ZANCO Journal of Pure and Applied Sciences
The official scientific journal of Salahaddin University-Erbil
https://zancojournals.su.edu.krd/index.php/JPAS

ISSN (print):2218-0230, **ISSN (online):** 2412-3986, **DOI: http://dx.doi.org/10.21271/zjpas**

RESEARCH PAPER

Enhancing the Wireless System Security based on Chaotic Encryption

Hardi N. Ahmed[1] , Raghad Zuhair Yousif[2,3]
1Department of Physics, College of Science, Salahaddin University-Erbil in Erbil,Kurdistan Region-Iraq
2Department of Physics - Communication, College of Science, Salahaddin University- Erbil
3Department of information, College of information technology and Computer science technology, Catholic University in Erbil

ABSTRACT:

In the setting of 5th generation, where the amount of information transferred has drastically expanded along with the skills of communication system attackers, the necessity for a strong security system has garnered crucial relevance. This work proposes and experimentally validates a physical-layer based poly technique for securing orthogonal frequency division multiplexing for machine-to-machine communication (OFDM-M2M). The proposed model is based on a 4-D hyper digital chaotic sequences keys generator that is used to provide the necessary keys to encrypt input image data in the spatial domain using two sub-stages of permutation and one-time pad (XOR) before sending the encrypted data to the second layer of security that involves independently scrambling Quadrature Amplitude Modulation (QAM) symbols into a complex plane. The proposed system proved to enhance the capability to withstand exhaustive attacks and making it more difficult for unauthorized attackers to obtain user data. with 4-D hyper digital chaos, high-security levels are achieved in the simulation result with a sizable key space. The simulation results revealed that the proposed secure OFDM system successfully achieved zero BER at SNR=15, whereas a SNR deterioration of 1.5 dB at 10^{-4} BER has been recorded with respect to unsecure OFDM system which can be tolerated by the robustness of proposed system with massive key space of $\sim 10^{220}$, which is adequate to fend off any exhaustive attacks.

KEY WORDS: OFDM, Quadrature Amplitude Modulation (QAM), 4-D hyper digital chaos, Encryption, Signal to Noise Ratio (SNR), Bit Error Rate (BER)
DOI: http://dx.doi.org/10.21271/ZJPAS.35.SpB.2
ZJPAS (2023) , 35(SpB);9-23 .

1.INTRODUCTION :

Data interchange across open networks and internet is expanding quickly, necessitating dependable and strong security measures to maintain content privacy and avoid unwanted access (Ng et al., 2006). Different intelligent devices are connected via wireless or wired connections in M2M communication to build Internet of Things (IoT) generation networks. Without any effective human involvement, these devices communicate with one another. Due to M2M communication which take place over an open network, the confidentiality of data that includes private information is a top priority. For several reasons, M2M communication is particularly vulnerable to attackers. At first, its components frequently expend more of their power unsupervised, also this makes it simple to physically harm them. Second, since most conversations take place remotely, it is quite easy to spy on transmission links (Hussain et al., 2016).In recent years a significant increase in interest have been paid for digital chaos as a flexible substitute of device-based optical chaos that avoids the implementation challenges. Considering data encryption, it offers extremely desirable qualities like ergodicity, pseudo-randomness, and high sensitivity to the initial values. Due to high sensitivity of the hyper chaotic system to initial values, the proposed system implements the 4-D hyper chaotic map as a perfect tool to obtain chaotic sequences utilizing parameters and initial conditions. For security applications, digital chaos offers a large key space, additionally a digital chaos is simpler to use in the electric domain due to flexible digital signal processing (DSP).

Thus, this work proposed a wireless multi-layer and polytechnic security system to secure data transmitted by OFDM modulator based on 4-D hyper chaotic map. Traditionally ,AES (Advanced

* **Corresponding Author:**
Hardi N. Ahmed
E-mail: hardi.ahmed@su.edu.krd

Article History:
Received: 05/01/2023
Accepted: 12/03/2023
Published: 01/11 /2023

Encryption Standard) and DES (Data Encryption Standard) are two conventional digital encryption which they are commonly used in digital encryption systems, that may provide a high level of security (Ambika *et al.,* 2012). Due to the limited key space, these encryption methods are vulnerable to brute force attacks. These methods take a lot of processing time and power in real-time communication systems, which might cause delays (Alvarez *et al.*, 2006).

Chaotic systems are a form of complex nonlinear system that have initial values for sensitivity, pseudo randomness, and non-periodicity that are corresponding with the qualities required for cryptography. Chaotic sequences could be employed as a random key, producing the same encryption result as the first time and making it impossible to decrypt data (Farhan and Ali, 2017). As a consequence, chaotic encryption technologies especially in the field of image cryptography have become widely used (Yu *et al.*, 2019).

Data security is improved when digital chaos is combined with physical-layer encryption techniques because of its features, such as ergodicity and sensitivity to initial value. To ensure data security in OFDM, chaos-based physical-layer encryption techniques have recently been investigated and deployed (Zhang *et al.*, 2017a, Zhang *et al.*, 2017b).

Due to its beneficial impact on spectral efficiency, low multipath interference, and enormous capacity, OFDM technology still an attracted modulation technique in wireless communication system (Chen *et al.*, 2016). In recent years, several chaos-based encryption techniques have been proposed. For instance, In (Yasser *et al.*, 2020), author proposed a hybrid-chaotic multimedia encryption and decryption process has been presented; it is based on new 2-D dynamical chaotic maps and can encode and decode texts, images, audio, and videos. In (Abdallah and Farhan, 2022), the authors created a new IP table based on a 1-D logistic map to enhance the robustness of the permutation of all image pixels, secondly, a new S-Box based on 2-D Henon chaos was developed to replace the G-channel image data.

In (Yang *et al.*, 2019), a contemporary image encryption strategy has been demonstrated. This method relies on IP and S-Box proposals for the encryption process. Thus, various shuffling operations utilizing the 3D-Lorenz chaos theory, and the key process confusion and diffusion operation has been tested. Utilizing constellation-shifting mapping, dimension-constrained mapping, and circular QAM mapping.

(Rahman *et al.*, 2021), demonstrated a unique approach for OFDM-based NOMA (Non-orthogonal multiple access) physical layer security by utilizing confused constellation movement for several layers of OFDM modulates signal encryption. A method of randomly and independently mapping permutated QAM symbols onto newly chosen chaotic regions on the complex plane had been proposed by (Sultan *et al.*, 2019). The work reported by (Yang *et al.*, 2016), was based on using a 4-D digital hyper chaos to design and implement a physical-layer encryption technique against chosen-plaintext attacks (CPAs) in Optical-OFDM (OOFDM) transmission. In(Wu *et al.*, 2021), a physical-layer based dynamic key encryption system had been proposed to secure OFDM –based Passive Optical Network (OFDM-PON). In order to ensure physical-layer security in both (Direct Detection)DD and Coherent OFDM-PONs, the 7D hybrid chaotic method had been proposed by (Olewi and Fyath, 2020).

(Wang *et al.*, 2021), depicted a unique constellation encryption system based on probabilistic shaping (PS) has been suggested, where two bit-level encryption operations were initially carried out using hash values and chaotic sequences. In (Luo *et al.*, 2022), a chaos-based multi-stage encryption system and novel 3-D selective probabilistic shaping (3D-SPS) in (OFDM-PON) for improving physical layer security and transmission performance (OFDM-PON) had been demonstrated.

This study has demonstrated a novel encryption method for the physical layer security of OFDM. To accomplish the highest level of protection for data transmitted via wireless channel, the suggested scheme is built on multi-layer and poly-techniques. As a result, input data (image) in the spatial domain has been secured using both permutation and one-time pad (XOR) as the first tier of security. The QAM symbols are randomly and dynamically mapped within the complex plane at the second step, in contrast. The technique challenges conventional mapping by incorporating movable constellation points. The new QAM symbol mapping produces a constellation that resembles noise and effectively conceals the original data. To create dynamic changes in QAM dimensions, multifold encryption uses digitalized chaotic sequences. By combining various scrambling techniques with a standard QAM, the OFDM modulated signal is permutated. However, because the symbols are mapped onto predetermined locations by the scrambling algorithms, the signals are vulnerable to attacks by statistical analysis. The dynamic mapping of QAM prevents statistical analysis from exposing user info. The chaotic shifting of the QAM constellation enhances the physical-layer security of OFDM modulated data transfer.

The remainder of this paper is structured as follows. The suggested chaotic maps of the cryptosystems are described in section 2, along with the design idea of the proposed image encryption approach. Section 3 contains a full and extensively discussion of the simulation, analytical, and security analysis results. The article's conclusion is presented in section 4.

2.Materials and Methods

The presented method utilizes four-dimensional (4-D) hyper digital chaos to accomplish chaotic encryption. The following 4-D chaotic system is employed to generate the chaotic sequences: (Wei *et al.*, 2021)

$$\begin{aligned} \dot{X}_1 &= a(-X_1 + X_2) - X_2X_3X_4 \\ \dot{X}_2 &= b(X_1 + X_2) - X_1X_3X_4 \\ \dot{X}_3 &= cX_2 - X_4 + dX_1X_2X_4 \\ \dot{X}_4 &= -eX_4 + X_1X_2X_3 \end{aligned} \quad (1)$$

Where the real constants a, b, c, d, and e are the parameters. The independent chaotic sequences X_1, X_2, X_3 and X_4 acquired using the Runge-Kutta technique when the digital chaos reaches the chaotic region after a certain number of repetitions.

The four chaotic sequences (X_1, X_2, X_3, and X_4) produced by the aforementioned collection of questions serve the following main purposes: X_1 controls the row and column variations of the matrix, leading to a chaotic matrix. The chaotic output X_2, which also manages the row and column, regulates the XOR. The other two chaotic sequences, X_3 and X_4, are used to provide flexibly chaotic shifting for the in-phase (I) and quadrature (Q) constellation components of QAM modulation. The first step in the encryption algorithm is to pre-process the user's image by turning it gray and resizing it to a pre-determined size (256 x 256). Next, the user's image is presented to the first encryption layer from the poly-techniques encryption that is suggested, which is image permutation. As shown in Figure 1(which described the block diagram of proposed transmitter and receiver), two transformation vectors have been created. generated using the following process, both from the random sequence X_1. The sequence X_1 has been generated from the 4-D hyper digital chaotic is then passed to a block in which two sub-chaotic sequences X_1^1 , X_1^2 are generated.

$$X_1^1 = mod\ (Extract(X_1\ ,(m,n,p), M)) \quad (2)$$

$$X_1^1 = mod\ (Extract(X_1\ ,(m,n,p), imsz)) \quad (3)$$

And

$$X_1^2 = mod\ (Extract(X_1\ ,(n,p,m), M)) \quad (4)$$

$$X_1^2 = mod\ (Extract(X_1\ ,(n,p,m), imsz)) \quad (5)$$

Where m is the 14th digit in the decimal part of the chaotic sequence X_1 while n and p are the 15th and 16th digits of the same previously mentioned chaotic sequence. It is worth to mention that M is equal to 256 (to match the input image bitrate). These two generated random sequences then used to permutate the entire image matrix data based on the equation below:

$$I_{perm}(i,j) = I_m\ (X_1^1 + 1\ , X_1^2 + 1) \quad (6)$$

Where I_m is the original image matrix and I_{perm} is the permutated resulted image.

The second technique in the first layer is then started by XORing each pixel in image with its corresponding randomly generated symbol (from chaotic sequence X_2) and then located in random matrix XOR-matrix following procedure below:

After generating the sequence X_2 from the 4-D hyper digital chaotic its passed to a doubling block by which two sub-chaotic sequences X_2^1 , X_2^2 are generated based on the set of equations below:

$$X_2^1 = mod\ (Extract(X_2\ ,(m,n,p), imsz)) \quad (7)$$

$$X_2^2 = mod\ (Extract(X_2\ ,(p,n,m), imsz)) \quad (8)$$

By applying the One-time pad, which contributes to boosting the confusion and diffusion for the techniques in the first layer, these two sub-chaotic sequences are used to generate the XOR-matrix, which has a size similar to the original image size (256 x 256). The process of creating the XOR-matrix and then applying it to the permuted image is demonstrated by the following algorithm.

```
XRT = [ ];
for i = 1: No.of rows in the permutated image
    temp = circshift ($X_2^1$, $X_2^2$(i));
    XRT = [XRT;temp];
end
```

Thus, the sub-chaotic sequence $X_2^1 \in [0,1,2,\ldots\ldots,255]$ has been circularly shifted with a random number of times produced by the random sequence $X_2^2 \in [1,2,\ldots\ldots 256]$ which has 256 elements. Thus, one chaotic element from X_2^2 is used to produce each individual row in XOR-matrix.

Then the obtained final encrypted image matrix after XORing it with matrix can be mathematically represented by:

$$I_{enc}(i,j) = I_{perm}(i,j) \oplus XRT(i,j) \qquad (9)$$

The detailed demonstration of the proposed encryption method for the physical layer of OFDM is conducted in Algorithm 1. In the second layer of security an encryption method for the QAM modulated symbols after segmenting the input image in to frames each with 64 symbol is started dynamically map user data onto the dimensions of a higher QAM.

To implement the idea of flexibility target mapping, each QAM symbol is mapped independently from the others. New in-phase and quadrature values for each QAM symbol would be determined using the chaotic sequences X_3 and X_4 generated by applying 4D hyper digital chaos. As a result, a new mapping location will be predetermined within the constraints of traditional QAM. Due to the flexible and independent mapping of each QAM symbol, the data signals theoretically fill any space inside the dimensions, and the resulting constellation would appear to be strongly influenced by chaos. The resulting constellation improves security due to the random, independent mapping and built-in QAM symbol scrambling. The dynamic distribution of QAM symbols in the complex plane would result in the random distribution and scrambling of the new array. Despite the fact that the mapping of each QAM signal is independent of the others, noise significantly affects the final constellation for an unauthorized user. Thus, the in-phase and Q-phase components of the QAM symbol are shifted by the values(Ie, Qe) calculated below(Rahman et al., 2021):

$$Ie = -2 + 4 * \left[mod\left(abs(X_3), floor\left(abs(X_3)\right)\right)\right] \qquad (10)$$

$$Qe = -2 + 4 * \left[mod\left(abs(X_4), floor\left(abs(X_4)\right)\right)\right] \qquad (11)$$

The encryption procedure at this level is implemented by adding both of (Ie, Qe) to the output symbol from the traditional QAM *(I,Q)* :

$$Ienc = I + Ie \qquad (12)$$

$$Qenc = Q + Qe \qquad (13)$$

After serial to parallel (S/P) conversion, conventional QAM mapping, and QAM symbol permutation (to determine a new dynamic position), the IFFT is applied to each frame to bring it back into the time domain. Before adding a cyclic prefix of duration 1/16 of the OFDM signal, the time signal of each frame is converted from parallel to serial. After that, the encrypted OFDM modulated signal is transmitted over an AWGN channel with an SNR of between 1 and 20 dB. Table 1 contains a list of the specifics of the simulated parameters used in the suggested system simulation. The receiver side will perform the decryption using the reverse sequence of each step in the encryption process. A minor difference ($\sim 10^{-15}$) from the initial value will result in new chaotic sequences, making restoration of the original data impossible due to the security provided by the proposed scheme's employment of 4-D digital chaos.

This section is demonstrated Algorithm 1. describes the mechanism of encryption and decryption process.

The Encryption and Decryption proposed Algorithm1

```
Results: Compute proposed system BER, Output encrypted and decrypted images.
Calculation processes: Hyperchaotic4D($imsz,N_{subcarriers},m,n,p,key$), XorMatrix(imszs,imsiz),imageperm(I, $X_1^1$,$X_2^1$), Xor_enc($I_{perm}$, Xor_Matrix) modulmap(mod_type,img_vec),imagetovec(I,$N_{subcarriers}$,$\log_2(M)$),iqdetection(y,ref), vectoimage(y,imsz, $\log_2(M)$),BER_Calculation(X,Y);
Initialize: key=initial key; EsNodB=setting the range of symbol energy to noise ratio; mod_type=set the type of modulation either ‘MPSK’ or ‘MQAM’; M=Modulation order; $N_{subcarriers}$ =total number of subcarrier in OFDM system; imsz=square image size;m,n,p=the $m^{th}$, $n^{th}$ $p^{th}$ order numbers after decimal points in chaotic sequence Xi;
 Procedures: At transmitter side
Read digital image I;
Convert I from RGB to gray;
Resize I to [imsz, imsz];
Generate the four chaotic sequences by simulation the function   Hyperchaotic4D($imsz,N_{subcarriers},m,n,p,key$)
The outputs are:  $X_1^1$,$X_2^1$, $X_2^1$ ,  $X_2^2$;
Generate the first two chaotic sub-sequences $X_1^1$,$X_2^1$ as shown below:
$X_1^1 = mod\ (Extract(X_1\ ,(m,n,p),imsz))$;
$X_1^2 = mod\ (Extract(X_1\ ,(n,p,m),imsz))$;
Generate the second two sub-sequences $X_2^1$ ,  $X_2^2$ as shown below:
$X_2^1 = mod\ (Extract(X_2\ ,(m,n,p),imsz))$;
$X_2^2 = mod\ (Extract(X_2\ ,(p,n,m),imsz))$;
Generate the XOR-Matrix
For each row in input image
    Xor_Row=circshift($X_2^1$ ,  $X_2^2$);
    Xor_Matrix=[Xor_Matrix; Xor_Row];
End
For All elements of EsNodB
    $I_{perm}$=imageperm(I, $X_1^1$,$X_2^1$);
    Apply xor between permutated image and Xor_Matrix : d_xor= Xor_enc($I_{perm}$, Xor_Matrix );
    Convert image to vectors: [imgvec,$N_{vect}$]=imagetovec (d_xor, $N_{subcarriers}$ , $log_2(M)$);
    Apply MPSK or MQAM modulation to each vector: [d_mod,ref]= modulmap(mod_type,imgvec)
    Generate the scattering formula to encrypt I, and Q data:
    $Ie = -2 + 4 * \left[mod\left(abs(X_3), floor\left(abs(X_3)\right)\right)\right]$;
    $Qe = -2 + 4 * \left[mod\left(abs(X_4), floor\left(abs(X_4)\right)\right)\right]$;
    Calculate the encrypted modulated complex vector using the formula below:
    $I_{enc}$=d_modI+$I_e$
    $Q_{enc}$=d_modQ+$Q_e$
    Construct the complex vector $X_{enc}$ form both components $I_{enc}$ and $Q_{enc}$
    Applying IFFT on the vector $X_{enc}$ then adding cyclic prefix to the vector to it before transmission over AWGN channel.
    At receiver side:
    Generating the vector Y by applying FFT to each received vector R after removing the cyclic prefix.
    Decrypt Y by subtracting the same values of scattering vectors calculated at transmitter side.
    $I_{dec}$=$Y_I$-$I_e$;
    $Q_{dec}$=$Y_Q$-$Q_e$;
    Constructing the vector $Y_{dec}$ from the two components $I_{dec}$ and $Q_{dec}$ then calculate the demodulated vector $Y_{demod}$.
    $Y_{demod}$ =iqdetection($Y_{dec}$, ref);
    Calculate the BER: BER_Calculation (imgvec, $Y_{demod}$);
    Reconstruct image from its vectors: Irec= vectoimage ($Y_{demod}$, imsz, $log_2(M)$)
End
Decrypt the image by first Xor its matrix with the same Xor_Matrix generated at transmitter then decipher the image finally by
 inverse permutation.
Show encrypted image
Show the decrypted image
End
Draw the calculated BER.
```

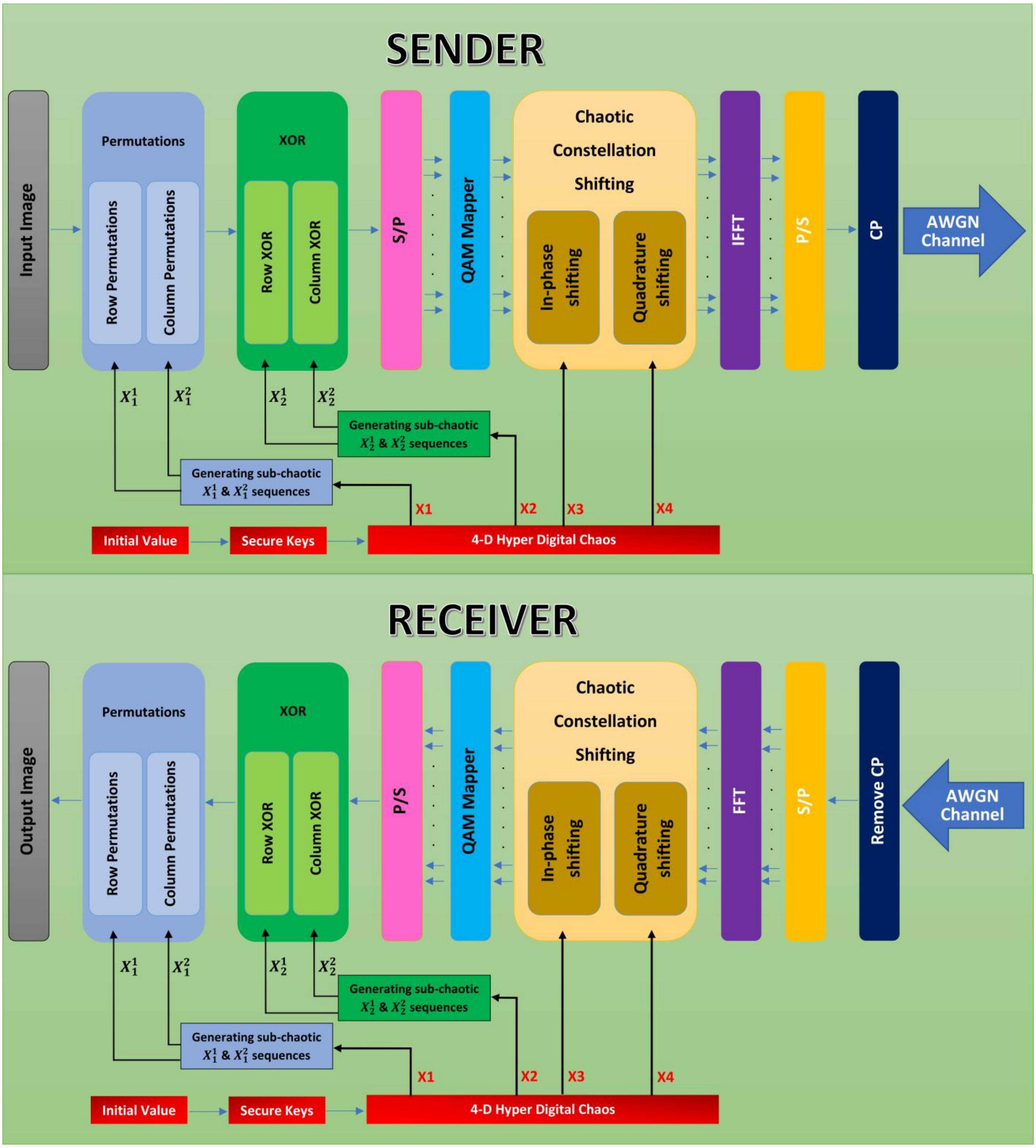


Figure 1. Block diagram of the proposed chaotic encryption scheme

Table 1: Parameters used in the OFDM encryption system

Parameters	Values
SNR	**1-20 (dB)**
Modulation order	**16**
FFT/IFFT size or total number of subcarriers	**64**
Cyclic prefix	**16**
Key	**10.253698741251084**
a	**35**
b	**10**
c	**80**
d	**0.5**
e	**10**

3.Results and Discussion

The computer simulation demonstrates the viability of the suggested encryption method. The effectiveness of the suggested secure OFDM with 16-QAM modulator is shown in Figure 2. Both legitimate and unauthorized recipients are taken into account on the recipient side in this simulation. The authorized user who is conscious of the pre-shared keys is referred to as the legal receiver, while the unauthorized user who is ignorant of the pre-shared keys is referred to as the illegal receiver. The same encrypted OFDM signal that the approved user receives can also be received by the unauthorized user. The approved user would be able to de-map the noisy constellation into a typical 16-QAM constellation using the pre-shared keys. An unauthorized person cannot obtain any information from the constellation.

The state-of-the-art OFDM signal has been compared to our suggested encryption physical layer security OFDM system. When compared to an unsecure OFDM signal, Figure 2 shows that the proposed secure OFDM signal system exhibited SNR degradation of 1.5 dB at 10^{-4} BER. Only legitimate user, which exchanges the right initial keys with the Sender, can decode and retrieve the original data from the encoded OFDM data, as demonstrated in Figure 2. for the lower BERs. The received noisy constellation doesn't provide correct information to an unauthorized user. It's important to note that the theoretical BER for theoretical OFDM drops to zero at SNR (16–20 dB), meaning the original data can be received entirely noise-free. The simulated secure OFDM signal performs similarly to the theoretical OFDM until 15 dB of SNR. The constellation diagram for both authorized Figure 3(a) and unauthorized Figure 3(b) receivers is shown in Figure 3. Even though channel noise has an impact on the original QAM symbol created at the transmitter part, it is evident that the receiver can still demodulate the QAM symbol after computing the FFT for each farm. In contrast, Figure 3(b) displayed the constellation map retrieved by the unauthorized person, in which channel noise in addition to the chaotic sequence mapping that was used at the transmitter part to create the chaotic constellation map in Figure 3(b) that completely chaotic and by which the unauthorized person demodulate the OFDM signal correctly. At first layer of security (After introducing the original image to the system), permutation process is executed. Thus, every pixel of the image is replaced with a new position inside the limited size of the original image. Consequently, the image will be shuffled totally. Permutation is depicted in the Figure 4 by displaying the scattering diagram of rows vs. columns after permutation. Figure 5 also demonstrates the scattering diagram of the one-time pad matrix that would be XORed symbol by symbol with the permutated image. The XOR process its contributes in increasing the encryption system complexity and hence enlarges the key space for the system. It’s obvious that the pixels changed their positions to the new position based on the mathematical function applied for the XOR operation.

Figure 6, is presented to better explain what occurred to the transmitted image by presenting the original image that was transmitted through various SNR levels. As can be seen subjectively in the images, the BER reduced as the SNR increased (image quality improved gradually as channel SNR improved), the first image is at BER of 1dB sounds to be deeply affected by channel noise than the second at 2 dB, and so on. From images (16-20), 100% of the images have been successfully recovered.

Figure 7 shows the histogram analysis for the original, encrypted, and decrypted pictures, respectively. In this context, it is evident that the encrypted image's histogram almost resembles a uniform probability distribution, indicating that the encrypted image's entropy, which is a measure of uncertainty, is near to its maximum value.

After the encrypted image was broadcast (b) through an OFDM channel to the receiver after the transmission of the plain image (a), the receiver was able to decrypt the ciphered image as shown in (c). Without the encryption keys used to encrypt the image, it would be difficult to decrypt the image, so this was made feasible by the receiver's prior knowledge of the keys. It can be seen that the encrypted image contains no information about the original image. Additionally, the encrypted image's histogram (e) is almost uniform. Any attempt to expose information about the image by attacking the histogram will fail. As a result, the suggested approach offers effective image encryption. The set of all keys used for encoding and decoding can be used to evaluate how strong the proposed chaotic encryption system is.

Figure 8 depicts the 4-D chaotic system used in the presented system's sensitivity to initial key shift. When the initial key x_0 is marginally altered (x_{01}=10.236987412510844, x_{02}=10.236987412510855) by about 10^{-15}, it can be demonstrated that the chaotic sequence X_1 has been significantly altered.

Figure 9 illustrates the sensitivity to initial key value selection and demonstrates that the decrypted image would be accurate if the initial value chosen by the transmitter is x_{01}=10.236987412510844 and this value is used at the receiver side without any modification (9).b. However, if the receiver marginally altered the initial key, such as by changing it to x_{02}=10.236987412510855 for example, the decrypted image would be chaotic, as shown in Figure 9(c).

Key sensitivity is one of the most important characteristics of chaotic cryptography. Encrypted data cannot be decrypted because even a small change to the key will result in various outcomes during decryption, regardless of whether only one parameter has changed. In order to decode the data, it is also necessary to know the order of the keys. Since 16-QAM signals use 64 subcarriers, each of which is represented by 4 bits, the key space generated by the chaotic XOR sequence is 2^{256} bits, and the key generated by the permutation procedure is also 2^{256} bits. The key space of the 4-D hyper chaos is typically estimated to be 1060 ($10^{15} \times 10^{15} \times 10^{15} \times 10^{15}$). The accuracy of 10^{-3} is recommended for the in-phase and quadrature shifting parameters for significant shifting on the final constellation, so it produced an extra key space of $10^{3} \times 10^{3}$. To increase the security of the suggested scheme against any brute force attacks, a key space of $2^{256} \times 2^{256} \times 10^{3} \times 103 \times 10^{60}$ ($\sim 10^{220}$) is accomplished overall. To further ensure the high degree of security during data transmission, a higher order QAM and an increasing number of subcarriers can be used. With the usage of 4-D hyper digital chaos to perform encryption, the confidentiality is improved. Moreover, this sensitivity of the 4-D hyper digital chaos system will alone provide a key space of $\sim 10^{220}$.

A digital hyper-chaotic system was used to acquire the chaotic sequences X_1, X_2, X_3, and X_4 in order to confirm the output of the chaos generator was truly random. Chaotic attractors are seen in Figure 10. The complex forms of the attractors demonstrate chaotic behavior, indicating that the chaos generator has reached the chaotic region. This makes the hyper-chaotic system much more random and makes it more challenging for an attacker to identify the chaotic sequences since the dynamic properties of the hyper-chaotic system are exceedingly complex under this circumstance.

Therefore, when using the 4-D hyper-chaotic map, the proposed encryption technique is reliable and secure. Further evaluation of proposed encryption scheme, has been achieved by a comparison with some literatures (Rahman et al., 2021, Wang et al., 2021, Wei et al., 2021)(Table 2) in term of the key space which proved the superiority of the proposed method. The method suggested by the proposed secure system also demonstrated better performance in terms of BER vs. SNR, with zero

BER achieved at 16 SNR as opposed to Rahman et al., 2021's other work, which did not achieve zero BER at that SNR.

Table 2: Comparison of our proposed method to the other related methods

Encryption method	**Key space**
Our proposed method	~10^{220}
Ref (Hu *et al.*, 2015)	~10^{120}
Ref (Ren *et al.*, 2020)	1.98×10^{73}
Ref (Zhao *et al.*, 2020)	10^{126}
Ref (Wu et al., 2021)	10^{66}
Ref (Cheng *et al.*, 2014)	10^{67}
Ref (Zong *et al.*, 2020)	10^{45}
Ref (Wang et al., 2021)	10^{121}

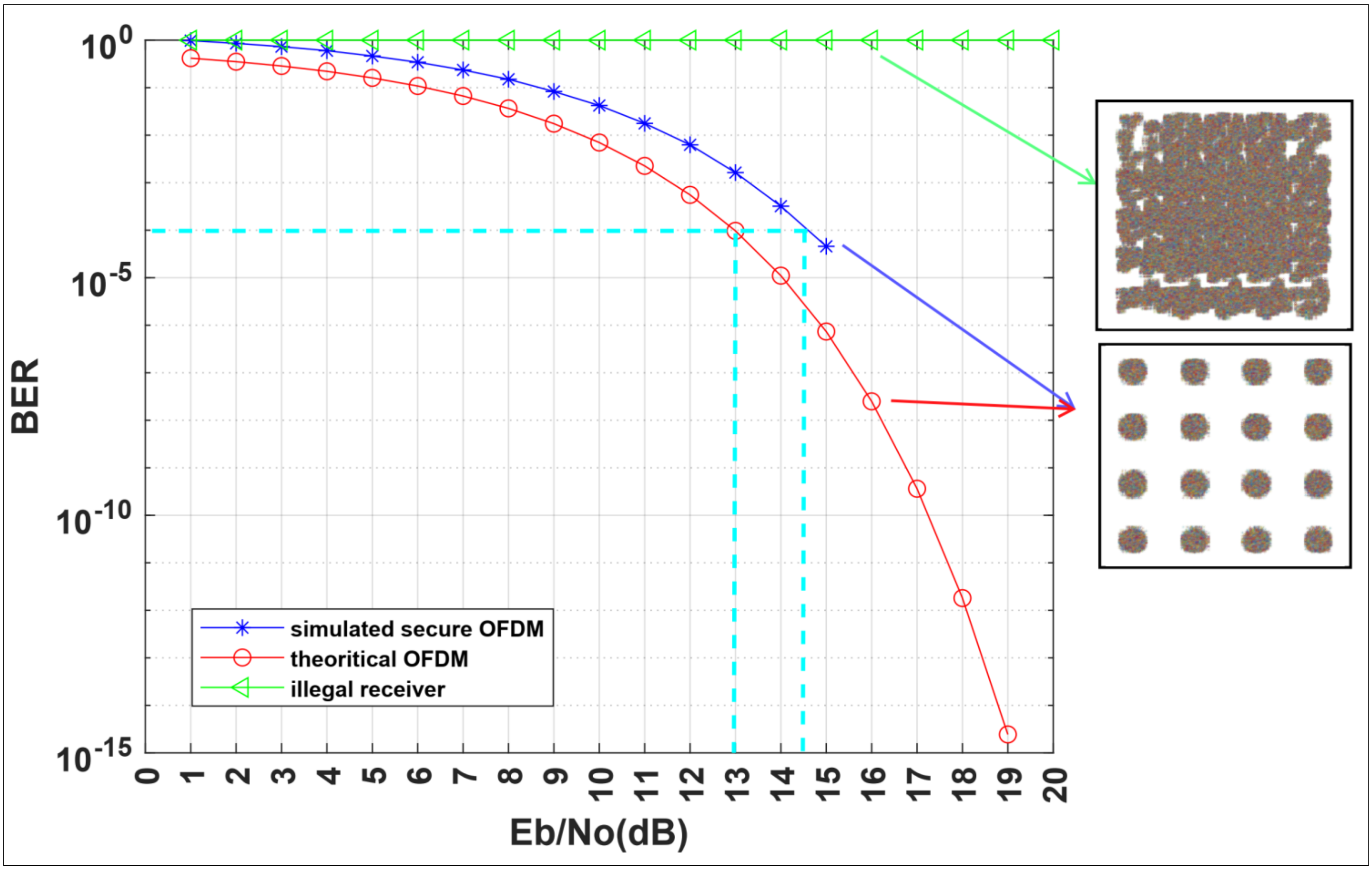


Figure 2. In the QAM-16, the signal-to-noise ratio (SNR) vs bit-error rate (BER) is shown.

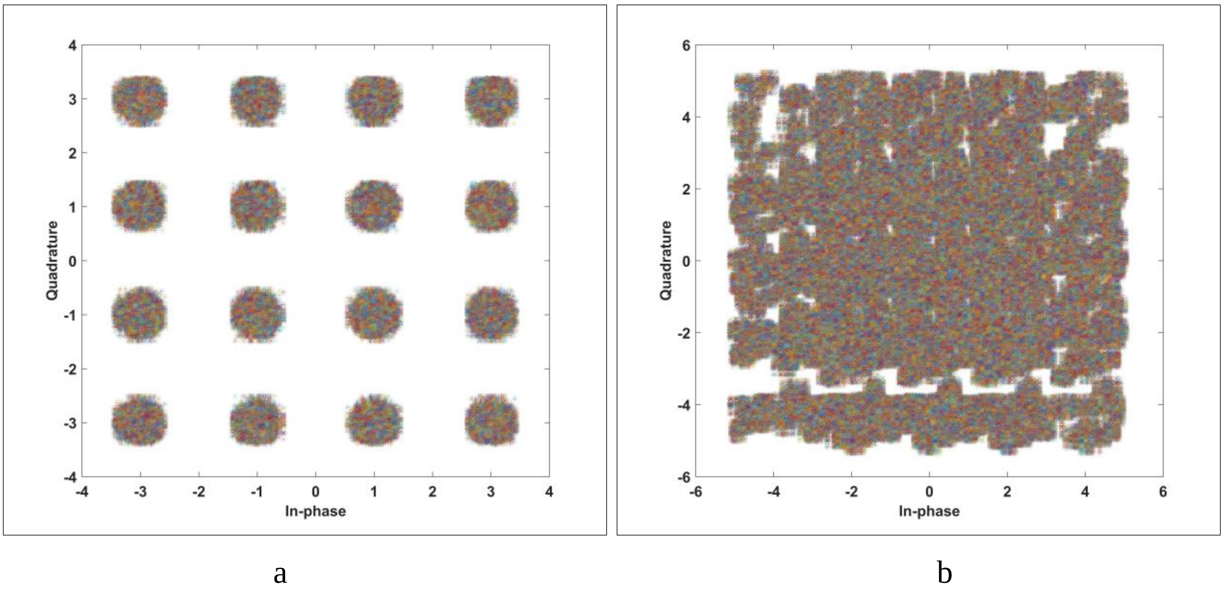


Figure 3. (a) the conventional constellation of 16-QAM, (b) the noisy constellation of 16-QAM

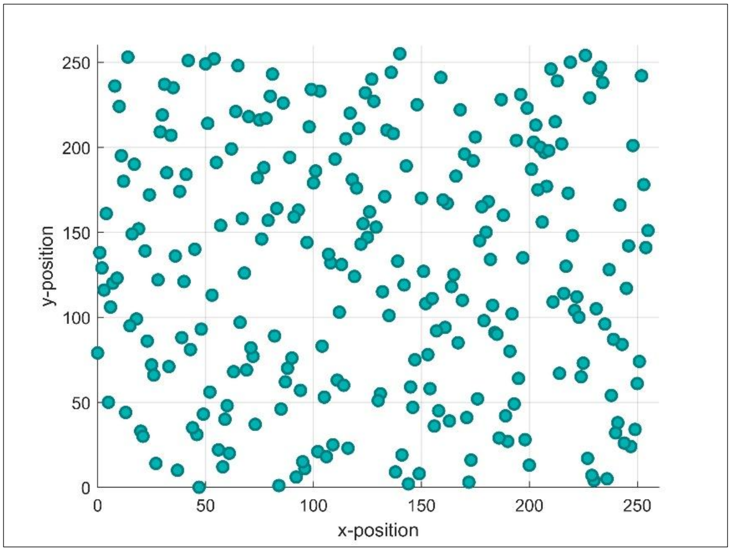


Figure 4. Rows vs Columns Hyperchaotic permutation arrays

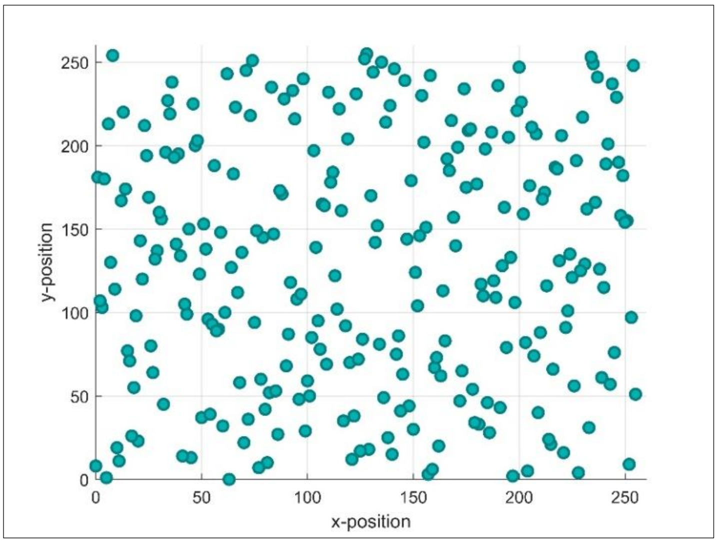


Figure 5. Rows vs Columns Hyperchaotic XOR array

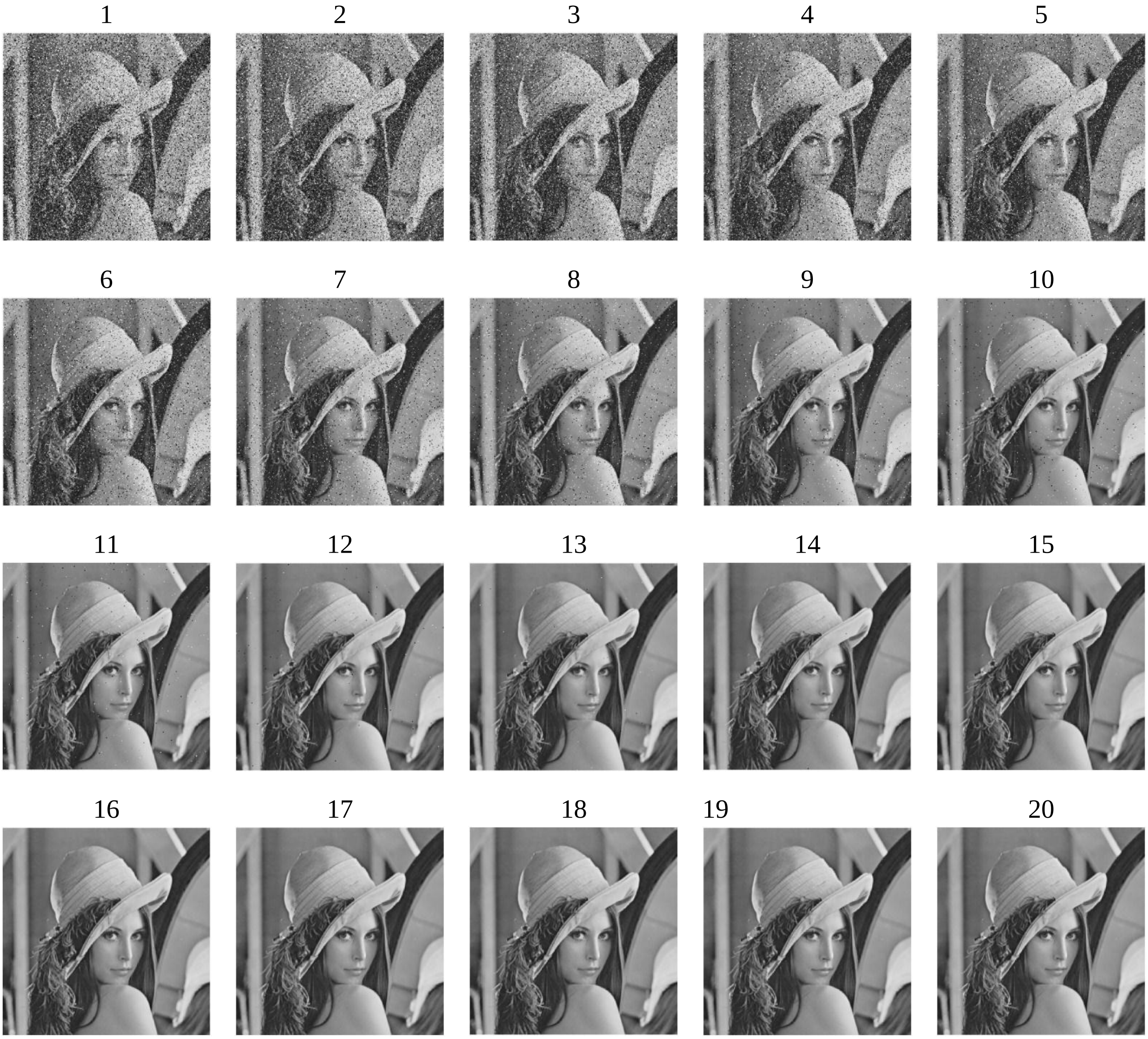


Figure 6. Transmitted image with SNR (1-20) dB

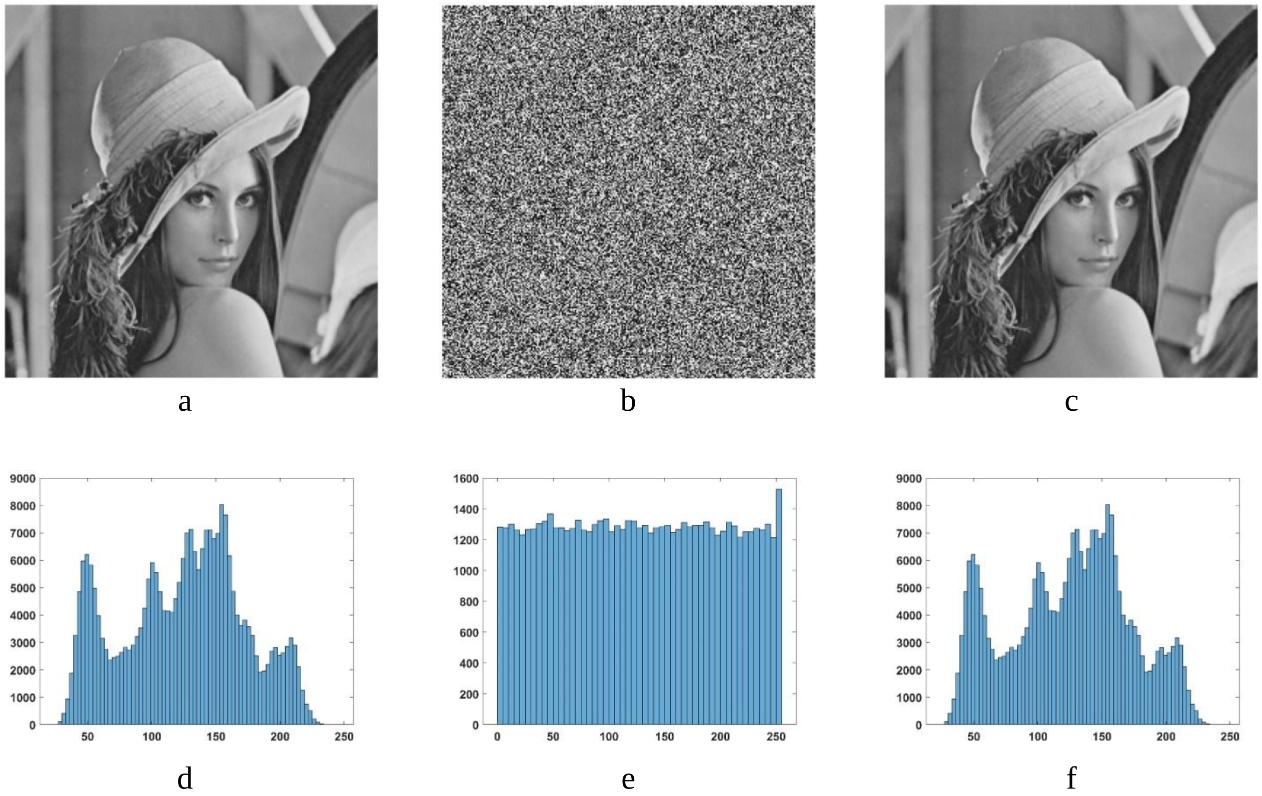


Figure 7. Image encryption and decryption with corresponding histograms of the following images: (a) plain image, (b) encrypted image, (c) decrypted image, (d) histogram for plain image, (e) histogram for encrypted image, (f) histogram for the decrypted image.

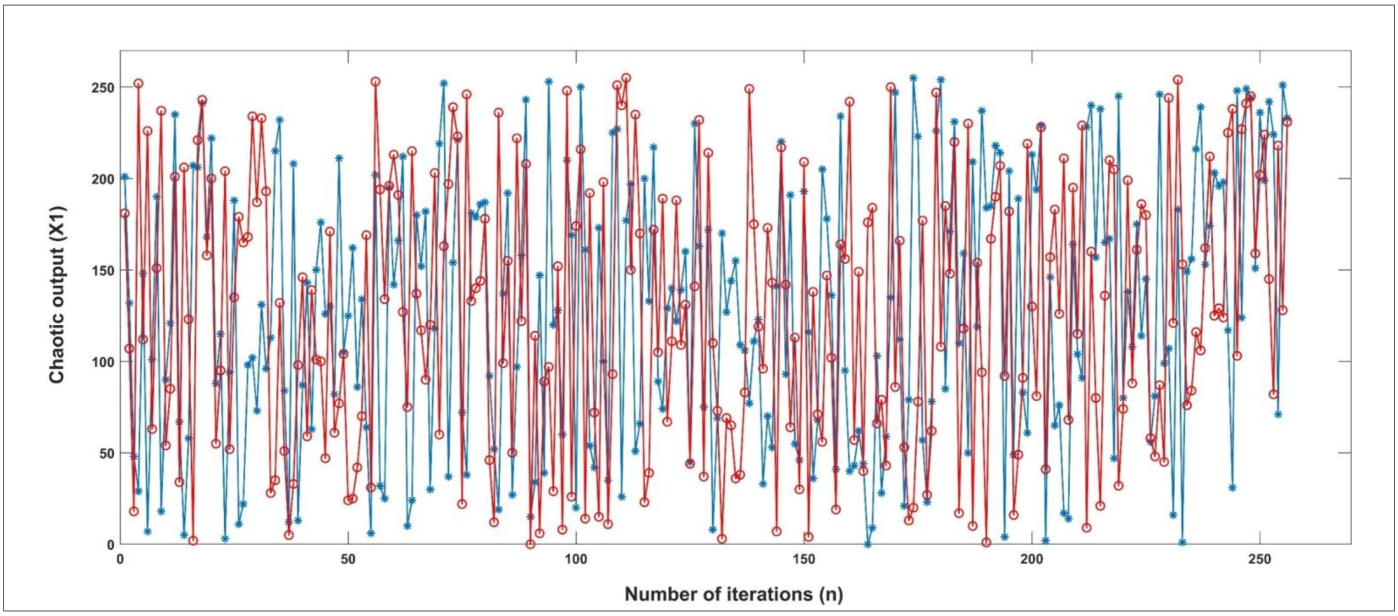


Figure 8. shows how sensitive the chaotic output sequences are to the initial key, taking X1 as an example.
X01= 10.253698741251084
X02= 10.253698741251085

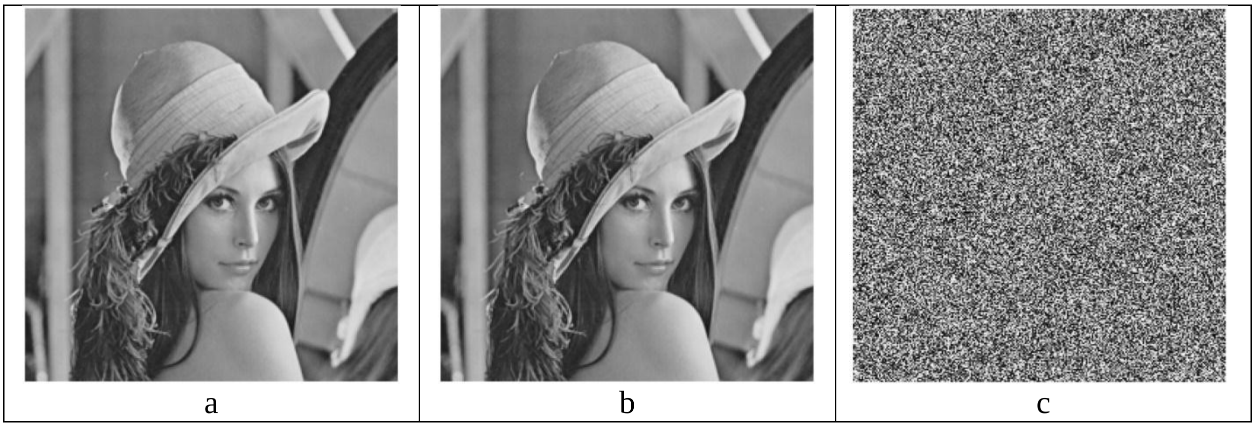
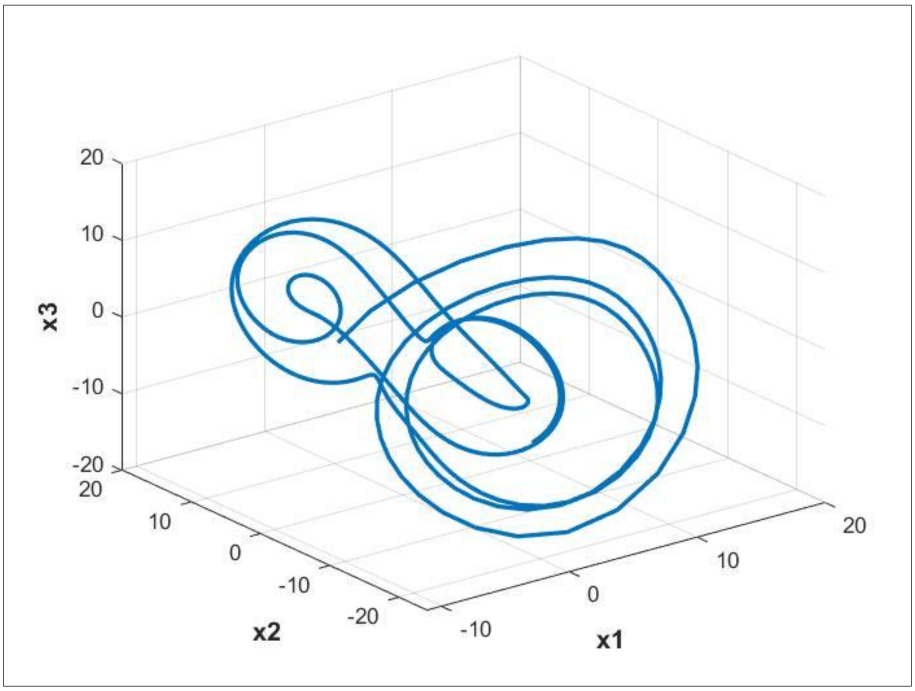
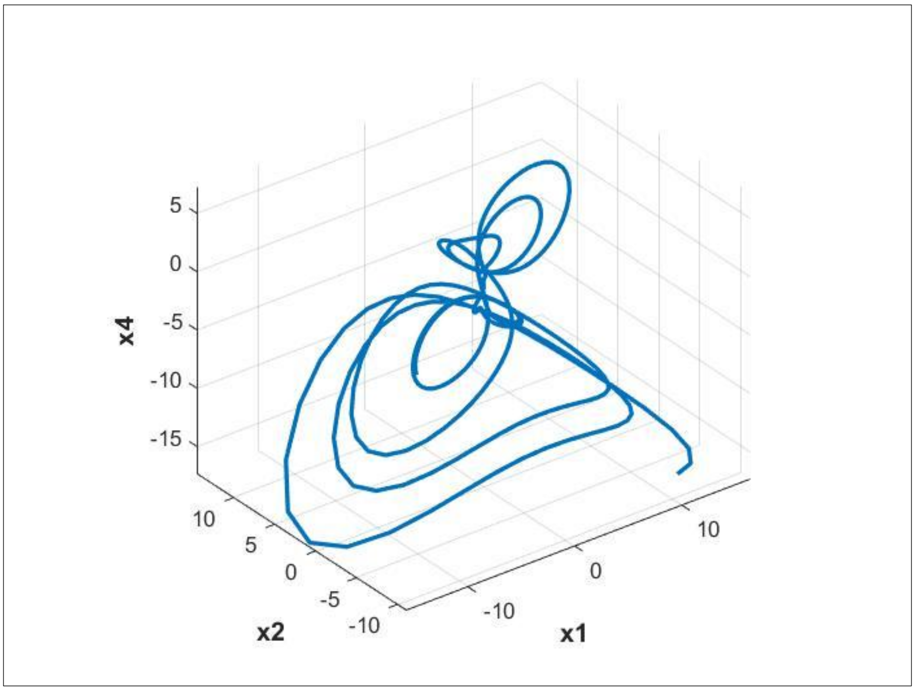


Figure 9. displaying the key sensitivity and the encryption and decryption processes using various keys.
Figure 9(a) the original image
Figure 9(b) the decrypted image with correct initial key. X01= 10.253698741251084
Figure 9(c) the decrypted image in case of initial key at transmitter is different from that used at receiver. X02= 10.253698741251085



a



b

Figure 10. Hyperchaotic attractor of 4-D hyper-chaotic system (a) phase space X_1 versus X_2 versus X_3, (b) phase space X_1 versus X_2 versus X_4.

4.Conclusion

In this paper, the confused constellation moving to multifold OFDM information encryption, a 4-D chaotic encryption algorithm has been proposed to improve both the security performance and transmission performance in OFDM in M2M communication. According to the results of the simulation, the constellation shifting was successfully carried out, resulting in an elastic constellation with dynamic in-phase and quadrature shifting dimensions. Additionally, permutation and XOR were carried out to achieve a greater security level.

The proposed chaotic scheme is very sensitive to the initial values, and any change in any value leads to a significant change result in all the chaos output sequences, which are utilized for permutation, XOR operations, in-phase shifting, and quadrature shifting in the constellation diagram.

In addition to efficiently transmitting a noisy constellation to encrypt user data, the techniques also offer a large key space ~10^{220} to secure the original data from any comprehensive cyberattacks, since key space is the most important parameter, therefore this huge key space can guarantee the high security for the system.

In the simulation, the suggested chaotic OFDM data encryption approach has been effectively shown. Additionally, the transmission performance for the data that is chaotically encrypted is enhanced by the change in SNR. These cryptographic techniques could make good alternatives for reliable OFDM transmission.

Since the dynamic properties of the hyper-chaotic system are extremely complicated, the hyper-chaotic system becomes much more random and more difficult for an attacker to identify the chaotic sequences. Therefore, the suggested encryption method is safe and secure when used with the 4-D hyper-chaotic map.

References

ABDALLAH, A. A. & FARHAN, A. K. J. I. J. O. S. 2022. A New Image Encryption Algorithm Based on Multi Chaotic System. 324-337.

ALVAREZ, G., LI, S. J. I. J. O. B. & CHAOS. 2006. Some basic cryptographic requirements for chaos-based cryptosystems. 16**,** 2129-2151.

AMBIKA, D., RADHA, V. J. I. J. O. E. R. & APPLICATIONS. 2012. Secure Speech Communication–A Review. 2**,** 1044-1049.

CHEN, M., XIAO, X., HUANG, Z. R., YU, J., LI, F., CHEN, Q. & CHEN, L. J. J. O. L. T. 2016. Experimental demonstration of an IFFT/FFT size efficient DFT-spread OFDM for short reach optical transmission systems. 34**,** 2100-2105.

CHENG, M., DENG, L., WANG, X., LI, H., TANG, M., KE, C., SHUM, P. & LIU, D. J. I. P. J. 2014. Enhanced secure strategy for OFDM-PON system by using hyperchaotic system and fractional Fourier transformation. 6**,** 1-9.

FARHAN, A. K. & ALI, M. Database protection system depend on modified hash function. Conference of Cihan University-Erbil on Communication Engineering and Computer Science, 2017. 84.

HU, X., YANG, X., SHEN, Z., HE, H., HU, W. & BAI, C. J. I. P. T. L. 2015. Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON. 27**,** 2429-2432.

HUSSAIN, F., FERDOUSE, L., ANPALAGAN, A., KARIM, L., WOUNGANG, I. J. C. S. S. & ENGINEERING. 2016. Security threats in M2M networks: a survey with case study. 270.

LUO, Y., ZHANG, C., LIANG, X., PENG, J., LIU, B. & QIU, K. J. O. E. 2022. Secure OFDM-PON using three-dimensional selective probabilistic shaping and chaos. 30**,** 25339-25355.

NG, T. T., CHANG, S. F., LIN, C. Y. & SUN, Q. 2006. Passiveblind image forensics. Chapter 15, Multimedia Security Technologies for Digital Rights Management, edited by Zeng, W., Yu, H., and Lin, C.-Y. Academic Press,(2006).

OLEWI, H. I. & FYATH, R. S. Hybrid Chaotic Scheme for Secure OFDM-PON Transmission. 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020. IEEE, 232-237.

RAHMAN, S. U., SULTAN, A., ALROOBAEA, R., TALHA, M., HUSSAIN, S. B., RAZA, M. A. J. W. C. & COMPUTING, M. 2021. Secure OFDM-Based NOMA for Machine-to-Machine Communication. 2021.

REN, J., LIU, B., ZHAO, D., HAN, S., CHEN, S., MAO, Y., WU, Y., SONG, X., ZHAO, J. & LIU, X. J. O. E. 2020. Chaotic constant composition distribution matching for physical layer security in a PS-OFDM-PON. 28**,** 39266-39276.

SULTAN, A., YANG, X., HAJOMER, A. A., HUSSAIN, S. B. & HU, W. J. O. F. T. 2019. Chaotic distribution of QAM symbols for secure OFDM signal transmission. 47**,** 61-65.

WANG, Z., XIAO, Y., WANG, S., YAN, Y., WANG, B., CHEN, Y., ZHOU, Z., HE, J. & YANG, L. J. O. E. 2021. Probabilistic shaping based constellation encryption for physical layer security in OFDM RoF system. 29**,** 17890-17901.

WEI, H., CUI, M., ZHANG, C., WU, T., WEN, H., ZHANG, Z., CHEN, Y. & QIU, K. J. O. C. 2021. Chaotic key generation and application in OFDM-PON using QAM constellation points. 490**,** 126911.

WU, Y., YU, Y., HU, Y., SUN, Y., WANG, T. & ZHANG, Q. J. I. P. J. 2021. Channel-based dynamic key generation for physical layer security in OFDM-PON systems. 13**,** 1-9.

YANG, X., SHEN, Z., HU, X. & HU, W. J. I. P. T. L. 2016. Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission. 28**,** 2499-2502.

YANG, X., SULTAN, A., HAJOMER, A., ZHANG, L. & HU, W. Physical-layer OFDM data encryption using chaotic QAM mapping. 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019. IEEE, 1-3.

YASSER, I., MOHAMED, M. A., SAMRA, A. S. & KHALIFA, F. J. E. 2020. A chaotic-based encryption/decryption framework for secure multimedia communications. 22**,** 1253.

YU, F., LI, L., TANG, Q., CAI, S., SONG, Y., XU, Q. J. D. D. I. N. & SOCIETY. 2019. A survey on true random number generators based on chaos. 2019.

ZHANG, W., ZHANG, C., CHEN, C. & QIU, K. J. J. O. L. T. 2017a. Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement. 35**,** 1524-1530.

ZHANG, W., ZHANG, C., CHEN, C., ZHANG, H. & QIU, K. J. I. P. T. L. 2017b. Brownian motion encryption for physical-layer security improvement in CO-OFDM-PON. 29**,** 1023-1026.

ZHAO, J., LIU, B., MAO, Y., ULLAH, R., REN, J., CHEN, S., JIANG, L., HAN, S., ZHANG, J. & SHEN, J. J. O. E. 2020. High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization. 28**,** 21236-21246.

ZONG, J., HAJOMER, A. A., ZHANG, L., HU, W. & YANG, X. J. O. C. 2020. Real-time secure optical OFDM transmission with chaotic data encryption. 473**,** 126005.