Secure Image Encryption Using Single-Mode Fiber and Dense Wavelength Division Multiplexing in Chaotic Systems

Nadia M. G. Al-Saidi[1], Suzan J. Obaiys[2(✉)], Nawras A. Alwan[2], Arkan J. Mohammed[3], Alaa Kadhim Farhan[4], and Yeliz Karaca[5]

[1] Department of Applied Sciences, University of Technology, Baghdad, Iraq
[2] Department of Computer System and Technology, Faculty of Computer Science and, Information Technology, University of Malaya, Kuala Lumpur, Malaysia
suzan@um.edu.my
[3] Department of Mathematics, College of Science, Mustansiriyah University, Baghdad, Iraq
[4] Department of Computer Sciences, University of Technology, Baghdad 110066, Iraq
[5] Chan Medical School, University of Massachusetts (UMass), 55 Lake Avenue North, Worcester, MA, 01655, USA

Abstract. The integration of the advanced technologies of the current landscape (The Internet of Things (IoT), Artificial Intelligence (AI), smart devices, and so forth) has converted the security issue into a significant matter, particularly in cases, when the data is transferred through different insecure channels. However, the necessity for robust and innovative security of data through transmission is still a challenge. The sensitivity of the chaotic systems to their initial conditions and control parameters makes them a reasonable choice for such purposes. This application for Dense Wavelength Division Multiplexing (DWDM) is designed to enhance long-distance communication by increasing the transmission capacity. Our design uses four channels each with a bit rate of 10 Gbs. To ensure the security of the data sent through this method, a novel 5D-chaotic system serves as an encryption key for images. This approach enables the safe transmission of images over a 150 km distance at a capacity of 40 Gbps. The simulation results are obtained by hybridizing Matlab and Optisystem software. Accordingly, the study evaluates the encryption's security using measures such as histogram analysis, correlation coefficient analysis, and information entropy. Findings show enhanced security and efficiency across longer distances.

Keywords: Dense Wavelength Division Multiplexing · Chaotic Encryption · Information Entropy · Chaotic System · Fiber Networks · Chaotic Encryption · Complex oscillations · Lyapunov Exponents · Bifurcations of 5D System · Optical Communication System · Shannon Entropy

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024
O. Gervasi et al. (Eds.): ICCSA 2024 Workshops, LNCS 14815, pp. 72–90, 2024.
https://doi.org/10.1007/978-3-031-65154-0_5

1 Introduction

In the fast-emerging era of the technology and internet, dealing with and sharing thousands of images at times may lead to the disclosure of some private information unknowingly. Their large size, high redundancy, and pixel interconnectivity require diverse structural approaches for encryption that process the given image data into a form almost unreadable to unauthorized readers. Thus, they are needed for securing information and ensuring their integrity. Image encryption is the instance of the strategies for transforming image data to the encoded format since it contains information about privacy and integrity of the data. Many encryption techniques based on diverse technologies have therefore been developed to serve this purpose, such as chaos-based, S-Box-based, optical compression, frequency-domain, DNA-based encryption, and many others [1–3].

Chaotic systems, with their complicated dynamics, present a chance to boost the security of communication systems. The characteristics are therefore rather unpredictable, which makes them very suitable for an encryption process and serves to provide protection against intrusion and interception. Chaotic systems are characterized by their sensitivity to initial conditions, their irregular patterns, and their nonlinearity. These systems yield many studies in the field of nonlinear dynamics due to their complex, unpredictable nature and have found broad applications across many fields. They can be used to model behaviors in the market and develop trading strategies in finance [4], examine population dynamics in biology and the behavior of biological systems in pharmacology [5, 6], model neurons and advance machine learning and AI algorithms in neural networks, and through their structural similarities they can be used to create secure communication systems in cryptography [7]. The concept of "chaotic encryption" was first introduced by Robert Matthews in 1989 [8], since then there have been significant studies on using encryption methods based on chaos to convert the systems from order to chaos [9].

Continuous chaotic systems offer the benefit of exhibiting more complex dynamic behaviors and enhanced adaptability. However, they come with the drawbacks of needing more computational resources and intricate mathematical models. Additionally, they require discretization to fit real-world applications. In this paper, we present a system that builds upon the well-known Lorenz model [10]. This system is defined by a series of equations and positive variables. We extensively investigate the dynamics of this system using techniques, including phase plane analysis Lyapunov exponent calculations and bifurcation diagrams. Through these analyses, we uncover the behavior and significant level of chaos displayed by the system which is essential for its potential use in secure communications.

The proposed system is practically employed in communication in a setup called Dense Wavelength Division Multiplexing (DWDM) channel in Single Mode Fiber (SMF). It performs well in long-distance communication by improving the bandwidth and thereby increasing the transmission capacity. The paper provides information, about the design of both the transmitter, which consists of a pseudo random bit generator and a Mach Zehnder Modulator (MZM) and the receiver equipped with a PIN photodiode, low pass filter, 3R regenerator, and bit error rate analyzer [11–13]. A significant aspect of this study involves utilizing chaotic Stream Segmentation (CSS) technology for transmitting data over distances [14]. The effectiveness and security of the system

are thoroughly assessed using metrics such as histogram analysis, correlation coefficient and information entropy evaluations. These assessments confirm that both the system and its encryption algorithm are secure and efficient for transmitting data over distances.

The available works in this regard were devoted to using the signals of semiconductor lasers to ensure the reliability of communication. It should be noted that in 1992 Mork et.al.[15] performed a study that proves the real possibility of using semiconductor lasers, that is the starting point of chaos-aided communication. The next work appeared in 2005 by Argyris et. al. [16] was directed towards the development of encryption and decryption algorithms for signals transmitted using diode lasers in fiber optics. The work on the technology Dense Wavelength Division Multiplexing was continued [17]. In 13 years later since the last publication, they showed, for example, that Zhou et al. [18] proved that DWDM has the ability to increase the data capacity of fiber optic systems. Their work extensively examined the effectiveness of DWDM in managing large-scale data transmission an aspect of our study. Moreover, in 2018, Simarpreet, and Singh [19] explored encryption techniques including algorithms, within the context of fiber optics. Their findings emphasized the vital role encryption plays in ensuring the security of data transmitted over distances. In 2016 Huang et. al. [20] worked on optimizing signal integrity and security over extended distances. Their findings provided insights, into managing signal degradation and preventing security breaches in transmissions.

Given the inputs of the previous studies, the aim of this study emphasizes on proposing of a new 5D chaotic system, which is designed specifically to be implemented in a DWDM Single Mode Fiber system. Through this integration, security is enhanced and the problem of optical communication over long distances and high capacity is overcome. Moreover, the security and efficiency of fiber optic communication will be enhanced too.

The remainder of this paper is organized as follows: In addition to this section that represents the introduction to chaos-based image encryption in optical communications, this work includes another five sections. Section 2 proposes a new 5D-Chaotic system and discusses its dynamic properties. Section 3 introduces the technology of optical communication as a multiplexing operation in fiber networks using DWDM technology. Section 4 four evaluates the effectiveness of the proposed encryption method based on some performance metrics. The transmission of the image data over a long distance is shown as a result of the optical setup in Sect. 5. Finally, the conclusion about the efficiency and security of the proposed system along with the future directions are provided in Sect. 6.

2 The Proposed Chaotic System

In this section, we proposed a 5D-chaotic system to be used for generating high random sequences to encrypt images and ensure safe transitions. The proposed system is given in (1).

$$\begin{aligned} x_1' &= (y - w)u - x + a \\ y_1' &= (z - u)x - y + b \\ z_1' &= (w - x)y - z + c \\ w_1' &= (u - y)z - w + d \\ u_1' &= (x - z)w - u + e \end{aligned} \tag{1}$$

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

3 Numerical Analysis of System (1)

The behavior of system (1) is investigated through some numerical simulations such as; trajectory (Fig. 1), phase space (Fig. 2), Sensitivity parameter (Fig. 3), Lyapunov exponent (Fig. 4), and bifurcation diagram (Fig. 5). This simulation is also important for choosing the control parameters that ensure a high chaosity range [21]. The simulation results have been obtained by hybridizing Matlab [22] and Optisystem software [23].

A. System Attractor

The complex attractor in phase space is an indicator of an efficient chaotic system. Figure 1 displays the attractor diagrams and time series for system (1), which are generated under varying parameter values of $a = 6$, $b = 10$, $c = 0.85$, $d = 2$, and $e = 0.1$. And an initial state of $(x, y, z, w, u) = (1, 1, 1, 1, 1)$. Figure 2 illustrating the phase space of a system (1) -specifically through the direct trajectories between the variable pairs (x vs y, y vs z, z vs w, and w vs u) -we capture the essence of the system's complex dynamics, with the control parameters $a = 6$, $b = 10$, $c = 0.85$, $d = 2$, and $e = 0.1$. These visualizations reveal the interplay and feedback mechanisms among the variables, showcasing the chaotic system's sensitivity to initial conditions and parameter changes. By examining the figures, we observe how each pair of variables interacts within the larger system, offering insights into the unpredictable and aperiodic paths that characterize the system's evolution. The detailed exploration of these phase space plots deepens our understanding of the dynamical processes controlling the chaotic behavior, providing invaluable information for theoretical and practical applications aimed in various fields. Figure 3 show demonstrates profound sensitivity to parameter changes of system (1), based on the change parameter b (10:11) significantly impacts both the attractor structure and the time series of state variables, which shows the system's responsiveness. This sensitivity reveals itself through changes in the attractor's geometry in phase space a visual representation of the system's state evolution over time and in the aperiodic, complex oscillations observed in the time series plots for variables *(x,y,z,w)* and *(u)*.

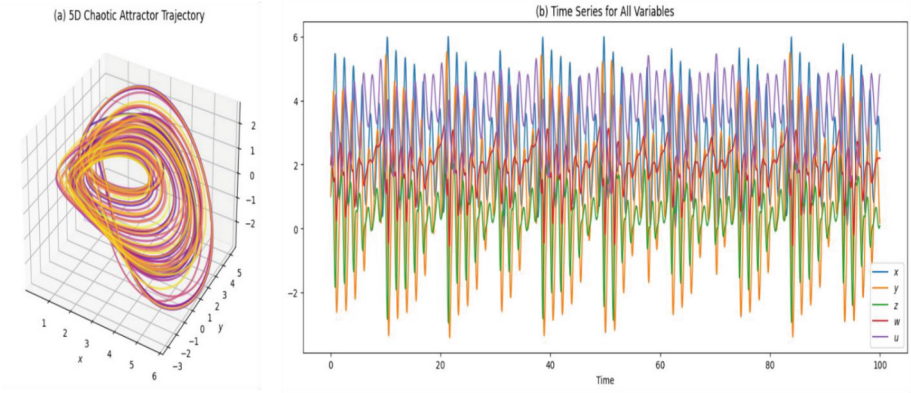


Fig. 1. Attractors and time series of system (1)

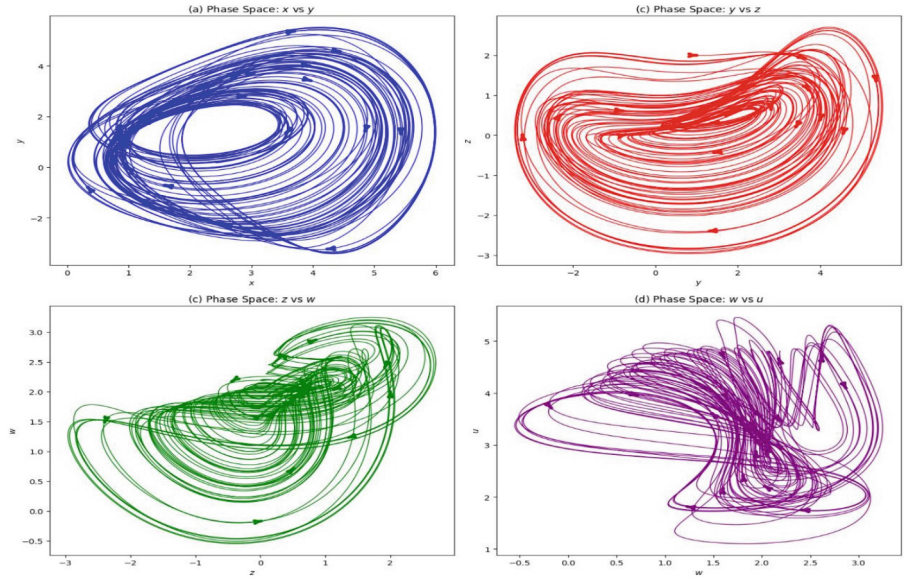


Fig. 2. Phase space of system (1) with the control parameters a = 6; b = 10; c = 0.85; d = 2; e = 0.1, as shown in (a),(b),(c), and (d)

B. Lyapunov Exponents

Lyapunov Exponent (LE) is an important measure used to demonstrate the chaotic behavior of the nonlinear dynamical system. It is a method employed to show that, when two starting values that differ slightly are introduced into the same chaotic system, the paths they create diverge exponentially as time increases. The Lyapunov exponents of the system (1) are given by: LE1 = 0.256625, LE2 = 0, LE3 = -0.647382, LE4 = -1.852560, LE5 = -2.756661. Figure 4 depicts the LE of hyperchaotic behavior of system (1).

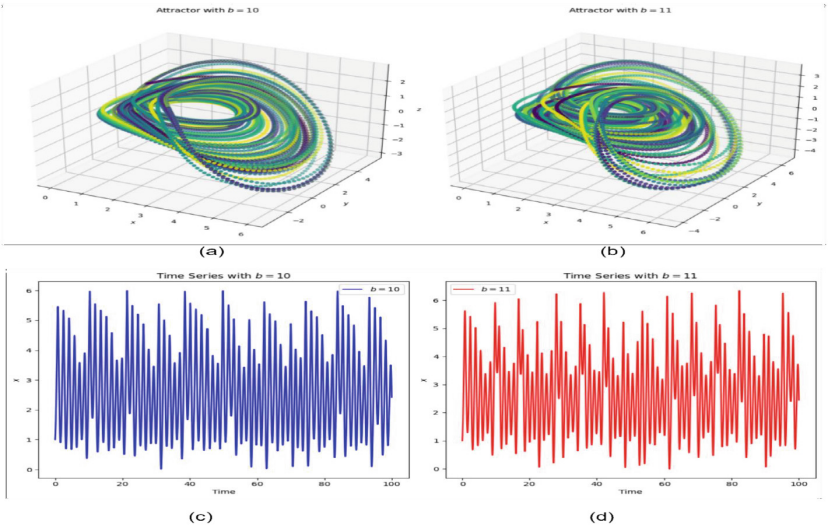


Fig. 3. Sensitivity parameter

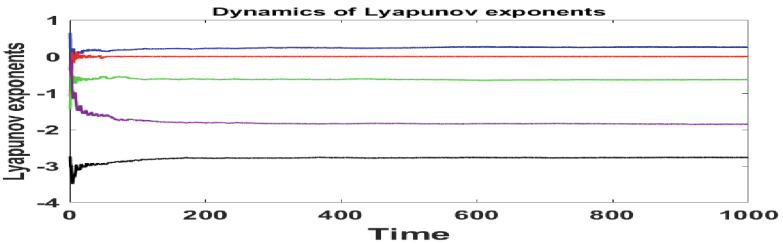


Fig. 4. Lyapunov exponent of system (1)

III. Bifurcations of 5D propose system

The term "bifurcation" is utilized to describe the behavior variation as a result of a small change in a system parameter. The correlation between the control parameters and the features of the chaotic system can be illustrated by a diagram known as a bifurcation diagram. It shows how system performance changes as parameters vary and indicates sudden changes in performance as critical parameters are reached. Bifurcations are essential in the evaluation of dynamic systems in a variety of fields, including physics, engineering, biology, and economics. The bifurcation diagram in Fig. 5 illustrates the long-term behavior of the x variable in a system (1) as a function of the parameter a, which varies from (1: 0.1: 10). Despite the system (1) having 5D (x, y, z, w, u), we actually focusing on variable x, which allows us to understand how this component of the system (1) stay stabilizes or varies over time, based on some variables or parameters. The bifurcation refers to the point on the diagram representing the state of the x variable after the system has evolved or changed time, during the interval [90,100], indicating the system's steady-state or periodic behavior at different values of a. We take this interval

[90,100] to ensure that the system has had sufficient time to evolve into its steady state or a characteristic periodic orbit if one exists. Now, the color of points changes from dark purple to bright yellow based on the value of the parameter a increases, facilitating a clear visual distinction between different regions of the parameter space. This change of color allows for an immediate visual to understand the bit change in the parameter a how long influence the system's dynamics over time, highlighting regions where changes lead to significant changes in the system's behavior. These bifurcations point to the sensitivity of the chaotic system to initial conditions and parameters.

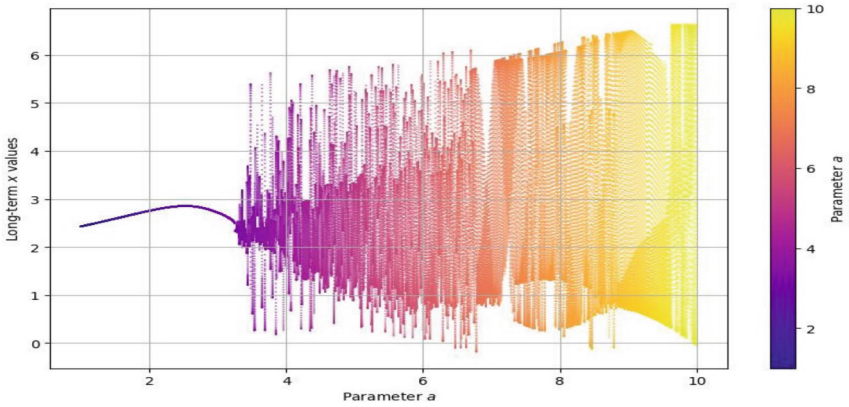


Fig. 5. Bifurcations diagram of system (1)

4 Optical Communication System

The multiplexing operation in optical networks is a technology utilized to improve their bandwidth. This is done through the DWDM technology. DWDM is an optical fiber multiplexing technology which can deliver multiple signals simultaneously and raise the information capacity, which is transferred through optical fibers, so that it can reach higher bandwidth and transmission capability [24]. This technology makes it perfect for high-speed applications such as broadband, video conferences and cloud computing. Moreover, it is appropriate for telecom networks, which need to transmit data over long distances. Furthermore, DWDM enables numerous data signals to be transmitted in various wavelength channels. The following are three main components of the proposed system;

i. The transmitter: The suggested transmitter has four parts, which are:
   1. The pseudo-random bit sequence generator (PRSG) is to be used as input to the Matlab connector.
   2. Matlab connector: used to encrypt the input image.
   3. The input image data is carried by a nonreturn to zero (NRZ) generator [25].

4. A continuous laser (CW) with a power of 5 dBm modulates the data optically at wavelengths between 193.1 and 193.8 THz with a Mach-Zehnder-Modulator (MZM) [24].

ii. Optical fiber: The single-mode fiber (SMF) is used to transmit the plain and encrypted image. The attenuation and dispersion are considered challenges in communications-based optical fiber. The dispersion compensating fiber (DCF) can be used to overcome image dispersion, while an Erbium-Doped Fiber Amplifier (EDFA) is used to amplify the signal strength [11].

iii. The receiver section: Consists of a PIN photodiode for data detection, a filter of low-pass Bassel, a 3R regenerator for signal reshaping, and the Matlab implementation for image decryption. A bit error rate (BER) analyzer receives and examines the delivered data. Table 1, and Figs. 4 and 5, display the input parameters that were utilized to define the system in more detail.

Table 1. SMF system components

	Component	Specifications
Transmitter part	Pseudo random bits generator	Bit Rate: 5E + 9 bps
	MATLAB connector	Used to encrypt/decrypt the signal message
	CW Laser	Power = 5dBm, wavelength:193.1 THz-193.8 THZ,linewidth: 10 MHz
	RZ	Amplitude = 5
	MZM	Extinction ratio = 30db
	Wavelength division multiplexing	WDM 4 × 1 channel, bandwidth = 30 Ghz
Channel	SMF	Length = 100km, Attenuation = 0.2dB/km
	DCF	Length = 15.22, Dispersion = -110 ps/ns/km, Attenuation = 0.44 dB/km
	EDFA	Gain = 31 dB, Wavelength = 980nm Noise figures = 3 dB
Receiving part	PIN Photodetector	Responsivity = 1 A/W
	Low pass Bessel filter	Cutoff frequency = 0.75xBit rate, depth: 100 dB
	3R Regenerator	WDM 4 × 1 channel, bandwidth = 30 GHz,

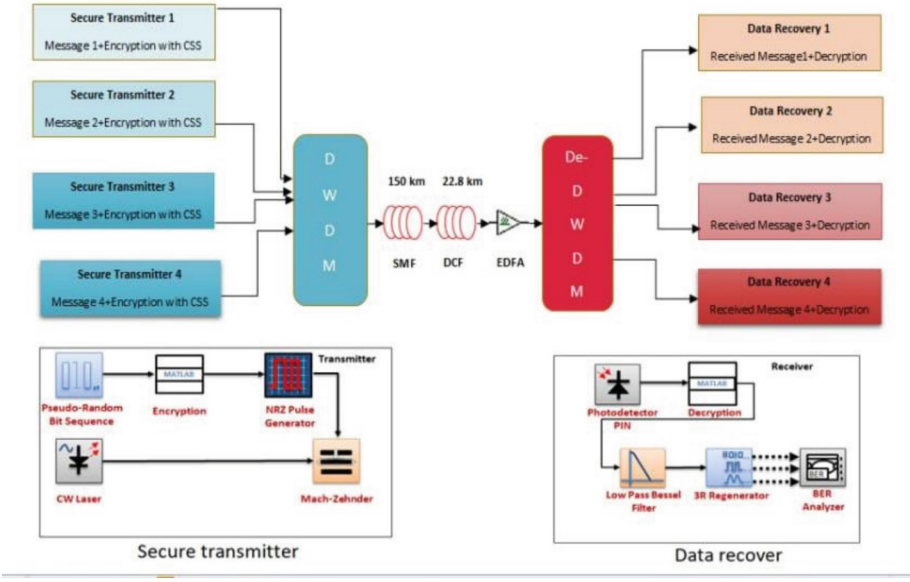


Fig. 6. Schematic diagram of the proposed DWDM system

5 Security Evaluation and Experimental Results

In this part, the effectiveness of implementation results are evaluated using some performance metrics. The system of encryption is used for color and grayscale images [26].

5.1 Histogram

The histogram of an image is a graphical representation of the distribution of pixel intensities in the image. It is a useful tool for image analysis because it provides information about the distribution of pixel values and can reveal important characteristics of an image, such as its contrast, brightness, and color balance. The encrypted image whose histogram is as uniform as possible, meaning that all pixel values should have approximately the same frequency of occurrence, making it difficult for an attacker to extract any meaningful information from the histogram. If the histogram of the encrypted image appears to be quite uniform, it is a good indication that the encryption has been successful in hiding the information. Figure 8 shows the histogram of the original image (b), the encrypted images (d), and the decryption image (f). The histogram of the cipher image appears to be quite uniform, whereas the histograms of the original and decipher images are different.

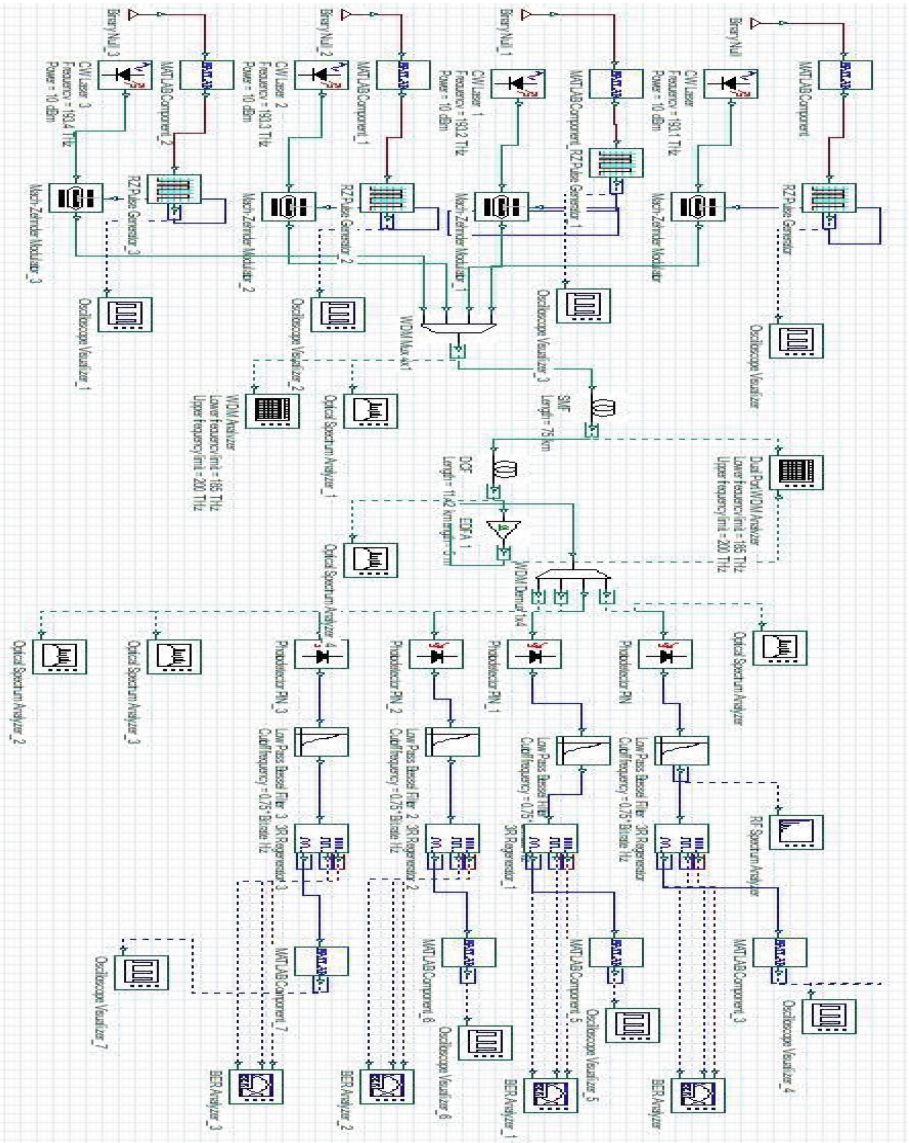


Fig. 7. The implemented DWDM system via Optisystem

5.2 Correlation Coefficient Analysis

In a plain image, if the correlation value is close to 1, it means that the adjacent pixel, whether it is vertical, horizontal, or diagonal, has a high correlation with each other. So, a close to 1 correlation value, is an indication of a high correlation in the image, whereas, a close to zero value is an indicator for high randomly distributed pixels. Therefore, the strong correlation between the adjacent pixels needs to be eliminated by a good

encryption method. The results of the Sunflower image correlation are shown in Fig. 9 in three different directions (horizontal (b), vertical (c), and diagonal (d) for the plain and cipher images shown in (a)). Table 2, shows the correlation between adjacent pixels in plain and cipher images using (2), which indicates that adjacent pixels in the plain image have a correlation value near 1, while adjacent pixels in the encrypted image have a correlation value close to 0, which lead us to conclude that the cipher image pixels are randomly distributed.

The correlation coefficient is calculated by:

$$\mathrm{CC} = \frac{E(X - E(X))E(Y - E(Y))}{\overline{\sqrt{D(X)}\sqrt{D(Y)}}} \tag{2}$$

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

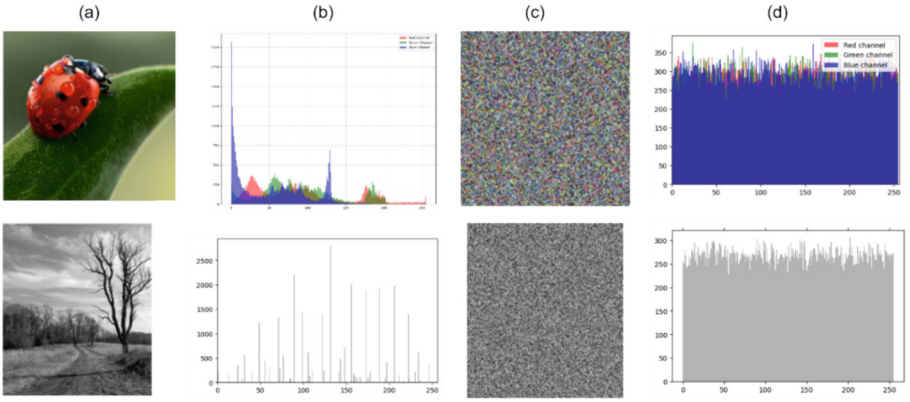


Fig. 8. Histogram of some color and grayscale images before and after the encryption process

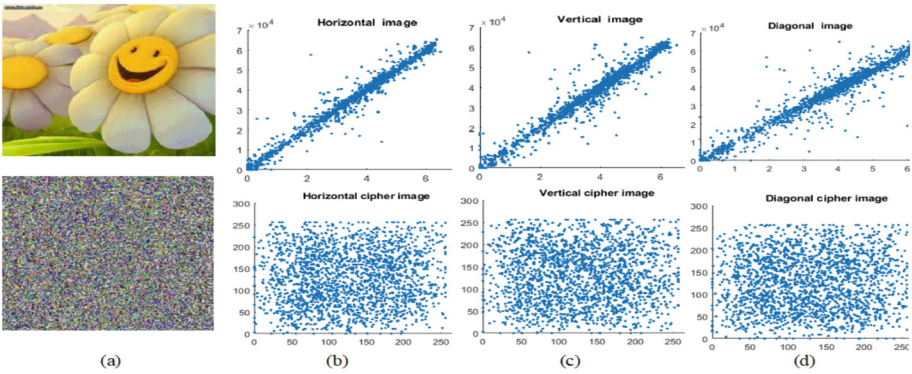


Fig. 9. The correlation between pixels before and after the encryption process

5.3 Information entropy

Shannon's entropy is a measure of the randomness or unpredictability of an information source, and it is commonly used in image analysis to quantify the degree of randomness in an image (3). Which can be calculated as:

$$H(e) = -\sum_{i=0}^{2N-1} P(e_i) \log_2 P(e_i) \tag{3}$$

where (e) is the source, N is the grey-level number with a probability P(ei). The recommended value for H(e) for entirely random images is equal to 8. Table 3, shows the entropies of some images before and after the encryption process.

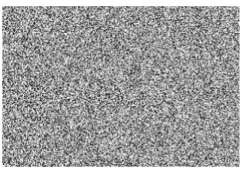
As a conclusion, from the histogram in Fig. 6, it is evident that the encrypted image has a distribution indicating the concealment of features from the original image. This uniformity plays a role in preventing attackers from gaining insights into data. The correlation measure for the neighbouring pixels in the encrypted image indicates an efficient encryption method that successfully disrupts the patterns of the original image as shown in Fig. 7, and Table 2. The results of information entropy (Table 3) approach the value for random images indicating a high degree of randomness and unpredictability in the encrypted images.

6 Results of the Optical Setup

This work aims to secure the transmission of data at a rate of Gb/s over longer distances using Chaotic Stream Segmentation (CSS) technology [14]. The input signal is generated from a pseudo-random bit sequence generator at a rate of 10 Gbps and fed into a nonreturn to zero (NRZ) pulse generator. The output from the NRZ is then modulated with a Mach-Zehnder modulator (MZM) and transmitted via a continuous wave (CW) laser. The performance of the proposed system was evaluated based on Q-factor and bit error rate (BER) as a function of link distance, with andwithout encryption, across four different channels at varying wavelengths (1550 nm, 1550.8 nm, 1551.6 nm, 1552.4 nm).

The results of the study are presented in two figures: Fig. 7 shows the system's performance without encryption, while Fig. 8 shows its encryption performance with the help of EDFA, and Fig. 10 shows the performance with encryption using DCF and EDFA together. The maximum link distance achieved without encryption was 110 km, with encryption was 69.5 km, and with encryption using DCF and EDFA was 150 km. The Q-factor and BER values are displayed in Tables 4, 5, 6, 7, 8, 9 sequentially.The quality factor (Q-factor) of a plain image for several wavelengths is depicted in (a). Whereas, (b) depicts the bit error rate (BER) for the same wavelengths as shown in Fig. 10, and Tables 4 and 5. The system achieved a link distance of approximately 110 km.

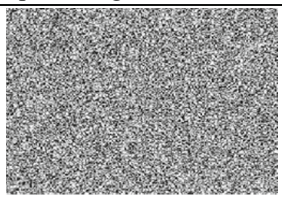
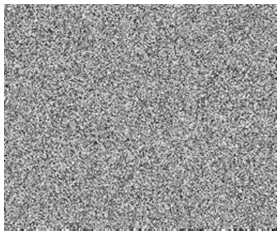
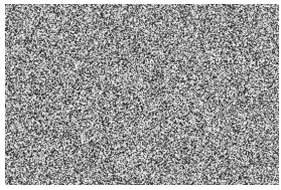
Table 2. Correlation analysis

Image	Correlation coefficient
	0.9841
	0.0039
	0.9823
	0.0035

The quality factor (Q-factor) for several wavelengths of an encrypted image is shown in Fig. 11 (a), while (b) depicts the bit error rate (BER) for the same wavelengths with EDFA. The system achieved a link distance of approximately 69.5 km as shown in Tables 6 and 7.

The quality factor and bit error rate for different wavelengths of the communication system. The system incorporates encryption, with the help of dispersion compensation fiber (DCF), and erbium-doped fiber amplifiers (EDFAs) to enhance transmission distance as shown in Fig. 12, and Tables 8 and 9. The system realized a link distance of about 150 km.

Table 3. Information entropy analysis

Plain image	Entropy	Cipher image	Entropy
	7.7087		7.9679
	7.4499		7.9683
	6.0733		7.9563

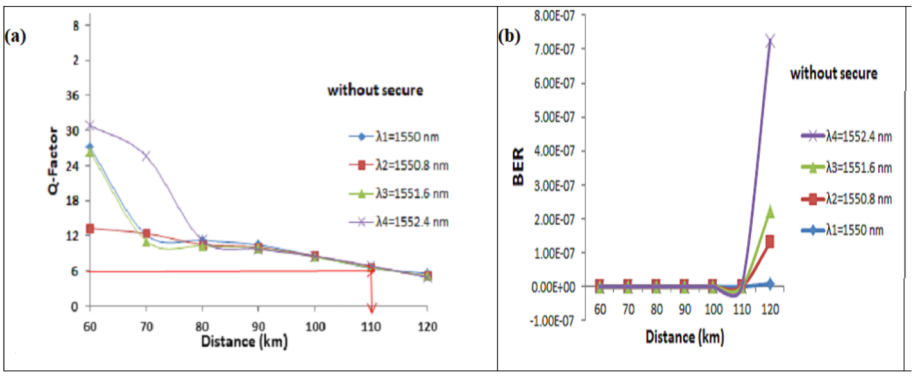


Fig. 10. (a) The quality factor (Q-factor) for several wavelengths, (b) the bit error rate (BER) for plain image.

Table 4. The Q-factor values of various distances for plain image

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
60	27.1324	13.2877	26.4014	30.9064
70	12.2056	12.4228	11.1756	25.6449
80	11.2365	10.5183	10.2846	11.2532
90	10.4468	10.0459	9.91854	9.76129
100	8.56135	8.60103	8.41555	8.53719
110	6.51525	6.69968	6.57875	6.893
120	5.62462	5.14927	5.19446	4.88372

Table 5. The BER value of various distances for a plain image

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
60	1.40E-162	1.33E-40	4.35E-154	3.60E-210
70	1.41E-34	9.34E-36	2.46E-29	1.83E-145
80	1.29E-29	3.38E-26	3.94E-25	1.06E-29
90	7.48E-26	4.78E-24	1.69E-23	7.55E-23
100	5.45E-18	3.64E-18	1.81E-17	6.62E-18
110	3.45E-11	9.59E-12	2.11E-11	2.66E-12
120	9.02E-09	1.21E-07	9.44E-08	5.02E-07

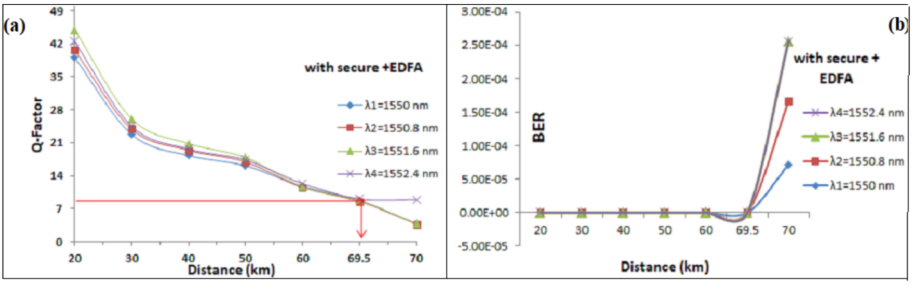


Fig. 11. (a) The quality factor (Q-factor) for several wavelengths of an encrypted image, while (b) shows the bit error rate (BER) for the same wavelengths with EDFA.

The system's performance is evaluated by measuring the Q-factor and bit error rate (BER) at distances of various wavelengths (Figs. 10, 11 and 12; Tables 4, 5, 6, 7, 8, 9). Without using the encryption process, we were able to achieve a link distance of 110 km. Whereas, when the encryption process was implemented, this distance was reduced to 69.5 km due to dispersion effects caused by the encryption process. To

Table 6. Q-factor values of various distances for the encrypted images with EDFA

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
20	39.0983	40.6591	44.998	42.4285
30	22.791	23.9233	26.0789	24.535
40	18.3037	19.4257	20.8236	19.6616
50	16.1195	16.9178	17.8958	17.3363
60	11.715	11.531	11.671	12.3529
69.5	8.73365	8.56599	8.70018	9.09824
70	3.80227	3.73188	3.74327	8.96017

Table 7. BER values of various distances for the encrypted images with EDFA

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
20	0.00E + 00	0.00E + 00	0.00E + 00	0.00E + 00
30	2.79E-115	8.70E-127	3.16E-150	3.12E-133
40	3.85E-75	2.31E-84	1.29E-96	2.27E-86
50	8.64E-59	1.51E-64	5.63E-72	1.13E-67
60	5.03E-32	4.38E-31	8.58E-32	2.18E-35
69.5	1.20E-18	5.21E-18	1.62E-18	4.45E-20
70	7.15E-05	9.45E-05	9.03E-05	1.57E-19

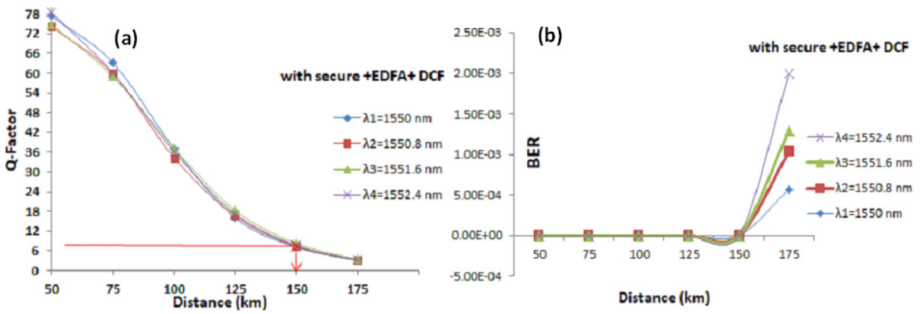


Fig. 12. (a) The quality factor for different wavelengths with (DCF), and (EDFAs), (b) the BER for different wavelengths with (DCF), and (EDFAs).

counteract this reduction in link distance caused by encryption effects we incorporated dispersion compensation fibers (DCF) and erbium-doped fiber amplifiers (EDFA) into our system. This resulted in an improvement in link distance up to approximately 150 km.

Table 8. The Q-factor values for various distances for encrypted images with EDFA and DCF

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
50	77.286	74.1772	74.769	78.3244
75	63.2239	59.8862	58.9592	60.1082
100	37.1807	34.3323	37.2323	36.2179
125	16.0668	16.6539	18.3037	17.2585
150	7.131	7.32753	8.24748	7.62268
175	3.21525	3.2846	3.45289	3.1555

Table 9. The BER values for various distances for encrypted images with EDFA and DCF

Length	$\lambda 1 = 1550nm$	$\lambda 2 = 1550.8nm$	$\lambda 3 = 1551.6nm$	$\lambda 4 = 1552.4nm$
50	0.00E + 00	0.00E + 00	0.00E + 00	0.00E + 00
75	0.00E + 00	0.00E + 00	0.00E + 00	0.00E + 00
100	5.11E-303	9.37E-259	7.43E-304	1.11E-287
125	1.51E-58	1.00E-62	2.82E-75	3.34E-67
150	3.84E-13	9.00E-14	6.49E-17	9.45E-15
175	5.71E-04	4.65E-04	2.55E-04	6.99E-04

This improvement demonstrates that we can effectively mitigate any impacts, on signal quality caused by encryption through compensatory mechanisms.

In general, the findings of this research indicate that incorporating the system into the DWDM SMF system greatly improves security while maintaining the overall performance of the system. By utilizing CSS technology for encryption data transmission over distances can be effectivelyprotected by employing DCF and EDFA. The potential issues related to signal integrity arising from encryption can be successfully addressed. This study presents a method, for achieving high-capacity and long-range optical communication.

7 Conclusion

The advanced information technologies in the current time entail the sharing of voluminous digital data through both public and private networks. These developments pose a challenge and an essential task in terms of protecting the data from vulnerable access. This paper tries to enrich the field of optical communication by focusing on security and data transmission efficiency. By incorporating a chaotic system into the DWDM-SMF system, it offers an approach to achieving high bandwidth and long-distance data communication. System (1) has a complex and unpredictable nature. By implementing CSS technology within the DWDM-SMF system, data encryption is effectively carried out

over extended distances. By using encryption, the link distance is lowered from 100 km to 69.5 km due to dispersion effects, but the issue is addressed through the use of DCF to achieve a 150 km link distance. According to the study, DWDM can be used to increase the transmitted bit rate, which can be considered to be an input obtained as a result of our analyses. The security analysis is demonstrated using measures like histogram uniformity, correlation coefficient and information entropy to ensure that the system exhibits a level of security. This robustness makes it resilient, against attacks, and with the utilization of DCF and EDFA, there emerges a significant impact on the performance of the system ensuring that the integrity of signals is maintained even over distances as long as 150 km. Notwithstanding, this study not only enhances data transmission security but also ensures high efficiency and performance over extended distances, which can pave the way for more sophisticated and advanced applications in various fields for the attainment of optimized solutions.

Acknowledgments. This work was accomplished at the University of Technology, Iraq, and the Faculty of Computer Science and Information Technology, Universiti Malaya, Malaysia and it is funded by the Universiti Malaya RMFI2067-2021 Grant.

References

1. Wazi, M.T., Ali, D.S., Al-Saidi, N.M., Alawn, N.A.: A secure image cryptosystem via multiple chaotic maps. Discrete Math. Algorithms Appl. **14**(4), 2150141 (2021)
2. Veeman, D., Natiq, H., Al-Saidi, N.M., Rajagopal, K., Jafari, S., Hussain, I.: A new megastable chaotic oscillator with blinking oscillation terms. Complexity **2021**(1), 5518633 (2021)
3. Al-Saidi, N.M.G., Younus, D., Natiq, H., Ariffin, M.R.K., Asbullah, M.A., Mahad, Z.: A new hyperchaotic map for a secure communication scheme with an experimental realization. Symmetry **12**(11), 2021 (1881)
4. Vogl, M.: Chaos measure dynamics in a multifactor model for financial market predictions. Commun. Nonlinear Sci. Numer. Simul. Nonlinear Sci. Numer. Simul. **130**, 107760 (2024)
5. Salih, S.H., Al-Saidi, N.M.G.: 3D-Chaotic discrete system of vector borne disease using environment factor with deep analysis. AIMS Math. **7**(3), 3972–3987 (2022)
6. Sadkhan Al Maliky, S.B.(ed.) Multidisciplinary Perspectives in Cryptology and Information Security. IGI Global (2014)
7. Balakrishnan, H.N., et al.: ChaosNet: a chaos based artificial neural network architecture for classification. Chaos Interdisc. J. Nonlinear Sci. **29**(11) (2019)
8. Matthews, R.: On the derivation of a "chaotic" encryption algorithm. Cryptologia **13**(1), 29–42 (1989)
9. Natiq, H., Al-Saidi, N.M., Obaiys, S.J., Mahdi, M.N., Farhan, A.K.: Image encryption based on local fractional derivative complex logistic map. Symmetry **14**(9), 2022 (1874)
10. Lorenz, E.N.: Designing chaotic models J. Atmos. Sci. **62**(5), 1574–1587 (2005)
11. Abdulsatar, S.M., Saleh, M.A., Abass, A.K., Ali, M.H., Yaseen, M.A.: Bidirectional hybrid optical communication system based on wavelength division multiplexing for outdoor applications. Opt. Quantum Electron. **53**(10), 1–11 (2021)
12. Khadir, A.A., Dhahir, B.F., Fu, X.: Achieving optical fiber communication experiments by optisystem. Int. J. Comput. Sci. Mob. Comput.Comput. Sci. Mob. Comput. **3**(6), 42–53 (2014)
13. Mohammed, S.H., Abass, A.K., Ali, M.H., Rashid, F.F.: Design and simulation of secure fiber optic communication system utilizing hill cipher algorithm. J. Opt. **53**(2), 1499–1507 (2023). https://doi.org/10.1007/s12596-023-01313-8

14. Al-Saidi, N.M. and Ali, M.H.: Assessment of highly performance secure optical communication systems based on chaotic design. Al-Iraqia J. Sci. Eng. Res. **1**(1), 109–123 (2022)
15. Mork, J., Tromborg, B., Mark, J.: Chaos in semiconductor lasers with optical feedback: theory and experiment. IEEE J. Quantum Electron. **28**(1), 93–108 (1992)
16. Argyris, A., et al.: Chaos-based communications at high bit rates using commercial fibre-optic links. Nature **438**(7066), 343–3466 (2005)
17. Qiao, J.: Dense wavelength division multiplexing (DWDM) for optical networks. The University of Texas at Austin (2001)
18. Zhou, R., et al.: 80-km coherent DWDM-PON on 20-GHz grid with injected gain switched comb source. IEEE Photonics Technol. Lett. **26**(4), 364–367 (2013)
19. Kaur, S., Singh, S.: Review on developments in all-optical spectral amplitude coding techniques. Opt. Eng. **57**(11), 116102 (2018)
20. Huang, C., et al.: A bounded model of the communication delay for system integrity protection schemes. IEEE Trans. Power Delivery **31**(4), 1921–1933 (2016)
21. Al-Saidi, N.M., et al.: The dynamic and discrete systems of variable fractional order in the sense of the Lozi structure map. AIMS Math. **8**(1), 733–751 (2023)
22. The MathWorks, Inc.: MATLAB 2023 version 9.12.0(R2023a), Software, Natick, MA (2023)
23. Atieh, A., Mirza, J., Ghafoor, S.: Optical fiber sources design in OptiSystem software. Photonics North (PN) (cdn.optiwave.com, 2022). https://cdn.optiwave.com/wp-content/uploads/2022/05/Photonics-North-2022_May-25-2022.pdf. Accessed 25 May 2022
24. Cheung, N.K., Nosu, K., Winzer, G.: Dense wavelength division multiplexing techniques for high capacity and multiple access communication systems. IEEE J. Sel. Areas Commun. **8**(6) (1990)
25. Xu, L., Li, Z., Li, J., Hua, W.: A novel bit-level image encryption algorithm based on chaotic maps. Opt. Lasers Eng. **78**, 17–25 (2016)
26. Al-Saidi, N.M., Yahya, H., Obaiys, S.J.: Discrete dynamic model of a disease-causing organism caused by 2D-quantum Tsallis entropy. Symmetry **14**(8), 1677 (2022)