A lightweight radio frequency fingerprint enhancement and recognition method

1st Dawei Luo
School of Computer Science and Information Security
Guilin University of Electronic Technology
Guilin, China
dived_luo@163.com

2nd Xiaonan Luo
School of Computer Science and Information Security
Guilin University of Electronic Technology
Guilin, China
luoxn@guet.edu.cn

Abstract—**This study addresses the challenges of source identification in increasingly complex electromagnetic environments driven by the rapid development of wireless communication technologies. With the proliferation of Internet of Things (IoT) devices, traditional identification techniques face significant limitations. To overcome these challenges, a Lightweight Radio Frequency Fingerprint Enhancement (LRFFE) framework is proposed, which innovatively integrates a Time–Spatial–Channel (TSC) triple modeling module. The framework performs comprehensive feature extraction from IQ signals through parallel branches of temporal, spatial, and channel modeling. Experiments conducted on the public ORACLE dataset demonstrate that LRFFE achieves an identification accuracy of 99.16% and a single inference time of 0.062 seconds, significantly outperforming existing mainstream methods. Under a 10 dB signal-to-noise ratio (SNR) condition, the proposed model maintains an accuracy of 97.5%, indicating excellent anti-interference capability. Ablation experiments further verify the effectiveness of each component within the TSC module, showing that the collaborative operation of temporal, spatial, and channel modeling branches enables the model to maintain a very low confusion rate even among devices with highly similar features. This research provides an efficient and reliable solution for individual radiation source identification in complex electromagnetic environments and is particularly suitable for resource-constrained embedded deployment scenarios.**

Index Terms—**Deep learning, radio frequency fingerprint recognition, IoT security, wireless network security**

I. Introduction

With the deep integration of fifth-generation mobile communication (5G) and Internet of Things (IoT) technologies, the world is rapidly entering an intelligent era of ubiquitous connectivity. IoT devices are being deployed at an unprecedented rate across critical infrastructures such as smart cities, industrial internet, and vehicular networks, greatly improving operational efficiency and productivity [1]. However, the rapid expansion of device scale and deep penetration into core sectors has also broadened the scope of cybersecurity threats, posing new challenges to the protection of critical information infrastructures. Due to the openness of wireless communication media, IoT devices are highly vulnerable to security threats such as identity spoofing and data theft. Recent incidents, including the Mirai botnet attacks, have revealed the fragility of existing IoT device authentication mechanisms [2].

In current security practice, traditional encryption-based authentication schemes face serious limitations. On one hand, software-defined identifiers such as MAC and IP addresses can be easily tampered with or forged [3]. On the other hand, conventional cryptographic mechanisms such as AES and RSA require complex computation and key management, making them difficult to deploy effectively on resource-constrained IoT terminals [4], [5]. Furthermore, with the advancement of quantum computing, traditional cryptographic systems based on computational complexity are facing fundamental challenges [6]. These limitations have motivated the rapid development of physical-layer security technologies, particularly radio frequency fingerprinting (RFF). RFF identification serves as a new paradigm for device authentication by exploiting inherent hardware imperfections introduced during manufacturing as unique device identifiers. Due to process variations, even wireless devices produced on the same production line exhibit slight differences in radio-frequency front-end components, such as power amplifiers, mixers, and filters. These differences leave distinctive signatures embedded in the transmitted IQ signals [7]–[9]. Compared with software-defined identifiers, RFF features are physically unclonable and resistant to tampering, providing a promising alternative for secure device authentication.

Early RFF identification methods mainly rely on manually designed handcrafted features, such as instantaneous amplitude and phase statistics, spectral characteristics, and wavelet-based features [10]. Although these methods can distinguish devices to some extent, they suffer from low feature extraction efficiency and poor generalization ability. In complex wireless propagation environments, factors such as multipath fading and noise interference severely degrade the stability of RFF features, leading to significant recognition performance loss [11]. Recently, advances in deep learning have brought new opportunities for RFF identification. Convolutional neural network (CNN)-based approaches are capable of learning discriminative representations directly from raw IQ signals, avoiding labor-intensive feature engineering [12]. However, conventional CNN models still face limitations, as their local

This work was supported in part by the National Natural Science Foundation of China under Grant 62495081, in part by the Science and Technology Major Project of Guangxi under Grant AA24263013, and in part by Specific Research Project of Guangxi for Research Bases and Talents under Grant AD23026034. (Corresponding author: Xiaonan Luo.)

receptive fields restrict their ability to capture long-range temporal dependencies.

To address these challenges, a Lightweight Radio Frequency Fingerprint Enhancement (LRFFE) framework is proposed in this study. The framework aims to achieve high identification accuracy while significantly reducing model complexity and inference cost, enabling efficient deployment in resource-constrained environments. Unlike previous approaches that focus on single-dimensional modeling, LRFFE integrates a Time–Spatial–Channel (TSC) triple modeling module. Through parallel temporal, spatial (constellation/2D-CD), and channel modeling branches, the TSC module extracts potential hardware fingerprint features from three complementary dimensions: time structure, spatial constellation distribution, and channel importance. A feature fusion mechanism is then employed to combine the outputs of these branches, generating more discriminative and robust feature representations. This design effectively balances multidimensional information learning and model lightweightness, allowing LRFFE to maintain high accuracy with low computational and memory costs in complex electromagnetic environments.

To evaluate the effectiveness of the proposed method, comprehensive experiments are conducted on the public ORACLE dataset and on simulated IQ data generated using MATLAB Communication Toolbox under various signal-to-noise ratio (SNR) conditions (-10 dB to 20 dB) [13]. Experimental results show that LRFFE achieves 99.16% identification accuracy with only 469,963 parameters and an inference time of 0.062 seconds per sample. Even under a 10 dB SNR condition, the model maintains 97.5% accuracy, demonstrating strong anti-interference capability. Ablation experiments further confirm that the cooperative operation of the temporal, spatial, and channel modeling branches within the TSC module plays a critical role in distinguishing highly similar devices.

In summary, the proposed LRFFE framework provides an efficient, reliable, and easily deployable solution for individual radiation source identification in complex electromagnetic environments through multidimensional collaborative modeling and lightweight network design.

The main contributions of this study are as follows:

- A LRFFE framework is proposed. By structural optimization and parameter constraint, LRFFE achieves 99.16% identification accuracy with only 469,963 parameters, significantly reducing model complexity and computational cost while maintaining high precision. Its lightweight nature enables efficient deployment on resource-constrained embedded and edge devices, supporting real-time radiation source identification in practical wireless communication scenarios.
- A TSC triple feature modeling module is introduced. The TSC module combines temporal structure modeling, spatial constellation feature extraction, and adaptive channel weighting through parallel branches and an attention-based fusion mechanism. This design captures deep-level hardware-induced variations in RF signals. Experimental results demonstrate that TSC effectively enhances feature discriminability, allowing LRFFE to maintain high accuracy and low confusion rates in complex electromagnetic environments.
- The robustness and generalization of LRFFE are validated under noisy conditions. Tests conducted on both real ORACLE data and MATLAB-simulated datasets show that LRFFE achieves 97.5% accuracy at a 10 dB SNR, outperforming mainstream models such as AlexNet, ResNet, MRFE, and ARFNet. Ablation studies further confirm that TSC provides consistent performance gains across different architectures, demonstrating the framework's structural independence and environmental adaptability.

The remainder of this paper is organized as follows. Section II reviews related work on RF fingerprint identification. Section III presents the LRFFE framework and the TSC module design. Section IV describes the experimental setup and evaluation metrics. Section V analyzes the experimental results and discusses the advantages of the proposed approach. Section VI concludes the paper and outlines future research directions.

II. Related Work

In recent years, with the rapid development of Internet of Things (IoT) technologies, physical-layer-based wireless device identification has attracted increasing attention due to its unique advantages. This technique authenticates device identities by analyzing subtle differences in signals caused by inherent hardware characteristics of transmitters, providing a new technical pathway for IoT security. According to the feature extraction strategy, existing studies can be categorized into two main groups: traditional handcrafted-feature methods and modern deep learning-based methods.

In traditional approaches, researchers rely heavily on domain expertise and signal processing techniques to construct handcrafted features. These methods typically extract feature parameters from multiple domains, including the time, frequency, and transform domains, such as power spectral density, phase noise, time-domain statistics, and frequency-domain descriptors [13]–[15]. Commonly used techniques include the Fourier transform, wavelet analysis, short-time energy statistics, and higher-order cumulant analysis. For example, Jin et al. [16] fused time-domain statistical features and frequency-domain spectral features and applied multivariate discriminant analysis combined with a support vector machine, achieving high identification accuracy. Dong et al. [17] utilized time–frequency spectral analysis to capture device-specific differences and proposed an effective specific emitter identification method. Zhang et al. [18] designed a logarithmic power cosine spectrum analysis approach that constructs a seven-dimensional feature vector for precise device classification. Tu et al. [19] extracted multiple statistical features and applied robust principal component analysis for dimensionality reduction, improving classification performance. Notably, Liu et al. [20] converted I/Q signals into spectrum waterfall diagrams and processed them using image recognition networks, maintaining stable performance under low SNR conditions.

Jafar et al. [21] further extended the applicability of spectral features under a wide range of SNR levels.

However, handcrafted-feature methods have inherent limitations. Their feature design depends strongly on expert knowledge and lacks generalization capability. Their performance is also highly sensitive to channel conditions and noise interference. Furthermore, these approaches struggle to scale with the increasing number of devices and the growing complexity of wireless signals. These shortcomings have motivated a shift toward deep learning-based automatic feature extraction methods.

Deep learning enables end-to-end feature learning directly from raw I/Q signals, effectively uncovering deep and discriminative representations and significantly improving identification accuracy [22]. Mainstream models include convolutional neural networks (CNNs), recurrent neural networks (RNNs), generative adversarial networks (GANs), and attention-based architectures. Qing et al. [23] proposed a lightweight CNN model for Zigbee device identification, achieving strong performance; however, its fixed convolutional kernels limit adaptability to multi-dimensional features. Zeng et al. [24] designed a multi-channel convolutional structure based on ResNeXt modules to enhance feature extraction capability, though its feature fusion remained relatively simple. Merchant et al. [25] integrated CNN and RNN architectures to improve recognition under complex channel conditions, but the inherent training inefficiency of RNNs restricted broader application.

Recently, the introduction of attention mechanisms has brought new breakthroughs to RFF-based identification. Zhang et al. [26] developed the ARFNet model, which achieved 95.7% accuracy in ADS-B device identification. However, the limited application of attention modules constrained further improvement. Nousain et al. [27] employed GANs for data augmentation, achieving excellent performance under small-sample conditions, though challenges such as training instability and feature authenticity remain unresolved.

Overall, while existing deep learning models have greatly improved recognition performance, they still suffer from high structural complexity, heavy computational cost, and insufficient feature utilization, making them difficult to deploy in resource-constrained IoT environments. To address these challenges, a LRFFE framework is proposed in this study. The framework introduces an innovative TSC triple feature modeling module that performs multi-dimensional feature extraction and fusion. This design significantly reduces computational overhead while maintaining high recognition performance. Experimental results demonstrate that LRFFE exhibits superior accuracy and robustness under complex electromagnetic conditions, providing an efficient and practical solution for IoT device authentication and physical-layer security.

III. LRFFE Model

A. Model Overview

This section provides a detailed introduction to the proposed LRFFE and Recognition model, whose overall structure is illustrated in Fig1. First, the design concept of the feature extraction module in the LRFFE model is systematically described. Subsequently, the structure and working principle of the TSC, which serves as the core component of this feature extraction module, are analyzed in detail. Through the thorough exploration of implicit features in IQ signals, the robustness and accuracy of wireless device identification are effectively improved.

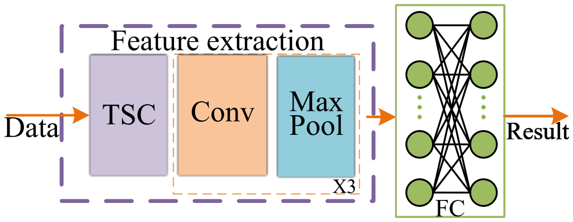

Fig. 1. LRFFE Model Framework

B. Feature extraction module

The primary objective of this module is to extract effective hardware fingerprint features from the raw I/Q signals. The processing procedure is as follows. First, the input signal is passed through an innovative TSC module for initial feature extraction (the detailed structure is described in the following subsection). Subsequently, the extracted features are fed into a network composed of three convolution stacked units for deep processing.

This stacked architecture enables hierarchical learning, allowing the model to capture multi-level feature representations from low-level to high-level abstractions. The max-pooling operation is employed to reduce the dimensionality of feature maps and to enhance the model's translation invariance with respect to feature locations. As a result, the overall robustness and generalization capability of the extracted features are significantly improved. The convolutional layer is mathematically formulated as follows:

$$out(B_i, C_j) = \sum_{k=0}^{C_n-1} W(C_j, k) \otimes input(B_i, k) + bias(C_j) \quad (1)$$

where $\otimes$ denotes the cross-correlation operation, B_i the batch size, C_j the number of channels, and k the length of the signal sequence.

C. TSC Structure

The TSC module, an innovative radio frequency fingerprint enhancement structure proposed in this work, integrates three core modeling components: temporal modeling, spatial modeling, and channel modeling, as shown in Fig2. The temporal modeling is employed to extract sequential fingerprints from signals, while the spatial modeling is dedicated to mining deep constellation diagram features. The channel modeling is designed to generate weights for individual features. All information is ultimately integrated via an attention-based fusion mechanism, aiming to generate enhanced device fingerprints with high discriminability. The design principles of each module are elaborated in the following section.

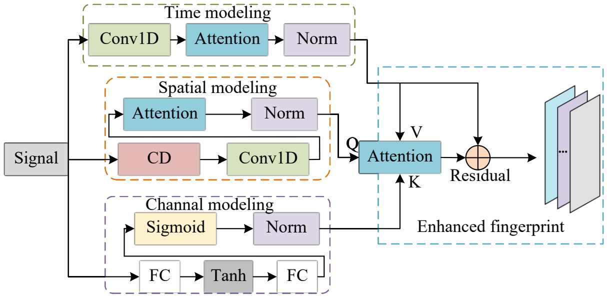

Fig. 2. TSC structure diagram.

1) Time modeling: The primary function of this branch is to extract temporal structural information embedded in the I/Q data. The processing flow is as follows: the input signal is first passed through a convolutional module to capture key temporal features. The extracted features are then fed into an attention module to model long-term temporal dependencies, followed by a layer normalization operation to stabilize the learning process and further enhance temporal representation capability.

Experimental results indicate that although one-dimensional convolution can effectively capture basic temporal features, its expressive power remains limited when dealing with complex hardware fingerprints from multiple sources. This limitation arises because the sub-features extracted by different convolutional channels vary significantly in discriminative strength, and the contribution of different spatial regions within the feature map to device identity is highly uneven. Therefore, additional spatial and channel modeling branches are introduced to compensate for the limitations of single-branch temporal modeling.

2) Spatial modeling: The core objective of the spatial modeling branch is to extract two-dimensional constellation diagram (CD) features from the received I/Q signals to improve the discriminative ability of the overall representation. In implementation, the input I/Q signal is first transformed into its constellation representation, allowing the periodic variations of subcarriers in amplitude and phase distributions to be analyzed. This transformation amplifies the implicit patterns caused by hardware imperfections such as power amplifier nonlinearity, I/Q imbalance, and sampling deviation, making subtle device-specific differences more prominent and easier to model. The generated sequence is then processed by a temporal attention module to capture its time-domain dependencies. Through this process, the spatial modeling branch significantly enhances the distinctiveness and robustness of the final feature representation.

3) Channel modeling: The main function of the channel modeling branch is to assign adaptive dynamic weights to different channels, thereby selecting and enhancing the most discriminative channel features in the current signal. Structurally, this branch consists of two fully connected layers and two nonlinear activation functions, designed to balance feature dimension compression and distribution normalization. Its purpose is to improve model training stability and feature generalization capability.

The specific process is as follows: first, the input features are mapped nonlinearly using a hyperbolic tangent (Tanh) activation function. The Tanh output is constrained within the range [-1, 1], exhibiting zero-centered symmetry, which helps alleviate gradient vanishing issues and strengthens network expressiveness. Next, the Sigmoid function maps the features into the [0, 1] range to generate normalized channel weights, ensuring interpretability and numerical stability. Finally, a Layer Normalization (LayerNorm) operation is applied to standardize the output, enhancing both local consistency and global coherence of the feature representation.

The fully connected layer computation is expressed as follows:

$$y = \sigma(W_2 \cdot \tanh(W_1 \cdot x + b_1) + b_2) \tag{2}$$

where x denotes the input features, W_1 and W_2 are defined as the weight matrices of the first and second layers, respectively, b_1 and b_2 as the corresponding bias terms, and Tanh as the hyperbolic tangent function.

4) Enhanced fingerprint: The TSC module employs an attention mechanism to integrate the outputs from the temporal, FFT, and channel modeling branches for generating enhanced fingerprint features. Within this mechanism, the spatial modeling output is utilized as the Query (Q), the channel modeling output as the Key (K), and the temporal modeling output as the Value (V). The attention is computed using the following formula:

$$Attention(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \tag{3}$$

where T denotes the transpose operation, and d_k represents the length of the input signal.

Additionally, a residual connection utilizing the V path is introduced to mitigate the issues of vanishing or exploding gradients, as V retains the original temporal information. The final enhanced fingerprint is thus represented as:

$$F_{enhanced} = V + Attention(Q, K, V) \tag{4}$$

IV. Experimental Setup

A. Data Set Information

To evaluate the performance of the proposed LRFFE model, experiments were conducted using both real-world and simulated data. For the real-world data, the publicly available ORACLE dataset, specifically designed for radio frequency fingerprint identification, was utilized. This dataset was collected in an open area with minimal reflections to reduce environmental interference. The transmission system consisted of 16 X310 USRP SDR devices with highly consistent hardware design as transmitters, and a B210 radio as the receiver. These transmitters, sharing identical hardware, communication protocols, and network identifiers, exhibited minimal hardware impairment variations, thereby presenting significant challenges for the identification task. The devices transmitted data frames compliant with the IEEE 802.11a standard, containing random payloads. To further validate the model's generalization capability, simulated IQ fingerprint data were generated using the MATLAB Communications Toolbox. Different phase and amplitude errors were introduced to emulate hardware impairments. The data were generated over a signal-to-noise ratio range from -10 dB to 20 dB to assess the model's classification robustness under various noise conditions. Finally, the combined dataset was partitioned into training, testing, and validation sets in an 8:1:1 ratio.

B. Experimental Environment

The hardware platform for this experiment was configured with an Intel i5-12600KF CPU and an NVIDIA RTX 4060 Ti GPU. This configuration provided sufficient computational capacity for both model training and inference. On the software side, the experiments were conducted using the PyTorch deep learning framework, which offered flexible and efficient tools for model construction, training, and data processing.

C. Performance Index

To systematically evaluate the performance of the LRFFE model for device RF fingerprint identification, four metrics were adopted: Accuracy, Precision, Recall, and F1-score. Accuracy is utilized to measure the overall correctness of the classification. Precision reflects the accuracy of positive predictions, while Recall indicates the model's ability to identify all true positive instances. The F1-score, serving as the harmonic mean of Precision and Recall, is employed to assess the overall performance on imbalanced datasets. Regarding the experimental setup, the batch size was fixed at 64 and the sequence length at 512. The initial learning rate was set to 0.001, with a step decay strategy applied where the learning rate was reduced by 50% every 10 epochs. This configuration was implemented to ensure the reproducibility of the experiments and the comparability of the results.

V. Experimental Results

In this section, a comprehensive comparative analysis is conducted between the proposed LRFFE model and four current mainstream RF fingerprint classification models: AlexNet-1D [28], MRFE [29], ResNet [30], and ARFNet [31]. AlexNet-1D, an architecture specifically adapted for one-dimensional RF signals, enhances feature representation and mitigates overfitting through increased network depth, a greater number of convolutional kernels, and the integration of ReLU activation functions with Dropout regularization. The MRFE model employs a multi-dimensional decomposition strategy, where multi-dimensional RF features are first extracted from the original I/Q signals. These features are then fused using an attention mechanism to generate a more discriminative device fingerprint representation. ResNet addresses the vanishing gradient problem in deep networks by introducing residual modules with skip connections, thereby enhancing the capability to learn complex RF patterns. ARFNet, designed for device identification using I/Q signals, is primarily composed of multiple convolutional, pooling, and fully-connected layers. The convolutional layers are utilized for the automatic extraction of RF feature fingerprints, while classification is ultimately performed by the fully-connected layers in conjunction with a Softmax function.

A. Analysis of Training Results

This section analyzes the training results of the LRFFE model and other baseline models on the ORACLE dataset. For a comprehensive performance comparison, several metrics were evaluated, including the number of parameters, inference time, number of layers, and convergence epoch, as summarized in Table I. The LRFFE model contains only 469,963 parameters, demonstrating a significant advantage over the baseline models. This lightweight design indicates higher efficiency, with reduced memory and computational requirements, making it suitable for resource-constrained hardware environments. Furthermore, the inference time of the LRFFE model is merely 0.062 seconds, which is considerably shorter than that of other models, highlighting its superior computational efficiency during inference and suitability for real-time applications. Additionally, the LRFFE model converges in just 9 epochs, enabling faster training and reduced computational cost. This rapid convergence also reflects the high efficiency of its optimization design. During training and evaluation, the LRFFE model achieved the highest accuracy of 99.3%, while the MRFE (Multi-Resolution Feature Extraction) model also reached an accuracy of 99%. The superior performance of LRFFE can be attributed to its innovative interactive attention mechanism, which effectively captures and utilizes complex feature relationships in the input data. The training results of LRFFE and the baseline models, illustrated in Fig. ref fig:3, further emphasize its outstanding performance by comparing the training progress within the first 20 epochs.

This section systematically evaluates the comprehensive performance of the LRFFE model and various baseline models on the ORACLE dataset. As summarized in Table I, key metrics—including parameter count, inference time, number of layers, and accuracy—were analyzed. The LRFFE model is shown to achieve optimal performance with only 469,963 parameters, demonstrating significantly superior parameter efficiency compared to other models. This compact architectural design not only substantially reduces memory usage and computational overhead but also makes the model particularly suitable for deployment in resource-constrained embedded platforms. In terms of inference efficiency, a single forward pass of the LRFFE model requires merely 0.062 seconds, which is considerably faster than competing models. This result highlights its exceptional real-time inference capability and suitability for industrial applications with strict low-latency requirements.

In terms of identification performance, the highest accuracy of 99.16% was achieved by the LRFFE model, while MRFE also attained an excellent result of 98.38%. This performance advantage is primarily attributed to the innovative TSC module

TABLE I
MODEL PERFORMANCE COMPARISON

Modal	LRFFE	AlexNet	MRFE	ResNet	ARFNet
Parameter	469963	654752	871046	743823	547892
Layer count	5	10	14	10	15
Infrence tiem	0.062	0.081	0.092	0.089	0.076
Accuracy	99.16%	96.52%	98.38%	96.88%	95.12%

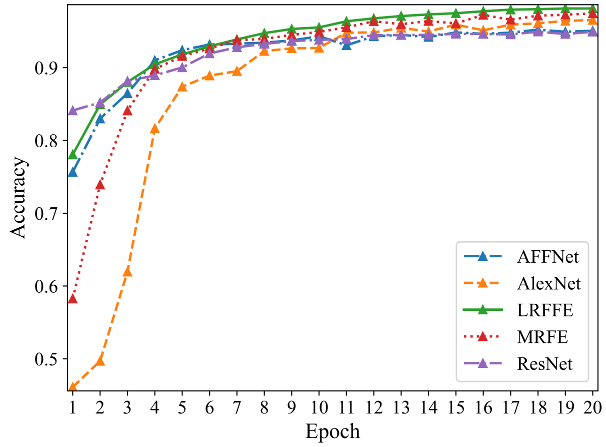

Fig. 3. Training status of LRFFE and baseline model.

in LRFFE, where subtle hardware fingerprint features in RF signals are collaboratively extracted through parallel temporal, spatial, and channel modeling paths. The superiority of LRFFE is further demonstrated by the training curves shown in Fig.3. During the first 20 training epochs, consistently faster convergence speed and higher final accuracy were maintained compared to other baseline models, indicating stable and efficient learning characteristics.

To comprehensively evaluate the performance of the LRFFE model against other baseline models, a comparative test was conducted under different SNR conditions. IQ fingerprint data with SNR ranging from -10 dB to 20 dB were generated using the MATLAB Communications Toolbox. The data incorporated 16 distinct levels of both phase and amplitude errors to simulate hardware impairments. This SNR range covers a wide variety of scenarios, enabling an effective assessment of the models' classification capability in noisy environments. The performance of each model across SNR levels is illustrated in fig4. Considerable differences in accuracy were observed among the models under varying SNR conditions. The LRFFE model achieved higher accuracy than other baseline models when the SNR exceeded 2 dB. At 10 dB, an accuracy of 97.5% was attained by LRFFE, surpassing all other models and demonstrating its strong robustness and superior performance in low-to-medium SNR environments. In contrast, AlexNet and ARFNet exhibited slower accuracy improvement under low SNR conditions, suggesting a relatively weaker capability in feature extraction and signal classification in highly noisy environments.

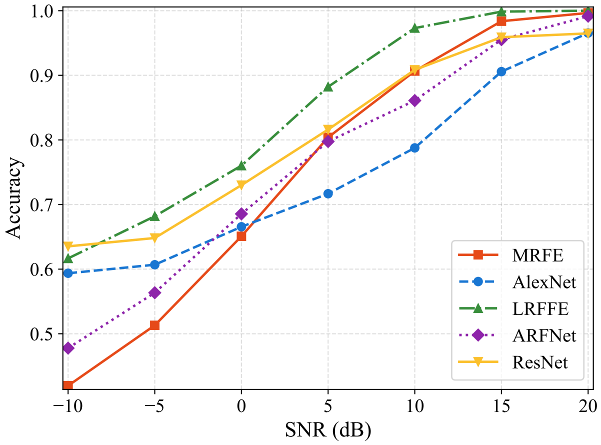

Fig. 4. Model accuracy under different SNRs.

Overall, high accuracy is maintained by the LRFFE model across a wide SNR range. Its exceptional performance under low SNR conditions demonstrates advanced capability in handling noise interference and signal classification. This advantage is attributed to the parallel temporal, spatial, and channel modeling mechanism incorporated in LRFFE, which effectively captures and utilizes complex features in signals, thereby sustaining high classification accuracy under noisy conditions. These characteristics make LRFFE particularly valuable for practical applications, especially in scenarios with unstable communication channels or significant noise interference.

B. Confusion Matrix Analysis

The confusion matrix clearly illustrates the fine-grained identification performance of the LRFFE model across 16 device classes in the ORACLE dataset. As shown in Fig. 5, the dominant values along the main diagonal indicate that accurate classification was achieved for most devices, with only a limited number of misclassifications observed. These misclassifications were primarily concentrated among a few specific device classes, suggesting that highly similar RF characteristics may be shared by these devices, thereby presenting challenges to classification boundaries. Overall, through its innovative parallel temporal, spatial, and channel modeling mechanism, complex features in signals are effectively captured and utilized by the LRFFE model, enabling the extraction of more discriminative RF fingerprints. This mechanism significantly enhances the perception of subtle feature differences, allowing a very low confusion rate to be maintained even among devices with highly similar characteristics and demonstrating exceptional inter-class differentiation capability.

C. Ablation Experiment Analysis

1) Influence of Signal Length: To investigate the impact of IQ data length on identification performance, a systematic analysis was conducted on model performance under four different sequence lengths: 64, 128, 256, and 512, as shown

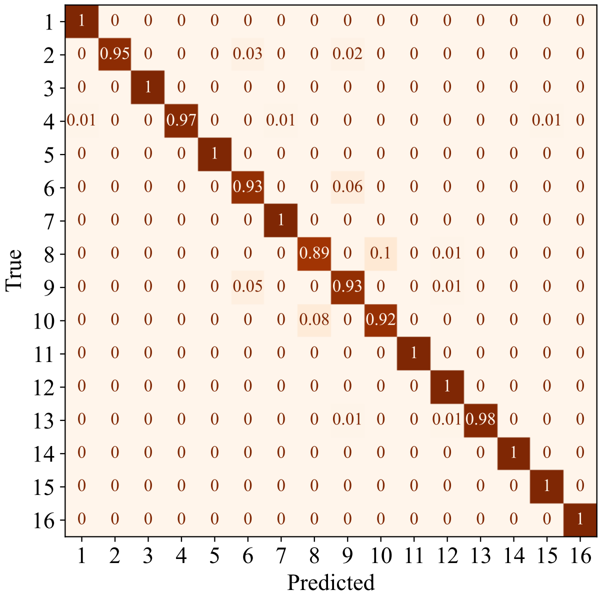

Fig. 5. Caption

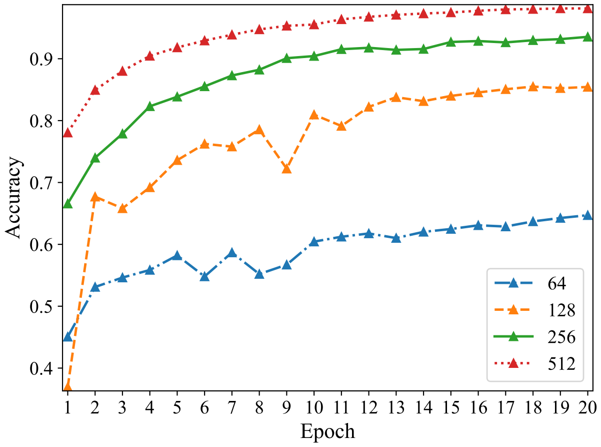

Fig. 6. Model training with different signal lengths.

in Fig.6. The experimental results indicate that the highest identification accuracy was achieved when the sequence length was set to 512. This phenomenon can be attributed to the balance between sequence length and feature completeness. Shorter sequences, such as 64 or 128, contain limited RF fingerprint features, which are insufficient to support adequate discrimination by the model. Although longer sequences provide richer feature information, they significantly increase computational complexity and training costs. Furthermore, the dataset construction strategy directly influences the selection of sequence length. A balance must be sought between feature information content and computational efficiency, ensuring that sequences are sufficiently long to capture device fingerprint characteristics while avoiding the training efficiency degradation caused by excessive length.

TABLE II
EXPERIMENTAL COMPARISON RESULTS OF TSC AND CONV

Method	Model	Accuracy	Precision	Recall	F1 score
TSC	LRFFE	99.16%	99.01%	99.21%	99.16%
	Alexnet	96.64%	96.65%	96.64%	96.64%
	ResNet	96.88%	96.89%	96.88%	96.88%
Conv	LRFFE	96.91%	96.88%	96.96%	96.91%
	Alexnet	94.92%	94.93%	94.92%	94.92%
	ResNet	93.86%	93.86%	93.86%	93.85%

2) Impact of LRFFE: Based on the ablation study results presented in Table II, the LRFFE model demonstrates exceptional performance in RF fingerprint feature extraction. When integrated with the TSC architecture, an accuracy of 99.16% is achieved by LRFFE, significantly surpassing 96.64% of AlexNet and 96.88% of ResNet. Under the conventional convolutional architecture, superior performance is also maintained by LRFFE (96.91%), exceeding 94.92% of AlexNet and 93.86% of ResNet by 1.99 and 3.05 percentage points, respectively, confirming its architectural independence. Of particular note is that a notable improvement of 2.25 percentage points is observed when the LRFFE is combined with the TSC module, validating the effectiveness of TSC in extracting discriminative time-frequency domain features. These results conclusively demonstrate that highly discriminative RFF features can be extracted by the LRFFE model, while its synergistic interaction with the TSC module further enhances feature representation capability. This approach provides an effective solution for lightweight RF fingerprint identification.

VI. Conclusion

This paper addresses the challenges of emitter identification in complex electromagnetic environments by investigating deep learning-based methods for fine-grained radio frequency fingerprint extraction. A LRFFE recognition framework is proposed, whose core contribution lies in the novel design of a TSC triple modeling module. Through parallel temporal, spatial, and channel modeling branches, discriminative multi-dimensional features in I/Q signals are collaboratively explored, enabling the generation of highly robust device fingerprints. Experimental results on the public ORACLE dataset demonstrate that the proposed LRFFE framework achieves outstanding recognition performance while maintaining an extremely compact structure. Specifically, an accuracy of 99.16% is attained with an inference time of only 0.062 seconds, significantly outperforming several mainstream baseline models and confirming its high efficiency. Moreover, the model maintains 97.5% accuracy even at a low SNR of 10 dB, highlighting its strong anti-interference capability and practical applicability. In summary, LRFFE provides an efficient and reliable solution for emitter identification on resource-constrained embedded platforms.

Despite the promising performance of the LRFFE model, several limitations should be noted. The training and validation are primarily based on the ORACLE dataset collected in specific scenarios and MATLAB-generated simulated data. Although phase and amplitude errors are introduced in simulation, real-world electromagnetic environments are more dynamic and complex, involving diverse unknown modulation types, channel fading, and transient interference. The generalization capability of the model to broader device models and dynamic scenarios requires further verification. Therefore, future work will include the collection of data under more communication protocols and extreme environmental conditions to evaluate and enhance the model's generalizability.

References

[1] P. Mishra and G. Singh, "Internet of vehicles for sustainable smart cities: Opportunities, issues, and challenges," *Smart Cities*, vol. 8, no. 3, p. 93, 2025.

[2] P. K. Swain, L. M. Pattnaik, and S. Satpathy, "Iot applications and cyber threats: Mitigation strategies for a secure future," in *Explainable IoT Applications: A Demystification*. Springer, 2025, pp. 403–428.

[3] N. Anand, M. Saifulla, R. B. Ponnuru, G. R. Alavalapati, R. Patan, and A. H. Gandomi, "Securing software defined networks: A comprehensive analysis of approaches, applications, and future strategies against dos attacks," *IEEE Access*, 2024.

[4] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE access*, vol. 9, pp. 28 177–28 193, 2021.

[5] A. S. D. Alluhaidan and P. Prabu, "End-to-end encryption in resource-constrained iot device," *IEEE access*, vol. 11, pp. 70 040–70 051, 2023.

[6] S. R. Kandula, "Breaking traditional encryption: Quantum computing risks to web and mobile applications," *International Journal of Advanced Research in Engineering and Technology (IJARET) Volume*, vol. 16, pp. 329–342, 2025.

[7] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3974–3987, 2021.

[8] W. Wang and L. Gan, "Radio frequency fingerprinting improved by statistical noise reduction," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 3, pp. 1444–1452, 2022.

[9] X. Huan, Y. Hao, K. Miao, H. He, and H. Hu, "Carrier frequency offset in internet of things radio frequency fingerprint identification: An experimental review," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7359–7373, 2023.

[10] M. Priyadarshini, M. Bajaj, L. Prokop, and M. Berhanu, "Perception of power quality disturbances using fourier, short-time fourier, continuous and discrete wavelet transforms," *scientific reports*, vol. 14, no. 1, p. 3443, 2024.

[11] J. Zhang, R. Woods, M. Sandell, M. Valkama, A. Marshall, and J. Cavallaro, "Radio frequency fingerprint identification for narrowband systems, modelling and classification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3974–3987, 2021.

[12] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "Oracle: Optimized radio classification through convolutional neural networks," in *IEEE INFOCOM 2019-IEEE conference on computer communications*. IEEE, 2019, pp. 370–378.

[13] L. Xie, L. Peng, J. Zhang, and A. Hu, "Radio frequency fingerprint identification for internet of things: A survey," *Security and Safety*, vol. 3, p. 2023022, 2024.

[14] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, vol. 61, no. 10, pp. 110–115, 2023.

[15] S. Abbas, M. Abu Talib, Q. Nasir, S. Idhis, M. Alaboudi, and A. Mohamed, "Radio frequency fingerprinting techniques for device identification: a survey," *International Journal of Information Security*, vol. 23, no. 2, pp. 1389–1427, 2024.

[16] Y. Jin, M. Wei, and Q. Li, "An rf fingerprint extraction method based on time-frequency domain feature fusion," in *Journal of Physics: Conference Series*, vol. 2424, no. 1. IOP Publishing, 2023, p. 012030.

[17] W. Dong, Y. Wang, G. Sun, and M. Xing, "A specific emitter identification method based on time-frequency feature extraction," in *IGARSS 2023-2023 IEEE International Geoscience and Remote Sensing Symposium*. IEEE, 2023, pp. 6302–6305.

[18] J. Zhang, Q. Wang, X. Guo, X. Zheng, and D. Liu, "Radio frequency fingerprint identification based on logarithmic power cosine spectrum," *IEEE Access*, vol. 10, pp. 79 165–79 179, 2022.

[19] Y. Tu, Z. Zhang, Y. Li, C. Wang, and Y. Xiao, "Research on the internet of things device recognition based on rf-fingerprinting," *Ieee Access*, vol. 7, pp. 37 426–37 431, 2019.

[20] D. Liu, M. Wang, and H. Wang, "Rf fingerprint recognition based on spectrum waterfall diagram," in *2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*. IEEE, 2021, pp. 613–616.

[21] N. Jafar, A. Paeiz, and A. Farzaneh, "Automatic modulation classification using modulation fingerprint extraction," *Journal of Systems Engineering and Electronics*, vol. 32, no. 4, pp. 799–810, 2021.

[22] C. Tang, T. Yan, and Y. An, "Radio frequency fingerprint recognition based on deep learning," in *2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*. IEEE, 2021, pp. 708–711.

[23] G. Qing, H. Wang, and T. Zhang, "Radio frequency fingerprinting identification for zigbee via lightweight cnn," *Physical Communication*, vol. 44, p. 101250, 2021.

[24] Y. Zeng, Y. Gong, J. Liu, S. Lin, Z. Han, R. Cao, K. Huang, and K. B. Letaief, "Multi-channel attentive feature fusion for radio frequency fingerprinting," *IEEE Transactions on Wireless Communications*, vol. 23, no. 5, pp. 4243–4254, 2023.

[25] K. Merchant and B. Nousain, "Enhanced rf fingerprinting for iot devices with recurrent neural networks," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 590–597.

[26] W. Zhang, W. Zhao, X. Tan, L. Shao, and C. Ran, "Adaptive rf fingerprints fusion via dual attention convolutions," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25 181–25 195, 2022.

[27] K. Merchant and B. Nousain, "Securing iot rf fingerprinting systems with generative adversarial networks," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 584–589.

[28] K. Merchant, S. Revay, G. Stantchev, and B. Nousain, "Deep learning for rf device fingerprinting in cognitive communication networks," *IEEE journal of selected topics in signal processing*, vol. 12, no. 1, pp. 160–167, 2018.

[29] Q. Lu, Z. Yang, H. Zhang, F. Chen, and H. Xian, "Mrfe: A deep-learning-based multidimensional radio frequency fingerprinting enhancement approach for iot device identification," *IEEE Internet of Things Journal*, vol. 11, no. 18, pp. 30 442–30 454, 2024.

[30] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[31] W. Zhang, W. Zhao, X. Tan, L. Shao, and C. Ran, "Adaptive rf fingerprints fusion via dual attention convolutions," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25 181–25 195, 2022.