# 4-Weighted Fractional Fourier Transform based Multiple Image Encryption Approach with PAN

Arvind Singh Choudhary[1*], Manoj Kumar[2], Sudhir Keshari[3]

[1]*Dept. of Computer Science Engineering, Government Engineering College Bharatpur, Rajasthan, India*
[2]*Dept. of Computer Engineering &Application, GLA University Mathura, Uttar Pradesh, India*
[3]*Dept. of Electronics & Communication Engineering, Govt. Engineering College Bharatpur, Raj., India*

***Abstract:***

In this manuscript, a new encryption approach for multiple images is proposed based on 4-weighted fractional frequency transform (4-WFRFT) domain. First, the low frequency-components of all the images are obtained by applying Fourier Transform on each image, which positioned at corner position of image, shifted to the central position. Low-frequency component of each individual image is then scrambled with help of Arnold cat map with its parameters and combined all scrambled image to form a single image with the same size that of original image which is now ready for encryption process. Here, parameters of Arnold cat map and transform order of 4-WFRFT treated as secret keys which are converted from Permanent Account Number (PAN) of authorize person. The encrypted image information generated by authorize person can be recovered by applying PAN at receiver side.

**Keywords***:*4-Weighted fractional Fourier transform, Fourier transform, Arnold Cat Map, Encryption Process.

*Corresponding author Email: arvindbecs@gmail.com

## 1. Introduction

The concept of cryptography came into the existence when the huge data is being transmitted between sender and receiver through the wireless communication channel. Cryptography is more general form of encryption. The basics of cryptography can be easily understood mainly in term of encryption, authentication, and integrity. Encryption is the process in which the original form of data is converted into unreadable form so that malicious users cannot easily decode the content of the original data. Encryption is performed at the trainmaster side. On other hand, at receiver side, decryption process is taken place, of which performance is just reverse of the encryption process and of which purpose is to retrieve the original image/data from the encrypted data. Some encryption techniques have same encryption keys involved between transmitter and receiver is called symmetrical cryptography and some have distinct keys i.e. private keys and public keys is called unsymmetrical cryptography.

The second key parameter of cryptography is authentication of the content of the message which is being transferred. This can be understood like suppose a sender send any secret message to the receiver. Receiver receives that message but want to know the proof that the message which is received by receiver is actually sent by that sender or not. So this concept comes under the umbrella of authentication concept.

The third parameter of cryptography is integrity of the message in which it is studied when any sender send that secret message to the recipient then he want to confirm the content of the message where it is discard or not.

In recent year, the applications of Multiple Image Encryption (MIE) technology are very much popular. The advantages of using MIE technology in these applications are that, it increases not only encryption efficiency but also enhance the facilities of huge data transmission. MIE technology is now–a–days widely used in areas of optical image processing [01-05].

From the past decades, many forms of Fourier transform are available, which are used in various techniques of image encryption applications. But general form of Fourier Transform called fractional Fourier transform (FRFT) is more utilized in image encryption algorithms [06]. Some researchers have contributed their efforts to make more secure system by including scrambling technique in their image encryption algorithms [07]. Some researchers approached double random encoding techniques in image encryption technique to make their work superior to others [08]. Here, it is required to mention important fact about fractional Fourier transform (FRFT) is that it has large computational time and more complexity compare to the other one. Therefore, system based on fractional Fourier transform become very sluggish and its efficiency becomes very poor.

On the other hand, 4-weighted fractional Fourier transform (4-WFRFT) is other form of Fourier transform although has same significance as that of FRFT and therefore, it is widely used only on account of low computational complexity and consequently provides quick response in the system compare to the FRFT [09-10].

The work is segregated as follow: in section I, the present scenario of existing technologies carried out to our proposed work are illustrated, in section II, the basic fundamental concept of 4-weighted fractional Fourier transform and Arnold cat map involved in our work, are described. In section III, detailed illustration of proposed work along with its block diagram is presented on describing each block involved in that. In section IV, simulations have been performed on MATLAB® and discussion about obtained results, and Finally, Section V concludes the paper.

### 2.1 Materials and Methodology Concept of 4-Weighted Fractional Fourier Transform (4-WFRFT)

The significance of fractional Fourier transform is conversion of image domain from spatial to its intermediate domain. Same features also happen in 4-WFRFT but due to its inherent property as compare to

FRFT, it is very easy to utilize in image encryption of image processing applications. The 4-WFRFT with its transform order for one dimensional signal is expressed as follows:
For an invertible continuous time signal $f(x)$, 4-WFRFT with transform order *a* is expressed as follows [11-13]:

$$\mathcal{F}^{a}[f(x)] = w_0(a)f(x) + w_1(a)F(x) + w_2(a)f(-x) + w_3(a)F(-x) \quad (1)$$

$$\text{where } F(k) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} f(x)e^{-jkx}dx \quad (2)$$

$$w_l(a) = cos\left[\frac{(a-l)\pi}{4}\right] cos\left[\frac{2(a-l)\pi}{4}\right] exp\left[\frac{3(a-l)\pi i}{4}\right] \quad (3)$$

$F(k)$is frequency domain representation of a signal $f(x)$, where, $k$ denotes as frequency domain and$w_l(a)$denotesweighted coefficients, where $l = 0,1,2,3$. Here, symbols *f*(*x*), *f*(−*x*) *F*(*x*), and *F*(−*x*) denote the same signal, time inversion of signal, Fourier transform, and inverse Fourier transform respectively.
Second core ideal behind the processing on low-frequency component of an image is that Fourier transform of an image produces the frequency domain based information, and main image information is concentrated into low frequency spectrum which is represented on logarithm scale as shown in Fig. 01. Therefore, here only low-frequency component is considered and high-frequency components are left as only low-frequency components are responsible to retrieve original image by applying inverse-Fourier transform on that components.

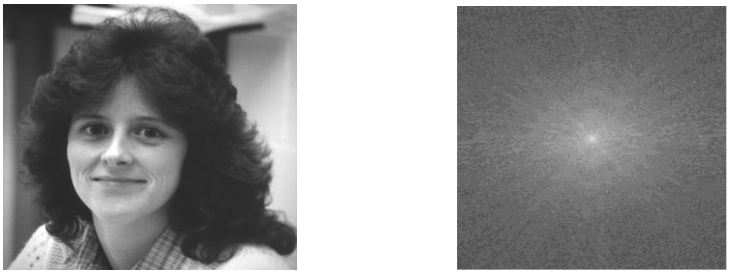


**Fig.01: Image and generated low frequency component**

### 2.2 Concept of Arnold Cat Map

The Arnold Cat map is also included here for purpose of scrambling the pixels of low-frequency component of an image obtained from previous steps, which is represented as follow [03]:

$$\begin{bmatrix} x_{\varphi+1} \\ y_{\varphi+1} \end{bmatrix} = \begin{bmatrix} 1 & \varepsilon \\ \eta & \eta\varepsilon + 1 \end{bmatrix} \begin{bmatrix} x_{\varphi} \\ y_{\varphi} \end{bmatrix} mod(N) \quad (4)$$

where $x_{\varphi}$, $y_{\varphi}$ are $\varphi^{\text{th}}$location of pixels in *N*×*N* image, and $\boldsymbol{\varepsilon}$, $\eta$ are positive integers constant parameters.The inherent property of Arnold Cat map is to rearrange the positions of image pixels and restores the same pixels positions after certain iterations consequently obtained image resemble to the original image. For 256 × 256 image with parameters $\boldsymbol{\varepsilon}$ =10, $\eta$ =8, pixel positions are restored thereafter formed same image after 128 iterations.

## 2. Proposed Work

### 3.1 Key Manegment and Generation

To encrypt the multiple images by proposed technique, the key which is used for encryption process is first generated by PAN of the sender at transmitter side with following steps as follows:

1.The PAN assigned is converted into the American Standard Code for Information Interchange (ASCII) code for further processing of the keys.

2. PAN is a unique code assigned to individual person of India for identification is issued by Income Tax Department, Government of India. As PAN consists of 10 words in which five characters are capital letter (from A to Z), next four are numerals (from 0 to 9) and last character is letter. The decimal conversion of PAN from the ASCII table consists of total 20 digits, which are serially arrangedas per following manner:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $a1$ | $a_2$ | $a_3$ | $a_4$ | $a_5$ | $a_6$ | $a_7$ | $a_8$ | $a_9$ | $a_{10}$ |
| $a_{11}$ | $a_{12}$ | $a_{13}$ | $a_{14}$ | $a_{15}$ | $a_{16}$ | $a_{17}$ | $a_{18}$ | $a_{19}$ | $a_{20}$ |

Fig. 02: Generation of keys.

3. The decimal conversionof PAN is represented in Fig. 02 from ASCII table, in which, two-two digits as per shown pattern are extracted from that code, combined them to form iteration parameter of Arnold cat map to shuffle all low-frequency component of each image, therefore, total 08 digits ($a_1a_{12}, a_2a_{13}, a_3a_{14}, a_4a_{15}$)are used for Arnold cat-map. After that 02 ($a_5a_{16}$)digits are used by transform order of 4-WFRFT to convert into intermediate domain of image.

**3.2 Proposed Encryption/Decryption algorithm**

In recent years, Multiple Image Encryption (MIE) technology is widely used to increase the transmission efficiency and capability of the system. Here, multiple images are encrypted simultaneously, by first extracting low frequency component from individual image with help of Fourier transform and obtained low frequency component are scrambled with help of Arnold cat map with its parameters, produced scrambled-low-frequency (SLF) as illustrated in Fig. 03.These SLF images are combined to form a single image with same size as that of original image, and now, it is transformed into 4-WFRFT domain by applying 4-WFRFT transform along with its transform order on the formed image. Now, generated image is called encrypted image which is suitable for transmission over the communication channel.

During encryption process, parameters of Arnold cat map and transform order of 4-WFRFT are taken from ASCII code converted from PAN of sender as shown in the Fig. 02, in which 08 digits are taken for Arnold cat map and two digits are for 4-WFRFT. And furthermore, remaining ASCII code can be utilized in future purpose to make more secure system. Now encrypted image is produced and ready to transmit over the wireless communication channel.

On the other hand, encrypted image is accessed by the authorized recipient their login detail. The procedure to retrieve the original multiple images from encrypted image is the just reverse of process adopted at the transmitter side.

To retrieve the original images at receiver end, firstly 4-WFRFT with same transform order used at transmitter side is applied on that image, then each SLF components corresponding to each medical image is separated and re-scrambled low-frequency components with help of Arnold cat map with same parameter used at transmitter side to obtain the low-frequency component. Finally, inverse Fourier transform is applied on obtained low-frequency components to obtain all images at the receiver end.

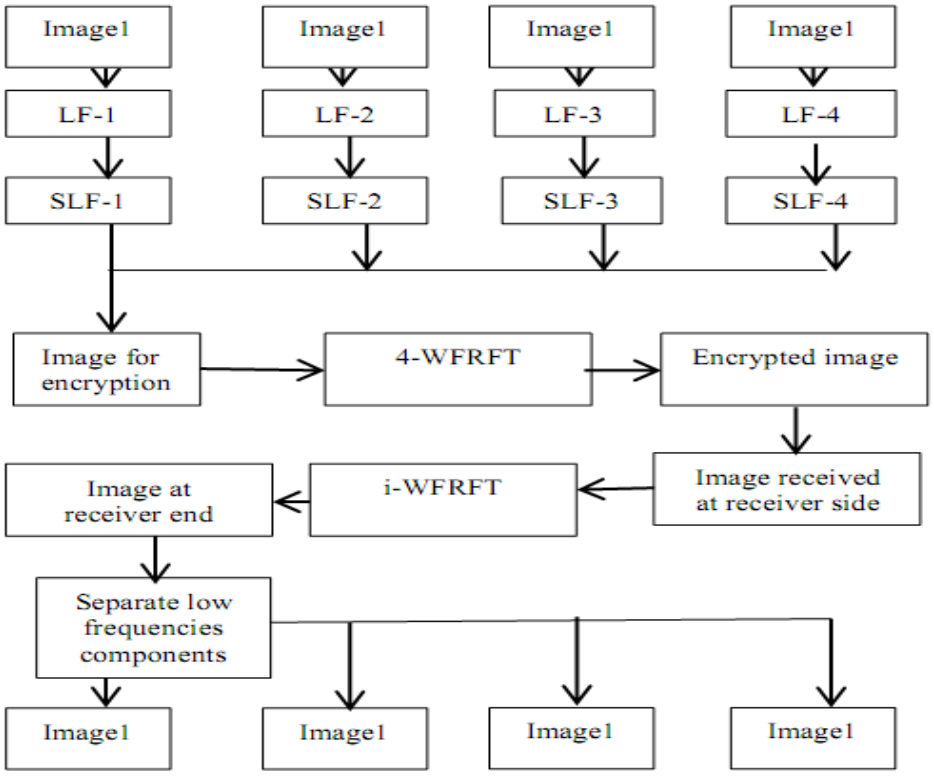
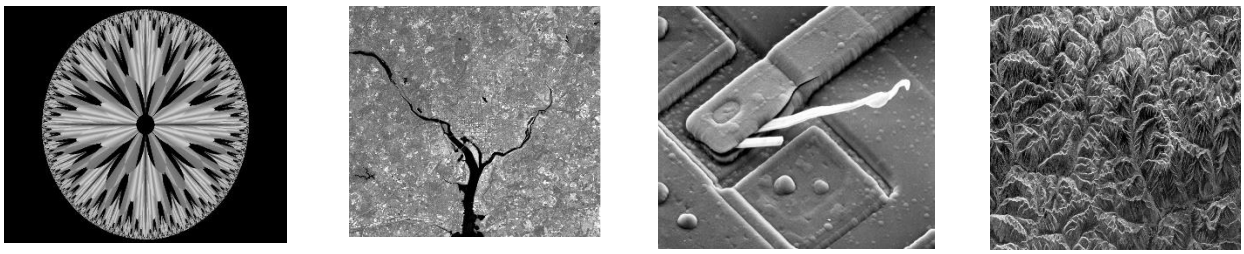



**Fig. 03: Proposed Multiple Image Encryption technique based on 4-WFRFT.**

## 3. Results and Discussion

Before performing experiment on MATLAB®, it is necessary to mention about images on which experiment is performed. Here, four images or scan images form with size 256 × 256 are involved which are shown in Fig. 04.



(a) (b) (c) (d)

**Fig. 04: Multiple images**

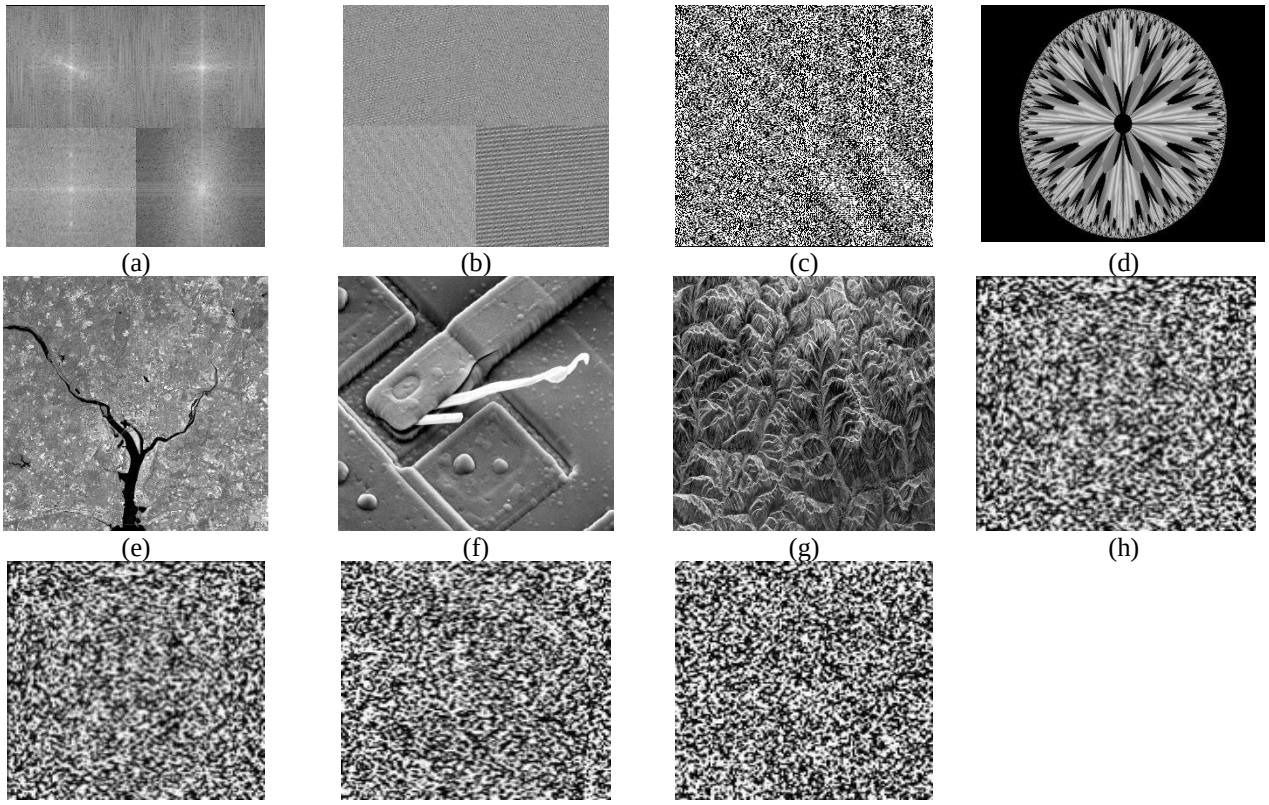
Its low-frequency components are extracted by applying the Fourier transform on each image and combined low-frequency components which are represented on logarithm scale as shown in Fig. 05 (a).In our experiment, an arbitrary PAN "CBAOE4321A" of sender is used, of which decimal conversion from ASCII Table is written below:

a={'67' '66' '65' '79' '69' '52' '51' '50' '49' '65'}

ASCII numbers is obtained after conversion of PAN number which comes into character category. Here, now each low-frequency component is scrambled by using Arnold cat-map with iterations {$itr_1$=62, $itr_2$ =75,

$itr_3$=61, $itr_4$=65} for each image taken from PAN of authorize person. And then combined all produced images to from a single image with same size 256 × 256 as shown in Fig.05 (b) and after that 4-WFRFT with transform order (i.e. 60)is performed on that image to produce encrypted image which is suitable for transmission over the communication channel as shown in Fig.05 (c).

Now, to discuss the security attack of proposed technique against the malicious users, it is stated about important point is that multiple image encrypted images are decrypted at the receiver end if correct PAN of authorize person will be used in the system, which are being generated through simulationas shown in Fig. 05(d) – 05(g). Now, if correct secret keys are not entered into the system, then negative results are obtained at receiver end as shown in Fig. 05 (h) – 05(k).




(a) Low-frequency component of each image Logarithm Scale, (b) scrambled low-frequency, (c) Encrypted multiple images, (d)-(g) decrypted digital image with correct keys, (h)-(k) Negative result when wrong keys.

**Fig. 05: Results of the proposed encryption/decryption technique**

## 4. Conclusion

In this manuscript, a novel approach for encryption of multiple secret images/digital documents of person have been proposed and this can be widely used for those person who are always connected with professional society where certification/authentication of documents are required. It provides better facility in term of transmission efficiency and capability of the system also, due to simultaneously transmission of multiple images over the communication channel.

**Conflict of interest**: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

**References**

[1]. Xianye Li, Xiangfeng Meng, Xiulun Yang, Yongkai Yin, Yurong Wang, Xiang Peng, Wenqi He, Guoyan Dong, Hongyi Chen. "Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling"IEEE Photonics Journal. 8/4 (2016)01-03. https://doi.org/10.1109/JPHOT.2016.2591441

[2]. Wen Chen. "Optical Multiple-Image Encryption Using Three-Dimensional Space" IEEE Photonics Journal 8/6(2016)01-09. https://doi.org/10.1109/JPHOT.2016.2550322

[3]. Nihal F. F. Areed and Salah S. A. Obayya. "Multiple Image Encryption System Based on Nematic Liquid Photonic Crystal Layers" Journal of Lightwave Technology 32/7 (2014)1344-1350. https://doi.org/10.1109/JLT.2014.2300553

[4]. Muhammad Rafiq Abuturab. "Multiple information encryption by user-image-based gyrator transform hologram"Optics and Lasers in Engineering. 92 (2017)76-84. https://doi.org/10.1016/j.optlaseng.2017.01.001

[5]. Xiaoqiang Zhang, Xuesong Wang. "Multiple-image encryption algorithm based on mixed image element and permutation"Optics and Lasers in Engineering. 92 (2017)6-16. https://doi.org/10.1016/j.optlaseng.2016.12.005

[6]. Qianrong Lu, Kaizhi Wang and Xing Zhao Liu. "A Novel SAR Imaging Processing Method Based On Fractional Fourier Transform" International Geoscience and Remote Sensing Symposium:Milan, Italy(2015) 4472-4475.

[7]. Y.B. Li, F. Zhang, X.J. Kang, L.Y. Xu. "Image Encryption Based on the iterative Fractional Fourier Transform and a Novel Pixel Scrambling Technique"IET International Radar Conference, Hangzhou(2015) 1-6.

[8]. Sudheesh K. Rajput and Naveen K. Nishchal. "Double Image Encryption Scheme Based on Known-Plaintext attack in Fractional Fourier Transform Domain"Workshop on Recent Advances in Photonics (WRAP)New Delhi, India(2013) 1-2. https://doi.org/10.1109/WRAP.2013.6917709

[9]. Xiaolu Wang Weiming Zhong Lin Mei. "Signal Clipping for PAPR in Hybrid Carrier System Based on 4-Weighted Fractional Fourier Transform" Third International Conference on Instrumentation, Measurement, Computer, Communication and Control (IMCCC)Shenyang, China (2013) 638-642. https://doi.org/10.1109/IMCCC.2013.142

[10]. Yongtao Hui, Bingbing Li and Zhao Tong. "4-weighted fractional Fourier transform over doubly selective channels and optimal order selecting algorithm"Electronics Letters, 51 (2015)177-179. https://doi.org/10.1049/el.2014.2268

[11]. Sudhir Keshari, Mohammad Salim, Shri Gopal Modani. "Single channel modified multiple-parameter fractional Fourier transform and scrambling technique" Optik - International Journal for Light and Electron Optics, 126/24 (2015)5845-5849. https://doi.org/10.1016/j.ijleo.2015.09.114

[12]. Sudhir Keshari and Shri Gopal Modani. "Weighted Fractional Fourier Transform based Image Steganography" in IEEE International Conference on Recent Trends in Information Systems (ReTIS)Kolkata, India(2011) 214-217. https://doi.org/10.1109/ReTIS.2011.6146870

[13]. Tao Li, Xuanli Wu1,Lin Mei, Xuejun Sha, "Performance Analysis of 4-WFRFT Based Carrier Modulations under Burst Interference", Advanced Materials Research Vols 171-172 (2011) pp 500-503 Online: 2010-12-06. https://doi.org/10.4028/www.scientific.net/AMR.171-172.500