Numerical analysis of systematic errors in an optical encryption system

David S. Monaghan [a], Unnikrishnan Gopinathan [a], Damien P. Kelly [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 Encryption/Decryption system in which the image encryption/decryption process is performed numerically. In this paper we look at the effect of quantisation in the decryption process due to the discrete values which a spatial light modulator can display. We look at the characterisation of a transmissive spatial light modulator and we present results from simulations of the system.

Keywords: Optical Encryption, Digital Holography, Optical Signal Processing

1. INTRODUCTION

Recent technological advances, such as high quality spatial light modulators (SLMs), high resolution digital cameras and powerful desktop computers, coupled with the overwhelming advantage of high through-put and computational speed of optical processing systems, due to their inherent parallel nature, have stimulated increased interest in the field of information security by means of optical encryption. Optical Encryption[1,2] offers the possibility of high-speed parallel encryption of image data. Such Encryption can involve the capture of full field information, amplitude and phase. Since holograms are intrinsically three dimensional (3D), a hologram is an attractive way to represent 3D information. Digital holographic techniques[3,4,5,6] are employed to allow pre- and post- digital signal processing of the wave front. When in digital form, these holograms can be easily stored, transmitted, processed and analysed. Digital compression techniques have been used to enable efficient storage and transmission of encrypted holographic data over digital communication channels[7,8].

In the decryption process, it is usual for the complex-valued encrypted image to be physically displayed on one or more SLMs and then propagated through the decryption system. To date, there have been numerous systems of this type proposed in the literature however there has been relatively little experimental evaluation of the practical performance of SLMs in Encryption/Decryption systems.

Lohmann[9] has shown that the Space-Bandwidth Product (SBP) of the signal propagating through an optical system can not exceed the SBP of the optical system. Wigner Transform has been used to track the SBP of an optical signal propagating through an optical system[10]. There are many factors that affect the SBP of the optical system. These include: (1) the finite aperture of the elements like lenses, SLM, CCD cameras and other elements; (2) the pixel size and fill factor of discrete devices like SLMs and CCD cameras; (3) quantisation effects of discrete devices like SLMs and CCD cameras. These errors can be classified as systematic noise in the optical system as opposed to random noise due to internal noise of SLMs, detector noise, laser light fluctuations etc.

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

There are advantages of performing encryption using coherent optical signal processors are due to their ability to process and relay information in two dimensions, and the inherent parallel nature of optics. The majority of these systems involve a coherent field propagated through some bulk optical system consisting of thin lenses and sections of free space. Such paraxial Quadratic Phase Systems (QPS) can be described mathematically using the Linear Canonical Transformation[10]. These systems often incorporate a Spatial Light Modulator (SLM), such as liquid crystal displays, which may be used to modulate the input digital data onto a coherent wave-field as well as to modulate the amplitude and/or phase of the complex wave-field at any desired plane. Therefore, in the 2D and 3D case, SLMs can be used to encode the inputs and can be used as part of an optical reconstruction technique and can also represent the key during encryption and decryption.

Double random phase encoding, as proposed by Refregier and Javidi[11] in 1995, is a unique method of optically encrypting a primary image to stationary white noise by use of two statistically independent random phase keys. One in the input domain and one in the Fourier domain. In this encryption system the random key located at the Fourier plane serves as the only key. The method can be numerically simulated by means of matrices of discrete values and the Fast Fourier Transform (FFT). Figure 1 show an optical implementation of a double random phase encoding system.

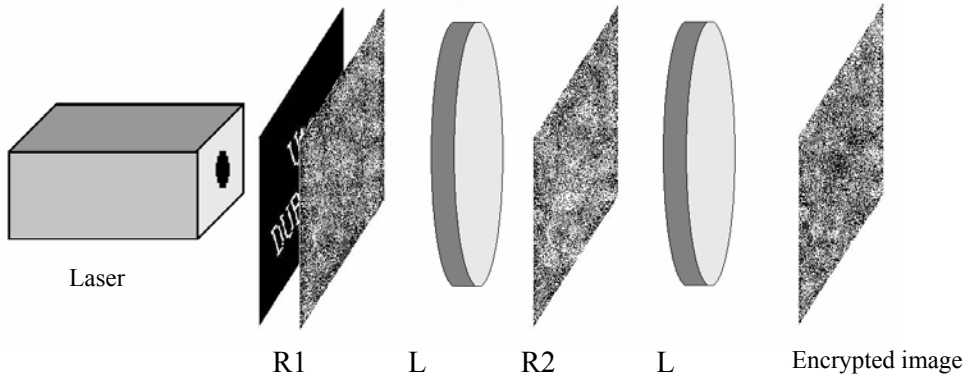

Figure 1. An optical implementation of double random phase encoding. R1 is the random phase mask in the input domain, R2 is the random phase mask in the Fourier domain and L are lenses.

To decrypt the image you would simply reverse the setup and capture the intensity at the output. When implementing the double random phase encoding algorithm numerically on a computer the complex values can easily be stored. The representation of complex numbers in an optical implementation is a more complicated problem. Spatial Light Modulators (SLMs) are employed to solve such problems. SLMs can operate in amplitude mode or in phase mode and some of them have a coupled mode, however on most SLMs there is no independent control of the amplitude and phase and this presents an obstacle when trying to code complex numbers to SLMs. Cohn[12] and Duelli[13] have devised a method of using pseudorandom encoding as a method of statistically approximating desired complex values with those values that are achievable with a given spatial light modulator. The method was originally developed for phase-only SLMs but has been extended to SLMs for which amplitude is a function of phase.

This paper is organised as follows: In Section 2 we discuss the characterisation of our SLM, which is a Holoeye[16] LC2002. In Section 3 we discuss our application of the pseudorandom encoding algorithm. In Section 4 we explain our decryption setup. In Section 5 we present the results from our numerical simulations and in Section 6 we conclude. References are listed in Section 7.

2. SLM Characterisation

In any physical optical system the polarisation of a light beam can be described by it's corresponding Jones vector and any linear optical element can be described by it's corresponding Jones matrix[14]. Jones calculus was invented by American physicist R. Clark Jones in 1941 and is an extremely useful tool for representing optical systems in terms of the polarisation of light and the effect that linear optical element have on the polarisation state. Beings as the Jones vectors are only applicable to polarised waves the most sensible way to represent the beam is in terms of the electric vector:

$$\vec{E} = \begin{bmatrix} E_x(t) \\ E_y(t) \end{bmatrix} \tag{1}$$

where $E_x(t)$ and $E_y(t)$ are the instantaneous scalar components of $\vec{E}$.

Therefore it stands to reason that if we know $\vec{E}$ that we know everything about the polarisation state. The Jones vector of a beam can also be written in complex form:

$$\tilde{E} = \begin{bmatrix} E_{0x}e^{i\varphi x} \\ E_{0y}e^{i\varphi y} \end{bmatrix} \tag{2}$$

where φx and φy represent the phase. The Jones vector of a beam is made up of two elements, an *x*-component and a *y*-component. Therefore horizontal and vertical polarisation states are thus given by:

$$\tilde{E}_h = \begin{bmatrix} E_{0x}e^{i\varphi x} \\ 0 \end{bmatrix} \text{ and } \tilde{E}_v = \begin{bmatrix} 0 \\ E_{0y}e^{i\varphi y} \end{bmatrix} \tag{3}$$

Suppose we have a linear polarised incident beam, represented by it's Jones Vector, which passes through an optical element and emerges as a new vector. The optical element has transformed the original vector into a new vector by a process that can be described mathematically using a 2×2 ABCD matrix. A single cell transmissive SLM acts as a linear optical element if a constant gray level is displayed on it. A SLM with many pixels acts in the same way as long as all the pixels are set to the same constant gray level and a 100% fill factor is assumed. By calculating the SLMs corresponding Jones matrix for each gray level we can completely characterise the device. We carried out two experiments to characterise the SLM, one to determine the amplitude and one to determine the phase. The first experiment was to determine the amplitude characteristics of the SLM:

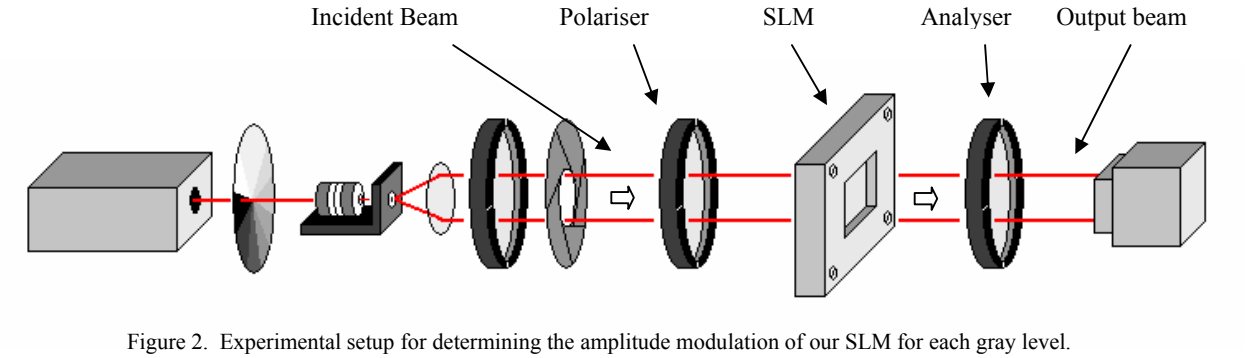

Figure 2. Experimental setup for determining the amplitude modulation of our SLM for each gray level.

The Jones vector that corresponds to the incident beam can be written by:

$$\begin{bmatrix} \sqrt{I}/\sqrt{2} \\ \sqrt{I}/\sqrt{2} \end{bmatrix} = \begin{bmatrix} \sqrt{I_0} \\ \sqrt{I_{90}} \end{bmatrix} \tag{4}$$

where I is the intensity and the current polarisation of the light beam is 45˚. The Jones Matrix corresponding to a polariser is:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} or \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \tag{5}$$

for a polariser set at 0˚ or 90˚. Therefore the Jones vector for the output beam, when the polariser and the analyser are set to 0˚, is given by:

$$\begin{bmatrix} A\sqrt{I_0} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} A & B \\ C & D \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} \sqrt{I_0} \\ \sqrt{I_{90}} \end{bmatrix} \tag{6}$$

By measuring the intensity of the output beam for the four combinations of the polariser and the analyser being set to either 0˚ or 90˚ we can fully determine the ABCD matrix corresponding to the SLM for amplitude modulation of the device for each gray level using the following formulae:

$$\begin{bmatrix} A\sqrt{I_0} \\ 0 \end{bmatrix} \rightarrow |A|^2 I_0 = I_{measured} \quad \Rightarrow \quad |A| = \sqrt{\frac{I_{measured}}{I_0}} \tag{7a, b}$$

To measure the phase modulation of the SLM we make use of a digital holography setup and capture a digital hologram with a CCD camera. The second experiment was to determine the phase characteristics of the SLM:

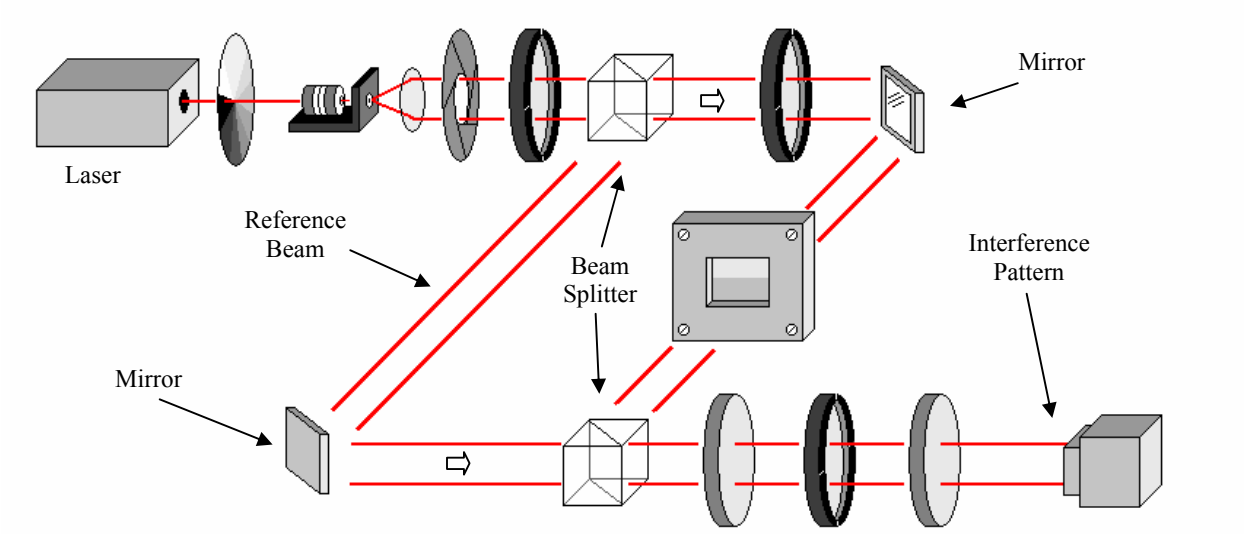

Figure 3. Experimental setup for determining the phase modulation of our SLM for each gray level.

Therefore by measuring the relative phase shift of the recorded interference fringes for the four different combinations of the polariser and the analyser (i.e. each being set to either 0˚ or 90˚), we can fully determine the ABCD matrix corresponding to the SLM for phase modulation of the device for each gray level. The Polariser/Analyser combinations of 0˚/0˚, 90˚/0˚, 90˚/90˚ and 0˚/90˚ correspond to ϕ_1, ϕ_2, ϕ_3 and ϕ_4 which then give us:

$$\begin{bmatrix} |A|\angle\phi_1 & |B|\angle\phi_2 \\ |C|\angle\phi_3 & |D|\angle\phi_4 \end{bmatrix} \tag{8}$$

The SLM is now fully characterised. The next problem is to map complex numbers on the computer to complex numbers that the SLM can represent.

3. Pseudorandom Encoding (PE)

The SLM, which works in a coupled phase/amplitude mode, can only achieve certain complex numbers which can be determined by characterising the SLM. Due to the fact that our encrypted image and decrypting phase mask, which we want to display on the SLM, are both complex images spread randomly from 0 to 2π and have normalised amplitude we need to map there complex values to complex values that the SLM can achieve. To do this we employ a technique called PE[12,13,15]. PE is a statistical method of approximating a required complex value using those complex values that are achievable on a SLM. A very simple explanation of the pseudorandom encoding algorithm is as follows:

Figure 4 represents a complex number in polar form, where the distance from the origin represents the amplitude or real component and the tilt or angle of the vector represents the phase or imaginary component. Let a_c be the complex value that we require and M_1 and M_2 be the modes achievable on a given SLM.

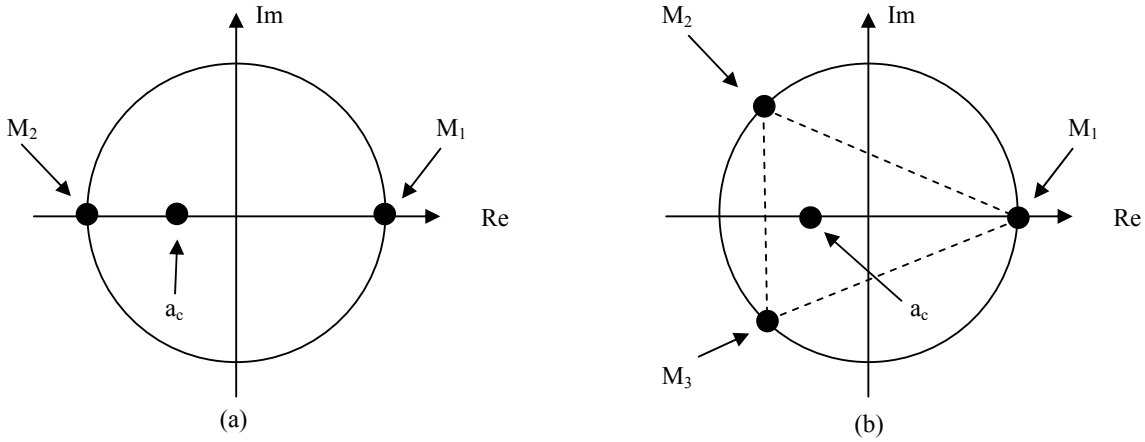

Figure 4. Polar plots displaying required and achievable complex modes.

A simple minimum distance algorithm would map the state a_c to M_2 every time. In the PE algorithm a probability is given to each to the distance from a_c to each of the SLM modes, in this simple example there are only two modes. Let us say that a probability of 0.7 is associated for the distance between a_c and M_2 and a probability of 0.3 is associated with the distance between a_c and M_1. Therefore each value at a_c is mapped to one of the SLM modes with the given probabilities. The PE design[12] finds a value of the ensemble average of a random variable, a, such that $\langle a \rangle = a_c$. Due to the fact that this is a statistical method the more values that we require which are at a_c the more accurate the algorithm becomes.

In relation to our problem we select three modes. Therefore determining the probability associated with each distance becomes more complicated albeit straightforward. The three states form a triangle and any required complex values inside the triangle can be mapped to one of the SLM states. Any values that fall outside the triangle will firstly get translated to the nearest point on the triangle so as to avoid a negative probability. For Figure 4b there will be three probabilities:

$$P_1 + P_2 + P_3 = 1 \tag{9}$$

therefore this implies that a_c will be given by:

$$a_c = P_1 a_{M_1} + P_2 a_{M_2} + P_3 a_{M_3} \tag{10}$$

where a_{M_n} is a value, a, at a state, M_n. Extrapolating Eqn (2) for the real and imaginary parts gives us:

$$\mathrm{Re}[a_c] = P_1 \mathrm{Re}[a_{M_1}] + P_2 \mathrm{Re}[a_{M_2}] + P_3 \mathrm{Re}[a_{M_3}] \tag{11}$$

and

$$\mathrm{Im}[a_c] = P_1 \mathrm{Im}[a_{M_1}] + P_2 \mathrm{Im}[a_{M_2}] + P_3 \mathrm{Im}[a_{M_3}] \tag{12}$$

By using Eqns (9), (11) and (12) as simultaneous equations:

$$\begin{bmatrix} \mathrm{Re}[a_c] \\ \mathrm{Im}[a_c] \\ 1 \end{bmatrix} = \begin{bmatrix} \mathrm{Re}[a_{M_1}] & \mathrm{Re}[a_{M_2}] & \mathrm{Re}[a_{M_3}] \\ \mathrm{Im}[a_{M_1}] & \mathrm{Im}[a_{M_2}] & \mathrm{Im}[a_{M_3}] \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \tag{13}$$

and by simple matrix algebra we can work out the probabilities P_1, P_2 and P_3. Figure 5 shows the achievable modes of the SLM and the three selected modes which we map the complex value to.

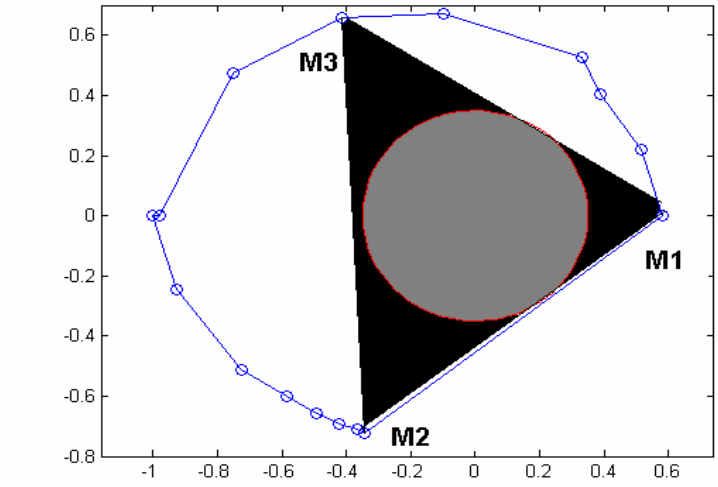

Figure 5. Shows the modulation states of the SLM used for the present study, denoted by the small circles. The states M1, M2 and M3 are used to encode the complex valued data. The shaded region in dark shows the encoding range of SLM. The inner circle shows the fully complex encoding range.

Figure 6 shows the extension to four modes in which two triangular regions are established.

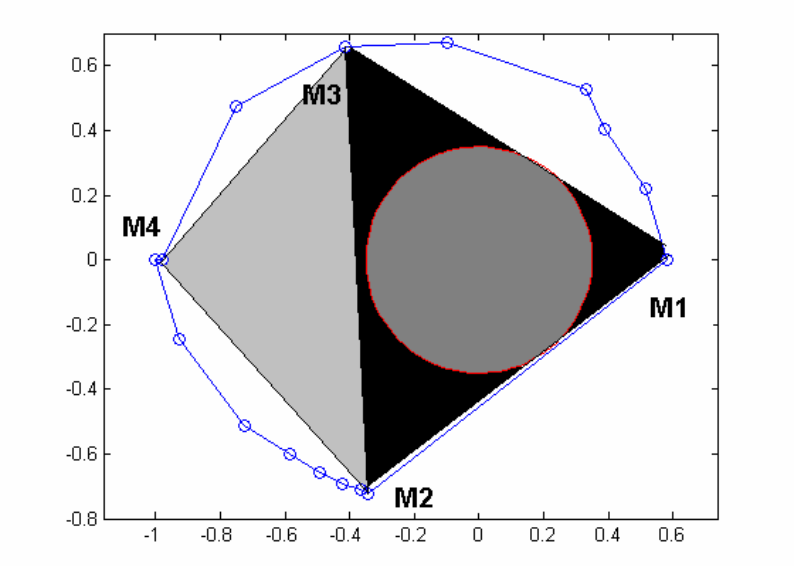

Figure 6. Shows the modulation states of the SLM used for the present study. The states M1, M2, M3and M4 are used to encode the complex valued data. The two triangular shaded regions show the two encoding regions of the SLM.

4. The Decryption Set-up

In the decryption process for double random phase encoding two Fourier transforms are required, however to simplify the optical implementation we have done the first Fourier transform numerically. This first Fourier transform is an unambiguous step as no knowledge of the decrypting phase key is required. By using two transmissive SLMs, imaged into one another by means of an imaging system, operating in a phase only mode we display the Fourier transform of the encrypted image on SLM1 and the decryption mask on SLM2. The complex images are mapped to the SLMs by employing Cohn's method of pseudorandom encoding. The second Fourier transform is carried out by mean of free space and a Lens and the intensity of the wave front is then capture by a CCD camera, beings as we are concerned with images the intensity of the wave front is all we required to recover the image.

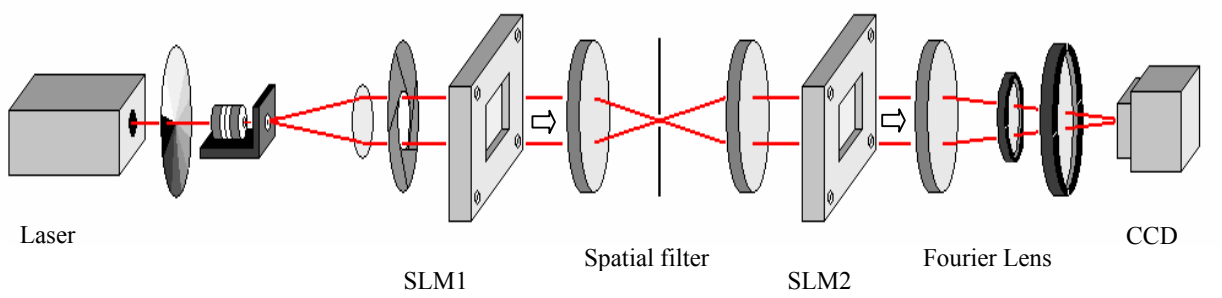

Figure 7. Shows the experimental optical decryption set-up.

A spatial filter is placed in between the two SLMs so as to cut out the higher order terms introduced by SLM1.

5. Results

We studied the effect of quantisation in the decryption process due to the discrete values which an SLM can display. The encrypted image and the random key are continuous complex valued. When an encrypted image and random key is displayed on a discrete valued SLM that can display only a finite number of values, this results in error in the decryption process. Therefore we use an algorithm[12,13] that maps complex valued data to the modulation states which an SLM can produce.

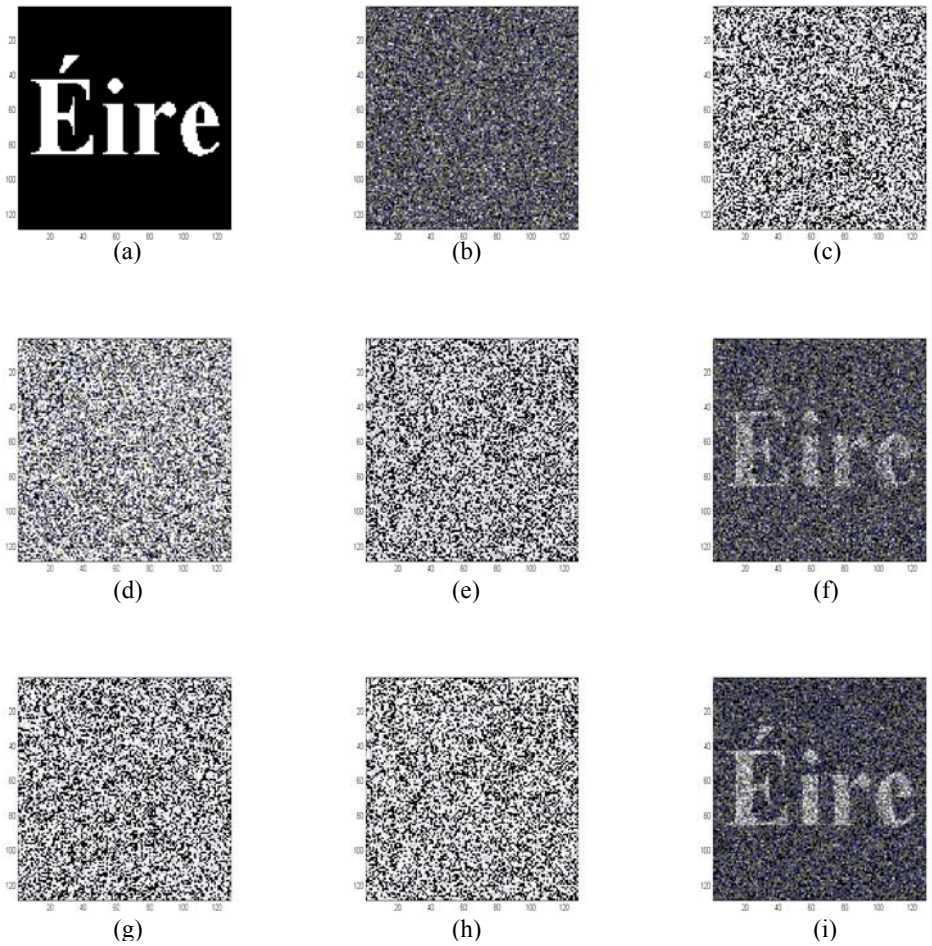

Figure 8. (a) Original image; (b) Encrypted image; (c) encrypted image as represented on SLM with three quantised levels; (d) Random phase mask; (e) Random phase mask as represented on SLM with three quantised levels; (f) Decrypted image with three quantised levels; (g) encrypted image as represented on SLM with four quantised levels; (h) Random phase mask as represented on SLM with four quantised levels; (i) Decrypted image with four quantised levels.

6. Conclusions

In this paper we looked at the effect of quantisation in the decryption process due to the discrete values which a spatial light modulator can display. We characterised the modulation states of an SLM. The fully complex valued encrypted image and phase mask is quantised to the modulation states of an SLM. We have studies the effects of quantisation with three and four SLM states in the decryption process by quantifying the error in the decryption process. We have presented results from computer simulation.

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.Unnikrishnan, J.Joseph, and K.Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain", Opt. Lett., **25,** 2000
2. B.Hennelly and J.T.Sheridan, "Optical image encryption by random shifting in fractional Fourier domains", Opt. Lett., **28,** 2003
3. J.W.Goodman and R.W.Lawrence, "Digital Image Formation from Electronically Detected Holograms", Appl. Phys. Lett., **11,** 1967
4. J.H.Bruning, D.R.Herriott, J.E.Gallaghe, D.P.Rosenfel, A.D.White, and D.J.Brangacc, "Digital Wavefront Measuring Interferometer for Testing Optical Surfaces and Lenses", Appl. Opt., **13,** 1974
5. U.Schnars and W.Juptner, "Direct Recording of Holograms by A CCD Target and Numerical Reconstruction", Appl. Opt., **33,** 1994
6. L.Onural and P.D.Scott, "Digital Decoding of In-Line Holograms", Opt. Eng., **26,** 1987
7. T.J.Naughton and B.Javidi, "Compression of encrypted three-dimensional objects using digital holography", Opt. Eng., **43,** 2004
8. T.J.Naughton, Y.Frauel, B.Javidi, and E.Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition", Appl. Opt., **41,** 2002
9. A.W.Lohmann, R.G.Dorsch, D.Mendlovic, Z.Zalevsky, and C.Ferreira, "Space-bandwidth product of optical signals and systems", JOSA A, **13,** 1996
10. B.M.Hennelly and J.T.Sheridan, "Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms", JOSA A, **22,** 2005
11. P.Refregier and B.Javidi, "Optical-Image Encryption Based on Input Plane and Fourier Plane Random Encoding", Opt. Lett., **20,** 1-4-1995
12. R.W.Cohn, "Pseudorandom encoding of complex-valued functions onto amplitude-coupled phase modulators", JOSA A, **15,** 1998
13. M.Duelli, M.Reece, and R.W.Cohn, "Modified minimum-distance criterion for blended random and nonrandom encoding", JOSA A, **16,** 1999
14. E.Hecht and A.Zajac, "Optics", Addison-Wesley Publishing company1980
15. R.W.Cohn and M.Duelli, "Ternary pseudorandom encoding of Fourier transform holograms (vol 16, pg 71, 1999)", JOSA A, **16,** 1999
16. http://www.holoeye.com/

The author has requested enhancement of the downloaded file. All in-text references underlined in blue are linked to publications on ResearchGate.