Optical triple random phase encryption

Esmail Ahouzi,[a,*] Wiam Zamrani,[a,*] Nawfel Azami,[a] Angel Lizana,[b] Juan Campos,[b] Maria J. Yzuel[b]

[a]Institut National des Postes et Télécommunications, Département EMO, Madinat Al Irfane, Rabat, 10000, Morocco
[b]Departament de Física, Universitat Autònoma de Barcelona, Bellaterra, 08193, Spain

Abstract. We propose an optical security technique for image encryption using triple random phase encoding (TRPE). In the encryption process, the original image is first double random phase encrypted. The obtained function is then multiplied by a third random phase key in the output plane, to enhance the security level of the encryption process. This method reduces the vulnerability to certain attacks observed when using the conventional double random phase encoding (DRPE). To provide the security enhancement of the proposed TRPE method, three attack cases are discussed: Chosen-plaintext attacks (CPA), Known-plaintext attacks (KPA) and chosen-ciphertext attacks (CCA). Numerical results are presented to demonstrate feasibility and effectiveness of the proposed method. Compared with conventional DRPE, the proposed encryption method can provide an effective alternative and has enhanced security features against the above-mentioned attacks.

Keywords: image encryption, cryptanalysis, double random phase encoding, optical security.

***First Authors, E-mail:** Ahouzi@inpt.ac.ma
Zamrani@inpt.ac.ma

1 Introduction

In recent years, research on optical techniques for image encryption has gained a great potential owing to their high parallel processing speed and large storage memories [1–10]. The main motivation for using optics for information security is that optical waveforms possess many complex degrees of freedom such as amplitude, phase, polarization, large bandwidth, nonlinear transformations, quantum properties of photons, and multiplexing that can be combined in many ways to make information encryption more secure and more difficult to attack. Several methods for optical image encryption have been proposed such as those based on digital holography [11,12], virtual optics [13], diffractive imaging [14], ghost imaging [15], ptychography [16], interferometry [17], polarization [18,19], photon-counting [20], etc. In 1995, Refrégier and Javidi [21], proposed the 'double random phase encoding' (DRPE) scheme. The DRPE method has awakened the interest of many authors and it has been extended to different canonical transforms which have been protected by several patents. Its principle consists in encrypting the input image into stationary white noise by using two random phase masks under a $4f$ optical processor. Recently, some experimental realization of the optical encryption-decryption have been achieved by researchers [22-25].

The strength of any good encryption scheme resides in its behavior against unauthorized resources that wants to reveal some encrypted information. The security of DRPE method has been thoroughly analyzed [24-41], showing that such scheme is robust against the brute force attack, and vulnerable to known-plaintext attack (KPA) [28-31], chosen-plaintext attack (CPA) [32-35], chosen-ciphertext attack (CCA) [36], and ciphertext-only attack [37,38,24,25]. In order to enhance security level of DRPE, multiple works have been proposed by several authors. Among them, Hennely and Sheridan [42] proposed an encryption scheme based on an image scrambling technique that uses the Jigsaw Transform. The image security of scrambling techniques was studied in Ref. [43]. In particular, efficient hierarchical chaotic image encryption (HCIE) algorithm was analyzed in detail and they concluded that the security of the HCIE against ciphertext-only attack was overestimated. Cheng et al. [44] proposed a security enhanced double random phase-amplitude encryption (DRPAE) by adding an undercover amplitude-modulating operation in the Fourier domain. They also demonstrated that the DRPAE can resist the traditional (KPA). However, Kumar et al. [34] have demonstrated the vulnerability of (DRPAE) scheme in front of a point spread function attack and He et al. [33] have proved that DRPAE is also vulnerable to a Hybrid two-step attack, which utilizes a chosen-plaintext attack followed by a known-plaintext attack. Recently, Elshamy et al. [45] proposed an optical image encryption method based on chaotic Baker map and DRPE, which consists of two layers. The first layer is a preprocessing chaotic baker map which performs the randomization of the image pixels and the second layer is the conventional DRPE. However, Zhang et al. [35] have demonstrated the vulnerability to chosen-plaintext attack (CPA) of the encryption model using scrambling preprocessing before DRPE. Recently, there are several attack methods that were proposed based on correlated imaging [39], ptychographical imaging [40] and wavefront shaping technique [41].

In this paper, we propose a triple random phase encryption (TRPE) scheme. In particular, the proposed encryption system has a major purpose, which is to improve the security of optical encryption based on double-random phase encryption (DRPE) in a 4f system against different type of attacks. This means that the TRPE method here proposed shows appropriate security levels in front of different particular attacks where the DRPE method fails. Note that the DRPE vulnerability in front of such specific attacks has been extensively proved by different authors in the literature.

Therefore, we want to emphasize that the extension of the DRPE by including a third random phase (TRPE method) is not only increasing the complexity of the system, in terms of more keys required to descript the system, but we want to show how specific attacks that already proved the DRPE vulnerability, are not effective when attacking a system encrypted with the TRPE method. Thus, the applicability and the security levels of the method are improved when compared with the DRPE approach.

In addition, we want to note that the number of the phase random keys used in the encryption process (TRPE case) to increase the security levels, does not correspond to a random guess, but it is the optimal key number in terms of applicability. This means that we have to look for the minimum number of keys providing enough security levels in front of the above-stated attacks, but leading to an optical scheme that can be experimentally implemented. As logical, a large number of random keys will lead to a bulky set-up of large complexity, which could not be practical for experimental proposes. However, in this paper we provide how by including just a third key, the resulting optical scheme can be still considered for an experimental implementation and the security levels are significantly improved.

The above-stated security novelty with a faceable optical scheme is provided thorough the paper by discussing three different attacks where the DRPE proves to be vulnerable: chosen-plaintext attacks (CPA), known-plaintext attacks (KPA) and chosen-ciphertext attacks (CCA). In all the analyzed cases, the security levels of the TRPE method are robust where the DRPE fails.

Accordingly, this paper is arranged as follows: in section 2, the theoretical method to design the proposed TRPE scheme is first described. In section 3, we present simulation results to illustrate the effectiveness of the proposed method by working out an example of a grayscale image and binary image of size (256×256 pixels). We further test the strength of this encryption process against CPA, KPA, and CCA. Finally, the main conclusions of the work are given in section 4.

2 TRPE basic concepts

Let us briefly describe the concept of optical encryption system based on a DRPE scheme. Let $f(x,y)$ be the input image to be encrypted, $e(x,y)$ the encrypted image, and $\phi_{k_1}(x,y)$ and $\phi_{k_2}(u,v)$ two random noises that are uniformly distributed over the interval [0, 1], where (x,y) and (u,v) denote the spatial and frequency domain coordinates, respectively. First, the input image $f(x,y)$ is multiplied by a phase-only mask $k_1(x,y)=\exp\left[i2\pi\phi_{k_1}(x,y)\right]$. Then, the image resulting from this product is Fourier transformed to the spatial frequency domain, where it is multiplied by a second random phase mask $k_2(u,v)=\exp\left[i2\pi\phi_{k_2}(u,v)\right]$. Finally, another Fourier transformation is applied to the obtained image, this leading to the final encrypted image. This process is mathematically described by:

$$e_{DRPE}(x,y)=\left\{f(x,y)\times\exp\left[i2\pi\phi_{k_1}(x,y)\right]\right\}\otimes h(x,y),$$

11* MERGEFORMAT ()

where × denotes the dot product , ⊗ denotes convolution and $h(x,y)$ is a mask whose inverse Fourier transform (FT) is equal to the $k_2(u,v)$ mask, i.e. $h(x,y)=FT\{k_2(u,v)\}=FT\left\{\exp\left[i2\pi\phi_{k_2}(u,v)\right]\right\}$.

We propose to add a third phase-only mask to the standard DRPE encryption scheme. Let us call this new encryption scheme as Triple Random Phase Encryption (TRPE). In particular, we suggest multiplying the $e_{DRPE}(x,y)$ image in Eq. (1) by the $k_3(x,y)=\exp\left[i2\pi\phi_{k_3}(x,y)\right]$ phase-only mask, where $\phi_{k_3}(x,y)$ is a random noise image limited within the range [0,1]. Under this scenario, the encrypted image for the proposed TRPE scheme is expressed as:

$$\begin{aligned}e_{TRPE}(x,y)&=e_{DRPE}(x,y)\times k_3(x,y)\\&=\left\{\left[f(x,y)\times\exp\left[i2\pi\phi_{k_1}(x,y)\right]\right]\otimes h(x,y)\right\}\times\exp\left[i2\pi\phi_{k_3}(x,y)\right]\end{aligned}$$

22* MERGEFORMAT ()

Due to symmetry considerations, the decryption process for the TRPE scheme is the reverse of the above-explained encryption process. First, the encrypted image $e_{TRPE}(x,y)$ is multiplied by the complex conjugate of the $k_3(x,y)$ phase mask, i.e. by $k_3^{¿}(x,y)$ (where the symbol * denotes complex conjugate). Then, the inverse Fourier transform (IFT) of the product is taken. The result is then multiplied by the complex conjugate of the second phase-only mask $k_2^{¿}(u,v)$. Finally, the IFT is taken once again on the resulting image, this transformation leading to the product of the input image $f(x,y)$ with the first mask used in the encryption process, $k_1(x,y)$. Therefore, this product is multiplied by $k_1^{¿}(x,y)$ and the decrypted image $f'(x,y)$ is obtained. The decryption process is mathematically written as,

$$\begin{aligned} f'(x,y) &= IFT\left\{ IFT\left[e_{TRPE}(x,y)\cdot k_3^*(x,y) \right]\cdot k_2^* \right\}\cdot k_1^* \\ &= IFT\left\{ IFT\left[e_{TRPE}(x,y)\cdot \exp\left[-i2\pi\phi_{k_3}(x,y)\right]\right]\cdot \exp\left[-i2\pi\phi_{k_2}(u,v)\right] \right\} \\ &\quad \cdot \exp\left[-i2\pi\phi_{k_1}(x,y)\right] \end{aligned}$$

33* MERGEFORMAT ()

For the sake of clarity, the flowchart of the encryption and decryption processes is shown in Figs. 1(a) and 1(b), respectively.

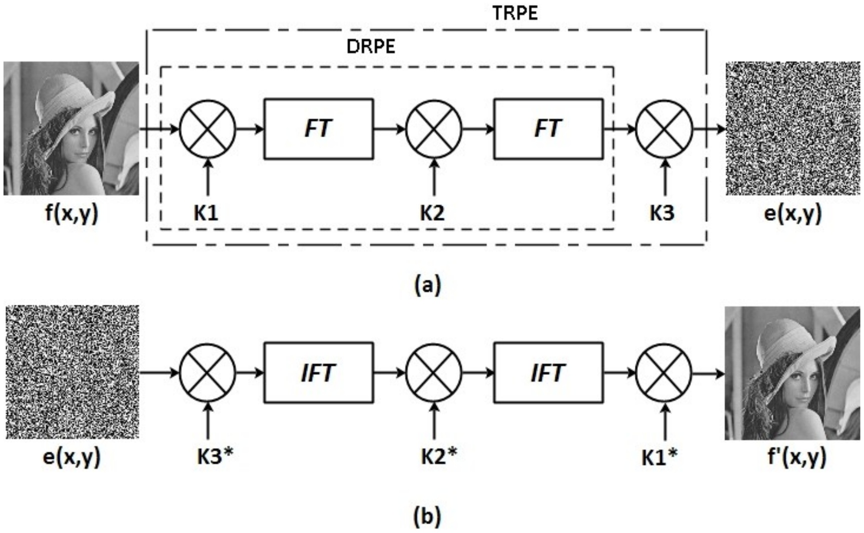

Fig. 1 The block diagrams for the TRPE scheme: (a) Encryption process; (b) Decryption process.

Afterwards, we also provide an example of a possible optical setup useful to implement the encryption process of the TRPE scheme (Fig. 2). The optical scheme is based on the well-known 4*f* optical processor (see Fig. 1(a)). Note that the function $e(x,y)$ in Fig. 1(a) is a complex valued function. Therefore, the 4*f* processor has to be experimentally implemented on an interferometric based set-up, this allowing us to both obtain the amplitude and the phase of the encrypted image. To this aim, we propose an optical scheme inspired on the phase-shifting interferometric correlation set-up implemented in Ref. [46], which was based on a March-Zehnder interferometer. In particular, a coherent monochromatic light source illuminates the optical system. The input beam is split in two light beams by means of a non-polarizing Beam-Splitter (BS1). The reflected beam, let us call it Reference Beam (RB), is filtered and collimated by using a spatial filter (PH1) properly combined with a convergent lens (L). Then, the RB is steered to the CCD, placed at the coordinate plane (X4,Y4), by using the Mirror 3 and a second Beam-Splitter (BS2). By contrast, the light transmitted on the BS1, let us call it as Transmitted Beam (TB), is filtered and collimated thanks to the combined action of the spatial filter (PH2) and the convergent lens (L1). Afterwards, the 4*f* optical processor is assembled by using the convergent lenses L2 and L3. The desired input object $f(x,y)$ is multiplied by the phase-only mask $k_1(x,y)$ at the (X1,Y1) plane. The phase function corresponding to the first key $k_1(x,y)$ can be physically implemented by addressing the function to a Spatial Light Modulator (SLM1) placed at the $(X1,Y1)$ plane. Next, the Fourier Transform (FT) of the phase function addressed to the SLM1 $(f(x,y)k_1(x,y))$ is obtained at convergent lens L2 focal lane, i.e. at the (X2,Y2) plane. At this plane, the SLM2 is placed, being responsible of generating the second phase mask, $k_2(u,v)$. Afterwards, the third phase-only mask, $k_3(x,y)$ is generated at the (X3,Y3) plane thanks to the use of the SLM3. Note that the FT of the phase distribution at the (X2,Y2) plane is obtained at the (X3,Y3) plane because of the lens L3. Finally, a convergent lens L4 images the (X3,Y3) plane on the CCD camera. This beam interferes with the reference beam, and the corresponding interference pattern is registered at the CCD camera. Note that this final intensity distribution can be subsequently used for the decryption process.

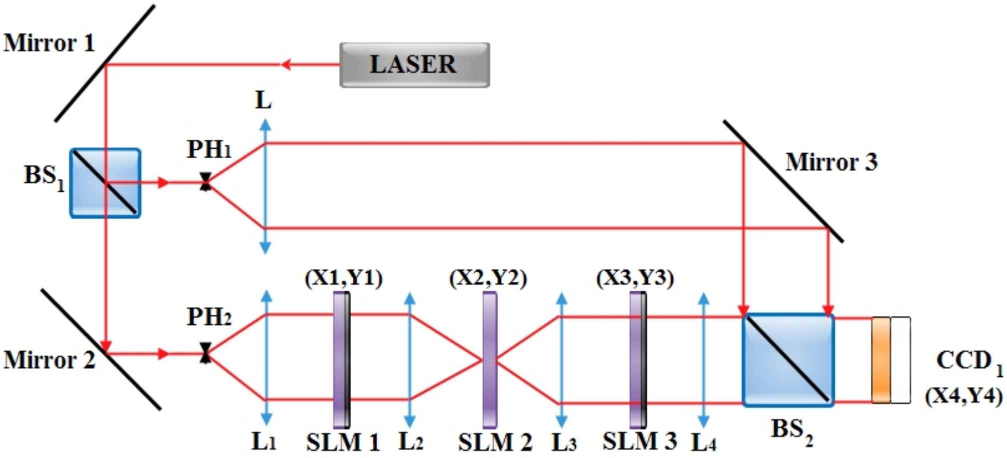

Fig. 2 Optical setup for the implementation of the encryption procedure of the TRPE scheme.

3 Numerical simulations and analysis

Numerical simulations were carried out to analyze the performance of the proposed encryption scheme. As illustrated in Fig. 3, the original images used for encryption in our case are: a multiple gray levels based image (Lena image, Fig. 3(a)) and a two-gray level based image (text "OPTICS", Fig. 3(e)). All the images used in this work present a size of 256×256 pixels. First, in Section 3.1., we test the suitability of the TRPE method for image encryption, as well as for retrieving original images after decryption. In addition, the robustness of the method under attacks using slightly modified keys for the decryption process is also analyzed. Afterwards, in Section 3.2, we prove the superior performance of the TRPE method under several attacks, when compared with the classical DRPE scheme.

3.1 TRPE encryption-decryption testing

Original images in Fig. 3 were encrypted by using the TRPE method, and the corresponding results are shown in Figs. 3(b) and 3(f), for the Lena image (Fig. 3(a)) and the binary text image (Fig. 3(e)) respectively. Afterwards, the decryption process explained in Section 2 (Eq.(3)) is applied on the encrypted images. To test the influence of the security keys on the decrypted images, the corresponding decrypted images are calculated under two different scenarios: (case A) on the basis of the exact masks k_1, k_2 and k_3, so the correct keys are used; and (case B) by using incorrect keys, i.e. keys resulting from applying some modification on the original keys.

In particular, we generated tree random masks k_1, k_2 and k_3 (see Figs. 4(a)-(c)) which were used for the encryption process. When using these exact three masks for decryption, we use the correct keys (case A). Then, we generated a fourth random mask, k4 (Fig. 4(d)). To perform the incorrect keys case (case B), we use the k_4 phase mask instead of the k_3 mask. Thus, the incorrect key case is performed by using the k_1, k_2 and k_4 phase-masks for the decryption process.

The decrypted images obtained by using the incorrect keys (case B) are shown in Figs. 3(c) and 3(g), for the Lena image and for the binary image respectively. By contrast, decrypted images obtained by using the correct keys (case A) are shown in Figs. 3(d) and 3(h) respectively.

To evaluate the quality of the decrypted images, we use the mean-square error (MSE) and the peak-signal-to noise (PSNR) metrics, which are calculated as,

$$MSE = \frac{1}{N \cdot M} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \left| f'\left(x, y\right) - f\left(x, y\right) \right|^2 ,$$

44* MERGEFORMAT ()

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\sqrt{MSE}} \right)$$

55* MERGEFORMAT ()

Where $f(x,y)$ and $f'(x,y)$ denote the original image and the decrypted image, respectively.

By using the decrypted images obtained from the correct keys (case A), the calculated MSE and PSNR values between the original Lena image (Fig. 3(a)) and the decrypted image (Fig. 3(d)) are of 1.28×10^{-31} and 357.05 respectively. For the binary image case (images in Figs. 3(e) and 3(h)), the MSE and PSNR obtained values are 3.52×10^{-32} and 362.65, respectively. The obtained values state for the similarity between the original and the decrypted images. In addition, obtained MSE and PSNR results are in the order of those obtained by using the standard DRPE, this providing the equivalence of the two methods when using correct keys.

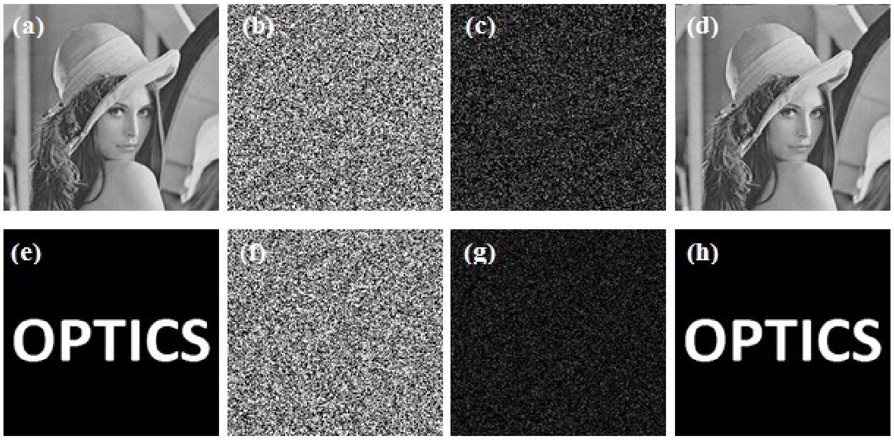

Fig. 3 (a) Lena image; (b) Lena encrypted image; (c) Lena decrypted image by using incorrect keys; (d) Lena decrypted image by using correct keys; (e) Binary text (BT) image; (f) encrypted BT image; (g) BT decrypted image by using incorrect keys; (h) BT decrypted image by using correct keys.

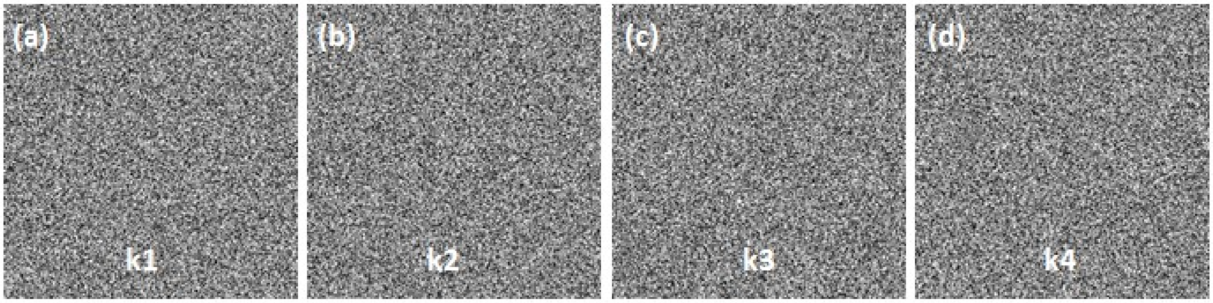

Fig. 4 Generated phase masks for the encryption-decryption steps.

3.2 TRPE cryptanalysis

To highlight the interest of using the TRPE method over the classical DRPE scheme, we tested the resistance of the proposed TRPE scheme against three different types of attacks: chosen-plaintext attack (CPA), known-plaintext attacks (KPA), and chosen-ciphertext attack (CCA). Those mentioned attacks have already been used to break the DRPE encryption system in the Fourier domain. A comparison of the security results obtained under the above-stated attacks for the two considered schemes (DRPE and the proposed TRPE) is also presented.

3.2.1 TRPE method resistance to chosen-plaintext attacks

In CPA, the attackers have the capability to choose arbitrary designed input plaintext in order to determine the secret keys. To perform the above-stated comparison between methods, we assume that the attackers choose a Dirac delta function $\delta\left(x,y\right)$ as a plaintext to be encrypted, as this approach has already proved the vulnerability of the DRPE scheme in Fourier and Fresnel domains [26,27,32,33].

The Dirac delta function can be written as,

$$\delta(x,y)=\begin{cases}1, & x=0,y=0\\ 0, & otherwise\end{cases},$$

66* MERGEFORMAT ()

Thus, the Dirac delta function is displayed as an image with only one nonzero value located at the center and all the other values being equal to 0. For a resolution of 256x256 pixels, this function is depicted in Fig. 5(a). For the sake of clarity, a 3D representation of the Dirac delta function is also provided at the bottom of Fig. 5(a).

Let us start the security analysis by analyzing the DRPE scheme. When the input image of the classical DRPE scheme is replaced with the Dirac delta function (i.e. $\left(f(x,y)=\delta(x,y)\right)$), Eq. (1) becomes,

$$e_{DRPE}(x,y)\Big|_{CPA}=\left\{\delta(x,y)\times\exp\left[i2\pi\phi_{k_1}(x,y)\right]\right\}*h(x,y)=h(x,y),$$

77* MERGEFORMAT ()

and thus, the obtained encrypted image $e_{DRPE}(x,y)\big|_{CPA}$ is equivalent to the $h(x,y)$ function, from which the phase mask $k_2(u,v)$ could be retrieved by applying the IFT of the $h(x,y)$ function. Note that if the object function $f(x,y)$ is a real function, it is not necessary to know the phase mask k_1 for the decryption process. Consequently, the attackers can retrieve the secret keys, and then reveal the input image.

The above-stated situation was analyzed in more detail for the Lena image case. To this aim, we used the DRPE method and the particular k_1 and k_2 keys stated in Section 3.1 (see Figs. 4 (a) and (b)). The following procedure was followed. First, by using $f(x,y)=\delta(x,y)$ in Eq. (1), the encrypted image in Fig. 5(b) was obtained. Second, we applied the FT on Eq. (1), this leading to,

$$FT\left\{e_{DRPE}(x,y)\right\}=FT\left\{f(x,y)\times\exp\left[i2\pi\phi_{k_1}(x,y)\right]\right\}\times FT\left\{h(x,y)\right\},$$

88* MERGEFORMAT ()

By replacing (7) into (8) and rearranging, we obtain,

$$f(x,y)\cdot\exp\left[i2\pi\phi_{k_1}(x,y)\right]=IFT\left[\frac{FT\left\{e_{DRPE}(x,y)\right\}}{FT\left\{e_{DRPE}(x,y)\big|_{CPA}\right\}}\right]$$

99* MERGEFORMAT ()

Afterwards, we used the encrypted Lena image $e_{DRPE}(x,y)$ (calculated by applying the DRPE method) in the numerator of Eq. (9) and the encrypted image $e_{DRPE}(x,y)\big|_{CPA}$ (obtained by using the Dirac delta function as an input function with the DRPE scheme; see image in Fig. 5(b)) in the denominator of Eq. (9). By doing this, and by applying the modulus of the obtained result, we finally recovered the information of the input image, as shown in Fig. 5(c). Therefore, by using the Dirac delta function as a chosen-plaintext image in the DRPE method, any encrypted input image can be retrieved.

For comparison, we repeated the same study but now for the proposed TRPE scheme. Note that when the input image is replaced by the Dirac delta function in Eq. (2) (TRPE case), this formula is rewritten as,

$$\begin{aligned}e_{TRPE}(x,y)\big|_{CPA}&=\left\{\left[\delta(x,y)\exp\left[i2\pi\phi_{k_1}(x,y)\right]\right]*h(x,y)\right\}\exp\left[i2\pi\phi_{k_3}(x,y)\right]\\&=h(x,y)\cdot\exp\left[i2\pi\phi_{k_3}(x,y)\right]\end{aligned}$$

1010* MERGEFORMAT ()

Note that according to the Eq. (10) we will be unable to directly retrieve any information of the used keys, as in the DRPE case given by Eq. (7). Thus, the relevant key information is still encrypted and an external chosen-plaintext attack based on the Dirac delta function does not retrieve the keys distributions.

We analyzed this statement by using again the Lena image as a particular case. To this aim, we used the exact phase masks k_2 and k_3 provided in Section 3.1 (see Figs. 4(b) and (c)) into the TRPE encryption process given in Eq. (10). By doing this, the Dirac delta function encrypted image $e_{TRPE}(x,y)\big|_{CPA}$ was obtained for the TRPE case, which is pictured in figure 5(d). Next, this calculated $e_{TRPE}(x,y)\big|_{CPA}$ image was introduced to the denominator of Eq. (9). By contrast, for the numerator we used the encrypted Lena image $e_{TRPE}(x,y)$, which was calculated by applying the TRPE method according to Eq. (2) (see Fig. 3(b)). Finally, we applied the modulus of the resulting image, this leading to the final decrypted image, which is pictured in Fig. 5(e). We see how the decrypted image presents a noisy appearance when dealing with the TRPE scheme. Therefore, unlike the traditional DRPE method, the TRPE scheme does not allow retrieving any information about the generated security keys by using the Dirac delta function as CPA. Consequently, the actual object image cannot be revealed.

The results provided in this sub-section invalidate the DRPE method to be used when chosen-plaintext attacks are conducted, in particular, when the Dirac delta function is used as CPA. Unlike this, the interest of using the TRPE method was highlighted because we proved its reliability and security under the same attack, showing that no input object information was retrieved.

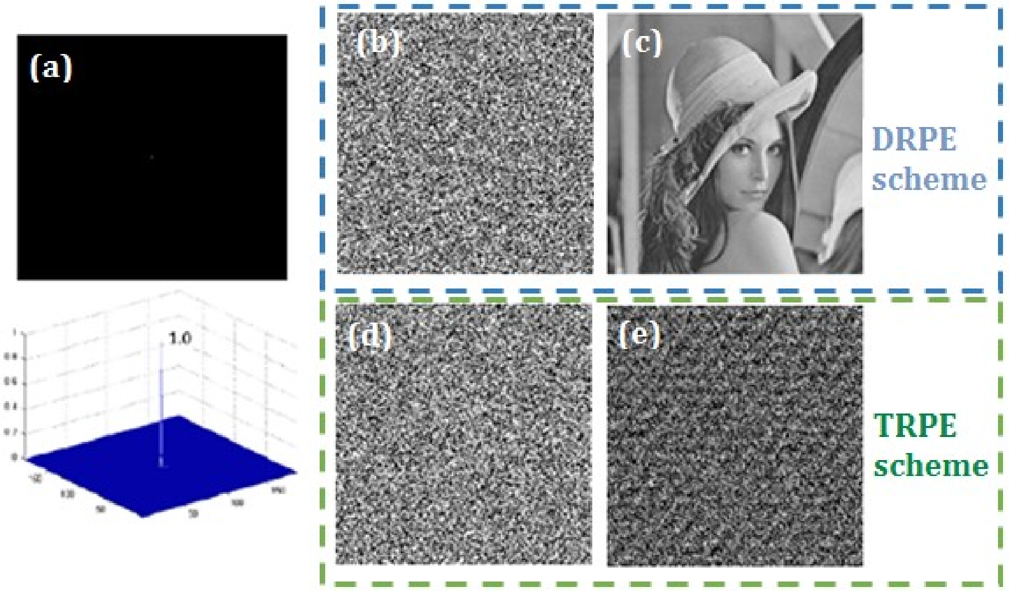

Fig. 5 (a) chosen plaintext (Dirac delta function), (b) encrypted image of DRPE with CPA, (c) decrypted image of DRPE with the CPA algorithm, (d) encrypted image of TRPE with CPA algorithm, (e) decrypted image of TRPE with CPA algorithm.

3.2.2 TRPE method resistance to known-plaintext attacks

In this section, we analyze the strength of TRPE encryption method against known-plaintext attack (KPA). In KPA the attackers have a priori knowledge of the encryption method as well as a pair of the plaintext and corresponding ciphertext. Gopinathan et al. proposed a known-plaintext attack scheme where the key is obtained through a simulated annealing process [28]. Afterward, Peng et al. demonstrated an approach to known-plaintext attack on DRPE system by using phase retrieval algorithm [29]. In our analysis we perform the KPA with an iterative process that is based on the Gerchberg-Saxton (GS) algorithm [47] in order to have the access to the phase key $k_1(x,y)$ in the input plane. Then, we deduce the second key $k_2(u,v)$ of the frequency plane from the retrieved $k_1(x,y)$.

In the case of the DRPE encryption scheme, the second key $k_2(u,v)$ can be retrieved using the following expression,

$$k_2(u,v)\big|_{DRPE} = \exp\left[i2\pi\phi_{k_2}(u,v)\right] = \frac{FT\left\{f(x,y)\,\phi_{k_1}(x,y)\right\}}{e_{DRPE}(u,v)},$$

1111* MERGEFORMAT ()

Figure 6 reveals the simulation results with the use of known-plaintext attack applied to DRPE encryption system. Figure 6(a) and 6(b) illustrate the input images used on the simulation. The corresponding encrypted images in the case of DRPE are presented in Figs. 6(c) and 6(e), respectively. The decrypted images obtained after going through the KPA algorithm are displayed in Figs. 6(d) and 6(f), respectively. As it shown, the decrypted images provide enough information to recognize the input images, proving the vulnerability of the DRPE scheme to known-plaintext attacks.

By contrast, if we try to explore the resistance of the proposed TRPE to KPA using the same above-described algorithm (Eq. 11), and after going through the retrieved random phase key k$_2$, we obtain,

$$k_2(u,v)\big|_{TRPE} = \exp\left[i2\pi\phi_{k_2}(u,v)\right] = \frac{FT\{\,f(x,y)\,k_1(x,y)\}}{e_{TRPE}(u,v)\,k_3(x,y)},$$

1212* MERGEFORMAT ()

We see from Eq. (12) that we are not able to retrieve the key $k_2(u,v)$ because the key $k_3(x,y)$ is still unknown. Figure 6 presents the conducted simulation results with the use of KPA algorithm to the proposed TRPE scheme. Figure 6(g) and 6(i) present the encrypted images corresponding to input images 6(a) and 6(b) respectively, in the case of the TRPE scheme. Figure 6(h) and 6(j) show the corresponding decrypted images when using the KPA algorithm. As shown in Figs. 6(h) and 6(j), the decrypted images are very noisy and the attack does not provide any information of the original input images. From these results we conclude that the TRPE scheme improves the vulnerability of DRPE against KPA.

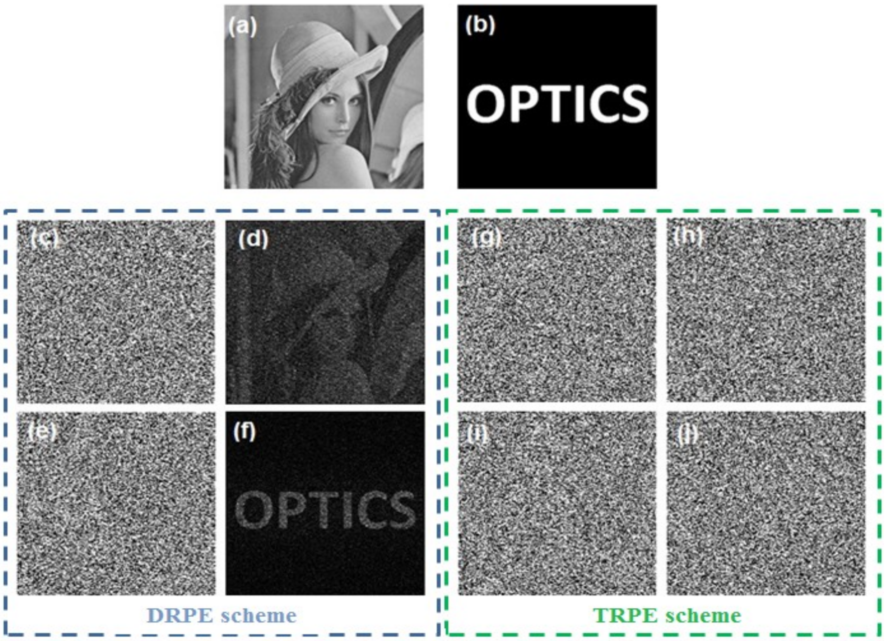

Fig. 6 (a) Lena input image; (b) binary text input image; (c) and (e) DRPE encrypted images of Lena and binary text, respectively; (d) and (f) DRPE decrypted images of Lena and binary text with KPA algorithm; (g) and (i) TRPE encrypted images of Lena and binary text, respectively; (h) and (j) TRPE decrypted images of Lena and binary text with KPA algorithm.

3.2.3 TRPE method resistance to chosen-ciphertext attacks

The chosen-ciphertext attack (CCA) is an attack model for cryptanalysis where the cryptanalyst can collect information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the attacker can attempt to recover the hidden secret keys used for decryption. To accomplish this attack, the attacker must be able to enter a one-to-many ciphertexts into the decryption system and then obtain the resulting plaintext. From this information, the secret keys can be recovered for use in the decryption process. We perform the CCA reported by Carnicer et al [34], where the attacker uses the ciphertext signal defined by the following expression,

$$e_b\left(x,y\right)\frac{1}{2}\left[\exp\left(i2\pi f_{x_1}x\right)\exp\left(i2\pi f_{y_1}y\right)+\exp\left(i2\pi f_{x_2}x\right)\exp\left(i2\pi f_{y_2}y\right)\right]$$

1313* MERGEFORMAT ()

The Fourier transform of $e_b(x, y)$ consists of two Dirac delta centered at frequencies (f_{x_1}, f_{y_1}) and (f_{x_2}, f_{y_2}) respectively, and it is given by,

$$FT\{e_b(u,v)\} = \frac{1}{2}\left[\delta\left(u - f_{x_1}, v - f_{y_1}\right) + \delta\left(u - f_{x_2}, v - f_{y_2}\right)\right]$$

1414* MERGEFORMAT ()

In the optical decryption system, the captured intensity would have a cosine-type distribution, such as the following one [4],

$$\left|f_b^{'}(x,y)\right|^2 = \frac{1}{2} + \frac{1}{2}\cos\left[\begin{array}{l} 2\pi\left(f_{x_1} - f_{x_2}\right)x + 2\pi\left(f_{y_1} - f_{y_2}\right)y \\ +\phi_{k_2}\left(f_{x_2}, f_{y_2}\right) - \phi_{k_2}\left(f_{x_1}, f_{y_1}\right) \end{array}\right]$$

1515* MERGEFORMAT ()

Where ϕ_{k_2} represents the phase distribution of the key used in Fourier plane ($k_2(u, v) = \exp\left[i 2\pi \phi_{k_2}(u, v)\right]$).

The value of the phase difference $\phi_{k_2}(f_{x_2}, f_{y_2}) - \phi_{k_2}(f_{x_1}, f_{y_1})$ can be computed with respect to a reference, and then the decryption key can be completely recovered. In the case of DRPE the light distribution at the output is given by:

$$f_b^{'}(x,y)\Big|_{DRPE} = FT\left[e_b(u,v)\, k_2^{*}(u,v)\right]$$

1616* MERGEFORMAT ()

If we apply the same algorithm described above on the TRPE, the light distribution at the output will be,

$$f_b^{'}(x,y)\big|_{TRPE} = FT\Big\{ FT \text{��}_b(x,y)\, k_3^{*}(x,y) \text{���} k_2^{*}(u,v)\Big\},$$

1717* MERGEFORMAT ()

According to Eq. (17), the designed ciphertext $e_b(x,y)$ is distorted by the random phase mask $k_3^{\text{¿}}(x,y)$ and becomes an optical random function. Thus, the attacker cannot collect any useful information by obtaining the decryptions of chosen ciphertexts. As reported by Carnicer et al [36], ciphertext attack is only efficient for real input signal. Hence, TRPE anticipates any kind of ciphertext attack due to the complex nature of the random phase mask.

4 Conclusion

Summarizing, we propose a new method on image encryption which is based on a Triple Random Phase Encoding (TRPE) scheme. The TRPE is achieved by extending the well-known Double Random Phase Encryption (DRPE) technique by adding an extra randomly generated phase-only mask at the output plane.

The performance of the TRPE method was tested by conducting some numerical simulations. We found that the TRPE scheme leads to a performance equivalent to that of the DRPE method for the encryption-decryption process, in terms of mean-square error and peak-signal-to noise metrics. In addition, the TRPE scheme enhances the performance of the DRPE method in terms of security. Such improvement is proved by testing the method against different attacks to which the DRPE method is vulnerable: chosen-plaintext attacks (CPA), known-plaintext attacks (KPA) and Chosen-ciphertext attacks (CCA).The results obtained by using the TRPE scheme fulfill the requirements of invisible content, and thus, an illegal user neither can recover the decryption keys nor any plaintext. Therefore, the TRPE scheme proved its resistance to the attack above mentioned in comparison with the DRPE and finds application in security data.

References

1. B. Javidi, ed., *Optical and Digital Techniques for Information Security (Advances Sciences and Technologies for Security Applications)*, Springer-Verlag, (2005).

2. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millán, and B. Javidi, “Optical techniques for information security,” *Proceedings of the IEEE* , **97**, 1128–1148 (2009).

3. A. Alfalou and C. Brosseau, “Optical image compression and encryption methods,” *Adv. Opt. Photon.* **1**, 589–636 (2009).

4. M. S. Millán and E. Pérez-Cabré, *Optical data encryption, Optical and Digital Image Processing: Fundamentals and Applications*, G. Cristobal, P. Schelkens and H. Thienpont, ed., Verlag: Wiley-VCH, (2011).

5. W. Chen, B. Javidi and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon*. **6**, 120–155 (2014).

6. S. Liu, C-L. Guo and J. T. Sheridan, “A review of optical image encryption techniques,” *Opt. Lasers Eng.* **57**, 327–342 (2014).

7. B. Javidi and E. Ahouzi, “Optical security system with Fourier plane encoding,” *Appl. Opt.* **37**, 6247–6255 (1998).

8. B. Javidi, A. Sergent, and E. Ahouzi, “Performance of double phase encoding encryption technique using binarized encrypted images,” *Opt. Eng*. **37**, 565–569 (1998).

9. 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**, (2016).

10. W. Zamrani, E. Ahouzi, A. Lizana, J. Campos, and M. J. Yzuel, “Optical image encryption technique based on deterministic phase masks,” *Opt. Eng*. **55**, 103108 (2016).

11. B. Javidi and T. Nomura, “Securing information by use of digital holography,” *Opt. Lett*. **25**, 28–30 (2000).

12. E. Tajahuerce and B. Javidi, “Encrypting three-dimensional information with digital holography,” *Appl. Opt*. **39**, 6595–6601 (2000).

13. X. Peng, Z. Cui, and T. Tan, “Information encryption with virtual-optics imaging system,” *Opt. Commun*. **212**, 235–245 (2002).

14. W. Chen, X. Chen, and C. J. R. Sheppard, “Optical image encryption based on diffractive imaging,” *Opt. Lett*. **35**, 3817–3819 (2010).

15. P. Clemente, V. Durán, V. Torres-Company, E.Tajahuerce, and J. Lancis, “Optical encryption based on computational ghost imaging,” *Opt. Lett*. **35**, 2391–2393 (2010).

16. Y. Shi, T. Li, Y. Wang, Q. Gao, S. Zhang, and H. Li, “Optical image encryption via ptychography,” *Opt. Lett*. **38**, 1425–1427 (2013).

17. Y. Zhang and B. Wang, “Optical image encryption based on interference,” *Opt. Lett*. **33**, 2443–2445 (2008).

18. N. Zhu, Y. Wang, J. Liu, J. Xie, and H. Zhang, “Optical image encryption based on interference of polarized light,” *Opt. Express* **17**, 13418–13424 (2009).

19. A. Alfalou and C. Brosseau, “Dual encryption scheme of images using polarized light,” *Opt. Lett*. **35**, 2185–2187 (2010).

20. E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” *Opt. Lett*. **36**, 22–24 (2011).

21. P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett*. **20**, 767–769 (1995).

22. A. V. Zea, J. F. Barrera, and R. Torroba, “Experimental optical encryption of grayscale information,” *Appl. Opt*. **56**, 5883-5889 (2017).

23. 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).

24. G. Li, L. Dayan, and G. Situ, "Optical image encryption based on classical double random phase encoding: Cyphertext-only attack via speckle correlation," in *Digital Holography and Three-Dimensional Imaging*, OSA Technical Digest (online) (Optical Society of America, 2017), paper Th2A.4.

25. 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).

26. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* **15**, 10253–10265 (2007).

27. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "*Security analysis of optical encryption*," in Un-manned/Unattended Sensors and Sensor Networks II, E. M. Carapezza, ed., Proc. SPIE 5986, 25-34 (2005).

28. U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Express* **14**, 3181–3186 (2006).

29. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett*. **31**, 1044–1046 (2006).

30. G. Situ, G. Pedrini, and W. Osten, "Strategy for cryptanalysis of optical encryption in the Fresnel domain," *Appl. Opt*., **49**, 457—462 (2010).

31. W. Qin and X. Peng, "Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys," J. Opt. A, Pure Appl. Opt., 11, (2009).

32. X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett*. **31**, 3261–3263 (2006).

33. W. He, X. Peng, and X. Meng, “A hybrid strategy for cryptanalysis of optical encryption based on double-random phase-amplitude encoding,” *Opt. Laser Technol*., **44**, 1203–1206, (2012)

34. P. Kumar, A. Kumar, J. Joseph, and K. Singh, “Vulnerability of the security enhanced double random phase amplitude encryption scheme to point spread function attack,” *Opt. Lasers Eng*. **50**, 1196–1201 (2012).

35. Y. Zhang, D. Xiao, W. Wen, and H. Liu, “Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding,” *Opt. Lett*. **38**, 4506–4509 (2013).

36. 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).

37. X. Peng, H. Tang, and J. Tian, “ Ciphertext-only attack on double random phase encoding optical encryption system,” Acta. Phys. Sinica, 56, 2629–2636, (2007).

38. 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. Exp*., **23**, 18955–18968, (2015).

39. J. Wu, W. Liu, Z. Liu, and S. Liu, “ Correlated-imaging-based chosen plaintext attack on general cryptosystems composed of linear canonical transforms and phase encodings,” *Opt. Commun*., **338**, 164–167, (2015).

40. T. Li and Y. Shi, “Attack on optical double random phase encryption based on the principle of ptychographical imaging,” *Chin. Phys. Lett*., **33**, (2016).

41. M. Liao, D. Lu, W. He, X. Peng, “Optical cryptanalysis method using wavefront shaping,” *IEEE Photonics J*., **9**, (2017).

42. B. Hennelly and J. T. Sheridan, “Optical image encryption by random shifting in fractional Fourier domains,” *Opt. Lett*. **28**, 269–271 (2003).

43. C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Sign. Proc.*, **118**, 203–210, (2016).

44. X. C. Cheng et al, "Security enhancement of double-random phase encryption by amplitude modulation," *Opt. Lett*. **33**, 1575–1577 (2008).

45. A. M. Elshamy, A. N. Z Rashed, Abd El-Naser A. Mohamed, O. S. Faragalla, Y. Mu, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding,"*J. of Lightwave Technology*, **31**, 2533–2539 (2015).

46. E. Ahouzi et al., "Pattern recognition with a phase-shifting interferometric correlator Discrimination-capability enhancement," *Appl. Phys. B Lasers and Opt*. **64**, 331–338 (1997).

47. R. Gerchberg and W. Saxton, " A practical algorithm for the determination of phase from image and diffraction plane pictures," *Optik* **35**, 237–246 (1972).

Caption List

Fig. 1 The block diagrams for the TRPE scheme: (a) Encryption process; (b) Decryption process.

Fig. 2 Optical setup for the implementation of the encryption procedure of the TRPE scheme.

Fig. 3 (a) Lena image; (b) Lena encrypted image; (c) Lena decrypted image by using incorrect keys; (d) Lena decrypted image by using correct keys; (e) Binary text (BT) image; (f) encrypted BT image; (g) BT decrypted image by using incorrect keys; (h) BT decrypted image by using correct keys.

Fig. 4 Generated phase masks for the encryption-decryption steps.

Fig. 5 (a) chosen plaintext (Dirac delta function), (b) encrypted image of DRPE with CPA, (c) decrypted image of DRPE with the CPA algorithm, (d) encrypted image of TRPE with CPA algorithm, (e) decrypted image of TRPE with CPA algorithm.

Fig. 6 (a) Lena input image; (b) binary text input image; (c) and (e) DRPE encrypted images of Lena and binary text, respectively; (d) and (f) DRPE decrypted images of Lena and binary text with KPA algorithm; (g) and (i) TRPE encrypted images of Lena and binary text, respectively; (h) and (j) TRPE decrypted images of Lena and binary text with KPA algorithm.

Esmail Ahouzi received his degree in physics from the University Sidi Mohamed Ben Abdellah, Fes, Morocco, in 1990 and his MS and PhD degrees from the Autonomous University of Barcelona in 1992 and 1996, respectively. He made a postdoctoral stay at the University of Connecticut in 1997 and is a research collaborator at the Autonomous University of Barcelona. Since 2000 he has been a full professor of optical communications with the Institut National des Postes et Telecommunications. His research involves optical pattern recognition and filter behavior characterization. He is a member of the Spanish Optical Society (SEDO), the European Optical Society, OSA, and the Optical Moroccan Society (SMOP).

Wiam Zamrani received the B.S. degree in Electronics Electrotechnics and Automatic in 2010 and the M.S. degree in Laser Instrumentation and Optoelectronic Components in 2012. She is currently a Ph.D. student in the department of Optics and Embedded Microwave for Telecommunication at the National Institute of Posts and Telecommunication, Rabat. Her research interests are in optical information processing, encryption techniques and pattern recognition. She is a member of SPIE and OSA.

Nawfel Azami received his MS and PhD degrees from the University of Nice-Sophia Antipolis in 1995 and 1998. He worked as new products manager at medi telecom operator. From 2000 to 2004 he worked as research scientist at optical technologies, an optical telecommunication devices manufacturer in Canada. Since 2004 he has been a full professor of optical communications at National Institute of Posts and Telecommunications. His research involves optical devices and systems design.

Angel Lizana completed his MSc degree in physics and his PhD in physics at the Autonomous University of Barcelona (Spain) in 2006 and 2011, respectively. His research interests include polarimetry and diffractive optics. He has been a postdoctoral scientist in the Laboratoire de Physique des Interfaces et des Couches Minces (LPICM) of the École Polytechnique (France) in 2011–2012 and in 2013–2014. He has been a postdoctoral researcher at the Autonomous University of Barcelona (UAB), since 2014.

Juan Campos received his BSc and MSc degrees in physics from University of Zaragoza, Spain, in 1981 and his PhD degree at the Universitat Autònoma de Barcelona, Spain, in 1986. Currently, he is a full professor at this University. He has worked in the fields of image quality evaluation, optical pattern recognition, spatial light modulators, polarimetry, and surface shape metrology. He is a fellow member of the SPIE, OSA, and EOS.

María J. Yzuel obtained the MSc and PhD degrees in physics from the University of Zaragoza (Spain) in 1962 and 1966, respectively. She has been a professor of optics at the Universities of Zaragoza and Granada, and from 1983 to 2011 she has been a full professor at the Autonomous University of Barcelona. She is currently Emeritus Professor. She has worked in the field of diffraction image theory and image quality evaluation as well as in optical pattern recognition. She has also contributed during several years in the field of image techniques in medical diagnosis (gammagraphy and radiology). She is a Fellow of OSA, IOP, SPIE, EOS, SEDOPTICA and RSEF. She was the president of the Spanish Optical Society from 1993 to 1996. She was a vice-president of the International Commission of Optics from 1990 to 1996 and currently from 2011 to 2017. She was the secretary general of the European Optical Society from 1996 to 1998. Member of the SPIE Board of Directors 2001-2003. She received in 2005 the SPIE Board of Directors Award. She was Vice-President, President and Past-President of the SPIE from 2007 to 2010.