Telecommunication of a Secure Data in Optical Fiber

Arwa A. Moosa,(Asst.Lecturer)* May H.Abood,(Asst.Lecturer)*

Abstract

One of the most important issue in networking is the tremendous demand for a huge bandwidth with a great security. Optical network is an efficient telecommunications networks used to transfer data with great facilities. To provide an additional capacity for higher bandwidth, different frequencies and longer distance, optical Dense Wavelength Division Multiplexing (DWDM) and Erbium-Doped Fiber Amplifiers (EDFA) will be used. To transfer data securely, an important encryption method RC4 will be used to protect data on the common channel as it's cryptographic technique is faster, simpler to implement and the keystream is a arbitrary sequence of bits which guarantees the security of used cipher. MATLAB program will used to encrypt and decrypt the image with transferring it optically by Optisystem simulation program.

Keyword : Fiber optic, DWDM, Image encryption, RC4, stream ciphers, keystream generator, lasers, Matlab Optisystem communication programs.

*Al Iraqiya University

1.Introduction

Fiber optics is a prime base in the telecommunication structure. Its high transfer speed capacities and low lessening attributes to be perfect for huge data transmission [1]. Optical fiber communication system is the same of any communication system as shown in figure (1), which is consist of transmitting side consist of optical source and modulator to modulate the data from the source, then transmit it through the transmitting medium (optical fiber), and receiving side consist of detector and demodulator at the destination point [2].

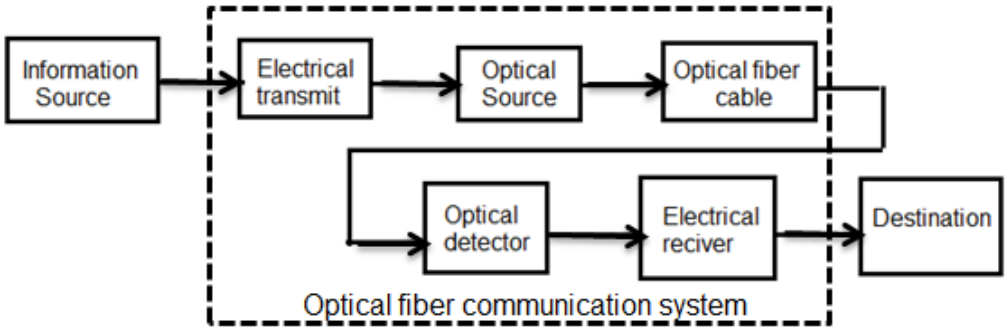


Fig.1 : The optical fiber communication system

The data send from the source was encrypted using RC4 stream cipher technique that is most important popular symmetric encryption technique because of its simplicity, pace and performance in which bits are infeasible because of the large memory constraints and the operations of the key schedule technique. It can be applied to many security applications in real time security such as protocol standards that have benefits of it to make networks secure like WPA, SSL, and WEP.

In proposed stream ciphers, A keystream is created in a technique which produce an arbitrary sequence of bits. A plaintext is transformed to ciphertext of same size of plaintext by concealing the plaintext with a created keystream, utilizing a simple XORing operation. The encryption

algorithm strength is the arbitrary keystream which guarantees the the stream cipher computational security [3].
In this paper, optical fiber was proposed as transmitting media to a encrypted data. The image was modulate and demodulated with a different distance and designs were implemented using Matlab and Optisystem simulation programs, as the image was encrypted by Matlab then transfer it to Optisystem using Matlab-Optisystem communicator to modulated with an optical source and send it to optical fiber. At the receiver side the image was detect using photodetector and demodulate and again sent to Matlab program using Optisystem-Matlab communicator to decrypt to its original image and review the image at the receiving side.

2. Methodology

2.1 Signal analysis

Optical fiber system consist of three parts, transmitter that convert the electrical signal to optical ,optical fiber cable carrying the optical signal , and finally the receiver which convert it to electrical signal again[4][5].

The signal pass through the optical fiber is under attenuation effect. Attenuation is the amount of losing in light power or signal strength that happen in the optical fiber as light pulses propagate through it. The signal attenuation can be measured typically in dB/km or decibels by comparing the two power level, the ratio between the input and the output power per length unit as shown in equation (1)[6]:

$$\alpha_{dB} \mathrm{L} = 10 \log \mathrm{Pi/Po} \qquad \ldots\ldots (1)$$

where α_{dB} is signal attenuation in dB ,L is the fiber length, and Pi Po is the input power and the output power sequentially[6].
To measure the quality of the data in the optical link Bit error rate (BER) is used to compare the quality of different systems for data transmission [7], BER can be defined by the equation (2) [8]:

$$\mathrm{BER} = \mathrm{erfc}(\mathrm{Q}/\sqrt{2})/2 \ldots\ldots\ldots \quad (2)$$

where the Q-factor is determined by:

$$Q = \frac{A_1 - A_0}{\sigma_1 - \sigma_0} \qquad \ldots\ldots\ldots \quad (3)$$

Here $A_1 and A_0$ are the electrical current with low-pass filter in sampling time for spaces and marks, sequentially, $\sigma_1 \text{and } \sigma_0$ are considered as a stander deviations. In the integrate-and-dump receiver, the Q-factor can be defined as the signal to noise ratio, SNR = $(A_1 - A_0)/ A_0$, by [8]:

$$Q = \frac{SNR \sqrt{2TB_{opt}}}{1+\sqrt{1+2*SNR}} \quad \ldots\ldots\ldots\ldots \quad (4)$$

where T is the bit interval and B_{opt} is the bandwidth of the rectangular optical filter [8].

To manipulate signal attenuation, Dense wavelength-division multiplexing (DWDM) with erbium-doped fiber amplifiers (EDFA) has been utilized to raise the data-rate to (>1000 Gb/s) over 100Km distance [9].

2.2 Wavelength-division multiplexing (WDM)

(WDM) is an algorithm requiring that every end-client's hardware work just at electronic rate, however numerous WDM channels from various end-clients might be multiplexed on the same fiber and they can use same frequency or different frequencies supporting a single communication channel as shown in figure 2. WDM permitting different data to coincide on a single optical fiber, thus it can tap into a huge bandwidth, by using a demultiplexer (demux) the receiving signal can be separates out to a streams of data to a multi –user. EDFA amplifier employing for long-haul optical communication due to its ability to amplify the carried signal on fibers [10] .

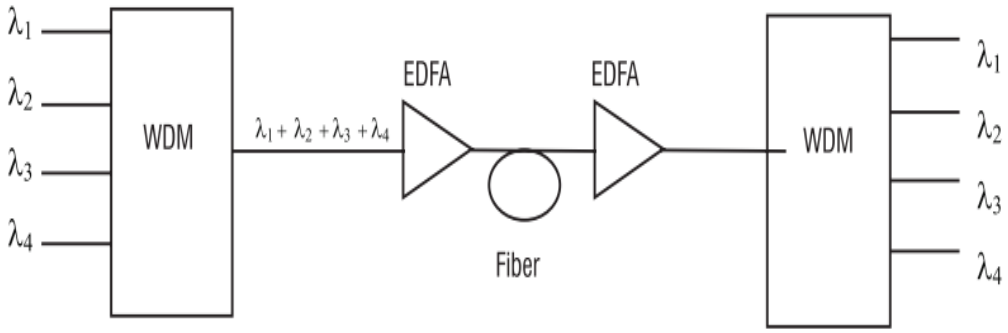


Fig. 2: Wavelength-division multiplexing

The DWDM is working with a multiple closely wavelength to send different data on the same optical fiber line. The International Telecommunications Union (ITU) realize ∆f spacing of frequency equal to 100 GHz, therefore ∆λ should equal to 0.8-nm spacing of wavelength from equation (5) [9].

$$\Delta\lambda = \frac{\lambda\,\Delta f}{f} \qquad \ldots\ldots \quad (5)$$

Therefore the DWDM systems operate with wavelength of 1550-nm due to the low glass attenuation characteristics and due to the fact that the EDFA amplifier can operate in wavelengths between 1530-nm–1570-nm[9].

2.3 RC4 stream cipher algorithm

Stream ciphers are utilized in applications with low delay and high speed requirements. Though most stream ciphers depend on linear feedback shift registers, the software-oriented implementation of stream ciphers has led to many alternative ideas. One of the favorable techniques, RC4, introduced by R. Rivest in RSA incorporated of Data Security.RC4 has been incorporated to numerous mercantile products like Lotus Notes and BSAFE, and it's considered in forthcoming standards like TLS [11].

The proposed system identified and implement RC4 algorithm. the abbreviation of RC4 is "Ron's Code 4" or "Rivest Cipher 4" [12]. It uses a variable key length which can range between 1- 256 bytes (8 - 2048 bits) and is utilized to initialize a state vector S of 256 byte. The key stream is totally independent of the plaintext. The state table utilized to produce subsequent creation of arbitrary bits that is XORed with plaintext to produce the ciphertext[13].

General Model of RC4 Stream Cipher

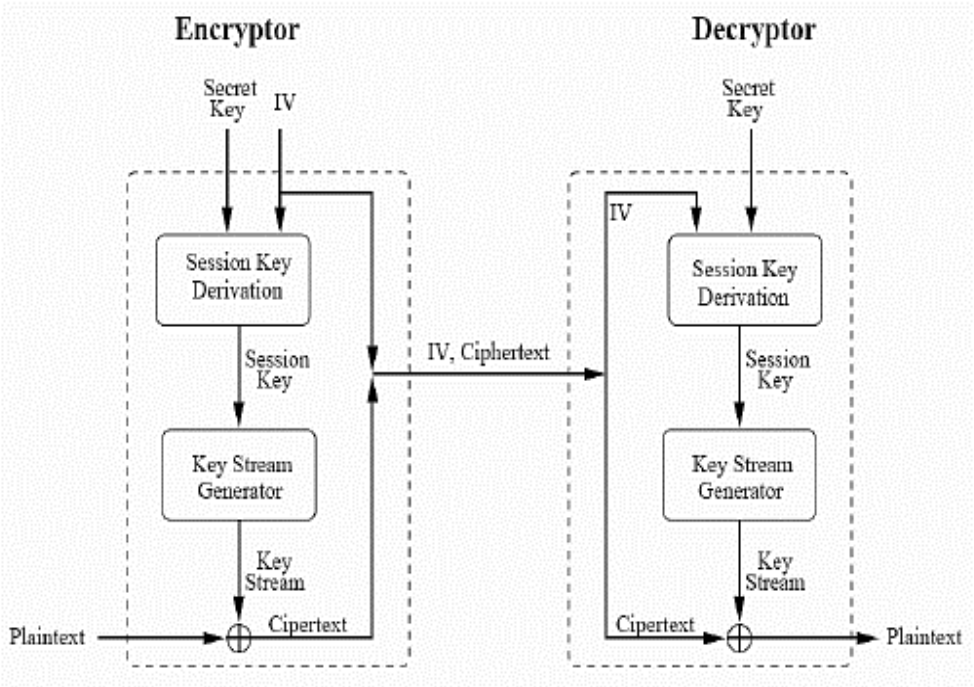


Fig. 3 : General Model of RC4 Stream Cipher

RC4 provides the following architectural choices[14]:

- RC4 state is very large, in compared with previous stream cipher proposals.

- The major part of the state S is a 256 byte array that perform a permutation of ZN = {0,1; … ,N }.

- Fast update and output
- RC4 cipher is suitable for any value of N > 2
- The length of supplied key is random (up to 256 bytes).
- Key execution technique is intended to be hard to invert, it must be difficult to reconstruct the key.
- Next state function is invertible, this make some guarantee the large period of the next state function.
- Output function of the current state is a complex function.

3. Design and Consideration

Optical Fiber is a low attenuation system Characterized by its long distance signal transmission with secure large bandwidth data[1].Our proposed algorithm for transmitted data security is RC4 stream cipher.

In RC4 encryption algorithm, the encryption process consists of two Algorithms namely Key Scheduling Algorithm (KSA) and Pseudo Random Generation Algorithm (PRGA) to produce the keystream of the stream cipher.

Algorithm 1. (KSA)

The **KSA** is utilized to initialize the array "S". Key length is the number of bytes of used key and can be in the range 1B to 256B. The array "S" is generated to the identity alteration and then enters to 256 iterations that will mix with the used key.

KSA Input: K[K_1, K_2,…. K_l],m
KSA Outputs: S
S[i]=i, i =0,1,2,3,…,255
j = 0
For i = 0 to 255 D_0
j = (j+S[i]+K[i mod L]) mod 256
Swap S[i] and S[j]
Return (S)

Algorithm 2. (PRGA).

the PRGA changes the state and gives a byte of the key sequence. For all iterations, the PRGA accounts *i* , output to the *ith* values of *S* (*S*[*i*]), and adds it to *j* . Then swap *S* [*i*] with *S* [*j*]. and utilize the summation *S*[*i*]+*S*[*j*] (mod 256) to get a third value of S, then S value will *XORed* with the following byte of plaintext to output the next byte of plaintext or cipher text. Each value of S is exchange with other value one time at least for each "256" iterations.

PRGA Input: S
PRGA Output: Key sequence K_{seq}
i = 0
j = 0
While sequence not end Do
i = (i+1) mod 256
j = (j+S[i]) mod 256
Swap S[i] and S[j]
K_{seq} = S[(S[i]+ S[j]) mod 256]
Return (K_{seq})

The two used algorithms output a stream of random values. These values is XORed with the input stream, bit by bit. Due to the symmetrical encryption process and decryption process, the data stream is XORed with the produced key sequence.

In this paper,RC4 design is implemented for image cryptography by select an image as input and applying the proposed method to encrypt

the image to produce encrypted image. By implementing the same method we will decrypt the encrypted image. The original image can be got back at the end of this step. Figure 4 showing the overall procedure.

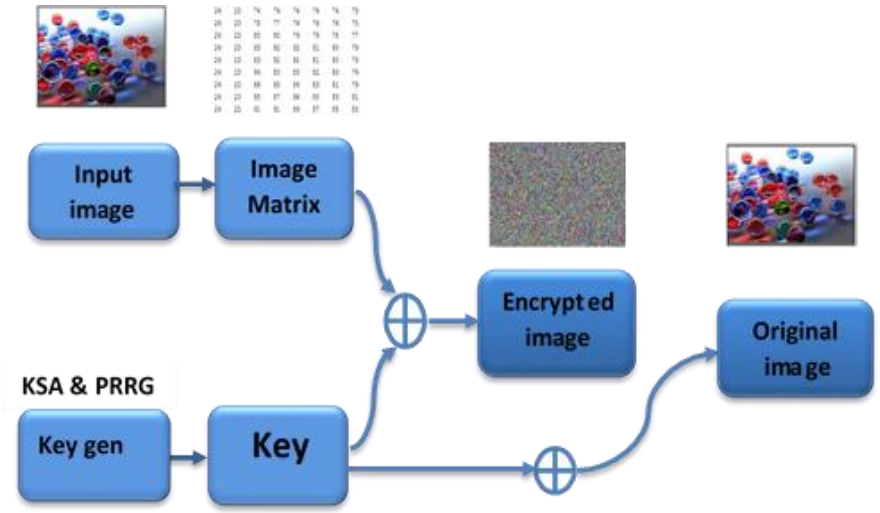


Fig.4: Procedure of Encryption & Decryption algorithm

The design of the essential concepts and the devices that were used in the secure optical fiber system utilized optical communication designed in “Optisystem™” program as shown in figure 5. The system was connected with its both sides, transmitter and receiver, to Matlab program using Matlab-Optisystem communicator to transfer the encrypted image for an additional system security.

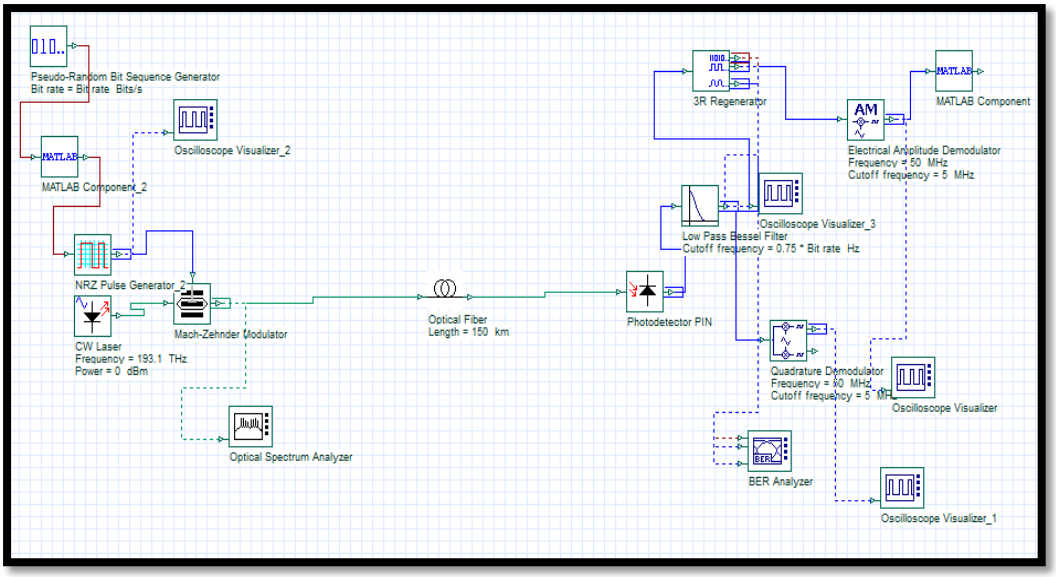


Fig. 5: One channel Optical Fiber system components in"*Optisystem*™"

Table1: Optical Fiber system components used in *Optisystem*™

Input data	Pseudo – random bit sequence generator
	Matlab componant
Transmitter part	NRZ pulse Generator
	CW laser
	Mach-Zehner Modulator
Transmitting Media	Optical Fiber
Receiving part	Photodetector PIN
	Low pass Bessel filter
	3R Regenerator
	Electrical Amplitude Demodulator
	Quadrature Demodulator

Data out	Matlab component
Measurements component	Oscilloscope Visualizer
	Optical Spectrum Analyzer
	BER Anlyzar

As shown in figure 5 and table1, Optical fiber system is consisted of three part:

Transmitting part: To transmit the encrypted image , a pseudo-random bit generator was used as an input to Matlab program to generate the encryption. Using Matlab- Optisystem communicator the encrypted image was transfer to optisystem program ,consist of continuous wave (CW) diodes laser and non-return-to-zero (NRZ) pulse generator where it acts as the carrier source to the image with wavelength of 1550nm, Finally the encrypted image modulated using Mach-Zehnder modulator .

Transmitting Media: Optical fibre

Receiving part: low-pass Gaussian filter and PIN photodiode detector were utilized in the received side, which it cause to reduce the time jitter and the traveling-wave electron absorption modulator (TW-EAM) switch window loss[10]. Two type of demodulators have been used electrical amplitude demodulator and Quadrator demodulator , the output of these demodulators was transfer to Matlab using Optisystem- Matlab communicator to receive the final unencrypted image.

Several Optical spectrum analyzers and oscilloscopes have been used as a signal visualizer.

In this research, performance comparison is handled for the previous design that have one fiber channel with another design having DWDM with EDFA amplifiers as shown in figure6. The new design constructed with a WDM MUX 2×1 with two EDFA amplifiers of loss 0.1dB/m and WDM DMUX 2×1.

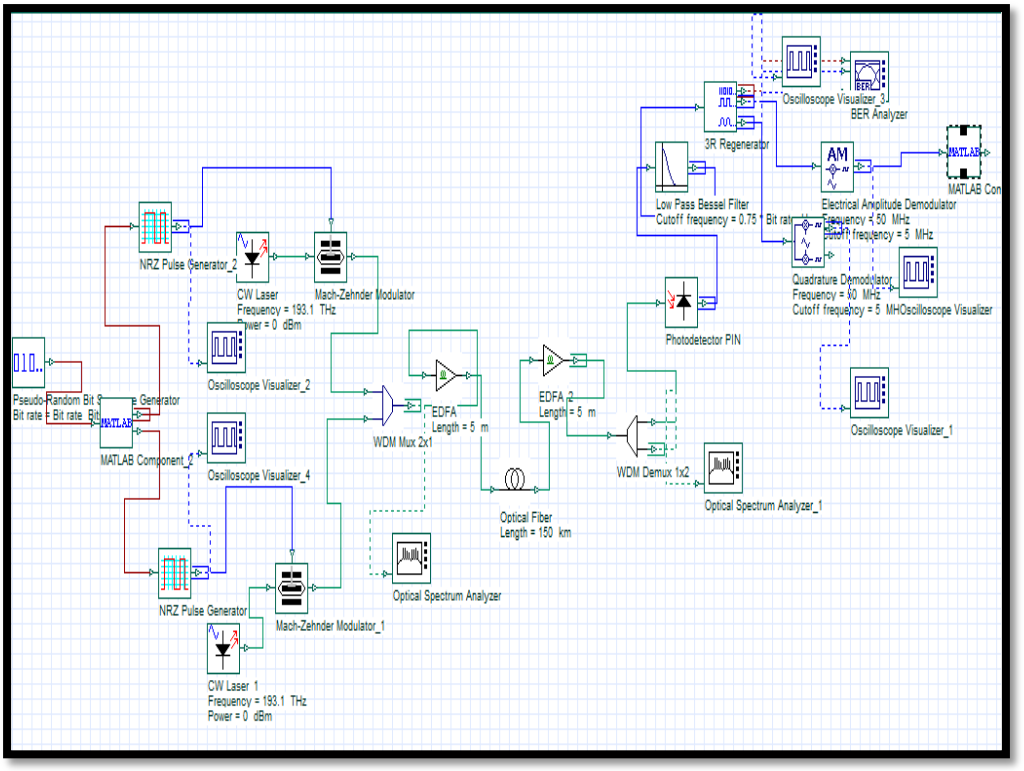


Fig.6 : DWDM system components in"*Optisystem*™"

Table2: DWDM system components used in *Optisystem*™

Input data	Pseudo – random bit sequence generator
	Matlab componant
Transmitter part	NRZ pulse Generator
	CW laser
	Mach-Zehner Modulator
Transmitting Media	WDM Mux 2*1
	Optical Fiber

	EDFA amplifier
	WDM Dmux 2*1
Receiving part	Photodetector PIN
	Low pass Bessel filter
	3R Regenerator
	Electrical Amplitude Demodulator
	Quadrature Demodulator
Data out	Matlab component
Measurements component	Oscilloscope Visualizer
	Optical Spectrum Analyzer
	BER Anlyzar

4. Results and Discussions

The models described in figure (5&6) is a simulation of Optical Fiber system, which it's used to send and receive a secure data. This data was encrypted in the transmitting side and decrypted again to the original image in the receive side using Matlab program. This proposed CR4 encryption algorithm is implemented using the Matlab simulation program, and the following images was taken as a test colors (RGB) and gray images.

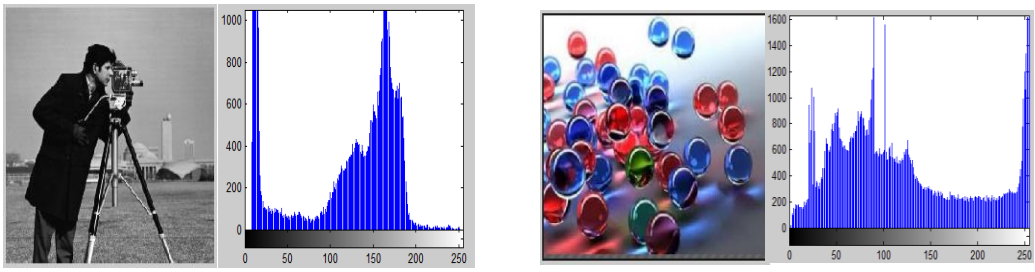
(a) Cameraman

(b) Colors

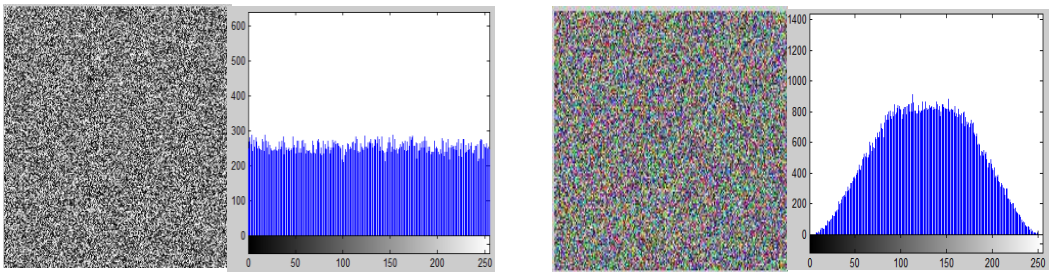
Fig 7 :(a)Gray (b) RGB test images

Histogram Analysis

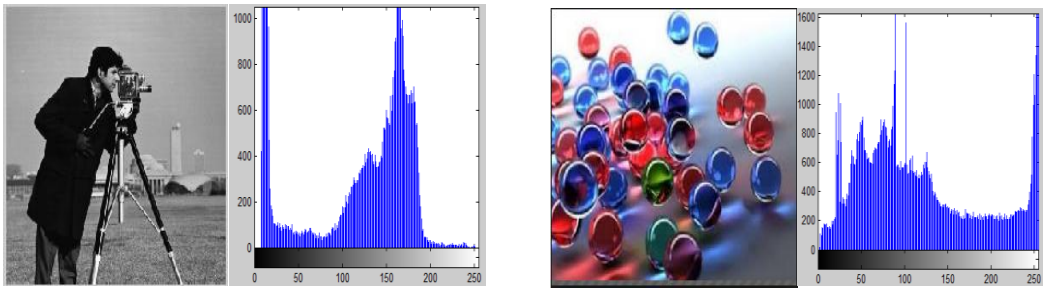
The statistical features of images are presented using histogram that plots the occurrences frequency of image pixel value, this analysis is done to compare original and encrypted images where there should be no similarities between histograms of original and encrypted image. The Figure (9) shows the original images with its histogram, encrypted and decrypted images with their histogram.



Original images and its histogram



Encrypted image and its histogram



Decrypted image and its histogram

(a)Gray image (b) RGB image

Fig.8: Histogram result of RC4 image encryption and decryption for (a) Gray (b) RGB

This encrypted data was transfer to a NRZ pulse generator, and then modulated with 1550nm CW laser using the Mach-Zender modulator as show in figures 5&6. The modulated signal shows using optical spectrum analyzer, figure 9, was sent through optical fiber in different distance from 10 to 150KM. In the receiving side the signal was demodulated using electrical amplitude demodulator and Quadrator modulator as shown in figure 10 using Oscilloscope visualizer, the output of these demodulators was transfer to Matlab using Optisystem- Matlab communicator to receive the final unencrypted image.

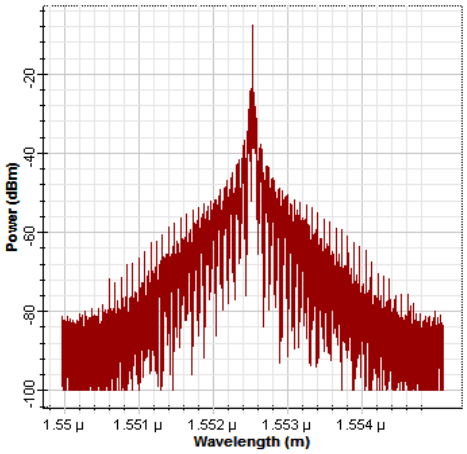


Fig. 9: Modulated signal as seen by optical spectrum analyzer

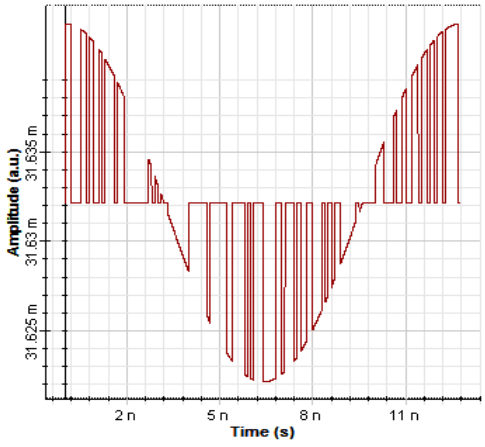


Fig. 10: Demodulated signal as seen by Oscilloscope visualizer

To measure the optical fiber link performance, BER and Q- factor of optical fiber links based on the above system model were calculated for various numbers of designs with different distances as shown in figure 11&12.

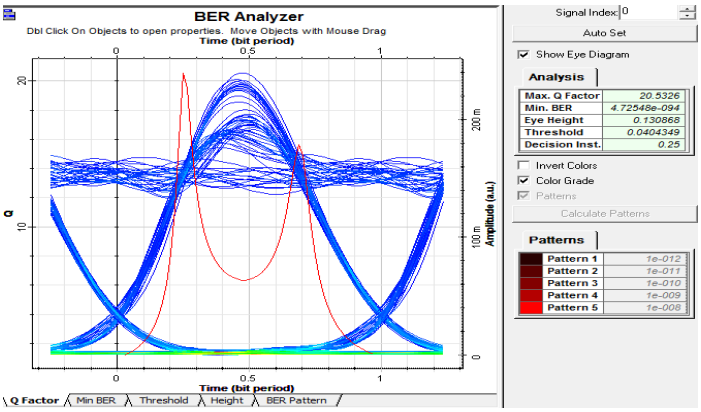


Fig. 11: Eye diagram showing BER performance when using one optical fiber and with 30KM

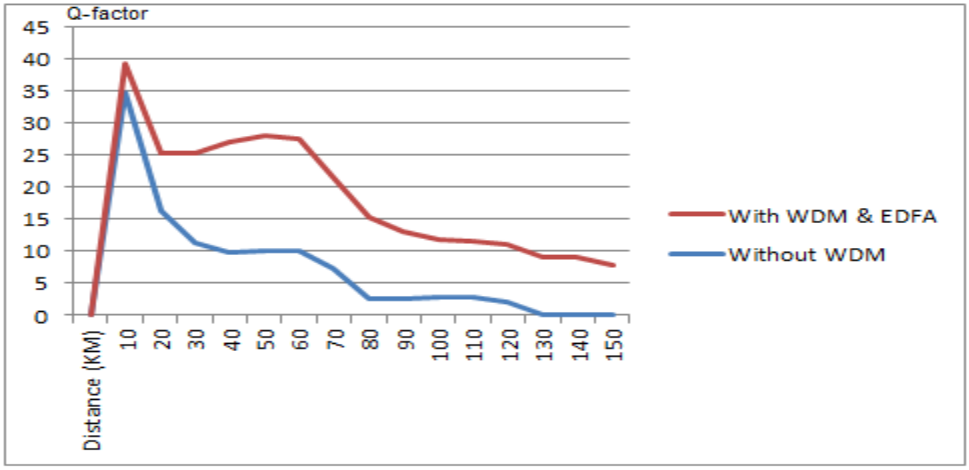


Fig.12: Q- Factor of optical fiber system with and without DWDM with distance 10-150Km

It is obvious from figure 12 that using DWDM with EDFA amplifiers at 1550nm could be obtain the better results, since DWDM is work with a

multiple closely (or same) wavelength to send different data on the same optical fiber line, therefore it can be send a greater bandwidth, and because of the EDFA amplifiers its work to amplify the signal and can have abettor performance for a longer distance.

5. Conclusion

From the software test that have been performed and analyzed, the following conclusions have been deduced:

1. The Fiber Optic system can be used to send a huge data with a high security, Using DWDM with EDFA amplifier increase the system performance by sending larger bandwidth and for longer distance

2. DWDM systems operate with wavelength of 1550-nm due to the low glass attenuation characteristics and due to the fact that the EDFA amplifier can operate in wavelengths between 1530-nm–1570-nm

3. low-pass Gaussian filter and PIN photodiode detector were utilized in the received side, which it cause to reduce the time jitter and the traveling-wave electron absorption modulator (TW-EAM) switch window loss
4. The proposed algorithm of the RC4 can achieve efficient data encryption up to 256 byte to avoid limited data constraint. The submitted architecture should satisfy the need of high-speed data encryption and can be applied to various data types.
5. Image ciphering by RC4 algorithm has a considerable security quality factor which implies the intensity distributions for the secret image and distorted image are different. When analyze the encrypted image histogram we recognized that they have the same distribution.
6. Our suggested technique implemented using RGB, Gray Scale, PNG or BMP images, but future modification can be made to apply the technique for audio and video encryption..

References

[1] T. Z. Abbas, "**Fiber Optics**," Ph.D thesis ,UOT,2012.

[2] J. M. Senior and M. Y. Jamro, *Optical Fiber Communications: Principles and Practice*. 2009.

[3] P. Jindal , B. Singh,"A Survey on RC4 Stream Cipher", I. J. Computer Network and Information Security, 20157, 37-45.

[4] T. Education, *Principles of Fiber Optic Communication*.,STEP (Scientific and Technological Education in Photonics), an NSF ATE Project ,2008.

[5] S. Kwan, "Principles of Optical Fibers," fulfillment of course requirement for MatE 115, Fall,San Jose State University, 2002

[6] N. Uddin, M. R. M, and S. Ali, "Performance Analysis of Different Loss Mechanisms in Optical Fiber Communication," *Comput. Appl. An Int. J.*, 2015, vol. 2, no. 2, pp. 1–13.

[7] Tomáš Ivaniga1, "Evaluation of the bit error rate and Q-factor in optical networks\n," *IOSR J. Electron. Commun. Eng.*, 2014 vol. 9, no. 5, pp. 01–04.

[8] J. Zweck, I. T. L. Jr, Y. Sun, A. O. Lima, C. R. Menyuk, and G. M. Carter, "Modeling Receivers in OPTICAL COMMUNICATION," *Opt. Photonics News*, vol. November, 2003, p. 31.

[9] N. Massa, "Fiber Optic Telecommunication," *Fundam. Photonics*, 2008 pp. 293–347.

[10] B. Mukherjee, "WDM optical communication networks: progress and challenges," *IEEE J. Sel. Areas Commun.*, 2000 vol. 18, no. 10, pp. 1810–1824.

[11] S. Mister , S. E. Tavares2." Cryptanalysis of RC4-like Ciphers", S. Tavares and H. Meijer (Eds.): SAC'98,1999, LNCS 1556, pp. 131-143.

[12] http://en.wikipedia.org/wiki/RC4 accessed at 25 Jan 2013.

[13] A. Mousa ,A. Hamad,"Evaluation of the RC4 Algorithm for Data Encryption",International Jornal of coputer science and applications ,June 2006, vol 3,no.2.

[14]R. L. Rivest, J. C. N. Schuldt," Spritz|a spongy RC4-like stream cipher and hash function ",October 27, 2014

[15] E. M. R. Oscillator, Z. Hu, K. Nishimura, H. Chou, L. Rau, M. Usami, J. E. Bowers, and D. J. Blumenthal, "40-Gb / s Optical Packet Clock Recovery Using a Travelling-wave,",2004, vol. 16, no. 1, pp. 1–2.

الاتصالات السلكية لتأمين نقل البيانات في الألياف الضوئية

م.م. اروى عامر موسى* م.م. مي حاتم عبود **

مستخلص

واحدة من أهم القضايا في مجال الشبكات هو الطلب الهائل على عرض النطاق الترددي و الأمن في نقل البيانات. الشبكة الضوئية هي شبكة ذات سعة عالية تستخدم لنقل البيانات مع توفر امكانيات كبيرة. ولتوفير قدرة اضافية في استخدام نطاق ترددي اوسع، و ترددات مختلفة ومسافات أطول سيتم استخدام مكثف تقسيم الطول الموجي (DWDM) ومكبرات الضوء الألياف الإربيوم المشوب .(EDFA) ولنقل البيانات بشكل امن سيتم استخدم واحدة من اهم طرق التشفير وهي RC4 لحماية البيانات في القناة المشتركة وذالك لانها توفر طريقة تشفير اسرع وابسط في التطبيق وجدول المفاتيح المستخدم هو عبارة عن تسلسل عشوائي من البتات التي تضمن امن الشفرات المستخدمة . برنامج Matlab سوف يستخدم لتشفير وفك تشفير الصورة المستخدمة مع نقلها ضوئيا باستخدام برنامج المحاكاةOptisystem .

*الجامعة العراقية