*Optica Applicata, Vol. XLIX, No. 4, 2019*
DOI: 10.37190/oa190403

# Hybrid image encryption based on digital pre-encryption and optical single random phase encoding

Tewfik BEKKOUCHE[1*], Nacira DIFFELLAH[2], Lahcene ZIET[3]

[1]ETA Laboratory, Department of Electronics, Faculty of Technology, University Bordj Bouarreridj, Bordj Bouarreridj 34000, Algeria

[2]ETA Laboratory, Department of Electronics, Faculty of Technology, University Bordj Bouarreridj, Bordj Bouarreridj 34000, Algeria

[3]LEPCI Laboratory, Department of Electronics, Faculty of Technology, University of Setif 1, Setif 19000, Algeria

[*]Corresponding author: bekkou66@hotmail.com

In this paper, the optical image encryption scheme based on the double random phase encoding system is modified by introducing a nonlinear digital image pre-encryption coupled with a real to complex conversion. It consists in performing the bit-wise XOR operation recursively between successive pixels of an input image together with chaotic scrambling in the spatial domain. The resulting real-valued pre-encrypted image is halved into two equal parts, one being considered as the real part and the other one as an imaginary part. The complex image thus constructed by concatenating the two previous parts, passes into the second stage of the double random phase encoding where it will be multiplied by a random phase mask and then transformed into a frequency domain by the two-dimensional Fourier transform or any of its derivatives to obtain the encrypted image. The advantage of halving is to save the same information and reduce the size of encrypted image to store or transmit a single complex image instead of double as in all existing based double random phase encoding methods. Results of computer simulations prove the effectiveness of the proposed method toward different attacks and confirm its security when compared to existing works, especially in terms of key sensitivity and histogram analysis.

Keywords: nonlinear pre-encryption, halving, double random phase encryption.

## 1. Introduction

With the increasing flow of internet communications, the interchanged information that is in the form of textual data, speech, or in the form of images or other multimedia can be easily corrupted, and their protection becomes an absolute necessity. Images are widely used in our life and to be protected, several encryption techniques have emerged either in the spatial or in frequency domains. Among the techniques used in the frequency domain, we come back to the well-known double random phase encoding (DRPE) which finds its application much more in the optical field. Since its first appearance by Refrigier and Javidi in 1995 [1], based on the bidirectional Fourier transform (FT), the DRPE has expanded to several modifications. Parametric transforms [2–16] have been introduced instead of bidirectional FT and their independent parameters are beneficially exploited as an additional secret key, amongst them, the reciprocal-orthogonal parametric (ROP) transform [2–4], the fractional Fourier transform (FRFT) [5–8], the multiple discrete fractional Fourier transform (MDFRFT) [9–12], gyrator transform [13], Fresnel transform [14], discrete parametric Fourier transform [15] and angular transform [16].

Even more, opto-digital hybrid DRPE versions have emerged; these versions use chaotic maps by introducing a scrambling therein the DRPE system [10, 17]. Although the improvements observed in terms of the widening in the encryption key and the increase of the sensitivity of this key, these DRPE versions remain vulnerable toward some attacks [18–20] because of the linearity observed in all these DRPE's versions. To remedy this problem of linearity, Bouguezel *et al.* have proposed recently two works [11, 12] which consist in injecting a nonlinear pre-encryption before any DRPE to give other opto-digital hybrid DRPE versions. It has been shown in these works that this nonlinear pre-encryption associated with the different-optical DRPE versions leads to a new opto-digital DRPE that outperforms other existing versions of DRPE. Although the above improvements mentioned seem efficient and attractive, the DRPE technique and its different versions suffer from the fact that the encrypted image is complex, which requires the storage and the transmission of two images (real and imaginary parts). To overcome this problem, a new hybrid opto-digital image encryption is proposed.

The basic idea of the proposed encryption method consists in substituting the first block of the DRPE (composed of the first mask applied in the spatial domain and the first Fourier transform or its derivatives) by a pre-encryption applied to the original image in the spatial domain and which is based on the XOR operator coupled with a recursive scrambling performed by chaotic sequences (logistic map). The pre-encrypted image is converted from a real-valued image into a complex image using a real to complex (R2C) converter, then the resulting complex image is applied to a stage called here single random phase encoding (SRPE) [21]. This stage consists of the second mask of the DRPE and its second Fourier transform or its derivatives.

The remaining part of the present paper is as follows: in Section 2, we detailed both the proposed encryption and decryption schemes; simulation results and security analysis are discussed in Section 3 and some concluding remarks are given in Section 4.

## 2. Proposed encryption/decryption schemes

### 2.1. Encryption scheme

According to Fig. 1, we can subdivide the proposed encryption scheme into three parts: digital pre-encryption, real to complex conversion and single random phase encoding

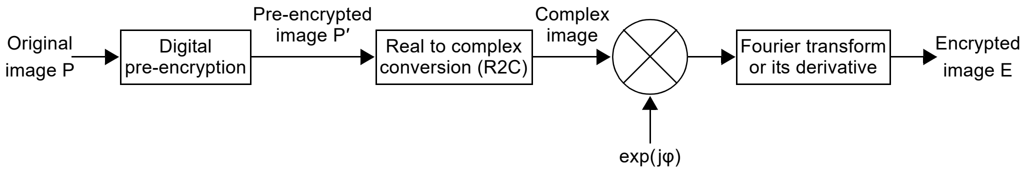


Fig. 1. Proposed encryption scheme.

stage. For its simplicity and high sensitivity to initial conditions, the logistic map is chosen and used as a chaotic system in this work and it is expressed as

$$X_{n+1} = \mu X_n(1 - X_n) \tag{1}$$

where $\mu$ is a control parameter and $\mu \in [3.5699456, 4]$ [22], $X_n$ is a real number in the range [0, 1], and $X_0$ is an initial condition.

#### 2.1.1. Digital pre-encryption

The digital pre-encryption process is detailed as follows.

Step 1: Let $P$ be the original image of size $m \times n$. It is resized to a vector $\mathbf{v}$ of length $(1, m \times n)$.

Step 2: The vector $\mathbf{v}$ is scrambled (change of position of the pixels) according to an order imposed by a chaotic sequence (logistic map) of parameters $\{x_1, \mu_1\}$, with $x_1$ being the initial condition and $\mu_1 \in (0, 4]$ is the parameter of control, to obtain another vector $\mathbf{v}'$ of length $(1, m \times n)$.

Step 3: Generate chaotically another vector using another chaotic map (logistic map) of parameters $\{x_2, \mu_2\}$. In order to be adapted to the gray level, this vector is multiplied by 255 and then rounded to give another vector called $\mathbf{v}''$ of length $(1, m \times n)$.

Step 4: Diffusion phase (change of the pixel values) is ensured by applying the XOR operator recursively between the vector $\mathbf{v}'$ and the vector $\mathbf{v}''$ to give a resulting vector $\mathbf{vv}$ according to the following formula:

$$\begin{cases} \mathbf{vv}(1) = \mathbf{v}'(1) \oplus \mathbf{v}''(1) \oplus s_0 & \text{for} \quad i = 1 \\ \mathbf{vv}(i) = \mathbf{v}'(i) \oplus \mathbf{v}''(i) \oplus \mathbf{vv}(i-1) & \text{for} \quad i = 2 \ \text{ to } \ m \times n \end{cases} \tag{2}$$

where $s_0$ is an integer chosen randomly from the gray level and $\oplus$ designed the bit XOR operator.

Step 5: The obtained vector $\mathbf{vv}$ of length $(1, m \times n)$ is resized to an image which is the pre-encrypted image $p'$.

#### 2.1.2. Real to complex (R2C) conversion

As illustrated in Fig. 2, the pre-encrypted image $p'$ of size $(m, n)$ which is a real valued, is divided into two equal parts $p'_1$ and $p'_2$, and converted by R2C to construct a complex image given by $c = p'_1 + jp'_2$ of size $(m, n/2)$.

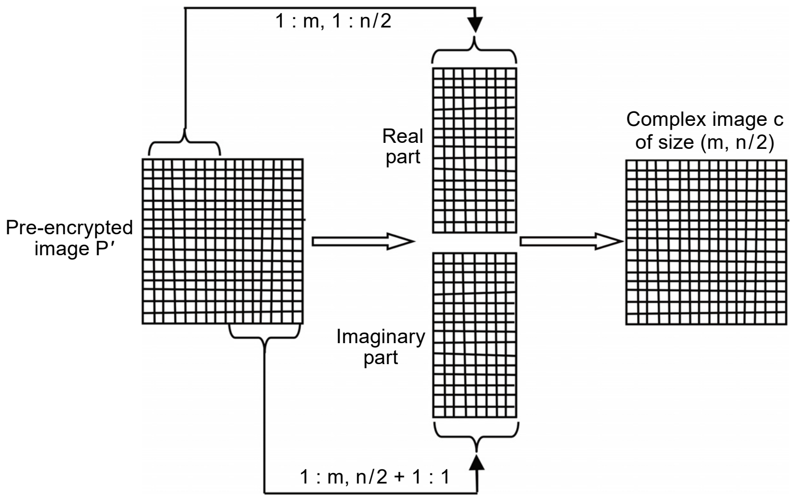


Fig. 2. Illustration of real to complex conversion (R2C).

#### 2.1.3. Single random phase encoding stage

The complex constructed image passed to a stage named here the single random phase encoding. It consists in multiplying this image element-by-element by a random phase mask $\exp(j\varphi)$, then transforming the obtained result using the discrete fractional Fourier transform (DFRFT) to obtain the encrypted image $E$ expressed by

$$E = F^a(c \otimes \exp(j\varphi))F^b \tag{3}$$

where $F^a$ and $F^b$ are DFRFT matrices with fractional orders $a$ and $b$, and $\otimes$ designed an element-by-element multiplication.

### 2.2. Decryption scheme

As shown in Fig. 3, the encrypted image $E$ is transformed to the spatial domain using the inverse discrete fractional Fourier transform (IDFRFT), then multiplied element -by-element by the conjugate random phase mask $\exp(-j\varphi)$ to obtain a complex valued matrix $E'$ expressed by

$$E' = (F^{-a} \cdot E \cdot F^{-b}) \otimes \exp(-j\varphi) \tag{4}$$

where $F^{-a}$ and $F^{-b}$ are IDFRFT matrices with fractional orders $a$ and $b$, $\otimes$ denotes an element-by-element multiplication.

The obtained complex valued matrix $E'$ is converted by the C2R converter to a real valued matrix $E''$ which is exactly the pre-decrypted image.

The digital pre-decryption process is detailed as follows.

Step 1: Generate chaotically the same vector $\mathbf{v}''$ obtained in the previous step 3 of digital pre-encryption using logistic map of parameters $\{x_2, \mu_2\}$.

Step 2: The pre-decrypted image $E''$ is resized to a vector $\mathbf{k}$ of length $(1, m \times n)$.

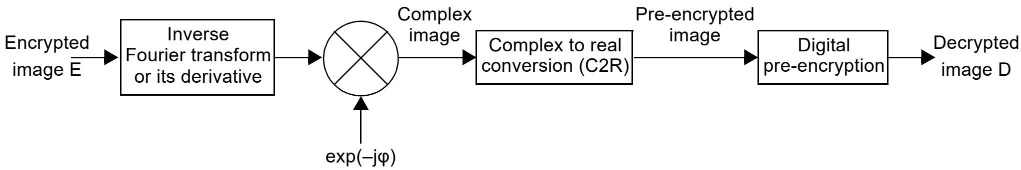


Fig. 3. Proposed decryption scheme.

Step 3: Performing the bit-wise XOR operation recursively between $\mathbf{v}''$ and $\mathbf{k}$ vector's elements according to the following expression:

$$\begin{cases} \mathbf{aa}(1) = \mathbf{k}(1) \oplus \mathbf{v}''(1) \oplus s_0 & \text{for} \quad i = 1 \\ \mathbf{aa}(i) = \mathbf{k}(i) \oplus \mathbf{v}''(i) \oplus \mathbf{aa}(i-1) & \text{for} \quad i = 2 \ \text{ to } \ m \times n \end{cases} \tag{5}$$

where $s_0$ is the memorized integer generated previously in step 4 of digital pre-encryption process and $\oplus$ designed the bit XOR operator.

Step 4: Generate chaotically the same vector $\mathbf{v}'$ obtained in the previous step 2 of digital pre-encryption process using logistic map of parameters $\{x_1, \mu_1\}$, then unsort the obtained vector **aa** according to an order imposed by the chaotic sequence of $\mathbf{v}'$.

Step 5: The obtained unsorted vector is reshaped to give the decrypted image $D$.

We notice that the decryption process takes the steps of encryption process in an inverse manner to obtain decrypted image $D$ as shown in Fig. 3.

An approximate opto-digital implementation is suggested as illustrated in Fig. 4, in which a computer unit is used to perform digitally the nonlinear pre-encryption, the spatial light modulator (SLM) is used to display the complex valued image both in encryption and decryption processes, and a holographic technique conjointly with the reference beam allow the complex valued image to be recorded digitally in a CCD camera.

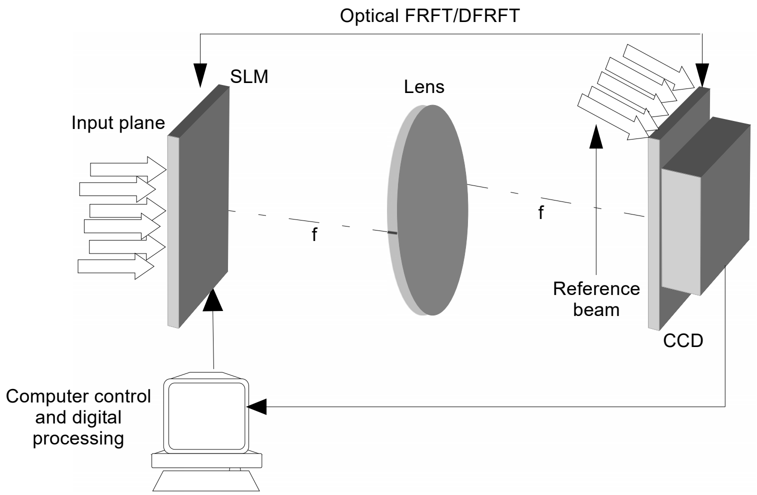


Fig. 4. An opto-digital setup for the proposed FRFT-SRPE/DFRFT-SRPE encryption/decryption.

## 3. Simulation results and security analysis

Results of simulation are performed under the environment MATLAB version 7.10.0.499 (R2010a), the used test images are those of (*Lena*, *Barbara* and *Baboon*) of size 256 × 256. The two chaotic sequences having the following parameters: ($\mu_1 = 3.97$; $x_1 = 0.125$), ($\mu_2 = 3.98$; $x_2 = 0.225$), and the fractional orders of the discrete fractional Fourier transform (DFRFT) ($a$, $b$) are randomly selected from the interval [0, 1] and the phases of the mask $\exp(j\varphi)$ are randomly and uniformly distributed in the interval $[0, 2\pi]$. To evaluate the proposed method, we have used different metrics: the peak signal-to-noise ratio (PSNR), the mean square error (MSE) and the standard correlation coefficient which are widely defined in previous works.

### 3.1. Histogram analysis

As shown in Fig. 5, the original images of *Lena*, *Barbara* and *Baboon* have different histograms, and their encrypted images are complex valued and all have identical amplitude histograms Fig. 6, which proves the effectiveness of the proposed method because a possible attacker cannot extract any significant information from those histograms to discover the original image.

### 3.2. Loss data attack

To test the resistance and the robustness of the method proposed in front of error transmission, Fig. 7 illustrates the simulation results that are performed on the *Lena* image assuming that part of the encrypted image was lost during transmission. We consider

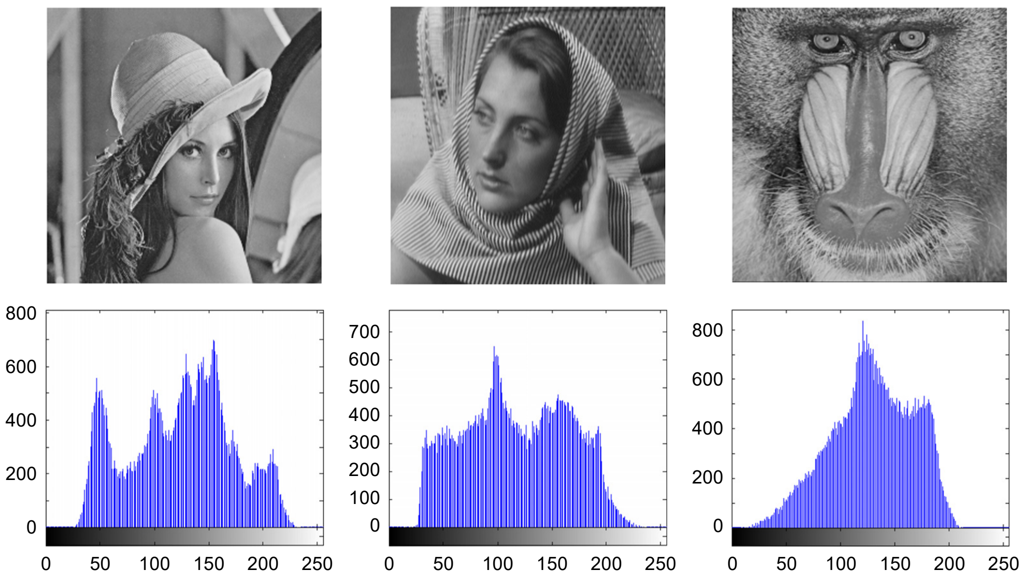


Fig. 5. Original test images of *Lena*, *Barbara*, *Baboon* and their histograms.

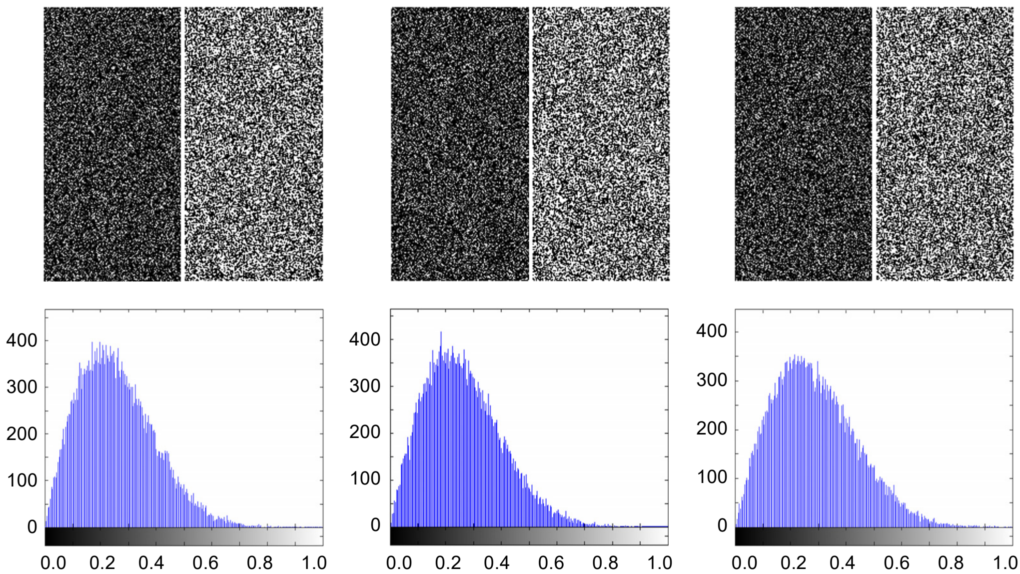


Fig. 6. Real and imaginary encrypted images of *Lena*, *Barbara*, *Baboon* and their amplitude histograms.

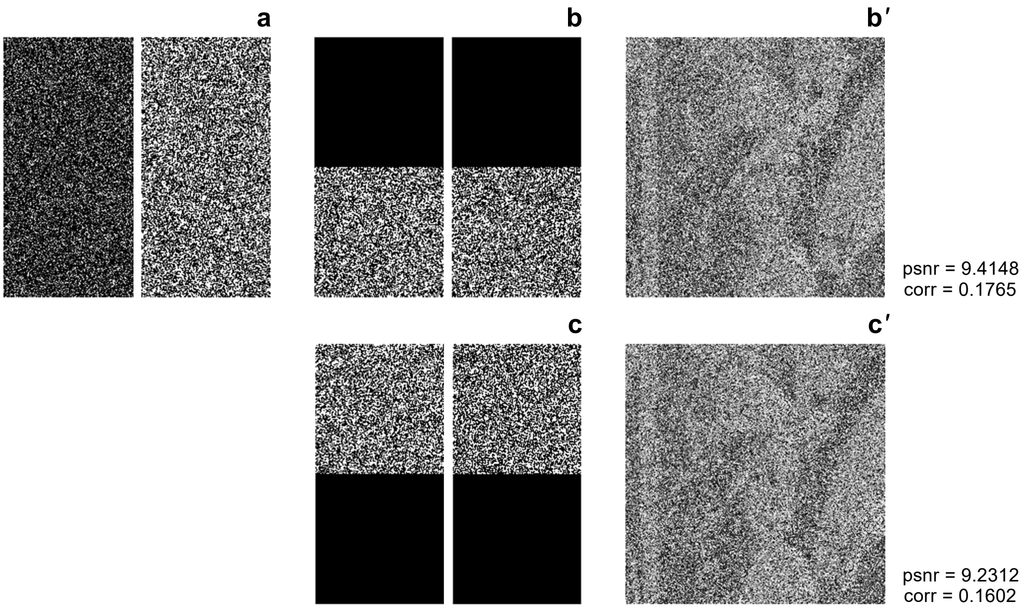


Fig. 7. Results of the loss data test. Encrypted image of *Lena* (**a**), encrypted image of *Lena* with 50% loss data (**b**, **c**), and corresponding decrypted *Lena* image (**b′**, **c′**).

the case with the loss data percentage of 50%. It is very clear that decrypted images are decipherable although they have lost half of the information, which confirms the resistance of the proposed method to data loss.

### 3.3. Noise attack

To test the resistance of the proposed method to adding noise, we assume that the encrypted image is embedded in a Gaussian noise $G$ with zero mean and that the standard deviation equals to unity ($\mu = 0$, $\sigma = 1$) according to the following formula:

$$I_{\text{enc + noise}} = I_{\text{enc}}(1 + kG) \tag{6}$$

where $I_{\text{enc + noise}}$ is the noisy encrypted image, $I_{\text{enc}}$ is the encrypted image of *Lena*, and $k$ indicates the force of the noise. Figure 8 illustrates the simulation results of this test by adding the noise to the encrypted image for different values of $k$, and to see its repercussion on the decrypted image, we notice that the decrypted noisy image starts to lose its visibility from $k = 0.4$. Therefore, we find that despite a percentage of 30% of noise embedded in the encrypted image, the decrypted image remains decipherable, which confirms that the proposed method is highly resistant to noise addition.

### 3.4. Key sensitivity analysis

The encryption key of the proposed method is composed of the parameters of the two logistic maps $(\mu_1, x_1)$, $(\mu_2, x_2)$ and the fractional orders $a$ and $b$ of the discrete fractional Fourier transform DFRFT. We denote by $k\{\mu_1, x_1, \mu_2, x_2, a, b\}$ this encryption key, and the corresponding decryption key is $k'\{\mu'_1, x'_1, \mu'_2, x'_2, a', b'\}$. In the decryption phase, if $k' = k$, so $\{\mu'_1 = \mu_1, x'_1 = x_1, \mu'_2 = \mu_2, x'_2 = x_2, a' = a, b' = b\}$, the decrypted image is exactly the input image (original image). To test the sensitivity of the encryption key toward chaotic parameters, we make an error of $10^{-15}$ each time in a single chaotic

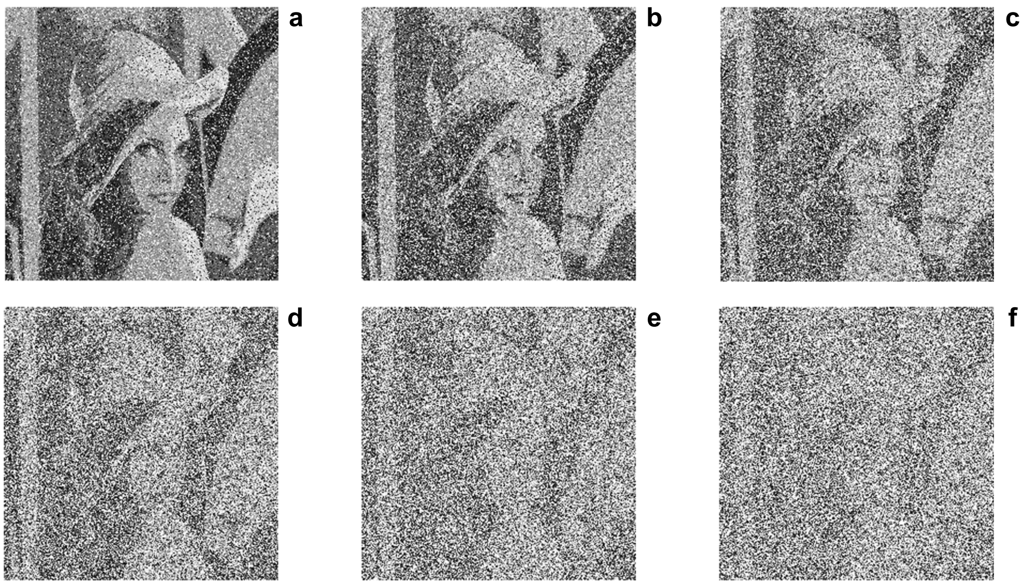


Fig. 8. Decrypted *Lena* image with additive noise in the case of $k = 0.1$ (**a**), $k = 0.2$ (**b**), $k = 0.3$ (**c**), $k = 0.4$ (**d**), $k = 0.5$ (**e**), and $k = 0.6$ (**f**).

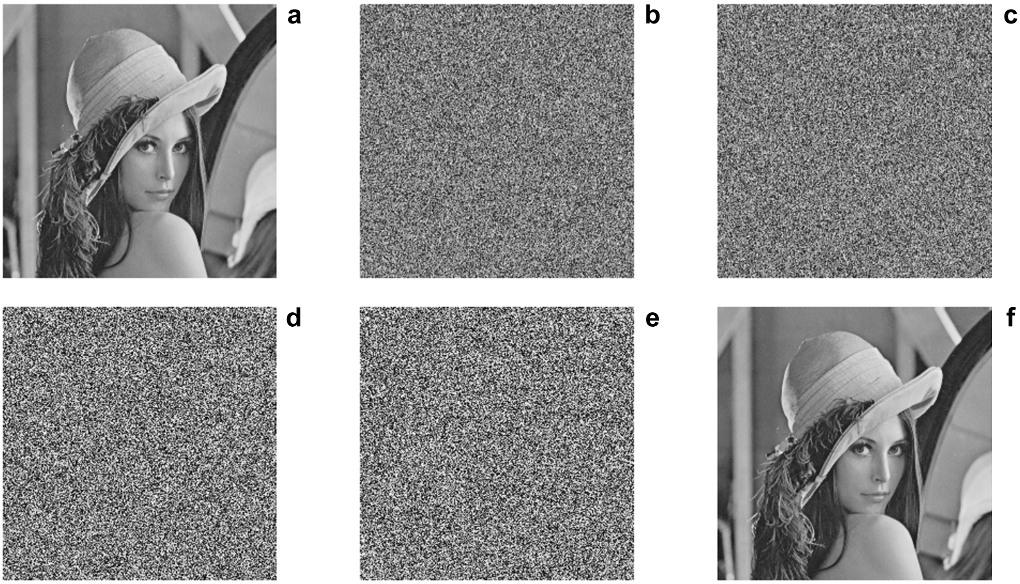


Fig. 9. Decrypted *Lena* image with an error in the decryption key: original image of *Lena* (**a**), $\mu_1' = \mu_1 + 10^{-15}$ (**b**), $x_1' = x_1 + 10^{-15}$ (**c**), $\mu_2' = \mu_2 + 10^{-15}$ (**d**), $x_2' = x_2 + 10^{-15}$ (**e**), and $k' = k$ (**f**).

parameter and we keep the others. The test results are shown in Fig. 9 and confirm that the sensitivity of its parameters is $10^{+1}$ (the error of $10^{-15}$ is the limit of the scrambling before the appearance of the image in clear at $10^{-16}$). The sensitivity of the encryption key to the fractional order parameters of the DFRFT is tested by making a small error $\delta$ ranging from –0.04 to +0.04 in the two parametric orders $a' = a + \delta$ and $b' = b + \delta$ and we calculate the corresponding MSE. Figure10 illustrates the results obtained and con-

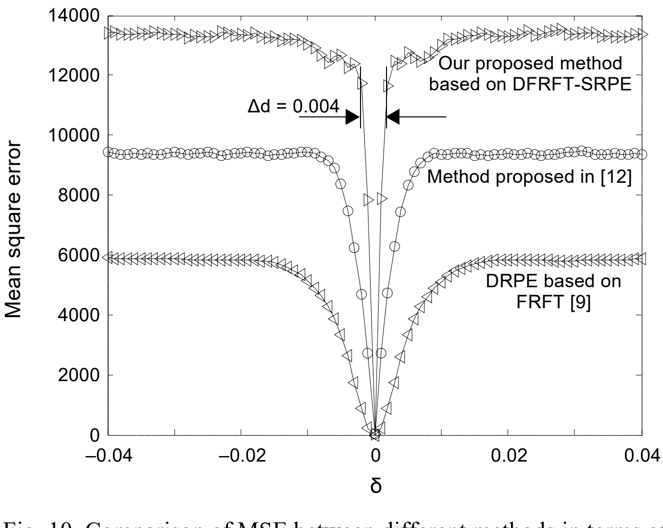


Fig. 10. Comparison of MSE between different methods in terms of the deviation error $\delta$.

firms the superiority of the proposed method when it is compared with the method of the reference [12], and with the DRPE method based on FRFT [9].

### 3.5. Key space analysis

According to the obtained results found in key sensitivity analysis, the accuracy of the chaotic parameters is $10^{-15}$ and the precision of fractional orders is $1/\Delta d = 1/0.004 = 250$, so the key space of the method proposed is $10^{15 \times 4} \times 250 \times 250 \cong 2^{195}$ which is much higher than that required in cryptography $2^{100}$ [23, 24].

## 4. Conclusions

In this paper, we have proposed a new hybrid encryption method (opto-digital) which consists of soft parts. The first part is based on the operator X or coupled with a scrambling performed by logistic maps, and the second part is based on SRPE (single random phase encoding). The results of the simulation show the feasibility of the proposed method and show that the dimensions of encrypted image are reduced to the half. In addition, the results of histograms prove the effectiveness of the proposed method because a possible attacker cannot extract any information to discover the original image. Loss data and addition noise tests prove the strength and robustness of the proposed method against brute force attacks and transmission errors. Comparison results clearly show that the proposed method is more efficient than existing methods in terms of sensitivity and secret key space.

*Acknowledgments* – I (TB) would like to thank the ETA research laboratory of Bordj Bouarreridj University for providing me with all the financial and logistical resources. Without forgeting to mention the full care of the General Directorate for Scientific Research and Technological Development of the Algerian Republic in accomplishing this work.

## References

[1] Refregier P., Javidi B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[2] Bouguezel S., Ahmad M.O., Swamy M.N.S., *Image encryption using the reciprocal-orthogonal parametric transform*, [In] *Proceedings of 2010 IEEE International Symposium on Circuits and Systems*, 2010, pp. 2542–2545, DOI: 10.1109/ISCAS.2010.5537110.

[3] Azoug S., Bouguezel S., *Double image encryption based on the reciprocal-orthogonal parametric transform and chaotic map*, [In] *2013 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA)*, 2013, pp. 156–161, DOI: 10.1109/WoSSPA.2013.6602354.

[4] Bouguezel S., Ahmad M.O., Swamy M.N.S., *A new involutory parametric transform and its application to image encryption*, [In] *2013 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2013, pp. 2605–2608, DOI: 10.1109/ISCAS.2013.6572412.

[5] Liu S., Sheridan J.T., *Optical encryption by combining image scrambling techniques in fractional Fourier domains*, Optics Communications **287**, 2013, pp. 73–80, DOI: 10.1016/j.optcom.2012.09.033.

[6] Sinha A., Singh K., *Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes*, Optical Engineering **44**(5), 2005, article ID 057001, DOI: 10.1117/1.1906240.

[7] HENNELLY B., SHERIDAN J.T., *Optical image encryption by random shifting in fractional Fourier domains*, Optics Letters **28**(4), 2003, pp. 269–271, DOI: 10.1364/OL.28.000269.

[8] SUI L., LU H., WANG Z., SUN Q., *Double-image encryption using discrete fractional random transform and logistic maps*, Optics and Lasers in Engineering **56**, 2014, pp. 1–12, DOI: 10.1016/j.optlaseng.2013.12.001.

[9] PEI S.-C., HSUE W.-L., *The multiple-parameter discrete fractional Fourier transform*, IEEE Signal Processing Letters **13**(6), 2006, pp. 329–332, DOI: 10.1109/LSP.2006.871721.

[10] LANG J., TAO R., WANG Y., *Image encryption based on the multiple-parameter discrete fractional Fourier transform and chaos function*, Optics Communications **283**(10), 2010, pp. 2092–2096, DOI: 10.1016/j.optcom.2010.01.060.

[11] AZOUG S.E., BOUGUEZEL S., *A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform*, Optics Communications **359**, 2016, pp. 85–94, DOI: 10.1016/j.optcom.2015.09.054.

[12] BEKKOUCHE T., BOUGUEZEL S., *A recursive non-linear pre-encryption for opto-digital double random phase encoding*, Optik **158**, 2018, pp. 940–950, DOI: 10.1016/j.ijleo.2017.12.142.

[13] RODRIGO J.A., ALIEVA T., CALVO M.L., *Applications of gyrator transform for image processing*, Optics Communications **278**(2), 2007, pp. 279–284, DOI: 10.1016/j.optcom.2007.06.023.

[14] SITU G., ZHANG J., *Double random-phase encoding in the Fresnel domain*, Optics Letters **29**(14), 2004, pp. 1584–1586, DOI: 10.1364/OL.29.001584.

[15] BEKKOUCHE T., BOUGUEZEL S., *Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform*, Journal of Electronic Imaging **27**(2), 2018, article ID 023033, DOI: 10.1117/1.JEI.27.2.023033.

[16] YU J., LI Y., XIE X., ZHOU N., ZHOU Z., *Image encryption algorithm by using logistic map and discrete fractional angular transform*, Optica Applicata **47**(1), 2017, pp. 141–155, DOI: 10.5277/oa170113.

[17] HUANG H., YANG S., *Colour image encryption based on logistic mapping and double random-phase encoding*, IET Image Processing **11**(4), 2017, pp. 211–216, DOI: 10.1049/iet-ipr.2016.0552.

[18] PENG X., ZHANG P., WEI H., YU B., *Known-plaintext attack on optical encryption based on double random phase keys*, Optics Letters **31**(8), 2006, pp. 1044–1046, DOI: 10.1364/OL.31.001044.

[19] QIN W., PENG X., *Vulnerability to known-plaintext attack of optical encryption schemes based on two fractional Fourier transform order keys and double random phase keys*, Journal of Optics A: Pure and Applied Optics **11**(7), 2009, article ID 075402, DOI: 10.1088/1464-4258/11/7/075402.

[20] ZHANG Y., XIAO D., WEN W., LIU H., *Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding*, Optics Letters **38**(21), 2013, pp. 4506–4509, DOI: 10.1364/OL.38.004506.

[21] TSANG P.W.M., *Single-random-phase holographic encryption of images*, Optics and Lasers in Engineering **89**, 2017, pp. 22–28, DOI: 10.1016/j.optlaseng.2016.01.017.

[22] YANG J., GAO J., SUN B., *An improvement approach of logistic chaotic series encryption*, Automatic Technology Application **23**(4), 2004, pp. 58–61.

[23] JOLFAEI A., WU X.-W., MUTHUKKUMARASAMY V., *On the security of permutation-only image encryption schemes*, IEEE Transactions on Information Forensics and Security **11**(2), 2016, pp. 235–246, DOI: 10.1109/TIFS.2015.2489178.

[24] ZHOU N., JIANG H., GONG L., XIE X., *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018, pp. 72–79, DOI: 10.1016/j.optlaseng.2018.05.014.

*Received November 21, 2018*
*in revised form February 2, 2019*