STATISTICS, OPTIMIZATION AND INFORMATION COMPUTING
Stat., Optim. Inf. Comput., Vol. **16**, December 2026, pp 5456–5483.
Published online in International Academic Press (www.IAPress.org)

Color image encryption strategy of Ro-FSO network systems based on CBC and Blowfish cipher

Hasanain M. Jasim[1], Ayoob A. Qasim[1], Ahmed Hussein Ali[2], Essam N. Abdulla[3,*]

[1] *Construction and Projects Department, University of Technology–Iraq, Baghdad, Iraq Baghdad 10021, Iraq*
[2] *Computer Techniques Engineering Department, Al Hikma University College, Baghdad, Iraq*
[3] *College of Laser and Optoelectronics Engineering, University of Technology-Iraq, Baghdad, Iraq*

Abstract The escalating demand for critical network functions has intensified the urgency of addressing security vulnerability in optical communication systems. This work builds a secure a 64-channel scheme to study the execution of a hybrid Radio over Free Space Optics (RoFSO) communication system under variable conditions of weathers using a Blowfish coding cipher. The system is designed to send data at 640 Gbps over an FSO communication link, the radio frequency (RF) signal parameters were set at 35 GHz (high band 5G) in optical form, with the receiver able to clearly receive data. Under the considered atmospheric conditions, the maximum transmission distance achieved with the optical pre-amplifier was approximately 1.9 km under dim (light) fog, 1.55 km under light rain, 0.9 km under moderate fog, 0.76 km under intense rain, and 0.75 km under haze. Accordingly, the maximum bit-rate–distance product was approximately 1216 Gb/s·km, calculated from the aggregate data rate of 640 Gb/s and the maximum transmission distance of 1.9 km under dim fog conditions. The degree of protection offered is demonstrated by its large key space, resistance to brute-force, differential, and anti-differential attacks, reducing correlation between neighbouring pixels, flattened histogram of the encoded original picture, and rising entropy for the scenarios examined. Based on the results, data security in FSO systems is preserved through the successful integration of cryptographic encryption and decryption techniques.

Keywords CBC, Pre-amplifier, RoFSO, RF, FSO, security, Blowfish, weather conditions.

DOI: 10.19139/soic-2310-5070-4335

1. Introduction

The rapid growth of high-capacity wireless applications has increased the demand for communication technologies capable of providing high data rates, low latency, and reliable transmission while maintaining data security. Radio-over-Free-Space-Optical (Ro-FSO) communication combines the advantages of radio-frequency (RF) communication and free-space optical (FSO) transmission, providing a promising approach for high-capacity wireless links. Additionally, by sending several wavelength streams at once, wavelength-division multiplexing (WDM) can be used to boost an optic link's bandwidth. Nevertheless, meteorological factors including fog, rain, and haze can impair FSO lines by introducing optic attenuation, which can lower the link quality and attainable distance of transmission [1, 2]. In addition to the performance at the physical layer, the security of transmitted data is a crucial factor for wireless optical communication systems. Encryption may be utilized on digital data prior to its entry into the communication channel, ensuring that the conveyed information is safeguarded while its transit across the communication infrastructure. In this study, color photographs serve as illustrative digital payloads to assess the security features of the proposed system. The picture data undergo encryption prior to transmission

*Correspondence to: Essam N. Abdulla (Email: Essam.N.Abdulla@uotechnology.edu.iq). Optoelectronics Engineering Department, Laser and Optoelectronics College, University of Technology–Iraq, Baghdad, Iraq.

ISSN 2310-5070 (online) ISSN 2311-004X (print)
Copyright © 2026 International Academic Press

and are then transformed into a binary sequence for integration into the WDM-Ro-FSO connection [3]. Digital data may be protected using a variety of symmetric-key encryption methods, including contemporary standards like the Advanced Encryption Standard (AES) and alternative lightweight or application-specific cryptographic systems. Because Blowfish is a well-known symmetric-key block cipher with a clear implementation and has been extensively studied in the context of digital data security, it was chosen as the encryption technique for this study. Instead of asserting that Blowfish is cryptography better than more recent algorithms, the choice is meant to offer a workable and repeatable cryptographic layer for integration with the suggested Ro-FSO system [3, 4]. In particular, the present work does not introduce a new Blowfish variant, chaotic mapping mechanism, or non-standard key-generation technique. The use of Blowfish in this work is therefore considered from a system-integration perspective. Prior to the physical-layer transfer, the encryption process is carried out, and the communication link is then assessed using standard physical-layer criteria. Since communication efficiency and cryptography performance reflect distinct facets of the suggested system, this division is crucial. The Ro-FSO communication link is characterized by quality factor (Q-factor), bit error rate (BER), and transmission distance, while the security characteristics of the encrypted picture are characterized by histogram, entropy, pixel correlation, key-space, and differential analyzes. With 64 WDM channels running at 10 Gb/s each, the suggested system has an overall transmission rate of 640 Gb/s. Under various air attenuation circumstances, the encrypted data are sent over the Ro-FSO connection. Additionally, the impact of an optical pre-amplifier on the maximum transmission distance is examined. Thus, the study investigates communication and security features within shared system architecture by combining high-capacity WDM-Ro-FSO transmission with a well-established symmetric encryption layer. This work's primary contribution is the system-level integration and assessment of Blowfish-Cipher Block Chaining (CBC) encryption using a 64-channel, 640-Gb/s WDM-Ro-FSO architecture. The study investigates the influence of atmospheric attenuation on Q-factor, BER, and transmission distance, while also analysing the statistical security properties of encrypted color-image payloads. The study does not claim uniqueness in the Blowfish method, WDM technologies, or Ro-FSO architecture separately; rather, it explores their integration and performance within the specified secure communication arrangement. It is also worth noting that the current work does not give a direct experimental comparison between Blowfish and contemporary encryption algorithms such as AES or lightweight authenticated encryption techniques. As a result, no promise is made that Blowfish is more secure, computationally efficient, or suitable than these alternatives. A comparative examination of encryption processing time, computational overhead, authentication capabilities, and influence on high-speed data transmission is an essential avenue for future investigation.

The suggested system uses the word "hybrid" to describe the merging of the RF and free-space optical (FSO) transmission domains in the identical communication architecture. It does not refer to a dynamic switching mechanism between RF and FSO links. Instead, the RF signal is used as the information-bearing electrical signal that drives the optical transmission stage, while the FSO channel provides the wireless optical propagation path. The encrypted digital data are first introduced into the RF transmission stage, where the information is modulated onto the RF carrier. The resulting RF signal is then used to drive the optical transmitter, where the electrical/RF information is converted into an optical signal suitable for free-space propagation. The optical signal is transmitted through the FSO channel and is affected by the corresponding atmospheric attenuation conditions. At the receiver, the received optical signal is detected by the photodetector and converted back into an electrical signal. The retrieved electrical signal is then filtered and processed to extract the sent data. As a result, the RF and optical domains are connected through the electro-optical conversion stages, rather of acting as two distinct communication lines.

The entire signal route can be described as:

Encrypted Digital Data $\rightarrow$ RF Modulation $\rightarrow$ Electrical/RF Signal $\rightarrow$ Electro-Optical Conversion $\rightarrow$ Optical Transmission through FSO Channel $\rightarrow$ Optical Detection $\rightarrow$ Electrical Signal Recovery $\rightarrow$ Filtering/Demodulation $\rightarrow$ Recovered Data.

In the proposed arrangement, the 64 channels are sent at 10 Gb/s each, for a total data rate of 640 Gb/s. The FSO channel is then analyzed under different atmospheric attenuation circumstances to determine its impact on the quality and dependability of the RF-over-FSO transmission.

The choice of Blowfish for the proposed secure Ro-FSO system is based on the simulation requirements and should not be understood as a declaration that Blowfish is cryptographically superior to contemporary standards such as AES. However, Blowfish was chosen because its execution features are suitable with the aims of the current proof-of-concept system and allow the cryptography stage to be included into the large-scale optical transmission architecture. Firstly, Blowfish is a symmetric block encryption with a variable-length key, allowing you to choose the key length based on the desired security level. This feature is appropriate for a simulation in which the cryptography module is assessed separately of the physical Ro-FSO channel. The current technology employs Blowfish in CBC mode before to transfer across the optical communication chain. Second, the selection is inspired by operational simplicity and the availability of existing Blowfish implementations. This is especially important since the proposed design utilizes encryption as a preprocessing layer prior to the 64-channel optical transmission system. The physical communication system delivers 64 channels at 10 Gb/s each, resulting in an aggregate nominal capacity of 640 Gb/s. Thus, the cryptographic process stage must be assessed using observable quantities such as encryption time, decryption time, memory/resource consumption, and encryption throughput rather than assuming that the nominal optical capacity is equivalent to cryptographic processing throughput. Third, Blowfish provides a relatively flexible key-length range and an established CBC implementation, making it convenient for investigating the relationship between encryption parameters and communication performance. In the proposed system, this permits the cryptographic analysis to include key-space, key sensitivity, ciphertext statistics, correlation, entropy, and processing time while maintaining the same underlying Ro-FSO transmission architecture. However, the selection of Blowfish also involves important limitations. Blowfish uses a 64-bit block size, whereas AES uses a 128-bit block size and standardized key lengths of 128, 192, and 256 bits. AES is also an established NIST standard. Consequently, Blowfish should not be presented as preferable to AES in terms of contemporary cryptographic standardization or as a universally better choice for high-speed optical communication.

2. Related work

Consequently, integrating RoF with FSO combines their complementary advantages to achieve enhanced reliability, extended coverage, and improved overall system performance [5]. These systems provide last-mile communication, maintaining data transmission over as long a distance as possible. In RoF technology, transmitting data with high bandwidth is efficient; however, the cost of installing fiber cables and the impracticality of using fiber in certain regions are major challenges. Thus, implementing Ro-FSO systems is one of the achievable solutions [6, 7, 8]. FSO systems are also included in 5G and 6G next-generation wireless systems that provide cost-effective, accessible technologies. Furthermore, various applications require avoidance of RF interference, such as in hospitals [7, 8]. Several healthcare techniques utilize RF for specific medical purposes, such as radiofrequency identification (RFID) and 5G smart hospitals [9, 10]. In addition, since FSO systems may be exposed to line-of-sight (LOS) loss due to obstacles such as flying birds, airplanes, or other objects, implementing a hybrid Ro-FSO system maintains LOS connectivity [11]. Previous machine learning methods have shown promising results in QoT prediction and network optimization; nevertheless, a number of these methods rely on short datasets or single-model structures, which may hinder accuracy in generalization across a range of system settings [12], protect communication that is optical employing the Hill method cipher[13, 14], secure division multiplexing of time and wavelength -passive optical network (TWDM-PON) leveraging the Hill algorithm [15, 16, 17] and a security strategy that incorporates the Blowfish and Hill ciphers [18]. These developments achieve extremely challenging for communications designers as the demand for greater internet broadband increases rapidly [19].

2.1. Our contribution

The contributions of this paper can be summarized as follows:

(1) A secure, high-capacity hybrid Radio over Free-Space Optics (Ro-FSO) communication system incorporating the established Blowfish symmetric encryption algorithm in CBC mode is investigated. The

proposed architecture consists of 64 channels, each operating at 10 Gb/s, providing an aggregate transmission capacity of 640 Gb/s.

(2) The proposed secure Ro-FSO system is evaluated under different atmospheric conditions, including light fog, light rain, moderate fog, intense rain, and haze. The communication performance is investigated in terms of Q-factor, BER, and achievable transmission distance, with and without the use of an optical pre-amplifier.

(3) The effect of optical amplification on the transmission performance of the proposed Ro-FSO architecture is investigated. The obtained results demonstrate the improvement in achievable transmission distance under different atmospheric attenuation conditions when the optical amplifier is employed.

(4) The security performance of the encrypted image data is evaluated using established cryptographic analysis metrics, including key-space analysis, histogram analysis, entropy, and correlation coefficients. These analyses are used to assess the statistical characteristics of the encrypted data within the proposed Ro-FSO transmission system.

(5) The proposed system is compared with previously reported Ro-FSO and FSO-based communication systems in terms of transmission capacity, achievable link distance, and bit-rate–length performance. The results demonstrate the feasibility of integrating an established encryption algorithm with a high-capacity Ro-FSO architecture while maintaining reliable communication performance under different atmospheric conditions. The document is organized as follows: Section 1 provides an introduction; Section 2 describes the simulation model; Section 3 displays the findings and discussion for the communication and security technique; and Section 4 summarizes the conclusion.

2.2. Integration of Image Encryption with the Ro-FSO Transmission Link

The color photographs employed in this study are not treated as distinct post-processing analyzes from the communication system. Rather, they serve as representational digital payloads for the security layer of the proposed Ro-FSO communication architecture. The input picture is initially processed and encrypted with the Blowfish method in CBC mode. The generated ciphertext is then transformed into a binary data sequence and delivered to the communication model as the sent information. The encrypted data is then transferred using the proposed 64-channel WDM Ro-FSO architecture. Each channel operates at 10 Gb/s, resulting in an aggregate system data rate of 640 Gb/s. Therefore, the encryption stage represents the data-security layer preceding the physical-layer transmission rather than an independent image-processing experiment. The communication and security evaluations are performed at two complementary levels. The physical-layer performance of the encrypted data transmission is evaluated using Q-factor, BER, and achievable transmission distance under different atmospheric attenuation conditions. In parallel, the encrypted image payload is used to evaluate cryptographic characteristics through histogram, entropy, correlation, and key-space analyses. Accordingly, the use of color images in the title and security analysis represents the selected test payload for validating the encryption layer, whereas the underlying communication architecture is a high-capacity 64-channel Ro-FSO system. The study therefore investigates the integration of data encryption with high-capacity Ro-FSO transmission rather than proposing a standalone image-encryption algorithm.Secure 64-Channel Ro-FSO Communication System Based on Blowfish-CBC Encryption: Performance and Security AnalysisSecure Color-Image Transmission over a 64-Channel Ro-FSO System Using Blowfish-CBC EncryptionWe appreciate this observation. We agree that the original title could give the impression that the main contribution is a standalone color-image encryption algorithm, whereas the manuscript primarily investigates a high-capacity 64-channel Ro-FSO communication architecture.

3. Simulation model

Figure 1 clarifies the secure Ro-FSO system, which includes three subsystems: the transmitter, the free-space transmission, and the receiver. These are three crucial elements of the suggested scheme.

1. An illustration of the transmitter subsystem in Figure 2 comprises 64 channels. Each single channel forms an input message utilizing a pulse non-return-to-zero (NRZ) generator and a pseudo generator of bit random sequence operating at 10 Gbps. An electrical multiplier integrates this message with a radio wave signal at

a frequency of 35 GHz. Then, a mach- modulator zehnder ratio of extinction with a 30 dB applies this radio signal modulator to a continuous wave laser (CW) laser with a frequency ranging between 192 and 195.15 THz and 0.05 THz channel spacing.

2. Free-space channel: As the setting values of the operating system (summarized in Table 1) were employed, the RF message was sent via the transmitter to the free space. Because the air attenuation that results in a decreased received power is nearly unanticipated, the FSO direction is regarded as the main constraint in FSO networks. With attenuation losses listed in Table 2, this study examined the FSO's performance in variable weather conditions (rain, fog, and haze).
3. For the purpose of regaining the input pulse message, a Re-amplification, Re-shaping, and Re-timing (3R-regenerator) was inserted into the receiver subsystem. Furthermore, a low-pass filter was used, as well as a Positive-Intrinsic-Negative photodiode (PIN) photodiode, which had a function of transforming the signal from optical to electrical and eventually subsequently into an RF signal.
4. Blowfish Algorithm Implementation: Blowfish offers many benefits and is faster and more efficient than other symmetric encryption techniques. Compared to algorithms like AES and Data Encryption Standard (DES), it is faster. Blowfish provides strong security with customizable key sizes ranging from 32 to 448 bits, making it resistant to brute-force attacks because no effective cryptanalysis has been able to break it thus far. Because Blowfish is free and open-source, there are no license concerns when utilizing it for both non-commercial and commercial applications. Additionally, it works well with small information blocks and can be utilized in a number of encryption techniques, including electronic codebook (ECB) and CBC [17, 18, 19]. Numerous strategies have been employed to ensure safe data transfer.

Bruce Schneier created Blowfish, an established symmetric-key block encryption, in 1993. This work uses Blowfish as a known encryption technique rather than a freshly designed cryptographic algorithm. The goal of its implementation is to offer secrecy for the sent data prior to transmission over the proposed high-capacity Ro-FSO communication system. The Blowfish cipher employs a 64-bit block size and supports variable key lengths ranging from 32 to 448 bits. In the proposed system, Blowfish is operated in CBC mode, in which each plaintext block is combined with the preceding ciphertext block before encryption. An initialization vector (IV) is used for the first block. The resulting ciphertext is then incorporated into the proposed communication chain and transmitted through the Ro-FSO link. The encryption process is integrated with the 64-channel communication architecture, where each channel operates at 10 Gb/s, resulting in an aggregate data rate of 640 Gb/s. At the receiver, the encrypted data are recovered and decrypted using the corresponding secret key. The 2 main elements of the procedure are key creation and data security. A key a maximum of 448 bits can be expanded into several sub- arrays key up to 4168 bytes. Cryptography data uses a 16- Feistel round system. Blowfish utilizes 4 boxes substitution (S-Boxes), each with 4*256 entries, and eighteen iteration arrays (P-Boxes), each 32 bits long and designated as p1; p2; :: :; p18. Blowfish encoding uses a 64- block bit, which is composed of two 32-bit halves. The F-function, which transforms one 32-bit block into another, is used to run the result after XORing the left half with the original array p1. The two halves are then switched for the next round after this modified block is XORed with the right half. Fig. 4(a) provides a graphical representation of the blowfish method. The structure of this method, known as a Feistel network, is illustrated graphically by the function F in Fig. 4(b). There is no need to recalculate the S and P arrays because the key stays fixed and secure. Before being encrypted, each plaintext block is XORed with the previous ciphertext block using the blowfish algorithm in CBC mode. Steps outlining how CBC mode operates: 1. Fill a matrix with image data. 2. Select a secret key that is between 32 and 448 bits long (a minimum of 128 bits is advised to achieve security). 3. Create an IV at random that is the same size as my data block (8 bytes for blowfish). The blowfish algorithm's CBC mode phases are displayed in Figure 5. The sequence in which P1, P2, and P18 are applied is the only the distinction between decoding and encoding. The blowfish algorithm is made simpler by the following stages:

1. First split: divide the 64-bit data into 2 identical blocks, R and L, each of which is 32 bits long.
2. To begin a 16- encryption cycle procedure, XOR the left half L with the first element P1 from the P-array for each cycle.Next, XOR the right half R with the outcome of the F function applied to L, where the F function makes use of the four-sectioned S-box. Lastly, switch L and R before moving on to the following cycle.
3. End loop: switch L and R once more after the 16 cycles are finished.

4. Final XOR: To include the final 2 additional P-box elements, P17 and P18, XORR with P17 and P18 with L.
5. Retrieve ciphertext: To create the final ciphertext, combine L and R.

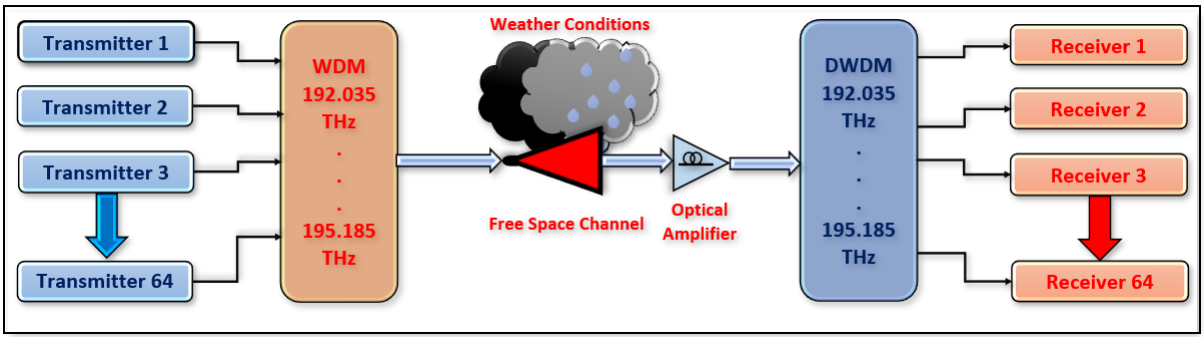


Figure 1. Ro-FSO system schematic diagram.

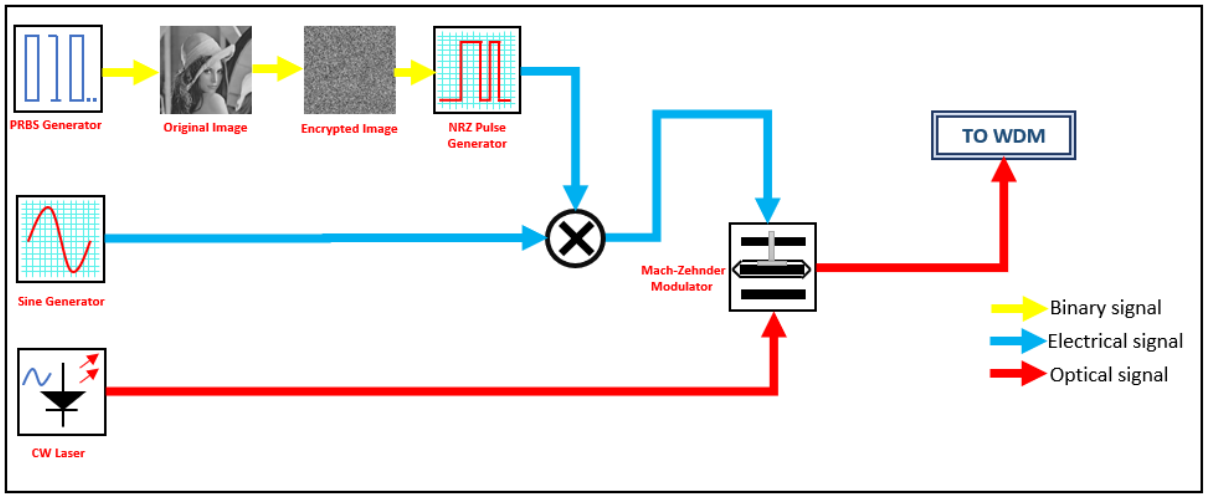


Figure 2. The components of the transmitter subsystem.

Table 1. The FSO implementation and arrangement of parameters.

Parameters	Value
Range	0.1-2Km
Diameter Aperture of Transmitter	15Cm
Diameter Aperture of Receiver	20Cm
Divergence Beam	1mrad
CW power Laser	5 dBm
CW frequency Laser	192 - 195.15 THz
Amplifier gain	20dB

3.1. Integration of Blowfish Encryption with the OptiSystem Model

The Blowfish encryption algorithm was implemented in MATLAB and integrated with the OptiSystem simulation through the digital data-processing stage. MATLAB was used to perform the encryption of the input color image

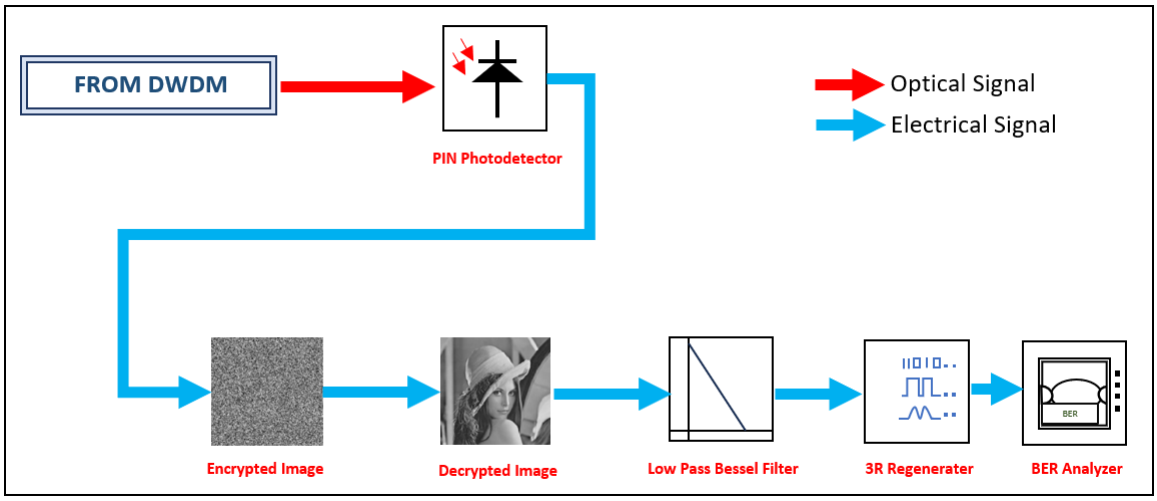


Figure 3. The components of the subsystem of the receiver.

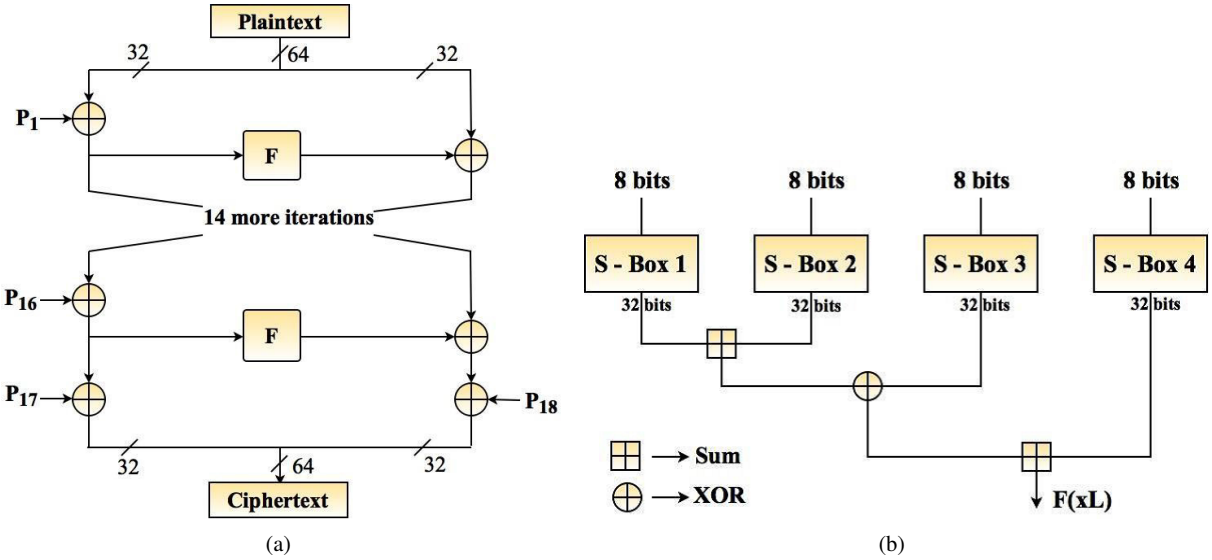


Figure 4. Graphical representation of (a) Blowfish algorithm (b) Function module (F) [18, 19].

Table 2. losses of the atmospheric circumstances [20]

The state of the weather	Attenuation dB/km
Dim Fog	4.285
Little rainfall	6.2702
Moderate Fog	15.555
Intense Rain	19.795
Haze	20.68553

before the encrypted data were introduced into the optical communication system. The input image was first converted into a digital data sequence, which was then processed using the Blowfish algorithm in CBC mode with a predefined secret key. The resulting encrypted data sequence was subsequently formatted as a binary stream

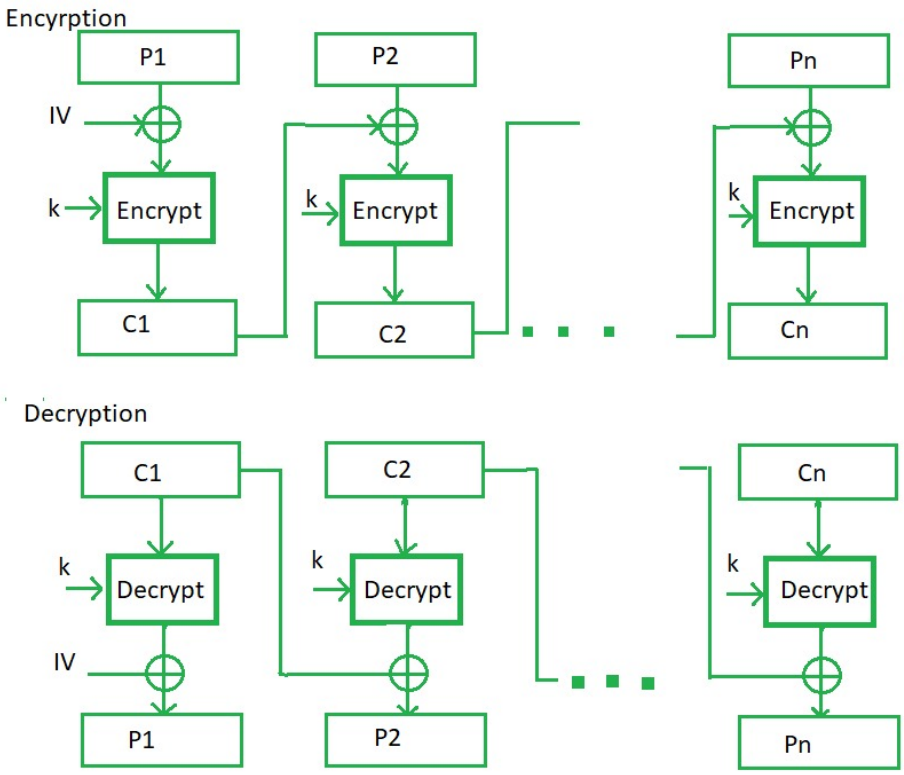


Figure 5. shows the steps of CBC mode for blowfish algorithm.

and supplied to the OptiSystem model as the information signal. Within OptiSystem, the encrypted binary sequence was used as the input data for the 64-channel Ro-FSO communication architecture. Each channel was operated at 10 Gb/s, resulting in an aggregate transmission capacity of 640 Gb/s. The encrypted data were modulated onto the optical carriers and transmitted through the modeled radio-over-free-space-optical (Ro-FSO) link under the considered atmospheric attenuation conditions. The encryption process was therefore performed before optical transmission, while OptiSystem was used to model the physical transmission of the encrypted data through the RF/FSO communication link. At the receiver side, the received signal was analyzed in terms of communication performance, including Q-factor and BER. The encrypted image data were also used for the subsequent security analysis, including histogram, entropy, key-space, and correlation analyses. This implementation allows the security layer provided by Blowfish-CBC to be evaluated together with the transmission performance of the high-capacity Ro-FSO system. The integration can consequently be summarized as follows: MATLAB performs image preprocessing and Blowfish-CBC encryption $\rightarrow$ the encrypted binary sequence is transferred to OptiSystem $\rightarrow$ OptiSystem performs the 64-channel Ro-FSO transmission and receiver processing $\rightarrow$ the received encrypted data are analyzed to evaluate both communication performance and security characteristics. This interface separates the cryptographic processing from the physical-layer communication simulation while allowing the encrypted data generated by MATLAB to be evaluated over the proposed high-capacity Ro-FSO communication architecture as shown in Fig.6.

The simulation is based on the following assumptions:

1. The 64 WDM channels operate at 10 Gb/s per channel, giving an aggregate nominal data rate of 640 Gb/s.
2. The encrypted payload is treated as the digital information transmitted through the physical communication system.
3. The RF carrier frequency is fixed at 35 GHz for the simulated channels.

4. The optical carriers are separated according to the specified 0.05-THz channel spacing.
5. Atmospheric effects are represented through the specified attenuation conditions used in the FSO channel.
6. The transmitter and receiver configurations remain unchanged when different atmospheric conditions are compared unless the experiment explicitly states otherwise.
7. The 3R regenerator is used for physical signal recovery and does not provide cryptographic protection.
8. The cryptographic key is assumed to be available to the transmitter and intended receiver; a complete key-establishment protocol is not modeled in the current simulation.
9. Color images are representative test payloads and are not intended to imply that the proposed communication architecture is limited to image transmission.
10. Security metrics and communication metrics are evaluated independently to distinguish cryptographic characteristics from physical-channel degradation.
11. Parameters that are not explicitly specified in the simulation configuration, such as receiver sensitivity, exact amplifier gain, amplifier noise figure, transmitter optical power, and detailed framing parameters, should not be inferred from the reported results and must be obtained directly from the corresponding OptiSystem model.

This complete description defines the simulation environment at the level supported by the implemented model while explicitly identifying parameters that require direct reporting from the simulation file for full reproducibility.

3.2. Security Scope and Data Transmission

The proposed 64-channel Ro-FSO system is intended to provide secure transmission of digital data rather than being restricted to static image transmission. In this study, color images such as Lena, Peppers, and other test images are used as representative digital payloads for evaluating the encryption and security characteristics of the proposed architecture. The images provide a reproducible data source that allows the effectiveness of the Blowfish-CBC encryption scheme to be investigated using histogram, entropy, correlation, key-space, and related security analyses. After encryption, the image data are converted into a binary data sequence and introduced into the communication system. The resulting bit sequence represents the digital information carried by the Ro-FSO link. Therefore, the use of images in the security analysis does not imply that the proposed communication system is limited to static image transmission. The 64-channel architecture is designed and evaluated in terms of its aggregate data-transmission capability, with 10 Gb/s per channel and a total data rate of 640 Gb/s. In this work, the image data serve primarily as a test payload for validating the security layer, whereas the Ro-FSO model represents the underlying high-capacity digital communication link. Accordingly, the results concerning Q-factor, BER, transmission distance, and atmospheric attenuation characterize the communication link, while the image-based analyses characterize the security performance of the Blowfish-CBC.

3.3. Simulation Workflow and Channel Generation

The simulation process is divided into steps that process data and transmit it sequentially. First, the input color picture data is encrypted using the Blowfish method in CBC mode. The encrypted data is subsequently represented as a binary data sequence and transmitted across the communication system. This encryption level occurs before the physical-layer Ro-FSO transmission. The transmitting architecture is composed of 64 WDM channels, each running at a data rate of 10 Gb/s, for an aggregate data rate of 640 Gb/s. The data sequence for every channel is created utilizing a pulse NRZ generator and a 10 Gb/s pseudo-random bit sequence generator. The electrical information signal is coupled with a 35-GHz RF carrier using an electrical multiplier. The resultant RF signal is then sent into a Mach-Zehnder modulator, which modulates a CW optical carrier. The optical carriers occupy the wavelength range of roughly 192 to 195.15 THz and have a channel spacing of 0.05 THz. The 64 optic streams are then merged using the WDM transmission system and launched into the FSO connection. The FSO route includes the atmospheric attenuation circumstances studied in this work, such as fog, rain, and haze. The sent signal thus comprises the encrypted information while being subject to the same physical propagation restrictions as any other digital data delivered via the Ro-FSO link. At the receiver, the multiplexed optical signal is received and transformed from the optical domain to the electrical domain using a PIN photodiode. A low-pass filter is

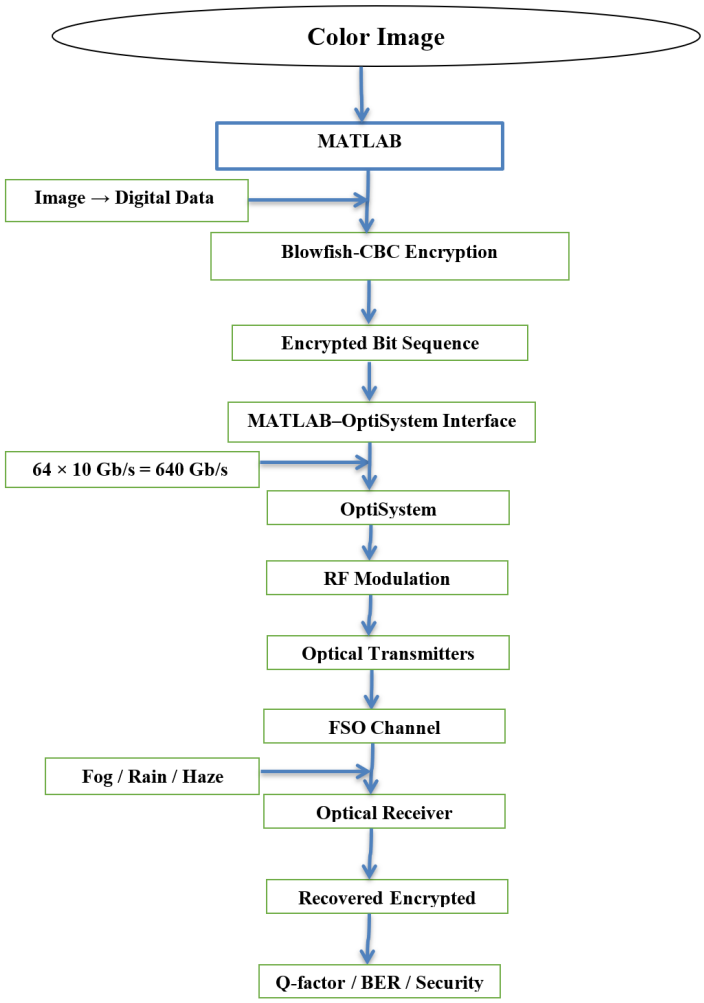


Figure 6. Block Diagram of the integration process OptiSystem with Matlab.

subsequently applied to retrieve the appropriate electrical/RF signal components. The receiver subsystem includes a 3R regenerator, which restores the received digital signal before data recovery and performance evaluation. The 3R regeneration function encompasses signal re-amplification, re-shaping, and re-timing. Its aim in this system is to compensate for signal deterioration that accumulates during transmission and to regenerate a cleaner digital representation of the received information. Moreover, the 3R regenerator does not execute decryption or encryption, nor does it change the crypto process. The sent data remains encrypted as it passes through the physical transmission and regeneration steps. As a result, the 3R regenerator is regarded as a physical-layer signal-recovery component, not a security component.

The entire simulation flow may thus be stated as follows:

Color Image → Blowfish-CBC Encryption → Encrypted Binary Data → 64 × 10-Gb/s Data Channels → RF Modulation at 35 GHz → Mach–Zehnder Electro-Optical Modulation → WDM Multiplexing → FSO Atmospheric Channel → Optical Reception → PIN Photodetection → Low-Pass Filtering → 3R Regeneration → Recovered Digital Signal → BER and Q-Factor Evaluation.

This workflow explains that encryption occurs before transmission, whereas WDM multiplexing, atmospheric propagation, optical detection, filtering, and 3R regeneration are part of the physical communication layer. As

a result, the security features of the encrypted data and the communication performance of the Ro-FSO link may be assessed as distinct but interrelated elements of the proposed system.

4. Results and Discussion

The effectiveness of the suggested secured Ro-FSO communication architecture is assessed via numerical simulation using the system configuration provided in Section 3. The analysis focuses on two complementary aspects: communication performance and data-security characteristics. For the communication link, Q-factor, BER, and achievable transmission distance are investigated for the 64-channel, 640 Gb/s configuration under different atmospheric attenuation conditions. The atmospheric scenarios are considered as a practical performance evaluation rather than as a theoretical contribution, with the objective of determining the operating limits of the proposed architecture. The influence of an optical pre-amplifier on the achievable transmission distance is also investigated. The results obtained with and without amplification are compared for the considered weather conditions to quantify the improvement in link performance. In parallel, the security characteristics of the encrypted data are evaluated using key-space, histogram, entropy, and correlation analyses. The combined results are subsequently compared with previously reported systems to establish the performance characteristics of the proposed secure Ro-FSO architecture. Additionally, the impact of attenuation FSO was examined under several of meteorological circumstances. In Figure 7 (a) shows the input signal. The electrical data transmission needs to be sent over the free space. Figure 7 (b) illustrates the radio wave spectrum that was successfully produced using a sine wave, and Figure 7 (c) shows the optical delivered signal following the combination of the RF signal and electrical data message. A 3R regenerator and a low-pass filter are used to carry out the recovery procedure, as seen in Figure 7 (d).

4.1. Enhanced Security Analysis

The security analysis in this study focuses primarily on the protection of color-image data using the Blowfish algorithm in CBC mode before transmission through the Ro-FSO link. Therefore, the cryptographic security of the encrypted image is evaluated separately from the physical-layer communication performance. The latter is characterized using Q-factor, BER, and achievable transmission distance under different atmospheric conditions. In addition to histogram, information entropy, pixel-correlation, key-space, and differential analyses, key-sensitivity and occlusion analyses are considered to provide a more comprehensive evaluation of the image-encryption performance.

4.1.1. Key-Sensitivity Analysis Key sensitivity evaluates the effect of a small change in the secret key on the encryption and decryption processes. In this analysis, two keys that differ by a small change are considered. The same plaintext image is encrypted using the two closely related keys, and the resulting ciphertext images are compared. A secure encryption scheme should exhibit high sensitivity to the secret key, such that a small modification of the key produces a substantially different ciphertext. Similarly, during decryption, using an incorrect key that differs slightly from the correct key should not recover the original image. The resulting ciphertext images and their statistical characteristics can therefore be compared to demonstrate the avalanche behavior of the encryption process. This analysis complements the key-space evaluation. While key-space analysis considers the number of possible secret keys and the corresponding brute-force search space, key-sensitivity analysis examines how strongly the encryption output depends on the exact secret key used.

4.1.2. Occlusion and Partial Data-Loss Analysis An occlusion/partial data-loss test is used to evaluate the behavior of the encrypted image when a portion of the ciphertext is missing, corrupted, or unavailable. In this analysis, a selected portion of the encrypted image/data is intentionally removed or replaced before the decryption process. The objective is not to demonstrate physical-layer protection against an attacker but to investigate the effect of partial encrypted-data loss on the recovered image. The resulting decrypted image is compared with the original image using appropriate image-quality and statistical measures. Because Blowfish-CBC encrypts data in

chained blocks, corruption or loss of ciphertext blocks can affect the corresponding decrypted data and subsequent blocks according to the CBC structure. This test therefore provides additional information about the behavior of the encryption scheme under partial data corruption.

4.1.3. Separation of Cryptographic and Communication Security The security evaluation is divided into two complementary categories. Cryptographic security is investigated through histogram, entropy, pixel correlation, key-space, differential, key-sensitivity, and occlusion analyses. In contrast, the robustness of the Ro-FSO communication link is evaluated through Q-factor, BER, and transmission-distance measurements under different atmospheric attenuation conditions. This distinction prevents communication reliability metrics from being interpreted as direct measures of cryptographic security. The proposed system therefore evaluates both the confidentiality characteristics of the encrypted image payload and the ability of the Ro-FSO physical link to transmit the encrypted information under atmospheric impairments.

4.1.4. Weather condition formulas

4.1.4.1 Fog attenuation This form of attenuation occurs when an impulse is absorbed by the water molecules inside the fog particles. Formula 1 [14] shows how the model of Kim can calculate fog attenuation ($\beta_{\lambda(f)}$) as a function of visibility.

$$\beta_{\lambda(f)} = \frac{3.91}{V}\left(\frac{\lambda}{\lambda_o}\right)^{-p}, \ldots\ldots \tag{1}$$

Where V indicates the variety visible in kilometers (km), and λ is the performing wavelength in nanometers.
λ_o Indicates the wavelength reference, typically $550 * 10^{-9}$ m;
p Is the coefficient size of distribution scattering for the Kim model.
Table 3 shows the value of coefficient size of distribution scattering for the Kim model versus Variety visible.

Table 3. p versus V

p	V
1.6	$50 > V$
1.3	$50 < V < 6$
$0.16V + 0.34$	$1 < V < 6$
$V - 0.5$	$1 < V < 0.5$
0	$0.5 > V$

Iraqi related weather difficulties state that on 2024/22/ December visibility in Baghdad was decreased to 0.8 km due to fog. Formula 6 was used to calculate the attenuation's fog, which came out to be 4.2 dB/km for light fog and 15.5 dB/km for medium fog.

4.1.4.2 Rain attenuation Due to scattering, a distinct occurring on the wavelength, big raindrops may reduce the transmitted signal. As a result, rainfall attenuation and rainfall velocity have a linear connection. The reference [14] provides the specific attenuation (β_{rain}) for a rate of rainfall R in mm/h:

$$\beta_{rain} = 1.076R^{0.67} \ldots\ldots \tag{2}$$

The Iraqi Meteorology Association reports that Baghdad had the greatest rainfall rates on 2024, 23, March and the raining was 68.5 mm every hour. The attenuation caused by rain is 6.2 for little rain and 19.7 dB/km for intense rain, according to the formula 2.

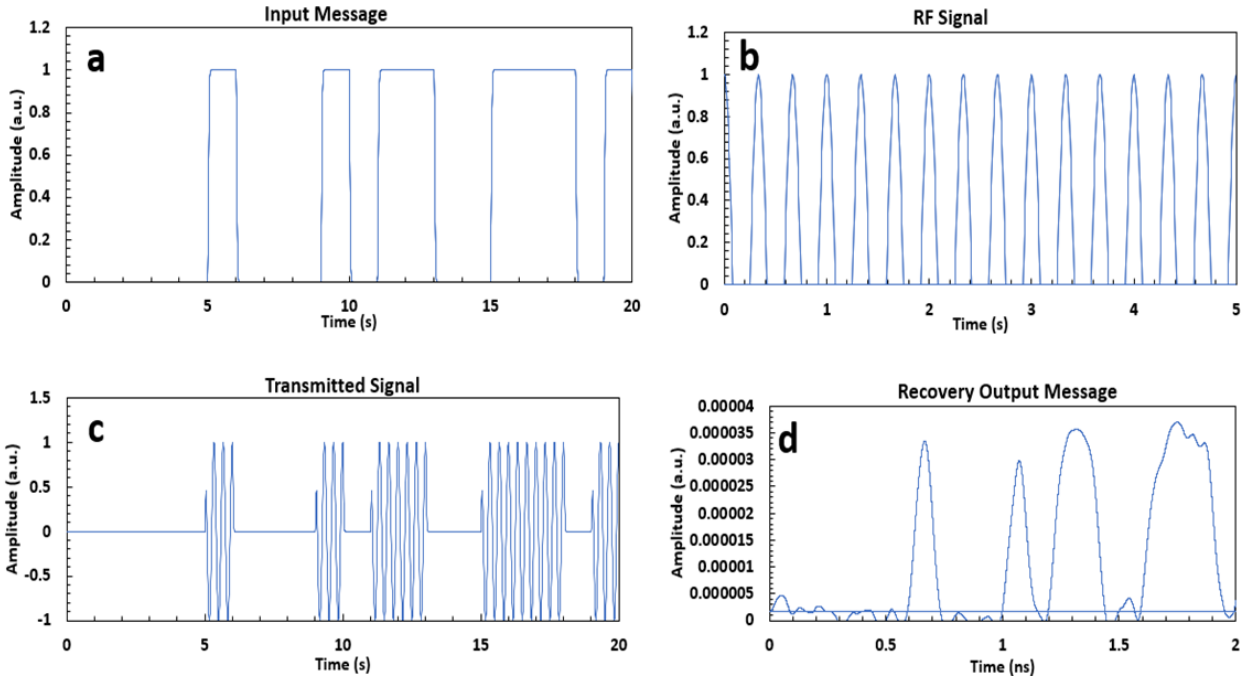


Figure 7. Time domain of signal spectrum's (a) the signal of input electrical message, (b) the signal of RF, (c) the transmitted signal in the optical form, (d) the recovered electrical signal at a maximum transmitted distance of 1.9 km under a light fog.

4.1.5. System Latency and Throughput Measurement Latency is the entire delay or quantity of time it takes to complete a certain action or function within a computer system. Users expect virtually immediate links while chatting, video calling, phone calling, and live video streaming, hence low latency or zero latency is a critical component of in-app interactions. High latency causes delays in sending messages, phone conversations, and file synchronization, especially for video files, degrading the user experience [3]. System latency refers to the end-to-end delay experienced by an optical signal as it travels from Tx to Rx. Time-domain monitoring tools developed inside the OptiSystem simulation platform are utilized to measure latency in the proposed Ro-FSO architecture. Along the transfer chain, two Optical Time Domain Visualizers (OTDVs) are strategically placed:

1. At the MZM output in the Tx to collect the transmitted timestamp, and
2. The APD/Bessel in the Rx captures the data bit's receipt timestamp.

After starting PRBS, the delay is determined as follows:

$$t_\{Latency\} = t_\{arrival\} - t_\{sent\} \ldots\ldots \tag{3}$$

t_{sent} packet's transmission timestamp, whereas t_{arrival} indicates its successful reception timestamp. Some elements that impact are FSO delay of propagation, MUX/DEMUX computation, and photodetector reaction time. The FSO ($\leq$180 m) adds less than 0.6 μs to the estimated delay of around 100 μs. The entire system latency is around 101 μs, which is well within the milisecond-level latency requirements of 5G/6G fronthaul and fully compatible with next-generation high-capacity access networks. Throughput is a computer service or device completes tasks during a certain time period [3]. System throughput measures the effective data rate given to end users without bit errors. The aggregate wavelength by the Ro-FSO architecture in the proposed configuration influences throughput. The OLT produces a total nominal capacity of 64 channel wavelengths modulated at 10 Gbps.

Throughput = 64 $\times$ * 10~Gbps = 640Gbps

These data demonstrate the conditions tested, the system consistently delivers the entire 640-Gbps speed. From a computational standpoint, since the downstream processing chain involves encrypting the binary image pixels before NRZ generation and MZM-based optical modulation throughout the multi-channel configuration, the proposed secure Ro-FSO architecture imposes a greater centralized processing burden at the Tx side. The published obtained using MATLAB 2017a on a general-purpose PC, reveal encryption timings of around 3.44-3.92 s for 256×256 test pictures. This is not a direct indicative of real-time hardware implementation at deployed Tx/Rx devices.

4.1.6. Security Validation Using End-to-End Ro-FSO Ciphertext To ensure that the cryptographic analysis reflects the actual proposed communication system rather than only the original test images, the security evaluation is defined on ciphertext generated and recovered through the complete Ro-FSO transmission chain. The test images are used only as plaintext input sources; the security measurements are performed on the resulting encrypted data and, where applicable, on the ciphertext recovered at the receiver. The end-to-end security-validation procedure is defined as follows:

Plaintext image/data → Blowfish-CBC encryption → ciphertext generation → binary conversion/framing → 64-channel WDM Ro-FSO transmission → atmospheric channel → optical detection and signal recovery → recovered ciphertext → Blowfish-CBC decryption → recovered plaintext.

The ciphertext produced immediately after Blowfish-CBC encryption is retained as the reference ciphertext. After transmission through the complete Ro-FSO link, the recovered binary sequence is reconstructed as ciphertext and compared with the transmitted ciphertext. This separation makes it possible to distinguish cryptographic properties from physical-channel impairments.mFor the ciphertext statistical analysis, the following measurements are applied to the actual ciphertext generated by the proposed system:

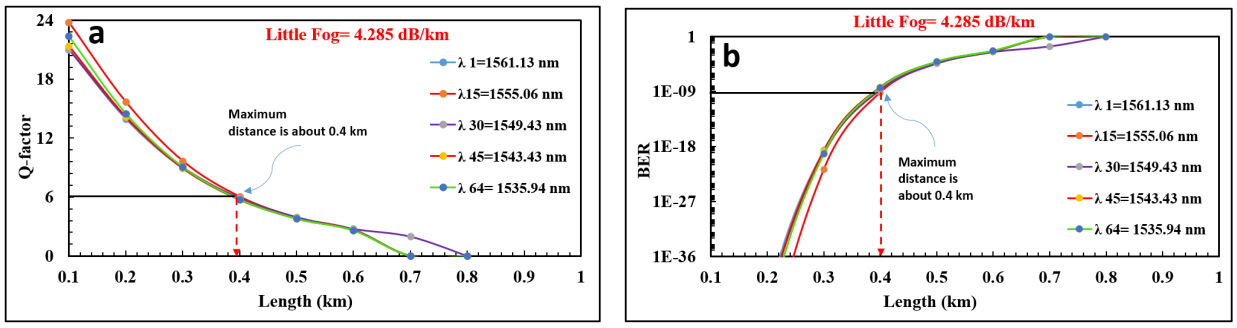
1. Ciphertext histogram: The distribution of ciphertext byte/pixel values is analyzed to see if significant statistical patterns from the plaintext are discernible after encryption.
2. Ciphertext entropy: Throughout the experiment, the ciphertext's entropy is computed using the same representation. The finding is provided as an empirical statistical feature and is not regarded only as confirmation of cryptographic security.
3. Ciphertext correlation: The correlation between neighboring ciphertext samples in the horizontal, vertical, and diagonal directions is computed. The goal is to assess if spatial relationships existing in the plaintext remain observable after encryption.
4. Key-space analysis: The theoretical key space is calculated from the actual Blowfish key length used in the implementation. It is reported independently from the ciphertext statistics because key-space size represents the number of possible keys rather than a measured property of a particular ciphertext.
5. Key-sensitivity analysis: Two encryption experiments are performed using keys that differ by a small controlled modification while keeping the plaintext and other parameters unchanged. The resulting ciphertexts are compared using an explicitly defined differential metric. An additional wrong-key decryption experiment can be used to verify that a small key modification prevents successful plaintext recovery.
6. IV analysis: Because Blowfish-CBC uses an initialization vector, the IV used for each encryption experiment is recorded separately from the secret key. The IV is not included in the key-space calculation. Its handling, transmission, and reuse policy are reported independently.
7. End-to-end ciphertext integrity: The ciphertext before transmission and the recovered ciphertext after the Ro-FSO receiver are compared. If the recovered ciphertext differs from the transmitted ciphertext because of channel impairments, the corresponding BER and Q-factor are reported together with the cryptographic results. This prevents channel-induced errors from being incorrectly interpreted as cryptographic effects.
8. Statistical bitstream testing: When a sufficiently long recovered ciphertext bitstream is available, statistical tests such as those described in NIST SP 800-22 Rev. 1a may be applied as supplementary evidence. NIST specifies multiple tests, including frequency, runs, linear-complexity, approximate-entropy, and related tests. However, these tests are statistical diagnostics and should not be presented as a standalone certification of cryptographic security. (NIST Computer Security Resource Center)

The resulting analysis therefore evaluates security at two related but distinct points: (i) ciphertext immediately after encryption, which characterizes the cryptographic transformation, and (ii) ciphertext recovered after the Ro-FSO link, which characterizes the combined effect of encryption and physical-channel transmission. Communication metrics such as BER, Q-factor, and transmission distance are reported separately from cryptographic metrics so that atmospheric degradation is not confused with weaknesses in the encryption algorithm.

As illustrated in Figures 8 and 9, the suggested system's performance is examined both with and without a preamplifier regarding BER and quality of factor (Q-factor) as a function the maximum link length, in accordance with the FSO communication limit (Q-factor = 6 and BER = 10-9). Without the use of an optical amplifier, the maximum system length in light fog is around 0.4 km, as shown in Figure 5. With the addition of an amplifier, this value can be increased to 1.9 km under the same weather conditions, as seen in Figure 9.

Under light rain weather conditions, a slight reduction in the system length is observed, becoming 0.35 km and 1.55 km without and with optical amplifier, receptively, as shown in Figures 10 and 11. A further reduction in the implemented system length to 0.26 km without an amplifier and 0.9 km after adding an optical amplifier is obtained when the weather becomes moderately foggy, as displayed in Figures 12 and 13, respectively. As seen in Figures 14 and 15, the suggested system length drops to just 0.22 km and 0.24 km without an optical amplifier, respectively, in the severe weather conditions (such as intense rain and haze). These values change to 0.76 km for intense rain (Figure 15) and 0.75 km for haze (Figure 17) upon the addition of an optical amplifier. According to the results, there is a significant deterioration along the FSO link's length of about 1.1 km, starting from transmission through a mild fog condition (which is thought to be the most suitable weather condition for our suggested system in this study) and ending with haze.

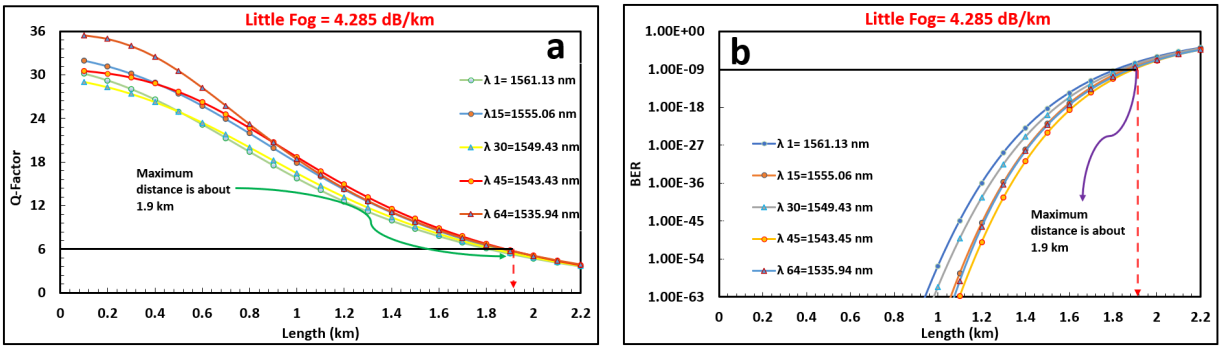
Without an optical amplifier, the maximum link length is roughly 0.4 km for dim fog, 0.35km for light rainfall, 0.26 km for moderate fog, intense rain of 0.24 km, and haze with 0.22 km, as seen in Figs. 8, 10, 12, 14, and 16. As illustrated in Figs. 10, 11, 13, 15, and 17, these ranges rose to 1.9 km (dim light fog), 1.55 km (light rainfall), 0.9 km (moderate fog), 0.76 km (intense rain), and 0.75 km (haze) when the optical amplifier was added to the broadcast signal. Compared to the setup in which an optical amplifier is not used, this indicates an improvement in system performance of roughly 375%, 342%, 246%, 216%, and 240% for dim fog, light rainfall, moderate fog, intense rain, and weather events of haze, respectively.



(a) (b)

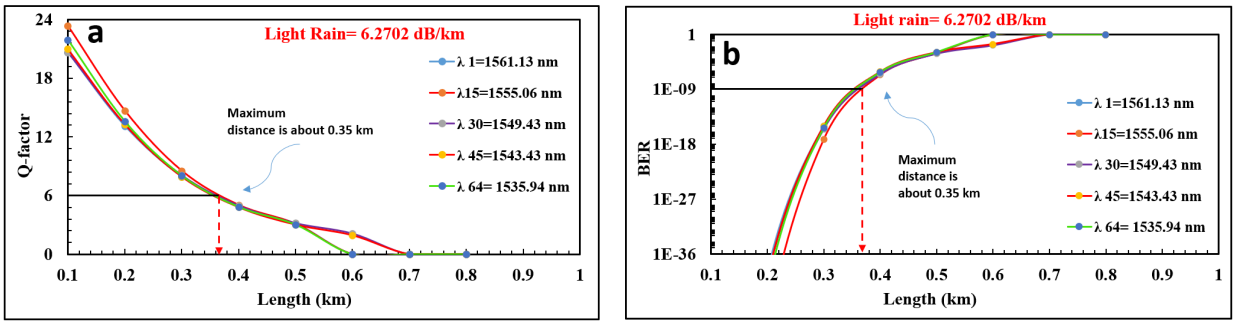
Figure 8. (a) Q-Factor as a goal of a link path and (b) BER as a goal of a link length for multi-wavelengths without an amplifier. The obtained link the distance approximates 0.4 km under attenuation equal (4.285 dB/km) with dim weather fog condition.

This section contrasts the findings from the suggested system with those from a previous study [21]. The comparison is conducted under various weather conditions, utilizing a single FSO channel as opposed to the mean lower cost, and at atmospheric attenuation values that are greater than those used in earlier work. Although the prior work achieved an approximate link range in every weather situation, our work's bit rate is roughly eight times higher than that of the prior work, which leads to a higher Bit-Rate–Distance Product (BL) in every weather condition. Also, in this work, worse weather conditions were used, as Table 4 illustrates. This is due to investigating the function of the Erbium-doped fiber amplified (EDFA) which was used in the proposed system. The possibility



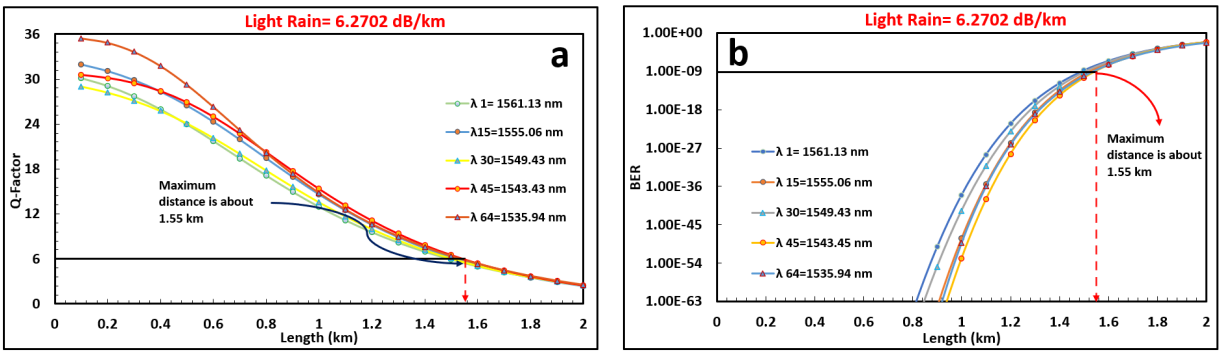
(a) (b)

Figure 9. (a) Q-Factor as a goal of a link path and (b) BER as a goal of a link length for multi-wavelengths. The obtained link the distance approximates 1.9 km under attenuation equal (4.285 dB/km) with dim weather fog condition.



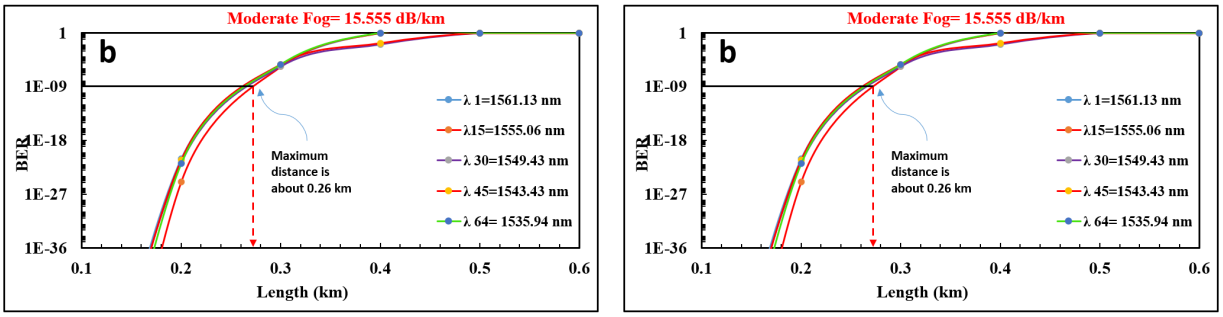
(a) (b)

Figure 10. (a) an illustration of the Q-Factor as a goal of link path, (b) BER as a goal of link range at a little rainfall weather condition under attenuation equal 6.2702 (dB/km) for many wavelengths without an amplifier, and approximately 0.35 km as the achieved link range.



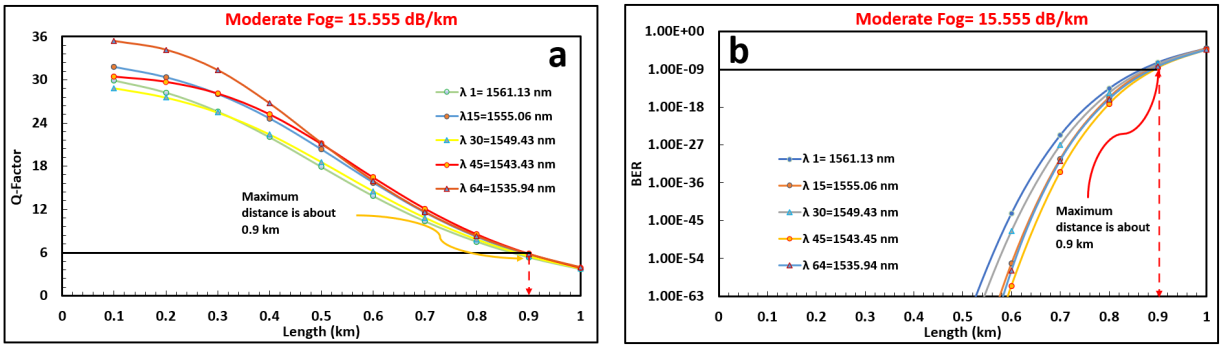
(a) (b)

Figure 11. (a) an illustration of the Q-Factor as a goal of link path, (b) BER as a goal of link range at a little rainfall weather condition with an attenuation of 6.2702 (dB/km) for many wavelengths, and approximately 1.55 km as the connection length attained.



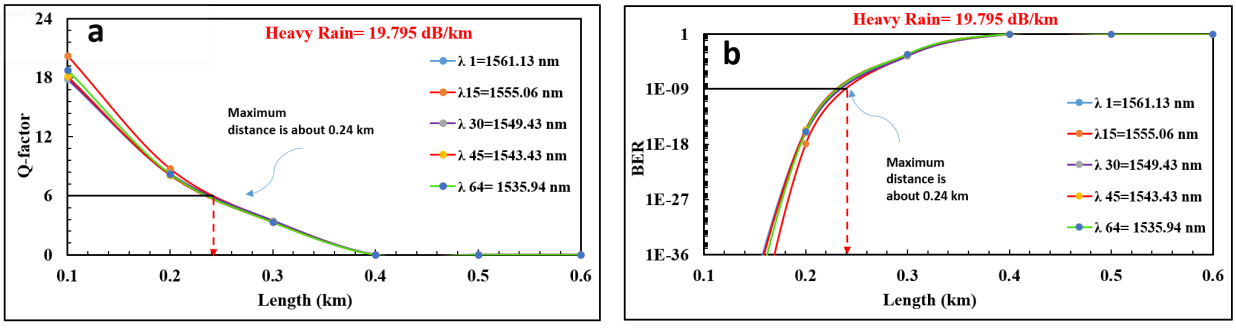
(a) (b)

Figure 12. (a) Q-Factor as a goal of length and (b) BER as a goal of link length range at Medium fog with an attenuation recorded as 15.555 (dB/km) for many wavelengths without an amplifier and 0.26 km as the achieved link range.



(a) (b)

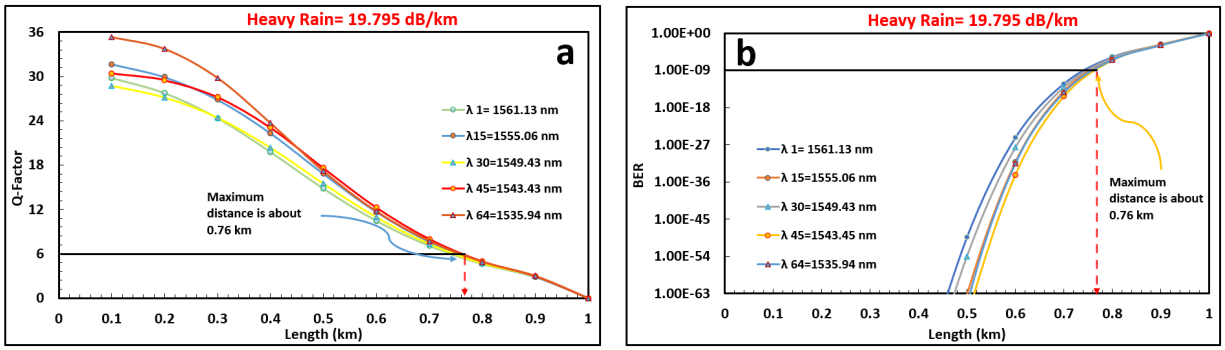
Figure 13. (a) Q-Factor as a goal of length and (b) BER as a goal of link length range at Medium fog equal attenuation at 15.555 (dB/km) for many wavelengths and 0.9 km as the achieved link range.



(a) (b)

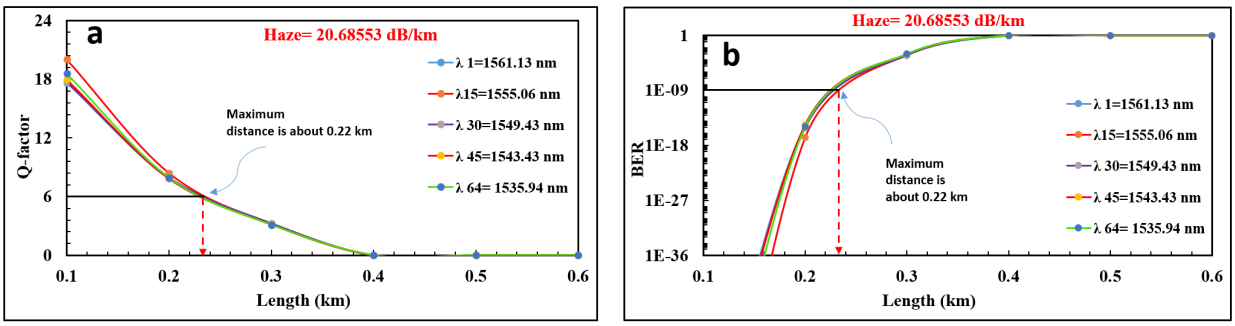
Figure 14. (a) Q-Factor as a goal of a length and (b) BER as a goal of a link length investigated at intense rain equal attenuation at 19.795 dB/km for a number of wavelengths with no amplifier and about 0.24 km is the achieved link range.

of transmission for longer transmission lengths could be accomplished via using this amplifier, which led to an improvement in the signal strength. Even though the cited study used an FSO system without amplification, the reported results of this study are greatly improved by using EDFA. However, in practice, a coupler or lens would



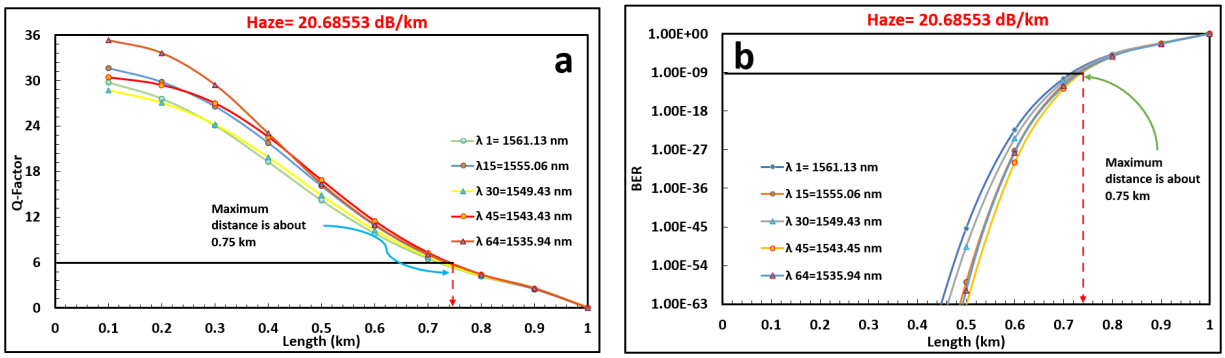
(a) (b)

Figure 15. (a) Q-Factor as a goal of a link and (b) BER as a goal of a link length investigated at intense rain equal attenuation at 19.795 (dB/km) for many wavelengths and about 0.76 km is the achieved link range.



(a) (b)

Figure 16. (a) Q-Factor as a goal of the link and (b) BER as a goal a link length at a hazy weather under attenuation equal 20.68553 (dB/km) for many wavelengths without an amplifier and about 0.22 km is the achieved link range.



(a) (b)

Figure 17. (a) Q-Factor as a goal of the length and (b) BER as a goal a link length at a hazy weather under attenuation equal 20.68553 dB/km for several wavelengths and about 0.75 km is the achieved link range.

be required to effectively guide the amplified signal via the optical line because the system is an FSO-based rather than a fiber-based.

Table 4. Investigation of the proposed employment performance in comparison to previously work [21].

The weather conditions	***Impact of Weather conditions is represented in dB km in our work***	***Impact of Weather conditions is represented in dB km in Previous work***	***Bit rate Gbps in our work***	***Bit rate Gbps in previous work***	***The link rang km in Our work***	***The link range Km in previous work***	***$B \times L$ (Gbps). Km in Our work***	***$B \times L$ (Gbps). Km in Previous work***
light fog	*4.285*	*0.2*	**640**	**80**	*1.9*	*1.9*	*1216*	*152*
Little rain	*6.2702*	*2.3*			*1.55*	*1.35*	*992*	*108*
Medium fog	*15.555*	*4.3*			*0.9*	*1.1*	*576*	*88*
Intense rain	*19.795*	*8*			*0.76*	*0.85*	*486.4*	*68*
Haze	*20.68553*	-			*0.75*	-	*480*	-

The strength of an encryption system in resilient communication programs is mostly based on the key space's size, which should be sufficient to withstand systematic attacks. The key space should be larger than 2^{100} in order to guarantee the security of picture techniques. Those that follow keys are used in the decoding process: (1) argument n indicates the key's byte count. The initial step is to use n*8 to transform that into a number of bits. The keys a binary representation is then kept in bin_x. The amount bin_x_N_Minus_1 is then used to identify the subsequent bit. Bin_x and bin_x_N_Minus_1's double precision enables a key space size of up to 10^{14}. The space key for blowfish is 264 with $(2^{64})^2 \times (10^{14})^2 \times (10^{14})^2 = 2^{314} \simeq 3.3 \times 10^{94} > 2^{100}$, which is big enough to survive a sustained attack. As a result, the design plan satisfies the secure Ro-FSO design specifications. The essential spaces of the suggested approach and those of contemporary methods documented in academic publications are contrasted in Table 5.

Table 5. The comparison of the suggested key space with the sources.

Cipher	Ref.[22]	Ref.[23]	Ref.[24]	Ref.[25]	Ref. [26]	Suggested Cipher
Space key	2^{186}	2^{149}	2^{203}	2^{199}	$3.4 \times 10^{80} \approx 2^{267}$	$10^{84} \approx 2^{314}$

The secret Blowfish key must be available to both the encryption and decryption endpoints. However, the current simulation does not implement a key-establishment or key-distribution protocol. Therefore, the simulation assumes that the transmitter and receiver already possess the same secret key through a secure external mechanism. Accordingly, the present cryptographic analysis evaluates the security characteristics of the Blowfish-CBC encryption layer but does not claim to provide a complete end-to-end key-management solution. In a practical Ro-FSO deployment, a secure key-establishment mechanism, key storage and protection, key renewal, and key

revocation procedures would need to be implemented as part of the overall security architecture. NIST defines key management as covering the lifecycle of cryptographic keys and related security parameters, including generation, storage, establishment, use, and destruction. The revised analysis therefore distinguishes four independent aspects:

1. Key space: the number of possible secret-key values for the selected key length.
2. Key sensitivity: the effect of changing the secret key on the resulting ciphertext and plaintext recovery.
3. IV handling: generation, uniqueness/unpredictability requirements, transmission, and correct use of the CBC initialization vector.
4. Key distribution: the mechanism by which the secret key is securely established or delivered to the transmitter and receiver.

Image analysis frequently uses histograms. Each intensity level's pixel count can be displayed in order to comprehend the distribution of image pixels. To stop statistical assaults, the distinctions between the plain photo and the matching encoded photograph must be shown. The corresponding pictures encrypted and the 256x256 histograms of the (Lake, Peppers, and Airplane) picture have been determined. Regarding the Lena picture, Figure 18 shows the histogram and the original images A1 corresponding to A2, while the image of encryption A3 and A4 histograms are equally scattered and substantially unique from the photographs of plain. The photo that was recovered is shown in A5. The photo used for ciphering is noisy and totally distinct from the picture of plain; consequently, no quality of the photograph of the plain is discerned from it. The proposed cryptography technique is therefore quite secure. The outcomes display how well the recommended method works to counter statistical assaults.

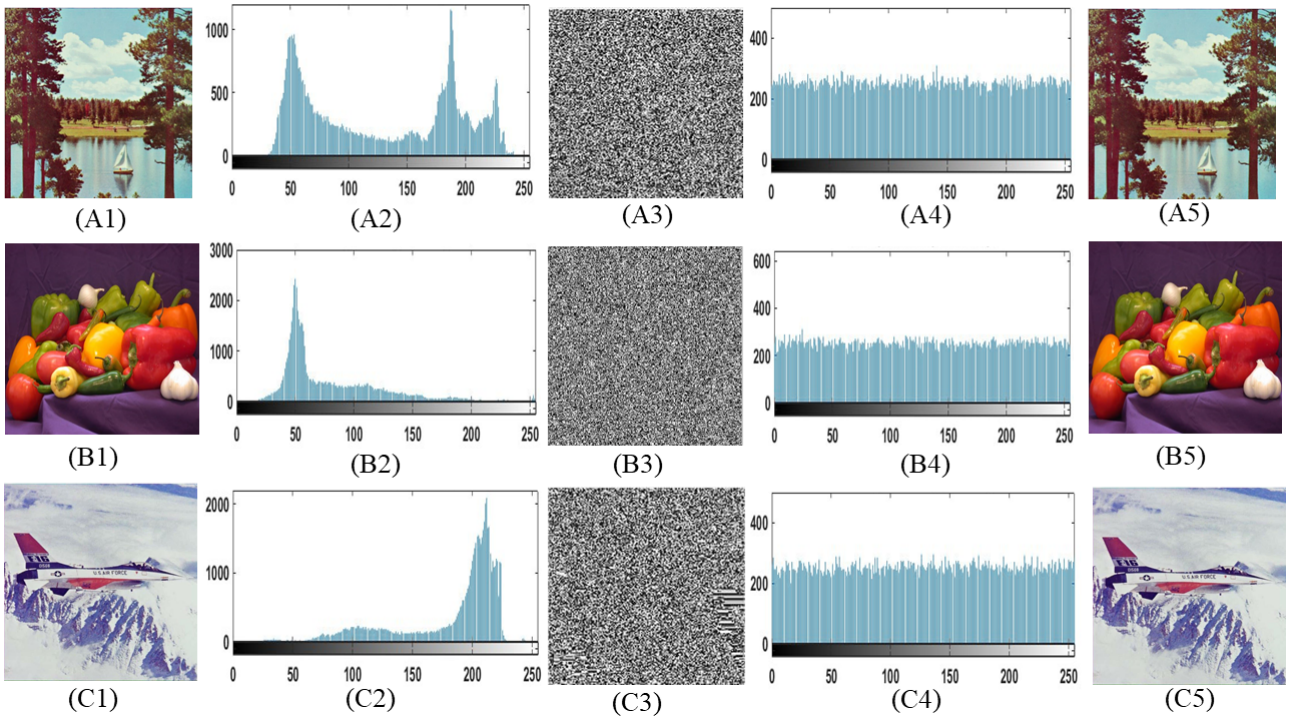
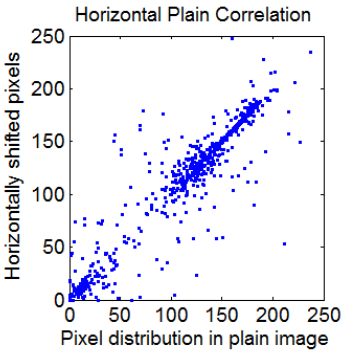
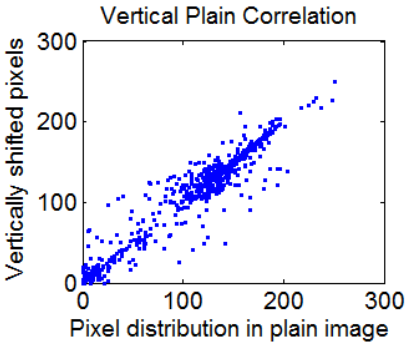


Figure 18. The simulation result: plain images (A1–C1), histogram of the plain images (A2–C2), encrypted image (A3-C3) histogram of the encrypted image (A4-C4) and the retrieved images (A5–C5).

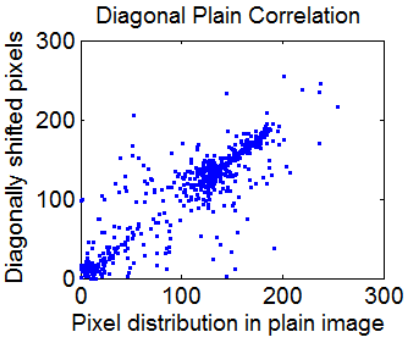
The (Lake, Peppers, and Airplane) examination image's spread of pixels in the D', V', and H' directions is seen in fig. 19. It appears that every pixel in picture that has been encrypted is evenly spaced everywhere the coordinate scheme.


Horizontal Plain Correlation
Horizontally shifted pixels
Pixel distribution in plain image
0 50 100 150 200 250

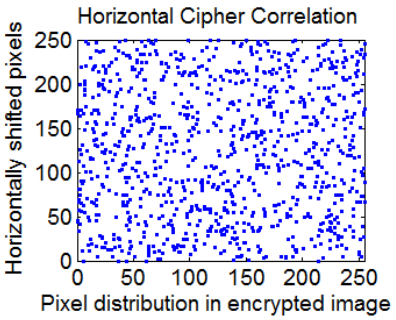
(a)


Vertical Plain Correlation
Vertically shifted pixels
Pixel distribution in plain image
0 100 200 300

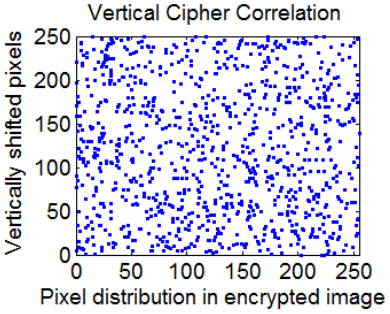
(b)


Diagonal Plain Correlation
Diagonally shifted pixels
Pixel distribution in plain image
0 100 200 300

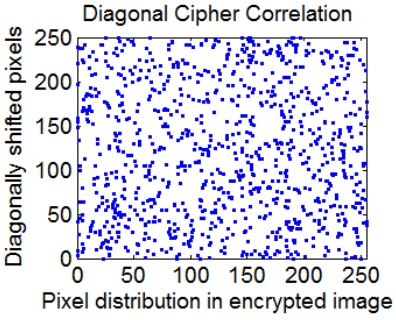
(c)


Horizontal Cipher Correlation
Horizontally shifted pixels
Pixel distribution in encrypted image
0 50 100 150 200 250

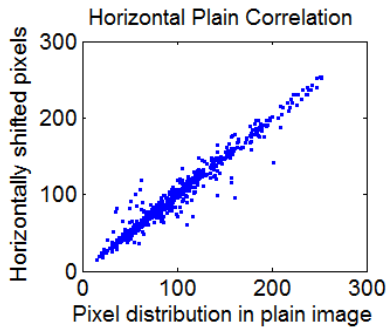
(d)


Vertical Cipher Correlation
Vertically shifted pixels
Pixel distribution in encrypted image
0 50 100 150 200 250

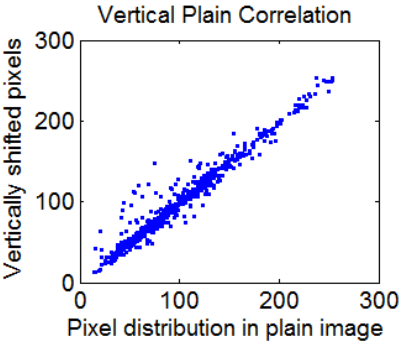
(e)


Diagonal Cipher Correlation
Diagonally shifted pixels
Pixel distribution in encrypted image
0 50 100 150 200 250

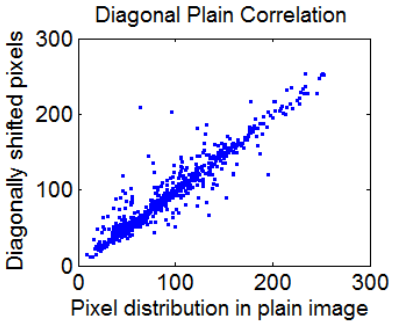
(f)


Horizontal Plain Correlation
Horizontally shifted pixels
Pixel distribution in plain image
0 100 200 300

(g)


Vertical Plain Correlation
Vertically shifted pixels
Pixel distribution in plain image
0 100 200 300

(h)


Diagonal Plain Correlation
Diagonally shifted pixels
Pixel distribution in plain image
0 100 200 300

(i)

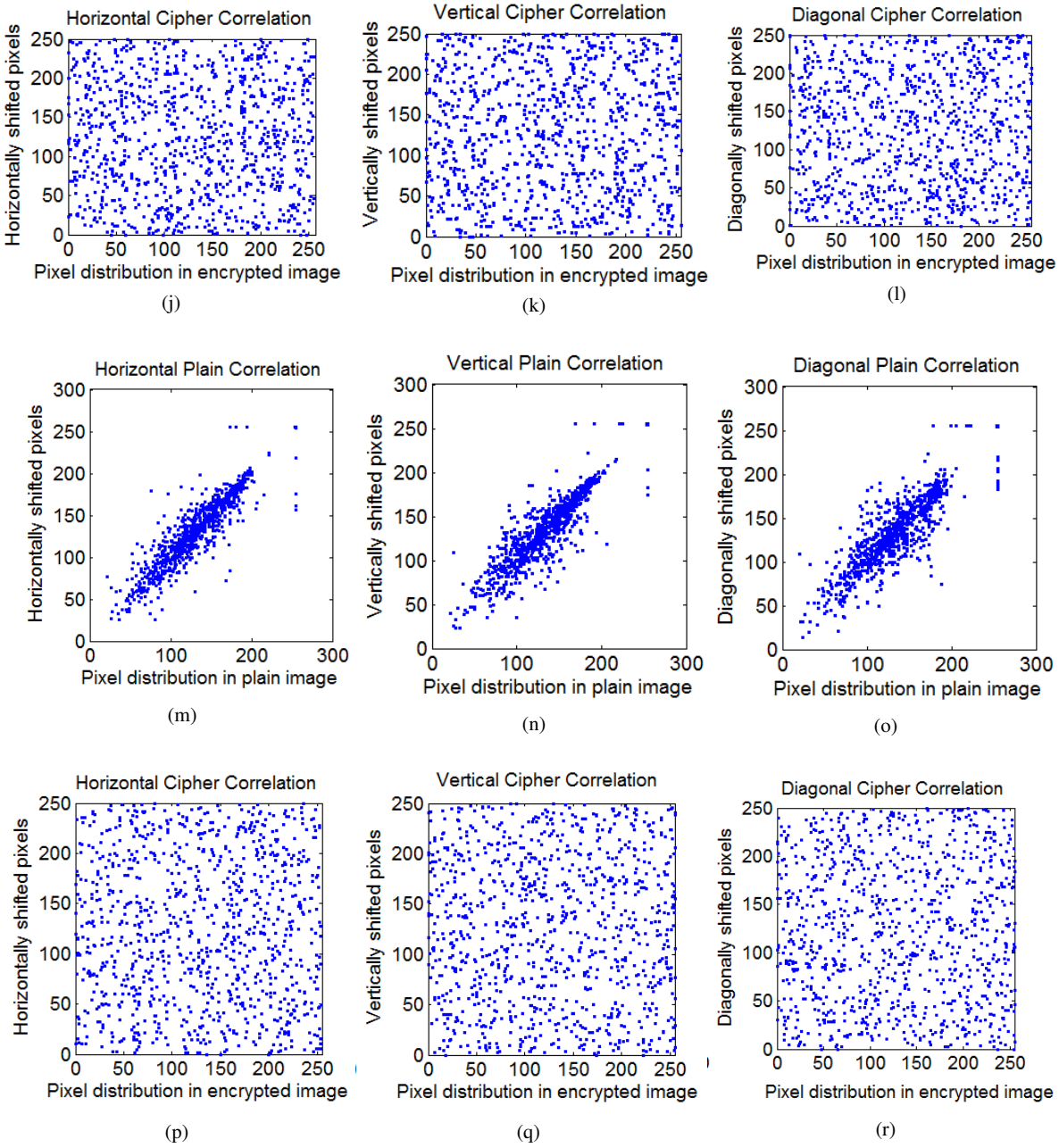


Figure 19. The correlation between the original photo a–c Lake, g–i Peppers, m–o Airplane respectively, and their congruent encrypted image Lake d–f , Peppers j–l ,and Airplane p–r.

The protection evaluation of the suggested cipher, applied to the Lena image, is benchmarked against prior research [19] and detailed in Table 6. The data presented in Table 6 highlights the superior accuracy, robustness, and encryption speed of the proposed Blowfish coding when contrasted. The proposed approach is safe, as seen by Table 6's coefficients of association, which are nearer to zero compared to the prior research. This implies that the encrypted information demonstrates greater randomness and unpredictability.

Table 6. The security evaluations of the Blowfish coding in comparison with previous work.

Analysis of security	Parameter for Security Evaluation	Proposed coding	[19]
Perceptual security analysis	peak signal-to-noise ratio (PSNR)	9.45	9.33
	square mean error	7681.78	7653.58
	absolute mean error	74.51	72.53
	Similarity Structural Index (SSIM)	1	1
	Visual Information Fidelity (VIF)	0.99987	0.99836
Correlation examination	Vertical	-0.0054	-0.0110
	Horizontal	-0.0044	0.0720
	Diagonal	0.0025	-0.0323
Differential attack	Number of Pixels Change Rate (NPCR)	99.59	99.420
examination	Unified Average Intensity Changing	28.79	27.02
Entropy examination	Entropy of coded picture	7.9972	7.9811
Time examination of encryption		2.01	2.22

Table 7. Comparison of previous research with our suggested work.

Parameter	[27]	[28]	[29]	Proposed system	Proposed novelty
System layout	Yes (FSO only)	Yes (FSO only)	Yes (Hybrid-FSO + OF)	Yes (Hybrid-Ro+FSO)	This paper has leaded a protect Ro-FSO
Transmitted power (dBm)	N.S.	7.8	15	0	Practical and secure transmission power level
Maximum data rate	N.S.	1.25	10	640	Application-specific fast data connection with a throughput of 640 Gbps
Maximum transmission range (km)	1.4	2	1.72	1.9	Transmission ranges are realistically and practically achieved in this work.
N.S : Not specified					

The simulation results show that the transmission distance depends strongly on the atmospheric attenuation condition. With the optical pre-amplifier, the maximum achievable distance was approximately 1.9 km for dim (light) fog. Under moderate fog, the achievable distance decreased to approximately 0.9 km. The corresponding maximum distances for light rain, intense rain, and haze were approximately 1.55 km, 0.76 km, and 0.75 km, respectively. These results confirm that the 1.9-km transmission distance corresponds specifically to the dim/light-fog condition and should not be associated with moderate fog. The findings of our investigation are contrasted to those associated with other investigations. By using the Blowfish cipher, the proposed system's results are equivalent to those of the other systems, which helps to explain the improvement in the secure Ro-FSO system [27, 28] and [29]. Prior technologies could only achieve maximum data rates of 10 Gbps and 1.25 Gbps. Upgrading the capacity to 640 Gbps is possible for a safe Ro-FSO system. Links with FSO transmission distances of 1.4, 2, and 1.72 kilometers are the longest. These ranges can be extended to 1.9 km when there is minimal fog. In contrast to the results above, Table 7 demonstrates that the data rate of the recommended secure configuration has the highest distance and capacity communication.

Although previous studies have demonstrated the potential of Ro-FSO and WDM-FSO technologies for high-capacity wireless optical communication, several limitations remain. These limitations can be summarized in terms of capacity, atmospheric robustness, security integration, and comprehensive system-level evaluation.

1. Limited channel capacity and scalability.
   Several previous Ro-FSO studies have investigated relatively small numbers of WDM channels. For example, an earlier WDM Ro-FSO system used eight channels at 10 Gb/s per channel, corresponding to an aggregate capacity of 80 Gb/s, and evaluated transmission under clear air, heavy rain, and heavy fog [21]. Another study increased the capacity to 160 Gb/s using 16 channels at 10 Gb/s per channel and investigated clear, haze, rain, and fog conditions. These studies demonstrate the feasibility of WDM-based capacity enhancement but leave a gap in evaluating substantially larger channel configurations within a secure Ro-FSO architecture [30]. The proposed study addresses this limitation by considering 64 WDM channels, each operating at 10 Gb/s, resulting in a nominal aggregate capacity of 640 Gb/s. Therefore, the research of the Ro-FSO design to a larger channel count while retaining the same per-channel data throughput.
2. Limited evaluation under multiple atmospheric conditions.
   One of the most FSO transmission is atmospheric attenuation. Fog, rain, haze, turbulence, and other environmental factors can dramatically affect the received power and transmission distance. Previous investigations have of weather situations or concentrated on specific bad circumstances. For example, the 160-Gb/s WDM-RoFSO research took into account clear weather, haze, rain, and fog [31]. The research suggestion compares five different meteorological conditions: light fog, light rain, moderate fog, severe rain, and haze. The greatest amplified distances obtained are around 1.90, 1.55, 0.90, 0.76, and 0.75 km, respectively. This gives a more comprehensive weather-dependent assessment of the planned high-capacity infrastructure.
3. Limited combination of high-speed Ro-FSO transfer.
   A substantial portion of previous Ro-FSO research concentrates on physical communication performance, such as BER, Q-factor, link distance, multiplexing, and atmospheric attenuation. Security may be addressed separately through physical-layer techniques or hybrid RF/FSO approaches. The literature also recognizes that FSO's narrow optical beam does not completely eliminate interception risks and that additional encryption can therefore be required [32].The proposed study integrates Blowfish-CBC payload encryption with the Ro-FSO transmission chain, allowing the communication system and cryptographic layer to be evaluated within the same overall framework. The encryption stage is applied before transmission, while the physical link is evaluated independently using communication metrics.
4. Lack of joint communication and cryptographic evaluation.
   Previous studies frequently emphasize either communication performance or security performance. This separation makes it difficult to determine how a security mechanism interacts with a high-capacity optical communication system. The proposed study addresses this issue by separating the evaluation into two complementary categories. Communication efficiency BER, Q-factor, and feasible transmission distance, whereas cryptographic behavior is investigated using ciphertext histograms, entropy, correlation, key-space

analysis, and encryption-time analysis. This distinction is significant since a good communication result does not necessarily establish cryptographic security, and favorable cryptographic statistics do not guaranty reliable optical transmission.

5. Limited consideration of amplification in conjunction with weather-dependent performance.
   Previous FSO/Ro-FSO optical amplification and other range-enhancement methods. However, the performance advantage is heavily dependent on the channel model and the accompanying atmospheric losses. Previous research has also looked into relay-assisted WDM-FSO systems particularly to reduce the impacts of rain and haze [33]. In the proposed study, system performance is evaluated both with and without optical amplification. Without amplification, the maximum distances are approximately 0.40, 0.35, 0.26, 0.24, and 0.22 km for light fog, light rain, moderate fog, intense rain, and haze, respectively. With the amplifier, these distances increase to approximately 1.90, 1.55, 0.90, 0.76, and 0.75 km. This enables the effect of amplification to be evaluated within the same system and weather conditions.
6. Insufficient end-to-end system perspective.
   Some earlier specific features such as weather attenuation, multiplexing, connection extension, and security. However, real implementation necessitates examination of the entire chain, from data production and encryption to optical transmission and receiver recovery. The suggested analysis takes into account the encryption step as well as the 64-channel WDM/Ro-FSO transmitter, atmospheric channel, optical amplification, and receiver recovery processes. The suggested model describes the system's architecture and transmission parameters.

To achieve a the suggested system was only compared to earlier research that used sufficiently comparable Ro-FSO setups. The comparison took into account four major criteria: the number of WDM channels, the per-channel data rate and aggregate capacity, the amplifier arrangement, and the atmospheric/weather model. Studies with significant variations in these factors were not utilized as direct performance benchmarks. The proposed system uses 64 WDM channels, each transmitting at 10 Gb/s, for a total notional capacity of 640 Gb/s. The system operates with a 35-GHz RF signal and evaluates light fog, light rain, moderate fog, intense rain, and haze. The current manuscript reports maximum amplified link distances of 1.90, 1.55, 0.90, 0.76, and 0.75 km for these conditions, respectively.

A particularly relevant previous study investigated a 16-channel WDM-RoFSO system with 10 Gb/s per channel, giving an aggregate capacity of 160 Gb/s. It used a 30-GHz RF carrier and evaluated clear weather, haze, rain, and fog with attenuation values of 0.2, 2.3, 4.3, and 8 dB/km, respectively. The study also investigated a dual-FSO-channel configuration to improve link range [34]. Although this study is comparable in per-channel rate, RF operation, WDM-RoFSO architecture, and weather-dependent evaluation, it is not identical to the proposed system. Its channel count is 16 rather than 64, its aggregate capacity is 160 rather than 640 Gb/s, and its channel configuration uses dual FSO paths rather than the single-link configuration considered here. In addition, its atmospheric attenuation values and weather categories differ from those used in the present study. Therefore, its reported link distances should be interpreted as a contextual benchmark rather than as a direct one-to-one performance comparison. Another study investigated a 16-channel WDM-RoFSO system operating at 60 GHz, with 10 Gb/s per channel and an aggregate rate of 160 Gb/s. It considered light fog, moderate fog, moderate rainfall, and heavy rainfall and reported attenuation values of 5.8, 7.7, 9.2, and 26 dB/km, respectively. The system incorporated range-enhancement techniques under adverse weather conditions [35]. Because its RF frequency, channel count, aggregate capacity, and weather attenuation values differ from those of the present system, it is not treated as a strict quantitative benchmark. A further study considered a hybrid WDM-RoFSO/fiber system with 16 channels at 2.5 Gb/s per channel and a 20-GHz RF carrier. Its architecture incorporated a Raman/ Erbium-Doped Fiber Amplifier (EDFA) hybrid optical amplifier with gain 4 dB and noise figure (NF) is 20 dB and investigated fog, dust, and rain. Although this work is relevant because it explicitly includes optical amplification and multiple atmospheric conditions, its aggregate Ro-FSO rate is only 40 Gb/s and the optical-fiber segment and hybrid Raman/EDFA configuration make the architecture substantially different from the proposed 640-Gb/s Ro-FSO system [36]. It is therefore excluded from direct numerical ranking. The comparison is summarized in table 8 as follows:

Table 8. Comparison of previous research by using comparable channel counts, data rates, amplifier configurations, and weather models with other studies.

Study	Channels	Rate/channel	Aggregate rate	RF	Weather model	Direct comparability
Present work	64	10 Gb/s	640 Gb/s	35 GHz	Optical amplifier	Light fog, light rain, moderate fog, intense rain, haze
[34]	16	10 Gb/s	160 Gb/s	30 GHz	Dual FSO channel	Clear, haze, rain, fog
[35]	16	10 Gb/s	160 Gb/s	60 GHz	Range-enhancement configuration	Light/moderate fog and rain
[36]	16	2.5 Gb/s	40 Gb/s	20 GHz	Raman/EDFA	Fog, dust, rain

5. Conclusion

The Opti-System program is used with MATLAB devices to simulate a Blowfish cipher-based Ro-FSO communication system and create a 64-channel, 640 Gbps system. A key benefit of this technology is its ability to facilitate last-mile applications and support the smart city concept. The installation of an optical amplifier led to an examination of the functioning of the system operational capability according to its transmission range across various weather conditions. A high BL of roughly 1216 Gb/s km (640*1.9) was created by the suggested work under conditions with low fog, and in hazy weather, it was reduced to around 39%, or 480 Gb/s km. Furthermore, by using the pre-amplifier technique, the BL of the proposed work was clearly improved for the worst weather conditions when compared to the earlier work [21]. Under the considered atmospheric conditions, the maximum transmission distance achieved with the optical pre-amplifier was approximately 1.9 km under light (dim) fog, 1.55 km under light rain, 0.9 km under moderate fog, 0.76 km under intense rain, and 0.75 km under haze. Without optical amplification, the achievable transmission distances were substantially reduced under the corresponding atmospheric conditions. Based on the performance analysis, our suggested system has a considerable key space, minimal correlations between its coefficients, a comparable distribution of histograms, and enhanced resistance to typical attacks, consisting of statistical, Brute-force, and anti-attacks differential. It is a useful tool for safe communication with grayscale images.

Disclosures: The authors declare no conflicts of interest.

REFERENCES

1. O. Aboelala, I. E. Lee, and G. C. Chung, *A Survey of Hybrid Free Space Optics (FSO) Communication Networks to Achieve 5G Connectivity for Backhauling*, Entropy, vol. 24, art. no. 1573, 2022, doi: 10.3390/e24111573.
2. Z. A. Okbi, I. K. Alak, E. N. Abdulla, and H. H. Al-khaylani, *Design and security analysis of an image encryption based on gigabit passive optical network employing fiber-FSO protection at the last mile*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0466.
3. L. A. Salman and E. N. Abdulla, *Capacity and security enhancement in hybrid TWDM–FSO–NG–PON2 access network with self-protected fiber–FSO link paths effective against fiber breaks*, Optik, vol. 350, art. no. 172734, 2026, ISSN 0030-4026, doi: 10.1016/j.ijleo.2026.172734.
4. S. Phuchortham and H. Sabit, *A Review of the Structure of Free-Space Optical Channel Models: Physical Meaning, Assumptions, and Atmospheric Conditions*, Photonics, vol. 13, art. no. 425, 2026, doi: 10.3390/photonics13050425.
5. A. Kumar and P. Krishnan, *RoFSO system based on BCH and RS coded BPSK OFDM for 5G applications in smart cities*, Optical and Quantum Electronics, vol. 54, art. no. 18, 2022, doi: 10.1007/s11082-021-03392-y.
6. M. Esmail, A. Ragheb, H. Fathallah, M. Altamimi, and S. Alshebeili, *5G-28 GHz Signal Transmission Over Hybrid All-Optical FSO/RF Link in Dusty Weather Conditions*, IEEE Access, vol. 7, pp. 24404–24410, 2019, doi: 10.1109/ACCESS.2019.2900000.

7. I. Ismail, U. Saulaiman, W. Z. Wan Ismail, F. Mustafa, M. Sahrim, J. Jamaludin, and S. Rao Balakrishnan, *A study on Malaysia atmospheric effect on radio over free space optic through radio frequency signal and light propagation in fiber for future communication development*, AIP Conference Proceedings, vol. 2203, art. no. 020018, 2020, doi: 10.1063/1.5142110.
8. K. H. Shakthi Murugan, A. Sharma, and J. Malhotra, *Performance analysis of 80 Gbps Ro-FSO system by incorporating hybrid WDM-MDM scheme*, Optical and Quantum Electronics, vol. 52, art. no. 505, 2020, doi: 10.1007/s11082-020-02613-0.
9. A. Kumar, R. Dhanagopal, M. Albreem, and D.-N. Le, *A comprehensive study on the role of advanced technologies in 5G based smart hospital*, Alexandria Engineering Journal, vol. 60, pp. 5527–5536, 2021, doi: 10.1016/j.aej.2021.04.016.
10. S. Salahshour, *SR2AS: An Efficient and Reliable ultralightweight RFID Authentication Scheme for Healthcare Systems*, Journal of Intelligent and Fuzzy Systems, 2020.
11. T. Jose, *Performance Analysis of a RoFSO Link for 5G Networks Under Adverse Weather Conditions*, PRZEGLĄD ELEKTROTECHNICZNY, vol. 1, pp. 69–71, 2021, doi: 10.15199/48.2021.04.11.
12. F. F. Ridha, E. N. Abdulla, and A. H. Abdulhadi, *Machine learning based on raw ensemble predictions scheme for TWDM-PON*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0373.
13. E. Mousa, E. N. Abdulla, and S. A. Adnan, *Enhancing network security based on 10G-EPON with the use of the Hill cipher algorithm*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0201.
14. A. H. Ali, E. N. Abdulla, and R. J. Al-Azawi, *Security and network performance analysis of coexistence TWDM–NG-PON2, GPON and 10G-EPON systems based on Hill Cipher*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0435.
15. A. H. Ali, B. Al-Hamadani, E. N. Abdulla, et al., *Enhancing communication security of an image encryption based on XGS-PON with utilizing Hill group cipher*, Journal of Optics, 2026, doi: 10.1007/s12596-026-03056-8.
16. E. N. Abdulla, S. A. Adnan, R. Musadaq, R. A. Hussien, and A. S. Ahmed, *Capacity and Security Enhancing of 4 Gigabit Passive Optical Networks Based on Hill Algorithm*, In: W. A. Mahmoud et al. (eds.), Advanced Communications and Digital Networks, ACDN 2025, Communications in Computer and Information Science, vol. 2798, Springer, Cham, 2026, doi: 10.1007/978-3-032-15448-4_1.
17. A. J. Mansoor, M. M. Salih, E. N. Abdulla, and H. H. Al-khaylani, *Hybrid-enhanced secure strategy for encryption image and key management based on WDM/TDM-PON using hill group cipher*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0507.
18. A. H. Ali, R. M. Zaal, E. N. Abdulla, and H. H. Al-khaylani, *Capacity and security enhancement in TWDM-NG-PON2 networks based on hybrid algorithms for image transmission*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0363.
19. A. B. F. A. Mohammed, S. T. Al-hadeethi, H. H. Al-khaylani, T. A. Elwi, and E. N. Abdulla, *An investigation of success probability and fidelity of quantum repeater in asymmetry in midpoint placement in fiber-based quantum networks*, Journal of Optics, 2025, in press, doi: 10.1007/s12596-025-02866-6.
20. A. Niaz, F. Qamar, M. Ali, R. Farhan, and M. Islam, *Performance analysis of chaotic FSO communication system under different weather conditions*, Transactions on Emerging Telecommunications Technologies, vol. 30, art. no. e3486, 2019, doi: 10.1002/ett.3486.
21. M. A. Saleh, A. K. Abass, and M. H. Ali, *Enhancing performance of WDM-RoFSO communication system utilizing dual channel technique for 5G applications*, Optical and Quantum Electronics, vol. 54, art. no. 497, 2022, doi: 10.1007/s11082-022-03857-8.
22. X. Wang, X. Zhu, and X. Wu, *Image encryption algorithm based on multiple mixed hash functions and cyclic shift*, Optics and Lasers in Engineering, vol. 107, 2017, doi: 10.1016/j.optlaseng.2017.06.015.
23. J.-x. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, *Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression*, Optics & Laser Technology, vol. 99, 2017, doi: 10.1016/j.optlastec.2017.09.008.
24. X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, *Color image DNA encryption using NCA map-based CML and one-time keys*, Signal Processing, vol. 148, 2018, doi: 10.1016/j.sigpro.2018.02.028.
25. J.-x. Chen, Z.-l. Zhu, C. Fu, H. Yu, and L.-b. Zhang, *A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism*, Communications in Nonlinear Science and Numerical Simulation, vol. 20, pp. 846–860, 2015, doi: 10.1016/j.cnsns.2014.06.032.
26. R. Guesmi, M. Farah, A. Kachouri, and M. Samet, *A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2*, Nonlinear Dynamics, vol. 83, 2015, doi: 10.1007/s11071-015-2392-7.
27. U. A. Korai, F. Shaikh, S. Kalwar, K. Kumar Soothar, B. Muneer, and A. Solangi, *Analyzing The Quality of Free Space Optical Signal in Fog: A Case Study of Pakistan*, Wireless Personal Communications, 2017, doi: 10.1007/s11277-016-3910-8.
28. W. Ruslan, S. Idrus, A. Ramli, N. Ramli, A. Supa'at, and F. Nor, *Terrestrial Free Space Optic Propagation Analysis Considering Malaysia Weather Condition*, Jurnal Teknologi, 2012, doi: 10.11113/jt.v54.811.
29. H. Singh, R. Miglani, N. Mittal, H. Singh, J. Kaur, and A. Gupta, *Development of a cost-effective optical network based on free space optical (FSO) and optical fiber links for enabling smart city infrastructure: A hybrid approach*, Optical Fiber Technology, art. no. 103544, 2023, doi: 10.1016/j.yofte.2023.103544.
30. S. Kaur and A. Sharma, *Impairment analysis of WDM Ro-FSO system under different weather conditions employing machine learning*, Journal of Optoelectronics and Advanced Materials, vol. 25, pp. 444–452, 2023.
31. A. Nafis Khan, S. Saeed, Y. Naeem, M. Zubair, Y. Massoud, and U. Younis, *Atmospheric Turbulence and Fog Attenuation Effects in Controlled Environment FSO Communication Links*, IEEE Photonics Technology Letters, vol. 34, pp. 1341–1344, 2022, doi: 10.1109/LPT.2022.3217072.
32. S. Al-Gailani, M. F. Mohd Salleh, A. Salem, R. Shaddad, U. Sheikh, N. Algeelani, and T. Almohamad, *A Survey of Free Space Optics (FSO) Communication Systems, Links, and Networks*, IEEE Access, vol. 9, pp. 7353–7373, 2020, doi: 10.1109/ACCESS.2020.3048049.
33. M. R. Hayal, E. Elsayed, D. Kakati, M. Singh, A. Elfikky, A. Boghdady, A. Grover, S. Mehta, S. A. H. Mohsan, and I. Nurhidayat, *Modeling and investigation on the performance enhancement of hovering UAV-based FSO relay optical wireless communication systems under pointing errors and atmospheric turbulence effects*, Optical and Quantum Electronics, vol. 55, pp. 1–23, 2023, doi: 10.1007/s11082-023-04772-2.

34. P. Kumari, V. Kumar, and S. Arya, *Modified modelling of 16-channels WDM-RoF system in the presence of OPC and FBG for 5G applications*, Journal of Optical Communications, 2025, doi: 10.1515/joc-2025-0274.
35. K. Kaur and A. Nain, *Range augmentation of 16 × 60 GHz WDM RoFSO system in foggy & rainy weather*, Journal of Optical Communications, vol. 45, 2023, doi: 10.1515/joc-2023-0316.
36. S. Zuhair, S. Alnajjar, and F. Arif, *Performance Analysis of WDM-hybrid RFoFSO\FO System Under Different Weather Conditions Utilizing A Hybrid Optical Amplifier*, IOP Conference Series: Materials Science and Engineering, vol. 1105, art. no. 012035, 2021, doi: 10.1088/1757-899X/1105/1/012035.