Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

SCIFINITI PUBLISHING

OPEN ACCESS

Research Article

Integrating Rivest–Shamir–Adleman (RSA) Encryption and Forward Error Correction (FEC) Codes for Secure and Robust Underwater Optical Wireless Communication

Kalyani Pawar, Dhanush Devappa B C, Soumit Banerjee, Appala Ventaka Ramana Murthy*

Department of Applied Physics, Defence Institute of Advanced Technology, Pune, India

Kalyani Pawar (email: kalyani_jap23@diat.ac.in)

(ORCID: 0009-0000-7498-9120)

Dhanush Devappa B C (email: dhanush.pap24@diat.ac.in)

(ORCID: 0009-0008-6304-8606)

Soumit Banerjee (email: soumitbanerjee06@gmail.com)

(ORCID:0000-0002-1400-3187)

*Corresponding Author: Appala Ventaka Ramana Murthy (email: avrmurthy@diat.ac.in)

(ORCID: 0000-0003-4875-9991)

Abstract

Underwater Optical Wireless Communication (UOWC) offers a potential alternative to traditional Radio Frequency (RF) and acoustic methods, which suffer from low speed, short range, and high latency in underwater conditions. Reliability and security are both impacted by signal deterioration brought on by turbidity, scattering, and absorption, which is still a concern in UOWC. This study

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

investigates a key for a UOWC system by combining different modulation formats and Forward Error Correction (FEC) codes with Rivest-Shamir-Adleman (RSA) encryption and tested on a 4m in-house underwater channel. While FEC codes aid in reducing bit errors brought on by the underwater channel, RSA encryption provides additional security for data by preventing eavesdropping. The information is encrypted initially and is then sent to undergo modulation and Forward Error Corrections if needed. The experimental studies of execution size for modulation schemes and FEC were in line with the theoretical value, repeat code (3) file size was thrice the original, repeat code (5) increased the file size by 5 times, OOK-RZ had twice the file size has OOK-NRZ, and PPM file size was 16 times, and so on. Among the various FEC codes and the modulation schemes employed, the results show that using Hamming, Bose–Chaudhuri–Hocquenghem (BCH), and Reed-Solomon codes improves stability and security by almost 1.5 times than that of no FEC when integrated with PPM and DPIM modulation schemes. This approach offers a promising solution for applications in underwater robotics, environmental monitoring, and defence, demonstrating the potential of UOWC as a secure communication system for challenging and dynamic underwater conditions.

Keywords— Underwater Optical Wireless communication, Underwater Testbed, Modulation Techniques, Forward Error Correction Code, Link Performance.

1. Introduction

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

Underwater operations, from scientific exploration to naval defence, increasingly demand high-speed, low-latency communication systems. Conventional acoustic and radio frequency systems struggle in aquatic environments. Acoustic signals, despite their range, suffer from low bandwidth and susceptibility to noise, while RF signals attenuate rapidly in seawater [1–4]. Underwater Optical Wireless Communication (UOWC) offers a promising alternative, using blue-green light to achieve high data rates over short to moderate distances. The optical source at the transmitter end modulates the light as per the input data and transmits through the underwater medium. The received signal demodulates the light signal back to the information. The complete UOWC system can be used for several potential applications in underwater surveillance, underwater sensor networks, submarine-to-submarine/Unmanned Underwater Vehicles (UUVs) [5–7].

UOWC, however, faces significant hurdles in the ocean's complex environment. Signal attenuation, scattering by suspended particulates, and variations in salinity and turbidity degrade performance, leading to high bit error rates (BER) and unreliable links, especially in turbulent conditions like turbid harbours [8–10]. The major challenge in UOWC is to overcome the channel effects, which are uncontrolled [11–13]. The only solution is to implement the different modulation and encoding schemes that make the communication turbulence resistant and ensure the optimal link performance. Continuous efforts were made to improve the modulation schemes, including On-Off Keying Non-Return to Zero (OOK-NRZ), Return-to-Zero (RZ), Pulse Position Modulation (PPM), and Differential Pulse Interval Modulation (DPIM), and other modulation schemes which balance complexity, noise resilience, and bandwidth efficiency [14–21]. Kaushal et al. [1], Jain et al. [17], and Geldard et al. [16] have shown how modulation choices critically affect system performance across diverse seawater conditions.

In addition to the modulation schemes, which can ensure the energy and bandwidth efficiency, the encoding techniques (also called error correction codes) ensure the reliability of the link. Out of the two kinds of error correction codes (forward and backward), the Forward Error Correction (FEC) codes have the advantage of instantaneous implementation along with the

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

modulation scheme. There are several types of FEC codes, among which a few codes, such as Repeat, Hamming, Bose–Chaudhuri–Hocquenghem, and Reed-Solomon (RS) codes, are feasible to implement and allow receivers to correct transmission errors without retransmission [22,23]. Tzimpragos et al. [22] and Xu et al. [23] demonstrate that advanced FEC codes maintain stable BER in turbulent waters. Adnan et al. [24] and Ata et al. [25] further confirm FEC's effectiveness in highly turbid environments. Repeat codes are simple but less robust; while Hamming and BCH codes offer stronger correction with moderate complexity. RS codes, though computationally intensive, excel at handling burst errors in fluctuating conditions [22–28].

Recent studies have also explored convolutional coding as a robust alternative for underwater systems. Operating on streaming data, convolutional codes are ideal for low-latency, real-time applications. Yousuf et al. [29] found that convolutional codes outperform block-based codes in high-turbidity visible light communication, maintaining lower BER in dynamic conditions. Similarly, Fathurrahman et al. [30] highlighted the efficiency of soft-decision Viterbi decoding, which adapts to rapid channel variations and enhances signal integrity [30]. These results suggest that convolutional coding can complement traditional FEC in UWOC. While FEC addresses reliability, data security remains underexplored in many UWOC deployments. Sensitive applications, such as naval communications, require protection against unauthorized access. RSA encryption, a public-key algorithm based on prime factorization, ensures data confidentiality despite added processing demands [30–33].

Data security plays a very important role in modern times, as information is the major key factor in all progressions from our daily life to important decisions of a nation. Thus, there is a need for encryption techniques in communication systems to maintain privacy between the sender and the receiver. There are mainly two types of encryption techniques, Symmetric and Asymmetric[34]. In the Symmetric encryption technique same key can be used for encrypting and decrypting, whereas in the Assymetric encryption technique, two different keys are used, one for encryption and the other for decryption. RSA is an Asymmetric encryption technique as it uses a

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

public key to encrypt the data and a private key to decrypt it. The keys are created using two distinct prime numbers[35,36].

Integrating RSA with FEC enhances both security and resilience. Chaudhary et al. [9], Xu et al. [37], and Mohamed et al. [38] underscore the importance of cryptographic integrity in underwater sensor networks. Afifah [39] proposed a layered approach where FEC mitigates environmental interference and RSA secures data. Concurrently, Dong et al. [40] and Zhang et al. [41] developed high-speed UWOC systems using multi-channel laser diodes and turbidity-tolerant wavelength-division multiplexing (WDM), achieving data rates exceeding 10 Gbit/s with minimal crosstalk. Jiang et al. [42] introduced deep learning-based signal detection to improve physical-layer performance, while Tang et al. [43] advanced simplified detection for coherent UWOC systems, signaling a trend toward hardware and algorithmic innovation.

This paper presents a complete end-to-end system demonstrating underwater optical wireless communication for real-time data transfer. The in-house developed system has several features to select the modulation scheme and data transfer rate of our choice, which enables the user to execute smoothly. It also has advanced features like embedding the encoding and encryption schemes, which are essential for data reliability and data security. The customized graphical user interface will allow a free choice that enables a guaranteed data transfer with minimum error fraction even in adverse conditions. We have further tested and validated the same on the 4m long underwater testbed. This paper also highlights the experimental details of building such a testbed and integrating the software and hardware. Further, we present the results obtained and analyze the link performance by various metrics like the execution time, encryption strength, data rate, data size, and error fraction for various encryption strengths, encoding schemes, and modulation formats. Figure 1 shows a model diagram of UOWC.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

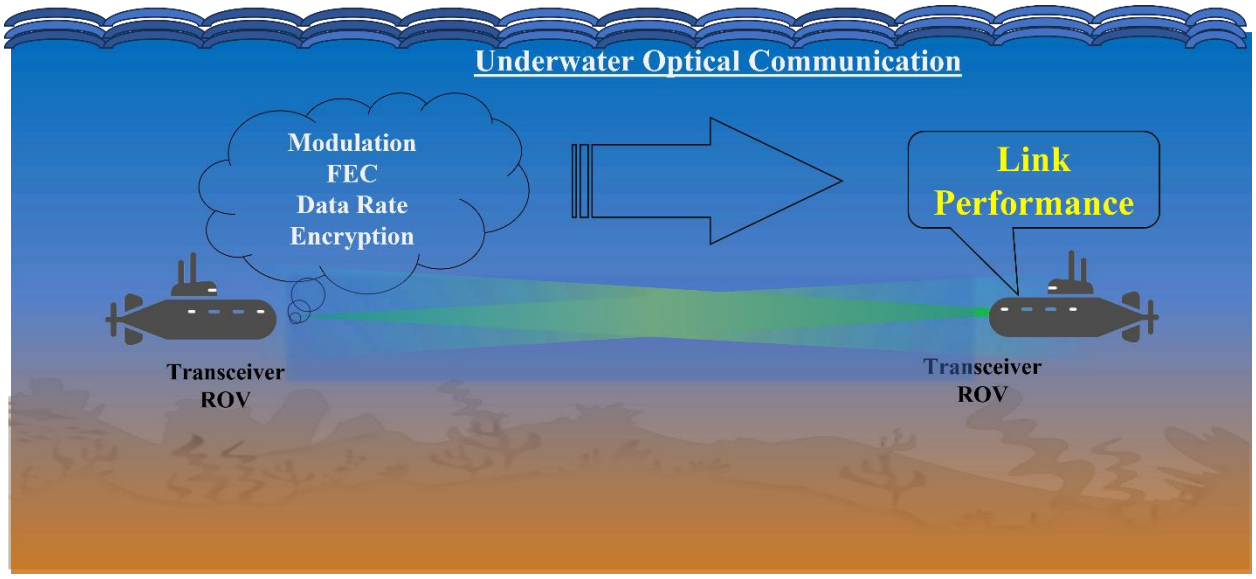

Figure 1: Showcasing a typical UOWC system between two ROVs

2. Theoretical Framework

In underwater optical wireless communication, modulation schemes and error correction codes are essential in ensuring effective, reliable data transmission. Modulation schemes such as OOK-NRZ, OOK-RZ, PPM, and DPIM each offer distinct benefits depending on the communication needs and environmental conditions. In addition to the modulation, Forward Error Correction codes help mitigate data loss by adding redundant data at the transmitter end to correct errors introduced during transmission over various channels.

2.1. Various Modulation Formats

Modulation techniques like OOK with Non-Return-to-Zero, Return-to-Zero formats, Pulse Position Modulation and Differential Pulse Interval Modulation were employed in this work. These modulation techniques offer energy efficiency, bandwidth efficiency, and transmission reliability with their own ease of implementation. The data train of symbols 8 and 1 for all four modulation schemes mentioned has been provided in Figure 2.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

On-Off Keying: OOK is the most basic modulation technique where the laser is 'on' when the bit is '1' and the laser is off when the bit is '0'. OOK can be implemented using two main types of pulse formats: Non-Return-to-Zero (NRZ) and Return-to-Zero (RZ)[44]. In NRZ, the pulse duration is the complete bit period (T_b), whereas in RZ, the pulse duration is half of the bit period.

i.e., $$\text{Slot duration, } T_s = T_b, \tag{1}$$

$$\text{Slot duration, } T_s = \frac{T_b}{2} \tag{2}$$

Pulse Position Modulation: PPM is power power-efficient modulation technique, where the information lies in the position at which the pulse is transmitted[45]. The laser 'on' period in PPM is 'T_s'.

i.e., $$\text{Slot duration, } T_s = \frac{m\,T_b}{2^m} \tag{3}$$

where 'm' is the number of bits used to describe the symbol.

Differential Pulse Interval Modulation: DPIM is both power efficient and bandwidth efficient as the redundant space is not present, i.e., the clock restarts every time a pulse is received, and the empty slots following it are removed. In PIM, the information is present in the number of empty slots between two pulses. A guard band can also be added right after the pulse to efficiently identify the slots; this is called Differential Pulse Interval Modulation 1 Guard Slot (DPIM 1GS), and if there is no guard band present, then it is called Differential Pulse Interval Modulation No Guard Slot (DPIM NGS)[46]. Since the symbol duration in DPIM is variable, the slot duration is chosen such that the mean symbol duration is equal to the time taken to send the same number of bits using a fixed frame length, like OOK and PPM[47].

i.e., $$\text{Slot duration, } T_s = \frac{T_b\, m}{\overline{L}_{DPIM}} \tag{4}$$

Where, $$\overline{L}_{DPIM} = \frac{2^m+1}{2} \text{ for DPIM(NGS)} \tag{5}$$

And $$\overline{L}_{DPIM} = \frac{2^m+3}{2} \text{ for DPIM(1GS)} \tag{6}$$

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

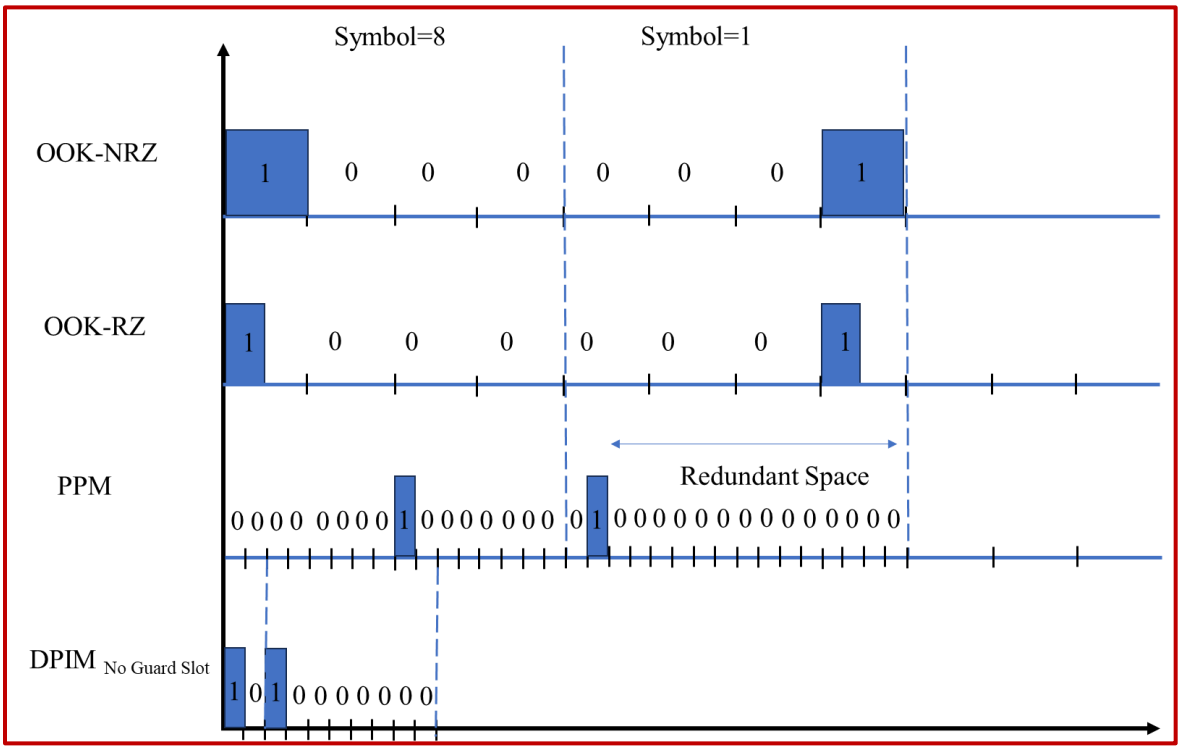

Figure 2: Data train of different modulation schemes for the symbols 8 and 1

2.2. Forward Error Correction (FEC) Codes

Comparing these formats along with the encoding techniques will provide a comparative feasibility and link performance analysis of a UOWC system[48–50]. We have employed several forward error correction codes for which a brief explanation is presented below[51].

Repeat Codes: Repeat codes, such as Repeat (3) and Repeat (5), ensure data integrity in communication systems by multiple repetition of the bits. For example, it is three times in Repeat (3), five times in Repeat (5) and n times in Repeat (n), the higher the repetitions more secure the data will be. These simple error-correction methods are effective in low-data-rate applications and work across all formats.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

In Repeat (5), the bits '1101' will be encoded as '11111111110000011111'. If the receiver receives a different bit sequence instead, i.e., one or two bits are flipped, leading to '11111101110010011111', the decoder will take the most likely bit, i.e., the bit which is repeated a greater number of times in the 5-bit duration, leading to the decoded data as '1101' which was the originally transmitted data sequence. The similar logic is applied in repeat (3) and other repeat codes.

The Hamming Code: This ensures the correction of single-bit errors by adding parity bits to the data block. Their efficiency makes them ideal for scenarios with moderate noise interference. Each block of four data bits in Hamming code is converted into a block of seven bits by adding three parity bits to the block. The purpose of these parity bits is to identify and fix transmission mistakes. Parity bits are added at 2^k (k=0,1,2,3…n) and are obtained by performing XOR operations on the data bits present in the remaining positions, the same is done in the receiver to decode and obtain the original data.

1	2	3	4	5	6	7
P1	P2	D1	P3	D2	D3	D4
x	x	1	x	0	1	1

The parity bits are calculated as follows:

P1: Bit positions 3, 5, 7 -> P1 = 0

P2: Bit positions 3, 6, 7 -> P2 = 1

P3: Bit positions 5, 6, 7 -> P3 = 0

BCH Code: BCH code is based on Galois field theory. BCH codes correct multiple random errors, making them well-suited for high bit-error-rate environments. The number of bits that can be corrected by the code depends on the size of the Galois field, which is utilized to carry out arithmetic operations in the code. Choosing a generator polynomial—a polynomial that produces a set of code words that satisfy specific error-correction properties—is a step in the development of BCH codes. The generator polynomial is built by choosing a basic Galois field component and

calculating its powers. The generator polynomial is then created by combining these powers. The data is encoded using the generator polynomial after it has been created by conducting polynomial division.

The encoded data consists of the original data and the residual bits from the division, which are a set of parity bits. The number of parity bits depends on the generating polynomial's degree. Data corruption may result from transmission errors. The receiver can spot these errors in the received data by figuring out the data syndrome. The syndrome is computed by multiplying the supplied data by the generating polynomial. If the remainder is 0, the data is error-free. If the remainder is not zero, the syndrome identifies the location of the data errors. To fix the errors, the receiver uses the error position and syndrome to solve a sequence of linear equations. These equations can be solved using matrix algebra, and the solution provides the correct values for the missing bits.

Reed-Solomon Code: RS codes encode data in multi-bit symbols, effectively handling burst errors in fluctuating water conditions. While computationally intensive, they are crucial for maintaining high data integrity in deep-sea applications. Before transmission, redundant symbols are added to the original message; these redundant symbols are calculated utilizing finite field-based mathematical techniques. The desired level of error correction and the design of the code both affect how many redundant symbols are used.

By selecting a finite field and defining a generator polynomial, a Reed-Solomon code is constructed. With ‘n’ representing the number of redundant symbols, the generator polynomial has the degree ‘n’. The generator polynomial is used to generate a set of code words that satisfy particular error-correction requirements. Throughout the encoding process, the message is separated into blocks of ‘k’ symbols, where ‘k’ is the total number of information symbols. The encoder uses the generating polynomial to calculate ‘n’ redundant symbols, which are then appended to the original message to create a code word of length ‘n+k’. Once the issues have been resolved, the receiver can remove the extra symbols to restore the original message.

A flowchart showcasing the algorithms used in encoding has been added below in Figure 3 and also in the supplementary information (Figures S1-S8).

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

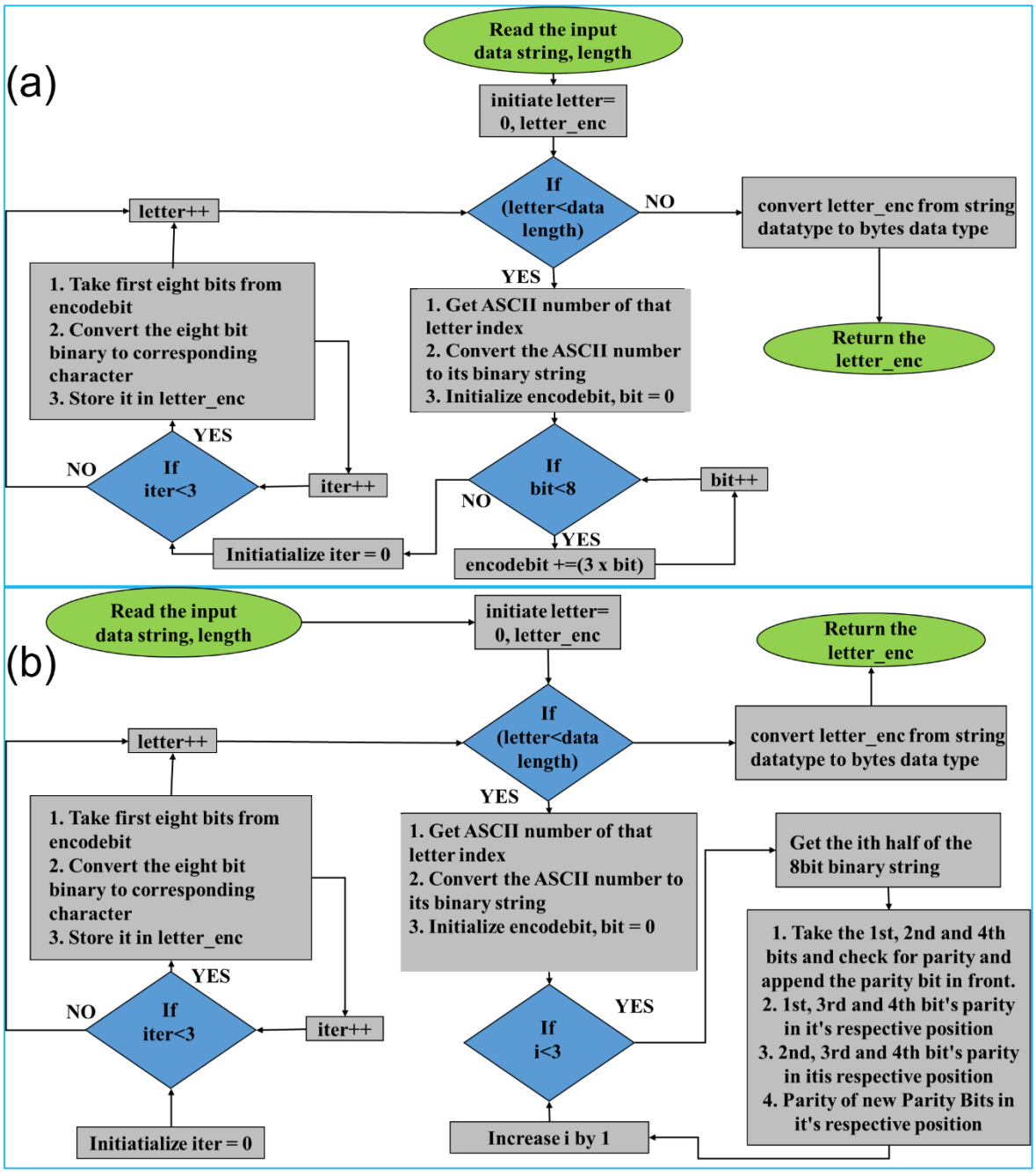

Figure 3: A flowchart showing the encoding algorithm for (a) Repeat code and (b) Hamming code in Python

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

Table 1 shows a comparative summary of the above FEC codes as below.

Error Correction Code	Execution Time	Error Correction Effectiveness	Link Performance
No FEC	Minimal	No Error Correction	Dependent on environmental conditions
Reed-Solomon (FEC)	High (Due to complexity)	Excellent (Handles burst errors)	Stable under fluctuating conditions
BCH (FEC)	Moderate (Higher than Hamming)	Very Good (Handles random errors)	Good in challenging environments
Hamming (FEC)	Low (Efficient)	Good (Single-bit errors)	Effective in moderate noise
Repeat Code (3 & 5)	Very Low (Simplest)	Basic (Low resilience)	Effective for low-data-rate applications

Table 1: Comparison of the execution time, error correction effectiveness, and link performance of various Forward Error Correction codes used.

2.3. Rivest-Shamir-Adleman (RSA) encryption:

In addition to its speed, affordability, and limitless bandwidth, optical wireless communication offers excellent data security because of its Line of Sight (LOS) property. However, using an encryption technique will further solidify the protection. RSA is an asymmetric encryption technique; RSA uses a pair of keys: a public key for encryption and a private key for decryption. The encryption strength of RSA lies in the difficulty of factoring large prime numbers, making unauthorized decryption nearly impossible without the private key. This provides a robust security measure for UOWC systems, particularly useful for high-stakes applications such as military or scientific data transfer, where protection from interception is paramount. RSA's computational demands are a trade-off for its high level of security, making it an optimal choice in applications where secure communication outweighs the need for rapid data processing. The working of the RSA algorithm is represented in Figure 4.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

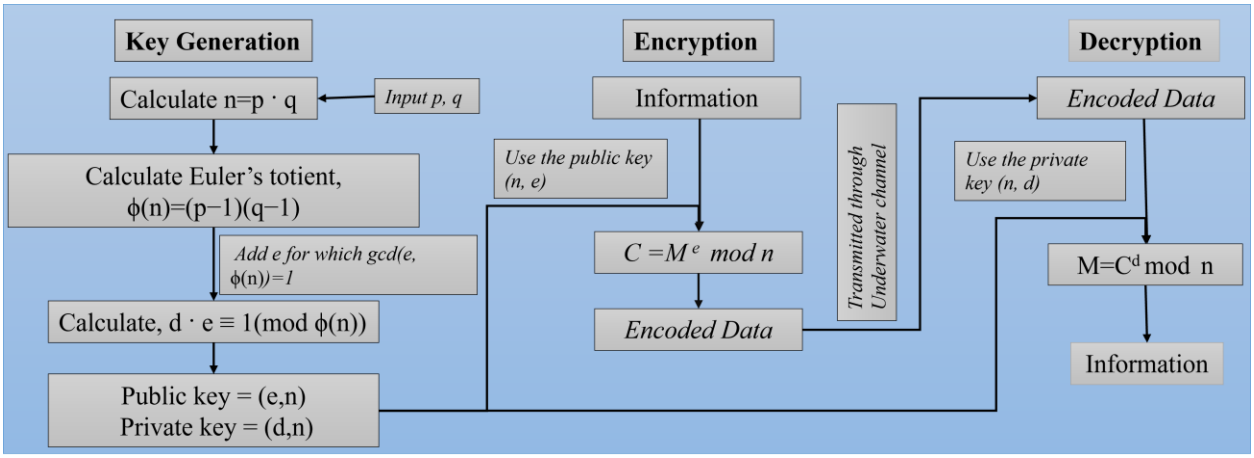

Figure 4: Overview of RSA Encryption and Modulation Techniques for Enhancing Secure and Reliable Underwater Optical Communication Systems

The proof for RSA can be obtained by using Fermat's Little Theorem[36,52], to prove we have to show that the decryption function is the inverse of the encryption function. Fermat's Little Theorem states,

$$a^{p-1} \equiv 1\ (mod p) \tag{7}$$

Here, $p \in \mathbb{Z}^+$ and $p \nmid a$ and p is a prime number

Let us apply the decryption function to the encryption function,

$$(m^e)^d \equiv m(mod\ pq) \tag{8}$$

Theoretically, it should give us the original data, thus proving the RSA algorithm.

The equation, $$d.e \equiv 1 mod(\phi(n)) \tag{9}$$

Where, $\phi(n)$ is Euler's totient represented as

$$\phi(n) = (p-1)(q-1) \tag{10}$$

Thus, equation 9, $d.e \equiv 1 mod\big(\phi(p-1)(q-1)\big) \Rightarrow de - 1 = k(p-1)(q-1)$ (11)

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

Where $k \in \mathbb{Z}^+$.

Let us consider two equations,

$$(m^e)^d \equiv m(mod\ p) \tag{12}$$

$$(m^e)^d \equiv m(mod\ q) \tag{13}$$

We can prove equation 12 by considering two cases:

1. $m \equiv 0(mod\ p)$

   Then, $p|m$ or, $m = \alpha p$ for any $\alpha \in \mathbb{Z}^+$,

   $\therefore (m^e)^d = (p\ \alpha)^{de} = p \cdot p^{ed-1} \cdot \alpha^{de}$ or, $p|m\text{^}de$ or, $(m^e)^d \equiv m(mod\ p)$

2. $m \not\equiv 0(mod\ p) \Rightarrow p \nmid m$

   According to Fermat's Little Theorem: $m^{ed-1} \equiv 1(mod\ p)$

   Now, $ed - 1 - k\ (p-1)(q-1)$ for any integer k

   $$\therefore m^{de} = m^{ed-1} \cdot m = m^{k(p-1)(q-1)} \cdot m \equiv (m^{p-1})^{q-1 \cdot k}$$

   Or, $$m^{de} \equiv (1)^{q-1 \cdot k} \cdot m \equiv m(mod\ p)$$

Using similar logic as shown above, it is possible to prove equation 13 as well.

If for two distinct prime numbers p and q, i.e., $\gcd(p, q) = 1$

$$a \equiv c(mod\ p) \text{ and } a \equiv c(mod\ q)$$

Then we can conjecture that $a \equiv c(mod\ pq)$

So, from equations 12 and 13, which have been proved, we can obtain

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

$$m^{de} \equiv m(mod\ pq) \quad (14)$$

That is the required equation to prove RSA encryption.

Together, these modulation schemes, Error Correction codes, and encryption methods form a comprehensive framework to enhance the effectiveness, reliability, and security of underwater optical communication systems.

3. Experimental Setup of Underwater Optical Communication Testbed

To perform UOWC experiments, a test bed has been developed in-house at a length of 4 meters, which is used to simulate underwater communication conditions in a controlled environment. We have carried out numerous experiments over this 4m setup using several in-house developed modulation schemes, forward error correction codes, and RSA encryption for different data rates. This system includes a laser source of 532nm wavelength as an optical transmitter and a photodetector at the receiver end placed across the channel. Both the transmitter and the receiver are connected with the appropriate electronics and to the PC for the implementation of a real-time data transfer. We have used an in-house developed, Python-based Graphical User Interface (GUI) which will allow us to select any data format such as text, video, or image file and to implement the choice of modulation schemes, forward error correction codes and RSA encryption. Various modulation schemes are tested, including OOK-NRZ, OO-RZ, PPM, and DPIM, are implemented and the performance of the system is evaluated in this environment. Figure 5 shows the schematic and the pictures of the working experimental setup. Figure 5a describes the complete schematic of the working of the UOWC system whereas Figures 5b, c, d, e, show the experimental pictures. Various Forward Error Correction codes including Repeat Code 03, Repeat Code 05, Hamming, BCH, and Reed Solomon Code, were applied and the performance was estimated.

We have also estimated the practical error fraction of receiving files, which helps define link performance. We have developed a separate Graphical User Interface to calculate the error

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

fraction using Python code. RSA encryption is also used to secure the data during transmission, protecting it from potential breaches. We have studied how the nature of the transmitting signal changes after applying all these parameters to the system. This setup enables a detailed analysis of how RSA and FEC improve secure and reliable underwater communication.

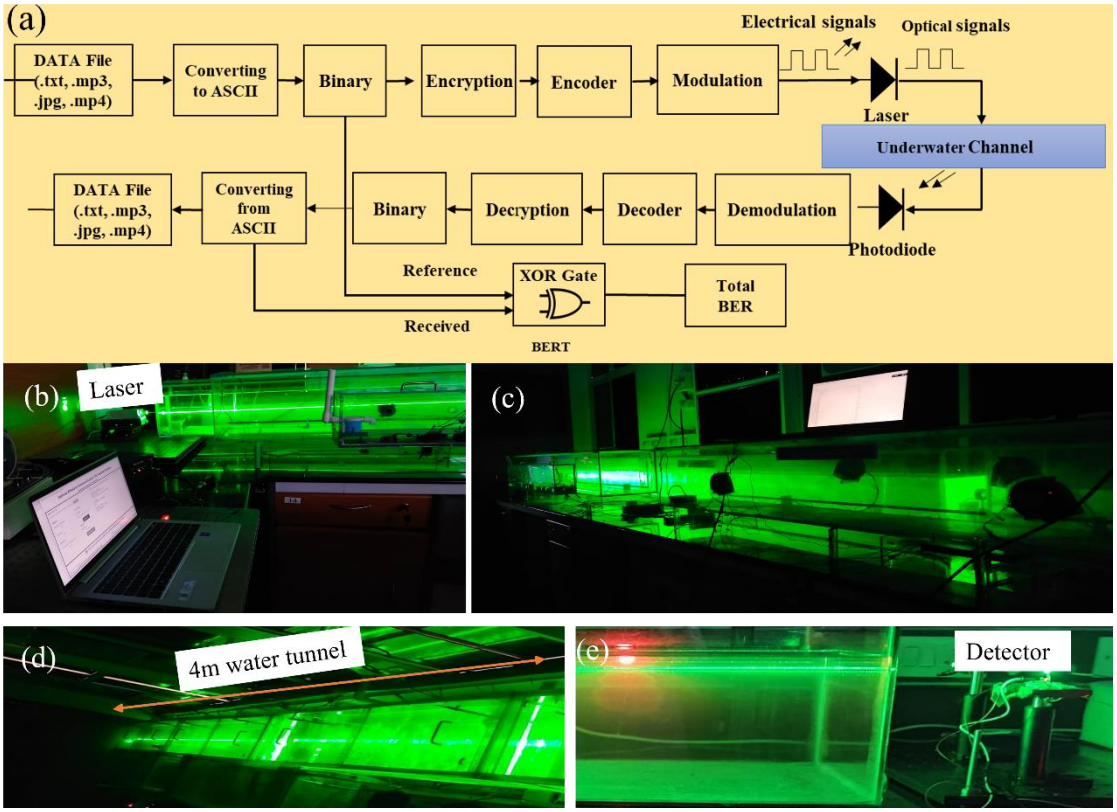

Figure 5: shows an experimental setup featuring a 4-meter water tunnel illuminated by a green laser: (a) Schematic diagram of 4m underwater optical wireless communication testbed and Integrated RSA Encryption and FEC Codes(b) Transmitter end (c) External view of the full tunnel setup, (d) Top-down perspective, and (e) Detector end capturing data.

The software part consists of two GUIs, as shown in Figure 6, one is used for communication, and the other deals with the calculation of BER by comparing the bits between the sent file and the received file. The GUI used for transmission is capable of handling all formats of files, as the files are brought down to binary format (0 and 1) using ‘latin1’ encoding. The GUI

ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

can act as both a transmitter and a receiver,i.e., a Transceiver, and can communicate with different Baud rates (Data rates). It houses various advanced techniques like Modulation techniques, Forward Error Correction techniques, and Encryption Techniques, which improve the quality and reliability of the communication link. To make the communication between the transmitter and the receiver less complex, the GUI has an inclusion of metadata that carries all the information like file name, file size, baud rate, and techniques used for transmission, this information is sent a second before the file transfer takes place. The receiver receives this and automatically calibrates itself to receive the file using this metadata, thus reducing the effort to select everything manually on the receiver end. The file received is saved in the folder whose path can be specified in the GUI code. A table (Table S1) consisting of all the standard Baud Rates used has been provided in the supplementary information.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

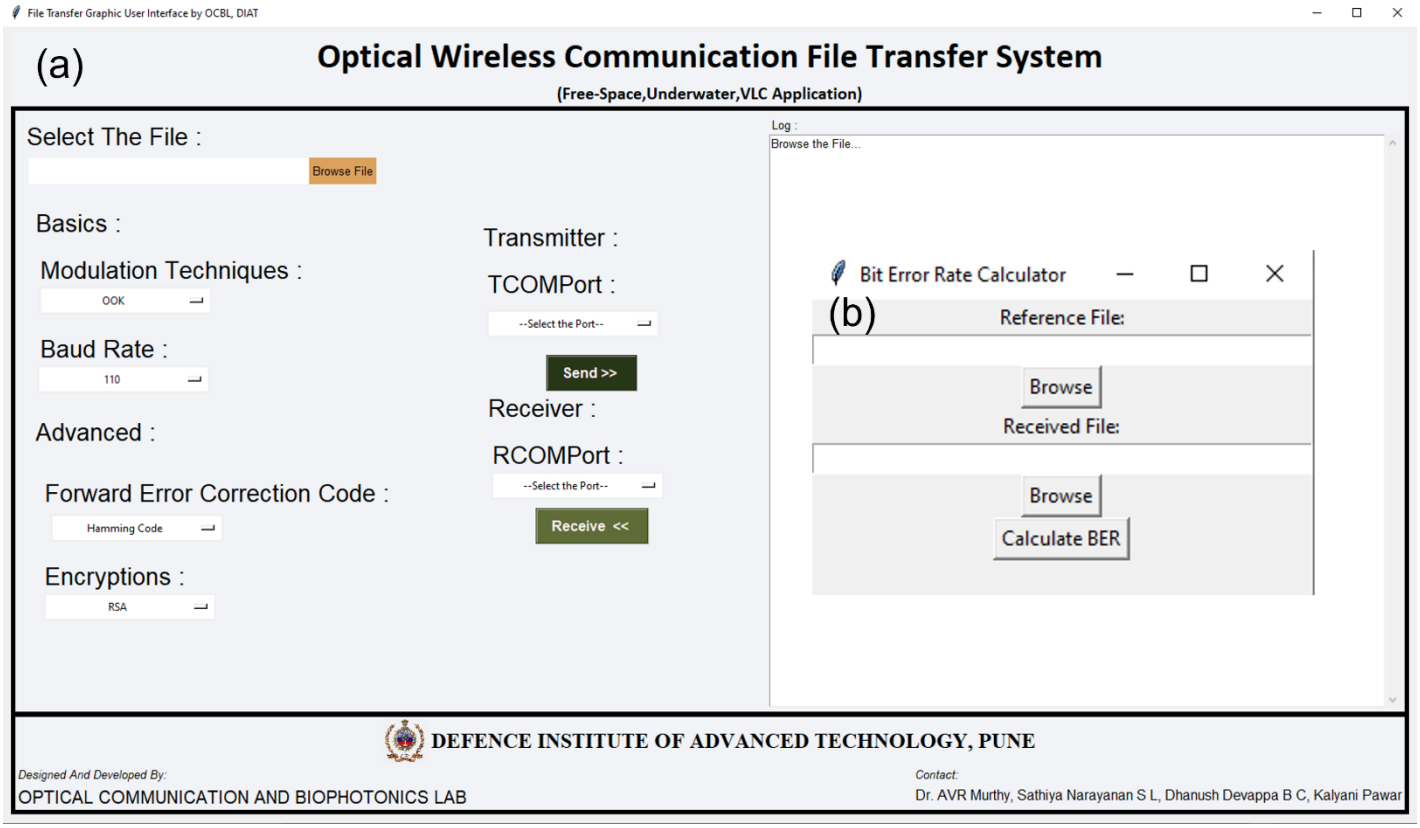

Figure 6: (a) Graphical User Interface for File transfer. (b) Graphical User Interface for BER calculation

The hardware component of the experiment includes an in-house 4m water channel, lasers, photodetectors, a laser driver circuit, USB to TTL converters, and two laptops. The 4m tank is filled with tap water, and the attenuation coefficient also known as beam extinction coefficient $c(\lambda)$[53], This can be obtained using

$$c(\lambda) = a(\lambda) + b(\lambda) \tag{15}$$

Where, $a(\lambda)$ and (λ) are the absorption and scattering coefficients.

Using the extinction coefficient, we can obtain the received optical power $p(r)$ at the detector[54],

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

$$\text{i.e., } p(r) = p(t) \cdot e^{-c(\lambda)\cdot L} \quad (16)$$

here p(t) = transmitted optical power, L= Communication range, $c(\lambda)$ = attenuation coefficient.

By using the above equations, appropriate components can be selected for the desired experimentation.

The parameters for all the hardware components used for the experimentation are provided in Table 2.

System Parameters used in the Experiment set up	Details
Source: DPSS Laser	MGL-FN-532-2W
Transmission Wavelength (λ)	532nm Laser diode
Transmitted power	2W
Receiver: Photodetector	TIFSS0054 laser receive module
Operating voltage	5V dc
Operating Conditions	-30°C to 85°C
ADC: USB to TTL converter	Waveshare 6Mbps
Operating voltage	3V and 5V DC
Channel	Underwater testbed
Communication range	4m
Baud Rate	9.6kbps-1Mbps

Table 2: Parameters of the hardware setup used in the experimentation.

4. Results & Discussion

4.1. RSA encryption Analysis

As explained in Section 2, a public key and private key will be generated with a prime number of combinations and data will be transmitted with encryption. The received data will be decrypted only with the combination of these two keys. Figure 7 shows the graph of the trends of increase in the encryption strength i.e., public key and private key with the rise of the prime numbers p,q. It can be noticed that there is an increasing trend in both; however, the combination of keys is unpredictable, making the decryption difficult, particularly at higher values of p, q. A table (Table

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

S1) consisting of the prime numbers used and their respective public keys and private keys has been added in the supplementary information.

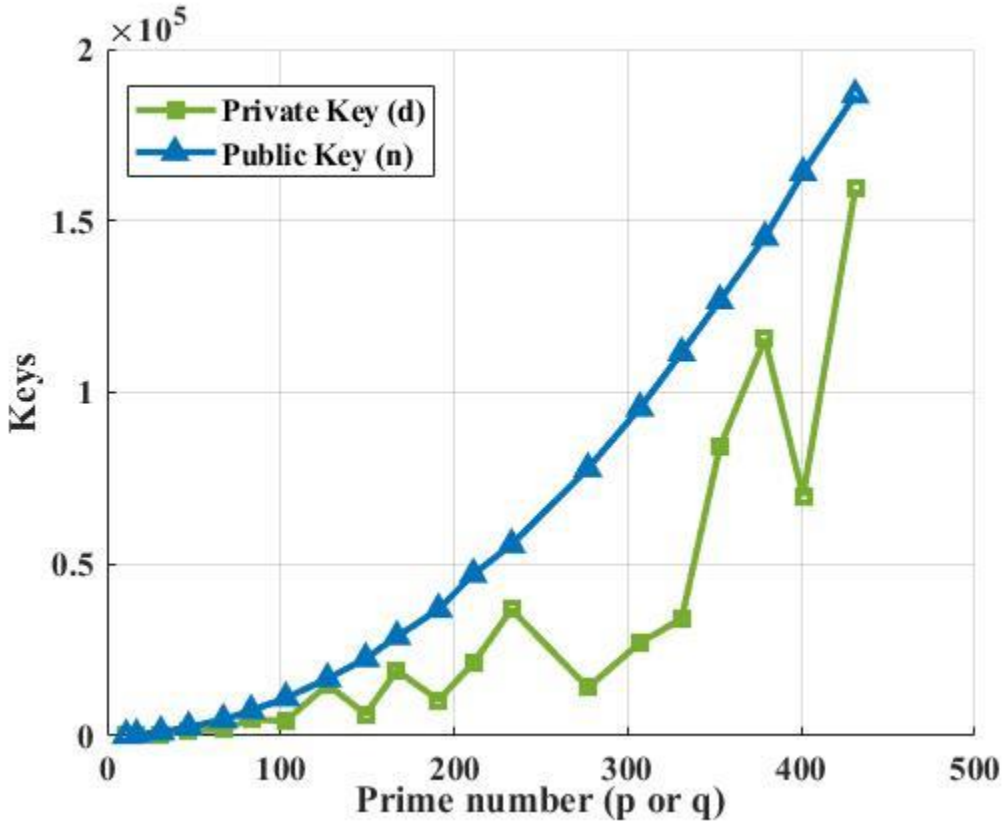

Figure 7: Graph shows the trends of public key (n) and private key (d)with sequential increase of p or q

4.2. RSA encryption and performance analysis of UWOC with different modulation schemes

We have developed RSA encryption and used it over various modulation schemes i.e., OOK-NRZ, RZ, PPM, and DPIM. To verify the impact of RSA encryption on different modulation schemes, we have estimated the practical execution time for different sequential combinations of *p, q*. This gives rise to different public keys (n) and private keys (d). Figure 8a shows the execution time versus the public key from 143 (11,13) to 186623 (431,433), up to 20 data points. This experiment was performed with a data rate of 19.200 kbps. A similar experiment was performed to check the effective implementation of RSA at various speeds and as shown in Figure 8b, the values

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

chosen for *p, q* are 47,53 for a public key value of 2491. The two experiments show that the systematic variation suggests the robustness of the RSA implementation.

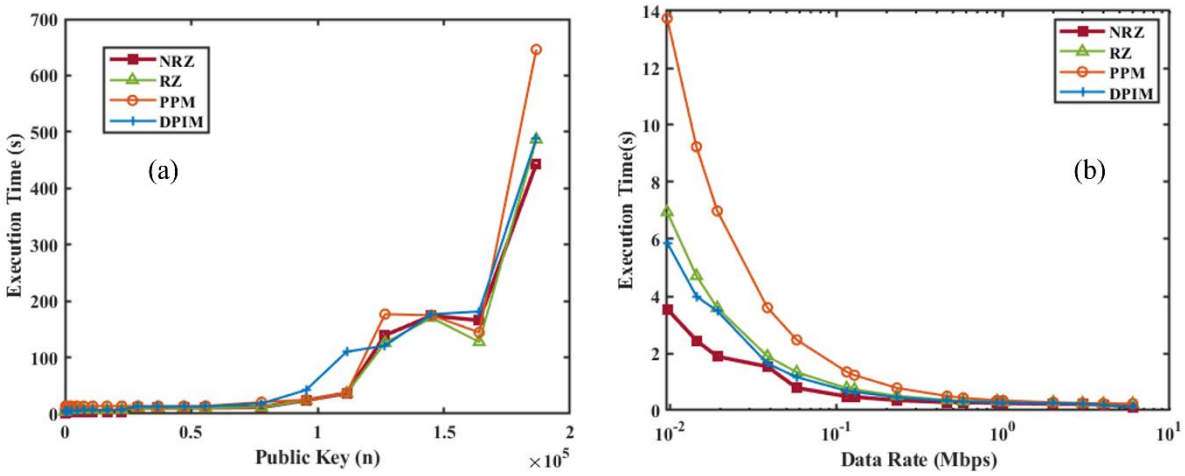

Figure 8: (a) Execution Time vs. Public Key Size. (b) Execution Time vs. Data Rate. The results highlight the trade-offs between encryption strength, modulation scheme efficiency, and transmission reliability in underwater optical communication systems.

After that, we compared the originally sent data and the received data from the UOWC system to estimate the error fraction without RSA encryption and with RSA encryption. This comparative study provided information on communication reliability. Figure 9(a) presents the error fraction versus data rate without RSA encryption applied and Figure 9(b) shows error fraction versus different modulation schemes with RSA encryption. In both cases, there is an increase in the error fraction at higher data rates. RSA encryption highlights the additional challenges introduced by encryption, due to processing overhead and synchronization issues. Together, these subfigures demonstrate the trade-offs between encryption strength and transmission reliability. This can be overcome by implementing Ethernet protocols.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

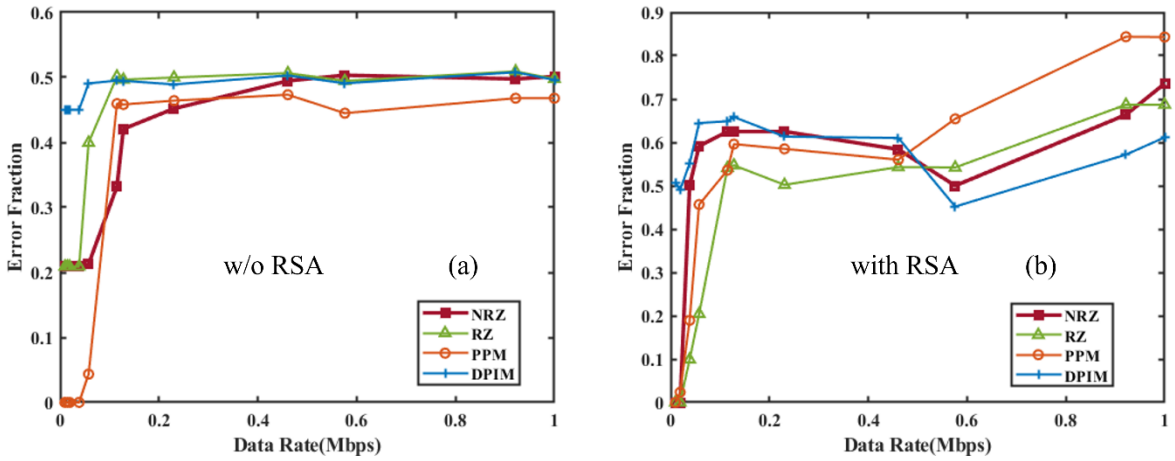

Figure 9: Impact of RSA encryption on different modulation schemes for OOK-NRZ, RZ, PPM, and DPIM modulation schemes; (a) Error fraction vs. data rate without encryption; (b) Error fraction vs. baud rate with RSA encryption

4.3. Integration of Forward Error Correction codes with RSA encryption

Despite offering higher security to the data, RSA encryption is prone to a higher error fraction. One of the solutions to overcome this is to implement mitigation techniques such as error correction codes along with the modulation to optimize/minimize the errors, if possible, to investigate the same, we have employed five forward error correction codes like Repeat Codes, Hamming Codes, BCH Codes, and Reed-Solomon Codes along with encryption and modulation schemes. We choose a data rate of 19.2 kbps and p, q as 47,53 to conduct initial experiments. Figure 10 shows the initial results of Forward Error Correction with RSA encryption across various modulation schemes. In Figure 10(a), the execution time is plotted against different FEC codes and Figure 10(b) shows the increase in data size with the effect of FEC implementation. The findings indicate that more complex FEC codes, like Reed-Solomon and BCH, significantly increase execution times due to their computational demands, especially when paired with encryption.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

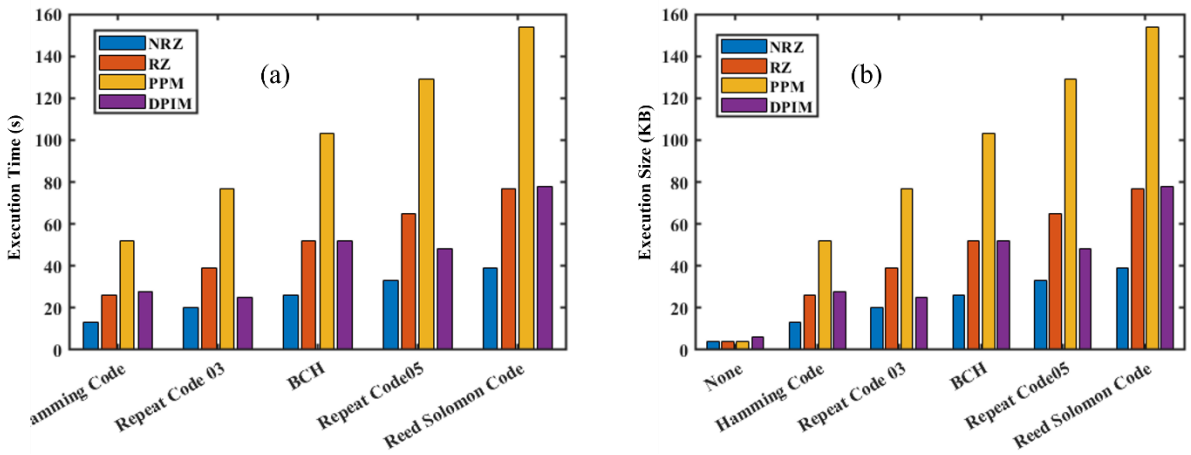

Figure. 10: Evaluation of RSA encryption with the Forward Error Correction (FEC) codes: (a) Execution Time vs. FEC code type; (b) Execution Size vs. FEC code type for different modulation schemes.

Figure 10 (b) shows the execution size with various error correction codes along with RSA encryption. There is an increase in the file size of the data with the error correction codes. It is more for PPM modulation and a mere increase of OOK schemes where whereas introducing the differential schemes like DPIM has further reduced the size, offering an advantage over other pulse modulation schemes.

After proving the basic RSA encryption with modulation and encoding formats, a systematic study was conducted to investigate the effect of encryption strength. For the same, we used a combination of "*p, q"* to generate various public keys from 143 (11,13) to 186623 (431,433) up to 20 data points and estimated the execution time for all error correction codes for all modulation separately.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

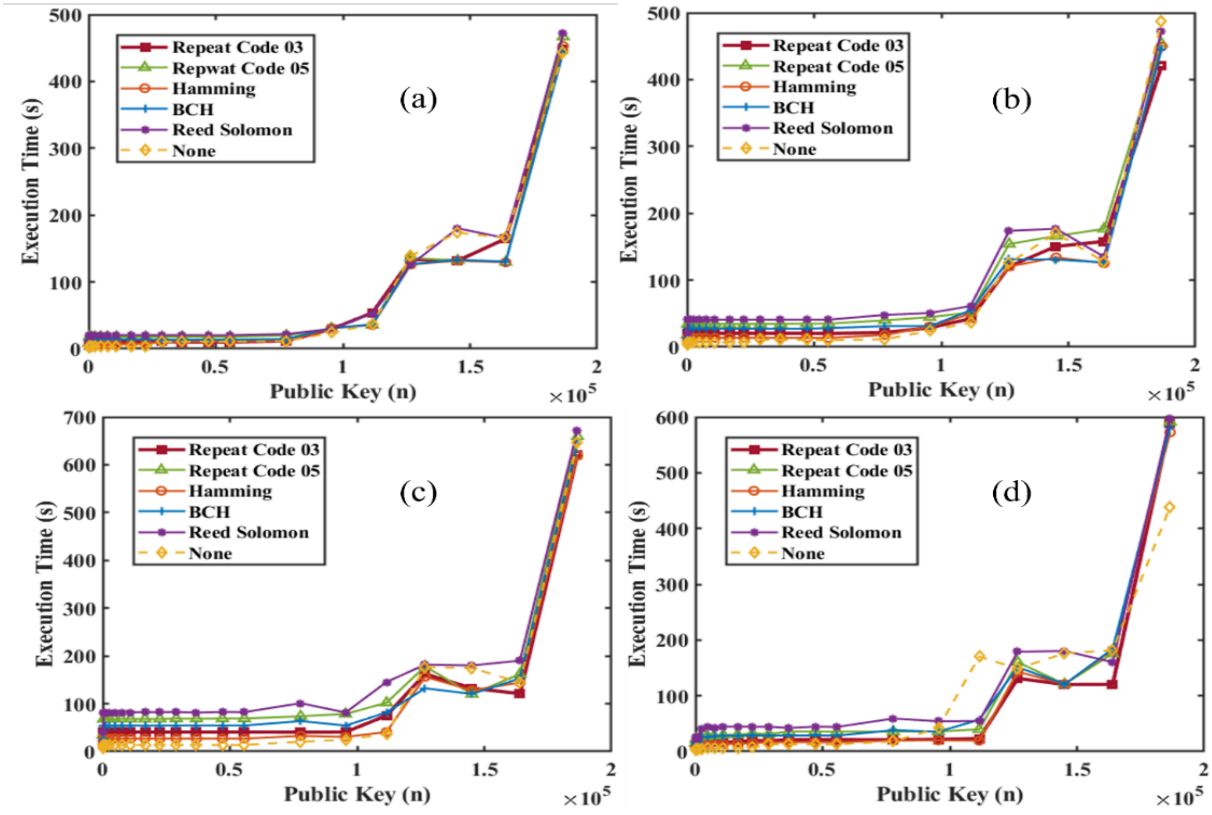

Figure 11: Analysis of RSA encryption strength (Execution Time vs Public key) combined with different Forward Error Correction codes across modulation schemes (a) NRZ, (b) RZ, (c) PPM, and (d) DPIM.

An in-depth analysis of the execution time required for RSA encryption when combined with different Forward Error Correction codes across various modulation schemes is provided in Figure 11. The graphs illustrate the relationship between the size of the RSA public key and execution time for various modulation schemes like OOK-NRZ, OOK-RZ, PPM, and DPIM. In the NRZ case, the execution time consistently increases with larger public key sizes, This trend shows the complexity of FEC codes like Reed-Solomon compared to simpler ones such as Repeat Codes. Similarly, RZ modulation shows a steady rise in execution time, with its synchronization advantages somewhat mitigating the overhead of FEC codes, though more complex codes like

ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

BCH still introduce significant delays PPM which offers better noise immunity, the execution time remains relatively manageable, with robust FEC codes becomes evident as public key sizes grow. Lastly, DPIM, known for its lower power requirements. Across all modulation schemes, the trade-offs between encryption strength, error correction, and computational efficiency are clear, emphasizing the importance of optimizing these factors for secure and reliable underwater optical communication.

4.4. Performance analysis of UWOC system with forward error correction codes and RSA encryption

After the successful implementation of the various FECs, modulation schemes, and RSA encryption combined, we have saved the data and measured the error fraction in the received file compared to the original sent file. This will give us a clear idea about which modulation scheme, with which error correction, will reduce the error, and where it will increase the error. For this, we have again used a data rate of 19.2 kbps and p, q as 47,53. The results found show interesting trends and are presented in Figure 12. OOK-NRZ modulation has shown a reduction in error fraction for almost all error correction codes. OOK-RZ has also shown a reduction in error fraction for all FECs except the repeat code 5. The PPM modulation scheme did not help in any reduction in the error; rather, it increased the error. This could be due to the bandwidth inefficiency and strong attenuations due to the channel. DPIM did not have much effect on FEC implementation.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

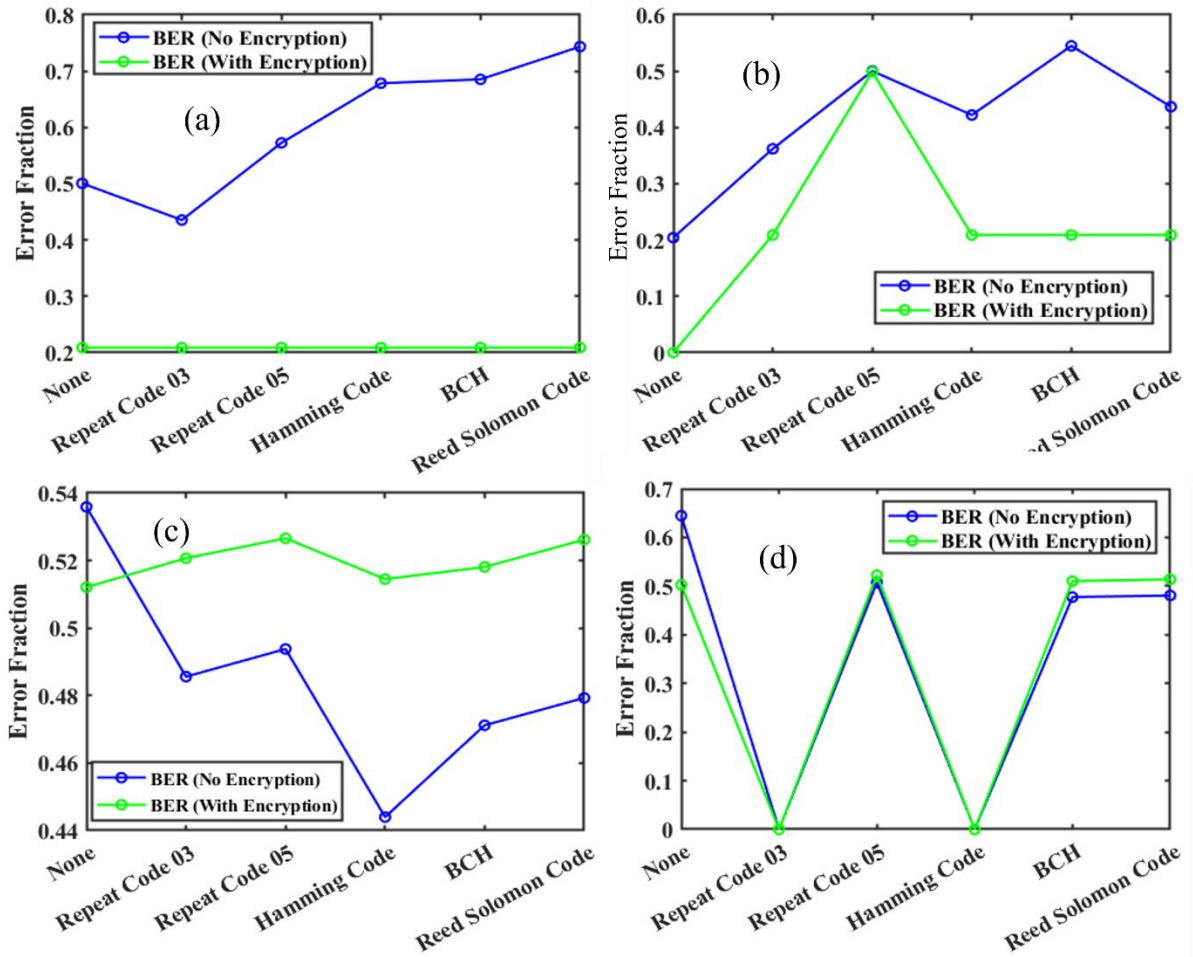

Figure 12**:** Performance analysis of various Forward Error Correction (FEC) codes combined with RSA encryption across different modulation schemes, a) NRZ, b) RZ, c) PPM, and d) DPIM, evaluating execution time, error correction effectiveness, and link performance. The results highlight the trade-offs between computational overhead, error resilience, and transmission efficiency, demonstrating the impact of FEC techniques and encryption on secure and reliable underwater optical communication.

Analysis of the link performance of various Forward Error Correction codes combined with RSA encryption across different modulation schemes is shown in Figure 12. The findings indicate

that more robust FEC codes, such as Reed-Solomon and Bose-Chaudhuri-Hocquenghem, result in significantly higher execution times due to their complex algorithms, while simpler codes like Repeat Codes exhibit lower execution times but reduced error correction capability. The error correction effectiveness of these codes reveals that advanced FEC techniques provide flexibility against underwater signal disruptions, ensuring reliability even in adverse conditions, but with the additional load of increased computational overhead due to the larger data sizes due from added parity bits and encryption payloads. Modulation schemes with inherent noise immunity, such as PPM, perform better in terms of both execution time and error correction compared to conventional schemes. The results indicate that a choice of advanced modulation schemes are good choice of selection is a good option for the UOWC system.

5. Conclusion:

To conclude, this paper presented a successful integration of RSA encryption and FEC codes with different modulation schemes. It tested the end-to-end data communication in a 4-meter UOWC testbed, which can be further extended to several meters with a reasonable increase in intensity. The results were analyzed for various metrics such as execution time, encryption and encoding strengths, and error fraction that evaluates the link performance. This combinational approach not only improves both data security and communication reliability but also provides flexibility of implementation in dynamic underwater environments. RSA encryption protects sensitive data, while FEC codes correct errors caused by factors like turbidity, salinity with enhancing data integrity and reducing errors. Link performance tests with different modulation schemes reveal trade-offs between encryption strength, error correction, and computational requirements. More advanced FEC codes, like Reed-Solomon and BCH, offer better error correction but need more processing power, while simpler codes like Repeat codes are less complex but less effective. Our studies showed that BER can be improved effectively by 20-40% if we include error correction codes, execution time increases almost 4 times (Quadruples) the original value, and execution size (KB) increases 16 times as compared to no FEC. In underwater settings, this can be a pivotal and practical solution for implementing the technology in real-life scenarios.

Communications & Networks Connect
ISSN: 3006-4813
2025, Article ID. x, Cite as: https://www.doi.org/10.69709/xxx

There is a lot of opportunity to improve the existing underwater optical wireless communication (UOWC) system we propose in this paper. Lightweight encryption schemes, such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES), can reduce computational complexity, and enable efficient real-time data transfer in resource-constrained underwater environments. Additionally, we can add an advanced error correction technique, such as turbo codes and concatenated codes, and study its impact on link reliability in highly turbulent conditions characterized by varying turbidity and salinity. We can also study and develop an adaptive modulation and coding protocol that dynamically adjust to environmental fluctuations which can further optimize bit error rate (BER) and link performance. We can also extend the system to multi-nodal configurations with Acquisition, Tracking, and Pointing (ATP) mechanisms that will facilitate robust underwater communication networks for defence and surveillance applications. Moreover, experimental validation over longer channel lengths under controlled oceanic conditions and the integration of deep learning-based signal detection techniques will strengthen the system's applicability in real-world underwater scenarios, ensuring secure and reliable communication in dynamic environments.

List of abbreviations:

- UOWC: Underwater Optical Wireless Communication
- RSA: Rivest Shamir Adleman
- FEC: Forward Error Correction
- BCH: Bose Chaudhuri Hocquenghem
- RS: Reed Solomon
- WDM: Wavelength Division Multiplexing
- BER: Bit Error Rate
- OOK-NRZ: On-Off Keying Non-Return to Zero
- OOK-RZ: On-Off Keying Return to Zero
- PPM: Pulse Position Modulation
- DPIM: Digital Pulse Interval Modulation
- GUI: Graphical User Interface
- USB: Universal Serial Bus
- TTL: Transistor-Transistor Logic
- Mbps: Megabit per second

- KB: Kilobyte
- 1GS: One Guard Slot
- NGS: No Guard Slot
- AES: Advanced Encryption Standard
- DES: Data Encryption Standard
- ATP: Acquisition, Tracking, and Pointing

Authors Contribution

Conceptualization and supervision, A.V.R.M; methodology, D.D.B.C.; validation, A.V.R.M.; formal analysis, D.D.B.C.; investigation, K.P.; resources, A.V.R.M.; data curation. K.P.; writing—original draft preparation, K.P. and D.D.B.C.; writing—review and editing, K.P. and D.D.B.C., A.V.R.M.; project administration, A.V.R.M.; funding acquisition, A.V.R.M.; All authors have read and agreed to the published version of the manuscript.

Availability of Data and Materials:

Data supporting the results of this study are available upon request from the corresponding author.

Figures Originality: The figures used in the manuscript are original and not reproduced from any published articles

Consent for Publication:

Not applicable.

Funding

This work received a grant from the TIDF-IIT Guwahati with the grant number **TIH/TD/0408.**

Conflicts of Interest: The authors declare that they have no conflicts of interest, financial or personal, that could have influenced the work reported in this manuscript.

Acknowledgments: All Authors Acknowledge IIT Guwahati Technology Innovation and Development Foundation and Defence Institute of Advanced Technology for financial and infrastructural support.

Supplementary Material

Supplementary material associated with this article has been published online and is available at: Link to the DOI

References

[1] Kaushal H and Kaddoum G 2016 Underwater Optical Wireless Communication *IEEE Access* **4** 1518–47

[2] Zeng Z, Fu S, Zhang H, Dong Y and Cheng J 2017 A Survey of Underwater Optical Wireless Communications *IEEE Communications Surveys and Tutorials* **19** 204–38

[3] Zhou L, Zhu Y and Zheng W 2017 Analysis and Simulation of Link Performance for Underwater Wireless Optical Communications *EAI Endorsed Transactions on Wireless Spectrum* **3** 153467

[4] Mohammed A S, Adnan S A, Ali M A A and Al-Azzawi W K 2022 Underwater wireless optical communications links: Perspectives, challenges and recent trends *Journal of Optical Communications* **45** 937–45

[5] Johnson L J, Jasman F, Green R J and Leeson M S 2014 Recent advances in underwater optical wireless communications *Underwater Technology* **32** 167–75

[6] Gkoura L K, Roumelas G D, Nistazakis H E, Sandalidis H G, Vavoulas A, Tsigopoulos A D and Tombras G S 2017 Underwater Optical Wireless Communication Systems: A Concise Review *Turbulence Modelling Approaches* ed K Volkov (IntechOpen)

[7] Khan I U, Iqbal B, Songzou L, Li H, Qiao G and Khan S 2021 Full-duplex Underwater Optical Communication Systems: A Review *Proceedings of 18th International Bhurban Conference on Applied Sciences and Technologies, IBCAST 2021* (Institute of Electrical and Electronics Engineers Inc.) pp 886–93

[8] Alatawi A S 2022 A Testbed for Investigating the Effect of Salinity and Turbidity in the Red Sea on White-LED-Based Underwater Wireless Communication *Applied Sciences (Switzerland)* **12**

[9] Chaudhary S, Sharma A, Khichar S, Shah S, Ullah R, Parnianifard A and Wuttisittikulkij L 2023 A Salinity-Impact Analysis of Polarization Division Multiplexing-Based

Underwater Optical Wireless Communication System with High-Speed Data Transmission *Journal of Sensor and Actuator Networks 2023, Vol. 12, Page 72* **12** 72

[10] Kumar S, Prince S, Aravind J V and G S K 2020 Analysis on the effect of salinity in underwater wireless optical communication *Marine Georesources and Geotechnology* **38** 291–301

[11] Zhang K, Sun C, Shi W, Lin J, Li B, Liu W, Chen D and Zhang A 2024 Turbidity-tolerant underwater wireless optical communications using dense blue–green wavelength division multiplexing *Opt. Express* **32** 20762–75

[12] Weng Y, Guo Y, Alkhazragi O, Ng T K, Guo J-H and Ooi B S 2019 Impact of turbulent-flow-induced scintillation on deep-ocean wireless optical communication *Journal of Lightwave Technology* **37** 5083–90

[13] Oubei H M, Zedini E, Elafandy R T, Kammoun A, Ng T K, Alouini M-S and Ooi B S Efficient Weibull Channel Model for Salinity Induced Turbulent Underwater Wireless Optical Communications

[14] Ali M A A 2015 Comparison of modulation techniques for underwater optical wireless communication employing APD receivers *Research Journal of Applied Sciences, Engineering and Technology* **10** 707–15

[15] Jeong G and Kim S M 2022 Performance Evaluation of Underwater Optical Wireless Communication Depending on the Modulation Scheme *Current Optics and Photonics* **6** 39–43

[16] Hamilton A, Popoola W O, Guler E and Geldard C T 2022 An Empirical Comparison of Modulation Schemes in Turbulent Underwater Optical Wireless Communications *Journal of Lightwave Technology, Vol. 40, Issue 7, pp. 2000-2007* **40** 2000–7

[17] Jain S, Devappa B C D, Pawar K and Murthy A V R 2024 Feasibility analysis of modulation formats in different seawater types and practical implementation on underwater optical communication testbed *Journal of Optics (India)*

[18] Mangrio H B, Baqai A, Umrani F A and Hussain R 2019 Effects of Modulation Scheme on Experimental Setup of RGB LEDs Based Underwater Optical Communication *Wirel Pers Commun* **106** 1827–39

[19] Gabriel C, Khalighi M A, Bourennane S, Leon P and Rigaud V 2012 Investigation of suitable modulation techniques for underwater wireless optical communication *2012 International Workshop on Optical Wireless Communications, IWOW 2012*

[20] Song Y, Lu W, Sun B, Hong Y, Qu F, Han J, Zhang W and Xu J 2017 Experimental demonstration of MIMO-OFDM underwater wireless optical communication *Opt Commun* **403** 205–10

[21] Oubei H M, Duran J R, Janjua B, Wang H-Y, Tsai C-T, Chi Y-C, Ng T K, Kuo H-C, He J-H, Alouini M-S, Lin G-R and Ooi B S 2015 48 Gbit/s 16-QAM-OFDM transmission based on compact 450-nm laser for underwater wireless optical communication *Opt Express* **23** 23302

[22] Tzimpragos G, Kachris C, Djordjevic I B, Cvijetic M, Soudris D and Tomkos I 2016 A Survey on FEC Codes for 100 G and beyond Optical Networks *IEEE Communications Surveys and Tutorials* **18** 209–21

[23] Xu X, Li Y, Huang P, Ju M and Tan G 2022 BER Performance of UWOC with APD Receiver in Wide Range Oceanic Turbulence *IEEE Access* **10** 25203–18

[24] Adnan S A, Hassan H A, Alchalaby A and Kadhim A C 2021 Experimental study of underwater wireless optical communication from clean water to turbid harbor under various conditions *International Journal of Design and Nature and Ecodynamics* **16** 219–26

[25] Joudha M M, Hmood J K and Adnan S A 2023 Engineering and Technology Journal Performance Analysis of Underwater Optical Communication System in Turbulent Link A R T I C L E I N F O *Engineering and Technology Journal* **41** 1082–90

[26] Puri R and Ramchandran K *Multiple Description Source Coding using Forward Error Correction Codes* *

[27] Leven A and Schmalen L 2014 Status and recent advances on forward error correction technologies for lightwave systems *Journal of Lightwave Technology* vol 32 (Institute of Electrical and Electronics Engineers Inc.) pp 2735–50

[28] Narayanan S L S, Devappa B C D, Pawar K, Jain S and Murthy A V R 2024 Implementation of forward error correction for improved performance of free space optical communication channel in adverse atmospheric conditions *Results in Optics* 100689

[29] Yousif A E, Al-Jammas M H and Abdulaziz A S 2024 Progress in MIMO Channel Coding Methodologies: An Extensive Overview and Comparative Evaluation *Lecture Notes in Networks and Systems* **1138 LNNS** 373–89

[30] Rahman Universitas Islam Kalimantan MAB Banjarmasin F 2015 APLIKASI KENDALI KESALAHAN PADA JARINGAN KOMPUTER DENGAN MENGGUNAKAN METODE ARQ (AUTOMATIC REPEAT REQUEST) *AL ULUM: JURNAL SAINS DAN TEKNOLOGI* **1**

[31] Wardlaw W P 2000 The RSA Public Key Cryptosystem *Coding Theory and Cryptography* 101–23

[32] Kumar M 2018 Advanced RSA cryptographic algorithm for improving data security *Advances in Intelligent Systems and Computing* **729** 11–5

[33] Zhang Z, Mou J, - al, Wang D, Wu Z, Cui - Y, Marto Hasugian P, Barita Nauli Simangunsong P, Iqbal Panjaitan M, Tamando Sihotang H, Efendi S, Zamzami E M, Mawengkang H and Program D 2020 Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security *J Phys Conf Ser* **1641** 012042

[34] Zhang Q 2021 An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption *Proceedings - 2021 2nd International Conference on Computing and Data Science, CDS 2021* 616–22

[35] Sihotang H T, Efendi S, Zamzami E M and Mawengkang H 2020 Design and Implementation of Rivest Shamir Adleman's (RSA) Cryptography Algorithm in Text File Data Security *J Phys Conf Ser* **1641** 012042

[36] Rivest R L, Shamir A and Adleman L 1978 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems *Commun ACM* **21** 120–6

[37] Xu J, Kishk M A, Zhang Q and Alouini M S 2023 Three-Hop Underwater Wireless Communications: A Novel Relay Deployment Technique *IEEE Internet Things J* **10** 13354–69

[38] Mohamed A G, El-Mottaleb S A A, Singh M, Ahmed H Y, Zeghid M, Abdulkawi W M, Bouallegue B and Abdalla O A 2024 Chaos Fractal Digital Image Encryption Transmission in Underwater Optical Wireless Communication System *IEEE Access* **12** 117541–59

[39] Afifah S, Wei J K, Marlina L, Liaw S K, Lee P J and Yeh C H 2025 Performance evaluation of multi-wavelength visible light underwater optical communication *Opt Lasers Eng* **192** 109026

[40] Dong X, Zhang K, Sun C, Zhang J, Zhang A and Wang L 2025 Towards 250-m gigabits-per-second underwater wireless optical communication using a low-complexity ANN equalizer *Opt Express* **33** 2321

[41] Zhang K, Sun C, Shi W, Lin J, Li B, Liu W, Chen D and Zhang A 2024 Turbidity-tolerant underwater wireless optical communications using dense blue–green wavelength division multiplexing *Opt Express* **32** 20762

[42] Jiang R, Sun C, Zhang L, Tang X, Wang H and Zhang A 2020 Deep learning aided signal detection for SPAD-Based underwater optical wireless communications *IEEE Access* **8** 20363–74

[43] Chen Z, Tang X, Sun C, Li Z, Shi W, Wang H, Zhang L and Zhang A 2021 Experimental Demonstration of over 14 AL Underwater Wireless Optical Communication *IEEE Photonics Technology Letters* **33** 173–6

[44] Dwivedy P, Dixit V and Kumar A 2023 Cooperative VLC system using OOK modulation with imperfect CSI *Phys Scr* **98** 25509

[45] Luo S, Miao M and Li X 2025 A multi-dimensional modulation format for spectral efficiency improvement of PPM system and its BER performance analysis in free-space optical communication *Journal of Optics (United Kingdom)* **27**

[46] Ghassemlooy Z and Hayes A R 2000 Digital pulse interval modulation for IR communication systems—a review *International Journal of Communication Systems* **13** 519–36

[47] Arun K. Majumdar A A, Toshimitsu Asakura U, Theodor Hänsch J W, Takeshi Kamiya G, Ferenc Krausz J, Bo Monemar G A, Herbert Venghaus S, Horst Weber G and Harald Weinfurter G *Springer Series in Optical Sciences*

[48] Miroshnikova N E and Sattarova A I 2022 Analysis of Error-Correction Codes Properties for Underwater Optical Communication Systems with OCDM Modulation *2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2022 - Conference Proceedings*

[49] Elfikky A, Boghdady A I, AbdElkader A G, Elsayed E E, Palitharathna K W S, Ali Z, Singh M, Mohsan S A H, Mahmoud M and Aly M H 2024 Performance analysis of convolutional codes in dynamic underwater visible light communication systems *Opt Quantum Electron* **56** 1–17

[50] Devappa D, Banerjee S, Pawar K and Murthy Dr A V R 2025 Practical realization and performance analysis of Rivest-Shamir-Adleman encryption for secure underwater optical communication *Next Research* 100225

[51] Cai Y, Ramanujam N, Morris J M, Adali T, Lenner G, Puc A B and Pilipetskii A Performance limit of forward error correction codes in optical fiber communications *OFC 2001. Optical Fiber Communication Conference and Exhibit. Technical Digest Postconference Edition (IEEE Cat. 01CH37171)* **2** TuF2-T1-3

[52] Anon Number Theory - Tristin Cleveland - Google Books

[53] Kaushal H and Kaddoum G 2016 Underwater Optical Wireless Communication *IEEE Access* **4** 1518–47

[54] Ramley I, Alzayed H M, Al-Hadeethi Y, Chen M and Barasheed A Z 2024 An Overview of Underwater Optical Wireless Communication Channel Simulations with a Focus on the Monte Carlo Method *Mathematics 2024, Vol. 12, Page 3904* **12** 3904