TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

DERİN ÖĞRENME YÖNTEMLERİYLE İMZA SAHTECİLİĞİNİN TESPİTİ

Mehmet Türkay YOLDAR

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
KRİMİNALİSTİK PROGRAMI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Nergis CANTÜRK

ANKARA
2024

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

DERİN ÖĞRENME YÖNTEMLERİYLE İMZA SAHTECİLİĞİNİN TESPİTİ

Mehmet Türkay YOLDAR

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
KRİMİNALİSTİK PROGRAMI
YÜKSEK LİSANS TEZİ

DANIŞMAN
Prof. Dr. Nergis CANTÜRK
İKİNCİ DANIŞMAN
Prof. Dr. Recep ERYİĞİT

ANKARA
2024

ETİK BEYAN

Ankara Üniversitesi

Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum "Derin Öğrenme Yöntemleriyle İmza Sahteciliğinin Tespiti" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Mehmet Türkay YOLDAR

Tarih:

İmza:

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Kriminalistik Programında
Mehmet Türkay YOLDAR tarafından hazırlanan
"DERİN ÖĞRENME YÖNTEMLERİYLE İMZA SAHTECİLİĞİNİN TESPİTİ"
adlı tez çalışması aşağıdaki jüri tarafından YÜKSEK LİSANS TEZİ olarak
OY BİRLİĞİ/OY ÇOKLUĞU ile kabul/ret edilmiştir.

Tez Savunma Tarihi: 19.07.2024

İmza
Prof. Dr. Nergis CANTÜRK
Ankara Üniversitesi
Jüri Başkanı

İmza
Prof. Dr. Sait ÖZSOY
Sağlık Bilimleri Üniversitesi
Üye

İmza
Dr. Öğr. Üyesi Yılmaz AR
Ankara Üniversitesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

İmza
Prof. Dr. Fügen AKTAN
Sağlık Bilimleri Enstitüsü Müdürü

ÖZET

Derin Öğrenme Yöntemleriyle İmza Sahteciliğinin Tespiti

Bu tez çalışmasında, adli belge incelemelerinin önemli bir ayağını oluşturan imza sahteciliği tespiti görevinin derin öğrenme yöntemleriyle gerçekleştirilmesi amaçlanmıştır. Bu amaç doğrultusunda, çeşitli derin öğrenme mimarileri (*VGG16, ResNet18, ResNet50, Inception, Xception, EfficientNet* ve *Vision Transformer*) kullanılarak farklı modeller eğitilmiştir. Modeller sıkıştırma ve uyarım dikkat mekanizması ile çok başlıklı öz dikkat mekanizması ile geliştirilmiştir. Model sonuçları *Bütünleşik Gradyanlar* yöntemi ile görselleştirilmiştir. Bu sayede modelin karar süreçleri açıklanarak alan uzmanlarına açıklanabilir ve şeffaf bir karar desteği sağlanması hedeflenmiştir.

Farklı mimarilerin karşılaştırıldığı deneylerde elde edilen bulgular farklı başarım ölçütleri ile değerlendirilmiştir. *Xception* ve *ResNet50* modelleri sırasıyla %93,19 ve %91,04 doğruluk oranı ile en yüksek başarım gösteren iki mimari olmuştur. Sonuçlar modellerin sahte imzaları tespit etmede oldukça başarılı olduğunu göstermektedir.

Veri seti büyüklüğünün model başarımına etkisi incelenmiş ve büyük veri setleriyle eğitilen modellerin genelleme yeteneğinin daha yüksek olduğu görülmüştür. Küçük veri setleriyle eğitilen modellerin aşırı öğrenme eğilimi gösterdiği ve genelleme yeteneklerinin düşük olduğu gözlemlenmiştir.

Birden fazla mukayese imzanın kullanıldığı karşılaştırma deneyleri yapılmış ve mukayese imza sayısının arttıkça başarımın yükseldiği gözlemlenmiştir. İki mukayese imzası kullanıldığında durumda doğruluk oranı %91,90 iken, beş mukayese imzası kullanıldığında bu oran %94,10'a yükselmiştir. Bu deneyde farklı birleştirme operatörlerinin etkinliği de incelenmiş, sonuçlar arasında istatistiksel olarak anlamlı bir fark bulunamamıştır.

Bu çalışmada elde edilen sonuçlar, imza sahteciliği tespitinde derin öğrenme modellerinin etkinliğini ve dikkat mekanizmalarının model başarımına olan katkısını ortaya koymaktadır. Sonuçların anlamlı bir şekilde görselleştirilebilmesi, bu tür yaklaşımların alan uzmanları tarafından kabul göreceğine işaret etmektedir. Derin öğrenme yöntemlerinin kullanımının yaygınlaşması adli belge incelemelerinde daha objektif ve güvenilir değerlendirmeler yapılmasına olanak tanıyacaktır.

Anahtar Sözcükler: Açıklanabilir Yapay Zekâ, Derin Öğrenme, Dikkat Mekanizması, İmza Sahteciliği

SUMMARY

Detection of Signature Forgery with Deep Learning Methods

In this thesis, the objective is to perform the task of signature forgery detection, a crucial step in forensic document examinations, using deep learning methods. For this purpose, different models were trained using various deep learning architectures, including *VGG16, ResNet18, ResNet50, Inception, Xception, EfficientNet,* and *Vision Transformer*. These models were enhanced with a squeeze-and-excitation attention mechanism and a multi-head self-attention mechanism. The results of the models were visualized using the *Integrated Gradients* method. This approach explains the decision processes of the model and aims to provide explainable and transparent decision support to domain experts.

The results obtained from experiments comparing different architectures were evaluated using various performance criteria. The *Xception* and *ResNet50* models were the two highest performing architectures, achieving accuracy rates of 93.19% and 91.04%, respectively. These results demonstrate the models' high effectiveness in detecting forged signatures.

The effect of data set size on model performance was examined, revealing that models trained with large data sets exhibited higher generalization ability. Conversely, models trained with small data sets tended to overfit and showed low generalization ability.

Comparison experiments were conducted using multiple reference signatures, revealing that performance improved with an increased number of reference signatures. The accuracy rate was 91.90% with two reference signatures and increased to 94.10% with five reference signatures. The effectiveness of different merging operators was also examined in this experiment, and no statistically significant difference was found between the results.

The results obtained in this study demonstrate the effectiveness of deep learning models in signature forgery detection and the contribution of attention mechanisms to model performance. The ability to visualize the results meaningfully indicates that such approaches will be accepted by experts in the field. The widespread use of deep learning methods will enable more objective and reliable evaluations in forensic document examinations.

Keywords: Attention Mechanisms, Deep Learning, Explainable Artificial Intelligence, Signature Forgery

İÇİNDEKİLER

Etik Beyan ii
Kabul ve Onay iii
Özet iv
Summary v
İçindekiler vi
Önsöz viii
Simgeler ve Kısaltmalar ix
Şekiller xii
Çizelgeler xiv

1. GİRİŞ 1
1.1. İmza 1
1.2. İmza Sahteciliği 2
1.3. İmza Sahteciliği Tespitinde Klasik Yöntemler 3
1.3.1. Klasik Yöntemlerde Karşılaşılan Problemler 4
1.4. İmza Sahteciliği Tespitinde Modern Yaklaşımlar 5
1.4.1. Tanımlamalar 5
1.4.2. Bulanık Modelleme ve Destek Vektör Makineleri 6
1.4.3. Derin Sinir Ağları 7
1.4.4. Dikkat Mekanizmaları 11
1.4.5. Açıklanabilir Yapay Zekâ 12
1.5. Tezin Amacı ve Katkısı 13

2. GEREÇ ve YÖNTEM 15
2.1. Veriler 15
2.1.1. Veri Seti 15
2.1.2. Veri Ön İşleme 16
2.1.3. Veri Zenginleştirme 17
2.1.4. İmza Setlerinin Hazırlanması 18
2.1.4.1. İkili İmza Setleri 18
2.1.4.2. Üçlü İmza Setleri 19
2.2. Derin Öğrenme Teknikleri 19
2.2.1. İkiz Sinir Ağları 20
2.2.2. Kayıp Fonksiyonları 21
2.2.2.1. Karşıt Kayıp Fonksiyonu 21
2.2.2.2. Üçlü Kayıp Fonksiyonu 22
2.2.3. Derin Öğrenme Mimarileri 23
2.2.3.1. VGG16 24
2.2.3.2. ResNet18 24
2.2.3.3. ResNet50 24
2.2.3.4. Inception (v4) 24
2.2.3.5. Xception 24
2.2.3.6. EfficientNet (B0) 25
2.2.3.7. Vision Transformer 25
2.2.4. Dikkat Mekanizmaları 25
2.2.4.1. Sıkıştırma ve Uyarım Dikkat Mekanizması 25
2.2.4.2. Öz Dikkat Mekanizması 26
2.2.4.3. Çok Başlıklı Öz Dikkat 27
2.2.5. Dikkat Mekanizmalarının Mimarilere Eklenmesi 27
2.2.6. Görselleştirme Teknikleri 28
2.2.6.1. Grad-CAM 28
2.2.6.2. Bütünleşik Gradyanlar 29
2.3. Sıralı Ağırlıklı Ortalama Operatörü 29

2.4. Deneyler 30
2.4.1. Mimarilerin Başarımlarının Karşılaştırılması 30
2.4.2. Veri Seti Büyüklüğünün Başarıma Etkisi 31
2.4.3. Çoklu İmza Karşılaştırmaları 31
2.4.4. Sonuçların Görselleştirilmesi 32
2.5. Başarım Değerlendirme Yöntemleri 32
2.6. Kullanıcı Arayüzü 33
2.7. Geliştirme ve Test Ortamı 35

3. BULGULAR 36
3.1. Veri Hazırlığı 36
3.2. Mimari Başarımlarının Karşılaştırılması 36
3.2.1. VGG16 38
3.2.2. ResNet18 39
3.2.3. ResNet50 40
3.2.4. Inception 41
3.2.5. Xception 43
3.2.6. EfficientNet 44
3.2.7. Vision Transformer 45
3.2.8. Tüm Mimarilerin Karşılaştırılması 47
3.3. Veri Seti Büyüklüğünün Başarıma Etkisi 48
3.4. Çoklu İmza Karşılaştırmaları 50
3.5. Sonuçların Görselleştirilmesi 51
3.5.1. Gerçek Pozitif Örnekler 52
3.5.2. Gerçek Negatif Örnekler 52
3.5.3. Yanlış Pozitif Örnekler 53
3.5.4. Yanlış Negatif Örnekler 54

4. TARTIŞMA 55
5. SONUÇ ve ÖNERİLER 60
KAYNAKLAR 62
ÖZGEÇMİŞ 68

ÖNSÖZ

Bu tez çalışmasında imza sahteciliği tespiti için derin öğrenme yöntemlerinin uygulanması ele alınmıştır. Çalışma kapsamında farklı derin öğrenme mimarileri kullanılarak modeller eğitilmiştir. Modellerin performansını artırmak amacıyla kullanılan mimarilere dikkat mekanizması eklenmiştir. Model çıktıları *Bütünleşik Gradyanlar* yöntemiyle görselleştirilmiştir. Bu sayede modellerin karar verme süreçleri açıklanarak, adli belge inceleme uzmanlarına şeffaf ve anlaşılabilir bir karar destek sistemi sunulması hedeflenmiştir. Çalışma derin öğrenme modellerinin imza sahteciliği tespitinde etkin olduğunu, dikkat mekanizmalarının model başarımına ve açıklanabilirliğine katkı sağladığını ortaya koymuştur.

Çalışmalarım boyunca yardım ve desteğini esirgemeyen, kıymetli tecrübelerinden faydalandığım danışmanım Prof. Dr. Nergis CANTÜRK'e teşekkürlerimi sunarım.

Çalışmanın her aşamasında bilgi ve deneyimleriyle çalışmaya yön veren Prof. Dr. Recep ERYİĞİT'e içtenlikle teşekkür ederim.

Tecrübelerini paylaşmaktan çekinmeyen değerli mesai arkadaşlarım Yiğit Burak AKKAŞ'a ve Oğuzcan TURAN'a teşekkür ederim.

Tez süreci boyunca manevi desteğiyle beni hiçbir zaman yalnız bırakmayan çok değerli eşim Zeynep AKKUTAY YOLDAR'a tüm kalbimle çok teşekkür ederim.

SİMGELER VE KISALTMALAR

2C2S	İki Kanallı ve İki Akışlı Dönüştürücü
α	İntegral Sabiti (Bütünleşik Gradyanlar Fonksiyonu)
α	Marjin Değeri (Üçlü Kayıp Fonksiyonu)
A	Referans Örnek
AVG	Ortalama Operatörü
AVN	Çekişmeli Varyasyon Ağı
CEDAR	İmza Veri Seti
CNN	Evrişimli Sinir Ağları
δ	ReLU Aktivasyon Fonksiyonu
D	İki Özellik Vektörü Arasındaki Öklid Mesafesi
DCSNN	Derin Evrişimli İkiz Sinir Ağı
d_k	Anahtar Boyutu
dpi	İnç Başına Düşen Nokta Sayısı
DRT	Aralıklı Radon Dönüşümü
EER	Eşit Hata Oranı
F_1	F_1 Değeri (Hassasiyet ve Hatırlama Değerlerinin Harmonik Ortalaması)
F_{ex}	Uyarım Fonksiyonu
f_i	Özellik Vektörü (i'inci İmzaya Ait)
FN	Yanlış Negatif
FP	Yanlış Pozitif
F_{scale}	Ölçeklendirme Fonksiyonu
F_{sq}	Sıkıştırma Fonksiyonu
GPDS	İmza Veri Seti
Grad-CAM	Gradyan Ağırlıklı Sınıf Aktivasyon Haritalaması
H	Uzaysal Boyut (Yükseklik)
IG	Bütünleşik Gradyanlar

I_i	Karşılaştırılacak İmzalardan i'incisi
K	Anahtar Matrisi
k	Çapraz Doğrulama Kat Sayısı
L	Kayıp Fonksiyonu
LSTM	Uzun Kısa Süreli Hafıza
m	Marjin Değeri (Karşıt Kayıp Fonksiyonu)
MA-SCN	Çok Yollu Dikkat Mekanizmalı İkiz Evrişim Ağı
MSN	Çoklu İkiz Sinir Ağı
N	Negatif Örnek
OCSVM-GA	Genetik Algoritma Temelli Sınıf Destek Vektör Makinesi
OWA	Sıralı Ağırlıklı Ortalama Operatörü
P	Pozitif Örnek
PCA	Ana Bileşen Analizi
PNN	Olasılıksal Sinir Ağı
Q	Sorgu Matrisi
σ	Sigmoid Aktivasyon Fonksiyonu
s	Ölçekleme Vektörü
s_c	Ağırlık (c'inci kanala ait)
SE	Sıkıştırma ve Uyarım
SNN	İkiz Sinir Ağları
ST-ATT	Dikkat Yönlendirmeli Mekânsal-Zamansal Sinir Ağı
SVM	Destek Vektör Makinesi
TN	Gerçek Negatif
TP	Gerçek Pozitif
U	Girdi Özelliği Haritası
U_c	Girdi Özelliği Haritası (c'inci kanala ait)
V	Değer Matrisi
ViT	Vision Transformer
W	Uzaysal Boyut (Genişlik)

W^K	Öğrenilebilir Ağırlık Matrisi (Anahtar)
W^O	Son Ağırlık Matrisi
W^Q	Öğrenilebilir Ağırlık Matrisi (Sorgu)
W^V	Öğrenilebilir Ağırlık Matrisi (Değer)
XAI	Açıklanabilir Yapay Zekâ
X_c	Ölçeklendirilmiş Özellik Haritası
Y	Etiket Değeri
YKO	Yanlış Kabul Oranı
YRO	Yanlış Ret Oranı
z	Sıkıştırılmış Vektör

ŞEKİLLER

Şekil 2.1. CEDAR veri setinde yer alan imzalardan bazı örnekler 16
Şekil 2.2. Farklı ön işleme yöntemlerinin imzalara uygulanması 17
Şekil 2.3. Farklı veri zenginleştirme yöntemlerinin imzalara uygulanması 18
Şekil 2.4. Üçlü imza seti 19
Şekil 2.5. Özellik vektörleri 20
Şekil 2.6. Öklid mesafesi 20
Şekil 2.7. Karar fonksiyonu 21
Şekil 2.8. İkiz sinir ağı mimarisinin imza sahteciliğinde kullanımı 21
Şekil 2.9. Karşıt kayıp fonksiyonu 22
Şekil 2.10. Üçlü kayıp fonksiyonu 22
Şekil 2.11. Üçlü kayıp fonksiyonu ile mesafelerin ayarlanması 23
Şekil 2.12. Sıkıştırma fonksiyonu 26
Şekil 2.13. Uyarım fonksiyonu 26
Şekil 2.14. Yeniden ölçekleme fonksiyonu 26
Şekil 2.15. Sorgu, anahtar ve değer matrisleri 26
Şekil 2.16. Dikkat fonksiyonu 27
Şekil 2.17. Tek bir başlık için dikkat fonksiyonu 27
Şekil 2.18. Çok başlıklı dikkat fonksiyonu 27
Şekil 2.19. Bütünleşik Gradyan fonksiyonu 29
Şekil 2.20. Sıralı ağırlıklı ortalama operatörü 29
Şekil 2.21. Model eğitim sürecinin akış şeması 31
Şekil 2.22. Doğruluk 32
Şekil 2.23. Hassasiyet 32
Şekil 2.24. Hatırlama 33
Şekil 2.25. F_1 Değeri 33
Şekil 2.26. Yanlış kabul oranı 33
Şekil 2.27. Yanlış ret oranı 33
Şekil 2.28. Kullanıcı arayüzü 34
Şekil 2.29. İki aynı imzanın karşılaştırılması 35
Şekil 3.1. Veri setinin k-katlamalı çapraz doğrulama için bölünmesi 37
Şekil 3.2. VGG16 modelinin eğitim ve doğrulama sürecinde başarımının değişimi 38
Şekil 3.3. ResNet18 modelinin eğitim ve doğrulama sürecinde başarımının değişimi 39
Şekil 3.4. ResNet50 modelinin eğitim ve doğrulama sürecinde başarımının değişimi 40
Şekil 3.5. Inception modelinin eğitim ve doğrulama sürecinde başarımının değişimi 42
Şekil 3.6. Xception modelinin eğitim ve doğrulama sürecinde başarımının değişimi 43

Şekil 3.7. EfficientNet modelinin eğitim ve doğrulama sürecinde başarımının değişimi 44
Şekil 3.8. Vision Transformer modelinin eğitim ve doğrulama sürecinde başarımının değişimi 46
Şekil 3.9. Eğitilen tüm mimarilerin doğruluk ve F_1 değeri üzerinden karşılaştırılması 48
Şekil 3.10. %60'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi 49
Şekil 3.11. %40'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi 49
Şekil 3.12. %20'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi 49
Şekil 3.13. Modelin çıktısının gerçek pozitif olduğu bir örnek (1) 52
Şekil 3.14. Modelin çıktısının gerçek pozitif olduğu bir örnek (2) 52
Şekil 3.15. Modelin çıktısının gerçek pozitif olduğu bir örnek (3) 52
Şekil 3.16. Modelin çıktısının gerçek negatif olduğu bir örnek (1) 53
Şekil 3.17. Modelin çıktısının gerçek negatif olduğu bir örnek (2) 53
Şekil 3.18. Modelin çıktısının gerçek negatif olduğu bir örnek (3) 53
Şekil 3.19. Modelin çıktısının yanlış pozitif olduğu bir örnek (1) 53
Şekil 3.20. Modelin çıktısının yanlış pozitif olduğu bir örnek (2) 53
Şekil 3.21. Modelin çıktısının yanlış pozitif olduğu bir örnek (3) 54
Şekil 3.22. Modelin çıktısının yanlış negatif olduğu bir örnek (1) 54
Şekil 3.23. Modelin çıktısının yanlış negatif olduğu bir örnek (2) 54
Şekil 3.24. Modelin çıktısının yanlış negatif olduğu bir örnek (3) 54

ÇİZELGELER

Çizelge 2.1. İkili set sayıları 19
Çizelge 2.2. Üçlü set sayıları 19
Çizelge 2.3. Başlıca derin öğrenme mimarileri ve teknik özellikleri 23
Çizelge 2.4. Dikkat mekanizmalarının uygulandığı katmanlar 28
Çizelge 3.1. VGG16 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 38
Çizelge 3.2. VGG16 modeli için test sonucunda elde edilen başarım ölçütleri 39
Çizelge 3.3. ResNet18 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 39
Çizelge 3.4. ResNet18 modeli için test sonucunda elde edilen başarım ölçütleri 40
Çizelge 3.5. ResNet50 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 41
Çizelge 3.6. ResNet50 modeli için test sonucunda elde edilen başarım ölçütleri 41
Çizelge 3.7. Inception mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 42
Çizelge 3.8. Inception modeli için test sonucunda elde edilen başarım ölçütleri 42
Çizelge 3.9. Xception mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 43
Çizelge 3.10. Xception modeli için test sonucunda elde edilen başarım ölçütleri 44
Çizelge 3.11. EfficientNet mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri 45
Çizelge 3.12. EfficientNet modeli için test sonucunda elde edilen başarım ölçütleri. 45
Çizelge 3.13. Vision Transformer mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri46
Çizelge 3.14. Vision Transformer modeli için test sonucunda elde edilen başarım ölçütleri 46
Çizelge 3.15. Farklı modellerin doğrulama sürecinde elde ettikleri başarım ölçütleri 47
Çizelge 3.16. Farklı modellerin test verisi üzerinde elde ettikleri başarım ölçütleri 48
Çizelge 3.17. Modellerin doğrulama sürecinde elde ettikleri başarım ölçütleri 50
Çizelge 3.18. Modellerin test verisi üzerinde elde ettikleri başarım ölçütleri 50
Çizelge 3.19. Çoklu imza karşılaştırmaları sonuçları 51

1. GİRİŞ

Günümüzde imza hem bireysel kimlik doğrulama hem de belgelerin yasal geçerliliğinin sağlanmasında kritik bir rol oynamaktadır. İmzanın benzersiz yapısı imzalayan kişinin kimliğini ve belgenin onayını güvence altına alırken, imza sahteciliği ve sahte imzaların tespiti önemli bir sorun olarak karşımıza çıkmaktadır. İmza şahısların kimliğini tespit etmeye yarayan önemli bir delildir. Ancak bazı fiziksel delillerin aksine, imzalar tek ve benzersiz özellikte olmayabilir; değişebilir ve değiştirilebilir niteliktedir (Birincioğlu ve Özkara, 2010).

Adli belge incelemelerinin önemli bir kısmını el yazıları ve el yazısı imzalar oluşturmaktadır (Birincioğlu ve Özkara, 2010). İncelenen belge sayısının yıl içinde yüz binleri aştığı bilinmektedir. İmzaların basit tersimli olmaları nedeniyle aidiyetin tespit edilemediği durumlar olduğu gibi, aynı şahsa ait imzaların farklılık gösterdiği durumlar da oldukça yaygındır (Yolcu vd., 2010). Bu nedenle, adli belge inceleme süreci oldukça subjektif olup, iki uzmanın görüşü farklılık gösterebilmektedir.

Özellikle imza sahteciliğinin belirlenmesinde objektif bir yöntem geliştirilmesi için bilgisayar destekli çözümler uzun bir süredir geliştirilmektedir. Bu çalışmada derin öğrenme yöntemleri ile imza sahteciliği tespiti amaçlanmış ve tespit sonuçlarının uzmanların doğru karar vermesine yardımcı olacak şekilde açıklanabilir hale getirildiği bir yöntem önerilmiştir.

Bu bölümde kavramsal çerçeve ve ilgili literatür sunulmakta, ardından tezin amacı ve katkısından bahsedilmektedir.

1.1. İmza

İmza, kişinin herhangi bir belgeyi yazdığını ya da onayladığını gösteren, 2525 sayılı Soyadı Kanunu'nun 2. maddesine göre adın önde, soyadın sonda yer aldığı bir işarettir. İmza kelimesi, dilimize Arapça ya da Farsçadan geçmiş olabileceği gibi, “İm” (işaret, iz) köküne dayalı bir Türkçe köken de mümkündür.

El yazısı imzalar, iş anlaşmaları, sözleşmeler ve diğer resmî belgeleri tamamlamada uzun yıllardır önemli bir rol oynamaktadır. İmzanın belirginliği, imzalayan kişinin kimliğini kanıtlamaya yardımcı olurken, bir belgenin imzalanması, imzalayan kişinin şartlarını kabul ettiğini ve belgenin imzalandığı anda resmi ve tamamlanmış olduğunu gösterir (Hanmandlu vd., 2005). İmzalar yüzyıllardır bir kişinin kimliğini doğrulamada önemli bir unsur olarak

kullanılmaktadır. Bir kişinin benzersiz imza özellikleri, kişinin kimliğini ve belgenin şartlarını kabul ettiğini temsil eder (Prakash ve Sharma, 2014).

Aydoğdu ve Ataç (2011) imzaların atılış şekillerine göre üçe ayrıldığını belirtmiştir. Bunlar kişilerin ad ve soyadlarının genellikle bitişik el yazısıyla yazılması ile oluşan *yazı tarzında imzalar*; kişinin kendine has, her zaman aynı tarzda atılan, belirli bir deseni veya sembolü temsil eden *şekilsel imzalar* ve herkes tarafından kolayca taklit edilebilecek, belirgin karakteristik özellikleri olmayan *basit tersimli imzalar*dır.

El yazısı imzalar, yasal belgelerde kimlik doğrulama, kabul, bütünlük ve inkâr edememe olmak üzere dört temel işlevi yerine getirir. Kimlik doğrulama, imzalayan kişinin kimliğinin doğrulanmasına olanak tanır. Kabul, imzalayanın belgede belirtilen şartları isteyerek kabul ettiğini gösterir. Bütünlük, imzanın, imzalanmış belgenin değiştirilmediğini belirtir. İnkâr edememe, imzalayanın imzayı inkar edemeyeceği anlamına gelir (Hanmandlu vd., 2005).

Günümüzde imzaların hızlı bir şekilde doğrulanması zorunludur. Örneğin, yargı sürecinin erken aşamalarında, adli makamlar hızlı bir imza analizi yaparak davaya yön verebilir (Kao ve Wen, 2020).

El yazısı imzalar biyometrik doğrulama ve adli belge incelemelerinde önemli bir rol oynar. Finans, hukuk ve ticaret sektörlerinde sıklıkla karşılaşılan imza sahteciliği ise tespiti uzmanlık gerektiren bir alandır. Bu nedenle gerçek imzalar ile sahte imzalar arasındaki küçük detayları keşfetmek önemlidir (Xiong ve Cheng, 2021).

1.2. İmza Sahteciliği

İmza tanımlama ve sahtecilik tespiti belge inceleme alanının en zorlu ve önemli konularındandır (Herkt, 1986). Bu sürecin temel amacı, imzaların görsel ve dinamik özelliklerine dayanarak gerçek imzaları sahtelerinden ayırt edebilmektir. Otomatik imza doğrulama sistemlerinin, sahte imzaları ve deneyimli sahtekârları tespit edebilmesi bu nedenle büyük önem taşır (Brault ve Plamondon, 1993).

İmza sahteciliği çeşitli teknikler kullanılarak gerçekleşmektedir (Aydoğdu ve Ataç, 2011; Birincioğlu ve Özkara, 2010; Yalçın ve Gürbüz, 2015). Bunlardan en yaygın olanları serbest taklit, üstünden kopya, bakarak kopya, uydurma ve transfer yöntemleridir.

Serbest taklit yöntemi, sahtecinin imzayı tamamen hafızasına kazıyarak tekrar yaratma sürecidir. Bu yöntemde, yüksek görsel ve motor becerileri gerektirir; çünkü sahteci, imzanın

bütün karakteristik özelliklerini kapsamlı bir şekilde öğrenir. Sonuçta elde edilen imza, orijinal imzaya yakın olmasına rağmen, belli başlı hatalar ve düzensizlikler içerebilir (Birincioğlu ve Özkara, 2010).

Üstünden kopya yöntemi, orijinal imzanın üzerine şeffaf bir materyal konularak, alttan iz bırakacak şekilde kopyalanması işlemidir. Bu teknik oldukça düşük bir beceri gerektirir ve genellikle orijinal imzadaki doğal doku ve hat detaylarını yakalayamaz. Bu nedenle imzanın kötü bir kopyası çoğunlukla kolaylıkla fark edilir (Aydoğdu ve Ataç, 2011).

Bakarak kopya yöntemi, sahtecinin orijinal imzayı gözlemleyerek onu kopyalama çabasıdır. Bu süreçte, orijinal imzayı bir şablona veya önüne koyarak, her bir detayı gözlem altına alır. Bu yöntem, orijinal imza üzerindeki ince detayları yakalamada zorlanır ve sıklıkla imza akıcılığını kaybeder, sonuçta mekanik ve titrek bir görünüm ortaya çıkar (Aydoğdu ve Ataç, 2011).

Uydurma imzalar genellikle gerçek bir imza örneği olmadan oluşturulur. Bu tür sahteciliklerde, taklitçi, imza sahibinin ismini ve belki de bazı karakteristik harf biçimlerini kullanarak kendi versiyonunu yaratır. Ancak, gerçek imzayla uydurma imza arasındaki benzerlikler genellikle sınırlıdır ve detaylı bir inceleme kolayca farklılıkları ortaya çıkarabilir (Aydoğdu ve Ataç, 2011).

Transfer yöntemi, orijinal imzanın başka bir belgeye kopyalanması için dijital veya fotografik yöntemlerin kullanılmasıdır. Bu yöntem, özellikle resmî belgelerin manipüle edilmesinde kullanılır. Transfer edilmiş imzalar, orijinalinin bir kopyası olarak görünebilir, ancak kâğıt, mürekkep ve bası kalitesindeki farklılıklar, detaylı bir incelemeyle tespit edilebilir (Yalçın ve Gürbüz, 2015).

1.3. İmza Sahteciliği Tespitinde Klasik Yöntemler

İmza doğrulama ve sahtecilik tespiti, adli incelemelerde önemli bir yer tutmaktadır. Bir kişinin kimliğini doğrulamak ve belgelerin güvenliğini sağlamak için hayati öneme sahiptir. El yazısı imzalar kişiden kişiye büyük farklılıklar gösterir ve bu farklılıklar, imzanın sahte olup olmadığını anlamayı kolaylaştırabileceği gibi, zorlaştıra da bilir (Prakash ve Sharma, 2014). İmzanın temel bir özelliği, imza atan kişinin imzasını iki ayrı durumda tamamen aynı şekilde tekrarlamasının imkansız olmasıdır. Bu olgu doğal varyasyon olarak adlandırılır. Buna karşılık uzmanlar, her yönüyle paralel ve örtüşen iki imzanın varlığını sahte imzanın göstergesi olarak kabul etmektedir (Sayıcı, 2009).

İmza analizi iki ana yöntemle gerçekleştirilir. Statik analiz tamamlanmış bir imzanın kâğıda yansıyan hali üzerinden, çizgilerin uzunluğu, eğimi ve genişliği gibi geometrik özellikleri değerlendirir. Dinamik analiz ise imzanın oluşum sürecini mercek altına alır; bu süreçte kalem basıncı, yazma ritmi ve hareket yönü gibi dinamik faktörler analiz edilir (Gideon vd., 2018; Yusof ve Madasu, 2003).

İmza sahteciliği tespitinde kullanılan klasik yöntemler, imzanın fiziksel ve görsel özelliklerinin incelenmesine dayanır. İncelemeler genellikle adli belge inceleme uzmanları tarafından gerçekleştirilir. Görsel karşılaştırma, sahte imzanın orijinal imza ile şekil, boyut, eğim ve harflerin bağlanma şekli gibi unsurlar üzerinden incelenmesini içerir. Mikroskobik inceleme ise imzanın kalem basıncı, mürekkep dağılımı ve kâğıt üzerindeki izlerin detaylı analizini kapsar. Büyüteç kullanımı ile imzanın küçük farklılıkları tespit edilir, şeffaf kopyalar üst üste bindirilerek iki imza arasındaki farklılıklar belirginleştirilir. Basınç analizi, kaligrafik inceleme ve belirgin özelliklerin incelenmesi gibi yöntemlerle de imzanın orijinalliği değerlendirilir. Bu işlemlerin gerçekleştirilmesi için yıllar içinde farklı türde süreç, teknik ve cihazlar geliştirilmiştir.

Klasik yöntemlerin en büyük artısı, yıllar içinde defalarca test edilmiş olmalarıdır. Ayrıca, çoğu zaman ek bir donanım olmadan da uygulanabilirler. Bu yöntemler karmaşık sahtecilik tekniklerini belirlemede zayıf kalabilirler. Aynı zamanda alanında uzman personel ihtiyacı bu tekniklerin uygulanmasını zaman ve maliyet bakımından artırır. Adli belge incelemeleri, genellikle eğitimli uzmanlar tarafından yapılır ve sonuç büyük ölçüde uzmanların deneyim ve bilgi birikimine dayanır (Kao ve Wen, 2020).

1.3.1. Klasik Yöntemlerde Karşılaşılan Problemler

Klasik imza tespit yöntemlerinde karşılaşılan problemler arasında sübjektiflik, yeterli örnek eksikliği, detaylı analiz gerekliliği, fiziksel izlerin incelenmesindeki zorluklar ve teknolojiye erişilebilirlik bulunur. Uzmanların kişisel deneyimlerine dayalı değerlendirmeleri tutarsızlıklara yol açabilir. Yeterli sayıda orijinal imza örneğinin bulunmaması ve detaylı analizlerin zaman alıcı olması da diğer önemli sorunlardır. Ayrıca, imza atılırken kullanılan kalemin basıncı ve mürekkep dağılımı her zaman net olmayabilir, bu da doğru yorum yapmayı zorlaştırır. Klasik yöntemlerin genellikle insana bağımlı süreçler olması hata payını artırır. Bu sorunlar imza sahteciliğinin tespitinde güvenilirliği azaltabilir. İmza doğrulama sistemleri gibi modern teknolojik yöntemler ve cihazlar ise her zaman erişilebilir olmayıp, onlar da hataya açıktır.

İmza doğrulama sistemlerinin başarımının bozulmasının ana nedenlerinden biri istikrarsız ve kolay taklit edilebilen imzalardır. İmza doğrulama sistemlerinin çalışmasının, imzaların değişmez (değişken olmayan) özelliklerine dayanması gerektiği belirtilmiştir (Brault ve Plamondon, 1993). Fakat bu özellikleri belirlemek her zaman kolay olmayabilir. Daha da önemlisi farklı yazı stilleri nedeniyle, tüm imza sahiplerine uyan tek bir küresel eşik değeri belirlemek mümkün değildir (Deng vd., 2003).

İmza doğrulama görevinde en büyük zorluklardan bir diğeri ise aynı kullanıcının imzaları arasında yüksek değişkenlik olmasıdır. Bu durum özellikle yetenekli sahte imzalar için daha da zorlayıcıdır çünkü bu sahte imzalar gerçek imzalara büyük ölçüde benzemektedir (Hafemann vd., 2017).

Mukayese imza sayısının yetersiz kaldığı durumlarda da bu sistemlerin başarımı tartışılmaktadır. Sınırlı sayıdaki örneklerden faydalı öznitelikler çıkarmak zorlayıcı bir işlemdir (Kao ve Wen, 2020).

1.4. İmza Sahteciliği Tespitinde Modern Yaklaşımlar

Bilgisayar destekli imza sahteciliği tespit yöntemleri sahte imzaların tespiti için çeşitli algoritmalar ve modeller kullanır. Bu yöntemler arasında bulanık modelleme, destek vektör makineleri, derin sinir ağları ve dikkat mekanizmaları gibi ileri teknikler bulunmaktadır. Özellikle derin öğrenme tabanlı yöntemler imza sahteciliği tespitinde büyük ilerlemeler kaydetmiştir. Derin sinir ağları ham veri üzerinde çalışarak öznitelik çıkarımını kendisi yapar. Bu yöntemler imzaların statik veya dinamik olarak incelenmesini sağlar.

1.4.1. Tanımlamalar

İmza sahteciliği tespitinde literatürde birçok çalışma bulunmaktadır. Bu çalışmalarda farklı yöntem ve analizlerin birbirinden ayrılması amacıyla birçok terim kullanılmaktadır (Hafemann vd., 2017). Bu terimlerden sıkça karşılaşılanlar bu bölümde yer almaktadır.

Çevrimdışı İmza; kâğıt üzerine atılan ve daha sonra tarayıcı ile dijital ortama aktarılan, sadece statik görüntüden oluşan imzadır.

Çevrimiçi İmza; bir dijital cihaz veya tablet üzerinde imza atılırken kaydedilen basınç, hız, yön gibi dinamik bilgileri içeren imzadır.

Statik Analiz; imzanın kâğıt üzerindeki hali üzerinden yapılan çizgi uzunluğu, eğim, genişlik gibi geometrik özelliklerin değerlendirilmesi işlemidir.

Dinamik Analiz; imzanın atılma sürecindeki hareket bilgilerini inceleyen analiz yöntemidir.

El ile Tasarlanmış Öznitelik Çıkarımı; uzmanların öznel algıya dayalı olarak belirli özellikleri tanımladığı yöntemdir.

Kendiliğinden Öznitelik Öğrenme; derin öğrenme algoritmalarının verilerden kendi kendine özellik çıkarma yeteneğidir.

Yazar Bağımlı Sistem; her kullanıcı için ayrı bir modelin eğitildiği imza doğrulama sistemidir.

Yazar Bağımsız Sistem; tüm kullanıcılar için tek bir modelin eğitildiği ve farklı kullanıcı kümeleri üzerinde test edilen imza doğrulama sistemidir.

1.4.2. Bulanık Modelleme ve Destek Vektör Makineleri

Veriler arasındaki belirsizlikleri yönetmek için bulanık mantık kullanan modelleme yöntemi olan bulanık modelleme, derin öğrenme yöntemlerinin yaygınlaşmadığı dönemde imza doğrulama görevi için oldukça kullanışlı bulunmuş ve farklı çalışmalar yapılmıştır. Destek vektör makineleri de yüksek doğruluk oranları sunarak ve farklı veri setleri üzerinde etkili bir şekilde çalışarak imza doğrulama görevlerinde kullanılmaktadır. Bu yöntemler genellikle basit, anlaşılır ve uygulanabilirdir.

Yusof ve Madasu (2003), bulanık modellemeye dayalı bir imza doğrulama ve sahtecilik tespit sistemi tanıtmışlardır. İmza görüntüleri ikili hale getirilir, sabit boyutlu bir pencereye göre yeniden boyutlandırılır ve inceltilir. İnceltildikten sonra, yatay yoğunluk yaklaşımla sekiz alt resimden oluşan kutulara bölünür. Her bir alt resim daha sonra yeniden boyutlandırılır ve eşit bölme yaklaşımı ile on iki alt resme bölünür. Her kutudan çıkarılan özellikler, örnek imzalardan alınan özellikler ile, yapısal parametrelerle uyarlanabilir bir yeni bulanıklaştırma fonksiyonu kullanılarak bulanık kümeler oluşturur. Hazırlanan sistem Takagi–Sugeno modelini temel almakta ve yüksek başarım göstermektedir.

Hanmandlu vd. (2005) otomatik çevrimdışı imza doğrulama ve sahtecilik tespiti konusuna yoğunlaşmışlardır. Kullandıkları yöntem Takagi–Sugeno modelini temel alan bulanık modellemeye dayanmaktadır. Çalışmada çoklu kural içeren modelin tek kural içeren modele göre daha üstün olduğu gözlemlenmiştir.

Madasu ve Lovell (2008) bulanık modelleme temelli bir çevrimdışı imza doğrulama ve sahtecilik tespit sistemi üzerine çalışmışlardır. Çeşitli el yazısı imza özellikleri incelenmiş ve kararlı bir doğrulama sistemi oluşturmak için bu özellikler dikkate alınmıştır. Gerçek imzaların doğrulanması ve sahteciliklerin tespiti, bir ızgara yöntemi kullanılarak çıkarılan açı özellikleri aracılığıyla gerçekleştirilmiştir. Önerilen sistemin etkinliği kendi oluşturdukları büyük bir imza veri tabanında test edilmiştir.

Ghanim ve Nabil (2018) çevrimdışı imza doğrulama ve sahtecilik tespiti konusuna yoğunlaşmış ve farklı özniteliklerin sistemin tanıma yeteneği üzerindeki etkisini raporlamışlardır. Kullandıkları yöntemler arasında öbekleme ağacı, rastgele orman ve Destek Vektör Makinesi (SVM) bulunmakta olup, SVM Gradyan Histogramı özellikleri üzerinde diğer sınıflandırıcılardan daha üstün başarım gösterdiği değerlendirilmiştir. Her ne kadar bu çalışma bulanık modelleme ile ilgili olmasa da öznitelik çıkarımının sonuçlara nasıl etki ettiğini göstermesi açısından önemlidir.

Abdulhussien vd. (2023) imza doğrulama sistemlerinde özellik çıkarımı ve sınıflandırmanın zorluklarına odaklanmış ve bu problemleri çözmek için genetik algoritma temelli bir sınıf destek vektör makinesi modeli (OCSVM-GA) önermişlerdir. Dengesiz imza verisiyle başa çıkmak için dört ana adım içeren bu yöntem, kıyaslandığı diğer yöntemlere göre daha iyi sonuçlar vermektedir.

Bu yöntemlerin karmaşık el ile tasarlanmış öznitelik çıkarım ve modelleme süreçleri gerektirdiği ve genellikle belirli parametrelerin elle ayarlanması gerektiği gözlemlenmiştir. Bulanık modelleme yöntemlerinin karmaşık ve büyük veri setlerini işleme kapasitesinin de sınırlı olması daha yüksek doğruluk ve genelleme yeteneği sunan yeni çözümlere geçilmesine neden olmuştur. Derin sinir ağları bu süreçleri daha az insan müdahalesi ile daha kapsamlı bir şekilde gerçekleştirebilmektedir.

1.4.3. Derin Sinir Ağları

Makine öğreniminin bir alt dalı olan derin öğrenme, özellikle görüntü tanıma ve sınıflandırma gibi konularda başarılı sonuçlar elde etmektedir (LeCun vd., 2015). Derin öğrenme çok katmanlı yapay sinir ağların üzerinde çalışır ve bu katmanlar verilerdeki öznitelikleri kendiliğinden öğrenme yeteneğine sahiptir. Donanım alanında yaşanan teknolojik gelişme, görüntü işlem birimlerinin yaygınlaşması ve büyük veri setleri üzerinde işlem yapabilme, derin sinir ağlarında bir atılım gerçekleşmiştir (Shrestha ve Mahmood, 2019). Derin öğrenmenin gösterdiği yüksek başarım, bu yöntemlerin imza sahteciliği tespiti alanında da kullanılmasını

kaçınılmaz hale getirmiştir. Bu alanda yapılan birçok çalışma, derin öğrenmenin el ile tasarlanmış öznitelik çıkarımı gerektirmeyen çok katmanlı yapısıyla karmaşık ve doğrusal olmayan fonksiyonları haritalayabilme yeteneğinin, imza sahteciliği tespiti için de son derece uygun olduğunu göstermektedir (Hafemann vd., 2017). Her ne kadar derin öğrenme algoritmaları yüksek başarım gösterse de tüm imzaların benzersiz ve karmaşık doğası, bu alanda özelleştirilmiş yöntemler üzerinde daha fazla çalışma yapılmasına yol açmıştır.

Ribeiro vd. (2011) yaptıkları çalışmada çevrimdışı imza tanıma için derin öğrenme ağlarını incelemişlerdir. Biyometri alanında, imzaların bireyin psikolojik faktörlerine bağlı olarak değişebilmesi nedeniyle bu görev zorlayıcı bir bilgisayar görüşü problemi olarak kabul edilmiştir. Çalışmada yüksek seviyeli öznitelikleri çıkartabilen imza tanıma için bir derin öğrenme modeli geliştirilmiştir. Aynı zamanda yanlış sınıflandırma oranını iyileştiren iki aşamalı bir hibrit model de önerilmiştir.

Ooi vd. (2016) çevrimdışı imza doğrulaması konusuna yoğunlaşmış ve statik imza görsellerinden dinamik bilgi eksikliğini göz önüne alarak, Aralıklı Radon Dönüşümü (DRT), Ana Bileşen Analizi (PCA) ve olasılıksal sinir ağı (PNN) hibrit yöntemlerini önermişlerdir. Bu yöntemler resim seviyesine dayanarak sahte imzaları gerçek imzalardan ayırt etmeyi amaçlamaktadır. Çalışma sonucunda rastgele, gündelik ve uzman sahtecilikler için sırasıyla %1,51, %3,23 ve %13,07 eşit hata oranları (EER) rapor etmişlerdir.

Hafemann vd. (2017) el yazısıyla atılan imzanın doğrulama yöntemlerini ele almışlardır. Özellikle imzanın dinamik bilgisinin olmadığı durumlarda bu doğrulamanın zorlayıcı olduğunu belirtmişlerdir. Son yıllarda derin öğrenme yöntemlerinin imza görüntülerinden öznitelik çıkarmak için nasıl kullanıldığına dikkat çekmişlerdir. Öznitelik çıkarma yöntemleri, küresel ve yerel öznitelikler olarak ikiye ayrılır. Küresel öznitelikler imza görüntüsünün tamamını tanımlarken, yerel öznitelikler görüntüyü parçalara ayırarak her bir bölümde öznitelik çıkarımı yapar (Hafemann vd., 2017).

Gideon vd. (2018) yaptıkları çalışmada el yazısı imza sahteciliğinin tespiti konusuna yoğunlaşmış ve Evrişimli Sinir Ağlarını (CNN) temel alan bir çözüm sunmuşlardır. Geliştirilen model, sorgulanan imzanın gerçek olup olmadığına dair tahminlerde bulunmaktadırlar. İmzaların aynı kişi tarafından atıldığında bile birçok özelliğinin değişkenlik gösterebileceği, bu nedenle sahtecilik tespitinin zorlayıcı bir görev olduğu vurgulanmıştır.

Alajrami vd. (2020) kişisel tanımlama ve önemli belgelerin doğrulanması için kullanılan el yazısıyla atılan imzaları doğrulama konusuna yoğunlaşmışlardır. Bu doğrulamalar çevrimdışı

ve çevrimiçi olarak iki kategoriye ayrılmıştır. Çalışmalarında çevrimdışı imza için bir CNN modeli oluşturmuşlar ve eğitim ve doğrulamanın ardından test başarımını %99,70 olarak belirlemişlerdir.

Ruiz vd. (2020) yaptıkları çalışmada, yazar bağımsız bir sistemde rastgele sahteciliklerle çevrimdışı imza doğrulama problemine çözüm getirmek için İkiz Sinir Ağları'nın (SNN) kullanımını önermişlerdir. Önerilen çözüm ek eğitim gereksinimi olmaksızın yeni imza sahipleri üzerinde kullanılabilmektedir. Ayrıca derin sinir ağlarını eğitmek için gereken örnek miktarını ve değişkenliği artırmak için üç tür sentetik veriyi analiz etmişlerdir. Yaklaşımlarında GAVAB veri tabanından imzalar ve farklı sentetik veri kombinasyonları kullanarak SNN'i eğitmişlerdir. Eğitim için orijinal ve sentetik imzaların kombinasyonu kullanıldığında en iyi doğrulama sonuçları elde edilmiştir.

Jain vd. (2021) imza doğrulamanın güvenlik yönetimi için kimlik doğrulamanın anahtar bir önem taşıdığına dikkat çekmişlerdir. İmza sahteciliği tespitini zor bir görev haline getiren durumun, bireyler tarafından atılan iki veya daha fazla imzanın aynı olma ihtimalinin çok düşük olduğunu vurgulamışlardır. Çalışmada el yazısıyla atılan imzaları tanımlamak ve doğrulamak için İkiz Sinir Ağları'nın farklı çeşitleri arasında bir karşılaştırma analizi gerçekleştirmişlerdir.

Liu vd. (2021) yaptıkları çalışmada çevrimdışı imza doğrulamanın zorluklarına yoğunlaşmış ve bölge tabanlı Derin Evrişimli İkiz Sinir Ağı (DCSNN) kullanarak bir metrik öğrenme[1] yöntemi önermişlerdir. Kullandıkları yöntem GPDS ve CEDAR veri setlerinde yazara bağımsız senaryoda %6,74 ve %8,24 ve yazara bağlı senaryoda %1,67 ve %1,65 eşit hata oranı başarımı elde etmiştir.

Li vd. (2021) el yazısı imza doğrulamasında, mevcut verileri aktif olarak değiştirerek ve yeni veri üreterek etkili öznitelikler kazma konusuna odaklanan yeni bir çekişmeli varyasyon ağı[2] (AVN) modeli önermişlerdir. Kullandıkları yöntem, derin ayrıştırıcı özellikler çıkarmak, çıkarılan özelliklere dayanarak doğrulama kararları yapmak ve daha ayırt edici bir model oluşturmak için imza çeşitleri üretmek amacıyla tasarlanmış üç farklı modülü birleştirmektedir. Bu karmaşık model, imza doğrulama başarımını iyileştirmek için üç modülün birlikte çalıştığı ve rekabet ettiği bir min-max kayıp fonksiyonuyla eğitilmiştir.

[1] Metrik Öğrenme veriler arasındaki benzerlikleri ve farklılıkları öğrenerek mesafe ölçütlerini optimize eden öğrenme yöntemidir.
[2] Çekişmeli varyasyon ağı yapay veri üretimi ve veri dağılımının modellenmesi gibi görevlerde kullanılır. Daha gerçekçi ve yüksek kaliteli veri örnekleri üretmeyi amaçlar.

Yan vd. (2022) çevrimdışı imza sahteciliği tespitine odaklanmışlardır ve bu alanda karşılaşılan zorluklara dikkat çekmişlerdir. Yazarlar farklı görevleri kapsayan yeni bir Çince çevrimdışı imza sahteciliği tespit etme ölçütü oluşturmuşlardır. Kullandıkları yöntemler derin öğrenme tabanlıdır ve üç farklı görevde (imza tespiti, restorasyonu ve doğrulama) çeşitli yaklaşımları kapsamlı bir şekilde karşılaştırmışlardır. Derin öğrenme modelleri yalnızca imza sahteciliği tespitinde değil, imzanın belge üzerinde tespit edilmesine ve arka planda bulunan yazı, mühür, ya da pul gibi görüntülerden ayıklanarak restore edilmesinde de kullanılmaktadır.

Zhang vd. (2022) yazar bağımsız çevrimdışı imza doğrulama için yüksek doğruluk ve düşük model kapasitesini dengelemek için farklı bir mimari önermişlerdir. İmzaların eş boyutlandığı (farklı boyut ve arka planlara sahip imzaların çizgi kalınlıklarının eşitlendiği), dikkat mekanizmasına dayalı öznitelik çıkarımının gerçekleştirildiği ve optimal ağırlık katsayılarına sahip doğrulama modülüne sahip, yeni bir derin öğrenme modeli olan Çok Yollu Dikkat Mekanizmalı İkiz Evrişim Ağı (MA-SCN) geliştirilmiştir.

Singh ve Koundal (2024) 3D imza tanıma sistemlerinin başarımını artırmak için dikkat yönlendirmeli mekânsal-zamansal sinir ağı (ST-ATT) önerilmiştir. CNN'ler mekânsal olarak verileri işlerken, LSTM'ler zaman içinde analiz eder ve dikkat mekanizması karar vermede önemli olan 3D giriş yollarının önemli yönlerine odaklanır.

Paylaşılan literatür göz önüne alındığında; özellikle görüntü tanıma ve sınıflandırma görevlerinde kullanılan, katmanlı yapıya sahip derin öğrenme mimarisi olan Evrişimli Sinir Ağı imza sahteciliği tespitinde de oldukça tercih edilmektedir. İki girdinin benzerliğini ölçmek için kullanılan, iki özdeş alt ağdan oluşan derin öğrenme mimarisi olan İkiz Sinir Ağları ise alt ağ olarak çoğu zaman evrişimli sinir ağlarını kullanmaktadır. Bu yöntem iki imzanın karşılaştırılması için kullanılan en yaygın yöntem olarak göze çarpmaktadır.

Öznitelik çıkarımı imza doğrulama sistemlerinin en kritik adımıdır ve el ile tasarlanmış öznitelik çıkarımı ile kendiliğinden öznitelik öğrenme yöntemleri olarak ikiye ayrılır. El ile tasarlanmış yöntemlerde kullanıcılar öznel algıya dayalı öznitelik çıkarıcılar tasarlar, oysa kendiliğinden öznitelik öğrenme yöntemleri insan müdahalesi olmadan öznitelikleri çıkarır (Kao ve Wen, 2020). Derin öğrenme yöntemleri aynı zamanda el ile tasarlanmış öznitelik çıkarıcılarına dayanmayan ve bunun yerine ham verilerden öznitelikleri kendiliğinden öğrenen tekniklerdir.

Hibrit yaklaşımlar ve dikkat mekanizmaları imza doğrulama süreçlerini daha da iyileştirmekte ve sahtecilik tespitinde daha düşük hata oranları sağlamaktadır.

1.4.4. Dikkat Mekanizmaları

Dikkat mekanizması derin öğrenme modellerine önemli olan girdi bölgelerine odaklanma yeteneği kazandırır. Girdilerin önemli ve ilgili kısımlarını seçerek modelin bu kısımlara daha fazla dikkat etmesini sağlar. Dikkat mekanizmasının temel amacı modelin tüm girdilere eşit şekilde odaklanmak yerine, önemli kısımları vurgulamasını sağlamaktır.

İmza sahteciliği tespitinde, dikkat mekanizması bir imzanın belirli kısımlarının sahtecilik açısından daha belirleyici olabileceğini göz önünde bulundurarak kullanılabilir. Örneğin bir kişinin imzasındaki belirli şekil sahtecilik tespitinde kritik bir rol oynayabilir. Dikkat mekanizması, modelin bu tür belirleyici bölümlere odaklanmasını sağlayarak, genel tespit başarısını artırabilir. Literatürde, dikkat mekanizmasının farklı derin öğrenme mimarileriyle birleştirilerek imza sahteciliği tespitinde kullanıldığına dair sınırlı sayıda çalışma bulunmaktadır.

Shaikh vd. (2020) el yazısı örneklerinin aynı yazar tarafından yazılıp yazılmadığını belirlemek için dikkat mekanizmalarını kullanan bir yöntem önermişlerdir. Kullandıkları yöntem, girişin ilgili alanlarına daha fazla odaklanmayı sağlayarak sınıflandırma başarımını artırır. Bu yöntem CEDAR veri setinde %86 doğruluk elde etmiştir.

Xiong ve Cheng (2021) el yazısı imzalarından ayırt edici öznitelik çıkarmak için dikkat temelli çoklu ikiz sinir ağı (MSN) modeli önermişlerdir. MSN, referans ve sorgu imza görüntülerini ve bunların ters görüntülerini alır. Alınan görüntüler, dört paralel dala beslenir ve her bir dal bağımsız olarak ön kararlar üretir. Son doğrulama sonucu ise bu ön kararlardan oy birliği ile belirlenir. Yazarlar bu dalların baskın yazı özelliklerini keşfetmesi için etkili bir dikkat modülü geliştirmişlerdir. Önerilen yöntem CEDAR, BHSig-B ve BHSig-H gibi imza veri setinde önceki yaklaşımlardan daha iyi başarım göstermiştir.

Zeng (2022) imzaların orijinal ve gri ters versiyonları üzerinden elle yazılmış imza doğrulama için dikkat tabanlı bir yaklaşım geliştirmiştir. Önerilen yeni bir ikiz sinir ağı imza özniteliklerini çıkarmak için kullanılmıştır. Kullanılan yöntem SigComp2011 veri setinde %82 başarı oranı elde etmiştir.

Swin Transformer (Chu vd., 2023) görüntü tanımada önemli bir yöntem haline gelmiştir. Swin Transformer hiyerarşik yapıyı ve yerellik fikrini kullanarak öz dikkat mekanizmasının hesaplama karmaşıklığını önemli ölçüde azaltır ve girdi görüntüsünün boyutuna benzer bir doğrusal karmaşıklık sağlar. Shifted Windows yöntemi ile komşu gruplar arasında bilgi

alışverişi sağlanır. Çok başlıklı dikkat mekanizması (Ashish, 2017) gelişmiş bir dikkat mekanizmasıdır. Çok başlıklı dikkat modelin farklı yönler ve konumlardaki özniteliklere odaklanmasına olanak tanır, bu da sinir ağının temsil hiyerarşisini artırır ve daha fazla bilginin aktarılmasını sağlar (Ashish, 2017; Chu vd., 2023).

Dönüştürücü tabanlı yaklaşımlar, doğal dil işleme (NLP) alanındaki üstün başarımıyla dikkat çekerken, görüntü işleme problemlerini ele almak için de kullanılmaya başlanmıştır. Ancak, imza doğrulama konusunda dönüştürücü tabanlı araştırmalar nadiren odaklanmıştır. Ren vd. (2023) iki kanallı ve iki akışlı dönüştürücü yaklaşımını (2C2S) önermektedir. 2C2S modeli orijinal ve merkez akışlarından oluşur. Orijinal akış, orijinal imza çiftini alırken, merkez akış, orijinal çiftin merkezinden kırpılan imza çiftini alır. İki standart Swin Transformer bloğu arasında bir sıkıştırma ve uyarma işlemi uygulanarak öznitelik kanalları arasındaki ilişkiler kurulmuştur. Ayrıca bir yukarı örnekleme iyileştirme modülü modelin yararlı bilgilere odaklanmasını sağlar.

Mevcut literatürde dikkat mekanizmaları ve dönüştürücü tabanlı yaklaşımlar, imza doğrulama konusundaki başarımı önemli ölçüde artırmıştır. Dikkat mekanizmaları ve dönüştürücü tabanlı yöntemlerin doğrulamada faydalı teknikler olduğu açıktır. Ancak bu modellerin karmaşıklığı ve açıklanabilirliği hala birer zorluk olarak durmaktadır. Bu noktada açıklanabilir yapay zeka (XAI) yöntemleri model kararlarının anlaşılabilirliğini artırarak bu zorlukları aşmada önemli bir rol oynamaktadır.

1.4.5. Açıklanabilir Yapay Zekâ

Derin öğrenme tabanlı modellerin karmaşık yapısı ve kapalı bir kutu[3] gibi çalışmaları, modellerin kararlarının genellikle şeffaf olmamasıyla sonuçlanır. Kullanıcıların bu modellere karşı mesafeli durmasına neden olan bu belirsizliği gidermek ve daha açıklanabilir hale getirmek için yapılan araştırmalar, Açıklanabilir Yapay Zekâ olarak adlandırılmaktadır. Bilgisayarla görü alanında XAI için en önemli yaklaşımlardan biri, gradyan tabanlı görsel belirginlik (İng. saliency) yöntemidir (Kao vd., 2020). Belirginlik haritası, belirli bir sınıflandırıcıdan kategoriye özgü puanların gradyanını hesaplayarak oluşturulur. Bu gradyan, bir pikseldeki değişikliğin sınıflandırıcı çıktısını ne kadar etkileyeceğini gösterir. Belirginlik haritası ağın kararının insan bilişiyle tutarlı olup olmadığını kontrol etmek için kullanılabilir (Kao vd., 2020). Grad-CAM gibi teknikler, modelin karar verme sürecinde önemli bulduğu

[3] Yazılım geliştirme alanında sıklıkla kullanılan kapalı kutu ya da kara kutu terimi, girdi ve çıktının açık bir şekilde bilindiği fakat ara adımların belirsiz olduğu durumlar için kullanılır.

imza görüntüsündeki bölgeleri belirleyerek adli uzmanların hangi bölümlerin karar vermede kritik rol oynadığını anlamalarına yardımcı olabilir (Diaz vd., 2024).

1.5. Tezin Amacı ve Katkısı

Bu çalışmanın amacı imza sahteciliği tespitinde derin öğrenme tabanlı dikkat mekanizmalarının kullanıldığı ve sonuçların açıklanabilir yapay zekâ yöntemleriyle desteklendiği bir yaklaşım sunmaktır.

Bu amaçla farklı derin öğrenme mimarileri dikkat mekanizmaları ile entegre edilerek başarımları karşılaştırılmış, sonuçlar açıklanabilir bir yapıya dönüştürülmüş ve son kullanıcıya basit bir arayüz ile sunulmuştur. Ayrıca farklı veri seti büyüklüklerinin ve çoklu imza karşılaştırmalarının başarıma olan etkileri de detaylı bir şekilde analiz edilmiştir.

Çalışma kapsamında sadece statik imzalar incelenmiş olup, dinamik imza verileri ve çevrimiçi imza doğrulama yöntemleri kapsam dışı bırakılmıştır. Çalışmada kullanılan veri seti farklı coğrafya ve dillerden imzaları içermemektedir, bu tür farklılıkların araştırılması çalışma kapsamına alınmamıştır.

Çalışma mevcut yöntemlerin karşılaştırmalı analizini yaparak ve dikkat mekanizmaları yardımıyla imza sahteciliği alanında açıklanabilir bir derin öğrenme yaklaşımı sunarak literatüre önemli bir katkı sağlamayı hedeflemektedir.

Çalışma beş ana bölümden oluşmaktadır;

- *Bölüm 1: Giriş* bölümünde, konu hakkında genel bilgiler verilmiş, literatürdeki ilgili araştırmalar paylaşılmış, son olarak da tezin amacı, kapsamı ve sağlayacağı bilimsel katkıdan bahsedilmiştir.
- *Bölüm 2: Gereç ve Yöntem* altında, kullanılan veri seti, veri ön işleme ve veri zenginleştirme teknikleri ile derin öğrenme mimarileri, model eğitim süreçlerinde kullanılan kayıp fonksiyonları ve dikkat mekanizmaları hakkında detaylı bilgi verilmektedir. Ayrıca çalışma kapsamında yapılan deneyler detaylandırılmış ve başarım değerlendirme yöntemleri tanıtılmıştır.
- *Bölüm 3: Bulgularda*, farklı derin öğrenme mimarilerinin eğitim ve test süreçlerindeki başarımları sunulmuş, veri seti büyüklüğünün model başarımına etkisi ve çoklu imza karşılaştırma deneylerinin sonuçları da paylaşılmıştır.
- *Bölüm 4: Tartışma* bölümünde ise elde edilen bulgular ve bulgulara dayalı çıkarımlar, ilgili literatürden yararlanılarak yorumlanmıştır. Literatürdeki çalışmalarla uyumlu ve

uyumsuz bulguların nedenleri tartışılmış, modellerin başarımlarını etkileyen faktörler ve genelleme yetenekleri ele alınmıştır. Sonuçların görselleştirilmesi için kullanılan teknikler ve bunların modelin karar verme süreçlerini anlamaya katkıları da değerlendirilmiştir.

- Son olarak *Bölüm 5: Sonuç ve Öneriler*'de çalışmanın sonuçları ve gelecek çalışmalar için öneriler sunulmaktadır.

2. GEREÇ VE YÖNTEM

Bu çalışma kapsamında kullanılan gereç ve yöntemler bu bölümde detaylandırılmaktadır. Öncelikle kullanılan veriler tanıtılmakta, veri ön işleme ve veri zenginleştirme yöntemleri açıklanmaktadır. İmza setlerinin nasıl hazırlandığına dair bilgiler sunulmaktadır. Ardından, ikiz sinir ağları, kayıp fonksiyonları, derin öğrenme mimarileri ve dikkat mekanizmaları ele alınmakta, bu mekanizmaların mimarilere eklenmesi ve görselleştirme teknikleri paylaşılmaktadır. Sıralı ağırlıklı ortalama operatörü hakkında bilgi verilmektedir. Deneyler bölümünde, farklı mimarilerin başarımlarının karşılaştırılması, veri seti büyüklüğünün başarıma etkisi, çoklu imza karşılaştırmaları ve sonuçların görselleştirilmesi detaylandırılmaktadır. Başarım değerlendirme yöntemleri açıklanmakta, kullanıcı arayüzü tanıtılmakta ve geliştirme ile test ortamı hakkında bilgiler verilmektedir.

2.1. Veriler

Bu çalışmada imza sahteciliği üzerine yapılan çalışmalarda sıklıkla kullanılan CEDAR veri seti[4] kullanılmıştır. Veri setinde yer alan imza görselleri üzerinde farklı görüntü ön işleme yöntemleri uygulanmış, veri çeşitliliğini artırmak için veri zenginleştirme işlemleri yapılmış ve modellerin eğitiminde kullanılacak imza setleri hazırlanmıştır.

2.1.1. Veri Seti

CEDAR imza sahteciliği veri seti gerçek ve sahte imzaları içermekte olup, bu imzaların farklı bireyler tarafından üretilmiş olması sebebiyle geniş bir varyasyon sunmaktadır. Veri seti imza sahteciliğini tespit etme konusunda yaygın olarak kullanılan bir kaynak olduğu için tercih edilmiştir.

Veri setinde 55 farklı kişiye ait imzalar bulunmaktadır. Her bir kişi için 24 gerçek imza ve 24 sahte imza bulunmaktadır. Veri seti toplamda 1320 gerçek ve 1320 sahte imza olmak üzere 2640 adet imza içermektedir. Her imza 300 dpi gri tonlamada taranmış ve gri ton histogramı kullanılarak ikili hale getirilmiştir.

Şekil 2.1'de CEDAR veri setinde yer alan gerçek ve sahte imzalardan bazı örnekler yer almaktadır. İlk iki sütunda gerçek imzalar, son iki sütunda ise bu imzalara ait serbest taklit yöntemiyle atılmış sahte imzalar bulunmaktadır.

[4] Açık erişimli veri seti https://cedar.buffalo.edu/signature/ adresinde yer almaktadır.

Şekil 2.1. CEDAR veri setinde yer alan imzalardan bazı örnekler

2.1.2. Veri Ön İşleme

Veri setinde yer alan görüntülerdeki arka plan gürültüsünün azaltılması ve renk tonlarının standartlaştırılması gibi ön işleme adımları gerçekleştirilmiştir. Bu süreçte görüntüler üzerinde farklı eşikleme ve normalizasyon yöntemleri denenerek en iyi başarım gösteren ön işleme yöntemi seçilmiştir. Uygulanan yöntemlerden biri olan Otsu Eşikleme (Otsu, 1975) görüntüleri ikili hale getirmek için kullanılan bir yöntemdir. Bu yöntem piksel değerlerinin histogramını analiz ederek en iyi eşik değerini otomatik olarak belirler. Uyarlamalı Eşikleme (Bradley ve Roth, 2007) görüntüleri ikili hale getirmek için kullanılan başka bir yöntemdir. Bu yöntem her pikselin çevresindeki yerel bölgeyi analiz ederek eşik değerini belirler, bu sayede değişen aydınlatma koşullarına uyum sağlar.

Tüm imza görüntüleri modellerin işleyebileceği 220 x 155 (Vision Transformer için 224 x 224) piksel boyutuna yeniden boyutlandırılmıştır.

Şekil 2.2'de farklı ön işleme yöntemlerin imza görselleri üzerindeki etkileri görsel olarak karşılaştırılabilir. İlk sütunda veri setindeki haliyle imza görseli ve ardından sırasıyla Otsu

Eşikleme, Uyarlamalı Eşikleme ve normalizasyon yöntemleriyle işlenmiş imza görselleri yer almaktadır.

Şekil 2.2. Farklı ön işleme yöntemlerinin imzalara uygulanması

2.1.3. Veri Zenginleştirme

Modelin genelleme yeteneğini artırmak ve eğitim sırasında aşırı öğrenmeyi önlemek için çeşitli veri zenginleştirme teknikleri (Krizhevsky vd., 2012) kullanılmıştır. Görüntülerin boyutlarını küçültüp büyütme işlemi yaparak modelin farklı boyutlardaki imzaları tanıma yeteneğini geliştirmek için *ölçeklendirme*; görüntü üzerine hafif bir bulanıklık efekti uygulanarak, modelin imza çizgilerinin netliği azalmış durumlarda da başarımını sürdürebilmesi için *bulanıklaştırma*; modelin farklı aydınlatma koşullarında imza tespiti yapabilme kabiliyeti arttırmak için *parlaklık ayarı*; modelin düşük veya yüksek kontrastlı imzaları tanıyabilmesi için *kontrast değiştirme* ve son olarak imzaların farklı açılardan algılanabilmesi için *döndürme* teknikleri uygulanmıştır. Bu teknikler sayesinde modelin farklı boyutlarda, düşük netlikte, farklı aydınlatma koşullarında ya da farklı açılardan görülen imzalarda da etkili sonuçlar vermesi hedeflenmektedir.

Şekil 2.3'te uygulanan farklı zenginleştirme yöntemlerinin etkileri görsel olarak karşılaştırılabilir. İlk sütunda veri setindeki haliyle imza görseli ve ardından sırasıyla ölçeklendirme, bulanıklaştırma ve parlaklık ayarı yöntemleriyle üretilmiş imza görselleri yer almaktadır.

Şekil 2.3. Farklı veri zenginleştirme yöntemlerinin imzalara uygulanması

2.1.4. İmza Setlerinin Hazırlanması

Derin öğrenme modellerinin eğitimi için imza setlerinin hazırlanmasına ihtiyaç duyulmuştur. İmza setleri Kayıp Fonksiyonları bölümünde bahsedilen yöntemler için ikili ve üçlü setler halinde oluşturmuştur.

2.1.4.1. İkili İmza Setleri

İkili imza setleri iki farklı imzanın karşılaştırılmasına dayanır. Bir referans imza ve bir karşılaştırma imzasından oluşur. Karşılaştırma imzası, ya aynı kişiye ait bir gerçek imza (pozitif örnek) ya da farklı bir kişi tarafından atılmış sahte bir imza (negatif örnek) olabilir. İkili imza setleri, karşıt kayıp fonksiyonu kullanıldığı eğitim sürecinde kullanılır. Oluşturulabilecek toplam ikili imza setlerinin sayısı Çizelge 2.1'de verilmiştir.

Çizelge 2.1. İkili set sayıları

Set Türü	Hesaplama (Tek Kişi)	Set Sayısı (Tek Kişi)	Set Sayısı (Toplam)
Pozitif İkili Setler	$\binom{24}{2}$	276	15180
Negatif İkili Setler	$24\ x\ 24$	576	31680
Toplam		**852**	**46860**

Derin öğrenme modellerinin eğitimi sırasında dengeli bir şekilde dağılmış verilere ihtiyaç vardır. Bu yüzden eğitim sırasında eşit sayıda pozitif ve negatif setler kullanılmıştır. Aynı zamanda eğitimlerinin gerçekleştirildiği ortam sınırlamaları nedeniyle daha az sayıda ikili set kullanılmıştır.

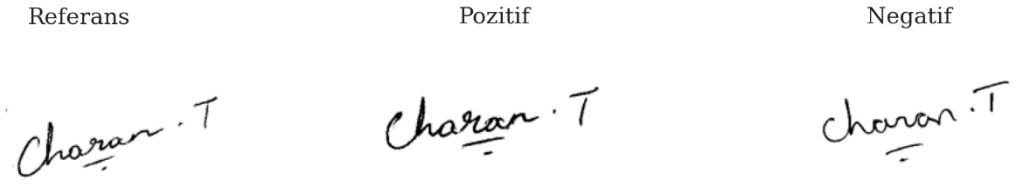
2.1.4.2. Üçlü İmza Setleri

Üçlü imza setleri, üç farklı imzanın karşılaştırılmasına dayanır. Bir referans imza, bir pozitif imza ve bir negatif imzadan oluşur. Referans imza, gerçek imzayı temsil ederken, pozitif imza aynı kişiye ait başka bir gerçek imzayı, negatif imza ise farklı bir kişi tarafından atılmış sahte bir imzayı temsil eder. Üçlü imza setleri, üçlü kayıp fonksiyonu kullanıldığı eğitim sürecinde kullanılır. Oluşturulabilecek toplam üçlü imza seti sayısı Çizelge 2.2'de verilmiştir.

Çizelge 2.2. Üçlü set sayıları

Set Türü	Hesaplama (Tek Kişi)	Set Sayısı (Tek Kişi)	Set Sayısı (Toplam)
Üçlü Setler	$24\ x\ 23\ x\ 24$	13248	728640

Derin öğrenme modellerinin eğitimlerinin gerçekleştirildiği ortam sınırlamaları nedeniyle daha az sayıda üçlü set kullanılmıştır. Şekil 2.4'te örnek bir üçlü set gösterilmektedir.



Şekil 2.4. Üçlü imza seti

2.2. Derin Öğrenme Teknikleri

Bu çalışmada imzaların görüntülerinin karşılaştırılması için bir ikiz sinir ağı oluşturulmuş, ağın kullanacağı mimari yapı ise literatürde yer alan üstün başarımlı mimarilerden seçilmiştir. Seçilen derin öğrenme mimarileri arasında VGG16, ResNet18, ResNet50, Inception,

Xception, EfficientNet ve Vision Transformer bulunmaktadır. Bu mimariler görüntü analizi için özgün özellikleri ile ön plana çıkmaktadırlar.

2.2.1. İkiz Sinir Ağları

Siyam sinir ağları olarak da adlandırılan ikiz sinir ağları benzer veya farklı görüntüleri karşılaştırmak için kullanılabilecek özel bir derin öğrenme mimarisidir (Bromley vd., 1993). Bu ağ yapısı iki ya da daha fazla aynı ağı içerir; bu ağlar aynı ağırlıkları paylaşıp, farklı girdilerle beslenirler ve aralarındaki farkı veya benzerliği ölçmek için kullanılan bir kayıp fonksiyonuna bağlanır.

Kayıp fonksiyonu olarak üçlü kayıp veya karşıt kayıp kullanılabilir. Üçlü kayıpla öğrenmede, bir referans vektörü, pozitif ve negatif vektörler ile aynı anda karşılaştırılır (Schroff vd., 2015). Negatif vektör ağda öğrenmeyi zorlar, pozitif vektör ise düzenleyici olarak işlev görür. Karşıt kayıpla öğrenmede ise referans vektör ile her defasında yalnızca bir pozitif veya negatif vektör karşılaştırılır (Chopra vd., 2005). Ağırlıkları düzenlemek için bir ağırlık azalması veya benzeri bir normalizasyon işlemi gerekir.

İkiz sinir ağı kullanılarak iki imzanın kıyaslanması, imzaların ayrı ayrı aynı sinir ağından geçirilmesi ve elde edilen özellik vektörlerinin karşılaştırılması ile gerçekleştirilir. İkiz sinir ağları, aynı ağırlıkları paylaşan iki özdeş alt ağdan oluşur. Bu ağlar imzaları bir özellik uzayına dönüştürür.

$$f_1 = \text{Ağ}(I_1), \qquad f_2 = \text{Ağ}(I_2)$$

Şekil 2.5. Özellik vektörleri

Şekil 2.5'te I_1 ve I_2 karşılaştırılacak iki imzayı, f_1 ve f_2 ise bu imzaların özellik vektörlerini temsil eder. Daha sonra iki imza arasındaki mesafe ölçülür.

$$D(f_1, f_2) = \sqrt{\sum_{i=1}^{n} (f_{1i} - f_{2i})^2}$$

Şekil 2.6. Öklid mesafesi

Şekil 2.6'da D, iki özellik vektörü arasındaki Öklid mesafesidir. Ölçülen mesafe önceden belirlenmiş bir eşik değeri ile kıyaslanarak imzaların sahte mi yoksa gerçek mi olduğu belirlenir.

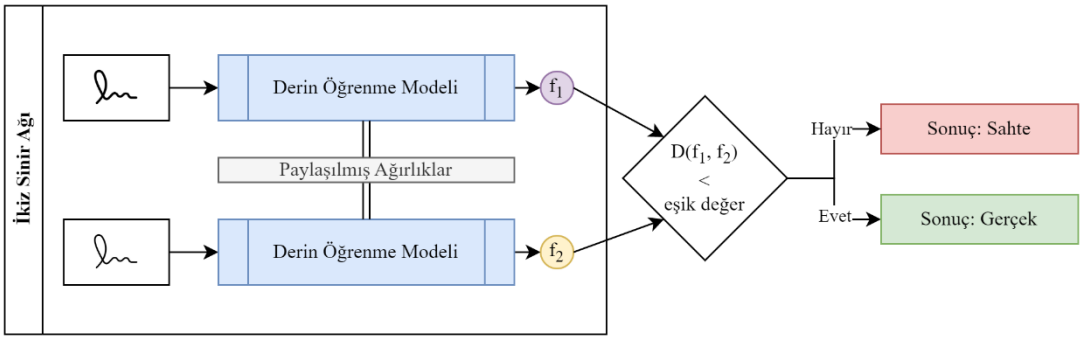
$$Karar = \begin{cases} Gerçek, & D(f_1, f_2) < eşik\ değer \\ Sahte, & D(f_1, f_2) \geq eşik\ değer \end{cases}$$

Şekil 2.7. Karar fonksiyonu

Şekil 2.7'de gösterildiği şekilde eğer mesafe eşik değerinden küçükse imzalar benzer yani gerçek, büyükse farklı yani sahte olarak değerlendirilir.

Bu sürecin görselleştirilmiş hali Şekil 2.8'de gösterilmektedir. İkiz sinir ağına girdi olarak verilen iki imza, aynı ağırlıkları paylaşan özdeş derin öğrenme modelleriyle işlenir ve imzalara ait özellik vektörleri elde edilir. Bu vektörlerin birbirlerine olan uzaklığı üzerinden imzaların sahte ya da gerçek olduğuna karar verilir.

Bu çalışmada imza görüntülerinin karşılaştırılması için ikiz sinir ağları tercih edilmiş, ikiz sinir ağlarında ise karşılaştırılmak istenen farklı derin öğrenme mimarileri kullanılmıştır.



Şekil 2.8. İkiz sinir ağı mimarisinin imza sahteciliğinde kullanımı

2.2.2. Kayıp Fonksiyonları

Derin öğrenme modelleri eğitilirken farklı kayıp fonksiyonları kullanılmaktadır. Kayıp fonksiyonu, beklenen sonuç ile modelin verdiği sonucu kıyaslayan matematiksel bir eşitliktir. Kayıp fonksiyonunun değerine göre model öğrenmesini iyileştirmeye çalışır.

Bu çalışmada modeller karşıt kayıp ve üçlü kayıp fonksiyonları ile ayrı ayrı eğitilmiştir.

2.2.2.1. Karşıt Kayıp Fonksiyonu

Karşıt Kayıp Fonksiyonu karşılaştırılacak iki örnek arasındaki benzerlikleri öğrenmek için kullanılan bir kayıp fonksiyonudur (Chopra vd., 2005). Çiftler halinde sunulan verilerde benzer çiftler arasındaki mesafeyi minimize etmeyi, farklı çiftler arasındaki mesafeyi ise

maksimize etmeyi hedefler. İki örneğin özellik vektörleri arasındaki mesafe Öklid mesafesi olarak ölçülür. Eğer iki örnek benzer ise bu mesafenin küçük olması, farklı ise büyük olması beklenir.

$$L(Y, D) = (1 - Y)\frac{1}{2}D^2 + Y\frac{1}{2}\max(0, m - D)^2$$

Şekil 2.9. Karşıt kayıp fonksiyonu

Şekil 2.9'da karşıt kayıp fonksiyonu verilmiştir. Burada *D*, iki örnek arasındaki Öklid mesafesi; *Y*, benzer çiftler için 0, farklı çiftler için 1 değerini alan etiket; *m*, negatif çiftler arasındaki minimum mesafeyi belirten marjin değeridir.

2.2.2.2. Üçlü Kayıp Fonksiyonu

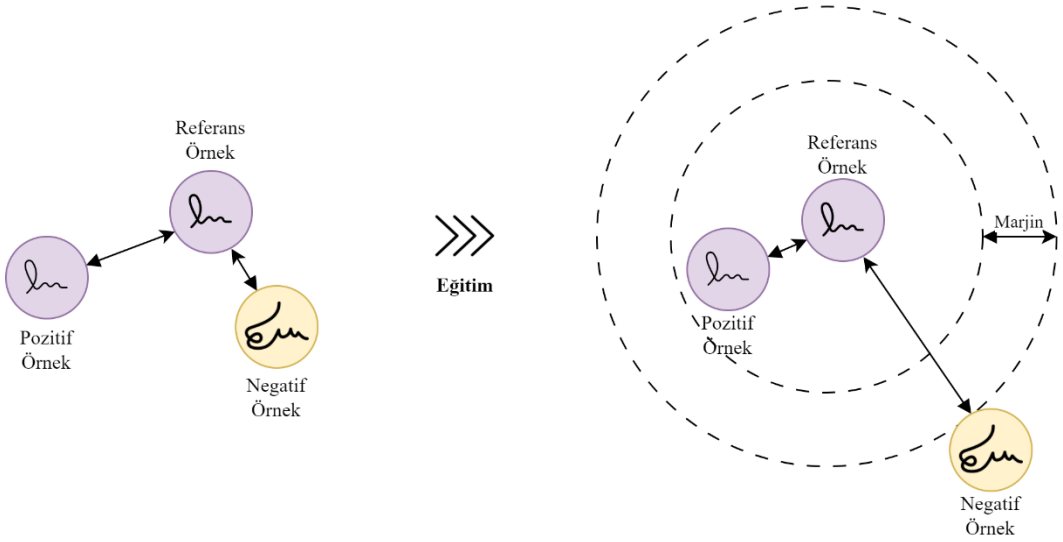
Üçlü Kayıp Fonksiyonu, bir referans örnek, bu örneğe benzer bir pozitif örnek ve farklı bir negatif örnek olmak üzere üçlüler halinde sunulan verilerde kullanılır (Schroff vd., 2015). Amaç, referans ve pozitif örnek arasındaki mesafeyi minimize ederken, referans ve negatif örnek arasındaki mesafeyi maksimize etmektir. Benzer nesneleri daha yakın, farklı nesneleri ise daha uzak konumlandırarak özellik uzayını daha anlamlı hale getirir.

$$L(A, P, N) = \max(0, |f(A) - f(P)|^2 - |f(A) - f(N)|^2 + \alpha)$$

Şekil 2.10. Üçlü kayıp fonksiyonu

Şekil 2.10'da üçlü kayıp fonksiyonu verilmiştir. Burada *A*, referans örnek; *P*, pozitif örnek; *N*, negatif örnek; *f*, özellik vektörünü çıkaran fonksiyon ve *α*, marjin değeridir.

Şekil 2.11'de üçlü kayıp fonksiyonu ile mesafelerin marjin değerine göre nasıl ayarlandığı görselleştirilmiştir. Fonksiyon sayesinde referans ve pozitif örnekler arasındaki mesafe azaltılırken, negatif örnek ile arasındaki mesafe artırılır. Pozitif ve negatif örnek arasında marjin değeri kadar bir mesafe oluşturulmaya çalışılır. Bu yapı karşıt kayıp fonksiyonunda bulunmamaktadır.



Şekil 2.11. Üçlü kayıp fonksiyonu ile mesafelerin ayarlanması

2.2.3. Derin Öğrenme Mimarileri

Bu çalışmada kullanılan derin öğrenme mimarileri Çizelge 2.3'te verilmiş, mimariler hakkında özet bilgiler alt başlıklarda paylaşılmıştır.

Çizelge 2.3. Başlıca derin öğrenme mimarileri ve teknik özellikleri

Mimari	Referans	Katman Sayısı	Parametre Sayısı	Hesaplama Maliyeti
VGG16	Simonyan ve Zisserman (2014)	16	138M	Yüksek
ResNet18	He vd. (2016)	18	11,7M	Orta
ResNet50	He vd. (2016)	50	25,6M	Yüksek
Inception v4	Szegedy vd. (2017)	55	42M	Yüksek
Xception	Chollet (2017)	36	22,9M	Orta
EfficientNet B0	Tan ve Le (2019)	24	5,3M	Düşük
Vision Transformer	Dosovitskiy vd. (2020)	12	86M	Yüksek

2.2.3.1. VGG16

VGG16 görüntüleri ayrıntılı bir şekilde incelemek için basit ve derin bir yapıya sahip olan bir yapay zeka mimarisidir (Simonyan ve Zisserman, 2014). Bu mimari 16 katmanlı derin bir sinir ağı kullanarak görüntüdeki detayları yakalar. VGG16 basit ve düz yapısı sayesinde diğer mimarilere göre daha kolay anlaşılabilir ve uygulanabilir olmasıyla öne çıkar.

2.2.3.2. ResNet18

ResNet18 çok derin olmasına rağmen daha hızlı ve hafif olan bir yapay zeka mimarisidir (He vd., 2016). Kayıp gradyan problemini çözmek için rezidüel bağlantılar kullanır, bu sayede daha derin ağlar oluşturabilir. ResNet18 daha derin ve karmaşık modellerin oluşturulmasına imkân tanıyarak o dönemdeki diğer mimarilere kıyasla daha verimlidir.

2.2.3.3. ResNet50

ResNet50 daha karmaşık ve derin bir yapıya sahip olduğu için görüntüleri çok daha ayrıntılı ve doğru bir şekilde analiz edebilir (He vd., 2016). Bu mimari 50 katmanlı derin bir sinir ağı kullanır ve rezidüel bağlantılarla çalışır. ResNet50 derinlik ve doğruluk açısından diğer mimarilere göre üstün başarım gösterir.

2.2.3.4. Inception (v4)

Inception aynı anda farklı boyutlardaki detayları inceleyerek görüntülerdeki bilgileri daha iyi yakalayan bir yapay zeka mimarisidir (Szegedy vd., 2017). Mimari çoklu filtreler ve katmanlar kullanarak görüntülerin farklı özelliklerini eşzamanlı olarak işler. Inception ölçeklenebilirliği ve detayları yakalama yeteneği ile diğer mimarilerden daha esnek ve güçlüdür.

2.2.3.5. Xception

Xception görüntülerdeki detayları daha verimli bir şekilde analiz etmek için özel bir yöntem kullanarak çalışan gelişmiş bir yapay zeka mimarisidir (Chollet, 2017). Bu mimari derinlemesine ayırılabilir evrişimler (İng. depthwise separable convolutions) kullanarak hem kanal içi hem de mekansal ilişkileri yakalar. Xception verimlilik ve başarım açısından diğer mimarilerden daha iyi sonuçlar elde etmesiyle dikkat çeker.

2.2.3.6. EfficientNet (B0)

EfficientNet hem hızlı hem de doğru sonuçlar almak için yapılandırılmış, verimli ve dengeli bir yapay zeka mimarisidir (Tan ve Le, 2019). Bu model derinlik, genişlik ve çözünürlüğü optimize eden bir bileşik ölçeklendirme yöntemi kullanır. EfficientNet optimize edilmiş yapısı sayesinde diğer mimarilere göre daha az hesaplama gücüyle yüksek doğruluk sağlar.

2.2.3.7. Vision Transformer

Vision Transformer görüntüleri parçalara ayırıp her bir parçanın diğerleriyle ilişkisini inceleyerek çalışan yenilikçi bir yapay zeka mimarisidir (Dosovitskiy vd., 2020). Dönüştürücü mimarisini temel alarak öz dikkat mekanizması ile görüntülerin bağlamını ve detaylarını öğrenir. Vision Transformer büyük veri setlerinde ve karmaşık desenlerde üstün başarım göstererek günümüzdeki evrişimli sinir ağı temelli diğer mimarilerden ayrılır.

2.2.4. Dikkat Mekanizmaları

Dikkat mekanizmaları derin öğrenme modellerinin belirli özelliklere odaklanarak daha iyi başarım göstermesini sağlayan tekniklerdir (Ashish, 2017). Özellikle imza sahteciliği tespiti gibi görevlerde modelin sahte ve gerçek imzalar arasındaki farkları daha iyi saptamasına yardımcı olabilir. Dikkat katmanları, genellikle evrişimli ağların son katmanlarına eklenir ve modelin eğitimi sırasında öğrenilen özelliklerin ağırlıklandırılmasını sağlar. Vision Transformer mimarisi dikkat mekanizması içerdiğinden ayrıca eklemeye gerek bulunmamaktadır.

Dikkat mekanizmalarının kullanıldığı mimariler ikiz sinir ağı yapısı içinde kullanıldığında, çift girişli bir yapıda hem pozitif hem de negatif örnekler arasındaki benzerlikleri ve farklılıkları değerlendirerek imza sahteciliğini tespit etme kapasitesini artırabilir.

2.2.4.1. Sıkıştırma ve Uyarım Dikkat Mekanizması

Sıkıştırma ve Uyarım (SE) Dikkat Mekanizması (Hu vd., 2018) her bir kanalın önemini öğrenir ve bu bilgiyi kullanarak özellik haritalarını yeniden ölçeklendirir. Sıkıştırma, uyarım ve yeniden ölçeklendirme adımlarından oluşur. Bu dikkat mekanizması modelin belirli özelliklere daha fazla odaklanmasını sağlar.

Şekil 2.12'de verilen sıkıştırma adımında boyut bilgileri sıkıştırılır ve kanal başına küresel ortalama havuzlama kullanılarak bir vektöre indirgenir.

$$z = F_{sq}(U) = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} U_{i,j}$$

Şekil 2.12. Sıkıştırma fonksiyonu

Şekil 2.12'de z küresel ortalama havuzlama sonucunda elde edilen sıkıştırılmış vektör, F_{sq} sıkıştırma fonksiyonu, U girdi özelliği haritası, H ve W ise uzaysal boyutlardır.

Uyarım adımında ise sıkıştırılmış vektör üzerine tam bağlantılı katmanlar ve aktivasyon fonksiyonları uygulanarak kanal başına ağırlıklar hesaplanır.

$$s = F_{ex}(z, W) = \sigma\big(W_2 \delta(W_1 z)\big)$$

Şekil 2.13. Uyarım fonksiyonu

Şekil 2.13'te s uyarım sonucu elde edilen ölçekleme vektörü, F_{ex} uyarım fonksiyonu, δ ve σ sırasıyla ReLU ve Sigmoid aktivasyon fonksiyonlarıdır.

Son adım olan yeniden ölçekleme Şekil 2.14'de gösterilmiştir. Bu aşamada girdi özellik haritası kanal başına ağırlıklarla ölçeklendirilir.

$$X_c = F_{scale}(U_c, s_c) = U_c \cdot s_c$$

Şekil 2.14. Yeniden ölçekleme fonksiyonu

Şekil 2.14'de X_c ölçeklendirilmiş özellik haritası, U_c kanala ait girdi özelliği haritasını, s_c ise kanal başına ağırlığı ifade etmektedir.

2.2.4.2. Öz Dikkat Mekanizması

Öz Dikkat Mekanizması (Ashish, 2017), bir verinin her parçasının diğer parçalarla olan ilişkisini öğrenir. Böylelikle modelin farklı özellikler arasındaki bağıntıları anlaması kolaylaşır. İki adımdan oluşan mekanizma sorgu, anahtar ve değer matrislerinin hesaplanmasına, ardından bu matrisler üzerinden de dikkat skorunun hesaplanmasına dayanır.

$$Q = XW^Q, \quad K = XW^K, \quad V = XW^V$$

Şekil 2.15. Sorgu, anahtar ve değer matrisleri

Şekil 2.15'te sırasıyla Q, K ve V sorgu, anahtar ve değer matrisi, W^Q, W^K ve W^V öğrenilebilir ağırlık matrisleri, X ise girdi özelliği haritasıdır.

Şekil 2.16'da dikkat sonucunun eşitliği verilmiştir. Sorgu ve anahtar matrislerinin çarpımı normalize edilerek dikkat skoru elde edilir. Dikkat skoru ile değer matrisi çarpılarak dikkat sonucuna dönüştürülür.

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

Şekil 2.16. Dikkat fonksiyonu

Burada QK^T sorgu ve anahtar matrislerinin nokta çarpımının transpozesini, d_k anahtar boyutunu ifade etmektedir.

2.2.4.3. Çok Başlıklı Öz Dikkat

Çok başlıklı öz dikkat mekanizması (Ashish, 2017), öz dikkat işlemini paralel olarak birden fazla başlıkta gerçekleştirir. Her başlık farklı bir bağıntıyı öğrenir ardından başlıklar birleştirilerek sonuç matrisi oluşturulur. Bu sayede modelin daha kapsamlı ve çeşitli dikkat paternleri öğrenmesi sağlanır.

Birden fazla başlığa ayrılan girdiye öz dikkat uygulanır.

$$\text{Başlık}_i = \text{Dikkat}\left(\boldsymbol{QW_i^Q}, \boldsymbol{KW_i^K}, \boldsymbol{VW_i^V}\right)$$

Şekil 2.17. Tek bir başlık için dikkat fonksiyonu

Şekil 2.17'de $Başlık_i$ i'inci başlığı, W_i^Q, W_i^K ve W_i^V başlığa ait öğrenilebilir ağırlık matrislerini ifade etmektedir. Tüm başlıklar birleştirilerek son ağırlık matrisi ile çarpılır. Şekil 2.18'de çok başlıklı dikkat sonucunun eşitliği verilmiştir.

$$\text{ÇokBaşlıkıDikkat}(Q, K, V) = Birleştir(\text{Başlık}_1, \text{Başlık}_2, \dots, \text{Başlık}_h)W^O$$

Şekil 2.18. Çok başlıklı dikkat fonksiyonu

Burada W^O son ağırlık matrisi ve *Birleştir* birleştirme fonksiyonudur.

2.2.5. Dikkat Mekanizmalarının Mimarilere Eklenmesi

İkiz sinir ağı yapısı üzerinde kullanılan derin öğrenme mimarileri kendi aralarında da yapısal farklılık göstermektedir. Bu nedenle dikkat mekanizmalarının bu mimarilere eklenmesi aşamasında her mimarinin farklı bir katmanı kullanılmak zorunda kalınmıştır.

Her modelin son katmanı bir kimlik katmanı ile değiştirilmiştir. Kimlik katmanı modelin son tam bağlantılı katmanını devre dışı bırakır. Dikkat mekanizması kimlik katmanıyla değiştirilen katmanın hemen öncesindeki katmana uygulanmıştır. Dikkat mekanizmasının çıkışında ise modelin imza sahteciliğini tespit edebilmesi için önemli özelliklerin vurgulandığı bir özellik haritası elde edilir.

Çizelge 2.4 farklı mimarilerin hangi katmanının dikkat mekanizması için kullanıldığı gösterilmektedir.

Çizelge 2.4. Dikkat mekanizmalarının uygulandığı katmanlar

Mimari	Etkilenen Katmanlar[5]	Katman Adı
VGG16	Baş kısmındaki tam bağlantılı katman	head.fc
ResNet18	Son tam bağlantılı katman	fc
ResNet50	Son tam bağlantılı katman	fc
Inception v4	Son tam bağlantılı katman	last_linear
Xception	Sınıflandırıcı modülünün son katmanı	classifier[-1]
EfficientNet B0	Sınıflandırıcı modülünün son katmanı	classifier[-1]

Kendi öz dikkat mekanizmasına sahip olduğu için Vision Transformer mimarisinde bir değişiklik yapılmamıştır.

2.2.6. Görselleştirme Teknikleri

Modelin karar verme sürecini anlamak için çeşitli görselleştirme teknikleri kullanabilir (Samek vd., 2019). Modelin hangi girdi özelliklerini önemli bulduğunu ve nasıl bir karar verdiğini gösteren görselleştirme teknikleri modelin açıklanabilirliğine önemli bir katkı sağlar. İmza sahteciliği tespitinde bu teknikler sayesinde modelin dikkate aldığı imza özellikleri belirlenebilir ve sahte imzaları ayırt etmede hangi özelliklerin kritik rol oynadığı anlaşılabilir (Kao ve Wen, 2020).

2.2.6.1. Grad-CAM

Grad-CAM derin öğrenme modellerinin iç işleyişini anlamak için yaygın olarak kullanılan bir tekniktir (Selvaraju vd., 2017). Grad-CAM, bir modelin belirli bir sınıf için yaptığı tahminin arkasındaki önemli bölgeleri görselleştirir. Bu teknik, sınıflandırma sonucu ile ilgili son katmanın gradyanlarını hesaplar ve bu gradyanları kullanarak özellik haritalarını ağırlıklandırır. Literatürde farklı Grad-CAM türevleri (Chattopadhay vd., 2018; Draelos ve Carin, 2020; Omeiza vd., 2019; Ramaswamy, 2020) bulunmakta olup modelin karar verme

[5] Çizelge 2.4'te kimlik katmanı ile değiştirilmiş katman belirtilmiş olup, bu katmandan bir önceki katmana da dikkat mekanizması uygulanmıştır.

sürecini görselleştirerek hangi özelliklerin önemli olduğunu belirleyen ve bu sayede modelin şeffaflığını artıran bir yöntemdir.

2.2.6.2. Bütünleşik Gradyanlar

Bütünleşik Gradyanlar, modelin karar verme sürecini anlamak için kullanılan başka bir güçlü tekniktir (Sundararajan vd., 2017). Bu teknik, bir başlangıç girdisi ile son girdi arasında modelin dikkate aldığı özelliklerin katkılarını integral olarak hesaplayarak sunar. Bütünleşik Gradyanlar, modelin hangi girdi özelliklerini önemli bulduğunu ve nasıl bir karar verdiğini daha kesin bir şekilde gösterir.

Bütünleşik Gradyanlar, modelin dikkate aldığı tüm yollar boyunca gradyanları hesaplar ve bu gradyanların ortalamasını alarak her bir girdi özelliğinin modelin kararına olan katkısını belirler. Şekil 2.19'da Bütünleşik Gradyan fonksiyonu verilmiştir.

$$IG_i(x) = (x_i - x_i') \times \int_{\alpha=0}^{1} \frac{\partial F\left(x' + \alpha \times (x - x')\right)}{\partial x_i} d\alpha$$

Şekil 2.19. Bütünleşik Gradyan fonksiyonu

Burada *x* gerçek girdiyi, x_i baz girdiyi, *F* modelin girdi üzerinde tahminini, α integral boyunca ve *0-1* arasında değişen bir sabiti, $IG_i(x)$ ise girdi *x*'in *i*'inci özelliği için hesaplanan Bütünleşik Gradyan değerini ifade etmektedir.

2.3. Sıralı Ağırlıklı Ortalama Operatörü

Çok kriterli karar verme süreçlerinde başarımını ispatlamış bir yöntem olan sıralı ağırlıklı ortalama operatörü (OWA) (Yager, 1988), çoklu imza karşılaştırmalarında birleştirme operatörü olarak tercih edilmiştir. Birden fazla imza karşılaştırma bilgisini birleştirerek karar verme sürecini farklı parametreler çerçevesinde yönlendirir. Bu yöntem farklı imza örneklerinden elde edilen bilgilerin ağırlıklı bir ortalamasını alarak bir karar puanı üretir.

$$OWA(a_1, \cdots, a_n) = \sum_{j=1}^{n} w_j b_j$$

Şekil 2.20. Sıralı ağırlıklı ortalama operatörü

Şekil 2.20'de *a* girdi değerleri, *w* ağırlık vektörünü, b_j ise a_i değerlerinin *j*'inci büyük olanını (sıralandıktan sonra) ifade etmektedir. Bu operatörün önemi girdilerin sıralamasına göre ağırlık ataması yapmasıdır. Ağırlıklar sıralama pozisyonlarına göre girdilerin değerlerine bağlı olmadan atanır. Dolayısıyla ağırlık vektörünün seçimine göre operatör farklı sonuçlar verecektir.

Çoklu İmza Karşılaştırmaları deneyinde kullanılan ağırlıklar Yager (1988, 1993) tarafından önerilen yöntem ile farklı dilsel niceleyiciler için hesaplanmıştır.

2.4. Deneyler

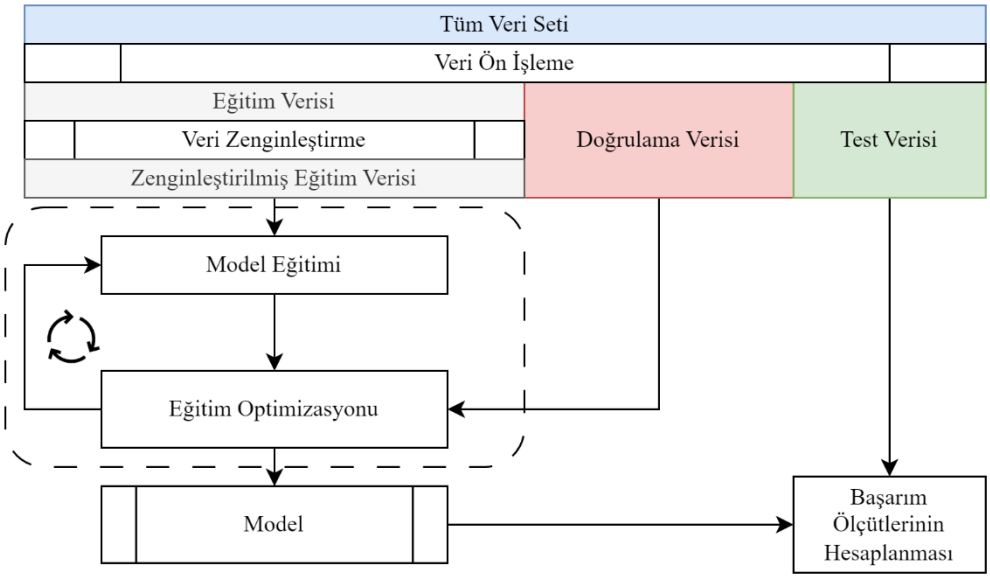
Çalışmada kapsamında farklı deneyler gerçekleştirilmiştir. İlk olarak imza sahteciliği tespiti için farklı derin öğrenme mimarilerinin başarımları karşılaştırılmıştır. Bu ilk aşama ile en yüksek başarıyı gösteren mimari belirlenmiş ardından diğer deney aşamalarına geçilmiştir. Ardından veri seti büyüklüğünün model başarımına etkisi incelenmiştir. Son olarak, çoklu imza testleri yapılarak başarımın artıp artmadığı incelenmiştir. Tüm deneylerde çeşitli başarım ölçütleri hesaplanarak deneyler arasındaki farklılıklar takip edilmiştir.

2.4.1. Mimarilerin Başarımlarının Karşılaştırılması

İlk aşamada, VGG16, ResNet18, ResNet50, Inception, Xception, EfficientNet ve Vision Transformer mimarileri ayrı ayrı eğitilerek test edilmiştir. Her bir mimarinin başarımı, çeşitli başarım ölçütleri üzerinden değerlendirilmiş ve en yüksek başarımı sağlayan mimari tespit edilmiştir. Her mimari üzerinde sıkıştırma ve uyarım dikkat mekanizması ile çok başlıklı öz dikkat mekanizması uygulanmıştır. Dikkat mekanizmaları mimarilerin hangi katmanına eklendiği Dikkat Mekanizmalarının Mimarilere Eklenmesi bölümünde belirtilmiştir.

Karşıt kayıp ve üçlü kayıp fonksiyonu ile ayrı ayrı ön eğitimler yapılmıştır. Yüksek başarım veren kayıp fonksiyonu tercih edilmiştir.

Veri setinin %80'i eğitim ve doğrulama, %20'si ise test için ayrılmıştır. Eğitim ve doğrulama süreci için k-katlamalı çapraz doğrulama yöntemi uygulanmıştır. Şekil 2.21'de eğitim, doğrulama ve test süreçlerinde veri setinin nasıl kullanıldığı görselleştirilmiştir.



Şekil 2.21. Model eğitim sürecinin akış şeması

2.4.2. Veri Seti Büyüklüğünün Başarıma Etkisi

Veri seti büyüklüğünün başarıma etkisini gözlemlemek için öncelikle veri seti farklı oranlara ayrılmıştır. En yüksek başarımlı mimari kullanılarak farklı veri seti oranları için yeni modeller eğitilmiştir. Her bir modelin başarım değişiklikleri gözlemlenmiştir. Bu deney, veri büyüklüğünün modelin genelleştirme yeteneği üzerindeki etkisini belirlemek amacıyla tasarlanmıştır.

Veri setinin %20'si yine test için ayrılmıştır. Eğitim ve doğrulama için ise sırasıyla %60, %40 ve %20'lik oranlarda verinin kullanıldığı üç eğitim daha yapılmıştır.

2.4.3. Çoklu İmza Karşılaştırmaları

Çoklu imza karşılaştırma deneyleri farklı sayıda (2, 3, 4 ve 5) referans imzadan oluşan gruplarla gerçekleştirilmiştir. Önceki deneylerde farklı olarak bu defa bir referans imza yerine birden fazla referans imza girdi olarak kullanılmış ve sorgulanmak istenen imza ile kıyaslanmıştır. Her bir referans imza için elde edilen sonuçlar birleştirilerek nihai sonuca ulaşılmıştır. Birleştirme yöntemi olarak farklı OWA ve ortalama operatörleri kullanılmış ve bu operatörlerin başarıma etkisi incelenmiştir.

2.4.4. Sonuçların Görselleştirilmesi

İmza sahteciliği tespitinde kullanılan modellerin karar verme süreçlerini ve hangi girdilere odaklandıklarını anlamak amacıyla Grad-CAM ve Bütünleşik Gradyanlar yöntemleri uygulanmıştır. Grad-CAM modelin iç katmanlarındaki aktivasyonları kullanarak, belirli sınıflandırma kararları için önemli olan bölgeleri gösteren aktivasyon haritaları oluşturur. Bütünleşik Gradyanlar ise modelin çıktısına en çok katkı sağlayan girdileri vurgulayan önem haritaları oluşturur.

Oluşturulan bu haritalar ısı haritasına dönüştürülmüştür. Modelin imzanın hangi bölgelerine dayanarak karar verdiği referans imza ve sorgulanan imza için oluşturulan ısı haritalarının bu imzaların üzerine eklenerek görselleştirilmesiyle açıklanmaya çalışılmıştır.

2.5. Başarım Değerlendirme Yöntemleri

Elde edilen modellerin başarımını değerlendirmek için çeşitli ölçütler kullanılmıştır.

Kayıp: Modelin tahminlerinin gerçek değerlerden ne kadar sapma gösterdiğinin bir ölçütüdür. Karşıt Kayıp Fonksiyonu ve Üçlü Kayıp Fonksiyonu yardımıyla hesaplanmıştır.

Doğruluk: Modelin tüm sınıflandırmaları ne kadar doğru yaptığının oranıdır.

$$\text{Doğruluk} = \frac{TP + TN}{TP + TN + FP + FN}$$

Şekil 2.22. Doğruluk

Burada *TP* gerçek pozitif, *TN*, gerçek negatif, *FP* yanlış pozitif ve *FN* yanlış negatifleri belirtmektedir.

Hassasiyet: Gerçek pozitif sınıflandırmaların, gerçek pozitif ve yanlış pozitif sınıflandırmaların toplamına oranıdır. Modelin sahte imzaları ne kadar iyi tespit ettiğini gösterir.

$$\text{Hassasiyet} = \frac{TP}{TP + FP}$$

Şekil 2.23. Hassasiyet

Hatırlama: Pozitif olarak sınıflandırılanların ne kadarının gerçekten pozitif olduğunu gösterir.

$$\text{Hatırlama} = \frac{TP}{TP + FN}$$

Şekil 2.24. Hatırlama

F_1 Değeri: Hassasiyet ve hatırlama dengesini gösteren bir ölçüttür, özellikle dengesiz veri setlerinde önemlidir.

$$\text{F}_1\ \text{Değeri} = 2 \cdot \frac{\text{Hassasiyet} \cdot \text{Hatırlama}}{\text{Hassasiyet} + \text{Hatırlama}}$$

Şekil 2.25. F_1 Değeri

Yanlış Kabul Oranı: Yanlış pozitiflerin toplam negatiflere oranıdır. Sahte imzaların yanlışlıkla gerçek olarak kabul edilme olasılığını gösterir.

$$\text{YKO} = \frac{FP}{TN + FP}$$

Şekil 2.26. Yanlış kabul oranı

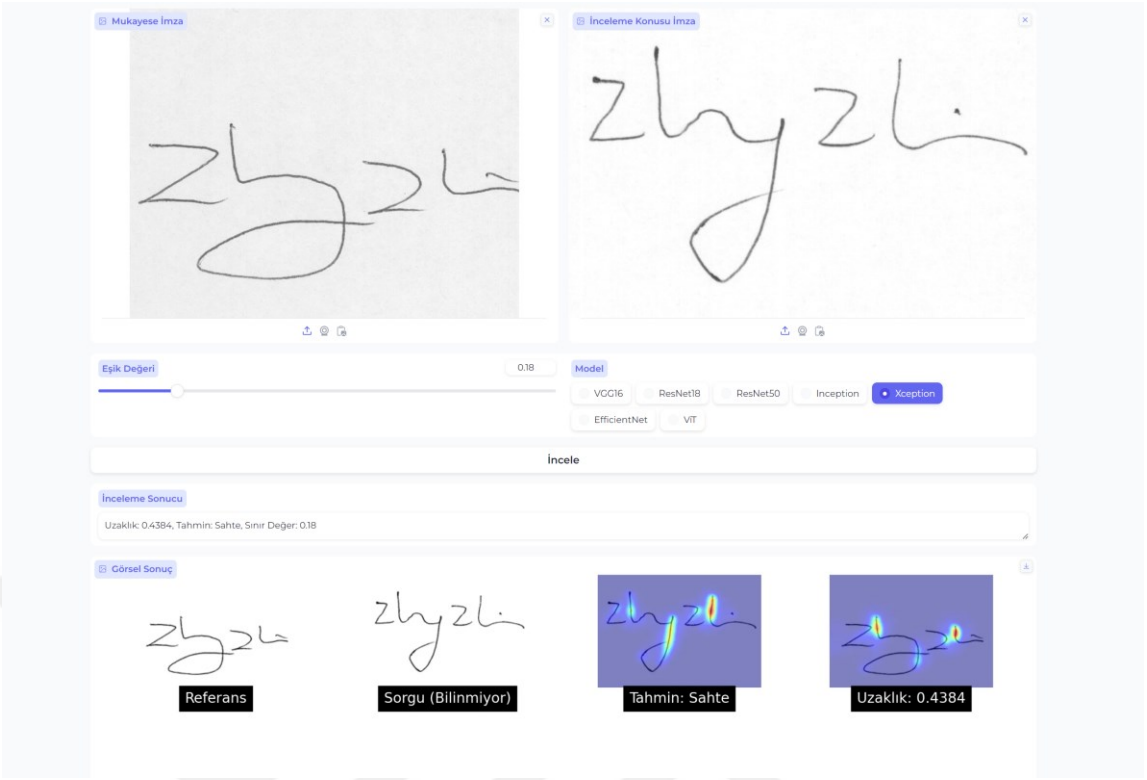
Yanlış Ret Oranı: Yanlış negatiflerin toplam pozitiflere oranıdır. Gerçek imzaların yanlışlıkla sahte olarak reddedilme olasılığını gösterir.

$$\text{YRO} = \frac{FN}{TP + FN}$$

Şekil 2.27. Yanlış ret oranı

2.6. Kullanıcı Arayüzü

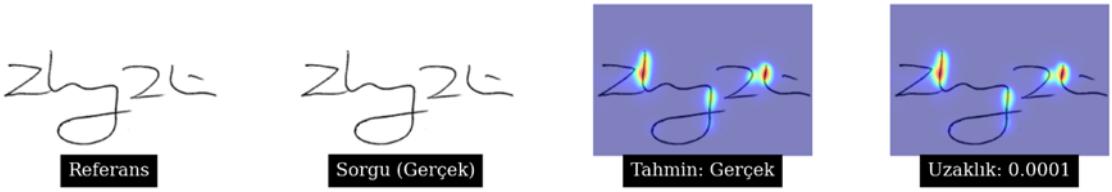
Bu çalışma kapsamında kullanıcıların gerçek kullanım senaryolarını test edilebilmesi için imzaları karşılaştırarak sonuçları görebilecekleri bir kullanıcı arayüzü de hazırlanmıştır. Arayüzün özellikleri arasında imza yükleme, karşılaştırma ve sonuç görselleştirme yer almaktadır. Şekil 2.28'de arayüze ait bir ekran görüntüsü yer almaktadır.



Şekil 2.28. Kullanıcı arayüzü

Kullanıcılar karşılaştırmak istedikleri imzaları kolayca yükleyebilirler. Yüklenen imzalar eğitilmiş olan ikiz sinir ağı modeli kullanılarak karşılaştırılır. Sonuç ekranında modelin kararı ve mesafe ölçümünü gösterilir. Modelin karar verme sürecini açıklamak için dikkat mekanizması kullanılarak hangi özelliklerin önemli olduğu ısı haritası yardımıyla görselleştirilir.

Derin öğrenme modellerinin veri seti üzerinden öğrenemeyeceği durumlar için kullanılan farklı teknikler model çıkışına eklenebilir. Örneğin bu durumlardan birisi iki imzanın neredeyse birebir aynı olduğu durumdur. Eğitilen modeller aynı iki imzayı gerçek olarak sınıflandıracaktır, çünkü modelin hesaplayacağı uzaklık 0'a yakın olacaktır. Şekil 2.29'da bu durumu gösteren bir görsel sunulmuştur. Fakat iki farklı imza arasında doğal varyasyon bulunmaması alan uzmanları tarafından sahte imzanın göstergesi olarak kabul etmektedir (Sayıcı, 2009). Bu nedenle model çıkısının sonuna ek bir kontrol durumu eklenmiş ve modelin gerçek kullanım senaryosunda bu durumu yakalaması sağlanmıştır.



Şekil 2.29. İki aynı imzanın karşılaştırılması

2.7. Geliştirme ve Test Ortamı

Çalışma sırasında donanım olarak Google Colab üzerinde NVIDIA A100 GPU (40GB VRAM) barındıran, 84GB RAM ve 80GB disk kapasiteli sanal sunucu kullanılmıştır.

Kodlama dili olarak Python (v 3.8) kullanılmıştır. PyTorch (v 1.11.0) kütüphanesi derin öğrenme modellerinin geliştirilmesi için tercih edilmiştir. Veri ön işleme ve analizi için pandas (v 2.1) ve NumPy (v 1.24.3) kütüphaneleri kullanılmış, görüntü ön işleme işlemleri için ise OpenCV (v 4.5.2) tercih edilmiştir. ResNet18, ResNet50 ve EfficientNet mimarilerinin TorchVision (v 0.18) kütüphanesindeki uyarlamaları; Inception, Xception, VGG16 ve Vision Transformer mimarilerinin ise PyTorch Image Models (v 1.0.3) kütüphanesindeki uyarlamaları kullanılmıştır. sklearn (v 1.4.2) kütüphanesi ile modellere ait başarım ölçütleri hesaplanmıştır. Derin öğrenme modellerini açıklamak amacıyla grad-cam (v 1.5.0) ve Captum (v 0.4.0) kütüphanelerinden yararlanılmıştır. Model sonuçlarını görselleştirme için Matplotlib (v 3.4.2), istatistiksel analizler için SciPy (v 1.7.1) kütüphaneleri tercih edilmiştir. Kullanıcı arayüzü Gradio (v 4.22.0) kütüphanesi ile oluşturulmuştur.

3. BULGULAR

Bu bölümde çalışmada elde edilen bulgular yer almaktadır. İlk olarak, veri hazırlığı sürecinde elde edilen bulgular sunulmakta, ardından, farklı derin öğrenme mimarilerinin imza sahteciliği tespitindeki başarımları karşılaştırılmaktadır. VGG16, ResNet18, ResNet50, Inception, Xception, EfficientNet ve Vision Transformer mimarilerin eğitim, doğrulama ve test süreçlerinde elde ettikleri başarımlara ait bulgular detaylı olarak paylaşılmaktadır. Veri seti büyüklüğünün model başarımına etkisi ve çoklu imza karşılaştırma deneylerine ait sonuçlar verilmektedir. Elde edilen sonuçlar görselleştirilmekte ve farklı durumlar için örnek görüntüler sunulmaktadır.

3.1. Veri Hazırlığı

Derin öğrenme mimarileri eğitilmeden önce farklı veri ön işleme adımları denenerek, eğitim sürecinde en yüksek başarım elde edilebilecek ön işleme yöntemi belirlenmeye çalışılmıştır. Eşikleme ve normalizasyon yöntemleri hem ayrı ayrı hem de birlikte uygulanmış, en iyi sonuçlar Otsu Eşikleme yönteminin tek başına kullanıldığı durumda elde edilmiştir. Bu nedenle tüm deneylerde imza görüntüleri üzerinde Otsu Eşikleme yöntemi uygulanmıştır.

Veri zenginleştirme işlemi her on imzadan birine ve Veri Zenginleştirme bölümünde bahsedilen yöntemlerden yalnızca biri uygulanacak şekilde yapılmıştır. Bu işlemler rastgele yapılmış olsa da tüm eğitimler esnasında aynı imzaların aynı zenginleştirme yöntemiyle değiştirilmesi sabit bir tohum[6] değeri kullanılarak sağlanmıştır.

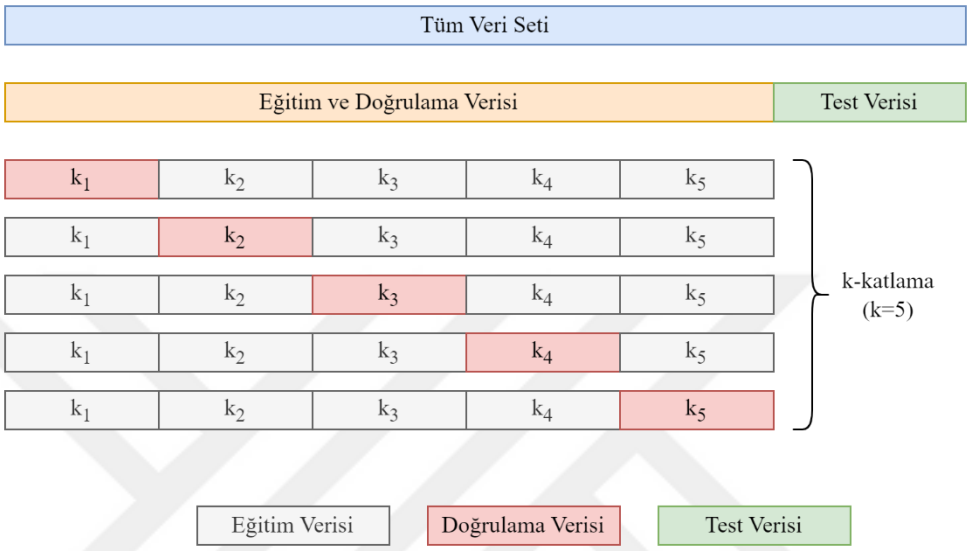
3.2. Mimari Başarımlarının Karşılaştırılması

Bu bölümde dikkat mekanizması eklenerek eğitilmiş farklı mimarideki modellerin başarım sonuçları paylaşılmaktadır.

Eğitim ve doğrulama süreçlerinde k-katlamalı çapraz doğrulama yöntemi (Kohavi, 1995) kullanılmıştır. Bu yöntemle veri seti k sayıda parçaya bölünür ve bu parçalardan biri doğrulama verisi, diğerleri ise eğitim verisi olarak kullanılır. Model her eğitim döneminde bu doğrulama verisiyle test edilir ve bu işlem k kez tekrarlanır. Bu yöntem modelin genelleme yeteneğini artırmayı amaçlar. Kohavi (1995) orta seviyede k değerlerinin varyansı azalttığını,

[6] Tohum (İng. seed) sözde rastgele sayı üretecini başlatmak için kullanılan bir sayıdır. Bu üreteç başlangıç ağırlıklarını belirleme, veri karıştırma ve verilerin eğitim ve doğrulama setlerine ayrılması gibi farklı aşamalarda kullanılan rastgele sayılar üretir. Tohum değerinin sabitlenmesi durumunda bu rastgelelik her defasında aynı olur.

ancak çok yüksek k değerlerinin hesaplama zorluklarına yol açtığını belirtmiştir. Bu çalışmada k değeri olarak 5 seçilmiştir. Şekil 3.1'de veri setinin k-katlamalı çapraz doğrulama için nasıl bölündüğü görselleştirilmiştir. Bu aşamadan sonra elde edilen modeller ise tamamen bağımsız test verisi üzerinden bir kez daha sınanmış ve modellere ait nihai başarım ölçütleri hesaplanmıştır.



Şekil 3.1. Veri setinin k-katlamalı çapraz doğrulama için bölünmesi

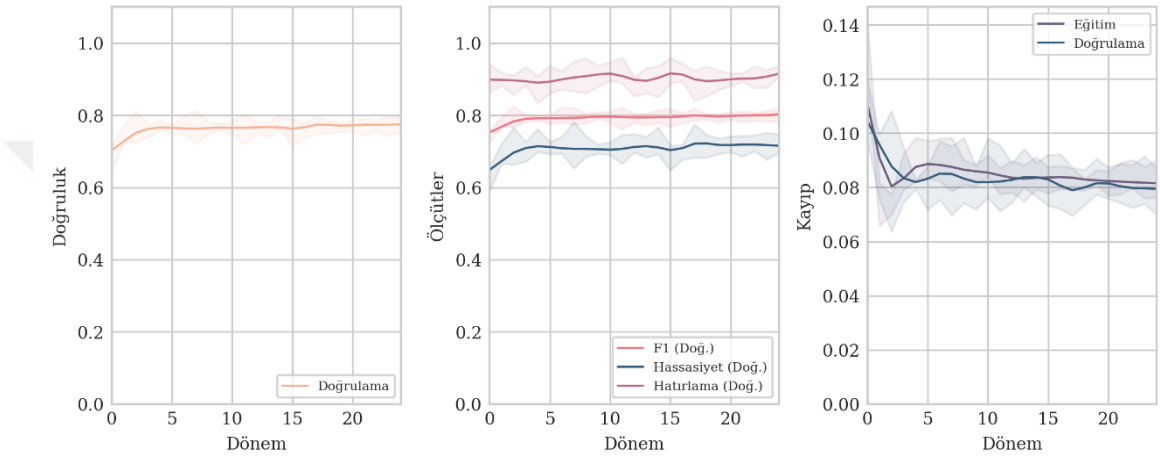
Deney öncesi hazırlıklar esnasında karşıt kayıp ve üçlü kayıp fonksiyonları ile farklı eğitimler gerçekleştirilmiştir. Üçlü kayıp fonksiyonun daha yüksek başarımlı sonuçlar vermesi nedeniyle tüm deneylerde kayıp fonksiyonu olarak üçlü kayıp kullanılmıştır.

Yine farklı ön hazırlık çalışmaları dahilinde mimarilerin son katmanlarına sıkıştırma ve uyarım dikkat mekanizması ve çok başlıklı öz dikkat mekanizmaları eklenmiştir. Hem model başarımını artırması hem de görselleştirme adımında daha anlamlı görüntülerin oluşmasına yardımcı olması nedeniyle çok başlıklı öz dikkat mekanizması tercih edilmiştir.

Aksi belirtilmedikçe, model parametreleri için öğrenme oranı 0,0001 ve ağırlık azaltma değeri 0,05 olarak ayarlanmış bir *Adam* optimizasyon algoritması kullanılmıştır. Öğrenme hızını öğrenmenin yavaşlaması durumunda azaltan bir zamanlayıcı (ReduceLROnPlateau) kullanılmıştır. Zamanlayıcı öğrenmenin yavaşladığı dönemlerde öğrenme hızını %20 oranında düşürecek şekilde ayarlanmıştır. Modellerin aşırı öğrenme yapmasını engellemek için atılma oranı %50 olarak belirlenmiştir.

3.2.1. VGG16

VGG16 mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.2'de paylaşılmıştır. Modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları döneme göre çok yavaş bir şekilde artış göstermektedir. Şekil 3.2'de görüldüğü gibi doğrulama kaybı, eğitim kaybına paralel olarak azalmış ve belirli bir noktadan sonra sabitlenmiştir. Bu da modelin eğitim sürecinin başarılı bir şekilde ilerlediğini ve aşırı öğrenme yaşanmadığını göstermektedir.



Şekil 3.2. VGG16 modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.1'de verilmiştir. En iyi modellerin birçoğu erken eğitim dönemlerinde elde edilmiştir.

Çizelge 3.1. VGG16 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
3	**0,8099**	**0,766**	0,8924	**0,8244**	**0,0774**	**0,0638**	4
12	0,8021	0,7458	0,9167	**0,8224**	0,0775	0,0714	2
18	0,7969	0,7429	0,9080	0,8172	0,0849	0,0695	3
22	0,7917	0,7428	0,8924	0,8107	0,0850	0,0793	5
15	0,7595	0,6919	**0,9358**	0,7956	0,0859	0,0848	1

Çizelge 3.2 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. VGG16 modeline ait eğitim ve test verilerindeki ölçütlerin birbirine yakın olması, modelin eğitildiği veriye fazla bağımlı olmadan genelleme yapabildiğini göstermektedir. Doğruluk ve hassasiyet değerlerinin düşük kalması, modelin bazı sahte imzaları doğru bir şekilde tespit etmekte zorlandığını işaret etmektedir. Hatırlama oranının

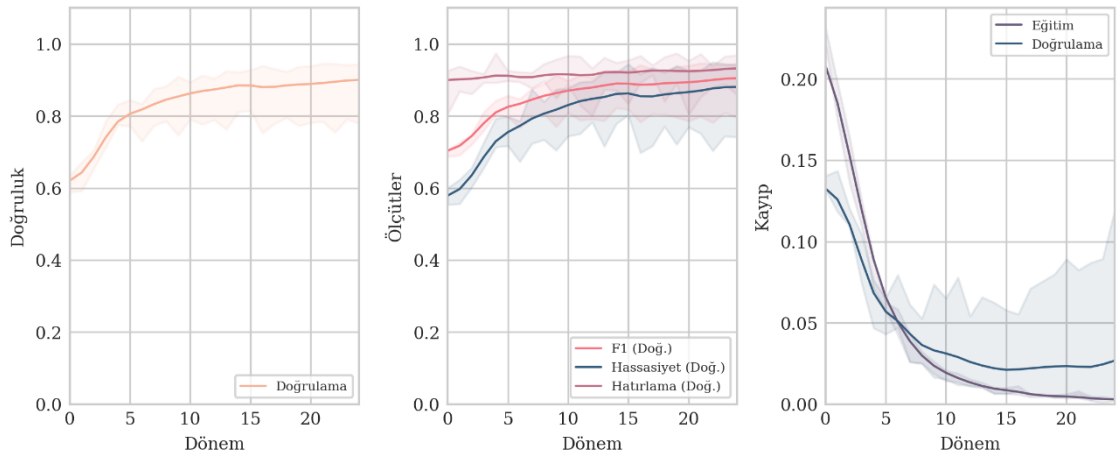
yüksek çıkması ise modelin sahte imzaları tespit etme yeteneğinin güçlü olduğunu göstermektedir.

Çizelge 3.2. VGG16 modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,7914	0,7418	0,8939	0,8108

3.2.2. ResNet18

ResNet18 mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.3'te paylaşılmıştır. ResNet18 modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları döneme göre belirgin bir artış göstermiştir. Özellikle ilk on dönemde hızlı bir iyileşme gözlemlenmektedir. Eğitim ve doğrulama kayıpları da hızla azalmış, ardından sabit bir seviyeye ulaşmıştır. Bu durum modelin iyi bir genelleme kapasitesine sahip olduğunu ve aşırı öğrenme yaşanmadığını göstermektedir.



Şekil 3.3. ResNet18 modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.3'te verilmiştir. Elde edilen modellerin çoğu birbirine yakın başarım göstermektedir.

Çizelge 3.3. ResNet18 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
22	**0,9453**	0,9268	**0,9670**	**0,9465**	0,0038	0,0064	2
25	0,9358	**0,9419**	0,9288	0,9353	**0,0027**	0,0043	4
23	0,9332	0,9416	0,9236	0,9325	**0,0027**	**0,0027**	1
24	0,9184	0,8938	0,9497	0,9209	0,0033	0,0095	5
15	0,8116	0,7783	0,8715	0,8223	0,0064	0,0624	3

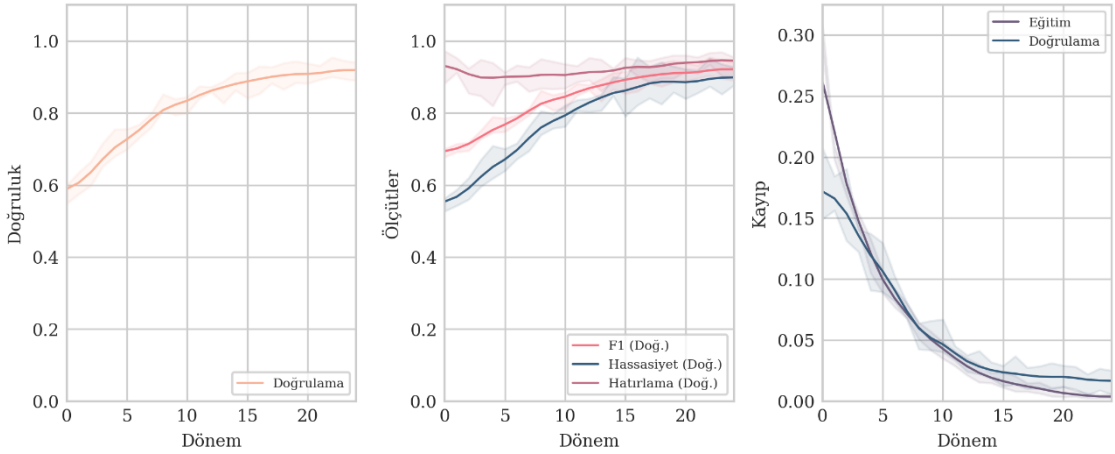
Çizelge 3.4 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. Bu sonuçlar ResNet18 modelinin başarımının test verisinde daha düşük çıktığını göstermektedir. Yine de ResNet18 modeli, VGG16 modeli ile karşılaştırıldığında daha yüksek bir başarım sergilemektedir. ResNet18'in eğitim ve test ölçütleri, modelin sahte imzaları tespit etme konusunda oldukça başarılı olduğunu ve genel olarak iyi bir genelleme kapasitesine sahip olduğunu göstermektedir. Fakat test verisindeki başarımın eğitim verisindeki kadar yüksek olmaması, modelin daha geniş ve çeşitli veri setleri ile eğitilerek genelleme yeteneğinin daha da artırılabileceğini işaret etmektedir.

Çizelge 3.4. ResNet18 modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,8837	0,8598	0,9169	0,8874

3.2.3. ResNet50

ResNet50 mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.4'de paylaşılmıştır. ResNet50 modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları düzenli bir artış göstermiştir. İlk birkaç dönemde hızlı bir iyileşme görülmekte ve ardından başarım değerleri stabilize olmaktadır. Eğitim ve doğrulama kayıpları da döneme bağlı olarak hızlı bir şekilde azalmış ve düşük seviyelerde sabitlenmiştir. Bu, modelin hem eğitim hem de doğrulama verilerinde iyi başarım sergilediğini ve genelleme kapasitesinin yüksek olduğunu göstermektedir.



Şekil 3.4. ResNet50 modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.5'te verilmiştir. En iyi modellerin eğitim döneminin sonlarında elde edilmesi, eğitimin devam ettirilmesi durumunda daha yüksek başarımlı modeller elde edilebileceğini göstermektedir. Eğitimin devam ettirilmesi aşırı öğrenmeye de yol açabilir.

Çizelge 3.5. ResNet50 mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
23	**0,9540**	**0,9516**	0,9566	**0,9541**	0,0063	**0,0050**	4
24	0,9436	0,9223	**0,9688**	0,9450	0,0041	0,0108	1
23	0,9219	0,8869	0,9670	0,9252	**0,0025**	0,0155	2
25	0,9175	0,8911	0,9514	0,9202	**0,0025**	0,0200	5
23	0,9002	0,8736	0,9358	0,9036	0,0031	0,0220	3

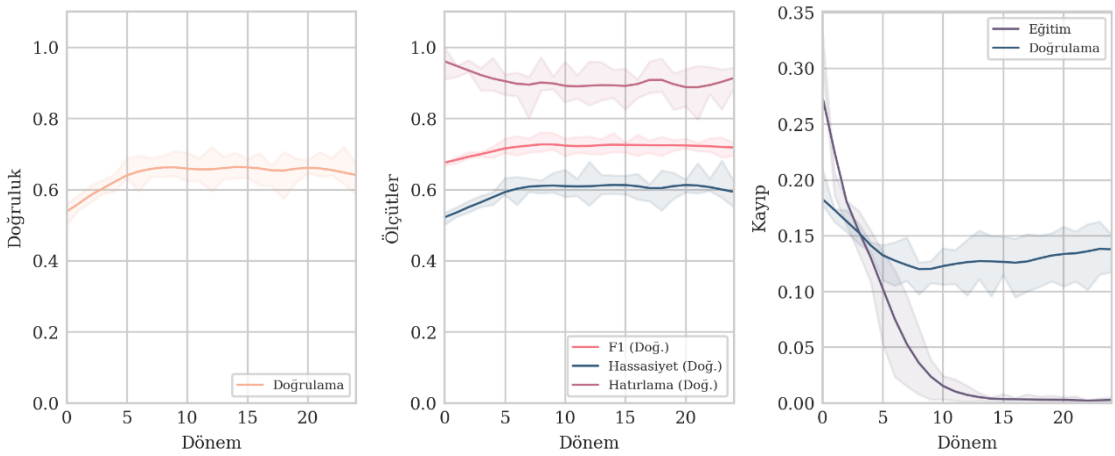
Çizelge 3.6 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. ResNet50 modeli hem eğitim sürecinde hem de test sonucunda oldukça yüksek başarım değerleri elde etmiştir. Modelin sahte imzaları tespit etme yeteneğinin güçlü olduğu söylenebilir. Eğitimde elde edilen ölçütlere kıyasla test sonuçlarında bir miktar düşüş yaşanması modelin genelleme yeteneğinin artırılabileceğini göstermektedir.

Çizelge 3.6. ResNet50 modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,9104	0,8934	0,9321	0,9124

3.2.4. Inception

Inception mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.5'te paylaşılmıştır. Bu mimari için öğrenme oranı 0,00005 olarak seçilmiştir. Inception modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları başlangıçta artış göstermiş, ancak daha sonra belirli bir seviyede dalgalanmalar gözlemlenmiştir. Eğitim kaybı hızlı bir şekilde azalmışken, doğrulama kaybı daha yüksek seviyelerde sabitlenmiş ve bu modelin doğrulama verisinde aşırı öğrenme problemi yaşadığını göstermektedir. Genel olarak, modelin doğrulama başarımı eğitim başarımına kıyasla daha düşük kalmıştır ve genelleme yeteneği sınırlı görünmektedir.



Şekil 3.5. Inception modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.7'de verilmiştir.

Çizelge 3.7. Inception mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
9	0,6953	0,6257	**0,9722**	**0,7614**	0,0562	0,0973	1
17	**0,7031**	**0,6444**	0,9063	0,7532	**0,0040**	**0,0946**	3
10	0,6849	0,6326	0,8819	0,7368	0,0170	0,1076	2
25	0,6745	0,6227	0,8854	0,7312	0,0002	0,1507	5
21	0,6467	0,5984	0,8924	0,7164	0,0018	0,1579	4

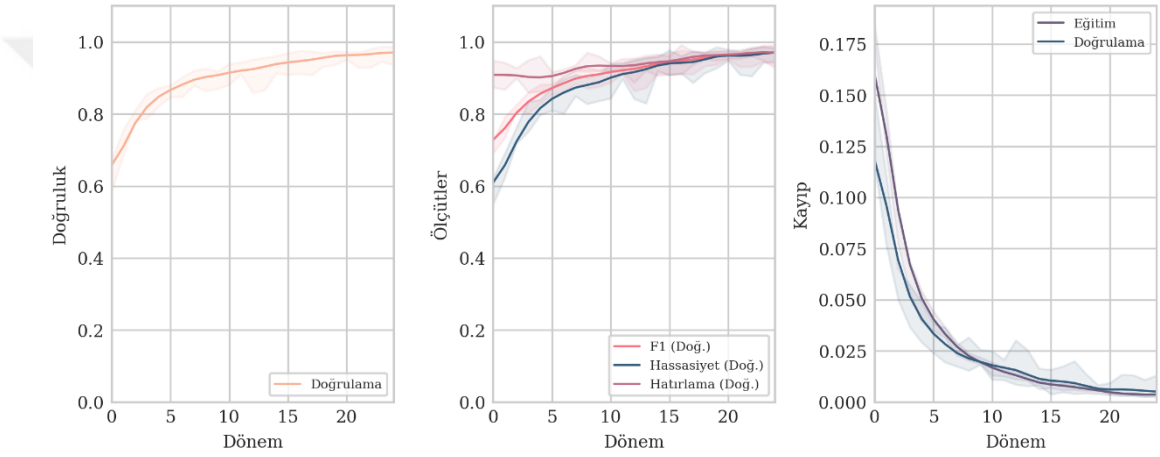
Çizelge 3.8 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. Test verisinde eğitim verisine kıyasla daha yüksek doğruluk ve hassasiyet değerleri elde etmiştir. Bu durum modelin farklı veri setlerinde sahte imzaları tespit etme yeteneğinin güçlü olduğunu göstermektedir. Diğer modellerle kıyaslandığında, eğitim başarımı daha düşük olmasına rağmen, test verisinde daha iyi genelleme yapabildiği görülmektedir. Yine de modelin genel başarımı diğer modellerden oldukça düşüktür.

Çizelge 3.8. Inception modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,7769	0,6976	0,9776	0,8142

3.2.5. Xception

Xception mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.6'da paylaşılmıştır. Xception modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları düzenli bir şekilde artış göstermiştir ve yüksek seviyelerde sabitlenmiştir. Eğitim ve doğrulama kayıpları hızlı bir şekilde azalmış ve oldukça düşük seviyelerde sabitlenmiştir. Bu durum, modelin hem eğitim hem de doğrulama verilerinde yüksek başarım sergilediğini ve genelleme kapasitesinin çok iyi olduğunu göstermektedir. Özellikle doğrulama doğruluğunun yüksek olması, modelin yeni veriler üzerinde de etkili bir şekilde çalışabileceğini göstermektedir.



Şekil 3.6. Xception modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.9'de verilmiştir. Tüm modellerin kusursuza yakın başarım gösterdiği söylenebilir.

Çizelge 3.9. Xception mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
24	**0,9878**	**0,9862**	0,9896	**0,9879**	**0,0035**	0,0027	5
25	0,9861	0,9811	**0,9913**	0,9862	0,0042	**0,0025**	4
23	0,9800	0,9759	0,9844	0,9801	0,0048	0,0031	2
25	0,9783	0,9775	0,9792	0,9783	0,0044	0,0034	3
21	0,9514	0,9483	0,9549	0,9516	0,0039	**0,0093**	1

Çizelge 3.10 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. Xception modeli eğitim sürecinde oldukça yüksek doğruluk, hassasiyet ve hatırlama değerlerine ulaşmıştır. Test verisinde de yüksek başarım göstermiş ve sahte imzaları

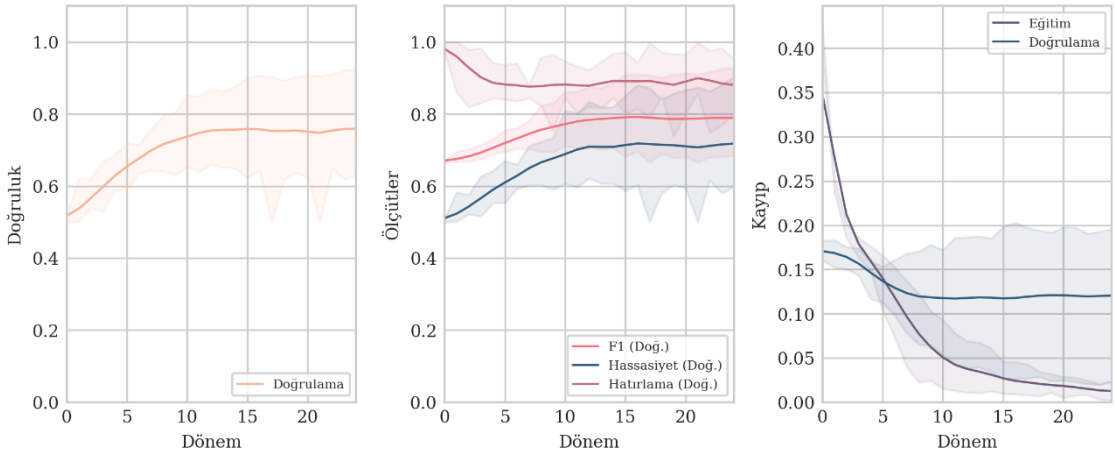
tespit etme yeteneğinin çok güçlü olduğu görülmüştür. Diğer modellerle kıyaslandığında, Xception en yüksek test başarımına sahip modeldir.

Çizelge 3.10. Xception modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,9319	0,9221	0,9435	0,9327

3.2.6. EfficientNet

EfficientNet mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.7'de paylaşılmıştır. EfficientNet modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları belirgin bir artış göstermiştir, ancak bu artış belirli bir noktadan sonra dalgalanmalar göstermektedir. Eğitim kaybı hızlı bir şekilde azalırken, doğrulama kaybı belirli bir seviyede sabitlenmiştir ve dalgalanmalar göstermektedir. Bu durum, modelin doğrulama verisinde aşırı öğrenme problemi yaşadığını ve genelleme yeteneğinde sınırlamalar olduğunu göstermektedir. Modelin doğrulama doğruluğundaki dalgalanmalar, daha fazla veri ile eğitilmesi gerektiğini işaret etmektedir.



Şekil 3.7. EfficientNet modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.11'de verilmiştir. Elde edilen modellerin birbirinden farklı başarımlar göstermesi mimarinin eğitildiği veri setinden oldukça etkilendiğini göstermektedir.

Çizelge 3.11. EfficientNet mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
25	**0,9253**	**0,9030**	**0,9531**	**0,9274**	0,0240	0,0227	5
17	0,8672	0,8190	0,9427	0,8765	0,0455	0,0433	1
16	0,7917	0,7449	0,8872	0,8098	**0,0163**	**0,1137**	2
8	0,6693	0,6230	0,8576	0,7217	0,0837	0,1514	3
13	0,6832	0,6435	0,8212	0,7216	0,0109	0,1815	4

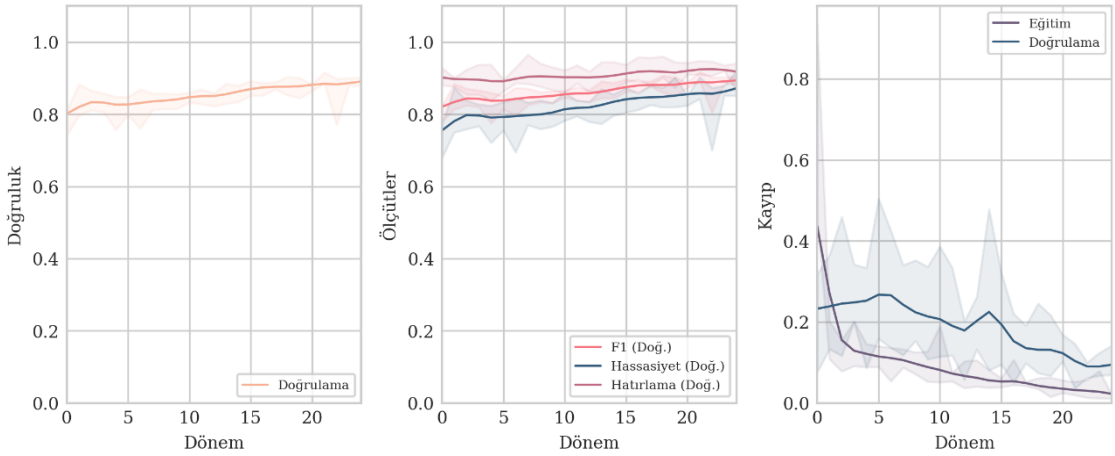
Çizelge 3.12 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. EfficientNet modeli eğitim sürecinde yüksek başarım değerleri elde etmiştir. Test verisinde ise bu değerlere kıyasla bir miktar düşüş gözlemlenmiştir. Modelin genelleme yeteneği sınırlı olabilir. Model sahte imzaları tespit etme konusunda kabul edilebilir bir başarım sergilemektedir. Diğer modellerle kıyaslandığında, genelleme konusunda bazı zorluklar yaşadığı görülmektedir.

Çizelge 3.12. EfficientNet modeli için test sonucunda elde edilen başarım ölçütleri.

Doğruluk	Hassasiyet	Hatırlama	F_1
0,8665	0,8492	0,8912	0,8697

3.2.7. Vision Transformer

Vision Transformer mimarisi ile yapılan eğitim sonucunda elde edilen başarım grafiği Şekil 3.8'de paylaşılmıştır. Bu mimari için atılma oranı %70 olarak uygulanmıştır. Vision Transformer modelinin eğitim sürecinde doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları belirgin bir artış göstermiştir ve nispeten yüksek seviyelerde sabitlenmiştir. Eğitim kaybı hızlı bir şekilde azalırken, doğrulama kaybı daha yüksek seviyelerde dalgalanmalar göstermiştir. Bu durum, modelin doğrulama verisinde aşırı öğrenme yaşama eğilimi olduğunu ve genelleme kapasitesinde sınırlamalar olabileceğini işaret etmektedir. Özellikle doğrulama kaybındaki dalgalanmalar, modelin daha stabil bir başarım elde edebilmesi için daha fazla veri ve düzenleme gerektirebileceğini göstermektedir.



Şekil 3.8. Vision Transformer modelinin eğitim ve doğrulama sürecinde başarımının değişimi

Eğitim sürecince elde edilen en iyi beş modelin başarım ölçütleri Çizelge 3.13'te verilmiştir. En iyi modellerin eğitim döneminin sonlarında elde edilmiş ve modeller arasında başarım açısından çok büyük farklar bulunmamaktadır.

Çizelge 3.13. Vision Transformer mimarisi için eğitim sürecinde elde edilen en iyi başarım ölçütleri

Dönem	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı	k
22	**0,9158**	**0,9025**	0,9323	**0,9172**	**0,0194**	**0,0363**	3
19	0,9036	0,8732	**0,9444**	0,9074	0,0369	0,0740	2
25	0,9010	0,8825	0,9253	0,9034	0,0165	0,0768	5
24	0,9002	0,8785	0,9288	0,9030	0,0794	0,0982	1
24	0,8924	0,8645	0,9306	0,8963	0,0119	0,0674	4

Çizelge 3.14 eğitim sürecinde elde edilen en iyi modelin test verisi üzerindeki başarımını göstermektedir. Vision Transformer modeli eğitim sürecinde yüksek başarım değerlerine ulaşmıştır. Test verisinde ise bu değerlere kıyasla düşüş gözlemlenmiştir. Modelin genelleme yeteneğinin sınırlı olduğu ve aşırı öğrenme yapmış olabileceği söylenebilir. Modelin başarımını artırmak için daha fazla veri ile eğitilmesi gerekebilir. Diğer modellerle kıyaslandığında Vision Transformer'ın başarımı daha düşüktür.

Çizelge 3.14. Vision Transformer modeli için test sonucunda elde edilen başarım ölçütleri

Doğruluk	Hassasiyet	Hatırlama	F_1
0,8186	0,8002	0,8492	0,8240

3.2.8. Tüm Mimarilerin Karşılaştırılması

Çizelge 3.15 farklı derin öğrenme modellerinin eğitim ve doğrulama sürecinde elde ettikleri en yüksek başarım ölçütlerini göstermektedir. Modeller, doğruluk, hassasiyet, hatırlama ve F_1 değeri gibi önemli ölçütler üzerinden karşılaştırılmıştır. Eğitim kaybı ve doğrulama kaybı değerleri de dikkate alınarak, modellerin genelleme kapasitesi değerlendirilmektedir. Xception ve ResNet50 gibi modeller yüksek başarım sergilerken, Inception ve VGG16 gibi modeller nispeten daha düşük başarım göstermektedir. EfficientNet ve Vision Transformer gibi optimize edilmiş ve yenilikçi modeller, çeşitli ölçütlerde dengeli başarım sergilemektedir.

Çizelge 3.15. Farklı modellerin doğrulama sürecinde elde ettikleri başarım ölçütleri

Mimari	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı
Xception	**0,9878**	**0,9862**	**0,9896**	**0,9879**	**0,0035**	**0,0027**
ResNet50	0,9540	0,9516	0,9566	0,9541	0,0063	0,0050
ResNet18	0,9453	0,9268	0,9670	0,9465	0,0038	0,0064
EfficientNet	0,9253	0,9030	0,9531	0,9274	0,0240	0,0227
Vision Transformer	0,9158	0,9025	0,9323	0,9172	0,0194	0,0363
VGG16	0,8099	0,7660	0,8924	0,8244	0,0774	0,0638
Inception	0,6953	0,6257	0,9722	0,7614	0,0562	0,0973

Eğitim ve doğrulama sürecindeki başarımlarına göre modeller arasında istatistiksel olarak anlamlı farklılıklar[7] bulunmaktadır. Birbirine benzer başarım gösteren modeller iki ana grupta toplanmıştır. Xception, ResNet18, ResNet50 ve Vision Transformer modelleri istatistiksel olarak birbirine benzemektedir. Aynı zamanda EfficientNet, Inception, VGG16 ve Vision Transformer modelleri arasında da anlamlı bir fark bulunmamaktadır. Fakat gruplar arasındaki modellerin başarımlarının anlamlı derecede farklı olduğu görülmektedir.

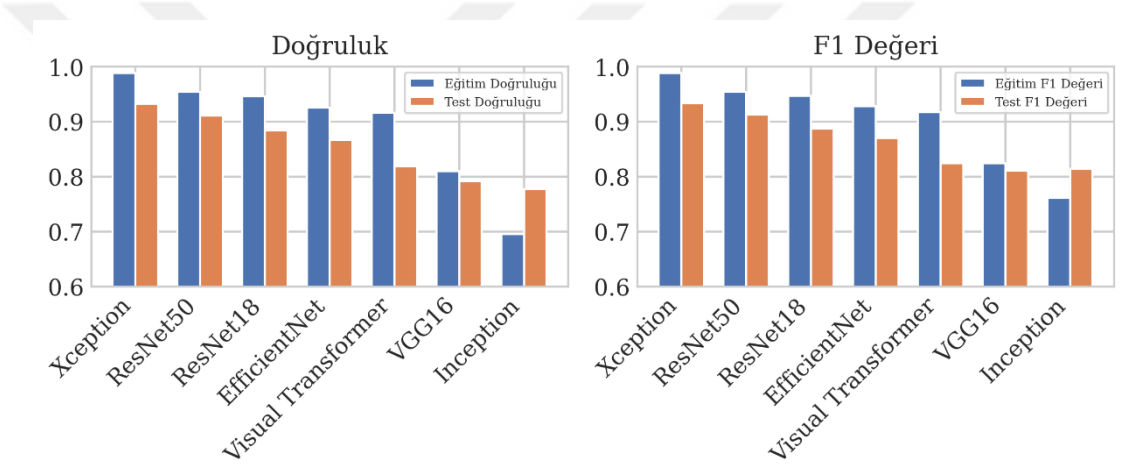
Çizelge 3.16 farklı modellerin test verisi üzerinde elde ettikleri başarım ölçütlerini sunmaktadır. Bu süreçte modellerin eğitim ve doğrulama sırasında öğrendiklerini yeni ve görmediği verilere nasıl uygulayabildiği değerlendirilmektedir. Xception ve ResNet50 modelleri test verisinde de yüksek başarımlarını korumaktadır. Diğer yandan, Inception ve VGG16 gibi modeller test verisinde daha düşük başarım göstermektedir. EfficientNet ve Vision Transformer modelleri test verisinde de eğitim ve doğrulama süreçlerinde elde ettikleri dengeli başarımı büyük ölçüde korumaktadır.

[7] F_1 değerleri üzerinden tek yönlü varyans analizi (One-way ANOVA) uygulanmış ve sonuçlar arasında %95 güven aralığında anlamlı farklar bulunmuştur (F-istatistiği=19.8987, $p<0.0001$). Bu farkların hangi modeller arasında olduğunu belirlemek için Tukey'in HSD testi uygulanmıştır.

Çizelge 3.16. Farklı modellerin test verisi üzerinde elde ettikleri başarım ölçütleri

Mimari	Doğruluk	Hassasiyet	Hatırlama	F_1	YKO	YRO
Xception	**0,9319**	**0,9221**	0,9435	**0,9327**	**0,0797**	0,0565
ResNet50	0,9104	0,8934	0,9321	0,9124	0,1112	0,0679
ResNet18	0,8837	0,8598	0,9169	0,8874	0,1495	0,0831
EfficientNet	0,8665	0,8492	0,8912	0,8697	0,1582	0,1088
Vision Transformer	0,8186	0,8002	0,8492	0,8240	0,2120	0,1508
Inception	0,7769	0,6976	**0,9776**	0,8142	0,4238	**0,0224**
VGG16	0,7914	0,7418	0,8939	0,8108	0,3112	0,1061

Şekil 3.9'da yedi farklı derin öğrenme modelinin eğitim ve test süreçlerindeki doğruluk ve F_1 değeri başarımlarını karşılaştırmaktadır. Inception modeli hariç tüm modeller eğitim başarımından daha düşük test başarımı göstermiştir.

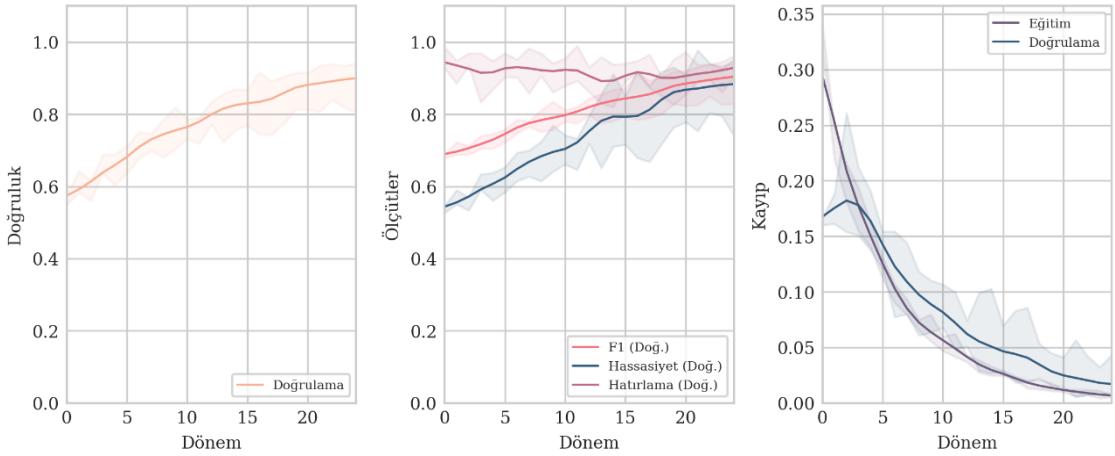


Şekil 3.9. Eğitilen tüm mimarilerin doğruluk ve F_1 değeri üzerinden karşılaştırılması

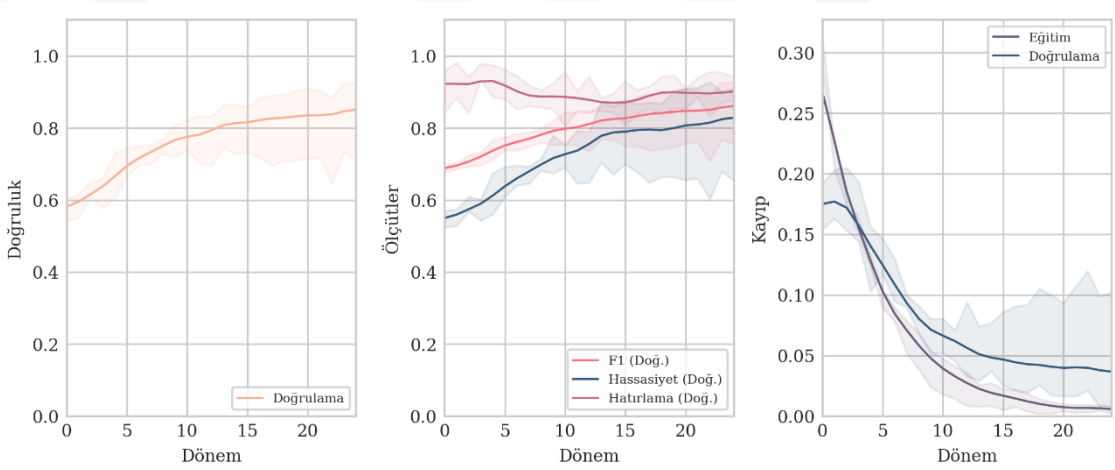
3.3. Veri Seti Büyüklüğünün Başarıma Etkisi

Bu bölümde farklı veri seti büyüklükleri ile aynı şekilde eğitilmiş farklı ResNet50 mimarisindeki modellerin başarım sonuçları paylaşılmaktadır. Veri setinin eğitim ve doğrulama için kullanılacak kısmı sırasıyla %60, %40 ve %20 olarak sınırlandırılmış, elde edilen en başarımlı modeller aynı test veri seti üzerinden test edilerek başarımları ölçülmüştür.

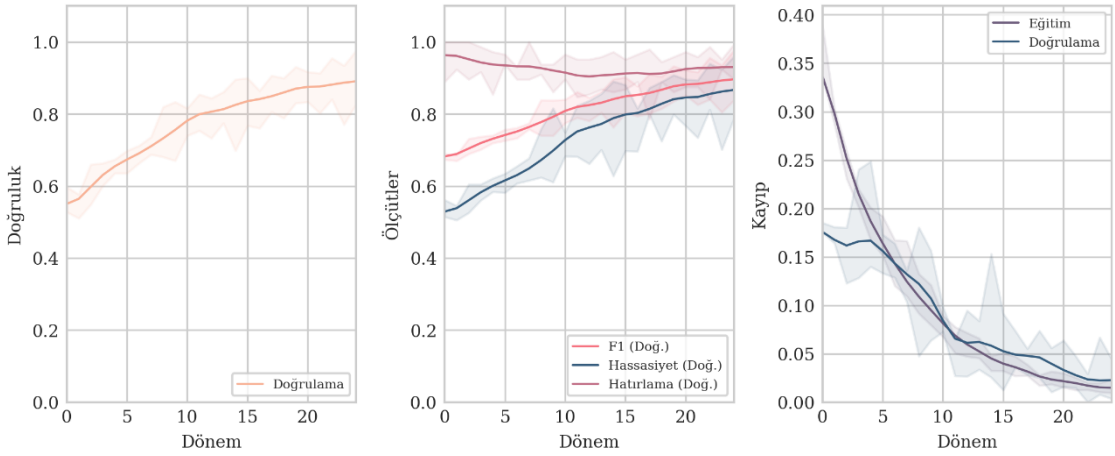
Şekil 3.10, Şekil 3.11 ve Şekil 3.12'de sırasıyla %60, %40 ve %20'lik veri setleriyle gerçekleştirilen deneylere ait eğitim ve doğrulama süreçlerinin başarım grafikleri yer almaktadır. Tüm eğitimler boyunca doğruluk, F_1 değeri, hassasiyet ve hatırlama oranları genel olarak artış göstermektedir. Küçük veri setleriyle eğitilen modellerde doğruluk ve hassasiyet oranlarının dalgalanma göstermesi, bu modellerin genelleme yapmada zorluk yaşadığını ve aşırı öğrenme riski taşıdığını göstermektedir.



Şekil 3.10. %60'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi



Şekil 3.11. %40'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi



Şekil 3.12. %20'lık veri seti ile gerçekleştirilen eğitim ve doğrulama sürecinde başarımın değişimi

Çizelge 3.17'de modellerin doğrulama sürecinde elde ettikleri başarım ölçütleri verilmiştir. Eğitim ve doğrulama sonuçlarına incelendiğinde, veri seti büyüklüğünün azalmasıyla birlikte başarım ölçütlerinde artış gözlemlenmektedir. Özellikle %20 veri seti ile eğitilen model en yüksek değerleri elde etmiştir. Bu durum modelin eğitim verisine daha iyi adapte olduğunu gösterebileceği gibi aşırı öğrenmeye de işaret edebilir.

Çizelge 3.17. Modellerin doğrulama sürecinde elde ettikleri başarım ölçütleri

Mimari	Doğruluk	Hassasiyet	Hatırlama	F_1	Eğitim Kaybı	Doğrulama Kaybı
%80[8]	0,9540	0,9516	0,9566	0,9541	0,0063	0,0050
%60	0,9248	0,9015	0,9537	0,9269	0,0076	0,0077
%40	0,9410	0,9504	0,9306	0,9404	**0,0053**	0,0087
%20	**0,9757**	**0,9597**	**0,9931**	**0,9761**	0,0096	**0,0034**

Çizelge 3.18'de ise modellerin test verisi üzerindeki başarım ölçütleri sunulmuştur. Test sonuçlarına bakıldığında veri seti büyüklüğünün azalmasıyla birlikte başarım ölçütlerinde belirgin bir düşüş gözlemlenmiştir. En büyük veri seti ile eğitilen model test verisinde en yüksek başarımı elde etmiştir. Veri seti büyüklüğü %20'ye düştüğünde ise başarım ölçütlerinde ciddi bir düşüş yaşanmıştır. Küçük veri setleriyle eğitilen modellerin hiç karşılaşmadığı veriler üzerinde genelleme yapma yeteneğinin azaldığı anlaşılmakta, aynı modellerin eğitim sürecinde yüksek başarım göstermesi de aşırı öğrenme yaptıklarını ortaya koymaktadır.

Çizelge 3.18. Modellerin test verisi üzerinde elde ettikleri başarım ölçütleri

Test Verisi Büyüklüğü	Doğruluk	Hassasiyet	Hatırlama	F_1	YKO	YRO
%80	**0,9104**	**0,8934**	**0,9321**	**0,9124**	**0,1112**	**0,0679**
%60	0,8095	0,7625	0,8953	0,8236	0,2764	0,1047
%40	0,7335	0,6955	0,8345	0,7587	0,3675	0,1655
%20	0,5816	0,5554	0,8189	0,6619	0,6557	0,1811

3.4. Çoklu İmza Karşılaştırmaları

Bu bölümde çoklu imza karşılaştırma deneylerinin bulguları yer almaktadır. Deneyler sırasıyla 2, 3, 4 ve 5 referans imza kullanılarak gerçekleştirilmiş ve her bir referans imza için elde edilen sonuçlar birleştirilerek nihai sonuca ulaşılmıştır. Bu süreçte model yeniden eğitilmemiş, sadece modelden çıkan sonuçlar OWA operatörü ve ortalama operatörü (AVG) ile tekrar hesaplanmıştır. OWA operatöründe kullanılan ağırlıklar için dilsel niceleyiciler kullanılmıştır.

[8] 3.2.3 bölümünde elde edilen modele ait veriler kullanılmıştır.

Referans sayısının sınırlı olması nedeniyle “en az biri” ve “birçoğu” dilsel niceleyicileri tercih edilmiştir.

Çizelge 3.19’da farklı sayıdaki referans imzalar için elde edilen başarım ölçütleri verilmiştir. İki referans imza kullanıldığında, tüm ölçütlerde genel bir iyileşme gözlemlenmiştir. "En az biri" OWA operatörü, diğerlerine kıyasla daha iyi sonuçlar vermiştir. "Birçoğu" OWA operatörü ise biraz daha düşük başarım göstermiştir. Üç ve dört referans imza kullanıldığında, ölçütlerdeki iyileşme devam etmektedir. "En az biri" operatörü, yine en iyi başarımı sergilemektedir. Ortalama ve "birçoğu" operatörleri arasında çok büyük farklar gözlemlenmemiştir. Beş referans imza kullanıldığında, başarım ölçütleri genel olarak iyileşmeye devam etmektedir, ancak üç ve dört referans imza ile elde edilen sonuçlara benzerlik göstermektedir. Beş imza kullanmanın sadece "En az biri" operatörü için ek bir fayda sağladığı söylenebilir. Bu bulgular imza sahteciliği tespitinde çoklu referans imza kullanımının faydasını ve "en az biri" operatörünün etkinliğini gösteriyor olsa da operatör seçiminin sonuçlara istatistiksel olarak anlamlı bir fark[9] kattığı söylenememektedir.

Çizelge 3.19. Çoklu imza karşılaştırmaları sonuçları

	Ortalama				**OWA (En Az Biri)**				**OWA (Birçoğu)**			
İmza Sayısı	Doğruluk	Hassasiyet	Hatırlama	F_1	Doğruluk	Hassasiyet	Hatırlama	F_1	Doğruluk	Hassasiyet	Hatırlama	F_1
1	0,9104	0,8934	0,9321	0,9124	-	-	-	-	-	-	-	-
2	0,9170	0,9017	0,9360	0,9185	**0,9190**	**0,9037**	**0,9380**	**0,9205**	0,9150	0,8998	0,9340	0,9166
3	0,9230	0,9075	0,9420	0,9244	**0,9270**	**0,9114**	**0,9460**	**0,9284**	0,9210	0,9056	0,9400	0,9225
4	0,9310	0,9152	0,9500	0,9323	**0,9390**	**0,9229**	**0,9580**	**0,9401**	0,9290	0,9133	0,9480	0,9303
5	0,9270	0,9114	0,9460	0,9284	**0,9410**	**0,9249**	**0,9600**	**0,9421**	0,9250	0,9094	0,9440	0,9264

3.5. Sonuçların Görselleştirilmesi

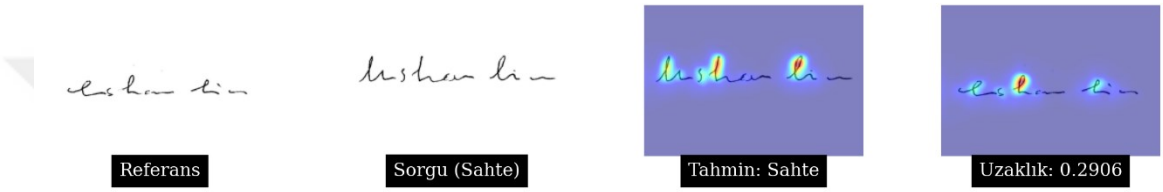
Bu deneyde karar verme süreçlerini anlamak ve görselleştirmek için ilk olarak Grad-CAM yöntemi denenmiş, ancak tatmin edici sonuçlar elde edilememiştir. Bunun üzerine bir diğer görselleştirme yöntemi olan Bütünleşik Gradyanlar yöntemi kullanılmıştır. Modelin çıktısına en çok katkı sağlayan girdileri vurgulayan önem haritaları oluşturulmuş, bu haritalar ısı haritasına dönüştürülerek imza görselleri üzerine eklenmiştir. Modelin imzanın hangi bölgelerine dayanarak karar verdiği görselleştirilmiştir. Elde edilen görseller modelin karar verme süreçlerini daha iyi anlamak için kritik öneme sahiptir. Gerçek pozitif ve gerçek negatif

[9] F_1 değerleri üzerinden tek yönlü varyans analizi (One-way ANOVA) uygulanmış ve sonuçlar arasında %95 güven aralığında anlamlı bir fark bulunamamıştır. (F-istatistiği=0.7491, p=0.4937)

örneklerde modelin hangi özelliklere dikkat ettiğini, yanlış pozitif ve yanlış negatif örneklerde ise hangi özelliklerin modelin hata yapmasına neden olduğunu görselleştirerek, alan uzmanlarının ve karar vericilerin modelin kararlarını daha iyi yorumlamalarına ve güvenilirliklerini değerlendirmelerine olanak tanır. Bu sayede imza sahteciliği tespiti sürecinde daha bilinçli ve doğru kararlar alınabilir.

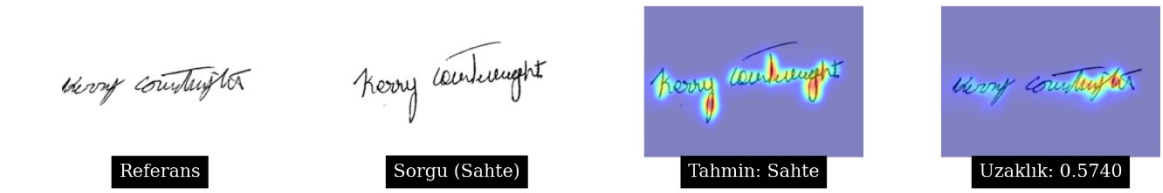
3.5.1. Gerçek Pozitif Örnekler

Modelin sahte imzayı sahte olarak doğru bir şekilde sınıflandırdığı durumdur. Bu durumun gerçekleştiği bazı örnekler Şekil 3.13, Şekil 3.14 ve Şekil 3.15'de gösterilmektedir.



Şekil 3.13. Modelin çıktısının gerçek pozitif olduğu bir örnek (1)

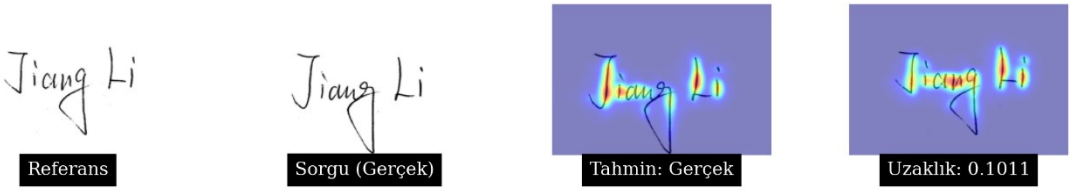
Şekil 3.14. Modelin çıktısının gerçek pozitif olduğu bir örnek (2)



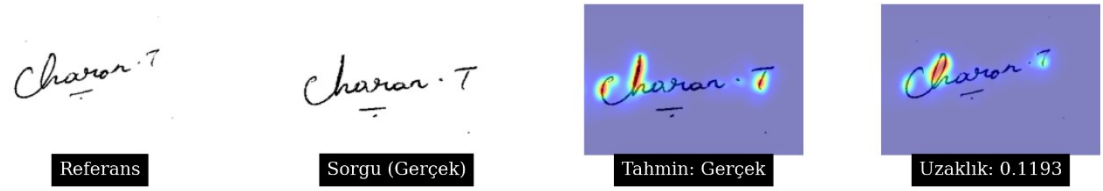
Şekil 3.15. Modelin çıktısının gerçek pozitif olduğu bir örnek (3)

3.5.2. Gerçek Negatif Örnekler

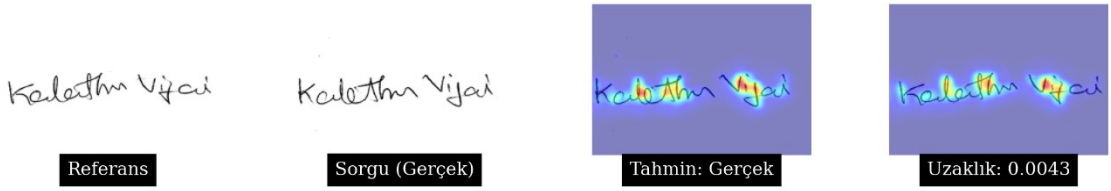
Modelin gerçek imzayı gerçek olarak doğru bir şekilde sınıflandırdığı durumdur. Bu durumun gerçekleştiği bazı örnekler Şekil 3.16, Şekil 3.17 ve Şekil 3.18'de gösterilmektedir.



Şekil 3.16. Modelin çıktısının gerçek negatif olduğu bir örnek (1)



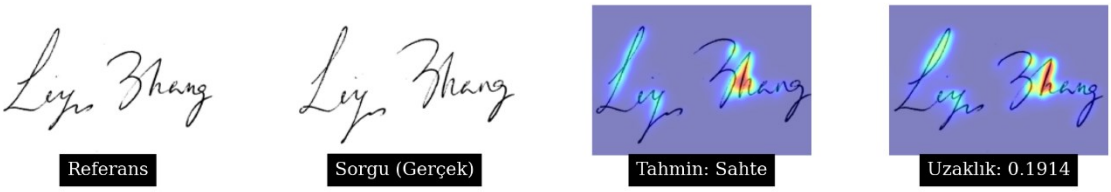
Şekil 3.17. Modelin çıktısının gerçek negatif olduğu bir örnek (2)



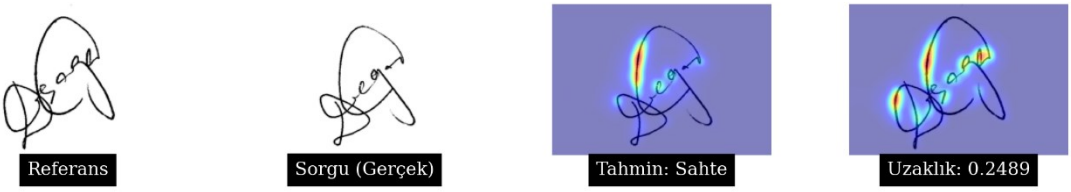
Şekil 3.18. Modelin çıktısının gerçek negatif olduğu bir örnek (3)

3.5.3. Yanlış Pozitif Örnekler

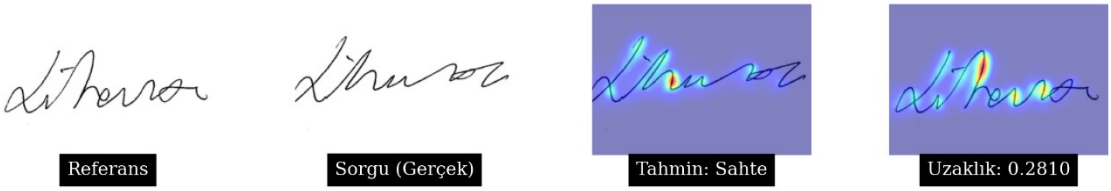
Modelin gerçek imzayı sahte olarak yanlış bir şekilde sınıflandırdığı durumdur. Bu durumun gerçekleştiği bazı örnekler Şekil 3.19, Şekil 3.20 ve Şekil 3.21'de gösterilmektedir.



Şekil 3.19. Modelin çıktısının yanlış pozitif olduğu bir örnek (1)



Şekil 3.20. Modelin çıktısının yanlış pozitif olduğu bir örnek (2)

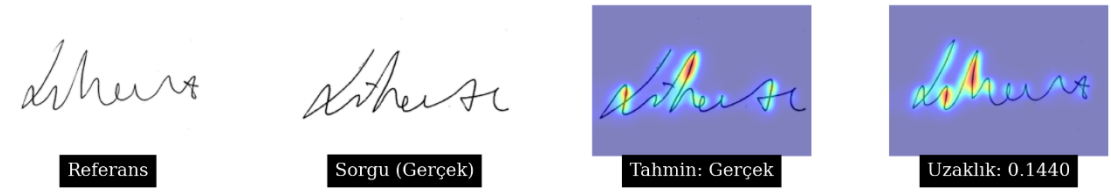


Şekil 3.21. Modelin çıktısının yanlış pozitif olduğu bir örnek (3)

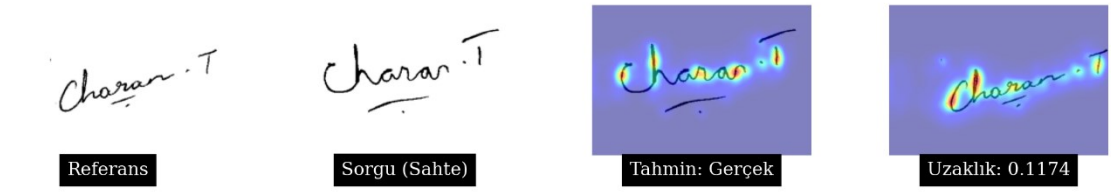
3.5.4. Yanlış Negatif Örnekler

Modelin sahte imzayı gerçek olarak yanlış bir şekilde sınıflandırdığı durumdur. Bu durumun gerçekleştiği bazı örnekler Şekil 3.22, Şekil 3.23 ve Şekil 3.24'de gösterilmektedir.

Şekil 3.22. Modelin çıktısının yanlış negatif olduğu bir örnek (1)



Şekil 3.23. Modelin çıktısının yanlış negatif olduğu bir örnek (2)



Şekil 3.24. Modelin çıktısının yanlış negatif olduğu bir örnek (3)

4. TARTIŞMA

Bu çalışmada adli belge inceleme alanının en zorlu ve önemli konularından biri olan imza sahteciliği tespiti için çeşitli derin öğrenme modellerinin dikkat mekanizmaları ile kullanımına yönelik bir seri deney gerçekleştirilmiştir. Elde edilen modellerin sonuçları görselleştirilerek derin öğrenme modellerinin karar süreçlerinin açıklanabilir hale getirilmeye çalışılmıştır.

Ülkemizde imza sahteciliği tespitinde derin öğrenme yöntemlerinin kullanıldığı çalışmalar (Arısoy, 2021; Çalik vd., 2017; Ebrahimpour, 2023; Majidpour vd., 2023; Ozkan ve Erdogmus, 2024) yapılmış olsa da dikkat mekanizmalarının kullanıldığı ve karar süreçlerinin açıklanabilir hale getirildiği bir çalışma bilindiği kadarıyla bulunmamaktadır. Uluslararası literatürde ise benzer çalışmaların (Diaz vd., 2024; Hamm vd., 2023; Kao ve Wen, 2020; Kao vd., 2020; Solanke, 2022) sayısı ise oldukça sınırlıdır.

Deneylere başlamadan önce gerçekleştirilen veri hazırlığı aşamasında gerçek ve sahte imza görsellerinin (Şekil 2.1) arka planlarında kolayca ayırt edilebilir şekilde ton farkı olduğu dikkat çekmiştir. Verilerin ön işlemeye tabii tutulmadan model eğitimine başlanılması, eğitim sürecinin ilk dönemlerinde hızlı bir şekilde öğrenmeyi ve test aşamasında da yüksek başarımı sağlayacaktır. Bu yanıltıcı durum modelin veri seti dışındaki hiç görmediği verilerde başarısız olmasına neden olacaktır. Model imzalardaki özellikler yerine arka plandaki özelliklere odaklanmaktadır. Veri hazırlığı aşamasında uygulanan Otsu eşikleme yöntemi sayesinde, eğitilen modellerin bu durumdan etkilenmesi engellenmiştir. Otsu eşiklemesi yalnızca derin öğrenme modellerini eğitirken değil, literatürde imza sahteciliği tespitinde çalışılan birçok farklı yöntemde (Anagha ve Kumar, 2023; Ferrer vd., 2012; Hameed vd., 2021; Narayana vd., 2017; Yan vd., 2022) de sıklıkla kullanılmaktadır.

Modellerin eğitim sürecinde kullanılan üçlü kayıp fonksiyonu, karşıt kayıp fonksiyonuna göre daha başarılı eğitimlerin gerçekleşmesini sağlamıştır. İmza özniteliklerinin öğreniminde farklı kayıp fonksiyonlarını karşılaştıran Viana vd. (2023) göre üçlü kayıp fonksiyonu marjin değerinin uygun şekilde ayarlanması durumunda daha yüksek model başarımı sağlamakta, karşıt kayıp fonksiyonu ile eğitilen modeller ise farklı veri setlerine karşı genelleme yeteneğini kaybetmektedir. Ayrıca, Guo vd. (2024) çevrim dışı imza doğrulama modellerinde karşıt kayıp fonksiyonunun kullanımının saldırılara açık olduğundan bahsetmektedir, yani sahte imzalar sayısal olarak manipüle edilerek modeller kandırılabilmektedir.

Çalışma kapsamında derin öğrenme mimarilerin son katmanlarına sıkıştırma ve uyarım dikkat mekanizması ve çok başlıklı öz dikkat mekanizmaları eklenmiştir.

Sıkıştırma ve uyarım dikkat mekanizmasının model başarımına etkisi olmamış ve görselleştirme adımında açıklanabilir sonuçlar elde edilememiştir. Bu durum literatürdeki diğer çalışmalarla (Ren vd., 2022; Xiong ve Cheng, 2021; Xiong vd., 2024) çelişmektedir. Bunun nedeni sıkıştırma ve uyarım dikkat mekanizmasının belirli veri setleri ve imza türleri üzerinde etkili olmaması veya modelin bu dikkat mekanizmalarını tam olarak öğrenememesi olabilir. Diğer çalışmalarda da CEDAR veri setinin kullanıldığı düşünüldüğünde, modellerin mimari yapısı, eğitim sürecindeki hiper parametre ayarları gibi diğer faktörler başarısız sonuçlara yol açmış olabilir.

Çok başlıklı öz dikkat mekanizması ile model başarımı yükseltilmiş ve sonuçları görselleştirme aşamasında daha anlamlı ısı haritaları elde edilmiştir. Chu vd. (2023) ile Li vd. (2024) tarafından yapılan çalışmalarda da çok başlıklı öz dikkat mekanizmalarının imza sahteciliği tespitinde model başarımlarını arttırdığı görülmektedir.

Deneylerde kullanılan modeller VGG16, ResNet18, ResNet50, Inception, Xception, EfficientNet, ve Vision Transformer'dır.

VGG16 modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %80,99, %76,6 ve %89,24'e ulaştığı görülmüştür. Test verisinde ise sırasıyla %79,14, %74,18 ve %89,39 değerleri elde edilmiştir. Bu değerler VGG16'nın sahte imzaları tespit etmede başarılı olduğunu, ancak sahte olarak değerlendirdiği imzaların dikkate değer bir oranının aslında gerçek olduğunu göstermektedir. VGG16'nın daha düşük başarım sergilemesinin olası nedeni, bu modelin daha eski ve daha az karmaşık bir yapıya sahip olmasıdır; dolayısıyla daha yeni ve daha karmaşık modellerle karşılaştırıldığında daha düşük bir genelleme yeteneği göstermiştir.

ResNet18 modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %94,53, %92,68 ve %96,7'e ulaştığı görülmüştür. Test verisinde ise sırasıyla %88,37, %85,98 ve %91,69 değerleri elde edilmiştir. Bu bulgular ResNet18'in sahte imzaların çoğunu başarılı bir şekilde tespit ettiğini ve sahte olarak değerlendirdiği imzaların büyük bir kısmının gerçekten sahte olduğunu göstermektedir.

ResNet50 modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %95,4, %95,16 ve %95,66'ya ulaştığı görülmüştür. Test verisinde ise sırasıyla %91,04,

%89,34 ve %93,21 değerleri elde edilmiştir. Bu sonuçlar ResNet50'nin sahte imzaları tespit etme yeteneğinin güçlü olduğunu ve sahte olarak değerlendirdiği imzaların çoğunun gerçekten sahte olduğunu göstermektedir.

Inception modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %69,53, %62,57 ve %97,22'ye ulaştığı görülmüştür. Test verisinde ise sırasıyla %77,69, %69,76 ve %97,76 değerleri elde edilmiştir. Bu değerler Inception'ın sahte imzaların neredeyse tamamını tespit edebildiğini ancak sahte olarak değerlendirdiği imzaların dikkate değer bir kısmının aslında gerçek olduğunu göstermektedir.

Xception modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %98,78, %98,62 ve %98,96'ya ulaştığı görülmüştür. Test verisinde ise sırasıyla %93,19, %92,21 ve %94,35 değerleri elde edilmiştir. Bu sonuçlar Xception'ın sahte imzaları tespit etme konusunda çok güçlü olduğunu ve sahte olarak değerlendirdiği imzaların büyük çoğunluğunun gerçekten sahte olduğunu göstermektedir.

EfficientNet modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %92,53, %90,3 ve %95,31'e ulaştığı görülmüştür. Test verisinde ise sırasıyla %86,65, %84,92 ve %89,12 değerleri elde edilmiştir. Bu bulgular EfficientNet'nın sahte imzaları tespit etme yeteneğinin kabul edilebilir olduğunu, ancak sahte olarak değerlendirdiği imzaların dikkate değer bir kısmının aslında gerçek olduğunu göstermektedir.

Vision Transformer modelinin eğitim sürecinde doğruluk, hassasiyet ve hatırlama değerlerinin sırasıyla %91,58, %90,25 ve %93,23'e ulaştığı görülmüştür. Test verisinde ise sırasıyla %81,86, %80,02 ve %84,92 değerleri elde edilmiştir. Bu değerler Vision Transformer'ın sahte imzaların çoğunu başarılı bir şekilde bulduğunu, ancak sahte olarak değerlendirdiği imzaların dikkate değer bir oranının aslında gerçek olduğunu göstermektedir.

Xception ve ResNet50 modelleri hem eğitim hem de test verilerinde yüksek başarım göstermesinin nedeni modellerin derin mimarileri ve yüksek genelleme kapasiteleri ile açıklanabilir. Bu modellerin karmaşık öznitelikleri ve örüntüleri tespit etme yetenekleri, imza sahteciliği tespitinde yüksek başarım göstermelerine katkıda bulunmuş olmalıdır. Eğitim sürecinde kullanılan veri ön işleme ve zenginleştirme tekniklerinin de bu modellerin başarımlarına olumlu katkıda bulunduğu söylenebilir.

Vision Transformer modeli genellikle görsel görevlerde başarılı başarım sergilemesi beklenen bir modeldir. Bu çalışmada düşük başarım göstermesinin nedeni, modelin büyük veri setleriyle

eğitildiğinde yüksek başarım göstermesi fakat daha küçük ve sınırlı veri setlerinde genelleme yeteneğinin azalması olabilir. Dönüştürücü modelleri yüksek hesaplama kaynakları gerektirmesi ve çalışmada kullanılan donanımın sınırlı kapasitede olması model başarımını olumsuz etkilemiş olabilir. EfficientNet modeli de beklenen başarımın altında kalmıştır. Modelin aşırı öğrenme eğilimi göstermesinden kaynaklanabilir. Inception modeli genellikle karmaşık yapıların tespitinde başarılı olmasına rağmen, bu çalışmada düşük başarım sergilemiştir. Modelin eğitimi esnasında öğrenme oranının aşırı öğrenmeyi engellemek için oldukça düşürülmesine rağmen, modelin yaşadığı aşırı öğrenme problemleri engellenememiştir. Bu durum hiper parametre seçimine daha fazla zaman ayrılarak ve veri seti daha fazla zenginleştirilerek çözülebilir. VGG16 modeli diğer mimarilere göre daha eski bir modeldir ve derinlik açısından sınırlı kalabilir. Bu da modelin daha karmaşık sahtecilik tespit görevlerinde yeterince iyi başarım göstermemesine yol açmış olabilir. Eğitim verisine bağımlılık ve veri zenginleştirme eksiklikleri de bu başarım düşüklüğüne katkıda bulunmuş olabilir.

Yan vd. (2022) çalışmasında özellikle Inception gibi yeni mimarilerin ResNet mimarilerinden daha başarılı sonuç verdiğini, VGG16 mimarisinin ise daha düşük başarımlarda kaldığını göstermiştir. Başka bir çalışmada (Adak vd., 2020) da Inception'ın Xception'dan el yazısı analizinde daha yüksek başarım gösterdiği görülmektedir. Vision Transformer tabanlı bir başka çevrimdışı imza doğrulama yöntemi (Li vd., 2024) ise raporlanmış en yüksek başarımı göstermektedir. Lodha ve Malani (2022) yaptıkları çalışmada ise imza sahteciliği tespiti için EficientNet ile Xception modellerini de kıyaslamışlar, en düşük başarımı EfficientNet'in sergilediğini ve Xception'ın en yüksek başarımı gösterdiğini belirtilmişlerdir. Literatürdeki sınırlı bilgiler göz önüne alındığında, Inception ve Vision Transformer modellerinin imza sahteciliği tespitinde daha yüksek başarım göstermesi beklenmektedir. Bu uyumsuzluğun nedeni çalışmalar arasında uygulanan eğitim stratejilerinin farklılığı olmalıdır. VGG16 ve EfficientNet mimarilerinin daha düşük, ResNet ve Xception mimarilerinin ise yüksek başarım sergilemeleri literatür ile uyumludur.

Çalışma kapsamında yapılan bir diğer deneye ise veri seti büyüklüğünün model başarımına etkisinin incelenmesidir. %60, %40 ve %20'lik veri setleriyle gerçekleştirilen deneyler veri seti büyüklüğünün azalmasıyla birlikte başarım ölçütlerinde belirgin bir düşüş olduğunu göstermektedir. En büyük veri seti ile eğitilen model, test verisinde en yüksek başarımı elde etmiştir. Küçük veri setleriyle eğitilen modeller, eğitim sürecinde yüksek başarım göstermiş ancak test verisinde genelleme yapmada zorlanmışlardır. Bu durum küçük veri setlerinin aşırı öğrenme riskini artırdığını ve modelin genelleme yeteneğini azalttığını göstermektedir.

Çoklu imza karşılaştırma deneylerinde birden fazla referans imza kullanımının başarımı arttırdığı gözlemlenmiştir. Bu sonuç Diaz vd. (2024) tarafından çalışmayla uyumludur. Yazarlar birden fazla referans imza kullanmanın etkisi incelendiğinde, sistemin daha fazla bilgiye sahip olması durumunda hatanın azalacağını belirtmiştir. Daha fazla referans imza kullanıldıkça, sistemin başarımı artmıştır. Bu deneylerde en iyi sonucu veren birleştirme operatörü OWA (En az biri) olarak tespit edilmiştir. Referans imza sayısı arttıkça başarım artmıştır fakat başarım artışlarına seçilen operatörün etkisi istatistiksel olarak anlamsız çıkmıştır.

Model kararlarının anlaşılabilirliğini artırmak için yapılan son deneyde, model sonuçlarını görselleştirmek için Bütünleşik Gradyanlar yöntemi kullanılmıştır. Modelin karar sürecine en çok etki eden girdileri öne çıkaran önem haritaları oluşturulmuş, bu haritalar ısı haritasına dönüştürülerek imza görsellerine yansıtılmıştır. Bu sayede modelin imzanın hangi bölgelerine dayanarak karar verdiği görselleştirilmiştir. Modelin oluşturduğu görseller gerçek pozitif ve gerçek negatif örnekler için incelendiğinde, ısı haritasının etkin bölgelerinin imzalardaki farklılıkları ya da benzerlikleri denk geldiği görülmektedir. Yanlış pozitif ve yanlış negatif örnekler için ısı haritasında vurgulanan bölgeler ise ilgisizdir. Modelin yanlış yanıt verdiği durumlarda yapılan görselleştirmeler hatalı olmaktadır. Bu nedenle modelin hatasız çalışmaması nedeniyle bu yöntemin uzmanlara bir karar destek sistemi olarak yardımcı olabileceği söylenebilir. Sonuçların görselleştirilmesi deneyinde elde edilen görüntülerin farklı görselleştirme teknikleri kullanan çalışmalar (Diaz vd., 2024; Hamm vd., 2023; Kao ve Wen, 2020; Kao vd., 2020; Solanke, 2022) ile kıyaslandığında ise önerilen yöntemin sonuçlarının dikkat çekici olduğu ortaya çıkmaktadır. Bu sonuçları objektif olarak değerlendirecek bir başarım ölçütü bulunmadığı için elde edilen sonuçlar ile literatürdeki sonuçların karşılaştırılması mümkün olmamıştır. Buradaki sonuçların anlamlılığının adli belge inceleme uzmanları tarafından yorumlanması gerekmektedir.

5. SONUÇ VE ÖNERİLER

Bu çalışmada imza sahteciliği tespiti için derin öğrenme modellerinin dikkat mekanizmaları ile kullanımı incelenmiştir. Çeşitli derin öğrenme modelleri kullanılarak elde edilen sonuçlar, dikkat mekanizmalarının model başarımını ve açıklanabilirliğini artırabileceğini göstermiştir. Özellikle, çok başlıklı öz dikkat mekanizmasının kullanılması, model başarımını artırmış ve sonuçların görselleştirilmesinde daha anlamlı ısı haritaları elde edilmesini sağlamıştır.

Veri seti büyüklüğünün model başarımına önemli bir etkisi vardır. Daha büyük veri setleri ile eğitilen modeller, test verisinde daha yüksek başarım göstermiştir. Bu bulgu, literatürde de desteklenmekte olup, küçük veri setlerinin aşırı öğrenme riskini artırdığı ve genelleme yeteneğini azalttığı bilinmektedir. Bu nedenle, imza sahteciliği tespitinde kullanılan veri setlerinin çeşitlendirilmesi ve zenginleştirilmesi, model başarımını artırmak için önemlidir.

Çoklu imza karşılaştırma deneylerinde, birden fazla referans imza kullanmanın model başarımını artırdığı gözlemlenmiştir. Ancak referans imza sayısının artışının aksine kullanılan birleştirme operatörünün model başarımına etkisi istatistiksel olarak anlamsızdır.

Model sonuçlarının görselleştirilmesi için Bütünleşik Gradyanlar yöntemi kullanılmıştır. Modelin karar sürecine en çok etki eden girdiler öne çıkarılarak, ısı haritasına dönüştürülmüş ve imza görselleri üzerine eklenmiştir. Bu sayede modelin imzanın hangi bölgelerine göre karar verdiği görselleştirilmiştir. Gerçek pozitif ve gerçek negatif örneklerde ısı haritalarının açıklanabilirliğe faydası ortaya çıkarken, yanlış pozitif ve yanlış negatif örneklerde ise oluşturulan ısı haritaları anlamlı değildir. Bu sonuçlar modelin kararlarını daha anlaşılır hale getirmekte ve alan uzmanlarının karar destek sistemi olarak kullanabileceği bir araç sunmaktadır. Ancak bu görsellerin adli belge inceleme uzmanları tarafından değerlendirilerek, daha objektif bir yorum yapılması gerekmektedir.

Vision Transformer ve diğer dönüştürücü tabanlı modellerin, büyük veri setleri ile eğitildiğinde yüksek başarım gösterdiği bilinmektedir. Gelecekteki çalışmalarda, bu modellerin daha büyük ve çeşitli veri setleri ile yeniden eğitilmesi, imza sahteciliği tespitindeki başarımlarını artırabilir.

Bu çalışma yalnızca sınır bir veri seti üzerinde gerçekleştirilmiştir. Veri setlerinin çeşitlendirilmesi, modelin genelleme yeteneğini artırmak için kritiktir. Farklı kaynaklardan ve farklı imza stillerinden oluşan veri setlerinin kullanılması, modelin sahte imzaları daha etkili bir şekilde tespit etmesini sağlayacaktır.

Son olarak, modellerin sahte imzalar üzerinde daha dayanıklı hale getirilmesi için çekişmeli eğitim (İng. adversarial training) yöntemleri kullanılabilir. İlerleyen çalışmalar kapsamında bu yöntem araştırılarak, modellerin sahte imza manipülasyonlarına karşı daha dayanıklı olmasını sağlanabilir, gerçek dünya başarımı artırılabilir.

KAYNAKLAR

Abdulhussien, A. A., Nasrudin, M. F., Darwish, S. M., & Alyasseri, Z. A. A. (2023). A Genetic Algorithm Based One Class Support Vector Machine Model for Arabic Skilled Forgery Signature Verification. *Journal of Imaging*, *9*(4), 79.

Adak, C., Chaudhuri, B. B., Lin, C.-T., & Blumenstein, M. (2020). Intra-variable handwriting inspection reinforced with idiosyncrasy analysis. *IEEE Transactions on Information Forensics and Security*, *15*, 3567-3579.

Alajrami, E., Ashqar, B. A., Abu-Nasser, B. S., Khalil, A. J., Musleh, M. M., Barhoom, A. M., & Abu-Naser, S. S. (2020). Handwritten signature verification using deep learning. *International Journal of Academic Multidisciplinary Research (IJAMR)*, *3*(12), 39-44.

Anagha, R., & Kumar, C. (2023). Signature Recognition and Forgery Detection. *TechRxiv*, *2*.

Arısoy, M. V. (2021). Signature verification using siamese neural network one-shot learning. *International Journal of Engineering and Innovative Research*, *3*(3), 248-260.

Ashish, V. (2017). Attention is all you need. *Advances in neural information processing systems*, *30*, I.

Aydoğdu, E., & Ataç, Y. (2011). İmza sahteciliğinin türleri, tespiti ve önlenmesi. *Polis Bilimleri Dergisi*, *13*(S 2).

Birincioğlu, İ., & Özkara, E. (2010). Adli belge incelemelerinde bilinmeyenler, örneklerle yazı ve imza analizi ile ıslak imza kavramı. *Türkiye Barolar Birliği Dergisi*(87), 403-433.

Bradley, D., & Roth, G. (2007). Adaptive thresholding using the integral image. *Journal of graphics tools*, *12*(2), 13-21.

Brault, J.-J., & Plamondon, R. (1993). A complexity measure of handwritten curves: Modeling of dynamic signature forgery. *IEEE Transactions on systems, Man, and Cybernetics*, *23*(2), 400-413.

Bromley, J., Guyon, I., LeCun, Y., Säckinger, E., & Shah, R. (1993). Signature verification using a" siamese" time delay neural network. *Advances in neural information processing systems*, *6*.

Çalik, N., Kurban, O. C., Yilmaz, A. R., Ata, L. D., & Yildirim, T. (2017). Signature recognition application based on deep learning. 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, Türkiye.

Chattopadhay, A., Sarkar, A., Howlader, P., & Balasubramanian, V. N. (2018). Grad-cam++: Generalized gradient-based visual explanations for deep convolutional networks. 2018 IEEE winter conference on applications of computer vision (WACV), Lake Tahoe, NV, USA.

Chollet, F. (2017). Xception: Deep learning with depthwise separable convolutions. Proceedings of the IEEE conference on computer vision and pattern recognition, Honolulu, HI, USA.

Chopra, S., Hadsell, R., & LeCun, Y. (2005). Learning a similarity metric discriminatively, with application to face verification. 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05), San Diego, CA, USA.

Chu, J., Zhang, W., Zheng, Y., & Ahmad, R. (2023). Signature verification by multi-size assembled-attention with the backbone of swin-transformer.

Deng, P. S., Jaw, L.-J., Wang, J.-H., & Tung, C.-T. (2003). Trace copy forgery detection for handwritten signature verification. IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings., Taipei, Taiwan.

Diaz, M., Ferrer, M. A., & Vessio, G. (2024). Explainable offline automatic signature verifier to support forensic handwriting examiners. *Neural Computing and Applications*, *36*(5), 2411-2427.

Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., & Gelly, S. (2020). An image is worth 16x16 words: Transformers for image recognition at scale. *arXiv preprint arXiv:2010.11929*.

Draelos, R. L., & Carin, L. (2020). Use HiResCAM instead of Grad-CAM for faithful explanations of convolutional neural networks. *arXiv preprint arXiv:2011.08891*.

Ebrahimpour, N. (2023). Handwritten Signatures Forgery Detection Using Pre-Trained Deep Learning Methods. International Congress of New Horizons in Sciences, İstanbul/Türkiye.

Ferrer, M. A., Vargas, J. F., Morales, A., & Ordonez, A. (2012). Robustness of offline signature verification based on gray level features. *IEEE Transactions on Information Forensics and Security*, *7*(3), 966-977.

Ghanim, T. M., & Nabil, A. M. (2018). Offline signature verification and forgery detection approach. 2018 13th international conference on computer engineering and systems (ICCES), Cairo, Egypt.

Gideon, S. J., Kandulna, A., Kujur, A. A., Diana, A., & Raimond, K. (2018). Handwritten signature forgery detection using convolutional neural networks. *Procedia computer science*, *143*, 978-987.

Guo, Z., Li, W., Qian, Y., Arandjelovic, O., & Fang, L. (2024). A White-Box False Positive Adversarial Attack Method on Contrastive Loss Based Offline Handwritten Signature Verification Models. International Conference on Artificial Intelligence and Statistics, Valencia, Spain.

Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Offline handwritten signature verification—literature review. 2017 seventh international conference on image processing theory, tools and applications (IPTA), Montreal, Canada.

Hameed, M. M., Ahmad, R., Kiah, M. L. M., & Murtaza, G. (2021). Machine learning-based offline signature verification systems: A systematic review. *Signal Processing: Image Communication*, *93*, 116139.

Hamm, P., Klesel, M., Coberger, P., & Wittmann, H. F. (2023). Explanation matters: An experimental study on explainable AI. *Electronic Markets*, *33*(1), 17.

Hanmandlu, M., Yusof, M. H. M., & Madasu, V. K. (2005). Off-line signature verification and forgery detection using fuzzy modeling. *Pattern Recognition*, *38*(3), 341-356.

He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. Proceedings of the IEEE conference on computer vision and pattern recognition, Las Vegas, NV, USA.

Herkt, A. (1986). Signature disguise or signature forgery? *Journal of the Forensic Science Society*, *26*(4), 257-266.

Hu, J., Shen, L., & Sun, G. (2018). Squeeze-and-excitation networks. Proceedings of the IEEE conference on computer vision and pattern recognition, Salt Lake City, UT, USA.

Jain, S., Khanna, M., & Singh, A. (2021). Comparison among different cnn architectures for signature forgery detection using siamese neural network. 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Noida, India.

Kao, H.-H., & Wen, C.-Y. (2020). An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. *Applied Sciences*, *10*(11), 3716.

Kao, H.-H., Wen, C.-Y., & Chang, K.-P. (2020). An Improvement of the Interpretability for the Deep Learning Based Signature Examination Assistance Method. *Forensic Science Journal*, *19*(1), 9-21.

Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. IJCAI, Montreal, Canada.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. *Advances in neural information processing systems*, *25*.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *nature*, *521*(7553), 436-444.

Li, H., Wei, P., & Hu, P. (2021). AVN: An adversarial variation network model for handwritten signature verification. *IEEE Transactions on Multimedia*, *24*, 594-608.

Li, H., Wei, P., Ma, Z., Li, C., & Zheng, N. (2024). TransOSV: Offline signature verification with transformers. *Pattern Recognition*, *145*, 109882.

Liu, L., Huang, L., Yin, F., & Chen, Y. (2021). Offline signature verification using a region based deep metric learning network. *Pattern Recognition*, *118*, 108009.

Lodha, S., & Malani, H. (2022). A Unique Approach to Efficient Fraudulent Signature Detection Using Deep Convolutional Neural Network, Xception, and EfficientNet. 2022 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR), Virtual.

Madasu, V. K., & Lovell, B. C. (2008). An automatic off-line signature verification and forgery detection system. In *Pattern Recognition Technologies and Applications: Recent Advances* (pp. 63-89). IGI Global.

Majidpour, J., Ozyurt, F., Abdalla, M. H., Chu, Y. M., & Alotaibi, N. D. (2023). Unreadable offline handwriting signature verification based on generative adversarial network using lightweight deep learning architectures. *Fractals*, *31*(6), 2340101.

Narayana, M., Annapurna, L. B., & Mounika, K. (2017). Offline signature verification. *International Journal of Electronics and Communication Engineering and Technology (IJECET)*, *8*(2), 120-128.

Omeiza, D., Speakman, S., Cintas, C., & Weldermariam, K. (2019). Smooth grad-cam++: An enhanced inference level visualization technique for deep convolutional neural network models. *arXiv preprint arXiv:1908.01224*.

Ooi, S. Y., Teoh, A. B. J., Pang, Y. H., & Hiew, B. Y. (2016). Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network. *Applied Soft Computing*, *40*, 274-282.

Otsu, N. (1975). A threshold selection method from gray-level histograms. *Automatica*, *11*(285-296), 23-27.

Ozkan, Y., & Erdogmus, P. (2024). Evaluation of Classification Performance of New Layered Convolutional Neural Network Architecture on Offline Handwritten Signature Images. *Symmetry*, *16*(6), 649.

Prakash, G. S., & Sharma, S. (2014). Computer vision & fuzzy logic based offline signature verification and forgery detection. 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India.

Ramaswamy, H. G. (2020). Ablation-cam: Visual explanations for deep convolutional network via gradient-free localization. proceedings of the IEEE/CVF winter conference on applications of computer vision, Snowmass Village, CO, USA.

Ren, J.-X., Chen, J., & Xiong, Y.-J. (2022). SET: a squeeze-and-excitation transformer for offline signature verification. 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles, Haikou, China.

Ren, J.-X., Xiong, Y.-J., Zhan, H., & Huang, B. (2023). 2C2S: A two-channel and two-stream transformer based framework for offline signature verification. *Engineering Applications of Artificial Intelligence*, *118*, 105639.

Ribeiro, B., Gonçalves, I., Santos, S., & Kovacec, A. (2011). Deep learning networks for off-line handwritten signature recognition. 16th Iberoamerican Congress on Pattern Recognition (CIARP 2011), Pucón, Chile.

Ruiz, V., Linares, I., Sanchez, A., & Velez, J. F. (2020). Off-line handwritten signature verification using compositional synthetic generation of signatures and Siamese Neural Networks. *Neurocomputing*, *374*, 30-41.

Samek, W., Montavon, G., Vedaldi, A., Hansen, L. K., & Müller, K.-R. (2019). *Explainable AI: interpreting, explaining and visualizing deep learning* (Vol. 11700). Springer Nature.

Sayıcı, B. (2009). *Türkiye'de hukuk ve adli bilimler açısından imza ve karşılaşılan sorunlar* [Yüksek Lisans Tezi, İstanbul Üniversites].

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. Proceedings of the IEEE conference on computer vision and pattern recognition, Boston, MA, USA.

Selvaraju, R. R., Cogswell, M., Das, A., Vedantam, R., Parikh, D., & Batra, D. (2017). Grad-cam: Visual explanations from deep networks via gradient-based localization. Proceedings of the IEEE international conference on computer vision, Venice, Italy.

Shaikh, M. A., Duan, T., Chauhan, M., & Srihari, S. N. (2020). Attention based writer independent verification. 2020 17th International Conference on Frontiers in Handwriting Recognition (ICFHR), Dortmund, Germany.

Shrestha, A., & Mahmood, A. (2019). Review of deep learning algorithms and architectures. *IEEE access*, *7*, 53040-53065.

Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

Singh, A. K., & Koundal, D. (2024). Attention guided spatio-temporal network for 3D signature recognition. *Multimedia Tools and Applications*, *83*(11), 33985-33997.

Solanke, A. A. (2022). Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. *Forensic science international: digital investigation*, *42*, 301403.

Sundararajan, M., Taly, A., & Yan, Q. (2017). Axiomatic attribution for deep networks. International conference on machine learning, Sydney, Australia.

Szegedy, C., Ioffe, S., Vanhoucke, V., & Alemi, A. (2017). Inception-v4, inception-resnet and the impact of residual connections on learning. Proceedings of the AAAI conference on artificial intelligence, San Francisco, CA, USA.

Tan, M., & Le, Q. (2019). Efficientnet: Rethinking model scaling for convolutional neural networks. International conference on machine learning, Long Beach, CA, USA.

Viana, T. B., Souza, V. L., Oliveira, A. L., Cruz, R. M., & Sabourin, R. (2023). A multi-task approach for contrastive learning of handwritten signature feature representations. *Expert Systems with Applications*, *217*, 119589.

Xiong, Y.-J., & Cheng, S.-Y. (2021). Attention based multiple siamese network for offline signature verification. Document Analysis and Recognition–ICDAR 2021: 16th International Conference, Lausanne, Switzerland.

Xiong, Y.-J., Cheng, S.-Y., Ren, J.-X., & Zhang, Y.-J. (2024). Attention-based multiple siamese networks with primary representation guiding for offline signature verification. *International Journal on Document Analysis and Recognition (IJDAR)*, *27*(2), 195-208.

Yager, R. R. (1988). On ordered weighted averaging aggregation operators in multicriteria decisionmaking. *IEEE Transactions on systems, Man, and Cybernetics*, *18*(1), 183-190.

Yager, R. R. (1993). Families of OWA operators. *Fuzzy Sets and Systems*, *59*(2), 125-148.

Yalçın, N., & Gürbüz, F. (2015). *Islak İmza Kavramı, İmza Sahteciliği ve Islak İmza Konusunda Türkiye'de Yapılan Akademik Çalışmalar* Eskişehir, Türkiye.

Yan, K., Zhang, Y., Tang, H., Ren, C., Zhang, J., Wang, G., & Wang, H. (2022). Signature detection, restoration, and verification: A novel chinese document signature forgery detection benchmark. Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, New Orleans, Louisiana.

Yolcu, K., Yılmaz, R., Özdemir, V., Günaydın, U., & Tırtıl, L. (2010). Basit Tersimli 5 İmzanın Adli Belge İncelemesi Açısından Değerlendirilmesi. *Turkiye Klinikleri Journal of Forensic Medicine and Forensic Sciences*, *7*(1), 1-6.

Yusof, M. H. M., & Madasu, V. K. (2003). Signature verification and forgery detection system. Proceedings. Student Conference on Research and Development, 2003. SCORED 2003., Putrajaya, Malaysia.

Zeng, Z. (2022). Multi-scale attention-based individual character network for handwritten signature verification. 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Sanya, China.

Zhang, X., Wu, Z., Xie, L., Li, Y., Li, F., & Zhang, J. (2022). Multi-path siamese convolution network for offline handwritten signature verification. Proceedings of the 2022 8th International Conference on Computing and Data Engineering, Bangkok, Thailand.