Journal of Theoretical and Applied Information Technology
30th June 2019. Vol.97. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT LOW DETAILED IMAGE ENCRYPTION USING LOGISTIC MAP AND FrFT TRANSFORM IN DIFFERENT MODES OF OPERATION

ASHRAF AFIFI[1,2]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Kingdom of Saudi Arabia

[2]Department of Electrical Engineering and Computers, Higher Technological Institute, 10th of Ramadan, Egypt ashrafifi@yahoo.com

ABSTRACT

This paper presents an efficient encryption for low detailed image using logistic map and fractional Fourier transform (FrFT) in different modes of operation. The proposed cryptosystem employed logistic map with the FrFT using different modes of operation. The proposed cryptosystem is composed of two phases; encryption phase and decryption phase. The encryption phase began with applying the FrFT on the few detailed plain image. Then, the plain image is encrypted using logistic map in different operation modes. While in the decryption phase, this scenario will be reversed. The efficiency of the proposed image cryptosystem is investigated using different encryption quality metrics via simulation. The obtained results confirmed the viability of the proposed cryptosystem in CBC,CFB, and OFB operation modes. Moreover, the proposed system is successively applicable in terms of security encryption.

Keywords: *Five Image Encryption, ECB, CBC, OFB, CFB, Digital Communications, Few Details Images.*

1. INTRODUCTION

With the rapid growth in multimedia and communication technology, security becomes an important issue in data transmission, Image encryption is essential to keep the confidentiality between users in many applications, such as video conference, mobile, military communications, telecommunications, and telemedicine [1,2]. Image encryption methods can be classified into confusion-based and diffusion-based schemes. Diffusion means spreading out of the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this idea is to spread the influence of a single key digit over many digits of ciphertext. Confusion means use of transformations which complicate the dependence of the statistics of ciphertext on the statistics of plaintext. For secure data transmission over wireless channels, confusion based schemes are preferred in image encryption. However, diffusion based schemes are sensible to the accumulation of errors [3]. So, chaos-based algorithms have shown their superiority for image encryption [4-5].

The DES, IDEA, EL-Gamal and RSA traditional ciphering methods are based on complicated mathematical problems [6]. such methods can be classified into single and double keys encryption schemes which have been employed only in encrypting textual data [7]. In contrast to textual data, images are characterized by various features like huge data blocks redundancy, which cannot be dealed using traditional encryption techniques. A main barrier for constructing an influential image ciphering techniques is realizing both diffusing and shuffling using traditional methods which will be an extremely tough process [8]. One more barrier is that traditional methods need extra processing steps for handling the compressed image data. Consequently, they require extra processing capacity and long processing time.

The RC5 [9], RC6 [10] , Rijndael [11,12] ciphering methods have been introduced to solve the limitations of traditional encryption methods. RC6 has been found in 1998 as a substitution for RC5 to satisfy Advanced Encryption Standard (AES) requirements [12]. It utilizes data-dependent rotations to overcome the limitations of traditional ciphering methods. RC6 also utilizes four acting 32-bit registers and includes integer multiplication as an extra operation increasing the attained diffusion per iteration [13]. It can process 128-bits blocks of size and can be easily implemented. The low detailed images encryption may be considered as a great challenge for the majority encryption techniques. Block ciphering methods cannot efficiently encrypt detailed images because the values of pixels in specified area of an image are very close to each other. Indeed, spatial domain's

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

chaotic encryption methods have a drawback of keeping the same histogram with respect to the plain image. Consequently, the problem of low detailed image encryption is a great challenge for the majority of encryption methods which is not fully studied up till now.

An image cryptosystem for encrypting low detailed gray scale image is proposed in [13]. This proposed image cryptosystem is based on utilizing wavelet fusion, which perform some types of preprocessing operations on the plain image before encryption aiming at deleting homogeneity of flat areas. Such preprocessing could be by fusing the low details image with other rich details image using the Discrete Wavelet Transform (DWT). After the fusion step, the fused image is encrypted using RC6 or chaotic Baker map.

In this research, an efficient image cryptosystem is proposed with employing a FrFT in different operation modes. The proposed cryptosystem begins with applying the FrFT on the plain images in fractional domain . Then the plain image is fed to the logistic in different operation modes. This scenario is reversed in the decryption phase. The performance of the proposed low details image cryptosystem is assessed and evaluated using encryption/decryption quality measures via simulation. The results show that; the proposed low details cryptosystem in CBC, CFB and OFB can effectively encrypt low details images and no one can distinguish between the plain image and its corresponding cipher image one. This paper presents an efficient algorithm for low detailed image encryption. The study investigates the proposal algorithm through a series of experiments. The results confirms the effectively the proposed encryption algorithm.

The rest of the paper is organized as follows: Sect. 2 survey on the basic fundamentals of knowledge . Sect. 3, presents the proposed low details image cryptosystem. Sect. 4 gives the encryption quality in evaluating the performance of the proposed image cryptosystem. Sect. 5 presents the achieved results and their discussions. At the end, Sect. 6 concludes the research.

2. BASIC FUNDAMENTALS KNOWLEDGE

2.1 The Fractional Domain

The FrFT is a generalization of the Fourier Transform (FT). The classical FT corresponds to a rotation in the time-frequency plane over an angle α = n π / 2, the FrFT will correspond to a rotation over an arbitrary angle α = nπ / 2 with n ∈ R. Where the parameter α is called the fractional order of the transform. The parameter a can be limited to 0 ≤ n ≤ 1. The FrFT is represented and defined as [16-17]:

$$X_\alpha(t,u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}}\cdot\exp\left(j\frac{t^2+u^2}{2}\cot\alpha - j\frac{tu}{\sin\alpha}\right) & if \quad \alpha \neq n\pi \\ \partial(u-t) & if \quad \alpha = 2n\pi \\ \partial(u+t) & if \quad \alpha = (2n+1)\pi \end{cases} \tag{1}$$

The FrFT of a signal x(t), with a transformation angle α is represented as $X_\alpha(u)$. The free variable u can be interpreted as some hybrid time frequency variable.

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t)\, k_\alpha(t,u)\, dt \tag{2}$$

2.2 2-D Chaotic Logistic

The basic dependency of logistic map on control parameters makes it widely used in chaos based applications, which offers a great sensitivity to initial conditions.

The 1-D logistic map is one of the simplest models that exhibits a chaotic behavior which can be mathematically described as (1) [18]:

$$X_{n+1} = rX_n(1 - X_n) \tag{3}$$

where X_n takes values in the interval [0, 1], the parameter r is a positive constant and takes values up to 4. Its value controls the behavior of the logistic map.

The two-dimensional logistic map has a more complex, chaotic behavior than the one-dimensional logistic map which that is sufficient enough to make information encrypted by this map are more difficult to be extracted. It can be defined: where r is a system parameter and (x_i, y_i) is the pair-wise point at the i^{th} iteration [19].

$$2D\ Logistic\ \ map\ :\ \begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_i + 1)y_i(1 - y_i) \end{cases} \tag{4}$$

2.3 Modes of Operation

The operation mode is a procedure which utilizes block ciphering for providing various information services like authenticity and confidentiality [20]. The operation mode explains how one can repetitively execute a one-block

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cipher's technique for securing and transmitting amount of information larger than one block [21,22]. In this section, we will discuss the operation modes recognized by the abbreviations ECB, CBC, CFB, and OFB and how they can be used in block ciphering to construct a cryptosystem. During the discussion, the following variables are used: n length of block, K secret key, EK encryption maps and DK decryption maps.

2.3.1. The electronic codebook (ECB) mode

The ECB mode is the easiest method for using with a block cipher. The information message to be encrypted is partitioned into blocks. Each block in turn is autonomously encrypted which means that there is no dependency between blocks in the decryption process. Encryption and decryption are done using same secret key.

$$A_i = E_K(B_i) \quad (5)$$

$$B_i = D_K(A_i) \quad (6)$$

This can be expressed as $\{B\}_k --> A$; which means that original plaintext B block is encrypted using secret key k to generate ciphertext A block.

In ECB mode, identical input blocks always have similar ciphered output blocks and the are encrypted in the same way. This feature is considered as major drawback for the ECB operation mode because it does not hide patterns of data.

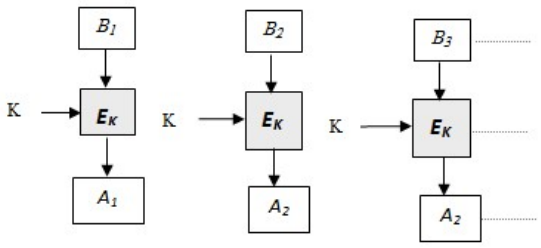


Fig. 1: Block ciphering in ECB operation mode

2.3.2. The cipher block chaining (CBC) mode

The CBC operation mode is the most widely used one. It overcomes the main drawback of EBC mode by XORing bits of the input plaintext block with the previously ciphered block before the encryption process takes place. The enciphering process is initialized by a dummy selected message (block of a specified length that is known as Initialization Vector (IV). This IV can be sent openly to the receiver, i.e., the security of the encryption system is based on securing the key and not on securing IV. The deciphering process can be paralyzed because only the jth and (j-1)th ciphered blocks are needed in obtaining jth plaintext block. The operation of CBC mode is illustrated in Fig. 2. The encryption and decryption procedures are done in CBC mode according to Eq. 5 and Eq. 6, respectively.

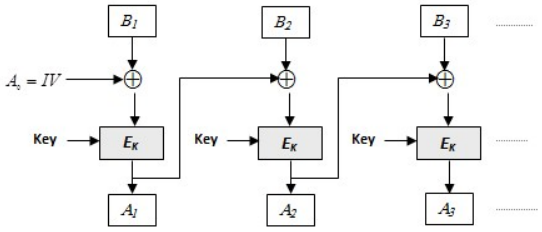


Fig. 2: Block ciphering in CBC operation mode

$$A_j = E_K(A_{j-1} \oplus B_i) \quad (7)$$

$$B_j = D_K(A_j) \oplus A_{j-1} \quad (8)$$

$$A_0 = IV \quad (9)$$

2.3.3. The cipher feedback (CFB) mode

The CFB mode is proposed for encrypting and transferring some values of plaintext instantaneously one after. The decryption operation in CFB is very close to reverse execution of encryption operation in CBC mode. Th

is mode also utilizes the IV and selects it similarly as in CBC operation mode. The CFB operation mode works by XORing the recent block of plaintext with the encryption of the former ciphered text block to create the recent ciphered text block. The XORing has a great effect in concealing the patterns of plaintext. Fig. 3 shows how the CFB mode works. The encryption/and decryption procedures are done in CFB mode according to Eq. 8 and Eq. 9, respectively.

$$A_j = B_j \oplus I_j \quad (10)$$

$$B_j = A_j \oplus I_j \quad (11)$$

$$I_j = E_K(A_{j-1}) \quad (12)$$

$$j = 1,2,3,.....$$

$$A_0 = IV \quad (13)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

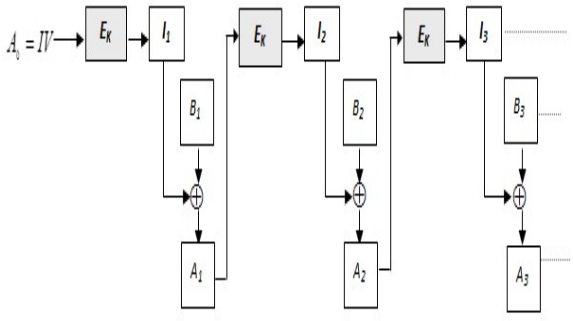


Fig. 3: Block ciphering in CFB operation mode

2.3.4. The output feedback (OFB) mode

The OFB operation mode transformed block ciphering to concurrent stream ciphering. It produces blocks of key stream. The encryption/decryption procedures are similar as a result of symmetric property of XOR operation. The OFB operation mode cannot be paralyzed as every result of feedback block cipher step relies entirely on the previously conducted ones [23] Fig. 4 shows how the OFB operation mode works. The decryption/encryption procedures are conducted according to Eq. 10 , Eq. 11, Eq. 12 and Eq. 13 respectively.

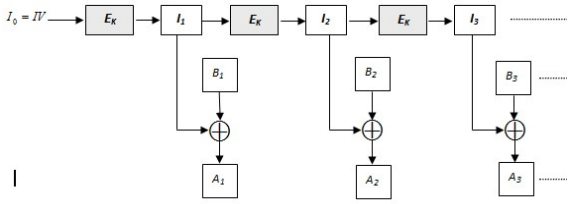


Fig. 4: Block ciphering in OFB operation mode

$$I_j = E_K(I_{j-1}) \quad (14)$$

$$j = 1,2,3,.....$$

$$I_0 = IV \quad (15)$$

3. THE PROPOSED FEW DETAILS FRACTIONAL LOGISTIC IMAGE CRYPTOSYSTEM

The proposed few detailed logistic image cryptosystem utilizes logistic map in FrFT in different operation modes. As shown in Fig. 5, it has two modules for encryption/decryption, respectively. The encryption module starts by reading the few detailed plainimage. Then, fed to the FrFT and apply logistic map encryption using EBC or CBC or CFB or OFB operation modes. The encryption steps can be summarized as follows:

1. Read the few details image.
2. Apply FrFT on the few details plainimage.
3. Apply 2-D logasitic map on the FrFT few details image.
4. Apply inverse FrFT on the logistic transform few details image.
5. Apply on the resulted ciphered low details image EBC or CBC or CFB or OFB operation modes.

The receiver starts by applying the decryption module in the same operation mode used in the encryption module.

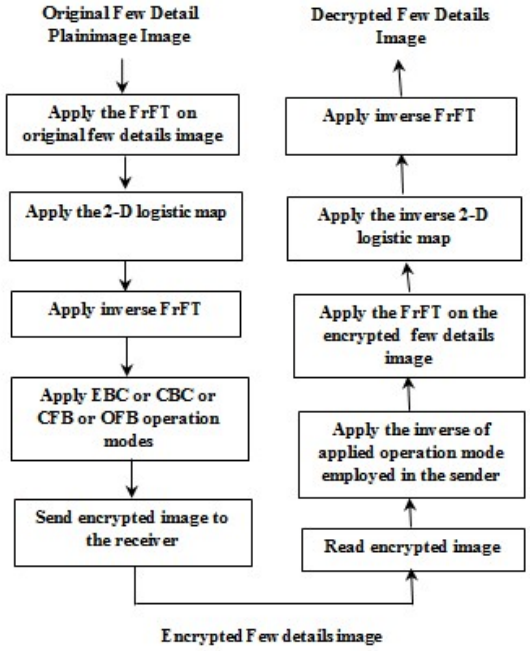


Fig. 5: The Proposed Few Details Image Cryptosystem

The steps of decryption module is summarized as follows:

1. Read the few details cipher image
2. Apply the same operation mode (EBC or CBC or CFB or OFB) as used in the sender.
3. Apply the FrFT on the resulted ciphered low details image.
4. Apply the inverse **2-D** logistic map.
5. Apply the inverse FrFT to obtain the find decrypted few details image.

4. ENCRYPTION PERFORMANCE MEASURES

This section is dedicated for introducing measures in assessing the encryption performance of the proposed few detailed image cryptosystem. The encryption/decryption quality are inspected visually

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and evaluated quantatively with encryption/ decryption quality measures.

4.1. Visual Inspection

Visual inspection can detect the convergences of plainimage to its corresponding encrypted one. But, it is not a sufficient measure to evaluate the hiding accuracy of image details [12,13,24]. so other encryption quality measures must be used to quantitatively estimate the encryption degree.

4.2. Entropy

The Entropy is used to evaluate the information involved within the encrypted image.

show how the entropy can be evaluated [13,24]:

$$Entropy = -\sum_{i=1}^{n} P_r(x_i)\log P_r(x_i) \quad (16)$$

where x_i is the i^{th} intensity value and P_r is its corresponding probability. Consequently, high entropy value indicates good encryption.

4.3. Encryption Quality Tests

The encryption quality test measures include irregular deviation, correlation coefficient and histogram deviation.

4.3.1.Correlation coefficient (CC)

The CC is calculated between the original image $I(x_i, y_j)$ and its corresponding encrypted $E(x_i, y_j)$ It can be calculated as [25,26]:

$$CC(I,E) = \frac{\mathrm{cov}(I,E)}{\sqrt{D(I)}\sqrt{D(E)}},$$
$$\mathrm{cov}(I,E) = \frac{1}{L}\sum_{i=1}^{L}(x(i)-E(x))(y(i)-E(y)), \quad (17)$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L}(x(i)-E(x))^2, \quad D(y) = \frac{1}{L}\sum_{i=1}^{L}(y(i)-E(y))^2$$

, and

L is the whole image pixels number. The small the value of CC(I, E) between the original image $I(x_i, y_j)$ and encrypted image $E(x_i, y_j)$, the better the encryption quality.

4.3.2. Irregular deviation (ID)

The ID measure the encryption accuracy in terms of how much the irregularity is the ID can be calculated as follows [27]:

$$ID(I,E) = \frac{\left|\sum_{i=0}^{255} h_d(i)\right|}{MxN}, \quad (18)$$

$$h_d(i) = \left|h(i) - M_h\right|, \quad (19)$$

where *h(i)* is encrypted image histogram having i intensity level and M_h is the ideal encrypted image uniform histogram. So lower *ID values* indicate better encryption quality.

4.3.3.Histogram deviation (HD)

The HD determine how it enlarges the difference among the original plainimage $I(x_i, y_j)$ and cipher image $E(x_i, y_j)$ The HD is estimated as follows [13,28]:

$$HD(I,E) = \frac{\left|\sum_{i=0}^{255} d(i)\right|}{MxN}, \quad (20)$$

where $d(i)$ is the absolute value of the difference between the original $I(x_i, y_j)$ and encrypted $E(x_i, y_j)$ histograms at pixel level i. M and N are the image dimensions. Consequently, high *HD* value lead to a strong deviation between the original $I(x_i, y_j)$ and encrypted image $E(x_i, y_j)$.

4.4. Differential Test

The differential test is performed to inspect the impact of changing one pixel on the encrypted image using the proposed few details image cryptosystem.

4.4.1 Number-of Pixels Changing Rate (NPCR)

Assume that E_1 and E_2 are two ciphered images whose respective plain images have single one-pixel difference. The NPCR computes the percentage of changed pixels number to the while pixels number between the two encrypted images. The values of pixels at location (x_i, y_j) in E_1 and E_2 are $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$. Assume a bipolar array $D(x_i, y_j)$ which equals in size to both of encrypted E_1 and E_2 images. The $D(x_i, y_j)$ is calculated by $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$ as:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$D(x_i, y_j) = \begin{cases} 0 & if \quad E_1(x_i, y_j) = E_2(x_i, y_j) \\ 1 & \text{Otherwise} \end{cases} \tag{21}$$

The *NPCR* can be calculated as follows [13,27]:

$$NPCR\ (E_1, E_2) = \frac{\sum_{i,j} D(x_i, y_j)}{M \times N} \times 100\ \%, \tag{22}$$

where M, N are the E_1 and E_2 width and height.

4.4.2. Unified average changing intensity (UACI)

The UACI estimates the average intensity difference between two encrypted images E_1 and E_2 .The UACI can be calculated as follows [28]:

$$UACI(E_1, E_2) = \frac{1}{MXN}\left[\Sigma x_i, y_i \frac{E_1(x_i, y_i) - E_2(x_i, y_i)}{255}\right] x100\% \tag{23}$$

4.5. Noise Immunity Test

4.5.1. The peak signal to noise ratio (PSNR)

The robustness of the proposed few details image cryptosystem with respect to the presence of Salt & peppers and Speckle is tested during decryption. The PSNR is calculated as follows [13]:

$$PSNR(I, D) = 10\log \frac{(255)^2}{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}[I(x_i, y_j) - D(x_i, y_j)]^2} \tag{24}$$

where $I(x_i, y_j)$ and $D(x_i, y_j)$ are the original and decrypted images pixel values at position (x_i, y_j), respectively. High values of PSNR indicate good immunity against noise .

4.5.2. The structural similarity (SSIM)

The SSIM is performed to assess decrypted image quality. Based on [13], the SSIM is calculated as follows:

$$SSIM(x, y|w) = \frac{(2\bar{w}_x\bar{w}_y + C_1)(2\sigma_{w_x w_y} + C_2)}{(\bar{w}_x^2 + \bar{w}_y^2 + C_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + C_2)} \tag{25}$$

where, C1, C2 denote minor constants, $\bar{w}_x$ and $\bar{w}_y$ denote the average of w_x and w_y regions respectively. $\Sigma_{w_x}^2$ denotes the variance of w_x region and $\sigma_{w_x w_y}$ is covariance among the two regions w_x and w_y. If the SSIM value is high, this means good immunity with respect to noise.

4.5.3. The feature similarity index (FSIM)

The FSIM is employed to assess the decrypted images quality. Based on [13], the FSIM is calculated as follows:

$$FSIM = \frac{\Sigma_{x\in\Omega} S_L(x).PC_m(x)}{\Sigma_{x\in\Omega} PC_m(x)} \tag{26}$$

where Ω denotes spatial domain of mage, $S_L(x)$ denotes overall similarity among two images and $PC_m(x)$ denotes value of phase congruency. High FSIM values means the noise immunity is good.

5. SIMULATION EXPERIMENTS

The performance of the proposed low details image cryptosystem is verified under a Set of experimental tests to study the impact of utilizing different operation modes (ECB, CBC, CFB, and OFB). Various sets of performance metrics are utilized in evaluating the proposed cryptosystem including general indicators like visual inspection, entropy, encryption quality differential and noise immunity measures. These tests are conducted using 512x512-sized images; namely Brain image, Chessboard, Tux and Logo Cs as illustrated in Fig.6.

a) Brain b) Chessboard c) Tux d) Logo Cs

Fig. 6: Color Test Images

5.1. Experiment 1:

In this experiment, the impact of operation modes using the proposed low details image cryptosystem on the encryption quality is investigated. The result of encrypting Brain, Chessboard, Tux and Logo CS images using the proposed low details image cryptosystem in different operation modes are shown in Figs. 7, respectively. The proposed low detailed image cryptosystem in different operation modes works fine and produces good result with CBC, CFB, OFB operation modes. The proposed low detailed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

image cryptosystem hides completely all information and nothing is visible.

On contrary, as shown from Fig. 7, the proposed low detailed image cryptosystem in ECB operation mode cannot hide all of the original image information. Based on visual investigation of results, one can say that employing CBC, CFB, OFB modes with the proposed low detailed image cryptosystem can totally secure transmitted information but ECB cannot do that.

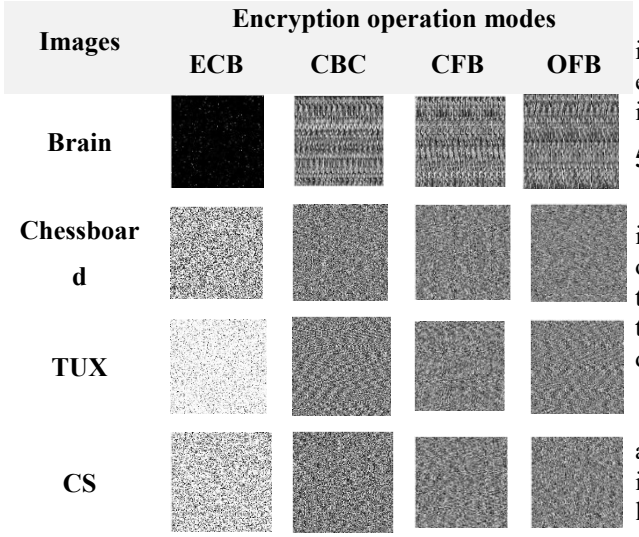


Fig. 7: Encryption results for the Brain, Chessboard, Tux, and CS images using the proposed few detailed fractional logistic image cryptosystem in different operation modes.

5.2. Experiment 2:

In this experiment, the entropy measure is utilized to estimate the information contained within the cipher image using the proposed low detailed image cryptosystem. The entropy results for the encrypted Brain, Chessboard, Tux and CS images using the proposed low detailed image cryptosystem in CBC, CFB, ECB and OFB operation modes are shown in Table 1.

Table 1: Entropy test results of encrypted for Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes.

Image	The proposed low detailed fractional logistic image cryptosystem in different operation modes			
	ECB	CBC	CFB	OFB
Brain	0.2550	7.7061	7.7152	7.7025
Chessboard	1.5147	7.9231	7.9666	7.9597
TUX	2.4982	7.9915	7.9875	7.9861
CS	1.0579	7.4057	7.4665	7.2912

The results listed in Table 1 ensures the visual inspection interpretation for results listed in Fig. 7. The proposed low detailed image cryptosystem in CBC, CFB, and OFB can fully secure information as satisfying high and comparable entropy estimation for all tested images. The ECB operation mode gives lowest entropy values for all of the tested images which means that the ECB operation mode can be used in securing information.

5.3. Experiment 3:

The performance of the proposed low detailed image cryptosystem in different operation modes for encrypting tested Brain, Chessboard, Tux and CS images is investigated.

5.3.1. Correlation coefficient (CC):

The performance of the proposed low detailed image cryptosystem is tested using CC. The results of assessed CC values among original and encrypted tested Brain, Chessboard, Tux and CS images using the proposed low detailed image cryptosystem in different operation modes is presented in Table 2.

Table 2: Correlation coefficient between original and encrypted for Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes.

Image	The proposed low detailed fractional logistic image cryptosystem in different operation modes			
	ECB	CBC	CFB	OFB
Brain	-0.0034	0.0087	-0.0036	0.0018
Chessboard	0.0489	0.2541	0.0026	-0.0089
TUX	0.0006	0.0008	-0.0030	0.0031
CS	0.0015	-0.0039	-0.0031	-0.0032

From Table 2, it is easy to notice that the CC values among the original and encrypted Brain, Chessboard, Tux and CS images in CBC, CFB and OFB operation modes are very low and close to zero. This indicates a good encryption quality for the proposed low detailed image cryptosystem in such modes. On the other hand, the obtained CC values for the tested Brain, Chessboard, Tux and CS images in ECB operation mode are the highest among the obtained CC values which show the unsuitability of this mode in securing information.

5.3.2. Irregular deviation (ID)

The performance of the proposed low detailed image cryptosystem in different operation modes for encrypting the tested Brain, Chessboard, Tux and CS images using ID is started. It is known that low values for ID means high encryption quality. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

attained ID results for the encrypted tested Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes are presented in Table 3.

Table 3: Irregular Deviation between source and encrypted images for Brain, Chessboard, Tux and CS using the proposed low detailed fractional logistic image cryptosystem in different operation modes.

Images	The proposed low detailed fractional logistic image cryptosystem in different operation modes			
	ECB	CBC	CFB	OFB
Brain	-0.4799	0.1239	0.1235	0.1252
Chessboard	0.4532	0.04347	0.0426	0.0436
Tux	0.3919	0.0235	0.0257	0.0264
Logo	0.4881	0.1780	0.1657	0.1868

As seen from Table 3, the ID values for the encrypted Brain, Chessboard, Tux and CS images using the proposed low detailed image cryptosystem in CBC, CFB and OFB operation modes are very small. Results show high quality for encrypted images. On contrary, ID values for encrypted tested Brain, Chessboard, Tux and CS images in ECB operation mode are the highest which ensures that ECB mode is poor in securing information.

5.3.3. Histogram deviation (HD):

The performance of the proposed low detailed image cryptosystem in encrypting tested using histogram deviation (HD) is examined. For good encryption, the HD of the encrypted image must be entirely different from the original image. The HD test results for the encrypted Brain, Chessboard, Tux and CS images and their corresponding plain images in CBC, CFB, ECB, and OFB operation modes are shown in Fig. 8, respectively.
Fig. 8: Histogram results of encrypted/decrypted for Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes.

It is easily to realize that, the HDs of encrypted Brain, Chessboard, Tux and CS images Also, the HDs of encrypted Brain, Chessboard, Tux and CS images in ECB operation mode are not homogeneous which show the unsuitability of this operation mode in securing information.

5.4. Experiment 4:

The differential tests are used to check the effect of modifying one-pixel on the encrypted image. The following two measures are employed; the NPCR and UACI. The NPCR estimates the percentage of dissimilar pixels number to the whole pixels number between two encrypted images E_1 and E_2 with similar original images except one single difference in one-pixel while the UACI computes the average intensity difference among the two encrypted images E_1 and E_2. Table 4 lists the NPCR and UACI values between two encrypted Brain, Chessboard, Tux and CS images with one-pixel change.

Table 4: The NPCR and UACI estimations for two encrypted tested Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes.

Image		The proposed low detailed RC6-based color image cryptosystem in different operation modes			
		ECB	CBC	CFB	OFB
Brain	NPCR	3.6804	99.8199	99.8443	99.315
	UACI	0	0	0	0
Chessboard	NPCR	50.938	99.5895	99.5743	99.544
	UACI	0	0	0	0
Tux	NPCR	58.835	99.6582	99.599	99.569
	UACI	0	0	0	0
CS	NPCR	39.571	99.9969	99.933	99.268
	UACI	0	0	0	0

It could be seen from the NPCR and UACI results in Table 4, that the proposed low detailed image cryptosystem in different operation modes is sensitive to tiny change in original images

5.5. Experiment 5:

The immunity of the proposed low detailed image cryptosystem in different operation modes with respect to salt& peppers and speckle is examined during the decryption

5.5.1. The PSNR

The PSNR is utilized to examine the quality of decrypted images. Table 5 presents the PSNR values for the decrypted Brain, Chessboard, Tux and CS images with the existence of different noise variances on the encrypted image. that the highest and lowest PSNR values for all tested images are obtained with the OFB and CFB operation modes, respectively. This means that the OFB is the best operation mode in terms of noise immunity and CFB is the worst one. This results ensure the immunity of the proposed low detailed image cryptosystem regarding noise which reveals high encryption quality.

Table 6 shows the decrypted Brain, Chessboard, Tux and CS images using the proposed low detailed image cryptosystem in different operation modes with the presence of noise of different variances. It is easy to notice visually that the best and worst decrypted images are obtained with OFB and CFB operation modes, respectively. We can conclude

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

that OFB operation mode is the superior over the other examined operation modes in terms of noise immunity and CFB is the worst one .

5.5.2 The structural similarity (SSIM)

The SSIM is employed to test quality of decrypted image. Table 7 lists the calculated SSIM values for the decrypted Brain, Chessboard, Tux and CS images using the proposed low detailed image cryptosystem in different operation modes with the existence various noise variances. From Table 7, We can notice that the highest and lowest SSIM values are obtained with the OFB and CFB operation modes, respectively. This again ensures the results listed in Tables 5 and 6 which indicate that OFB operation mode is the optimal one to utilize in terms of noise immunity.

5.5.3 the feature similarity index (FSIM)

The FSIM is employed to test the decrypted images quality. High values for FSIM show that the proposed low details image cryptosystem immunity against noise is high. In Table 8, the SSIM values for the decrypted Brain, Chessboard, Tux and Cs images using the proposed low detailed image cryptosystem in different operation modes with the presence various noise variances are listed. Again, the OFB and CFB operation modes yield the highest and lowest FSIM values, respectively. These results confirm the results shown in Tables 5, 6 and 7. It is clear that is the OFB operation has the superiority terms of noise immunity.

6. CONCLUSION

This paper proposed an efficient low detailed image cryptosystem employing chaotic logistic with FrFT in different operation modes. A simulation model is built to examine the performance of the proposed low details image cryptosystem in different operation modes using different encryption quality measures. The results show that utilizing CBC, CFB and OFB operation modes is powerful in hiding all information within the tested low details images. On the other hand, the results also show that utilizing ECB mode is not good. Also, the results show the superiority of OFB operation mode in terms of noise immunity compared with the others operation modes. The obtained results ensures the applicability of the proposed low image cryptosystem and its efficiency regarding of security, encryption quality, and immunity to noise.

REFERENCES

[1] Mohamed Amin, Osama S. Faragallah, Ahmed A. Abd El-Latif, "A Chaotic Block Cipher Algorithm for Image Cryptosystems," Communications in Nonlinear Science and Numerical Simulation, vol. 15(1), pp. 3484–3497, 2010.

[2] Osama S. Faragallah, "An Efficient Block Encryption Cipher Based on Chaotic Maps for Secure Multimedia Applications," Information Security Journal: A Global Perspective, vol. 20(3), pp. 135-147, 2011.

[3] Osama S. Faragallah, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm," Sensing and Imaging: An International Journal, vol. 12(3), pp. 73-94, 2011, Springer.

[4] Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas, S. El-Rabaie, Fathi E. Abd El-Samie, "A New Method for Encrypting Images with Few Details Using Rijndael and RC6 Block Ciphers in the Electronic Code Book Mode," Information Security Journal: A Global Perspective, vol. 21(4), pp. 193-205, 2012.

[5] Ahmad M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragallah, Yi Mu, Saleh A. Alshebeili and F. E. Abd El-Samie, "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding," IEEE/OSA Journal of Lightwave Technology, vol. 31(15), pp. 2533-2539, 2013.

[6] Fatma Elgendy, Amany M. Sarhan, Tarek E. Eltobely, S. F. El-Zoghdy, Hala S. El-sayed and Osama S. Faragallah, "Chaos-based model for encryption and decryption of digital images," Multimedia Tools and Applications, vol. 75(18), pp. 11529–11553, September 2016.

[7] T. Xiang, K. W. Wong, X. Liao, "Selective image encryption using a spatiotemporal chaotic system. Chaos: An Interdisciplinary Journal of Nonlinear Science," vol. 17(2), 2007.

[8] Luo Y, DuM, "A novel digital image encryption scheme based on spatial-chaos," J. Converg. Inf. Technol. (JCIT), vol. 7(3), 2012.

[9] Hossam El-din H. Ahmed, Hamdy M. Kalash, Osama S. Faragallah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Digital Images," Journal of Optical Engineering, vol.45, 2006.

[10] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, The RC6™ Block Cipher, 1998. http://www.rsasecurity.com/rsalabs/rc6/

[11] B. Gladman, A Specification for Rijndael, the AES Algorithm, May 2003, http://fp.gladman.plus.com/cryptography technology/rijndael/aes.Spec.311.pdf.

[12] Nawal El-Fishawy, Osama M. Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms," International Journal of Network Security, vol. 5(3), pp. 241-251, Nov. 2007.

[13] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with Few Details", Computers and Electrical Engineering, vol. 60, pp. 450-470, 2016.

[14] A. C. McBride and F. H. Kerr, "On Namias' Fractional Fourier Transforms", IMA J.Appl. Math., vol. 39, pp. 159–175, 1987.

[15] H. M. Ozaktas, "Fractional Fourier Domains", Signal Process, vol. 46, pp. 119–124,1995.

[16] H.M. Ozaktas, Z. Zalevsky, and M.A. Kutay, "The fractional Fourier transform," Wiley,

Chichester, 2001.

17. H.M. Ozaktas, M.A. Kutay, G. Bozdağı, "Digital computation of the fractional Fourier

transform," IEEE Trans. Signal Process., 44 (1996), pp. 2141–2150.

[18] Chai Wah Wu, Nikolai F. Rul kov, "Studying Chaos via 1-D Maps", IEEE Transactions on

[19] Circuits and Systems: Fundamental Theory and Applications", Vol.40, No.10, 1993.

[20] Yue Wu, Gelan Yang, Huixia Jin, and Joseph P. Noonan, "Image Encryption using

the Two-dimensional Logistic Chaotic Map", Journal of Electronic Imaging, 2012.

[21] NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes". Cryptographic Toolkit. NIST. Retrieved April 12, 2013.

[22] N. Ferguson, B. Schneier, T. Indianapolis, "Cryptography Engineering: Design Principles and Practical Applications," Wiley Publishing Inc. 2010.

[23] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996), Handbook of Applied Cryptography. CRC Press. pp. 228-233. ISBN 0-8493-8523-7.

[24] http://www.crypto.rub.de/its_seminar_ws080 9.html

[25] Abdul Hamid M. Ragab, Osama S. Faragalla, Amin Y. Noaman, "Encryption Quality Analysis of the RCBC Block Cipher Compared with RC6 and RC5 Algorithms," IACR Cryptology ePrint Archive, 2014.

[26] C.C. Chang, M.S. Hwang, T.S. Chen, "A New Encryption Algorithm for Image Cryptosystems," Journal of Syst. Software, vol. 58, pp. 83–91, 2003.

[27] S. Li, G. Chen and X. Zheng, "Chaos-Based Encryption for Digital Images and Videos," Chapter 4 in Multimedia Security Handbook, CRC Press LLC, 2004.

[28] H. Elkamchouchi and M. A. Makar, "Measuring encryption quality of Bitmap images encrypted with Rijndael and KAMKAR block ciphers," in Proceedings Twenty second National Radio Science Conference (NRSC 2005), pp. C11, Cairo, Egypt, Mar. 15,17, 2005.

[29] I. Ziedan, M. Fouad, and D. H. Salem, "Application of Data encryption standard to bitmap and JPEG images," in Proceedings Twentieth National Radio Science Conference, pp. C16, Egypt, Mar. 2003.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

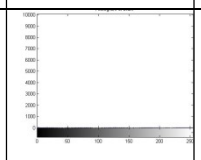
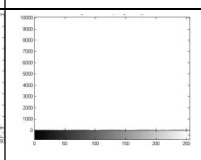
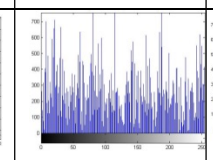
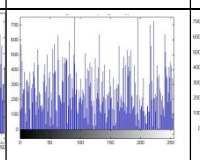
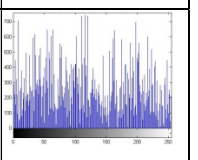
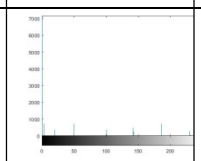
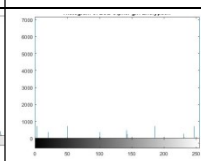
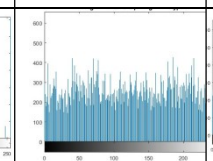
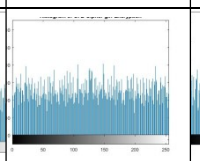
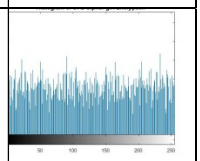
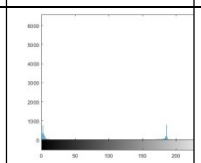
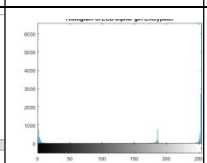
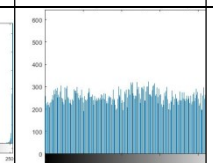
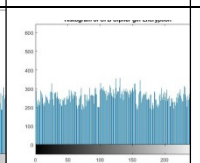
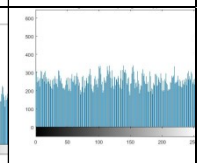
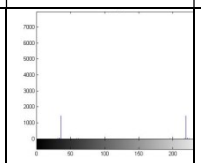
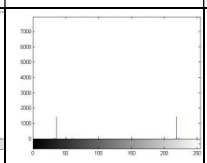
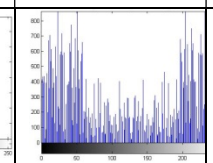
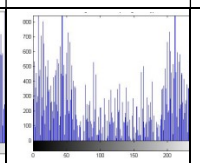
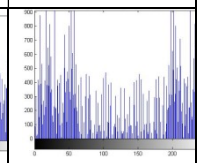
Image	Original image	The proposed low detailed fractional logistic image cryptosystem in different operation modes			
		ECB	CBC	CFB	OFB
Brain					
Chess board					
Tux					
Cs					

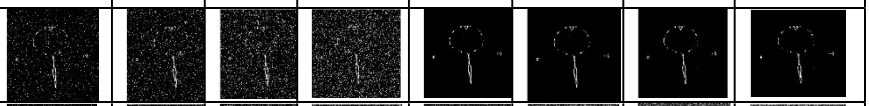
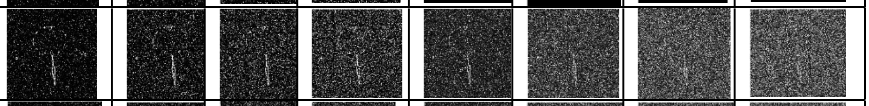
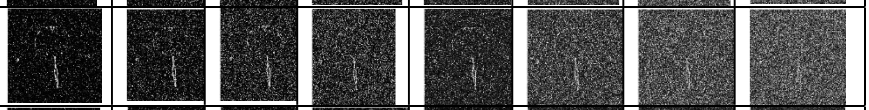
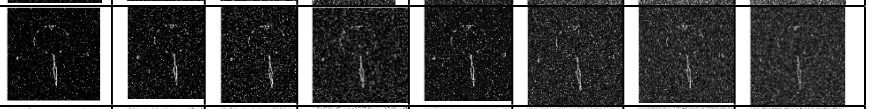
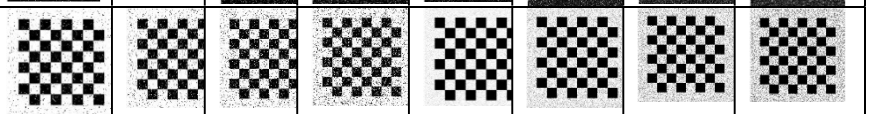
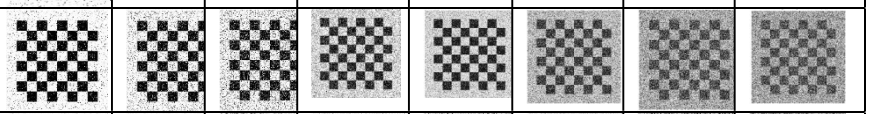
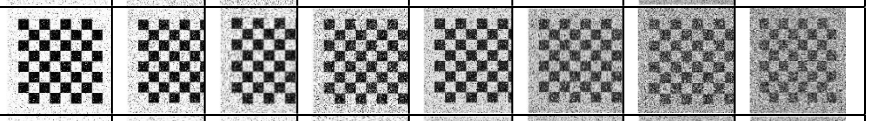
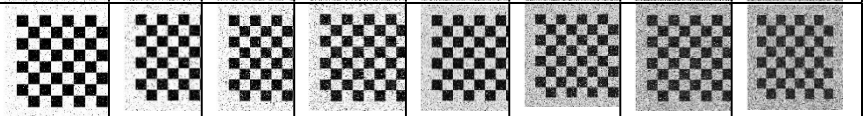
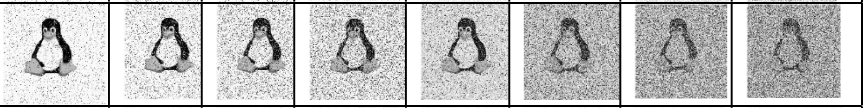
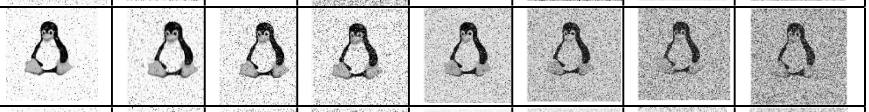
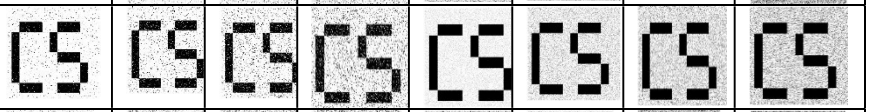
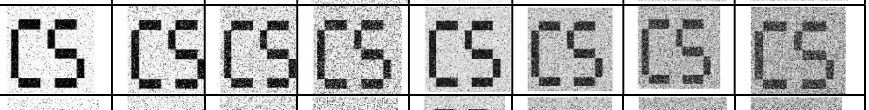
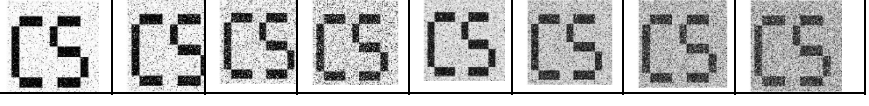
Fig. 7: Encryption results for the Brain, Chessboard, Tux, and CS images using the proposed few detailed fractional logistic image cryptosystem in different operation modes.

Table 5: The PSNR in dBs for the decrypted of Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes with the presence of noise of different variances.

Image	Algorithm	Peak Signal to Noise Ratio (PSNR)							
		Salt & peppers				Spackle			
		0.05	0.1	0.15	0.2	0.01	0.05	0.1	0.15
Brain	ECB	15.9783	1.3291	1.4011	1.4906	1.5298	1.9517	2.2483	2.4585
	CBC	14.6041	11.9361	10.0862	9.0094	10.6308	8.5978	7.5215	7.1142
	CFB	14.7674	11.8876	10.0403	8.9869	11.1525	8.2759	7.3809	7.0993
	OFB	17.4643	14.5219	12.8107	11.4493	14.3662	12.3282	11.7211	11.2981
Chessboard	ECB	16.0625	13.2045	11.3600	10.1518	24.5926	17.6842	14.6815	12.9558
	CBC	15.0279	11.8964	10.2499	9.1512	10.9248	8.3032	7.2551	6.9711
	CFB	15.1078	11.9693	10.3254	9.1573	10.6301	8.1553	7.3952	6.9567
	OFB	17.6234	14.5293	12.7649	11.4732	12.4649	10.5307	9.2488	8.7754
Tux	ECB	16.1854	13.0244	11.4289	10.1849	23.2524	16.3549	13.3545	11.6185
	CBC	15.0746	12.1737	10.4244	9.1991	10.6800	8.1393	7.4349	6.9946
	CFB	15.1697	12.1083	10.3233	9.1469	10.6098	8.1692	7.4549	7.0355
	OFB	17.5222	14.6736	12.9699	11.7494	11.9498	10.0895	8.6819	8.1691
Cs	ECB	16.1679	13.0107	11.3217	10.0456	24.0395	17.0721	14.1174	12.3514
	CBC	14.6135	11.6052	9.8812	8.6471	12.1171	9.7916	8.5065	7.8906
	CFB	14.5621	11.6711	9.9511	8.7368	11.8351	9.7471	8.4328	7.9235
	OFB	17.4666	14.5044	12.7712	11.5337	12.2035	10.9256	8.9140	8.4743

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6: The Decrypted Brain, Chessboard, Tux and CS images using the proposed low detailed fractional logistic image cryptosystem in different operation modes with the presence of noise of different variances

Image	Algorithm	Peak Signal to Noise Ratio (PSNR)							
		Salt & peppers				Spackle			
		0.05	0.1	0.15	0.2	0.01	0.05	0.1	0.15
Brain	ECB								
	CBC								
	CFB								
	OFB								
Chessboard	ECB								
	CBC								
	CFB								
	OFB								
Tux	ECB								
	CBC								
	CFB								
	OFB								
Cs	ECB								
	CBC								
	CFB								

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

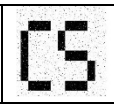
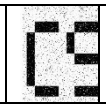
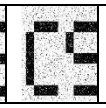
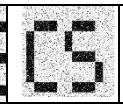
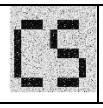
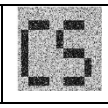
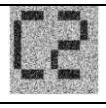
	OFB								

Table 7: The SSIM estimations of Decrypted of Brain, Chessboard, Tux and CS images using the proposed low detailed Fractional logistic image cryptosystem in different operation modes with the presence of noise of different variances

Image	Algorithm	Structural Similarity index (SSIM)							
		Salt & peppers				Spackle			
		0.05	0.1	0.15	0.2	0.01	0.05	0.1	0.15
Brain	ECB	**0.2488**	**0.0787**	**0.0394**	**0.02764**	**0.9991**	**0.9971**	**0.9964**	**0.9943**
	CBC	**0.0600**	**0.0293**	**0.01231**	**0.01866**	**0.0218**	**0.0152**	**0.0124**	**0.0108**
	CFB	**0.0631**	**0.0289**	**0.0225**	**0.0195**	**0.0233**	**0.0157**	**0.0112**	**0.0101**
	OFB	**0.1914**	**0.06224**	**0.0369**	**0.0279**	**0.0339**	**0.0254**	**0.0228**	**0.0199**
Chessboard	ECB	**0.4544**	**0.3054**	**0.2357**	**0.2045**	**0.6486**	**0.5291**	**0.4884**	**0.4647**
	CBC	**0.3162**	**0.2305**	**0.1902**	**0.1647**	**0.2053**	**0.1343**	**0.1011**	**0.0901**
	CFB	**0.3189**	**0.2354**	**0.1921**	**0.1622**	**0.1965**	**0.1304**	**0.1060**	**0.0930**
	OFB	**0.4455**	**0.3083**	**0.2542**	**0.2219**	**0.2551**	**0.2042**	**0.1746**	**0.1589**
Tux	ECB	**0.3029**	**0.1369**	**0.0940**	**0.0698**	**0.3384**	**0.1668**	**0.1294**	**0.1137**
	CBC	**0.1486**	**0.0926**	**0.0694**	**0.0547**	**0.0756**	**0.0459**	**0.0385**	**0.0336**
	CFB	**0.1564**	**0.0911**	**0.0691**	**0.05561**	**0.0747**	**0.0469**	**0.0389**	**0.0335**
	OFB	**0.2788**	**0.1511**	**0.1061**	**0.0871**	**0.0977**	**0.0767**	**0.0608**	**0.0554**
Cs	ECB	**0.3571**	**0.1856**	**0.1358**	**0.1075**	**0.4999**	**0.3608**	**0.3287**	**0.3120**
	CBC	**0.1904**	**0.1252**	**0.1004**	**0.0814**	**0.1353**	**0.1003**	**0.0792**	**0.0689**
	CFB	**0.1940**	**0.1253**	**0.0999**	**0.0842**	**0.1314**	**0.0996**	**0.0793**	**0.0703**
	OFB	**0.3139**	**0.1862**	**0.1446**	**0.1225**	**0.1451**	**0.1162**	**0.0964**	**0.0886**

Table 8: The FSIM estimations of Decrypted Brain, Chessboard, Tux and CS images using the proposed low detailed Fractional logistic image cryptosystem in different operation modes with the presence of noise of different variances.

Image	Algorithm	Feature Similarity Index (FSIM)							
		Salt & peppers				Spackle			
		0.05	0.1	0.15	0.2	0.01	0.05	0.1	0.15
Brain	ECB	**0.6429**	**0.5327**	**0.4349**	**0.3691**	**0.9991**	**0.9982**	**0.9983**	**0.9974**
	CBC	**0.4262**	**0.2541**	**0.1658**	**0.1128**	**0.1286**	**0.0845**	**0.0710**	**0.0653**
	CFB	**0.4338**	**0.2519**	**0.1625**	**0.1143**	**0.1406**	**0.0814**	**0.0691**	**0.0656**
	OFB	**0.5755**	**0.4317**	**0.3289**	**0.2430**	**0.2859**	**0.1568**	**0.1359**	**0.1252**
Chessboard	ECB	**0.8445**	**0.7264**	**0.6256**	**0.5494**	**0.7878**	**0.6846**	**0.6471**	**0.6259**
	CBC	**0.6383**	**0.4507**	**0.3553**	**0.3015**	**0.3367**	**0.2549**	**0.2217**	**0.2125**
	CFB	**0.6443**	**0.4584**	**0.3591**	**0.2998**	**0.3273**	**0.2316**	**0.2259**	**0.2139**
	OFB	**0.7914**	**0.6331**	**0.5231**	**0.4343**	**0.4224**	**0.3317**	**0.2991**	**0.2829**
Tux	ECB	**0.6284**	**0.5105**	**0.4336**	**0.3672**	**0.3968**	**0.2451**	**0.1995**	**0.1776**
	CBC	**0.4302**	**0.2752**	**0.1922**	**0.1485**	**0.1689**	**0.1206**	**0.1094**	**0.1036**
	CFB	**0.4396**	**0.2726**	**0.1908**	**0.1457**	**0.1661**	**0.1206**	**0.1089**	**0.1040**
	OFB	**0.5632**	**0.4359**	**0.3369**	**0.2704**	**0.1911**	**0.1553**	**0.1322**	**0.0162**
Cs	ECB	**0.8111**	**0.6772**	**0.5757**	**0.4923**	**0.6788**	**0.5493**	**0.5085**	**0.4837**
	CBC	**0.5934**	**0.4032**	**0.2983**	**0.2359**	**0.2928**	**0.2293**	**0.1975**	**0.1829**
	CFB	**0.5951**	**0.4022**	**0.2992**	**0.2352**	**0.2863**	**0.2287**	**0.1955**	**0.1845**
	OFB	**0.7434**	**0.5784**	**0.4606**	**0.3743**	**0.3314**	**0.2574**	**0.2264**	**0.2148**