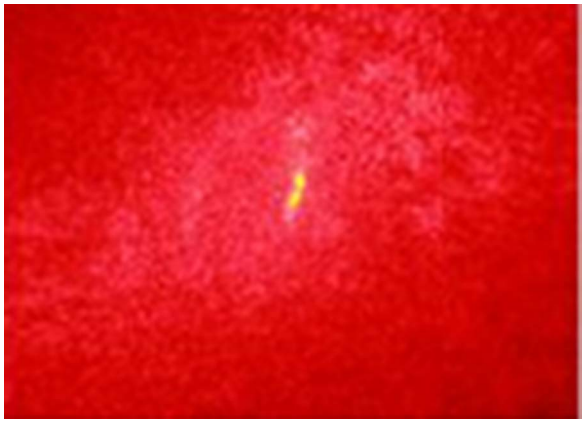
IEEE Photonics Journal
An IEEE Photonics Society Publication

Photon-Counting Security Tagging and Verification Using Optically Encoded QR Codes

Volume 6, Number 1, February 2014

A. Markman
B. Javidi, Fellow, IEEE
M. Tehranipoor, Senior Member, IEEE



DOI: 10.1109/JPHOT.2013.2294625
1943-0655 © 2014 IEEE

Photon-Counting Security Tagging and Verification Using Optically Encoded QR Codes

A. Markman, B. Javidi, *Fellow, IEEE*, and M. Tehranipoor, *Senior Member, IEEE*

Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269-2157 USA

DOI: 10.1109/JPHOT.2013.2294625

Manuscript received October 25, 2013; accepted December 1, 2013. Date of publication December 17, 2013; date of current version February 13, 2014. This work was supported in part by the National Science Foundation under Award #CNS-1344271. Corresponding author: A. Markman (e-mail: amarkman89@gmail.com).

Abstract: We propose an optical security method for object authentication using photon-counting encryption implemented with phase encoded QR codes. By combining the full phase double-random-phase encryption with photon-counting imaging method and applying an iterative Huffman coding technique, we are able to encrypt and compress an image containing primary information about the object. This data can then be stored inside of an optically phase encoded QR code for robust read out, decryption, and authentication. The optically encoded QR code is verified by examining the speckle signature of the optical masks using statistical analysis. Optical experimental results are presented to demonstrate the performance of the system. In addition, experiments with a commercial Smartphone to read the optically encoded QR code are presented. To the best of our knowledge, this is the first report on integrating photon-counting security with optically phase encoded QR codes.

Index Terms: Optical security and encryption, photon counting imaging, speckle, coherent imaging.

1. Introduction

Information security with optical techniques has been widely investigated [1]–[15]. Many variations of random phase encoding for security and encryption have been proposed [16]–[32]. Optical techniques in security provide many advantages including the ability to secure data with multi dimensional keys such as wavelength [3], polarization [4], and placing the keys in the Fresnel domain [5]. Recently, photon-counting imaging has been integrated with the double-random-phase encryption for optical security [26]. The motivation for using photon-counting is that the integration of photon-counting imaging generates an additional layer of complexity that enhances the security of the system against an attacker. A photon-limited encrypted image is very sparse compared with a conventional encrypted data. When photon-counting is used, the decrypted data is not recognizable by visual inspection making it more robust to attacks due to the sparse photon counting data. In addition, photon-counting imaging follows the Poisson distribution which is a nonlinear transformation unlike the conventional double random phase encryption which is a linear encoding. The nonlinear transformation is advantageous in making the system more robust against attacks.

In this paper, we propose a novel method for optical security and tagging. In this approach, we encrypt the data using the full phase double-random-phase encryption with photon-counting [28], and then apply an iterative compression technique based on Huffman coding [33] to compress the photon counting encrypted image. The data can then be stored in an optically encoded Quick Response (QR) code [34], [35] and placed on the object to be authenticated. Commercial QR scanners built into Smartphones such as an iPhone or Android device [36] can be used to scan the QR code and capture the encrypted data. The encrypted data can then be decrypted and decompressed using the correct keys and dedicated algorithms to deal with the photon-counting nature of the data. Image recognition algorithms such as nonlinear correlation filters [37]–[39] can be used to verify the decrypted image against the primary image for authentication. In addition, the QR code is optically phase encoded with a pseudo-random key so that the QR code is more secure against unauthorized duplication of the optical tag. The optical phase mask is then verified using an examination of its speckle diffraction signature using statistical analysis.

The proposed method may be particularly useful for authentication of integrated circuits (ICs). It adds an additional layer of security against counterfeiting of the IC by removing printed information located on the IC and storing its encrypted version in an optically phase encoded binary image. Thus, the IC will not contain any printed information about the chip, making it difficult for an attacker to identify the IC.

The paper is arranged as follows: Section 2 briefly describes the full phase double-random-phase encryption with photon-counting (PC-DRPE) and the correlation algorithms for authentication. In Section 3, the proposed method of combining the iterative Huffman Coding method with the PC-DRPE to store data in an optically encoded QR code is examined along with optical experimental results, including optical encoding mask verification to demonstrate the proposed concept. Section 4 presents the conclusion.

2. Full Phase Double-Random-Phase Encoding With Photon-Counting

The full phase double-random-phase encryption with photon-counting (PC-DRPE) can be used to encrypt the input image [28]. For convenience, one-dimensional notation will be used in explaining the encryption method. To implement the encryption scheme, let (x) and (υ) denote the spatial and frequency domains, respectively. In addition, let $f(x)$ be the primary input image and $n(x)$ and $b(\upsilon)$ be two random noises that are uniformly distributed over the interval {0, 1]. The encrypted image is generated by first phase encoding the input image yielding $\exp[i\pi f(x)]$ and then multiplying the phase encoded image by the phase mask $\exp[i2\pi n(x)]$. This product is then convolved with a phase mask, $h(x)$, whose Fourier transform is $\exp[i2\pi b(v)]$. The encrypted image is then

$$\psi(x) = \{\exp[i\pi f(x)] \times \exp[i2\pi n(x)]\} * h(x) \tag{1}$$

where $*$ denotes convolution and $\times$ denotes multiplication.

Photon-counting imaging [26]–[28], [40] is then applied to the amplitude of the encrypted image, $|\psi(x)|$, by limiting the number of photons arriving at each pixel. It has been shown that this process can be modeled as a Poisson distribution. Moreover, the fewer the number of photons, the sparser the scene becomes due to less photons arriving at a pixel. The number of photons arriving at pixel j can be modeled as:

$$P(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j!}, \quad \text{for } \lambda_j > 0, \quad l_j \in \{0,1,2,\ldots\} \tag{2}$$

where l_j is the number of photons detected at pixel j and λ_j is the Poisson parameter defined as $N_p x_j$, where N_p is the number of photons in the scene and x_j is the normalized irradiance at pixel j such that $\sum_{j=1}^{M} x_j = 1$ with M being the total number of pixels. Moreover, the normalized irradiance is defined as $|\psi(x_j)| / \sum_{j=1}^{M} |\psi(x_j)|$, where $|\psi(x_j)|$ is the amplitude information.

The full phase PC-DRPE encrypted image, $\psi_{ph}(x)$, can then be decrypted. The Fourier transform of $\psi_{ph}(x)$ is taken and multiplied by the complex conjugate of the phase mask used in the frequency

domain, $\exp[-i2\pi b(\nu)]$. The Fourier transform is then taken once more. In the full phase PC-DRPE decryption process, the resulting product must be multiplied by the complex conjugate of the phase mask used in the spatial domain, $\exp[-i2\pi n(x)]$. The final decrypted image, $f_{ph}(x)$, which is real and positive, is then found as [8], [28]:

$$\left|f_{ph}(x)\right| = \left|Arg\left\{A\exp\left[i\pi f_{ph}(x)\right]\right\}/\pi\right| \tag{3}$$

where A is the amplitude of the decrypted image, Arg is the argument function and $||$ is the modulus operator.

Rather than recover the decrypted image, a noise-like decrypted image is obtained which is difficult to visually authenticate. However, the decrypted can be authenticated using classification algorithms such as nonlinear-processors [37]–[39]. To authenticate the decrypted image [Eq. (3)], a number of image recognition techniques can be used. We have selected the kth order nonlinear processor [38] for its simplicity and effectiveness in the experiments that we have presented. In this approach, the Fourier transforms of the decrypted image, $f_{ph}(x)$, and the input image, $f(x)$, are first taken. The processor is implemented by the following equation:

$$c(x) = IFT\left\{\left|F_{f_{ph}}(v)F_f(v)\right|^k \exp\left[j\left(\phi_{f_{ph}}(v) - \phi_f(v)\right)\right]\right\} \tag{4}$$

where IFT is the inverse Fourier transform, k is the strength of the applied nonlinearity and determines the performance features of the processor, and $\phi(v)$ is the phase information.

3. Embedding Encrypted Data Into Optically Phase Encoded QR Code

The data encrypted using the full phase double-random-phase encryption with photon-counting needs to be compressed and inserted into an optically encoded QR code. Currently, it is not possible to insert an image into a QR code [See Appendix I for more information about QR codes] due to data size restrictions and the limited resolution of commercial Smartphones when scanning the QR code [41]. To overcome this limitation, an image is inserted into a QR code via a hyperlink: A user scans the QR code containing the hyperlink which automatically redirects the user to the image. We present an iterative Huffman coding method to compress an image so it can be stored in a QR code allowing a Smartphone to read the QR code.

In the iterative Huffman coding method, we begin by applying Huffman coding [33] on the photon-limited amplitude data, $|\psi_{ph}(x)|$, for low N_p [Eq. (2)] by converting the image into a 1 dimensional array. Note that each pixel is an integer value due to the Poisson distribution being a discrete distribution. The first Huffman code compression reduces the image into a series of bits. The Huffman code can then be represented as a series of integers by first padding the Huffman code with zeros to ensure the code can be separated into groups of 8 bits. Each group can then be converted to an integer; this is advantageous since the QR code is character limited. For example, if a group of 10 pixels has corresponding values [0 1 1 0 0 2 1 4 2 1] in the image, the Huffman code is then a series of bits corresponding to the symbol 0, 1, 2, or 4. Suppose a group of 8 bits is 10110111, this can be rewritten as 183. Once there has been one iteration of Huffman coding, Huffman coding can be repeated since there will be repeated integers between 1 and 256 which ranges from 1 to 3 characters each. The described Huffman coding procedure can be repeated until there is a low number of characters present in the compressed data.

Once the QR code has been scanned, the data can be decompressed if both the dictionary and the length of the unpadded Huffman code, in bit form, associated with each Huffman iteration are known (allowing for the zero padding to be removed). Moreover, the data can then be successfully decrypted if the phase mask keys and phase information used in the full phase PC-DRPE are known.

Currently, the resolution of the iPhone camera cannot discern the details of the QR code if the QR code is too small; however, the QR code can be enlarged using the cameras built into Smartphones. The enlarged QR code can then be scanned using a QR reader revealing the compressed and encrypted data. Fig. 1(a) depicts a 449 $\times$ 641 pixel binary image and Fig. 1(b) depicts a 3.15 mm $\times$ 3.15 mm QR code, generated using the ZXing Project [42], and placed on a

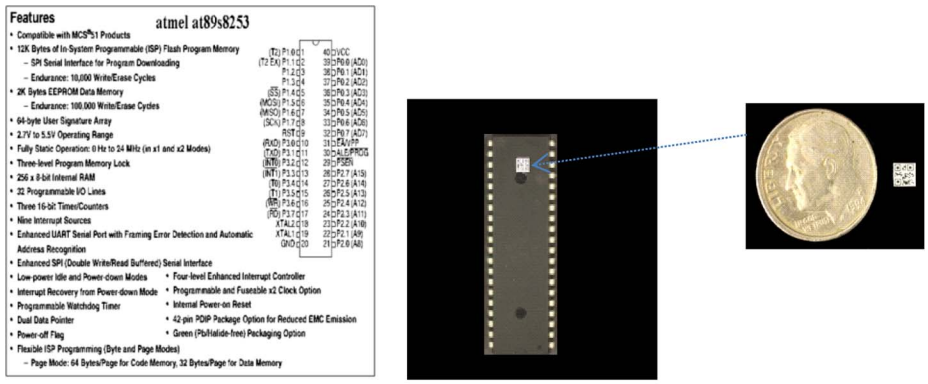


Fig. 1. (a) 449 × 641 pixel binary image. (b) 3.15 mm × 3.15 mm QR code storing the encrypted and compressed image shown in (a) placed on a 14.5 mm × 52.1 mm IC; an image of the QR code placed next to a dime is also depicted.

Fig. 2. (a) Enlarged QR code taken using the iPhone 4 camera; (b) scanned QR code depicting the encrypted and compressed data using the iPhone SCAN Application.

14.5 mm × 52.1 mm IC chip. The QR Code is also shown next to a dime in Fig. 1(b). Fig. 2(a) shows an enlarged QR Code obtained from the QR code shown in Fig. 1(b) using the iPhone 4 camera. Fig. 2(b) depicts the scanned QR code which reveals the compressed and encrypted (for $N_p = 500$ or $1.73e-3$ photons/pixel) data using the iPhone SCAN application.

Once the data has been scanned, it can be decompressed and decrypted. Fig. 3(a) shows the decrypted input image at $N_p = 500$. Note that it is impossible to visually authenticate the decrypted image. However, a nonlinear correlation filter [Eq. (4)] can be used to authenticate the primary image with the input image. Fig. 3(c) shows the output of the kth order nonlinear filter normalized to 1 with $k = 0.3$. A distinct peak is obtained indicating the filter recognizes the decrypted image as a true class object. Fig. 3(b) shows a 449 × 641 pixel false class image, $g(x)$, that is used in the kth order nonlinear filter to verify that it can distinguish between true and false class objects. Fig. 3(d) shows the output of the filter using $g(x)$ which has a maximum peak of 0.330.

A vulnerability of the proposed technique is that the QR code can be replicated while preserving the information stored inside of the code. One way to circumvent this security issue is to optically encode the QR code. To do this, we pasted a phase mask on the QR code and used coherent optical imaging to verify whether the QR code has been copied. Fig. 4(a) shows a QR code generated using the ZXing Project [42] encoded with a random phase mask placed on the QR code. An advantage of a phase mask is that it is transparent, which allows the QR code located on the IC to be scanned. Note that Reed Solomon Error correction incorporated into the QR code design [34] can account for any minor physical anomalies in the QR code. Fig. 4(b) shows the enlarged QR code shown in Fig. 4(a) successfully scanned using the iPhone SCAN Application.

To verify that the correct phase mask is used, a laser source illuminates the QR code located on the IC chip which is covered by the phase mask. The mask used in the experiments is a piece of

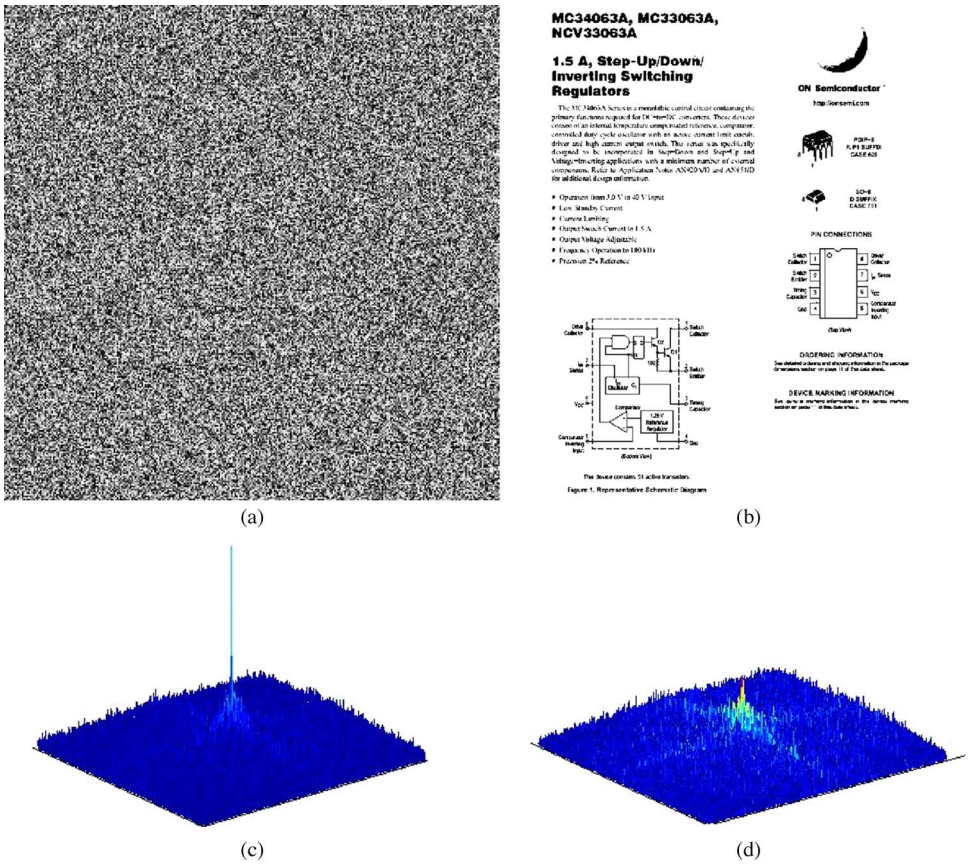


Fig. 3. (a) Decrypted image obtained from the full phase PC-DRPE using the image shown in (a) as the input image (true class object); (b) 449 $\times$ 641 pixel binary false class image; (c) output of the kth order nonlinear filter between the true class decrypted image and the true class object with $k = 0.3$ normalized to 1; (d) output of the kth order nonlinear filter between the true class decrypted image and the false class object which has a maximum peak of 0.330 with $k = 0.3$.

Fig. 4. (a) QR code encoded with a random phase mask placed on an IC and (b) scanned QR code shown in (a).

scotch tape. The light scatters off of the random phase mask and generates a speckle pattern which can be seen on a projection screen, as shown in Fig. 5. The intensity of the speckle pattern can be recorded using a camera. Each phase mask generates a unique speckle pattern. Thus, the QR code along with the correct phase mask must be used to verify the QR code. Fig. 6(a) shows an example of the speckle intensity pattern of the QR code without a phase mask illuminated by a HeNe laser. Fig. 6(b) depicts the speckle intensity pattern of the QR code shown in Fig. 4(a).

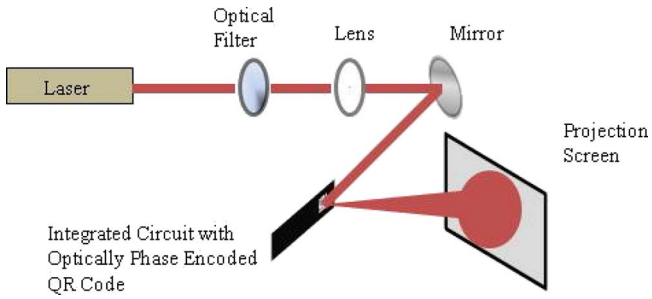


Fig. 5. Experimental set-up for verifying the phase encoded QR code speckle pattern.

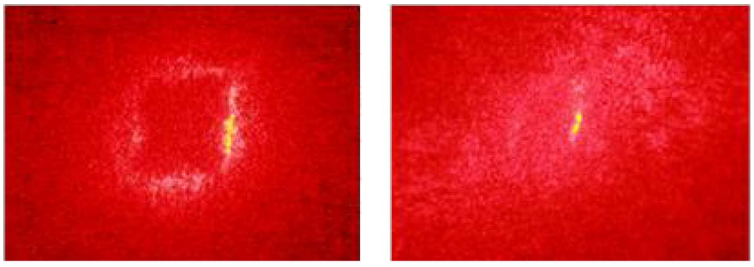


Fig. 6. Speckle intensity patterns generated by (a) a QR code without a phase mask and (b) an optically encoded QR code with a phase mask.

We note that the speckle intensity pattern of each individual point on the QR code can be modeled as a negative exponential distribution. Thus, the recorded speckle intensity pattern can be modeled as a sum of independent negative exponential distributions which is a gamma distribution [40], [43], [44]:

$$\Gamma\left(I; n_o, \frac{n_o}{\langle I\rangle}\right) = \left(\frac{n_o}{\langle I\rangle}\right)^{n_o} \frac{I^{n_o-1}\exp(-In_o/\langle I\rangle)}{\Gamma(n_o)} \tag{5}$$

where $\langle\ \rangle$ denotes the mean ensemble, I represents the speckle intensity pattern data points and n_o is the number of independent correlation cells (speckles) within the scanning aperture and chosen so that the variance of the approximate and exact distributions are equal: $n_o = \langle I\rangle^2/\sigma_b^2$, where σ_b is the standard deviation of the intensity fluctuation relative to the mean intensity.

The likelihood ratio test [45] can be used for classification between a true and false class speckle intensity pattern. Let H_o be the null hypothesis representing the true class object and H_1 be the alternative hypothesis representing the false class object. The log-likelihood function of Eq. (5) is

$$\log[l(\theta)] = Nn_o \log\left(\frac{n_o}{\langle I\rangle}\right) + (n_o - 1)\sum_{j=1}^{N}\log(I_j) - N\log[\Gamma(n_o)] - \frac{n_o}{\langle I\rangle}\sum_{j=1}^{N} I_j \tag{6}$$

where θ represents the distribution parameters, $(n_o, n_o/\langle I\rangle)$, and N is the total number of I_j.

The log-likelihood ratio can be written as:

$$\log[l(\theta_o)]\ -\log[l(\theta_1)] \underset{H_1}{\overset{H_o}{\gtrless}} 0, \tag{7}$$

where θ_o and θ_1 represent the true and false class distribution parameters, respectively.

Using the likelihood ratio test [Eq. (7)], the true class parameters are obtained from Fig. 6(b) and calculated as $n_o/\langle I\rangle = 18.08$ and $n_o = 3.43$. Moreover, the false class parameters are obtained

(a) (b)

Fig. 7. (a) QR code with 10 characters and (b) QR code with over 400 characters.

from Fig. 6(a) and calculated as $n_o/\langle I \rangle = 31.85$ and $n_o = 7.47$. Using a true class image, such as Fig. 6(b), a log-likelihood difference of 20,682 was calculated indicating that the test favors the true class and thus can potentially be used for phase mask authentication.

4. Conclusion

We propose an optical security method for object authentication using photon-counting encryption implemented with phase encoded QR codes. The experiments are presented to demonstrate authentication of integrated circuits (IC). A binary image containing information used to identify an IC is encrypted using the full phase double-random-phase encryption with photon-counting (PC-DRPE). The encrypted data is then compressed using an iterative Huffman coding technique and embedded in a QR code. Thus, information used to identify the IC does not need to be printed on the integrated circuit. Experimental results show that the encrypted and compressed data stored in the QR code can be read by a commercial Smartphone. The data can then be decompressed and decrypted; however, the decrypted image is noise-like making it difficult to visually authenticate the image. Using correlators, the decrypted image can be verified as the original binary image. In addition, an optical phase mask was used to encode the QR code and it was verified by examining the speckle signature of the mask using statistical analysis. By not requiring the QR scanning device to be connected to the World Wide Web, many security vulnerabilities can be avoided such as malware being installed on the QR scanner. Moreover, if the IC is intercepted by an attacker, it will be difficult to identify the IC. Future work may include various types of encryption and security strategies, storing various parts of encrypted and photon-limited data followed by compression in the QR code.

Appendix I

The QR code is a 2D barcode created by D. Wave [34], [35]. The advantage of a QR code is that it can be scanned regardless of scanning direction or if the QR code is damaged. Online QR Code generators can be used to generate QR codes including the level of error correction and version number [42]. The QR code itself is a binary image consisting of black squares known as modules placed on a white background, as shown in Fig. 7(a), where each module represents some information about the input text. The QR code can be read by a QR reader built into Smartphones [36] to retrieve the text. However, as the number of characters stored in the QR code increases, the size of the modules decreases. As a result, if too much information is stored in a QR code, as shown in Fig. 7(b), the module size will fall below the resolution limit of the camera used in Smartphones making it difficult for the QR reader to scan.

References

[1] B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," *Opt. Eng.*, vol. 33, no. 6, pp. 1752–1756, Jun. 1994.
[2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.

[3] O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes," *Appl. Opt.*, vol. 38, no. 32, pp. 6785–6790, Nov. 1999.
[4] X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure optical memory system with polarization encryption," *Appl. Opt.*, vol. 40, no. 14, pp. 2310–2315, May 2001.
[5] O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.*, vol. 24, no. 11, pp. 762–764, Jun. 1999.
[6] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Opt. Lett.*, vol. 30, no. 13, pp. 1644–1646, Jul. 2005.
[7] Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Exp.*, vol. 15, no. 16, pp. 10 253–10 265, Aug. 2007.
[8] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 16, no. 8, pp. 1915–1927, Aug. 1999.
[9] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, Jun. 2000.
[10] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 15, no. 10, pp. 2629–2638, Aug. 1998.
[11] O. Matoba and B. Javidi, *Encrypted optical memory systems based on multidimensional keys for secure data storage and communications*
[12] O. Matoba and B. Javidi, "The keys to holographic data security," *IEEE Circuits Devices Mag.*, vol. 16, no. 5, pp. 8–15, Sep. 2000.
[13] B. Javidi and T. Nomura, "Polarization encoding for optical security systems," *Opt. Eng.*, vol. 39, no. 9, pp. 2439–2443, Oct. 2000.
[14] J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," *Opt. Commun.*, vol. 260, no. 1, pp. 109–112, Apr. 2006.
[15] H. Suzuki, M. Yamaguchi, M. Yachida, N. Ohyama, H. Tashima, and T. Obi, "Experimental evaluation of fingerprint verification system based on double random phase encoding," *Opt. Exp.*, vol. 14, no. 5, pp. 1755–1766, Mar. 2006.
[16] W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," *Opt. Lett.*, vol. 35, no. 22, pp. 3817–3819, Nov. 2010.
[17] T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 25, no. 10, pp. 2608–2617, Oct. 2008.
[18] Mehra, S. K. Rajput, and N. K. Nishchal, "Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification," *Opt. Eng.*, vol. 52, no. 2, p. 028202, Feb. 2013.
[19] N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," *Opt. Commun.*, vol. 284, no. 3, pp. 735–739, Feb. 2011.
[20] P. Kumar, J. Joseph, and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Appl. Opt.*, vol. 50, no. 13, pp. 1805–1811, May 2011.
[21] E. Tajahuerce, J. Lancis, B. Javidi, and P. Andrés, "Optical security and encryption with totally incoherent light," *Opt. Lett.*, vol. 26, no. 10, pp. 678–680, May 2001.
[22] A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," *Adv. Opt. Photon.*, vol. 1, no. 3, pp. 589–636, Nov. 2009.
[23] O. Matoba, T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, "Optical techniques for information security," *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.
[24] P. Kumar, A. Kumar, J. Joseph, and K. Singh, "Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions," *Opt. Lett.*, vol. 34, no. 3, pp. 331–333, Feb. 2009.
[25] W. Chen, X. Chen, A. Anand, and B. Javidi, "Optical encryption using multiple intensity samplings in the axial domain," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 30, no. 5, pp. 806–812, May 2013.
[26] E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," *Opt. Lett.*, vol. 36, no. 1, pp. 22–24, Jan. 2011.
[27] E. Pérez-Cabré, H. C. Abril, M. S. Millan, and B. Javidi, "Photon-counting double-random-phase encoding for secure image verification and retrieval," *J. Opt.*, vol. 14, no. 9, p. 094001, Sep. 2012.
[28] A. Markman and B. Javidi, *J. Opt. Soc. Amer. A, Opt. Image Sci.,* submitted for publication.
[29] R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.*, vol. 35, no. 9, pp. 2464–2469, Sep. 1996.
[30] Y. Li, K. Kreske, and J. Rosen, "Security and encryption optical systems based on a correlator with significant output images," *Appl. Opt.*, vol. 39, no. 29, pp. 5295–5301, Oct. 2000.
[31] W. Chen, X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," *IEEE Photon. J.*, vol. 5, no. 2, p. 6900113, Apr. 2013.
[32] J. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: Secure and noise-free information retrieval," *Opt. Exp.*, vol. 21, no. 5, pp. 5373–5378, Mar. 2013.
[33] D. Huffman, "A method for the construction of minimum-redundancy codes," *Proc. IRE*, vol. 40, no. 9, pp. 1098–1101, Sep. 1952.
[34] D. Wave, *Answer to your questions about the QR Code*. [Online]. Available: http://www.qrcode.com/en/
[35] Information Technology—Automatic Identification and Data Capture Techniques—QR Code 2005 Bar Code Symbology Specification, ISO, IEC 18004: 2006, 2006.
[36] E. Ohbuchi, H. Hanaizumi, and L. A. Hock, "Barcode readers using the camera device in mobile phones," in *Proc. Int. Conf. Cyberworlds*, M. Nakajima, Ed., 2004, pp. 260–265.
[37] F. Sadjadi and B. Javidi, *Physics of Automatic Target Recognition*. New York, NY, USA: Springer-Verlag, 2007.
[38] B. Javidi, "Nonlinear joint power spectrum based optical correlation," *Appl. Opt.*, vol. 28, no. 12, pp. 2358–2367, Jun. 1989.

[39] F. Dubois, "Automatic spatial frequency selection algorithm for pattern recognition by correlation," *Appl. Opt.*, vol. 32, no. 12, pp. 4365–4371, Jun. 1993.
[40] J. W. Goodman, *Statistical Optics*. Hoboken, NJ, USA: Wiley, 2000.
[41] QR Code Minimum Size. [Online]. Available: http://www.qrstuff.com
[42] [Online]. Available: http://zxing.appspot.com/generator
[43] J. C. Dainty, "The statistics of speckle patterns," in *Progress in Optics*, E. Wolf, Ed. Amsterdam, The Netherlands: North-Holland, 1976.
[44] S. Yuan, "Sensitivity, noise and quantitative model of laser speckle contrast imaging," Ph.D. dissertation, Tufts Univ., Medford, MA, USA, 2012, UMI Dissertation Pub.
[45] R. J. Schalkoff, *Pattern Recognition: Statistical, Structural and Neural Approaches* 1st ed.,, Hoboken, NJ, USA: Wiley, 1991.