JAUES

Journal Of Al-Azhar University Engineering Sector

Vol. 14, No. 51, April, 2019, 575-587

COMPARITIVE STUDY BTEWEEN DES ALGORITHM, AND FRFT FOR DATA ENCRYPTION USING FPGA

Ahmed Elbadawy.Rabie, Ali.Rashed, Khaled. El Shafie, and Mohammed.Rohiem
Computers and systems engineering department, faculty of engineering, EL AZHR University, Cairo, Egypt,

ABSTRACT
Cryptography techniques need some algorithms for encryption of data. Many of available encryption techniques are used for textual data, a few of encryption methods are used for multimedia data; however, this algorithms that are used for textual data may be inefficient for multimedia. The most popular symmetric key algorithms are Data Encryption Standard (DES). However, DES may not be suitable for multimedia because it consumes times. Encryption and decryption of these data require different methods. This paper proposes an encryption and decryption of data by using the nature of Fractional Fourier Transform (FrFT) in signals analysis, based on multi-order FrFT. A different indicators to evaluate the security of an encryption technique have been discussed. These indicators are: sensitivity proposed techniques for the key, the complexity of the processes, and statistical analysis. The key is formed by combination of order of FrFT. The encrypted data is obtained by the summation of different orders. Numerical simulation results are given to demonstrate this proposed method.

KEYWORDS: Data Encryption Standard (DES); Fractional Fourier Transform (FrFT); Xilinx Platform Studio (XPS); Field-Programmable Gate Array (FPGA); Symmetric Key Cryptography.

1. INTRODUCTION
The encryption plays a major role in securing the data in transmission [1]. Different encryption techniques are used to protect confidential data from unauthorized uses. Cryptography technique needs some algorithms for encryption of data [2]. One of The most popular symmetric key algorithms is Data Encryption Standard (DES).
A 64-bits key are used with DES, while 128,192,256 bits keys uses for AES [3]. DES, AES offer the greatest security to sensitive data compared to other cryptographic algorithms. The AES was accepted as a standard in November 2001 [4].
One of the most popular tools used in signal processing and analysis are the fourier transform (FT) [5]. The idea of fractional powers of the fourier operator appears in the mathematical literature as early as 1929 [6 - 8]. It has been rediscovered in quantum mechanics [9, 10], optics [11 - 13], and signal processing [14]. The fractional Fourier transform (FrFT) was mathematically introduced by Namias in 1980. Recently, Mendlovic and Ozaktas introduced a new tool for image analysis in optics [15, 16].
The remaining sections are: a literature review has been introduced in section 2, the proposed data encryption method has been introduced in Section 3, comparative study between DES algorithm and FrFT has been introduced in section 4, in section 5 implementation of DES using FPGA are performed. A brief conclusion has been introduced in Section 6.

2. LITERATURE REVIEW

The literature review includes a brief description of the cryptographic algorithms: symmetric cipher such as DES, and theory of FrFT.

2.1. Data Encryption Standard (DES)

The DES is a block cipher developed by IBM and NIST (National Institute Standard Technology) in the 1970s as a modification of the previous system called LUCIFER, DES operates on blocks of 64-bits at a time, the input key is 64 bits. Every 8th bit in the input key is a parity check bit which means that in fact the key size is effectively reduced to 56 bits. DES consists of 16-rounds of substitution and permutation as shown in Fig.1 and Fig 2

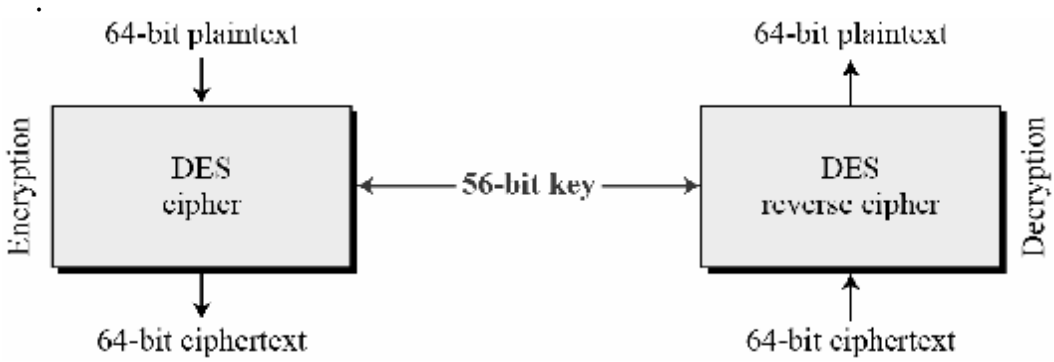

Fig.1. DES Encryption and Decryption Process

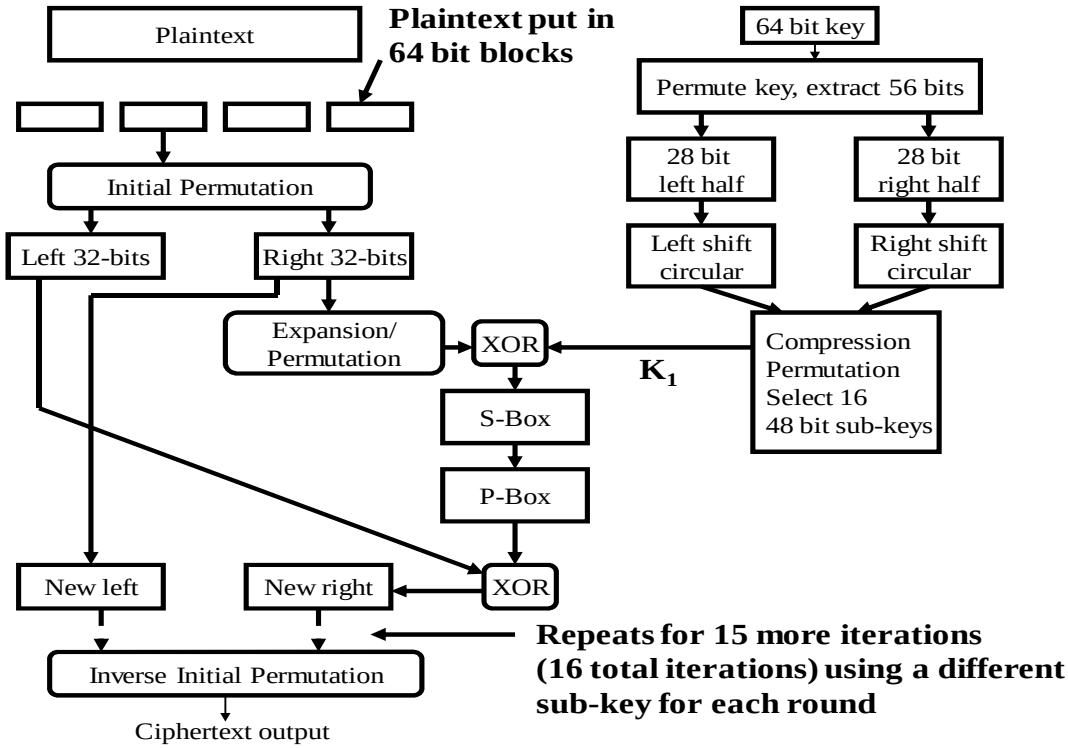

Fig.2. DES Algorithm

2.2. Theory of Fractional Fourier Transform

The Fourier transform is a rotation by angle $\pi/2$ in the time-frequency plane, the fractional Fourier transform interpreted as the counterclockwise rotation by an angle α in the time-frequency plane. FRFT is the generalization of the classical FT.

Conventionally, *FrFT* of α order of input function $x(t)$ can be defined as follows [17]:

$$X_a(u) = \int_{-\infty}^{\infty} x(t)\, K_a(t,u)\, dt \tag{1}$$

Where $k_\alpha(t,u)$ of transform is:

$$K_a(t,u) = C_a\, e^{-i\frac{ut}{\sin a} + \frac{i}{2}(t^2+u^2)\cot a} \tag{2}$$

And

$$C_a = \sqrt{\frac{-ie^{ia}}{2p\sin a}} = \sqrt{\frac{1-i\cot a}{2p}}$$

$$K_a(t,u) = \sqrt{\frac{1-i\cot a}{2p}}\, e^{\frac{i}{2}((t^2+u^2)\cot a - iut\csc a)} \tag{3}$$

$x(t)$ signal recovered by FrFT operation with backward angels –α:

$$x(t) = \int_{-\infty}^{\infty} X_a(u)\, K_{-a}(t,u)\, du \tag{4}$$

The 2-D FrFT of a function $f(x,y)$ can be define as:

$$f^{a_x a_y}[FrFT[f(x,y)]](u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(x,y) K_{a_x a_y}(x,y;u,v)\, dxdy \tag{5}$$

Where $K_{a_x}(x,u) = C_a\, e^{i/2[x^2+u^2]\cot a_x - ixu\csc a_x}$ (6)

Then, *by* substituting ***y*** for ***x*** and ***v*** for ***u,*** *y-axis,* $K_{a_y}(y,v)$ can be obtained.

The signal $f(x,y)$ can be recovered by FrFT operation with backward angles($-\alpha_x$,$-\alpha_y$):

$$f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_a(u,v) K_{-a_x-a_y}(x,y;u,v)\, dudv \tag{7}$$

$$K_{-a_x-a_y}(x,y;u,v) = K_{-a_x}(x,u) K_{-a_y}(y,v) \tag{8}$$

3. PROPOSED APPROACH

The proposed encryption technique is shown in Fig.3. The original data *S* represents the input data to be encrypted Using FrFT. In Encryption steps based on FrFT, we use one – dimensional analysis to describe our methods, then we can extend all formulae to Two-dimensions. To obtain encrypted data, firstly, input data is multiplied by matrix R, and their results are transformed through first FrFT system with first order of transform a_1 to get data, the result from this stage is transformed through second order of transform a_2 by taking second FrFT, then it passes the result by taking FrFT with third order of transform a_3 to get encrypted data 'L', The encrypted data is obtain by summations of different orders, and the key for encryption/decryption process is a combination of order of Fractional Fourier Transform and matrix R. Encryption model as shown in Fig.3. Is secure and more robust towards brute force attack, but the complexity of the system is increased.

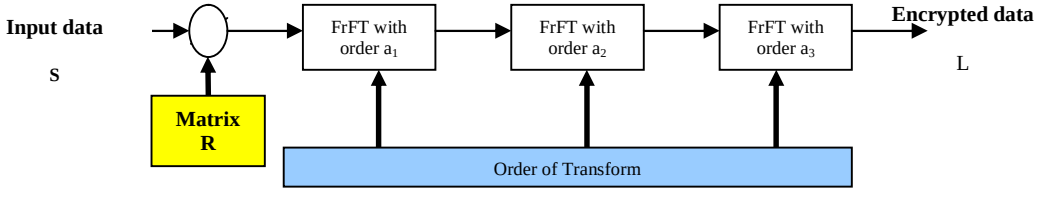

Fig.3. Proposed Encryption System

In decryption process, the reverse for encryption process, is applied as shown in Fig.4. Firstly, transformed encrypted data 'L' through first FrFT with order of transform $-a_3$, and passes the result again through second FrFT with order of transform $-a_2$, then the result from last stage passes through last FrFT with order of transform $-a_1$, finally, the result is multiplied with matrix conjugate of the matrix R^* to get input data S.

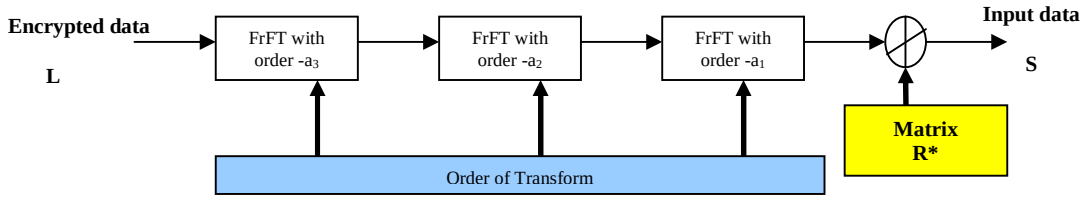

Fig.4. Proposed Decryption System

3.1. Example 1: Enc/Dec Proposed Method for an Image:

Mathematically, the encryption process in Fig.3, Summarized as: input data *S(x,y)* is multiplied with matrix R and passes through *FrFT* with order a_1 till a_k ; as in equations bellow:

$$L' = S_{(x,y)} \times R \tag{9}$$

$$L'' = F_{a_1}[S_{(x,y)} \times R] \tag{10}$$

$$L''' = F_{a_2}[F_{a_1}[S_{(x,y)} \times R]] \tag{11}$$

Encrypted data is given by:

$$L'''' = \sum_{k=1}^{k=3} F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]] \tag{12}$$

The decryption process is in Fig.4 and mathematically is given as:

$$L'''' = F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]]$$

$$L''' = F_{-a_k}[F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]]] \tag{13}$$

$$L'' = F_{-a_2}[F_{-a_k}[F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]]]] \tag{14}$$

$$L' = F_{-a_1}[F_{-a_2}[F_{-a_k}[F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]]]]] \tag{15}$$

Finally; decrypted image is given by:

$$L = F_{-a_1}[F_{-a_2}[F_{-a_k}[F_{a_k}[F_{a_2}[F_{a_1}[S_{(x,y)} \times R]]]]]] \times R^* \tag{16}$$

The time in seconds for encryption and decryption operations of an Image, and audio signals are shown in Table 1 and Table 2.

Table 1. Encryption / Decryption Time of proposed method for an Image

Image Name	DES [23]	AES [23]	Proposed Enc/Dec system based on Three FrFT
Average Time (s)	215.9359 / 183.5455	99.871 / 84.8904	6.8726 / 5.84032

Table 2 Encryption / Decryption Time of proposed method for an Audio

Audio	DES [24]	AES [24]	Proposed Enc/Dec system based on Three FrFT
Average Time (s)	32 / 23	54 / 53	4.04005 / 5.98425

Table 3 Encryption / Decryption Time of proposed method for a Text [25]

Text1	DES [25]	AES [25]	Proposed Enc/Dec system based on Three FrFT
Average Time (s)	5.07 / 5.01	3.8 / 3.08	4.2932 / 3.1719

4.6 Example 2: Enc/Dec Proposed Method for Audio Files

Another type of data is an audio signal. Audio cryptography encryption is the method of including the key to the plain audio, while decryption is the process of taking out the original plain back by using the same key.

In this part we offer the possibility of encryption and decryption for data by using our proposed methods with FrFT for an audio signal, through use of the nature of FrFT in signals analysis, Fig.5., and Fig.6. shows original audio1 and histogram.

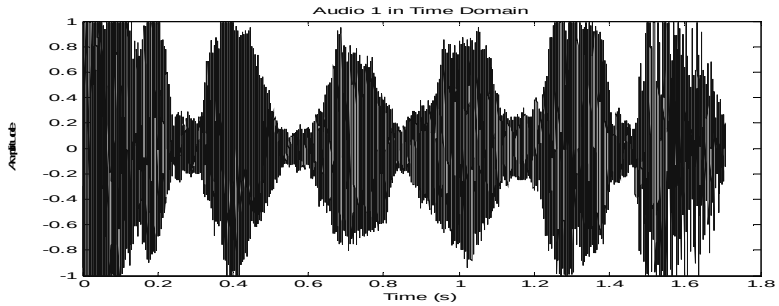

Fig.5. original Audio1

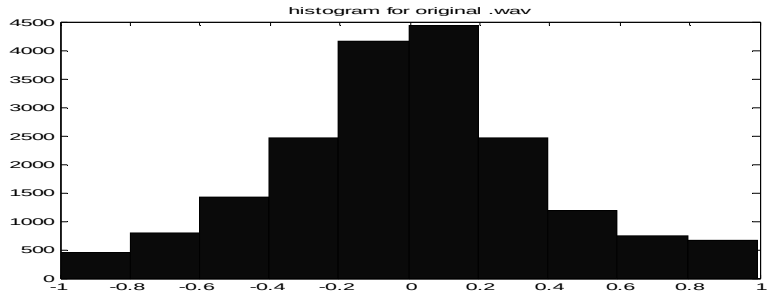

Fig.6. Audio1 histogram

Fig.7. is shows encrypted audio1 signal with FrFT, while Fig.8. shows decrypted audio1 signal (reconstructed audio1).

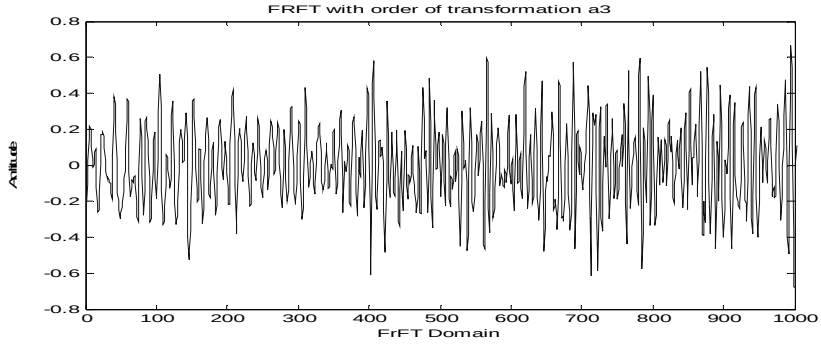

Fig.7. third FrFT for audio signal (Encrypted)

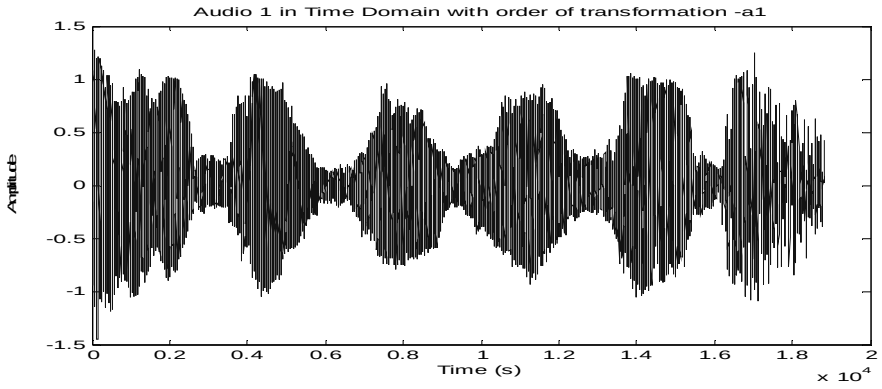

Fig.8. Reconstructed audio1 signal (Decrypted)

4. COMPARATIVE STUDY BETWEEN DES & FrFT USING SOFTWARE SIMULATIOM

Computer simulations have been done of the proposed encryption technique. The image is shown in Fig.9., is "Image1" and 140 x 200 pixels, and 28.8 KB size of data; and the matrix R; orders of transform a_1, a_2, And a_3.

Fig.9. Original Image1

A good encryption algorithm should always resist the known attacks. The security analysis of encryption techniques can be done by using following parameters execution time, sensitivity to the key, information hiding, and statistical analysis . A simulation result has been discussed and it will be seen that data encryption based on FrFT provided criteria for security.

4.1. Security Analysis

4.1.1. Key space analysis:

Let us suppose that an encryption scheme has k-bit key. So an attacker needs 2^k operations to determine the key. The key in our proposed encryption methods based on FrFT is formed by combination of orders of transform values of Fractional Fourier Transform and matrix R.

4.1.2. Sensitivity to key:

If we encrypt data by K_1 and decrypt by a different key K_2, decryption should be unsuccessful. Our Proposed method is sensitive to the key changes. Fig.10. and Fig.11. shows decryption with correct and incorrect keys.

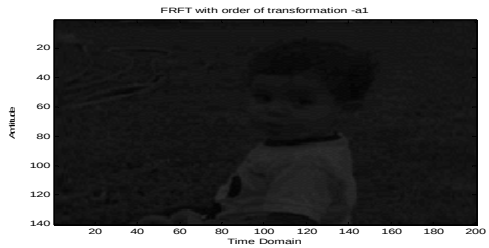

Fig.11. Decrypted Image1 with correct Key

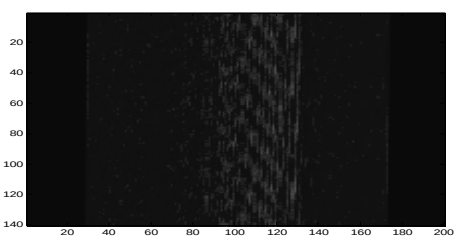

Fig.10. Decrypted Image1 with Incorrect Key

4.1.3. Information hiding:

One of the important properties provided by encryption techniques is information hiding. It means that no information of original data can be extracted from the encrypted. Our encryption method is encrypting data successfully, and no information of original data can be extracted as shown in Fig.12 and Fig.13.

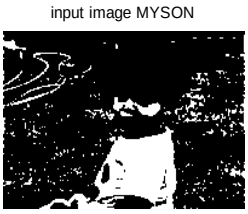

Fig.12. Original Image1

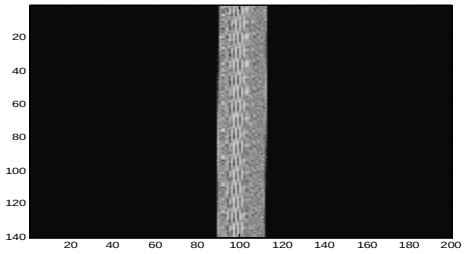

Fig.13. Encrypted Image1

4.3 Statistical Analysis:

Statistical analysis has been performed by calculating the histograms.

4.3.1 Histograms Analysis: one of the important features in data statistical analysis is Histogram. When encrypted data have a uniform histogram distribution, no useful information according to the statistical properties can be obtained. Fig.14 and Fig.15 are two gray images: Image1 and Image4, respectively.

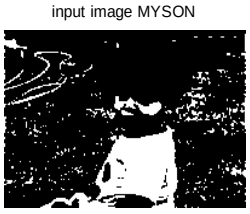

Fig.14. Original Image1

Fig.15. Original Image4

The histograms in Fig.16 and Fig.17 illustrate the original images pixels distributed at each gray level.

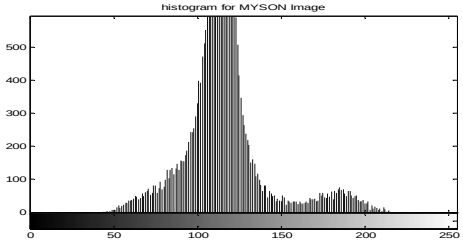

Fig.16. Image1 histogram

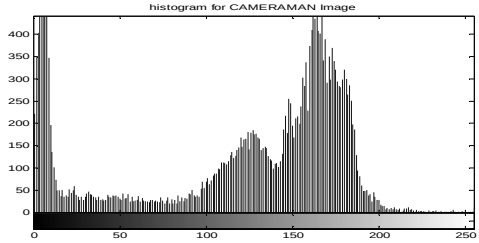

Fig.17. Image4 histogram

The histogram of two images is very different as shown in Fig.16 and Fig.17. The histograms of the encrypted images Image1 and Image4 as shown in Fig.18 and Fig.19 are quite similar.

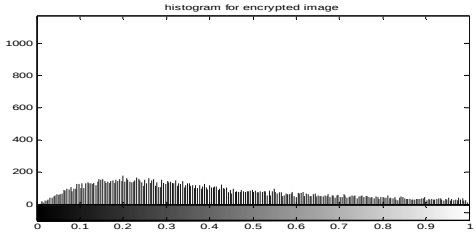

Fig.18. Histogram for encrypted Image1

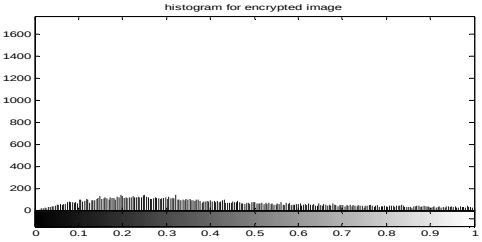

Fig.19. Histogram for encrypted Image4

From Fig.18 and Fig.19, the cipher data of both different original data have similar histograms, according to statistical properties, attackers cannot obtain useful information.
The performance of the encryption and decryption approach is evaluated based on MSE and PSNR. The Mean Square Error (MSE) defined as a function of the errors in the decrypted fractional orders. Let **o** (i,j) and **r**(i,j) is values of the original and the recovered at the pixel (i,j), where M and N indicted the size. the MSE defined as follows in Eq. (17) [19,20] [24-30]::

$$MSE = \|r - o\|^2 = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |r(i, j) - o(i, j)|^2 \quad (17)$$

to evaluate an encryption scheme and encryption quality Peak signal-to noise ratio (PSNR) can be used. PSNR is usually expressed in decibels. Mathematically, PSNR can be described in Eq. (18) [20] [24-30]::

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (18)$$

The experimental results that show the MSE and PSNR for an Image are shown in Table 4, and Table 5.

Table 4. Mean Square Error

Image	DES	Proposed Enc/Dec system based on Three FrFT
Average MSE	0.202	0.226

Table 5. Peak Signal to Noise Ratio (db)

Image	DES	Proposed Enc/Dec system based on Three FrFT
Average PSNR	55.329	54.587

The experimental results that show the MSE and PSNR for an Audio are shown in Table 6, and Table 7.

Table 6. Mean Square Error

Audio	Proposed Enc/Dec system based on Three FrFT
Average	0.0192

Table 7. Peak Signal to Noise Ratio

Audio	Proposed Enc/Dec system based on Three FrFT
Average	66.36

4.4 Differential Analysis

In image encryption, the cipher resistance to differential attacks is commonly analyzed via the NPCR and UACI tests [19,20]. Number of Pixels Change Rate while one pixel of plain image is changed is refers to Number of Pixels Change Rate (NPCR). To determines the average intensity of differences between the plain and ciphered, Unified Average Changing Intensity (UACI) is using. The NPCR and the UACI are defined in Eq. (19) and Eq. (21):

$$NPCR = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100 \% \quad (19)$$

where C1 and C2 are two cipher-images whose plain are different by only one bit. The gray value at grid (i; j) in C1 and C2, by C1(i; j) and C2(i; j). D array is determined by C1(i; j) and C2(i; j), if C1(i; j) = C2(i; j) then D(i; j) = 0 ; otherwise, D(i; j) = 1.
D (i, j) is defined as in Eq. (20) [21] [24-30]::

$$D(i,j) = \left\{ \begin{matrix} 0, if\ .C_1(i,j) = C_2(i,j) \\ 1, if\ .C_1(i,j) \neq C_2(i,j) \end{matrix} \right\} \quad (20)$$

UACI Mathematically can define in Eq. (21) [21]:

$$UACI = \frac{1}{M \times N} \sum_{i,j} [\frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100 \quad \% \quad (21)$$

Table 8. NPCR value for proposed method

Image	Proposed Enc/Dec system based on Three FrFT
Average	97.493

Table 9. UACI value for proposed method

Image	Proposed Enc/Dec system based on Three FrFT
Average	34.16

4.5 Correlation Coefficient Analysis

The relationship and similarity between two variables are described by Correlation. If correlation coefficient is equal to one, then two data are identical and they are in perfect correlation, In case of perfect correlation (correlation coefficient is equal to 1). Encryption process completely fails because the encrypted data is same as the plain data, When correlation coefficient is -1 then encrypted is negative of original (plain). Mathematically correlation coefficient can be shown as in Eq. (22) [19,20] [24-30]:

$$\text{Correlation Coefficient} = \frac{\sum_{i=1}^{N} (c_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N} c_i - E(x)^2))} \sqrt{\sum_{i=1}^{N} y_i - E(y)^2))} \quad (22)$$

Where $E(x) = \frac{1}{N} \sum_{i=1}^{N} x_{,i}$ x and y are values of the plain and cipher data.

The values of the Correlation Coefficient between original, encrypted, and decrypted Images are showing in Table 10, and Table 11.

Table 10. Correlation Coefficient between original and encrypted Image

Image	Proposed Enc/Dec system based on Three FrFT
Average	0.108

Table 11. Correlation Coefficient between original and decrypted Image

Image	Proposed Enc/Dec system based on Three FrFT
Average	0.991

The values of the Correlation Coefficient between original, encrypted, and decrypted audio are showing in Table 12, and Table 13.

Table 12. Correlation coefficient between original and encrypted Audio

Audio	Proposed Enc/Dec system based on Three FrFT
Average	0.011

Table 13. Correlation coefficient between original and decrypted Audio

Audio	Proposed Enc/Dec system based on Three FrFT
Average	0.968

Table 14 is shows a comparative study, between DES, AES [23], and proposed encryption-decryption system based-on FrFT.

Table 14. Experimental Analysis of DES and Proposed Enc / Dec system based on FrFT

Parameters	DES [23]	AES [23]	Proposed Enc/Dec system based on three FrFT
Encryption Time (in sec)	215.9359	99.871	6.8726
Decryption Time (in sec)	183.5455	84.8904	5.84032
MSE	0.226	0.007	0.226
PSNR(db)	54.587	69.7082	54.587
NPCR (%)	99.6643	99.60	97.493
UACI (%)	51.249	33.53	34.16

5. HARDWARE IMPLEMENTATION OF DES USING FPGA

5.1 Simulation Results of DES algorithm:

In this section, analysis of the simulation results has been introduced, Fig.20. and Fig.21. shows Xilinx Platform Studio and Graphical design view. Fig.22. shows the block of DES algorithms showing input and output pins, in this we give 64-bit data and 64-bit key, so that it gives us 64-bit encrypted data after whole encryption 16 rounds

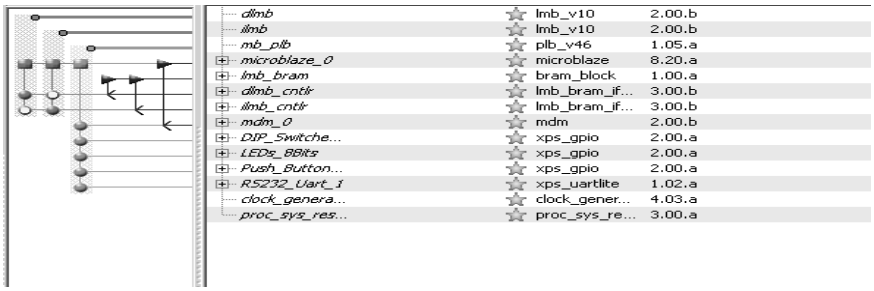

Fig. 20 Xilinx Platform Studio - system assembly view

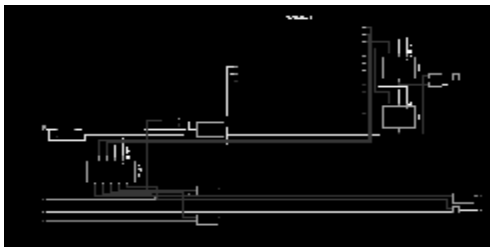

Fig. 21 Graphical design view

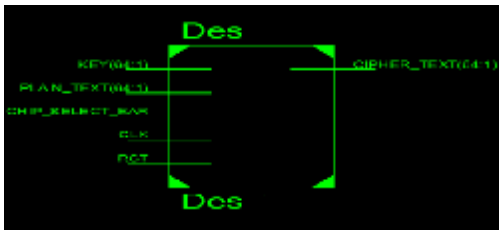

Fig.22. DES block

Fig.23. is show the simulated result of encryption and decryption on ISE13.1.

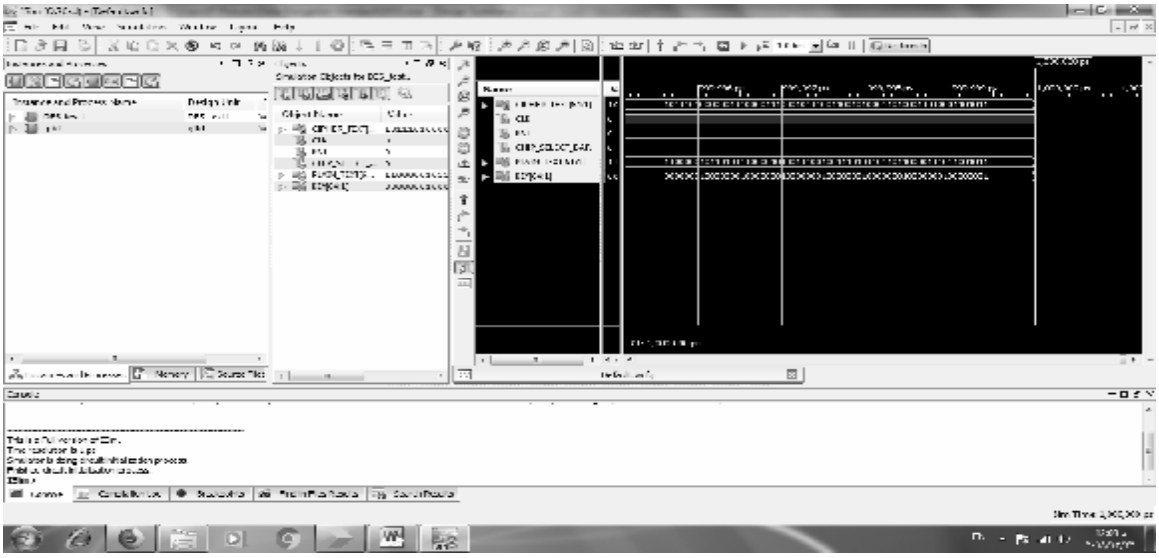

Fig. 23 Simulation results of DES using Xilinx ISE

Plain-Text (64bit)
1011101000000111000011100010111001100101000110100011010001101011
Key (64bit)
1100000101101011100001010011100100111010110110110000111011001011
Cipher-Text (64bit)
0000000100000001000000010000000100000001000000010000000100000001
RST : 0
CLK : 0

6. CONCLUSIONS

Nowadays the security of data in the digital world becomes more and more important. A method to encrypt and decrypt data based on multi-order Fractional Fourier Transform has been introduced. Compared with the traditional Fourier method, FrFT is safer in encryption operations because it can provide additional cryptographic keys to make it more difficult to break. The key is formed by combination of order of Fractional Fourier Transform. Indicators that are used to measure the security of the encryption method such as: the key space analysis, statistical analysis, and key sensitivity analysis, have been carrying out to demonstrate the security of the data encryption techniques.

To evaluate the encryption performance and quality of the proposed schemes, the mean square error (MSE), peak signal to noise ratio (PSNR), number of pixel change rate (NPCR), and unified average change intensity (UACI) have been introduced. to measure the number of changing pixels and the number of averaged changed intensity between cipher data, the NPCR and UACI have been introduced, respectively.

Implementation of DES algorithm using FPGA has been introduced, FPGA implantation of DES Algorithm, and the simulation result performed on Xilinx ISE for implementing encryption and decryption module, with NEYXS 3 FPGA board.

The use of FrFT in data encryption may better than DES in time to encryption and decryption operations, and design, because it provides a little number of rounds, unlike cryptographic algorithms that need a fixed number of encryption rounds. The use of FrFT for encryption offers a safe way for data encryption without adding additional costs or burdens and up nearly applicable safety standard in encryption systems.

REFERENCES

1. Zaidan .A.A., Zaidan .B.B., and Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology (WASET),Vol,54, No: 2070-3724, pp.468-479.
2. M.Kaur, S.Kaur , " Survey of Various Encryption Techniques for Audio Data", Fatehgarh Sahib, Punjab, India, Volume 4, Issue 5, May 2014, ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.
3. SCHNEIER.B., Applied Cryptography: Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc. 2nd Ed, 1996.
4. Bracewell.R.N., The Fourier transforms and its applications, McGraw-Hill ,1986.
5. Namias.V., The fractional order Fourier transform and its application in quantum mechanics.J., Inst. Math. Appl, 25:241–265, 1980.
6. Alieva T., Lopez,V., Agullo-Lopez .F., and Almeida.L.B., "The fractional Fourier transform in optical propagation problems". J. Mod. Opt., 41:1037–1044, 1994.
7. Almeida.L.B., The fractional Fourier transform and time-frequency representation. IEEE Trans. Sig. Proc., 42:3084–3091, 1994.
8. Ozaktas.H.M., and Mendlovic.D., "Fractional Fourier transforms and their optical implementation: II," J. Opt. Soc. Am. A 10, 2522–2531, 1993.
9. Namias.V., "The fractional Fourier transform and its application in quantum mechanics," J. Inst. Math. It's Appl. 25, 241–265, 1980.
10. FIPS FIPS-197, Federal Information Processing, Standards Publication FIPS-197,Advanced Encryption, Standard(AES),http://csrc.nist.gov/publications/fips/fips 197/fips-197.pdf, 1999.
11. Unnikrishnan.G., Joseph.J., and Singh.K., Opt.Lett., 25, 887, 2000.
12. Qing Guo, Jun Guo, Zhengjun Liu, and Shutian Liu. An adaptive watermarking using fractal dimension based on random fractional Fourier transform, Opt. Laser Technol, pp. 124 – 129, 2012.
13. Sanjay Rawat, Balasubramanian Raman. "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography", Signal Process, pp. 1480 – 1491, 2012.
14. Linfei Chen, Daomu Zhao, Fan Ge. Gray images embedded in a color image and encrypted with FRFT and Region Shift Encoding methods, Opt. Commun, pp. 2043 – 2049, 2010.
15. Zhengjun Liu, Qiuming Li, Jingmin Dai, Xiaogang Sun, Shutian Liu, and Muhammad Ashfaq Ahmad. A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transforms domains, Opt. Commun, pp. 1536 – 1540, 2009.
16. Xiang Peng, Lingfeng Yu, and Lilong Cai. Digital watermarking in three-dimensional space with a virtual-optics imaging modality, Opt. Commun, pp. 155 – 16, 2003.
17. Anoop M.S, Public key Cryptography (Applications Algorithm and Mathematical Explanations).
18. Ozaktas.H.M., Zalevsky.Z., and Kutay.M.A., "The Fractional Fourier Transform with Applications in Optics and Signal Processing", Wiley, new yourk, 2001.
19. Shraddha Soni, Himani Agrawal, and Dr. (Mrs.) Monisha Sharma, International Journal of Engineering and Innovative Technology (IJEIT),"Analysis and Comparison between AES and DES Cryptographic Algorithm ", December 2012.
20. Junlei LIN, Jinghui FAN, School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China, Journal of Computational Information Systems 8: 18 (2012) 7485–7492,'Image Encryption Based on Cat Map and Fractional Fourier Transform '.

21. Sunjiv Soyjaudah, Sumithra Devi, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-3, February 2013, " Image Quality Assessment For Partial Encryption Using Modified Cyclic Bit Manipulation".
22. Khanzadi, Himan, Mohammad Eshghi, and Shahram Etemadi Borujeni. "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", Arabian Journal for Science and Engineering, 2014.
23. Shraddha Soni, Himani Agrawal, and Monisha Sharma, International Journal of Engineering and Innovative Technology (IJEIT),"Analysis and Comparison between AES and DES Cryptographic Algorithm ", December 2012.
24. A.Usha, and A. Subramani,'Performance Study of Key Developer Data Encryption and Decryption Algorithm (KDDEDA) with AES, DES and BLOWFISH', International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issue 12 Dec. 2016, Page No. 19596-19611
25. Vinay Verma, Rajesh Kumar,'A Unique Approach to Multimedia Based Dynamic Symmetric Key Cryptography', International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1119 – 1128.
26. Yudong Zhang, Xiao-Jun Yang, and Zhengchao Dong, School of Computer Science and Technology Nanjing Normal University, China, ' Theory and Applications of Fractional Fourier Transform and its Variants', Fundamenta Informaticae 151 (2017) i-viii I DOI 10.3233/FI-2017-1476.
27. X. Liu, G. Han, J. Wu, and Z. Shao ,'Fractional Krawtchouk transform with an application to image watermarking IEEE Transactions on Signal Processing. 65(7) 1894-1908 (2017).
28. S. Kumar, R. Saxena, and K.Singh. Fractional Fourier transform and Fractional-order calculus-based image edge detection. Circuits Systems and Signal Processing. 36(4) 1493-1513 (2017).
29. G..Manmadaleela ,M.Priscilla Dinkar, Department of Electronics and Communications Engineering, Srivenkateswara college of engineering and technology, Andhra Pradesh, India, ' Frft based 2rd order Poly -Bohman window for ECG de-noising', International Journal of Science, Engineering and Technology Research (IJSETR), Volume 6, Issue 2, February 2017, ISSN: 2278 -7798.
30. ZHIZ.HONG, YABIN.ZHANG,AND MINGGUANG.SHAN, College of Information and Communication Engineering, Harbin Engineering University, Harbin, China , ' Silhouette-free image encryption using interference in the multiple-parameter fractional Fourier transform domain', Vol. 25, No. 6 | 20 Mar 2017 | .
31. Shengnan Mi, Xinzhuo Liu, and Zhiyu Qu, School of Information and Communication Engineering, Harbin Engineering University, Harbin, China, ' Recognition of Radar Signal Modulation Based on Fractional Fourier Transform ', International Journal of Signal Processing Systems Vol. 5, No. 2, June 2017.
32. Nugyen.YTH, M.Lernon, D.Ghogho, 'Sparse Reconstruction of Time-Frequency Representation using the Fractional Fourier Transform', In: 2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing ,2017, International Conference on Recent Advances in Signal Processing, Telecommunications & Computing.