2-28-2014

Optical Security using the Double-Random-Phase Encryption with Photon-Counting

Adam Markman
University of Connecticut - Storrs, amarkman89@gmail.com

Optical Security using the Double-Random-Phase Encryption with Photon-Counting

Adam Markman

B.S., University of Connecticut, Storrs, CT, 2011

A Thesis

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Science

At the

University of Connecticut

2014

APPROVAL PAGE

Master of Science Thesis

Optical Security using the Double-Random-Phase Encryption with Photon-Counting

Presented by:

Adam Markman, B.S.

Major Advisor _____

Bahram Javidi

Associate Advisor _____

Rajeev Bansal

Associate Advisor _____

Quing Zhu

University of Connecticut

2014

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my major advisor, Board of Trustees Distinguished Professor Bahram Javidi, for his support and encouragement throughout the course of my studies and research. I thank him for his cooperative idea brainstorming sessions and guidance in carrying out experiments. I would also like to thank my associate advisors, Professors Rajeev Bansal and Quing Zhu for their support, comments, and invaluable contributions to my growth as an engineer.

I was very fortunate to have an exceptionally talented group of lab mates who were always happy to discuss novel ideas in addition to helping make the laboratory a warm and enjoyable working environment. I wish to thank Xiao Xiao, Dr. Myungjin Cho, Dr. Dipak Dey, Dr. Jingang Wang, and Dr. Xiaoxi Chen for their support, encouragement, and collaboration.

I dedicate my M.Sc. thesis to my family and friends for their constant encouragement. I would also like to thank my parents and sister for their love and guidance.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

This chapter is organized into six sections: The first section outlines the motivation for this thesis. The second section provides background information on the double-random-phase encryption. The third section presents the double-random-phase encryption with photon-counting (PC-DRPE). The fourth section discusses how to authenticate the decrypted image from the PC-DRPE. The fifth section discusses combining the Quick Response (QR) code with the double-random-phase encryption. Lastly, section 6 presents the conclusion.

1.1. MOTIVATION

Millions of transactions of sensitive information are performed every day ranging from the exchange of credit card information to using a passport for identification. Ensuring that these transactions do not compromise the security of the information being exchanged is critical. In the Unites States, there were over 13.5 million passport books and passport cards issued in Fiscal Year 2009 [1]. The Department of State government states that in Fiscal Year 2012, there were over 3,900 new cases of passport and visa fraud. Of the fraudulent transactions, counterfeiting, forgery or alteration of a visa is included. If a person is able to obtain a fraudulent passport, they can use this to flee from prosecution, facilitate drug trafficking and terrorist operations, assist with other crimes, such as remain in the Unites States illegally, or smuggle illegal aliens to the United States [2]. According to the Consumer Sentinel Network, the largest number of complaints in 2012 was identify theft [3]. In addition, credit card fraud is up by 87% since 2010 and results in a total loss of $6 billion [4].

Methods exist meant to ensure the authenticity and security of sensitive information. For example, credit cards contain a Holographic image meant to make it difficult to duplicate or

manufacture a false credit card. Moreover, credit cards include a tamper-evident signature panel and embossed numbers that raise the account numbers on the front of the card and extends into a hologram [5]. However, as new security measures are introduced into existing items, security flaws are also exposed. Although the hologram on a credit card increases the complexity of duplicating a credit card, advances in imaging technologies have allowed for the holographic image to be captured using a charged coupled device (CCD) camera allowing a skilled holographer to duplicate the hologram [6].

In addition to physical duplication of sensitive information, many transactions of sensitive information is also passed through the internet and possible insecure networks. If an attacker were to intercept this data, they will have the opportunity to steal this information and use it for their own use. Whether it is the electronic transmission of credit card information or social security numbers, the protection of this information is of utmost importance. Users must be vigilant of phishing scams, malware, and online identity theft [7]. Currently there are encryption algorithms and methods for secure electronic communication such as the Advanced Encryption Standard (AES), which is a symmetric key algorithm meaning that the encryption and decryption keys are identical [8]. Moreover, there is the RSA algorithm, which is a public-key cryptography meaning there is a public key and an associated private key used in the encryption/decryption process [9,10].

Optical technologies have been widely explored to encrypt sensitive information. These technologies have applications ranging from securing fingerprints to identifying a person based on their facial features [7]. One major advantage of optical processing is the speed of processing large amounts of information. In addition, optical security can employ numerous parameters for encryption including wave length, phase information, spatial frequency or polarization of light.

In addition, image information can remain as 256 discrete pixel values instead of having to be converted to ones and zeros for an electronic security processor. Although optical methods can add further layers of security, it does have its disadvantages such as the cost of the equipment to optically implement the encryption scheme or the poor quality of images obtained by optically encrypting or decrypting an image [7]. It is possible to combine optical results with computational algorithms to improve the image quality at the cost of adding further complexity to the system. Nonetheless, current methods of optical encryption are becoming more feasible and can be integrated with current technology.

The double-random-phase encryption (DRPE) [11] is a very popular optical encryption method due to its simplicity. Moreover, it is robust against many different attacks [10,15,16] in practical use such as the brute-force attack and chosen plain-text attacks by simply updating the encryption keys. There have been numerous improvements to the DRPE including the full phase processor [16], applying the DRPE in the Fresnel domain [17] or incorporating the DRPE with digital holography [18]. In addition, the DRPE has had applications in data storage [19-21] and biometrics [22,23].

1.2 The Double-Random-Phase encryption

The double-random-phase encryption will be reviewed. For convenience, one-dimensional notation will be used. To begin, let (x,y) and (v,w) denote the spatial and frequency domain, respectively. In addition, let $f(x,y)$ be the input image and $n(x,y)$ and $b(v,w)$ be two random noises that are uniformly distributed over the interval [0,1]. The encrypted images for the amplitude-based DRPE is given as [11]

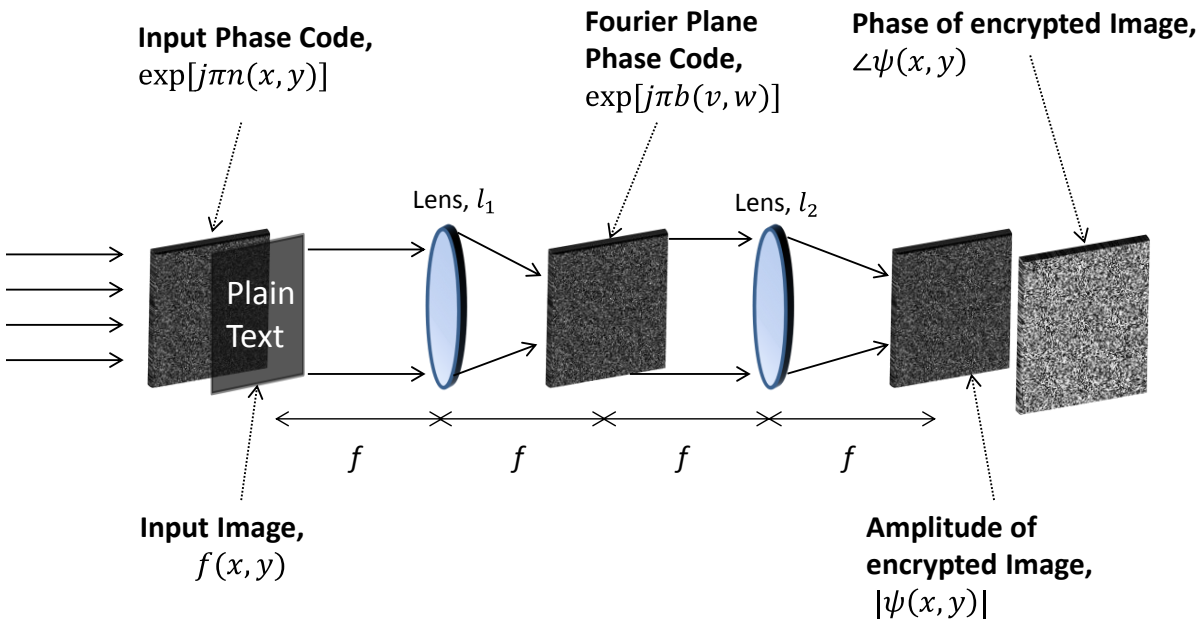
$$\psi(x,y) = \left\{ f(x,y)\exp\left[j2\pi n(x,y)\right]\right\} * h(x,y), \tag{1.1}$$

where $*$ denotes convolution, $\exp[\,j2\pi n(x,y)]$ is a phase mask in the spatial domain, and $h(x,y)$ is a phase mask whose Fourier transform is $\exp[\,j2\pi b(\upsilon,w)]$.

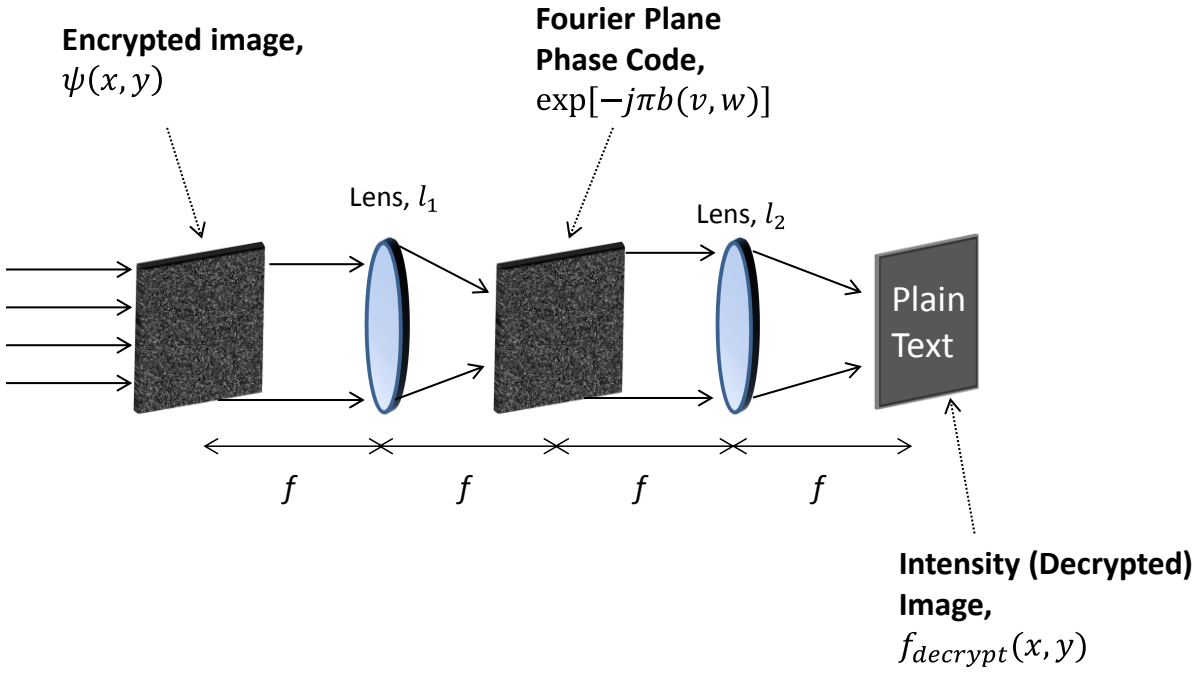
The encrypted images are white stationary noise. It is worth noting that both amplitude and phase information must be encrypted since an image can be partially recovered by either bit of information. Thus, by using phase masks in both the frequency and spatial domains, both of these components of the image are encrypted. Figure 1.1(a) depicts the encryption process.

To decrypt the image, the decryption process of the DRPE method is used. The Fourier transform of $\psi(x,y)$ is taken. It is then multiplied by the complex conjugate of the phase mask used in the encryption process in the frequency domain, $\exp[-j2\pi b(\upsilon,w)]$. The Fourier transform is taken once more bringing this back to the spatial domain so that the function $f_{decrypt}(x,y)\exp[\,j2\pi n(x,y)]$ is obtained where $f_{decrypt}(x,y)$ is the decrypted image. Using an intensity-sensitive device such as a CCD camera can then recover the input image as $\left| f_{decrypt}(x,y)\right|^2$ which is equivalent to $f_{decrypt}(x)$ since the input image is real and positive [11]. Figure 1.1(b) depicts the decryption process.

The security of the DRPE has been analyzed. It was found that the encryption scheme is robust to many attacks, such as the brute force attack. Moreover, many of the attacks can be prevented by simply updating the phase keys [16]. Regardless though, the encryption scheme can still be compromised, such as if an attacker tricks a legitimate user into encrypting a known image or plain text (chosen- plaintext attack). In this situation, it is possible to recover the phase



(a)



(b)

Fig. 1.1. Schematic of (a) double-random-phase encryption (DRPE) encryption process and (b) the DRPE decryption process.

key from the frequency domain. For example, a user may introduce a Dirac signal image into the input system. Thus, the ciphered image is simply the phase key presented in the frequency domain [10,15,16] compromising the security of the encryption scheme.

1.3 The Double-Random-Phase encryption with Photon-Counting

As previously discussed, there are security flaws in the traditional double-random-phase encryption processes. Pérez-Cabré et al. proposed a modification to the DRPE: Instead of using this algorithm as a linear encryption/decryption scheme, modify the process as an authentication method [24]. To do this, photon-counting is performed on the amplitude of the encrypted image. Photon-counting is a process that limits the number of photons arriving at a pixel in an image. Note that this is a nonlinear transformation of the data. Since photon-counting is performed on the amplitude of the encrypted image, information is lost. Thus, rather than recover the primary input image in the decryption process, a noise-like decrypted image is obtained. Since only the amplitude information was modified, and not the phase information, it is possible to authenticate the photon-limited encrypted image using nonlinear processors [25-31. This can have many applications in security including correctly verifying an identification card.

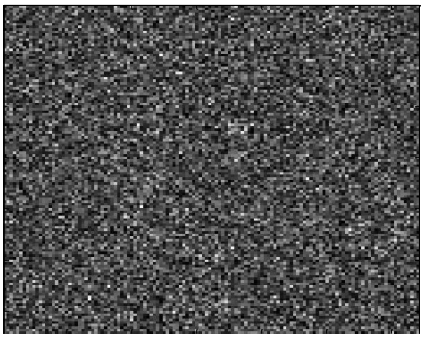
Photon-counting itself is modeled as a Poisson distribution [31-34]. That is not to say that a Poisson distribution is the only model. Depending on the coherent state of light, the photons may follow a binomial, negative binomial, multinomial distribution, or negative multinomial distribution [36]. For experiments, we assume that the coherent state can be modeled as a Poisson distribution. Moreover, the fewer the number of photons arriving at a pixel, the sparser the scene becomes. The probability density function for counting the number of photons at an observation area or arriving at pixel j can be modeled as [32]:

$$P(l_j;\lambda_j)=\frac{[\lambda_j]^{l_j}e^{-\lambda_j}}{l_j!},\ \text{for}\ \lambda_j>0,\ l_j\in\{0,1,2,...\}, \tag{1.2}$$

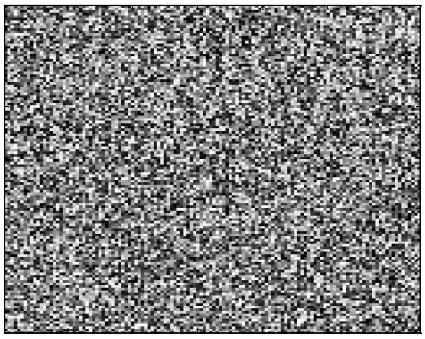
where l_j is the number of photons detected at pixel j and λ_j is the Poisson parameter defined as $N_p x_j$, where N_p is the number of photons in the scene and x_j is the normalized irradiance at pixel j such that $\sum_{j=1}^{M} x_i = 1$ with M being the total number of pixels.

Using Eq. (1.2), the photon-counting approach can be applied to the amplitude of the encrypted images for the DRPE [Eq. (1.1)]. Note that Eq. (1.1) can be rewritten in terms of amplitude and phase of the form $\psi(x,y)=|\psi(x,y)|\exp[j\phi(x,y)]$, where $|\psi(x,y)|$ is the amplitude data and $\phi(x,y)$ denotes the phase information.

(a)

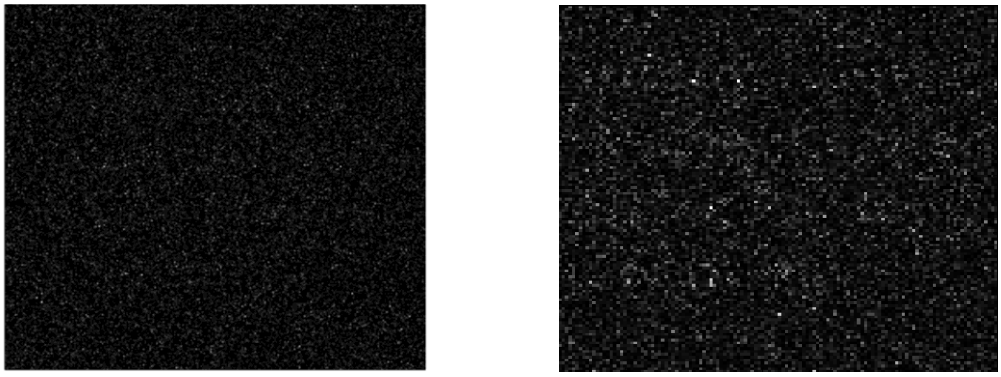


(b)



(c)

Fig. 1.2. (a) 128 x 128 binary input image. (b) the amplitude of the DRPE encrypted image and (c) the phase of the DRPE encrypted images.



(a) (b)

Fig. 1.3. (a) Photon-limited PC-DRPE encrypted image, $\left|\psi_{ph}(x, y)\right|$, using the image shown in Fig. 1.2 (b) at N_p=1000 or 0.0610 photons/pixel and (b) decrypted image from the PC-DRPE of Fig. 1.3 (a).

The photon-counting method can be implemented by normalizing the amplitude of the encrypted images such that $\Gamma\left(x, \mathrm{y}\right) = \left|\psi(x_i, \mathrm{y}_i)\right| / \sum_{i=1}^{M}\sum_{j=1}^{N}\left|\psi(x_i, \mathrm{y}_j)\right|$, where M and N are the total number of pixels in the x and y directions, respectively. The Poisson parameter in Eq. (1.2) is then calculated by multiplying $\Gamma\left(x, \mathrm{y}\right)$ by N_p . For a given N_p, a photon-limited encrypted image for the double-random-phase encryption with photon counting (PC-DRPE), $\psi_{ph}(x, y)$, is obtained. Fig. 1.2(a) shows a 128 x 128 pixel binary input image, $f(x)$. Figures 1.2(b) and 1.2(c) depicts the amplitude and phase, respectively, of the encrypted images for the DRPE, $\psi(x, y)$. Fig. 1.3(a) depicts the photon-limited encrypted image, $\left|\psi_{ph}(x, y)\right|$, at N_p=1000 or 0.0610 photons/pixel.

The process to decrypt the PC-DRPE is identical to the decryption process of the DRPE. The Fourier transform of $\psi_{ph}(x, y)$ is taken. It is then multiplied by the phase mask $\exp[-j2\pi b(\upsilon, w)]$ and the Fourier transform of this product is taken once more yielding $f_{ph}(x, y)\exp[j2\pi n(x, y)]$, where $f_{ph}(x, y)$ is the noise-like decrypted image. The intensity of this product can then be taken yielding

$|f_{ph}(x,y)|^2$ which is equivalent to $f_{ph}(x,y)$ since the primary input image is real and positive. Fig. 1.3(b) depicts the decrypted image of the encrypted image shown in Fig. 1.3(a).

1.4 The Double-random-phase encryption with Photon-Counting Authentication

Using the double-random-phase encryption with photon-counting, the decrypted image is still noise-like [Fig. 1.3(b)] and cannot be verified visually. One possible way to authenticate the decrypted image is by using nonlinear correlation filters [26-31]. The k^{th} order nonlinear filter is an example of a nonlinear correlation filter and was used for authentication due to its simplicity and ease of implementation. The filter is presented, using (v,w) to represent the coordinates in the frequency domain, as:

$$c(x,y) = IFT\left\{\left|F_{ph}(v,w)F(v,w)\right|^k \exp\left[j\left(\phi_{ph}(v,w)-\phi(v,w)\right)\right]\right\}, \quad (1.3)$$

where k is the strength of the applied nonlinear that suppresses the amplitude thus determining the performance of the filter, *IFT* is the inverse Fourier transform, $F(v,w)$ is the Fourier transform of the input image, $F_{ph}(v,w)$ is the Fourier transform of the photon-limited decrypted image, $\phi_{ph}(v,w)$ and $\phi(v,w)$ are the Fourier phase obtained for the decrypted image and input image, respectively, and $||$ is the modulus operator.

Fig. 1.4 (a) depicts the decrypted image of the PC-DRPE using Fig. 1.2 (a) as the input image to the PC-DRPE . Fig. 1.4. (b) depicts a 128 x 128 pixel binary false class image. Figure 1.4(c) shows the output of the k^{th} order nonlinear for k=0.3 with the graph normalized to 1. Fig. 1.4(d) shows the output of the k^{th} order nonlinear filter with k=0.3 using the false class image; the maximum peak is 0.18 indicating that the filter was able to distinguish between a true and false class image.

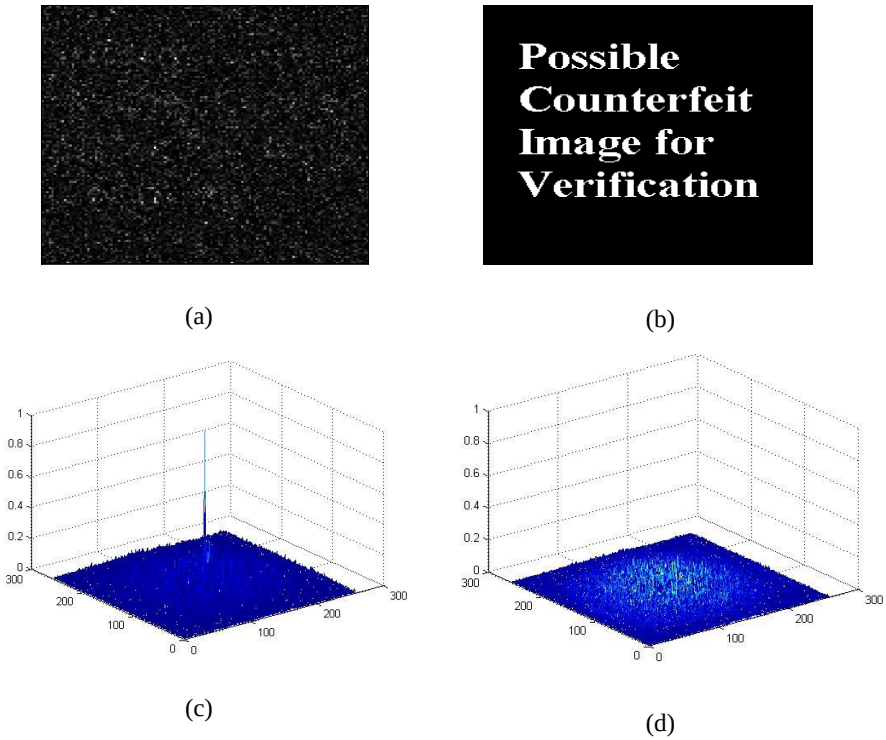


Fig. 1.4. (a) Decrypted (true class) image of the image shown in Fig. 1.2 (a) used in the PC-DRPE encryption scheme; (b) 128 x 128 pixel binary false class image; (c) output of the k^{th} order nonlinear filter with k=0.3 using the true class image normalized to 1; (d) output of the k^{th} order nonlinear filter with k=0.3 using the false class image with a maximum peak of 0.18.

Much research has been done incorporating photon-counting in optical security. In [37], the PC-DRPE was extended into three dimensions using three dimensional (3D) integral imaging. It was shown that the noise-like decrypted image required fewer photons for authentication than the 2D. Moreover, sparse encoding has been investigated [38]. In this technique, the input image is encoded into two phase masks M_1 and M_2. Sparsity is introduced in one of two ways: One way is to generate sparse data from the two phase masks and the second method is to generate sparse data from the plaintext image itself. As with the photon-counting method, it is visually impossible to authenticate the decrypted images; however, correlation filters can be used verify the decrypted images [25-31].

1.5 Quick Response (QR) Code with the Double-Random-Phase Encryption

The Quick Response (QR) code is a two dimensional (2D) barcode that has gained rapid popularity. It was created by D. Wave to serve in the automotive industry in Japan to replace the 1D barcode [39]. The advantage of using a QR code is that it can be scanned regardless of scanning direction or if the QR code is damaged. Moreover, it has much greater storage capabilities than a 1D barcode. Thus, the QR code has found many applications including helping ID patients in hospitals, providing additional information on business cards, and being used in lottery tickets. The QR code has the ability to store upwards of 4,296 alpha numerics, 7,089 numbers, and 2,953 bytes of 8 bit binary data [40-41]. In addition, online QR generators can be used to generate QR codes including the level of error correction and version number [41].

Figure 1.5(a) shows an image of a QR code generated using the ZXing Project [41] containing 36 characters. The QR code itself is a binary image consisting of black squares known as modules placed on a white background where each black square represents some bit of information about the input text. The QR code can be read by a QR reader built into Smartphones such as an iPhone or Android device [42] to retrieve the text. However, as the number of characters stored in the QR code increases, the size of the modules decreases, as shown in Fig. 1.5(b) which is a QR code containing over 200 characters. As a result, if too much information is stored in a QR code, the module size will fall below the resolution limit of the camera used in Smartphones making it difficult for the QR code to be read [43].

Some of the components of the QR code are described in Fig. 1.5(c). A timing pattern is used to tell the QR reader the size of the QR code [39]. Moreover, the finder pattern and alignment pattern are used by the QR reader to determine the position of the QR code. Most

importantly, the QR code contains format information that informs the QR reader what type of mask was used in the QR code, which aides in reading the QR code. Lastly, the QR code contains information regarding the Reed Solomon Error correction [39] to determine the level of error correction needed. Note though that as the error correction level increases, the amount of data that can be stored in the QR code decreases [43]. The QR code also contains information indicating the QR code version number; the higher the version number, the more information that can be stored in the QR code.

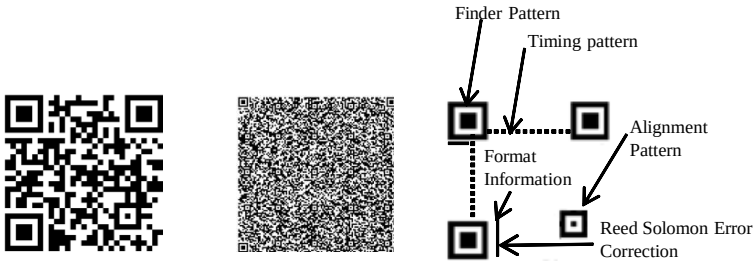
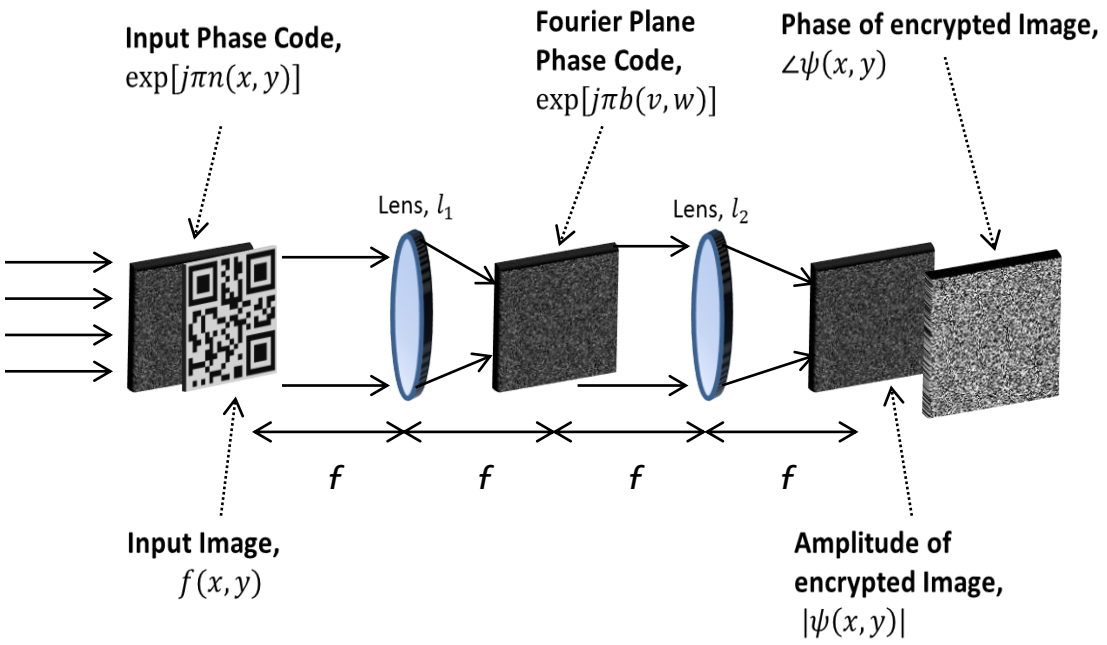


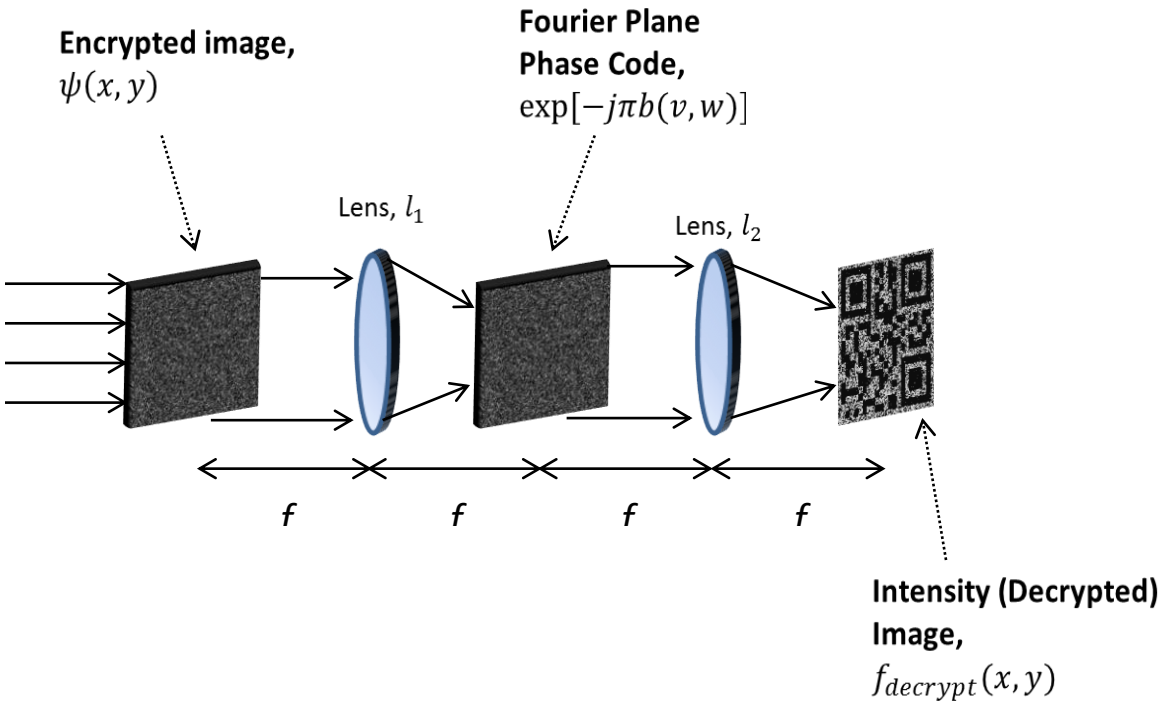
Fig. 1.5 (a) QR Code generated using ZXing Project [22] containing 36 characters; (b) QR code containing over 200 characters; (c) some components of the QR code.

It is worth noting the security flaws inherently in the QR code. One major flaw is that the information inside the QR code cannot be visually seen. Thus, the user must scan the QR code which contains unknown information. With commercial Smartphones, if a QR code is scanned and contains a URL, the phone is automatically redirected to that URL. As a result, the QR code may direct a user to a malicious website that can compromise the security of the QR reader such as phishing and malware attacks [44].

Barrera et. al [45]combined the QR code with the double-random-phase encryption. One disadvantage of optically encoding the DRPE is that the decrypted image is noisy due to random



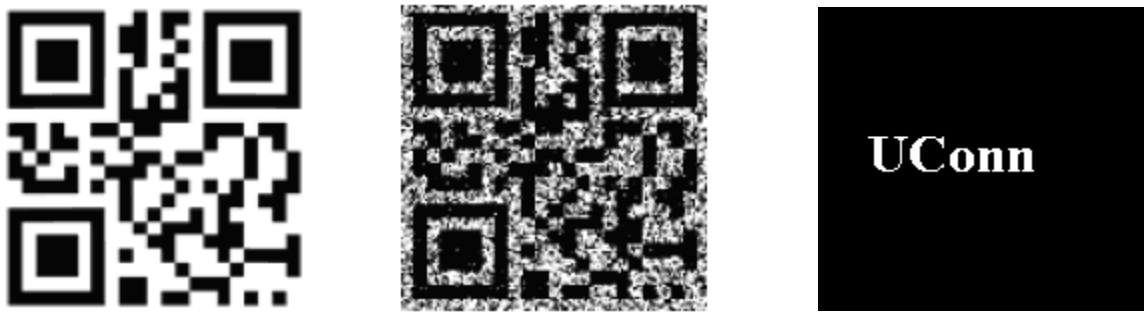
(a)



(b)

Fig. 1.6 (a) Optically encrypting the QR code using the double-random-phase encryption and (b) optically decrypting the encrypted QR code

perturbations and speckle effects degrading the quality of the recovered primary image. To overcome this, text is stored inside of the QR code. The QR code is then optically encoded as shown in Fig. 1.6(a). The encrypted image is then optically decrypted as seen in Fig. 1.6(b); however, the decrypted image is noisy. Due to reed-Solomon error correction incorporated into the QR code design, a Smartphone is capable of scanning the QR code and retrieving the information stored inside of the QR code. Fig. 1.7(a) depicts the original QR code while Fig. 1.7(b) shows the optically decrypted QR code shown in Fig. 1.7(a). Figure 1.7 (c) shows the scanned text stored inside of the QR code shown in Fig. 1.7(b).



(a) (b) (c)

Fig. 1.7 (a) Optically encrypting the QR code using the double-random-phase encryption and (b) optically decrypting the encrypted QR code

1.6 Conclusion

Improving the security of sensitive information is extremely important. To mitigate the ability of an attacker to gain access to this information is a challenging task. As new security measures are introduced, established security schemes are compromised. Sensitive information can be transported physically, such as a passport, or electronically, such as sending credit card information over the internet. Many methods exist to add security to these methods; however, optical encryption schemes hold many advantages, such as the ability to be implemented either

optically or electronically or a combination of both. Moreover, optical schemes have the ability to contain multiple keys for decryption including wavelength, phase mask information, or reconstruction distance. Although the technology needed to perform optical experiments can be expensive, with further research optical security methods can become more common.

The double-random-phase encryption is a widely researched encryption scheme. It has many nice properties including its ease of implementation and robustness to noise and attacks especially when the phase masks are updated. The DRPE has found applications in image authentication by applying a photon-counting technique to the amplitude of the encrypted image. Although the decrypted image cannot be visually authenticated as the primary input image, it is possible to verify the decrypted image using optical nonlinear filters. In this manuscript, further investigation of the DRPE with photon-counting is performed along with potential applications.

Chapter 2

Full phase photon-counting double-random-phase encryption*

We investigate a full phase based photon-counting double-random-phase encryption (PC-DRPE) method. A photon-counting technique is applied during the encryption process creating sparse images. The statistical distribution of the photon-counting decrypted data for full phase encoding and amplitude phase encoding are derived and their statistical parameters are used for authentication. The performance of the full phase PC-DRPE is compared with the amplitude-based PC-DRPE method. The photon-counting decrypted images make it difficult to visually authenticate the input image; however, advanced correlation filters can be used to authenticate the decrypted images given the correct keys. Initial computational simulations show that the full phase PC-DRPE has the potential to require fewer photons for authentication than the amplitude-based PC-DRPE.

The chapter is arranged as follows: in Section 2, the encryption and decryption process for the full phase and amplitude-based double-random-phased encryption with photon-counting (PC-DRPE) is discussed. In Subsection 3. A, the decrypted image from the amplitude-based PC-DRPE is analyzed. In Subsection 3. B, the decrypted image from the full phase PC-DRPE is analyzed. The statistical distributions are derived for each case. In Section 4, an optical processor is used to verify the decrypted images obtained from both encryption methods. In Section 5, a comparison between the full phase and amplitude-based PC-DRPE using the optical processor is discussed. In Section 6, the conclusion is presented.

*A. Markman and B. Javidi, " Full phase photon counting double-random-phase encryption," Journal of the Optical Society of America A, doc. ID 196636 (posted 1 Dec 2013, in press).

2.1. INTRODUCTION

The role of optical imaging for information security has been investigated by many researchers [1-20]. The double-random-phase encryption (DRPE) technique [11] is able to encrypt and decrypt an image; however, there may be security flaws in the system [14-15]. Some of these issues may be resolved by frequently updating the phase masks used in the DRPE [15]. Over the years, many improvements to the DRPE have been developed [16-20,24,45-57]. These include the full phase processor [16], applying the DRPE in the Fresnel domain [17] or incorporating the DRPE with digital holography [18]. Moreover, the DRPE has had applications in data storage [19-21] and biometrics [22,23]. In [24], Pérez-Cabré et al. proposed an additional layer of security to the amplitude-based DRPE by applying photon-counting to the encrypted image generating a photon-limited image. This technique is able to control the number of photons that arrive at a pixel through a stochastic Poisson process. By limiting the number of photons, a sparse encrypted image is created. Thus, rather than recover the entire input image in the decryption process, the decrypted image is sparse. However, correlation processors [25-31] can be used to verify the decrypted image.

2.2. ENCRYPTION AND DECRYPTION PROCESS

The double-random-phase encryption (DRPE) will be reviewed briefly for both the amplitude-based and full phase DRPE. For convenience, one-dimensional notation will be used. To begin, let (x) and (υ) denote the spatial and frequency domain coordinates, respectively. In addition, let $f(x)$ be the input image and $n(x)$ and $b(\upsilon)$ be two random keys that are uniformly distributed over the interval [0,1]. The encrypted images for the amplitude-based DRPE and full phase DRPE are given as [11,16]

$$\psi_{amp}(x) = \left\{ f(x) \times \exp\left[j2\pi n(x) \right] \right\} * h(x), \tag{2.1}$$

$$\psi_{full}(x) = \left\{ \exp\left[j\pi f(x) \right] \times \exp\left[j2\pi n(x) \right] \right\} * h(x), \tag{2.2}$$

where $\times$ denotes multiplication, $*$ denotes convolution, $\exp[j2\pi n(x)]$ is a phase mask in the spatial domain, and $h(x)$ is a mask whose Fourier transform is $\exp[j2\pi b(\upsilon)]$.

Photon-counting is then applied to the encrypted image. This process limits the number of photons arriving at each pixel according to a statistical distribution process [24]. It has been shown that this process can be modeled as a Poisson distribution [32-35]. Moreover, the fewer the number of photons arriving at a pixel, the sparser the scene becomes. The probability density function for counting the number of photons at an observation area or arriving at pixel *i* can be modeled as [32]:

$$P(l_i; \lambda_i) = \frac{[\lambda_i]^{l_i} e^{-\lambda_i}}{l_i!}, \quad \text{for } \lambda_i > 0, \; l_i \in \{0,1,2,...\}, \tag{2.3}$$

where l_i is the number of photons detected at pixel i and λ_i is the Poisson parameter defined as $N_p x_i$, where N_p is the number of photons in the scene and x_i is the normalized irradiance at pixel i such that $\sum_{i=1}^{M} x_i = 1$ with M being the total number of pixels.

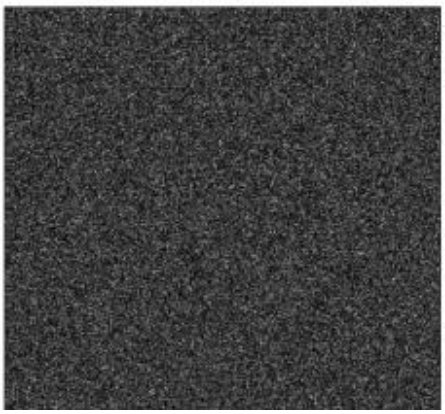
Using Eq. (2.3), the photon-counting approach can be applied to the encrypted images for both the full phase and amplitude-based DRPE [see Eqs. (2.1) and (2.2)]. Note that Eqs. (2.1) and (2.2) can be rewritten in terms of amplitude and phase of the form $\psi(x) = |\psi(x)| \exp[j\phi(x)]$, where $|\psi(x)|$ is the amplitude data and $\phi(x)$ denotes the phase information.

More specifically, photon-counting is applied to the amplitude of the encrypted images for both the amplitude based and full phase DRPE [see Eqs. (2.1) and (2.2)] to generate the photon-limited

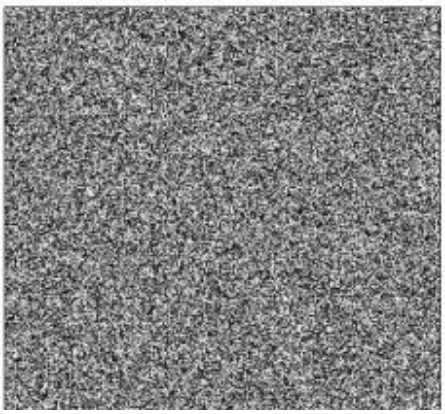
encrypted image, $|\xi(x)|$. Note that Eqs. (2.1) and (2.2) can be rewritten in terms of amplitude and phase of the form $\psi(x) = |\psi(x)| \exp[j\phi(x)]$, where $|\psi(x)|$ is the amplitude data and $\phi(x)$ denotes the phase information. The normalized irradiance is calculated such that $\Gamma(x) = |\psi(x_i)| / \sum_{i=1}^{M} |\psi(x_i)|$. The Poisson parameter in Eq. (3) is then calculated by multiplying $\Gamma(x)$ by N_p. Using Eq. (3), the encrypted and photon-limited amplitude data, $|\xi(x)|$, is generated. For a given N_p, photon-limited encrypted images for the amplitude based and full phase PC-DRPE, $\xi_{amp}(x)$ and $\xi_{full}(x)$, respectively, are obtained. Fig. 2.1(a) shows a 256 x 256 pixel binary input image, $f(x)$. Figures 2.1(b) and 2.1(c) depict the amplitude of the encrypted images for the amplitude based DRPE, $\psi_{amp}(x)$ and $\psi_{full}(x)$, respectively. Figures 2.1(d) and 2.1(e) show the sparse encrypted images $|\xi_{amp}(x)|$ and $|\xi_{full}(x)|$, respectively, for N_p =1000 photons or 0.0152 photons/pixel.

To decrypt the image, the decryption process of the DRPE method is used. For the amplitude based PC-DRPE, the Fourier transform of $\xi_{amp}(x)$ is taken. It is then multiplied by the complex conjugate of the phase mask used in the encryption process in the frequency domain, $\exp[-i2\pi b(\upsilon)]$. The Fourier transform is taken once more bringing this back to the spatial domain so that the function $f_{ph\,amp}(x)\exp[i2\pi n(x)]$ is obtained where $f_{ph\,amp}(x)$ is the noise-like decrypted image. Using an intensity-sensitive device such as a CCD camera can then recover the input image as $|f_{ph\,amp}(x)|^2$ which is equivalent to $f_{ph\,amp}(x)$ since the input image is real and positive [1]. Figure 2.2(a) shows the decrypted image at N_p = 1000 or 0.0152 photons/pixel. It is impossible to visually identify the input image.

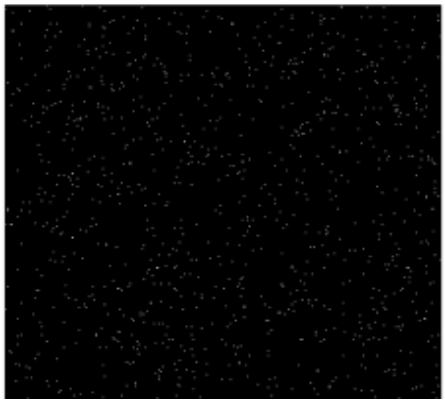
(a)



(b)



(c)



(d)

(e)

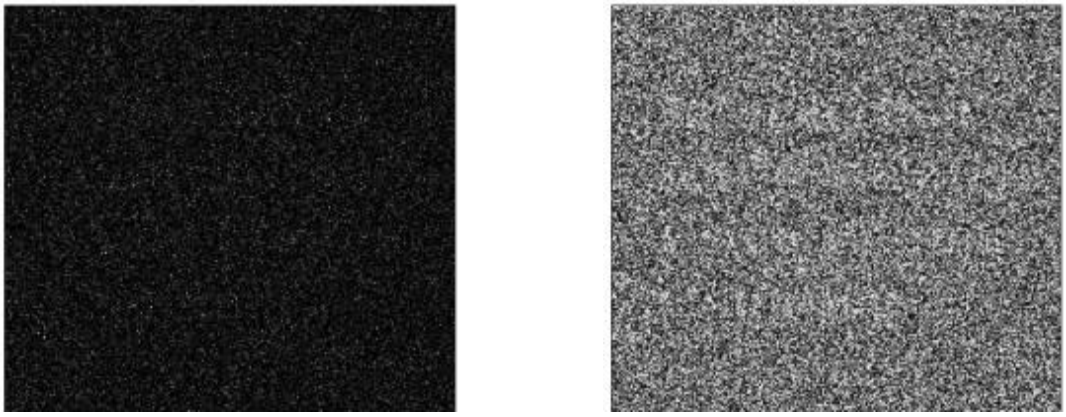
Fig. 2.1 (a) 256 x 256 pixel input image, $f(x)$; amplitude of the encrypted image for the (b) amplitude based DRPE, $\psi_{amp}(x)$, and the (c) full phase DRPE, $\psi_{full}(x)$; photon-limited encrypted images with 1000 photons in the scene (N_p) or 0.0152 photons/pixel for the (d) amplitude based PC-DRPE, $|\xi_{amp}(x)|$, and the (e) full phase PC-DRPE, $|\xi_{full}(x)|$.

The full phase PC-DRPE encrypted image can be decrypted in a similar fashion. Since the input image is real and positive, the photon-limited decrypted image, $f_{ph_{full}}(x)$, is [16]:

$$\left| f_{ph_{full}}(x) \right| = \left| Arg\left\{ A\exp\left[j\pi f_{ph_{full}}(x) \right] \right\} / \pi \right|, \tag{2.4}$$

where A is the amplitude of the decrypted image, $\|$ is the modulus operation, and Arg is the argument function that restricts the phase angle from $-\pi$ to π.

Figure 2.2(b) shows the decrypted image for N_p = 1000 or 0.0152 photons/pixel. As with the amplitude based PC-DRPE, we cannot visually identify the input image.



(a) (b)

Fig. 2.2 Decrypted images for the (a) amplitude-based and the (b) full phase PC-DRPE at N_p = 1000.

3. ANALYSIS OF THE PHOTON-COUNTING DECRYPTED IMAGES

The statistical distributions of the noise-like decrypted images are derived for the amplitude-base and full phase PC-DRPE. Showing that the noise-like distributions are not random can potentially aide in determining whether the encrypted image has been tampered or to possibly reconstructing the primary

image from the decrypted image. Moreover, the statistical properties can be utilized in correlation processors that require the statistical parameters of a scene

A. Amplitude-based PC-DRPE

For the amplitude-based PC-DRPE, the decrypted image is defined as $\left| f_{ph\,amp}(x) \right|^2$. Since $f_{ph\,amp}(x)$ consists of both real and imaginary terms, it can be rewritten as:

$$f_{ph\,amp}(x) = \Re\left\{ f_{ph\,amp}(x) \right\} + j\Im\left\{ f_{ph\,amp}(x) \right\}, \tag{2.5}$$

where $\Re\{\cdot\}$ and $\Im\{\cdot\}$ represent the real and imaginary terms, respectively.

For a low number of photons in the scene (N_p), the Shapiro-Wilks test [58] can be used to verify that $\Re\left\{ f_{ph\,amp}(x) \right\}$ and $\Im\left\{ f_{ph\,amp}(x) \right\}$ each come from a normal distribution. More specifically, it tests:

$$\begin{aligned} &H_o : \text{data comes from } N\left(\mu, \sigma^2\right) \text{ vs.} \\ &H_a : \text{data not come from } N\left(\mu, \sigma^2\right). \end{aligned} \tag{2.6}$$

where μ $\left(-\infty < \mu < \infty\right)$ is the mean and σ^2 (>0) is the variance.

To construct the test, the data, which is assumed to be independent and identically distributed (iid), is arranged in ascending order:

$$x_1 \le x_2 \le \ldots \le x_n. \tag{2.7}$$

The following equation is then implemented:

$$W = \left[\sum_{i=1}^{k} a_i \left(x_{n-i+1} - x_i\right)\right]^2 \Big/ \sum_{i=1}^{n} \left(x_i - \bar{x}\right)^2, \quad \text{for i=1,2,…}k, \tag{2.8}$$

where $\bar{x}$ is the sample mean, a_i is a tabulated constant, and k is defined as

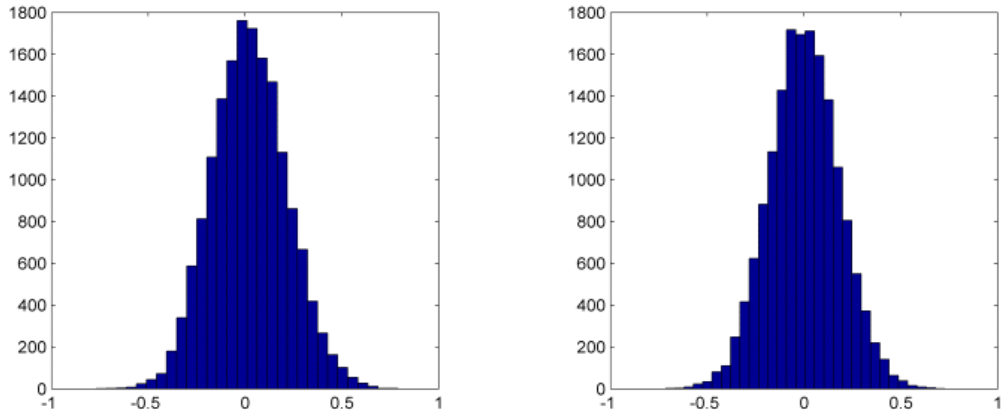
$$k = \begin{cases} (n+1)/2, & \text{if n is odd} \\ n/2, & \text{if n is even} \end{cases}. \tag{2.9}$$

The null hypothesis is then rejected if W is less than some critical value of the test, W_α, where α is the significance level [59].

Figures 2.3(a) and 2.3(b) depict a histogram of $\Re\{f_{ph\,amp}(x)\}$ and $\Im\{f_{ph\,amp}(x)\}$, respectively, for the image shown in Figure 2.2(a); both terms appear to be normally distributed. Using the Shapiro-Wilks test at $\alpha = 0.05$, the calculated p-values [59] are 0.9125 and 0.5600 for $\Re\{f_{ph\,amp}(x)\}$ and $\Im\{f_{ph\,amp}(x)\}$, respectively, indicating that we fail to reject the null hypothesis that the data is normally distributed. Moreover, both distributions are approximately zero mean with different variances that can be estimated using maximum-likelihood estimation for the variance of a normally distributed random variables [59] :

$$\hat{\sigma}^2 = \frac{1}{n}\sum_{i=1}^{n} x_i^{\,2}, \tag{2.10}$$

where n is the total number of x_i.



(a) (b)

Fig. 2.3. Histogram of (a) $\Re\{f_{ph\,amp}(x)\}$, which is $N(0,0.0159)$, and (b) $\Im\{f_{ph\,amp}(x)\}$, which is $N(0,0.0146)$, for image shown in Fig. 2.2(a).

Using Eq. (2.10), the variance of $\Re\{f_{ph\,amp}(x)\}$, $\hat{\sigma}^2_{1,\text{amp}}$, was equal to 0.0159 while the variance for $\Im\{f_{ph\,amp}(x)\}$, $\hat{\sigma}^2_{2,\text{amp}}$, was equal to 0.0146. The distributions of $\Re\{f_{ph\,amp}(x)\}$ and $\Im\{f_{ph\,amp}(x)\}$ can be written as:

$$\Re\left\{f_{ph_{amp}}(x)\right\} \sim N\left(0,\hat{\sigma}^2_{1,amp}\right), \tag{2.11}$$

$$\Im\left\{f_{ph_{amp}}(x)\right\} \sim N\left(0,\hat{\sigma}^2_{2,amp}\right). \tag{2.12}$$

The decrypted image can be expressed as

$$\left|f_{ph_{amp}}(x)\right|^2 = \left[\Re\left\{f_{ph_{amp}}(x)\right\}\right]^2 + \left[\Im\left\{f_{ph_{amp}}(x)\right\}\right]^2. \tag{2.13}$$

Using Eqs. (2.11-2.13), the distributions of $\Re\{f_{ph\,amp}(x)\}^2$ and $\Im\{f_{ph\,amp}(x)\}^2$ can be written as a gamma distribution [See Appendix A for the derivation]:

$$\left[\Re\left\{f_{ph_{amp}}(x)\right\}\right]^2 \sim \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{1,amp}\right), \tag{2.14}$$

$$\left[\Im\left\{f_{ph_{amp}}(x)\right\}\right]^2 \sim \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{2,amp}\right). \tag{2.15}$$

The derived distribution of the decrypted image is then

$$\begin{aligned}\left|f_{ph_{amp}}(x)\right|^2 &\sim \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{1,amp}\right) + \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{2,amp}\right), \\ &\sim \sum_{i=1}^{2} \Gamma_i\left(\frac{1}{2}, 2\hat{\sigma}^2_{\mathrm{i},amp}\right).\end{aligned} \tag{2.16}$$

The two-sample Kolmogorov-Smirnov (K-S) test [60] is used to verify that the decrypted image follows a $\sum_{i=1}^{2}\Gamma_i\left(1/2, 2\hat{\sigma}^2_{i,amp}\right)$ distribution by comparing the empirical cumulative distribution function (ECDF) of simulated data from $\sum_{i=1}^{2}\Gamma_i\left(1/2, 2\hat{\sigma}^2_{i,amp}\right)$ with the ECDF of the decrypted image. If the difference of the ECDF between the decrypted image and the theoretical distribution is below some threshold for each corresponding data point, then we can conclude that the decrypted image follows a $\sum_{i=1}^{2}\Gamma_i\left(1/2, 2\hat{\sigma}^2_{i,amp}\right)$. To calculate the ECDF for iid X_i , the data is first arranged in ascending order [Eq. (2.7)].

The ECDF is then calculated as

$$F(x) = \frac{1}{n}\sum_{i=1}^{n} I[\mathrm{X}_i \le \mathrm{x}], \tag{2.17}$$

where n is the total number of samples and I is the indicator function.

The hypothesis test is:

$$H_o : F_{amp}(x) = F_{1,t}(x) \text{ vs. } H_a : F_{amp}(x) \neq F_{1,t}(x), \tag{2.18}$$

where $F_{amp}(x)$ is the ECDF of the decrypted image and $F_{1,t}(x)$ is the ECDF of the theoretical distribution $\sum_{i=1}^{2} \Gamma_i\left(1/2, 2\sigma_{i,amp}^2\right)$.

H_o is then rejected if

$$\max_x \left|F_{amp}(x) - F_{1,t}(x)\right| > K_\alpha, \tag{2.19}$$

where K_α is a tabulated value and α is the significance level.

Note that bootstrapping [61] is used to estimate the parameters of the simulated $\sum_{i=1}^{2} \Gamma_i\left(1/2, 2\sigma_{i,amp}^2\right)$ to ensure that that K-S test does not favor the null hypothesis. The test was performed using the image shown in Fig. 2.2(a). After 1000 bootstraps, $\hat{\sigma}_{1,amp*}^2$ and $\hat{\sigma}_{2,amp*}^2$ were 0.0159 and 0.0146, respectively. Using the K-S test at $\alpha = 0.05$, a p-value of 0.1350 was calculated indicating that we fail to reject H_o. Thus, we can conclude that the distribution of the photon-counting decrypted image for a low N_p is $\sum_{i=1}^{2} \Gamma_i\left(1/2, 2\sigma_{i,amp}^2\right)$. Figure 2.4 shows a histogram of the decrypted amplitude-based PC-DRPE image shown in Fig. 2.2(a).

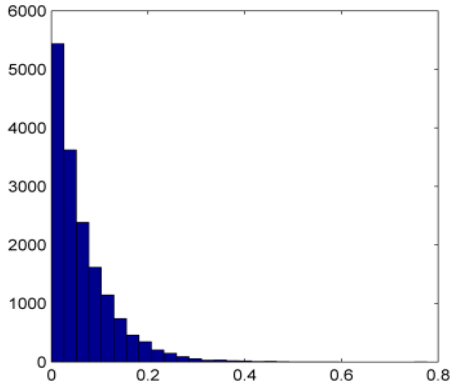


Fig. 2.4. Histogram of the decrypted amplitude-based PC-DRPE image [Fig. 2.2(a)] which follows a sum of Gamma distributions , $\sum_{i=1}^{2}\Gamma_i\left(1/2, 2\sigma_{i,amp}^2\right)$, with $\hat{\sigma}_{1,\text{amp}}^2 = 0.0159$ and $\hat{\sigma}_{2,\text{amp}}^2 = 0.0146$ at N_p=1000.

If we assume that $\Re\{f_{ph\,amp}(x)\}$ and $\Im\{f_{ph\,amp}(x)\}$ are independent, the expected value and variance of $\sum_{i=1}^{2}\Gamma_i\left(1/2, 2\sigma_{i,amp}^2\right)$ are

$$E\left[\sum_{i=1}^{2}\Gamma_i\left(\frac{1}{2}, 2\sigma_{i,amp}^2\right)\right] = \sigma_{1,amp}^2 + \sigma_{2,amp}^2, \tag{2.20}$$

$$Var\left[\sum_{i=1}^{2}\Gamma_i\left(\frac{1}{2}, 2\sigma_{i,amp}^2\right)\right] = 2\sigma_{1,amp}^4 + 2\sigma_{2,amp}^4. \tag{2.21}$$

The derived mean and variance can then be used in spatial filters or correlators [25-31] to authenticate the decrypted image.

B. Full phase PC-DRPE

For the decrypted full phase based PC-DRPE [Eq. (2.4)], $A\exp\left[j\pi f_{ph\,full}(x)\right]$ can be rewritten in terms of real and imaginary components:

$$A\exp\left[j\pi f_{ph\,full}(x)\right] = A\cos\left[\pi f_{ph\,full}(x)\right] + jA\sin\left[\pi f_{ph\,full}(x)\right], \tag{2.22}$$

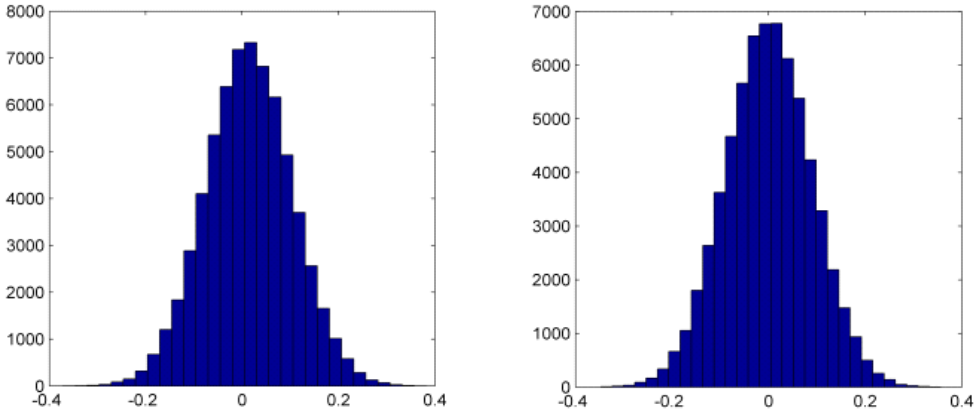
where $A\cos\left[\pi f_{ph\,full}(x)\right]$ represents the real component and $A\sin\left[\pi f_{ph\,full}(x)\right]$ is the imaginary component.

For a low N_p, the Shapiro-Wilks test [49] shows that $A\cos\left[\pi f_{ph\,full}(x)\right]$ and $A\sin\left[\pi f_{ph\,full}(x)\right]$ are both Gaussian. Using the image shown in Fig. 2.2(b), the p-values from the Shapiro-Wilks test at $\alpha = 0.05$ for $A\cos\left[\pi f_{ph\,full}(x)\right]$ and $A\sin\left[\pi f_{ph\,full}(x)\right]$ are 0.3012 and 0.8047, respectively, indicating that we fail to reject the null hypothesis that the data is normally distributed. Moreover, both distributions are zero mean with slightly different variances [Eq. (2.10)]: for $A\cos\left[\pi f_{ph\,full}(x)\right]$, $\hat{\sigma}^2_{1,\,full}$ =0.0075 while for $A\sin\left[\pi f_{ph\,full}(x)\right]$, $\hat{\sigma}^2_{2,\,full}$ = 0.0076. Thus, the distributions of $A\cos\left[\pi f_{ph\,full}(x)\right]$ and $A\sin\left[\pi f_{ph\,full}(x)\right]$ are

$$A\cos\left[\pi f_{ph\,full}(x)\right] \sim N\left(0, \hat{\sigma}^2_{1,\,full}\right), \tag{2.23}$$

$$A\sin\left[\pi f_{ph\,full}(x)\right] \sim N\left(0, \hat{\sigma}^2_{2,\,full}\right). \tag{2.24}$$

Figure 2.5 depicts a histogram of $A\cos\left[\pi f_{ph\,full}(x)\right]$ and $A\sin\left[\pi f_{ph\,full}(x)\right]$ which appear Gaussian.



(a) (b)

Fig. 2.5. Histogram of (a) $A\cos\left[\pi f_{ph\,full}(x)\right]$, which is $N\left(0,0.0075\right)$, and (b) $A\sin\left[\pi f_{ph\,full}(x)\right]$, which is $N\left(0,0.0076\right)$, of the full phase PC-DRPE image shown in Fig. 2.2(b).

The final decrypted image [Eq. (2.4)] can be rewritten as

$$\left|Arg\left\{\exp\left[j\pi f_{ph\,full}(x)\right]\right\}/\pi\right| = \left|Arg\left\{A\cos\left[\pi f_{ph\,full}(x)\right] + jA\sin\left[\pi f_{ph\,full}(x)\right]\right\}/\pi\right|. \tag{2.25}$$

The $\arctan(\cdot)$ function is used to compute the argument of complex data [Eq. (2.4) and Eq. (2.25)]. Since $A\cos\left[\pi f_{ph\,full}(x)\right]$ and $A\sin\left[\pi f_{ph\,full}(x)\right]$ are both normally distributed [Eq. (2.23) and Eq. (2.24), respectively], the quantity inside the $\arctan(\cdot)$ function is the quotient of two independent normally distributed random variables which is a Cauchy distribution [53]. This can be written as

$$\frac{\sin\left[\pi f_{ph\,full}(x)\right]}{\cos\left[\pi f_{ph\,full}(x)\right]} \sim \frac{N\left(0,\hat{\sigma}^2_{2,\,full}\right)}{N\left(0,\hat{\sigma}^2_{1,\,full}\right)} = Cauchy\left(0,\frac{\hat{\sigma}_{2,\,full}}{\hat{\sigma}_{1,\,full}}\right), \tag{2.26}$$

where 0 is the location parameter and $\hat{\sigma}_{2,\,full}/\hat{\sigma}_{1,\,full}$ represents the scale parameter that dictates the spread of the distribution.

The *Arg* function wraps the Cauchy distribution around the unit circle on the interval $(-\pi,\pi]$. The distribution Z= $Arg\left[A\exp\left[j\pi f_{phfull}(x)\right]\right]$ is then the wrapped Cauchy distribution, $WC(\gamma,\rho)$, with probability density function (PDF) [62-65]

$$\mathrm{Z}\sim\frac{1}{2\pi}\frac{1-\rho^2}{1+\rho^2-2\rho\cos(z-\gamma)},$$

$$-\pi<\gamma\le\pi,\ \ 0<\rho<1. \tag{2.27}$$

where γ is the mean angle defined for all wrapped distributions as:

$$\gamma=Arg\left\{\sum_{i=1}^{n}\cos(z_i)+j\sum_{i=1}^{n}\sin(z_i)\right\}, \tag{2.28}$$

where *Arg* is the argument function and *n* is the total number of z_i.

The variable ρ is the mean vector length defined for all wrapped distributions as:

$$\rho=\left[\left(\sum_{i=1}^{n}\cos(z_i)/n\right)^2+\left(\sum_{i=1}^{n}\sin(z_i)/n\right)^2\right]^{1/2}, \tag{2.29}$$

where *n* is the total number of z_i.

To estimate γ and ρ, maximum likelihood estimation can be used based on the recursive algorithm [54-56]. To begin, we reparameterize Eq. (2.27) by letting

$$\gamma_1=\frac{2\rho\cos\gamma}{1+\rho^2},\qquad \gamma_2=\frac{2\rho\sin\gamma}{1+\rho^2}. \tag{2.30}$$

The wrapped Cauchy distribution can then be rewritten as [See Appendix B for the derivation]

$$Z \sim \frac{1}{2\pi} \frac{1}{c\left(1-\gamma_1 \cos z - \gamma_2 \sin z\right)}, \tag{2.31}$$

where

$$c = c\left(\gamma_1, \gamma_2\right) = \frac{1}{\sqrt{1-\gamma_1^2-\gamma_2^2}} \ . \tag{2.32}$$

We then make an additional parameterization to simplify the likelihood equations:

$$\eta_1 = c\gamma_1 \text{ and } \eta_2 = c\gamma_2. \tag{2.33}$$

We also note that Eq. (2.32) can be rewritten in terms of η_1 and η_2 [See Appendix C for the derivation]:

$$c = \sqrt{1+\eta_1^2+\eta_2^2}. \tag{2.34}$$

Thus, Eq. (2.31) can be rewritten as

$$Z \sim \frac{1}{2\pi} \frac{1}{\left(\sqrt{1+\eta_1^2+\eta_2^2} - \eta_1 \cos z - \eta_2 \sin z\right)}. \tag{2.35}$$

Taking the log likelihood of Eq. (2.35) along with the derivative with respect to η_1 and η_2 yields

$$\frac{1}{c}\sum_{i=1}^{n} w_i \left[\cos z_i - \gamma_1\right] = 0, \tag{2.36}$$

$$\frac{1}{c}\sum_{i=1}^{n} w_i \left[\sin z_i - \gamma_2\right] = 0, \tag{2.37}$$

where $w_i = 1/\left(1-\gamma_1 \cos z_i - \gamma_2 \sin z_i\right)$ for i=1,..,n.

We can rearrange Eqs. (2.36) and (2.37) to solve for γ_1 and γ_2:

$$\gamma_1 = \left\{\sum_{i=1}^{n} w_i \cos z_i\right\} \Big/ \sum_{i=1}^{n} w_i \,, \tag{2.38}$$

$$\gamma_2 = \left\{\sum_{i=1}^{n} w_i \sin z_i\right\} \Big/ \sum_{i=1}^{n} w_i \,. \tag{2.39}$$

To calculate $\hat{\gamma}$ and $\hat{\rho}$, an iterative re-weighting algorithm [65,66] is used to find the maximum likelihood estimators of $\hat{\gamma}_1$ and $\hat{\gamma}_2$ which is given by:

1) Initialize $\gamma_1^{[0]}$ and $\gamma_2^{[0]}$ with $\gamma_1^{[0]} + \gamma_2^{[0]} < 1$ using Eq. (2.30).

2) Calculate $w_i^{[0]}$.

3) Given $\gamma_1^{[k]}, \gamma_2^{[k]}$, and $w_i^{[k]}$ at iteration k, calculate $\gamma_1^{[k+1]}$ and $\gamma_2^{[k+1]}$ using Eqs. (2.38) and (2.39), respectively.

4) Repeat step 3 until the algorithm converges for $\hat{\gamma}_1$ and $\hat{\gamma}_2$.

The maximum likelihood estimates for $\hat{\gamma}$ and $\hat{\rho}$ can be calculated as [54-56]

$$\hat{\gamma} = \tan^{-1}\left[\frac{\hat{\gamma}_2}{\hat{\gamma}_1}\right], \tag{2.40}$$

$$\hat{\rho} = \frac{1 - \sqrt{1 - \hat{\gamma}_1 - \hat{\gamma}_2}}{\sqrt{\hat{\gamma}_1^{\,2} + \hat{\gamma}_2^{\,2}}}\,, \tag{2.41}$$

where $\tan^{-1}(\cdot)$ is the four quadrant inverse tangent.

We note that γ is approximately 0 for low N_p. Thus, $Arg\left[A\exp\left[j\pi f_{ph\,full}(x)\right]\right]$ is distributed as $WC(0,\rho)$.

As $\rho \to 0$, which coincides with $N_p \to 0$, $Arg\left\{A\exp\left[j\pi f_{ph\,full}(x)\right]\right\} \Big/ \pi$ converges to a uniform distribution [53-56] on the interval (-1,1). Thus:

$$\left| Arg\left\{ A\exp\left[j\pi f_{ph_{full}}(x) \right] \right\} / \pi \right| \to U(0,1) \text{ as } \rho \to 0. \tag{2.42}$$

Figure 2.6(a) shows an unwrapped histogram [40] from the full phase PC-DRPE decrypted image shown in Fig. 2.1(a) at N_p =10 or 1.52e-4 photons/pixel which appears to follow a uniform distribution $U(0,1)$ at $\hat{\rho} = 0.0115$.

Using variable transformation [50], if we let y=$\left| Arg\left\{ A\exp\left[j\pi f_{ph_{full}}(x) \right] \right\} \right|$, which is equivalent to the absolute value of the wrapped Cauchy distribution, the PDF of y then becomes [See Appendix D for the derivation]

$$h(y) \sim \frac{1}{\pi} \frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)},\ 0 \le y \le \pi,\ 0 < \rho < 1. \tag{2.43}$$

Since the range of y is $0 \le y \le \pi$, the expected value of the decrypted image [Eq. (2.4)] can be calculated as :

$$\frac{1}{\pi} E[y] = \frac{1}{\pi} \int_0^{\pi} y \frac{1}{\pi} \frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)} dy, \tag{2.44}$$

where $E[\cdot]$ is expected value.

Moreover, the variance can be found by first calculating $E\left[y^2 \right]$:

$$E\left[y^2 \right] = \int_0^{\pi} y^2 \frac{1}{\pi} \frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)} dy. \tag{2.45}$$

Using Eq. (2.44) and Eq. (2.45), the variance of the decrypted image is:

$$\frac{1}{\pi^2}Var[y]=\frac{1}{\pi^2}\left\{E\left[y^2\right]-E^2[y]\right\}. \tag{2.46}$$

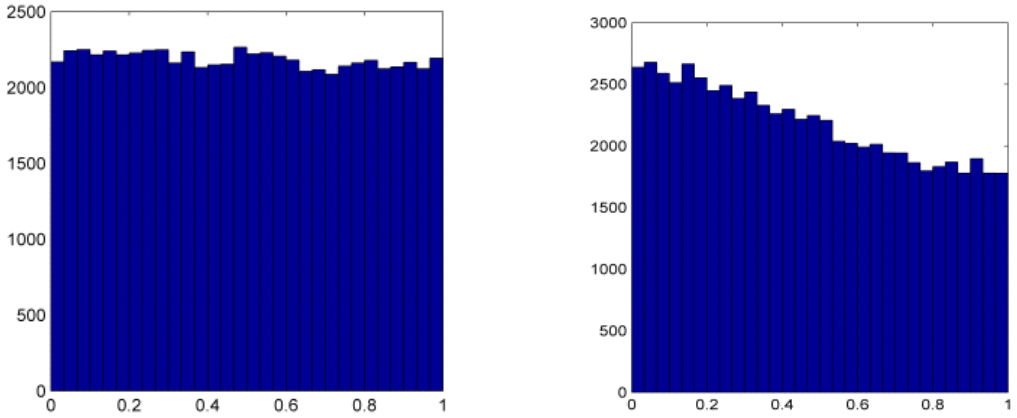
The derived mean and variance can be used in optimum correlation processors [25-31] to authenticate the decrypted image.

The K-S test [60] can then be repeated to show that the decrypted full phase PC-DRPE follows $\left|WC(0,\rho)\right|/\pi$ under the hypothesis test:

$$H_o: F_{full}(x)=F_{2,t}(x) \text{ vs. } H_a: F_{full}(x)\neq F_{2,t}(x), \tag{2.47}$$

where $F_{full}(x)$ is the ECDF of the decrypted image of the full- phased PC-DRPE and $F_{2,t}(x)$ is the ECDF of the simulated distribution $\left|WC(0,\rho)\right|/\pi$.

The K-S test was performed using the image shown in Fig. 2.2(b). Bootstrapping was used to estimate ρ; it was found that $\hat{\rho}$ =0.1030. Using the K-S test at $\alpha=0.05$, a p-value of 0.7398 was calculated indicating that we fail to reject H_o. Thus, we can conclude that for low N_p, the decrypted image comes from $\left|WC(0,\rho)\right|/\pi$. Fig. 2.6(b) shows a histogram of the image shown in Fig. 2.2b which is the decrypted image from the full phase PC-DRPE at N_p=1000.



(a) (b)

Fig. 2.6. An unwrapped circular histogram of the decrypted image from the full phase PC-DRPE using the image shown in Fig. 2.1(a) as the input at (a) $N_p = 10$ or 1.52e-4 photons/pixel which follows a uniform distribution $U(0,1)$ and (b) $N_p = 1000$ or 1.52e-2 photons/pixel (Fig. 2.2b) which follows the absolute value of the wrapped Cauchy distribution $\left|WC(0, 0.1030)\right|/\pi$.

4. CORRELATION PROCESSOR FOR IMAGE VERIFICATION

Although many pattern recognition processors can be used to authenticate the decrypted images [25-31], the optimum filter, which optimizes the peak-to-output energy (POE), will be used to authenticate the decrypted image with the input image [29]. The complex conjugate of the filter, presented in the frequency domain, i

$$H_{opt}^{*}(\upsilon) =$$

$$\frac{R(\upsilon) + m_b W_1(\upsilon) + m_r W_r(\upsilon)}{\left|R(\upsilon) + m_b W_1(\upsilon) + m_r W_r(\upsilon)\right|^2 + \frac{1}{2\pi} W_2(\upsilon) * N_b^0(\upsilon) + \frac{1}{2\pi}\left|W_r(\upsilon)\right|^2 * N_r^0(\upsilon) + m_b{}^2\left[W_2(\upsilon) - \left|W_1(\upsilon)\right|^2\right]},$$

(2.48)

where * denotes convolution, $R(\upsilon)$ denotes the Fourier Transform (FT) of the target located at position τ, m_b and m_r are the expected value of the background and target noise, respectively, $W_r(\upsilon)$ is the FT of the window function which is unity within the target and zero elsewhere, and $N_r^0(\upsilon)$ and $N_b^0(\upsilon)$ are the power spectrum of the zero mean target and background noise, respectively. Moreover, $W_1(\upsilon)$ and $W_2(\upsilon)$ are defined as:

$$W_1(\upsilon) = \left|W_0(\upsilon)\right|^2 / d - W_r(\upsilon), \tag{2.49}$$

$$W_2(\upsilon) = \left|W_0(\upsilon)\right|^2 + \left|W_r(\upsilon)\right|^2 - 2\left|W_0(\upsilon)\right|^2 real\left[W_r(\upsilon)\right] / d, \tag{2.50}$$

where $W_0(\upsilon)$ is the FT of the window function where it is unity within the input and zero outside the input, and d=$W_0(0) = \int w_0(t)\,dt$.

The Peak-to-Output energy (POE) [26,29] is computed and used to compare the outputs of the optimum filter for the full phase and amplitude-based PC-DRPE. This metric is defined, using 2D spatial coordinates (x, ς), as:

$$\mathrm{POE} = \left|E\left[a(0,0)\right]\right|^2 \left(E\left\{ \frac{1}{LH} \sum_{x=0}^{L-1} \sum_{\varsigma=0}^{H-1} \left|a(x,\varsigma)\right|^2 \right\} \right)^{-1}, \tag{2.51}$$

where $a(0,0)$ is the value of the output signal at the target location τ and L and H are the number of pixels in the x and ς directions, respectively.

5. RESULTS

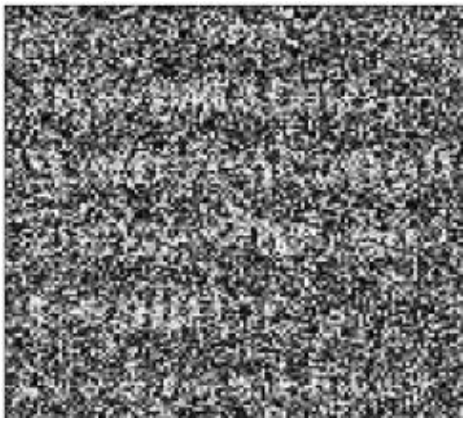
When comparing the output of the optimum filter for the full phase and amplitude-based PC-DRPE, both graphs were normalized to one and the average of 100 simulations was taken. Moreover, the logarithm of the POE is used in the POE graphs so that the POE values for a lower number of photons in the scene, N_p, [Eq. (2.3)] can easily be seen. Note that we assume the background and overlapping noise are equivalent

A 128 x 128 binary input, shown in Fig. 2.7(a), is used as the input. Figures 2.7(b) and 2.7(c) show the decrypted image for the amplitude-based and full phase PC-DRPE, respectively, at N_p=1000 or 0.061 photon/pixel. For both images, it is impossible to visually authenticate the decrypted images.

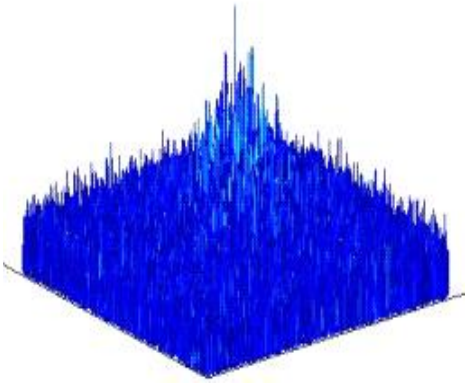
Figures 2.7(d) and 2.7(e) show the output of the optimum filter for the amplitude-based and full phase PC-DRPE, respectively, at N_p=1000. The mean and standard deviation of the amplitude-based PC-DRPE are 0.0849 and 0.0054, respectively, while the mean and standard deviation of the full phase PC-DRPE are 0.4343 and 0.2881, respectively**.** Note that there is no clear peak for the amplitude-based PC-DRPE while there is a distinct peak for the full phase PC-DRPE. Figure 2.8 shows a graph of the log of the POE versus the number of photons in the scene (N_p) . The graph shows that the full phase PC-DRPE has a higher POE than the amplitude-based PC-DRPE at lower N_p. At N_p=1000 and N_p =500, the full phase PC-DRPE has a log(POE) of 6.3214 and 5.4934, respectively, which corresponds to a POE of 556.3513 and 243.0823, respectively. Moreover, at N_p =1000 and N_p =500, the amplitude based PC-DRPE has a

(a)

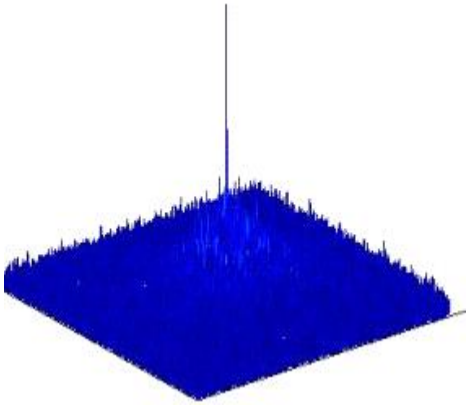
(b)



(c)



(d)



(e)

Fig. 2.7 (a) 128 x 128 pixel binary input image; photon-limited decrypted images with 1000 photons in the scene (N_p) or 0.061 photon/pixel for the (b) amplitude based DRPE, $f_{ph\,amp}(x)$ and the (c) full phase PC-DRPE, $f_{phfull}(x)$; output of optimum filter for the (d) amplitude based PC-DPRE and the (e) full phase PC-DRPE.

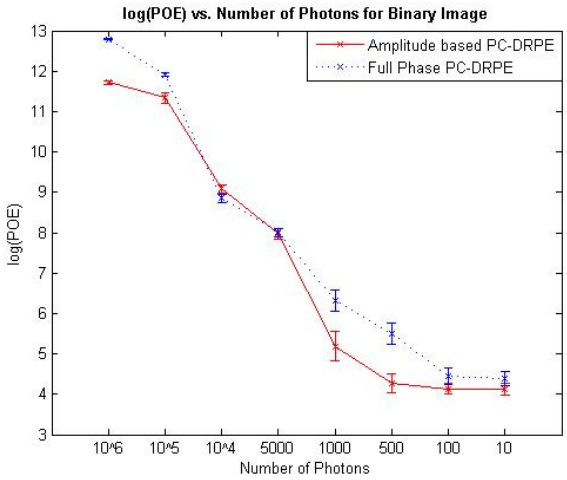
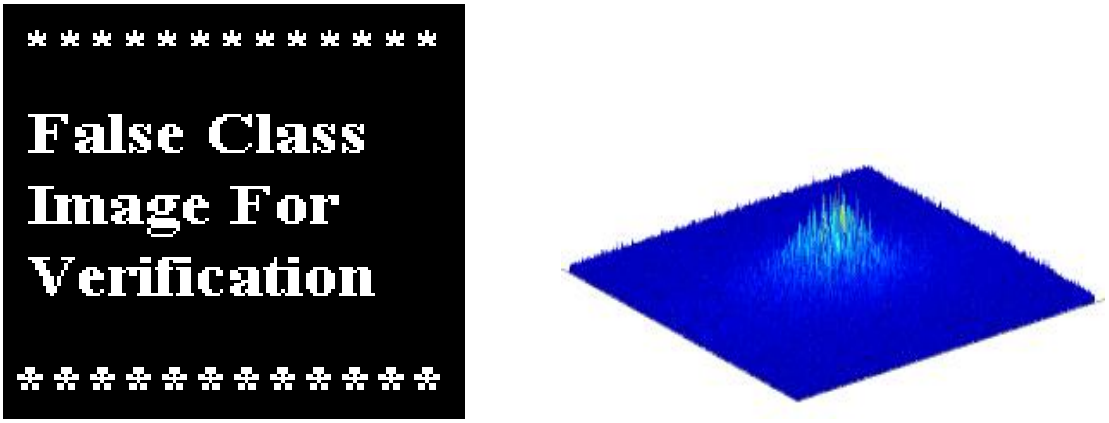


Fig. 2.8. Log of the Peak-to-Output Energy (POE) versus the number of photons in the scene (N_p) for the amplitude-based and full phase PC-DRPE for a binary image.

log(POE) of 5.1855 and 4.2643, respectively, which corresponds to a POE of 178.66 and 71.1151, respectively.

Figures 2.9(a) and 2.9(b) show the false class binary image, $g(x)$, and the output of the optimum filter using the false class image, respectively for the full phase PC-DRPE. The maximum peak of the output is 0.360 which indicates that the processor is able to distinguish between a true and false class image.



(a) (b)

Fig. 2. 9 (a) A 128 x 128 pixel false class binary image, $g(x)$; (b) optimum filter output for the full phase PC-DRPE with $g(x)$ at $N_p = 1000$ which has a maximum correlation peak value of 0.360.

4. CONCLUSION

In this paper, we have investigated a full phase photon-counting double-random-phase encryption (PC-DRPE) method. A photon-counting technique is used during the encryption process creating sparse photon limited images. The statistical distribution of the photon counting decrypted data for full phase encoding and amplitude phase encoding are derived and used for authentication of the data. The amplitude based PC-DRPE was shown to have a Gamma distribution whereas the full phase PC-DRPE was shown to have the absolute value of the wrapped Cauchy distribution. Simulations are performed for photon-limited encrypted and decrypted images for the full phase and amplitude based PC-DRPE. These decrypted images are verified using the optimum filter. Initial computational simulations showed that the full phase PC-DRPE encryption method may require fewer photons for authentication than the amplitude based PC-DRPE. Future work is needed to compare the performance of the full phase PC-DRPE to the amplitude based PC-DRPE for different images.

Chapter 3

Photon-counting Security Tagging and Verification Using Optically Encoded QR Codes *

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.

The chapter 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.

*A. Markman, B. Javidi, and M. Tehranipoor, "Photon-Counting Security Tagging and Verification Using Optically Encoded QR Codes," IEEE Journal of Photonics, doc. ID PJ-002016-2013 (posted 1 Dec 2013, in press).

3.1 INTRODUCTION

Information security with optical techniques has been widely [11], [14-17], [23],[30], [48], [53],[66-70]. Many variations of random phase encoding for security and encryption have been proposed [24],[27], [71-82]. Optical techniques in security provide many advantages including the ability to secure data with multi-dimensional keys such as wavelength [67], polarization [68], and placing the keys in the Fresnel domain [17]. Recently, photon-counting imaging has been integrated with the double-random-phase encryption for optical security [24]. 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 [80], and then apply an iterative compression technique based on Huffman coding [83] to compress the photon-counting encrypted image. The data can then be stored in an optically encoded QR code [39], [40] and placed on the object to be authenticated. Commercial QR scanners built into Smartphones such as an iPhone or Android device [42] 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 [25]-[31] 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.

3.2 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 [80]. 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

$$\psi(x) = \left\{\exp\left[i\pi f(x)\right] \times \exp\left[i2\pi n(x)\right]\right\} * h(x), \tag{3.1}$$

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

Photon-counting imaging [24], [32]-[35] is then applied to the amplitude of the encrypted image, $\left|\psi(x)\right|$, 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:

$$P(l_j;\lambda_j) = \frac{[\lambda_j]^{l_j} e^{-\lambda_j}}{l_j!}, \text{ for } \lambda_j > 0 \text{ , } l_j \in \{0,1,2,...\}, \tag{3.2}$$

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 $\left|\psi(x_j)\right| / \sum_{j=1}^{M} \left|\psi(x_j)\right|$, where $\left|\psi(x_j)\right|$ 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, $\exp\left[-i2\pi b(v)\right]$.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, $\exp\left[-i2\pi n(x)\right]$. The final decrypted image, $f_{ph}(x)$, which is real and positive , is then found as [16],[71]:

$$\left| f_{ph}(x) \right| = \left| Arg\left\{ A\exp\left[i\pi f_{ph}(x) \right] \right\} / \pi \right|, \tag{3.3}$$

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 [25]-[31]. To authenticate the decrypted image [Eq. (3.3)], a number of image recognition techniques can be used. We have selected the k^{th} order nonlinear processor [28] 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:

$$c(x) = IFT\left\{ \left| F_{f_{ph}}(\nu) F_f(\nu) \right|^k \exp\left[j\left(\phi_{f_{ph}}(\nu) - \phi_f(\nu) \right) \right] \right\}, \tag{3.4}$$

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

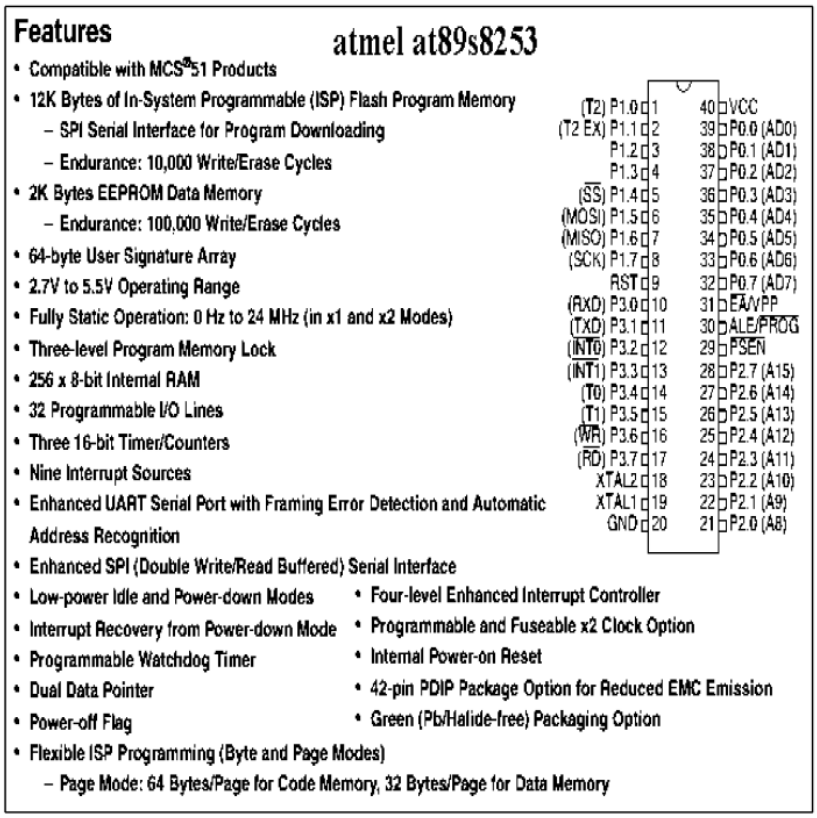
3.3 Embedding Encrypted Data into Optically Phase Encoded QR Code

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 E for more information about QR codes] due to data size restrictions and the limited resolution of commercial Smartphones when scanning the QR code [43]. 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 [73] on the photon-limited amplitude data, $\left|\psi_{ph}(x)\right|$, for low N_p [Eq. (3.2)] 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.

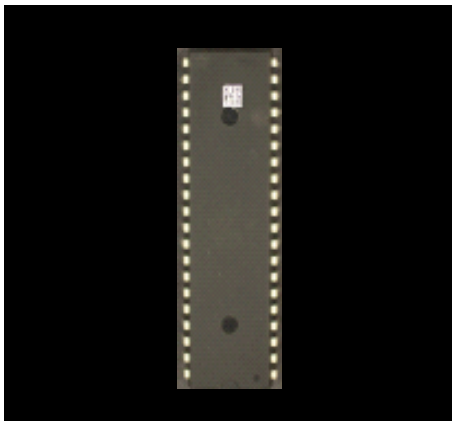
Once the QR code has been scanned, the data can be decompressed if both the dictionary and the length of the unpadded Huffman code, in bit form, associated with each Huffman iteration are known (allowing for the zero padding to be removed). Moreover, the data can then be successfully decrypted if the phase mask keys 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. 3.1(a) depicts a 449 x 641 pixel binary image and Fig. 3.1(b)



(a)

(b)

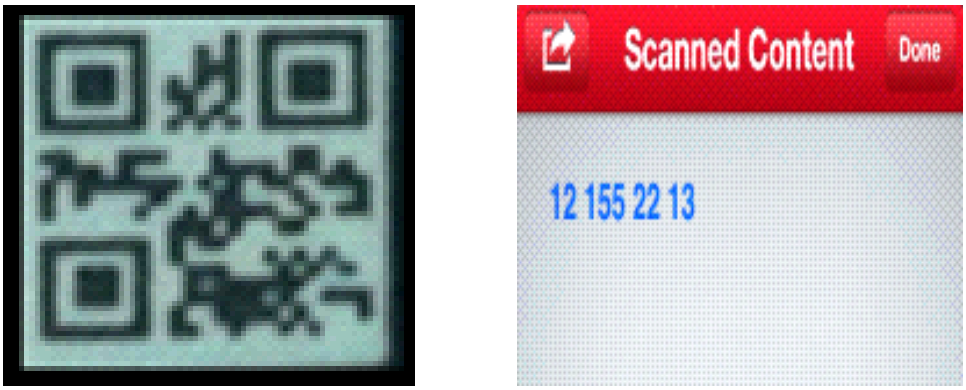


(c)

Fig. 3.1 (a) 449 x 641 pixel binary image. (b) 3.15 mm x 3.15 mm QR code storing the encrypted and compressed image shown in (a) placed on a 14.5 mm x 52.1 mm IC; an image of the QR code placed next to a dime is also depicted .

depicts a 3.15 mm x 3.15 mm QR code, generated using the ZXing Project [41], and placed on a 14.5 mm x 52.1 mm IC chip. The QR Code is also shown next to a dime in Fig 3.1(b). Figure 3.2(a) shows an enlarged QR Code obtained from the QR code shown in Fig. 3.1(b) using the iPhone 4 camera. Figure 3.2(b) depicts the scanned QR code which reveals the compressed and encrypted (for N_p= 500) data using the iPhone SCAN application.

Once the data has been scanned, it can be decompressed and decrypted. Figure 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. (3.4)] can be used to authenticate the primary image with the input image. Fig. 3.3(c) shows the output of the k^{th} 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. 3.3(b) shows a 449 x 641 pixel false class image, $g(x)$, that is used in the k^{th} order nonlinear filter to verify that it can distinguish between true and false class objects. Fig. 3.3(d) shows the output of the filter using $g(x)$ which has a maximum peak of 0.330.



(a) (b

Fig. 3.2 (a) enlarged QR code taken using the built-in IPhone 4 camera; (b) scanned QR Code depicting the encrypted and compressed data using the IPhone SCAN Application .

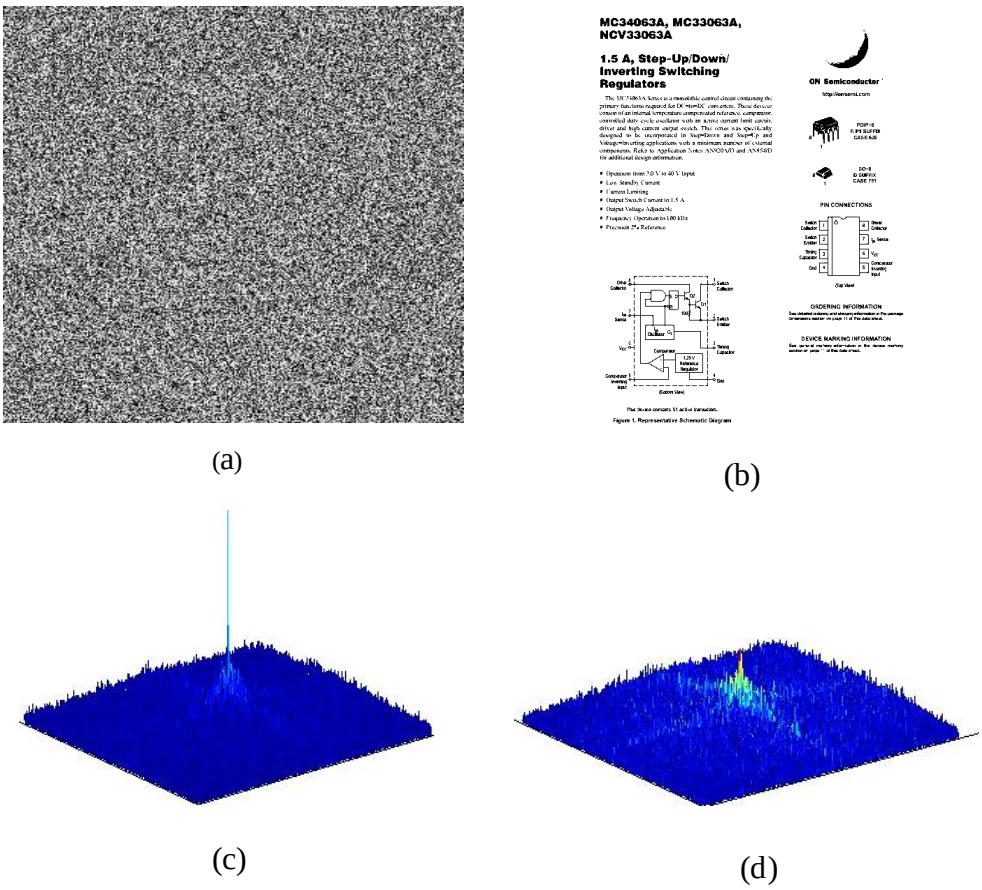


Fig.3.3 (a) Decrypted image obtained from the full phase PC-DRPE using the image shown in Fig. 3(a) as the input image (true class object); (b) 449 x 641 pixel false class image; (c) output of the k^{th} order nonlinear filter between the true class decrypted image and the true class object with k=0.3; (d) output of the k^{th} 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.

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. Figure 3.4(a) shows a QR code generated using the ZXing Project [41] 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 [76] can account for any minor physical anomalies in the QR code. Figure 3.4(b) shows the enlarged QR code shown in Fig. 3.4(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 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 Figure 3.5. 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. 3.6(a) shows an example of the speckle intensity pattern of the QR code without a phase mask illuminated by a HeNe laser. Fig. 3.6(b) depicts the speckle intensity pattern of the QR code shown in Fig. 3.4(a).

(a) (b)

Fig. 3.4 (a) QR code encoded with a random phase mask placed on an IC and (b) scanned QR code shown in (a).

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 [32,84,85]:

$$\Gamma\left(I; n_o, \frac{n_o}{\langle I\rangle}\right) = \left(\frac{n_o}{\langle I\rangle}\right)^{n_o} \frac{I^{n_o-1}\exp\left(-I\, n_o/\langle I\rangle\right)}{\Gamma\left(n_o\right)}, \tag{3.5}$$

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.

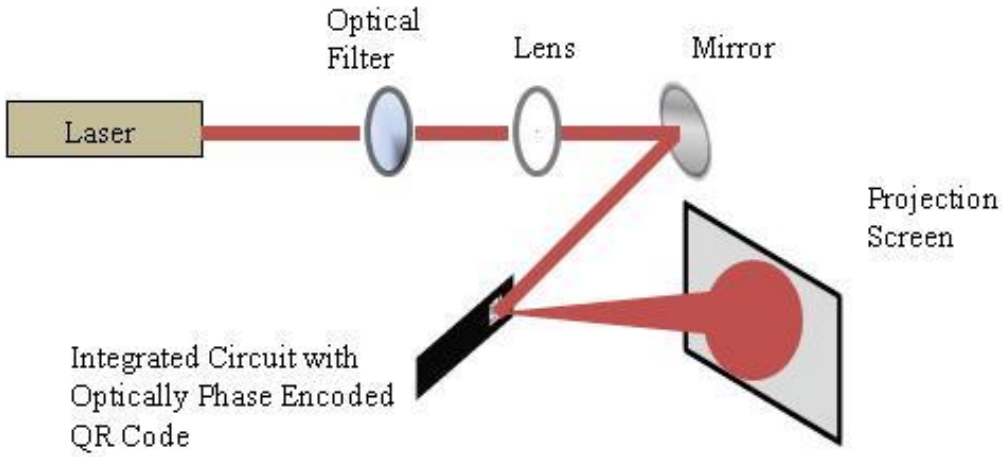


Fig. 3.5. Experimental set-up for verifying the phase encoded QR code speckle pattern.

The likelihood ratio test [86] 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. (3.5) is :

$$\log\left[l(\theta)\right] = N n_o \log\left(\frac{n_o}{\langle I\rangle}\right) + \left(n_o - 1\right)\sum_{j=1}^{N}\log\left(I_j\right) - N\log\left[\Gamma\left(n_o\right)\right] - \frac{n_o}{\langle I\rangle}\sum_{j=1}^{N} I_j, \tag{3.6}$$

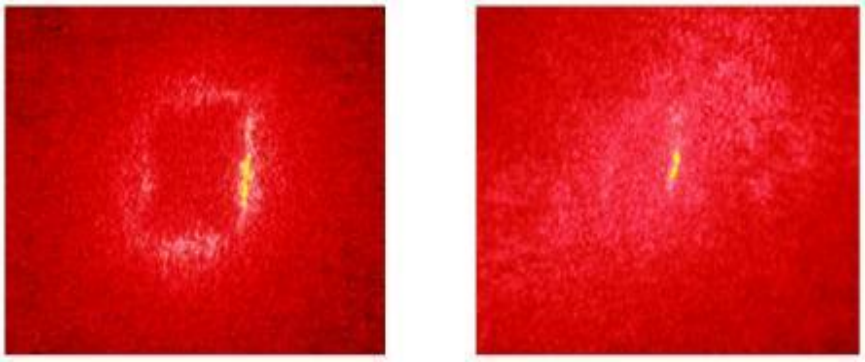
where θ represents the distribution parameters and N is the total number of I_j.

The log-likelihood ratio can be written as:

$$\log\left[l(\theta_o)\right] - \log\left[l(\theta_1)\right] \underset{H_1}{\overset{H_o}{\gtrless}} 0, \tag{3.7}$$

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

Using the likelihood ratio test [Eq. (3.7)], the true class parameters are obtained from Fig. 3.6(b) and calculated as $n_o / \langle I \rangle$ =18.08 and n_o = 3.43. Moreover, the false class parameters are obtained from Fig. 3.6(a) and calculated as $n_o / \langle I \rangle$ = 31.85 and n_o =7.47. Using a true class image, such as Fig. 3.6(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.



(a) (b)

Fig. 3.6 Speckle intensity patterns generated by a (a) QR code without a phase mask and (b) an optically encoded QR code with a phase mask.

3.4 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

APPENDIX A

To show that the decrypted image of the amplitude-based PC-DRPE [Eq. (2.16)], which is

$$\left| f_{ph_{amp}}(x) \right|^2 = \left[\Re\left\{ f_{ph_{amp}}(x) \right\} \right]^2 + \left[\Im\left\{ f_{ph_{amp}}(x) \right\} \right]^2, \tag{A1}$$

is the sum of two gamma distributions denoted by :

$$\begin{aligned} \left| f_{ph_{amp}}(x) \right|^2 &\sim \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{1,amp} \right) + \Gamma\left(\frac{1}{2}, 2\hat{\sigma}^2_{2,amp} \right), \\ &\sim \sum_{i=1}^{2} \Gamma_i \left(\frac{1}{2}, 2\hat{\sigma}^2_{\mathrm{i},amp} \right), \end{aligned} \tag{A2}$$

we note that $\Re\left\{ f_{ph_{amp}}(x) \right\}$ and $\Im\left\{ f_{ph_{amp}}(x) \right\}$ can be shown to be distributed as $N\left(0, \hat{\sigma}^2_{1,\mathrm{amp}}\right)$ and $N\left(0, \hat{\sigma}^2_{2,\mathrm{amp}}\right)$, respectively, where 0 is the mean and σ^2 (>0) is the variance [Eqs. (2.5-2.12)]. Equation (A1) shows the sum of the square of $\Re\left\{ f_{ph_{amp}}(x) \right\}$ and $\Im\left\{ f_{ph_{amp}}(x) \right\}$. We note that

$$\left[N\left(0, \sigma^2\right) \right]^2 = \left[\sigma N(0,1) \right]^2 = \sigma^2 \left[N(0,1) \right]^2. \tag{A3}$$

It is known that the square of a standard normal distribution, $[N(0,1)]^2$, is a chi-squared distribution with one degree of freedom , $\chi^2(1)$. The $\chi^2(1)$ distribution can be rewritten as a gamma distribution:

$$\chi^2(1) = \Gamma\left(\frac{1}{2}, 2 \right), \tag{A4}$$

where $\Gamma(1/2,2)$ is the gamma distribution with shape parameter $1/2$ and scale parameter 2. Multiplying both sides of Eq. (A4) by σ^2 yields:

$$\sigma^2\chi^2(1)=\Gamma\left(\frac{1}{2},2\sigma^2\right). \tag{A5}$$

Since $\Re\{f_{ph\,amp}(x)\}$ and $\Im\{f_{ph\,amp}(x)\}$ are both normally distributed with different variances, the distribution of the decrypted image becomes:

$$\begin{aligned}\left|f_{ph_{amp}}(x)\right|^2 &\sim \Gamma\left(\frac{1}{2},2\hat{\sigma}^2_{1,amp}\right)+\Gamma\left(\frac{1}{2},2\hat{\sigma}^2_{2,amp}\right),\\ &\sim \sum_{i=1}^{2}\Gamma_i\left(\frac{1}{2},2\hat{\sigma}^2_{\mathrm{i},amp}\right).\end{aligned} \tag{A6}$$

This is the sum of two gamma distributions.

APPENDIX B

We claim that the wrapped Cauchy distribution [Eq.(2.27)] can be rewritten as:

$$Z = Arg\left\{A\exp\left[j\pi f_{ph\,full}(x)\right]\right\} \sim \frac{1}{2\pi}\frac{1}{c\left(1-\gamma_1\cos z-\gamma_2\sin z\right)}, \tag{B1}$$

where

$$\gamma_1 = \frac{2\rho\cos\gamma}{1+\rho^2}, \qquad \gamma_2 = \frac{2\rho\sin\gamma}{1+\rho^2}, \tag{B2}$$

$$c = c\left(\gamma_1,\gamma_2\right) = \frac{1}{\sqrt{1-\gamma_1^2-\gamma_2^2}}, \tag{B3}$$

and ρ is the mean resultant vector and γ is the mean direction of the Wrapped Cauchy distribution [Eq. (2.29) and Eq. (2.30), respectively].

We can then substitute Eq. (B3) into Eq. (B1) to obtain

$$Z \sim \frac{1}{2\pi}\frac{\sqrt{1-\gamma_1^2-\gamma_2^2}}{\left(1-\gamma_1\cos z-\gamma_2\sin z\right)}. \tag{B4}$$

We then substitute Eq. (B2) into equation Eq. (B4) to yield:

$$\mathrm{Z} \sim \frac{1}{2\pi}\frac{\sqrt{1-\left(\frac{2\rho\cos\gamma}{1+\rho^2}\right)^2-\left(\frac{2\rho\sin\gamma}{1+\rho^2}\right)^2}}{\left(1-\frac{2\rho\cos\gamma\cos z}{1+\rho^2}-\frac{2\rho\sin\gamma\sin z}{1+\rho^2}\right)}. \tag{B5}$$

In the numerator of Eq. (B5) we can factor out $2\rho/(1+\rho^2)$ and get common denominators for the terms in the denominator:

$$Z \sim \frac{1}{2\pi} \frac{\sqrt{1-\left(\frac{2\rho}{1+\rho^2}\right)^2\left[(\cos\gamma)^2+(\sin\gamma)^2\right]}}{\left(\frac{1+\rho^2-2\rho\cos\gamma\cos z-2\rho\sin\gamma\sin z}{1+\rho^2}\right)}. \tag{B6}$$

We can then use the trigonometric identities $\cos^2(x)+\sin^2(x)=1$ and $\cos(x\pm\theta)=\cos(x)\cos(\theta) \mp \sin(x)\sin(\theta)$ to further simplify Eq. (B6) yielding

$$Z \sim \frac{1}{2\pi} \frac{\sqrt{1-\left(\frac{2\rho}{1+\rho^2}\right)^2}}{\left(\frac{1+\rho^2-2\rho\cos(z-\gamma)}{1+\rho^2}\right)}. \tag{B7}$$

We can rewrite the numerator of Eq. (B7) as

$$Z \sim \frac{1}{2\pi} \frac{\sqrt{\frac{\rho^4+1-2\rho^2}{(1+\rho^2)^2}}}{\left(\frac{1+\rho^2-2\rho\cos(z-\gamma)}{1+\rho^2}\right)}. \tag{B8}$$

After further simplification of the numerator of Eq. (B8), we obtain

$$Z \sim \frac{1}{2\pi} \frac{\sqrt{\frac{(\rho^2-1)^2}{(1+\rho^2)^2}}}{\left(\frac{1+\rho^2-2\rho\cos(z-\gamma)}{1+\rho^2}\right)}. \tag{B9}$$

We note that ρ^2 is less than 1, thus Eq. (B9) can be rewritten as

$$Z \sim \frac{1}{2\pi} \frac{1-\rho}{(1+\rho-2\rho\cos(z-\gamma))}. \tag{B10}$$

Eq. (B10) is the PDF of the wrapped Cauchy distribution [Eq. (2.27)].

APPENDIX C

To show that Eq. (2.32) and Eq. (2.34) are equivalent, we begin by defining the parameters

$$c = c(\gamma_1, \gamma_2) = \frac{1}{\sqrt{1-\gamma_1^2-\gamma_2^2}}, \tag{C1}$$

$$\eta_1 = c\gamma_1 \text{ and } \eta_2 = c\gamma_2, \tag{C2}$$

where γ_1 and γ_2 are defined in Eq. (B2).

By substituting Eq. (C2) into Eq. (C1), we obtain :

$$c = \frac{1}{\sqrt{1-\frac{\eta_1^2}{c^2}-\frac{\eta_2^2}{c^2}}} \ . \tag{C3}$$

We can then rewrite Eq. (C3) as

$$\sqrt{1-\frac{\eta_1^2}{c^2}-\frac{\eta_2^2}{c^2}} = \frac{1}{c} \ . \tag{C4}$$

Solving for c yields

$$c = \sqrt{1+\eta_1^2+\eta_2^2}. \tag{C5}$$

APPENDIX D

To derive the PDF of the absolute value of the zero mean Wrapped Cauchy distribution with mean resultant vector ρ, $|WC(0,\rho)|$ we let $Z = Arg\left\{A\exp\left[j\pi f_{ph\ full}(x)\right]\right\}$. If we define $y=|z|$, variable transformation [38] can be used to find the distribution of y:

$$h(y) \sim \frac{1}{2\pi}\frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)}|1| + \frac{1}{2\pi}\frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)}|-1|,$$

$$= \frac{1}{\pi}\frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)}, \quad 0 \le y \le \pi, \ 0 < \rho < 1, \tag{D1}$$

where $|\cdot|$ is the absolute value of the Jacobian of transformation, $\left|\frac{d}{dy}g^{-1}(y)\right|$, with $g^{-1}(y)$ being the inverse function of the transformation of z, $g(z)$.

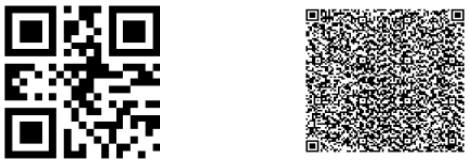
We also note that :

$$\int_0^{\pi}\frac{1}{\pi}\frac{1-\rho^2}{1+\rho^2-2\rho\cos(y)}dy = 1. \tag{D2}$$

Thus, Eq. (D1) is a valid PDF.

APPENDIX E

The QR code is a 2D barcode created by D. Wave [76],[77]. 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 [76]. The QR code itself is a binary image consisting of black squares known as modules placed on a white background, shown in Fig. E.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 [78] 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. E.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.



(a) (b)

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

REFERENCES

1. J.Solomon, “Undercover Feds Able to Easily Obtain Fraudulant Passpowers,” http://abcnews.go.com/Blotter/undercover-feds-easily-obtain-fraudulent-passports/story?id=11274031 (September, 2013)

2. U.S. Department of State “Passport and Visa Fraud: A Quick Course,” http://www.state.gov/m/ds/investigat/c10714.htm (September, 2013).

3. H. Welsbaum, “Bad guys are getting better at credit card fraud,” http://www.nbcnews.com/business/bad-guys-are-getting-better-credit-card-fraud-829477 (September, 2013).

4. Federal Trade Commission, *Consumer Sentinel Network Data Book for January-December 2012* (2012).

5. Fidelity, “Protecting your mobile and online banking,” https://www.fidelity.com/viewpoints/secure-online-banking (September, 2013).

6. Mastercard, “Protecting your card from fraud, http://www.mastercard.us/security.html (Seeptember, 2013)”.

7. B. javidi, “Securing Information with Optical Technologies,” Physics Today 50(3), 27-32 (2007).

8. R. Anderson, E. Biham, L. Knudsen, “Serpent: A proposal for the Advanced Encryption Standard,” NIST AES Proposal (1998).

9. R. Rivest, A. Shamir and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, 21 (2), pp. 120-126, February 1978

10. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. 1, 589-636 (2009).

11. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767-769 (1995).

12. T. Nomura and B. Javidi, “Optical encryption using a joint transform cor-relator architecture,” Opt. Eng.39, 2031–2035 (2000).

13. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595-6601 (2000).

14. 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. 30, 1644-1646 (2005).

15. Y. Frauel, A. Castro, T. Naughton, and B. Javidi, "Resistance of the double-random-phase encryption against various attacks," Opt. Express 15, 10253-10265 (2007).

16. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915-1927 (1999).

17. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," Opt. Lett. **24**, 762-764 (1999).

18. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595-6601 (2000).

19. T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, "Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator," Appl. Opt. **42**, 1508-1514 (2003).

20. O. Matoba and B. Javidi, "Encrypted Optical Storage with Angular Multiplexing," Appl. Opt. **38**, 7288-7293 (1999).

21. M. Toishi, M. Hara, K. Tanaka, T. Tanaka and K. Watanabe, "Novel Encryption Method Using Multi Reference Patterns in Coaxial Holographic Data Storage," Jpn. J. Appl. Phys. **46**, 3775 (2007).

22. E. Johnson and J. Brasher, "Phase encryption of biometrics in diffractive optical elements," Opt. Lett. **21**, 1271-1273 (1996).

23. 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. Express **14**, 1755-1766 (2006).

24. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22-24 (2011).

25. F. Dubois, "Automatic spatial frequency selection algorithm for pattern recognition by correlation," Appl. Opt. **32**, 4365-4371 (1993).

26. F. Sadjadi and B. Javidi, *Physics of Automatic Target Recognition* (Springer, 2007).

27. A.,Mahalanobis, R. Muise, "Object Specific Image Reconstruction using a Compressive Sensing Architecture for Application in Surveillance Systems," IEEE Transactions on Aerospace and Electronic Systems **45** , 1167-1180 (2009)

28. B. Javidi, "Nonlinear joint power spectrum based optical correlation," Appl. Opt. **28**, 2358-2367 (1989).

29. B. Javidi and J. Wang, "Design of filters to detect a noisy target in nonoverlapping background noise," J. Opt. Soc. Am. A **11**, 2604-2612 (1994).

30. B. Javidi and J.L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 1752-1756 (1994).

31. P. Réfrégier, V. Laude, and B. Javidi, "Basic properties of nonlinear global filtering techniques and optimal discriminant solutions," Appl. Opt. **34**, 3915-3923 (1995).

32. J. W. Goodman, *Statistical Optics* (Wiley, 2000).

33. B. Tavakoli, B. Javidi, and E. Watson, "Three dimensional visualization by photon-counting computational Integral Imaging," Opt. Express **16**, 4426-4436 (2008).

34. M. Guillaume, P. Melon, P. Réfrégier, and A. Llebaria, "Maximum-likelihood estimation of an astronomical image from a sequence at low photon levels," J. Opt. Soc. Am. A **15**, 2841-2848 (1998).

35. D. Aloni, A. Stern, and B. Javidi, "Three-dimensional photon-counting integral imaging reconstruction using penalized maximum likelihood expectation maximization," Opt. Express **19**, 19681-19687 (2011).

36. H-C. F, R. Sasaki, "Probability Distributions and Coherent States of B_r, C_r, and D_r Algebras," Yukawa Institute Kyoto (1997).

37. Myungjin Cho and Bahram Javidi, "Three-dimensional photon counting double-random-phase encryption," Journal of Optics Letters Journal, 38, 3198-3201 (19 August 2013).

38. W. Chen, X. Chen, A. Stern, and B Javidi, "Phase-Modulated Optical System with Sparse Representation for Information Encoding and Authentication," IEEE Journal of Photonics; Vol 5. No. 2. April, 2013

39. D. Wave, "Answer to your questions about the QR Code," http://www.qrcode.com/en/.

40. ISO, IEC 18004: 2006, "Information technology - Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification," *International Organization for Standardization*, Geneva, Switzerland (2006).

41. http://zxing.appspot.com/generator.

42. E. Ohbuchi, H. Hanaizumi, and L. A. Hock, “Barcode readers using the camera device in mobile phones,” in *Proceedings of IEEE 2004 International Conference on Cyberworlds*, M. Nakajima , ed. (IEEE, 2004), pp. 260 – 265.

43. “QR Code Minimum Size,” http://www.qrstuff.com.

44. http://usa.kaspersky.com/about-us/press-center/press-blog/malicious-qr-codes-attack-methods-techniques-infographic

45. J. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: Secure and noise-free information retrieval," Opt. Express **21**, 5373-5378 (2013).

46. O. Matoba, T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, “Optical techniques for information security,” Proc. IEEE **97,** 1128–1148 (2009).

47. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, "Known plaintext attack on double-random-phase encoding using fingerprint as key and a method for avoiding the attack," Opt. Express **18**, 13772-13781 (2010).

48. X. Tan, O. Matoba, Y. Okada-Shudo, M. Ide, T. Shimura, and K. Kuroda, "Secure Optical Memory System with Polarization Encryption," Appl. Opt. **40**, 2310-2315 (2001).

49. J.F. Barrera, R. Henao, M. Tebaldi, R.Torroba, and N. Bolognini, “Multiplexing encryption-decryption via lateral shifting of a random phase mask,” Opt. Commun. **259**, 532-536 (2006)

50. P. Clemente, V. Durán, V. Torres-Company, E. Tajahuerce, and J. Lancis, "Optical encryption based on computational ghost imaging," Opt. Lett. **35**, 2391-2393 (2010).
51. W. Chen and X. Chen, "Space-based optical image encryption," Opt. Express **18**, 27095-27104 (2010).

52. Y. Hayasaki, Y. Matsuba, A. Nagaoka, H. Yamamoto, and N. Nishida, "Hiding an Image with a Light-Scattering Medium and Use of a Contrast-Discrimination Method for Readout," Appl. Opt. **43**, 1552-1558 (2004).

53. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**, 887-889 (2000).

54. Y. Li, K. Kreske, and J. Rosen, "Security and Encryption Optical Systems Based on a Correlator with Significant Output Images," Appl. Opt. **39**, 5295-5301 (2000).

55. S. Fukushima, T. Kurokawa, and Y. Sakai, “Image encipherment based on optical parallel processing using spatial light modulator,” IEEE Trans. Photonics Technol. Lett. **3,** 1133-1135 (1991).

56. B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," Appl. Opt. **36**, 1054-1058 (1997).
57. J. Heanue, M. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. **34**, 6012-6015 (1995).

58. S. Shapiro and M. Wilk, "An analysis of variance test for normality (complete samples)," Biometrika **52**, 591-611 (1965).

59. N. Mukhopadhyay, *Probability and Statistical Inference* (Marcel Dekker, 2000).

60. F. Massey, Jr., "The Kolmogorov-Smirnov Test for Goodness of Fit," Journal of the American Statistical Association **46**, 68-78 (1951).

61. B. Efron, "Bootstrap Methods: Another Look at the Jackknife," The Annals of Statistics **7,** 1-26 (1979).

62. N.I. Fisher, *Statistical Analysis of Circular Data* (Cambridge University Press, 1996).

63. A. Vo and S. Oraintara, "On the distributions of the relative phase of complex wavelet coefficients," in *IEEE International Symposium on Circuits and Systems*, J. Wang, Y. Huang, Y. Lim, ed. (ISCAS,2009) pp. 529-532.

64. S. Jammalamadaka and A. SenGupta, *Topics in Circular Statistics* (World Scientific, 2001).

65. K. Mardia and P. Jupp, *Directional Statistics* (Academic Press Inc., 1972).

66. O. Matoba and B. Javidi, "Encrypted optical memory systems based on multidimensional keys for secure data storage and communications," IEEE Circ. Dev. Mag. **16**, 8–15 (2000).

67. O. Matoba and B. Javidi, "Encrypted optical storage with wavelength-key and random phase codes," Appl. Opt. **38**, 6785–6790 (1999).

68. B. Javidi and T. Nomura, "Polarization encoding for optical security systems," Opt. Eng. **39**, 2439–2443 (2000).

69. F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," J. Opt. Soc. Am. A **15**, 2629–2638 (1998).

70. J. F. Barrera, R. Henao, M. Tebaldi, R. Torroba, and N. Bolognini, "Multiplexing encrypted data by using polarized light," Opt. Commun. **260**, 109–112 (2006).

71. W. Chen, X. Chen, and C. J. R. Sheppard, "Optical image encryption based on diffractive imaging," Opt. Lett. **35**, 3817–3819 (2010).

72. T. J. Naughton, B. M. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A **25**, 2608–2617 (2008).

73. N. K. Nishchal and T. J. Naughton, “Flexible optical encryption with multiple users and multiple security levels,” Opt. Commun. **284**, 735–739 (2011).

74. Mehra, S. K. Rajput, and N. K. Nishchal, “Collision in Fresnel domain asymmetric cryptosystem using phase truncation and authentication verification,” Opt. Eng. **52**, 028202 (2013).

75. 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. **50**, 1805–1811 (2011).

76. E. Tajahuerce, J. Lancis, B. Javidi, and P. Andrés, “Optical security and encryption with totally incoherent light,” Opt. Lett. **26**, 678–680 (2001).

77. P. Kumar, A. Kumar, J. Joseph, and K. Singh, “Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions,” Opt. Lett. **34**, 331–333 (2009).

78. W. Chen, X. Chen, A. Anand, and B. Javidi, “Optical encryption using multiple intensity samplings in the axial domain,” J. Opt. Soc. Am. A **30**, 806–812 (2013).

79. 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. **14**, 094001 (2012).

80. A. Markman and B. Javidi submitted to JOSA A, September 2013.

81. R. K. Wang, I. A. Watson, and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng. **35**, 2464–2469 (1996).

82. W. Chen, X. Chen, A. Stern, and B. Javidi, “Phase-modulated optical system with sparse representation for information encoding and authentication,” IEEE Photon. J. **5**, 6900113 (2013).

83. D. Huffman, "A Method for the Construction of Minimum-Redundancy Codes," *Proc of IRE* (IEEE, 1952), pp. 1098-1101.

84. J.C. Dainty, *The Statistics of Speckle Patterns* (1976).

85. S. Yuan, Sensitivity, *Noise and Quantitative Model of Laser Speckle Contrast Imaging, UMI Dissertation Pub.* (2012).

86. R. J. Schalkoff, *Pattern Recognition: Statistical, Structural and Neural Approaches* (Wiley, 1991), 1st ed.