A CHAOTIC CONFUSION-DIFFUSION IMAGE ENCRYPTION BASED ON HENON MAP

Ashraf Afifi

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

ABSTRACT

This paper suggests chaotic confusion-diffusion image encryption based on the Henon map. The proposed chaotic confusion-diffusion image encryption utilizes image confusion and pixel diffusion in two levels. In the first level, the plainimage is scrambled by a modified Henon map for n rounds. In the second level, the scrambled image is diffused using Henon chaotic map. Comparison between the logistic map and modified Henon map is established to investigate the effectiveness of the suggested chaotic confusion-diffusion image encryption scheme. Experimental results showed that the suggested chaotic confusion-diffusion image encryption scheme can successfully encrypt/decrypt images using the same secret keys. Simulation results confirmed that the ciphered images have good entropy information and low correlation between coefficients. Besides the distribution of the gray values in the ciphered image has random-like behavior.

.

KEYWORDS

Chaos, Encryptions, Henon map, Shuffle, Confusion, Diffusion.

1. INTRODUCTION

This document describes and is written to conform to, author guidelines for the journals of AIRCC series. The rapid development of digital technology and network communications during the past decade has made a great change in people's work and life. Images have special features is used how the bulk data capacity and the high level of data redundancy. These features make image encryption harder than texts. To overcome this limitation, several methods of image encryption have been suggested to secure the digital image contents. The chaotic systems properties have been reported to be suitable for images ciphering. The main properties are the sensitivity to initial conditions, the ergodicity and mixing and the determinism [1-9]. Therefore, the secure transmission of confidential and sensitive information on networks has become a major research problem.

Image chaotic ciphering in previous works relied on either image confusion or diffusion process. Confusion image is generated by permuting positions of pixels. The confusion functions are mainly the Standard map [10], the Arnold cat map [2], the Baker map [11], and the logistic map. Diffusion is the process of changing pixels gray values of the image. The main diffusion functions are Chen's map, logistic map, and the Henon map.

In [2], Peterson ciphered "cat image" by scrambling it based on Arnold cat map. However, after iterating enough times the ciphering algorithm, the plain image reappeared. So, we concluded that image ciphering by confusing or diffusing alone is not enough to resist to an eventual attack. In Gao et al.'s image cryptosystem [3], the plain image pixels are masked by a pseudo-random chaotic sequence generated by power and tangent function. In Kwok scheme [4], the keystream for masking is obtained by the cascading of the skewed Tent map and a high-dimensional Cat map. Nien at [5] suggested encrypting the RGB components of a digital color image separately

using three variables of a third-order RLC chaotic circuit. Pareek at [6] used an external key and a logistic map output to select one of the eight possible operations is selected to encrypt image pixel.

In [7], Fridrich reported that chaos-based image encryption includes two iterative stages namely chaotic confusion and pixel diffusion. Zhang at [12] used a discrete exponential chaotic map for pixel permutation and simple XOR logic function for diffusion.

Our paper suggests a Henon map based confusion-diffusion, then compares it with the logistic map, and then uses the suggested modified Henon map for confusion-diffusion mechanism in the suggested chaotic image encryption system.

The rest of the paper is structured as follows: The Henon map based confusion and diffusion is explored in Section 2. Section 3 introduces the suggested image encryption technique with confusion and diffusion. The test results discussions are presented in section 4. Finally, section 5 concludes this work.

2. FUNDAMENTALS KNOWLEDGE

2.1. Henon Chaotic System

A Henon chaotic system is a 2-D dynamic system as suggested in [13] to simplify the Lorenz map [14] defined by properties of eq.1 .

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

The initial parameters are a, b and the initial point is. (x_0, y_0) Each point (x_n, y_n) is mapped to a new point (x_{i+1}, y_{i+1}) through the Henon map. For a=0.3 and b=1.4 as suggested in [15].

The parameter a, the parameter b, initial value x_0 and the initial value x_1 may represent the key and make it is hard to predict the secret information.

2.1.1. Pixel Permutation

In the permutation level, the new location of each bit is computed by eq.2. The pair of (x', y') is the new position of (x, y). At this phase, the n x n input image is permuted r times with different parameters P and Q, where $i = 1,.....r$.

Let's consider

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & P_i \\ Q_i & P_iQ_i + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod n \tag{2}$$

By setting P and Q as:

$P_i = 1 - 0.3P_i^2 + Q_i$

$Q_i = 1.4P_i$

$P_0 = 1.2, Q_0 = 0.36), i = 0,1,2,.....$.

2.1.2. Pixel diffusion

In the diffusion phase, each pixel diffusion is calculated by eq. 3. The pair of $(x(i+1), y(i+1))$ is the new value of (x', y'). At this phase, the scrambled image is diffused by n iterations based on the image size.

$$\begin{bmatrix} x(i+1) \\ y(i+1 \end{bmatrix} = \begin{bmatrix} 1 - 0.3x^2(i) + y(i) \\ 1.4x(i) \end{bmatrix}, \quad (3)$$

$i = 0,1,2,..... .....$

2.2. The Chaotic 2-D Logistic Map

The chaotic 2-D logistic map [16] is another ciphering scheme. The definition of the 2-D logistic map $F(x, y)$ can be described by the following eq. 4.

$$F(x,y) = \begin{Bmatrix} x_{i+1} = \alpha_1 x_i (1 - x_i) + \beta_1 N_i^2 \\ \\ y_{i+1} = \alpha_2 y_i (1 - y_i) + \beta_2 (x_i^2 + x_i y_i) \end{Bmatrix} \quad (4)$$

Where $\alpha_1, \beta_1, \alpha_2, \beta_2$ are the control system parameters, and i varies as 0, 1, 2… and so on, x_0 and y_0 are initial conditions values. For $2.75 \le \alpha_1 \le 3.4$, $0.15 \le \beta_1 \le 0.21$, $2.7 \le \alpha_2 \le 3.45$, $0.13 \le \beta_1 \le 0.15$ and $0 < a_i, b_i \le 1$.

3. THE PROPOSED IMAGE ENCRYPTION TECHNIQUE

In the suggested modified Henon map will be defined in terms of two basic processes namely ciphering and deciphering. As shown in Fig.1, it has two stages for ciphering /deciphering, respectively. The ciphering stage starts by reading the plain image. Then, fed to the chaotic Henon map confusion and apply the chaotic Henon map diffusion ciphering is applied according to eq. 3 and eq. 4.

The ciphering steps can be summarized as follows:

- Read the plainimage.
- Apply a chaotic Henon map confusion on the plainimage.
- Apply a chaotic Henon map diffusion on the previously confused plainimage.

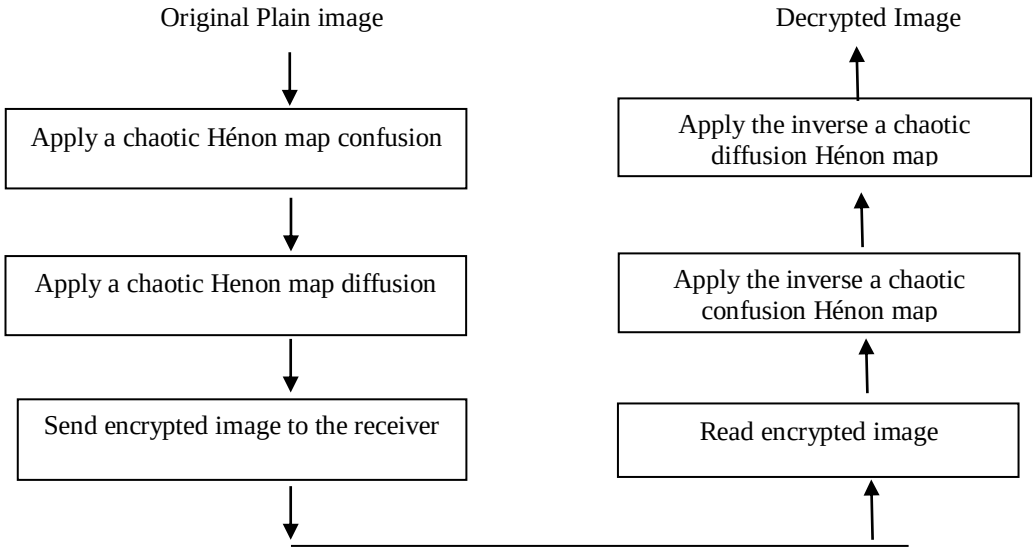


Figure 1: The Proposed Image Encryption

The receiver starts by applying the deciphering stage in the same steps but reverse order used in the ciphering stage.

The steps of deciphering stage are summarized as follows:

- Read the cipher image.
- Apply the inverse of the chaotic diffusion Henon map on the ciphered image.
- Apply the inverse of the chaotic confusion Henon map on the resulted image produced in step 2 to obtain the find decrypted image.

4. SIMULATION RESULTS

In this section, some security analysis results on the suggested ciphering technique are described, including some important tests like statistical and differential analysis [17-20] and comparing its performance with a chaotic 2-D logistic map ciphering. The three images of the Bata, Girl, and peppers of 256x256-sized are shown in Fig.2 have been used in the tests.

a) Bata b) Girl c) Peppers

Figure 2: Test Images - Bata, Girl and Peppers Images

The encryption outcomes of plainimages employing the proposed chaotic Henon map encryption technique and conventional 2-D logistic map are illustrated in Fig. 3 for Bata, Girl and Peppers images, respectively. It is obvious that the encryption with the proposed chaotic Henon map outperforms in the concealment of all images details.

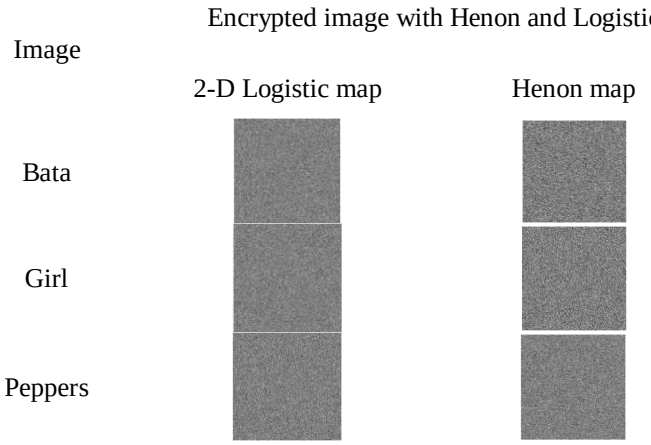


Figure 3: Encrypted images using proposed a chaotic Henon map and 2-D Logistic map.

4.1. Abstract Correlation Analysis

The Abstract section begins with the word, The correlation rxy is calculated as [15-16, 21]:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2, \tag{6}$$

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)), \tag{7}$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{8}$$

where ; x and y are gray values of pixels of the two images x, y.

After measuring the correlation between the plainimage and encrypted image, if it does not equals 1, the plainimage and its encrypted image are the same, if it equals 0, the encrypted image is completely different from the original and if it equals -1, the encrypted image is the negative of the plainimage.

4.2. Entropy Analysis

Shannon entropy calculates the information involved within the image. It is calculated in bits. It can be calculated as [16]:

$$H(m) = \sum_{i=0}^{2^N - 1} P(m_i) \log_2 \frac{1}{P(m_i)} \; bits \tag{9}$$

Where ; mi is a symbol and 2N-1 is the occurrence number of mi in the image. Consequently, large entropy value indicates good encryption.

4.3. The Histogram Analysis

The histogram deviation (HD) asses the encryption quality by examining how it enlarges between the difference between the plain and the encrypted images according to [22]. The D_H can be estimated as follows:

$$D_H = \frac{\left(\frac{d(0)+d(255)}{2} + \sum_{i=1}^{254} d(i) \right)}{W \times H} \tag{10}$$

Where d(i) is the absolute value of the difference between the histograms of the plain image and encrypted images at pixel level i. the variables W and H are the dimensions of the image. The objective is to obtain as high D_H as possible.

The irregular deviation (D_I) asses the encryption accuracy in terms of how much the irregularity is the deviation caused by encryption. The irregular deviation D_I is calculated as [22]:

$$D_I = \frac{\sum_{i=0}^{255} h_D(i)}{W \times H} \tag{11}$$

$$h_D(i) = \left| h(i) - M_H \right| \tag{12}$$

where $h(i)$ is the histogram of the encrypted image at level i, and MH is the uniform histogram mean value for an ideal encrypted image. Therefore, achieving low values for D_I means high encryption quality.

4.4. Unified Average Changing Intensity (UACI)

The UACI asses the mean intensity of the difference among the plain image C1 and the encrypted image C2 according to [16, 21]. UACI can be calculated as follows:

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%, \tag{13}$$

To obtain more security, the output of such encrypted image outperforms symbols with UACI near to 33%.

4.5. The NPCR Measure

The NPCR asses the percentage of dissimilar pixels number to the entire pixels number among the two encrypted images $E_1(x_i, y_j) and E_2(x_i, y_j)$. When a single pixel changes.

The $D(x_i, y_j)$ is calculated by $E_1(x_i, y_j) and E_2(x_i, y_j)$ as follows:

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

According to [16,21] [21], the NPCR can be calculated as follows:

$$NPCR(E_1,E_2)=\frac{\sum_{i,j} D(x_i,y_j)}{WxH}x100\% \quad (14)$$

achieving greater NPCR value**,** the algorithm is more secure.

we will compare the chaotic 2-Logistic map to the suggested a chaotic Henon map numerically. Table 1 shows entropy, corr., HI, HD, NPCR , and UACI of the three images compared with their ciphered ones when being ciphered with a chaotic 2-D Logistic map and the suggested a chaotic Henon map.

Table 1: The quality matrices results of the estimated correlation, entropy, HD, HI, NCPR, and UACI for encrypted images using a chaotic 2-D Logistic map and by the suggested a chaotic Henon map

Image	Bata		Girl		Peppers	
	Logistic	Henon	Logistic	Henon	Logistic	Henon
Entropy	7.9993	7.9999	7.9929	7.9990	7.9990	7.9993
Corr.	0.00061	0.00113	0.0182	0.00034	0.000764	0.0018
HI	0.4616	0.4703	0.5709	0.5750	0.6349	0.6388
HD	0.8677	1.4986	0.8399	1.4838	0.5528	1.4999
NCPR	% 99.9634	% 99.6125	% 97.9763	% 99.5754	% 99.6082	% 99.5964
UACI	%29.82	%33.21	%32.58	%31.94	%29.63	%29.56

From this table, The entropy in the suggested a chaotic Henon map is greater than the chaotic 2-D Logistic map in “Bata”,” Girl” and in ”Peppers” images and it is near 8. it is noticed that the corr., HD, and HI in all encrypted images by the suggested a chaotic Henon map are better than those of encrypted by a chaotic 2-D Logistic map.

From Figure 4, the HD and HI in the suggested a chaotic Hanon map is better than the chaotic 2-D Logistic map.

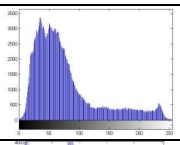
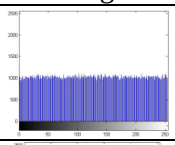
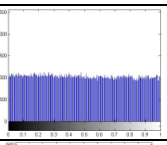
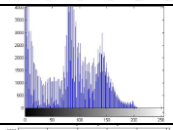
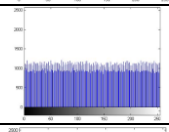
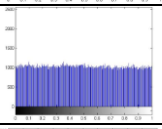
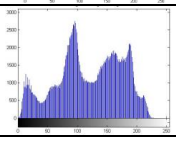
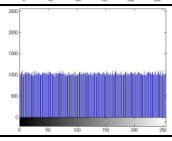
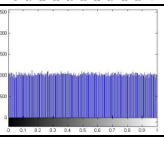
Image	Original image	Encrypted image with Henon and 2-D Logistic	
		2-D Logistic	Henon
Bata			
Girl			
Peppers			

Figure 4: Histogram results of the plainimages and encrypted using the proposed Henon and 2-D Logistic

It is also noticed that the values of UACI are very near to 33%. So, the suggested encryption technique is secure. The NPCR values are higher than 99% and therefore, changing a single pixel in the plainimage to be ciphered will lead to a ciphered image that is quite different from the outcoming encrypted image of the plainimage.

4.6. The PSNR measure

The PSNR is a calculation that quantifies the difference between the plainimage and the decrypted image. It is computed as [15,17-18]:

$$PSNR(I,D)=10\log_{10}\left(\frac{(255)^2}{\sum_{m=1}^{M}\sum_{n=1}^{N}\left(I(x_m.y_n)-D(x_m,y_n)\right|^2}\right) \quad (15)$$

Where $I(x_m,y_n)$ and $D(x_m,y_n)$ are the pixel values of the original and decrypted image at position (x_m,y_n), respectively. High PSNR values indicate good immunity against noise. The noise immunity results are given in Tables 2, 3, 4, 5 and 6. The results demonstrated that the proposed chaotic Henon map image encryption has a better immunity against AWGN and speckle noise than 2-D logistic which verifies the best choice for ideal optical telecommunication applications that can cancel the noise effects.

Table 2: The PSNR for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of AWGN noise for zero mean and different variances (0.05, 0.1, 0.15, and 0.2).

Image	PSNR							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata	9.8060	8.7381	8.4292	8.2652	14.2682	11.8853	10.6056	9.7804
Girl	9.5594	8.9466	8.6681	8.5212	13.9399	11.5771	10.3719	9.6379
Peppers	11.6611	10.3500	9.8276	9.4888	13.7447	11.4455	10.2872	9.5879

Table 3: The decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of AWGN noise for zero mean and different variances (0.05,0.1,0.15, and 0.2).

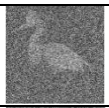
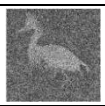
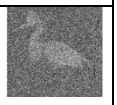
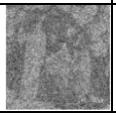
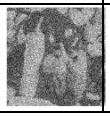
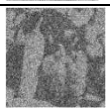
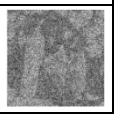
Image	PSNR							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata								
Girl								
Peppers								

Table 4: The PSNR for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of Speckle noise for different variances (0.05,0.1,0.15, and 0.2).

Image	PSNR							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata	12.2715	11.2794	9.5478	8.8939	22.1912	19.4066	17.7472	16.5825
Girl	10.3008	9.9735	9.9786	9.5904	21.3148	18.3272	16.6205	15.4219
Peppers	14.8926	12.9859	12.1722	11.4799	18.8753	16.0799	14.5075	13.4376

Table 5: The decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of Speckle noise for different variances (0.05,0.1,0.15, and 0.2).

Image	PSNR							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata								
Girl								
Peppers								

4.7. The Structure Similarity Index (FSIM)

The FSIM evaluate the deciphered image and can be defined as [23]:

$$\mathrm{FSIM} = \frac{\sum_{x\in\Omega} S_L(x).PC_m(x)}{\sum_{x\in\Omega} PC_m(x)} \tag{16}$$

Where Ω is the spatial domain of image, $S_L(x)$ denotes overall similarity among two images and $PC_m(x)$ denotes a value of phase congruency. High value for FSIM means noise immunity is better. The obtain FSIM results are given in Table 6, and 7 for decrypted images. These results confirm that the suggested a chaotic Henon map image encryption technique is noise resistant.

Table 6: The FSIM for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of AWGN noise for zero mean and different variances (0.05,0.1,0.15, and 0.2).

Image	FSIM							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata	0.5846	0.5524	0.5439	0.5425	0.7223	0.6482	0.6060	0.5776
Girl	0.4942	0.4460	0.4329	0.4264	0.6178	0.5355	0.4922	0.4640
Peppers	0.5658	0.5051	0.4792	0.4669	0.6534	0.5763	0.5361	0.5099

Table 7: The FSIM for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of Speckle noise for different variances (0.05,0.1,0.15, and 0.2).

Image	FSIM							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata	0.6683	0.6245	0.5749	0.5837	0.9330	0.8945	0.8675	0.87463
Girl	0.5277	0.4991	0.5015	0.4752	0.8637	0.8082	0.7712	0.77440
Peppers	0.7104	0.6257	0.5829	0.5506	0.8201	0.7551	0.7131	0.6840

4.8. The Structure Similarity Index (SSIM)

The SSIM can be computed as [23]:

$$SSIM(x,y|w) = \frac{(2\bar{w}_x\bar{w}_y + C_1)(2\sigma_{w_xw_y} + C_2)}{(\bar{w}_x^2 + \bar{w}_y^2 + C_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + C_2)} \quad (17)$$

Where, C_1, C_2 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 $\sigma_{w_xw_y}$ denotes covariance among two regions w_x and w_y. High value for SSIM means noise immunity is better. The obtain SSIM results are given in Table 8 and 7. These results confirm that the suggested a chaotic Henon map image encryption technique has better resistance to noise.

Table 8**:** The SSIM for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of AWGN noise for zero mean and different variances (0.05,0.1,0.15, and 0.2).

Image	SSIM							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0.15	0.2
Bata	0.1399	0.0853	0.0684	0.0588	0.4055	0.2942	0.2390	0.2040
Girl	0.1249	0.0786	0.0613	0.0531	0.2709	0.1911	0.1553	0.1328
Peppers	0.2007	0.1245	0.0956	0.0748	0.3245	0.2360	0.1952	0.1708

Table 9: The SSIM for decrypted images using a chaotic Henon map and 2-D logistic map.in the presence of Speckle noise for different variances (0.05,0.1,0.15, and 0.2).

Image	SSIM							
	2-D Logistic				Henon			
	0.05	0.1	0.15	0.2	0.05	0.1	0,15	0.2
Bata	0.3005	0.2322	0.1336	0.1508	0.8378	0.7467	0.6798	0.6313
Girl	0.1763	0.1421	0.1447	0.1215	0.6675	0.5765	0.5246	0.4905
Peppers	0.4108	0.2794	0.2278	0.1875	0.5918	0.4787	0.4170	0.3758

5. CONCLUSIONS

Aiming to improve the encryption security, we purpose in this paper a chaotic confusion-diffusion image encryption scheme based on Henon map. The security measures are performed on both the 2-D logistic map and the proposed chaotic confusion-diffusion Hénon map to compare their performance.

The test results have proved that the proposed image encryption technique offers high-security level, and outperforms with its excellent potential of encryption. Compared to other methods of encryptions from the state of arts, the suggested technique offers high-security level and can immune many types of attacks such as the known-plaintext, cipher text-only attack, differential attack, and statistical attack.

REFERENCES

[1] Lee, S.hyun. & Kim Mi Na, (2008) “This is my paper”, ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[2] Gizem, Aksahya & Ayese, Ozcan (2009) Coomunications & Networks, Network Books, ABC Publishers.

[3] G. Chen, Y. Mao, and C.K. Chui, (2004) "A symmetric image encryption scheme based on 3D chaotic Cat maps," Chaos, Solitons and Fractals, Vol. 21, pp. 749-61.

[4] G. Peterson, (1997) "Arnold’s Cat map," Math Linear Algebra.

[5] H. Gao, Y. Zhang, S. Liang, and D. Li, (2006) "A new chaotic algorithm for image encryption," Chaos, Solutions and Fractals, Vol. 29, pp. 393-399.

[6] H.S. Kwok, and K.S. Tang, (2007) "A fast image encryption system based on chaotic maps with finite precision representation," Chaos, Solitons and Fractals, Vol. 32(4), pp. 1518–1529.

[7] H.H. Nien, C.K. Huang, et al., (2007) "Digital color image encoding and decoding using a novel chaotic random generator," Chaos, Solitons and Fractals, Vol. 32, pp. 1070–1080.

[8] N.K. Pareek, V. Patidar, and K.K. Sud, (2006) "Image encryption using chaotic logistic map," Image & Visual Computing, Vol. 24, pp. 926–934.

[9] J. Fridrich, (1998)"Symmetric Ciphers Based on Two-dimensional Chaotic Maps," International Journal of Bifurcation and Chaos, Vol. 8(6), pp. 1259-1284.

[10] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Faragallah, (2007) "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," An International Journal of Computing and Informatics, Vol. 31(1), pp. 121-129.

[11] Jiahui Wu, Xiaofeng Liao, Bo Yang, (2018) “Image encryption using 2D Hénon-Sine Map and DNA approach” , ELSEVIER, Signal Processing, Vol. 153, pp. 11-23.

[12] S. Lian, G. Sun, and Z. Wang, (2005) "A block cipher based on a suitable use of chaotic Standard map," Chaos, Solutions and Fractals, Vol. 26, pp. 117-129.

[13] J. Fridrich , (1998) “Symmetric ciphers based on two-dimensional chaotic maps,” Int. J. Bifurcation and Chaos, Vol. 8, pp. 1259-1284.

[14] X. Zhang, and W. Chen, (2008) "A New Chaotic Algorithm for Image Encryption," Proceedings of the International Conference on Audio Language and Image processing,.

[15] M. Hénon, “A two-dimensional mapping with a strange attractor, (1976) ” Communications in Mathematical Physics, Vol. 50, no. 1, pp. 69–77. View at Publisher.

[16] E. Lorenz, (1963) ”Deterministic nonperiodic flw”, Journal of Atmospheric Science, Vol.20, No. 2, pp.130-141.

[17] Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Springer, June 2013 "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," Signal, Image and Video Processing Journal, DOI 10.1007/s11760-013-0490-x.

[18] Guan ZH, Huang F, Guan W., (2005) "Chaos-based image encryption algorithm". Phys Lett A; 346(1--3):153–7.

[19] K. Wong, B. Kwok, and W. Law W, (2007) "A Fast Image Encryption Scheme based on Chaotic Standard Map," Phys. Lett A.

[20] M. Rafikov, J.M. Balthazar, "On control and synchronization in chaotic and hyperchaotic systems via linear feedback control, Sept. (2008)" Communications in Nonlinear Science and Numerical Simulation, vol. 13(7), pp. 1246–1255, Elsevier.

[21] J.M.V. Grzybowski, M. Rafikov, J.M. Balthazar, June (2009)"Synchronization of the unified chaotic system and application in secure communication," Communications in Nonlinear Science and Numerical Simulation, vol. 14(6), pp. 2793–2806, Elsevier,.

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

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

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

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

AUTHOR

Ashraf Afifi received the B.Sc.(Hons.), M.Sc., and Ph.D. degrees in Electronic and Communication Engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently Associate Professor with the Department of Computer Engineering, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. He is a coauthor of about 30 papers in international journals and conference proceedings. His research interests cover communication security, image processing, and image encryption. Email: a.afifi@tu.edu.sa, Mobile: 00966507275265.