Journal of Engineering Science and Technology
Vol. 17, No. 4 (2022) 2602 - 2614
© School of Engineering, Taylor's University

A LOW LATENCY SCHEME FOR SECURING OFDM-BASED COMMUNICATIONS

ODAY A. L. A. RIDHA, GHASSAN NIHAD JAWAD*

Department of Electronics and Comm., College of Engineering,
University of Baghdad, Al Jadriya Campus, Baghdad, Iraq
*Corresponding Author: Ghassan.n.jawad@ieee.org

Abstract

In this paper, a secure OFDM-based communication system with low complexity is proposed. The encryption/decryption process is based on remapping the Quadrature Amplitude Modulation (QAM) symbols at the transmitter/receiver side using three locally-generated chaotic sequences. These sequences are generated by solving a three-dimensional Lorenz chaotic system in the digital domain. The main feature of the proposed scheme -in addition to providing a high level of security in the physical layer- is the simplicity with which the encryption/decryption processes are performed. This is achieved by replacing complex operations required by other schemes by simple logic operations that have the ability to substantially reduce the computational power and resources. The proposed encryption technique is tested by transmitting images over the system, which results in a complete obliteration of the residual intelligibility of the images for any unauthorized user. Moreover, the Peak to Average Power Ratio (PAPR) of the signal resulted from transferring images has been significantly reduced by more than 6 dB without using any additional stage or operation that would increase the complexity of the system. This reduction would yield a lower Bit Error Rate (BER) for any given modulation scheme and/or number of OFDM carriers. These results indicate that the proposed scheme should be highly beneficial to high-speed networks, where secure transmission with low latency is essential to cope with the increased traffic load.

Keywords: Data security, OFDM, Physical layer security, Quadrature amplitude modulation, Random sequences.

1. Introduction

The increasing demand for higher data rates, combined with the limited available spectrum, have drawn attention to spectrally-efficient high speed communication networks during the last decade. Orthogonal Frequency Division Multiplexing (OFDM) has been proposed as the optimal solution for such networks due to its high spectrum efficiency and feasible implementation [1-3]. However a significant challenge emerged as numerous modern applications required maintaining a high level of security while coping with the increased traffic load.

Many techniques are used to enhance the security of an OFDM networks by focusing on the encryption of the upper layers of the system. Such approach confines the security to the data frames, leaving control frames and headers without protection. Meanwhile, the physical layer features a transparent pipe meant for all services and users. Hence, applying the encryption in the physical layer can prevent vicious attacks by encrypting all the frames and their headers [4].

Among other techniques, chaos-based secure communication systems have gained prominence as superior approaches to provide data confidentiality in the physical layer while maintaining a relatively low level of complexity. In chaotic-based OFDM systems, the transmitted signal is concealed by an unpredictable random-like chaos sequence that efficiently counteract malicious users. Numerous chaos-based encryption approaches have been reported. A quadrature amplitude modulation (QAM) encryption was proposed [5-8], where real and imaginary parts of the QAM symbols were separately multiplied by chaotic sequences.

Alternatively, chaotic scrambling has also been deployed in the frequency domain, using either Discrete Fourier Transform [9], Fractional Fourier Transform (FrFT) [10], Discrete Hartley Transform (DHT) [11], or Welsh-Hadamard Transform (WHT) [12]. Most of these approaches require complex operations, rendering their implementation significantly costly and impractical for fast communications. Moreover, the main focus of the aforementioned works has been on the complexity of the encryption process rather than the random sequence generation.

In this work, a low-complexity chaotic-based QAM encryption technique is proposed. Contrary to the reported techniques in [5-7, 9-11, 13-16], the proposed technique can efficiently secure data in the physical layer by using a 3-Dimensional (3D) chaotic system without requiring complex multiplication or excessive memory usage. Therefore it can be efficiently implemented using traditional DSP processors or FPGA [17]. Since chaotic-based systems are sensitive to initial conditions and control parameter changes [18], a small variation in the initial states and/or the parameters of the chaos system might lead to a considerably different behavior [5]. To overcome the problems associated with physical continuous time chaotic systems, such as synchronization and regenerating the same sequences, the differential equations used to generate the chaotic signals in the proposed system are digitized. Moreover, simulation of the proposed OFDM arrangement shows that the provided randomization will enhances the performance of the transmission system in terms of Peak to Average Power Ratio (PAPR) and, consequently, Bit Error Rate (BER) without any additional stage that might compromise the applicability of the system for high speed data transmission [19-21].

The rest of this paper is organized as follows: an overview of some basic OFDM principle is given in Section 2, the proposed system is illustrated in terms of concept and implementation in Section 3, simulation results are introduced and discussed in Section 4, and Section 5 highlights the main conclusions drawn from the results provided in the previous sections.

2. Theoretical Background

Orthogonal Frequency Division Multiplexing (OFDM) is a multi-carrier scheme that is used to enhance the spectrum efficiency in modern communication systems [22]. It is based on modulating, multiplexing, and transmitting N subcarriers in parallel. By doing so, the baud rate increases by a factor of N.

OFDM Spectral efficiency is based on making the subcarriers orthogonal to each other, which allows them to overlap without sacrificing the accuracy of the signal recovery. To achieve orthogonality, subcarrier frequencies are equally distanced from each other such that the i^{th} subcarrier will be described by Rohling [22]:

$$f_i = f_0 + i \times f_s \tag{1}$$

where f_i is the i^{th} subcarrier frequency, f_0 is the lowest frequency of the OFDM spectra, f_s is the frequency spacing, and i is the subcarrier index ($i = 0, 1, 2, \dots, N$).

Modulation is usually applied to the subcarriers by modifying both phase and amplitude of the transmitted signal using Quadrature Amplitude Modulation (QAM).

Figure 1 shows a generic block diagram of an OFDM communication system. As the data stream enters the transmitter, a parallelization process is performed to distribute the stream over N paths entering the QAM mapper. The QAM mapper converts m bits from each path into a QAM symbol ($a_i + jb_i$). Therefore the i^{th} symbol can be one of 2^m possible symbol combinations in the selected QAM modulation [23].

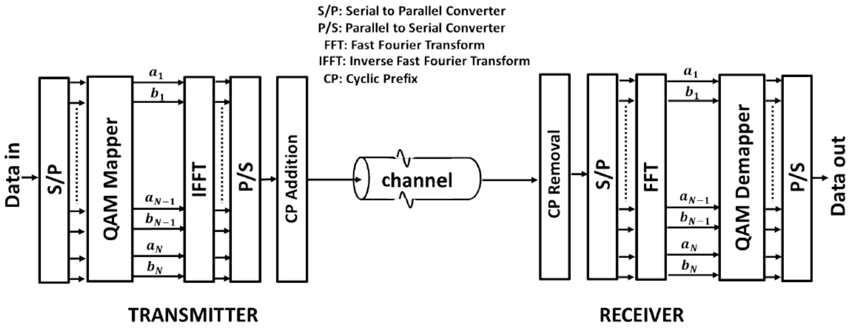


Fig. 1. Block diagram of a generic OFDM communication system.

The superposition of the orthogonal subcarriers is performed using inverse Discrete Fourier Transform (IDFT), practically realized using the Inverse Fast Fourier Transform (IFFT) algorithm.

The final step is performed by converting the N parallel paths resulted from the IFFT stage into one serial stream to be sent through the communication channel. However, to overcome the effects of Inter-Symbol Interference (ISI), a Cyclic Prefix (CP) extension is added between adjacent OFDM symbols by taking a limited length from the symbol's beginning and copying it to its end [24].

At the receiver side, the same steps are applied in the reverse order: after removing the Cyclic Prefix, the received stream is converted to N parallel paths. An FFT algorithm is then used to implement the DFT process required to obtain the N recovered symbols, which are de-mapped to get the original m bits associated with each symbol.

3. Principles of the Proposed Secure OFDM System

The main goal of the proposed encryption system is to make the BER of any unauthorized receiver as high as possible. Meanwhile, the system attempts to reduce the BER for authorized receivers.

As stated in the previous section, each m bit of the parallelized data stream is represented by a specific QAM symbol. In the proposed secure OFDM scheme, the security feature is added by changing this assignment according to pre-defined sequences that are known only by authorized receivers. To achieve this, additional stages are inserted between the QAM mapper/demapper and the IFFT/FFT stages in both the transmitter and the receiver. This stage is responsible of altering the QAM symbol assignment according to the pre-defined sequences.

The basic principles of the proposed scheme and the approaches used to implement it are respectively illustrated in the following subsections.

3.1. Proposed security scheme

Figure 2(a) shows the block diagram of the proposed OFDM transmitter. The receiver diagram is the complement of the transmitter, where the process is performed in the reverse order. The role of the N re-mappers shown in Fig. 2(a) is to reassign the parallel symbols resulted from the QAM mapping process into a new set of symbols according to three predefined, random-like binary sequences, namely x_1, x_2, and x_3 generated by a 3-Dimensional (3D) Chaos Generator.

Previous studies have shown that the behavior of such system is very sensitive to its initial state, where changing the value of any of the initial variables by as little as 10^{-16} would cause a totally different behavior and, consequently, a different sequence [11, 12, 25, 26]. Therefore, the proposed system is based on using the three initial conditions as part of the encryption/decryption key. As for the remainder of the encryption key, it consists of the bit orders used in the chaotic generator, as will be illustrated in the next subsection.

It is worth noting that the N re-mappers used in Fig. 2(a) can be replaced by a single re-mapper to be used N times to perform the same operation sequentially. Since flexibility is of high importance for embedded system designers [27], the above feature would be highly beneficial for system designers since it allows allowing a trade-off between maintaining high transmission speed when choosing the costly parallel implementation and compromising the speed by choosing the more affordable sequential implementation.

For the i^{th} re-mapper, the function is to change the real and imaginary parts of the i^{th} symbol according to the bits $x_1(i), x_2(i)$ and $x_3(i)$

As shown in Fig. 2(b), the sign of the real and imaginary parts of each symbol (a_i and b_i) are changed according to the value of the bits $x_1(i)$ and $x_2(i)$, respectively. In addition, the third bit $x_3(i)$ is used to swap the real and imaginary parts when its value is 1.

The pre-defined encryption/decryption sequences are generated using a 3D Lorenz chaotic system, as described by the following state equations [22]:

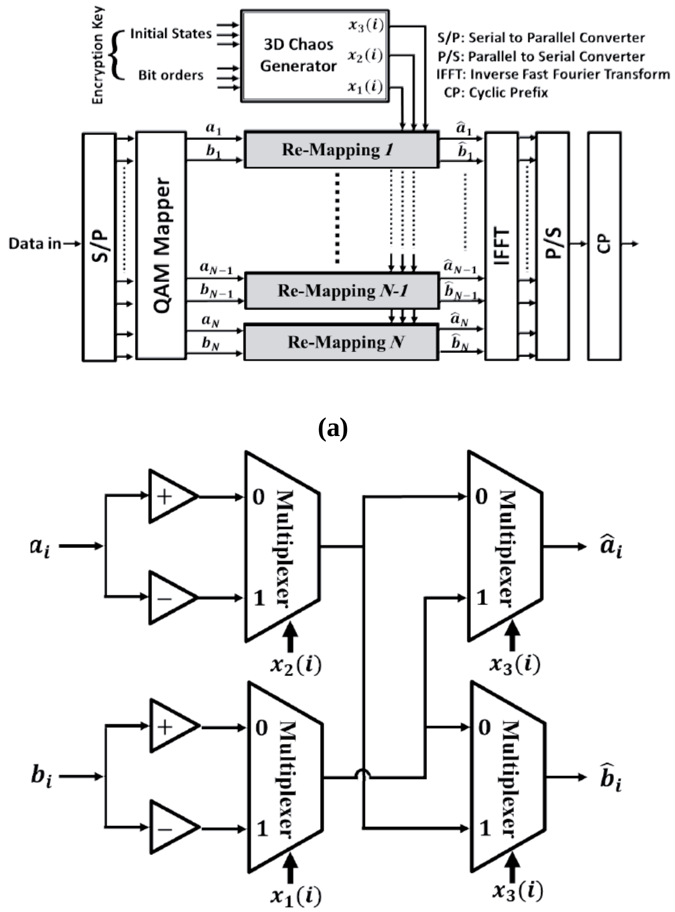
$$\dot{x}(t) = p[y(t) - x(t)] \tag{2}$$

$$\dot{y}(t) = rx(t) - y(t) - x(t)z(t) \tag{3}$$

$$\dot{z}(t) = x(t)y(t) - bz(t) \tag{4}$$

where $p, r,$ and b are the system constants [28].

Having the same binary sequences, authorized receivers can apply the opposite process to retrieve the original symbols. Unlike [11-12], the proposed remapping process doesn't require operations such as multiplications/division and addition/subtraction, which makes it fast and require less resources when implemented.



(a)

(b)

Fig. 2. (a) Block diagram of the proposed OFDM transmitter, (b) Block diagram of the i^{th} re-mapper.

3.2. Implementation of the proposed scheme

As can be seen in Fig. 2(a), the additional re-mapping stage in both the transmitter and receiver consists of two parts: N re-mappers and a chaotic binary sequence generator. Figure 2(b) shows a schematic diagram of the i^{th} re-mapper. It is shown that multiplexers are used to achieve the previously described re-mapping function. This makes hardware implementation of this stage easier in electrical domain or optical domain (in case of optical communications). This arrangement would also offer the lowest possible latency for performing the re-mapping operation.

On the other hand, in order to implement the chaotic signal generator in the digital domain, equations (2-4) have to be converted to discrete form using Euler method [29]. Here, the numerical solution is modified by choosing the system constants to be power of 2 numbers:

$$X(i+1) = X(i) + \frac{Y(i)-X(i)}{2^6} \tag{5}$$

$$Y(i+1) = Y(i) + \frac{X(i)}{2} - \frac{X(i)}{2^6}Z(i) - \frac{Y(i)}{2^6} \tag{6}$$

$$Z(i+1) = Z(i) + \frac{X(i)}{2^6}Y(i) - \frac{Z(i)}{2^4} \tag{7}$$

In these equations, the sampling time is taken to be 10^{-6} s. As mentioned earlier, the constants $p, b,$ and r in Eqs. (2)-(4) are considered to be 8, 4, and 32, respectively. These values have been chosen as a power of two to reduce the multiplication and division processes in the discrete equations Eqs. (5-7) to simple binary right/left binary shift operations, respectively. The digital arithmetic process is performed using 64-bit signed operation to ensure that the system is in the chaotic region while maintaining a reasonable level of complexity.

To obtain the binary encryption sequences $x_1, x_2,$ and x_3 from X, Y and Z in Eqs. (5-7), one bit from each of each variable is used, as in the following equations:

$$x_1(i) = \left\lfloor \frac{X(i)}{2^w} \right\rfloor mod\, 2 \qquad 0 \le w \le 31 \tag{8}$$

$$x_2(i) = \left\lfloor \frac{Y(i)}{2^q} \right\rfloor mod\, 2 \qquad 0 \le q \le 31 \tag{9}$$

$$x_3(i) = \left\lfloor \frac{Z(i)}{2^s} \right\rfloor mod\, 2 \qquad 0 \le s \le 31 \tag{10}$$

where $\lfloor \ \rfloor$ represents the floor operation, and $w, q,$ and s are the order of the bits used to determine the value of $x_1, x_2,$ and x_3, respectively.

In order to extend the encryption key space, the variables $w. q,$ and s are used as part of the full encryption key. Despite considering 64 bits to represent each of these variables, it is proposed that only the lowest order bits (1 to 32) of X, Y, and Z can be selected to form sequences $x_1, x_2,$ and x_3, respectively. This is because the lower order bits of X; Y; and Z change more frequently than higher order bits, therefore they appear more random-like and provide better security performance.

It should be noted that implementing the mod and $floor$ operations in (8-10) requires only digital multiplexers, as illustrated in Fig. 3. According to this arrangement, the full encryption key in the proposed technique will consist of the three initial values of the Lorenz system, in addition to the aforementioned variables: $w, q,$ and s.

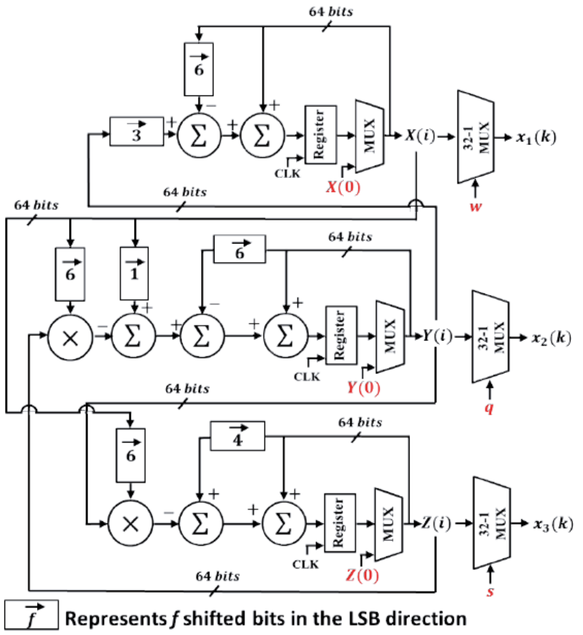


Fig. 3. Block diagram of the secure key generation circuit. The encryption key consists of $\{X(0), Y(0), Z(0), w, q, s\}$.

Figure 4 shows a 1500-points 3D line plot of the chaotic sequence resulted from solving the system in (5-7), which demonstrates the level of randomness in the generated chaotic sequence.

It can be seen from the 3-D chaotic signal generation block diagram shown in Fig. 3 that only two multiplications are used, which is a significant advantage over previously reported systems [29]. The shift blocks shown in Fig. 3 can be easily implemented using a simple reconnection.

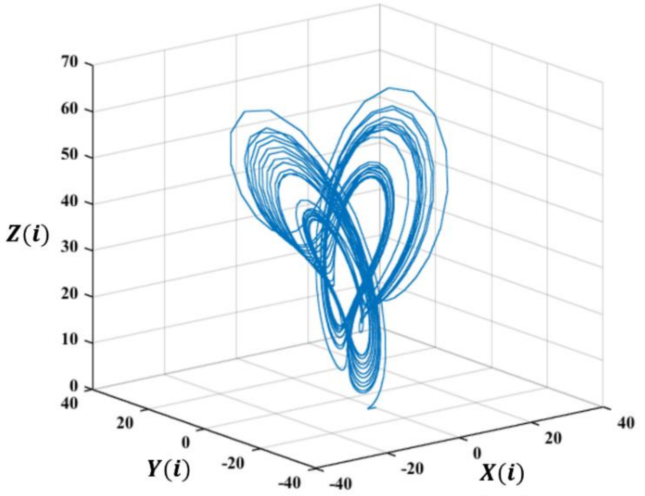


Fig. 4. A solution of the 3-D Lorenz system.

4. Simulation Results and Discussion

To evaluate the effectiveness of the proposed technique in encrypting images, a Matlab 2019® code is used to simulate the transmission of a coloured 480×480 image (shown in Fig. 5(a)) over the proposed OFDM system using $N = 1024$ subcarriers, half of which are utilized for data transmission.

Figure 5(b) shows the output of an unauthorized receiver when the image is sent using 64-QAM modulation scheme. It is obvious that it is not possible to visually identify any of the image's features, which is the case for any modulation scheme that can be employed. As for an authorized receiver, the use of a correct decryption keys will result in a fully recovered image, as shown in Fig. 5(c).

The proposed OFDM encryption system is also evaluated in terms of PAPR. The Complementary Cumulative Distribution Function (CCDF) is used to estimate the PAPR for the original signal alongside the signal resulted from the proposed system. Figure 6 shows the difference in CCDF of the transmitted image in Fig. 5(a) when using an OFDM system with and without the proposed re-mapping stage.

It can be seen that the proposed system exhibits smaller PAPR by more than 6 dB at a CCDF of 10^{-3}. The PAPR improvement shown in Fig. 6 is also found to be consistent with other types of QAM and number of QAM parallel symbols, as illustrated in Table 1. The lower values of PAPR would necessarily result into a significant reduction in the BER for any given modulation index and number of subcarriers [30, 31].

It is worth noting that the value of PAPR for each case illustrated in Table 1 depends on the distribution of the information in the two-dimensional image over the OFDM symbols (i.e., on the modulation index and the number of subcarriers). Therefore, data from pixels in the far right and far left of the image might end up in the same OFDM symbol, which makes their PAPR higher than that of symbols containing data from adjacent pixels.

This explains the inconsistency of the different PAPR values shown in Table 1. Nevertheless, it can be seen that the reduction in PAPR is consistent when comparing the values of each individual case before and after encryption.

To assess the feasibility of implementing the proposed technique, a thorough evaluation of the computational complexity of the applied scheme/algorithm has to be performed. It can be seen from Fig. 2(b) that 4 multiplexers and 2 sign inverters are required for each parallel QAM symbol. Thus, for the encryption/decryption process, only 4N multiplexers and 2N sign inverters are needed.

Table 2 illustrates the number of arithmetic operations used in the encryption process (without the sequence generator) compared to the same values for the previously reported methods [9, 11, 12].

It is clear from this comparison that the proposed system requires less arithmetic operations when compared to the other listed techniques. This reduction implies lower latency and ore applicability to high speed communication schemes, such as optical networks since it has minimum effect on the information transmission.

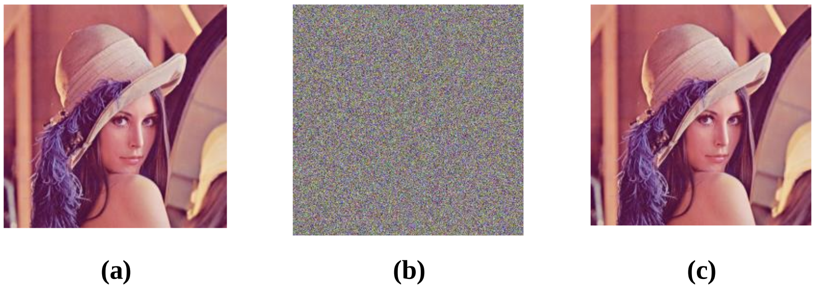


Fig. 5. Transmitted image through the proposed OFDM encryption system using 64-QAM. (a) the original image, (b) recovered image for an unauthorized receiver, (c) recovered image for an authorized receiver.

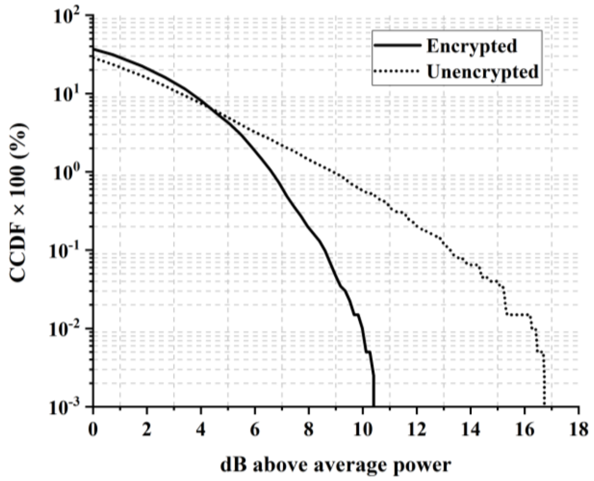


Fig. 6. CCDF of the transmitted image shown in Fig. 5(a) |using encrypted and unencrypted OFDM system.

Table 1. Effect of the encryption process on the PAPR.

Modulation Index	N	Original Image			Encrypted Image		
		Average Power (dB)	Peak Power (dB)	PAPR (dB)	Average Power (dB)	Peak Power (dB)	PAPR (dB)
4 QAM	256	9.03	29.09	20.06	8.74	18.68	9.94
16 QAM	256	14.03	33.68	19.65	15.79	30.72	14.94
64 QAM	256	21.98	37.96	15.98	21.94	32.74	10.80
64 QAM	512	19.11	34.88	15.77	19.00	29.97	10.96
64 QAM	1024	16.09	34.28	18.19	16.03	26.49	10.46

Since the generation of the chaotic sequence is inherent to the encryption process, it is essential to evaluate the computational complexity of these operations as well. From Eqs. (5)-(7) and Fig. 3, it can be noted that for each chaotic bit set (i.e., x_1, x_2, and x_3), only two multiplication and 7 addition/subtraction operations are needed. This indicates a much lower computational complexity than the chaotic sequence generation reported in [11, 12, 25]. The low number of operations is also comparable to the numbers reported in [29] and [31]. Next, the robustness of the encryption process has to be evaluated in terms of the total key space used by the system. Most researchers focus on the strength of the chaotic part by determining the number of variables and the active places each variable occupies [20, 21]. However, other researchers rely on the maximum number of trials needed to acquire the correct information from the encrypted data regardless of the chaos-generating part [11, 12]. Here, the key space will be determined from min ($key\ space_1$, $key\ space_2$), where $key\ space_1$ and $key\ space_2$ are the ones found using the first and second approach, respectively [11, 25, 26] . Since the chaotic-based systems are affected by the 16^{th} place, so the key space for a k-dimensional system is 10^{15k}. In the proposed system, one bit out of 32 is chosen for each variable as source of the chaotic sequence, therefore $key\ space_1 = 10^{15k} \times 32^k$.

On the other hand, when considering the second approach to evaluate the key space, the three bits $x_1(i), x_2(i),$ and $x_3(i)$ will results in 8 possible combinations. Taking into account the N QAM symbols, the value of $key\ space_2$ will be 8^N for each QAM symbol. Consequently, the key space for the proposed system is min ($\approx 3.2 \times 10^{49}, 8^N$). For $N = 32$, the total key space will be $\approx 3.2 \times 10^{49}$, meaning that obtaining a correct OFDM symbol through exhaustive brute force trials by the fastest computer to date (25 Tera Floating Point Operations Per Second (TFOPS)) would take around 4.05×10^{28} years.

Despite the lower security robustness of the proposed system when compared to [11, 12, 25, 26, 32], it offers much better feasibility for high speed communication networks such as Passive Optical Networks (PONs) and Visual Sensor Networks for secure image and video transmission.

Table 2. Comparison between the proposed technique and the previously reported encryption systems.

Operation Type/Method	Proposed System	[11]	[12]	[25]
Addition	$2N$	$N(N$-1)	$N(N$-1)	$N(N$-1)
Multiplication	*None*	*None*	$2N^2$	$4N^2$
Memory	*None*	N^2	N^2	$2N^2$

5. Conclusions

In this paper, a secure OFDM system for high speed communication networks has been proposed. The main advantage of the proposed system is its significantly low complexity and latency, which highly increase the feasibility of implementation for high-speed communications applications.

By re-mapping the QAM symbols in the transmission according to chaotic-generated sequences, the transmitted signal is encrypted to a high level of security with minimum number of operations and, consequently, lower latency. The proposed encryption technique has been evaluated by transmitting a coloured 480×480 image over the system.

The results show high level of security represented by the inability of unauthorized receivers to reconstruct the transmitted image regardless of the QAM modulation scheme or the number of IFFT points. In addition, the randomness resulted from the re-mapping process reduces the PAPR of the transmitted signals by at least 6 dB, which reduces the nonlinearity requirements and hence, improve the BER at the receiver side.

As a result, the proposed system represents an optimal solution for implementing secure high-speed communications networks such as Passive Optical Networks (PONs) and Visual Sensor Networks.

Nomenclatures

a_i	Real part of the i^{th} symbol
b_i	Imaginary part of the i^{th} symbol
f_0	Lowest frequency of the OFDM spectrum
i	Subcarrier index
k	Dimension of the system
m	Log$_2$ the number of constellation points in the QAM.
N	Number of Subcarriers
p, r, b	System constants
w, q, s	Bit orders
$x(t)$, $y(t)$, $z(t)$	Variables of the state equations
X, Y, Z	Digitized state equations

Abbreviations

3D	Three-Dimensional
BER	Bit Error Rate
CCDF	Complementary Cumulative Distribution Function
CP	Cyclic Prefix
DHT	Discrete Hartley Transform
DSP	Digital Signal Processing
FPGA	Field-Programmable Gate Array
FrFT	Fractional Fourier Transform
IDFT	Inverse Discrete Fourier Transform
IFFT	Inverse Fast Fourier Transform
ISI	Inter-Symbol Interference
OFDM	Orthogonal Frequency Division Multiplexing
PAPR	Peak-to-Average Power Ratio
PON	Passive Optical Network

References

1. Prasad, R. (2004). *OFDM for wireless communications systems*. Artech House.
2. Esttaifan, B.A.; AbdulRidha, O.A.; and Mahmoud, W.A. (2013). Design and Implementation of a multiplier free fpga based OFDM transmitter. *Journal of Engineering*, 19(8), 1056-1072.
3. Liu, J.; Hu, Q.; Suny, R.; Du, X.; and Guizani, M. (2020). A physical layer security scheme with compressed sensing in OFDM-based IoT systems.

Proceedings of ICC 2020-2020 *IEEE International Conference on Communications* (*ICC*), Dublin, Ireland, 1-6.

4. Liu, B.; Zhang, L.; Xin, X.; and Liu, N. (2016). Piecewise chaotic permutation method for physical layer security in OFDM-PON. *IEEE Photonics Technology Letters*, 28(21), 2359-2362.
5. Zhang, W.; Zhang, C.; Jin, W.; Chen, C.; Jiang, N.; and Qiu, K. (2014). Chaos coding-based QAM IQ-encryption for improved security in OFDMA-PON. *IEEE Photonics Technology Letters*, 26(19), 1964-1967.
6. Zhang, W.; Zhang, C.; and Chen, C. (2016). Chaos based IQ encryption for PAPR reduction and security enhancement in OFDMA PON system. *Procedia Engineering*, 140, 30-35.
7. Xiao, Y.; Chen, M.; Li, F.; Tang, J.; Liu, Y.; and Chen, L. (2015). PAPR reduction based on chaos combined with SLM technique in optical OFDM IM/DD system. *Optical Fiber Technology*, 21, 81-86.
8. Jabori, H.A.W.; and Ridha, O.A. (2019). Simple 2D chaotic remapping scheme for securing optical communication networks. *Journal of Engineering*, 25(12), 85-95.
9. Shen, Z.; Yang, X.; He, H.; and Hu, W. (2016). Secure transmission of optical DFT-S-OFDM data encrypted by digital chaos. *IEEE Photonics Journal*, 8(3), 1-9.
10. Cheng, M.; Deng, L.; Wang, X.; Li, H.; Tang, M.; Ke, C.; and Liu, D. (2014). Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation. *IEEE Photonics Journal*, 6(6), 1-9.
11. Hajomer, A.A.E.; Yang, X.; and Hu, W. (2017). Secure OFDM transmission precoded by chaotic discrete Hartley transform. *IEEE Photonics Journal*, 10(2), 1-9.
12. Hajomer, A.A.E.; Yang, X.; and Hu, W. (2017). Chaotic Walsh–hadamard transform for physical layer security in OFDM-PON. *IEEE Photonics Technology Letters*, 29(6), 527-530.
13. Zhang, W.; Zhang, C.; Chen, C.; Jin, W.; and Qiu, K. (2016). Joint PAPR reduction and physical layer security enhancement in OFDMA-PON. *IEEE Photonics Technology Letters*, 28(9), 998-1001.
14. Zhang, L.; Xin, X.; Liu, B.; and Wang, Y. (2011). Secure OFDM-PON based on chaos scrambling. *IEEE Photonics technology letters*, 23(14), 998-1000.
15. Zhang, L.; Xin, X.; Liu, B.; and Yu, J. (2012). Physical-enhanced secure strategy in an OFDM-PON. *Optics Express*, 20(3), 2255-2265.
16. Ridha, O.A.L.A.; Jawad, G.N.; and Kadhim, S.F. (2018). Modified blind source separation for securing end-to-end mobile voice calls. *IEEE Communications Letters*, 22(10), 2072-2075.
17. Muthuswamy, B.; and Banerjee, S. (2015). *A route to chaos using FPGAs* (1st ed.). Springer International Publishing.
18. Hossen, M.; Kim, K.-D.; and Park, Y. (2010). Synchronized latency secured MAC protocol for PON based large sensor network. *Proceedings of the* 12*th IEEE International Conference on Advanced Communication Technology* (*ICACT*). Gangwon, South Korea, 1528-1532.

19. Cuteanu, V.; Isar, A.; and Nafornita, C. (2011). PAPR reduction of OFDM signals using multiple symbol representations–clipping hybrid scheme. *Proceedings of SPAMEC*. Cluj-Napoca, Romania, 45-48.
20. Palanivelan, M.; Lakshmanan, M.; and Mohammed, V. N. (2019). WARP implementation of sliding taxicab norm transform technique for PAPR reduction in OFDM systems. *Telecommunications and Radio Engineering*, 78(13), 1143-1165.
21. Chitra, S.; Ramesh, S.; Jackson, B.; and Mohanraj, S. (2020). Performance enhancement of generalized frequency division multiplexing with RF impairments compensation for efficient 5G wireless access. *AEU-International Journal of Electronics and Communications*, 127, 153467.
22. Buchali, F.; Dischler, R.; and Liu, X. (2009). Optical OFDM: A promising high-speed optical transport technology. *Bell Labs Technical Journal*, 14(1), 125-146.
23. Rohling, H. (2011). *OFDM: concepts for future communication systems* (1st ed.). Springer Science & Business Media.
24. Djordjevic, I.B.; and Vasic, B. (2006). Orthogonal frequency division multiplexing for high-speed optical transmission. *Optics Express*, 14(9), 3767-3775.
25. Hu, X.; Yang, X.; and Hu, W. (2015). Chaos-based selected mapping scheme for physical layer security in OFDM-PON. *Electronics Letters*, 51(18), 1429-1431.
26. Hu, X.; Yang, X.; Shen, Z.; He, H.; Hu, W.; and Bai, C. (2015). Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON. *IEEE Photonics Technology Letters*, 27(23), 2429-2432.
27. Ridha, O.A.L.A.; and Jawad, G.N. (2020). Design considerations for a microprocessor-based Doppler radar. *Microprocessors and Microsystems*, 77, 103182.
28. Zhang, L.; Liu, B.; Xin, X.; and Liu, D. (2013). A novel 3D constellation-masked method for physical security in hierarchical OFDMA system. *Optics express*, 21(13), 15627-15633.
29. Chiu, R.; Mora-Gonzalez, M.; and Lopez-Mancilla, D. (2013). Implementation of a chaotic oscillator into a simple microcontroller. *IERI Procedia*, 4, 247-252.
30. Proakis, J.G.; and Salehi, M. (2008). *Digital communications.* (5th Ed.). McGraw-Hill, New York.
31. Giannopoulos, T.; and Paliouras, V. (2008). Relationship among BER, power consumption and PAPR. 2008 3*rd International Symposium on Wireless Pervasive Computing*, Santorini, Greece, 633-637.
32. Li, W.; Wang, C.; Feng, K.; Huang, X.; and Ding, Q. (2018). A multidimensional discrete digital chaotic encryption system. *International Journal of Distributed Sensor Networks*, 14(9), 188.