entropy

MDPI

Article

Physical-Layer Security in Power-Domain NOMA Based on Different Chaotic Maps

Mariam Abu Al-Atta [1,*], Karim A. Said [2], Mohamed A. Mohamed [2] and Walid Raslan [1]

[1] Electronics and Communications Department, Faculty of Engineering, Delta University for Science and Technology, Gamsaa 35712, Egypt

[2] Electronics and Communication Engineering Department, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt

* Correspondence: maryam.abualata@deltauniv.edu.eg

Abstract: Nonorthogonal multiple access (NOMA) is a relevant technology for realizing the primary goals of next-generation wireless networks, such as high connectivity and stability. Because a rising number of users are becoming connected, user data security has become a critical issue. Many chaotic communication systems have been established to address this important issue via exhibition of affordable physical-layer-security solutions. In this study, we propose a chaotic downlink NOMA (C-DL-NOMA) system over the additive white Gaussian noise and Rayleigh-fading channels to enhance the security of the DL-NOMA system. The proposed algorithm is based on a coherent analog modulation technique that combines various chaotic maps for chaotic masking of encrypted data. On the transmitter, chaotic encryption was used for transmitted data with fixed power-allocation-level control, whereas on the receiver, successive interference-cancellation demodulation was utilized to detect multiple users, after which chaotic decryption was performed. Simulation results were evaluated based on security analyses, such as statistical analysis (histogram and correlation analyses and information entropy), bit-error-rate performance, and achievable-data-rate performance. According to these security analyses and numerical results, the proposed C-DL-NOMA system outperformed traditional unencrypted NOMA systems.

Keywords: nonorthogonal multiple access; physical-layer security; power domain; downlink; encryption; chaos; logistic map; Arnold's cat map; decryption; hyperchaotic DNA; Hénon map

check for updates

Citation: Abu Al-Atta, M.; Said, K.A.; Mohamed, M.A.; Raslan, W. Physical-Layer Security in Power-Domain NOMA Based on Different Chaotic Maps. *Entropy* **2023**, *25*, 140. https://doi.org/10.3390/e25010140

Academic Editor: José F. F. Mendes

Received: 17 November 2022
Revised: 4 January 2023
Accepted: 6 January 2023
Published: 10 January 2023

1. Introduction

Nonorthogonal multiple access (NOMA) is a multiple-access technology for next-generation (5G) mobile networks. It is a nonorthogonal multiplexing method that allows users to be multiplexed in the power domain, which had previously been neglected by wireless mobile systems. Many users' signals are combined at the transmitter and then segregated via successive interference cancellation (SIC) at the receiver [1]. In recent years, the multiple access (MA) system has been considered a significant high-tech advancement that has defined each generation of wireless communication networks. From the 1G mobile communication system to the 4G system, orthogonal MA (OMA) has been extensively used in current wireless systems. OMA systems include the widely used frequency-division MA for 1G, time-division MA for 2G, code-division MA (CDMA) for 3G, and orthogonal-frequency-division MA for 4G. Notably, only a limited number of users are multiplexed orthogonally within the frequency, time, or code domain in these OMA methods [2]. Several promising technologies have been proposed in recent years to address this critical issue. One such technology is nonorthogonal multiple access (NOMA): a way of serving numerous users from a single wireless resource. NOMA can be accomplished in different domains, including power, code, and others. For participation in the total resource, code-domain NOMA uses user-specific spreading sequences, whereas power-domain NOMA uses channel-gain changes among users for multiplexing through power allocation [3]. Owing to the open propagation environment, wireless networks are prone to interception from unauthorized receivers, and the enormous rise in NOMA users and related data traffic could result in more information security breaches, thereby making standard wireless security techniques depend on upper-layer cryptography. Because use of upper-layer security in NOMA systems with power-limited devices is ineffective due to cost and complexity restrictions, a reliable and economical physical-layer security (PLS) strategy that depends on channel-coding methods has been developed [4–6]. This strategy improves the performance gap between the intended user and the eavesdropper, using basic channel features such as noise, fading, diversity, and interference [4]. In addition, when combined with encryption-based systems, it can increase the entire system's security [7,8]. Several types of encryption algorithm exist, each designed for a specific purpose. When existing algorithms become insecure, new ones are developed. The Data Encryption Standard, the Advanced Encryption Standard, Blowfish encryption, and Rivest Cipher 4 are some of the most well-known cryptographic algorithms. Some recent encryption methods have been shown to be untrustworthy for ciphering [9]. Owing to its sensitivity to control parameters and initial conditions, chaos-based encryption is inherent in chaotic methods of meeting security demands.

Several studies have described various chaos-based secure communication (CBSC) methods that offer cost effective and robust PLS for multiuser wireless applications. Chaos-based, secure power-domain NOMA was introduced in [6] for the uplink large-scale and Rician channels, with effective dynamic power control for transmitted multilevel chaos-shift-keying signals. For multiuser detection, an advanced receiver scheme that depends on SIC and chaos demodulation is suggested. The authors in [7] introduced a downlink (DL) chaotic NOMA (C-NOMA) method that used the C-MIMO idea to achieve high-capacity allocation and PLS. In [8], an uplink C-NOMA transmission technique, in which C-MIMO was used with NOMA to improve system throughput while providing PLS to other cell users and an eavesdropper, was proposed. NOMA successfully replicated the impacts of channel coding and PLS in C-MIMO. The authors in [10] offered a DL-C-NOMA transmission technique that achieves better capacity while providing PLS that is resistant to eavesdroppers and other users without initial keys. They used the C-MIMO scheme principle in NOMA to achieve this aim. Furthermore, while a low-complexity decoding technique for C-NOMA, which combined partial maximum-likelihood sequence estimation and the popular NOMA decoding method of SIC, was proposed in [11], an effective chaos-based NOMA (CB-NOMA) system for secure wireless communication was proposed in [12] over a Rayleigh-fading environment. Equal power allocation for linked users with a chaotic code domain is used in an integrated CB-NOMA design. Various chaotic-code-formation schemes with varying levels of security, implementation, and complexity have been studied for signaling via chaos shift keying (CSK).

The aforementioned studies indicated that different coherent modulation techniques, such as chaos modulation [6,11], CSK [6], and chaos-based code-domain MA [12], have been used over NOMA. To improve the security of the DL-NOMA scheme, a chaotic downlink NOMA (C-DL-NOMA) system is proposed in this study. The proposed system uses a coherent analog modulation technique that combines various chaotic maps for chaotic masking (CM) of encrypted data and SIC decoding for complexity reduction over additive white Gaussian noise (AWGN) and Rayleigh-fading single-input–single-output (SISO) DL power-domain NOMA channels. This study's main contributions are summarized below.

- The effects of various hybrid chaotic maps on DL-NOMA performance are investigated using security analysis represented by statistical analyses, which include histogram and correlation analyses.
- The proposed C-DL-NOMA system provides robust PLS and a low bit error ratio (BER) with fixed power-allocation-level control, depending on the distance from the base station (BS).

- The proposed C-DL-NOMA system is compared with traditional unencrypted NOMA in terms of BER and achievable data rate.

The rest of this paper is organized as follows: Section 2 explains the DL-NOMA system model; Section 3 presents a C-DL-NOMA system model and different chaotic maps; Section 4 explains and discusses the simulation results; and finally, Section 5 concludes this study.

2. System Model

This section describes the SISO DL power-domain NOMA system model (Figure 1). One-cell NOMA combines M users and one BS, each with one antenna. The channel response is perfectly known at the base station. The BS transmits the superposed signal to all mobile users on the transmitter side of the DL-NOMA system; this is a superposition of several users' required signals with varying fixed power-coefficient allocations based on their distances from the BS [13]. The SIC procedure is supposed to be implemented sequentially on each user's receiver side until the user's signal is retrieved. The user with the greatest transmission power retrieves its signal with no execution of any SIC procedure and treats the other users' signals as noise. However, other users must perform the SIC procedure. In the SIC procedure, every user's receiver first discovers signals that are stronger than the user's required signal. These signals are then subtracted from the received signal, and the procedure is repeated until the user's required signal is identified. Finally, through consideration of users with lower power coefficients as noise, every user decodes its signal [5].

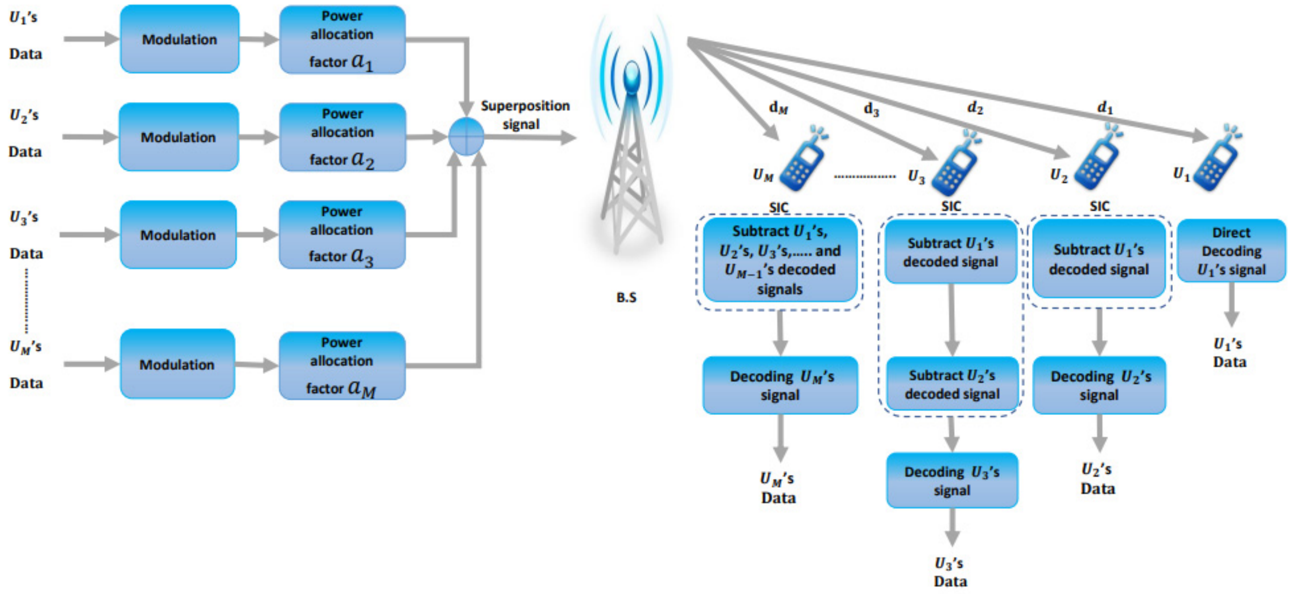
U_1's Data
Modulation
Power allocation factor a_1
U_2's Data
Modulation
Power allocation factor a_2
U_3's Data
Modulation
Power allocation factor a_3
U_M's Data
Modulation
Power allocation factor a_M
Superposition signal
B.S
d_M
d_3
d_2
d_1
U_M
U_3
U_2
U_1
SIC
Subtract U_1's, U_2's, U_3's,..... and U_{M-1}'s decoded signals
Decoding U_M's signal
U_M's Data
SIC
Subtract U_1's decoded signal
Subtract U_2's decoded signal
Decoding U_3's signal
U_3's Data
SIC
Subtract U_1's decoded signal
Decoding U_2's signal
U_2's Data
Direct Decoding U_1's signal
U_1's Data

Figure 1. SISO DL-NOMA system model.

As in [13], the transmitted superposed signal at the BS is expressed as follows:

$$x_s = \sum_{i=1}^{M} \sqrt{a_i P_t}\, x_i \tag{1}$$

where x_i is the data of user i (U_i) with unit energy, P_t is the transmitted power at the BS, and a_i is the power-allocation coefficient for user i; the allocation of power levels depends on the distance of every user so that $a_i' = \frac{\mathrm{d}_i}{d_{max}}$ ($i = 1, 2, \ldots M$), where a_i' is the absolute power factor and d_i is the distance between the BS and the ith user, with $d_{max} = 200$ m (a typical BS radius in 5G networks). The power factors are normalized between 0 and 1 as follows: $a_i = \frac{a'_i}{\sum_{v=1}^{M} a'_v}$ $(v = 1,\ 2,\ \ldots M)$ [14]. In other words, $\sum_{i=1}^{M} a_i = 1$ and $1 > a_1 \geq\ a_2\ \geq\ \ldots\ a_M > 0$ because without loss of generality, the channel gains are supposed to be arranged as $|h_1|^2\ \leq\ |h_2|^2\ \leq\ \ldots\ |h_M|^2$, where h_i is the Rayleigh-fading channel coefficient among the BS and the m^{th} user.

As in [13], the received signal at the m^{th} user can be written as follows:

$$y_m = h_m x_s + n_m = h_m \sum_{i=1}^{M} \sqrt{a_i P_t} x_i + n_m \tag{2}$$

where n_m is complex, zero-mean AWGN with a variance of σ^2 and is denoted as $n_m\ \sim\ CN\left(0, \sigma^2\right)$.

Notably, users use SIC to obtain desired signals from the received signal, y_m. In particular, U_m starts by decoding the stronger U_1 signal through treatment of the remaining part of the signal as interference. Thereafter, to acquire a signal free of the U_1 signal, U_m remodulates the decoded signal and removes it from the received signal, y_m. Executing an identical process, U_m progressively cancels the whole signals corresponding to users $U_2, U_3, \ldots, U_{m-1}$ from the received signal, y_m, lastly decoding its signal through treatment of the rest of the signal parts, corresponding to users $U_{m+1}, U_{m+2}, \ldots, U_M$, as interference [15].

From Equation (2), the m^{th} user's signal to interference and noise ratio (SINR) is used to discover the j^{th} user, $j\ \leq\ m$, with $j\ \neq\ M$, expressed as follows [13]:

$$SINR_{j \to m} = \frac{a_j \rho_s |h_m|^2}{\rho_s |h_m|^2 \sum_{i=j+1}^{M} a_i + 1} \tag{3}$$

where $\rho_s = P_t/\sigma^2$ indicates the signal-to-noise ratio (SNR). To obtain the m^{th} user's required data, the SIC procedure is performed on the signal of user $j\ \leq\ m$. Thus, the m^{th} user's SINR is expressed as follows [13]:

$$SINR_m = \frac{a_m \rho_s |h_m|^2}{\rho_s |h_m|^2 \sum_{i=m+1}^{M} a_i\ + 1} \tag{4}$$

Then, the M^{th} user's SINR is given with [13]:

$$SINR_M = a_M \rho_s |h_M|^2 \tag{5}$$

After the SINR terms of DL-NOMA are acquired, when all of the symbols ($x_1, x_2, \ldots, x_{m-1}$) have been accurately decoded, the achievable rate at U_m for decoding signal x_m can be gained as follows [13]:

$$R_m^{DL} = \log_2(1 + SINR_m) = \log_2(1 + \frac{a_m \rho_s |h_m|^2}{\rho_s |h_m|^2 \sum_{i=m+1}^{M} a_i + 1}) \tag{6}$$

Thus, the sum rate of DL-NOMA is described as follows [13]:

$$\begin{aligned} R_{sum}^{DL} &= \sum_{m=1}^{M} \log_2(1 + SINR_m) \\ &= \sum_{m=1}^{M-1} \log_2(1 + \tfrac{a_m \rho_s |h_m|^2}{\rho_s |h_m|^2 \sum_{i=m+1}^{M} a_i + 1}) + \log_2\left(1 + a_M \rho_s |h_M|^2\right) \\ &= \sum_{m=1}^{M-1} \log_2(1 + \tfrac{a_m}{\sum_{i=m+1}^{M} a_i + 1/\rho_s |h_m|^2}) + \log_2\left(1 + a_M \rho_s |h_M|^2\right) \end{aligned} \tag{7}$$

With a high SNR that is as $\rho_s \to \infty$, the sum rate of DL-NOMA becomes [13]

$$R^{DL}_{sum} \approx \sum_{m=1}^{M-1} \log_2(1 + \frac{a_m}{\sum_{i=m+1}^{M} a_i}) + \log_2\left(\rho_s |h_M|^2\right) \approx \log_2\left(\rho_s |h_M|^2\right) \tag{8}$$

3. The Proposed C-DL-NOMA System Model

Having introduced the DL power-domain NOMA communication system, we want to support the security of data transmission through it via encryption of this data (Figure 2) using different chaotic maps. In the area of CBSC, chaotic signals are frequently employed for various modulation techniques, including chaos on–off keying (COOK), CSK, chaos-parameter modulation, and CM. In this study, we applied CM modulation to DL power-domain NOMA using hybrid chaotic maps. In this technique, plain data are added to the chaotic signal sequence, after which the produced data are transmitted through the NOMA channel. The plain data can be restored through subtraction of the regenerated chaotic signal sequence from the received data. We now explain the chaotic maps used in our proposed C-DL-NOMA system and how we employ them to encrypt the data. Chaotic maps have attractive characteristics, such as easy generation that utilizes low-cost circuits, a noise-like spectrum, unpredictable behavior, sensitivity to initial conditions, and rapid iteration. Therefore, chaos-based data encryption techniques are suitable for real-time applications. Some existing chaotic maps are discussed below.

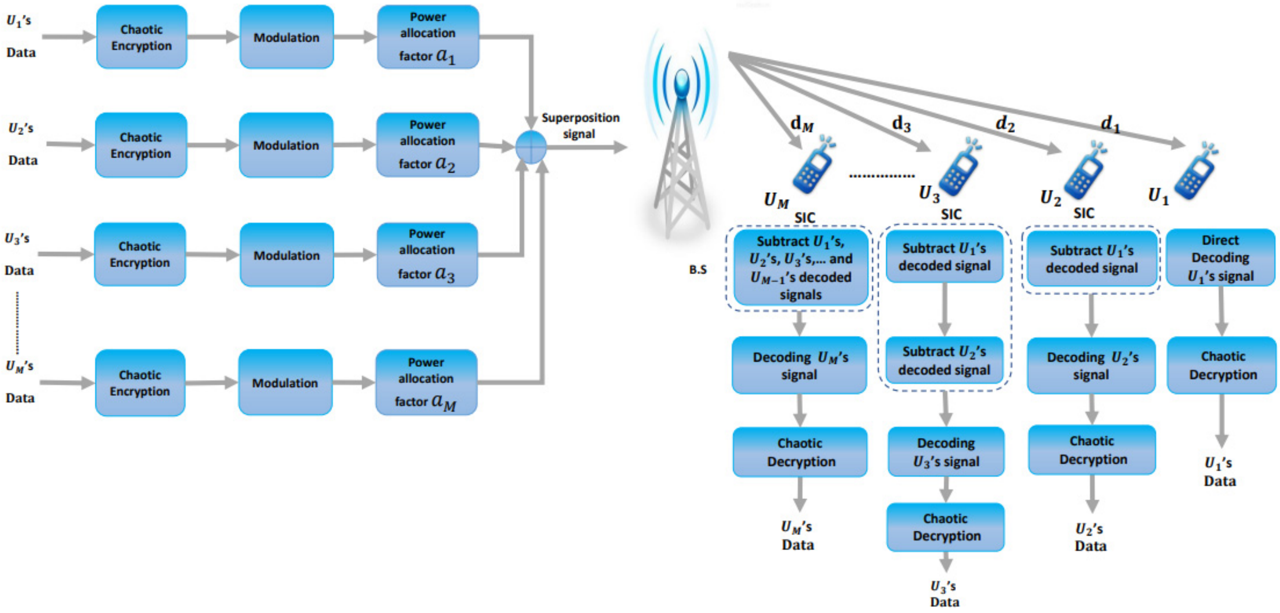

Figure 2. Proposed C-DL-NOMA system model.

3.1. Logistic Chaotic Map

The logistic map is very basic and is often used as a normal chaotic map. It appears to be quite simple and predictable, but its dynamic behavior is extremely complicated. The logistic map is defined in [16] as:

$$\chi_{n+1} = r\chi_n(1 - \chi_n) \tag{9}$$

where $n = 0,\ 1,\ 2,\ 3,\ \ldots (0 < \chi_0 < 1$ and $0 < r \le 4)$.

Here, χ_0 and r determine the sequences generated with the logistic map (which is the initial value of χ). If even one of the two values changes slightly, the result will differ significantly. The system will exhibit varied properties depending on deviation level [17]. When $3.56994 < r \le 4$ is reached, chaotic behavior occurs, as indicated in Figure 3 [18].

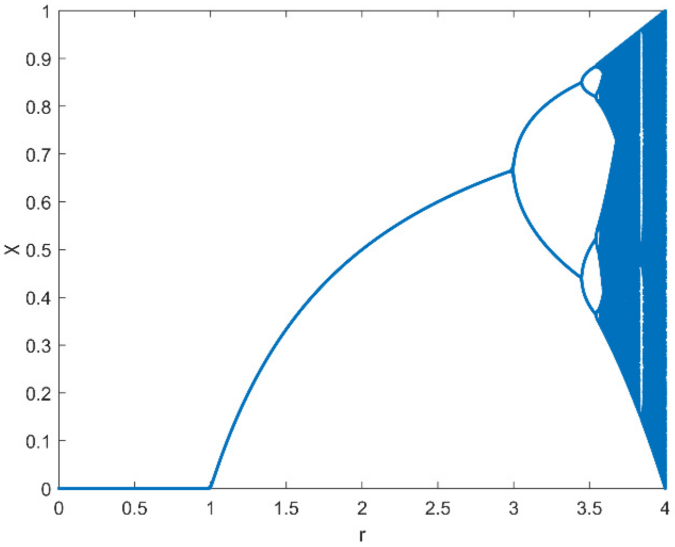

Figure 3. The logistic map bifurcation diagram.

Encryption and Decryption Process:

1. Assume the following parameters: $\chi_0 = 0.1$ and $r = 4$. When this is iterated, we obtain $\chi_1, \chi_2, \ldots, \chi_n$ for the N value. This is a chaotic one-dimensional sequence (A).
2. To encrypt the MN-size original image, a matrix of the same size must be created through transformation of the one-dimensional sequence (A) to a two-dimensional sequence (B), where B is the cipher.
3. The original image is encrypted using an XOR cipher.
4. The encrypted image is decrypted using the XOR cipher.

Encryption and Decryption Algorithm:
Input: original image, χ_0, and r.
Output: encrypted image.
Step 1. Transform the original image of a size of $M \times N$ pixels with an array of $P = p_{i,j}$, where $(1 < i < M)$ and $(1 < j < N)$.
Step 2. Next, convert the pixel values to unsigned integers in the range of 0 to 255, using mod operation $P_m = mod\ \{P, 255\}$.
Step 3. Generate the n number of chaotic sequence $A = \{\chi_1\ , \chi_3\ , \chi_3\ \ldots, \chi_n\}$ in the range of 0 to 1 using the logistic map in Equation (9), with an initial condition of $\chi_0 = 0.1$ and taking the parameter of $r = 4$.
Step 4. Transform the chaotic sequence, A, to an array, B, of a size of $M \times N$.
Step 5. Next, convert B into unsigned integers in the range of 0 to 255, using mod operation $B_m = mod\ \{\text{B}, 255\}$.
Step 6. Encrypted image = $P_m \oplus B_m$.
Step 7. The decryption process is identical to that of encryption in reverse order.

3.2. Hénon Chaotic Map

The Hénon chaotic map is a discrete-time dynamic system that depends on two parameters, a and b, which are essential because they control the system's dynamic behavior. The classical Hénon map uses the values $a = 1.4$ and $b = 0.3$, which results in chaotic behavior. This map can be chaotic, be intermittent, or converge to a periodic orbit for alternative values of a and b [19]. The Hénon chaotic map is formed using the following equations:

$$x_{n+1} = 1 - \text{a}x_n^2 + y_n \quad (10)$$

$$y_{n+1} = \text{b}x_n \quad (11)$$

where (n = 0, 1, 2, . . .); x_n and y_n are the current point positions; and x_{n+1} and y_{n+1} are the next point positions. Initial points x_1 and y_1 [20] act as a symmetric key for a chaotic cryptographic system that is utilized for encryption and decryption at the sender's and receiver's terminals. Since the Hénon map is deterministic, decryption of the cipher image will reconstruct the original image on the receiver's end with the same initial points: x_1 and y_1 [21].

Figure 4a [22] shows the $x - y$ plane graph of the Hénon map's attractor. Figure 4b [23] shows the Hénon map's bifurcation behavior, with $b = 0.3$. The attractive set's x coordinate is plotted along the horizontal axis for various values in the range of a from 0 to 1.4. The repetition sequence begins to divide into a two-period oscillation at $a = 0.35$, which continues until $a = 0.85$. Periodic-doubling bifurcation is another name for this dividing mechanism. In the approximate range of a from 0.85 to 1.1, periods are successively doubled. In the dark region, periodicity switches to chaotic behavior when $a \geq 1.1$. The Hénon map is used to generate two random sequences that permute an image's row and column positions, respectively, due to this chaotic tendency [24].

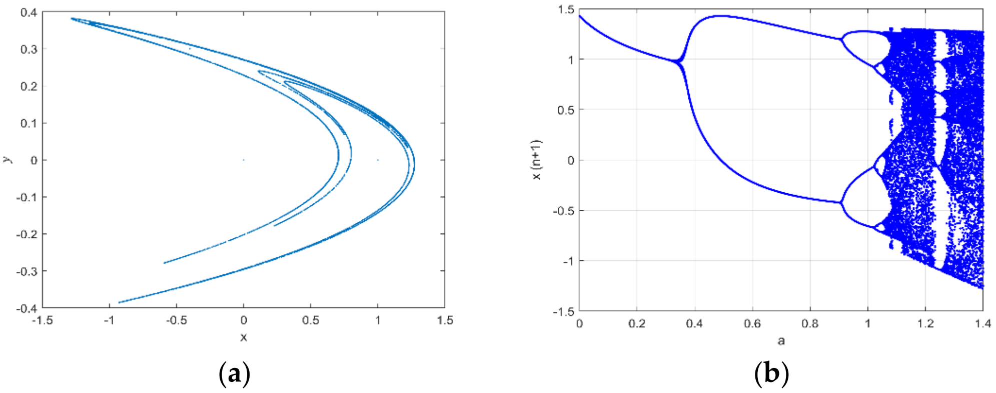

Figure 4. (**a**) The strange attractor of the Hénon map for a = 1.4 and b = 0.3. (**b**) Hénon map bifurcation diagram for b = 0.3.

Encryption and Decryption Process:

Encryption Process, as shown in Figure 5:

1. The number of pixels of the original image are extracted via multiplication of the image's height and width.
2. The Hénon chaotic map is used to scramble the original image's pixels.
3. The logistic chaotic map is used to generate key values or pseudorandom numbers.
4. The encrypted image is obtained via the XOR operation, which is performed between the key values gained from the logistic map and the pixel values obtained from the scrambled image that resulted from the operation with the Hénon chaotic map.

Decryption Process, as shown in Figure 5:

1. The encrypted image's pixels are extracted via measurement of the image's height and width.
2. The XOR operation is performed between the pixel values obtained from the encrypted image and the key values gained from the logistic map.
3. The decrypted image is obtained via use of the Hénon chaotic map to scramble the pixels of the image that resulted from the XOR operation.

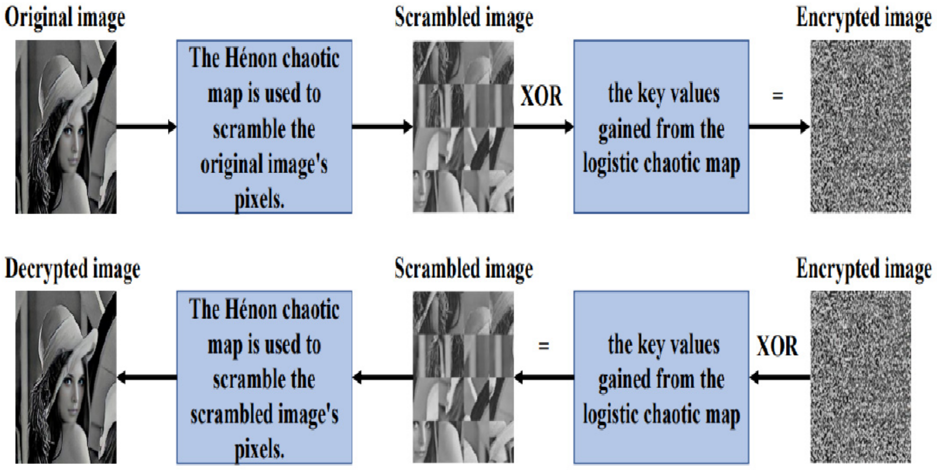
Original image
The Hénon chaotic map is used to scramble the original image's pixels.
Scrambled image
XOR
the key values gained from the logistic chaotic map
=
Encrypted image
Decrypted image
The Hénon chaotic map is used to scramble the scrambled image's pixels.
Scrambled image
=
the key values gained from the logistic chaotic map
XOR
Encrypted image

Figure 5. Encryption and decryption processes using the Hénon chaotic map.

3.3. Arnold's Cat Chaotic Map

Arnold's cat map was designed as a confusion technique to randomize the pixel position of an image so that it does not appear the same. This can be achieved using Equation (12) [21]:

$$\begin{bmatrix} \text{Ϗ}' \\ \text{ϒ}' \end{bmatrix} = \text{Đ} \begin{bmatrix} \text{Ϗ} \\ \text{ϒ} \end{bmatrix} (mod\ \text{ŋ}) = \begin{bmatrix} 1 & \text{ĩ} \\ \text{ɉ} & \text{ĩɉ} + 1 \end{bmatrix} \begin{bmatrix} \text{Ϗ} \\ \text{ϒ} \end{bmatrix} (mod\ \text{ŋ}) \tag{12}$$

where (Ϗ′,ϒ′) is the new position of the original pixel position, (Ϗ, ϒ); ĩ and ɉ are positive integers; and determinant (Đ) = 1. Arnold's cat map includes a unique hyperbolic fixed point. The linear transformation that describes the map is categorical: eigenvalues are irrational numbers, one higher and one lower than 1; hence, they correspond to expanding and contracting eigenspaces, which are also stable and unstable bifurcations. Because the matrix is identical, the eigenspace is orthogonal [20].

As shown in Figure 6, the process of mapping via returning to the unit square continuously shuffles the image (the phase space). The first step demonstrates shearing in the x and y directions, followed by image reassembly [25].

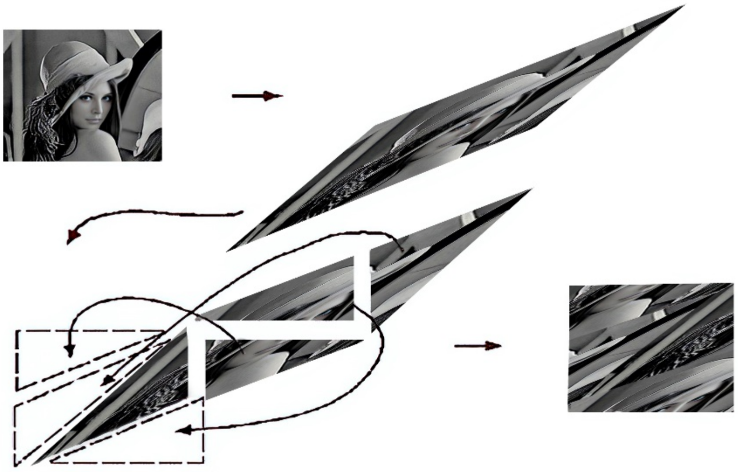

Figure 6. Graphical illustration of Arnold's cat map.

Encryption Process:

1. The number of pixels of the original image are extracted via multiplication of the image's height and width.

2. Arnold's cat chaotic map is utilized to scramble the original image's pixels.
3. The logistic chaotic map is used to generate key values or pseudorandom numbers.
4. The encrypted image is obtained via performance of the XOR operation using the key values obtained from the logistic map and the pixel values obtained from the scrambled image that resulted from the operation with Arnold's cat chaotic map.

Decryption Process:

1. The encrypted image's pixels are extracted via measurement of the image's height and width.
2. The XOR operation is performed between the pixel values obtained from the encrypted image and the key values gained from the logistic map.
3. The decrypted image is obtained via use of Arnold's cat chaotic map to scramble the pixels of the image that resulted from the XOR operation.

3.4. Hyperchaotic Map

A hyperchaotic system is a chaotic system with a positive Lyapunov exponent that exceeds 1, indicating that its chaotic dynamics are provided simultaneously in multiple directions [26]. Hyperchaos occurs in high-dimensional, nonlinear schemes with at least four dimensions. A high-dimensional chaotic system has a larger key space and more complex and unpredictable nonlinear behavior due to the increased number of state variables in a hyperchaotic system [27].

DNA (deoxyribonucleic acid) computing has recently been utilized in chaos-based image-encryption schemes because of its many advantages: enormous parallelism, massive storage, and ultralow power consumption [28].

As illustrated in Figure 7, the authors in [28] combined DNA sequencing and hyperchaotic sequencing for encryption, and we followed the same approach for our proposed C-DL-NOMA system.

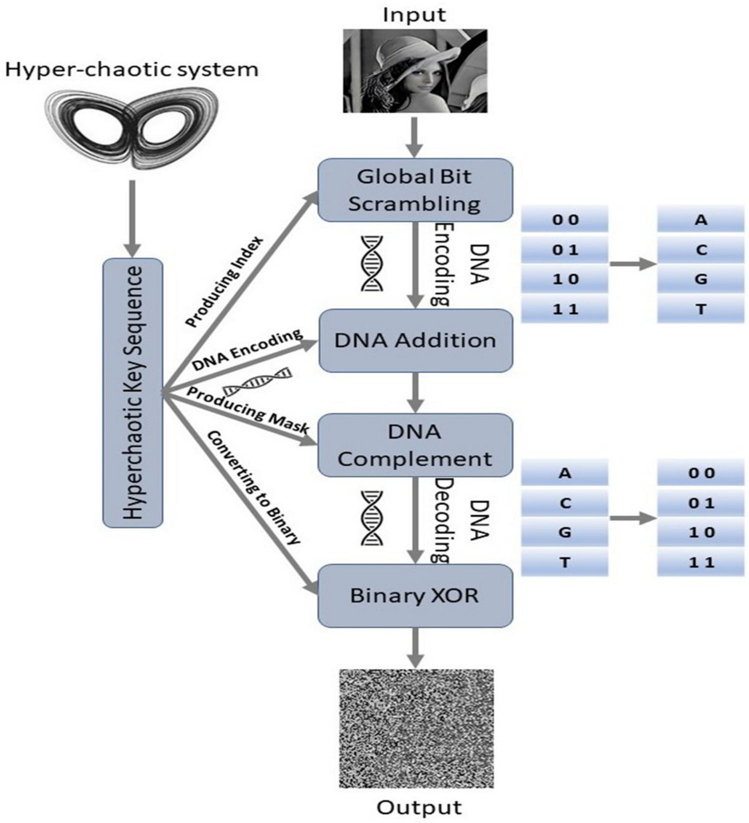

Figure 7. Schematic diagram of encryption using DNA sequencing and hyperchaotic sequencing.

The following nonlinear equations govern the hyperchaotic system [29], which they adopted [28]:

$$\dot{y}_1 = \alpha(y_2 - y_1) + \lambda_1 y_4 \tag{13}$$

$$\dot{y}_2 = \xi y_1 - y_1 y_3 + \lambda_2 y_4 \tag{14}$$

$$\dot{y}_3 = -\beta y_3 + y_1 y_2 + \lambda_3 y_4 \tag{15}$$

$$\dot{y}_4 = -\tau y_1 \tag{16}$$

where the system's control parameters are α, ξ, β, τ, λ_1, λ_2, and λ_3. This system describes hyperchaotic performance when $\alpha = 35$, $\xi = 35$, $\beta = 3$, $\tau = 5$, $\lambda_1 = 1$, $\lambda_2 = 0.2$, and $\lambda_1 = 0.3$.

The DNA sequence includes four bases of nucleic acid, which are permanently denoted by the letters G (Guanine), C (Cytosine), A (Adenine), and T (Thymine). "G" and "C" are complementary, as are "A" and "T". We utilized two-bit binary digits to represent a DNA base, since the binary digits "0" and "1" are complementary. For the representation shown in [30], there are twenty-four different types of rule, and only eight of them satisfy the Watson–Crick complement rule [31]. DNA computing follows conventional binary addition and subtraction rules [32].

Four Steps to Generate the Hyperchaotic Sequence, i:

1. To avoid negative effects and to increase security, the hyperchaotic system is pre-iterated N_0 times.
2. After iteration of N_0 times, the process is repeated $m \times n$ times. We utilized $\hat{\jmath}$ to indicate the iteration index. For every iteration, $\hat{\jmath}$, four state values, $\{\hat{y}_1^{\hat{\jmath}}, \hat{y}_2^{\hat{\jmath}}, \hat{y}_3^{\hat{\jmath}}, \hat{y}_4^{\hat{\jmath}}\}$ are saved.
3. Every state value, $\hat{y}_{\text{i}}^{\hat{\jmath}}$, is utilized to produce two various key values—$\left(v_{\text{į}}^{\text{ɐ}}\right)^{\hat{\jmath}} \in [0, 255]$, ($\text{į}$ = 1, 2, 3, 4) and $v_{\text{į}}^{\text{ɓ}} \in [0, 255]$—through the iteration. They are determined as follows [28]:

$$\left(v_{\text{į}}^{\text{ɐ}}\right)^{\hat{\jmath}} = mod\,\{\left\lfloor\frac{[(|\hat{y}_{\text{į}}^{\hat{\jmath}}| - \lfloor|\hat{y}_{\text{į}}^{\hat{\jmath}}|\rfloor) * 10^{15}]}{10^8}\right\rfloor, 255\,\}, \qquad \text{į} = \ 1,2,3,4 \tag{17}$$

$$\left(v_{\text{į}}^{\text{ɓ}}\right)^{\hat{\jmath}} = mod\left(\left\lfloor mod\left\{\frac{[(|\hat{y}_{\text{į}}^{\hat{\jmath}}| - \lfloor|\hat{y}_{\text{į}}^{\hat{\jmath}}|\rfloor) * 10^{15}]}{10^8}\right\}\right\rfloor, 255\right), \qquad \text{į} = \ 1,2,3,4 \tag{18}$$

Here, $mod(.)$ indicates the modulo operation and $\lfloor . \rfloor$ indicates the flooring process, which rounds the element to the closest integer to negative infinity. These key values are connected with Equation (19) to become a vector, $v^{\hat{\jmath}}$:

$$v^{\hat{\jmath}} = \ v_1^{\text{ɐ}} + \ v_2^{\text{ɐ}} + v_3^{\text{ɐ}} + v_4^{\text{ɐ}} + v_1^{\text{ɓ}} + v_2^{\text{ɓ}} + v_3^{\text{ɓ}} + v_4^{\text{ɓ}} \tag{19}$$

4. After the entire iteration, these sequences are connected with the next equation to obtain k, $k = \left[v^1,\ v^2,\ \ldots, v^{m \times n}\right]$. $k_{\text{į}}$ can be used to represent one element in k, $\text{į} \in [1, 8mn]$.

A global bit scrambling (GBS) system significantly enhances execution of image encryption. An input image, F, has eight bits and an intensity value between 0 and 255. The image's intensity values are globally shuffled, bit by bit, to decrease the correlations among adjacent pixels. GBS also modifies the intensity value of each pixel, meaning it introduces pixel substitution simultaneously.

GBS is achieved using the following two steps:

1. To obtain a one-dimensional binary sequence, ɓ^0, the intensity value per pixel is defined as binary digits, one by one. To obtain the index sequence, $k^{\hat{y}}$, in ascending order, the hyperchaotic sequence, k, is organized.
2. ɓ^0 is globally shuffled to be a one-dimensional binary sequence depending on the index sequence, $k^{\hat{y}}$; $\text{ɓ}^1_{\text{ᶖ}} = \text{ɓ}^0_{k^{\hat{y}}_{\text{ᶖ}}}, \text{ᶖ} \in [1, 8mn]$.

GBS is produced via a complex nonlinear relationship between the input and the encrypted images, which enhances security.

The Encryption and Decryption Process are carried out in seven steps:

1. $m \times n$ indicates the input image $(F)'s$ size. The binary sequence, ɓ^1, is achieved through GBS operation on an image, F.
2. According to the first DNA coding rule, ɓ^1 is encoded in a DNA sequence, d^1. The DNA addition to each element of d^1 is executed to obtain d^2 [28];

$$d^2 = \begin{cases} d^2_1 {=} \mathrm{d}_0 {+}{+} d^1_1 \\ d^2_{\text{ᶖ}} {=} d^2_{\text{ᶖ}-1} {+}{+} d^1_{\text{ᶖ}} \end{cases} \qquad \text{ᶖ} \in [2, 4mn] \tag{20}$$

   where $++$ indicates the DNA addition process and d_0 is a specific initial value.
3. A sequence, $k^v = [k_1, k_2, \ldots, k_{mn}]$, is reduced from k, and the decimal sequence, k^v, is transformed into binary digits, b^k. According to the third DNA encoding rule, b^k is encrypted into d^k. To obtain a sequence, d^3, DNA addition among d^2 and d^k is performed.
4. A threshold function, $f(s)$, is expressed as follows [28]:

$$f(s) = \begin{cases} 0\,, 0 \leq \frac{s}{255} \leq 0.5 \\ 1,\ 0.5 < \frac{s}{255} \leq 1 \end{cases} \tag{21}$$

A cut sequence of k, $[k_1, k_2, \ldots, k_{4mn}]$, is converted to a mask sequence, w, using Equation (21). The mask sequence, w, and d^3 are utilized to create d^4. To obtain $d^4_{\text{ᶖ}}$, the corresponding $d^3_{\text{ᶖ}}$ is complemented. If $w_{\text{ᶖ}} = 1$, or else it is not varied. This is how the DNA sequence, d^4, is obtained.

5. To obtain the binary sequence, ɓ^2, d^4 is decoded using the first DNA coding rule.
6. To obtain the encrypted binary sequence, ɓ^3, bitwise XOR is executed between ɓ^2 and ɓ^{k}.
7. The encrypted binary sequence, ɓ^3, is converted to an encrypted image, T. The decryption process is identical to that of encryption in reverse order.

4. Simulation Results

This section discusses the performance of the proposed C-DL-NOMA system, based on different chaotic maps, through simulation results. This simulation was performed using MATLAB. The impacts of various chaotic maps assigned to Users 1, 2, and 3 on SISO DL power-domain NOMA performance, in terms of BER and some security analyses, were demonstrated via the simulation results. The proposed model for evaluating the quality of the system performance was simulated based on the parameters listed in Table 1.

4.1. Security Analysis

Regarding encryption, simply encrypting data is insufficient. Encrypted data should be extremely reliable. Some security analyses, such as statistical analyses represented by histogram and correlation analyses (Figure 8) and information entropy analysis (Table 2), must be performed to demonstrate high reliability.

Table 1. Simulation parameters.

Monte Carlo Simulation	MATLAB Programming
User Number	Three Users (U_1, U_2, U_3)
Data Type/Size	Image Message/(128 × 128)
Bandwidth	1 MHZ
Transmit SNR	0 to 40 dB
Thermal Noise Density	$\text{Log}_{10}(\text{kT}) = -174$ dBm/Hz
Path Loss Exponent	4
Modulation Scheme	QPSK
Channel Type	AWGN and Rayleigh-Fading Channel
Number of Antennas	Tx = 1, Rx = 1
Power Allocation Factors	$a_1 = 0.62,\ a_2 = 0.3,\ a_3 = 0.08$
Distances (m)	$d_1 = 186,\ d_2 = 90,\ d_3 = 24$
Cryptographic Algorithm	Chaotic Map-Based Cryptography

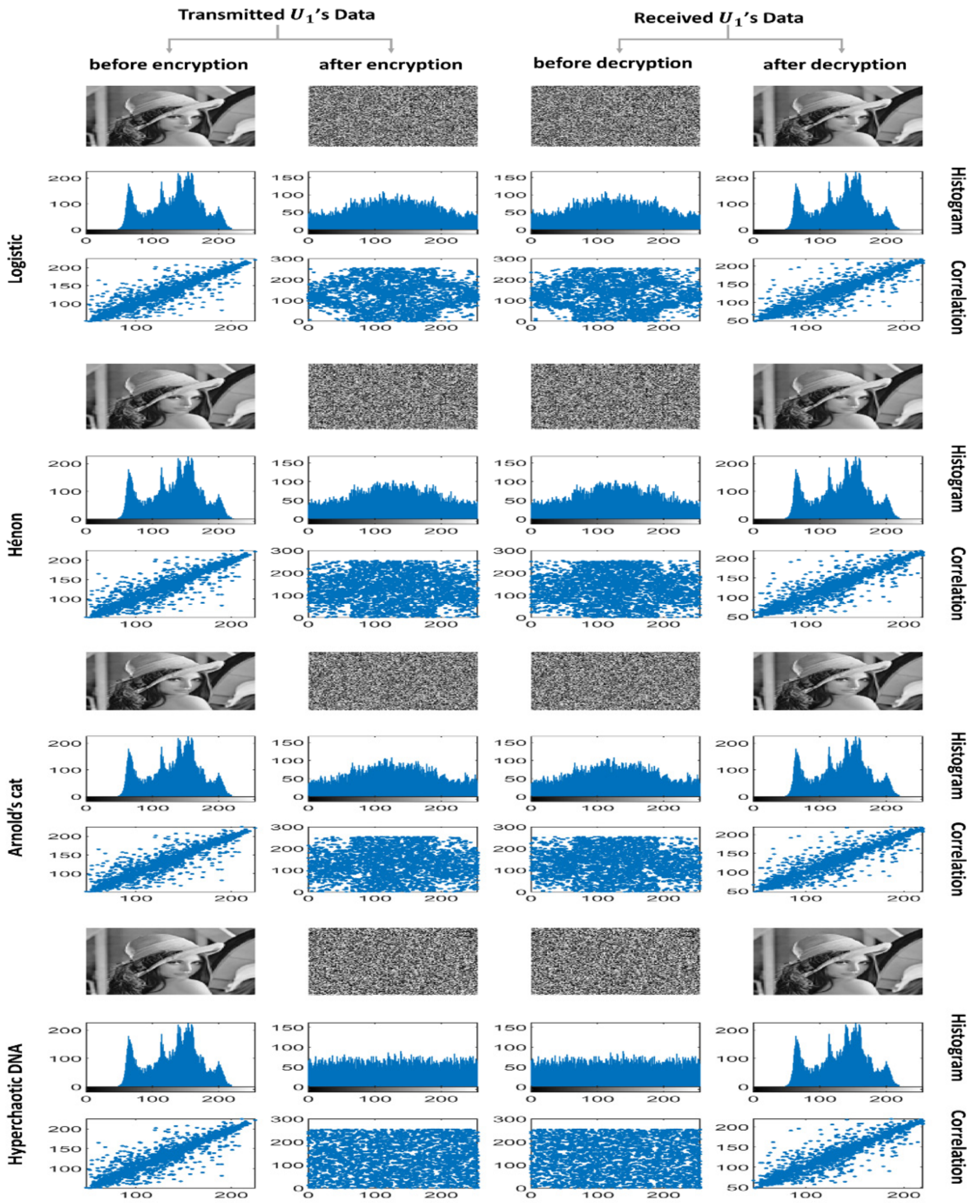

Figure 8. Histogram and correlation analyses.

Table 2. Information entropy of encrypted images.

	Logistic	**Hénon**	**Arnold's Cat**	**Hyperchaotic DNA**
U_1**'s Data**	7.9974	7.9963	7.9977	7.9964
U_2**'s Data**	7.9967	7.9975	7.9969	7.9979
U_3**'s Data**	7.9982	7.9984	7.9987	7.9985

4.1.1. Statistical Analysis

Because the efficiency of an encryption system is determined from its ability to reject statistical attacks, statistical analyses are utilized to distinguish original data from encrypted data. Such statistical analyses are discussed below.

Histogram Analysis

A histogram distribution is a graphical representation of data distribution. It comprises the frequency of the data group. Several fields can use histogram analysis. Encryption is effective if the histogram's distribution of the ciphered data has similar values. The closer the values of a data set are to each other, the more difficult it is to decode encrypted data. The histogram distribution in the image data is from left to right, that is, from dark to light colors. On the left side, dark colors prevailing indicate much distribution, whereas on the right side, light colors prevailing indicate much distribution. For this reason, the more uniform the distribution is, the more difficult it is to form a thought of the image or decode the ciphered data. Notably, hyperchaotic DNA has a better histogram distribution than do the logistic, Hénon, and Arnold's cat maps because its ciphered data has similar values (Figure 8).

Correlation Analysis

Correlation analysis is commonly used in image-data security analysis. For correlation analysis to be useful, the relationship among variables must be linear. Testing the relationship among adjacent pixels can be used to execute correlation analysis.

The relationship among the variables on the plain image is linear, whereas the relation after analysis is nonlinear (scattered) with a highly complex distribution, and a correlation value close to zero indicates that the analysis result is good and there is no relation between the two images. An adjacent pair of pixels in any number is chosen at random from the image; the correlation coefficient of each pair is calculated using the following formulas [18]:

$$E(\text{Ꭓ}) = \frac{1}{\tilde{\text{N}}}\sum_{\text{ɨ}=1}^{N} \text{Ꭓ}_{\text{ɨ}} \tag{22}$$

$$E(\text{Ꭓ}) = \frac{1}{\tilde{\text{N}}}\sum_{\text{ɨ}=1}^{N} \text{Ꭓ}_{\text{ɨ}} \tag{23}$$

$$\text{cov}(\text{Ꭓ}, \text{Ӌ}) = \frac{1}{\tilde{\text{N}}}\sum_{\text{ɨ}=1}^{N} \left(\text{Ꭓ}_{\text{ɨ}} - E(\text{Ꭓ})\right)\left(\text{Ӌ}_{\text{ɨ}} - E(\text{Ӌ})\right) \tag{24}$$

$$r_{\text{ᎫӋ}} = \frac{\text{cov}(\text{Ꭓ}, \text{Ӌ})}{\sqrt{D(\text{Ꭓ})D(\text{Ӌ})}} \tag{25}$$

X̄ and Ч are the grayscale values of the two adjacent pixels in the image, and Ñ refers to the total number of pixels chosen from the image. In the horizontal direction, 3000 pairs of adjacent pixels are chosen at random from the images to display their adjacent pixel distribution maps. This indicates that input images have a strong correlation effect, whereas encrypted images have a weak correlation impact, confirming that robust correlation is absent among adjacent pixels in encrypted images. As shown in Figure 8, through the four chaotic encryption schemes, the hyperchaotic DNA algorithm has a good encryption effect that damages correlation and achieves the weakest correlation impact.

4.1.2. Information Entropy Analysis

The information entropy of an image can reveal its information repeatability. The density of an eight-bit grayscale image has 2^8 possible values, so its ideal information entropy value is 8. If the encoded image's information entropy is closer to 8, it is closer to random distribution. Information entropy is described below [33]:

$$\text{Information entropy } (\underline{\mathrm{T}}) = -\sum_{i=0}^{2^{n_b-1}} P\left(\underline{\mathrm{T}}_{\text{ị}}\right) \log_2 P\left(\underline{\mathrm{T}}_{\text{ị}}\right) \tag{26}$$

where Ṯ indicates the encrypted image, n_b indicates the total number of bits that represent the symbol $\underline{\mathrm{T}}_{\text{ị}}$, and $P(\underline{\mathrm{T}}_{\text{ị}})$ indicates the probability that $\underline{\mathrm{T}}_{\text{ị}}$ will appear. The information entropy of the encrypted images is computed. As listed in Table 2, the encrypted images were close to a random source, and the proposed systems were sufficiently secured against entropy attacks.

4.2. Numerical Results

4.2.1. Bit Error Rate (BER)

Figure 9 shows the BER versus the transmission SNR (dB) for each user in the four C-DL-NOMA schemes. Notably, the closest user (User 3) had the worst performance because two levels of SIC were performed for User 3, whereas User 2 outperformed User 3 because one level of SIC was performed at User 2. Otherwise, since User 1 demodulated the data directly without performing SIC, this user provided the best performance. In addition, we can see that the logistic scheme had the best BER performance and that the BERs of the Hénon and Arnold's cat schemes were semisimilar, as they used the same method to generate key values. Finally, the hyperchaotic DNA scheme had the worst BER performance among the rest of the schemes because of the number of layers in the encryption and decryption processes. Compared with the 3 UE's SUI-6 model in [14], we obtained better BER performance.

In Table 3, we chose the BER to be 10^{-3} to compare the achieved SNR (dB) per user in the four C-DL-NOMA schemes and the 3 UE's SUI-6 model in [14]. The closest user (User 3), with the lowest power factor and two levels of SIC, achieved a BER of 10^{-3} at SNRs of 30 dB for NOMA with no encryption, 30.1 dB for the logistic scheme, 33.3 dB for the Hénon and Arnold schemes, and 33.6 dB for the hyperchaotic DNA scheme; the second-nearest user (User 2), with a single level of SIC, achieved a BER of 10^{-3} at SNRs of 26.8 dB for NOMA with no encryption, 26.9 dB for the logistic scheme, 29.5 dB for the Hénon and Arnold schemes, and 29.6 dB for the hyperchaotic DNA scheme; and the farthest user (User 1) achieved a BER of 10^{-3} at SNRs of 19.6 dB for NOMA with no encryption, 19.8 dB for the logistic scheme, 22 dB for the Hénon and Arnold schemes, and 22.18 dB for the hyperchaotic DNA scheme.

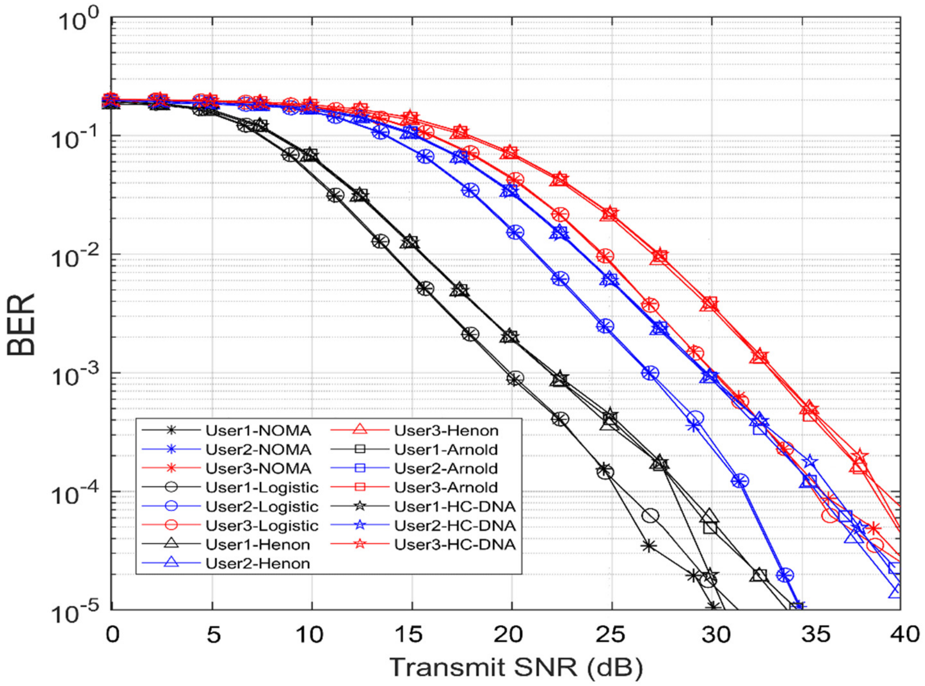

Figure 9. BER performance for the four C-DL-NOMA schemes with three users.

Table 3. BER performance for the four C-DL-NOMA schemes with three users.

	User 1	**User 2**	**User 3**
	SNR (dB)	**SNR (dB)**	**SNR (dB)**
NOMA	19.6	26.8	30
Logistic	19.8	26.9	30.1
Hénon	22	29.5	33.3
Arnold's Cat	22	29.5	33.3
Hyperchaotic DNA	22.18	29.6	33.6
Asif Mahmood [14]	26	30.5	-
BER	10^{-3}	10^{-3}	10^{-3}

4.2.2. Achievable and Sum Data Rates

Considering Equations (7) and (8), neither achievable nor sum data rates depend on transmitted data encrypted with different chaotic maps. Therefore, the rates for the four C-DL-NOMA schemes are similar. Figure 10 shows the simulation results of the achievable data rate per user and the sum rate versus the transmit SNR in dB. Notably, the achievable data rate of User 3 outperformed those of Users 1 and 2. Furthermore, the achievable data rates of Users 1 and 2 increased slightly in the low-SNR area and were saturated in the high-SNR area, but that of User 3 increased exponentially with the SNR because User 1 did not utilize SIC but only discovered the signal itself. Concurrently, User 2 needed to utilize first-order SIC first, after which User 3 should have utilized second-order SIC, implying that the effect of interference on User 1 was higher than on Users 2 and 3. Compared with the achievable rate for the three users in [34], we obtained a better data-rate performance.

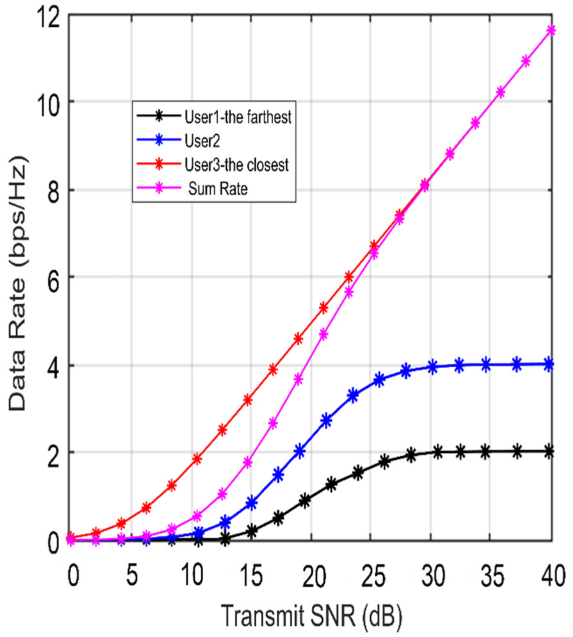

Figure 10. Achievable data rates and sum rates for the three users in C-DL-NOMA.

5. Conclusions

In this study, we proposed a C-DL-NOMA method to support data transmission security through SISO DL power-domain NOMA over the AWGN and Rayleigh-fading channels. The proposed method is based on a coherent analog modulation technique for CM of encrypted data, where different hybrid chaotic maps, such as the logistic, Hénon, hyperchaotic, and Arnold's cat maps, were considered. BER findings obtained utilizing various chaotic schemes confirmed the effectiveness of the proposed C-DL-NOMA model when compared to typical NOMA systems. Moreover, our DL power-domain NOMA with fixed allocated power factors based on the users' distances from the BS achieved better achievable-data-rate performance. In addition, the security analysis revealed that our proposed C-DL-NOMA model has robust PLS to support data-transmission security. Future studies can incorporate any type of noncoherent modulation to obtain high connectivity with various quality services. The proposed encryption method can be applied to code-domain NOMA. It can also use dynamic power-allocation factors based on channel-state information values in C-DL-NOMA to offer user fairness and maximize the sum rate.

Author Contributions: Conceptualization, M.A.A.-A. and M.A.M.; methodology, M.A.A.-A., K.A.S. and W.R.; software, M.A.A.-A. and W.R.; validation, M.A.A.-A., M.A.M., K.A.S. and W.R.; formal analysis, M.A.A.-A. and W.R.; writing—original draft preparation, M.A.A.-A.; writing—review and editing, M.A.M., K.A.S. and W.R.; supervision, M.A.M., K.A.S. and W.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhang, Z.; Sun, H.; Lei, X. Non-orthogonal Multiple Access. *Encycl. Wirel. Netw.* **2020**, 1–4. [CrossRef]
2. Kim, J.H.; Lee, W.S.; Song, H.K. Performance enhancement using receive diversity with power adaptation in the NOMA system. *IEEE Access* **2019**, *7*, 102867–102875. [CrossRef]
3. Shin, W.; Vaezi, M.; Lee, B.; Love, D.J.; Lee, J.; Poor, H.V. Non-orthogonal multiple access in multi-cell networks: Theory, performance, and practical challenges. *IEEE Commun. Mag.* **2017**, *55*, 176–183. [CrossRef]

4. Ghous, M.; Abbas, Z.H.; Hassan, A.K.; Abbas, G.; Baker, T.; Al-Jumeily, D. Performance analysis and beamforming design of a secure cooperative miso-noma network. *Sensors* **2021**, *21*, 4180. [CrossRef] [PubMed]
5. Melki, R.; Noura, H.N.; Chehab, A. Physical layer security for NOMA: Limitations, issues, and recommendations. *Ann. Telecommun.* **2021**, *76*, 375–397. [CrossRef]
6. Al-Musawi, I.; Al-Hussaibi, W.; Ali, F. Chaos-Based Physical Layer Security in NOMA Networks over Rician Fading Channels. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021. [CrossRef]
7. Horiike, N.; Okamoto, E.; Yamamoto, T. A downlink non-orthogonal multiple access scheme having physical layer security. *Eurasip J. Wirel. Commun. Netw.* **2018**, *2018*, 205. [CrossRef]
8. Masuda, Y.; Okamoto, E.; Ito, K.; Yamamoto, T. An uplink non-orthogonal multiple access scheme having physical layer security based on chaos modulation. In Proceedings of the International Conference on Information Networking, Kuala Lumpur, Malaysia, 9–11 January 2019.
9. Stallings, W. *Cryptography and Network Security: Principles and Practice 7th Global Edition*; William Stallings: England, UK, 2017.
10. Horiike, N.; Kitagawa, H.; Okamoto, E.; Yamamoto, T. Chaos MIMO-based downlink non-orthogonal multiple access scheme with physical layer security. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018.
11. Masuda, Y.; Okamoto, E.; Yamamoto, T. Low Complexity Decoding of Downlink Chaos NOMA Scheme with Physical Layer Security. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020.
12. Almusawi, I.; Al-Hussaibi, W.; Tahir, Y. Chaos-Based NOMA for Secure Wireless Communications over Rayleigh Fading Channels. In Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP 2020, Cyperspace, 28–30 June 2020.
13. Kucur, O.; Kurt, G.K.; Aldababsa, M.; Toka, M. Nonorthogonal Multiple Access for 5G and Beyond. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 4–5. [CrossRef]
14. Mahmood, A.; Khan, S.; Hussain, S.; Zeeshan, M. Performance Analysis of Multi-User Downlink PD-NOMA under sui Fading Channel Models. *IEEE Access* **2021**, *9*, 52851–52859. [CrossRef]
15. Agarwal, A.; Chaurasiya, R.; Rai, S.; Jagannatham, A.K. Outage Probability Analysis for NOMA Downlink and Uplink Communication Systems with Generalized Fading Channels. *IEEE Access* **2020**, *8*, 220461–220481. [CrossRef]
16. Mohammad, M.; Alavı, R.; Pehlivan, H.; Pour, S.H. Kaos Tabanlı Bir Şifreleme Yöntemi ve Analizi. In *Proceedings of the Akademik Bilişim Konferansı Bildirileri, 2–4 February, 2011*; İnönü University: Malatya, Turkey, 2011.
17. Akgül, A.; Kaçar, S.; Aricioglu, B.; Pehlivan, I. Text encryption by using one-dimensional chaos generators and nonlinear equations. In Proceedings of the 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 28–30 November 2013.
18. Akgul, A.; Kacar, S.; Pehlivan, I.; Aricioglu, B. Chaos-based encryption of multimedia data and design of security analysis interface as an educational tool. *Comput. Appl. Eng. Educ.* **2018**, *26*, 1336–1349. [CrossRef]
19. Raghava, N.S.; Kumar, A. Image Encryption Using Henon Chaotic Map With Byte Sequence. *Int. J. Comput. Sci. Eng. Inf. Technol. Res. (IJCSEITR)* **2013**, *3*, 11–18.
20. Sankhe, P.; Pimple, S.; Singh, S.; Lahane, A. An Image Cryptography using Henon Map and Arnold Cat Map. *Int. Res. J. Eng. Technol.* **2018**, *5*, 1900–1904. Available online: www.irjet.net (accessed on 17 November 2022).
21. Ratna, A.A.P.; Surya, F.T.; Husna, D.; Purnama, I.K.E.; Nurtanio, I.; Hidayati, A.N.; Purnomo, M.H.; Nugroho, S.M.S.; Rachmadi, R.F. Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion. *Adv. Sci. Technol. Eng. Syst.* **2021**, *6*, 316–326. [CrossRef]
22. Lozi, R. Complexity Leads to Randomness in Chaotic Systems. *Math. Sci. Technol.* **2011**, 93–125. [CrossRef]
23. Krishnaiah, J.; Kumar, C.S.; Faruqi, M.A. Modelling and control of chaotic processes through their Bifurcation Diagrams generated with the help of Recurrent Neural Network models: Part 1-simulation studies. *J. Process Control* **2006**, *16*, 53–66. [CrossRef]
24. Hanchinamani, G.; Kulkarni, L. An Efficient Image Encryption Scheme Based on: Henon Map, Skew Tent Map and S-Box. *3D Res.* **2015**, *6*, 30. [CrossRef]
25. Varvoglis, H. Chaos, Random Walks and Diffusion in Hamiltonian Systems. Available online: https://www.researchgate.net/publication/264419522_Chaos_random_walks_and_diffusion_in_Hamiltonian_systems (accessed on 17 November 2022). [CrossRef]
26. Dyson, F.J.; Falk, H. Period of a Discrete Cat Mapping. *JSTOR* **2013**, *99*, 603–614. [CrossRef]
27. Gao, Y.; Liang, C. A new 4D hyperchaotic system and its generalized function projective synchronization. *Math. Probl. Eng.* **2013**, *2013*, 1–13. [CrossRef]
28. El-Khamy, S.E.; Mohamed, A.G. An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion. *Multimed. Tools Appl.* **2021**, *80*, 23319–23335. [CrossRef]
29. Rehman, A.; Liao, X.; Kulsoom, A.; Abbas, S.A. Selective encryption for gray images based on chaos and DNA complementary rules. *Multimed. Tools Appl.* **2015**, *74*, 4655–4677. [CrossRef]
30. Li, C.L.; Yu, S.M. A new hyperchaotic system and its adaptive tracking control. *Wuli Xuebao/Acta Phys. Sin.* **2012**, *61*, 1–7. [CrossRef]

31. Zhan, K.; Wei, D.; Shi, J.; Yu, J. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J. Electron. Imaging* **2017**, *26*, 013021. [CrossRef]
32. Watson, D.; Acid, N. Molecular Structure of Nucleic Acids. *Nature* **1953**, *171*, 737–738. [CrossRef] [PubMed]
33. Talhaoui, M.Z.; Wang, X.; Talhaoui, A. A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. *Vis. Comput.* **2021**, *37*, 1757–1768. [CrossRef]
34. Kim, K.J.; Liu, H.; Lei, H.; DIng, Z.; Orlik, P.V.; Poor, H.V. A dCDD-Based Transmit Diversity Scheme for Downlink Pseudo-NOMA Systems. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 1217–1232. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.