Chaotic Complex-Valued Hopfield Neural Network for Secure OFDM Communication

Quanli Deng, Chunhua Wang, Yichuang Sun *Senior Member, IEEE*, Gang Yang

***Abstract*—The extension of chaotic dynamics into the complex domain offers a promising avenue to overcome the limitations of real-valued chaotic systems in terms of complexity and applicability. This paper presents a comprehensive study on a complex-valued Hopfield neural network (CVHNN) for generating high-complexity chaos and its application in physical layer security. First, a novel CVHNN model is proposed, and its dynamics are rigorously analyzed. Detailed characterization via Lyapunov exponents and bifurcation diagrams confirms the existence of rich chaotic regimes. Second, the CVHNN is successfully implemented on a FPGA platform, validating its physical realizability as a high-speed entropy source. Finally, a secure Orthogonal Frequency-Division Multiplexing (OFDM) scheme is developed, which intrinsically leverages the native complex-valued chaos. The proposed scheme employs a multi-domain encryption strategy, where a single complex chaotic sample directly encrypts a corresponding OFDM symbol in the code, modulation, and time-frequency domains. Overall, this work presents a framework containing chaotic system design, hardware implementation, and application development for complex-valued chaos, offering both a new theoretical foundation in chaotic neural networks and a practical physical-layer security solution for industrial wireless communications.**

***Index Terms*—Complex-valued chaos, Hopfield neural network, OFDM, Multi-domian encryption.**

I. Introduction

As digital connections steadily expand, the need for reliable information security becomes increasingly important. Conventional cryptographic methods primarily operate at the upper layers and can be complemented by security measures at the physical layer [1]–[3]. Consequently, physical layer security has been developed as an additional line of defense to enhance confidentiality by exploiting the intrinsic properties of the transmission medium [4]–[6]. In this context, chaotic systems are considered a suitable candidate for generating pseudo-random sequences due to their deterministic dynamics, sensitivity to initial conditions, and noise-like spectra [7]. Designing high-performance chaotic systems that run reliably and efficiently in hardware-based communication setups is a key step forward.

Building on the foundation of chaotic dynamics, research has extended into the realm of artificial neural networks, where the collective dynamics of interconnected neurons can exhibit rich nonlinear behavior [8]. Among these, the Hopfield neural network (HNN) has been a particularly important model for generating and studying chaos. This is largely due to its clear physical interpretation and tractable dynamics [9]–[11]. Subsequent research has focused on enhancing the complexity of the classical HNN. For instance, the incorporation of memristors has been shown to emulate synaptic connection and introduce multiscroll attractors [12]. Similarly, the introduction of fractional-order derivatives has provided a mechanism to encompass memory effects and historical dependencies, leading to more intricate dynamical behaviors [13]. Furthermore, the integration of external stimulus induces non-autonomous dynamics, which can induce complex structure of attractors [14]. However, most of these models have been confined to the real-valued domain. This inherent constraint bounds the dynamical complexity they can achieve and presents a significant disconnect when considering their application to communication systems that are fundamentally built upon the manipulation of complex-valued signals, such as those in Orthogonal Frequency-Division Multiplexing (OFDM).

To transcend the inherent limitations of real-valued dynamics, a promising pathway is to extend the system's state space into the complex domain. The imperative for such an extension is grounded in fundamental physics, for example, the state vector of quantum systems, the propagation of electromagnetic waves, and the laser systems all inherently rely on complex-valued formulations. This foundational role motivates the exploration of complex-valued chaotic systems. Recent studies have continued to explore this field, demonstrating that systems with complex state variables can yield dynamics of higher complexity and dimensionality [15]–[17]. These properties, including an expanded phase space and inherent nonlinear coupling between real and imaginary components, make them compelling for cryptographic applications [18]. Unlike conventional complex-valued chaotic systems, such as complex Lorenz or complex Chua, where complex variables appear in linear or simple product nonlinearities [19]–[21], the complex-valued neural network (CVNN) features complex-valued weights and activation functions that induce structured real-imaginary coupling through neural dynamics. However, existing CVNN research has primarily focused on stability, synchronization, and learning algorithms, the investigation of

Manuscript received Month xx, 2xxx; revised Month xx, xxxx; accepted Month x, xxxx. This work was supported in part by the National Natural Science Foundation of China under Grants 62271197 and 62571183.

Quanli Deng, Chunhua Wang, and Gang Yang are with the College of Information Science and Engineering, Hunan University, Changsha, 410082, China (Corresponding author: Chunhua Wang, e-mail: wch1227164@hnu.edu.cn).

Yichuang Sun is with the School of Engineering and Computer Science, University of Hertfordshire, Hatfield AL10 9AB, U.K.

their chaotic dynamics remains relatively underexplored. To this end, this paper introduces a novel CVHNN model and conducts a comprehensive study of its chaotic characteristics.

The application of chaos to secure OFDM systems has been extensively explored as a means to enhance physical layer security. Existing approaches can be broadly categorized, with each presenting specific limitations. One common strategy employs low-dimensional chaotic maps for subcarrier indexing or scrambling [22]. While simple to implement, such schemes offer a limited key space and may be vulnerable to brute-force attacks. Another category utilizes high-dimensional or hyperchaotic real-valued systems to increase randomness and security [23]. However, the computational overhead for generating these sequences can be prohibitive for high-speed communication. It is worth noting that nearly all previous work still rests on real-valued chaotic sequences. Thus, real-valued samples must be mapped onto the in-phase and quadrature parts of each OFDM symbol. This decoupled approach not only introduces design inefficiency but may also weaken the encryption's nonlinear integrity. In contrast, this paper proposes to leverage the native complex-valued chaos generated by our CVHNN. We refer to this approach as a complex-to-complex encryption paradigm, where a single complex-valued chaotic sample generated by the CVHNN is used as a cryptographic unit to directly encrypt a single complex-valued OFDM symbol through a unified complex-domain operation, without decomposing either quantity into its real and imaginary components for separate processing.

To overcome the limitations of real-valued chaotic systems in both dynamical complexity and direct applicability to complex-modulated communications, we propose a CVHNN that natively operates in the complex domain. The dynamical behavior of the CVHNN is thoroughly characterized, its hardware realization on FPGA is demonstrated, and a secure OFDM scheme leveraging its complex-valued chaotic outputs is constructed. The main contributions are as follows.

1) Unlike most existing chaotic neural networks confined to the real domain, we propose a novel complex-valued neural network and provide a comprehensive analysis of its chaotic dynamics.
2) The FPGA-based implementation of the CVHNN is presented, validating its physical realizability as a high-speed entropy source for real-time secure communication systems.
3) A novel secure OFDM scheme is introduced, which uniquely leverages native complex-valued chaos in a multi-domain encryption paradigm.

The remainder of this paper is structured as follows: Section II details the CVHNN model and its dynamical analysis. Section III presents numerical simulations of its chaotic behaviors. Section IV describes the FPGA implementation. Section V elaborates on the secure OFDM application and security evaluation. Finally, Section VI concludes the work.

II. CVHNN COMPOSED OF THREE NEURONS

A. Model description

The well-known Hopfield neural network (HNN), which can be suitable for simulating complex brain dynamics, is an important model in artificial neural networks. The traditional HNN can be expressed by a group of differential equations of real number field. For the i-th neuron in an HNN, its state variation function can be expressed mathematically as

$$\dot{x}_i = -x_i + \sum_{j=1}^{N} w_{ij} f(x_j) + I_i \tag{1}$$

where x_i and w_{ij} represent the state variable of neuron i and the connection strength between neuron i and neuron j, respectively. I_i denotes the external input to the neuron, which is set to 0 for simplicity. The activation function $f(\cdot)$ regulates the output region of the neuron, which is always the hyperbolic tangent function or the sigmoid function in the traditional HNNs.

The complex-valued HNN (CVHNN) is an extended form of the traditional HNN, which has complex-valued state variable and connection strength ($x_i, w_{ij} \in \mathbb{C}$). It should be pointed out that the expansion into the complex domain empowers the HNN with higher-dimensional information and richer computational possibilities by incorporating both amplitude and phase components. This broader foundation allows for a wider design space of potential activation functions. In this work, we consider the hyperbolic tangent function applied in a split fashion to the real and imaginary parts of the complex input z, defined as follows

$$f(z) = \tanh(x) + i\tanh(y) \tag{2}$$

where x and y denote the real and imaginary parts of z, respectively.

We consider a CVHNN composed of three neurons, which is the minimal architecture that supports non-trivial recurrent feedback in a Hopfield network and serves as a natural starting point for investigating chaotic dynamics in the complex-valued domain. Higher-order CVHNNs would introduce more complex coupling among neurons, which could make it possible to generate hyperchaos with multiple positive Lyapunov exponents. However, the significantly larger parameter space would pose considerable challenges for both dynamical analysis and numerical simulation. Therefore, as a first step toward understanding chaos in the CVHNN, we focus on the three-neuron architecture as the fundamental case. The connection weight matrix is mathematically described by

$$W = \begin{bmatrix} w_{11} & w_{12} & w_{13} \\ w_{21} & w_{22} & w_{23} \\ w_{31} & w_{32} & w_{33} \end{bmatrix} = \begin{bmatrix} a & 0 & 2+1.5i \\ -(3+2.5i) & 0 & b \\ -2i & -(2+2i) & -2.5i \end{bmatrix} \tag{3}$$

where i denotes the imaginary unit. The parameters $a = a_r + ia_i$ and $b = b_r + ib_i$ are two complex-valued control parameters. Therefore, the mathematical model describing the proposed CVHNN can be expressed as follows

$$\begin{cases} \dot{z}_1 = -z_1 + (a_r + a_i i) f(z_1) + (3 + 1.5i) f(z_3) \\ \dot{z}_2 = -z_2 - (3 + 2.5i) f(z_1) + (b_r + b_i i) f(z_3) \\ \dot{z}_3 = -z_3 - 2i f(z_1) - (2 + 2i) f(z_2) - 2.5i f(z_3) \end{cases} \tag{4}$$

where $z_n \in \mathbb{C}$ is the complex-valued state variable of the n-th neuron.

B. Equilibrium points calculation and stability analysis

The equilibrium point of an ordinary differential dynamical system can be solved by setting the left side of the equation to zero.

$$\mathcal{F}(\mathbf{z}) = 0, \quad \mathbf{z} \in \mathbb{C}^3 \tag{5}$$

It is obvious that the origin $\mathbf{E0} = (0, 0, 0)$ is always an equilibrium point, as directly verified by substitution into the system. However, the activation function does not satisfy the Cauchy-Riemann equations and is therefore non-holomorphic, which precludes the use of complex analytical methods. The resulting equilibrium equations form a system of transcendental equations with both linear and nonlinear terms, and their equivalent six-dimensional real formulation is highly nonlinear and non-convex. Consequently, obtaining closed-form solutions for non-trivial equilibria presents significant challenges. To address these difficulties, we employ a rigorous numerical framework in Python, leveraging the PyTorch library for efficient automatic differentiation and gradient computation, combined with SciPy's optimization suite for the L-BFGS-B algorithm. This computational approach, as depicted in Algorithm 1, integrates global sampling (Sobol sequence and Latin hypercube), local optimization (L-BFGS-B with convergence criterion $|F(\mathbf{x})| < 10^{-10}$), cluster analysis (DBSCAN), and hierarchical refinement. In our implementation, we use $N_{\text{global}} = 2000$ initial samples over $\mathcal{B} = [-10, 10]^6$, a DBSCAN clustering radius $\varepsilon = 0.5$, and hierarchical refinement with an initial radius of 0.5 reduced to 0.1 across two steps, with $N_{\text{local}} = 50$ samples per step. These parameters were chosen to balance computational cost and numerical precision, and all reported equilibria satisfy the convergence tolerance. While the algorithm combines multiple steps to ensure accuracy, it does not fully overcome inherent limitations. It cannot theoretically guarantee the discovery of all equilibrium points, as the completeness of the results inevitably depends on the coverage of the initial sampling and the choice of hyperparameters such as the clustering radius. To enhance confidence in our results, we have verified the consistency of the identified equilibria under different random seeds and sampling sizes.

To enable numerical computation, the complex-valued system is first transformed into an equivalent real-valued formulation. Each complex variable $z_n = x_n + iy_n$ $(n = 1, 2, 3)$ is decomposed into its real and imaginary components, converting into a six-dimensional system

$$\mathbf{x} = [x_1, y_1, x_2, y_2, x_3, y_3]^T \in \mathbb{R}^6. \tag{6}$$

The complex-valued activation function becomes

$$f(z_n) \to [\tanh(x_n), \tanh(y_n)]^T. \tag{7}$$

For parameters $a_r = 2.5$, $a_i = 1$, $b_r = 2.8$, $b_i = 2.2$, this approach identifies five equilibrium points after clustering and hierarchical refinement. The equilibrium points can be obtained as $E_0(0, 0, 0)$, and the symmetric pairs $E_{1,2}$=$\pm(3.63 - 1.22i, -4.76 - 0.04i, 0.06 - 0.07i)$ and $E_{3,4}$=$\pm(1.22+3.63i, 0.04-4.76i, 0.07+0.06i)$. Their stability is determined by the eigenvalues of the Jacobian matrix. All equilibrium points are unstable, as the eigenvalue spectrum of each possesses at least one eigenvalue with a positive real part. The configuration of multiple unstable equilibria indicates rich dynamical behavior including potential chaotic oscillation.

Algorithm 1 Equilibrium Point Search Algorithm

Require: Dynamics $F(z)$, bounds $\mathcal{B}$, tolerance $\tau = 10^{-10}$
Ensure: Equilibrium points $\mathcal{E}$
$\mathcal{G} \leftarrow \text{SobolSample}(N, \mathcal{B})$ {Global sampling}
$\mathcal{E} \leftarrow \emptyset$
for $\mathbf{z}_0 \in \mathcal{G}$ **do**
  $\mathbf{z}^* \leftarrow \arg\min_{\mathbf{z}} \|F(\mathbf{z})\|^2$ {L-BFGS-B optimization}
  if $\|F(\mathbf{z}^*)\| < \tau$ **then**
    $\mathcal{E} \leftarrow \mathcal{E} \cup \{\mathbf{z}^*\}$
  end if
end for
$\mathcal{E} \leftarrow \text{DBSCAN}(\mathcal{E})$ {Cluster and remove duplicates}
$\mathcal{E} \leftarrow \text{LocalRefine}(\mathcal{E})$ {Hierarchical refinement}
return $\mathcal{E}$

III. Numerical Simulation and Dynamical Analysis

A. Chaotic attractor under fixed parameters

The analysis presented in the above section confirms the existence of multiple unstable equilibrium points for a specific parameter set, (a=2.5+1i, b=2.8+2.2i), suggesting the potential for complex dynamics. To verify this and explore the resulting behaviors, we proceed with numerical simulations using the same parameter set. The initial condition for the simulation is set to z_0=[0.1+0.1i,0.1+0.1i,0.1+0.1i]. Fig.1 depicts the simulation results in the phase space, along with the distribution of the five equilibrium points. The trajectories are bounded within a finite region and evolve in an aperiodic manner, indicating a chaotic attractor.

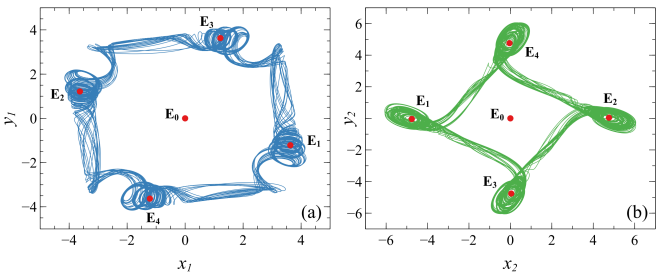

Fig. 1. Phase plot with equilibrium points in (a)$x_1 - y_1$ plane, (b) $x_2 - y_2$ plane

To confirm the chaotic nature of the attractor, we employ two quantitative techniques: the Poincaré map and 0-1 test. The Poincaré map is constructed by recording the intersections of trajectory with a hyperplane, $x_3 = 0$. The resulting section, shown in Fig.2(a), reveals a collection of points forming a structured, fractal-like pattern. This indicates that the dynamics are constrained to a strange attractor with non-periodic. The diffusive-like trajectory in the auxiliary $(p-s)$ plane generated by the 0-1 test is depicted in Fig.2(b). It can be seen that the trajectory exhibits Brownian-like, unbounded diffusion, which is characteristic of chaotic systems. The corresponding

quantitative value K=0.996 (close to 1) provides numerical evidence confirming the chaotic nature of the attractor.

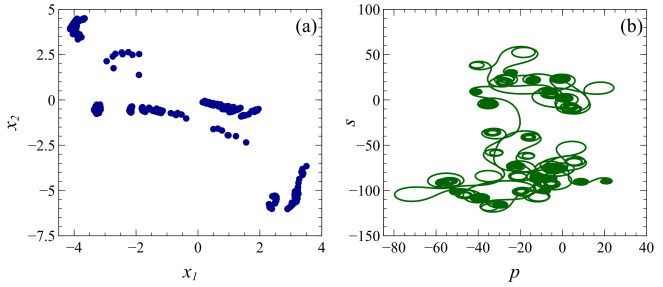

Fig. 2. Test for the chaotic attractor by (a) Poincaré map, (b) 0-1 test trajectory in *p-s* plane

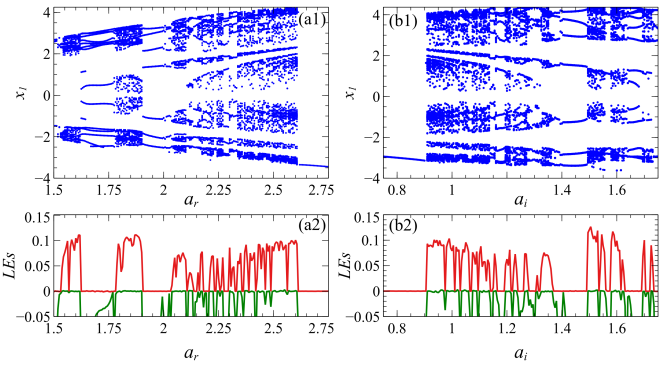

Fig. 3. Dynamics variation with parameter a for fixed $b = 2.8 + 2.2i$ (a) $a_r \in [1.5, 2.75]$, $a_i = 1$, (b) $a_i \in [0.75, 1.75]$, $a_r = 2.5$

B. Dynamical variation with parameters

The analysis in the previous subsection confirms the existence of a chaotic attractor for a specific parameter set. To comprehensively identify transitions between different dynamical regimes, we investigate how the dynamics evolve with parameters. This exploration is conducted using multiple numerical simulation methods, such as Lyapunov exponents (LE) spectra, bifurcation diagrams, and largest LE (LLE)-based two-parameter dynamical maps. The LEs are calculated utilizing the Wolf's Jacobian matrix-based algorithm, which provides a rapid and accurate numerical computation. The bifurcation diagram is obtained by evaluating the local maximum value of the x_1, which is the real part of state z_1.

The initial condition is held constant at z_0, consistent with previous section. The dynamical behavior transition with respect to the complex-valued parameter a as $b = 2.8 + 2.2i$ is depicted in Fig.3. For varying parameter $a_r \in [1.5, 2.75]$ with $a_i = 1$, the first two LEs in Fig.3(a2) identifies three intervals ([1.53,1.62], [1.78,1.9] and [2.0,2.6]) characterized by positive values, indicating chaotic behavior. Notably, the LLE in interval [2.0,2.6] fluctuates between positive value and zero suggesting intense alternations between chaotic and periodic dynamics. The corresponding bifurcation diagram in Fig.3(a1) reveals multiple periodic windows embedded within the chaotic region. Similarly, variations of the parameter a_i induce significant dynamical transitions. As a_i increases, the LLE in Fig.3(b2) shifts from zero to positive and organizes into three chaotic regions ([0.9,1.37], [1.49,1.63] and [1.68,1.73]). Among these, region [0.9,1.37] is interspersed with several periodic windows, highlighting the system's sensitivity to minor parameter changes. The bifurcation diagram in Fig.3(b1) further illustrates the dynamical behavior evolution, commencing with a crisis-induced transition to chaos, where a periodic attractor vanishes, leading to the sudden emergence of a chaotic attractor.

The dynamical behavior variation with respect to parameter b as depicted in Fig.4, reveals both shared and distinct features when compared to the behavior governed by a. A prominent characteristic of parameter b_r is its capacity to sustain chaos over extensive ranges, with two primary chaotic intervals, [1.27,6.0] and [6.94,12], identified by positive LLE in Fig.4(a2). Notably, the onset of chaos with b_r, observed in the bifurcation diagram Fig.4(a1), changes abruptly without a preceding period-doubling cascade suggesting that sudden chaotic bursts are fundamental mechanism within this system. Similarly, the dynamics under parameter b_i also features two main chaotic regions ([1.74,3.58] and [3.87,3.96]). The first region is interspersed with multiple periodic windows, indicating a balance where slight parameter variations can suppress or reignite chaos. The second region is characterized by a relatively small yet positive LLE. The corresponding bifurcation diagram in Fig.4(b1) reveals that this weak chaos is preceded by a sequence of periodic regimes.

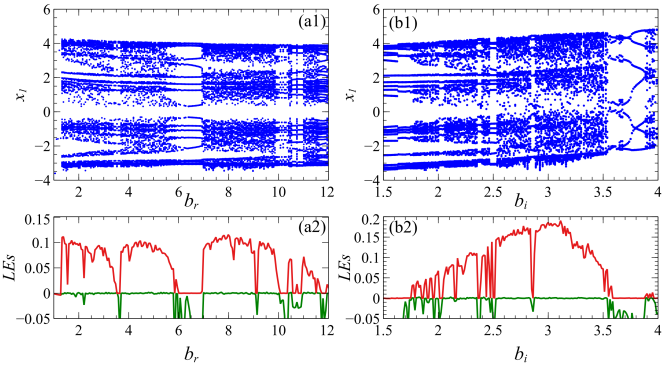

Fig. 4. Dynamics variation with parameter b for fixed $a = 2.5 + 1i$ (a) $b_r \in [1, 12]$, $b_i = 2.2$, (b) $b_i \in [1.5, 4]$, $b_r = 2.8$

Following the analysis of the dynamical behavior under variation of single parameter, a two-dimensional parameter study was conducted to gain deeper insight. Fig.5 presents the resulting colored maps, which illustrate the transitions in dynamics across two distinct parameter planes: the $a_r - a_i$ plane with $b = 2.8 + 2.2i$ and $b_r - b_i$ plane with $a = 2.5 + 1i$. To create each subplot, a dense grid of 500 by 500 parameter pairs was defined for the respective plane. In these plots, the LLE is used as the metric to characterize the dynamical behavior, with different colors representing different values of the exponent. Regions colored in deep red, indicating the highest positive LE and thus the most chaotic behavior, are not randomly distributed. In the $a_r - a_i$ plane, Fig.5(a), the strongest chaos is predominantly concentrated in a central

region. In contrast, within the $b_r - b_i$ plane, Fig.5(b), the most chaotic dynamics are primarily located in the upper portion of the parameter space. These distinct patterns highlight how different parameter groups govern the system's nonlinearity in fundamentally different ways.

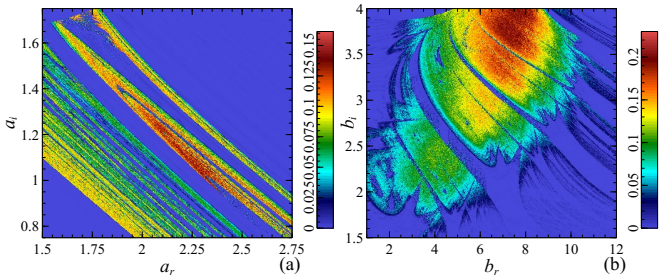

Fig. 5. Dynamical map for parameter in (a) $a_r - a_i$ plane with b=$2.8 + 2.2i$, (b) $b_r - b_i$ plane with $a = 2.5 + 1i$

IV. FPGA-BASED IMPLEMENTATION

The realization of neural networks in software is often hindered by limited computational speed, especially for real-time applications. Hardware implementation offer a compelling solution, providing a significant acceleration in processing the complex, nonlinear dynamics inherent to chaotic neural networks. Among hardware platforms, Field-Programmable Gate Arrays (FPGAs) are uniquely suited for this task for their inherent parallelism and their reconfigurability [24]–[26]. To experimentally validate this approach, our design was implemented on a Xilinx Zynq-7000 SoC (specifically, the xc7z020clg400-1 chip). The system, clocked at 50 MHz, computes the chaotic system's state in hardware, and the resulting chaotic signals are converted to analog voltage via an AD9767 dual-channel 14-bit Digital-to-Analog Converter (DAC), facilitating direct observation of the phase portraits on an oscilloscope.

To facilitate a resource-efficient hardware implementation on the FPGA, the proposed complex-valued system (4) is decomposed into its equivalent real and imaginary parts, resulting in a set of six first-order ordinary differential equations governing the dynamics of x_1, y_1, x_2, y_2, x_3, y_3. For numerical solution, the four-order Runge-Kutta (RK4) method is implemented using a highly optimized, parallel, and pipelined architecture. The overall hardware system overview and detailed execution pipeline are depicted in Fig.6. As illustrated in Fig.6, the system is architected around a central RK4 compute engine. The six state variables and system parameters are stored in registers, formatted as fixed-point represented by Q5.27 (32 bits in total, with 1 sign bit, 4 integer bits, and 27 fractional bits). The computation is managed by a control FSM (Finite State Machine), which sequences the four stages of the RK4 method.

The hyperbolic tangent function, serving as the activation is a critical nonlinearity whose hardware implementation directly impacts both resource consumption and numerical accuracy. While software implementations can utilize high-precision library function, a direct mapping to hardware would require

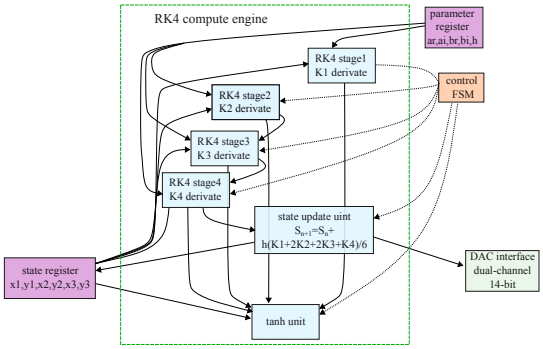

Fig. 6. Scheme of FPGA-based implementation.

either resource intensive iterative arithmetic units or inefficient lookup tables [27]–[29]. To overcome this bottleneck and achieve a high speed and area efficient design, we employ a piece-wise linear approximation strategy [26]. The approximation is designed to balance precision and hardware cost, defined by the following function:

$$\tanh(x) \approx \begin{cases} +1 & \text{if } x > 2 \\ x \cdot (1 - |x|/4) & \text{if } |x| \leq 2 \\ -1 & \text{if } x < -2 \end{cases} \tag{8}$$

The saturation regions ($|x| > 2$) are implemented by simple comparators. The core linear operation for $|x| \leq 2$, $x \cdot (1 - |x|/4)$, can be decomposed into low-cost arithmetic operations: the absolute value $|x|$, a right-shift to compute $x/4$(equivalent to division by 4), a subtraction, and a final multiplication.

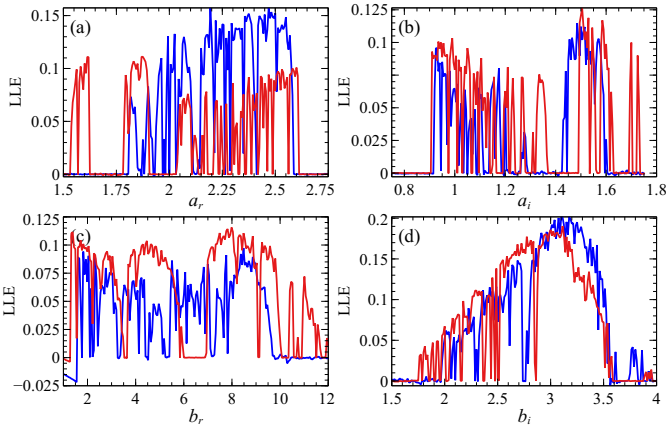

Fig. 7. The LLE of tanh function-based (red) and approximation function-based (blue) system for (a) a_r ∈[1.5,2.75], (b) a_i ∈[0.75,1.75], (c) b_r ∈[1,12], (d)b_i ∈[1.5,4]

To evaluate the impact of the approximation function on the dynamical behavior of the system, we calculated the LLE of the system under different parameters using both the original tanh function and the approximation function. The results under four parameter conditions are presented in Fig.7, where the red curves correspond to the original tanh function and the blue curves correspond to the approximation function. It can be observed from Fig.7 that the piece-wise linear approximation function preserves the dynamical evolution trend induced by the original tanh function. Across the variation intervals of

the four parameters, the overall shapes of the red and blue LLE curves are generally similar, except in certain parameter regions where the use of the approximation function leads to disappearance of chaos. Therefore, while the approximation function does not perfectly preserve chaos in all parameter regions, it captures the main parameter-dependent characteristics of the system and is suitable for FPGA implementation, as long as the affected regions are avoided.

To validate the functionality and performance of the proposed hardware architecture, the implemented system was tested experimentally. Fig.8 displays the chaotic attractor observed directly from the oscilloscope, plotted in the x_1-y_1 and x_2-y_2 phase space. The hardware generated phase portraits exhibit the characteristic topological structure and dynamics of chaos. Furthermore, the structure of the experimentally obtained attractors is in agreement with the numerical results in Fig.1, confirming the correct functionality of the FPGA implementation. Minor discrepancies in the fine details can be attributed to the inherent limitations of physical hardware, such as the finite resolution of the digital-to-analog converters and the presence of minimal analog noise. Nonetheless, the core finding stands: the proposed architecture faithfully reproduces the complex dynamics of the chaotic neural network on an FPGA platform.

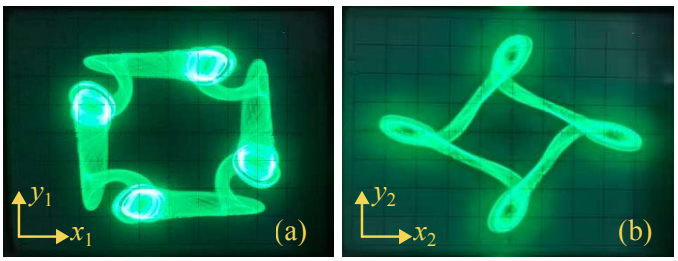

Fig. 8. FPGA implemented chaotic attractor in (a) $x_1 - y_1$ plane (b) $x_2 - y_2$ plane.

The above hardware experimental results were obtained through iterative design and careful debugging. Several inherent limitations of the FPGA implementation merit further discussion, as they point toward valuable directions for future improvement. Among them, a persistent challenge in hardware chaos generation is the degradation of chaotic dynamics under finite-precision arithmetic. To evaluate this effect, five fixed-point formats with data widths ranging from 16 to 64 bits were tested under the same chaotic parameter set and initial condition. Brent's cycle detection algorithm was applied to 1000 random initial states per configuration, with each test running until either a cycle was detected or a maximum of 5×10^{11} samples was reached. Table I summarizes the results. The 16-bit format consistently exhibited periodic behavior with short cycle lengths ($\approx 1.44\times10^5$), confirming severe chaos degradation under low precision. The 24-bit format showed periodic behavior in 85.5% of tests, with cycle lengths exceeding 8.76×10^8 in the remaining cases, indicating weak or intermittent chaos. In contrast, both 32-bit and 64-bit implementations maintained chaotic characteristics throughout all tests, with no cycles detected even at the maximum test length. Nevertheless, this result does not theoretically guarantee the absence of periodicity beyond the 5×10^{11} sample limit; the possibility of chaos degradation under finite precision cannot be completely eliminated. Therefore, the choice of data width must be carefully evaluated against the security requirements and expected sequence length of the target application.

V. Application in Secure OFDM Communication

The security of OFDM, the cornerstone of modern high-speed wireless communication, has become a subject of paramount importance. As the physical layer of choice for technologies ranging from Wi-Fi to 5G, the inherent broadcast nature of OFDM transmissions makes them intrinsically vulnerable to interception and eavesdropping. While conventional cryptographic methods provide security at higher layers, there is a growing need for the physical layer security solutions that can offer an additional, robust line of defense. The proposed secure OFDM scheme is considered in the context of industrial wireless edge communications, where OFDM-based physical layers are increasingly adopted for low-latency data transmission between distributed sensors, controllers, and edge devices in smart manufacturing systems. These environments are characterized by rich multipath propagation, electromagnetic interference from machinery, and resource constrained nodes where upper layer encryption may be impractical. In such systems, conventional upper-layer cryptographic protocols may introduce additional latency and computational overhead that are undesirable for real-time industrial control loops and lightweight edge devices. This work proposes a secure OFDM communication scheme utilizing the CVHNN. The CVHNN's capability to generate highly random, non-periodic, and unpredictable complex-valued sequences presents a suitable match for requirements of secure OFDM, which fundamentally relies on complex-valued symbols for modulation.

A. Proposed secure OFDM system

The architecture of the proposed multi-layer secure OFDM communication system is illustrated in Fig.9. The system leverages the native complex-valued output of the proposed CVHNN to perform concurrent encryption across three domains: code, modulation, and time-frequency. The entire process is governed by the chaotic sequence $\mathbf{C}_m$ generated by the CVHNN (4). This sequence is partitioned into four segments to independently drive the different encryption stages, ensuring a high level of security and randomness.

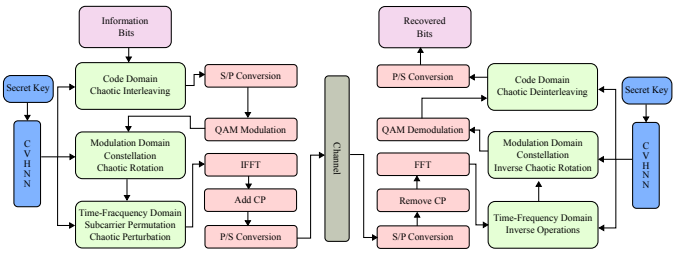

Fig. 9. Block diagram of the CVHNN-based secure OFDM communication.

TABLE I
CHAOS DEGRADATION UNDER DIFFERENT FIXED-POINT PRECISIONS
(BRENT'S CYCLE DETECTION ALGORITHM, 1000 RANDOM INITIAL STATES PER CONFIGURATION)

Precision	Periodic ratio	Max detected cycle length	Observed dynamics
16-bit	100% (1000/1000)	$\approx 1.44 \times 10^5$	Periodic / limit cycle
24-bit	85.5% (855/1000)	$> 8.76 \times 10^8$ (incomplete)	Intermittent / weak chaos
32-bit	0% (0/1000)	Not detected ($> 5 \times 10^{11}$ samples)	Fully chaotic
64-bit	0% (0/1000)	Not detected ($> 5 \times 10^{11}$ samples)	Fully chaotic

The encryption process begins in the code domain. The input binary stream $\mathbf{b}$ is first permuted using a chaotic interleaver. The interleaving pattern $\mathbf{P}_{\text{inter}}$ is generated directly from the sorted indices of the real part of a chaotic sequence segment $\mathbf{c}_{\text{code}}$:

$$[\sim, \mathbf{P}_{\text{inter}}] = \text{sort}(\text{real}(\mathbf{c}_{\text{code}})) \tag{9}$$

where $\mathbf{c}_{\text{code}} = \mathbf{C}_m(1 : L, 1)$ and L is the length of $\mathbf{b}$. The interleaved bits $\mathbf{b}'$ are then obtained as $\mathbf{b}' = \mathbf{b}(\mathbf{P}_{\text{inter}})$. This step disperses the original bits sequence, providing initial security and robustness against burst errors.

Following the interleaving, the bits are mapped to QAM symbols, which are then encrypted using a dynamic constellation. Each QAM symbol s_i is rotated by a chaotic phase derived from the second chaotic segment $\mathbf{c}_{\text{qam}}$:

$$\tilde{s}_i = s_i \cdot exp(j \cdot k_\phi \cdot \angle \mathbf{c}_{\text{qam},i}) \tag{10}$$

Here, k_ϕ is a system parameter controlling the phase perturbation strength. The resultant encrypted symbol vector $\tilde{s}$ is reshaped into a matrix $\mathbf{S} \in \mathbb{C}^{N_{\text{sub}} \times N_{\text{sym}}}$ for subsequent spatial encryption. In practice, the complex-to-complex paradigm means that each complex chaotic sample $c \in \mathbb{C}$ and each complex OFDM symbol $s \in \mathbb{C}$ are treated as complex entities, and the encryption operation $s \mapsto s_{enc}$ is a function f: $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ that does not explicitly separate the real and imaginary parts of either input. Specifically, all encryption operations described above follow the complex-to-complex paradigm. Specifically, each chaotic sample c and each OFDM symbol s are treated as complex quantities. For instance, in the QAM-level encryption the complex c_i provides a single phase angle $\angle c_i$ that simultaneously rotates the entire complex symbol s_i, rather than separately controlling its real and imaginary parts. This unified treatment preserves the intrinsic coupling between the I and Q components of the OFDM symbol, making the encryption match to the complex modulation format.

In the time domain, the encryption involves a three-step process on each OFDM symbol column. A collective phase rotation of the symbols, governed by the expression:

$$\mathbf{S}_{\text{phase}} = \mathbf{S} \odot exp(j \cdot k_\phi \cdot \angle \mathbf{c}_{\text{time}}) \tag{11}$$

where $\odot$ denotes the Hadamard product. Subsequently, the temporal sequence of symbols within each OFDM symbol is scrambled through a permutation pattern generated from the imaginary of $\mathbf{c}_{\text{time}}$. The process generates the final time-domain encrypted matrix:

$$\mathbf{S}_{\text{time}} = \mathbf{S}_{\text{perm}} \odot (1 + 0.1 \cdot \text{real}(\mathbf{c}_{\text{time}})) \tag{12}$$

This composite operation ensures that both the phase and amplitude characteristics of the original signal are effectively masked. The encrypted matrix $\mathbf{S}_{\text{time}}$ is further encrypted in the frequency domain before IFFT. First, the mapping of data to subcarriers is dynamically altered by permuting the rows of $\mathbf{S}_{\text{time}}$ based on a pattern derived from the real part of a dedicated chaotic sequence $\mathbf{c}_{\text{freq}}$. Following this permutation, a subcarrier specific phase perturbation is applied, finalizing the frequency domain encrypted signal as:

$$\mathbf{S}_{\text{freq}} = \mathbf{S}_{\text{map}} \odot exp(j \cdot k_\phi \angle \mathbf{c}_{\text{freq}}) \tag{13}$$

This two-stage frequency-domain encryption effectively decouples the logical subcarrier indexing from the physical transmission, adding a layer of distortion that is deterministic only to the legitimate receiver possessing the correct chaotic key.

Finally, the multi-domain encrypted symbol matrix $\mathbf{S}_{\text{freq}}$ is transformed into a time-domain OFDM signal through conventional modulation. The encrypted complex symbols are converted to a time-domain waveform via an inverse fast Fourier transform (IFFT) operation, which is mathematically expressed as:

$$\mathbf{x}_{\text{ifft}} = \sqrt{N_{\text{sub}}} \cdot \text{IFFT}(\mathbf{S}_{\text{freq}}) \tag{14}$$

where $\sqrt{N_{\text{sub}}}$ ensures the conservation of power. To combat inter-symbol interference in multipath channels, a cyclic prefix (CP) of length N_{cp} is appended to each time domain OFDM symbol, forming the final baseband transmitted signal $\mathbf{x}_{\text{tx}}$.

At the receiver, the decryption process systematically reverses the transmitter's operations to recover the original data. Upon receiving the time-domain signal, the receiver first performs standard OFDM demodulation, which involves removing the cyclic prefix and applying an FFT to convert the signal back to the frequency domain. The encrypted signal then undergoes a sequential decryption procedure: first in the frequency domain, where the inverse of the chaotic subcarrier permutation and phase perturbation is applied, followed by decryption in the time domain, which inverts the amplitude perturbation, symbol permutation, and phase rotation. The resulting symbols are then corrected for the QAM-level chaotic phase shift, demodulated into bits, and finally passed through a chaotic deinterleaver. Crucially, this entire process is contingent upon the receiver's ability to regenerate the identical chaotic sequences used during encryption, ensuring that only an authorized party with the correct initial key can successfully recover the information.

To validate the performance and security of the proposed secure OFDM system, a series of simulations are conducted

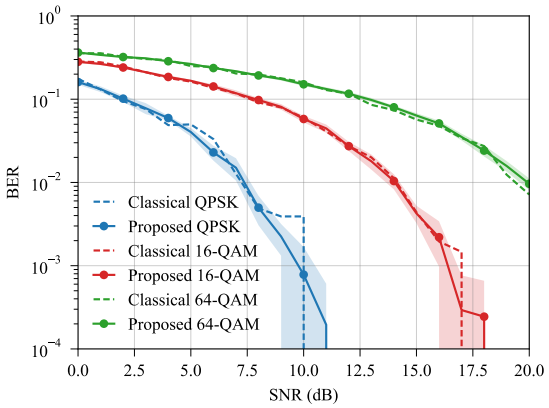

Fig. 10. BER performance comparison between the proposed secure OFDM system and classical OFDM system

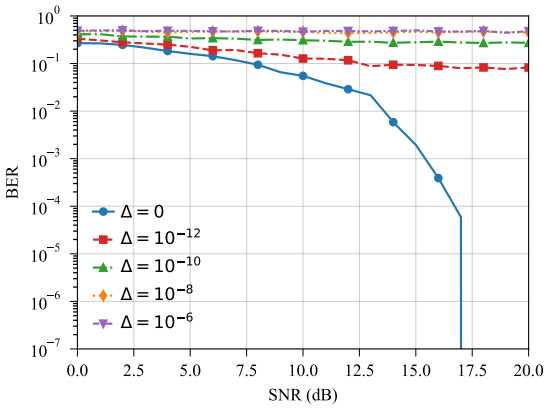

Fig. 11. BER performance comparison between the correct key and minor change in the key.

in MATLAB. The adopted OFDM parameters are consistent with practical wireless communication systems employing QPSK/16-QAM modulation and multipath-resistant OFDM transmission. The core simulation parameters are summarized in Table II.

TABLE II
PARAMETER SETTINGS FOR THE SECURE OFDM

Parameter	Symbol	Value
Number of subcarries	N_{sub}	64
Number of OFDM symbols	N_{sym}	8
Cyclic prefix length	N_{cp}	16
Modulation order	M	16(QAM)
Initial conditions	z_0	$0.1 + 0.1j$
Phase scaling factor	k_ϕ	0.1

B. Communication effectiveness

To evaluate the impact of the proposed chaotic encryption scheme on communication quality, the Bit Error Rate (BER) performance of the proposed secure OFDM system was compared against that of a classical (non-encrypted) OFDM system over an Additive White Gaussian Noise (AWGN) channel. Fig.10 depicts the BER versus SNR curves for both systems under QPSK (M=4), 16-QAM, and 64-QAM modulations. Each data point for the proposed system was obtained from 50 independent Monte Carlo runs, with shaded error band indicating the statistical variability of the BER measurements.

The simulation results demonstrate that the BER curve of the proposed encrypted system, when decrypted by the legitimate user with the correct key, aligns almost perfectly with that of the classical OFDM system across all modulation orders and the entire SNR range. The close alignment of the curves indicates that the complex perturbations introduced in the code, time, and frequency domains during encryption do not introduce any additional, non-invertible deterministic distortion to the transmitted signal. For the authorized receiver, the entire encryption process is effectively equivalent to a transparent layer, perfectly restoring the original signal after correct decryption and thereby preserving the intrinsic error rate performance of the classical OFDM system.

C. Security performance evaluation

Having established the communication effectiveness for the legitimate user, we now proceed to evaluate the security performance of the proposed encryption scheme. The security lies in the extreme sensitivity to the encryption key, which provided by the initial condition of the CVHNN. To investigate the key sensitivity property, we focus on a configured with 16-QAM modulation. The scenario where the legitimate receiver employs the correct key (Δ=0) with those where an eavesdropper use keys with minute deviations (Δ=10^{-12}, 10^{-10},10^{-8}, 10^{-6}) from the correct initial condition. as shown in Fig.11. The results reveal that the legitimate user experiences a characteristic BER-SNR curve that follows the theoretical performance. In contrast, eavesdroppers with key deviations as minute as 10^{-12} exhibit a constant high BER, completely independent of the channel SNR.

The simulation results demonstrate extreme key sensitivity, a necessary condition for security. The resilience of the proposed scheme against cryptanalytic attacks, such as know-plaintext attacks (KPA), chose-plaintext attacks (CPA), and differential attacks is analyzed as follows. Let $\mathbf{K} = (\mathbf{z}_0, a, b)$ denote the secret key, and let $\Psi_{\mathbf{K}} : \mathbf{b} \mapsto \mathbf{S}_{\text{freq}}$ denote the overall encryption mapping from the plaintext bit sequence to the encrypted frequency-domain symbol matrix. This mapping is realized as the composition $\Psi_{\mathbf{K}} = \mathcal{F} \circ \mathcal{T} \circ \mathcal{R}_{\text{QAM}} \circ \mathcal{I}$, where each component operation is key-driven by distinct segments of the chaotic trajectory generated by the CVHNN from $\mathbf{K}$. The security analysis hinges on three properties. Firstly, the CVHNN defines a chaotic map $\Phi : \mathbb{C}^3 \to \mathbb{C}^3$ whose n-step iteration $\Phi^n(\mathbf{z}_0)$ produces the complex-valued sequence used for encryption. For any finite-length observation $\{\Phi^t(\mathbf{z}_0)\}_{t=1}^{L}$, the problem of recovering $\mathbf{z}_0$ satisfies the following Lipschitz-based lower bound on reconstruction error:

$$\|\mathbf{z}_0 - \hat{\mathbf{z}}_0\| \geq \frac{1}{\Lambda^L} \|\Phi^L(\mathbf{z}_0) - \Phi^L(\hat{\mathbf{z}}_0)\|, \tag{15}$$

where $\Lambda > 1$ is the maximum Lyapunov exponent of the CVHNN. Since Λ^L grows exponentially with L, even a minuscule observation error in the chaotic sequence translates into an exponentially amplified uncertainty in the estimated key,

making exact recovery computationally infeasible. Secondly, differential attack analysis examines how a plaintext difference propagates through $\Psi_{\mathbf{K}}$. Consider two distinct plaintexts $\mathbf{b}$ and $\mathbf{b}'$ with Hamming distance $d_H(\mathbf{b}, \mathbf{b}') = 1$, and let $\Delta\mathbf{S} = \mathbf{S}_{\text{freq}} - \mathbf{S}'_{\text{freq}}$ denote the resulting ciphertext difference. The multi-domain structure ensures that $\Delta\mathbf{S}$ depends on the chaotic permutations and phase rotations in a manner that is statistically decoupled from the input difference. Specifically, the expected correlation satisfies:

$$\mathbb{E}_{\mathbf{K}}\left[\langle \Delta\mathbf{S}, \nabla_{\mathbf{b}} \Psi_{\mathbf{K}} \cdot \mathbf{e} \rangle\right] = 0, \tag{16}$$

where $\mathbf{e}$ is the unit vector in the direction of the bit flip, and $\langle \cdot, \cdot \rangle$ denotes the inner product over the complex symbol space. This zero-correlation condition implies that no systematic differential pattern exists across different keys, rendering classical differential cryptanalysis ineffective. Finally, under a chosen-plaintext attack, Eve may query the encryption oracle with arbitrary plaintexts. However, because the CVHNN state evolves deterministically without reset between queries, the chaotic subsequence used for each encryption is unique and non-repeating. Consequently, the encryption mapping satisfies:

$$\Pr\left(\Psi_{\mathbf{K}}(\mathbf{b}_1) \oplus \Psi_{\mathbf{K}}(\mathbf{b}_2) = \Psi_{\mathbf{K}}(\mathbf{b}_1 \oplus \mathbf{b}_2)\right) \approx \frac{1}{|\mathcal{M}|^{N_{\text{sub}}}}, \tag{17}$$

where $\oplus$ denotes bitwise XOR for plaintexts and complex difference for ciphertexts, and $|\mathcal{M}|$ is the constellation size. The probability approaches that of a random mapping, confirming the absence of linear or affine structures that could be exploited in CPA. Together, these analyses establish that the proposed scheme meets physical-layer security requirements under standard cryptanalytic threat models.

Statistical analysis attacks often exploit the distinct patterns present in modulated signal to deduce modulation scheme or extract information. A secure encryption system should effectively eliminate these patterns in the transmitted signal. To evaluate this aspect, we examine the constellation diagrams at different stages of the proposed system under 16-QAM modulation. The ideal 16-QAM constellation at the transmitter, as shown in Fig.12(a), showcasing 16 well-defined and distinct symbol points prior to any encryption and transmission. The constellation of the signal after application of the chaotic encryption is depicted in Fig.12(b). The effect of the chaotic phase rotation is clearly visible, in which the original discrete constellation points are transformed into a set of concentric circular rings. The security and reversibility of the process are validated in Figs.12(c) and (d), which depict the decrypted constellations under a noisy channel with SNR of 20dB. Fig.12(c) shows the constellation after decryption by the legitimate receiver using the correct key, demonstrating the lossless and precise nature of the encryption and decryption process for an authorized user. In contrast, Fig.12(d) shows the constellation after a decryption attempt by an eavesdropper using a key with minor deviation of 10^{-8}. The result remains a structured but incorrect scatter plot, failing to obtain the original points. The constellation diagram analysis further visually attests to its robustness against statistical analysis. Therefore, this scheme establishes a secure and reliable communication framework by seamlessly embedding confidentiality into the very fabric of the OFDM signal generation process.

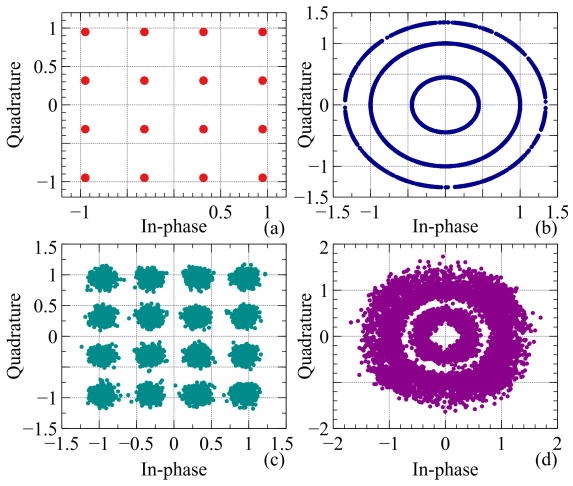

Fig. 12. Constellation diagram analysis for 16-QAM modulation (a) original constellation (b) encrypted constellation (c) correctly decrypted constellation (d) illegally decrypted constellation.

The secret key of the proposed scheme consists of the initial conditions of the three complex-valued neurons and the two complex-valued control parameters. Decomposing each complex quantity into its real and imaginary parts yields a total of ten real-valued key components. For security analysis, considering the IEEE double-precision floating-point accuracy of 10^{-15} for each real-valued component, the total key space is 10^{150}. As shown in Table III, this key space is substantially larger than those reported in recent chaos-based OFDM encryption schemes. Regarding bit error rate performance, unlike some existing schemes that trade off BER for security, the proposed encryption introduces no BER degradation for the legitimate user. This is because all encryption operations, including code-domain interleaving, QAM phase rotation, and time-frequency domain scrambling, are fully invertible and do not alter the Euclidean distance between constellation points in a way that affects the decoder's decision metric. Consequently, the authorized receiver recovers the original signal without any additional error penalty, preserving the inherent BER performance of standard OFDM.

Beyond security and communication effectiveness, the practical deployability of the proposed scheme in industrial settings deserves further attention. In modern industrial wireless systems, OFDM-based physical layers are typically implemented on FPGA-DSP heterogeneous platforms, following standards such as IEEE 802.11ax, 5G NR, or industrial variants like WIA-FA [33]. The proposed CVHNN-based encryption module is purely digital and operates entirely in the baseband domain, requiring no modification to the existing frame structure, cyclic prefix, or synchronization mechanisms. It can be encapsulated as a lightweight intellectual property (IP) core and seamlessly integrated into the existing baseband pipeline at the symbol mapping stage. Moreover, since the CVHNN is utilized as a parameter-fixed chaotic generator, it requires no channel state information or offline training,

TABLE III
COMPARISON BETWEEN THE PROPOSED SCHEME AND REPRESENTATIVE CHAOS-BASED OFDM ENCRYPTION SCHEMES.

Scheme	Encryption domains	Chaotic system	BER degradation (legitimate)	Key space
Zhan et al. [30]	Subcarriers only	Logistic map	$\sim$0.5 dB gain	$\sim 10^9$
Xiao et al. [31]	Subcarrier phase only	Henon map	Not reported	$\sim 10^4$
Lu et al. [32]	Info + frozen bits	Logistic map	0.3 dB loss	2^{128}
This work	Code + modulation + time-frequency	Complex-valued HNN	identical to classic OFDM	$\sim \mathbf{10^{150}}$

which significantly lowers the deployment barrier in resource-constrained industrial edge nodes compared to learning-based or channel-dependent security solutions. Moreover, the FPGA architecture described in the above section employs a fully pipelined computation engine, where each neuron state update is completed within a fixed number of clock cycles. Given that the CVHNN core operates independently of the FFT/IFFT modules and can be scheduled in parallel with them, the encryption process incurs no additional latency beyond the initial chaotic sequence generation. The purely combinational nature of the CVHNN state update allows its throughput to be scaled with the system clock, making it adaptable to various industrial OFDM configurations without fundamental architectural limitations.

VI. CONCLUSION AND OUTLOOK

This paper has investigated a complex-valued Hopfield neural network (CVHNN) and its application in secure OFDM communications. The CVHNN exhibits chaotic dynamics as confirmed by Lyapunov exponent analysis and bifurcation diagrams. An FPGA implementation demonstrates the feasibility of generating complex-valued chaotic sequences in hardware. A secure OFDM scheme based on the CVHNN is proposed, where a single complex chaotic sample directly encrypts a complex OFDM symbol through multi-domain operations. The scheme preserves the BER performance of standard OFDM for legitimate users while providing key sensitivity and resistance to statistical analysis.Beyond the above findings, several aspects of the present work can be further extended. The CVHNN uses only three neurons, which represents the minimal architecture for chaos generation; higher-order networks with more complex topologies may yield hyperchaos and are left for future study. The FPGA implementation, while functional, involves a trade-off between hardware resources and chaos preservation under finite-precision arithmetic, and the current design lacks modular flexibility for rapid reconfiguration across different platforms. The secure OFDM scheme has been validated under AWGN channels with standard parameters; its performance in resource-constrained industrial edge scenarios, particularly the encryption overhead and real-time throughput, requires further characterization. For future work, we plan to explore higher-dimensional CVHNNs to achieve hyperchaos and enhanced security. A more modular and reconfigurable FPGA framework will be developed to facilitate flexible deployment across different precision and resource constraints. Finally, the proposed encryption scheme will be evaluated under practical fading channels and resource-limited edge computing environments to assess its viability for real-world industrial wireless communications.

REFERENCES

[1] H. Bao, M. Xi, H. Tang, X. Zhang, Q. Xu, and B. Bao, "Discrete two-heterogeneous-neuron HNN and chaos-based hardware poisson encoder," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 2, pp. 1862–1871, 2025.

[2] J. Liu, K. Sun, H. Wang, and W. Liu, "An anti-degradation chaotic map and its statistical robustness analysis," *IEEE Transactions on Industrial Electronics*, vol. Early Access, DOI 10.1109/TIE.2025.3581189, pp. 1–10, 2025.

[3] F. Yu, X. Wang, Y. Xiao, Y. He, W. Yao, S. Cai, and J. Jin, "Extreme multistability in discrete memristive neuron maps and implications for dual-field applications," *Integration*, vol. 109, p. 102688, 2026.

[4] S.-Y. Li, H. Yang, and G.-P. Jiang, "Generalized multilevel code-shifted differential chaos shift keying modulation system," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 72, no. 11, pp. 7225–7237, 2025.

[5] G. Yang, C. Wang, Y. Sun, and Q. Deng, "Delayed discrete memristive ring neural network and application in pseudorandom number generator," *IEEE Internet of Things Journal*, vol. 13, no. 6, pp. 11 425–11 435, 2026.

[6] Z. Tang, Y. Zhang, X. Luo, X. Gou, B. Xu, and S. Tang, "n-dimensional hyperchaotic discrete maps with desired positive Lyapunov exponents and its application in secure communication," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 6, pp. 6412–6421, 2025.

[7] G. Yang, C. Wang, Y. Sun, and Q. Deng, "A discrete memristive Hopfield neural network with grid multi-structure/scroll-like attractors," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. Early Access, p. 10.1109/TCAD.2026.3661893, 2026.

[8] G. Yang, C. Wang, Y. Sun, and Q. Deng, "A class of discrete memristive hyperchaotic maps with multicavity multistructure attractors and its application in secure communication," *IEEE Transactions on Industrial Informatics*, vol. Early Access, p. 10.1109/TII.2026.3663427, 2026.

[9] B. Bao, H. Tang, H. Bao, Z. Hua, Q. Xu, and M. Chen, "Simplified discrete two neuron Hofpield neural network and FPGA implementation," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 4, pp. 4105–4115, 2025.

[10] S. Zhang, Y. Li, X. Wang, and Z. Zeng, "Initial offset-boosted coexisting hidden chaos and firing multistability in memristive ring neural network with hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 72, no. 2, pp. 2024–2033, 2025.

[11] T. He, F. Yu, Y. Lin, S. He, W. Yao, S. Cai, and J. Jin, "Multi-scroll Hopfield neural network excited by memristive self-synapses and its application in image encryption," *Chinese Physics B*, vol. 34, no. 12, p. 120506, 2025.

[12] G. Yang, C. Wang, Y. Sun, and Q. Deng, "A discrete memristive heterogeneous Hopfield neural network with multi-penguin-like/silkworm-like attractors and its application in secure communication," *Nonlinear Dynamics*, vol. 114, p. 259, 2026.

[13] Y. Li, J. Zhu, and C. Wang, "Dynamics analysis and FPGA implementation of discrete-time fractional-order memcapacitor-based Hopfield neural network," *Chaos, Solitons & Fractals*, vol. 208, p. 118364, 2026.

[14] X. Peng, C. Li, Y. Zeng, and C.-L. Li, "Adjusting dynamics of hopfield neural network via time-variant stimulus," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 71, no. 7, pp. 3242–3255, 2024.

[15] Y. Zhang, Z. Hua, H. Bao, and H. Huang, "Multi-valued model for generating complex chaos and fractals," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 71, no. 6, pp. 2783–2796, 2024.

[16] S. He, F. Yu, R. Guo, M. Zheng, T. Tang, J. Jin, and C. Wang, "Dynamic analysis and FPGA implementation of a fractional-order memristive hopfield neural network with hidden chaotic dual-wing attractors," *Fractal and Fractional*, vol. 9, no. 9, p. 561, 2025.

[17] Z. Hua, J. Yao, Y. Zhang, and H. Bao, "Two-dimensional coupled complex chaotic map," *IEEE Transactions on Industrial Informatics*, vol. 21, no. 1, pp. 85–95, 2025.

[18] C. Jiang, Y. Yue, F. Zhang, L. Kou, H. Bao, J. Zhang, and H. Liu, "Hardware implementation and information security application of a novel chaotic system with a cubic memristor and complex parameters," *Chaos, Solitons & Fractals*, vol. 196, p. 116379, 2025.
[19] A. C. Fowler, J. D. Gibbon, and M. J. McGuinness, "The complex lorenz equations," *Physica D: Nonlinear Phenomena*, vol. 4, no. 2, pp. 139–163, 1982.
[20] D. Wei, X. Luo, and Y. Qin, "Random shortcuts induce phase synchronization in complex chua systems," *Chinese Physics B*, vol. 18, p. 2184, 2009.
[21] Y. Gu, G. Li, X. Xu, X. Song, and S. Wu, "Multistable dynamics and attractors slef-reproducing in a new hyperbolic complex lü system," *Chaos*, vol. 33, no. 9, p. 093112, 2023.
[22] Z. Hua, Z. Wu, Y. Zhang, H. Bao, and Y. Zhou, "Two-dimensional cyclic chaotic system for noise-reduced OFDM-DCSK communication," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 72, no. 1, pp. 323–336, 2025.
[23] J. Zhao, B. Liu, Y. Mao, R. Ullah, J. Ren, S. Chen, L. Jiang, S. Han, J. Zhang, and J. Shen, "High security OFDM-PON with a physical layer encryption based on 4D-hyperchaos and dimension coordination optimization," *Optics Express*, vol. 28, no. 14, pp. 21 206–21 246, 2020.
[24] G. Yang, C. Wang, and Q. Deng, "A discrete memristive cyclic Hopfield neural network with multi-cavity-like attractors and application in secure communication," *Neural Networks*, vol. 201, p. 108953, 2026.
[25] F. Yu, X. Wang, R. Guo, Z. Ying, Y. He, and Q. Zou, "Discrete neuron models and memristive neural network mapping: A comprehensive review," *Chinese Physics B*, vol. 34, p. 120501, 2025.
[26] C. Wang, Z. Gong, and Q. Deng, "Grid multi-structure hyperchaotic attractors in discrete memristive Hopfield neural network with multi-level logic pulse stimulation," *Nonlinear Dynamics*, vol. 114, p. 598, 2026.
[27] C. Wang, Z. Gong, and Q. Deng, "Discrete bidirectional memristive neural network-based hyperchaotic system and its FPGA implementation," *Neural Networks*, vol. 201, p. 108887, 2026.
[28] F. Yu, X. Kong, W. Yao, J. Zhang, S. Cai, H. Lin, and J. Jin, "Dynamics analysis, synchronization and FPGA implementation of multiscroll Hopfield neural networks with non-polynomial memristor," *Chaos, Solitons, & Fractals*, vol. 179, p. 114440, 2024.
[29] Q. Deng, C. Wang, and G. Yang, "Discrete memristor-based complex-valued chaotic system dynamics and application in dual-image encryption," *Acta Physica Sincia*, vol. 75, no. 01, pp. 31–45, 2026.
[30] L. Zhang, X. Xin, B. Liu, and Y. Wang, "Secure ofdm-pon based on chaos scrambling," *IEEE Photonics Technology Letters*, vol. 23, no. 14, pp. 998–1000, 2011.
[31] Y. Xiao, J. Cao, Z. Wang, C. Long, Y. Liu, and J. He, "Polar coded optical OFDM system with chaotic encryption for physical-layer security," *Optics Communications*, vol. 433, pp. 231–235, 2019.
[32] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," *IEEE Access*, vol. 7, pp. 4380–4390, 2019.
[33] P. Angueira, I. Val, J. Montalban, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 810–838, 2022.

Quanli Deng received the B.S. degree in microelectronics from the School of Physics and Optoelectronics, Xiangtan University, Xiangtan, China, in 2016, the M.S. in information and communication engineering from the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, in 2020 and the Ph.D. degree in computer science and technology from the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, in 2024.

He is currently a Postdoctoral Research Fellow with the College of Computer Science and Electronic Engineering, Hunan University. His research interests include modeling and analysis of neural systems, fundamental theory of nonlinear systems and circuits, and analog implementation of neuromorphic systems.

Chunhua Wang received the M.S. degree in microphysics from Zhengzhou University, Zhengzhou, China, in 1994, and the Ph.D. degree in microelectronics and solid-state electronics from the Beijing University of Technology, Beijing, China, in 2003.

He is currently a Professor with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, where he is a Doctor Tutor and Director of the Advanced Communication Technology Key Laboratory. He has presided more than eight national and provincial projects and authored or coauthored more than 200 papers retrieved by SCI, among which 20 papers were highly cited. His research interests include chaotic circuit, memristor circuit, chaotic encryption, neural networks based on memristor, complex networks, and current-mode circuit.

Dr. Wang is the Director of the Chaos and Nonlinear Circuit Professional Committee of Circuit and System Branch of the China Electronic Society.

Yichuang Sun (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from Dalian Maritime University, Dalian, China, in 1982 and 1985, respectively, and the Ph.D. degree from the University of York, York, U.K., in 1996, all in communications and electronics engineering.

Dr. Sun is currently Professor of Communications and Electronics, Head of Communications and Intelligent Systems Research Group, and Head of Electronic, Communication and Electrical Engineering Division in the School of Engineering and Computer Science of the University of Hertfordshire, UK. He has published over 420 papers and contributed 10 chapters in edited books. He has also published four text and research books: Continuous-Time Active Filter Design (CRC Press, USA, 1999), Design of High Frequency Integrated Analogue Filters (IEE Press, UK, 2002), Wireless Communication Circuits and Systems (IET Press, 2004), and Test and Diagnosis of Analogue, Mixed-signal and RF Integrated Circuits - the Systems on Chip Approach (IET Press, 2008). His research interests are in the areas of wireless and mobile communications, RF and analogue circuits, memristor circuits and systems, and machine learning and neuromorphic computing.

Gang Yang received the B.S. degree in communications engineering and the M.S. degree in artificial intelligence form the Jiangxi University of science and technology, Ganzhou, China, in 2020 and 2023, respectively. He is currently working toward the Ph.D. degree with the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China.

His current research interests include chaotic systems and circuits, memristor neural networks, and memristor systems and circuits.