IOP Publishing Journal of Optics

J. Opt. **18** (2016) 025701 (7pp) doi:10.1088/2040-8978/18/2/025701

Single-random phase encoding architecture using a focus tunable lens

E F Mosso[1], **N Bolognini**[2,3] **and D G Pérez**[1]

[1] Instituto de Física, Facultad de Ciencias, Pontificia Universidad Católica de Valparaíso (PUCV),
Av. Brasil 2950, 234–0025 Valparaíso, Chile
[2] Facultad de Ciencias Exactas, Universidad Nacional de La Plata (UNLP), Argentina
[3] Centro de Investigaciones Ópticas (CONICET La Plata-CIC), and OPTIMO (Facultad Ingeniería, UNLP),
PO Box 3, 1897 M.B. Gonnet, Argentina

E-mail: edward.mosso@ucv.cl

Received 15 September 2015, revised 30 November 2015
Accepted for publication 2 December 2015
Published 6 January 2016

Abstract

We propose a new nonlinear optical architecture based on a focus tunable lens and an iterative phase retrieval algorithm. It constitutes a compact encryption system that uses a single-random phase key to simultaneously encrypt (decrypt) amplitude and phase data. Summarily, the information encoded in a transmittance object (phase and amplitude) is randomly modulated by a diffuser when a laser beam illuminates it; once the beam reaches a focus tunable lens, different subjective speckle distributions are registered at some image plane as the focal length is tuned to different values. This set of speckle patterns constitutes a delocalized ciphertext, which is used in an iterative phase retrieval algorithm to reconstruct a complex ciphertext. The original data are decrypted propagating this ciphertext through a virtual optical system. In this system, amplitude data are straightforwardly decrypted while phase data can only be restored if the random modulation produced in the encryption process is compensated. Thus, an encryption–decryption process and authentication protocol can simultaneously be performed. We validate the feasibility of our proposal with simulated and experimental results.

S Online supplementary data available from stacks.iop.org/jopt/18/025701/mmedia

Keywords: Fourier optics and signal processing, data processing by optical means, optical security and encryption, phase retrieval

(Some figures may appear in colour only in the online journal)

1. Introduction

In the past two decades, many optical cryptographic systems have been reported. The first contributions were based on linear systems—e.g., $4f$ and JTC correlation architectures [1]. In the classical $4f$ DRPE [2], two random phase masks are used to transform the input object into a white noise distribution which is then holographically recorded. Henceforth, this architecture involves an interferometric arrangement including many optical elements. Numerous linear versions of this architecture have been presented in the fractional Fourier domain and Fresnel domain [3–10]. Nevertheless, it has been reported that some of these schemes are unsecure; some cryptoanalysis strategies have shown that any inherently linear optical encryption system is vulnerable [11–18]. Thus, optical encoding–decoding architectures overcoming this weakness, without losing confidence level, are valuable [19–22].

Recently, Chen *et al* [23], have proposed an optical encoding system based on multiple intensity samples of the ciphertext. Two systems are proposed: the input data are encrypted by using three phase masks and the ciphertext is registered at three different positions by displacing the image sensor along the optical axis; alternatively, a pair of beam splitters allow simultaneous speckle recording at three CCD cameras—located, in this way, at different distances of the optical axis. A successful decryption can only be achieved by a receiver having a replica of the phase masks and knowledge

2040-8978/16/025701+07$33.00

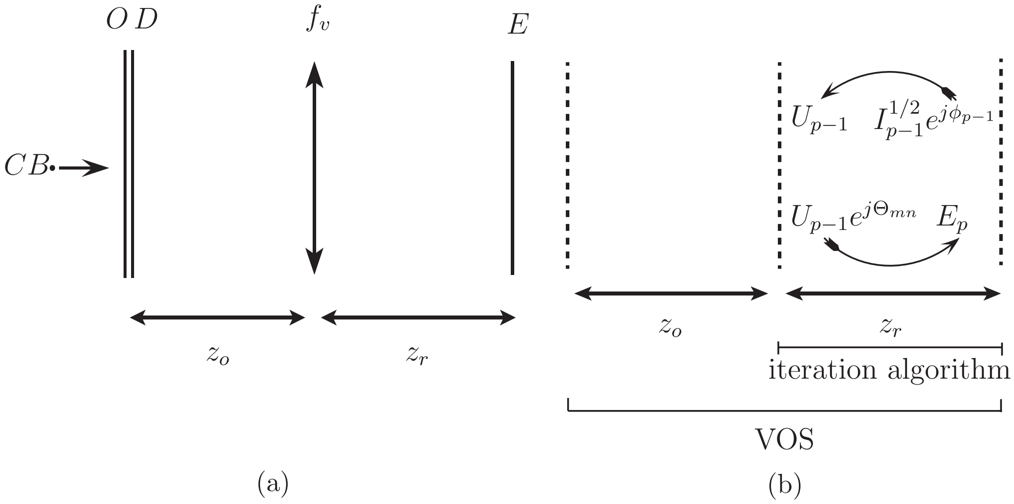

Figure 1. Encryption and decryption stages: (a) proposed encoding architecture by using a tunable lens, and (b) decryption process by using the registered speckle images at the plane E in (a)—p is the iteration step with $m = p$, $n = p - 1$.

of the encoding optical parameters. They verified these architectures by numerical simulations. Lately, in Mosso *et al* [24], we have proposed an optical encoding system employing a three-dimensional subjective speckle distribution as a secure information carrier. In this system, the ciphertext is sampled by registering consecutive planes along the optical axis with a CMOS camera. Then, the original data are successfully decrypted by employing a simulation of the optical encoding system and an iterative phase retrieval algorithm on the set of speckle patterns registered by the camera. Also, we have presented a DRPE architecture based on a single-lens imaging system and a phase retrieval procedure applied to a set of intensity samples produced by a tridimensional speckle distribution (ciphertext) [25]. These contributions highlight the advantages of using a delocalized ciphertext instead of standard encryption techniques based on holographic recording.

Our previous proposals [24, 25] have been oriented towards the design of compact optical architectures capable of encrypting data through a secure process, with minimal optical components and employing delocalized recordings of encrypted information. In these works a mobile platform is used to capture diffracted intensity recordings planes of speckle patterns (delocalized ciphertexts) either in a free-space propagating architecture or with a single-lens imaging system. In the present proposal, we have removed the moving platform that displaces the digital camera and replaced it with a focus tunable lens (comparatively less expensive than a moving platform). This change presents three important advantages: avoids positioning errors, achieves faster acquisition times, and further reduces the size of the encryption system. In this work, condensed versions of the architectures reported in [24, 25] are discussed by the introduction of a focus tunable lens. To our knowledge, this is the first discussion of such setup; furthermore, the introduction of a variable focal length requires a new iterative phase retrieval algorithm.

2. Single-random phase encoding architecture with a focus tunable lens

Instead of using a translation platform or multiple optical elements to sample the three-dimensional speckle field, as in [23–25], we set at a fixed position a focus tunable lens, f_v, and a CMOS camera—at z_o and $z_o + z_r$ from the object, respectively, figure 1(a). By tuning the lens to different focal length values, $\{f_0, f_1, ..., f_N\}$, multiple intensity distributions of the speckle field (delocalized ciphertext) are sampled at a single plane (improving recording times). This delocalized ciphertext overcomes the security vulnerabilities caused by any combination of linear encrypting architectures (4f, JTC, 2f, single-lens, lens-less, etc) and a single holographic record of the ciphertext. It has been demonstrated [24] that each speckle distribution plays both roles as coder of information and encoding parameter (several of these are required to recover the original data). Then, in order to successfully decrypt the original data, these speckle distributions are used in an iterative phase retrieval algorithm, depicted in figure 1(b). Briefly, it starts by backward propagating the initial wavefront $\sqrt{I_0}\,\mathrm{e}^{j\phi_0}$ (here $\phi_0 = 0$) a distance z_r; at this plane, the propagated field U_0 is multiplied by a complex factor $\mathrm{e}^{j\Theta_{10}}$. In general, Θ_{mn} is the difference between two quadratic phases corresponding to two succesive focal length values from the tunable lens: $\Theta_{mn} = \frac{k}{2}(f_m^{-1} - f_n^{-1})\|\mathbf{r}\|^2$ ($m = 1$ and $n = 0$ corresponds to the two first focal length values f_0 and f_1; $k = 2\pi/\lambda$ is the wavenumber and $\mathbf{r}$ represents an arbitrary position on the lens plane). The constructed field, $U_0\mathrm{e}^{j\Theta_{10}}$, freely propagates a distance z_r to produce the field E_1, but at this plane the true amplitude is provided by $\sqrt{I_1}$; therefore, the field $\sqrt{I_1}\,\mathrm{e}^{j\phi_1}$ is built with phase $\phi_1 = \arg E_1$. The resulting complex field is used in the next iteration ($m = 2$ and $n = 1$). This procedure is sequentially repeated forward until the quadratic phase from the last focal length, f_N, is reached. Then backwards by starting with $m = N - 1$ and $n = N$, and going in decrements up to $m = 0$ and $n = 1$. This back and forth iteration is truncated when a difference between the calculated

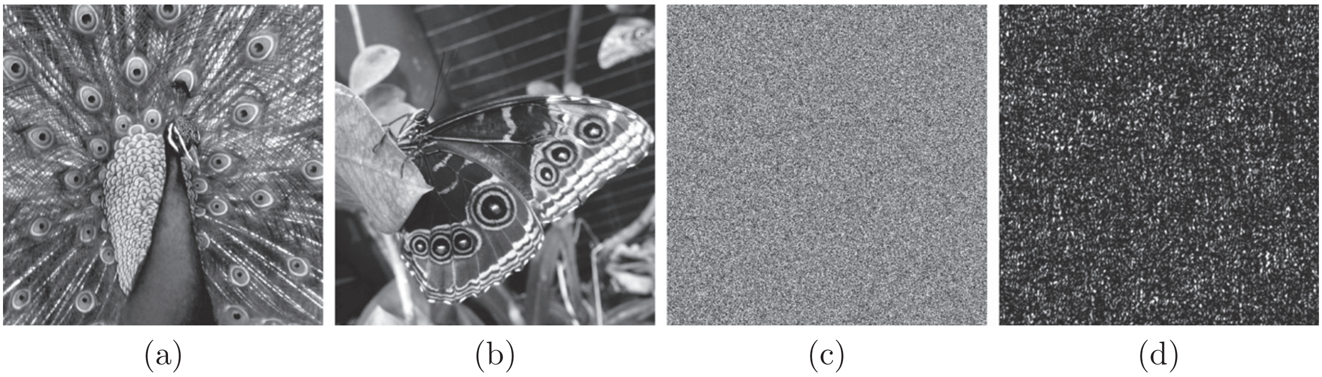

Figure 2. Simulated results: (a) amplitude mask, (b) phase mask, (c) diffuser phase, and (d) zoomed image from the ciphertext.

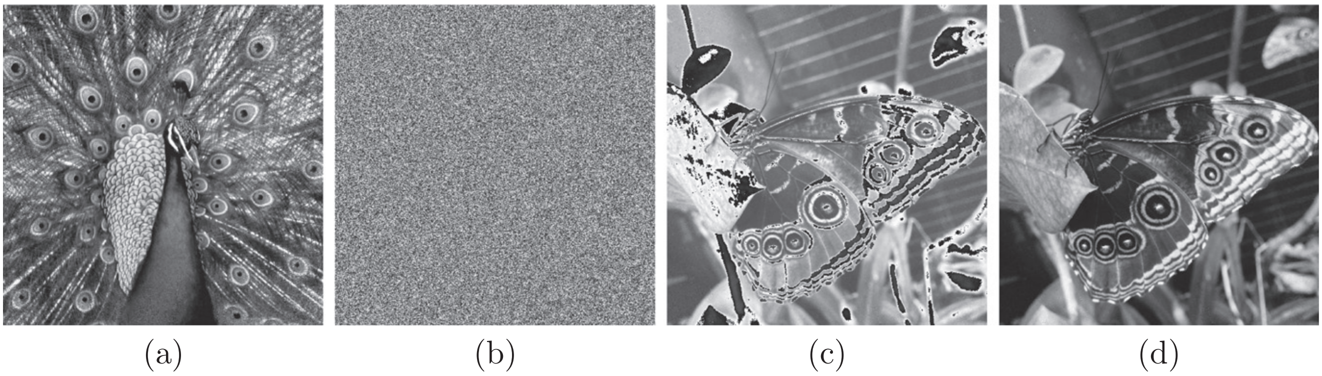

Figure 3. Simulated results: (a) reconstructed amplitude, (b) reconstructed phase modulated by the initial diffuser D, (c) modulo-2π phase as in (b) but with this diffuser removed (correct security key), and (d) unwrapped version of (c).

and recorded intensity is sufficiently small. At this point the complex ciphertext has been successfully recovered; finally, a by using the first or last variable focal length (depending on where the algorithm is truncated), VOS is used to decode the initial message.

3. Simulated and experimental results

In order to test the proposed encoding system, numerical simulation were carried on. Figure 1(a) shows the optical scheme: a collimated beam CB ($\lambda = 635$ nm) illuminates the input plane; in the simulation, the initial data at O are represented by amplitude (peacock) and phase (butterfly) images—figures 2(a) and (b), respectively. The complex object is modulated by a random diffuser D (figure 2(c)) acting as security key for encrypting (decrypting) the phase data. The outgoing wavefront is collected by a focus tunable lens f_v (at $z_o = 12$ mm); then, after a free-space propagation of $z_r = 45$ mm, the encrypted data are registered at the plane E. Figure 2(d) shows a zoom in of a single pattern from a set of ten images, $\{I_0, I_1, ..., I_9\}$, produced by the following focal length values $f_v = 103.7$, 96.9, 91.6, 87.2, 83.6, 80.5, 77.9, 75.5, 73.7 and 72.0 mm. Applying the decryption process over the delocalized ciphertext, we obtain the original message: amplitude and phase, figure 3—recovered phase after removing the diffuser is in modulo 2π in (c), and it is unwrapped in (d). With the introduction of a delocalized ciphertext (and the knowledge of the optical parameters), a successful decryption of the information encoded in amplitude is obtained; since the random diffuser D only randomly shuffles the phase, it plays no active role on the amplitude encryption. Otherwise, the phase can only be decoded using a virtual replica of the diffuser—and the optical parameters. Notice that the proposed system has the inherent advantage of restricting an access level to part of the encrypted

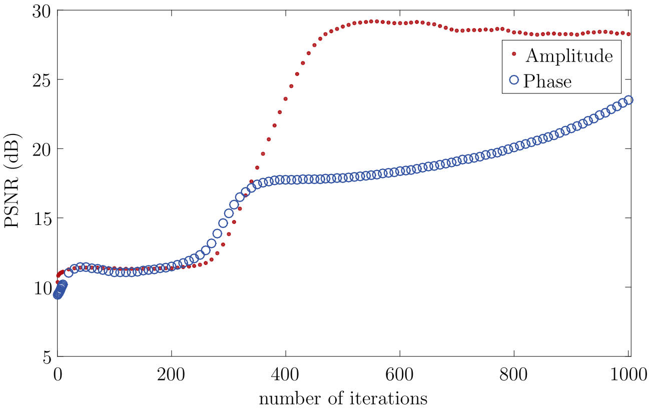

Figure 4. PSNR dependence, of phase and amplitude, versus the number of iterations performed with the proposed decryption algorithm (Movie 01 shows full convergence of decrypted information, amplitude and phase).

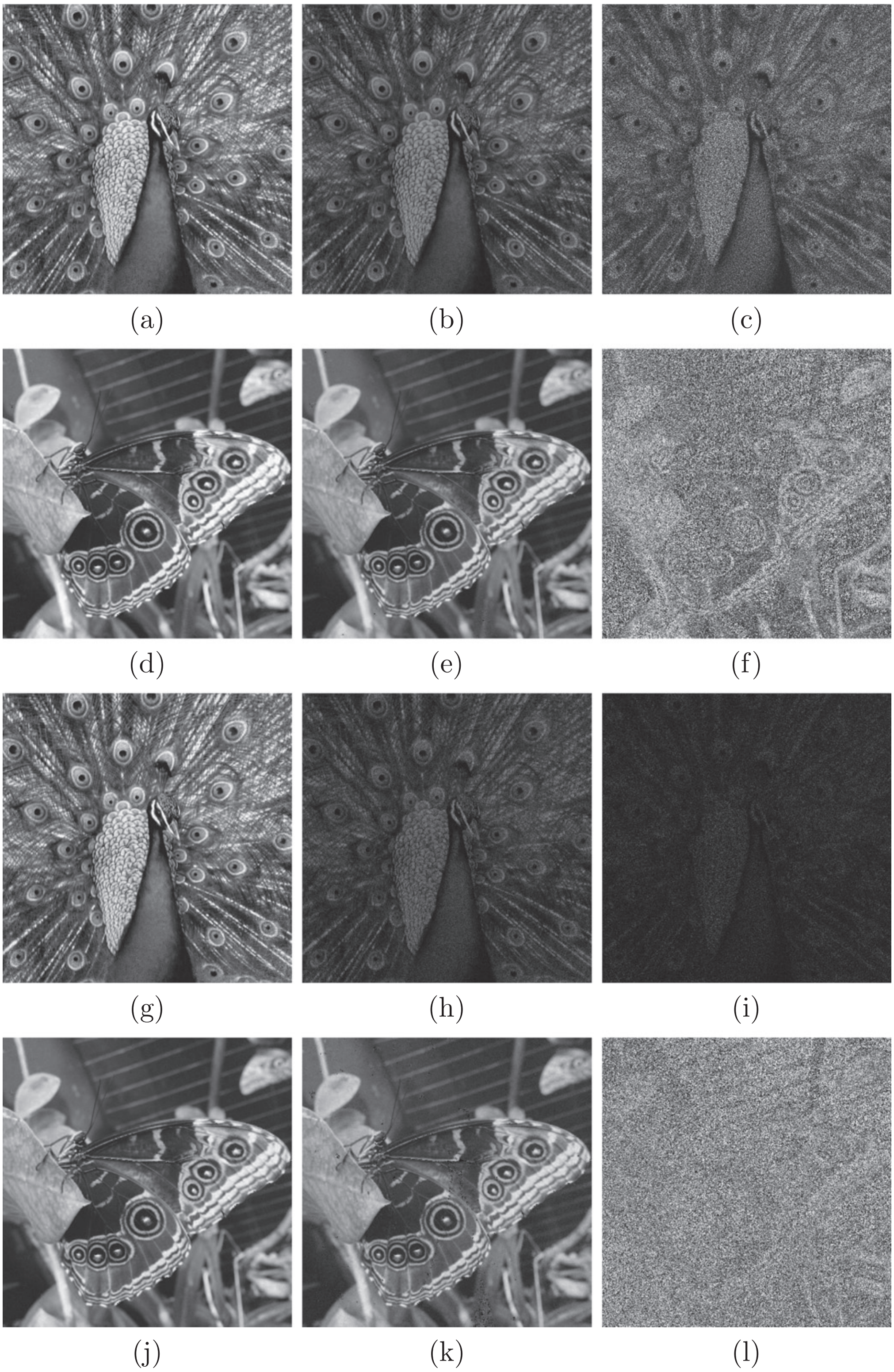

Figure 5. Robustness test for information loss. Decrypted amplitude and phase for a 50% occlusion for one delocalized cyphertext, (a) and (d), respectively; (b) and (e) for two; (c) and (f) for three. Decrypted amplitude and phase for a 90% occlusion for one delocalized cyphertext, (g) and (j), respectively; (h) and (k) for two; (i) and (l) for three.

information. Henceforth, this access level can be used as watermark, digital signature or other means of authentication.

As a measure of the performance, figure 4 shows the convergence in amplitude and phase under the decoding procedure, using an accurate conjugation of optical parameters, ciphertext, and encrypting key. The *peak signal-to-noise ratio* (PSNR) is calculated as a quality measure on the decrypted images (in phase and amplitude). This performance

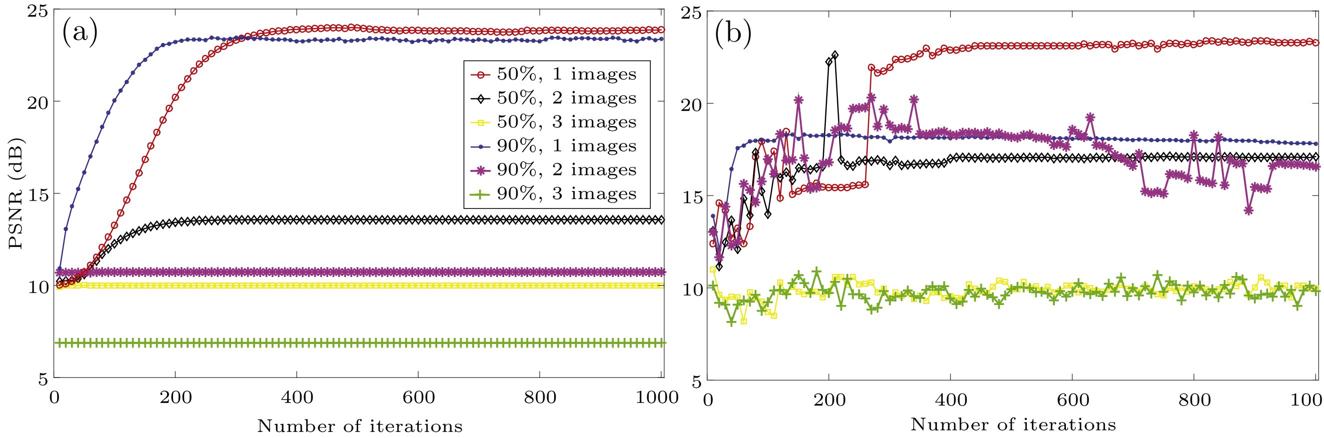

Figure 6. Quality of the decrypted images. PSNR for the amplitude (a) and phase (b) in terms of the number of iterations of the reconstruction algorithm.

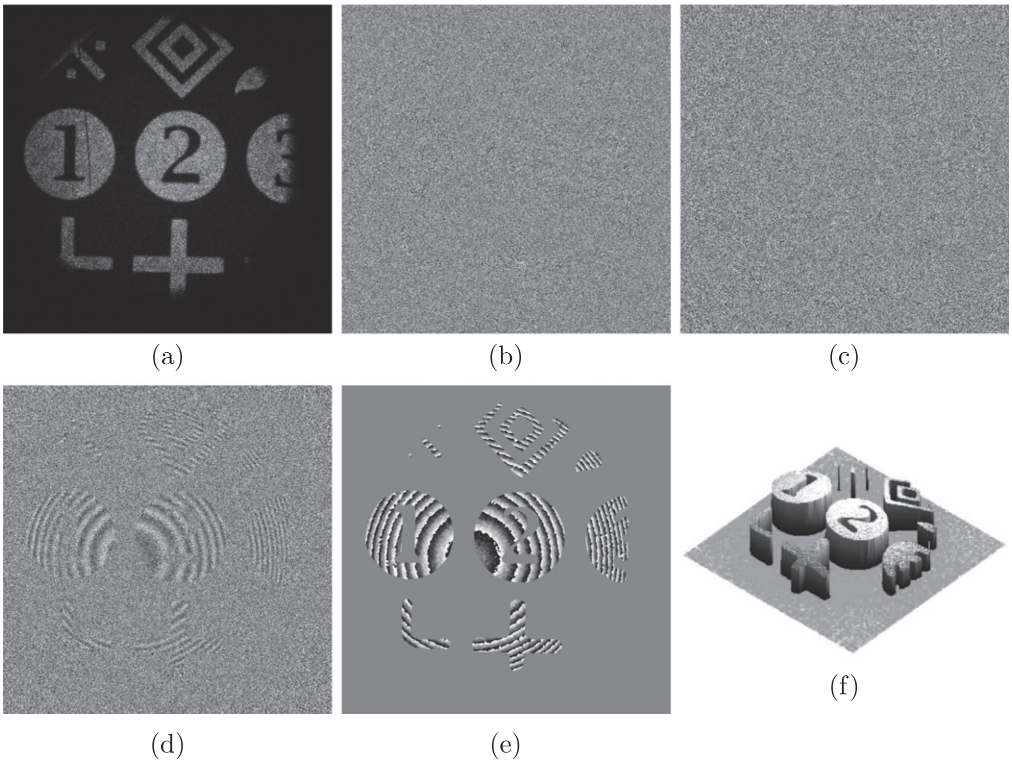
(a) (b) (c)
(d) (e) (f)

Figure 7. Experimental results. (a) Amplitude decrypted, (b) reconstructed phase which is modulated by the initial diffuser D, (c) diffuser D, (d) phase in modulo 2π retrieved by using (b) and (c), (e) phase modulo 2π filtered, (f) phase decrypted and unwrapped.

matches experimental results previously reported in [24, 25] for the phase. Moreover, we studied the robustness of the system simulating information loss by partially occluding some of the image set composing the delocalized cyphertext. For this test, we used a set of 15 images as cyphertext with the purpose of a faster convergence. That is, using less iterations of the phase retrieval algorithm. Figure 5 shows reconstructions to the original complex field (phase and amplitude). The system is tolerant to information loss in one or two images but loss in more images favours the noise contamination present in the reconstruction, see figure 6. The robustness to this test is due to the decreasing exponential distribution of the grey levels forming the speckle pattern—the occlusion is more likely to occur in the dark regions of the field. There exists an equivalence between the speckle patterns produced by the focus tunable lens at the plane of the CCD sensor and those registered at different positions in a free-space propagation. Therefore, the resistance to brute-force attacks of this architecture is analogous to the one appearing in [24]. Otherwise, the security will be compromised, like in other conventional systems [11–18], if an intruder has access to a subset of images belonging to the cyphertext and the optical parameters sent by different transmission channels as discussed in [24, 25]. Consequently, this system is more secure than conventional holographic systems.

Additionally, the validity of this proposal was experimentally verified. Following figure 1(a), the arrangement consists of a binary mask (numbers and simple shapes), a diffuser (GRIT 220), and an electrically focus tunable lens (Optotune EL-10–30-VIS-LD)—its focal length dependence with the applied current was determined through a SH wavefront sensor. In this case, by illuminating with a convergent beam we introduce a quadratic phase as part of the message (produced by a THORLABS LA1708 lens, $\lambda = 635$ nm). The distances z_o and z_r were set to 10 and 28 mm, respectively. A set of ten intensities of delocalized ciphertext were produced by setting the focal length values of $f_v = 104.9, 99.3, 94.4, 90.2, 86.5, 83.2, 80.3, 77.6, 75.3$, and 73.0 mm. These intensities were registered with a CMOS camera (JAI CM-200 GE, 8 bit monochrome, $4.4 \times 4.4\ \mu\text{m}^2$ pixel size). Once these images are saved to a memory device, the encrypted message is ready to be sent; thus, the recipient must have the optical parameters to retrieve the intensity of the object (focal length values $\{f_0, f_1, ..., f_{N-1}\}$ and distances z_o and z_r), and the encrypting key to recover the phase. The decoded information from the amplitude and phase is shown in figure 7. PSNR value for the recovered complex amplitude is 22.73 dB (here the noise of the amplitud mask is reduced by filtering it out before evaluating). In particular, the phase is decrypted by compensating with the diffuser acting as encrypting key—modulo 2π and unwrapped phase are in figures 7(d)–(f). To test the success in the decryption of the phase, the focal length is estimated from the obtained phase. A value of 198.6 mm ($\pm 1\%$) is obtained, which is in agreement with the value given by the manufacturer—differences are due to collimation and positioning errors (the lens has a tabulated back focal value of 197.5 mm).

4. Conclusions

Throughout this work, we have introduced a new encoding architecture by a single random phase diffuser based on a focus tunable lens and a phase retrieval method. We have validated it with simulations and experimental results. An effective phase retrieval algorithm is applied over subjective speckle intensity distributions produced to a high rate by a focus tunable lens. This set of speckle distributions constitutes a delocalized ciphertext which, together with distance parameters, allow us to decrypt data transmitted in amplitude and phase—the latter still modulated by the initial diffuser. On the sender side, the focus tunable lens is able to produce an optimal succession of subjective speckles at high rates (our model has a latency time of 25 ms), and this succession can be recorded accordingly by a high-speed camera; while on the recipient side, the reconstruction algorithms work as fast as holographic techniques. Henceforth, the lack of reference beams eliminates one of the main vulnerability issues of the (linear) encryption systems. Moreover, the use of a focus tunable lens provides a secure compact encrypting architecture.

Acknowledgments

FM and DGP were supported by Comisión Nacional de Investigación Científica y Tecnológica (CONICYT, FONDECYT Postdoctoral Grant No. 3130433, FONDECYT Grant No. 1100895, Chile), partially by Pontificia Universidad Católica de Valparaíso (PUCV, Grant No. 123.731/2014, Chile). NB was supported by Consejo Nacional de Investigaciones Científicas Técnicas (CONICET, Grant No. 112-200801-00863, Argentina), and Facultad de Ingenieŕia, Universidad Nacional de La Plata (UNLP, Grant No. 11/I168, Argentina).

References

[1] Goodman J W 2004 *Introduction to Fourier Optics* 3rd edn (Greenwood Village: Roberts and Company)

[2] Refregier P and Javidi B 1995 Optical image encryption based on input plane and Fourier plane random encoding *Opt. Lett.* **20** 767–9

[3] Unnikrishnan G, Joseph J and Singh K 2000 Optical encryption by double-random phase encoding in the fractional Fourier domain *Opt. Lett.* **25** 887–9

[4] Hennelly B and Sheridan J T 2003 Optical image encryption by random shifting in fractional Fourier domains *Opt. Lett.* **28** 269–71

[5] Tao R, Xin Y and Wang Y 2007 Double image encryption based on random phase encoding in the fractional Fourier domain *Opt. Express* **15** 16067–79

[6] Tao R, Lang J and Wang Y 2008 Optical image encryption based on the multiple-parameter fractional Fourier transform *Opt. Lett.* **33** 581–3

[7] Matoba O and Javidi B 1999 Encrypted optical memory system using three-dimensional keys in the Fresnel domain *Opt. Lett.* **24** 762–4

[8] Situ G and Zhang J 2004 Double random-phase encoding in the Fresnel domain *Opt. Lett.* **29** 1584–6

[9] Nelleri A, Joseph J and Singh K 2007 Digital Fresnel field encryption for three-dimensional information security *Opt. Eng.* **46** 045801–8

[10] Chen W, Chen X and Sheppard C J R 2012 Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain *Opt. Express* **20** 3853–65

[11] Carnicer A, Montes-Usategui M, Arcos S and Juvells I 2005 Vulnerability to chosen-ciphertext attacks of optical encryption schemes based on double random phase keys *Opt. Lett.* **30** 1644–6

[12] Peng X, Wei H and Zhang P 2006 Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain *Opt. Lett.* **31** 3261–3

[13] Peng X, Zhang P, Wei H and Yu B 2006 Known-plaintext attack on optical encryption based on double random phase keys *Opt. Lett.* **31** 1044–6

[14] Gopinathan U, Monaghan D S, Naughton T J and Sheridan J T 2006 A known-plaintext heuristic attack on the Fourier plane encryption algorithm *Opt. Express* **14** 3181–6

[15] Frauel Y, Castro A, Naughton T J and Javidi B 2007 Resistance of the double random phase encryption against various attacks *Opt. Express* **15** 10253–65

[16] Kumar P, Kumar A, Joseph J and Singh K 2009 Impulse attack free double-random-phase encryption scheme with randomized lens-phase functions *Opt. Lett.* **34** 331–3

[17] Wang X and Zhao D 2013 Amplitude-phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a random amplitude mask *Opt Lett.* **15** 3684–6

[18] Nakano K, Takeda M, Suzuki H and Yamaguchi M 2014 Security analysis of phase-only DRPE based on known-plaintext attack using multiple known plaintext–ciphertext pairs *Appl. Opt.* **53** 6435–43

[19] Hwang H E, Chang H T and Lie W N 2009 Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain *Opt. Lett.* **34** 3917–9

[20] Deng X and Zhao D 2011 Single-channel color image encryption using a modified Gerchberg-Saxton algorithm and mutual encoding in the Fresnel domain *Appl. Opt.* **50** 6019–25

[21] Chen W and Chen X 2011 Optical image encryption using multilevel Arnold transform and non-interferometric imaging *Opt. Eng.* **50** 117001

[22] Huang J, Hwang H, Chen C and Chen M 2012 Lensless multiple-image optical encryption based on improved phase retrieval algorithm *Appl. Opt.* **51** 2388

[23] Chen W, Chen X, Anand A and Javidi B 2013 Optical encryption using multiple intensity samplings in the axial domain *J. Opt. Soc. Am.* A **30** 806–12

[24] Mosso F, Peters E, Bolognini N, Tebaldi M, Torroba R and Pérez D G 2013 Experimental imaging coding system using three-dimensional subjective speckle structures *J. Opt.* **15** 125403

[25] Mosso F, Bolognini N and Pérez D G 2015 Experimental optical encryption system based on a single-lens imaging architecture combined with a phase retrieval algorithm *J. Opt.* **17** 065702