IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 June 2023, accepted 21 June 2023, date of publication 26 June 2023, date of current version 30 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3289204

RESEARCH ARTICLE

Physical-Layer Security Improvement in MIMO OFDM Systems Using Multilevel Chaotic Encryption

MOHAMMAD MAHMUDUL HASAN[1], MICHAEL CHEFFENA[1], AND SLOBODAN PETROVIC[2]
[1]Faculty of Engineering, Norwegian University of Science and Technology (NTNU), 2815 Gjøvik, Norway
[2]Faculty of Information Technology and Electrical Engineering, NTNU, 2815 Gjøvik, Norway

Corresponding author: Mohammad Mahmudul Hasan (mohammad.m.hasan@ntnu.no)

This work was supported by the Research Council of Norway under Project 324061.

ABSTRACT Ensuring physical-layer security (PLS) in wireless communication has always been a challenge due to the broadcasting nature of the transmission. In this work, a multilevel chaotic encryption (MCE) system is proposed to improve PLS in Multiple-Input Multiple-Output (MIMO) Orthogonal Frequency Division Multiplexing (OFDM) systems under Rayleigh fading channel. Additionally, the proposed technique improves the transmission performance by reducing the high Peak-to-Average-Power Ratio (PAPR) which is also considered as one of the major drawbacks of Multicarrier Modulations (MCM) like OFDM. In the proposed scheme, multilevel encryption is achieved in two steps. In the first step, a precoding matrix based on a unique chaotic sequence scrambles the modulated symbols. In the second step, phase scrambling is used based on chaotic sequence for selective mapping to provide a second level of encryption for the entire transmission. We evaluated the security performances using randomness of the proposed MCE, achievable key-space, and security analysis under cryptographic attacks from the perspective of Cryptanalysis. We verified the communication performances in terms of computational complexity of the system, PAPR, and error performances considering multipath Rayleigh fading wireless channel. The proposed MCE provides a huge key-space of $\sim 10^{302}$ which can resist any cryptographic attacks. Also, the pseudo-random nature of the multilevel chaotic scrambling reduces the PAPR by reducing autocorrelation of the OFDM signal. The proposed low-complexity MCE solution outperforms existing encryption schemes when compared in terms of security, computational complexity, and PAPR. Mathematical analysis and simulation results show that the proposed MCE scheme can enhance physical layer security along with significant reduction in PAPR without compromising the error performances of the system.

INDEX TERMS Physical-layer security, chaotic function, MIMO, OFDM, SLM, PAPR.

I. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier (MC) transmission technique that has played a vital role in wireless communication over the past two decades as it supports high speed data rate, provides high spectral efficiency, protection against inter-symbol interference (ISI) and multipath frequency selective channels. Rapid growth of mobile users and demand for high-speed stable data rate has always been on the rise. To achieve additional data rates and improve throughput, multiple-input-multiple-output (MIMO) has become one of the most promising techniques in wireless communications. Wireless communication is already more vulnerable to security attacks than wired cables due to mobility, multipath propagation, openness, and broadcasting nature of the transmission. This becomes more critical with multiple transmission and reception of MIMO systems when eavesdroppers can be equipped with multiple receiving antennas. In general, security is addressed at higher layers with complex encrypting algorithms. Recently, Physical-Layer Security (PLS) has received huge attention as it can effectively prevent illegitimate users from over-

The associate editor coordinating the review of this manuscript and approving it for publication was Adao Silva.

hearing confidential transmission. Additionally, encryption at the physical layer can keep both the data and the header information safe. Therefore, a reliable scheme for physical layer security in wireless communication is of great importance. The PLS ensures secure communication between only the legitimate parties while eavesdroppers receive noise-like signals. Many researchers used chaotic functions to address this issue. Yang et al. proposed an encryption algorithm for PLS using multiple-fold chaotic transformation and phase rotation and achieved a total key-space of $\sim 10^{194}$ to prevent brute force attacks [1]. Additional parameters in the chaotic functions can further extend the key-space [2]. A hybrid solution is proposed in [3] where downstream and upstream data are separately encrypted to improve the PLS significantly. A computationally efficient orthogonal chaotic encryption technique is proposed in [4] using vector reference groups for OFDM. Wei et al. used 1D chaotic functions for data encryption and successfully transmitted 22.06 Gigabits per second (Gbps) over passive optical network in [5]. In [6], a logistic mapping is used for key generation and polar codes for security enhancement. In this work, multilevel chaotic function is used to produce pseudo-random sequence to encrypt the transmission at the physical layer. Chaos based low-complex precoding techniques are proposed in [7] to enhance PLS by row/column permutation and combination and achieved 8.9 Gbps encrypted data rate. Two novel security improvement techniques are proposed in [8] using chaotic signal scrambling along with partial transmit sequence and selective mapping (SLM). A multi-fold digital chaos-based symbol modulation and synchronization is proposed in [8]. Authors showed their technique can enhance data security greatly, however with large complexity. Chaotic encryption techniques can also scramble the modulated symbols [9] and can achieve a huge key-space in the order of $\sim 10^{162}$ [10] and $\sim 10^{231}$ [11]. Additional level of encryption extends key-space and provides further security, however with added complexity [12]. Chen et al. proposed a fast encryption method for secure image transmission in [13] using row and column encryption matrix separately. Wang and Lv presented a novel PLS technique based on two-level encryption for visible light communication without degrading error performance of the system [14]. A 7D hyper-chaos is proposed for multilayer encryption with two-layer transformation to achieve large key-space with PAPR reduction [15]. A low-complex chaotic multitone communication technique is presented in [16] that improves spectrum efficiency with a key-space of $\sim 3.096 \times 10^{106}$. Another low-complex multilayer dynamic encryption scheme is proposed in [17] with cryptanalysis for OFDM-PON and achieves 10^{91} key-space. Several other researchers considered stream cipher for encryption as they can provide good speed of transmission with less memory consumption [18].

Most of the multicarrier modulation (MCM) techniques suffer from high Peak-to-Average-Power-Ratio (PAPR) due to the superimposed subcarriers of coincident phases. This introduces non-linear distortion when signal passes through a Solid-State Power Amplifier (SSPA). One solution to this problem is to operate the amplifier in a linear region which ultimately reduces power efficiency. Several solutions are reviewed in [19] to address this issue such as clipping the occasional high amplitudes or filtering the input signal to reduce autocorrelation among subcarriers. However, both techniques degrade bit-error-rate (BER) performance of the system. Precoding is another powerful signal transformation technique to whiten the input signal and reduce the autocorrelation. Non-linear companding techniques have been widely used where higher amplitudes are compressed and lower amplitudes are expanded to normalize the entire dynamic range of amplitudes. Here, trade-offs can be made between BER and PAPR performances. Constellation shaping, partial transmit sequence, and SLM use phase scrambling to reduce the chances of sudden high peaks occurrences.

TABLE 1. Simulation parameters.

Parameter	Specification
OFDM symbols	10^7 randomly generated data
Channel model	10-path Rayleigh fading
Channel estimation	MMSE
OFDM standard	IEEE 802.11a
Number of FFT points	64
Number of subcarriers (SC)	52 (48 data SC, 4 pilot SC)
Symbol length (T_s)	3.2 µs
Guard interval	¼ of symbol length
Oversampling Factor	$L = 4$
Pilot symbol modulation	BPSK
Subcarrier modulation	16QAM, 64 QAM
MIMO at Bob and/or Alice	2×2, 4×4, 8×8, 16×16
MIMO at Eve	16×16, 256×256

While most of the research works studied the performances of chaotic based encryption for optical networks, this work jointly improves the physical-layer security as well as provides PAPR reduction in MIMO OFDM systems under Rayleigh fading wireless channel. The contribution of this work is twofold:

a) Firstly, we construct a unitary precoding matrix based on a unique chaotic sequence for linear transformation of the modulated symbols and provide first level of encryption to the physical layer.
b) Secondly, we consider an additional layer of chaotic transformation during phase scrambling in SLM which also ensures a significant reduction in PAPR.

The proposed Multilevel Chaotic Encryption (MCE) scheme provides a huge key-space of $\sim 10^{302}$ and protects the transmission against several cryptographic attacks.

II. SYSTEM MODEL AND DESIGN OF TECHNIQUES

The proposed system model to improve PLS using MCE over a conventional wireless channel is illustrated in Fig. 1 where 'Alice', a legitimate user, wants to establish a secure communication with another legitimate user 'Bob', while an illegitimate user 'Eve' tries to eavesdrop on this communication. A secret key that is used as an initial key to

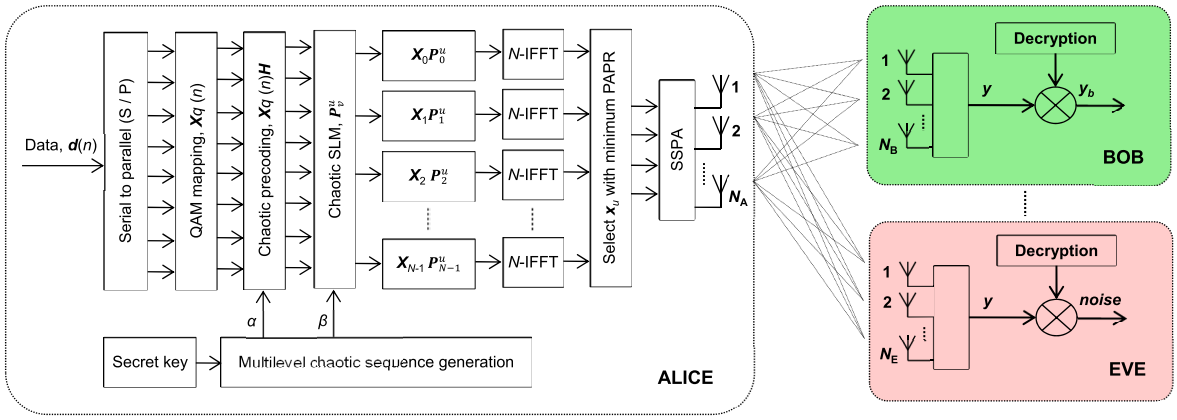

FIGURE 1. Block diagram of the proposed MIMO-OFDM system using MCE.

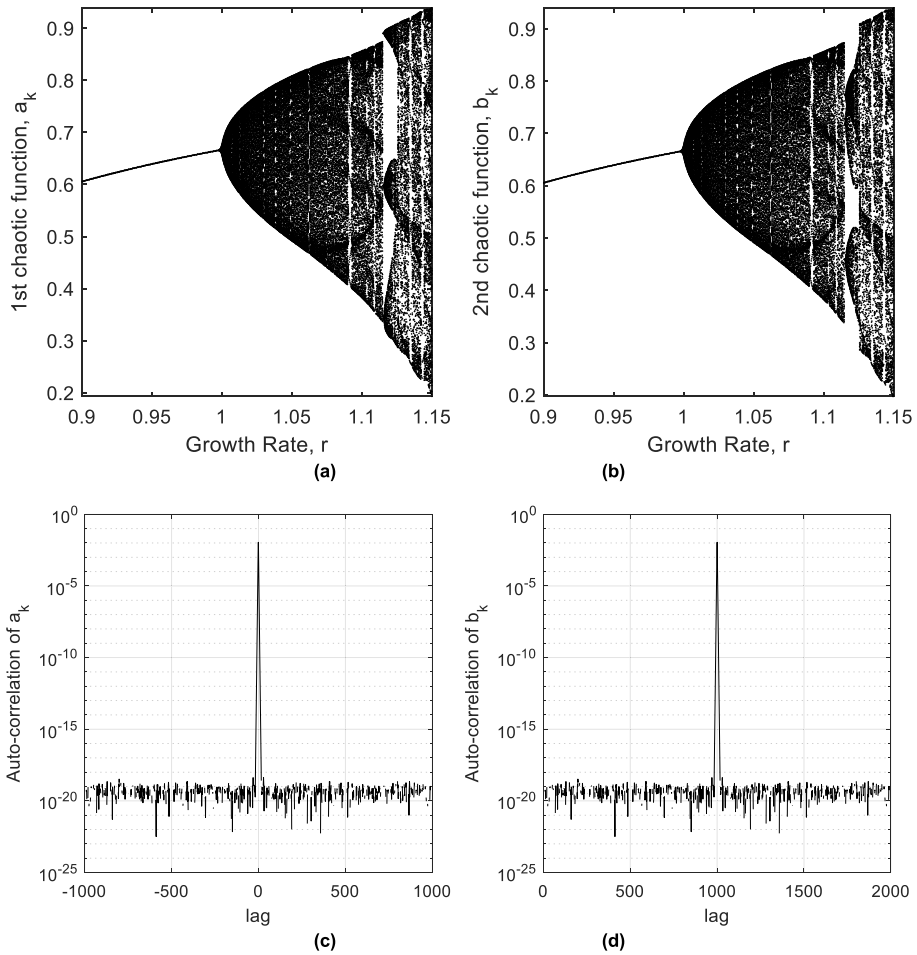

FIGURE 2. Bifurcation diagrams (a-b) of logistic chaotic functions and their auto-correlation functions (c-d).

generate chaotic sequences ($\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$) will be known only to the legitimate users (i.e., Alice and Bob) and used for multilevel data encryption at the transmitter and decryption at the receiver. As the illegitimate users (Eve and others) do not have any information about the secret key, they will not be able to decrypt the data on their devices. Moreover, the PAPR is greatly reduced as an outcome of multilevel chaotic scrambling of the signal. A pseudo-random binary data sequence is converted into parallel streams before Quadrature Amplitude Modulation (QAM) modulation.

A. MULTILEVEL CHAOTIC FUNCTIONS

Chaotic systems are widely used in military communication (using spread spectrum) and applications that demand high

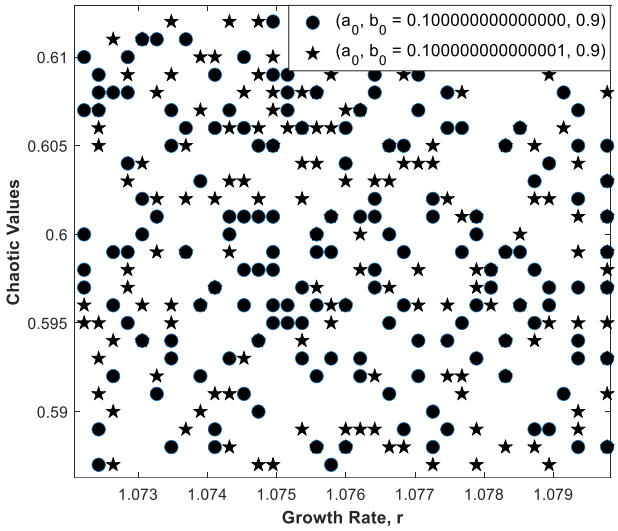

FIGURE 3. Sensitivity to initial value difference of 10^{-15}.

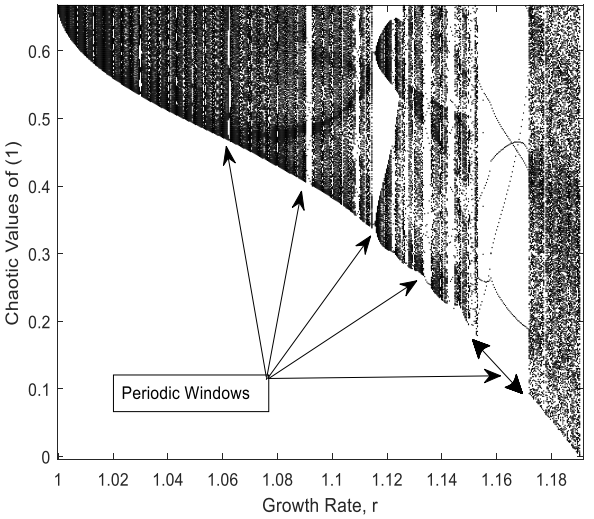

FIGURE 4. Example of periodic windows.

level of secrecy as they generate pseudo-random sequences and are extremely sensitive to its initial values. In this work, a two-level logistic discrete mapping (a_k, b_k) (with initial keys a_0, b_0 and growth rate 'r' that are known only to the legitimate parties) is used for the following chaotic functions as

$$a_{k+1} = r\,(3b_k + 1)\,a_k\,(1 - a_k)\,, \tag{1}$$
$$b_{k+1} = r\,(3a_{k+1} + 1)\,b_k\,(1 - b_k)\,, \tag{2}$$

where $k = 0, 1, 2 \cdots$ and $r \in (0.9, 1.15]$. Using (1) and (2), a unique chaotic sequence $(\boldsymbol{\beta})$ is then produced, which is then used for phase scrambling (see section II-C) and precoding (see section II-D) as,

$$\boldsymbol{\beta} = \boldsymbol{C}_1 \oplus \boldsymbol{C}_2, \tag{3}$$

where $\boldsymbol{C}_1 = |\lceil \mathrm{mod}\ (a_k,\ 2)\rceil|$, $\boldsymbol{C}_2 = |\lceil \mathrm{mod}(b_k,\ 2)\rceil|$, $|\square|$ is the absolute value, and $\lceil\square\rceil$ is the ceil function. Fig. 2 (a-b) shows the scatter plots of logistic chaotic functions given in (1) and (2), also known as the bifurcation diagram. The Autocorrelation Function (ACF) (in the order of $\sim 10^{-20}$) in Fig. 2 (c)- (d) ensures a very good pseudo-randomness of the chaotic sequences.

Chaotic behavior is extremely sensitive to the initial parameters given to the system. A small change in the initial values will take it to a whole new chaotic state with a completely different sequence. Illegal users cannot retrieve any information without the information about the key. Fig. 3. shows the sensitivity of the system even with a small difference of 10^{-15} in any of the parameters of the initial values.

The x-axis shows different values of r between 0.9 and 1.15 and the y-axis shows the trajectory map for each value of r. Fig. 2 (a)-(b) show that the values of the functions oscillate between the fixed points. The fixed points show the values of the growth rate, for which values of successive populations are the same. To find the fixed points of the functions, we set $a_{k+1} = a_k = a$ and $b_{k+1} = b_k = b$ in (1) and (2), respectively. We set $f\,(a) = a = r\,(3b + 1)\,a\,(1 - a)$ and $f\,(b) = b = r\,(3a + 1)\,b\,(1 - b)$. So, the fixed points are $a^{(1)} = 0$, $a^{(2)} = 1 - 1/\,[r(3b + 1)]$ for (1) and $b^{(1)} = 0$, $b^{(2)} = 1 - [1/r\,(3a + 1)]$ for (2).

To further understand the chaotic behavior of the functions, we illustrated the graph over 500,000 growth points using initial values (a_0, b_0) at (0.1, 0.9). The observed behavior can be summarized as follows:

- When $r \in (0, 0.8)$, the system is stable to a fixed static point at 0 that is independent of the initial conditions. This is commonly known as the extinction of population in chaotic systems.
- When $r \in (0.8, 1)$, the system shows asymptotic growth to approach the second fixed points of the functions.
- When $r \in (1, 1.2]$, the system oscillates and shows a periodic attractor. During this interval, the system splits into several bifurcations for several values of r. However, the initial values should be selected properly to avoid the presence of 'Periodic Windows' (as shown in Fig. 4, and the problem has been reported in several articles [20]). Thus, the selection of initial values and key controlling parameters becomes very critical to achieve a good pseudo-randomness in the phase sequence.
- When $r > 1.2$, system damps itself and stops any further growth.

Since the system produces chaotic pseudo-randomness but becomes predictable when the driving key parameters r, a_0, and b_0 are known, it can be used to generate pseudo-random numbers to provide security.

B. OFDM SIGNAL AND PAPR

The discrete-time complex OFDM symbol can be given as [19].

$$\boldsymbol{x}_n = IFFT_N\left[\boldsymbol{X}_\beta\,(u)\right]_{M\times 1} = \frac{1}{\sqrt{N}}\sum_{k=0}^{1}\boldsymbol{X}_k\boldsymbol{W}_N^{nk} \tag{4}$$

where each symbol of $\boldsymbol{X}_k$ modulates a corresponding sub-carrier from a set of orthogonal subcarriers and is carried by the kth sub-carrier, IFFT_N is the N-point Inverse Fast Fourier Transform (IFFT), and $\mathbf{W}_\text{N} = \text{e}^{-\text{j}2\pi/\text{N}}$. Signals with higher side-lobes are highly correlated and will have high PAPR when given to the IFFT because the subcarriers will be aligned in-phase. Considering the OFDM signal in (4), the definition of PAPR can be given as [20],

$$PAPR\,(dB) = 10\log_{10} max\left\{|\boldsymbol{x}_n|^2\right\}/E\left\{|\boldsymbol{x}_n|^2\right\} \quad (5)$$

where $E\{\quad\}$ is the expectation operator.

C. SYMBOL SCRAMBLING WITH CHAOTIC PRECODER

First, a Skew-Hermitian matrix ($\boldsymbol{S}$) is created using the chaotic sequence $\boldsymbol{\beta}$ from (3) as $\boldsymbol{S} = (\boldsymbol{\beta} + \boldsymbol{\beta}^\dagger)/2$, where the dagger ($\square^\dagger$) denotes the Hermitian conjugate. Then, a unitary precoding matrix ($\boldsymbol{P}$) is constructed using Cayley Transform as,

$$\boldsymbol{P} = (\boldsymbol{I} + \boldsymbol{S})^{-1}(\boldsymbol{I} - \boldsymbol{S}) \quad (6)$$

The chaotic based precoding matrix ($\boldsymbol{P}$) in (6) is an orthogonal unitary matrix with elements from [21]. $\boldsymbol{P}$ is invertible and follows the condition $\boldsymbol{P}\boldsymbol{P}^\dagger = \boldsymbol{I}$. In this work, the first level of encryption is achieved using $\boldsymbol{P}$ to scramble the modulated symbols $\boldsymbol{X}_q$ as,

$$\boldsymbol{X}_p = \boldsymbol{P}\boldsymbol{X}_q \quad (7)$$

where each row of X_p represents the linear transformation of each of the QAM symbols.

D. PHASE SCRAMBLING WITH CHAOTIC SEQUENCE

The concept of SLM is widely used in PAPR reduction for many years [16] where each of the symbols in (7) is multiplied with M different phase sequences given by

$$\boldsymbol{P}_v^u = e^{j\beta\phi_v^u} \quad (8)$$

where $\phi_v^u \in (0, 2\pi]$ for $v = 0,1,\ldots,N\text{-}1$ and $u = 1, 2, \ldots, M$. Thus, the scrambled sequences are given as

$$\boldsymbol{X}_\beta(u) = \boldsymbol{X}_p \odot \boldsymbol{P}_v^u = [\boldsymbol{X}_0\boldsymbol{P}_0^u, \boldsymbol{X}_1\boldsymbol{P}_1^u, \ldots, \boldsymbol{X}_{N-1}\boldsymbol{P}_{N-1}^u] \quad (9)$$

where $\odot$ represents the symbol-to-symbol multiplication. Among these M sequences, the sequence with lowest PAPR is selected for the transmission. The receiver needs the information of the index of the selected sequence for phase decryption. This information is additionally sent to the receiver.

III. RESULTS AND ANALYSIS

In this section, we evaluate the communication and security performances of the proposed MCE scheme. The idea of this work is to use the pseudo-random nature of a chaotic system for signal transformation and phase scrambling to encrypt the entire transmission including the overhead information from the higher layers and the side information in SLM technique. We assume that the eavesdroppers have complete knowledge of the transmission parameters such as channel characteristics, protocols, frame structures, pilot positions, etc. The sensitive initial keys (r, a_0, b_0) are pre-shared with the legitimate users which they can use to generate the unique chaotic sequence, phase sequence, and precoding matrix as in (3), (7), and (8), respectively.

TABLE 2. Comparison of performances using chaotic schemes.

Schemes	Key space	Complexity	PAPR
Chaotic multilevel encryption [5]	10^{72}	22 N	15 dB
Noise-like constellation [10]	10^{162}	46 N	14 dB
Multilayer dynamic encryption [16]	10^{91}	19 N	14 dB
7D chaotic encryption [15]	10^{253}	343 N	13.2 dB
The proposed MCE scheme	10^{302}	17 N	5.8 dB

A. KEY-SPACE

The robustness of chaotic based encryption techniques can be evaluated in terms of the key-space they provide for encryption. Using the precoding matrix $\boldsymbol{P}$ in (6), the linear transformation in (7) creates a key-space of $N! \times N!$ where N is the order of the matrix. During phase scrambling in (9), each of the OFDM symbols is scrambled through a phase matrix of $M \times N$ where M is the total number of the phase sequences. The transmitter selects the one with the lowest PAPR for transmission. This selection is random for each OFDM symbol and independent from previous choices. As a result, the total key-space can be estimated as $N! \times N! \times M! \times N!$ ($\sim 10^{302}$ for $N = 64$, and $M = 32$). So, the proposed MCE provides a huge key-space for encryption that is enough to withstand any cryptographic attacks.

B. CRYPTANALYSIS

An efficient encryption scheme should resist various cryptographic attacks such as brute force, statistical, differential, and plaintext attacks. In this section, we evaluate the resiliency of the proposed algorithm against such attacks and its ability to resist such illegal attackers.

Brute-force attacks are frequently used for cryptanalysis where illegal users know the encryption and decryption algorithms but do not have access to the key. In this attack, eavesdroppers exhaustively try out all possible combinations of the keys to decrypt the ciphertext. To prevent this, encryption algorithms are generally designed in such a way so that this search becomes computationally infeasible to carry out. The strength of the encryption algorithm depends on the size of the key-space (see section III-A). In a brute-force attack, the expected number of attempts before the correct key is obtained is half the size of the key-space which is $\sim 0.5 \times 10^{302}$ (for $N = 64$, and $M = 32$) for the proposed algorithm. This is enough to resist any brute-force attack. With the increase of N and M, this number increases exponentially.

Eavesdroppers may also exploit statistical changes in the signal to launch statistical attacks. To prevent this, ciphertext is expected to exhibit a high level of randomness. It is clear

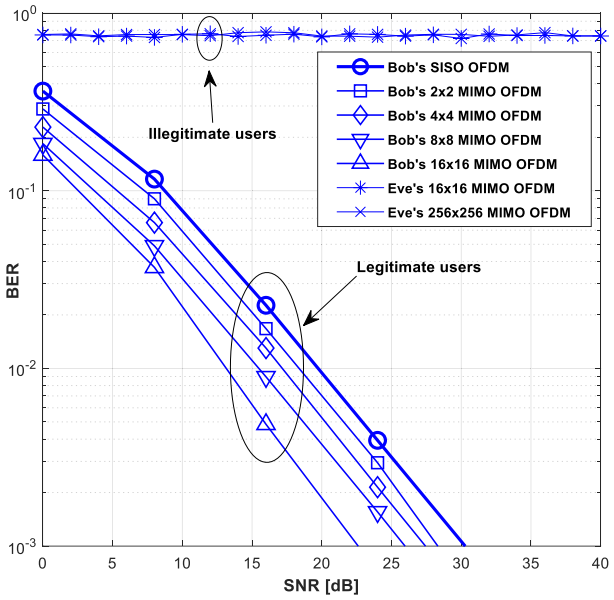

FIGURE 5. BER Performances at legitimate users (i.e., Alice and Bob) and illegitimate users (i.e., Eve) under Rayleigh fading wireless channel using 16QAM.

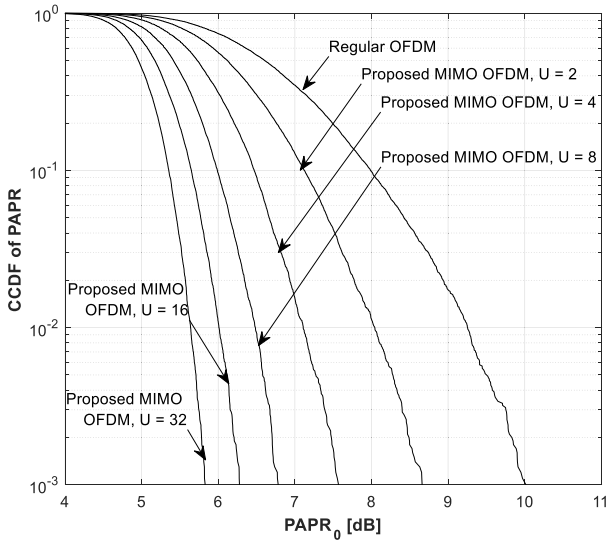

FIGURE 6. PAPR reduction using MCE for 64QAM.

from Fig. 2 (c)- (d) that the ACF coefficients of adjacent samples are close to zero (in the order of $\sim 10^{-20}$). This means that the proposed algorithm effectively eliminates any association among adjacent samples. This removes any statistical information present in the signal which can resist statistical attacks and eavesdroppers cannot retrieve any useful information.

In differential attack, illegal users may use successive plaintexts that are closely related to reveal statistical information with the intention of deriving the key. As shown in Fig. 3, the sensitivity of the proposed scheme is extremely high. A tiny difference of 10^{-15} in any of the parameters of initial values produces completely different noncoincidental trajectories, thereby producing highly uncorrelated successive symbols. Therefore, it is difficult for the differential attackers to find any relation from successive ciphertext symbols.

Encryption algorithms are also designed to be secured against ciphertext attacks that are often used in cryptanalysis. Illegal users may launch ciphertext attacks when they know (or can guess) few of the modulated symbols. Attackers then recover the encryption key and use it to decrypt the next ciphertext. For the proposed method, however, there is no direct way to recover the key (or initial parameters) from modulated symbols. This is because the first level of encryption in this work scrambles the modulated symbols with chaotic precoder using (6). Then, the symbol-to-symbol multiplication using (9) provides phase scrambling which makes it impossible to decrypt the next plaintext through a (or few) known set of plaintext/ciphertext pair(s). This can resist known/chosen plaintext attacks. Further, the phase sequence in (8) is different for each OFDM frame, which changes every 3.2 μs for each symbol (T_s in IEEE.11a applications. See Table 1).

C. COMPUTATIONAL COMPLEXITY

Next, we compute the computational complexity of the proposed MCE scheme. The generation of the chaotic sequences using (1)-(3) requires 17 *N*operations which is very less compared to most of the existing multilevel chaotic systems (see Table 2). The total complexity for the encryption comes from the operations during symbol scrambling and phase scrambling using (7) and (9), respectively. The linear transformation of the modulated symbols using unitary precoding matrix in (7) requires N^2 multiplication and $N(N\text{-}1)$ addition, where N represents the length of the input data. Then, each sub-block in SLM has an IFFT operation that requires approximately $(N/2)\log_2 N$ complex multiplication and $N\log_2 N$ complex addition. However, it should be noted that the complexity due to the SLM is added (only to the transmitter side) to improve the PAPR performance and not a part of the encryption algorithm. The generation of the phase sequences, however, for the phase scrambling requires $u \times N$ complex multiplication and $u \times (N-1)$ complex additions. The complexities in SLM operation using $u$number of phase sequences are $u \times (N/2)\log_2 N$ complex multiplications and $u \times N\log_2 N$ complex additions. The PAPR performance can be further improved using a larger value of u, which also increases computational complexity. So, a trade-off can be made among PAPR performances, computation time, and security.

D. BER AND PAPR PERFORMANCES

Error performance of the proposed model was evaluated in terms of BER, and the PAPR reduction performance was evaluated using the Complementary Cumulative Distribution Function (CCDF). CCDF calculates the probability that the

PAPR of OFDM signal may exceed a reference threshold level $PAPR_0$, given as [19],

$$CCDF\left[PAPR\left(\boldsymbol{x}_n\right)\right] = prob\left[PAPR\left(\boldsymbol{x}_n\right) > PAPR_0\right],$$

where *prob* [.] is the probability operator. Fig. 5 shows the BER performances of a regular OFDM, and the proposed MCE MIMO OFDM systems considering additive white gaussian noise and Rayleigh fading channels with 10 taps. Other simulation parameters are mentioned in Table 1. It is clear from the figure that the legitimate users (i.e., Alice, Bob) receive the exact signal while illegitimate users (i.e., Eve and others who do not have the initial keys) receive a noise-like signal. The illegitimate users could not access the secured communication despite using a higher number of receiving antennas than the transmitter. Further, we have assumed that the illegitimate users have managed to retrieve the side information (regarding the number of phase sequence, u) to claim the complete level of security compared to existing SLM based OFDM systems. The simulation results also confirm that the proposed MCE works for higher order of MIMO configuration and does not degrade the BER performance of the conventional OFDM system. Additionally, the signal transformation and phase scrambling proposed in this work reduce the autocorrelation of the signal. This can yield a significant PAPR gain over a regular OFDM system. The proposed MCE scheme can achieve a 1.4 dB to 4.7 dB PAPR gain over a regular OFDM system as shown in Fig. 6.

Table 2 compares the performances of the proposed MCE scheme with existing multilevel encryption schemes. When compared to the existing security schemes, the proposed MCE scheme requires low computation yet provides a huge key-space to resist several attacks with a very high PAPR gain to improve overall communication and security performances of the system.

IV. CONCLUSION

In this paper, we propose the use of chaotic functions for improving the PLS in MIMO OFDM systems considering Rayleigh fading wireless channel. The proposed MCE technique also scrambles the phases of the subcarriers on multiple levels and reduces the autocorrelation of the signal which effectively reduces the high PAPR in MCM which has been a major inherent drawback of OFDM transmission. A unique pseudo-random chaotic sequence generation technique is proposed to construct a precoding matrix that linearly transforms and scrambles the modulated symbols. Then, the security is further enhanced by phase scrambling which also reduces the PAPR up to 4.7 dB without degrading the BER performances of the conventional MIMO OFDM systems under Rayleigh fading wireless channel. The proposed scheme ensures secured transmission even when eavesdroppers are equipped with multiple receiving antennas. The proposed MCE technique provides a huge key-space of $\sim 10^{302}$ for encryption to withstand any cryptographic attacks. We believe that the proposed MCE technique can have a broad application prospect in improving the security of wireless communication.

REFERENCES

[1] X. Yang, Z. Shen, X. Hu, and W. Hu, "Chaotic encryption algorithm against chosen-plaintext attacks in optical OFDM transmission," *IEEE Photon. Technol. Lett.*, vol. 28, no. 22, pp. 2499–2502, Nov. 15, 2016.
[2] Z. Hu and C.-K. Chan, "A real-valued chaotic orthogonal matrix transform-based encryption for OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 30, no. 16, pp. 1455–1458, Jul. 5, 2018.
[3] M. Cheng, L. Deng, X. Gao, H. Li, M. Tang, S. Fu, P. Shum, and D. Liu, "Security-enhanced OFDM-PON using hybrid chaotic system," *IEEE Photon. Technol. Lett.*, vol. 27, no. 3, pp. 326–329, Nov. 13, 2015.
[4] F. S. Hasan and A. A. Valenzuela, "Design and analysis of an OFDM-based orthogonal chaotic vector shift keying communication system," *IEEE Access*, vol. 6, pp. 46322–46333, 2018.
[5] H. Wei, C. Zhang, T. Wu, H. Huang, and K. Qiu, "Chaotic multilevel separated encryption for security enhancement of OFDM-PON," *IEEE Access*, vol. 7, pp. 124452–124460, 2019.
[6] X. Lu, Y. Shi, W. Li, J. Lei, and Z. Pan, "A joint physical layer encryption and PAPR reduction scheme based on polar codes and chaotic sequences in OFDM system," *IEEE Access*, vol. 7, pp. 73036–73045, 2019.
[7] A. A. E. Hajomer, X. Yang, and W. Hu, "Secure OFDM transmission precoded by chaotic discrete Hartley transform," *IEEE Photon. J.*, vol. 10, no. 2, pp. 1–9, Apr. 2018.
[8] X. Yang, X. Hu, Z. Shen, H. He, W. Hu, and C. Bai, "Physical layer signal encryption using digital chaos in OFDM-PON," in *Proc. 10th Int. Conf. Inf., Commun. Signal Process. (ICICS)*, Dec. 2015, pp. 1–6.
[9] W. Dai, H. Yang, Y. Song, and G. Jiang, "Two-layer carrier index modulation scheme based on differential chaos shift keying," *IEEE Access*, vol. 6, pp. 56433–56444, 2018.
[10] A. Sultan, X. Yang, A. A. E. Hajomer, and W. Hu, "Chaotic constellation mapping for physical-layer data encryption in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 30, no. 4, pp. 339–342, Feb. 15, 2018.
[11] X. Huang, L. Zhang, W. Hu, J. P. Turkiewicz, E. Leitgeb, and X. Yang, "Secure OFDM-PON using chaotic constellation mapping and probabilistic shaping," *IEEE Photon. Technol. Lett.*, vol. 33, no. 20, pp. 1139–1142, Aug. 30, 2021.
[12] A. Sultan, X. Yang, A. A. E. Hajomer, S. B. Hussain, and W. Hu, "Dynamic QAM mapping for physical-layer security using digital chaos," *IEEE Access*, vol. 6, pp. 47199–47205, 2018.
[13] H. Chen, E. Bai, X. Jiang, and Y. Wu, "A fast image encryption algorithm based on improved 6-D hyper-chaotic system," *IEEE Access*, vol. 10, pp. 116031–116044, 2022.
[14] Z. Wang and J. Lv, "Secure image transmission in orthogonal frequency division multiplexing visible light communication systems," *IEEE Access*, vol. 7, pp. 107927–107936, 2019.
[15] Z. Hu and C.-K. Chan, "A 7-D hyperchaotic system-based encryption scheme for secure fast-OFDM-PON," *J. Lightw. Technol.*, vol. 36, no. 16, pp. 3373–3381, May 28, 2018, doi: 10.1109/JLT.2018.2841042.
[16] S. Guo and Y. Fu, "A time-varying chaotic multitone communication method based on OFDM for low detection probability of eavesdroppers," *IEEE Access*, vol. 9, pp. 107566–107573, 2021.
[17] M. Cui, C. Zhang, Y. Chen, Z. Zhang, T. Wu, and H. Wen, "Multilayer dynamic encryption for security OFDM-PON using DNA-reconstructed chaotic sequences under cryptanalysis," *IEEE Access*, vol. 9, pp. 18052–18060, 2021.
[18] Y. M. Al-Moliki, M. T. Alresheedi, Y. Al-Harthi, and A. H. Alqahtani, "Robust lightweight-channel-independent OFDM-based encryption method for VLC-IoT networks," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4661–4676, Mar. 2022, doi: 10.1109/JIOT.2021.3107395.
[19] T. Jiang and Y. Wu, "An overview: Peak-to-average power ratio reduction techniques for OFDM signals," *IEEE Trans. Broadcast.*, vol. 54, no. 2, pp. 257–268, Jun. 2008.
[20] D. P. Feldman, *Chaos and Fractals: An Elementary Introduction*. New York, NY, USA: Oxford Univ. Press, 2012, pp. 110–112.
[21] R. Gerzaguet, N. Bartzoudis, L. G. Baltar, V. Berg, J.-B. Doré, D. Kténas, O. Font-Bach, X. Mestre, M. Payaró, M. Färber, and K. Roth, "The 5G candidate waveform race: A comparison of complexity and performance," *EURASIP J. Wireless Commun. Netw.*, vol. 2017, no. 1, p. 13, Jan. 2017.

MOHAMMAD MAHMUDUL HASAN received the B.Tech. and M.Tech. degrees in electronics and telecommunication engineering from KIIT University, India. He is currently pursuing the Ph.D. degree in information and communication technology from NTNU, Norway. He was an Assistant Professor with KIIT University, in 2010. From 2011 to 2022, he was an Assistant Professor with the Department of Electronics and Communication Engineering, UITS, Bangladesh. He has written and edited several journals and conference papers. His research interests include addressing the issues related to wireless communications, signal processing, machine learning and intelligent systems, antenna engineering, antenna sensors, massive MIMO, and millimeter wave communications.

MICHAEL CHEFFENA received the M.Sc. degree in electronics and computer technology from the University of Oslo, Norway, in 2005, and the Ph.D. degree from the Norwegian University of Science and Technology (NTNU), Trondheim, Norway, in 2008. In 2007, he was a Visiting Researcher with the Communications Research Centre, Ottawa, ON, Canada. From 2009 to 2010, he conducted a Postdoctoral study with University Graduate Center, Kjeller, Norway; and with the French Space Agency, Toulouse, France. He is currently a Full Professor with NTNU, Gjøvik, Norway. His research interests include modeling and prediction of propagation radio channels, signal processing, medium access control protocol design, antenna sensors, and sensor systems.

SLOBODAN PETROVIC received the Ph.D. degree from the University of Belgrade, Serbia, in 1994. He was with the Institute of Applied Mathematics and Electronics and with the Institute of Mathematics, Belgrade, from 1986 to 2000. He worked on various information security related projects with the Institute of Applied Physics, Madrid, Spain, from 2000 to 2004. From 2004 to 2015, he was with Gjøvik University College, Norway. Since January 2016, he has been a Professor of information security with the Norwegian University of Science and Technology (NTNU), where he teaches cryptology and intrusion detection and prevention. He is the author of more than 50 scientific articles from the field of information security, digital forensics, and cryptology. His research interests include cryptology, intrusion detection, and digital forensics.