



# Physical Layer Security Based on Cascaded Multi-Modular Chaotic Logistic Map for ML-I-NOMA Image Transmission

Esam A. A. Hagra<sup>1,\*</sup>, Ahmed E. Zein El-Din<sup>2</sup>

**Citation:** Hagra, E. A. A.; Zein El-Din, A. E. *International Journal of Telecommunications, IJT* 2021, Vol. 01, Issue 01, pp. 1-18, December 2021. <https://ijt-adc.org/articles/2805-3044/489749>

**Editor-in-Chief:** Yasser M. Madany

Received: 10-11-2021

Accepted: 13-12-2021

Published: 29-12-2021

**Publisher's Note:** The International Journal of Telecommunications, IJT, stays neutral regarding jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Submitted for possible open access publication under the terms and conditions of the International Journal of Telecommunications, IJT, Air Defense College, ADC, (<https://ijt-adc.org>) and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

<sup>1</sup> Electronics and Communications Dept., Faculty of Eng., Delta University for Science and Technology, Coastal International Road, Gamasa City, Egypt; [esam.hagra@deltauniv.edu.eg](mailto:esam.hagra@deltauniv.edu.eg)

<sup>2</sup> PhD in Electronics and Communications, Giza, Egypt; [a3hzein@yahoo.com](mailto:a3hzein@yahoo.com)

\* Correspondence [esam.hagra@deltauniv.edu.eg](mailto:esam.hagra@deltauniv.edu.eg);

**Abstract:** In this paper, a new cascaded multi modular chaotic logistic map (CMM-CLM) is proposed. The bifurcation diagram for the proposed CMM-CLM is very complex and it has strong chaos properties. The strong chaos leads to a very high Lyapunov exponent values. Based on the proposed CMM-CLM, a new robust physical layer security for the interleaved NOMA based on the multilayers concept (ML-I-NOMA) with the iterative decoder has been introduced. The analysis of the proposed ML-I-NOMA cryptosystem is studied in the both encrypted and non-encrypted image transmission. The main contribution of this paper is to prove that, the different layer effect has a slight performance change compared with the bandwidth consumption. Finally, the simulation results clarified that, the proposed MLI-NOMA achieves 50% and 75% bandwidth efficiency at 2 and 4 layers with an excellent visual quality metric in the correct detection. In addition, the security analysis reveals that, the proposed ML-I-NOMA cryptosystem has large key space and good key sensitivity, and its entropy approaches to the idea value. Hence, the proposed ML-I-NOMA cryptosystem based on the CMM-CLM can strongly resist traditional cipher attacks.

**Keywords:** I-NOMA; Chaotic Map; Encryption; CBC-I Detection; ML-I-NOMA.

## 1. Introduction

Recently, wireless/mobile technology represents a wide spread of communications. Multiple access techniques can widely be categorized into two different approaches [1], namely orthogonal multiple access (OMA) which is an actual choice for developing good performance in terms of system-level throughput and Non-Orthogonal Multiple Access (NOMA). NOMA is a robust radio access technique for the future fifth generation (5G) systems because of its capability to deliver higher spectral efficiency. The current NOMA techniques can generally be divided into two main classes, i.e., power-domain NOMA (PD-NOMA) and code-domain NOMA [2]. NOMA exploits the power domain to full-fill multiple-access strategies, which is different to the classical orthogonal multiple access models, for instance, frequency division multiple access (FDMA) [3]. Some of the NOMA schemes comprises Interleaved Division Multiple Access (IDMA) [4], Pattern Division Multiple Access (PDMA) [5], Sparse Code Multiple Access (SCMA) [6], Resource Spread Multiple Access (RSMA) [7]. IDMA is a distinctive type of Code Division Multiple Access (CDMA) as the receiver distinguishes each station (STA) depending on its unique interleaving patterns instead of unique spreading codes, this gains a developed spectral efficiency and insensitivity to clipping distortion. Within several NOMA structures IDMA is believed to provide more advantages [8]. The PDMA pattern describes the transmitted data mapping to a resource group that can comprised of frequency, time, and spatial resources or any combination of these resources [9].

SCMA reflects a hybrid of CDMA and OFDMA techniques. In SCMA, the coded patterns of various data layer are directly mapped to the code words related to the corresponding codebook set in the time and frequency domain. In this scenario, the several data streams can share the same time-frequency resources of the signal [10]. RSMA employs the low cross-correlation characteristics of extended pseudo-random scrambling codes. Really, after the descrambling, the signal to interference power ratio is proportional to the scrambling-code length. Multi-carrier RSMA is used in the downlink access for the receiver complexity simplification in the frequency-selective wireless fading channels. RSMA also can be expanded to multiple layers. Considering the layers as virtual users, data is partitioned into several parallel layers for each user, so the multi-layer RSMA scenario is more complex than the single-layer RSMA scenario [11].

On the other hand, code-domain NOMA can be categorized into numerous multiple access paradigms that depending on low-density spreading and sparse code multiple access. Related multiple access schemes are: multi-user shared access, lattice-partition multiple access, and pattern-division multiple access. Modern researches demonstrate that NOMA has the prospective to be used in different fifth generation (5G) communication scenarios, comprising the Internet-of-Things (IoT) and Machine-to-Machine (M2M) communications. Furthermore, there are some existing evidence of performance improvement when NOMA is combined with several effective wireless communications systems, such as multiple-input multiple-output (MIMO), cooperative communications, space-time coding, beam forming, full-duplex and network coding, etc. As the NOMA principle, it can manage a wide range of users to be superimposed on the same resource, this leads to systems interference [12]. A special form of superposition modulation [13] is IDM concept, which is presented as an efficient bandwidth scheme. The most important IDM key structures are: Gaussian-like signal pattern, layer structure provide multi-level data processing as well as appropriate data-rate adjustment/adaptive modulation, and no orthogonality. The Peak to Average Power Ratio (PAPR) problem is one of the most significant IDM drawbacks, especially with increasing the IDM layers. Similarly, OFDMA and CDMA schemes have the same PAPR concern [13]. Spreading and interleaving are essential components in system design. Spread Spectrum techniques (SS) generates a transmitted spectrum much larger than the required minimal bandwidth. SS advantages are: resistant against multipath distortion, high flexibility, simple frequency design, adaptive transmission rate, and immunity to interference [14].

Interleavers are essential in I-NOMA as interleaving process, which is considered a layer specific separation to randomize the burst errors [15]. Many interleavers types are presented, random interleavers are used to scramble different users' data with randomized patterns. Due to data scrambling, channel burst error is randomized at the receiver side. In [16] random permutation in the randomization process is applied, the received data is re-ordered based on a series of generated permute indices that produces pseudo-random permutation of given memory addresses related to the pseudo-random order of memory addresses. Because of the random interleavers are used for user separation, then considerable bandwidth and a lot of memory space required for transmission of all these interleaver as well as increased computational complexity at receiver ends. Turbo-type Iterative Detection (ID) has been widely investigated for interference mitigation. A turbo process comprises two major functions: an elementary multi-layer detector and a bank of correlations based on soft-in-soft output detection [17].

As the secure transmission of digital images is facing huge challenges, digital image encryption is considered an attractive research area. There are various types of encryption algorithms, each developed for a certain purpose. When existing algorithms become vulnerable, new ones are created. Some of the most well-known cryptographic algorithms are, Data Encryption Standard (DES), 3DES, Advanced Encryption (AES), Twofish encryption and RC4 [18]. Some recent encryption approaches are known to be unreliable for image cyphering [19]. Chaos based encryption depending on the sensitivity to control parameters and initial condition is intrinsic in chaotic approaches to achieve the security demands [20]. The chaos structure presented in [21] has two steps of diffusion and confusion processes.

There are two types of chaotic maps, one dimensional and higher dimensional chaotic maps. The 1-D chaotic maps such as a logistic map, Tent map, Sine map that have a single variable over discrete steps in time [22, 23]. 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 [24,25]. 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 [26, 27], but they have high-computing costs and difficult to implement in hardware which means it is not real-time processing [28,29]. To overcome the limitation of the one-dimension chaotic maps. The authors in [28, 29] introduce a new 1-D chaotic system for image encryption based on the modular one concept to improve the range of the control parameters. Zhou et. al [30] 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 et.al [31] 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. In this research, ML-I-NOMA Physical Layer Security Based on High Lyapunov Exponent Chaotic Encryption is proposed for Image Transmission is presented. Different standard grey scale test images are used. Image pixels are converted into binary data format and equally divided into layers. Convolutional coding is used as a forward error correction. The coded data sequence is mapped onto the Binary Phase Shift Keying (BPSK) modulated symbols which is considered over wireless communication channel with equal power allocation using a non-linear PA, Rapp model. A simple CBC-ID is applied. The proposed system performance clarity investigation is tested under AWGN channel effect. Also, statistical and security analysis include histogram analysis, adjacent pixel correlation analysis, Key space analysis, NPCR and UACI tests. The suggested ML-INOMA system has been studied and analyzed from three points of view: the system performance, the bandwidth efficiency and security. First, the proposed ML-INOMA system performance is studied in AWGN channel with several number of layers and different iterations number with HPA Rapp model effect.

This paper is organized as follows: the proposed CMM-CLM is investigated and analyzed in section 2. The proposed ML-I-NOMA is presented in section 3. The performance evaluation of the suggested ML-I-NOMA system is depicted in section 4, the security analysis of the encrypted ML-I-NOMA is introduced in section 5. Finally, the conclusions are introduced in section 6.

## 2. Proposed Cascaded MM-CLM

In this section, the proposed system will utilize the simple 1-D chaotic logistic map to present a new CCS capable of achieving a complex bifurcation diagram and high large Lyapunov Exponent value. The single chaotic logistic map can be computed as follow:

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

The control parameters  $r \in [0, 4]$ ,  $n$  is the iteration number,  $x_{n+1}$  is the interval  $[0, 1]$ . From equation (1) it can be designed the proposed CMM-CLM with four 1D modular chaotic logistic map as given in equation (2).

$$x_{n+1} = F_4 \left( F_3 \text{ mod } 1 (F_2 \text{ mod } 1 (F_1 \text{ mod } 1)) \right) \text{ mod } 1 \quad (2)$$

The modular operation used in equation (2) improved the control parameter by increasing the non-linearity. The bifurcation diagram and LE values of the non-modular logistic map are shown in Figure 1. It presents the limitation of the control parameters which started from 0 to 4 and large negative LE values. The modular function performs an iterative folding process, thus producing uncorrelated random data.

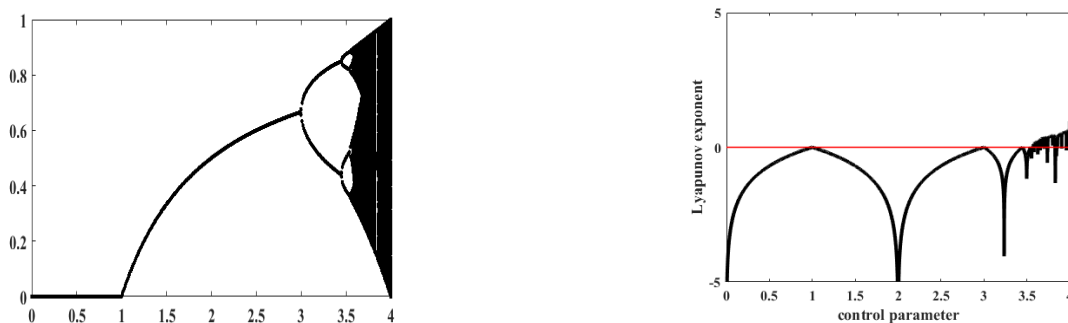


Figure 1. The bifurcation diagram and LE for Non-cascaded-Non-modular CLM.

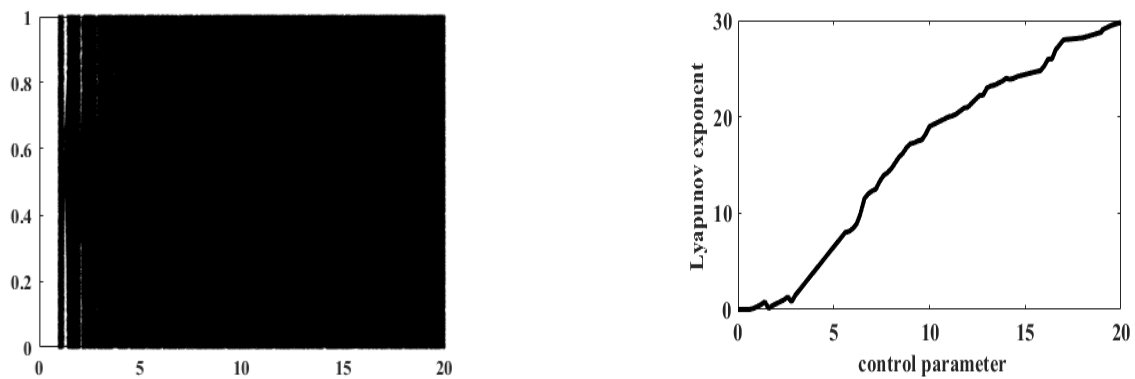


Figure 2. The bifurcation diagram and Lyapunov exponent for the proposed CMM-CLM.

The proposed CMM-CLM has appositve LE values for all control parameters from 4 to 20 as shown in Figure 2. In the proposed cascaded map, four cascaded modular chaotic logistic maps are used to achieve more complex bifurcation diagram and high Lyapunov exponent.

### 3. Proposed Secure ML-I-NOMA system

In this section, we assumed the transmitter and the receiver has the correct key. IDM has been inspected by many authors [1-3], [5, 7]. The proposed ML-I-NOMA transmitter structure is presented in Figure 3. The grey scale test image is transformed into binary format. Using layered IDM concept, the input data,  $d$  is equally partitioned into  $k$  layers/sub-sequences,  $\{k = 2^n, n = 1, 2, 3, \dots\}$ , each layer can be written as:  $\{d = d^1, \dots, d^k, k = 1, 2, \dots, K\}$ . Convolutional coding is used as a foreword error correction technique with a code rate ( $R = 1/2$ ), the resultant coded sequence can be formulated as  $\{C = C^1, \dots, C^k, k = 1, 2, \dots, K\}$ . Spreading process is applied to each coded sub-sequence utilizing the same balanced spreading code  $S$  for all layers,  $S^k \in \{+1, -1\}$ . The produced chip sequence is formulated as:  $\{S_j^k, j = 1, 2, \dots, J\}$ , where,  $J = N \times S$  is the frame length. A unique chip layered random interleavers are utilized to distinguish layer data sequence  $\{\pi_j^k, k = 1, 2, \dots, K\}$ , to generate interleaved chip layered data sequences  $\{I_j^k, k = 1, 2, \dots, K\}$ . The interleaved chips layered data sequences are mapped onto the modulated symbols,  $\{x_j^1, \dots, x_j^k\}, x_j^k \in \{+1, -1\}$  which are BPSK constellation elements.

For the encryption, two processes: the confusion and diffusion processes are used in order to permute the pixel positions and pixel values change, respectively. The proposed CMM-CLM is used to generate four different matrices of size  $(M/4, N/4)$  for each part of the image of size  $(M, N)$  and the values in the four matrices are in the range of  $[1, 256]$ . The four matrices are used to satisfy the diffusion processes in the encryption step. Also, based on the proposed CMM-CLM, different four confusion matrices of length  $(1, 2 \times M \times N)$  are generated to convert the all of the four interleavers in each layer to secure interleavers.

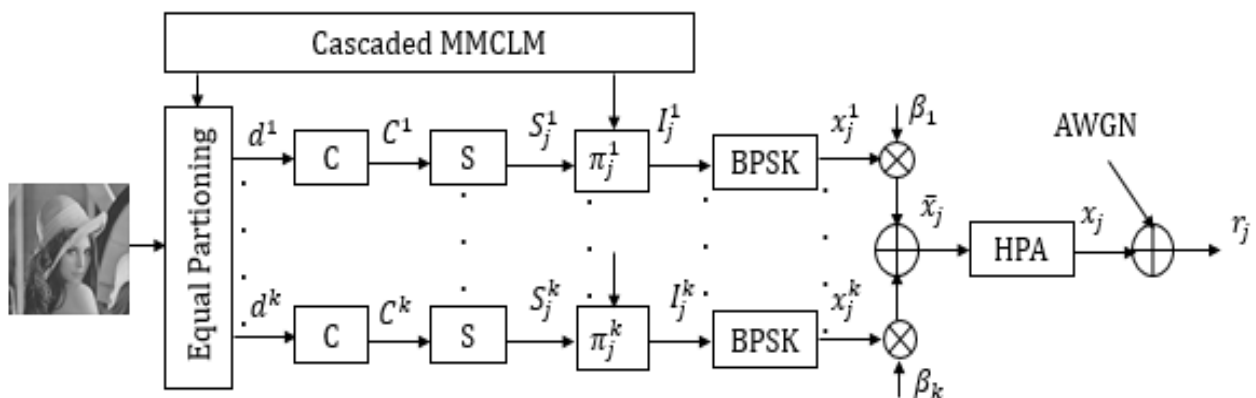


Figure 3. ML-I-NOMA Transmitter structure

The detailed encryption steps of the proposed scheme are described as follows:

1. Read the plain image and divided it into four sub-images of size  $(M/4, N/4)$ .
2. Use the proposed CMM-CLM to generate four different diffusion matrices of size  $(M/4, N/4)$  and the values in the four matrices are in the range  $[1, 256]$  by using equation (3) with different four initial conditions  $x_0^1, x_0^2, x_0^3, x_0^4$  and different four control parameters  $r^1, r^2, r^3, r^4$ .

$$x_{n+1}^{\frac{M}{4} \times \frac{N}{4}} = (F_4 (F_3 \text{ mod } 1 (F_2 \text{ mod } 1 (F_1 \text{ mod } 1))) \text{ mod } 1) \times 10^8 \text{ mod } 256 \tag{3}$$

3. For the diffusion process, Xor the four matrices of size  $(M/4, N/4)$  with the four sum images to produce four diffused sum images  $d^1, d^2, d^3, d^4$
4. After coding and spreading, use the proposed CMM-CLM to generate four different confusion matrices of size  $(1, M/2 \times N/2)$  called  $w^1, w^2, w^3, w^4$  with different four initial conditions  $x_0^5, x_0^6, x_0^7, x_0^8$  and different four control parameters  $r^5, r^6, r^7, r^8$  in order to produces different four secret keyed interleavers  $\pi^1, \pi^2, \pi^3, \pi^4$ .

The resultant signal  $\bar{x}_j$  is a linear superposition of distinct symbol as shown:

$$\bar{x}_j = \sum_{k=1}^K \beta_k \times x_j^k \tag{4}$$

The signal,  $\bar{x}_j$  is amplified as given in [9], Rapp model is utilized for modeling memory-less HPA behavior models for the proposed ML-I-NOMA system, the HPA output,  $x_j$ , is written as:

$$\bar{x}_j(t) = A(t) \cos (\omega_c t + \varphi(t)) \tag{5}$$

$$x_j(t) = F[A(t)] \cos [\omega_c t + \varphi(t) + \Psi(A(t))] \tag{6}$$

where,  $F[A(t)], \Psi[A(t)]$  are the gain distortion function that characterizes the Amplitude to Amplitude transfer characteristics (AM/AM), and the phase distortion function that characterizes Amplitude to Phase transfer characteristics (AM/PM), of the HPA non-linearity, which are given by:

$$AM/AM: F[A(t)], x_j = \frac{\bar{x}_j}{\left( (1 + \bar{x}_j/v_{sat})^{2r} \right)^{1/2r}} \tag{7}$$

$$AM/PM: \Psi(A(t)) = 0 \tag{8}$$

$\bar{x}_j, x_j$  are the input signals voltage and output signals voltage respectively,  $v_{sat}$  is the amplifier input saturation voltage,  $r$ , is called "knee factor". As the value of  $r$  increases, the HPA approaches the limiter model [22].

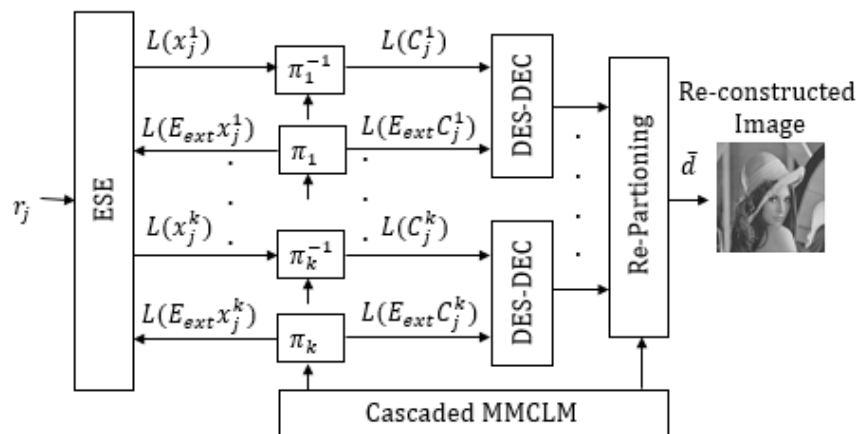


Figure 4. CBC-ID for ML-I-NOMA Receiver

The following detection principle is developed based on IDMA [9]. An iterative CBC-ID is employed to mitigate the multiple access interference and the channel fading. The receiver is supposed to have complete knowledge of the channel state information. Iteratively, the received signal is processed, as there are great numbers of interference terms, even after the last iteration, the Gaussian approximation is still valid. The CBC iterative detection, in Figure 4, constructed from an Elementary Signal Estimator (ESE) and a bank of  $k$  single layer A Posteriori Probability (APP) detectors for the De-Spreading operation (DES) working in turbo type manner [16]. The DES achieves a coarse CBC estimation.

Firstly, for decryption steps:

1. The receiver generates the same different four secret keyed interleavers  $\pi^1, \pi^2, \pi^3, \pi^4$  by using the proposed CMM-CLM with the same initial conditions and the same control parameters.
2. Using the proposed CMM-CLM to generate four different diffusion matrices of size  $(M/4, N/4)$  and the values in the four matrices are in the range  $[1, 256]$ , by using equation (3) with the same initial conditions and the same control parameters and using it till the final step in the re-partitioning process to decrypt the four sub images.

Secondly, for data recovery step, at time instant  $j$ , the received signal can be expressed as:

$$r_j = F \left[ \sum_{k=1}^K \beta_k \times x_j^k \right] + \xi_j^k, \quad j = 1, 2, \dots, J \quad (9)$$

where,  $r_j$  signified the user received data symbols at time instant  $j$ , and  $\xi_j^k$  zero mean AWGN with variance  $\sigma^2 = N_0/2$ . For simplicity, we consider real  $\beta_k$  only, however, the result can be easily applied to quadrature channels [2]. Suppose that  $\beta_k$  have a priori knowledge at the receiver side. The expression  $\xi_j^k = r_j - \beta_k x_j^k$ , denotes a distortion term w.r.t.,  $x_j^k$ .  $x_j^k$  is considered as a random variable with mean  $E(x_j^k)$  and variance  $Var(x_j^k)$ . The initial value for mean  $E(x_j^k)$  is "0" and the initial value for variance  $Var(x_j^k)$  is "1".

$$E(r_j) = \sum_{k=1}^K \beta_k \times E(x_j^k) \quad (10a)$$

$$Var(r_j) = \sum_{k=1}^K |\beta_k| Var(x_j^k) + \sigma^2 \quad (10b)$$

Using the central limit theorem (CLT),  $\xi_j^k$  can be approximated by a Gaussian random variable with:

$$E(\xi_j^k) = E(r_j) - \beta_k E(x_j^k) \quad (11)$$

$$Var(\xi_j^k) = Var(r_j) - |\beta_k|^2 Var(x_j^k) \quad (12)$$

The ESE produces the Logarithm Likelihood Ratio (LLRs) about  $\{x_j^k\}$  calculated as:

$$L(x_j^k) = \log \left( \frac{Pr(x_j^k) = +1|r_j}{Pr(x_j^k) = -1|r_j} \right) = \log \left( \frac{\exp \left( -\frac{(r_j - E(\xi_j^k) - \beta_k)^2}{2Var(\xi_j^k)} \right)}{\exp \left( -\frac{(r_j - E(\xi_j^k) + \beta_k)^2}{2Var(\xi_j^k)} \right)} \right) = \frac{2\beta_k (r_j - E(\xi_j^k))}{Var(\xi_j^k)} \quad (13)$$

For the layer  $k$ , the ESE outputs  $L(x_j^k, j = 1, 2, \dots, J)$ , are de-interleaved to form  $L(C_j^k, j = 1, 2, \dots, J)$ , and forwarded to the DSE-DEC for layer  $k$ . The DES-DEC achieves a soft in soft out CBC process. Straightforward, we concentrate on the chip associated with  $d_1^k$ , the first bit of layer  $k$ . It is assumed that,  $L(C_j^k)$  are uncorrelated because of interleaving process [13]. Let the interleaving for layer  $k$  be written as  $\pi_j^k = j$ , i.e.,  $C_j^k = x_j^k$ . Then A posteriori LLR for  $d_1^k$  can be calculated using  $L(C_j^k)$  as:

$$L(d_1^k) = \log \left( \frac{\Pr(d_1^k = +1|r)}{\Pr(d_1^k = -1|r)} \right) = \log \left( \frac{\prod_{j=1}^S \Pr(C_j^k = S_j^k | r_j)}{\prod_{j=1}^S \Pr(C_j^k = -S_j^k | r_j)} \right) = \sum_{j=1}^S \log \frac{\Pr(C_j^k = S_j^k | r_j)}{\Pr(C_j^k = -S_j^k | r_j)} \quad (14)$$

$$L(d_1^k) = \sum_j^S S_j^k \times L(C_j^k) \quad (15)$$

The Extrinsic LLRs  $\{Ext(C_j^k)\}$  create the output of the DES-DEC and fed back to the ESE after interleaving. In the next iteration,  $\{Ext(x_j^k)\}$  are used to update  $\{E(x_j^k)\}$  and  $\{Var(x_j^k)\}$  as [17].

$$E(x_j^k) = \left( \frac{\exp(Ext(x_j^k)) - 1}{\exp(Ext(x_j^k)) + 1} \right) = \tanh \left( \frac{Ext(x_j^k)}{2} \right) \quad (16)$$

$$Var(x_j^k) = 1 - E(x_j^k)^2 \quad (17)$$

Iterative operation is repeated a certain number of times until a pre-defined termination criterion is satisfied. Finally, the DES-DEC of Figure 4, which denotes the original information bits, is subjected to a soft/hard decision which is re-segmented to re-construct the transmitted image.

#### 4. Proposed ML-I-NOMA simulation results

In this section, the correct decryption case study is assumed, so the performance of the proposed BW efficient ML-I-NOMA for wireless AWGN channel system is evaluated. The test images of size  $(256 \times 256)$  is transformed into binary data sequence  $d \in \{0,1\}$ , and then, equal portioning is applied into  $k$  layers, ( $k = 2^n, n = 1, 2, 3$ ), the same spreading code is applied for each layer, it carries ( $S = 16$ ) balanced spreading sequence,  $S^k \in \{+1, -1, +1, -1, \dots\}$ . The iterations number for the CBC-ID receiver was set to ( $Iter = 3$ ).

The Simulation parameters for the proposed system are summarized below in Table 1. The Key Performance Indicators (KPI) for the suggested ML-I-NOMA system uses Peak Signal to Noise Ratio (*PSNR*) as a visual quality test of the re-constructed image compared to the original transmitted image, and the Bit Error Rate (*BER*) which assesses the full end to end performance of a system including the transmitter, receiver and the medium between them.

KPIs are presented in the form  $E_b N_0$  vs. *BER*, and  $E_b N_0$  vs. *PSNR*. The *PSNR* values of the received image are calculated for different  $E_b N_0$  values from 0 to 16 dB in 2 dB steps. The *BER* is defined as:

$$BER = \frac{\text{Number of bit errors}}{\text{Total number of transferred bits}} \quad (18)$$

Also, the *PSNR* is defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2 \times (M \times N)^2}{\sum_{m=1}^M \sum_{n=1}^N (f(m,n) - f'(m,n))^2} \quad (19)$$

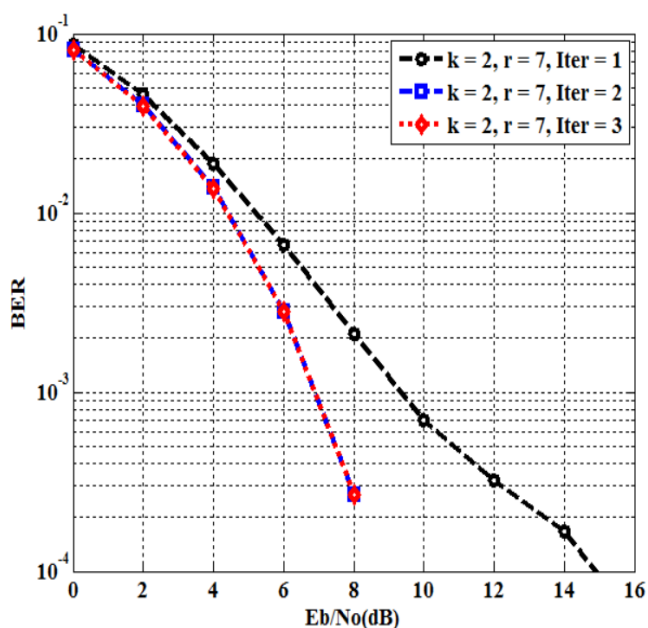
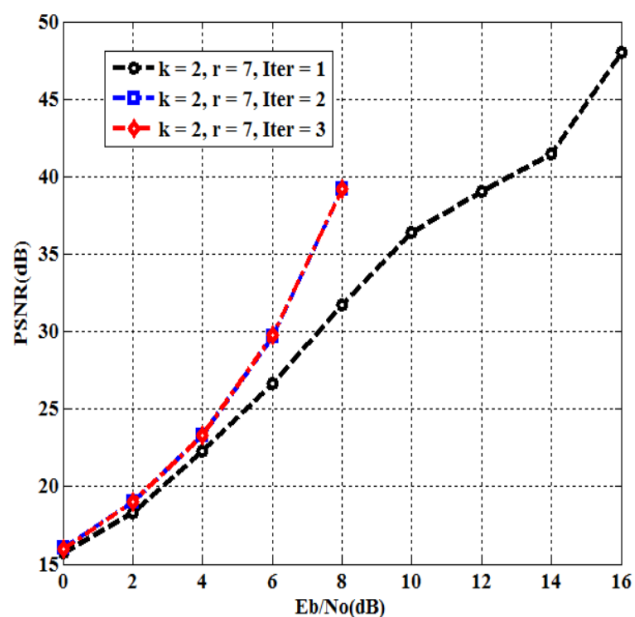
where,  $f(m,n)$  is the original test image pixel,  $f'(m,n)$  is the received image pixel values, and  $(M \times N)$  is the image size.

Firstly, studying the effect of iteration numbers ( $Iter = 1, 2, 3$ ) for different number of layers ( $k = 2^n, n = 1, 2$ ) with HPA at smoothness factor value ( $r = 7$ ), to obtain an exact iteration number value that utilized along with the proposed ML-I-NOMA system.

Figures 5 and 6 show the performance of ML-I-NOMA at variant iteration number, for  $n = 1 \rightarrow k = 2$  layers,  $E_b N_0 = 8$  dB, and  $Iter = 1$ . As depicted in Figures 5 and 6, the *BER* is 0.0021 and *PSNR* performance is 31.71 dB. The same *BER* and *PSNR* performance is gained for  $Iter = 2, 3$  iterations, where the *BER* performance is  $2.67 \times 10^{-4}$  and *PSNR* is 39.19 dB, the outcomes clarify that, the *BER* performance is enhanced by 0.0018 and *PSNR* is improved by 7.48 dB compared to single iteration scenario.

Table 1. System simulation parameters

Parameter	Value
Image size	$128 \times 128$
Layers ( $k$ )	$k = 2^n, n = 1, 2, 3$
Interleaver type ( $\pi$ )	Random
Spread length ( $S$ )	$16, \in \{+1, -1\}$
Modulation type	BPSK
Smoothness factor value ( $r$ )	3, 5, 7
Channel model	AWGN
Iteration ( $Iter$ )	1, 2, 3
Detection type	CBC-ID
Key Performance Indicators (KPI)	
	$E_b N_0$ vs. BER
	$E_b N_0$ vs. PSNR

Figure 5. BER performance, ( $k = 2, r = 7, Iter = 1, 2, 3$ ).Figure 6. PSNR performance, ( $k = 2, r = 7, Iter = 1, 2, 3$ )

Figures 7 and 8 display the ML-I-NOMA performance at variant iteration number, for  $n = 2 \rightarrow k = 4$  layers,  $E_b N_0 = 8$  dB, and  $Iter = 1$ . As presented in Figure 7 and Figure 8, the BER performance is 0.0124 and PSNR performance is 23.9562 dB. Approximately, the same BER and PSNR performance is found for  $Iter = 2, 3$  iterations. For  $Iter = 2$ , the BER performance is  $7.4005 \times 10^{-4}$  and PSNR is 34.778 dB. For  $Iter = 3$ , the BER performance is  $8.3923 \times 10^{-4}$  and PSNR is 34.9193 dB. So, for ( $Iter = 3$ ), the performance shows that: the BER performance is developed by 0.0116 and  $1.5260 \times 10^{-5}$ , and, PSNR is enhanced by 10.9631 and 0.1405 dB compared to ( $Iter = 1, 2$ ) respectively. Then,  $Iter = 3$  is the chosen value to be used with the suggested ML-I-NOMA system. On the other hand, results in Table 2 are plotted in Figures 8 and 9.



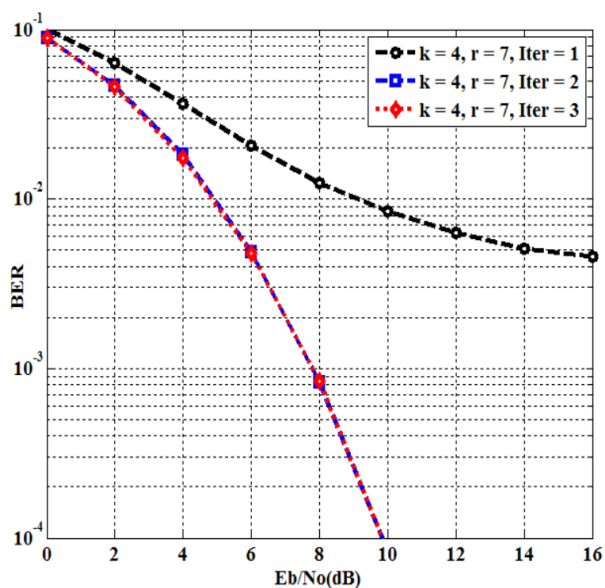


Figure 7. BER performance, ( $k = 4, r = 7, Iter = 1, 2, 3$ ).

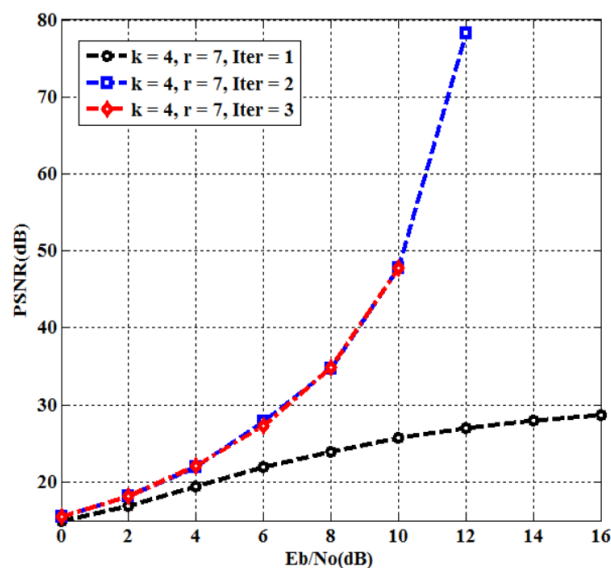


Figure 8. PSNR performance, ( $k = 4, r = 7, Iter = 1, 2, 3$ ).

Table 2. KPI for ML-I-NOMA, ( $k = 2, 4, r = 7$  at  $E_bN_0 = 8 \text{ dB}, Iter = 3$ ) with HPA

		Layers ( $k$ )	2	4
		Knee Factor ( $r$ )	7	
		Iteration ( $Iter$ )	3	
$E_bN_0$ (dB)	0	BER	0.0810	0.0896
		PSNR (dB)	16.0021	15.4332
	2	BER	0.0396	0.0463
		PSNR (dB)	19.0237	18.1972
	4	BER	0.0137	0.0175
		PSNR (dB)	23.3298	22.1234
	6	BER	0.0028	0.0048
		PSNR (dB)	29.7424	27.3216
	8	BER	$2.67 \times 10^{-4}$	$8.39 \times 10^{-4}$
		PSNR (dB)	39.1987	34.9193
	10	BER	0	$8.39 \times 10^{-5}$
		PSNR (dB)	Inf.	47.7911
12	BER	0	0	
	PSNR (dB)	Inf.	Inf.	

The presented results in Figure 9 and Figure 10 clarify that, for  $E_bN_0 = 10 \text{ dB}$ , the BER performance for  $k = 2$  layers refers to "0" in a received image with-no error thus with-no alteration and the PSNR performance refers to "Inf", while for  $k = 4$  layers, the BER is  $8.39 \times 10^{-5}$ , and the PSNR performance is 47.7911 dB. For  $E_bN_0 = 12 \text{ dB}$ , the BER performance for  $k = 2, 4$  layers refers to "0" and the PSNR performance refers to "Inf" according to the comparison over AWGN channel at ( $Iter = 3$ ).

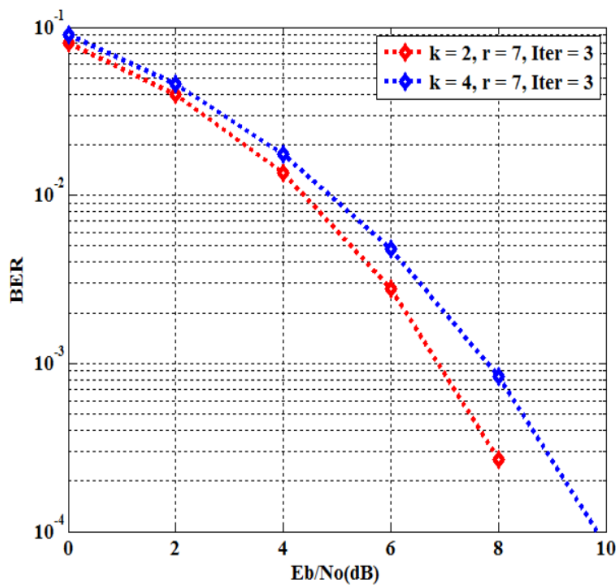


Figure 9. BER, ( $k = 2, 4, r = 7, Iter = 3$ ).

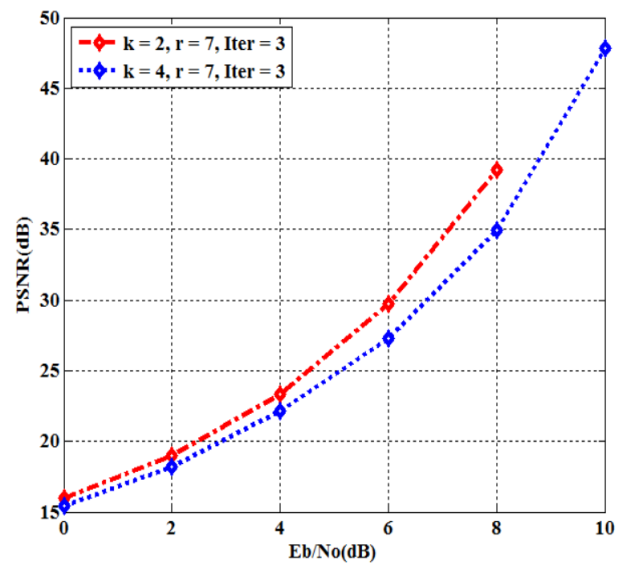


Figure 10. PSNR, ( $k = 2, 4, r = 7, Iter = 3$ ).

Secondly, studying the HPA control parameter (smoothness factor value) effect ( $r = 5, 7, 10$ ) is examined for various number of layers ( $k = 2^n, n = 1, 2$ ) under  $Iter = 3$  to determine an accurate value of  $r$  that employed for the proposed ML-I-NOMA system. For  $n = 1 \rightarrow k = 2, Iter = 3$  case study, Figure 11 and Figure 12 display the effect of different smoothness factor values ( $r = 5, 7, 10$ ) for non-linear HPA Rapp model on the proposed ML-I-NOMA system performance.

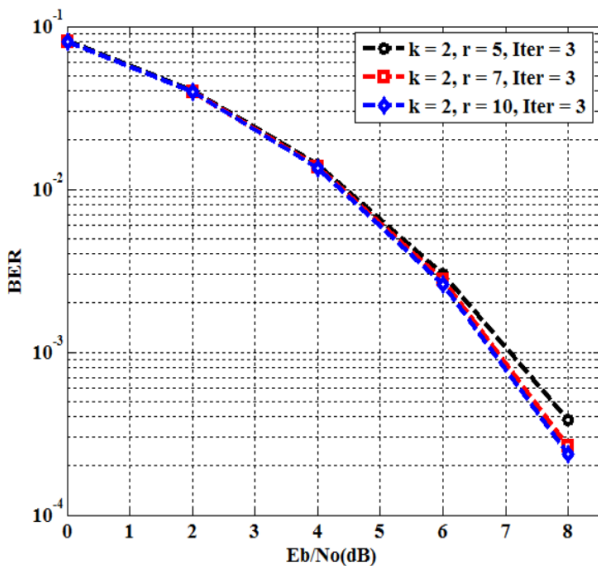


Figure 11. BER, ( $k = 2, r = 3, 5, 7, Iter = 3$ ).

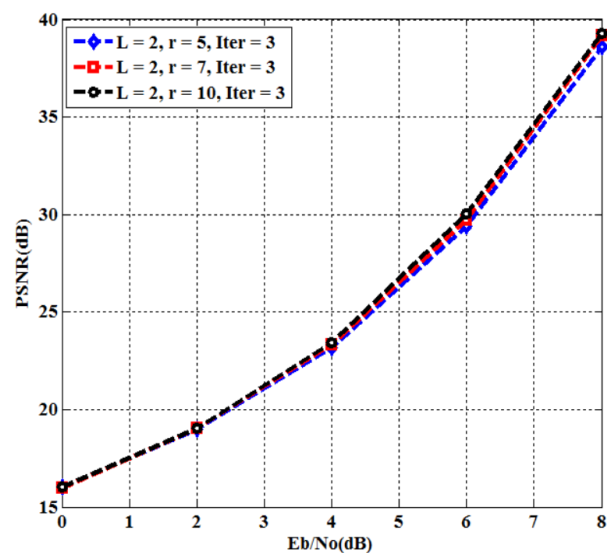


Figure 12. PSNR, ( $k = 2, r = 3, 5, 7, Iter = 3$ ).

At  $E_b N_0 = 8 \text{ dB}$ ,  $Iter = 3$  for  $r = 5$  the BER value is  $3.8147 \times 10^{-4}$ , PSNR value is  $38.5964 \text{ dB}$ , for  $r = 7$  the BER is  $2.6703 \times 10^{-4}$ , PSNR is  $39.1987 \text{ dB}$  and for  $r = 10$  the BER is  $2.3651 \times 10^{-4}$  and PSNR is  $39.2792 \text{ dB}$ . So, for ( $r = 10$ ) the performance clarifies that: the BER is enhanced by  $1.4496 \times 10^{-4}$ ,  $3.0520 \times 10^{-5}$  and, the PSNR is developed by  $0.6828 \text{ dB}$  and  $0.0805 \text{ dB}$  compared to ( $r = 5, 7$ ) scenario, respectively.

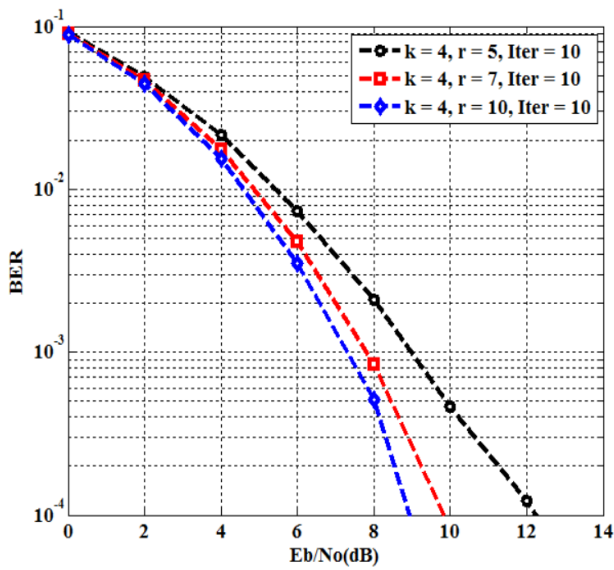


Figure 13. BER, ( $k = 4, r = 5, 7, 10, Iter = 10$ ).

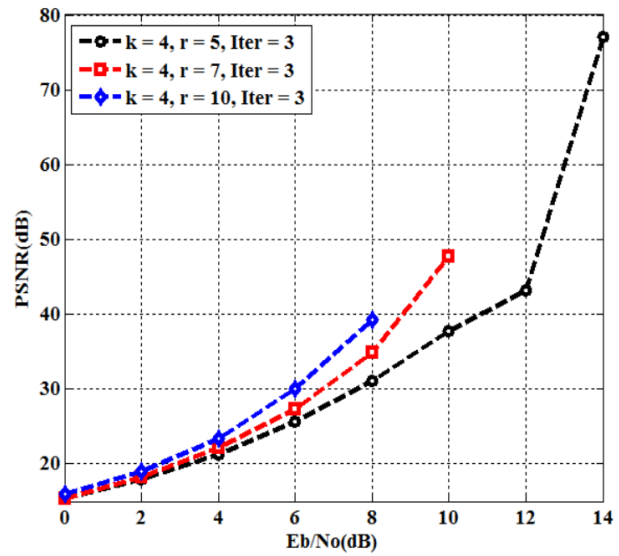








Figure 14. PSNR, ( $k = 4, r = 5, 7, 10, Iter = 3$ ).

For  $n = 2 \rightarrow k = 4, Iter = 3$  scenario, Figures 13 and 14 display the effect of different values of ( $r = 5, 7, 10$ ) for non-linear HPA Rapp model on the suggested ML-I-NOMA system evaluation. At  $E_b N_0 = 8 \text{ dB}$ ,  $Iter = 3$  for  $r = 5$  the BER performance is  $0.0021$ , PSNR is  $31.1195 \text{ dB}$ , for  $r = 7$  the BER performance is  $8.3923 \times 10^{-4}$ , PSNR is  $34.9193 \text{ dB}$  and for  $r = 10$  the BER evaluation is  $5.1117 \times 10^{-4}$  and PSNR is  $39.2792 \text{ dB}$ . As the result, for the chosen smoothness factor value ( $r = 10$ ) based on that: the BER evaluation is developed by  $0.0016$  and  $3.2806 \times 10^{-4}$ , and, the PSNR performance is enhanced by  $8.1597 \text{ dB}$  and  $4.3599 \text{ dB}$  compared to ( $r = 5, 7$ ), respectively.

Table 3. BER & PSNR performance for, ( $k = 2, 4, r = 5, 7, 10$  at  $E_b N_0 = 8 \text{ dB}, Iter = 3$ ).

$r$	5	7	10
$Iter$	3		
$k$	2		
KPI at $E_b N_0 = 8 \text{ dB}$			
BER	$3.8147 \times 10^{-4}$	$2.6703 \times 10^{-4}$	$2.3651 \times 10^{-4}$
PSNR	$38.5964 \text{ dB}$	$39.1987 \text{ dB}$	$39.2792 \text{ dB}$
$k$	4		
KPI at $E_b N_0 = 8 \text{ dB}$			
BER	$0.0021$	$8.3923 \times 10^{-4}$	$5.1117 \times 10^{-4}$
PSNR	$31.1195 \text{ dB}$	$34.9193 \text{ dB}$	$37.3068 \text{ dB}$

Results in Table 3 show the standard grey scale Lena image transmission with the proposed ML-I-NOMA system. The obtained findings provide an overview of the smoothness factor's performance effect at  $E_b N_0 = 8 \text{ dB}$ , for  $k = 2, 4$  layers represented by BER and PSNR. As the high cost of spectrum is a challenging task. The concept

of the suggested ML-I-NOMA is structured on equal layer Partitioning for input data sequence. The proposed ML-I-NOMA system design trade-off can be found in: as the number of layers is increased, it leads to BW consumption compared with a minor performance degradation in system reliability.

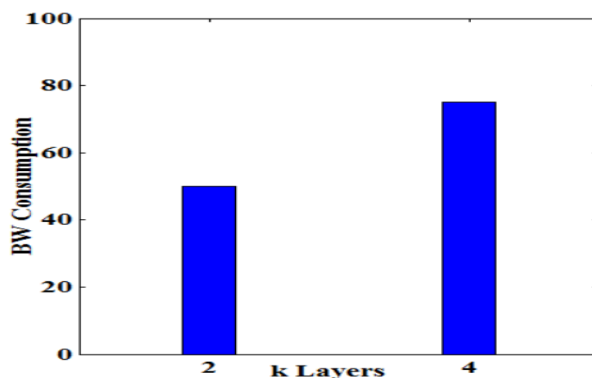





Figure 15. BW Consumption %, ( $k = 2, 4$ ) layers.

So, for different number of layers ( $k = 2^n, n = 1, 2$ ), bandwidth consumption is calculated as:

$$BW \text{ Consumption} = \left( \left( 1 - \left( \frac{1}{k} \right) \right) \times 100\% \right) \quad (20)$$

Finally, Figure 15 clarifies the relation between the bandwidth consumption and the number of layers in the proposed ML-I-NOMA system. Regardless, the image size, the BW consumption ratio is depending on the number of layers. Table 4 presented various standard grey scale test images performance under the proposed ML-I-NOMA to guarantee the evaluation of the proposed system. The findings for  $k = 4, r = 7$  achieved both perfect visual quality in-terms of PSNR and system reliability in-terms of BER.

Table 4. BER & PSNR performance for different standard test images, ( $n = 2 \rightarrow k = 4, r = 7$ , at  $E_b N_0 = 8 \text{ dB}$ , Iter = 3).

$k$	4		
HPA	Test Image		
	Fruit	Lake	Peppers
With, $r = 7$			
BER	$8.5449 \times 10^{-4}$	$8.9264 \times 10^{-4}$	$9.6893 \times 10^{-4}$
PSNR	37.2346 dB	36.6457 dB	35.3338 dB

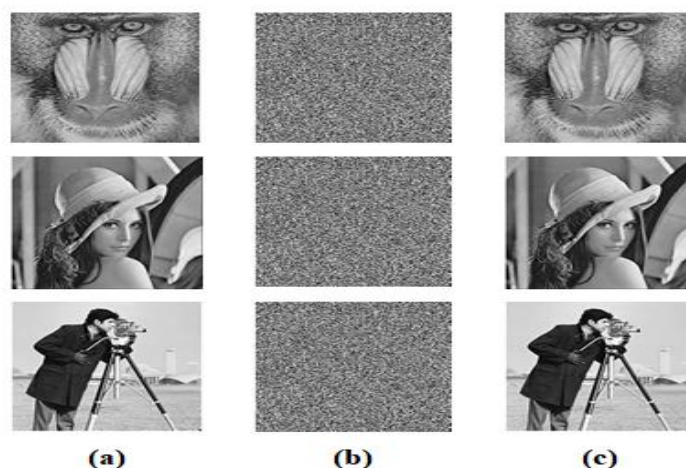
## 5. Security analysis of Encrypted ML-I-NOMA

In this section, we assumed that the non-correct keys are used in the detection process (encryption study). So, the non-correct image will be analyzed as encrypted image. 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.

### 5.1. Key space analysis

The key space calculates total number of different keys that can be used in the encryption algorithm. In the proposed encryption, the secret keys include 8 initial values ( $x_0^1, x_0^2, x_0^3, x_0^4, x_0^5, x_0^6, x_0^7, x_0^8$ ) in the range of  $[0, 1]$  and 8 control parameters ( $r^1, r^2, \dots, r^8$ ) are valid within 4 to 20, if the length of every initial value or control

parameter is set to 16 decimals. The overall complexity (total key space) can be calculated as:  $10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{15} = 10^{8 \times 15} = 10^{120}$ . If the key space of an image of size  $128 \times 128$  is  $128 \times 128 \times 2^8 = 4 \times 10^5$ . So, total key space can be calculated as:  $10^{120} \times 4 \times 10^5 = 4 \times 10^{125} = 2^{415}$ . The key space of the proposed algorithm is greater than  $2^{100}$ , the results proved that the key space of our algorithm is very large to prevent all types of brute force attacks. Figure 16 and Table 5 shows the results and analysis of the key space analysis.



**Figure 16.** Encryption and decryption results of the grey images Baboon, Lena, and Cameraman

**Table 5.** Proposed key space analysis compared with other method results

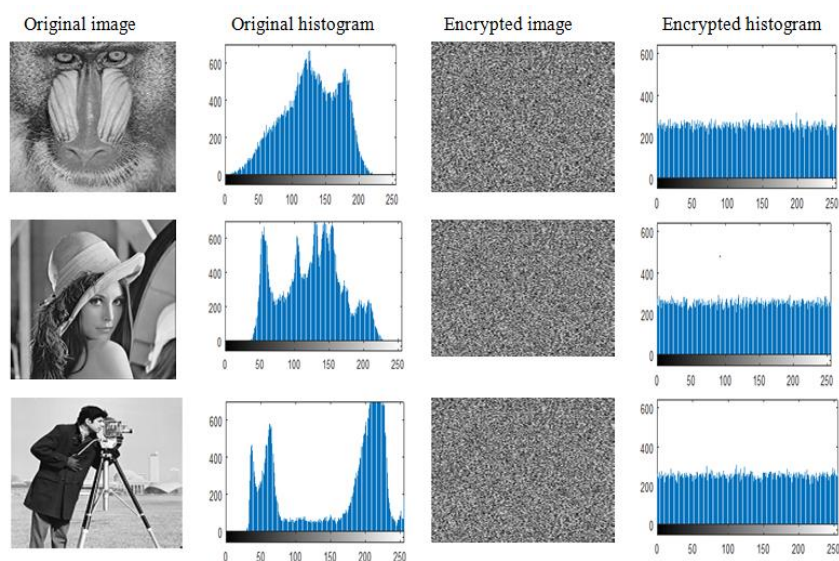
Methods	Ref [25]	Ref [31]	Ref [32]	Proposed
Key space	$10^{58}$	$10^{56}$	$10^{60}$	$10^{125}$

## 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 will be used to determine the difference between them.

### 5.2.1. Histogram analysis

The pixel distribution of the encoded images is shown in Figure 17. The encrypted histogram can reduce the correlation between pixel values. Thus, image information can be protected from statistical attack.



**Figure 17.** 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 [23]. The correlation coefficient  $\rho_{xy}$  can calculate by the following formula.

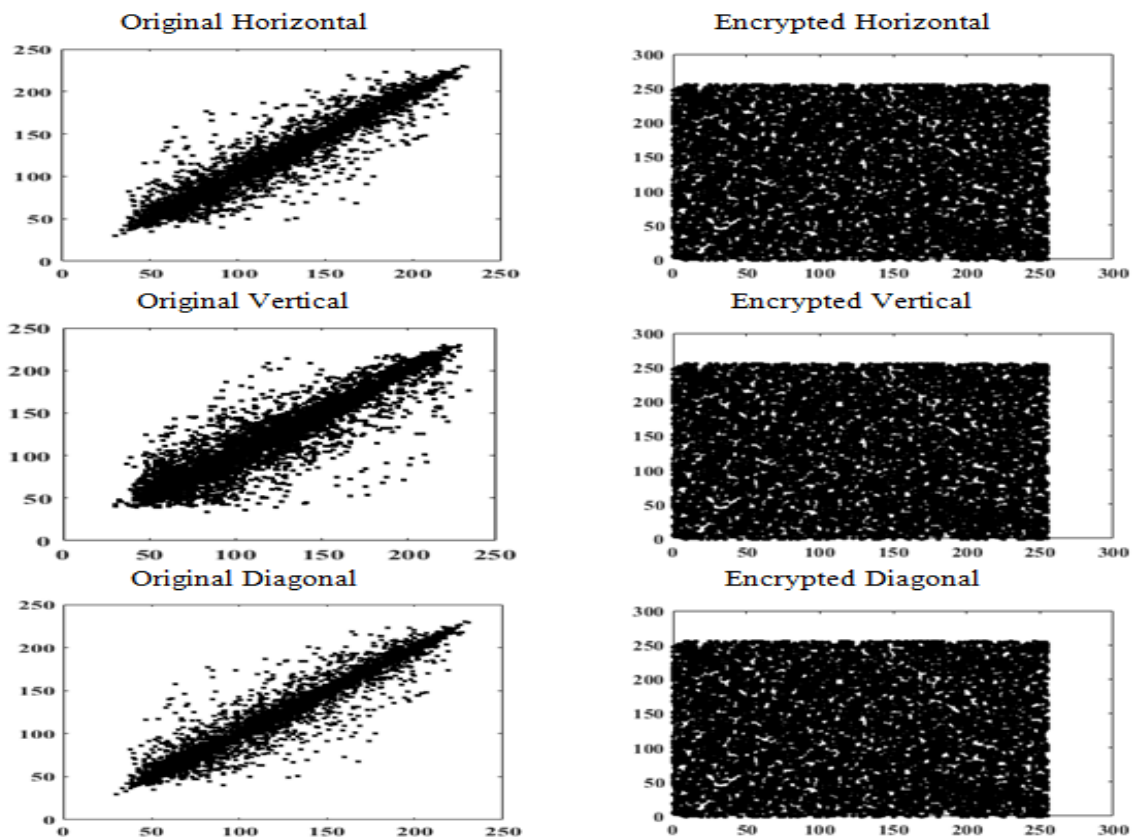
$$\rho_{xy} = \frac{Cov(x,y)}{\sqrt{D(x).D(y)}} \quad (21)$$

$$E_x = \frac{1}{N} \sum_{i=1}^N x_i \quad (22)$$

$$D_x = \frac{1}{N} \sum_{i=1}^N (x_i - E_x)^2 \quad (23)$$

$$Cov(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - E_x)(y_i - E_y) \quad (24)$$

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 18.



**Figure 18.** Correlation distribution in the three directions before and after encryption of Lena image

The results appear the correlation coefficients of the encoded image are near to 0 in all iteration. Table 6 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 6.** 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
proposed	-0.00501	-0.0012	0.00195
Ref [22]	-0.07600	-0.0034	-0.0074
Ref [32]	-0.00260	-0.0054	0.00820

### 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, and can be defined as [33-34]:

$$PSNR = 10 \times \log_{10} \frac{M \times N \times (2^n - 1)^2}{\sum_{i=1}^N \sum_{j=1}^M [I(i, j) - C(i, j)]^2} \quad (25)$$

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 represents the low value of PSNR. The result values of encrypted images baboon, Lena, cameraman is shown in Table 7 which clarifies that the proposed algorithm is better than other algorithms.

**Table 7.** Proposed Peak signal-to-noise ratio compared with other method results

Image	PSNR (dB)
Lena	7.736859
Ref [24]	7.9872
Ref [26]	8.4124

### 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 [23]. The entropy of the information system is defined as [35-36]:

$$H(m) = - \sum_{i=0}^{2^N-1} p(m_i) \times \log_2 p(m_i) \quad (26)$$

where, "m" is the source of information, N total number of bits represents the symbol  $m_i$ ,  $p(m_i)$  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 8, which is near to 8. That means the minimal probability for the attacker to decode a cipher image.

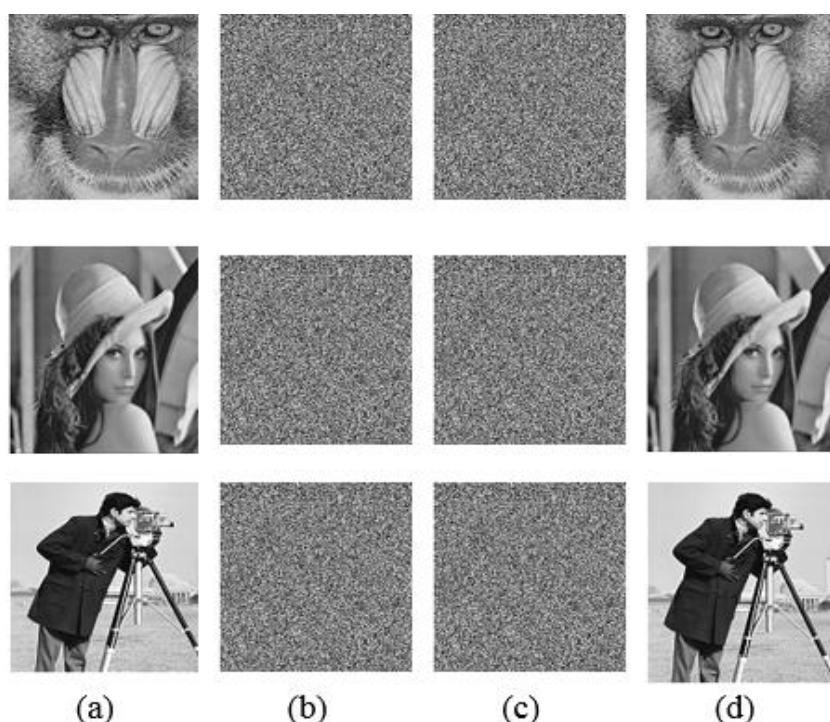
**Table 8.** Information entropy of cipher-image by the proposed algorithm and references.

Image (Lena)	Entropy
Proposed	7.9978
Ref [22]	7.9974
Ref [25]	7.9972
Ref [31]	7.9891

### 5.2.5. Key sensitivity analysis

A robust encryption system should have a high sensitivity for any minor change in the secret keys [37]. To test the key sensitivity, assume the control parameters and initial values that are used to encrypt plain images  $(x_0^1, x_0^2, x_0^3, x_0^4, x_0^5, x_0^6, x_0^7, x_0^8)$  and  $(r^1, r^2, \dots, r^8)$ . After the encryption step, change the key by adding  $10^{-16}$  to any initial condition or control parameter and use it to decode the image.

Thus, the key sensitivity test is shown in Figure 19, 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.



**Figure 19.** Key sensitivity analysis: (a) Original images, (b) cipher-images of the original key. (c) Decrypted images for the incorrect decryption key, (d) decrypted images for the correct decryption key.

### 5.3. Differential 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, the number of pixels change rate (i.e. NPCR) and unified average changing intensity (i.e. UACI). 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 [37]:

$$NPCR = \frac{\sum_{i=1}^N \sum_{j=1}^M D(i, j)}{M \times N} \times 100\% \quad (27)$$

$$UACI = \frac{1}{M \times N} \frac{\sum_{i=1}^N \sum_{j=1}^M |C_1(i, j) - C_2(i, j)|}{2^n - 1} \times 100 \quad (28)$$

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

$$D(i, j) = \begin{cases} 1 & \text{if } C_1(i, j) \neq C_2(i, j) \\ 0 & \text{if } C_1(i, j) = C_2(i, j) \end{cases} \quad (29)$$

The value of the first pixel in the plain images is  $p_i$ . It is altered to  $p_i = (p_i + 100) \bmod 256$  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 9. 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 9.** Result of NPCR and UACI of proposed algorithm and references

Proposed (Lena)	NPCR	99.6277
	UACI	33.5211
Ref [31] (Lena)	NPCR	99.5500
	UACI	33.6000
Ref [32] (Lena)	NPCR	99.6095
	UACI	33.4623

## 6. Conclusions

This paper introduced a new scheme to improve the physical layer security of the interleaved NOMA communication system. Also, this paper suggested a new type of interleaved NOMA based on the multi-layers concept (ML-I-NOMA) with the iterative decoder. In addition, a new cascaded multi modular chaotic logistic map is proposed. The bifurcation diagram of the proposed cascaded multi modular chaotic logistic map is very complex and it has strong chaos properties. The strong chaos leads to a very high Lyapunov exponent values. The analysis of the proposed ML-I-NOMA system is study in both encrypted and non-encrypted image transmissions. The simulation results show that the proposed MLI-NOMA achieves 50% and 75% bandwidth efficiency at two and four layers respectively. The results of statistical tests provided sufficient evidence for the superiority of the proposed chaotic image encryption system over other algorithms.

## References

1. Wang, P.; Xiao, J.; Ping, Li. Comparison of orthogonal and nonorthogonal approaches to future wireless cellular systems. *IEEE Trans. Veh. Technol.* **2006**, Volume 1(3), pp. 4–11.
2. Saito, Yuya ; Yoshihisa Kishiyama. Non-Orthogonal Multiple Access (NOMA) for Cellular Future Radio Access. *IEEE VTC Spring* **2013**, pp. 1–5.
3. Lei, Zhiguo Ding Xianfu; Karagiannidis, George K. A Survey on Non-Orthogonal Multiple Access for 5G Networks: Research Challenges and future Trends. *IEEE J-SAC* **2017**, Volume 35(10), pp. 2181-2195.
4. Luo, Fa-Long; Zhang, Charlie. *Non-Orthogonal Multiple Access (NOMA): Concept and Design*, 1st ed.; Wiley-IIEEE Press, USA, **2016**; pp. 143–168.
5. Ping; Liu; Keying. Interleave Division Multiple Access. *IEEE Trans. Wireless Commun.* **2006**, Volume 5(4), pp. 938–947.
6. Abbas, S. Syed Ameer; Priyadarsini, S. Realization of NOMA Scheme using Interleaved Division Multiple Access for 5G. *IJAER* **2018**, Volume 13(12), pp. 10580-10587
7. Rebhi, Manel; Hassan, Kais . Sparse Code Multiple Access: Potentials and Challenges. *IEEE (OJ-COMS)* **2021**, Volume 2, pp. 1205-1238.
8. Cao, Yiqing; Sun, Haitong. Resource Spread Multiple Access - A Novel Transmission Scheme for 5G Uplink. *IEEE VTC-Fall* **2017**, pp. 14-22.
9. Shukla, M. K. Performance Evaluation of IDMA Scheme in Wireless Communication, Role of Tree Based Interleaver and its Comparison. PhD thesis, Motilal Nehru National Institute of Technology, Degree-Granting University, India, **2011**.
10. Li, Shufeng; Su, Baoxin; Jin, Libiao. Research on PDMA Communication System Based on Complete Complementary Sequence. *EURASIP Journal on Wireless Communications and Networking* **2020**, pp. 1-18.
11. Chen, Yan; Bayesteh, Alireza. SCMA: A Promising Non-Orthogonal Multiple Access Technology for 5G Networks. *IEEE VTC-Fall* **2016**, pp. 34-42.
12. Rahmati, Ali; Yapici, Yavuz. Energy Efficiency of RSMA and NOMA in Cellular-Connected mmWave UAV Networks. *IEEE ICC Workshops* **2019**, pp. 88 - 96.
13. Thirunavukkarasu, Ramya; Balasubramanian, Ramachandran. An Efficient Code Domain NOMA Scheme with Enhanced Spectral and Energy Efficiency for Networks Beyond 5G. *Wireless Personal Communications* **2020**, pp. 353–377.
14. Hoehner, P. A.; Wo. Superposition Modulation: Myths and Facts. *IEEE Communications Magazine* **2011**, Volume 49(12), pp. 110-116.
15. Krikidis I. Analysis and Optimization Issues for Superposition Modulation in Cooperative Networks. *IEEE Trans. Veh. Technol.* **2009**, Volume 58(9), pp. 4837–4847.
16. Özyurt, Serdar; Kucur, Oğuz. Quadrature NOMA: A Low-Complexity Multiple Access Technique with Coordinate Interleaving. *IEEE Wireless Communications Letters* **2020**, Volume 9(9), pp. 1452-1456.
17. Wu H; Li, Ping; Perotti A. User-Specific Chip-Level Interleaver Design for IDMA System. *IEEE Electronics Letters* **2006**, Volume 42(4), pp. 233-234.
18. Dahiya, Priyanka; Sharma, Kanchan; White, G. P. Turbo Coded MIMO-OFDM systems. *IJEIT* **2013**, Volume 3(3), pp. 312-316.
19. Stallings, William. *Cryptography and Network Security, principles and practices*, 4<sup>th</sup> ed; Prentice Hall Press, United Kingdom, 2005; pp. 171–438.

20. Zhu, S.; Wang, G.; Zhu, C. A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes. *Entropy (Pasel)* **2019**, Volume 21(8), pp. 1-20.
21. Li, Zhen; Peng, Changgen. An Effective Chaos-Based Image Encryption Scheme Using Imitating Jigsaw Method. *Hindawi Complexity and Chaos-Based Engineering Applications* **2021**, pp. 1-18.
22. Fridrich, J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. *Int. J. Bifurcation Chaos* **2011**, Volume 8(6), pp. 1259-1284.
23. Parvaz, R.; Zarebnia, M. A Combination Chaotic System and Application in Color Image Encryption. *Optics & Laser Technology* **2018**, Volume 101, pp. 30-41.
24. Hua Z.; Zhou Y. One-Dimensional Nonlinear Model for Producing Chaos. *IEEE Transactions on Circuits and Systems* **2018**, Volume 65, pp. 235-246.
25. Zhou Y.; Bao L.; Philip Chen C L. A New 1D Chaotic System for Image Encryption. *Signal Processing* **2014**, Volume 97, pp. 172-182.
26. Liu, Lingfeng; Miao, Suoxia. A New Image Encryption Algorithm Based on Logistic Chaotic Map with Varying Parameter. *Springer plus* **2016**, pp. 1-12.
27. Liu L.; Miao S. A New Simple One-Dimensional Chaotic Map and Its Application for Image Encryption. *Multimedia Tools Appl* **2018**, Volume 77(16), pp. 21445-21462.
28. Lan, Rushi; He, Wang, Jinwen; Shouhua. Tianlong Gu; Xiaonan Luo. Integrated Chaotic Systems for Image Encryption. *Signal Processing* **2018**, Volume 147, pp. 133-145.
29. Huang H.; Yang S.; Ye R. Efficient Symmetric Image Encryption By using a Novel 2D Chaotic System. *IET Image Processing*, **2020**, Volume 14, pp.1157-1163.
30. Liu L.; Wang D.; Lei Y. An Image Encryption Scheme Based on Hyper Chaotic System and DNA with Fixed Secret Keys. *IEEE Access* **2020**, Volume 8, pp. 46400-46416.
31. Zhou Y.; Hua Z.; Pun C M.; Chen C L. Cascade Chaotic System with Applications. *IEEE transaction on cybernetics* **2015**, Volume 45(9), pp. 2001-2012.
32. Hua Z.; Zhou Y. Dynamic Parameter Control Chaotic System. *IEEE transaction on cybernetics* **2016**, Volume 46(12), pp. 3330-3341.
33. Wang, Xingyuan; Chen, Shengnan; Zhang, Yingqian. A Chaotic Image Encryption Algorithm Based on Random Dynamic Mixing. *Optics & Laser Technology* **2021**, Volume 138, pp. 122-130.
34. Wang, Xingyuan; Li, Yanpei. Chaotic Image Encryption Algorithm Based on Hybrid Multi-Objective Particle Swarm Optimization and DNA sequence. *Optics and Lasers in Engineering* **2021**, Volume 137, pp. 266-304.
35. Talhaoui, Mohamed Zakariya; Wang, Xingyuan; Talhaoui, Abdallah. A New One-Dimensional Chaotic Map and its Application in a Novel Permutation-less Image Encryption Scheme. *The Visual Computer* **2021**, Volume 37, pp. 1757-1768.
36. Zhou, Yang; Li, Chunlai; Li, Wen; Li, Hongmin; Wei Feng; Kun Qian. Image Encryption Algorithm with Circle Index Table Scrambling and Partition Diffusion. *Nonlinear Dynamics* **2021**, Volume 103, pp. 2043-2061.
37. Patro, K. Abhimanyu Kumar; Acharya, Bibhudendra. An Efficient Dual-Layer Cross-Coupled Chaotic Map Security-Based Multi-Image Encryption system. *Nonlinear Dynamics* **2021**, Volume 104, pp. 2759-2805.