual rather than digital equivalence. Our recent work [32], presents an effective solution to this problem by leveraging high capacity watermarks within a cryptographically secure framework. The approach illustrated in Fig.6, uses the high capacity embedding to digitally embed a signed/encrypted thumbnail of the image content into its printed rendition. Verification then proceeds by chaining together the validation of the thumbnail via cryptography and verification of the image content against the thumbnail that provides a visual facsimile for comparison. Notably, the methodology plugs some unappreciated security holes in previously proposed printed image authentication methods and also enables localization of intelligently architected malicious manipulations. A sample result illustrating this latter aspect is shown in Fig. 7, where the caption is self-explanatory.

(a) Manipulated image (b) Extracted thumbnail from the manipulated images (c) Detected manipulated regions

Fig. 7. Detection of the manipulated regions when a nonauthentic printed image is generated by *local manipulation and signature transfer attack*. Manipulations are performed in digital domain after scanning the original printed image. Images in the second row are the thumbnails extracted from the manipulated images. (from [32])

IV. Image-based Data Communication vs. Alternatives

The applications for image-based data interfaces that we highlighted in Section III naturally categorize into two main classes: (1) applications that use the interfaces purely as carriers of digital data in a machine accessible format, which can be read from an image of interface's physical "tag", and (2) applications that were enabled by the close coupling between the interface and the image or the substrate in which the image is rendered. For the latter class of applications, there are effectively no viable alternatives that provide functionality similar to the image-based data interfaces. For the former class of applications, however, the connectivity that image-based data interfaces provide between the physical and cyberworlds can also be accomplished by alternative technologies. In particular, radio frequency identification (RFID) tags [34]–[36] and the closely associated near field communication (NFC) [37] technologies also enable noncontact communication of data. Specifically, for NFC, the tag is a passive device comprised of a loop antenna connected to a chip. When a suitably equipped



(a) Signature embedding

(b) Authentication

Fig. 6. Content authentication framework for printed images: (a) Signature embedding and (b) Authentication verification. (from [32])

interrogating device, such as an NFC enabled smartphone, is placed in close proximity of the tag, an electromagnetic signal that it emits couples inductively with the antenna powering the tag allowing two way communication. Like QR codes, NFC tags can communicate digital data to the interrogating device such as a web URL that provides access to additional information/resources. Additionally, however, NFC tags can also receive data from the interrogating device and update their stored data. Table I compares several key attributes of image-based data interfaces against NFC. The table highlights that each of these modes of noncontact communication offers its own advantages. In particular, the negligible cost of creating barcodes, broad current availability of barcode readers as software apps for smartphones with cameras, and ease with which users can create barcodes on-their-own argue strongly in favor of continued use of this preexisting technology over NFC alternatives in applications where their functionality suffices. For other applications, for instance, for smartphone based automation of point of sale transactions, NFC offers compelling advantages. The user experience with NFC tags is more seamless because the user can simply tap their NFC enabled smartphone in the vicinity on the NFC tag to read and act upon the tag; the user does not need to open an app and appropriately position the camera to capture a suitably focused image of the barcode. Additional features such as security through the use of encryption and updateability of stored information also make NFC better suited, for some applications, than the image-based data interface alternatives. For some of the attributes compared in Table I the attributes can depend, in part, on the usage scenarios - this is indicated by the * superscripts. For instance, though NFC communcation is itself unobtrusive, (obtrusive) visual indicators may be required to alert users to the existence of NFC capability. Similarly, in display applications of image-based data interfaces, network interaction can allow the use of cryptography.

Attribute	Technology	
	Image	NFC
Communication	One way	Two way
Tag Cost	Negligible	Small
Range	Visible	Proximity
Obtrusive	Maybe	No*
Connection setup	Interactive	Seamless
Current availability	Broad	Limited
Tag Creation	Easy	Complex
Field Update	No	Yes*
Encryption	No*	Yes
Control	Yes	On/Off
Privacy	Field-of-view	If encrypted
Lighting	Required	Unnecessary

TABLE I
ATTRIBUTE COMPARISON FOR IMAGE-BASED DATA INTERFACES (IMAGE) VERSUS NEAR FIELD COMMUNICATION (NFC) TECHNOLOGIES FOR NONCONTACT, CLOSE PROXIMITY COMMUNICATIONS.

V. CONCLUSION

The ubiquitous availability of image sensors embedded in smartphones and other mobile computing devices makes image-based data interfaces, viz. barcodes and watermarks, an attractive option for communicating data for a variety of applications. For physical tagging, new technology alternatives such as RFID and NFC are also becoming available. In these applications, the image-based data interfaces will likely coexist with the newer NFC technologies instead of competing for replacement. Given the ubiquitous availability of the smartphone camera and display and the limited availability of NFC readers on current smartphones, in the near term, for physical to cyber connectivity, it is likely combined tags will be a promising alternative that allow users to access a common piece of information using either the image-based interface or NFC. Based on the close coupling between the image content and the digital data carried by image-based data interfaces, they also enable other applications for which RFID and NFC are not viable alternatives. In these applications, the use of image-based data interfaces will continue and expand. Ongoing research continues to adapt and improve image-based data interfaces for existing as well as emerging application scenarios.

ACKNOWLEDGMENT

As indicated by the citations, several of the figures in this paper are reused from prior work done jointly with students and collaborators. Their contributions to these figures are gratefully acknowledged.

REFERENCES

[1] R. W. Burns, *Communications: an international history of the formative years*. Bodmin, Cornwall, UK: IEE, 2004, vol. 32, history of Technology Series.

[2] ISO/IEC, "Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification," http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=46143, 2009, accessed Jan 2011.

[3] ——, "Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification," http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=43655, 2006, accessed Jan 2011.

[4] ——, "Information technology – Automatic identification and data capture techniques – Aztec Code bar code symbology specification," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41548, 2008, accessed Apr 2011.

[5] A. Longacre and R. Hussey, "Two dimensional data encoding structure and symbology for use with optical readers," United States Patent 5,591,956, 7 Jan. 1997.

[6] C. Sant'Anselmo, R. Sant'Anselmo, and D. C. Hopper, "Identification symbol system and method with orientation mechanism," United States Patent 5,612,524, Mar. 1997.

[7] "Data Matrix barcode FAQ & tutorial," accessed Jan 2008. [Online]. Available: http://idautomation.com/datamatrixfaq.html

[8] S. Lin and D. J. Costello, Jr., *Error Control Coding*. Englewood Cliffs, NJ: Prentice-Hall, 2004.

[9] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. New York, NY: Wiley-Interscience, 2005.

[10] H. Kato, K. Tan, and D. Chai, *Barcodes for Mobile Devices*. New York, NY, USA: Cambridge University Press, 2010.

[11] H. Kato and K. Tan, "Pervasive 2D barcodes for camera phone applications," *IEEE Pervasive Computing*, vol. 6, no. 4, pp. 76–85, Oct.–Dec. 2007.

[12] D. Parikh and G. Jancke, "Localization and Segmentation of A 2D High Capacity Color Barcode," in *IEEE Workshop on Applications of Computer Vision (WACV) 2008.*, 2008, pp. 1–6.

[13] S. J. Simske, J. S. Aronoff, and M. Sturgill, "Revenge of the physical - mobile color barcode solutions to security challenges," in *Proc. Optical Document Security*, San Francisco, 20–22 Jan. 2010, pp. 184–197, also available as [38].

[14] O. Bulan and G. Sharma, "High capacity color barcodes: Per channel data encoding via orientation modulation in elliptical dot arrays," *IEEE Trans. Image Proc.*, vol. 20, no. 5, pp. 1337–1350, May 2011.

[15] H. Blasinski, O. Bulan, and G. Sharma, "Color barcodes for mobile applications: A per channel framework," *IEEE Trans. Image Proc.*, vol. 22, no. 4, pp. 1498–1511, Apr. 2013.

[16] J. Brassil, S. Low, N. Maxemchuk, and L. O'Gorman, "Electronic marking and identification techniques to discourage document copying," *IEEE J. Selected Areas in Comm.*, vol. 13, pp. 1495–1504, 1995.

[17] A. M. Alattar, "Smart images using digimarc's watermarking technology," in *Proc. SPIE: Security and Watermarking of Multimedia Contents II*, P. W. Wong and E. J. Delp, Eds., vol. 3971, Jan. 2000, pp. 264–273.

[18] S. Decker, "Engineering considerations in commercial watermarking," *IEEE Comm. Mag.*, vol. 39, no. 8, pp. 128–133, Aug. 2001.

[19] A. K. Mikkilineni, G. N. Ali, P. J. Chiang, G. T. Chiu, J. P. Allebach, and E. J. Delp, "Signature-embedding in printed documents for security and forensic applications," in *Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI*, E. J. Delp and P. W. Wong, Eds., vol. 5306, Jan. 2004, pp. 455–466.

[20] O. Bulan, G. Sharma, and V. Monga, "Orientation modulation for data hiding in clustered-dot halftone prints," *IEEE Trans. Image Proc.*, vol. 19, no. 8, pp. 2070–2084, Aug. 2010.

[21] A. Reed, E. Rogers, and D. James, "Chrominance watermark for mobile applications," in *Proc. SPIE: Multimedia on Mobile Devices*, R. Creutzburg and D. Akopian, Eds., vol. 7528, Jan. 2010, pp. 75 420V–75 420V–8. [Online]. Available: http://dx.doi.org/10.1117/12.839134

[22] A. Reed, T. Filler, K. Falkenstern, and Y. Bai, "Watermarking spot colors in packaging," in *Proc. SPIE: Media Watermarking, Security, and Forensics*, A. M. Alattar, N. D. Memon, and C. D. Heitzenrater, Eds., vol. 9409, Feb. 2015, pp. 940 906–940 906.

[23] Digimarc, "Digimarc®discover mobile app." [Online]. Available: https://www.digimarc.com/products/discover/mobile-app

[24] D. L. Hecht, "Printed embedded data graphical user interfaces," *IEEE Computer*, vol. 34, no. 3, pp. 47–55, Mar. 2001.

[25] ——, "Embedded data glyph technology for hardcopy digital documents," in *Proc. SPIE: Color hard copy and graphic arts III*, J. Bares, Ed., vol. 2171, Mar. 2001, pp. 341–352.

[26] O. Bulan, G. Sharma, and B. Oztan, "High capacity image barcodes using color separability," in *Proc. SPIE: Color Imaging XVI: Displaying, Processing, Hardcopy, and Applications*, R. Eschbach, G. G. Marcu, and A. Rizzi, Eds., vol. 7866, Jan. 2011, pp. 7866–N,1–9.

[27] DigiMarc Corp, "Digimarc mediabridge," 2000. [Online]. Available: https://www.digimarc.com/resources/docs/tech_papers/dmrc_media_bridge.pdf

[28] "Nexguard: A civolution company." [Online]. Available: http://www.nexguard.com/

[29] D. Milano, "Content control: Digital watermarking and fingerprinting," White Paper, Rhozet, a business unit of Harmonic Inc., accessed July 2015. [Online]. Available: http://www.resource.holdan.eu/specs/Fingerprinting_Watermarking.pdf

[30] B. Zhu, J. Wu, and M. S. Kankanhalli, "Print signatures for document authentication," in *Proc. of the 10th ACM conference on Computer and communications security*, Oct. 2003, pp. 145–154.

[31] 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*, vol. 1, no. 4, pp. 405–420, December 2006. [Online]. Available: http://vision.unige.ch/publications/postscript/2006/TIFS-multilevel-2D-barcodes.pdf

[32] O. Bulan and G. Sharma, "Content authentication for printed images utilizing high capacity data hiding," *J. Electronic Imaging*, vol. 22, no. 3, pp. 033 006–1–13, Jul.-Sept. 2013.

[33] Y. Tian, X. Zhan, C. Wu, and W. Ming, "Self-verifiable paper documents and automatic content verification," in *Proc. SPIE: Media Watermarking, Security and Forensics 2014*, A. M. Alattar, N. D. Memon, and C. D. Heitzenrater, Eds., vol. 9028, Feb. 2014, pp. 902 835–1–902835–8.

[34] K. Finkenzeller, *RFID Handbook: Radio-frequency identification fundamentals and applications*. Wiley, 1999.

[35] ISO/IEC, "ISO/IEC 15693-1:2010 Identification cards – Contactless integrated circuit cards – Vicinity cards – Part 1: Physical characteristics," 2010. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39694

[36] ——, "ISO/IEC 14443-1:2008 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39693

[37] ——, "ISO/IEC 18092:2013 Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)," 2013. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/c056692_ISO_IEC_18092_2013.zip

[38] S. J. Simske, J. S. Aronoff, and M. Sturgill, "Revenge of the physical-mobile color barcode solutions to security challenges," Hewlett-Packard Lab., Palo Alto, CA, Tech. Rep. HPL-2010-7, 21 Jan. 2010. [Online]. Available: http://www.hpl.hp.com/techreports/2010/HPL-2010-7.pdf