Applications of Chaotic Maps and Coding for Secure Transmission of Images over Wireless Channels

Mona F. M. Mursi[1], Ayman H. Abd El-aziem[2]

[1, 2] Department of Electrical Engineering, Shubra Faculty of Engineering, Benha University, Egypt.

Abstract-In this paper we present the applications of image encryption techniques and channel coding techniques, to design scheme effective for secure image transmission over wireless channels, we present three proposed scheme as follow: First scheme apply image encryption by a combination of hybrid chaotic maps using Baker map and our proposed Hénon chaotic map 3 in three different modes of operations, beside using fractional Fourier transform (FRFT). Second image encryption scheme is combine the main advantages of FRFT, Arnold cat map for confusion and our proposed Hénon chaotic map 3 for diffusion. Third scheme based on combination of hybrid chaotic encryption and low density parity check (LDPC) to secure transmission of image over wireless channel. Our proposed scheme improve throughput. The proposed scheme enhanced the performance parameters and achieved both security and reliability of image transmission over wireless channels.

Keywords: Image encryption Chaotic maps ECC.

1. Introduction

Nowadays, the world lives in the age of communications revolution which necessitates multimedia transmission in a secure manner. Encryption is important in transferring images through the communication networks to protect them against reading, alteration of its contents, adding false information, or concealing part of its contents [1]. Owing to the frequent flow of digital images across the world over the transmission media, it has become essential to secure them from threatening or brute force attacks.

In recent years, there are many algorithms introduce the image security in different principle as [2-3]. Chaos based encryption algorithms are considered good for practical use as it provide a good combination of high speed, good security, and computational power. The security of image transmission strategy through wireless networks is considered a great challenge. However, the majority of encrypted image transmission schemes don't consider well the effect of bit errors occurring during transmission. These errors are due to the factors that affect the information such attenuation, nonlinearities, bandwidth limitations, multipath propagation and noise [4]. That should be handled by an efficient channel coding scheme.

Nowadays the usage of wireless network is increased, but the transmission of data over wireless network is subject to noise and intruder. So that it should to increase the security and the error protection to make wireless network reliable and high secure [5]. Error control codes (ECC) are an important issue in wireless transmission, and are used to protect data from channel errors. To improve the throughput in noisy environments, channel coding is performed after encryption.

There are many researchers who have introduced error correction and encryption in communication networks that have been addressed independently [6- 7]. Several researchers have studied the trade-off between encryption and error correction by trying to combine these functionalities in one unit. For instance, Gligoroski et al [8].

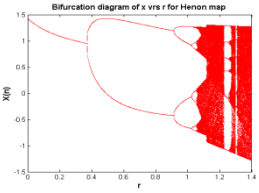
2. Two Dimensional Chaotic Map

2.1 Hénon chaotic system

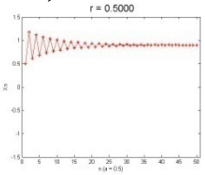
The Hénon map is two dimensional chaotic maps. It takes a point (x_i, y_i) and maps it to a new point in the same plane. It can be describing as follows [9-10-11]:

$$\begin{aligned} x_{i+1} &= 1 - rx_i^2 + y_i \\ y_{i+1} &= bx_i \qquad\qquad ,i = 0,1,2,..... \end{aligned} \tag{1}$$

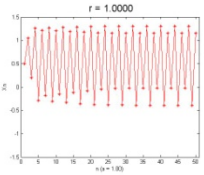
Hénon map presents a simple 2-D chaotic map with quadratic nonlinearity, depends on two parameters, r and b, which for the canonical Hénon map have values of r = 1.4 and b = 0.3. For the canonical values the Hénon map is chaotic. This map has chaotic behavior in range [1.07, 1.4], for other values it behave as periodic or convergence to constant value. The initial value and the value of parameter r are very important to make the Hénon strange attractor, or diverge to infinity. Hénon map gave a first example of the strange attractor with a fractal structure. Because of its simplicity, the Hénon map easily lends itself to numerical studies. Thus a large amount of computer investigations followed. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters r and b is far from completeness.



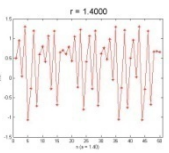
a) The bifurcation diagram for $r \in [0,1.4]$



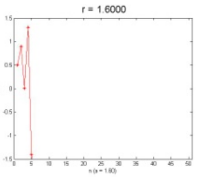
c) Iteration property when $r = 0.5$



d) Iteration property when $r = 1$



e) Iteration property when $r = 1.4$



f) Iteration property when $r = 1.6$

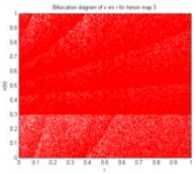
Figure (1) Analysis of Hıınon chaotic map

2.2 The proposed Hénon chaotic map 3

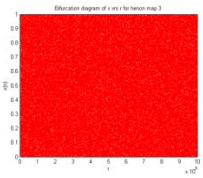
Our proposed Hénon chaotic map 3, which is developed to give a chaotic function, can be used in cryptography application. Hénon map 3 is expressed as followed:

$$x_{i+1} = (r \times x_i + y_i) mod\ 1$$
$$y_{i+1} = \frac{b}{1 - x}\ , i = 0,1,2 \qquad (2)$$

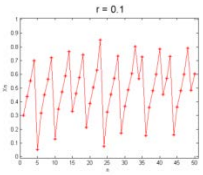
The development of the Hénon chaotic map 3 increases the chaotic range of parameter $r \in [0, \infty]$ that will increase the available chaotic value of parameter r to be used in encryption. The proposed Hénon chaotic map 3 gives a very wide range of variable r for using in encryption and we can use any value of variables r in encryption.



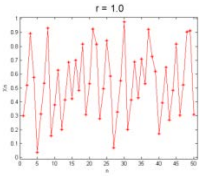
a) The bifurcation diagram for $r \in [0,1]$



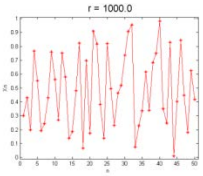
b) The bifurcation diagram for $r \in [0,10^6]$



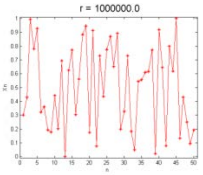
c) Iteration property when r = 0.1



d) Iteration property when r = 1



e) Iteration property when r = 1000



f) Iteration property when $r = 10^6$

Figure (2) Analysis of proposed Hénon chaotic map 3

3. Fractional Fourier Transform Domain

The Fourier Transform (FT) is one of the most frequently used tools in signal analysis. A generalization of the FT is the FRFT. It has been proposed in [12] and has become a powerful tool for time-varying signal analysis. The FT can be interpreted as a rotation of the signal by an angle of $\pi/2$ in the time–frequency plane and represented as an orthogonal signal representation for sinusoidal signals. The FRFT performs a rotation of the signal in the continuous time–frequency plane to any angle and serves as an orthogonal signal representation for the chirp signal, the FRFT is related to other time-varying signal analysis tools, such as the Wigner distribution, the short-time FT, the wavelet transform.

The chaotic map in the spatial domain has a drawback that keeps the statistical characteristics of the image intact after scrambling. The transform domains provide the ability to transform correlated data patterns into transforming domains to carry the substitution or diffusion process in these domains. Chaotic encryption is performed in this transform domain to make use of the characteristics of this domain. The angle of the Fractional Fourier transform does not affect encryption quality. This is considered a good property for the FrFT domain as it allow using a wide range of angles without any restriction this make it very hard to any attacker to exactly expect the angle used in the domain. This increases the sensitivity of the transform.

4. Hybrid Chaotic Map for Image Encryption schemes

We proposed two image encryption schemes, first scheme based on using a multiple of chaotic maps in different modes of operation using the fractional Fourier transform domain as shown in figure 3. The proposed algorithm is divided into two parts: first applying the fractional Fourier transform to the original image; the second part combines the confusion with diffusion. The confusion algorithm using 2-D chaotic Baker map. The diffusion applied on the proposed of Hénon map 3. The proposed algorithm cryptosystem has high security performance as it fulfills the classic Shannon requirements of confusion and diffusion [13]. We examine its implementation for digital images along with its detailed security analysis to study the effect of modes of operation on the performance of chaotic cryptosystem implemented in the FRFT domain. Besides that, applying the development of the Hénon chaotic map to increase the security and make the relation between image and encrypted image more complex. We examine its implementation for digital images along with its detailed security analysis.

The diagram of the combination of the confusion and diffusion algorithm with FRFT to produce cipher image is shown in figure 3.

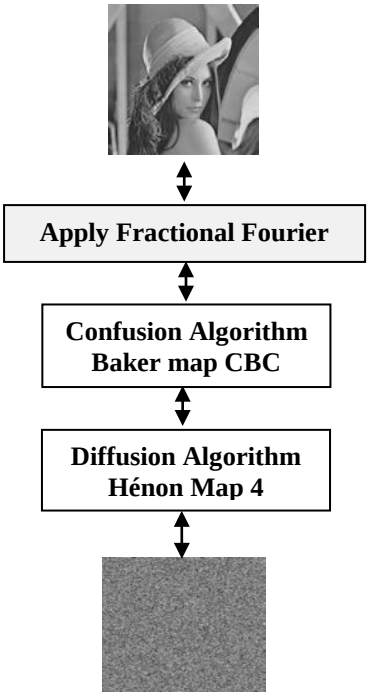


Figure 3 The block diagram of the proposed scheme 1

Second scheme propose a new image encryption algorithm based on the development of Hénon chaotic map using FRFT. The proposed algorithm is divided into two parts; first applying FRFT to original image, then combine the confusion with diffusion. The confusion algorithm is the Arnold Cat map which is applied on the FRFT image. This procedure achieves shuffling of the positions of the pixels of the plainimage. The diffusion algorithm using proposed Hénon chaotic map 3. The proposed algorithm cryptosystems have high security performance to fulfill the classic Shannon requirements of confusion and diffusion. The Diagram of our proposed algorithm can be shown in figure 3.

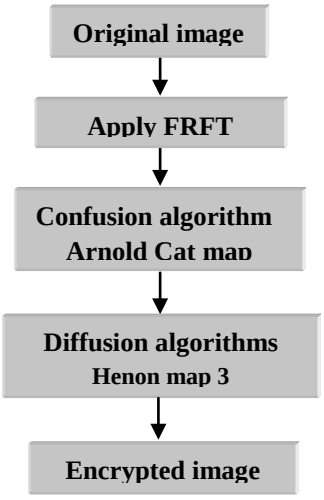
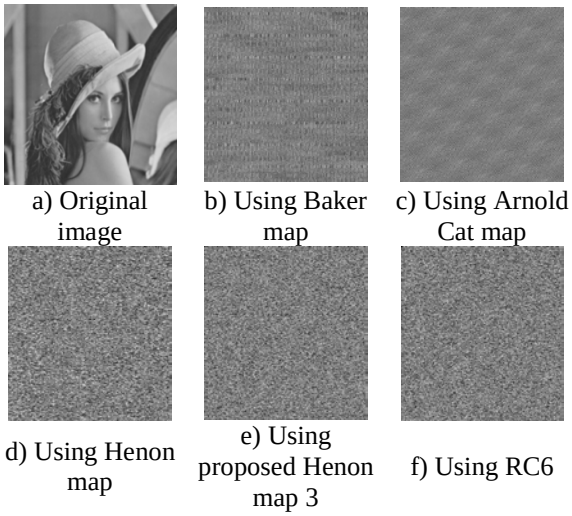


Figure 4 The block diagram of the proposed scheme 2.

5. Encryption Evaluation Metrics and Experimental Results

In this section we examine the quality of the two schemes of image encryption by measure the evaluation metrics. Visual inspection is the most important method to examine of the quality of image encryption. It is clear there are not any details of using our encrypted image using proposed algorithms, but it is not sufficient to depend on the visual inspection only. So, other metrics are measure to determine the degree of image encryption [9 14]. Our proposed scheme 2 has been applied to the original image, and compared with some different chaotic maps as Arnold cat map, Baker map, Hénon map and RC6 algorithms [14-15] as can be shown in Figure 6. It is clear that the different algorithms show hidden details of the image. It gives good results for encryption, but we can't determine which of these algorithms give better results; hence we perform different tests to the algorithms to determine the best. So that it should to measure other metrics to evaluate the degree of encryption quantitatively.



a) Original image b) Using Baker map c) Using Arnold Cat map

d) Using Henon map e) Using proposed Henon map 3 f) Using RC6

Figure (5) The encrypted image using Different chaotic Maps

5.1 Statistical Analysis

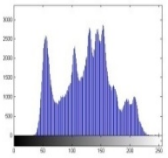
To examine the quality of encryption and the stability via statistical attacks, the histogram is calculated for all images, correlation coefficient (CC) between original image and cipher-image, maximum deviation factor (MD), and irregular deviation factor (ID).

5.1.1 Histogram Analysis.

The original image Lena with the size 512×512 pixels is shown in Figure 6 (a) and the histogram of the original-image and encrypted image using scheme 1 is shown in Figure 6 (b, c) respectively. As we can see, the histogram of the encrypted image is fairly uniform and completely different from the histogram of the original image because of the diffusion caused

by the effect of modes of operation beside the diffusion caused by applying our proposed Hènon chaotic map 3. So, modes of operation beside Hènon chaotic map 3 and using chaotic cryptosystem applied in FRFT domain improve the histogram of the encrypted images.


a) The original image


b) Histogram of original image

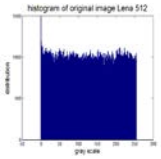
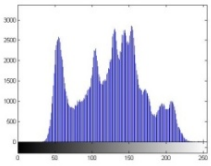
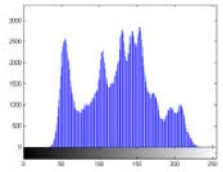

b) Histogram of encrypted image

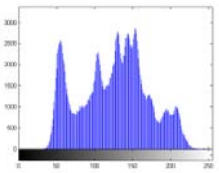
Figure (6) Histogram analysis of proposed scheme 1

The histogram of the original image, shuffled-image by using an Arnold Cat and shuffled-image by using the Baker Chaotic map is shown in figure 7(a, b, c) respectively. It is clear that the Baker map and Arnold cat map doesn't change the histogram of the encrypted image from the original image because it makes only permutation to the pixels of the image.

Figure 7(d) illustrate our proposed algorithm using our proposed scheme 2 it is uniformly distributed and totally different from the original histogram. As we can see from the visual inspection, our proposed algorithm improves the encrypted image as their hiding information and has no symmetric blocks. Also, they improve the histogram of the encrypted image


a) The histogram of the original image


b) The histogram of encrypted image using Baker map.


b) The histogram of encrypted image using Arnold Cat map

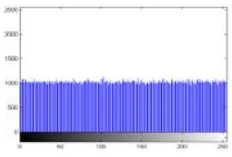

c) The histogram of encrypted image using Proposed Henon map 3.

Figure (7) The histogram analysis of proposed scheme 2

5.1.2 Correlation Coefficient Analysis

The correlation coefficient (CC) measure the correlated between the pixels in the encrypted image and the original image it is equal to one when the original and encrypted image high correlated and it equal to zero when there are not correlated [3- 17-18].

The correlation coefficient between the original image and the encrypted image using our proposed scheme 1 can be shown in table 1. It is clear that the correlation coefficient decrease as the block size increase. This is due to the fact that the number of XOR operations used in any mode of operation to decrease as the block size increase.

Table 1 The CC between the original image and encrypted images using the proposed scheme 1

Mode of operation	Block size		
	W_1	W_2	W3
CBC	**0**	0.0008	0.0041
CFB	**0**	**0**	0.0011
OFB	**0**	0.0011	0.0011

5.1.3 Maximum Deviation analysis

We measure the deviation between original and encrypted image to determine the quality of image encryption [3-18]. Table 2 illustrates the maximum deviation measuring factor using proposed scheme 1 [3-17] of the encrypted images. As we can see, the CBC mode with W_2 achieved better results compared to other cases and CFB mode with W_2 makes the worst results between all modes.

Table 2 The maximum deviation metric of the proposed scheme 1.

Mode of operation	Block size		
	W_1	W_2	W_3
CBC	187898	**188346**	187850
CFB	187973	187320	186720
OFB	188285	188100	188100

5.1.4 Irregular deviation analysis

This analysis it measure the deviation caused by encryption in the histogram by measure how it irregular [3]. The irregular deviation metric can be used alone to test the quality of encryption in the field of image encryption. So, if this factor agrees with other metrics, it will be a good judge, otherwise the final decision on measuring the quality of the encryption algorithms will be on the irregular deviation on this test. From the results shown in Table 3 which represent our proposed scheme 1, the CFB with W_2 has better results than the other cases but CFB mode with W_3 has the worst result.

Table 3 The irregular deviation metric of the proposed scheme 1

Mode of operation	Block size		
	W_1	W_2	W_3
CBC	180464	180676	181114
CFB	180378	**180296**	181286
OFB	180826	180988	180988

5.1.5 NPCR and UACI analysis

To evaluate the variations between the original image and the decrypted images, there are two additional tests: NPCR and UACI.

Table 4 The UACI between encrypted image and original image using proposed scheme 1

Mode of operation	Block size		
	W_1	W_3	W_5
CBC	28.6269	28.6053	28.5549
CFB	28.6140	**28.6469**	28.5595
OFB	28.6260	28.5988	28.5988

Table 5 The NPCR between encrypted image and original image in using proposed scheme 1

Mode of operation	Block size		
	W_1	W_3	W_5
CBC	99.61	99.62	**99.63**
CFB	99.61	99.61	99.61
OFB	99.61	**99.63**	**99.63**

5.2 Time Analysis

The processing time has also been tested for our proposed scheme 1. First, it is defined as the times required to encrypt/decrypt data. The smaller the processing time, the higher the speed of encryption is. From table 6 we can conclude that the processing time doesn't depend on the mode of operation used, and the processing time increases with the decrease of the block size. This is due to the number of XOR operations increases with the decrease of the block size.

Table 6 The processing time of the encryption process versus block size in sec.

Mode of operation	Block size		
	W_1	W_3	W_5
CBC	**2.63**	3.15	15.41
CFB	**2.53**	3.05	15.51
OFB	**2.78**	3.43	15.04

The rest of all tests of our proposed scheme 2 are applied and the results of measuring factors of the proposed algorithm with FRFT domain and other algorithms are given in Table 7 where CC indicates the correlation coefficient between the original image and encrypted one, MD indicates the maximum deviation measures, ID indicates the irregular deviation measures, T indicates the processing time in seconds, UACI indicate Unify average change intensity between original image and encrypted one and NPCR indicate number per change rate between original image and encrypted one

Table 7 The encryption evaluation measurements of the encrypted images in SD and FRFT domains.

		CC	MD	ID	Time	UACI	NPCR	Entropy
Chaotic Baker Map	**SD**	0.0032	0	256816	3.66	20.23	99.28	7.4379
	FrFT	**0**	56029	248988	3.65	20.77	99.35	7.4379
Arnold Cat Map	**SD**	0.0008	0	256968	0.6412	20.28	99.33	7.4379
	FrFT	**0**	56029	252780	**0.6303**	20.63	99.33	7.4379
Hybrid system (Cat + Hénon3)	**FrFT**	**0**	**187430**	**183490**	1.77	**28.55**	**99.6418**	**7.9993**
RC6	**S D**	0.0013	186907	184910	800	22.31	99.60	7.4379

Based on this table, we can conclude that:

1. The correlation coefficient CC is measuring factor: In general, all the algorithms have a good correlation. But the encrypted image has the best results with our proposed algorithm using Hènon map 3, the correlation coefficient between the original image and the encrypted image, has been improved through our proposed algorithm besides FRFT improves the CC with any algorithm.
2. The Maximum deviation MD measuring factor: proposed algorithm using Hènon map 3 achieved the highest result. But the Baker and Cat map in spatial domain (SD) and FRFT domain has the worst result compared to all algorithms.
3. The irregular deviation ID measuring factor: In this test, our proposed algorithm using Hénon map 3 has the best result. FRFT domain improves the results with each algorithm. But the spatial domain with cat and baker maps has the worst results in the proposed algorithms.
4. The NPCR: in general, all the algorithms have a good NPCR, the best result with our proposed algorithm using Hénon map 3 and the worst case with Baker map at spatial domain.
5. In UACI, the best result is with the proposed algorithm using Hénon map 3 and the worst case obtained with baker map in spatial domain.
6. It is clear that RC6 algorithm has a very large computational time that made it unsuitable for real time applications.
7. The processing time, in our proposed algorithm, takes much more time because of the complexity of the system. In general, to improve the processing time. We use the proposed Hénon map 3 in the FRFT domain, which give good

results than the single algorithms and provide higher encryption quality.

In general, all maps in FR FT domains have results better than RC6 algorithm.

5.2 Security Analysis

A good encryption scheme should resist most kinds of known attacks, it should be sensitive to the secret keys, and has large key space to make brute force attacks infeasible. And the key space it should be very large to can resist all kinds of brute-force attacks.

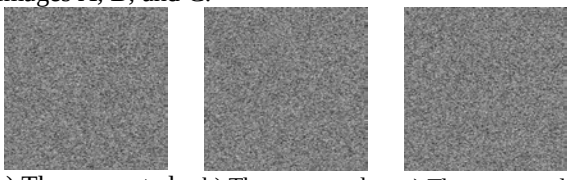
5.2.1 Key Sensitivity Analysis

The sensitivity of key is more important in the measuring of security of the image cryptosystem, which means that the cipher image cannot be decrypted correctly if there is only a very small difference between the keys used for encryption and decryption.

For the proposed scheme 1, we test the sensitivity of the key by two methods, fist we make small changes in one parameter of key (r, b, x_0 ,x_1,) of the our proposed Hénon map 3. We can also test the sensitivity by a change in angle of FRFT by changing the value **a**; change key which using an encryption we can perform the following steps:

1. The original image is encrypted using the secret keyusing b = 0.4, r = 11, x_0 = 0.01, x_1 = 0.02. The encrypted image can be shown in figure 8 (a).
2. The same image is encrypted by making a slight modification in the secret key using *r*=11.1 the encrypted image can be shown in figure 8 (b).
3. Again, the same image is decrypted by making another slight modification in the secret key using *r*= 11.2, the encrypted image can be shown in figure 8 (c).

Finally, we compare among the three encrypted images A, B, and C.



a) The encrypted image A b) The encrypted image B. c) The encrypted image C

Figure 8 Applying the proposed algorithm using different keys

We cannot compare among the previous three encrypted images by depend on observing them. Thus, for comparison, we can calculate the correlation coefficients between the original image and the three encrypted images. The lower the correlation coefficient, the higher key sensitivity is.

Table 8 The correlation coefficients between the three encrypted images A, B, and C

Image 1	Image 2	C.C
Encrypted image A	Encrypted image B	-0.0006
Encrypted image B	Encrypted image C	0.0014
Encrypted image A	Encrypted image C	0.0017

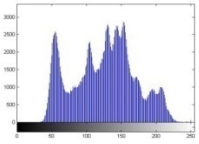
From the previous table we can see that the correlation coefficients for the three cases are low thus proving a high key sensitivity and the three different images are completely different.

Second method for test sensitivity of our proposed algorithm 1 can be done as follows: we test the sensitivity of the key by making a small change in the constant r, b, xo and x1 of the our proposed hénon map 3. We can also test sensitivity by changing the angle of FRFT by changing the value a1; changing the key which is used in encryption, we can perform the following steps:

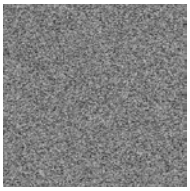
1. The original image is encrypted using the secret key using, r=11, b=0. 4, x0 = 0.01, x1=0. 02, the original image is shown in figure 9 (a) and the decrypted image using the same key shown in figure (b) it is clear that the decrypted as original image and its histogram has been illustrated in figure 9 (c).
2. The same image is decrypted by making a slight modification in the secret key using r=11.000000000000001, such that r is changed a little (10^{-15}), as shown in figure 9 (d) the decrypted image is completely different than the original image The original image is encrypted using the secret keyusing b=0.4, r=11 x0 =0.01, x1=0.02 and the encrypted image using the same key as shown in figure 10 (d) it is clear that the decrypted as the encrypted image and its histogram has been illustrated in figure 9 (e).

a) The original image

b) decrypted image at *r*=11, *b*=0.4, *x0*=0.01, *x1*=0.02



c) Histogram of the decrypted image.



d) decrypted image (at *b*=0.4, *x0*=0.01, *x1*=0.02 *r*=11.00000000000001,

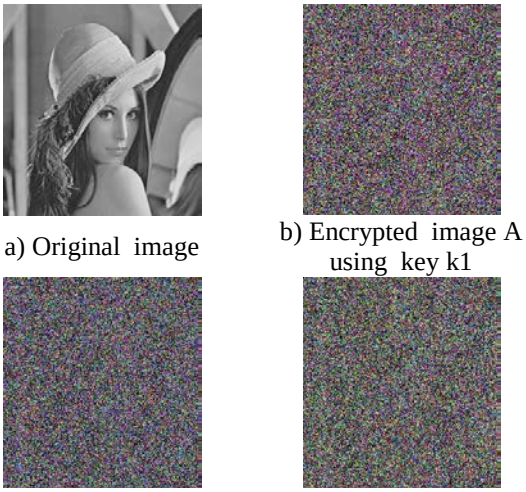
e) Histogram of the decrypted image.

Figure (9) Applying the proposed algorithm using different keys

For testing the sensitivity of key for our proposed image encryption scheme 2 by using Hènon chaotic map 3, we have performed the following steps:

- As shown in figure 10 (a, b) is original image and encrypted image (A) respectively by applying our proposed algorithm using the following parameter of Hénon map 3 using the secret key1 as follows: r=11, b = 0.3, x_0=0.01, x_1 = 0.02, p=1, q=2 and iteration =10.
- We make slight modification at parameter r = 11.1 and apply the proposed algorithm at this in case the key called k2, the encrypted image (B) is shown in figure 10 (c)
- Again, the same original image is encrypted by making the slight modification in the secret key3 to become r=11.2 as shown in figure 10 (d) encrypted image (C).
- Finally, we compare among three encrypted images A, B and C.

We have shown the original image and the three encrypted images produced, it is clear that it not sufficient to judge the difference between the three encrypted images by visual inspection. So that, we have calculated the CC between the corresponding pixels in the three encrypted images, also we measure the NPCR between the three encrypted images. All these results are tabulated in table 8.



a) Original image b) Encrypted image A using key k1

c) Encrypted image B using key k2 d) Encrypted image C using key k3

Figure (10) Key sensitive result with using proposed Hınon chaotic map 3

It is clear from the following results in table 9 there are no correlation exists among three encrypted images and the value of NPCR are larger than %99.6 which mean that our algorithm are very sensitive for any small change in the key.

Table 9 Correlation coefficients and NPCR between the three different encrypted images

Image 1	Image 2	C.C	NPCR
Encrypted image A	Encrypted image B	**0**	99.6132
Encrypted image B	Encrypted image C	**0**	99.6155
Encrypted image C	Encrypted image A	**0**	99.6239

5.2.2 Exhaustive Key Search

When we design image encryption it should to design algorithm with large key space enough to make the brute force attack infeasible. An exhaustive key search will take 2^k operations to succeed, where k is the key size in bits. An attacker simply tries all keys, and this will be very exhaustive. For our proposed scheme 1 using chaotic maps, the key is dependent on the width (or height) of the image to be encrypted. This is due to the scrambling phenomenon of the chaotic map. For the 512x512 Lena image, the number of possible keys =10^{128}. Thus, in this case the computations will require:

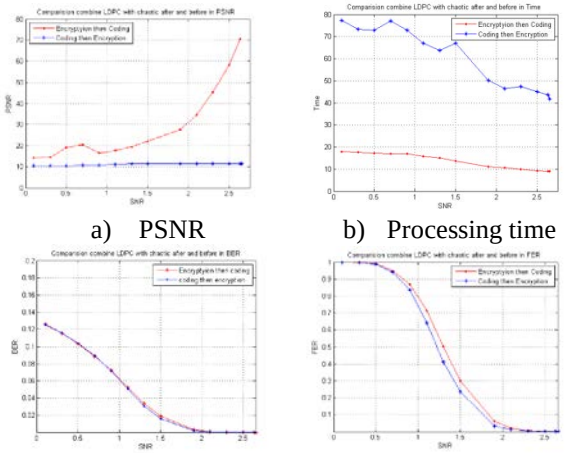
$$\frac{10^{128}}{1 \times 10^9 \times 60 \times 60 \times 24 \times 365} = 4.3675 \times 10^{11}\ year$$

This is practically infeasible. Beside that we have the parameter r, b, x_0, x_1 of our proposed Hénon chaotic map are another key and the angle of FRFT, all these parameters are key of our proposed algorithm.

6. Combination of Hybrid Chaotic Encryption and LDPC Code

6.1 Procedure of Combining Encryption with Coding

The encryption and LDPC algorithms are applied in two different methods; first we applied coding, then encryption as follows: we first applied encoding the original image (cameraman.bmp) using LDPC then applied encryption using the Arnold cat map as a type of encryption [4], we use BPSK for modulation and AWGN as a channel. The second method is using the same algorithm but in this case we applied the encryption first, then coding. At the destination, we applied decode, and then decrypted the decoded image. We compare between the two methods by measuring BER, FER, PSNR and processing time. The simulation results of the two methods can be shown in the following figures 11.



a) PSNR b) Processing time

c) BER d) FER parameter

Figure (11) The experimental result of combining encryption with LDPC coding after and before

From the previous figure 11 we can conclude that:

1. By measuring the parameter PSNR, as can be shown in figure 11, it is evident that applying encryption, then coding gives better results in the reconstruction of the decoded decrypted image.
2. There are small improvements in BER and FER by applying coding then encryption, as is clear from figures 8 and 9.
3. The performance of applying encryption then coding has smaller execution time compared to the time executed by applying coding then encryption. That is due to the fact that in the coding then encryption, we encrypt the parity which is added to the image in encoding the image. So combining encryption with coding is preferable to apply encryption and then coding.

6.2 Combination of Hybrid Chaotic Encryption and LDPC Code

We proposed a new scheme which combines encryption and then coding in one algorithm. We use a hybrid chaotic system as follow: first an image is transformed to FRFT domain [18]. Secondly, the transformed image is encrypted using two stages of image encryption using confusion and diffusion presented by Arnold Cat map for confusion and proposed Hénon map 3 for diffusion [18]. Finally the encrypted image is obtained. More details about this algorithm are shown in [18]. We combine this encryption algorithm with LDPC codes for channel coding. The encoded encrypted image is then modulated by Binary Phase Shift Keying (BPSK), transmission over channel Additive white Gaussian noise (AWGN), which is considered in our simulation. AWGN is a basic noise model used in information theory to mimic the effect of many random processes that occur in nature. At the receiver side, the received image was demodulated, decoded and decrypted. After decryption, we will pass the image through a median filter to reduce noise.

We compare our proposed algorithm by combining LDPC code with three different algorithms. First applying RC6 [21], second applying Baker chaotic map [21], and finally applying LDPC without encryption. We compare among all these algorithms in tests for BER, FER, and PSNR. We will carry out a comparison between the image transmission using this proposed scheme and the transmission of the original image using the previous algorithms. We compare between them to determine the performance of our proposed scheme and measure the ability for secure image transmission and error correction in the noisy channels.

6.3 Experimental Results

We combine three different image encryption algorithms with LDPC to decide on the best of them. First we combine Baker chaotic map with LDPC code [21]. Second, combine RC6 with LDPC code [20]. Third apply LDPC without encryption; finally our proposed algorithm hybrid chaotic map using FRFT [19] combined with LDPC code. We make comparisons among all these algorithms in some tests as BER, FER, and PSNR. The result of the combination of different encryption and LDPC can be shown in the following tables and figures.

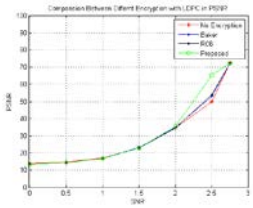


Figure 12 PSNR vs. SNR for combining different encryption models with LDPC

Peak Signal to Noise Ratio

Figure 12 shows the PSNR against SNR. Which measure the ratio between the maximum possible power of a signal and the power of corrupting noise which affects the quality of its representation. PSNR values are measured Appling four models for the combination of Hybrid chaotic and LDPC coding for various Signal to Noise Ratios (SNRs) of the received cameraman image. The higher PSNR for the proposed scheme indicates more efficient system performance.

Bit Error Rate and Frame Error Rate

Figures 13 illustrate the BER and FER versus SNR. BER and FER are computed after decoding, as a function of signal to noise ratio BER and FER are measured for four models of combination of Hybrid chaotic and LDPC code for various SNRs. It is clear that the proposed scheme has very a small value of BER and FER at small SNR so that it has better error performance.

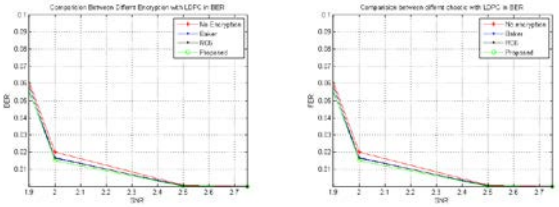
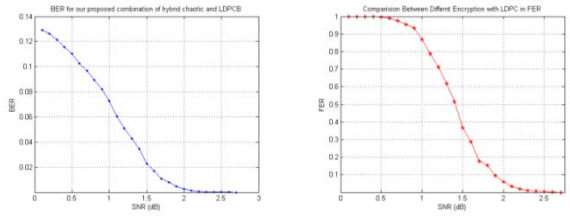


Figure (13) BER and FER for combining different encryption models with LDPC

From the previous figures and it is clear that our proposed algorithm with LDPC gives the best results compared with RC6, Baker and the original image without encryption.

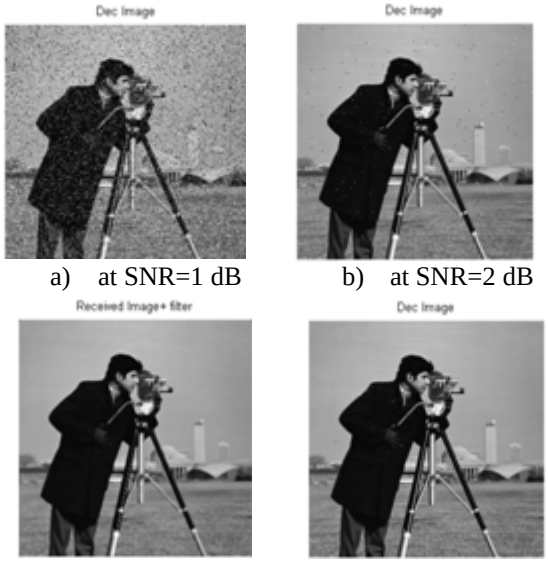
We introduce the performance analysis of our proposed algorithm to secure transmission of image through a noisy channel by drawing figures 14, which measure the BER, FER and processing time. It is clear that our proposed algorithm gives very small BER at small SNR and it has also high PSNR at small SNR. It executes at a short time when applying encryption, encoding, decoding and decryption of image all these algorithms execute in 14.55 sec at SNR = 2. Also, it can reconstruct the decoded decrypted image as the original image with noisy channel, besides, it could secure the transmission of image.



a) BER b) FER

Figure (14) BER and FER vs. SNR of the received Cameraman image with combination hybrid chaotic and LDPC

The following figures are produced from applying our proposed algorithm to secure transmission of the image besides error correction. We show the ability of the algorithm to correct the errors at different SNRs



a) at SNR=1 dB b) at SNR=2 dB

c) at SNR=2 dB using median filter d) at SNR=2.5 dB

Figures (15) Reconstructing image at different SNR besides error correction code

We can show the ability of the proposed scheme 3 to correct the errors at different SNRs by shown the reconstructed image at different values of SNR over AWGN channels. As shown a small change in SNR yields high quality in the reconstructed image. So that our proposed algorithm able to secure transmission of the image besides error correction in noisy channel.

It is observed that in the case of the reconstructed image for a channel with SNR = 1, 2, 2.5 dB with the combination of hybrid chaotic map and LDPC coding, it is possible to reconstruct the image clearly with the combination of LDPC coding, and the image is reconstructed without distortion. We don't need to retransmission of image when it noisy therefore our proposed algorithm increases the throughput of the system. The use of median filter on the receiver side improves the reconstruction of the image in the presence of noise as is clear in figure 15 (c, d). Our proposed scheme is effective for secure image communication over the wireless noisy channel.

7. CONCLUSION

This paper focuses on two main parts: first part introduced, a proposed two image encryption schemes based on multiple of chaotic system by combining confusion algorithm with diffusion algorithm. All of these procedures for encryption are used in FRFT domain. The experimental results and analysis show that the proposed cryptosystem has high security such that, the proposed scheme has very sensitive to all members of the secret keys.

Beside the development of Hénon chaotic map, by increases the available chaotic range of parameter "r" to be very wide.

Second part, we proposed a scheme for the combination of image encryption and error correction code. The proposed scheme combines image encryption based on hybrid chaotic encryption, and error control coding based on LDPC channel coding. Simulation results show that the proposed scheme enhanced the performance parameters and achieved both security and reliability of image transmission through the wireless channel. The proposed scheme is suggested for secure image transmission over wireless channels. It proposes to apply encryption before coding because of shorter execution time than when applying coding, prior to encryption.

References

[1] N. k. Pareek, Vinod Patidar, K. K. Sud." Image Encryption Using Chaotic Logistic Map" Image and Vision Computing 24, P.P (926-934) 2006.

[2] Ahmed, H. E. H., Kalash, H. M., & Faragallah, O. S. " Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images" In Proceedings of the International Conference on Electrical Engineering (ICEE) (pp. 1-7), 2007

[3] El-Fishawy, N., & Abu Zaid, O. M. "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms" International Journal of Network Security, pp. 241–251, 2006.

[4] Daniel J. Costello, Jr. and G. David Forney, Jr, Channel Coding: The Road to Channel Capacity, IEEE, Vol. 95, No. 6, June 2007.

[5] M. A. El-Iskandarani, Saad M. Darwish, Saad M. Abuguba, Combination of 2D chaotic Encryption and Turbo Coding for Secure Image Transmission, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.11, November 2010.

[6] Deergha Rao—A Robust and Secure Scheme for Image Communication over Wireless Channels‖, IEEE CAS on ETW Conference, pp.88-91, 2005.

[7] A. Padmaja and M. Shameem, —Secure Image Transmission over Wireless Channels‖, IEEE ICCIMA Conference, Sivakasi, Tamil Nadu, pp.44-48, January 2007.

[8] D. Gligoroski, S. Knapskog, and S. Andova, "Cryptcoding - Encryption and Error Correction Coding in a Single Step" International Conference on Security and Management, pp. 1-7, June 2006.

[9] E. Petrisor. Entry and exit sets in the dynamics of area preserving Hénon map. Chaos, Solitons and Fractals, pp. 651– 658, Oct. 2003.

[10] L. Guo-hui, Z. Shi-ping, X. De-ming, L. Jian-wen." An Intermittent Linear Feedback Method for Controlling Hénon- like Attractor". Journal of Applied Sciences, pp. 288–290, Dec 2001.

[11] Chen Wei-bin, Zhang Xin. "Image Encryption Algorithm Based on Hénon Chaotic System" 978-1-4244-3986-7/09/$25.00 © IEEE 2009.

[12] B. M. Hennelly and J. T. Sheridan, "Image encryption based on the fractional Fourier transform," *Proc. SPIE*, vol. 5202, pp. 76–87, 2003.

[13] C.E. Shannon, A Mathematical Theory of Communication, Bell Sys. Tech. J. 27:379 {423, 623 {656,} 1949.

[14]-Patel, K. D., & Belani, S. (2011). "Image encryption using different techniques: A review" *IJETAE, 1*(1).2011.

[15] Shang, Z., Ren, H., & Zhang, J. (2008). A block location scrambling algorithm of digital image based on Arnold transformation. In *the 9th International Conference for Young Computer Scientists*. 978-0-7695- 3398-8/08 © IEEE. doi:10.1109/ICYCS.2008.99, 2008.

[16] Hazem M. El-bakry, and Nikos Mastorakis, "Design of Anti-GPS for Reasons of Security,"Proc. of Recent Advances in Applied Mathematics and Computational and Information Sciences, Houston, USA, April 30- May 2, 2009, pp. 480-500.

[17] 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.

[18] 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 (NRSC 2003), pp. C16, Egypt, Mar. 2003.

[19] Mona F. M. Mursi, Hossam Eldin H. Ahmed, Ayman H. Abd El-aziem "Image Encryption Based On Development of Hénon Chaotic Maps Using Fractional Fourier Transform" International Journal of Strategic Information Technology and Applications, 5(3), 62-77, July-September 2014.

[20] H. E. H. Ahmed, H. M. Kalash, and O. S. Faragallah, ―Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images‖, International Conference on Electrical Engineering, pp. 1-7, April 2007.

[21] J. Fridrich. Image encryption based on chaotic ma.ps. In Proc. IEEE Int. Conference on systems, Man and Cybernetics, volume 2, pages 1105–1110, 1997.

[22] Hazem M. El-Bakry, and Nikos Mastorakis, "A Novel Fast Kolmogorov's Spline Complex Network for Pattern Detection" WSEAS Transactions on Systems, Issue 11, vol. 7, November 2008, pp. 1310-1328.

[23] Nikos Mastorakis, "New method for designing 2-D (two-dimensional) IIR Comb filters" WSEAS Trans. Systems, Issue 1, Vol. pp.1-6, 2011