

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DERİN ÖĞRENME YÖNTEMLERİ
KULLANILARAK ELEKTRONİK
CİHAZLARIN YAYDIĞI VE ÜRETTİĞİ
SİNYALLER ÜZERİNDEN
KİMLİKLENDİRİLMESİ

Furkan Hasan SAKACI

DOKTORA TEZİ

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Programı

Danışman

Prof. Dr. Tülay YILDIRIM

Şubat, 2025

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**DERİN ÖĞRENME YÖNTEMLERİ KULLANILARAK
ELEKTRONİK CİHAZLARIN YAYDIĞI VE ÜRETTİĞİ
SİNYALLER ÜZERİNDEN KİMLİKLENDİRİLMESİ**

Furkan Hasan SAKACI tarafından hazırlanan tez çalışması 10/02/2025 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı, Elektronik Programı **DOKTORA TEZİ** olarak kabul edilmiştir.

Prof. Dr. Tülay YILDIRIM
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Prof. Dr. Tülay YILDIRIM, Danışman

Yıldız Teknik Üniversitesi

Prof. Dr. Umut Engin AYTEN, Üye

Yıldız Teknik Üniversitesi

Doç. Dr. Şuayb Çağrı YENER, Üye

Sakarya Üniversitesi

Doç. Dr. Peyman MAHOUTİ, Üye

Yıldız Teknik Üniversitesi

Prof. Dr. Osman ÇEREZCİ, Üye

Üsküdar Üniversitesi

Danışmanım Prof. Dr. Tlay YILDIRIM sorumluluęunda tarafımca hazırlanan Derin Öğrenme Yöntemleri Kullanılarak Elektronik Cihazların Yaydığı ve Ürettięi Sinyaller Üzerinden Kimliklendirilmesi başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, dięer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Furkan Hasan Sakacı

İmza



Bu çalışma, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından 123E010 numaralı projesi ile desteklenmiştir.



Aileme
ve
biricik eşime

TEŞEKKÜR

Doktora eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Tülay YILDIRIM’a teşekkürlerimi sunarım.

Eğitim ve çalışma hayatımın temposu sırasında beni sürekli motive ederek doktora tezim kapsamındaki her türlü maddi ve manevi desteği sağlayan, bunlarla beraber kişisel olarak gelişimime etki ederek iletişim yeteneklerimi arttıran sevgili eşim Nisanur SAKACI’ya teşekkürlerimi sunarım. Hayatım boyunca maddi ve manevi olarak desteğini her zaman hissettiğim aileme ve bilgilerini hiçbir zaman esirgemeyen kıymetli hocalarıma teşekkür ederim.

Tez kapsamında gerekli bilgi birikimimi arttırdığım ve çalışmaktan keyif aldığım GOHM Elektronik firmasına ve doktora tezim kapsamında yaptığımız ortak çalışmalar sayesinde doktora tezimin daha nitelikli hale gelmesini sağlayan HAVELSAN firmasına teşekkür ederim.

Furkan Hasan SAKACI

İÇİNDEKİLER

SİMGE LİSTESİ	ix
KISALTMA LİSTESİ	xi
ŞEKİL LİSTESİ	xiii
TABLO LİSTESİ	xvii
ÖZET	xviii
ABSTRACT	xx
1 GİRİŞ	1
1.1 Kimliklendirmenin Tarihçesi	5
1.2 Literatür Özeti	7
1.2.1 Kablosuz Haberleşme	8
1.2.2 Kablolı Haberleşme	11
1.2.3 Elektromanyetik Emisyon	13
1.3 Tezin Amacı	19
1.4 Hipotez	19
1.5 Tezin Organizasyonu	20
2 KULLANILAN TEKNOLOJİLER VE ARAÇLAR	21
2.1 Makine Öğrenmesi	21
2.1.1 Yapay Sinir Ağları (Artificial Neural Network, ANN)	22
2.1.2 Çok Katmanlı Perceptron (Multi Layer Perceptron, MLP)	24
2.1.3 Evrişimsel Sinir Ağı (Convolutional Neural Network, CNN)	26

2.1.4 Zamansal Konvolüsyon Ağı (Temporal Convolutional Network, TCN).....	27
2.1.5 Tekrarlayan Sinir Ağı (Recurrent Neural Network, RNN)	28
2.1.6 Uzun Kısa Süreli Bellek (Long Short-Term Memory, LSTM).....	30
2.1.7 Kapılı Tekrarlama Ünitesi (Gate Recurrent Unit, GRU)	31
2.2 Paralel Programlama ve CUDA.....	33
3 RF TEMELLİ KİMLİKLENDİRME	37
3.1 Wi-Fi Cihazlarının Kimliklendirilmesi.....	37
3.1.1 Önerilen Tasarım.....	37
3.1.2 WiFi Sinyal Karakteristiği.....	38
3.1.3 Paket Tespiti	39
3.1.3.1 Senkronizasyon	40
3.1.3.2 Demodülasyon	41
3.1.3.3 Çözümleme	43
3.1.4 Veri Setinin Oluşturulması.....	44
3.1.5 Derin Öğrenme	46
3.1.6 Deneysel Sonuçlar	50
3.2 LoRa (Long Range) Cihazlarının Kimliklendirilmesi	54
3.2.1 LoRa Sinyal Karakteristiği.....	55
3.2.2 Veri Setinin Oluşturulması	58
3.2.2.1 Paket Tespiti.....	58
3.2.2.2 Senkronizasyon	59
3.2.2.3 Demodülasyon	60
3.2.2.4 Çözümleme	62
3.2.3 Derin Öğrenme	63
3.2.4 Deneysel Sonuçlar	64

4 ANALOG SİNYAL İLE KİMLİKLENDİRME	79
4.1 Ethernet Sinyali Üzerinden Kimliklendirme.....	79
4.1.1 Teorik Yaklaşım	79
4.1.2 Ethernet Sinyal Karakteristiği	82
4.1.3 Önerilen Tasarım	83
4.1.4 Derin Öğrenme	86
4.1.5 DeneySEL Sonuçlar	87
5 ELEKTROMANYETİK EMİSON İLE KİMLİKLENDİRME	91
5.1 İletilen Elektromanyetik Sinyal ile Kimliklendirme.....	91
5.1.1 Önerilen Tasarım	91
5.1.2 Veri Setinin Oluşturulması	93
5.1.3 Derin Öğrenme Modeli	98
5.1.4 Simülasyon Sonuçları.....	100
5.1.5 DeneySEL Sonuçlar	103
5.2 Havadan Yayılan Elektromanyetik Sinyal ile Kimliklendirme	115
5.2.1 Önerilen Tasarım	115
5.2.2 Veri Setinin Oluşturulması	116
5.2.3 Derin Öğrenme Modeli	120
5.2.4 DeneySEL Sonuçlar	121
6 SONUÇ	126
KAYNAKÇA	130
A CİHAZLARIN ELEKTROMANYETİK SPEKTROGRAMLARI	143
TEZDEN ÜRETİLMİŞ YAYINLAR	147

SİMGE LİSTESİ

$\tilde{h}_t$	Aday hücre durumu
$W_z,$	Ağırlık matrisini
I	Akım (amper)
$f^{(l)}$	Aktivasyon fonksiyonu
G_r	Alıcı anten kazancı
P_r	Alıcı gücü (watt)
L	Anten uzunluğu (metre)
k_B	Boltzmann sabiti (1.38×10^{-23} J/K)
μ_0	Boşluk permütivitesi (8.85×10^{-12} F/m)
Q_L	Boyutsuz bir parametre olan yüklenmiş Q faktörü
F	Cihazın çalışma güç seviyesindeki gürültü faktörünü
λ	Dalga boyu (metre)
d	Dilasyon faktörü
$\odot$	Eleman çarpımı
$S(i,j)$	Evrşim işlemi sonucunda elde edilen özellik haritasının elemanı
k	Filtre boyutu
w_i	Filtre katsayıları
W	Filtre matrisi
$F(s)$	Filtre
l	Gecikme parametresi
V	Gerilim (volt)
I	Giriş matrisi
W_{hx}	Giriş ile gizli durum arasındaki ağırlık matrisi
W_{hh}	Gizli durum ile gizli durum arasındaki ağırlık matrisi
W_{io}	Gizli durum ile gizli çıkış arasındaki ağırlık matrisi
b_h	Gizli durum için bias terimi
h_t	Gizli durum

z_t	Güncelleme aşamasının çıkışı (update gate output)
c_t	Hafıza hücresi
I	In-Phase
G	İletim kaybı faktörü
G_i	i'ninci girdi
A_i	i'ninci ağırlık
S	Kaynak yoğunluğu (watt/m ²)
Q	Quadrature
$W^{(l)}$	l'ninci katmandaki ağırlık matrisi
$a^{(l)}$	l'ninci katmandaki aktivasyon öncesi değer
$h^{(l)}$	l'ninci katmandaki aktivasyon sonrası değer
$b^{(l)}$	l'ninci katmandaki bias terimini
r	Mesafe (metre)
A	Osilatör çıkış gücü (watt)
$f_o,$	Osilatör taşıyıcı frekansı
α	Öğrenme oranı
h_{t-1}	Önceki zaman adımındaki gizli durumu
P	Radyasyon gücü (watt)
T	Sıcaklık (Kelvin)
σ	Sigmoid aktivasyon fonksiyonu
f_m	Taşıyıcıdan olan frekans sapması
L_{PM}	Tek yan bant faz gürültü yoğunluğu (dBc/Hz)
y_t	t zaman adımındaki çıkış
x_t	t zaman adımındaki giriş
h_t	t zaman adımındaki gizli durum vektörü
G_t	Verici anten kazancı
P_i	Verici gücü (watt)
K_o/s	Voltaj kontrollü osilatör (Voltage Control Oscillator, VCO)

KISALTMA LİSTESİ

ACTF	Bitişik Takımyıldız İzi Şekli (Adjacent Constellation Trace Figure)
ADC	Analog Dijital Dönüştürücü (Analog Digital Converter)
ANN	Yapay Sinir Ağları (Artificial Neural Networks)
AWS	Amazon Web Servisleri
BPSK	İkili Faz Kaydırmalı Anahtarlama (Binary Phase Shift Keying)
CB-DNA	Koşullu Takımyıldız Tabanlı-Ayrı Yerel Nitelik
CNN	Evrişimsel Sinir Ağı (Convolutional Neural Network)
CPU	Merkezî işlem birimi (Central Process Unit)
CRC	Döngüsel Yedeklilik Denetimi (Cyclic Redundancy Check)
CSS	Cıvıltı Yayılım Spektrumu (Chirp Spread Spectrum)
CSV	Virgülle Ayırılan Değerler (Comma Separated Values)
CR	Kod oranı (Code Rate)
CUDA	Birleşik Cihaz Mimarisi Hesaplama
DSP	Dijital Sinyal İşleme (Digital Signal Processing)
EMC	Elektromanyetik Uyumluluk (Electromagnetic Comability, EMC)
FFT	Hızlı Fourier dönüşümü (Fast Fourier Transform)
GPU	Grafik İşleme Birimi (Graphics Processing Unit)
GRU	Kapılı Tekrarlayan Ünite (Gated Recurrent Unit)
IoT	Nesneleri İnterneti (Internet of Things)
LISN	Şebeke Empedansı Dengeleme Ağı
LSTM	Uzun Kısa Süreli Bellek (Long Short-Term Memory)
LTS	Uzun Başlangıç Dizisi
LoRaWAN	Uzun Menzilli Geniş Alan Ağı (Long Range Wide Area Network)
M2M	Makineden Makineye (Machine to Machine)
MAC	Medya Erişim Kontrolü (Media Access Control)
MLP	Çok Katmanlı Algılayıcı (Multilayer Perceptron)
OFDM	Ortogonal Frekans Bölmeli Çoklama

OSI	Açık Sistemler Ara Bağlantısı (Open Systems Interconnection)
RAM	Rastgele Erişimli Bellek (Random Access Memory)
PLL	Faz kilitlemeli çevrim (Phase Lock Loop)
RF	Radio Frekans (Radio Frequency)
RNN	Tekrarlayan Sinir Ağı (Recurrent Neural Network)
SDR	Yazılım Tanımlı Radyo (Software Defined Radio)
SEI	Spesifik Verici Tanımlaması (Specific Emitter Identification)
SFD	Başlangıç Çerçevesi Ayırıcısı (Start Frame Delimiter)
SF	Yayılım Faktörü (Spreading Factor)
STS	Kısa Başlangıç Dizisi
TCN	Zamansal Evrişimsel Ağlar (Temporal Convolutional Networks)
TLS	Taşıma Katmanı Güvenliği (Transport Layer Security)
TÜİK	Türkiye İstatistik Kurumu
SNR	Sinyal-Gürültü Oranı (Signal Noise Ratio)
SSL	Güvenli Soket Katmanı (Secure Sockets Layer)
VCO	Voltaj Kontrollü Osilatör (Voltage Controlled Oscillator)
WiFi	Kablosuz Bağlantı (Wireless Fidelity)

ŞEKİL LİSTESİ

Şekil 1.1 İnternet kullanımının yıllara göre kullanım grafiği	2
Şekil 1.2 Cihaz kimliklendirme için kullanılan hiyerarşi	4
Şekil 1.3 Elektromanyetik emisyon ölçümünün mesafeye bağlı değişimi	16
Şekil 2.1 Örnek bir ANN algoritmasının blok olarak gösterimi	23
Şekil 2.2 Örnek bir MLP algoritmasının blok olarak gösterimi	25
Şekil 2.3 RNN algoritmasında kullanılan hücre yapısı.....	29
Şekil 2.4 LSTM algoritmasında kullanılan hücre yapısı	30
Şekil 2.5 GRU algoritmasında kullanılan hücre yapısı.....	32
Şekil 3.1 WiFi cihazlarının kimliklendirilmesi için önerilen sistem	38
Şekil 3.2. WiFi sinyalindeki OFDM sembollerinin paket yapısı.....	39
Şekil 3.3 Paketin yakalanması sırasında kullanılan grafiğin gösterimi	40
Şekil 3.4 Senkronizasyon için elde grafiğin gösterimi	41
Şekil 3.5 Ham sinyalin takım yıldız diyagramı	41
Şekil 3.6 Düzeltme işlemlerinden sonra elde edilen takımyıldız diyagramı	43
Şekil 3.7 Veri seti üretimi için SDR ile WiFi Sensörleri iletişiminin dinleme diyagramı	44
Şekil 3.8 Veri seti oluşturma algoritması ve etiketleme mimarisi	45
Şekil 3.9 Derin öğrenme modeli için kullanılan sistemin kod mimarisi	47
Şekil 3.10. RAM'i belirli bir sınırdan tutmak için giriş boru hattı yapısı	48
Şekil 3.11 WiFi cihazlarını kimliklendirmek için kullanılan model	49
Şekil 3.12 SDR ile AGX cihazının ağ üzerinde bağlantısı	50
Şekil 3.13 Derin öğrenme modelinin dönem sayılarına göre doğruluk oranı.....	51
Şekil 3.14 Sistemde tanımlı bir cihaz için gerçek zamanlı başarımlı oranı	53
Şekil 3.15 LoRa haberleşmesi için oluşturulmuş OSI katmanları	54
Şekil 3.16 LoRa cihazlarının kimliklendirilmesi için önerilen sistem.....	55
Şekil 3.17 LoRa paket çerçevesinin yapısı	57
Şekil 3.18 LoRa paketinin spektrogram gösterimi	58
Şekil 3.19 LoRa paketinin başlangıç noktasının bulunması için Senkronizasyon paketi ile korelasyon sonucu.....	60

Şekil 3.20 LoRa paketindeki bir sembol içeriğinin spektrogram gösterimi	61
Şekil 3.21 LoRa sembol içeriğindeki bir verinin frekans cevabı.....	62
Şekil 3.22 LoRa cihazlarının kimliklendirilmesinde kullanılan derin öğrenme modellerinin gösterimi.....	64
Şekil 3.23 Önerilen tasarımı test etmek için oluşturulmuş kurulum.....	65
Şekil 3.24 (a) TCN (b) LSTM (c) GRU (d) CNN derin öğrenme modellerinin dönem sayılarına göre doğruluk oranları	68
Şekil 3.25 LoRa paketlerini kimliklendirmede (a) TCN (b) LSTM (c) GRU (d) CNN derin öğrenme modellerinin gün bazında ortalama doğruluk oranı	71
Şekil 3.26 (a) TCN (b) CNN derin öğrenme modellerinin LoRa paketlerini kimliklendirmede günlere göre ortalama doğruluk oranı	73
Şekil 3.27 Bir taklit saldırısı sırasında CNN modelinin gerçek zamanlı doğruluk oranları	77
Şekil 3.28 Bir taklit saldırısı sırasında CNN modelinin gerçek zamanlı doğruluk oranları	78
Şekil 4.1. Ethernet haberleşmesinde kullanılan LAN9514 entegre devresinin iç yapısı.....	79
Şekil 4.2 Ethernet haberleşmesinde kullanılan LAN9514 entegre devresinin elektronik modeli	80
Şekil 4.3 Ethernet sinyali üzerinden cihaz kimliklerinin tespitine yönelik sistemin genel mimarisi.....	83
Şekil 4.4 Ethernet sinyallerinden veri seti oluşturulması için kullanılan mimari. .84	
Şekil 4.5 Ethernet sinyalinin GPU üzerinde işlenebilmesi için gerekli işlem adımları	85
Şekil 4.6 Ethernet sinyal kabloları ile oluşturulmuş olan sistemin birleşik gösterimi	86
Şekil 4.7 Ethernet iletişim (a) zaman alanı (b) frekans alanı sinyali özellikleri	88
Şekil 4.8 Epok sayısına göre doğruluk oranı	89
Şekil 4.9 İki Raspberry Pi 3 cihazının derin öğrenme modeli tahminleri için Karışıklık Matrisi	90
Şekil 5.1 Elektromanyetik emisyon tabanlı kimliklendirme sisteminin genel mimarisi	92
Şekil 5.2 Elektromanyetik emisyon ölçümünde kullanılan LISN devresi.....	93
Şekil 5.3 Spice üzerinden veri toplamak için oluşturulmuş olan devre kurulumunun şematik gösterimi	93
Şekil 5.4 Spice'tan alınan iki farklı cihaz sinyallerinin FFT dönüşümü	94
Şekil 5.5 Spice'tan alınan iki farklı cihaz sinyallerinin FFT dönüşümünün farkı .95	
Şekil 5.6 Spice aracılığıyla elde edilen sinyalin spektrogramı	96

Şekil 5.7 Spice aracılığıyla elde edilen sinyalin spektrogram farkı.....	97
Şekil 5.8 Veri kümesi oluşturmada kullanılan veri segmentasyon yöntemi.....	98
Şekil 5.9 Kullanılan CNN derin öğrenme modelinin mimarisi.	99
Şekil 5.10 Dönem sayısına göre doğruluk oranı.....	100
Şekil 5.11 Simülasyon verilerinden elde edilen sınıflandırma sonuçlarının karışıklık matrisi.	101
Şekil 5.12 Sistemde bir cihazı taklit eden bilinmeyen bir cihazın doğruluk oranı	103
Şekil 5.13 İletilen Emisyon sinyalleri aracılığıyla tanımlama yapmak için oluşturulan kurulum.....	104
Şekil 5.14 İletilen Emisyon sinyalleri aracılığıyla tanımlama yapmak için kullanılan cihazlar.....	105
Şekil 5.15 Dönem sayısına göre doğruluk oranı.....	107
Şekil 5.16 Deneyisel verilerden elde edilen sınıflandırma sonuçlarının karışıklık matrisi.	108
Şekil 5.17 Deneyisel verilerden elde edilen sınıflandırma sonuçlarının, Boost Konvertörler için uygulanan iç yük ile ilgili karışıklık matrisi.	110
Şekil 5.18 Gün içerisinde belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla cihaz kimliğini tahmin etmedeki doğruluk oranı.	112
Şekil 5.19 Bir gün boyunca belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla 5 verinin ortalaması alınarak cihaz kimliğini tahmin etmedeki doğruluk oranı	113
Şekil 5.20 Bir gün boyunca belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla 50 verinin ortalaması alınarak cihaz kimliğini tahmin etmedeki doğruluk oranı	114
Şekil 5.21 Yakın alan problemleri ile cihazların kimliklendirilmesi için oluşturulmuş sistemin mimarisi.....	116
Şekil 5.22 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucu.	117
Şekil 5.23 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucunun FFT dönüşümü.....	118
Şekil 5.24 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucunun spektrogram dönüşümü.	119
Şekil 5.25 Önerilen tasarım mimarisi içerisinde geliştirilen TCN modeli.	120
Şekil 5.26 Önerilen sistemin uygulamasını test etmek için oluşturulmuş düzenek.	121
Şekil 5.27 Raspberry Pi cihazlarının kimlik doğrulama testinden elde edilen Karmaşıklık Matrisi	122

Şekil 5.28 (a) 100 MSPS ve (b) 800 MSPS'ye sahip Raspberry Pi cihazları için geliştirilen derin öğrenme modellerinin kimlik doğrulama testinden elde edilen Karışıklık Matrisi.....	123
Şekil 5.29 Ham sinyalin, ham sinyale gürültü eklenerek oluşturulan sinyallerle karşılaştırılması.....	124
Şekil 5.30 Sentetik gürültü ile test edildikten sonra 100 MSPS ve 800 MSPS'de örneklenen veriler üzerinde eğitimden elde edilen derin öğrenme modelinin doğruluk oranları.....	125



TABLO LİSTESİ

Tablo 3.1 Modelin farklı algoritmalar ile oluşturulmasının analizi.....	52
Tablo 3.2 CPU ve GPU üzerinde yapılan işlemlerin hız karşılaştırmaları	66
Tablo 3.3 Günlük paket miktarına göre eğitilen modellerin başarımları	75
Tablo 5.1 Modelinin Kesinlik, Duyarlılık ve F1 Puanı değerleri	102
Tablo 5.2 Kullanılan cihazların listesi ve özellikleri	106
Tablo 5.3 Modelinin Kesinlik, Duyarlılık ve F1 Puanı değerleri	111



Derin Öğrenme Yöntemleri Kullanılarak Elektronik Cihazların Yayıdığı ve Ürettiği Sinyaller Üzerinden Kimliklendirilmesi

Furkan Hasan SAKACI

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Programı

Doktora Tezi

Danışman: Prof. Dr. Tülay YILDIRIM

Günümüzde elektronik cihazların kritik ortam ve sistemlerde bulunması güvenlik kontrollerinin yapılmasını karmaşıktırabilmektedir. Sinyallerin dijital formata çevrildikten sonra güvenlik kontrollerinin yapılması dijital kimlik ya da sertifikaların ele geçmesi durumunda cihazların kimliğinin taklit edilmesine yol açmaktadır. Bu tez çalışması kapsamında kablolu sinyaller, kablosuz sinyaller ve yayılan elektromanyetik sinyallerin ham formatı kullanılarak üç ayrı başlıkta cihazların kimliklendirilmesi sağlanmıştır. Kablolu sinyal olarak Ethernet sinyalleri, kablosuz sinyaller olarak WiFi ve LoRa sinyalleri, elektromanyetik sinyal olarak ise iletilen emisyon sinyalleri ile havadan yayılan elektromanyetik emisyon sinyalleri kullanılmıştır. Önerilen sistemlerin geliştirilmesi için öncelikli olarak sistemlerde tanımlı cihazlar üzerinden ilgili sinyaller toplanmıştır.

Sinyallerin toplanarak veri seti oluşturulabilmesi için kullanılan protokole bağı olarak cihazlardan alınan sinyallerin çözümlenmesi de sağlanmış olup elde edilen sinyaller çözümlenen paket içindeki kimlikleri ile etiketlenmiştir. Oluşturulan veri setleri ile derin öğrenme modelleri eğitilerek cihazların ham sinyalleri üzerinden kimlikleri oluşturulmuştur. Elde edilen derin öğrenme modeli daha sonrasında cihazların kimlik kontrolünün yapılması için kullanılarak kritik ortam ve sistemlerin güvenliği sağlanmıştır. Bu çalışmaların sonucunda, Ethernet sinyalleri üzerinden yapılan kimliklendirme ile birebir aynı modele sahip iki cihaz %98,7 başarımlarında kimliklendirilmiştir. WiFi sinyalleri ile yapılan çalışmada aynı özelliklere sahip altı farklı cihaz %99,47 başarımlarında kimliklendirilirken LoRa sinyalleri ile yapılan çalışmada ise dört farklı cihaz %99 başarımları ile kimliklendirilmiştir. Bununla beraber LoRa sinyalleri ile yapılan çalışma kapsamında cihazların uzun süreli testleri de yapılarak eğitim için gerekli minimum sinyal analizleri de yapılmış olup eğitim için saatte bir paket atılmasının bile önerilen sistemin başarısı için yeterli olduğu görülmüştür. Elektromanyetik sinyaller ile yapılan kimliklendirme çalışmalarında ise iletilen emisyon çalışmasında 15 cihaz kimliklendirilmiş olup %99,8 başarımları sağlanırken havadan elektromanyetik sinyaller üzerinden yapılan çalışmada aynı model iki cihaz %100 oranında başarımları ile kimliklendirilmiştir. Yapılan çalışmalarda cihazların stabil çalışmasına yönelik analizleri de yapılarak sistemlerin avantaj ve dezavantajları belirlenmiştir. Böylece kritik ortam ve sistemlerde bulunan her çalışma koşulundaki elektronik cihaz için kimliklendirme yöntemi önerilmiş olup bunların ilgili yerlerde kullanılabilmesi için literatüre katkı sağlanmıştır.

Anahtar Kelimeler: Siber güvenlik, cihaz kimliklendirme, derin öğrenme, sinyal işleme, sistem güvenliği

Identification of Electronic Devices Through Signals Emitted and Produced Using Deep Learning Methods

Furkan Hasan SAKACI

Department of Electronics and Communications Engineering

Doctor of Philosophy Thesis

Supervisor: Prof. Dr. Tulay YILDIRIM

The presence of electronic devices in critical environments and systems can complicate security assessments. Conducting security checks after converting signals into digital formats poses a significant risk, as the compromise of digital identities or certificates can lead to the impersonation of devices. This thesis investigates the identification of devices under three distinct categories using raw signal formats: wired signals, wireless signals, and emitted electromagnetic signals. Ethernet signals were used as the representative wired signals, Wi-Fi and LoRa signals as wireless signals, and transmitted as well as airborne electromagnetic emissions as electromagnetic signals. To develop the proposed systems, signals were initially collected from devices defined within the systems. Depending on the protocol used, the collected signals were analyzed and labeled with the identities extracted from the decoded signal packets. The curated datasets were then utilized to train deep learning models, enabling the generation of device identities based on raw signals. These models were subsequently applied to verify device identities, thereby enhancing the security of critical environments and systems.

The results demonstrate the effectiveness of the proposed methods. Identification based on Ethernet signals achieved a 98.7% success rate in distinguishing two identical devices of the same model. In the Wi-Fi signal study, six devices with identical specifications were identified with a success rate of 99.47%. Similarly, the LoRa signal study achieved a 99% success rate in identifying four different devices. Furthermore, long-term testing of LoRa signals revealed that the system could maintain high accuracy even with minimal signal data, requiring only one packet per hour for effective training. In the electromagnetic signal study, 15 devices were identified with a 99.8% success rate using transmitted emissions, while airborne electromagnetic emissions enabled the identification of two identical devices of the same model with 100% accuracy. Additionally, stability analyses were conducted to evaluate the reliability of the proposed methods, highlighting their advantages and limitations. This comprehensive study offers a novel identification approach tailored to electronic devices operating under various conditions in critical environments and systems. The findings provide valuable insights and practical contributions to literature, emphasizing the potential applicability of these methods in relevant fields.

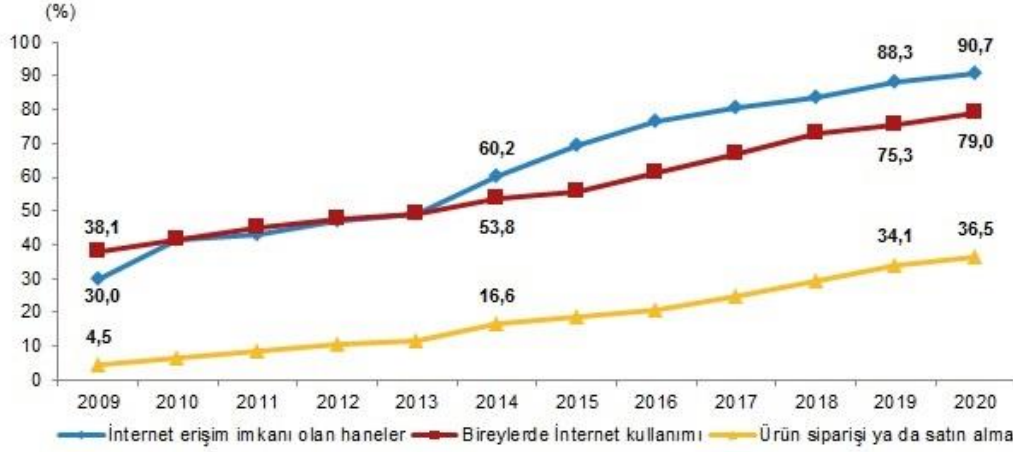
Keywords: Cybersecurity, device identification, deep learning, signal processing, system security

1 GİRİŞ

Gelişen Dünya’da, küresel ölçekte elektronik cihazların kullanımı önemli ölçüde artmıştır. Bu cihazlar haberleşme, beyaz eşya, savunma sanayi gibi farklı sektörlerde yaygın olarak kullanılmaktadır. Bu trend, taleplerin değişmesiyle birlikte mekanik sistemlerin yerini daha küçük, daha konforlu ve daha etkili olan elektronik sistemlere bıraktığını göstermektedir. Fabrikalar, evler, kampüsler, taşıtlar gibi çeşitli alanlarda elektronik cihazlar verimliliği artırmak, süreçleri otomatikleştirmek, enerji tasarrufu sağlamak ve kullanıcıya daha iyi bir deneyim sunmak için kullanılmaktadır. Otomasyon sistemleri, fabrikalarda üretim süreçlerinin optimize edilmesini sağlar. Savunma sanayiinde ise elektronik cihazlar, güvenlik sistemlerinde, iletişim ağlarında ve askeri teçhizatın kontrolünde kullanılmaktadır. Bu gelişmeler, elektronik cihazların önemini ve yaygınlığını artırmıştır. Teknolojik ilerlemelerle birlikte daha da küçülen, daha güçlü ve daha verimli elektronik cihazlar geliştirilmektedir. Araştırmalar nano teknoloji, mikroelettronik, yapay zekâ gibi alanlarda yapılmaktadır ve gelecekte elektronik cihazların daha da yaygınlaşması ve daha gelişmiş işlevlere sahip olması beklenmektedir [1]–[3].

Küresel bir istatistik kurumu olan Statista'ya göre, 2022 yılında tüketiciler tarafından 726 milyar dolar değerinde tüketici elektroniğı ürünü satın alınmıştır [4]. Bu istatistik, tüketici elektroniğı sektörünün hızla büyüdüğünü ve insanların elektronik cihazlara olan taleplerinin arttığını göstermektedir. Gelişen teknoloji, daha gelişmiş ve çeşitli elektronik cihazların piyasaya sürülmesini sağlamakta ve tüketicilerin bu ürünlere olan ilgisini artırmaktadır. Elektronik cihazların küresel ekonomideki önemini ve hızla büyüyen bir sektör olduğunu göstermektedir. Türkiye İstatistik Kurumu’nun (TÜİK) yaptığı bir istatistiğe göre ise internet

kullanımı araştırılmıştır. Hane halkının yüzdesel olarak internet kullanımına yönelik grafiği Şekil 1.1 [5] ile verilmiştir. Grafikten de anlaşılabileceği gibi elektronik ürünlerin tüketimi her geçen sene daha da artmaktadır.



Şekil 1.1 İnternet kullanımının yıllara göre kullanım grafiği

Elektronik cihazlardaki kullanımın artışı bazı güvenlik problemlerini de beraberinde getirmiştir. Özellikle haberleşme teknolojileri ve internet sebebi ile yaşanan mağduriyetler her sene daha da artmaktadır [6]–[8]. Her ne kadar toplum bilinçlendirilmeye çalışılarak bunların önüne geçmek için çaba gösterilse de bu durumun önüne tam anlamı ile geçilememektedir. Sivil endüstride olduğu kadar savunma endüstrisinde de güvenliğin sağlanması çok önemlidir ve özellikle cihazların taklit edilebilir yapıda olması büyük problemlere yol açmaktadır. Cihazlarda ve sistemlerde kullanılan elektronik kartların elektronik karakteristiklere bağlı olarak benzersiz kimliklerinin çıkarılması oldukça önemli bir konu olmuştur.

Elektronik kartların ve sistemlerin benzersiz kimliklerinin çıkarılması, elektronik karakteristiklere dayanan önemli bir araştırma konusudur [9]–[12]. Bu benzersiz kimlikler, cihazları ve bileşenleri benzersiz bir şekilde tanımlamak ve izlemek için kullanılır. Elektronik kartların benzersiz kimliklerinin doğru bir şekilde tespit edilmesi ve kullanılması, birçok alanda önemli avantajlar sağlamaktadır. Benzersiz kimlikler, cihazların takip edilebilirliğini artırır ve izleme süreçlerini güçlendirmektedir. Özellikle büyük ölçekli ağlar veya karmaşık sistemlerde cihazların benzersiz kimlikleri, yöneticilere cihazların durumunu ve konumunu

kolaylıkla belirleme imkânı vermektedir. Bu da sorun giderme, güvenlik yönetimi ve verimlilik açısından büyük bir avantaj sağlamaktadır. Ayrıca, elektronik kartların benzersiz kimlikleri, güvenlik mekanizmalarının etkin bir şekilde katkıda bulunmaktadır. Kimlik doğrulama ve yetkilendirme süreçlerinde cihazların benzersiz kimlikleri kullanılarak güvenlik kontrolleri sağlanmakta ve bu sayede yetkisiz erişim ve taklit girişimleri engellenerek sistemlerin güvenliği arttırmaktadır.

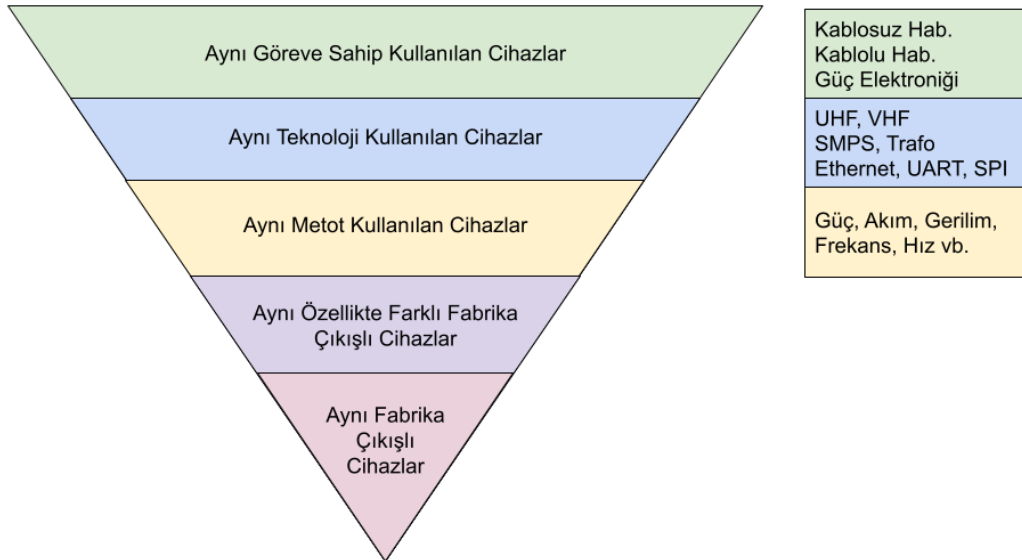
Elektronik cihazların üretimi sırasında bileşenler arasında ve bileşenlerin kendisinde tolerans değerleri bulunmaktadır. Bu tolerans değerleri, elektronik cihazların elektronik karakteristiklerinde doğal olarak ortaya çıkan farklılıkları ifade etmektedir [13]. Elektronik bileşenlerin tolerans değerleri, örneğin dirençlerin nominal değerlerinden sapma, kapasitörlerin kapasitans değerlerindeki değişim gibi faktörlerden kaynaklanabilmektedir. Toleransların birbirlerinden farklı değerde olması üretim sürecindeki farklılıklardan, malzeme özelliklerinden ve diğer etkenlerden oluşmaktadır. Bu durum, aynı fabrikadan üretilen elektronik cihazların bileşen toleranslarına bağlı olarak farklı elektronik karakteristiklere sahip olabileceği anlamına gelmektedir. Bu nedenle, devre kartlarının benzersiz kimlikleri elektronik karakteristikleri üzerinden oluşturulması durumunda aynı fabrikadan üretilse bile benzersiz olarak oluşturulabilmektedir. Elektronik karakteristikleri kullanarak cihazları birbirinden ayırmak için elektriksel özellikler, frekans tepkisi, spektral özellikler, fiziksel özellikler ve optik özellikler gibi birçok yöntem mevcuttur.

- **Elektriksel Özellikler:** Cihazların elektriksel özellikleri, benzersiz bir şekilde farklılık gösterebilir. Örneğin, direnç, kapasitans, endüktans gibi elektriksel özellikler cihazların karakteristiğini belirler ve bu özelliklerin ölçümüyle cihazlar arasındaki farklılıklar tespit edilebilir.
- **Frekans Tepkisi:** Elektronik cihazların frekans tepkisi, sinyal işleme veya iletişim uygulamalarında önemli bir özelliktir. Her bir cihazın frekans tepkisi benzersiz olabilir ve bu tepkilerin analiziyle cihazların ayırt edilmesi mümkün olabilir.
- **Spektral Özellikler:** Elektronik cihazların spektral özellikleri, sinyal analizi ve spektrum analizi gibi tekniklerle incelenebilir. Cihazların

ürettikleri veya işledikleri sinyallerin spektral özellikleri, cihazlar arasındaki farklılıkları ortaya koyabilir.

- **Fiziksel Özellikler:** Elektronik cihazların fiziksel özellikleri de ayırt edici olabilir. Boyut, şekil, malzeme, renk gibi özellikler cihazları birbirinden ayırmak için kullanılabilir.
- **Optik Özellikler:** Bazı elektronik cihazlar, optik özelliklere sahip olabilir. Örneğin, ışık emisyonu, optik sensörler veya ekran teknolojileri gibi özellikler cihazları tanımlamak için kullanılabilir.

Elektronik devreler kablolu haberleşme, kablosuz haberleşme ve güç elektroniği cihazları gibi herhangi bir haberleşmeye sahip olmayan yapılardan oluşabilmektedir. Kritik görev bölgelerinde bulunan cihazların taklit edilebilir ya da kimliklerinin kopyalanabilir olması sistem güvenliği açısından büyük önem arz etmektedir. Cihazların kimliklendirilmesi açısından görev tanımına, teknolojisine ve metot yapısına göre belirli bir hiyerarşi ile oluşturulmuş olan taksonomik sınıflandırılması Şekil 1.2 ile verilmiştir. Bu hiyerarşide görüldüğü üzere aşağı doğru gidildikçe iki ayrı elektronik devrenin kimliklendirilmesi zorlaşmaktadır. Tez çalışması kapsamında hiyerarşinin en altında bulunan aynı fabrika çıkışlı cihazlar için bile kimliklendirme ve ayırıştırma yapılması üzerine çalışılmıştır.



Şekil 1.2 Cihaz kimliklendirme için kullanılan hiyerarşi

Elektronik devrelerde tolerans, bileşenlerin belirli bir nominal değerden ne kadar sapma gösterebileceğini belirten bir parametredir. Tolerans genellikle yüzde (%) cinsinden ifade edilir ve elektronik bileşenlerin belirli bir tolerans aralığına sahip olduğunu gösterir. Elektronik devre tasarımında tolerans, devrenin istikrarlı bir şekilde çalışmasını sağlamak için önemlidir. Devrenin performansının daha tutarlı olmasına katkıda bulunması için özellikle hassas uygulamalarda, düşük toleranslı bileşenler tercih edilmektedir. Tolerans ayrıca çevresel koşullar altında bileşenlerin davranışını anlamak için de kullanılır. Sıcaklık değişimleri, voltaj dalgalanmaları ve diğer çevresel faktörler, toleransın devre performansına olan etkilerini belirlemek için dikkate alınmalıdır. Tolerans değerinin yüksek olması devre kararlılığını etkilerken düşük olması ise devre kartlarının elektronik karakteristiğini çıkarabilmek için daha yüksek çözünürlüklü Analog Dijital dönüştürücülerin (Analog-Digital Converter, ADC) ya da örnekleyicilerin kullanılması ile mümkün olmaktadır. Bu nedenle cihaz kimliklendirme tasarımının kullanılacağı sistemlerde kullanılacak olan modül seçimi buna göre belirlenmelidir. Elektronik karakteristiğe bağlı kimliklerin çıkarılabilmesi için öncelikle kimliklendirmenin tarihçesini ve literatürünü sonrasında ise kullanılacak teknolojilerini ele almak gerekmektedir.

1.1 Kimliklendirmenin Tarihçesi

Elektronik cihazlar ve ürünler tabiatın taklit edilerek tasarlandığı bakış açısıyla düşünüldüğünde kimliklendirme için öncelikli olarak canlıların benzersiz nasıl kimliklendirildiğine bakılması gerekmektedir. Bu bakış açısı ile düşünüldüğünde ses izi, odontoloji, iskelet tanımlama ve parmak izleri ile canlılar için benzersiz kimliklendirme oluşturulabilmektedir [14]–[17]. Canlılar üzerindeki kimliklendirmenin tarihçesine bakıldığında zaman ilk olarak antik çağlarda, kimlik doğrulamanın insanların tanınmasıyla gerçekleştirildiği görülmektedir. İnsanlar, yüz hatları, vücut şekilleri, ses tonu gibi özelliklerini kullanarak birbirlerini tanımaktadırlar. Orta Çağ'da ise, mühürler ve imzalar gibi fiziksel işaretler kimlik doğrulama için kullanıldı. Özellikle resmî belgelerde mühür kullanımı oldukça yaygın olduğu görülmektedir. 18. Yüzyılda, fotoğrafın icadıyla birlikte fotoğraflar kimlik doğrulama için kullanılmaya başlandı. 19. Yüzyılda ise günümüzde de

sıkça kullanılan parmak izi tespiti, kimlik doğrulama yöntemleri arasında önemli bir adım oldu. 1892 yılında İngiliz bilim insanı Sir Francis Galton, parmak izlerinin benzersiz olduğunu ve kişiyi tanımlamak için kullanılabileceğini keşfetti. Antik çağlardan günümüze gelinceye kadar anlaşılabileceği üzere teknolojinin gelişimine bağlı olarak birçok farklı yaklaşım ve yöntemlerle kimliklendirme yapılmıştır [18]–[20].

Günümüzde kimliklendirme, cihazların artışına bağlı olarak artık sadece insanlarda değil ayrıca cihazlarda da önemli bir konu olmaktadır. Cihazlar ve sistemlerin de kimlik bilgilerine sahip olması ve bunları kullanarak erişim sağlaması gerekmektedir. Genel olarak Nesnelerin İnterneti (Internet of Things, IoT) ve Makineden Makineye (M2M) iletişimde, güvenlik konusu hayati bir öneme sahiptir, çünkü bu teknolojilerin geniş bir yüzey alanına ve farklı bileşenlere yayılan bir yapıya sahip olması, güvenlik açıklarının ve saldırı potansiyelinin artmasına neden olmaktadır [21]–[23]. Bu tür senaryolarda, cihazlar belirli bir ağa veya hizmete erişmek için kimlik doğrulama sürecinden geçerler. Bunun için cihazların benzersiz bir kimlik bilgisine sahip olması ve bu kimlik bilgisini kullanarak kendilerini doğrulayabilmeleri gerekmektedir. Cihaz kimliklendirme süreci, genellikle önceden tanımlanmış kimlik bilgilerini içeren sertifikalar veya erişim anahtarları kullanılarak gerçekleştirilir [24]. Cihazlar, bu kimlik bilgilerini kullanarak hedef ağ veya hizmete kimlik doğrulama talebinde bulunur ve erişim izni alırlar. Bu kimliklendirme süreci, cihazların güvenli bir şekilde haberleşebilmesini ve yetkisiz erişimlerin engellenmesini sağlar. Aynı zamanda, cihazların güvenlik politikalarına uygun olarak yetkilendirilmelerini sağlar ve ağ veya hizmetin güvenliğini artırır. Kimliklendirme sürecinde insanlardan cihazlara doğru bir kayma yaşanmasının nedeni, giderek artan sayıda cihazın birbiriyle iletişim kurması ve otomatik işlemlerin gerçekleşmesidir. Bu durum, güvenliğin önemini artırmış ve kimliklendirme yöntemlerinin cihazlar için uyarlanması gerektirmiştir. Sonuç olarak, kimliklendirme süreci artık sadece insanların değil, aynı zamanda cihazların da erişim kontrolünü sağlamak için kullanılmaktadır [25]–[27]. Bu, güvenliğin sağlanması ve yetkisiz erişimlerin engellenmesi açısından önemlidir.

Cihazlar için kullanılan kimlik sertifikaları ya da erişim anahtarları yapay olarak cihazlara tanımlanmakta olup bilinmeyen cihazlar tarafından taklit edilebilir bir yapıdadır. Özellikle güvenlik kontrolünün sinyaller dijital forma dönüşmesinden sonra yapılması ağ saldırılarına ve sızmalarına karşı cihazları savunmasız bırakmaktadır. Bu nedenle cihazların kendi elektronik karakteristiklerine bağlı olarak oluşturulan kimlikler ile yapılması oldukça popüler olmuştur. Bunun için ise Radyo Frekans haberleşmesi üzerinden, kablolu haberleşme sinyalleri üzerinden ve cihazların yaydığı elektromanyetik emisyon üzerinden kimliklendirmeler yapılabilmektedir.

Spesifik Verici Tanımlaması (Specific Emitter Identification, SEI), bir elektromanyetik kaynağın (verici veya cihaz) fiziksel özelliklerine dayalı olarak tanımlanması ve diğer benzer cihazlardan ayrıştırılması sürecidir [28]–[30]. Bu yöntem, cihazların ürettiği ince fiziksel imzaları kullanarak kimliklendirme yapılmasını sağlar. SEI, her cihazın benzersiz üretim varyasyonları nedeniyle, gönderdiği sinyalin genlik, faz, frekans veya dalga formunda küçük, ayırt edici özellikler taşır. Bu varyasyonlar, cihazların elektromanyetik emisyonlarında tespit edilebilir ve SEI sistemleri, bu tür farklılıkları analiz ederek her bir cihaz için benzersiz bir imza oluşturur. Bu teknik özellikle güvenlik, izinsiz erişim tespiti ve sinyal taklit saldırılarına karşı savunma amacıyla kullanılır. SEI ile belirli bir vericinin kimliği doğrulanabilir ve taklitçi cihazlar veya yetkisiz cihazlar sistemden ayrıştırılabilir.

1.2 Literatür Özeti

Elektronik cihazların sinyalleri üzerinden kimliklendirilmesi için literatürde matematiksel modellemeler ve makine öğrenmesi mimarileri kullanılarak yapılan çalışmalar bulunmaktadır. Kimliklendirme çalışmaları kablosuz sinyaller, kablolu sinyaller ya da elektromanyetik emisyon sinyalleri olmak üzere üç ayrı başlıkta incelenmektedir. Bu nedenle literatürdeki çalışmaların daha kapsamlı verilebilmesi amacıyla Bölüm 1.2.1 ile kablosuz haberleşme üzerinden, Bölüm 1.2.2 ile kablolu haberleşme üzerinden ve Bölüm 1.2.3 elektromanyetik emisyon sinyalleri üzerinden yapılan kimliklendirme çalışmaları üç ayrı başlıkta literatür incelemesi yapılmıştır.

1.2.1 Kablosuz Haberleşme

Gelişmekte olan Dünya’da, telefon, radyo, televizyon ve internet gibi iletişim teknolojilerinin kullanımı her geçen gün artmaktadır. Bu artış, elektronik ürünlerde hız, güvenlik ve konforu ön plana çıkarmıştır. Sadece insanlar arasındaki iletişim değil, aynı zamanda yaygın yapay zekâ teknolojileri ile cihazlar arasındaki iletişim de son derece önemli hale gelmiştir. Özellikle, insan müdahalesi olmaksızın bağımsız bir şekilde çalışan elektronik ürünlerin davranışları, literatürde popüler bir konu haline gelmiştir. Aynı ağa bağlı birden fazla cihazın bulunduğu fabrikalarda, kampüslerde ve kamu ağlarında tanımlanamayan cihazların varlığı, ağ güvenliğine bir tehdit oluşturmaktadır.

Literatürde, OSI modelinin farklı katmanlarında farklı yöntemleri kullanarak ağ güvenliğini sağlamak amacıyla uygulamalar bulunmaktadır. Bilgisayar ağlarında Medya Erişim Kontrolü (Media Access Control, MAC) filtreleme, cihazların MAC adreslerine dayalı olarak ağa erişimi kontrol etmek için yaygın olarak kullanılan bir güvenlik özelliğidir. MAC filtreleme kullanarak, ağ yöneticileri cihazların benzersiz MAC adreslerine dayalı olarak belirli cihazlara ağ erişimine izin verebilir veya engelleyebilirler [31]–[33]. Ayrıca, SSL (Secure Sockets Layer) gibi sertifikalar kullanarak paketleri korumak da mümkündür [34], [35]. Sung-Min Kim ve diğer yazarlar, çalışmalarında TLS (Transport Layer Security) yük verilerinden hizmet imzalarını otomatik olarak oluşturmak ve ağ trafiğini uygulama hizmetlerine göre sınıflandırmak için yeni bir yöntem önermişlerdir [36]. Sertifikalar, gönderenin kimliğini doğrulamak ve verilerin bütünlüğünü sağlamak için bir yol sağladığından, yetkisiz erişimi engellemek için oldukça etkilidir. Sertifikalar, genellikle TLS gibi güvenli iletişim protokollerinde, bir istemci ile bir sunucu arasında güvenli bir bağlantı kurmak için kullanılır [37], [38]. Ancak, sertifikaların kendilerinin bilinmeyen bir kişi veya kurumun eline geçmesi durumunda bir güvenlik riski oluşturabileceği literatürde önemli bir endişe konusudur. Bir saldırgan geçerli bir sertifikaya erişim sağlarsa, meşru göndereni taklit edebilir ve paket içeriğini şifreleyerek hassas bilgileri ortaya çıkarabilir veya yetkisiz eylemler gerçekleştirebilir. Bu nedenle, potansiyel saldırgan cihazları doğrudan OSI modelinin en alt katmanı olan fiziksel katmanda [39] engelleyebilen bir yapıya sahip olmak gereklidir [40]–[42].

İletişim ortamını dinleme ve analiz yapma yeteneğine sahip varlıkların bulunmasından dolayı özellikle kablosuz iletişimde büyük bir güvenlik endişesi bulunmaktadır. Bu nedenle, her cihaza özgü yarıiletken ve pasif bileşenler tarafından üretilen farklı sinyalleri kategorize etmek zorunlu hale gelmektedir. Akademik literatürde, bu yaklaşım genellikle RF Parmak İzi (RF Fingerprinting) olarak adlandırılır ve WiFi gibi 802.11 standardında çalışan cihazlarda, Bluetooth gibi 802.15.1 standardında çalışan cihazlarda, ZigBee gibi 802.15.1 standardında çalışan cihazlarda uygulanır. RF Parmak İzi metodolojisi, antenler aracılığıyla Yazılım Tanımlı Radyo (Software Defined Radio, SDR) üzerinden elde edilen ham Radyo Frekansı tabanlı I/Q (In-Phase ve Quadrature) sinyallerinin alınmasını içerir.

SDR, geleneksel radyo iletişim sistemlerinden farklı bir yaklaşım sunarak, alıcı ve verici fonksiyonlarını yazılım tarafından programlanabilir bir donanım üzerinde gerçekleştiren bir teknoloji olarak öne çıkmaktadır [43]. Bu sistem, radyo frekansı sinyallerini işlemek ve iletmek için I/Q verilerini kullanır. I/Q verileri, bir radyo sinyalini temsil etmek için kullanılan temel bir kavramdır. In-Phase (I) bileşeni, sinyalin gerçel kısmını, Quadrature (Q) bileşeni ise sinyalin hayali kısmını temsil eder. Bu iki bileşen bir araya geldiğinde, kompleks sayılarla ifade edilen bir veri elde edilir. Bu kompleks sayı temsil biçimi, genellikle dijital sinyal işleme (Digital Signal Processing, DSP) algoritmalarında kullanılır.

SDR'nin önemli avantajlarından biri programlanabilir olması ve geniş frekans aralıklarında çalışabilmesidir. Yazılım tarafından yönetilen alıcı ve verici fonksiyonları, kullanıcılara geniş bir frekans yelpazesi üzerinde çalışma esnekliği sağlar. Bu esneklik, çeşitli uygulama alanlarında SDR'nin kullanılmasını mümkün kılar. SDR ile alınan I/Q verileri, genellikle dijital işlemlerden geçirilerek sinyalin demodülasyonu, filtreleme ve işleme aşamalarında kullanılır. Bu sayede, gelen sinyallerin dijital olarak işlenmesi ve çeşitli modülasyon formatlarına uyum sağlanması mümkün hale gelir. Bu esnek ve programlanabilir yapı, iletişim sistemlerinin hızla değişen ihtiyaçlarına uyum sağlama yeteneği sunar.

Alınan sinyaller, ilgili iletişim protokollerinde kullanılan çözme teknikleriyle analiz edilir. Daha sonra bu sinyallere benzersiz adresler (MAC, cihaz adresi, ID vb.) ile eklenir ve sınıflandırma amaçları için makine öğrenimi tabanlı modellerle

birlikte kullanılır [44]–[47]. Makine öğrenmesi, belirli giriş ve çıkış parametrelerine bağlı ağ modeli oluşturulması ve ağ modelinin veri ile eğitilerek kullanılmasını sağlamaktadır [48]–[50]. Makine öğrenmesinin sınıflandırma metodu ile her cihazın benzersiz bir kimliğe sahip olması üzerine çalışılmıştır. Sınıflandırma, kullanılan verilerin etiketlenmesi ile kategorilere ayrılması olarak ifade edilmektedir [51].

Cihaz kimlikleri cihazların elektronik karakteristiklerine bağlı olarak oluşturulmaktadır. Elektronik kart aynı komponentlere ve aynı yapıya sahip olsa bile komponentlerin tolerans değerinden dolayı farklılıklar oluşmaktadır. Kimliklendirme çalışmalarında bu farklılıklarından yararlanılarak SDR cihazı ile ortam dinlenmiş ve haberleşme sinyalleri üzerinden benzersiz karakteristikler oluşturulmuştur. Bu çalışmalar literatürde RF Parmak İzi dışında RF-DNA ve RF Kimliklendirme (Identification) olarak da adlandırılabilir [52]–[54].

Kablosuz haberleşme sistemlerinde kullanılan birçok protokol ile kimliklendirme çalışmaları yapılmıştır. Bu protokollerden LoRa teknolojisi uzun menzilli ve dış ortamda kullanılabilirliği nedeniyle radar ve IoT çalışmalarında oldukça sık kullanılmaktadır. LoRa, Cıvıltı Yayılım Spektrumu (Chirp Spread Spectrum, CSS) teknolojisinden türetilen bir kablosuz modülasyon tekniğidir [55]. Bu nedenle demodülasyon ve çözümleme çalışmaları için CSS modülasyon tekniğinin altyapısı kullanılmaktadır [56]–[58]. Literatürde, LoRa gibi uzun menzilli haberleşmeye sahip sistemler için farklı teknoloji ve matematiksel model yapıları kullanılarak yapılan kimliklendirme çalışmaları bulunmaktadır [59]–[62]. Literatürdeki çalışmalardan birinde Robyns ve arkadaşları denetimli makine öğrenimi ve sıfır vuruşlu (zero-shot) öğrenme ile görüntü sınıflandırma kullanarak Lora cihazlarını parmak izi için yeni bir metodoloji önerir ve analiz eder [60]. Başka bir çalışma kapsamında da Hamdaoui ve Elmaghrib [62], literatürdeki LoRa kimliklendirme çalışmalarına benzer bir şekilde cihaz kimliklendirmelerini oluşturmuştur. Sonrasında da donanım distorsiyonlarının neden olduğu bant dışı bozulma bilgilerinin engellendiği yeni bir teknik sunmuştur.

Haberleşme sistemlerinde paketlerin çözülmesi hız gerektirmesi sebebiyle bir donanım ile yapılmaktadır. Yazılım ile çözümleme için yüksek hızlı ya da paralel işlemcilerle ihtiyaç vardır. Literatürde FPGA kullanılarak paralel çözümleme

çalışmaları vardır [63]. Bu çalışmada, FPGA paralel yapısı sayesinde WiFi sinyallerinin çözümlemesini paket kaçırmadan yapabilmektedir. Ayrıca WiFi sinyallerinin GPU kullanılarak çözümlendiği bir çalışmada bulunmaktadır [64]. Burada WiFi sinyallerinin çözümlemesi CPU ve GPU'da ayrı ayrı yapılarak hız analizi yapılmıştır.

1.2.2 Kablolu Haberleşme

Kablolu haberleşme sistemleri, elektriksel sinyallerin kullanımına dayalı olarak, veri iletimi ve alımı sağlayan bir iletişim paradigması sunar. Bu sistemler, analog sinyallerin iletimi, işlenmesi ve alınması üzerine odaklanarak, bilgi aktarımını sağlayan elektriksel sinyallerin kompleks bir dizi işleme tabi tutulmasını gerektirir. Analog sinyaller, sürekli değişen voltaj veya akım seviyelerini temsil eder ve genellikle ses, video veya diğer türdeki verileri taşımak üzere kullanılır. Ancak, kablolu iletişim sistemlerinde sinyallerin güvenli iletimi ve doğru bir şekilde alınabilmesi için, bu analog sinyallerin dijital formata dönüştürülmesi gerekmektedir. Bu dönüşüm sürecini gerçekleştiren temel bileşenlerden biri olan ADC, analog sinyalleri belirli bir örnekleme periyodunda örnekleyerek ve bu örneklemeleri dijital bir temsile dönüştürerek çalışır.

Dijital sinyallerin oluşturulmasının ardından, bu sinyaller daha fazla işleme tabi tutulur. Bu işlemler arasında sinyal güçlendirme, filtreleme ve modülasyon yer alır. Güçlendirme, sinyalin iletim hatları boyunca zayıflamasını dengelemek için kullanılırken, filtreleme, sinyalin istenmeyen frekans bileşenlerinden arındırılmasına yöneliktir. Modülasyon ise, dijital sinyallerin taşınmasını sağlamak üzere bir taşıyıcı sinyalle birleştirilmesini ifade eder. Kablolu iletişimde, bu süreçlerin yanı sıra elektriksel sinyallerin iletim hatları boyunca uzaklık, çevresel etkenler ve elektromanyetik girişimlere karşı direnç göstermesi gereklidir. İletim hattındaki güvenilirlik ve hata oranının düşük olması, iletilen verinin bütünlüğünün korunması açısından kritik öneme sahiptir. Sonuç olarak, kablolu iletişim sistemleri, analog sinyallerin dijital forma dönüştürülmesi, işlenmesi ve iletimi süreçlerini içeren karmaşık bir teknolojik altyapıyı barındırır. Bu süreçler, modern iletişim altyapısının temelini oluşturan ve bilgi aktarımının güvenli ve etkili bir şekilde gerçekleştirilmesini sağlayan önemli adımlardan biridir.

Kablolu bağlantılarda fiziksel katmanda kimliklendirme yapmak için analog sinyal üzerinden yapılan bir çalışmada [65] farklı cihazlardaki Ethernet sinyalleri analog olarak okunup filtre eşleştirme yöntemi ile cihazların parmak izleri çıkarılmıştır. Buna benzer farklı bir çalışmada [66] ise Ryan M. Gerdes ve diğer yazarlar filtre eşleştirme yöntemi ile 27 farklı cihazın kimliklendirilmesi üzerine çalışmışlardır. Filtre eşleştirme yönteminde bilinmeyen sinyalde şablonun varlığını tespit etmek için bilinen bir gecikmeli sinyal veya bilinmeyen bir sinyalle ilişkilendirilerek eşleşen bir filtre elde edilir. Filtre eşleştirme ile yapılan kimliklendirme çalışmalarında da bu şekilde sinyaller üzerinden kimlikler oluşturulmaktadır. Filtre eşleştirmeye benzer şekilde yapılan bir çalışmada [67] Manchester kodlama tekniğinde kullanılan ideal sinyal ile gerçekteki sinyalin adaptif filtreye girmesinden sonra çıkan sinyal kullanılarak kimliklendirme yapılmıştır. Az sayıdaki cihazlar için bu çalışmalar kullanılabilir olsa da çok fazla cihazın bulunduğu ve farklı kodlama tekniğine sahip cihazlarla birlikte kullanım için farklı filtre tasarımları da gerektirmesinden dolayı iş yükü gerektirmektedir. Çok fazla elektronik cihazın bulunduğu ortamlarda cihazların analog sinyali üzerinden kimliğinin çıkarılması literatürde önemli bir konudur. Ethernet sinyallerinden kaynaklı emisyon verileri kullanılarak cihazların ayırt edildiği bir çalışma da bulunmaktadır [68]. Çalışma kapsamında Carbino ve diğer yazarlar Koşullu Takımyıldız Tabanlı-Ayrı Yerel Nitelik (Conditional Constellation Based-Distinct Native Attribute, CB-DNA) yöntemini kullanarak kimliklendirme üzerine çalışmışlardır. Çalışmada yakın alan probu kullanılarak CAT-6 Ethernet kablosu üzerinden 16 farklı cihaz için sinyaller alınmıştır. Alınan sinyaller CB-DNA yöntemi ve matematiksel işlemlerle kategorilendirilerek cihazlar ayırt edilmiştir. Bu çalışmada analog sinyal yerine sinyalin emisyon seviyesi üzerinden kimliklendirme yapılması cihazların metal yoğun olduğu veya farklı elektromanyetik emisyon sinyallerinin de olduğu ortamlarda sistemin stabil sonuç vermemesine neden olabilir. Bu nedenle Ethernet kimliklendirme çalışmalarında analog sinyal üzerinden yapılan çalışmaların daha verimli sonuç vereceği ön görülmektedir. Analog sinyal üzerinden yapılan bir çalışmada [69] ise Liu ve diğer yazarlar toplam 65 adet farklı Ethernet kartını sınıflandırmıştır. Çalışmada farklı kodlama tekniğine sahip Ethernet sinyallerinden veriler toplanmış ve spektrum tabanlı özellikler çıkarılarak kimliklendirme çalışması yapılmıştır. Her

ne kadar bu çalışma da analog sinyal kullanılsa da spektrum tabanlı bir çalışma olması ve zaman domenindeki bilginin kaybedilmesi cihazların daha da artması durumunda sınıflandırmanın kötüye gitmesine sebep olmaktadır. Benzer biçimde başka bir çalışmada [70] Fiber Optik Ethernet sinyalleri Bitişik Takımyıldız İzi Şekli (Adjacent Constellation Trace Figure, ACTF) yöntemi kullanılarak Ethernet çerçevesi içinde sırası ile bulunan semboller üzerinden I/Q formuna dönüştürülmüş ve Takım Yıldızı (Constellation Diagram) oluşturulmuştur. Oluşturulan bu form 2D-CNN ile derin öğrenme yapısında kullanılarak kimliklendirme yapılmıştır. Bu çalışmada da Ethernet sinyallerin ham hali yerine özellik çıkarımı yapılarak sinyalde olası kayıplara sebep olabilmektedir

1.2.3 Elektromanyetik Emisyon

Elektromanyetik emisyon, elektrikli cihazların çevreye yaydığı elektromanyetik radyasyonu ifade etmektedir. Cihazların içinde bulunan elektronik devreler ve bu devrelerdeki komponentlerin birbirleri arasındaki etkileşimden kaynaklı olarak oluşmaktadır. Özellikle güç elektroniği gibi yüksek akıma sahip ve anahtarlama devrelerinde elektromanyetik emisyon değeri yükselmektedir. Bu tür devrelerde, anahtarlama sırasında hızlı voltaj ve akım değişimleri gerçekleşir ve bu da parazitik etkileşimlere neden olabilir.

Elektromanyetik emisyonla etki eden faktörler arasında elektriksel tasarım, sinyal yolları, yerleştirme ve kablolama, tolerans, parazitler ve girişimler, elektriksel güç ve frekans gibi faktörler bulunmaktadır [71]–[73].

- **Elektriksel Tasarım:** Elektrik devrelerinin tasarımı, devre bileşenlerinin düzenlenmesi ve devre kartı düzeni gibi faktörler, elektromanyetik emisyonu etkiler. İyi bir elektriksel tasarım, istenmeyen emisyonların azaltılmasına yardımcı olabilir.
- **Sinyal Yolları:** Sinyal yolları ve iletişim hatları, elektromanyetik emisyonu etkileyen önemli bir faktördür. Yanlış yerleştirilmiş veya uygun şekilde tasarlanmamış sinyal yolları, emisyonları artırabilir.
- **Yerleştirme ve Kablolama:** Elektronik bileşenlerin doğru yerleştirilmesi ve kablolama yöntemleri, elektromanyetik emisyonu etkileyebilir. Yanlış yerleştirme veya kablolama, emisyonları artırabilir.

- **Parazitler ve Girişimler:** Dışarıdan gelen parazitler ve elektromanyetik girişimler, emisyonları etkileyebilir. Örneğin, diğer elektronik cihazlardan kaynaklanan girişimler emisyonları artırabilir.
- **Elektriksel Güç ve Frekans:** Elektrik gücü düzeyi ve frekansı, elektromanyetik emisyon üzerinde önemli bir etkiye sahiptir. Yüksek güç seviyeleri ve yüksek frekanslar genellikle daha fazla emisyon üretebilir.
- **Tolerans Değerleri:** Elektronik devrelerde bulunan komponentlerin ve sinyal yollarının belirli tolerans değerleri bulunmaktadır. Bu tolerans değerlerine bağlı olarak aynı fabrika üretimi olsa bile farklı emisyonlara sahip olmaktadır.

Elektronik devrelerden kaynaklı yayılan elektromanyetik emisyon gücünü hesaplamak için teorik olarak bazı formüller bulunmaktadır. Bu formüller içinden Hertz Dipol Radyasyon formülü (1.1) ile verilmiştir.

$$P = (\mu_0 * I * L)^2 (4 * \pi * r)^2 \quad (1.1)$$

Hertz dipolü, anten olarak kabul edilen bir devredir ve elektromanyetik emisyonu hesaplamak için kullanılmaktadır. Burada parametreler,

P: Radyasyon gücü (watt)

μ_0 : Boşluk permütivitesi (8.85×10^{-12} F/m)

I: Akım (amper)

L: Anten uzunluğu (metre)

r: Mesafe (metre)

olarak ifade edilmektedir. Hertz dipolü radyasyonu formülü, dipolün uzunluğu, akım şiddeti ve alıcı noktasına olan uzaklık gibi faktörlerin etkileşimini açıklamaktadır. Bu formül, anten tasarımı ve elektromanyetik emisyon analizlerinde kullanılmaktadır. Bu formülü kullanarak, belirli bir dipol antenden yayılan elektromanyetik radyasyonun gücünü hesaplanabilir ve alıcı noktasında emisyonun seviyesi tahmin edilebilmektedir [74]. Elektromanyetik emisyonun bir antenden belirli bir mesafede alıcıya iletimini hesaplamak için ise (1.2) ile verilen Friis formülü kullanılmaktadır. Friis formülü, elektromanyetik dalgaların serbest alan (free space) koşullarında yayılmasını temsil etmektedir. Kablosuz iletişim

sistemlerinde iletim gücünün, anten kazançlarının, dalga boyunun ve mesafenin etkileşimini hesaplamak için kullanılmaktadır [75]. İletişim sistemlerinin tasarımında, vericiden alıcıya iletilen gücü tahmin etmek ve iletim performansını analiz etmek için önemli bir araçtır.

$$P_r = \frac{(P_i * G_t * G_r * \lambda^2)}{(16 * \pi^2 * R)^2} \quad (1.2)$$

Verilen formülde kullanılan parametreler;

P_r : Alıcı gücü (watt)

P_i : Verici gücü (watt)

G_t : Verici anten kazancı

G_r : Alıcı anten kazancı

λ : Dalga boyu (metre)

R : Mesafe (metre)

olarak ifade edilmektedir. Bu formüllerle beraber dalgacık teorisi formülü (1.3), elektromanyetik emisyonun yayılmasını ve iletimini hesaplamak için kullanılan bir yöntemdir. Bu yöntem, bir kaynaktan yayılan elektromanyetik dalgaların dalga boyu, frekans ve iletim ortamı gibi parametreleri kullanmaktadır.

$$P = \frac{(4 * \pi * r^2) * S * G * \lambda^2}{(16 * \pi^2 * R)^2} \quad (1.3)$$

Formülde kullanılan parametrelerin açıklaması,

P : Radyasyon gücü (watt)

r : Mesafe (metre)

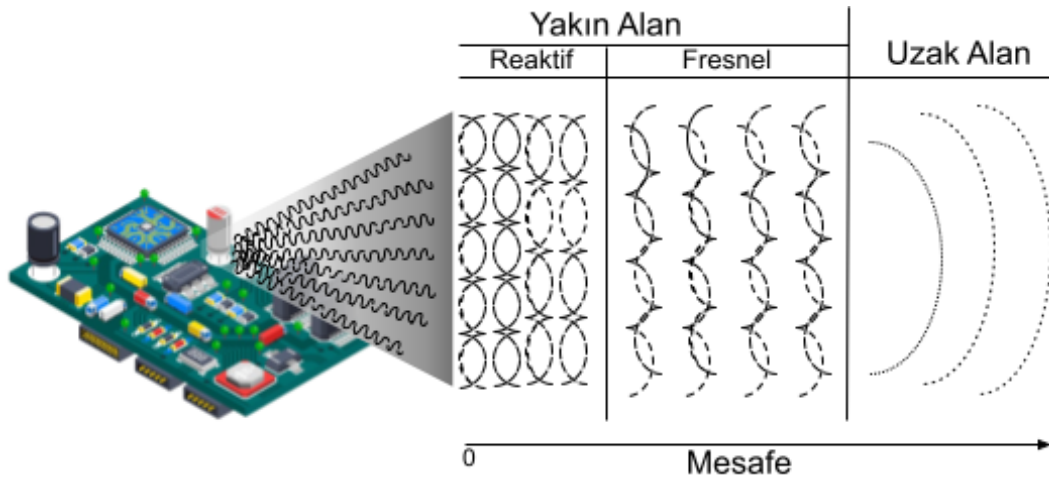
S : Kaynak yoğunluğu (watt/m²)

G : İletim kaybı faktörü

λ : Dalga boyu (metre)

R : Mesafe (metre)

olarak ifade edilmektedir. Elektromanyetik sinyal ölçümleri yakın alan ve uzak alan olarak iki şekilde yapılabilir [76]–[79]. Şekil 1.3 ile verildiği gibi, yakın alan ölçümleri, elektronik bileşenler arasındaki etkileşimlerin daha ayrıntılı gözlemlenmesine olanak tanır. Uzak alan ölçümlerinde ise elektrik ve manyetik alanlardan oluşan elektromanyetik alan, bu bileşenlerin vektörel toplamı olarak ifade edilir. Ölçüm noktası ile sinyal kaynağı arasındaki mesafe dalga boyunu aştığında bu uzak alan olarak sınıflandırılırken, mesafe dalga boyundan daha kısa olduğunda yakın alan olarak kabul edilir. Yakın alan bölgesi ayrıca Reaktif ve Fresnel bölgeleri olarak iki alt kategoriye ayrılır [80], [81].



Şekil 1.3 Elektromanyetik emisyon ölçümünün mesafeye bağlı değişimi

"Reaktif" terimi, elektromanyetik dalgaların etkileşimi sırasında ortaya çıkan endüktif ve kapasitif reaktansı tanımlamak için kullanılır. Bir elektromanyetik dalganın reaktif bileşeni, elektrik veya manyetik alanlarda depolanan enerjiyi temsil eder. Gerçek gücün aksine, reaktif bileşen bir devrenin gerçek gücünün (aktif güç) hesaplanmasında kritik bir rol oynar. Reaktif bileşenler genellikle endüktörler ve kapasitörler gibi cihazlarda bulunur. Bu bölgede, E-Alanı (Elektrik Alan) ve H-Alanı (Manyetik Alan) arasında 90 derecelik bir faz farkı vardır ve bu durum onları reaktif hale getirir. Radyasyon veya yayılmanın gerçekleşebilmesi için, E/H alanlarının birbirine dik ve faz uyumlu olması gerekir.

"Fresnel" terimi, elektromanyetik dalgaların bir ara yüzeyde yansıma ve kırılma sırasında meydana gelen etkileri ifade eder. Özellikle, elektromanyetik bir dalga bir ortamdan başka bir ortama geçtiğinde oluşan yansıma ve kırılma açılarındaki

değişiklikler Fresnel etkileri olarak bilinir. Bu etkiler, optik ve elektromanyetik haberleşme sistemlerinde önemli bir rol oynar. Fresnel yasaları, yansıma ve kırılma açıları arasındaki ilişkileri tanımlar ve elektromanyetik dalgaların bir ortamdan diğerine nasıl geçtiğini açıklar.

Elektromanyetik emisyon ölçümleri için ise doğrudan formüller kullanmak yerine özel ekipmanlar ve test prosedürleriyle birlikte Elektromanyetik Uyumluluk (EMC) testleri yapılmaktadır. Bu ekipmanlar ve prosedürler, EMC gereksinimlerine uyumu değerlendirmek ve olası gelişmiş tasarım veya filtreleme yöntemleri ile iletilen emisyonu azaltmak için kullanılmaktadır. İletilen emisyonun spesifik bir formülü olmamakla birlikte, denklem (1.1-1.3) arasında verilen temel formüller genel bir anlayış sağlamaktadır. Ancak, spesifik bir devre veya EMC gereksinimine yönelik hesaplamalar yapmak için CISPR-25 ve IEC 61000 serisi gibi ilgili standartlar ve kaynaklar, EMC standartları veya ilgili EMC yönergeleri kullanılmaktadır. EMC testlerinden olan iletilen emisyon (conducted emission), elektronik devrelerde oluşan ve iletkenler (kablolar, yollar, devre izleri vb.) üzerinden yayılan elektromanyetik gürültü veya parazit sinyalleri olarak tanımlanmaktadır. Bu emisyonlar, devre elemanlarının ana sinyal üzerine ek olarak yaydığı istenmeyen frekans bileşenleridir.

İletilen emisyon, elektriksel sinyallerin devre elemanları ve iletkenler aracılığıyla iletilirken, bu iletim sürecinde oluşan parazit sinyalleri olarak ortaya çıkmaktadır. Bu emisyonlar, yüksek frekanslı elektriksel sinyallerin devre elemanlarından diğer elemanlara veya ortama yayılması sonucu oluşmaktadır. İletilen emisyon, elektronik devrelerde istenmeyen sinyallerin yayılmasına ve elektromanyetik uyumluluk sorunlarına yol açabilmektedir [82]–[84]. İletilen emisyonun miktarı, devrenin tasarımı, sinyal seviyeleri, frekans aralığı, devre elemanlarının özellikleri ve iletkenlerin düzenlemesi gibi birçok faktöre bağlıdır. İletilen emisyonu azaltmak için devre tasarımında ve elektronik bileşenlerin yerleşiminde çeşitli tedbirler alınabilmektedir.

Devre elemanlarının yüksek frekanslı parazit bileşenlerini bastıran filtreler kullanılabilir, topraklamalar ve sinyal yolları düzenlemeleri optimize edilebilmekte veya ekranlama teknikleri uygulanabilmektedir. Akademik araştırmalarda iletilen emisyon genel olarak EMC konusu altında incelenir. Bu

alıřmalar, iletilen emisyonun sınırlarını belirlemek, standartlara uyum saęlamak, emisyon azaltma teknikleri geliřtirmek ve elektromanyetik uyumluluk gereksinimlerini karřılamak iin stratejiler sunmak amacıyla yapılmaktadır. Akademik alıřmalarda, iletilen emisyonun m, analizi, modellenmesi ve azaltılması gibi konular ele almaktadır. İletilen emisyonun frekans spektrumu analizi, elektromanyetik emisyonun elektriksel sinyaller zerindeki etkileri, EMC test ve sertifikasyon yntemleri gibi konular altında incelenmektedir. Ayrıca, devre tasarımı, topraklama, filtreleme teknikleri ve elektromanyetik ekranlama gibi pratik mler zerine alıřmalar yrtlmektedir.

Cihazların LISN baęlantısı aracılıęıyla aęa baęlı olması durumunda LISN baęlı olamayacaęı yerlerde gvenlik aęı devam etmiř olmaktadır. Dolayısıyla, cihazların pil gcyle alıřtıęı durumlarda veya bir LISN baęlantısının mmkn olmadığı durumlarda sistem gvenlięi risk altında kalmaktadır. Bu sorunu ele almak iin, yakın alan elektromanyetik mlerinin gerekleřtirilmesiyle cihazların kimliklendirilmesi kritik bir nem tařımaktadır. Literatrde, elektromanyetik yayılım kullanarak elektronik cihazları sınıflandıran doęrudan bir uygulama bulunmamaktadır. Ancak, DeMiCPU olarak bilinen bir alıřmada, CPU'lerden yayılan manyetik alan sinyallerinin analiz edilmesi yoluyla yakın alan manyetik alan mleri kullanılarak CPU'ların kimliklendirilmesi gerekleřtirilmiřtir [85]. Bu alıřma, CPU'lerden yayılan manyetik alan sinyalleri ile cihaz kimliklendirmesi iin yakın alan prob kullanımını gstermektedir. Benzer řekilde, dięer alıřmalar da CPU modllerinin yaydıęı manyetik indksiyon sinyallerine dayanarak cihazları tanımlamaya ynelik DeMiCPU alıřmasından esinlenmiřtir [86].

CPU kimliklendirmesine benzer řekilde, Birleřik Entegre (Integrated Circuit, IC) tanımlamaya odaklanan alıřmalar da mevcuttur [87]. Bu baęlamda, Zhang ve arkadařları, derin ęrenme tekniklerini kullanarak drt kategoriye yayılan 28 farklı IC'yi bařarıyla sınıflandırmıřtır [88]. Kablosuz iletiřim sinyalleri kullanan bir alıřmada, İbrahim ve arkadařları, iletiřim sinyallerinin iletim veya alım noktalarındaki istenmeyen elektromanyetik parazitleri erek cihazlara benzersiz tanımlayıcılar atamıřtır [89]. Ayrıca, elektromanyetik emisyonlar aracılıęıyla cihazların kimliklendirmeye ynelik yakın alan prob kullanımıyla ilgili patentler

bulunmaktadır; ancak bu yaklaşım akademik literatürde henüz kapsamlı bir şekilde analiz edilmemiştir [90]–[92].

1.3 Tezin Amacı

Kritik ortam ve sistemlerde bulunan elektronik cihazların bilinmeyen cihazlar tarafından taklit edilebilmesi büyük bir güvenlik açığını oluşturmaktadır. Bu durumun önüne geçmek için literatürde yapılan çalışmalarda cihazlara fiziksel olarak ya da dijital olarak kimlik numaraları atanmaktadır. Ancak elektronik cihazlara yapay olarak atanan kimlikler hem fiziksel ortamda hem de dijital ortamda basitçe değiştirilebilmektedir. Bu nedenle elektronik cihazların kimliklendirilebilmesi için benzersiz özelliklerinden yararlanılması son yıllarda popüler bir konu olmaya başlamıştır. Elektronik devre kartları aynı düzen ve komponentlere sahip olsa bile komponentlerde bulunan tolerans seviyeleri nedeniyle oluşturduğu sinyaller farklı olabilmekte bu da cihazların kimliğinin taklidini mümkün kılmamaktadır. Tez çalışması kapsamında, kritik ortam ya da sistemlerde bulunan elektronik cihazların kendi ürettiği kablolu, kablosuz ya da elektromanyetik emisyon sinyallerinin ham halindeki farklılıkları derin öğrenme modeli ile saptayarak cihazların kimliklendirilmesi hedeflenmiştir. Ayrıca birden fazla sinyal türü kullanılması nedeniyle çalışmaların birbirlerine göre avantaj ve dezavantajlarının analiz edilmesi ve uygulamalara göre daha iyi çalışacak sinyal türünün verilmesi amaçlanmıştır. Bunlarla beraber kullanılan sistemlerin stabilitesi de araştırılarak cihazların çalışmasıyla beraber elektronik komponentlerin özelliklerindeki değişimler nedeniyle oluşan sinyal değişimlerinin saptanması ve sistemin bu durumdan etkilenmeden güvenlik kontrollerine devam etmesi hedeflenmiştir.

1.4 Hipotez

Elektronik cihazların dijital kimlik ya da sertifikalarının taklit edilebilir bir formatta olması güvenlik problemlerine yol açmaktadır. Elektronik cihazlara kimlik vermek için cihazların kendi ürettiği sinyaller üzerinden dijital formatta sinyal işleme adımlarından geçmeden sinyalin ham hali ile kimlik çıkarılması cihazların benzersiz kimliklerinin elde edilmesini sağlayabilir. Cihazlar kablolu

haberleşme sinyalleri, kablosuz haberleşme sinyalleri ve çalışması sırasında komponentlerinin yaydığı elektromanyetik emisyon sinyalleri üzerinden kimliklendirilebilir. Bunu yapmak için ise öncelikle veri seti oluşturulmasına ve sonrasında oluşturulan veri seti kullanılarak derin öğrenme modelleri eğitilmesine gerek vardır. Elde edilen derin öğrenme modellerinin testleri için ise elde edilen test verilerinden Karışıklık Matrisi çıkarılması ilk testlerin yapılmasını sağlamaktadır. Ardından da sistemin stabilitesini test etmek için uzun süreli testler yapılarak cihazların tanıma oranındaki değişimlere bakılması, sistemin stabil çalışmasını öğrenmek açısından önemli bir bilgi sağlamaktadır. Bunlarla beraber özellikle düşük güç tüketime sahip ve kablosuz sinyaller üzerinden kimliklendirme yapılan cihazlar için günlük atılan paket sayısı analiz edilerek başarımlar oranı karşılaştırılması oldukça önemlidir.

1.5 Tezin Organizasyonu

Tez çalışması kapsamında kullanılan Makine Öğrenmesi ve CUDA Programlama teknolojileri Bölüm 2 ile anlatılmıştır. Anlatılan bu teknolojiler Bölüm 3, Bölüm 4 ve Bölüm 5 içinde kullanılmış olup teorik altyapısı Bölüm 2 ile sunulmuştur. Tez çalışması kapsamında kablosuz sinyallerin kimliklendirilmesi Bölüm 3 içinde yapılmış olup Bölüm 3.1 ile WiFi haberleşme sinyalleri üzerinden kimliklendirme yapılırken Bölüm 3.2 içinde LoRa haberleşme sinyalleri üzerinden kimliklendirme yapılmıştır. Kablolu sinyaller üzerinden kimliklendirme ise Bölüm 4 ile yapılmış olup burada Ethernet sinyalleri üzerinden kimliklendirme Bölüm 4.1 ile verildiği gibi yapılmıştır. Elektromanyetik emisyon sinyalleri üzerinden kimliklendirme Bölüm 5 ile yapılmış olup burada Bölüm 5.1 ile iletilen emisyon sinyalleri üzerinden ve Bölüm 5.2 ile havadan yayılan elektromanyetik sinyaller üzerinden kimliklendirme yapılmıştır. Çalışmaların sonucunda elde edilen çıktılar ve analizler ise Bölüm 6 ile verilmiştir.

2 KULLANILAN TEKNOLOJİLER VE ARAÇLAR

2.1 Makine Öğrenmesi

Elektronik cihazları kimliklendirmek için yapılan çalışmalarda makine öğrenmesi metotları kullanılarak elektronik kartların sınıflandırılması yapılabilmektedir. Makine öğrenmesi, gelecekteki değerleri tahmin etmek için geçmiş verilerin kullanıldığı bir yapay zekâ alanıdır. Makine öğrenmesi, doğru sonuçları elde etmek için veriye dayalı bir modelin oluşturulması ve bu modelin yeni veriler üzerinde kullanılması sürecini içerir [93]–[95]. Makine öğrenmesi için kullanılan veri, önceden belirlenmiş giriş özelliklerine ve bu özelliklere karşılık gelen hedef çıktılarına sahip olmalıdır. Giriş özellikleri verinin niteliklerini temsil ederken, hedef çıktıları tahmin etmek istenilen değerleri veya sınıfları ifade etmektedir. Makine öğrenmesi genellikle gözetimli (supervised) öğrenme, gözetimsiz (unsupervised) öğrenme ve takviyeli (reinforced) öğrenme olarak 3'e ayırmak mümkündür [96].

- **Gözetimli Öğrenme (Supervised Learning):** Gözetimli öğrenme, etiketlenmiş veriye dayalı olarak yapılan öğrenme yöntemidir. Bu yöntemde önceden belirlenmiş etiketlerle ilişkilendirilmiş giriş verileri kullanılarak bir model eğitilir [97]–[99]. Eğitim sürecinde modele giriş verileri sunulur ve model, bu verilere dayanarak çıktıları tahmin etmeye çalışır. Ardından, tahmin edilen çıktılar gerçek etiketlerle karşılaştırılır ve modelin hata miktarı hesaplanır. Bu hata geriye yayılarak modelin parametreleri güncellenerek daha iyi tahminler yapılması sağlanmaktadır.
- **Gözetimsiz Öğrenme (Unsupervised Learning):** Gözetimsiz öğrenme, etiketlenmemiş veriye dayalı olarak yapılan öğrenme yöntemidir [98],

[99]. Bu yöntemde, verilerin yapısı ve ilişkileri hakkında bilgi elde etmek için veri seti analiz edilmektedir. Modelin belirli bir çıktıya dayalı olarak eğitilmediği için veri setindeki gizli desenler, gruplamalar veya ilişkiler keşfedilmeye çalışılmaktadır. Örneğin, kümeleme (clustering) veya boyut indirgeme (dimensionality reduction) gibi teknikler gözetimsiz öğrenme yöntemlerine örnek olarak verilebilmektedir.

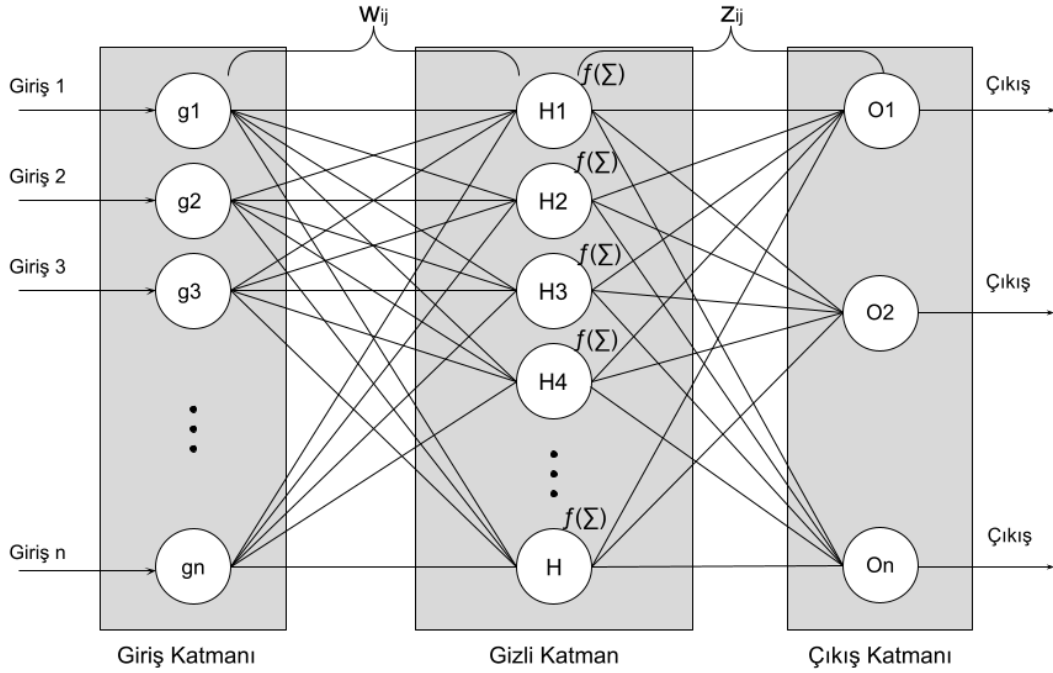
- **Takviyeli Öğrenme (Reinforcement Learning):** Takviyeli öğrenme, bir ajanın (agent) çevreyle etkileşime girerek deneyimler yoluyla öğrenme yöntemidir. Bu yöntemde, bir ajan, çevreyle etkileşim halinde olur ve belirli bir hedefi elde etmek için en iyi eylemleri öğrenmeye çalışır [100]–[102]. Ajan, belirli bir durumda bulunur, bir eylem seçer, çevreden bir geri bildirim alır ve bu geri bildirimle dayanarak davranışını günceller. Amacı, uzun vadede en yüksek ödül (reward) elde etmektir. Takviyeli öğrenme genellikle oyun teorisi, robotik ve otomatik kontrol gibi alanlarda kullanılmaktadır.

Elektronik devrelerin karakteristikleri üzerinden kimliklendirilmesi için kullanılan teknolojilere göre farklı makine öğrenmesi algoritmaları bulunmaktadır.

2.1.1 Yapay Sinir Ağları (Artificial Neural Network, ANN)

ANN, biyolojik sinir sistemlerinden ilham alarak tasarlanmış matematiksel modellerdir. Bu modeller genellikle üç katmandan oluşur: giriş katmanı, gizli katmanlar ve çıkış katmanı. Her katmandaki nöronlar birbirleri arasındaki ağırlıklı bağlantılarla önceki katmanın çıkışlarını alır ve belirli bir aktivasyon fonksiyonuna tabi tutularak çıkış üretirler [103]–[106]. ANN’ler, bu bağlantı ağı ve ağırlıkları öğrenme yeteneği sayesinde veri setlerindeki karmaşık ilişkileri modelleyebilir. Özellikle büyük veri setlerinde, görüntü işleme, dil işleme, sınıflandırma ve tahmin gibi çeşitli görevlerde başarıyla kullanılırlar. Eğitim süreci boyunca ağırlıkların ve bağlantıların optimizasyonu, ağın doğru sonuçlar üretebilmesi için gerçekleştirilir. Yapay sinir ağları, geniş bir uygulama yelpazesine sahip olup, endüstriyel kullanımdan akademik araştırmalara kadar pek çok alanda kullanılmaktadır. ANN’de kullanılan katmanların blok gösterimi Şekil

2.1 ile verilmiştir. Burada verilen nöron yapılarının hepsi bir katsayıya sahiptir ve bu katsayılar belirli matematiksel işlemler ile güncellenerek çalışmaktadır.



Şekil 2.1 Örnek bir ANN algoritmasının blok olarak gösterimi

Modeldeki ağırlık katsayıları rastgele değerlerden başlatılarak toplam net bilgi; girdi (G), ağa verilen toplam girdi (n) ve ağırlıklar (A) kullanılarak formül (2.1) ile verildiği gibi hesaplanır [107].

$$NET = \sum_i^n G_i A_i \quad (2.1)$$

Hesaplanan bu bilgi çıkışta kullanılan aktivasyon fonksiyonuna girdi olarak verilir. Burada aktivasyon fonksiyonu gelen girdiyi işleyerek çıktıyı belirlemek için kullanılmaktadır. Genel olarak kullanılan aktivasyon fonksiyonları;

- Birim,
- Doğrusal,
- Sigmoid,
- Tanjant Hiperbolik

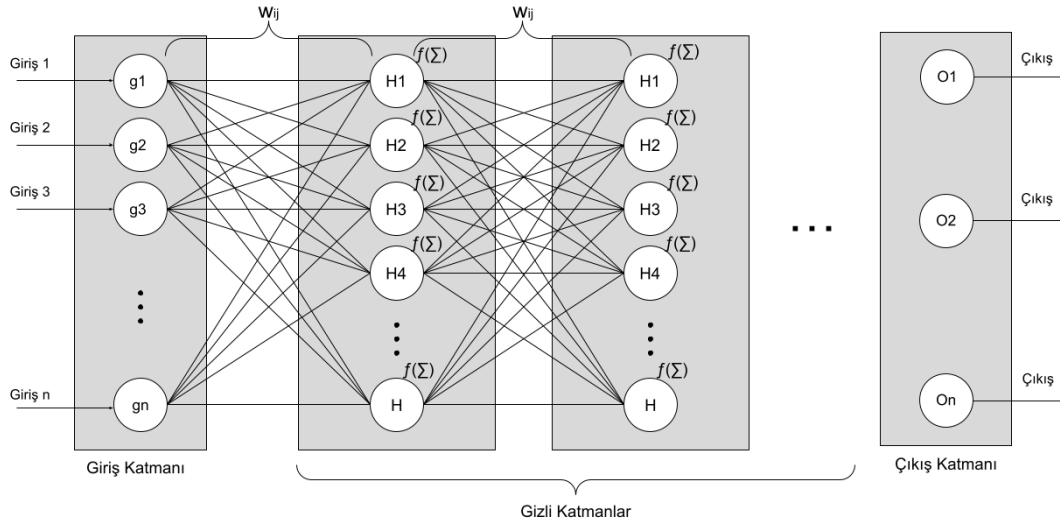
olabilmektedir. Bu fonksiyonlardan birine göre yapılan hesaplardan sonra gerçek çıkış ile elde edilen değer karşılaştırılır. Sonrasında geriye yayılım yapılarak ağırlıklar güncellenir ve bu işlem ağ istenilen seviyeye gelene kadar

yapılır. Normal ANN yapısına göre derin öğrenmede kullanılan ANN daha çok katmana sahip olması nedeniyle daha karmaşık sistemleri öğrenerek model oluşturabilmektedir.

2.1.2 Çok Katmanlı Perceptron (Multi Layer Perceptron, MLP)

MLP, yapay sinir ağlarının bir türüdür ve derin öğrenme alanında yaygın olarak kullanılır. Bu ağlar, birbiri ardına gelen katmanlardan oluşur ve her katmanda bir veya daha fazla nöron bulunur. Her nöron, önceki katmandaki nöronların çıktılarına dayalı olarak hesaplanan ağırlıklarla birbirine bağlanır. Bu yapı, veri üzerinde ardışık ve karmaşık hesaplamaların gerçekleştirilmesini sağlar.

Bu yapay sinir ağı modeli, bir giriş katmanı ile başlar. Giriş katmanı, verinin ağa girdiği ve her özelliğin ayrı bir giriş nöronuna karşılık geldiği katmandır. Giriş katmanının ardından, gizli katmanlar ile hesaplamalar yapılmaktadır. Gizli katmanlar, karmaşık ilişkileri ve özellikleri öğrenmek için kullanılır. Bu katmanlarda, önceki katmanların çıktıları alınıp işlenerek ağın girdi verilerinden özellikler çıkarması sağlanır. Her gizli katmanda, birbirine bağlı bir dizi nöron bulunur ve bu katmanlar arasında farklı sayılarda nöronlar olabilir. Son olarak, gizli katmana bağlı çıkış katmanı bulunmaktadır ve ağın nihai çıktıları üretir. Özellikle sınıflandırma problemlerinde, çıkış katmanında sınıf etiketlerine karşılık gelen nöronlar bulunabilir. Bu nöronların çıktıları, ağın veri üzerindeki tahminlerini ifade eder. MLP algoritmasının blok görünümü Şekil 2.2 ile verilmiştir. Burada da görüldüğü üzere MLP birden fazla gizli katmana sahiptir ve bu nedenle de ANN'e göre daha karmaşık problemleri çözebileceği anlaşılmaktadır.



Şekil 2.2 Örnek bir MLP algoritmasının blok olarak gösterimi

MLP'ler, bu katmanlar arasındaki bağlantıların ağırlıklarını öğrenerek, veri üzerindeki karmaşık ilişkileri modelleyebilir. Ağın tahminleri ve gerçek değerler arasındaki farkları azaltmak için eğitim süreci boyunca ağırlıkların uygun şekilde güncellenmesi sağlanır. Bu sayede ağ belirli bir amaca yönelik olarak öğrenir ve veri üzerindeki desenleri keşfeder.

MLP algoritmasının matematiksel alt yapısı incelendiğinde geri yayılım, ileri geçiş, kayıp (loss) ve aktivasyon fonksiyonları ile hesaplamaların yapıldığı görülmektedir. Geri yayılımda ağırlık güncelleme formülü (2.2) ile ve bias güncelleme ise (2.3) ile verilmiştir. Burada $W^{(l)}$ l'ninci katmandaki ağırlık matrisi, $b^{(l)}$ l'nin katmandaki bias terimini ve α öğrenme oranını temsil etmektedir.

$$W_{yeni}^{(l)} = W_{eski}^{(l)} - \alpha \frac{\partial L}{\partial W^{(l)}} \quad (2.2)$$

$$b_{yeni}^{(l)} = b_{eski}^{(l)} - \alpha \frac{\partial^2 L}{\partial b^{(l)}} \quad (2.3)$$

İleri geçiş fonksiyonuna bakıldığında ise l'ninci katmandaki öncesi değer formül (2.4) ile l'ninci katmandaki fonksiyon sonrası değer ise formül (2.5) ile bulunmaktadır. Burada $f^{(l)}$ aktivasyon fonksiyonunu, $a^{(l)}$ l'ninci katmandaki aktivasyon öncesi değer ve $h^{(l)}$ l'ninci katmandaki aktivasyon sonrası değerdir.

$$a^{(l)} = W^{(l)} h^{(l-1)} + b^{(l)} \quad (2.4)$$

$$h^{(l)} = f^{(l)}(a^{(l)}) \quad (2.5)$$

2.1.3 Evrişimsel Sinir Ağı (Convolutional Neural Network, CNN)

Evrişimsel Sinir Ağı (CNN), özellikle görüntü işleme alanında büyük başarılar elde etmiş derin öğrenme modellerinden biridir. CNN'ler, öğrenme yeteneklerini, verinin lokal özelliklerini vurgulama ve hiyerarşik özelliklerin karmaşıklığını artırma kabiliyeti ile bilinir. Genellikle karmaşık görsel veri setleri üzerinde kullanılan bu yapı, girdi verisini evrişim (convolution) ve pooling işlemleriyle işleyerek özellik haritaları oluşturur. Bu özellik haritaları, nesne tanıma, sınıflandırma ve diğer görevler için kullanılarak öğrenme gerçekleştirir.

CNN'lerin temelini evrişim (convolution) katmanları oluşturur. Bu katmanlar, belirli boyutlardaki filtrelerin girdi verisi üzerinde kaydırılması yoluyla lokal özellikleri vurgular. ReLU aktivasyon fonksiyonu, evrişim işlemlerinin ardından negatif değerleri sıfırlayarak ağı daha hızlı öğrenmesini sağlar. Ardından, alt örnekleme (pooling) katmanlar özellik haritasındaki boyutu küçültmek için kullanılır.

CNN'lerin sonunda genellikle tam bağlı (fully connected) katmanlar gelir. Bu katmanlar, önceki katmanlardan elde edilen özellikleri kullanarak sınıflandırma veya regresyon görevleri için çıkış üretir. Özellikle sınıflandırma problemlerinde çıkış katmanında softmax aktivasyon fonksiyonu kullanılarak çoklu sınıflı problemlerde olasılıklar üretilir.

Ağ yapısı, özellikle büyük veri setleri üzerinde öğrenme yeteneği ile bilinmektedir. CNN'ler, genellikle önceden belirlenmiş özellikleri kodlamaya gerek kalmadan veriden özellikleri öğrenme yeteneği ile öne çıkar. Özellikle nesne tanıma, yüz tanıma, otonom araçlar ve medikal görüntüleme gibi birçok uygulama alanında büyük başarılar elde edilmesini sağlamıştır. Klasik olarak kullanılan CNN yapısının formülasyonuna bakıldığında evrişim işlemi formül (2.6) ile ifade edilmektedir. Burada $S(i,j)$, evrişim işlemi sonucunda elde edilen özellik haritasının bir elemanını, I giriş matrisini ve W filtre matrisini temsil etmektedir.

$$S(i, j) = \sum_m \sum_n I(i + m, j + n) * W(m, n) \quad (2.6)$$

ReLU aktivasyon fonksiyonu, negatif deęerleri sıfır yaparak formül (2.7) ile verildięi gibi non-linearity (doęrusallık dıřılıęı) ekler.

$$f(x) = \max(0, x) \quad (2.7)$$

Daha sonrasında alt örnekleme işlemi, belirli bir bölge içindeki deęerlerin özetlenmesi amacıyla kullanılır. Max pooling, bu bölgedeki maksimum deęeri seçer. Tam baęlı katmanlar, formül (2.8) ile verildięi gibi önceki katmanın tüm nöronlarıyla baęlantılıdır. Burada W , aęırlık matrisini; x , önceki katmanın çıkıřlarını; b , bias terimini ve f , aktivasyon fonksiyonunu temsil etmektedir.

$$y = f(Wx + b) \quad (2.8)$$

Çıkıř katmanında sınıflandırma yapılması durumunda genel olarak fomül (2.9) ile verilen Softmax fonksiyonu kullanılmaktadır.

$$P(y_i) = \frac{e^{y_i}}{\sum_j e^{y_j}} \quad (2.9)$$

Günümüzde klasik CNN modeli yerine LeNet-5, AlexNet, VGGNet, GoogLeNet, ResNet, MobileNet ve EfficientNet gibi yöntemler kullanılmaktadır. Bu modeller, CNN mimarilerinin geniř bir yelpazesini temsil eder ve her biri belirli görevler veya kısıtlamalar için tasarlanmıřtır.

2.1.4 Zamansal Konvolüsyon Aęı (Temporal Convolutional Network, TCN)

Zamansal Konvolüsyon Aęı (TCN), ardışık verilerin işlenmesi için tasarlanmış özel bir mimaridir. Bu yapı, konvolüsyon katmanlarını kullanarak zamansal baęımlılıkları etkili bir şekilde yakalamaya odaklanır. TCN'ler, ses tanıma, doęal dil işleme ve sensör verisi analizi gibi uygulamalar için özellikle uygundur. Geleneksel konvolüsyonel sinir aęlarından farklı olarak, TCN'ler zamansal kalıpları ve iliřkileri anlamaya yönelik bir yapıya sahiptir.

TCN'lerin temel özelliklerinden biri, nedensel konvolüsyonlar kullanmasıdır. Nedensel konvülüsyon, modelin gelecekteki verilerden bilgi sızdırmamasını saęlayarak yalnızca mevcut ve geçmiş zaman adımlarını kullanarak tahmin yapmasına olanak tanır. Örneęin, belirli bir zaman adımında, çıkıř deęeri sadece o zaman adımındaki girdi ve daha önceki zaman adımlarındaki girdilere dayanır. Bu özellik, zaman sırasını korumak için oldukça önemlidir. Matematiksel olarak, bu işlem formül (2.10) ile verildięi gibi ifade edilebilir. Burada y_t , t zaman

adımındaki çıkış; $x_t, x_{t-1}, \dots, x_{t-k}$ parametreleri, giriş verilerini; f , aktivasyon fonksiyonunu; l , gecikme parametresini ifade etmektedir

$$y_t = f(x_t, x_{t-1}, \dots, x_{t-l}) \quad (2.10)$$

Bir diğer önemli özellik ise dilasyonlu (dilate) konvolüsyonlar kullanılmasıdır. Dilation, konvolüsyon işlemi sırasında çekirdeklerin zaman adımlarını atlayarak daha geniş bir bağlam penceresi elde etmesine olanak tanır. Bu, TCN'lerin daha uzun süreli bağımlılıkları öğrenmesine yardımcı olur, çünkü model daha geniş bir veri seti üzerinde çalışırken belirli bir zamana ait bilgilere ulaşabilir. Matematiksel olarak, dilasyonlu konvolüsyon formül (2.11) ile verildiği gibi tanımlanabilmektedir. Burada w_i , filtre katsayılarını; d , dilasyon faktörünü; k , filtre boyutunu ifade etmektedir.

$$y_t = \sum_{i=0}^{k-1} w_i \cdot x_{t-d \cdot i} \quad (2.11)$$

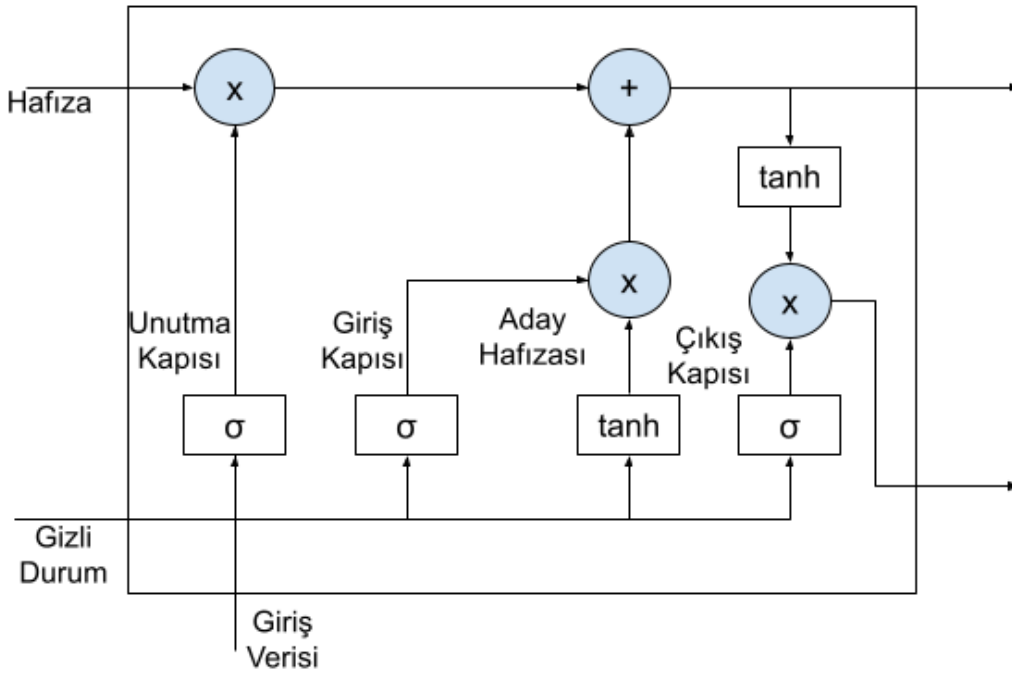
TCN mimarisinde genellikle birden fazla konvolüsyon katmanı bulunur. Bu katmanlar, özellik çıkarımında derinleşerek daha karmaşık özelliklerin öğrenilmesine olanak tanır. Ayrıca, TCN'ler dropout katmanları ile kullanılarak aşırı öğrenmenin önüne geçilir. Sonuç olarak, TCN'ler zaman serisi verileri ile çalışırken hem daha yüksek performans hem de daha iyi genelleme yeteneği sunar.

Genel olarak, TCN'ler zamansal verileri anlamada etkili bir yaklaşım sunar ve hem nedensel hem de dilate konvolüsyon tekniklerini kullanarak karmaşık zamansal bağımlılıkları öğrenme kapasitesine sahiptir. Bu nedenle, TCN'ler, geleneksel yöntemlere göre daha iyi performans gösterme potansiyeline sahip, yenilikçi bir derin öğrenme mimarisi olarak öne çıkmaktadır.

2.1.5 Tekrarlayan Sinir Ağı (Recurrent Neural Network, RNN)

RNN'ler, sıralı veri yapılarının modellenmesi için özel olarak tasarlanmış bir yapay sinir ağı sınıfıdır. Temelde, içerdikleri gizli durum (hidden state) mekanizması sayesinde önceki bilgileri hatırlayabilme özelliğine sahiptirler. Bu özellik, doğal dil işleme, zaman serileri analizi ve diğer sıralı veri problemlerinin çözümünde yaygın olarak kullanılır. RNN'ler, geleneksel sinir ağı modellerinden farklı olarak zaman içindeki bağlantıları dikkate alabilme özelliğine sahiptir. Bu özelliği,

önceki zaman adımlarından gelen bilgileri saklamak ve gelecekteki tahminleri etkileyebilmek için bir hücre yapısı içerir. Temel RNN hücre yapısının blok olarak gösterimi ise Şekil 2.3 ile verilmiştir. Burada görüldüğü üzere hücre yapısında hafıza, unutma kapısı, gizli durum, giriş kapısı, aday hafızası ve çıkış kapısı gibi parametreler bulunmaktadır. Alınan veri ya da sinyaller bu adımlardan geçerek doğru sonuca ulaşmaya çalışarak parametrelerdeki katsayılar güncellenmektedir.



Şekil 2.3 RNN algoritmasında kullanılan hücre yapısı

RNN'lerin matematiksel formülasyonunu derinlemesine bakıldığında ise formül (2.12) ile verilen ileri geçiş fonksiyonundan ve farklı formlarda seçilebilen kayıp fonksiyonundan oluşmaktadır. Burada verilen x_t t'ninci zaman adımıdaki giriş vektörü, h_t t'nin zaman adımıdaki gizli durum vektörü, W_{hx} giriş ile gizli durum arasındaki ağırlık matrisi, W_{hh} gizli durum ile gizli durum arasındaki ağırlık matrisi ve b_h gizli durum için bias terimini ifade etmektedir.

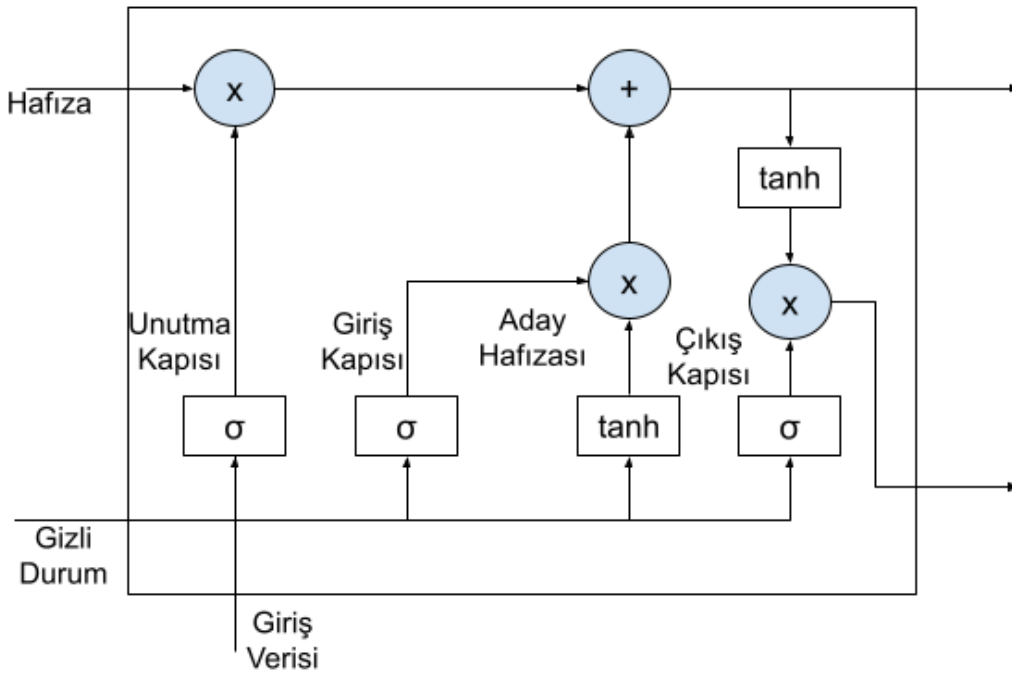
$$h_t = \tanh(W_{hx}x_t + W_{hh}x_{t-1} + b_h) \quad (2.12)$$

RNN'ler, sıralı verilerle çalışmak için tasarlanmış olsa bile uzun vadeli bağımlılıkları (vanishing gradient problem) ele alma konusunda zayıf kalmaktadır. Bu zayıflık, sıralı veri içindeki uzun vadeli bağımlılıkları etkin bir

şekilde modelleme ve hatırlama yeteneğindeki eksikliklerden kaynaklanır. LSTM ve GRU, RNN'lerin bu zayıflıklarını ele almak üzere tasarlanan özel varyasyonlardır.

2.1.6 Uzun Kısa Süreli Bellek (Long Short-Term Memory, LSTM)

LSTM hücreleri, sıralı veri analizi için geliştirilen ve uzun vadeli bağımlılıkları başarılı bir şekilde ele alan bir yapay sinir ağı mimarisidir. Temelde, geleneksel RNN'ler karşılaştığı kaybolan gradyan sorununu aşmak ve sıralı verilerdeki uzun vadeli bağımlılıkları daha etkili bir şekilde modellemek üzere tasarlanmıştır. LSTM katmanlarında kullanılan hücrelerin yapısı Şekil 2.4 ile verildiği gibidir.



Şekil 2.4 LSTM algoritmasında kullanılan hücre yapısı

LSTM'nin temel yapı taşlarından biri, hafıza hücresidir (c_t). Hafıza hücresi, geçmiş bilgiyi saklayan uzun vadeli bir belleği temsil eder. Aynı zamanda, o anki giriş ve önceki gizli durum bilgileri kullanılarak güncellenir. Bu güncelleme süreci, bir dizi kapı (gate) mekanizması ile kontrol edilir. Bu kapılar; giriş kapısı (input gate, i_t), unutma kapısı (forget gate, f_t), hücre güncellemesi (cell update g_t), ve çıkış kapısı (output gate, o_t) olarak adlandırılır. Giriş kapısı, giriş bilgilerini hafıza hücresine eklemek için kullanılır ve sigmoid fonksiyonu aracılığıyla bu kararı alır. Unutma kapısı, geçmiş bilgilerin hafıza hücresinden silinip

silinmeyeceğini belirler. Hücre güncellemesi, hafıza hücresine eklenen yeni bilgileri tanımlar. Çıkış kapısı ise, gizli durumun o anki bilgilerini belirleyerek dış dünyaya sunar. Bu kapılar, içerdikleri sigmoid ve hiperbolik tanjant aktivasyon fonksiyonları aracılığıyla belirli bir kontrol ve filtreleme mekanizması sağlarlar. Matematiksel ifadelerle, LSTM'nin hafıza hücresi ve gizli durum güncellemesi formül (2.13-2.16) arasında verilmiştir. Burada verilen x_t t'ninci zaman adımıdaki giriş vektörü, h_t t'nin zaman adımıdaki gizli durum vektörü, W_{ii} giriş ile gizli durum arasındaki ağırlık matrisi, W_{if} gizli durum ile gizli durum arasındaki ağırlık matrisi, W_{ig} gizli durum ile gizli durum arasındaki ağırlık matrisi, W_{io} gizli durum ile gizli çıkış arasındaki ağırlık matrisi ve b_h 'lar gizli durum için bias terimini ifade etmektedir.

$$i_t = \sigma(W_{ii}x_t + b_{ii} + W_{hi}h_{t-1} + b_{hi}) \quad (2.13)$$

$$f_t = \sigma(W_{if}x_t + b_{if} + W_{hf}h_{t-1} + b_{hf}) \quad (2.14)$$

$$g_t = \tanh(W_{ig}x_t + b_{ig} + W_{hg}h_{t-1} + b_{hg}) \quad (2.15)$$

$$o_t = \sigma(W_{io}x_t + b_{io} + W_{ho}h_{t-1} + b_{ho}) \quad (2.16)$$

LSTM hücresindeki tüm bu bileşenler kullanılarak hafıza hücresi (c_t) ve gizli durum (h_t) güncellenir. Güncellenen verilerin yansıması için ise $\odot$ sembolü eleman çarpımı olmak üzere hafıza hücresinin güncellenmesi formül (2.17) ile gizli durum güncellemesi ise formül (2.18) ile yapılmaktadır.

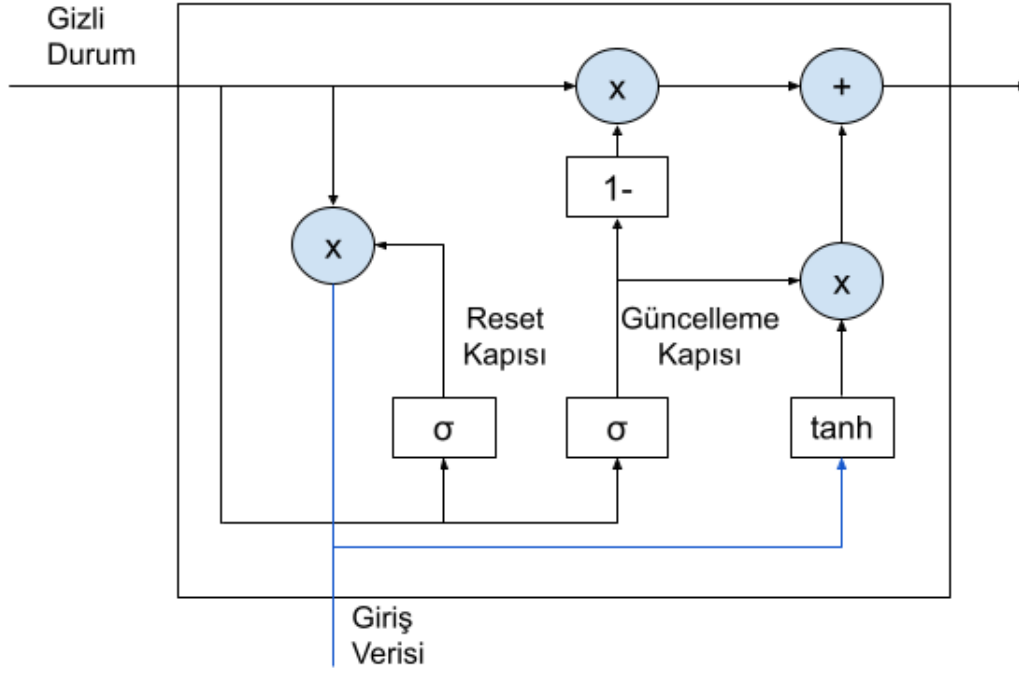
$$c_t = f_t \odot c_{t-1} + i_t \odot g_t \quad (2.17)$$

$$h_t = o_t \odot \tanh(c_t) \quad (2.18)$$

2.1.7 Kapılı Tekrarlama Ünitesi (Gate Recurrent Unit, GRU)

GRU, sıralı veri setlerinde kullanılan bir RNN modelidir. GRU, özellikle dil işleme ve zaman serisi analizi gibi alanlarda başarıyla uygulanabilen bir rekürrent yapısı sunmaktadır. Temelde GRU'nun iç yapısı, hücre durumu adı verilen bir iç belleği içerir. Bu hücre durumu, önceki zaman adımlarından gelen bilgileri saklamak ve güncellemek amacıyla kullanılır. GRU'nun güncelleme ve sıfırlama aşamaları, hücre durumunu kontrol etmek için önemlidir. Güncelleme aşaması, hücre durumunun ne kadarının güncelleneceğini belirlerken, sıfırlama aşaması önceki hücre durumunun ne kadarının atılacağını belirler. Aday hücre durumu,

yeni bilgileri taşıyan bir vektördür ve güncelleme ile sıfırlama aşamalarının hesaplamalarına dayanarak oluşturulur. Yeni hücre durumu, önceki hücre durumu ve aday hücre durumu kullanılarak güncellenir. Bu süreç, modelin önceki zaman adımlarından gelen bilgileri dikkate alarak zaman içindeki ilişkileri öğrenmesini sağlar. GRU algoritmasında kullanılan hücrenin iç yapısı Şekil 2.5 ile verilmiştir.



Şekil 2.5 GRU algoritmasında kullanılan hücre yapısı

GRU'nun avantajlarından biri, kaybolan gradyan (vanishing gradient) sorununu hafifletmeye yönelik tasarlanmış olmasıdır. Geleneksel RNN yapıları, uzun zaman serilerinde gradyanların çok küçük hale gelmesine ve eğitimin zorlaşmasına neden olabilen bir sorunla karşılaşabilir. GRU, bu sorunu azaltarak daha etkili bir öğrenme sağlar. Bu özellikleriyle GRU, zaman serileri ve dil modelleme gibi uygulamalarda sıkça tercih edilen bir Tekrarlayan (Recurrent) yapısıdır. Matematiksel ifadeler ile bakıldığında güncelleme aşamasında formül (2.19) ile verilen denklem ile modelin hangi bilgilerin önceki zaman adımından taşınması gerektiğini ve hangi bilgilerin unutulacağını belirlenmektedir. Burada z_t , güncelleme aşamasının çıkışı (update gate output); W_z , ağırlık matrisini; h_{t-1} ,

önceki zaman adımındaki gizli durumu; x_t , mevcut zaman adımındaki girdiyi; b_z , bias terimini ve σ , sigmoid aktivasyon fonksiyonunu ifade etmektedir.

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t] + b_z) \quad (2.19)$$

Önceki zaman adımından hangi bilgilerin unutulacağı ise sıfırlama aşamasında yapılmaktadır. Sıfırlama aşamasında formül (2.20) ile verilmiş olan denklem kullanılmaktadır. Burada r_t , sıfırlama aşamasının çıkışını (update gate output); W_r , ağırlık matrisini; h_{t-1} , önceki zaman adımındaki gizli durumu; x_t , mevcut zaman adımındaki girdiyi; b_r , bias terimini ve σ , sigmoid aktivasyon fonksiyonunu ifade etmektedir.

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t] + b_r) \quad (2.20)$$

Aday hücre durumu ise formül (2.21) ile bulunmaktadır ve sıfırlama kapısının etkisiyle bir sonraki zaman adımında kullanılabilecek geçici bir bilgiyi temsil etmektedir. Burada $\tilde{h}_t$, aday hücre durumunu (candidate hidden state); W , ağırlık matrisini; r_t , sıfırlama aşamasının çıkışını; h_{t-1} , önceki zaman adımındaki gizli durumu; x_t , mevcut zaman adımındaki girdiyi; b , bias terimini; $\tanh$, hiperbolik tanjant aktivasyon fonksiyonunu ve $\odot$, eleman bazında çarpma işlemi ifade etmektedir.

$$\tilde{h}_t = \tanh(W \cdot [r_t \odot h_{t-1}, x_t] + b) \quad (2.21)$$

Son adımda ise güncelleme kapısı yardımıyla (z_t) mevcut hücre durumu (h_t) formül (2.22) ile verildiği gibi hesaplanmaktadır. Burada h_t , güncellenmiş gizli durum; z_t , güncelleme aşamasının çıkışını; h_{t-1} , önceki zaman adımındaki gizli durumu; $\tilde{h}_t$, aday hücre durumunu ve $\odot$, eleman bazında çarpma işlemi ifade etmektedir.

$$h_t = z_t \odot h_{t-1} + (1 - z_t) \odot \tilde{h}_t \quad (2.22)$$

2.2 Paralel Programlama ve CUDA

Tez çalışması kapsamında elektronik cihazların kimliklendirilebilmesi için öncelikle alınan sinyallerin işlenmesi ve sinyal içinden gerekli bilgilerin

ıkarılması gerekmektedir. Gerek zamanlı olarak alınan sinyallerin iřlenmesi ve matematiksel iřlemlerin yapılabilmesi yksek seviyede hız gerektirebilmektedir. Bunun iin ise paralel olarak ya da yksek frekansa sahip iřlemciler zerinde bu iřlemlerin yapılması gerekmektedir. Paralel programlama, bilgisayar sistemlerinde ve iřlemcilerde eřzamanlı olarak birden ok grevin yrtlmesini saėlayan bir programlama paradigmasıdır. Bu yaklařım, genellikle byk veri setleri, yoėun hesaplamalar veya karmařık problemlerle uėrařan uygulamalarda performansın artırılması amacıyla kullanılır [108]–[110]. Ancak, paralel programlama, beraberinde karmařıklık ve zel zorluklar getirir.

Paralel programlamanın temel karmařıklıklarından biri, iřlemlerin veya iř paracıklarının (thread) eřzamanlı olarak alıřtırılması durumunda ortaya ıkan senkronizasyon sorunlarıdır. Birden ok iřlemcinin aynı veriye eriřmeye alıřması, yarıř kořulları ve tutarsız veri durumlarına yol aabilir. Bu durumlar, programcının zenli bir řekilde senkronizasyon mekanizmalarını kullanması gerektiėi anlamına gelir. Ayrıca, paralel programlamada veri baėımlılıkları da nemli bir karmařıklık kaynaėıdır. Bir iřlem veya iř paracıėı tarafından retilen verinin, bařka bir iřlem veya iř paracıėı tarafından kullanılması durumunda uygun senkronizasyon mekanizmalarının kullanılması gerekmektedir. Bu durum, genellikle programcılar iin karmařık ve hata eėilimli bir sretir. İletiřim ve senkronizasyon maliyeti, paralel programlamanın bir diėer nemli karmařıklık faktrdr. İřlemler veya iř paracıkları arasındaki veri paylařımı ve koordinasyonun gerekliliėi, sistem performansını etkileyen nemli bir faktrdr. Son olarak, paralel programlamanın leklendirebilme zorlukları da dikkate alınmalıdır. İřlemci sayısını artırarak performansın iyileřtirilmesi beklentisi, her zaman doėru olmayabilir. Programcılar, paralel algoritmaları doėru bir řekilde tasarlamalı ve uygulamalı, ayrıca sistem zerindeki iř ykn dengeli bir řekilde daėıtmalıdır. Paralel programlama, performans artıřı saėlamak aısından nemlidir, ancak bu avantajlar elde edilirken ortaya ıkan karmařıklıkların anlařılması ve etkili bir řekilde ynetilmesi gerekmektedir.

Paralel programlamanın karmařıklıėı ayrıca veri baėımlılıkları ve iletiřim maliyeti ile de iliřkilidir. İřlemler arasındaki veri baėımlılıklarını ynetmek, iřlemler arasında doėru ve gvenilir bir iletiřim kurmak, karmařıklıėı artırır. Bu nedenle,

paralel programlama, yazılım mühendislerinden, veri akışlarını ve etkileşimleri özenle yönetmelerini, paylaşılan verilere güvenli bir şekilde erişmelerini ve iletişim maliyetini minimize etmelerini gerektirir. Paralel programlama, yüksek performans ve hız elde etmek için birden çok işlemcinin veya işlemci çekirdeğinin etkili bir şekilde kullanılmasını hedefler. Ancak, bu avantajlar elde edilirken, bazı maliyetleri de beraberinde getirir. İşlemler veya iş parçacıkları arasındaki iletişim ve senkronizasyon maliyeti, önemli bir faktördür. İletişim maliyeti, veri paylaşımının ve senkronizasyonun gerekliliği nedeniyle ortaya çıkar ve bu maliyet, performans üzerinde belirleyici bir rol oynar. Ayrıca, iş parçacığı veya işlem oluşturma, başlatma ve sonlandırma işlemleri de maliyeti etkileyen faktörler arasında yer alır. Bu işlemler, sistem kaynaklarını kullanırken ek maliyetlere neden olabilir. Dolayısıyla, paralel programlama projelerinde, iş yükünün doğru bir şekilde bölünmesi, verimli algoritmaların seçilmesi ve performans analizlerinin detaylı bir şekilde yapılması, maliyetin etkili bir şekilde yönetilmesini sağlamak adına kritiktir. Paralel programlamada başarılı olabilmek, karmaşıklıkları anlamayı, uygun algoritmaları seçmeyi, etkili iletişim ve senkronizasyon mekanizmalarını uygulamayı ve maliyetleri analiz etmeyi gerektirir. Bu, programcılardan özenli bir planlama ve tasarım süreci yürütmelerini ve paralel programlamanın özel zorluklarına uygun çözümler üretmelerini bekler.

Grafik İşlem Birimi (Graphical Processing Unit, GPU), temelde bilgisayarın grafik ve görüntü işleme görevlerini yerine getiren özel bir işlem birimidir. Ancak, GPU'lar yalnızca grafik işleme amacıyla kullanılmaktan çıkarak genel amaçlı hesaplamalarda da kullanılmaya başlanmıştır. Genel amaçlı kullanım için tasarlanan bu GPU'lar, paralel hesaplamalarda özellikle yüksek performanslı işlemler için optimize edilmiş güçlü işlem birimlerine sahiptir. GPU'lar, paralel işlem kapasitesi açısından oldukça güçlüdür. Geleneksel CPU'lar genellikle daha az sayıda işlemci çekirdeği üzerinde yoğunlaşırken, GPU'lar binlerce işlem birimini eşzamanlı olarak çalıştırma kapasitesine sahiptir. Bu özellik, geniş veri setlerinde ve karmaşık hesaplamalarda büyük performans artışları sağlamak için oldukça etkilidir. GPU'lar, paralel hesaplamalar için özel olarak tasarlanan CUDA (Compute Unified Device Architecture) gibi programlama modelleri ile genel

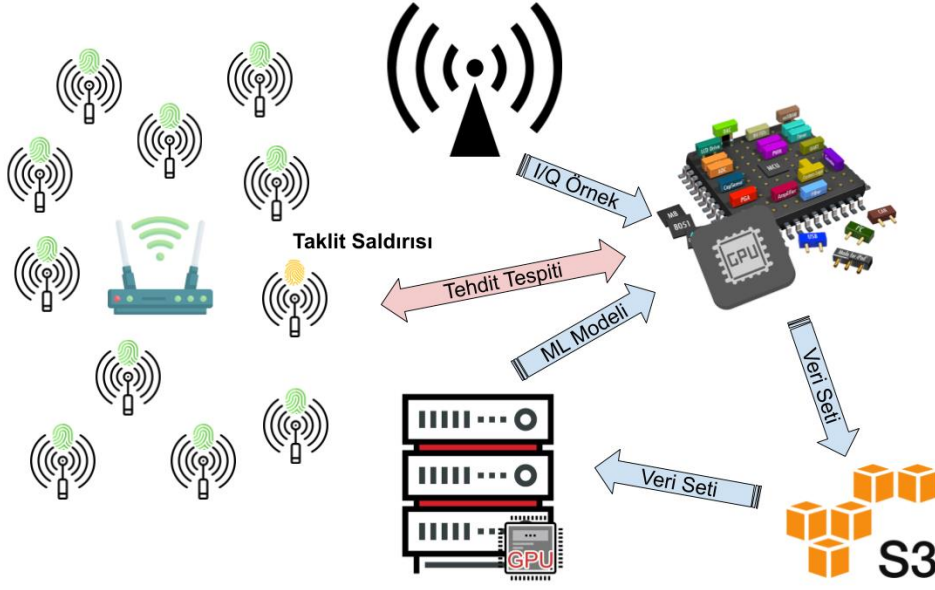
amaçlı hesaplamalarda kullanılabilir hale gelmiştir [111]–[113]. Bu genel amaçlı GPU kullanımı, genel CPU'lardan daha yüksek performans elde etme ve hesaplama kapasitesini artırma imkânı sunar.

CUDA, genel amaçlı paralel hesaplamaları destekleyen ve özellikle grafik işlem birimleri üzerindeki hesaplamaları hızlandırmak için tasarlanmış bir platform ve programlama modelidir. Paralel hesaplamaların etkin bir şekilde yapılabilmesi için C programlama dilini temel almaktadır ve GPU'ları genel amaçlı işlemler için kullanılabilir kılmaktadır. CUDA'nın temel özelliklerinden biri, SIMD (Single Instruction, Multiple Data) modelini benimsemesidir. Bu model, aynı komutun birçok veri ögesi üzerinde eş zamanlı olarak uygulandığı bir yapı sunmaktadır. CUDA programları, paralel hesaplamaları gerçekleştirmek için çekirdek (kernel) adı verilen özel fonksiyonlardan oluşur. Her bir çekirdek fonksiyonu, GPU üzerindeki iş parçacıkları tarafından aynı anda çalıştırılır ve genellikle çok sayıda veri ögesi üzerinde aynı işlemleri gerçekleştirir. CUDA'nın iş parçacığı hiyerarşisi, iş parçacıklarını bloklar içinde düzenler ve bu bloklar bir ızgara (grid) oluşturur. İş parçacıkları, belirli bir düzen içinde çalışarak GPU içindeki kaynaklarla ve birbirleriyle etkileşimde bulunmaktadır. Bu hiyerarşi, paralel hesaplamaların düzenli ve etkili bir şekilde yapılabilmesini sağlamaktadır. Hafıza modeli açısından CUDA, GPU üzerinde global bellek, paylaşılan bellek ve özel bellek gibi farklı türlerde bellek alanları sunmaktadır. Bu hafıza hiyerarşisi, veri transferini ve kullanımını optimize etmeyi amaçlamaktadır. Özellikle GPU ve CPU arasındaki veri transferini minimize ederek performans artışı sağlamayı hedeflemektedir. CUDA, genel amaçlı paralel hesaplamalarda bir standart haline gelmiş ve özellikle bilimsel hesaplamalar, derin öğrenme, simülasyonlar gibi yoğun hesaplama işlemlerinde yaygın olarak kullanılmaktadır. Bu platform, GPU'ları geniş bir paralel hesaplama kapasitesine sahip güçlü hesap birimlerine dönüştürerek, yüksek performanslı hesaplamaların gerçekleştirilmesine olanak tanımaktadır.

3.1 Wi-Fi Cihazlarının Kimliklendirilmesi

3.1.1 Önerilen Tasarım

Elektronik cihazların WiFi bağlantısı üzerinden birbirleri ile haberleşmesi sırasında güvenlik önlemleri genel olarak sinyaller dijital formata dönüştürüldükten sonra alınmakta bu da sinyallerin taklit edilerek ağ güvenliğini tehdit etmesine sebep olmaktadır. Bu nedenle önerilen tasarım kapsamında SDR kullanılarak sisteme bağlı olan WiFi cihazlarından alınan sinyaller ham olarak elde edilip etiketlenerek veri seti oluşturulmuş ardından da bu veri seti kullanılarak WiFi cihazlarının ham sinyalleri üzerinden kontrolü yapılarak kimliği belirsiz bir cihazın sisteme dahil olmaya çalışması durumunda sistemde devre dışı bırakılmıştır. Oluşturulan sisteminin genel mimarisi Şekil 3.1 ile verilmiştir. Görüldüğü gibi, SDR üzerinden alınan sinyaller cihazların MAC adresleri ile etiketlenerek AWS (Amazon Web Servisleri) S3 Depolama üzerine aktarılmaktadır. Burada MAC adreslerinin çıkarılabilmesi için gömülü GPU içinde WiFi sinyallerinin çözümüleme işlemi yapılmaktadır. AWS S3 Depolama üzerinde veri göleti oluşturulduktan sonra, ham sinyal dosyaları veri göletinden sunucuya aktarılır ve sinyal dosyaları kullanılarak derin öğrenme eğitimi sunucuda başlatılır. Eğitim tamamlandıktan sonra, derin öğrenme modeli gömülü GPU'ya transfer edilir ve sistem gerçek zamanlı olarak çalıştırılır. Literatürdeki çalışmalara karşı, önerilen tasarımda derin öğrenme eğitimi sadece OFDM (Orthogonal Frequency Division Multiplexing) paketinin Başlangıç (Preamble) bilgileri kullanılarak gerçekleştirilmiştir.



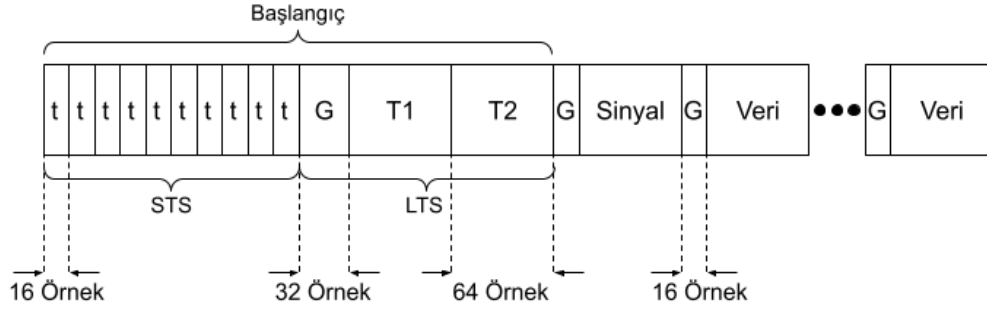
Şekil 3.1 WiFi cihazlarının kimliklendirilmesi için önerilen sistem

Veri setinin elde edilebilmesi için öncelikli olarak WiFi sinyalleri üzerinden MAC adreslerinin çıkarılabilmesi bunun için ise sinyal karakteristiği, demodülasyon tekniği ve çözümleme işlemlerinin ayrıntılandırılması gerekmektedir.

3.1.2 WiFi Sinyal Karakteristiği

WiFi sinyalleri, veri iletiminde OFDM (Orthogonal Frequency Division Multiplexing) teknolojisini kullanmakta olup, bu teknoloji geniş bir frekans bandını birden fazla alt taşıyıcıya bölmek ve her bir taşıyıcıda veriyi paralel iletmek suretiyle spektrum verimliliğini artırmakta ve çok yollu yayılım gibi fiziksel bozulmalara karşı dayanıklılık sağlamaktadır. Yüksek hızlı veri iletimine olanak tanımakla birlikte, WiFi protokollerinin temelini oluşturmakta olan OFDM, alıcının doğru algılama yapabilmesi için senkronizasyon sekansları içermekte, bu süreçte Kısa Eğitim Sekansı (Short Training Sequence, STS) sinyal algılama, zaman senkronizasyonu ve kaba kanal tahmini için kullanılmakta, ardından Uzun Eğitim Sekansı (Long Training Sequence, LTS) devreye girerek hassas kanal tahmini yapmakta ve frekans kaymalarını düzeltmektedir. Ayrıca, OFDM sinyallerinde veri blokları arasına yerleştirilen Koruma Bölgeleri (Guard Intervals), zaman gecikmesi ve çok yollu yayılımdan kaynaklanan girişimleri önlemek için kullanılmakta, bu sayede sinyalin bütünlüğü korunarak bozulmalar azaltılmakta ve ardından gelen veri bölümü kullanıcıya iletmek üzere kodlanmış

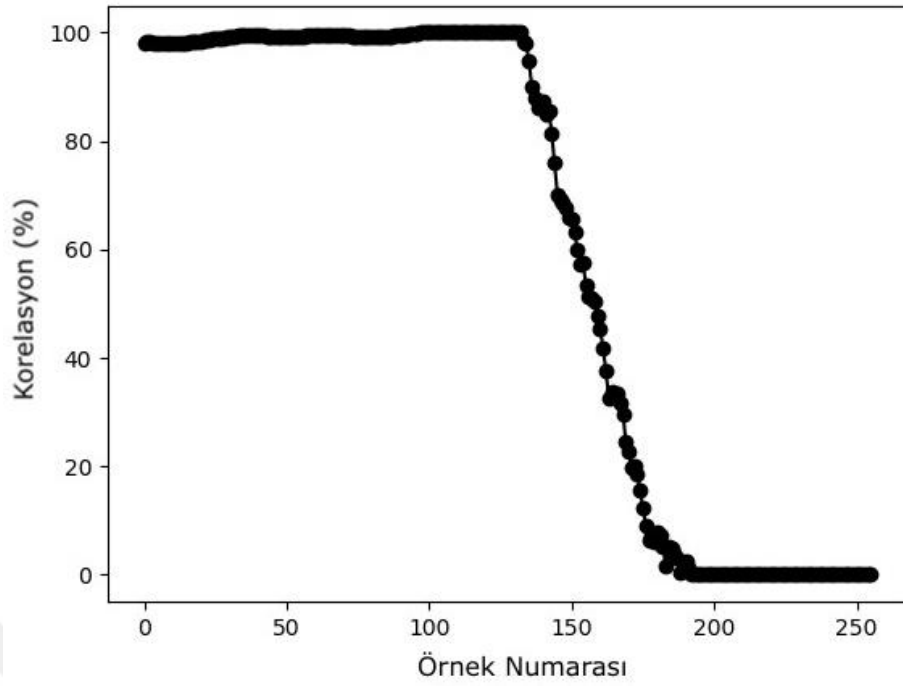
asıl bilgiyi taşımaktadır. OFDM paket yapısının görsel temsili Şekil 3.2 [64] ile verilmiştir. OFDM'nin bu yapılandırması, WiFi sinyallerinin hem verimli hem de güvenilir bir şekilde aktarılmasını mümkün kılmaktadır.



Şekil 3.2. WiFi sinyalindeki OFDM sembollerinin paket yapısı

3.1.3 Paket Tespiti

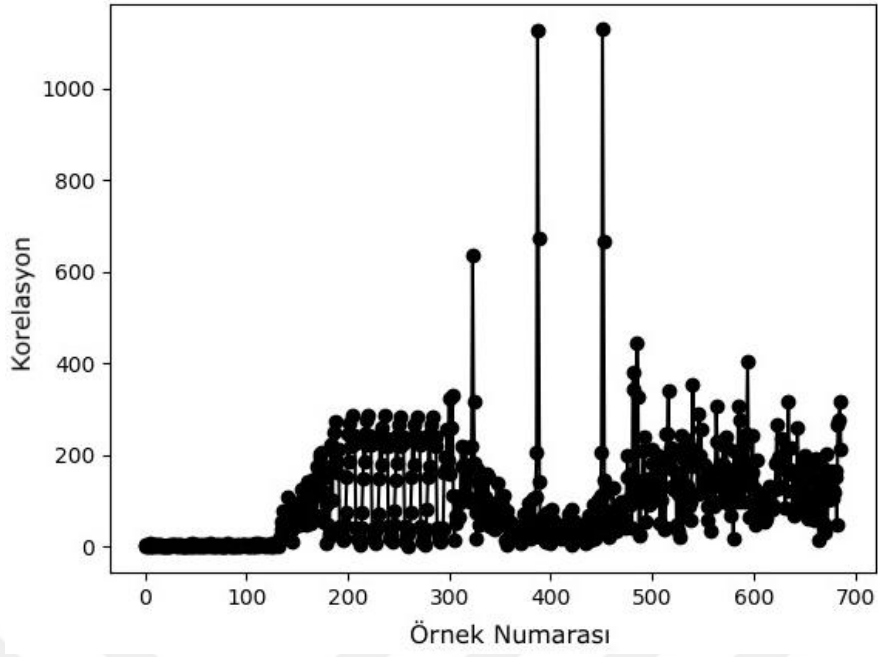
OFDM sembolleri içinde paketin algılamasını kolaylaştırmak için kısa bir başlangıç dizisi göndermektedir. Bu dizi, toplamda 16 I/Q örneğinden oluşan ve 10 kez tekrar eden bir yapı ile tasarlanmış olup, böylece toplamda 160 örnek içermektedir. Alıcının paketin varlığını tespit edebilmesi için, tekrar eden bu diziler arasında bir korelasyon ilişkisi kurulması gerekmektedir. Her örneğin, 16 örnek sonrasındaki değerle korelasyonu hesaplandığında, eğer paket gelmişse, korelasyonun bir artış gösterdiği bir grafik elde edilir. Bu durum, Şekil 3.3 [64] ile verilen grafikte açıkça görülebilir. Grafikte, korelasyonun tutarlı bir şekilde kurulduğu gözlemlenmiş ve bu süreç, bir algoritma yardımıyla otomatik olarak değerlendirilerek, OFDM paketinin varlığı doğru bir şekilde tespit edilmiştir.



Şekil 3.3 Paketin yakalanması sırasında kullanılan grafiğin gösterimi

3.1.3.1 Senkronizasyon

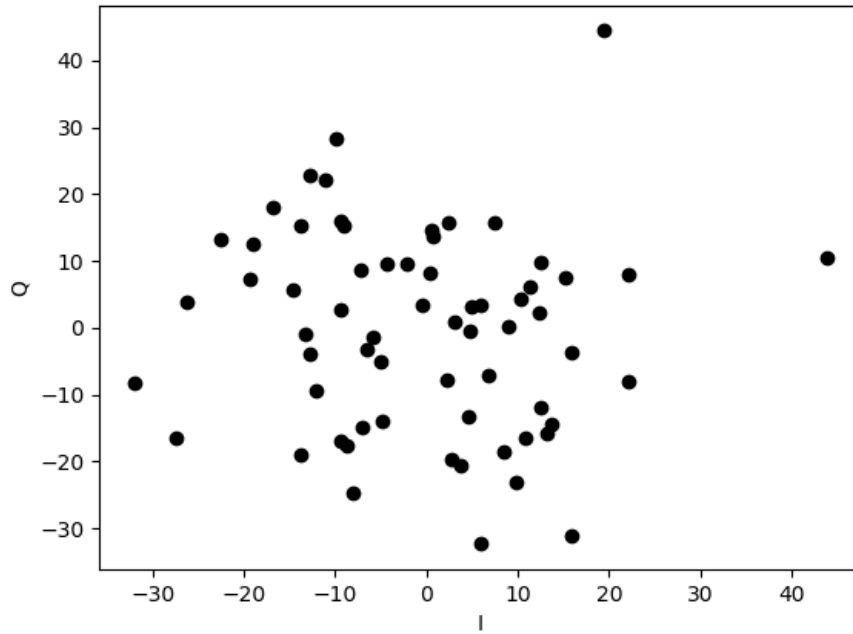
Paketin tespit edilmesinin ardından, OFDM sinyalinin başlangıç noktasını belirlemek için uzun başlangıç dizisi (LTS) kullanılmaktadır. Bu dizi, gelen sinyalin belirli bir referans işaret ile matematiksel olarak karşılaştırılarak eşlenik bir filtreleme yöntemiyle analiz edilmesi yoluyla tespit edilmektedir. İşlem sonucunda, Şekil 3.4'te [64] gösterilen sinyal elde edilmekte ve sinyal üzerinde iki belirgin tepe noktası ortaya çıkmaktadır. Bu tepe noktaları, uzun başlangıç dizisinin başlangıcını işaret eder. Paketin başlangıç noktasını belirlemek için bu tepe noktaları kullanılır. İlk tepe noktasından itibaren koruma aralığı ve kısa başlangıç dizisinin uzunluğu kadar geri gidilerek, OFDM sinyalinin kesin başlangıç noktası hesaplanır. Bu yöntem, zaman senkronizasyonunu doğru bir şekilde yapmayı mümkün kılarken, aynı zamanda sinyal işleme algoritmalarının hassasiyetini artırır. Uzun başlangıç dizisinin bu kritik rolü, OFDM tabanlı iletişim sistemlerinde sinyal algılama ve senkronizasyon süreçlerinin temel taşlarından birini oluşturmaktadır.



Şekil 3.4 Senkronizasyon için elde grafiğinin gösterimi

3.1.3.2 Demodülasyon

Radyo frekans sinyallerin iletimi sırasında faz kayması meydana gelebilmekte ve bu durum sinyallerin değişmesine yol açabilmektedir. Senkronizasyon işleminin ardından elde edilen OFDM paketine ait sinyal çerçevesi, Şekil 3.5 [64] ile sunulmuştur.



Şekil 3.5 Ham sinyalin takım yıldız diyagramı

Alınan sinyallerin doğruluğunu sağlamak ve hataları düzeltmek için kaba düzeltme, ince düzeltme ve pilot düzeltme olarak üç aşamalı bir süreç izlenmektedir. OFDM paketlerinde, veri bölümlerinde kullanılan modülasyon türü ve hız bilgileri “sinyal” paketinde saklanır ve bu bilgiler İkili Faz Kaydırmalı Anahtarlama (Binary Phase Shift Keying, BPSK) yöntemiyle kodlanmıştır. Bu süreçte ilk olarak, sinyal paketindeki olası faz kaymaları düzeltilir ve ardından bu paket analiz edilerek veri çerçevelerinde kullanılan modülasyon tekniği ve hız parametreleri tespit edilir. Bu yöntem, iletilen verinin doğru bir şekilde çözümlenmesini ve iletişim kanalındaki bozulmaların etkisinin minimuma indirilmesini sağlar.

Kaba Düzeltme

Kaba düzeltme, OFDM sinyalindeki zamanlama ve frekans kaymalarını yaklaşık olarak gidermek için gerçekleştirilir. Bu adım, sinyalin genel yapısını hizalamayı ve sonraki ince düzeltme aşamasına uygun bir temel oluşturmayı amaçlamakta olup (3.1) denklem ile kaba düzeltme bulunabilmektedir.

$$a_s = \frac{1}{16} \angle \sum_{i=1}^n \bar{S}_i S_{i+16} \quad (3.1)$$

Denklem (3.1) ile elde edilen kaba düzeltme ise denklem (3.2) ile sinyal üzerine uygulanabilmektedir.

$$S'[m] = e^{-jma} \quad (3.2)$$

İnce Düzeltme

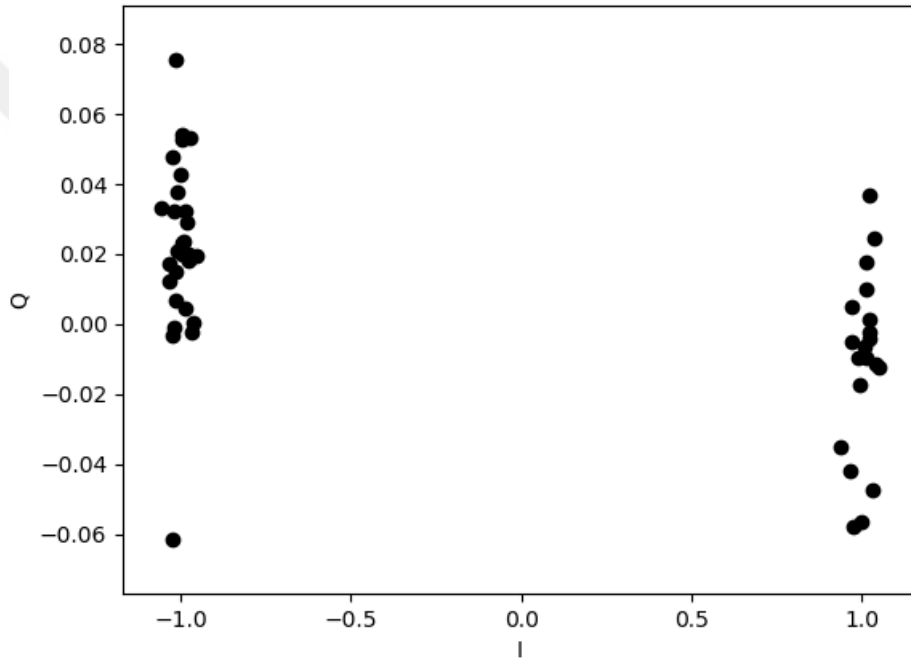
İnce düzeltme, OFDM sinyalinde zamanlama ve frekans kaymalarını daha hassas bir şekilde gidermek için yapılan detaylı bir işleme adımındır. Bu aşamada, kaba düzeltmeden kalan küçük hata bileşenleri minimize edilerek sinyalin alt taşıyıcıları tam olarak hizalanır ve veri iletimi için ideal koşullar sağlanır. İnce düzeltme, genellikle sinyalin faz ve genlik bilgilerinin detaylı analizine dayanır ve yüksek doğruluk gerektiren uygulamalar için kritik bir rol oynar. Uzun başlangıç dizisi, birbirinin aynısı olan iki 64 örnekten oluşan paket serisi şeklindedir. Bu paketlerin her biri, aynı faz açısına sahip örnekler içermektedir. İki paket arasındaki faz farkları hesaplanarak, ince düzeltme için gerekli ofset değerleri denklem (3.3) yardımıyla elde edilir.

$$a_L = \frac{1}{64} \sum_{i=1}^{64} \bar{S}_i S_{i+64} \quad (3.3)$$

Kaba düzeltmedekine benzer bir biçimde elde edilen ince düzeltme değeri denklem (3.2) ile sinyal üzerine uygulanmaktadır.

Pilot Düzeltme

Pilot sinyaller, protokolde belirli bir faz açısına sahip sabit işaretlerdir ve gelen sinyaldeki kaymalar, bu sinyallere bakılarak düzeltilebilmektedir. Bu işlem sonucunda elde edilen düzeltilmiş sinyal, Şekil 3.6 [64] ile gösterilmektedir.



Şekil 3.6 Düzeltme işlemlerinden sonra elde edilen takımyıldız diyagramı

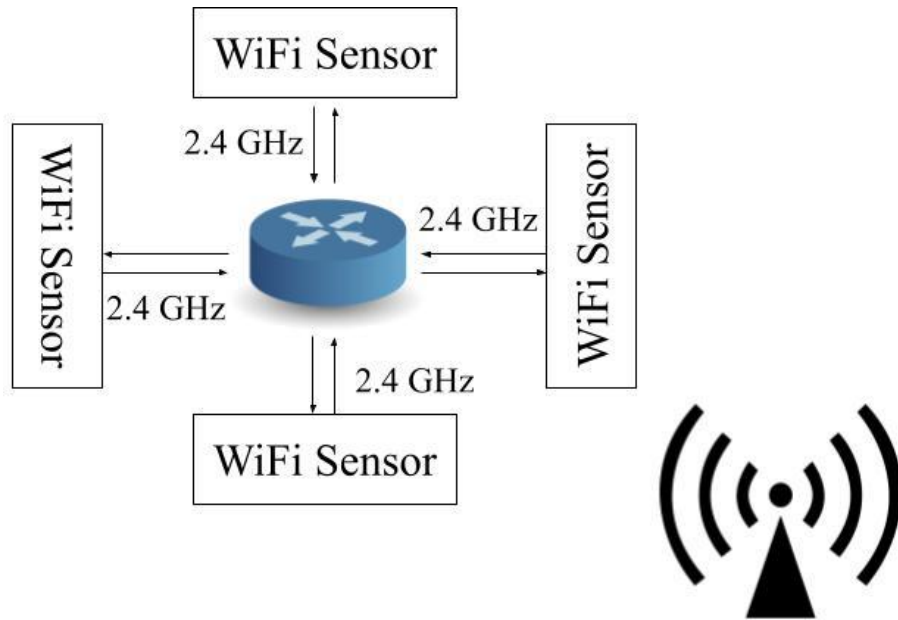
3.1.3.3 Çözümleme

Sinyal başlığında bulunan bilgilerin modülasyonu, BPSK yöntemiyle gerçekleştirilmiş olmasına rağmen, veri modülasyonlarının bilgileri sinyalin içinde gizli bir şekilde bulunmaktadır. Sinyal bileşenlerdeki modülasyon türü ve iletim hızı gibi kritik bilgiler başlangıç paketi üzerinden tespit edilir. Bu bilgiler çözümlendikten sonra, veri sinyaline uygun demodülasyon yöntemleri kullanılarak sinyaldeki kaymalar düzeltilir ve düzeltme işlemlerinin ardından,

sinyalin modülasyon tekniğine uygun olarak veriler demodüle edilip bit dizileri oluşturulur. Ardından, Viterbi algoritması kullanılarak bu bit akışının hata düzeltme kodları çözülür ve veri çıkartılır. Bu süreçte, oluşturulan bitler içinde yer alan MAC adresi ve paket içeriği, 802.11 protokolüne uygun olarak yapılandırılmıştır. Bu protokol bilgisi sayesinde, MAC adresi ve veri içeriği doğru bir şekilde ayrıştırılabilir.

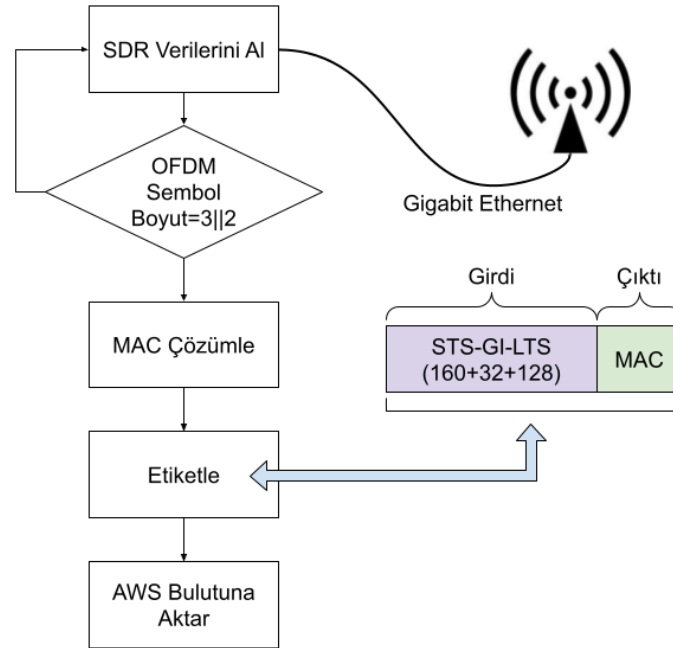
3.1.4 Veri Setinin Oluşturulması

Veri toplama için oluşturulan düzenek, Şekil 3.8 ile gösterildiği gibi yapılandırılmıştır. 2.4 GHz frekansında 20 MHz bant genişliğini dinleyebilen SDR cihazı, veri setini toplamak için kullanılmıştır. WiFi sinyalleri üretmek için ise 802.11g protokolünü destekleyen WiFi Sensor cihazları kullanılmıştır. Ortamda düzenli WiFi sinyali, 6 adet WiFi Sensor cihazı ile “hping” programı aracılığıyla üretilmiştir. Hping modülü, normal ping modülüne kıyasla belirli bir IP adresine çok daha kısa aralıklarla paket gönderebilme yeteneğine sahiptir. Yazılım ve hizmetler sayesinde, her bir WiFi Sensor cihazından yönlendiriciye saniyede 100 paket gönderilmiştir.



Şekil 3.7 Veri seti üretimi için SDR ile WiFi Sensörleri iletişiminin dinleme diyagramı

SDR cihazı, paketleri alır ve cihazın geçici belleğinde saklar. SDR belleğindeki verileri çözümlmek ve etiketlemek için Nvidia Jetson AGX Xavier cihazı kullanılmıştır. Gigabit Ethernet üzerinden SDR'a bağlanan Xavier cihazı, kullanılan SDR'ın kütüphanesi aracılığıyla gerçek zamanlı olarak alır. OFDM paketleri, GPU üzerinde WiFi sinyallerinin çözümlendiği [64] referansındaki çalışmada kullanılan yöntemlerle çözülmüştür. Çözümleme işlemlerinin ardından, Önsöz (Preamble) sinyal verileri MAC adresi ile etiketlenmiş ve bir NumPy dosyası olarak kaydedilmiştir. Ayrıca, OFDM sembol numarası kullanılarak tüm veri bir NumPy dosyası olarak saklanmıştır. Bu sayede hem OFDM hem de Önsöz verilerinin eğitim sırasında kullanılabileceği bir sistem oluşturulmuştur. Ek olarak, oluşturulan hizmet sayesinde verilerin sürekli olarak alınması da sağlanmıştır. Verilerin etiketlenmesi için kullanılan yapının genel blok diyagramı Şekil 3.8 ile sunulmuştur. Verilerin geniş bir veri havuzunda toplanabilmesi için, ağın kullanılmadığı zaman dilimlerinde iş zamanlayıcısı (cron job) kullanılarak AWS Bucket'a aktarımı gerçekleştirilmiştir. Aktarım sırasında bit bozulmaları nedeniyle oluşan MAC hatalarında dosyalar AWS'ye aktarılmadan önce silinmiştir. Alınan verilerin %0,9'unda bit bozulmaları gözlemlenmiştir. Bit bozulmalarını önlemek ve bozuk bitleri düzeltmek için özel çalışmalar bulunmaktadır [114], [115].

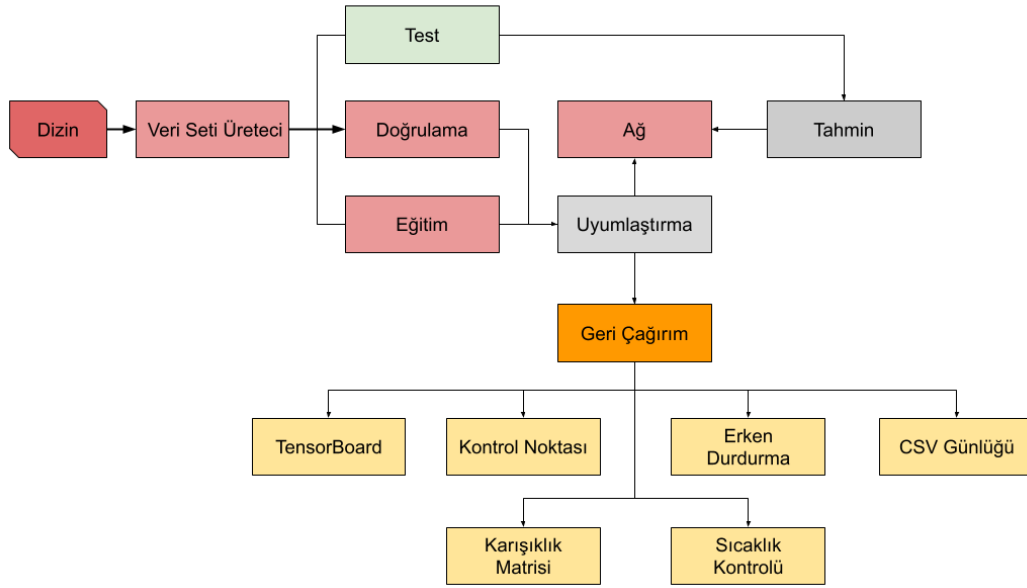


Şekil 3.8 Veri seti oluşturma algoritması ve etiketleme mimarisi

3.1.5 Derin Öğrenme

Derlenen verilerin derin öğrenmede kullanılabilmesi için bir model oluşturma sürecinde birkaç aşamadan geçilmesi gereklidir. Derin öğrenme için kullanılan yapının mimarisi Şekil 3.9 ile gösterilmiştir. Modelin eğitimi sırasında, eğitimi izlemek ve gerektiğinde modeli geri yüklemek için birkaç geri çağırım (callback) kullanılmıştır. Sistemde TensorBoard, kontrol noktası (checkpoint), erken durdurma, CSV kaydedici, karışıklık matrisi ve sıcaklık sınırı olmak üzere altı geri çağırım (4 yerleşik ve 2 özel) uygulanmıştır.

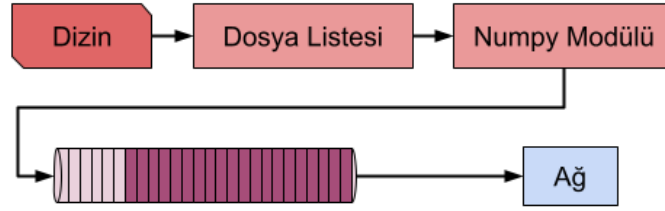
TensorBoard, modelleri karşılaştırmak, eğitim ve doğrulama doğruluklarını izlemek, bellek kullanımını kontrol etmek gibi işlemleri gerçekleştirmek için bir grafik kullanıcı arayüzü sağlar. Kontrol noktası, bir epok sırasında daha yüksek doğrulama doğruluğu elde edildiğinde model ağırlıklarını kaydeder ve önceden eğitilmiş ağırlıklar kullanılarak modelin geri yüklenmesini sağlar. Erken durdurma, tanımlı bir epok süresi boyunca önemli bir iyileşme gözlemlenmediğinde eğitimi durdurur ve model ağırlıklarını kaydetmek için düzenli bir protokol sunar. CSV kaydedici, istenen metrikleri bir tablo olarak CSV dosyasına kaydeder. Karışıklık matrisi, modeli düzenli olarak bir tahmin görevi için çalıştırır ve karışıklık matrisini oluşturur. Bu, modelin iyileştirmesini takip etmeyi ve hataların nerede olduğunu görmeyi kolaylaştırır. Sıcaklık sınırı, GPU'nun aşırı ısınmasını önler. Bu durumda, GPU sıcaklığının tanımlanan eşik değerinin çok üzerine çıktığını tespit eder ve erken durdurma protokolünü tetikler.



Şekil 3.9 Derin öğrenme modeli için kullanılan sistemin kod mimarisi

Girdi hattı (input pipeline), verimli bir bellek yönetim sistemini ifade etmekte olup dizindeki tüm örneklerin okunup bellekte saklanmasını içermektedir. Bu yöntem dosya yönetimini oldukça kolaylaştırır da büyük veri kümeleri için büyük miktarda bellek gerektirir. Verilerin toplam boyutunun büyük olması ve GPU belleğinde yeterli alan bulunmaması nedeniyle veri setindeki dosyaların yolları kullanılarak bir girdi hattı oluşturulmuştur. Girdi hattı belirtilen dizindeki tüm NumPy dosyalarının yollarını alır ve bunları belleğinde bir liste olarak tutar. Eğitim sırasında veriler NumPy modülü ile açılır ve girdi hattı üzerinden derin öğrenme ağına iletilir. Ayrıca girdi olarak verilen verilerin yanı sıra çıktı vermek için dosya adından MAC adresi ayrıştırılarak elde edilmektedir. MAC adresi elde edildikten sonra kullanılan cihaz sayısı algoritma ile belirlenir. Oluşturulan veri kümesinde altı farklı cihaz bulunmaktadır. Ağ yapısında kullanılan kategorik eğitim modeline göre çıktı katmanının otomatik olarak 20 olması gerekmektedir. Böylece, altı farklı MAC adresi için altı farklı ikili (binary) veri bulunmaktadır. Çıktı verileri de bu formatta girdi verileriyle birlikte girdi hattına iletilmiştir. Oluşturulan girdi hattı yapısının mimarisi Şekil 3.10 ile verilmiştir. Literatürde dosyaları okumak ve alınan sinyaller hakkında bilgi vermek için bir meta dosya oluşturulup kullanıldığı görülmektedir [116]. Ancak bu çalışmada yalnızca belirli

bir frekans, protokol ve bant genişliği kullanıldığından bir meta dosyasına ihtiyaç duyulmamıştır.



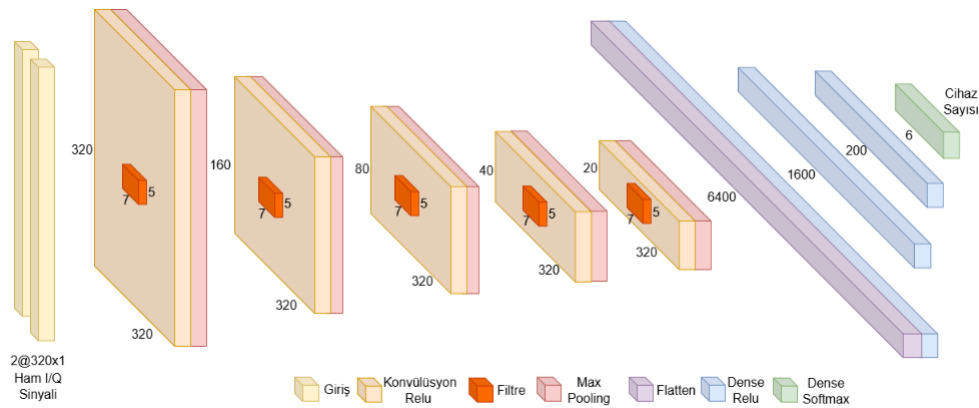
Şekil 3.10. RAM'i belirli bir sınırdan tutmak için giriş boru hattı yapısı

Veri kümesi uygun bir model eğitim aşaması için eğitim (train), doğrulama (validation) ve test olmak üzere üç alt kümeye bölünmelidir. Bu sistemde tanımlanan varsayılan bölme oranına göre veri kümesinin %80'i eğitim setine ayrılırken, doğrulama ve test setleri için %10'ar oranında veri ayrılmaktadır. Doğrulama seti, her bir epoktan sonra eğitim sırasında değerlendirme yapmak için kullanılır. Modelin aşırı öğrenme (overfitting) yapıp yapmadığını izlemek için doğrulama doğruluğu ve kaybı raporlanır. Öte yandan test seti modelin ağırlıkları bir daha güncellenmeyecek şekilde eğitimin tamamen sona erdiği noktada değerlendirme yapmak için kullanılır. Eğitim, doğrulama ve test jeneratörleri, eğitim veya test partilerini oluşturmak için bölmeleri (splits) bir araya getirmekten sorumludur. Her bir jeneratörün bir bölmeyi yalnızca bir kez kullanmasını sağlamak amacıyla, benzersiz tanımlayıcılar bir liste halinde saklanır. Bu liste daha sonra karıştırılır ve önceden belirtilen bölme oranlarına göre öge sayılarına sahip üç ayrı alt kümeye ayrılır. Bellek trafiğini verimli bir şekilde yönetmek için sistem, indeks listesinden indeksleri alır ve bölmeleri kayıt dosyalarına göre gruplandırarak oluşturur. Bu fikir, sistemin tek bir dosya I/O (girdi/çıkış) işlemiyle birden fazla bölme oluşturmaya olanak tanır ve okuma işlemlerinin sayısını batch boyutundan dosya sayısına indirerek performansı artırır.

Girdi hattından alınan verilerle eğitim yapmak için uygun bir derin öğrenme modeli oluşturulmalıdır. Literatürde zaman serisi sinyallerinin eğitimi konusunda yüksek performansıyla bilinen TCN modeli, Şekil 3.11 ile gösterildiği gibi oluşturulmuştur. TCN modeli, Python'da TensorFlow kütüphanesi kullanılarak geliştirilmiştir. TensorFlow kütüphanesi hem CPU hem de GPU üzerinde eğitim yapılmasına olanak tanımaktadır. Böylece derin eğitim sırasında kullanılan ve

GA102 çekirdeği üzerine kurulu 10.496 CUDA çekirdeğine sahip GeForce RTX 3090 cihazının GPU'su kullanılabilmektedir.

İlk olarak, ağı girişine I bileşenini temsil eden bir vektör ve Q bileşenini temsil eden bir diğer vektör olmak üzere iki adet 1D vektör beslenmiştir. Bu, 320 örnekten oluşan iki kanallı bir sinyal gibi davranmaktadır. İleri geçiş (forward pass) sırasında bu giriş, her biri aynı parametrelere sahip beş evrişimsel bloktan geçirilmiştir. Bir evrişimsel blokta, filtre boyutu (320, 320) ve çekirdek boyutu (7, 5) olan iki evrişimsel katman bulunmaktadır. Evrişimsel bloğun son işlemi olan maksimum havuzlama (max pooling) işlemi, kayma değişmezliği (shift-invariance) sağlamak ve çıktı özellik haritalarının boyutlarını azaltmak için uygulanmıştır. Evrişimsel bloklar boyunca filtre boyutu sabit kaldığı için, özellik haritalarının sayısı ilk geçişte 2'den 320'ye çıkmakta ve sonraki geçişlerde aynı kalmaktadır. Ancak, maksimum havuzlama katmanı her adımda iki değer arasından maksimum olanı seçtiğinden, özellik haritalarının uzunluğu her adımda yarıya inmektedir. Bu azaltma işlemi ardışık olarak dört kez uygulandığında, 1x6 boyutlarında 320 özellik haritası elde edilmiştir. Daha sonra bu haritalar, 6400 uzunluğunda bir vektör halinde düzleştirilmiştir (flatten). Sınıflandırıcı bloğunda, sırasıyla (1600, 200, sınıf sayısı) nöronlara sahip üç yoğun katman (dense layer) bulunmaktadır ve bu katmanlarda vektörün uzunluğu daha da azaltılmaktadır. Son katmanda Softmax sınıflandırıcı fonksiyonu kullanıldığı için, çıktı vektöründeki her bir indeksin bir etiketi temsil ettiği ve her etiket için sınıfa özgü olasılıkların görülebildiği bir yapı elde edilmiştir.



Şekil 3.11 WiFi cihazlarını kimliklendirmek için kullanılan model

3.1.6 Deneysel Sonular

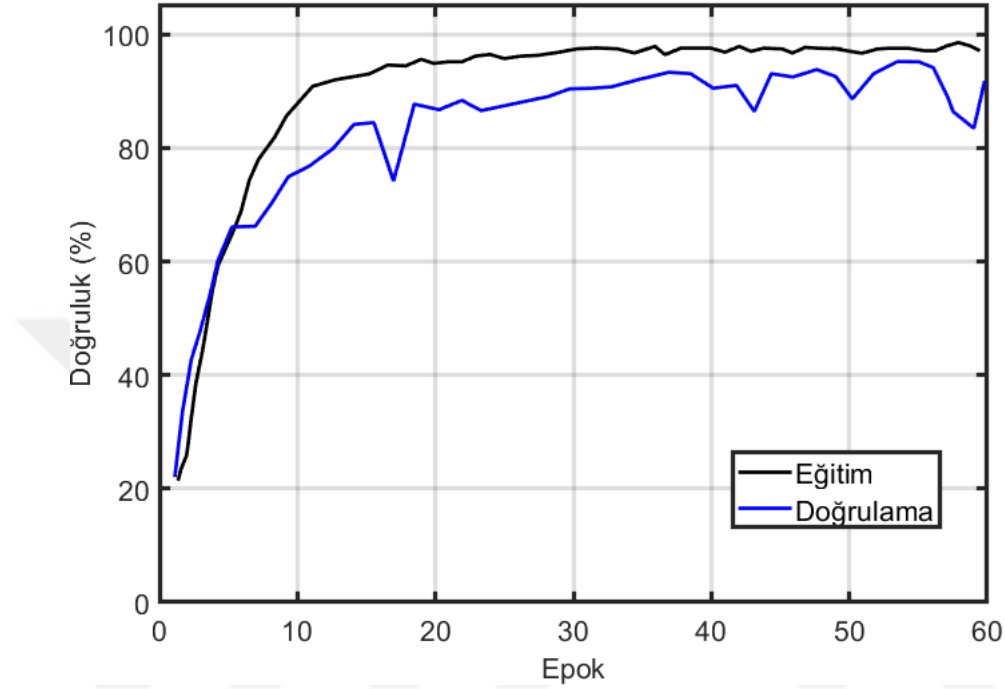
Oluřturulan sistemde NVIDIA Jetson AGX Xavier geliřtirme kiti, SDR zerinden verileri Python ile anlık olarak almaktadır. Burada oluřturulan sistemin fiziksel grnts řekil 3.12 ile verilmiřtir. Grldė zere SDR antenleri zerinden aldėėı sinyalleri Gigabit Ethernet zerinden aktarabilmektedir. Bu nedenle yksek hızlarda verilerin AGX zerine aktarımı gerek zamanlı olarak saėlanabilmektedir.



řekil 3.12 SDR ile AGX cihazının aė zerinde baėlantısı

Sistemin gerekli testlerini gerekleřtirmek ve sonuların tutarlılıėını incelemek amacıyla, oluřturulan veri kmesinin son 10 gnlk verileri ile eėitim yapılmıřtır. Eėitilen TCN modeli, toplamda altı farklı MAC cihazı ve  milyon dosyayı

içermektedir. Kullanılan verilerin toplam boyutu 16.4 GB'dir. Veri toplama sürecinde gerçekleştirilen normalizasyon işlemi sayesinde, toplanan veriler derin öğrenme sürecinde herhangi bir ön işleme tabi tutulmadan derin öğrenme modeline beslenmiştir. Eğitim sonucunda elde edilen doğruluk oranı eğrisi Şekil 3.13 ile sunulmaktadır.



Şekil 3.13 Derin öğrenme modelinin dönem sayılarına göre doğruluk oranı

Ayrıca, LSTM (Long Short-Term Memory) ve RNN (Recurrent Neural Networks) gibi çeşitli derin öğrenme algoritmaları kullanılarak eğitim gerçekleştirilmiş ve elde edilen sonuçlar Tablo 3.1 ile detaylandırılmıştır. LSTM ve RNN mimarileri için kullanılan modeldeki katman ve hücre sayıları da Tablo 3.1 ile sunulmuştur. Giriş ve çıkış katmanları, derin öğrenme bölümünde açıklanan TCN algoritması ile tutarlıdır. Sistemin periyodik yeniden eğitim süreçlerine tabi tutulacağı göz önünde bulundurularak, derin öğrenme modelinin eğitim süresi seçim sürecinde dikkate alınmıştır. TCN modeli hem eğitim süresi hem de doğruluk açısından en iyi sonuçları verdiği gözlemlenmiştir.

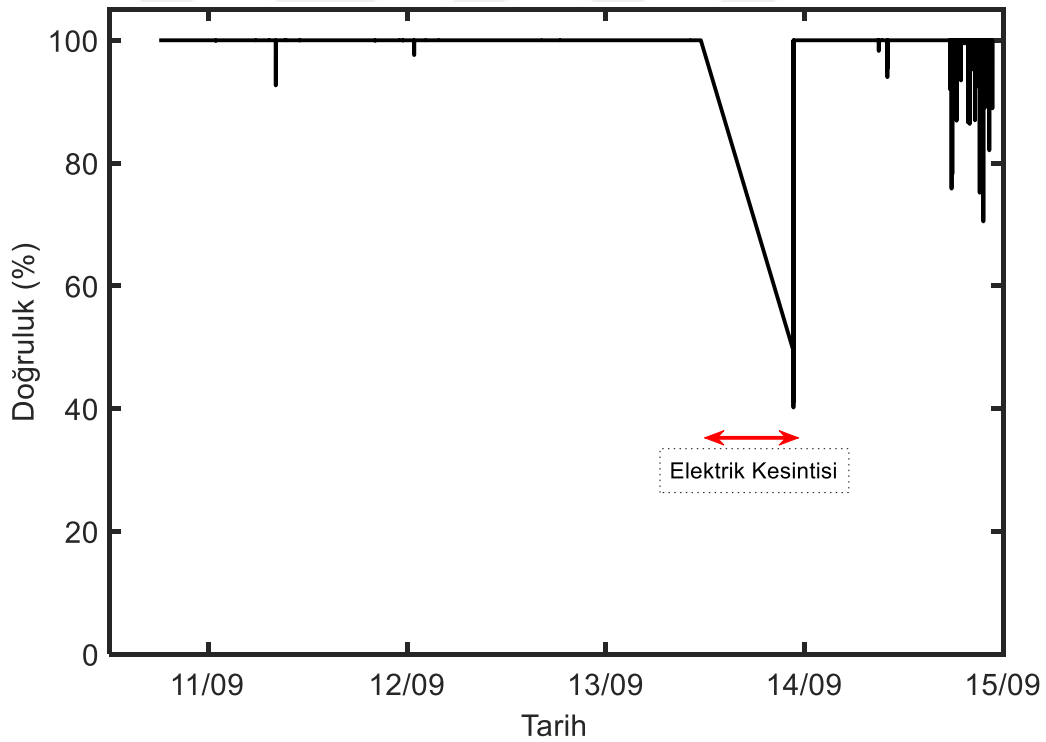
Tablo 3.1 Modelin farklı algoritmalar ile oluşturulmasının analizi

Algoritma	Katman Sayısı	Hücre Sayısı	Doğruluk (%)	Epoch Süresi
CNN	5	-	99.47	34 Dakika
LSTM	5	10	98.45	3 Saat
RNN	3	2	95.34	17 Saat

Derin öğrenme eğitimi sonrasında oluşturulan model, uç birim hesaplama için eGPU'ya aktarılmış ve sistemin gerçek zamanlı testi başlatılmıştır. Sistem testleri sırasında elde edilen sonuçlar, yalnızca bir cihaz için olup Şekil 3.14 ile gösterilmiştir. Gerçek zamanlı testin sonuna doğru, derin öğrenme modelinin performansında belirgin bir düşüş gözlemlenmiştir. Bu durum, cihazın içindeki pasif bileşenlerin ve yarı iletkenlerin zamanla değişen özelliklerine bağlanmıştır. Bu nedenle, sistemin bütünlüğünü sağlamak amacıyla güvenli zaman dilimlerinde yeni toplanan verilerle periyodik olarak yeniden eğitilmesi gerektiği açıkça görülmüştür. Yeniden eğitim sürecinin hızlı bir şekilde gerçekleştirilebilmesi gömülü GPU'ya sahip bir uç cihazda verimli bir şekilde yürütülebileceğini göstermektedir. Bu doğrultuda kapalı ağ sistemlerinde yalnızca ilk eğitim sırasında Önsöz verisinin iletilmesi yeterli olmakta ve sonraki süreçlerde GPU sunucusuna ihtiyaç duyulmamaktadır. Transfer öğrenimi (transfer learning) yaklaşımı kullanılarak, mevcut modele belirli aralıklarla yeni veriler eklenmiş ve periyodik olarak yeniden eğitilmiştir. Ayrıca, sistemin başlangıç durumundaki performansını değerlendirmek amacıyla sistemin gücü bilinçli olarak kesilmiş ve altı saatlik bir süre sonrasında yeniden başlatılmıştır. Şekil 3.14 ile görüldüğü üzere, sistemin performansı başlangıçta düşük bir seviyede başlamış ve zamanla iyileşmiştir. SDR cihazının bileşenleri ısıdıkça elektriksel sinyal özelliklerinde değişiklikler meydana gelmektedir. Bu değişimler, yarı iletken malzemelerin sıcaklığa bağlı özelliklerinden kaynaklanmakta olup iletkenlik davranışı, kapasitans ve diğer elektriksel parametreler üzerinde önemli bir etkiye sahiptir.

Bu durum özellikle sinyal işleme ve analiz görevlerinde SDR'nin genel performansını ve doğruluğunu etkilemektedir.

Veri toplama sırasında SDR cihazı ısınmış bir durumda çalışırken veri toplandığından SDR'nin soğuk olduğu durumlarda modelin performansı daha düşük olmaktadır. Bu nedenle, önerilen yaklaşımda sistemin güvenlik kontrollerine başlamadan önce SDR'nin belirli bir süre çalıştırılarak kararlı bir sıcaklık seviyesine ulaşması sağlanmıştır. Bununla beraber ayrıca kimliklendirme çalışmalarında verinin gönderildiği kartın karakteristik özelliği kadar alıcı tarafındaki SDR cihazının da karakteristik özelliği önemlidir. Aynı marka ve modelde olsalar bile tolerans değerinden kaynaklı olarak her SDR cihazı farklı pasif bileşen değerlerine ve yarı iletken özelliklerine sahiptir. Bundan dolayı kimliklendirme çalışmalarında sinyallerin toplandığı SDR cihazı ile güvenlik kontrollerinin yapıldığı sıradaki SDR cihazı aynı olmalıdır.



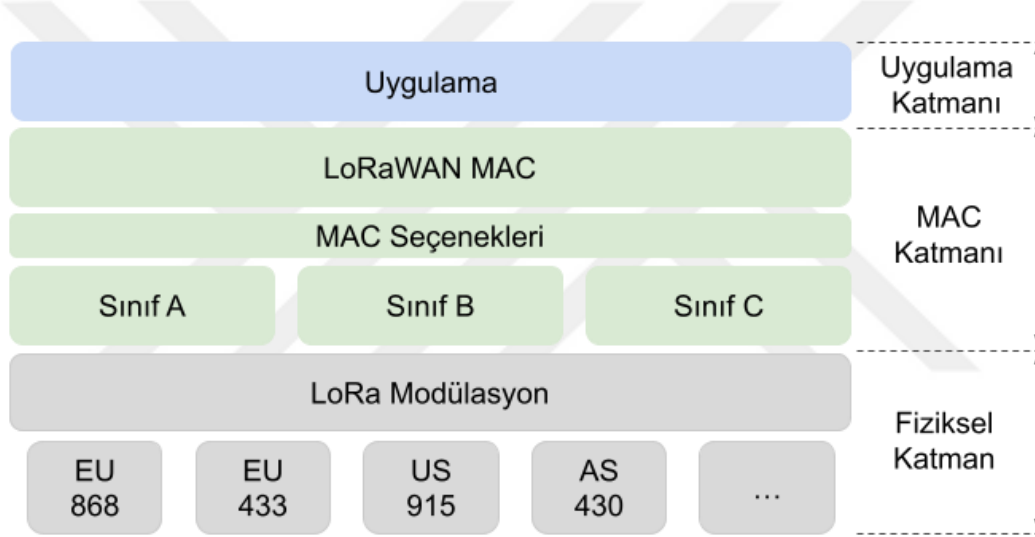
Şekil 3.14 Sistemde tanımlı bir cihaz için gerçek zamanlı başarım oranı

Sahtecilik amacıyla dijital kimliklerin çalınmasının ötesinde, farklı bir SDR kullanılarak WiFi sinyallerinin dinlenip yeniden iletilmesi yoluyla da sahtecilik yapılması mümkündür. Ancak, bir SDR cihazı kullanılarak gizli bir şekilde sinyal

dinleme ve yeniden iletim girişiminde bulunulduğunda, SDR'nin elektronik özellikleri hem sinyalin alınması hem de iletilmesi sırasında bu sinyalleri etkiler. Sonuç olarak, aynı sinyal iletilse bile, güvenlik kontrolü yapan SDR'de tamamen aynı sinyalin alınma olasılığı düşüktür. Bu durum, sinyallerin dinlenip kopyalanarak sistemi ele geçirme girişimlerinin mümkün olmadığını göstermektedir.

3.2 LoRa (Long Range) Cihazlarının Kimliklendirilmesi

Haberleşme sistemlerinde verinin kullanıcılara ulaşması için geçtiği belirli katmanlar bulunmaktadır. LoRa haberleşmesinde bu katmanları ifade etmek için oluşturulmuş OSI modeli Şekil 3.15 ile verilmiştir.

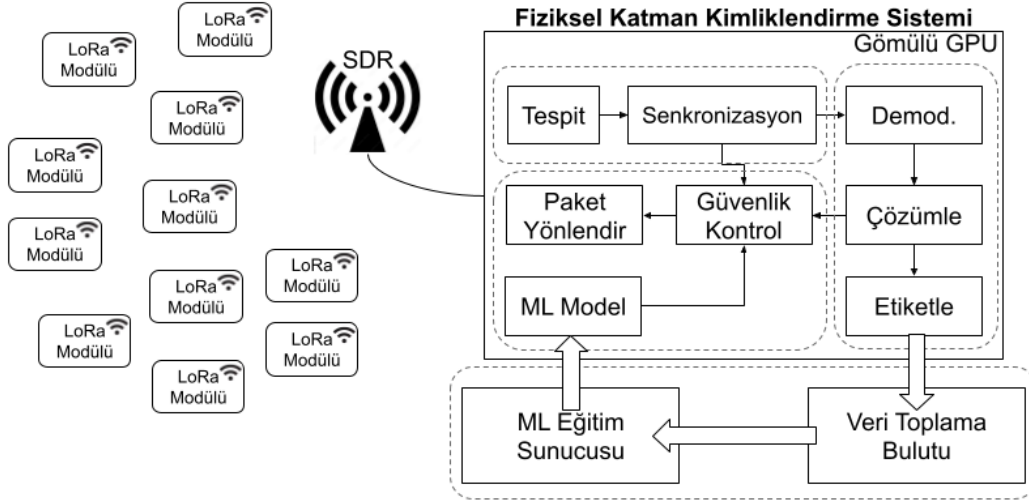


Şekil 3.15 LoRa haberleşmesi için oluşturulmuş OSI katmanları

Görüldüğü üzere gelen veri öncelikle fiziksel katmanda alınmakta ve demodülasyon işlemleri yapılmaktadır. Elde edilen veri çözülünerek MAC katmanına aktarılmaktadır. MAC katmanından sonra ise Uygulama Katmanına aktarılarak kullanıcının işlemine sunulmaktadır. Literatürde bulunan çalışmalarda genel olarak güvenlik kontrolü çözümü yapıldıktan sonra dijital olarak yapılmaktadır. Bu da farklı teknikler ile cihazların taklit edilebilir olmasına sebep olmaktadır.

Kimliğe bürünme ataklarına karşı sinyalin dijitale dönüşmeden önce fiziksel katmanda güvenlik sağlanması gereklidir. Güvenliğin sağlanması için ham sinyal üzerinden cihaz kimliğinin oluşturulması ve sonrasında da bu kimliğin gerçek

zamanlı kontrol edilmesi gerekmektedir. Fiziksel katmanda ham sinyalin bilgisayar ortamına alınması SDR ile yapılabilmektedir. Cihazların kimliklendirilmesi için alınan ham sinyalin paket içeriği çözümlenmeli ve ham sinyaller cihazlara göre etiketlenmelidir. Sistemin gerçek zamanlı çalışması da gerekmesinden dolayı sistem çözümleme ve derin öğrenme ile kimlik kontrolünü paralel bir şekilde gömülü GPU üzerinde yapılmaktadır. Önerilen sistemin mimarisi Şekil 3.16 ile verilmiştir.



Şekil 3.16 LoRa cihazlarının kimliklendirilmesi için önerilen sistem

3.2.1 LoRa Sinyal Karakteristiği

LoRa cihazlarının modülasyon tekniği, CSS modülasyonuna dayanmaktadır ve bir "civıltıyı" tek bir sembol olarak tanımlar. Standart, modüle edilmemiş bir lineer civıltı, "temel civıltı" olarak adlandırılır ve matematiksel olarak denklem (3.4) ile verildiği gibi tanımlanabilmektedir [56]. Burada $s(t)$ işareti, civıltı sinyalini; f_c , taşıyıcı frekansını; β , bant genişliği (Band Width, BW) ile sembol süresi (T_{sym}) arasındaki oranı ve t , zamanı temsil etmektedir.

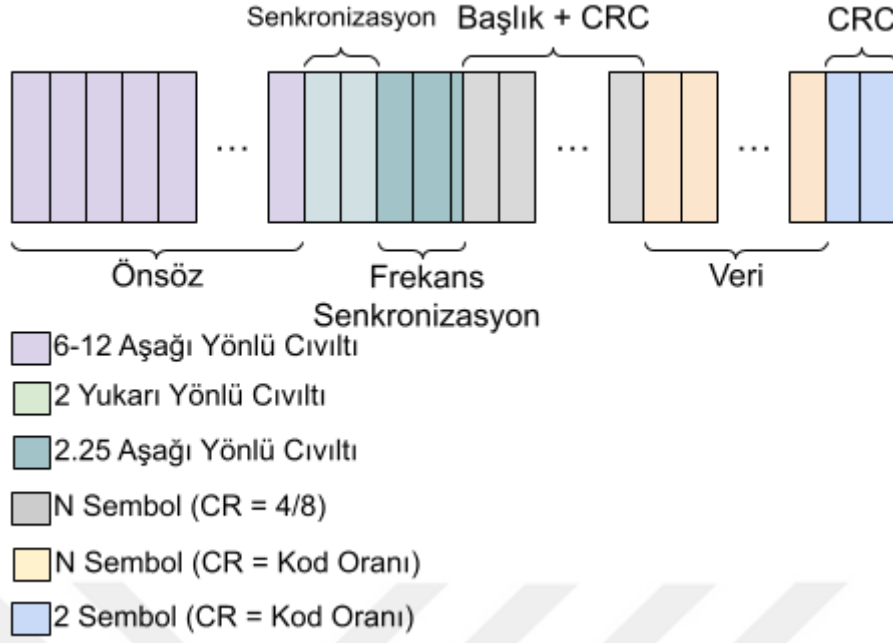
$$s(t) = e^{j\left(2\pi f_c t + 2\frac{\beta}{2}t^2\right)} \quad (3.4)$$

Gönderilecek olan paketin uzunluğunu ve hızını ayarlamak için Yayılım Faktörü (Spreading Factor, SF) kullanılmaktadır. SF'in artması haberleşme mesafesinin artmasını sağlamaktadır ve LoRa haberleşmesinde SF 7 ile 12 arasında

ayarlanabilmektedir. Paket içindeki sembollerin uzunluğu ise 2^{SF} ile belirlenmektedir ve SF değişimine göre veri aktarım hızı denklem (3.5) ile verilmiştir. Görüldüğü üzere SF'in artması ile aktarım hızı yavaşlamaktadır. Burada DR , veri oranını; BW , bant genişliğini; SF , yayılım faktörünü ve CR , kodlama oranını (coding rate) ifade etmektedir.

$$DR = SF \times \frac{BW}{2^{SF}} \times \frac{4}{CR + 4} \quad (3.5)$$

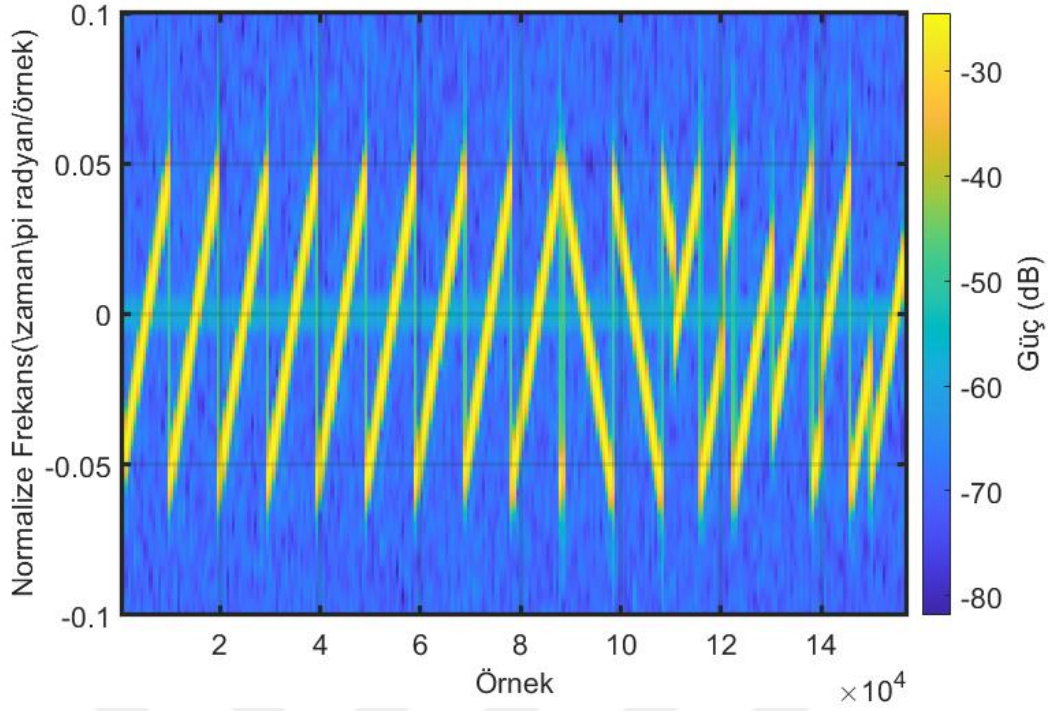
LoRa haberleşmesinde kullanılan çerçevesinin yapısı, Şekil 3.17 ile gösterildiği gibi, birden fazla temel bileşenden oluşmaktadır. Çerçeve, alıcının senkronizasyonunu sağlayan ve senkronizasyon dizisi olarak işlev gören Önsöz ile başlar. Önsöz'ün hemen ardından, sembol senkronizasyonunu desteklemek amacıyla kullanılan sabit bir desen olan Sync Word gelmektedir. Daha sonra, adres ve veri yükünün uzunluğu gibi önemli kontrol bilgilerini içeren Başlık (Header) bölümü yer alır. Bu bölüm, alıcının çerçeveyi doğru bir şekilde yorumlaması için gerekli kritik bilgileri sağlar. Başlık bölümünden sonra, iletilmesi hedeflenen kullanıcı verisini ya da gerçek veri yükünü taşıyan Veri (Data) bölümü bulunur. Çerçevenin sonunda, veri bütünlüğünü ve güvenilirliğini sağlamak amacıyla bir Döngüsel Yedeklilik Denetimi (Cyclic Redundancy Check, CRC) alanı eklenmiştir. CRC, hata tespitini mümkün kılarak alıcının alınan verinin doğruluğunu teyit edilmesini sağlar.



Şekil 3.17 LoRa paket çerçevesinin yapısı

LoRa haberleşmesinde sinyal karakteristiğini analiz etmek ve çözümlemek için SDR ile alınan LoRa paketinin spektrogram görüntüsü Şekil 3.18 ile verilmiştir. Şekil 3.18 ile sunulan spektrogram, SDR üzerinden alınan bir LoRa paketinin özelliklerini göstermekte ve sinyalin kod çözme ve analizine olanak tanımaktadır. Spektrogramda, 16 sembolük LoRa paketinin ilk 8 sembolünü oluşturan Önsöz'ün ardından, senkronizasyonu ifade eden sonraki 2 sembol ve frekans senkronizasyonunu işaret eden 2.25 sembol yer almaktadır. Bu sembolleri takip eden kalan semboller ise iletilen veriyi temsil etmektedir.

Paket içindeki her bir sembol, spektrogramdan görülebileceği üzere zaman eksenı boyunca bir frekans geçişi ile karakterize edilmektedir. Bu frekans değişimleri, demodülasyon ve kod çözme süreçlerinde kullanılarak sinyalden iletilen bilginin çıkarılmasını sağlar. Spektrogram, LoRa sinyalinin frekans davranışlarına ilişkin değerli bilgiler sunarak alınan paketin yorumlanması ve işlenmesine yardımcı olmaktadır.



Şekil 3.18 LoRa paketinin spektrogram gösterimi

3.2.2 Veri Setinin Oluşturulması

LoRa sinyalinin otomatik olarak etiketlenerek toplanabilmesi için sinyal içeriğinin çözümlenmesi ve LoRa cihazına ait kimlik numarasının bulunması gerekmektedir. Ayrıca oluşturulan güvenlik sisteminin sürekli zamanda çalışabilmesi için yapılan çözümlemenin hızlı olması gerekmektedir. Bu nedenle de çözümleme işlemleri paralel olarak hesaplama yapabilen GPU'nun CUDA çekirdekleri kullanılarak yapılmıştır. Paralel olarak yapılması mümkün olmayan işlemler ise CPU frekansının daha yüksek olması sebebiyle CPU üzerinde yapılmıştır.

3.2.2.1 Paket Tespiti

Haberleşme sistemlerinde gönderilen paketlerin alınabilmesi için belirli sayıda tekrar eden bir paket yapısı Şekil 3.8 ile görüldüğü gibi Önsöz olarak gönderilmektedir. LoRa cihazlarında bu paket yapısı birbirini tekrar eden yukarı yönlü cıvıltılardan (upchirp) oluşmaktadır. Önsöz'de bulunan yukarı yönlü cıvıltı sembolü sayısı gönderici tarafından ayarlanabilmektedir. Gönderilen paketi tespit edebilmek için SDR ortamı 868MHz merkez frekansında ve 2.4 MSPS örnekleme hızında dinlemektedir. Gönderici tarafından gönderilen veri 125ksps bant genişliğinde gönderilmekte ve paket içeriğindeki indekslemeler buna göredir. Bu

nedenle paket alındıktan sonra ise 2.4MHz frekansından 125kHz frekansına yeniden örneklendirilmiştir. Her 1 saniyelik veri içinde LoRa paketlerini aramaktadır.

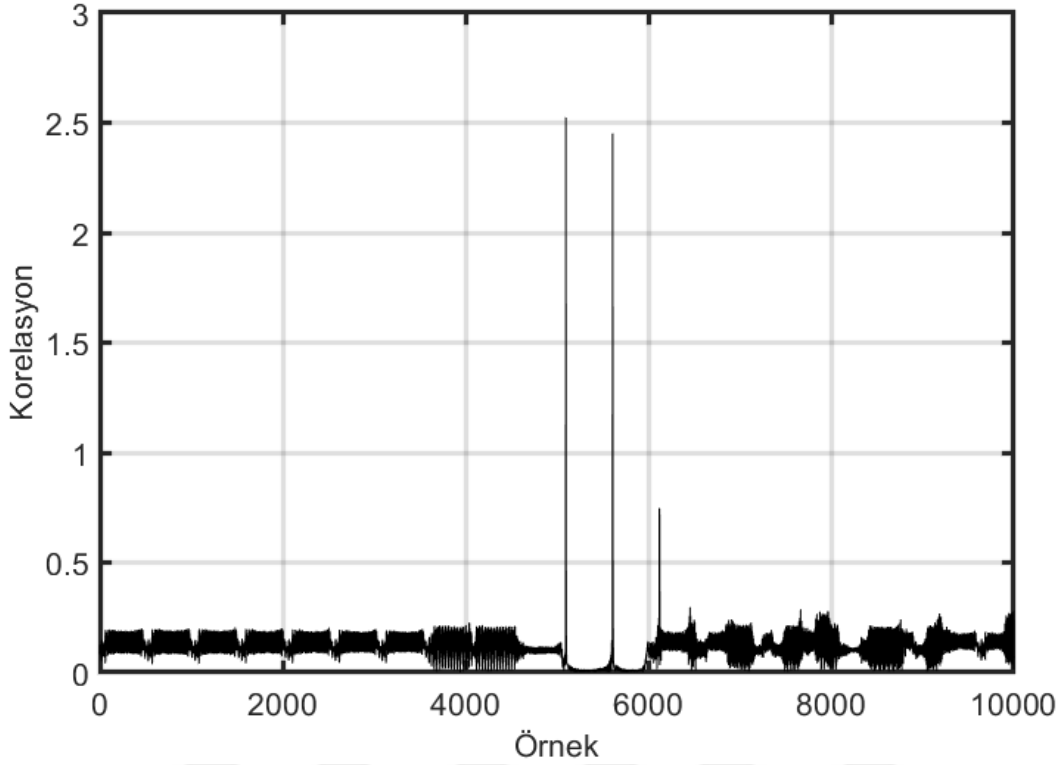
125.000 örnek veri noktası, bir saniyeyi temsil etmekte olup doğrudan CUDA çekirdeklerine giriş olarak verilir. CUDA çekirdeklerinde LoRa paketinin bulunabilmesi için yayılma faktörü ve Önsöz içerisindeki sembol sayısının bilinmesi gerekmektedir. Bu çalışma kapsamında, orta menzilli iletişim ve iletim hız seviyesi dikkate alınarak yayılma faktörü 9, Önsöz içindeki sembol sayısı ise 8 olarak seçilmiştir. Böylece, Önsöz'ün 512 (2^9) uzunluğundaki tekrarlayan 8 sembolü aranarak bir paket tespit edilmektedir. CUDA çekirdeklerinin ızgara, blok ve iş parçacığı yapısından yararlanılarak, her bir indeksin verisi, takip eden semboldeki verinin eşleniği ile çarpılmaktadır. Elde edilen değer 0.9'u aşıyorsa, konumsal veri küresel bir diziye eklenir. CUDA çekirdeğinde (3.6) numaralı formülde gerçekleştirilen hesaplama, f küresel dizisini ifade etmektedir; burada i, bir iş parçacığının indeksini, x_i , i indeksindeki veriyi ve x_{i+512} , takip eden semboldeki veriyi temsil etmektedir.

$$f(i) = \frac{|x_i * \bar{x}_{i+512}|}{x_i * \bar{x}_i} \quad (3.6)$$

3.2.2.2 Senkronizasyon

Veri paketlerinin oluşturulmasından sonra paket içeriğinin demodülasyon ve çözümleme işlemleri yapılabilmesi için paketin tam başlama noktası bulunmalıdır. Bunun için ise Şekil 3.17 ve Şekil 3.18 ile verilen Senkronizasyon çerçevesi kullanılmalıdır. Şekil 3.17 ile görülebileceği gibi Senkronizasyon çerçevesi 2.25 adet aşağı yönlü cıvıltıdan (downchirp) oluşmaktadır. Bu nedenle bu çerçevenin yakalanması için lokal olarak aşağı yönlü cıvıltı üretilmiştir. Üretilen aşağı yönlü cıvıltı sinyal yapısı ise parçalanmış paket içinde korelasyon ile aranmaktadır. Bu arama işlemi ise CUDA çekirdeklerinde her indeks içinde ayrı ayrı paralel olarak yapılmıştır. Arama sonrası her indeks için oluşan grafik Şekil 3.19 ile verilmiştir. Görüldüğü üzere 2 yüksek tepe noktası ve 1 düşük tepe noktası bulunmuştur. Buradaki 2 tepe noktası 2 aşağı yönlü cıvıltı sinyalini ve 1 tepe noktası ise 0.25'lik aşağı yönlü cıvıltı sinyalini temsil etmektedir. Bu noktaların kullanılması

ile paketin başlangıç noktası ilk tepe noktasından 2.25 sembol uzaklıkta olarak bulunmaktadır.



Şekil 3.19 LoRa paketinin başlangıç noktasının bulunması için Senkronizasyon paketi ile korelasyon sonucu

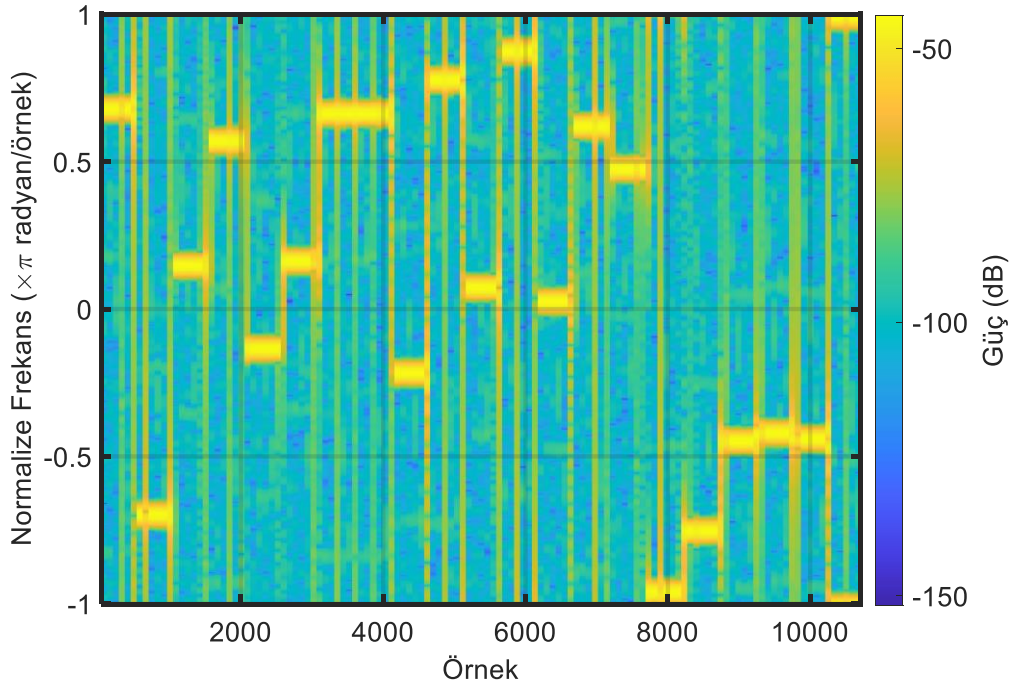
3.2.2.3 Demodülasyon

Senkronizasyon sonrasında paket başlangıç noktasından itibaren semboller demodüle edilmelidir. Demodülasyon işleminin yapılabilmesi için LoRa modülasyonunun da bilinmesi gerekmektedir. LoRa modülasyonu, maksimum sembol değeri (2^{SF}) ve bant genişliği bilgileri ile gönderilecek veriyi modüle etmektedir. Bunun için formül (3.7) ile verildiği gibi bant genişliği maksimum sembol değerini kullanarak belirli frekanslara parçalanmakta ve veri göndermek için verinin karşılığı olan frekans değeri kullanılmaktadır.

$$frekans = veri \times \frac{BW}{2^{SF}} \quad (3.7)$$

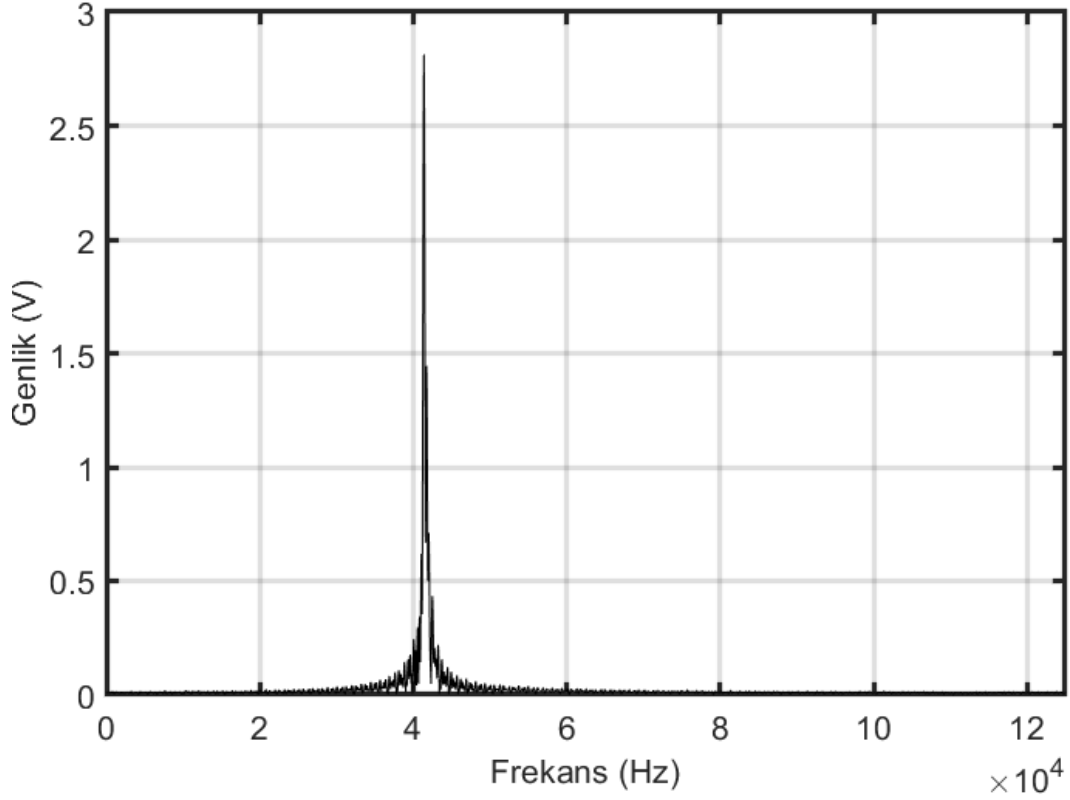
Gönderilecek frekans belirlendikten sonra bu frekansta 2^{SF} uzunluğunda sinyal oluşturulmaktadır. Elde edilen sinyal yukarı yönlü cıvıltı sinyali ile çarpılarak cıvıltı modülasyonu tamamlanmaktadır. Bu nedenle demodülasyon işlemi

yapılması için öncelikli olarak sinyal aşağı yönlü cıvıltı ile çarpılarak çözömlenmelidir (dechirp). Çözömleme işlemleri için CUDA çekirdeklerinin paralel yapısı kullanılmıştır. Oluşturulan yapı da toplam sembol sayısı kadar blok bulunmakta ve her blok içinde de sembol uzunluğu (2^{SF}) kadar iş parçacığı bulunmaktadır. İş parçacıkları aldığı her veriyi karşılığı gelen aşağı yönlü cıvıltı indeksi ile çarpmakta ve sonucunu global bir dizi içine yazmaktadır. Çözömleme sonucunda elde edilen sinyalin spektrogram görüntüsü 20 sembol için Şekil 3.20 ile verilmiştir.



Şekil 3.20 LoRa paketindeki bir sembol içeriğinin spektrogram gösterimi

Elde edilen spektrogram görüntüsünden de anlaşıldığı gibi her sembol için belirli frekanslarda baskın bir sinyal görünmektedir. Bu nedenle öncelikle her sembolün FFT'si alınarak frekans eksenine de bakılmalıdır. Örnek olarak bir sembolün frekans eksenini grafiği Şekil 3.21 ile verilmiştir.



Şekil 3.21 LoRa sembol içeriğindeki bir verinin frekans cevabı

Görüldüğü üzere alınan sinyal belirli bir frekansta değerinde gelmektedir. Bu frekans değerinden denklem (3.8) kullanılarak modüle edilmiş veri çıkarılabilmektedir. Bulunan her sembol için bu işlemler yapılarak demodülasyon işlemi tamamlanmaktadır.

$$veri = frekans \times \frac{2^{SF}}{BW} \quad (3.8)$$

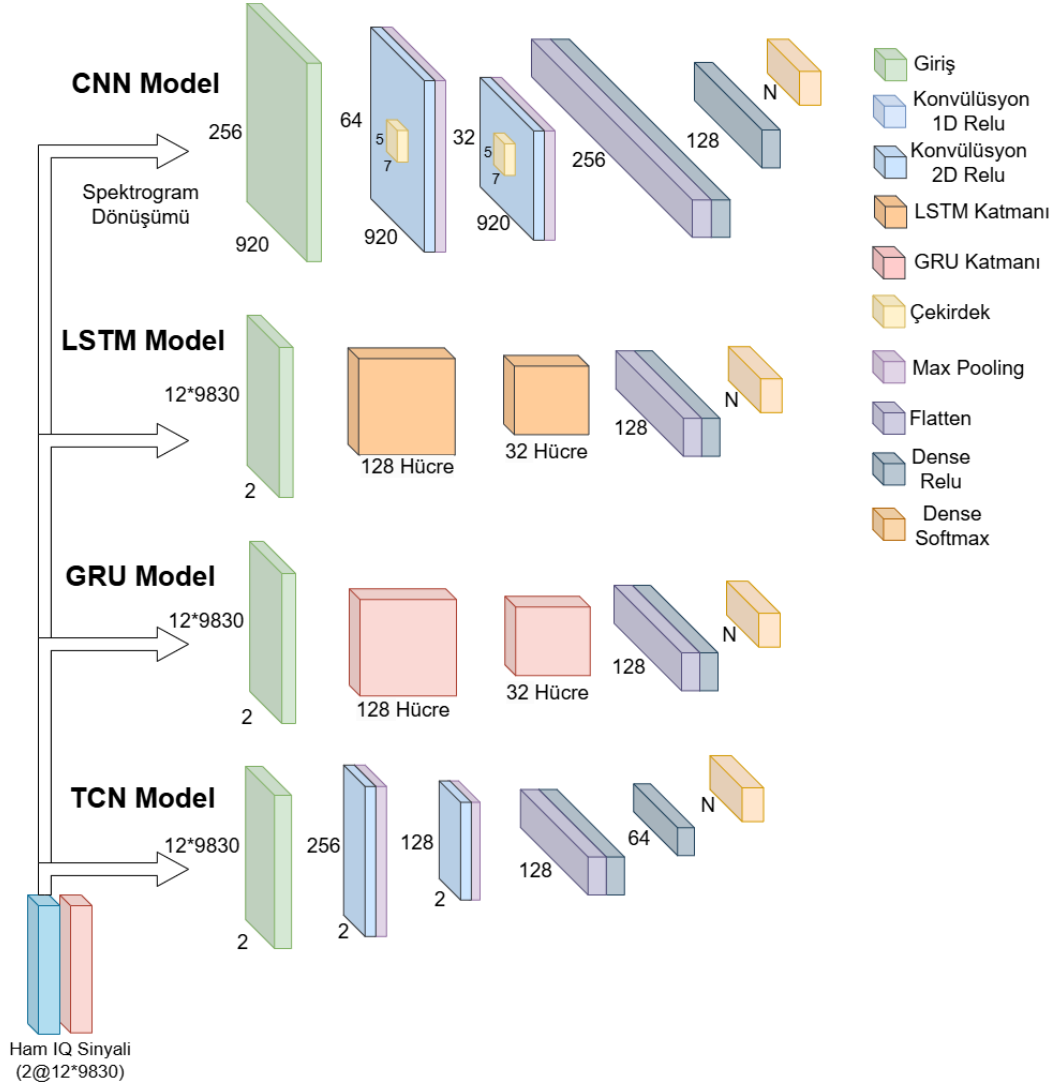
3.2.2.4 Çözümleme

Demodülasyon sonucunda elde edilen sembol içinden verinin çekilebilmesi için çözülmesi gerekmektedir. Çözümleme için öncelikle kodlama tekniğinin bilinmesi gereklidir. LoRa’da paket içinden veriyi çıkarmak için sırasıyla gri kod çözümleme, deinterleaving ve hamming kod çözümleme işlemlerinin sırasıyla yapılması gerekmektedir. Alınan verinin gri kod çözümleme işlemi verinin kaydırılıp ham veri ile özel veya (xor) işleminden geçirilmesi ile oluşturulmaktadır. İşlemden geçen veri interleaving matrinden çıkarılması için deinterleave işleminden geçmektedir. Elde edilen sembolden verinin çıkarılması

için ise hamming kod çözümü yapılmalıdır. Hamming çözümü için Kod Oranı (Code Rate, CR) bilgisinin bilinmesi gerekmektedir. Bu bilgi ise Başlık paketinin içinde bulunmaktadır. Başlık paketinin Kod Oranı ise 4/8 olarak sabittir. Hamming çözümü sonrasında elde edilen veri etiketleme için kullanılarak veri setinin toplanmasını sağlamaktadır.

3.2.3 Derin Öğrenme

Etiketlenerek bir depolama alanına aktarılan veri seti makine öğrenmesi modelinin oluşturulması için kullanılacaktır. Makine öğrenmesi modelinin oluşturulabilmesi için veri setleri dışında makine öğrenmesi ağına ihtiyaç vardır. Makine öğrenmesi ağının yapısı giriş katmanı, gizli katman ve çıkış katmanından oluşmaktadır. Çalışma da giriş katmanı olarak ham sinyal üzerinden elde edilen Önsöz ve Senkronizasyon paketlerinin I/Q verileri kullanılmıştır. Önsöz ve Senkronizasyon paketleri 125ksps örnekleme hızı için 512 veriden oluşan 12 sembolü içermektedir. Ham sinyalin 2.4MHz örnekleme hızına sahip olmasından dolayı bir sembolün uzunluğu $(512 \cdot 2.4 \cdot 10^6) / (125 \cdot 10^3)$ olmaktadır. Hesaplama yapıldıktan sonra giriş katmanının I ve Q için $2 \times (12 \times 9830)$ boyutuna sahip olduğu bulunmuştur. Giriş katmanından sonra ara katmanda 6 tane Relu katmanı, 7×5 'lik filtre ve Max Pooling ile kullanılmıştır. ReLu katmanından sonra Flatten kullanılarak vektörel hale getirilmiştir. Vektörel hale getirilen ağ 3 adet Dense Relu'dan geçirilmiş ve ara katman ile sonlandırılmıştır. Derin öğrenme modelinin çıkış katmanında ise kullanılan cihazların kategorilendirilmesi ikili olarak verilmiştir. Cihazların ID bilgisine göre her cihaz bir bite karşılık gelmektedir. Çalışmada 4 cihaz kullanıldığı için 4 bitlik bir Softmax katmanı oluşturulmuştur. Derin öğrenme için kullanılan ağ yapısı Şekil 3.22 ile verilmiştir.



Şekil 3.22 LoRa cihazlarının kimliklendirilmesinde kullanılan derin öğrenme modellerinin gösterimi

3.2.4 DeneySEL Sonuçlar

Gerçek zamanlı olarak elektronik cihazların kimliklendirme sistemini test etmek amacıyla Şekil 3.23 ile verilen kurulum oluşturulmuştur. Bu kurulumda, RFM95 modülü LoRa paketlerini gönderirken, bu paketler Jetson Orin Nano cihazına sinyalleri yakalayan RTL-SDR cihazı tarafından alınmaktadır. RTL-SDR cihazı 8-bit çözünürlük, 2.4 MSPS örnekleme hızı ve 868 MHz merkez frekansına sahiptir. Bu nedenle, alınan veriler 2.4 MSPS'den 125 kSPS'ye yeniden örneklenmiştir. Ayrıca, SDR cihazındaki bileşenlerin sıcaklığı arttıkça elde edilen sinyal özelliklerinde değişiklikler meydana gelebilmektedir. Bu nedenle hem sinyal alınırken hem de sistem güvenliğini sağlarken SDR cihazının kararlı bir

duruma geçmesi ve hafifçe ısınması beklenmektedir. Benzer şekilde, sinyallerin alındığı ortamdaki sinyal-gürültü oranı (Signal Noise Ratio, SNR) ve nem seviyelerinin yüksek değişkenlik göstermemesi gerekmektedir. Aksi halde, ortam koşullarındaki yüksek değişkenlik alınan elektromanyetik sinyallerin genlik, frekans ve faz özelliklerini etkileyerek cihaz kimliklendirmede sorunlara yol açabilir. Açıklanan yeniden örnekleme ve analiz süreçlerinden sonra, ham sinyaller etiketlenerek veri kümesi oluşturulmuştur. Etiketleme işlemi, cihazlardan alınan benzersiz kimlik numaralarının çözülmesi ile gerçekleştirilmiştir. Alınan sinyaller bu kimlik numaralarından oluşturulan dosya adlarıyla kaydedilerek veri kümesi oluşturulmuştur. Toplamda 250 GB yer kaplayan bu veri kümesi, 11 gün boyunca alınan 350.000 örnekten oluşmaktadır.



Şekil 3.23 Önerilen tasarımı test etmek için oluşturulmuş kurulum

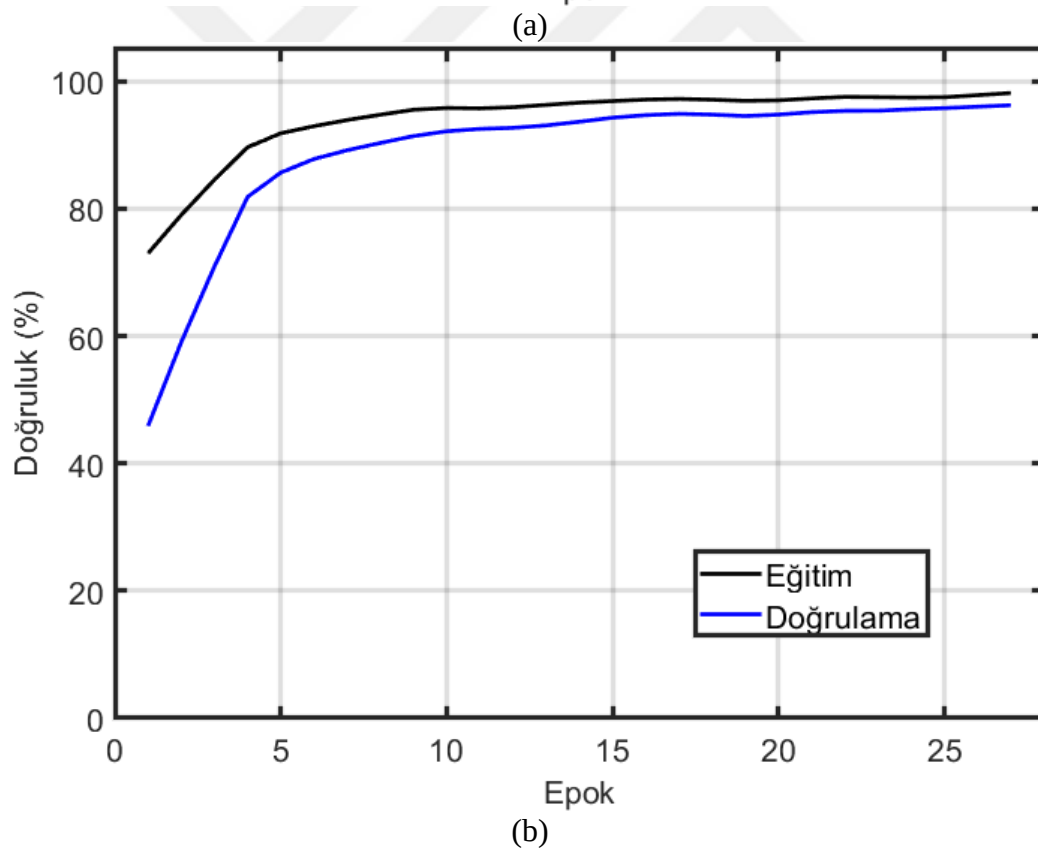
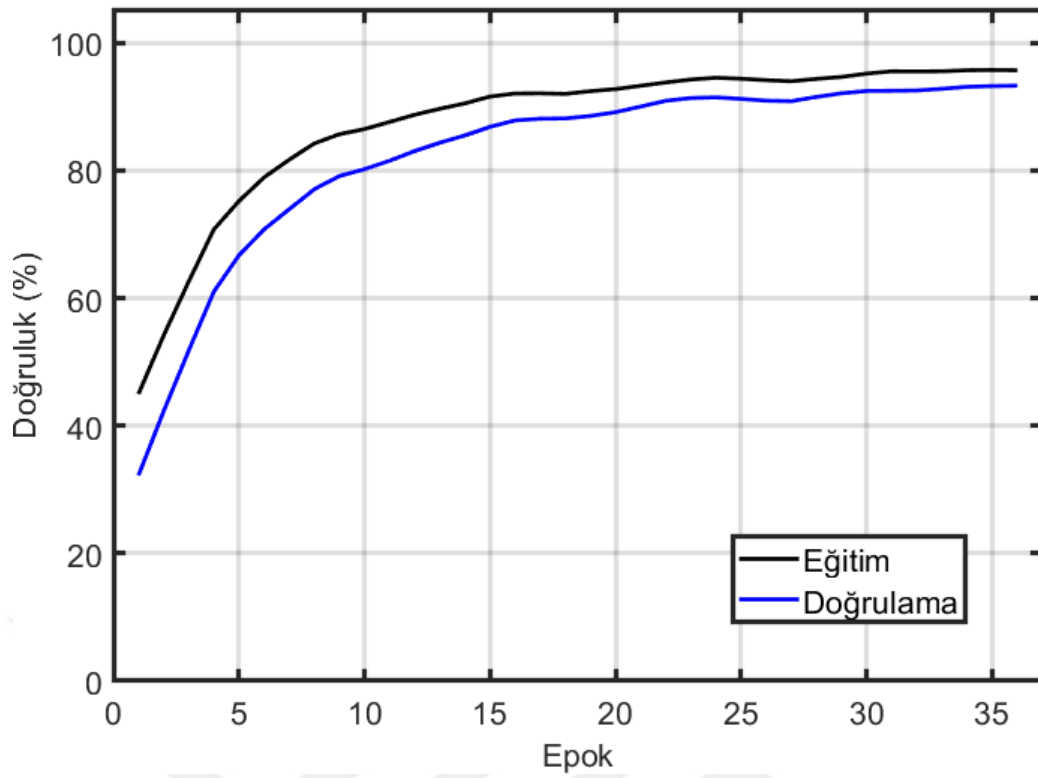
Veri toplama ve gerçek zamanlı test sırasında, önerilen sistemin geleneksel sistemlerden farkı, CUDA çekirdekleri kullanılarak yapılan hesaplamalar ile CPU üzerinde gerçekleştirilen geleneksel yöntemlerdeki gecikmeler karşılaştırılarak gözlemlenmiştir. Önerilen sistemde paket tespiti, senkronizasyon, kod çözme ve eğitim için dört kuyruk yapısı kullanılmıştır. Analiz kapsamında kod çözme için

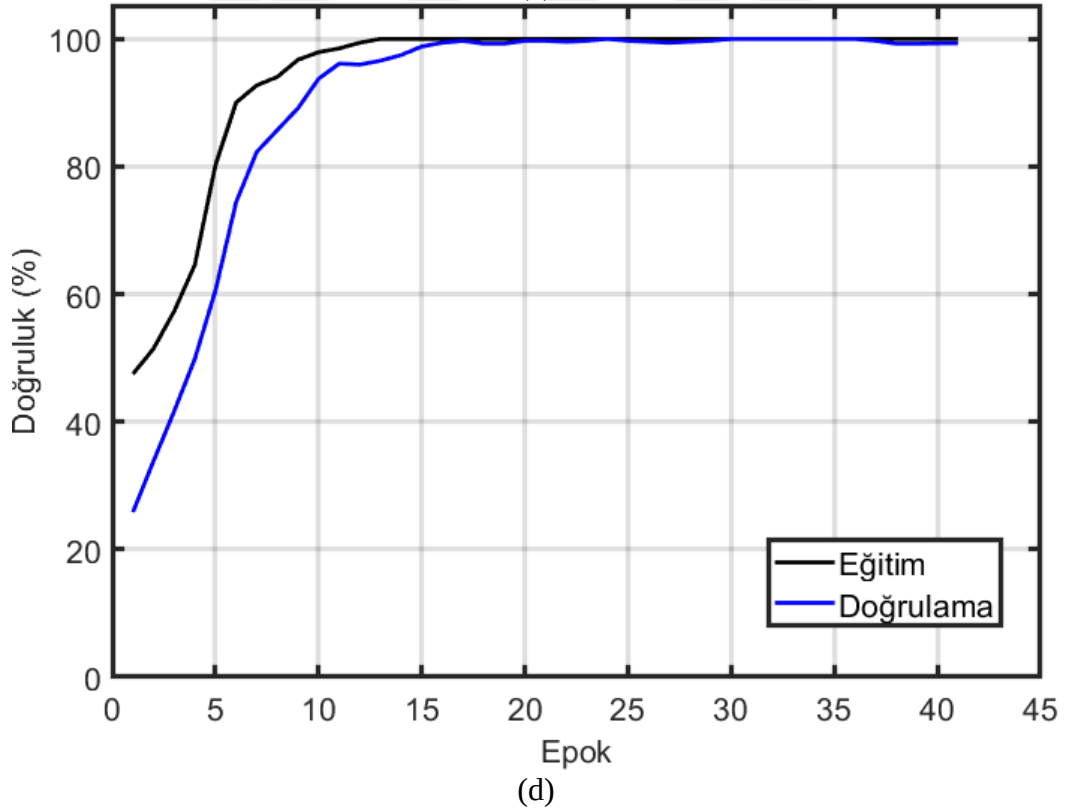
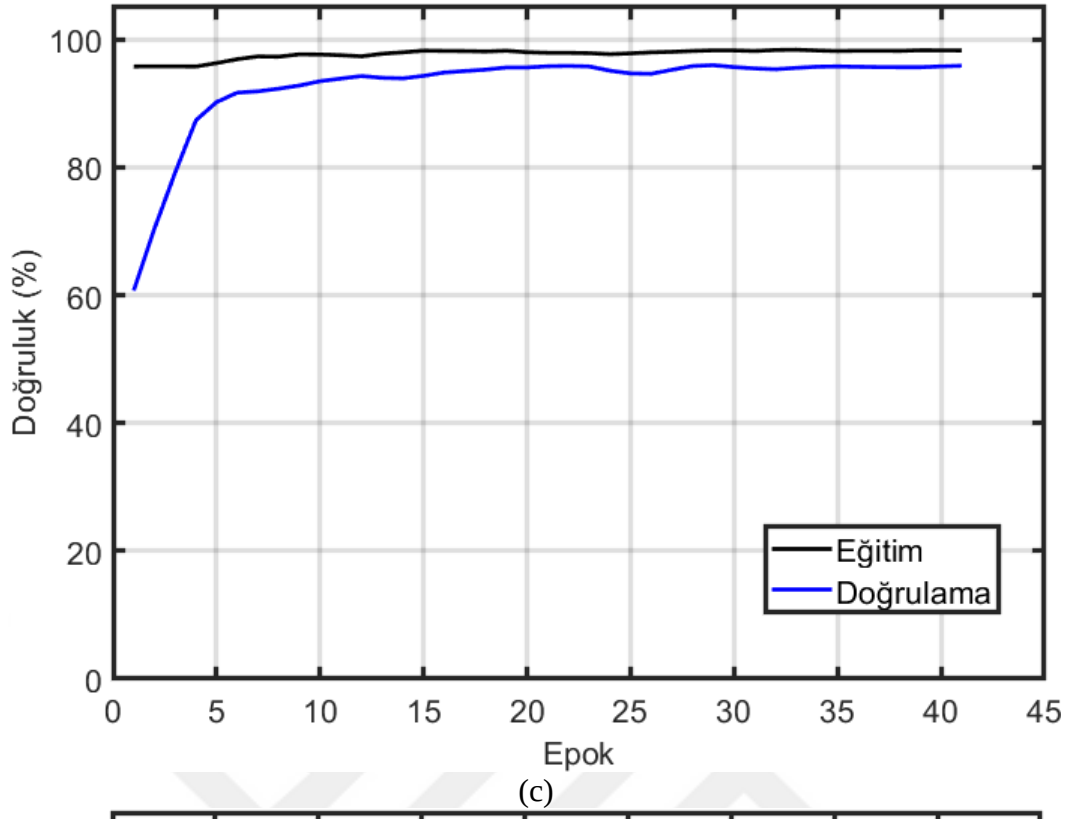
FFT, eğitim için spektrogram dönüşümü yapılmıştır. Tablo 3.2 ile sunulan analiz sonuçları, paralel hesaplamalar için CUDA çekirdeklerinin kullanılmasının sistemi önemli ölçüde hızlandırdığını ve sistemin sağlam bir şekilde gerçek zamanlı çalışmasına katkıda bulunduğunu göstermektedir. Özellikle Başlangıç paketinin algılama sürecindeki paralel hale getirilebilen hesaplamalar sayesinde, geleneksel CPU tabanlı yöntem 65 ms sürerken, CUDA çekirdekleri ile bu süre yalnızca 4 ms'ye düşmekte ve sistem %1625 daha hızlı çalışmaktadır. Diğer hesaplamalarda ise birbirine bağlı işlemler olması nedeniyle daha az paralel yapılabilir yapı bulunmaktadır ve bu nedenle Başlangıç paketinin algılama sürecine göre daha sınırlı bir hızlanma sağlanmıştır.

Tablo 3.2 CPU ve GPU üzerinde yapılan işlemlerin hız karşılaştırmaları

Metod İsmi	CPU Tabanlı İşleme Hızı	GPU Tabanlı İşleme Hızı
Önsöz Tespiti	65 ms	4 ms
Senkronizasyon Tespiti	2 ms	0.8 ms
FFT Dönüşümü	2 ms	1.2 ms
Spektrogram Dönüşümü	25 ms	6 ms

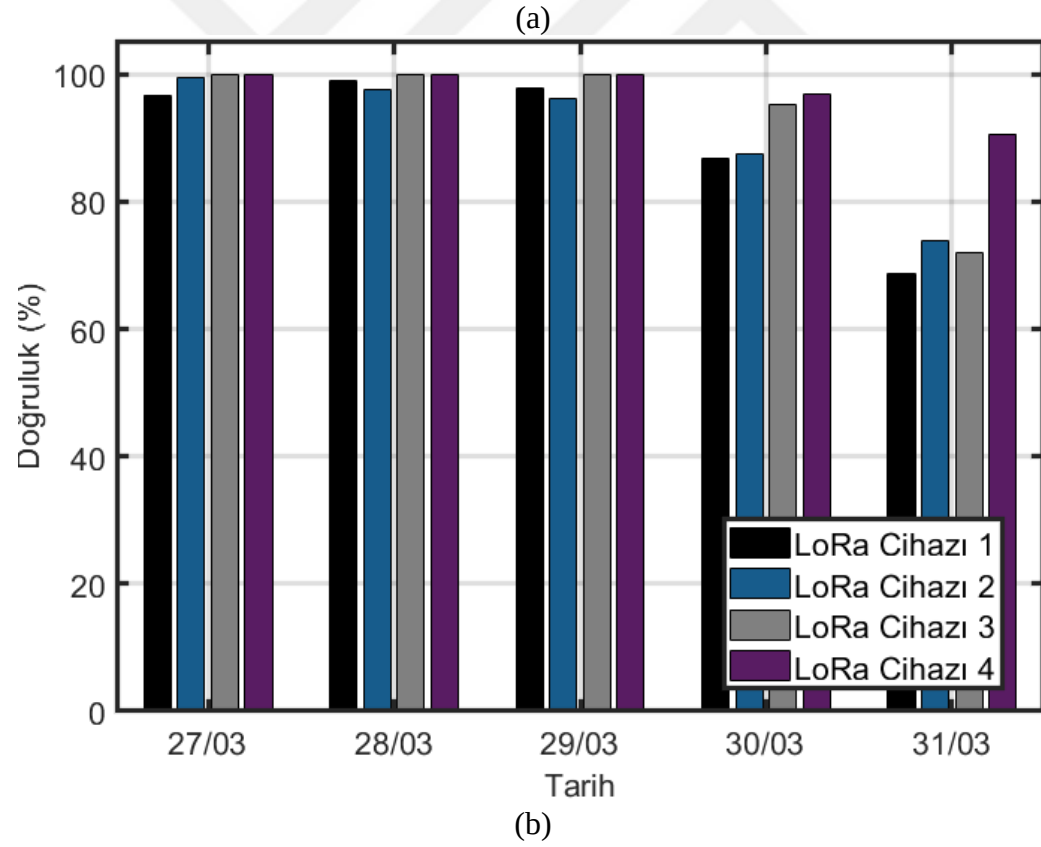
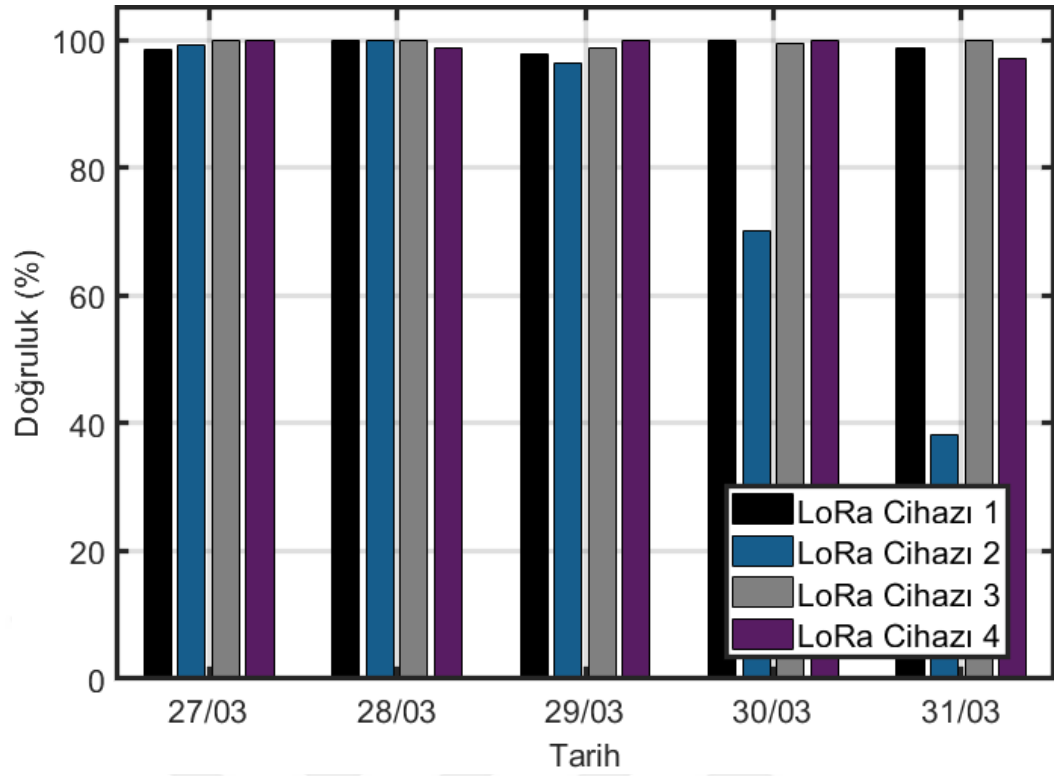
Sistemin gerçek zamanlı veri işleme yeteneğinin doğrulanmasının ardından, güvenliği sağlamak amacıyla oluşturulmuş olan derin öğrenme modelleri, elde edilen veri seti kullanılarak eğitilmiştir. Eğitim sürecinde toplamda 63 GB veri ve 72000 örnek kullanılmıştır. Kullanılan veri seti üç günlük bir sürede toplanan verilerden oluşmakta olup, derin öğrenme deneylerinde veri ayırma işlemlerinde standart uygulamalara uyularak eğitim (%70), test (%15) ve doğrulama (%15) alt kümelerine bölünmüştür. Derin öğrenme modellerinin eğitimi sonucunda elde edilen doğruluk eğrileri Şekil 3.24 ile verilmiştir.

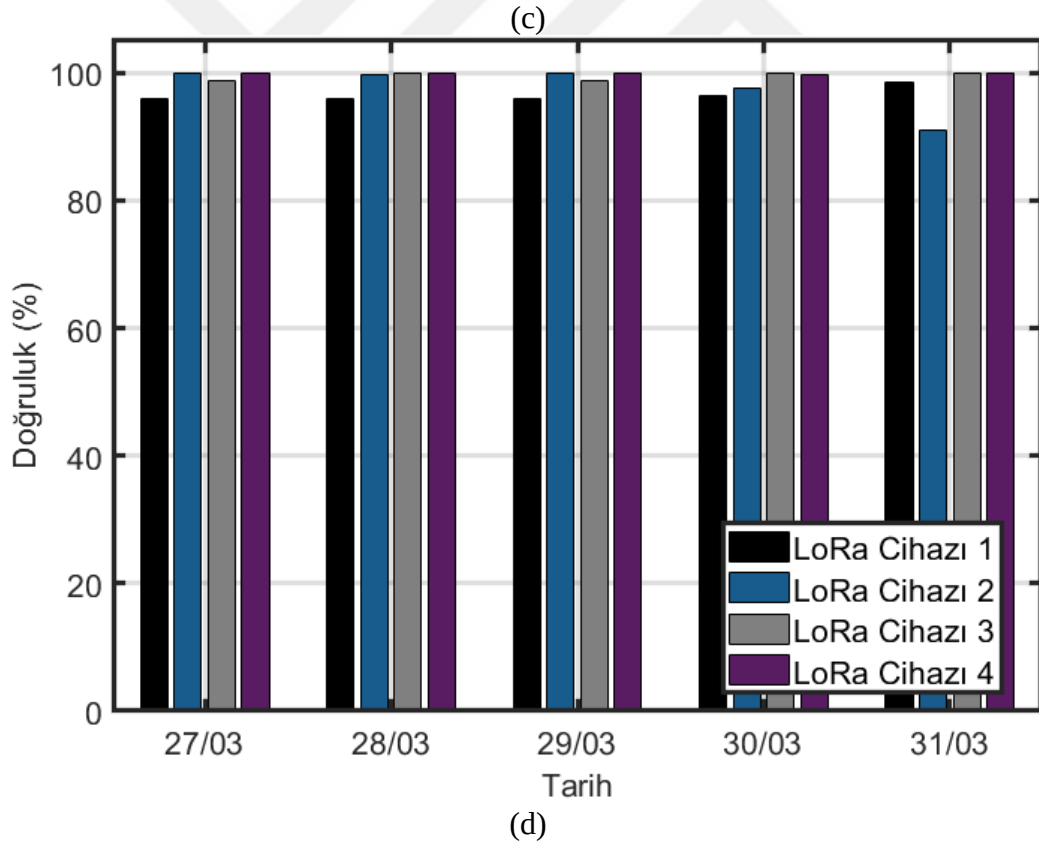
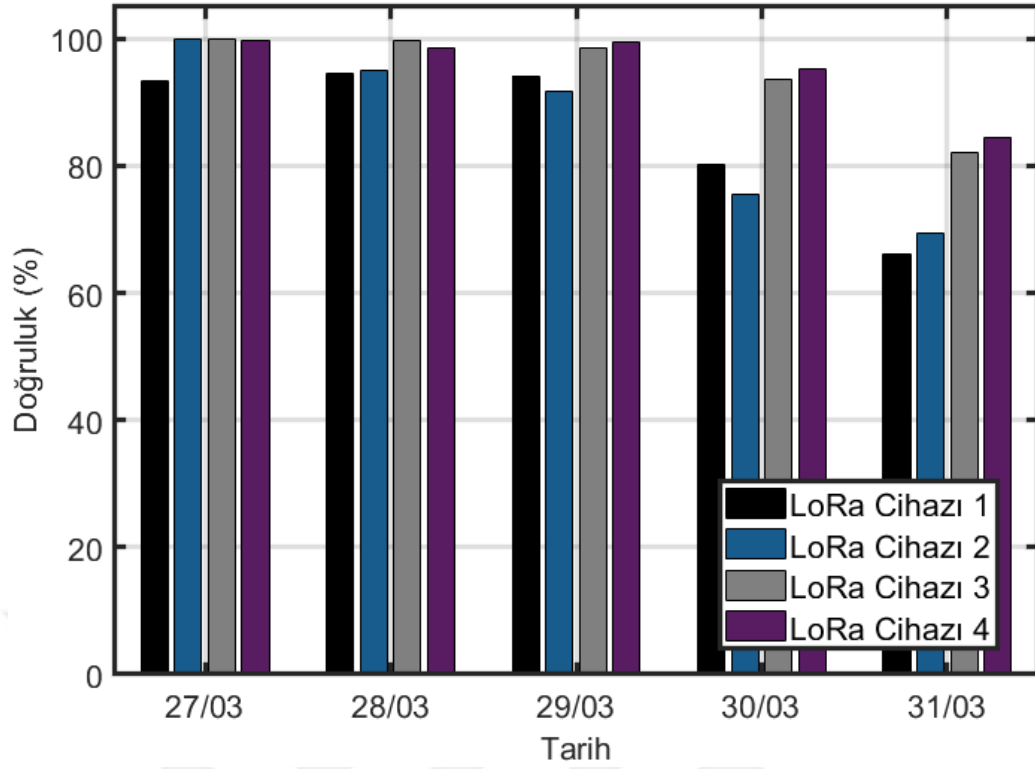




Şekil 3.24 (a) TCN (b) LSTM (c) GRU (d) CNN derin öğrenme modellerinin dönem sayılarına göre doğruluk oranları

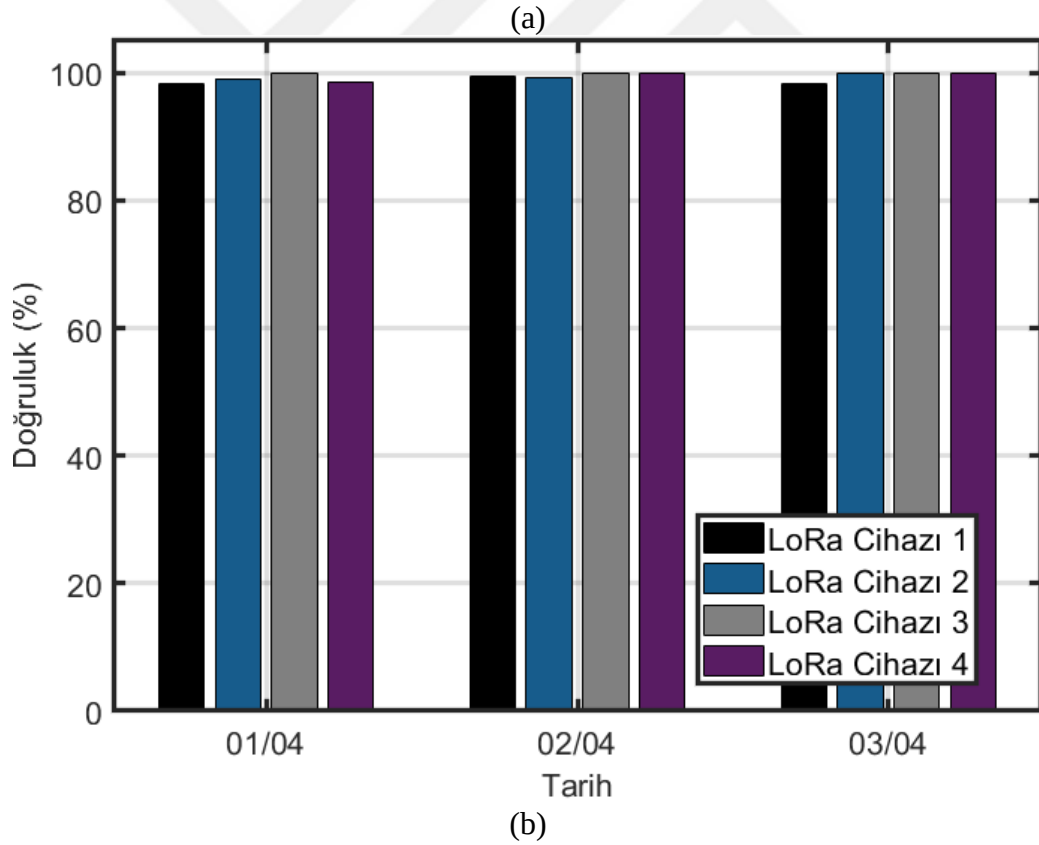
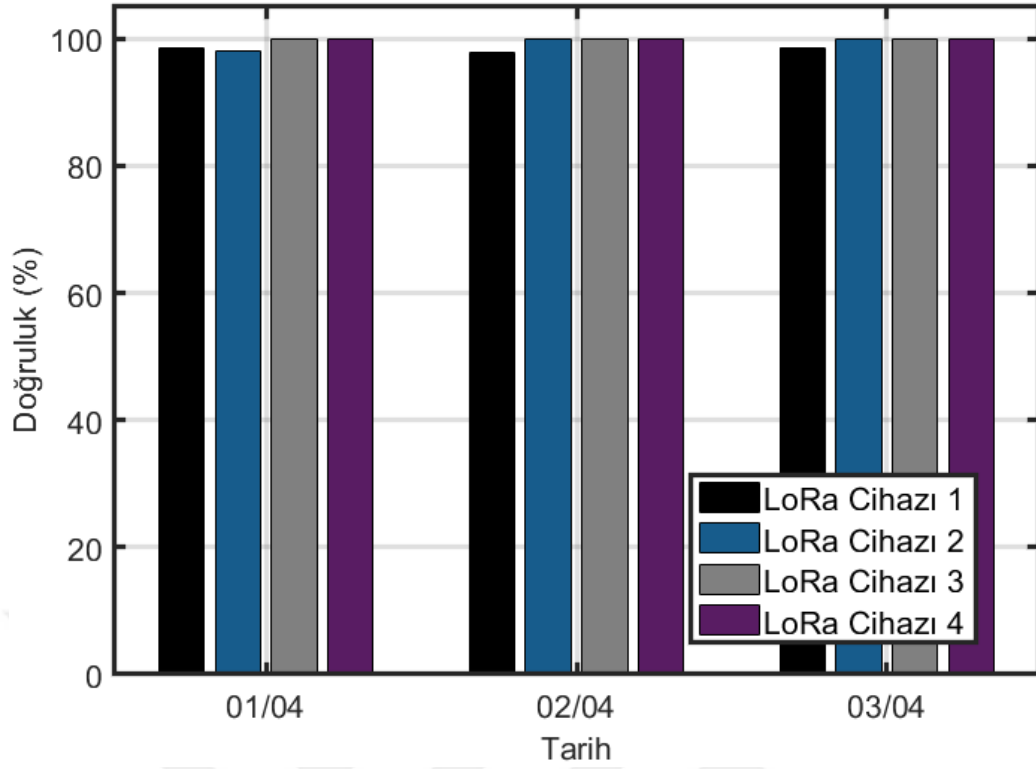
Derin öğrenme sonucunda elde edilen modellerin testi, Şekil 3.25 ile verildiği gibi 5 gün boyunca gerçekleştirilmiştir. Günlük olarak toplamda 24000 veri alınmış ve verilen grafik, LoRa cihazlarının günlük ortalama sınıflandırma doğruluğunu göstermektedir. Derin öğrenme modelleri arasında, spektrogram verileri ile eğitilmiş CNN modelinin en iyi sonuçları verdiği, ham sinyaller ile yapılan eğitimde ise TCN yönteminin en başarılı sonuçları sağladığı belirlenmiştir. Sonuçlar, LoRa cihazlarının sınıflandırma doğruluğunun zamanla azalan bir eğilim gösterdiğini ortaya koymaktadır. Elektronik cihaz bağlantılarının kararsızlığı ve elektronik bileşenlerin yaşlanması nedeniyle zaman içinde cihazların elektronik özelliklerinde değişimler gözlemlenmiştir. Bu nedenle, derin öğrenme modellerinin performansını artırmak için yeni verilerle yeniden eğitilmesi zorunlu hale gelmiştir. Sınıflandırma doğruluğu düşen cihazların güvenliğini sağlamak amacıyla, daha önce eğitilmiş modelin, cihazların tanımlama yöntemi ile güvenliğinin sağlandığı dönemde alınan yeni veriler ile yeniden eğitilmesi gereklidir. Sistemin operasyonel sürecinde, derin öğrenme modeli düzenli aralıklarla yüksek performans dönemlerinde toplanan veriler ile arka planda otomatik olarak yeniden eğitildiğinden, ek bir işleme gerek kalmamaktadır. Derin öğrenme modeli, yalnızca yeni verilerle eğitim yapılmasını sağlamakla kalmayıp, oluşturulan yapılandırılmış çıktı katmanı sayesinde farklı cihazların da baştan eğitimi gerektirmeden modele eklenmesine olanak tanımaktadır. Bu sayede önceden eğitilmiş modele yapılan güncellemeler sayesinde yeni verilerle daha hızlı eğitim yapılabilmekte ve yeni cihazların modele eklenmesi ilk eğitime kıyasla daha kısa sürede gerçekleşmektedir. Ayrıca, cihazın güvenli iletişimi sırasında alınan yeni veriler, potansiyel saldırı cihazlarının sürece müdahale etmesini engellemektedir.





Şekil 3.25 LoRa paketlerini kimliklendirmede (a) TCN (b) LSTM (c) GRU (d) CNN derin öğrenme modellerinin gün bazında ortalama doğruluk oranı

Diğer modellere göre daha başarılı olarak bulunmuş olan TCN ve CNN modelleri, yeni verilerle transfer öğrenimi gerçekleştirilmiştir. Yeni modeller ile yapılan test sonucunda, Şekil 3.26 ile gösterilen sonuç elde edilmiştir. Görüldüğü üzere, LoRa cihazlarının günlük sınıflandırma doğruluk oranları tekrar kabul edilebilir seviyelere ulaşmıştır. Elektronik cihazların stabilitesi, üretim sırasında düzgün kablolama, stabil bağlantı noktaları ve kablolarda temas sorunlarının azalması, zamanla elektronik özelliklerdeki değişimlerin en aza indirilmesine katkı sağlamaktadır. Bu durum, eğitilen modelin sık sık yeniden eğitilmesine gerek kalmadan uzun süreler boyunca çalışmasını mümkün kılmaktadır. Ancak, elektronik özelliklerin yalnızca stabilite ile sınırlı olmadığını, bileşen yaşlanmasının da etkili olduğunu belirtmek önemlidir. Dolayısıyla, zamanla özelliklerde değişimlerin olması ve yeniden eğitime ihtiyaç duyulması beklenmektedir. Cihazların güvenliğinin sağlandığı durumda, performans oranlarının düştüğü dönemlerde yeni alınan sinyaller ile yeniden eğitim yapılarak sistemin etkinliği korunabilir. Derin öğrenme ile sağlanan performansın, daha sonraki zaman noktalarında toplanan verilerle kıyaslanması, yalnızca o günlerde elde edilen verilerle kıyaslanmasından daha önemlidir. Ayrıca, yeniden eğitim sürecinin gömülü GPU'ya sahip dağıtık bir sistem olan Jetson Orin Nano üzerinde doğrudan yapılabilmesi ve bu sürecin önemli bir zaman kaybına neden olmaması, sistemlerin sunucuya erişiminin mümkün olmadığı yerlerde kullanımına olanak tanımaktadır.



Şekil 3.26 (a) TCN (b) CNN derin öğrenme modellerinin LoRa paketlerini kimliklendirmede günlere göre ortalama doğruluk oranı

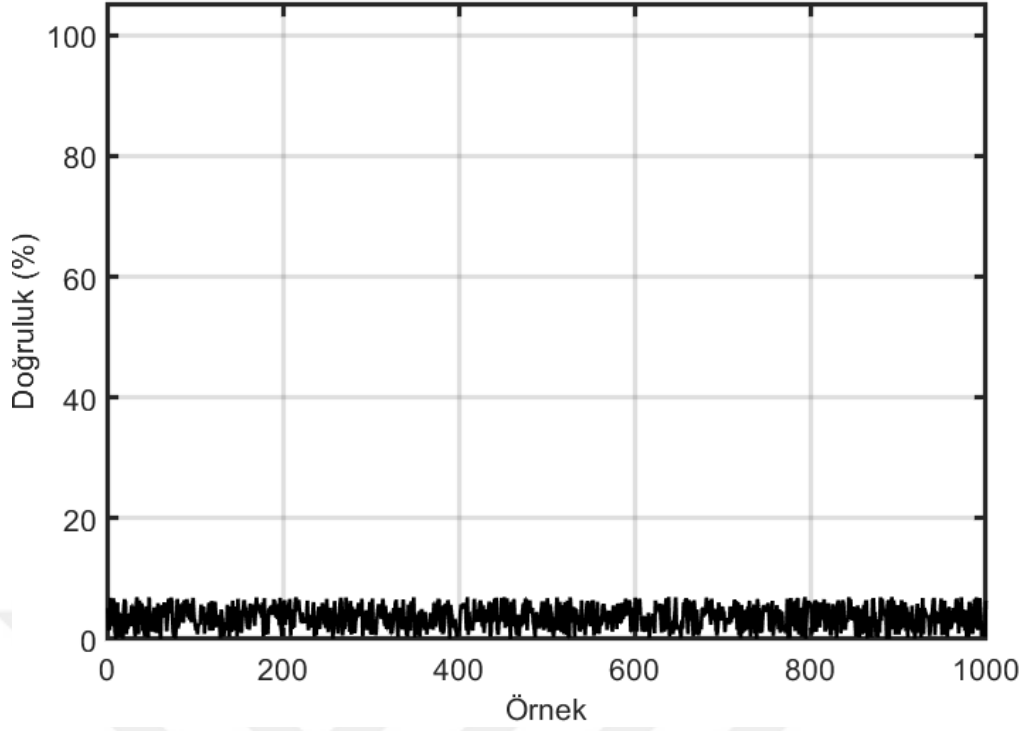
Test aşamasında, derin öğrenme modellerinin eğitiminin ardından CNN modelinin cihazlar için ortalama %99,8 sınıflandırma doğruluğu elde ettiği bulunmuştur. Derin öğrenme modellerinin karmaşık yapıları, sınıflandırma yapabilmek için özellikleri bu verilerden çıkararak çözümleme adına büyük miktarda veriye ihtiyaç duyar. Bu nedenle, spektrogram gibi özelliklerin tarafımızca çıkarılması, derin öğrenme modelinin öğrenme sürecini kolaylaştırmaktadır.

Düşük güçlü cihazlar, enerji tüketimini en aza indirmek için ilettikleri paket sayısını kasıtlı olarak sınırlandırmaktadır. Bu durum, etkili eğitim amacıyla yeterli veri sağlanmasında kısıtlılık yaratabilir. Düşük güçlü sistemlerde, önerilen kimlik doğrulama sisteminin stabil çalışmasını sağlamak adına minimum paket analizi yapılması kritik önem taşır. Derin öğrenme sistemleri, karmaşık yapılardan kendi başlarına özellik çıkararak istenilen öğrenmeyi gerçekleştirir. Ancak veri hacmi sınırlı olduğunda bu özelliklerin çıkarımı zorlaşmakta ve performans oranları düşmektedir. Bu nedenle, spektrogramları giriş katmanı olarak kullanan CNN modeli, ham sinyal girişlerini kullanan modellere kıyasla daha yüksek performans sergilemiştir. Bu bağlamda, Tablo 3.3 ile CNN modelinin veri miktarına bağlı olarak sınıflandırma doğruluğu oranları analiz edilmiştir. Analizde, eğitim için günlük minimum veri miktarı ve eğitim için gereken toplam gün sayısı incelenmiştir. Yedi gün boyunca alınan verilerle farklı derin öğrenme modelleri oluşturulmuş ve ortalama sınıflandırma doğruluğu oranları bulunmuştur. Analiz sonucunda, önerilen kimlik doğrulama sisteminin, saatte bir veri alındığı senaryoda bile stabil çalıştığı gözlemlenmiştir. Böylece, Jetson Orin Nano gibi Gömülü GPU'ya sahip cihazlar ile sunucuya çıkılmadan düşük güçlü LoRa modülleri bile kimliklendirilebilmektedir. Sistem ve ağ güvenliğinin kritik olduğu durumlarda, LoRa Geçitlerinin geleneksel kullanımı yerine, ham sinyaller aracılığıyla fiziksel katmanda güvenlik sağlayan bir sistem tasarlanmıştır.

Tablo 3.3 Günlük paket miktarına göre eğitilen modellerin başarımları

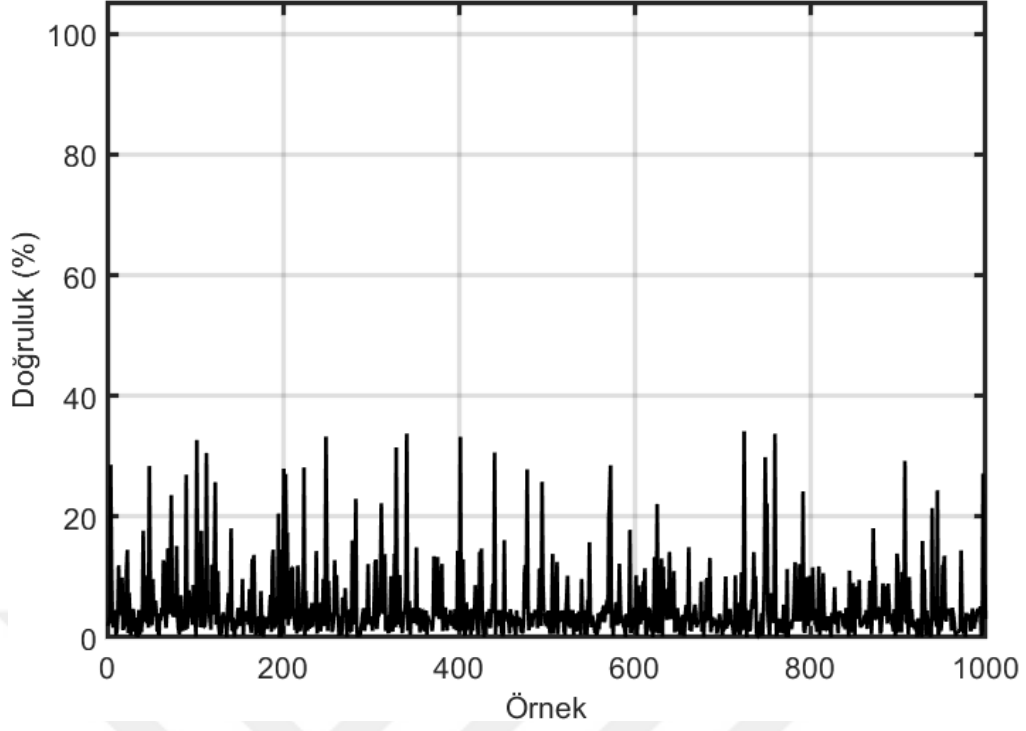
Günlük Paket Adeti	Eğitim İçin Kullanılan Veri				Gün Başına Başarımları Oranı (%)							Ortalama Başarımları (%)
	03/24	03/25	03/26	03/27	03/28	03/29	03/30	03/31	04/01	04/02	04/03	
24					97,89	97,86	97,61	97,95	97,10	97,27	94,11	97,1161
24					97,59	98,16	97,10	97,23	96,68	97,95	96,54	97,3266
24					96,82	96,60	96,53	94,47	95,83	97,16	96,30	96,2494
24					99,54	99,34	99,16	93,17	91,51	99,84	99,88	97,4906
50					98,43	98,74	98,36	97,52	97,34	98,71	96,75	97,9852
50					95,13	95,41	94,74	92,57	92,12	94,50	93,60	94,0140
50					97,24	97,43	94,89	93,70	93,14	96,54	96,95	95,7021
50					99,66	98,61	97,68	96,29	91,93	98,27	99,52	97,4281
250					99,57	99,83	99,76	98,36	99,62	98,86	96,11	98,8764
250					99,28	99,06	98,66	97,09	95,47	99,04	98,07	98,0999
250					95,14	95,43	95,27	94,80	94,30	95,13	93,55	94,8088
250					99,36	99,99	97,15	87,87	89,49	99,99	99,64	96,2174
1000					98,30	98,72	99,30	98,03	97,87	98,86	97,77	98,4121
1000					98,45	98,11	97,19	94,61	94,70	97,03	97,70	96,8331
1000					98,69	98,69	98,55	96,96	97,26	97,88	96,93	97,8556
1000					99,62	99,21	88,84	81,37	90,23	98,98	99,99	94,0398
2500					97,59	97,57	97,67	96,30	95,44	97,08	96,63	96,9042
2500					96,03	95,71	96,41	96,18	95,5	95,88	94,20	95,7359
2500					95,87	96,06	95,98	94,88	94,56	95,37	93,36	95,1609
2500					99,53	99,68	97,78	91,68	89,86	99,38	99,82	96,8231

Kimlik doğrulama sisteminin gerçek zamanlı izlenmesi, güvenlik kriterlerini karşılayan paketlerin, herhangi bir Gateway gereksiz LoRa Gateway veya özel yöntemlerle istenilen sunucuya yönlendirilmesini sağlamaktadır. Geleneksel iletişimde LoRa geçitleri (gateway), modüllerden alınan paketleri AES-128 ile şifre çözme işlemiyle işleyip, MAC katmanında modül kimlik bilgilerini çıkararak belirli sunucu adreslerine iletmektedir. Bu çalışmada, derin öğrenme modeli tarafından güvenlik kriterlerini karşılayan paketler, Bölüm 3.2.2’de sağlanan CUDA çekirdeği kullanılarak çözümlenmiş ve cihaz bilgileri AES-128 işleme adımlarıyla çıkarıldıktan sonra belirlenen sunucuya iletilmiştir. Güvenlik kriterlerini karşılamayan paketler için çözümleme adımlarının kasıtlı olarak atlanması, Gömülü Linux ortamında gereksiz işlem yükünü azaltmakla kalmayıp, bu paketlerin sunucuya iletilmesini engelleyerek ağ tıkanıklığını önlemektedir. Taklit ve kimlik sahtekarlığı saldırılarına karşı gerçek zamanlı güvenliği doğrulamak amacıyla, farklı LoRa modülleri ve SDR kullanılmıştır. Bir kimlik sahtekarlığı saldırısı için cihazın dijital kimliği, cihaz adresi, ağ oturumu ve uygulama oturumu bilgileri başka bir LoRa modülüne kopyalanarak sisteme sızma girişimi yapılabilmektedir. Alınan paketin dijital formata dönüştürülmesinden sonra yapılan güvenlik kontrolleri, LoRa modülünün sisteme sızmasını engellemekte yetersiz kalmaktadır. Bu nedenle, önerilen çerçevede açıklandığı üzere, gelen ham sinyale dayanarak cihazın sisteme kayıtlı olup olmadığının tespiti zorunludur. Bu bağlamda, Gömülü GPU’ya aktarılan CNN modeli, kimlik sahtekarlığı saldırılarına karşı gerçek zamanlı olarak test edilmiştir. Taklit saldırısı gerçekleştiren cihaz tarafından alınan sinyalin CNN modeline iletilmesi sonucu elde edilen doğruluk oranları Şekil 3.27 ile gösterilmektedir. Doğruluk değerinin incelenmesi, çıkış katmanında hedeflenen belirli cihaz kimliğine ait çıktının gözlemlenmesi yoluyla gerçekleştirilmiştir.



Şekil 3.27 Bir taklit saldırısı sırasında CNN modelinin gerçek zamanlı doğruluk oranları

Farklı bir taklit saldırısı olarak SDR ile ham sinyaller dinlenmekte ve kaydedilmektedir. Bu saldırı, kaydedilen bu sinyallerin istenilen herhangi bir zamanda yeniden yayınlanmasını içermektedir. Sinyallerin dijital formatta yakalanıp yeniden üretilmesi fark edilmeyebilir; ancak ham sinyal alanında bazı farklılıklar mevcuttur. Aynı sinyalin yeniden yayınlanmaya çalışılması durumunda, kullanılan elektronik bileşenlerden dolayı genlik, faz ve frekansta elektriksel karakteristiklerde değişiklikler meydana gelmektedir. Önerilen sistem, güvenliği sağlamak amacıyla bu elektriksel karakteristik farklılıklarını tespit etmektedir. Önerilen sistemin doğruluğunu test etmek amacıyla, bir LoRa modülünden bir gün boyunca sinyaller gönderilmiş ve farklı bir SDR ile kaydedilmiştir. Daha sonra bu kaydedilen sinyaller SDR tarafından yayınlanarak, önerilen sistemin güvenliği sağlama yeteneği değerlendirilmiştir. Önerilen sistemin testi için alınan sinyaller üzerinden elde edilen doğruluk oranı Şekil 3.28 ile gösterilmektedir.



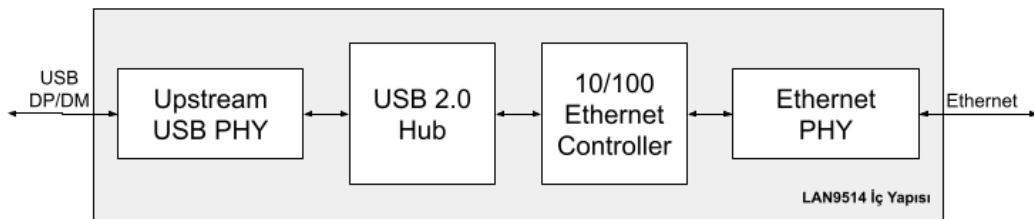
Şekil 3.28 Bir taklit saldırısı sırasında CNN modelinin gerçek zamanlı doğruluk oranları

Hem kimlik hırsızlığı hem de taklit saldırısı testlerinden elde edilen sonuçlara göre, saldırı yapan cihazların sinyal karakteristiklerini doğru bir şekilde kopyalayamadığı açıkça görülmektedir. Sonuç olarak, LoRa iletişim destekli cihazlarda fiziksel katmanda kimlik doğrulaması yapılarak sistem güvenliği sağlanabilir.

4.1 Ethernet Sinyali Üzerinden Kimliklendirme

4.1.1 Teorik Yaklaşım

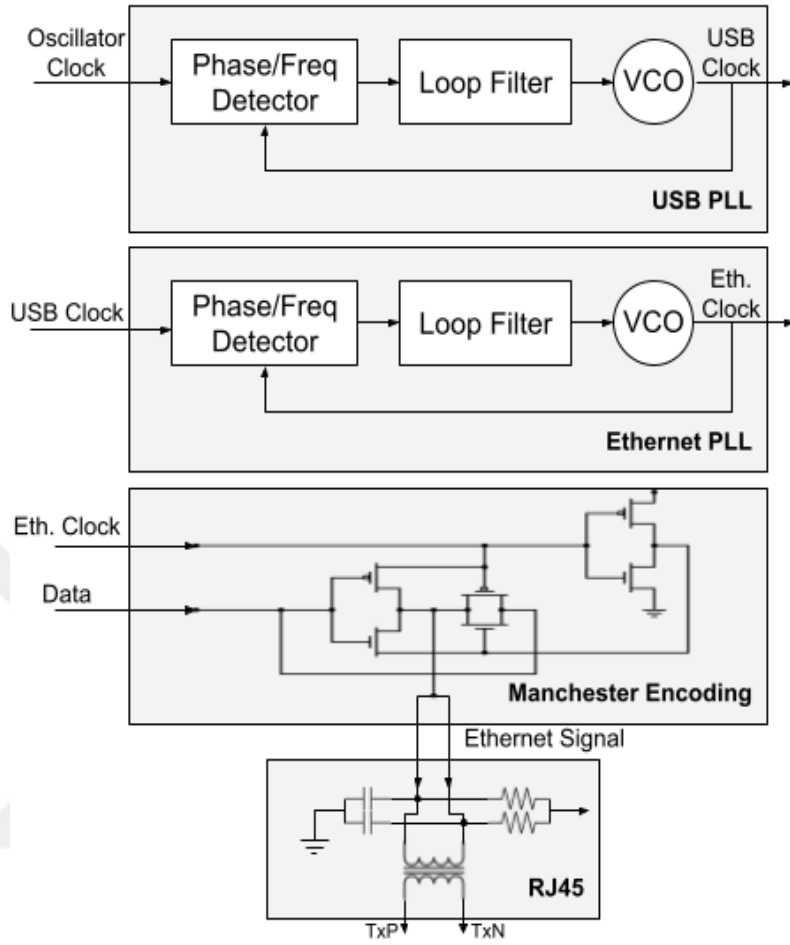
Ethernet üzerinden iletişim kuran elektronik cihazlar, genellikle bir modem veya yönlendiriciye doğrudan bağlanmaktadır. Cihaz kimliklerinin (MAC adresleri veya kimlikler) elle atanması, cihaz kimliğinin taklit edilmesi gibi güvenlik açıklarına yol açabilmektedir. Bu nedenle, cihazların kimliklerinin benzersiz özelliklerine dayanarak çıkarılması gereksinimi ortaya çıkmıştır. Elektronik cihazlarda bulunan bileşenler ve bu bileşenlerin entegrasyonu, belirli tolerans değerlerine sahiptir ve bu tolerans değerlerinin sinyal üzerindeki etkisi, cihazlar için bir parmak izi oluşturmaktadır. Literatürde yaygın olarak kullanılan Raspberry Pi 3 cihazının donanımı incelendiğinde, Ethernet bağlantısı için LAN9514 entegre devresinin kullanıldığı görülmektedir. Bu entegre devre içerisinde Ethernet sinyalinin oluşturulmasında kullanılan dahili bileşenler Şekil 4.1 ile verilmiştir.



Şekil 4.1. Ethernet haberleşmesinde kullanılan LAN9514 entegre devresinin iç yapısı

Entegre devrenin iç yapısı incelendikten sonra tolerans değerlerini matematiksel olarak ifade etmek için kullanılan devre yapıları Şekil 4.2 ile verilmiştir. Sunulan

yapı, ürün kataloğunda yer alan bilgiler temel alınarak hazırlanmış olup yalnızca Manchester Kodlaması için sunulmaktadır.



Şekil 4.2 Ethernet haberleşmesinde kullanılan LAN9514 entegre devresinin elektronik modeli

Elektronik devrelerde, öncelikli olarak saat sinyalini üretmek için bir kristal kullanılmaktadır. Kullanılan kristalin katalog bilgileri incelendiğinde, ± 20 ppm (milyonda bir parça) frekans toleransına ve sinyalin yükselme-düşme durumları için 5 ns gecikmeye sahip olduğu görülmüştür. Üretilen osilatör sinyalinin frekansını istenilen değere ayarlamak için Faz Kilitlemeli Döngü (Phase-Locked Loop, PLL) yapısı kullanan elektronik devreler tercih edilmektedir. Kullanılan PLL yapısında, bir geri besleme filtresi ve Gerilim Kontrollü Osilatör (Voltage-Controlled Oscillator, VCO) bulunmaktadır ve bu bileşenlerin oluşturduğu kapalı döngü transfer fonksiyonu denklem (4.1) ile ifade edilmektedir. Burada, filtre $F(s)$ ile, VCO ise K_o/s ile gösterilmektedir.

$$H(s) = \frac{F(s) * K_o / s}{1 + F(s) * K_o / s} \quad (4.1)$$

Frekans dönüşümü sürecinde faz gürültüsünün oluşumu, literatürde önemli bir konu olarak ele alınmaktadır. Bu faz gürültüsünün oluşma nedeni, kullanılan elektronik bileşenlerin yapısına dayandırılmaktadır. Kullanılan filtre yapısının oluşturduğu faz gürültüsü, bileşen toleransları nedeniyle sinyallerde kendine özgü bir karakteristik oluşturur. Literatürde, PLL için faz gürültüsü Leeson denklemi (4.2) ile ifade edilmektedir [117], [118]. Tek yan bant faz gürültü yoğunluğunu ifade eden L_{PM} , dBc/Hz biriminde ölçülmektedir. F , cihazın çalışma güç seviyesindeki gürültü faktörünü (lineer ölçekli) temsil etmektedir. Boltzmann sabiti, k_B , 1.38×10^{-23} J/K değerindedir. T , sıcaklığı Kelvin cinsinden ifade eder. A , osilatör çıkış gücünü watt cinsinden temsil etmektedir. Q_L , boyutsuz bir parametre olan yüklenmiş Q faktörüdür. f_o , osilatör taşıyıcı frekansını; f_m , taşıyıcıdan olan frekans sapmasını ifade etmektedir.

$$L_{PM} = 10 \log \left[\frac{F k_B T}{A} \frac{1}{8 Q_L^2} \left(\frac{f_o}{f_m} \right)^2 \right] \quad (4.2)$$

Gerekli Ethernet saat sinyali, PLL yapıları aracılığıyla üretilmekte ve Ethernet sinyallerinin oluşturulmasına olanak tanımaktadır. Örneğin, Manchester kodlama tekniğinde, iletilecek bit ile saat sinyalinin giriş olarak kullanıldığı bir XOR (Özel VEYA) kapısı kullanılmaktadır. XOR kapısı içerisindeki yarı iletken ve pasif bileşenlerin tolerans değerlerinin sinyali etkileyebileceği ve potansiyel olarak değişiklikler yaratabileceği unutulmamalıdır. LAN9514 entegre devresi aracılığıyla üretilen sinyalin, RJ45 konektörü üzerinden iletilmesi sürecinde kullanılan dirençler, kapasitörler ve transformatörlerden oluşan yapı da sinyalin karakteristiklerini etkilemektedir. Örneğin, Raspberry Pi 3 cihazının elektronik kartı üzerinde, Ethernet sinyalinin iletim aşamasına kadar olan süreç için genel bir model geliştirilmiştir. Bu modellere ek olarak, elektronik kartın yerleşim düzeni, Ethernet kablosu ve bağlı ağ cihazı da Ethernet sinyalinin karakteristikleri üzerinde etkide bulunmaktadır.

4.1.2 Ethernet Sinyal Karakteristiđi

Ethernet, bilgisayar ađlarında veri iletimi için kullanılan yaygın bir teknolojidir ve sinyal karakteristikleri önemli bir rol oynar. Ethernet'in sinyal karakteristiklerini anlamak için öncelikle fiziksel katmanı ve veri bađlantı katmanını incelemek gereklidir.

Fiziksel katman, veri sinyallerinin fiziksel ortamda nasıl iletileceđini belirler. Bu katmanda, elektriksel ve optik sinyaller kullanılarak veri taşınır. Elektriksel sinyaller bakır kablolar üzerinden iletilirken, optik sinyaller fiber optik kablolar üzerinden iletilir. Ethernet'in elektriksel sinyal karakteristikleri, voltaj seviyeleri ve sinyal sürekliliđi ile tanımlanır. Örneđin, 10BASE-T Ethernet standardında, Manchester kodlama kullanılarak veri iletilir. Bu kodlama yöntemi, her bitin başlangıcında ve ortasında voltaj seviyesinin deđiştii bir sinyal oluşturur. Bu sayede, alıcı cihaz, veri sinyalini dođru bir şekilde çözebilir. 100BASE-TX ve 1000BASE-T gibi daha yüksek hızlara sahip Ethernet standartlarında ise, farklı kodlama yöntemleri ve voltaj seviyeleri kullanılır. 100BASE-TX'de 4B5B kodlama ve MLT-3 sinyalizasyonu kullanılırken, 1000BASE-T'de 4D-PAM5 kodlama yöntemi kullanılır. Optik sinyaller, Ethernet'in fiber optik versiyonlarında kullanılır ve bu sinyaller ışık dalga boyları ile tanımlanır. Fiber optik Ethernet standartlarında, verinin iletimi için genellikle 850 nm, 1310 nm ve 1550 nm dalga boyları kullanılır. Bu dalga boyları, fiber optik kablonun türüne ve iletim mesafesine göre seçilir. Optik sinyaller, yüksek bant genişliđi ve düşük kayıp oranları sayesinde, özellikle uzun mesafeli veri iletiminde avantaj sağlar.

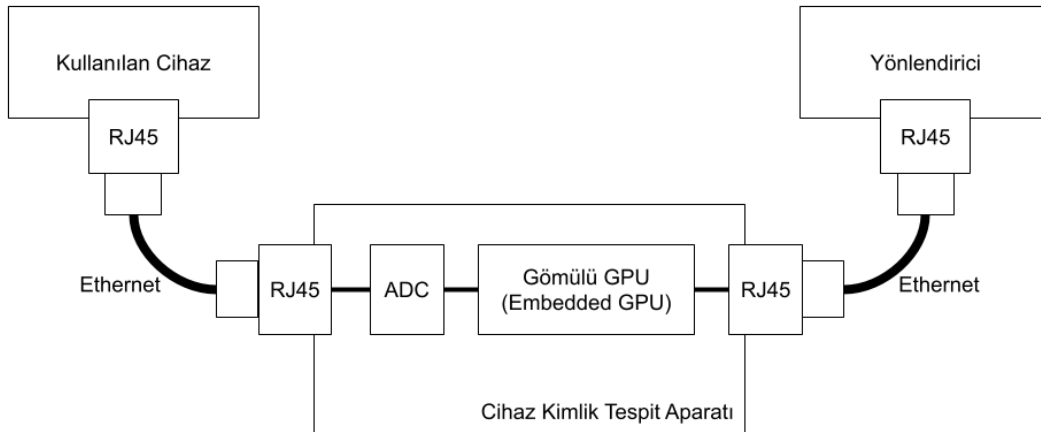
Veri bađlantı katmanı, Ethernet çerçevelerinin oluşturulması ve iletilmesi ile ilgilendir. Bu katmanda, çerçeveleme, hata tespiti ve düzeltme, akış kontrolü gibi işlemler gerçekleştirilir. Ethernet çerçeveleri, belirli bir yapıya sahiptir ve başlık (header), veri (payload) ve sonlandırma (trailer) kısımlarından oluşur. Başlık kısmında kaynak ve hedef MAC adresleri, protokol türü gibi bilgiler yer alır. Veri kısmı, iletilen gerçek veriyi içerir ve sonlandırma kısmı ise çerçevenin bitişini belirtir.

Ethernet'in sinyal karakteristikleri, ađın performansı ve güvenilirliđi açısından kritik öneme sahiptir. Dođru sinyal seviyesi ve sürekliliđi sağlanmazsa, veri

iletiminde hatalar meydana gelebilir ve ağ performansı düşebilir. Bu nedenle, Ethernet ağlarının tasarımı ve kurulumu sırasında, sinyal karakteristiklerinin doğru bir şekilde yönetilmesi gereklidir. Bu, uygun kablo türlerinin seçimi, kablo uzunluklarının sınırlandırılması ve uygun sinyalizasyon yöntemlerinin kullanılması ile sağlanabilir.

4.1.3 Önerilen Tasarım

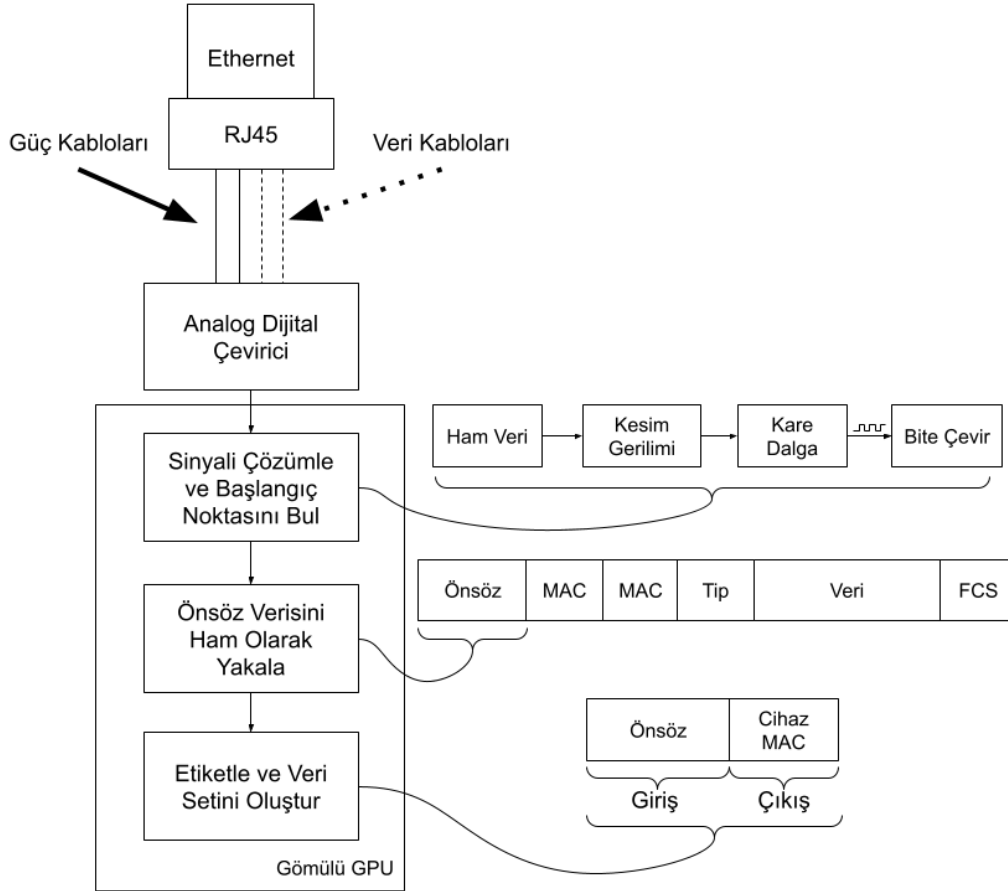
Elektronik cihazlar Ethernet üzerinden haberleşirken direkt olarak modem ya da yönlendiriciye bağlı olmaktadır. Aynı ağa bağlı tanımlanmayan cihazlar güvenlik bakımından sorun oluşturmaktadır. Bu nedenle oluşturulan yapı ile cihazların gerçek kimlikleri Şekil 4.3 ile verilmiş olan Cihaz Kimlik Tespit Aparatı ile tespit edilebilmektedir. Bunun için cihaz üzerinden alınan Ethernet sinyalleri analog olarak okunup içinde makine öğrenmesi modeli bulunan Gömülü GPU ile cihazın kimliği saptanmaktadır. Cihazın gerçek kimliği ile MAC adresi arasında uyumsuzluk bulunması durumunda da cihaz sisteme dahil olmadan direkt fiziksel katmanda engellenmektedir.



Şekil 4.3 Ethernet sinyali üzerinden cihaz kimliklerinin tespitine yönelik sistemin genel mimarisi.

Önerilen sistem, iki farklı adım temelinde çalışmaktadır. Birinci aşamada, veriler toplanarak derin öğrenme modelinin eğitimi gerçekleştirilirken, ikinci aşamada elde edilen model uç cihaza aktarılmakta ve güvenlik kontrolleri bu cihazda yapılmaktadır. Paketin güvenlik kontrolünün gerçekleştirileceği noktanın

belirlenebilmesi için öncelikle Önsöz verisinin yakalanması gerekmektedir. Bu yakalama işlemi için, Şekil 4.4 ile verilen veri kablolarındaki sinyaller kullanılacaktır. Ethernet Önsöz bilgisi bilinen bir formata sahiptir ve bu formata dayanarak paketin varışı tespit edilip başlangıç noktası belirlenmektedir. Bu keşif işlemi, gelen verilerin GPU'ya gönderilmesi ve paket konumlarının belirlenmesi için gerekli hesaplamaların yapılması ile gerçekleştirilir. Bu konumlar belirlendikten sonra, gelen sinyalin ham haliyle birleştirilerek sinyalin Önsöz kısmı, gelen sinyalin cihazına ait MAC adresiyle etiketlenerek kaydedilir.

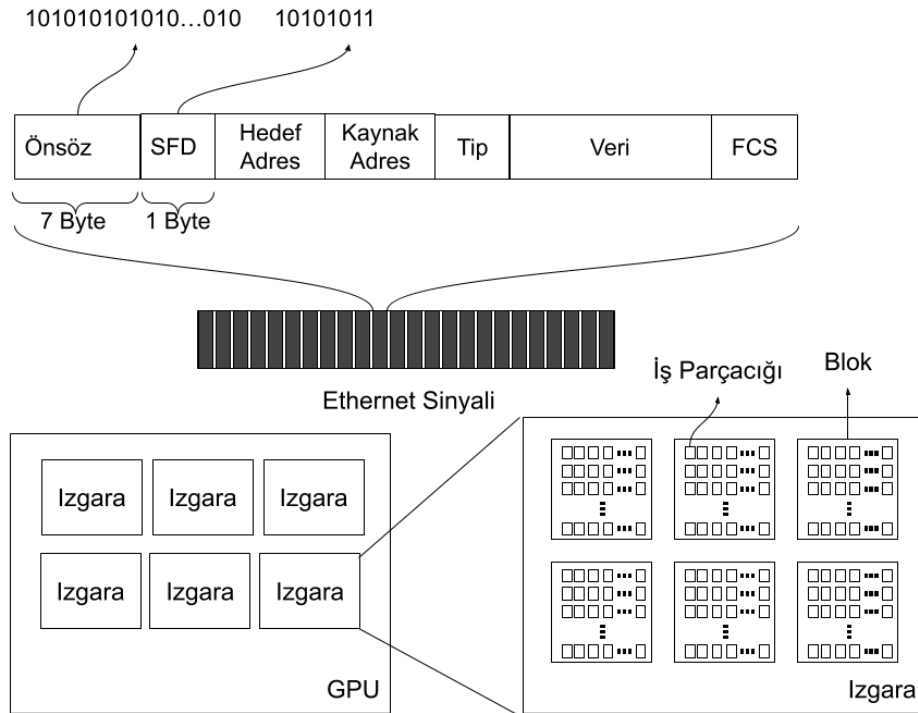


Şekil 4.4 Ethernet sinyallerinden veri seti oluşturulması için kullanılan mimari.

İkinci adımda, yeterli miktarda veri seti toplandıktan sonra, uygun bir derin öğrenme algoritması kullanılarak model oluşturmak amacıyla eğitim gerçekleştirilmelidir. Oluşturulan derin öğrenme modeli, Ethernet iletişim hattı üzerinden alınan analog sinyalle birleştirilerek cihaz kimliklerinin tahmin edilmesini sağlamaktadır. Bu çalışma ile Ethernet iletişimde yarı iletken ve pasif bileşenlerin birbirleri üzerindeki doğrudan etkisi yakalanmış ve bu sayede cihaz

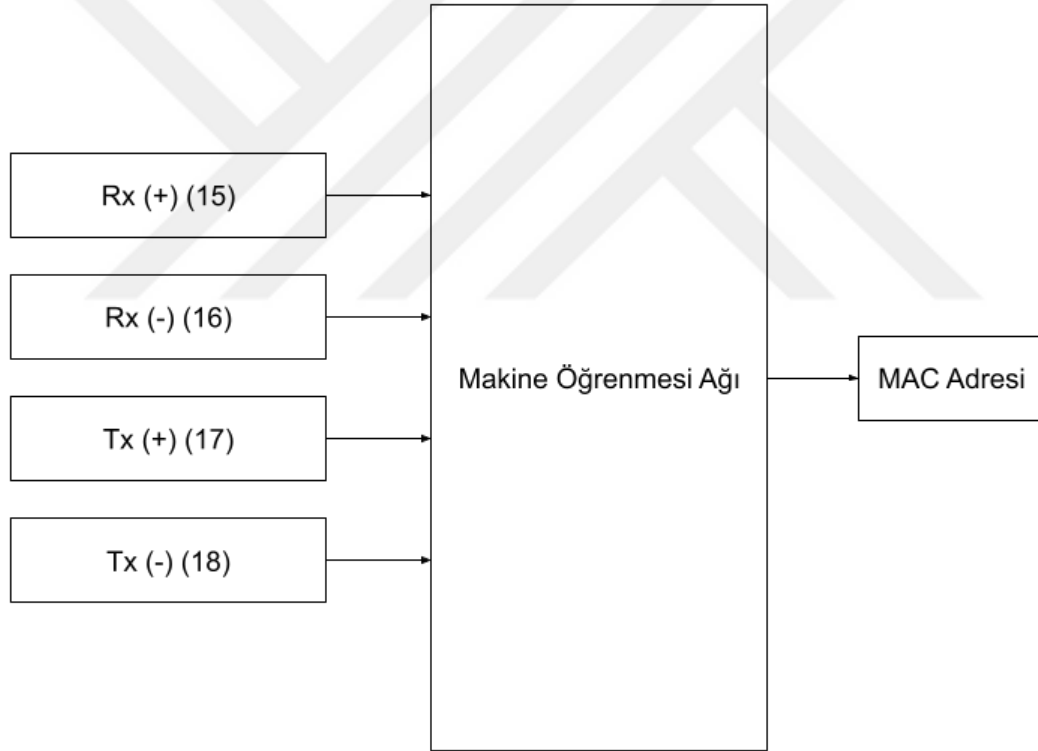
kimliklerinin belirlenmesi mümkün olmuştur. Belirlenen bu kimlikler, sistem güvenliğini sağlamak amacıyla kullanılmaktadır.

Elde edilen verilerden Ethernet paketlerinin konumlarını tespit etmek için Şekil 4.5 ile sunulan yapılar kullanılmıştır. Bu yapının içinde, Önsöz ve Başlangıç Çerçeve Ayırıcısı (Start Frame Delimeter, SFD) bilgisi, standart formatın bir parçası olarak her pakette tutarlı bir şekilde bulunmaktadır. Bu nedenle, alınan sinyalde bu paket formatının aranması gerekmektedir. Paketlerin keşfedilmesini ve analiz edilmesini hızlandırmak için, paralel işlem yapabilme yeteneklerinden dolayı GPU'daki CUDA çekirdekleri kullanılmıştır. Gelen sinyal her saniye doğrudan GPU'ya gönderilmekte ve ızgara, iş parçacığı ve blok yapıları kullanılarak paketler paralel olarak taranmaktadır. Arama süreci sırasında her bir iş parçacığı, tüm verileri paylaşılan bir bellek alanında tutmakta ve her bir veriye indeks bilgisiyle paralel olarak erişebilmektedir. Aynı anda, gelen paketin içindeki çerçevelerin indeksleri CPU'ya geri döndürülmektedir. Sonuç olarak, bu yaklaşım CPU üzerindeki yükü azaltmakla kalmayıp, sistem içinde gerçekleştirilen paralel tarama sayesinde CPU tabanlı işlemlere kıyasla daha hızlı çalışmaktadır.



Şekil 4.5 Ethernet sinyalinin GPU üzerinde işlenebilmesi için gerekli işlem adımları

Ethernet sinyalindeki paketlerin konumlarının belirlenmesi ve elde edilen verilerin cihaz kimliklendirmesi için kullanılması gerekmektedir. Ethernet çerçevesinin Önsöz kısmı, SFD dahil olmak üzere toplamda 8 bayttan oluşmaktadır. Her bir bit analog olarak okunduğunda, toplamda 64 veri noktası elde edilmektedir. Makine öğrenimi eğitimi kolaylaştırmak amacıyla, Ethernet sinyalindeki veri pinlerinden voltaj değerlerinin çıkarılması gereklidir. Bu işlem, Şekil 4.6 üzerinde verilmiş olan Rx (+), Rx (-), Tx (+) ve Tx (-) pinleri kullanılarak gerçekleştirilmekte ve bu da toplamda 2x64 boyutunda giriş verisi sağlamaktadır. 40 MSPS hızında bir ADC ve 10 MBPS hızında bir Ethernet kullanılması göz önüne alındığında, toplam veri boyutu 2x256 olmaktadır. Bu nedenle derin öğrenme modelinde giriş katmanı 2x256 olarak tanımlanmış, çıkış katmanının boyutu ise sistemde kullanılan cihazların sayısına göre belirlenmiştir.



Şekil 4.6 Ethernet sinyal kabloları ile oluşturulmuş olan sistemin birleşik gösterimi

4.1.4 Derin Öğrenme

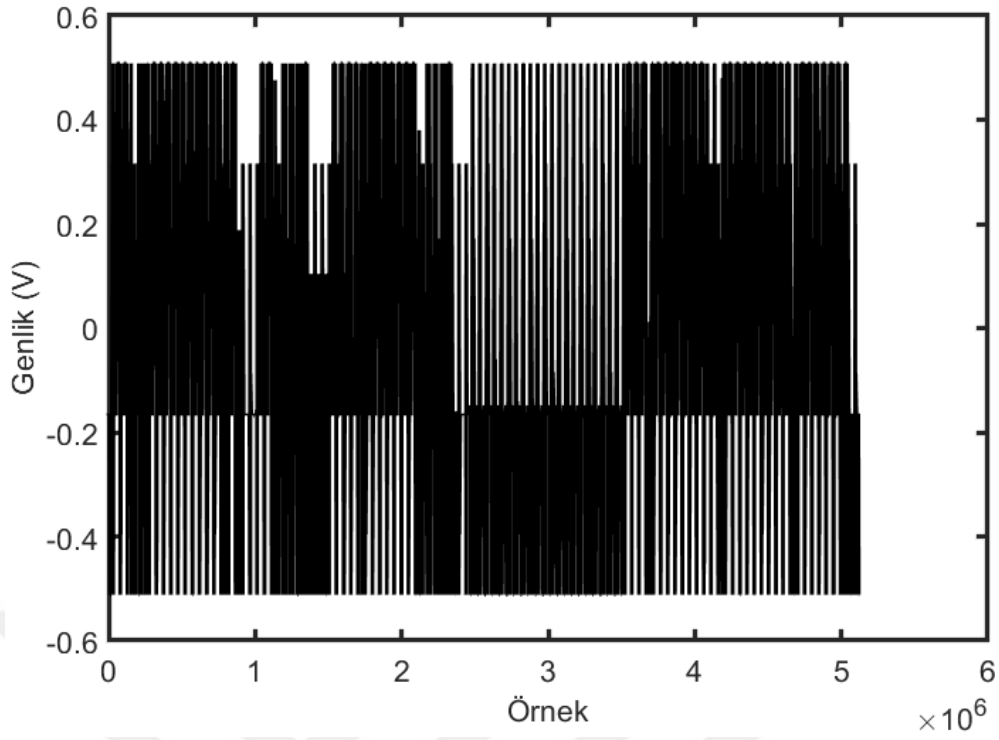
Mevcut literatürde kullanılan yöntemlere göre, yalnızca iletilen sinyallerden temel özellikleri çıkarmak için ön işleme adımları uygulanmış ve matematiksel

formülasyonlar oluşturulmuş ya da cihaz kimliklendirmesi için makine öğrenimi yöntemleri kullanılmıştır. Önerilen sistemde, Ethernet kablosunun her iki uca bağlı olması nedeniyle sinyal karakteristiklerinin yalnızca gönderici tarafından değil, aynı zamanda alıcı (modem, yönlendirici vb.) tarafından da etkilendiği gözlemlenmiştir. Bu nedenle, bu çalışma kapsamında hem alıcı hem de gönderici sinyalleri kullanılmıştır. Derin öğrenmede kullanılacak giriş-çıkış parametreleri belirlendikten sonra uygulanacak yöntem seçilmiştir. Girişlerin zaman serisi verisi niteliğinde olması nedeniyle bu çalışmada derin öğrenmenin LSTM algoritması kullanılmıştır. LSTM algoritmasına giriş olarak Ethernet sinyali verilmiş, çıkış ise sistemde bulunan cihaz sayısını bitlerle kodlanmış şekilde temsil etmiştir.

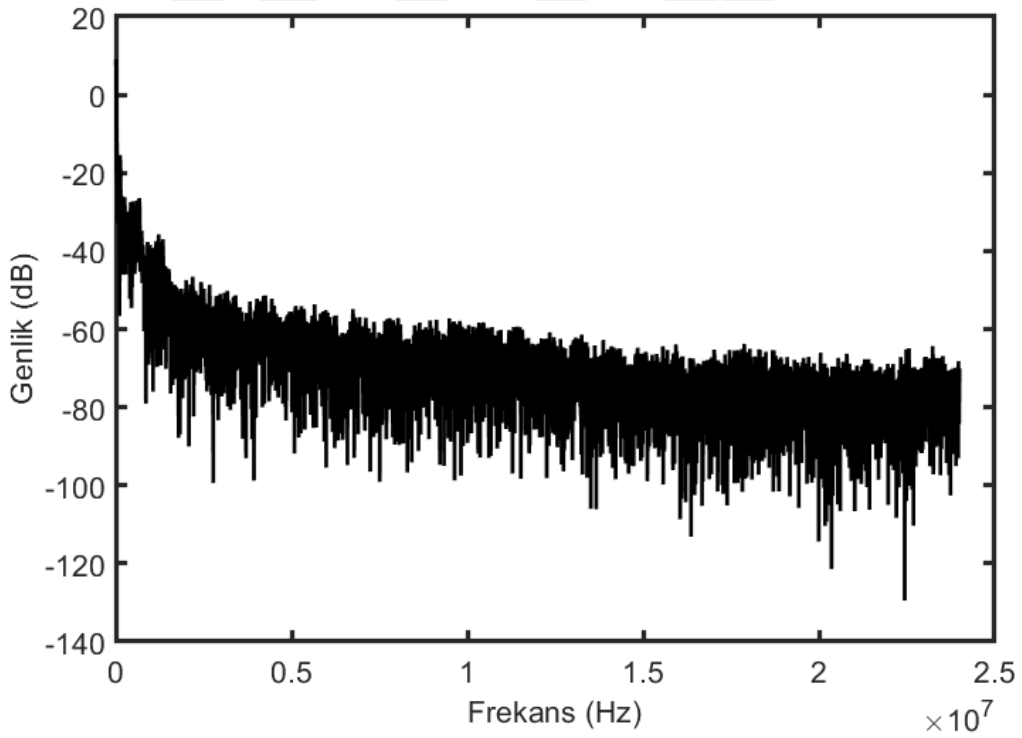
Kullanılan LSTM modeli, her biri 50 hücreden oluşan üç katmandan meydana gelmiş ve Adam optimizasyon algoritmasını kullanmıştır. Oluşturulan model sisteme entegre edildikten sonra, gelen analog sinyal verisi, Ethernet üzerinden modeme veya yönlendiriciye ulaşmadan önce kontrol edilmiştir. Sistem içerisinde cihaz kimliğinde bir uyumsuzluk gibi bir sorun tespit edilmesi durumunda, sistem sunucuya bir uyarı göndermiştir.

4.1.5 Deneysel Sonuçlar

Ethernet iletişim sinyalleri aracılığıyla elektronik devrelerin karakteristiklerini belirlemek için öncelikle veri setinin toplanması gereklidir. Önerilen sistemin doğruluğunu kanıtlamak amacıyla, aynı model ve işletim sistemine sahip iki adet özdeş Raspberry Pi 3 cihazı kullanılmıştır. Raspberry Pi 3 cihazlarında Ethernet iletişimi 10 MBPS olarak yapılandırılmış ve ölçümler bir ADC kullanılarak gerçekleştirilmiştir. Örnek bir ölçüm sonucu, zaman eksenini için Şekil 4.7 (a) ve frekans eksenini için Şekil 4.7 (b) olacak şekilde grafiksel olarak sunulmuştur.



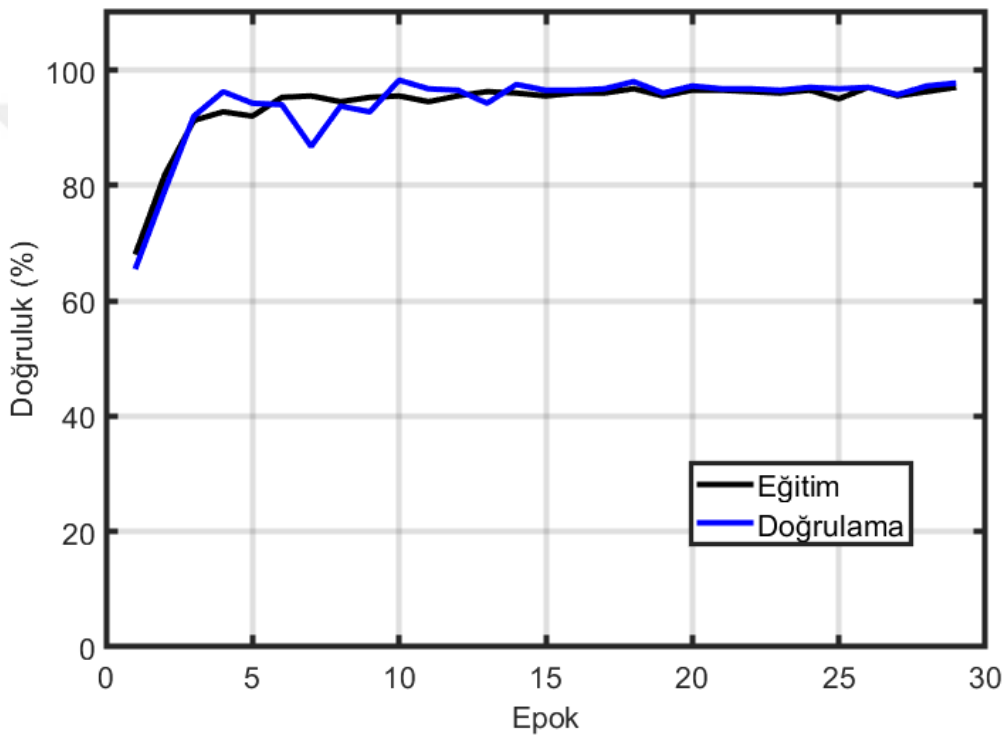
(a)



(b)

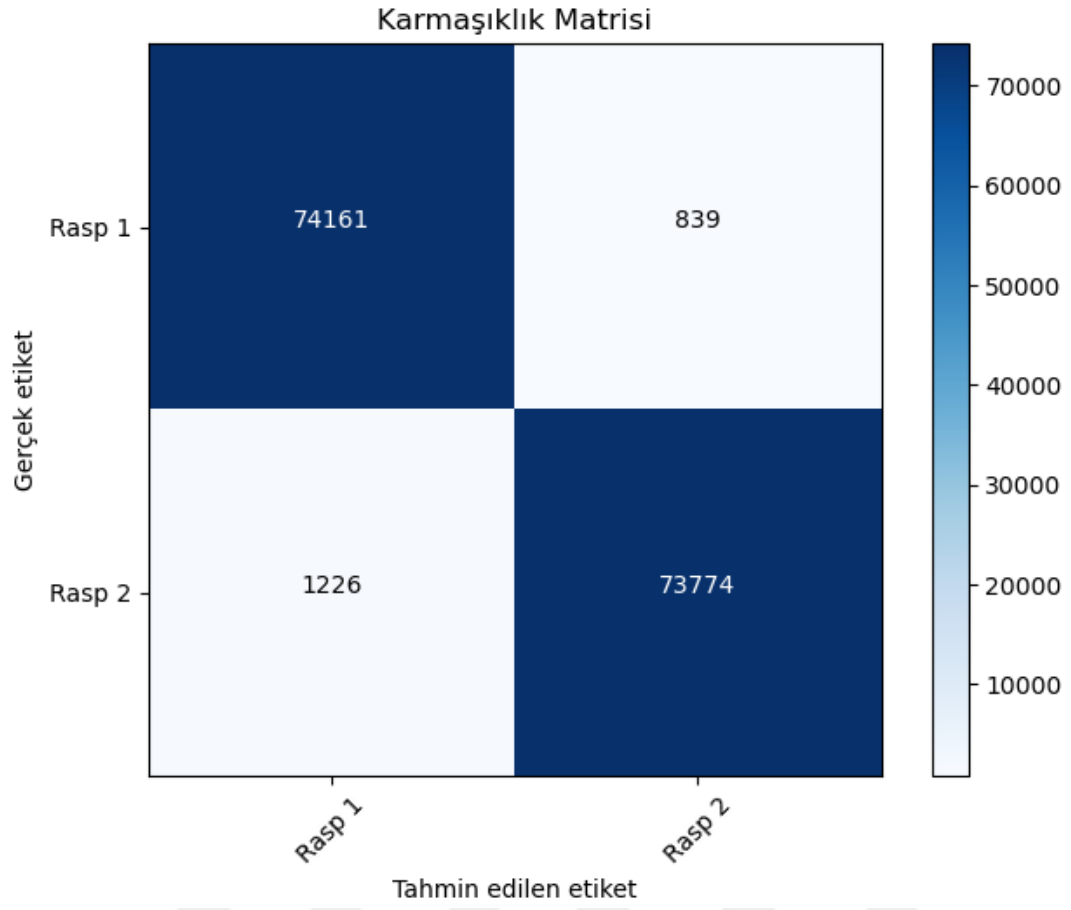
Şekil 4.7 Ethernet iletişim (a) zaman alanı (b) frekans alanı sinyali özellikleri

Fiziksel katman güvenliği ve cihaz tanımlamasını geliştirmek amacıyla, Ethernet sinyallerinden bir veri seti toplanmıştır. Bu veri seti, bir derin öğrenme modeli eğitmek için kullanılmıştır. Özellikle, iki adet Raspberry Pi 3 cihazından toplam bir milyon Önsöz verisi örneği elde edilmiştir. Toplanan veri seti, zaman serisi sinyallerinde yüksek performansı ile bilinen bir derin öğrenme algoritması olan LSTM algoritması kullanılarak eğitilmiştir. Eğitim sürecinin ardından, Şekil 4.8 ile gösterilen eğriye göre %98 doğruluk oranına ulaşılmıştır. Elde edilen bu doğruluk oranı, cihazların doğru kimliğe ulaşma oranının ortalama yüzdesini ifade etmektedir.



Şekil 4.8 Epok sayısına göre doğruluk oranı

Doğrululuk oranının elde edilmesinin ardından, doğru ve hatalı tahminler Şekil 4.9 ile sunulan Karışıklık Matrisi ile görselleştirilmiştir. Görülebileceği üzere, cihazlar aynı donanım ve yazılıma sahip olsa dahi, cihazların içindeki bileşenlerin toleransları Ethernet iletişim sinyalleri aracılığıyla benzersiz tanımlama yapılmasını sağlamaktadır. Bu doğrultuda, cihazlar fiziksel katmanda benzersiz bir şekilde tanımlanmış ve ayrıca, taklit cihazların ağa bağlanmadan önce ağı aşırı yüklemesi engellenmiştir.



Şekil 4.9 İki Raspberry Pi 3 cihazının derin öğrenme modeli tahminleri için Karmaşıklık Matrisi

5

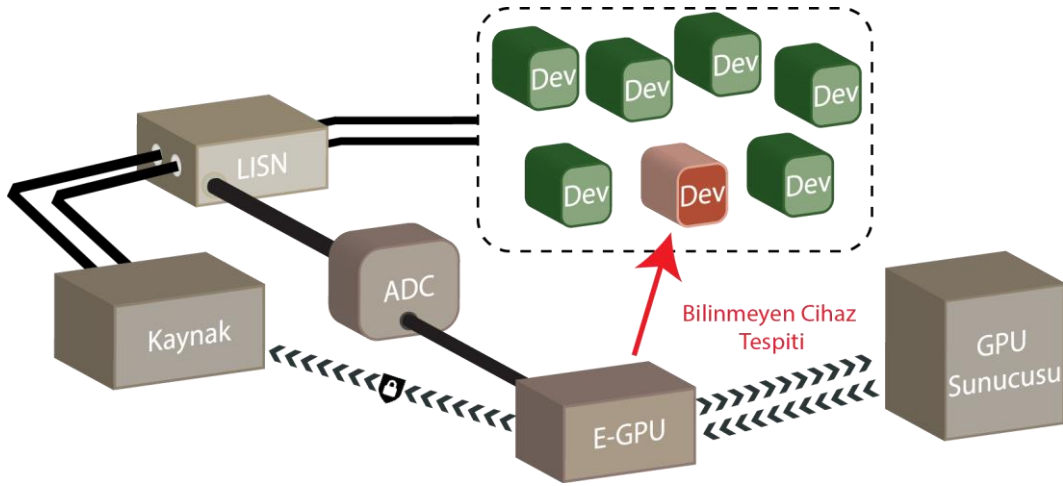
ELEKTROMANYETİK EMİSON İLE KİMLİKLENDİRME

5.1 İletilen Elektromanyetik Sinyal ile Kimliklendirme

Elektronik cihazlar bulunduğu güç hattı üzerinden geriye doğru gürültü oluşturmaktadır. Oluşturulan bu gürültü elektronik cihazın komponentlerine bağlı olarak oluşmakta ve spesifik bir kartın tanımlanmasına yardımcı olabilmektedir. Bununla beraber cihazın bağlı bulunduğu kaynağı da gürültü oluşturmaktadır ve bu gürültü ile elektronik cihazın gürültüsü LISN ile ayrıştırılabilmektedir.

5.1.1 Önerilen Tasarım

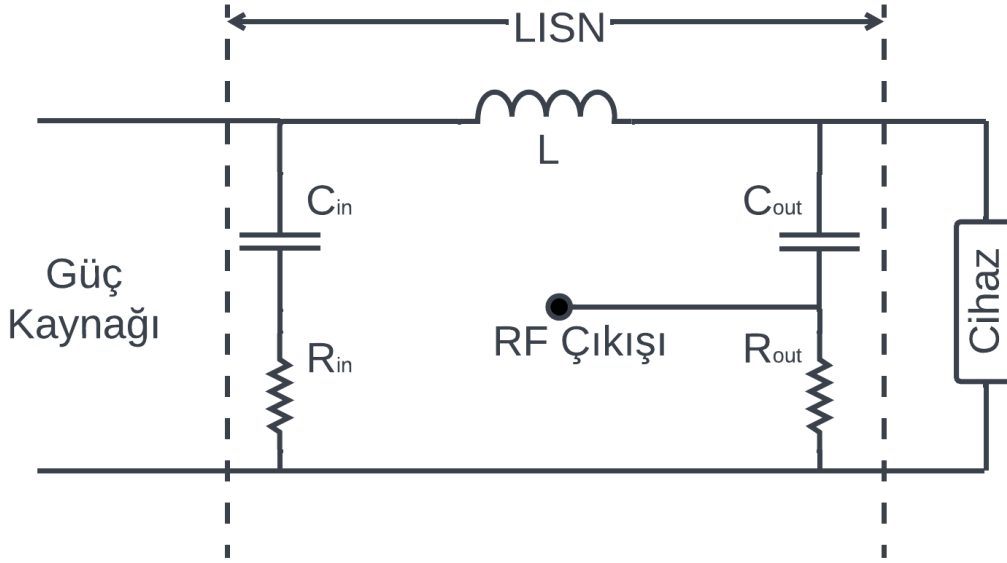
Önerilen sistemin genel mimarisi Şekil 5.1 ile gösterilmektedir. Verilen senaryoda gözlemlendiği gibi, cihazların kaynağa bağlandığı bir ortamda, sistemde tanımlı olmayan bir cihaz bulunmaktadır. Önerilen tasarımda, her bir cihaz bir LISN cihazına bağlanmış ve LISN'ın RF portu bir ADC ile bağlantılıdır. ADC, analog veriyi dijital formata çevirir ve bu veriyi bir Gömülü GPU'ya (E-GPU) iletir. E-GPU, veriyi iki farklı şekilde kullanır. İlk durumda, veri, bir veri seti oluşturmak için kullanılır ve bir GPU sunucusuna gönderilir; bu sunucu, derin öğrenme modeli oluşturmak için verileri kullanır. İkinci durumda ise, derin öğrenme modeli sunucu tarafından E-GPU'ya yüklendikten sonra, gelen sinyallerin bu modele uygun olup olmadığını tespit ederek güvenliği sağlar. Eğer tanınmayan bir cihaz tespit edilirse, E-GPU, kaynağa bu cihazın bağlantısını kesmesini bildiren bir sinyal gönderir. Bu doğrulama işlemi, cihaz yeniden başlatıldığında ve sürekli gerçek zamanlı çalışmaya geçtiğinde tekrarlanır.



Şekil 5.1 Elektromanyetik emisyon tabanlı kimliklendirme sisteminin genel mimarisi

Elektronik devrelerde bulunan komponentler, sinyal hatları ve elektromanyetik uyumluluğun sağlanabilmesi için yapılan eklemelerin tolerans değerleri cihazların ve elektronik devre kartlarının ayrıştırılması açısından en önemli faktördür. İletilen emisyon ölçümünün yapılabilmesi için LISN cihazı kullanılmaktadır. LISN, EMC testleri sırasında elektrikli cihazların güç hattındaki giriş ve çıkış emisyonlarını ölçmek için kullanılan bir test cihazıdır. Bu test cihazının çalışma kapsamında kullanılan elektronik devre şeması Şekil 5.2 ile verilmiştir. LISN, elektrikli cihazın güç hattına (elektrik şebekesine) bağlanır ve cihazın iletilen veya yayılan elektromanyetik emisyonunu ölçmek amacıyla kullanılmaktadır ve güç hattı üzerindeki giriş-çıkış emisyonlarını ayırmak için iki ayrı devre bulundurmaktadır.

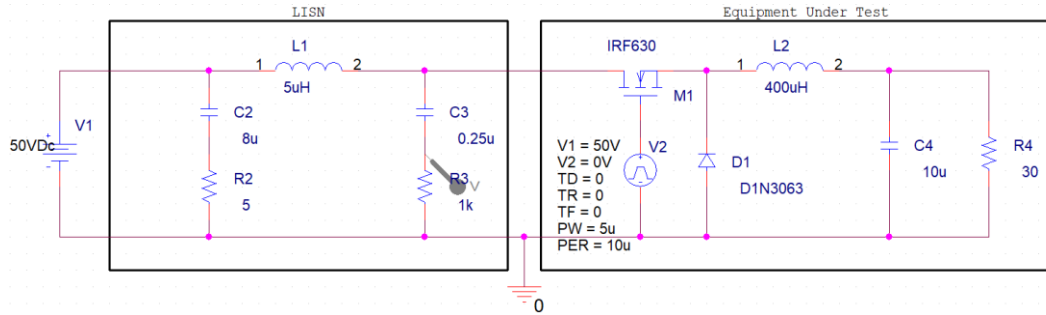
Giriş tarafında bulunan devre, elektrik şebekesinden gelen güç sinyalini almakta ve giriş emisyonlarını ölçmek için bir yük direnci ve filtreler içermektedir. Bu devre, elektrik şebekesi üzerindeki parazitlerin cihaza etkisini azaltmakta ve sadece cihazın girişinden kaynaklanan emisyonları ölçmeye odaklanmaktadır. Çıkış tarafındaki devre ise, cihazın güç hattına geri beslediği emisyonları ölçmek için kullanılmaktadır. Bu devre, çıkış emisyonlarını ölçmek için bir yük direnci ve filtreler içermektedir. Böylece, cihazın güç hattına geri beslediği emisyonlar belirlenmektedir.



Şekil 5.2 Elektromanyetik emisyon ölçümünde kullanılan LISN devresi.

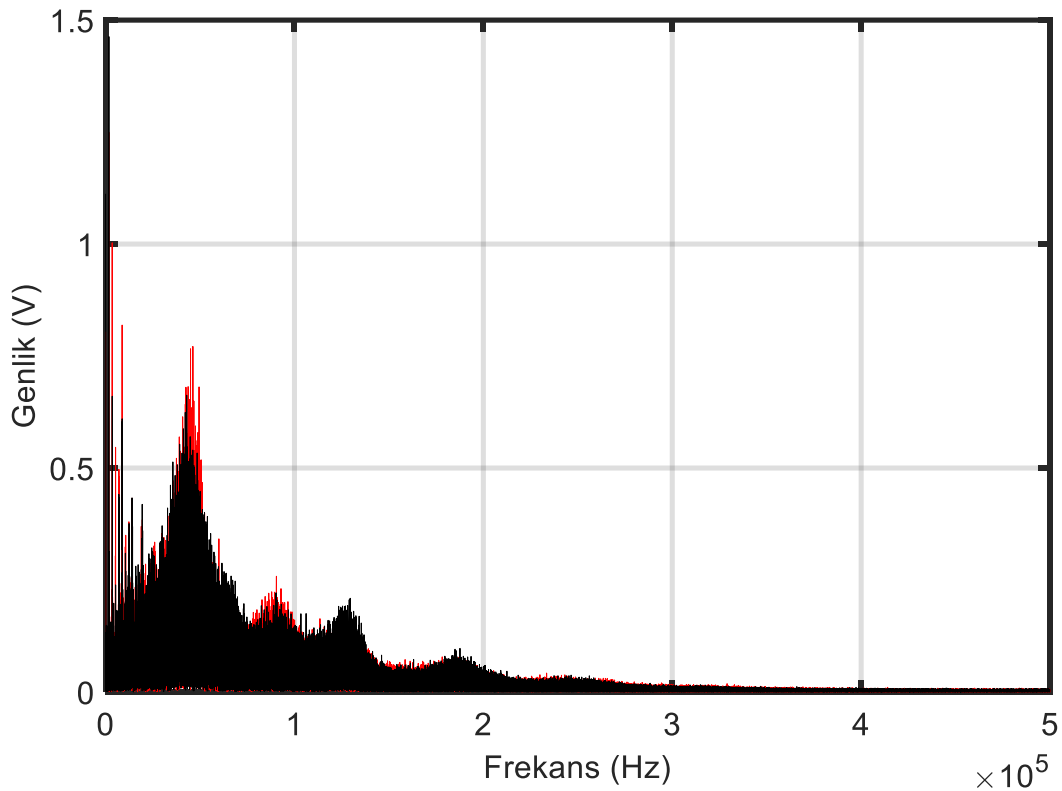
5.1.2 Veri Setinin Oluşturulması

Elektronik devre kartlarının yaydığı elektromanyetik emisyon değerleri simülasyon programları kullanılarak LISN ve test edilecek devrenin modellendiği çalışmalar bulunmaktadır [119]–[122]. Bu çalışmalar kapsamında belirli bir devre modeli ve LISN modeli oluşturularak devre modelinden kaynaklanan emisyon değeri simülasyon ve teorik yaklaşımlar ile çözülmektedir. Elektromanyetik kimliklendirme için de benzer şekilde LISN ve test ekipmanı modellenerek alınan sinyaller ile kimliklendirme çalışmaları yapılabilir. Bu kapsamda Şekil 5.3 ile verilen devre modeli oluşturulmuştur. Bu model kapsamında sol tarafta bulunan LISN cihazı üzerinden sağ tarafta bulunan test ekipmanı beslemesi sağlanmakta ve LISN cihazının çıkış pininden emisyon sinyalleri alınabilmektedir.

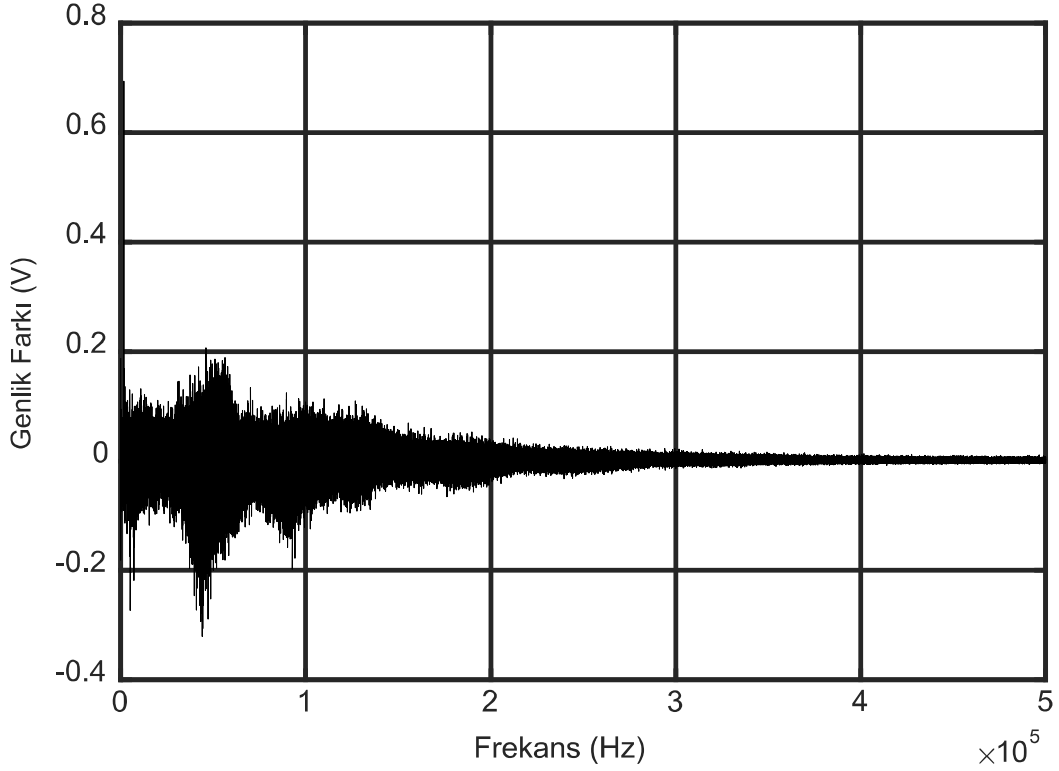


Şekil 5.3 Spice üzerinden veri toplamak için oluşturulmuş olan devre kurulumunun şematik gösterimi

Sinyallerin farklı kartlar için zaten ayırt edilebilir bir özellik verdiği hem literatür kapsamında hem de EMC testlerinde görülmektedir. Aynı elektronik devre yapısına sahip devrelerin yaydığı elektromanyetik emisyon üzerinden kimliklendirme yapmak için ise elektronik devrelerin tolerans değerleri kullanılmaktadır. Elektronik devre kartlarında kullanılan pasif komponentlerin tolerans değerleri ideal davranış yerine pratik olarak kullanılan değerleri kullanılmıştır. Sadece pasif komponentlerin %5 toleranslı çalıştırılması ile elde edilen iki ayrı devrenin sürekli zamandaki 30ms çalıştırılmasından sonra elde edilen sinyalin frekans domenindeki grafikleri Şekil 5.4 ile verilmiştir. Grafik üzerinden görüldüğü üzere pasif komponentlerdeki tolerans değerlerinden kaynaklı olarak özellikle baskın olan frekansta kaymaların olduğu anlaşılmaktadır. İki devrenin sinyalleri arasındaki farka bakmak için ise elde edilen veriler interpolasyon yapılmış sonrasında da birbirinden çıkarılarak Şekil 5.5 ile verilen grafik elde edilmiştir.

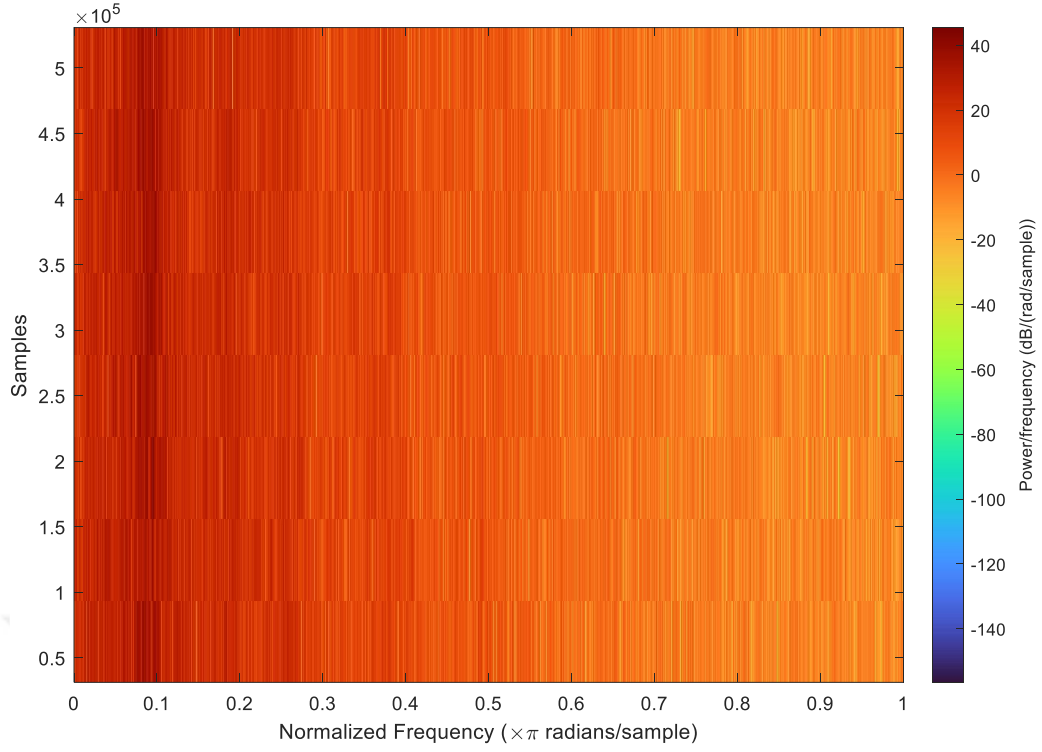


Şekil 5.4 Spice'tan alınan iki farklı cihaz sinyallerinin FFT dönüşümü



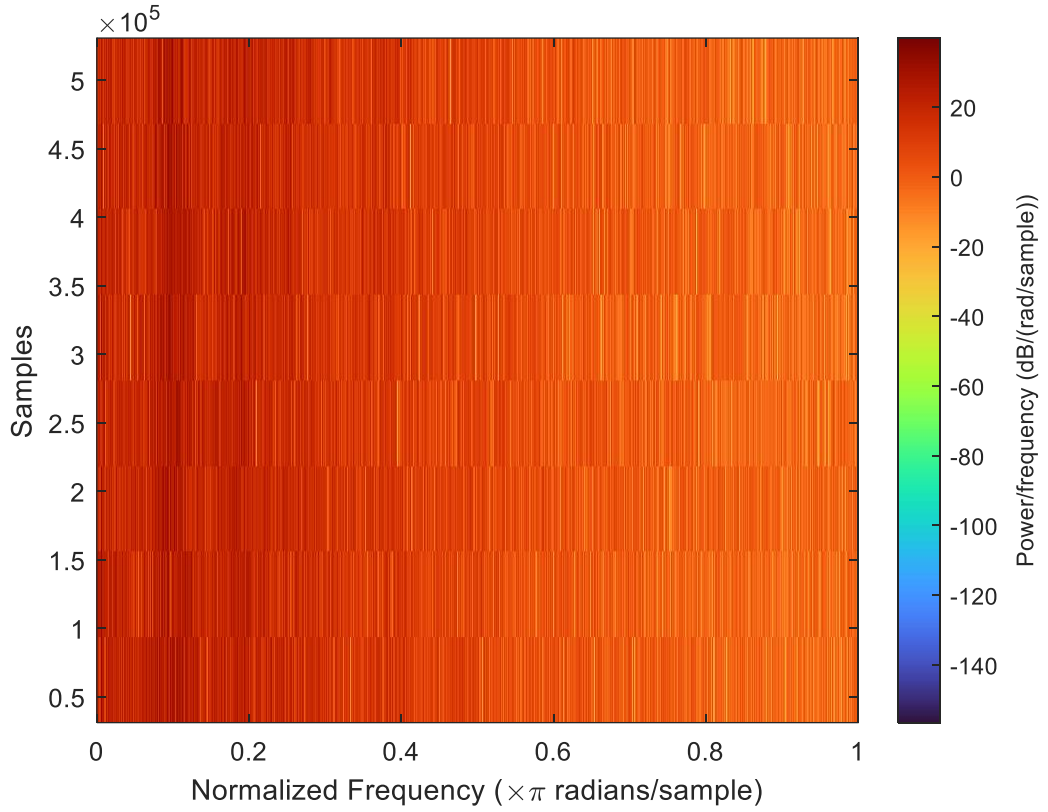
Şekil 5.5 Spice'tan alınan iki farklı cihaz sinyallerinin FFT dönüşümünün farkı

Sadece pasif komponentlerdeki tolerans değerlerinin bile frekans domenindeki farklılığa etkisi elektronik kartları ayırt etmeye yetmektedir. Ayrıca aktif komponentler ve elektronik kartlardaki sinyal hatlarındaki toleranslarda eklenince teorik olarak sinyallerin daha benzersiz olacağı anlaşılmaktadır. Elektronik devre kartlarını sadece frekans eksenini değil ayrıca zaman ekseninde de incelemek kimliklendirme açısından önem arz etmektedir. Bu nedenle hem frekans hem de zaman ekseninde inceleme yapmak için elektronik sinyallerin spektrogramı Şekil 5.6 ile verildiği gibi görüntülenebilmektedir. Bu grafik üzerinde elektronik devrelerden sadece birinin zaman ve frekansa bağlı olarak değişimi görülmektedir.



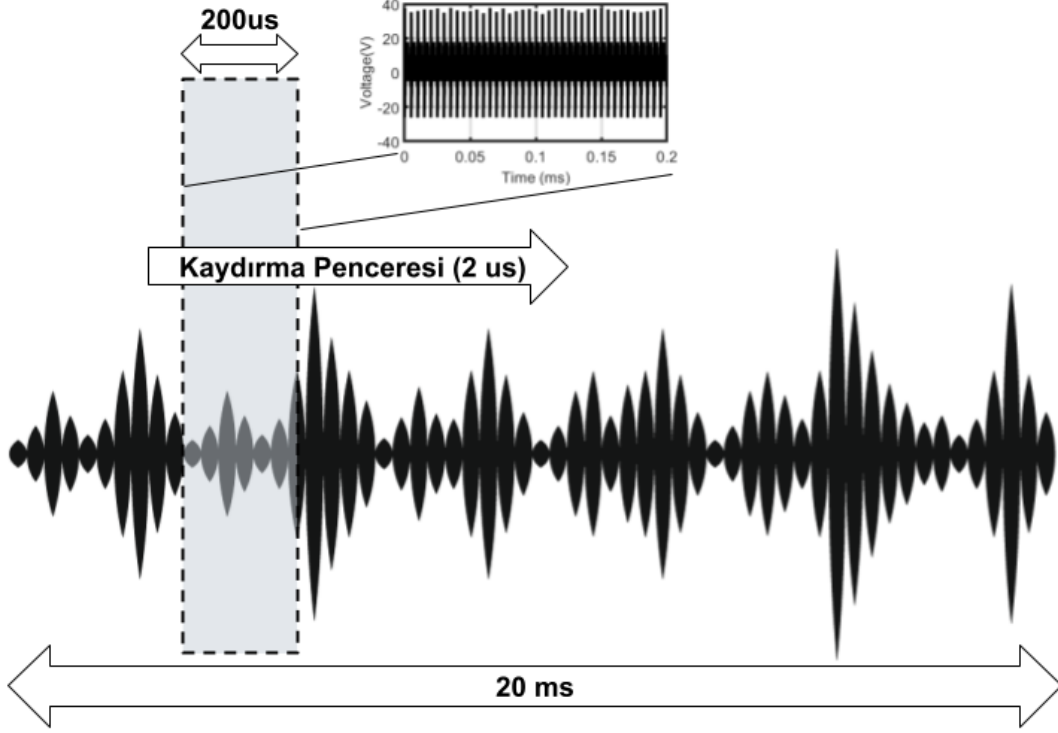
Şekil 5.6 Spice aracılığıyla elde edilen sinyalin spektrogramı

Spektrogram üzerinde elektronik sinyallerinin birbirleri arasındaki farkı bulmak için ise iki sinyalin spektrogramı arasındaki farka bakmak gerekmektedir. Bu farka bakıldığında ise Şekil 5.7 ile verilen grafik elde edilmiştir. Elde edilen spektrogram grafiğinden anlaşılabileceği gibi sadece pasif komponent toleransları göz önünden bulundurulduğu için frekans eksenindeki grafiklere benzer grafikler elde edilmiştir. Pratik uygulamada elektronik devre kartlarında daha farklı tolerans değerlerinin de oluşacağından dolayı spektrogram grafiğinde daha ayırt edici nitelikler çıkacağı ön görülmüştür.



Şekil 5.7 Spice aracılığıyla elde edilen sinyalin spektrogram farkı

Gerçekleştirilen yayılım sinyallerinin analizinden sonra, simülasyonlardan elde edilen veriler kullanılarak eğitim amaçlı bir veri seti oluşturulmuştur. Bu süreçte, beş farklı cihaz devresindeki pasif bileşenlere ideal değerlerinden sapacak şekilde rastgele %5 tolerans değerleri atanmıştır. Tolerans değerlerinin atanmasının ardından, 20 ms süreyle veri toplanmış ve Şekil 5.8 ile gösterildiği gibi segmentlere ayrılmıştır. Segmentasyon işlemi sırasında, her bir segment 200 μ s'lik çerçeveler halinde yakalanmış ve her çerçeve arasında 2 μ s'lik kayma uygulanmıştır. Beş devrede gerçekleştirilen simülasyonlar sonucunda toplam 350.000 sinyal içeren bir veri seti oluşturulmuştur.



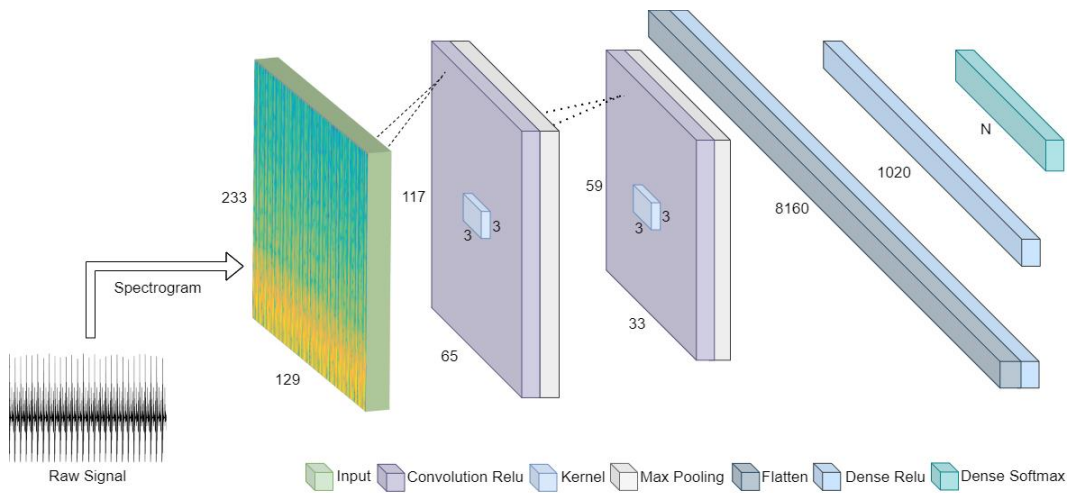
Şekil 5.8 Veri kümesi oluşturmada kullanılan veri segmentasyon yöntemi

5.1.3 Derin Öğrenme Modeli

Spektrum analizi, belirli zaman dilimlerine ayrılan sinyallerin FFT (Hızlı Fourier Dönüşümü) uygulanarak elde edilen spektrumlarının kullanımı, elektronik devrelerin her bir zaman diliminde ürettiği frekans bileşenlerini tanımlamak ve dışsal gürültüleri tespit etmek açısından büyük önem taşımaktadır. Bu nedenle, spektrum tabanlı temsil, derin öğrenme modeline girdi olarak kabul edilmiştir. Derin öğrenme modelini spektrum verisiyle eğitmek için önce uygun bir derin öğrenme mimarisi oluşturulmalıdır. Mimari seçimi, girdi-çıkı parametrelerinin yanı sıra problemin özel özellikleri ve gereksinimlerine dayanarak yapılır. Derin öğrenme alanında, CNN'ler, konvolüsyonel tekniklerden faydalandıkları için spektrumlar gibi çok boyutlu verileri analiz etme konusunda büyük başarı göstermiştir. Zaman serisi verisi gibi tek boyutlu sinyallerde daha iyi performans sergileyen LSTM, RNN ve TCN gibi diğer derin öğrenme algoritmaları, bu çalışmanın kapsamında ham sinyallerle test edilmiştir ve doğruluk sonuçlarının düşük olduğu gözlemlenmiştir. Ham sinyallerle eğitim yapabilmek için büyük

miktarda sinyal verisi gerekmekte ve eğitim sürecinde karmaşık modellerin oluşturulması gerekmektedir. Kullanılacak derin öğrenme modelinin, gömülü bir Linux cihazında çalışması gerektiğinden, modelin gömülü Linux'un sınırlı belleği göz önünde bulundurularak tasarlanması gerekmektedir. Bu sebeple, spektrum verisi kullanarak eğitim yapmak üzere bir CNN modeli inşa edilmiştir ve ardından performansı değerlendirilmiştir. Ayrıca, bellek kısıtlamaları nedeniyle, VGGNet, GoogLeNet/Inception, ResNet, DenseNet gibi karmaşık CNN modelleri yerine temel bir CNN modeli kullanılmıştır.

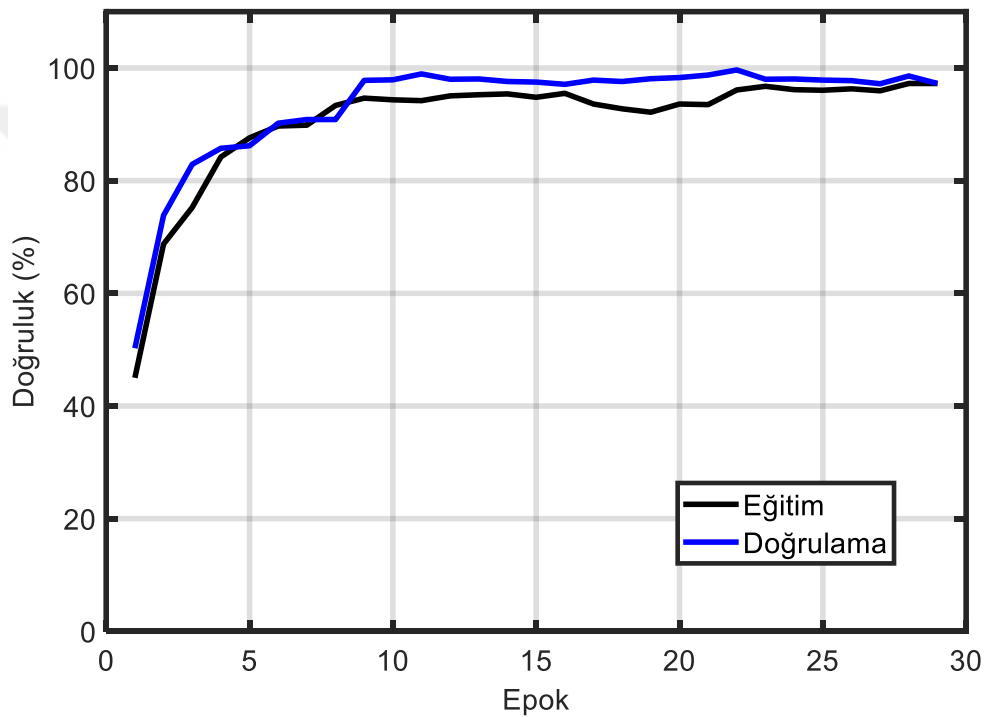
Derin öğrenme için kullanılacak CNN modelinin yapısı Şekil 5.9 ile gösterilmektedir. Kullanılan derin öğrenme modeli, spektrumları kabul edebilecek şekilde (233, 129) boyutlarında bir giriş katmanına sahiptir. Giriş katmanını takiben, (3, 3) boyutlarında iki Conv2D katmanı bulunmakta ve sonrasında bir Flatten işlemi yapılmaktadır. Flatten işleminden sonra, iki Dense katmanı eklenmiş ve çıkış katmanında SoftMax aktivasyon fonksiyonu kullanılmaktadır. SoftMax katmanının boyutu, sistemde dikkate alınacak cihaz sayısına karşılık gelmektedir. Derin öğrenme modelinde kullanılan parametreler, sistemin gereksinimlerine dayalı olarak deneme yanılma yoluyla seçilmiştir. Deneme yanılma sürecinde, gömülü GPU cihazının bellek sınırlamaları da göz önünde bulundurulmuştur. CNN modeli farklı boyutlarda tasarlanmış ve bu kısıtlamalar doğrultusunda pratik kullanım için en optimal model seçilmiştir.



Şekil 5.9 Kullanılan CNN derin öğrenme modelinin mimarisi.

5.1.4 Simülasyon Sonuçları

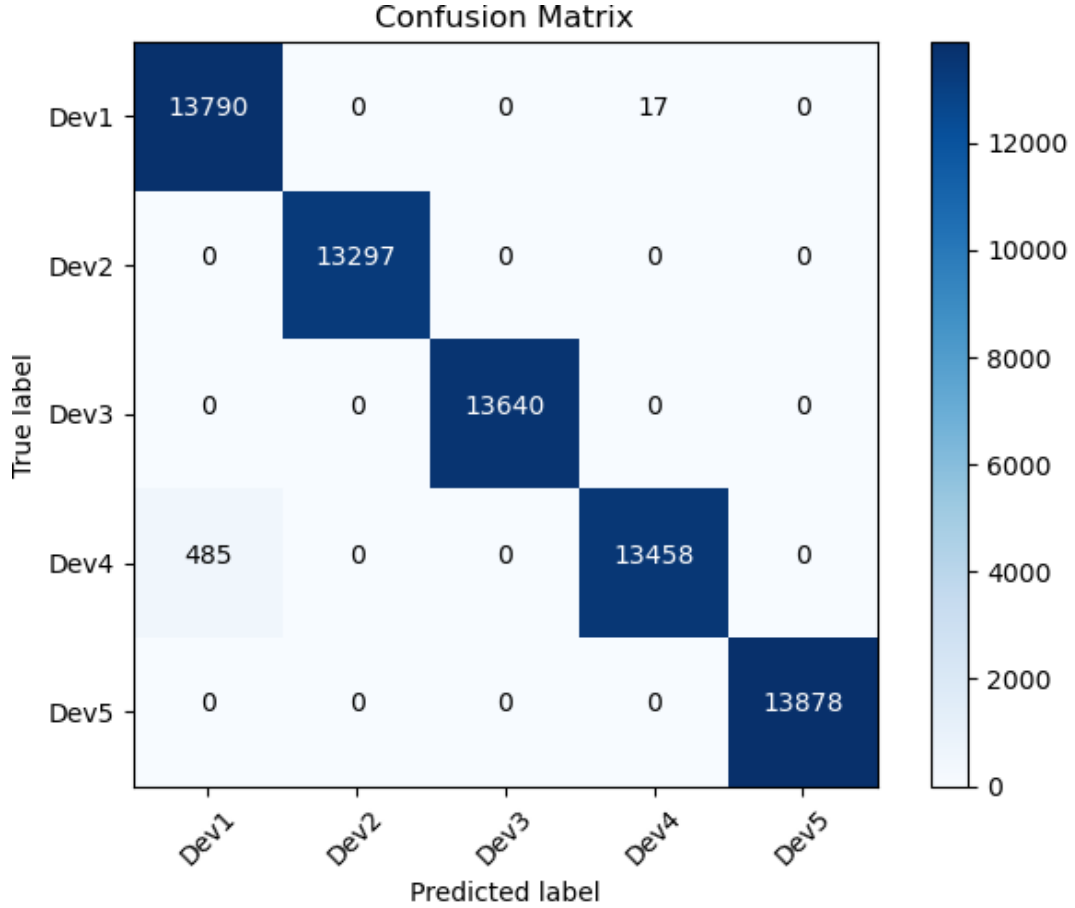
Eğitim aşamasında, ham 200 μ s sinyalin spektrogramı elde edilerek Şekil 5.9 gösterildiği gibi CNN modeline girdi olarak sağlanmıştır. Eğitim öncesinde, uygun sinyal temsillerinin oluşturulabilmesi için sinyal ön işleme teknikleri uygulanmıştır. Daha sonra, işlenmiş veriler kullanılarak derin öğrenme modeli eğitilmiştir. CNN ağı ile gerçekleştirilen eğitim süreci, Şekil 5.10 ile gösterilen epok-doğruluk eğrisinin de ortaya koyduğu üzere, %99,8 gibi yüksek bir doğruluk oranı sağlamıştır.



Şekil 5.10 Dönem sayısına göre doğruluk oranı

Eğriyi takiben, cihaz sınıflandırmasının incelenmesine olanak sağlamak amacıyla Şekil 5.11 ile gösterilen bir Karışıklık Matrisi oluşturulmuştur. Matematiksel yaklaşımlar kullanarak simülasyon verilerini elde eden derin öğrenme modeli, devre modelinin teorik çözümlerini etkili bir şekilde yaklaştırmış ve pasif bileşenlerdeki tolerans değişimlerinden kaynaklanan farklılıkları kullanarak devreleri ayırt etmiştir. Elektronik devrelerin ideal sinyaller yerine gerçek dünya davranışları açısından incelenmesi için Spice simülasyonlarında Monte Carlo

analizi gibi teknikler veya sinyal kaynağına gürültü eklenmesi gibi yöntemler uygulanabilir. Ancak, bu durumlarda dahi devre yerleşimi, birbirine bağlı elektromanyetik girişimler ve gürültü seviyelerinin kapsamlı bir analizi tam anlamıyla mümkün olmayabilir ve bu durum deneysel sonuçların elde edilmesini gerekli kılmaktadır.



Şekil 5.11 Simülasyon verilerinden elde edilen sınıflandırma sonuçlarının karışıklık matrisi.

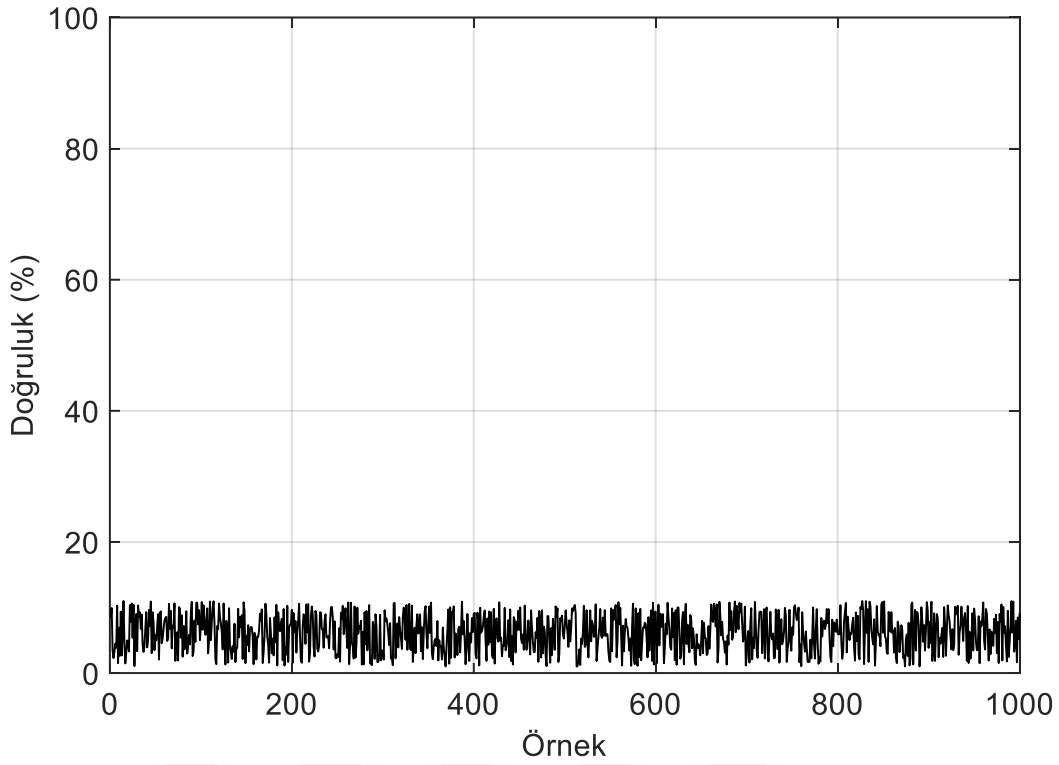
Ayrıca, derin öğrenme modelinin F1 skoru belirlenmek üzere her bir sınıf için doğruluk (precision) ve geri çağırma (recall) değerleri ayrı ayrı hesaplanmış ve sonuçlar Tablo 5.1 ile sunulmuştur. Daha sonra, F1 skorları formül (5.1) kullanılarak elde edilmiş ve ortalama F1 skoru 0,99 olarak bulunmuştur.

$$F1 = \frac{2 * Precision * Recall}{Precision + Recall} \quad (5.1)$$

Tablo 5.1 Modelinin Kesinlik, Duyarlılık ve F1 Puanı değerleri

Cihaz İsmi	Kesinlik (Precision)	Duyarlılık (Recall)	F1 Skoru
Dev 1	1.00	0.97	0.98
Dev 2	1.00	1.00	1.00
Dev 3	1.00	1.00	1.00
Dev 4	0.96	1.00	0.98
Dev 5	1.00	1.00	1.00

Sistemde tanımlı bir cihaz yerine, farklı tolerans değerlerine sahip bir devreden sinyaller alındığında ve bu sinyallerle sistemde tanımlı bir cihaz taklit edilerek sisteme sızma girişiminde bulunulduğunda, güvenlik sisteminin davranışı Şekil 5.12 ile gösterilmiştir. Bu grafikten de anlaşılacağı üzere, derin öğrenme modeli düşük bir başarı oranı sergilemiş ve bu durum, sistemin cihazı tanımadığını ve ortamda tanımlanmayan bir cihazın çalıştığını göstermektedir.



Şekil 5.12 Sistemde bir cihazı taklit eden bilinmeyen bir cihazın doğruluk oranı

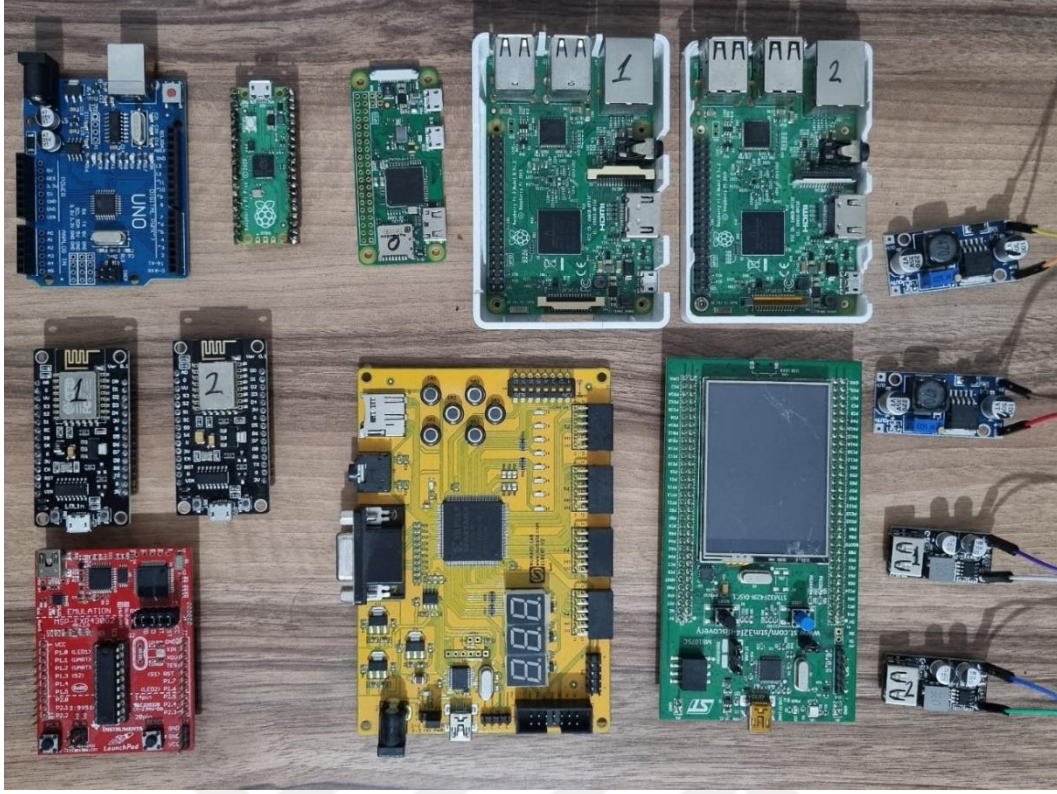
5.1.5 DeneySEL Sonuçlar

Elektronik devrelerin simülasyon tabanlı çalışmalarında, aktif bileşen özellikleri, kaynak-yük etkileşimleri, parazitler ve idealize varsayımlar, elektronik sinyallerin davranışını doğru bir şekilde yansıtmaz. Bu nedenle, önerilen sistemin çalışmasını doğrulamak ve göstermek amacıyla Şekil 5.13 ile gösterilen düzenek kurulmuştur. Bu düzenekte, güç kaynağı LISN'a (Line Impedance Stabilization Network) bağlanmış ve sinyaller, LISN'nin RF portu üzerinden Hantek 6022BE osiloskop kullanılarak alınmıştır. Alınan sinyaller, bağlı cihazların derin öğrenme modeli tarafından tanınıp tanınmadığını analiz etmek amacıyla Jetson Orin Nano (Gömülü GPU) platformunda işlenmiştir. Eğer LISN'a bağlı bir cihaz sistem tarafından tanınmazsa, cihazı devre dışı bırakmak için güç kaynağı kesilmektedir.



Şekil 5.13 İletilen Emisyon sinyalleri aracılığıyla tanımlama yapmak için oluşturulan kurulum

Sistemin cihazları tanımlayabilmesi için, cihazlardan elde edilen sinyallerle bir veri seti oluşturulması gereklidir. Bu amaçla, sisteme tanıtılacak cihazlar LISN'a bağlanmalı, cihazlar çalıştırıldıktan sonra sinyaller gömülü GPU üzerinde yakalanmalıdır. Deneysel test sonuçlarının doğrulanmasında kullanılan test düzeneği Şekil 5.13, kullanılan cihazlar ise Şekil 5.14 ile gösterilmiştir. Şekil 5.14'den görüldüğü üzere, aynı modelden iki elektronik kartın bulunduğu durumlar mevcuttur. Ayrıca, bu elektronik kartların yanı sıra bir akıllı telefon da tanımlama amacıyla kullanılmıştır.



Şekil 5.14 İletilen Emisyon sinyalleri aracılığıyla tanımlama yapmak için kullanılan cihazlar

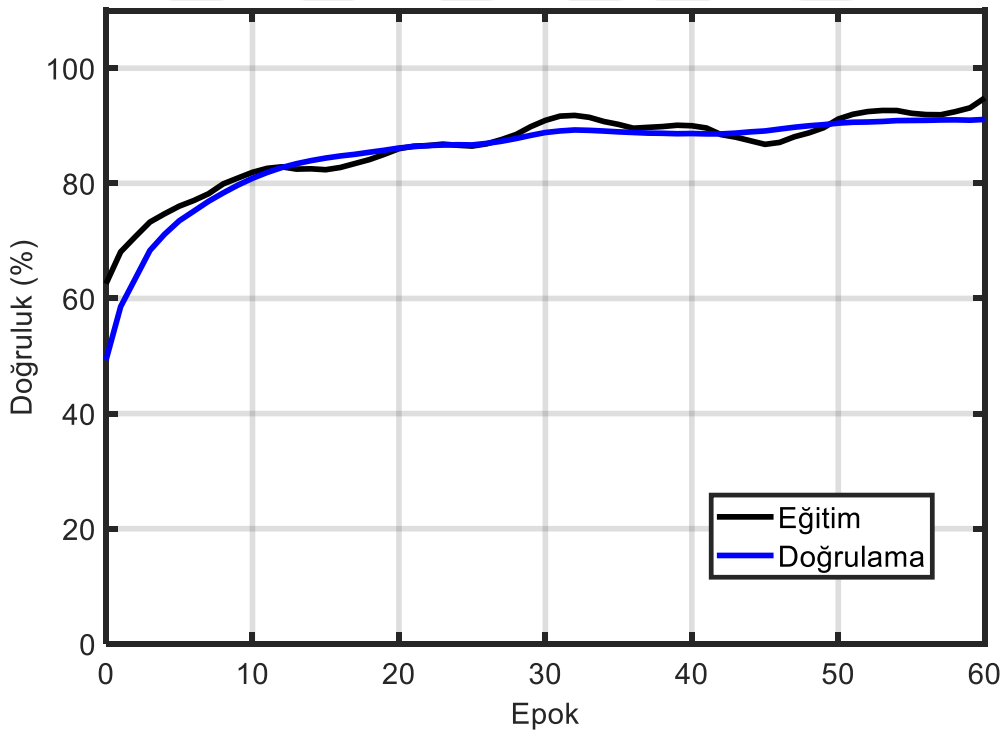
Deneyisel sonuçlar için kullanılacak cihazlar ve bu cihazların özellikleri Tablo 5.2 ile sunulmuştur. Bu tabloda, elektronik cihazlar kullanım alanlarına göre kategorize edilmiş ve kablolu/kablosuz iletişim teknolojilerine sahip olup olmadıkları belirtilmiştir. Ayrıca, cihazların güç hatlarına bağlı bir yük içerip içermediği durumu da tabloda ifade edilmiştir. Bu cihazlardan Yayılım Sinyali verisi toplamak amacıyla, LISN'ye bağlanan 8-bit Hantek 6022BE cihazı kullanılarak, 48 MSPS örnekleme hızında veri elde edilmiştir. Kullanılan LISN, 100 kHz ile 1 GHz frekans aralığında yayılım sinyalleri üretebilmektedir. Derin öğrenme modeline giriş olarak kullanılan spektrogram boyutu ve örnekleme frekansı göz önüne alındığında, spektrogramdaki frekans aralıklarının yaklaşık 100 kHz ile 24 MHz arasında olduğu tespit edilmiştir. Bu nedenle, daha yüksek örnekleme hızına sahip ADC'lerin kullanımı, özellikle yüksek frekanslarda yüksek yayılım seviyelerine sahip cihazların sınıflandırılmasında daha anlamlı bir tanımlama yapılmasını sağlayabilir ve bu durum, gelecekteki çalışmalar için önemli bir katkı sunabilir.

Tablo 5.2 Kullanılan cihazların listesi ve özellikleri

No	Cihaz İsmi	Uygulama Alanı	Kablosuz Haberleşme	Kablolu Haberleşme	Dahili Yük
1	LM2596 Boost Konvertör	Güç Devresi	-	-	-
2	LM2596 Boost Konvertör	Güç Devresi	-	-	-
3	HW-298 Şarj Cihazı	Güç Devresi	-	-	-
4	HW-298 Şarj Cihazı	Güç Devresi	-	-	-
5	ESP32	Mikroişlemci	+	+	+
6	ESP32	Mikroişlemci	+	+	+
7	Honor 9 Lite Telefon	Akıllı Telefon	+	+	+
8	MSP430G2553	Mikroişlemci	-	+	+
9	Raspberry Zero	Mikroişlemci	+	+	+
10	Raspberry 3	Gömülü Linux	+	+	+
11	Raspberry 3	Gömülü Linux	+	+	+
12	Raspberry Pico	Mikroişlemci	-	+	+
13	Spartan 3A	FPGA	+	+	+
14	STM32F429	Mikroişlemci	-	+	+
15	Arduino Uno	Mikroişlemci	-	+	+

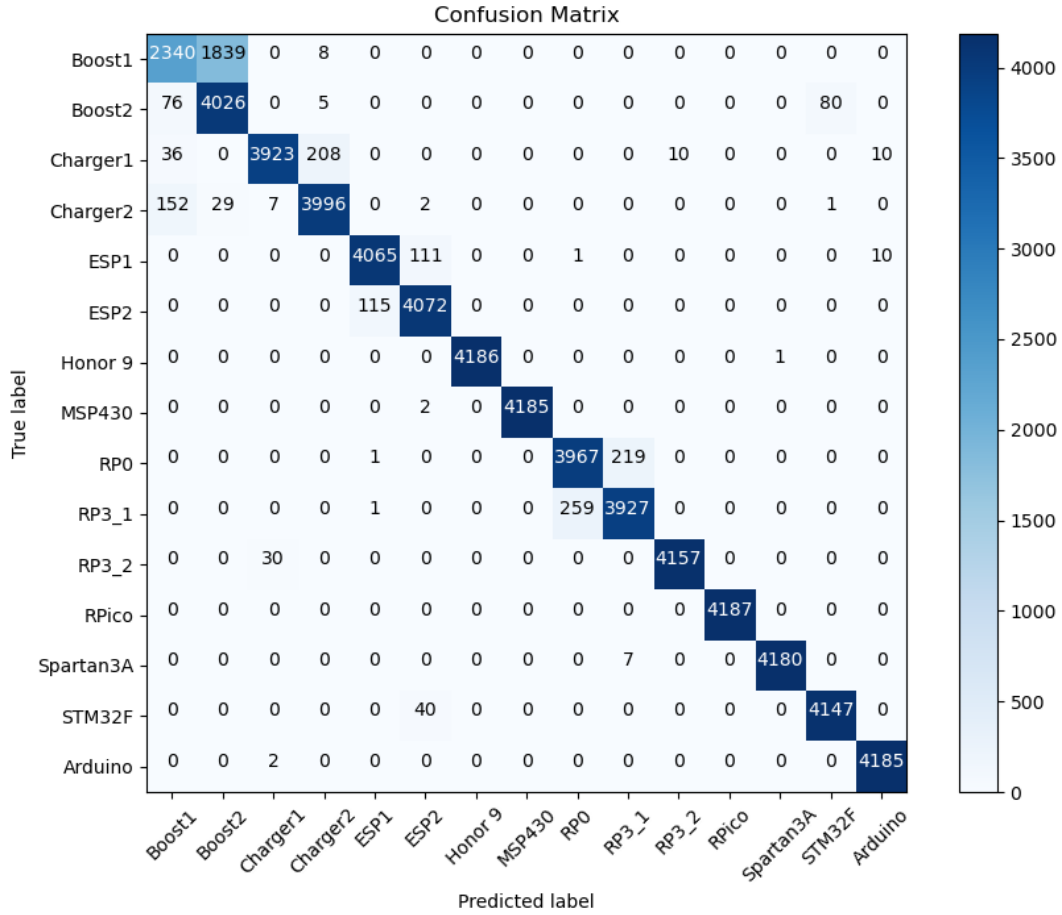
Bu cihazlardan elde edilen veri seti, 5 GB boyutunda olup toplamda 1.256.000 sinyale kadar veri içermektedir. Tanımlama sisteminde, farklı tür ve modeldeki ürünlerin ayırt edilmesi, sinyal seviyelerindeki farklılıklar aracılığıyla kolaylıkla tespit edilebilmektedir. Ancak, aynı marka ve modele ait elektronik devrelerin ayrıştırılması, elektronik bileşenler ve devre yollarındaki tolerans değerlerindeki farklılıkların kullanılmasıyla mümkün olmaktadır. Bu nedenle, veri setinin toplanmasının ardından bir derin öğrenme modelinin eğitilmesi gerekmekte ve cihazlar, modelin içerisinde yer alan katsayılar aracılığıyla birbirinden ayrıştırılmalıdır.

Veri seti toplandıktan sonra, cihazların farklılaştırılması için derin öğrenme kullanılarak eğitilmesi gerekmektedir. Bu amaçla, veri seti Şekil 5.15 ile gösterildiği gibi bir derin öğrenme modelini eğitmek için kullanılmıştır. Eğitim sürecinin ardından elde edilen epok-doğruluk eğrisi, Şekil 5.15’de sunulmuş olup, modelin %95,2 doğruluk oranına ulaştığını göstermektedir.



Şekil 5.15 Dönem sayısına göre doğruluk oranı

Cihazların sınıflandırma hatalarının analizi, Şekil 5.16'da gösterildiği gibi bir Karışıklık Matrisi oluşturularak gerçekleştirilmiştir. Görüldüğü üzere, özellikle iki aynı tür Boost Konvertörün tanımlanmasında doğruluk oranı düşüktür. Bunun nedeni, kullanılan Boost Konvertörlere bağlı bir yük bulunmaması ve bunun sonucunda çok düşük Yayılım Sinyali seviyelerinin elde edilmesidir; ayrıca 8-bit ADC ile cihazın elektronik karakteristiğinin alınamamasıdır.

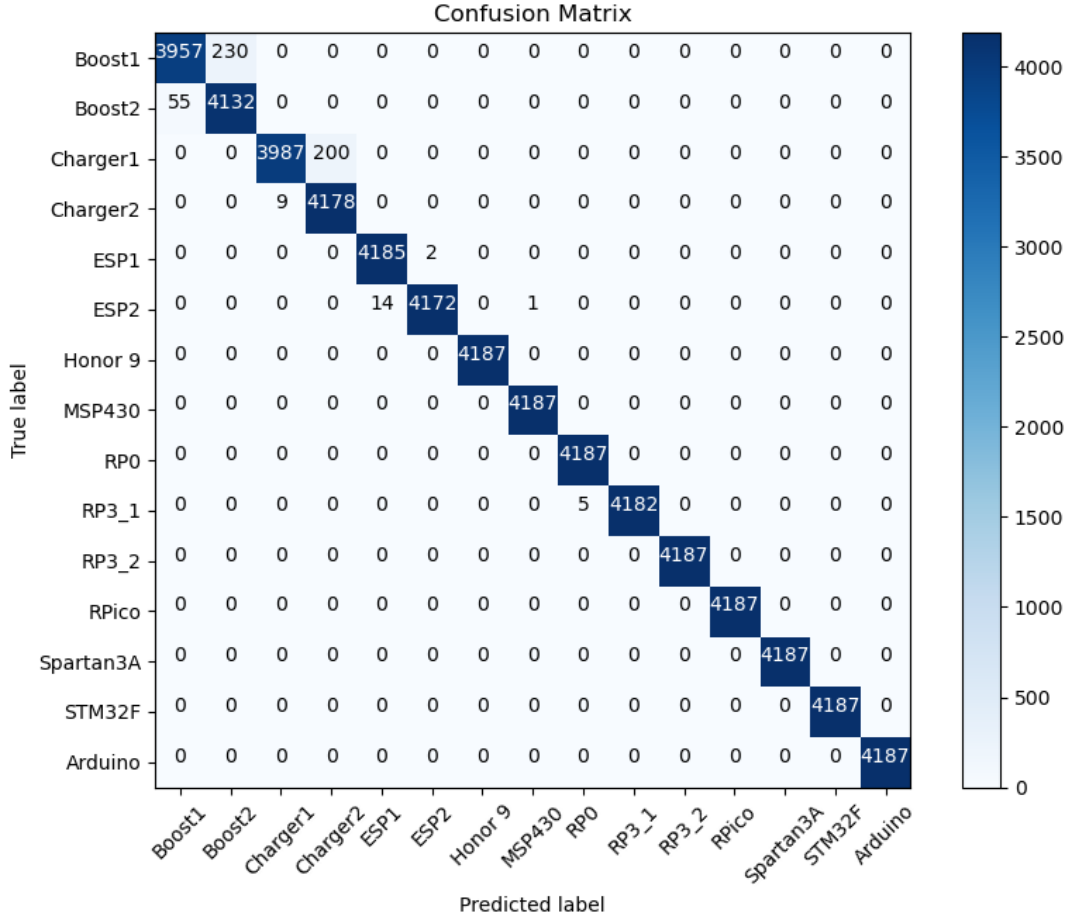


Şekil 5.16 Deneysel verilerden elde edilen sınıflandırma sonuçlarının karışıklık matrisi.

Güç elektroniği cihazları, pratik uygulamalarda boşa çalışma koşullarında çalıştırılmadığından, bağlı bir yükte test edilmeleri gerekmektedir. Güç elektroniği cihazlarına yük bağlanarak sistem testlerinin yapılması önemlidir, çünkü bu cihazlar boşa çalışma koşullarında çalışacak şekilde tasarlanmamıştır ve böyle bir durumda bile sistem üzerinde bir etki yapmazlar. Boost Konvertörler, anahtarlama süreçleri sırasında yayılım sinyalleri üretir ve eğer Boost Konvertörler bir yük

bağlı değilse, akım yalnızca kaçak akımlar ile sınırlı olduğundan, yayılım seviyeleri önemli ölçüde düşer. Boşta çalışma koşullarında yüksek hassasiyetli ölçümler yapmak, çok daha yüksek çözünürlüklü ADC'lerin kullanılmasını gerektirir. Ancak, güç devrelerinin boşta senaryolarında ihmal edilebilir bir etkisi olduğundan, bu çalışma yük bağlı durumlara odaklanmaktadır.

Bu nedenle, kullanılan Boost Konvertörlerin nominal çalışma koşulları göz önünde bulundurularak, 5V çıkış modunda ayarlandığında, 50 Ohm'luk dirençli bir yük bağlanmış ve veriler tekrar toplanmıştır. Ardından, bu veriler kullanılarak aynı derin öğrenme modeli eğitilmiş ve elde edilen Karışıklık Matrisi yapısı Şekil 5.17 ile gösterilmiştir. Elde edilen sonuçlara göre, eğitim süreci başarıyla tamamlanmış ve ortalama doğruluk oranı %99,8 olarak bulunmuştur. Cihaza göre en düşük ortalama doğruluk oranı ise %94,1 olarak tespit edilmiştir. Sistem, güvenlik testlerini yalnızca bireysel sinyaller üzerinden değil, aynı zamanda elde edilen sinyalleri bölgelere ayırarak da gerçekleştirmektedir. Bu yaklaşım, sistemin, gürültülü koşullarda alınan sinyallerin veya doğru tahmin edilemeyen sinyallerin etkisini azaltmasına olanak sağlar. Bu tür sinyalleri doğrudan güvenlik tehdidi olarak değerlendirmek yerine, sistem sinyal parçalarının ortalamasını dikkate alır. Bu metodoloji, sinyallerin gürültü veya öngörülemezlik nedeniyle bozulabileceği senaryolarda bile güvenliği sağlama konusunda sistemin başarılı olduğunu göstermektedir.



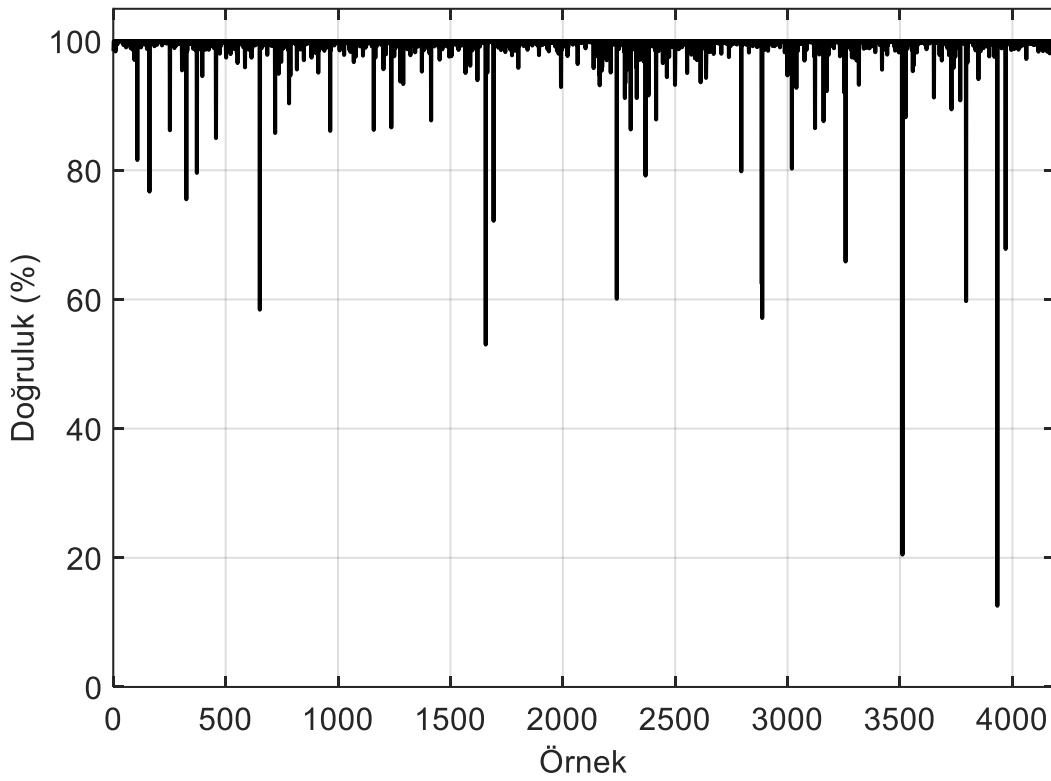
Şekil 5.17 Deneyisel verilerden elde edilen sınıflandırma sonuçlarının, Boost Konvertörler için uygulanan iç yük ile ilgili karışıklık matrisi.

Derin öğrenme modelinin F1 skorunu belirlemek amacıyla, doğruluk (precision) ve geri çağırma (recall) değerleri her bir sınıf için ayrı ayrı hesaplanmış ve sonuçlar Tablo 5.3 ile sunulmuştur. Daha sonra, F1 skorları formül (5.1) kullanılarak elde edilmiştir. Elde edilen değerlerin ortalaması, boşta çalışma koşulunda 0,94 ve yüklü koşulda ise 0,99 F1 skoru sonucunu vermiştir.

Tablo 5.3 Modelinin Kesinlik, Duyarlılık ve F1 Puanı değerleri

No	Cihaz İsmi	Yük Mevcut Değil			Yük Mevcut		
		Kesinlik	Duyarlılık	F1 Skoru	Kesinlik	Duyarlılık	F1 Skoru
1	LM2596 Boost Konvertör	0.56	0.90	0.69	0.95	0.99	0.97
2	LM2596 Boost Konvertör	0.96	0.68	0.80	0.99	0.95	0.97
3	HW-298 Şarj Cihazı	0.94	0.99	0.96	0.95	1.00	0.97
4	HW-298 Şarj Cihazı	0.95	0.95	0.95	1.00	0.95	0.98
5	ESP32	0.97	0.97	0.97	0.99	1.00	1.00
6	ESP32	0.97	0.96	0.97	1.00	1.00	1.00
7	Honor 9 Lite Telefon	1.00	1.00	1.00	1.00	1.00	1.00
8	MSP430G2553	1.00	1.00	1.00	1.00	1.00	1.00
9	Raspberry Zero	0.95	0.94	0.94	1.00	1.00	1.00
10	Raspberry 3	0.94	0.95	0.94	1.00	1.00	1.00
11	Raspberry 3	0.99	1.00	1.00	1.00	1.00	1.00
12	Raspberry Pico	1.00	1.00	1.00	1.00	1.00	1.00
13	Spartan 3A	1.00	1.00	1.00	1.00	1.00	1.00
14	STM32F429	0.99	0.98	0.99	1.00	1.00	1.00
15	Arduino Uno	1.00	1.00	1.00	1.00	1.00	1.00

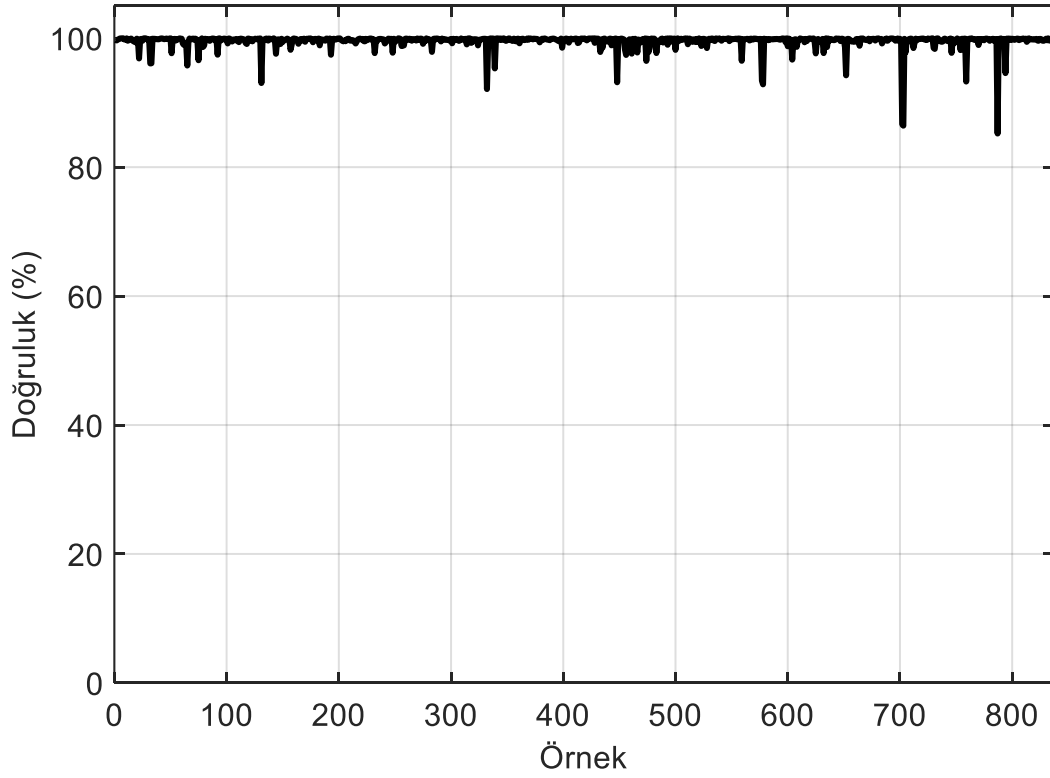
Geliştirilen derin öğrenme modelinin gerçek zamanlı işlevselliğini değerlendirmek amacıyla, sistemdeki belirtilen Boost Konvertör 1 cihazı için bir gün boyunca düzenli aralıklarla elde edilen sinyaller analiz edilerek güvenlik durumu araştırılmış ve sonuçlar Şekil 5.18 ile gösterilmiştir. Özellikle, modelin etkinliği, belirli sinyal örneklerine yanıt olarak performans değişiklikleri göstermiştir; bu değişiklikler, sinyal kalitesindeki dalgalanmalara bağlanmıştır. Bu farklılıklara rağmen, cihazın güvenliğini onaylayan yaklaşık %99,54 oranında bir genel başarı oranı elde edilmiştir. Sonuç olarak, önerilen sistemin güvenlik odaklı ortamlar ve sistemler için pratik uygulanabilirliği doğrulanmıştır.



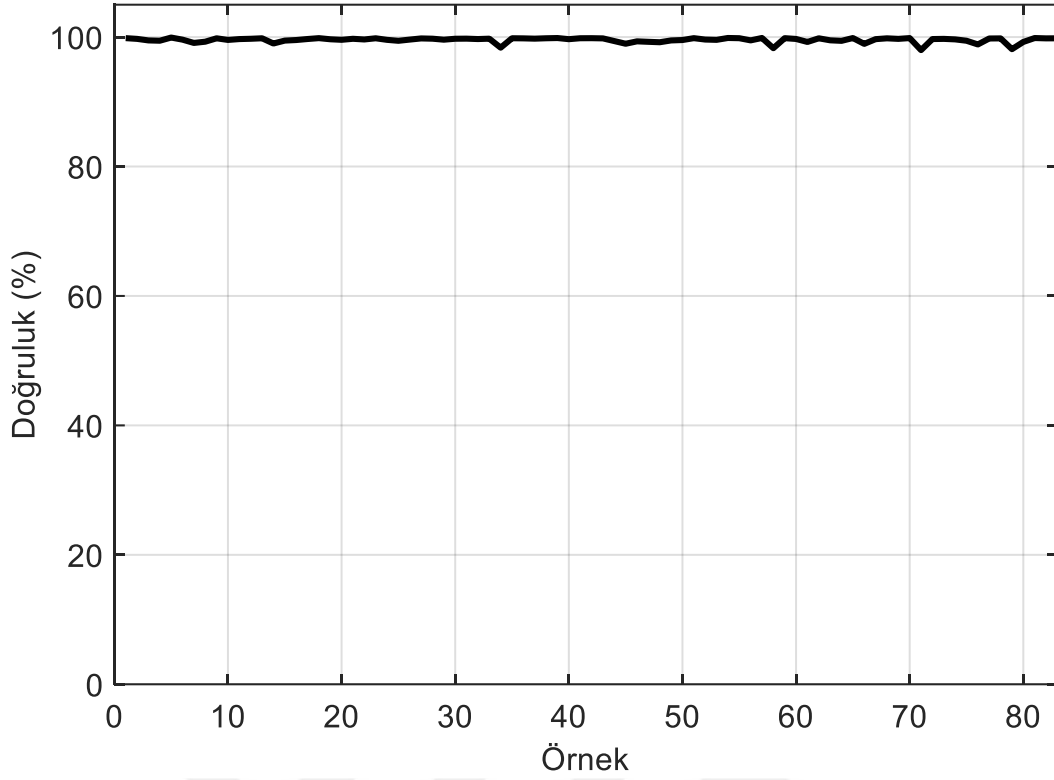
Şekil 5.18 Gün içerisinde belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla cihaz kimliğini tahmin etmedeki doğruluk oranı.

Güvenlik kontrolünün sağlanmasında, yalnızca tek bir veriye dayanılarak yapılan değerlendirmelerde zaman zaman hataların meydana gelebileceği açıkça görülmektedir, bu durum Şekil 5.18 ile gösterilmektedir. Cihazların elektronik özellikleri nedeniyle, normal durumlarından farklı sinyaller üretebilirler ve bazen kaotik davranışlar sergileyebilirler. Bu tür sinyaller, doğrudan matematiksel

modelleme ile tanımlanamayacak, benzersiz ve öngörülemez özelliklere sahip sinyallerdir. Sonuç olarak, güvenlik kontrollerinde, tek bir sonuca dayanmak yerine belirli sayıda sonucun ortalamasını dikkate almanın daha avantajlı olacağı değerlendirilmiştir. Bu nedenle, sistemi 5 ve 50 tanımlama doğruluğu sonuçlarının ortalamasını alarak test ettiğimizde, sırasıyla Şekil 5.19 ve Şekil 5.20 ile elde edilmiştir.



Şekil 5.19 Bir gün boyunca belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla 5 verinin ortalaması alınarak cihaz kimliğini tahmin etmedeki doğruluk oranı



Şekil 5.20 Bir gün boyunca belirli zaman aralıklarında toplanan emisyon sinyalleri aracılığıyla 50 verinin ortalaması alınarak cihaz kimliğini tahmin etmedeki doğruluk oranı

Derin öğrenme kapsamında kullanılan model, $200\mu\text{s}$ sinyal verisi ile beslenmektedir ve sistem, ortalama olarak test edildiğinde, 5 sinyal için 1ms, 50 sinyal için ise 10ms veri gerekmektedir. Sistemin istenen maksimum gecikmeyi karşılayacak şekilde ayarlanarak sistem kararlılığı sağlandığında, bu yöntem, kritik ortamlarda ve sistemlerde elektronik cihazlar ile bilgisayarların güvenliğini sağlamak için önerilmektedir. Sonuç olarak, iletişim sistemi bulunmasa bile, geleneksel tanımlama yöntemlerine kıyasla çevredeki cihazların güvenli bir şekilde tanımlanmasını sağlar ve böylece güvenlik alanına yenilikçi bir yaklaşım sunar.

5.2 Havadan Yayılan Elektromanyetik Sinyal ile Kimliklendirme

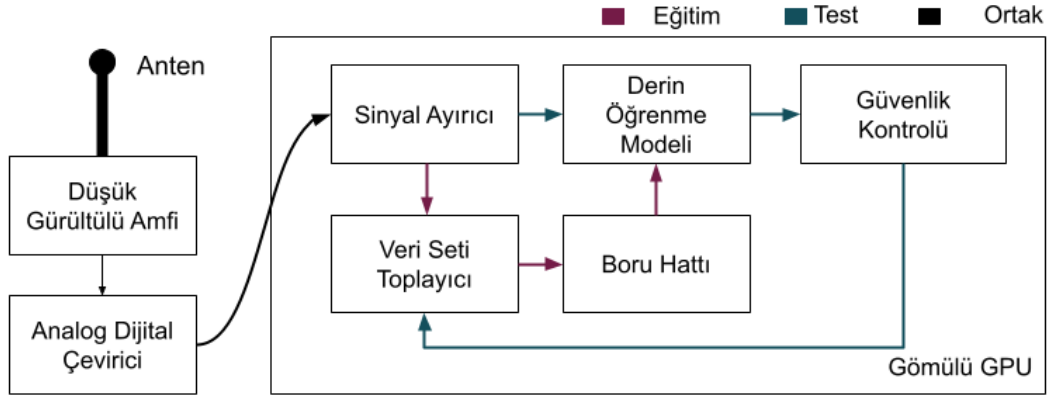
Havadan elektromanyetik emisyon, bir cihazın çalışması sırasında etrafına yaydığı elektromanyetik dalgalardır. Elektronik devrelerdeki akımlar ve voltajlar sonucunda oluşan bu emisyonlar, cihazın dışına yayılır ve özellikle cihazın etrafında bir elektromanyetik alan oluşturur. Her cihazın elektromanyetik emisyonları kendine özgü bir frekans, genlik ve faz özelliği taşımaktadır. Bu bilgi, cihazların güvenlik ve kimliklendirme gibi alanlarda sınıflandırılması ve taklit edilemez bir yapıya kavuşturulması için kullanılabilir.

Yakın alan problemleri, cihazların çevresindeki elektromanyetik alanları ölçmek için kullanılan hassas algılayıcılardır. Genellikle milimetre düzeyinde ölçüm hassasiyetine sahip olan bu problemler, cihazların dışına yayılan elektromanyetik sinyalleri alır ve bu sinyalleri analiz edebilmek için dijital sinyallere dönüştürür. Bu sayede, her cihazın kendine özgü bir "parmak izi" gibi düşünülebilecek sinyal karakteristikleri belirlenebilir.

Yakın alan problemleri ile elde edilen sinyaller, özellikle güvenlik araştırmalarında cihazların taklit edilme veya izinsiz kullanımlara karşı korunmasında önemli bir yer tutar. Çünkü cihazların ürettikleri bu özgün elektromanyetik emisyonlar, diğer cihazlardan kolaylıkla ayırt edilebilmelerini sağlar.

5.2.1 Önerilen Tasarım

Elde edilen sinyaller kullanılarak cihaz kimliklendirmesi ve sonrasında güvenlik kontrolleri için önerilen tasarım Şekil 5.21 ile gösterilmektedir. Anten tarafından yakalanan sinyal, bir amplifikatör aracılığıyla güçlendirilir ve ardından bir ADC ile işlenir. ADC tarafından örneklenen sinyaller, gömülü bir GPU'ya aktarılır. CUDA çekirdekleri ile donatılmış olan bu gömülü GPU hem eğitim hem de işleme görevlerini hızlandırmak için kullanılır ve internet bağlantısı gerektirmeden yerel olarak çalışacak şekilde tasarlanmıştır. Gömülü GPU tarafından işlenen sinyallerin iki ana işlevi bulunmaktadır. Birincisi, elde edilen sinyallerden bir veri seti oluşturmak ve bu veri setini derin öğrenme modelini eğitmek için kullanmaktır. İkincisi ise, eğitilen derin öğrenme modelini kullanarak cihaz kimliklerini test etmek ve güvenlik kontrollerini sağlamaktır.



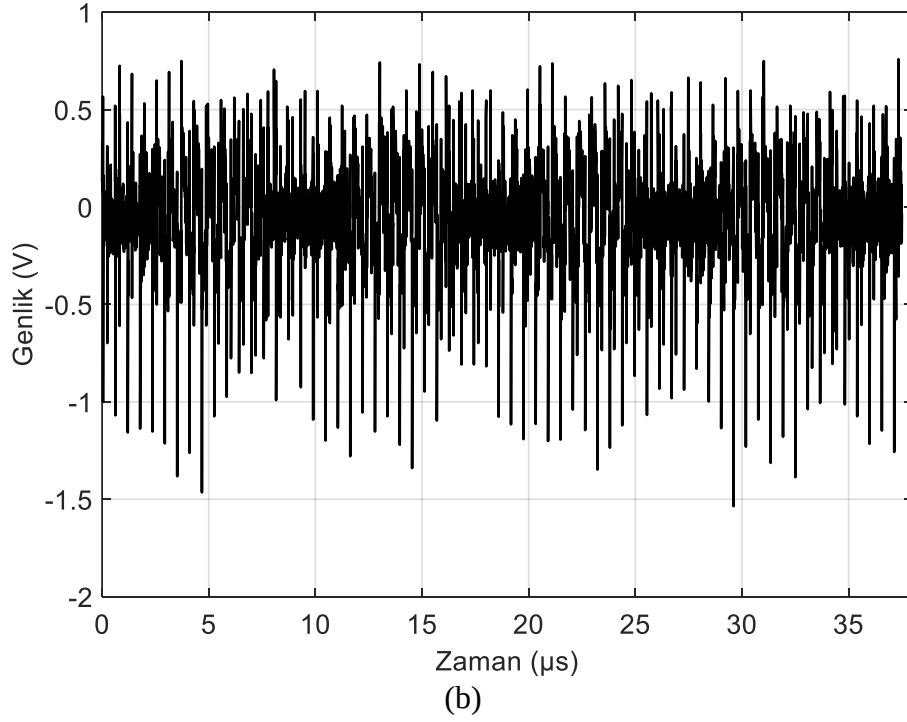
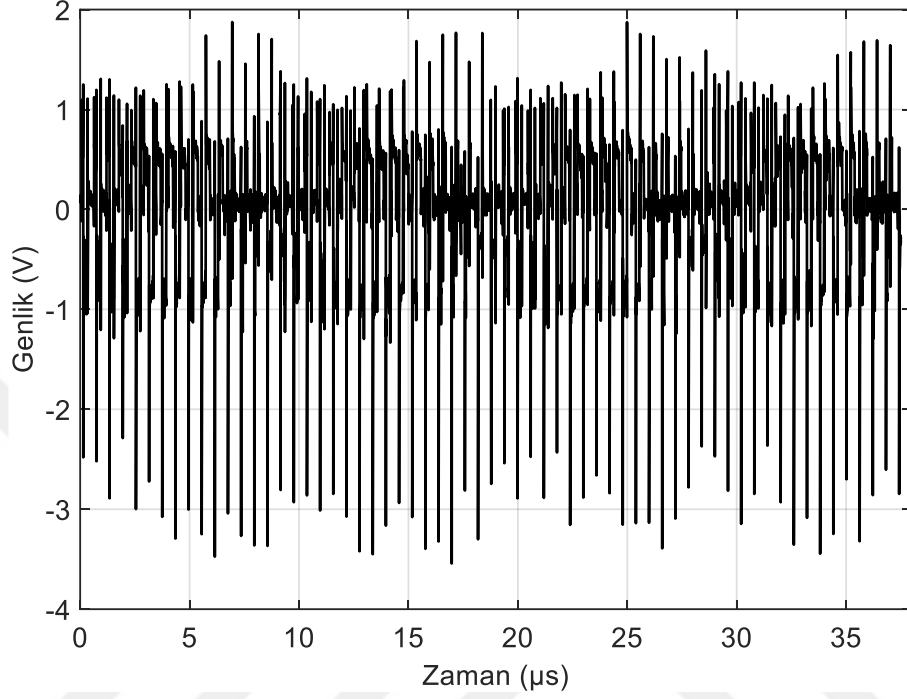
Şekil 5.21 Yakın alan problemleri ile cihazların kimliklendirilmesi için oluşturulmuş sistemin mimarisi

5.2.2 Veri Setinin Oluşturulması

Elektromanyetik sinyalleri kullanarak bir model eğitmek amacıyla öncelikle verilerin toplanması ve bir veri setinin oluşturulması gerekmektedir. Başlangıçta, veri toplama işlemi için 48 MSPS, 8-bit çözünürlükte bir ADC kullanılmıştır. Ancak deneysel testler sırasında bu ADC'nin yeterli olmadığı ve yeterince detaylı veri sunmadığı belirlenmiştir. Bu nedenle, 100 MSPS ile 800 MSPS arasında değişen örnekleme hızına ve 12 bit çözünürlüğe sahip bir ADC kullanılarak çeşitli veri setleri üretilmiştir. Bu veri setleri, hangi örnekleme hızlarının yeterli detay sağladığını ve eğitim sürecinde kararlılığı temin ettiğini belirlemek amacıyla örnekleme hızları değiştirilerek oluşturulmuştur. Toplanan verilerin boyutu, arayüz üzerinden seçilebilmekte olup, veri görüntüleme ve kayıt boyutları için ayrı seçenekler bulunmaktadır. Veri toplama sırasında, kayıt başlatıldıktan sonra, ölçümler yakın alan probu kullanılarak yapılmış, özellikle cihazın güç bağlantı noktaları üzerinde gerçekleştirilmiştir. Bu noktalar üzerinde ölçüm yapılmasının nedeni, akım dalgalanmalarının bu alanlarda daha belirgin olma eğiliminde olmasıdır; bu durum daha güçlü ve tespit edilebilir manyetik alan ölçümlerine yol açmaktadır.

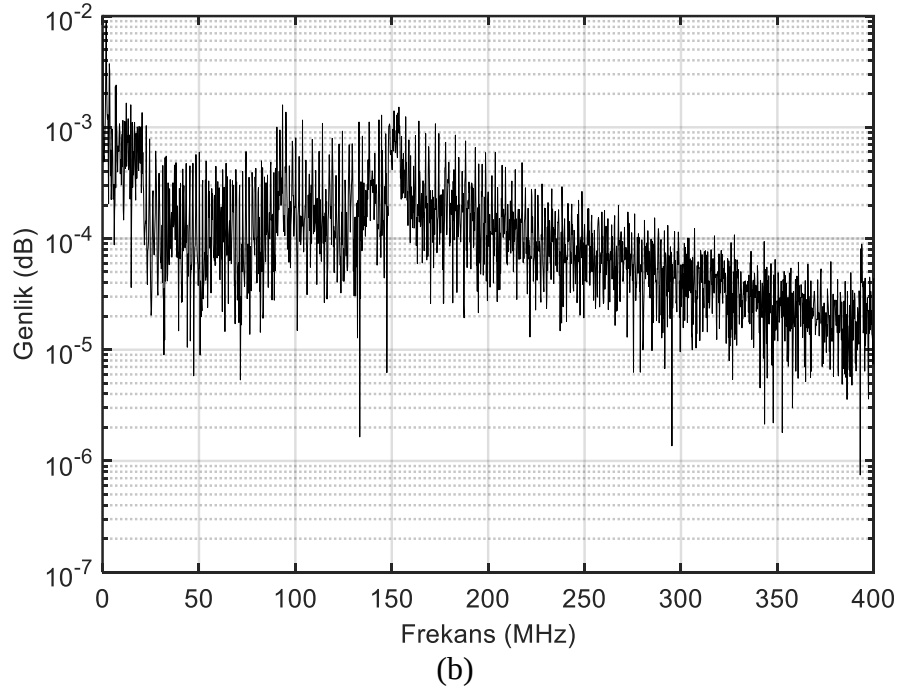
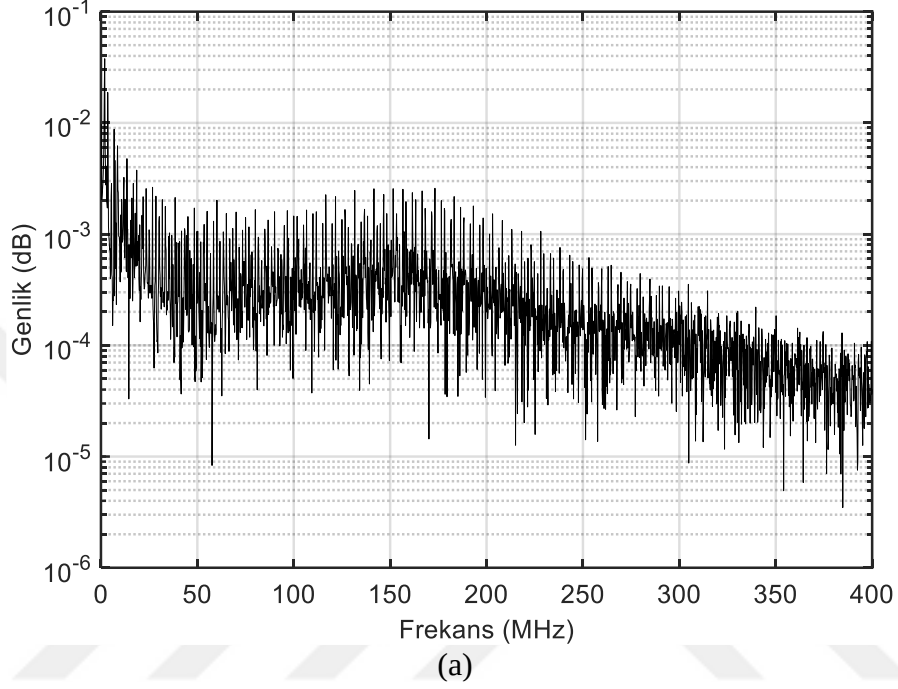
Veri toplama süreci boyunca elde edilen veriler, geliştirilecek derin öğrenme modelinin mimarisini belirlemek amacıyla da analiz edilmiştir. Örneğin, Şekil 5.22 (a) ve Şekil 5.22 (b)'de gösterildiği üzere, donanım ve yazılım açısından aynı olan iki farklı Raspberry Pi 3B geliştirme kartından manyetik alan ölçümleri

alınmıştır. Ölçüm, toplamda tek bir konumdan 30,000 veri noktası içeren 800 MSPS örnekleme hızında gerçekleştirilmiştir. Sonuç olarak, toplanan veriler, 26.6 kHz ile 400 MHz arasındaki frekans bandında değerleri temsil etme kapasitesine sahiptir.



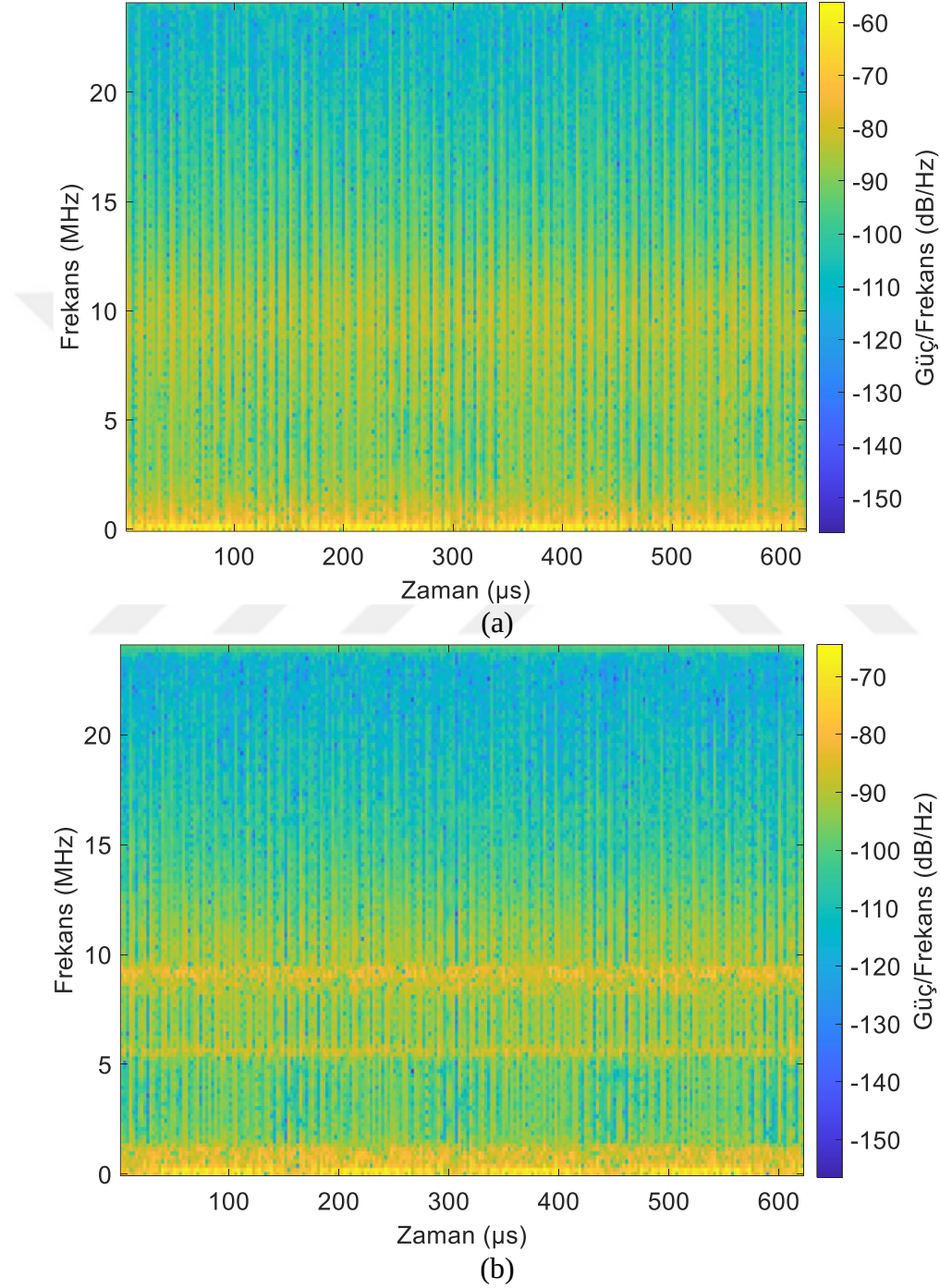
Şekil 5.22 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucu.

Ölçümler, sinyallerin FFT (Hızlı Fourier Dönüşümü) analizi yapılarak incelenmiş ve frekans domeni Şekil 5.23 (a) ve Şekil 5.23 (b) gösterildiği gibi değerlendirilmiştir. Bu analizden görülebileceği üzere, donanım ve yazılım aynı olsa bile, elektronik bileşenler toleransları ve birbirleriyle etkileşimleri nedeniyle farklı frekansta salınımlar yapabilmektedir.



Şekil 5.23 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucunun FFT dönüşümü.

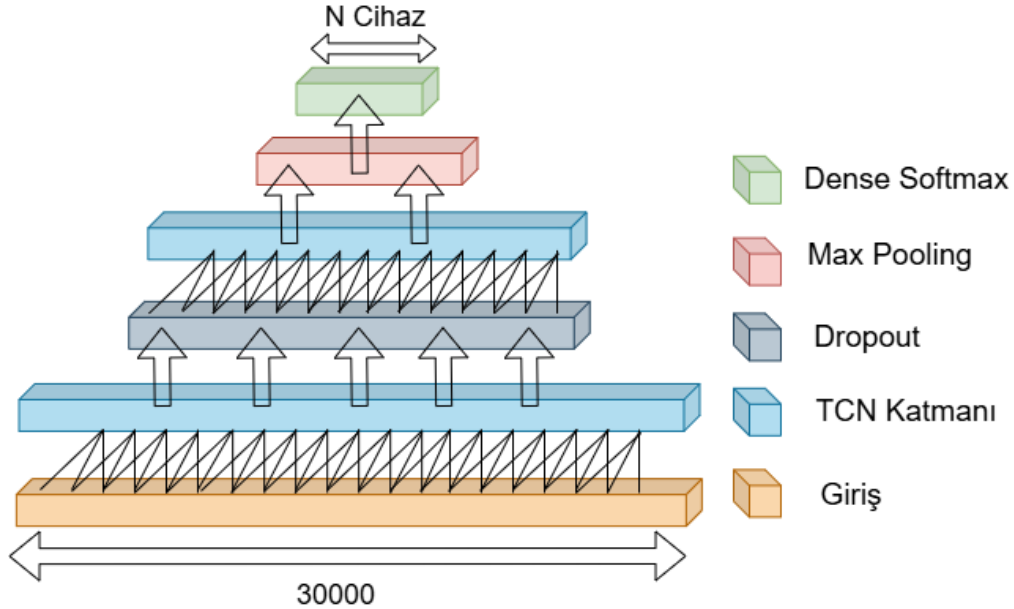
Ayrıca, Şekil 5.24 ile gösterildiği üzere, her iki sistem için zamanla değişen frekans varyasyonlarını göstermek amacıyla spektrogram analizleri gerçekleştirilmiştir. Gözlemlendiği gibi, zamanla değişen frekans kaymaları her cihaz için belirgin olup, görsel olarak ayırt edilebilmektedir. Ayrıca farklı cihazlardan alınmış sinyallerle oluşturulan spektrogramlar Ek A ile verilmiştir.



Şekil 5.24 İki farklı Raspberry pi 3 cihazlarından alınan manyetik alan ölçüm sonucunun spektrogram dönüşümü.

5.2.3 Derin Öğrenme Modeli

Derin öğrenme modeli eğitmek için elde edilen veri kümelerini kullanmadan önce, derin öğrenme modelini inşa etmek gerekmektedir. Bir derin öğrenme modeli, bir giriş katmanı, bir çıkış katmanı ve gizli katmanlardan oluşur. Önerilen çalışmada, manyetik alan ölçümlerinin zaman serisi doğası nedeniyle literatürde de başarısı bilinen TCN kullanılmıştır. Bu çalışmada, verinin zaman serisi olarak işlenmesi ve gelecekteki verilere erişime ihtiyaç duymadan çalışacak şekilde tasarlanması nedeniyle TCN tercih edilmiştir. Kullanılan derin öğrenme modelinin yapısı ise Şekil 5.25 ile sunulmaktadır. Görüldüğü üzere, giriş katmanından gelen zaman serisi sinyali, öncelikle TCN katmanlarından geçmekte, ardından aşırı öğrenmeyi önlemek amacıyla bir dropout katmanı uygulanmaktadır. Sonraki adımda bir başka TCN katmanı daha eklenmiş ve önemli özellikleri vurgulamak amacıyla zaman serisindeki en yüksek aktivasyon değerini çıkaran Global Max Pooling işlemi uygulanmıştır. Modelin son katmanı, cihaz sayısına eşit boyutlarda Dense katmanından oluşmakta ve SoftMax aktivasyon fonksiyonu kullanılmaktadır. Ek olarak, modelin verinin genliğinden ziyade dalga formunu öğrenebilmesini sağlamak için, her ölçüm modele girilmeden önce normalize edilmiştir.



Şekil 5.25 Önerilen tasarım mimarisi içerisinde geliştirilen TCN modeli.

5.2.4 Deneyisel Sonuçlar

Önerilen sistemin deneyisel testleri için, Şekil 5.26 ile verilen kurulum kullanılmıştır. 9 kHz ile 6 GHz aralığında sinyalleri ölçebilen, 20 mm'lik bir manyetik alan probu, yakın alan probu olarak kullanılmıştır. Bu kurulumda, sistem, manyetik probdan ADS5408 ADC aracılığıyla sinyalleri alır ve bu sinyaller TSW1400EVM yakalama kartında depolanır. TSW1400EVM kartı, bir FPGA içerir ve bu sayede sinyal alımı ve dijital iletişim bu kart üzerinden sağlanır. Dijital ortam olarak standart bir bilgisayar kullanılabilse de bu amaçla özel yazılımlarla birlikte Jetson Kitlerinin kullanımı da mümkündür.



Şekil 5.26 Önerilen sistemin uygulamasını test etmek için oluşturulmuş düzenek.

Derin öğrenme modeli geliştirildikten sonra, bir ay boyunca günlük olarak ölçümler alınarak sistemin testleri gerçekleştirilmiştir. Elde edilen sonuçlara göre, sistem 100 MSPS ve 800 MSPS örnekleme hızlarında cihazları başarılı bir şekilde tanımlamıştır. Eğitim tarihinden tam bir ay sonra gerçekleştirilen bir test, her iki örnekleme hızı için de Şekil 5.27 ile verilmiş olan aynı Karmaşıklık Matrisi elde edilmiştir. Bu durum, sistemin gürültüsüz ve ideal koşullar altında her iki

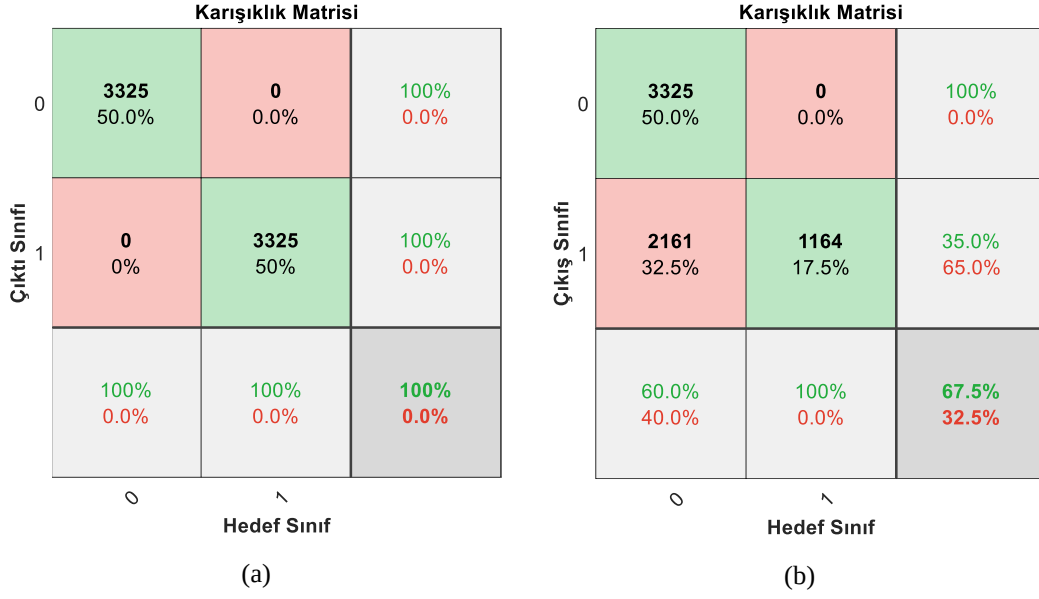
örnekleme hızında da cihazları tutarlı ve yüksek doğrulukla sınıflandırabildiğine işaret etmektedir.

Karışıklık Matrisi

	0	1	
0	3325 50.0%	0 0.0%	100% 0.0%
1	0 0%	3325 50%	100% 0.0%
	100% 0.0%	100% 0.0%	100% 0.0%
	0	1	
	Hedef Sınıf		
	Çıktı Sınıfı		

Şekil 5.27 Raspberry Pi cihazlarının kimlik doğrulama testinden elde edilen Karmaşıklık Matrisi

Aynı yazılıma sahip Raspberry Pi 3 cihazlarının bir aylık süre boyunca başarılı bir şekilde tanımlanabildiği doğrulandıktan sonra, CPU test aracı [123] kullanılarak yüksek akım çekimini tetiklemek amacıyla bir sistem stres testi sırasında ek ölçümler alınmıştır. Bu ölçümler, derin öğrenme modelinin yeniden test edilmesinde kullanılmış ve 100 MSPS ile toplanan veriler için Şekil 5.28 (a) ve 800 MSPS ile toplanan veriler için Şekil 5.28 (b)'de gösterilen Karmaşıklık Matrisleri oluşturulmuştur. Gözlemlendiği üzere, 100 MSPS hızında eğitilmiş derin öğrenme modeli, yüksek akım çekimi koşullarında dahi dalga formu özelliklerini üstün bir şekilde öğrenmiş ve dalga formlarını başarıyla yakalayabilmiştir.

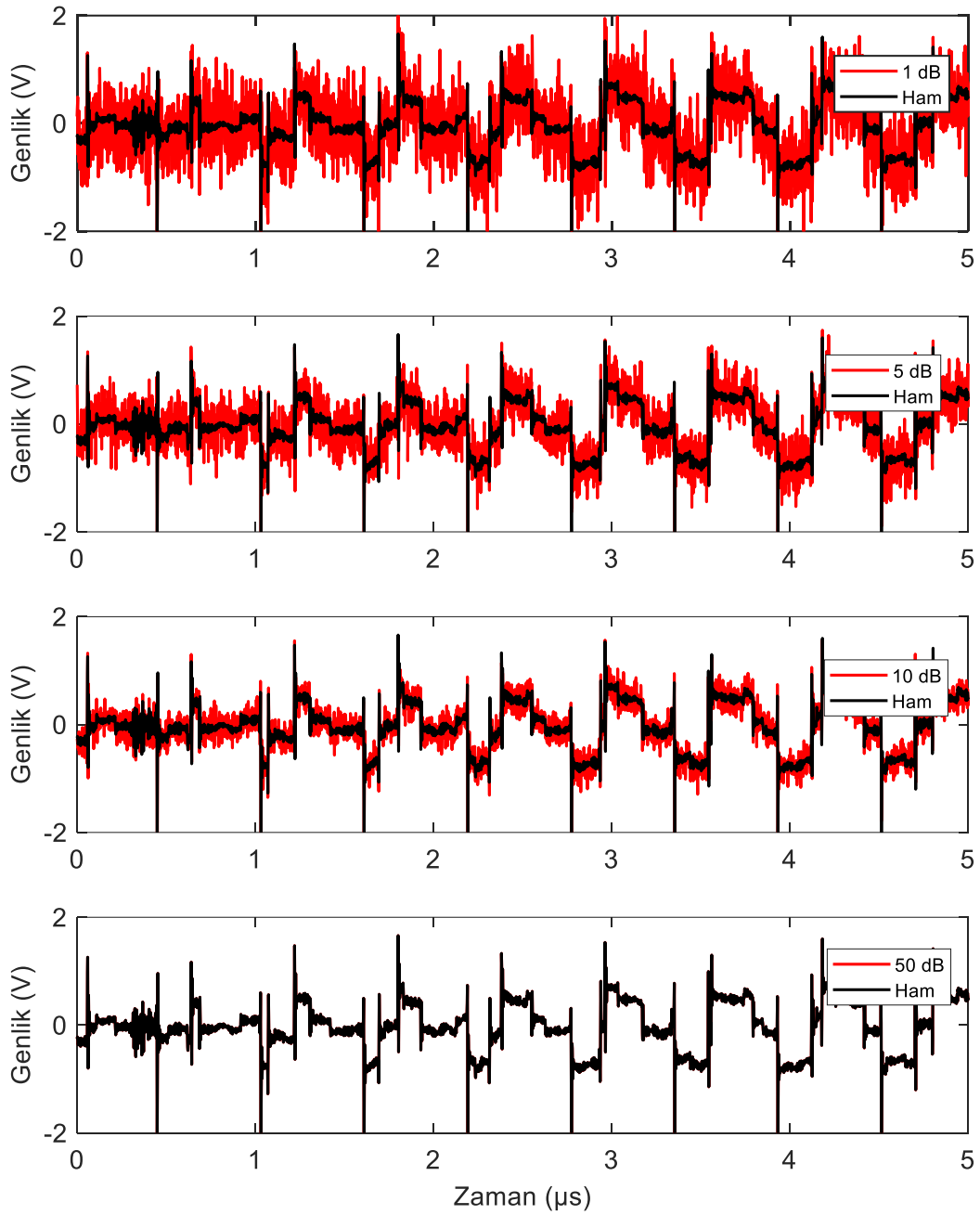


Şekil 5.28 (a) 100 MSPS ve (b) 800 MSPS'ye sahip Raspberry Pi cihazları için geliştirilen derin öğrenme modellerinin kimlik doğrulama testinden elde edilen Karışıklık Matrisi

100 MSPS ile örneklenmiş verilerle geliştirilen modelin stres testlerinde daha yüksek performans gösterdiği gözlemlendiğinden, çalışmada derin öğrenme modelinin gürültülü bir ortamda nasıl davrandığını incelemek amaçlanmıştır. Bu doğrultuda, 100 MSPS ve 800 MSPS için geliştirilen derin öğrenme modelleri, elde edilen test verilerine sentetik olarak Gauss gürültüsü eklenerek ayrı ayrı test edilmiştir. Gauss gürültüsü, farklı SNR seviyelerinde uygulanmış ve sonuçlar buna göre analiz edilmiştir. SNR formülü denklem (5.2) ile verilmiştir.

$$SNR(dB) = 10 \cdot \log_{10} \left(\frac{Signal}{Noise} \right) \quad (5.2)$$

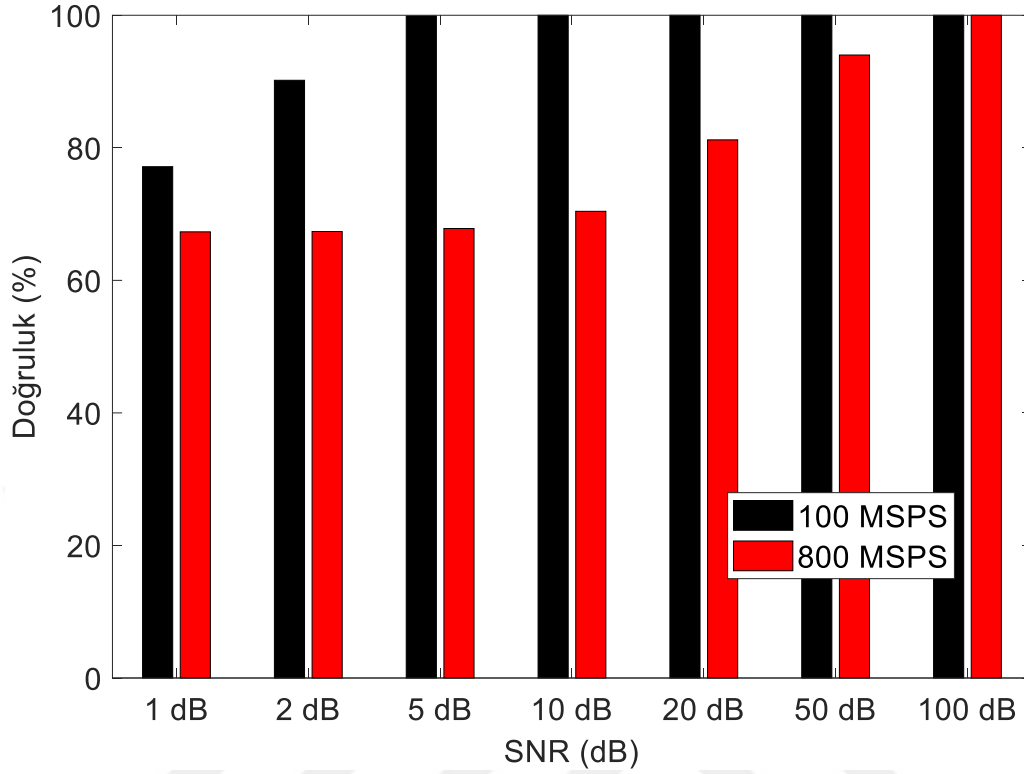
Analizleri gerçekleştirebilmek amacıyla, farklı SNR seviyelerinde gürültü eklenerek Şekil 5.29 ile verildiği gibi yeni bir veri seti oluşturulmuştur. Örnek grafik, 800 MSPS hızında elde edilen 5 µs'lik bir segmenti sunmakta olup, ham sinyallerin 1 dB, 5 dB, 10 dB ve 50 dB SNR seviyelerindeki ölçümlerle karşılaştırmalarını göstermektedir.



Şekil 5.29 Ham sinyalin, ham sinyale gürültü eklenerek oluşturulan sinyallerle karşılaştırılması

Sınıflandırma oranlarını incelemek amacıyla farklı SNR değerleri için Karmaşıklık Matrisleri oluşturulmuştur. Tüm Karmaşıklık Matrislerinin dahil edilmesi geniş bir alan gerektireceğinden, analiz Şekil 5.30 ile verildiği gibi çubuk grafik olarak sunulmuştur. Görüldüğü üzere, 100 MSPS ile örneklenmiş verilerle eğitilen derin öğrenme modeli, 800 MSPS verileriyle eğitilen modele kıyasla daha

iyi performans göstermektedir. Bu durum, modelin 100 MSPS veri setinde belirli dalga formlarını gözlemlemedeki artan kararlılığına atfedilmektedir.



Şekil 5.30 Sentetik gürültü ile test edildikten sonra 100 MSPS ve 800 MSPS'de örneklenen veriler üzerinde eğitimden elde edilen derin öğrenme modelinin doğruluk oranları

Yapılan testler, yüksek bir örnekleme oranının özellik çıkarımı için önemli olduğunu gösterse de derin öğrenme modelinin dalga formlarını daha iyi öğrenebilmesi için optimal örnekleme oranının belirlenmesinin kritik olduğu ortaya konmuştur. Bu durum, bu koşula uygun giriş verilerinin seçilmesini veya derin öğrenme modelinin buna göre uyarlanmasını gerektirebilir.

Elektronik cihazların kimlik numaralarının yapay olarak verilmesi cihazların taklit edilebilir bir yapıda olmasına neden olmaktadır. Bu durum özellikle kritik ortam ve sistemlerde büyük bir güvenlik problemi oluşturmaktadır. Kimlik bilgilerinin benzersiz bir biçimde tanımlanabilmesi için elektronik cihazların öz nitelikleri üzerinden çıkarım yapılması gerekmektedir. Yapılan tez çalışması kapsamında elektronik cihazların ürettiği ya da yaydığı sinyaller üzerinden kimliklendirme yapılarak cihazlara benzersiz kimlikler verilmiştir. Çalışma kapsamında kablosuz haberleşme, kablolu haberleşme ve elektromanyetik emisyon sinyalleri kullanılmış olup bu sinyaller üzerinden kimliklendirme için ise CNN, TCN, LSTM ve GRU gibi derin öğrenme modelleri kullanılmıştır. WiFi sinyalleri ile yapılan çalışmada aynı özelliklere sahip 6 farklı cihaz TCN modeli kullanılarak %99,47 başarımlı oranda kimliklendirilmiştir. Bu çalışmada ayrıca cihazların uzun süreli testleri yapılarak SDR'ın soğuk olması durumunda cihazların iyi kimliklendiremediği gözlemlenmiştir. Gözlem sonucunda yapılan araştırmalarda SDR'ın ısınmasına bağlı olarak elektronik karakteristiğinin farklı olması bu nedenle veri seti oluşturulurken ki sıcaklık ile sistemin kullanımı sırasındaki sıcaklığının benzer olması gerektiği saptanmıştır. Bu nedenle sistem çalıştırıldıktan bir süre sonra güvenlik kontrollerine başlamaktadır. Kablosuz haberleşmede yapılan farklı bir çalışmada ise LoRa sinyalleri üzerinden 4 aynı modeldeki cihaz TCN, CNN, LSTM ve GRU modelleri eğitilmiş olup TCN modelinde %99 başarımlı orana kadar kimliklendirilmiştir. Bununla beraber LoRa sinyalleri ile yapılan çalışma kapsamında cihazların uzun süreli testleri de yapılarak eğitim için gerekli minimum sinyal analizleri de yapılmış olup eğitim için saatte bir paket atılmasının bile önerilen sistemin başarısı için yeterli olduğu görülmüştür. Elektromanyetik sinyaller ile yapılan kimliklendirme çalışmalarında ise iletilen emisyon

çalışmasında 15 cihaz kimliklendirilmiş olup %99,8 başarımlı oranın sağlanırken havadan elektromanyetik sinyaller üzerinden yapılan çalışmada aynı model 2 cihaz %100 oranında başarımlı ile kimliklendirilmiştir.

Yapılan çalışmalar neticesinde güç elektroniği gibi haberleşme sinyalleri bulunmayan sistemler için elektromanyetik emisyon üzerinden kimliklendirmenin daha uygun olacağı saptanmıştır. Burada şebeke üzerinden beslenmeyip pil ile çalışan sistemler için yakın alan elektromanyetik sinyaller üzerinden kimliklendirmek hem ekonomik hem de pratik açıdan daha uygunken sabit şebeke üzerinden beslenen cihazlar için iletilen emisyon üzerinden kimliklendirme yapılarak hem daha fazla cihazın bir bağlantı üzerinden kimliklendirmesi mümkün olmakta hem de kullanıcıların herhangi bir eforu olmadan güvenlik kontrolleri yapılmaktadır. Elektromanyetik emisyon kimliklendirmesi herhangi bir haberleşme sinyali gerektirmemektedir ancak ortamda bulunan gürültülerden daha fazla etkilenebilmektedir. Bu nedenle elektromanyetik gürültünün fazla bulunduğu noktalarda haberleşme sinyalleri üzerinden kimliklendirme daha ayırt edici olabilmektedir. Kablolu sinyaller üzerinden yapılan kimliklendirme çalışmalarında da iletilen emisyon çalışmasına benzer bir biçimde yapılmaktadır. Ancak genel olarak sinyal kabloları üzerinde bir koruma (shield) bulunması sinyallerin dışarıdan gelen gürültülerin önüne geçilmesine ve sadece elektronik kartların öz niteliklerinin daha iyi çıkarılmasını sağlamaktadır. Kablosuz haberleşme sinyalleri kullanılarak kimliklendirme işleminde ise sinyallerin çözülünerek veri setinin otomatik oluşturulabilmesi elektromanyetik sinyallere göre avantaj sunmaktadır. Ayrıca hem SDR hem de elektronik kartın özelliklerinin kimliklendirmeye etki etmesinden dolayı daha keskin sonuçlar verdiğini söylemekte mümkündür.

Bu çalışma, elektronik cihazların kimliklendirilmesi için kablosuz haberleşme sinyalleri, kablolu haberleşme sinyalleri ve elektromanyetik emisyonların kullanımını incelemiş ve yüksek başarımlı oranları elde etmiştir. Ancak, bu alanda yapılabilecek pek çok geliştirme bulunmaktadır ve gelecekte daha kapsamlı araştırmalarla kimliklendirme sistemlerinin daha güvenilir ve etkin hale getirilmesi mümkündür.

İlk olarak, daha büyük ve çeşitlendirilmiş veri setleri üzerinde çalışmalar yapılması önerilmektedir. Çalışmada kullanılan veri setleri sınırlı sayıda cihaz ve sinyal türü ile sınırlandırılmıştır. Gelecekte, farklı marka ve modellerden oluşan daha geniş veri setleri oluşturularak modellerin genelleme yeteneği değerlendirilebilir. Ayrıca, ortam sıcaklığı, nem ve elektromanyetik gürültü gibi çevresel değişkenlerin etkisi daha detaylı incelenebilir ve modellerin bu değişkenlere dayanıklılığı artırılabilir. Kullanılan CNN, TCN, LSTM ve GRU gibi derin öğrenme modellerinin yanı sıra, Transformer tabanlı modeller gibi daha güncel tekniklerin kullanımıyla performans iyileştirmeleri yapılabilir. Aynı zamanda, modellerin parametre sayısı, eğitim süresi ve enerji tüketimi gibi faktörler açısından optimizasyon çalışmaları yapılması da önem taşımaktadır. Bu sayede daha verimli ve hızlı çalışan kimliklendirme sistemleri geliştirilebilir. SDR cihazlarının başlangıç sıcaklığının kimliklendirme performansına etkisi bu çalışmada gözlemlenmiştir. Gelecekte, bu sorunun üstesinden gelmek için sıcaklık dengeleme mekanizmaları veya sıcaklık değişimlerine dayanıklı sinyal işleme teknikleri geliştirilebilir. Bu tür iyileştirmeler, özellikle gerçek zamanlı sistemlerde daha güvenilir sonuçlar elde edilmesine katkı sağlayacaktır. Kimliklendirme sistemlerinin gerçek zamanlı uygulamalarda kullanılabilmesi için düşük gecikmeli ve hızlı çalışan algoritmalar geliştirilmelidir. Özellikle güvenlik açısından kritik ortamlarda, cihazların anlık olarak tanınması büyük önem taşımaktadır. Bu nedenle, gerçek zamanlı veri işleme tekniklerinin entegrasyonu ve bu süreçlerin test edilmesi gelecekteki çalışmalar için öncelikli bir alan olabilir. Elektromanyetik emisyon tabanlı kimliklendirme sistemlerinin gürültü yoğunluğu yüksek ortamlarda daha dayanıklı hale getirilmesi gerekmektedir. Gürültü azaltma algoritmaları veya hibrit yaklaşımlar (örneğin, elektromanyetik emisyon ve kablosuz sinyallerin bir arada kullanılması) bu bağlamda geliştirilebilir. Bu yöntemler, hem gürültü etkilerini azaltmak hem de kimliklendirme doğruluğunu artırmak için etkili olacaktır. Gelecekte yapılacak diğer bir önemli çalışma, kimliklendirme sistemlerinin güvenlik açısından güçlendirilmesidir. Cihazların kimlik bilgilerinin güvenilirliğini artırmak ve kimlik taklitlerinin önüne geçmek için şifreleme teknikleri veya blokzincir tabanlı kimlik yönetim sistemleri entegre edilebilir. Bu tür güvenlik önlemleri, özellikle hassas verilerin korunduğu sistemlerde büyük bir değer taşıyacaktır. Son olarak, güç elektroniği, IoT

cihazları, tıbbi cihazlar gibi farklı cihaz türleri ve uygulama alanları üzerinde çalışmalar yapılması önerilmektedir. Endüstriyel tesisler, akıllı şehirler ve kritik altyapılar gibi karmaşık ortamlarda kimliklendirme sistemlerinin performansı değerlendirilebilir. Bu çalışmalar, cihazların uzun süreli performansını, yaşlanma etkilerini ve sinyal karakteristiklerindeki değişimleri analiz ederek daha dayanıklı sistemler geliştirilmesine katkı sağlayacaktır.

Bu öneriler, elektronik cihaz kimliklendirme alanında gelecekte yapılacak araştırmalar için yol gösterici nitelikte olup, sistemlerin güvenilirlik, esneklik ve verimlilik açısından daha da geliştirilmesini sağlayacaktır. Bu tür çalışmalar, özellikle güvenlik gereksinimleri yüksek olan kritik ortamlarda önemli yeniliklere kapı aralayacaktır.



KAYNAKÇA

- [1] P. Corke, 2017, “Robotics, Vision and Control,” vol. 118.
- [2] M. J. Madou, Faceting due to angle-dependent sputter rate, 3rd edit. CRC Press, 2011.
- [3] P. Sethi and S. R. Sarangi, 2017, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering, vol. 2017.
- [4] “Global major electronic device shipments 2015-2022 | Statista.” [Online]. Available: <https://www.statista.com/statistics/220120/global-mobile-device-sales-forecast-by-device/>. [Accessed: 20-May-2023].
- [5] “TÜİK Kurumsal.” [Online]. Available: [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(BT\)-Kullanım-Arastirmasi-2022-45587](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanım-Arastirmasi-2022-45587). [Accessed: 20-May-2023].
- [6] “IoT Security Statistics (2022): What You Should Know - Intersog.” [Online]. Available: <https://intersog.com/blog/iot-security-statistics/>. [Accessed: 20-May-2023].
- [7] “Statistics of research on IoT Security | Download Scientific Diagram.” [Online]. Available: https://www.researchgate.net/figure/Statistics-of-research-on-IoT-Security_fig1_326403602. [Accessed: 20-May-2023].
- [8] “Electronic Security Market Size & Share Analysis - Industry Research Report - Growth Trends.” [Online]. Available: <https://www.mordorintelligence.com/industry-reports/electronic-security-market>. [Accessed: 20-May-2023].
- [9] M. L. Das, P. Kumar, and A. Martin, “Secure and privacy-preserving RFID Authentication Scheme for Internet of Things Applications.”

- [10] P. Mezzanotte, V. Palazzi, F. Alimenti, and L. Roselli, Jan. 2021, "Innovative RFID Sensors for Internet of Things Applications," *IEEE Journal of Microwaves*, vol. 1, no. 1, pp. 55–65.
- [11] J. SathishKumar and D. R. Patel, Mar. 2014, "A Survey on Internet of Things: Security and Privacy Issues," *Int J Comput Appl*, vol. 90, no. 11, pp. 20–26.
- [12] Y. Yilmaz, S. R. Gunn, and B. Halak, Oct. 2018, "Lightweight PUF-based authentication protocol for IoT devices," 2018 IEEE 3rd International Verification and Security Workshop, IVSW 2018, pp. 38–43.
- [13] M. N. K. Patil, M. A. S. Hendre, and D. P. Narsale, 2018, "Design and Analysis of Electronics Devices V-I Characteristics Using Universal Component Tester," *International Research Journal of Engineering and Technology*.
- [14] J. G. Barnes, *The Fingerprint*. 2011.
- [15] R. M. Caplan, Jul. 1990, "How fingerprints came into use for personal identification," *J Am Acad Dermatol*, vol. 23, no. 1, pp. 109–114.
- [16] A. K. Jain, A. Ross, and S. Prabhakar, Jan. 2004, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20.
- [17] N. K. Ratha, J. H. Connell, and R. M. Bolle, 2001, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634.
- [18] R. Saad, Apr. 2005, "Discovery, development, and current applications of DNA identity testing," *Proc (Bayl Univ Med Cent)*, vol. 18, no. 2, p. 130.
- [19] J. H. Liu and J. László, 2007, "A Narrative Theory of History and Identity," *Social Representations and Identity*, pp. 85–107.
- [20] S. A. Cole, Apr. 2006, "History of Fingerprint Pattern Recognition," *Automatic Fingerprint Recognition Systems*, pp. 1–25.

- [21] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, Mar. 2011, "Key management systems for sensor networks in the context of the Internet of Things," *Computers and Electrical Engineering*, vol. 37, no. 2, pp. 147–159.
- [22] L. Atzori, A. Iera, and G. Morabito, Oct. 2010, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805.
- [23] F. Hu, Security and privacy in internet of things (IoTs): models, algorithms, and implementations. .
- [24] A. J. Showail and A. J. Showail, Mar. 2021, "Internet of Things Security and Privacy," *Internet of Things*.
- [25] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, Jan. 2015, "A Survey on Internet of Things from Industrial Market Perspective," *IEEE Access*, vol. 2, pp. 1660–1679.
- [26] A. Čolaković and M. Hadžialić, Oct. 2018, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39.
- [27] K. Stouffer, J. Falco, and K. Scarfone, "Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) Recommendations of the National Institute of Standards and Technology."
- [28] L. E. Langley, 1993, "Specific emitter identification (SEI) and classical parameter fusion technology," *Proceedings of WESCON 1993 Conference Record*, pp. 377–381.
- [29] L. Ding, S. Wang, F. Wang, and W. Zhang, Dec. 2018, "Specific Emitter Identification via Convolutional Neural Networks," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2591–2594.

- [30] G. Huang, Y. Yuan, X. Wang, and Z. Huang, Dec. 2016, "Specific Emitter Identification Based on Nonlinear Dynamical Characteristics," *Canadian Journal of Electrical and Computer Engineering*, vol. 39, no. 1, pp. 34–41.
- [31] P. Rengaraju, S. S. Kumar, and C. H. Lung, Nov. 2017, "Investigation of security and QoS on SDN firewall using MAC filtering," 2017 International Conference on Computer Communication and Informatics, ICCCI 2017.
- [32] T. Girdler and V. G. Vassilakis, Mar. 2021, "Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses," *Computers & Electrical Engineering*, vol. 90, p. 106990.
- [33] A. P. U. Siahaan, Jan. 2024, "A Review of IP and MAC Address Filtering in Wireless Network Security."
- [34] S. Pukkawanna, G. Blanc, J. Garcia-Alfaro, Y. Kadobayashi, and H. Debar, Apr. 2016, "Classification of SSL Servers based on their SSL Handshake for Automated Security Assessment," *Proceedings - 3rd International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2014*, pp. 30–39.
- [35] F. Chen, K. Wu, W. Chen, and Q. Zhang, 2013, "The research and implementation of the VPN gateway based on SSL," *Proceedings - 2013 International Conference on Computational and Information Sciences, ICCIS 2013*, pp. 1376–1379.
- [36] S. M. Kim, Y. H. Goo, M. S. Kim, S. G. Choi, and M. J. Choi, Sep. 2015, "A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP," 17th Asia-Pacific Network Operations and Management Symposium: Managing a Very Connected World, APNOMS 2015, pp. 487–490.
- [37] K. A. Shaikh, A. Karthik Bhat, and M. Moharir, Aug. 2018, "A Survey on SSL Packet Structure," 2nd International Conference on Computational

Systems and Information Technology for Sustainable Solutions, CSITSS 2017.

- [38] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson, Nov. 2014, “Analyzing forged SSL certificates in the wild,” *Proc IEEE Symp Secur Priv*, pp. 83–97.
- [39] J. D. Day and H. Zimmermann, 1983, “The OSI Reference Model,” *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334–1340.
- [40] H. Kim, S. Oh, and P. Viswanath, May 2020, “Physical Layer Communication via Deep Learning,” *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 1, pp. 5–18.
- [41] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, 2021, “Physical Layer Security Enhancement with Reconfigurable Intelligent Surface-Aided Networks,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3480–3495.
- [42] Z. Qin, H. Ye, G. Y. Li, and B. H. F. Juang, Apr. 2019, “Deep learning in physical layer communications,” *IEEE Wirel Commun*, vol. 26, no. 2, pp. 93–99.
- [43] M. N. O. Sadiku and C. M. Akujobi, Oct. 2004, “Software-defined radio: A brief overview,” *IEEE Potentials*, vol. 23, no. 4, pp. 14–15.
- [44] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, Sep. 2020, “A Review of Radio Frequency Fingerprinting Techniques,” *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222–233.
- [45] Y. Yang and T. Yan, Jun. 2021, “Radio Frequency Fingerprint Recognition Method Based on Generative Adversarial Net,” *2021 13th International Conference on Communication Software and Networks, ICCSN 2021*, pp. 361–364.
- [46] M. Cekic, S. Gopalakrishnan, and U. Madhow, “Wireless Fingerprinting via Deep Learning: The Impact of Confounding Factors.”
- [47] S. S. Hanna and D. Cabric, Apr. 2019, “Deep Learning Based Transmitter Identification using Power Amplifier Nonlinearity,” *2019 International*

- Conference on Computing, Networking and Communications, ICNC 2019, pp. 674–680.
- [48] G. Rebala, A. Ravi, and S. Churiwala, 2019, “Machine Learning Definition and Basics,” *An Introduction to Machine Learning*, pp. 1–17.
 - [49] G. Rebala, A. Ravi, and S. Churiwala, 2019, “An Introduction to Machine Learning.”
 - [50] M. Pandey and S. S. Rautaray, 2021, “Machine Learning: Theoretical Foundations and Practical Applications,” vol. 87.
 - [51] G. Rebala, A. Ravi, and S. Churiwala, 2019, “Classification,” *An Introduction to Machine Learning*, pp. 57–66.
 - [52] M. Lukacs, P. Collins, and M. Temple, May 2015, “Classification performance using ‘RF-DNA’ fingerprinting of ultra-wideband noise waveforms,” *Electron Lett*, vol. 51, no. 10, pp. 787–789.
 - [53] X. Wang, Y. Zhang, H. Zhang, X. Wei, and G. Wang, Dec. 2019, “Identification and authentication for wireless transmission security based on RF-DNA fingerprint,” *EURASIP J Wirel Commun Netw*, vol. 2019, no. 1, pp. 1–12.
 - [54] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, 2010, “RF-DNA fingerprinting for airport WiMax communications security,” *Proceedings - 2010 4th International Conference on Network and System Security, NSS 2010*, pp. 32–39.
 - [55] J. C. Liando, A. Gamage, A. W. Tengourtius, and M. Li, Feb. 2019, “Known and Unknown Facts of LoRa,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 15, no. 2.
 - [56] V. Fialho and F. Azevedo, Dec. 2018, “Wireless Communication Based on Chirp Signals for LoRa IoT Devices,” *i-ETC : ISEL Academic Journal of Electronics Telecommunications and Computers*, vol. 4, no. 1, p. 6.
 - [57] P. Robyns, P. Quax, W. Lamotte, and W. Thenaers, 2018, “A multi-channel software decoder for the LoRa modulation scheme,” *IoTBDS 2018* -

Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, vol. 2018-March, pp. 41–51.

- [58] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, Jan. 2020, “A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 371–388.
- [59] N. Chen, A. Hu, and H. Fu, Mar. 2021, “LoRa radio frequency fingerprint identification based on frequency offset characteristics and optimized LoRaWAN access technology,” *IAEAC 2021 - IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference*, pp. 1801–1807.
- [60] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelee, and B. Preneel, Jul. 2017, “Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning,” *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017*, pp. 58–63.
- [61] A. Elmaghbub and B. Hamdaoui, 2021, “LoRa Device Fingerprinting in the Wild: Disclosing RF Data-Driven Fingerprint Sensitivity to Deployment Variability,” *IEEE Access*, vol. 9, pp. 142893–142909.
- [62] B. Hamdaoui and A. Elmaghbub, 2022, “Deep-Learning-Based Device Fingerprinting for Increased LoRa-IoT Security: Sensitivity to Network Deployment Changes,” *IEEE Netw*, vol. 36, no. 3, pp. 204–210.
- [63] E. Sourour, H. El-Ghoroury, and D. McNeill, 2004, “Frequency offset estimation and correction in the IEEE 802.11a WLAN,” *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, vol. 60, no. 7, pp. 4923–4927.
- [64] F. H. Sakaci, I. Basaran, V. Yildirim, and C. Ayyildiz, 2021, “Real-Time Decoding and Analysis of WiFi Signals on CPU and GPU,” *Proceedings - 2021 Innovations in Intelligent Systems and Applications Conference, ASYU 2021*.

- [65] R. M. Gerdes, R. M. Gerdes, T. E. Daniels, M. Mina, and S. F. Russell, 2006, "Device identification via analog signal fingerprinting: A matched filter approach," IN 144 PROCEEDINGS OF THE NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (NDSS), p. 78.
- [66] R. M. Gerdes, M. Mina, S. F. Russell, and T. E. Daniels, 2012, "Physical-layer identification of wired ethernet devices," IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1339–1353.
- [67] S. Li, A. Hu, J. Liu, and J. Yu, 2021, "Adaptive Filter-Based Approach for PHY Fingerprints Extraction of Fast Ethernet Network," Proceedings - 2021 2nd International Conference on Electronics, Communications and Information Technology, CECIT 2021, pp. 180–185.
- [68] T. J. Carbino, M. A. Temple, and J. Lopez, Jul. 2016, "Conditional Constellation Based-Distinct Native Attribute (CB-DNA) fingerprinting for network device authentication," 2016 IEEE International Conference on Communications, ICC 2016.
- [69] J. Liu, A. Hu, and S. Li, 2022, "Spectrum-based Fingerprint Extraction and Identification Method of 100M Ethernet Card," Proceedings - 2022 6th International Conference on Cryptography, Security and Privacy, CSP 2022, pp. 102–107.
- [70] L. Peng and A. Hu, May 2019, "A Design of Deep Learning Based Optical Fiber Ethernet Device Fingerprint Identification System," IEEE International Conference on Communications, vol. 2019-May.
- [71] R. R. Tummala and E. J. Rymaszewski, Microelectronics packaging handbook. Chapman & Hall, 1997.
- [72] C. R. Paul, R. C. Scully, and M. Steffka, "Introduction to electromagnetic compatibility."
- [73] H. W. Ott, 2009, "Gound Plane Current Distributon and Impedance," Electromagnetic Compatibility Engineering, pp. 391–411.
- [74] W. L. Stutzman and G. A. Thiele, 2013, "Antenna theory and design," p. 822.

- [75] Constantine A. Balanis, 2016, "Antenna Theory: Analysis and Design, 4th Edition | Wiley," p. 1104.
- [76] L. Zhang, H. Zhu, and W. D. Li, 2022, "Near-field to Far-field Transformation with an Equivalent Magnetic Current Approach," 2022 International Applied Computational Electromagnetics Society Symposium, ACES-China 2022.
- [77] H. F. Arnoldus, Apr. 2001, "Representation of the near-field, middle-field, and far-field electromagnetic Green's functions in reciprocal space," JOSA B, Vol. 18, Issue 4, pp. 547-555, vol. 18, no. 4, pp. 547–555.
- [78] H. ; Chen et al., Feb. 2023, "Research on the Method of Near-Field Measurement and Modeling of Powerful Electromagnetic Equipment Radiation Based on Field Distribution Characteristics," Energies 2023, Vol. 16, Page 2005, vol. 16, no. 4, p. 2005.
- [79] J. Ghigo, A. C. Erwin, and C. W. Erwin, 1991, "Near-field vs. Far-field Evoked Potentials," American Journal of EEG Technology, vol. 31, no. 2, pp. 109–118.
- [80] S. Laybros, P. F. Combes, and H. J. Mametsa, Aug. 2005, "The 'very-near-field' region of equiphase radiating apertures," IEEE Antennas Propag Mag, vol. 47, no. 4, pp. 50–66.
- [81] A. Capozzoli, C. Curcio, F. D'Agostino, and A. Lisenò, Jun. 2024, "A Review of the Antenna Field Regions," Electronics 2024, Vol. 13, Page 2194, vol. 13, no. 11, p. 2194.
- [82] G. A. Jackson, 1992, "Introduction to Electromagnetic Compatibility," IEE Review, vol. 38, no. 7–8, p. 280.
- [83] P. González-Vizueté, J. Bernal-Méndez, and M. A. Martín-Prats, Jun. 2021, "Reducing Conducted Emissions at the Output of Full-Bridge DCDC Converters with High Voltage Steps," Electronics 2021, Vol. 10, Page 1373, vol. 10, no. 12, p. 1373.
- [84] H. W. Ott, "Electromagnetic Compatibility Engineering."

- [85] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y. C. Chen, Nov. 2019, “DemicPU: Device fingerprinting with magnetic signals radiated by CPU,” *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1149–1162.
- [86] X. Ji, Y. Cheng, J. Zhang, Y. Chi, W. Xu, and Y. C. Chen, Dec. 2021, “Device Fingerprinting with Magnetic Induction Signals Radiated by CPU Modules,” *ACM Transactions on Sensor Networks (TOSN)*, vol. 18, no. 2.
- [87] A. Stern, U. Botero, F. Rahman, D. Forte, and M. Tehranipoor, Feb. 2020, “EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification,” *IEEE Trans Very Large Scale Integr VLSI Syst*, vol. 28, no. 2, pp. 363–375.
- [88] H. xin Zhang, J. Liu, J. Xu, F. Zhang, X. tong Cui, and S. fei Sun, Dec. 2020, “Electromagnetic radiation-based IC device identification and verification using deep learning,” *EURASIP J Wirel Commun Netw*, vol. 2020, no. 1, pp. 1–23.
- [89] O. A. Ibrahim and R. Di Pietro, May 2023, “Mag-Auth: Authenticating Wireless Transmitters and Receivers on the Receiver Side via Magnetic Emissions,” *WiSec 2023 - Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 305–316.
- [90] S. A. Edmiston, C. Norman, and M. J. Wilson, “Electronic Device Identification,” 2021.
- [91] E. Hiromichi and F. Junya, “Device Identification Apparatus and Program,” 2020.
- [92] F. H. Sakacı and T. Yıldırım, Oct. 2024, “Conducted Emission signal-based identification and real-time hardware security with deep learning,” *Eng Appl Artif Intell*, vol. 136, p. 109025.
- [93] A. Géron, 2017, “Hands-on Machine Learning with Scikit-Learn, Keras, and TensorFlow (2019, O’reilly),” *Hands-On Machine Learning with R*, p. 510.

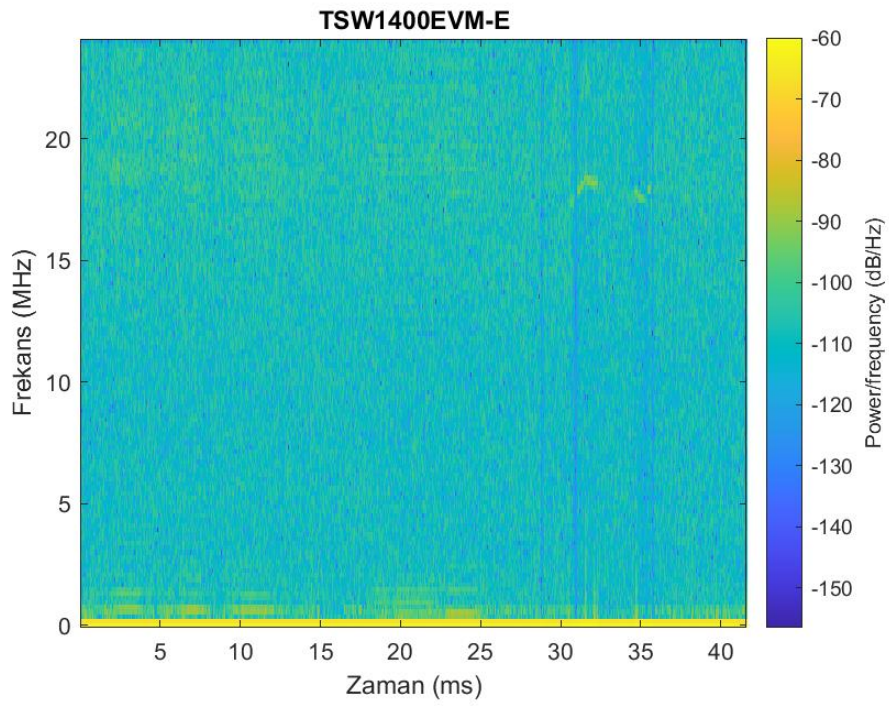
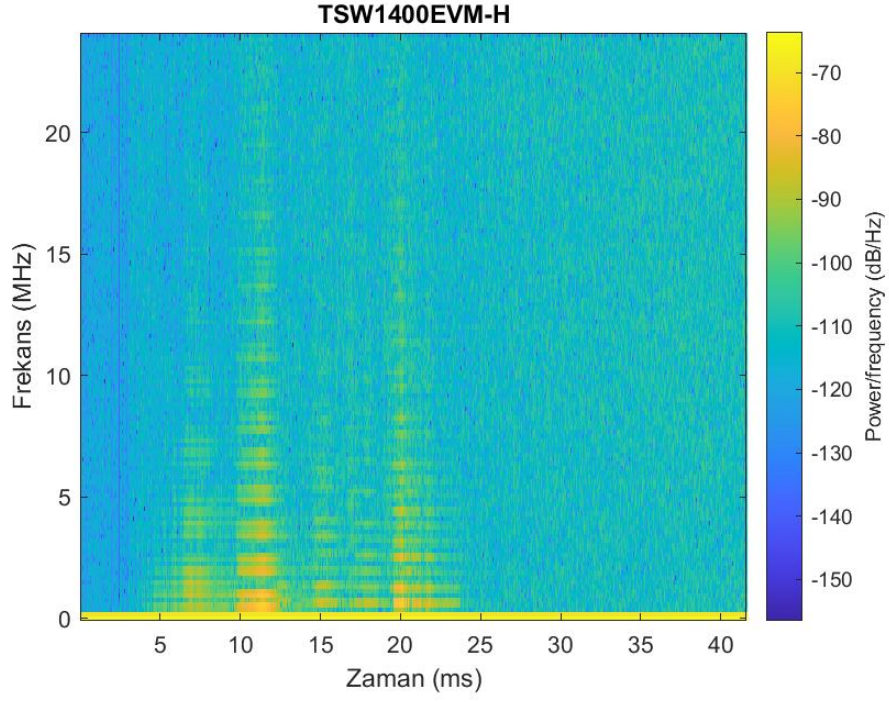
- [94] K. P. Murphy, "Machine learning: a probabilistic perspective." 2012.
- [95] C. M. Bishop, Pattern Recognition and Machine Learning. 2006.
- [96] T. M. Mitchell, Machine learning, vol. 45, no. 13. Wiley, 2017.
- [97] A. Lindholm, N. Wahlström, F. Lindsten, and T. B. Schön, "Supervised Machine Learning," Mar. 2019.
- [98] M. Colins, 2017, "Machine learning: an introduction to supervised and unsupervised learning algorithms," p. 60.
- [99] M. W. Berry, M. Azlinah, and B. Wah Yap, 2020, "Supervised and Unsupervised Learning for Data Science."
- [100] P. Stone, "Reinforcement Learning," in Encyclopedia of Machine Learning, Boston, MA: Springer, Boston, MA, 2011, pp. 849–851.
- [101] S. Bhatnagar, H. Prasad, and L. Prashanth, "Reinforcement learning," in Lecture Notes in Control and Information Sciences, vol. 434, Springer Verlag, 2013, pp. 187–220.
- [102] M. Wiering and M. Otterlo, "Reinforcement Learning," in Adaptation, Learning, and Optimization , vol. 12, M. Wiering and M. van Otterlo, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012.
- [103] Dec. 2019, "Artificial Neural Networks," Condition Monitoring with Vibration Signals, pp. 239–258.
- [104] R. E. Uhrig, "Introduction to artificial neural networks," Proceedings of IECON '95 - 21st Annual Conference on IEEE Industrial Electronics, vol. 1, pp. 33–37.
- [105] D. J. Livingstone, Artificial Neural Networks, vol. 458. Totowa, NJ: Humana Press, 2009.
- [106] I. N. da Silva, D. H. Spatti, R. A. Flauzino, L. H. B. Liboni, and S. F. dos Reis Alves, Jan. 2016, "Artificial neural networks: A practical course," Artificial Neural Networks: A Practical Course, pp. 1–307.

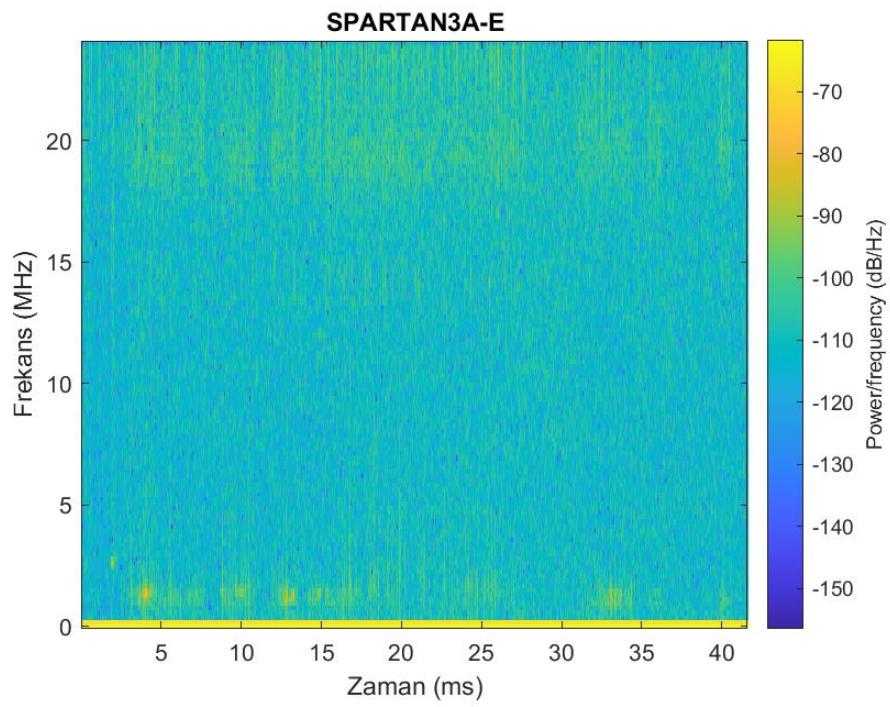
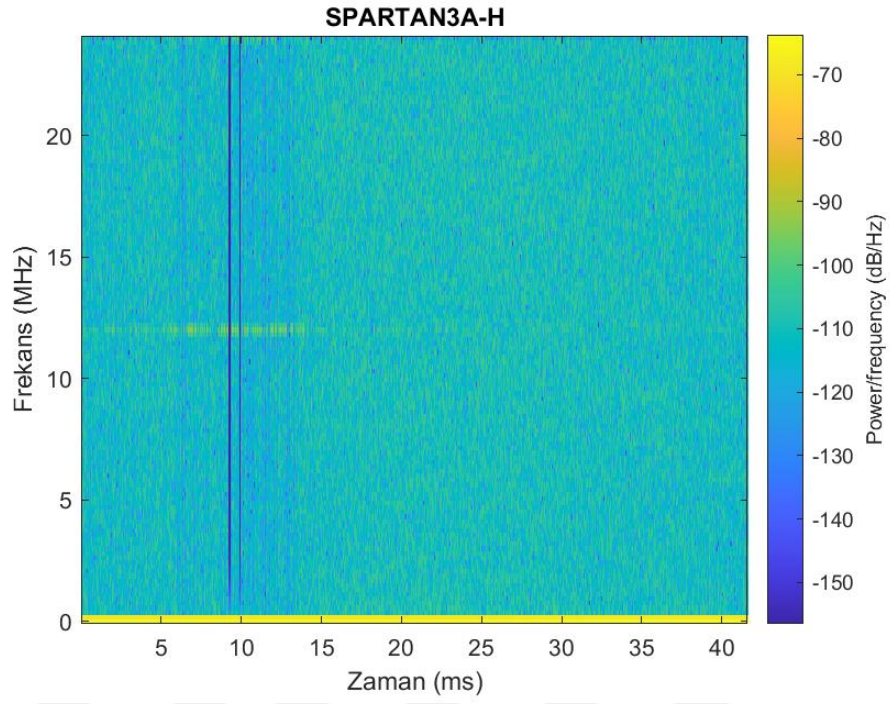
- [107] F. H. SAKACI, “Buck-Boost Dc-Dc Dönüştürücü Kaynaklı Emi/Emc Problemlerinin Çözümüne Yönelik Makine Öğrenmesi Temelli Yaklaşımlar,” 2021.
- [108] T. Rauber and G. Rünger, *Parallel programming*. Springer Berlin Heidelberg, 2013.
- [109] Y. Huang, 2022, “Parallel computing and its applications,” 2022 IEEE International Conference on Artificial Intelligence and Computer Applications, ICAICA 2022, pp. 715–718.
- [110] D. B. Davidson, 1995, “Parallel computing: Computing for the impatient and indomitable,” *IEEE Potentials*, vol. 14, no. 2, pp. 6–10.
- [111] D. De Donno, A. Esposito, L. Tarricone, and L. Catarinucci, Jun. 2010, “Introduction to GPU computing and CUOA programming: A case study on FOTO,” *IEEE Antennas Propag Mag*, vol. 52, no. 3, pp. 116–122.
- [112] J. Nickolls, May 2016, “GPU parallel computing architecture and CUDA programming model,” 2007 IEEE Hot Chips 19 Symposium, HCS 2007.
- [113] J. Nickolls, May 2016, “Scalable parallel programming with CUDA introduction,” 2008 IEEE Hot Chips 20 Symposium, HCS 2008.
- [114] T. Dominguez-Bolano, J. Rodriguez-Pineiro, J. A. Garcia-Naya, and L. Castedo, Oct. 2020, “Bit Error Probability and Capacity Bound of OFDM Systems in Deterministic Doubly-Selective Channels,” *IEEE Trans Veh Technol*, vol. 69, no. 10, pp. 11458–11469.
- [115] A. Ligata, H. Gacanin, F. Adachi, M. Smolnikar, and M. Mohorcic, Mar. 2011, “Bit Error Rate Analysis for an OFDM System with Channel Estimation in a Nonlinear and Frequency-Selective Fading Channel,” *EURASIP Journal on Wireless Communications and Networking* 2011 2011:1, vol. 2011, no. 1, pp. 1–12.
- [116] K. Sankhe et al., Mar. 2020, “No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments,” *IEEE Trans Cogn Commun Netw*, vol. 6, no. 1, pp. 165–178.

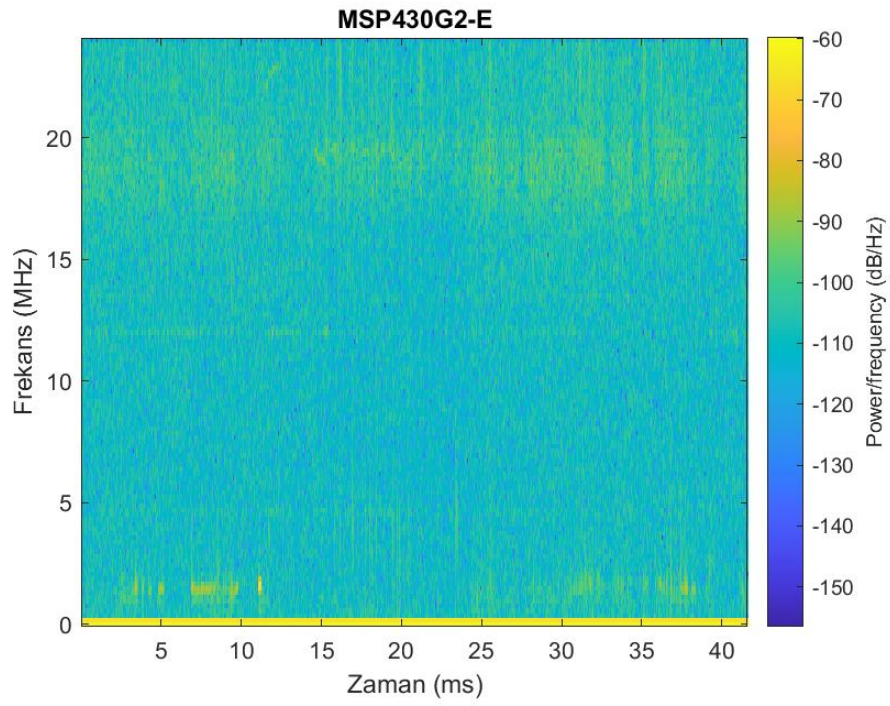
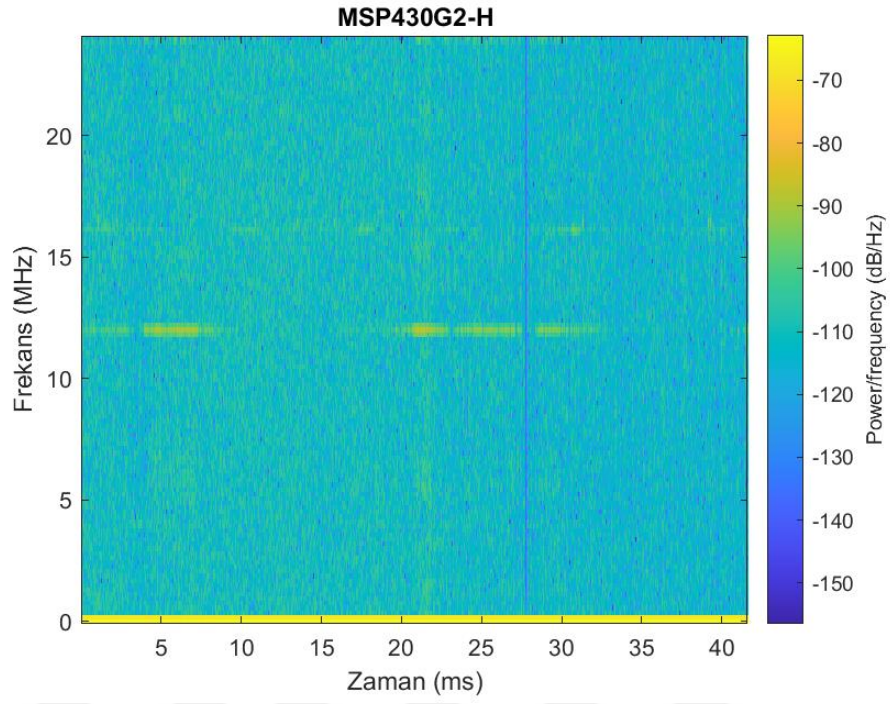
- [117] D. B. Leeson, 1966, "A Simple Model of Feedback Oscillator Noise Spectrum," *Proceedings of the IEEE*, vol. 54, no. 2, pp. 329–330.
- [118] "Phase-locked loops for high-frequency receivers and transmitters-Part 2 | Analog Devices." [Online]. Available: <https://www.analog.com/en/analog-dialogue/articles/pll-for-high-frequency-receivers-and-transmitters-2.html>. [Accessed: 25-Dec-2022].
- [119] J. Liu, X. Wang, and R. Gong, 2011, "Analysis and simulation of common-mode conducted interference source in separately excited DC motor," *Proceedings of the 6th International Forum on Strategic Technology, IFOST 2011*, vol. 2, pp. 1145–1148.
- [120] V. V. Bodake, S. Gupta, S. Bhat, and V. R. Vasanth, Nov. 2019, "Modelling and simulation of conducted emission for electronic control module," *IEEE 5th Global Electromagnetic Compatibility Conference, GEMCCON 2019 - Proceedings*.
- [121] Z. Feng, A. Berry, P. Ellis, and W. Lawson, 2021, "SPICE models for predicting EMC performance of a MOSFET based half-bridge configuration," *PEAS 2021 - 2021 IEEE 1st International Power Electronics and Application Symposium, Conference Proceedings*.
- [122] O. Coskun, Ö. Çevik, R. Eken, S. B. Yazici, and G. Yilmaz, 2021, "Modeling and Simulation the Effect of Different Structures in A LED Driver Board on Conducted Emission Level," *2021 13th International Conference on Electrical and Electronics Engineering, ELECO 2021*, pp. 152–156.
- [123] "cpuburn-arm/cpuburn-a53.S at master · ssvb/cpuburn-arm · GitHub."

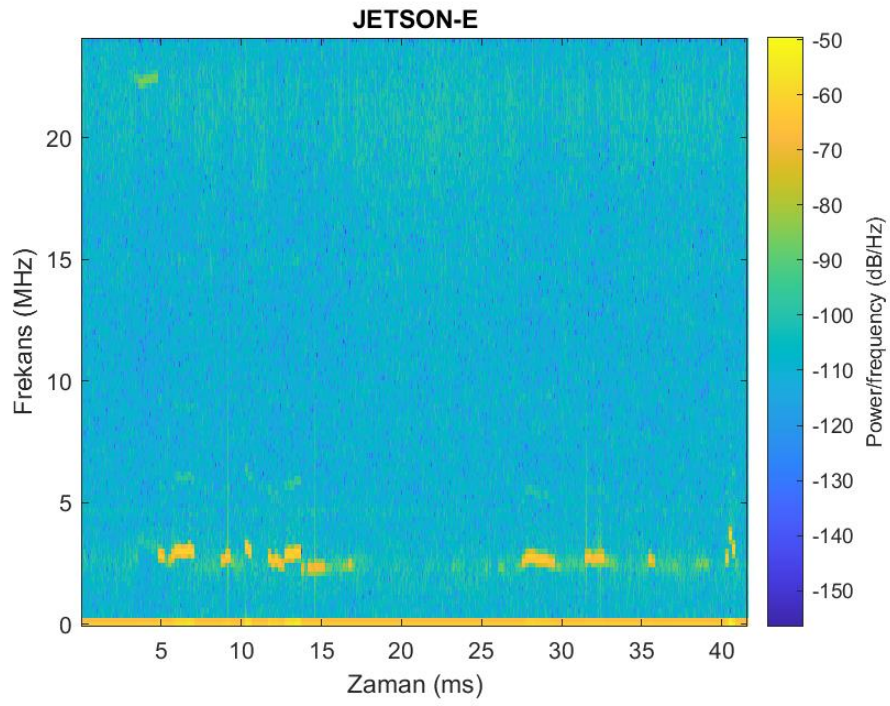
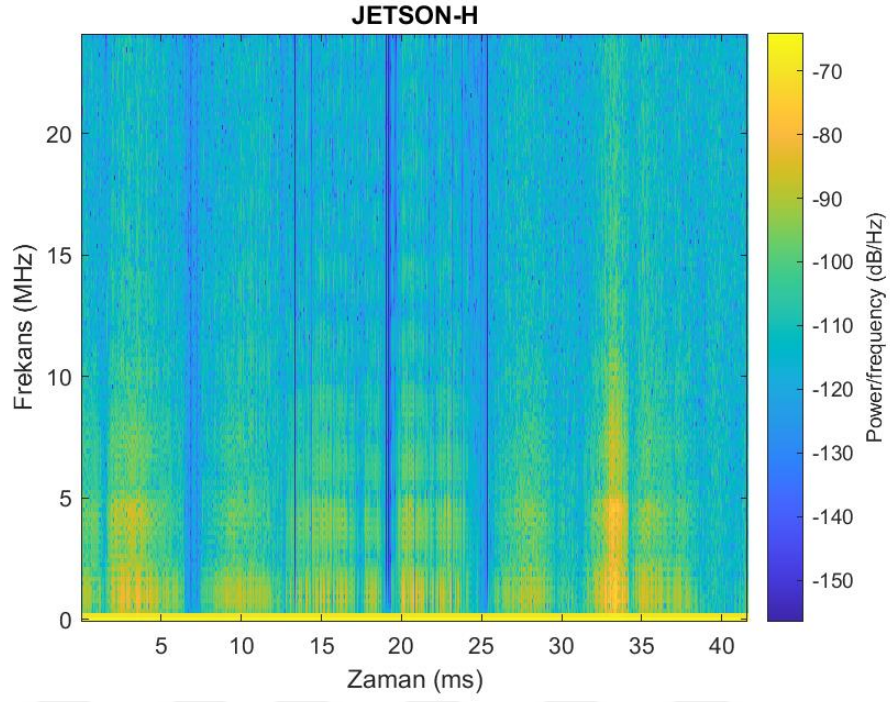
A

CİHAZLARIN ELEKTROMANYETİK SPEKTROGRAMLARI









TEZDEN ÜRETİLMİŞ YAYINLAR

Konferans Bildirileri

1. F. H. Sakacı and T. Yıldırım, "Uniquely Identifying Device Fingerprint via Deep Learning over Ethernet Communication Signals," 2023 14th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Türkiye, 2023, pp. 1-5, doi: 10.1109/ELECO60389.2023.10416037.

Patentler

1. Sakacı, F.H., Yıldırım, T., Özçelik, M.O., Solmaz, M., 2024. İletilen Elektromanyetik Emisyon Üzerinden Cihaz Kimliğinin ve Parmak İzinin Çıkarılması. 2023/006702.

Makaleler

1. F. H. Sakacı and T. Yıldırım, Oct. 2024, "Conducted Emission signal-based identification and real-time hardware security with deep learning," Eng Appl Artif Intell, vol. 136, p. 109025.

Projeler

1. Ethernet Sinyali Üzerinden Cihaz Kimliğinin ve Parmak İzinin Bulunması, Furkan Hasan Sakacı, Tülay Yıldırım, TÜBİTAK 1002A 123E010, 15/04/2023-15/04/2024, proje yürütücüsü.