Nonlinear encryption system based on the fractional Fourier operators and truncation operations

J M Vilardy\textsuperscript{1}, R Perez\textsuperscript{1}, and C Jimenez\textsuperscript{1}

\textsuperscript{1} Grupo de Investigación en Física de Estado Sólido, Universidad de La Guajira, Riohacha, Colombia

E-mail: jmvilardy@uniguajira.edu.co

Abstract. In this paper, the fractional Fourier operators, the random phase masks and the nonlinear operations of amplitude and phase truncations are utilized to encrypt and decrypt images. We use the following fractional Fourier operators in the image encryption-decryption system: the fractional Fourier transform, the fractional translation and the fractional correlation. The proposed encryption system uses nonlinear operations, such as phase encoding and truncation operations, in order to increase the security of the encrypted image. The encryption-decryption system has the following security keys: one fractional order of the fractional Fourier transform, two random phase masks and two pseudorandom code images. When all the proper security keys are used in the decryption system, the obtained decrypted image is a replica of the image to encrypt.

1. Introduction
Optical image security systems have been getting a lot of attention in recent years, because the fact that optical information technologies offer high speed parallel data processing, parameter selection and high level security [1]. The double random phase encoding (DRPE) is a well-known optical technique for image encryption [2], the DRPE encodes an amplitude image into a stationary white noise pattern (encrypted image) by using two random phase masks (RPMs) [3]. The DRPE was extended from the Fourier domain to the Fresnel domain [4–6] and the fractional Fourier domain (FrFD) [7–13], in order to increase the security of the DRPE system.

In this paper, we propose a nonlinear image encryption-decryption system based on the DRPE, the fractional Fourier operators (FrFOs), phase encoding, RPMs and truncation operations. The image to encrypt is encoding in phase with the purpose of getting an increase of security over the encrypted image. We use the following FrFOs: the fractional Fourier transform (FrFT), the fractional traslation and the fractional correlation to improve the security of the original DRPE by adding a new key for the encryption system (the fractional order of the FrFT). We use the amplitude and phase truncations in order to introduce nonlinear operations in the encryption-decryption system [14].

2. The fractional Fourier operators (FrFOs)
The FrFT of order $\alpha$, is a linear integral operator that maps a given function $f(x)$ onto function $f_{\alpha}(u) = \mathcal{F}^{\alpha}\{f(x)\}$. The definition and the properties of the FrFT operator ($\mathcal{F}^{\alpha}$) are defined in the following references [12,13].
2.1. The fractional translation operator

We use the fractional translation operator of order fractional $\alpha$ and real value $\tau$ given by the Equation (1) [13].

$$\mathcal{F}_{\tau;\alpha} f(x) = f(x - \tau) \exp\left\{ i2\pi\tau \left( x - \frac{\tau}{2} \right) \cot \alpha \right\}$$  \hspace{1cm} (1)

The FrFT at fractional order $\alpha$ of Equation (1) is presented in Equation (2).

$$\mathcal{F}^{\alpha} \{ \mathcal{F}_{\tau;\alpha} f(x) \} = f_\alpha(u) \exp \{ i2\pi\tau u \csc \alpha \} \hspace{1cm} (2)$$

2.2. The fractional correlation operator

The fractional correlation operator is given by the Equation (3) [13].

$$f(x) \circlearrowleft_{\alpha} g(x) = \int_{-\infty}^{+\infty} f(z)g^*(z - x) \exp \{ -i2\pi x(z - x) \cot \alpha \} \, dz \hspace{1cm} (3)$$

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 the Equation (4).

$$f(x) \circlearrowleft_{\alpha} g(x) = \mathcal{F}^{-\alpha} \left[ f_\alpha(u)g^*_\alpha(u) \exp \{ -i\pi u^2 \cot \alpha \} \right] \hspace{1cm} (4)$$

3. Amplitude and phase truncation operations

The amplitude and phase truncations are nonlinear operations that can be applied to a complex-valued image. Let $f(x) = a(x)e^{i2\pi\phi(x)}$ be a complex-valued function, the amplitude truncation (AT) and the phase truncation (PT) are defined using the Equation (5) [14].

$$\text{AT}\{f(x)\} = \text{AT}\left\{ a(x)e^{i2\pi\phi(x)} \right\} = \phi(x), \hspace{0.5cm} \text{PT}\{f(x)\} = \text{PT}\left\{ a(x)e^{i2\pi\phi(x)} \right\} = a(x) \hspace{1cm} (5)$$

4. Nonlinear image encryption and decryption

4.1. Encryption stage

Let $f(x)$ be the real-valued image to encrypt with values in the interval $[0, 1]$, and let $r(x)$ and $h_\alpha(u)$ be two random phase masks (RPMs) given by $r(x) = \exp\{i2\pi s(x)\}$ and $h_\alpha(u) = \exp\{i2\pi n(u)\}$, respectively, 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 $[0, 1]$. The image $f(x)$ is encoded in phase $f_{ph}(x) = \exp\{i2\pi f(x)\}$ [16]. Then, the image $f_{ph}(x)$ is multiplied by the RPM $r(x)$ and this product is shifted to $x = a$ using the fractional traslation at fractional order $\alpha$. The previous distribution is transformed using the FrFT at parameter $\alpha$ and the result is described in Equation (6).

$$g_\alpha(u) = \mathcal{F}^{\alpha}\{ \mathcal{F}_{\tau;\alpha} [r(x)f_{ph}(x)] \} = q_\alpha(u) \exp\{i2\pi\phi_\alpha(u)\}, \hspace{1cm} (6)$$

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 FrFOs (the fractional traslation and the FrFT operators) and the encoded image in phase $f_{ph}(x)$. Using the amplitude and phase truncation operations, we obtain $q_{\alpha}(u) = PT\{g_{\alpha}(u)\}$ and $\phi_{\alpha}(u) = AT\{g_{\alpha}(u)\}$.

The image $q_{\alpha}(u)$ is multiplied by the complex conjugated of the RPM $h_{\alpha}(u)$ and the phase factor $\exp\{-i\pi u^2 \cot \alpha\}$. This product is transformed using the FrFT at parameter $-\alpha$ and the resulting distributions are presented in Equation (7).

$$q(x) \circledast_{\alpha} h(x) = \mathcal{F}^{-\alpha}\{q_{\alpha}(u)h_{\alpha}^*(u)\exp\{-i\pi u^2 \cot \alpha\}\} = t(x) = e(x)\exp\{i2\pi \theta(x)\}, \tag{7}$$

where the images $q(x)$ and $h(x)$ correspond to the FrFTs at fractional order $-\alpha$ of $q_{\alpha}(u)$ and $h_{\alpha}(u)$, respectively, and the image $t(x)$ is the fractional correlation between $q(x)$ and $h(x)$. The functions $e(x)$ and $\theta(x)$ denote the amplitude and the phase of the complex-valued image $t(x)$, respectively. Using the amplitude and phase truncation operations, we obtain $e(x) = PT\{t(x)\}$ and $\theta(x) = AT\{t(x)\}$. The encrypted image is given by the real-valued data distribution $e(x)$, this encrypted distribution is very convenient for either its transmission or storage. The five security keys of the encryption system are the fractional order $\alpha$ introduced by using the FrFOs, the two RPMs $r(x)$ and $h_{\alpha}(u)$ and the two pseudorandom images $\phi_{\alpha}(u)$ and $\theta(x)$.

The encrypted image $e(x)$ and the pseudorandom image $\theta(x)$ of Equation (7) are totally different with respect to the distributions obtained for the encrypted image and the last pseudorandom image of our former work [15], because the distributions presented in Equation (7) are defined in the FrFD using the fractional correlation between $q(x)$ and $h(x)$ functions, whereas that the distributions of the encrypted image and the last pseudorandom image in [15] are defined using the Gyrator transform for a determined rotation angle. The nonlinear image encryption presented in [15] is similar in some aspects to the security system described in this work, for instances both encryption systems use the DRPE, phase encoding, RPMs and truncation operations, but the resulting encrypted images and the pseudorandom images in both security systems are completely different.

4.2. Decryption stage

The decryption process is the same encryption process applied in the inverse sense on the encrypted image $e(x)$ along with the five security keys used in the encryption stage. The output image of the decryption system is the decrypted image $d(x)$, given by the Equation (8) and Equation (9).

$$q_{\alpha}(u) = h_{\alpha}(u)\exp\{i\pi u^2 \cot \alpha\}\mathcal{F}^{\alpha}\{e(x)\exp\{i2\pi \theta(x)\}\}, \tag{8}$$

$$f_{ph}(x) = r^*(x)\mathcal{F}_{-\alpha}{\mathcal{F}^{-\alpha}\{q_{\alpha}(u)\exp\{i2\pi \phi_{\alpha}(u)\}\}}, \quad d(x) = AT\{f_{ph}(x)\} = f(x) \tag{9}$$

The fractional order $\alpha$, the two RPMs $r(x)$ and $h_{\alpha}(u)$ and the two pseudorandom images $\phi_{\alpha}(u)$ and $\theta(x)$ were used as security keys in the Equation (8) and Equation (9). When the values of the all security keys used in the decryption stage are equal to the values corresponding to the all security keys used in the encryption stage, the decrypted image $d(x)$ will be equal to the image $f(x)$ to encrypt.

5. Numerical simulations

The images used for the numerical simulations of Figure 1 have $512 \times 512$ pixels in grayscale. The image $f(x)$ to encrypt and the random distribution code $s(x)$ of the RPM $r(x)$ are depicted in
Figure 1(a) and Figure 1(b), respectively. The random distribution code \( n(u) \) of RPM \( h_\alpha(u) \) has different values but the same appearance of the image presented in Figure 1(b). The fractional order of the FrFOs used in the encryption system is equal to \( \alpha = 0.4721\pi \).

The real-valued encrypted image \( e(x) \) for the fractional order \( \alpha = 0.4721\pi \) of the FrFOs is shown in Figure 1(c). The two obtained pseudorandom images \( \phi_\alpha(u) \) and \( \theta(x) \) in the encryption process, are depicted in Figure 1(d) and Figure 1(e), respectively. The real-valued images \( \phi_\alpha(u) \) and \( \theta(x) \) have a noisy appearance very similar to the random code \( s(x) \) of Figure 1(b), but these two images are pseudorandom because they are dependent on the values of the image \( f_{\phi h}(x) \), the fractional order \( \alpha \) and the RPMs \( r(x) \) and \( h_\alpha(u) \), used in Equation (6) and Equation (7). When the decryption process is computed using the encrypted image \( e(x) \) and the proper values of the security keys (the fractional order \( \alpha \), the two RPMs \( r(x) \) and \( h_\alpha(u) \) and the two pseudorandom images \( \phi_\alpha(u) \) and \( \theta(x) \)), the image \( d(x) \) recovered at the output of the decryption stage will be a replica of the image to encrypt \( f(x) \). The decrypted image \( d(x) \) obtained from the encrypted image \( e(x) \) and the true values of the all security keys is displayed in Figure 1(f). The resulting noisy decrypted images from the encrypted image of Figure 1(c) using a wrong RPM \( r(x) \) or an incorrect pseudorandom image \( \phi_\alpha(u) \), are depicted in Figure 1(g) and Figure 1(h), respectively.

![Figure 1](image1.png)

**Figure 1.** (a) Image to encrypt \( f(x) \). (b) Random distribution code \( s(x) \) of the RPM \( r(x) \). (c) Encrypted image \( e(x) \) for the fractional order \( \alpha = 0.4721\pi \) of the FrFOs. Pseudorandom images for the fractional order \( \alpha = 0.4721\pi \): (d) \( \phi_\alpha(u) \), and (e) \( \theta(x) \). (f) Decrypted image \( d(x) \) using the all correct security keys. Decrypted images for the following wrong security keys: (g) the RPM \( r(x) \), and (h) the pseudorandom image \( \phi_\alpha(u) \).

### 6. Conclusions

We have presented the nonlinear image encryption and decryption systems based on the FrFOs, phase encoding, RPMs and truncation operations. The encrypted image was a real image which can easily be stored or transmitted. It introduces an additional key, which is the fractional order introduced by using the FrFOs, that increases the security level of the proposed system. The nonlinear truncation operations improve the security of the encrypted image due to the generation of two security key, given by two pseudorandom images. The security keys of the encryption-decryption system are the fractional order of the FrFT, two RPMs and two pseudorandom images.
Acknowledgments
This research has been funded by the Universidad de La Guajira.

References
[1] Chen W, Javidi B and Chen X 2014 Adv. Opt. Photonics 6 120–155
[2] Réfrégier P and Javidi B 1995 Opt. Lett. 20 767–769
[3] Vilardy J, Millán M S and Pérez-Cabré E 2013 J. Opt. 15 025401
[4] Situ G and Zhang J 2004 Opt. Lett. 29 1584–1586
[5] Vilardy J, Millán M S and Pérez-Cabré E 2014 Appl. Opt. 53 1674–1682
[6] Vilardy J, Millán M S and Pérez-Cabré E 2013 Proc. of SPIE 8785 87853J
[7] Unnikrishnan G, Joseph J and Singh K 2000 Opt. Lett. 25 887–889
[8] Vilardy J, Torres C and Mattos L 2008 Revista Colombiana de Física 40 143–146
[9] Vilardy J, Torres C and Mattos L 2011 Revista Colombiana de Física 43 523–527
[10] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 J. Opt. 16 125405
[11] Vilardy J, Millán M S and Pérez-Cabré E 2014 Opt. Puray Apl. 47 35–41
[12] Ozaktas H M, Zalevsky Z and Kutay M A 2001 The Fractional Fourier Transform: With Applications in Optics and Signal Processing (Weinheim: Wiley)
[13] Torres R, Pellat-Finet P and Torres Y 2010 Signal Process. 90 1976-1984
[14] Qin W and Peng X 2010 Opt. Lett. 35 118–120
[15] Perez R, Vilardy J and Jimenez C 2017 J. Phys.: Conf. Ser. 792 012046 1–7
[16] Towghi N, Javidi B and Luo Z 1999 J. Opt. Soc. Am. A 16 1915-1927