Image encryption using the fractional wavelet transform

This content has been downloaded from IOPscience. Please scroll down to see the full text.
(http://iopscience.iop.org/1742-6596/274/1/012047)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 54.191.40.80
This content was downloaded on 01/09/2017 at 11:39

Please note that terms and conditions apply.

You may also be interested in:

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-Cabré et al.

Digital Correlation based on Wavelet Transform for Image Detection
L Barba, L Vargas, C Torres et al.

Sign Language Recognition System using Neural Network for Digital Hardware Implementation
Lorena P Vargas, Leiner Barba, C O Torres et al.

Phase alteration compensation in reflection digital holography
O Rincon, R Amezquita and F Monroy

Color multiplexing using directional holographic gratings and linear polarization
L I Lugo, A Rodríguez, G Ramírez et al.

Simple optical setup implementation for digital Fourier transform holography
G N de Oliveira, D M C Rodrigues and P A M dos Santos

Design and implementation of an algorithm for creating templates for the purpose of iris biometric authentication through the analysis of textures implemented on a FPGA
F J Giacometto, J M Vilardy, C O Torres 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]:

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

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:

$$W^a(a, b) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} B_a(x, x') f(x') \psi_{a, b}(x) dx' dx$$

$$B_a(x, x') = e^{-\frac{j \phi}{4}} e^{\frac{j \phi}{2}}$$

where:

$$\phi = \pi \frac{p}{2}$$

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:

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

The kernel is:

$$F^p[m, n] = \sum_{k=0}^{N} u_k[m] e^{-\frac{j \phi}{2}} u_k[n]$$

where $u_k[n]$ is the $k$th discrete Hermite-Gauss function and $(N) = N_{mod}{2}$; 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 MxN 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:

$$\{CA, DH, DV, DD\} = DWT_2 \{F^x \times I \times F^y, \text{family}\}$$

$$CAM = CA \times Mask1; \quad DHM = DH \times Mask2$$

$$DVM = DV \times Mask3; \quad DDM = DD \times Mask4$$

$$I_E = IDWT_2 \{CAM, DHM, DVM, DDM, \text{family}\}$$

$$Maskn = \exp[2\pi r_n(x, y)]$$

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). $CAM$, $DHM$, $DVM$ and $DDM$ are the matrices $CA$, $DH$, $DV$ and $DD$ multiplied by the RPMs. $F^x$ and $F^y$ 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 (-α) [7]. Thus, we have the following equations:

\begin{align}
\{CA', DHM', DVM', DDM'\} &= DWT[x_\alpha, \text{family'}] \\
CA' &= CAM' \times \text{inv}(\text{Mask1}); \quad DH' = DHM' \times \text{inv}(\text{Mask2}) \\
DV' &= DVM' \times \text{inv}(\text{Mask3}); \quad DD' = DDM' \times \text{inv}(\text{Mask4}) \\
I_x &= F^{-\alpha} \times \{\text{DWT}_x(CA', DH', DV', DD', \text{family'})}\} \times F^{-\alpha}
\end{align}

When the family’ used in the decryption process is equal to the family used in the encryption process and, it is used the same fractional order α 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.

![Figure 1. Block diagram of the digital image encryption process.](image)

4.3. Decryption Digital Algorithm

The decryption process is the same encryption process, but in the inverse sense with the fractional orders of the DFrFT 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 MxN 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:

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

The SNR is defined as:

\[
SNR = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} \left[ I[x,y] \right]^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} \left[ I[x,y] - I_1[x,y] \right]^2}
\] (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 5. Recovered image using a wrong wavelet family in the decryption process.](image)

![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)
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.

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 bruteforce 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

