Journal of Engineering
journal homepage: www.joe.uobaghdad.edu.iq
Number 12 Volume 25 December 2019

Electrical, Electronics and communications, and Computer Engineering

Simple 2D chaotic remapping scheme for securing optical communication networks

Hiba Abdel Wahab Jabori *
College of Engineering -Baghdad University
Baghdad, Iraq
Email: Hibaabd.alwahab@yahoo.com

Oday A.L.A Ridha
College of Engineering -Baghdad University
Baghdad, Iraq
Email: oday_ridha@yahoo.com

ABSTRACT

In this work, a simple and new method is proposed to simultaneously improve the physical layer security and the transmission performance of the optical orthogonal frequency division multiplexing system, by combining orthogonal frequency division multiplexing technique with chaotic theory principles. In the system, a 2-D chaotic map is employed. The introduced system replaces complex operations such as matrix multiplication with simple operations such as multiplexing and inverting. The system performance in terms of bit error rate (BER) and peak to average ratio (PAPR) is enhanced. The system is simulated using Optisystem15 with a MATLAB2016 and for different constellations. The simulation results showed that the BER of an unauthorized receiver reaches 0.5. Furthermore, the peak-to-average-power-ratio (PAPR) of the transmitted OFDM signal can be decreased by about 0.8 dB at BER equal to 10^{-4}.

Keywords: OFDM, Chaotic system, Optical Communications.

أسلوب بسيط لتأمين اتصالات الشبكات الضوئية بالاعتماد على اعادة التوزيع الفوضوي الثنائي الأبعاد

هبة عبد الوهاب جبوري
قسم الهندسة الالكترونية والاتصالات
كلية الهندسة/ جامعة بغداد

أ. م. د. عدي عبد اللطيف عبد الرضا
قسم الهندسة الالكترونية والاتصالات
كلية الهندسة/جامعة بغداد

الخلاصة

في هذا العمل تم استخدام أسلوب بسيط و جديد لتحسين امان الطبقة الفيزيائية انيا مع الاداء الخاص بمنظومة ضوئية تعتمد على دمج تقسيمات الترددات المتعامدة, من خلال دمج تقنية دمج تقسيمات الترددات المتعامدة مع مبادئ نظرية الفوضى. في المنظومة المقدمة تم استخدام خارطة فوضوية ثنائية الابعاد. في المنظومة المقدمة تم الاستعاضة عن العمليات المعقدة بعمليات بسيطة كالعكس والتوجيه. تقييم أداء المنظومة المقدمة اظهر تحسنا ملحوظا في نسبة الخطأ وكذلك معامل قمة الموجة الى معدلها. تم بناء ومحاكاة المنظومة المقدمة في بيئة Mathlab2016 مع برنامج Optisystem 15 ولعدة مجاميع (constellation). نتائج المحاكاة اظهرت نسبة خطأ للمستلم الغير مخول بلغت 0.5. كما انه اظهر ان معامل قمة القدرة الى معدل القدرة انخفض حوالي 0.8 دي بي عند نسبة خطا 10^{-4}.

الكلمات الرئيسية : دمج تقسيمات الترددات المتعامدة, النظام الفوضوي ,نظام اتصالات ضوئي.

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2019.12.07

Article received: 4/8/2018
Article accepted: 4/2/2019
Article published: 1/12/2019

1. INTRODUCTION

The optical network has been playing an important role in broadband services. It provides several potential benefits such as high capacity, low cost, and energy efficiency. Optical orthogonal frequency division multiplexing (O-OFDM) has been regarded as a promising candidate for next-generation since it reduces the guard band between subcarriers. It has high robustness to fiber dispersion, high spectrum efficiency, and cost-effectiveness **Jean Armstrong, 2009**. The physical layer of an optical network is vulnerable to a variety of attacks, including jamming, physical infrastructure attacks, eavesdropping, and interception. As the demand for network capacity grows dramatically, security has become one of the major concerns in an optical OFDM system, **Mable P. Fok, et al., 2011**. Different technologies have been explored to enhance system security. However, most of the previous secure technologies focus on both upper and physical layers. At the upper layer, the data frames encrypted but the control frames and headers lifted without protection, **Lijia Zhang, Zhang, et al. , 2011.** On the other side, the physical layer is a transparent pipe for all services and users. Therefore, the encryption on physical layer can prevent the vicious attacks. This came from the fact that the whole data frame and its header are encrypted .

High PAPR is one of the major drawbacks of OFDM modulation. It is defined as the relation between the maximum power of a sample in a given OFDM transmitted frame divided by the average power of that OFDM frame This peak comes from the nature of IFFT where adding a number of modulated data on each subcarrier, so a large PAPR is produced when all subcarriers added coherently **Adnan A.E. Hajomer, 2018**. This factor made the OFDM receiver high sensitive to the nonlinear devices, such as digital-to-analog converter (DAC) and high power amplifier (HPA), which may severely degrade system performance, **Tao Jiang, and Wei Zhang, 2008.** Another challenge in security O-OFDM system is complexity, most currently available technologies require complex implementation with high computational cost.

In this work, a new strategy of chaos-I (In phase) and Q (Quadrature) encryption for secure OFDM is proposed. An initial value of 2-Dimensional logistic map is employed to serve as the security key. In the proposed strategy, the chaos-IQ encryption is executed by controlling mapping according to chaotic sequences instead of multiplying I and Q with chaotic sequences, which suffer from high complexity since this method requires two multipliers for each mapped symbol. In the proposed system, a 10 Gb/s with optical 16QAM-OFDM transmission and chaos encryption is successfully achieved.

2. RELATED WORKS

In this section, an overview of some relevant works is presented:

Jones, 1994, and **Mohammed Kasim Al-Haddad, 2014,** the simplest technique for PAPR reduction is produced, which is clipping technique, where the peak envelope of the input signal limited to the desired value. In general, the receiver must estimate two parameters, location of clipping and size of the clip. However, getting this information is difficult. Moreover, this method introduces both in band and out of band radiation which degrades the system performance. This technique reduces PAPR and discards security issue.

Marco Breiling, 2001, proposed a scheme that generated a set of OFDM symbols in transmitter, these sets representing the same information encrypted by IQ encryption or by multiplying the mapped data with a phase sequence. Then IFFT is applied to all of them. After that, the one with minimum PAPR for transmission is selected and the corresponding selected code should be transmitted to receiver as side information. Therefore, the ability of PAPR reduction in this technique depends on the numbers of codes and number of FFT/IFFT blocks. This technique reduces PAPR with high complexity due to number of fast Fourier transform (IFFT) / fast Fourier transform (FFT) blocks and multipliers and selection of minimum PAPR; also the security issue remains unsolved.

In**2011 Lijia Zhang** proposed a scheme that improves the physical layer security of O-OFDM system. The scheme is based on chaos scrambling in the frequency domain of OFDM. By using one-dimensional logistic map, the data stream is encrypted with a certain number of N- order scrambling matrices. System security is enhanced since different scrambling matrices allocated are to different OFDM frames. And these matrices are reversible as to descramble the data at the receiver, where it can be recovered by the inheritance matrix of the scrambling matrices and initial values. The disadvantage of this system is presented in the requirement of relatively complex operations, the dependence of keyspace on the order of inheritance matrix, and the effects on the PAPR are not considered.

In **Lei Deng, 2014** joint PAPR reduction with the enhancement of physical layer security through chaos and fractional Fourier transform (FrFT) techniques in an O-OFDM-PON, this improvement achieved by building multi-stage data encryption consist of time synchronization, OFDM subcarriers masking, and control operation on the fractional-order of the FrFT. The weakness of this system is its high complexity because of FrFT, PAPR reduction of the transmitted OFDM signal was little enhancement compared with the cost and complexity of design.

In **2014 Wei Zhang** proposed a quadrature amplitude modulation (QAM) encryption method based on chaos coding scheme to improve the security of O-OFDM. In chaos coding scheme, the real part and imaginary part of QAM symbols are separately multiplied by chaotic sequences. These chaotic sequences are generated from a modified Logistic mapping. The initial value and iteration parameters of the mapping formula are set as the security keys. The weakness of this novel is mainly based on difficult implementation because of multiplication process, and the effect of the proposed system on PAPR was not discussed.

In **2015 Wei Zhanga** combined a QAM encryption technique in **Wei Zhang, 2014,** with the selective mapping technique (SLM), where number of multipliers and IFFT / FFT blocks are required. The results showed that BER of eavesdropper was around 0.5, also show that high physical layer security combined with enhancement in terms of PAPR. However, its high complexity is one of the main disadvantages with the dependence of performance on the number of multipliers and IFFT/FFT blocks.

Xiaonan Hu, **2015** experimentally demonstrated a chaotic partial transmit sequence (PTS) technique for O-OFDM system. A 4-D hyperchaotic system is used to generate the chaotic phase weighing factors in PTS and the chaotic training sequence for OFDM symbol synchronization. This scheme suffers from high complexity due to a large number of multipliers and number of IFFT/FFT blocks and DSP system for phase optimization.

Zanwei Shen, 2016 proposed and demonstrated a multi-stage system for physical layer security with PAPR enhancement based on discrete Fourier transform (DFT) within O-OFDM. This multi-stage system is divided into the following stages: the chaotic training sequence for OFDM symbol synchronization, the reconfigurable DFT matrix, and chaotic subcarrier allocation. The main disadvantage of this system is high complexity.

Adnan A.E. Hajomer, 2018 examined the same system proposed in **Zanwei Shen, 2016,** but using DHT instead of DFT. The multi-stage data encryption provided a reduction in PAPR. This system has a lower computational complexity compared with FrFT, and SLM but it still required complex operation as explained later.

Up to now, the security approaches have been proposed to enhance the physical-layer security for transmission in OFDM, but most of them disregarded both simplicity and transmission performance enhancement. In this work, a low complexity, secure, and enhanced performance optical communication system is introduced.

3. PROPOSED SECURE OPTICAL COMMUNICATION SYSTEM

The basic idea of the introduced system is to control mapping of the IQ of QAM mapper at transmitter using predefined sequences (encryption sequences). At authorized receiver, the same sequences are used to control the remapping of the IQ to it is original position (before encryption). In this work, only the signs of IQ are changed according the encryption sequences. Usually these sequences are only known by transmitter and authorized receivers. The predefined sequences (x_1 and x_2) are generated using 2D chaotic system. The schematic diagram of the transmitter of proposed system is illustrated in **Fig. 1**.

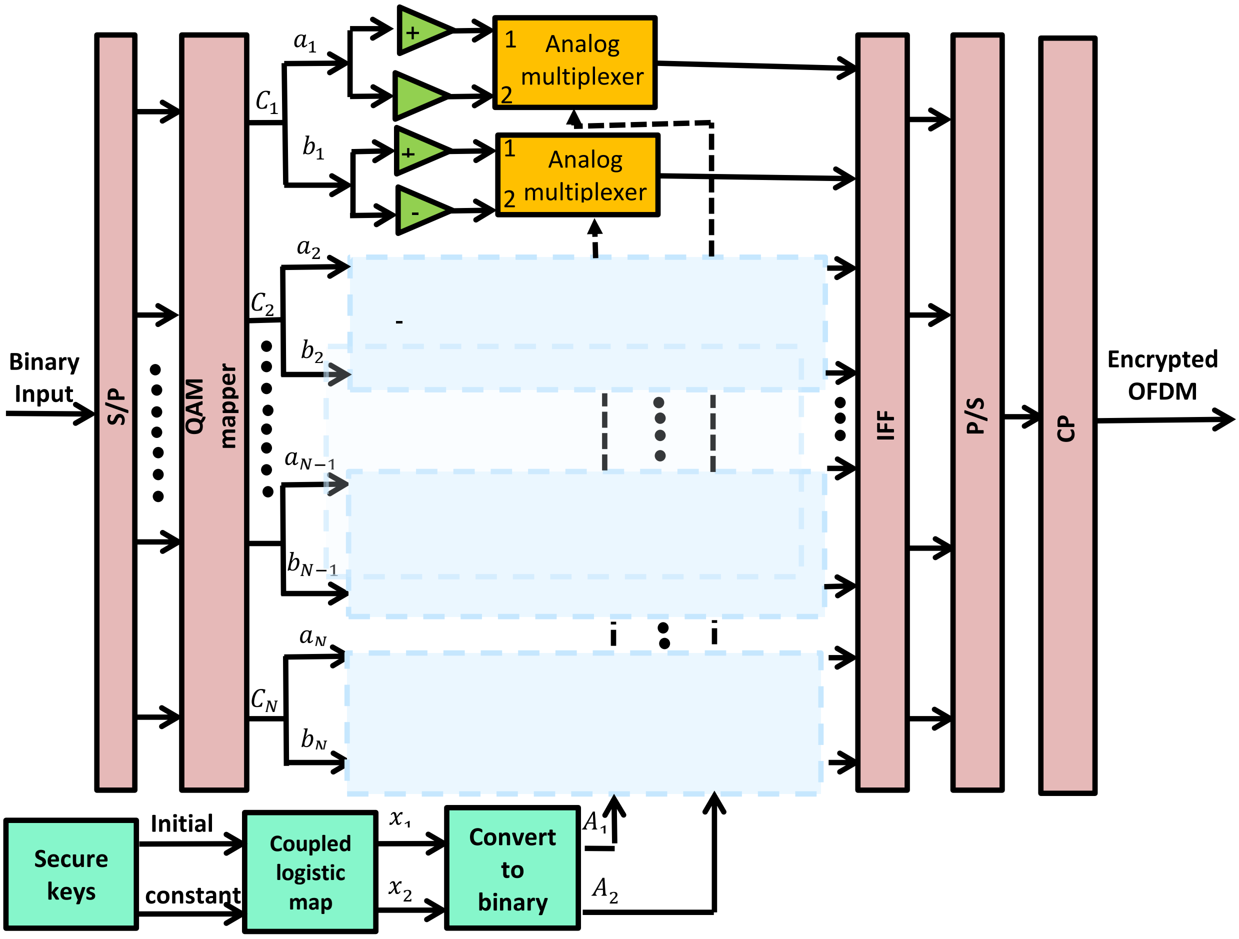

Figure 1. Proposed optical communication transmitter.

The transmitted binary data stream are QAM mapped to symbols after converting it from serial form to parallel form by (S/P) conversion. After that, these QAM mapped symbols are encrypted by the two binary encryption sequences (A_1 and A_2), these sequences are generated from the two chaotic sequences (x_1 and x_2).

From **Xingyuan Wang, Q Shi, 2005,** the state equations of 2D coupled Logistic mapping are :

$$x_{1_{i+1}} = \mu_1 x_{1_i}\left(1 - x_{1_i}\right) + \mu_3 {x_{2_{i+1}}}^2 \qquad (1)$$

$$x_{2_{i+1}} = \mu_2 x_{2_i}\left(1 - x_{2_i}\right) + \mu_4\left({x_{1_i}}^2 + x_{1_i} x_{2_i}\right) \qquad (2)$$

where $x_1, and\ x_{2,}$ are state variables, and $2.75 < \mu_1 < 3.4$, $2.75 < \mu_2 < 3.45$, $0.15 < \mu_3 < 0.21$, and $0.13 < \mu_4 < 0.15$. The generated sequences $x_1$and x_2 are chaotic in interval (0, 1). **Fig. 2** shows the chaotic sequences of x_1 and x_2.

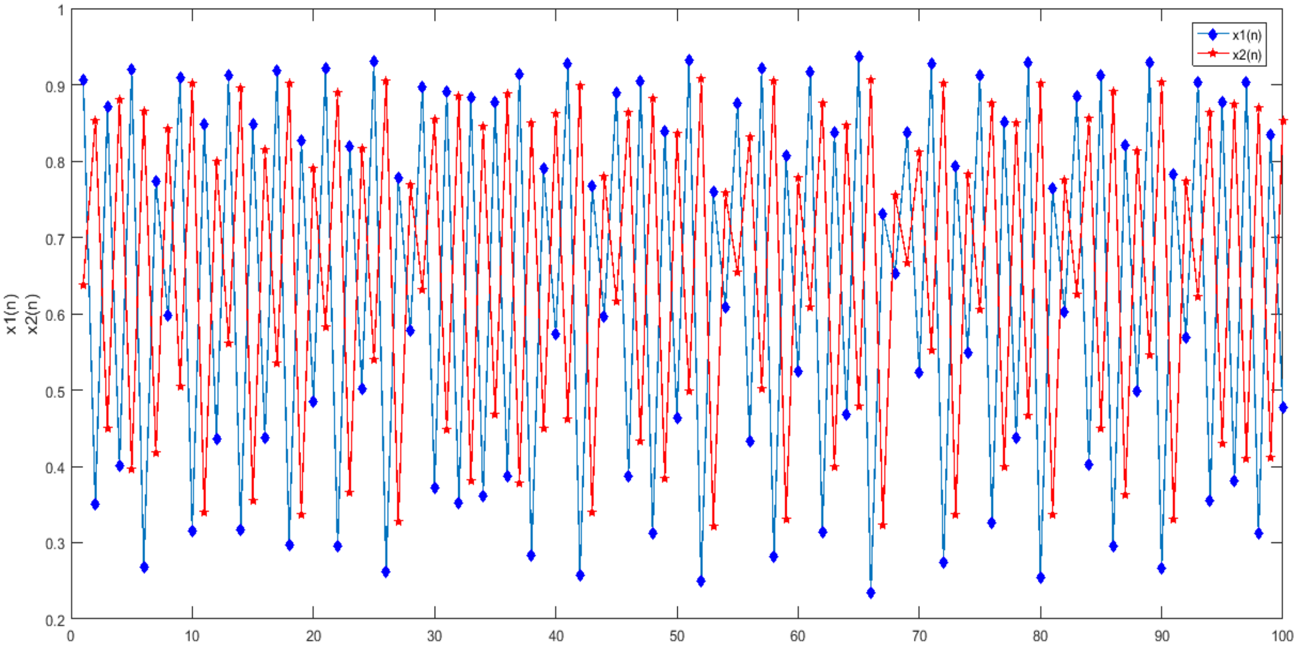

Figure 2. Generated x_1 and x_2 chaotic sequences.

To convert x_1 and x_2 to binary form and to improve the statistical properties of the generated encryption sequences, the following preprocessing is performed, **Wie Zhang, 2015.**

$$A_1 = sign(x_1 10^6 - floor(\ x_1 10^6) - 0.5) \qquad (3)$$

$$A_2 = sign(x_2 10^6 - floor(\ x_2 10^6) - 0.5) \qquad (4)$$

At first assume that the QAM mapped symbol at *nth* subcarrier is:

$$C\ _n = a_n + j\ b_n \qquad (5)$$

Where a_n and b_n is the real and imaginary part of mapped symbol at *nth* subcarrier, respectively. And $0 \le n \le N$, and N is number of IFFT points. From (3) and (4), two binary sequences (A_1 and A_2) are generated simultaneously. A_1 and A_2 sequences are used to control the signs of a_n and b_n of QAM mapped symbol, respectively, and as shown below in **Table (1)**:

Table 1. IQ encryption scheme according to A_1 and A_2.

A_1	A_2	**IQ encryption scheme**
0	0	Don't change the signs of the real part and imaginary part of the transmitted point in signal constellation, so $C'_n = a_n + j\, b_n$.
0	1	Changes the sign of the imaginary part of the transmitted point in signal constellation, so $C'_n = a_n - j\, b_n$.
1	0	Changes the sign of the real part of the transmitted point in signal constellation, so $C'_n = -\, a_n + jb_n$.
1	1	Changes the signs of real parts and imaginary parts of transmitted point in the signal constellation, so $C'_n = -\, a_n - jb_n$.

Where C'_n is the output of IQ encryption at the n^{th} subcarrier. The parameters and initial condition of chaotic system are used as encryption keys. The transmitter and the authorized receiver must have the same encryption key for generating encryption and decryption sequence, respectively. The schematic diagram of proposed control mapper is illustrated in **Fig. 3**. So that for implementation only two analog multiplexers are required with operational amplifier, this results in low complexity compared with other techniques.

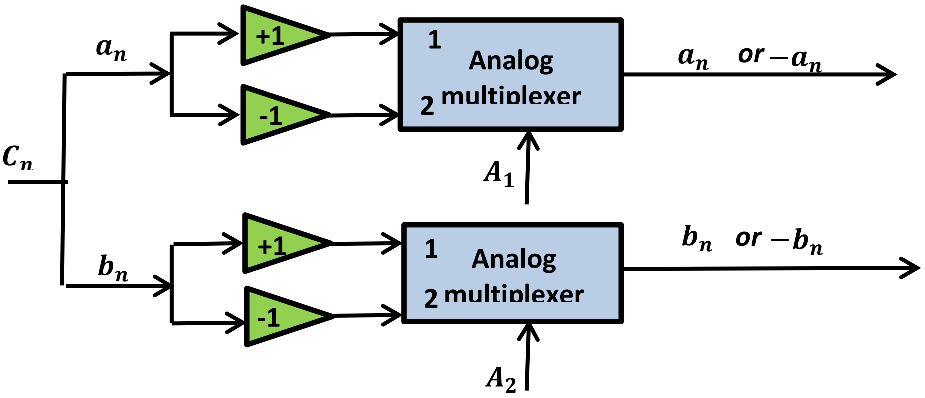

Figure 3. Schematic diagram for proposed control mapper.

Where IQ encryption that used in **Wie Zhang, 2014,** required more complexity for implementation, because of using multipliers that can be implemented by FPGA as **Bashar Adel Esttaifan, 2013**, shows. The system proposed in **Lei Deng, 2014,** required FrFT that need ($\frac{N}{2}\log_2 N$) complex multiplication and ($N \log_2 N$) complex addition. The system proposed in **Wei Zhanga**, **2015**, needs large number of multiplier and IFFT/FFT blocks. At the same time, PTS technique proposed in **Xiaonan Hu**, **2015**, suffers from high complexity due to a large number of multipliers, IFFT/FFT blocks and DSP system for phase optimization. **Zanwei Shen, 2016** the proposed system used DFT that needs number of operations less than **Lei Deng, 2014,** where (N^2) complex multiplication with

$(N^2 - N)$ complex addition is required. The technique proposed in **Adnan A.E. Hajomer, 2018**, number of complex multiplication $2N^2$ and number of complex addition is $N(N-1)$.

It is clear that the influence of the proposed IQ encryption can be extended as PAPR reduction technique. This idea stems from the fact that PAPR is determined by the sequence of the transmit data vectors, changing the mapped data vectors by controlling mapping will change the PAPR properties after the IFFT.

Adnan A.E. Hajomer, 2018 presented an interesting paper which can be used to specify the PAPR reduction capability of proposed IQ encryption, where the upper bound of peak factor is :

$$\zeta \leq 1+\frac{2}{N}\sum_{k=1}^{N-1}|\rho(k)| \tag{6}$$

$$\rho(k) = \sum_{n=1}^{N-k} C_{n+k}{C^*}_k \tag{7}$$

where ζ is the upper bound of the peak factor, $\rho(k)$ is the aperiodic autocorrelation coefficients. It is clear from the above equation that the capability of PAPR reduction via proposed IQ encryption came from the reduction of the autocorrelation coefficients of the corresponding QAM sequence.

4. SIMULATION SETUP

The simulation setup of the proposed secured O-OFDM is shown in **Fig. 4.** This simulation had been performed using OptiSystem Version 15 co-simulated with MATLAB 2016 to perform IQ encryption and 2D coupled Logistic mapping. Firstly, binary data with length 2^{19} are sent to the OFDM transmitter.

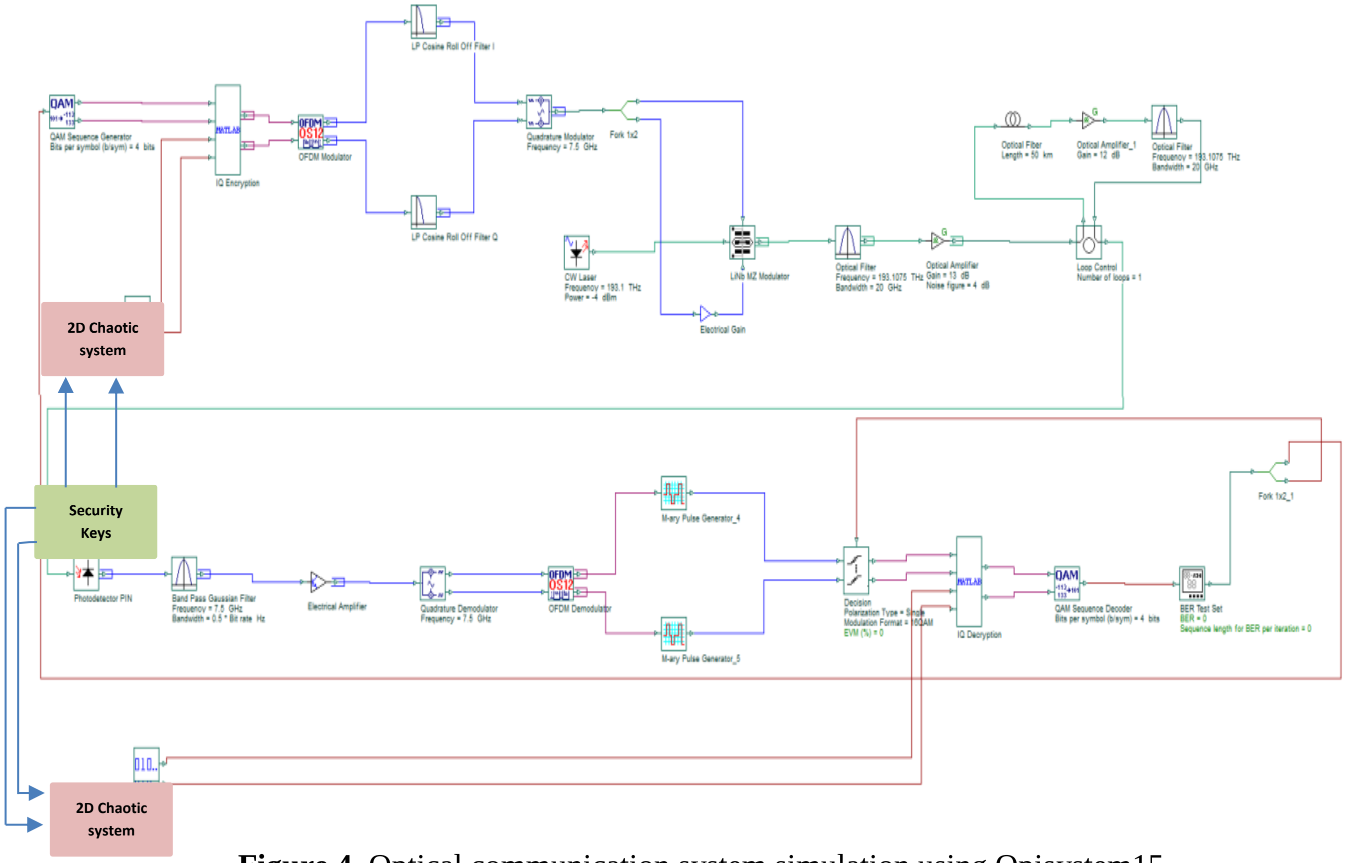

Figure 4. Optical communication system simulation using Opisystem15.

where QAM sequence generator used to mapped the binary data to 16-QAM mapped symbols. After that, the I and Q encryption is taken place by two sequences generated from the 2D chaotic system. OFDM modulator is used with total number of Inverse Fast Fourier Transform (IFFT)/ Fast Fourier Transform (FFT) subcarriers is 1024. Only 512 active subcarriers are utilized to transmit valid data. The whole bandwidth is 5 GHz. Firstly, the OFDM baseband signal is up-converted to 7.5 GHz. Then Mach-Zehnder Modulator (MZM) with A 1552 nm CW laser is used to convert OFDM baseband signal to the optical domain, where optical OFDM signal is double side-band (DSB), MZM works at 4 V with a half-wave voltage of 2V, and the linewidth of 0.1 M Hz was used as the optical carrier. The double sideband O-OFDM is filtered by optical filter with 193.1075 THz, then directly sent into the 50 km Standard Single Mode Fiber link (SSMF) with a launched optical power of -6.014 dBm. After that, the received encrypted OFDM signal is converted from the optical domain to an electrical domain by a photodiode (PD). After that the OFDM signal is down-converted by 7.5 GHz. Then FFT is applied by OFDM demodulator block. Finally, the resulted signal is decrypted by same IQ encryption and chaotic system and then QAM demapped by QAM sequence decoder.

5. RESULTS

The introduced secured optical communication system is simulated using Optisystem15 co-simulated with MATLAB2016 to perform IQ encryption. The performance of bit-error-rate (BER) for authorized receiver for different carrier wave (CW) laser optical power is shown in **Fig. 5**. It can be observed that there is power reduction due to using of IQ encryption, where the CW optical power is reduced by 1.5 dB to achieves same value of BER (at log(BER) =10^{-4}).

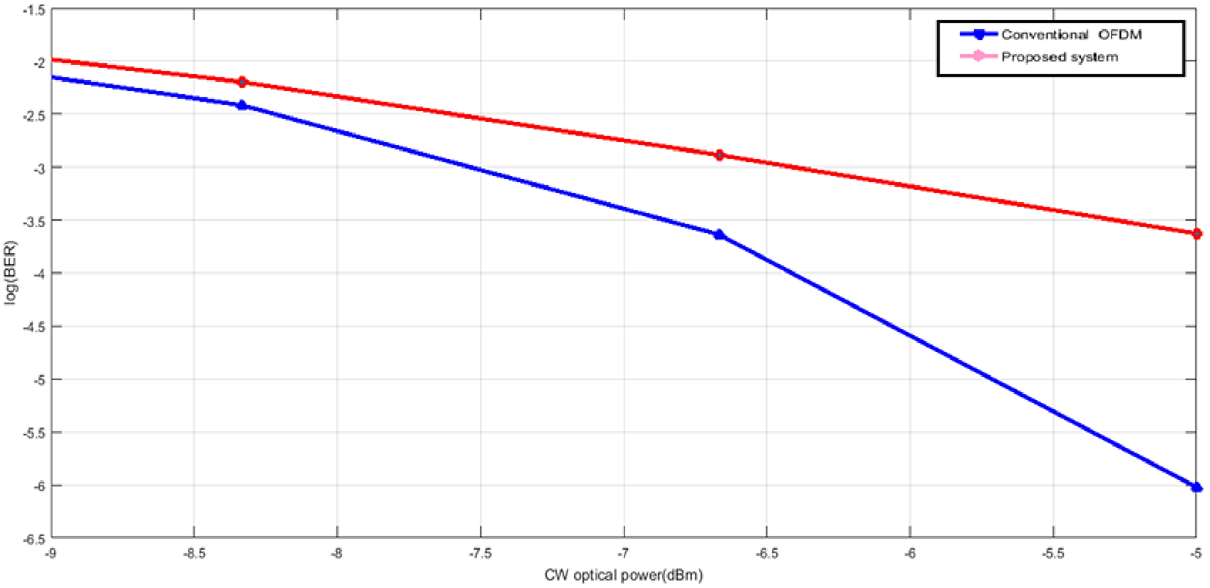

Figure 5. BER versus CW optical power for conventional OFDM system and proposed system.

This enhancement came from the fact of reducing IQ encryption to the PAPR. This is shown by Complementary Distribution Function (CCDF) of PAPR for the proposed system and conventional OFDM system that displayed in **Fig. 6**, where 65000 OFDM frames are used. Compared with conventional OFDM signal, the peak to average power of encrypted OFDM signal can be decreased by 0.8 dB at CCDF equal to10^{-4} and this reduction enhances transmission performance.

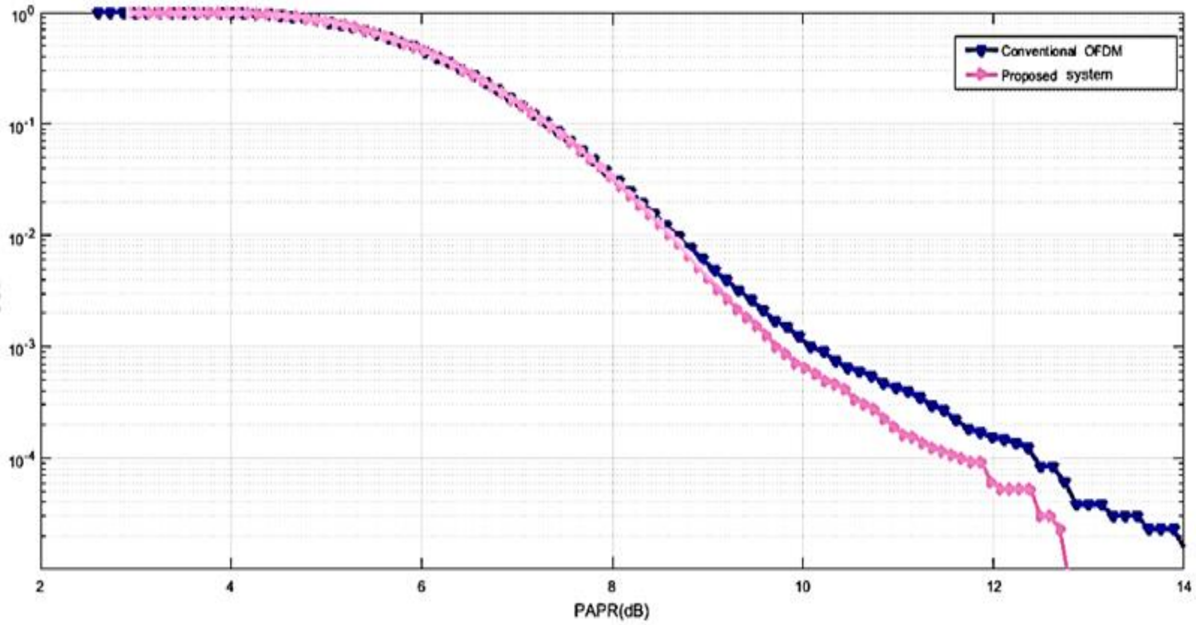

Figure 6. CCDF curves for the conventional OFDM and proposed system.

Fig. 7. Illustrates the BER for different signal constellation diagrams and different chaotic sequences. Moreover, BER of the unauthorized receiver about 0.5, 0.25, 0.23, and 0.19 corresponding to square constellation diagram, star constellation diagram with 4 radii, circular constellation diagram with 1 radius and 2 radii, and circular constellation diagram with 4 radii and star constellation diagram with 2 radii, respectively. So constellation diagram is one of the parameters that affect BER of the unauthorized receiver.

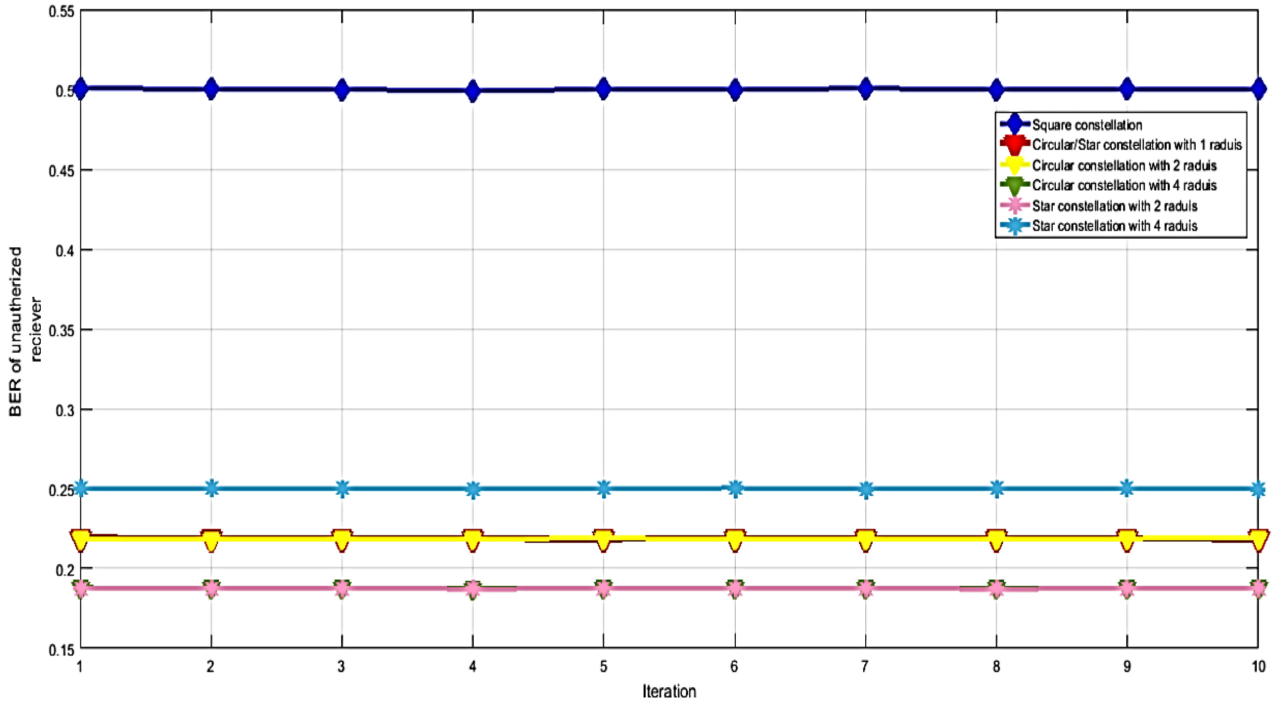

Figure7. BER for different 16-QAM constellations and chaotic sequence for each iteration.

6. CONCLUSIONS

A secured and low computation complexity O-OFDM of 10 Gb/s has been designed and investigated. In the system, a 2D logistic map generator is used to control the mapping. The introduced system replaces complex operations such as matrix multiplication with simple operations such as multiplexing and inverting. The simulation results showed that the BER of unauthorized receiver reaches 0.5. Furthermore, how signal constellation diagram large difference in BER of authorized receiver reached to 0.31. The CW power reduction due to using of IQ encryption is about 1.5 dB; this enhancement came from PAPR reduction of the transmitted OFDM signal that is about 0.8 dB at BER equal to10^{-4}.

7. REFERENCES

- A.E. Jones, T.A. Wilkinson, and S.K. Barton, 1994, *Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission scheme*, Vol. 30, No. 25.PP 2098-2099.
- Adnan A.E. Hajomer, Xuelin Yang, Weisheng Hu, 2018, *Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform*, IEEE Photonics Journal, Vol. 10, No. 2.
- Bashar Adel Esttaifan, Oday AbdulLateef, Waleed Ameen Mahmoud, 2013, *Design and Implementation of a Multiplier free FPGA based OFDM Transmitter, Journal of Engineering*, Vol.19, No.8, PP. 1056-1072.
- Jean Armstrong, 2009, *OFDM for Optical Communications, Journal of light wave technology*, vol. 27, No. 3, pp. 189-203.
- Lei Deng, Mengfan Cheng, Songnian Fu, and Ping Shum, 2014, *Secure OFDM-PON System Based on Chaos and Fractional Fourier Transform Techniques*, Journal of light wave technology, Vol. 32, No. 15, PP. 2629- 2635.
- Lijia Zhang, Xiangjun Xin, Bo Liu, and Yongjun Wang, 2011, *Secure OFDM-PON Based on Chaos Scrambling, IEEE photonics technology letters*, Vol. 23, No. 14, PP. 998-1000.

- Mable P. Fok, Zhexing Wang, Yanhua Deng, and Paul R. Prucnal, *Fellow, IEEE*, 2011, *Optical Layer Security in Fiber-Optic Networks, IEEE transaction on information forensic and security*, Vol. 6, No. 3, PP. 725-736.
- Marco Breiling, 2001, *SLM Peak-Power Reduction without Explicit Side Information*, IEEE COMMUNICATIONS LETTERS, Vol. 5, No. 6. PP. 239–41.
- Mohammed Kasim Al-Haddad, 2014, *PAPR Reduction of OFDM Signals Using Clipping and Coding,* Journal of Engineering, Vol. 20 No. 8 , PP. 18-34.
- Tao Jiang, and Yiyan Wu, 2008, *An Overview: Peak-to-Average Power Ratio Reduction Techniques for OFDM Signals*, IEEE transaction on broadcasting, Vol. 54, No. 2, PP. 257-268.
- Wei Zhang, Chongfu Zhang, Wei Jin, Chen Chen, Ning Jiang, and Kun Qiu, 2014, *Chaos Coding Based QAM IQ-Encryption for Improved Security in OFDMA*-PON, IEEE Photonics Technology, Vol. 26, No. 19, PP. 1- 4,
- Wei Zhang, Chongfu Zhang, Chen Chen, Wei Jin and Kun Qiu, 2015, *Joint peak-to-average power ratio (PAPR) reduction and physical layer security enhancement*, IEEE Photonics Technology Letters, Vol. 28, No. 9, PP. 1-4.
- Wei Zhanga, Chongfu Zhanga, Chen Chenb, 2016, *Chaos Based IQ Encryption for PAPR reduction and security enhancement in OFDMA PON system*, Procedia Engineering, Vol. 140, PP. 30-35.
- Xiaonan Hu, Xuelin Yang, Zanwei Shen, Hao He and Weisheng Hu, 2015, *Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON*, IEEE Photonics Technology Letters, PP. 1-4.
- Xingyuan Wang, Q Shi, 2005, *New type crisis: hysteresis and fractal in coupled logistic map*, Chin. Journal, Vol.4, PP.501-506.
- Zanwei Shen, Xuelin Yang, Hao He, and Weisheng Hu, 2016, *Secure Transmission of Optical DFT-S-OFDM Data Encrypted by Digital Chaos, IEEE Photonics Journal*, Vol. 8, No. 3.

8. NOMENCLATURE

x_1 = The generated chaotic sequences, dimensionless.

x_2 = The generated chaotic sequences, dimensionless.

$\mu_1, \mu_2, \mu_3,$ and μ_4 = Coupled of logistic map, dimensionless.

A_1 and A_2 = Binary chaotic sequences are used to control the signs of I and Q of QAM symbol**,** dimensionless.

C_n = QAM mapped symbol at *nth* subcarrier, dimensionless.

a_n and b_n = Real and imaginary part of mapped symbol at n^{th} subcarrier, dimensionless.

N = Number of IFFT points, dimensionless.

C'_n = The output of IQ encryption at the n^{th} subcarrier, dimensionless.

$\rho(k)$ = The aperiodic autocorrelation coefficients, dimensionless.