Multiple Image Encryption using Fractional Multiresolution Transforms

S.Arivazhagan
ECE department
Mepco Schlenk Engineering College

W.Sylvia Lilly Jebarani
ECE department
Mepco Schlenk Engineering College

M.Lakshmi
ECE department
Mepco Schlenk Engineering College

ABSTRACT
Secured communication has been a common practice in the social life. The main idea of encryption is to transform the message in which its original information can only be reconstructed by a desired recipient. As data significance can easily be determined in the transformation domain, it is a preferable domain for encryption of digital images. In this work, secured multiple image transmission is chosen as the primary application and hence a method is proposed for securing multiple images during communication and transmission over insecure channel. The multiple images are encrypted using Arnold cat Map and then using several Fractional Multiresolution transforms followed by sharing. Recent years have also witnessed Fractional Fourier transform (FrFT) domain as a potential transformation domain for encryption. Fractional combined Multiresolution domain inherits the virtues of Multiresolution transform and Fractional domain providing improved security. This offers the Fractional order as an extra key, in addition to the keys offered by any Multiresolution based encryption technique. In the proposed work, Fractional Undecimated Dual Tree Complex Wavelet Transform (FrUDT-CWT) is introduced by coalescing Fractional Fourier Transform (FrFT) and Undecimated Dual Tree Complex Wavelet Transform (UDT-CWT) inheriting the properties of both FrFT and UDT-CWT. Multiple image encryption is done using FrUDT-CWT and the results are compared with FrDT-CWT and FrWT.

General Terms
Fractional multiresolution transforms, Image encryption, Multiple image encryption.

Keywords
Arnold cat map, Encryption, Fractional Dual Tree Complex Wavelet Transform, Fractional Wavelet Transform, Fractional Undecimated Dual Tree Complex Wavelet Transform.

1. INTRODUCTION
In the recent years, the security of digital images attracts much attention and different methods for image encryption have been proposed.

Nidhi Taneja, Balasubramanian Raman and Indra Gupta [1] introduced an efficient selective encryption in Fractional Wavelet domain that encrypts only significant subbands using a chaotic stream cipher. Relationship between normalized information energy and perceptual information of a subband is utilized to select the significant subbands. Thorough performance and security analysis reflects better perceptual and cryptographic security with less computational time.

Gaurav Bhatnagar, Jonathan Wu and Balasubramanian Raman [2] proposed multiple image encryption scheme which is consolidated by Fractional Wavelet Transform and chaotic maps. First, all the images are encrypted followed by their sharing. The sharing process is done considering numerical techniques by making the sharing process a system of linear equations.

Hill.P, Achim.A and Bull.D [5] proposed the technique where Undecimated Dual Tree Complex Wavelet Transform (UDT-CWT) is introduced together with its application in image denoising. The UDT-CWT extends the traditional DT-CWT using the methods of filter upsampling and the removal of downsampling developed for the Undecimated Discrete Wavelet Transform (UDWT). The UDT-CWT results in a one-to-one relationship between co-located complex coefficients in all subbands and offers improved lower scale subband localisation together with improved directional selectivity (compared to the UDWT).

This article develops a simple, yet efficient selective encryption technique that considers fractional order as a part of the key structure and not the entire security key using various fractional multiresolution transforms. Chaos based Arnold cat map is utilized to achieve data confidentiality [1]. Multiple image encryption is performed using linear sharing process [2]. To achieve exact translational invariance, a one-to-one relationship between all co-located coefficients at all scales and improved directional selectivity with the property of describing the information of spatial and frequency domain time–frequency, FrDT-CWT is proposed by performing UDT-CWT [5] in the fractional domain.

2. PRELIMINARIES FOR PROPOSED TECHNIQUE
2.1 Fractional Wavelet Transform (FrWT)
FrWT is a realization of the wavelet transform in FrFT domain [1]. FrFT has a unique property of describing the information of spatial and frequency domain, due to the rotation of time–frequency plane over an arbitrary angle [9]. In contrast, Wavelet transform has multiresolution property. A combination of these two domains results in FrWT, exhibiting multiresolution property and describing the spatial as well as frequency domain information.

The mathematical representation for the FrWT of a one dimensional function \( f(t) \), having a fractional order \( 0 < \alpha < 2 \), is given as follows:

\[
W_{\alpha}(a, s, \tau) = \int_{-\infty}^{\infty} F^{-\alpha}[f(t)](x) e^{-\alpha \Psi_{\alpha}(x)} dx
\]  

(1)

where \( s, \tau \) and \( \Psi \) denote the dilation parameter, translation parameter and the mother Wavelet function respectively.
2.2 Fractional Dual Tree Complex Wavelet Transform (FrDT-CWT)

The Fractional Dual Tree complex Wavelet transform (FrDT-CWT) is a realization of the DT-CWT in the Fractional Fourier domain [3]. The FrFT has a unique property of describing the information of spatial and frequency domain due to the rotation of the time–frequency plane over an arbitrary angle. In contrast, the DT-CWT has Multiresolution property. A combination of these two domains results in FrDT-CWT, which exhibits the Multiresolution property, describing the spatial as well as the frequency domain information. Mathematically, the FrDT-CWT [4] of any finite energy signal \( f(t) \) is defined as

\[
f(t) = \sum_{n} C_{-\alpha} \phi_{n}(t-n) + \sum_{\alpha,n} D_{\alpha} \psi_{\alpha,n}(t-n)
\]

where \( \phi \) and \( \psi \) are the scaling and Wavelet functions, respectively. The function \( \phi \) gives the scaling coefficients \( C(n) \) whereas \( \psi \) gives the Wavelet coefficients \( D(j, n) \), which are further obtained by the inner product with \( f(t) \), i.e.,

\[
C_{\alpha} = \int f(t) K_{\alpha}(t, x) \phi(t-n) dt dx
\]

\[
D_{\alpha} = \int f(t) K_{\alpha}(t, x) \psi(t-n) dt dx
\]

where \( \alpha \) is the transform order and \( K_{\alpha}(t, x) \) is the transform kernel and is given by

\[
K_{\alpha}(t, x) = C_{\alpha} e^{j\alpha t x / \sin \alpha}
\]

(5)

The core idea behind DT-CWT is the use of complex valued scaling and Wavelet functions in Equations (2) - (4), i.e.,

\[
\phi(t) = \phi^r(t) + j \phi^i(t)
\]

\[
\psi(t) = \psi^r(t) + j \psi^i(t)
\]

where \( \phi^r \) and \( \psi^r \) are the real parts and even functions whereas \( \phi^i \) and \( \psi^i \) are the imaginary parts and odd functions respectively.

Using the concept of a complex Wavelet, the complex Wavelet transform is given as (i.e., Equations (2) – (4) reduce to)

\[
f(t) = \sum_{n} C_{\alpha} \left( \phi^r(t-n) + j \phi^i(t-n) \right) + \sum_{\alpha,n} D_{\alpha} \left( \psi^r(t-n) + j \psi^i(t-n) \right)
\]

where \( C_{\alpha} \) and \( D_{\alpha} \) are the scaling and Wavelet coefficients associated with complex Wavelet transform, and are given as

\[
C_{\alpha} = \left\{ f K_{\alpha}, \phi \right\} \int \int f(t) K_{\alpha}(t, x) \left( \phi^r(t-n) + j \phi^i(t-n) \right) dt dx = C_{\alpha} + j i C_{\alpha}
\]

(10)

\[
D_{\alpha} = \left\{ f K_{\alpha}, \psi \right\} \int \int f(t) K_{\alpha}(t, x) \left( \psi^r(t-n) + j \psi^i(t-n) \right) dt dx = D_{\alpha} + j i D_{\alpha}
\]

(11)

Using Equations (10) and (11), Equation (9) becomes

\[
f(t) = \sum_{\alpha} \left( C_{\alpha} + j i C_{\alpha} \right) \left( \phi^r(t-n) + j \phi^i(t-n) \right) + \sum_{\alpha,n} \left( D_{\alpha} + j i D_{\alpha} \right) \left( \psi^r(t-n) + j \psi^i(t-n) \right)
\]

(12)

The above equation can be rearranged as

\[
f(t) = \sum_{\alpha} \left( C_{\alpha} \phi^r(t-n) + i \phi^i(t-n) \right) + \sum_{\alpha,n} \left( D_{\alpha} \psi^r(t-n) + i \psi^i(t-n) \right)
\]

By separating the real and imaginary parts, Equation (13) becomes

\[
f(t) = \sum_{\alpha} \left( C_{\alpha} \phi^r(t-n) + i \phi^i(t-n) \right) + \sum_{\alpha,n} \left( D_{\alpha} \psi^r(t-n) + i \psi^i(t-n) \right)
\]

Further, Equation (14) can be written as

\[
f(t) = Tree_{\text{real}} + iTreec_{\text{imaginary}}.
\]

From the above equation, it is clear that two Wavelet tree structures are obtained using complex valued scaling and Wavelet functions. Hence, this transform is usually denoted as the DT-CWT [4]. The most important property of DT-CWT is that both trees have the ability to reconstruct the signal perfectly. Therefore, the inverse DT-CWT can be viewed as the inverse Wavelet transform of both the real and imaginary trees, which gives the two signals, and the optimum signal is calculated by averaging these two obtained signals. These two real signals are then averaged to obtain the final output. Due to the separability of the transform, the higher-dimension FrDTCWT can be obtained by taking 1D transform along each direction.

2.3 Arnold cat map

An Arnold Cat Map is a mapping of the form: \((x, y)\) to modulus \((x + y, x + 2y, N)\). The mapping shears the original image, and the modulus function folds the image into the original image area.

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix} \mod(N)
\]

(16)

where \( A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \), \((x', y')\) is the new position of original pixel position \((x, y)\), when the Arnold cat map is performed once. As determinant of the transformation matrix \( A \) is 1, the map is area preserving by nature.

3. PROPOSED TECHNIQUE

3.1 Fractional Undecimated Dual Tree Complex Wavelet Transform (FrUDT-CWT)

The DT-CWT provides near shift invariance and improved
directionality within a more compact representation. The structure of the DT-CWT uses two separate trees to form Hilbert filter pairs within each subband. The magnitude response of this pair of filters is very near to being shift invariant. Another benefit of this transform is improved directional resolution (in the two dimensional version). But the subsampled subbands of the DT-CWT have a restricted number of coefficients directly related to each spatial position in the signal or image: a relationship that is often required within analysis applications.

To enable such analysis, undecimated form of the DT-CWT i.e., UDT-CWT is used where each subband has the same resolution as the signal. As the UDT-CWT contains no subsampling it exhibits perfect shift invariance. It also offers a one-to-one relationship between all co-located coefficients and the original samples and also between collocated coefficients.

\[
M(i, j) = A(i, j) \oplus B(i, j) \tag{17}
\]

where \(A(i, j)\) denotes the Arnold scrambled coefficient, \(B(i, j)\) denotes value from random binary matrix and \(M(i, j)\) denotes the modified subband.

5. Take the inverse Fractional Multiresolution transform to retrieve the encrypted images.

6. Generate a random matrix \(W\) with a seed value (Key\(_y\)). Multiply the generated random matrix with the key value lesser than 0.01 (Key\(_x\)) to get positive weight factor matrix.

7. Construct a linear system with the help of positive weight factor matrix as shown in Eq. 18.

8. The pixels are shared for all values of \(x\) and \(y\) and hence shared encrypted images are obtained [2].

The linear system is constructed as follows:

\[
\tilde{I}_x(x, y) = w(1, 1) \tilde{I}_x(x, y) + w(1, 2) \tilde{I}_x(x, y) + \ldots + w(1, L) \tilde{I}_x(x, y)
\]

\[
\tilde{I}_y(x, y) = w(2, 1) \tilde{I}_y(x, y) + w(2, 2) \tilde{I}_y(x, y) + \ldots + w(2, L) \tilde{I}_y(x, y)
\]

\[
\ldots (18)
\]

where \(x\) and \(y\) are pixel positions in the images and \(j = 1, 2, \ldots, L\) gives the corresponding pixel in the shared encrypted images.

4. RESULTS AND DISCUSSION

For multiple image encryption in Fractional multiresolution transforms, 15 test images of size 256 x 256 are chosen. The test images are encrypted individually using FrWT, FrDT-CWT and FrUDT-CWT followed by sharing. The test images used in this work are shown in Figure 2.

4.1 Multiple image encryption using Fractional Wavelet Transform

5-level Wavelet Transform is performed over FrFT of order \((1, 1)\) to get 5-level FrWT. After performing 5-level FrWT, every subband is encrypted separately. For each level, 4 subbands are obtained and hence 20 subbands are obtained after 5-level FrWT. Here, the size of the subbands is reduced by the factor of 2 at each level. So, it is not possible to find an iteration value for which Net Pixel Change Rate (NPCR) value is high for all subband. Hence, iteration value is taken as 7 as it produces better overall NPCR value on all subbands of various sizes. Inverse 5-level FrWT is performed to obtain the

![Fig 1: Decomposition using UDT-CWT](image1)

![Fig 2: Test Images of size 256 * 256](image2)
encrypted image. The encrypted images using FrWT of test images in Figure 2 are shown in Figure 3.

![Fig 3: Encrypted images using FrWT](image)

Fig 3: Encrypted images using FrWT

The multiple encrypted images are shared using the linear system for increased security. The seed value used for positive weight matrix generator is taken as $K_3 \times K_4$, where $K_3$ is 6345921 and $K_4$ value taken here is 0.00234 which is used as a security key while desharing at the receiver. The shared encrypted images are shown in Figure 4.

When compared with the encrypted images, the shared encrypted images show better confusion.

### 4.2 Multiple image encryption using Fractional Dual Tree Complex Wavelet Transform

5-level DT-CWT is performed over FrFT of order (1,1) to get 5-level FrDT-CWT. After performing 5-level FrDT-CWT, every subband is encrypted separately. For each level, 16 subbands are obtained and hence 80 subbands are obtained after 5-level FrDT-CWT.

![Fig 5: Encrypted images using FrDT-CWT](image)

Fig 5: Encrypted images using FrDT-CWT

Here, the size of the subbands is reduced by the factor of 2 at each level. The subbands are encrypted separately followed by multiple image encryption as done in section 4.1. The encrypted image and shared encrypted images for various test images in Figure 2 are shown in Figure 5 and Figure 6 respectively.

### 4.3 Multiple image encryption using Fractional Undecimated Dual Tree Complex Wavelet Transform

5-level UDT-CWT is performed over FrFT of order (1,1) to get 5-level FrUDT-CWT. After performing 5-level FrUDT-CWT, every subband is encrypted separately. For each level, 16 subbands are obtained and hence 80 subbands are obtained after 5-level FrUDT-CWT.

![Fig 7: Encrypted images using FrUDT-CWT](image)

Fig 7: Encrypted images using FrUDT-CWT

Here, the size of the subbands is same as that of the original image at each level. It is found that for an iteration value of $n = 20$, highest Net Pixel Change Rate (NPCR) value is obtained and hence 20 iterations are performed in encryption process. Inverse 5-level UDT-CWT is performed to obtain the encrypted image. The sharing process for multiple image encryption is performed the same way as given in sections 4.1 and 4.2. The encrypted images and shared images for various test images in Figure 2 are shown in Figure 7 and Figure 8 respectively.

![Fig 8: Shared encrypted images using FrUDT-CWT](image)

Fig 8: Shared encrypted images using FrUDT-CWT
4.4 Correlation Coefficient Analysis

To estimate the encryption quality of the proposed encryption algorithm, the correlation coefficient between adjacent pixel values is calculated using Equation (19). Correlation computes the degree of similarity between two variables for highly correlated images, the correlation coefficient is almost 1.

\[
\rho(w, \overline{w}) = \frac{\sum \sum (w(i) - \mu(w))(\overline{w}(i) - \overline{\mu(w)})}{\sqrt{\sum \sum (w(i) - \mu(w))^2 \sum \sum (\overline{w}(i) - \overline{\mu(w)})^2}}
\]

where \( w, \overline{w}, \mu(w), \) and \( \overline{\mu(w)} \) are the original image, encrypted image, mean of original image and mean of encrypted image.

The correlation between adjacent horizontal and vertical pixels are analysed for the original and encrypted images in various Fractional Multiresolution Transforms and the results are shown in Table 1.

Correlation coefficients between two variables X and Y are expressed as values between +1 and -1. A coefficient of +1 indicates a perfect positive correlation i.e., Very strong positive linear relationship between X and Y. Y increases as X increases. A coefficient of -1 indicates a perfect negative correlation i.e., Very strong negative linear relationship between X and Y. Y decreases as X increases. A coefficient of zero indicates zero linear relationship i.e., Y does not tend to increase or decrease as X increases.

<table>
<thead>
<tr>
<th>Table 1. Correlation Coefficient Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Images</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Cameraman</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Lena</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Barbara</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Baboon</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Boat</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Clown</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Bird</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Plane</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>House</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Pepper</td>
</tr>
</tbody>
</table>

It is observed from Table 1 that the correlation between adjacent pixels is highly reduced in all the encrypted images than the original images. It is inferred that encrypted images using FrWT has reduced correlation coefficient when compared with FrDT-CWT and FrUDT-CWT.

4.5 NPCR Analysis

Net Pixel Change Rate (NPCR) test is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images. The NPCR value for the encrypted images calculated using the formula in Equation (20) for various Fractional Multiresolution Transforms are shown in Table II.

The range of NPCR is 0 to 1. NPCR value of 0 implies that all pixels in the encrypted image remain with same values as in original image. NPCR value of 1 implies that all pixel values in the encrypted image are changed compared to those in the original image.

<table>
<thead>
<tr>
<th>Table 2. NPCR ANALYSIS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Images</td>
</tr>
<tr>
<td>Cameraman</td>
</tr>
<tr>
<td>Lena</td>
</tr>
<tr>
<td>Barbara</td>
</tr>
<tr>
<td>Baboon</td>
</tr>
<tr>
<td>Boat</td>
</tr>
<tr>
<td>Clown</td>
</tr>
<tr>
<td>Bird</td>
</tr>
<tr>
<td>Plane</td>
</tr>
<tr>
<td>House</td>
</tr>
<tr>
<td>Pepper</td>
</tr>
</tbody>
</table>
It is observed in Table 2 that the NPCR value is higher for all the encrypted images obtained using FrUDT-CWT when compared with the encrypted images using FrWT and FrDT-CWT.

### 4.6 UACI Analysis

UACI (Unified Average Changing Intensity) test is one of the common tests to find the difference between encrypted and original image. A small change in original image must cause some significant change in encrypted image. UACI is helpful to identify the average intensity of difference in pixels between the two images.

\[
UACI = \frac{1}{M \times N} \sum_{i,j} \left| \frac{A(i,j) - A'(i,j)}{255} \right| \times 100\% \tag{21}
\]

where A and A' are the pixel positions in the original image and encrypted image respectively. M is the height by pixels of the images and N is the width by pixels of the images.

The UACI value for the encrypted images using various Fractional Multiresolution Transform are shown in Table 3.

<table>
<thead>
<tr>
<th>Test Images</th>
<th>FrWT (%)</th>
<th>FrDT-CWT (%)</th>
<th>FrUDT-CWT (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cameraman</td>
<td>27.2174</td>
<td>42.5706</td>
<td>43.1509</td>
</tr>
<tr>
<td>Lena</td>
<td>23.6202</td>
<td>38.7063</td>
<td>40.0356</td>
</tr>
<tr>
<td>Barbara</td>
<td>24.1763</td>
<td>39.4857</td>
<td>41.2558</td>
</tr>
<tr>
<td>Baboon</td>
<td>23.1484</td>
<td>37.7682</td>
<td>39.2854</td>
</tr>
<tr>
<td>Boat</td>
<td>24.4752</td>
<td>38.2389</td>
<td>39.4481</td>
</tr>
<tr>
<td>Clown</td>
<td>24.8429</td>
<td>44.3755</td>
<td>45.9091</td>
</tr>
<tr>
<td>Bird</td>
<td>23.9202</td>
<td>39.9640</td>
<td>42.2597</td>
</tr>
<tr>
<td>Plane</td>
<td>35.4970</td>
<td>36.8611</td>
<td>37.6544</td>
</tr>
<tr>
<td>House</td>
<td>25.2705</td>
<td>37.9128</td>
<td>37.9516</td>
</tr>
<tr>
<td>Pepper</td>
<td>25.0825</td>
<td>40.7574</td>
<td>41.6699</td>
</tr>
<tr>
<td>Rays</td>
<td>42.5832</td>
<td>76.8021</td>
<td>77.8054</td>
</tr>
<tr>
<td>Building</td>
<td>23.7346</td>
<td>45.5502</td>
<td>47.5815</td>
</tr>
<tr>
<td>Gull</td>
<td>29.0275</td>
<td>63.9282</td>
<td>65.2508</td>
</tr>
<tr>
<td>View</td>
<td>24.0782</td>
<td>40.8686</td>
<td>43.7240</td>
</tr>
<tr>
<td>Fly</td>
<td>27.9609</td>
<td>36.4838</td>
<td>39.2784</td>
</tr>
</tbody>
</table>

It is observed that the UACI value is higher for encrypted images obtained using FrUDT-CWT when compared with the encrypted images using FrWT and FrDT-CWT.

### 5. CONCLUSION

In Multiple Image Encryption using Multiresolutional Fractional Transforms, Arnold Cat Map is used. FrUDT-CWT is introduced by coalescing Fractional Fourier Transform and Undecimated Dual Tree Complex Wavelet Transform inheriting the properties of both FrFT and UDT-CWT. It is observed from NPCR and UACI analysis that encryption is better in FrUDT-CWT than in FrDT-CWT and FrWT due to perfect shift invariance property of FrUDT-CWT. In the proposed work, four security keys are used i.e., Fractional order (K = 1), Seed value used in Encryption (K = 2), Arnold Iteration Value (K = 5 for FrWT and FrDT-CWT; K = 20 for FrUDT-CWT), Key value used in Sharing Process (K = 0.00234). As a future scope of this work, multiple image encryption technique can be done using other Fractional Multiresolution transforms and other chaotic maps like Baker’s map, Henon map, etc as well as other sharing processes with increased security keys.

### 6. REFERENCES


