A Numerical analysis of double random phase encryption

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

[a] School of Electrical, Electronic and Mechanical Engineering, College of Engineering,
Mathematics and Physical Sciences, University College Dublin, Belfield,
Dublin 4, Ireland.

[b] Department of Computer Science, National University of Ireland Maynooth,
Maynooth, Ireland.

ABSTRACT:

We consider a Double Random Phase Encoding (DRPE) Encryption/Decryption system in which the image encryption/decryption process is performed numerically. In this paper we present a key-space analysis of the (DRPE) algorithm which is used to encrypt two dimensional (2-D) images. We map the assiocated error for every phase-key in the key-space of a particular system to get a visual representation of the spread of phase-keys for the system and so assess it's security from a key-space perspective.

Keywords: Optical Encryption, Digital Holography, Optical Signal Processing

1. INTRODUCTION

Major technological advances in both computer technology and global communications have occurred in the last 50 years. Cryptography[1,2,3,4] and information security have been recognised as an important fields by governments and armies throughout history. In the digital information age access to powerful computers brings with it an increased demand for information security. With this demand for secure communication, faster and more powerful encryption systems are being continually developed. Optical encryption[5,6,7,8,9,10] is such a system. Optical encryption is a particularly interesting method of encryption as it offers the possibility of high-speed parallel encryption of image data. Newly available low cost technology such as high quality spatial light modulators (SLMs), high resolution digital cameras (CCDs) and powerful desktop computers have made optical encryption physically realisable One such method of optical encryption is Double Random Phase Encoding[5] (DRPE).

DRPE was originally proposed by Refregier and Javidi[5] in 1995 and is a unique method of optically encoding an image, (see figure 1). The primary input image, X, is encoded to stationary white noise by the use of two statistically independent random phase keys and two Fourier transforms. One key is placed in the input domain and the other key is placed in the Fourier domain, (see figure 2 for an optical implementation of DRPE). The method can be numerically simulated by means of matrices of discrete values and the fast Fourier transform (FFT). In our study we are concerned only with the intensity of the output image. Therefore in this encryption system the random key located at the Fourier plane serves as the only decryption key to the system. Since only the output intensity is required the output phase can be discarded.

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

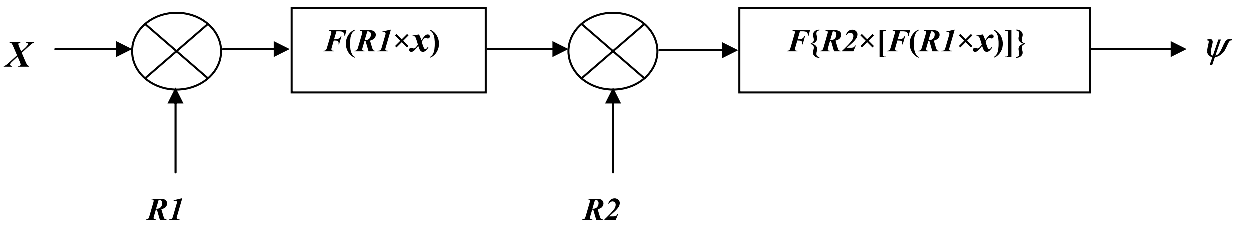


Figure 1. Double Random Phase Encoding.

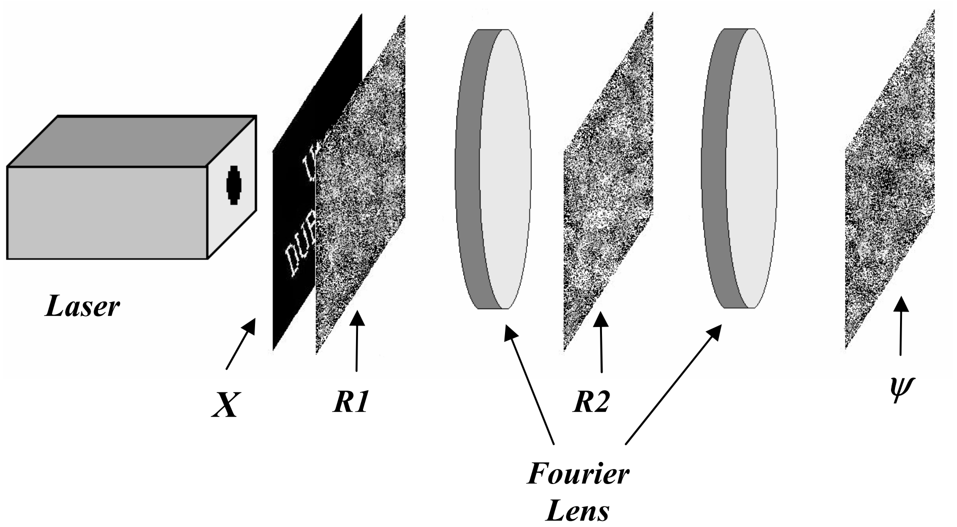


Figure 2. Schematic of a possible optical implementation of Double Random Phase Encoding.

In a physical implementation of this optical encryption system it is necessary to capture the full field information, amplitude and phase. This introduces a problem. Charged coupled device (CCD) cameras can only capture the intensity of a wave field so digital holographic[11,6,12,13] techniques need to be employed to extract a representation of the complex wave field. These digital holographic techniques may involve the inclusion of a reference beam which is interfered with the information beam, or object beam, and the resulting interference fringes are created and captured in the plane of the CCD camera. Phase retrieval techniques[14,15] are then used to recover a representation of the phase.

Although this encryption system is an optical operation such systems have been implemented numerically in a computer. The analysis of the system under study in this paper was carried out numerically.

An algorithm's key-space is a set of all the possible keys that can be used to initialise that algorithm. For instance, a simple combination lock with three dials, each with ten digits, has a key-space of one thousand keys. The number of possible combinations that can be tried on an encryption system is the size of the key-space and the key that decrypts or open the system must lie in that key-space. In an ideal encryption algorithm only one key would decrypt the encoded message and every other key would give an error of 100%, i.e. the decryption would contain no useful information and be completely uncorrelated from the input image. However, this is not the case with the DRPE algorithm. As we show in our results there are typically several keys which will decrypt the encoded message to error levels as low as 10%.

We represent the algorithm's key-space as a histogram in terms of the number of keys which decrypt an encoded message to given error levels. An analysis on the key-space for large image systems is computationally insurmountable due to the large number of keys in the key-space. We therefore carry out our analysis for small input images and extrapolate our results for larger input images, under certain assumed conditions. By mapping the decrypting error across the entire key-space we can provide an analysis of the strength of the optical encryption algorithm.

Whereas a review of the different existing optical encryption method has been carried out in the past[16], to date, to the best of our knowledge, no one has carried out this type of key-space analysis of the DRPE algorithm. This type of analysis may have been neglected as impractical due to the size of the key-space involved. For instance, a random phase key with 4 quantisation levels between 0 to 2π and 10×10 pixels has 1.6×10^{60} unique solutions. For large dimensions the sheer volume of phase keys would imply that the key-space would appear infinite and checking every key would be an improbability. However, by performing this analysis for small phase keys, with pixel sizes such as 2×2, 3×3, 4×4 and 5×5 we hope to identify certain trends in key space which, if consistent across all experiments, might reasonably be assumed to be consistent in larger random key-spaces. Using this knowledge we may be able to limit our search of the key space when trying to break this encryption system.

Our analysis is based on the key-space of the encryption system. The key to the system is the phase-masks needed to decrypt the system. In this system our key is the phase-mask ***R2*** the phase key in the Fourier plane, see figure 1, as it is the only phase-mask of interest to us. We are only interested in ***R2*** because we required the output intensity of the image and whereas ***R1*** is necessary to encrypt the original image it is not necessary to decrypt the image because the output amplitude to the system is simply squared to find the intensity and the phase associated with ***R1*** is lost. Therefore the number of keys in the key-space is determined by the resolution of the phase key, ***R2***.

The resolution is made up of:

1) The key dimensions in pixels and

2) The number of phase quantisation levels used in the phase key i.e. a system with a phase key that has a resolution of $N\times M$ pixels with Q quantisation levels has a key space with $Q^{(N\times M)}$ unique keys.

2. ERROR ANALYSIS

In our analysis the encryption/decryption process is performed numerically. This set-up utilises the Fast Fourier Transform (FFT) algorithm and each pixel is represented by a single complex value in the computer. This would assume a 100% fill factor on the discrete virtual optical elements which otherwise could not be realised using conventional SLMs. This assumption can be tolerated beings as it is the nature of the DRPE algorithm under study here and not the non-ideality introduced by the physical limitations of SLMs.

The Error that we use to quantify the decrypting ability of a certain phase-mask is the normalised root mean squared (NRMS) error. The error, NRMS, in the decrypted image is calculated using the following equation:

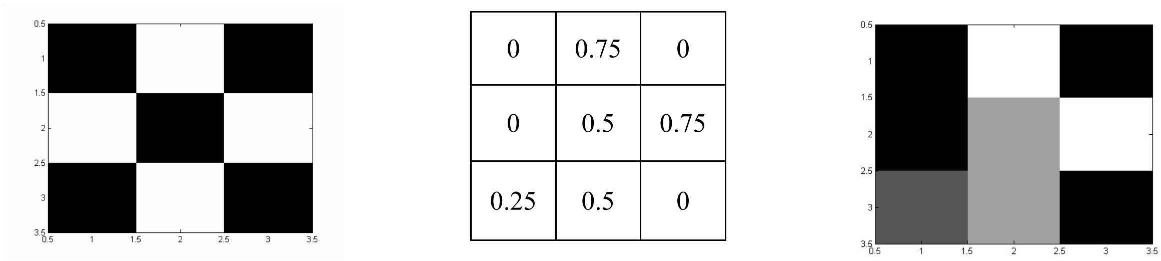
$$r=\left(\sum_{i=1}^{N}\sum_{j=1}^{N}\left|I_d(i,j)-I(i,j)\right|^2\right)^{1/2}\left(\sum_{i=1}^{N}\sum_{j=1}^{N}\left|I(i,j)\right|^2\right)^{-1/2} \tag{1}$$

where $I_d(.)$ and $I(.)$ are the intensities of the decrypted and original images, respectively.

3. RESULTS

The following test was carried out using a 3×3 image with four quantisation levels. Therefore there are 262,144 possible unique phase-masks in the key-space for this system. The possible values for the phase mask levels are 2π × [0, 0.25, 0.5, 0.75]. It should be note that 0 and 1 or 0 and 2π correspond to the same value.

In this study we are concerned only with the intensity of the output image and therefore the phase mask ***R1*** is not necessary for decryption as at the output the image is squared and the phase information is lost. The original image is encrypted by a random chosen phase-mask from the key-space and is subsequently decrypted by every possible phase-mask and the NRMS error associated with each phase-mask is recorded. Figure 3 shows the original image and ***R2***.



0	0.75	0
0	0.5	0.75
0.25	0.5	0

(a) (b) (c)

Figure 3. Original image (a) is a binary real image, (b) R2 values which are multiplied by 2π and (c) a graphical representation of R2.

The system was decrypted using every single phase-key in the key-space and the error of the decrypted output image was recorded. Figure 4 shows the NRMS error for the entire key-space of this system. As we move along the x-axis of the graph we are trying different phase-keys and logging the error that each of these keys produces. As is indicated by the four circles there are exactly four phase-masks which perfectly decrypt the encrypted image. There are many phase-keys that decrypt the image to an error under 0.2.

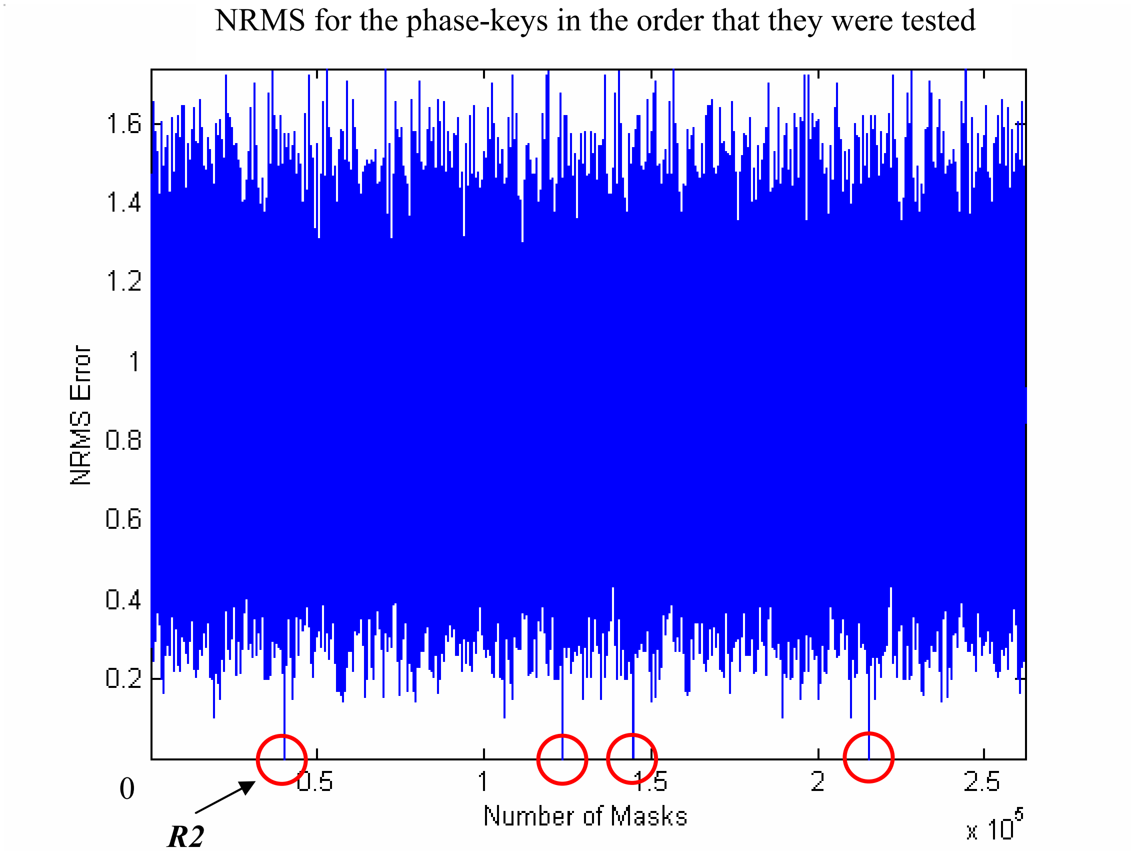
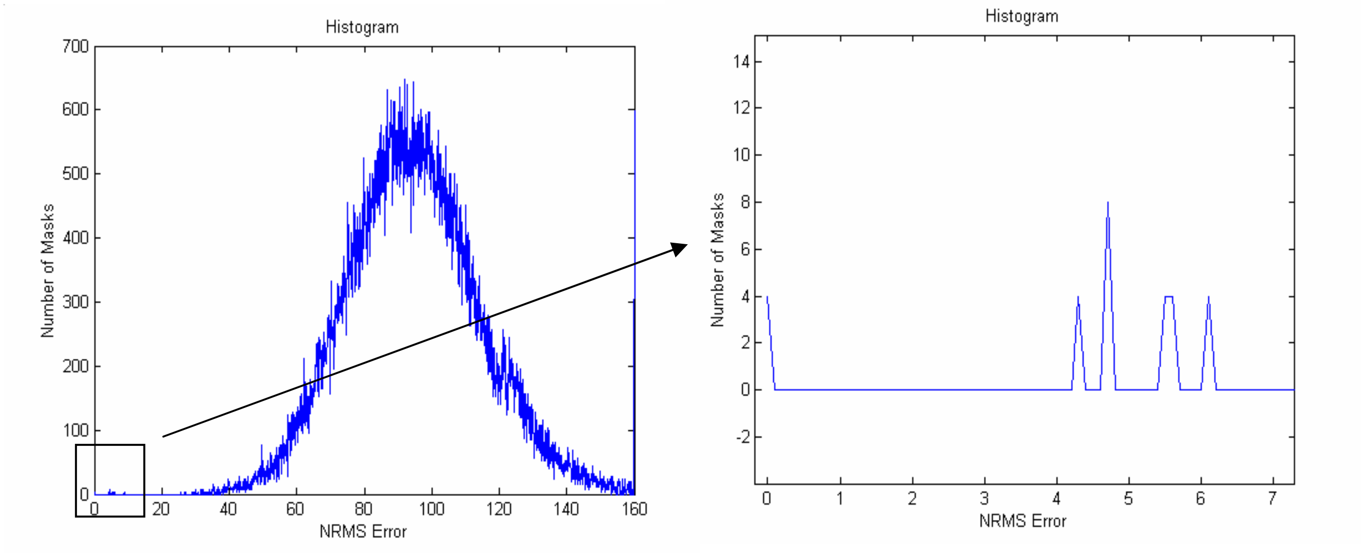


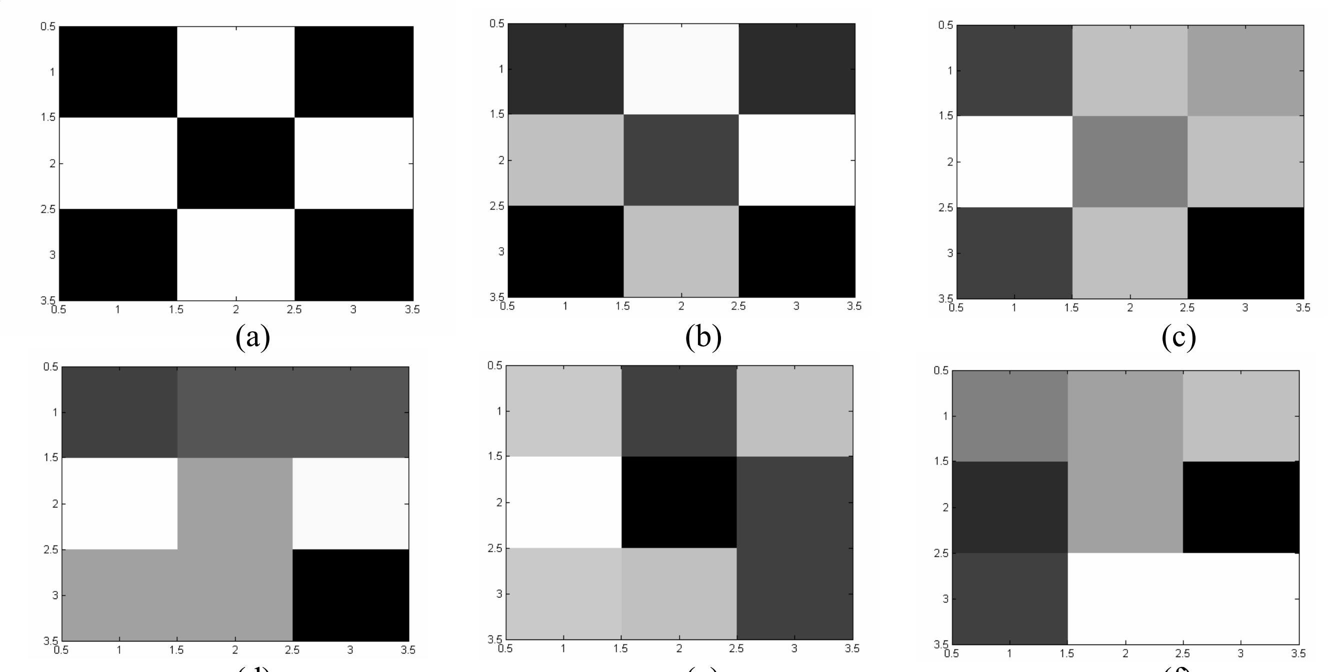
Figure 4. The error produced by each phase-key when used to decrypt the system.

Figure 5 is a histogram with the same information as figure 4 however it is easier to see the spread of phase-keys. The system under study uses four quantisation levels in it's phase-key and it has subsequently been observed that it has four phase-keys that perfectly decrypt it. One of these four keys is ***R2*** and the others are found to be a variation of ***R2***, where the relative phase shift between each individual pixel of the phase-key remains the same as ***R2***. The three other masks are ***R2*** plus a phase shift and that phase shift is equal to that of the quantisation shift, i.e. 90 (see Figure 6) because there are four quantisation levels and four 90 shifts gives us a full 360 revolution. This situation arises due to the fact that we are not interested in ***R1*** in the decryption process or the output phase and only the output intensity. Figure 7 shows the four phase-keys that perfectly decrypt the system.



(a) (b)

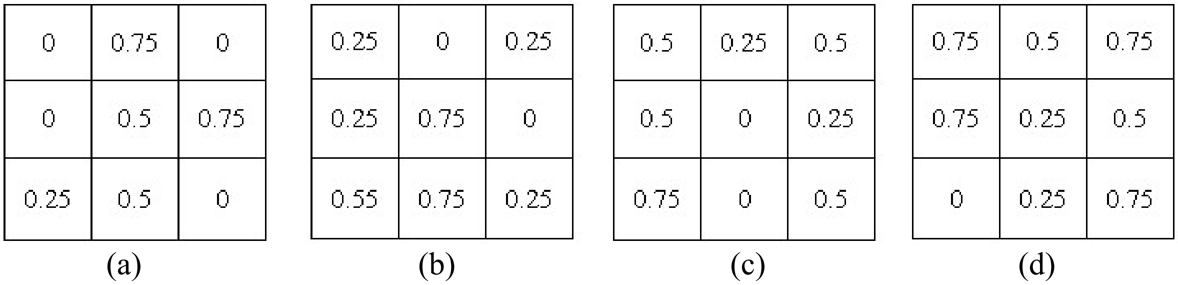
Figure 5. (a) A histogram of the NRMS error associated with every phase-mask in key-space which shows the number of phase-masks that decrypt to a certain error. (b) A zoomed in plot of (a) near the origin which shows that there are four phase-masks which achieve an error of almost zero.



(a) (b) (c)

(d) (e) (f)

Figure 6. Shows the decrypted image at (a) 0% error, (b) 20%, (c) 40%, (d) 60%, (e) 80% and (f) 100% error.



0	0.75	0
0	0.5	0.75
0.25	0.5	0

(a)

0.25	0	0.25
0.25	0.75	0
0.55	0.75	0.25

(b)

0.5	0.25	0.5
0.5	0	0.25
0.75	0	0.5

(c)

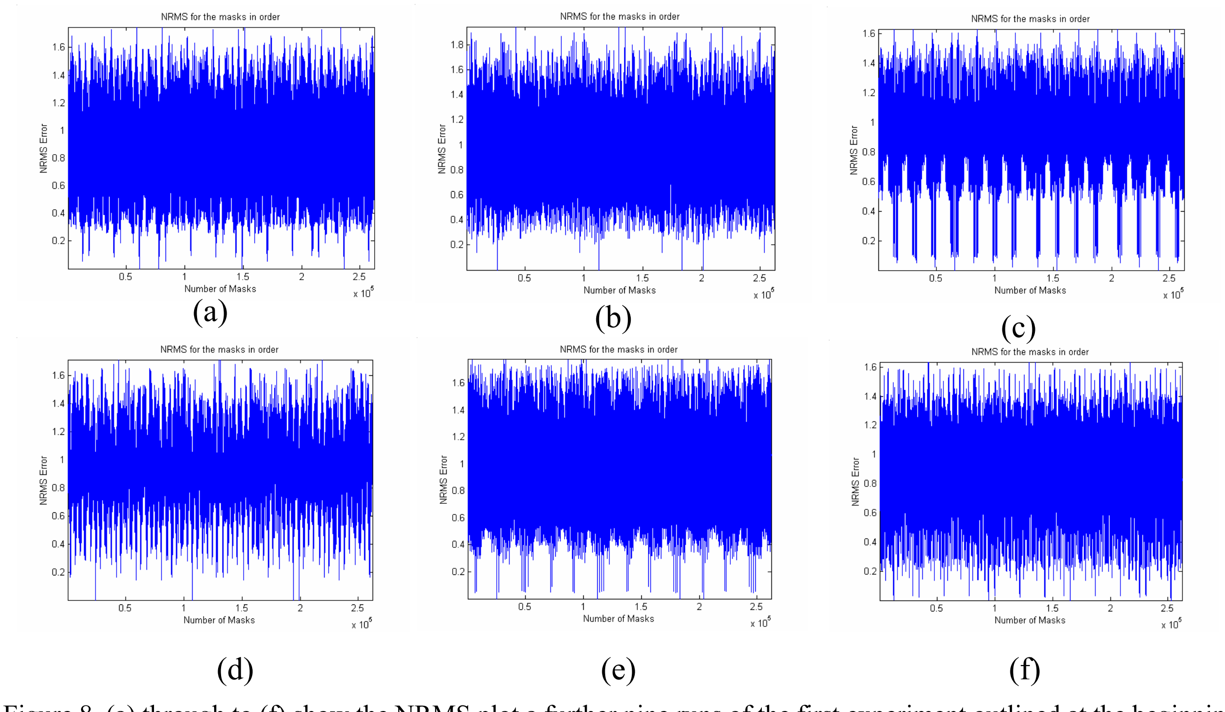
0.75	0.5	0.75
0.75	0.25	0.5
0	0.25	0.75

(d)

Figure 7. (a) is the phase-mask R2 which was used to encrypt the original image and so stand to reason that it will also decrypt the encrypted image. (b) is R2 plus 90 , (c) is R2 plus 180 and (d) is R2 plus 270

The fact that there are four phase-keys that decrypt the system makes logical sense beings as we are only looking for the intensity of the image, the relative phase of the pixels is the only thing that matters. Therefore in a system with 256 quantisation levels there are 256 masks that can perfectly decrypt the system.

Figure 8 shows the NRMS plot for a further six runs for the same input image. R2 is randomly generated at the start of every experiment so is different in each run. Each run consistently gave four correct masks.



(a)

(b)

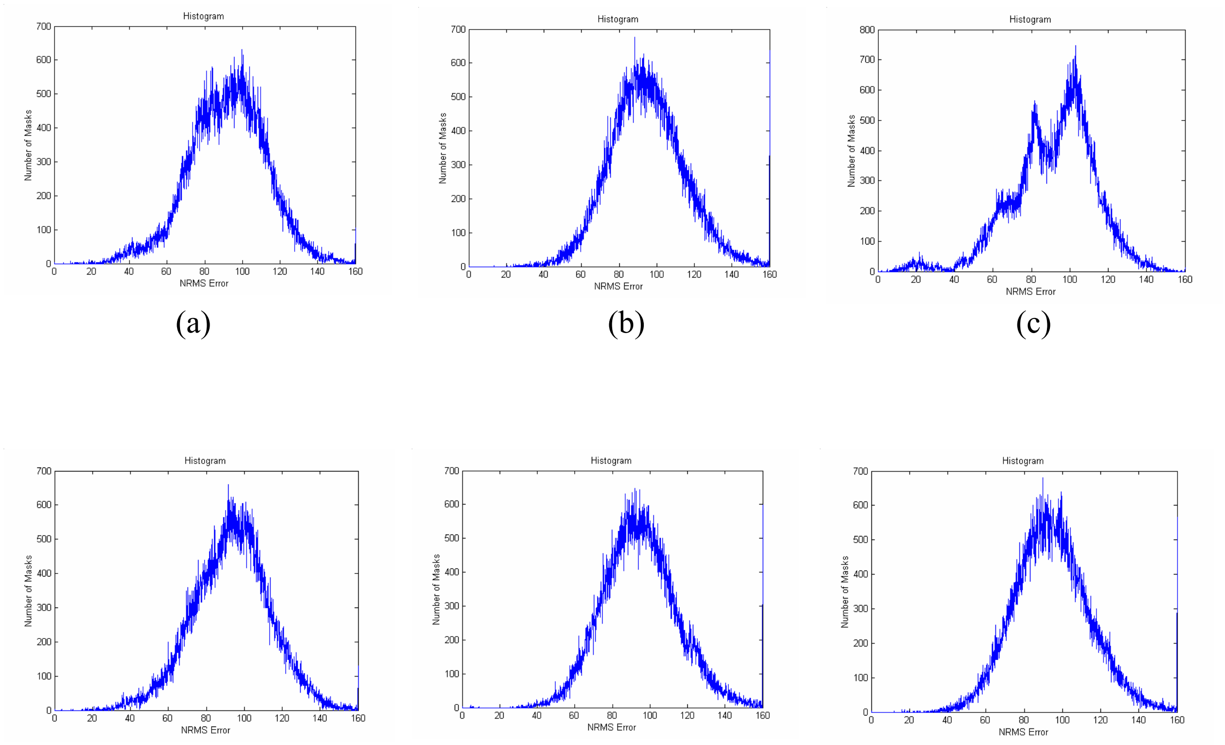
(c)

(d)

(e)

(f)

Figure 8. (a) through to (f) show the NRMS plot a further nine runs of the first experiment outlined at the beginning of Section 3.



(a) (b) (c)

Figure 9. (a) through to (f) shows the histogram of the NRMS plots for the nine runs of Figure 8.

All of the above results in figures 8 and 9 correspond to the original result discussed except for Figure 8 & 9 (c). In this experiment the phase key used is a 3 × 3 pixel sized image and this is too small to be considered as random as truly random because there are only nine pixels in the mask. We extended the experiments to bigger mask and repeated all tests for phase-keys which were 4 × 4 and 5 × 5 pixels in size with two levels of quantisation. Even with the increase in the size of the key-space, from 262,144 to 33,554,432 phase-keys for a 3 × 3 key with four quantisation levels to a 5 × 5 key with two quantisation, the observed trends seen in the results remained consistent.

4. CONCLUSION

Although it was observed that a system with 256 quantisation levels will have 256 phase-keys that perfectly decrypt the system, it should be noted that because the size of the key-space is dependant on the number of quantisation levels, i.e. from the end of section 1 $Q^{(N\times M)}$ where Q is the number of quantisation levels, an increased number of quantisation levels will produce a much larger key-space. So it is infact advantageous to the security of the system to have more quantisation levels.

The optical encryption system has the majority of its phase-keys centred at about 95% error. For larger masks, > 128×128 pixels, the size of key-space is so larger that any brut force method of mapping the entire key-space is unrealistic with today's computers. Although there exists certain techniques which can find a phase-key that produces low errors such as 10%[17] from a key-space standpoint the encryption system is a strong one.

ACKNOWLEDGEMENTS

We acknowledge the support of Enterprise Ireland and Science Foundation Ireland through the Research Innovation, Fund, Proof of Concept Fund, the Basic Research Program and the Research Frontiers Program and of the Irish Research Council for Science, Engineering and Technology.

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 T.I.T., **22,** 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,** 1995
6. E.Tajahuerce and B.Javidi, "Encrypting three-dimensional information with digital holography", Appl. Opt., **39,** 2000
7. B.Hennelly and J.T.Sheridan, "Optical image encryption by random shifting in fractional Fourier domains", Opt. Lett., **28,** 2003
8. B.M.Hennelly and J.T.Sheridan, "Optical encryption and the space bandwidth product", Opt. Comm., **247,** 2005
9. L.E.M.Brackenbury and K.M.Bell, "Optical encryption of digital data", Appl. Opt., **39,** 2000
10. G.Unnikrishnan, J.Joseph, and K.Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain", Opt. Lett., **25,** 2000
11. J.W.Goodman and R.W.Lawrence, "Digital Image Formation from Electronically Detected Holograms", Appl. Phys. Lett., **11,** 1967
12. U.Schnars and W.Juptner, "Direct Recording of Holograms by A CCD Target and Numerical Reconstruction", Appl. Opt., **33,** 1994
13. B.H.Zhu, H.F.Zhao, and S.T.Liu, "Image encryption based on pure intensity random coding and digital holography technique", Optik, **114,** 2003
14. M.Liebling, T.Blu, and M.Unser, "Complex-wave retrieval from a single off-axis hologram", JOSA A, **21,** 2004
15. J.R.Fienup, "Phase Retrieval Algorithms - A Comparison", Appl. Opt., **21,** 1982
16. B.M.Hennelly and J.T.Sheridan, "Random phase and jigsaw encryption in the Fresnel domain", Opt. Eng., **43,** 2004
17. 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,** 2006