Statistical investigation of the double random phase encoding technique

David S. Monaghan,[1] Unnikrishnan Gopinathan,[1,2] Guohai Situ,[1,3] Thomas J. Naughton,[4,5] and John T. Sheridan[1,*]

[1]*UCD Communications and Optoelectronic Research Centre, SFI–Strategic Research Cluster in Solar Energy Conversion, and School of Electrical, Electronic and Mechanical Engineering, College of Engineering, Mathematics and Physical Sciences, University College Dublin, Belfield, Dublin 4, Ireland*
[2]*Instrument Research and Development Establishment, Raipur Road, Dehradun, India*
[3]*Institut für Technische Optik, Universität Stuttgart, Pfaffenwaldring 9, 70569 Stuttgart, Germany*
[4]*Department of Computer Science, National University of Ireland, Maynooth, Ireland*
[5]*University of Oulu, RFMedia Laboratory, Oulu Southern Institute, Vierimaantie 5, 84100 Ylivieska, Finland*
**Corresponding author: john.sheridan@ucd.ie*

Received February 27, 2009; revised July 3, 2009; accepted July 26, 2009; posted July 28, 2009 (Doc. ID 108113); published August 24, 2009

The amplitude-encoding case of the double random phase encoding technique is examined by defining a cost function as a metric to compare an attempted decryption against the corresponding original input image. For the case when a cipher–text pair has been obtained and the correct decryption key is unknown, an iterative attack technique can be employed to ascertain the key. During such an attack the noise in the output field for an attempted decryption can be used as a measure of a possible decryption key's correctness. For relatively small systems, i.e., systems involving fewer than 5×5 pixels, the output decryption of every possible key can be examined to evaluate the distribution of the keys in key space in relation to their relative performance when carrying out decryption. However, in order to do this for large systems, checking every single key is currently impractical. One metric used to quantify the correctness of a decryption key is the normalized root mean squared (NRMS) error. The NRMS is a measure of the cumulative intensity difference between the input and decrypted images. We identify a core term in the NRMS, which we refer to as the difference parameter, d. Expressions for the expected value (or mean) and variance of d are derived in terms of the mean and variance of the output field noise, which is shown to be circular Gaussian. These expressions assume a large sample set (number of pixels and keys). We show that as we increase the number of samples used, the decryption error obeys the statistically predicted characteristic values. Finally, we corroborate previously reported simulations in the literature by using the statistically derived expressions.

OCIS codes: 200.4740, 100.2000, 070.2580, 030.6600.

1. INTRODUCTION

Cryptography [1–4] has been recognized as important by governments and individuals throughout history. With recent technological advances in computer networking and global communication, information security has become ever more significant. Access to powerful desktop computers, which can be used to attack such systems, is therefore accompanied by a demand for higher security, and this leads to increasingly powerful encryption techniques being developed.

Information security based on optical encryption [5–13] is of particular interest, as it offers the possibility of high-speed parallel encryption of 2D image data. One such method of optical encryption is known as the double random phase encryption (DRPE) technique [5]. DRPE involves the use of two 2D random phase keys, one placed in the input image domain and one placed in the Fourier domain of an optical $2f$ imaging system. If the two phase keys are generated by using statistically independent white noises, then the encrypted image is also stationary white noise. Since its introduction in 1995, the DRPE has generated much interest and has been the focus of many studies [14–21]. The physical implementation of such an optical system gives rise to many practical issues; however, a thorough analysis of the DRPE technique itself is extremely important if it is to be utilized.

Depending on the form of the input data to be encrypted, two modes of operation of the DRPE technique can be identified:

1. Amplitude encoding (AE), with a grayscale input image, and
2. Phase encoding (PE), where the input phase is modulated.

While the optical systems used to encrypt the data in both cases are very similar, there are significant differences in the decryption, analysis, and breaking of these encoding systems.

In the case when a PE input image (phase data) is used, both the image and the Fourier plane encryption keys, $R_{1,e}=\exp[+j2\pi\, a(x,y)]$ and $R_{2,e}=\exp[+j2\pi\, b(u,v)]$, are needed during the decryption process [21], where x and y denote spatial coordinates, u and v denote coordinates in the frequency domain, and a and b are the input and the Fourier plane phase key values, respectively. For the AE case discussed here, it is only necessary to know the Fourier plane key, $R_{2,e}$, for decryption [22].

In the analysis presented below it is always assumed

that the phase key will be the same size (have the same number of pixels) as the input image. It is possible, when using a DRPE system, to get partial (imperfect) decryptions using keys unrelated to the correct key. In order to have a complete overview of the decryption capabilities of all the keys in key space [22] one should evaluate the output decryption produced by every possible key. For relatively small systems, i.e., systems with an input image of up to 5×5 pixels, this can easily be done; however, for larger systems examining the key space is numerically impractical.

An encryption algorithm's key space is the set of all possible keys that can be used to encode data by using that algorithm. For instance, a simple combination lock with three dials, each with ten digits, has a key space of 1000 keys, i.e., 10^3. The number of possible combinations grows exponentially with the number of dials (equivalent to the number of pixels in our study). The size of the key space determines the number of possible unique keys that can be used by the DRPE algorithm. The number of keys in the key space is given by the number of quantization levels used in the key, raised to the power of the number of pixels in the key. Thus, for example, a system with $N=5\times5$ pixels and 2 quantization levels has 2^{25} keys, or 33,554,432 keys in its key space. Recently reported simulations for such a system have shown [23] that there is minimal security improvement if keys with more than 16 quantization levels are employed. However, for larger systems, i.e., 256×256 pixels with 16 quantization levels (having $16^{65,536}$ keys in the key space), checking every single key is currently not practical. Like most encryption techniques DRPE relies heavily on the large size of its key space to provide security from brute-force attacks, i.e., that the probability of randomly guessing a correct key is statistically insignificant.

The way in which the wrongness of the decryption key is quantified is of great significance in estimating both the robustness to noise and the security of the system. Typically, in the DRPE literature, the deviation of the decrypted image from the input image is quantified by using the normalized root mean squared (NRMS) error. It is popular since, given a cipher–text pair, the success of attempts at decryption can be quantified naturally by using the intensity-error-based NRMS. Heuristic attempts to break the DRPE have been implemented in which the NRMS error is used as the Cost Function (CF) in an iterative search procedure [19]. Thus the NRMS value assigns a quantitative level of validity, or correctness, to each possible decryption key in the key space.

The presence of an incorrect Fourier key will introduce errors in both the amplitude and the phase of the output field. In this paper we begin by verifying that this complex noise is circular Gaussian. Given the statistical properties of this noise we then derive analytic expressions for the mean and variance of the sum of the square of the difference between the intensity values of the pixels in the original input image and the decrypted image. This is the difference parameter d, which we explicitly define in Section 3.

Should the attacker have access to a cipher–text pair, it has already been shown that in the case of AE, heuristic methods [19] can be used to extract the DRPE Fourier key, $R_{2,e}$, with an NMRS error less than 10%, within a reasonable amount of time, i.e., within less than an hour, by using a standard PC (Intel P4 2.5 GHz). Extensions of this method can also be used if several cipher–text pairs are available when the system is attacked, and such techniques can be very effective [24,25].

We wish to study the errors in the output (decrypted) image intensity for a sample set of keys in a large system (256×256 pixels). In previous work [22] we examined the DRPE technique's key space, using histograms showing the number of keys that decrypt an encoded message to particular NRMS values. As noted, this analysis was performed only for small input image sizes, i.e., $<5\times5$ pixels. By deriving statistical expressions for the mean and the variance of the intensity difference parameter d, which is closely related to the NRMS, we aim to facilitate study and analysis of the key space for larger input images.

In [22] (see Fig. 7 in Ref. [22]), we presented the results of a simulation where one million random phase keys were used in an attempt to decrypt a large system (256×256 pixels with 8 phase quantization levels) via a brute-force method. In [22] it is shown that for such a large key space the mean value of the NRMS is ~1 and that the variance of the NRMS, which is related to the distribution of the keys in key space, decreases significantly from that observed for smaller key spaces. However, these results were based on examining the results from a very small number of possible keys from the total key space. To verify this result a statistical analysis must be used. In this paper it is shown that as the number of samples is increased (i.e., the number of pixels in a phase key or image increases, and/or the number of simulation runs for a large number of possible decryption keys increases), the NRMS values tend toward the statistically predicted limiting results. In this way we verify the validity of the statistical results derived and presented here and also confirm the observations made in [22] regarding the differences between the results for large and small systems.

At the heart of this paper are d and the NRMS, which we use as metrics to quantify key error. One other possible metric might be the Euclidean distance in key space between an incorrect decryption key and the correct key. However, such a distance is not a good measure of the correctness of the key, as it does not predict the resulting NMRS error in the decrypted image. To prove this we note that in a previous paper [22] we showed that, for AE DRPE, the key space for a system with 256 quantization levels will have 256 valid keys that decrypt the system with zero NRMS error. All but one of these keys are large Euclidean distances from the encryption key, $R_{2,e}$. Therefore, given the typical assumption that a potential attacker may have access to a cipher–text pair but definitely does not have access to the correct decryption key, the NRMS clearly has a practical role in providing an indirect measure of a possible decryption key's accuracy.

This paper is organized as follows: In Section 2 some statistical results, regarding the properties of circular Gaussian noise, are provided. In Section 3 the NRMS CF and the difference parameter d, for use in relation to the DRPE technique are presented. A significant conjecture is

also made in this section regarding the mathematical description of such a field. In Section 4, assuming power conservation, we derive analytic expressions for the mean and variance of d in terms of the circular Gaussian noise in the decrypted output field. In Section 5 we provide the results of some numerical simulations which, for a large number of samples, confirm both the circular Gaussian nature of the output field noise and support the validity of the conjecture made in Section 3, (when errors are randomly introduced in the Fourier plane key). In this section we also show that when the errors in $R_{2,d}$ are randomly distributed spatially there is a highly correlated linear relationship between the number of pixels in error in $R_{2,d}$ and the expected value of the parameter λ, $E_{\%R}[\lambda]$, (used in our conjecture, in Section 3), calculated for a subset of keys from the key-space in which the percentage of pixels in error are the same. In Section 6 we make some comparisons with previous results in the literature [22], and in Section 7 we present our overall conclusions.

2. STATISTICS: DEFINITIONS AND NOTATION

Some statistical definitions and mathematical results used throughout this paper are presented.

A. Mean and Variance

Let us assume the existence of a real valued continuous function, $f(x)$, which has been sampled discretely K times, $0<k<K+1$. Denoting this sampled function as $f(k)$, if it is real, then $f(k)=f^*(k)$, where * denotes complex conjugation. For a real valued random variable, the mean can be defined as the expectation of that random variable. For a large number of samples, the population mean, or expected value of the data set f, is given by

$$E[f] = \mu = \frac{1}{K}\sum_{k=1}^{k=K} f(k). \tag{1}$$

The variance of the data set f is a measure of the statistical dispersion of data about the mean and is calculated by averaging the squared distances of the possible values from the expected value, i.e., it is the square of the standard deviation, and for $K \gg 1$ it is given by

$$V[f] = \sigma^2 = \frac{1}{K}\sum_{k=1}^{k=K} \{f(k) - E[f]\}^2. \tag{2}$$

The variance of f can also be written as

$$V[f] = E[f^2] - E[f]^2. \tag{3}$$

B. Properties of Gaussian Noise

Let us assume we have a set, g, of samples, $g(k)$, whose statistical properties are well described by a normalized Gaussian probability distribution function (PDF) of mean $E[g]=\mu$, and variance $V[g]=\sigma^2$. The PDF of g is of the form

$$N(\mu,\sigma;x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[\frac{(x-\mu)^2}{2\sigma^2}\right], \tag{4}$$

where x represents a particular value taken by $g(k)$ when K is very large, and the probability distribution function indicates the probability (frequency) of such a value occurring.

Gaussian distributions obey the Gaussian moment theorem. If we define the nth moment of the Gaussian random variable x about the value z as

$$M_{n,z} = \int_{-\infty}^{+\infty} (x-z)^n N(\mu,\sigma;x)\mathrm{d}x, \tag{5}$$

then $E[x]=M_{1,0}$, and $V[x]=M_{2,\mu}$.

The assumption of the presence of Gaussian noise has important ramifications:

1. First, and equivalent to Eq. (3), we note that the mean of the data values squared is equal to the sum of the square of their mean and their variance:

$$E[g^2] = \mu^2 + \sigma^2. \tag{6}$$

2. Second, and of particular significance to our analysis, when the noise is complex valued it is referred to as circular Gaussian noise. In this case we define a complex noise function, n, and a sampled version, $n(k)=n_r(k)+jn_i(k)$. Both n_r and n_i are assumed to be two uncorrelated white noises with zero means, $\mu_r=\mu_i=0$, and identical standard variations, $\sigma_r=\sigma_i=\sigma$, where r denotes the real, and i denotes the imaginary parts.

We can summarize the statistical properties of such noise as follows:

$$E[n] = E[n_{r,i}] = 0, \tag{7}$$

$$V[n_{r,i}] = \sigma^2 = E[n_{r,i}^2]. \tag{8}$$

The positive real valued intensity (magnitude squared) of the noise is defined as

$$nn^* = n^*n = |n|^2 = |n_r|^2 + |n_i|^2; \tag{9}$$

therefore

$$E[|n|^2] = E[|n_r|^2 + |n_i|^2] = E[|n_r|^2] + E[|n_i|^2] = 2\sigma^2. \tag{10}$$

Some further properties are discussed in Section 3. First we define and examine the NRMS.

3. NORMALIZED ROOT MEAN SQUARED ERROR

We first recall that all incorrect phase keys are in the system key space and can be used as possible decryption keys. We wish to compare an image (data array) and a perturbed or noisy version of that image. In this paper these noisy output images arise because an incorrect Fourier decryption key, $R_{2,d}=\exp[-j2\pi b'(u,v)]$, is used following perfect encryption. For perfect decryption $b=b'$, implying that $R_{2,d}=R_{2,e}^*$. Such a comparison corresponds to one step (iteration) of a process by which an attacker attempts to acquire the correct decryption key. In this case the attacker knows *a priori* the number of pixels and

quantization levels, but applying an incorrect phase key, from within the key space, achieves only partial or incomplete decryption. In our case the output data sets correspond to intensities (images) captured by a CCD. More specifically, the two 2D data sets, that we compare (i.e., use to generate the NRMS CF) correspond to the intensities (images) input to the encryption system and the resulting decrypted image at the output of the decryption system. We denote the original image by I and the decrypted image by I_d, where I_d can be a correctly or incorrectly decrypted image. It should be noted, for clarity, that if the correct $R_{2,d}$ is used then the NRMS error value should be 0; however, for an $R_{2,d}$ containing randomly chosen pixel values, i.e., typically an incorrect key from the key space of the system, the NRMS error value has been numerically observed to be on average ~1 [22].

We note that the effects on the output of perturbations away from the exact encryption key can be analogous to the effects of noise accumulated in the system during any experimental implementation. Analyzing such effects therefore also provides insights into the robustness against noise of the DRPE technique.

As stated, the metric employed to quantify the quality of the decryption is the NRMS:

$$\sqrt{\frac{\sum_{p=1}^{p=N}|I(p)-I_d(p)|^2}{\sum_{p=1}^{p=N}|I(p)|^2}}, \tag{11}$$

where N is the number of pixels in the image. Central to this metric is the difference term

$$d=\sum_{p=1}^{p=N}|I(p)-I_d(p)|^2. \tag{12}$$

This difference term is used to form the basis of the following analysis of the effects of the noise in I_d on the performance of the DRPE technique for the AE case.

The decrypted complex field data is given by

$$A_d=\mathfrak{I}^{-1}(\mathfrak{I}^{-1}\{\mathfrak{I}[\mathfrak{I}(f\times R_{1,e})]\})\otimes\mathfrak{I}^{-1}\{\mathfrak{I}^{-1}[\mathfrak{I}(R_{2,e})]\}\otimes\mathfrak{I}^{-1}(R_{2,d}) \tag{13}$$

$$=[f\times R_{1,e}]\otimes[\mathfrak{I}(R_{2,d})\oplus\mathfrak{I}(R_{2,e})], \tag{14}$$

where $\otimes$ and $\oplus$ denote the convolution and correlation operations.

Following [15] we now make a conjecture regarding the form of the output decrypted complex field. We propose that the amplitude of an attempted decryption can be written as

$$A_d(\cdot)\cong\lambda f(\cdot)+n(\cdot), \tag{15}$$

where λ is a different constant for each decryption key examined, f is the input signal (image), and n represents circular white Gaussian noise with zero mean; see Section 2. In [21] it was reported that an incorrect $R_{2,d}$ key resulted in such Gaussian noise n being observed in the output image. The parameter λ plays a significant role in our later analysis; see Section 5.

In the case of AE the input intensity is given by $I=|f|^2=f^2$. Applying our conjecture, Eq. (15), the corresponding output decrypted image intensity is given by

$$I_d=|\lambda f+n|^2=\lambda^2f^2+\lambda f[2n_r]+|n|^2. \tag{16}$$

Since our encryption system is lossless, power will be conserved and the total input intensity must be equal to the total output intensity. The implications of this requirement are examined later in Subsection 4.B; however, we first return to our definition of d, given in Eq. (12). For each particular case, i.e., an input image and decryption key, we substitute from Eq. (16) and then rewrite Eq. (12) in terms of the individual image pixel values ($1\leqslant p\leqslant N$), giving

$$d=\sum_{p=1}^{p=N}|(\lambda^2-1)f^2(p)+2\lambda f(p)n_r(p)+|n(p)|^2|^2. \tag{17}$$

Expanding Eq. (17) this gives

$$\begin{aligned}d=&(\lambda^2-1)^2\sum_{p=1}^{p=N}\{f^4(p)\}+4\lambda(\lambda^2-1)\sum_{p=1}^{p=N}\{f^3(p)n_r(p)\}\\&+2(\lambda^2-1)\sum_{p=1}^{p=N}\{f^2(p)|n(p)|^2\}+4\lambda^2\sum_{p=1}^{p=N}\{f^2(p)n_r^2(p)\}\\&+4\lambda\sum_{p=1}^{p=N}\{f(p)n_r(p)|n(p)|^2\}+\sum_{p=1}^{p=N}\{|n(p)|^4\}.\end{aligned} \tag{18}$$

The mean and variance of d are now discussed.

4. STATISTICS OF THE DIFFERENCE TERM

A. Expected Value of *d*

All of the sums over the number of pixels N in Eq. (18) are replaced by the corresponding average values multiplied by N:

$$\begin{aligned}d=&(\lambda^2-1)^2E[f^4(p)]N+4\lambda(\lambda^2-1)E[f^3(p)n_r(p)]N\\&+2(\lambda^2-1)E[f^2(p)|n(p)|^2]N+4\lambda^2E[f^2(p)n_r^2(p)]N\\&+4\lambda E[f(p)n_r(p)|n(p)|^2]N+E[|n(p)|^4]N.\end{aligned} \tag{19}$$

If in Eq. (19) the expected values are calculated over the large number of pixels, and based on the assumption that f and n are statistically independent, we can assume [26] that

$$E[f^kn_r^l]\approx E[f^k]\times E[n_r^l], \tag{20}$$

$$E[f^k|n|^{2l}]\approx E[f^k]\times E[|n|^{2l}]. \tag{21}$$

We note that while we use these expressions at this point in our calculation, later we will proceed to calculate expected values, i.e., sums, over all R possible keys in key space, and this should further improve the validity of Eq. (20) and (21).

Using Eq. (20) and (21) we can rewrite Eq. (19) as

$$\begin{aligned}d/N=&(\lambda^2-1)^2E[f^4(p)]+4\lambda(\lambda^2-1)E[f^3(p)]E[n_r(p)]\\&+2(\lambda^2-1)E[f^2(p)]E[|n(p)|^2]+4\lambda^2E[f^2(p)]E[n_r^2(p)]\\&+4\lambda E[f(p)]E[n_r(p)|n(p)|^2]+E[|n(p)|^4].\end{aligned} \tag{22}$$

Note that we now express d per pixel. From Eq. (1),

$$f_m = E[f^m(p)] \approx \frac{1}{N}\sum_{p=1}^{p=N} f^m(p), \tag{23}$$

$$(n_p)^m = E[n^m(p)] \approx \frac{1}{N}\sum_{p=1}^{p=N} n^m(p), \tag{24}$$

$$|n_p|^m = E[|n(p)|^m] \approx \frac{1}{N}\sum_{p=1}^{p=N} |n(p)|^m. \tag{25}$$

Equations (23)–(25) simplify Eq. (22) to

$$d' = d/N = (\lambda^2-1)^2 f_4 + 4\lambda(\lambda^2-1)f_3 n_{r,p} + 2(\lambda^2-1)f_2|n_p|^2 + 4\lambda^2 f_2 n_{r,p}^2 + 4\lambda f_1 n_{r,p}|n_p|^2 + |n_p|^4. \tag{26}$$

The expected value of $d' = d/N$ is now calculated over a large number of runs, i.e., over all R possible decryption phase keys in key space. During each run it is assumed that the same input image is used; however, as the decryption keys change, the λ value will also change:

$$\underset{R}{E}[d'] = \underset{R}{E}[(\lambda^2-1)^2]f_4 + 4f_3\underset{R}{E}[\lambda(\lambda^2-1)n_{r,p}] + 2f_2\underset{R}{E}[(\lambda^2-1)\times|n_p|^2] + 4f_2\underset{R}{E}[\lambda^2 n_{r,p}^2] + 4f_1\underset{R}{E}[\lambda n_{r,p}|n_p|^2] + \underset{R}{E}[|n_p|^4]. \tag{27}$$

Expanding Eq. (27) gives that

$$\underset{R}{E}[d'] = f_4(\underset{R}{E}[\lambda^4] - 2\underset{R}{E}[\lambda^2] + 1) + 4f_3\underset{R}{E}[\lambda](\underset{R}{E}[\lambda^2]-1)\underset{R}{E}[n_{r,p}] + 2f_2(\underset{R}{E}[\lambda^2]-1)\underset{R}{E}[|n_p|^2] + 4f_2\underset{R}{E}[\lambda^2]\underset{R}{E}[n_{r,p}^2] + 4f_1\underset{R}{E}[\lambda]\underset{R}{E}[n_{r,p}]\underset{R}{E}[|n_p|^2] + \underset{R}{E}[|n_p|^4]. \tag{28}$$

Recalling that the noise is assumed to be circular Gaussian, we apply the Gaussian moment theorem, using Eq. (2.8.22) in [26], to obtain

$$E[|n|^4] = 2E[|n|^2]^2, \tag{29}$$

$$E[|n|^2 n] = 0, \qquad E[n^2] \neq 0. \tag{30}$$

Recall that averaging has already taken place over N. Substituting into Eq. (28), using Eqs. (20), (21), (23)–(25), (29), and (30), and assuming that R is very large (all possible keys in key space), we can write that

$$\underset{R}{E}[d'] = \left(\lim_{R\to\infty}\frac{1}{R}\sum_{\tilde{r}=1}^{R}\{\lambda^4(\tilde{r})\} - 2\lim_{R\to\infty}\frac{1}{R}\sum_{\tilde{r}=1}^{R}\{\lambda^2(\tilde{r})\} + 1\right)f_4 + 2f_2\left(\lim_{R\to\infty}\frac{1}{R}\sum_{\tilde{r}=1}^{R}\{\lambda^2(\tilde{r})\} - 1\right)2\sigma^2 + 4f_2\lim_{R\to\infty}\frac{1}{R}\sum_{\tilde{r}=1}^{R}\{\lambda^2(\tilde{r})\}\sigma^2 + 8\sigma^4. \tag{31}$$

B. Power Conservation

In order that power be conserved, and recalling Eq. (15), we note that

$$\frac{1}{N}\sum_{p=1}^{N}|\lambda f + n|^2 = \frac{1}{N}\sum_{p=1}^{N}|f|^2. \tag{32}$$

Calculating the expected value over R of Eq. (32) gives us an expression for σ^2. Simplifying Eq. (32) and using Eq. (10), We can derive Eq. (8) (see Appendix 10.1 of [27]):

$$\sigma^2 = \left[\lim_{R\to\infty}\frac{1}{R}\sum_{\tilde{r}=1}^{R}(1-\lambda(\tilde{r})^2)\right]\frac{f_2}{2}. \tag{33}$$

It is observed from numerical simulations (see Subsection 5.B) that the expected values of λ and λ^2 (over all R keys in key space) are very small, $\underset{R}{E}[\lambda] \approx \underset{R}{E}[\lambda^2] \approx 0$, and all the other terms in Eq. (31) are large in comparison. Thus, substituting Eq. (33) back into Eq. (31) and applying the limit as R tends to infinity, it can be shown that

$$\underset{R}{E}[d'] = \{1 - \underset{R}{E}[\lambda(\tilde{r})^2]\}\{-2f_2^2\underset{R}{E}[\lambda(\tilde{r})^2] + f_4(1 - \underset{R}{E}[\lambda(\tilde{r})^2])\} \approx f_4, \tag{34}$$

where f_2 and f_4 are as defined in Eq. (23). The assumptions made regarding $\underset{R}{E}[\lambda]$ and $\underset{R}{E}[\lambda^2]$ are discussed later in Subsection 5.B.

C. Variance of d'

We now wish to find $\underset{R}{V}[d']$, therefore we must calculate $\underset{R}{E}[d'^2]$. Equation (35), derived by using Eq. (5), is employed to derive the higher-order expected values of the noise terms:

$$E[n_{r,i}^q] = \frac{\sigma^q}{\sqrt{\pi}}2^{(q/2-1)}[1+(-1)^q]\Gamma\left(\frac{1+q}{2}\right). \tag{35}$$

Using this, it can be shown that

$$\underset{R}{E}[d'^2] = -4f_2^2 f_4\underset{R}{E}[\lambda^2](-1+\underset{R}{E}[\lambda^2])^3 + f_4^2(-1+\underset{R}{E}[\lambda^2])^4 + 4f_2^4\underset{R}{E}[\lambda^2](4-5\underset{R}{E}[\lambda^2]+2\underset{R}{E}[\lambda^4]). \tag{36}$$

Applying this result, and using Eqs. (3), (34), and (36), the variance of d' is given by

$$\underset{R}{V}[d'] = [-4f_2^2 f_4\underset{R}{E}[\lambda^2](-1+\underset{R}{E}[\lambda^2])^3 + f_4^2(-1+\underset{R}{E}[\lambda^2])^4 + 4f_2^4\underset{R}{E}[\lambda^2](4-5\underset{R}{E}[\lambda^2]+2\underset{R}{E}[\lambda^4])] - [\{1-\underset{R}{E}[\lambda(\tilde{r})^2]\}\times\{-2f_2^2\underset{R}{E}[\lambda(\tilde{r})^2] + f_4(1-\underset{R}{E}[\lambda(\tilde{r})^2])\}]^2 \approx f_4^2 - f_4^2 \approx 0. \tag{37}$$

In summary, $\underset{R}{E}[d/N] = (1/N)\Sigma_1^N I^2(p)$, and $\underset{R}{V}[d/N] = 0$.

5. NUMERICALLY TEST THE VALIDITY OF THE CONJECTURE, EQ. (15): GAUSSIAN NOISE AND λ PARAMETER

The analysis presented in Section 4 assumes that Eq. (15) is valid, i.e., that $A_d(p) \cong \lambda f(p) + n(p)$. Using the mean and variance of d', Eq. (34) and (37), we can test the conjec-

ture to see whether it holds true. We begin by splitting Eq. (15) into real and imaginary parts:

$$\mathrm{Re}[A_d(p)] \cong \lambda\, \mathrm{Re}[f(p)] + \mathrm{Re}[n(p)], \tag{38}$$

$$\mathrm{Im}[A_d(p)] \cong \lambda\, \mathrm{Im}[f(p)] + \mathrm{Im}[n(p)]. \tag{39}$$

For the AE case $\mathrm{Im}[f(p)]=0$; furthermore, if there is no noise present, then $A_d(p)=f(p)$ and $\lambda=1$. In general the kth pixel of the decrypted image, $A_d(p)$, is a complex valued random variable, and since we assume that $n(p)$ is circular Gaussian noise, we can calculate λ for any particular input image and decryption key as follows:

$$\lambda = \sum_{p=1}^{N} \mathrm{Re}[A_d(p)] \Big/ \sum_{p=1}^{N} f(p), \tag{40}$$

where $\mathrm{Re}[A_d(p)]$ is the real part of the pth pixel in the decrypted image.

A. Gaussian Noise and the Normalized Root Mean Squared

Using the standard 256×256 pixel Lena test image [28] simulations were run of the AE DRPE technique for decryption by using incorrect random phase keys, $R_{2,d}$. Using a completely random choice of decryption keys our simulations lead us to expect to calculate a high error value, i.e., NRMS$\approx$1. Such a simulation was performed 1000 times using different random phase keys, both for encryption and decryption, but always assuming perfect encryption and performing incorrect decryption. A pseudorandom number generator from Matlab [29] was used to generate the random phase keys with the generator being initialized by a 35-element vector based on the current state of the clock, thus avoiding repetition. For each run, once λ was found, $\mathrm{Re}[A_d(p)]-\lambda f(p)$ was plotted for each of the pixels. The average is calculated over the entire 1000 runs. If the noise is circular Gaussian, the result should have a Gaussian distribution with a mean value of zero. This is found to be the case (see Fig. 1). The corresponding imaginary parts, $\mathrm{Im}[A_d(p)]$, are also plotted, and the two curves coincide and are visually indistinguishable.

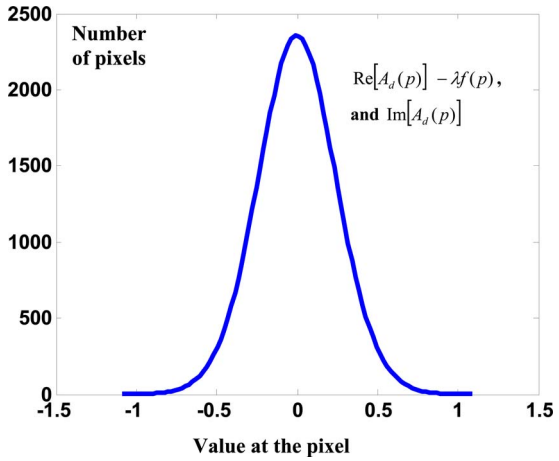

Fig. 1. (Color online) $\mathrm{Re}[A_d(p)]-\lambda f(p)$ and $\mathrm{Im}[A_d(p)]$ averaged over 1000 runs, for randomly chosen keys, for the 256×256 pixel Lena test image. The results are Gaussian and support the conjecture made in Eq. (15). As the total NRMS error value for an attempted decryption decreases, the area under the corresponding Gaussian noise graph decreases.

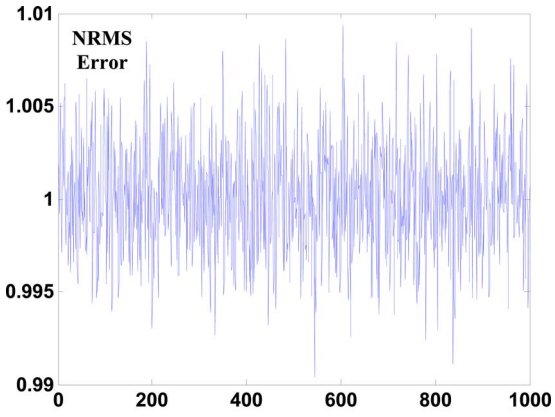

Fig. 2. (Color online) NRMS, Eq. (11), error values for each of the 1000 runs, with different keys used to generate Fig. 1. The average NRMS value here is calculated to be 1.0001, which is very close to 1.

Figure 2 is a plot of the individual NRMS error values for these 1000 runs and highlights the fact that completely random key selection produces large random NRMS error values with an average value close to ~1.

In Fig. 3 the NRMS errors (vertical axis) are plotted as a function of the fixed percentage of the pixels in the decryption key that are incorrect. For example, on the horizontal axis at the 50% mark every single pixel in this particular Fourier decrypting key (65,536 pixels in total) is assigned a value with a 50% probability that it is from the correct decryption key and a 50% probability that it is a pseudorandomly chosen phase value. The range of Fourier keys examined includes incorrect keys, with NRMS $\approx$1, and decryption keys resulting in almost perfect decryption, i.e., NRMS$\approx$0.

It should be emphasized that the incorrect pixels in $R_{2,d}$ are randomly distributed spatially throughout the

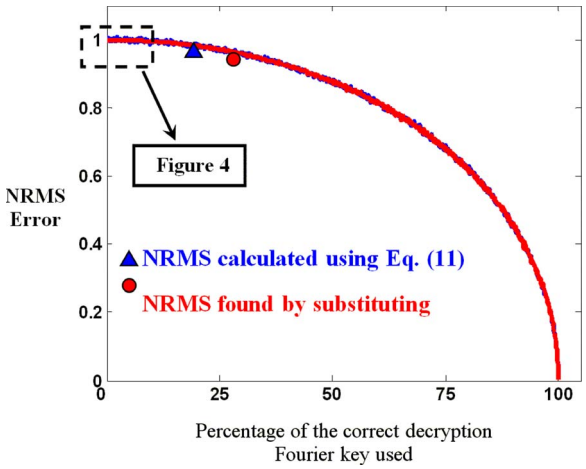

Fig. 3. (Color online) The blue curve (hidden blue triangles), plotted using Eq. (11), represents the direct NRMS calculated from the standard error metric. The red curve (red overlapping circles) is plotted by using Eq. (34), derived in Section 4, and is a close approximation to the numerical NRMS values (small black triangle). The dashed box relates to Fig. 4.

decryption key. It has been observed from numerical simulations that if these errors are concentrated within a particular region of the decryption key, then results are produced that are not consistent with those presented later in this section.

In Fig. 3 the NRMS error values calculated by using Eq. (11) are represented by blue triangles (nearly hidden here). They are compared with the values calculated when Eq. (34) is substituted back into Eq. (11), represented by red circles. The two curves in Fig. 3 deviate slightly from one another but are very similar. In Fig. 4 an enlarged section of Fig. 3 is shown. As in Fig. 3, Fig. 4(a) is based on a single run of the simulation and highlights the deviations between the NRMS calculated by using Eq. (11) (blue triangles) and the NRMS calculated when Eq. (34) is substituted back into Eq. (11) (red circles). Figure 4(b) shows the average curves plotted, generated for 500 individual simulations, i.e., runs using different decryption keys.

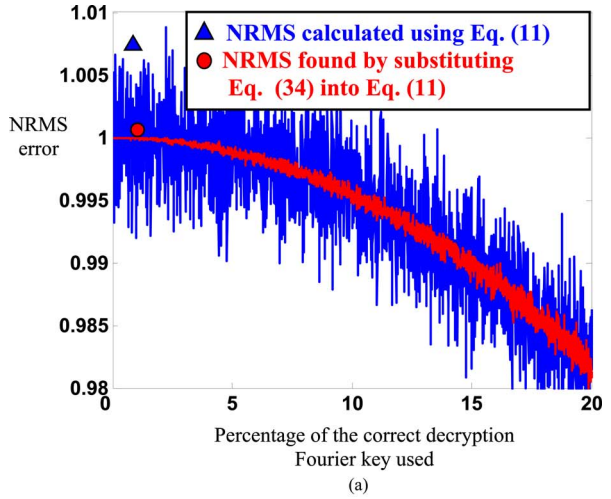

Fig. 4. (Color online) (a) Enlarged region indicated by the dashed box in Fig. 3. The NRMS error is plotted against the percentage of correct pixel values retained in $R_{2,d}$, during decryption. If 20% of $R_{2,d}$ is correct, then it implies that 80% of $R_{2,d}$ is made up of pseudorandomly generated, incorrect, quantization levels. (a) Two curves for 1 run of the simulation, large variations in the actual NRMS (blue curve) can be seen. (b) Curves plotted when averaged over 500 runs.

It can be observed that as the number of samples (pixels and runs) used increases, the simulated NRMS values, Eq. (11), approaches the NRMS curve based on the values predicted by using Eq. (34). The same trend is observed when, instead of averaging over many different decryption key runs for an image with a small number of pixels, averaging takes place over fewer runs but for an image with a much larger number of pixels. This highlights the validity and accuracy of the theoretical expressions. Different input grayscale images [28] were tested for image sizes of up to 10^6 pixels. All of the trends observed above using the Lena image were consistently reproduced.

Figure 5 contains three curves: (i) $(E_R[d'])^2$, Eq. (34) (blue with triangle); (ii) $E_R[d'^2]$, Eq. (36) (red with circle); and (iii) $V_R[d']$, Eq. (37) (green with square). Examining this figure, we can see that the variance of d', assuming $E_R[\lambda] \approx 0$, is very small, i.e., $V_R[d'] = 5.4 \times 10^{-7}$. The curves in Figure 5 show the corresponding relationship between the expected value squared, $(E_R[d'])^2$, and the variance, $V_R[d']$. It should be noted that in order to calculate the corresponding mean of the NRMS, $E_R[d']$ must be substituted back into Eq. (11).

B. λ Parameter

Intensive numerical simulations have been performed involving thousands of randomly chosen keys (though still a small percentage of all R possible keys in the key space). It has been observed that $E_R[\lambda] \approx 0$. However, in general, for a particular subset of the R keys, this does not have to be the case. To clarify, let us now examine a very particular subset of R, namely those keys in which 10% (90%) of the pixels in the decryption Fourier key are correct (incorrect).

First, using the following combinatorial based expression, we calculate how many keys in the key space will have a particular percentage of pixels in error:

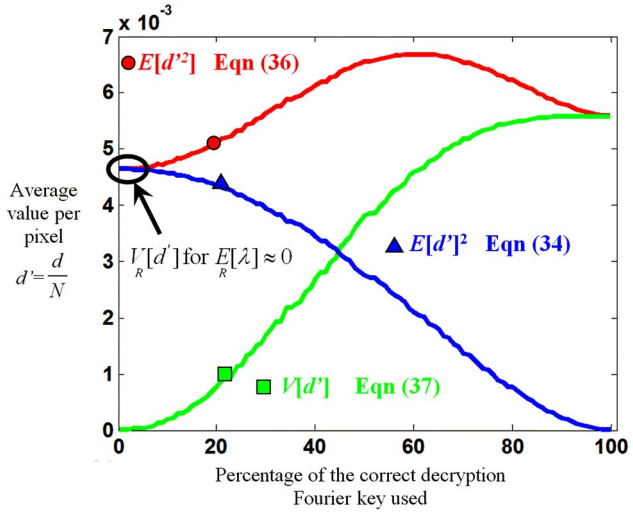

Fig. 5. (Color online) (i) $(E_R[d'])^2$ (blue with triangle), (ii) $E_R[d'^2]$ (red with circle), and (iii) $V_R[d']$ (green with square). These curves are plotted by using the same input data and system as was used to generate Fig. 3. For all possible keys, i.e., over all R, $V_R[d'] = 5.4 \times 10^{-7}$. It should be noted that, for any case where the expected value for λ is not 0, the expectation has been calculated over a subset of R.

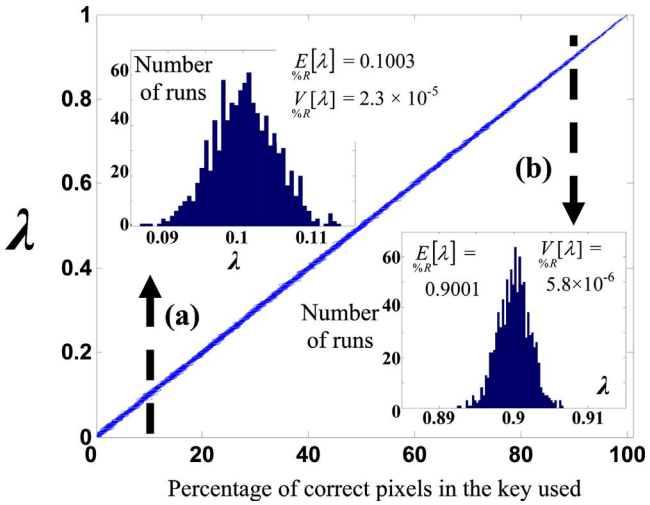

Fig. 6. (Color online) The diagonal line is made up of 100 runs for each percentage correct pixel case (in total 10^4 points). The cross sections shown are for the cases when (a) 10% and (b) 90% of the correct decryption key is present. Insets, histograms showing the distribution of λ values for the specific percentages of pixels in error (1000 runs).

$$\binom{N}{N-x} \times (q-1)^x. \tag{41}$$

In this expression q is the number of phase quantization levels used in the key, and x is the number of incorrect pixels (which defines the particular subset). In a system with 256×256 pixels and 16 quantization levels there are $R=1.6\times10^{78,913}$ possible keys in the key space. The large number of keys that have 10% of the pixels correct is $4.3\times10^{9,249}$; however this is only 2.6×10^{-293}% of the total number of keys, R. Clearly this is an extremely small percentage of the total.

The expected value of λ in this case, i.e., the 10% correct subset key case, is nonzero, i.e., $E_{\%R}[\lambda]\neq0$ (see below). This is in contrast to the expected value of λ calculated over the total set of R keys (the entire key-space), which is as stated approximately zero, $E_R[\lambda]\approx0$. As emphasized earlier, when performing this analysis we require that the incorrect keys used are generated by introducing errors at random spatially distributed positions in the decryption keys. This extra requirement will in fact reduce still further the number of possible keys, within any such subset, $\%R$, of all keys, R.

The central diagonal line appearing in Fig. 6 was generated numerically. It shows the λ values found for keys with percentage errors introduced into $R_{2,d}$ as described above. For each value of percentage pixels in error the resulting λ values for 100 such keys are plotted. As can be observed, there is a highly correlated linear relationship between $E_{\%R}[\lambda]$ and the percentage of randomly located pixels in errors in $R_{2,d}$.

To more closely examine the variation of λ two histograms appear as insets in Fig. 6. Each of the histograms was generated for 1,000 runs, i.e., for the 1,000 randomly chosen decryption Fourier keys, each of which is in a subset of key space with the same percentage error. Specifically, the histograms are for the cases when (a) 10% and (b) 90% of the pixels in the decryption Fourier keys are correct. In both histograms the $E_{\%R}[\lambda]$ found supports the existence of the linear relationship, while the low $V_{\%R}[\lambda]$ values indicate the high correlation of the linear relationship. Furthermore, since $V_{\%R}[\lambda]$ decreases from (a) 2.3×10^{-5} to (b) 5.8×10^{-6}, it is clear that even as $E_{\%R}[\lambda]$ and the number of keys in a particular key space subset change, the validity of the linear relationship between the λ value and the % of pixels in error still holds true.

In this section it has been shown that $E_{\%R}[\lambda]$ is linearly related (with high correlation) to the percentage of correct pixels in the decryption Fourier key. Based on these numerical results we now claim that if, for a particular incorrect key, a value of λ is calculated, we know with high certainty the percentage of correct pixels in the decryption Fourier key used. Therefore, while the NRMS error can tell us whether or not we have a good or a bad key, the corresponding λ value can provide us with quantitative information regarding the percentage of correct pixels in the decryption key.

6. COMPARISON WITH PREVIOUS RESULTS

To proceed we ask the reader to examine Fig. 7 of [22]. This figure presents NRMS values calculated for 10^6 randomly generated decrypting phase keys, $R_{2,d}$, applied to perfectly encrypted image data. In a numerically intensive and incomplete way these results demonstrated that the resultant NRMS errors, when plotted, have a bell shaped curve with a mean value of ~1.

In this paper we now have put in place all the tools needed to provide theoretically based insights into the above observations. We derived a set of statistical expressions, which allow us to gain knowledge about NRMS when it is used as the CF in the examination of the DRPE technique (and thus the key space) for very large numbers of samples (pixels or runs). Using our expression for $E[d']$, given in Eq. (34), and substituting it into Eq. (11),

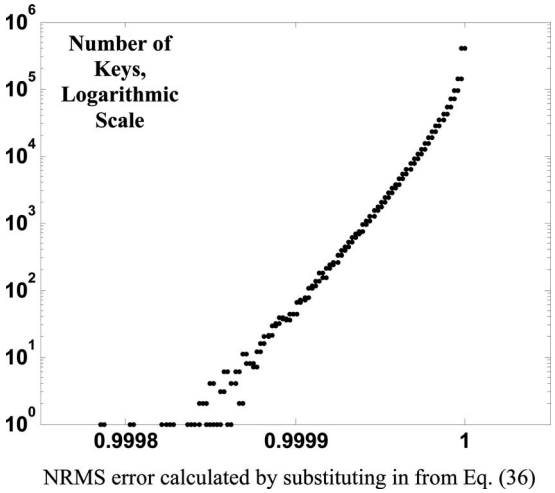

Fig. 7. Following perfect encryption of a 256×256 pixel, 16 quantization level Lena test image, 10^6 decrypting phase keys, $R_{2,d}$, are randomly generated. It can be seen that the expected value of NRMS≈1. Furthermore, even after attempting decryption with 10^6 different phase keys, the lowest NRMS value calculated was 0.9998. The calculated $V_R[d']$ value of this curve, with $R=10^6$, is 3.275×10^{-11}.

to calculate the mean of the NMRS error, we now repeat the study performed to produced Fig. 7 in [22]. The result, generated by using 10^6 randomly chosen decryption keys, is presented in Fig. 7 in this paper.

Figure 7 in this paper indicates that the most likely theoretical NRMS value expected, when a randomly generated decryption key is used, has a mean value of ~1. As in Fig. 7 of [22], all one million randomly chosen decryption keys produced NRMS values between 0.9998 and 1. In this case the calculated $V_R[d']$, for the results presented in Fig. 7 in this paper, is 3.2751×10^{-11}. Since the NRMS produced has a very small statistical variance and a large mean value, this indicates that employing a brute-force method of attack on this system would prove unsuccessful. The statistical results presented therefore confirm the previous observation made in [22] based solely on simulations,. Considering the very narrow variance value of the NRMS, we can confirm that the hypothesis made in [22], that the vast majority of keys will fall within a narrow range of NRMS values, i.e., (0.9998, 1] in Fig. 7 in this paper, has been shown to be true.

Visually, the most noticeable difference between the result presented in Fig. 7 in [22] and those appearing in Fig. 7 here is that the curve here no longer has the symmetric distribution appearing in Fig. 7 of [22]. In this paper the highest possible error value achievable by using the statistically calculated expressions, i.e., the largest value of the NRMS value calculated using $E[d]$, is 1. This is because power conservation is required, which is not the case for the unconstrained numerically calculated NRMS value whose maximum value is $\sqrt{2}$ in [22]. This maximum theoretical value of the NRMS occurs only when the original input image is compared with its inverse (negative image). We note however, that owing to our application of the law of conservation of energy, which is explicitly built into the methodology employed here, it is not always possible to decrypt an encrypted image to its own negative image by using a phase key from the allowed systems key space. In other words in this paper our possible NRMS values are constrained by the fact that a dark low-power image cannot be decrypted to the corresponding bright negative.

7. CONCLUSION

The amplitude-encoding (AE) case of the double random phase encoding (DRPE) technique is examined by using statistical techniques. Throughout the analysis it is assumed that perfect encryption takes place and the decryption process is then analyzed. This approach is of practical interest as it corresponds to the case when an attacker has knowledge of a cipher–text pair. A cost function (CF) is needed during such an attack to gauge a possible decryption keys' accuracy, or closeness, to a valid decryption key. The CF typically used in the literature to quantify the success of an attempted decryption compared with the original input image is the normalized root mean squared (NRMS) error. The NRMS CF, in the AE DRPE case, is based on an intensity difference parameter, d. Thus the amount of error in the output intensity following an attempted decryption is used as a measure of the accuracy (validity) of a particular test decryption key. The smaller the error present in the decrypted image, the closer the decryption key used is to the correct key. We note that the Euclidean distance in key space, between an incorrect and the correct $R_{2,d}$ key, is not a good measure of the validity of that key (i.e., its ability to decrypt correctly), and is not a good predictor of the resulting NMRS error. Previously [22] it has been shown that keys that are a large Euclidean distance away from the correct key can still decrypt with very low NRMS errors

To analyse the AE DRPE case we assumed that the noise in the output field is circular Gaussian and made a conjecture regarding the form of the output field by introducing the λ parameter. Based on simulations we first confirmed that the resulting output field noise is circular Gaussian. Since the DRPE is lossless we then examined how power conservation places restrictions on the properties of the possible output fields. We then proceeded to derive analytical expressions for the mean and the variance of the intensity difference parameter d in terms of the statistical properties of the output field. A series of simulations were performed to show that as the sample size used increases (i.e., the number of pixels and runs for different $R_{2,d}$ keys), the numerical results tend toward the statistically derived analytic expressions. Our results verify the validity of the theoretical expressions for large systems and also confirm our observation that for small systems the NRMS values can vary significantly.

We have shown for the case where the errors in $R_{2,d}$ are randomly distributed spatially that there is a highly correlated linear relationship between $E_{\%R}[\lambda]$ and the subset of keys with a particular percentage of pixels in error, $\%R$. Based on our results it can be stated that, in general, if λ is known, then, with high certainty, the percentage of correct pixels in the decryption Fourier key used is also known. This observation might be used to significantly reduce the size of the key space to be searched during an attack or conversely be used to improve AE DRPE security.

In a previous publication [22] both small and large key spaces were examined. The results presented here have been shown to corroborate the previously published results based solely on intensive but limited numerical simulations [22]. Thus the hypothesis made in [22] that the vast majority of keys in this AE DRPE key-space, lie on the curve formed by these one million randomly chosen keys, has been statistically confirmed.

ACKNOWLEDGMENTS

We acknowledge the support of Enterprise Ireland (EI) and Science Foundation Ireland (SFI). We also thank the Irish Research Council for Science, Engineering and Technology. D. S. Monaghan acknowledges the support of The International Society for Optical Engineering (SPIE) through a SPIE Educational Scholarship.

REFERENCES

1. H. O. Yardley, *The American Black Chamber* (Naval Institute Press, 1931).
2. G. F. Gaines, *Cryptanalysis: A Study of Ciphers and Their Solution* (Dover, 1939).

3. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory **22**, 644–654 (1976).
4. C. A. Deavours, *Cryptology Yesterday, Today and Tomorrow* (Artech House, 1987).
5. P. Réfrégier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
6. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**, 224–230 (1994).
7. B. Javidi, *Optical and Digital Techniques for Information Security* (Springer Verlag, 2005).
8. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt. **39**, 6595–6601 (2000).
9. L. E. M. Brackenbury and K. M. Bell, "Optical encryption of digital data," Appl. Opt. **39**, 5374–5379 (2000).
10. 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).
11. B. M. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett. **28**, 269–271 (2003).
12. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng. **43**, 2233–2238 (2004).
13. B. M. Hennelly and J. T. Sheridan, "Optical encryption and the space bandwidth product," Opt. Commun. **247**, 291–305 (2005).
14. B. Javidi, A. Sergent, G. S. Zhang, and L. Guibert, "Fault tolerance properties of a double phase encoding encryption technique," Opt. Eng. **36**, 992–998 (1997).
15. 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).
16. B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption," Appl. Opt. **39**, 4117–4130 (2000).
17. B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," Optik (Stuttgart) **114**, 251–265 (2003).
18. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng. **43**, 2239–2249 (2004).
19. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Express **14**, 3181–3186 (2006).
20. T. J. Naughton, B. Hennelly, and T. Dowling, "Introducing secure modes of operation for optical encryption," J. Opt. Soc. Am. A **25**, 2608–2617 (2008).
21. D. S. Monaghan, G. Situ, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Role of phase key in the double random phase encoding technique: an error analysis," Appl. Opt. **47**, 3808–3816 (2008).
22. D. S. Monaghan, U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Key-space analysis of double random phase encryption technique," Appl. Opt. **46**, 6641–6647 (2007).
23. D. S. Monaghan, G. Situ, G. Unnikrishnan, T. J. Naughton, and J. T. Sheridan, "Analysis of phase encoding for optical encryption," Opt. Commun. **282**, 482–492 (2008).
24. G. Situ, U. Gopinathan, D. S. Monaghan, and J. T. Sheridan, "Cryptanalysis of optical security systems with significant output images," Appl. Opt. **46**, 5257–5262 (2007).
25. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**, 10253–10265 (2007).
26. J. W. Goodman, *Statistical Optics* (Wiley, 2000).
27. D. S. Monaghan, "Practical implementations and theoretical analysis of optical encryption," Ph.D. dissertation (University College Dublin, 2009).
28. Lena Test Image, http://sipi.usc.edu/database/.
29. Matlab 7.0.1, http://www.mathworks.com/.