JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Performance Analysis of Multi Modulation System in Optical Network and Multi Encryption Security Algorithm

[1]Mamta Patankar, [2]Dr. Aditya Goel
[1]Research Scholar, [2]Professor
Department of Electronics and Communication Engineering,
Maulana Azad National Institute of Technology, Bhopal, India

Abstract : Optical communication network provides the high speed data transmission with the advance digital modulation and enhanced security. The cryptography is also a science to secure the data during the long distance transmission. This paper presents the multi encryption approach based on the advance encryption standard and RSA approach as very high security algorithm and multi modulation technique to improve the data safety during the communication in optical network. The Limb Mach Zehnder Modulator is used for the optical digital modulation. Digital modulation provides the digital data security during the data transmission. The multi modulation stands the modulation of the already modulated signal. The designing and analysis of the multi modulation is performed using Optisystem-7.0 software and cryptography based multi encryption algorithm implement and simulate using the MATLAB 9.4 software**.**

***IndexTerms* - Optical, Cryptography, MATLAB, Limb Mach Zehnder, Modulation, RSA, AES.**

I. Introduction

An optical organization is a correspondence framework that utilizations light signals, rather than electronic ones, to send data between at least two focuses. The focuses could be PCs in an office, enormous metropolitan communities or even countries in the worldwide media communications framework. Optical organizations include optical transmitters and beneficiaries, fiber optic links, optical switches and other optical parts. Optical and electronic organizations can take a few distinct structures. Highlight point networks create lasting associations among at least two focuses so any pair of hubs can speak with one another; highlight multipoint networks broadcast similar signals all the while to a wide range of hubs; exchanged organizations like the phone framework incorporate switches that make transitory associations among sets of hubs.

Optical code division multiple access (OCDMA) has been perceived as quite possibly the main advances for supporting numerous concurrent clients in shared media, and at times can expand the bandwidth of an optical fiber. OCDMA has unmistakable highlights that incorporate chance of full nonconcurrent correspondence, upgraded security and a delicate variety of the framework properties to the quantity of clients. In any case, for inappropriately planned codes, the greatest number of synchronous clients and the exhibition of the framework can be truly restricted by the crosstalk from different clients. Thus, different code families have been proposed, from the one-dimensional (1D) optical symmetrical code (OOC) to the new two-dimensional (2D) codes.

In Code Division Numerous Entrance has been broadly utilized as a multichannel access innovation in remote organizations, for example, the mobile phone framework for quite a while due to its strength to multiuser impedance and smooth debasement under substantial burden. Its utilization on an optical connection has been concentrated widely. Nonetheless, a few concerns have been communicated about the utilization of spread range on an optical connection Be that as it may; a few concerns have been communicated about the utilization of spread range on an optical connection because of low organization throughput. The essential distinction among remote and optical CDMA is that optical fiber is force medium. A beat of light is utilized to communicate a sign.

Code-division different access (CDMA) is a spread range procedure, which has been well-informed and executed in portable radio correspondences utilizing electrical sign preparing. In this methodology every collector on the organization is relegated a one of a kind 'address' grouping that is roughly symmetrical to the arrangements allocated to any remaining recipients. Information pieces to be communicated are then balanced by the doled out succession of the focused on beneficiary prior to being sent. The focused on beneficiary thusly identifies the approaching information by associating it to its own 'address' arrangement. It is (Hence, making it) feasible for various clients to at the same time access the organization as long as the absolute amount of the cross-relationships of the roughly symmetrical successions to the focused on recipient isn't extreme.

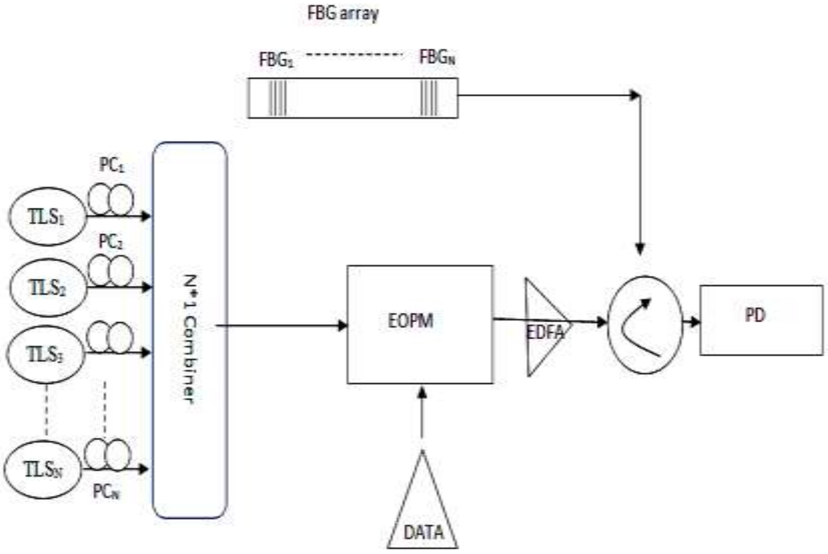


Figure 1: Bipolar encoding system

The exploratory chart of the proposed bipolar encoding framework is appeared in Fig. 1 was reproduced mathematically utilizing MATLAB and OptiSystem bundle. The encoding activity is to plan low piece rate electrical information grouping to a high piece rate optical information succession with a particular code for every client. In our proposed encoding framework, the light waves from a laser exhibit with N frequencies are stage regulated by a low piece rate electrical information succession at an EOPM and afterward shipped off a FBG cluster that comprises of N uniform FBGs, with every frequency being situated at the left or right incline of the comparing FBG.

Cryptography is an information security tactic used to protect enterprise information and communication from cyber threats through the use of codes. Cryptography achieves several information security-related objectives including confidentiality, integrity, and authentication, and non-repudiation.

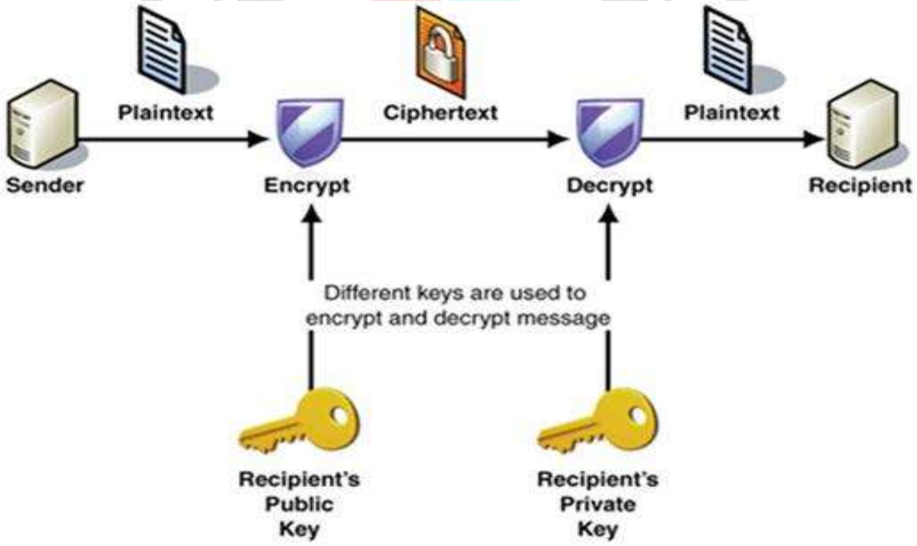


Figure 2: Cryptography Process

Cryptography provides for secure communication in the presence of malicious third-parties known as adversaries. Encryption uses an algorithm and a key to transform an input (i.e., plaintext) into an encrypted output (i.e., ciphertext). A given algorithm will always transform the same plaintext into the same ciphertext if the same key is used. Algorithms are considered secure if an attacker cannot determine any properties of the plaintext or key, given the ciphertext. An attacker should not be able to determine anything about a key given a large number of plaintext/ciphertext combinations which used the key.

II. METHODOLOGY

The objective of this work is to design an optical network based multi modulation system. The work also includes the performance analysis of multi encryption cryptography system with use of AES and RSA methods. There are various parameters which can be varied to analyze the security check. This work focuses on methods to improve the bit-error-rate (BER) performance of multi modulation optical system. For this limb mach zehnder modulator that is optical modulation techniques have been proposed as a modulation schemes

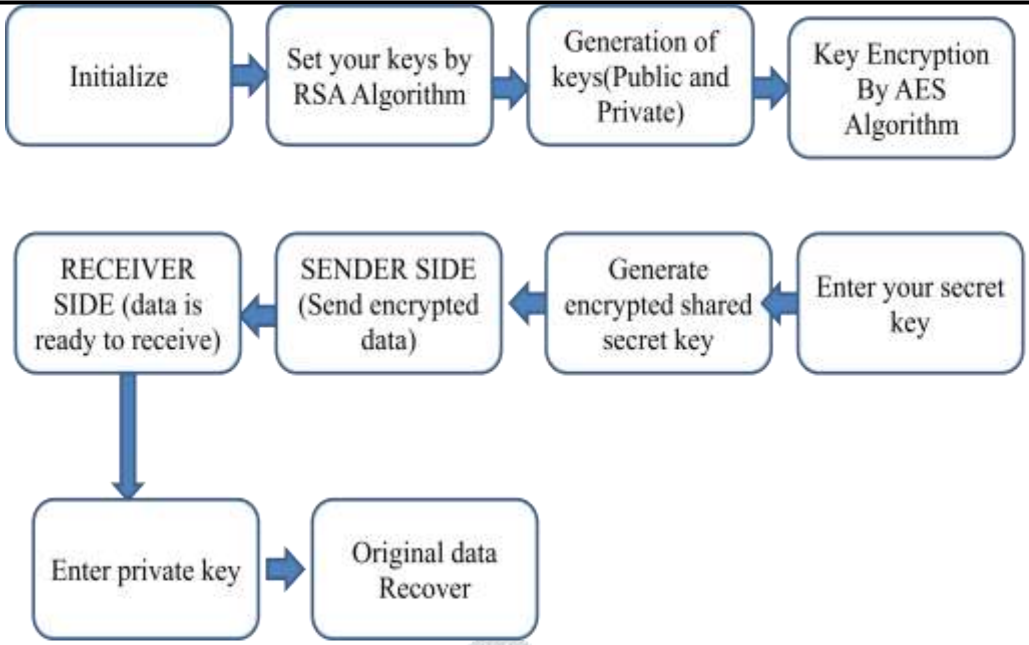

Initialize
Set your keys by RSA Algorithm
Generation of keys(Public and Private)
Key Encryption By AES Algorithm
Enter your secret key
Generate encrypted shared secret key
SENDER SIDE (Send encrypted data)
RECEIVER SIDE (data is ready to receive)
Enter private key
Original data Recover

Figure 3: Flow Chart

Steps-

1. Take the input data of any multimedia.
2. Now apply the proposed cryptographic based asymmetric RSA algorithm.
3. It generates the public and private key.
4. Now apply the advance encryption standard algorithm (AES) and secure the RSA key with the AES encryption key.
5. Now create the secret key.
6. Multi encryption process generates the encrypted shared key.
7. This encrypted shared key encrypts the input data.
8. Receiver accepts this image but for decryption provide the RSA private key.
9. Now the original data recovered and calculate the performance parameters.

III. RESULTS AND DISCUSSION

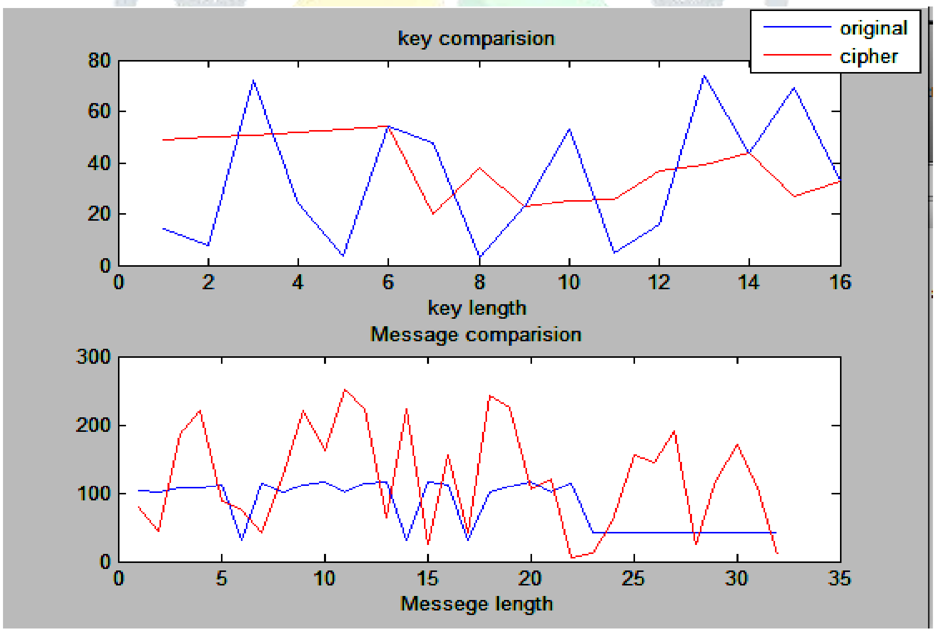


Figure 4: Graph of Original key Vs Cipher key

Figure 4 showing the comparison of original key and cipher key. The cipher key vs original key, where blue color line show original key and red color line show cipher key.

Table 1: Result compare of all algorithms with proposed approach

Input Size(bytes)	Method	Simulation Time(seconds)		Throughput	
		Encryption	Decryption	(Encryption)	(Decryption)
512	AES	0.0981	0.1531	9133.5	5852.4
512	RSA	0.5362	0.5613	1671.1	1596.3
512	Proposed Method	0.1146	0.1144	7818.5	7859.7

Table 1 is showing the simulation time and throughput value of cryptography based algorithm. It is clear from the simulated results the proposed (hybrid cryptography) approach gives better results than existing.

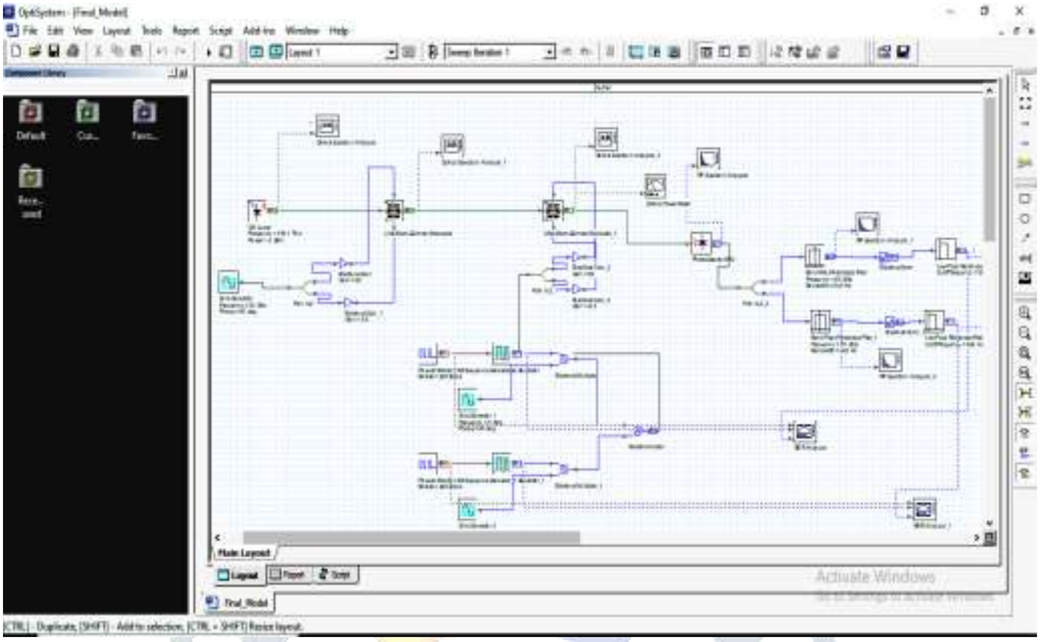
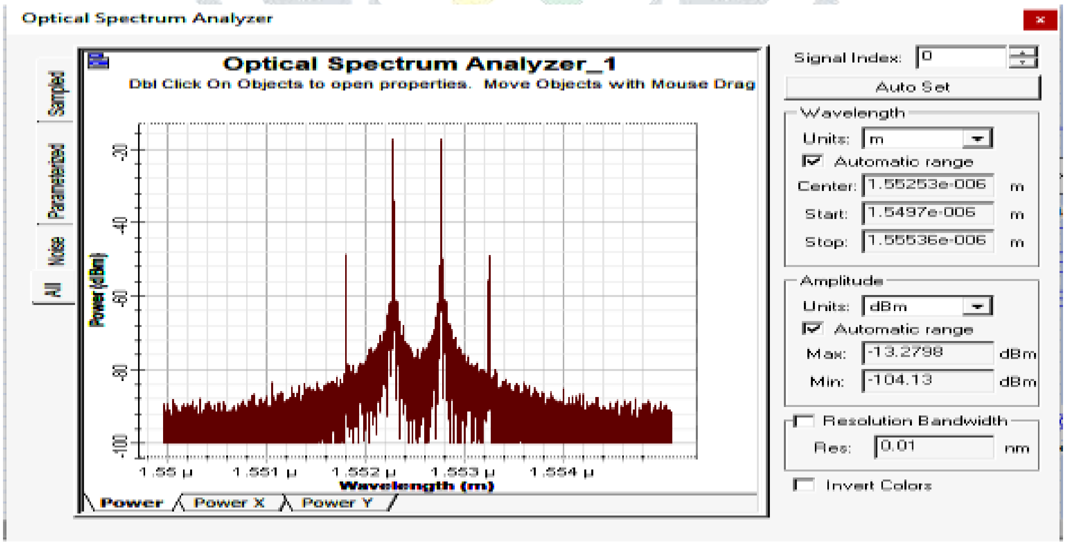


Figure 5: Optical model in software environment

Figure 5 demonstrate the proposed Optical Model. Let’s consider the Sine that generates in the model and the continuous Wave laser which emits a laser beam that is continuous in nature with the controlled heat output, as intensity and beam duration.



Signal Index: 0

Auto Set

Wavelength

Units: m

☑ Automatic range

Center: 1.55253e-006 m

Start: 1.5497e-006 m

Stop: 1.55536e-006 m

Amplitude

Units: dBm

☑ Automatic range

Max: -13.2798 dBm

Min: -104.13 dBm

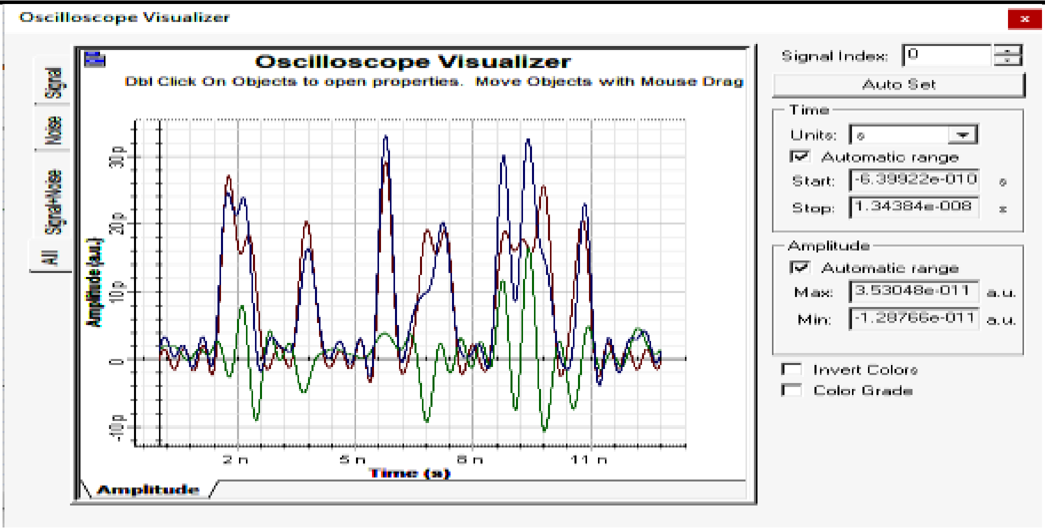
□ Resolution Bandwidth

Res: 0.01 nm

□ Invert Colors

Figure 6: Power analysis using optical spectrum analyzer

Figure 6 is showing the power analysis using optical spectrum analyzer the minimum power is -100db and maximum power value is -18db. This spectrum is generated by the modulation process of the waveform generated by the CW laser block and sine generator. The limb mach zehnder modulator is used for the modulation.



Signal Index: 0

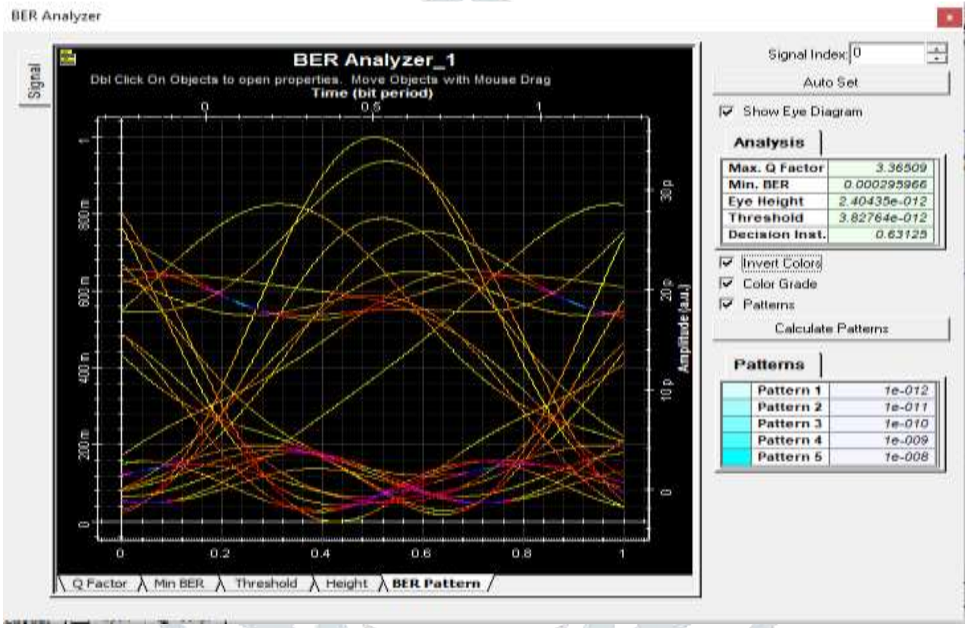
Time
Units: s
☑ Automatic range
Start: -6.39922e-010 s
Stop: 1.34384e-008 s

Amplitude
☑ Automatic range
Max: 3.53048e-011 a.u.
Min: -1.28766e-011 a.u.

□ Invert Colors
□ Color Grade

Figure 7: Oscilloscope Visualize

Figure 7 is showing the signal amplitude level after the complete process. The signal duration is 11ns and amplitude is 30 a.u.



Signal Index: 0

☑ Show Eye Diagram

Analysis

Max. Q Factor	3.36509
Min. BER	0.000295966
Eye Height	2.40435e-012
Threshold	3.82764e-012
Decision Inst.	0.63125

☑ Invert Colors
☑ Color Grade
☑ Patterns

Patterns

🟦	Pattern 1	1e-012
🟦	Pattern 2	1e-011
🟦	Pattern 3	1e-010
🟦	Pattern 4	1e-009
🟦	Pattern 5	1e-008

Figure 8: BER analyzer pattern with eye diagram.

Figure 8 is showing the waveform in various patterns with eye diagram. The simulation values are showing in the analysis table in figure.

Table 2: Simulation Parameters

Sr No	Parameter	Value
1	CW laser frequency	193.1 THz
2	Sine wave generator	30 GHz
3	Optical transmitted power	-3 dBm
4	Optical transmitted power	18 dBm
5	Line width	10MHz
6	Modulation format	MZM
7	Phase	0 and 90 degree
8	Threshold	5.03776e-012
9	Decision inst.	0.503125

In table 2, simulation parameters are showing which is taken during the execution of optical model.

Table 3: Comparison chart of proposed work with previous work results

Sr No.	Parameters	Previous work	Proposed Work
1	Cryptography Method	AES	RSA + AES
2	Modulation	Single	Multi
3	Q Factor	Not Mention	2.60
4	Min BER	Not Mention	0.0032
5	Eye Height	22	-3.20433e-012
6	Optical transmitted power	0 dBm	-3 dBm

Table 3 is showing the comparison of proposed and previous work results. Proposed approach used the hybrid cryptography approach to secure the data. The multi modulation technique is applied.

IV. CONCLUSION

This paper proposed the implementation of the multi encryption security algorithm based on cryptography and multi modulation system on optical network model. The limb mach zehnder modulator based modulation schemes are used on Optisystem-7.0 software. Analysis of the designed system has been done on the basis of the performance parameters i.e. Q-factor, BER, Eye height. A multi modulation study has been done for the MZM modulation schemes and it is found that it is better modulation schemes which perform significant improved. Therefore, this research work is concluded that that the multi encryption cryptography gives the significant improved results than single AES and RSA and multi modulation provides better digital signal performance in terms of safety BER, Q-factor etc., instead of single modulation.

REFERENCES

[1]. J. Ji, W. Li, B. Wu, K. Wang, M. Xu and L. Sun, "Design and Investigation on Image Transmission in Multi-User Cross-Layer Security Network," in IEEE Access, vol. 7, pp. 132066-132073, 2019, doi: 10.1109/ACCESS.2019.2940057.

[2]. Z. Wang, "Secure Image Transmission in Wireless OFDM Systems Using Secure Block Compression-Encryption and Symbol Scrambling," in IEEE Access, vol. 7, pp. 126985-126997, 2019, doi: 10.1109/ACCESS.2019.2939266.

[3]. Z. Wang and J. Lv, "Secure Image Transmission in Orthogonal Frequency Division Multiplexing Visible Light Communication Systems," in IEEE Access, vol. 7, pp. 107927-107936, 2019, doi: 10.1109/ACCESS.2019.2932908.

[4]. L. Li et al., "Exploiting Optical Chaos for Color Image Encryption and Secure Resource Sharing in Cloud," in IEEE Photonics Journal, vol. 11, no. 3, pp. 1-12, June 2019, Art no. 1503112, doi: 10.1109/JPHOT.2019.2919576.

[5]. C. Yang, H. Wu and S. Su, "Implementation of Encryption Algorithm and Wireless Image Transmission System on FPGA," in IEEE Access, vol. 7, pp. 50513-50523, 2019, doi: 10.1109/ACCESS.2019.2910859.

[6]. W. Xingyuan and Z. Hongyu, "Cracking and Improvement of an Image Encryption Algorithm Based on Bit-Level Permutation and Chaotic System," in IEEE Access, vol. 7, pp. 112836-112847, 2019, doi: 10.1109/ACCESS.2019.2935017.

[7]. X. Zhang and X. Wang, "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem," in IEEE Access, vol. 6, pp. 70025-70034, 2018, doi: 10.1109/ACCESS.2018.2879844.

[8]. X. Fu, B. Liu, Y. Xie, W. Li and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," in IEEE Photonics Journal, vol. 10, no. 3, pp. 1-15, June 2018, Art no. 3900515, doi: 10.1109/JPHOT.2018.2827165.

[9]. M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615.

[10]. H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang and D. Wang, "Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks," in IEEE Transactions on Biomedical Circuits and Systems, vol. 11, no. 3, pp. 558-573, June 2017, doi: 10.1109/TBCAS.2017.2665659.

[11]. M. Kar, M. K. Mandal and D. Nandi, "RGB image encryption using hyper chaotic system," 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), Kolkata, 2017, pp. 354-359, doi: 10.1109/ICRCICN.2017.8234534.

[12]. Y. Xie, J. Li, Z. Kong, Y. Zhang, X. Liao and Y. Liu, "Exploiting Optics Chaos for Image Encryption-Then-Transmission," in Journal of Lightwave Technology, vol. 34, no. 22, pp. 5101-5109, 15 Nov.15, 2016, doi: 10.1109/JLT.2016.2606121.

[13]. Y. Lee and W. Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 4, pp. 695-703, April 2014, doi: 10.1109/TCSVT.2013.2283431.

[14]. H. Wang, D. Peng, W. Wang, H. Sharif and H. Chen, "Image transmissions with security enhancement based on region and path diversity in wireless sensor networks," in IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 757-765, Feb. 2009, doi: 10.1109/TWC.2009.070769.

[15]. L. Guo-wei, Z. Ming-jie and G. Dong-hui, "STBC-MIMO Communication System for Image Encrypt via CNN," 2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID), Xiamen, Fujian, 2007, pp. 270-274, doi: 10.1109/IWASID.2007.373742.