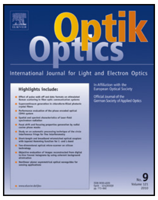
Optik 158 (2018) 940–950

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



Original research article

A recursive non-linear pre-encryption for opto-digital double random phase encoding

Toufik Bekkouche[a], Saad Bouguezel[b,*]

[a] ETA Laboratory, Department of Electronics, Faculty of Technology, Bordj Bouarreridj, 34000, Algeria
[b] LCCNS Laboratory, Department of Electronics, Faculty of Technology, University Ferhat Abbas Setif-1, Setif, 19000, Algeria

ARTICLE INFO

Article history:
Received 29 August 2016
Received in revised form 20 May 2017
Accepted 28 December 2017

Keywords:
Chaotic maps
Double random phase encoding
Fractional Fourier transforms
Image encryption
Recursive non-linear pre-encryption

ABSTRACT

In this paper, we propose a recursive non-linear pre-encryption to be carried out digitally on the input image in the spatial domain before applying any double random phase encoding (DRPE). It consists of firstly scrambling the input image chaotically and then performing the bit-wise XOR operation recursively between two consecutive pixels following a given pattern. The starting two consecutive pixels are formed by the initial pixel in the pattern and a random eight-bit integer. The proposed pre-encryption-based DRPE image encryption system and existing DRPE cryptosystems are compared in terms of the sensitivity of the various encryption keys to decryption attacks.

© 2017 Elsevier GmbH. All rights reserved.

1. Introduction

Modern communication systems and their different applications in military, commercial, medical and social sectors necessitate highly robust and fast information security tools. Encryption is one of the most powerful tools in information security. Specifically, optical image encryption systems are of great importance for their parallel processing and high speed [1]. One of such systems is the well-known optical double random phase encoding (DRPE) introduced by Refregier and Javidi in [2]. It consists of (1) multiplying the input image by a random phase mask (RPM_1) in the spatial domain, (2) transforming the result obtained from (1) using the two-dimensional Fourier transform (FT), (3) multiplying the result obtained from (2) by another random phase mask (RPM_2) in the frequency domain, and finally (4) transforming the result obtained from (3) using the two-dimensional FT to obtain the encrypted image. The two masks RPM_1 and RPM_2 are statistically independent, where the first is used to whiten the image, whereas the second is employed as a secret key for encryption and decryption processes. This technique is called here FT-DRPE.

In order to increase the security of the FT-DRPE, parametric transforms such as the fractional Fourier transform (FrFT) [3], Fresnel transform [4], multiple-parameter discrete fractional Fourier transform (MPDFrFT) [5], Gyrator transform [6], reciprocal-orthogonal parametric transforms [7,8] and involutory parametric transform [9] have been used instead of the FT, where their independent parameters have been exploited as an additional secret key. Specifically, the optical FrFT-based DRPE (FrFT-DRPE) and MPDFrFT-based DRPE (MPDFrFT-DRPE) are of great importance and have extensively been considered in the literature to develop more secured versions by introducing therein scrambling schemes [10–13]. The resulting DRPE versions generally need a computer to perform the scrambling and hence are considered as opto-digital encryption techniques.

[*] Corresponding author.
E-mail address: bouguezel_saad@yahoo.com (S. Bouguezel).

https://doi.org/10.1016/j.ijleo.2017.12.142
0030-4026/© 2017 Elsevier GmbH. All rights reserved.

Although the above optical and opto-digital DRPE versions are efficient, they may not resist to some attacks [14–16]. This is mainly due to the fact that the transforms employed are linear operators and the associated scrambling schemes can also be considered as linear transformations, which make the entire resulting DRPE a linear image encryption technique and hence fragile to some attacks. In order to overcome this linearity problem, a non-linear pre-processing has recently been proposed in [17]. It consists of obtaining a pre-processed image by performing the XOR operation in the spatial domain between each pixel of the input image and its corresponding pixel in the same position of a randomly created image before applying a DRPE. It has been shown in [17] that this non-linear pre-processing coupled with an opto-digital MPDFrFT-DRPE leads to a new opto-digital DRPE that outperforms the other existing DRPE versions, specifically in terms of the secret key sensitivity. Even though the pre-processing proposed in [17] is very efficient and attractive, the non-linearity offered by the XOR operation has been introduced therein for each pixel separately and independently. However, from the encryption point of view, it is highly desirable to construct a more complex non-linear pre-processing. This is achieved in this paper by introducing a new recursive non-linear pre-encryption to be applied prior to any DRPE. It consists of (1) resizing the input image into a vector, (2) chaotically scrambling the resulting vector using the piecewise linear chaotic map (PLCM), (3) performing the bit-wise XOR operation recursively between two adjacent elements of the resulting scrambled vector, where the first element is bit-XORed with a random eight-bit integer, and (4) reshaping the resulting XORed vector into a matrix to obtain the pre-encrypted image. The recursive property of the proposed pre-encryption introduces some dependency between the pixels of the pre-processed image and hence ensures the accumulation and propagation of the error to all pixels in the case of any wrongness in the decryption key. Therefore, any opto-digital cryptosystem obtained by coupling the proposed pre-encryption with an optical DRPE cryptosystem including the FT-DRPE would resist to decryption attacks. As mentioned above, in order to further increase the security of an opto-digital cryptosystem, it is highly desirable to use transforms having optical implementation and increased number of independent parameters such as FrFT and MPDFrFT.

This paper is organized as follows. In Section 2, we introduce a new recursive non-linear pre-encryption and review the PLCM used to scramble images. The proposed opto-digital image encryption and decryption systems are described in Section 3. Section 4 presents performance analysis and comparison.

2. Proposed recursive non-linear pre-encryption

It is well-known in the numerical methods that the main serious drawback of any recursive approach is the accumulation and propagation of the error. In contradiction with these methods, encryption techniques strongly search for any approach having this drawback or property. Therefore, we beneficially exploit this property of a recursive approach in image encryption to achieve the desired dependency between the pixels of the pre-processed image by introducing in this paper a new recursive non-linear pre-processing. It consists of firstly scrambling the input image and then applying the bit XOR operation recursively on each pair of consecutive pixels following a given pattern. The starting or initial pair is formed by the initial pixel in the pattern and a random eight-bit integer. The secret key for the proposed digital pre-processing (pre-encryption) is this random integer that can be chosen arbitrarily from 0 to 255, and the scrambling, which has $(N \times M)!$ possibilities, where $N \times M$ is the size of the input image. For computer simulations, we consider here square input images, i.e. $M = N$.

In order to efficiently accomplish the above required scrambling, we exploit chaos maps, which are known to have attractive cryptographic properties such as high sensitivity to their initial parameters, ergodicity, and pseudo-randomness. Specifically, we consider the piecewise linear chaotic map (PLCM) proposed in [18] and expressed iteratively as [17]

$$z_{k+1} = F(z_k, \lambda) = \begin{cases} \dfrac{z_k}{\lambda}, & 0 \le z_k < \lambda \\ \dfrac{z_k - \lambda}{0.5 - \lambda}, & \lambda \le z_k < 0.5 \\ F(1 - z_k, \lambda), & 0.5 \le z_k < 1 \end{cases} \tag{1}$$

where z_0 is the initial condition parameter and $\lambda \in (0, 0.5)$ is the control parameter. Therefore, one scheme for digitally implementing the proposed pre-encryption can be achieved by the following steps:

1 Resize the input image into a vector **i** of length $1 \times (N \times N)$
2 Generate a chaotic vector **z**, $\{z_k,\ k = 1, 2, 3, \ldots, N \times N\}$, using the PLCM given by Eq. (1) with the parameters $\left\{z_0, \lambda\right\}$
3 Sort the vector **z** into an ascending order to form a vector **y** and then form a permutation map vector **m** such as m_k is the position of the element y_k in the vector **z**, i.e., $\{y_k = z_{m_k},\ k = 1, 2, 3, \ldots, N \times N\}$
4 Scramble the vector **i** using the permutation map vector **m** to form a vector **s** such as s_k is the (m_k)th element of **i**, i.e., $\{s_k = i_{m_k},\ k = 1, 2, 3, \ldots, N \times N\}$
5 Perform the bit-wise XOR operation recursively on the adjacent elements of **s** to form a vector **x** as

$$x_k = \begin{cases} s_k \oplus r, & k = 1 \\ s_k \oplus x_{k-1}, & k = 2, 3, \ldots, N \times N \end{cases} \tag{2}$$

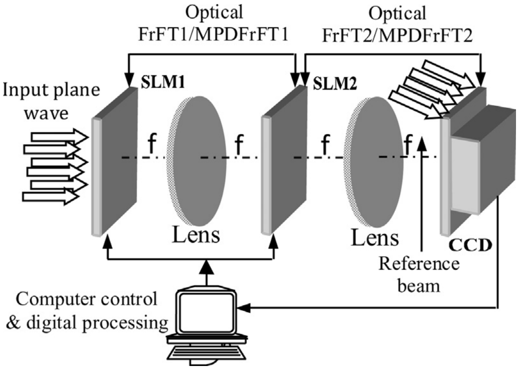


Fig. 1. An opto-digital setup for the proposed FrFT-DRPE/MPDFrFT-DRPE encryption/decryption.

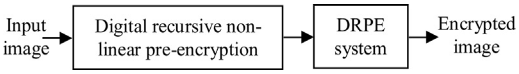


Fig. 2. Proposed encryption system.

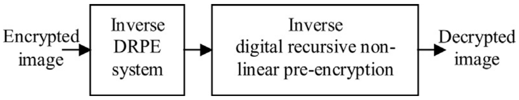


Fig. 3. Proposed decryption system.

where $r = round\left(255 * z_{(N\times N)}\right)$, i.e., the random integer r is chosen to be the last element of the chaotic vector $\mathbf{z}$ converted to an eight-bit integer

6 Finally, the pre-encrypted image is obtained by reshaping the vector $\mathbf{x}$ into an $N \times N$ matrix.

The random integer r is chosen in Step 5 to be a scalar and the pre-encrypted pixel x_k in (2) is obtained by only one XOR operation. This scheme is adopted in the computer simulations below for its simplicity. However, another scheme can be established by choosing r as an eight-bit integer random $1 \times (N \times N)$ vector $\mathbf{r}$ and then performing XOR operation element-by-element between the vectors $\mathbf{s}$ and $\mathbf{r}$ before performing XOR operation recursively on the adjacent elements of the resulting vector. It is worth to mention that for any selected scheme, a recursive application of the XOR operation in the pre-encryption is mandatory to achieve high key sensitivity for the entire image encryption system.

3. Proposed pre-encryption-based DRPE technique

The proposed digital pre-encryption, which combines a scrambling scheme with a recursive non-linear approach and has a secret key constituted of the parameters $\left\{z_0, \lambda\right\}$, can be followed by any of the existing DRPE versions to construct a highly secure image encryption technique. This construction can efficiently exploit any of the existing well-established DRPE systems without any alteration. Without lose of generality, the proposed pre-encryption can be used at the input of the existing optical FrFT- or MPDFrFT-DRPE cryptosystem. Therefore, an opto-digital implementation similar to the one reported in [1] can be suggested for the proposed FrFT-DRPE/MPDFrFT-DRPE encryption/decryption as shown in Fig. 1, in which the computer is used to digitally perform the proposed recursive non-linear pre-encryption and PLCM-based permutations. This implementation has a well-known 4-f optical setup for implementing the FrFT/MPDFrFT. The spatial light modulators SLM1 and SLM2 are used to display the complex-valued signal during the encryption/decryption steps. The CCD camera is employed to digitally record the complex-valued signal using digital holographic techniques and a reference beam.

The resulting proposed pre-encryption-based DRPE significantly differs from the existing scrambling-based DRPE versions not only because of its non-linearity property, but also for its recursive property that ensures the accumulation and propagation of the error to all pixels in the case of any wrongness in the decryption key.

Figs. 2 and 3 show the proposed opto-digital image encryption and decryption systems, respectively. The decryption system takes the steps of the encryption system in an inverse manner. For the encryption system, the input image, which is generally a real-valued eight-bit gray-scale image, is passed through two main blocks. The first block consists of digitally pre-encrypting the input image to obtain a uniformly distributed image with the same format to the input. For instance, we take the 256 × 256 gray-scale Lena image given by Fig. 4 as the input. Its pre-encrypted image is given by Fig. 5, which is clearly a uniformly distributed image. The pre-encrypted image is fed to the second block, which can be any of the existing optical or opto-digital DRPE systems, to produce the encrypted image. If the second block is chosen to be the FrFT-DRPE

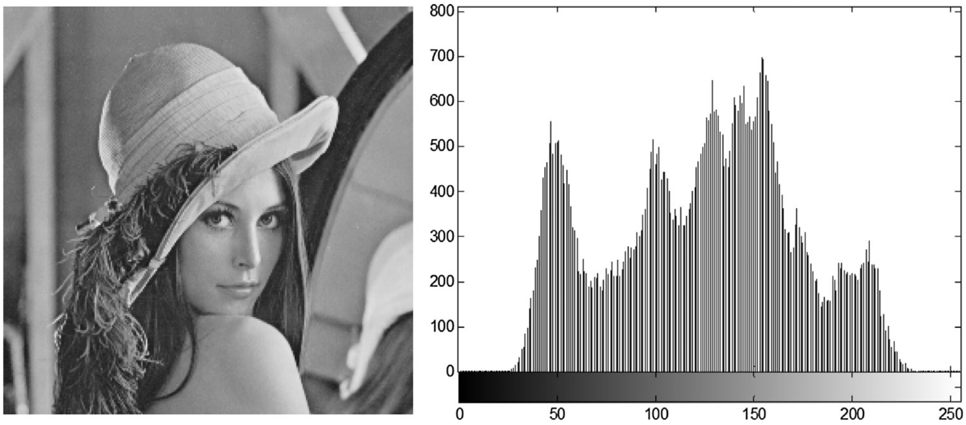


Fig. 4. Input Lena image and its histogram.

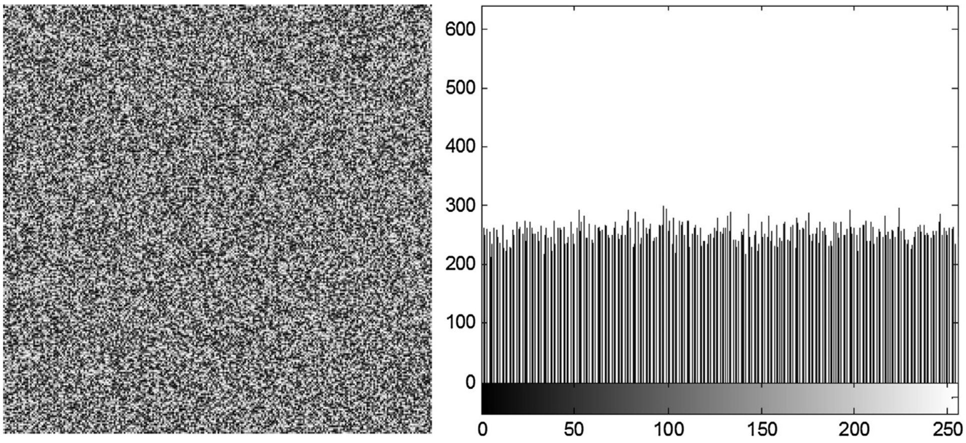


Fig. 5. Pre-encrypted Lena image and its histogram.

system, which has four independent fractional order parameters $\{a, b, c, d\}$ [3], or the MPDFrFT-DRPE system, which has four independent $1 \times N$ vectors $\{-a, -b, -c, -d\}$ of independent fractional order parameters that can be chosen randomly from the interval $[0, 2]$ [5], then the encrypted image is given by Figs. 6 or 7 .

4. Performance analysis and comparison

4.1. Histogram analysis

To show the robustness of the proposed technique against histogram analysis, we encrypt three different images, namely Lena, Barbara and Baboon images shown in Figs. 4, 8 and 10, respectively, and then compare the histograms given in Figs. 7, 9 and 11, respectively, of the resulting encrypted images. It is clear from these figures that even though the histograms of the original images are completely different, the histograms of the amplitude (or the phase) of the corresponding encrypted images are very similar. These results confirm that no information leakage about the original image can be learned by an attacker from histogram analysis of encrypted images, thus, the proposed scheme is robust against histogram analysis.

4.2. Noise attack

Any encrypted image can be corrupted by the noise during transmission or storage. To verify the resistance against the additive noise of a given image encryption technique, we add a white Gaussian noise with zero mean and standard deviation equals to unity to the encrypted Lena image. The decryption of the resulting noisy encrypted Lena image is given in Fig. 12 for different techniques in terms of the PSNR between the original and decrypted images. It is seen from this figure that the three techniques have similar performance in the case of noise attack and the original image can be obtained from the decrypted noisy image after using some known denoising techniques.

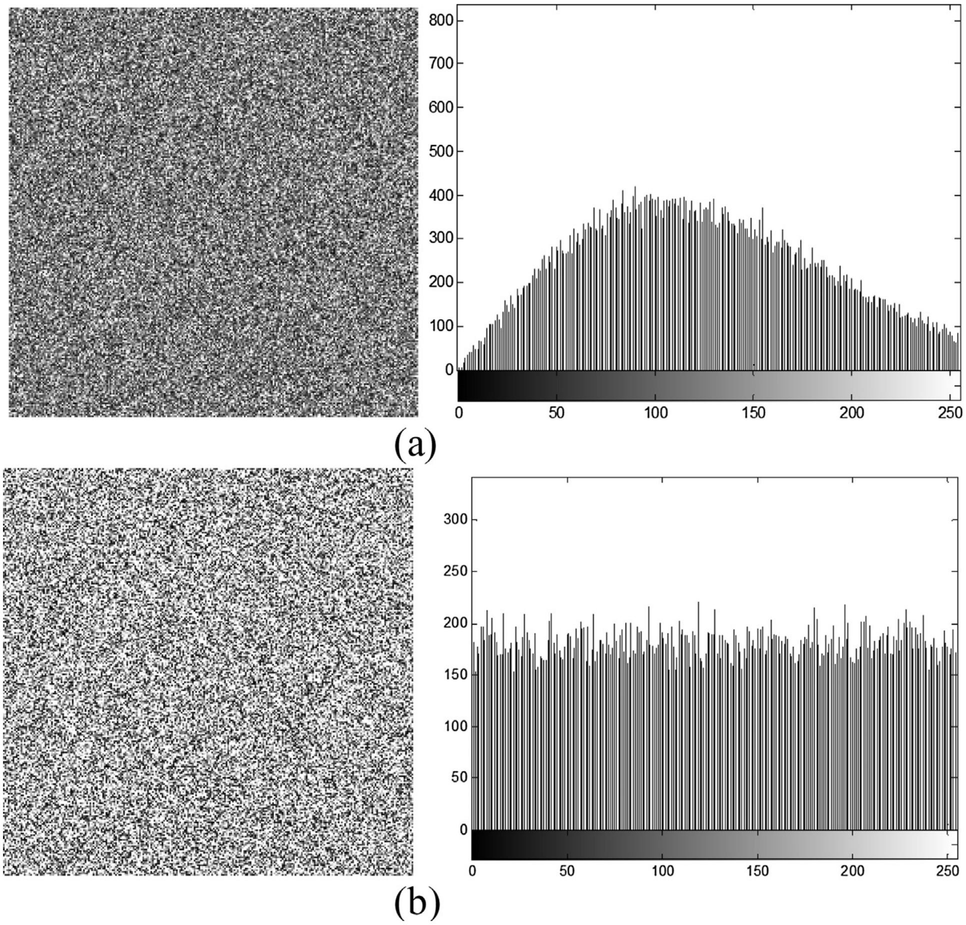


Fig. 6. Encrypted Lena image using the proposed pre-encryption-based FrFT-DRPE system: (a) amplitude and its histogram, (b) phase and its histogram.

4.3. Key sensitivity analysis

It can be seen from Section 2 that the secret key constitutes of $\{z_0, \lambda, a, b, RPM_2, c, d\}$ in the case of the proposed pre-encryption-based FrFT-DRPE system and $\{z_0, \lambda, -a, -b, RPM_2, -c, -d\}$ in the case of the proposed pre-encryption-based MPDFrFT-DRPE system. The corresponding decryption keys are $\{z_0', \lambda', a', b', RPM_2', c', d'\}$ and $\{z_0', \lambda', -a', -b', RPM_2', -c', -d'\}$, respectively. If $\{z_0' = z_0, \lambda' = \lambda, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}$ or $\{z_0' = z_0, \lambda' = \lambda, -a' = -a, -b' = -b, RPM_2' = RPM_2, -c' = -c, -d' = -d\}$, then the corresponding decrypted image is exactly the original image given by Fig. 4. To verify the key sensitivity of the proposed system, the encrypted image is decrypted by introducing small errors in one or some of the parameters that constitute the secret key. If the decryption key is set to be $\{z_0' = z_0 + 10^{-16}, \lambda' = \lambda, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}$, $\{z_0' = z_0, \lambda' = \lambda + 10^{-16}, a' = a, b' = b, RPM_2' = RPM_2, c' = c, d' = d\}$, $\{z_0' = z_0 + 10^{-16}, \lambda' = \lambda, -a' = -a, -b' = -b, RPM_2' = RPM_2, -c' = -c, -d' = -d\}$ or $\{z_0' = z_0, \lambda' = \lambda + 10^{-16}, -a' = -a, -b' = -b, RPM_2' = RPM_2, -c' = -c, -d' = -d\}$, then the corresponding decrypted image remains totally encrypted. This shows that the proposed system is highly sensitive to the pre-encryption key $\{z_0, \lambda\}$.

We now compute the mean square error (MSE) between the input image and the image decrypted by the proposed pre-encryption-based FrFT-DRPE system using $\{z_0' = z_0, \lambda' = \lambda, a' = a, b' = b, RPM_2' = RPM_2, c' = c + \delta_1, d' = d + \delta_2\}$, where the errors δ_1 and δ_2 are independent and uniformly distributed on the set $\{-\delta, \delta\}$. For different values of δ, the MSE obtained by the proposed system is plotted in Fig. 13 and compared with the corresponding MSE obtained by using only the FrFT-DRPE system considered in [5], for which the employed decryption key is $\{a' = a, b' = b, RPM_2' = RPM_2, c' = c + \delta_1, d' = d + \delta_2\}$. It is clear from this figure that the proposed pre-encryption-based FrFT-DRPE system significantly improves the key sensitivity of FrFT-DRPE system. In order to further improve the key sensitivity of proposed pre-encryption-based FrFT-DRPE

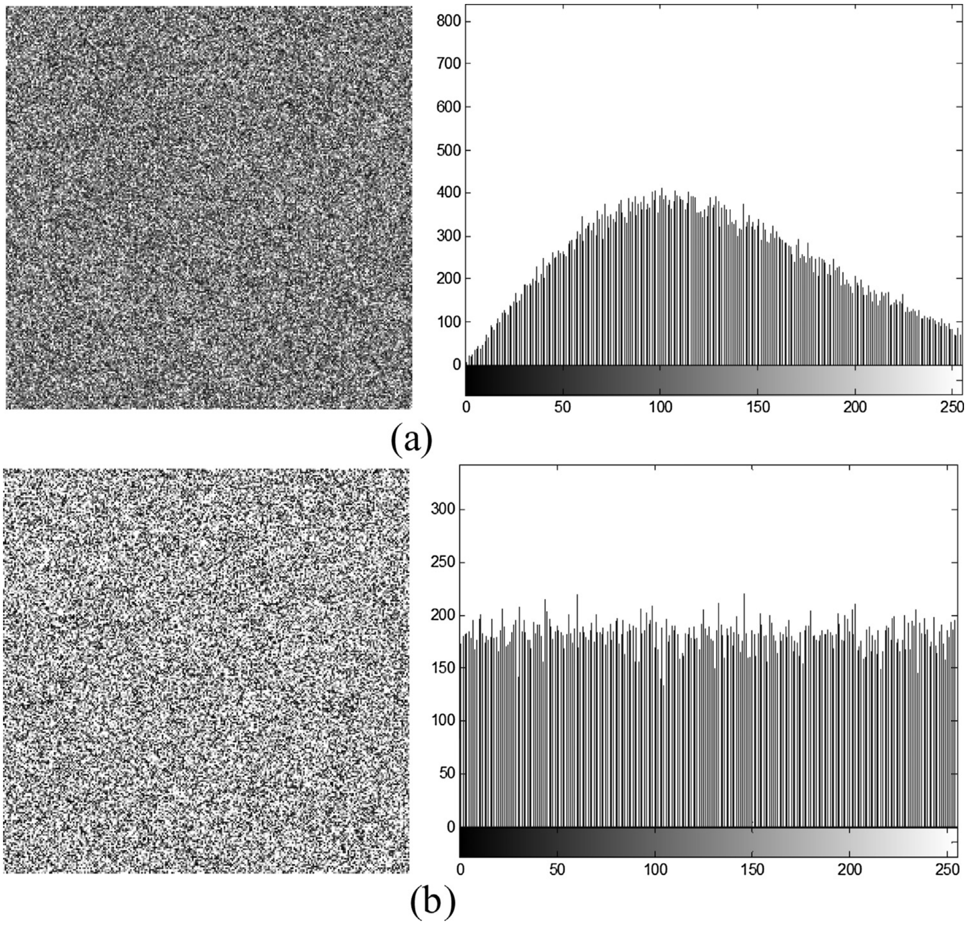


Fig. 7. Encrypted Lena image using the proposed pre-encryption-based MPDFrFT -DRPE system: (a) amplitude and its histogram, (b) phase and its histogram.

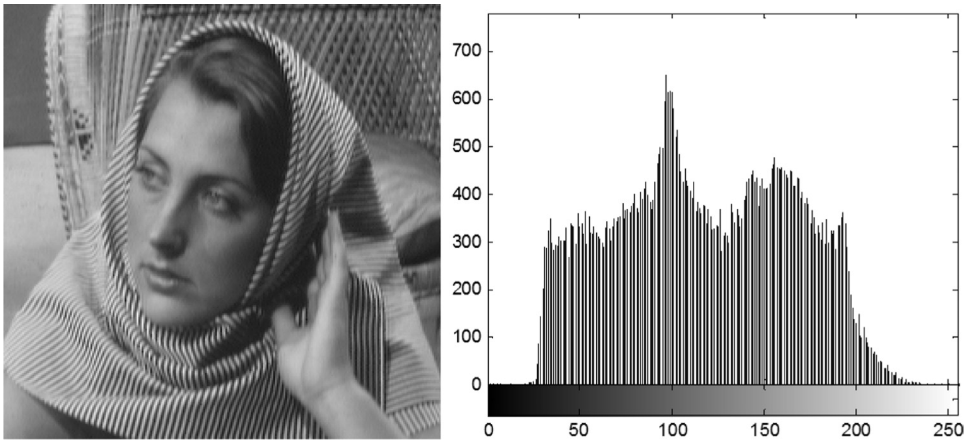


Fig. 8. Input Barbara image and its histogram.

system, we introduce a dependency between the encryption keys of the first and second blocks. For instance, we replace z_0 by $z_0 + 0.1a + 0.1c$ in the encryption and decryption keys. The resulting MSE curve is depicted in Fig. 13, which clearly shows the importance of the introduced dependency.

Let us now perform computer simulations on the proposed pre-encryption-based MPDFrFT-DRPE system similar to the above ones carried out on the proposed pre-encryption-based FrFT-DRPE system. The MSE obtained using $\left\{z_0^{'} = z_0, \lambda^{'} = \lambda,\ -a^{'} = -a,\ -b^{'} = -b,\ RPM_2^{'} = RPM_2,\ -c^{'} = -c + -\delta_1,\ -d^{'} = -d + -\delta_2\right\}$, where the error vectors $-\delta_1$ and

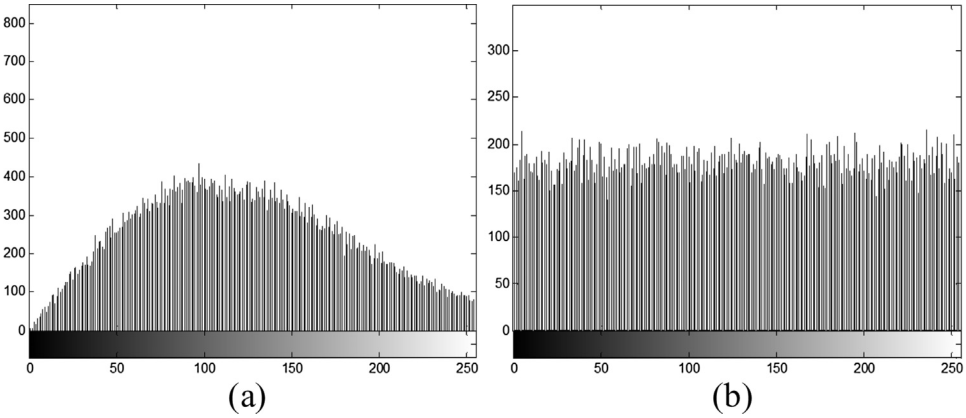


Fig. 9. Histogram of the (a) amplitude and (b) phase of the encrypted Barbara image using the proposed pre-encryption-based MPDFrFT-DRPE system.

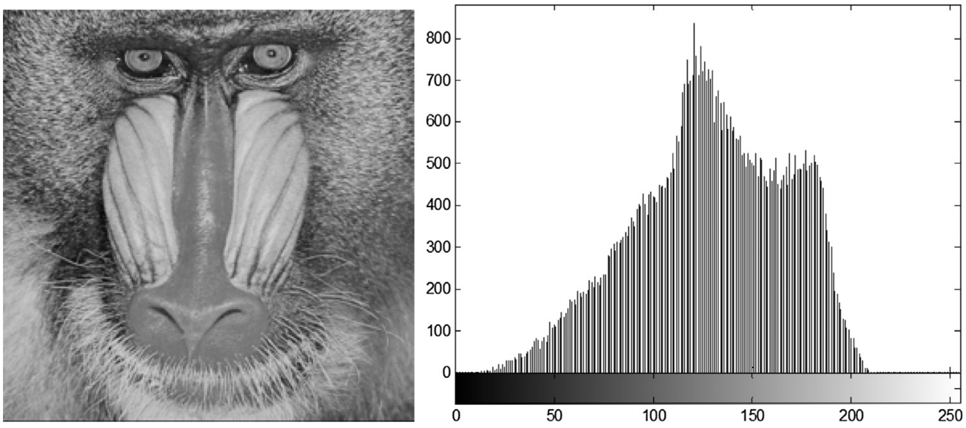


Fig. 10. Input Baboon image and its histogram.

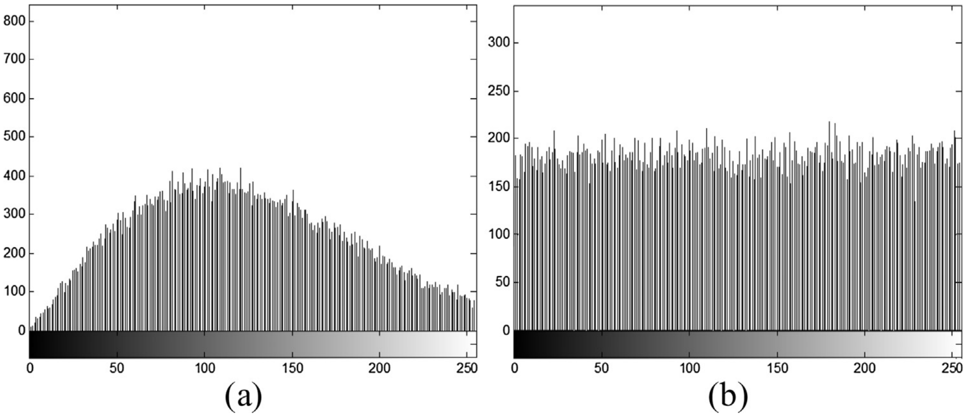
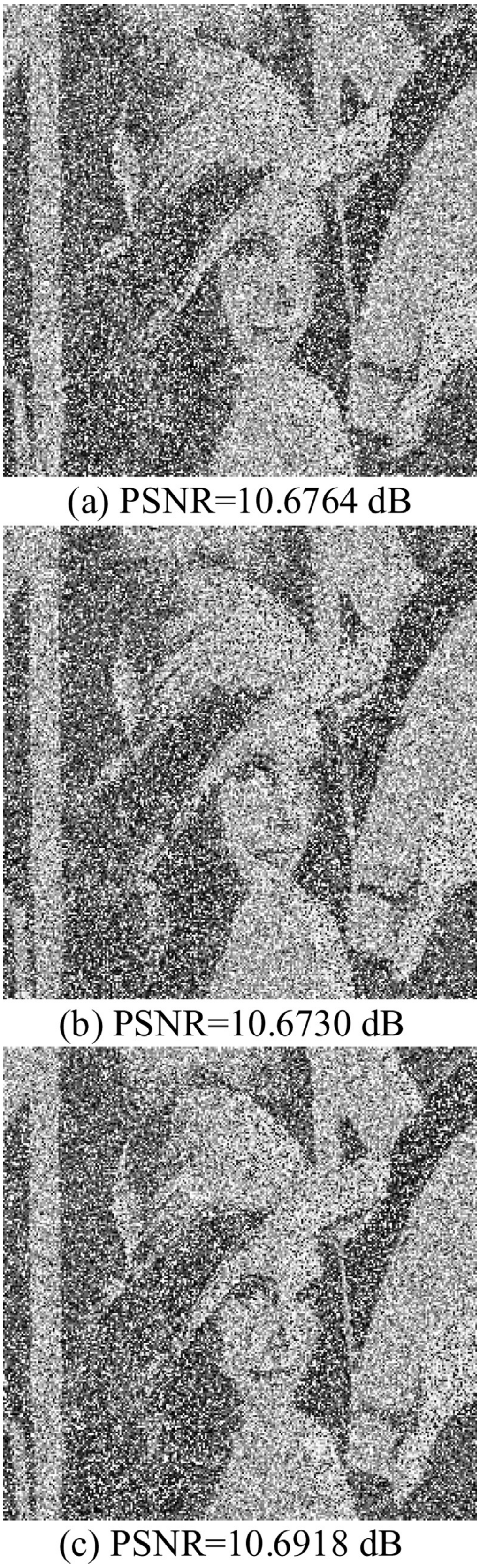


Fig. 11. Histogram of the (a) amplitude and (b) phase of the encrypted Baboon image using the proposed pre-encryption-based MPDFrFT-DRPE system.

$-\delta_2$ are independent and their elements are also independent and uniformly distributed on the set $\left\{-\delta, \delta\right\}$, is plotted in Fig. 14 and compared with the corresponding MSE obtained by using only the MPDFrFT-DRPE system reported in [5], for which the used decryption key is $\left\{-a^{'} = -a,\ -b^{'} = -b,\ RPM_2^{'} = RPM_2,\ -c^{'} = -c + -\delta_1,\ -d^{'} = -d + -\delta_2\right\}$. It is clear from this figure that the proposed system significantly improves the key sensitivity compared to the system in [5]. We also include in Fig. 14 the MSE obtained in [17] to show that the proposed recursive non-linear pre-encryption leads to key sensitivity better than that reached by the non-linear pre-processing introduced in [17], which has been shown to be better than those of all the other existing DRPE-based systems. To further improve the key sensitivity of the proposed pre-encryption-based



(a) PSNR=10.6764 dB

(b) PSNR=10.6730 dB

(c) PSNR=10.6918 dB

Fig. 12. Results of noise attack in the case of the (a) proposed pre-encryption-based FrFT-DRPE technique, (b) proposed pre-encryption-based MPDFrFT-DRPE technique, and (c) technique in [17].

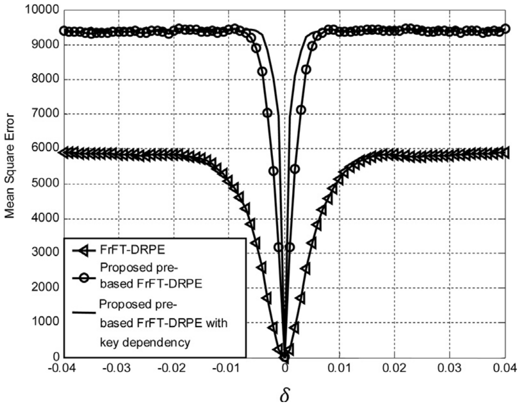


Fig. 13. MSE in terms of the deviation error δ for different FrFT-DRPE systems.

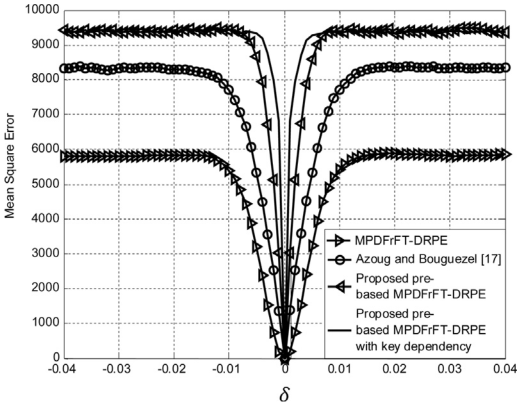


Fig. 14. MSE in terms of the deviation error δ for different MPDFrFT-DRPE systems.

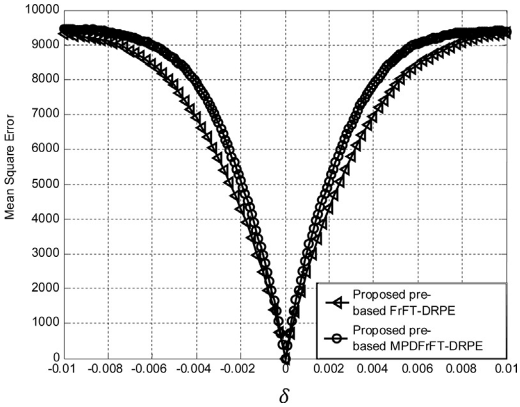


Fig. 15. MSE in terms of the deviation error δ for the proposed pre-encryption-based FrFT- and MPDFrFT-DRPE systems.

MPDFrFT-DRPE system, we introduce a dependency between the encryption keys of the first and second blocks. For instance, we replace z_0 in the encryption and decryption keys by $z_0 + 0.1 - a(N/2) + 0.1 - c(N/2)$, where $-a(N/2)$ and $-c(N/2)$ are the $(N/2)$th elements of the vectors $-a$ and $-c$, respectively. The resulting MSE curve is depicted in Fig. 14, which clearly confirms again the importance of the introduced dependency.

Figs. 13 and 14 compare separately the key sensitivity of the systems that are based on the FrFT and MPDFrFT, respectively, in the interval [-0.04, 0.04] of the deviation error δ. This is to clearly show the improvements that can be achieved by the proposed system either in the FrFT domain or in the MPDFrFT domain. The comparison between the classical DPREs employing these two domains has already been carried out in [5], which shows that the latter outperforms the former in terms of the key sensitivity. In order to closely compare these two domains in the case of the proposed system, we restrict

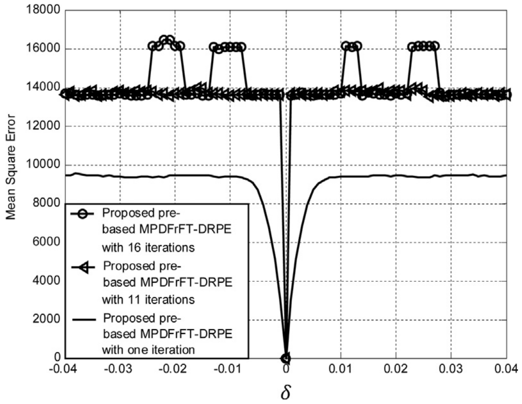


Fig. 16. MSE in terms of the deviation error δ for the proposed pre-encryption-based MPDFrFT-DRPE system for different numbers of pre-encryption iterations.

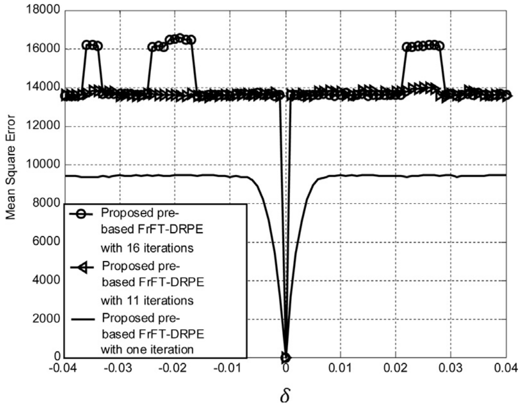


Fig. 17. MSE in terms of the deviation error δ for the proposed pre-encryption-based FrFT-DRPE system for different numbers of pre-encryption iterations.

in Fig. 15 the interval of the deviation error δ to [-0.01, 0.01] and then depict the MSE curves obtained by the proposed pre-encryption-based FrFT-DRPE and MPDFrFT-DRPE systems. It is seen from this figure that the latter, which can reach an MSE greater than 9000 in the interval $\left|\delta\right| \geq 6 \times 10^{-3}$, outperforms the former for which the corresponding interval is smaller and is $\left|\delta\right| \geq 8 \times 10^{-3}$. This is mainly due to the fact that the MPDFrFT domain possesses 4*N* independent parameters, whereas the FrFT domain has only four.

The key sensitivity of the proposed pre-encryption-based technique can significantly be improved by repeating the proposed recursive non-linear pre-encryption for a fixed number of times before applying the DRPE. The simulation results corresponding to the experiments carried out for this purpose are given in Figs. 16 and 17 for different numbers of repetitions or iterations. It is clear from these figures that, for both the proposed pre-encryption-based FrFT-DRPE and MPDFrFT-DRPE systems, the MSE can be increased from about 9500 for one iteration to about 13,700 for 11 or 16 iterations

5. Conclusion

We have shown that by introducing a new digital pre-encryption based on a recursive XOR operation, the key sensitivity of the existing DRPE-based cryptosystems can significantly be improved. We have also shown that farther improvements can be achieved by the proposed pre-encryption-based DRPE system by introducing a dependency between the keys of the pre-encryption and DRPE blocks and/or by repeating the proposed recursive non-linear pre-encryption a number of times before applying the DRPE. Computer simulations confirm that the proposed pre-encryption-based FrFT- or MPDFrFT-DRPE system outperforms the existing DRPE systems. Moreover, the proposed pre-encryption can easily be incorporated at the input of the existing well-established optical or opto-digital DRPE systems without any alteration. Therefore, the optical or opto-digital implementation of the proposed pre-encryption-based DRPE system is straightforward.

References

[1] S. Liu, C. Guo, J.T. Sheridan, A review of optical image encryption techniques, Opt. Laser Technol. 57 (2014) 327–342.
[2] P. Refregier, B. Javidi, Optical image encryption based on input plane, Opt. Lett. 20 (1995) 767–769.

[3] G. Unnikrishnan, K. Singh, Double random fractional Fourier-domain encoding for optical security, Opt. Eng. 39 (2000) 2853–2859.
[4] G. Situ, J. Zhang, Double random phase encoding in the Fresnel domain, Opt. Lett. 29 (2004) 1584–1586.
[5] S. Pei, W. Hsue, The multiple-parameter discrete fractional Fourier transform, IEEE Sig. Process. 13 (2006) 329–332.
[6] J.A. Rodrigo, T. Alieva, M.L. Calvo, Applications of gyrator transform for image processing, Opt. Commun. 278 (2007) 279–284.
[7] S. Bouguezel, M.O. Ahmad, M.N.S. Swamy, Image encryption using the reciprocal–orthogonal parametric transform, in: Proceedings of the IEEE International Symposium on Circuits and Systems, 2010, pp. 2542–2545.
[8] S. Bouguezel, A reciprocal–orthogonal parametric transform and its fast algorithm, IEEE Signal. Process. Lett. 19 (2012) 769–772.
[9] S. Bouguezel, M.O. Ahmad, M.N.S. Swamy, A new involutory parametric transform and its application to image encryption, in: Proceedings of the IEEE International Symposium on Circuits and Systems, 2013, pp. 2605–2608.
[10] B. Hennelly, J.T. Sheridan, Optical image encryption by random shifting in fractional Fourier domains, Opt. Lett. 28 (2003) 269–271.
[11] N. Singh, A. Sinha, Optical image encryption using fractional Fourier transform and chaos, Opt. Lasers Eng. 46 (2008) 117–123.
[12] J. Lang, R. Tao, Y. Wang, Image encryption based on the multiple parameter discrete fractional Fourier transform and chaos function, Opt. Commun. 283 (2010) 2092–2096.
[13] S. Liu, J.T. Sheridan, Optical encryption by combining image scrambling techniques in fractional Fourier domains, Opt. Commun. 287 (2013) 73–80.
[14] X. Peng, P. Zhang, H. Wei, B. Yu, Known-plaintext attack on optical encryption based on double random phase keys, Opt. Lett. 31 (2006) 1044–1046.
[15] W. Qin, 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) 075402.
[16] Y. Zhang, D. Xiao, W. Wen, 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 (2013) 4506–4509.
[17] S.E. Azoug, S. Bouguezel, A non-linear preprocessing for opto-digital image encryption using multiple-parameter discrete fractional Fourier transform, Opt. Commun. 359 (2016) 85–94.
[18] H. Zhou, X. Ling, Problems with the chaotic inverse system encryption approach, IEEE Trans. Circ. Syst. 44 (1997) 268–271.