ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Image encryption using fractional random wavelet transform

V .Ramamohan Reddy [1], Dr. T.Sreenivasulu Reddy [2]

M.Tech student, Department of ECE, SVU college of Engineering, Tirupati, Andhra Pradesh, India[1]

Associate Professor, Department of ECE, SVU college of Engineering, Tirupati, Andhra Pradesh, India[2]

Abstract-In this paper we proposed fractional random wavelet transform which is generalized form of wavelet transform and fractional random transform. applications of fractional random transform are image security, finger print authentication, etc… in this paper a new algorithm for image encryption using fractional random wavelet transform (FrRnWT) and Arnold cat map is developed. and efficiency of algorithm is obtained by calculating peak signal to noise ratio (PSNR) and universal image quality index(UIQ).

Keywords: DWT, fractional random wavelet transform, Arnold cat map, PSNR, UIQ

I. INTRODUCTION

Encryption is nothing but coding the data in un readable form by using different algorithms. We can encrypt the images by shuffling pixels for secure transmission. Encryption of data or image is called as cryptography.

A. Discrete Wavelet Transform (DWT):

1-D DWT can be extended to 2-D transform using separable low pass & high pass wavelet filters. With separable filters, applying a 1-D transform to all the rows of the input and then repeating on all of the columns can compute the 2-D transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. As depicted in Figure 2.1(c), the four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass or high pass filter to the rows, and the second letter refers to the filter applied to the columns.

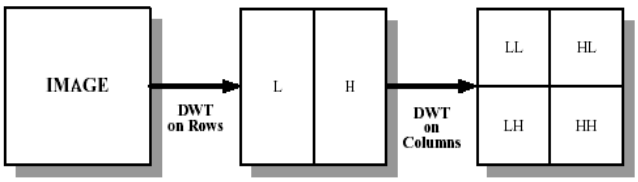

Fig 1. Block Diagram of DWT (a) Original Image (b) Output image after the 1-D applied on Row input (c) Output image after the second 1-D applied on row input.

B. Arnold cat map(ACM):

Arnold cat map is simple mathematical relation which is used for image encryption by shuffling the image pixels. ACM rearranges the pixels of image. The ACM is mathematically represented by the following map,

$$\Gamma: \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix};$$

Here we can see more clearly what p and q are. There are a few conditions for the parameters p, q, they both need to be integers and the

$$\det\left(\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}\right)=1,$$

Therefore making it area preserving, this will keep the size of the image the same throughout the iterations.

C. Fractional random wavelet transform:

Fractional random transform for image is obtained by as following procedure

1).first we apply the fractional random transform for an image. This is given below.

The DFRNT can be defined by a symmetric random matrix Q. The matrix Q is generated by an N × N real random matrix P with a relation of

$$\mathbf{Q = (P + \text{trans}\,(P))\,/\,2}$$

We can also calculate N real orthogonal Eigen vectors of matrix Q. these eigen vectors are normalized using gram schmidt standard normalization procedure. Then we have N orthonormal vectors{v1,v2,v3…..vN}. from these column vectors form the matrix

$$V = [v1\ v2\ v3 \ldots vN]$$

The coefficient matrix, corresponds to the eigen values of discrete fractional random transform can be defined as

$$D=\text{diag}(1,\exp(-2\pi\alpha/M),\exp(-4\pi\alpha/M)\ldots..\exp(-2(N-1)\pi\alpha/M))$$

In above equation there is no jump for odd and even integer N. We introduce here an integer number M in the coefficients. It indicates the periodicity of DFRNT with respect to the fractional order whose significance will be shown below. The kernel transform matrix of DFRNT can thus be expressed as

$$R\alpha=V*D*\text{trans}\,(V)$$

Therefore the DFRNT of a one-dimensional discrete signal is written as

$$DFRNT(x) = R\alpha * x$$

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

The expansion of DFRNT for two dimensional signal is straightforward as

$$DFRNT(x) = R\alpha * x * trans(R\alpha)$$

2).then applying DWT for fractional random transformed image we can fractional random wavelet transform.
3). Reconstruction of image is obtained by applying IDWT and -α order fractional random transform.

II. PROPOSED METHOD

A. Encryption:

Encryption of image is explained below step by step. It is done at transmission end.

1).first decompose the image using fractional random wave let transform as four sub bands LL, LH, HL,HH
2).shuffle the coefficients of LL, LH, HL, and HH by using Arnold cat map s1, s2, s3, s4 times respectively.
3).apply the inverse fractional random wavelet transform for shuffled sub bands .then we get the encrypted image.

Encryption process is shown below by flow chart.

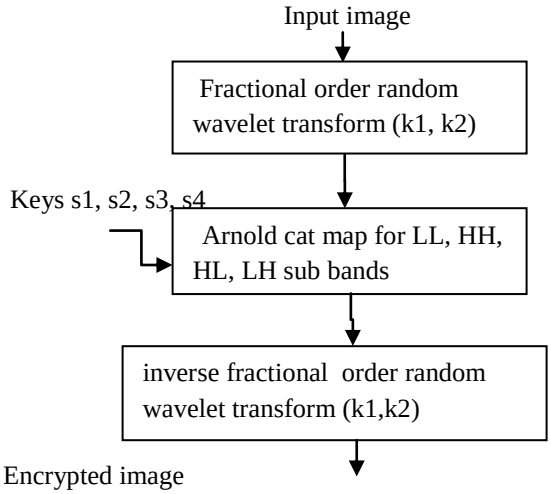

Fig 2. The algorithm for encryption

B. Decryption:

Decryption process is explained below step by step as follows. it is done at receiving end.

1).received encrypted image is decomposed using fractional random wavelet transform. Then we get four sub bands LL, HL, LH, HH.
2). shuffle the coefficients of LL, LH, HL, HH by using Arnold cat map T-s1,T-s2,T-s3,T-s4 times respectively. Where T is period sub bands.
3).apply inverse fractional random wavelet transform for shuffled sub bands. Then we get the original image.

Decryption process shown below by flow chart

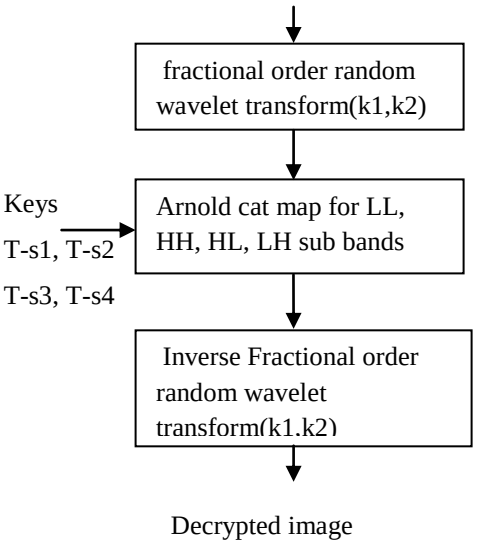

Fig 3. The algorithm for decryption

III. RESULTS

Efficiency of this algorithm is obtained by calculatig the peak signal to noise ratio(PSNR), universal image quality index(UIQ). PSNR value is obtained by the following formula.

$$PSNR=10*\log10(255\hat{}2/MSE)$$

Where MSE is mean square error calculated between the original image and decrypted image.

Fig 3Original image

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

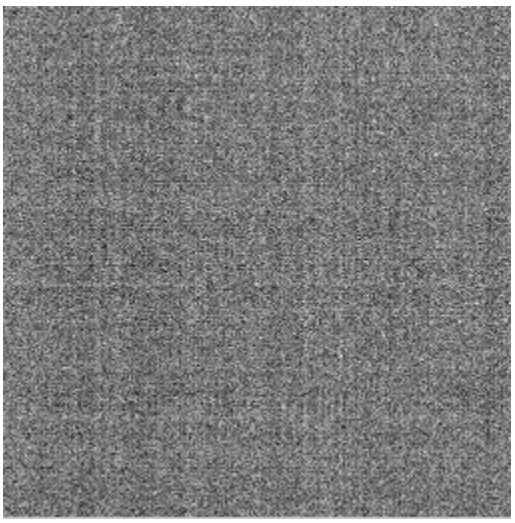

Fig 4 encrypted image

Fig 5 decrypted image

Fig6 decrypted image

Fig4 is encrypted image of input image when keys k1=0.33 k2=0.66 s1=12 s2=23 s3=34 s4=45. Fig5 is decrypted image when correct keys
are used. Fig6 is decrypted image when k1 is entered as 0.55 instead of 0.33 and all other keys entered correctly.

PSNR and UIQ values are calculated and tabulated below

Table 1

metric	**Values between fig 3 and**	
	Fig 5	**Fig 6**
PSNR	304	9.37
UIQ	0.9955	0.0014

IV .CONCLUSIONS

In this paper, a new fractional random wavelet transform is defined which consists all properties of wavelet transform and random fractional transform image encryption achieved by using this transform along with the logistic and Arnold catmap. This technique is suitable for securing the images during communicating on insecure channel.

V. REFERENCES

[1] "A New Fractional Random Wavelet Transform for Fingerprint Security "IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, VOL. 42, NO. 1, JANUARY 2012 , 1083-4427/$26.00 © 2011 IEEEGaurav Bhatnagar, Member, IEEE,Q. M. Jonathan Wu, Senior Member, IEEE, and Balasubramanian Raman, Member, IEEE.

[2] "A discrete fractional random transform"Zhengjun Liu, Haifa Zhao, Shutian Liu Harbin Institute of Technology, Department of Physics, Harbin 150001 P. R.CHINA

[3] V. Namias, "The fractional order Fourier transform and its application toquantum mechanics," J. Inst. Math. Appl., vol. 25, no. 3, pp. 241–265,Mar. 1980.,

[4] Z. Liu and S. Liu, "Random fractional Fourier transform," Opt. Lett..vol. 32, no. 15, pp. 2088–2090, Aug. 2007.

[5] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1996.