Fractional convolution and nonlinear operations applied to the image encryption

Juan M. Vilardy¹, Cesar O. Torres¹, and Carlos Jimenez²

¹Grupo de óptica e informática. Department of electronic engineering. Universidad Popular del Cesar, Valledupar (Cesar), Colombia
²Grupo GIFES. Faculty of engineering. Universidad de La Guajira, Riohacha (La Guajira), Colombia
E-mail: vilardy.juan@unicesar.edu.co

Abstract. We use the fractional convolution, nonlinear operations and random phase masks (RPMs) in order to encrypt images. The definition used in this paper of the fractional convolution is based on the fractional Fourier transform (FrFT). The amplitude and phase truncation are nonlinear operations that allow to select a specific information of a complex-valued image. The encryption and decryption systems are based on the double random phase encoding (DRPE). At the beginning of the encryption process, the image to encrypt is encoded in phase. The rest of the encryption and decryption process use two RPMs, the fractional convolution and the amplitude and phase truncation operations in a sequential way in order to get the encrypted and decrypted image. The amplitude and phase truncation and the phase encoding are nonlinear operations that improving the security of the encrypted image, because the obtained key space of the proposed encryption process is very larger. The fractional order of the FrFT introduces a new key for the security system and the encrypted image of the proposed encryption system is a real-valued image. The encryption-decryption system has five security keys. All these five keys with their correct values are necessary in the decryption process with the purpose of obtaining the original image that was encrypted in the encryption process.

1. Introduction
In the last two decade, the information processing using optical systems have shown a great potential for the field of the optical security [1, 2]. Several important techniques of optical encryption have been proposed with the purpose of taking advantage of the security, high speed parallel data processing and the physical parameters selection allowed by the optical processing system. The double random phase encoding (DRPE) is a technique for optical image encryption that uses two random phase masks (RPMs) with the purpose of encoding the image to encrypt (original image) into a stationary white noise pattern (encrypted image) [3]. The optical DRPE can be implemented using a processor 4f [4] or a joint transform correlator [5, 6]. The optical image encryption systems based on the initial DRPE are vulnerable to security attacks, this weakness is due to the linear property of the DRPE technique [6, 7]. The DRPE has been further extended from the Fourier domain to the Fresnel domain [8–10], the fractional Fourier domain (FrFD) [11–18] and the Gyrator domain [19–21], with the purpose of adding more keys and increasing the security of the DRPE system.

We present a nonlinear image encryption-decryption system based on the DRPE, random phase masks (RPMs), phase encoding, the fractional convolution and truncation operations. The RPMs
have random images which are used as keys of the encryption system. The fractional convolution improves the security of the original DRPE by adding a new key for the encryption system given by the the fractional order of the FrFT. The original image is encoding in phase because this encoding allows a better protection of the encrypted image against security attacks [12,13,19,22]. The amplitude and phase truncations operations are nonlinear [23] and we use these operations in order to make the encryption-decryption system becomes nonlinear, generate two new security keys and improve the security of the encrypted image.

The rest of the paper is organized as follows. The definition of the fractional Fourier transform and the fractional convolution are presented in section 2. The amplitude and phase truncation operations are introduced in section 3. The formulation of the encryption-decryption processes are described in section 4. In section 5 are presented the computer simulations of the encryption and decryption systems. Finally, the main ideas of the paper are summarized in section 6.

2. The Fractional Fourier transform and the fractional convolution

2.1. The Fractional Fourier transform (FrFT)

The fractional Fourier transform (FrFT) of order \( \alpha \), is a linear integral operator that maps a given function \( f(x) \) onto function \( f_\alpha(u) \), by [17,18]

\[
f_\alpha(u) = \mathcal{F}_\alpha \{ f(x) \} = \int_{-\infty}^{+\infty} f(x) K_\alpha(u,x) dx,
\]

\[
K_\alpha(u,x) = C_\alpha \exp \left\{ -i\pi \left[ (u^2 + x^2) \cot \alpha - 2ux \csc \alpha \right] \right\},
\]

\[
C_\alpha = \frac{\exp \left\{ i\frac{\pi}{2} \text{sgn}(\alpha) - \frac{\alpha}{2} \right\}}{\sqrt{|\sin \alpha|}}, \quad -\pi < \alpha \leq \pi, \quad \alpha = \frac{p\pi}{2}, \quad -2 < p \leq 2,
\]

(1)

where \( K_\alpha \) is the fractional Fourier kernel and \( \text{sgn} \) is the sign function. For \( \alpha = 0 \) (\( p = 0 \)), it corresponds to the identity transform. For \( \alpha = \pi/2 \) (\( p = 1 \)), it reduces to the Fourier transform. For \( \alpha = \pi \) (\( p = 2 \)), the reverse transform is obtained. For \( \alpha = -\pi/2 \) (\( p = -1 \)), it corresponds to the inverse Fourier transform. The inverse FrFT corresponds to the FrFT at fractional order \(-\alpha\). The FrFT operator is additive with respect to the fractional order, \( \mathcal{F}_\alpha \mathcal{F}_\beta = \mathcal{F}_{\alpha+\beta} \).

2.2. The fractional convolution

The definition of the fractional convolution that it will be used in the encryption-decryption systems of the next sections was proposed in [18]. The fractional convolution is given by

\[
f(x) *_\alpha g(x) = \int_{-\infty}^{+\infty} f(z)g(x-z) \exp \left\{ i2\pi z(x-z) \cot \alpha \right\} dz.
\]

(2)

Using the FrFTs \( \mathcal{F}_\alpha \{ f(x) \} = f_\alpha(u) \) and \( \mathcal{F}_\alpha \{ g(x) \} = g_\alpha(u) \), the previous equation can be expressed as

\[
f(x) *_\alpha g(x) = \mathcal{F}^{-\alpha} \left\{ f_\alpha(u)g_\alpha(u) \exp \left\{ i\pi u^2 \cot \alpha \right\} \right\}.
\]

(3)

3. Amplitude and phase truncation operations

The amplitude and phase truncations are nonlinear operations that can be applied to a complex-valued image [23]. Let \( f(x) = a(x) \exp \{i2\pi \phi(x)\} \) be a complex-valued function, where \( a(x) \) and \( \phi(x) \) represent the amplitude and the phase of the function \( f(x) \), respectively.
The amplitude truncation (AT) allows to select the phase function \( \phi(x) \) from the complex-valued function \( f(x) \). Therefore, the result of the AT when is applied to the complex-valued function \( f(x) \) is

\[
AT\{f(x)\} = AT\{a(x)\exp\{i2\pi\phi(x)\}\} = \phi(x).
\]

(4)

The phase truncation (PT) allows to select the amplitude function \( a(x) \) from the complex-valued function \( f(x) \). When the PT is applied to the complex-valued function \( f(x) \), we obtain

\[
PT\{f(x)\} = PT\{a(x)\exp\{i2\pi\phi(x)\}\} = a(x).
\]

(5)

Using the AT and PT operations, the complex-valued function \( f(x) \) can be expressed as

\[
f(x) = PT\{f(x)\}\exp\{i2\pi AT\{f(x)\}\}.
\]

(6)

4. Nonlinear Image encryption and decryption processes using the fractional convolution and nonlinear operations

4.1. Encryption process

We describe the mathematical formulation of the encryption process in this section. Let \( f(x) \) be the real-valued image to encrypt (original image) with values in the interval \([0, 1]\), and let \( r(x) \) and \( h(u) \) be two random phase masks (RPMs) given by

\[
r(x) = \exp\{i2\pi s(x)\}, \quad h(u) = \exp\{i2\pi n(u)\},
\]

(7)

where \( x \) and \( u \) represent the coordinates for the spatial domain and the FrFD, respectively, \( s(x) \) and \( n(u) \) are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval \([0, 1]\) [3,11]. The original image \( f(x) \) is encoded in phase \( f_{ph}(x) = \exp\{i2\pi f(x)\} \) [22]. Then, the image \( f_{ph}(x) \) is multiplied by the RPM \( r(x) \) and the previous product is transformed using the FrFT at parameter \( \alpha \)

\[
g_{\alpha}(u) = \mathcal{F}^{\alpha}\{r(x)f_{ph}(x)\} = q_{\alpha}(u)\exp\{i2\pi\phi_{\alpha}(u)\},
\]

(8)

where the real-valued functions \( q_{\alpha}(u) \) and \( \phi_{\alpha}(u) \) represent the amplitude and the phase of the complex-valued image \( g_{\alpha}(u) \), respectively. The functions \( q_{\alpha}(u) \) and \( \phi_{\alpha}(u) \) are dependent on the values of the RPM \( r(x) \), the fractional order \( \alpha \) introduced by using the FrFT and the encoded image in phase \( f_{ph}(x) \). We apply the amplitude and phase truncation operations to the complex-valued image \( g_{\alpha}(u) \) to obtain

\[
q_{\alpha}(u) = PT\{g_{\alpha}(u)\}, \quad \phi_{\alpha}(u) = AT\{g_{\alpha}(u)\}.
\]

(9)

The image \( q_{\alpha}(u) \) is multiplied by the RPM \( h(u) \) and the pure phase factor \( \exp\{i\pi u^2 \cot \alpha\} \). This product is transformed using the FrFT at parameter \(-\alpha\)

\[
q(x) *_{\alpha} h(x) = \mathcal{F}^{-\alpha}\{q_{\alpha}(u)h(u)\exp\{i\pi u^2 \cot \alpha\}\} = t(x) = e(x)\exp\{i2\pi \theta(x)\},
\]

(10)

where the image \( t(x) \) is the fractional convolution between \( q(x) \) and \( h(x) \), and the images \( q(x) \) and \( h(x) \) correspond to the FrFTs at fractional order \(-\alpha\) of \( q_{\alpha}(u) \) and \( h(u) \), respectively. The functions \( e(x) \) and \( \theta(x,y) \) denote the amplitude and the phase of the complex-valued image \( t(x) \), respectively. Finally, we apply the amplitude and phase truncation operations over the complex-valued image \( t(x) \)

\[
e(x) = PT\{t(x)\}, \quad \theta(x) = AT\{t(x)\}.
\]

(11)

The encrypted image is given by the real-valued data distribution \( e(x) \). The five security keys of the encryption system are given by the two RPMs \( r(x) \) and \( h(u) \), the fractional order \( \alpha \) introduced by using the FrFT and the two pseudorandom images \( \phi_{\alpha}(u) \) and \( \theta(x) \).
4.2. Decryption process

In this section, the mathematical formulations of the decryption process is presented. The
decryption is the reverse process of the encryption process. The output image of the
decryption system is the decrypted image \( d(x) \). In the first step of the decryption process, we use the
encrypted image \( e(x) \), the pseudorandom image \( \theta(x) \), the fractional order \( \alpha \) and the RPM \( h^*(u) \)
in order to get the following image

\[
q_\alpha(u) = h^*(u) \exp \{-i\pi u^2 \cot \alpha\} \mathcal{F}^\alpha \{ e(x) \exp \{i 2\pi \theta(x) \} \}.
\]

(12)

The previous equation is the inverse of the Eq. (10) with the purpose of getting the real-valued
image \( q_\alpha(u) \). For the second step of the decryption process, the intermediate image \( f_{ph}(x) \)
is obtained when the image \( q_\alpha(u) \), the RPM \( r^*(x) \), the pseudorandom image \( \phi_\alpha(u) \) and the
fractional order \(-\alpha\) is used in the following equation

\[
f_{ph}(x) = r^*(x) \mathcal{F}^{-\alpha} \{ q_\alpha(u) \exp \{i 2\pi \phi_\alpha(u) \} \}.
\]

(13)

The previous equation is the inverse of the Eq. (8) with the purpose of obtaining the phase-only
distribution \( f_{ph}(x) \). In the last step of the decryption process, the amplitude truncation is applied
over the result of the Eq. (13) in order to obtain the decrypted image

\[
d(x) = AT \{ f_{ph}(x) \} = f(x).
\]

(14)

The two pseudorandom images \( \phi_\alpha(u) \) and \( \theta(x) \), the two RPMs \( r(x) \) and \( h(u) \), and the
fractional order \( \alpha \) were used as security keys in the Eqs. (12) and (13). If these previous values
of the five security keys used in the decryption process are equal to the values corresponding to
the five security keys used in the encryption process, the decrypted image \( d(x) \) is a replica of the
original image \( f(x) \). Therefore, it is necessary provide the proper values of the five security keys,
in order to retrieve the original image \( f(x) \) at the output of the decryption process.

5. Computer simulations

The numerical simulations of the encryption and decryption processes following the steps described
in section 4 are shown in figure 1. The images used in the encryption and decryption systems
have \( 512 \times 512 \) pixels in grayscale. The original image \( f(x) \) and the random distribution code
\( n(u) \) of the RPM \( h(u) \) are shown in figures 1(a) and 1(b), respectively. The random distribution
code \( s(x) \) of RPM \( r(x) \) has different values but the same appearance of the image presented in
figure 1(b). The fractional order of the FrFT used in the encryption system is equal to
\( \alpha = 0.3471\pi \).

The two resulting pseudorandom images \( \phi_\alpha(u) \) and \( \theta(x) \) in the encryption process, are
presented in figures 1(c) and 1(d), respectively. These real-valued images have a noisy appearance
very similar to the random code \( s(x) \) of figure 1(b), but the two images \( \phi_\alpha(u) \) and \( \theta(x) \) are pseudorandom data distributions because these images are dependent on the values of the
fractional order \( \alpha \), image \( f_{ph}(x) \) and the RPMs \( r(x) \) and \( h(u) \), used in Eqs. (7)–(10).

The real-valued encrypted image \( e(x) \) for the fractional order \( \alpha = 0.3471\pi \) of the FrFT is
presented in figure 1(e). This encrypted image is a noisy data function which does not reveal
any information of the original image \( f(x) \). If the decryption process is performed along with
the encrypted image \( e(x) \) and the proper values of the five security keys (the fractional order \( \alpha \),
the two RPMs \( r(x) \) and \( h(u) \) and the two pseudorandom images \( \phi_\alpha(u) \) and \( \theta(x) \)), the original
image \( f(x) \) will be recovered at the output of the decryption process. The decrypted image \( d(x) \)
obtained from the encrypted image \( e(x) \) and the true values of the five security keys is displayed in
figure 1(f).
In order to evaluate the quality of the decrypted images, we use the root mean square error (RMSE) between the decrypted images \(d(x)\) and the original image \(f(x)\) [6] 

\[
RMSE = \left( \frac{\sum_{x=1}^{M} [f(x) - d(x)]^2}{\sum_{x=1}^{M} [f(x)]^2} \right)^{\frac{1}{2}}.
\] (15)

The values of the RMSE metric for evaluating image quality are between 0 and 1; when the value of the RMSE is close or equal to 0, this metric indicates an excellent quality image for the retrieval of the decrypted image at the output of the decryption system whereas the values of the RMSE close or equal to 1 represent a worse quality image. The RMSE between the original image of figure 1(a) and the decrypted image of figure 1(f) is \(3.21 \times 10^{-7}\).

The resulting decrypted images from the encrypted image of figure 1(e) using an incorrect pseudorandom image \(\phi_\alpha(u)\) or a wrong RPM \(r(x)\), are shown in figures 1(g) and 1(h), respectively. The RMSEs between the original image of figure 1(a) and the decrypted images of figures 1(g) and 1(h) are 0.91 and 0.85, respectively. If the values of the fractional order \(\alpha\) of the FrFT, the RPM \(h(u)\) or the pseudorandom image \(\theta(x)\) used in the decryption process are not equal to the values used in the encryption process, the decrypted image will be a noisy distribution very similar to the figure 1(g). The correct retrieval of the original image is possible only when all the five security keys with their correct values are provided in the decryption process.

The key space analysis for the proposed encryption system consists of every possible combination of the security keys: the fractional order \(\alpha\) of the FrFT, the two RPMs \(r(x)\) and \(h(u)\), and the two pseudorandom images \(\phi_\alpha(u)\) and \(\theta(x)\). From computational experiments it was found that the fractional order \(\alpha\) is sensitive to a variation of \(1 \times 10^{-5}\). Therefore, the key space for the fractional order of the FrFT is \(2\pi \times 10^5\). The two RPMs \(r(x)\) and \(h(u)\), and the two pseudorandom images \(\phi_\alpha(u)\) and \(\theta(x)\) have a size of \(512 \times 512\) pixels and each pixel has 256 possible values. The number of attempts required to retrieve both RPMs and pseudorandom

![Figure 1](image-url)

**Figure 1.** (a) Original image to be encrypted \(f(x)\). (b) Random distribution code \(n(u)\) of the RPM \(h(u)\). Pseudorandom images for the fractional order \(\alpha = 0.3471\pi\): (c) \(\phi_\alpha(u)\), and (d) \(\theta(x)\). (e) Encrypted image \(e(x)\) for the fractional order \(\alpha = 0.3471\pi\) of the FrFT. (f) Decrypted image \(d(x)\) using the five correct security keys (\(\alpha\), \(r(x)\), \(h(u)\), \(\phi_\alpha(u)\) and \(\theta(x)\)). Decrypted images for the following incorrect security keys: (g) the pseudorandom image \(\phi_\alpha(u)\), and (h) the RPM \(r(x)\).
images is of the order of $2^{56(512)(512)}$. Therefore, the brute force attacks are intractable just considering every possibility of the two RPMs and the two pseudorandom images [7]. Finally, the key space of the proposed encryption process is $(2\pi \times 10^5) \cdot 256^{1048576}$, this number represents a very larger key space.

6. Conclusions

A nonlinear image encryption-decryption process has been proposed using the fractional convolution, nonlinear operations and RPMs. The use of the fractional convolution allowed the addition of a new key, which is the fractional order $\alpha$ introduced by using the FrFT. This fractional order improves the security of the proposed encryption process in comparison to those security systems based on the Fourier transform. The nonlinear operation given by the phase encoding and truncation operations improve the security of the encrypted image, because the RPM $r(x)$ becomes a security key and it were generated two security key represented by two pseudorandom images, respectively. An important advantage of the proposed encryption process is that the encrypted image is purely real and has the same size as the image (also purely real) to encrypt, this feature is much more convenient for the transmission or storage of the encrypted image. The security keys of the nonlinear encryption-decryption system are: the two pseudorandom images, the fractional order $\alpha$ of the FrFT and the two RPMs. The encrypted image is well-protected because the key space for the proposed encryption system is very larger. Finally, the numerical simulations have shown that the proposed security systems are more secure because the decrypted image is very sensitive to the changes introduced on the true five security keys.

Acknowledgments

This research has been funded by the Universidad Popular del Cesar and the Universidad de La Guajira.

References

[1] Javidi B, Carnicer A, Yamaguchi M, Nomura T, Pérez-Cabré E, Millán M, Nishchal N, and Torroba R, Barrera J, He W and others 2016 J. Opt. 18 083001
[2] Chen W, Javidi B and Chen X 2014 Adv. Opt. Photonics 6 12055
[3] Réfrégier P and Javidi B 1995 Opt. Lett. 20 767–9
[4] Goodman J W 1996 Introduction to Fourier Optics (Columbus: McGraw-Hill)
[5] Nomura T and Javidi B 2000 Opt. Eng. 39 2031–5
[6] Vilardy J, Millán M S and Pérez-Cabré E 2013 J. Opt. 15 025401
[7] Frauel Y, Castro A, Naughton T J and Javidi B 2007 Opt. Express 15 1025365
[8] Situ G and Zhang J 2004 Opt. Lett. 29 1584–6
[9] Vilardy J, Millán M S and Pérez-Cabré E 2014 Appl. Opt. 53, 1674–82
[10] Vilardy J, Millán M S and Pérez-Cabré E 2013 Proc. of SPIE 8785, 87853J
[11] Unnikrishnan G, Joseph J and Singh K 2000 Opt. Lett. 25 887–9
[12] Vilardy J, Torres C and Mattos L 2008 AIP Conf. Proc. 992 1067–72
[13] Vilardy J, Torres C and Mattos L 2008 Revista Colombiana de Física 40 143–6
[14] Vilardy J, Torres C and Mattos L 2011 Revista Colombiana de Física 43 523–7
[15] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 J. Opt. 16 125405
[16] Vilardy J, Millán M S and Pérez-Cabré E 2014 Opt. Pura y Apl. 47 35–41
[17] Ozaktas H M, Zalevsky Z and Kutay M A 2001 The Fractional Fourier Transform: with Applications in Optics and Signal Processing (Weinheim: Wiley)
[18] Torres R, Pellat-Finet P and Torres Y 2010 Signal Process. 90 1976-84
[19] Vilardy J, Millán M S and Pérez-Cabré E 2017 Opt. Laser Eng. 89 88-94
[20] Vilardy J, Jimenez C and Perez R 2017 J. Phys.: Conf. Ser. 850 012012
[21] Perez R, Vilardy J and Jimenez C 2017 J. Phys.: Conf. Ser. 850 012012
[22] Towghi N, Javidi B and Luo Z 1999 J. Opt. Soc. Am. A 16 1915-27
[23] Qin W and Peng X 2010 Opt. Lett. 35 118–20