A New Parallel Fuzzy Multi Modular Chaotic Logistic Map for Image Encryption

Mahmoud Gad[1], Esam Hagras[2], Hasan Soliman[1], and Noha Hikal[1]
[1]Faculty of Computers and Information Sciences, Mansoura University, Egypt
[2]Faculty of Engineering, Delta University for Science and Technology, Egypt

Abstract: *This paper introduces a new image encryption algorithm based on a Parallel Fuzzy Multi-Modular Chaotic Logistic Map (PFMM-CLM). Firstly, a new hybrid chaotic system is introduced by using four parallel cascade chaotic logistic maps with a dynamic parameter control to achieve a high Lyapunov exponent value and completely chaotic behavior of the bifurcation diagram. Also, the fuzzy set theory is used as a fuzzy logic selector to improve chaotic performance. The proposed algorithm has been tested as a Pseudo-Random Number Generator (PRNG). The randomness test results indicate that system has better performance and satisfied all random tests. Finally, the Arnold Cat Map with controllable iterative parameters is used to enhance the confusion concept. Due to excellent chaotic properties and good randomization test results, the proposed chaotic system is used in image encryption applications. The simulation and security analysis indicate that this proposed algorithm has a very high security performance and complexity.*

Keywords: *Image encryption, parallel multi modular chaotic maps, pseudo-random number generation, fuzzy logic selector.*

Received August 24, 2019; accepted September 7, 2020
https://doi.org/10.34028/iajit/18/2/12

1. Introduction

Recently, secure image storage and transmission over the public network have been increased for essential uses and sharing purposes. There is a big challenge to protect the image from unauthorized users, especially in sensitive fields like the military, politics, economics, medical, and education. The protection of multimedia content must be provided through privacy, integrity, and identity management. In order to achieve the information security task in an efficient manner. Cryptology based approach has been utilized wildly in many applications. The traditional cryptographic techniques such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [28] are not suitable for an image due to their distinguishing features including bulk data capacity, high redundancy [33].

In the last ten years, many studies have proved that the chaotic system has many essential features that can be used efficiently for encrypting images. The chaotic properties are, high sensitivity to the initial condition, control parameters, periodicity, and pseudo-randomness that can be profitably applied to both confusion and diffusion process [4, 17], many researchers suggested many strategies in the chaotic cryptographic algorithms such as chaotic synchronization [32], bit-level permutation [23, 31], combination permutation with diffusion method [22, 24] and extended diffusion substitution [25]. Other chaos-based image encryption algorithms used multiple chaotic maps [2, 11], two-dimensional Arnold cat map [12, 13, 36], barker map [21], quantum chaotic system [37], parametric switching [38], spatiotemporal chaotic system [1], nonlinear dynamical system [16] parallel computing system [30], and chaotic fuzzy image encryption [5, 6] were suggested.

The chaotic maps can be classified into two types, one dimensional and higher dimensional chaotic maps. The 1-D chaotic maps such as a logistic map, Tent map, Sine map have a single variable over discrete steps in time [9, 18, 26]. Although the 1-D chaotic maps have a simple structure, low complexity, and it is easy to implement, these types of maps have many weaknesses such as the small number of control parameters, chaotic ranges are limited and it can easily change to periodic map [14, 39]. On the other hand, the higher dimension chaotic maps have at least two variables and they have better performance and their chaotic orbits are more difficult to predict [7, 10, 20], but they have high-computing costs and difficult to implement in hardware which means it is not real-time processing [3, 29, 34]. To overcome the limitation of the one dimension chaotic maps. The authors introduce a new 1-D chaotic system for image encryption based on the modular one concept [16, 39] to improve the range of the control parameters. Zhou *et al.* [40] have proposed a Cascade Chaotic System (CCS) as a general 1-D chaotic framework to produce a new nonlinear chaotic system using any two 1-D chaotic maps as seed maps. Also, Hua and Zhou [8] have proposed a Dynamic Parameter-Control Chaotic System (DPCCS). The DPCCS has a simple structure that used the output of a chaotic map (control map) to

dynamically control the parameters of another chaotic map (seed map). CCS and DPCCS have simple structures, highly chaotic behavior, and easy hardware implementation. However, there are some weaknesses when cascading more seed maps, such as time delaying, complex analysis, and difficult implementation in hardware [40].

To address these above-mentioned problems, this paper introduced a new chaotic system based on the idea of hybrid CCS and DPCCS. Based on the simple 1-D chaotic logistic maps, a new hybrid CCS with DPCCS will be present to achieve a very complex bifurcation phase diagram and large Lyapunov Exponent value. Also, the fuzzy set theory is used as a fuzzy logic selector to improve key space and security protection. Besides, the concept of parallel processing is used in the proposed system. The introduced system is called Parallel Fuzzy Multi Modular Chaotic Logistic Maps (PFMM-CLM). In this paper, the diffusion and confusion mechanism are used in the proposed image encryption, many statistical and sensitivity analysis are calculated for evaluation performance of our algorithm. In summary, the most important contributions in this paper are:

1. Design a new chaotic system based on hybrid CCS and DPCCS techniques.
2. Design a new PFMM-CLM with a complex bifurcation diagram and a large LE.
3. A Fuzzy chaotic Pseudo-Random Number Generator (PRNG) based on the proposed PFMM-CLM has been introduced.
4. Parallel processing computation concept to speed up the processing time is used.
5. New controllable iterative parameters for Arnold cat map are suggested.

The remnant of the paper is arranged as follows: in section 2, the related work will be introduced. The proposed PFMM-CLM-PRNG is designed in section 3. The image encryption and decryption mechanism based on the fuzzy technique is discussed in section 4. Security and performance analysis of the proposed encryption scheme is given in section 5. Finally, the conclusions are given in section 6.

2. Related Works

In this section, a one-dimensional chaotic logistic map is presented and its prior researches of developing nonlinear chaotic systems.

2.1. Logistic Map

A Logistic map is the 1-D discrete chaotic map that largely applied in many applications such as social, science, and economics, the generated sequence using a logistic map is (x) and it can be computed mathematically using the following equation [9]:

$$x_{n+1} = r\, x_n\, (1 - x_n) \quad (1)$$

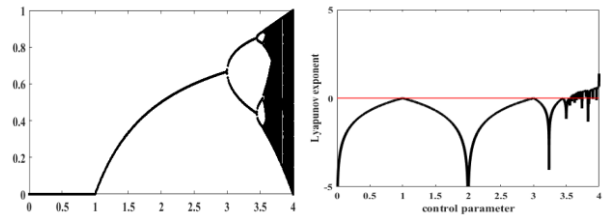
Where: "r" is a control parameter ϵ [0, 4], n is the iteration number, x_{n+1} is interval [0, 1]. The bifurcation diagram and LE values of the non-modular logistic map are shown in Figure 1-a), it appears the limitation of the control parameters which started from 0 to 4 and large negative LE values [39]

2.2. Modulo Operation

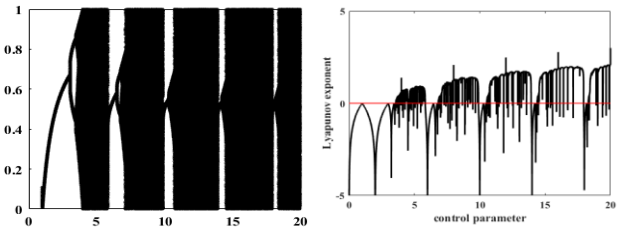
The modular function performs an iterative folding process, thus producing uncorrelated random data, it used to increase non-linearity and rang of control parameters [16]. The modular logistic map achieves a large control parameter started from 0 to 20 as shown in Figure 1-b), but also it has multi gaps and large negative LE values.

2.3. Cascaded Operation

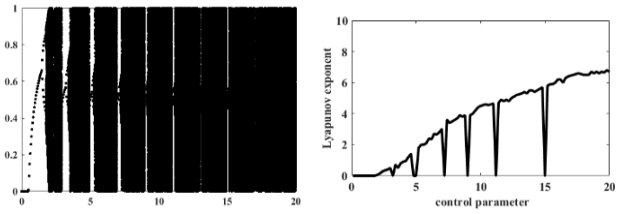
CCS connects two 1-D chaotic maps (seed maps) in series, the output of the first seed map is linked to the input of the second seed map. The output is fed back into the input of the first one for recursive iterations, the bifurcation diagram, and the LE values of the two cascaded logistic maps are improved compared with the single modular chaotic logistic maps [40]. Despite the cascaded modular chaotic logistic maps have a highly LE value of 6.3 but they have multi negative LE values (multi gaps) of zero LE values as shown in Figure 1-c).



a) The bifurcation diagram and LE for non-modular CLM.



b) The bifurcation diagram and LE for modular CLM.



c) The bifurcation diagram an d LE for cascaded M-CLM

Figure 1. The bifurcation diagram and Lyapunov exponent for (a) non-modular CLM (b) modular CLM (c) cascaded MCLM.

2.4. Modulation Operation

The Modulation function is used to generate dynamic control parameters by using the output of a chaotic map for another chaotic map to display chaotic behaviors [8].

The bifurcation diagram and LE values of non-modular, modular, and cascaded chaotic logistic maps have multi gaps and negative LE values as shown in Figure 1, for this limitation, this paper introduced a new chaotic system based on fuzzy multi-modular chaotic Logistic maps to solve the multi gaps problem and negative LE value show in the chaotic logistic maps and their nonlinear operations.

3. Proposed PFMM-CLM-PRNG

In this section, the main idea of the proposed system will be introduced to use the simple 1-D modular chaotic logistic map to present a new hybrid CCS with DPCCS to achieve a good bifurcation phase diagram and large lyapunov exponent value. The bifurcation diagram outlines the sequences of chaotic system output with changing parameters, Lyapunov exponent is used to testing the chaotic behavior of the proposed PMM-CLM [8], a positive LE value for a dynamic system points to the sequential output paths generated from very close initial inputs diverge significantly in each iteration. The larger positive LE values indicate faster spacing in the output paths, thus better chaotic performance [40]. The authors improved the control parameter based on modulo operation to increases non-linearity and rang of control parameter [16], the output of the master modular logistic map is $F_{(X)}$ and it can be computed as follow:

$$F_{(X)} = x_{n+1} = F(r, x_n)\ mod\ 1 \qquad (2)$$

The control parameters of master map rϵ [4, 20] at the positive LE value. Now, let's explain how the proposed PFMM-CLM-PRNG sequence will be generated by using the output of master M-CLM.

- *Step* 1. used the output of Equation (2) to satisfy and achieve the following characteristics:

1. Dynamic control parameters for PMM-CLM as modulation process.
2. Cascaded chaotic system by using output value x_{n+1} as input for PMM-CLM.
3. Fuzzy logic selector to control the output of the proposed PMM-CLM.

- *Step* 2. in this step, the scaling process (S) used the output from Equation (2) to generate dynamic control parameter as modulation operation [11] by multiplying the output value x_{n+1} by scaling factor of 10^{10} and use the modular of 16 as follow:

$$r_{1n} = S(F_{(X)}) = x_{n+1} * 10^{10}\ mod\ 16 \qquad (3)$$

To avoid zero or negative LE value, add 4 to the output of Equation (3), to ensure that the dynamic control parameters "r_n" is greater than 4 as shown in Equation (4).

$$r_n = r_{1n} + 4 \qquad (4)$$

Where: "r_n" are the dynamic control parameter values which confused between the values 4 and 20.

- *Step* 3. use the output of the master map as input for PMM-CLM to generate four cascaded system in parallel form with dynamic control parameters. In addition to, initial value for each logistic map as follows:

$$x^1_{n+1} = F_{(X)}\ \Theta\ F_1(r_n, x^1_n))\ mod\ 1 \qquad (5)$$

$$x^2_{n+1} = F_{(X)}\ \Theta\ F_2(r_n, x^2_n)\ mod\ 1 \qquad (6)$$

$$x^3_{n+1} = F_{(X)}\ \Theta\ F_3(r_n, x^3_n))\ mod\ 1 \qquad (7)$$

$$x^4_{n+1} = F_{(X)}\ \Theta\ F_4(r_n, x^4_n))\ mod\ 1 \qquad (8)$$

Where, "Θ" is the cascaded operation and x^1_n is the iteration value, r_n and x_{n+1} are the output of scaling step and master map respectively

- *Step* 4. in this step, fuzzy logic selector is used to design fuzzy rules based on the output of master PMM-CLM to control the output of the proposed PFMM-CLM to generate chaotic fuzzy sequence x^f_n as follows:

If $(0 < x_{n+1} \le 0.2)$ then output is
$x^f_n = (x^1{}_{n+1} + x^2{}_{n+1} + x^3{}_{n+1})\ mod\ 1$
If $(0.2 < x_{n+1} \le 0.4)$ then output is
$x^f_n = (x^1{}_{n+1} + x^2{}_{n+1} + x^4{}_{n+1})\ mod\ 1$
If $(0.4 < x_{n+1} \le 0.6)$ then output is
$x^f_n = (x^1{}_{n+1} + x^3{}_{n+1} + x^4{}_{n+1})\ mod\ 1$
If $(0.6 < x_{n+1} \le 0.8)$ then output is
$x^f_n = (x^2{}_{n+1} + x^3{}_{n+1} + x^4{}_{n+1})\ mod\ 1$
If $(0.8 < x_{n+1} \le 1)$ then output is
$x^f_n = (x^1{}_{n+1} + x^2{}_{n+1} + x^3{}_{n+1} + x^4{}_{n+1})\ mod\ 1$

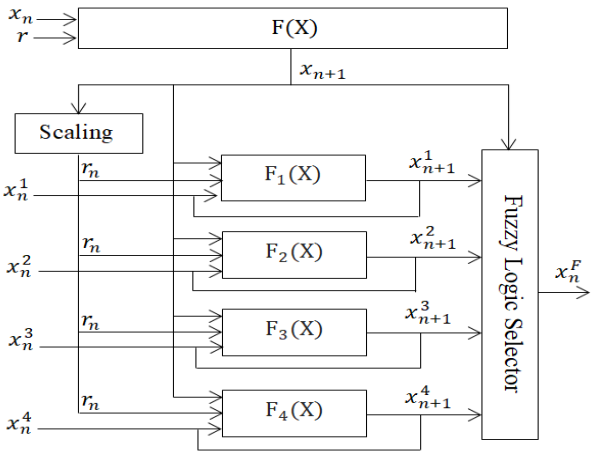


Figure 2. The proposed PFMM-CLM-PRNG.

- *Step* 5. convert all the output sequence x_n^f into integer values by multiply the output by the scaling factor of 10^{10} and the output is modular by 256 through the following process.

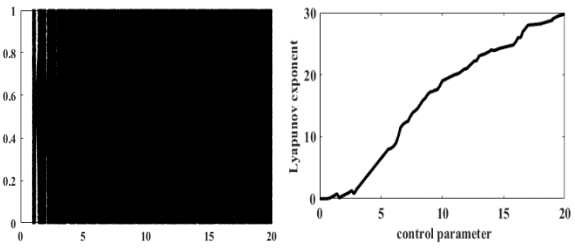
$$x_n^F = (x_n^f * 10^{10}) \; mod \; 256 \tag{9}$$

x_n^F refer to the PRNG for the proposed PFMM-CLM as shown in Figure 2.

3.1. Dynamic Characteristic of Proposed PFMM-CLM-PRNG

The proposed PMM-CLM-PRNG has appositive LE values for all control parameters from 4 to 20 as shown in Figure 3. From this result, four modular cascaded logistic maps are select as the core of the proposed parallel multi-modular chaotic logistic map.

In order to satisfy a fast hardware implementation, the designs of the proposed four cascaded modular chaotic logistic maps are designed in a parallel processing concept. Each map from the four modular chaotic logistic maps is injected with its security parameters in parallel form. The bifurcation diagram and Lyapunov exponent for proposed PFMM-CLM-PRNG are given in Figure 3 can be compared with Figure 1 a)-c). It can be concluded from this comparison that the bifurcation diagram of the proposed PFMM-CLM is more complex compared with the bifurcation diagram shown in Figure 1. Also, the Lyapunov exponent for the proposed PFMM-CLM is completely continuous (no gaps in LE) which gives a robust chaotic system.



a) Bifurcation diagram. b) Lyapunov exponent.

Figure 3. The Bifurcation diagram and lyapunov exponent for the proposed PMM-CLM-PRNG.

3.2. Randomness Analysis

The 2010 version statistical test suite published by the National Institute of Science and Technology (NIST SP800-22) is used to check the randomization of a generated binary sequence by PRNGs [27], a statistical test is used to calculate p_value, If p_value equal 1, it means that the sequence being tested is completely random, while p_value equal 0 indicates a non-random character. A significance level (α) is selected in the range [0.001, 0.01]. In this paper, the NIST SP800-22 is used to test the bit a sequence of the proposed PFMM-CLM- PRNG, and the value of α is set to 0.01. The results of the proposed PFMM-CLM- PRNG are shown in Table 1.

Table 1. Randomness test results of the proposed PFMM-CLM-PRNG using NIST SP800-22.

Statistic Tests for ciphered image	p value	Result
Frequency (monobit) test	0.9243	Pass
Frequency test within a block	0.2219	Pass
Runs test.	0.2219	Pass
longest run of ones in a block	0.6638	Pass
Binary matrix rank test	0.7214	Pass
Discrete Fourier transform (spectral)	0.9293	Pass
Non-overlapping template	0.5495	Pass
Overlapping template	0.6257	Pass
Maurer's "universal statistical" test	0.6127	Pass
Linear complexity test.	0.8895	Pass
Serial test	0.7215	Pass
Approximate entropy	0.7621	Pass
Cumulative sums	0.8164	Pass
Random excursions	0.6732	Pass
Random excursions variant	0.7765	Pass

4. Proposed PFMM-CLM Image Encryption

In this section, the proposed image encryption and decryption mechanism based on PFMM-CLM and CI-ACM will be discussed. The modular 1D chaotic logistic map will be used as a master map to generate both secure parameters for PMM-CLM and the fuzzy logic selector which is used to generate controllable iterative parameters for Arnold cat map.

The Arnold cat map is a 2-D chaotic map and it can be represented in the matrix as follow [36]:

$$\begin{bmatrix} X_{m+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_m \\ Y_n \end{bmatrix} mod \; (256) \tag{10}$$

Where, X_m, Y_n is the position in (m, n) of the pixel in the original image, X_{m+1}, Y_{n+1} is the new position of the pixel, (a, b) are two parameters of the Arnold cat map. In this paper, controllable iterative parameter Arnold cat map is introduced and it can be given as follow:

$$\begin{bmatrix} X_{m+1}^i \\ Y_{n+1}^i \end{bmatrix} = \begin{bmatrix} 1 & a^i \\ b^i & a^i b^i + 1 \end{bmatrix} \begin{bmatrix} X_m^i \\ Y_n^i \end{bmatrix} mod \; (256) \tag{11}$$

The values of "i" represented the iteration number, "a^i, b^i" are the iterative dynamic control parameters used as secret parameters for the proposed CI-ACM and it can be generated as follow.

- *Step* 1. Use the proposed PFMM-CLM-PRNG output $x^F{}_{(n)}$ from Equation (9) to generate the secure iteration number for ACM:

$$i = \sum x_n^F \; mod \; Z + 1 \tag{12}$$

Where, "Z" is the maximum number of iteration.

- *Step* 2. Generate the controllable iterative parameters a^i, b^i for the proposed CI-ACM:

$$a^i = \sum (i * 100) mod \; 80 + 1 \tag{13}$$

$$b^i = (a^i)^2 mod \; 80 + 1 \tag{14}$$

The controllable iterative values of "i, a^i, b^i" also will be a secret parameter for the proposed system which is used in the confusion process to produce the permutated image.

- *Step* 3. The permutated image generated from the proposed CI-ACM will be XORed with the chaotic random numbers x_n^F with size L*K as given in Equation (9) in a diffusion process. The proposed image encryption and decryption mechanism based on PF-MMCLM and CI-ACM is shown in Figure 4.

The decryption process is exactly like the previous encryption procedure but in invert order.

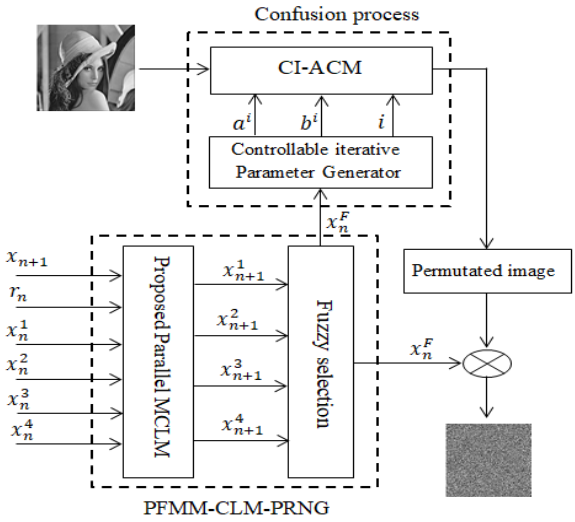


Figure 4. The proposed PFMM-CLM image encryption.

5. Security and Performance Analysis

In this section, the simulation results will be presented to measure the performance of the proposed algorithm including key space analysis, statistical analysis, sensitivity analysis, and differential attack analysis. Matlab 2016a is used to evaluate the encryption and decryption programs. All experiments are performed on a computer with Intel (R) Core(TM) i5-3210, 2.50GHz, RAM 8.00GB. The grey images size is 256*256 for all simulations, the secrete key, and parameters used in all simulations are given in Table 2.

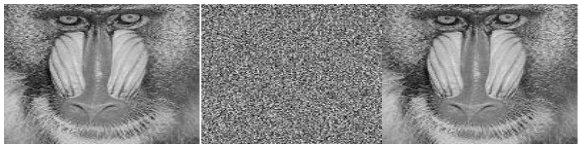
Table 2. Secret keys and simulation parameters.

Initial Values	$x_0 = 0.35715925874180$ $x_0^1 = 0.48729605028420$ $x_0^2 = 0.78259558126530$ $x_0^3 = 0.258946758453370$ $x_0^4 = 0.25894671584570$
Master M-CLM Control parameter	$r_0 = 12.95135785245652$
Dynamic control parameter for PMM-CLM	r_n=10.7630004881250
Arnold Cat Map parameter	$i = 1, a^1 = 9, b^1 = 82$

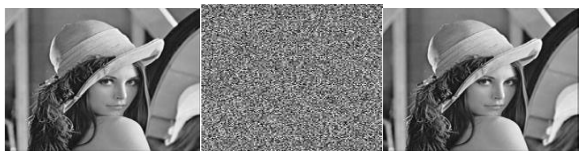
Figure 5 shows the encryption and decryption results of the grey images Baboon, Lena, and Cameraman using Secret keys and simulation parameters given in Table 2.

5.1. Key Space Analysis

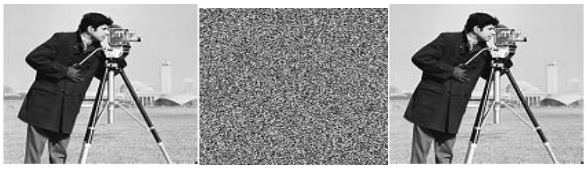
The key space indicates a total number of different keys that can be used in an algorithm [10]. In the proposed algorithm, the secret keys include five initial values ($x_0, x_0^1, x_0^2, x_0^3, x_0^4$) in the range of [0, 1] and two control parameters (r_0,r_n) are valid within 4 to 20, if the length of every initial value or control parameter is set to 14 decimals [14].



a) Encryption and decryption of the grey image Baboon.



b) Encryption and decryption of the grey image Lena.



c) Encryption and decryption of the grey image cameraman.

Figure 5. Encryption and decryption images using secret keys and simulation parameters in Table 2.

The key space of the proposed algorithm is greater than 10^{98}, the results proved that the key space of our algorithm is very large to prevent all types of brute force attacks.

Table 3. Proposed key space analysis compared with other method results.

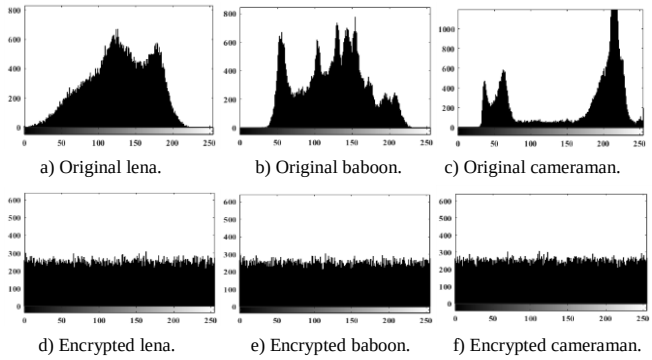
Methods	**Chen *et al*. [4]**	**Huang *et al*. [10]**	**Lan *et al*. [14]**	**Proposed**
Key space	10^{58}	10^{40}	10^{56}	10^{98}

5.2. Statistical Analysis

The effective encryption system is measured by its ability to repel statistical attacks. The statistical analysis of plane images and encrypted images are used to determine the difference between them [15].

5.2.1. Histogram Analysis

The image graph shows the distribution of pixel density values in the image [35]. The pixel distribution of the ciphered images is shown in Figure 6. The encrypted histogram can reduce the correlation between pixel values. Thus, image information can be protected from statistical attack.



a) Original lena. b) Original baboon. c) Original cameraman.

d) Encrypted lena. e) Encrypted baboon. f) Encrypted cameraman.

Figure 6. Histogram analysis of original and encrypted images.

5.2.2. Correlation Analysis

The correlation analysis is used to measure similarities between two adjacent pixels in an image. For the original image, each pixel is strongly correlated with its neighbouring pixels, whether horizontally, vertically, or diagonally, good encryption algorithm can produce an encrypted image with a very small correlation value to resist statistical attacks [16]. The correlation coefficient ρ_{xy} can calculate by the following formula.

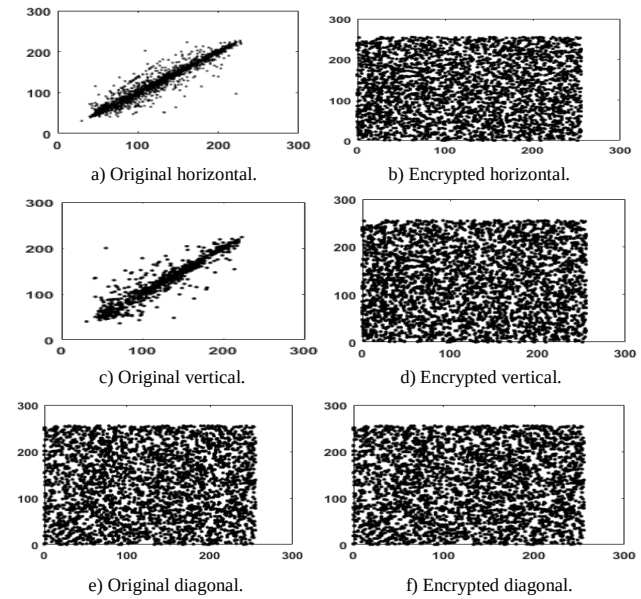
$$\rho_{xy=}\frac{Cov(x,y)}{\sqrt{D(x).D(y)}} \quad (15)$$

$$E_{x=}\frac{1}{N}\sum_{i=1}^{N} x_i \quad (16)$$

$$D_{x=}\frac{1}{N}\sum_{i=1}^{N}(x_i - E_x)^2 \quad (17)$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E_x)(y_I - E_y) \quad (18)$$

Where x and y are the grey scale values of two adjacent pixels in the image, and *N* is the total number of pixels selected from the image, first randomly select 1000 or more pairs of adjacent pixels from both images. The correlation distribution of two adjacent pixels is shown in Figure 7.



a) Original horizontal. b) Encrypted horizontal.

c) Original vertical. d) Encrypted vertical.

e) Original diagonal. f) Encrypted diagonal.

Figure 7. Correlation distribution in the three directions (Horizontal, Vertical, and Diagonal) before and after encryption of Lena image.

According to Equation (15), the results appear the correlation coefficients of the encoded image are near to 0 in all iteration. Table 4 shows that the pixels adjacent to the encoded image have very minimal correlation and that the proposed image encoding scheme has perfect confusion and diffusion characteristics.

Table 4. Correlation coefficients of two adjacent pixels in the original image and encrypted image compared with other method results.

Direction	Horizontal	Vertical	Diagonal
Original Image (Lena)	0.97470	0.95133	0.92766
1-iteration encryption	-0.00501	-0.0012	0.00195
2-iteration encryption	-0.00259	0.00432	0.00186
3-iteration encryption	-0.00273	-0.0029	-0.0001
Kar *et al*. [11]	-0.07600	-0.0034	-0.0074
Lin and Ng [16]	-0.00260	-0.0054	0.00820
Liu and Miao [18]	0.002100	0.00460	-0.0033

5.2.3. Peak Signal-to-Noise Ratio (PSNR)

The similarity between original and encrypted image can be measured by PSNR. High PSNR means a high correlation between original and received image [11], and can be defined as:

$$\text{PSNR}=10log_{10}\frac{M*N*(2^n-1)^2}{\sum_{i=1}^{N}\sum_{J=1}^{M}[I(i,j)-C(i,j)]^2} \quad (19)$$

Where *I(i, j)* is the pixel value in the plane image at pixel point (*i, j*) and *C(i, j)* is the pixel value in cipher image at pixel point *(i, j)*, good encryption represent the low value of PSNR. The result values of encrypted images baboon, Lena, cameraman are shown in Table 5 which clarifies that the proposed algorithm is better than other algorithms.

Table 5. Proposed Peak signal-to-noise ratio compared with other method results.

Image	1-iteration	2-iteration	3-iteration
Baboon	7.744520	7.743574	7.745826
Lena	7.736859	7.750716	7.748231
Cameraman	7.756323	7.745371	7.735761
El-Khamy *et al*.[5]	8.4124	-	-
Kar *et al*. [11]	7.9872	-	-

5.2.4. Entropy Analysis

The randomness of the received image is calculated by using entropy, it represents uncertainty in the cipher image. If the entropy of the encoded image is high, that means high randomness and high confidentiality [15]. The entropy of the information system is defined as

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i)log_2 p(m_i) \quad (20)$$

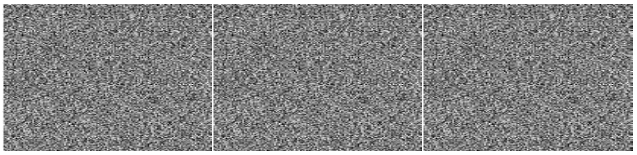
Where *m* is the source of information, N total number of bits represents the symbol m_i,$p_{(mi)}$ probability of symbol m_i, the best value of the information entropy close to the value 8. The information entropy of the cipher-image produced by our algorithm is shown in Table 6, which is near to 8. That means the minimal probability for the attacker to decode a cipher image.

Table 6. Information entropy of cipher-image by the proposed algorithm and references.

Image	1-iteration	2-iteration	3-iteration
Baboon	7.997067	7.997074	7.997471
Lena	7.997268	7.997265	7.996797
Cameraman	7.997414	7.997292	7.996637
Li *et al*.[15]	7.9972	-	-
Tong *et al*. [29]	7.9891	-	-
Xu *et al*. [35]	7.9974	-	-

5.2.5. Key Sensitivity Analysis

A robust encryption system should have a high sensitivity for any minor change in the secret keys [4]. To test the key sensitivity, assume the control parameters and initial values that are used to encrypt plain images $(r_0, x_{0,}, x_0^1, x_0^2, x_0^3, x_0^4)$. After the encryption step, change the key by adding 10^{-14} to any initial condition or control parameter and use it to decode the image. Thus, the key sensitivity test is shown in Figure 8, which proved that the proposed encryption system has highly sensitive to the security key. That means the least modification of the secret keys during the decoding process. The results will be a completely unencrypted image.



a) Decrypted image by the key $+10^{14}$.

b) Decrypted image by the correct key.

Figure 8. Key sensitivity analysis, Decrypted image by the incorrect decryption key are shown in (a), decrypted image by the correct decryption key is shown in (b).

Also, any minor changes in the initial condition cause a total change for controllable iterative parameter value and number of iteration as shown in Table 7.

Table 7. Effect of slightly different keys in controllable iterative values.

Test keys	*i*=1		*i*=2		*i*=3	
	a_1	b_1	a_2	b_2	a_3	b_3
$x_0, r_0, x_0^1, x_0^2, x_0^3, x_0^4$	9	82				
$r_0, x_0^1, x_0^2, x_0^3, x_0^4, x_0 + 10^{-14}$			63	130		
$x_0, x_0^1, x_0^2, x_0^3, x_0^4, r_0 + 10^{-14}$					70	37
$x_0, r_0, x_0^2, x_0^3, x_0^4, x_0^1 + 10^{-14}$			93	202		
$x_0, r_0, x_0^1, x_0^3, x_0^4, x_0^2 + 10^{-14}$	34	133				
$x_0, r_0, x_0^1, x_0^2, x_0^4, x_0^3 + 10^{-14}$			46	69		
$x_0, r_0, x_0^1, x_0^2, x_0^3, x_0^4 + 10^{-14}$					74	101

5.3. Deferential Attack Analysis

Effective image cryptosystem should have a sensibility to plane image and secret key, which means any teeny modification in the plain image, should make a large disturbance in the cipher-image to increase resistance to the differential attack,

Two common tests that were used to examine the sensitivity of the plane image, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI), the ideal values of NPCR and UACI are 99.61% and 33.46% [19].

Consider C_1 and C_2 two cipher images for two plane images p_1 and p_2 which have only one pixel difference, Consider $C_1(i,j)$ and $C_2(i,j)$ is the gray scale pixel values at position (i, j) of two images C_1 and C_2. The NPCR and UACI are defined as:

$$\text{NPCR}=\frac{\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)}{M*N} * 100\% \quad (21)$$

$$\text{UACI}=\frac{1}{M*N}\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|C_1(i,j)-C_2(i,j)|}{2^n-1}*100 \quad (22)$$

Where $D(i,j)$a bipolar array of the same size as the cipher image and is defined as

$$\text{D(i,j)}=\begin{cases}1 \text{ if } C_1(i,j) \neq C_2(i,j)\\ 0 \text{ if } C_1(i,j) = C_2(i,j)\end{cases} \quad (23)$$

The value of the first pixel in the plain images is p_i. It is altered to $p_i = (p_i+100)$ *mod256* with no changing on the other value to get other image and encrypt the two images to evaluate the value of NPCR and UACI of the two encoded images. The results of NPCR and UACI are shown in Table 8. From this table, and the comparison with other systems for Lena image, it can be concluded that the proposed algorithm is more efficient than other algorithms.

Table 8. Result of NPCR and UACI of proposed algorithm and references.

Proposed scheme		Lena.256	Cam. 256	Babbon.256
1-iteration	NPCR	99.627686	99.627686	99.627686
	UACI	33.521154	33.424252	33.507140
2-iteration	NPCR	99.578857	99.578857	99.578857
	UACI	33.454416	33.446554	33.480500
3-iteration	NPCR	99.650574	99.650574	99.650574
	UACI	33.482816	33.516870	33.466378
Liu and Miao [19]	NPCR	99.5500	-	-
	UACI	33.6000	-	-
Lan *et al*. [14]	NPCR	99.6095	-	-
	UACI	33.4623	-	-
Zhou *et al*. [40]	NPCR	99.6098	-	-
	UACI	33.4384	-	-

6. Conclusions

This paper has proposed a new Parallel Fuzzy Multi-Modular Chaotic Logistic Map (PFMM-CLM). The proposed chaotic system used one modular chaotic logistic map as a master map to inject the main parameters for the parallel multi-modular chaotic logistic maps. Also, the fuzzy set theory is used as a fuzzy logic selector to improve chaotic performance. The simulation and performance analysis for the proposed PFMM-CLM show the excellent chaotic properties, such as the robust bifurcation diagram and high Lyapunov exponent value (LE = 30 at control parameter of 20) that can satisfy the wide range of

chaotic parameters. The proposed PFMM-CLM has been evaluated as a Pseudo-Random Number Generator (PRNG) and satisfies all randomness tests. We introduce the image encryption algorithm to investigate the PFMM-CLM's application in image encryption. It is shown to have excellent diffusion and confusion properties. The Simulation results, security analysis, and comparisons for the proposed PFMM-CLM image encryption have been introduced and compared with different algorithms. The results show that our algorithm has an excellent security performance.

References

[1] Bechikh R., Hermassi H., Abd A., and Rhouma R., "Breaking an Image Encryption Scheme Based on A Spatiotemporal Chaotic System," *Signal Process-Image Communication*, vol. 39, pp. 151-158, 2015.

[2] Bisht A., Dua M., and Dua S., "A Novel Approach to Encrypt Multiple Images Using Multiple Chaotic Maps and Chaotic Discrete Fractional Random Transform," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 3519-3531, 2019.

[3] Chai X., Yang K., and Gan Z., "A New Chaos-Based Image Encryption Algorithm with Dynamic Key Selection Mechanisms," *Multimedia Tools Application*, vol. 76, no. 7, pp. 9907-9927, 2017.

[4] Chen J., Zhu Z., Fu C., Zhang L., and Zhang Y., "An Efficient Image Encryption Scheme Using Lookup Table Based Confusion and Diffusion," *Nonlinear Dyn*, vol. 81, no. 3, pp. 1151-1166, 2015.

[5] El-Khamy S., Korany N., and Mohamed A., "A New Fuzzy-DNA Image Encryption and Steganography Technique," *IEEE Access*, vol. 8, pp. 148935-148951, 2020.

[6] Gqaid G. and Talbar S., "Encrypting Image by Using Fuzzy Logic Algorithm," *International Journal of Image Processing and Vision Sciences*, vol. 2, no. 1, pp. 25-29, 2013.

[7] Hikal N. and Eid M., "A New Approach for Palmprint Image Encryption Based on Hybrid Chaotic Maps," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 7, pp. 870-882, 2020.

[8] Hua Z. and Zhou Y., "Dynamic Parameter Control Chaotic System," *IEEE Transaction on Cybernetics*, vol. 46, no. 12, pp. 3330-3341, 2016.

[9] Hua Z. and Zhou Y., "One-Dimensional Nonlinear Model for Producing Chaos," *IEEE Transactions on Circuits and Systems*, vol. 65, no. 1, pp. 235- 246, 2018.

[10] Huang H., Yang S., and Ye R., "Efficient Symmetric Image Encryption By Using A Novel 2D Chaotic System," *IET Image Processing*, vol. 14, no. 6, pp.1157-1163, 2020.

[11] Kar M., Mandal M., Nandi D., Kumar A., and Banik S., "Bit-plane Encrypted Image Cryptosystem Using Chaotic, Quadratic, and Cubic Maps," *Iete Technical Review*, vol. 33, no. 6, pp. 651-661, 2016.

[12] Kang X., Luo X., Zhang X., and Jiang J., "Homogenized Chebyshev-Arnold Map and Its Application to Color Image Encryption," *IEEE Access*, vol. 7, pp. 114459-114471, 2019.

[13] Keshari S. and Modani S., "Image Encryption Algorithm based on Chaotic Map Lattice and Arnold Cat Map for Secure Transmission," *International Journal of Computer Science and Telecommunications*, vol. 2, no.1, pp. 134-139, 2011.

[14] Lan R., He J., Wang S., Gu T., and Luo X., "Integrated Chaotic Systems for Image Encryption," *Signal Processing*, vol. 147, pp. 133-145, 2018.

[15] Li Y., Wang C., and Chen H., "A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation," *Optics and Lasers in Engineering*, vol. 90, pp. 238-246, 2017.

[16] Lin R. and Ng T., "Secure Image Encryption Based on an Ideal New Nonlinear Discrete Dynamical System," *Hindawi*, vol. 2017, pp. 1-12, 2018.

[17] Liu L., Lie Y., and Wang D., "A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation," *IEEE Access*, vol. 8, pp. 27361-27374, 2020.

[18] Liu L. and Miao S., "A New Image Encryption Algorithm Based on Logistic Chaotic Map with Varying Parameter," *Springer Plus*, vol. 289, no. 5, pp. 1-12, 2016.

[19] Liu L. and Miao S., "A New Simple One-Dimensional Chaotic Map and Its Application for Image Encryption," *Multimedia Tools Application*, vol. 77, no. 16, pp. 21445-21462, 2018.

[20] Liu L., Wang D., and Lei Y., "An Image Encryption Scheme Based on Hyper Chaotic System and DNA with Fixed Secret Keys," *IEEE Access*, vol. 8, pp. 46400-46416, 2020.

[21] Luo Y., Yu J., Lai W., and Liu L., "A Novel Chaotic Image Encryption Algorithm Based on Improved Baker Map and Logistic Map," *Multimedia Tools Application*, vol. 78, no. 15, pp. 22023-22043, 2019.

[22] Mondal B., Kumar P., and Singh S., "A Chaotic Permutation and Diffusion Based Image Encryption Algorithm for Secure Communications," *Multimedia Tools*

Application, vol. 77, no. 23, pp. 31177-31198, 2018.

[23] Niu Y. and Zhanga X., "Novel Plaintext-Related Image Encryption Scheme Based on Chaotic System and Pixel Permutation," *IEEE Access*, vol. 8, pp. 22082-22093, 2020.

[24] Nkapkop J., Effa J., Borda M., Bitjoka L., and Mohamadou A., "Chaotic Encryption Scheme Based on a Fast Permutation and Diffusion Structure," *The International Arab Journal of Information Technology*, vol. 14, no. 6, pp. 812-819, 2017.

[25] Pareeka N., Patidar V., and Sud K., "Diffusion-Substitution Based Gray Image Encryption Scheme," *Digital Signal Processing*, vol. 23, no. 3, pp. 894-901, 2013.

[26] Parvaz R. and Zarebnia M., "A Combination Chaotic System and Application in Color Image Encryption," *Optics and Laser Technology*, vol. 101, pp. 30-41, 2018.

[27] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J., and Vo S., *Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology, 2010.

[28] Singh G. and Supriya S., "A Study of Encryption Algorithms (RSA, DES, 3DES And AES) for Information Security," *International Journal of Computer Application*, vol. 67, no. 19, pp. 33-38, 2013.

[29] Tong X., Zhang M., Wang Z., Liu Y., and Ma J., "An Image Encryption Scheme Based on A New Hyper Chaotic Finance System," *Optik*, vol. 126, no. 20, pp. 2445-2452, 2015.

[30] Wang X., Feng L., and Zhao H., "Fast Image Encryption Algorithm Based On Parallel Computing System," *Information Science*, vol. 486, pp. 340-358, 2019.

[31] Wang X. and Zhang H., "A Color Image Encryption with Heterogeneous Bit-Permutation and Correlated Chaos," *Optics Communications*, vol. 342, pp. 51-60, 2015.

[32] We Z., Zhang X., and Zhong X., "Generalized Chaos Synchronization Circuit Simulation and Asymmetric Image Encryption," *IEEE Access*, vol. 7, pp. 37989-38008, 2019.

[33] Wu X., Kan H., and Kurths J., "A New Color Image Encryption Scheme Based on DNA Sequences and Multiple Improved 1D Chaotic Maps," *Applied Soft Computing*, vol. 37, pp. 24-39, 2015.

[34] Wu Y., Zhou Y., and Bao L., "Discrete Wheel Switching Chaotic System and Applications," *IEEE Transaction on Circuits and Systems*, vol. 61, no. 12, pp. 3469-3477, 2014.

[35] Xu L., Li Z., Li J., and Hue W., "A Novel Bit-Level Image Encryption Algorithm Based on Chaotic Maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17-25, 2016.

[36] Ye G. and Wong K., "An Efficient Chaotic Image Encryption Algorithm Based on A Generalized Arnold Map", *Nonlinear Dynamics*, vol. 69, no. 69, pp. 2079-2087, 2012.

[37] Zhang J. and Huo D., "Image Encryption Algorithm Based on Quantum Chaotic Map and DNA Coding," *Multimedia Tools Application*, vol. 78, pp. 16505-16621, 2019.

[38] Zhou Y., Bao L., and Chen C., "Image Encryption Using A New Parametric Switching Chaotic System," *Signal Process*, vol. 93, no. 11, pp. 3039-3052, 2013.

[39] Zhou Y., Bao L., and Chen C., "A New 1D Chaotic System for Image Encryption," *Signal Processing*, vol. 97, pp. 172-182, 2014.

[40] Zhou Y., Hua Z., Pun C., and Chen C., "Cascade Chaotic System with Applications," *IEEE Transaction on Cybernetics*, vol. 45, no. 9, pp. 2001-2012, 2015.

Mahmoud Gad obtained his bachelor's degree in Elec. Eng., Dept. of Comm., Alexandria University, Egypt and is currently enrolled in a master's degree in the Dept. of Information Technology, Faculty of Computers and Information, Mansoura Univ., Egypt. His current research interests include nonlinear dynamics, bifurcation theory, chaos control and synchronization, chaos generation and chaos based cryptography.

Esam Hagras was born in Egypt in 1970. He received the B.Sc. degree in communications Eng. From Alexandria University, and M.Sc. degree in communication from Mansoura Univ., Egypt, in1994 and 2002, respectively, and the Ph.D. degree in Electrical engineering from Alex. University, in 2008. His current research interests are in the areas of nonlinear dynamics, wireless and optical communications, and chaos-based cryptography.

Hasan Soliman received his B.Sc. and M.Sc. degrees in 1983 and 1987 respectively from Faculty of Engineering, Mansoura University, Egypt. Through an Egyptian-funded joint scholarship, he received his PhD degree from Mansoura University with collaboration from a University in German in 1993. His current research interests are in the areas of WSN security, Ad hoc network security, cryptography, multimedia security. He is currently the Dean of Faculty of Computer and Information Sciences, Mansoura University.

Noha Hikal Received her B.Sc. and M.Sc. degrees in Communications Engineering from Mansura University in 1998, 2002 respectively and her Ph.D degree in Multimedia Communications in 2008. And Associated Prof. since 2016 . She currently works as a head of IT Dept., Faculty of Computers and Information Sciences, Mansoura University. She has more than twenty scientific research publications and book chapters. Her research interests include WSN security, Adhoc network security, cryptography, multimedia security, mobile crowed sensing security.