Optics Letters

Optimized random phase encryption

Alejandro Velez Zea,[1,2,*] John Fredy Barrera Ramirez,[3] and Roberto Torroba[1,4]

[1]Centro de Investigaciones Ópticas (CONICET La Plata- CIC-UNLP), P.O. Box 3, C.P 1897, La Plata, Argentina
[2]Facultad de Ciencias Exactas, Universidad Nacional de La Plata, La Plata, Argentina
[3]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
[4]UIDET OPTIMO, Departamento de Ciencias Básicas, Facultad de Ingeniería, Universidad Nacional de La Plata, La Plata, Argentina
*Corresponding author: alejandrov@ciop.unlp.edu.ar

Received 1 June 2018; accepted 4 June 2018; posted 26 June 2018 (Doc. ID 332951); published 19 July 2018

We propose for the first time, to the best of our knowledge, the use of optimized random phases (ORAPs) in a double random phase encryption scheme (DRPE). In DRPE schemes the convolution between two random phase functions encrypts the information to be secured. However, in actual encryption applications, this convolution of random phases also results in unwanted effects like speckle noise. In this Letter we show that under certain conditions this noise can be drastically reduced. These conditions can be easily achieved by using ORAPs. These ORAPs, besides containing information about the parameters of the optical system and maintaining all the security properties of a random phase function, ensure that the encrypted data is a phase-only function. This leads to a great increase in system performance, with decryption quality similar to the reconstruction of a phase-only hologram generated with the Gerchberg–Saxton algorithm. We show both numerical and experimental results confirming the validity of our proposal.

OCIS codes: (060.4785) Optical security and encryption; (070.4560) Data processing by optical means; (070.0070) Fourier optics and signal processing.

https://doi.org/10.1364/OL.43.003558

The staggering amount of information being generated by modern societies presents the challenges of how to adequately and efficiently process, store, protect, and transfer this data. To help address these challenges, optical systems have been the subject of intense research, due to their potential capability to achieve light-speed information processing.

One of the applications of optical information processing is encryption, whose objective is accomplishing fast and secure data protection. The first proposed method is the double random phase encryption (DRPE), introduced by Refreiger and Javidi with a 4f scheme [1]. Further developments lead to DRPE being implemented in many optical schemes [2,3], of which one of the most common is the joint transform correlator (JTC) [4]. In these schemes, information contained in an optical field is coded into stationary white noise by the optical correlation between two random phase-only functions. One of these phase-only functions multiplies the information to be encrypted, and the other will provide the encryption key.

The encryption procedure can be reversed by knowing the phase function corresponding to the encryption key, thus obtaining the original data.

Despite the many schemes proposed for optical encryption, and the possible advantages they present over traditional systems, there are some common issues to all DRPE schemes limiting their usefulness in real-world scenarios. The first of these issues is related to the security of the DRPE schemes itself. Several theoretical and experimental attacks against these systems have been demonstrated [5,6], and while most proven attacks require auxiliary information to be successful, proposals to harden the system are the subject of several recent works [7–9].

The other main issue with the DRPE schemes is related to the degradation of the decrypted data compared to the original information. This degradation manifests itself as speckle noise. There have been proposals to avoid this noise, most notably the use of containers that codify the information to be encrypted into a representation more resistant to the adverse effects of the encryption procedure [10,11]. However, other works have focused in identifying the source of this noise [12,13]. The main conclusion from these works is that the correlation between the random phase functions during decryption is one of the main sources of degradation, producing random correlation noise (RCN). With these findings, in previous works we implemented a pixel separation technique consisting in altering the geometry of the input object to minimize the degradation during the encryption–decryption process [13]. While the resulting increase in quality was remarkable, the approach has the drawback of requiring larger encryption setups to process the same input. In this Letter, we further examine the noise in encryption, and find a set of conditions for both the encryption key and the object that will theoretically allow the elimination of the RCN. To meet these conditions, we propose the use of specially tailored phase functions that take into account the dimensions and optical characteristics of the encrypting scheme. These optimized random phases (ORAPs) are random phase functions optimized to ensure that the Fourier transform (FT) of their product with an intensity

pattern is a near phase-only function. ORAPs were first proposed to generate phase-only holograms [14], and as such have the added advantage of allowing the use of phase-only spatial light modulators to achieve optical reconstruction of optically encrypted scenes.

We will study the JTC encryption scheme to demonstrate the effectiveness of our proposal. This cryptosystem is one of the most used, because encrypted data is stored as an intensity pattern and has lower experimental requirements compared to other schemes like the 4f.

In Fig. 1 we show a basic scheme of the JTC cryptosystem. In this scheme the input plane has the object and key window (which is simply an empty window) separated a distance 2b, placed in the focal plane of a convergent lens. The input plane is in contact with a ground glass diffuser (GGD) to generate the random phase functions. At the conjugate plane there is an intensity recording medium.

This recording medium registers the joint power spectrum (JPS) of the light coming from the input plane, given by

$$J(u,v) = |F(u,v)|^2 + |K(u,v)|^2 + F*(u,v)K(u,v)\exp(4\pi ibu) + F(u,v)K*(u,v)\exp(-4\pi ibu), \quad (1)$$

where $F(u,v)$ and $K(u,v)$ are the FT of $f(x,y) = o(x,y)r(x,y)$ and $k(x,y)$, respectively, with $o(x,y)$ the object to be encrypted, $2b$ the separation between the key window and the object, and $r(x,y)$ and $k(x,y)$ the random phases of the light propagating through the object and key window, respectively.

While the JPS contains the encrypted data, it also includes additional information about the system that can render it vulnerable to attacks [6]. We can perform a filtering procedure [15] to avoid this vulnerability, where we discard the information corresponding to the first three terms of Eq. (1), retaining the fourth, which is the encrypted object. For decryption, we just multiply the encrypted object by $K(u,v)$, obtaining

$$D(u,v) = F(u,v)K^*(u,v)K(u,v). \quad (2)$$

After performing the inverse FT of Eq. (2), we obtain the decrypted data as

$$d(x,y) = f(x,y) \otimes k^*(x,y) \otimes k(x,y). \quad (3)$$

As we can see, the decrypted data is the convolution between the object multiplied by a random phase function and the self-correlation of the key window random phase. The effect of this convolution is usually disregarded, by making the assumption that it is approximately equal to a delta Dirac function. However, this convolution is one of the main sources of degradation of the decrypted data. This is because the autocorrelation of $k(x,y)$ not only presents a sharp central peak like a Dirac delta, but also a low intensity "cloud" of noise around it. This "cloud" is the RCN [13].

Since this noise is convolved with the object, it leads to a speckle bloom effect around the borders of its bright regions, severely diminishing the overall contrast of the image. This effect can be minimized by segmenting and separating the bright regions of the image, yet this is not always possible or desirable.

However, another approach to reduce this noise can be done by guaranteeing that $K(u,v)$ is a phase-only function. Therefore, the product with its complex conjugate is equal to unity, and the RCN is avoided. We use the concept of ORAP to achieve this goal. An ORAP is generated from a random phase function by applying several iterations of the Gerchberg–Saxton (G–S) algorithm [16] using the pupils of the optical system in the input and output plane as intensity targets. In the input plane the target intensity is the key window and in the output plane is a window with the same dimensions as the recording medium. The result of this algorithm is a key function $k(x,y)$ whose FT $K(u,v)$ is nearly a phase-only function.

In Fig. 2 we show numerical results of the autocorrelation of a key function $k(x,y)$. We used a simulation space with resolution 1080 × 1080 pixels and generated a random phase with resolution 300 × 300 pixels to obtain the results in Fig. 2(a). For Fig. 2(b) we generated an ORAP with target size of 300 × 300 in the input plane and 1080 × 1080 in the Fourier plane with 10 iterations of the G–S algorithm. The sharp central peak of the autocorrelation has been suppressed to show the RCN, and both plots are normalized to the same value. As we expected, using an ORAP to generate the key function results in a significantly lower RCN.

We also found another approach to increase the quality of the decrypted data. This method consists in discarding the amplitude of Eq. (2), retaining only its phase. This eliminates the RCN, since it results from the amplitude part of $K(u,v)$. The disadvantage of this procedure is that by discarding the amplitude part of $F(u,v)$ we are losing information about the object, resulting in degradation after reconstruction. To avoid this issue, we use an ORAP in place of the random phase $r(x,y)$ that multiplies the object. Therefore, $F(u,v)$ will be nearly a phase-only function. In addition, if we use an ORAP to generate the key, then Eq. (2) will be nearly a phase-only function, and discarding its amplitude will result in very little degradation in the reconstructed data, while eliminating the RCN.

We test the effectiveness of our proposal by numerically simulating a JTC scheme to encrypt three input objects using random phases and then performing decryption before and

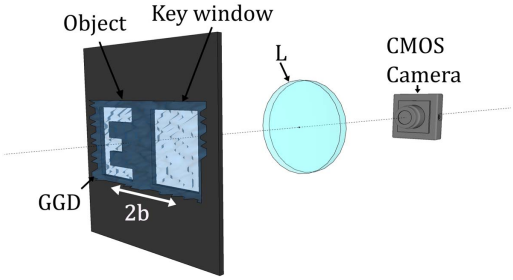

Fig. 1. Scheme of a JTC cryptosystem. L, lens; GGD, ground glass diffuser.

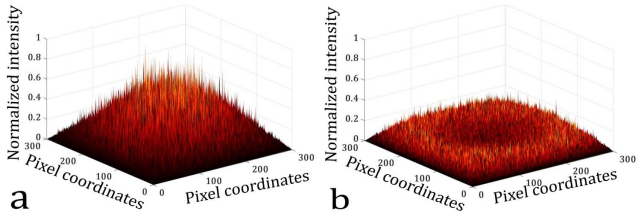

Fig. 2. Autocorrelation of $k(x,y)$ with central peak suppressed for: (a) random phase and (b) optimized random phase.

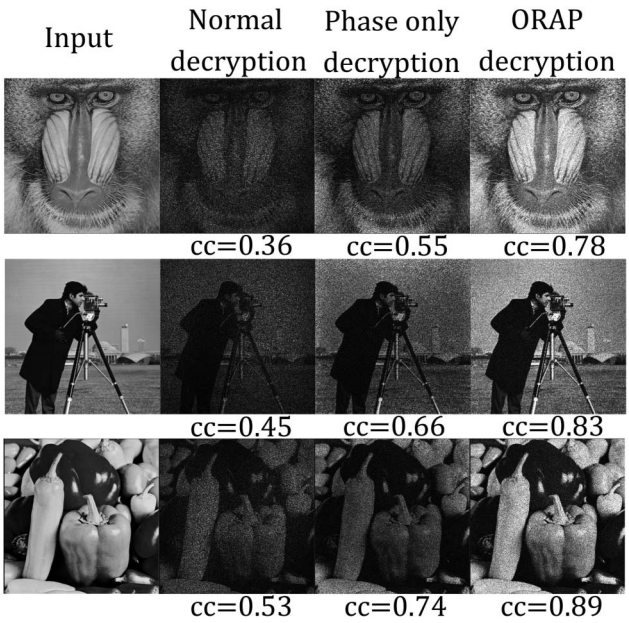

Fig. 3. Numerical results obtained with a JTC cryptosystem.

after discarding the amplitude of Eq. (2). Then we encrypt the same inputs using ORAPs in both the object and the key and decrypt after discarding the amplitude of Eq. (2). The results are shown in Fig. 3. In the decryption results using nonoptimized random phases, we can see that the effect of RCN causes considerable degradation in the decrypted data. This degradation is greatly reduced when using only the phase of Eq. (2) for decryption, since the amplitude part that is responsible for the RCN is discarded. As we show, the loss caused by discarding the amplitude part of the encrypted image is more than compensated by the reduction in RCN, resulting in a net increase of the correlation coefficient of the decrypted data when compared with the input. Using ORAPs produces further improvement; however, there is still some remaining noise also caused by the discarding of the amplitude part of Eq. (2), since the FT of an ORAP is only approximately a phase-only function, not a pure one.

In the results of Fig. 3, the key had 300 × 300 pixels and the object 450 × 450 pixels. The simulation space size was 1080 × 1080 pixels. For the generation of the ORAP that is used as the key, the intensity target in the input plane was a white square with 300 × 300 pixels. For the ORAP that will multiply the input object, the intensity target in the input plane was also a white square with 450 × 450 pixels. For both ORAPs the target in the Fourier plane was another white square covering the entire 1080 × 1080 simulation space. The ORAPs were obtained after 10 iterations of the G–S algorithm. As simulation parameters we used a wavelength of 532 nm, a lens focal length of 150 mm, and a pixel size of 8 μm.

An interesting consequence of the proposed method to increase the quality of the decrypted data is that it also makes straightforward the use of optical encryption in holographic displays. The reason is that both the encrypted data and its product with the FT of the key function [Eq. (2)] are nearly phase-only functions. This means that we can directly project it using a phase-only liquid crystal on silicon (LCoS) spatial

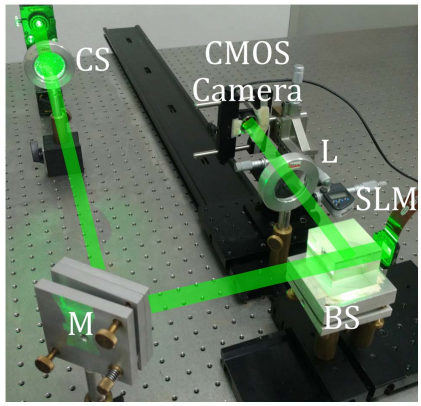

Fig. 4. Optical reconstruction scheme for decrypted data. M, mirror; L, lens; BS, beam splitter; CS, collimation system; SLM, spatial light modulator.

light modulator (SLM), performing a complete optical reconstruction of the object. However, it is worth noting that in holographic displays there are additional sources of noise than in the decryption-encryption process. In particular, the randomness of the phase in the reconstruction plane produces speckle, which is found in all diffuse holograms [17].

We now proceed to experimentally demonstrate the experimental reconstruction of decrypted objects by using the scheme of Fig. 4. To do this we take the phase of Eq. (2) obtained using both normal phase and ORAPs, using the same parameters as in the results of Fig. 3, discard its amplitude, and multiply it by a phase grating to achieve off-axis reconstruction of the object. This is necessary to avoid crosstalk with the nondiffracted light coming from the SLM in the reconstruction plane. The reconstruction is then performed optically with a converging lens.

As display we use a PLUTO-2-VIS-016 SLM with a resolution of 1920 × 1080 pixels and a pixel pitch of 8 μm. The SLM had 93% fill factor and 67% reflectivity, and was calibrated for a linear phase response in the range 0–2π. The light source was a diode-pumped solid-state (DPSS) laser with a wavelength of 532 nm and 150 mW of power. The reconstruction lens had a focal length of 150 mm. The intensity images of the reconstructed objects were registered using an EO-10012C CMOS camera with resolution of 3840 × 2748 pixels and pixel pitch of 1.67 μm.

First, we want to experimentally determine the optimal number of iterations of the G–S algorithm needed to generate the ORAPs for encryption and reconstruction of the decrypted data. To do this, we encrypted the same inputs of Fig. 3 using ORAPs with increasing number of iterations. Then, we calculated the correlation coefficient between the intensity of the experimentally decrypted objects and the original objects.

As we can see in Fig. 5, the correlation coefficient increases rapidly with the amount of iterations, until approximately 10 iterations. Further iterations produce a smaller gain in quality. Iteration number 0 corresponds to encryption–decryption using normal random phases.

In Fig. 6 we show the decrypted object with ORAPs generated with 10 iterations. As reference, we show the reconstruction of a Fourier phase-only hologram of the input object generated with 10 iterations of the G–S algorithm.

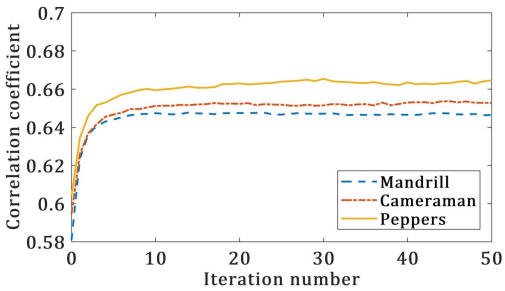

Fig. 5. Correlation coefficient between the intensity of experimentally decrypted data with ORAPs generated with increasing number of iterations and the original objects.

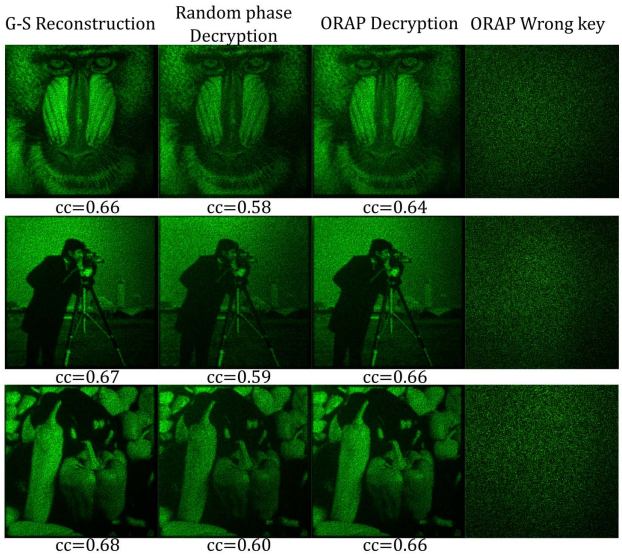

Fig. 6. Experimental reconstruction of phase-only holograms and decrypted objects.

We also show the correlation coefficients (CC) between the result and the original object (see inputs column in Fig. 3). As mentioned previously, there is additional degradation due to the random phase in the reconstruction plane; however, the reconstruction quality of the decrypted object is close to the reconstruction of the hologram generated with the G–S algorithm and surpasses the quality of the results with normal random phases. Additionally, we show the result of decryption with wrong keys. The resulting pattern is a stationary white noise, demonstrating that the ORAP does not compromise the security of the system.

The analysis and results shown in this Letter demonstrate a new approach to solve the issue of noise in double random phase encryption. We find that to eliminate the noise introduced by encryption with DRPE, both the FT of the object and the key must be phase-only functions. We accomplish this by replacing the random phases in DRPE encryption with ORAPs. ORAPs are obtained from a random phase using the G–S algorithm. The use of ORAPs instead of normal random phases means that the encrypted object is nearly a phase-only function, and its amplitude can be discarded without affecting the reconstruction. This makes straightforward the use of optical encryption in holographic displays that use phase-only spatial light modulators. The results shown in this Letter demonstrate that our proposal allows for a decryption quality similar to the reconstruction of a phase-only hologram, even with grayscale inputs with broad ranges of spatial frequencies. This technique opens up the possibility of using DRPE encryption in applications that were previously limited by the unwanted effects of noise. Furthermore, the mathematical and physical description of the DRPE scheme is not altered with the introduction of ORAPs instead of random phases; therefore, there should not be any vulnerabilities introduced with our proposal.

Funding. Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) (0849/16); Universidad Nacional de La Plata (UNLP) (11/I215); Comité para el Desarrollo de la Investigación-CODI (Universidad de Antioquia (UdeA), Colombia).

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

REFERENCES

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. W. Chen, B. Javidi, and X. Chen, Adv. Opt. Photon. **6**, 120 (2014).
3. 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, J. Opt. **18**, 083001 (2016).
4. T. Nomura and B. Javidi, Opt. Eng. **39**, 2031 (2000).
5. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, Opt. Lett. **30**, 1644 (2005).
6. X. Liu, J. Wu, W. He, M. Liao, C. Zhang, and X. Peng, Opt. Express **23**, 18955 (2015).
7. K. Falaggis, A. A. H. Ramírez, L. J. G. Gaxiola, C. Gutierrez Ojeda, and R. Porras-Aguilar, Opt. Lett. **41**, 4787 (2016).
8. H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, Opt. Express **18**, 13772 (2010).
9. A. Velez, J. F. Barrera, and R. Torroba, J. Opt. **19**, 105703 (2017).
10. J. F. Barrera, A. Mira, and R. Torroba, Opt. Express **21**, 5373 (2013).
11. A. Velez, J. F. Barrera, and R. Torroba, J. Opt. **18**, 125701 (2016).
12. J. M. Vilardy, M. S. Millán, and E. Perez-Cabré, J. Opt. **15**, 025401 (2013).
13. A. Velez, J. F. Barrera, and R. Torroba, J. Opt. **19**, 055704 (2017).
14. A. Velez, J. F. Barrera, and R. Torroba, Opt. Lett. **43**, 731 (2018).
15. E. Cuche, P. Marquet, and C. Depeursinge, Appl. Opt. **39**, 4070 (2000).
16. R. Gerchberg and W. Saxton, Optik **35**, 237 (1972).
17. D. Gabor, IBM J. Res. Dev. **14**, 509 (1970).