aurum

AURUM MÜHENDİSLİK SİSTEMLERİ VE MİMARLIK DERGİSİ
AURUM JOURNAL OF ENGINEERING SYSTEMS AND ARCHITECTURE

Cilt 9, Sayı 1 | Yaz 2025
Volume 9, No 1 | Summer 2025

A NOVEL COLOR IMAGE ENCRYPTION ALGORITHM BASED ON SIX-DIMENSIONAL (6D) HYPER-CHAOTIC SYSTEMS AND FIBONACCI Q-MATRIX FOR ENHANCED CYBERSECURITY IN OPTICAL COMMUNICATIONS

Wisam Mohammed Enad ALMUSAWI[1], N. Özlem ÜNVERDİ[2*]
[1] Department of Electrical and Computer Engineering, Istanbul Altinbas University, Turkey
wissammohmmed@gmail.com
(https://orcid.org/ 0009-0008-2259-5312)
[2] Department of Electronics and Communication Engineering, Yildiz Technical University, Turkey
unverdi@yildiz.edu.tr
(https://orcid.org/0000-0002-3995-3410)

Received: 25.04.2025
Accepted: 06.05.2025
Published: 30.06.2025
*Corresponding author

Research Article
pp.11-36

10.53600/ajesa.1683527

Abstract

This study introduces a novel approach to color image encryption aimed at enhancing the security of optical communication systems. The proposed method integrates six-dimensional (6D) hyper-chaotic systems with the Fibonacci Q-matrix to address the increasing complexity and demands of modern encryption. The dynamics of hyper-chaos generate highly intricate and unpredictable patterns that exhibit strong resistance to decryption attempts. Furthermore, the incorporation of the Fibonacci Q-matrix facilitates a unique switching mechanism that enhances the flexibility and robustness of the encryption process. This switching strategy leverages saturated rows of Fibonacci sequences, thereby increasing the complexity of reverse-engineering the encryption scheme. Experimental results demonstrate that the proposed algorithm significantly improves the confidentiality and integrity of data transmitted over optical channels. Its high sensitivity to initial conditions and key parameters renders brute-force attacks and statistical analyses ineffective. Integrating the Fibonacci Q-matrix also enhances algorithmic efficiency, making it suitable for high-speed data transmission within optical networks. Given the growing prevalence of cyber threats, the development of advanced encryption algorithms is essential for securing sensitive information in optical communication systems. This research not only contributes to the field of secure optical data transmission but also provides a practical framework for implementing hyper-chaotic systems and mathematical constructs in real-world applications. As such, it offers promising potential for enhancing the security and reliability of data transfer across various domains.

Keywords: Image Encryption, 6D Hyper-chaotic Systems, Fibonacci Q-Matrix, Cryptography, Security Analysis.

GELİŞMİŞ SİBER GÜVENLİK İÇİN OPTİK İLETİŞİMDE ALTI BOYUTLU HİPER-KAOTİK SİSTEMLER VE FİBONACCİ Q-MATRİSİ TABANLI YENİ BİR RENKLİ GÖRÜNTÜ ŞİFRELEME ALGORİTMASI

Özet

Bu çalışma, optik haberleşme sistemlerinin güvenliğini artırmaya yönelik olarak renkli görüntü şifrelemesi alanında yenilikçi bir yaklaşım sunmaktadır. Önerilen yöntemde, Fibonacci Q-Matrisi ile kullanılan altı boyutlu (6B) hiper-kaotik sistemler, şifreleme karmaşıklığına yönelik özgün bir çözüm sağlamaktadır. Hiper-kaotik dinamikler sayesinde, şifre çözmeye karşı yüksek direnç gösteren karmaşık ve öngörülemez desenler üretilmektedir. Fibonacci Q-Matrisinin kullanımı ise, geçiş (anahtar değiştirme) stratejisinin özgünlüğünü ortaya koymakta ve şifreleme algoritmasının esnekliğini artırmaktadır. Bu geçiş mekanizması, Fibonacci dizilerinin satırlarının doygunlaştırılması yoluyla gerçekleştirilmekte olup, şifreleme stratejisinin çözümünü zorlaştırarak güvenliği daha da üst seviyeye taşımaktadır. Elde edilen sonuçlar, optik iletişim kanalları üzerinden iletilen verilerin gizliliği ve bütünlüğünü sağlamada önerilen algoritmanın yüksek düzeyde etkili olduğunu göstermektedir. Geliştirilen algoritma, yalnızca teorik bir katkı sunmakla kalmayıp, 6B hiper-kaotik sistemin avantajlarından yararlanarak optik iletişim sistemlerinde pratik olarak uygulanabilir bir yapı sunmaktadır. Ayrıca, Fibonacci Q-Matrisinin algoritmaya entegrasyonu, şifreleme sürecinin verimliliğini ve güvenliğini artırmakta; böylece yüksek hızlı veri iletimi gereksinimlerini karşılayan etkili bir çözüm sağlamaktadır.

Artan siber tehditler bağlamında, optik kanallar üzerinden iletilen bilgilerin güvenliğinin ve gizliliğinin sağlanması, ileri düzey şifreleme algoritmalarının geliştirilmesini gerekli kılmaktadır. Bu çalışma, ilgili alandaki literatüre katkı sunmakta ve çeşitli uygulama alanlarında optik haberleşme sistemlerinin daha güvenli ve güvenilir veri aktarımı gerçekleştirmesine olanak tanımaktadır.

Anahtar Kelimeler: Görüntü Şifreleme, 6B Hiper-kaotik Sistemler, Fibonacci Q-Matrisi, Kriptografi, Güvenlik Analizi.

1. Introduction

In the digital age, as information is continuously exchanged across various communication channels, ensuring the security and reliability of data transmission over diverse networks has become a critical priority. Among these channels, optical fiber networks represent one of the most efficient communication systems, offering high-capacity and high-speed data transmission. However, despite their advantages, optical fiber networks remain inherently vulnerable to cyber-attacks. To address this challenge, recent research has explored the integration of hyper-chaotic cryptographic systems with mathematical constructions such as the Fibonacci Q-matrix to increase encryption complexity and resilience.

Several studies have proposed innovative techniques to enhance the security of optical and visual communication. For instance, Shaima introduced a method to increase image randomness by merging four color images into sequences based on their information content, applying random splitting, transmitting them through a secure key mechanism, and employing the Fibonacci Q-matrix to introduce further confusion (Aldin et al., 2024). In a related approach, Hala and Sarah demonstrated a color image separation encryption technique by applying confusion and diffusion processes independently to each channel using the Lorenz chaotic system in conjunction with partial ordering and the Fibonacci Q-matrix (Mohamed et al., 2024).

Elaf proposed the design of a chaotic and cloud-based visual communication system to enhance security in free-space optical (FSO) communication, emphasizing its applicability in real-time data transmission (Fadil et al., 2023). Similarly, Udayakumar and Sathiyaprasad suggested improvements to optical communication systems through high modulation schemes and quantum coding techniques to mitigate transmission noise, integrating wave-based security methods with automated high-bitrate optical communication (Allimuthu et al., 2023).

Fatma demonstrated the implementation of revocable hybrid bifatmaic authentication by combining hyper-chaotic dynamics with the Fibonacci Q-matrix for secure image encryption (Hossam Eldein Mohamed & El-Shafai, 2024). Maharshi developed an RGB channel-based encoding technique that utilizes pixel position and value adjustments governed by a 6D hyper-chaotic system and symmetrical maps, with a confusion phase that generates random sequences for encryption (Panwar et al., 2024). Likewise, Xiaoyuan and Chunhua proposed a color image encryption algorithm based on a 3D memristor-driven hyper-chaotic system. Their approach included generating initial keys from plaintext images and applying pixel- and bit-level permutations via a hash table structure built on chaotic sequences (Wang et al., 2023).

Duzhong introduced a coding scheme named HCZRNA for color image encryption, combining a 6D hyper-chaotic system with zigzag propagation and RNA-based transformations. This method employed pseudo-random arrays to replace the original image, embedding it into a three-dimensional cube, followed by converting the diffused image into an RNA codon matrix to enhance security (Zhang et al., 2021).

Furthermore, Khalid and Sara proposed an image encryption algorithm based on fractional-order chaotic systems. Their method utilized a 4D hyper-chaotic system with the Fibonacci Q-matrix in a three-stage process involving separation into RGB channels, independent confusion and diffusion phases, and block-wise operations (2×2) based on Fibonacci Q-matrix dynamics (Hosny et al., 2022).

In this study, we propose a novel encryption scheme that combines the dynamics of a six-dimensional (6D) hyper-chaotic system with the Fibonacci Q-matrix. Unlike approaches that merely increase encryption complexity, our method introduces structured yet unpredictable patterns through excessive chaotic dynamics, thereby significantly increasing resistance to decryption attempts. The Fibonacci Q-matrix is used to enhance the cryptographic process by contributing an additional layer of mathematical complexity, which strengthens the algorithm's resistance to various forms of cyberattack.

Our algorithm begins by using the 6D hyper-chaotic system to scramble the pixel coordinates of the original image. From the chaotic sequences generated, only three are randomly selected to initialize the scrambling process. The encrypted image is then further processed by deploying sub-blocks via the Fibonacci Q-matrix to create additional confusion and diffusion. The integration of these features demonstrates the robustness and reliability of the proposed method in protecting sensitive visual data during transmission over optical communication channels.

As cyber threats continue to escalate, the development of robust, unpredictable encryption techniques is essential to safeguard data privacy and integrity across optical communication networks. The proposed approach contributes to this growing body of research by offering a highly secure, efficient, and theoretically grounded encryption framework suitable for real-world optical communication systems.

2. Optical Communication System and Security

Optical communication systems are transforming the landscape of data transmission by enabling the transfer of information at exceptionally high speeds and large capacities, surpassing the limitations of traditional electronic systems. These systems rely on the fundamental principles of light propagation through optical fibers, leveraging the velocity of photons to transmit data across extensive distances with minimal power loss and low attenuation. The core advantage of this technology lies in its capacity to embed data within optical signals, transmit them efficiently through fiber-optic channels, and accurately recover and decode the embedded information at the receiving end. This marks a paradigm shift in telecommunications, facilitating the global exchange of vast amounts of data and paving the way for next-generation communication networks.

In optical communication systems, data is modulated onto light waves and transmitted through optical fibers, allowing for long-distance data transmission without the need for frequent signal amplification and with significantly

high data throughput (Senior, 2009). The efficiency of such systems is largely attributable to the minimal signal attenuation and electromagnetic interference experienced by light as it propagates within optical fibers. Moreover, optical communication is not limited to fiber-based systems; it also encompasses free-space optical (FSO) communication, in which light is transmitted through the atmosphere or space vacuum. This method is widely used in satellite communications and holds potential for future interplanetary communication applications.

Ongoing advancements in optical communication technologies aim to further improve the capacity, transmission speed, and range of these systems. For instance, Dense Wavelength Division Multiplexing (DWDM), a technique that allows multiple optical wavelengths to carry data simultaneously over a single optical fiber, has significantly enhanced the data-carrying capacity of optical networks (Koman & Ünverdi, 2019; Senior, 2009).

As optical communication becomes the backbone technology supporting the exponential growth of global data traffic (Aldin et al., 2024; Mohamed et al., 2024), its security and resilience against intrusion have become critical concerns. The widespread deployment of optical networks has introduced new vulnerabilities, prompting the development of advanced encryption methods and secure transmission techniques. Among these are optical vortices and chaotic signal generators, which are utilized to establish synchronized chaotic communication links. Such technologies are essential for cybersecurity, cryptography, and secure information systems, providing confidentiality and integrity in data transmission (Fadil et al., 2023).

Moreover, optical communication systems are increasingly being integrated into intelligent surveillance infrastructures and biometric recognition platforms. Their implementation enhances data protection, enables rapid threat detection, and supports efficient emergency response mechanisms, thereby contributing to a safer and more secure environment.

Given the pivotal role of optical communication in high-speed data transmission, concerns regarding cybersecurity have attracted significant scholarly attention. Researchers have proposed various strategies to ensure secure communication, including chaotic encoding of phase fields, the use of chaotic optical signals in hybrid free-space/fiber-optic (FSO/FO) systems, and cluster chaos synchronization in semiconductor laser networks. These methods aim to establish robust encryption frameworks that resist unauthorized access and signal compromise. Furthermore, the integration of quantum encryption techniques is being explored to achieve even higher levels of data security (Allimuthu et al., 2023; Hossam Eldein Mohamed & El-Shafai, 2024).

In summary, the evolving domain of optical communications not only underpins modern high-speed networks but also necessitates the parallel development of advanced encryption and cybersecurity mechanisms to protect sensitive data throughout its transmission lifecycle.

3. Hyper-chaotic Systems and Dynamics

Chaos theory is recognized as an interdisciplinary field concerned with the fundamental patterns and governing laws of dynamic systems. A chaotic system is highly sensitive to its initial conditions, which can lead to unpredictable and divergent outcomes (Murillo-Escobar et al., 2019). Even minor variations in the initial state may result in significantly different trajectories, a phenomenon commonly referred to as the "butterfly effect." Although deterministic systems evolve based solely on their current state and a set of governing equations (Moysis et al., 2023), their behavior can remain unpredictable over time due to this extreme sensitivity to initial conditions.

The study of chaotic—or anarchic—systems involve analyzing their inherent complexity and dynamic behavior. Researchers utilize mathematical tools such as recurrence plots and Poincaré maps to investigate chaotic trajectories and attractors. Despite being governed by deterministic laws, chaotic systems resist long-term predictability due to the exponential divergence of nearby trajectories.

Highly chaotic or hyper-chaotic systems exhibit a greater degree of complexity than standard chaotic systems, as they can produce multiple positive Lyapunov exponents and a wider range of chaotic attractors. These systems are particularly sensitive to initial conditions, making them highly effective for use in encryption, where even the slightest alteration in input can yield vastly different decryption outputs (Futami et al., 2020). This property is typically modeled using systems of nonlinear ordinary differential equations, and hyper-chaotic behavior can be generated by coupling or expanding these equations.

Examples of such systems include the Lorenz-96 model, the Rössler system with multiple attractors, and the highly complex Chen system, all of which exhibit intricate dynamics within high-dimensional phase spaces (Hosny et al., 2022). Due to their inherent unpredictability and structural complexity, hyper-chaotic systems are especially well-suited for cryptographic applications, where the goal is to ensure robustness against unauthorized access and resistance to cryptanalytic attacks.

4. Fibonacci Q-Matrix

The Fibonacci Q-matrix is constructed from a sequence of numbers in which each term is the sum of the two preceding terms, typically represented as (1, 1, 2, 3, 5, 8, 13) (Aldin et al., 2024; Mohamed et al., 2024). This matrix is formed by systematically arranging Fibonacci numbers into a square matrix, where each row and column reflects a progressive Fibonacci sequence. The Q-matrix exhibits inherent properties such as self-similarity, fractal structure, and exponential growth, which make it particularly valuable in a wide range of mathematical and computational applications. These characteristics have led to its widespread adoption in the field of cryptography.

In particular, the Fibonacci Q-matrix has been effectively utilized in image encryption schemes (Hossam Eldein Mohamed & El-Shafai, 2024; Mohamed et al., 2024). By integrating pixel values with elements of the matrix, it facilitates the dispersion of information across the image. This blending enhances the security, robustness, and unpredictability of the encryption process by obscuring pixel patterns and increasing resistance to statistical and brute-force attacks.

5. Proposed Methodology Based on 6D Hyper-Chaotic System and Fibonacci Q-Matrix

The proposed image encryption approach utilizes two primary stages, combining the complexity of a six-dimensional (6D) hyper-chaotic system with the structural advantages of the Fibonacci Q-matrix for the secure encoding of color images. Initially, the 6D hyper-chaotic system is employed to scramble the pixel coordinates of the original image. From the chaotic sequences generated, three are randomly selected to construct the initial condition for the encoding process. This dynamic scrambling enhances unpredictability and sensitivity to initial parameters.

Subsequently, the technique applies the Fibonacci Q-matrix to propagate the sub-blocks of the scrambled (blurred) image. This dual-stage process enables the dispersion of information throughout the image, effectively strengthening the encryption. According to the experimental results, the proposed method provides robust and efficient encryption of color images, highlighting both its theoretical and practical contributions to the field.

This technology integrates a high level of security by leveraging the combined strength of the Fibonacci Q-matrix and the 6D hyper-chaotic system. The algorithm's large key space offers strong resistance against brute-force attacks, while its structure effectively withstands a broad spectrum of potential cryptanalytic attacks. The performance evaluations validate the proposed method's effectiveness, demonstrating its potential for secure image transmission in advanced communication systems.

Mathematical analyses often reveal the non-linear and dynamic nature of chaotic functions, which inherently produce unpredictable behavior (Hossam Eldein Mohamed & El-Shafai, 2024; Liu et al., 2020). Prior studies have shown that hyper-chaotic systems, which are characterized by higher dimensional complexity, exhibit more intricate dynamics than their lower-dimensional counterparts. A system is considered hyper-chaotic if it possesses a minimum of four dimensions and at least two positive Lyapunov exponents (Jiang et al., 2021). The specific 6D hyper-chaotic system used in this study is defined as follows:

$$\begin{cases} X1 = a(X2 - X1) + X4 - X5 - X6 \\ X2 = CX1 - X2 - X1X2 \\ X3 = -bX3 + X1X2 \\ X4 = dX4 - X2X3 \\ X5 = eX6 + X3X2 \\ X6 = rX1. \end{cases} \quad (1)$$

In this system, X1, X2, X3, X4, X5, and X6 represent the state variables, while a, b, c, d, e, and r are constant values. For the purposes of this work, the constants were assigned the following values: a = 10, b = 8/3, c = 28, d = -1, e = 8, and r = 3. These parameter values guarantee that the system exhibits hyper-chaotic behavior, characterized by at least two positive Lyapunov exponents and a negative sum of all exponents.

The Fibonacci sequence Fn is defined recursively by:

$$F_n = F_{n-1} + F_{n-2},\ n > 1. \quad (2)$$

where $F_1 = F_2 = 1$.

The associated Fibonacci Q-matrix is defined as:

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}. \tag{3}$$

Raising the Q-matrix to the nth power yields:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}. \tag{4}$$

The determinant of the Q-matrix at power n is given by:

$$\text{Det}\,(Q^n) = F_{n+1}F_{n-1} - F_n^2 = (-1)^n. \tag{5}$$

The inverse of the Q-matrix at power n Q^{-n} is expressed as:

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix}. \tag{6}$$

These mathematical foundations provide the structural basis for the encryption mechanism, enabling efficient transformation and propagation of image data during the encoding process. The integration of hyper-chaotic dynamics with Fibonacci-based transformations enhances both the complexity and security of the proposed image encryption algorithm.

6. Encryption and Decryption Algorithm

The primary objective of encryption is to transform readable information into an unintelligible format, thereby preventing unauthorized access or tampering. In the proposed method, the encryption process is structured around two fundamental stages: confusion and diffusion (Aldin et al., 2024; Hossam Eldein Mohamed & El-Shafai, 2024). Pixel values and their spatial arrangements are altered accordingly.

The confusion phase leverages a six-dimensional (6D) hyper-chaotic system. Initially, the unmodified (plain) image is used to compute the initial conditions of the system. The system is iteratively computed to generate a sequence, from which three chaotic sequences (x1, x3 and x5) are extracted. The sorted version of the resulting sequence is then used to scramble the pixel positions of the image, producing a confused image.

Following this, the diffusion phase is conducted using the Fibonacci Q-matrix. The scrambled image is divided into sub-blocks, and each block is propagated using a matrix transformation based on a power of the Q-matrix. Together, these two steps—confusion and diffusion—yield the final encrypted image. The full encryption procedure is described in Algorithm 1.

Algorithm 1: Image Encryption Procedure

1. Set i =1.

2. Transform the image matrix into a one-dimensional vector P.

3. Compute the initial key of the hyper-chaotic system using:

$$X_1 = \frac{\sum_{i=1}^{MN} P(i) + (M.N)}{2^{32} + (M.N)} \tag{7}$$

and

$$X_i = \text{mod}\,(X_{i-1}.\,10^6, 1)\ i = 2, 3,.., 6. \tag{8}$$

4. With initial conditions (X_1, X_2, …, X_6), iterate the hyper-chaotic system (Equation 1) for N_0 + MN/3 times and discard the first N_0 values.

5. Construct a new sequence L of size M × N, and extract three sequences (X_1, X_3, and X_5).

6. Sort L in ascending order and record the index positions as vector S.

7. Generate the scrambled sequence R using:

$$R_i = P(S_i), i = 1, \ldots, MN. \tag{9}$$

8. Reshape R into a matrix R′ and divide it into sub-blocks of size 2 × 2.

9. Multiply each of the 2 × 2 sub-blocks of R′ by Q^{10}, the tenth power of the Fibonacci Q-matrix to obtain the Chipper image C:

$$\begin{bmatrix} C'_{i,j} & C'_{i,j+1} \\ C'_{i+1,j} & C'_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} R_{i,j} & R_{i,j+1} \\ R_{i+1,j} & R_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix} mod\ 256 \tag{10}$$

where i = 1:3:M, and j = 1:3:N.

10. Set I = C, and increment i.

11. Repeat Steps 2 to 8 for i <= 2.

Decryption Algorithm

Decryption is the inverse process of encryption and aims to restore the original image from the encrypted data. The following steps outline the decryption procedure:

1. Divide the encrypted image C into sub-blocks. For each block, apply the inverse transformation using Q^{-10}:

$$Q^{-n} = \begin{bmatrix} D'_{i,j} & D'_{i,j+1} \\ D'_{i+1,j} & D'_{i+1,j+1} \end{bmatrix} = \begin{bmatrix} C_{i,j} & C_{i,j+1} \\ C_{i+1,j} & C_{i+1,j+1} \end{bmatrix} \begin{bmatrix} 34 & -55 \\ -55 & 89 \end{bmatrix} mod\ 256 \quad (11)$$

where i = 1:3:M and j = 1:3:N.

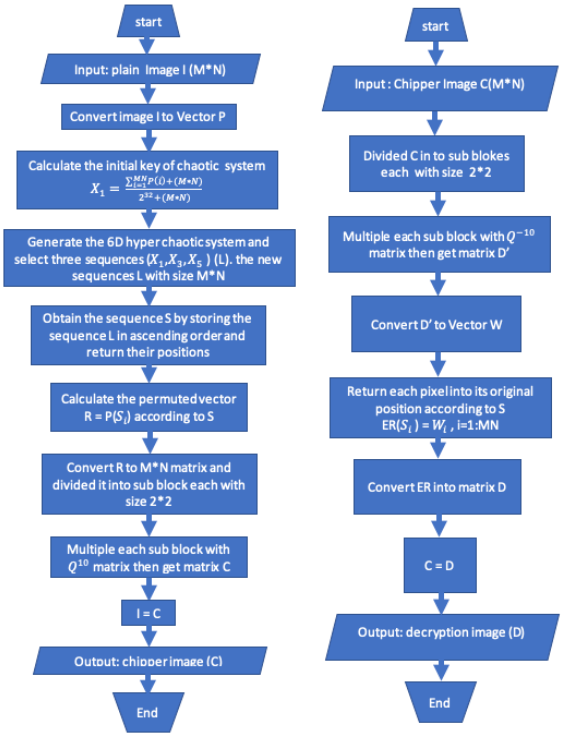
2. Construct vector W from the disordered image matrix D′ obtained in Step 1.

3. Use the permutation vector S (recorded during encryption) to restore the original pixel order:

$$ER(S_i) = W_i,\ i = 1, \dots, MN \quad (12)$$

4. Reshape the vector ER into the original image matrix D.

5. Two decryption passes are executed to obtain the final recovered image.



(a) Encryption Process **(b) Decryption Process**

Figure 1. Flowcharts of the Proposed Algorithm.

7. Testing Encryption in an Optical Communication Environment

The performance of the proposed encryption algorithm was assessed using a series of standard color images with varying resolutions. Simulations were conducted in MATLAB (R2023b) and implemented in OptiSystem 21 (Opti-Wave Corporation) on a server equipped with 512 GB RAM and dual Xeon® E5-2680 v4 processors at 2.40 GHz. A range of measurement instruments, outlined in **Figure 2** and **Table 1**, were employed to evaluate system performance.

The Bit Error Rate (BER) and Q-factor were calculated to quantify the effects of the encryption technique on the optical communication channel. A continuous-wave (CW) laser with an output power of 10 dBm served as the optical source. The signal was transmitted through an optical fiber, and its waveform, eye pattern, and spectral characteristics were recorded using an optical spectrum analyzer, photo-voltameter, energy meter, BER analyzer, and eye-chart analyzer. The BER, Q-factor, and eye height are widely recognized metrics for evaluating signal quality and integrity in optical communications.

Table 1. Sample Number and Resolution Specifications of the Color Images.

	Image Sample	Image Resolution
1	Test1	600*400 px
2	Test2	720*540 px
3	Test3	1920*1200 px
4	Test4	1024*701 px

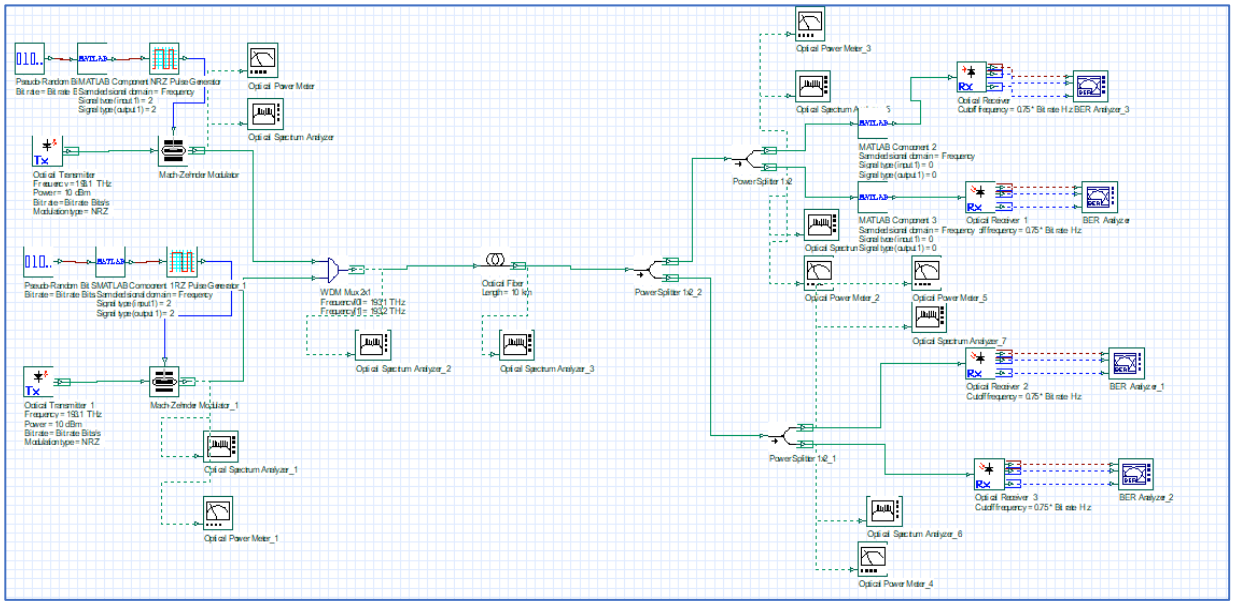


Figure 2. Schematic of the Hybrid WDM System Circuit Comprising Two Input Channels Employing Mach-Zehnder Modulators for Encryption. The System is Driven by a Laser Source with an Input Power of 10 dBm and Provides four Signal Outputs at the Receiver.

Figure 2 illustrates a hybrid WDM system incorporating two input channels encrypted by Mach–Zehnder modulators. Four receiver outputs were monitored to assess performance.

OptiSystem enabled comprehensive modeling, monitoring, and evaluation of the signal throughout the optical transmission chain, with representative block diagrams shown in **Figures 2, 12, and 19**. Tests were conducted over a 10 km fiber span to determine the impact of encryption under real-world transmission conditions. This included

analysis of both input and output signals and an assessment of encryption/decryption performance in practical optical fiber links. Variations in source frequency, laser power, and fiber length were also evaluated.

Figures 3 and 4 present the input optical spectrum, focused on the 1.550–1.554 μm wavelength range. Key spectral parameters—center wavelength, span, and resolution bandwidth—were recorded (resolution bandwidth = 0.1 nm). These measurements are critical for assessing source performance and transmission fidelity.

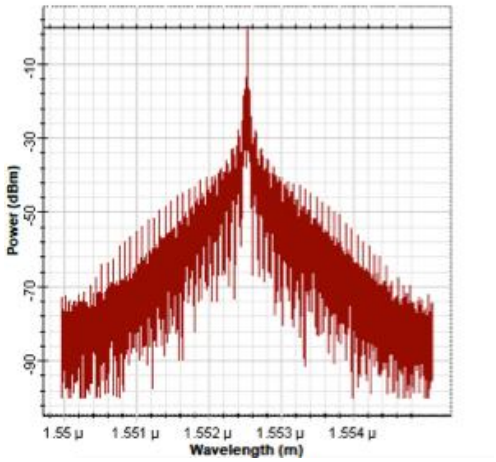


Figure 3. Optical Spectrum Analyzer Output for the Encrypted Input Signal.

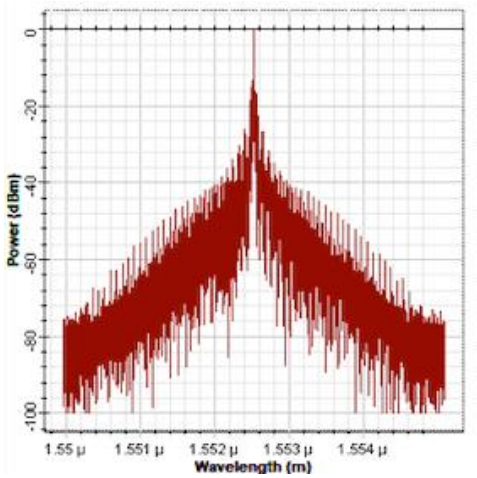


Figure 4. Optical Spectrum Analyzer 1 Output for the Encrypted Input Signal.

Figures 5–7 depict output spectra measured under encryption for wavelengths between 1.5501 and 1.5593 μm, demonstrating the spectral impact of the encryption process.

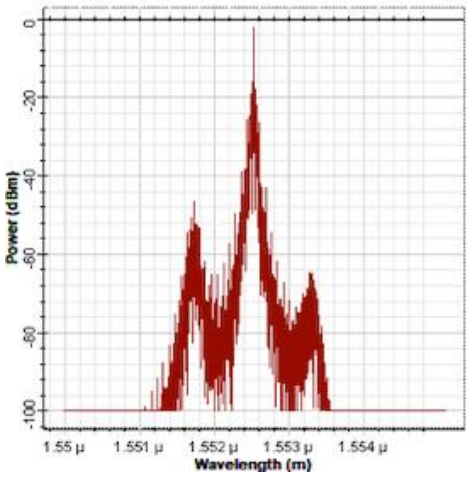


Figure 5. Optical Spectrum Analyzer 3 Output for the Encrypted Output Signal.

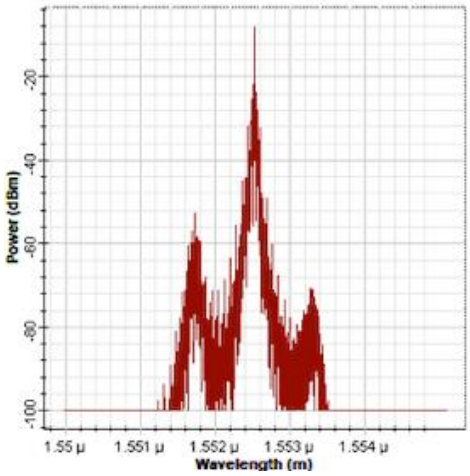


Figure 6. Optical Spectrum Analyzer 4 Output for the Signal from the Power Splitter in Branch 2.

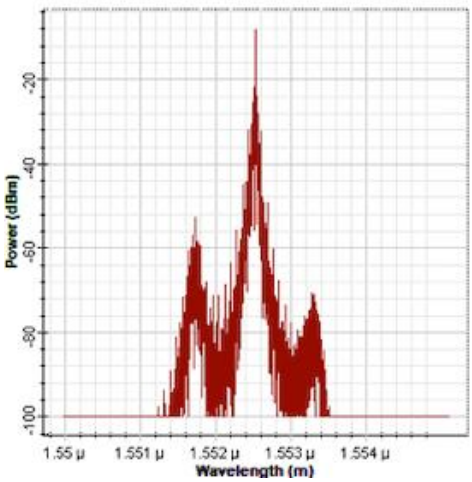


Figure 7. Output of the Optical Spectrum Analyzer for the Signal Obtained from the Power Splitter in Branch 3.

Figures 8–11 illustrate the corresponding spectral analyses, with each primary graph displaying a red spectral line that represents the energy distribution across a wavelength range of 1.5501 µm to 1.5593 µm. Optical spectrum

analyzers are instrumental in characterizing light sources and evaluating optical signal properties, particularly within the domains of telecommunications and fiber-optic systems.

Figure 8 demonstrates successful signal reconstruction with minimal distortion, thereby confirming the fidelity and reliability of the decryption process. In **Figure 9**, the pronounced eye opening indicates a low bit error rate (BER), signifying accurate data recovery following decryption. **Figure 10** exhibits significant eye closure, which reflects the obfuscation of the signal and thereby attests to the robustness of the encryption scheme. Similarly, the heavily distorted eye diagram in **Figure 11** further affirms the strength of the encryption, effectively preventing unauthorized signal interpretation.

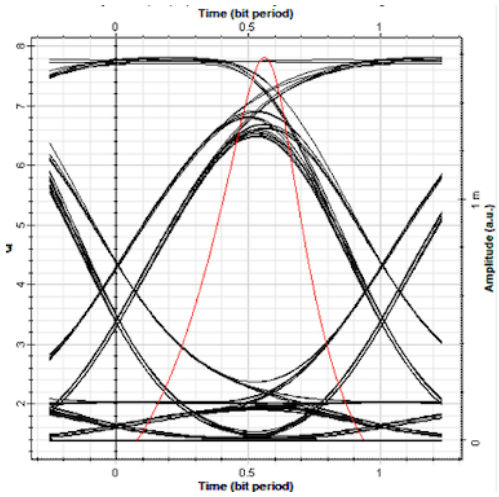


Figure 8. BER Analyzer with Eye Diagram for Output 1 Showing the Decrypted Signal.

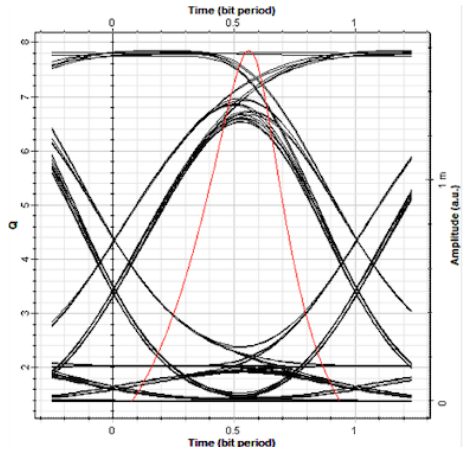


Figure 9. BER Analyzer 1 Displaying the Eye Diagram for Output 2 with the Decrypted Signal.

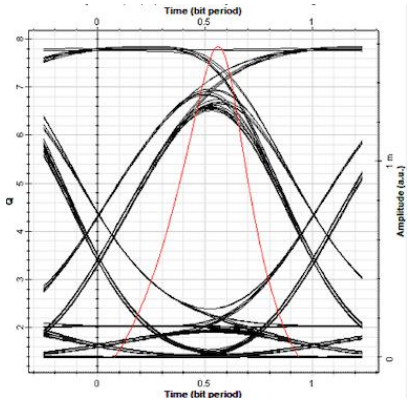


Figure 10. BER Analyzer 2 Displaying the Eye Diagram for Output 3 with the Encrypted Signal.

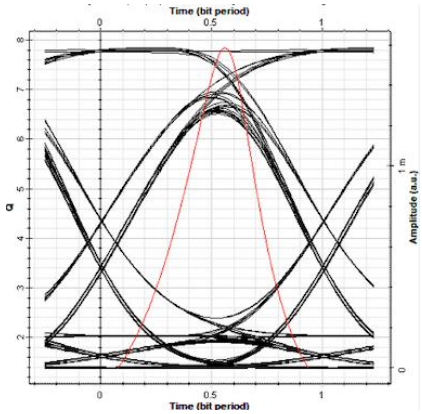


Figure 11. BER Analyzer 3 Displaying the Eye Diagram for Output 4 with the Encrypted Signal.

Likewise, similar results for the FTTH configuration and additional WDM tests are depicted in **Figures 12–23**.

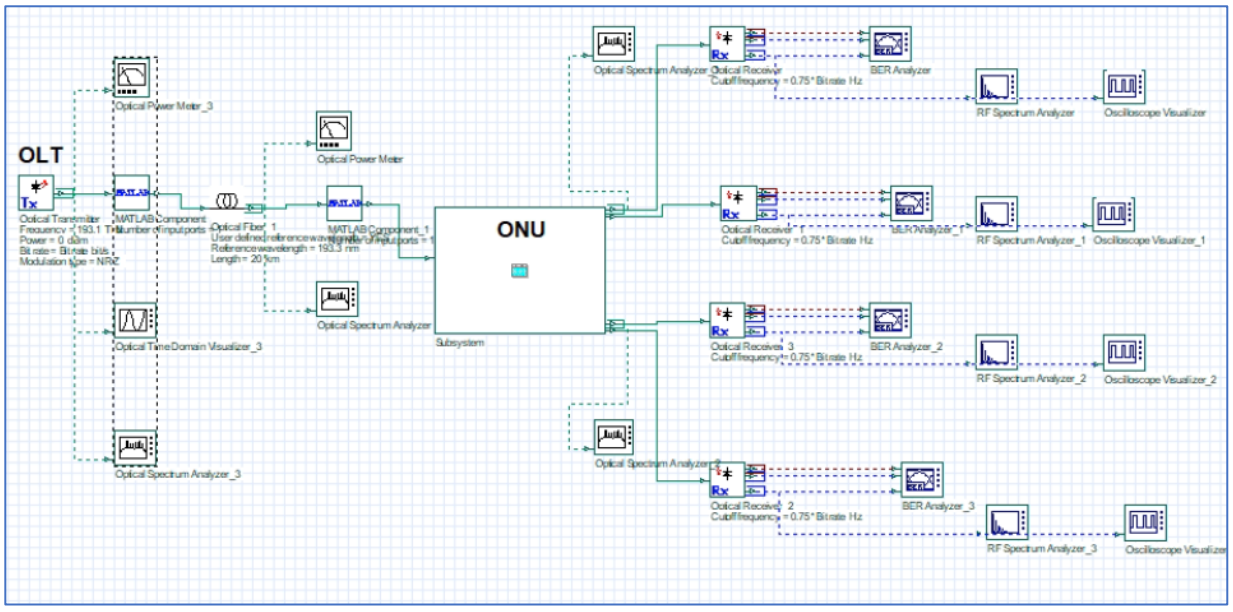


Figure 12. FTTH System Circuit Comprising a Single Input Laser Operating at an Input Power Level of 10 dBm, Transmitting over a 10 km Optical Fiber Link to four Receiver Output Channels.

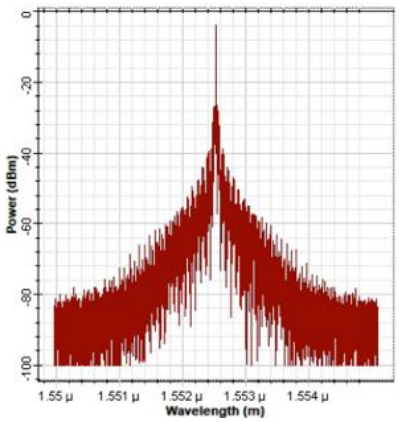


Figure 13. Optical Spectrum Analyzer 3 Output for the Encrypted Input Signal.

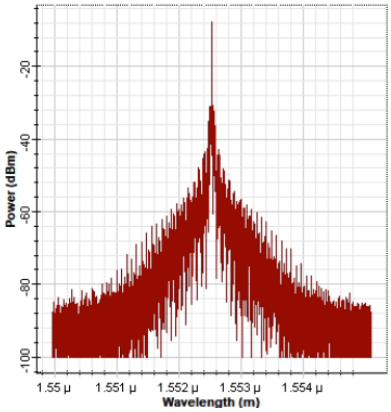


Figure 14. Optical Spectrum Analyzer Output for the Encrypted Output Signal.

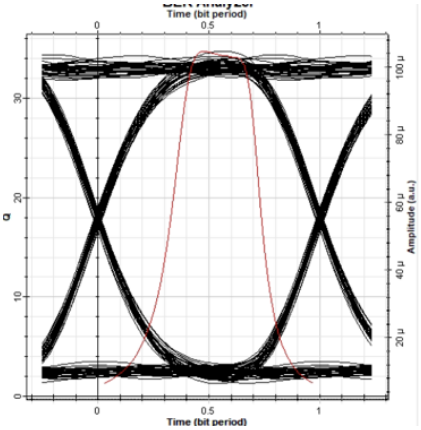


Figure 15. BER Analyzer Displaying the Eye Diagram for Output 1 with the Decrypted Signal.

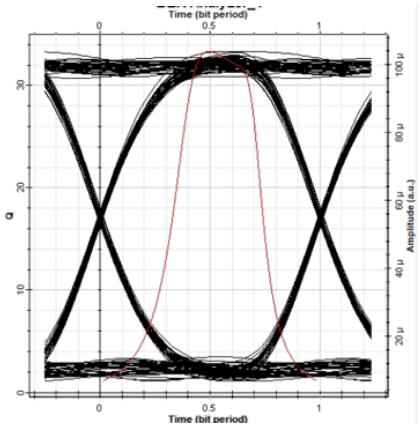


Figure 16. BER Analyzer 1 Displaying the Eye Diagram for Output 2 with the Decrypted Signal.

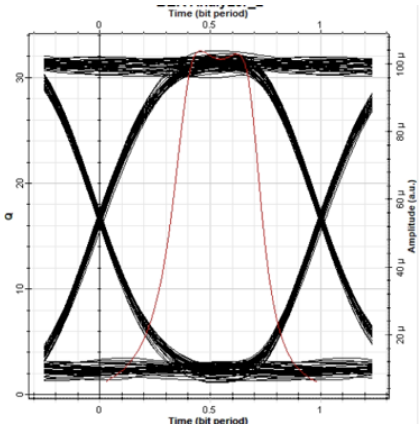


Figure 17. BER Analyzer 2 Displaying the Eye Diagram for Output 3 with the Decrypted Signal.

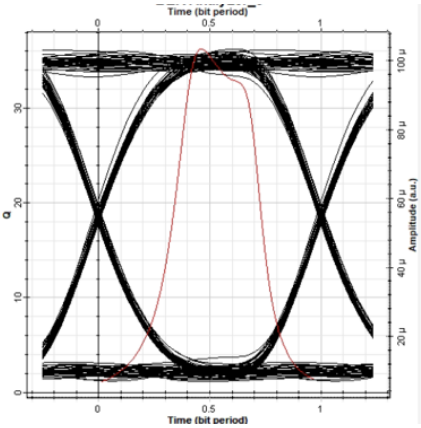


Figure 18. BER Analyzer 3 Displaying the Eye diagram for Output 4 with the Decrypted Signal.

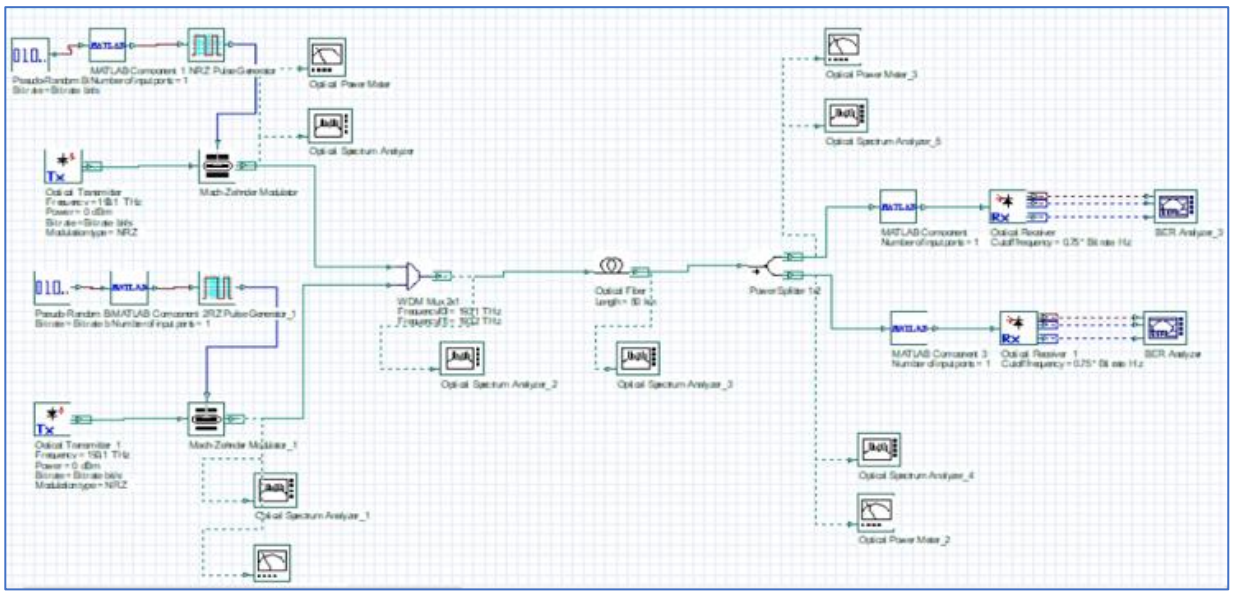


Figure 19. WDM System Circuit Comprising Two Input Channels Utilizing Mach-Zehnder Encryption. The Laser Operates at an Input Power Level of 10 dBm, Producing Two Receiver Signal Outputs.

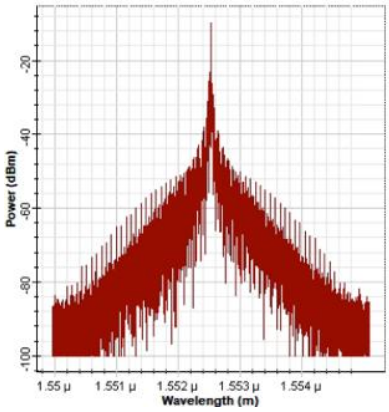


Figure 20. Optical Spectrum Analyzer Output for the Encrypted Input Signal.

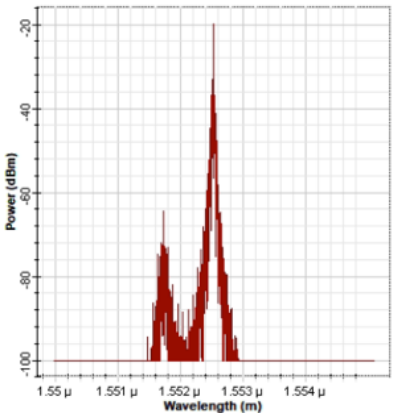


Figure 21. Optical Spectrum Analyzer 3 Output for the Encrypted Output Signal.

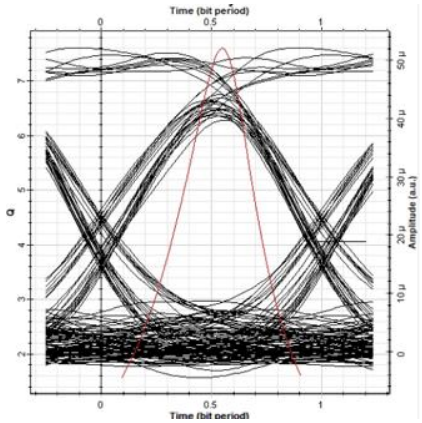


Figure 22. BER Analyzer Displaying the Eye Diagram for Output 1 with the Decrypted Signal.

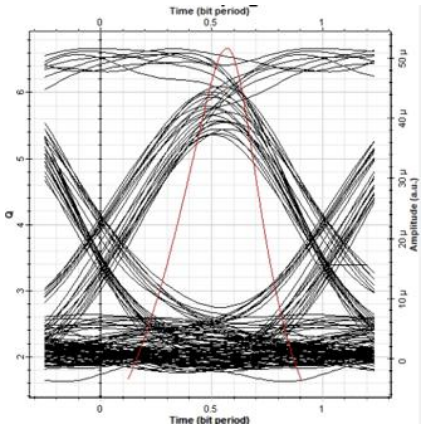


Figure 23. BER Analyzer 3 Displaying the Eye Diagram for Output 2 with the Decrypted Signal.

The experimental setup employed several key instruments, including an optical spectrum analyzer, BER analyzer, energy meter, and eye-chart analyzer, to evaluate the performance of the proposed encryption scheme. The test configuration involved hybrid WDM and FTTH systems, with encryption implemented via Mach–Zehnder modulators. Transmission was carried out using a continuous-wave (CW) laser at an input power level of 10 dBm over a 10 km optical fiber link. Performance was assessed through metrics such as bit error rate (BER), Q-factor, eye height, and spectral integrity. This comprehensive arrangement effectively demonstrates the viability and robustness of the encryption algorithm under practical optical communication conditions, highlighting its capability to preserve signal quality and mitigate errors across diverse system configurations and operating scenarios.

8. Encryption and Decryption of Color Images

This section presents a range of security analyses and statistical evaluations applicable to image-based encryption systems leveraging the properties of hyper-chaotic systems. Visual evaluation, a traditional and widely accepted method, serves as an initial and practical means to assess the quality of encryption results without requiring complex calculations or specialized equipment. By visually inspecting the images before and after encryption and decryption, one can readily identify any distortions or discrepancies that may arise during these processes. The encrypted images produced in this study appear as fully camouflaged abstract patterns, rendering the original content unrecognizable. Conversely, the decryption process successfully reconstructs the original images without any distortion or loss of quality.

Figure 24 illustrates this outcome using three images. The first image, with dimensions of 600 × 400 pixels, represents the original input prior to encryption. Upon processing, the encryption system transforms the original image into an abstract, color-rich pattern that conceals all identifiable features. After undergoing decryption, the recovered image matches the original exactly in both quality and structure. Similar results were consistently observed across all test images, as demonstrated in **Figures 24, 26, 28, and 30**. These findings confirm that the encryption mechanism effectively preserves data integrity and enables complete recovery of the original information.

The proposed encryption scheme thus establishes a secure communication channel by ensuring that confidential information remains protected during transmission and can only be accessed by authorized parties possessing the correct decryption key.

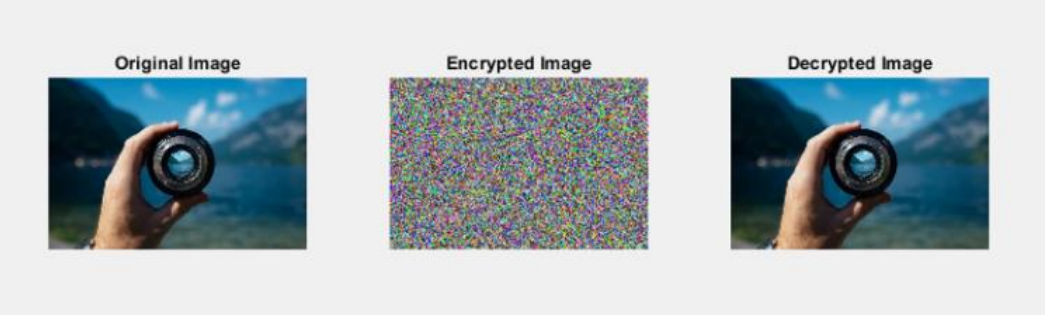


Figure 24. Test Image 1 with Dimensions of 600 × 400 Pixels.

9. Histogram Analysis

An image histogram is a graphical representation of the distribution of pixel intensities within an image. It serves as an important tool for evaluating image encryption techniques by assessing the uniformity of pixel value distributions in the encrypted images. Ideally, the histogram of an encrypted image should exhibit a uniform distribution to prevent leakage of information about the original image. **Figures 25, 27, 29, and 31** illustrate the histograms of both original and encrypted images, highlighting the distinctive characteristics inherent to each original image. Since each image has unique parameters, the histograms of original images differ accordingly. However, the histograms of encrypted images demonstrate a high degree of similarity and uniformity, reflecting the robustness of the encryption scheme and complicating any attempt by attackers to infer the original image content from the encrypted histograms.

Figure 25 shows the histogram for Test Image 1.

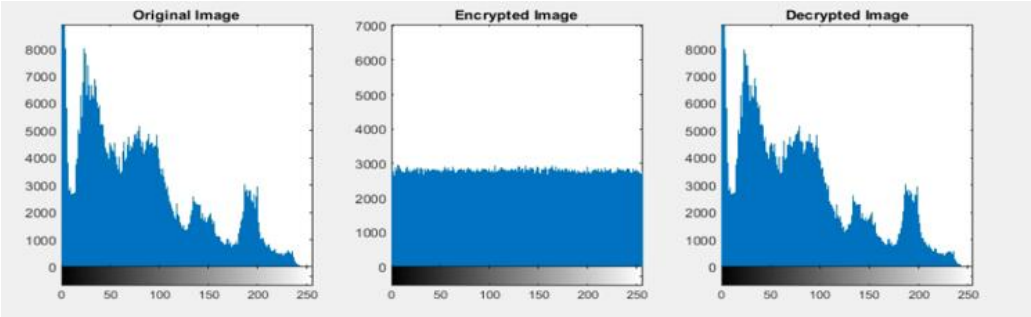


Figure 25. Histogram for Test Image 1.

To further evaluate the encryption performance across different image dimensions, **Figure 26** presents Test Image 2 with dimensions of 720 × 540 pixels.

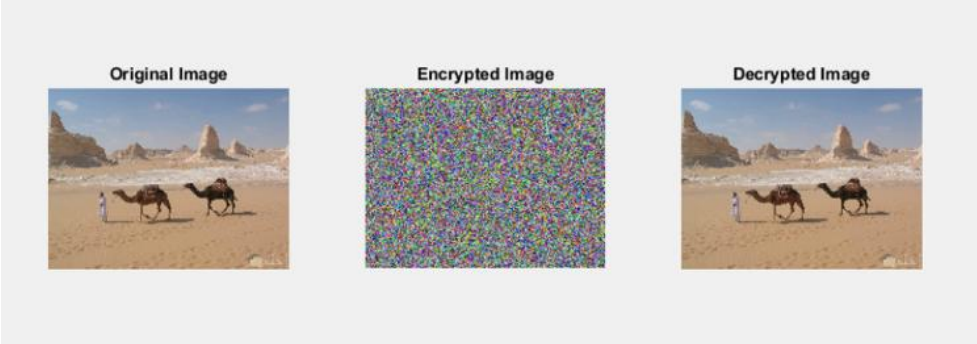


Figure 26. Test Image 2 with Dimensions 720 × 540 Pixels.

Figure 27 displays the corresponding histograms for this image, revealing variations in color values, pixel sizes, and image dimensions relative to the original. The encrypted image's histogram confirms the encryption system's ability to obscure the original image features effectively.

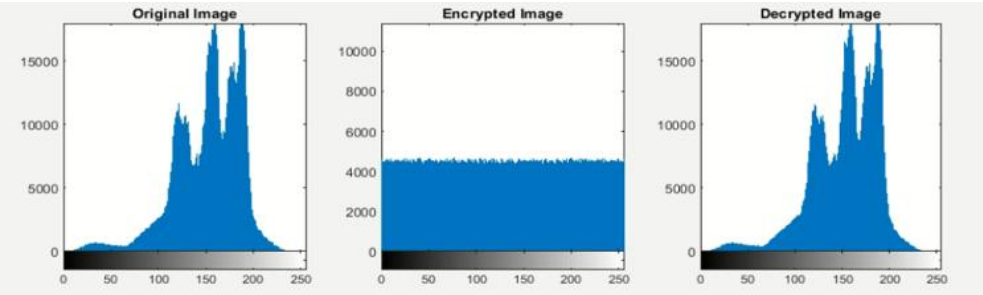


Figure 27. Histogram for Test Image 2.

Similarly, **Figure 28** presents Test Image 3, sized 1920 × 1200 pixels, with its histogram depicted in **Figure 29**.

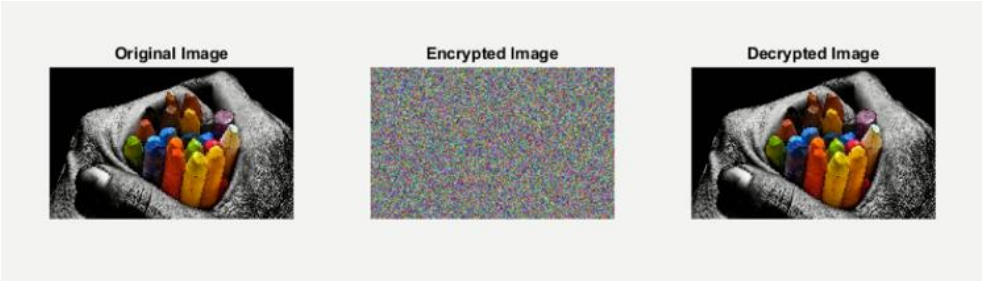


Figure 28. Test Image 3 with Dimensions 1920 × 1200 Pixels.

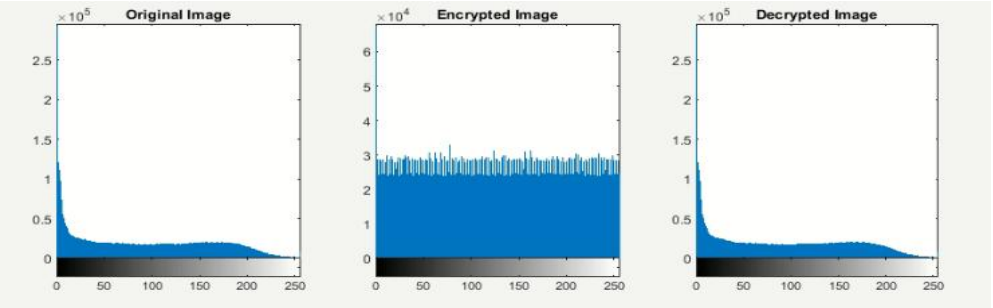


Figure 29. Histogram for Test Image 3.

Figure 30 and Figure 31 show Test Image 4 (1024 × 701 pixels) and its histogram, respectively.

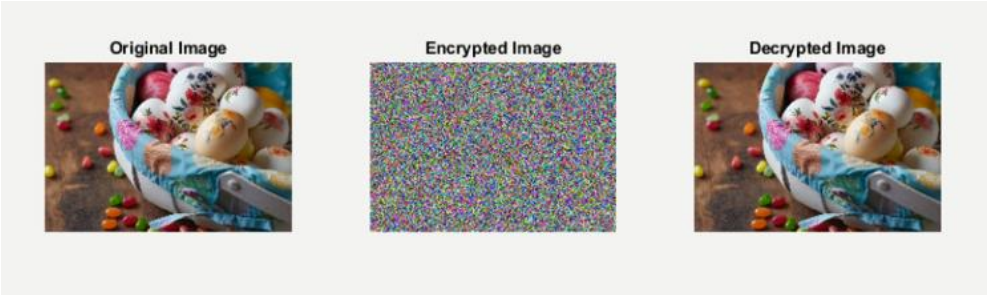


Figure 30. Test Image 4 with Dimensions 1024 × 701 Pixels.

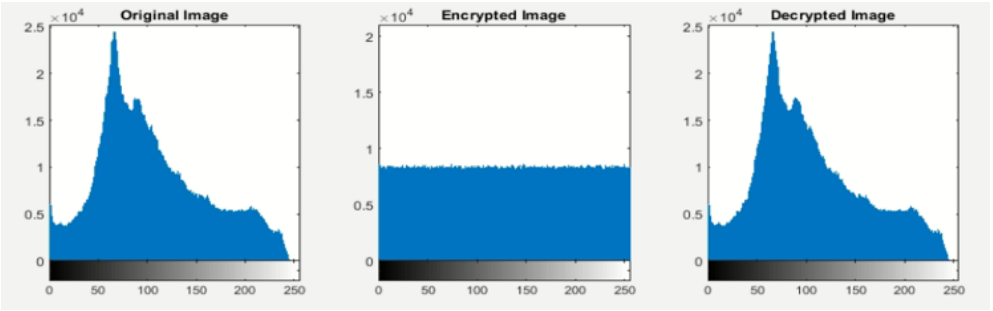


Figure 31. Histogram for Test Image 4.

Further analysis of the RGB histograms (**Figures 32–39**) evaluates the encryption strength in concealing the original image features by examining the pixel intensity distribution across the three-color channels: red, green, and blue. Each color channel is analyzed independently, with pixel intensity values ranging from 0 to 255, where 0 indicates no color intensity (black) and 255 represents full intensity. The original images exhibit non-uniform distributions of pixel intensities reflective of their color content and structure. In contrast, the encrypted images display nearly

uniform pixel intensity distributions across all channels, demonstrating the encryption algorithm's effectiveness in disrupting the original image statistics. This uniformity across the RGB channels in encrypted images indicates that the encryption process successfully obscures the original image's features, preventing the extraction of useful information. Consequently, the significant differences between the histograms of original and encrypted images confirm that the proposed encryption algorithm performs well in encoding and securely hiding image features.

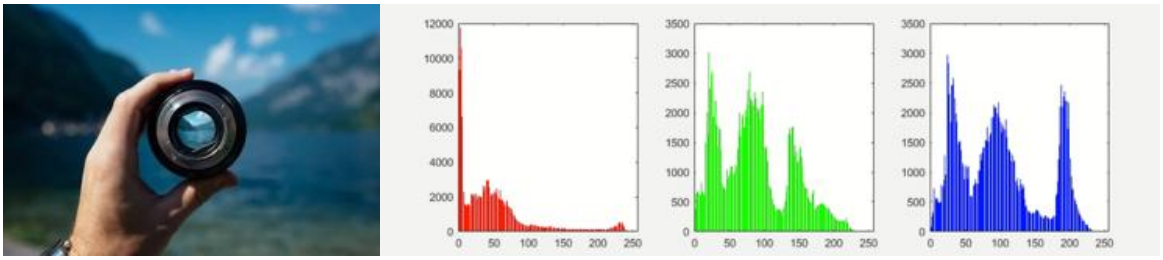


Figure 32. RGB Histogram for Test Image 1. The original image shows a non-uniform pixel intensity distribution reflective of its content.

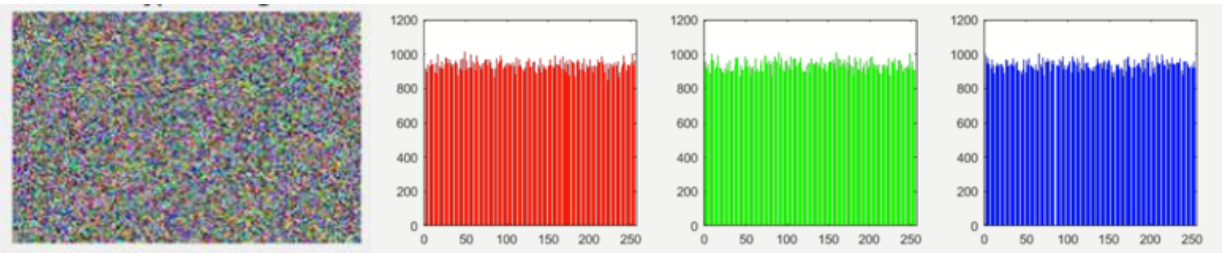


Figure 33. RGB Histogram for Encrypted Image 1. A nearly uniform distribution indicates strong encryption, concealing image features.

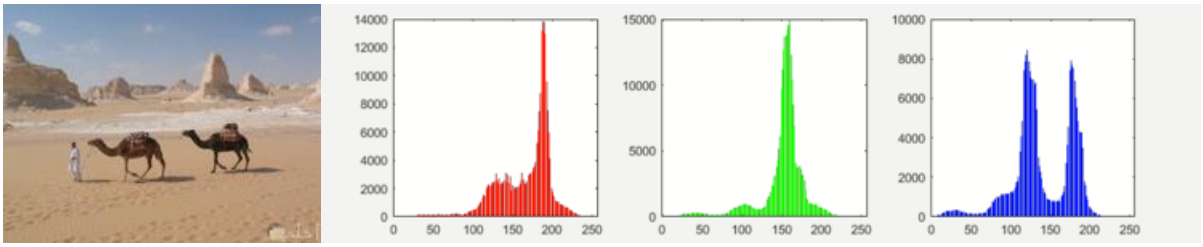


Figure 34. RGB Histogram for Test Image 2. Pixel intensity distribution reveals the image's structural and color characteristics.

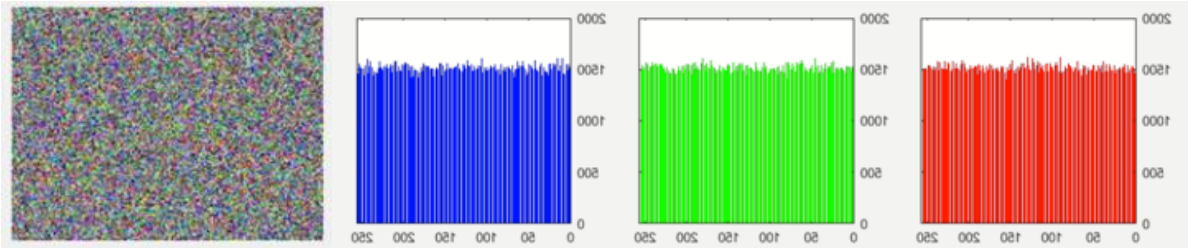


Figure 35. RGB Histogram for Encrypted Image 2. Uniform distribution confirms effective scrambling of original image data.

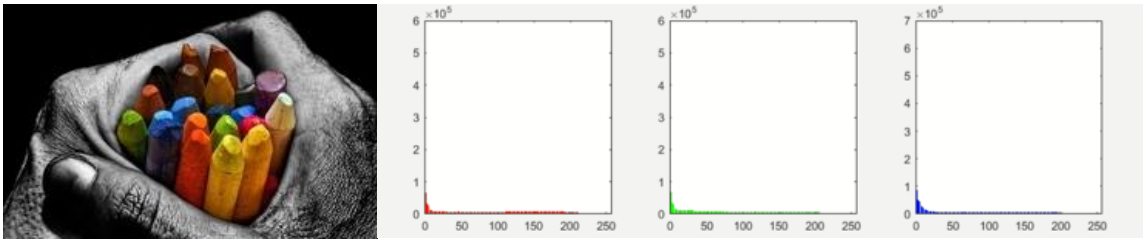


Figure 36. RGB Histogram for Test Image 3. Distinct intensity variations are visible across color channels.

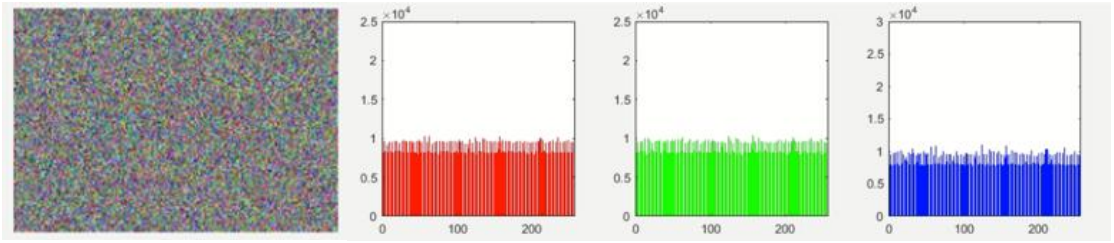


Figure 37. RGB Histogram for Encrypted Image 3. Randomized distribution across all channels obscures original details.

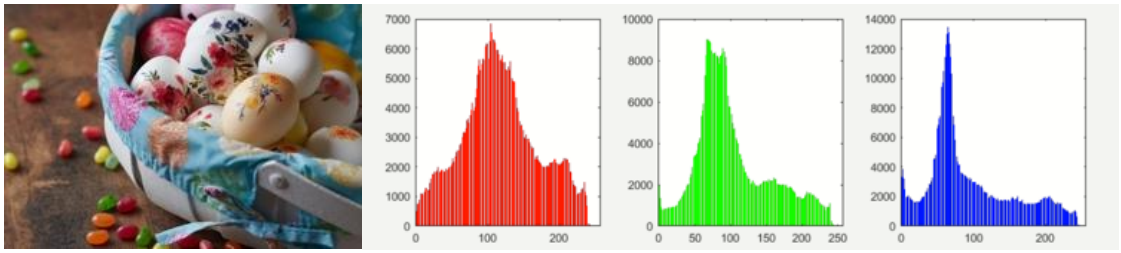


Figure 38. RGB Histogram for Test Image 4. Non-uniform pixel intensities reveal the original image structure.

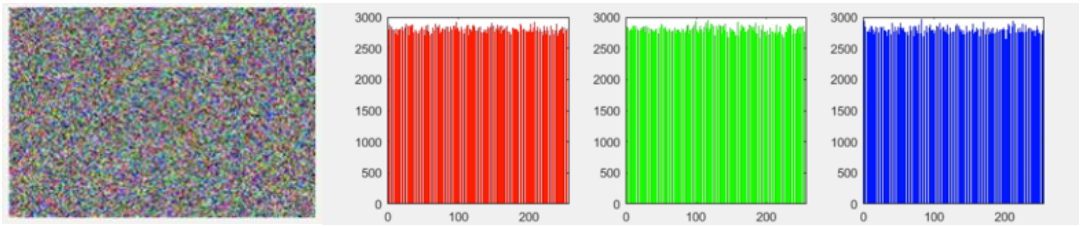


Figure 39. RGB Histogram for Encrypted Image 4. Uniform channel distribution affirms successful encryption.

10. Entropy Analysis

To evaluate the level of randomness and the effectiveness of the proposed encryption scheme, Shannon entropy analysis was conducted on all images used in the study. Entropy serves as a quantitative measure of uncertainty or unpredictability within a dataset, and it is widely applied in image and text encryption to assess the degree of chaos introduced by an encryption algorithm. In this context, higher entropy values indicate greater randomness, suggesting stronger encryption.

The analysis was applied to original images of varying resolutions—600 × 400, 720 × 540, 1920 × 1200, and 1024 × 701 pixels—as well as their corresponding encrypted and decrypted counterparts. The average entropy values and standard deviations were computed, and the results are summarized in **Table 2**. The findings demonstrate that the entropy values of the decrypted images are identical to those of the original images, confirming that the decryption process successfully restored the images without loss of quality or information. In contrast, the encrypted images consistently exhibit entropy values approaching the theoretical maximum of 8, indicating a high level of randomness and strong resistance to statistical attacks.

These results confirm that the proposed encryption algorithm performs effectively across various image sizes, ensuring high-quality image recovery and maintaining the original resolution and structure without distortion. The significant difference in entropy between the original/decrypted and encrypted images further validates the robustness and reliability of the encryption approach.

Table 2. Entropy Analysis Results for Original, Encrypted, and Decrypted Images.

Picture	Original Image	Encrypted Image	Decrypted Image
Test1	7.5641	7.9997	7.5641
Test2	6.9878	7.9998	6.9878
Test3	6.4453	7.9893	6.4453
Test4	7.6906	7.9999	7.6906

11. Conclusion

This study proposes a novel method for encrypting color images by integrating the Fibonacci Q-matrix with a six-dimensional (6D) hyper-chaotic system. The encryption process begins with the generation of random sequences using the six-dimensional (6D) hyper-chaotic system. Three of these sequences are then employed to alter the pixel positions within the image, introducing spatial confusion. Subsequently, the Fibonacci Q-matrix is applied to modify the pixel values, with a parameter n = 10. Further, each sub-block of the mixed image, sized 2x2, is processed using the Fibonacci Q-matrix to enhance diffusion and strengthen the encryption.

The proposed technique demonstrates significant improvements in security by increasing both confusion and diffusion. Experimental results confirm the method's sensitivity to minor variations in pixel distribution and secret keys, yielding distinctly different encrypted outputs for even slight modifications. This property renders the algorithm highly resistant to differential attacks. Additionally, the large key space ensures robustness against brute-force attacks.

The effectiveness of the proposed approach was thoroughly evaluated using multiple criteria, including histogram analysis, RGB histogram distribution, Shannon entropy, correlation coefficients, and resilience to noise and partial data attacks. Across all metrics, the method exhibited high encryption strength, reliable data protection, and accurate image recovery with no perceptible loss in quality. These findings validate the efficacy and robustness of the algorithm in securing image data against a wide range of cryptographic threats.

12. Future Work and Limitations

While the proposed encryption scheme demonstrates strong security performance and practical applicability in optical communication systems, several avenues remain for future exploration. One potential limitation lies in the computational complexity associated with real-time implementation in resource-constrained environments. Future research may focus on optimizing the algorithm for hardware acceleration or lightweight embedded systems. Additionally, expanding the framework to support dynamic key generation or integration with quantum key distribution could further enhance its security. Evaluating the algorithm's performance under various noise conditions and across different optical modulation schemes would also provide deeper insights into its robustness in diverse real-world scenarios.

References

Aldin, S. S., Aldin B., Aykaç, M., & Aldin, N. B. (2024). Quad-color image encryption based on Chaos and Fibonacci Q-matrix. *Multimedia Tools and Applications*, *83*(3), 7827–7846. https://doi.org/10.1007/s11042-023-15958-x

Allimuthu, U., Balasundaram, S., Mahalakshmi, K., & Ponsindhu, T. (2023). Wave-Based Signal Security and Privacy Studies Using Automatic High-Bit-Rate Optical Communications with Quantum Cryptographic. *Optica Open*.

Koman E., & Ünverdi N. Ö. (2019). Analysis and Applications of the Hybrid WDM/TDM Passive Optical Networks, *Sigma Journal of Engineering and Natural Sciences*, 37 (4), 1059-1073.

Fadil, E. A., Abass, A. K., & Tahhan, S. R. (2023). Design and simulation of optical chaotic-based secure hybrid optical communication system. *Journal of Optics (India)*, *52*(4), 1887–1896. https://doi.org/10.1007/s12596-023-01143-8

Futami, F., Tanizawa, K., & Kato, K. (2020). Y-00 Quantum-Noise Randomized Stream Cipher Using Intensity Modulation Signals for Physical Layer Security of Optical Communications. *Journal of Lightwave Technology*, *38*(10), 2773–2780. https://doi.org/10.1109/JLT.2020.2985709

Hosny, K. M., Kamal, S. T., & Darwish, M. M. (2022). Novel encryption for color images using fractional order hyperchaotic system. *Journal of Ambient Intelligence and Humanized Computing*, *13*(2), 973–988. https://doi.org/10.1007/s12652-021-03675-y

Hossam Eldein Mohamed, F. A., & El-Shafai, W. (2024). Cancelable biometric authentication system based on hyperchaotic technique and Fibonacci Q-Matrix. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-023-17855-9

Jiang, L., Pan, Y., Yi, A., Feng, J., Pan, W., Yi, L., Hu, W., Wang, A., Wang, Y., Qin, Y., & Yan, L. (2021). Trading off security and practicability to explore high-speed and long-haul chaotic optical communication. *Optics Express*, *29*(8), 12750. https://doi.org/10.1364/oe.423098

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

Mohamed, H. I., Alhammad, S. M., Khafaga, D. S., Komy, O. El, & Hosny, K. M. (2024). A New Image Encryption Scheme Based on the Hybridization of Lorenz Chaotic Map and Fibonacci Q-Matrix. *IEEE Access*, *12*, 14764–14775. https://doi.org/10.1109/ACCESS.2023.3341103

Moysis, L., Lawnik, M., Antoniades, I. P., Kafetzis, I., Baptista, M. S., & Volos, C. (2023). Chaotification of 1D Maps by Multiple Remainder Operator Additions—Application to B-Spline Curve Encryption. *Symmetry*, *15*(3). https://doi.org/10.3390/sym15030726

Murillo-Escobar, M. A., Meranza-Castillón, M. O., López-Gutiérrez, R. M., & Cruz-Hernández, C. (2019). Suggested integral analysis for chaos-based image cryptosystems. *Entropy*, *21*(8). https://doi.org/10.3390/E21080815

Panwar, A., Biban, G., Chugh, R., Tassaddiq, A., & Alharbi, R. (2024). An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images. *Heliyon*, e31618. https://doi.org/10.1016/j.heliyon.2024.e31618

Senior, J. M. (2009). Optical Fiber Communications: Principles and Practice, Third Edition. Prentice Hall. Gosport. www.pearson-books.com

Wang, X., Zhang, X., Gao, M., Tian, Y., Wang, C., & Iu, H. H. C. (2023). A Color Image Encryption Algorithm Based on Hash Table, Hilbert Curve and Hyper-Chaotic Synchronization. *Mathematics*, *11*(3). https://doi.org/10.3390/math11030567

Zhang, D., Chen, L., & Li, T. (2021). Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation. *Entropy*, *23*(3). https://doi.org/10.3390/e23030361