A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security

Osama M. Abu Zaid
Ph. D Researcher in Computer Science, Department of Mathematics, Faculty of Sciences, Zagazig University, Egypt.

Nawal A. El-Fishawy
Head of Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt.

E. M. Nigm
Department of Mathematics , Faculty of Sciences, Zagazig University, Egypt.

Osama S. Faragallah
Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Egypt.

ABSTRACT
In this paper, a proposed encryption scheme based on Henon chaotic system (PESH) is presented in order to meet the requirements of secure image transfer. Scheme based on Henon chaotic system by Chen Wei-bin et al., will be designated here as (SHCH). SHCH and a proposed encryption scheme (PESH) are applied for encrypting by changing the values of the image pixels. Combination of shuffling the positions and changing the values of image pixels is introduced to shuffle the relationship between the cipher-image and the plain-image. First, the Arnold Cat map or Baker chaotic map is used to shuffle the positions of the image pixels. Second, the shuffled-image is encrypted by using SHCH or a proposed (PESH) pixel by pixel. All of these procedures for encrypting are used with four modes of operations ECB, CBC, CFB, and OFB. The results of several experimental, statistical analysis, key sensitivity tests, NPCR and UACI analysis, and time analysis show that, a proposed image encryption scheme (PESH) alone or combined with whatever of confusion algorithms Arnold Cat map or Baker chaotic map, is the best scheme and provides an efficient and secure way for image encryption.

General Terms
Security, Algorithms, Chaotic, Encryption.

Keywords
Arnold Cat map ; Baker chaotic map; Henon chaotic system; Image encryption; and Modes of operations .

1. INTRODUCTION
In recent years, the world living the age of communications revolution which necessitates multimedia transmission in a secure manner. encryption is important in transferring image through the communication networks to protect it against reading, alteration of its content, adding false information, or deleting part of its content.

Owing to frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakages [1]. The requirements to fulfill the security needs of digital images have led to the development of good encryption techniques. Chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power.

The characteristic of the chaotic maps have attracted the attention of cryptographers to develop new encryption algorithms. As these chaotic maps have many fundamental properties such as ergodicity, mixing property and sensitivity to initial condition/system parameter and which can be considered analogous to some cryptographic properties of ideal ciphers such as confusion, diffusion, balance and avalanche property [1].

Henon chaotic map system, which has been described in [2,3] presents a simple two-dimensional map with quadratic nonlinearity. The scheme based on Henon chaotic map system by Chen Wei-bin et al.[4] will be designated in this paper as (SHCH). The proposed encryption scheme will be designated in this paper as (PESH). Both of SHCH and PESH are diffusion algorithms; these algorithms are applied for encryption by changing the values of the image pixels. In this paper the encryption will be done by using SHCH and PESH. Also the encryption will be done by using the combination of SHCH and PESH with confusion algorithms separately.

Two confusion algorithms, which will be used are based on Arnold Cat map [4,5,6,7], and Baker Chaotic map [8] respectively. These confusion algorithms used for Shuffling the Image. The shuffling is changing the positions of pixels of the image without changing the pixels values, such that good shuffling increases the confusion. Both of them is a two-dimensional invertible chaotic map. The Baker map is a chaotic bijection of the unit square $I \times I$ onto itself. The Baker chaotic map system contains generalized Baker map and discretized Baker map.

The well-known modes of operations are the Electronic Code Book (ECB) mode, the Cipher Block Chaining (CBC) mode, the Output Feed Back (OFB) mode, and the Ciphering Feed Back (CFB) mode [9]. All procedures of encryption will be applied with that modes of operations.

This paper is organized as follows. Section 2, will presents the steps of a proposed encryption scheme (PESH). Section 3, will discuss the implementation of the combination for the proposed diffusion algorithm with confusion algorithms. Section 4, and its subsections 4.1, 4.2, and 4.3 will present the experimental results and analysis by implementing statistical analysis factors, time analysis, and security analysis tests. Section 5, will discuss the final conclusion.

2. A PROPOSED ENCRYPTION SCHEME BASED ON HENON CHAOTIC SYSTEM (PESH)

In this section, the proposed encryption scheme based on Henon chaotic system (PESH) is introduced. Figures 1 and 2 illustrate the flow charts for encryption and decryption of the proposed encryption/decryption scheme (PESH). The encryption process of a proposed scheme (PESH) consists of four steps of operations as following:

Step1: The Henon chaotic system is converted into one-dimensional chaotic map. The one dimensional Henon chaotic map is defined as:

$$x_{i+2} = 1 - ax_{i+1}^2 + bx_i \qquad 1$$

Where $a = 0.3$, $b \in [1.07, 1.4]$. The parameter a, the parameter b, initial value x_0, and initial value x_1.

Step2: similar to the step 2 of SHCH, Henon chaotic map is adopted to change the pixels values of the image, but with modification in the technique of creation transform matrix of pixels *(TM)*, by using the quadratic function $\mathbf{f(x_i) = x_i \times (2x_i + 1)}$ with each member will be created of *(TM)*, such that *TM* is one dimension matrix contains number of members equal to $m \times n$ such that m is width of the image by pixel and n is the height of the image by pixel.

Firstly, Henon chaotic map is obtained by formula 1. Then transform matrix *(TM)* of pixel values is created as shown in Fig.1, which illustrates the flow chart for the encryption of a proposed scheme. Fig.2, illustrates the flow chart for the decryption of a proposed scheme.

Note that, the particular choice of this quadratic function transformation $\mathbf{f(x) = x(2x + 1)}$ appears to meet the security goals while taking advantage of simple primitives that are efficiently implemented on most modern processors. Note that $\mathbf{f(x)}$ is one-to-one modulo $\mathbf{2^w}$ (256) [10]. The use of multiplication with addition and mod function greatly increases the diffusion achieved per round.

Step3: Two dimensions matrix *(W)* will be created, which has the same size of the image, m for width and n for height, such that each element of this matrix will be obtained by adding double of the quadrate of the element of the transformation matrix *(TM)* to value of the pixel of original image *(IM)*. Formula 2 will be used to obtain the element *W(i , j)* , such that $i = 1,\ldots,m$, *and* $j = 1,\ldots,n$.

$$W(i,j) = IM(i,j) + 2 \times TM(c) \times TM(c) \qquad 2$$

Such that, $c = 1,2,\ldots,m \times n$. Using this equation which contains addition and two multiplication greatly increases the diffusion achieved per round.

Step4: The cipher-image (*IME*) will be produced by implementing the exclusive OR operation bit-by-bit between the matrix (*W)* values, which created in *step 3* and the values of the image pixels such as in formula 3. The parameters are selected as $a = 0.3$, $b = 1.4$, $x_0 = 0.01$, and $x_1 = 0.02$.

$$IME(i,j) = IM(i,j) \oplus W(i,j) \qquad 3$$

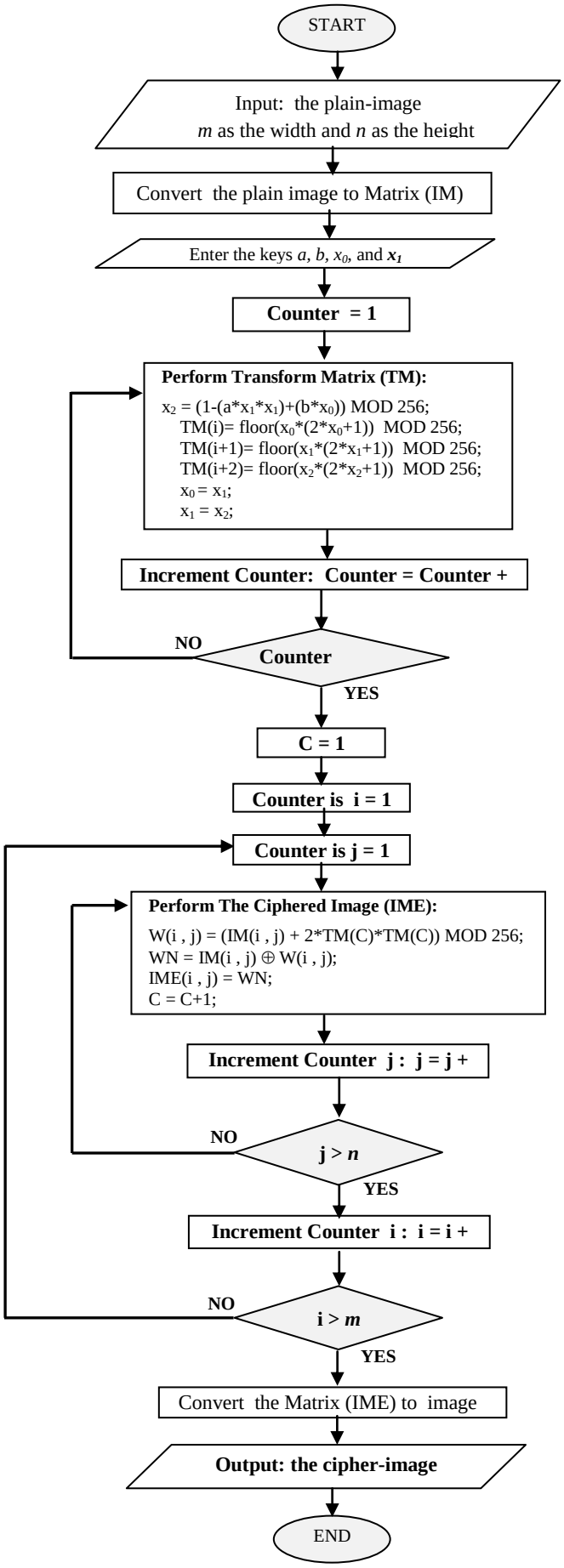


Fig 1: The Flow-Chart for encryption of a proposed scheme (PESH)

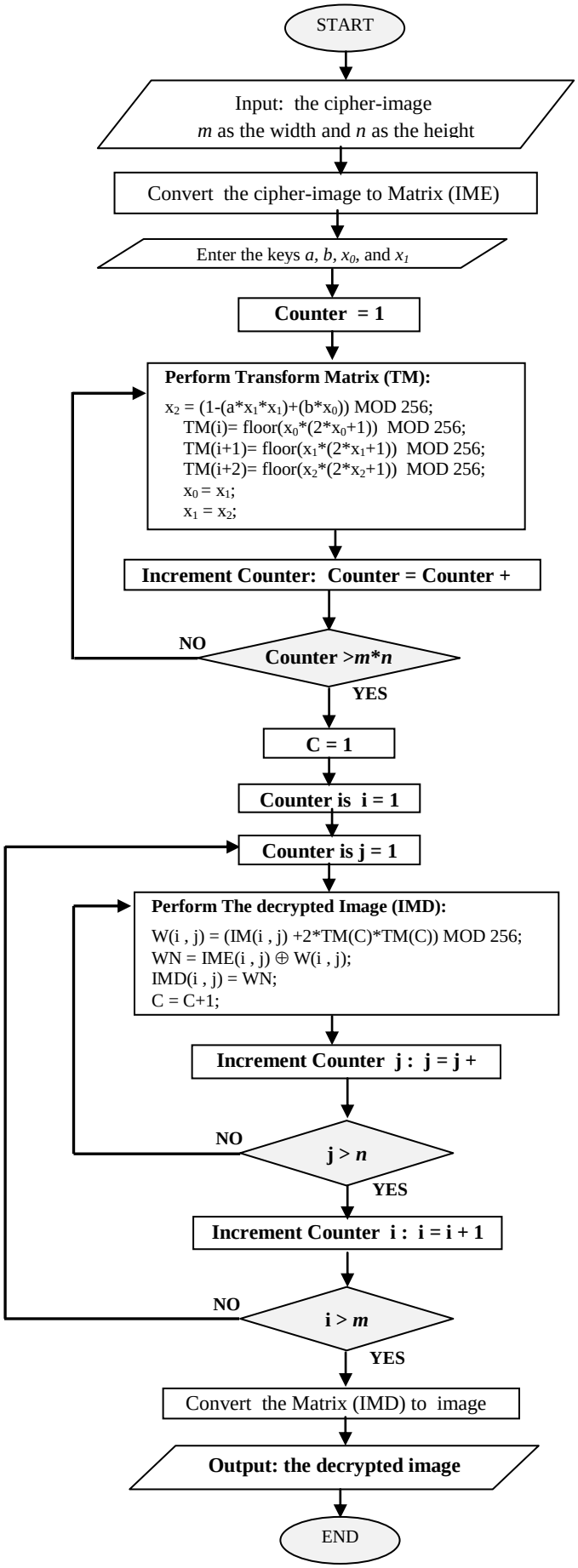


Fig 2: The Flow-Chart for decryption of a proposed scheme (PESH)

3. IMPLEMENTATION OF THE PROPOSED DIFFUSION ALGORITHM WITH CONFUSION ALGORITHMS

The confusion algorithm, which will be used are based on Arnold Cat map or Baker chaotic map. The diffusion algorithms are SHCH and the proposed algorithm (PESH). The confusion algorithms are applied on the image before applying the diffusion algorithms. This procedure achieve shuffling the positions of pixels of the plain-image before changing the values of the pixels. The image, which will be encrypted by the diffusion algorithm is the shuffled-image.

The confusion algorithm, Arnold Cat map or Baker chaotic map has been applied twice, five times, and ten times on the plain-image to produce shuffled-image. The diffusion algorithm, SHCH or PESH has been applied once on the shuffled-image to produce the ciphered-image. This technique has been applied with the four modes of encryption operations ECB, CBC, CFB, and OFB.

Figure 3, is the diagram of encryption/decryption for the combination of the confusion algorithm and the diffusion algorithm to produce good combination algorithm which, produce ciphered image with high quality of encryption.

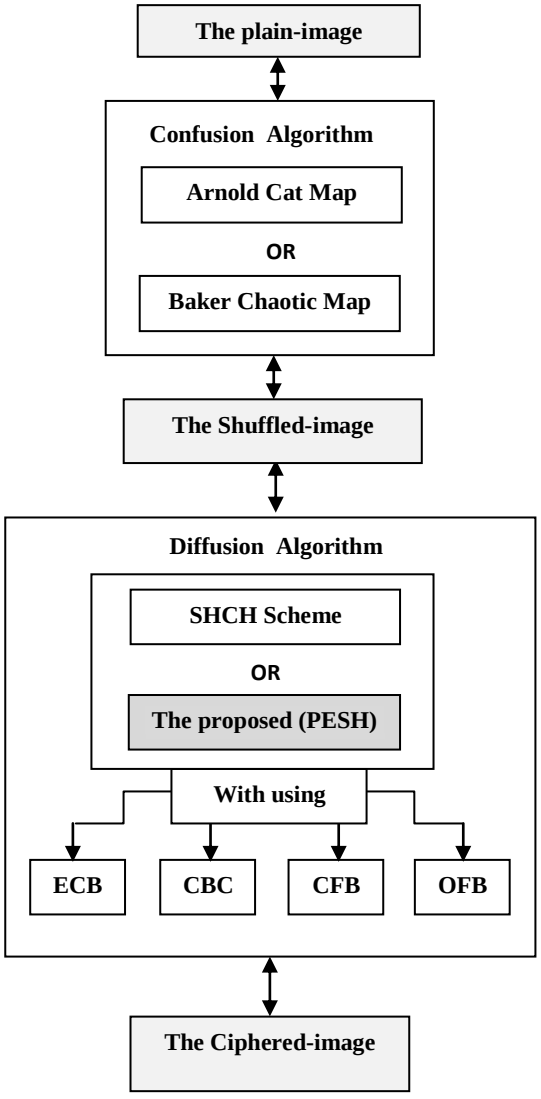


Fig 3: The Diagram for illustration of encryption / decryption for combination technique

4. EXPERIMENTAL RESULTS AND ANALYSIS

In this paper, a practical works programs of Arnold Cat map, Baker Chaotic map, SHCH scheme, a Proposed encryption scheme (PESH), and the combination schemes are designed by MATLAB 7.0 on windows 7 system on Laptop computer with Intel CORE I_3 Processor, 3.0 GB RAM, and 320 GB Hard Disk. All programs have been applied on the image (*boat.bmp*) as plain-image, which is shown in Fig.4(a).

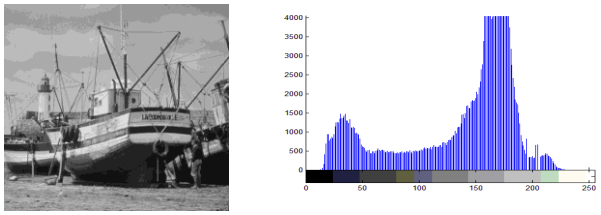
4.1 Statistical Analysis.

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).

4.1.1 Histogram Analysis.

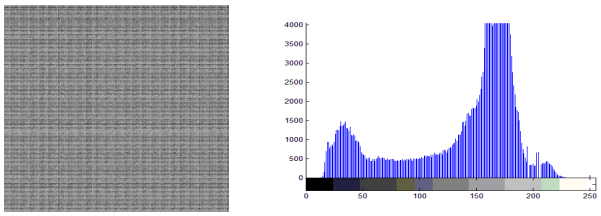
The original image (*boat.bmp*) with the size 512 × 512 pixels is shown in Fig.4(a). and the histogram of the original-image is shown in Fig.4(b). Figure. 5(a) is the shuffled-image by using Arnold Cat map and Fig. 5(b) is the histogram of this shuffled-image, such that the Arnold cat map is chosen as $p = q = 5$ and $R = 10$ times. Figure 6(a) is the shuffled-image by using the Baker Chaotic map and Fig. 6(b) is the histogram of this shuffled-image, such that the ciphering key of the Baker Chaotic map consists of the following sequence of 56 divisors of 512:

(10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14,10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, 10, 5, 12, 5, 10, 8, 14, **)**.



(a) (b)

Fig 4: original-image and its histogram (a) original-image (boat.bmp); (b) histogram of the original-image



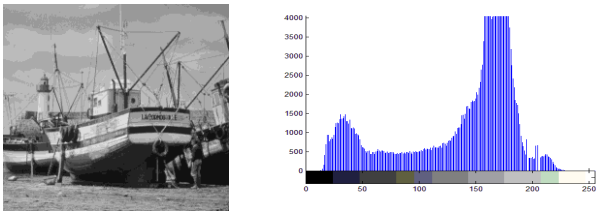
(a) (b)

Fig 5: Encryption by using Arnold Cat Map with 10 times : (a) shuffled-image ; (b) histogram of the shuffled-image.

Figure 5(b), and Fig. 6(b) illustrates the histogram of the shuffled-image by using both of Arnold Cat map and Baker chaotic map are the same as the histogram of the original-image in Fig. 4(b). As can be seen that, both of maps only shuffle the positions of pixels of the original-image.

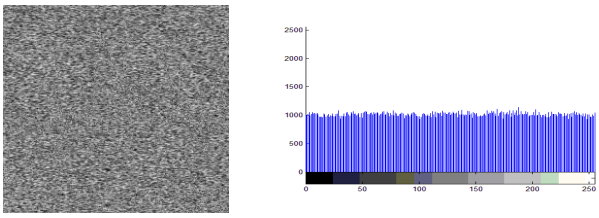
Figure 7(a) illustrates the cipher-image by using SHCH scheme and Fig. 7(b) is the corresponding histogram. The parameters are selected as $a = 0.3$, $b = 1.4$. The secret keys to change the pixel values of the original image are $x_0 = 0.01$, and $x_1 = 0.02$.

Figure 8(a) illustrates the cipher-image by using the proposed (PESH) and Fig. 8(b) is the corresponding histogram. The parameters are selected as $a = 0.3$ and $b = 1.4$. The secret keys to change the pixels values of the original image are $x_0 = 0.01$ and $x_1 = 0.02$. As anyone can see, the histogram of the ciphered image is fairly uniform and is significantly different from that of the original-image. The proposed procedure (PESH) is more complicated and better than SHCH procedure.



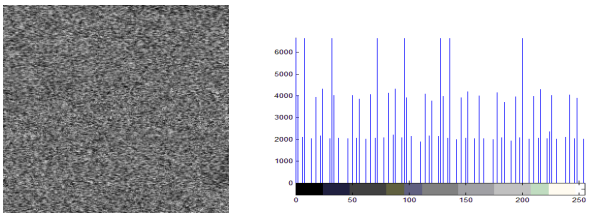
(a) (b)

Fig 6: Encryption by using Baker Chaotic Map with 10 times: (a) shuffled-image ; (b) histogram of the shuffled-image.



(a) (b)

Fig 7: Encryption by SHCH scheme : (a) cipher-image; (b) histogram of the cipher-image.



(a) (b)

Fig 8: Encryption by a proposed scheme (PESH) : (a) cipher-image; (b) histogram of the cipher-image.

Figures 9-12, illustrates the ciphered image, its histogram, and the decrypted image, which are produced by using the combination of Arnold Cat map and SHCH scheme with the four modes of operations ECB, CBC, CFB, and OFB respectively. In general this combination produces convergent histogram with all modes of operations. Figures 13-16, illustrates the ciphered image, its histogram, and the decrypted image, which are produced by using the combination of Arnold

Cat map and the proposed scheme (PESH) with the four modes of operations ECB, CBC, CFB, and OFB respectively. In general this combination produce results of histogram better than the combination of Arnold Cat map and SHCH scheme with the four modes.

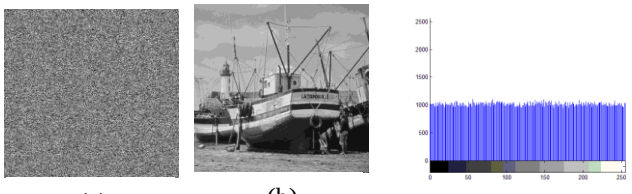
Figures 17-20, illustrates the ciphered image, its histogram, and the decrypted image, which are produced by using the combination of Baker chaotic map and SHCH scheme with the four modes of operations ECB, CBC, CFB, and OFB respectively. In general this combination produces convergent histogram with all modes of operations. Figures 21-24, illustrates the ciphered image, its histogram, and the decrypted image, which are produced by using the combination of Baker chaotic map and the proposed scheme (PESH) with the four modes of operations ECB, CBC, CFB, and OFB respectively. In general this combination produce results of histogram better than the combination of Baker chaotic map and SHCH scheme with the four modes.

(a) (b) (c)

Fig 9: Encryption by combination Arnold cat map (*R=5*) and SHCH with ECB mode : (a) the ciphered- image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 10: Encryption by combination Arnold cat map (*R=5*) and SHCH with CBC mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.



(a) (b) (c)

Fig 11: Encryption by combination Arnold cat map (*R=5*) and SHCH with CFB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 12: Encryption by combination Arnold cat map (*R=5*) and SHCH with OFB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 13: Encryption by combination Arnold cat map (*R=5*) and a proposed (PESH) with ECB mode : (a) the ciphered image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 14: Encryption by combination Arnold cat map (*R=5*) and a proposed (PESH) with CBC mode: (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 15: Encryption by combination Arnold cat map (*R=5*) and a proposed (PESH) with CFB mode: (a) the ciphered image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 16: Encryption by combination Arnold cat map (*R=5*) and a proposed (PESH) with OFB mode: (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp). (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 17: Encryption by combination Baker chaotic map (*R=5*) and SHCH with ECB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 18: Encryption by combination Baker chaotic map (*R=5*) and SHCH with CBC mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 19: Encryption by combination Baker Chaotic map (*R=5*) and SHCH with CFB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 20: Encryption by combination Baker Chaotic map (*R=5*) and SHCH with OFB mode :(a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 21: Encryption by combination Baker Map (*R=5*) and a proposed (PESH) with ECB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 22: Encryption by combination Baker Chaotic map (*R=5*) and PESH with CBC mode: (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 23: Encryption by combination Baker Chaotic map (R=5) and PESH with CFB mode : (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

(a) (b) (c)

Fig 24: Encryption by combination Baker Chaotic map (*R=5*) and PESH with OFB mode: (a) the ciphered-image; (b) decryption which produce the original image (boat.bmp); (c) histogram of the ciphered-image.

4.1.2 Correlation Coefficient analysis.

the correlation coefficient equals one if they are highly dependent , i.e. the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different. So, success of the encryption process means smaller values of the CC. The CC is measured by the following equation [9]:

$$\mathbf{CC} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \qquad 4$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$. x and y are gray-scale pixel values of the original and encrypted images.

4.1.3 Maximum Deviation analysis.

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [9]:

The maximum deviation (MD) is given by the following equation [9]:

$$\mathbf{MD} = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad 5$$

where h_i is the amplitude of the absolute difference curve at value i. Of course, the higher the value of MD, the more the encrypted image is deviated from the original image.

4.1.4 Irregular Deviation analysis.

This analysis is based on how much the deviation caused by encryption (on the encrypted image) is irregular. This method can be summarized in some of steps to obtain irregular deviation (ID)[9]. ID is given by the following equation :

$$\mathbf{ID} = \sum_{i=0}^{255} \left| H(i) - \frac{1}{256}\sum_{i=0}^{255} h_i \right| \qquad 6$$

H = histogram(D). and D can be represented as $D = | I - J |$, where I is the original image, and J is the encrypted image. h_i is the amplitude of the absolute difference histogram at the value i. The lower the ID value, the better the encryption algorithm.

In this paper, the previous three factors **CC**, **MD**, and **ID** are evaluated for encrypted images, which produced from encrypting the original image (*boat.bmp*) by using SHCH, the proposed (PESH), the combination procedure of Arnold Cat map with both of SHCH and PESH, and the combination procedure of Baker Chaotic map with both of SHCH and PESH.

The results of CC, MD, and ID are recorded in Tables 1-6, such that the three factors have been applied for all procedures with four modes of operations ECB, CBC, CFB, and OFB.

From Tables 1 and 2, the results illustrate that the proposed scheme (PESH) is better than SHCH scheme with all modes of operations. The proposed scheme gives better results with modes ECB, and CBC than CFB and OFB, such that OFB is the worst mode.

Table 1. Results of CC, MD, and ID factors for SHCH with the modes of operations

Modes	Results of CC , MD, and ID for SHCH.		
	CC	MD	ID
ECB	0.0016	224260	244874
CBC	-0.000648	226392	243730
CFB	-0.000648	226392	243730
OFB	-0.0031	225610	244170

Table 2. Results of CC, MD, and ID factors for a proposed (PESH) with the modes of operations.

Modes	Results of CC , MD, and ID for PESH.		
	CC	MD	ID
ECB	-0.0037	410620	217594
CBC	-0.0026	410520	215260
CFB	-0.0011	325340	243022
OFB	-0.0013	225750	243886

From Tables 3-6 in general, the results illustrates the combination of a proposed scheme (PESH) with both of Arnold and Baker is better than the combination of SHCH with both of Arnold and Baker with all modes of operations. The combination of the proposed (PESH) with both of Arnold and Baker gives better results with modes ECB, and CBC than CFB and OFB, such that the results with OFB mode is the worst.

From Tables 3-6 the results of the combination of the proposed (PESH) with Baker chaotic map is better than the results of the combination of the proposed (PESH) with Arnold Cat map with ECB and CBC modes, but with CFB and OFB the procedures are convergent.

Table 3. Results of CC, MD, and ID factors for combination of SHCH scheme with Arnold Cat map, with the modes of operations.

Modes	Arnold *R*	Results for combination of SHCH with Arnold Cat map		
		CC	MD	ID
ECB	**2**	-0.0012	225395	243784
	5	0.0019	225620	244556
	10	-0.0031	224490	244150
CBC	**2**	-0.0015	225182	243716
	5	0.000363	224982	244064
	10	-0.000856	225236	243542
CFB	**2**	-0.0015	225182	243716
	5	0.000363	224982	244064
	10	-0.000856	225236	243542
OFB	**2**	0.0042	225300	244230
	5	-0.0012	225727	244080
	10	0.0050	225170	244240

Table 4. Results of CC, MD, and ID factors for combination of PESH with Arnold Cat map, with the modes of operations.

Modes	Arnold *R*	Results for combination of PESH with Arnold Cat map.		
		CC	MD	ID
ECB	2	-0.0060	411060	209784
	5	-0.0046	410480	209878
	10	-0.0037	410570	209862
CBC	2	-0.0040	411310	215324
	5	-0.0038	410860	215484
	10	-0.0044	410780	214426
CFB	2	-0.000084	325540	242766
	5	-0.0026	325970	242308
	10	-0.0012	325370	243494
OFB	2	-0.000501	225652	243554
	5	-0.000959	225680	243792
	10	0.0016	226060	243812

Table 5. Results of CC, MD, and ID factors for combination of SHCH scheme with Baker map, with the modes of operations.

Modes	Arnold *R*	Results for combination of SHCH with Baker Chaotic map.		
		CC	MD	ID
ECB	2	-0.000955	225370	243854
	5	-0.0024	224650	244410
	10	-0.0016	224250	244876
CBC	2	0.0039	225450	244194
	5	-0.0015	224780	244094
	10	0.0011	225780	244208
CFB	2	0.0039	225450	244194
	5	-0.0015	224780	244094
	10	0.0011	225780	244208
OFB	2	-0.0017	225580	243826
	5	0.0031	225760	244674
	10	0.0018	225530	244310

Table 6. Results of CC, MD, and ID factors for combination of PESH with Baker map, with the modes of operations

Modes	Arnold *R*	Results for combination of PESH with Baker Chaotic map.		
		CC	MD	ID
ECB	2	-0.0044	411480	209526
	5	-0.0030	410680	209136
	10	-0.0039	411050	209442
CBC	2	-0.0034	410910	214404
	5	-0.0015	410770	214292
	10	-0.0059	411220	214708
CFB	2	-0.0024	325200	243410
	5	0.000439	325579	242790
	10	-0.0043	325750	243442
OFB	2	-0.0011	225610	243932
	5	0.0030	225840	243742
	10	0.0015	225830	243636

4.2 Time Analysis.

In this analysis, execution time of SHCH procedure, the proposed (PESH), and all procedures of the combinations has been estimated by seconds for encrypting the image (*boat.bmp*), which is (512 × 512) pixels and 257 Kilo Bytes. The time is measured for all procedures with the four modes of operations ECB, CBC, CFB, and OFB. The time is measured For procedures of the combinations with the rounds *R* equal 2, 5, and 10 for both Arnold Cat map and Baker Chaotic map.

Table 7. illustrates time by (Sec.) for encryption *boat.bmp* by using SHCH scheme and by using the proposed scheme (PESH). Table 8. illustrates time by (Sec.) for encryption *boat.bmp* by using a combination of Arnold Cat map with SHCH, such that Arnold with *R* equal 2, 5, and 10 times. Table 9. illustrate Time by (Sec.) for encryption *boat.bmp* by using a combination of Arnold Cat map with the proposed (PESH), such that Arnold with *R* equal 2, 5, and 10 times. Table 10. illustrates time by (Sec.) for encryption *boat.bmp* by using a combination of Baker Chaotic map with SHCH, such that Baker with *R* equal 2, 5, and 10 times.

Table 7. Time by (Sec.) for encryption boat.bmp using SHCH and PESH.

Time by (Sec.) for using SHCH with all modes of operations.			
ECB	CBC	CFB	OFB
0.6090	0.9360	0.9360	0.9200
Time by (Sec.) for A proposed (PESH) with all modes of operations. .			
ECB	CBC	CFB	OFB
0.6240	0.9360	0.9390	0.9520

Table 8. Time by (Sec.) for encryption boat.bmp using combination of SHCH with Arnold cat map.

Arnold *R*	Time by (Sec.) for using combination of SHCH with Arnold cat map.			
	ECB	CBC	CFB	OFB
2	1.0770	1.3570	1.2640	1.2330
5	1.6380	1.8410	1.8100	1.9820
10	2.3710	2.6200	2.9640	2.4810

Table 9. Time by (Sec.) for encryption boat.bmp using combination of PESH with Arnold cat map.

Arnold *R*	Time by (Sec.) for using combination of a proposed (PESH) with Arnold cat map.			
	ECB	CBC	CFB	OFB
2	1.1230	1.8720	1.4040	1.4200
5	1.5910	1.9810	1.8400	1.8560
10	2.3710	2.6210	2.6370	2.7140

Table 10. Time by (Sec.) for encryption boat.bmp using combination of SHCH with Baker Chaotic map.

Baker *R*	Time by (Sec.) for using combination of SHCH with Baker chaotic map.			
	ECB	CBC	CFB	OFB
2	1.7160	1.9190	1.9180	1.9040
5	2.4960	2.8240	2.6990	2.7150
10	3.7440	3.9310	3.9000	3.8540

Table 11. Time by (Sec.) for encryption boat.bmp using combination of PESH with Baker map.

Baker *R*	Time by (Sec.) for using combination of PESH with Baker chaotic map.			
	ECB	CBC	CFB	OFB
2	1.7790	1.9970	1.9970	1.9660
5	2.5110	2.7460	2.7150	2.8390
10	3.6820	4.0560	3.9940	3.9620

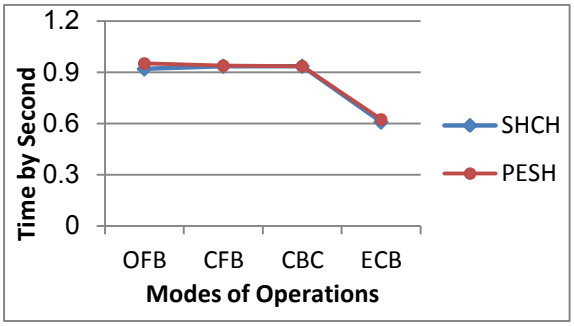


Fig 25: The time by (Sec.) of encryption boat.bmp by using SHCH and the proposed (PESH) with the four modes of operations.

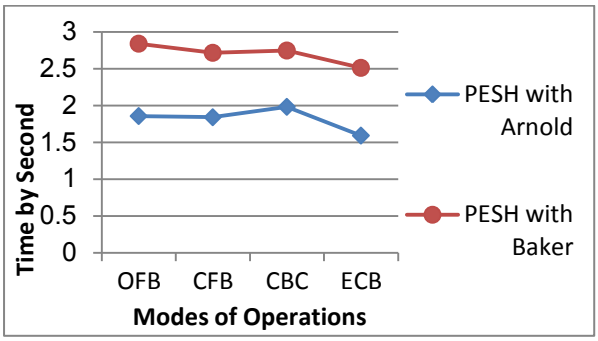


Fig 26: The time by (Sec.) of encryption boat.bmp by using the proposed (PESH) with Arnold cat map and Baker map at R=5

With precisely looking to Tables 7-11, and Fig. 25, in general, the execution time of a proposed (PESH) sometimes equal to, nearest to, or less than the execution time of SHCH, i.e. the proposed (PESH) implemented upward with the same execution time of SHCH but with good quality of encryption compared to SHCH procedure. Also by looking to Tables 9 and 11, and Fig. 26, the combination of the proposed (PESH) with Arnold Cat map has execution time less than execution time of the combination of the proposed (PESH) with Baker Chaotic map.

4.3 Security Analysis.

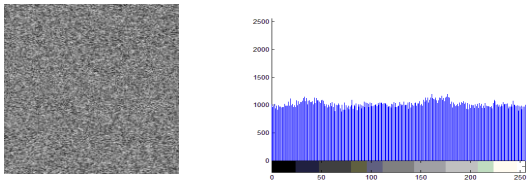
A good encryption scheme should resist most kinds of known attacks, it should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. In proposed scheme (PESH), the parameters a and b , the initial values x_0 and x_1, and extra parameter k are used as secret keys. The key space is large enough to resist all kinds of brute-force attacks. Number of Pixels Change Rate (*NPCR*), and Unified Average Changing Intensity (*UACI*) are measured for all of encrypted images by using all procedures.

4.3.1 Key Sensitivity Analysis.

The experimental results also demonstrate that scheme (PESH) is very sensitive to the secret key mismatch. Figures 13(b) and 21(b) illustrates the decrypted image by using a proposed procedure (PESH) such that, it is the same of original image which, its histogram has been illustrated in Fig. 4(b).

Figure 8(a) illustrates the cipher-image, which is decrypted by using the proposed scheme (PESH) with $a = 0.3$, $b = 1.4$, $x_0 = 0.01$, *and* $x_1 = 0.02$ to produce the original image.

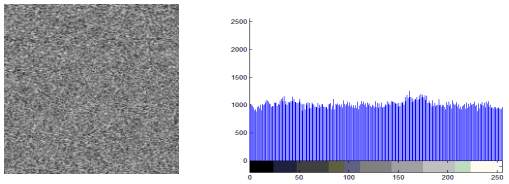
Figures 27–30 illustrates the sensitivity of the proposed scheme with the secret keys a, b, x_0, *and* x_1 respectively. The experimental results also demonstrate that the proposed scheme (PESH) is very sensitive to the secret keys a mismatch (10^{-16}), b mismatch (10^{-16}), x_0 mismatch (10^{-15}), and x_1 mismatch (10^{-14}).



(a) (b)

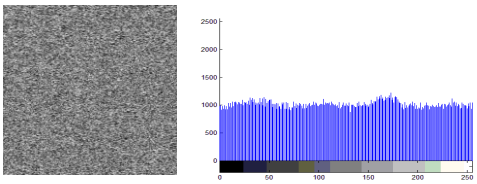
Fig 27: The sensitivity to the secret key a of the proposed (PESH): (a) decrypted image (at a = 0.30000000000000001,b=1.4, x_0=0.01, x_1=0.02); (b) histogram of the decrypted image.

Figure 27 illustrates the sensitivity of the proposed scheme with the secret key a, such that the cipher-image is shown in Fig. 8(a) decrypted using a = 0.3000000000000001, and the remains secret keys as the same as in the normal case. As can be seen that, even the secret key a is changed a little (10^{-16}), the decrypted image is absolutely different from the original image.



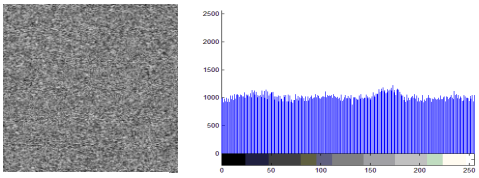
(a) (b)

Fig 28: The sensitivity to the secret key b of the proposed (PESH): (a) decrypted image (at a=0.3, b=1.4000000000000001, x_0=0.01, x_1=0.02); (b) histogram of the decrypted image.



(a) (b)

Fig 29: The sensitivity to the secret key x_0 of the proposed (PESH): (a) decrypted image (at a=0.3, b=1.4, x_0=0.010000000000001, x_1=0.02); (b) histogram of the decrypted image.



(a) (b)

Fig 30: The sensitivity to the secret key x_1 of the proposed (PESH): (a) decrypted image (at a=0.3, b=1.4, x_0=0.01, x_1=0.02000000000001); (b) histogram of the decrypted image.

Similar results for other secret keys all can be obtained, which are shown in Figs. 28-30, using b=1.4000000000000001, such that b is changed a little (10^{-16}), using x_0 = 0.010000000000001, such that x_0 is changed a little (10^{-15}), and using x_1 = 0.02000000000001, such that x_1 is changed a little (10^{-14}). As anyone can see, the decrypted image with wrong keys has a histogram with random behavior. The sensitivity to initial values which is the main characterization of chaos guarantees the security of the proposed scheme (PESH).

4.3.2 NPCR and UACI Analysis.

To evaluate the variations between the original image and the decrypted images, there are two additional tests: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity). NPCR and UACI are performed as follows [11]:

$$\mathbf{NPCR} = \frac{\sum_{i,j} \boldsymbol{D(i,j)}}{\boldsymbol{M \times N}} \times 100\% \qquad 7$$

$$\text{Where } \boldsymbol{D(i,j)} = \begin{cases} \mathbf{0}, & A(i,j) = AH(i,j) \\ \mathbf{1}, & A(i,j) \neq AH(i,j) \end{cases}$$

$$\mathbf{UACI} = \frac{\mathbf{1}}{\boldsymbol{M \times N}} \sum_{i,j} \frac{|\boldsymbol{A(i,j) - AH(i,j)}|}{\mathbf{255}} \times 100\% \qquad 8$$

A and AH are the matrices of the original image and encrypted image respectively. M is the height by pixels of the images and N is the width by pixels of the images. As shown in Tables 12-16, a proposed scheme (PESH) has great performances in NPCR and UACI tests. The two tests are estimated for SHCH scheme, a proposed (PESH), and all procedures of the combinations of the confusion algorithms and the diffusion algorithms with the four modes of operations ECB, CBC, CFB, and OFB.

From Table 12, and Figs. 31 and 32, a proposed encryption scheme (PESH) is better than SHCH scheme for *NPCR* and *UACI* tests with all modes of operations. For SHCH scheme, the results of tests with CBC, CFB, and OFB are convergent and better than SHCH scheme with ECB. For a proposed scheme (PESH), the results of tests with ECB and CBC are convergent and better than the results of a proposed scheme (PESH) with CFB and OFB.

Table 12. Results of NPCR and UACI tests for SHCH scheme, and A proposed Scheme (PESH).

	Results for SHCH scheme.			
Modes	**ECB**	**CBC**	**CFB**	**OFB**
NPCR %	99.580	99.611	99.611	99.587
UACI %	29.241	29.417	29.417	29.418
	Results for A proposed Scheme (PESH).			
Modes	**ECB**	**CBC**	**CFB**	**OFB**
NPCR %	99.711	99.685	99.623	99.616
UACI %	30.894	31.093	29.420	29.452

Table 13. Results of NPCR and UACI tests for combination of Arnold Cat Map with SHCH scheme.

Arnold *R*	**Results for combination of Arnold cat map with SHCH scheme.**				
		ECB	**CBC**	**CFB**	**OFB**
2	**NPCR%**	99.614	99.618	99.618	99.600
	UACI%	29.381	29.403	29.403	29.368
5	**NPCR%**	99.591	99.593	99.593	99.604
	UACI%	29.316	29.362	29.362	29.440
10	**NPCR%**	99.606	99.623	99.623	99.614
	UACI%	29.418	29.395	29.395	29.293

Table 14. Results of NPCR and UACI tests for combination of Arnold Cat Map with PESH.

Arnold *R*	**Results for combination of Arnold cat map with a proposed scheme (PESH).**				
		ECB	**CBC**	**CFB**	**OFB**
2	**NPCR%**	99.682	99.681	99.618	99.616
	UACI%	30.729	31.087	29.418	29.375
5	**NPCR%**	99.699	99.680	99.593	99.608
	UACI%	30.692	31.084	29.437	29.354
10	**NPCR%**	99.685	99.685	99.639	99.604
	UACI%	30.683	31.109	29.422	29.365

Table 15. Results of NPCR and UACI tests for combination of Baker Chaotic Map with SHCH .

Baker *R*	**Results for combination of Baker Chaotic map with SHCH scheme.**				
		ECB	**CBC**	**CFB**	**OFB**
2	**NPCR%**	99.637	99.618	99.618	99.602
	UACI%	29.373	29.363	29.363	29.433
5	**NPCR%**	99.590	99.594	99.594	99.603
	UACI%	29.359	29.404	29.404	29.346
10	**NPCR%**	99.638	99.632	99.632	99.591
	UACI%	29.329	29.402	29.402	29.343

Table 16. Results of NPCR and UACI tests for combination of Baker Chaotic Map with PESH.

Baker *R*	Results for combination of Baker Chaotic map with a proposed scheme (PESH).				
		ECB	CBC	CFB	OFB
2	NPCR%	99.691	99.698	99.606	99.614
	UACI%	30.713	31.079	29.440	29.410
5	NPCR%	99.677	99.670	99.619	99.620
	UACI%	30.664	31.039	29.415	29.352
10	NPCR%	99.687	99.689	99.617	99.604
	UACI%	30.677	31.132	29.449	29.348

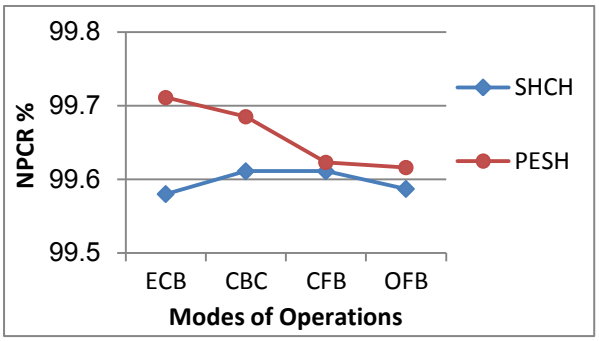


Fig 31: NPCR % of encryption boat.bmp by using SHCH and a proposed scheme (PESH) with the four modes.

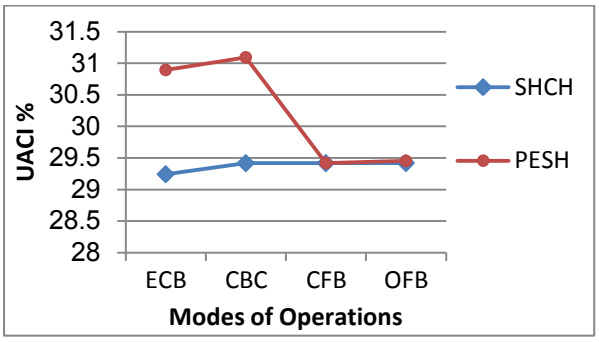


Fig 32: UACI % of encryption boat.bmp by using SHCH and a proposed scheme (PESH) with the four modes.

From Tables 13-16, results of tests for the combination procedures of the proposed (PESH) with both of the two shuffling algorithms is better than the combination procedures of SHCH scheme with both of the two shuffling algorithms for all modes of operations. The results for a proposed scheme (PESH) with Arnold with some of modes are sometimes better than results for a proposed (PESH) with Baker, and the reversal is true sometimes. But all the results for both of them are very convergent. In general, the *NPCR* and *UACI* of the proposed scheme (PESH) being all close to unity are evident that the encryption image has a highly confidential security.

5. CONCLUSIONS

In this paper, a proposed encryption scheme based on Henon chaotic system (PESH) is presented. The proposed is the diffusion scheme for encrypting the images by changing the pixels values of the image. Also, the combination schemes of the proposed (PESH) with both of the confusion schemes, Arnold Cat map and Baker chaotic map are presented. All of these procedures for encryption are used with the four modes of operations ECB, CBC, CFB, and OFB. The experimental results and analysis show that the proposed cryptosystem (PESH) is the best and has high security compared to SHCH scheme such that, the proposed scheme (PESH) has merits: 1) it has a large enough key space to resist most kinds of brute force attacks. 2) it is very sensitive to all members of the secret keys. 3) its results with all tests of statistical analysis are better than the results of SHCH scheme for the same tests. 4) its results of NPCR and UACI tests are better than the results of SHCH scheme for the same tests. 5) it is implemented upward with the same execution time of SHCH scheme, but the proposed (PESH) with high encryption quality. As demonstrated in the simulation, the proposed scheme (PESH) is suitable to provides an efficient and secure way for image encryption.

6. REFERENCES

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

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

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

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

[5] Z.-H. Guan, F. Huang, W. Guan. Aug. 2005. Chaos-based image encryption algorithm. Physics Letters A 346, pp. 153–157.

[6] Zhenwei Shang, Honge Ren, Jian Zhang. 2008. A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation. the 9th International Conference for Young Computer Scientists, 978-0-7695-3398-8/08/$25.00 © IEEE.

[7] Zhu Liehuang, Li Wenzhuo, Liao Lejian, Li Hong. 2006. A Novel Algorithm for Scrambling Digital Image Based on Cat Chaotic Mapping. Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), 0-7695-2745-0/06 $20.00 © IEEE.

[8] Jiri Fridrich. 1998. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. International Journal of Bifurcation and Chaos, Vol. 8, No. 6 , 1259-1284.

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

[10] Ronald L. Rivest, M.J.B. Robshaw, R.Sidney, and Y.L. Yin. August 20, 1998. The RC6™ Block Cipher. M.I.T. Laboratory forComputer Science, 545 Technology Square, Cambridge, MA 02139, USA,v1.1.

[11] H. H. Nien, S. K. Changchien, S. Y. Wu, and C. K. Huang. 2008. A New Pixel- Chaotic- Shuffle Method for Image Encryption. ICARCV, Hanoi, Vietnam, December 2008, and 978-1-4244-2287-6/08 © IEEE.