Enhancing Data Transmission Security and Reliability of OFDM-IM for 5G Wireless Communication Systems

Asaad H. Sahar[1], Aqiel N. Almamori[1], and Muhannad Y. Muhsin[2]

[1] *University of Baghdad, Baghdad, Iraq,*
[2] *University of Technology – Iraq, Bahdad, Iraq*

https://doi.org/10.26636/jtit.2026.1.2502

Abstract — Thanks to its improved spectral efficiency and immunity to frequency selective fading, OFDM with index modulation (OFDM-IM) has become a perspective option. Unfortunately, OFDM-IM systems are vulnerable to security risks due to their inherent openness encountered in wireless communications. Conventional encryption techniques, which focus on the upper layers, add complexity and might not be enough to fend off malicious attacks. To improve the selection of subcarrier indexes and modulation of data symbol modulation, this work proposes a new chaotic encryption approach for OFDM-IM systems that uses Lorenz chaotic maps. Comprehensive simulations show that, in comparison to traditional methods, the proposed approach provides better security against eavesdropping while maintaining transmission reliability.

Keywords* — *5G, chaotic encryption, Lorenz chaotic maps, OFDM-IM, subcarrier index selection

1. Introduction

5G and beyond communication systems provide high-capacity, high-security, ultra-reliable, low-latency connectivity, and high spectral efficiency features to support new services and applications. However, the growing demands faced by 5G communication systems might be difficult to handle by traditional orthogonal frequency division multiplexing (OFDM) solutions.

Recently, OFDM with index modulation (OFDM-IM) has gained popularity and is used extensively in several communication technologies, including optical communications, cognitive radio, and multiple input, multiple output (MIMO) networks [1]. As far as OFDM-IM systems are concerned, information is transmitted through constellation carrier and subcarrier indices [1]–[6]. The high spectral efficiency and reliability tradeoff, flexible spectral efficiency, and achievable ergodic rate are all attractive advantages that OFDM-IM displays over conventional OFDM systems [3]. Unfortunately, due to their inherent openness and broadcast nature, wireless communications are susceptible to eavesdropping and malicious attacks.

Eavesdroppers could blindly estimate several transmission parameters with respect to traditional OFDM-IM systems. Therefore, in practical applications, the issue of security of OFDM-IM systems should be considered. Upper layers are the main focus of most encryption techniques. Key management, distribution, and generation are all part of the matching encryption process. As a result, the computational overhead that has been introduced cannot be disregarded, and the encryption procedure at upper layers is also somewhat complicated.

Furthermore, with ever-growing computing power comes the possibility of security threats during the key distribution and key update phases. Consequently, there is a rather high level of complexity created and insufficient security is ensured by the encryption algorithms at the upper layers.

As an addition to upper-layer encryption, physical layer encryption may be rather advantageous [4]. With regard to encryptions of the physical layer, characteristics of wireless channels as well as the encryption technique are frequently used to protect the communication. Encryption keys could be generated by taking advantage of physical characteristics of the wireless channel, including reciprocity, randomness, as well as temporal and spatial variations [4], [7]. Furthermore, chaotic maps offering characteristics such as pseudo randomness, ergodicity, and sensitivity to initial values are frequently used in OFDM-tailed models to enhance security performance [8]–[10]. Chaotic systems are highly suitable for stream ciphering, randomization of signal order randomization, and other processes sue to their unpredictable and distinct characteristics regarding chaotic sequences.

2. Related Works

In the previous research, several encryption approaches of the physical layer have been proposed to improve the security of OFDM systems. Dynamic interleaving was utilized to create an eavesdropping-resistant OFDM system that has been described in [7]. In the time division duplexing (TDD) mode, sub-carrier interleaving depends on CSI (i.e., channel state information) between the authorized users. A constellation rotation approach based on chaos has been used in [8] to prevent eavesdropping on OFDM systems and chaotic maps were used for varying the phases of constellation symbols.

For the purpose of ensuring the security of OFDM systems, chaotic maps have been utilized in [9] for the randomization of the sub-carrier phase and order. For OFDM systems, an artificial noise-based encryption method has been used in [10], [11] and several algorithms for the physical layer encryption that have been designed specifically for OFDM-IM.

In [12], selection of the optimum subcarrier index as well as adaptive interleaving have been utilized for the purpose of improving the security of OFDM-IM systems. To prevent eavesdropping on the OFDM-IM system, a secure index and data symbol modulation have been relied upon in [13]. The rule of randomized mapping for the data symbols and index modulations has been developed based on the CSI. An encryption approach based upon artificial noise was introduced for OFDM-IM systems in [14], where artificial noise is coupled with a legitimate signal that can be eliminated at the side of the authorized receivers.

With regard to OFDM-IM systems, there is still potential for improvement over previous physical layer encryption techniques. The significant degree of modification and fairly high complexity added to the transceiver used in conventional OFDMIM systems are the recurring characteristics of the encryption techniques presented in [12]–[14]. Additionally, data symbol modulation security has not been considered by the encryption schemes, as they concentrate on the selection of the sub-carrier index.

In this work, we propose an efficient and straightforward encryption method for OFDM-IM systems. The method could protect modulation of the data symbol, additionally to ensuring security of the sub-carrier index selection process. The phase of modulated data symbols as well as indexes of the active subcarrier are both randomly generated using chaotic maps. In the TDD mode, legitimate users retrieve secret keys, being the initial chaotic map values, from CSI. Due to the reciprocity of the wireless channel in the TDD mode, legitimate users acquire identical secret keys.

Secure operation of the proposed technique may be ensured, since the spatial variance of the wireless channel prevents an eavesdropper at a third party from obtaining secret keys. Furthermore, there is a large space in the key space to defend against comprehensive attacks. Specifically, compared to the previous techniques presented in [12]–[14], only modest adjustments are required to typical OFDM-IM systems, and added complexity is not that great. Extensive simulations confirm that it could attain the same reliability as traditional OFDM-IM systems

3. Preliminaries

In this section, the basics of standard OFDM-IM systems using frequency-selective Rayleigh fading channel types are described, and then the foundations of Lorenz chaotic maps are covered in more detail.

3.1. OFDM-IM

The OFDM-IM transmitter receives a total of m bits of transmitted data. The condition $m = l \cdot q$ is satisfied by the first division of m bits of information into l subblocks, each of which is q long, as shown in Fig. 1. The OFDM subblock with a length of n was assigned to each of q bits. $N = l \cdot n$ represents the number of OFDM sub-carriers. The information bits of each subblock were split to data symbol bits and index bits due to bit-splitter effects. To calculate active sub-carrier indices, the first bits of q_1 serve as index bits. Based on a series of predefined instructions depending upon the incoming index bits, just k out of n subcarriers are active in OFDM-IM systems.

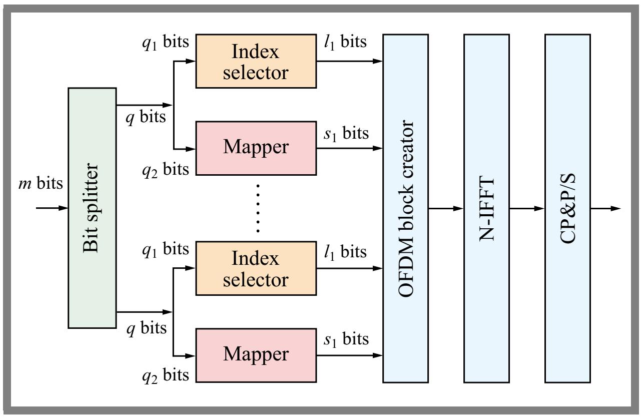

Fig. 1. Block diagram of a conventional OFDM-IM system.

In conventional OFDM-IM systems, a combinatorial or lookup table technique is a commonly used selection method [1]. The combinatorial technique can be viable in the cases where there is a considerable number of information bits, while the lookup table approach is frequently applied to conditions where there are few information bits. For the purpose of creating data symbols, the remaining $q_2 = k \log_2 M$ bits are mapped into an M-ary signal constellation over time. Additionally, data symbols use active indices for modulating subcarriers [1], [15]. Equation (1) is used to determine the sum of the information bits carried through subcarrier index values.

$$m_1 = q_1 l = \lfloor \log_2 C(n,k) \rfloor l \, . \tag{1}$$

The selected active subcarrier indices for subblock γ can be represented as:

$$l_\gamma = \{i_{\gamma,1}, i_{\gamma,2}, \ldots, i_{\gamma,k}\} \, , \tag{2}$$

where $\gamma = 1, \cdot \cdot \cdot, l$.

The total number of bits of information that are carried by constellation symbols is represented as [1]:

$$m_2 = q_2 l = k(\log_2 M) l \, . \tag{3}$$

Modulated symbols that are carried out through the active subcarrier k of subblock γ can be expressed as:

$$s_\gamma = \lfloor s_\gamma(1), \ldots, s_\gamma(k) \rfloor \, , \tag{4}$$

where $\gamma = 1, \cdot \cdot \cdot, l$.

After that, I_γ and s_γ are transmitted to the OFDM block creator, which constitutes the main block of the OFDM.

$$x_F = \left[x(1), x(2), \ldots, x(N)\right]^T \, , \tag{5}$$

The N-IFFT processing converting the frequency domain signal to a time domain signal could be written as follows:

$$x_T = \frac{1}{\sqrt{K}} F_N^H x_F \ , \tag{6}$$

where F_N^H represents the DFT matrix that satisfies $F_N^H F_N = NI_N$.

The time domain signal x_T is transmitted through a frequency-selective Rayleigh fading channel when the cyclic prefix is added and parallel to the serial conversion. In particular, a frequency domain signal satisfies the following equation:

$$y_F(\delta) = x(\delta) h_F(\delta) + n_F(\delta) \ , \tag{7}$$

where, $y_F(\delta)$ represents the received signal in the frequency domain, $n_F(\delta)$ and $h_F(\delta)$ represent the frequency domain of the noise and the frequency domain of the channel coefficient, respectively.

3.2. ML Detector

The ML detector for the OFDM-IM model takes under consideration all of the potential subblock realizations by searching for all of the potential combinations of the subcarrier index and points of signal constellation for the purpose of making joint decisions on constellation symbols and active indices for every one of the sub-blocks through the minimization of the following metric:

$$(\hat{I}_\beta, \hat{s}_\beta) = \arg \min_{I_\beta, s_\beta} \sum_{\gamma=1}^{k} \left| y_F^\beta(i_{\beta,\gamma}) - h_F^\beta(i_{\beta,\gamma}) s_\beta(\gamma) \right|^2 \ , \tag{8}$$

where $y_F^\beta(\xi)$ and $h_F^\beta(\xi)$ for $\xi = 1, \ldots, n$ represent received signals, as the well as corresponding fading coefficients for the subblock β, which can be represented as:

$$\begin{aligned} y_F^\beta(\xi) &= y_F\big(n(\beta-1)+\xi\big) \\ h_F^\beta(\xi) &= h_F\big(n(\beta-1)+\xi\big) \end{aligned} \ . \tag{9}$$

The total number of metric calculations that have been carried out in Eq. (8) is cM^k due to the fact that I_β and x_β have c and M^k various realizations, respectively. This is the reason why ML detector is considered as an impractical approach for larger c and k values as a result of its decoding complexity that is increasing exponentially [16], [17].

3.3. Hybrid Greedy Detector and Diversity Reception

Greedy detector is a detection model that has low complexity with a diversity reception. It requires a two-stage detection process: active subcarrier indices and corresponding M-ary symbols are calculated separately, as one may see in Fig. 2.

In the first stage, the greedy detector measures the combined output signal energy of every one of the sub-carriers $|y_\beta(j)|^2$ and, thereafter, detects active subcarriers with the highest level of energy. Subcarriers that are only under the favorable channel fading have a high probability of being estimated as active. For the purpose of reducing computational complexity, the initial stage does not require any information about the channel. After detecting non-zero M-ary symbols in x, the second step applies maximum likelihood (ML) decisions to every K estimated active subcarrier separately. Stages 1 and 2 of the greedy detector process are described below.

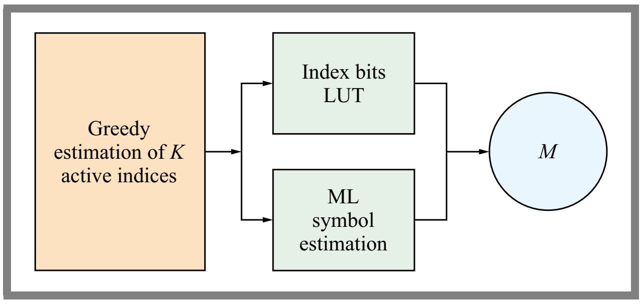

Fig. 2. Block diagram of a greedy detector.

Stage 1. Using K greatest amongst N received subcarrier signal powers, the receiver detects active subcarrier indices based on energy.

1) Assume a residual vector $z = y_\beta$, a demodulated vector r is set to 0 vector, i.e., $r = 0_{1\times N}$, and iteration count $t = 0$ is started.
2) Find the highest element whose index $\hat{\alpha}$ can be expressed as:
$$\hat{\alpha} = \arg \max_j |z(j)|^2 \ , \tag{10}$$
where $z(j)$ represents the j-th element of $\boldsymbol{z}$.
3) Assume $r(\hat{\alpha}) = z(\hat{\alpha})$ and $z(\hat{\alpha}) = 0$, and increment t by 1, where $r(\hat{\alpha})$ represents α-th element in r.
4) Steps 2 and 3 are repeated to the point where $t = K$.
5) Set all non-zero elements in $r = 1$. Recover m_I bits for r with the use of LUT. An example of LUT for cases where $K = 2$ and $N = 4$ is listed in Tab. 1.

Stage 2. M-ary symbols are estimated with the use of the ML criterion on the subcarriers of the active indices $\hat{\alpha}$ as:

$$\hat{x}(\hat{\alpha}) = \arg \max_{x(\hat{\alpha})\in\varsigma} \left| y_\beta(\hat{\alpha}) - h(\hat{\alpha}) \times (\hat{\alpha}) \right|^2 \ , \tag{11}$$

where $h(\hat{\alpha})$ represents the α-th diagonal element with respect to H in Eq. (7), representing the equivalent channel matrix after diversity reception.

Note that GD utilizes the process of energy detection, which eliminates the need for a brute-force search of every potential index combination and greatly reduces complexity of the process of estimating a set of active subcarrier indices. This results in an additional reduction of the complexity of the carrier index while detecting M-ary symbols, which the latter process performed independently of the subcarrier index detection rate [18], [19].

Tab. 1. Example of LUT for $N = 4$ and $K = 2$.

r_K	m_I bits
1100	00
1010	01
1001	10
0110	11

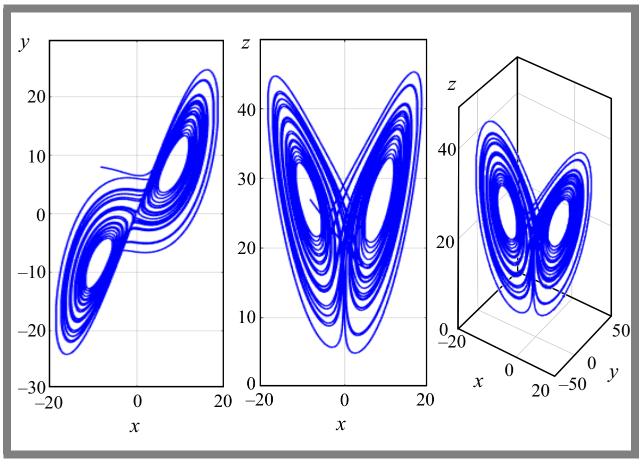

Fig. 3. Lorenz chaotic system phase diagram.

3.4. Lorenz Chaotic Maps

Chaotic sequences are particularly suited for secure communications due to their pseudo randomness, ergodicity, and sensitivity to initial values [15]. Unpredictable yet determined, chaotic sequences could produce entirely distinct output sequences with only a slight alteration from the initial value. As a result, chaotic systems are frequently used in watermarking, secure communication, and cryptography. Lorenz chaotic systems feature more dynamical behaviors and variables of the system than their low-dimensional counterparts, suggesting a larger key space and higher levels of unpredictability [16]. In order to finish the encryption in the proposed scheme, we use a Lorenz chaotic system due to the aforementioned features. The following is a mathematical expression of a typical Lorenz chaotic system [16]–[18]:

$$\begin{cases} \dot{x} = a(y - z) \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \end{cases} , \tag{12}$$

where $a = 10$, $b = 8/3$, $c = 28$.

A phase diagram of a Lorenz chaotic system has been depicted in Fig. 3. It starts with initial values x, y, and z which represent a set of CSI amplitude, phase, and frequency between legitimate users where the TDD mode is adopted. The following is the processing of chaotic sequences $\{xi\}$, $\{yi\}$, and $\{zi\}$, which have been based on the quantization approach introduced in [18]:

$$\begin{aligned} D_{xi} &= \mathrm{mod}(1\,000 \times x_i, 256)/256 \\ D_{yi} &= \mathrm{mod}(1\,000 \times y_i, 256)/256 \ , \\ D_{zi} &= \mathrm{mod}(1\,000 \times z_i, 256)/256 \end{aligned} \tag{13}$$

After that, each of the elements in D_{xi} is converted to 1 or 0 based on the binary sequence L_{xi}:

$$L_{xi} = \begin{cases} 0, & D_{xi} < 0.5 \\ 1, & D_{xi} \geqslant 0.5 \end{cases} , \tag{14}$$

We could acquire the corresponding chaotic binary sequences L_{yi} and L_{zi} through that same quantification technique. In the proposed scheme, two chaotic binary sequences are required to complete the encryption process. Thus, sequences L_{xi}, L_{yi} and L_{zi} are processed in the following way:

$$\begin{cases} B_1 = L_{xi} \bigoplus L_{yi} \\ B_2 = L_{yi} \bigoplus L_{zi} \end{cases} . \tag{15}$$

The Lorenz chaotic system generates two chaotic binary sequences as a result. The selection of the subcarrier index as well as the modulation of the data symbols are encrypted using the two chaotic binary sequences, respectively.

4. Problem Statement

Despite their efficiency, conventional OFDM systems are susceptible to eavesdropping and other security risks, as wireless communications are broadcast and open. Traditional encryption techniques concentrate primarily on the communication protocol's higher levels, which adds complexity and does not always offer enough protection. Furthermore, such techniques frequently entail complex key management procedures that could be time consuming and vulnerable to security breaches at the key distribution phase. A promising OFDM-IM encodes information in both the constellation symbols and subcarrier indices, thus increasing spectral efficiency and dependability. However, OFDM-IM systems are susceptible to security risks, just as their traditional OFDM counterparts are. Among the drawbacks of physical layer encryption techniques now in use for OFDM-IM are their high complexity, substantial transceiver structure modifications, and their major emphasis on the selection of the subcarrier index at the expense of data symbol modulation security.

Furthermore, the detection accuracy and computational complexity of OFDM-IM systems pose additional challenges. The maximum likelihood (ML) detector, while highly accurate, suffers from exponentially increased decoding complexity, making it impractical for larger values of subcarriers and modulation orders. On the other hand, simpler detection methods may not provide the required level of accuracy, especially in the presence of security mechanisms. Therefore, there is a need for a secure, efficient, and low-complexity encryption scheme that can protect both the subcarrier indices and the data symbols in OFDM-IM systems, while maintaining or improving performance and reliability of the transmission. In addition, an effective detection mechanism that balances accuracy and complexity is required. By introducing a new chaotic encryption approach, this work seeks to overcome such challenges. Furthermore, it employs a hybrid greedy detector (GD) alongside the ML detector to optimize the trade-off between computational complexity and detection accuracy, ensuring robust and efficient performance in practical applications.

5. System Model

The general model of a wiretap channel serves as a basis for security analysis [19]. As depicted in Fig. 4, Alice uses the wiretap channel for passive eavesdropping, whereas Eve

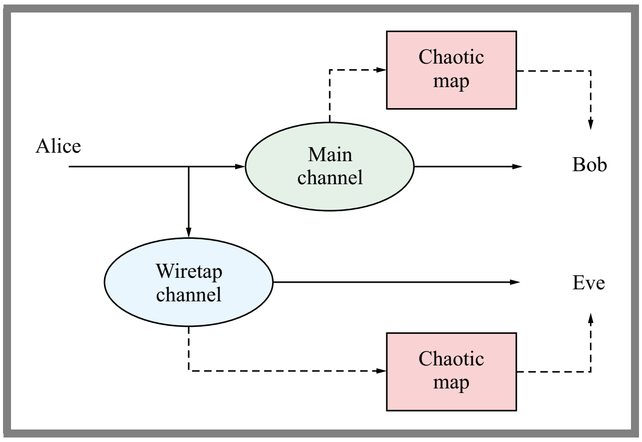

Fig. 4. General wiretap channel model.

tries to send Bob legitimate messages covertly via the secret channel. Given that Eve experiences independent channel fading, it is assumed that she is located half a wavelength away from the legitimate receiver. Because of the wireless channel's reciprocity, Bob and Alice could receive the same CSI if communication is conducted in the TDD mode and a perfect channel estimate is possible. It is important to remember that CSI must adhere to the wireless channel's reciprocity requirement and must not alter during the coherence time. Additionally, Bob and Alice establish the Lorenz chaotic system's initial values for the CSI's amplitude, frequency, and phase. Modulation of data symbols and subcarrier index selection are encrypted using the resulting chaotic sequences. Eve cannot acquire secret keys which represent initial Lorenz chaotic system.

The transmitter of the proposed chaotic encrypted OFDM-IM scheme, as depicted in Fig. 5, is mainly made up of a secure modulator of data symbols depending on chaotic maps and the index selector. Unlike traditional OFDM-IM systems, the method under consideration ensures two levels of security. Only the legitimate receiver is capable could accurately recovering original messages using the established mapping criteria.

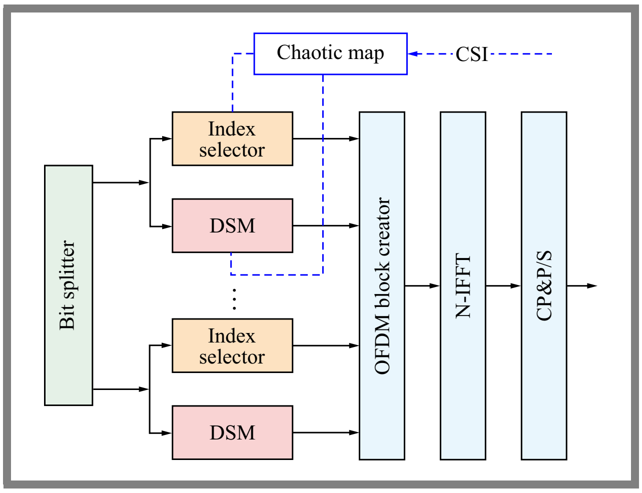

Fig. 5. Block diagram of the proposed transmitter of a chaotic encrypted OFDM-IM model.

5.1. Chaotic Maps on the Selections of the Subcarrier Indices

We provide an encrypted chaotic subcarrier index selector that is based on a combinatorial technique [1]. A natural number may be mapped to its corresponding combination by a combinatorial method, and the Lorenz chaotic system produces chaotic binary sequences which are used for randomizing the combination.

First, q_1 bits undergo conversion to the corresponding decimal value Z, and then this number is converted into the sequence $J = \{c_k, \cdots, c_1\}$ through the combinatory technique:

$$Z = C(c_k, k) + \ldots + C(c_2, 2) + C(c_1, 1)\,. \tag{16}$$

Indices regarding the active subcarrier are specified through $J + 1$. Let us assume that $D^k = \{d_k, \ldots, d_1\}$ denotes active sub-carrier indices and $k = 2^{r_1}, r_1 > 0$. We denote the corresponding chaotic binary sequence through $B_1^l = B_1(1), B_1(2), \ldots, B_1(l)$.

We convert each r_1 bit in B_1^l into a corresponding decimal number, therefore creating decimal sequence T^k that is k long. The decimal values that are contained in T^k traverse each one of the values between 0 and $k-1$ due to ergodicity of the chaotic sequences. After that, the indices of active subcarrier D^k are randomized.

Therefore, we acquire encrypted indices of active sub-carrier E^k:

$$\begin{cases} E(i_1) = D(i_2) \\ T(i_2) = i_1 \end{cases} \quad i_1, i_2 = 0, 1, \ldots, k-1\,. \tag{17}$$

5.2. Chaotic Maps on the Modulation of Data Symbols

We propose a data symbol modulator that is secure and relies on chaotic maps. Here, the chaotic encrypted data symbol modulation process is explained using 32-QAM as an example.

Let us assume $B_2^l = B_2(1), B_2(2), \ldots, B_2(l)$ represents a chaotic binary sequence that corresponds to modulation of encrypted data symbols. As shown in Fig. 6, $P_0(r_o, \theta_o)$ represents the original data symbol, while $P_c(r_c, \theta_c)$ represents a data symbol after mapping in a chaotic manner. Moreover, r_0, r_c represents symbol amplitude and θ_0, θ_c stands for symbols phase with following relation:

$$\begin{cases} r_c = r_0 \\ \theta_c = \theta_0 + 2\pi \frac{M_c}{M} \end{cases}, \tag{18}$$

where M represents a real constant and $M = 2^{r_2}, r_2 > 0$. Next, each r_2 bits in B_2^l are converted into decimal value M_c. Because of the ergodicity of chaotic maps, the range of M_c lies between 0 and $M-1$, thus $2 \times \pi \frac{M_c}{M}$ ranges between 0 and 2π. Let M be set as 256, r_2 be 8, and M_c could be specified through each eight bits in B_2^l.

5.3. Detection at the Receiver's Side

For the recovery of original messages, an ML detector has been used on the legitimate receiver side [1]. It is believed that the receiver side could accomplish a flawless CSI estimate.

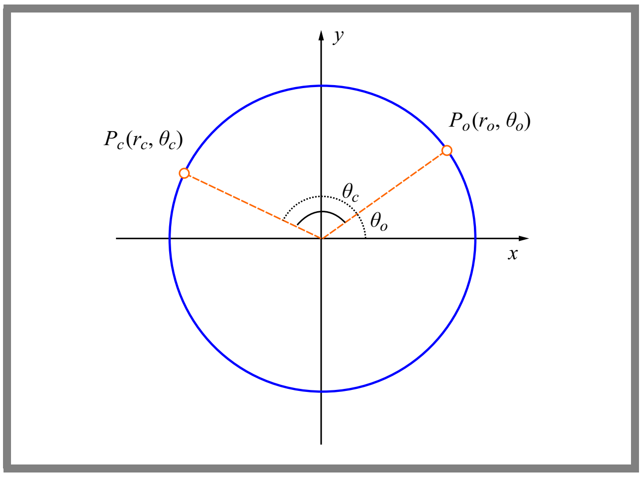

Fig. 6. Process of chaotic maps on the modulation of data symbols.

Inverse encryption operations could be carried out for Bob in order to recover the original key, because the secret users share secret keys as the well as the encryption method. The encrypted data symbol that has been carried by an active subcarrier could be recovered once indices of the sub-carrier are identified. Chaotic maps could be used to decrypt the secret key symbol using secret keys. Thus, at the legitimate receiver side, information carried through the encrypted modulated data symbols as well as the encrypted subcarrier indices could be recovered.

With regard to the multipath fading scenario, wireless channels are geographically separated. Therefore, Eve at a third party cannot acquire the same CSI as Bob and Alice. Eve is thus limited to trying to decode the message using a standard IM detector. Eve cannot decrypt the encrypted messages without secret keys, though, since the data symbol and indices of active the subcarrier are encrypted messages. Therefore, Eve could not get useful messages.

Furthermore, compared to schemes [12], [14], only modest modifications to the structure of the traditional OFDM-IM system are required throughout the detection phase. Because of the simplicity of the transceiver structure, this scheme is easy to implement in practical applications.

6. Performance Analysis

This section evaluates the performance of the proposed chaotic encryption method for the OFDM-IM systems, with a focus on both security and reliability.

6.1. Analysis of Secrecy

The proposed scheme leverages the initial values of the Lorenz chaotic system as secret keys. Given the sensitivity of the Lorenz system to initial conditions, even minute deviations (around 10^{-15}) can lead to entirely different output sequences. This characteristic results in a large key space, estimated at approximately 10^{45} ($10^{15} \times 10^{15} \times 10^{15}$), which offers robust protection against exhaustive search attacks and significantly improves system security compared to conventional encryption methods.

Traditional approaches, such as those referenced in [10] and [12], typically secure only one of these aspects, namely subcarrier indices or data symbols. Although method [13] addresses both, it is directly based on CSI without the additional chaotic encryption layer.

However, this approach integrates chaotic maps based on CSI, which are only known precisely to legitimate communication partners. Due to chaotic system's sensitivity, it is nearly impossible for an eavesdropper to replicate the same sequences without access to the initial conditions, making it exceedingly difficult for unauthorized parties to decode the intercepted signals. This dual-layer encryption significantly enhances OFDM-IM security.

6.2. Reliability Analysis

Monte Carlo simulations conducted over Rayleigh fading channels are used to validate the reliability of chaotic encrypted OFDM-IM system. The following parameters have been used in such simulations: each OFDM frame has 200 symbols, two of the four subcarriers are active, and the modulation method is 4QAM.

The results shown in Fig. 7 demonstrate that the bit error rate (BER) performance with respect to the encrypted OFDM-IM system is comparable to that of traditional OFDM-IM solutions. This indicates that the use of chaotic maps for encryption does not degrade the system's transmission performance.

Moreover, the simulation highlights that the transmission performance for unintended receivers – those without access to the secret keys – deteriorates significantly. This degradation validates the improved security offered by the proposed model, as eavesdroppers without private keys are not capable of effectively decoding transmitted signals.

6.3. Comparative Detection Performance

Besides the validation of transmission performance, the analysis compares the performance of two detection approaches: the hybrid greedy detector (GD) and the maximum likelihood

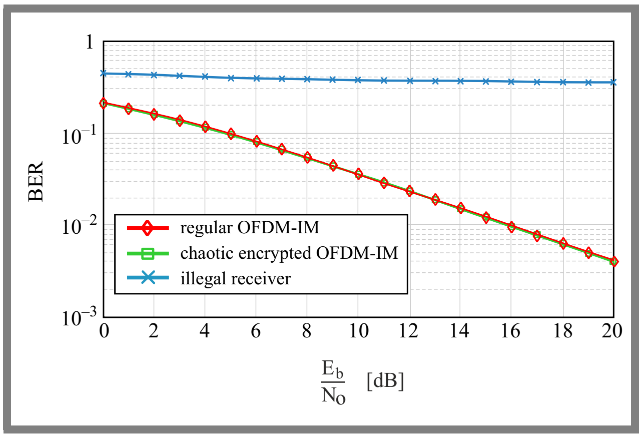

Fig. 7. BER performance of the proposed encrypted OFDM-IM system.

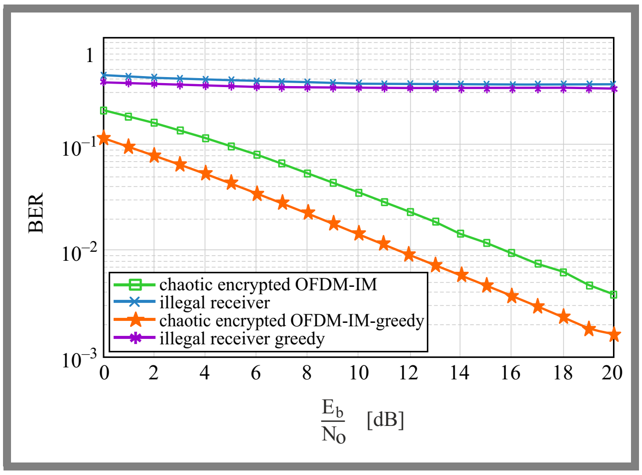

Fig. 8. Comparative detection performance: greedy vs. ML.

detector (ML). GD had demonstrated superior performance compared to ML in terms of computational efficiency and detection accuracy. GD operates in two stages: initially, it detects active subcarriers through the evaluation of received signal power, simplifying the detection process and reducing computational complexity. In the second stage, it applies the criterion of maximum potential for estimating M-ary symbols on identified active subcarriers. This method ensures good accuracy of the detection process and considerably reduces computational burden in comparison with the ML detector, in particular as the number of modulation orders and subcarriers is increased.

The ability of hybrid GD to efficiently and accurately detect active sub-carriers and their corresponding symbols makes it well-suited for the proposed encrypted OFDM-IM system. Its performance-related advantage over the ML detector is especially pronounced in scenarios with larger numbers of subcarriers and higher modulation schemes, where the computational complexity of the ML detector becomes impractical.

Although the proposed chaotic encryption approach based on Lorenz chaotic maps is responsible for boosting the security of OFDM-IM systems, the role of two-stage GD focuses primarily on reducing receiver side complexity and increasing detection robustness. Chaotic encryption randomizes both subcarrier indices and data symbol modulation, which enlarges the hypothesis space and increases index uncertainty at the receiver.

GD addresses this issue by performing an energy-based selection of active subcarriers in its first stage, thereby suppressing unlikely index hypotheses before symbol detection. This mechanism improves robustness against index uncertainty introduced by chaotic encryption and leads to improved BER performance that is shown in Fig. 8. It should be noted that GD does not enhance the security of the system itself, but rather enables efficient and reliable detection under the proposed encrypted OFDM-IM framework. This explains the BER behavior observed in Fig. 8 and confirms that the improved performance of GD under chaotic encryption does not contradict the theoretical optimality of the ML detector.

7. Conclusions

According to simulation results, the proposed scheme enhances the level of security without compromising transmission performance. Additionally, the illegal communication transmission performance has further validated the security. Furthermore, in comparison to the current encryption techniques, the added complexity and adjustment required for traditional OFDM-IM systems are negligible. It has been demonstrated that the suggested side-encrypted OFDM-IM system offers good prospects in terms of practical applications, taking into account both simulation results and theoretical analysis.

Future research could look into more techniques for removing secret keys from wireless channels. Moreover, various communication contexts could benefit from the application of chaotic encryption techniques to raise their security standards.

References

[1] B. Zhang and L. Liu, "Chaos-based Image Encryption: Review, Application, and Challenges", *Mathematics*, vol. 11, art. no. 2585, 2023 (https://doi.org/10.3390/math11112585).

[2] A. Dogukan and E. Basar, "Super-mode OFDM with Index Modulation", *IEEE Transactions on Wireless Communications*, vol. 19, pp. 7353–7362, 2020 (https://doi.org/10.1109/TWC.2020.3010839).

[3] X. Cheng, M. Zhang, M. Wen, and L. Yang, "Index Modulation for 5G: Striving to Do More with Less", *IEEE Wireless Communication*, vol. 25, pp. 126–132, 2018 (https://doi.org/10.1109/MWC.2018.1600355).

[4] X. Cheng, L. Wen, L. Yang, and Y. Li, "Index Modulated OFDM with Interleaved Grouping for V2X Communications", *17th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, Qingdao, China, 2014 (https://doi.org/10.1109/ITSC.2014.6957834).

[5] E. Basar, U. Aygolu, E. Panayirci, and H.V. Poor, "Orthogonal Frequency Division Multiplexing with Index Modulation", *IEEE Transactions on Signal Processing*, vol. 61, pp. 5536–5549, 2013 (https://doi.org/10.1109/TSP.2013.2279771).

[6] J. Wang *et al.*, "A High-security Physical Layer Encryption Scheme for Dual-mode Index Modulation–aided OFDM in Magnetic Induction Communication", *Optics Letters*, vol. 50, pp. 285–288, 2025 (https://doi.org/10.1364/OL.544682).

[7] H. Li, X. Wang, and J. Yves, "Eavesdropping-resilient OFDM System Using Sorted Subcarrier Interleaving", *IEEE Transactions on Wireless Communications*, vol. 14, pp. 1155–1165, 2015 (https://doi.org/10.1109/TWC.2014.2365031).

[8] A.A. Purwita, A. Yesilkaya, M. Safari, and H. Haas, "Generalized Time Slot Index Modulation for Optical Wireless Communications", *IEEE Transactions on Communications*, vol. 68, pp. 3706–3719, 2020 (https://doi.org/10.1109/TCOMM.2020.2979845).

[9] G. Cai *et al.*, "Design of a MISO-SWIPT-aided Code-index Modulated Multi-carrier M-DCSK System for e-health IoT", *IEEE Journal on Selected Areas in Communications*, vol. 39, pp. 311–324, 2021 (https://doi.org/10.1109/JSAC.2020.3020603).

[10] L. Fan, Q. Jiang, and F. Liu, "OFDM-based Waveform Design in Artificial Noise Aided Secure Communication", *2nd International Conference on Electronics Technology (ICET)*, Chengdu, China, 2019 (https://doi.org/10.1109/ELTECH.2019.8839524).

[11] L. Fan *et al.*, "Joint Resource Allocation for Temporal Artificial Noise Assisted Multiuser Wiretap OFDM Channels with Finite-alphabet Inputs", *2nd International Conference on Electronics Technology (ICET)*, Chengdu, China, 2019 (https://doi.org/10.1109/ELTECH.2019.8839391).

[12] J.M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services", *IEEE ACCESS*, vol. 5, pp. 25863–25875, 2017 (https://doi.org/10.1109/ACCESS.2017.2768558).

[13] Y. Lee, H. Jo, Y. Ko, and J. Choi, "Secure Index and Data Symbol Modulation for OFDM-IM", *IEEE ACCESS*, vol. 5, pp. 24959–24974, 2017 (https://doi.org/10.1109/ACCESS.2017.2768540).

[14] X. Zhang, S. Zhang, and Z. Qiao, "A Chaos-based Encryption Scheme for OFDM-IM Systems", *2021 IEEE Symposium on Computers and Communications (ISCC)*, Athens, Greece, 2021 (https://doi.org/10.1109/ISCC53001.2021.9631386).

[15] H.N. Abdullah, T.R. Saeed, and A.H. Sahar, "Suboptimal Detection of Modified Logistic Map-based Chaos Shift Keying Modulation", *UPB Scientific Bulletin, Series C*, vol. 80, pp. 85–94, 2018.

[16] P. Robertson, E. Villebrun, and P. Hoeher, "A Comparison of Optimal and Sub-optimal MAP Decoding Algorithms Operating in the Log Domain", *IEEE International Conference on Communications ICC '95*, Seattle, USA, 1995 (https://doi.org/10.1109/ICC.1995.524253).

[17] H.N. Abdullah, T.R. Saeed, and A.H. Sahar, "Efficient Error Correcting Scheme for Chaos Shift Keying Signals", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, pp. 3550–3557, 2019 (http://doi.org/10.11591/ijece.v9i5.pp3550-3557).

[18] M. Wen, X. Cheng, and L. Yang, "Optimizing the Energy Efficiency of OFDM with Index Modulation", *2014 IEEE International Conference on Communication Systems*, Macau, China, 2014 (https://doi.org/10.1109/ICCS.2014.7024760).

[19] Y. Ko and J. Choi, "Sparse Multi-carrier Index Keying OFDM with Index Separation over Correlated Sub-carriers", *2015 International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, South Korea, 2015 (https://doi.org/10.1109/ICTC.2015.7354553).

Asaad H. Sahar, Ph.D.
https://orcid.org/0000-0003-3655-0162
E-mail: asaad.ha87@gmail.com
University of Baghdad, Baghdad, Iraq
https://en.uobaghdad.edu.iq

Aqiel N. Almamori, Ph.D.
https://orcid.org/0000-0001-5632-9989
University of Baghdad, Baghdad, Iraq
https://en.uobaghdad.edu.iq

Muhannad Y. Muhsin, Ph.D.
https://orcid.org/0000-0003-3937-4467
E-mail: muhannad.y.muhsin@uotechnology.edu.iq
University of Technology – Iraq, Bahdad, Iraq
https://uotechnology.edu.iq