SAVUNMA BİLİMLERİ DERGİSİ
The Journal of Defense Sciences

https://dergipark.org.tr/tr/pub/khosbd

Deep Learning for Specific Emitter Identification in Modern Electronic Warfare: From Static Models to Cognitive Adaptation

Modern Elektronik Harpte Özgün Yayıcı Tanımlama İçin Derin Öğrenme: Statik Modellerden Bilişsel Adaptasyona

Mert KARAHAN [1*] Onur BATTAL [2]

[1,2] *National Defence University, Turkish Military Academy, Electronics and Communication Engineering Department, Ankara, Türkiye*

Makale Bilgisi

Derleme makalesi
Başvuru: 27.02.2026
Düzeltme: 19.03.2026
Kabul: 17.04.2026

Keywords

Specific Emitter Identification (SEI)
Electronic Warfare
Deep Learning
Radio Frequency Fingerprinting (RFF)

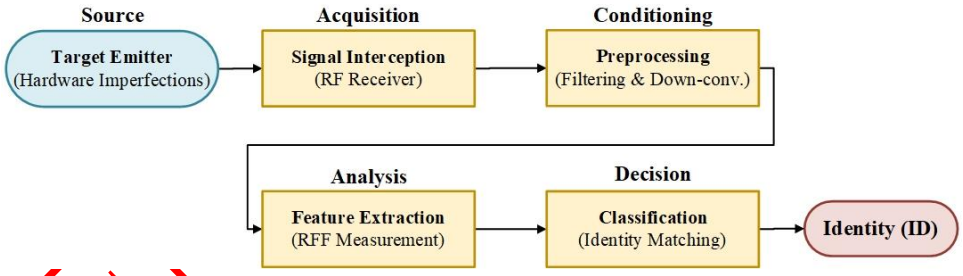
Anahtar Kelimeler

Özgün Yayıcı Tanımlama (SEI)
Elektronik Harp
Derin Öğrenme
Radyo Frekansı Parmak İzi (RFF)

Highlights

This study comprehensively examines the evolution of Specific Emitter Identification from conventional static models to self-healing cognitive architectures, proposing multimodal feature fusion techniques such as Variational Mode Decomposition and bispectral analysis to bridge the reliability gap under dynamic field conditions. By integrating Extreme Value Theory for autonomous open-set recognition and emphasizing adaptive strategies like adversarial training and meta-learning, the research addresses critical vulnerabilities including data scarcity and adversarial attacks, providing a robust framework for next-generation electronic warfare systems.

Graphical Abstract



Abstract

In modern Electronic Warfare (EW), identifying hostile elements via hardware-induced Radio Frequency Fingerprints (RFFs) is known as Specific Emitter Identification (SEI). This study examines the evolution of SEI from manual extraction to data-driven Deep Learning (DL). While static architectures like ResNets achieve over 96% accuracy in controlled laboratories, their reliability plummets to ~50% under real-world conditions involving data scarcity (few-shot), unknown threats (open-set), and adversarial attacks. To bridge this gap, the study highlights multimodal feature fusion techniques, specifically Variational Mode Decomposition (VMD) and bispectral analysis. Furthermore, it proposes integrating Extreme Value Theory (EVT) for open-set recognition alongside meta-learning strategies, enabling systems to autonomously identify threats and update dynamically. Consequently, transitioning from static models to a self-healing, adaptive cognitive architecture is imperative for sustaining EW superiority.

Özet

Modern Elektronik Harp (EH) ortamında, donanım kaynaklı Radyo Frekans Parmak İzleri (RFF) kullanılarak düşman unsurların bireysel kimlik düzeyinde tanınması, Özgün Yayıcı Tanımlama (SEI) olarak bilinmektedir. Bu çalışma, SEI'nin manuel özellik çıkarımından veri güdümlü Derin Öğrenme yaklaşımlarına evrimini incelemektedir. ResNet gibi statik mimariler kontrollü laboratuvarlarda 96%'nın üzerinde doğruluk elde ederken; veri kıtlığı, bilinmeyen tehditler ve çekişmeli saldırılar içeren gerçek saha koşullarında güvenilirlikleri 50% seviyelerine düşmektedir. Bu uçurumu kapatmak için, Varyasyonel Mod Ayrışımı ve bispektral analiz gibi çok modlu özellik füzyon teknikleri vurgulanmaktadır. Ayrıca sistemlerin tehditleri otonom olarak tanımasını ve güncellenmesini sağlamak amacıyla, Uç Değer Teorisi ile meta-öğrenme stratejilerinin entegrasyonu önerilmektedir. Sonuç olarak, EH üstünlüğünün sürdürülebilmesi için statik modellerden kendi kendini onaran, adaptif bilişsel bir mimariye geçiş zorunludur.

*Corresponding author, e-mail: mert.karahan@msu.edu.tr

DOI:10.17134/khosbd.1898855

Elektronik/Online ISSN: 2148-1776
Basılı/Printed ISSN: 1303-6831

1. INTRODUCTION

The modern battlefield has transformed into an environment where the electromagnetic spectrum is becoming increasingly complex, signal density is rising, and threats are becoming dynamic [1], [2]. In this chaotic environment, Cognitive Electronic Warfare (EW) systems must identify hostile elements not merely by their type but at the individual identity level to ensure situational awareness and determine countermeasures instantaneously [3]. Specific Emitter Identification (SEI) fulfills this critical need by distinguishing even emitters that come off the same production line and possess the same model parameters, utilizing Radio Frequency Fingerprints (RFFs) originating from hardware imperfections [4,5]. The detection of these features, which arise from the unique imperfections (micro-differences) of the emitter hardware, is of vital importance in terms of enhancing battlefield situational awareness and achieving tactical superiority [6,7].

To provide a deeper understanding, the foundation of SEI lies in the physical hardware imperfections introduced during the manufacturing process of electronic components. These unintentional micro-differences, such as oscillator phase noise, power amplifier non-linearities, modulator imbalances, and digital-to-analog converter variations, manifest as unique RFFs embedded within the transmitted signal. A conventional SEI system typically follows a four-stage standard pipeline, as illustrated in the general block diagram in Figure 1(a): (1) signal acquisition, which involves intercepting the raw electromagnetic signal; (2) preprocessing, performed to mitigate channel noise and prepare the data; (3) feature extraction, where these distinctive RFF features are obtained; and (4) classification, which utilizes an algorithm to match the extracted fingerprint against a database of known emitter identities.

The SEI discipline has a deep-rooted history dating back to early EW applications, where radar operators attempted to visually distinguish signal characteristics on analog oscilloscopes. For years, SEI studies have relied on the extraction of classical parameters such as pulse width (PW), pulse repetition interval (PRI), and radio frequency via manual analysis [4,8,9]. However, adaptive waveforms and complex electromagnetic interference in modern EW scenarios have rendered these traditional methods, which depend on expert experience, cumbersome and inadequate [1,10]. More importantly, the adversary in the field is no longer static; the presence of previously unseen emitters (open-set recognition) and hostile attempts to deceive systems exceed the limitations of classical approaches [11,12].

In response to these bottlenecks of traditional methods, literature has undergone a mandatory and sharp transition from manual feature extraction to data-driven Deep Learning (DL) architectures [13]. Structures such as Convolutional Neural Networks (CNNs) [14], Deep Residual Networks (ResNets) [15] and Transformers [3] have increased identification performance by automatically learning complex features from raw signals. Nevertheless, standard DL models alone are not a solution to the practical challenges of Cognitive EW. These

models typically require large amounts of labeled data; whereas, acquiring adversary signals in the battlefield is difficult and costly, leading to the few-shot learning problem [8,16,17]. Furthermore, DL-based systems can remain vulnerable to adversarial attacks conducted with virtually imperceptible signal distortions [18,19].

On the other hand, the modern EW battlefield has expanded beyond isolated systems to include Internet of Things (IoT) networks where civilian and military infrastructures intertwine. Recent studies emphasize the critical role of SEI in IoT security, drawing attention to the issue of the clonability of RFFs in low-cost devices [5]. Similarly, the complexity and geolocation requirements of modern emitter detection systems have been extensively detailed in the literature [2]. Moreover, in situations where aggregating data on a centralized server poses a tactical security risk, distributed SEI architectures based on federated learning offer a new security paradigm by allowing model training without sharing raw data [4].

In this context, the theoretical framework of this study is built upon the imperative transition from conventional static models to a fully adaptive Cognitive SEI architecture, as comprehensively illustrated in Figure 1. While Figure 1(a) outlines the standard SEI pipeline, Figure 1(b) delineates the scope of the proposed cognitive framework designed to address the critical vulnerabilities of modern EW systems. Traditional static DL models suffer from operational blindness under dynamic field conditions—specifically struggling with limited labeled data (few-shot learning), the emergence of unknown threats (open-set recognition), and adversarial perturbations. To address this theoretical and practical gap, the proposed architecture is structured upon four main dynamic stages. The process begins with the collection of raw In-phase and Quadrature (I/Q) data, followed by a preprocessing stage where signal quality is enhanced using Variational Mode Decomposition (VMD) and bispectral analysis [7,20]. The resulting cleaned data are processed through multimodal deep networks [3] and mapped into a latent feature space. Finally, an adaptive decision mechanism incorporating Extreme Value Theory (EVT) autonomously classifies the signals and recognizes unknown emitters, triggering a meta-learning-based cognitive feedback loop. Ultimately, this loop ensures that the system continuously updates its knowledge via continual learning, thereby bridging the reliability gap between theoretical laboratory accuracy and real-world EW resilience.

2. DEEP ARCHITECTURES FOR COGNITIVE SEI AND MODERN APPROACHES IN FEATURE EXTRACTION

The inadequacy of traditional SEI methods in the face of the complexity of the modern EW environment has directed researchers from hand-crafted features to DL architectures that automatically extract hidden patterns within the data. However, not every DL architecture is suitable for every problem; the type of signal (steady-state or transient), noise level, and data size are critical factors determining the choice of architecture. In this section, the dominant DL approaches in literature are comparatively examined in the context of the problems they solve, computational costs, and performance constraints.

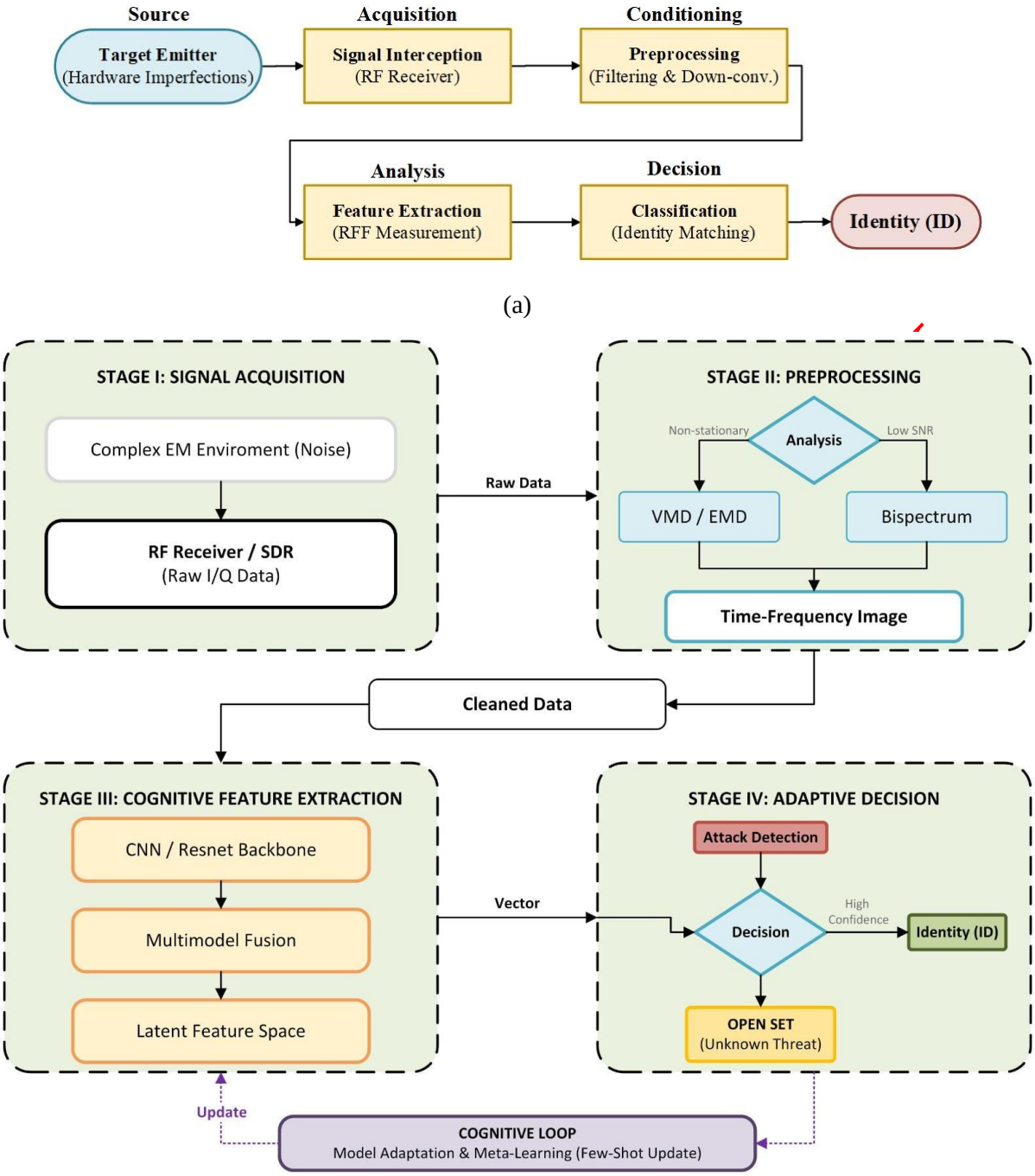


Figure 1: Overview of SEI systems: (a) The conventional four-stage SEI pipeline, and (b) the proposed Cognitive SEI system architecture.

2.1 Spectral Stability and the Curse of Dimensionality: CNN and Bispectral Analysis

Traditional approaches generally relied on classical parameters such as pulse width (PW) and pulse repetition interval (PRI); however, these methods fail in complex environments [4,8,9]. Focusing on the impact of signal quality, prior research [15] proved that noise and power spectrum distortions directly reduce the success of DL models [21]. Therefore, in SEI studies, especially under low Signal-to-Noise Ratio (SNR) conditions, there is a need for methods that preserve not only the amplitude information of the signal but also its phase information. In this

context, bispectral Analysis, which utilizes higher-order statistics, stands out with its ability to suppress Gaussian noise and preserve nonlinear phase relationships within the signal [7,22]. This fundamental flow, where the raw signal is processed and classified, is illustrated in Figure 2.

Studies in the literature demonstrate that hybrid structures, in which images obtained from the bispectrum are processed with CNNs, offer more robust discriminative features compared to models processing raw signals. However, bispectrum computation inherently generates high-dimensional data. This situation introduces the "curse of dimensionality" problem, increasing the computational load and potentially causing the model to overfit. To overcome this problem, recent studies subject the bispectral data to a supervised dimensionality reduction process first, rather than feeding it directly into the network, and then classify this compressed data with CNNs [14]. Furthermore, in scenarios where labeled data is scarce, bispectrum-based feature extraction has also proven its effectiveness in semi-supervised learning scenarios by being combined with Generative Adversarial Networks (GAN/CGAN) [22-24].

2.2. Spectral Stability and the Curse of Dimensionality: CNN and Bispectral Analysis

As deep learning architectures deepen and the number of layers increases, degradation in the network's learning performance and the vanishing gradient problem are frequently encountered issues in SEI models. To solve this structural problem, ResNets stand out with their skip connection architecture. Particularly when processing signals converted into images via methods such as the Hilbert-Huang Transform (HHT), ResNets can learn complex and high-dimensional features without the need for expert intervention [15]. In conducted field experiments, it has been reported that ResNet-based hybrid fusion methods achieve an accuracy of over 96% in challenging tasks such as frequency hopping (FH) signals [25].

Conversely, in situations where the "time-series" nature of the signals is dominant rather than their snapshot images, Temporal Convolutional Networks (TCNs) are presented as a more suitable candidate. Unlike traditional RNNs and LSTMs networks, the TCN architecture can model much longer-term temporal dependencies by using causal and dilated convolutions. The parallel processing capability of TCNs eliminates the training slowness caused by the sequential processing constraint of LSTMs, and exhibits superior stability on time-series signals, especially under low SNR conditions. Therefore, the trend in literature is evolving towards the use of ResNets/CNNs for instantaneous spectral images, and TCNs for long-term signal sequences [26]. Furthermore, to reduce the computational load of deep architectures, recent studies proposed a lightweight architecture named RFFsNet [27], while other approaches enhanced

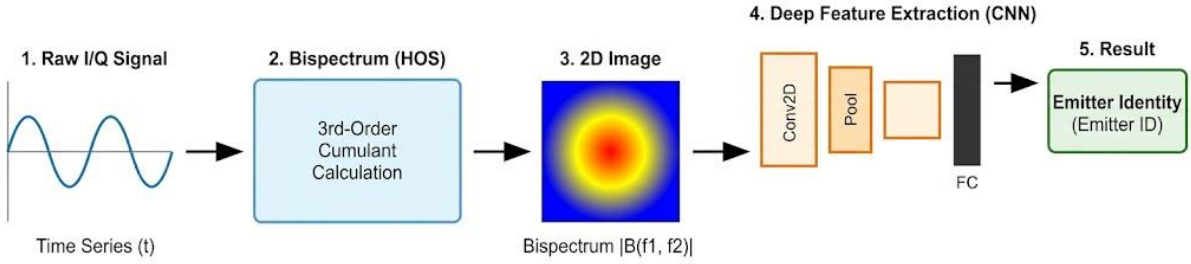


Figure 2: Bispectrum-based DL pipeline converting raw I/Q signals into noise-robust 2D images for CNN-based spatial feature extraction [14].

model stability with deep ensemble learning [28]. Similarly, a comprehensive review reveals that lightweight models, when combined with multimodal data representation, offer the most efficient solution in hardware-constrained environments [29].

2.3. Non-Stationary Signals and UMOP Extraction: The Role of VMD

Unintentional Modulation on Pulse (UMOP), observed in modern radars and transmitters, is one of the most critical "fingerprints" carrying the emitter identity. However, these subtle features are often lost under the dominance of noise and the main signal [3,10]. While classical methods remain inadequate for the analysis of such non-stationary signals, the VMD technique has emerged as a powerful alternative [20].

VMD, which solves the "mode mixing" problem (the biggest weakness of the Empirical Mode Decomposition method) with its non-recursive structure, decomposes the signal into intrinsic mode functions (IMFs) with different bandwidths. Through this decomposition, emitter-specific transient and steady-state features are isolated from each other; thus, enabling the clean extraction of discriminative RFF features such as entropy, spectral flatness, and brightness [20]. Considering different signal processing requirements and data types, a comparative analysis of these fundamental

Table 1: Comparative analysis of fundamental DL architectures used within the scope of cognitive SEI.

Method	Basic Principle & Input Type	Advantages for Cognitive EW (Pros)	Constraints and Challenges (Cons)
CNN + Bispectrum [7,14,22]	Convolutional feature extraction over higher-order statistics (bispectrum images).	Preserves phase and amplitude information; provides high resistance against Gaussian noise.	"Curse of dimensionality"; requires high computational cost, dimensionality reduction is mandatory.
ResNet [15,25,30]	Feature learning in very deep networks via skip connections (Input: time-frequency/HHT).	Solves the vanishing gradient problem; offers higher performance (96%+) than manual features in complex/FH signals.	Long training time; multi-layered structure requires high hardware resources.
TCN [26,31]	Sequence processing with causal and dilated convolutions.	Captures long-term temporal dependencies; suitable for parallel processing and trains faster compared to LSTMs/RNNs.	Focuses on long-term signal patterns rather than instantaneous spectral changes.
VMD [10,20]	Non-recursive decomposition of the signal into its IMFs.	Solves the "mode mixing" problem; effective in extracting UMOP from non-stationary signals.	Sensitive to parameter selection (number of modes, etc.); not a standalone classifier, requires preprocessing before DL.

approaches used in Cognitive SEI architectures is summarized in Table 1.

The success of DL models strictly depends not only on the architecture but also on the representation format of the data. Previous research demonstrated that multi-domain feature fusion increases classification success [7], rather than focusing on a single feature domain. In addition, while some studies combined time-frequency sequences in multimodal networks [32], others enhanced discriminability with deep subspace interactive networks [33]. As a more advanced approach, recent works adapted knowledge embedding techniques to SEI [9], enabling the representation of semantic relationships between signals in vector space, and strengthening the discriminability of the model, especially in noisy environments.

3. ADAPTIVE LEARNING STRATEGIES FOR CHALLENGING AND DYNAMIC ENVIRONMENTS

Traditional DL models exhibit high performance under the "closed-set" assumption based on massive amounts of labeled data. However, a real Cognitive EW battlefield violates these assumptions: hostile signals are rare, previously unseen novel threats may emerge in the field, and the adversary actively employs jamming/deception. This section critically examines adaptive approaches that go beyond static models to respond to these dynamic challenges. In order to scrutinize the numerical counterparts of these theoretical constraints in the field, the performances of current studies in the literature under different environmental conditions are comparatively presented in Table 2.

When the data in Table 2 are evaluated holistically, a distinct "reliability gap" between controlled laboratory conditions and the reality of the chaotic battlefield becomes apparent. Specifically, in studies where multimodal and feature fusion-based architectures were utilized, a high classification success in the 96% band was reported under ideal conditions [3,10]. Although these studies prove the competence of static models in learning the physical features (RFF) of the signal, this reliability is dramatically lost when the system is exposed to spoofing attacks generated by the adversary.

As a matter of fact, prior research demonstrated that an attack with a strength of -32 dB reduced model performance to the 55% level, but this rate could be increased back to 85.59% with adaptive

Table 2: Numerical performance comparison of the reviewed cognitive SEI studies.

Method & Dataset	Environmental Condition	Result / Performance
MuSEI (Radar Time Series + Vector) [3]	Variable Spectrum	96.67% accuracy (4% increase over unimodal).
IRelNet (Few-Shot Radar Data) [8]	Very Low SNR (4 dB)	90%+ performance maintained with channel attention.
ResNet + Fusion (15-Class Radio Data) [10]	Real Field Experiment	96.16% accuracy (with hybrid fusion).
HDA-DML (ADS-B and Wi-Fi) [17]	Data Scarcity (10% Data)	84.80% accuracy achieved with few samples.
Adversarial Training (Communication Signals) [18]	Strong Attack (-32 dB)	Accuracy increased from 55% to 85% under attack.

defense mechanisms such as adversarial training [18]. A similar need for adaptation applies in data scarcity scenarios; even in situations where the data collected from the field is highly limited, "Few-Shot" models augmented with an attention mechanism, as demonstrated in recent studies [8], [18], manage to hold onto the 84 – 90% band. These empirical findings clearly reveal that the high accuracy provided by static models under ideal conditions is insufficient to pass the "robustness" test required by Cognitive EW, and that the literature is now evolving towards self-healing adaptive architectures. Accordingly, the adaptive strategies developed to overcome the limitations of static models are detailed in the following subheadings.

3.1. The Data Scarcity Problem: Few-Shot and Meta-Learning

In the battlefield, collecting thousands of clean samples from non-cooperative hostile emitters is costly and difficult. In this "Few-Shot SEI" problem, standard CNN models tend to fail due to overfitting. The most prominent solutions to this problem in the literature are meta-learning and Deep Metric Learning (DML) approaches, where the model "learns how to learn" [8,16].

For instance, the IRelNet (Improved Relation Network) architecture focuses on learning the "similarity relationship" between samples rather than directly memorizing classes. Augmented with channel and spatial attention mechanisms, this structure can provide over 90% accuracy even under very low SNR (4 dB) conditions using limited samples [8,16]. Similarly, a Hybrid Data Augmentation and Deep Metric Learning (HDA-DML) approach has been proposed to overcome data scarcity. While this method expands the limited available data through rotation and mixing (CutMix) techniques, it simultaneously maximizes the inter-class distance using a "triplet loss" function [16,17]. These methods break the SEI system's dependence on massive data, enabling it to recognize novel threats with a small number of samples [34].

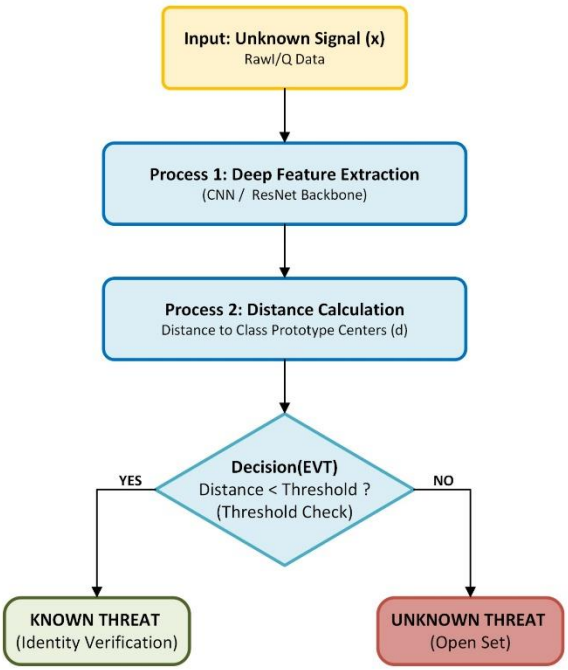


Figure 3: Flowchart of the open-set recognition mechanism.

3.2. Unknown Threats: Zero-Sample and Open-Set Recognition

Classical SEI systems can only recognize the classes they have seen in the training set ; therefore, during the test phase, when an unknown signal arrives, they err by forcibly assigning it to one of the existing classes. However, when a Cognitive EW system detects a novel hostile radar that is not in the database, it must be able to identify it as a novel entity—a capability formally known as open-set recognition [11,12].

For this critical capability, current studies propose hybrid models that combine prototypical

networks with statistical EVT [11]. The working principle of this proposed hybrid structure is illustrated in Figure 3. The process begins with the transformation of the unknown raw signal (I/Q data) into a low-dimensional feature vector (z) by passing it through deep neural networks (e.g., CNNs/ResNets). To achieve this, recent research developed a novel extreme value optimization method to reduce the sensitivity of prototypical networks to outliers, and class boundaries were determined utilizing EVT-based Weibull distributions [11]. In the decision phase, if the calculated distance remains above the established confidence threshold, the system confidently labels this signal as an unknown novel emitter. As an alternative to this statistical approach, other studies addressed the open-set problem by employing a deep feature-embedded discriminator [12]. This method enhances detection success by analyzing not only the distance to the class centers but also the distribution density in the feature space. Furthermore, zero-sample learning techniques have been developed for emitters whose operating parameters, such as pulse width or bandwidth, change. By correlating varying fingerprints with semantic features, these techniques enable identification even if there is no exact signal match in the database [35].

3.3. Robustness Against Adversarial Deceptions (Adversarial Robustness)

The most insidious threat faced by modern SEI systems is adversarial example attacks, which are virtually imperceptible but completely mislead artificial intelligence models. Research has shown that even very low-energy (–25 dB) perturbations can degrade the performance of a DL-based SEI system down to the 30% range [18]. The adversary can spoof the fingerprint of the target emitter using generative networks such as Conditional Generative Adversarial Networks (C-GANs) and sabotage the friend/foe discrimination [19].

The most effective defense strategy against this vulnerability is the adversarial training mechanism. This method, which grants a form of "digital immunity" by training the system not only with clean data but also with adversarial examples, can raise accuracy rates under attack from 55% back up to 85% levels [18]. Moreover, continual learning and domain adaptation techniques have been proposed to guarantee the long-term reliability of the system in order to adapt to hardware characteristics changing over time (aging) and domain differences created by various receivers [36].

Another aspect as critical as attack detection is the system's ability to continue recognizing the authorized user even under manipulated signals (identity verification). Prior research proposed robust architecture hybridizing statistical thresholding methods with DL to increase the reliability of RF fingerprint-based identity verification even in the presence of mimicking attacks [19]. To systematically synthesize these vulnerabilities and their corresponding countermeasures, a comprehensive threat-defense framework for Cognitive SEI systems is presented in Table 3.

Table 3: Threat-defense framework in cognitive SEI systems.

Threat Category	Attack / Challenge	Impact on SEI Systems	Recommended Defense Strategy
Adversarial Perturbations	Adversarial Examples (e.g., -25 dB to -32 dB low-energy noise perturbations) [18]	Severe degradation of classification accuracy (e.g., performance drops down to the ~30%-55% range).	Adversarial Training: Grants "digital immunity" by explicitly training the model with adversarial examples to restore accuracy and robustness.
Generative Spoofing	Fingerprint Spoofing (e.g., via C-GAN) & Mimicking Attacks [19], [23]	Sabotages friend/foe discrimination; effectively bypasses identity verification by replicating authorized fingerprints.	Hybrid Thresholding & DL: Combines statistical thresholding methods with deep architectures to reliably verify true identity despite mimicking.
Environmental & Hardware Dynamics	Hardware Aging & Receiver Domain Differences [36]	Causes gradual model drift and severe loss of long-term identification reliability over time.	Continual Learning & Domain Adaptation: Dynamically adapts the model to changing hardware characteristics and diverse receiver environments without forgetting prior knowledge.

4. CONCLUSIONS

The SEI technologies required by the modern Cognitive EW battlefield have been comprehensively examined in this study around the axes of data preprocessing, deep architecture selection, and dynamic environmental adaptation. The review conducted clearly demonstrates that the literature has undergone an irreversible evolution from traditional methods based on manual feature extraction to data-driven DL approaches that automatically discover hidden patterns within the data.

The obtained findings indicate that unimodal signal analyses remain inadequate in complex electromagnetic environments; conversely, as detailed in Table 1, multimodal architectures enriched with methods such as bispectral analysis and VMD significantly enhance signal discriminability. However, there is a striking gap between the laboratory environment and field reality. Although static DL models exhibit success rates of over 96% on controlled datasets, this performance can drop to levels around 50% under the effects of noise, data scarcity, and adversarial deceptions. This situation confirms that "high accuracy" does not always mean "high reliability," and that static models carry the risk of operational blindness. Therefore, it has become a vital necessity for a Cognitive EW system not only to identify the threats it recognizes in its database but also to distinguish unknown threats with open-set recognition capability and to continuously update itself via meta-learning strategies.

In this context, the future of SEI technology lies not merely in building deeper networks, but in creating smarter, more efficient, and adaptive cognitive loops. The focal point of future studies should be the development of lightweight architectures, similar to RFFsNet, that can operate on edge devices (Edge AI) with constrained hardware, such as Unmanned Aerial Vehicles (UAVs) and tactical field radios. Furthermore, transforming the system from a mere detecting analyzer into an autonomous entity that dynamically updates its own dataset upon encountering an unknown signal is essential for the completion of the cognitive loop. This capability, inherently driven by continual learning and open-set recognition paradigms, is a

prerequisite for maintaining resilience against time-varying threats. In addition to these advancements, rendering the decisions made by DL models interpretable to the operator (Explainable AI - XAI) is of critical importance for establishing trust in human-machine collaboration. Ultimately, the adaptive strategies and future projections presented in this study offer a solid roadmap for literature, moving towards making the invisible visible within the electromagnetic spectrum and ensuring the sustainability of EW superiority.

AUTHOR CONTRIBUTIONS

Mert KARAHAN: Data Curation, Formal Analysis, Investigation, Methodology, Methodology, Writing.

Onur BATTAL: Investigation, Methodology, Writing - Original Draft, Writing - Review & Editing.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] K. Z. Haigh and J. Andrusenko, Cognitive Electronic Warfare: an artificial intelligence approach. Boston: Artech House, 2021.

[2] N. O'Donoughue, Emitter Detection and Geolocation for Electronic Warfare. Artech House, 2019. doi: 10.7249/CB909.

[3] H. Peng, K. Xie, and W. Zou, "Research on an Enhanced Multimodal Network for Specific Emitter Identification," Electronics, vol. 13, no. 3, p. 651, Feb. 2024, doi: 10.3390/electronics13030651.

[4] H. Xiao, H. Liu, Y. Zhou, L. Yang, and Z. Ma, "Distributed Unknown Specific Emitter Identification Based on Federated Learning," in 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), Singapore, Singapore: IEEE, Jun. 2024, pp. 1–5. doi: 10.1109/VTC2024-Spring62846.2024.10683366.

[5] J. H. Tyler, M. K. M. Fadul, and D. R. Reising, "Considerations, Advances, and Challenges Associated with the Use of Specific Emitter Identification in the Security of Internet of Things Deployments: A Survey," Information, vol. 14, no. 9, p. 479, Aug. 2023, doi: 10.3390/info14090479.

[6] B. He, F. Wang, Y. Liu, and S. Wang, "Specific Emitter Identification Via Multiple Distorted Receivers," in 2019 IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China: IEEE, May 2019, pp. 1–6. doi: 10.1109/ICCW.2019.8757066.

[7] L.-Z. Qu, H. Liu, K.-J. Huang, and J.-A. Yang, "Specific Emitter Identification Based on Multi-Domain Feature Fusion and Integrated Learning," Symmetry, vol. 13, no. 8, p. 1481, Aug. 2021, doi: 10.3390/sym13081481.

[8] Z. Wu, M. Du, D. Bi, and J. Pan, "IRelNet: An Improved Relation Network for Few-Shot Radar Emitter Identification," Drones, vol. 7, no. 5, p. 312, May 2023, doi: 10.3390/drones7050312.

[9] S. Cao, Y. Liu, L. Sun, and Y. Lin, "Specific Emitter Identification Based on Knowledge Embedding," in ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA: IEEE, Jun. 2024, pp. 1661–1666. doi: 10.1109/ICC51166.2024.10622500.

[10] G. Gok, Y. K. Alp, and O. Arikan, "A New Method for Specific Emitter Identification With Results on Real Radar Measurements," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 3335–3346, 2020, doi: 10.1109/TIFS.2020.2988558.

[11] C. Wang, Y. Wang, Y. Zhang, H. Xu, and Z. Zhang, "Open-Set Specific Emitter Identification Based on Prototypical Networks and Extreme Value Theory," Appl. Sci., vol. 13, no. 6, p. 3878, Mar. 2023, doi: 10.3390/app13063878.

[12] Z. Wu, M. Hua, Y. Zhang, S. Wang, P. Liu, and G. Gui, "An Open Set Specific Emitter Identification Method Using Deep Feature Embedded Discriminator," in 2023 IEEE 23rd International Conference on Communication Technology (ICCT), Wuxi, China: IEEE, Oct. 2023, pp. 1415–1419. doi: 10.1109/ICCT59356.2023.10419658.

[13] P. Gupta, P. Jain, and O. G. Kakde, “Deep Learning Techniques in Radar Emitter Identification,” Def. Sci. J., vol. 73, no. 5, pp. 551–563, Aug. 2023, doi: 10.14429/dsj.73.18319.

[14] L. Ding, S. Wang, F. Wang, and W. Zhang, “Specific Emitter Identification via Convolutional Neural Networks,” IEEE Commun. Lett., vol. 22, no. 12, pp. 2591–2594, Dec. 2018, doi: 10.1109/LCOMM.2018.2871465.

[15] Y. Pan, S. Yang, H. Peng, T. Li, and W. Wang, “Specific Emitter Identification Based on Deep Residual Networks,” IEEE Access, vol. 7, pp. 54425–54434, 2019, doi: 10.1109/ACCESS.2019.2913759.

[16] C. Wang et al., “Few-Shot Specific Emitter Identification via Hybrid Data Augmentation and Deep Metric Learning,” Dec. 01, 2022, arXiv: arXiv:2212.00252. doi: 10.48550/arXiv.2212.00252.

[17] S. Mu, Y. Zu, S. Chen, S. Yang, Z. Feng, and J. Zhang, “Few-Shot Metric Learning with Time-Frequency Fusion for Specific Emitter Identification,” Remote Sens., vol. 16, no. 24, p. 4635, Dec. 2024, doi: 10.3390/rs16244635.

[18] L. Sun, D. Ke, X. Wang, Z. Huang, and K. Huang, “Robustness of Deep Learning-Based Specific Emitter Identification under Adversarial Attacks,” Remote Sens., vol. 14, no. 19, p. 4996, Oct. 2022, doi: 10.3390/rs14194996.

[19] D. R. Reising, J. H. Tyler, M. K. M. Fadul, M. R. Hilling, and T. D. Loveless, “Improved RF Fingerprint-based Identity Verification in the Presence of an SEI Mimicking Adversary,” J. Cyber Secur. Mobil., pp. 887–916, Sep. 2024, doi: 10.13052/jcsm2245-1439.1354.

[20] U. Satija, N. Trivedi, G. Biswal, and B. Ramkumar, “Specific Emitter Identification Based on Variational Mode Decomposition and Spectral Features in Single Hop and Relaying Scenarios,” IEEE Trans. Inf. Forensics Secur., vol. 14, no. 3, pp. 581–591, Mar. 2019, doi: 10.1109/TIFS.2018.2855665.

[21] A. Madhu, P. Prajeesha, and A. S. Kulkarni, “Radar Emitter Identification using Signal Noise and Power Spectrum Analysis in Deep Learning,” in 2022 Fifth International Conference of Women in Data Science at Prince Sultan University (WiDS PSU), Riyadh, Saudi Arabia: IEEE, Mar. 2022, pp. 52–57. doi: 10.1109/WiDS-PSU54548.2022.00022.

[22] C. Xie, L. Zhang, and Z. Zhong, “Virtual Adversarial Training-Based Semisupervised Specific Emitter Identification,” Wirel. Commun. Mob. Comput., vol. 2022, no. 1, p. 6309958, Jan. 2022, doi: 10.1155/2022/6309958.

[23] K. Tan, W. Yan, L. Zhang, Q. Ling, and C. Xu, “Semi-Supervised Specific Emitter Identification Based on Bispectrum Feature Extraction CGAN in Multiple Communication Scenarios,” IEEE Trans. Aerosp. Electron. Syst., vol. 59, no. 1, pp. 292–310, Feb. 2023, doi: 10.1109/TAES.2022.3184619.

[24] G.-J. Qi and J. Luo, “Small Data Challenges in Big Data Era: A Survey of Recent Progress on Unsupervised and Semi-Supervised Methods,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 4, pp. 2168–2187, Apr. 2022, doi: 10.1109/TPAMI.2020.3031898.

[25] M. Li, J. Xie, H. Yang, M. Geng, and J. Liu, “Specific Emitter Identification of Frequency Hopping Signals Based on Feature Extraction and Deep Residual Network,” IEEE Access, vol. 10, pp. 119084–119094, 2022, doi: 10.1109/ACCESS.2022.3221432.

[26] C. Zhu, L. Liu, and X. Peng, “Specific Emitter Identification Based on Temporal Convolutional Network Sequence Processing,” IEEE Commun. Lett., vol. 27, no. 10, pp. 2667–2671, Oct. 2023, doi: 10.1109/LCOMM.2023.3312390.

[27] R. Fan, C. Si, Y. Han, and Q. Wan, “RFFsNet-SEI: A Multidimensional Balanced-RFFs Deep Neural Network Framework for Specific Emitter Identification,” J. Syst. Eng. Electron., vol. 35, no. 3, pp. 558–574, Jun. 2024, doi: 10.23919/JSEE.2023.000069.

[28] Z.-M. Liu, “Multi-feature fusion for specific emitter identification via deep ensemble learning,” Digit. Signal Process., vol. 110, p. 102939, Mar. 2021, doi: 10.1016/j.dsp.2020.102939.

[29] W. Guo, J. Wang, and S. Wang, “Deep Multimodal Representation Learning: A Survey,” IEEE Access, vol. 7, pp. 63373–63394, 2019, doi: 10.1109/ACCESS.2019.2916887.

[30] J. Genova, Electronic warfare signal processing. in Artech house electronic warfare library. Boston: Artech house, 2018.

[31] G. Huang, Y. Yuan, X. Wang, and Z. Huang, “Specific Emitter Identification Based on Nonlinear Dynamical Characteristics,” Can. J.

Electr. Comput. Eng., vol. 39, no. 1, pp. 34–41, 2016, doi: 10.1109/CJECE.2015.2496143.

[32] Y. He, K. Wang, Q. Song, H. Li, and B. Zhang, "Specific Emitter Identification Algorithm Based on Time–Frequency Sequence Multimodal Feature Fusion Network," Electronics, vol. 13, no. 18, p. 3703, Sep. 2024, doi: 10.3390/electronics13183703.

[33] Z. Zhu, H. Ji, and L. Li, "Deep Multimodal Subspace Interactive Mutual Network for Specific Emitter Identification," IEEE Trans. Aerosp. Electron. Syst., vol. 59, no. 4, pp. 4289–4300, Aug. 2023, doi: 10.1109/TAES.2023.3240115.

[34] D. Lv, Z. Yu, J. Xie, and H. Zhang, "Review on the Development of Few-Shot Specific Emitter Identification Technology," in 2024 4th International Conference on Electronic Information Engineering and Computer Science (EIECS), Yanji, China: IEEE, Sep. 2024, pp. 1061–1068. doi: 10.1109/EIECS63941.2024.10800029.

[35] P. Man, C. Ding, W. Ren, and G. Xu, "A Specific Emitter Identification Algorithm under Zero Sample Condition Based on Metric Learning," Remote Sens., vol. 13, no. 23, p. 4919, Dec. 2021, doi: 10.3390/rs13234919.

[36] J. Liu, J. Wang, H. Huang, and J. Li, "Specific emitter identification unaffected by time through adversarial domain adaptation and continual learning," Eng. Appl. Artif. Intell., vol. 138, p. 109324, Dec. 2024, doi: 10.1016/j.engappai.2024.109324.