Cost function statistical analysis in double random phase encoding

David S. Monaghan [a], Unnikrishnan Gopinathan [b], Guohai Situ [b],
Thomas J. Naughton [c], John T. Sheridan [a*]

[a] Optoelectronic Research Centre, School of Electrical, Electronic and Mechanical Engineering,
University College Dublin, Belfield, Dublin 4, Ireland,
SFI Strategic Research Centre in Solar Energy Conversion.

[b] Institut für Technische Optik, Universität Stuttgart, Pfaffenwaldring 9,
70569 Stuttgart, Germany.

[c] Department of Computer Science,
National University of Ireland, Maynooth, Ireland,
and
University of Oulu, RFMedia Laboratory,
Oulu Southern Institute, Vierimaantie 5,
84100 Ylivieska, Finland. tomn@cs.nuim.ie

ABSTRACT

We examine the Amplitude-Encoding (AE) case of the Double Random Phase Encoding (DRPE) technique. A cost function is the function we use to evaluate an attempted decryption with our original input image. For systems with a relatively small key-space we can evaluate the output of every key to get an overall idea of the spread of these keys in key-space. However for larger systems this is not practical. Based on a normalised root mean squared cost function we wish to identify expressions for the mean and variance of the output (decrypted) intensity for a sample set of keys in a large system (256x256 pixels).

Keywords: Optical processing, Digital image processing, Fourier optics, Numerical approximation and analysis

1. INTRODUCTION

Cryptography[1-4] and information security has been recognised as important by governments and individuals throughout history. With the major technological advance in computer technology, optical fibre technology, global satellite communications and the 'world wide web', information security had become of paramount importance. The new digital information age has brought access to powerful desktop computers along side of which is a demand for high security. This demand has lead to ever faster and more powerful encryption systems being continually developed.

Optical encryption[5-11] is one such form on information security and is particularly interesting as it offers the possibility of high-speed parallel encryption of two dimensional (2-D) image data.

**Corresponding author:* e-mail: john.sheridan@ucd.ie; Tel:+353-(0)1-716-1927 Fax:+353-(0)1-283-0921

Optics and Photonics for Information Processing II, edited by Abdul Ahad Sami Awwal,
Khan M. Iftekharuddin, Bahram Javidi, Proc. of SPIE Vol. 7072, 70720Z, (2008)
0277-786X/08/$18 · doi: 10.1117/12.798202

One such method of optical encryption is known as the Double Random Phase Encryption [5] (DRPE) technique. DRPE is a unique optical-image encryption technique, which involves the use of two random phase keys, one placed in the input domain and one placed in the Fourier domain. If these two random phase-keys are generated using statistically independent white noises, then the encrypted image is also a stationary white noise. Since it's introduction in 1995, the DRPE has generated much interest and been the focus of many studies [10,12-16]. The physical implementation of such an optical system gives rise to many practical issues, however a thorough numerical analysis of DRPE is extremely important if it is to be utilised as an encryption system.

The two primary modes of operation of the DRPE technique, which depend on the form of the data to be encrypted, are:

(1) Amplitude-Encoding (AE), with a greyscale input image, and

(2) Phase-Encoding (PE), in which through out this paper we assume that only the input field phase is modulated.

While the optical system used to encrypt the data, in both cases is very similar, there are significant differences in the decryption, analysis and breaking of these encoding systems. Figure 1 shows a flow chart graph of the DRPE technique for AE and PE. In this paper we are primarily concerned with AE.

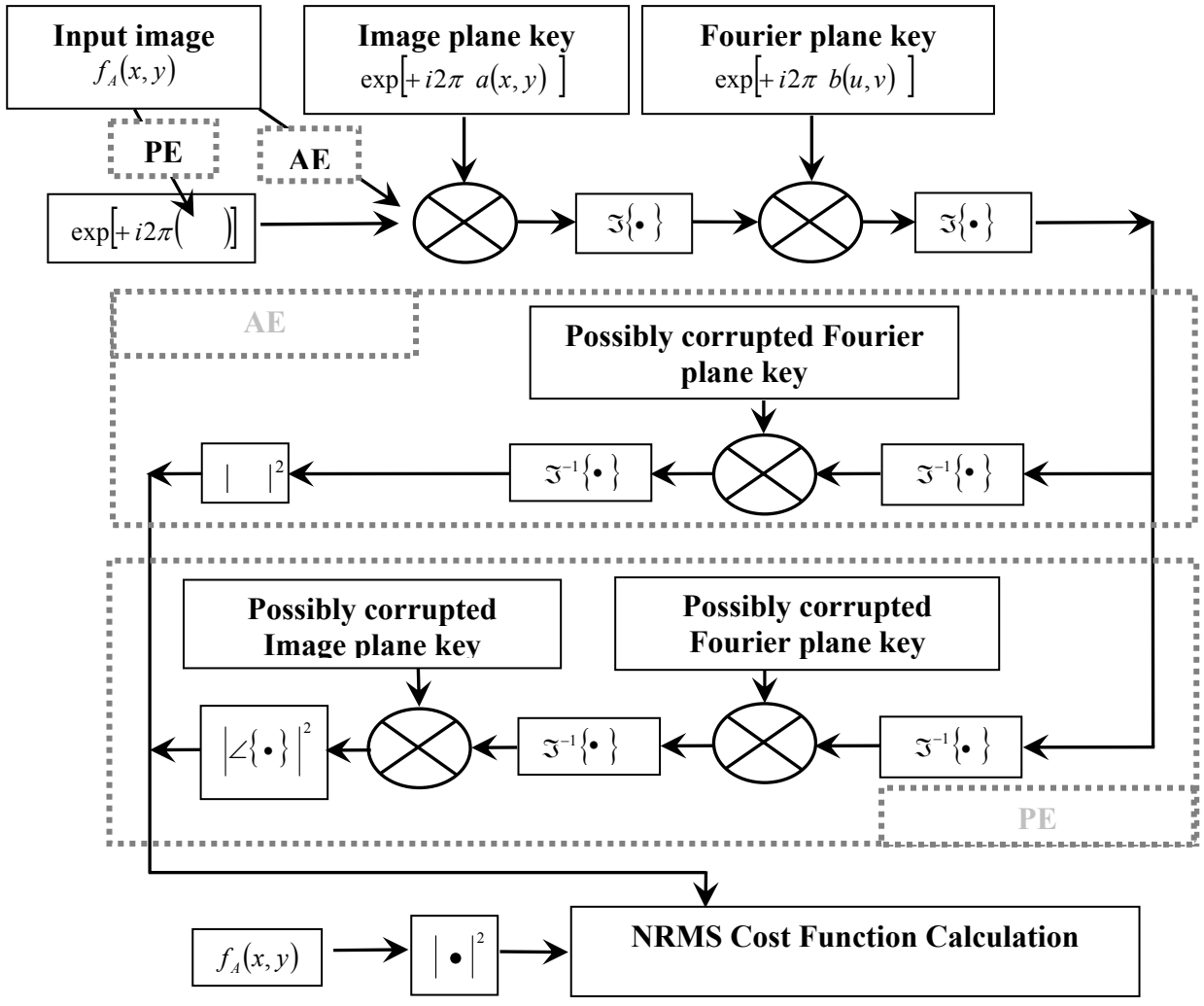

Figure 1. A block diagram of the similar encryption process for AE and PE and the different decryption processes which lead to an Normalised Root Mean Squared (NRMS) value for a decrypted image.

In the case when a PE input image (phase data) is used, both the Image and Fourier plane keys, $a(x, y)$ and $b(u, v)$, are required in the decryption process. However we are only concerned with the AE case in this paper and therefore only the Fourier pane key is necessary for decryption. It should be noted that the phase key will be the same size, number of pixels, as the input image in these simulations. For relatively small systems, i.e. systems with an input image of 5x5 pixels and under, we can easily evaluate the output decryption of every key to get an overall idea of the distribution of these keys in key-space.

An encryption algorithm's key-space is a set of possible keys that can be used to encode data using that algorithm. For instance, a simple combination lock with three dials, each with ten digits, has a key-space of one thousand keys, i.e. 10^3. The number of possible combinations therefore grows exponentially with the number of dials (equivalently, 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 encryption algorithm. The number of keys in the key-space is given by the number of quantisation levels, used in the key, raised to the power of the number of pixels in the key. For example a system with 5x5 pixels and 2 quantisation levels has 2^25 keys, or 33,554,432 keys in its key-space. However for larger systems, i.e. 256x256 pixels with 256 quantisation levels having 256^65,536 keys in the key-space, checking every single key is currently not practical. Like most encryption techniques DRPE relies heavily on the size of its key-space to provide security from brute-force attacks, i.e. the probability of randomly guessing a correct key being statistically insignificant.

Should the attacker have access to a cipher/text pair, it has already been shown that in the case of AE, heuristic methods [15] can be used to extract the DRPE Fourier key, $b(u, v)$, with NMRS errors below 10%, within a reasonable amount of time, i.e. within less than an hour using a PC. Other methods can be used if several cipher/text pairs are available when attacking the system, and such techniques have been found to be very effective [17,18].

Using the normalised root mean squared cost function, discussed below in Section 3, we wish to identify expressions for the mean and variance of the output (decrypted) intensity for a sample set of keys in a large system (256x256 pixels). By relating the mean and variance of the sample set from the larger system to that of the smaller system we wish to make conclusions about the distribution of keys in the key-space of the DRPE technique.

In our previous work[19] we examined the algorithm's key-space using histograms showing the number of keys which decrypt an encoded message to given quantitative error levels. We carried out our analysis for small input image sizes, i.e. 5×5 pixels. By mapping the decrypting error across the entire key-space we attempt to provide an analysis of the strength of the optical encryption algorithm. An analysis of the key-space for large image sizes (large number of pixels) was computationally too intensive due to the large number of keys. By defining analytical expressions for the mean and the variance for the NRMS cost function we hope to provide useful tools to permit the study and analysis of the key space for larger input images, i.e. 256×256. These tools will allow us, in future work, to relate our previous work on small key space systems to those of large ones thus furthering our overall understanding of the DRPE technique.

The paper is organised as follows: In Section 2 will introduce some statistical definitions regarding the mean, the variance and the noise. In Section 3 we will look at our NRMS cost function in relation to the DRPE technique. In Section 4 we derive analytic expressions for the mean and for the variance and in Section 5 we finally conclude.

2. STATISTICAL DEFINITIONS

2.1 Mean and Variance

Let us assume that we have a real valued continuous function, $f(x)$, which we have sampled discretely K times, $0 < k < K+1$. Denoting this sampled function as $f(k)$ then if it is real, $f(k) = f^*(k)$. For a real valued random variable, the mean can be defined as the expectation of that random variable and represents the central location of the data set. The population mean or expected value of the data set f is therefore given by:

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

The variance of the data set *f* is a good measure of the statistical dispersion away from its 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 is given by:

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

(2)

The variance of *f* can also be written as:

$$V[f]=E(f^2)-E(f)^2\ .$$

(3)

2.2 Gaussian Noise

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

$$pdf\sim\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left[\frac{(x-\mu)^2}{2\sigma^2}\right],$$

(4)

where *x* represents a particular value taken by *g*(*k*) if *K* is very large and the PDF indicates the probability (frequency) of such a value occurring.

Such Gaussian noise distributions have several properties, one of which is referred to as the The *Gaussian Moment Theorem*. If we define the nth moment of the Gaussian random variable *x* about the value *z* as:

$$M_{n,z}=\int_{-\infty}^{+\infty}(x-z)^n\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left[\frac{(x-\mu)^2}{2\sigma^2}\right]dx\ ,$$

(5)

then we note that $E[x]=\mu=M_{1,0}$ and $V[x]=\sigma^2=M_{2,\mu}$.

Eqn (5) has two important ramifications for our case:

(1) Firstly we note that the mean of the data values squared is equal to the sum of the square of their mean and their variance:

$$E[\ g^2]=\frac{\sum_{k=1}^{k=K}g^2(k)}{K}=\left\{\ E[\ g\ ]\right\}^2+V[\ g\ ]=\mu^2+\sigma^2\ .$$

(6)

(2) Secondly, 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 and identical standard variations, where '*r*' denotes the real part and '*i*' denotes the imaginary part.

(3)

We can summarise the statistical properties of the noise as follows:

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

(7)

and

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

(8)

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

$$nn^*=n^*n=|n|^2=|n_r|^2+|n_i|^2\ ,$$

(9)

therefore

$$E\left[\,|n|^2\right] = E\left[\,|n_r|^2 + |n_i|^2\right] = E\left[\,|n_r|^2\right] + E\left[\,|n_i|^2\right] = 2E\left[\,|n_{r,i}|^2\right] = 2\sigma^2 \tag{10}$$

Furthermore[20]:

$$E[nn^*nn^*] = 2(E[nn^*])^2 = 2E\left[|n|^2\right]^2. \tag{11}$$

3. Normalised Root Mean Squared (NRMS) error

We wish to quantitatively compare an image (data array) and a perturbed or noisy version of that image. In our case these data sets correspond to intensities (images) captured by a CCD camera or simulated intensities generated by a computer programme. More specifically the data sets, which, under ideal noise error free conditions should be identical and which we wish to compare, 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.

During the encoding/decoding process an image is encrypted and must then be decrypted upon receipt. During these processes errors are accumulated. Furthermore attempts to break or crack the encryption system will involve searching a key space for the exact solution key. The effects on the outputs of perturbations away from the exact encryption keys, is analogous to the effects of noise and also provides insights into the robustness of the encryption system to attack.

One metric that allows us to make such a comparison is the NRMS

$$NRMS = \sqrt{\frac{\sum_{k=1}^{k=N}\left|I(k) - I_d(k)\right|^2}{\sum_{k=1}^{k=N}\left|I(k)\right|^2}}. \tag{12}$$

At the core of this metric is the difference term

$$d = \sum_{k=1}^{k=N}\left|I(k) - I_d(k)\right|^2. \tag{13}$$

This difference term will be used to form the basis of our analysis of the effects of noise on the performance of the DRPE technique in the AE case, see Figure 1.

From Figure 1 we can get the following expression for the decrypted complex data:

$$= \Im^{-1}\left\{\Im^{-1}\left\{\Im\left\{\Im\left\{f \times R_{image}\right\}\right\}\right\}\right\} \otimes \Im^{-1}\left\{\Im^{-1}\left\{\Im\left\{R_{Fourier\_encryption}\right\}\right\}\right\} \otimes \Im^{-1}\left\{R_{Fourier\_decryption}\right\}, \tag{14}$$

with simplifies to:

$$A_d = \left[f \times R_{image}\right] \otimes \left[\Im\left\{R_{Fourier\_decryption}\right\} \oplus \Im\left\{R_{Fourier\_encryption}\right\}\right], \tag{15}$$

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

We now make a conjecture regarding the form of the output-decrypted field. We propose that

$$A_d(k) \cong \lambda f(k) + n(k), \tag{16}$$

where λ is a constant, *f(k)* is the sampled input signal and *n* represents circular white Gaussian noise with zero mean as discussed in Section 2.

For the AE case we define the input intensity to be $I = \left| f \right|^2 = f^2$, and from Eqn (16) the corresponding output decrypted image intensity is given by:

$$I_d = \lambda^2 f^2 + \lambda f\left[2n_r\right] + \left|n\right|^2 .$$

(17)

We now return to our definition of the intensity difference error metric, *d*, given in Eqn (13). Substituting in from Eqn (17), and rewriting, we get that:

$$d = \sum_1^K \left| \lambda^2 f^2(k) + \lambda f(k)\left[2n_r(k)\right] + \left|n(k)\right|^2 - f^2(k) \right|^2 .$$

(18)

Expanding Eqn (18) and expressing in terms of a continuous function gives that:

$$d = \left(\lambda^2 - 1\right)^2 f^4 + 4\lambda\left(\lambda^2 - 1\right) f^3 n_r + 2\left(\lambda^2 - 1\right) f^2 \left|n\right|^2 + 4\lambda^2 f^2 n_r^2 + 4\lambda f n_r \left|n\right|^2 + \left|n\right|^4 .$$

(19)

3.2 The Expected Value of the NRMS

We recall from Eqn (1) the expected value of a function and introduce the notation following:

$$f_p = E\left[f^p(k)\right] = \frac{\sum_{k=1}^K f^p(k)}{K} .$$

(20)

Therefore the expected value of d can be written as:

$$E\left[\ d\ \right] = \sum\ \left(\lambda^2 - 1\right)^2 E\left[f^4\right] + 4\lambda\left(\lambda^2 - 1\right) E\left[f^3 n_r\right] + 2\left(\lambda^2 - 1\right) E\left[f^2 \left|n\right|^2\right] + 4\lambda^2 E\left[f^2 n_r^2\right] + 4\lambda E\left[f\ n_r \left|n\right|^2\right] + E\left[\ \left|n\right|^4\right] .$$

(21)

Which can also be expressed in terms of sampled data sets as:

$$E\left[\ d\ \right] = \frac{\left(\lambda^2 - 1\right)^2}{K} \sum_{k=1}^{k=K} f^4(k) + \frac{4\lambda\left(\lambda^2 - 1\right)}{K} \sum_{k=1}^{k=K} f^3(k) n_r(k) + \frac{2\left(\lambda^2 - 1\right)}{K} \sum_{k=1}^{k=K} f^2(k) \left|n(k)\right|^2$$
$$+ \frac{4\lambda^2}{K} \sum_{k=1}^{k=K} f^2(k) n_r(k)^2 + \frac{4\lambda}{K} \sum_{k=1}^{k=K} f(k) n_r(k)\ \left|n(k)\right|^2 + \frac{1}{K} \sum_{k=1}^{k=K} \left|n(k)\right|^4 .$$

(22)

If we can assume that *K* is large and we are thus dealing with a large number of samples (pixels), then we can assume

$$E\left[f^p(k) n_r^q(k)\right] \approx E\left[f^p(k)\right] \times E\left[n_r^q(k)\right] ,$$

(23)

and

$$E\left[f^p(k) \left|n(k)\right|^{2q}\right] \approx E\left[f^p(k)\right] \times E\left[\ \left|n(k)\right|^{2q}\right] .$$

(24)

Furthermore as discussed above, since the noise is assumed to be a circular random Gaussian variable using the Gaussian Moment Theorem we can write that

$$E\left[\ \left|n(k)\right|^4\right] \approx 2E\left[\ \left|n(k)\right|^2\right]^2$$

(25)

and that

$$E\left[\ \left|n(k)\right|^2 n(k)\right] = 0 , \text{ and } E\left[\ n^2(k)\right] = 0 .$$

(26)

Then substituting back into Eqn (22) using Eqns (23), (24), (25), (26) and (20) and simplifying we get that

$$E\left[\ d\ \right] = \left(\lambda^2 - 1\right)^2 f_4 + 4\left(\lambda^2 - 1\right) f_2 \sigma^2 + 4\lambda^2 f_2 \sigma^2 + 8\sigma^4 \ . \tag{27}$$

We have now derived the expected value of the intensity difference error metric in terms of the statistical properties of the perturbation in the decrypted field and the constant parameter λ.

In our analysis the encryption/decryption process is performed numerically. The FFT algorithm is used and each pixel is represented by a single complex value in the computer. Thus we neglect all physical modelling issues, e.g. SLM fill factor, polarisation and diffraction effects. Such simplifications are tolerated only because it is the nature of the DRPE algorithm, which is our primary consideration here and not the non-ideality introduced by the physical limitations of the use of SLMs in physically implemented optical systems.

When dealing with numerical simulations of the DRPE technique, implemented using lossless linear Fourier transforms and lossless phase masks, requires that power (total intensity) be conserved between the encryption input and decryption output. This implies that:

$$\sum_1^K \ \left|A_d(k)\right|^2 = \sum_1^K \ \left|\lambda f(k) + n(k)\right|^2 = \sum_1^K \ \left|f(k)\right|^2 \tag{28}$$

$$\Rightarrow \sum_1^K \ \left\{\lambda^2 f^2(k) + 2\lambda f(k) n_r(k) + \left|n(k)\right|^2\right\} = \sum_1^K \ f^2(k) \tag{29}$$

and thus

$$\lambda^2 f_2 + E\left[\ \left|n(k)\right|^2\right] = f_2 \Rightarrow E\left[\ \left|n(k)\right|^2\right] \ = 2\sigma^2 = \left(1 - \lambda^2\right) f_2 \tag{30}$$

Therefore in order that power be conserved

$$\lambda^2 \equiv 1 - \frac{2\sigma^2}{f_2} \tag{31}$$

3.3 The Variance of the Intensity Difference Error Metric

We now wish to find the variance of d, $V[d]$. We recall Eqn (3), $V[f] = E\left(f^2\right) - E(f)^2$. So in order to obtain the variance we must calculate the expected value of d^2, i.e. $E[d^2]$, which is algebraically not trivial.
To simplify our calculations we substitute each of the six terms in 'd', Eqn (19), with a Greek letter as follows:

$$\alpha = \left(\lambda^2 - 1\right)^2 f^4 \ , \beta = 4\lambda\left(\lambda^2 - 1\right) f^3 n_r \ , \chi = 2\left(\lambda^2 - 1\right) f^2 \left|n\right|^2 \ , \delta = 4\lambda^2 f^2 n_r^2 \ , \varepsilon = 4\lambda f n_r \left|n\right|^2 \ \& \ \phi = \left|n\right|^4 \ . \tag{32}$$

therefore our calculation simplifies to:

$$E\left[d^2\right] = E\left[\left(\alpha + \beta + \chi + \delta + \varepsilon + \phi\right)^2\right] \tag{33}$$

Expanding Eqn (33) give us:

$$\begin{aligned} E\left[d^2\right] \ = \sum \ & E\left[\alpha^2\right] + E[\alpha\beta] + E[\alpha\chi] + E[\alpha\delta] + E[\alpha\varepsilon] + E[\alpha\phi] + E[\beta\alpha] + E\left[\beta^2\right] \ + E[\beta\chi] + E[\beta\delta] + E[\beta\varepsilon] + E[\beta\phi] \\ & + E[\chi\alpha] + E[\chi\beta] + E\left[\chi^2\right] \ + E[\chi\delta] + E[\chi\varepsilon] + E[\chi\phi] + E[\delta\alpha] + E[\delta\beta] + E[\delta\chi] + E\left[\delta^2\right] \ + E[\delta\varepsilon] + E[\delta\phi] \\ & + E[\varepsilon\alpha] + E[\varepsilon\beta] + E[\varepsilon\chi] + E[\varepsilon\delta] + E\left[\varepsilon^2\right] \ + E[\varepsilon\phi] + E[\phi\alpha] + E[\phi\beta] + E[\phi\chi] + E[\phi\delta] + E[\phi\varepsilon] + E\left[\phi^2\right] \ . \end{aligned} \tag{34}$$

However we recall when we simplified Eqn (22) that previously, terms which included $E[\beta]$ or $E[\varepsilon]$ averaged to zero. If we apply this to Eqn (34) it reduces to:

$$E\left[d^2\right] \ = \sum \ E\left[\alpha^2\right] + E\left[\chi^2\right] + E\left[\delta^2\right] + E\left[\phi^2\right] + 2E[\alpha\chi] + 2E[\alpha\delta] + 2E[\alpha\phi] + 2E[\delta\phi] + 2E[\delta\chi] + 2E[\chi\phi] \ .$$

(35)

We can use the following equation, derived using Eqn (5), to define the expected value of the noise terms:

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

(36)

This gives that:

$$\begin{aligned} E\left[d^{2}\right] \ = \ & \left(\lambda^{2}-1\right)^{4} f_{8} + 32\left(\lambda^{2}-1\right)^{2} f_{4}\sigma^{4} + \left(16\lambda^{4} f_{4} \ \times \ 52.5\sigma^{6}\right) + 1912.5\sigma^{8} \ + 8\left(\lambda^{2}-1\right)^{3} f_{6}\sigma^{2} \\ & + 8\left(\lambda^{2}-1\right)^{2} \lambda^{2} f_{6}\sigma^{2} + 16\left(\lambda^{2}-1\right)^{2} f_{4}\sigma^{4} + 64\lambda^{2} f_{2}\sigma^{6} + 32\lambda^{2}\left(\lambda^{2}-1\right) f_{4}\sigma^{4} + \left(4\left(\lambda^{2}-1\right) f_{2} \ \times \ 172.5\sigma^{6}\ \right) \end{aligned}$$

(37)

Therefore using Eqn (31), our expression for the variance becomes:

$$v[d] = \frac{1}{f_{2}^{4}} \left(\begin{aligned} & -16 f_{2}^{6}\sigma^{4} + 128 f_{2}^{2}\left(f_{2}^{3} + 6.6\left(-0.1+f_{2}\right) f_{2} f_{4} + 0.25 f_{6}\right)\sigma^{6} \\ & + 340.5\left(f_{2}^{4} + 1.1 f_{2}^{2} f_{4} - 9.9 f_{2}^{3} f_{4} - 0.05 f_{4}^{2} - 0.4 f_{2} f_{6} + 0.05 f_{8}\right)\sigma^{8} + 3360 f_{2}^{2} f_{4}\sigma^{10} \end{aligned} \right).$$

(38)

Eqns (27) and (38) combined allow us to calculate the mean and variance for any greyscale input image having any pixel size.

5. CONCLUSION

We examined the Amplitude-Encoding (AE) case of the Double Random Phase Encoding (DRPE) technique. The cost function primarily used in the literature to evaluate an attempted decryption with an original input image is the Normalised Root Mean Squared (NRMS) error. For systems with a relatively small key-space we can evaluate the output of every key to get an overall idea of the spread of these keys in key-space. However for larger systems this is not practical. In this paper we have derived analytical expressions for the mean and the variance for the NRMS cost function. These tools will allow us, in future works, to systematically study the key space for larger input images, i.e. 256 × 256 pixels, which should agree in the limit to our previous work on the key space analysis of small, 5 × 5 pixels key DRPE systems. By fully analysing the DRPE technique we hope to further advance our overall knowledge of this important optical encryption technique.

6. ACKNOWLEDGEMENTS

We acknowledge the support of Enterprise Ireland and Science Foundation Ireland through the Research Innovation and Proof of Concept Funds, and the Basic Research and Research Frontiers Programmes. We would also like to thank the Irish Research Council for Science, Engineering and Technology. One of the authors (DM) acknowledges the support of The International Society for Optical Engineering SPIE through an SPIE Educational Scholarship.

References

1. G. F. Gaines, "*Cryptanalysis: A study of ciphers and their solution*", Dover Pulications, 1939.
2. H. O. Yardley, "The American Black Chamber", Naval Institude Press, 1931.
3. W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE, **22,** 644-654, 1976.
4. C. A. Deavours, "Cryptology Yesterday, Today and Tomorrow," Artech House, 1987.
5. P. Refregier and B. Javidi, "Optical-Image Encryption Based on Input Plane and Fourier Plane Random Encoding," Opt. Lett., **20,** 767-769, 1995.
6. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," Appl. Opt., **39,** 6595-6601, 2000.
7. B. M. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett., **28,** 269-271, 2003.

8. B. M. Hennelly and J. T. Sheridan, "Optical encryption and the space bandwidth product," Opt. Comm., **247,** 291-305, 2005.
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. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," Opt. Eng., **43,** 2233-2238, 2004.
12. 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.
13. 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.
14. B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," Optik, **114,** 251-265, 2003.
15. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," Opt. Exp., **14,** 3181-3186, 2006.
16. B. M. Hennelly and J. T. Sheridan, "Random phase and jigsaw encryption in the Fresnel domain," Opt. Eng., **43,** 2239-2249, 2004.
17. 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.
18. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Exp., **15,** 10253-10265, 2007.
19. 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.
20. J. W. Goodman, "*Statistical Optics,*" John Wiley and Sons INC, 2000.