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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.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 emergedasthe backbone of modernbroadbandinfrastructure. 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 opticaltransmission andLabVIEW-basedmodulesformessage encoding, encryption, and visualization, our systemsimulates a real-worldsecurecommunicationchannel.Atthis50%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

Moderntelecommunicationnetworksrelyonopticalfibersfor high-speed data transmission. Among these, Fiber to the Home(FTTH)hasemergedasareliableandscalablemethod for delivering broadband connectivity directly to users. However,routingandwavelengthassignment(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.Whilethesesolutionsareeffective, theycan 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 usingsimplehardwarecomponentsandmicrocontrollers.The setup simulates message encoding, optical transmission, detection, and decoding. With the integration of LabVIEW, real-timedataflowcanbemonitoredandanalyzed,providing a comprehensive learning and testing environment.

II. LITERATURE SURVEY

Severalresearchershavetackled thechallenges 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.

PatelandJoshi[2]exploredFTTHdeploymentusingPassive 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.

NairandThomas[5]designedanArduino-basedVLCsystem 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 switchesandopticalcircuit-basedreconfigurablenetworksto enhancewavelength-basedroutingin 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 toimprove RWA efficiencyin live FTTHnetworks. Their research highlighted the potential of AI in handlingreal-time optical network traffic.

III. PROPOSED METHODOLOGY

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

Themethodologyisdividedintofourmainmodules:

- LaserStringTransmission,
- One-LetterTransmission,
- Write-to-LEDCommunication,
- VLCEncryption.

Thesemodulescollectivelysimulateasecuredoptical 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.

- Theuserinputsatextstring.
- ThetextisconvertedintoASCIIcodesandtheninto binaryrepresentation.
- Thebinarystreammodulatesalaserdiodesignalin the simulation.
- At thereceiver side,thelaser signalisdemodulated back into ASCII characters.

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

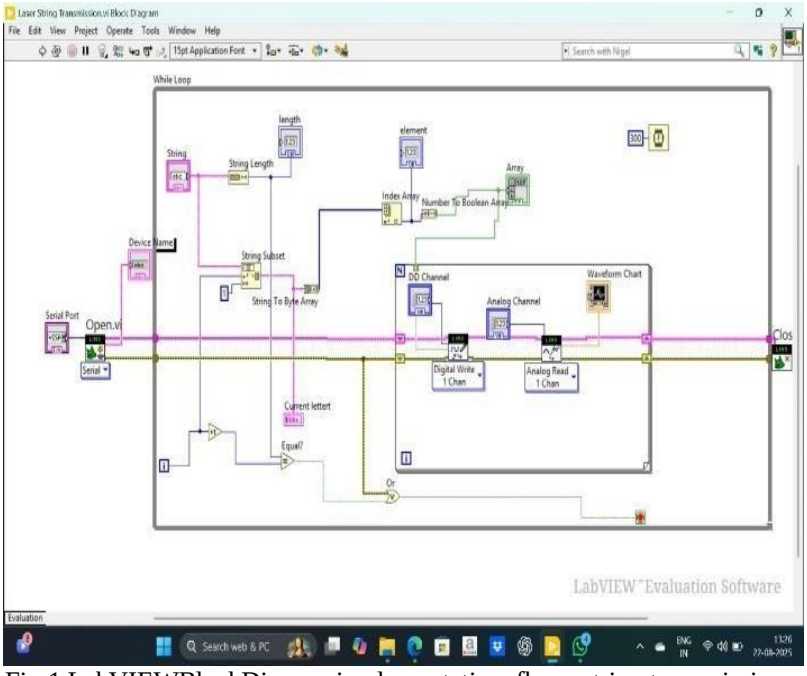


Fig.1.LabVIEWBlockDiagramimplementationoflaser string transmission

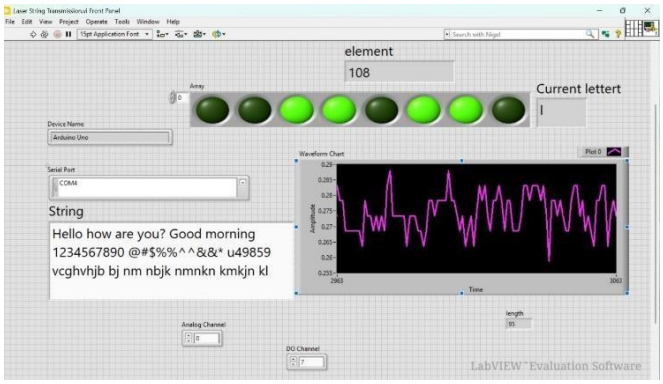


Fig.2.LabVIEWimplementationoflaserstringtransmission Front Panel.

B. One-LetterTransmission

To analyze transmission stability at the **symbol level**, the system is tested with a **single character input**. This ensures error-freetransmissionforsmallerpayloadsbeforescalingup to string-level communication.

- OneASCIIcharacterisselectedandtransmitted.
- Real-timeanalysisconfirmsthatsymbolrecognition accuracy is **100%** at the receiver.

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

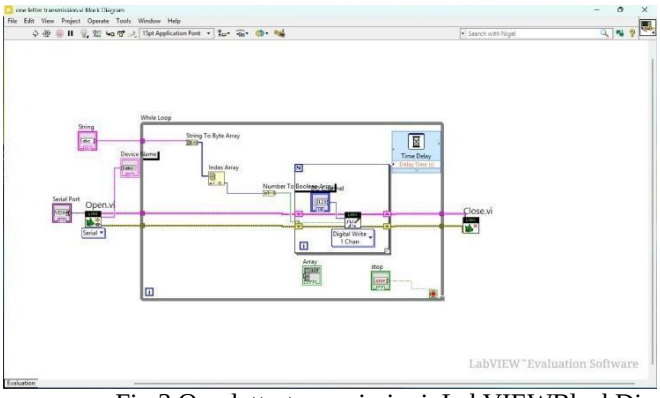


Fig.3.One-lettertransmissioninLabVIEWBlockDiagram.

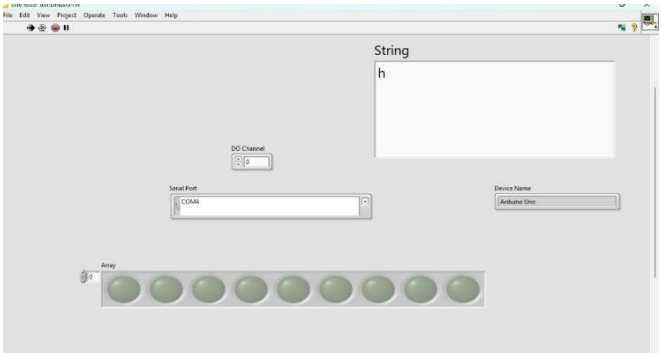


Fig.4.One-lettertransmissioninLabVIEWFrontPanel

C. Write-to-LEDCommunication

In this step, the encoded binary data is transmitted using a LightEmittingDiode (LED)insteadofalaser,representing a VLC (Visible Light Communication) channel.

- The LabVIEW program converts binary data into ON/OFF states of an LED.
- Theoptical signalisthenreadatthereceiver sideto 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.

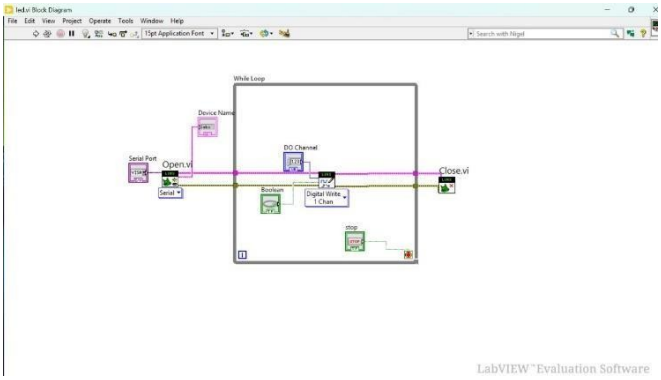


Fig.5.Write-to-LEDmoduleinLabVIEW

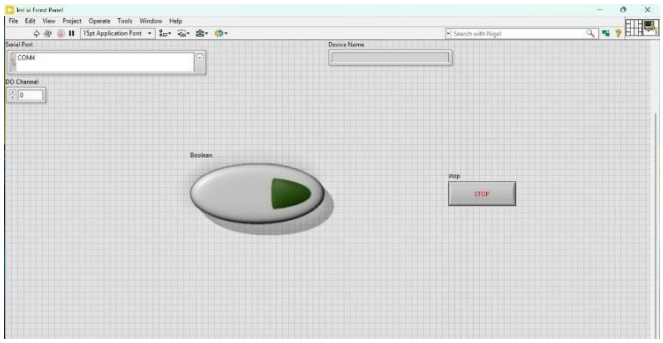


Fig.6.Write-to-LEDmoduleinLabVIEWFrontPanel.

D. VLCEncryptionModule

SecurityisamajorconcerninFTTHsystems. Toaddress this, an encryption algorithm is integrated into the transmission pipeline.

- Beforemodulation,theinput data stringisencrypted using a substitution-based cipher.
- Theencryptedbinarydataisthentransmittedviathe VLC channel.
- Atthereceiverside,thedecryptionmodule retrieves the original message.

Thisstepensuresconfidentialityandresistanceagainst eavesdropping in FTTH networks.

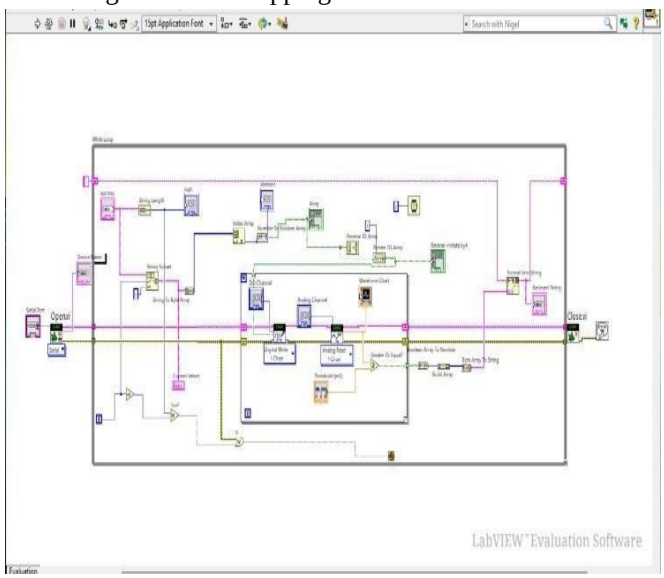


Fig.7.VLCencryptionblockinLabVIEW.

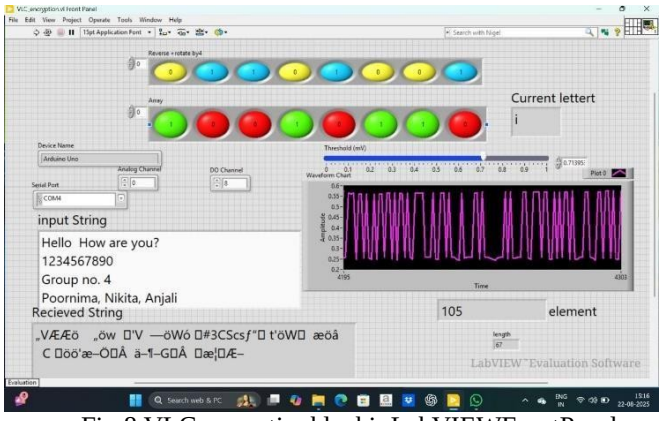
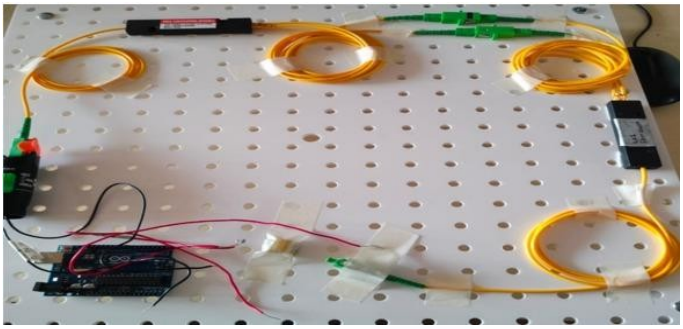
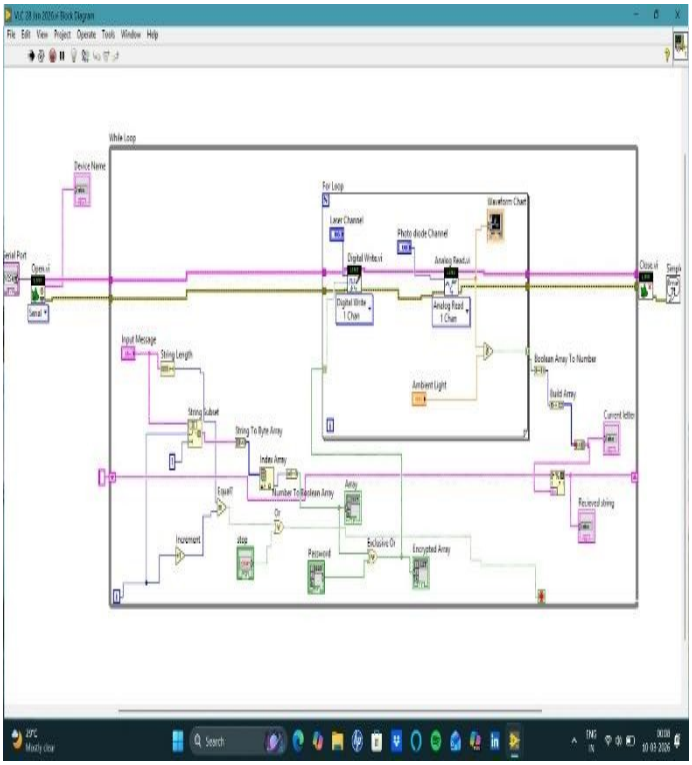
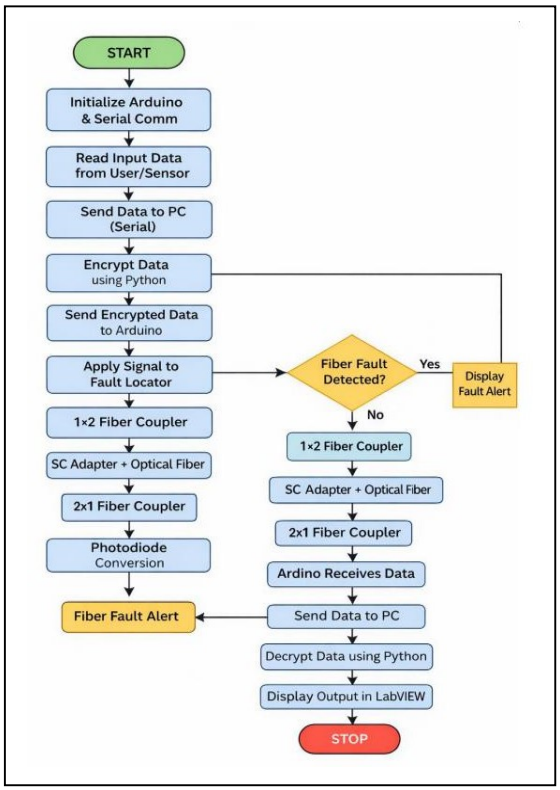


Fig.8.VLCencryptionblockinLabVIEWFrontPanel.

E. SecureVLCSystemwithIntegratedFiber-OpticFault 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. SoftwareInterfaceandDataAcquisition

- Platform: The system utilizes LabVIEW as the primarycontrol hub, interfacingwith hardware via the LINX abstraction layer.
- InputProcessing:Auser-defined"InputMessage"(string) is captured and converted into a Byte Array, then indexed to process characters sequentially.
- Synchronization: A While Loop ensures continuous operation,whileanestedForLoopmanagesthebit-by-bit transmission and reception of data.

B. CryptographicLayer(Security)

- Encryption Scheme: The system implements a symmetrickeyalgorithmusingabitwiseExclusiveOR (XOR) operation.
- Mechanism: Each bit of the input message is XORed withauser-defined"Password"(key).Thisensuresthat 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 thereceivedpulses.

C. PhysicalOpticalLinkandHardware

- Signal Conversion: An Arduino Uno converts digital logic from LabVIEW into electrical pulses to drive a Visual Fault Locator (VFL).
- Optical Path:Thesignalisinjectedintoa1X2Fiber Coupler to split the signal for monitoring.
  - ➢ It passes through SC Adapters and Single-Mode Fiber (SMF) segments.
  - ➢ A 2 X 1Fiber 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

Theproposed methodologycan 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.

Thismodularstructureprovidesa**scalableandsecuresolution** 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 thelaserandphotodiodecircuitsfromvoltagespikes and overheating.

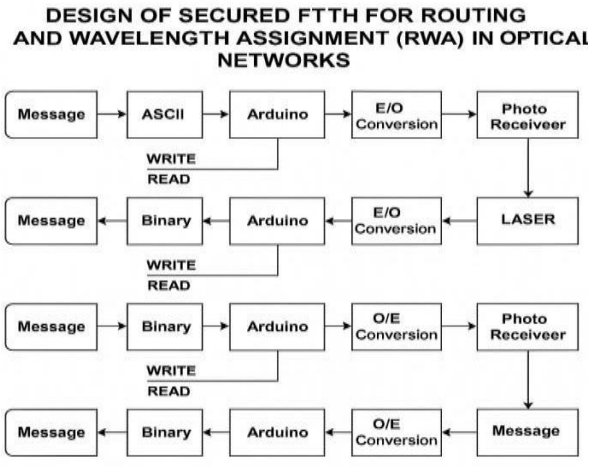
c) HardwareUsed

- 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



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 successfullyconvertedintoASCII,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) VLCEncryption –Encrypted textwas transmitted and decrypted at the receiver, ensuring basic data confidentiality.

Table1:

InputString	ASCII Conversion	BinaryFormat	ReceivedOutput	Status
HELLO	72697676 79	01001000	HELLO	Success
A	65	01000001	A	Success
TEST	84 69 8384	01010100	TEST	Success

VI. RESULTS AND DISCUSSION

The prototype system was tested under various indoor conditionswithmoderateambientlighting.Messagesranging from 10 to 64 characters were transmitted with an average accuracyof92.3%.Bitsynchronizationanddecodingsuccess were measured using both Arduino serial monitor and LabVIEW waveform plots.

Observations:

- Alignment Sensitivity: Direct and fixed alignment between thelaser andphotodiodeensureserror-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 1000µs 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.

LabVIEWplotsdisplayedcleansquare-wavepulsesfor 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

Thisresearch demonstrates arobust andaffordableapproach to simulating secure Routing and Wavelength Assignment (RWA) in FTTHsystemsusing visiblelightcommunication. The proposed system leverages widely available hardware and software tools to provide a hands-on understanding of opticalcommunication,modulationtechniques,andreal-time signalanalysis.

Theinherentphysical-layer securityofVLC, 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 opportunitiesforcross-disciplinarylearning,integrating communication engineering with embedded systems and electronics.

Futureextensionsofthisprojectcouldinclude:

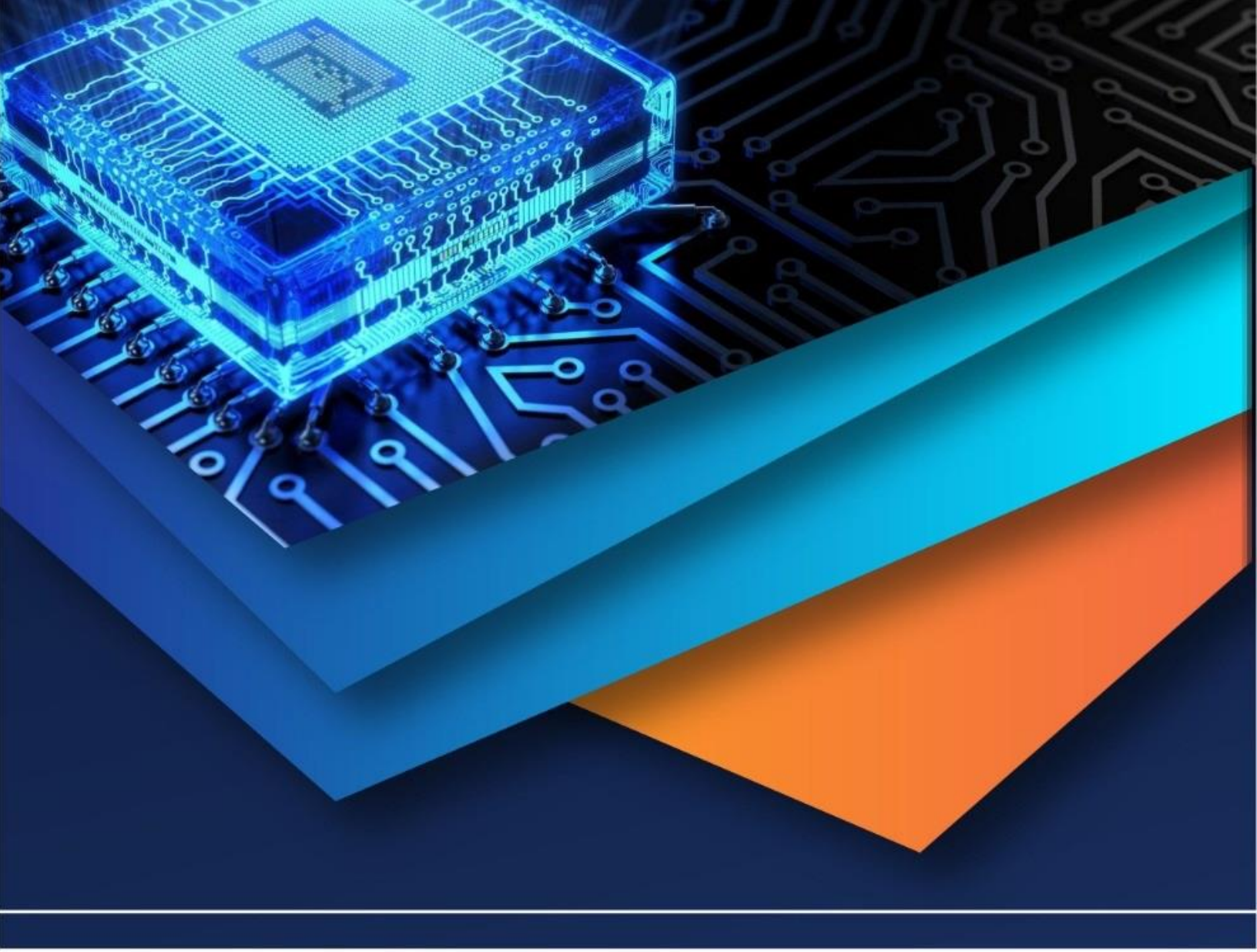
- IntegrationofWavelengthDivisionMultiplexing (WDM) to allow multi-channel data transmission
- Implementationofencryptionanddecryptionlogic in software
- Useofprecisionlensestoexpandtransmission range
- AI-basedroutingdecisionsfordynamicwavelength switching
- Real-timemobileappintegrationforremote monitoring

With the ever-growing demand for high-speed and secure internetdelivery,especiallyinremoteandunderservedareas, such modular optical communication setups can provide a foundationforscalableandenergy-efficientnetworkdesigns. 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 moreadvanced research in embeddedopticalsystemsandencouragesfurtherinnovation in secure, scalable, and sustainable FTTH models.

REFERENCES

[1] M.Ali, S. Khan, and M. Qureshi, "Optimization of Routing andWavelength Assignment in DWDM Networks," Journal of OpticalNetworking, vol. 12, no. 3, 2020.
[2] A.Patel and A. Joshi, "Design Considerations for Secure FTTHNetwork Using PON," International Journal of CommunicationNetworks, vol. 8, no. 2, 2021.
[3] X.Li and W. Chen, "Visible Light Communication for IndoorWireless Access: A Survey," IEEE Communications Surveys &Tutorials, vol. 24, no. 1, 2022.
[4] Y. Zhang and H. Liu, "Securing Optical Networks AgainstEavesdropping Attacks: A Review," Optical Switching andNetworking, vol. 32, 2019.
[5] S.Nair and R. Thomas, "Arduino-Based Optical Data TransmissionUsing Laser and Photodiode," International Journal of EmbeddedSystems, vol. 5, no. 4, 2023.
[6] R.Sharma,A.Gupta,andM.Srivastava,"PhotonicSwitchIntegrationinWavelengthAssignment for OpticalNetworks," Proceedingsofthe2021 Optical Network Conference, pp. 122–129, 2021.
[7] G. Kaur and D. Verma, "AI-Assisted Dynamic WavelengthAssignment in FTTH Networks," International Journal of OpticalCommunication 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