IOP Publishing Journal of Optics
J. Opt. 19 (2017) 055704 (8pp) https://doi.org/10.1088/2040-8986/aa6526

Innovative speckle noise reduction procedure in optical encryption

Alejandro Vélez Zea[1], John Fredy Barrera[2] and Roberto Torroba[1,3]

[1] Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) CC N° 3, C.P 1897, La Plata, Argentina
[2] Grupo de Óptica y Fotónica, Instituto de Física, Facultad de Ciencias Exactas y Naturales, Universidad de Antioquia UdeA, Calle 70 No. 52-21, Medellín, Colombia
[3] UIDET OPTIMO, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina

E-mail: alejandrov@ciop.unlp.edu.ar

Received 1 December 2016, revised 5 February 2017
Accepted for publication 7 March 2017
Published 4 April 2017

Abstract

Encrypting techniques are currently of interest in the optical domain. A common issue when using coherent techniques is speckle noise which influences the final results. Most efforts to solve this issue were directed towards processing the output of the systems. Instead, we present an alternative approach where we seek to control the input to enhance the performance of these techniques. In particular, we analyze an encoding procedure with a joint transform correlator architecture as a case study. We first demonstrate the dependence of the output noise on the spatial distribution of the input, showing the existence of a neglected random correlation noise which contributes to the degradation of the output. We then propose a rearrangement of the input that results in a reduction of the noise level in the outcome. This rearrangement consists of separating the pixels of the input by introducing black pixels between them, keeping the usual remaining procedure unaltered. Our experimental approach opens up new possibilities for the applications of optical security techniques beyond the limitations imposed by noise.

Keywords: optical encryption, speckle, noise

1. Introduction

The existence of noise in coherent optical processing is generally related to speckle patterns. Speckle appears whenever highly coherent light is scattered by diffuse media. Applications in optical security involve speckle patterns from which information must be extracted [1–4], as well as in optical metrology [5, 6], digital holography [7] and ghost imaging [8]. Besides, it was remarked in a recent contribution [1] that decryption noise is one of the main issues optical security must address in the future. In cryptosystems, problems usually take the form of a low signal to noise ratio of the information extracted from the decryption. This low signal to noise ratio is a common problem for correlations of speckle or other statistically random patterns, whose solution is of great importance in order to validate many applications.

There are a large variety of optical encryption systems, most of them are inspired by the double random phase encryption (DRPE) technique, or include the use and generation of random or quasi-random phase masks and amplitude distributions. Some recent examples include an encryption setup based on phase truncation in the Fresnel domain [9], the use of random intensity masks as keys with encoding into phase only masks [10], scanning with Fresnel telescope imaging [11], single pixel detection [12], methods based on three-dimensional space [13] or encryption of three-dimensional objects [14] and correlated photon imaging [15], among others. These novel techniques offer an increase in the security or in the flexibility over the basic DRPE schemes; however, in most of them, the decryption step involves the correlation between random functions and results in noisy outputs. Among the efforts to deal with this problem we find a non-linear modification of the decryption setup consisting of dividing the cyphertext by the key intensity prior to decryption [16], the use of Fresnel [17] or fractional transforms [18].

Additionally, depending on the input, the noise after decryption can cause the loss of small details, leading to the inclusion of techniques where the input is encrypted by pieces, taking advantage of the fact that each piece would be simpler and less affected by noise [19]. The individual pieces

can be multiplexed into a single cyphertext that when recovered can result in a vast improvement in the decryption quality. However each piece must be processed individually, increasing the time and effort required to obtain the encrypted data.

Finally, Barrera *et al* presented a way to overcome the noise problem by introducing the concept of an 'information container' [20, 21]. In their work, they codified the message to be encrypted into a QR code. The QR code was then optically encrypted in a DRPE setup. After decryption, the code would remain readable despite the noise introduced in the procedure, allowing the noise-free recovery of the original message. A variety of contributions adapted this approach, like the combination of optical encryption with a scrambling technique to increase the security of the process [22], multiplexing and retrieval of noise-free messages [23], the experimental implementation of incoherent optical encryption [24], grayscale encryption [25] and validation [26]. A recent contribution presents the proposal and the experimental demonstration of a tailor-made information container for optical security. The contribution presents a simpler custom code for optical security (CCOS) that can store more information in the same area and is less affected by noise. The CCOS is designed taking into account the features of the optical cryptosystem [27]. Although the information containers allow recovery of the messages free of any kind of degradation, their practical applications remain limited by the restriction in the complexity of the codes that can be successfully encrypted-decrypted and then read.

The noise found in optical encryption involving random patterns has been studied from a statistical point of view, allowing prediction of its behavior to a certain degree and impact in each application [28]. This analysis was applied over the final output; however, so far, besides the container approach, the noise problem has not been studied from the input point of view. That is, to exploit the possibility of rearranging the input spatial distribution into one that is not only more resistant to noise like containers, but one that presents less noise altogether. The dependence between the input distribution and the output noise level is found in a variety of encoding systems, which means that an analogous rearrangement approach can be used to greatly reduce the noise of several applications.

2. Test cryptosystem and random correlation noise description

In order to demonstrate the relation between the output noise and the input in systems correlating random functions, we present as a case study a scheme frequently used in optics for image recognition and security: the joint transform correlator (JTC) [29, 30].

We will analyze the noise problem using the JTC encryption system shown in figure 1. The scheme is an interferometer, where one arm contains the JTC system. In this system, the input consists of two windows, separated by a distance $2b$ that are projected on a SLM placed in the focal plane of a convergent lens. The SLM is in contact with a random phase mask, provided by a ground glass diffuser. In the conjugate plane of the lens, there is a CMOS camera as an intensity recording medium. The CMOS camera registers the intensity of the interference between the Fourier transforms (FTs) of both windows, called the joint power spectrum (JPS). The other arm of the interferometer provides a reference beam.

As shown in figure 1, one of the windows limits the area of the encrypting key, while the other is where the input object is located. Encryption is achieved by blocking the reference beam and registering the JPS of these windows, given by

$$\begin{aligned} JPS(u, v) = {} & |F(u, v)|^2 + |K(u, v)|^2 \\ & + F^*(u, v)K(u, v)\exp(4\pi ibu) \\ & + F(u, v)K^*(u, v)\exp(-4\pi ibu) \end{aligned} \tag{1}$$

where * means complex conjugate, $F(u, v)$ and $K(v, w)$ are the FT of the product of the object $o(x, y)$ by a random phase mask $r(x, y)$ and of the key window $k(x, y)$, respectively. This JPS contains the encrypted information $E(u, v) = F(u, v)K^*(u, v)$, which is extracted and retained with a filtering procedure [22].

The decryption procedure requires knowledge of $K(v, w)$, which is extracted from the hologram resulting from the projection of only the key window in the input of the SLM and then registering the interference of the TF of this window with the reference beam. $K(v, w)$ is then multiplied by the encrypted object, and after performing an inverse Fourier transform, the original object is recovered along a residual noise.

After applying the recovering procedure, the decrypted object $d(x, y)$ is given by

$$d(x, y) = [o(x, y)r(x, y)] \otimes [k^*(x, y) \otimes k(x, y)] \tag{2}$$

where $k(x, y)$ is a random noise function and $\otimes$ is the autocorrelation operator. The autocorrelation of $k(x, y)$ is usually taken as a Dirac delta function by applying the broadband noise approximation [31],

$$[k^*(x, y) \otimes k(x, y)] = \delta(x, y). \tag{3}$$

This approximation is validated under the assumption that the peak of the autocorrelation is much higher than the noise background, and serves to greatly simplify the treatment of many applications. Yet, we note that this background noise severely degrades the output, diminishing the potential use of these applications and therefore must not be neglected. The right way of representing this autocorrelation should be

$$[k^*(x, y) \otimes k(x, y)] = \delta(x, y) + N(x, y) \tag{4}$$

where we assume $N(x, y)$ as a random correlation noise (RCN) whose characteristics will be determined by the statistics of $k(x, y)$.

A large part of the output noise, usually attributed to the speckle inherent to these applications, is in fact due to $N(x, y)$ disregarded when using the broadband noise approximation. In this contribution, we will show that the impact of this last noise to the degradation in the performance of these schemes can be largely eliminated by an object rearrangement.

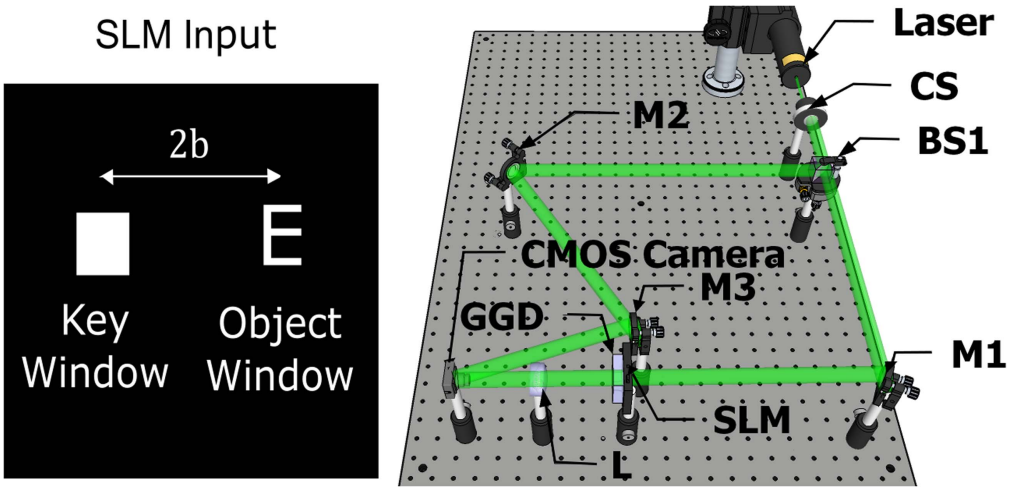

Figure 1. Experimental JTC cryptosystem (SLM: spatial light modulator, CS: collimation system, M: mirror, L: lens, BS: beam splitter, GGD: ground glass diffuser).

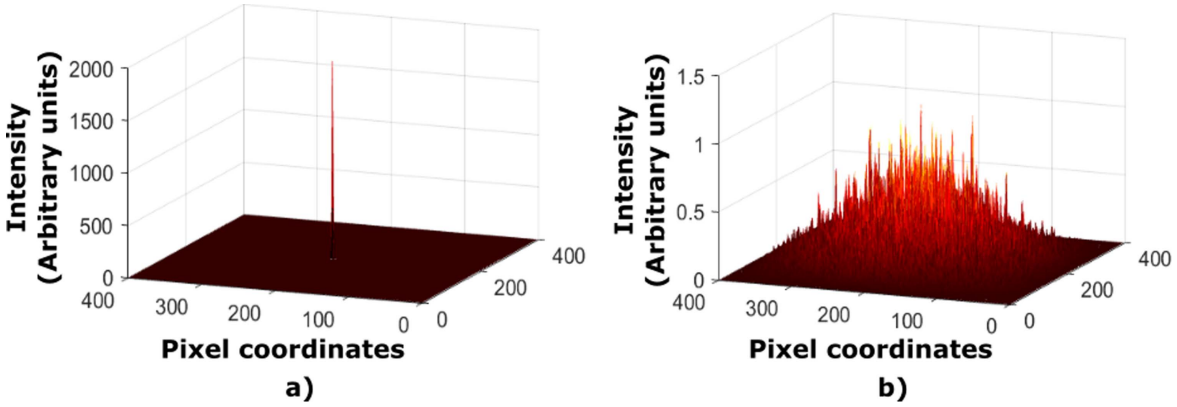

Figure 2. Encoding key autocorrelation (a) with the central peak and (b) when the central peak is suppressed.

Figure 2(a) shows the autocorrelation of a simulated 100×100 pixel random phase mask used as encryption key $k(x, y)$, while in figure 2(b) we show the same autocorrelation after suppressing the central peak.

The RCN (see figure 2(b)) indeed shows a very low intensity compared with the peak of the autocorrelation of $k(x, y)$ (figure 2(a)), which primarily leads to the assumption that the RCN factor is negligible. On the other side, considering that every object can be decomposed into single points, then after decryption each point of the recovered object will be convolved with the RCN function. Consequently, the final reconstruction will show the overlapping of the RCN around each point, thus increasing the total noise intensity and resulting in a significant degradation of the whole decrypted information.

The RCN is centered on each decrypted point and falls off as the distance from the point increases (as can be seen in figure 2(b)). It is expected that an object consisting of spatially separated discrete points will have less overlapping of RCN, and therefore a lower overall noise intensity, resulting an increased reconstruction quality. The simplest way to take advantage of this RCN feature for improving the quality of optical encryption is preparing the inputs prior to encryption. First, the inputs are digitally divided into pixels, then these pixels are separated and finally the space among pixels is filled with black pixels. We then define this proposed method as the pixel separation technique (PST).

3. Numerical results

To show the effectiveness of the PST in reducing the RCN, we encrypted three objects (figures 3(a)–(c)). One of them is a 66 by 66 pixels letter E (figure 3(a)), which is then decrypted. The other two objects are the result of applying the PST to letter E. This is accomplished by introducing black pixels between every pixel of the original object. In our example, we introduce one (figure 3(b)) and two (figure 3(c)) pixels. The resulting objects are also processed by the same encryption-decryption system. We have to note that for visual comparison, all images are scaled to the same size.

In figure 3(d) letter E shows a large amount of surrounding noise after decryption, while as the separation between the pixels increases (figures 3(b) and (c)), the noise level falls (figures 3(e) and (f)). These results demonstrate that the PST leads effectively to a noise reduction. Taking into account these results, we can easily apply the PST to any input object to minimize the amount of noise in the decrypted

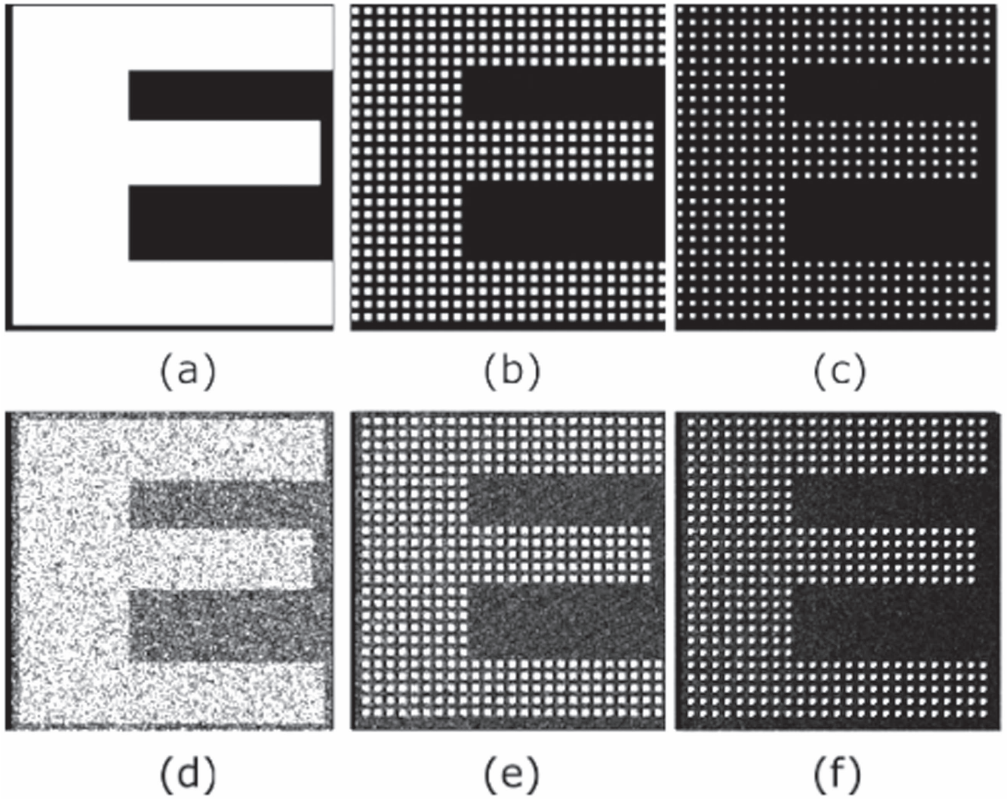

Figure 3. Input objects: (a) 66 × 66 pixel letter E, (b) the same letter with one pixel separation, and (c) with two pixel separation. In (d), (e) and (f) we show the respective decrypted results.

data. After performing this PST, the new inputs are encrypted-decrypted, and the separation can be digitally removed, thus recovering the decrypted object with the same size as the original.

We evaluate quantitatively the technique by measuring the normalized mean square error (NMSE) between the original object before and after the encryption-decryption process with different amounts of pixel separation. The NMSE between the object before encryption-decryption $i(m, n)$, and after $i_p(m, n)$ is defined as

$$NMSE = \frac{\sum_{m,n}^{N,M} |i(m, n) - i_p(m, n)|^2}{\sum_{m,n}^{N,M} |i(m, n) - i_w(m, n)|^2} \quad (5)$$

where (m, n) are the pixel coordinates, $M \times N$ is the number of pixels of the recovered object and $i_w(m, n)$ is the worst expected case (the decrypted object obtained without the PST).

In figure 4 we show that as the pixel separation increases, the error drops abruptly. Furthermore, a small pixel separation is enough to show a significant noise reduction, while larger separations result in smaller subsequent reductions of the NMSE. We explicitly see a dependency on the separation between the pixels in the input, thus confirming our previous assumption about the RCN influence on the output. From the plot we observe a significant noise reduction until a pixel separation value of three. Beyond this point, a further increase in pixel separation does not imply a substantial improvement. As a consequence, it is not necessary to introduce a greater pixel separation to get satisfactory results.

4. Experimental results

We now proceed to test the effects of the pixel separation in an experimental cryptosystem using the scheme of figure 1. We used a CMOS EO-10012C camera, with a pixel size of 1.67 μm × 1.67 μm and 3480 × 2748 pixel resolution. A Coherent (TM) diode pumped solid state (DPSS) laser operating at a wavelength of 532 nm and an output power of 300 mW was employed. The input objects had maximum dimensions of 12.9 mm × 12.9 mm and were projected in a Holoeye 2002 spatial light modulator with 32 μm × 32 μm pixel size. The focal length of the lens was 200 mm. In the experiments the phase masks are provided by a ground glass diffuser.

In figure 5(a) we show three input objects that were processed with our JTC setup, along their respective decrypted results (figure 5(b)), without any alteration on the input. There is a clear degradation of the output in these cases. In figure 5(c) we show the same input with a pixel separation of 2. The resulting decryption can be seen in figure 5(d), showing almost no degradation compared with the respective input and additionally an increased quality compared with the results of figure 5(b).

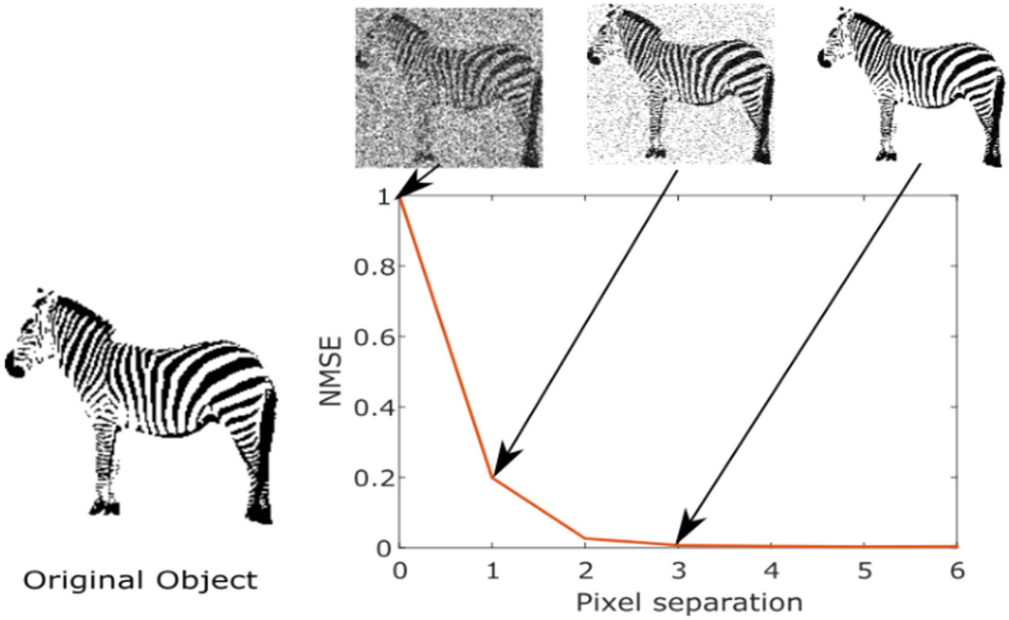

Figure 4. NMSE between the original object before and after the encryption-decryption process with different amounts of pixel separation.

We experimentally demonstrate, by comparing lines (a) and (b) and (c) and (d), the success of implementing the proposed pixel separation technique, where we appreciate a substantial noise reduction over the decrypted images in the last case. The spatial expansion can be reversed by digitally eliminating the added space between pixels in the decrypted objects, as show in figure 5(e). The object shown in the first column corresponds to a plaintext that can be recognized with or without our proposed method, despite the difference in noise. However, this is not the case in the second column, where some details cannot be identified without performing the PST. For the QR code in the third column, containing the message GOF CIOP, only the result of figure 5(e) can be read besides the original code. Although with naked eye the images could be seen as similar, the code reading application is not able to recover the message, including those results with the pixel separation not reversed.

As an additional proof of the PST effectiveness, we now test the resistance to occlusion of the encrypted data with and without PST. We measure the NMSE of the recovered object from a cyphertext with different levels of occlusion, against the result when there is no occlusion. This measurement is performed to the same input with and without PST.

The NMSE curves of figure 6 show that cyphertext resulting from inputs with PST are significantly more resistant to occlusion than those from inputs without PST. This means that PST is not only beneficial to enhance the quality of the recovered data, but also ensures greater resistance to transmission losses, besides allowing high levels of loss compression.

The PST allows a large noise reduction on any kind of input, and can be combined with optical security containers to vastly increase their possible applications. An actual example is the processing of more complex QR codes or other 2D bar codes that contain greater amounts of information. In this sense, the presented technique is a complement to the container concept. It is worth noting that there might be ways of codifying information into containers that directly take advantage of the PST, like the recently introduced CCOS [27], where white blocks containing the message are separated by controllable black regions. Furthermore, since this is an input rearrangement technique, the results can also be improved with methods that alter the decryption step, like the non-linear modification [16], and other general post-processing methods.

5. Conclusions

Optical encoding techniques have great potential; however, as we discuss in this work, their advantages come at the cost of increased noise. In this contribution, we demonstrate the existence of an additional source of noise, so far not considered. Nevertheless, with a simple rearrangement of the input information we obtain a significant noise reduction, while retaining all the other advantages provided by the diffuse media (data security). The results suggest that a specially designed input display with a spatial separation between pixels would produce a great improvement in our case study, thus avoiding the existence of unused pixels. Moreover, this original insight might generate other innovative developments in the optical processing domain. More generally, by sampling regions of a known object with a certain spatial separation, we can also obtain a similar result in those applications where the input cannot be easily manipulated. This can be achieved by using structured illumination [32]. A similar approach could be successfully applied to other optical cryptosystems or any other optical processing technique that relies on the speckle correlation operation where the input signal can be controlled.

Figure 5. Experimental results for noise reduction. (a) Input objects, (b) decrypted objects without PST, (c) spatially expanded inputs with 2 pixel separation, (d) decrypted objects from (c), and (e) after reassembly from (d).

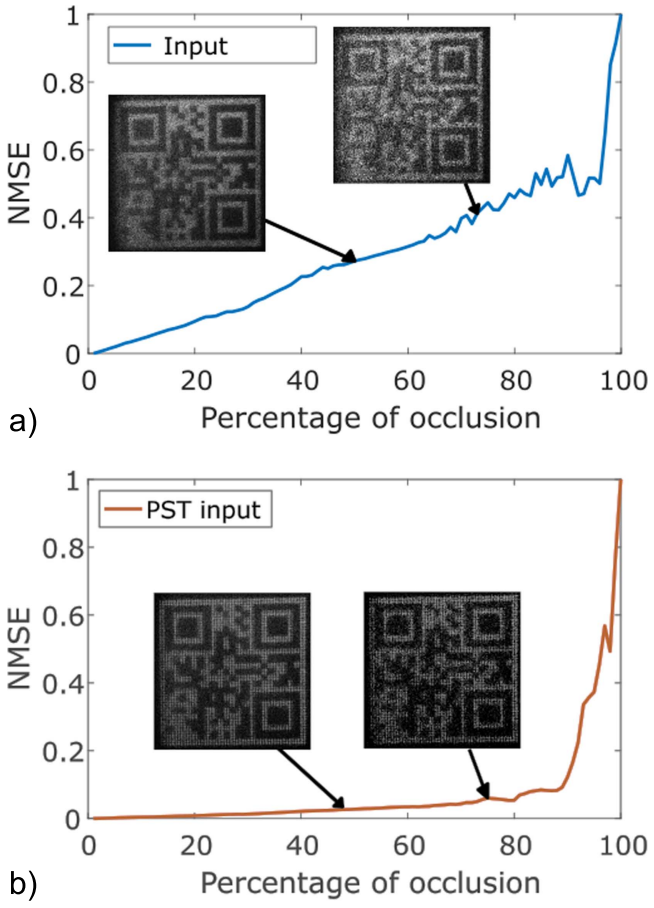

Figure 6. NMSE curve between the decrypted object from a cyphertext without occlusion versus different degrees of occlusion. (a) Input and (b) input with PST.

Acknowledgments

This research was performed under grants from Estrategia de Sostenibilidad 2014-2015 and Comité para el Desarrollo de la Investigación -CODI- (Universidad de Antioquia-Colombia), MINCyT-COLCIENCIAS CO/13/05, CONICET Nos. 0849/16 and 0549/12 (Argentina), and Facultad de Ingeniería, Universidad Nacional de La Plata No. 11/I215 (Argentina). John Fredy Barrera Ramirez acknowledges support from the International Centre for Theoretical Physics ICTP Associateship Scheme.

References

[1] Javidi B *et al* 2016 Roadmap on optical security *J. Opt.* **18** 083001
[2] Wang X, Chen W, Mei S and Chen X 2015 Optically secured information retrieval using two authenticated phase-only masks *Sci. Rep.* **5** 15668
[3] Situ G and Zhang J 2005 Multiple-image encryption by wavelength multiplexing *Opt. Lett.* **30** 1306–8
[4] Graydon O 2013 Cryptography: quick response codes *Nat. Photon.* **7** 343
[5] Berg-Johansen S, Töppel F, Stiller B, Banzer P, Ornigotti M, Giacobino E, Leuchs G, Aiello A and Marquardt C 2015 Classically entangled optical beams for high-speed kinematic sensing *Optica* **2** 864–8
[6] Hanzhong W, Fumin Z, Tingyang L, Balling P, Jianshuang L and Xinghua Q 2016 Long distance measurement using optical sampling by cavity tuning *Opt. Lett.* **41** 2366–9
[7] Kim M K 2013 Full color natural light holographic camera *Opt. Express* **21** 9636–42
[8] Bertolotti J, Putten E G, Ladgendijk A, Vos W L and Mosk A P 2012 Non-invasive imaging through opaque scattering layers *Nature* **491** 232–4
[9] Wang J, Song L, Liang X, Liu Y and Liu P 2016 Secure and noise-free nonlinear optical cryptosystem based on phase-truncated Fresnel diffraction and QR code *Opt. Quant. Electron.* **48** 523
[10] Chen W 2016 Optical cryptosystem based on single-pixel encoding using the modified Gerchberg–Saxton algorithm with a cascaded structure *J. Opt. Soc. Am.* A **33** 2305–11
[11] Aimin Y, Jianfeng S, Zhijuan H, Jingtao Z and Liren L 2015 Novel optical scanning cryptography using Fresnel telescope imaging *Opt. Express* **23** 18428–34
[12] Chen W 2016 Optical data security system using phase extraction scheme via single-pixel detection *IEEE Photon. J.* **8** 7801507
[13] Chen W 2016 Optical multiple-image encryption using three-dimensional space *IEEE Photon. J.* **8** 6900608
[14] Velez A, Barrera J F and Torroba R 2016 Three-dimensional joint transform correlator cryptosystem *Opt. Lett.* **41** 599–602
[15] Chen W 2016 Correlated-photon secured imaging by iterative phase retrieval using axially-varying distances *IEEE Photon. Technol. Lett.* **28** 1932–5
[16] Vilardy J M, Millán M S and Perez-Cabre E 2013 Improved decryption quality and security of a joint transform correlator-based encryption system *J. Opt.* **15** 025401
[17] Barrera J F, Jaramillo A, Velez A and Torroba R 2016 Experimental analysis of a joint free space cryptosystem *Opt. Laser Eng.* **83** 126
[18] Vilardy J M, Torres Y, Millán M S and Perez-Cabre E 2013 Generalized formulation of an encryption system based on a joint transform correlator and fractional Fourier transform *J. Opt.* **16** 125405
[19] Barrera J F, Rueda E, Ríos C, Tebaldi M, Bolognini N and Torroba R 2011 Experimental opto-digital synthesis of encrypted sub-samples of an image to improve its decoded quality *Opt. Commun.* **284** 4350–5
[20] Barrera J F, Mira A and Torroba R 2013 Optical encryption and QR codes: secure and noise-free information retrieval *Opt. Express* **21** 5373–8
[21] Barrera J F, Mira A and Torroba R 2014 Experimental QR code optical encryption: noise-free data recovering *Opt. Lett.* **39** 3074–7
[22] Barrera J F, Vélez A and Torroba R 2014 Experimental scrambling and noise reduction applied to the optical encryption of QR codes *Opt. Express* **22** 20268
[23] Trejos S, Barrera J F and Torroba R 2015 Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval *J. Opt.* **17** 085702
[24] Cheremkhin P A, Krasnov V V, Rodin V G and Starikov R S 2017 QR code optical encryption using spatially incoherent illumination *Laser Phys. Lett.* **14** 026202
[25] Shuming J, Wenbin Z and Xia L 2017 QR code based noise-free optical encryption and decryption of a gray scale image *Opt. Commun.* **387** 235
[26] Wen-Song L, Yuan S, Zhi-Jie C, Qian C, Sen-Sen L and Lu-Jian C 2017 Demonstration of patterned polymer-stabilized cholesteric liquid crystal textures for anti-counterfeiting two-dimensional barcodes *Appl. Opt.* **56** 601–6

[27] Velez A, Barrera J F and Torroba R 2016 Customized data container for improved performance in optical cryptosystem *J. Opt.* **18** 125702
[28] Skipetrov S E, Peuser J, Cerbino R, Zakharov P, Weber B and Scheffold F 2010 Noise in laser speckle correlation and imaging techniques *Opt. Express* **18** 14519–34
[29] Towghi N, Javidi B and Luo Z 1999 Fully phase encrypted image processor *J. Opt. Soc. Am.* A **16** 1915
[30] Javidi B, Sergent A and Ahouzi E 1998 Performance of double phase encoding encryption technique using binarized encrypted images *Opt. Eng.* **37** 565–9
[31] Goodman J W 2007 *Speckle Phenomena in Optics: Theory and Applications* (Greenwood, CO: Roberts & Co.)
[32] Mudry E, Belkebir J, Girard J, Savatier E, Le Moal C, Allain M and Sentenac A 2012 Structured illumination microscopy using unknown speckle patterns *Nat. Photon.* **6** 312–5