EFFICIENT WAY OF IMAGE ENCRYPTION USING GENERALIZED WEIGHTED FRACTIONAL FOURIER TRANSFORM WITH DOUBLE RANDOM PHASE ENCODING

Priyanka Chauhan¹, Girish Chandra Thakur²
M. Tech. Scholar¹, Associate Professor²,
Dept. of Electronics & Communication Engg., Institute of Engineering & Technology,
Alwar-301030 (Raj.), India

ABSTRACT

Data transfer between the users over different network technologies is increasing day by day. With the data transfer, concern about the information theft by any eavesdropper is also increasing. To prevent this information theft, our information is converted into unreadable form using some algorithm and it can only be converted into readable form using key. This process of conversion the information into secured form is called encryption. At present information transfer is also in the form of images. In this paper we are going to discuss some of the methods of encrypting the images. In any encryption technique, the major role is played by its key i.e. larger the number of parameters in the key stronger is the encryption technique. So in the thesis we will develop the GWFRFT which is based on the properties of conventional FRFT and discuss random phase encoding technique in FRFT domain. Then study random phase encoding technique in GWFRFT domain. And at last to make the scheme more efficient and strong we encrypt two images in to single image.

Keywords: Encryption, FRFT, FT, GWFRFT, Image.

1. INTRODUCTION

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing extra ordinary information, more often than not referred to while a key. This product of the process is encrypted in order in cryptography, referred to cipher text. The invalidate process, i.e., to make the encrypted information readable again, is referred to as decryption (i.e. to make it unencrypted). In recent years there have been numerous reports of confidential data such as
customers’ personal records being exposed through loss or theft of laptops or endorsement drives. Encrypting like files at rest help guard them should physical security events fail. Digital liberties organization systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection) are another somewhat different example of using encryption on data at rest. There have been numerous reports of data in transit being intercepted in current years. Encrypting information in shipment also helps to secure it as it is often difficult to physically secure all access to networks. In this paper we are using Generalized Weighted Fractional Fourier Transform with random phase encoding technique for the encryption of two images in to single image. GWFRFT will be derived from the FRFT. The fractional Fourier transform (FRFT) is a superset of the Fourier transform and has been applied in optics, quantum mechanics, and signal processing areas [15,20,21]. In this paper, we discuss a generalized weighted fractional Fourier transform (GWFRFT) which is weighted sum of the integer order fractional Fourier transform.

2. DEFINITION OF FRFT AND GWFRFT

FRFT is a generalization of FT [1, 13]. It is not only richer in theory and more flexible in application, but is also not expensive in implementation. It is a powerful tool for the analysis of time-varying signals. With the advent of FRFT and related concepts, it is seen that the properties and applications of the conventional FT are special cases of those of the FRFT. However, in every area where FT and frequency domain concepts are used, there exists the potential for generalization and implementation by using FRFT. Mathematically, $\alpha$th order FRFT is the $\alpha$th power of FT operator. Hence $\alpha$th order FRFT of any signal $s(t) \in L(R^2)$ is given by

$$F^{\alpha}[s(t)] = \int_{-\infty}^{+\infty} s(t)K(\alpha; \omega, t)dt$$  \hspace{1cm} (1)

Where

$$K(\alpha; \omega, t) = K(\alpha) \exp[(B(\alpha)\omega^2 - C(\alpha)\omega t + B(\alpha)t^2)]$$ \hspace{1cm} (2)

Is the kernel of $F^{\alpha}$, $\alpha$ is the fraction, and

$$K(\alpha) = \sqrt{\frac{1-j \cot(\alpha)}{2\pi}}$$ \hspace{1cm} (3)

$$B(\alpha) = \cot(\alpha)$$ \hspace{1cm} (4)

$$C(\alpha) = \frac{1}{\sin(\alpha)}$$ \hspace{1cm} (5)

$$\alpha = \frac{\pi a}{2}$$ \hspace{1cm} (6)
For integer values of $\alpha$ it can be deduced that any fractional Fourier transform repeat itself at an interval of 4 that can be shown as

$$F^{4m+l}[s(t)] = F^l[s(t)]$$  \hspace{1cm} (7)

Where $m$ is any integer and $l$ can be any real number.

As we discussed the periodic nature of integral order fractional Fourier transform in the previous chapter i.e. integer order fractional Fourier transform is periodic with period 4. So now it is given that $\alpha^{th}$ order FRFT of any signal can be represented in terms of these four integral order FRFT i.e.

$$F^\alpha_w[s(t)] = A_0(\alpha)F^0[s(t)] + A_1(\alpha)F^1[s(t)] + A_2(\alpha)F^2[s(t)] + A_3(\alpha)F^3[s(t)]$$ \hspace{1cm} (8)

Where the coefficients $A_l(\alpha), l = 0,1,2,3$ are continuous functions of $\alpha$.

Generalized weighted fractional Fourier transform obeys the following axioms.

I. Continuity axiom: $F^\alpha_w : L(R^2) \longrightarrow L(R^2)$ is continuous in fractional order $\alpha$.

II. Boundary axiom: $F^\alpha_w$ degenerates into $F^\alpha$ when $\alpha$ is an integer multiple of $\frac{\pi}{2}$ or $\alpha$ is an integer. i.e. for integer order the weighted fractional Fourier transform reduces into the normal Fourier transform of signal $s(t)$ or the signal itself. For different integer values of order $a$, the values of weighted coefficient is shown in the Table 1.

<table>
<thead>
<tr>
<th>A(or $\alpha$)</th>
<th>$A_0$</th>
<th>$A_1$</th>
<th>$A_2$</th>
<th>$A_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (or 0)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1 (or $\pi/2$)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2 (or $\pi$)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3 (or $3\pi/2$)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

III. Additive axiom: For real numbers $\alpha$ and $\beta$, the GWFRFT operator $F^\alpha_w$ has the following additive property

$$F^\alpha_w F^\beta_w = F^\beta_w F^\alpha_w = F^{\alpha+\beta}_w$$ \hspace{1cm} (9)

So using these properties and calculating the value of coefficient $A_l(\alpha)$ the final equation of generalized weighted fractional Fourier transform comes out to be

$$F^\alpha_{w(M,N)}[s(t)] = \sum_{j=0}^{3} \sum_{k=0}^{3} \exp\{(-j2\pi / 4)((4m_j + 1)\alpha(4n_k + k) - kl)]F^l[s(t)]$$ \hspace{1cm} (10)
3. PROPOSED IDEA OF DOUBLE IMAGE ENCRYPTION BASED ON RANDOM PHASE ENCODING USING GWFRFT

Most of the encryption techniques in the literature are dealing with a single amplitude image (i.e., binary text, grayscale or color image). However, in some cases, one need to encrypt two images with certain relations such as two pictures of an object or a picture and its binary text for description, etc., which are often stored or transmitted together. Encrypting the two images directly using the single-image encryption algorithms mentioned in the literature results in two separate encrypted images with random noise distribution, and sometimes, there arises the difficulty in distinguishing between them before decryption and the decryption has to be conducted twice to recover the two images. Multiple images can also be encrypted by using wavelength multiplexing [18] or position multiplexing methods [21], but the qualities of decrypted images are not perfect due to the cross-talk effects between images. Inspired by the architecture of the fully phase encoding [2, 17] and pixel scrambling (random shifting) techniques [18, 20]. The schematic of a method which can convert two images into one encrypted image based on the random phase encoding in the generalized weighted fractional Fourier domain is given in Fig 1.

Let $f(x_0)$ and $g(x_0)$ represent the two primary normalized amplitude images to be encrypted together, $J$ denotes the pixel scrambling operation [20], which interchanges the pixels according to some random permutation, and the image can be retrieved by repositioning the disturbed image according to the special order. For encryption, the pixel scrambling is applied to one of the primary images $g(x_0)$, and then, the scrambled result $J [g(x_0)]$ is encoded into a phase only function, which can be mathematically expressed as $\exp[j \pi J [g(x_0)]]$, within the range $[0, \pi]$ of the phase variation.

![Fig 1: Schematic of double image encryption](image)

The resulting function is multiplied by the other primary image $f(x_0)$ to obtain the complex combination signal

$$C(x_0) = f(x_0) \exp[j \pi J [g(x_0)]]$$ (11)

Let us consider $R_1=\exp[j \varphi_1(x_0)]$ and $R_2=\exp[j \varphi_2(x_a)]$ are the two random phase masks, where $\varphi_1(x_0)$ and $\varphi_2(x_a)$ are statistically independent white sequences uniformly distributed in $[0, 2\pi]$. As shown in Fig 1, $C(x_0)$ is first multiplied by the first random phase mask $R_1$, then transformed by GWFRFT with order $\alpha$ with two 4-D vectors $(M_1, N_1)$, multiplied by the second random phase mask $R_2$, and then transformed by GWFRFT with order $\beta$ with two 4-D vectors $(M_2, N_2)$. Thus, we obtain the final expression of the output encrypted image $\psi(x_b)$, which is given by

$$\psi(x_b) = F_{w(M_2,N_2)}^{\beta} \cdot \{ [F_{w(M_1,N_1)}^{\alpha} \cdot (C(x_0) \otimes \exp[j \varphi_1(x_0)])] \otimes \exp[j \varphi_2(x_a)] \}$$ (12)

Where $\otimes$ represent the element-by-element multiplication operation of matrices and the input image for encryption `f` is assumed to be real and nonnegative.
The Decryption shown in Fig 2 is the reverse process of the encryption. For decryption, $\psi(x_b)$ is transformed by the $-\beta th$ GWFRFT and the resultant function is multiplied by the conjugate of the second random phase mask $R_2$, then GWFRFT of order $-\alpha th$ is then applied, resulting in the following decrypted combination function $C(x_0)$ after multiplying by the conjugate of the first random phase mask $R_1$ i.e.

$$C(x_0) = \{F^{-\alpha}_{w(M_1,N_1)} \cdot [(F^{-\beta}_{w(M_2,N_2)} \cdot \psi(x_b)) \otimes \exp(-j\phi_1(x_0))] \otimes \exp(-j\phi_2(x_0))] \}$$

(13)

Now the amplitude-based image $f(x_0)$ can be simply retrieved from the decoded $C(x_0)$ by taking amplitude, whereas the phase-based image $g(x_0)$ requires extracting the phase of $C(x_0)$, and dividing it by $\pi$, then taking the inverse pixel scrambling transform denoted by $J^{-1}$ as shown in Fig 2.

![Fig 2: Schematic of double image decryption](image)

3. SIMULATION RESULTS

Computer simulations are performed to verify the proposed encryption technique for double images. Two types of amplitude image, image of college main gate and college logo (Fig 3), are serving as the two primary images to be encrypted together. Each of them has a size of $256 \times 256$ pixels. We use college main gate image as the amplitude-based image $f(x_0)$, and college logo image as the phase-based image $g(x_0)$. The two random phase masks, order and 4D vector are as follow $(a, b, c, d)$ is $(0.4, 3.8, 1.7, 2.9)$ and 4D vector are $M1=[\ 1309\ ], M2=[\ 102338\ ], M3=[12309], M4=[42338], N1=[8257], N2=[79464], N3=[925111], N4=[79164]$. 

49
Then the encrypted and decrypted images are shown in fig 4 and 5 respectively.

Fig 3: Primary Images which are used for encryption

Fig 4: Single encrypted image using double random phase encoding using GWFRFT

Fig 5: Decrypted Images after applying the reverse process
4. COMPARISON WITH THE EXISTING TECHNOLOGY

Advanced encryption technique is the symmetric key algorithm similar to double image encryption where we are using the same key for encryption as well as decryption. AES is introduced in year 2001 and since then it is the standard technique for encryption. AES comes for different key sizes like 128 bit, 192 bits or 256 bits.

Number of permutations for AES-128 = $2^{128}$
Number of permutations for AES-192 = $2^{192}$

Now let us calculate the number of permutation required in double image encryption.
Let $M1 = [0-63, 0-63, 0-63, 0-63] = [2^6, 2^6, 2^6, 2^6]$  
Similar to $M1$ other vectors i.e. $M2, M3, M4, N1, N2, N3, N4$ also can take any value between 0-63.
Number of possible permutations from vectors = $(2^6)^32 = 2^{192}$

Now order “a” can take any value between 0-100 with an interval of 0.1 i.e. 0.1 0.2, 0.3, 0.4 and so on.
So Number of possible permutation for order “a” = $1000 = 2^{10}$
Number of possible permutation for order “(a, b, c, d)” = $2^{40}$
So, Total number of possible permutation = $2^{192} * 2^{40} = 2^{232}$

As from this the key size is 232 bits and for this key size AES also require $2^{232}$ permutations so the performance of this encryption technique is comparable to the AES.

5. CONCLUSION

In this paper, a novel approach to implement the image encryption is discussed. As in any encryption the key which is used for encryption serves an important role means larger the number of parameters in the key stronger the encryption techniques. So in GWFRFT, order as well as 4D vectors served as the key making encryption stronger than the encoding in FRFT. To make this encryption technique more efficient and stronger an encryption technique is proposed in which two images is converted into a single complex distribution and finally encrypted into a single image. This proposed encoding technique is successfully implemented for encryption and decryption. And in the last the double image phase random encoding encryption technique is compared with the advanced encryption techniques (AES) using the number of permutation required by the eavesdropper to decode the key in a brute force method of attacking. By this comparison it is clearly shown that proposed encryption technique is more efficient and robust against any attack.

REFERENCES


