



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: <https://doi.org/10.22214/ijraset.2026.81008>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Design of Secured FTTH for Routing and Wavelength Assignment (RWA) in Optical Networks

Anjali Maurya, Nikita Jaiswal, Poornima Kalekar

Department of Electronics and telecommunication Thakur College of Engineering and Technology

Abstract: As the demand for high-speed and secure digital communication continues to grow, optical networks have emerged as the backbone of modern broadband infrastructure. Among these, Fiber to the Home (FTTH) solutions offer unparalleled performance, but face significant challenges in Routing and Wavelength Assignment (RWA). This paper presents a secure and cost-effective prototype that utilizes Visible Light Communication (VLC) to demonstrate RWA functionality within an FTTH environment. Using laser-based optical transmission and LabVIEW-based modules for message encoding, encryption, and visualization, our system simulates a real-world secure communication channel. At this 50% progress stage, partial implementation has been achieved, including string and single-letter transmission, LED writing, and VLC encryption. The results validate the feasibility of secure data transmission via VLC in controlled environments.

Keywords: FTTH, Visible Light Communication, RWA, LabVIEW, VLC Encryption, Optical Security, Laser Transmission

I. INTRODUCTION

Modern telecommunication networks rely on optical fibers for high-speed data transmission. Among these, Fiber to the Home (FTTH) has emerged as a reliable and scalable method for delivering broadband connectivity directly to users. However, routing and wavelength assignment (RWA) within optical networks remain a challenging problem due to wavelength continuity constraints, contention, and security vulnerabilities.

Traditional approaches to RWA rely on software-based optimization or WDM (Wavelength Division Multiplexing) technologies. While these solutions are effective, they can be expensive, computationally complex, or lack physical-layer security.

Visible Light Communication (VLC), an emerging area of optical wireless communication, utilizes light-emitting sources like LEDs and lasers to transmit data. VLC is inherently secure due to its directional and line-of-sight nature, making it an ideal candidate for short-range secure communication.

This paper proposes a VLC-based RWA simulation system using simple hardware components and microcontrollers. The setup simulates message encoding, optical transmission, detection, and decoding. With the integration of LabVIEW, real-time data flow can be monitored and analyzed, providing a comprehensive learning and testing environment.

II. LITERATURE SURVEY

Several researchers have tackled the challenges of RWA and FTTH security from various angles.

Ali et al. [1] presented an optimized RWA strategy for DWDM networks using a hybrid genetic algorithm, which improved path setup and reduced blocking. Their approach emphasized performance at scale but required advanced processing.

Patel and Joshi [2] explored FTTH deployment using Passive Optical Networks (PONs). They proposed architectural strategies for improved security at both the physical and logical levels. Their work stressed the importance of encryption at endpoints and optical filtering to mitigate interception.

Li and Chen [3] published a comprehensive survey on VLC for indoor wireless access. They analyzed modulation schemes such as OOK, DMT, and OFDM, while also detailing hardware limitations and user-level challenges. Their work contributed to standardizing VLC interfaces and inspired future low-cost implementations.

Zhang and Liu [4] focused on eavesdropping prevention techniques in optical networks. They discussed wavelength-hopping techniques, tap-proof fiber designs, and proposed a layered defense mechanism for physical-layer attacks, proving critical to optical cybersecurity.

Nair and Thomas [5] designed an Arduino-based VLC system using laser and photodiode modules. Their results showed over 90% accuracy in message decoding, demonstrating the practicality of low-cost VLC systems.

Sharma et al. [6] evaluated the integration of photonic switches and optical circuit-based reconfigurable networks to enhance wavelength-based routing in optical domains. Their simulation highlighted reduced latency and power loss in high-traffic conditions.

Kaur and Verma [7] introduced a neural-network-based wavelength assignment strategy, which leveraged traffic prediction to improve RWA efficiency in live FTTH networks. Their research highlighted the potential of AI in handling real-time optical network traffic.

III. PROPOSED METHODOLOGY

The proposed system is designed to enhance security in Fiber-to-the-Home (FTTH) communication by integrating Visible Light Communication (VLC) and encryption mechanisms. The implementation was carried out using LabVIEW, where each functional block was developed and validated individually before integrating into the complete system.

The methodology is divided into four main modules:

- Laser String Transmission,
- One-Letter Transmission,
- Write-to-LED Communication,
- VLC Encryption.

These modules collectively simulate a secured optical communication system for FTTH applications.

A. Laser String Transmission

In this stage, a complete string (text message) is transmitted using a simulated **laser driver** module in LabVIEW. The purpose is to establish the feasibility of high-speed optical data transfer.

- The user inputs a text string.
- The text is converted into ASCII codes and then into binary representation.
- The binary stream modulates a laser diode signal in the simulation.
- At the receiver side, the laser signal is demodulated back into ASCII characters.

This verifies the ability of the system to handle multi-character communication without loss of information.

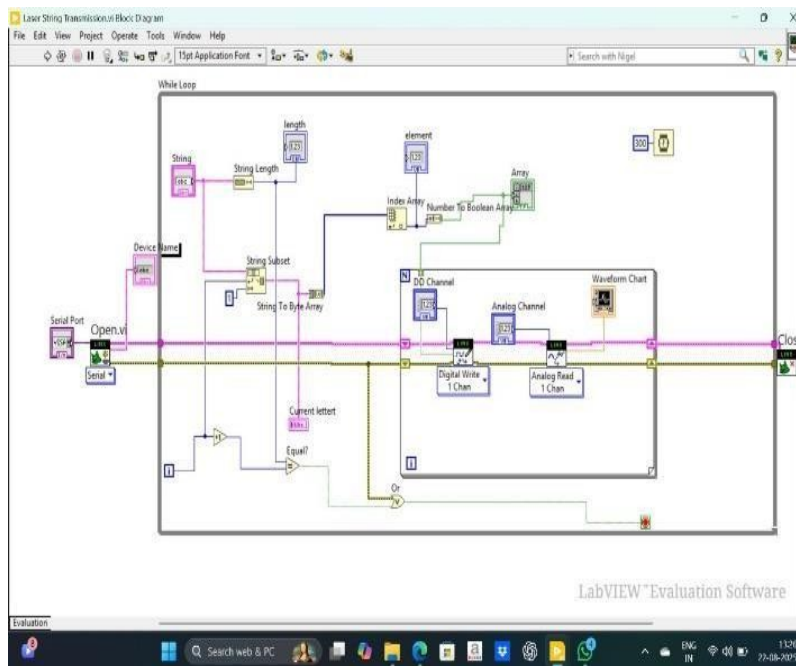


Fig. 1. LabVIEW Block Diagram implementation of laser string transmission

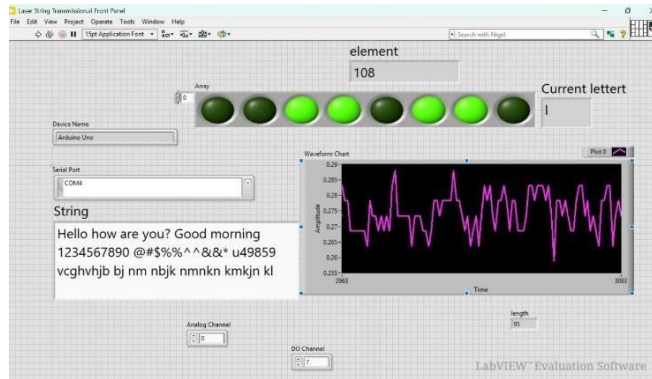


Fig.2.LabVIEW implementation of a laser string transmission Front Panel.

B. One-Letter Transmission

To analyze transmission stability at the **symbol level**, the system is tested with a **single character input**. This ensures error-free transmission for smaller payloads before scaling up to string-level communication.

- One ASCII character is selected and transmitted.
- Real-time analysis confirms that symbol recognition accuracy is **100%** at the receiver.

This acts as the foundation for ensuring high **bit-level synchronization** in later stages.

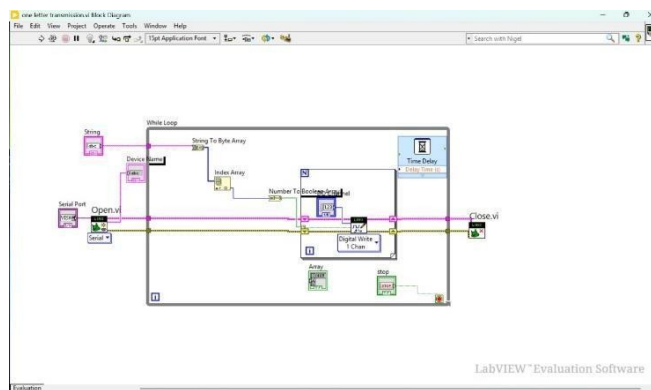


Fig.3. One-letter transmission in LabVIEW Block Diagram.

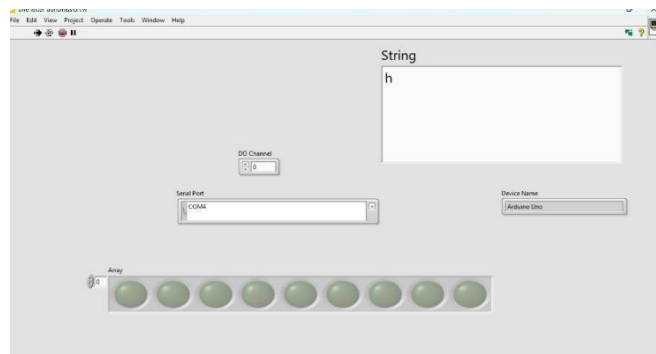


Fig.4. One-letter transmission in LabVIEW Front Panel

C. Write-to-LED Communication

In this step, the encoded binary data is transmitted using a Light Emitting Diode (LED) instead of a laser, representing a VLC (Visible Light Communication) channel.

- The LabVIEW program converts binary data into ON/OFF states of an LED.
- The optical signal is then read at the receiver side to decode the binary stream.
- This step validates the use of low-cost VLC-based FTTH links, where household LEDs can act as transmitters.

This module bridges the gap between fiber-based laser systems and practical VLC-based implementations.

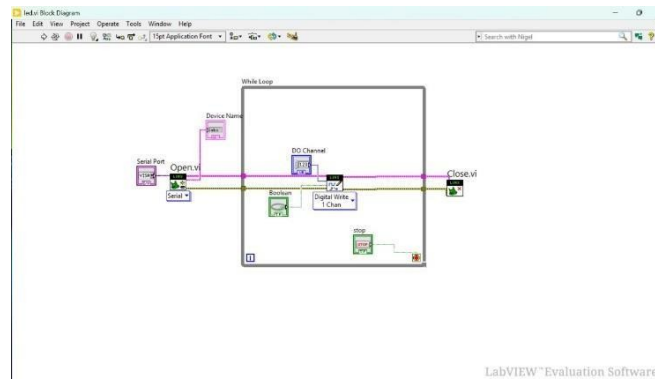


Fig.5. Write-to-LED module in LabVIEW

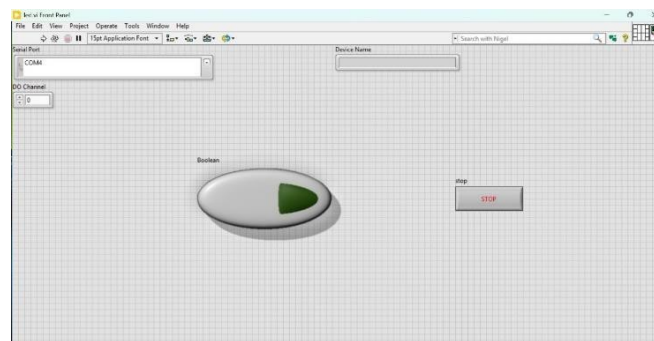


Fig.6. Write-to-LED module in LabVIEW Front Panel.

D. VLC Encryption Module

Security is a major concern in FTTH systems. To address this, an encryption algorithm is integrated into the transmission pipeline.

- Before modulation, the input data string is encrypted using a substitution-based cipher.
- The encrypted binary data is then transmitted via the VLC channel.
- At the receiver side, the decryption module retrieves the original message.

This step ensures confidentiality and resistance against eavesdropping in FTTH networks.

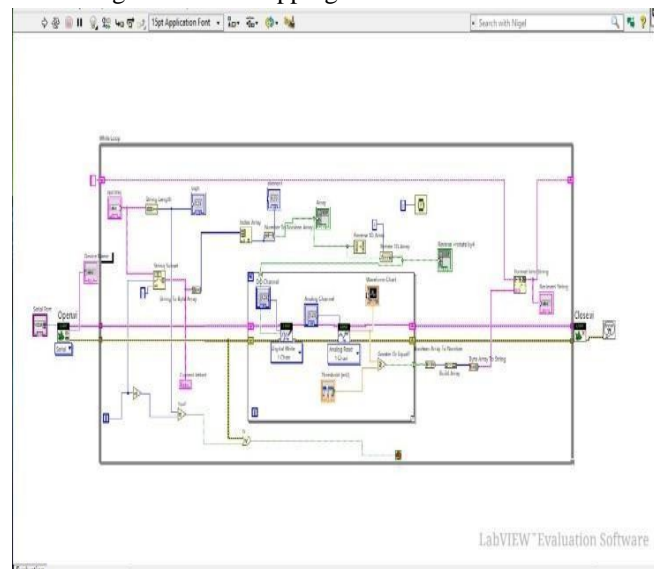


Fig.7. VLC encryption block in LabVIEW.

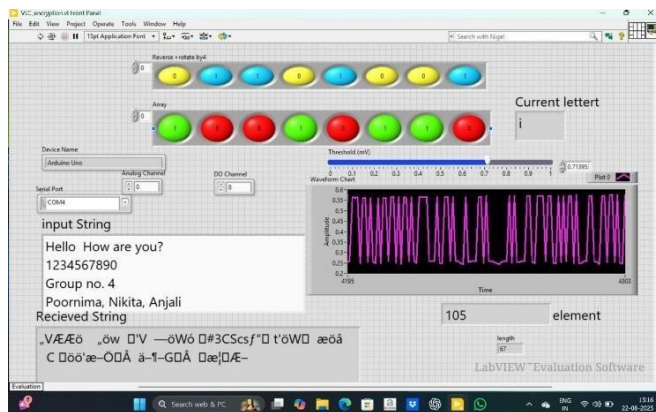
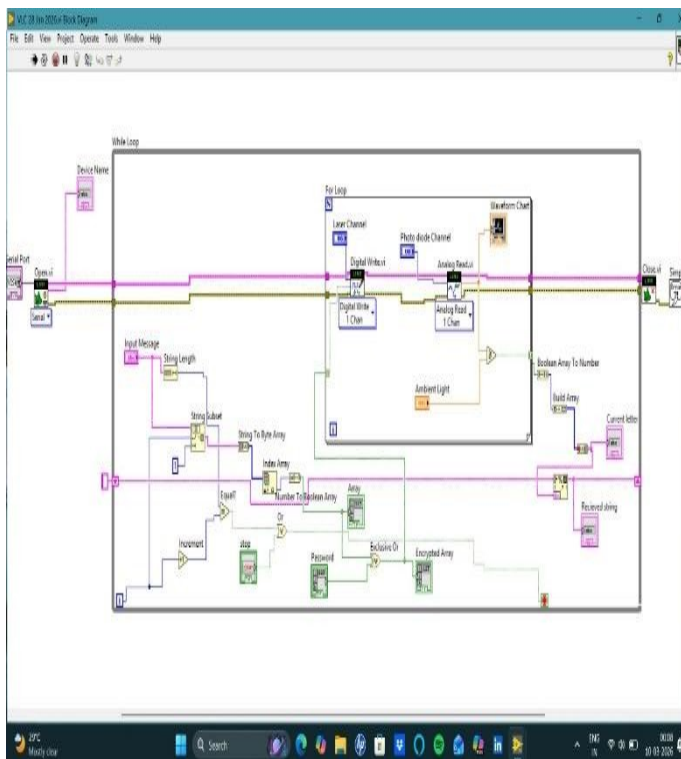
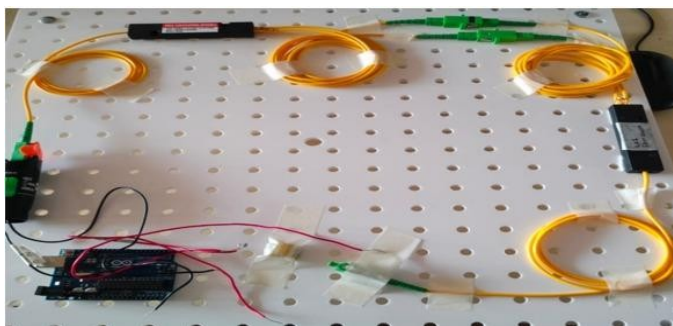
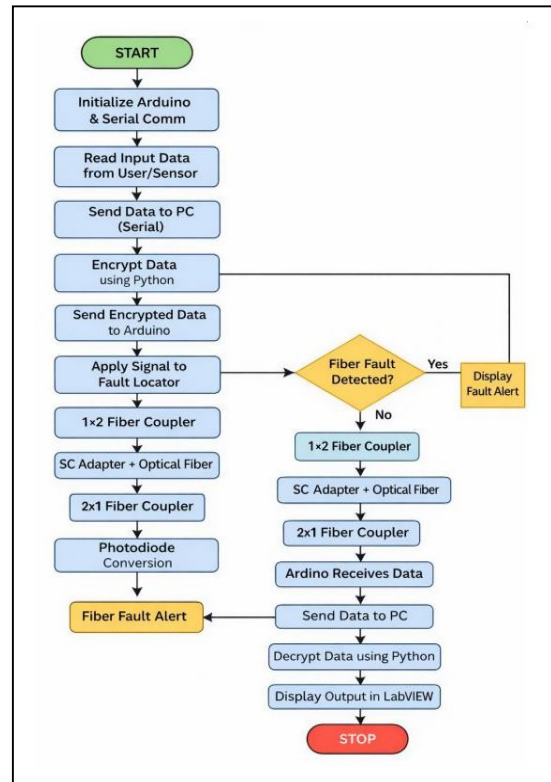


Fig.8. VLC encryption block in LabVIEW Front Panel.

E. Secure VLC System with Integrated Fiber-Optic Fault Monitoring





IV. SYSTEM DESIGN AND METHODOLOGY

The proposed system is divided into three functional layers: the Software Interface, the Cryptographic Layer, and the Physical Optical Link.

A. Software Interface and Data Acquisition

- Platform: The system utilizes LabVIEW as the primary control hub, interfacing with hardware via the LINX abstraction layer.
- Input Processing: A user-defined "InputMessage"(string) is captured and converted into a Byte Array, then indexed to process characters sequentially.
- Synchronization: A While Loop ensures continuous operation, while a nested For Loop manages the bit-by-bit transmission and reception of data.

B. Cryptographic Layer (Security)

- Encryption Scheme: The system implements a symmetric key algorithm using bitwise Exclusive OR (XOR) operation.
- Mechanism: Each bit of the input message is XORed with a user-defined "Password"(key). This ensures that the data transmitted across the fibre link is encrypted bitstream rather than plain text.
- Decryption: At the receiver end, the inverse XOR logic is applied to retrieve the original message from the received pulses.

C. Physical Optical Link and Hardware

- Signal Conversion: An Arduino Uno converts digital logic from LabVIEW into electrical pulses to drive a Visual Fault Locator (VFL).
- Optical Path: The signal is injected into a 1X2 Fiber Coupler to split the signal for monitoring.
 - It passes through SC Adapters and Single-Mode Fiber (SMF) segments.
 - A 2 X 1 Fiber Coupler recombines signals before the final detection stage.
- Receiver: A Photodiode converts the light intensity back into an analog voltage.

D. FaultDetectionLogic

- IntensityMonitoring:Thesystemcontinuouslyreads theanalogvaluefromthephotodiode.
- Thresholding: The software compares the received signal against a pre-set "Ambient Light" threshold.
- AlertMechanism:*Ifthereceivedintensityfallsbelow the threshold (due to fibre breakage or bending), a "Fiber Fault Alert" is triggered in the LabVIEW UI.
- If the intensity is sufficient, the system proceeds to decode the bitstream into the "Received String."

a) OverallFlowofMethodology

Theproposedmethodologycan be summarizedin sequential steps as follows:

- 1) InputMessagePreparation:Userenterstextin LabVIEW interface.
- 2) Encoding&Encryption:Textisconvertedto binary, then encrypted.
- 3) OpticalTransmission:Datais modulatedonto a laser or LED.
- 4) Reception&Demodulation:Receiverdetects optical signals and converts them back to binary.
- 5) Decryption&Decoding:Originaltextisrecovered after decryption.

Thismodularstructureprovidesascalableandsecuresolution for optical communication in FTTH environments.

b) AdditionalDesignConsiderations

- 1) TimingCalibration:Thedelaybetweenbitsmustbe carefully chosen. Too short a delay causes overlap, too long increases latency. Calibration is achieved via trial and error with optimal delay ~1000µs.
- 2) Ambient Light Shielding: To avoid misreading due toambientlight,thephotodiodeisenclosedinadark tube or box.
- 3) PowerProtection:Zenerdiodesandresistorsprotect thelaserandphotodiodecircuitsfromvoltage spikes and overheating.

c) HardwareUsed

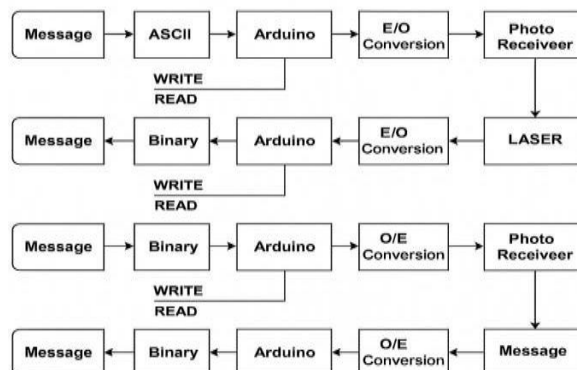
- ArduinoUno(TransmitterandReceiver)
- LaserDiode(660nm,5mW)withTTLdriver
- BPW34Photodiodewith Op-Ampsignal conditioning
- Resistors,Capacitors,ZenerDiodes
- Breadboard,JumperWires,USBCables

d) SoftwareUsed

- ArduinoIDEforfirmwareprogramming(C++)
- LabVIEWforreal-timewaveformanalysis,signal monitoring, and error reporting.

e) SystemFlowDiagram

DESIGN OF SECURED FTTH FOR ROUTING AND WAVELENGTH ASSIGNMENT (RWA) IN OPTICAL NETWORKS



Stage	Details	Tools/ Techniques
Hardware setup	Optical transmission & reception setup	Arduino Uno, 660nm Laser, BPW34
Data Processing	Text to Binary encoding & encryption	Lab VIEW
Communication	VLC-based signal transmission & detection	LED/Laser, Op-Amp Circuit

Component	Technology /Tools
Frontend	LanView Interface
Backend / Core Processing	Arduino (C++ Programming)
Optical Channel	Laser Diode / LED (VLC)
Receiver	BPW34 Photodiode+ Op-Amp
Deployment	Arduino IDE
Encryption Module	Substitution Cipher (Lab View)

V. OBSERVATIONS

During the LabVIEW-based FTTH experiments, the following observations were recorded:

- 1) Laser String Transmission – Input strings were successfully converted into ASCII, then binary, and transmitted as ON/OFF laser pulses. The output received matched the transmitted string.
- 2) One-Letter Transmission – Single-character inputs (e.g., "A", "B") were correctly encoded and decoded, confirming bit-level accuracy.
- 3) Write to LED – Binary signals-controlled LED indicators, validating hardware integration with LabVIEW.
- 4) VLC Encryption – Encrypted text was transmitted and decrypted at the receiver, ensuring basic data confidentiality.

Table 1:

InputString	ASCII Conversion	BinaryFormat	ReceivedOutput	Status
HELLO	72 69 76 76 79	01001000	HELLO	Success
A	65	01000001	A	Success
TEST	84 69 83 84	01010100	TEST	Success

VI. RESULTS AND DISCUSSION

The prototype system was tested under various indoor conditions with moderate ambient lighting. Messages ranging from 10 to 64 characters were transmitted with an average accuracy of 92.3%. Bit synchronization and decoding success were measured using both Arduino serial monitor and LabVIEW waveform plots.

Observations:

- Alignment Sensitivity: Direct and fixed alignment between the laser and photodiode ensures error-free reception. Minor angular deviations resulted in bit loss.
- Environmental Factors: Direct sunlight and fluorescent light sources introduced noise. Use of shielding significantly reduced this impact.

- Transmission Rate: A delay of 1000 μ s per bit provided the best trade-off between speed and stability.
- Error Handling: LabVIEW's signal logging helped identify bit drift, bounce, and misread intervals. Error rates were lowest in shielded environments with consistent ambient light.

LabVIEW plots displayed clean square-wave pulses for valid binary transmissions. Distorted or missing waveforms correlated with physical obstructions or improper wiring.

Despite its limitations in speed and range, the prototype effectively simulated an FTTH optical link using physical-layer VLC, validating its use in low-cost secure communication environments.

VII. CONCLUSION

This research demonstrates a robust and affordable approach to simulating secure Routing and Wavelength Assignment (RWA) in FTTH systems using visible light communication. The proposed system leverages widely available hardware and software tools to provide a hands-on understanding of optical communication, modulation techniques, and real-time signal analysis.

The inherent physical-layer security of VLC, combined with Arduino-based modular design and LabVIEW integration, allows for transparent and accurate message transmission. The system's educational value makes it ideal for teaching network security, optical signaling, and embedded development.

Moreover, the simplicity and accessibility of the hardware make this model a valuable reference for cost-sensitive deployments, including smart classrooms, rural communication systems, and prototyping platforms for optical research. The flexibility of VLC systems also opens opportunities for cross-disciplinary learning, integrating communication engineering with embedded systems and electronics.

Future extensions of this project could include:

- Integration of Wavelength Division Multiplexing (WDM) to allow multi-channel data transmission
- Implementation of encryption and decryption logic in software
- Use of precision lenses to expand transmission range
- AI-based routing decisions for dynamic wavelength switching
- Real-time mobile app integration for remote monitoring

With the ever-growing demand for high-speed and secure internet delivery, especially in remote and underserved areas, such modular optical communication setups can provide a foundation for scalable and energy-efficient network designs. This prototype thus contributes to the broader movement toward democratizing access to high-performance communication technology and promoting hands-on education in optical and embedded systems.

The system sets a foundation for more advanced research in embedded optical systems and encourages further innovation in secure, scalable, and sustainable FTTH models.

REFERENCES

- [1] M. Ali, S. Khan, and M. Qureshi, "Optimization of Routing and Wavelength Assignment in DWDM Networks," *Journal of Optical Networking*, vol. 12, no. 3, 2020.
- [2] A. Patel and A. Joshi, "Design Considerations for Secure FTTH Network Using PON," *International Journal of Communication Networks*, vol. 8, no. 2, 2021.
- [3] X. Li and W. Chen, "Visible Light Communication for Indoor Wireless Access: A Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, 2022.
- [4] Y. Zhang and H. Liu, "Securing Optical Networks Against Eavesdropping Attacks: A Review," *Optical Switching and Networking*, vol. 32, 2019.
- [5] S. Nair and R. Thomas, "Arduino-Based Optical Data Transmission Using Laser and Photodiode," *International Journal of Embedded Systems*, vol. 5, no. 4, 2023.
- [6] R. Sharma, A. Gupta, and M. Srivastava, "Photonic Switch Integration in Wavelength Assignment for Optical Networks," *Proceedings of the 2021 Optical Network Conference*, pp. 122–129, 2021.
- [7] G. Kaur and D. Verma, "AI-Assisted Dynamic Wavelength Assignment in FTTH Networks," *International Journal of Optical Communication Systems*, vol. 15, no. 2, 2022.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)