Received: 27 October 2025 | Revised: 29 January 2026 | Accepted: 7 May 2026 | Published online: 28 May 2026

RESEARCH ARTICLE

Journal of Optics and Photonics Research
2026, Vol. 00(00) 1–15
DOI: 10.47852/bonviewJOPR62027992

BON VIEW PUBLISHING

Performance of Encoding, Encryption, and Modulation Schemes in Free-Space Optical Communication Evaluated on the Atmospheric Testbed

Shashank Shekhar[1], Dhanush Devappa B C[1], Moksh Chandrakar[2] and Appala Venkata Ramana Murthy[1*]

[1] *Department of Applied Physics, Defence Institute of Advanced Technology, India*

[2] *Center for Basic Sciences, Pt. Ravishankar Shukla University, India*

Abstract: In this paper, we investigate the adverse atmospheric effects, including wind disturbance, dry fog, wet fog, and smoke conditions, which are simulated on an atmospheric testbed specifically built for free-space optical communication (FSOC) experiments. We have also developed an FSOC system that can modulate the optical signals with the choice of the modulation, encoding scheme, and encryption. A robust, secure link that is operated by the user from a single graphical user interface. We have further tested the secure link with two encryption schemes, three error correction codes, and five different modulation formats with various combinations and in different atmospheric conditions. We have evaluated the link performance by two important metrics, that is, execution time and bit error rates. The results obtained can explicitly show the effect of the adverse channel. Initial experiments, with a clean chamber, showed the behavior of link performance with data rate. Further results show that the smoke chamber can adversely impact the FSOC system with an early onset of error occurrence and contributes to 10–20% of additional error compared to a clean chamber. Among error correction codes, the Reed–Solomon code helps to improve the error in all adverse conditions. This study further expands to the real-time and on-field investigation of free-space optical links for better performance.

Keywords: free-space optical communication, modulation techniques, forward error correction codes, Rivest–Shamir–Adleman, Advanced Encryption Standard

1. Introduction

In recent years, the need for improved and more secure communication systems has generated growing interest in free-space optical (FSO) communication (FSOC). Unlike conventional radio frequency (RF) links that transmit data on a free-space RF wave, free-space optical (FSO) systems transmit data through a narrow optical beam, which can reach extremely high data rates without concern for obtaining a licensed spectrum [1, 2]. The need for high-speed long-haul communication also gives rise to FSO setups; the community is developing techniques such as multiple-input multiple-output (MIMO), hybrid RF-FSO, or optical beam correction to sustain Gbps/Tbps rates for FSO links of several kilometers [3–5].

FSO systems are also naturally immune to electromagnetic interference and present a reduced risk of interception due to the highly directional nature of light [6]. These properties make FSOC appealing in applications covering links between buildings, satellite and ground communications, and defense communications [7, 8]. However, because the transmission medium is open air, the performance of the FSOC system is sensitive to ambient conditions [9].

The information-carrying optical signal traveling through the atmosphere is subject to multiple unpredictable factors. Variations in ambient temperature and pressure lead to variations in the refractive index, which causes turbulence and intensity scintillation at the receiver [10, 11]. Fog, rain, dust, and smoke scatter and absorb the transmitted light, adding to the optical power loss and fading some distance along the link [12]. Collectively, these factors can lead to increased bit error rate (BER) and lower link reliability. Modern FSOC systems utilize a variety of digital modulation techniques such as On–Off Keying (OOK), Pulse Position Modulation (PPM), Differential Pulse Interval Modulation (DPIM), and Dual Header Pulse Interval Modulation (DHPIM), each offering unique advantages in bandwidth efficiency and robustness against channel impairments [13]. Many modulation techniques require external modulators, which are expensive and complex to set up. Some modulation techniques do not require external modulators; one, for example, is OOK, which is the simplest modulation technique possible [14].

***Corresponding author:** Appala Venkata Ramana Murthy, Department of Applied Physics, Defence Institute of Advanced Technology, India. Email: avrmurthy@diat.ac.in

Numerous researchers have explored many approaches to mitigate atmospheric turbulence effects, absorption, and scattering effects, which significantly improve the optical beam quality and link performance. Some of the techniques are aperture averaging, adaptive optics, and spatial diversity techniques such as MIMO and the use of multiple lenses from Vertical-Cavity Surface-Emitting Laser (VCSELs) [15]. In the time domain, several temporal diversity techniques can improve the link performance. Among those, forward error correction (FEC) is relatively easy to implement and promises a reliable improvement [16]. These FEC techniques have demonstrated improvement in maintaining signal stability and increasing the signal-to-noise ratio at the receiver [17]. For instance, aperture averaging reduces turbulence-induced scintillation by using a larger receiver to average out intensity fluctuations, while adaptive optics can dynamically adjust the transmitted beam in real time to compensate for wavefront distortions caused by environmental variations using deformable mirrors and wavefront sensors to restore the original shape, ensuring better link alignment and power reception under varying weather conditions.

Modern communication poses challenges to data security, and hence, additional security layers become essential. While FSO, being a line-of-sight (LOS) communication, offers an inherent physical layer security, it is not guaranteed to have security in other layers. Hence, integration of conventional security features into optical communication is also essential. Commonly described methods to secure the data packets are encryption algorithms, such as the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) [18, 19]. Nonetheless, these security mechanisms introduce processing burdens or overhead, making it less than ideal for real-time or high-speed systems developing what scientists are calling "physical layer security," taking the actual randomness of the channel to secure communications without encryption. In 1997, Ron Rivest, Adi Shamir, and Leonard Adleman designed a family of public-key encryption algorithms to encrypt data, which was named RSA after them [20]. In addition, the National Institute of Standards and Technology began researching a much higher level of encryption, that is, the AES, which later became the default encryption. Securing the data in FSOC is not a new concept; researchers have been trying to incorporate cryptography since the early 2000s. The recent progress in the domain of FSOC encryption has been shown in Table 1.

This study will evaluate the impacts of adverse atmospheric conditions of turbulence, fog, smoke, and wind on the FSOC link,

Table 1
Comparative studies on recent work on encrypting the FSOC link

Authors	Year	Research focus	Study
Rivest et al. [20]	1978	A method for obtaining digital signatures and public-key cryptosystems	Theoretical
Wardlaw [21]	2000	The RSA public-key cryptosystem	Theoretical
Kuo and Verbauwhede [22]	2001	Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm	Theoretical
Somani et al. [23]	2010	Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing	Theoretical
Khatarkar and Kamble [24]	2015	A survey and performance analysis of various RSA-based encryption techniques	Theoretical
Abd El-Malek et al. [25]	2016	Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling	Theoretical
Mostafa [26]	2017	Physical layer security for visible-light communication systems	Theoretical
Abd El-Malek et al. [27]	2017	Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference	Theoretical
Blinowski et al. [28]	2018	LuxSteg: First practical implementation of steganography in Visible Light Communication (VLC)	Experimental
Ai et al. [29]	2019	Physical layer security of hybrid satellite-FSO cooperative systems	Theoretical
Yesilkaya et al. [30]	2020	Physical-layer security in visible light communications	Theoretical
Banerjee and Murthy [31]	2021	Simulation of a secure optical communication system using different optical modulation schemes coupled with the Rivest–Shamir–Adleman algorithm	Experimental
Kim and Han [32]	2022	A novel model was developed and studied for alignment error with multiple incident beams	Simulation
B. C. et al. [33]	2025	Performance analysis of RSA-encrypted secure free-space optical communication link under adverse atmospheric conditions implemented on a testbed	Experimental
Joseph et al. [34]	2025	Security enhancement in mission-critical free-space optical communication using AES-128 encryption algorithm	Experimental
This work	2025	Investigation of various encoding, encryption, and modulation schemes with atmospheric channel effects on an optical wireless communication link	Experimental

both reliability and security, in a 2m FSOC link with different modulation techniques (On-Off Keying with Non-Return-to-Zero [OOK-NRZ], On-Off Keying with Return-to-Zero [OOK-RZ], DPIM, DHPIM) with FEC codes (Repeat codes, BCH code, Reed–Solomon code [RSC]) and encryption techniques such as RSA and AES. This will include an assessment based on the metrics of BER and secrecy capacity based on diverse channel scenarios to provide insight into how performance may fluctuate based on environmental disturbances. Insight and results from the study are anticipated to potentially assist in designing a more robust and secure optical system architecture applicable for deployment in real environments. Figure 1 shows the experimental setup and graphical user interface (GUI).

2. Theoretical Framework

Modulation techniques are important to establish reliable and efficient data transmission in free-space optical communication (FSOC) and also FEC codes. The advantages of various modulation types, including OOK-NRZ, OOK-RZ, PPM, and DPIM, differ based on the link requirements and cumulative atmospheric conditions. In addition to modulation schemes, FEC

Figure 1
Schematic of the optical wireless communication with an in-house developed GUI

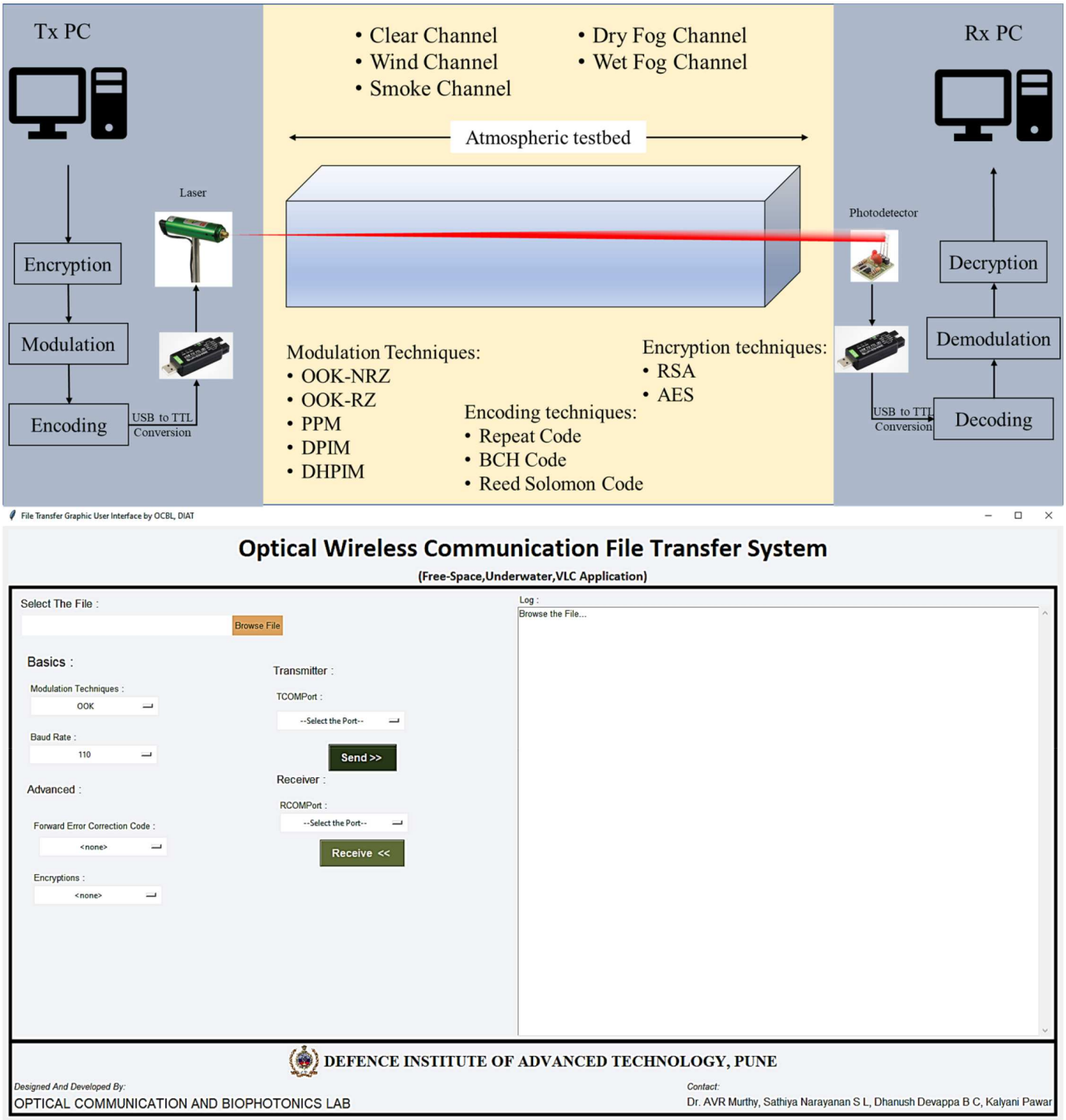
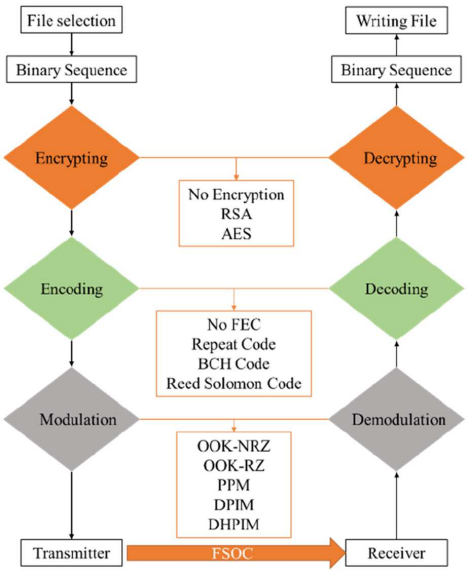


Figure 2
Flow chart showing the working of transmitter and receiver systems in the GUI



approaches utilize structured redundancy at the transmitter side to minimize data loss—helping the receiver to identify the occurrence of and address the physical layer impairment due to noise, attenuation, or turbulence of the FSOC channel. Figure 2 shows the flow chart of the receiver and transmitter mechanics used.

2.1. Modulation schemes

This incorporated modulation techniques such as DPIM, OOK-NRZ, PPM, and Return-to-Zero formats. These modulation schemes are not only relatively trivial but also provide other benefits such as transmission reliability, energy efficiency, and bandwidth efficiency.

On-Off Keying NRZ, RZ, and PPM modulation schemes: The very basic way to modulate information is called "on-off keying," or OOK. The laser is "on" for bit "1" and "off" for bit "0." OOK can be implemented using two pulse formats: Non-Return-to-Zero (NRZ) and Return-to-Zero (RZ) [35]. PPM is a power-efficient modulation technique in which the position of the pulse being transmitted contains the information [36].

Differential Pulse Interval Modulation: DPIM is energy- and bandwidth-efficient because there are no wasted slots each time a pulse is received, the clock starts over, and all the slots after the received pulse are discarded. The number of empty slots between any two pulses constitutes the information in PIM (pulse interval modulation). To facilitate tracking of the slots, a guard band can be added immediately after the pulse, which is referred to as Differential Pulse Interval Modulation 1 Guard Slot; if there is no guard band, it is referred to as Differential Pulse Interval Modulation No Guard Slot [37].

Dual Header Pulse Interval Modulation: DHPIM is a modification of the PIM. DHPIM performs well for lowered error rates and will also provide higher capacity throughput reliability. DHPIM has two different header pulses for each symbol frame, and each header is followed by different linked intervals to represent data bits. DHPIM is similar to DPIM; DPIM uses a single header to encode its symbols, whereas DHPIM allows dual headers and single headers. Meaning the modulation requires fewer data symbol slots to be representable [38].

2.2. Forward error correction schemes

Repeat Codes: By duplicating the bits several times, communication systems can ensure that data preservation is guaranteed. For example, if the bits are replicated 5 times, then the code is called Repeat (5), or can be repeated n times, called Repeat (n). As the number of repetitions increases, the error correction ability also increases. These simple techniques of error correction are beneficial for low-data-rate applications with all types of files.

BCH Code: It is possible to create BCH codes using Galois fields. BCH codes have advantages in handling a high BER because they will correct many different errors. The number of bits a code will correct is determined by the size of the Galois field, within which the coding happens via arithmetic operations. The construction of BCH codes involves one important step, and that is the selection of a generator polynomial, which generates a set of code words that have predetermined error correction capability. The generator polynomial is produced from a primitive element within the Galois field and its integer powers. These integer powers are then multiplied together to give the generator polynomial. When data is constructed via polynomial division, it is encoded using the generator polynomial [39].

Reed–Solomon Code: The RSC effectively handles burst errors in varying atmospheric conditions using multi-bit symbols to encode data as opposed to single bits. The use of RSCs is important for maintaining a high level of data integrity in deep-water applications by being computationally intensive to encode as an important aspect of RSCs. The original message is used to generate redundant symbols before transmission by mathematical operations with a finite field. The number of redundant symbols used will depend on the design of the code and the error correction level required [40].

2.3. Encryption schemes

Encryption schemes are widely used to enhance data security, ensuring that third parties do not have access to sensitive information. Encryption techniques are mainly classified into two types: symmetric encryption (AES, Data Encryption Standard (DES), etc.) and asymmetric encryption (RSA, Elliptic Curve Cryptography (ECC), etc.), depending on the keys. Symmetric encryption uses the same keys for both encryption and decryption, whereas asymmetric encryption uses a public key for encryption and a private key for decryption.

Rivest–Samir–Adleman: RSA is an asymmetric encryption technique that uses two prime numbers and their combinations to create the public keys and private keys. The higher the value of the prime numbers used, the stronger the encryption will be. It uses the modulo operation and Euler's totient on prime numbers to develop the keys. This encryption technique requires higher processing power at both transceivers.

Advanced Encryption Standard: AES is a symmetric encryption technique that jumbles the bits in the data such that it is unreadable by a third party. It supports three key lengths: 128-bit (10 rounds of encryption), 192-bit (12 rounds of encryption), and 256-bit (14 rounds of encryption). Each round of encryption consists of SubBytes, Shiftrows, MixColumns, and Add Roundkey. In the final round of encryption, MixColumns is omitted. This encryption is easy on the processing side as compared to the RSA, thus having lesser execution time.

3. Experimental Setup

We designed and constructed the experimental setup of the FSOC system entirely in-house to test its performance under multiple environmental conditions. The experimental setup includes both hardware and software components that recreate practical optical communication channels, working under environmental factors including fog, smoke, and wind. The hardware portion includes a 635 nm red diode laser with 5.3 mW of optical power as the optical transmitter, a photodetector for the receiver, and a modular atmospheric chamber that provides the propagation path.

The software interface, developed with Python, provides a GUI for real-time control of system parameters, including baud rate, modulation type, FEC code, and encryption algorithms. Data from the transmitter computer is converted into binary format and passed through the selected encryption and encoding before being transmitted optically through the laser. The receiver demodulates the signal and decodes the message signal back to its original data. This integrated design facilitates precision in the control of environmental and system-level parameters, which promotes the assessment of the combined effect of the modulation, encoding, and encryption on signal quality and reliability in different atmospheric conditions.

3.1. Optical wireless testbed construction

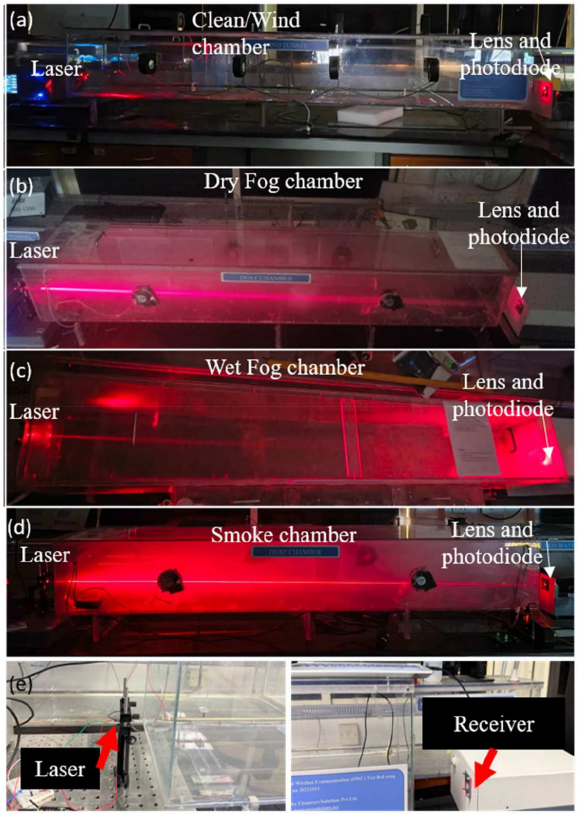
As illustrated in Figure 3, the optical wireless testbed was built to measure the performance of the FSOC system in controlled laboratory conditions to simulate atmospheric effects observed outside. The testbed consists of four transparent linear chambers, corresponding to distinct atmospheric conditions, specifically clean/wind, dry fog, wet fog, and smoke conditions.

The arrangement allows for the controlled introduction of particulates or aerosols to simulate the scattering of light and absorption that exists in nature. Fog generators were implemented to create dry and wet fogs at varying droplet densities. Smoke generators were used to generate the particulate-heavy environmental conditions. Finally, an air blower was used to introduce wind into the chamber to simulate beam wander and turbulence. The transmitter and receiver are both aligned at the opposite end of the chamber along the LOS axis to maintain maximum coupling efficiency.

On the transmitter side, the data is converted from a digital data stream to electrical signals using a USB-to-TTL converter, which is then sent to a laser driver circuit. The laser modulates according to the digital bits, remaining ON for logic "1" and OFF for logic "0." The switching speed is determined by the baud rate used for transmission. Different modulation, FEC code, and encryption are also applied.

The optical source used is a 635 nm diode laser with continuous-wave optical power output of 5.3 mW; the laser operates with a supply voltage of 3–5 V and current ~100 mA. The beam focus is adjustable using a lens ring head of the laser, which allows optimization of the beam diameter (~0.75 mm) and divergence (>0.5 mrad) in the FSO link. The receiver consists of a bi-convex lens of 1 inch diameter and 5 cm of focal length, which focuses the incident beam into commercially available silicon photodiode module operating at 5 V, having a signal processing circuitry with responsivity of 0.4–0.6 A/W for red wavelengths and a typical switching speed with rise time and fall time ranging from 0.05 µs to 9 µs, which converts the optical signal into electrical data, which is then decoded and decrypted using the receiver software. The modularity of this testbed allows for a flexible testing approach and repeatability of measurements in controlled, defined environmental scenarios.

Figure 3
Experimental setup FSOC testbed showing (a) clean/wind chamber, (b) dry fog chamber, (c) wet fog chamber, (d) smoke chamber, and (e) laser and receiver section of the FSOC communication setup



3.2. Characterization of testbed for various atmospheric conditions

To evaluate typical transmission quality and optical losses due to each environmental condition, the testbed was experimentally evaluated in terms of attenuation (A), using the standard logarithmic power-loss relation:

$$A = -10\log_{10}\left(\frac{P_r}{P_t}\right)$$

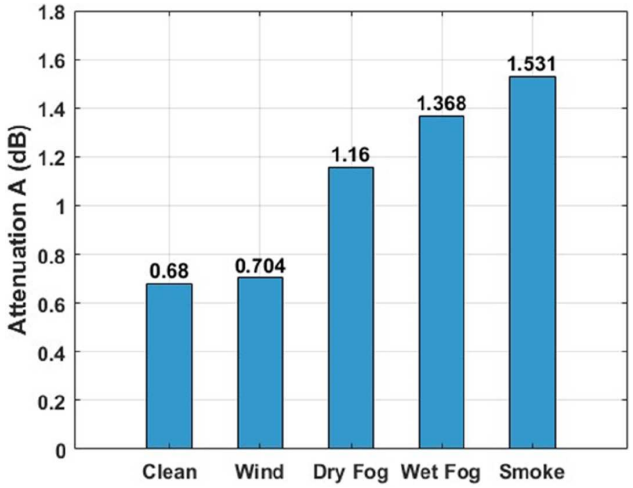
here
P_r = received power
P_t = transmitted power

This equation measures the optical signal attenuation in decibels (dB) while traveling through the atmospheric medium, imparting optical losses. For the clean chamber, the transmitted power P_t = 5.3 mW and the received power P_r = 4.53 mW. Substituting these values into the formula gives:

$$A = -10\log_{10}\left(\frac{4.53}{5.3}\right) = -10\log_{10}(0.8547) = 0.68\ \text{dB}$$

Similarly, we measured attenuation values for the atmospheric medium under each condition, which can be found in Figure 4. The clean and wind chambers exhibit the lowest

Figure 4
Attenuation for adverse atmospheric conditions



attenuation at 0.68 dB and 0.704 dB, respectively, due to low scattering or absorption phenomena. In the dry fog, the attenuation was 1.16 dB, associated with scattering of smaller water droplets. The wet fog also showed some degradation at 1.368 dB of attenuation due to larger droplet size and increased density, resulting in increased Mie scattering. Finally, the smoke chamber had the highest overall attenuation at 1.531 dB, due to absorption and multiple scattering from the fine carbonaceous particles.

These findings substantiate a definitive link between medium density and optical signal quality degradation, congruent with theoretical atmospheric attenuation models. This type of empirical characterization creates a departure point for assessing the robustness of systems and data integrity under variable channel conditions for secure FSOC links.

4. Results and Discussions

4.1. Feasibility studies on the implementation of various encryption, encoders, and modulation schemes in the clean chamber

After characterizing various atmospheric conditions such as wind circulation, wet fog, dry fog, and smoke conditions, we initially conducted the experiments in a clean chamber as a preliminary experiment with all modulation schemes, with two encryption schemes and three encoding schemes. We have conducted these experiments with increasing data rates and measured the total time of data transfer that includes file encryption/encoding, electrical to optical (E/O) conversion, actual transfer of optical data in an atmospheric channel (with adverse conditions), O/E conversion, and final decryption/decoding to the original form of the file. The total time is considered the execution time of a particular encryption, encoding, and modulation combination. We have used a 4 KB text file to measure this execution time and other metrics.

As described in earlier sections, we have implemented OOK (NRZ and RZ), PPM, DPIM, and DHPIM modulation schemes, RSA and AES encryption, and Repeat, BCH, and RSC error correction schemes and measured the execution time. Figure 5 shows the graphs of all these measurements. Figure 5(a) shows all five modulation schemes with RSA and AES encryptions. We have used RSA with a nominal encryption strength of (47,53) and 128-bit AES encryption with all the modulation schemes. It is noted that while OOK offers the lowest execution time with both encryptions, the DHPIM and RZ schemes are the second lowest. The DHPIM, being a differential scheme, matches the time scale of RZ followed by DPIM. PPM takes the largest execution time, even with encryption schemes. Comparing the RSA and AES schemes for a given modulation scheme, AES takes almost the same time as that of no encryption. This offers encryption with no additional delays in security. Table 2 describes the number of modulation schemes that are used with the different combinations of encryptions and encoding schemes and the metrics analyzed.

Further, we have added three FEC schemes, that is, repeat 03, BCH, and Reed–Solomon codes, along with encryption for all modulation schemes. Figures 5(b–f) show the graphs for all modulation schemes starting from OOK-NRZ to DHPIM. It is noted that all error correction codes with AES show less execution time compared with RSA. They also follow similar trends with and without error correction addition. However, among the error correction codes, the BCH code with AES encryption shows the minimum execution times. This is followed by the repeat code and RSCs. The RSA combination has almost double the execution times for all modulation schemes except the PPM modulation scheme.

4.2. Atmospheric channel studies (wind, smoke, dry fog, and wet fog)

Four different adverse atmospheric channel conditions were created with cross-wind circulation, dry fog, wet fog, and smoke conditions and measured for the performance of FSOC in terms of execution time. Figure 6 presents the data of RSA and AES encryptions with BCH, Repeat 5, and Reed–Solomon encoding schemes in the four different atmospheric conditions for the OOK-NRZ modulation scheme. This data can be directly compared with the clean chamber data shown in Figure 5(b). Even though the trends seem to be similar to the clean chamber, there is a fluctuation in the execution time with the increase in the attenuation strength. The smoke chamber has higher attenuation (refer to Figure 4) and shows clear fluctuation in execution time, as shown in Figure 6(d). However, AES encryption took smaller execution times for all encoding schemes compared to RSA. Among the encoding schemes, the BCH had the shortest execution time, and Reed–Solomon had the highest execution time, as seen from Figure 6.

4.3. Performance evaluation with different encoders and encryptions

Another important metric used to evaluate link performance is the error fraction of the data transferred. As mentioned earlier, we have used a 4 KB text file for all the measurements. The execution time data mimicking the clear weather condition was measured using a clean chamber, and then the wind circulation was turned on with cross-wind speed (20 m/s), moderate wet fog, dry fog, and smoke conditions. The received data under these conditions for every modulation scheme, encryption, and encoding configuration was saved to analyze the error fraction by comparing with the original sent data, and the error fraction was estimated for every data rate.

Initially, we have recoded data for all modulation formats in the clean chamber, with RSA and AES encryptions.

Figure 5
Execution time versus data rates for (a) all modulation rates with AES and RSA encryption. Error correction and encryption for (b) OOK-NRZ, (c) OOK-RZ, (d) DHPIM, (e) DPIM, and (f) PPM modulation schemes

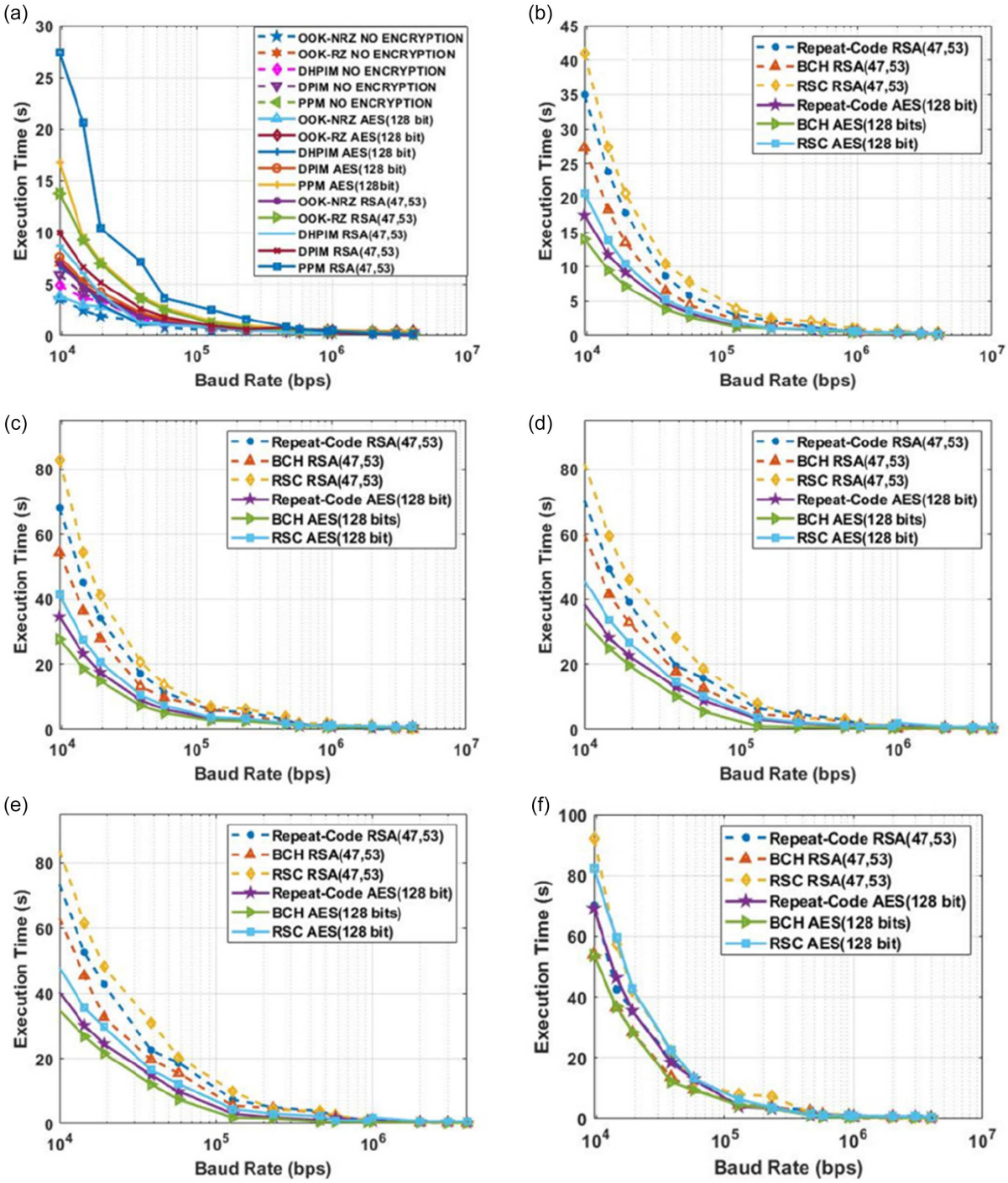


Table 2
The experimental combinations of modulation, encoding, and encryption schemes

Sl. No	Modulation schemes	Forward error correction codes	Encryption codes	Adverse atmospheric conditions	Metrics analyzed
1	OOK-NRZ	• Repeat 5 code	• w/o encryption	• Clear	• Execution time
2	OOK-RZ	• BCH code	• AES encryption	• Wind	• Error Fraction
3	PPM	• RS code	• RSA encryption	• Dry Fog	• File size
4	DPIM			• Wet Fog	
5	DHPIM			• Wet Fog	

Figure 6
Execution time versus data rates for OOK-NRZ in (a) wind chamber, (b) dry fog chamber, (c) wet fog chamber, and (d) smoke chamber

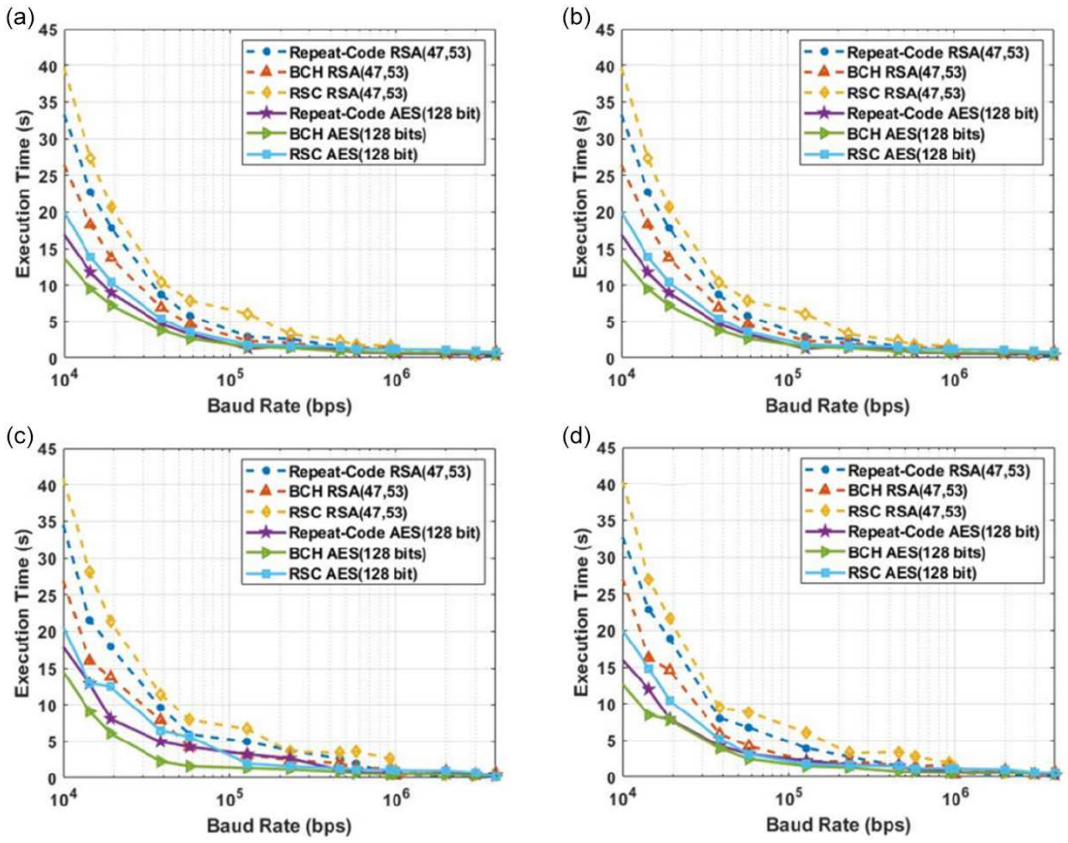


Figure 7(a) shows the error fraction versus data rate of all modulation schemes. Broadly, there are two categories of modulations, that is, basic OOK schemes (NRZ and RZ) and pulse modulation schemes (PPM, DPIM, DHPIM). There are different ways of error occurrences for these two categories. For NRZ and RZ, it is a bit "1" wrongly read as bit "0" or vice versa, often known as an erasure error. For the pulse modulation schemes, two more possibilities, that is, wrong slot error and false alarm error, are added to the total symbol error. From Figure 7(a), it is evident that the pulse modulation schemes have an onset of error at lower data rates (125 kbps) compared to the OOK modulation formats (576 kbps). Further, RSA encryption with pulse modulation schemes shows an even earlier onset of error occurrence due to the encryption complexity and the total symbol error.

Further, we have implemented error correction codes on all the modulation formats along with encryptions under clear conditions. Figure 7(b–f) shows the graphs of error fraction versus data rate for all three error correction codes along with encryption. It can be clearly seen that the AES encryption with all error correction codes has a higher onset of error at 125 kbps and above. Among the error correction codes for AES encryption, it is the RSC that has offered a higher onset and varies with the modulation scheme. The OOK-NRZ, OOK-RZ, and DHPIM modulation formats are better compared to the DPIM and PPM schemes. It should be noted that the BCH code was efficient in the execution time; however, the error fraction data shows that the RSC offered the least error with the better link performance. Figure 8(a) shows that file size increases with different modulation schemes when encryption is applied, with RSA giving the highest overhead compared to AES and no encryption. Figure 8(b) shows a similar trend for FEC techniques, where more advanced error correction methods such as RSC increase size due to added redundancy. Encryption and FEC improve reliability and security but at the cost of increased data size.

Figure 7
Error fraction versus data rates for (a) all modulation rates with AES and RSA encryption. Error correction and encryption for (b) OOK-NRZ, (c) OOK-RZ, (d) DHPIM, (e) DPIM, and (f) PPM modulation schemes

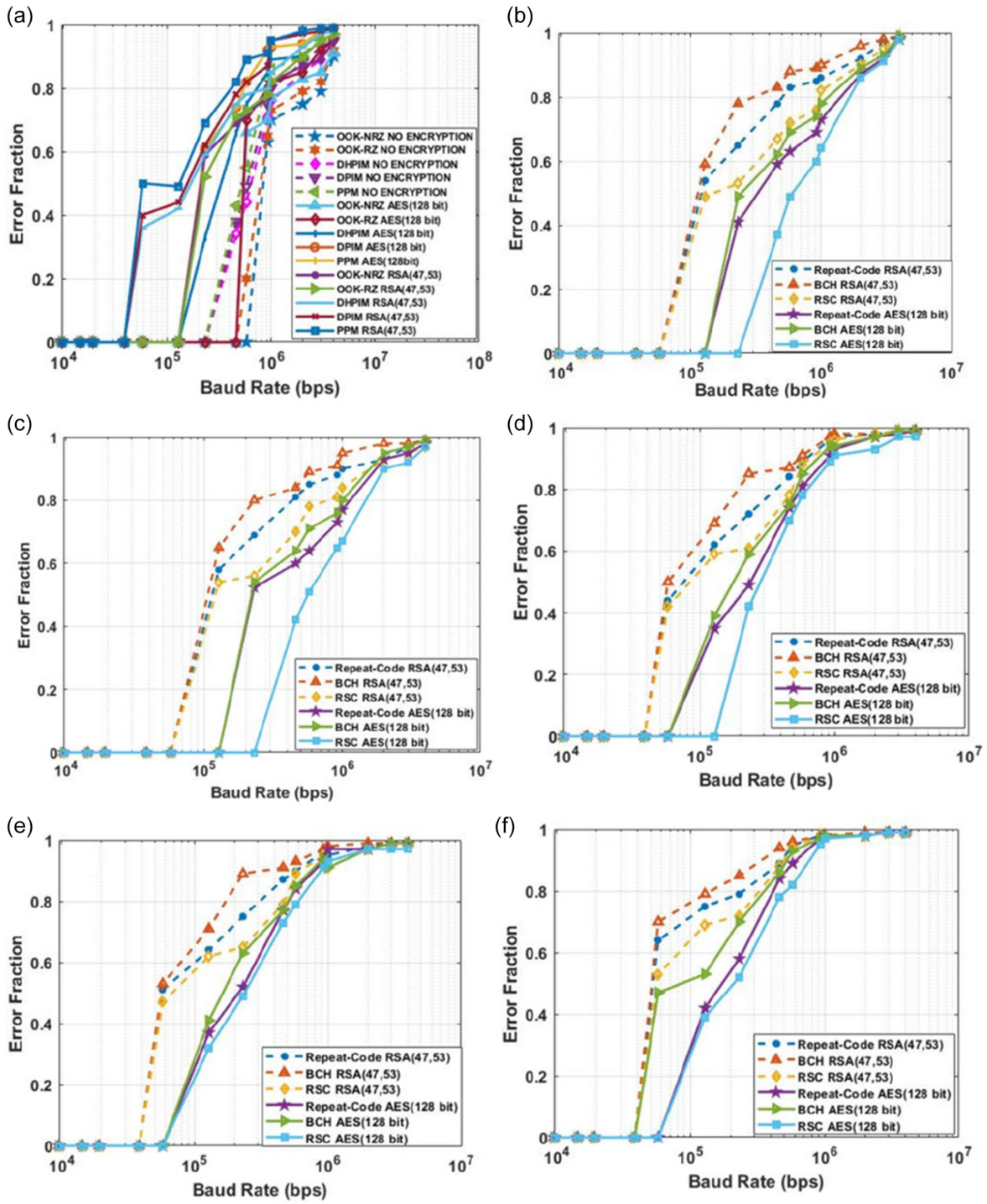


Figure 8
Variation of transmitted file size with and without encryption techniques for different (a) modulation techniques without encoding and (b) different encoding techniques for OOK-NRZ modulation

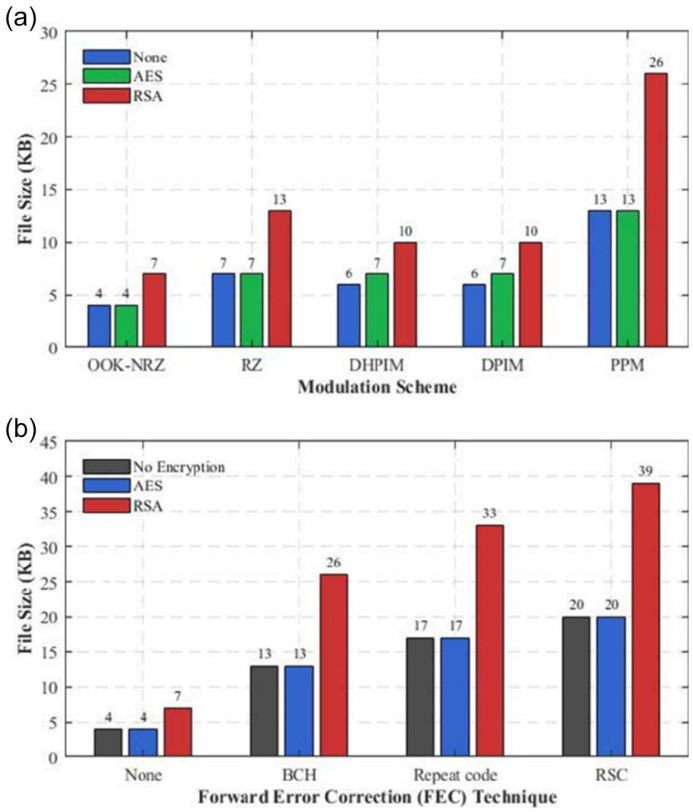


Figure 9
Error fraction versus data rates for OOK-NRZ in (a) wind chamber, (b) dry fog chamber, (c) wet fog chamber, and (d) smoke chamber

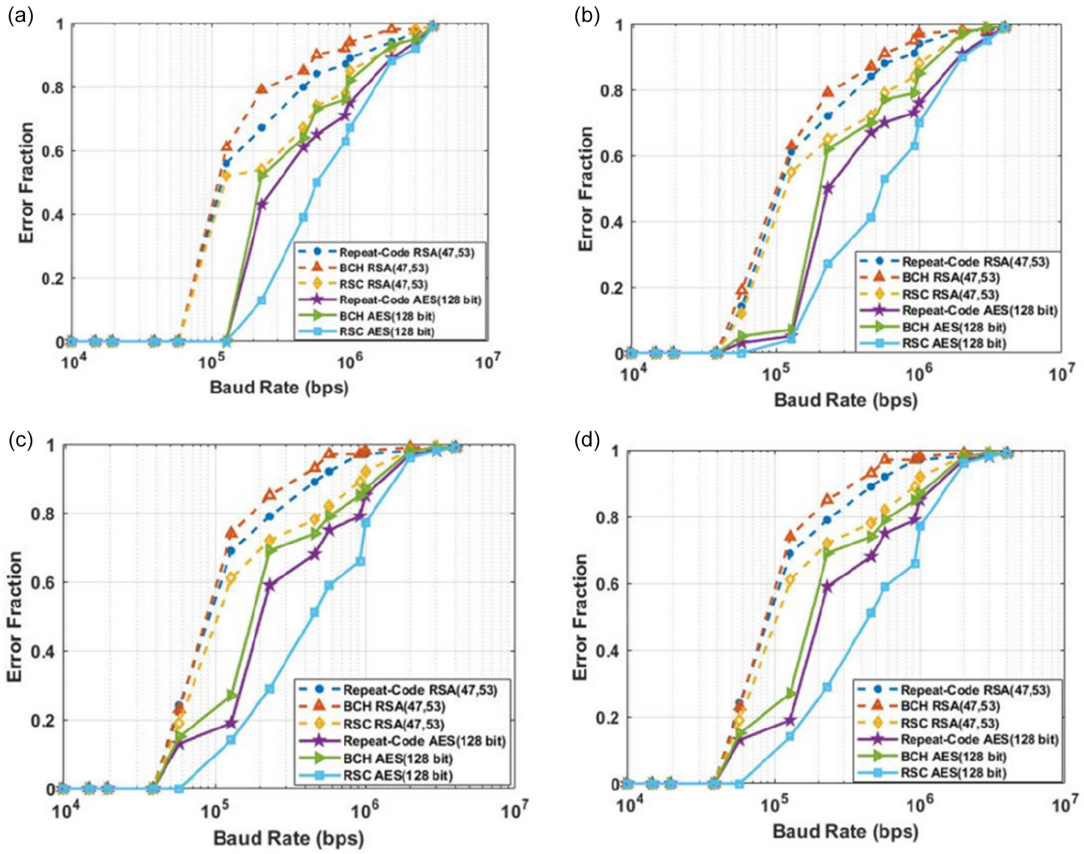
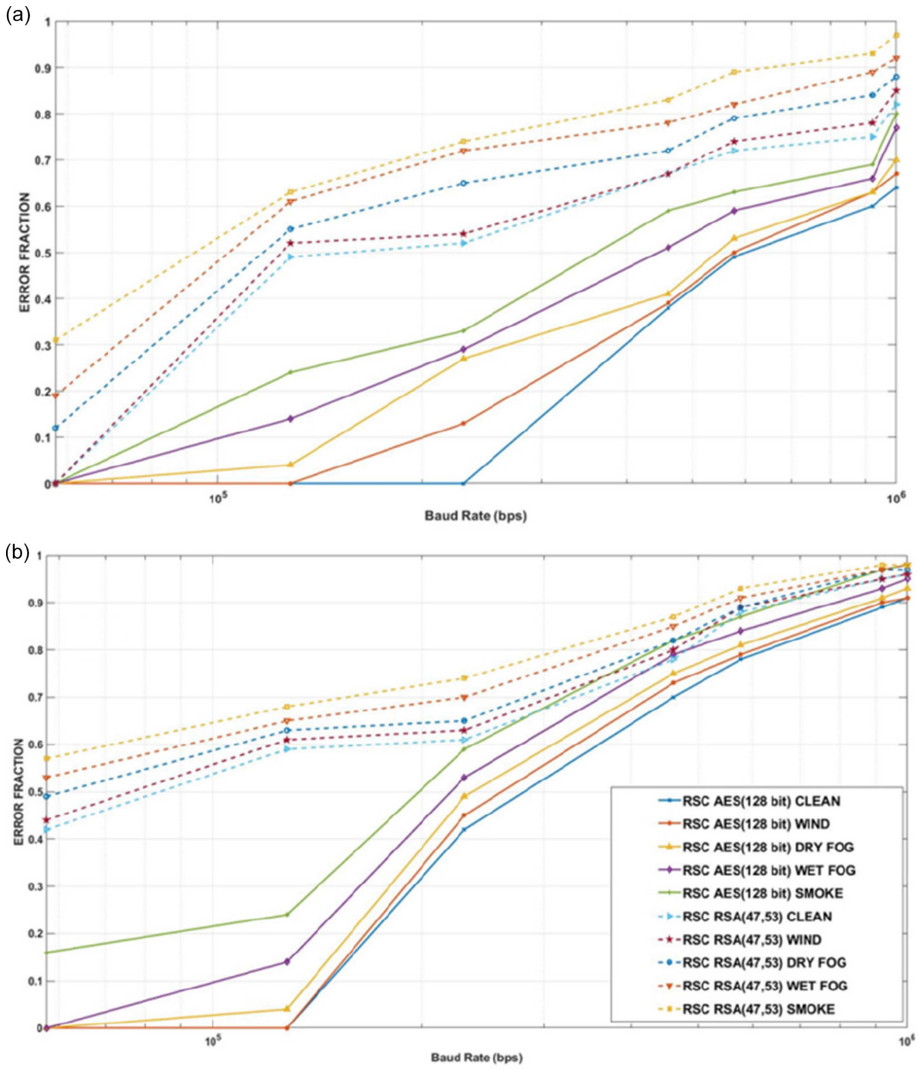


Figure 10
Error fraction vs baud rate with AES and RSA encryption for different chambers using (a) OOK-NRZ and (b) DHPIM modulation



4.4. Atmospheric effects on link performance

Similar to the execution time measurements in various atmospheric channel conditions, we have performed the Error fraction measurements for the OOK modulation scheme with both encryptions and the error correction codes in the wind channel, dry fog, wet fog, and the smoke conditions. The results were presented in Figure 9. Figure 9(a) shows data for cross-wind conditions (20 m/s). Figure 9(b) shows that, compared to the clean chamber error fraction data, the atmospheric conditions had altered the error fraction based on the channel conditions. These distortions occurred mostly between the 50 kbps and 1 Mbps data rates and are clearly evident from the graphs. Another important point to be noted is that the onset of the error occurrence had clearly started earlier for dry fog, wet fog, and smoke, which explicitly shows the adverse condition effect. Here also, the trends suggest that the RSC is better compared to other error correction schemes with the AES encryption.

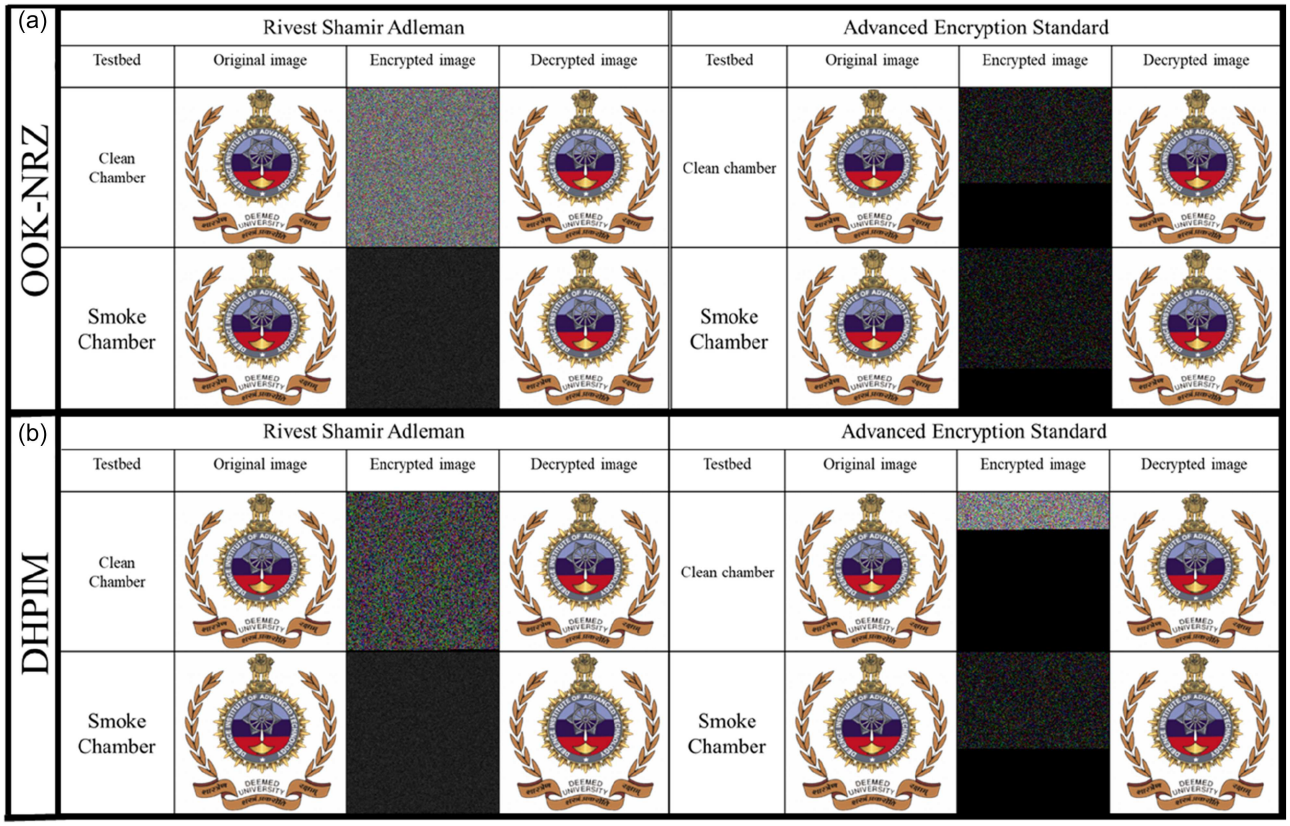
To gain a more explicit understanding of the data and the effects of modulation schemes and channel conditions, experiments were conducted for the OOK and DHPIM modulation schemes, and the error fraction was calculated across data rate ranges from 50 kbps to 1 Mbps. Figure 10(a) and (b) shows data for OOK and DHPIM modulation schemes. Figure 10(a) shows that the OOK scheme with AES encryption has an onset of error at 50kbps for all atmospheric conditions; however, the dry for is always 10–20% higher than the clean/wind chamber data. For the RSA scheme, it shoots to almost a 40–50% error rate and slowly increases further. In DHPIM modulation schemes, which is the most complex modulation scheme, also had similar trends, but the onset of error occurs even at early data rates for dry fog conditions. Table 3 provides the onset of errors in each condition for OOK-NRZ modulation.

Figure 11 shows the image transmission at different stages, that is, original image and received image with and without encryption in two different FSOC channels (clean and smoke) for two different modulations (OOK-NRZ and DHPIM) and two different encryption schemes (RSA and AES). This is transmitted at a data rate of 128 kbps**.** We can notice that there is a difference in the encrypted image clearly from the clean channel to an

Table 3
Baud rates for all conditions where the error starts in OOK-NRZ modulation

		Onset of error	
Chamber	Error Correction Code	RSA(kbps)	AES(kbps)
Clean	Repeat Code	128	230
	BCH	128	230
	RSC	128	460
Wind	Repeat code	128	230
	BCH	128	230
	RSC	128	230
Dry fog	Repeat Code	57.6	57.6
	BCH	57.6	57.6
	RSC	57.6	128
Wet fog	Repeat Code	57.6	57.6
	BCH	57.6	57.6
	RSC	57.6	128
Smoke	Repeat Code	57.6	57.6
	BCH	57.6	57.6
	RSC	57.6	128

Figure 11
Visual representation of the encryption strength of RSA and AES for (a) OOK-NRZ and (b) DHPIM



adverse atmospheric condition. However, the decrypted image is the same. This is due to the lower or error-free data rates. This offers additional security to the FSOC system.

5. Conclusions and Future Perspectives

In summary, we have presented a combination of encryption and encoding schemes implemented along with different modulation schemes from a single GUI operation. Further, we have investigated the adverse atmospheric channel effects by simulating the four different possible scenarios, such as cross-winds, dry fog, wet fog, and smoke conditions. The attenuation coefficients were measured for these simulated conditions. Further, we measured the execution times and error fractions with different configurations and in different adverse atmospheric channels. Results suggest that OOK-NRZ (basic modulation scheme) works better in all weather conditions. In the differential modulation schemes, the DHPIM works better, and the results can be compared with the OOK-RZ scheme. PPM is inefficient due to redundant space. Among the three error correction codes implemented, the RSC offers the least error fraction, and in encryption schemes, AES has an advantage as it does not increase data size for encryption.

This paper proposes various possibilities that can be integrated in FSOC, and of course, many such configurations can be added as per the requirements of the industry and defense to enhance security with high data rates. The study also proposes to have a versatile approach with combinational schemes that can offer data security and feasibility of communication as per the adverse channel conditions. Further investigations, in a similar line, can make the FSOC an alternative for traditional RF communications, and the same can be further extended to all branches of Optical Wireless Communication (OWC), such as Underwater Wireless Optical Communication (UWOC), VLC, etc. This should be incorporated in a real-time working system and investigate the on-field atmospheric effects for a reliable FSOC system. The advantage of such systems is that the user-defined choice of data rate, modulation, encryption, and error correction can make them operationally friendly. This can be further integrated with spatial diversity techniques to further improve the performance and to create an FSO network.

Acknowledgments

All authors acknowledge IIT Guwahati Technology Innovation and Development Foundation and Defence Institute of Advanced Technology for financial and infrastructural support.

Funding Support

This work has been supported financially by Technology Innovation Hub—IIT Guwahati (TIH-IITG) under Grant Number TIH/TD/0408 and Defence Institute of Advanced Technology (DIAT), Pune.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Shashank Shekhar: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Visualization. **Dhanush Devappa B C:** Methodology, Software, Data curation, Writing – original draft. **Moksh Chandrakar:** Investigation. **Appala Venkata Ramana Murthy:** Resources, Writing – original draft, Supervision, Project administration, Funding acquisition.

References

[1] Kaur, S., Kaur, J., & Sharma, A. (2023). Predicting the performance of radio over free space optics system using machine learning techniques. *Optik*, *281*, 170798. https://doi.org/10.1016/j.ijleo.2023.170798

[2] Dong, Y., Hassan, M. Z., Cheng, J., Hossain, M. J., & Leung, V. C. (2018). An edge computing empowered radio access network with UAV-mounted FSO fronthaul and backhaul: Key challenges and approaches. *IEEE Wireless Communications*, *25*(3), 154–160. https://doi.org/10.1109/MWC.2018.1700419

[3] Ghassemlooy, Z., Khalighi, M.-A., Zvanovec, S., Stevens, N., Alves, L. N., Shrestha, A., . . . , & Amay, M. (2024). *Final white paper*. *NEWFOCUS CA19111 COST Action: European network on future generation optical wireless communication technologies [Report]*. https://hal.science/hal-04671609v1/document

[4] Chen, J., Gutema, T. Z., & Popoola, W. O. (2025). Modeling, design and implementation of beam tracking for misalignment mitigation in optical wireless communications. *IEEE Open Journal of the Communications Society*, *6*, 9090–9099. https://doi.org/10.1109/OJCOMS.2025.3624621

[5] Guan, M., Liu, Y., Wang, H., Xiao, H., Lu, H., Zhang, H., . . . , & Zhang, Z. (2025). High-performance 100 Gbps free-space optical communication via optical pin beam receiver. *Communications Engineering*, *4*(1), 203. https://doi.org/10.1038/s44172-025-00536-w

[6] Sun, N., Wang, Y., Zhu, H., Zhang, J., Du, A., Wang, W., . . . , & Liu, J. (2022). Self-alignment FSOC system with miniaturized structure for small mobile platform. *IEEE Photonics Journal*, *14*(6), 1–6. https://doi.org/10.1109/JPHOT.2022.3193112

[7] Liu, N., Ju, C., Wang, D., Zhang, X., & Li, C. (2023). Carrier recovery for satellite-to-ground coherent laser communication systems using double feedback loop and Viterbi–Viterbi feedforward cascade structure. *Optics Communications*, *534*, 129312. https://doi.org/10.1016/j.optcom.2023.129312

[8] Saeed, N., Almorad, H., Dahrouj, H., Al-Naffouri, T. Y., Shamma, J. S., & Alouini, M.-S. (2021). Point-to-point communication in integrated satellite-aerial 6G networks: State-of-the-art and future challenges. *IEEE Open Journal of the Communications Society*, *2*, 1505–1525. https://doi.org/10.1109/OJCOMS.2021.3093110

[9] Geldard, C. T., Thompson, J. S., & Popoola, W. O. (2024). On the relative effect of underwater optical turbulence in different channel conditions. *IEEE Access*, *12*, 11104–11113. https://doi.org/10.1109/ACCESS.2024.3352914

[10] Wang, Z., Dedo, M. I., Guo, K., Zhou, K., Shen, F., Sun, Y., . . . , & Guo, Z. (2019). Efficient recognition of the propagated orbital angular momentum modes in turbulences with the convolutional neural network. *IEEE Photonics Journal*, *11*(3), 1–14. https://doi.org/10.1109/JPHOT.2019.2916207

[11] Elsayed, E. E. (2026). Investigations on modified OOK and adaptive threshold for wavelength division multiplexing free-space optical systems impaired by interchannel crosstalk, atmospheric turbulence, and ASE noise. *Journal of Optics*, *55*(1), 493–506. https://doi.org/10.1007/s12596-024-01929-4

[12] Singh, H., Mittal, N., & Singh, H. (2022). Evaluating the performance of free space optical communication (FSOC) system under tropical weather conditions in India. *International Journal of Communication Systems*, *35*(18), e5347. https://doi.org/10.1002/dac.5347

[13] Yu, N., Wang, P., & Zhuang, Z. (2021). Design of digital pulse-position modulation system. *Journal of Physics: Conference Series*, *2093*(1), 012030. https://doi.org/10.1088/1742-6596/2093/1/012030

[14] Dwivedy, P., Dixit, V., & Kumar, A. (2023). Cooperative VLC system using OOK modulation with imperfect CSI. *Physica Scripta*, *98*(2), 025509. https://doi.org/10.1088/1402-4896/acb095

[15] Song, Y., Lu, W., Sun, B., Hong, Y., Qu, F., Han, J., . . . , & Xu, J. (2017). Experimental demonstration of MIMO-OFDM underwater wireless optical communication. *Optics Communications*, *403*, 205–210. https://doi.org/10.1016/j.optcom.2017.07.051

[16] Devappa, B. C. D., Pawar, K., Jain, S., Narayanan, S. L. S., Mahale, K. P., & Murthy, A. V. R. (2025). Practical implementation and performance evaluation of different modulation and forward error correction techniques in underwater optical communication testbed. *Journal of Optics. Advance online publication*. https://doi.org/10.1007/s12596-025-02847-9

[17] Cheng, Q., Cui, S., Zhou, K., & Liu, D. (2020). Training-aided joint frame and frequency synchronization for free space optical communication signals with low OSNR. *Optics Communications*, *473*, 126046. https://doi.org/10.1016/j.optcom.2020.126046

[18] Sahoo, A., Mohanty, P., & Sethi, P. C. (2022). Image encryption using RSA algorithm. In *Intelligent Systems: Proceedings of ICMIB 2021*, 641–652. https://doi.org/10.1007/978-981-19-0901-6_56

[19] Al Mamun, S., Mahmood, M. A., & Amin, M. A. (2021). Ensuring security of encrypted information by hybrid AES and RSA algorithm with third-party confirmation. In *2021 5th International Conference on Intelligent Computing and Control Systems*, 337–343. https://doi.org/10.1109/ICICCS51141.2021.9432174

[20] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

[21] Wardlaw, W. P. (2000). The RSA public key cryptosystem. In D. Joyner (Ed.), *Coding theory and cryptography: From enigma and geheimschreiber to quantum theory (pp* (pp. 101–123). Springer. https://doi.org/10.1007/978-3-642-59663-6_6

[22] Kuo, H., & Verbauwhede, I. (2001). Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm. In *Cryptographic Hardware and Embedded Systems - CHES 2001: Third International Workshop* (pp. 51–64). https://doi.org/10.1007/3-540-44709-1_6

[23] Somani, U., Lakhani, K., & Mundra, M. (2010). Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In *2010 First International Conference on Parallel, Distributed and Grid Computing*, 211–216. https://doi.org/10.1109/PDGC.2010.5679895

[24] Khatarkar, S., & Kamble, R. (2015). A survey and performance analysis of various RSA based encryption techniques. *International Journal of Computer Applications*, *114*(7), 30–33. https://doi.org/10.5120/19993-1736

[25] El-Malek, Abd., H, A., Salhab, A. M., Zummo, S. A., & Alouini, M.-S. (2016). Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling. *IEEE Transactions on Wireless Communications*, *15*(9), 5904–5918. https://doi.org/10.1109/TWC.2016.2572681

[26] Mostafa, A. (2017). *Physical-layer security for visible-light communication systems*. *PhD Thesis*. The University of British Columbia. https://doi.org/10.14288/1.0345607

[27] El-Malek, Abd., H, A., Salhab, A. M., Zummo, S. A., & Alouini, M.-S. (2017). Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference. In *2017 IEEE Wireless Communications and Networking Conference*, 1–6. https://doi.org/10.1109/WCNC.2017.7925690

[28] Blinowski, G., Januszewski, P., Stepniak, G., & Szczypiorski, K. (2018). LuxSteg: First practical implementation of steganography in VLC. *IEEE Access*, *6*, 74366–74375. https://doi.org/10.1109/ACCESS.2018.2883250

[29] Ai, Y., Mathur, A., Cheffena, M., Bhatnagar, M. R., & Lei, H. (2019). Physical layer security of hybrid satellite-FSO cooperative systems. *IEEE Photonics Journal*, *11*(1), 1–14. https://doi.org/10.1109/JPHOT.2019.2892618

[30] Yesilkaya, A., Cogalan, T., Erkucuk, S., Sadi, Y., Panayirci, E., Haas, H., & Poor, H. V. (2020). Physical-layer security in visible light communications. In *2020 2nd 6G Wireless Summit* (pp. 1–5). https://doi.org/10.1109/6GSUMMIT49458.2020.9083799

[31] Banerjee, S., & Murthy, A. V. R. (2021). Simulation of a secure optical communication system using different optical modulation schemes coupled with Rivest-Shamir-Adleman algorithm. In *2021 Asian Conference on Innovation in Technology*, 1–5. https://doi.org/10.1109/ASIANCON51346.2021.9544853

[32] Kim, S.-J., & Han, S.-K. (2022). Estimation and performance analysis of multiple incident beam misalignment in spatial diversity based FSO transmissions. *Optics Communications*, *521*, 128618. https://doi.org/10.1016/j.optcom.2022.128618

[33] D, B. C. D., Kashyap, C., Jain, S., Banerjee, S., & Murthy, A. V. R. (2025). Performance analysis of RSA encrypted secure free-space optical communication link under adverse atmospheric conditions implemented on a testbed. *Journal of Optics and Photonics Research. Advance online publication*. https://doi.org/10.47852/BONVIEWJOPR52026038

[34] Joseph, C., Raj, A. A. B., & Kumar, E. S. V. (2025). Security enhancement in mission-critical free-space optical communication using AES-128 encryption algorithm. In *2025 IEEE Space, Aerospace and Defence Conference*, 1–6. https://doi.org/10.1109/SPACE65882.2025.11170517

[35] Darwesh, L., & Kopeika, N. S. (2020). Deep learning for improving performance of OOK modulation over FSO turbulent channels. *IEEE Access*, *8*, 155275–155284. https://doi.org/10.1109/ACCESS.2020.3019113

[36] Dixit, V., & Kumar, A. (2021). Performance analysis of L-PPM modulated NLOS-VLC system with perfect and imperfect CSI. *Journal of Optics*, *23*(1), 015702. https://doi.org/10.1088/2040-8986/abcea8

[37] Ma, J., Jiang, Y., Yu, S., Tan, L., & Du, W. (2010). Packet error rate analysis of OOK, DPIM and PPM modulation schemes for ground-to-satellite optical communications. *Optics Communications*, *283*(2), 237–242. https://doi.org/10.1016/j.optcom.2009.10.007

[38] Tao, M., Guan, J., Peng, T., Li, S., Yu, S., Song, J., …, & Gao, F. (2021). Simultaneous realization of laser ranging and communication based on dual-pulse interval modulation. *IEEE Transactions on Instrumentation and Measurement*, *70*, 2004610. https://doi.org/10.1109/TIM.2021.3082990

[39] Salman, M., Bolboli, J., & Chung, W.-Y. (2022). Experimental demonstration and evaluation of BCH-coded UWOC link for power-efficient underwater sensor nodes. *IEEE Access*, *10*, 72211–72226. https://doi.org/10.1109/ACCESS.2022.3188247

[40] Reed, I. S., & Solomon, G. (1960). Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, *8*(2), 300–304. https://doi.org/10.1137/0108018 [40]

How to Cite: Shekhar, S., B C, D. D., Chandrakar, M., & Murthy, A. V. R. (2026). Performance of Encoding, Encryption, and Modulation Schemes in Free-Space Optical Communication Evaluated on the Atmospheric Testbed. *Journal of Optics and Photonics Research*. https://doi.org/10.47852/bonviewJOPR62027992