

Secure Optical Communication Using a New 5D Chaotic Stream Segmentation

Nesreen M. Al-Saidi¹, Mudhafar H. Ali^{1*}, Waleed K.H. Al-Azzawi², Abdulla K.H. Abass³

¹ Computer Engineering Department, College of Engineering, Al-Iraqiya University, Baghdad 10054, Iraq

² Department of Medical Instruments, Medical Technical College, Al-Farahidi University, Baghdad 10022, Iraq

³ Laser and Optoelectronic Engineering Department, University of Technology, Baghdad 10066, Iraq

Corresponding Author Email: mudhafar.ali@aliraqia.edu.iq



<https://doi.org/10.18280/ijstdp.170519>

ABSTRACT

Received: 30 May 2022

Accepted: 3 August 2022

Keywords:

chaotic system, modulation, secure communication, multisim, encryption process

According to its complex properties like ergodicity, unpredictability, and sensitivity to its initial states, chaotic systems are attracting more and more attention and are widely used for security purposes. Moreover, the chaotic signals are considered suitable for spread spectrum modulation due to their wideband properties. It is able to reduce the peak to average power ratio (PAPA). This paper presents a new Dynamic Diffeo-Difference Multi-Dimensional (DDD-MD) system. It is used as a key for a new cryptosystem designed based on the chaotic stream segmentation (CSS) method. The proposed system provides the best trade-off between efficiency, robustness, and high data rate transmission. The behavior of the proposed chaotic system is evaluated numerically by analyzing the Lyapunov exponent spectrum, complexity, and attractor phase diagram. Besides, it is practically assessed based on the principle of system circuit design; the circuit diagram of the system is prepared and simulated by Multisim, which shows high consistency with the numerical simulation. These evaluations show that the proposed system has a rich dynamics behavior to be realized in an encryption system and provides a foundation for many engineering and physical applications.

1. INTRODUCTION

Some emerging technologies, such as chaotic systems, are considered a suitable choice for constructing secure encryption algorithms [1-5]. This is due to their promising features, namely, ergodicity, unpredictability, sensitivity to the initial condition, and generating random-like behavior sequences. These properties help enhance the security of the encryption/decryption system designed via chaotic systems. Therefore, such systems can guarantee to satisfy the security services, which are authentication, confidentiality, integrity, and non-repudiation. Furthermore, besides the security issue, chaotic systems are considered efficient because they can be implemented with high speed and low cost.

The information technology and communication era required sharing of digital data through public and private networks. So, protecting these data from vulnerable access is a challenge and an essential task. Encryption method based on some emerging techniques such as chaotic systems is one of the essential resources to ensure the protection of such documents. Most of the previous strategies were based on optical code [6-9] until a chaotic laser emerged that plays an important role in enhancing the security of optical communication [10-13]. In chaotic communication, the carrier is used to embed the message before sending it to the receiver side. Since then, many types of single and multi-carrier-based chaotic systems have appeared in the literature to achieve high-speed and broadband capability due to their wideband characteristic [14-16]. Besides, it produces a good synchronous signal, in which a big message is embedded into a chaotic carrier. Three categories for message encoding and

decoding using a laser system are introduced. These are; Chaos Masking (Ch-M), Chaos modulation (CM), and chaos shift keying (Ch-SK) [17-20]. Laser rate equations are used to describe and study the system's dynamic behavior. It is also used to formulate a mathematical equation in the transmitter and receiver sides. This paper proposes a new secure and high-speed optical communication scheme. It is based on designing a new 5D continuous chaotic system. The obtained chaotic signals are used as a key for the newly proposed encryption method using the principle of segmentation. The proposed cryptosystem was implemented for image encryption in this work. It shows high performance using some evaluation criteria.

The significant contributions in this work are as follows:

- (1) Proposing a new 5D continuous chaotic system to be used as a key generation.
- (2) Some numerical evaluation assesses the efficiency of the proposed chaotic system to investigate its dynamic properties
- (3) A circuit diagram of the proposed chaotic system is sketched based on the circuit design principle. Then it was simulated using Multisim software. It is used as a practical evaluation to consist the numerical simulation results and to demonstrate the realization of the proposed system for many applications.
- (4) A new cryptosystem is designed based on chaotic masking between the input and keystream.
- (5) The proposed cryptosystem is used in an optical communication system to ensure data security that transfers through this channel.
- (6) The images are used as a type of data encrypted before transmission. The performance evaluation for the encrypted

images is assessed based on some statistical analysis to prove the quality and efficiency of the proposed cryptosystem.

The organization of the remaining work is arranged as follows: Section 2 introduced a new hyperchaotic continuous system. Its dynamical evaluations to generate keys for the proposed encryption method are discussed in Section 3. Section 4 introduced the encryption and decryption algorithms. The workflow of the optical communication system is presented in Section 5. The results and their analysis utilizing different metrics used to evaluate the proposed method's efficiency and security are discussed in Section 6. Finally, the paper is concluded in Section 7.

2. THE PROPOSED CHAOTIC SYSTEM

A new 5D dynamical system is introduced based on the ND-Lorenz design [21]. This system is specified as follows: For $i=1, \dots, N \gg 4$:

$$\frac{dx_i}{dt} = (x_{i+1} - x_{i-2})x_{i-1} - x_i + Cx_i \quad (1)$$

where, it is expected that $x_0=x_N$ and $x_I=x_{N+1}$ at this point, x_i is the formal of the model, and C is an imposing constant (just like fixed force). It is a joint value known to affect chaotic conduct. Therefore, the proposed system is constructed mathematically by the following differential equations given in system (1). This system is called Dynamic Diffeo-Difference of Multiple Dimension (DDD-MD).

$$\begin{aligned} f(1) &= (y - w)u - x + ax \\ f(2) &= (z - u)x - y + by \\ f(3) &= (w - x)y - z + cz \\ f(4) &= (u - y)z - w + dw \\ f(5) &= (x - z)w - u + eu \end{aligned} \quad (2)$$

where, $x, y, z, w,$ and u are the state variables, and $a, b, c, d,$ and e are positive parameters.

3. NUMERICAL ANALYSIS OF (DDD-MD)

The dynamic properties of (1) are investigated through some multifarious dynamics such as; phase space (Figure 1), Lyapunov exponent (Figure 2), and sample entropy (Figure 3). The constant parameters (a, b, c, d, e) are chosen after intensive numerical analysis to ensure a high chaosity of the proposed system.

3.1 System attractor

As an indication of the system that has rich dynamics when its attractor in the phase space is complex. In our proposed 5D-hyperchaotic system, we found that it has a rich dynamic, which is oblivious from the projections of the attractors into different plans as shown in Figure 1 for the values of the parameters are $a=1, b=3, c=0.09, d=0.1, e=0.01$. This figure shows that the phase space is very complex and has disordered dynamic behavior.

3.2 Lyapunov exponents of DDD-MD

As an indication of the system that exhibits new behavior,

we use the Lyapunov Exponents (LE), which is a quality used to measure the exponential rate of convergence or divergence of two adjacent trajectories in the dynamical system. Its positive values refer to the chaosity of the given system. When more than one positive value considers that the system is hyperchaotic, we found that our proposed chaotic system is hyperchaotic by applying this evaluator. When the parameters values are: $a=1, b=3, c=0.09, d=0.1,$ and $e=0.01$.

3.3 Sample entropy

Based on the Shannon entropy, determining the amount of information needed to predict the new output in the system trajectory based on previous time output is known as sample Entropy (SamEn). Its higher value indicates the high complexity or irregularity of the given system. Figure 3 shows the reasonable complexity and irregularity of the system (1).

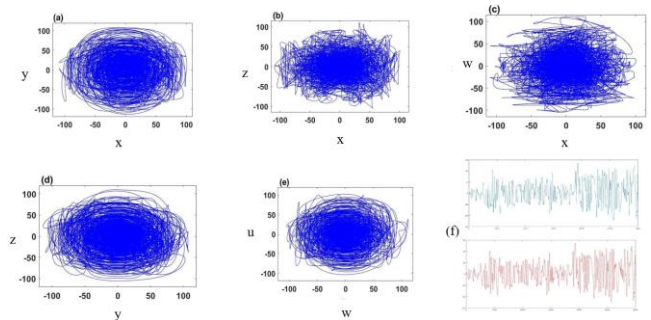


Figure 1. (a), (b), (c), (d), and (e) Phase space of system (1) for the parameters values $a=1; b=3; c=0.09; d=0.1; e=0.01$; (f) represent the plot of one axis in the face plane

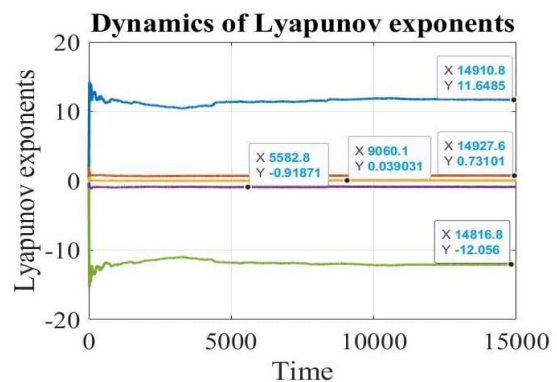


Figure 2. Lyapunov exponent of system (1) for the parameters $a=1; b=3; c=0.09; d=0.1; e=0.01$

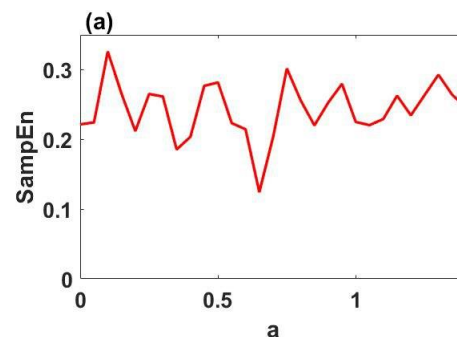


Figure 3. Sample Entropy of system (1) based on the parameter a , where the other parameters are: $b=3; c=0.09; d=0.1; e=0.01$

4. PRACTICAL EVALUATION USING CIRCUIT DESIGN WITH MULTISIM

The circuit design of the system (1) is developed to realize the proposed chaotic system. It is designed by the modular circuits using different resistance values and capacitors amplifier LM741 and the multipliers AD633 and $1/s^{0.96}$. This can be seen obviously in Figure 4. The limited voltage of LM741 and AD633 reduces the linearity of (1) to 0.1 times the original circuit [22, 23].

The simulation of the designed analog circuit by adjusting the horizontal axis is performed using Multisim12 for the circuit simulator. Finally, it is implemented on the oscilloscope to show the real-time results, as presented in Figure 4.

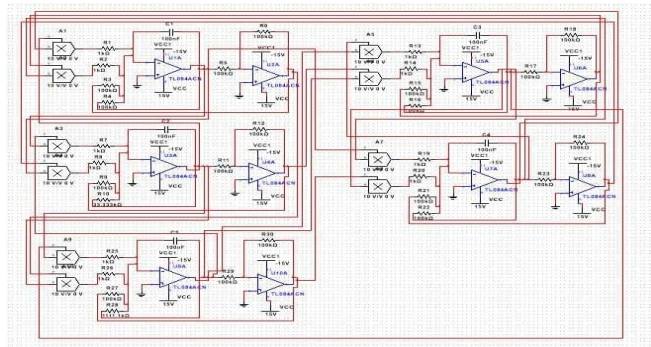


Figure 4. Circuit design of the system (1)

The state equation for the design in Figure 3 is given by:

$$\begin{aligned}
 c_1 x_1' &= \left(\frac{yu}{10 R_1} - \left(\frac{wu}{10 R_2} \right) \left(\frac{R_{24}}{R_{23}} \right) \right) - \left(\frac{R_6}{R_5} \right) \left(\frac{x}{R_3} \right) + \frac{ax}{R_4} \\
 c_2 y_1' &= \left(\frac{zx}{10 R_7} - \left(\frac{ux}{10 R_8} \right) \left(\frac{R_{30}}{R_{29}} \right) \right) - \left(\frac{R_{12}}{R_{11}} \right) \left(\frac{y}{R_9} \right) + \frac{by}{R_{10}} \\
 c_3 z_1' &= \left(\frac{wy}{10 R_{13}} - \left(\frac{xy}{10 R_{14}} \right) \left(\frac{R_{18}}{R_{17}} \right) \right) - \left(\frac{R_{18}}{R_{17}} \right) \left(\frac{z}{R_{15}} \right) + \frac{cz}{R_{16}} \\
 c_4 w_1' &= \left(\frac{uz}{10 R_{19}} - \left(\frac{yz}{10 R_{20}} \right) \left(\frac{R_{12}}{R_{11}} \right) \right) - \left(\frac{R_{24}}{R_{23}} \right) \left(\frac{w}{R_{21}} \right) + \frac{dw}{R_{22}} \\
 c_5 u_1' &= \left(\frac{xw}{10 R_{25}} - \left(\frac{zw}{10 R_{26}} \right) \left(\frac{R_{18}}{R_{17}} \right) \right) - \left(\frac{R_{30}}{R_{29}} \right) \left(\frac{u}{R_{27}} \right) + \frac{eu}{R_{28}}
 \end{aligned} \quad (3)$$

$$\begin{aligned}
 R_1 = R_2 = R_7 = R_8 = R_{13} = R_{14} = R_{19} = R_{20} = \\
 R_{25} = R_{26} = 1k\Omega \\
 R_3 = R_4 = R_5 = R_6 = R_9 = R_{11} = R_{12} = R_{15} = \\
 R_{21} = R_{22} = R_{23} = R_{24} = R_{27} = R_{28} = R_{29} = \\
 R_{30} = 100k\Omega \\
 R_{10} = 33.333k\Omega \\
 R_{16} = 1111.1k\Omega
 \end{aligned}$$

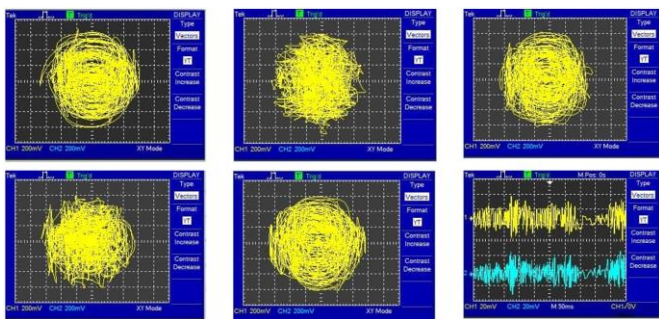


Figure 5. The attractors of the chaotic system (1), such that (a) xy , (b) xz , and (c) yz , (d) xu , and (e) xw , (f) represent one axis phase plane

After setting the right hand side of the system (1) equal to zero, we get $R_1=R_7=R_8=1k\Omega$, $R_4=R_5=R_{11}=R_{12}=100 k\Omega$, and $R_3=R_8=R_{10}=0.6666 k\Omega$, where $C_1=C_2=C_3=100$ nf. According to this circuit design, the implementation results for the time domain of x, y, z , are shown in Figure 5 (a-f).

4.1 The proposed cryptosystem

A new encryption method is proposed; it is based on the principle of stream segmentation. The DDD-MD system is used to provide the key. It is called the Chaotic Stream Segmentation (CSS) method. The schematic diagram of the proposed CSS method is illustrated in Figure 6. This method is used to encrypt different types of inputs (text, images, voice, etc.). It shows high encryption efficiency according to the used performance analyzes (histogram, Number of pixel change rate (NPCR), unified averaged changed intensity (UACI), correlation coefficient analysis, and information entropy). The algorithm of the proposed cryptosystem is presented as follows:

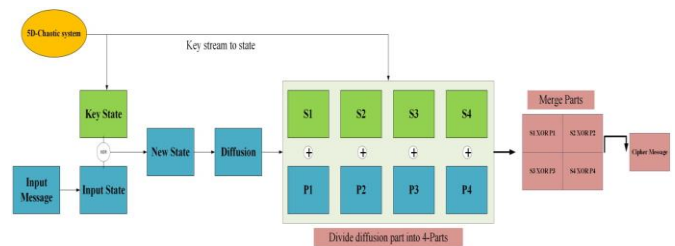


Figure 6. Schematic diagram for the CSS method

The Algorithm of the proposed cryptosystem

I. Key generating part

Key generating is the main part of any encryption scheme. When the keyspace is large, it is resulted in a highly secure system to resist brute force attack. In this work, this property is achieved because we used a chaos system for generating the key

Input: the chaotic system (1)

Initial condition $k=\{x_{10}, x_{20}, x_{30}, x_{40}, x_{50}, a_0, b_0, c_0, d_0, e_0\}$

Output: state as square arrangement, in which each pixel is 8 bits.

1. In each call, a different initial condition is used, which results in generating a different state.
2. Solving system (1) to find the trajectories using the given initial conditions with the help of 4-step Range Kutta method.
3. Iterates system (1) for m times to generate a chaotic sequence $X=\{x_1, x_2, \dots, x_m\}$.
4. Arrange the keystream generated by the system (1) in a matrix form with the same size of the given input such that $S_{ij} = \sum_{L=1}^5 x_{jL}$ when $i=1, \dots, m$, and $j=1:5$

II. Encryption part

Input: (image P of size $m \times n$)

Output: Cipher image C

1. Generate S matrix, the same size as P
 $SP = XOR(S, P)$
2. Do the following permutation to perform the diffused property
 - I. $a = \text{sort } SP$ in ascending order
 - II. Use the next steps to permute a :
 For $i=1$ to n


```

For j=1 to m
  For k=1 to m
    If a(j,i) = SP(k,i)
      t(j,i) = perm(k,i)
    k=m+z
  End
End k
End j
End i
NSP=t

```

3. Partition NSP into four parts (SP_1, SP_2, SP_3, SP_4)
4. Generate four new states $S_{ij}^z, z=1, \dots, 4$ each with the same size of SP_i .
5. For $i=1:4$

```

ST_i = XOR(S^i, SP_i)
End

```
6. Merge the output of step 6 in one state arrangement such that: $OP=[ST_1, ST_2; ST_3, ST_3]$
7. $C=OP$ % the cipher image

III. Decryption part

The decryption is the reverse of the encryption part.

5. THE PROPOSED COMMUNICATION SYSTEM

This section proposes a new design for the secure optical communication system, as shown in Figure 7. It is based on secure chaotic modulation.

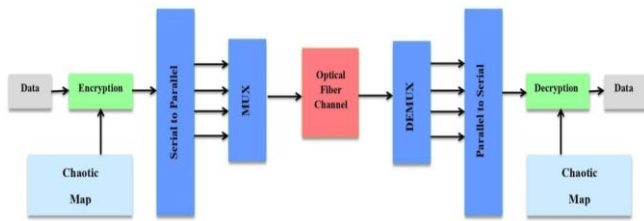


Figure 7. Design of secure optical communication system

5.1 Multi-carrier chaotic masking modulation (MCCMM)

Single carrier modulation approaches have grown more common in communication applications. Multicarrier modulation (MCM) gains a lot of attraction to improve the signal processing techniques.

In this part, the chaos masking technique has been proposed with multi-carrier modulation. This model can create c_i (where $i=1, 2, 3, \dots, N$) chaotic sequences, which may be used to build masking vectors. To create masking vectors, we use the binary form of the chaotic sequences c_i , which may be represented as c_1, c_2, \dots, c_N , to make the chaotic sequences more unpredictable. First, the symbols in the supplied data are divided into sub-sequences. Then, the masking vectors are created by assigning different beginning values to separate sub-sequences. Figure 8 illustrates the multi-masking design.

Multi-carrier approaches can improve data transmission rates. The Wavelength Division Multiplexing (WDM) technology is a key technique for achieving high data rates (increasing the transmission capacity of optical communication systems). WDM is a potential technology for exploiting the optical fiber's huge bandwidth. It is a technique

for simultaneously transmitting two or more optical signals on the same fiber. WDM divides the optical transmission spectrum into a number of non-overlapping wavelength bands. The multiplexer combines signals from many sources and feeds them into the transmission channel, an optical fiber. A de-multiplexer separates the signals at the receiving side, in which the photo-detectors can detect them.

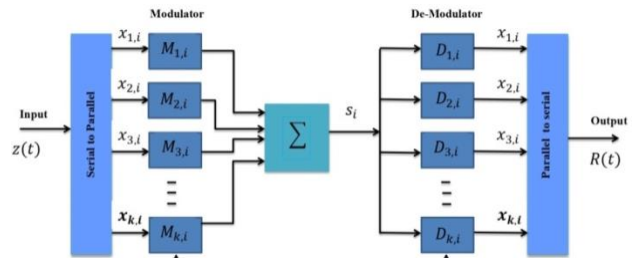


Figure 8. Multi-carrier chaotic masking

6. CRYPTANALYSIS AND EXPERIMENTAL RESULTS

In this section, several performance criteria are used to assess the efficiency of the proposed cryptosystem. The obtained result is also compared with other high-performance systems. The designed system has a high ability to encrypt various image types. This can be accomplished by converting images into random pixels, which are difficult to recognize without any knowledge of the original images. The implemented encryption system for different types of images (color and grayscale images) with the histograms of both of them is shown in Figure 9.

6.1 Histogram

A histogram is used to interpret the numerical data visually. It shows the number of points within a particular range of data. Besides, it can be used to display the value of the data frequency and their distribution, which displays its outliers or gaps. The histogram of the input images and the encrypted images are shown in Figure 9. Obviously, there is a significant difference between them. As a result, we may conclude that the given algorithm is statistically resistant.

6.2 Correlation analysis

The correlation measure effectively specifies the link between two existent random variables. It can be described as the relationship between two neighboring pixels in an image. As a result, the proposed encryption is utilized to shatter the association between image adjacent pixels, and the correlation value after encryption relates to the encryption system's efficiency. Figure 10 depicts the results of parrot image correlation in three orientations (horizontal, vertical, and diagonal). The correlation values can be calculated using the following equations:

$$CA = \frac{E(x-E(x))E(y-E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

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

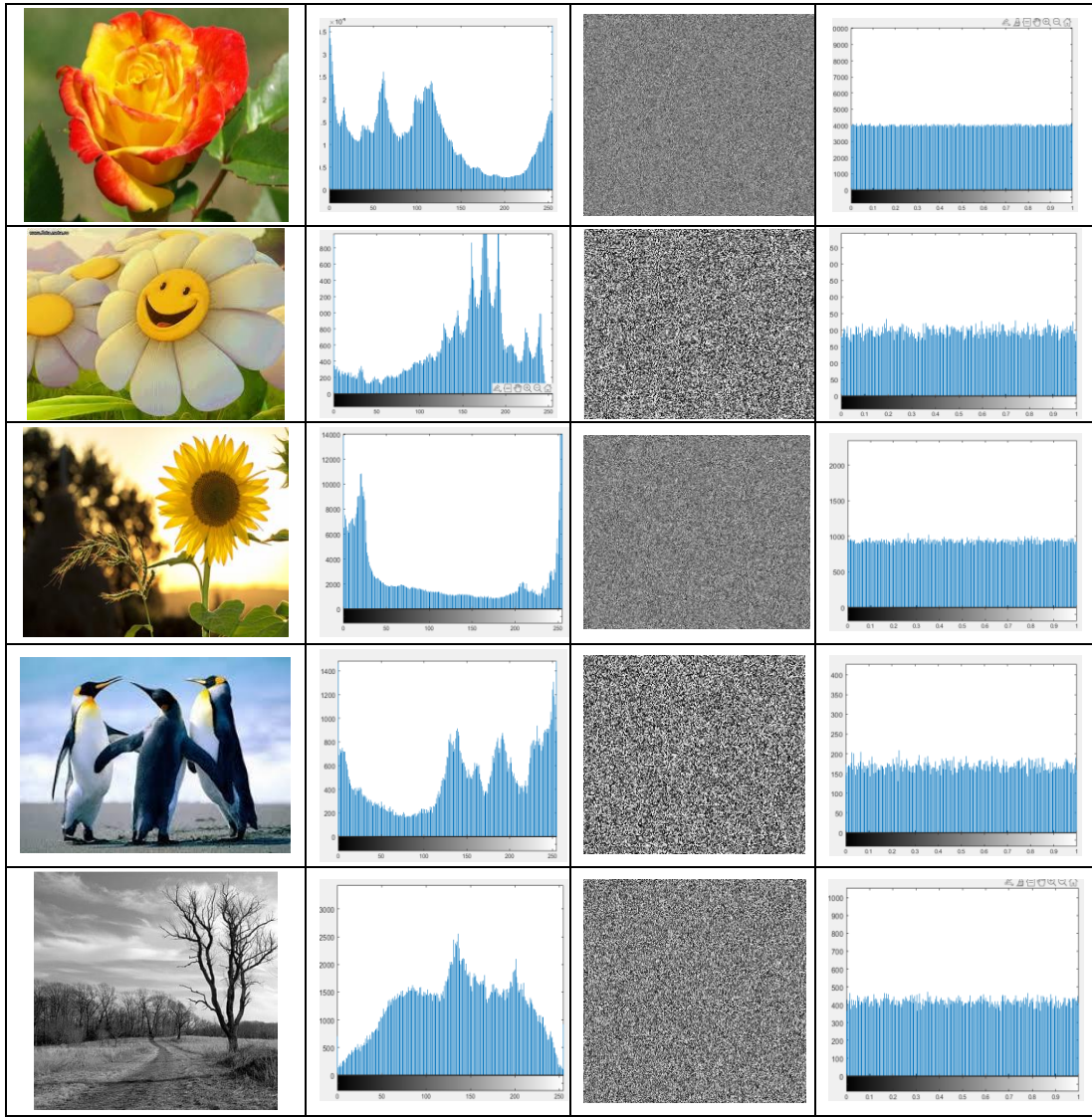
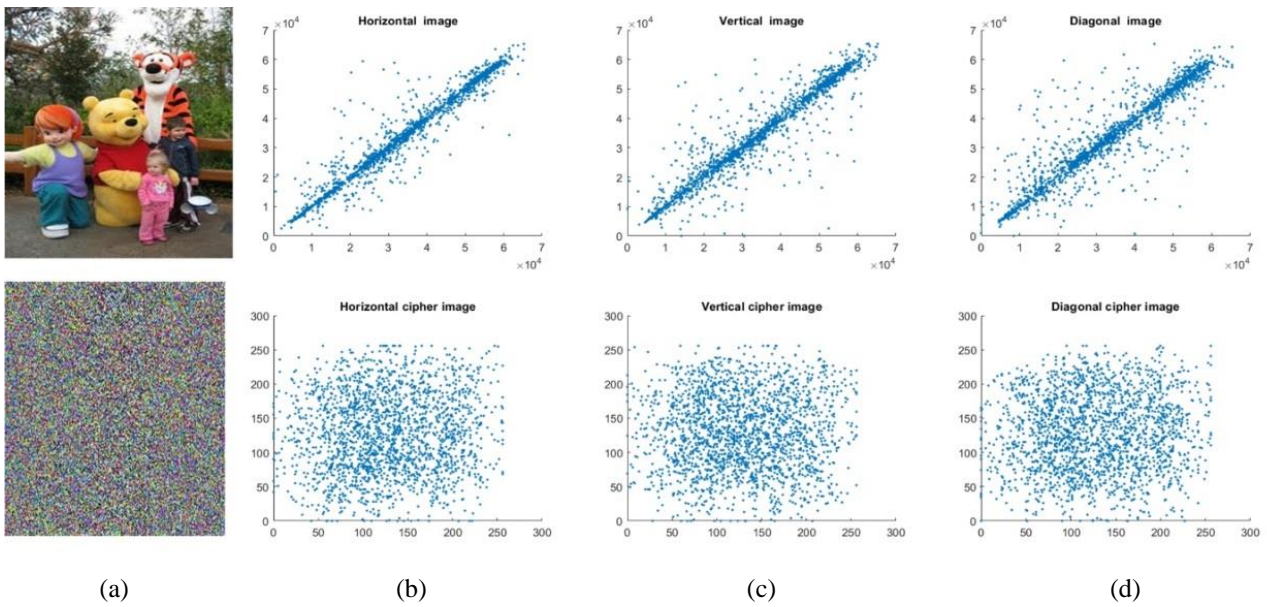


Figure 9. The of simulation results of CSS: (a) Color and grayscale plain images; (b) the histogram of (a); (c) cipher images of (a); (d) the histogram of (c)



(a) (b) (c) (d)

Figure 10. Pixels correlation: (a) the plain and cipher images, along with the directions of (b) horizontal, (c) vertical, and (d) diagonal

The fundamental goal of the encryption process is to break the correlation between pixels. The correlations between pixels in the original image are strong, whereas the correlations between pixels in the encrypted image are weak since these pixels are distributed randomly. As a result, the efficiency of the encryption system is indicated by how low the correlation value is. Some results for the correlation of pixels that have been used previously are shown in Table 2. Table 3 shows the comparison with some literatures results based on the correlation coefficients factor.

6.3 Information entropy

The entropy of information is a measure of disorder or unpredictability and thus of uncertainty. As a result, entropy can be used to evaluate the relevance of a ciphering approach. The effectiveness of the encryption algorithm is assessed with higher entropy. A message source's entropy $H(s)$ is defined as:

$$H(s) = - \sum_{i=0}^{2N-1} P(s_i) \log_2 P(s_i) \quad (5)$$

where, s is the source, N is the gray level number with a probability $P(s_i)$.

For completely random images, the value of $H(s)$ is recommended to be equal to 8. However, the proposed encryption algorithm is considered secured based on the entropy values presented in Table 1.

6.4 Differential attack

Another security criterion is the differential attack resistance, which is based on the sensitivity of ordinary images to change. The sensitivity to any change in the value of the pixels indicates that the encryption system is highly resistant to differential attacks. This attack is evaluated using two statistical tests: The NPCR (denotes the number of pixels

change rate in the encrypted image when changing one pixel in the plain image) and the UACI (used to measure the average intensity for the differences between inputs and encrypted images). Their ideal values are close to 100% and 33.33, respectively. To evaluate the ability of the proposed encryption method, some images are chosen, in which the average values are obtained by selecting their pixels randomly. The results in Table 1 show the high security of the proposed system against a differential attack. Eqns. 6, 7 that calculate the UACI and NPCR are given by:

$$UACI = \frac{\sum_{i=1}^N \sum_{j=1}^M |C1(i, j) - C2(i, j)|}{255 \times M \times N} \times 100\% \quad (6)$$

where, M , and N are the image's width and height, respectively, for an 8-bit image, and $C_k(i, j)$ represents the pixels of the ciphered image.

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^{MN} D(i, j)}{M \times N} \times 100\% \quad (7)$$

where, $D(i, j) = \begin{cases} 1, & \text{if } C1 \neq C2 \\ 0, & \text{if } C1 = C2 \end{cases}$, $C1$ and $C2$ are the two cipher images, M and N are the images' width and height, respectively.

The key sensitivity of the hyperchaotic system is examined by a little change in the initial values (x_0, y_0, z_0, w_0, u_0) or the control parameters (a, b, c, d, e). The UACI identifies the mean intensity of the difference in the two encrypted images, whereas the NPCR calculates the ratio of the different pixel counts between two encrypts images. Tables 4, and 5 show the key sensitivity based on tiny change in the system variables and control variables.

However, the deviation between the plain and encrypted image measures the encryption quality. The quality of the proposed encryption method is presented in Table 1, which shows good performance quality.

Table 1. The security tests






Image	Image dimension	Correlation coefficient	Entropy	UACI	NPCR
	1200×857	-0.0016	7.9583	33.30	99.60
	251×201	-0.0041	7.9566	33.78	99.43
	600×400	-0.0018	7.9589	33.73	99.74
	241×181	-0.0079	7.9546	33.82	99.43
	317×340	-0.0047	7.9573	33.46	99.38

Table 2. The correlations of some images in three directions (horizontal, vertical, and diagonal)

Name	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
tree	0.986980	0.990941	0.975238	0.00588	0.005920	0.005483
Winnie	0.903037	0.994729	0.959772	0.002021	0.001798	0.002173
ship	0.960820	0.949095	0.927689	0.006270	0.005713	0.005263

Table 3. The comparison with some other literature based on correlation coefficients factor

Direct	Plain image	Our proposal	Ref. [24]	Ref. [25]	Ref. [26]
Horizontal	0.98423	0.002182	0.0065	0.0230	0.0030
Vertical	0.99315	0.002131	0.0035	0.0019	0.0024
Diagonal	0.97691	0.002331	0.0036	0.0034	0.0034

Table 4. Key sensitivity based on tiny change in the system variables

Images	X ₀		Y ₀		Z ₀		W ₀		U ₀	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
Rose	99.6034	33.463	99.60934	33.4633	99.60933	33.46354	99.60937	33.46354	99.60933	33.4634
Lena	99.60934	33.4636	99.60935	33.4635	99.60937	33.46354	99.60934	33.46354	99.60934	33.46354
Tree	99.60934	33.4636	99.60937	33.4635	99.60933	33.46354	99.60935	33.46354	99.60932	33.4635

Table 5. Based on tiny change in the system variables

	a		b		c		d		e	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
	99.60934	0.3346	99.6034	33.4636	99.60935	33.4636	99.60934	33.4636	99.60937	33.4636
	99.60934	33.46354	99.60934	33.4636	99.6034	33.4635	99.60937	33.4635	99.60933	33.4637
	99.60935	33.46351	99.60934	33.4635	99.60934	33.4635	99.60934	33.4633	99.60934	33.4636

7. CONCLUSIONS

This paper proposes a new chaotic system based on the Lorenz design. The dynamical properties of this system are demonstrated through some well-known performance tests such as Lyapunov, which shows that the proposed system of equation is hyperchaotic system, sample entropy, and phase plain, which demonstrate the complex behavior of the system (1).

This system is a key generation for multi-carrier modulation, which is newly designed to enhance the security of optical communication channels. This design helps significant saving of energy and high spectral efficiency. This also helps speed the transition process and sends only reference signals of many parallel bits. The experimental and analytical findings show that the suggested method is capable of performing encryption operations and has a high level of robustness against the majority of known attacks.

REFERENCES

[1] Natiq, H., Said, M.R.M., Al-Saidi, N.M., Kilicman, A. (2019). Dynamics and complexity of a new 4d chaotic laser system. *Entropy*, 21(1): 34. <https://doi.org/10.3390/e21010034>

[2] Wazi, M.T., Ali, D.S., Al-Saidi, N.M., Alawn, N.A. (2022). A secure image cryptosystem via multiple chaotic maps. *Discrete Mathematics, Algorithms and Applications*, 14(4): 2150141. <https://doi.org/10.1142/S179383092150141X>

[3] Veeman, D., Natiq, H., Al-Saidi, N.M.G., Rajagopal, K., Jafari, S., Hussain, I. (2021). A new megastable chaotic

oscillator with blinking oscillation terms. *Complexity* 2021: 5518633. <https://doi.org/10.1155/2021/5518633>

[4] Al-Saidi, N.M., Younus, D., Natiq, H., Ariffin, M.R.K., Asbullah, M.A., Mahad, Z. (2020). A new hyperchaotic map for a secure communication scheme with an experimental realization. *Symmetry*, 12(11): 1881. <https://doi.org/10.3390/sym12111881>

[5] Younus, D., Al-Saidi, N.M., Hamoudi, W.K. (2019). Secure optical communication based on new 2D-hyperchaotic map. In *AIP Conference Proceedings*, 2183(1): 090006. <https://doi.org/10.1063/1.5136206>

[6] Alnajjar, S.H., Ali, M.H., Abass, A.K. (2022). Enhancing performance of hybrid FSO/fiber optic communication link utilizing multi-channel configuration. *Journal of Optical Communications*, 43(1): 165-170. <https://doi.org/10.1515/joc-2018-0193>

[7] Abdulsatar, S.M., Saleh, M.A., Abass, A.K., Ali, M.H., Yaseen, M.A. (2021). Bidirectional hybrid optical communication system based on wavelength division multiplexing for outdoor applications. *Optical and Quantum Electronics*, 53(10): 1-11. <https://doi.org/10.1007/s11082-021-03252-9>

[8] Alnajjar, S.H., Ali, M.H., Al-Obaidi, A., Alsaedi, M.A. (2020). Hybrid of multiple (TX/RX) FSO/Fiber optic communication system under environmental disturbances. *Journal of Multidisciplinary Approaches in Science*, 2(1): 7-16.

[9] Ali, M.H., Abass, A.K., Abd Al-Hussein, S.A. (2019). 32 Channel× 40 Gb/s WDM optical communication system utilizing different configurations of hybrid fiber amplifier. *Optical and Quantum Electronics*, 51(6): 1-8. <https://doi.org/10.1007/s11082-019-1842-8>

[10] Ohtsubo, J. (2017). Theory of optical feedback in

- semiconductor lasers. In *Semiconductor Lasers*, pp. 83-112. https://doi.org/10.1007/978-3-319-56138-7_4
- [11] Jia, Y.Q., Jiang, G.P., Yang, H., Yu, B., Du, M.D. (2021). Design and performance analysis of a multi-carrier M-ARY DCSK system with multilevel code-shifted modulation based on fractional-order chaos. *Electronics*, 10(19): 2343. <https://doi.org/10.3390/electronics10192343>
- [12] Korba, K.A., Abed, D., Fezari, M. (2021). Securing physical layer using new chaotic parametric maps. *Multimedia Tools and Applications*, 80(21): 32595-32613. <https://doi.org/10.1007/s11042-021-11226-y>
- [13] Kaddoum, G., Richardson, F.D., Gagnon, F. (2013). Design and analysis of a multi-carrier differential chaos shift keying communication system. *IEEE Transactions on Communications*, 61(8): 3281-3291. <https://doi.org/10.1109/TCOMM.2013.071013.130225>
- [14] Jiang, N., Zhao, A., Xue, C., Tang, J., Qiu, K. (2019). Physical secure optical communication based on private chaotic spectral phase encryption/decryption. *Optics Letters*, 44(7): 1536-1539.
- [15] Liu, S., Jiang, N., Zhao, A., Zhang, Y., Qiu, K. (2020). Secure optical communication based on cluster chaos synchronization in semiconductor lasers network. *IEEE Access*, 8: 11872-11879. <https://doi.org/10.1109/ACCESS.2020.2965960>
- [16] Zhao, A., Jiang, N., Liu, S., Zhang, Y., Qiu, K. (2020). Generation of synchronized wideband complex signals and its application in secure optical communication. *Optics Express*, 28(16): 23363-23373.
- [17] Qamar, F., Islam, M.K., Farhan, R., Ali, M., Shah, S.Z. A. (2019). Secure optical QAM transmission using chaos message masking. *Journal of Optical Communications*. <https://doi.org/10.1515/joc-2018-0225>
- [18] Ouannas, A., Karouma, A., Grassi, G., Pham, V.T. (2021). A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Engineering Journal*, 60(1): 1873-1884. <https://doi.org/10.1016/j.aej.2020.11.035>
- [19] Peng, Z., Yu, W., Wang, J., Zhou, Z., Chen, J., Zhong, G. (2022). Secure communication based on microcontroller unit with a novel five-dimensional hyperchaotic system. *Arabian Journal for Science and Engineering*, 47(1): 813-828. <https://doi.org/10.1007/s13369-021-05450-9>
- [20] Abuturab, M.R., Alfalou, A. (2022). Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform. *Optics & Laser Technology*, 151: 108071. <https://doi.org/10.1016/j.optlastec.2022.108071>
- [21] Lorenz, E.N. (2005). Designing chaotic models. *Journal of the Atmospheric Sciences*, 62(5): 1574-1587. <https://doi.org/10.1175/JAS3430.1>
- [22] Alattas, K.A., Mostafae, J., Sambas, A., Alanazi, A.K., Mobayen, S., Vu, M.T., Zhilenkov, A. (2021). Nonsingular integral-type dynamic finite-time synchronization for hyper-chaotic systems. *Mathematics*, 10(1): 115. <https://doi.org/10.3390/math10010115>
- [23] Wang, Z., Lei, T., Xi, X., Sun, W. (2016). Fractional control and generalized synchronization for a nonlinear electromechanical chaotic system and its circuit simulation with Multisim. *Turkish Journal of Electrical Engineering and Computer Sciences*, 24(3): 1502-1515. <https://doi.org/10.3906/elk-1303-104>
- [24] Diaconu, A.V. (2016). Circular inter-intra pixels bit-level permutation and chaos-based image encryption. *Information Sciences*, 355-356: 314-327. <https://doi.org/10.1016/j.ins.2015.10.027>
- [25] Xu, L., Li, Z., Li, J., Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 78: 17-25. <https://doi.org/10.1016/j.optlaseng.2015.09.007>
- [26] Liu, H., Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, 59(10): 3320-3327. <https://doi.org/10.1016/j.camwa.2010.03.017>