Journal of
Electronic Imaging

JElectronicImaging.org

Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform

Toufik Bekkouche
Saad Bouguezel

SPIE. IS&T imaging.org

Toufik Bekkouche, Saad Bouguezel, “Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform,” *J. Electron. Imaging* **27**(2), 023033 (2018), doi: 10.1117/1.JEI.27.2.023033.

Digital double random amplitude image encryption method based on the symmetry property of the parametric discrete Fourier transform

Toufik Bekkouche[a] **and Saad Bouguezel**[b,*]
[a]University Bordj Bouarreridj, ETA Laboratory, Department of Electronics, Faculty of Technology, Bordj Bou Arréridj, Algeria
[b]University Ferhat Abbas Setif-1, LCCNS Laboratory, Department of Electronics, Faculty of Technology, Setif, Algeria

Abstract. We propose a real-to-real image encryption method. It is a double random amplitude encryption method based on the parametric discrete Fourier transform coupled with chaotic maps to perform the scrambling. The main idea behind this method is the introduction of a complex-to-real conversion by exploiting the inherent symmetry property of the transform in the case of real-valued sequences. This conversion allows the encrypted image to be real-valued instead of being a complex-valued image as in all existing double random phase encryption methods. The advantage is to store or transmit only one image instead of two images (real and imaginary parts). Computer simulation results and comparisons with the existing double random amplitude encryption methods are provided for peak signal-to-noise ratio, correlation coefficient, histogram analysis, and key sensitivity. *© 2018 SPIE and IS&T* [DOI: 10.1117/1.JEI.27.2.023033]

Keywords: complex-to-real conversion; double random amplitude encryption; parametric discrete Fourier transforms; real-to-real image encryption.

Paper 170902 received Oct. 18, 2017; accepted for publication Apr. 5, 2018; published online Apr. 26, 2018.

1 Introduction

Communication networks are widely used for the exchange of information, such as audio, image, video, etc. The security of the exchanged information has become a major necessity in many civilian and military applications to ensure the confidentiality and prevent any modification or unauthorized duplication of such data. One of the known methods for effectively achieving this goal is the encryption that makes the exchanged information completely or partially unreadable and incomprehensible.

Several encryption techniques have been proposed and can be classified into two categories: temporal (or spatial) and frequency techniques. Traditional encryption algorithms such as data encryption standard, advanced encryption standard and Ronald Rivest, Adi Shamir Adleman and Leonard,[1] where the encryption is done in the spatial domain, are not adequate for image encryption, because these algorithms require a large number of operations, which substantially increases the calculation time. To provide better solutions for images, techniques have been proposed in Refs. 2–8, where the encryption is done in the frequency domain to exploit the fast algorithms of the discrete transforms. These techniques are the well-known double random phase encryption based on the discrete Fourier transform (DFT)[2,3] and the double random amplitude encryption based on the discrete Hartley transform.[4–8] To develop encryption techniques more robust and suitable for applications of recent communication services, parametric transforms have been used to exploit their independent parameters as additional secret keys for encryption.[9–18] However, all the existing image encryption techniques that are based on complex-valued transforms suffer from the fact that the resulting encrypted image is complex-valued, which requires the storage or transmission of two images (real and imaginary parts).

In this paper, we show that the above problem can efficiently be solved by exploiting the symmetry property of the considered complex-valued transform and introducing a complex-to-real (C2R) conversion. This new approach is applied here to develop a real-to-real image encryption method based on the parametric DFT reported in Ref. 19, which is a complex-valued transform. The method is a double random amplitude encryption technique coupled with a chaotic scrambling. It is designed to exploit the independent parameters of the parametric DFTs as an additional secret key for encryption and ensure that the resulting encrypted image is real-valued. The chaotic maps are used to reinforce the secret key. The rest of the paper is organized as follows. In Sec. 2, we recall the definitions of the parametric DFT and review its properties, specifically the symmetry property. We also elaborate the C2R conversion in one-dimensional (1-D) and two-dimensional (2-D) cases and present the chaos map used for scrambling. The proposed image encryption method is described in Sec. 3. Section 4 presents simulation results for the proposed and existing double random amplitude image encryption methods. Finally, some concluding remarks are given in Sec. 5.

2 Preliminaries

2.1 *Parametric Discrete Fourier Transform*

In this section, we review the parametric DFT and some of its pertinent properties, which are subsequently exploited in this paper for developing a new image encryption technique.

[*] Address all correspondence to: Saad Bouguezel, E-mail: bouguezel_saad@yahoo.com

1017-9909/2018/$25.00 © 2018 SPIE and IS&T

2.1.1 *Definitions*

Let us first define the forward DFT $X(n)$ of a real sequence $x(k)$ of length N as follows:

$$X(n)=\sum_{k=0}^{N-1}x(k)W_N^{nk}, \qquad 0\le n\le N-1 \tag{1}$$

and its inverse can then be obtained as follows:

$$x(k)=\frac{1}{N}\sum_{n=0}^{N-1}X(n)W_N^{-nk}, \qquad 0\le k\le N-1, \tag{2}$$

where $W_N=\exp(-j\frac{2\pi}{N})$ with $j=\sqrt{-1}$. Based on the DFT, Bouguezel et al.[19] introduced a three-parameter DFT of length N, where N is an integral power of 2, i.e., $N=2^r$, with r being a positive integer. Its forward version is defined as follows:

$$X^{a,b,c}(n)=\sum_{k=0}^{N-1}x(k)v_{F^{a,b,c}}(nk \bmod N), \qquad 0\le n\le N-1, \tag{3}$$

whereas its inverse is given by

$$x(k)=\frac{1}{N}\sum_{n=0}^{N-1}X^{a,b,c}(n)\frac{1}{v_{F^{a,b,c}}(nk \bmod N)}, \qquad 0\le k\le N-1, \tag{4}$$

where $v_{F^{a,b,c}}(i)$, $0\le i\le N-1$, denote the entries of the kernel vector given by

$$\mathbf{V}_{F^{a,b,c}}=[1 \quad \mathbf{V} \quad c \quad -j\mathbf{V} \quad -1 \quad -\mathbf{V} \quad -c \quad j\mathbf{V}] \tag{5}$$

with

$$\mathbf{V}=\left[W_N^1 \quad \dots \quad W_N^{\frac{N}{16}-1} \quad a \quad W_N^{\frac{N}{16}+1} \quad \dots \quad W_N^{\frac{N}{8}-1} \quad b \quad W_N^{\frac{N}{8}+1} \quad \dots \quad W_N^{\frac{3N}{16}-1} \quad -ja^* \quad W_N^{\frac{3N}{16}+1} \quad \dots \quad W_N^{\frac{N}{4}-1}\right], \tag{6}$$

and a, b, c being three nonzero parameters that can be chosen arbitrarily from the complex plane.

One of the most interesting special cases of the three-parameter DFT can be obtained when $a=e^{j\alpha}$, with α being a parameter that can be chosen arbitrarily from the interval $[-2\pi,0]$, $b=W_N^{N/8}$, and $c=W_N^{N/4}$. This case leads to a one-parameter DFT denoted by DFT$^\alpha$, which is used in the subsequent sections and simply called parametric DFT.

2.1.2 *Properties*

Among the most interesting properties of the parametric DFT, we cite the symmetry between the coefficients in the frequency domain. Let $s(k)$ be a real-valued sequence of length N. Its parametric DFT $F^\alpha(n)$ is a complex-valued sequence of length N having the symmetry property given by

$$s(k)\overset{\text{DFT}^\alpha}{\leftrightarrow}F^\alpha(n)=[F^\alpha(N-n)]^*, \tag{7}$$

where $(.)^*$ denotes the complex-conjugate operation. This property leads to $\text{real}[F^\alpha(n)]=\text{real}[F^\alpha(N-n)]$ and $\text{imag}[F^\alpha(n)]=-\text{imag}[F^\alpha(N-n)]$. Moreover, $F^\alpha(0)$ and $F^\alpha(N/2)$ are always pure real values.

By examining the above symmetry property of the parametric Fourier transform of a real sequence, it can be seen that the first and second halves of its real part are redundant in an inverted order and similar observation for its imaginary part except that the redundancy is in an inverted order with an opposite sign. Based on this symmetry property, we convert the parametric Fourier transform from its complex form to a purely real form by concatenating the first halves of its real and imaginary parts. With this new real form of the transform, which is reversible, we are able to process only half of the data compared to the use of the complex form. The mathematical analysis of this new real form is further clarified by the two illustrations given below. We first study the symmetry property given by Eq. (7) in the 1-D case and then in the 2-D case.

1-D case:

To illustrate the importance of the symmetry property given by Eq. (7), we consider a real-valued vector:

$$\mathbf{s}=[208 \quad 231 \quad 32 \quad 233 \quad 161 \quad 25 \quad 71 \quad 139 \quad 244 \quad 246 \quad 40 \quad 248 \quad 244 \quad 124 \quad 204 \quad 36]$$

of length 16. The value of the parameter α is chosen from the interval $[-2\pi,0]$ and set in this example to be $\alpha=-0.4\pi$. Then, the DFT$^{-0.4\pi}$ of the vector $\mathbf{s}$ is a complex-valued vector given by

$$\begin{aligned}F^{-0.4\pi}=[&2486 \quad 95.8+134.2\text{i} \quad 62.6-245.3\text{i} \quad -262.6-118.9\text{i} \quad 510+30\text{i} \quad 13.8-152.3\text{i} \quad 31.4-651.3\text{i} \quad 9-231.2\text{i}\\ &-78 \quad 9+231.2\text{i} \quad 31.4+651.3\text{i} \quad 13.8+152.3\text{i} \quad 510-30\text{i} \quad -262.6+118.9\text{i} \quad 62.6+245.3\text{i} \quad 95.8-134.2\text{i}].\end{aligned}$$

It can easily be verified that the relationship $F^{-0.4\pi}(n)=[F^{-0.4\pi}(16-n)]^*$ holds for the elements $F^{-0.4\pi}(n)$, $1\le n\le 15$, of the transformed vector $\mathbf{F}^{-0.4\pi}$. Moreover, the elements $F^{-0.4\pi}(0)$ and $F^{-0.4\pi}(8)$ of $\mathbf{F}^{-0.4\pi}$ are pure real values. In order to efficiently exploit the above relationship, we separate the real and imaginary parts of $\mathbf{F}^{-0.4\pi}$, respectively, as

$$\text{real}(\mathbf{F}^{-0.4\pi})=[2486 \quad 95.8 \quad 62.6 \quad -262.6 \quad 510 \quad 13.8 \quad 31.4 \quad 9 \quad -78 \quad 9 \quad 31.4 \quad 13.8 \quad 510 \quad -262.6 \quad 62.6 \quad 95.8]$$

and

$$\mathrm{imag}(\mathbf{F}^{-0.4\pi}) = [0 \quad 134.2 \quad -245.3 \quad -118.9 \quad 30 \quad -152.3 \quad -651.3 \quad -231.2 \quad 0 \quad 231.2 \quad 651.3 \quad 152.3 \quad -30 \quad 118.9 \quad 245.3 \quad -134.2].$$

It is also clear that the relationships $\mathrm{real}[F^{-0.4\pi}(n)] = \mathrm{real}[F^{-0.4\pi}(16-n)]$ and $\mathrm{imag}[F^{-0.4\pi}(n)] = -\mathrm{imag}[F^{-0.4\pi}(16-n)]$ are valid for the two parts of the vector $\mathbf{F}^{-0.4\pi}$, respectively. These two relationships show that only $N/2+1=9$ entries, namely $\mathrm{real}[F^{-0.4\pi}(n)]$, $n=0,1,\dots,N/2$, of $\mathrm{real}(\mathbf{F}^{-0.4\pi})$ and $N/2-1=7$ entries, namely $\mathrm{imag}[F^{-0.4\pi}(n)]$, $n=1,2,\dots,N/2-1$, of $\mathrm{imag}(\mathbf{F}^{-0.4\pi})$ are sufficient to represent the transformed vector $\mathbf{F}^{-0.4\pi}$. This reduced representation is called complex-to-real (C2R) conversion by which a transformed real-valued vector of length $N=16$ representing the transformed complex-valued vector $\mathbf{F}^{-0.4\pi}$ can be obtained as follows:

$$\mathbf{R} = [2486 \quad 95.8 \quad 62.6 \quad -262.6 \quad 510 \quad 13.8 \quad 31.4 \quad 9 \quad -78 \quad 134.2 \quad -245.3 \quad -118.9 \quad 30 \quad -152.3 \quad -651.3 \quad -231.2].$$

The above C2R conversion is illustrated graphically in Fig. 1. Now, by applying the real-to-complex conversion (R2C), the transformed complex-valued vector $\mathbf{F}^{-0.4\pi}$ can easily be obtained from the transformed real-valued vector $\mathbf{R}$ using the above relationships and the corresponding concept is also illustrated graphically in Fig. 2.

2-D case:

The application of the DFT$^{\alpha}$ to transform 2-D sequences or matrices can be performed in different ways. In order to exploit the above symmetry property in the case of real-valued matrices, we apply the DFT$^{\alpha}$ on the rows and then perform on each transformed row the C2R conversion discussed in the 1-D case. Therefore, a straightforward graphical illustration of this concept is given in Fig. 3, which shows that the resulting transformed matrix is also real-valued with the same size as the input. Figure 4 shows graphically how to obtain the original real-valued matrix from the transformed real-valued matrix. The application of the DFT$^{\alpha}$ on columns can be achieved by only transposing the original and transformed real-valued matrices in Figs. 3 and 4.

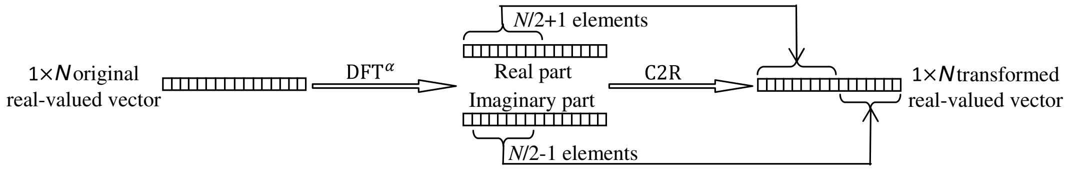

N/2+1 elements
1×N original real-valued vector
DFT^α
Real part
C2R
Imaginary part
1×N transformed real-valued vector
N/2-1 elements

Fig. 1 C2R conversion of the DFT$^{\alpha}$ of a real-valued vector.

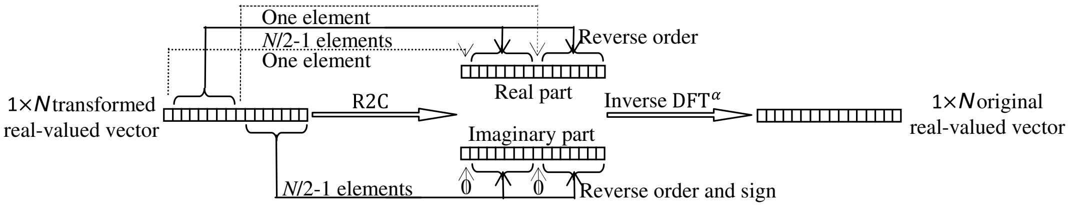


Fig. 2 Inverse DFT$^{\alpha}$ after R2C conversion of the transformed real-valued vector.

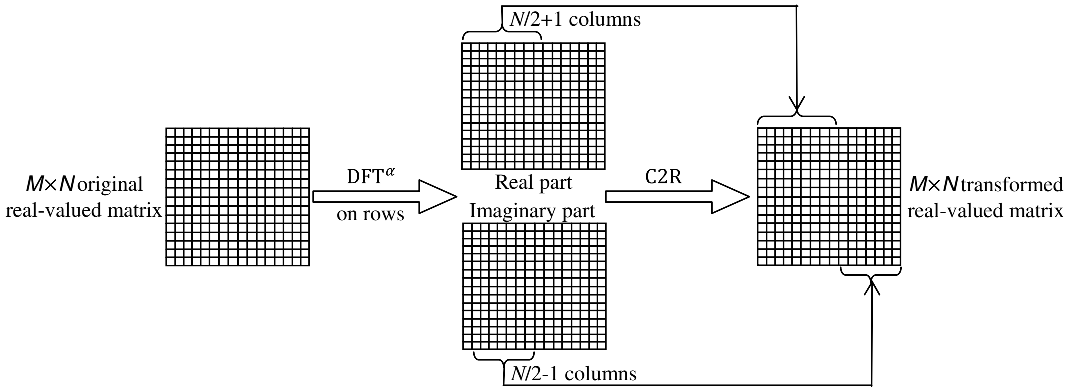

N/2+1 columns
M×N original real-valued matrix
DFT^α
on rows
Real part
Imaginary part
C2R
M×N transformed real-valued matrix
N/2-1 columns

Fig. 3 C2R conversion of the DFT$^{\alpha}$ of the rows of a real-valued matrix.

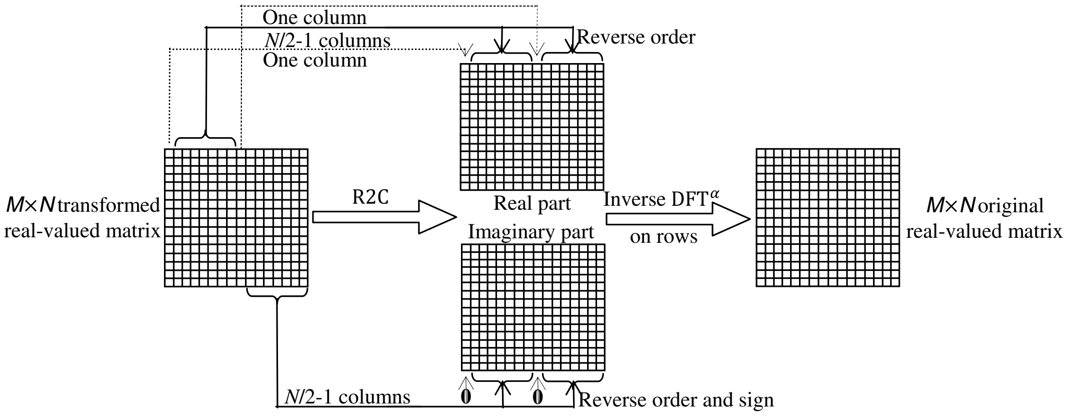


Fig. 4 Inverse DFT$^{\alpha}$ after R2C conversion of the transformed real-valued matrix.

2.2 *Chaos Maps*

Chaos maps are known to have attractive cryptographic properties, such as high sensitivity to their control parameters, ergodicity, and pseudo-randomness, and a wider range of image encryption applications.[20,21] Therefore, we adopt such maps for the scrambling required in the following proposed image encryption method. Specifically, we consider the piecewise linear chaotic map (PLCM) proposed in Ref. 20 as follows:

$$z_{k+1} = F(z_k, \lambda) = \begin{cases} \frac{z_k}{\lambda}, & 0 \le z_k < \lambda \\ \frac{z_k - \lambda}{0.5 - \lambda}, & \lambda \le z_k < 0.5 \\ F(1 - z_k, \lambda), & 0.5 \le z_k < 1 \end{cases}, \tag{8}$$

where $\mathbf{z_0}$ is the initial condition parameter and $\lambda \in (\mathbf{0}, \mathbf{0.5})$ is the control parameter.

3 Proposed Method

3.1 *Encryption Scheme*

The proposed encryption scheme, as shown in Fig. 5, can be achieved by the following steps:

Step 1: The original image, which is generally a real-valued image of size $M \times N$, is multiplied element-by-element by the first random intensity mask K_1.
Step 2: Apply the DFT$^{\alpha}$ on the rows of the real-valued image obtained in step 1.
Step 3: Apply the C2R conversion on the complex-valued image obtained in step 2.
Step 4: Reshape the transformed real-valued image obtained in step 3 to a vector and scramble the result using the first PLCM chaotic map with (z_0, λ_0). The resulting vector is then reshaped to an image.
Step 5: Apply the DFT$^{\beta}$ on the columns of the real-valued image obtained in step 4.
Step 6: Apply the C2R conversion on the complex-valued image obtained in step 5.
Step 7: Reshape the transformed real-valued image obtained in step 6 to a vector and scramble the result using the second PLCM chaotic map with (z_1, λ_1). The resulting vector is then reshaped to an image.
Step 8: Multiply the real-valued image obtained in step 7 element by element by the second random intensity mask K_2.
Step 9: Apply the DFT$^{\gamma}$ on the rows of the real-valued image obtained in step 8.
Step 10: Apply the C2R conversion on the complex-valued image obtained in step 9.
Step 11: Reshape the transformed real-valued image obtained in step 10 to a vector and scramble the result using the third PLCM chaotic map with (z_2, λ_2). The resulting vector is then reshaped to an image.
Step 12: Apply the DFT$^{\zeta}$ on the columns of the real-valued image obtained in step 11.
Step 13: Apply the C2R conversion on the complex-valued image obtained in step 12.
Step 14: Reshape the transformed real-valued image obtained in step 13 to a vector and scramble the result using the fourth PLCM chaotic map with (z_3, λ_3). The resulting vector is then reshaped to an image.
Step 15: The encrypted image is the real-valued image obtained in step 14.

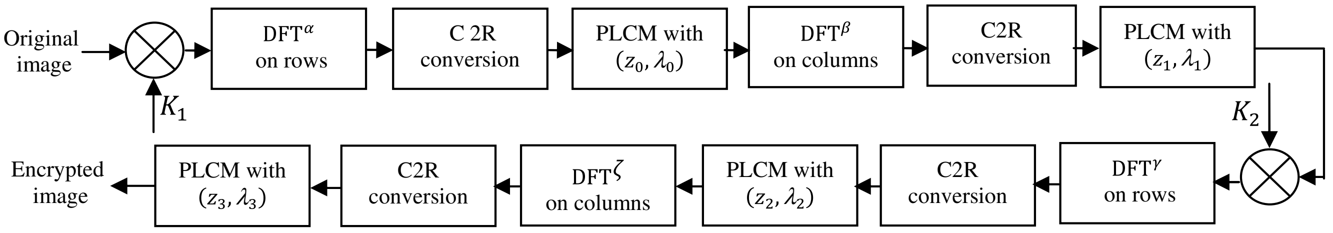


Fig. 5 Proposed image encryption scheme.

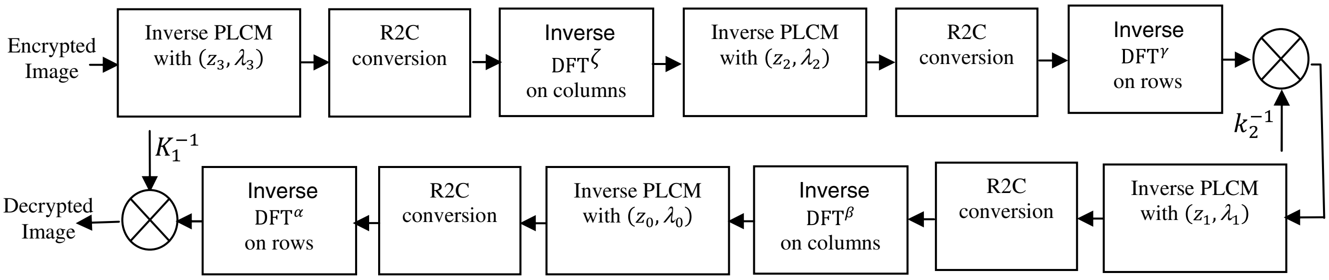

Encrypted Image
Inverse PLCM with (z_3, λ_3)
R2C conversion
Inverse DFT$^\zeta$ on columns
Inverse PLCM with (z_2, λ_2)
R2C conversion
Inverse DFT$^\gamma$ on rows
k_2^{-1}
Inverse PLCM with (z_1, λ_1)
R2C conversion
Inverse DFT$^\beta$ on columns
Inverse PLCM with (z_0, λ_0)
R2C conversion
Inverse DFT$^\alpha$ on rows
K_1^{-1}
Decrypted Image

Fig. 6 Proposed image decryption scheme.

3.2 *Decryption Scheme*

The decryption process, as shown in Fig. 6, takes the steps of the encryption process in an inverse manner to obtain the decrypted image. The encryption secret key in the proposed encryption scheme is composed of the two random intensity masks K_1 and K_2, the parameters $\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$, and $\{z_3, \lambda_3\}$ of the four chaotic maps, and the parameters $(\alpha, \beta, \gamma, \zeta)$ used for the parametric Fourier transforms.

In order to further reinforce the secret key, we introduce some dependencies between the independent parameters $(\alpha, \beta, \gamma, \zeta)$ of the parametric Fourier transforms and the parameters $\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$, and $\{z_3, \lambda_3\}$ of the chaotic maps. For instance, we replace in the encryption and decryption processes the initial condition parameters z_0, z_1, z_2, and z_3 by $z_0 + 0.01\alpha + 0.01\gamma$, $z_1 + 0.01\beta + 0.01\zeta$, $z_2 + 0.01\alpha + 0.01\gamma$, and $z_3 + 0.01\beta + 0.01\zeta$, respectively.

4 Numerical Results and Comparison

In order to demonstrate the efficiency of the proposed image encryption method, we present in this section some numerical results by considering standard test images Lena (256×256), Barbara (256×256), and Clown image of size (512×512). The two random intensity masks K_1 and K_2 are generated randomly from the interval [0,1], and the independent parameters $(\alpha, \beta, \gamma, \zeta)$ of the parametric Fourier transforms are randomly chosen from the interval $[-2\pi, 0]$. The four PLCM chaotic maps are preselected as $\{z_0, \lambda_0\} = \{0.1428 + 0.01\alpha + 0.01\gamma, 0.2567\}$, $\{z_1, \lambda_1\} = \{0.2857 + 0.01\beta + 0.01\zeta, 0.9856\}$, $\{z_2, \lambda_2\} = \{0.2428 + 0.01\alpha + 0.01\gamma, 0.1567\}$, and $\{z_3, \lambda_3\} = \{0.1857 + 0.01\beta + 0.01\zeta, 0.8856\}$. For the evaluation, we use different metrics.

The peak signal-to-noise ratio (PSNR) is used to measure the damage degree to the original image caused by applying an encryption method. It is defined for gray scale images as follows:

$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \text{ (dB)}, \tag{9}$$

where MSE is the mean square error between the encrypted image E and the corresponding original image I. It is defined as follows:

$$\text{MSE} = \left(\frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} |i_{m,n} - e_{m,n}|^2\right), \tag{10}$$

where $i_{m,n}$ and $e_{m,n}$ denote the pixel values at the position (m, n) of the original and encrypted images, respectively, and $M \times N$ denotes the size of the image. For computer simulations, we consider square input images, i.e., $M = N$.

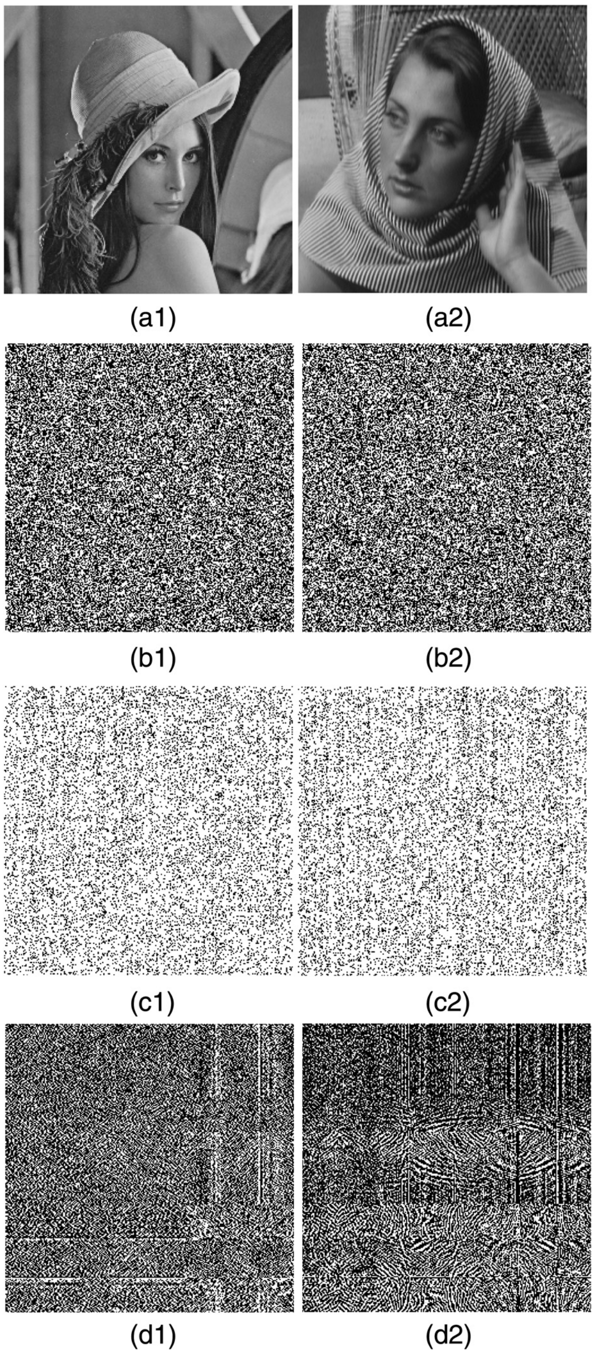


Fig. 7 Image encryption: (a_1) and (a_2) original test images, (b_1) and (b_2) the corresponding encrypted images using the proposed encryption method, (c_1) and (c_2) the corresponding encrypted images using the method in Ref. 5, (d_1) and (d_2) the corresponding encrypted images using the second method in Ref. 6.

The standard correlation coefficient is used to measure the similarity between the encrypted and original images. It can be defined as follows:

$$\mathrm{corr}(I,E)=\frac{\sum_m\sum_n(i_{m,n}-\overline{I})(e_{m,n}-\overline{E})}{\sqrt{\sum_m\sum_n(i_{m,n}-\overline{I})^2\sum_m\sum_n(e_{m,n}-\overline{E})^2}}, \tag{11}$$

where $\overline{I}=\mathrm{mean}(I)$ and $\overline{E}=\mathrm{mean}(E)$ are the mean values of the original and encrypted images, respectively.

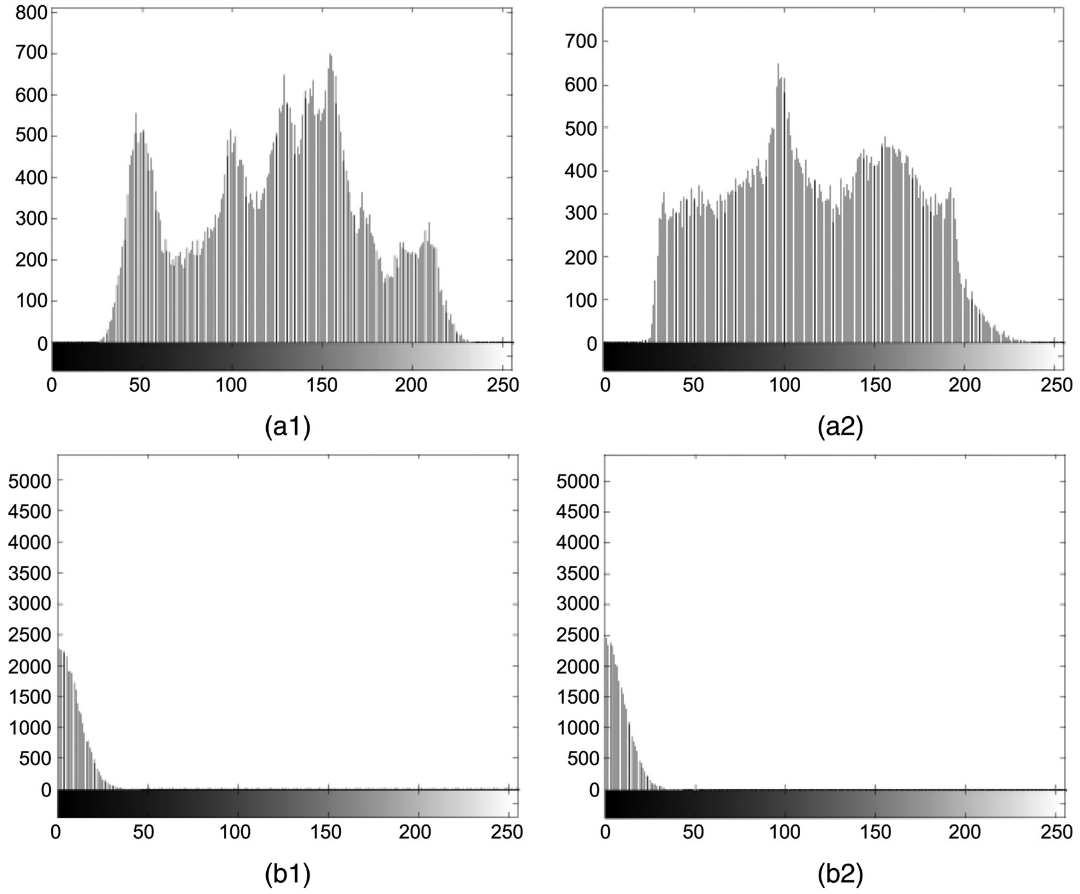
We also use the base 10 logarithm of mean square error (LMSE) given by

$$\mathrm{LMSE}=\log_{10}\left(\frac{1}{M\times N}\sum_{m=1}^{M}\sum_{n=1}^{N}|i_{m,n}-e_{m,n}|^2\right). \tag{12}$$

The encrypted versions of different standard test images obtained using the proposed image encryption method described in Sec. 3, the method reported in Ref. 5, which is based on the random Hartley transform, and the second method reported in Ref. 6, which is based on the Hartley transform, jigsaw transform, and logistic map, are presented in Fig. 7. It can be seen from this figure that the encrypted images provided by the three methods do not contain any visual information of the corresponding original images. Concerning the implementation of the transforms in the three methods, we have adopted the expressions $\mathbf{X}=\mathbf{T}\times\mathbf{x}/\sqrt{N}$ and $\mathbf{x}=\mathbf{Q}\times\mathbf{X}/\sqrt{N}$ or $\mathbf{E}=\mathbf{T}\times\mathbf{I}\times\mathbf{Q}/N$ and $\mathbf{I}=\mathbf{Q}\times\mathbf{I}\times\mathbf{T}/N$, where $\mathbf{x}$ is a column vector of length N to be transformed, $\mathbf{T}$ is a transform matrix of size $N\times N$, $\mathbf{Q}$ is the hermitian of $\mathbf{T}$ when $\mathbf{T}$ is unitary (e.g., DFT) and $\mathbf{Q}=\mathbf{T}$ when $\mathbf{T}$ is involutory (e.g., discrete Hartley

Table 1 PSNR and correlation coefficient obtained by the proposed and existing[5,6] methods for different test images.

	PSNR, dB			Correlation		
Image encrypted	Proposed method	Ref. 5	Ref. 6	Proposed method	Ref. 5	Ref. 6
Lena 256×256	5.6086	7.3581	5.4939	0.0029	0.041	-0.0041
Barbara 256×256	6.0188	7.7063	5.9322	−0.0056	−0.0094	0.0057
Clown 512×512	6.8340	8.3326	0.7683	−0.0031	−0.0068	0.0051



(a1)

(a2)

(b1)

(b2)

Fig. 8 Histograms of Lena and Barbara: (a_1) and (a_2) of original images, (b_1) and (b_2) of encrypted images using the proposed method.

transform), and $\mathbf{I}$ is an image of size $N \times N$ to be transformed in a row–column fashion.

The results obtained for the PSNR and correlation coefficient are summarized in Table 1 for different methods and test images. It is clear from this table that the proposed method outperforms the methods presented in Refs. 5 and 6 in terms of the correlation coefficient, whereas the second method in Ref. 6 provides better PSNR.

4.1 *Histogram Analysis*

To show the robustness of the proposed encryption method against histogram analysis, we encrypt two different standard test images, namely Lena and Barbara, and compute their histograms before and after encryption. The results are presented in Fig. 8, which shows that even though the histograms of the original images are completely different, the histograms of the corresponding encrypted images are very similar and hence no useful information can be extracted from the encrypted images. This demonstrates that the proposed method is effectively robust against histogram analysis.

4.2 *Key Sensitivity*

As mentioned in Sec. 3, the encryption secret key for the proposed encryption scheme is composed of the two random intensity masks K_1 and K_2, the parameters $\{z_0, \lambda_0\}$, $\{z_1, \lambda_1\}$, $\{z_2, \lambda_2\}$, and $\{z_3, \lambda_3\}$ of the four chaotic maps, and the parameters $(\alpha, \beta, \gamma, \zeta)$ used for the parametric Fourier transforms. In order to verify the sensitivity of the proposed encryption method to errors in the parameters of the four PLCM chaotic maps, we assume for the decryption process that all the parameters of the four PLCM chaotic maps, the two random intensity masks, and the parameters of parametric DFT are correct and only one of the parameters of the four PLCM chaotic maps is slightly different from the one used in the encryption process.

The decrypted Lena image is presented in Fig. 9 for different cases. The result for the cases of z_3 and λ_3 is similar to those shown for z_2 and λ_2, respectively. This figure confirms that the decrypted image remains totally encrypted and the proposed method is very sensitive to any small error in any parameter of the PLCMs.

Similarly, to show the robustness of the proposed encryption method against brute force attacks, we assume for the decryption process that all the parameters of the four PLCM chaotic maps and the two random intensity masks are correct, and only some parameters of the parametric Fourier transforms are slightly different from the ones used in the encryption process. The decrypted Lena image is shown in Fig. 10 for different cases. This figure again confirms that the decrypted image remains totally encrypted and the proposed method is very sensitive to any error in any parameter of the parametric transforms.

Moreover, to verify the key sensitivity of the proposed method to the two random intensity masks K_1 and K_2, let us consider that all the parameters that constitute the secret key are correct except K_1 (or K_2). In this case, the encrypted image is decrypted by introducing a small error δ_1 (or δ_2) in the random intensity mask as $K_1' = K_1 + \delta_1$ (or $K_2' = K_2 + \delta_2$), where the error δ_1 (or δ_2) is independent and uniformly distributed on the set $\{-\delta, \delta\}$. We then compute the LMSE between the original and decrypted images. The LMSEs obtained by the proposed and existing[5] method are plotted in terms of the deviation error δ in Figs. 11 and 12 for the first and second random intensity masks, respectively.

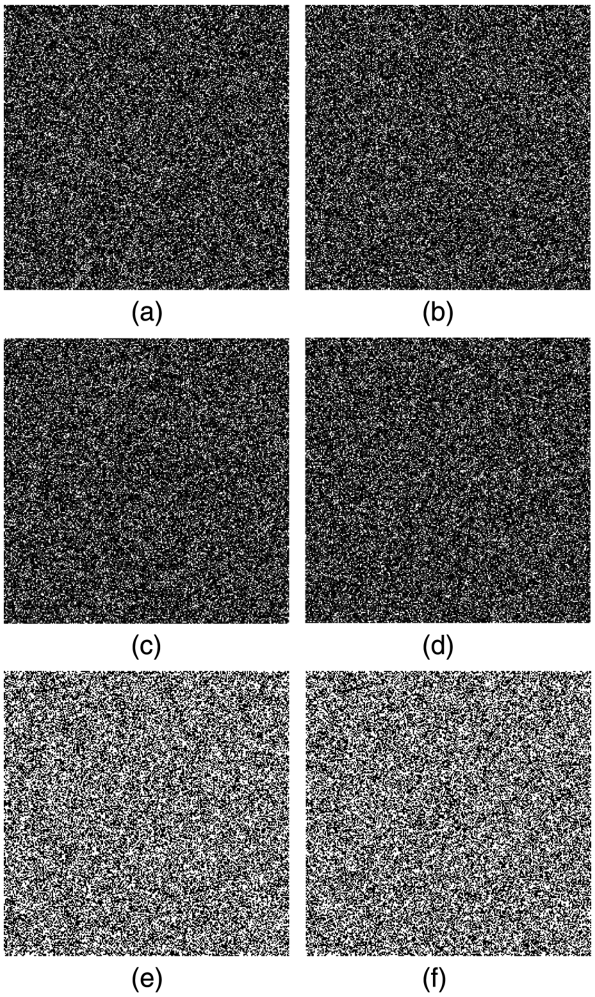


Fig. 9 Decrypted Lena image using (a) $z_0' = z_0 + 10^{-16}$; (b) $\lambda_0' = \lambda_0 + 10^{-16}$; (c) $z_1' = z_1 + 10^{-16}$; (d) $\lambda_1' = \lambda_1 + 10^{-16}$; (e) $z_2' = z_2 + 10^{-16}$; and (f) $\lambda_2' = \lambda_2 + 10^{-16}$.

These figures show that the two methods have similar sensitivities to the random intensity masks. Due to this result, we do not take into consideration the influence of the two random intensity masks K_1 and K_2 in the following analysis and comparison, and we consider that the encryption secret key is constituted only of the parameters $\{z_0, \lambda_0, z_1, \lambda_1, z_2, \lambda_2, z_3, \lambda_3, \alpha, \beta, \gamma, \zeta\}$. The corresponding decryption key is $\{z_0', \lambda_0', z_1', \lambda_1', z_2', \lambda_2', z_3', \lambda_3', \alpha', \beta', \gamma', \zeta'\}$. We now compute the LMSE between the original image and the image decrypted using $\{z_0' = z_0,\ \lambda_0' = \lambda_0,\ z_1' = z_1,\ \lambda_1' = \lambda_1,\ z_2' = z_2,\ \lambda_2' = \lambda_2,\ z_3' = z_3,\ \lambda_3' = \lambda_3,\ \alpha' = \alpha + \delta_1,\ \beta' = \beta + \delta_2,\ \gamma' = \gamma,\ \zeta' = \zeta\}$, where the errors δ_1 and δ_2 are independent and uniformly distributed on the set $\{-\delta, \delta\}$. For different values of δ, the LMSE obtained by the proposed method is plotted in Fig. 13 and compared with the corresponding LMSE obtained by the existing method reported in Ref. 5 for which the employed decryption key is $\{\mathrm{s}_0' = \mathrm{s}_0 + \delta, \mathrm{s}_1' = \mathrm{s}_1 + \delta\}$, where s_0 and s_1 are two random $N \times N$ matrices chosen arbitrarily from the interval [0 1]. It is clear from this figure that the proposed method is better than the method in Ref. 5. Other LMSEs are shown in

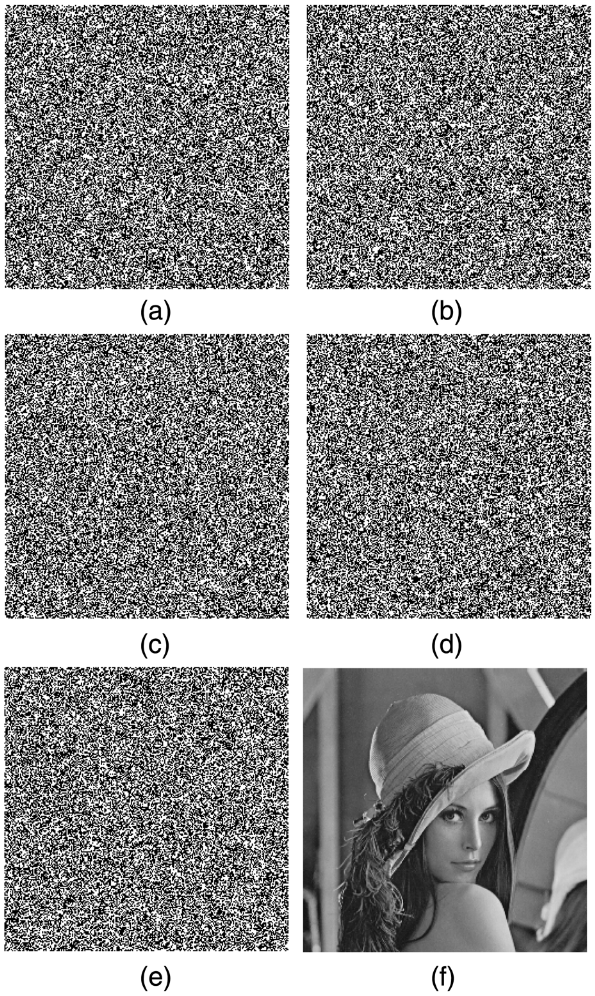


Fig. 10 Decrypted Lena image using (a) wrong α; (b) wrong β; (c) wrong γ; (d) wrong ζ; (e) wrong α, β, γ, and ζ; and (f) correct parameters $\alpha' = \alpha$, $\beta' = \beta$, $\gamma' = \gamma$, and $\zeta' = \zeta$.

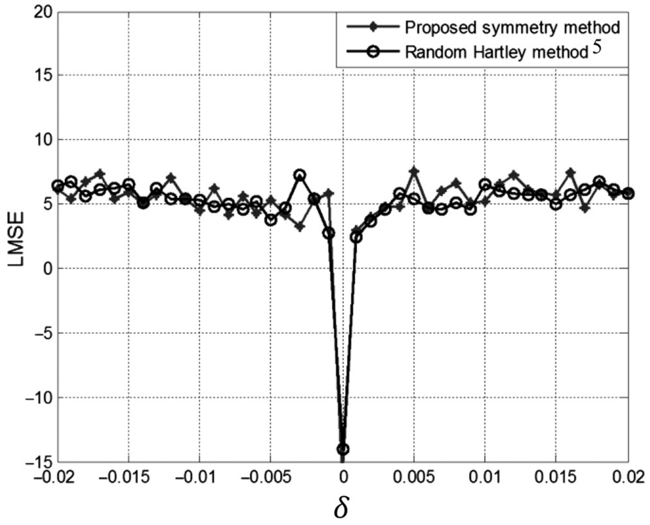


Fig. 11 LMSE in terms of the deviation error δ for K_1'.

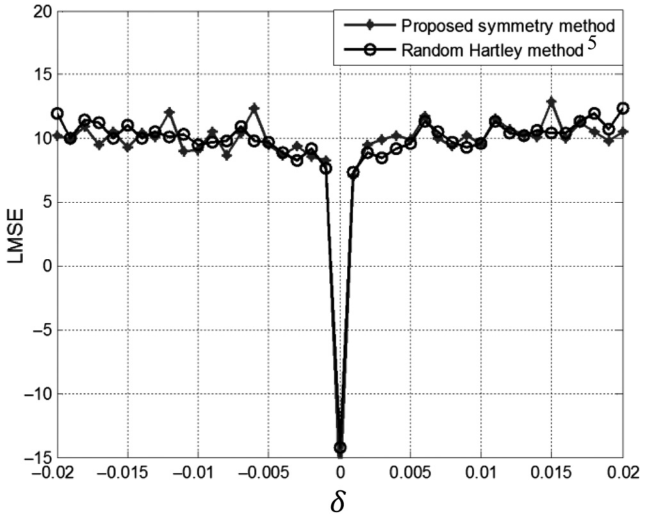


Fig. 12 LMSE in terms of the deviation error δ for K_2'.

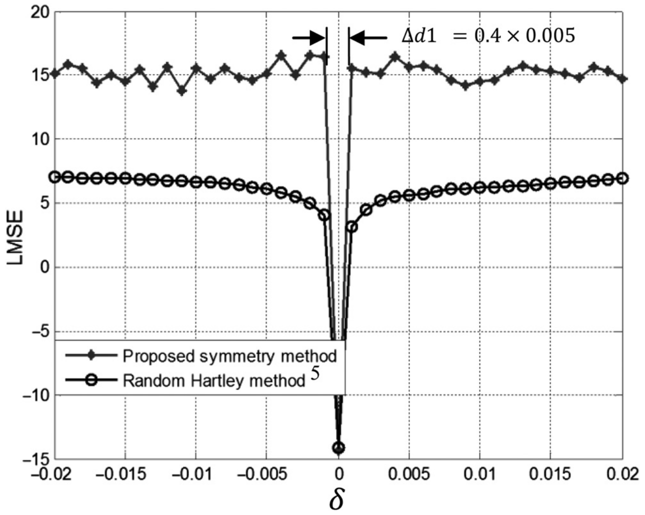


Fig. 13 LMSE in terms of the deviation error δ for α' and β' (proposed method) and for s_0' and s_1' (method in Ref. 5).

Fig. 14 for the proposed method with $\{z_0' = z_0,\ \lambda_0' = \lambda_0,\ z_1' = z_1,\ \lambda_1' = \lambda_1,\ z_2' = z_2,\ \lambda_2' = \lambda_2,\ z_3' = z_3,\ \lambda_3' = \lambda_3,\ \alpha' = \alpha,\ \beta' = \beta,\ \gamma' = \gamma + \delta_1,\ \zeta' = \gamma + \delta_2\}$, and for the method in Ref. 5 with $\{s_2' = s_2 + \delta, s_3' = s_3 + \delta\}$, where s_2 and s_3 are two random $N \times N$ matrix chosen arbitrarily from the interval [0 1]. This figure also shows that the proposed method is better than the method in Ref. 5.

In order to further confirm the efficiency of the proposed method, we perform a comparison with the second method in Ref. 6, which is better than the first method in Ref. 6 and based on the Hartley transform, jigsaw transform, and logistic map. For different values of δ, the LMSE obtained by the proposed method using $\{z_0' = z_0 + \delta, z_1' = z_1 + \delta\}$ is plotted in Fig. 15 and compared with the corresponding LMSE obtained by the method reported in Ref. 6 for which $\{x_0' = x_0 + \delta, \}$, where x_0 is the seed value of chaotic random intensity mask generated by the logistic map. Figure 15 shows clearly the superiority of the proposed method.

4.3 *Key Space Analysis*

As mentioned in the previous section, the secret key of the proposed encryption method is constituted of the parameters of the four PLCM chaotic maps and the four

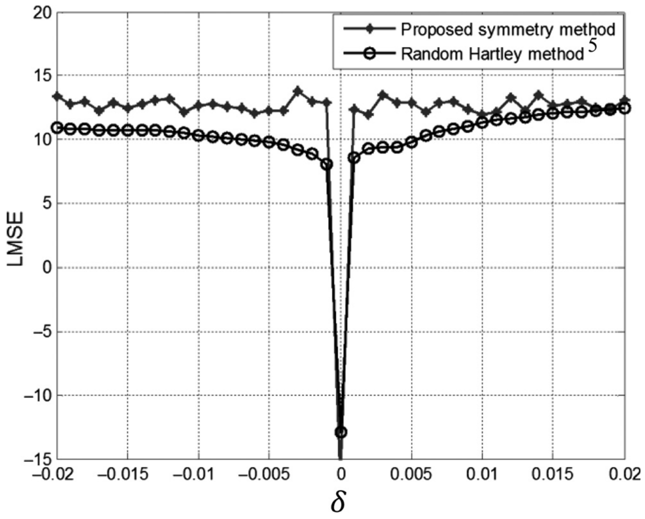


Fig. 14 LMSE in terms of the deviation error δ for γ and ζ' (proposed method) and for s_2' and s_3' (method in Ref. 5).

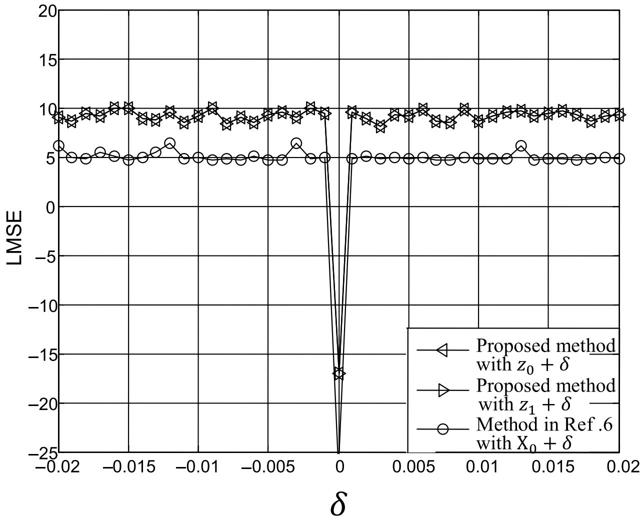


Fig. 15 LMSE in terms of the deviation error δ for z_0 and z_1 (proposed method) and for the seed value of the chaotic random intensity mask (method proposed in Ref. 6).

parameters of the parametric Fourier transforms, i.e., $\{z_0, \lambda_0, z_1, \lambda_1, z_2, \lambda_2, z_3, \lambda_3, \alpha, \beta, \gamma, \zeta\}$. According to the results presented in Fig. 9, each of the parameters of the PLCM chaotic maps have a sensitivity of 10^{-16}, so its precision is 10^{+16}. On the other hand, as shown in Figs. 13 and 14, the precision of the parameters α, β, γ, and ζ is evaluated approximately by $\frac{1}{\Delta d_1} = \frac{1}{0.4\times 0.005} \cong 2^8$. Therefore, the key space is approximatively equal to $10^{16\times 8} \times 4 \times 2^8 \cong 2^{435}$, which is greater than 2^{100} reclaimed for a cryptosystem.[21]

5 Conclusion

In this paper, we have proposed a double random amplitude encryption method based on the parametric DFT coupled with chaotic maps. The main idea behind this method is the introduction of a complex-to-real conversion by exploiting the symmetry property of the transform in the case of real-valued sequences. This conversion allows the encrypted image to be real-valued instead of being a complex-valued image as in all existing double random phase encryption methods. The advantage is to store or transmit only one image instead of two images (real and imaginary parts). Computer simulation results demonstrate that the proposed method outperforms the existing double random amplitude encryption methods.

References

1. R. F. Sewell, “Bulk encryption algorithm for use with RSA,” *Electron. Lett.* **29**(25), 2183–2185 (1993).
2. P. Refregier et al., “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.* **20**(7), 767–769 (1995).
3. H. Huang et al., “Colour image encryption based on logistic mapping and double random-phase encoding,” *IET Imaging Process.* **11**(4), 211–216 (2017).
4. L. Chen et al., “Optical image encryption with Hartley transforms,” *Opt. Lett.* **31**(23), 3438–3440 (2006).
5. Z. Liu et al., “Image encryption based on double random coding in random Hartley transform domain,” *Optik* **121**, 959–964 (2010).
6. N. Singh et al., “Optical image encryption using Hartley transform and logistic map,” *Opt. Commun.* **282**, 1104–1109 (2009).
7. H. E. Huang, “An optical image cryptosystem based on Hartley transform in the Fresnel transform domain,” *Opt. Commun.* **284**, 3243–3247 (2011).
8. K. K. Kesavan et al., “Optical color image encryption based on Hartley transform and double random phase encoding system,” in *3rd Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Budapest, Hungary, pp. 1–3 (2011).
9. G. Unnikrishnan et al., “Double random fractional-Fourier domain encoding for optical security,” *Opt. Eng.* **39**(11), 2853–2859 (2000).
10. R. Tao et al., “The multiple-parameter discrete fractional Hadamard transform,” *Opt. Commun.* **282**, 1531–1535 (2009).
11. C. C. Tseng et al., “Eigen values and eigenvectors generalized DHT, DCT-IV and DST-IV matrices,” *IEEE Trans. Signal Process.* **50**, 866–877 (2002).
12. S. C. Pei et al., “The multiple-parameter discrete fractional Fourier transform,” *IEEE Signal Process. Lett.* **13**(6), 329–332 (2006).
13. J. M. Vilardy et al., “Digital images phase encryption using fractional Fourier transform,” in *Electronics, Robotics and Automotive Mechanics Conf.*, Morelos, Mexico, Vol. 1, pp. 15–18 (2006).
14. L. Sui et al., “Double-image encryption using discrete fractional random transform and logistic maps,” *Opt. Lasers Eng.* **56**, 1–12 (2014).
15. S. Bouguezel et al., “Image encryption using the reciprocal-orthogonal parametric transform,” in *IEEE Int. Symp. on Circuits and Systems*, Paris, France, pp. 2542–2545 (2010).
16. S. Bouguezel et al., “A new class of reciprocal-orthogonal parametric transforms,” *IEEE Trans. Circuits Syst.* **56**(4), 795–805 (2009).
17. S. Bouguezel, “A reciprocal-orthogonal parametric transform and its fast algorithm,” *IEEE Signal Process. Lett.* **19**, 769–772 (2012).
18. S. Bouguezel, M. O. Ahmad, and M. N. S. Swamy, “A new involutory parametric transform and its application to image encryption,” in *IEEE Int. Symp. on Circuits and System (ISCAS)*, pp. 2605–2608 (2013).
19. S. Bouguezel et al., “New parametric discrete Fourier and Hartley transforms, and algorithms for fast computation,” *IEEE Trans. Circuits Syst.* **58**(3), 562–575 (2011).
20. H. Zhou et al., “Problems with the chaotic inverse system encryption approach,” *IEEE Trans. Circuits Syst.* **44**, 268–271 (1997).
21. G. Alvarez et al., “Some basic cryptographic requirements for chaos-based cryptosystems,” *Int. J. Bifurcation Chaos* **16**(8), 2129–2151 (2006).

Toufik Bekkouche received his magister degree in electronics (communication engineering) from University Ferhat Abbas Setif 1, Setif, Algeria, in 2009. He is currently pursuing his PhD degree in image encryption at the Department of Electronics, University Ferhat Abbas Setif 1, Setif, Algeria. Since 2013, he has been an assistant professor at the University of Bordj-Bouarreridj, Algeria. His research interests include digital image processing, watermarking, encryption, and compression.

Saad Bouguezel received his PhD in electrical engineering from Concordia University, Montreal, Quebec, Canada, in 2004. From March 2002 to June 2006, he worked at Concordia University as a research and teaching assistant and as a postdoctoral fellow. In 2006, he joined the Department of Electronics at University Setif 1, Algeria, where he is currently a professor. His research interests include discrete transforms and techniques for signal and image processing, compression, encryption, and watermarking.