applied optics

Experimental optical encryption of grayscale information

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

[1]Centro de Investigaciones Ópticas (CONICET La Plata-CIC-UNLP) 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
*Corresponding author: alejandrov@ciop.unlp.edu.ar

Received 28 April 2017; revised 12 June 2017; accepted 19 June 2017; posted 21 June 2017 (Doc. ID 294845); published 14 July 2017

In this paper, we present a new protocol for achieving lower noise and consequently a higher dynamic range in optical encryption. This protocol allows for the securing and optimal recovery of any arbitrary grayscale images encrypted using an experimental double random phase mask encoding (DPRE) cryptosystem. The protocol takes advantage of recent advances that help reduce the noise due to the correlation of random phase mask in the decryption procedure and introduces the use of a "reference mask" as a reference object used to eliminate the noise due to the complex nature of the masks used in experimental DRPE setups. This noise reduction increases the dynamic range of the decrypted data, retaining the grayscale values to a higher extent and opening new possible applications. We detailed the procedure, and we present the experimental results, including an actual experimental video of a grayscale scene, confirming the validity of our proposal.

OCIS codes: (060.4785) Optical security and encryption; (070.4560) Data processing by optical means; (100.4998) Pattern recognition, optical security and encryption.

https://doi.org/10.1364/AO.56.005883

1. INTRODUCTION

Information security is an ever-growing concern given the vast amounts of information being transmitted in modern networks. This has given rise to a large array of cryptographic systems designed to ensure that the information cannot be accessed by unauthorized users. Amongst these cryptographic schemes, we find those that take advantage of the properties of optical systems [1]. These properties are, to mention a few, wavelength, polarization, phase and amplitude coding, angular momentum, etc.

Among these optical systems, the original proposal was the double random phase mask encoding (DRPE) scheme. This scheme was first introduced by Refrieger and Javidi [2] and has been implemented with several variations, including the joint transform correlator (JTC) cryptosystem [3]. The JTC presents several advantages over other DRPE schemes, namely its low alignment requirements, a decryption procedure that does not require phase conjugation, and the encrypted data is codified as an intensity pattern. These advantages make the JCT cryptosystem especially suitable for experimental implementation.

There are, however, two main challenges that limit the usefulness of DRPE systems such as the JTC for information security. One is that there are multiple theoretical attacks against several DRPE implementations, supported by simulated [4–7] and experimental [8] results. Recent research in the optical encryption field has been focused in this problem, proposing alternative DRPE schemes that make use of the degrees of freedom found in optical systems as security parameters, such as polarization [9], free-space propagation distance [10], the use of digital methods inspired by optical systems such as phase-only mask encryption [11], three-dimensional keys [12], the use of incoherent illumination [13], and photon-counting encryption schemes [14].

Many of these proposals offer increased security and performance over basic DRPE schemes such as the JTC. Some recent examples with experimental implementation are the encryption of 3D scenes with computer-generated holograms [15], techniques using novel approaches based on integral imaging [16,17], computational ghost imaging [18], Fresnel telescope imaging [19], modified DRPE schemes with parallel encryption [20], and specially designed masks [21], among others [22,23]. Despite these advances, experimental encryption of arbitrary grayscale images remains difficult.

This difficulty is due to the other challenge faced by DRPE cryptosystems: the noise produced by the encryption–decryption procedure itself. The noise problem has been discussed in some of the first DRPE applications proposed [24] and remains a relevant factor even in very recent digital

implementations of asymmetrical DRPE systems [25]. Noise limits the dynamic range and complexity of the inputs that can be processed and has been identified as a sensitive area requiring further development [26]. A notable technique to avoid the detrimental effects of noise in the decrypted data consists of first coding the data to be encrypted into an "information container" that is then processed with the optical cryptosystem [27–29]. The information container is selected for its resistance to noise, ensuring that after decryption, is possible to decode it to retrieve the original data free of noise. This approach has found several interesting applications [30–36]. However, the complexity of the "information container" increases with the message enclosed, making this approach less attractive when a large amount of information is involved.

One interesting suggestion to reduce the noise issue was proposed by Vilardy *et al.* [37]. The method consists of a modification of the encrypted data produced by the JTC system, where these data are divided by the key intensity. This operation reduces the noise after decryption and makes the system resistant to common chosen plaintext attacks, such as the Dirac delta attack, increasing its security. An implementation of this technique in an experimental setup was later demonstrated [38], though the noise reduction was lower than the effect reported in simulated experiments. Recently, Velez *et al.* [39] analyzed the noise due to the correlation of the key, demonstrating that this noise is dependent on the geometry of the input object and then proposing a technique to greatly diminish the noise by modifying the input. In this way, the method allows achieving a reduction after decryption. The authors demonstrated the technique in an experimental setup, showing less noise for reconstructed binary objects.

At this point, we must remark that the previously mentioned procedures deal with the noise due to the key autocorrelation found in the decryption procedure. Nevertheless, as we will show, in an actual experimental setup, there are other sources of noise, mainly due to the fact that the physical keys are not random phase-only masks and also due to physical constraints not found in simulated experiments. In this work, we will show a series of techniques for noise reduction in an actual experimental JTC cryptosystem, including the use of a novel reference mask to eliminate amplitude noise due to the nonideality of the object phase mask. With these methods, we achieve a large reduction in noise in the decrypted data, allowing an effective encryption of grayscale images and structured objects, limited only by the physical dimensions of the setup.

2. CRYPTOSYSTEM DESCRIPTION AND NOISE REDUCTION

As a test cryptosystem, we built the optical setup of Fig. 1 in our laboratory and used it to achieve optical encryption of all the objects shown in this paper. This setup is an experimental realization of the JTC DPRE scheme with digital holography, where one arm contains the JTC system and the other provides a reference beam that will be used to register the encryption key as an off-axis Fourier hologram [40]. In the JTC system, the input plane has two windows, separated a distance $2b$, that are projected on an 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. To achieve encryption, the reference beam is blocked, and the CMOS camera registers the intensity of the interference between the Fourier transforms (FTs) of both windows displayed on the SLM, called the joint power spectrum (JPS):

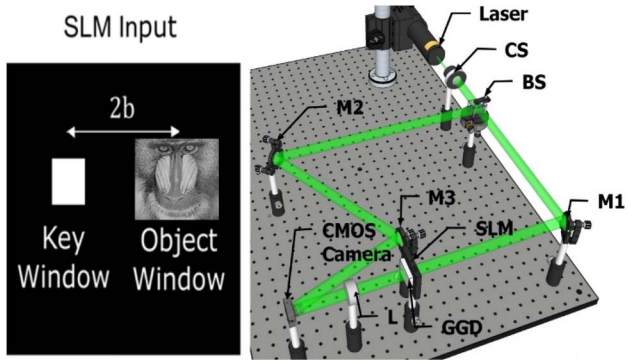

Fig. 1. Experimental JTC cryptosystem (SLM: spatial light modulator, CS: collimation system, M: mirror, L: lens, BS: beam splitter, GGD: ground-glass diffuser).

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

where * means complex conjugate, and $K(u,v)$ and $F(u,v)$ are the FT of the security key $k(x,y)$ and of the object window $f(x,y)$, respectively. The object window is $f(x,y) = o(x,y)r(x,y)$, with $o(x,y)$ the amplitude-only object displayed in the SLM, and $r(x,y)$ is a random phase function representing the effect of the ground-glass diffuser, while the key $k(x,y)$ is another phase function result of the light propagating through the key window and then through the ground glass. This JPS contains the encrypted information, which can be extracted by performing its inverse Fourier transform (IFT). This will result in an optical field with spatially separated orders, given by

$$\begin{aligned} j(x,y) &= f(x,y) \otimes f^*(x,y) \\ &\quad + k(x,y) \otimes k^*(x,y) \\ &\quad + f^*(x,y) \otimes k(x,y) \otimes \delta(x-2b,y) \\ &\quad + f(x,y) \otimes k^*(x,y) \otimes \delta(x+2b,y). \end{aligned} \tag{2}$$

The first two terms are the autocorrelations of the object and key windows, respectively, corresponding to a central order, while the remaining two terms are the IFT of the encrypted object and its complex conjugate, with a spatial separation given by $2b$. For optimal recovery, there should be no overlap between these terms, which can be achieved if b is large enough compared with the size of the key and object windows. In our experimental setup, however, the input plane size is limited by the area of the SLM where we project the windows, and large values of b can only by achieved with small object and key

windows. We can eliminate the central order represented by the first two terms in Eq. (2) to avoid this limitation. This can be achieved by projecting only the key window on the SLM and registering the intensity of its FT, then doing the same for the object window. Afterwards, these two intensities are subtracted from the JPS prior to performing the filtering procedure [40].

An additional issue in the experimental implementation, especially when using large objects, is that the interference fringes are better defined in the center of the optical axis than further away. This is because the lights coming from the nearest points of the object and key windows interfere, producing lower-frequency fringes than the outmost points. This means that the amplitude of the field represented in Eq. (2) near the central order has a higher amplitude than those further away. Therefore, the decrypted object from this JPS will display uneven illumination. We found that this can be compensated by dividing Eq. (2) by a hamming window [41].

Once we perform these two steps, we can filter the third term of Eq. (2) and keep the fourth, which is, after an FT of the encrypted object, given by

$$E(u,v) = F(u,v)K^*(u,v). \tag{3}$$

The decryption procedure consists of multiplying the encrypted object by the FT of the security key $K(u,v)$ and performing an IFT, obtaining the object as

$$d(x,y) = [o(x,y)r(x,y)] \otimes k^*(x,y) \otimes k(x,y). \tag{4}$$

If we attempt decryption with a wrong key, $k_W(x,y)$, we will obtain

$$d_W(x,y) = [o(x,y)r(x,y)] \otimes k^*(x,y) \otimes k_W(x,y). \tag{5}$$

Since the key correct key is a random function, its correlation with any other function results in a new random function, and, as such, the object remains encrypted; however, when we use the correct key, and if we consider $k(x,y)$ as a phase-only random function, then its autocorrelation is equal to a Dirac delta function, allowing retrieval of the object. In the experimental setup, however, a ground-glass diffuser is not an ideal phase-only mask, and, thus, $k(x,y)$ and $r(x,y)$ are complex valued functions, with both phase and amplitude. In this sense, the degradation of the decrypted object is due to the multiplication with the random complex function $r(x,y)$ and the convolution with the autocorrelation of $k(x,y)$. There are two successful approaches to reduce the noise due to the autocorrelation of the key.

The first, proposed by Vilardy *et al.* [37], is a non-linear modification of the encrypted object, achieved by dividing the encrypted object by the intensity of $K(u,v)$. This is relatively straightforward, since we already register this intensity to reduce the central order of Eq. (2). Two problems arise when applying this technique to the experimental data. First, the limited pixel size and dynamic range of the registering medium mean that we have a sampled version of the intensity of $K(u,v)$, and second, near-zero values of $K(u,v)$ can cause large errors in the amplitude of the decrypted object after the division procedure. We can round the near-zero values of the intensity of $K(u,v)$ to a higher value to limit these errors. These two factors combined with the vibrations present between the registering of the JPS and the intensity of $K(u,v)$, means that this technique cannot eliminate completely the effect on the noise due to the autocorrelation of the key.

Another technique was proposed by Velez *et al.* [39], taking advantage of the properties of the autocorrelation of the key. This autocorrelation consists of a sharp central peak, surrounded by a low-intensity random correlation noise (RCN). In the decrypted object, each point is convolved with this function, which means that the low-intensity RCN surrounding it will overlap, increasing the overall noise level. The proposed method to reduce the noise is the pixel separation technique (PST), consisting of separating each individual pixel or groups of pixels of the object with black pixels between them. This limits the amount of overlap of RCN and lowers the overall noise intensity.

Both the PST technique and the non-linear modification can be applied simultaneously, resulting in large suppression of the noise due to the correlation of the key, as we will show in the experimental result section.

Once we suppress the noise due to the autocorrelation using the previously discussed methods, the noise due to $r(x,y)$ remains in the decrypted data. When encrypting an amplitude-only object, the phase component of this noise can be eliminated simply by multiplying the decrypted data by its complex conjugate. After this, we obtain

$$|d(x,y)|^2 = |o(x,y)r(x,y)|^2. \tag{6}$$

This leaves the amplitude part of $r(x,y)$ as a source of noise, which we can eliminate by encrypting a white square as a reference mask. To do this, we replace the object $o(x,y)$ displayed in the SLM for a blank window of the same size without changing the diffuser and the key window positions. After filtering and decrypting the JPS registered by the CMOS camera [Eq. (4)], we obtain the reference mask given by $r(x,y) \otimes k^*(x,y) \otimes k(x,y)$.

If we suppress the noise due to the autocorrelation of the key by applying both the non-linear modification and the PST to the reference mask, and then multiply the reference mask by its complex conjugate, we obtain the intensity of $r(x,y)$. We can then divide the intensity of the decrypted object [Eq. (6)] by the intensity of the decrypted reference mask, therefore obtaining the intensity of the decrypted object $o(x,y)$ with low noise:

$$|d_r(x,y)|^2 = \frac{|o(x,y)r(x,y)|^2}{|r(x,y)|^2}. \tag{7}$$

This method has the same limitations as the non-lineal modification, since it is also a division procedure. This means that the near-zero values of the reference mask must be set to a higher value, and that, due to experimental constraints, it will not be possible to eliminate the noise completely. Additionally, this method requires that the noise due to the autocorrelation of the key is suppressed for both the reference mask and the encrypted object; otherwise, it will result in

$$|d_n(x,y)|^2 = \frac{|[o(x,y)r(x,y)] \otimes k^*(x,y) \otimes k(x,y)|^2}{|[r(x,y)] \otimes k^*(x,y) \otimes k(x,y)|^2}, \tag{8}$$

where the noise will be increased instead of reduced.

However, as we will show, this noise reduction allows for the encryption of grayscale images with higher dynamic ranges than

those achieved with direct decryption. Summarizing, our protocol for noise reduction has the following steps:

(1) Apply the PST to the object to reduce the noise due to the autocorrelation of the key.
(2) Subtraction of the intensity of $F(u, v)$, $K(u, v)$ to reduce the crosstalk when filtering the decrypted data.
(3) Division of the FT of the JPS by a hamming window to equalize the intensity of the encrypted object.
(4) Division of the encrypted object by the intensity of $K(u, v)$ prior to decryption to further reduce the noise due to the autocorrelation of the key.
(5) Register the encrypted reference mask with PST and decrypt by applying steps 1–4, and then divide the decrypted object by the resulting decrypted reference mask.

3. EXPERIMENTAL RESULTS

We will use the experimental scheme of Fig. 1 to test the effectiveness of our proposal. The recording medium was a CMOS EO-10012C camera, with a pixel size of 1.67 μm × 1.67 μm and a 3480 pixel × 2748 pixel resolution. The object and the key windows were projected using an SLM HOLOEYE LC2000, with a pixel size of 32 μm × 32 μm. The lens focal length was 200 mm. The key window had an area of 6.4 mm × 3.2 mm. The object window had an area of 19.2 mm × 19.2 mm. The separation between both windows was 11.2 mm. The images projected on the object window had a resolution of 600 pixels × 600 pixels without PST. The images projected with PST had an original resolution of 200 pixels × 200 pixels and were divided in blocks of 2 pixels separated by four pixels.

We register the JPS of a grayscale image and proceed to filter the encrypted object, showing the effect of subtracting the FT of $F(u, v)$ and $K(u, v)$ and the use of the hamming window.

In Fig. 2(a), we show the intensity of the IFT of the registered JPS. The gray squares (green in color online) correspond to the location of the orders containing the encrypted object and its complex conjugate, while the white square identifies the central order. Notice the uneven illumination of the side orders and the overlap with the central order. In Fig. 2(b), we show the intensity of the IFT of the JPS after subtracting the intensities of $F(u, v)$ and $K(u, v)$. As a result, the central order is now much smaller, and its overlap with the side orders is almost entirely eliminated. The intensity of the side orders, however, remains uneven, with the side near the central order having much more intensity than the one further away. In Fig. 2(c), we see the intensity of the IFT of the JPS after subtracting the intensities of $F(u, v)$ and $K(u, v)$ and dividing by the hamming window. Now the side orders have even intensity on their extension, and there is no overlap with the central order. This allows for optimal filtering of the unwanted terms of the JPS from the encrypted object.

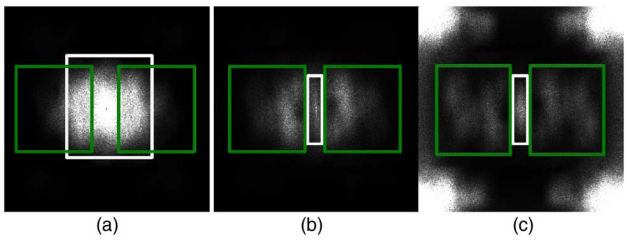

Fig. 2. (a) Intensity of the FT of the JPS. (b) Intensity of (a) after subtracting the intensity of the FT of the key and object windows, and (c) intensity of (b) after dividing by the hamming window.

We now proceed to show the result of applying the full noise reduction protocol to the encryption of a grayscale image without PST.

In Fig. 3(b), we show the result from direct encryption–decryption of the input of Fig. 3(a). Note the uneven intensity and the high amount of noise due to the overlap with the central order during filtering, as show in Fig. 2(b). In Figs. 3(c) and 3(d), we can appreciate the effect of subtracting the intensity of $K(v, w)$ and $F(u, v)$ and applying the hamming window division during filtering, as show in Figs. 2(b) and 2(c). In Fig. 3(e), we show the result after filtering with the central order suppression and the non-lineal modification. Notice how the noise around the bright parts of the scene is severely reduced when compared with Fig. 3(d). This noise "bloom" effect is caused by the RCN and can be reduced even more with the PST. Finally, in Fig. 3(f), we show the result with central order suppression, division by the hamming window, non-lineal modification, and division by the reference mask. We remark that the noise has a different distribution compared with Fig. 3(e). This is because the non-lineal modification alone is not enough to suppress the noise due to the autocorrelation of the key, and, as a result, dividing by the reference mask causes more noise.

In Fig. 4, we show the results of applying the previous procedures and PST to three different objects. The object shown in the first row is a text where the letters have decreasing gray values. In the decrypted result after division with the reference mask, we can identify clearly the different gray values. This is a demonstration of the increased dynamic range that can be achieved with our proposal. There is still remaining noise, caused by the previously discussed limitations of the non-linear modification and the division by the reference mask.

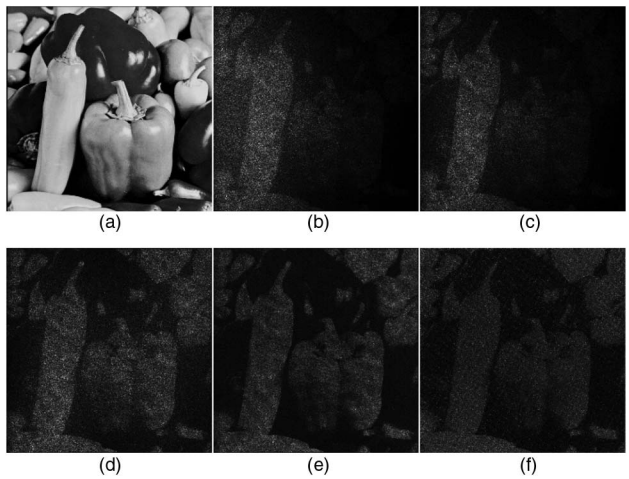

Fig. 3. Decryption of an image. (a) Input image, (b) direct decryption, (c) decryption with only the subtraction of the intensity of the FT of the key and object window, (d) decryption with (c) and the division by the hamming window, (e) decryption with (d) and the non-lineal modification, and (f) decryption with (e) and division with the reference mask.

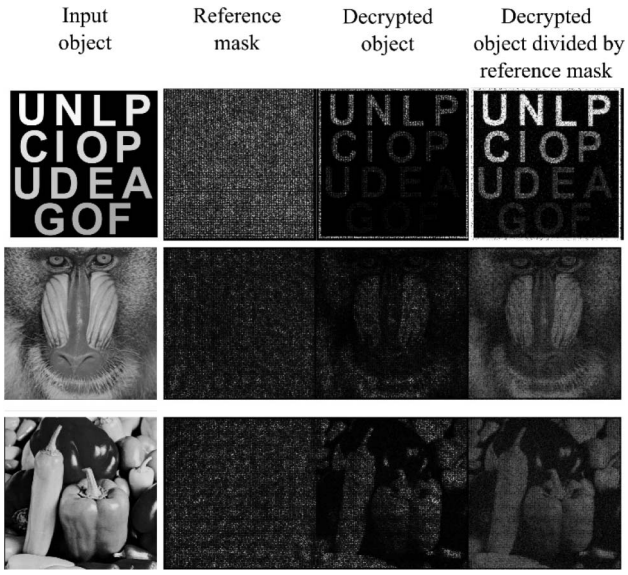

Fig. 4. Results of encryption–decryption of 3 objects with PST and reference mask.

Additionally, there is an increase in contrast in the results when compared with the input image, caused by two reasons. First, the recovered object is the square of the original object, since we multiply the decrypted object by its complex conjugate to eliminate the phase part of $r(x, y)$. Second, the amplitude modulation of the SLM is not linear and induces a change in the relative gray levels. This is a technical limitation that can be diminished using an SLM better suited for amplitude modulation or a DMD device.

We calculated the correlation coefficient r between the input images and the decrypted result in every stage of the protocol to further demonstrate the effectiveness of our proposal. This correlation coefficient is given by

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}, \quad (9)$$

where m, n are the pixel coordinates, A is the input image, B is the decrypted image, and $\bar{A}$, $\bar{B}$ are the mean values of A and B, respectively.

The resulting correlation coefficients can be found in Table 1. Observe how we achieve a near doubling of the correlation coefficient with the full method when compared with the direct decryption. The method proposed here has little computational cost; however, there is added complexity in registering the reference mask and the intensities of $K(u, v)$ and $F(u, v)$. This complexity is mitigated by the fact that these data only must be registered again if the ground-glass diffuser is replaced or moved; otherwise, many objects can be registered using the same key and reference mask. We present an encrypted–decrypted video to show this behavior. In Visualization 1, we show the video with direct decryption, in Visualization 2 with central order suppression, hamming window, and non-lineal modification, and in Visualization 3 with PST. There is a gradual increase in noise as the video advances. This is due to vibrations in the experimental setup and fluctuations on the laser beam causing a gradual "drift" of the key. Additional work is necessary to solve these issues; however, encryption of grayscale videos with low noise is achieved with our proposal for the first time to the best of our knowledge.

Table 1. Correlation Coefficient Between the Input Objects and the Decrypted Objects with the Different Steps of Our Protocol

Process	Correlation Coefficient (Letters)	Correlation Coefficient (Mandrill)	Correlation Coefficient (Peppers)
Direct decryption	0.1977	0.3612	0.4155
Suppression of central order	0.4049	0.4469	0.5030
Division by hamming window	0.4731	0.5841	0.6400
Non-lineal modification	0.5201	0.6240	0.7295
PST	0.6915	0.6688	0.7490
Division by reference mask	0.7531	0.7869	0.8088

In order to demonstrate that our proposed protocol does not degrade the robustness of the encryption system, we calculated and plotted the correlation coefficient [Eq. (9)] between the input image "mandrill" and the decrypted result from its occluded encrypted data. This was done for our protocol and for direct decryption. The occlusion was performed by multiplying the encrypted data by a square pupil of decreasing area. In the case of our protocol, both the encrypted object and the encrypted reference mask have the same amount of occlusion.

In Fig. 5, we can see that the objects decrypted with the proposed protocol exhibit a higher correlation coefficient than those obtained by direct decryption, no matter the level of occlusion. In this way, optimal decryption can be carried out even with incomplete encrypted data, maintaining the robustness of the JTC encryption scheme.

4. RESISTANCE TO ATTACKS

While our protocol is mainly intended to deal with noise, it will also increase the security of the system against known attacks. The first attack reported against the JTC encryption scheme was the chosen plaintext attack [4,5]. This attack works under the assumption that an attacker has full access to the encryption setup and can select any data (plaintext) to encrypt, with the purpose of recovering the encryption key. Vilardy *et al.* [37] demonstrated that the introduction of non-linear modification, included in our protocol, helps defeat this attack.

More recently, two contributions demonstrated successful ciphertext (encrypted data) -only attacks against both the JTC [7] and the experimental lensless DRPE [8] encrypting schemes. These attacks are based on the observation that the energy spectral density of the plaintext can be extracted from the ciphertext, and, thus, a phase retrieval procedure applied

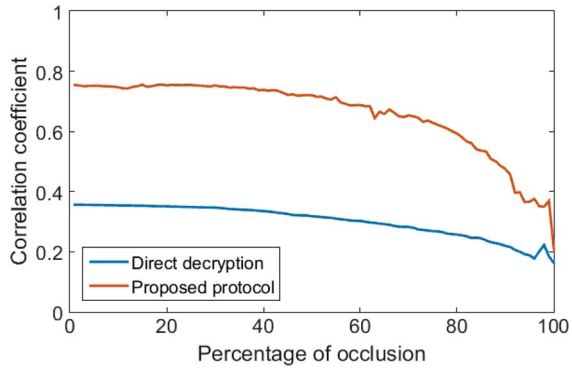

Fig. 5. Correlation coefficient between the input object and the decrypted object from the occluded encrypted data, comparing direct decryption with our proposed protocol.

over this energy spectral density can reconstruct the original object without the need for the decryption key.

The fact that in our experimental implementation, we use complex random masks and not phase-only masks, and the introduction of the non-linear modification, ensures that the energy spectral density of the plaintext can no longer be accurately retrieved from the ciphertext, securing the scheme against these kinds of attacks.

5. CONCLUSIONS

We present a protocol of several steps to reduce significantly the noise in experimentally encrypted–decrypted objects using a double random phase mask. This proposal doubles the correlation coefficient of the decrypted result with the input objects when compared with direct decryption. The lower noise results in an increase of the dynamic range of decrypted objects. Additional increases in quality can be achieved by using faster registering mediums with higher bit depths and the use of a projection system with better amplitude modulation.

We also discuss the implications of our protocol for the system security; however, further analyses are required to determine possible vulnerabilities.

This protocol could be combined with high-performance parallel computing to allow real-time encryption of video data or large data sets. In virtual optical cryptosystems, the proposed method results in a full elimination of noise. A high dynamic range increases the throughput of optical cryptosystems that use information containers, since information can be codified into the different gray values and not only as binary data.

Funding. Universidad de Antioquia (UdeA); Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) (0849/16, 0549/12); Universidad Nacional de La Plata (UNLP) (11/I215).

Acknowledgment. John Fredy Barrera Ramírez acknowledged the support from the International Centre for Theoretical Physics ICTP Associateship Scheme.

REFERENCES

1. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120–155 (2014).
2. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
3. T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," Opt. Eng. **39**, 2031–2035 (2000).
4. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," Opt. Lett. **30**, 1644–1646 (2005).
5. J. F. Barrera, C. Vargas, M. Tebaldi, R. Torroba, and N. Bolognini, "Known-plaintext attack on a joint transform correlator encrypting system," Opt. Lett. **35**, 3553–3555 (2010).
6. X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, "Vulnerability to ciphertext-only attack of optical encryption scheme based on double random phase encoding," Opt. Express **23**, 18955–18968 (2015).
7. C. Zhang, M. Liao, W. He, and X. Peng, "Ciphertext-only attack on a joint transform correlator encryption system," Opt. Express **21**, 28523–28530 (2013).
8. G. Li, W. Yang, D. Li, and G. Situ, "Cyphertext-only attack on the double random-phase encryption: Experimental demonstration," Opt. Express **25**, 8690–8697 (2017).
9. S. K. Rajput and N. K. Nishchal, "Image encryption using polarized light encoding and amplitude and phase truncation in the Fresnel domain," Appl. Opt. **52**, 4343–4352 (2013).
10. J. F. Barrera, A. Jaramillo, A. Velez, and R. Torroba, "Experimental analysis of a joint free space cryptosystem," Opt. Lasers Eng. **83**, 126–130 (2016).
11. S. Liansheng, Z. Bei, N. Xiaojuan, and T. Ailing, "Optical multiple-image encryption based on the chaotic structured phase masks under the illumination of a vortex beam in the gyrator domain," Opt. Express **24**, 499–515 (2016).
12. A. Velez, J. F. Barrera, and R. Torroba, "Three-dimensional joint transform correlator cryptosystem," Opt. Lett. **41**, 599–602 (2016).
13. P. A. Cheremkhin, V. V. Krasnov, V. G. Rodin, and R. S. Starikov, "QR code optical encryption using spatially incoherent illumination," Laser Phys. Lett. **14**, 026202 (2017).
14. E. Pérez-Cabré, M. Cho, and B. Javidi, "Information authentication using photon-counting double-random-phase encrypted images," Opt. Lett. **36**, 22–24 (2011).
15. D. Kong, L. Cao, G. Jin, and B. Javidi, "Three-dimensional scene encryption and display based on computer-generated holograms," Appl. Opt. **55**, 8296–8300 (2016).
16. Y. Xing, Q. Wang, Z. Xiong, and H. Deng, "Encrypting three-dimensional information system based on integral imaging and multiple chaotic maps," Opt. Eng. **55**, 023107 (2016).
17. H. Li, C. Guo, I. Muniraj, B. C. Schroeder, J. T. Sheridan, and S. Jia, "Volumetric light-field encryption at the microscopic scale," Sci. Rep. **7**, 40113 (2017).
18. W. Jingjing, X. Zhenwei, L. Zhengjun, L. Wei, Z. Yan, and L. Shutian, "Multiple-image encryption based on computational ghost imaging," Opt. Commun. **359**, 38–43 (2016).
19. A. Yan, J. Sun, Z. Hu, J. Zhang, and L. Liu, "Novel optical scanning cryptography using Fresnel telescope imaging," Opt. Express **23**, 18428–18434 (2015).
20. J. Liu, T. Bai, X. Shen, S. Dou, C. Lin, and J. Cai, "Parallel encryption for multi-channel images based on an optical joint transform correlator," Opt. Commun. **396**, 174–184 (2017).
21. C. Lin and X. Shen, "Design of reconfigurable and structured spiral phase mask for optical security system," Opt. Commun. **370**, 127–134 (2016).
22. S. Xi, X. Wang, L. Song, Z. Zhu, B. Zhu, S. Huang, N. Yu, and H. Wang, "Experimental study on optical image encryption with asymmetric double random phase and computer-generated hologram," Opt. Express **25**, 8212–8222 (2017).
23. X. Shen, S. Dou, M. Lei, and Y. Chen, "Optical image encryption based on a joint Fresnel transform correlator with double optical wedges," Appl. Opt. **55**, 8513–8522 (2016).

24. B. Javidi, G. Zhang, and J. Li, "Encrypted optical memory using double-random phase encoding," Appl. Opt. **36**, 1054–1058 (1997).
25. X. Wang, G. Zhou, C. Dai, and J. Chen, "Optical image encryption with divergent illumination and asymmetric keys," IEEE Photon. J. **9** 7801908 (2017).
26. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S. Millán, N. K. Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A. Alfalou, C. Brosseau, C. Guo, J. T. Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W. H. Pinkse, A. P. Mosk, and A. Markman, "Roadmap on optical security," J. Opt. **18**, 083001 (2016).
27. J. F. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: Secure and noise- free information retrieval," Opt. Express **21**, 5373–5378 (2013).
28. J. F. Barrera, A. Mira, and R. Torroba, "Experimental QR code optical encryption: Noise-free data recovering," Opt. Lett. **39**, 3074–3077 (2014).
29. A. Velez, J. F. Barrera, and R. Torroba, "Customized data container for improved performance in optical cryptosystem," J. Opt. **18**, 125702 (2016).
30. Y. Qin, H. Wang, Z. Wang, Q. Gong, and D. Wang, "Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal," Opt. Lasers Eng. **84**, 62–73 (2016).
31. Y. Qin and Q. Gong, "Optical information encryption based on incoherent superposition with the help of the QR code," Opt. Commun. **310**, 69–74 (2014).
32. X. Wang, W. Chen, and X. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," Opt. Express **23**, 6239–6253 (2015).
33. Y. Qin and Y. Zhang, "Information encryption in ghost imaging with customized data container and XOR operation," IEEE Photon. J. **9**, 7802208 (2017).
34. S. Jiao, W. Zou, and X. Li, "QR code based noise-free optical encryption and decryption of a gray scale image," Opt. Commun. **387**, 235–240 (2017).
35. J. Wang, L. Song, X. Liang, Y. Liu, and P. Liu, "Secure and noise-free nonlinear optical cryptosystem based on phase-truncated Fresnel diffraction and QR code," Opt. Quantum Electron. **48**, 523 (2016).
36. L. Sui, M. Xu, and A. Tian, "Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain," Opt. Lasers Eng. **91**, 106–114 (2017).
37. J. M. Vilardy, M. S. Millán, and E. Perez-Cabré, "Improved decryption quality and security of a joint transform correlator-based encryption system," J. Opt. **15**, 025401 (2013).
38. J. F. Barrera, A. Velez, and R. Torroba, "Experimental scrambling and noise reduction applied to the optical encryption of QR codes," Opt. Express **22**, 20268–20277 (2014).
39. A. Velez, J. F. Barrera, and R. Torroba, "Innovative speckle noise reduction procedure in optical encryption," J. Opt. **19**, 055704 (2017).
40. E. Rueda, J. F. Barrera, R. Henao, and R. Torroba, "Optical encryption with a reference wave in a joint transform correlator architecture," Opt Commun. **282**, 3243–3249 (2009).
41. A. H. Nuttall, "Some windows with very good sidelobe behavior," IEEE Trans. Acoust. Speech Signal Process. **29**, 84–91 (1981).