A simplification of the fractional Hartley transform applied to image security system in phase

Carlos J. Jimenez, Juan M. Vilardy, Ronal Perez
Grupo GIFES. Faculty of engineering. Universidad de La Guajira, Riohacha (La Guajira), Colombia

E-mail: carlosj114@gmail.com, jmvilardy@uniguajira.edu.co

Abstract. In this work we develop a new encryption system for encoded image in phase using the fractional Hartley transform (FrHT), truncation operations and random phase masks (RPMs). We introduce a simplification of the FrHT with the purpose of computing this transform in an efficient and fast way. The security of the encryption system is increased by using nonlinear operations, such as the phase encoding and the truncation operations. The image to encrypt (original image) is encoded in phase and the truncation operations applied in the encryption-decryption system are the amplitude and phase truncations. The encrypted image is protected by six keys, which are the two fractional orders of the FrHTs, the two RPMs and the two pseudorandom code images generated by the amplitude and phase truncation operations. All these keys have to be correct for a proper recovery of the original image in the decryption system. We present digital results that confirm our approach.

1. Introduction
The image encryption techniques use some mathematical tools related to the signal processing, such as the Fourier, Fresnel, fractional Fourier, Hartley, Gyrator, radial Hilbert and Wavelet transforms, among other transforms, in order to encode the image to encrypt into a random noise [1-22]. There are image encryption systems based on the fractional Fourier transform (FrFT) [7-12] or the fractional Hartley transform (FrHT) [14, 15], these fractional transforms improve the security of the encryption systems due to the fractional orders of these transforms represent new additional keys [1]. The FrFT [23] and the FrHT [24] are generalizations of the Fourier and Hartley transforms, respectively, that adding a new degree of freedom given by the fractional order of these fractional transforms. The FrFT and the FrHT are used in applications related to the analysis and processing of signals and images.

The encryption system that encoding the image to encrypt (original image) in phase, was proposed in ref. [25]. This phase encoding is a nonlinear operation that increases the security of the security system in comparison with the encryption systems that encoding the original image in amplitude. In other works, the Hartley transform [13] and the FrHT [14, 15] have been used in encryption systems in order to obtain a real-valued encrypted image and increasing the security of the encryption systems, respectively. The amplitude and phase truncation operations can introduce nonlinear effects in the encryption systems, allowing improve the security of these encryption systems [26].

In this work, we propose an image encryption-decryption system using the FrHT, phase encoding, random phase masks (RPMs) and truncation operations. The original image is encoding in phase because this encoding allows a better protection of the encrypted image against security attacks [1, 8,
We introduce a simplification for the computation of the FrHT in order to perform this transform in an efficient and fast way. We use two fractional orders of the FrHTs as key of the security system. The RPMs have random images which are used as keys of the encryption system. The amplitude and phase truncation operations are nonlinear mathematical tools, these truncation operations allow to generate two new keys for the encryption-decryption system. Finally, the main aim of the proposed security system in this paper is to provide a digital images encryption-decryption system with a high security for the protection of the encrypted images.

The rest of the paper is organized as follows: the section 2 shows the definition of the FrHT and introduces a simplification for the computation of this transform. The amplitude and phase truncation operations are presented in section 3. The mathematical description and the numerical simulations of the image encryption and decryption systems are described in section 4. Finally, conclusions are summarized in section 5.

2. A simplification of the fractional Hartley transform

The fractional Hartley transform (FrHT) can be defined using the fractional Fourier transform (FrFT) [24]. The FrFT at order $p$, is a linear integral transformation that maps a given function $f(x)$ (written in one-dimensional for the sake of simplicity) onto a function $F_p(u)$, by [23]

$$F^p(u) = F^p \{ f(x) \} = \int_{-\infty}^{+\infty} K_p(u,x) f(x) dx,$$  

with

$$K_p(u,x) = C_p e^{i [u^2 + x^2 \cot \alpha - 2ux \csc \alpha]}, \quad C_p = \frac{e^{-i \frac{\pi}{4} \sgn(\alpha) - \frac{\pi}{2} }}{\sqrt{|\sin \alpha|}}, \quad \alpha = \frac{\pi}{2} p, \quad -\pi < \alpha < \pi,$$  

where $K_p$ is the fractional Fourier kernel and $\sgn$ is the sign function. For $p = 0$, it corresponds to the identity transform. For $p = 1$, it reduces to the direct standard Fourier transform. For $p = 2$, the reverse transform is obtained. For $p = -1$, it corresponds to the inverse standard Fourier transform. The inverse FrFT corresponds to the FrFT at fractional order $-p$. The FrFT operator is additive with respect to the fractional order, $F^{p_1} F^{p_2} = F^{p_1+p_2}$. The FrFT has a periodicity of 4 with respect to the fractional order $p$.

The FrHT at fractional order $p$ of a function $f(x)$ is defined as [24]

$$f_p(u) = \mathcal{H}^p \{ f(x) \} = \frac{1+e^{i\pi p/2}}{2} F^p(u) + \frac{1-e^{i\pi p/2}}{2} F^p(-u),$$  

where $\mathcal{H}^p$ is the fractional Hartley operator, $f_p(u)$ is the FrHT at fractional order $p$ of $f(x)$, $F^p(u)$ is the FrFT at fractional order $p$ of $f(x)$. Due to the FrHT can be defined in terms of the FrFT, the FrHT verifies all properties of FrFT [24]. When $p = 1$, the FrHT reduces to the conventional Hartley transform. The FrHT has a periodicity of 2 with respect to the fractional order $p$. The computation of the FrHT by using the Eq. (3) uses the computation of two FrFTs. We propose the following simplification of the FrHT with the purpose of computing this transform in an efficient and fast way

$$\mathcal{H}^p \{ f(x) \} = \frac{1+e^{i\pi p/2}}{2} F^p(u) + \frac{1-e^{i\pi p/2}}{2} F^p(-u) = \frac{1+e^{i\pi p/2}}{2} F^p \{ f(x) \} + \frac{1-e^{i\pi p/2}}{2} F^p \{ f(-x) \} = F^p \left\{ \frac{1+e^{i\pi p/2}}{2} f(x) + \frac{1-e^{i\pi p/2}}{2} f(-x) \right\}.$$  

Therefore, the computation of the FrHT by using the Eq. (4) uses the computation of only one FrFT. In this way, the computation of the FrHT is more efficient and faster in comparison to the computation of the FrHT used in refs. [14, 15].
3. Amplitude and phase truncation operations

The truncation operations are nonlinear mathematical tools that can be applied to a complex-valued image [26]. Let \( f(x) = a(x)\exp(i2\pi \varphi(x)) \) be a complex-valued function, where \( a(x) \) and \( \varphi(x) \) represent the amplitude and the phase of the function \( f(x) \), respectively. The amplitude \( a(x) \) is a positive real-valued function and the phase \( \varphi(x) \) is a real-valued function with positive and/or negative values.

The amplitude truncation (AT) allows to select the phase function \( \varphi(x) \) from the complex-valued function \( f(x) \). Therefore, the result of the AT when is applied to the complex-valued function \( f(x) \) is

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

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

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

The complex-valued function \( f(x) \) can be expressed in terms of the AT and PT operations as

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

4. Image encryption and decryption systems

Let \( g(x) \) be the real-valued image to encrypt (original image) with values in the interval \([0, 1]\), and let \( r(x) \) and \( t(u) \) be two random phase masks (RPMs) given by

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

where \( x \) and \( u \) represent the coordinates for the spatial domain and the fractional Hartley domain (FrHD), respectively. \( s(x) \) and \( n(u) \) are normalized positive functions randomly generated, statistically independent and uniformly distributed in the interval \([0, 1]\).

The image to encrypt \( g(x) \) is encoding in phase \( g_{ph}(x) = \exp\{i2\pi g(x)\} \) [1, 8, 9, 14, 17]. Then, the image \( g_{ph}(x) \) bonded to the RPM \( r(x) \) is transformed using the FrHT at order \( p1 \)

\[
h_{p1}(u) = H^{p1}\{g_{ph}(x)r(x)\} = q_{p1}(u)\exp\{i2\pi \varphi_{p1}(u)\}.
\]

The data distributions \( q_{p1}(u) \) and \( \varphi_{p1}(u) \) denote the amplitude and the phase of the complex-valued image \( h_{p1}(u) \), respectively. When the amplitude and phase truncation operations are applied to the image \( h_{p1}(u) \), we obtain the following functions

\[
q_{p1}(u) = PT\{h_{p1}(u)\}, \quad \varphi_{p1}(u) = AT\{h_{p1}(u)\}.
\]

The image \( q_{p1}(u) \) bonded to the RPM \( t(u) \) is transformed using the FrHT at order \( p2 \)

\[
s_{p2}(v) = H^{p2}\{q_{p2}(u)t(u)\} = e(v)\exp\{i2\pi \theta_{p2}(v)\},
\]

where the functions \( e(v) \) and \( \theta_{p2}(v) \) represent the amplitude and the phase of the complex-valued image \( s_{p2}(v) \), respectively. Finally, the amplitude and phase truncation operations are applied to \( s_{p2}(v) \)

\[
e(v) = PT\{s_{p2}(v)\}, \quad \theta_{p2}(v) = AT\{s_{p2}(v)\}.
\]

The real-valued data distribution \( e(v) \) is the encrypted image. The six key of the encryption system are given by the two fractional orders \((p1 \text{ and } p2)\) of the FrHTs, the two pseudorandom images \( \varphi_{p1}(u) \) and \( \theta_{p2}(v) \) and the two RPMs \( r(x) \) and \( t(u) \). The RPMs \( r(x) \) and \( t(u) \) are used to spread the information content of the original image \( g(x) \) onto the encrypted distribution \( e(v) \). The data distribution keys \( \varphi_{p1}(u) \) and \( \theta_{p2}(v) \) are generated by the amplitude truncation operations applied in the encryption system. The keys \( \varphi_{p1}(u) \) and \( \theta_{p2}(v) \) are not truly random because these images are dependent on the values of the image \( g_{ph}(x) \), the two fractional orders \((p1 \text{ and } p2)\) of the FrHTs and the RPMs \( r(x) \) and \( t(u) \), used in Eqs. (8)-(12).
The retrieval of the original image \( g(x) \) is possible at the output of the decryption system from the encrypted image \( e(v) \) when the correct values keys are used. The decrypted image \( d(x) \) can be obtained using the following equations

\[
q_{p_1}(u) = t'(u)H^{-p_2}\{e(v)\exp\{2\pi \theta_{p_2}(v)\}\},
\]

\[
g_{p_1}(x) = r'(x)H^{-p_1}\{q_{p_1}(u)\exp\{2\pi \phi_{p_1}(u)\}\},
\]

\[
d(x) = AT\{g_{p_1}(x)\} = g(x).
\]

The original image \( g(x) \) can be correctly recovered at the output of the decryption system whenever the values of the keys used in the encryption and decryption systems are the same.

Figure 1 shows an example to illustrate the simulation results obtained when we evaluate the proposed image encryption and decryption systems presented in this section. All image used in the numerical simulations have \( 512 \times 512 \) pixels in grayscale. The original image \( g(x) \) and the random distribution code \( n(u) \) of the RPM \( t(u) \) are depicted in figures 1(a) and 1(b), respectively. The real-valued encrypted image \( e(v) \) for the fractional orders \( p_1 = 1.77 \) and \( p_2 = 0.43 \) of the FrHTs is shown in figure 1(c). This encrypted image is a noisy data distribution which does not disclose any information of the original image \( g(x) \). The two obtained pseudorandom images \( \phi_{p_1}(u) \) and \( \theta_{p_2}(v) \) in the encryption process, are presented in figures 1(d) and 1(e), respectively. These images have a noisy appearance very similar to the random code \( n(u) \) of figure 1(b), but the two images \( \phi_{p_1}(u) \) and \( \theta_{p_2}(v) \) are pseudorandom data distributions. The obtained decrypted image \( d(x) \) from the encrypted image \( e(v) \) and using the correct security keys is shown in figure 1(f).

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 \( g(x) \) [3].
\[ \text{RMSE} = \left\{ \frac{\sum_{x=1}^{M} [g(x) - d(x)]^2}{\sum_{x=1}^{M} [g(x)]^2} \right\}^{\frac{1}{2}}. \]

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 \(7 \times 10^{-14}\).

The noisy decrypted images displayed in figures 1(g) and 1(h), correspond to the retrieved images in the decryption system when the key of the pseudorandom image \(\theta_{p2}(v)\) or the value of the fractional order \(p1\) are wrong, respectively. The RMSEs between the original image of figure 1(a) and the decrypted images of figures 1(g) and 1(h) are 0.88 and 0.87, respectively. If the values of the fractional order \(p2\) of the FrHT, the RPMs \(r(x)\) and \(t(u)\) or the pseudorandom image \(\varphi_{p1}(u)\) used in the decryption system are not equal to the values used in the encryption system, the decrypted image is a noisy pattern very similar to figure 1(g). Therefore, the provided result prove that all keys (the two fractional orders \(p1\) and \(p2\) of the FrHTs, the two pseudorandom images \(\varphi_{p1}(u)\) and \(\theta_{p2}(v)\) and the two RPMs \(r(x)\) and \(t(u)\)) are required in the decryption system for correct retrieval of the original image.

We recall that the FrHT has a periodicity of 2 with respect to its fractional order. We evaluate the sensitivity on the fractional orders of the FrHTs by introducing small errors in these and leaving fixed the other four security keys in the decryption system. The RMSE is used to measure the level of protection on the encrypted image. For this deviation test of the fractional orders on the correct values for the decryption process, it is introduced an small error that varies between \(-1 \times 10^{-3}\) and \(1 \times 10^{-3}\), then for each variation is calculated the RMSE, the results for \(p1\) and \(p2\) are presented in figure 2. From figure 2, it was found that the fractional orders of the FrHTs are sensitive to a variation of \(1 \times 10^{-4}\).

![Figure 2. Deviation test of the fractional orders on the correct values for the decryption process.](image)

Using the obtained sensitivity of the fractional orders \(p1\) and \(p2\), the key space for the fractional orders of the FrHTs is \(4 \times 10^8\). The two RPMs \(r(x, y)\) and \(h(x, y)\), and the two pseudorandom images \(\varphi_{p1}(u)\) and \(\theta_{p2}(v)\) have a size of 512x512 pixels and each pixel has 256 possible values. The number of attempts required to retrieve both RPMs and pseudorandom images is of the order of \(256^{4512(512)}\). The total key space of the proposed encryption process is \((4 \times 10^8) \times 256^{1048576}\), this value for the key space is greater than the results obtained in refs. [2-16].

From numerical simulation developed for this paper, the time computing for the digital FrHT by implementing the Eq. (4) is reduced by half in comparison to the time computing of the Eq. (3). Therefore, the proposed computation for the FrHT is faster and efficient in comparison to the computation presented in refs. [14, 15].

5. Conclusions
We have presented an image encryption system based on the phase encoding, the FrHTs, the RPMs and the amplitude and phase truncation operations. We have introduced a simplification in the computation of the FrHT, this simplification allowed the computation of the FrHT in a more efficient and faster way. The encrypted image is a real-valued random distribution which is very well protected against security attacks because the very larger key space of the proposed encryption-decryption system. The security of the encrypted image is due to the nonlinear operations applied in the encryption-decryption system, these nonlinear operation are the phase encoding and the amplitude and phase truncation operations. The results of the numerical simulations have been shown that the retrieval of the original image in the decryption system is very sensitive to the changes on the six keys of the proposed security system in this work. The two pseudorandom images keys change when the image to encrypt, the two RPMs or the two fractional orders of the FrHTs are modified. Finally, in order to retrieve the original image with a high quality and free of noise at the output of the decryption system, the values of the six keys used in the encryption and decryption systems have to be the same.

Acknowledgments
This research has been funded by the Universidad de La Guajira.

References
[1] Millán M S and Pérez-Cabré E 2011 Optical and Digital Image Processing: Fundamentals and Applications ed G Cristóbal, P Schelkens and H Thienpont (Weinheim: Wiley) chapter 33 pp 739–67
[2] Réfrégier P and Javidi B 1995 Opt. Lett. 20 767–9
[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 1584–6
[5] Vilardy J, Millán M S and Pérez-Cabré E 2014 Appl. Opt. 53, 1674–82
[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. 25 887–9
[8] Vilardy J, Torres C and Mattos L 2008 AIP Conf. Proc. 992 1067–72
[9] Vilardy J, Torres C and Mattos L 2008 Revista Colombiana de Física 40 143–6
[10] Vilardy J, Torres C and Mattos L 2011 Revista Colombiana de Física 43 523–7
[11] Vilardy J, Torres Y, Millán M S and Pérez-Cabré E 2014 J. Opt. 16 125405
[12] Vilardy J, Millán M S and Pérez-Cabré E 2014 Opt. Pura y Aplic. 47 35–41
[13] Chen L and Zhao D 2006 Opt. Lett. 31 3438–40
[14] Vilardy J, Torres C and Jimenez C 2013 Proc. of SPIE 8785 87851R
[15] Zhao D, Li X and Chen L 2008 Opt. Commun. 281 5326–9
[16] Rodrigo J A, Alieva T and Calvo M L 2007 Opt. Commun. 278 79–84
[17] Vilardy J, Millán M S and Pérez-Cabré E 2016 Nonlinear image encryption using a fully phase nonzero-order joint transform correlator in the Gyrator domain Opt. Laser Eng. (Preprint http://dx.doi.org/10.1016/j.optlaseng.2016.02.013)
[18] Vilardy J, Torres C and Mattos L 2013 Proc. of SPIE 8785 87851Q
[19] Vilardy J, Millán M S and Pérez-Cabré E 2015 Proc. 20th Symposium on Signal Processing, Images and Computer Vision (STSIVA) (Bogotá) vol 1 (Washington: IEEE) pp 1–6
[20] Morales Y, Díaz L and Torres C 2015 J. Phys.: Conf. Series 582 012063
[21] Vilardy J, Torres C, Useech J and Mattos L 2011 J. Phys.: Conf. Series 274 012047
[22] Vilardy J, Torres C, Useech J and Mattos L 2011 Revista Colombiana de Física 43 170–4
[23] Ozaktas H M, Zalevsky Z and Kutay M A 2001 The Fractional Fourier Transform: with Applications in Optics and Signal Processing (Weinheim: Wiley)
[24] Pei S C and Ding J J 2002 IEEE Trans. Signal Process. 50 1661–80
[25] Towghi N, Javidi B and Luo Z 1999 J. Opt. Soc. Am. A 16 1915–27
[26] Qin W and Peng X 2010 Opt. Lett. 35 118–20