# Visible Light Communication based on Chaos Encryption Scheme

HUDA KADHIM RUMUH, IBRAHIM ABDULLAH MARDAS
College of Engineering, Electrical Engineering,
Babylon University,
Babylon,
IRAQ

*Abstract:* -To accommodate extremely high levels of data traffic, today's communications networks are undergoing several different technical transformations. In addition to the already present video and voice services, newly created technologies and applications, such as internet services, interactive gaming, and telemedicine, are adding to the already tremendous amounts of traffic and vulnerability generated. The semiconductor laser chaos generation is now being utilized to improve data security and protect data from theft during its transmission from the transmitter to receivers a means of concealing multi-level data signals to address these concerns regarding data security. The incoming signals are concealed before the optical chaotic signal's transmission via the optical fiber medium by our suggested method, which makes use of the double delay feedback technique to create the optical chaotic signal. The additive chaos masking system is utilized to execute the mixing of incoming signals with chaos. This method demonstrates several valuable qualities, including simplicity and the ease with which a message may be recovered. To explore the propagation concerns that are related to secure signal transmission, chaotic data, which is a combination of incoming signals and random noise, is transmitted via the medium of optical fiber. To properly regulate the linear impairments of optical fiber, which is required for the efficient transmission of a secure signal, the plan is put into action for long-haul communication to facilitate the long-distance transfer of data. Adjustments are made to the parameters on both the transmitting and receiving ends to achieve synchronization between the two processes. This is done in such a way that the received signal may be restored to its original state by subtracting the broadcast signal from the same chaos on the receiving side. Obtaining Q-factors allows the method to be evaluated for a variety of optical fiber cable lengths, during which the Q-factors serve to evaluate the quality of the signal that is received.

*Key-Words:* - Semiconductor laser, chaotic signal, double delay, Mach-Zehnder Modulator(MZM), optoelectronic feedback, opt electric oscillator.

Received: April 22, 2023. Revised: February 15, 2024. Accepted: March 15, 2023. Published: May 27, 2024.

## 1 Introduction

This study presents the method for secured communication in Optisystem software by making use of a chaotic laser. Spread spectrum signals are used in chaotic communication; these signals make use of a vast bandwidth and have a low power spectrum density. [1], to supply the security data signal, the chaotic masked signal is utilized. Using chaotic modulation, the message is first encrypted when it is sent from the sender to the receiver, and then it is decrypted when it is received, [2]. As comparative metrics, the Q factor and the BER are employed, [3]. The Q-factor is the minimum optical signal-to-noise ratio required to achieve a specific bit error rate. Optical fiber cable is currently the suggested choice for data transfer, with less noise interference, and a longer transmission range because of its high bandwidth. Furthermore, because chaos-based optical communication systems have better security features than traditional cryptography techniques, they offer improved security, [4].

The physical layer of the Open System Interconnection (OSI) architecture has advantages in terms of easier installation, streamlined key management, and flexibility for digital signal processing, [5]. There are two types of chaos-based communication in the physical layer: data encryption in the electrical domain using techniques like exclusive OR scrambling, optical key distribution, chaotic laser communication, and optical steganography, and data encryption in the optical domain using fractional Fourier transform and piecewise chaotic permutation, [6].

In the case of encryption using the electrical domain, the finite precision of the computer restricts the high unpredictability of chaotic sequences, [7].

Optical chaos for secure communication may be further subdivided into two forms, depending on the transmission channel. These two categories comprise wireless communication technologies including free space optics (FSO) and optical wireless communications (OWC) as well as optical fiber communication, [8], [9]. One of the types is communication through optical fiber. There are three different ways to hide messages inside the chaos of an optical communication system: Additive chaos masking (ACM), also known as chaos modulation (CM), or chaos shift keying (CSK), [10]. [ACM] stands for additive chaos masking; CSK stands for chaos shift keying; and CM is for chaos modulation. These three distinct strategies each have their own set of advantages and disadvantages; nevertheless, in the model that we have presented, we have decided to use ACM because of its ease of use, its ability to easily recover messages, and its implementation in Optisystem software version 14.0, [11]. In Figure 1, which depicts our suggested security implementation via the ACM method, as you can see, both the transmitting and receiving sides are equipped with two chaotic systems that are rather comparable to one another. The first data signal, represented by d(t), is covered up by the chaotic signal, denoted by c(t), which is produced at the transmitting end using the double delay feedback method. This is done to form a secure signal, denoted by s(t), which is then sent through the optical fiber channel. We take advantage of a technique known as direct modulation, in which the semiconductor laser and a current source are connected, to produce optical chaos through a chaotic laser, [12]. To generate chaos with the characteristics that are wanted, the settings of the current source and the semiconductor laser are altered. This signal (s(t)) serves as noise for potential intruders and conceals the original data (d(t)) in its transmissions, [13]. The signal, denoted by s(t), is then sent across the channel and is followed by the subtraction of another chaotic signal, denoted by c(t), which is analogous to s(t) but is instead produced by a second chaotic semiconductor laser that is positioned at the receiving end. Because all of the parameters of the second chaotic laser are maintained in the same manner as the parameters of the transmitting laser, the subtraction formula may be utilized to successfully extract the initial data (d(t)), [14]. The two chaotic lasers need to have identical properties, but synchronization between them is also an essential goal to work toward. It just takes a very slight misalignment between these lasers for this plan to be rendered completely ineffective.

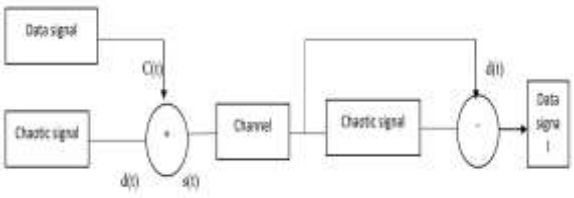



Fig. 1: A layering of additive chaos as a mask.

## 2 Related Work

Over the past few years, numerous researches have been carried out to develop communication systems for securing data. These studies have explored various approaches and techniques to enhance security with a low error rate. In this section, we will discuss some notable works that have contributed to the field.

In 2018, [15], research suggests that semi-conductor lasers are used to emulate chaotic lasers to reliably convey messages. To solve data security problems, semi-conductor laser chaos creation is being used to hide multi-level data signals. Dual binary modulation offers higher spectral efficiency than NRZ, RZ, and other modulation methods and optimizes bandwidth to increase channel capacity. Thus, it is crucial to encrypt communication delivery. The chaotic laser processed safe dual binary signal transmission in the optical communication network. Synchronize to get eye diagrams and quality. Simulation analysis was done with Optisystem 15.0. Using a chaotic laser, the optical communication network's transmitter and reception were synchronized. Before synchronization, the dual binary modulated signal is sent across SMF fibers of various lengths and DCF fibers to reduce dispersion. After 70 km, the received signal's Qfactor declined to 4.64 from 25.47 at 10 km fiber length.

In 2019, [16], authors used optics in a remote health monitoring system to protect EEG signals over an optical fiber link. They use a semiconductor laser source to create optical chaos to hide an EEG signal before transmitting it across an optical wire. This happens before signal transmission. The 14-channel Emotive headgear collects EEG data, which are analyzed and rescaled for the experimental context (Optisystem). The additive chaos masking approach, which boasts fast message retrieval and simplicity, is used to combine EEG signals with chaos to achieve the desired effect. For different optical fiber cable lengths, Q-factors can be used to

evaluate signal quality. They found that the received signal's Qfactor dropped to 5.72 from 66.67 at 5 km fiber length after 120 km.

In 2021, [17], they successfully implemented security. Their research report focuses on the implementation of a Radio-over-Fiber (RoF) network in the context of 5G front haul. The three most widely used approaches are CSK, CM, and CMS. CMS is the most cost-effective and user-friendly option. The initial phase of the study confirms the security of the RoF signal by employing optical time domain and spectrum graphs with the use of optical time domain visualizers and analyzers. In the second portion of the paper, laser power and fiber lengths are varied to evaluate system performance. The absence and presence of linear impairments are used to measure system performance.

Results demonstrate that the system functions well up to 15 km of fiber length with 10 Gbps data throughput and security features. By boosting laser power to 20 dBm, BER decreases considerably. However, linear impairment control is essential for optimal RoF signal quality.

In 2023, [18], they demonstrated Optisystem 7.0's chaos-based secure fiber-optic communication system. Standard single-mode fiber transmits a 10 Gb/s externally modulated signal across 100 kilometers. Changing semiconductor laser rate parameters generates a chaotic optical signal that hides modulated data. Chaos diminishes the efficiency of the system and limits the transmission range to 70 kilometers. Signal dispersion is mitigated via a chirped Fiber-Bragg grating with an erbium-doped fiber amplifier, which increases transmission distance to 104 km (80%). Data was retrieved at the receiver with a maximum Q-factor of 4.2 and a minimum bit error rate of.

In 2023, [19], an optical chaotic system was created and tested using OptiSystem software to evaluate its performance under different weather situations. The system is a secure hybrid combination of free space and fiber optic (FSO/FO) technology. The chaotic signal conceals the message within this highly secure communication mechanism. This security solution is potentially superior to encryption techniques. By incorporating the chaotic signal into the message, the link distance is decreased by 100 kilometers regardless of weather conditions. Under all circumstances, the use of dual Free-Space Optical (FSO) channels enhances the link distance by a significant margin of 37-40%.

# 3 Proposed Methodology

In our plane, we make use of chaos masking to accomplish both high data rate and security at the same time. To provide a more chaotic pattern of activity, the created chaos has a pulsing quality.

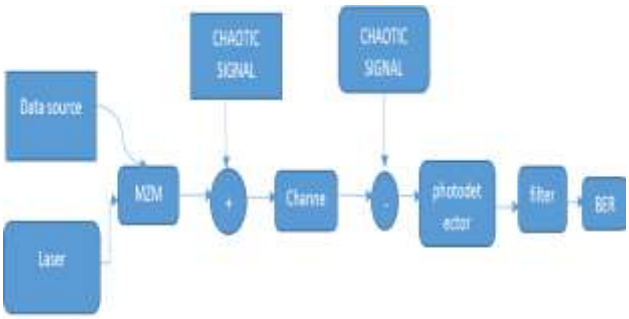



Fig. 2: The plan that we have developed is to introduce chaos to the incoming signals

In Figure 2 the input signal is fed and pre-processed into an MZM rectifier our suggested plan for the security of the communication system through optical chaos. The MZM rectifier modulates the input signal using the light beam produced by the CW laser. To transmit the signal with less attenuation loss, the CW laser's frequency is set to 500THz. To enable the modulation of the input signal with the laser light, the extinction ratio of the MZM—defined as the ratio of two levels of optical power to the digital signal produced by the laser—was set at 50:50. The chaotic semiconductor laser's optical output was then provided to the MZM, where it was combined with this waveform. The semiconductor laser's operating frequency was maintained at approximately 500THz, allowing the two waveforms—the light produced by the input waveform modulated by the CW laser and the chaos produced by the semiconductor laser—to be properly mixed. Over a single-mode fiber, the optical adder output is sent after the input signal has been made safe in the optical field, [14]. On the receiving side, a signal was removed from a comparable chaos that was produced using double delay feedback techniques before the optical receiver or signal was detected by the photodiode. The first location where the signal was detected was the optical receiver, whose function was to transform the signal from the visual field to the electric field. A low-pass filter was then employed to further lessen the impact of noise and recover the input signal, [20].

# 4 Generating Chaotic Signal

Generating Chaotic signals by using a double delay feedback system:

Optical detection, encrypted communication, and a variety of other applications make regular use of chaotic lasers for a variety of reasons, including their cacophonous chaos, exceptional anti-jamming capabilities, and other advantages. Within the scope of this study is an investigation of the chaotic laser's efficiency at a cheap cost. It has been seen how well a semiconductor laser functions with double delayed feedback in the course of an experimental study conducted with the OPtiSystem simulator. The characteristics of this laser have also been established. Initially, the Mach-Zehnder modulator (MZM) was constructed by sending the chaotic laser output back into the system. The system incorporates a second time delay in addition to the adjustment of the dynamic gain coefficient. We study the enhanced chaotic system's feedback duration and intensity under various input bias current, frequency, and modulation beak current circumstances. The optoelectronic oscillator's (OEO) chaotic laser output is more complex and exhibits lower delay characteristics, according to the bifurcation diagram. These revelations were made, [21].

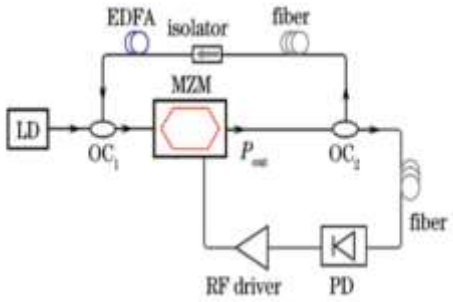



Fig. 3: Schematic for an OEO chaotic system with double delay feedback, [22]

Figure 3 depicts the chaotic system with a double feedback strategy. Figure 3, PD is a photodetector with a specific effect amplifier; LD is a continuous light laser; The MZM modulator is driven by a frequency (RF) driver; OC1 and OC2 are couplers; OC2 Light divides the MZM output into two; and finally, the RF and PD driver leads to the MZM optoelectronic reflection feedback. From the EDFA to the MZM optical feedback, the laser output is chaotic and has the power of Pout thanks to the MZM, [22].

Equation (1) represents the output property of the nonlinear device MZM of the OEO chaotic system with double delay feedback:

$$p_{out}=p_{in}\ cos^2\ [\frac{\pi V(t)}{2V_{\pi RF}}+\frac{\pi V_B}{2V_{\pi DC}}] \quad (1)$$

where VRF stands for the RF half-wave voltage, VDC for the bias half-wave voltage, and V (t) for the load on the MZM modulation voltage. The input optical power is shown by pin.

The development and simulation of an optical chaos-producing circuit with double delay feedback is accomplished with the help of the OptiSystem 16 software. Additionally, OptiSystem may be understood as a software package for optical communication devices. This software package gives users the ability to develop, test, and simulate optical links in the transmission layer of sophisticated optical networks. Figure 4 depicts the simulated circuit architecture of the proposed method, which makes use of built-in components and adheres to the appropriate standards. A MZM, amplifier, and photodetector (PD) are the components that make up this device. The MZM may be characterized as a device that is employed for the determination of the relative phase shifting between two collimated beams from a coherent source of the light either by altering the length of one of the arms or by inserting a sample in one of the beams' pathways. This can be accomplished in one of two ways: either by changing the length of one of the arms or by placing the sample in the path of one of the beams. MZM comes with two input ports as well as two output ports. Two couplers are utilized in the construction of a basic MZM. One coupler is located at the input and functions as a splitter, while the second coupler is located at the output and performs the duty of a combiner, [22].

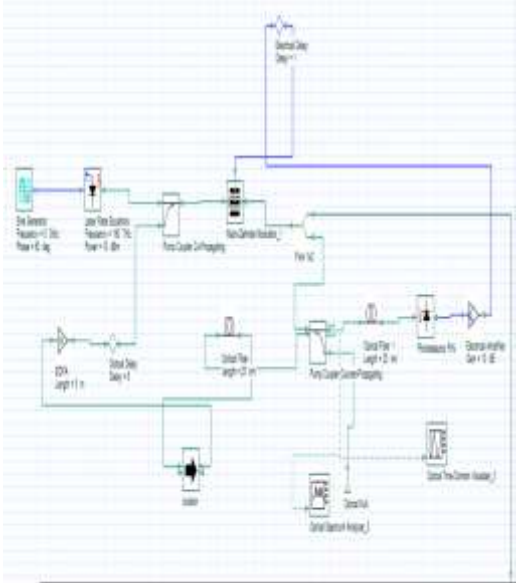


Fig. 4: The simulated diagram of a chaotic system (sub-system)

Light is shown to be coupled into two interferometer arms by an input coupler in Figure 4, and then recombined at an output-by-output coupler. The coupler produces two beams of light, each of which is equally strong, but only one of these is amplified by EDFA. After that, it is linked with the static fixed power laser that is generated by the continuous laser, and it is then entered into the MZM for a second time to carry out non-linear modulation and make chaotic lasers. The second one goes from the feedback arm (MZM) into the photodetector (PD) to transform an optical signal into an electrical signal. The photodetector is connected to the amplifier, which is subsequently coupled to the MZM feedback arm. Because the length of the optical channel along each of the two arms is different from one another, the phase shift that occurs as a result of the delay is a function of the wavelength of the input signal. Studies have been conducted to investigate the effects of MZM bias voltage on the chaotic behavior of OEFB. The output of the optoelectronic oscillator is sent back to the MZM over a delayed optical channel. This causes the gain coefficient of the original OEO to be dynamically altered, and it also adds an extra time delay to the system, which causes it to produce a more complicated and chaotic laser signal. The aforementioned features help construct a chaotic secure communication system that offers a better level of protection. The variation in the bias current and modulation peak current leads to the complexity chaotic to change. Table 1 shows the input parameters for generating the chaotic signal. With the decrease in the value of bias current, clear variation in the amplitude of pulses can be observed that is mean, chaotic behavior increased and the opposite happens with modulation peak current.

Table 1. Semiconductor laser Parameter of Chaotic Signal

| parameter | value |
|---|---|
| Frequency | 190 THz |
| Power | 10 dBm |
| Bias current | 70 mA |
| Modulation beak current | 40 mA |
| Threshold current | 33.45723 mA |
| Threshold power | 0.01516 mW |
| Frequency of current source | 5 GHz |
| Amplitude | 1 a.u |
| Phase | 90 Deg |

# 5 Result and Discussion

Simulations are performed with varying the length of the channel, the data rate of the system, and the power of the laser to perform an evaluation of the proposed setup. Since the NRZ pulse format is more efficient than the RZ format, we have chosen to use it. Figure 5 presents the encoded message that was received at a rate of 10 gigabits per second without any noise.

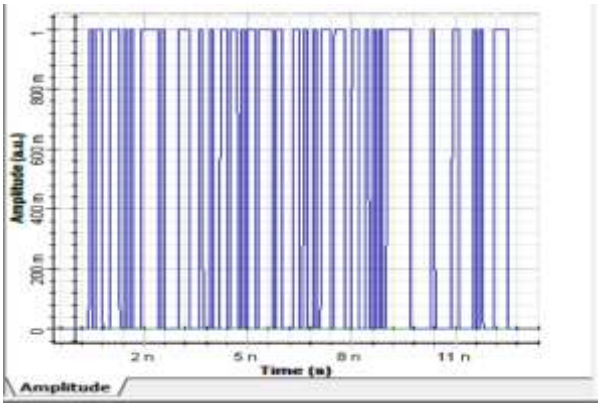



Fig. 5: Input encoded message

A continuous wave laser with an operating frequency of 500THz and a laser strength of 10 dBm is what is utilized here. In Figure 6, you can see the chaos that was created by the chaotic laser diode. The chaos that is produced in this method is exceedingly unpredictable and has amplitudes that are completely random. The disarray seen in Figure 6 may be utilized to conceal the information displayed in Figure 5.

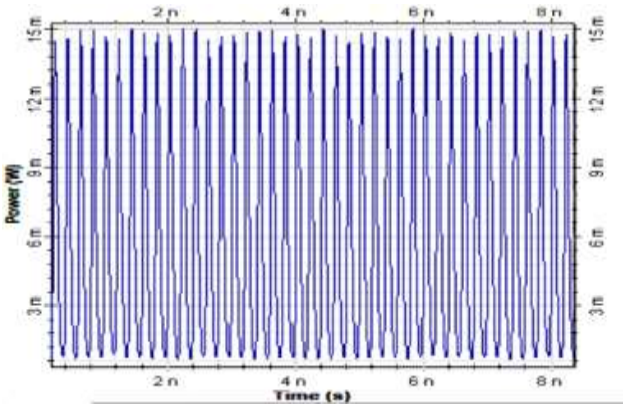



Fig. 6: Generated chaos

In the subsequent stage of our simulation model, optical adders are utilized to conceal the incoming signal within the produced chaos. Following the chaotic masking strategy allows for the mixing of both signals to take place within the optical domain. The intensity of the chaotic laser is adjusted to 10 dBm so that it may produce pulses with greater

amplitudes in comparison to the level of the message's amplitude. In addition to this, it is capable of fully encrypting the message while operating at 500 THz. Figure 7 illustrates a time domain signal that the invaders are unable to comprehend in any way. A person who does not have the appropriate information and understanding of the created chaotic signal is unable to recognize the original message signal that was transmitted from the transmitting end, as seen in Figure 7. This can be seen quite clearly in Figure 8. This ensured that our signal would not be intercepted by unauthorized parties and offered an adequate level of protection against potential invaders.

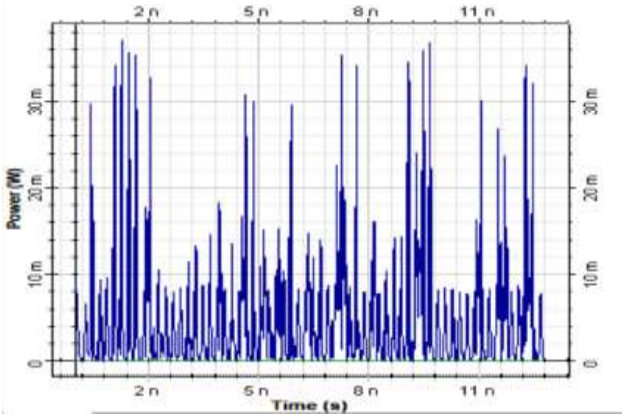
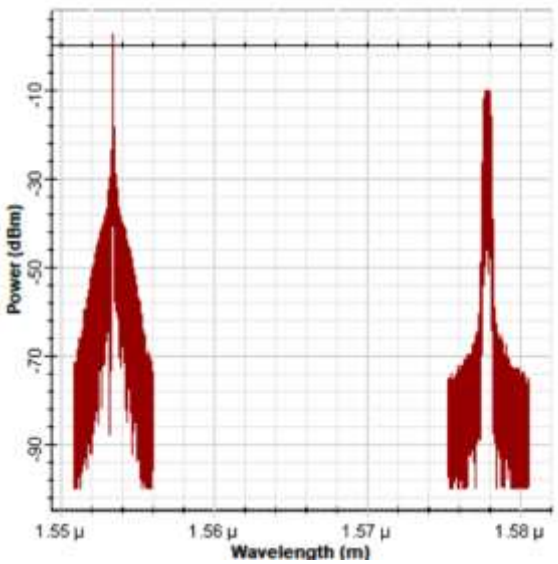


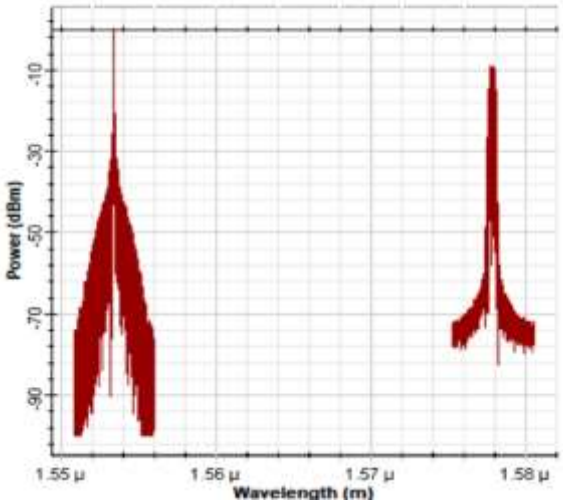

Fig. 7: Input message embedded in chaos

Analysing the signal in the frequency domain is another method that may be utilized to do an effect analysis of adding a security feature to an input message. To accomplish this goal, an optical spectrum analyzer is utilized. The change in the optical spectrum is seen in Figure 8 both before adding and after the subtraction of chaos to the signal. To reiterate, the intruder is unable to decipher the real information in the frequency domain.

At the receiving end, the chaotic signal that was found to have been contaminated with the official signal was removed from the similar chaos that had been generated by the second semiconductor laser. The signal was picked up by the photodiode, which then transformed it into a signal that was analogous to the signal that was initially coming in. To further purify the signal that was received, a low-pass filter was used. The unaltered and deciphered versions of the incoming signals are shown in Figure 8(a) and Figure (b), respectively. We determined the signal's Q-factor by measuring it (Figure 9) in preparation for long-distance transmission. We found that when the fiber lengths increased, the Q-factor dropped by a significant amount.




(a) : Before the addition of chaos, the optical spectrum of the input signal.




(b): After the addition of chaos, the optical spectrum of the input signal

Fig. 8(a) and (b): Before and after the addition of chaos, the optical spectrum of the input signal

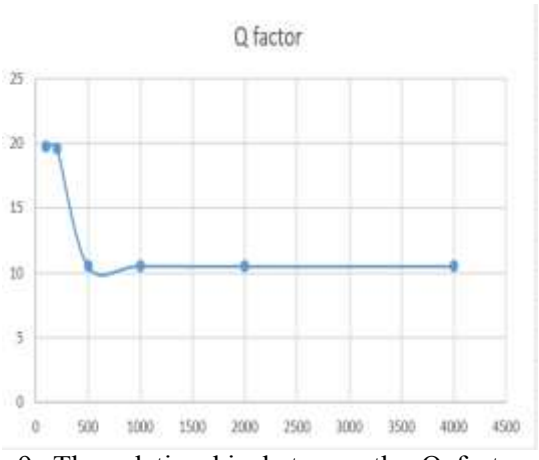



Fig. 9: The relationship between the Q factor and channel length

The next step involves calculating the bit error rate (BER) of the system against various lengths of optical fiber. Controlling the effects of dispersion and attenuation is required in order to carry out simulations. The results are displayed in Figure 10, which demonstrates that the system functions well up to a channel length of 4 km. After that, an exponential increase in bit error rate is detected, which suggests that it is feasible to recover the signal that was originally broadcast, although with errors. Since the suggested system is optimized for 10 Gbps, it can function satisfactorily up to a fiber length of 4 km because of this. An increase in the data rate will cause the channel lengths to be reduced to their lower limitations.

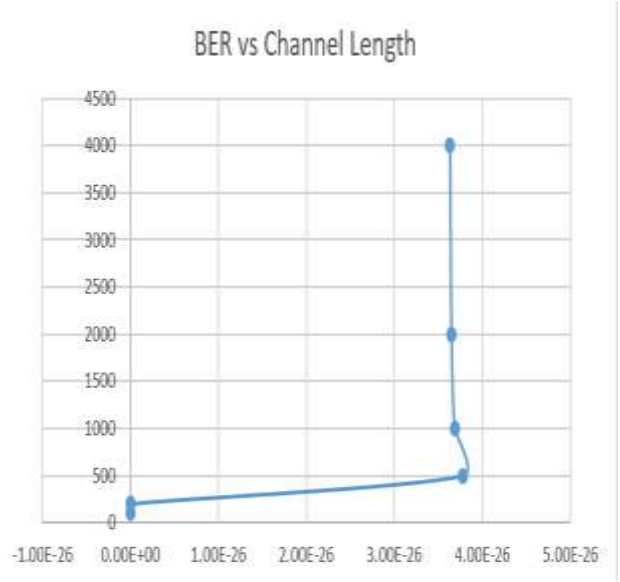



Fig. 10: Evaluation of performance (which is based on BER vs. length)

Table 2. RESULT of the simulation of Proposed double delay feedback with data rate (10Gbps)

| Channel Length | BER | Q factor |
|---|---|---|
| 100 m | $6.649506092 \times 10^{-38}$ | 19.7411 |
| 200 m | $3.266610488 \times 10^{-37}$ | 19.595 |
| 500 m | $1.928037362 \times 10^{-11}$ | 10.4998 |
| 1000 m | $1.882188397 \times 10^{-11}$ | 10.52 |
| 2000 m | $1.863913186 \times 10^{-11}$ | 10.503 |
| 4000 m | $1.855396335 \times 10^{-11}$ | 10.5034 |

The results of a comparison of the bit error rate and the Q-factor for various fiber lengths are presented in Table 2. After researching the bit error rate as well as the Q factor for fibers of varying lengths, the researchers concluded that the bit error rate was growing with the rising fiber lengths. On the other hand, the Q-factor decreased when the length of the fiber was increased. This nonlinear degradation, such as an amplifier and fiber non-linearity, is to blame for the dramatic fall in Q-factor that occurs with an increase in fiber length. Noise in the transmission channel, interference, distortion, issues with bit synchronization, and attenuation are all potential factors that might impact the bit error rate.

# 6 Conclusion

We suggested a method for the safe transmission of input signals that makes use of light that is visible to the human eye. The procedure of double delay feedback was employed to generate chaos, wherein the parameters were adjusted to get the desired bandwidth and amplitude. Subsequently, this disorder was integrated with incoming signals that had been altered by continuous-wave (CW) laser light before transmission through a single-mode optical fiber. The investigation and testing focused on the characteristics of chaos that obscure the incoming signal, to facilitate long-distance communication. The different lengths were deliberately selected with this objective in mind. Analyzed in both the frequency and temporal domains, the installation of security measures in the input signal was verified. An optical subtractor was employed to distinguish the incoming signals from the noise. Based on our inquiry and comparison with previous research, the QFactor of the received signal decreased to 10.5034 when the channel length was 4 kilometers, whereas it was 19.7411 when the channel length was 100 meters. These findings demonstrate favorable outcomes in comparison to prior research and the utilization of visible light technology. This technology is commonly employed in short-range underwater communications, the Internet, healthcare facilities, and various other applications.

*References:*

[1] A. Lender, "Correlative Digital Communication Techniques," *in IEEE Transactions on Communication Technology*, vol. 12, no. 4, pp.128-135, December 1964, doi:10.1109/TCOM.1964.1088964.

[2] C. Zhang, W. Zhang, X. He, C. Chen, H. Zhang, and K. Qiu, "Physically Secured Optical OFDM-PON by Employing Chaotic Pseudorandom RF Subcarriers," in *IEEE Photonics Journal*, vol. 9, no. 5, pp. 1-8, Oct. 2017, Art no. 7204408, doi 10.1109/JPHOT.2017.2754407.

[3] S. C. Gupta, *Textbook on optical fiber communication and its application*, PHI Learning Pvt. Ltd, 2018.

[4] C. Zhang, W. Zhang, X. He, C. Chen, H. Zhang, and K. Qiu, "Physical –Enhanced Secure Strategy for OFDM-PON Using Chaos and Deoxyribonucleic Acid Encoding, "in *Journal of Light wave Technology*, vol. 36, no. 9, pp. 1706-1712, 2018.

[5] T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," in *Optics express*, vol.26, no. 18, pp. 22857-22865, 2018.

[6] J. Ai, L. Wang, and J. Wang, "Secure Communications of CAP-4 and OOK Signals over MMF Based on Electro-optic Chaos," in *Optics letters*, vol. 42, no. 18, pp. 3662-3665, 2017, doi.org/10.1364/OL.42.003662.

[7] CH. Cheng, CY. Chen, JD. Chen, DK. Pan, KT. Ting, and FY. Lin., "3D Pulsed Chaos Lidar System," in *Optics Express,* vol. 26, no. 9, pp. 12230-12241, April 2018, doi.org/10.1364/OE.26.012230.

[8] CY Chen, CH Cheng, DK Pan, FY Lin., "Experimental Generation and Analysis of Chaos-Modulated Pulses for Pulsed Chaos Lidar Applications Based on Gain-Switched Semiconductor Lasers Subject to Optical Feedback," in *Optics Express*, vol. 26, no. 16, pp. 20851-20860, Aug 2018, doi.org/10.1364/OE.26.020851.

[9] M. Zhang, Y. Ji, Y. Zhang, Y. Wu, H. Xu, and W. Xu, "Remote Radar Based on Chaos Generation and Radio Over Fiber," in *IEEE Photonics Journal*, vol. 6, no. 5, pp. 1-12, Oct. 2014, Art no. 7902412, doi 10.1109/JPHOT.2014.2352628.

[10] M. Preishuber, T. Hütter, S. Katzenbeisser and A. Uhl, "Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2137-2150, Sept. 2018, doi: 10.1109/TIFS.2018.2812080.

[11] J. Ke, L Yi, G Xia, W Hu, "Chaotic Optical Communications Over 100-km Fiber Transmission at 30-Gb/s bit rate," in *Optics letters*, vol. 43, no.6, pp. 1323-1326, 2018, doi.org/10.1364/OL.43.001323.

[12] N. Xuan Quyen, K Kyamakya., "Chaos-Based Digital Communication Systems with Low Data-Rate Wireless Applications," In *Recent Advances in Nonlinear Dynamics and Synchronization*, pp. 239-269, Springer, 2018.

[13] B.Naderi, H. Kheiri, "Exponential Synchronization of Chaotic System and Application in Secure Communication" in *Optik-International Journal for Light and Electron Optics*, vol. 127, no.5, pp.2407-2412, March 2016.

[14] Mohammad Ali Khalighi,Murat Uysal, "Survey on Free Space Optical Communication: A Communication Theory Perspective," *IEEE Communications Surveys & Tutorials*, vol. 16 (4), p. 2231-2258, 26 June 2014.

[15] V. Gnanalakshmi, B.R.Santhoshi, R. N. Aswathy "Analysis of Chaos Masked Signal Transmission in Optical Communication Network,", in *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol.5, no.3, March 2018.

[16] R. Shahzadi, S. M. Anwar, F. Qamar, M. Ali, J. J. P. C. Rodrigues and M. Alnowami, "Secure EEG Signal Transmission for Remote Health Monitoring Using Optical Chaos," in *IEEE Access*, vol. 7, pp. 57769-57778, 2019, doi: 10.1109/ACCESS.2019.2912548.

[17] A. Ali, H. Naveed, F. Qamar, R.Shahzadi., "Design and Analysis of Secure RoF Based Communication in 5G Fronthaul," *2020 International Conference on Cyber Warfare and Security (ICCWS)*, Islamabad, Pakistan, 2020, pp. 1-6, doi: 10.1109/ICCWS48432.2020.9292380.

[18] AW. Abdulwahhab, A. K. Abass, M. A. Saleh, Fareed F. Rashid, "Enhancing Performance of Optical Chaotic–Based *Secure* Fiber-Optic Communication System," in *Opt. Quant Electron.*, vol.55, doi.org/10.1007/s11082-023-04757-1.

[19] E. A. Fadil, , A. K. Abass, S. R. Tahhan, "Design and Simulation of Optical Chaotic-Based Secure Hybrid Optical Communication System," in *J. Opt.*, vol.52,pp1887–1896, March 2023, doi.org/10.1007/s12596-023-01143-8.

[20] G Alvarez, S Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," in *International Journal of Bifurcation and Chaos*, vol.16,no.8, pp. 2129-2151, 2006.

[21] R. K. Al Khafaji, K. A.M. Al Naimee, "Chaos Modulation by Mach-Zehnder Interferometer," *in International Journal of Engineering Research & Science*, vol.3, no.1, pp. 2395-6992, January 2017.

[22] R. I. Ibrahim, "Enhancement of Optical Chaos Generator using Double Delayed Feedback", in *Kuwait Journal of Science*, vol.50,no.3, 2023,doi:10.48129/kjs.17025.

**Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)**

- Huda Kadhim has implemented the simulation in optisystem.
- Ibrahim Abdullah has supervised on the paper.

**Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself**

No funding was received for conducting this study.

**Conflict of Interest**

The authors have no conflicts of interest to declare.