MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS (2021) 4 (1) 17-26

DOI: *https://doi.org/10.37231/myjcam.2021.4.1.71*

Article: Received 11.11.2020; Accepted 21.03.2021; Published 31.03.2021

Using of Multi Chaotic System For Implementing A Good Cryptosystem

ALI CHERIF Khalfallah, HADJ SAID Naima, ALI PACHA Adda

Laboratory of coding and information security-LACOSI University of Science and Technology of Oran - USTO-MB Oran, Algeria.
alicherif.kha@gmail.com

Abstract: This article proposes an algorithm of confusion and diffusion of image encryption based on the logistic map and the attractor of Henon-Lozi. We chose the initial parameters of the logistic map and the Henon-Lozi Attractor as secret keys. The Henon-Lozi Attractor is used to generate a chaotic matrix to mask the pixel values and the logistic map uses to generate random sequences to make a permutation between the pixels. The computer experience such as statistical analysis, sensitivity analysis proves that the proposed image encryption algorithm is robust and secure enough to be used in practice.

Keywords: *Chaos, Encryption, Henon-Lozi, Attractor, Logistic map - P-box*.

1. INTRODUCTION

With the rapid growth of the image transmission requirement on the Internet, the protection of digital information from illegal uses is becoming increasingly important. Because of the large data capacity and the high correlation between pixels in image files, traditional techniques are not suitable for image encryption [1]. Compared to traditional methods (such as AES and DES), chaos-based image encryption schemes have shown superior performance [2-4].

The general permutation-diffusion procedure [5] for chaos- based image encryption consists of two steps: the diffusion and the permutation of the pixels. Fig. 1 illustrations its architecture. In the diffusion process, the pixel values are modified sequentially. In the permutation process, the position of the pixels in the image is changed, so that a tiny change for one pixel can extend to almost every pixel. of the entire image.

In this article, an image encryption method based on chaos is proposed. The key flow in the diffusion step generate by the Henon-Lozi function and combine with the pixel value of the image in clear, then the algorithm generates a permutation P-box with the same image size by a logistics map, which completely upsets the positions of the pixels. Theoretical analyzes and computer simulations verify the feasibility and the superiority of the proposed encryption algorithm, see the diagram of our proposed system. 6.

This document is organized as follows. In section 2, the confusion function generated by the Henon-Lozi function is introduced. In section 3, the logistic function and the permutation operation based on it are introduced. In section 4, the decryption algorithm, In section 5, performance analyzes and simulation results are reported. Section 6 gives some conclusions.

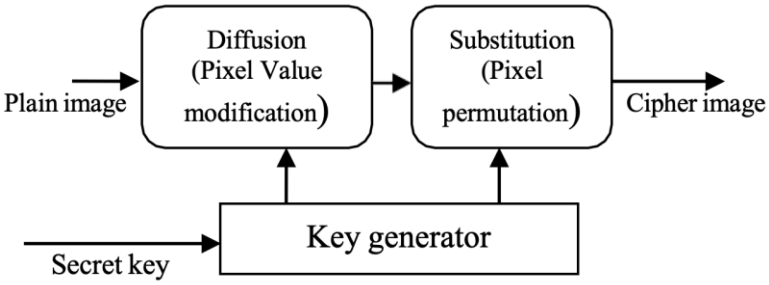


Fig. 1. General architecture diffusion-permutation

2. CONFUSION OPERATOR BASED ON THE HONON-LOZI ATTRACTOR:

A. The Hénon-Lozi Attractor [6] :

The attractor defined by the following system of equations (1), where a, b are constants: The initial values of X0, Y0 and a, b are considered the secret key.

$$\begin{cases} X(n+1)=1+Y(n)-a*|X(n)| \\ Y(n+1)= b*X(n) \end{cases} \quad (1)$$

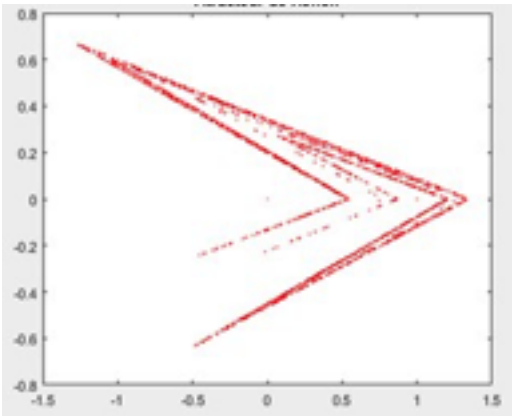


Fig. 2. The Henon-Lozi Attractor.

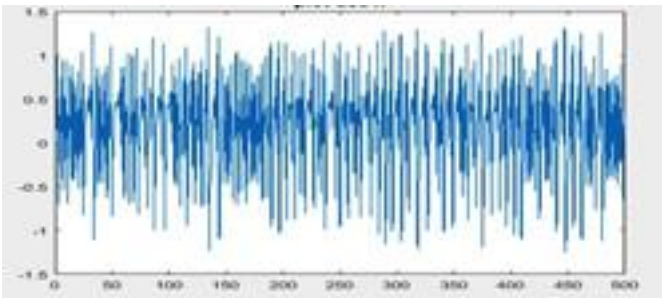


Fig.3. Plot of X.

B. Confusion operator based Henon-lozi system:

Henon-Lozi map was used to generate a confusion matrix of the same size of the original image. (We use as key the initial parameters of the Henon-Lozi function a, b, X0, Y0).
- We combine with an exclusive or XOR (bit by bit) between the pixels of the image in clear and the matrix of confusion generated by the first function (Henon-Lozi map).

Algorithm that generates the 'mat-conf' confusion matrix:

```
r=row*col ;
x=zeros(1,r);
y=zeros(1,r);
x(1)=x0;
y(1)=y0;
for n=1:r-1
    x(n+1)=1+y(n)-a*abs(x(n));
    y(n+1)=b*x(n);
end
for n=1:r
mat-conf(n)=mod(fix(x(n)*10^7),256)+1;
end.
```

3. PERMUTATION OPERATOR BASED ON LOGISTIC MAP

A. Logistic map [7]:

The logistic map shown in (2) is a discrete chaotic system when the parameter μ between 3.57 and 4. Here, the initial value X_0 and the parameter μ are considered as the secret key.

$$Xn+1 = \mu * Xn * (1-Xn) \qquad (2)$$

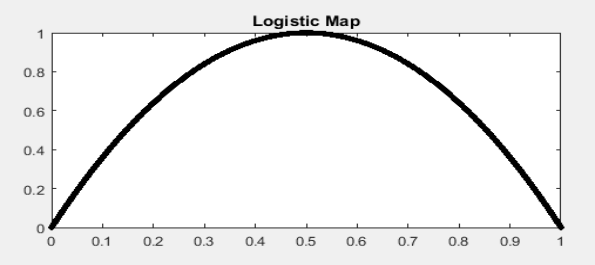


Fig. 4. The Logistic Map Equations.

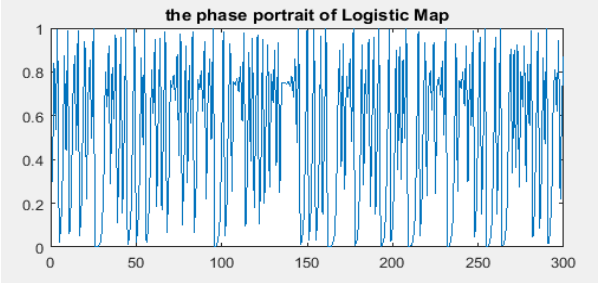


Fig. 5. The phase portrait of Logistic Map

B. Permutation Operator based on Logistic map:

For a gray scale image 256 of size M × N, it is an integer matrix of M rows and N columns, in which the values range from 0 to 255. Its data can be treated as a one-dimensional vector A = {a1, a2, .., aMN} where ai designates the gray level of the image pixel in the column (i/N) column mod (i, N). Given x0 and μ, to change the pixel position of the image, we take the following steps:

Step 1: Iterate the logistic map xi + 1 = F (x) using equation (2) for L times when L> M * N. and obtain P'= {x1, x2, ..., xMN, ...xL}.
Step 2: Obtain an entire random sequence P'' according to the following formula: for i = 1: L make p''(i) = mod (fix ((10 ^ 2) * x (i)), MN) +1;
Step 3: uses P = unique (p'', 'stable') the function MATLAB returns the same data as in p'', but without repetitions and P is in the same order as p''.
Step 4: use P as our P-box.

Unlike traditional block-based encryption methods such as DES and AES, the proposed algorithm completely swaps the pixel positions of the image, using a P-box with the same simple image size.

4. THE ALGORITHM OF DECRYPTION

The decryption procedure is similar to that of the encryption process in reverse order:

Step1: Generation of P-box by the logistic function with the same initial parameters X0,μ.
Step2: Get P' from C (Cipher image)
Step3: Generation of Confusion matrix by the Henon-Lozi.
Step4: We combine with an XOR (bit by bit) between the pixels of the P' and the matrix of confusion generated by the first function (Henon-Lozi map) we get the plain Image.

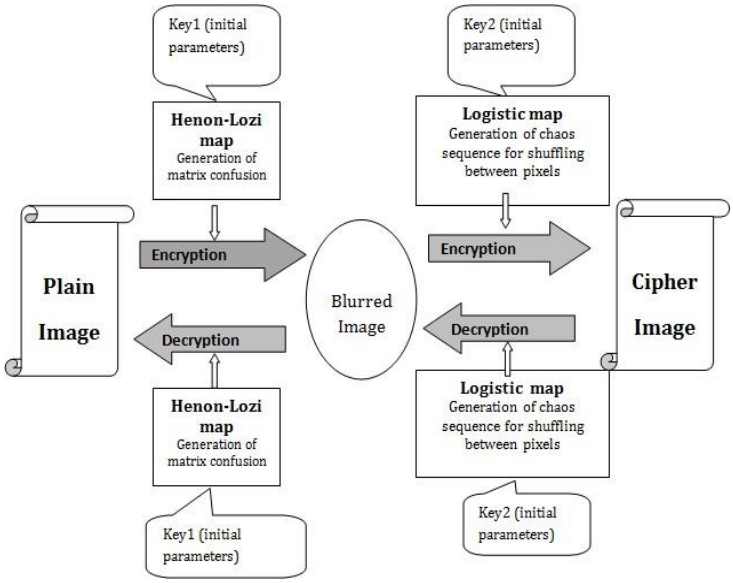


Fig. 6. Diagram of our proposed system

5. PERFORMANCE TEST AND ANALYSIS

A. Key Space Analysis

The size of the key space is the total number of different keys that can be used in encryption. A good encryption algorithm should be sensitive to secret keys, and the key space should be big enough to make a brute force attack impossible. In the proposed algorithm, one key one for the logistic function consists of the initial value x0 and the parameter μ, where 3.57 <μ <4. And the second key for the Henon-Lozi attractor consists of the initial values x0, Y0 and a, b; Thus, the proposed algorithm gives a completely different deciphered image for a slightly modified key.

B. Statistical analyzes

Shannon suggested that diffusion and confusion should be used in a cryptographic system [8] in order to frustrate powerful statistical analysis. In the proposed encryption algorithm, a sequence of random numbers was generated by Henon-Lozi map to modify the pixel values sequentially which can be considered a confusing process, and after a dynamic P-box generated by a logistics map is used to swap the normal image, which can be considered as a diffusion process.

As a result, the broadcast image is randomly distributed. This is shown by a test on the histograms of the encrypted images in Section C, the correlations between adjacent pixels in the encrypted image and the clear image in Section D, and the information entropy of the encrypted image in section E.

C. Histograms of the encrypted image:

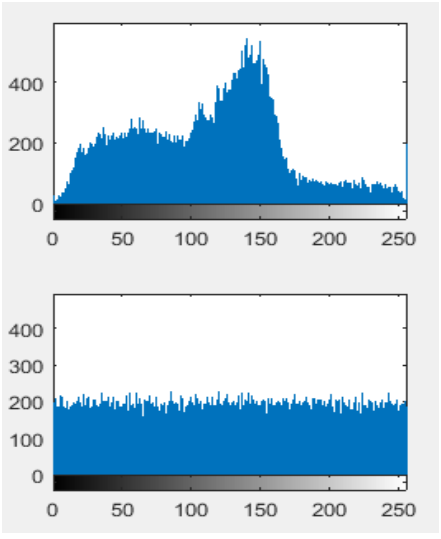
Figs. 4 and 5 illustrate the histograms of the "APCsaida" (a) single image and (b) the corresponding encrypted image. The histogram of the encrypted image is almost evenly distributed, which may well protect image information to resist statistical attack [9]

(a)

(b)

Fig. 7. (a) Plain-Image 'APCsaida'- and (b) corresponding Cipher-Image ''

(a1)



(b1)

(a2)

(b2)

(a3)

(b3)

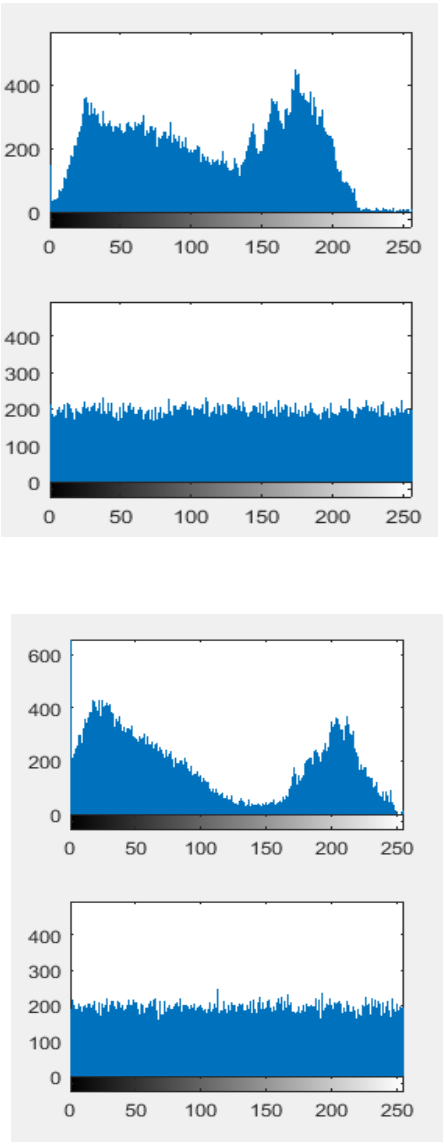


Fig. 8. Histogram (a) Plain-image 'APCsaida'- (b)Cipher image using proposed method 1:red canal - 2: green canal – 3: blue canal

D. Correlation of two adjacent pixels

There is a strong correlation between the pixels of an image that is called intrinsic feature. Thus, a secure encryption scheme should remove it to improve the resistance against statistical analysis. To test the correlation between two adjacent pixels in a single image and an encrypted image, we randomly select a group of adjacent pairs of pixels (vertically, horizontally and diagonally) from the simple image and the encrypted image, and calculate the coefficient of each pair by equation (6).

$$Y_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} \quad (3)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_{i-}\bar{x})(y_{i-}\bar{y}) \quad (4)$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{N}(x_{i-}\bar{x})^2 \quad (5)$$

$$\sigma_x = \frac{1}{N}\sum_{i=1}^{N}(y_{i-}\bar{y})^2 \quad (6)$$

Where x and y are gray scale values of two adjacent pixels in the image. Table 1 shows the correlation coefficients of two pixels adjacent to the image plain and the encrypted image. This correlation analysis proves that the chaotic encryption scheme satisfies zero co-correlation, which is a high-level private security.

TABLE I. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN THE PLAIN AND THE CIPHER-IMAGE.

Direction	**Plain-image**	**Cipher-image by proposed system**
Horizontal	0.86696	5.6835 **E**-05
Vertical	0.89084	0.0066414
diagonal	0.80294	-0.0037051

E. Entropy Analysis of Information

Entropy is the most remarkable feature of randomness. For entropy information H (s) of a message sources can be calculated as (7) [10]:

$$H(s) = \sum_{i=0}^{2^N-1} p(s) \times \log_2\left(\frac{1}{p(s_i)}\right) \quad (7)$$

Where p(si) indicates the symbol probability Si. For a true random source emitting 2N symbols, the entropy should be N. Take an image in 256 gray levels for example, and the pixel data have 28 possible values, so the entropy of a "real random» image must to be 8. The entropy of the encrypted images is shown in Table 2. The values obtained are very close to the theoretical value 8. This means that the leakage of information in the encryption process is negligible and that the encryption scheme is secure when an entropic attack

TABLE II. ENTROPY VALUE FOR THE ENCRYPTED IMAGE

Canals	**Entropy value for plain-image**	**Entropy value for cipher- image**
Canal 1 Red	7.67	7.9971
Canal 2 green	7.6903	7.9964
Canal 3 blue	7.5997	7.9963

F. Sensitivity analysis

In order to test the difference between two images, we measure the NPCR [11] (number of pixels changes rage) and UACI [12] (uniform average changing intensity) by Eqs. (11) and (12).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{w \times H} \times 100 \qquad (7)$$

$$UACI = \frac{1}{w \times H}\left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\right] \qquad (8)$$

where C1 and C2 are two images of the same size (M × N). If c (i, j) = c2 (i, j) then D (i, j) = 1, else D (i, j) = 0.

TABLE III. NPCR AND UACI VALUES BETWEEN THE ORIGINAL IMAGE AND THE ENCRYPTED IMAGE

Key (Henon-Lozi) a-b-x_0-y_0	**Key(Logisticmap)** x_0-μ	**NPCR()**	**UACI(%)**
(1.7-0.5-0-0)	(0.123456-4)	99.50	32.51
(1.7-0.5-0-0)	(0.1234560001-4)	99.58	33.56
(1.7-0.5-0-0)	(0.123456-4)	99.61	33.66
(1.7-0.5-0.0001-0)	(0.123456-4)	99.50	32.49

6. CONCLUSIONS

In this article, chaos-based image encryption with a diffusion-permutation architecture is proposed. In the broadcast step, the key flow depends on both the key (the initial value and the control parameters of the Henon-Lozi map) and the clear image. In the permutation step, the schema generates a P-box with the same plain-image size by a Logistics map. The key space is large enough to withstand brute force attacks. Statistical analysis shows that the scheme can well protect the image of the statistical attack. The system has a high key sensitivity and has good anti- differential attack capability. With high encryption speed, it can be used in Internet applications.

References

[1] S. Li, G. Chen, A. Cheung, B. Bhargava, K.-T. Lo, On the Design of Perceptual PEGvideo Encryption Algorithms, CoRR abs/cs/0501014, 2005.
[2] J. Fridrich, International Journal of Bifurcation and Chaos 8 (1998) 1259.
[3] F. Sun, S. Liu, Z. Li, Chaos, Solitons & Fractals 38 (2008) 631.
[4] Z. Liu, Q. Guo, L. Xu, M.A. Ahmad, S. Liu, Optics Express 18 (2010) 12033.
[5] G. Chen, Y. Mao, C.K. Chui, Chaos, Solitons & Fractals 21 (2004) 749
[6] R. Lozi. UN ATTRACTEUR_ETRANGE (?) DU TYPE ATTRACTEUR DE Henon Journal de Physique Colloques, 1978, 39 (C5), pp.C5-9-C5-10.
[7] May, Robert M. (1976). "Simple mathematical models with very complicated dynamics". Nature. 261 (5560): 459–467.
[8] C.E. Shannon, Bell Systems Technical Journal 28 (1949) 656.
[9] F. Sun, Z.L.S. Liu, Optics Communications 283 (2010) 2066.
[10] A.D. Santis, A.L. Ferrara, B. Masucci, Discrete Applied Mathematics 154 (2006) 2348 Coding and Cryptography.

[11] A.G. Bluman, Elementary Statistics: A Step by Step Approach, WCB/McGraw-Hill,1997.
[12] Y. Mao, G. Chen, S. Lian, International Journal of Bifurcation and Chaos 14 (2004)3613