Image encryption using the fractional wavelet transform

To cite this article: Juan M Vilardy et al 2011 J. Phys.: Conf. Ser. 274 012047

View the article online for updates and enhancements.

Related content
- Fractional Hartley transform applied to optical image encryption
  C Jimenez, C Torres and L Mattos
- Implementation of the 2-D Wavelet Transform into FPGA for Image
  M León, L Barba, L Vargas et al.
- Experimental color encryption in a joint transform correlator architecture
  Myrian Tebaldi, Sergi Horrillo, Elisabet Pérez-Cabrè et al.

Recent citations
- Image encryption using the Gyrorad transform and random phase masks generated by using chaos
  Juan M. Vilardy et al
- Nonlinear image encryption system using the Gyrorad transform and truncation operations
  Ronal Perez et al
- A simplification of the fractional Hartley transform applied to image security system in phase
  Carlos J. Jimenez et al
Image encryption using the fractional wavelet transform

Juan M Vilardy¹, J. Useche, C. O. Torres and L. Mattos
Laboratorio de Óptica e Informática, Universidad Popular del Cesar,
Sede balneario Hurtado, Valledupar, Cesar – Colombia

E-mail: vilardy.juan@unicesar.edu.co

Abstract. In this paper a technique for the coding of digital images is developed using Fractional Wavelet Transform (FWT) and random phase masks (RPMs). The digital image to encrypt is transformed with the FWT, after the coefficients resulting from the FWT (Approximation, Details: Horizontal, vertical and diagonal) are multiplied each one by different RPMs (statistically independent) and these latest results is applied an Inverse Wavelet Transform (IWT), obtaining the encrypted digital image. The decryption technique is the same encryption technique in reverse sense. This technique provides immediate advantages security compared to conventional techniques, in this technique the mother wavelet family and fractional orders associated with the FWT are additional keys that make access difficult to information to an unauthorized person (besides the RPMs used), thereby the level of encryption security is extraordinarily increased. In this work the mathematical support for the use of the FWT in the computational algorithm for the encryption is also developed.

1. Introduction
This paper presents an application for encoding digital images using Wavelet Transform but with its fractional version to include as additional keys the fractional orders in the encryption process, preserving the advantages of using the shift and scale parameters. The starting point of this research was in the previous work of digital images encryption made into the Optics and Informatics Laboratory from the University Popular of Cesar [1-4].

The results report on the investigation of digital images encryption via FWT is organized as follows: Section 2 and 3 are present the Wavelet transform and the FWT, respectively. The mathematical formulation of the encryption and decryption technique is described in Section 4, with the algorithms for the images encryption/decryption process. The results of the designed and implemented algorithm are shown in section 5. The analysis of the results obtained from digital algorithm proposed is discussed in Section 6. Finally, conclusions are drown in Section 7.

2. Wavelet transform
The Transform Wavelet \( W(a,b) \) expresses the signal \( f(x) \) in terms of an orthonormal basis formed by a mother wavelet family, defined as [5]:

\[
W(a,b) = \int_{-\infty}^{\infty} f(x) \frac{1}{\sqrt{a}} \psi^* \left( \frac{x-b}{a} \right) dx; \quad a > 0
\]  

¹ To whom any correspondence should be addressed.
In the equation (1), the parameter \( b \) corresponds to shift of the mother wavelet function, \( a \) is the scale parameter. The basis sets that which represents the function \( f(x) \) (mother wavelets), is constructed from a generating function or mother wavelet, to which it is changing the scale by a factor \( a \) and, while this is shifted in a quantity \( b \) [5].

3. Fractional wavelet transform

FWT of a function \( f(x) \) results from the Fractional Fourier Transform (FrFT) of \( f(x) \), and then Wavelet decomposition is applied to this result [6]. The expression mathematics for the FWT of a signal \( f(x) \) is thus the following:

\[
W^\alpha(a,b) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} B_a(x,x') f(x') \psi_{ab}^*(x) dx' dx
\]

\[
B_a(x,x') = \frac{e^{-\frac{\pi a \Phi}{4}}}{\left| \sin\Phi \right|^{\frac{1}{4}}} e^{\frac{1}{4} \left( \frac{1}{2} - i \frac{\Phi}{\tan\Phi} \right) \left( x^2 + x'^2 \right) - i \frac{x x'}{\sin\Phi}}
\]

\[
\Phi = \frac{\pi p}{2}
\]

Observing that \( \Phi \), when it’s defined as a real number only appears as argument of trigonometric functions in the equation (3); the definition (2) is periodic in \( p \), with period 4.

The Discrete Fractional Fourier Transform (DFrFT) used in this article is defined by Candan [7-8], which is in one-dimension:

\[
f_p[m] = \mathcal{F}^p(f[n]) = \sum_{n=0}^{N-1} \mathcal{F}^p[m,n]f[n]
\]

The kernel is:

\[
\mathcal{F}^p[m,n] = \sum_{k=0}^{N-1} u_k[m] e^{-\frac{i\pi kp}{2}} u_k[n]
\]

Where \( u_k[n] \) is the \( k \)th discrete Hermite-Gauss function and \( (N) = \!\! \text{mod} \!\! 2 \); this discrete transformation is also periodic in \( p \), with period 4.

4. Encryption and decryption technique

4.1. Encryption and Decryption Method, Mathematical Formulation

Let \( I(x,y) \) be a real image to be encrypted with \( M \times N \) pixels size (\( M \) and \( N \), number of rows and columns, respectively, in grayscale), the encryption process transforms this image with the DFrFT and Discrete Wavelet Transform (DWT), then RPM are applied and finally, one IWT is applied to obtain the encrypted image. The following equations describe the encryption process:

\[
\{ CA, DH, DV, DD \} = \text{DWT}_2 \{ F^{\alpha_x} \times I \times F^{\alpha_y}, \text{family} \}
\]

\[
\text{CAM} = CA \times \text{Mask1}; \; \text{DHM} = DH \times \text{Mask2}
\]

\[
\text{DVM} = DV \times \text{Mask3}; \; \text{DDM} = DD \times \text{Mask4}
\]

\[
I_E = \text{IDWDT}_2 \{ \text{CAM}, \text{DHM}, \text{DVM}, \text{DDM}, \text{family} \}
\]

\[
\text{Maskn} = \text{exp}[2\pi i r_n(x,y)]
\]

Where: \( I_E \) is the encrypted image, \( CA, DH, DV \) and \( DD \) are the matrices of approximation coefficients, horizontal, vertical and diagonal detail coefficients that result in applying the Wavelet transform of a given family in two-dimensions (DWT). \( \text{CAM}, \text{DHM}, \text{DVM} \) and \( \text{DDM} \) are the matrices \( CA, DH, DV \) and \( DD \) multiplied by the RPMs. \( F^{\alpha_x} \) and \( F^{\alpha_y} \) are the DFrFT in one-dimension with fractional orders: \( \alpha_x, \alpha_y \); finally \( r_n(x,y) \) is a matrix of random numbers with the right size to be multiplied by the corresponding \( CA, DH, DV \) and \( DD \) (\( n = 1, 2, 3, 4 \)).
For the decryption process is applied the encryption process in the inverse sense, ensuring that each operation produces the opposite effect in the sequence. The inverse FrFT has negative fractional order \((-\alpha)\) [7]. Thus, we have the following equations:

\[
\{CA', DHM', DV', DDM' \} = DWT_\alpha \{I_e, \text{family}' \} \\
CA' = CA' \times \text{inv}(\text{Mask1}) \\
DH' = DHM' \times \text{inv}(\text{Mask2}) \\
DV' = DV' \times \text{inv}(\text{Mask3}) \\
DD' = DDM' \times \text{inv}(\text{Mask4}) \\
I_e = F^{-\alpha} \times \{I DWT_\alpha \{CA', DH', DV', DD', \text{family}' \} \} \times F^{-\alpha}
\] (12) (13) (14) (15)

When the \text{family}' used in the decryption process is equal to the \text{family} used in the encryption process and, it is used the same fractional order \(\alpha\) in the directions \(x\) and \(y\), the decrypted image is the image that was encrypted, i.e. its recover the original image.

4.2. Encryption Digital Algorithm

For the implementation of the encryption and decryption digital algorithm, we used Matlab® v.7.4 programming platform, due to its great ease and their high performance in the matrixes manage (images). The block diagram of the digital image encryption process is shown in figure 1.

4.3. Decryption Digital Algorithm

The decryption process is the same encryption process, but in the inverse sense with the fractional orders of the DFRT negative, the inverse RPMs and the same mother wavelet family, in order to obtain the image that initially was encrypted.

5. Experimental results

When the encryption process with the original image of \(M \times N\) pixels size is done through the algorithm described in section 4.2, the encrypted image hides the totality of the information contained therein, as seen in figure 2.
When the decryption process is done with the keys correct (fractional orders, wavelet family and RPMs) is recover the original image with loses not visible to the human eye, as shown in figure 3.

If the keys used in the decryption process are not equal to the keys used in the encryption process, the original image will not be recovered. Figure 4 shows the image recovered when an error is introduced in the fractional orders, using 0.877 instead of 0.777 and it was used the same wavelet family.

From the previous figure it is observed that with small changes in the correct keys, appear much distortion in the recovered image. The decryption process is so sensitive to the fractional order $\alpha$ as the family wavelet used, this is seen in Figure 5 using the correct fractional orders 0.777 (the same used in the encryption process) and changes the wavelet family db4 by db2.
6. The analysis of the results

The Mean Square Error (MSE) and Signal-to-Noise Ratio (SNR) between the input image and our decrypted image are calculated to validate the reliability of this digital algorithm. The MSE can be defined by the difference of energy between the input and decrypted images, i.e:

$$MSE = \frac{1}{M \cdot N} \sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I_1(x,y)]^2$$  \hspace{1cm} (16)

The SNR is defined as:

$$SNR = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y)]^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I_1(x,y)]^2}$$  \hspace{1cm} (17)

Where $I(x,y)$ and $I_1(x,y)$ are the matrixes element of the input image and our decrypted image at the pixel $[x,y]$, respectively, and $M \cdot N$ is size of the image. The sensitivity on fractional orders of FWT are examined by introducing errors in these (individually) and leaving fixed the RPMs and the mother wavelet family. The MSE and SNR are used to measure the level of protection on encrypted images. In this Deviation test in fractional orders of the FWT on the correct values of the decryption process, its introduce an error that varies between -0.25 and 0.25, then for each variation is calculated MSE and the SNR, the results can be seen in figure 6. From computational experiments it was found that fractional orders are sensitive to a variation of $1 \times 10^{-4}$.

![Figure 6. Deviation test in fractional order (x-direction) of the FWT on the correct values in the decryption process: (a) MSE, (b) SNR.](image-url)
In the following test is checked tolerance to loss of information from the encrypted image when it is decrypted, for this test is performed occlusion of 25% and 50% of pixels on the encrypted image. The figure 7 shows the images occluded and corresponding recovered images. From this figure we can say that there is not correspondence of position between the pixels of the original image and the image to decrypt, because the matrix multiplication applied in the encryption and decryption process causes that the values of any part of the encrypted image intervene on the entire matrix of the recovered image.

![Occlusion pixels test on the encrypted image and its decrypted image obtained from encryption with FWT, respectively: (a) Occlusion of 25% from the encrypted image and decrypted image, (b) Occlusion of 50% from the encrypted image and decrypted image.](image)

Figure 7. Occlusion pixels test on the encrypted image and its decrypted image obtained from encryption with FWT, respectively: (a) Occlusion of 25% from the encrypted image and decrypted image, (b) Occlusion of 50% from the encrypted image and decrypted image.

For the analysis of key space of the implemented algorithm, we consider the universe of possibilities to introduce different values of the keys used to encrypt image. In our case, there are two fractional orders in the two-dimension (x and y), each one varies in a range of 0 to 4 with sensitive steps of $1 \times 10^{-4}$, the family of Wavelet transform and the RPMs.

7. Conclusions
A new scheme of digital images encryption using FWT has been proposed. For this encryption system was increased the level of security against brute force cracking by the large size of key space. The use FWT on digital images encryption increases a great deal the security parameters of the encrypted image, due to the sensitivity to any changes made on the fractional orders used (numeric key) and, in addition to this, the huge number of possibilities of using a wavelet family and several different RPMs, greatly increase the difficulty for anyone attempting to decrypt the image without being authorized.

8. References
[1] Vilardy J, Torres C, and Mattos L, 2009 Images Encryption via Discrete Fractional Fourier Transform and Jigsaw Transform. Case Study: Fingerprints, IEEE Int. Conf. on Ultra Modern Telecommunications - Workshop on Optical Networking Technologies and Data Security, ISBN: 9781-4244-3941-6/09.
[2] Vilardy J, Calderon J, Torres C, and Mattos L, 2006 The Digital Images Phase Encryption Using Fractional Fourier Transform, IEEE Int. Conf. Electronics, Robotics and Automotive Mechanics, ISBN: 0-7695-2569-5/06.
[3] Brito L, Torres C, 2003 Encriptamiento de imágenes digitales a color mediante transformada de Fourier, Revista Colombiana de Física, vol. 35, no.1.
[4] Brito L, Torres C, 2005 Empleo de tres llaves en la encriptación de imágenes digitales a color mediante transformada de Fourier, Proc. Symp. X Simposio de Tratamiento de Señales, Imágenes y Visión Artificial (Cali – Colombia), ed. School of electronic engineering (Universidad del Valle Press).
[5] Mallat S, 1999 *A Wavelet Tour of Signal Processing*, Ed Academic Press, San Diego, California, p. 3.

[6] Mendlovic D et al. 1997 *Fractional Wavelet Transform. Appl. optics*, vol. 36, no. 20.

[7] Bultheel A, Martínez H. 2004 *Computation of the Fractional Fourier Transform. Appl. and Comput. Harmonic Analysis*, vol. 16, 182-202.

[8] Candan C, 1998 *dFRT: The Discrete Fractional Fourier Transform, A Matlab Program*, http://www.ee.bilkent.edu.tr/~haldun/dFRT.m