Systematic errors of an optical encryption system due to the discrete values of a spatial light modulator

David S. Monaghan, MEMBER SPIE
University College, Dublin
College of Engineering, Mathematics and Physical Sciences
School of Electrical, Electronic and Mechanical Engineering
and
Optoelectronic Research Centre
and
SFI-Srategic Research Cluster in Solar Energy Conversion
Belfield, Dublin 4, Ireland

Unnikrishnan Gopinathan
Universität Stuttgart
Institut für Technische Optik
Pfaffenwaldring 9
70569 Stuttgart, Germany

Damien P. Kelly, MEMBER SPIE
National University of Ireland
Department of Computer Science
Maynooth 999, Ireland

Thomas J. Naughton, MEMBER SPIE
National University of Ireland
Department of Computer Science
Maynooth, 999
Ireland
and
University of Oulu
Oulu Southern Institute
RFMedia Laboratory
Vierimaantie 5
84100 Ylivieska, Finland

John T. Sheridan, MEMBER SPIE
University College, Dublin
College of Engineering, Mathematics and Physical Sciences
School of Electrical, Electronic and Mechanical Engineering
and
Optoelectronic Research Centre
and
SFI-Strategic Research Cluster in Solar Energy Conversion
Belfield, Dublin 4, Ireland
E-mail: john.sheridan@ucd.ie

Abstract. An optical implementation of the amplitude encoded double random phase encryption/decryption technique is implemented, and both numerical and experimental results are presented. In particular, we examine the effect of quantization in the decryption process due to the discrete values and quantized levels, which a spatial light modulator (SLM) can physically display. To do this, we characterize a transmissive SLM using Jones matrices and then map a complex image to the physically achievable levels of the SLM using the pseudorandom encoding technique. We present both numerical and experimental results that quantify the performance of the system. [DOI: 10.1117/1.3076208]

Subject terms: optical encryption; digital image processing; spatial light modulator; quantization.

Paper 080746R received Sep. 22, 2008; revised manuscript received Dec. 5, 2008; accepted for publication Dec. 7, 2008; published online Dec. xx, xxxx.

1 Introduction

Recent technological advances, such as the availability of high-quality spatial light modulators (SLMs), high-resolution digital cameras (CCDs) and powerful desktop computers, coupled with the advantages of high throughput and computational speed of optical processing systems (arising due to their inherent parallel nature and speed of light operation), continue to stimulate interest, most recently, in the field of information security by means of

0091-3286/2009/$25.00 © 2009 SPIE

optical encryption.[1–3] Optical encryption offers the possibility of high-speed parallel encryption of two-dimensional complex data. Such encryption techniques often involve the capture of the full field information (i.e., both the field amplitude and the phase).

Digital holographic (DH) techniques[4–7] are employed to allow pre- and postcapture digital signal processing of the wavefront. When in digital form, these holograms can be easily stored, transmitted, processed, and analyzed.[8,9] Digital compression techniques can be used to enable efficient storage and transmission of holographic data.[8,10]

In order to decrypt the data optically, the complex-valued, encrypted image must be physically displayed using an SLM and then propagated through the decryption system. To date, there have been numerous optical encryption systems of this type proposed in the literature;[2,11–17] however, there have been relatively few experimental evaluations of the practical performance of SLMs in optical encryption/decryption systems.

Lohmann et al.[18] have shown that the evolving space-bandwidth product (SBP) of a signal as it propagates through an optical system cannot exceed the SBP of the optical system without loss of information. The signals' Wigner distribution Function has been used to track the SBP of an optical signal propagating through an optical system.[19] By successfully tracking the SBP of a signal in this way, one can identify the sampling rate necessary in order to adhere to the Nyquist sampling criteria.[20] There are many factors that affect the SBP of a signal as it propagates through an optical system. These include the following:

1. the finite aperture of the elements such as lenses, SLMs, and CCD cameras
2. the effective pixel size and fill factor of discrete optoelectronic input and output devices, such as SLMs and CCD cameras,
3. the quantization effects introduced by these same optoelectronic devices.

These operations may also introduce systematic noise in the signal, as opposed to random noise introduced due to optical scatter (speckle) and electronic noise introduced by the SLMs, CCD, or lasers.

Typically, optical encryption techniques proposed in the literature involve a coherent field propagated through some bulk optical system that consists of thin lenses and sections of free space. Such lossless paraxial quadratic phase systems can be conveniently described mathematically using the linear canonical transformation (LCT).[19] The optical Fourier, fractional Fourier, and Fresnel transforms are simplified forms of the LCT.

Implementation of these systems often requires the use of several SLMs. Voltages applied to individual SLM pixels are used to discretely modulate the amplitude and/or phase of the complex wave field at the input plane. The behavior of SLMs are thus of considerable practical importance because they are used to present the input fields to the optical encryption systems or to provide the encryption/decryption phase keys within the system.

The double random phase encoding (DRPE) technique, as proposed by Refregier and Javidi[1] in 1995, is a method of optically encoding a primary image to stationary white noise by the use of two statistically independent random phase keys. One of these keys, R_1, is placed in the input plane and the other, R_2, in the Fourier plane of a 2f system. In this paper, we discuss the operation of the encryption system in an amplitude encoding (AE) mode, in this case the input image is grey scale and real, and the phase key R_2 located in the Fourier plane provides the only relevant encryption key.[21] The AE DRPE technique can be numerically simulated using finite matrices containing discrete complex values and the fast Fourier transform.

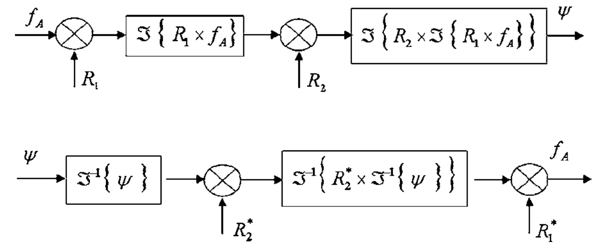

Fig. 1 Let f_A represent the input data to be encrypted. Let $\Im\{\bullet\}$ and $\Im^{-1}\{\bullet\}$ represent a Fourier and an inverse Fourier transform, respectively. In (a), the input signal f_A is multiplied by a random phase key R_1, a Fourier transform is performed, it is multiplied by a second random phase key R_2 and subsequently transformed by a second Fourier transform to provide the encrypted image $\psi(x)$. The decryption process in (b) is equivalent to the encryption process inverted.

Figure 1 illustrates encryption/decryption using the DRPE technique. It can be seen that the amplitude encoded input image, f_A, is multiplied by the input-plane encryption phase key, R_1. A Fourier transform is subsequently preformed with the resultant complex-valued image multiplied by the Fourier-plane encryption phase key, R_2. An additional Fourier transform is then performed to produce the encrypted image, ψ. This encrypted image can be mathematically described as

$$\psi = \Im[R_2 \times \Im(R_1 \times f_A)], \tag{1}$$

and the recovered decrypted image can be described as

$$f_A = \Im^{-1}[R_2^* \times \Im^{-1}(\psi)] \times R_1^*, \tag{2}$$

where the asterisk denotes the complex conjugate. It should be noted that when using the DRPE technique with an amplitude-encoded input image, the removable or multiplication of the conjugate input-plane phase key (R_1^*) is not required because the intensity can be obtained as follows:

$$I_{f_A} = |f_A|^2 = |\Im^{-1}[R_2^* \times \Im^{-1}(\psi)]|^2. \tag{3}$$

This is the case because the encryption/decryption phase keys have unit amplitude.

We perform our analysis by first numerically simulating the optical setup, and then we physically build and test our setup in the lab. It should be noted that in our simulations we do not model any of the physical limitations present in a real system other than that of quantization, which is our primary concern in this paper. Results measured in a physical system are compared to numerical simulations in Section 5.

When numerically implementing the DRPE technique, complex values can easily be simulated and stored. The experimental display or representation of complex values, using SLMs, in an optical implementation is significantly more complicated. SLMs can operate in an amplitude or in a phase mode; however, for most commercial SLMs there is no independent control of the amplitude and phase (i.e., they operate in a coupled mode), and this increases the difficulty when trying to display complex values. Cohn[22] and Duelli et al.[23] have devised a method using a pseudo-random encoding technique (PET) as a method of statistically approximating desired complex values with those values that are achievable with a given SLM.

This paper is organized as follows: In Section 2 we discuss a method using Jones algebra, of characterizing our SLM, which is a Holoeye LC2002.[8,15] In Section 3, we use the PET and apply it to our SLM using the parameters obtained from the characterization carried out in Section 2. In Section 4, we describe our experimental decryption setup. In Section 5, we present and compare numerical simulations and experimental results. Finally, in Section 6, we present a brief conclusion.

2 SLM Characterization

In all physical optical systems, the polarization of a light beam can be described using a Jones vector. Similarly, the effect of any linear optical element on the polarization state of a field can be described by a Jones matrix.[24] Jones calculus is an extremely useful tool for describing the effect that linear optical elements have on the polarization state of an incident field. The beam is described in terms of an electric vector[24]

$$\vec{E} = \begin{bmatrix} E_x(t) \\ E_y(t) \end{bmatrix}, \tag{4}$$

where $E_x(t)$ and $E_y(t)$ are the horizontal and vertical scalar components of $\vec{E}$, respectively. This instantaneous polarization state of $\vec{E}$ can also be written in complex form as

$$\tilde{E} = \begin{bmatrix} E_{0x}e^{i\varphi x} \\ E_{0y}e^{i\varphi y} \end{bmatrix}, \tag{5}$$

where φx and φy represent the horizontal and vertical phase components, respectively. Because the Jones vector of a beam is made up of orthogonal horizontal and vertical polarization states, each state can be separately written as

$$\tilde{E}_{\mathrm{h}} = \begin{bmatrix} E_{0x}e^{i\varphi x} \\ 0 \end{bmatrix} \quad \text{and } \tilde{E}_{\mathrm{v}} = \begin{bmatrix} 0 \\ E_{0y}e^{i\varphi y} \end{bmatrix}. \tag{6}$$

If a beam of light, which has linear polarization, is incident on a linear optical element, it emerges with a new polarization vector. The linear optical element has transformed the original vector into a new vector by a process that can be described mathematically using a 2×2 Jones matrix[24] Each pixel in a transmissive SLM acts as a linear optical element if a constant gray-scale level is displayed on it. In most SLMs, gray-scale values are set by applying a voltage and associated with each voltage are amounts of both phase and amplitude. The form of modulation of the incident beam depends on in which mode the SLM is operating. Typically, it can be assumed that each SLM pixel acts identically as long as all the pixels are set to the same constant gray-scale level. By finding the SLM pixel's Jones matrix, for each gray-scale level, we can characterize the device. In order to characterize the SLM, two experiments were carried out to determine (*i*) the amplitude and (*ii*) the phase, corresponding to a particular applied voltage.

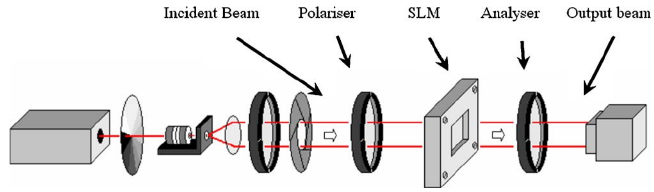

Fig. 2 Experimental setup for determining the amplitude modulation of our SLM for each gray-scale level voltage.

The first experiment was to determine the amplitude characteristics of the pixels of the SLM (see Fig. 2). The Jones vector of the incident beam in Fig. 2 can be written as

$$\begin{bmatrix} \sqrt{I}/\sqrt{2} \\ \sqrt{I}/\sqrt{2} \end{bmatrix} = \begin{bmatrix} \sqrt{I_0} \\ \sqrt{I_{90}} \end{bmatrix}, \tag{7}$$

where I is the intensity of the beam, and the polarization of the light beam has been set, by a linear polarizer, to 45 deg. The Jones matrix that corresponds to a polarizer that is set at either 0 or 90 deg is

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{or} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \tag{8}$$

respectively. Therefore, the Jones vector for the output beam, when the polarizer and the analyzer have been set to an angle of 0 deg, can be calculated as follows:

$$\begin{bmatrix} A\sqrt{I_0} \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} A & B \\ C & D \end{bmatrix} \times \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} \sqrt{I_0} \\ \sqrt{I_{90}} \end{bmatrix}. \tag{9}$$

By measuring the intensity of the output beam for the four possible combinations of the orientation of the polarizer and the analyzer (each set at either 0 or 90 deg), we can fully determine the 2×2 Jones matrix corresponding to that specific grey-scale level displayed on the SLM. Using the following formulas provides us with the amplitude modulation of the SLM for each grey-scale level:

$$\begin{bmatrix} A\sqrt{I_0} \\ 0 \end{bmatrix} \rightarrow |A|^2 I_0 = I_{\text{measured}}, \tag{10}$$

$$|A| = \sqrt{\frac{I_{\text{measured}}}{I_0}}. \tag{11}$$

In order to measure the phase modulation of the SLM, we make use of a DH setup[10] in which we capture the output interference pattern using a CCD camera (see Fig. 3). We split the SLM screen into two areas, displaying a reference grey scale on the top half and varying the gray-scale level on the bottom half. This allows us to measure the relative phase shift of the interference fringes recorded for each of

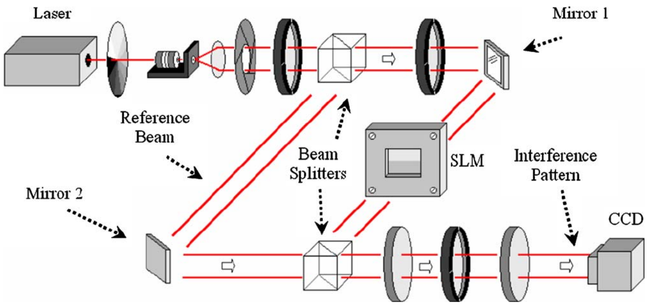

Fig. 3 Experimental setup for determining the phase modulation of our SLM for each gray-scale level voltage.

the four different combinations of the polarizer and analyzer (i.e., each again being set to either 0 or 90 deg). In this way, we can fully determine the 2×2 Jones matrix corresponding to the SLM for phase modulation of the pixels for each grey-scale level. The polarizer/analyzer combinations of 0/0, 90/0, 0/90, and 90/90 deg correspond to the individual phase components of ϕ_1, ϕ_2, ϕ_3, and ϕ_4. Combining this information with the amplitude modulation measurements gives us

$$\begin{bmatrix} |A|\angle\phi_1 & |B|\angle\phi_2 \\ |C|\angle\phi_3 & |D|\angle\phi_4 \end{bmatrix}. \tag{12}$$

Figure 4 shows the resulting polar plot that characterizes the SLM and clearly demonstrates that the SLM operates in the coupled mode.

Now that the SLM is fully characterized, the next problem is to map the complex numbers that we wish to display, to the complex numbers (quantized levels) that our SLM can physically represent. We do this using the PET.[22,23,25]

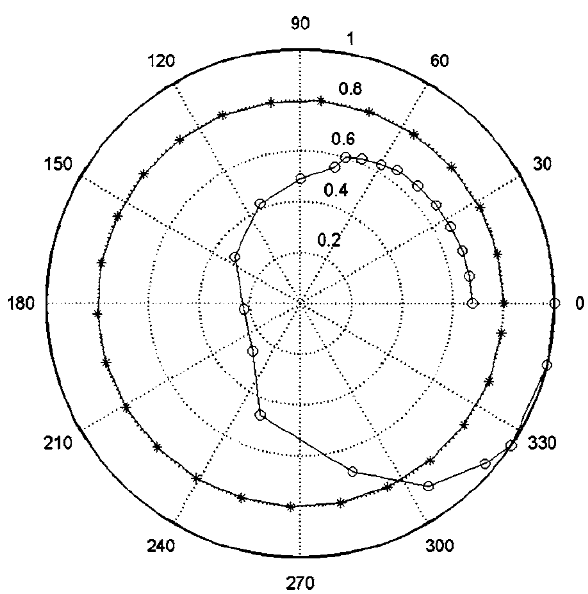

Fig. 4 A polar plot of the states physically achievable on our SLM, which operates in a coupled mode (denoted by circular dots). An ideal SLM operating in an ideal phase mode would have very little or no amplitude modulation (denoted by stars). Note that the circle has a radius of 0.8, only for ease of graphical presentation).

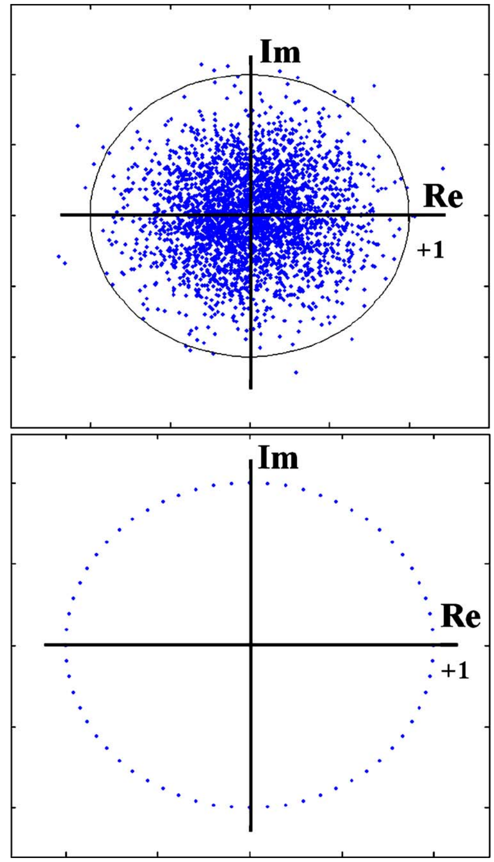

Fig. 5 (a) A polar plot of an encrypted image made up of complex values and (b) the encrypted image displayed in (a) that has been mapped to the achievable quantization levels of an ideal lossless phase-only mode SLM.

3 Pseudorandom Encoding Technique

Our SLM, which works in a coupled phase/amplitude mode, can only display a certain range of discrete complex values that we have determined in Section 2. Figure 5(a) shows a typical example of a polar plot displaying a complex-valued image. If this image where mapped directly to a lossless phase-only SLM, with $2^6=64$ finite quantization levels, then it would appear as the polar plot shown in Fig. 5(b). Because the encrypted image and the decrypting phase key, which we wish to display on the SLM, are normally randomly distribute in the complex plane (i.e., having phase values spread randomly from 0 to 2π), we need to map these complex values to the discrete complex values (quantization levels) that the SLM can display. To do this, we employ the PET,[22,23,25] which is a statistical method of approximating a required complex value using only those values that are achievable. Figure 6 shows an example of the application of PET to display a complex number, a_c. On a polar diagram, the distance from the origin represents the amplitude, while the angle of the vector represents the phase. We now wish to display a_c using the three possible SLM quantization levels, (V_1, V_2, and V_3) as shown in Fig. 6.

A simple minimum Euclidean distance algorithm would map the state a_c to V_2; however using the PET, a probability is assigned to each possible mapping, which is deter-

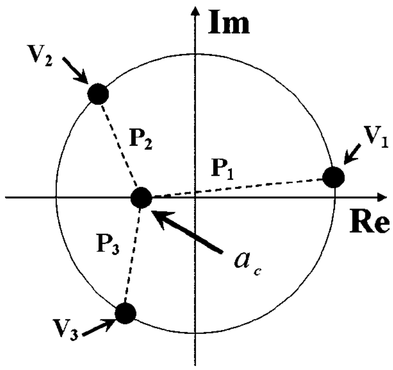

Fig. 6 A polar plot displaying a required complex value, a_c, and three achievable values that the SLM can display.

mined by the distance from a_{c} to each quantization level. If we have an image that has multiple values at a_{c}, each value at a_{c} is mapped to one of the SLM levels with the given associated probabilities. The PET[22] finds a value of the ensemble average of a random variable, a, such that $\langle a\rangle = a_{\mathrm{c}}$. Because this is a statistical method, the greater the number of values is at a_{c}, the more accurate the assignment method becomes.

When we increase the number of quantization levels that can be displayed, determining the probability associated with each distance becomes more complicated, and a linear relationship between Euclidean distances and probability does not always provide the most efficient method. In Fig. 6, we have assigned a probability to each of the three achievable levels, V_1, V_2, and V_3, such that

$$P_1 + P_2 + P_3 = 1. \tag{13}$$

This implies that a_{c} will be given by

$$a_{\mathrm{c}} = P_1 a_{V_1} + P_2 a_{V_2} + P_3 a_{V_3}, \tag{14}$$

where a_{V_n} is the number of points of value a_{c} mapped to level, V_n. Separating Eq. (14) into its real and imaginary parts gives

$$\mathrm{Re}[a_{\mathrm{c}}] = P_1\,\mathrm{Re}[a_{V_1}] + P_2\,\mathrm{Re}[a_{V_2}] + P_3\,\mathrm{Re}[a_{V_3}] \tag{15}$$

and

$$\mathrm{Im}[a_{\mathrm{c}}] = P_1\,\mathrm{Im}[a_{V_1}] + P_2\,\mathrm{Im}[a_{V_2}] + P_3\,\mathrm{Im}[a_{V_3}]. \tag{16}$$

Writing Eqs. (14)–(16) as simultaneous equations gives

$$\begin{bmatrix} \mathrm{Re}[a_{\mathrm{c}}] \\ \mathrm{Im}[a_{\mathrm{c}}] \\ 1 \end{bmatrix} = \begin{bmatrix} \mathrm{Re}[a_{V_1}] & \mathrm{Re}[a_{V_2}] & \mathrm{Re}[a_{V_3}] \\ \mathrm{Im}[a_{V_1}] & \mathrm{Im}[a_{V_2}] & \mathrm{Im}[a_{V_3}] \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}, \tag{17}$$

and using simple matrix algebra, we can determine the three mapping probabilities P_1, P_2, and P_3. Expanding this method, we can take a complex valued image, to be displayed on an SLM with a fixed number of available levels, and encode the image to those levels based on the calculated probabilities. In Section 5, we discuss the results found when encoding a complex-valued encrypted image and a complex-valued decryption key to a SLM, assuming 4, 8, and 16 available quantization levels.

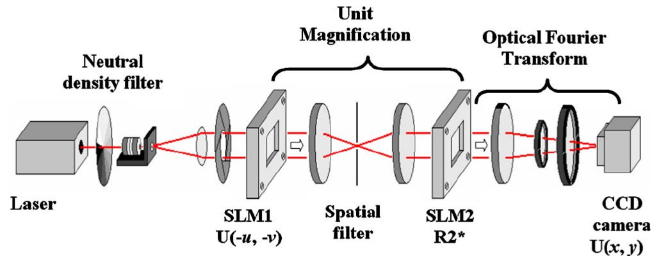

Fig. 7 The experimental optical decryption setup.

4 Decryption Experimental Setup

In the DRPE technique decryption process, two Fourier transforms are required. In our implementation, in order to simplify the optical setup, we perform the first Fourier transform numerically. This first Fourier transform is an unambiguous step because no knowledge of the decrypting phase key is required. Figure 7 shows a diagram of our experimental decryption setup. Using two transmissive SLMs (both operating in a mostly phase-only mode), which have been imaged onto one another by means of a 4f imaging system, we display the inverse Fourier transform of the encrypted image on SLM1 and the decryption phase key R_2^* on SLM2. The complex images are mapped to the SLMs employing Cohn's PET as described in Section 3. The second Fourier transform is performed optically using free-space propagation and a thin lens. The resulting intensity of the wavefront is then captured using a CCD camera.

As stated, we are concerned here with AE images; therefore, the intensity of the wavefront is all that is required in order to recover the encrypted image. A spatial filter (aperture) is placed in the Fourier domain of the 4f imaging system, between the two SLMs, so as to filter out the higher-order diffraction terms introduced by the periodicity of SLM1.

5 Results

We studied the effect of quantization in the decryption process due to the discrete levels that an SLM can display. The encrypted image and the random phase key R_2^* are complex valued, and when either is displayed on a practical SLM (one that can only display a finite number of levels), this gives rise to errors during the decryption process. For the experimental results [shown later in Fig. 9(d)–9(f)], a 532-nm wavelength laser was used.

Figure 8 shows a sequence of numerically simulated results in which we use an SLM that has three available quantization levels, and we simulate the setup described in Fig. 7. Significant differences can be noted between data encoded to 16 levels and the same data encoded to 3 levels. These differences correspond to a loss of information in the desired decrypted image [Fig. 8(b)] and inaccuracy in the phase key [Fig. 8(d)], the encoded decrypted image, [Fig. 8(c)]. and the encoded phase key [Fig. 8(e)]. Usually, this loss of detailed information, due to the reduction in quantization levels, has the effect of making the image appear brighter.

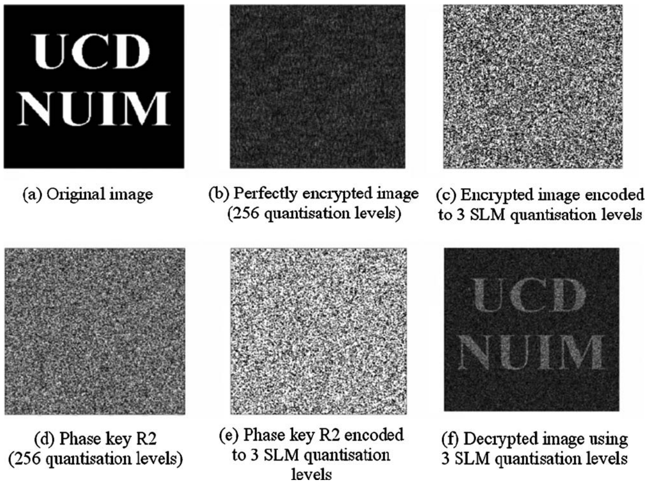

Fig. 8 (a) Original image, (b) encrypted image, (c) encrypted image as represented on SLM with three quantized levels, (d) Fourier decryption phase key, (e) Fourier decryption phase key as represented on SLM with three quantized levels, and (f) decrypted image with three quantized levels.

Figure 9 shows two sets each of three images, decrypted using a SLM with 4, 8, and 16 quantization levels. The first set [see Fig. 9(a)–9(c)] has been produced numerically as discussed the decryption setup shown in Fig. 7. The second set [see Fig. 9(d)–9(f)] gives the corresponding experimental results generated using the setup, shown in Fig. 7, captured with an Imperx IPX-1M48 CCD camera. It should be noted that there is a relatively strong central spot in the experimental results that is due to the <100% diffraction efficiency of the SLM. It arises due to nonideal SLM operation (fill factor, mixed mode operation, etc.) and to implementation errors and lens aberrations. Such physical effects, including the low-pass filter present in the optical system (see Fig. 7), are not modeled in the numerical simulation. In Table 1, NRMS and cross correlation values are presented. The resultant simulated and experimental decryptions are cross correlated with a perfectly decrypted image. NRMS values for the experimental results are not presented due to variations in the laser power used. We have also shown the cross correlation for the experimental results when a black circle is numerically applied to cancel the large bright term in the centre of the experimental images. We note that removing this bright spot has little effect on the resulting cross correlating values in Table 1. Despite the significant assumptions made when performing the simulations and the limitations of the experimental setup used, the trends observable for the numerical and experimental results match reasonably well.

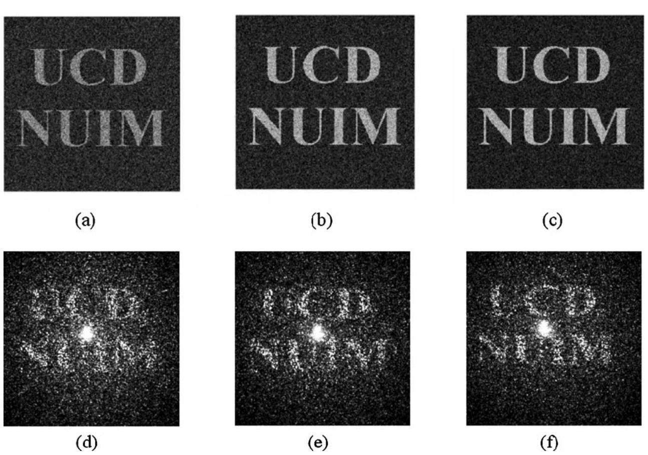

Fig. 9 Images decrypted using the setup shown in Fig. 7: (a–c) Results that have been numerically simulated for cases when we used a SLM with 4, 8, and 16 available values, respectively. (d–f) Experimental results for cases when we used a SLM with 4, 8, and 16 available values, respectively.

Table 1 The NRMS and cross-correlation values associated with the decrypted images shown in Fig. 9.

	SLM quantization levels	$2^2=4$	$2^3=8$	$2^4=16$
Simulations	NRMS	0.9324	0.8940	0.8636
	Cross correlation	0.2250	0.2620	0.3638
Experimental	Cross correlation	0.1835	0.2085	0.2147
	Cross correlation, blocking the central bright spot	0.1875	0.2135	0.2201

6 Conclusions

In this paper, the effects of quantization and imperfect operation of the SLM during decryption have been examined. Employing 2×2 Jones matrices, the SLM used was characterized by assuming that each pixel acts as a linear optical element. The Jones matrix was found for each voltage-controlled gray level possible by independently measuring both the amplitude and phase modulation of the device. By characterizing the SLM, which operates in a coupled mode, the complex values (quantization levels) it can display were determined.

In Section 3, the PET is applied to our SLM using the parameters presented in Section 2. This permits the minimization of the systematic errors that occur when a complex-valued image is displayed on the SLM. The decryption setup, which is implemented for AE DRPE technique decryption, is described in Section 4. In Section 5, both numerical and experimental results for such a system are presented. Although there was a relatively strong central spot in the experimental results, the trend observed in the cross correlations for the experimental results were in close agreement with those predicted by the numerical simulations.

Using the PET, it is possible to systematically display complex-valued images on a SLM that is only capable of displaying a limited range of quantization levels. We have shown that the PET can be applied when implementing the AE DRPE technique and that it is possible to perform satisfactory decryption.

These practical results have implications for the technique used to capture data in optical encryption systems[25] and, ultimately, for the security of such systems.[26] The full implications require further detailed study.

Acknowledgments

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 also thank the Irish Research Council for Science, Engineering and Technology. One of the authors (DSM) acknowledges the support of a SPIE Educational Scholarship.

References

1. P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767–769 (1995).
2. 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).
3. B. M. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.* **28**, 269–271 (2003).
4. J. W. Goodman and R. W. Lawrence, "Digital image formation from electronically detected holograms," *Appl. Phys. Lett.* **11**, 77–■ (1967).
5. 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**, 2693–2703 (1974).
6. U. Schnars and W. Juptner, "Direct recording of holograms by a CCD target and numerical reconstruction," *Appl. Opt.* **33**, 179–181 (1994).
7. L. Onural and P. D. Scott, "Digital decoding of in-line holograms," *Opt. Eng.* **26**, 1124–1132 (1987).
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**, 4124–4132 (2002).
9. U. Gopinathan, D. S. Monaghan, B. Hennelly, C. P. McElhinney, D. P. Kelly, J. B. McDonald, T. J. Naughton, and J. T. Sheridan, "A projection system for real world three dimensional objects using spatial light modulators," *J. Disp. Technol.* ■, ■ (2008).
10. T. J. Naughton and B. Javidi, "Compression of encrypted three-dimensional objects using digital holography," *Opt. Eng.* **43**, 2233–2238 (2004).
11. P. Refregier and B. Javidi, "Optical-image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767–769 (1995).
12. 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).
13. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Opt. Lett.* **24**, 762–764 (1999).
14. E. Tajahuerce and B. Javidi, "Encrypting three-dimensional information with digital holography," *Appl. Opt.* **39**, 6595–6601 (2000).
15. G. Unnikrishnan, M. Pohit, and K. Singh, "A polarization encoded optical encryption system using ferroelectric spatial light modulator," *Opt. Commun.* **185**, 25–31 (2000).
16. N. K. Nishchal, G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption using a localized fractional Fourier transform," *Opt. Eng.* **42**, 3566–3571 (2003).
17. U. Gopinathan, T. J. Naughton, and J. T. Sheridan, "Polarization encoding and multiplexing of two-dimensional signals: application to image encryption," *Appl. Opt.* **45**, 5693–5700 (2006).
18. A. W. Lohmann, R. G. Dorsch, D. Mendlovic, Z. Zalevsky, and C. Ferreira, "Space-bandwidth product of optical signals and systems," *J. Opt. Soc. Am. A* **13**, 470–473 (1996).
19. B. M. Hennelly and J. T. Sheridan, "Generalizing, optimizing, and inventing numerical algorithms for the fractional Fourier, Fresnel, and linear canonical transforms," *J. Opt. Soc. Am. A* **22**, 917–927 (2005).
20. B. M. Hennelly and J. T. Sheridan, "Optical encryption and the space bandwidth product," *Opt. Commun.* **247**, 291–305 (2005).
21. 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).
22. R. W. Cohn, "Pseudorandom encoding of complex-valued functions onto amplitude-coupled phase modulators," *J. Opt. Soc. Am. A* **15**, 868–883 (1998).
23. M. Duelli, M. Reece, and R. W. Cohn, "Modified minimum-distance criterion for blended random and nonrandom encoding," *J. Opt. Soc. Am. A* **16**, 2425–2438 (1999).
24. E. Hecht and A. Zajac, *Optics*, Addison-Wesley, Reading, MA (1980).
25. R. W. Cohn and M. Duelli, "Ternary pseudorandom encoding of Fourier transform holograms," *J. Opt. Soc. Am. A* **16**, 1089–1090 (1999).

David S. Monaghan received his BE (honors) in electronic engineering from University College Dublin (UCD) in 2004. This led him to pursue further studies within the Department of Electronic Engineering. He is currently working toward a PhD in applied optics and optical encryption at the School of Electrical, Electronic & Mechanical Engineering at UCD. He has been actively involved in the UCD SPIE Student Chapter for three years. His research interests include optical encryption, optical signal processing, digital holography, and spatial light modulator application with a view to optical encryption/decryption. His current research involves analyzing the Double Random Phase encoding algorithm and modeling of the physical behavior of spatial light modulators in paraxial optical systems.

Unnikrishnan Gopinathan received his PhD from the Indian Institute of Technology, New Delhi, India. He is currently a Humboldt research fellow at Stuttgart University, Stuttgart, Germany. His research interests include optical signal processing related to holographic displays and biomedical imaging.

Damien P. Kelly is currently a research fellow with the National University of Ireland, Maynooth, and has 17 published journal articles and more than 20 conference contributions. He earned a PhD in engineering from the School of Electrical, Electronic and Mechanical Engineering, University College, Dublin, Ireland, in 2006, and his BS in electronic engineering at the National University of Ireland, Cork, in 2000. He has worked as a postdoctoral researcher with Technical University in Vienna on experimental THz spectroscopy systems. His research interests include optical signal processing, terahertz spectroscopy systems, numerical and analytical modeling of optical systems, speckle metrology, and statistical optics. His current research involves 3-D display and capture systems, specifically, digital holography, sampling theory, and speckle statistics. He is a member of both SPIE and OSA.

Thomas J. Naughton received his BSc (double honors) in computer science and experimental physics from the National University of Ireland, Maynooth, Ireland. He has worked at Space Technology (Ireland) Ltd. and has been a visiting researcher at the Department of Radioelectronics, Czech Technical University, Prague, and the Department of Electrical and Computer Engineering, University of Connecticut, Storrs. He is a senior lecturer in the Department of Computer Science, National University of Ireland, Maynooth, with a permanent appointment since 2001. Since 2007, he has been a European Commission Marie Curie Fellow at Oulu Southern Institute, University of Oulu, Finland. He leads the EC FP7 three-year eight-partner collaborative project Real 3D. His research interests include optical information processing, computer theory, and distributed computing. He has served as a committee member on 12 international IEEE, ICO, and SPIE conferences. He has coauthored more than 150 publications, including 40 journal articles and 20 invited conference papers. He is a corecipient of the 2008 IEEE Donald G. Fink Prize Paper Award.

John T. Sheridan received his BS (H1) in electronic engineering, from University College Galway (NUIG) in 1985, and his MS in the science of electrical engineering, from Georgia Tech, in 1986. While at Georgia Tech, he worked as a research assistant to Prof. William T. Rhodes. In 1987, he matriculated as a member of Jesus College Oxford and, in 1991, he was awarded his PhD by Oxford University. This was followed by postdoctoral fellowships, supported first (1991) by the Alexander von Humboldt Foundation and later (1992) by a European Community Bursary, both held at the Lehrstuhl fur Angewandte Optik in Erlangen-Nürnberg University. In 1994, he served as a visiting scientist at the European Commission Joint Research Centre, in Italy. In 1997, he was appointed to the School of Physics, Dublin Institute of Technology as a permanent lecturer. He joined the Department of Electronic and Electrical, Engineering, UCD, in 2000, as a college lecturer. In 2005, he became a senior lecturer and, in 2007, professor of optical engineering within the School of Electrical, Electronic and Mechanical Engineering. He currently acts as deputy director of the UCD Optoelectronic Research Centre and deputy director of the SFI Strategic Research Cluster in Solar Energy Conversion. He has authored ~120 reviewed journal papers and ~100 conference proceedings papers.

AUTHOR QUERIES — 001902JOE

#1 Authors and affiliations reformatted for style. Please check details for accuracy. Correct postal code?
#2 Author, Please define NRMS.
#3 Ref. 4: Please provide ending page number.
#4 Ref. 9: Please give volume number and page range.
#5 Ref. 24: Reading, MA correct?