International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 9, No. 2, July 2020, pp. 141~152
ISSN: 2089-4864, DOI: 10.11591/ijres.v9.i2.pp141-152

Data ecryption based on multi-order FrFT, and FPGA implementation of DES algorith

A.Rabie, Kh.El Shafie, A.Hammuoda, M.Rohiem
Computers & Systems Engineering Department, Faculty of Engineering, EL AZHR University, Egypt

Article Info

Article history:

Received Apr 16, 2019
Revised Apr 25, 2019
Accepted Apr 04, 2020

Keywords:

Data encryption standard
Field-programmable gate array
Fourier transform
Fractional fourier transforms
Symmetric key cryptography.

ABSTRACT

Cryptography techniques need some algorithms for encryption of data. Most 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 not be inefficient for multimedia, because it is size is greater than the text. Therefore, Cryptosystems need to find and develop a new encryption schemes for such data. The most popular symmetric key algorithms are Data Encryption Standard (DES). However, DES is may be not suitable for multimedia because it consumes times. Encryption and decryption of these data require different methods. In this paper a method for encryption/decryption data by using the nature of FrFT in signals analysis, based on multi-order Fractional Fourier Transform has been introduced. The security of the method used in the encryption work was taken into account to identify the different indicators to measure the security of the encryption Techniques. 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 Fractional Fourier Transform. The encrypted data is obtained by the summation of different orders. Numerical simulation results are given to demonstrate this proposed method.

Corresponding Author:

A.Rabie,
Computers & systems engineering department,
EL AZHR University,
Cairo, Egypt.
Email: engahmed_rabie2010@yahoo.com

1. INTRODUCTION

The science of protecting the information by converting it into unreadable while stored and transmitted is Cryptography [1]. The encryption is plays a major role in securing the data in transmission. 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 are 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: Background introduced has been introduced in section 2, the proposed data encryption Methods has been introduced in Section 3, comparative study between DES algorithms 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. BACKGROUND

Data Encryption Standard (DES), Triple DES, and Advance Encryption Standard (AES) are the most popular symmetric key algorithms.

2.1. Data encryption standard (DES)

The DES is used for encryption. 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 was 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 a 16-rounds of substitution and permutation as shown in Figure 1 and Figure 2.

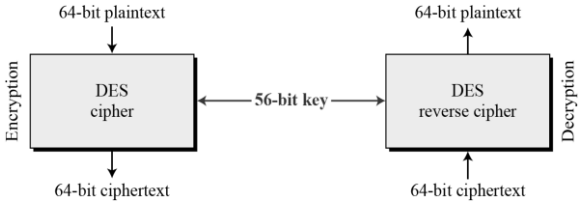

Figure.1. DES encryption and decryption process

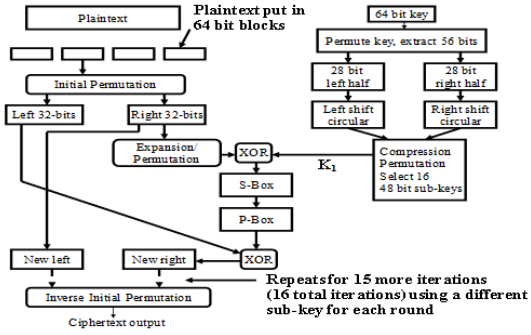

Figure 2. DES algorithm

2.2. Theory of fractional fourier transform

The Fourier transform is a rotation by angle π/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]:

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t)\, K_\alpha(t,u)\, dt \tag{1}$$

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

$$K_\alpha(t,u) = C_\alpha e^{-i\frac{ut}{\sin\alpha} + \frac{i}{2}(t^2+u^2)\cot\alpha} \tag{2}$$

And

$$C_\alpha = \sqrt{\frac{-ie^{i\alpha}}{2\pi\sin\alpha}} = \sqrt{\frac{1-i\cot\alpha}{2\pi}},\ K_\alpha(t,u) = \sqrt{\frac{1-i\cot\alpha}{2\pi}} e^{\frac{i}{2}((t^2+u^2)\cot\alpha - iut\csc\alpha)} \tag{3}$$

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

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

The 2-D FrFT of a function *f(x,y)* is:

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

Where

$$K_{\alpha_x}(x,u) = C_{\alpha}e^{i/2[x^2+u^2]\cot\alpha_x - ixu\csc\alpha_x} \tag{6}$$

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

The signal *f(x,y)* can be recovered by FrFT operation with backward angles(- α_x ,- α_y):

$$f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f_{\alpha}(u,v)K_{-\alpha_x-\alpha_y}(x,y;u,v)dudv \tag{7}$$

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

3. PROPOSED APPROACH

The proposed encryption technique is shown in Figure 3. Let 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 [18] and matrix R. Encryption model as shown in Figure 3. is secure and more robust towards brute force attack, but the complexity of the system is increased.

In decryption process, the reverse for encryption process, is applied as shown in Figure 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*.

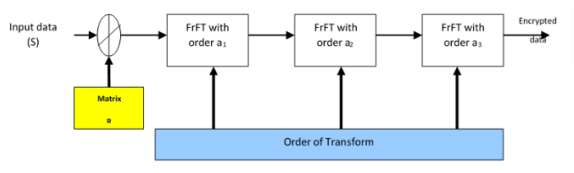

Figure 3. Proposed encryption system

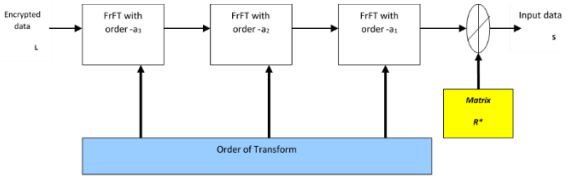

Figure 4. Proposed decryption system

3.1. Example 1: Enc/Dec proposed method for an image:

Mathematically, the encryption process in Figure 4, 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 figure 14 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. Complexity of proposed method for an image

Image Name	Size of Image	Encryption / Decryption Time (in sec) Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Image1	22.9 KB	0.6250 / 0.4840	3.7540 / 3.1396	8.3175 / 5.9066
Image2	23.1 KB	0.6410 / 0.4850	4.7837 / 3.2216	6.7218 / 5.9234
Image3	19.7 KB	0.6250 / 0.4840	4.1427 / 3.0015	6.8931 / 5.5883
Image4	20.7 KB	0.6250 / 0.4840	3.7237 / 3.0765	5.7728 / 5.6454
Image5	20.5 KB	0.6250 / 0.5000	3.7624 / 2.7117	6.6578 / 6.1379
Average Time		0.6282 / 0.4874	4.0333 / 3.03018	6.8726 / 5.84032

Table 2. Complexity of proposed method for an Audio

Audio	Size KB	Encryption / Decryption Time (in sec) Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Audio 1	18.4	0.3627 / 0.3089	2.2284 / 2.0757	4.2932 / 3.1719
Audio 2	55.7	1.0386 / 1.0737	3.6311 / 3.4801	7.2375 / 6.3850
Audio 3	21.5	0.3317 / 0.2575	2.4489 / 1.9185	4.8440 / 3.6142
Audio 4	61.7	1.0482 / 1.1170	3.7467 / 3.6868	7.7855 / 6.6226
Average Time		1.70568 / 1.65052	12.32298 / 9.91746	17.01664 / 10.93456

3.2. 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, Figue 5

and Figure 6. shows original audio1 and histogram. Figure 7. is shows encrypted audio1 signal with FrFT, while Figure 8. shows decrypted audio1 signal (reconstructed audio1).

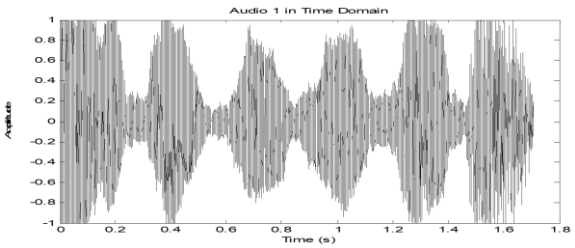

Figure 5. Original audio1

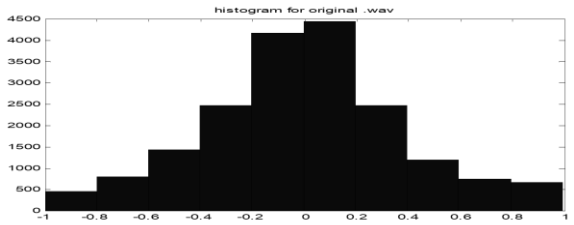

Figure. 6. Audio1 histogram

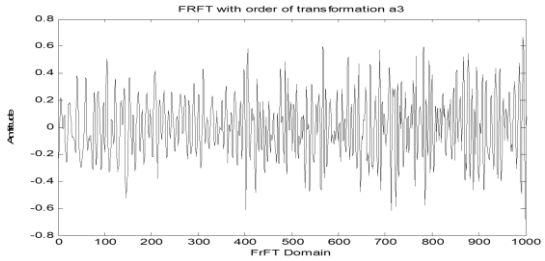

Figure7. third FrFT for audio signal (encrypted)

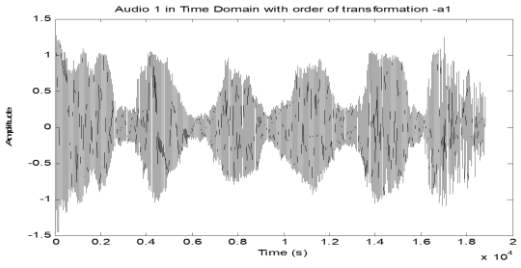

Figure 8. Reconstructed audio signal (decrypted)

4. COMPARATIVE STUDY BETWEEN DES & FrFT USING SOFTWARE SIMULATIOM

Computer simulations have been done of the proposed encryption technique, The image present in study is shown in Figure 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.

Figure 9. Original image1

This sub section, the security analysis of the proposed method, and statistical analysis have been introduced. 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. Figure 10. and Figure 11. shows decryption with correct and incorrect keys.

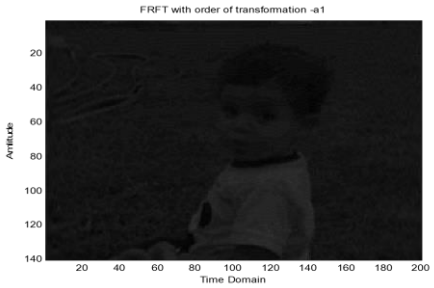

Figure 10. Decrypted image1 with correct key

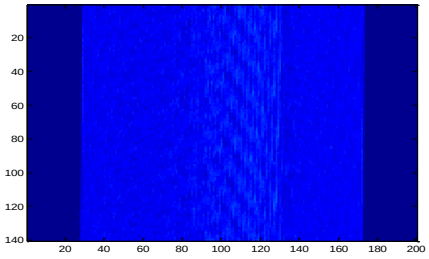

Figure 11. Decrypted image1 with incorrect key

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 Figure 12 and Figure 13.

Figure 12. Original image1

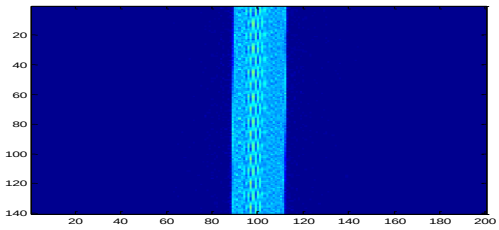

Figure 13. Encrypted image1

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. Figure 14 and Figure 15 are two gray images: Image1 and Image4, respectively.

Figure 14. Original image1

Fig.15. Original image4

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

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

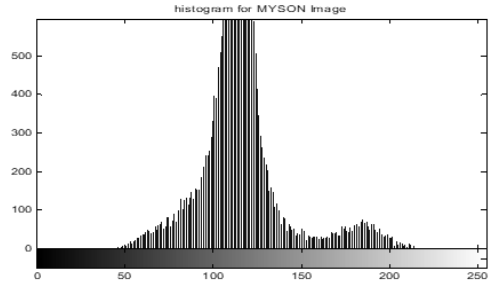

Figure 16. Image1 histogram

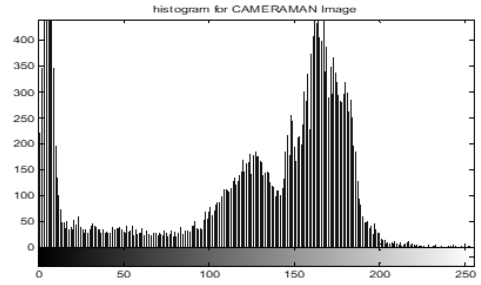

Figure 17. Image4 histogram

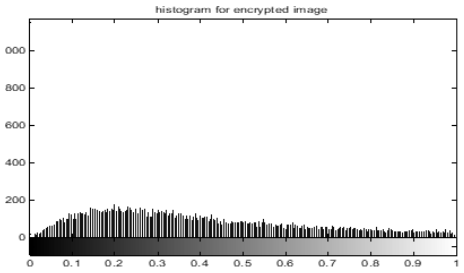

Figure18. Histogram for encrypted image1

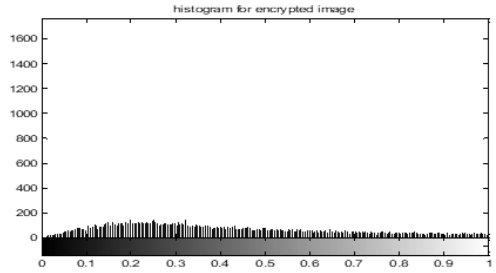

Figure 19. Histogram for encrypted image4

Note that 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 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 (17) [19]:

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

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 (18) [20]:

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

The experimental results that show the MSE and PSNR for an Image are shown in Table 2, Table 3, and Table 4 shows the peak signal to noise ratio (db).

Table 3. Mean square error

Image	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average MSE	0.01436	0.0253	0.10372

Table 4. Peak Signal to noise ratio (db)

Image	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average PSNR	66.81	64.3125	58.20214

The experimental results that show the MSE and PSNR for an Audio are shown in Table 5 and Table 6.

Table 5. Mean square error

Audio	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	0.000923968	0.001466514	0.02082

Table 6. Peak signal to noise ratio

Audio	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	114.9834	99.07484	80.95324

4.4. Differential analysis

In image encryption, the cipher resistance to differential attacks is commonly analyzed via the NPCR and UACI tests [19]. 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 (19) and (21):

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

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 (20) [21]:

$$D(i,j) = \left\{ \frac{0, if.C_1(i,j) = C_2(i,j)}{1, if.C_1(i,j) \neq C_2(i,j)} \right\} \tag{20}$$

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

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

Table 7. NPCR value for proposed method

Image	*NPCR%* Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	98.072	96.335	97.493

Table 8. UACI value for proposed method

Image	*UACI%* Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	33.79	34.55	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 (22):

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

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 9 and Table 10.

Table 9. Correlation coefficient between original and encrypted

Image	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	0.173	0.136	0.108

Table 10. Correlation coefficient between original and decrypted

Image	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	0.998	0.997	0.991

The values of the Correlation Coefficient between original, encrypted, and decrypted audio are showing in Table 11 and Table 12.

Table 11. Correlation coefficient between original and encrypted

Audio	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	0.004	0.005	0.011

Table12. Correlation coefficient between original and decrypted

Audio	Proposed Enc/Dec system based on One FrFT	Proposed Enc/Dec system based on Two FrFT	Proposed Enc/Dec system based on Three FrFT
Average	0.975	0.975	0.968

Table 13 shows a comparative study of an Image, between DES, AES [22], and proposed encryption-decryption system based-on FrFT.

Table 13. Experimental analysis of DES and proposed Enc/Dec system based on FrFT

Parameters	DES	AES	Proposed Enc/Dec system based on **One** FrFT	Proposed Enc/Dec system based on **Two** FrFT	Proposed Enc/Dec system based on **three** FrFT
Encryption Time (in sec)	215.9359	99.871	0.6282	7.1092	11.1856
Decryption Time (in sec)	183.5455	84.8904	0.4874	3.2654	6.7280
MSE	0.226	0.007	0.01436	0.0253	0.10372
PSNR(db)	54.587	69.7082	66.81	64.3125	58.20214
NPCR (%)	99.6643	99.60	98.072	97.335	96.493
UACI (%)	51.249	33.53	33.79	34.55	34.16

5. HARDWARE IMPLEMENTATION OF DES USING FPGA

5.1. DES Implementation using FPGA

Implementation Data Encryption Algorithms (DES), with FPAG to demonstrate the concept of system-on-chip approach (SoC). Xilinx provides Xilinx Embedded Development Kit (EDK) for building an embedded SoC on its FPGAs, EDK allow building processor based on embedded processor from Xilinx called Microblaze. The Tools has been used:

a. Nexys 3 FPGA board.
b. Xilinx Embedded Development Kit.

5.2. Xilinx Platform Studio

FPGA implemented is a simple design using VHDL and Verilog on FPGA. The applications will be written using "C or C++", finally to run the applications on processor system download bit file to the FPGA.

5.3. Simulation Results of DES algorithm:

In this section, analysis of the simulation results has been introduced, Figure 20 and Figure 21. shows Xilinx Platform Studio and Graphical design view. Figure 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. Figure 23. is show the simulated result of encryption and decryption on ISE13.1.

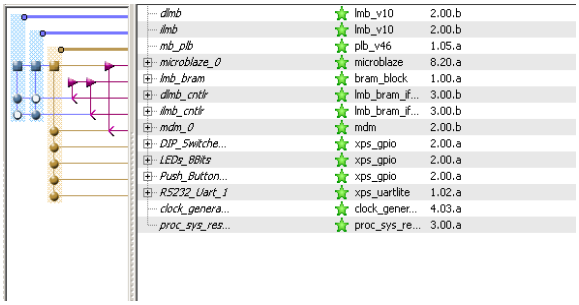

Figure 20. Xilinx platform studio - system assembly view

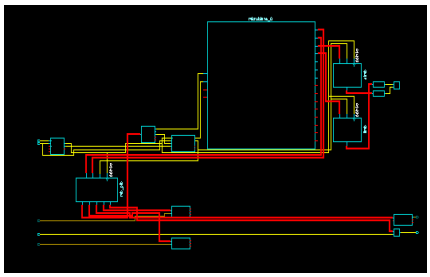

Figure 21. Graphical design view

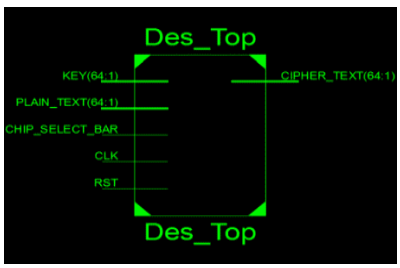

Figure 22. DES block

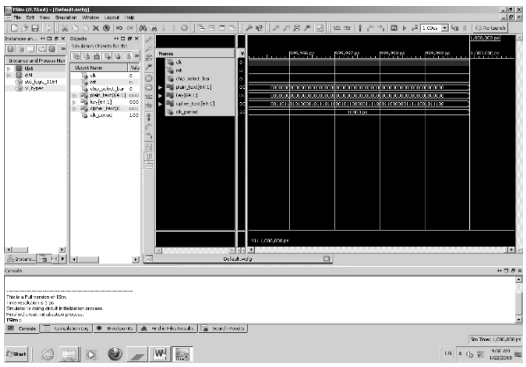

Figure 23. Simulation results of DES using Xilinx ISE

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

6. CONCLUSIONS

Nowadays the security of data in the digital world becomes more and more important. When using the encryption algorithms may add burdens on the system: in the design process, the financial cost, or in processing time according to the complexity of the internal processes that make up the algorithm, and this is to be expected.

A method to encrypt and decrypt data based on multi-order Fractional Fourier Transform has been introduced. For more security, and to make encryption model robust towards brute force attack the key is formed by combination of order of Fractional Fourier Transform and the matrix, data has been encrypted and decrypted data successfully. 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), PSNR, NPCR and 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 Algorithms, and the simulation result, was performed on Xilinx ISE for implementing encryption and decryption module, with NEYXS 3 FPGA board.

We do not compare the globally agreed between systems and between the use of encryption (FrFT) to encrypt data. We do not say that the use of FrFT for encrypt data is better, but trying to offer a safe way without adding additional costs or burdens and up nearly applicable safety standard in encryption systems. The future work will be: implementation of FrFT encryption and decryption model using FPGA.

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, pp. 468-479, 2009.

[2] Refregier.P., and Javidi.B., " Optical image encryption based on input plane and Fourier plane random encoding, " *Opt. Lett*., vol. 20, no. 7, pp. 767-769, 1995.

[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," *IMA Journal of Applied Mathematics*, vol. 25, no. 3, pp. 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.*, vol. 41, no. 5, pp. 1037–1044, 1994.

[7] Almeida.L.B., "The fractional Fourier transform and time-frequency representation," *IEEE Trans. Sig. Proc.*, vol. 42, no. 11, pp. 3084–3091, 1994.

[8] Ozaktas.H.M., and Mendlovic.D., "Fractional Fourier transforms and their optical implementation: II," *J. Opt. Soc. Am. A*, vol. 10, no. 12, pp. 2522–2531, 1993.

[9] Namias.V., "The fractional Fourier transform and its application in quantum mechanics," *J. Inst. Math. It's Appl*., vol. 25, no. 3, pp. 241–265, 1980.

[10] FIPS FIPS-197, *Federal Information Processing, Standards Publication FIPS-197, Advanced Encryption, Standard* (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 1999.

[11] Unnikrishnan.G., Joseph.J., and Singh.K., " Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt.Lett*., vol. 25, pp. 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*, vol. 44, no. 1, pp. 124–129, 2012.

[13] Sanjay Rawat, Balasubramanian Raman., "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography," *Signal Process*, vol. 92, no. 6, 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*, vol. 283, no. 10, pp. 2043-2049, 2010.

[15] Zhengjun Liu, *et al*, "A new kind of double image encryption by using a cutting spectrum in the 1-D fractional Fourier transforms domains," *Opt. Commun*, vol. 282, no. 8, 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*, vol. 226, no. 1, pp. 155-16, 2003.

[17] Anoop M.S, *Public key Cryptography Applications Algorithm and Mathematical Explanations*, India: Tata Elxsi 2007.

[18] Ozaktas.H.M., Zalevsky.Z., and Kutay.M.A., *The fractional Fourier transform with applications in optics and signal processing*, New Yourk: Wiley, 2001.

[19] Shraddha Soni, *el at*, "Analysis and comparison between AES and DES cryptographic algorithm," *International Journal of Engineering and Innovative Technology* (IJEIT), vol. 2 no. 6 pp. 362-365, 2012.

[20] Junlei LIN, Jinghui FAN, "Image encryption based on cat map and fractional Fourier transform," *Journal of Computational Information Systems*, vol. 8, no. 18, pp. 7485–7492, 2012.
[21] Parameshachari B D, K M Sunjiv Soyjaudah, Sumithra Devi K A, "Image quality assessment for partial encryption using modified cyclic bit manipulation," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 2, no. 3, pp. 84-87, 2013.
[22] Khanzadi, Himan, *et al*, "Image encryption using random bit sequence based on chaotic maps," *Arabian Journal for Science and Engineering*, vol. 39, no. 2, pp. 1039-1047, 2014.