Experimental imaging coding system using three-dimensional subjective speckle structures

2013 J. Opt. 15 125403

(http://iopscience.iop.org/2040-8986/15/12/125403)

IOP Publishing Journal of Optics
J. Opt. 15 (2013) 125403 (6pp) doi:10.1088/2040-8978/15/12/125403

Experimental imaging coding system using three-dimensional subjective speckle structures

F Mosso[1], E Peters[1], N Bolognini[2,3], M Tebaldi[3], R Torroba[3] and D G Pérez[1]

[1] Instituto de Física, Facultad de Ciencias, Pontificia Universidad Católica de Valparaíso (PUCV), Avenida Brasil 2950, 23-40025 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 Ingeniera, UNLP), PO Box 3, 1897 M B Gonnet, Argentina

E-mail: edward.mosso@ucv.cl

Received 27 June 2013, accepted for publication 27 September 2013
Published 29 October 2013
Online at stacks.iop.org/JOpt/15/125403

Abstract
We propose, and experimentally demonstrate, an optical encoding system employing a three-dimensional subjective speckle distribution as a secure information carrier. An image mask (containing the information to be sent) is illuminated by randomly distributed light. The outgoing wavefront reaches a lens, and thus three-dimensional subjective speckle distributions are generated in the normal direction of the scattering plane. These speckle structures are sampled by registering consecutive planes along the optical axis with a complementary metal-oxide semiconductor camera. Along with the optical parameters (keys), these intensity patterns are sent through independent channels to a receiver. By replicating the original system with the keys and implementing a single-beam multiple-intensity reconstruction, we show that the message recipient needs a minimum set of speckle images to successfully recover the original information. Moreover, intercepting a partial set of speckle images with the keys may not result in a successful interception.

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

S Online supplementary data available from stacks.iop.org/JOpt/15/125403/mmedia

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

1. Introduction

Optical cryptography provides many degrees of freedom to protect and interdict unauthorized distribution of information. Since the early introduction of double random phase encoding [1], optical encryption methods have been widely proposed for information protection and secure data transmission. Most of these have employed the interference between the complex fields diffracted by the object and reference beam as a method to retrieve an accurate wavefront reconstruction in the image decryption procedure (see [2] and references therein). Nevertheless, these methods are quite sensitive to system instabilities or environment perturbations; therefore, any perturbation may preclude a successful decryption. To overcome these limitations, optical metrology has resorted to *in-line* holographic systems. Indeed, by recording multiple holograms (irradiance distributions) at different propagation planes, the original object can be retrieved with less degradation. The use of an iterative algorithm to perform the field propagation between successive planes is essential to the technique [3]. Recently, Chen *et al* [4] have proposed an encrypting system based on this principle.

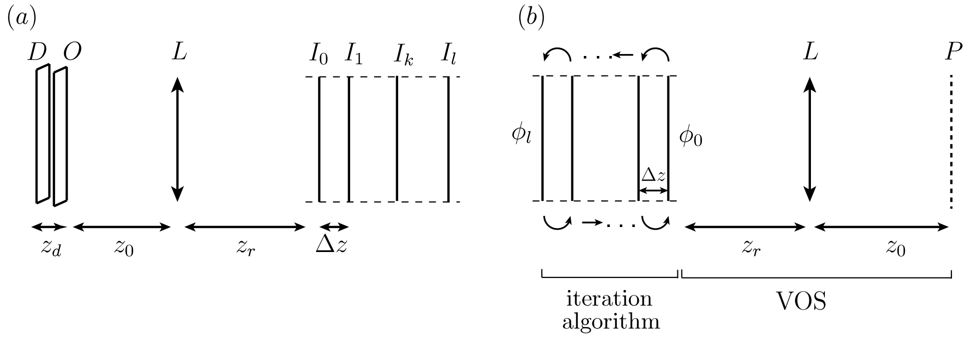

Figure 1. (a) Optical coding system: z_d is the separation between the diffuser, D, and mask, O; the latter is separated a distance z_0 from the lens, L, and the recording initial position is z_r. (b) Virtual decoding system.

The original object (the message) was encrypted by three phase masks through free-space propagation, and then the irradiance of the wavefront field was registered at three different positions. A successful decryption can only be achieved by a receiver having a replica of the phase masks and knowledge of the propagation parameters; they successfully proved this method by numerical simulations. Indeed, random phase modulation has been widely used in optical processing data and metrology [5, 6]. In all these proposals the main feature is the modulation of the wavefront by a diffuser.

However, a low count of registered intensities at the encryption stage may result in long decryption times because the number of iterations required for a successful reconstruction is too high. This particular drawback can be eliminated by significantly enlarging the set of recorded images and simplifying the complexity of the algorithm. This technique, referred to as single-beam multiple-intensity reconstruction (SBMIR), shortens the computation time taking advantage of the three-dimensional speckle distribution created by the original object [7, 8]. Moreover, later revisions [9, 10] have introduced diffusers along the optical path as high spatial frequency discriminators, thus significantly increasing the resolution of wavefront reconstruction.

In this work, we use this fact to implement an experimental encoding system that leaves the information carried by the three-dimensional speckle structure unaffected. This subjective speckle distribution is registered in sequential planes—each one having random features which individually are unable to disclose any information about the original object. This recording procedure, contrary to conventional systems employing holographic records of encrypted data, distributes the information for retrieving the original object into different independent channels. This feature allows one to securely transmit data without employing a second phase mask between the input and image planes as used in conventional methods. In this way there is no risk of finding a common element between multiple encoded data as is found in systems employing a unique second phase mask. It is the three-dimensional speckle structure of the original object that is acts as the coding element and supports the encoding parameters. Proper retrieval of the message is only possible with the knowledge of the encoding parameters and access to a significant number of consecutive speckle images.

2. Experimental encoding

The encoding procedure begins with a given message translated into a transmittance mask, O, an image. Then the information present in this mask is modulated by the speckled field produced by a collimated coherent beam illuminating a ground glass diffuser, D. The outgoing wavefront propagates freely until it reaches a positive lens, L, with focal length f. Finally, a camera samples a number of intensity patterns $(I_0, I_1, \ldots, I_k, \ldots, I_l)$ at equidistant planes, separated by Δz increments, figure 1. The encoding stage ends at this point. The addition of a lens is critical, as expected, and different messages produce different average aperture sizes in the mask; therefore, by adjusting z_0 and z_r, it is always possible to select adequate longitudinal and transverse speckle sizes to give a successful reconstruction for any message. For instance, free-space propagation setups lack this flexibility: small objects at O impose short distances to the initial image plane, I_0, thus limiting our ability to transmit a given message.

The message has been modulated on l speckle distributions, and it is apparently lost in each single-intensity pattern; nevertheless, the collection of these successive images with the addition of the optical setup parameters allow the existence of a recovery mechanism. The information contained in the complex field is decentralized, and thus it is sent through l independent channels. The receiver implements a *virtual optical system* (VOS) to retrieve the message using the optical parameters as decoding keys. The free-space propagation of any field inside the VOS is performed by a discrete version of the angular spectrum formalism, and the lens is modeled after the usual quadratic phase. For the purpose of recovering the wavefront phase, the SBMIR algorithm, described in detail by Almoro *et al* [8], is implemented between the successive speckle intensity planes. Initially, the complex field $U_0 = I_0^{1/2}e^{j\phi_0}$, with $\phi_0 = 0$, is propagated to the next plane giving U_1. But at this position the true amplitude is provided by I_1, then the field $I_1^{1/2}e^{j\phi_1}$ is built with phase $\phi_1 = \arg U_1$. This operation is sequentially repeated between adjacent image planes until the last plane l is reached. Then the propagation goes backwards with initial field $I_l^{1/2}e^{j\phi_l}$ until it reaches the initial plane (see figure 1(b)). Therefore, a new iteration may begin with a corrected initial phase, $\phi_0 = \arg U_0$. By iterating this procedure the phase at

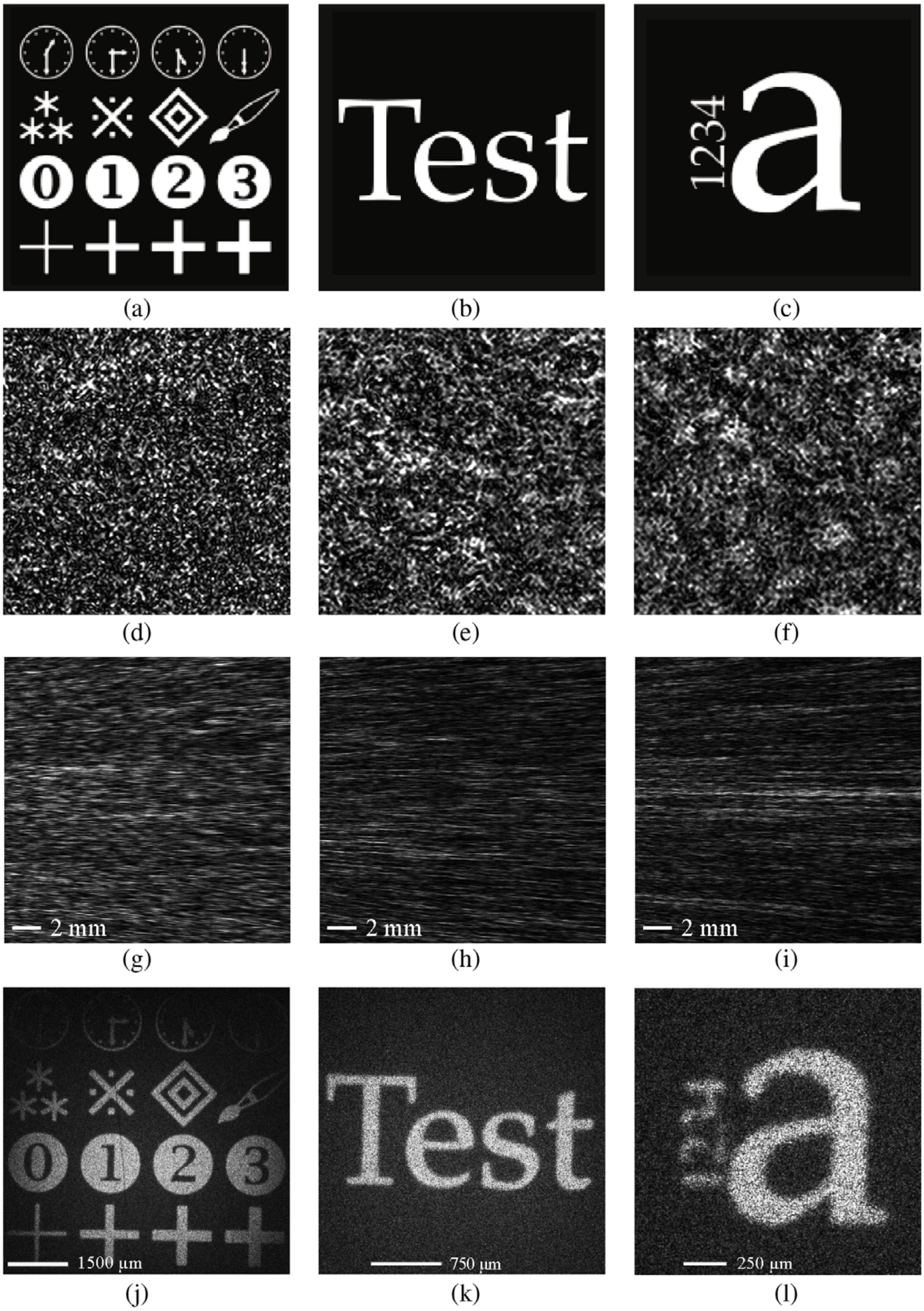

Figure 2. (a)–(c) The original objects, (d)–(f) speckle patterns depicted at the first plane for the initial objects and (g)–(i) longitudinal speckle distribution along the measurement distances. Parts (j)–(l) show the decoded images.

$l = 0$ converges to its real value. Finally, the last step consists of backward propagation through the VOS to properly retrieve the original image mask, P.

We performed an experiment to determine under which conditions the encoding–decoding procedure can successfully deliver a message. It was performed with three objects of sizes 7.5×7.5, 3.25×3.25 and 2×2 mm^2 (figures 2(a), (b) and (c), respectively). We used a 635 nm collimated laser beam with a spot diameter of 6.5 mm to illuminate a 220-grit ground glass diffuser. The $f = 50$ mm lens used in the encoding–decoding is at $z_0 = 20$ mm from the image mask and $z_r = 60$ mm from the first image plane,

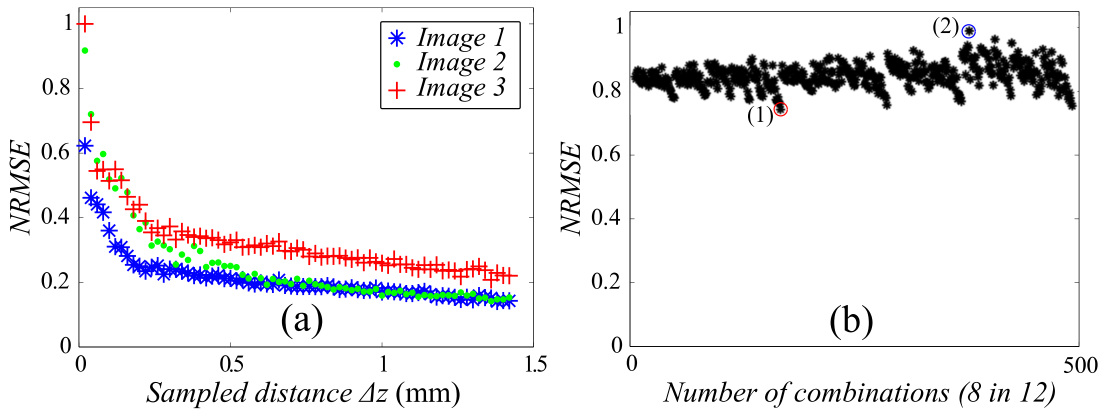

Figure 3. Reliability of the coding system.

while the separation between diffuser and object is $z_d = 10$ mm. An 8-bit monochromatic complementary metal-oxide semiconductor camera (JAI CM-200 GE, 4.4×4.4 μm^2 pixel size) is employed to record 1000 images for each mask. The camera is displaced by $\Delta z = 20$ μm between each plane by a motorized linear translation stage (Thorlabs PT1/M-Z8). An estimate of the average speckle size can always be calculated from the correlation area of the sampled speckle intensity [11]. Transverse speckle autocorrelations were from 13.2 to 26.4 μm for figure 2(a), from 15.4 to 19.8 μm for figure 2(b) and from 39.6 to 41.8 μm for figure 2(c) (illustrated in figures 2(d)–(f)). Longitudinal speckle autocorrelation gave (g) 0.98, (h) 1.87 and (i) 2.72 mm for the objects labeled as in figures 2(a)–(c). Observe that the transverse and longitudinal speckle distribution changes according to the shape of the illuminated object. In particular, the images in figures 2(f) and (i) show an irregular distribution of speckle sizes because they are composed of objects with quite dissimilar sizes—different coherence areas are present. By manipulating the distances z_d, z_0 and z_r and the lens aperture (size and shape) it is possible to control the three-dimensional sizes of speckle grains. Therefore, subjective speckle distributions on the camera can be achieved without significantly degrading the object resolution. For

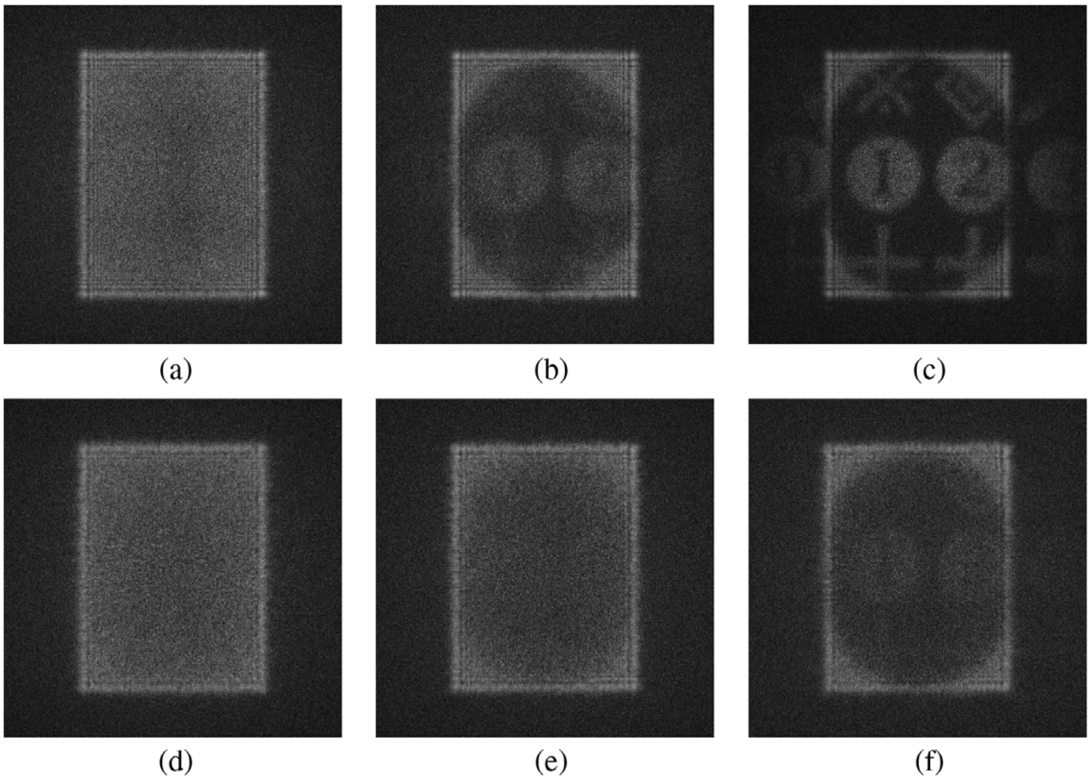

Figure 4. Reconstructed images by using a subset of six (a), seven (b) and eight (c) consecutive images from 12; each image from (d) to (f) corresponds to reconstructions from the same number of non-consecutive images.

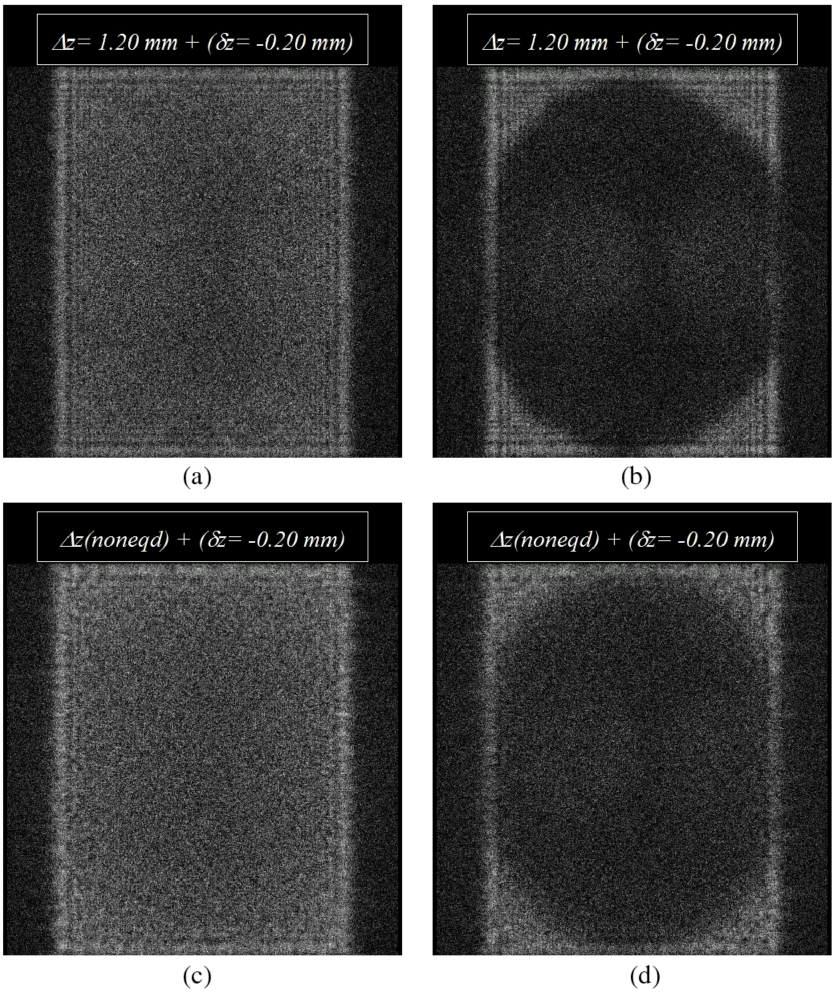

Figure 5. Message recovery with error in the separation between speckle image planes ($\Delta z + \delta z$) for: (a) six and (b) eight consecutive planes (media 4 and 5 available at stacks.iop.org/JOpt/15/125403/mmedia) and (c) six and (d) eight non-consecutive planes (media 6 and 7 available at stacks.iop.org/JOpt/15/125403/mmedia).

instance, by setting z_d to values near zero, the diffuser will only modulate the phase, leaving the complex amplitude almost unchanged. Then, the contribution of the amplitude module to the reconstruction is depreciated, and the receiver can recover the original information with less degradation.

A hypothetical receiver needs at least eight speckle distribution images to properly decode the message using the retrieval procedure and the VOS simulating the encoding architecture; fewer images than this leads to poor-quality (with seven speckle images) or illegible (with six or less) reconstructions. Figures 2(j)–(l) exemplify high quality reconstructions achieved from 15 images displaced by $\Delta z =$ 1.24 mm and 20 iterations of the phase retrieval algorithm. The mask dimensions in the retrieved image were verified experimentally, and coincide with their original size. The quality of the recovery processes is measured by the normalized root mean square metric (NRMSE): this evaluates the likeness of the reconstruction against the original. For instance, the accuracy in the retrieval process reaches a quasi-asymptotic value of NRMSE for a distance separation between consecutive images of more than 1 mm. Figure 3(a) shows the NRMSE versus Δz ranging from 20 μm to 1.42 mm (by increments of 20 μm. Supplementary video files (media 1, 2, and 3 available at stacks.iop.org/JOpt/15/125403/mmedia) for sample objects in figures 2(a)–(c) are provided to illustrate the improvement in the reconstruction with Δz. Subjectively, low quality reconstructions are found for inter-plane separations below 200 μm, average quality is reached for 200 μm $< \Delta z <$ 400 μm, and good to high quality above 400 μm. Also, to inspect the robustness of the coding system, we analyzed the quality of the reconstruction after losing some transmission channels. Since eight speckle image distributions is the minimum necessary to obtain a successful retrieval, we simulated a 12-channel coding system ($l = 12$) where randomly only eight channels survive interference. Then the separation distance between every two speckle distributions is not constant. After simulating all possible combinations of eight successful transmitted images from the 12 speckle distributions, we have found degraded reconstructions with speckle noise influence as a result of using non-consecutive sets. However, the use of sets of sequential recorded images produced the lowest NRMSE values, indicating reconstructions with a small influence of speckle noise. Figure 3(b) illustrates this observation, and the points labeled as (1) and (2) correspond to the reconstructions shown in figures 4(c) and (d), respectively.

Finally, the robustness and security of this coding system against eavesdropping by a third party can be tested by simulating a reconstruction with incomplete information. Consider a message transmitted through 12 channels, and a malicious attacker recovering only six, then seven and finally eight channels, randomly chosen from the original 12. The position between each plane at each attack can be consecutive or not; a consecutive arrangement (in the proper order) has a very low probability ($\sim 10^{-8}$) yet it can give a glimpse of the message when seven ordered channels are recovered, and eight or more produce a legible message, figures 4(a)–(c). Non-consecutive, still ordered, channels are more likely ($\sim 10^{-5}$) and yet a strongly noisy image can be recovered by intercepting eight channels (figures 4(d)–(f)). Although more likely, the latter produces unusable information. On the other hand, in the event that the attacker was unable to intercept the optical parameters, consecutive images will have a separation uncertainty δz; thus, the reconstruction of the message will be affected. Indeed, figure 5(a) (media 4 available at stacks.iop.org/JOpt/15/125403/mmedia) shows that reconstruction is impossible under any variation in the separation distance for six consecutive image planes: all reconstructions are illegible. Likewise, eight consecutive planes whose separation is uncertain produces illegible results for the whole tested range but inside a region of radius 300 μm around the right separation (figure 5(b)) (media 5 available at stacks.iop.org/JOpt/15/125403/mmedia). For non-consecutive image planes the noise is too high in any situation to obtain an appropriate reconstruction regardless of the number of image planes (see figures 5(c) and (d)) (media 6 and 7 available at stacks.iop.org/JOpt/15/125403/mmedia). Even for eight non-consecutive planes the reconstruction is practically unrecognizable at the smallest uncertainties.

3. Conclusions

We have experimentally shown that secure message transmission based on SBMIR is possible. By combining this phase retrieval technique with a virtual optical system, the recipient can properly recover the original message from the subjective speckle planes transmitted through multiples channels. The original image mask is unrecovered from a single channel; that is, since each speckle image is seemingly random, just stationary noise can be obtained from one of these without the proper phase information. More than seven channels must be transmitted successfully to produce a low error reconstruction of the original mask; successful transmission of fewer than seven channels will produce only illegible information upon retrieval. These three-dimensional subjective speckle structures are a secure random carrier by themselves, and the speckle distribution planes sent by individual channels protect data under this setup. Each speckle pattern distribution plays the role of both coding information and coding parameter (requiring several of these to recover data). In our scheme each encrypted message is sent through independent channels, unlike conventional ones. This is a huge benefit, since it results in delocalized information transport. As we have shown in figure 5, the main advantage of this procedure is against eavesdroppers fishing for information; they must intercept a set of consecutive images from the multiple transmission channels. Intercepting a set of non-consecutive images will result in poor quality reconstructions (for seven or more) or unrecognizable data (for less than seven channels). Finally, one last remarkable feature is the high quality reconstructions accomplished with this encoding technique. By using an imaging system, longitudinal correlation areas can be controlled to achieve optimal decoding conditions. Moreover, distances and contrast drawbacks can be overcome. In contrast with other opto-digital systems to secure information, the reconstructions provided by this procedure have optimal contrast defining the edges precisely and thus resembling the original data.

Acknowledgments

FM, EP 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 nos. 123.704/2010 and 123.722/2012, Chile). NB, MT and RT were supported by Consejo Nacional de Investigaciones Científicas Técnicas (CONICET, grant no. 112-200801-00863, Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata (UNLP, grant no. 11/I168, Argentina).

References

[1] Refregier P and Javidi B 1995 *Opt. Lett.* **20** 767
[2] Millán García-Varela M S and Pérez-Cabré E 2011 *Optical and Digital Image Processing: Fundamentals and Applications* ed G Cristobal, P Schelkens and H Thienpont (Weinheim: Wiley-VCH Verlag)
[3] Zhang Y, Pedrini G, Osten W and Tiziani H 2003 *Opt. Express* **11** 3234
[4] Chen W, Chen X, Anand A and Javidi B 2013 *J. Opt. Soc. Am.* A **30** 806
[5] Dainty J C 1975 *Laser Speckle and Related Phenomena* (Berlin: Springer)
[6] Bernet S, Harm W, Jesacher A and Ritsch-Marte M 2011 *Opt. Express* **19** 25113
[7] Pedrini G, Osten W and Zhang Y 2005 *Opt. Lett.* **30** 833
[8] Almoro P, Pedrini G and Osten W 2006 *Appl. Opt.* **45** 8596
[9] Almoro P F, Pedrini G, Gundu P N, Osten W and Hanson S G 2011 *Opt. Lasers Eng.* **49** 252
[10] Anand A, Chhaniwal V and Javidi B 2011 *J. Biomed. Opt.* **16** 060503
[11] Goodman J W 2007 *Speckle Phenomena in Optics: Theory and Applications* (Greenwood Village, CO: Roberts & Co.)