111Equation Chapter 1 Section 1Optical image encryption technique based on deterministic phase masks

Wiam Zamrani,[a,*] Esmail Ahouzi,[a] Angel Lizana,[b] Juan Campos,[b] María 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. The double random phase encoding (DRPE) scheme, which is based on a 4f optical correlator system, is considered as a reference for the optical encryption field. In this work, we propose a modification of the classical DRPE scheme based on the use of a novel class of structured phase masks, the deterministic phase masks. In particular, we propose to conduct the encryption process by using two deterministic phase masks, which are built from linear combinations of several sub-keys. For the decryption step, the input image is retrieved by using the complex conjugate of the deterministic phase masks, which were set in the encryption process. This new concept of structured masks gives rise to encryption-decryption keys which are smaller and more compact than those required in the classical DRPE. In addition, we show that our method significantly improves the tolerance of the DRPE method to shifts of the decrypting phase mask –when no shift is applied, it provides similar performance to the DRPE scheme in terms of encryption-decryption results-. This enhanced tolerance to the shift, which is proven by providing numerical simulation results for gray-scale and binary images, may relax the rigidity of an encryption-decryption experimental implementation set-up. To evaluate the effectiveness of the described method, the mean-square-error (MSE) and the peak signal-to-noise ratio (PSNR) between the input images and the recovered images are calculated. Different studies based on simulated data are also provided to highlight the suitability and robustness of the method when applied to image encryption-decryption processes.

Keywords: optical encryption, 4f correlator, image processing, random phase encoding.

***First Author**, E-mail: zamrani@inpt.ac.ma

1 Introduction

Optical technologies have become increasingly important for securing information, recognition, and have been widely explored to encrypt sensitive information because of their high-speed operation, parallel processing and multiple dimensional capabilities.[1-8] Optical security includes numerous parameters for encryption including wavelength, phase information, spatial frequency and polarization of light. Several optical encryption techniques have been suggested with the aim to broaden the research area of information security[3,4,5,6]. Among them, Réfrégier and Javidi proposed a forefather optical encryption method based on a double random phase encoding (DRPE)[7]. By using this encryption technique, which may be implemented by means of a

Vanderlugt 4f processor, original data embedded in two-dimensional amplitude information is transformed into a white stationary noise. This is done by setting two random phase masks in the input and the Fourier planes. Since the publication of this method, the DRPE scheme has been applied in different domains, such as fractional Fourier transform (FRT)[9,10], Fresnel transform (FrT)[11,12,13], gyrator transform (GT)[14,15], quaternion Fourier transform[16], diffractive imaging[17], dual fractional Fourier-wavelet[18], fractional Mellin[19], and Hartley transform[20]. Nevertheless, it has been demonstrated that DRPE scheme is vulnerable to some type of attacks[21,22,23] and due to its high shift sensitivity, it requires high alignment accuracy in the spatial domain systems. In this regard, several methods have been proposed to improve the shift tolerance of the decrypting phase mask[24,25]. Nomura and Javidi[26] proposed an optical double random phase encryption method using a joint transform correlator (JTC) architecture. Seo and Kim[25] suggested instead a scheme applying a virtual phase image to conceal the original one under a JTC architecture that is robust to shift of the encrypted image. These methods do not produce complex conjugates of the phase key and therefore suffer from autocorrelation terms that appear in the output plane. In addition, in the above-stated methods, the decryption process is performed by optical schemes based on a 4f correlator which still require an extremely precise alignment. To increase the security, asymmetric cryptosystem has been proposed, for instance, by Rajput and Nishchal[27] to make the decryption keys different from the encryption ones. Other alternatives to the classical DRPE scheme describe the use of structured phase masks in the encryption-decryption process based on Fresnel zone plate (FZP), toroidal zone plate (TZP) or radial Hilbert mask (RHM). Barrera et al[28,29] introduced toroidal phase masks as an alternative. Tebaldi et al[30] presented results on image encryption based on fractal encrypting masks. Abuturab[31] proposed a color information security scheme based on Arnold transform in the GT domain, in which the phase function of FZP is used to generate double structured phase masks. Vashisth et al[32] presented an image encryption by employing the phase retrieval algorithm in the fractional Mellin transform domain, in which two structured phase masks are constructed based on TZP and RHM, respectively. Singh et al[33] proposed the double phase-image encryption using GTs, in which the structured phase mask is derived from DVFL in the frequency plane. Some recent studies have also introduced structured phase mask based on devil's vortex Fresnel lens (DVFL)[34,35,36,37,38].

To properly use an encryption method in security applications, the system must be resistant to potential loss of data during the decryption process and very tolerant to alignment accuracy. To fulfill such requirements, in this paper we propose a modification of the DRPE encryption scheme, based on a novel category of structured masks that we called deterministic phase masks. Such deterministic masks, based on a linear combination of several sub-keys, allow the system to enhance the optical alignment tolerance to shifts of the required phase masks when compared to the classical DRPE method. Another advantage of our method is the compact and tiny size of the encoding-decoding keys, facilitating the keys exchange process. In addition, there is no need to send the mask itself for reconstruction, but only a small set of numerical parameters. This situation may substantially prevent the loss of information of the keys.

The outline of this manuscript is as follows: First, the principle of the encryption-decryption algorithm and the masks generation are described in Sec. 2. Sec. 3 presents several simulated results as a proof of concept of the proposed method. In particular, the encryption-decryption of two different images is analyzed: (*i*) a black and white text image; and (*ii*) a 256 gray-scale image. To evaluate the quality of the recovered images, the mean-square-error (MSE) and the peak signal-to-noise ratio (PSNR) between the input images and the recovered images are calculated. Next, the robustness of the deterministic phase masks based method is studied in Sec.

4. Three different situations are analyzed: Robustness to shifts of the phase masks in the Fourier plane (Sec. 4.1), robustness to loss of encrypted data (Sec. 4.2), and robustness to deterministic keys attacks (Sec. 4.3). Finally, the main conclusions of the work are provided in Sec. 5.

2 Principle of the encryption-decryption method

In this section, we first review the DRPE optical setup, which is used to conduct the deterministic keys approach that we propose (sub-Sec. 2.1). Afterwards, in sub-Sec. 2.2, we provide the theoretical background for the generation of deterministic masks.

2.1. Encryption and decryption schemes

The scheme for image encryption and decryption we propose in this work requires the use of the novel deterministic based masks. For the proper implementation of them, we use a modification of the well-known DRPE optical setup, which is based on a Vanderlugt $4f$ system. The schemes for the encryption and decryption processes are shown in Figs. 1(a) and 1(b) respectively, where L1 and L2 are two convergent lenses of focal length *f* and DK1 and DK2 are the generated deterministic phase masks.

During the encryption stage, the input image to be encrypted $f(x,y)$ is first multiplied by a deterministic phase mask $(DK1)$ in the input plane. The resulting complex image is Fourier transformed, and then multiplied by a second deterministic phase mask $(DK2)$ in the frequency plane. The encrypted image is then obtained by performing inverse Fourier transform (IFT). Note that in an optical scheme as in Fig. 1, the operation to be performed is not the IFT but the direct FT. In the simulated case, the complex output encrypted image $c(x,y)$ can be written as:

$$c\left(x,y \right)=IFT\left\{ FT\left\{ f\left(x,y \right)\cdot DK1\left(x,y \right) \right\}\cdot DK2\left(u,v \right) \right\},$$

22* MERGEFORMAT ()

where $FT\{.\}$ and $IFT\{.\}$ represent the Fourier transform and inverse Fourier transform, respectively. The decryption process is the reverse of the encryption process, where the encrypted image is Fourier transformed, and then multiplied by the complex conjugate of the mask $\left(DK2\right)$. An inverse Fourier transform is then performed, followed by multiplication by the complex conjugate of the first mask $\left(DK1\right)$. The decrypted image $f^{'}\left(x,y\right)$ can be expressed as:

$$f^{'}\left(x,y \right)=IFT\left\{ FT\left\{ c\left(x,y \right) \right\}\cdot DK2^{*}\left(u,v \right) \right\}\cdot DK1^{*}\left(x,y \right), \qquad 3$$

3* MERGEFORMAT ()

where * indicates the conjugate of the deterministic phase mask.

Note that in the case of registering the intensity of the decrypted image, the multiplication by DK1* is not needed.

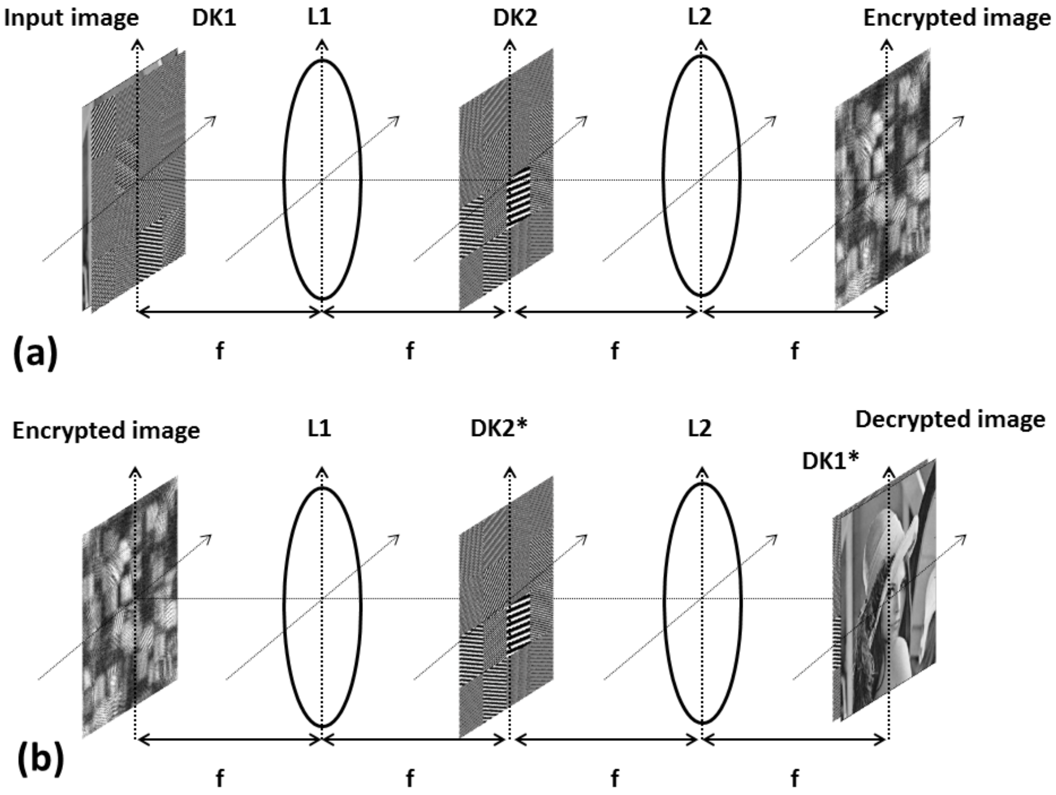

Fig. 1 Optical scheme for: (a) encryption process; and (b) decryption process.

As an example, an optical architecture has been depicted with the aim to implement the encryption-decryption scheme shown in Fig. 1. The setup of such architecture is presented in Fig. 2.

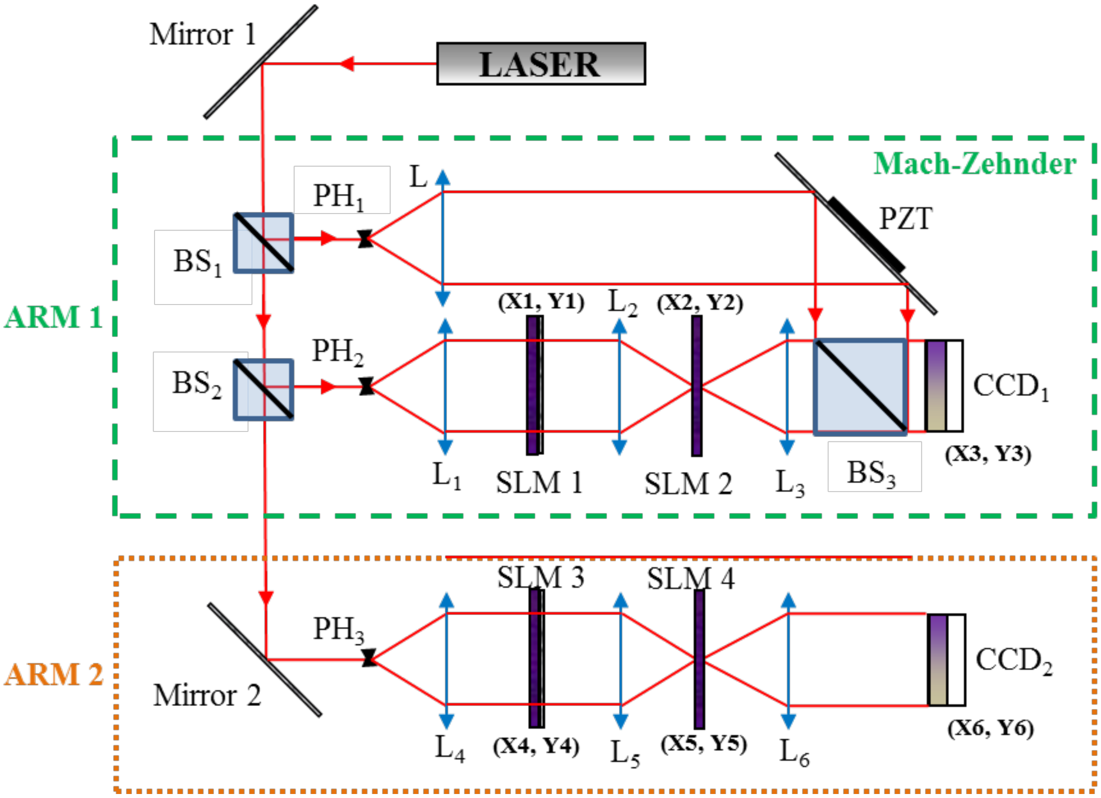

Fig. 2 (M) mirror, (BS) beam Splitter, (L) lenses, (PH) pinhole, (SLM) Spatial light modulator, (CCD) CCD camera, (PZT) piezo-electric transductor. **ARM1** phase-shifting interferometric correlator for image encryption. A 4f correlator (L1-L3) is introduced in the arm of a Mach-Zehnder interferometer (BS1, BS2, PZT, BS3). In this way we obtain the interferences of the encrypted image with a reference wave on CCD1 camera where the interferences are digitalized. **ARM2** the encrypted image is displayed in the SLM3 and its Fourier transform is obtained at the SLM4 plane. Finally the decrypted image is formed at the CCD2 camera.

The setup sketched in Fig 2 consists of two optical arms. In the ARM1 (green dashed line) the encrypted image is obtained, while in the ARM2 the decryption process is performed. In the ARM1, the 4f correlator in Fig 1(a) is introduced in a Mach-Zehnder interferometer (Phase-Shifting Interferometric Correlator[39]) to obtain the amplitude and phase of the encrypted image. The keys DK1 and DK2 are introduced on SLM1 and SLM2 respectively. In the ARM2 (orange dotted line), the 4f correlator of Fig 1(b) is implemented. The encrypted image is introduced in the SLM3 and the propagated beam is Fourier transformed by means of the convergent lens L_5. At the Fourier plane, the key DK2* is introduced on the SLM4, and finally the decrypted image is recorded by the CCD2. In ARM1 a single interference can be recorded. In this case a tilted reference should be used to separate the different diffracted orders. The same tilted reference has to be used in ARM2.

2.2 Deterministic masks generation

The first step in the deterministic mask (DK) construction procedure consists in defining an order of encryption (m) to specify the number of sub-keys (*NS*) into the mask, where $NS=(2^m \times 2^m)$. By setting the value of *m* (*m* is an integer number), we split the input image in NS equal sub-blocks of size $d=dim/2^m$, where (dim) is the size of the input image. Then, we generate a linear phase with random orientation and frequency for each available sub-key.

For simplicity, we show an example for the case $m=2$. Thus, we consider a deterministic key (DK) with size (256×256) divided into 16 sub-keys of size (64×64), where $d=dim/2^2$. The resulting DK can be written as a linear combination of the stated 16 sub-keys M_{ij}, as shown by the following relation:

$$DK=\sum_{i=1}^{4}\sum_{j=1}^{4} M_{ij}\left(d \times d\right), \qquad 4$$

4* MERGEFORMAT ()

More precisely, to set each particular sub-key to an appropriate spatial position, we construct the complete DK image in the spatial domain by using the following equation (for $m=2$):

$$DK_1\left(x,y\right)=\sum_{i=1}^{4}\sum_{j=1}^{4} rect\left[\frac{x-\left(i-\frac{1}{2}\right)d}{d},\frac{y-\left(j-\frac{1}{2}\right)d}{d}\right] M_{ij}\left(x,y\right), \qquad 5$$

5* MERGEFORMAT ()

where x and y are defined into the interval $\left[1, dim\right]$ and $rect$ is the rectangle function described as:

$$rect\left(x, y\right) = \begin{cases} , & for\left|x\right| < \frac{1}{2} and \left|y\right| < \frac{1}{2}, \\ 0, & otherwise \end{cases} \qquad 6$$

6* MERGEFORMAT ()

and M_{ij} is defined by:

$$M_{ij}\left(x, y\right) = exp\left(i2\pi\left(u_k.x + v_k.y\right)\right) = exp\left(i\varphi_{ij}\left(x, y\right)\right), \ k = 1,..,NS, \qquad 7$$

7* MERGEFORMAT ()

where u_k and v_k are randomly generated in the interval $\left[1, d\right]$.

To illustrate the above described procedure, an example of a deterministic key generated for *m*=2 is illustrated in Fig. 3.

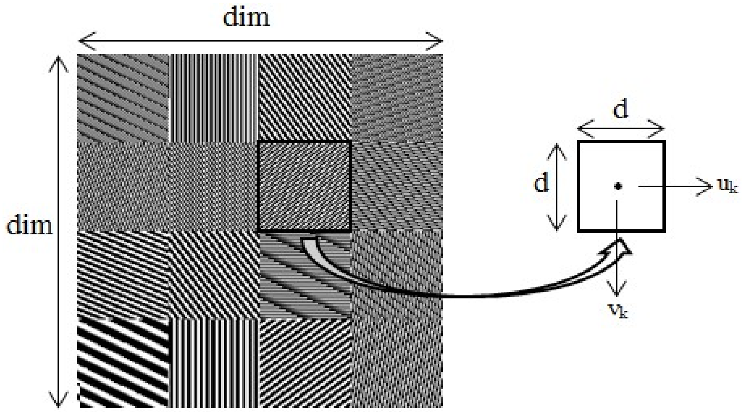

Fig. 3 Generation of deterministic keys.

In addition, the same scheme shown above for *m*=2 can be generalized for an arbitrary *m* value, and in such case, the deterministic key is expressed as follows:

$$\mathrm{DK} = \sum_{i=1}^{2^m} \sum_{j=1}^{2^m} \exp\left(\mathrm{i}\varphi_k\left(\mathrm{x},\mathrm{y}\right)\right), \quad k = \left(i-1\right) \cdot 2^m + \left(j-1\right), \qquad 8$$

8* MERGEFORMAT ()

and it is completely determined just by choosing the following set of parameters:

$\left\{ \dim, m, \left\{ w_k = v_k \cdot d + u_k \right\}_{k=\{1,\ldots,NS\}} \right\}$.

For the sake of clarity, Fig. 4 shows the real part of some generated deterministic masks for m = 2, 3 and 4 (in Figs. 4(a), 4(b) and 4(c), respectively).

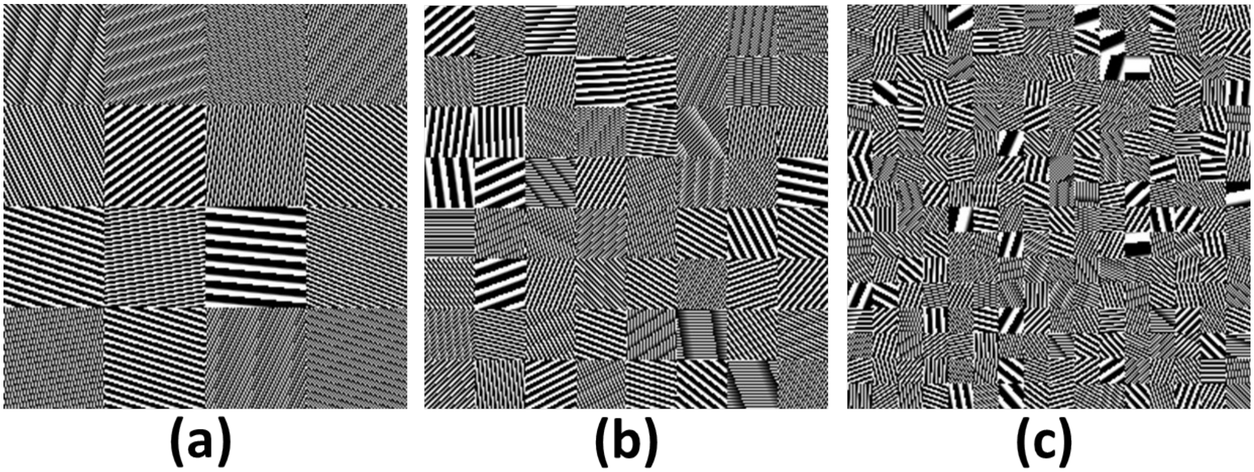

Fig. 4 Generated deterministic keys used for encryption: (a) m=2, (b) m=3, (c) m=4.

As shown in Fig. 2, for the experimental implementation of the proposed technique, a spatial light modulator (SLM) can be used to generate the deterministic keys proposed. In such a case, the largest number of sub-keys to be implemented is limited by the number of pixels of the modulator. Note that for a fixed size of the SLM, the larger the number m set to implement the sub-keys, the lower the number of pixels used to implement such sub-key. By increasing the order m, we can arrive to a minimum sub-key size of 1x1 pixels. In this particular case, the idea of a linear phase is lost and the classical DRPE method is obtained. Thus, the deterministic key based approach can be understood as a generalization of the classical DRPE method.

3 Proof of concept of the method: numerical simulations for the encryption-decryption process

In this section, we study the feasibility, effectiveness, and sensitivity of the proposed method based on simulated results. In this work, the influence of some experimental parameters on the imaging process has not been considered, such as SLM dimensions, bandwidth, etc. The simulation tests were carried out on the Matlab2014a platform. A gray-scale image (Lena image) and a binary image (with the text “Optical Encryption”), with the size of 256×256 pixels, are used as the original images to be encrypted, as shown in Fig.5 (a) and 5(b), respectively.

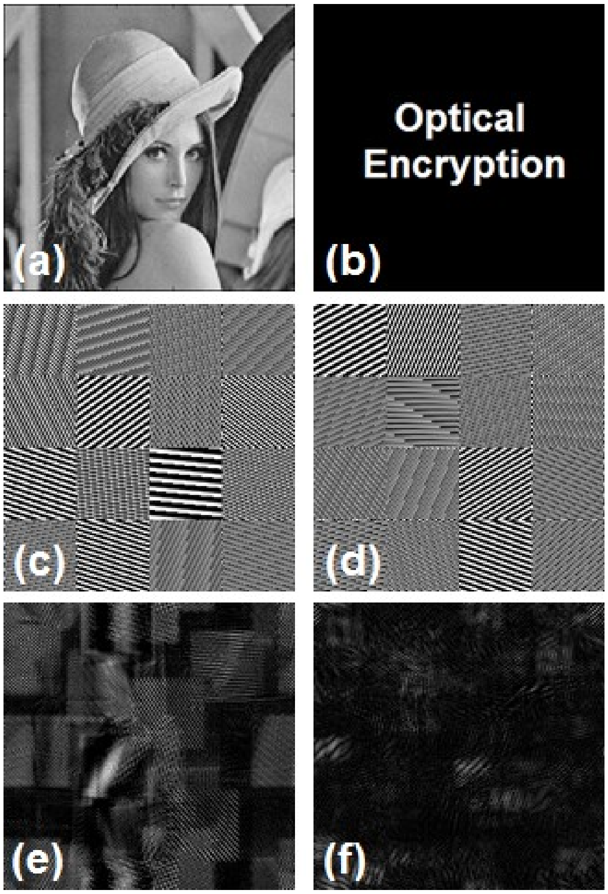

Fig. 5 Simulated results: (a) Input Lena image; (b) Input binary text image; (c) real part of the first deterministic key DK1 used in the encryption process (object plane, see Fig. 1); (d) real part of the second deterministic key DK2 used in the encryption process (Fourier Transform plane); (e) encrypted image for the Lena image; and (f) encrypted image for the text image.

In addition, Figs. 5(c) and 5(d) display, the real parts of the two deterministic keys $DK1$ and $DK2$ used in the encryption process, which have been generated according to Sec. 2 and by setting *m*=2. By contrast, Figs. 5(e) and 5(f) respectively show the images encrypted by using our method, which correspond to the original images in Figs. 5(a) and 5(b), respectively. As we can see, any information of the original images is observed at the encrypted images in Figs. 5(e) and 5(f).

In addition, to prove the validity of the proposed approach, we performed the image decryption of the encrypted images shown in Figs. 5(e) and 5(f) by using the correct keys (i.e., by using the masks obtained by conducting the complex conjugated of the deterministic keys DK1 and DK2 shown in Figs. 5(c) and (d), respectively). The corresponding results are as shown in Figs. 6(a) and 6(b), for the Lena image and the binary text image, respectively.

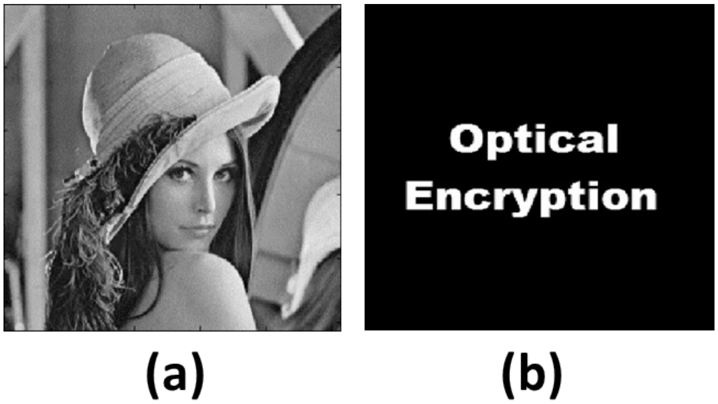

Fig. 6 Decrypted images: (a) decrypted image of Lena, and (b) decrypted text image.

To evaluate the quality of the recovered images, the mean-square-error (MSE), and the peak signal-to-noise ratio (PSNR) between the input images (Figs. 5(a) and 5(b)) and the recovered images (Figs. 6(a) and 6(b)) were calculated. The MSE and the PSNR are respectively defined as:

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

99* MERGEFORMAT ()

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

1010* MERGEFORMAT ()

where $f(x,y)$ and $f'(x,y)$ denote the original image and the decrypted image, respectively. In turn, $N \times M$ is the number of pixels of the original image. It may be noted that a smaller value of the MSE means greater similarity between the original and recovered image. In turn, the greater PSNR value, the better the quality of the retrieved image. The MSE between the retrieved image (Fig. 6(a)) and the original gray-scale image (Fig. 5(a)) is 7.31×10^{-32} , while the PSNR value obtained for the same images is 359.13 . When conducting the comparison for the binary text image (Fig. 5(b) and 6(b)), the obtained MSE and PSNR values are 2.22×10^{-32} and 364.77 , respectively. In both cases, the obtained MSE and PSNR values indicate that the images can be considered as practically equal to the original ones.

Table 1 summarizes the MSE and PSNR values obtained by comparing our proposed approach and the classical DRPE version. Results are given both for the Lena image (first table row) and for the binary text image (second table row).

Table 1 MSE and PSNR results between original and retrieved images for the DRPE scheme and our proposed method.

Input images	MSE		PSNR (dB)	
	Our method	DRPE	Our method	DRPE
Lena image	$7.31\cdot10^{-32}$	$1.23\cdot10^{-31}$	359.13	357.18
Text image	$2.22\cdot10^{-32}$	$2.33\cdot10^{-32}$	364.77	364.45

Note that the MSE and PSNR values obtained for the decrypted images when using our proposed deterministic key generation are quite similar to those obtained by using the DRPE scheme. Thus, our proposed technique appears a good alternative to the DRPE method in terms of decrypted image quality.

The performance of the proposed scheme is also calculated in terms of the relative error (RE) between the original and the decrypted image. The RE between original and decrypted image is defined as:

$$RE = \frac{\sum_{x=1}^{N}\sum_{y=1}^{M}\left\{\left|\hat{f}(x,y) - f(x,y)\right|^2\right\}}{\sum_{x=1}^{N}\sum_{y=1}^{M}\left\{\left|f(x,y)\right|^2\right\}},$$

1111* MERGEFORMAT ()

The RE value equal to zero indicates that the original image is perfectly retrieved. The calculated values of RE for Fig. 5(a) and 5(b) and their retrieved images Fig. 6(a) and 6(b) are $2{,}75 \times 10^{-31}$ and $4{,}07 \times 10^{-31}$, respectively, which means that the original images are successfully obtained. Note that the obtained RE values are in agreement with data given in Table 1.

4 Deterministic masks based method robustness

In this section, we analyze the robustness of the proposed method by applying it to three different situations that can arise in experimental implementations: (*i*) robustness to spatial shifts of the decrypting deterministic phase masks (Sec. 4.1), (*ii*) robustness to certain loss of encrypted data (Sec. 4.2), and (*iii*) robustness to external attacks (use of unauthorized deterministic keys; Sec. 4.3).

4.1 Robustness to spatial shifts of the decrypting phase mask in the Fourier plane

In this sub-section, we examine the robustness of the proposed method to the shift tolerance in comparison with the well-established DRPE method. Figure 7 shows the decrypted images obtained with the DRPE decryption method when the second phase mask in the Fourier plane (i.e., random phases mask set as encryption key 2, used in the decryption step) is shifted in *x* and *y* directions in steps of one (Fig. 7(a)), two (Fig. 7(b)) and three (Fig. 7(c)) pixels for the Lena image. Same results are respectively provided in Figs. 7(d), 7(e), and 7(f) for the binary text image. As can be seen, a slight shift of the key in the DRPE system results in large errors during decryption process, and the image cannot be recovered in any case.

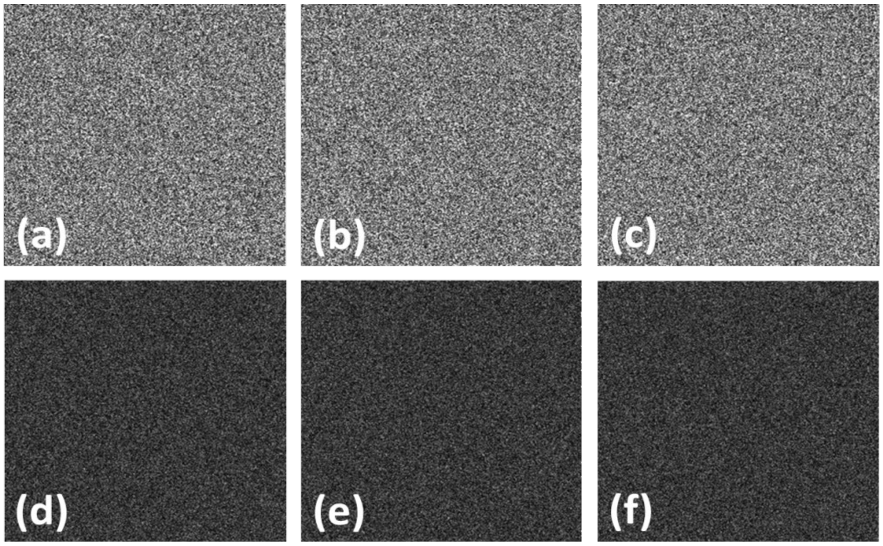

Fig. 7 Decrypted images on DRPE when the decrypting key is shifted at the Fourier plane for: (a) one, (b) two, (c) three pixels for the Lena image; and (d) one, (e) two, and (f) three pixels for the binary text image.

Figure 8 shows the same analysis discussed above but conducted with the new proposed method. In particular, we show the decrypted images obtained when the decrypting deterministic phase mask is shifted in the Fourier plane (i.e., the mask DK2*; see Fig. 1 for decryption step) by one (Fig. 8(a)), two (Fig. 8(b)) and three (Fig. 8(c)) pixels from the matching position, for the Lena image. The same simulations are conducted for the binary text image, and the corresponding results are provided in Figs. 8(d), 8(e) and 8(f), respectively. Even when the decrypted key mask is shifted from the matching position along the x-y axis, the decrypted images (Fig. 8) are still visually recognizable, being much better reconstructed than those obtained with the DRPE method (presented in Fig. 7). In fact, the MSEs obtained between the original and the decrypted images were: 0.0198 (for one pixel shift), 0.0246 (two) and 0.0328 (three) for the Lena image; and 0.0125 (for one pixel shift), 0.0237 (two) and 0.0285 (three) for the binary text image. These small MSE values indicate that, unlike the DRPE method (Fig. 7), our proposed technique allows some original information to be retrieved (Fig.8). The simulated results shown in Fig. 7 prove that the DRPE method is very sensitive to shifts of the key in the decryption process. Under such scenario, very small misalignments of the decrypting phase mask (1 pixel) prevent the DRPE method from image decryption. On the contrary, the proposed deterministic-based method enhances the shift tolerance of the system (see Fig. 8) when compared to the DRPE performance, and thus, the proposed encryption algorithm can be considered as an efficient alternative to the DRPE method.

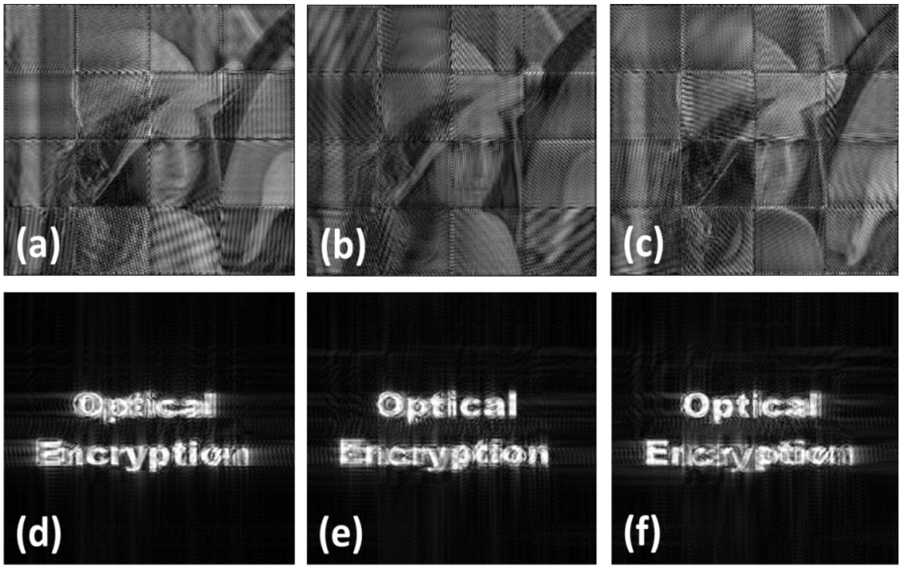

Fig. 8 Decrypted images obtained with our proposed technique when the decrypting key DK2* is shifted for: (a) one, (b) two, (c) three pixels for Lena image; and (d) one, (e) two, and (f) three pixels for the binary text image.

4.2 Robustness to the loss of the encrypted data

We have also studied the robustness to the loss of the encrypted data under network failure during the image transmission. To simulate losses of the encrypted information before decryption, some parts of the encrypted images were blocked by means of square black filters with different sizes (from 1x1 to 128x128 pixels), which were placed in random positions. Then, the MSE coefficient corresponding to the decrypted images was calculated. As an example, Fig. 9 shows the data loss in the encrypted images for the Lena image (9(a)-9(d)) and the binary text image (Figs. 9(e)-9(h)) when using different pixel sizes for the filter (i.e., the black squares): 15x15 pixels (Fig. 9(a) and 9(e)), 45x45 pixels (Fig. 9(b) and 9(f)), 75x75 pixels (Fig. 9(c) and 9(g)) and 128x128 pixels (Fig. 9(d) and 9(h)). In all the cases shown in Fig. 9, we generated the phase masks by setting *m*=3 (so, 64 sub-key masks were implemented). As stated above, in each case the generated filter was centered on arbitrary position of the encrypted image.

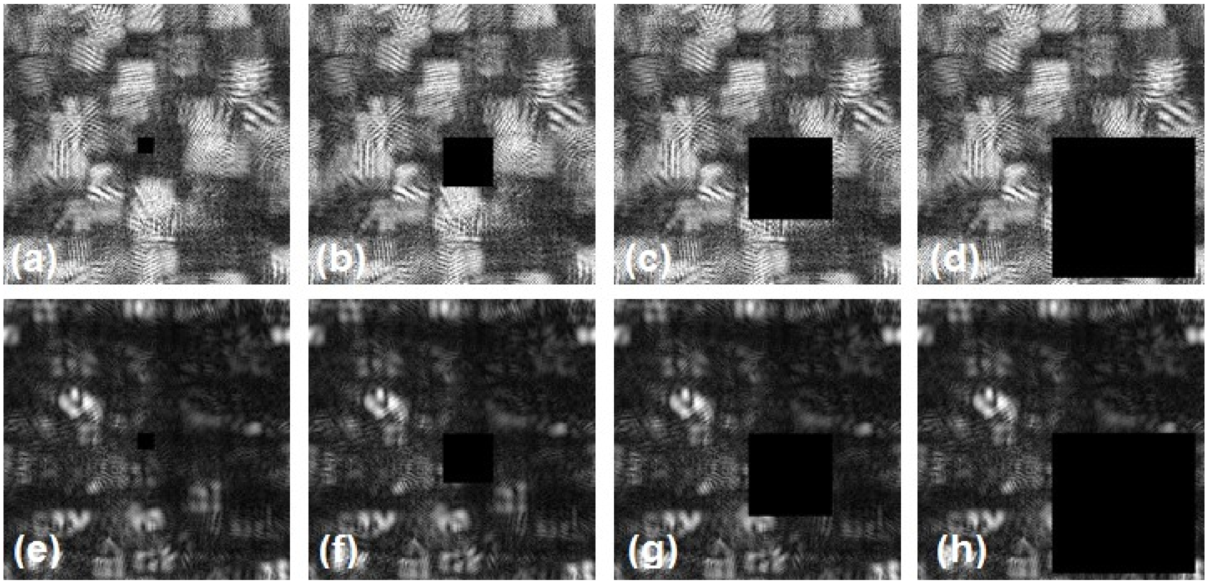

Fig. 9 Encrypted images for the Lena (a)-(d) and binary text (e)-(h) with loss of information of different pixels sizes: (a) and (e) 15x15 pixels, (b) and (f) 45x45 pixels, (c) and (g) 75x75 pixels and (d) and (h) 128x128 pixels.

The corresponding recovered images are respectively presented in Figs. 10(a)-(d) for the Lena image and in Figs. 10(e)-(h) for the binary text image. In addition, the corresponding MSE values between the original images and the decrypted ones are included as insets in the figures. It is evident that, the larger the information loss in the encrypted image, the larger the MSE value obtained. However, a rough version of the original image can be retrieved and recognized in all the cases. The quality of these decrypted images can be improved by image processing operations. From the above-stated simulations, we confirm that the proposed algorithm is robust to data encryption losses.

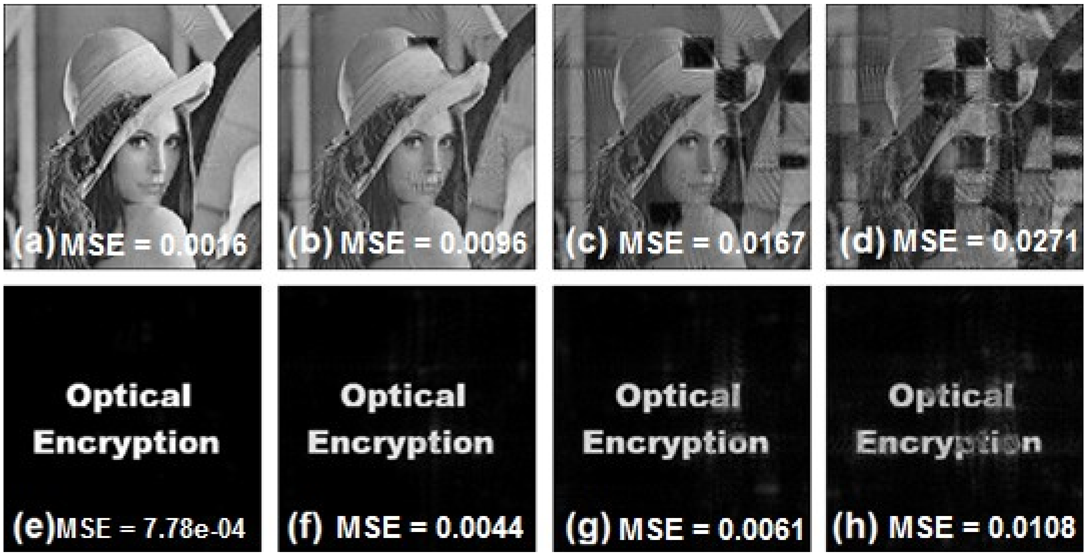

Fig. 10 Decrypted images obtained for the Lena (a)-(d) and binary text (e)-(h) encrypted images. The results provided correspond to an information loss in the encrypted images with a pixel size of: (a) and (e) 15x15 pixels; (b) and (f) 45x45 pixels; (c) and (g) 75x75 pixels; and (d) and (h) 128x128 pixels.

Finally, in addition to the visual analysis presented in Fig. 10, a more quantitative analysis is presented below. We have calculated the MSE for original-decrypted images (for the Lena case) when the decrypted image was obtained with a different amount of loss of information in the encrypted images. The information loss was performed by selecting a random position of the blocker which presented a random size (into a size range between 1x1 to 128x128 pixels). MSE results obtained after performing 1000 runs are shown in Fig. 11. In addition, the above-stated simulations were repeated for different values of the encryption order *m*: *m*=2 (Fig. 11(a)); *m*=3 (Fig. 11(b)) and *m*=4 (Fig. 11(c)). In all the cases, we observe how larger blocker sizes correspond to bigger MSE. In addition, the larger the parameter *m* we set, the lower the MSE fluctuation observed. Note that for the simulated results performed, even in the case of the largest information losses (i.e., information blocker with 128x128 pixels), the MSE values are always smaller than 0.1, which demonstrates robustness to the loss of encrypted data.

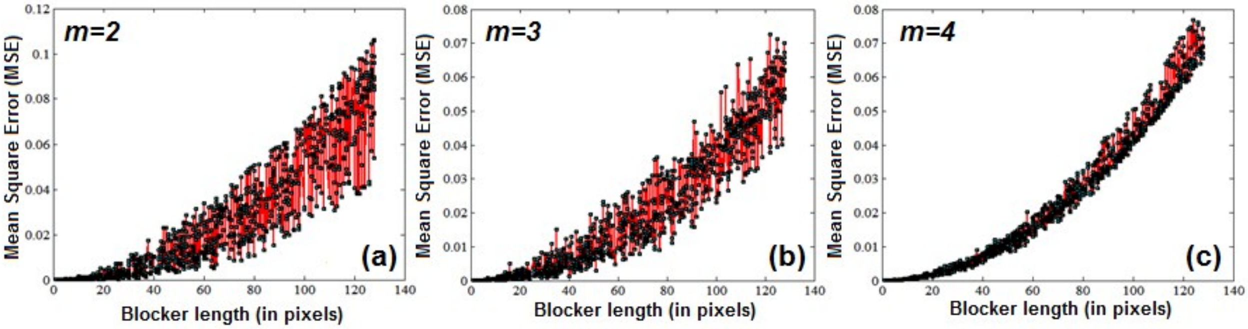

Fig. 11 MSE values obtained between the original-decrypted images (for the Lena case) as a function of the blocker length (in pixels) set at the encrypted image. Results are given for different *m* values.

4.3. Robustness to external attacks: decryption based on unauthorized deterministic keys

Because the calculation of a deterministic key (DK) is analytically performed, instead of sending the mask itself, we can send a set of numerical parameters to reproduce it: {*dim*, *m* and $\{w_{k=}v_k.d+u_k\}_{k=1,\ldots,NS}$ } (see Sec. 2.2). The change of a single bit in the numerical set should produce a huge different encrypted image, this ensuring the security of the system to external attacks. To analyze this fact, the sensitivity of the deterministic method to a slight change in the numerical set of the keys has been tested through a particular example. The original images –Lena image (Fig. 5(a)) and binary text image (Fig. 5(b)) were encrypted by using two secret deterministic keys DK1 and DK2, and as shown in Section 2.2, they were fully determined just by setting the following parameters: $\left\{\dim, m,\{\, w_k = v_k \cdot d + u_k\}_{k=\{1,\ldots,NS\}}\right\}$, where u_k and v_k are randomly generated in the interval $\left[1, d\right]$.

For a particular implementation, we took the following series of values:

DK1: {*dim*=256x256, *m*=2, {4112, 1420, 2652, 1916, 155, 2250, 123, 3286, 2974, 4015, 1722, 867, 143, 992, 2675, 262}}.

DK2: {*dim*=256x256, *m*=2, {842, 1169, 189, 1934, 2172, 2997, 2938, 2633, 215, 2163, 3636, 3525, 139, 2493, 3758, 84}}.

By using these deterministic keys DK1 and DK2, we obtained the corresponding encrypted images, which were illustrated in Figs. 5(e) and 5(f), respectively, and decrypted images illustrated in Figs. 6(a) and 6(b), respectively.

By contrast, Fig. 12 shows the decrypted images, for the Lena image (Fig. 12(a)) and the binary text image (Fig. 12(b)), which were obtained by using a false key DK2 in the decryption process, let us call it as DK2_b:

DK2_b: {*dim*=256x256, *m*=2, {520, 984, 1642, 346, 3161, 2554, 732, 3157, 1139, 514, 2873, 881, 965, 3512, 481, 1827}}.

As shown in Fig. 12, the use in the decryption process of a deterministic key (DK2_b) different from the original one (DK2), does not allow us to retrieve any information of the original image.

In turn, decrypted images shown in Fig. 13 for the Lena image (Fig. 13(a)) and the binary text image (Fig. 13 (b)), were obtained by performing a slight modification of the original deterministic key DK2. In particular, the modified deterministic key was achieved by only changing one of the 16-subkeys of DK2, i.e., the value $w_{(k=10)}$ = 2163 in DK2 was changed to 122. This situation led to the deterministic key DK2_c:

DK2_c:{*dim*=256x256, *m*=2, {842, 1169, 189, 1934, 2172, 2997, 2938, 2633, 215, <u>**122**</u>, 3636, 3525, 139, 2493, 3758, 84}}.

From the previous simulated results, we observed that for the *m*=2 case, a satisfactory decryption process was not possible when using incorrect deterministic keys (Figs. 12 and 13), even when only one of the decryption sub-keys was changed (Fig. 13). Thus, the use of the very exact pair of deterministic keys is mandatory to properly decrypt the original image with our proposed technique. This situation highlights the robustness of the method to external attacks.

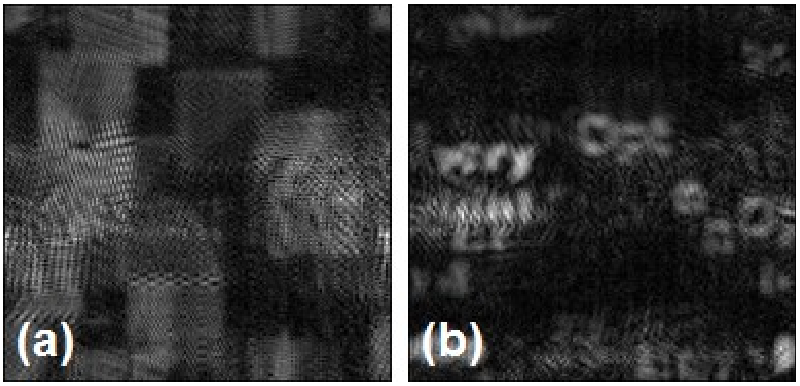

Fig. 12 Decrypted images obtained by using an incorrect deterministic key (DK2_b) in the decryption process: (a) for the Lena image; and (b) for the binary text image.

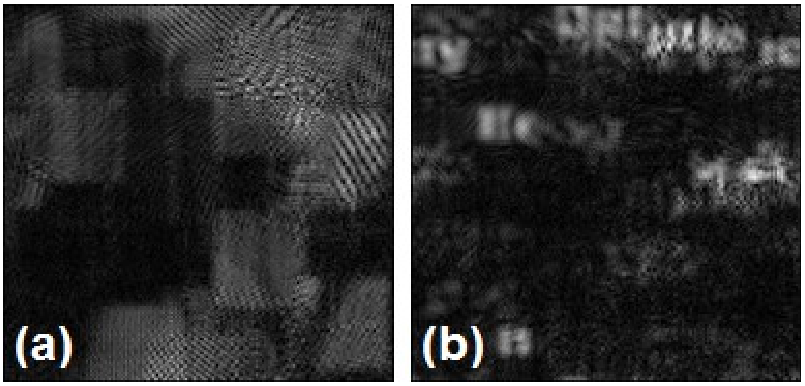

Fig. 13 Decrypted images obtained by using the incorrect deterministic key DK2_c: (a) for the Lena image; and (b) for the binary text image.

4 Conclusion

In the present manuscript we propose an encryption-decryption method to overcome the extremely difficult axis alignment requirements of the double random phase encoding (DRPE) method, which arises from the use of a 4f correlator in the decryption stage. Our technique uses a pair of deterministic phase masks defined by an order of encryption parameter *m* and a linear combination of several sub-keys. The numerical results provided in this work demonstrate that the proposed deterministic mask based encryption-decryption technique has several interesting features in comparison to the DRPE. First, the system provides similar results to the classical DRPE method, in terms of image retrieving for an ideally aligned system. However, our method is much less affected by spatial shifts of the phase mask in the Fourier plane than the DRPE, allowing for less precise alignment requirements during decryption processes. Second, we have demonstrated that our method is able to reconstruct the original image under distortions caused by the occlusion of specific parts of the encrypted images, which may be important in case of a network failure during image transmission. Last but not least, the phase masks generation relays on a simple set of numerical parameters and therefore, the reconstruction of the image does not necessary imply the sending of the totality of the mask, but only of the proper set of parameters. This situation largely reduces the chances of loss of information during the transmission stage. The proposed method can be then presented as a promising alternative to standard methods and may find an excellent application in securing data.

Acknowledgements

We acknowledge the financial support of Spanish MINECO (FIS2015-66328-C3-1-R and fondos FEDER); Catalan Government (SGR 2014-1639);

References

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

2. J. W. Goodman, *Introduction to Fourier Optics*, McGraw-Hill, New York, NY, USA, 2nd edition, (1996).

3. 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).

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

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

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

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

8. T. J. Naughton , B. Javidi, “Compression of encrypted three-dimensional objects using digital holography,” *Opt. Eng*. **43**(10), 2233-2238 (2004).

9. G. Unnikrishnan, J. Joseph, and K. Singh, “ Optical encryption by double-random phase encoding in the fractional Fourier domain ,” *Opt. Lett*. **25**, 887–889 (2000).

10. N. K. Nishchal, J. Joseph, and K. Singh, “ Fully phase encryption using fractional Fourier transform,” *Opt. Eng*. **42**, 1583–1588 (2003).

11. G. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” *Opt. Lett*. **29**, 1584–1586 (2004).

12. 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).

13. J. M. Vilardy, M. S. Millán, and E. Pérez-Cabré, “Nonlinear optical security system based on a joint transform correlator in the Fresnel domain,” *Appl. Opt*. **53**, 1674–1682 (2014).

14. J. A. Rodrigo, T. Alieva, and M. L. Calvo, “Applications of gyrator transform for image processing,” *Opt. Commun*. **278**, 279–284 (2007).

15. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, “Fully phase image encryption using double random-structured phase masks in gyrator domain,” *Appl. Opt*. **53**, 6472–6481 (2014).

16. X. Wang, H. Zhai, Z. Li, and Q. Ge, “Double random-phase encryption based on discrete quaternion fourier-transforms,” *Optik* **122**, 1856–1859 (2011).

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

18. L. Chen and D. Zhao, “Color image encoding in dual fractional Fourier-wavelet domain with random phases,” *Opt. Commun*. **282**, 3433–3438 (2009).

19. N.-R. Zhou, Y. Wang, and L. Gong, “Novel optical image encryption scheme based on fractional Mellin transform,” *Opt. Commun*. **284**, 3234–3242 (2011).

20. L. Chen and D. Zhao, “Optical image encryption with Hartley transforms,” *Opt. Lett*. **31**, 3438-3440 (2006).

21. 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).

22. 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).

23. 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**, 075402 (2009).

24. B. Wang, C. C. Sun, W. C. Su, and A. E. T. Chiou, “Shift-tolerance property of an optical double-random phase-encoding encryption system,” *Appl. Opt*. **39**, 4788–4792 (2000).

25. D. H. Seo and S. J. Kim, “Shift-tolerance property of optical security system using phase-based virtual image,” *Opt. Rev*. **10**, 175–178 (2003).

26. T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” *Opt. Eng*. **39**, 2031–2035 (2000).

27. S. K. Rajput and N. K. Nishchal, “Asymmetric color cryptosystem using polarization selective diffractive optical element and structured phase mask,” *Appl. Opt*. **51**, 5377–5386 (2012).

28. J.F. Barrera, R. Henao, R. Torroba, “Optical encryption method using toroidal zone plates,” *Opt. Commun*. **248**, 35–40 (2005).

29. J.F. Barrera, R. Henao, R. Torroba, “Fault tolerances using toroidal zone plate encryption,” *Opt. Commun*. **256**, 489–494 (2005).

30. M. Tebaldi, W. D. Furlan, R. Torroba and N. Bolognini, “Optical-data storage-readout technique based on fractal encrypting masks,” *Opt. Lett*. **34**, 316–318 (2009).

31. M. R. Abuturab, “Color information security system using Arnold transform and double structured phase encoding in gyrator transform domain,”*Opt. Laser Technol*. **45**, 524-532 (2013).

32. S. Vashisth, H. Singh, A. K. Yadav, and K. Singh, “Image encryption using fractional Mellin transform, structured phase filters, and phase retrieval,” *Optik* **125**, 5309-5315 (2014).

33. H. Singh, A. K. Yadav, S. Vashisth, and K. Singh, “Double phase-image encryption using gyrator transforms, and structured phase mask in the frequency plane,” *Opt. Laser Eng*. **67**, 145–156 (2015).

34. W. D. Furlan, F. Giménez, A. Calatayud, and Juan A. Monsoriu, “Devil’s vortex-lenses,” *Opt. Express* **17**, 21891-21896 (2009).

35. M. Mitry, D. C. Doughty, J. L. Chaloupka, and M. E. Anderson, “Experimental realization of the devil’s vortex Fresnel lens with a programmable spatial light modulator,” *Appl. Opt*. **51**, 4103-4108 (2012).

36. A. Calatayud, J. A. Rodrigo, L. Remon, W. D. Furlan, G. Cristobal, and J. A. Monsoriu, “Experimental generation and characterization of Devil’s vortex-lenses,” *Applied Physics B*. **106**, 915–919 (2012).

37. A. Calabuig, S. Sánchez-Ruiz, L. Martínez-León, E. Tajahuerce, M. Fernández-Alonso, W. D. Furlan, J. A. Monsoriu, and A. Pons-Martí, “Generation of programmable 3D optical vortex structures through devil’s vortex-lens arrays,” *Appl. Opt*. **52**, 5822-5829 (2013).

38. S. Vashisth, H. Singh, A. K. Yadav, and K. Singh, “Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform,” *Int’l. J. Opt*. **2014**, Article ID 728056, 9 pages (2014).

39. E. Ahouzi, C. Iemmi, S. Ledesma, V. Lashin, K. C. Macukov, J. Campos, M. J. Yzuel, “Pattern recognition with a phase-shifting interferometric correlator. Discrimination-capability enhancement,” *Appl. Phys. B* **64**, 331-338 (1997).

Caption List

Fig. 1 Optical setup for: (a) encryption process; and (b) decryption process.

Fig. 2 (M) mirror, (BS) beam Splitter, (L) lenses, (PH) pinhole, (SLM) Spatial light modulator, (CCD) CCD camera, (PZT) piezo-electric transductor. ARM1 phase-shifting interferometric correlator for image encryption. A 4f correlator (L1-L3) is introduced in the arm of a Mach-Zehnder interferometer (BS1, BS2, PZT, BS3). In this way we obtain the interferences of the encrypted image with a reference wave on CCD1 camera where the interferences are digitalized. ARM2 the encrypted image is displayed in the SLM3 and its Fourier transform is obtained at the SLM4 plane. Finally the decrypted image is formed at the CCD2 camera.

Fig. 3 Generation of deterministic keys.

Fig. 4 Generated deterministic keys used for encryption: (a) *m*=2, (b) *m*=3, (c) *m*=4.

Fig. 5 Simulated results: (a) Input Lena image; (b) Input binary text image; (c) real part of the first deterministic key DK1 used in the encryption process (object plane, see Fig. 1); (d) real part of the second deterministic key DK2 used in the encryption process (Fourier Transform plane); (e) encrypted image for the Lena image; and (f) encrypted image for the text image.

Fig. 6 Decrypted images: (a) decrypted image of Lena; and (b) decrypted text image.

Fig. 7 Decrypted images on DRPE when the decrypting key is shifted at the Fourier plane for: (a) one, (b) two, (c) three pixels for the Lena image; and (d) one, (e) two, and (f) three pixels for the binary text image.

Fig. 8 Decrypted images obtained with our proposed technique when the decrypting key DK2* is shifted for: (a) one, (b) two, (c) three pixels for Lena image and (d) one, (e) two, and (f) three pixels for the binary image.

Fig. 9 Encrypted images for the Lena (a)-(d) and binary text (e)-(h) with loss of information of different pixels sizes: (a) and (e) 15x15 pixels, (b) and (f) 45x45 pixels, (c) and (g) 75x75 pixels and (d) and (h) 128x128 pixels.

Fig. 10 Decrypted images obtained for the Lena (a)-(d) and binary text (e)-(h) encrypted images. The results provided correspond to an information loss in the encrypted images with a pixel size of: (a) and (e) 15x15 pixels; (b) and (f) 45x45 pixels; (c) and (g) 75x75 pixels; and (d) and (h) 128x128 pixels.

Fig. 11 MSE values obtained between the original-decrypted images (for the Lena case) as a function of the blocker length (in pixels) set at the encrypted image. Results are given for different m values.

Fig. 12 Decrypted images obtained by using incorrect deterministic key (DK2_b) in the decryption process: (a) for the Lena image; and (b) for the binary text image.

Fig. 13 Decrypted images obtained by using the incorrect deterministic key DK2_c: (a) for the Lena image; and (b) for the binary text image.

Caption List

Table 1 MSE and PSNR results between original and recovered images for DRPE and the proposed method.

Wiam Zamrani received the B.S. degree in Electronics Electrotechnics and Automatic from Abdelmalek Assaadi University, Tanger, in 2010 and the M.S. degree in Laser Instrumentation and Optoelectronic Components from Hassan 1st University 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.

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).

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.