
GAZİ ÜNİVERSİTESİ
Gazi
1926

EFFICIENTNET KONVOLÜSYONEL SİNİR AĞI MİMARİSİYLE MALWARE SINIFLANDIRMASI

Ceren Umay ÖZTEN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ARALIK 2024

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ceren Umay ÖZTEN
20/12/2024

EFFICIENTNET KONVOLÜSYONEL SİNİR AĞI MİMARİSİYLE MALWARE SINIFLANDIRMASI

(Yüksek Lisans Tezi)

Ceren Umay ÖZTEN

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Aralık 2024

ÖZET

Malware bilgi sistemlerin tehdit eden ve kullanımını engelleyen kötücül yazılımların bütününe verilen isimdir. Günlük hayatta kullanımı zorunlu hale gelen bilgisayarlar insan hayatını kolaylaştırdığı kadar kötücül yazılımların da sürekli tehdidi altındadır. Dolayısıyla bilgisayar sistemlerini tehdit eden malwarelerin denetlenmesi ve tespit edilmesi önemlidir. Literatürde kötücül yazılımları denetlemek ve tespit etmek için çok fazla çalışma yapılmaya devam etmektedir. Derin öğrenme yöntemlerinin de malware tespitinde son 10 yılda kullanımı giderek artmaktadır. Bu çalışma, malware sınıflandırmasına odaklıdır. Bu çalışmada malware sınıflandırması için EfficientNet mimarisi ve Dynamic Distribution Adaptation Network yaklaşımlı derin öğrenme modeli oluşturulmuştur. Çalışmada malware verilerinin görüntülere dönüşümü ve malware görüntülerinin EfficientNet model tabanında sınıflandırılması tartışılmıştır. Microsoft Malware Classification Challenge ve Dumpware10 bu çalışmanın veri kümeleridir. Deneysel çalışmalarda önerilen derin öğrenme modeli Microsoft Malware Classification Challenge veri kümesinde 97% validasyon doğruluk oranı ile 95% test doğruluk oranı, Dumpware10 veri kümesinde 96% validasyon doğruluk oranı ile 96% test doğruluk oranı elde edilmiştir.

Bilim Kodu	:	92432
Anahtar Kelimeler	:	EfficientNet mimarisi, malware sınıflandırması, veri ön işleme, mimari ölçeklendirme
Sayfa Adedi	:	69
Danışman	:	Doç. Dr. Adem TEKEREK

MALWARE CLASSIFICATION WITH EFFICIENTNET CONVOLUTIONAL NEURAL NETWORK ARCHITECTURE

(M. Sc. Thesis)

Ceren Umay ÖZTEN

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

December 2024

ABSTRACT

Malware is the name given to all malicious software that threatens information systems and prevents their use. Computers, which have become mandatory to use in daily life, are under constant threat from malware as well as facilitating human life. Therefore, it is important to control and detect malware that threatens computer systems. In the literature, a lot of work continues to be done to inspect and detect malware. The use of deep learning methods in malware detection has been increasing in the last 10 years. This study focuses on malware classification. In the study, EfficientNet architecture and Dynamic Distribution Adaptation Network approach based deep learning model is proposed. In the study, conversion of malware into images and classification of the malware images through EfficientNet backbone is discussed. Microsoft Malware Classification Challenge and Dumpware10 are the datasets of this study. In the experimental studies, the proposed deep learning model achieved 97% validation accuracy and 95% test accuracy on the Microsoft Malware Classification Challenge dataset and 96% validation accuracy and 96% test accuracy on Dumpware10 dataset.

Science Code	:	92432
Key Words	:	EfficientNet architecture, malware classification, data preprocessing, compound scaling
Page Number	:	69
Supervisor	:	Assoc. Prof. Dr. Adem TEKEREK

TEŞEKKÜR

Tez çalışmam boyunca değerli yardım ve katkılarıyla beni yönlendiren saygıdeğer hocam Doç. Dr. Adem TEKEREK'e ve yine kıymetli tecrübelerinden faydalandığım bilgisayar Mühendisliği Bölümü'ndeki kıymetli tüm hocalarıma, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli kişilere teşekkürü bir borç bilirim.

Bu çalışmayı hazırlarken geçirdiğim süreçte benden yardımını esirgemeyen ve desteklerini hiçbir zaman eksik etmeyen değerli aile üyelerime teşekkürler ederim.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ ix

ŞEKİLLERİN LİSTESİ xi

SİMGELER VE KISALTMALAR xiv

1. GİRİŞ 1

2. LİTERATÜR ARAŞTIRMASI 3

3. MATERYAL VE METOTLAR 9

3.1. Kullanılan Yöntemler 9

3.1.1. Transfer learning 9

3.1.2. EfficientNet 12

3.1.3. CORAL transfer learning algoritması ve dynamic distribution adaptation network 20

3.2. Kullanılan Veri Kümeleri 23

3.2.1. Dumpware10 23

3.2.2. Microsoft Malware Classification Challenge 24

4. ÖNERİLEN MODEL 25

4.1. Veri Ön İşleme 25

5. DENEYSEL SONUÇLAR 29

5.1. Transfer Learning Deneyleri 29

5.1.1. Maxpooling deneyi 48

Sayfa

5.1.2. CORAL kayıplı dynamic distribution adaptation network deneyi 52

6. SONUÇLAR VE ÖNERİLER 65

KAYNAKLAR 67

ÖZGEÇMİŞ 69

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 5.1. EfficientNet-b3 ve EfficientNet-b4 modellerinin Microsoft Malware Classification Challenge değerlendirme (validasyon) doğruluk oranları 30

Çizelge 5.2. Microsoft Malware Classification Challenge EfficientNet-b3 ve EfficientNet-b4 test doğruluk oranları 31

Çizelge 5.3. Microsoft Malware Classification Challenge (Gri tonlamalı) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları 33

Çizelge 5.4. Microsoft Malware Classification Challenge (Gri tonlamalı) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin test doğruluk oranı, F1-score, recall, precision sonuçları 34

Çizelge 5.5. Microsoft Malware Classification Challenge (RGB) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları 35

Çizelge 5.6. Microsoft Malware Classification Challenge (RGB) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin test doğruluk oranı, F1-score, recall, precision sonuçları 36

Çizelge 5.7. EfficientNet-b7 mimarisinde gri tonlamalı iki kanallı malware görüntülerin değerlendirme (validasyon) doğruluk oranı 37

Çizelge 5.8. EfficientNet-b5 mimarisinde üç kanallı (RGB) malware görüntülerin değerlendirme (validasyon) doğruluk oranı 37

Çizelge 5.9. Dumpware10 için EfficientNet-b0 - EffcientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları 38

Çizelge 5.10. EfficientNet-b6 mimarisinde Dumpware10 üç kanallı (RGB) malware görüntülerin değerlendirme (validasyon) doğruluk oranı 38

Çizelge 5.11. Microsoft Malware Classification Challenge ile Dumpware10 test doğruluk, F1-score, recall ve precision sonuçları 39

Çizelge 5.12. MaxPooling EfficientNet model eğitimlerine ait değerlendirme (validasyon) doğruluk oranları 49

Çizelge **Sayfa**

Çizelge 5.13. MaxPooling EfficientNet model test doğruluk, F1-score, recall ve precision sonuçları 50

Çizelge 5.14. CORAL kayıplı Dynamic Distribution Adaptation Network değerlendirme (validasyon) doğruluk oranları..... 53

Çizelge 5.15. CORAL kayıplı Dynamic Distribution Adaptation Network test sonuçları 53

Çizelge 5.16. Transfer learning, MaxPooling ve DDAN deneylerinin en başarılı sonuçları 63

Çizelge 5.17. DDAN deney sonuçlarıyla akademik sonuçların karşılaştırılması 64

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 3.1. Deep transfer learning model-tabanlı metotlar 12

Şekil 3.2. MBConv bloğu 14

Şekil 3.3. Linear Bottleneck bloğu 16

Şekil 3.4. Inverted residual bloğu 17

Şekil 3.5. Compound scaling gösterimi 20

Şekil 4.1. İki kanallı gri tonlamalı malware görüntü dönüşümü..... 25

Şekil 4.2. Üç kanallı RGB malware görüntü dönüşümü..... 26

Şekil 4.3. EfficientNet sinir ağı modeli 27

Şekil 5.1. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 eğitim kayıp oranı 40

Şekil 5.2. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 eğitim doğruluk oranı..... 40

Şekil 5.3. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme (validasyon) doğruluk oranı..... 41

Şekil 5.4. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme (validasyon) kayıp oranı 41

Şekil 5.5. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 konfüzyon matrisi 42

Şekil 5.6. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim kayıp oranı 43

Şekil 5.7. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim doğruluk oranı..... 43

Şekil 5.8. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme (validasyon) kayıp oranı 44

Şekil 5.9. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme (validasyon) doğruluk oranı..... 44

Şekil **Sayfa**

Şekil 5.10. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisi 45

Şekil 5.11. Dumpware10 EfficientNet-b6 değerlendirme kayıp oranı 46

Şekil 5.12. Dumpware10 EfficientNet-b6 değerlendirme doğruluk oranı..... 46

Şekil 5.13. Dumpware10 EfficientNet-b6 eğitim kayıp oranı 47

Şekil 5.14. Dumpware10 EfficientNet-b6 eğitim doğruluk oranı..... 47

Şekil 5.15. Dumpware10 EfficientNet-b6 konfüzyon matrisi 48

Şekil 5.16. MaxPooling EfficientNet-b5 Microsoft Malware Classification Challenge (RGB) konfüzyon matrisi 50

Şekil 5.17. MaxPooling EfficientNet-b7 Microsoft Malware Classification Challenge (Gri tonlamalı) konfüzyon matrisi 51

Şekil 5.18. MaxPooling EfficientNet-b6 Dumpware10 konfüsyon matrisi..... 51

Şekil 5.19. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 validasyon doğruluk oranı 54

Şekil 5.20. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 classification kayıp oranı 55

Şekil 5.21. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 transfer kayıp oranı 55

Şekil 5.22. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 total kayıp oranı 56

Şekil 5.23. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 validasyon doğruluk oranı 57

Şekil 5.24. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 classification kayıp oranı 57

Şekil 5.25. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 transfer kayıp oranı 58

Şekil 5.26. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 total kayıp oranı 58

Şekil 5.27. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 validasyon doğruluk oranı..... 59

Şekil **Sayfa**

Şekil 5.28. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 classification kayıp oranı 59

Şekil 5.29. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 transfer kayıp oranı 60

Şekil 5.30. CORAL kayıplı DDAN Dumpware10 EfficientNe-b6 total kayıp oranı 60

Şekil 5.31. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 konfüzyon matrisi 61

Şekil 5.32. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisi 61

Şekil 5.33. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 konfüzyon matrisi 62

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AE	AutoEncoder
API	Application Programming Interface
APK	Android Package Kit
ARPANET	Advanced Research Project Agency Network
AUC	Area Under Curve
B2IMG	Binary to Img
BIG	Behavioral Information Graphs
Bi-LSTM	Bi-directional Long Short - Term Memory
CNN	Convolutional Neural Network
ConvNet	Convolutional Network
CORAL	CORrelation ALignment
DAE	Domain Adaptive Ensemble
DAN	Deep Adaptation Network
DANN	Domain Adversarial Neural Network
DDA	Dynamic Distribution Adaptation
DDC	Deep Domain Confusion
DDoS	Distributed Denial of Service
DDP	Distributed Data Processing
DEC	Domain Transfer Support
DTS	Digital Equipment Corporation
GBM	Gradient Boosting Machine
GIST	Global Image Structure Tensor
HOG	Histogram of Gradients
IBM	International Business Machine
JPG	Joint Photographic experts Group
KNN	K-Nearest Neighbors

Kısaltmalar	Açıklamalar
MBConv	Mobile Bottleneck Convolution
MLP	Multi - Layer Perceptron
MMD	Maximum Mean Discrepancy
MMCC	Microsoft Malware Classification Challenge
MMDA	Multi Metric Domain Adaptation
MrMR	Maximum Redundancy Maximum Relevance
MS	MicroSoft veri kümesi
PCA	Principal Component Analysis
PDP	Programmed Data Processor
PE	Portable Executable
PNG	Portable Network Graphics
ReLU	Rectified Linear Unit
RGB	Red Green Blue
RMSProp	Root Mean Square Propagation
SCADA	Supervisory Control and Data Acquisition
SDA	Software Defined Architecture
SDIF	Stacking Deep Image Features
SGD	Stochastic Gradient Descent
SVM	Support Vector Machine
TIT	Teacher-student Incremental Training
TL	Transfer Learning
TrAda	Transfer AdaBoost
UCLA	University of California
UMAP	Uniform Manifold Approximation and Project
VBA	Visual Basic for Applications
VGG	Visual Geometry Group

1. GİRİŞ

UCLA araştırma laboratuvarı (Honeywell DDP 516 bilgisayarı), Stanford araştırma enstitüsü (SDS-940 bilgisayarı), Kaliforniya Üniversitesi, Santa Barbara Üniversitesi (IBM 360/75) ve Utah Üniversitesi (DEC PDP-10) sayılı kuruluşlarının desteğiyle askeri departmanda birleşen ARPANet ilk tarihsel internet noktasından günümüzün milyarlarca sunuculu network yumağına dönüşümüne kadar siber tehditler katlanarak artmaktadır. İlk bilgisayar zararlısı "böcek" (bug) kavramından spesifik saldırı yazılımlarına evirilmiştir ve saldırı yazılımları malware altında değişken ailelere ayrılarak yaygınlaşmıştır. Malware yapısı, bilgi sistemlerine, mobil cihazlara, devlet veri tabanlarına, dijital blok zincir otomasyonlarına ve kritik dijital aplikasyonlara sızabilmektedir. Bu durum saptanan malware sızıntısının doğru siber güvenlik analizinden geçirilmesini gerektirmektedir ve potansiyel malware girişlerine karşı bağlantılı malware ailesinin belirlenmesiyle yabancı yazılımlara ait malware ya da iyi huylu dosya ayrımının anlaşılması önem kazanmaktadır. Bu bağlamda hatalı ayrıştırılan malware örneği, tüm veri altyapısını parçalayabilmektedir, işlevsizleştirebilmektedir. Tez çalışmasının amacı, malware dosyalarının veri ön işlemesi ve derin öğrenme mimarisiyle malware aile karşılıklarına atanmasını gerçekleştirmektedir. Ve EfficientNet konvolüsyonel derin sinir ağı mimarisinden yararlanarak malware görüntü dönüşümlerini malware sınıflarına dağıtmaktadır. Bu kapsamda EfficientNet Inverted Residual (MBConv) katman blokları, Transfer Learning, MaxPooling ve Dynamic Distribution Adaptation Network deneylerine tanımlanmaktadır. Malware veri kümesinin toplanması, malware veri ön işlemesi, EfficientNet model geliştirmesi ve deneysel sonuç incelenmesi araştırmanın yöntem modellemesinde mevcuttur. Yöntem modellemesinde malware veri kümeleri toplanmaktadır, malware kümelerine ait malware örnekleri, veri ön işleminde tensor bloklarına parçalanmaktadır ve tensor blokları üç kanallı RGB ve iki kanallı gri tonlamalı malware görüntülerine dönüştürülmektedir. Ardından malware görüntüleri EfficientNet mimarisinde eğitilmektedir. Transfer Learning ve MaxPooling deneylerinde katman derinliği, girdi çözünürlüğü ve katman genişliği ayarlarına çalışılmıştır ve MaxPooling son katman değişimi denenmiştir. Dynamic Distribution Adaptation Network deneyinde malware görüntüleri source domain ve target domain alanlarına rastgele taşınmaktadır ve transfer learning algoritmasının CORAL loss kaybı source domain ve target domain eğitim döngüsüne katılarak derin öğrenme mimarisini malware öznitelik karakteristiğine yaklaştırmaktadır.

2. LİTERATÜR ARAŞTIRMASI

Literatür çalışmalarında malware veri ön işlemesi, konvolüsyonel katman dizilimlerinin gerçekleştirmesi, konvolüsyon CNN - BiLSTM iki kademeli sistematiğin kurulumu, Dense konvolüsyon katmanı ile LSTM katmanının bileşimi, Autoencoder sinir ağının gri tonlamalı malware görüntülerine uyarlaması ile malware veri setlerinin rastgele parçalanması ve SDA-tabanlı SCADA sistemlerinde DDoS tespiti için Ensemble araştırılmaktadır.

Huaxin Deng ve ekibi, Markov transfer matrislerini esas alan yeni malware görselleştirme metodunu konvolüsyonel derin öğrenmeye uyarlamıştır. Markov veri ön işlemesinde opcode ile operand bilgileri malware dokusundan çıkarılarak üç kanallı malware görüntüleri elde edilmiştir ve 4 konvolüsyon katmanı, 4 pooling filtreleme katmanı ile 1 fully-connected yoğun katmanlı mimariye girilmiştir. Markov transfer matrisleri, makine kodlarının her iki ardışık harf ya da sayı, opcode parçasının ilk harfleri ve son iki harfine ait kombinasyon geçiş olasılıklarının üç matris görüntü kanalına atanmasıdır. Markov metodu, Microsoft Malware Challenge veri kümesinde 99,4% doğruluk oranına erişmektedir [1].

Mumtaz Ahmed ve ekibi, malware verisini iki kanallı görüntüye çevirmiştir, veri ön işlemini malware bayt dosyalarından onaltılık sayılara dönüşümü, ikili onaltılık sayıların piksellere aktarımı ve total piksel görüntüde min-max normalizasyonu üzerinden gerçekleştirmiştir. Bağlantılı piksel görüntüleri, InceptionV3 modelinin gizli katmanları dondurularak softmax katmanının Microsoft Malware Classification Challenge veri kümesinin 9 malware sınıfına uyarlanmıştır. InceptionV3 modeli, Microsoft Challenge BIG15 test setinde 98,76% doğruluk oranına ulaşmıştır [2].

Sanjeev Kumar ve Kajal Panda, SDIF-CNN metodunda VGG16, VGG19, ResNet50 ile InceptionV3 modellerine ait öznitelik çıktıları, yatay uzayda birleştirilerek tek öznitelik çıktısına tamamlanmıştır ve filtrelenen öznitelik çıktısından fazlalık veriler filtrelenmiştir. Filtrelenen öznitelik çıktısı, KNN, SVM, Random Forest, Multi-layer Perceptron (MLP), Extra Tree ile Gauss Naive Bayes sınıflandırıcılarına iletilmiştir. Multi-layer Perceptron modeli, MalImg veri kümesinde 98,55% doğruluk oranı, 99% precision oranı, 99% recall oranı ve 99% f1-score oranını kaydetmiştir [3].

Seok-Jun Bu ve Sung-Bae Cho, evrimsel üçlü networkte malware yapısını sınıflandırma için çözmüştür ve karışık malware varyasyonunu genetik algoritma yardımıyla temsiller arası uzaklık gruplarına optimize etmiştir. Algoritma bağlamında bayt malware görüntüsü, evrimsel üçlü networke girilerek ağırlık değişimleri uzanımında yeni ağırlık paylaşımlı konvolüsyonel networkler üretilmiştir. Genetik algoritmaya bağlı üçlü kayıp, benzer malware örnekleri birbirine yaklaştırırken farklı malware örneklerini uzaklaştırmıştır [4].

Multi-view çok boyutlu öznitelik füzyonu anlayışında Rajasekhar Chaganti ve ekibi, malware verisine ait statik, dinamik ile görüntü öznitelik setlerini birleştirmiştir. Modellerin çok boyutlu öznitelik füzyon öğreniminde her öznitelik seti, malware verisinin ayrıştırıcı semantik karakteristiklerini sunmuştur. Ekibin çalışmasında PE Section ile PE Import, dinamik PE API ile PE Image malware öznitelik dosyaları birleştirilerek konvolüsyonel sinir ağına aktarılmıştır. Bağlantılı konvolüsyonel sinir ağı, convolution1D-Maxpooling-Dense katman diziliminden türetilmiştir. PE API tabanlı öznitelik seti 99% doğruluk değerini görmüştür [5].

İki aşamalı hibrid yaklaşımında Seungyeon Baek ve ekibi, statik aşamada opcode sekanslarını vektörleştirerek Bi-LSTM model geçişi sırasında iyi huylu dosya özniteliklerine ayrıştırmıştır. Dinamik aşamada ise ayrıştırılan iyi huylu dosya özniteliklerini sanal Cuckoo Sandbox ortamında çalıştırarak process memory ile API calls özniteliklerine çıkarmıştır ve ardından bağlantılı özniteliklerini, process memory, category ile API calls uzantılarında üç boyutlu tensör yapısına dönüştürmüştür. Sonunda üç boyutlu tensor yapısı, EfficientNet-b3 modelinde sınıflandırılmıştır. Bağlantılı EfficientNet-b3 modeli, 94,98% doğruluk oranına varmıştır [6].

Manish Kumar, konvolüsyonel sinir ağı CNN ile Bi-LSTM ağını, malware tespiti için birleştirmiştir. Dinamik malware API calls ile process execution sinyalleri, process tree ağacı ağacında vektöre dönüştürülmüştür. Bağlantılı yüksek seviye vektör çıktısı, embedded katmanında parçalanmıştır ve düşük seviyeli vektör parçaları, CNN1-BiLSTM1-CNN2-BiLSTM2-Dense-Softmax zincirleme katman örüntüsünden geçirilmiştir. Katman bağlamında konvolüsyon katmanları öznitelik verilerini LSTM katmanları için filtrelemiştir, farklı sinir ağı katman yapılandırmalarından ikili CNN modellemesi ile ikili BiLSTM katmanları en başarılı performansı göstermiştir. İkili CNN-BiLSTM katmanlı mimari yapı, 0,99 doğruluk oranı kaydetmiştir [7].

Autoencoder, gri tonlama yaklaşımında Xiaofei Xing ve ekibi, malware ile iyi huylu dosyaya ait APK kodu ondalık bayt verisine kodlayarak gri tonlamalı iki boyutlu matrise sabitlemiştir, bağlantılı gri tonlamalı malware görüntü verilerini AE-1 ile AE-2 autoencoder yapılarından geçirmiştir. AE-1 autoencoder, gri tonlamalı görüntünün öznitelik çıkarımını, asıl malware sınıflandırmasına yapılandırmıştır. AE-2 autoencoder ise AE-2 autoencoder ise önceden sınıflandırılan iyi huylu dosyaya ait malware ayrışımını üstlenmiştir. AE-1 autoencoder mimarisi, konvolüsyon, filtreleme ile upsampling katmanlarına sahiptir. AE-2 autoencoder mimarisi ise AE-1 mimari katmanlarına ek olarak multi-layer perceptron ağına sahiptir. Multi-layer perceptron modellemesi yoluyla 96% doğruluk oranı yakalanmıştır [8].

LSTM-Dense metodunda Esraa Saleh Alomari ve ekibi, derin öğrenme ile öznitelik seçimine dayanan malware tespitini sunmuştur ve veri setlerini işleyerek korelasyon matrisinde öznitelik seçimine uğratmıştır. Dense yoğun katman ile LSTM model uzanımında değişken öznitelik seçimlerine ait veri setleri eğitilmiştir. Eğitimde Dense yoğun katman modeli, 5 gizli katmanı ReLU aktivasyonuna girdi ile çıktı katmanları arasında tanımlanmıştır, LSTM modeli ise Dense yoğun katman modeline ait ilk Dense katmanın ReLU aktivasyonlu LSTM katmanla değiştirimini içermiştir. Öznitelik seçimi ile veri setlerinin daraltılması, neredeyse tüm veri kümesinin performansını karşılamıştır [9].

Vinayakumar ve ekibi, bias-derin öğrenme çizgisinde veri setlerini farklı ayrımlar uygulayarak bias durumunu kaldırmıştır. Ki veri setlerinden bağlantılı bias kaldırımı malware tespit model eğitimini bağımsızlaştırmıştır. Ember veri setinde Light GBM 100 ağaçlık modelleme, konvolüsyonel 1D katmanları ile LSTM hibrit MalConv varyantları irdelenmiştir. Esnek ve gerçek zamanlı hibrit derin öğrenme modelleri, malware veri ön işlemesi ile sınıflandırmasında yararlanılmıştır. Ember veri seti 60% eğitim ile 40% test setlerine rastgele parçalamalarla ayrıştırılarak modellere tanıtılmıştır [10].

Handhika Yanuar Pratama ve Jeckson Sidabutar, derin öğrenmeli malware sınıflandırmasında EfficientNet modelleri, -EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6 ve EfficientNet-b7-Malware Classification Challenge (BIG 2015) veri kümesinin gri tonlamalı iki kanallı ve üç kanallı RGB malware görüntülerine uygulanmaktadır. Çalışmada EfficientNet modelleri, etkin derin öğrenme transfer learning modellerindendir ve ImageNet veri kümesinde son teknoloji derin öğrenme sınıflandırması gerçekleştirebilmektedir. Ki çalışma deneylerinde

üç kanallı RGB malware görüntülerine uygulanan EfficientNet-b7 mimarisi, 99,63% doğruluk oranı, 98,36% precision oranı, 98,35% recall oranı, 98,34% F1-score oranı ve 98,30% AUC oranına erişmektedir [11].

SDN-tabanlı SCADA sistemlerinde DDoS saldırılarına karşı korunmak için siber ihlal tespit sistemleri geliştirilmektedir. Oyucu ve ekibi, SDN-tabanlı SCADA sistemlerde normal veri akışı ve DDoS saldırısını ayrıştırarak DDoS saldırılarını saptayan Decision Tree-based Ensemble Learning tekniğini önermiştir. Makine öğrenmesinin sınıflandırma metotlarını kullanan hibrid model önerisi, veri kümesi yaratılması, öznitelik düzeltimi, normalizasyon ve sınıflandırma aşamalarına sahiptir. Ensemble learning modellerinin eğitimi ve testi için normal trafik ve DDoS saldırısı veri akış trafiği, spesifik deneysel network topoloji simülasyonundan elde edilmiştir. Veri kümesindeki öznitelik dengesi için Minimum Redundancy Maximum Relevance (MrMR) yöntemi edinilmiştir. Öznitelik seçimi ve hiperparametre ayarlaması decision tree ensemble modellerinin optimizasyonunda yararlanılmıştır. Deneyler öznitelik seçimi, farklı decision tree ensemble model kombinasyonları ve hiperparametre ayarlamasının DDoS saldırılarına karşı daha başarılı tespit performansını yansıtmaktadır. Ekibin Ensemble Boosted Trees metodu en yüksek 92,9% doğruluk performansını göstermiştir [12].

Polat ve ekibi SDA-tabanlı SCADA sistemlerinde DDoS saldırılarının tespiti için 1-dimensional convolutional neural network (1D-CNN) ve karar ağacı tabanlı sınıflandırma birleştirilerek çok-aşamalı öğrenme modeli önermiştir. Önerilen modelde 1D-CNN konvolüsyonel sinir ağı modelinden çıkarılan öznitelik verileri, decision tree modeline girilmiştir. 1D-CNN network modeli, daha derin ve karmaşık öznitelik çıkarımını gerçekleştirirken karar ağacı modeli öznitelikleri karar yapısına tanımlamaktadır. Modelin eğitim ve testinde varyasyonlu saldırı senaryolarına dayanan spesifik deneysel network topolojisinin yeni veri kümesi kullanılmıştır. Önerilen model DDoS saldırı tespitinde 97,8 doğruluk oranı yakalamıştır [13].

Bu tez çalışması EfficientNet mimarisinin tam konvolüsyon donanımına yakınlaşırken gradyan hesabını düşüren katman yapılandırmasını malware görüntü veri kümelerine etkin bir şekilde uygulamaktadır. Backbone EfficientNet mimarisinin Dynamic Distribution Adaptation Network eğitim döngüsünde CORAL kaybıyla transfer learning algoritmasını gerçekleştirmektedir. Oldukça yaygın benchmark Microsoft Malware Classification

Challenge (BIG 2015) veri kümesi ve özel Dumpware10 veri kümesinin birlikte kullanılması, çalışma modelinin deneysel testlerinde farklı bakış açıları sunmaktadır. Microsoft Malware Classification Challenge (BIG 2015) veri kümesi genel benchmark görevi görürken Dumpware10 veri kümesi çalışma modelinin daha farklı bir benchmark açısından değerlendirilmesini sağlamıştır.

3. MATERYAL VE METOTLAR

3.1. Kullanılan Yöntemler

Malware sınıflandırması için konvolüsyonel EfficientNet sinir ağı mimarisine ait inverse residual block uzamındaki konvolüsyonel bottleneck ve depthwise separable convolution kullanılarak transfer learning modeli uygulanmıştır. Transfer learning model genellemesinin iyileştirilmesi için transfer learning algoritması CORAL kaybına sahip Dynamic Distribution Adaptation Network EfficientNet backbone yapısında eğitilmiştir.

3.1.1. Transfer learning

Transfer learning önceden eğitim döngüsüne tabi tutulan derin sinir ağı mimarisine ait aktivasyon donanımının farklı görev uzanımlarına kazandırılmasıdır. Bağlantılı derin sinir ağı mimarisinin son yoğun Dense nöron katmanı, görev uzanımının sınıflandırma dağılımına göre değiştirilmektedir. Derin sinir ağına ait katman mimarisi, ImageNet benzeri büyük çaplı benchmark veri kümesinde önceden eğitilerek görüntü verilerinin işlendiği optimizasyon öğrenimini gerçekleştirmektedir, derin sinir ağı katmanları ImageNet benzeri state-of-the-art benchmark veri kümesinde deneyimlediği optimizasyon öğrenimini, farklı veri kümelerine ait farklı sınıflandırma görevlerine aktarabilmektedir. Örneğin ImageNet veri kümesinin görüntü verileriyle önceden eğitilmiş ağırlıklı DenseNet121 sinir ağı mimarisi, insan yüz ifade görüntülerini içeren ve insan duygularını -mutluluk, öfke, üzüntü, nötr, sürpriz, korku, tiksinti- sınıflandırmayı amaçlayan bir veri kümesine uyarlanabilmektedir, DenseNet121 sinir ağı mimarisi, ImageNet veri kümesine ait görüntü verilerinden öğrendiği kenar, şekil, renk ve ilişkili doku piksel öznitelik bilgisini yüz ifade görüntülerinin insan duygu sınıflandırmasına uygulamaktadır. DenseNet121 sinir ağı mimarisinin son yoğun Dense katmanı değiştirilerek insan duygu sınıflandırmasının 7 ayrı duygusal sınıf ayrımıyla uyumlu softmax fonksiyonu tanımlanmaktadır. Daha ileri aşamada DenseNet121 mimarisinin düşük seviyeli piksel öznitelik bilgilerini taşıyan katman blokları eğitim sırasında gradyan genellemesine katılmazken yüksek seviyeli piksel öznitelik bilgilerini taşıyan son yoğun Dense katman grupları gradyan genellemesine katılmaktadır. Son yoğun Dense katmanına ait başarılı softmax sınıflandırması için gradyan genellemesini iyileştiren hiperparametre yapılandırmaları -aktivasyon fonksiyonu, optimizasyon fonksiyonu, öğrenme oranı, momentum, epoch döngü sayısı, weight decay fonksiyonu- eklenmektedir.

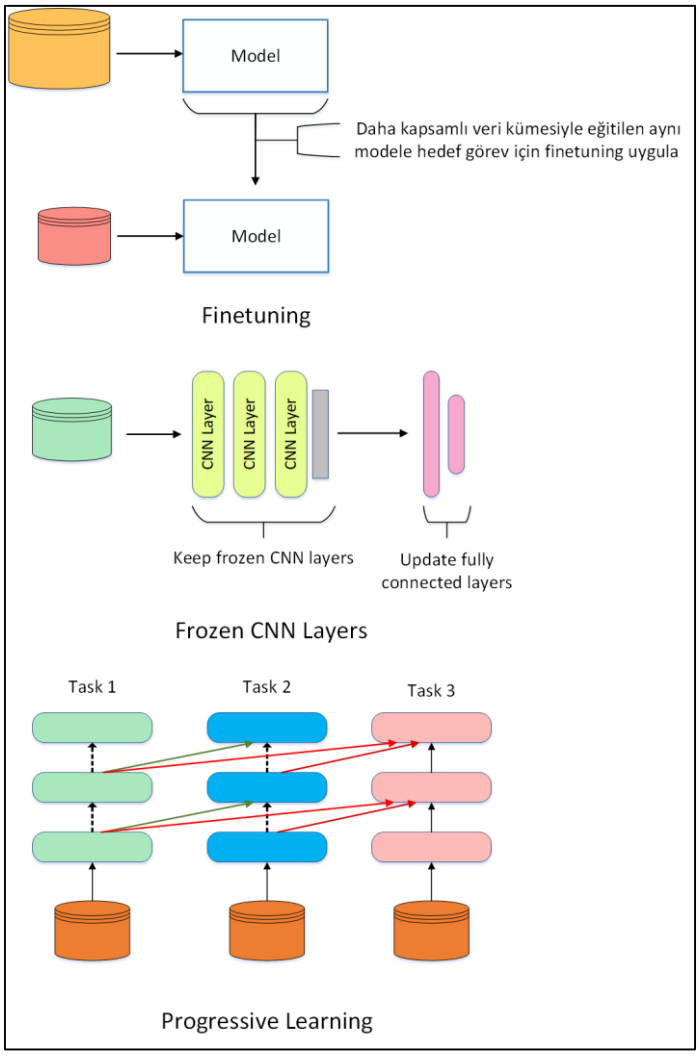
Bu durum ImageNet veri kümesine ait görüntü verileriyle önceden eğitilmiş DenseNet121 sinir ağı mimarisinin ağırlıkları, transfer learning uzanımında hiperparametre ile yoğun Dense katman bileşimleriyle görev alanının veri kümesine özgünleşmektedir. Hiperparametre yapılandırması, derin sinir ağı eğitim döngüsünün gradyan genellemesini yönlendirmektedir, özellikle Adam, SGD, Adagrad, RMSProp benzeri optimizasyon fonksiyonları sinir ağı mimari katmanlarının aktivasyon akışlarını düzenlemektedir ve sinir ağı mimarisinin eğitim döngüsünü daha başarılı gradyan genellemesine zorlayabilmektedir. Öğrenme oranı, momentum, weight decay fonksiyonu ve eğitim epoch döngü sayısının ayarlanması, bağlantılı optimizasyon fonksiyonlarının eğitim döngüsünde etkinliğini şekillendirmektedir. Transfer learning bağlamında sinir ağı mimarisinin yoğun Dense katman değişimi, sinir ağı mimarisine ait düşük seviyeli piksel öznitelik bilgilerini işleyen katman blokları ile yüksek seviyeli piksel öznitelik bilgilerini işleyen yoğun Dense katman blokları ve hiperparametre yapılandırması öne çıkmaktadır. Sınıflandırma alanında yüksek performanslı DenseNet121, ResNet50, InceptionV3, Xception, AlexNet, EfficientNet-b0-b7 benzeri kalıp sinir ağı mimarileri, yoğun Dense katman değişimi ve hiperparametre yapılandırmalarını transfer learning uzanımında dönüştürmektedir, veri kümelerine göre farklı eğitim döngüleri gerçekleştirmektedir. Bu kapsamda transfer learning metodu, kalıp sinir ağı mimarilerinin nöron aktivasyonlarını eğitim döngüsünde veri kümesinin gradyan genellemesine yakınlaştırmaktadır ve veri sınıflandırma görevlerinde başarılı sonuçlar göstermektedir. Transfer learning metodunda sinir ağı katmanları, yoğun Dense katmanına kadar gradyan hesaplamasını sabitleme ya da yalnızca düşük seviyeli piksel öznitelik bilgilerini işleyen katman bloklarının gradyan hesaplamasını sabitleme -yüksek seviyeli piksel öznitelik bilgilerini işleyen katman bloklarını gradyan hesaplamasına açık tutarak- seçeneklerine sahiptir.

Transfer learning, bahsi geçen derin sinir ağlarına ait derin öğrenme yönteminin etkisiyle derin transfer learning uzanımına evirilmektedir. Derin transfer learning uzanımında daha genel kapsamlı veri kümesine ait görev alanının bilgi tabanını, daha dar kapsamlı veri kümesine ait görev alanının bilgi tabanına aktarmaktadır. Örneğin bir araştırmacı var olan biyolojik proteinlerin yapısal bilgisini yapay zekâ yoluyla yeni protein yapılarının ortaya çıkarılmasında kullanabilmektedir. Genel metodolojide derin transfer learning uzanımına ait model tabanlı metotlar, önceden eğitilmiş sinir ağı modelini veri kümesine uyarlama (finetuning), düşük seviyeli CNN katmanlarını dondurma -yalnızca düşük seviyeli CNN sinir ağı katmanları dondurularak yan yoğun fully-connected katmanlar veri kümesinin

gradyan hesaplamasına dahil edilmektedir- ve progressive learning -önceden eğitilmiş sinir ağı modeline ait birtakım ya da tüm katmanlar seçilerek gradyan hesabına katılmadan (donmuş konvolüsyon katmanı) kullanılmaktadır ve sinir ağı modeline eklenen yeni katman yapılandırmaları hedef verilerde eğitilmektedir- yaklaşımlarına ayrılmaktadır.

Finetuning yaklaşımı, hedef görevin genel kapsamına yakın veri örnekleriyle önceden eğitilmiş sinir ağı modelini kullanarak hedef göreve ait veri kümesine genellemektedir. Bu yönüyle finetuning en yaygın deep transfer learning yaklaşımıdır. Finetuning yaklaşımı, veri kümesine ait eğitim döngüsünün hesaplama maliyetini azaltabilmektedir ve hedef görevin büyük çaplı veri kümesi ihtiyacını gidermektedir. Yalnız finetuning, eğitim döngüsü boyunca gradyan kaybolması problemiyle karşılaşmaktadır. Düşük seviyeli CNN katmanlarını dondurma yaklaşımı ise sinir ağı modeline ait düşük seviyeli konvolüsyon katmanlarını dondurarak eğitim döngüsünün gradyan hesabına girmemektedir ve yalnızca yan yoğun fully-connected katmanları hedef veri kümesinin eğitim döngüsündeki gradyan genellemesine katılmaktadır. Bağlantılı düşük seviyeli CNN katmanları, veri kümesinin öznitelik çıkarımını üstlenirken yan yoğun fully-connected katmanları, öznitelik çıkarımlarının sınıflandırmasını üstlenmektedir. Sonuçta düşük seviyeli CNN katmanlarını dondurma yaklaşımı, hedef veri kümesi için yeni göreve uyuşmayı sağlamaktadır. Progressive learning metodu, önceden eğitilmiş sinir ağı modeline ait birtakım ya da tüm katmanlar belirlenerek eğitim döngüsünün gradyan genellemesine girilmeden kullanılmaktadır ve sinir ağı modeline eklenen yeni katman yapılandırmaları hedef veri kümesinde eğitilmektedir. Üçlü katman bloklu autoencoder yapılandırması, eğitim ve hedef verisinin özniteliklerine maksimum uyuşmazlık terimi uygulayarak eğitim ve test öznitelik verileri arasındaki uyuşmazlık ceza terimini minimuma indirmektedir [14].

Şekil 3.1’de finetuning, düşük seviyeli CNN katmanlarını dondurma ve progressive learning derin transfer metotları gösterilmiştir.



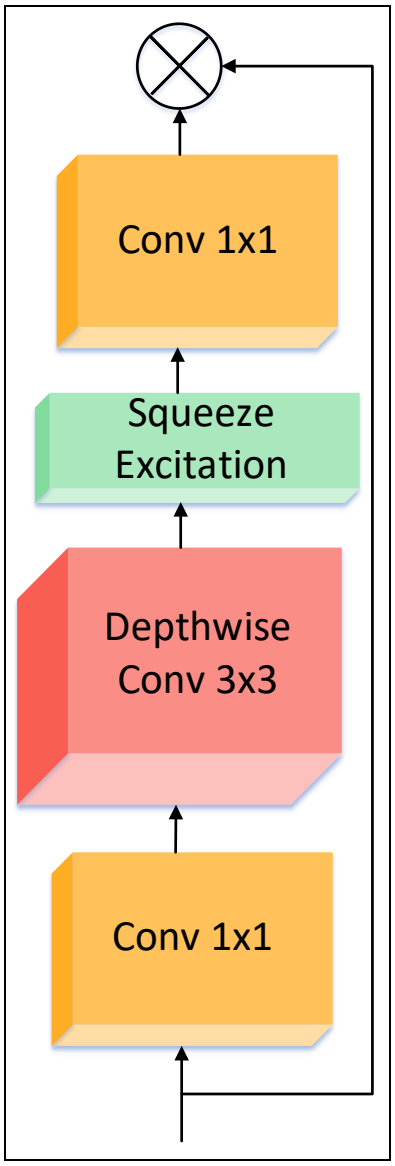
Şekil 3.1. Deep transfer learning model-tabanlı metotlar

3.1.2. EfficientNet

EfficientNet mimarisi, çözünürlük, katman genişliği ve katman derinlik bakımından MBConv yapılarının "compound scaling" modellemesinden oluşmaktadır. EfficientNet mimarisi, compound scaling ile MBConv yapılarının bütünleşmesiyle çok boyutlu genişleme esnekliğini mimarisine katmaktadır. MBConv yapısı, (inverted residual bloğu), ilk başta daralan ortada genişleyen ve en sonunda tekrar daralan konvolüsyonel katman yolunu takip etmektedir. İlk başta (1x1) konvolüsyon filtrelemesi, ardından (3x3) depthwise convolution blok filtrelemesini izleyen (1x1) konvolüsyon filtrelemesi orta katman uzanımında artan kanal parametre sayısını azaltmaktadır. MBConv bloğu, performans etkisi sebebiyle tersine katman dönüşümü içeren inverted residual bloğunun modellemesindedir.

MBConv bloğu

Şekil 3.2. gösteriminde MBConv blok yapısı ve bağlantılarını irdelemiştir. MBConv konvolüsyonel blok mimarisindedir. MBConv blok mimari yapısını, depthwise separable convolutions, BatchNormalization, Squeeze and Excitation modülü, Projection phase, BatchNormalization, activation ve Skip connection internals katman bileşenleri oluşturmaktadır. Full convolutional katman mimarisinin yerini linear bottleneck katmanları almaktadır. Depthwise separable convolutions blok mimarisinde full convolutional operator sinir ağı katmanı, faktörlere parçalanarak konvolüsyonel katman iki ayrı katmana ayrıştırılmaktadır. Ayrıştırılan ilk katman depthwise convolution katmanıdır, her girdi kanalı için hafif donanımlı tek konvolüsyon filtrelemesi uygulamaktadır. Ayrıştırılan ikincil katman (1x1) pointwise convolution katmanıdır, (1x1) pointwise convolution katmanı, girdi kanal parametrelerine ait lineer hesaplama bileşimlerinin yeni öznitelik çıktılarını birleştirmektedir. Standart konvolüsyon katmanları, hixwixdi girdi Li tensor yapısını girdi olarak almaktadır ve hixwixdj çıktı Lj tensor yapısını üretmek için K konvolüsyonel çekirdek (kernel) filtrelemesini işlemektedir. Standart konvolüsyon katmanı, hi*wi*di*dj*k*k hesaplama maliyetine sahipken depthwise separable konvolüsyon katmanı formal konvolüsyon işlevselliğinde daha düşük hesaplama maliyetine sahiptir. Depthwise katman ve (1x1) pointwise convolution katman toplamı, standart konvolüsyon katmanına kıyasla daha düşük çalışma maliyetindedir. Depthwise separable convolution katmanı, geleneksel katmanlara göre çalışma maliyetini k^2 faktör düşürmektedir [15].



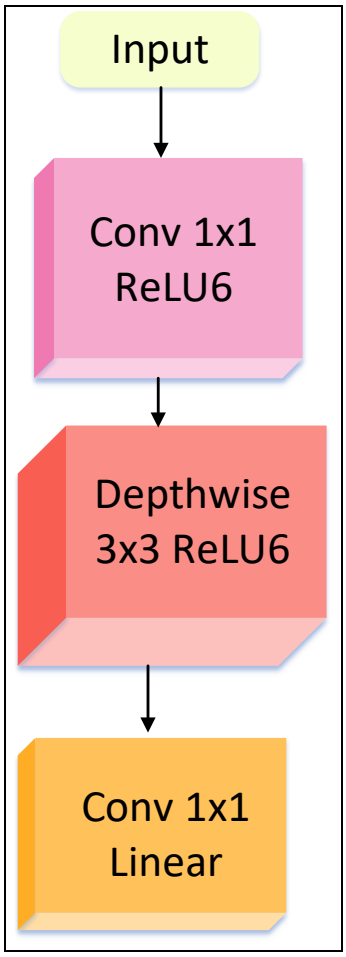
Şekil 3.2. MBConv bloğu

Linear Bottleneck bloğu

Şekil 3.3. figüründe linear bottleneck bloğu, (1x1), (3x3) Depthwise ve (1x1) Linear filtre boyutlarına ve sinir ağı aktivasyon tensor yapılarının ReLU katman dönüşümlerine sahip konvolüsyonel bloklar olarak gösterilmiştir. Sinir ağı katmanına ait aktivasyon tensor yapıları, hixwi pikselli di boyutunda blok bileşenleridir ve tam katman aktivasyonları, öznitelik değeri taşıyan "ilgi alanı" uzanımlarını genellemektedir. Sinir ağlarında öznitelik ilgi alanları, düşük-boyutlu parçalı alanlara aktarılabilmektedir. Derin konvolüsyon katmanındaki d-kanallı pikseller irdelendiğinde bağlantılı piksellere kodlanan sayısal değerlerin, öznitelik ilgi alanlarına bütünleşmesi görülmektedir. Öznitelik ilgi alanları, düşük boyutlu parçalı alanlara tanımlanabilmektedir. Bu durum derin konvolüsyon katman

boyutu düşürülerek öznitelik operasyon alanına ait uzaysal alan boyutunun düşürülmesini sağlamaktadır. Bu yaklaşım hesaplama maliyeti ve model doğruluk oranının birbirini dengelemesinde yararlanılmaktadır, katman genişliği çarpan parametresi, etkin model tasarımına bağlanmaktadır. Katman genişliği çarpan parametresi, derin mimari katmanında aktivasyon uzay boyutunu, nöron öznitelik ilgi alanını tamamlayana kadar düşürmektedir. Yalnız derin konvolüsyonel sinir ağlarına ait ReLU gibi lineer olmayan nokta koordinat dönüşümleri, bağlantılı yaklaşımı kırmaktadır. Genel anlamda ReLU katman dönüşümü, ful boyutsal çıktıyı karşılayan B girdi uzayına ait lineer dönüşüm üzerinden üretilen sıfır-olmayan S birimine sahiptir ve sıfır-olmayan S birimi lineer dönüşüme bağımlıdır. Derin sinir ağları, öznitelik çıktı alanına ait sıfır-olmayan birime odaklanan lineer sınıflandırıcının gücüyle sınırlıdır [15].

ReLU dönüşümü, sinir ağı kanal aktivasyonları geçişinde anlamlı öznitelik bilgisine çözümlenebilen bilgi akışı üretmektedir. ReLU dönüşümüne ait kanal parametresi dağıldığında o kanalın bilgi aktivasyonu kaybedilmektedir ve ReLU dönüşümünün bilgi akışı, sinir ağı kanal aktivasyonlarını tamamlayamamaktadır. Birden fazla sinir kanal parametresinin varlığında kaybolan sinir kanal parametresi haricindeki sinir ağı kanal parametreleri aktivasyon alan bilgisini barındırabilmektedir. Veri girdi alanı, oldukça düşük boyuttaki aktivasyon uzayına bütünleşebilmektedir, paralelde ReLU dönüşümü, lineer olmayan karmaşık dokuyu bilgi akışının fonksiyonelliğine katarken sinir ağı kanal aktivasyon bilgisini korumaktadır. Aktivasyon ilgi alanı uzanımının yüksek boyutlu aktivasyon uzayına ait düşük boyutlu uzay parçasına tanımlanması gerekmektedir. Bu durumda yüksek boyutlu aktivasyon uzayına ait yüksek seviyeli aktivasyon ilgi alanı, düşük boyutlu aktivasyon uzay parçalarına ayrılabilmektedir. Benzer olarak depthwise separable convolution blokları, yüksek boyutlu konvolüsyon filtre katman çekirdeklerini (kernel) daha düşük boyutlu konvolüsyon yapılarına ayırmaktadır. Depthwise konvolüsyon katmanlarına ait ReLU dönüşümü, lineer olmayan aktivasyon karakteristiklerini bilgi akışına katmaktadır. ReLU dönüşümü, düşük boyutlu aktivasyon uzay parçasında veri girdi alanına ait önemli detayları kaydedebilmektedir. Depthwise (3x3) konvolüsyon yapılarındaki linear bottleneck katman blokları, ReLU dönüşümüyle düşük boyutlu aktivasyon uzay parçalarını yakalamaktadır ve lineer olmayan dağıtık sıçramaların sebep olduğu bilgi kaybını önlemektedir.

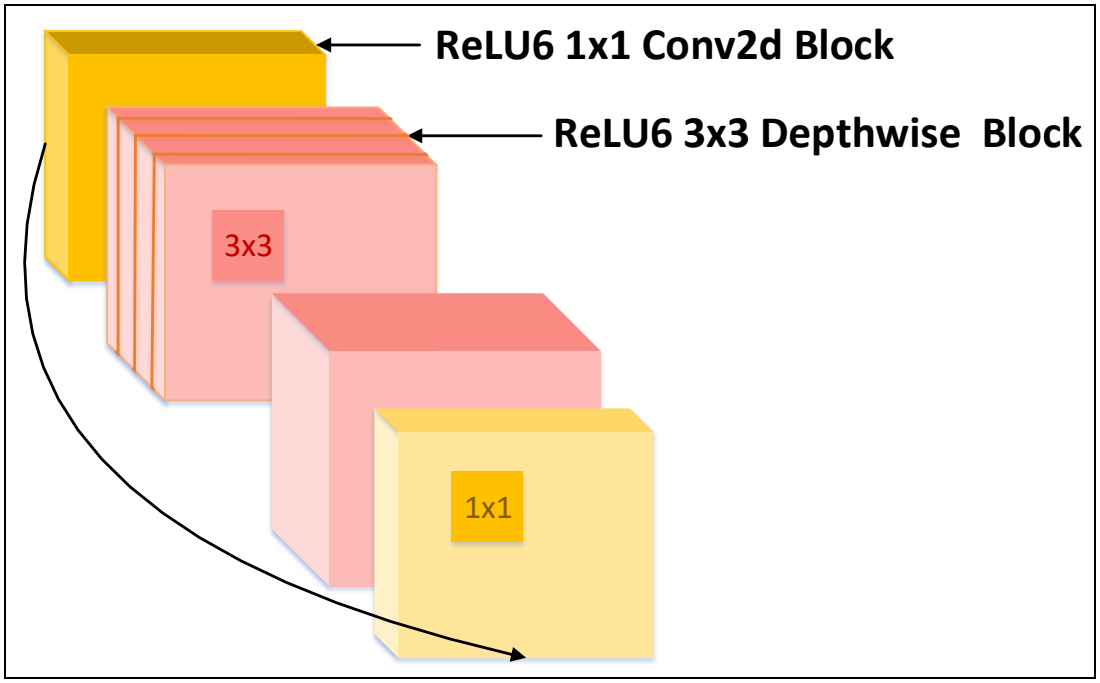


Şekil 3.3. Linear Bottleneck bloğu

Inverted residual bloğu

Şekil 3.4. gösteriminde inverted residual bloğu, bottleneck blokları ve katman genişlemelerini birleştiren (1x1) Conv2d ve (3x3) Depthwise bloklarına sahiptir. Bottleneck blokları, modelin öznitelik çıkarımı kapasitesinin büyük bir kısmını korurken sinir ağının parametre yoğunluğunu düşürmektedir. Bottleneck blokları, residual blok mimarisine benzemektedir, her residual blokta ilk başta girdi katmanını takip eden birden fazla bottleneck katmanı, genişleme (expansion) katmanıyla sürdürülmektedir. Sandler ve ekibine göre residual bloğu, ilk önce genişleyen sonra daralan ve ardından tekrar genişleyen katman uzanımına sahiptir ve girdi katmanının ardından birden çok bottleneck katmanıyla başlamaktadır. Inverted residual blok ise ilk önce daralan sonra genişleyen ve ardından tekrar daralan katman uzanımına sahiptir. Inverted residual bloğunun katman uzanımı, (1x1) Conv2d bloğu, (3x3) Depthwise bloğu ve (1x1) Conv blok yapılarını birleştirmektedir. Bottleneck blokları önemli öznitelik bilgisini taşırken genişleme katmanları lineer-olmayan

öznitelik dönüşüm detaylarını model ağırlığı eklemeden aktifleştirmektedir. Bu durumda bottleneck blokları arasında kestirme nöron bağlantıları "shortcut" altında yapılandırılmaktadır.



Şekil 3.4. Inverted residual bloğu

EfficientNet mimari ölçeklendirmesi

EfficientNet mimarisinin ölçeklendirmesinde sinir ağı derinlik, genişlik ve çözünürlük donanımları dengeli bir artışlara tabi tutularak model performansı iyileştirilebilmektedir. EfficientNet mimari ölçeklendirmesi, compound katsayısı yardımıyla networke ait derinlik, genişlik ve çözünürlük boyutları üzerinden aynı anda gerçekleştirilmektedir. Paralelinde sinir ağının mimari tabanı, EfficientNet model ailesine -EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6, EfficientNet-b7- genişletilmektedir. Örneğin basit EfficientNet-b0 mimarisi ve daha karmaşık EfficientNet-b7 mimarisi bu mimari genişlemeye örnektir. Konvolüsyonel tasarım yapısı, sinir ağı katman mimarisinin dönüşümünü irdelerken katman genişliği, kanal sayısı, girdi yüksekliği ve genişliği parametrelerini oldukça esnek bir anlamda analiz etmektedir. Katman derinlik (d), genişlik (w) ve çözünürlük (r) boyutlarının ölçeklendirmesi, ayrıcı parametrelerle bağımlıdır ve farklı kaynak sınırlamalarına sahiptir. Örneğin katman derinlik ölçeklendirilmesi katman sayısı, katman genişlik ölçeklendirmesi kanal sayısı ve çözünürlük

ölçeklendirmesi girdi genişliği ve yüksekliği parametrelerine bağlıdır. EfficientNet-b0 katman mimarisi, 224 çözünürlük ölçeklendirmesi ve 237 katman sayılı derinlik ölçeklendirmesine sahiptir, EfficientNet-b7 600 çözünürlük ölçeklendirmesi ve 813 katman sayılı derinlik ölçeklendirmesine sahiptir.

Derinlik (d)

Sinir ağı derinliğinin ölçeklendirilmesi, formal konvolüsyon yapılarında sıklıkla kullanılmaktadır. Derinlik artışıyla formal konvolüsyon yapıları (ConvNet) daha karmaşık ve veri dokusunca zengin öznitelik bilgilerini yakalayabilmektedir, daha önce görülmeyen görevlere daha iyi genelleyebilmektedir. Yalnız derin sinir ağları, kaybolan gradyan problemi sebebiyle daha zorlu eğitim döngüsüne sahiptir. Atlamalı nöron bağlantıları (skip connections) ve BatchNormalization eklentisi, eğitim döngüsü problemini seyreltse de derin sinir ağının eğitim doğruluğunu düşürmektedir [16].

Genişlik (w)

Sinir ağı genişliğinin ölçeklendirilmesi, küçük boyuttaki modeller için yaygın kullanılmaktadır. Genişliğinin ölçeklendirmesi, ilgili sinir ağı kanal sayısına göre ayarlanmaktadır ve sinir ağı genişliğinin arttırılması, Zagoruyko ve Komodakis çalışmasının bulgularıyla örtüşen şekilde modelin öznitelik çıkarma kapasitesini arttırmaktadır. Zagoruyko ve Komodakis çalışmasında bahsedildiği gibi daha geniş sinir ağları, daha ince detaylı öznitelik bilgilerini yakalayabilmektedir ve daha kolay eğitim döngüsüne tabi olabilmektedir. Yalnız oldukça geniş sinir ağları, daha yüksek seviyeli öznitelik bilgilerini yakalamakta zorlanmaktadır ve genişlik sınırları arttıkça eğitim döngüsünün doğruluk oranı tıkanmaktadır.

Çözünürlük (r)

Konvolüsyon yapıları, daha yüksek çözünürlüklü girdi görüntüleriyle potansiyel daha detaylı öznitelik örüntülerini yakalayabilmektedir. Çözünürlük ölçeklendirmesi, girdi görüntüsünün yükseklik ve genişlik parametrelerine bağlıdır. Girdi görüntüsü çözünürlük ölçeklendirmesinde (224x224) düşük boyut değerinden başlanarak daha yüksek boyutlu (300x300) boyutuna genişlendiğinde konvolüsyonel katmanlar yüksek çözünürlüklü

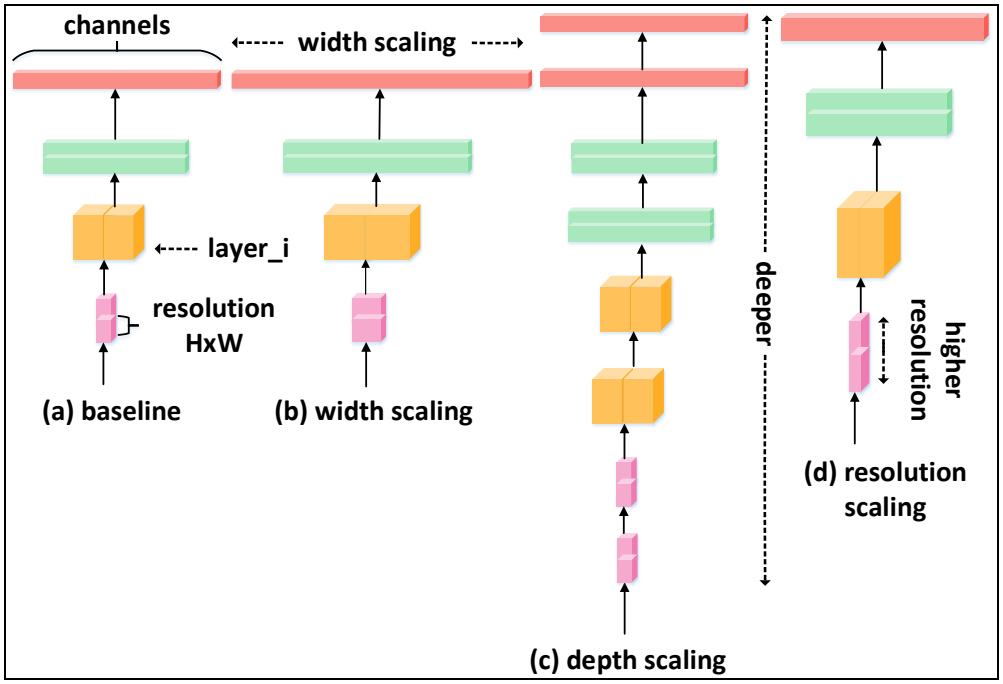
görüntü piksellerini daha başarılı sınıflandırmaya sahip özniteliklere birleştirebilmektedir. Sinir ağı çözünürlüğünün arttırılması, performans sonuçlarında doğruluk oranlarını arttırabilmektedir, yalnız doğruluk oranı artışı, çok yüksek sinir ağı çözünürlüklerinde bozulmaktadır.

Compound scaling

Şekil 3.5. gösteriminde compound scaling taban katman boyut parametrelerinin genişlik ölçeklendirme, derinlik ölçeklendirme ve çözünürlük ölçeklendirmesi olarak çizilmiştir. Sinir ağı mimarisinde katman boyut parametrelerinin ölçeklendirmesi, birbirine bağımlıdır. Daha yüksek girdi çözünürlüğünde sinir ağı derinliğinin arttırılması, nöron kanallarının alıcı alanlarını genişletmektedir ve daha geniş nöron kanallarının alıcı alanları, daha yüksek çözünürlüklü piksel yoğunluklarında benzer öznitelik örüntülerini yakalayabilmektedir. Sinir ağı kanal sayısının artışı, katman derinliği ve girdi çözünürlüğünün artışıyla dengeli ölçeklendirmeye tabi tutulmaktadır. Paralelinde daha yüksek girdi çözünürlüklerinde sinir ağı genişliği ve derinliğinin arttırılmasıyla daha detaylı öznitelik bilgileri, daha yüksek çözünürlüklü piksel yoğunluklarının etkisiyle sinir ağı networküne kazandırılmaktadır. Örneğin EfficientNet-b0 mimarisinden EfficientNet-b7 mimarisine geçişte katman derinliği ve girdi çözünürlüğü, konvolüsyon bloklarının sinir ağı kanal sayısıyla birlikte artmaktadır. Bu durum genişlik, derinlik ve çözünürlük ölçeklendirmesinde katman boyut parametrelerinin birleşik koordinasyonunu ve dengesini gerektirmektedir, sadece tek katman boyut parametresinin diğer katman boyut parametrelerinden bağımsız ölçeklendirmesi, yetersiz model performansına sebep olmaktadır. Tek-boyutlu katman parametre ölçeklendirmesi, yetersizdir.

Sinir ağı konvolüsyonel yapısının, katman derinlik, genişlik ve çözünürlük boyutlandırmalarını dengelemesi, daha etkin doğruluk performansı için kritiktir. Önerilen compound scaling metodu, compound katsayısı yardımıyla sinir ağı konvolüsyonel yapısına ait katman derinlik, genişlik ve çözünürlük boyutlandırmalarını, tutarlı düzlemde ölçeklendirmektedir. Sinir ağı katman derinlik, genişlik ve çözünürlük boyutlandırma sabitleri, küçük çaplı "grid search" araştırmasıyla belirlenebilmektedir. Compound katsayısı, sinir ağı konvolüsyonel yapısının model ölçeklendirmesinde kaynak dağılımını kontrol eden dinamik değerdir. Bağlantılı derinlik, genişlik ve çözünürlük sabitleri, ölçeklendirilen

kaynak dağılımının network derinlik, genişlik ve çözünürlüğüne nasıl aktarılacağını açıklayan değerlerdir [16].



Şekil 3.5. Compound scaling gösterimi

3.1.3. CORAL transfer learning algoritması ve dynamic distribution adaptation network

Transfer learning algoritmaları

Transfer learning algoritmalarında source domain ve target domain ayrımları görev bağlamında ya da veri dağılımı bağlamında ayrışabilen birbiriyle ilişkili veri örneklemlerini ifade etmektedir. source domain ayrımı, öznitelik bilgisini transfer learning algoritması üzerinden target domain ayrışımına aktararak görev alanına ait performansı arttırmaktadır. Yalnızca tek malware veri kümesi olması durumunda bağlantılı malware veri kümesi zaman gibi kıstaslara göre source domain ile target domain ayrımlarına bölünebilmektedir.

Tek malware veri kümesi source domain ve target domain bölünmeleri zamansal ya da anlamlı diğer bir karakteristik ölçütte gerçekleşmektedir. Örneğin yıllar içerisinde toplanan bir malware veri kümesi, geçmiş yıllara ait malware örneklerini “source domain” olarak ayırırken daha ileriki yıllara ait malware örneklerini “target domain” olarak ayırmaktadır.

Eğer zamansal bilgi mevcut değilse tek malware kümesi dengeli bir ayrımla “source domain” ve “target domain” olarak bölünebilmektedir.

An effectiveness analysis of transfer learning for the concept drift problem in malware detection araştırma çalışmasında malware verileri Temporal Split üzerinden source domain ve target domain alanlarına bölünmüştür. VirusShare malware verileri, 2015, 2017, 2019 ve 2020 yılları bandında source domain ve target domain alanlarına aktarılmıştır. Source domain alanı özellikli daha geçmiş yıl bandına ait malware verilerini içerirken target domain alanı daha ileriki yıl bandına ait malware verilerini içermektedir. Transfer learning algoritmaları ilgili source domain ve target domain alanlarına uygulanmıştır. TrAda, CORAL, DTS, DAE ve TIT transfer learning algoritmaları bahsi geçen araştırma çalışmasında bahsedilmiştir. İlk olarak TrAda transfer learning algoritması, AdaBoost genellemesinin transfer learning problemlerine aplikasyonudur. TrAda transfer learning algoritması, eğitim döngüsünün hata payı arttığında source domain örneklerine ait aktivasyon ağırlığını düşürmektedir. TrAda transfer learning algoritması, ensemble modellemesinde tahminleri yürütmektedir. CORAL transfer learning algoritması, source domain alanına ait öznitelik kovaryansını target domain alanına ait öznitelik kovaryansına yaklaştırmaktadır. Bu durum source verisinin beyazlaştırılmasıyla (öznitelik korelasyonunun 0’a düşürülmesiyle) ve target domain alanına ait kovaryansın aktivasyonuyla gerçekleşmektedir. Orijinal öznitelik alanı değiştirilmemektedir. DTS metodu, manifold öğrenmesine dayanmaktadır. Manifold öğrenmesi, veri örneklemini orijinal öznitelik uzayına ait veri aktivasyonları koruyan yeni aktivasyon uzayına yansıtmaktadır. Yansıtılan source domain veri aktivasyonları, komşu target domain veri aktivasyonlarının lineer kombinasyonuyla oluşturulabilmektedir. DAE metodu ise autoencoder kullanımına dayanmaktadır. Autoencoders orijinal veri uzayına ait maksimum bilgi uzanımını boyutsal indirgemeli yeni öznitelik uzayına dönüştürmektedir. Bu metot autoencoder target fonksiyonunu korunan bilgi uzayı source domain ve target domain alanlarını kapsayacak şekilde değiştirmektedir. TIT metodu, principal component analysis (PCA) uzanımının kernel (çekirdek) formülüne bağlıdır. Bu metot domain veri alanını yeni öznitelik uzayına yansıtmaktadır, yeni öznitelik uzayında birbirine komşu aynı sınıf örneklerine ait veri bilgisini korumaktadır ve optimizasyon problemine anlamlı öznitelik ayrımlarını eklemektedir [17].

İlgili araştırma çalışmasında transfer learning algoritmaları, etiketli malware verisinin yetersizliğine karşın yeni malware tespitinin geliştirilmesi amacıyla sunulmuştur. Özellikle TrAdaBoost, CORAL ve DAE transfer learning algoritmaları başarılı olmuştur. Bu tez çalışmasında CORAL transfer learning algoritmasının source domain ve target domain alanlarını kapsayan adaptasyon parçalaması tercih edilmektedir. CORAL kaybı, backbone sinir ağına uygulanmaktadır ve dynamic distribution adaptation networkünde target domain ve source domain alanlarının transfer edilebilirlik ölçümünü tanımlamaktadır.

Dynamic distribution adaptation network

Transfer learning with dynamic distribution adaptation araştırma çalışmasında Dynamic Distribution Adaptation (DDA) metodu sunulmuştur. Dynamic Distribution Adaptation metodu veri alanlarına ait her öznitelik dağılımının nicel ağırlığını değerlendirmektedir. DDA (Dynamic Distribution Adaptation) transfer learning problemlerinin çözümünde öznitelik sinir ağı transfer geçişlerinin yapısal risk minimizasyonuna katılabilmektedir. Araştırma çalışması DDA (Dynamic Distribution Adaptation) tabanında geleneksel transfer learning için MDDA (Manifold Dynamic Distribution Adaptation) ve derin transfer learning için Dynamic Distribution Adaptation Network (DDAN) öğrenme algoritmalarını önermiştir. Dynamic Distribution Adaptation transfer learning uzanımında marjinal ve koşullu öznitelik dağılımları, dinamik ve nicel adaptasyona dönüştürülmektedir. Dynamic Distribution Adaptation domain alan geçişlerinde ayrışma hesaplamasıyla dinamik öznitelik dağılım ağırlıkları öğrenilmektedir ve temsil öğrenmesi gerçekleştirilmektedir. Ardından marjinal ve koşullu öznitelik dağılımlarının karşılıklı önem değerleri çıkarılmaktadır ve daha aktarılabilir öznitelik temsilleri öğrenilmektedir. Relatif önem değerlerinin dinamik öğrenimi ve öznitelik öğrenmesi, domain-sabit transfer sınıflandırıcı öğrenmesinde döngüsel olarak optimize edilmektedir. Dynamic Distribution Adaptation Network (DDAN) öznitelik g(.) öğrenme fonksiyonu ve f sınıflandırma fonksiyonunun uçtan uca öğrenmesini gerçekleştirmektedir. DDAN derin sinir ağlarına ait uçtan uca eğitim döngüsüyle öznitelik temsillerini öğrenmiştir. Backbone network yararlı öznitelik temsillerini öğrenirken DDA metoduyla domain adaptasyonu uygulamaktadır [18].

Dynamic Distribution Adaptation Network DDAN mimarisinde source domain ve target domain alanlarına ait veri örnekleri derin sinir ağlarına girilmektedir. AlexNet ve ResNet gibi konvolüsyonel sinir ağları, veri örneklerinden yüksek-seviyeli öznitelikleri

çıkarmaktadır. Yüksek-seviyeli öznitelikler fully-connected katmanından geçirilerek softmax sınıflandırmasına atanmaktadır. Özgün mimari parça, dynamic distribution adaptation metodunun kullanılarak source domain ve target domain alanlarına ait öznitelik dağılımlarının yakınlaştırılmasıdır. DDAN mimarisinin derin sinir ağı eğitim döngüsüne mini-batch SGD (Stochastic Gradient Descent) algoritmasını katmaktadır. Dynamic distribution adaptation domain alanlarının batch parçaları üzerinden hesaplanmaktadır [18].

Deep and adversarial transfer learning

Derin transfer öğrenmesi, derin sinir ağlarının daha gelişmiş öznitelik çıkarımı kapasitesi ve kayıp fonksiyonları ya da optimizasyon fonksiyonlarının etkisiyle ilerlemiştir. Özellikle kayıp fonksiyonları, source domain bilgisinin target domain alanına ait öznitelik ayrışıma aktarılmasında değerlendirme modeli olmuştur. Ek olarak source domain ve target domain alanlarının birbirine adaptasyonu kayıp fonksiyon geçişiyle sağlanmaktadır. Örneğin Deep Domain Confusion (DDC) metodu MMD kaybını derin networke katmıştır ve domain alanları arasında derin network adaptasyonunu sağlamıştır. Benzer olarak DAN (Deep Adaptation Networks) çok-çekirdekli birinci dereceden kayıp formülüne sahip MMD yapısını katmıştır. Derin CORAL networkü ise ikinci dereceden kayıp formülüne sahip CORAL kaybını katmıştır. CORAL kaybı, Dynamic distribution adaptation networkünde kullanımdadır ve network eğitim döngüsünde source domain ve target domain alanlarının birbirine adaptasyonunu ölçmektedir. Dynamic distribution adaptation network ve CORAL, MMD gibi kayıp fonksiyonlarının yanında adversarial learning yaklaşımı, target domain ve source domain alanları arasında aktarım potansiyelli öznitelik temsil karakteristiklerinin öğrenimini desteklemektedir. DANN (Domain Adversarial Neural Network) modeli, uzaklık dağılımı formülüne bağlı MMD (Maximum Mean Discrepancy) benzeri kayıp fonksiyonları yerine domain adversarial kaybına sahiptir. Bu durumda network modeli, domain alanları arasında daha ayrıştırıcı öznitelik temsil bilgilerini öğrenmektedir.

3.2. Kullanılan Veri Kümeleri

3.2.1. Dumpware10

Hacettepe Üniversitesi tarafından üretilen Dumpware10 veri kümesi, kötü amaçlı yazılımların görüntü tabanlı bir yaklaşımla tespit edilmesi için oluşturulmuştur ve GIST ile

HOG (Histogram of Gradients) gibi görüntü tanımlayıcılarıyla birleştirilmiştir. Bu veri kümesine ait araştırma çalışması, kötü amaçlı yazılımların yakalanmasına dayanmış ve kripto kötü amaçlı yazılım durumunu yansıtmıştır. Dumpware10 veri kümesine ait kötü amaçlı yazılım görüntülerinin oluşturulmasında, 224 ile 4096 piksel aralığında dört farklı çözünürlük kullanılmıştır. GIST ve HOG görüntü tanımlayıcıları hem ayrı ayrı hem de birlikte bilgi füzyonu kapsamında değerlendirilmiştir. Boyutsal indirgeme ve çok yönlü öğrenme tekniği olan UMAP, kötü amaçlı yazılım görüntü dönüşüm problemleri kapsamında kullanılmıştır. Veri kümesi, 10 benzersiz kötü amaçlı yazılım ailesi ve bir iyi huylu yazılım sınıfını içeren toplam 11 veri sınıfından oluşmaktadır. Dumpware10 veri seti, 3433 eğitim seti ve 861 doğrulama seti örneği olmak üzere toplam 4294 veri örneğine sahiptir ve 300 piksel çözünürlükle (300x300) boyutlarında tercih edilmiştir. Çözünürlük artırımı, bileşik ölçekleme mantığında pozitif etkiye sahip olabilmektedir. Dumpware10 veri kümesi, kötü amaçlı yazılım ve iyi huylu yazılım tespitine yönelik önemli bir kaynaktır. 3686 kötü amaçlı yazılım örneği ve 608 iyi huylu yazılım örneği içeren toplam 4294 RGB görüntüsünden oluşur. Bu veri kümesi, kötü amaçlı yazılımları tanımlamanın yanı sıra iyi huylu dosyaları da ayırt ederek açık set sınıflandırmasına olanak tanır. Dumpware10, dört farklı görüntü genişliğiyle sunulur: 224 piksel, 300 piksel, dosya boyutu karekökü ve 4096 piksel. Veri kümesi, Adposhel, Allaple.A, Amonetize, AutoRun-PU, BrowseFox, Dinwod, InstallCore.C, MultiPlug, VBA ve Vilsel gibi 10 farklı kötü amaçlı yazılım ailesine ait dosyalar içermektedir.

3.2.2. Microsoft malware classification challenge veri kümesi

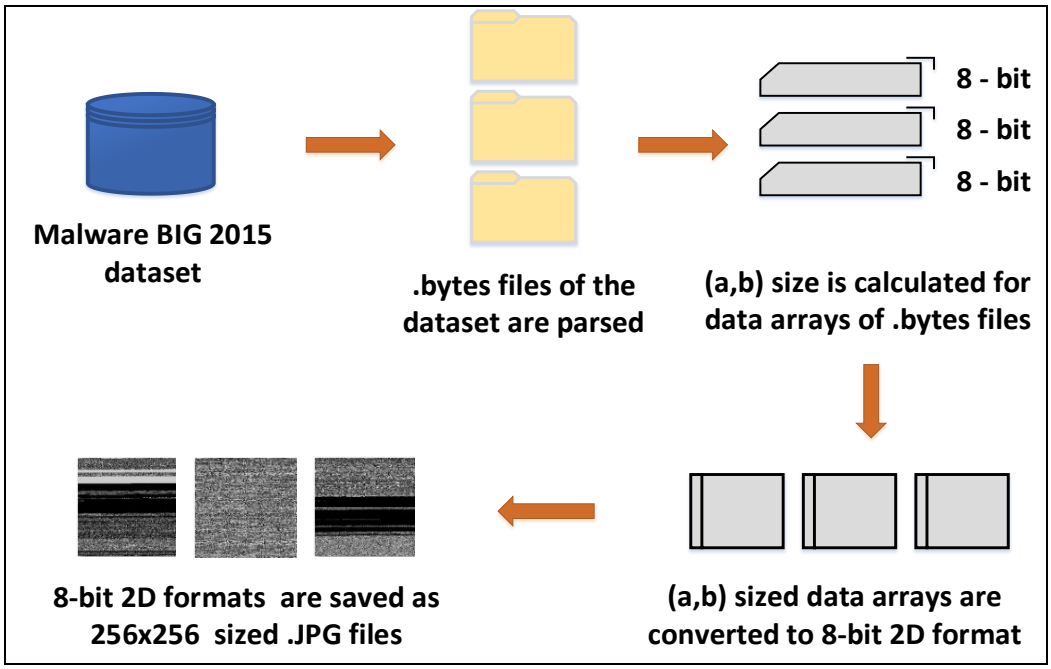
Microsoft Malware Classification Challenge, kötü amaçlı yazılımların sınıflandırılmasına yönelik bir yarışmadır ve bu yarışmada sağlanan eğitim verisi, araştırmacıların farklı kötü amaçlı yazılım ailelerini tanımlayabilmesi için geniş bir veri seti sunar. Yarışma kapsamında 10868 kötü amaçlı yazılım bayt dosyası eğitim verisi olarak sağlanmıştır. Bu veri kümesi, statik analizle kötü amaçlı yazılımların doğru bir şekilde sınıflandırılmasına olanak tanır. Dosyalar, çeşitli kötü amaçlı yazılım ailelerine ait olup, her bir dosya, belirli bir kötü amaçlı yazılım türünü temsil eden ham bayt dizilerini içermektedir. Bu veri seti, kötü amaçlı yazılım analizinde kullanılan makine öğrenimi modellerinin eğitiminde önemli bir kaynak teşkil eder ve araştırmacıların kötü amaçlı yazılım algılama algoritmalarını geliştirmelerine ve iyileştirmelerine yardımcı olur. Veriler, özellikle statik dosya özelliklerine dayanarak kötü amaçlı yazılım sınıflandırması yapmayı amaçlayan araştırmalar için uygundur.

4. ÖNERİLEN MODEL

4.1. Veri Ön İşleme

Araştırmanın veri ön işleme modellemesinde Microsoft Malware Classification Challenge (MMCC) veri kümesine ait malware bayt dosyaları (.bytes) gri tonlamalı iki kanallı malware görüntü dönüşümü ile üç kanallı RGB malware görüntü dönüşümüne tabi tutulmaktadır. Veri ön işlemesi B2IMG malware görüntü dönüşümü algoritmasına paraleldir.

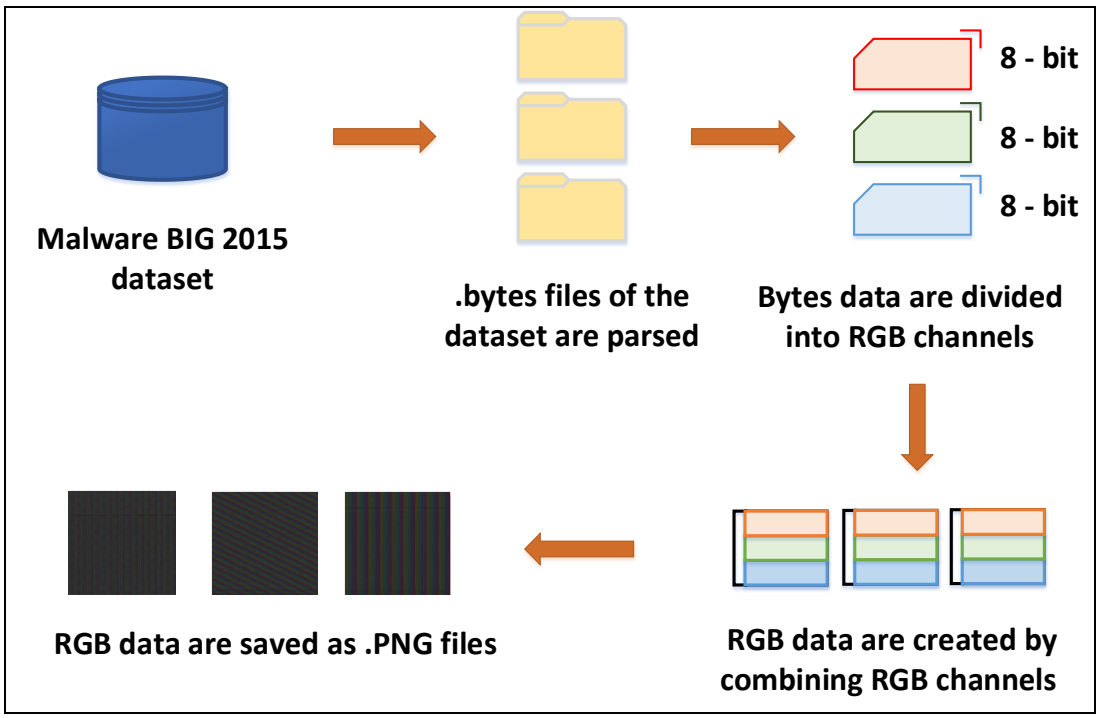
Şekil 4.1. figüründe bayt dosyalarının ayrıştırılması, (a,b) matris dizi modellemelerinin hesaplanması, matris dizi modellemelerinin 8-bitlik gri tonlamalı formatlara çevrilmesi ve 8-bitlik formatların (256x256) boyutlu jpg dosyalarına kaydedilmesi iki kanallı gri tonlamalı malware görüntü dönüşümünde tasvir edilmektedir. İki kanallı gri tonlamalı malware görüntü dönüşümünde bayt dosyaları, 16 sütunluk veri dizisi üzerinden (a,b) matris modellemesine dönüştürülerek 8-bitlik iki kanallı gri tonlamalı formatına atanmıştır ve jpg ya da png uzantılı görüntü dosyalarına kaydedilmiştir [19].



Şekil 4.1. İki kanallı gri tonlamalı malware görüntü dönüşümü

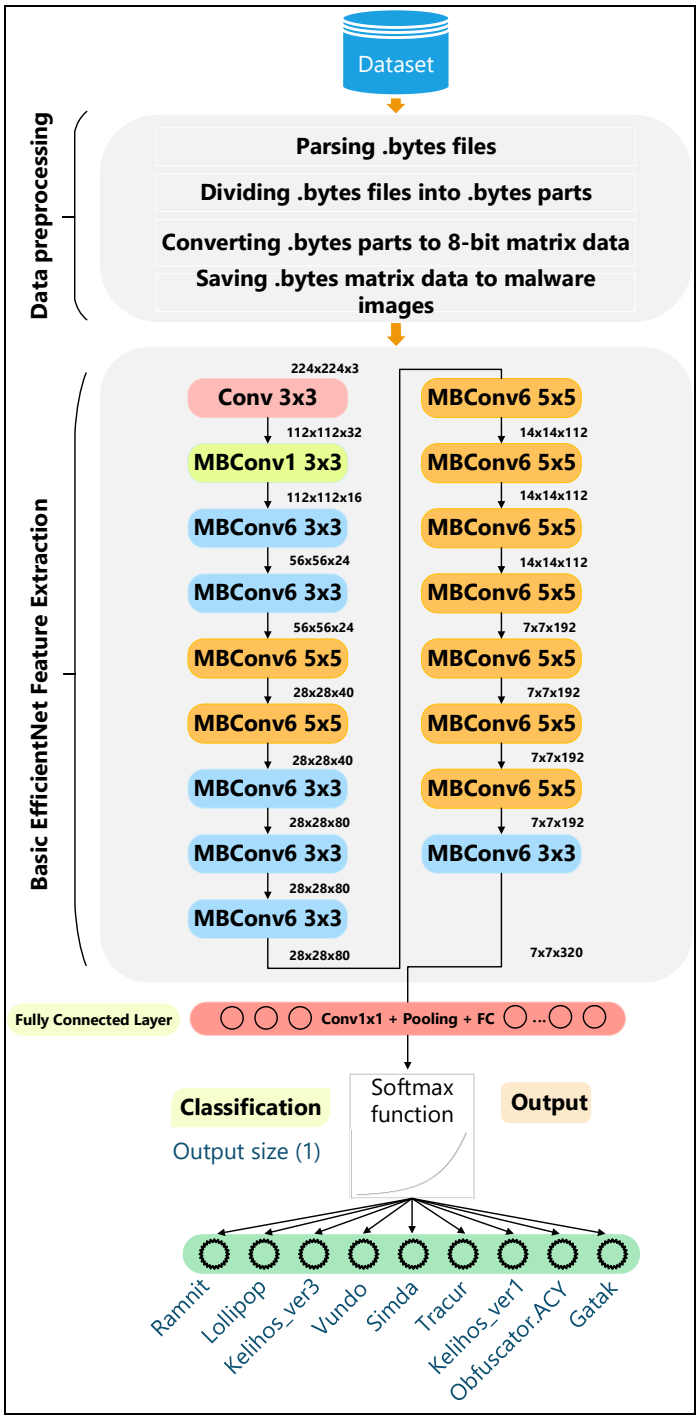
Şekil 4.2. gösteriminde bayt dosyalarının ayrıştırılması, bayt verisinin RGB kanal bloklarına bölünmesi, RGB kanal bloklarının anlamlı RGB verilerine birleştirilmesi ve RGB verilerinin

png dosyalarına kaydedilmesi üç kanallı RGB malware görüntü dönüşümünde tasvir edilmektedir. Üç kanallı RGB malware görüntü dönüşümünde bayt dosyalarından işlenen ikili (binary) veriler üçlü RGB kanal bloklarına bölünmüştür, ardından bağlantılı RGB kanal blokları birleştirilerek yeni RGB veriler oluşturulmuştur ve bağlantılı RGB veriler png görüntü dosyalarına kaydedilmiştir [19].



Şekil 4.2. Üç kanallı RGB malware görüntü dönüşümü

EfficientNet sinir ağı modeli şekil 4.3. figüründe görüldüğü gibi veri ön işleme ile EfficientNet öznitelik çıkarımı aşamalarına ayrılmaktadır. Veri ön işleme aşamasında malware veri kümesi bayt dosyalarına ayrıştırılarak 8 - bitlik matris formatına dönüştürülmektedir ve malware görüntülerine kaydedilmektedir. Ardından EfficientNet öznitelik çıkarımı aşamasında malware görüntüleri, EfficientNet mimarisine aktarılmaktadır ve öznitelik çıkarımından geçirilmektedir. Ve softmax katmanında malware ailelerine atanmaktadır. Veri ön işleme ile EfficientNet öznitelik çıkarımı, fully-connected katmanına bağlı softmax sınıflandırmasında son bulmaktadır. Öznitelik çıkarımı malware görüntülerine ait sınıflandırma karakteristiklerini üretmektedir.



Şekil 4.3. EfficientNet sinir ağı modeli

5. DENEYSEL SONUÇLAR

5.1. Transfer Learning Deneyleri

Microsoft Malware Classification Challenge (MMCC) veri kümesine ait 10868 malware byte dosya eğitim verisi, EfficientNet-b3 ile EfficientNet-b4 sinir ağı mimarilerine tanıtılmaktadır. SGD (Stochastic Gradient Descent) ile Adam algoritmaları, 0,01 öğrenme oranıyla bağlantılı EfficientNet modellerinin eğitiminde yararlanılmaktadır. Önceden eğitilmiş ImageNet-1K model ağırlıkları EfficientNet transfer learning uygulamasında kullanılmaktadır. Spesifik olarak EfficientNet mimarisinde önceden eğitilmiş ImageNet-1K ağırlıklarına ait öznitelik bilgisi, EfficientNet malware sınıflandırmasına finetuning yoluyla aktarılmıştır. Malware verileri iki kanallı gri tonlamalı malware görüntülerine ve üç kanallı RGB malware görüntülerine dönüştürülerek EfficientNet model eğitim döngüsüne katılmaktadır. Üç kanallı RGB malware görüntüleri ile iki kanallı gri tonlamalı malware görüntüleri, 80% oranında eğitim ve 20% test setine ayrılmaktadır. Eğitim setinin malware görüntüleri, 20% oranında değerlendirme (validasyon) setine ayrıştırılarak eğitime girilmektedir. Gri tonlamalı malware görüntüleri (256x256) boyutundadır, üç kanallı RGB malware görüntüleri dosya boyutuna göre değişken 32, 64, 128, 256, 384, 512, 768, 1024 ve 224 boyut genişliklerine atanmaktadır.

Çizelge 5.1. sonuçlarında görüldüğü gibi deneyde gri tonlamalı malware görüntüleriyle eğitilen EfficientNet-b3 ile EfficientNet-b4 mimarilerinde EfficientNet-b4 mimarisi SGD optimizasyonunda, 0,90 doğruluk oranına erişebilirken RGB malware görüntüleriyle eğitilen EfficientNet-b3 ile EfficientNet-b4 mimarilerinde EfficientNet-b3 mimarisi, SGD optimizasyonunda 0,91 doğruluk oranına erişmektedir. Adam algoritması, SGD algoritmasına kıyasla daha düşük doğruluk oranları göstermektedir. EfficientNet-b3 mimarisinin EfficientNet-b4 mimarisine genişletilmesi Adam optimizasyonunda doğruluk oranını yükseltirken RGB malware görüntülerinin eğitimine ait SGD optimizasyonunda nispeten düşürmektedir.

Çizelge 5.1. EfficientNet-b3 ve EfficientNet-b4 modellerinin Microsoft Malware Classification Challenge değerlendirme (validasyon) doğruluk oranları

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
gri tonlamalı malware	EfficientNet-b3	0,01	SGD	0,897642
gri tonlamalı malware	EfficientNet-b4	0,01	SGD	0,907418
gri tonlamalı malware	EfficientNet-b3	0,01	Adam	0,753306
gri tonlamalı malware	EfficientNet-b4	0,01	Adam	0,840713
rgb malware	EfficientNet-b3	0,01	SGD	0,917194
rgb malware	EfficientNet-b4	0,01	SGD	0,897067
rgb malware	EfficientNet-b3	0,01	Adam	0,826337
rgb malware	EfficientNet-b4	0,01	Adam	0,885566

Çizelge 5.2. sonuçlarında gri tonlamalı malware görüntülerinde SGD optimizasyonuyla eğitilen EfficientNet-b3 ile EfficienNet-b4 mimarileri en yüksek test doğruluk oranındadır. SGD optimizasyonu 0,01 öğrenme oranında Adam optimizasyonuna kıyasla daha başarılıdır.

Çizelge 5.2. Microsoft Malware Classification Challenge EfficientNet-b3 ve EfficientNet-b4 test doğruluk oranları

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
gri tonlamalı malware	EfficientNet-b3	0,01	SGD	0,89
gri tonlamalı malware	EfficientNet-b4	0,01	SGD	0,89
gri tonlamalı malware	EfficientNet-b3	0,01	Adam	0,70
gri tonlamalı malware	EfficientNet-b4	0,01	Adam	0,80
rgb malware	EfficientNet-b3	0,01	SGD	0,88
rgb malware	EfficientNet-b4	0,01	SGD	0,86
rgb malware	EfficientNet-b3	0,01	Adam	0,80
rgb malware	EfficientNet-b4	0,01	Adam	0,86

Malware classification and Visualization Using EfficientNet and B2IMG Algorithm araştırma çalışmasına ait Microsoft Malware Classification Challenge (MMCC) gri tonlamalı malware görüntüleri kullanılmıştır. Bağlantılı gri tonlamalı malware görüntüleri, dosya boyutu sınırlarının oluşturduğu 32, 64, 128, 256, 384, 512, 768, 1024 bantlarında eşit boyutta genişlik ve yükseklik değerlerine tanımlanmıştır [11]. İlişkili araştırma çalışmasına ait gri tonlamalı malware görüntüleri, B2IMG veri ön işleme algoritmasından -bu çalışmanın veri ön işlemesine paralel- önceden geçirilmiştir, sadece (256x256) boyut sabitlemesi yoktur ve 80% eğitim seti ile 20% test setine ayrılmıştır. Ardından gri tonlamalı malware görüntüleri, EfficientNet-b0...b7 mimarilerine girilmiştir. Eğitim seti ile test seti, Gatak, Kelihos_ver1, Kelihos_ver3, Lollipop, Obfuscator.ACY, Ramnit, Simda, Tracur, Vundo 9 malware ailesine dağılmıştır. Gri tonlamalı malware görüntülerinin eğitim seti, 20% oranında değerlendirme (validasyon) ayrımıyla 120 epoch döngüsünde eğitilmiştir. Bu eğitim döngüsü, 0,01 öğrenme oranlı SGD optimizasyonuna sahiptir. Eğitimin en yüksek doğruluk oranı, EfficientNet-b7 mimarisinde elde edilmiştir.

Bu çalışmada önceden veri ön işlemeli Microsoft Malware Classification Challenge (MMCC) RGB malware görüntüleri, EfficientNet geçişinde (224x224) rastgele parçalara boyutlanmıştır. Malware görüntüsünden rastgele parçalar kırpılmaktadır ve (224x224) boyutuna dönüştürülmektedir. Rastgele malware görüntü parçalarıyla EfficientNet modeli, malware görüntüsünün doku karakteristiğini daha başarılı öznitelik analiziyle çıkarabilmektedir. RGB malware görüntüleri sırasıyla EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6, EfficientNet-b7 mimarilerine girilmektedir. RGB malware görüntüleri 80% eğitim seti ile 20% test setine ayrılmıştır. Eğitim setine ait RGB malware görüntüleri, 20% oranında değerlendirme (validasyon) ayrımıyla 120 epoch döngüsünde eğitilmiştir. Bu eğitim döngüsü, 0,01 öğrenme oranlı SGD optimizasyonuna sahiptir.

Çizelge 5.3. sonucunda Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6 ve EfficientNet-b7 validasyon doğruluk oranları incelendiğinde EfficientNet-b7 model mimarisinin en yüksek validasyon doğruluk oranına sahip olduğu görülmektedir. Gri tonlamalı malware görüntüleri en derin EfficientNet-b7 mimarisinde bağlantılı validasyon doğruluk oranını yakalamaktadır.

Çizelge 5.3. Microsoft Malware Classification Challenge (Gri tonlamalı) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
Gri tonlamalı malware	EfficientNet-b0	0,01	SGD	0,914796
Gri tonlamalı malware	EfficientNet-b1	0,01	SGD	0,935521
Gri tonlamalı malware	EfficientNet-b2	0,01	SGD	0,931491
Gri tonlamalı malware	EfficientNet-b3	0,01	SGD	0,916523
Gri tonlamalı malware	EfficientNet-b4	0,01	SGD	0,933218
Gri tonlamalı malware	EfficientNet-b5	0,01	SGD	0,938400
Gri tonlamalı malware	EfficientNet-b6	0,01	SGD	0,944157
Gri tonlamalı malware	EfficientNet-b7	0,01	SGD	0,952792

Çizelge 5.4. sonucunda Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b0 - EfficientNet-b7 mimarilerinin test doğruluk oranı, F1-score, recall ve precision sonuçları incelendiğinde EfficientNet-b7 model mimarisinin en yüksek recall ve F1-score sonuçlarına sahip olduğu görülmektedir. Bütünde EfficientNet-b7 model mimarisi harici model mimarilerine kıyasla daha yüksek validasyon doğruluk oranı, recall ve F1-score sonuçlarına sahiptir.

Çizelge 5.4. Microsoft Malware Classification Challenge (Gri tonlamalı) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin test doğruluk oranı, F1-score, recall, precision sonuçları

Model	Görüntü kanalı	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı	F1-score	Recall	Precision
EfficientNet-b0	Gri tonlamalı	0,01	SGD	90	0,8434	0,8632	0,8314
EfficientNet-b1	Gri tonlamalı	0,01	SGD	92	0,8653	0,8849	0,8536
EfficientNet-b2	Gri tonlamalı	0,01	SGD	93	0,8743	0,8661	0,8902
EfficientNet-b3	Gri tonlamalı	0,01	SGD	92	0,8857	0,8832	0,8904
EfficientNet-b4	Gri tonlamalı	0,01	SGD	91	0,8608	0,8616	0,8625
EfficientNet-b5	Gri tonlamalı	0,01	SGD	94	0,8869	0,9034	0,8754
EfficientNet-b6	Gri tonlamalı	0,01	SGD	93	0,8876	0,9042	0,8749
EfficientNet-b7	Gri tonlamalı	0,01	SGD	93	0,8963	0,9163	0,8815

Çizelge 5.5. sonucunda Microsoft Malware Classification Challenge (RGB) için EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6 ve EfficientNet-b7 validasyon doğruluk oranları incelendiğinde EfficientNet-b5 mimarisinin en yüksek validasyon doğruluk oranına sahip olduğu görülmektedir.

Çizelge 5.5. Microsoft Malware Classification Challenge (RGB) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları

Malware görüntü türü	Model mimarisi	Öğrenme Oranı	Optimizasyon türü	Doğruluk oranı
RGB	EfficientNet-b0	0,01	SGD	0,918344
RGB	EfficientNet-b1	0,01	SGD	0,903968
RGB	EfficientNet-b2	0,01	SGD	0,928695
RGB	EfficientNet-b3	0,01	SGD	0,917194
RGB	EfficientNet-b4	0,01	SGD	0,897067
RGB	EfficientNet-b5	0,01	SGD	0,944796
RGB	EfficientNet-b6	0,01	SGD	0,925244
RGB	EfficientNet-b7	0,01	SGD	0,939045

Çizelge 5.6. sonucunda Microsoft Malware Classification Challenge (RGB) EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6 ve EfficientNet-b7 test sonuçları incelendiğinde EfficientNet-b5 mimarisinin en başarılı F1-score ve recall sonuçlarına sahip olduğu görülmektedir.

Çizelge 5.6. Microsoft Malware Classification Challenge (RGB) için EfficientNet-b0 - EfficientNet-b7 mimarilerinin test doğruluk oranı, F1-score, recall, precision sonuçları

Model	Görüntü kanalı	Öğrenme Oranı	Optimizasyon Türü	Doğruluk oranı	F1-score	Recall	Precision
EfficientNet-b0	RGB	0,01	SGD	89	0,8343	0,8494	0,8230
EfficientNet-b1	RGB	0,01	SGD	88	0,8010	0,8190	0,7897
EfficientNet-b2	RGB	0,01	SGD	89	0,8344	0,8364	0,8348
EfficientNet-b3	RGB	0,01	SGD	88	0,8404	0,8417	0,8429
EfficientNet-b4	RGB	0,01	SGD	86	0,8196	0,8235	0,8258
EfficientNet-b5	RGB	0,01	SGD	91	0,8646	0,8777	0,8550
EfficientNet-b6	RGB	0,01	SGD	89	0,8619	0,8741	0,8557
EfficientNet-b7	RGB	0,01	SGD	92	0,8440	0,8493	0,8418

Çizelge 5.7. sonucunda gri tonlamalı malware görüntülerinin EfficientNet-b7 mimarisinde en başarılı validasyon doğruluk oranını yakaladığını göstermektedir. Çizelge 5.8. sonucunda ise RGB malware görüntülerinin EfficientNet-b5 mimarisinde en başarılı validasyon oranını yakaladığını göstermektedir. Gri tonlamalı malware görüntüleri en başarılı doğruluk oranını RGB malware görüntülerine kıyasla daha derin bir sinir ağı mimarisinde gerçekleştirmektedir.

Gri tonlamalı malware, RGB malware verisine göre daha az gürültülüdür ve malware verisinin öznitelik doku örüntülerine odaklanmaktır. Bu durumda daha derin EfficientNet-b7 modeli ek bir karmaşıklık olmadan daha iyi malware görüntü detaylarını saptayabilmektedir. RGB malware verisi, daha karmaşık üç kanallı yapıdadır ve gri tonlamalı malware verisine göre daha karmaşık kanal gürültüsüne sahiptir. Bu durumda daha basit EfficientNet-b5 modeli eklenen RGB kanal gürültüsünü, daha derin EfficientNet-b7 modeline göre daha başarılı malware görüntü detaylarına çözümleyebilmektedir.

Çizelge 5.7. EfficientNet-b7 mimarisinde gri tonlamalı iki kanallı malware görüntülerin değerlendirme (validasyon) doğruluk oranı

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
Gri tonlamalı malware	EfficientNet-b7	0,01	SGD	0,952792

Çizelge 5.8. sonucunda Microsoft Malware Classification Challenge (MMCC) RGB malware görüntüleri EfficientNet-b5 mimarisinde en başarılı validasyon doğruluk oranına erişmektedir.

Çizelge 5.8. EfficientNet-b5 mimarisinde üç kanallı (RGB) malware görüntülerin değerlendirme (validasyon) doğruluk oranı

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
RGB malware	EfficientNet-b5	0,01	SGD	0,944796

Dumpware10 malware görüntüleri için 300 piksel görüntü çözünürlüğü ile (300x300) piksel görüntü genişliği tercih edilmiştir. Dumpware10 malware görüntüleri, 3433 eğitim seti ile 861 test seti örneğine ayrılarak sırasıyla EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6, EfficientNet-b7 mimarilerine girilmiştir. Bu araştırma kapsamında Dumpware10 malware görüntüleri, 20% oranında değerlendirme (validasyon) ayrımıyla 120 epoch döngüsünde eğitilmiştir. Eğitim seti ile test seti, Adposhel, Allaple, Amonetize, AutoRun, BrowseFox, Dinwod, InstallCore, MultiPlug, Other, VBA, Vilsel sınıflarına dağılmıştır.

Çizelge 5.9. sonucunda Dumpware10 için EfficientNet-b0, EfficientNet-b1, EfficientNet-b2, EfficientNet-b3, EfficientNet-b4, EfficientNet-b5, EfficientNet-b6, EfficientNet-b7 mimarilerinin validasyon doğruluk oranları incelendiğinde en yüksek validasyon doğruluk oranının EfficientNet-b6 mimarisinde olduğu görülmektedir.

Çizelge 5.9. Dumpware10 için EfficientNet-b0 - EfficientNet-b7 mimarilerinin değerlendirme (validasyon) doğruluk oranları

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
RGB	EfficientNet-b0	0,01	SGD	0,922853
RGB	EfficientNet-b1	0,01	SGD	0,921397
RGB	EfficientNet-b2	0,01	SGD	0,912664
RGB	EfficientNet-b4	0,01	SGD	0,909753
RGB	EfficientNet-b5	0,01	SGD	0,914119
RGB	EfficientNet-b6	0,01	SGD	0,934498
RGB	EfficientNet-b7	0,01	SGD	0,925764

Çizelge 5.10. sonucunda Dumpware10 (RGB) malware görüntüleri, EfficientNet-b6 mimarisinde en başarılı validasyon doğruluk oranını yakalamaktadır. Microsoft Malware Classification Challenge (MMCC) (RGB) malware görüntüleri ve Dumpware10 (RGB) malware görüntüleri farklı ölçekli EfficientNet mimarilerine odaklıdır.

Çizelge 5.10. EfficientNet-b6 mimarisinde Dumpware10 üç kanallı (RGB) malware görüntülerin değerlendirme (validasyon) doğruluk oranı

Malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
RGB malware	EfficientNet-b6	0,01	SGD	0,934498

Malware Classification and Visualization Using EfficientNet and B2IMG Algorithm çalışmasına ait gri tonlamalı iki kanallı malware görüntülerinin eğitiminde EfficientNet-b7 mimarisi 95% değeriyle en yüksek doğruluk oranına erişmektedir. Bu araştırma çalışmasına ait üç kanallı (RGB) malware görüntülerinin eğitim uzanımlarında EfficientNet-b5 mimarisi 94% değeriyle en yüksek doğruluk oranına ulaşmaktadır. Hacettepe üniversitesine ait

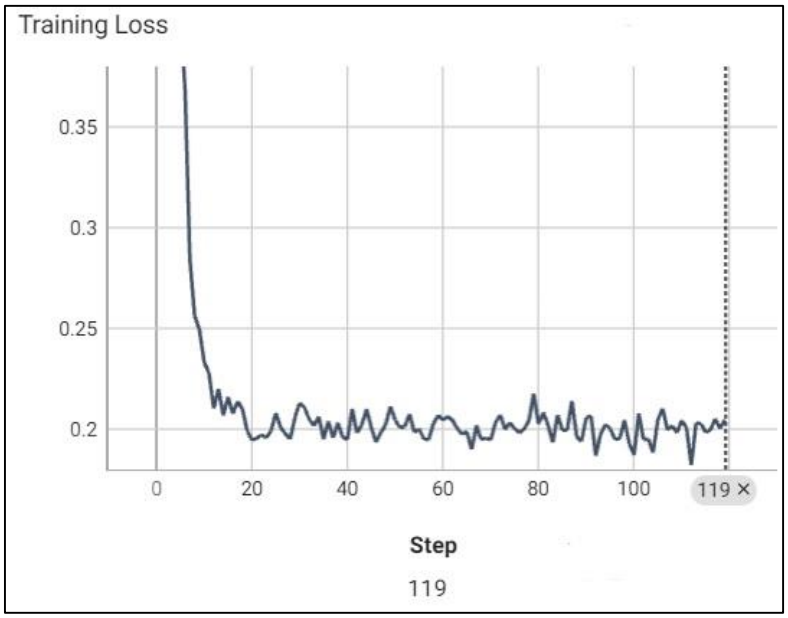
Dumpware10 veri setine ait üç kanallı (RGB) malware EfficientNet-b6 mimarisi 93% oranıyla en yüksek doğruluk oranına ulaşmaktadır.

Çizelge 5.11. sonuçlarında 0,01 öğrenme oranlı SGD optimizasyon türüne sahip EfficientNet-b7 mimarisi gri tonlamalı malware görüntülerinde en yüksek başarı değerlerini kaydetmektedir.

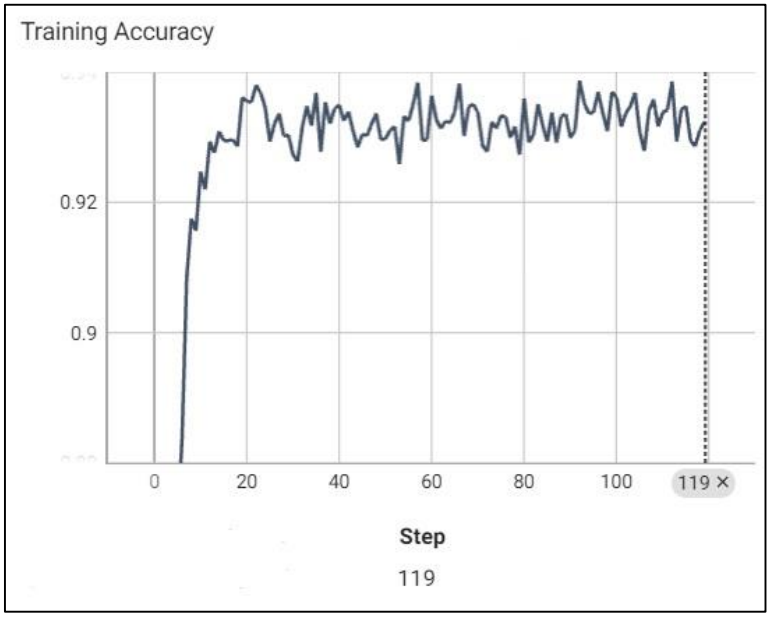
Çizelge 5.11.Microsoft Malware Classification Challenge ile Dumpware10 test doğruluk, F1-score, recall ve precision sonuçları

	Model	Görüntü kanalı	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı	F1-score	Recall	Precision
MS	EfficientNet-b7	Gri tonlamalı	0,01	SGD	0,93	0,8963	0,9163	0,8815
	EfficientNet-b5	RGB	0,01	SGD	0,91	0,8646	0,8777	0,8550
Dumpware10	EfficientNet-b6	RGB	0,01	SGD	0,91	0,8786	0,8843	0,8811

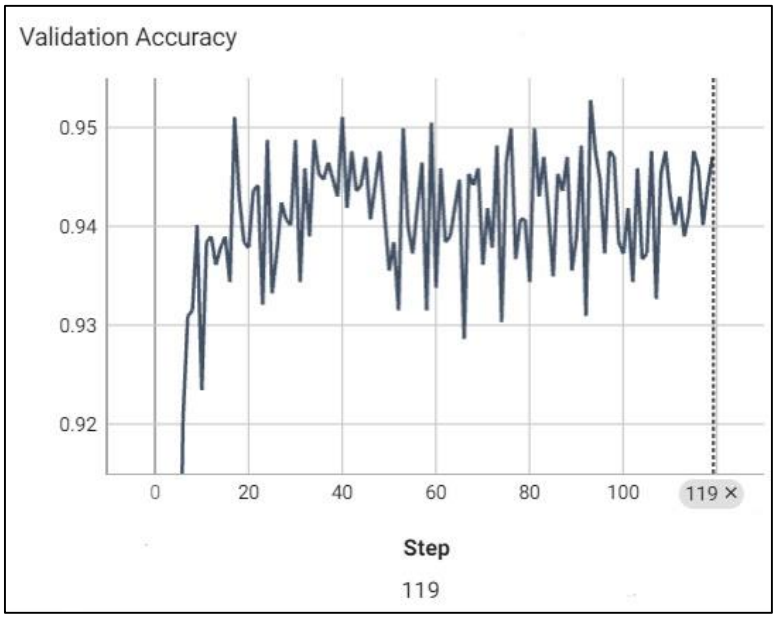
Şekil 5.1. grafiğinde Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 modeline ait eğitim kayıp oranı, şekil 5.2. grafiğinde Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 eğitim doğruluk oranı gösterilmiştir. Şekil 5.3. grafiğinde Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme doğruluk oranı, şekil 5.4. grafiğinde Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme kayıp oranı gösterilmiştir. Eğitim ve değerlendirme kayıp ile doğruluk oranı grafikleri incelendiğinde değerlendirme kayıp ve doğruluk oranı grafiklerinin daha değişken, zikzaklı yapıdadır. Bu durumda model eğitim verisi, modelde ezberlenerek daha formal, şişen eğriye yaklaşırken değerlendirme verisi overfitting sonucu daha zikzaklı, tutarsız eğriye yaklaşmaktadır. Bağlantılı model eğitimi, zikzaklı eğri çizerek öngörülemeyen değerlendirme verisine genellemekte zorlanmaktadır. Eğitim verisinin overfitting durumu, değerlendirme (validasyon) verisine yansımaktadır.



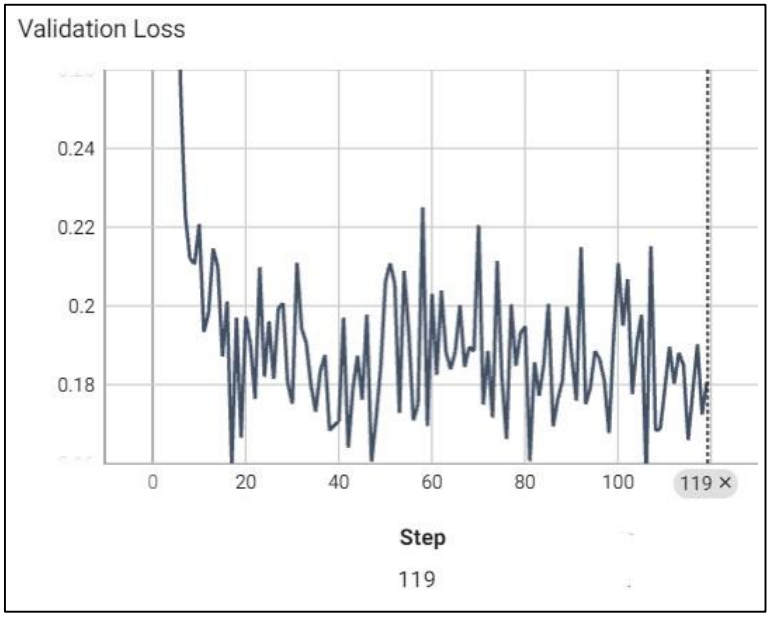
Şekil 5.1. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 eğitim kayıp oranı



Şekil 5.2. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 eğitim doğruluk oranı



Şekil 5.3. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme (validasyon) doğruluk oranı



Şekil 5.4. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 değerlendirme (validasyon) kayıp oranı

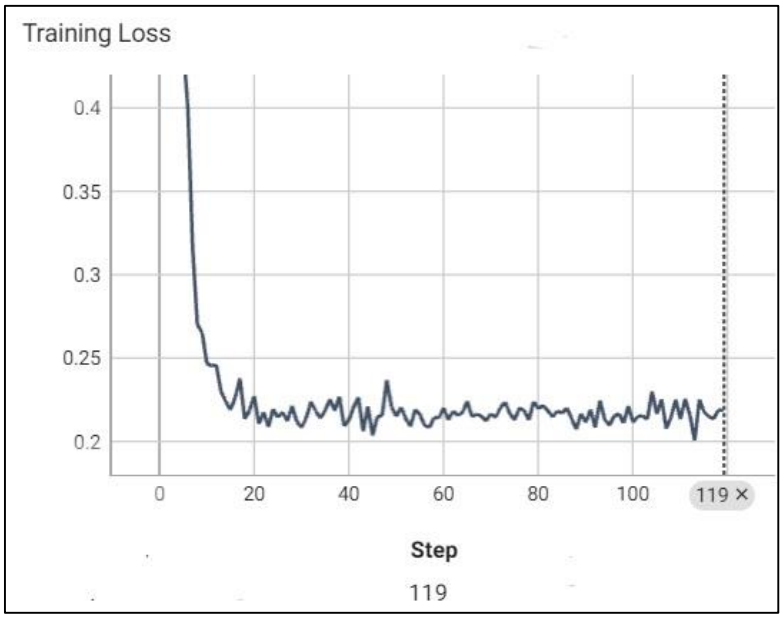
Şekil 5.5. figüründe Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 konfüzyon matrisi gösterilmiştir. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 konfüzyon matrisi incelendiğinde en düşük doğruluk değeri Simda sınıfında görülürken en yüksek doğruluk oranları Kelihos_ver1 ve

Kelihos_ver3 sınıflarında görülmektedir. Özellikle Simda sınıfının daha düşük doğruluk oranına sahip olması, Simda sınıfına ait verinin yetersizliğindendir.

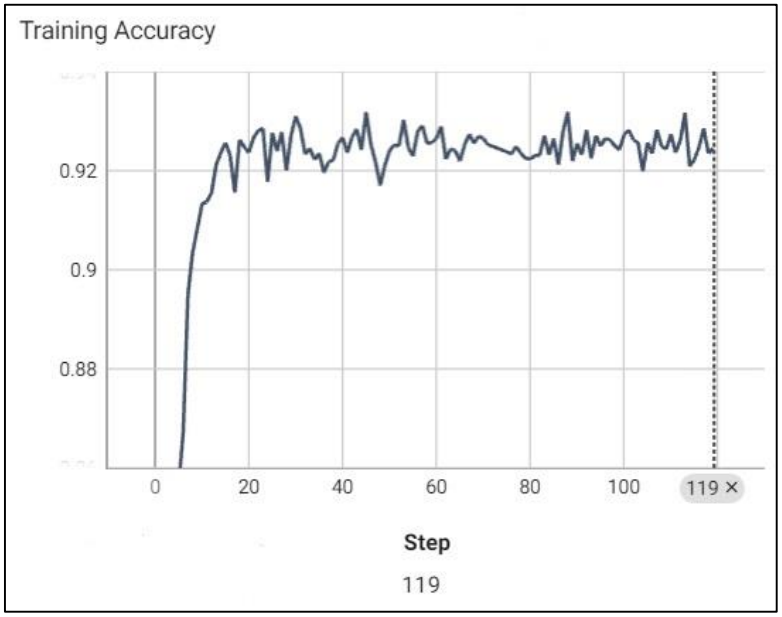


Şekil 5.5. Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b7 konfüzyon matrisi

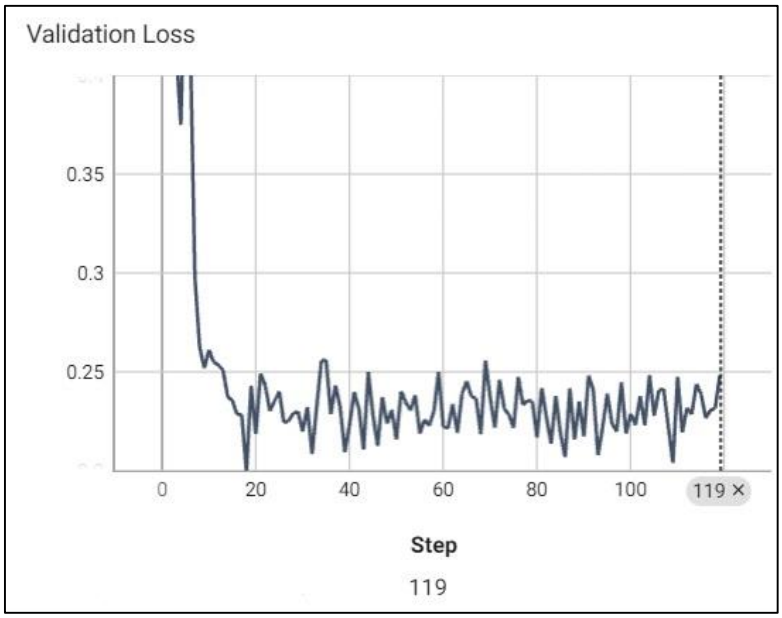
Şekil 5.6. grafiğinde Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim kayıp oranı ve şekil 5.7. grafiğinde Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim doğruluk oranı gösterilmektedir. Şekil 5.8. grafiğinde Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme kayıp oranı, şekil 5.9. grafiğinde Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme doğruluk oranı gösterilmiştir. Eğitim ve değerlendirme kayıp ile doğruluk oranı grafikleri incelendiğinde değerlendirme kayıp ve doğruluk oranlarının eğitim kayıp ile doğruluk oranlarına göre daha zikzaklı, tutarsız olduğu görülmektedir. Bu durum eğitim verisine ait overfitting probleminin değerlendirme verisinde zikzaklı eğriye dönüştürmektedir. RGB malware görüntüleri, gri tonlamalı malware görüntülerine kıyasla daha az zikzak eğrisine sahiptir.



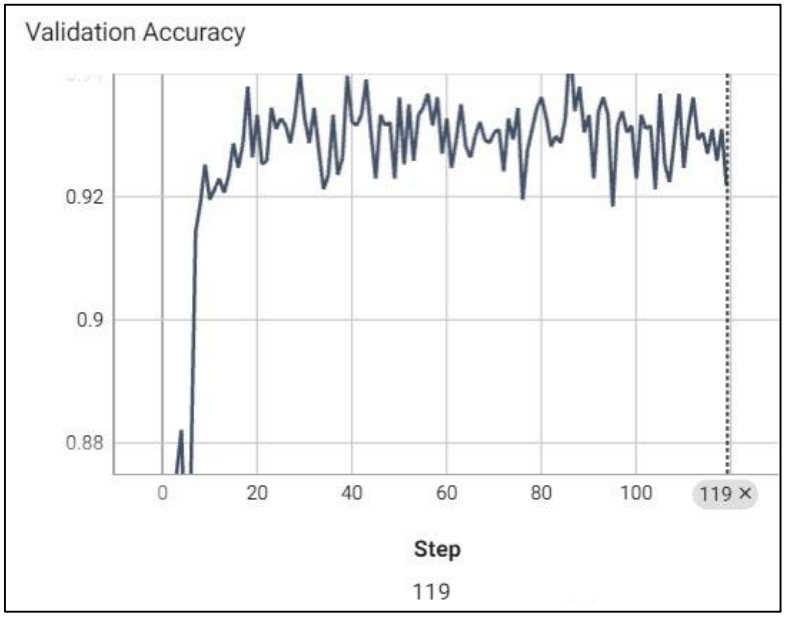
Şekil 5.6. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim kayıp oranı



Şekil 5.7. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 eğitim doğruluk oranı



Şekil 5.8. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme (validasyon) kayıp oranı



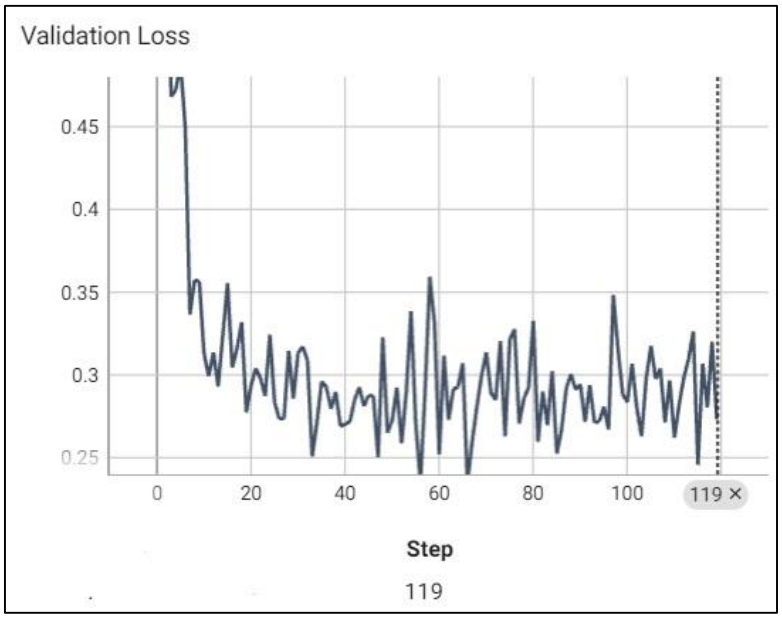
Şekil 5.9. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 değerlendirme (validasyon) doğruluk oranı

Şekil 5.10. gösteriminde Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisi incelendiğinde en düşük doğruluk değeri Simda sınıfına aitken en yüksek doğruluk oranı Kelihos_ver3 sınıfına aittir. Bu durum veri dağılımındaki dengesizlikten kaynaklanmaktadır.

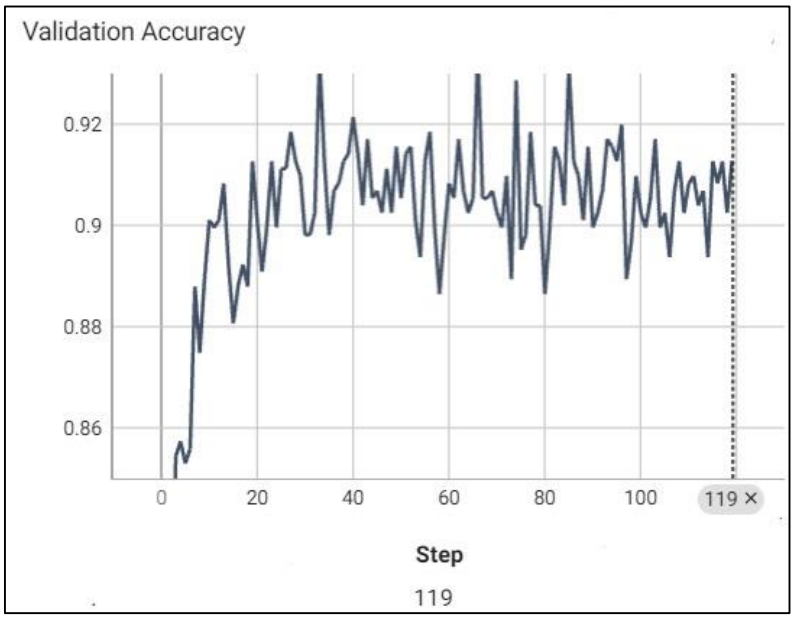


Şekil 5.10. Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisi

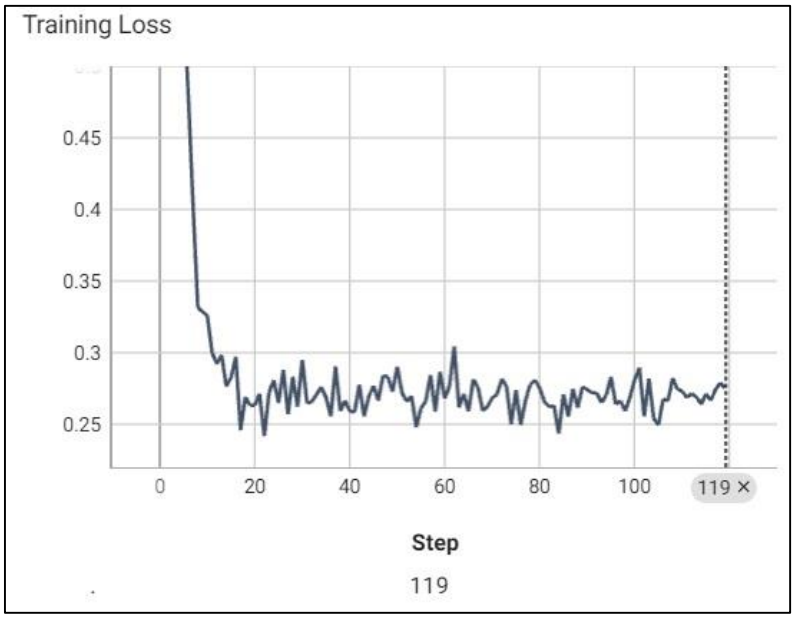
Şekil 5.11. grafiğinde Dumpware10 EfficientNet-b6 değerlendirme (validasyon) kayıp oranı gösterilmektedir ve şekil 5.12. grafiğinde Dumpware10 EfficientNet-b6 değerlendirme (validasyon) doğruluk oranı gösterilmektedir. Şekil 5.13. grafiğinde Dumpware10 EfficientNet-b6 eğitim kayıp oranı, şekil 5.14. grafiğinde Dumpware10 EfficientNet-b6 eğitim doğruluk oranı gösterilmiştir. Değerlendirme doğruluk ile kayıp oranı ve eğitim doğruluk ile kayıp oranı grafikleri incelendiğinde eğitim verisinin overfitting doygunluğuna ulaştığı ve paralelinde değerlendirme verisinin zikzak eğrileriyle genellemede zorluk yaşadığını göstermektedir. Model eğitiminde batch parçaları gradyan döngüsünde malware görüntü karakteristiklerini öğrenememektedir. Bu durum değerlendirme (validasyon) verisinde zikzaklı eğriler oluşturmaktadır.



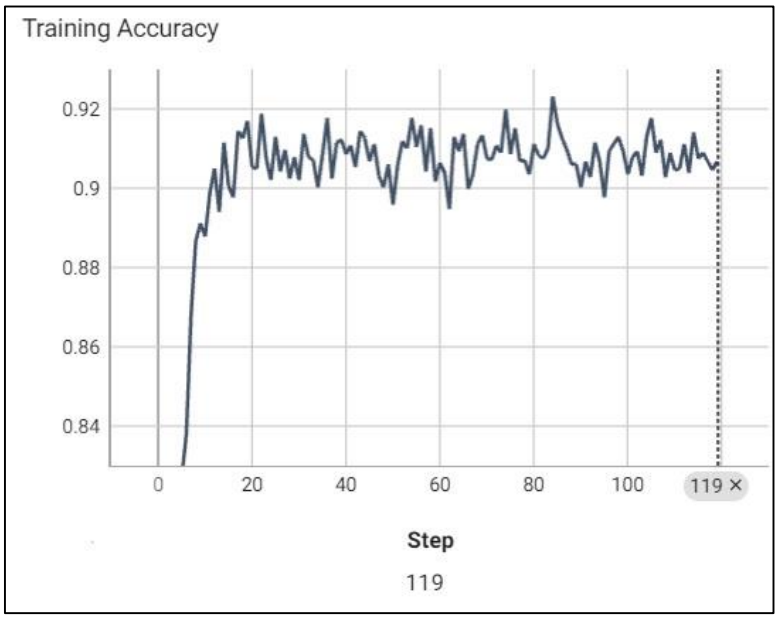
Şekil 5.11. Dumpware10 EfficientNet-b6 değerlendirme kayıp oranı



Şekil 5.12. Dumpware10 EfficientNet-b6 değerlendirme doğruluk oranı

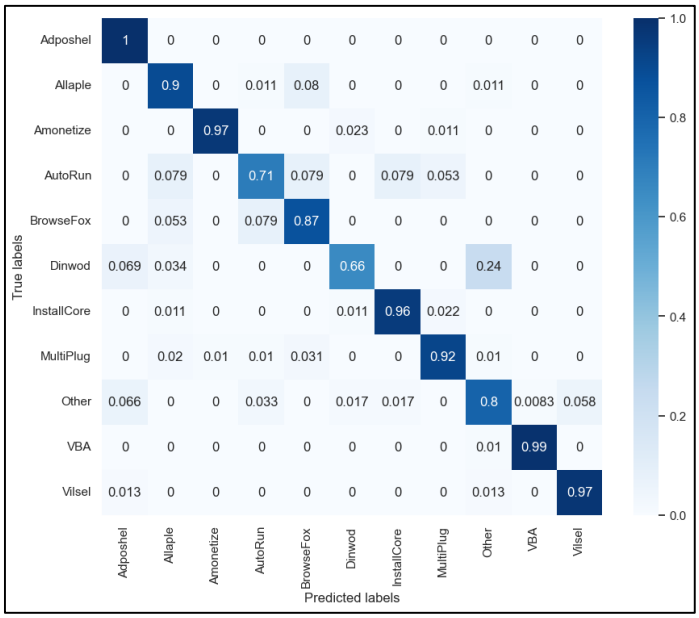


Şekil 5.13. Dumpware10 EfficientNet-b6 eğitim kayıp oranı



Şekil 5.14. Dumpware10 EfficientNet-b6 eğitim doğruluk oranı

Şekil 5.15. gösteriminin Dumpware10 EfficientNet-b6 konfüzyon matrisinde en düşük doğruluk oranı Dinwod sınıfına aitken en yüksek doğruluk oranı Adposhel ve VBA sınıflarına aittir. Bu durum sınıflar arası veri dağılımının dengesizliğinden kaynaklanmaktadır.



Şekil 5.15. Dumpware10 EfficientNet-b6 konfüzyon matrisi

5.1.1. Maxpooling deneyi

Transfer learning approach for malware classification araştırma çalışmasında konvolüsyonel sinir ağı tabanlı transfer learning uygulaması (TL-CNN), Android malware görüntü verilerinin sınıflandırmasında yararlanılmıştır ve transfer learning uzanımında eğitilen konvolüsyonel sinir ağı mimarisi, iyi huylu görüntü verileri ve zararlı malware görüntü verileri arasındaki ayrışımı üstenmiştir. Bağlantılı araştırma çalışmasına ait transfer learning uzanımında önceden eğitilen ResNet-50 sınıflandırma (classifier) bileşeni, özgün sınıflandırma bileşeniyle değiştirilmiştir, bağlantılı sınıflandırma bileşeni ImageNet veri setine ait 1000 görüntü sınıfını kaldırarak 25 malware sınıfını içeren fully-connected katmanını bütünleştirmiştir. Transfer learning uzanımına ait ResNet-50 modellemesinin ardından padding dolgulu, (2x2) çekirdek filtre boyutlu ve 2 adımlı (stride) MaxPooling katmanı, sınıflandırma bileşenin fully-connected katmanından önce getirilmiştir. Fully-connected katmanı ve Softmax fonksiyonu en son malware sınıflandırmasını gerçekleştirmiştir [20].

Bu araştırma kapsamında bahsi geçen transfer learning approach for malware images classification araştırma çalışmasına dayanarak EfficientNet mimarisine ait “feature” öznitelik çıkarımı bloğunun en son Global Average Pooling katmanı MaxPooling katmanıyla değiştirilerek Flatten, Dropout ve Linear fully-connected katmanı içeren

“classifier” sınıflandırıcısına bağlanmıştır. EfficientNet mimarisi, (7x7) çekirdek boyutlu ve 1 adımlı MaxPooling katmanına uyarlanabilmektedir. Global Average Pooling katmanı var olan görüntü örneğine ait çekirdek filtre boyutlu piksel alanlarını adımlayarak görüntü piksel değerlerine evrensel ortalama uygulamaktadır ve çekirdek filtre boyutlu piksel alanlarına ait evrensel ortalama değerlerini yeni çekirdek piksel alanında birleştirmektedir. MaxPooling katmanı, var olan görüntü örneğine ait çekirdek filtre boyutlu piksel alanlarını adımlayarak görüntü piksel değerlerine ait değer ağırlıklarını kullanmaktadır ve çekirdek filtre boyutlu piksel alanlarına ait en yüksek piksel değerlerini yeni çekirdek piksel alanında birleştirmektedir. EfficientNet mimarisinin classifier sınıflandırıcısı, (1x1) düzlem boyutlu girdi istemektedir ve EfficientNet mimarisi, (2x2) çekirdek filtre boyutlu ve 2 adımlı MaxPooling ayarlamasını karşılamamaktadır.

MaxPooling katmanıyla bütünleşen EfficientNet-b7 (Microsoft Malware Classification Challenge Gri tonlamalı) ve EfficientNet-b5 (Microsoft Malware Classification Challenge RGB) EfficientNet-b6 (Dumpware10 RGB) mimarileri 0,01 öğrenme oranlı SGD optimizasyonunda 120 epoch eğitim döngüsüne tabi tutulmuştur.

Çizelge 5.12. sonuçlarında MaxPooling EfficientNet model eğitimlerinden EfficientNet-b5 (RGB), en yüksek değerlendirme doğruluk oranına sahiptir. MaxPooling değişimi gerçekleştiğinde üç kanallı RGB malware görüntüleri, gri tonlamalı malware görüntülerine göre daha yüksek değerlendirme doğruluk oranı çıkarmıştır.

Çizelge 5.12. MaxPooling EfficientNet model eğitimlerine ait değerlendirme (validasyon) doğruluk oranları

malware görüntü türü	Model mimarisi	Öğrenme oranı	Optimizasyon türü	Doğruluk oranı
Gri tonlamalı malware	EfficientNet-b7	0,01	SGD	0,918250
RGB malware	EfficientNet-b5	0,01	SGD	0,926394
RGB malware	EfficientNet-b6	0,01	SGD	0,903930

Çizelge 5.13. sonuçlarında değerlendirme (validasyon) doğruluk oranlarının tersine EfficientNet-b7 (Gri tonlamalı), en yüksek test doğruluk oranına sahiptir. EfficientNet-b7

precision değerinin recall değerinden yüksek olması, modelin total doğru sınıf çıkarımında doğru sınıf eşleşmesinin yüksekliğini göstermektedir.

Çizelge 5.13. MaxPooling EfficientNet model test doğruluk, F1-score, recall ve precision sonuçları

Model	Görüntü kanalı	Öğrenme oranı	Optimizasyon türü	Test doğruluk	F1-score	Recall	Precision
EfficientNet-b7	Gri tonlamalı	0,01	SGD	90%	0,8529	0,8434	0,8893
EfficientNet-b5	RGB	0,01	SGD	89%	0,8288	0,8407	0,8207
EfficientNet-b6	RGB	0,01	SGD	88%	0,8299	0,8275	0,8469

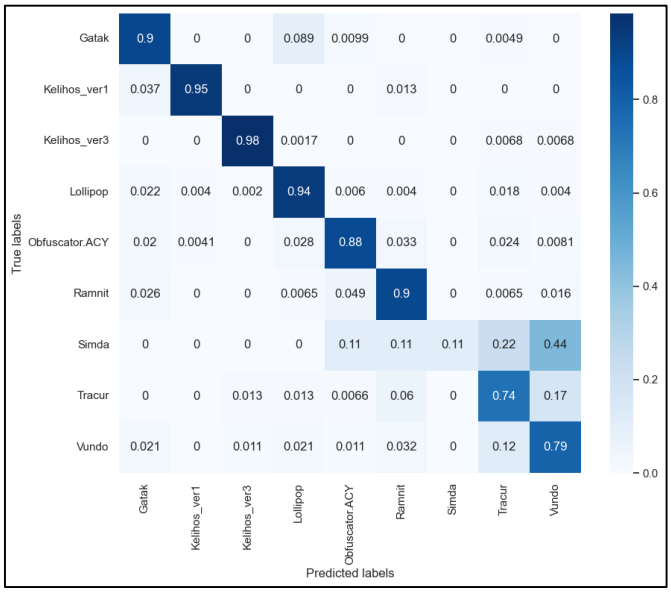
Şekil 5.16. gösteriminin MaxPooling EfficientNet-b5 Microsoft Malware Classification Challenge (RGB) konfüzyon matrisinde en yüksek doğruluk oranı Kelihos_ver3 sınıfına aitken en düşük doğruluk oranı Simda sınıfına aittir. Bu durum sınıflar arası veri dengesizliğinden kaynaklanmaktadır, Simda sınıfına ait veri donanımı oldukça zayıftır.



Şekil 5.16. MaxPooling EfficientNet-b5 Microsoft Malware Classification Challenge (RGB) konfüzyon matrisi

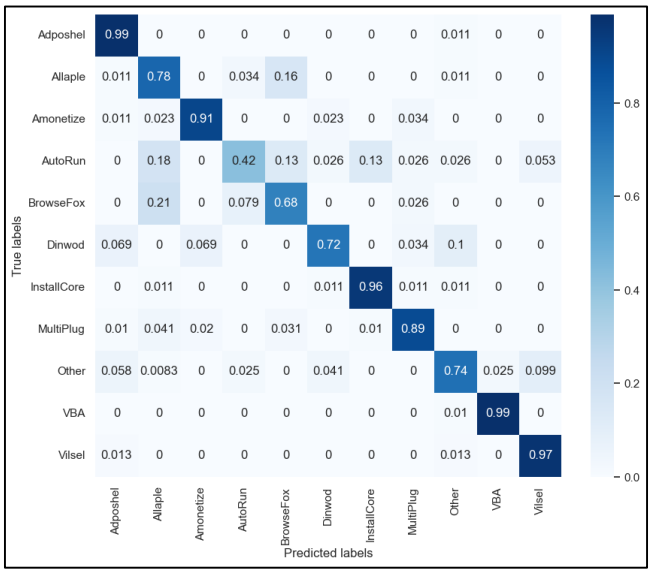
Şekil 5.17. gösteriminin MaxPooling EfficientNet-b7 Microsoft Malware Classification Challenge (Gri tonlamalı) konfüzyon matrisinde Simda sınıfına ait doğruluk oranı en

düşükken Kelihos_ver3 sınıfına ait doğruluk oranı en yüksektir. Simda sınıfında olumsuz eşleşme kaymaları görülmektedir ve bu durum doğruluk oranını kırmaktadır.



Şekil 5.17. MaxPooling EfficientNet-b7 Microsoft Malware Classification Challenge (Gri tonlamalı) konfüzyon matrisi

Şekil 5.18. gösteriminde MaxPooling EfficientNet-b6 Dumpware10 (RGB) konfüzyon matrisinde en yüksek doğruluk oranı, VBA sınıfına aitken en düşük doğruluk oranı AutoRun sınıfına aittir. Dumpware10 malware görüntülerinin sınıflar arası dengesiz dağılımı, doğruluk oranlarını etkilemektedir.



Şekil 5.18. MaxPooling EfficientNet-b6 Dumpware10 (RGB) konfüzyon matrisi

MaxPooling deney sonuçlarında Transfer Learning deneyine ait EfficientNet-b7 (Gri tonlamalı) uzanımının en yüksek başarı performansına sahip olduğu görülmektedir. MaxPooling deneyi, özellikle test doğruluk oranlarında gözle görülür bir iyileşme sunmamıştır ve EfficientNet mimarisine ait GlobalAveragePooling katmanı, MaxPooling katmanına göre daha başarılı sonuçlar çıkarmıştır.

5.1.2. CORAL kayıplı dynamic distribution adaptation network deneyi

CORAL transfer learning algoritması, domain adaptation altında veri kümesinin source domain ve target domain ayrımlarını kullanmaktadır. Dumpware10, Microsoft Malware Classification Challenge (RGB) ve Microsoft Malware Classification Challenge (Gri tonlamalı) veri kümeleri 60% oranla source domain ve 40% oranla target domain alanlarına ayrılmaktadır. Ardından source domain ve target domain alanlarını 20% oranla test ve validasyon (değerlendirme) ayrımlarını "test domain" ve "validasyon" domain alanlarına aktarmaktadır. Veri kümelerine ait source domain, target domain ve validasyon domain alanları CORAL transfer learning algoritmasının domain ayrışım mantığında CORAL kayıplı Dynamic Distribution Adaptation Network eğitimine katılmaktadır.

Dynamic Distribution Adaptation Network uzanımında backbone derin sinir ağı (ResNet) bu araştırma çalışmasının EfficientNet mimarisiyle değiştirilmektedir. Dumpware10 domain alan verileri EfficientNet-b6, Microsoft Malware Classification Challenge RGB domain alan verileri EfficientNet-b5 ve Microsoft Malware Classification Challenge gri tonlamalı domain alan verileri EfficientNet-b6 mimarilerine girilmektedir. EfficientNet mimarilerinin eğitim döngüsü EarlyStopping destekli ve 0,01 öğrenme oranlı SGD optimizasyonuna sahiptir. Batch parça boyutu 16 değerindedir. Dynamic Distribution Adaptation Network Backbone mimarisine bottleneck katmanı eklenmiştir ve başarı performansını iyileştirmiştir. Dynamic Distribution Adaptation Backbone mimarisi, source domain ve target domain alanlarına ait CORAL kaybını, transfer kaybına tanımlarken CrossEntropy kaybını classification kaybına tanımlamaktadır ve transfer kaybı ve classification kaybı toplamını total kayıp değerine atamaktadır. Dynamic Distribution Adaptation eğitim döngüsünde source domain ve target domain alanları birbirine yaklaşmaktadır, transfer kaybı azalmaktadır.

Çizelge 5.14. sonuçlarında Microsoft Malware Classification Challenge gri tonlamalı EfficientNet-b6 backbone modeli en yüksek validasyon domain doğruluk oranına sahiptir.

Çizelge 5.14. CORAL kayıplı Dynamic Distribution Adaptation Network değerlendirme (validasyon) doğruluk oranları

Malware veri kümesi	Malware görüntü türü	Backbone model	Validasyon doğruluk oranı
Microsoft Malware Classification Challenge	Gri tonlamalı	EfficientNet-b6	0,9706
Microsoft Malware Classification Challenge	RGB	EfficientNet-b5	0,9442
Dumpware10	RGB	EfficientNet-b6	0,9663

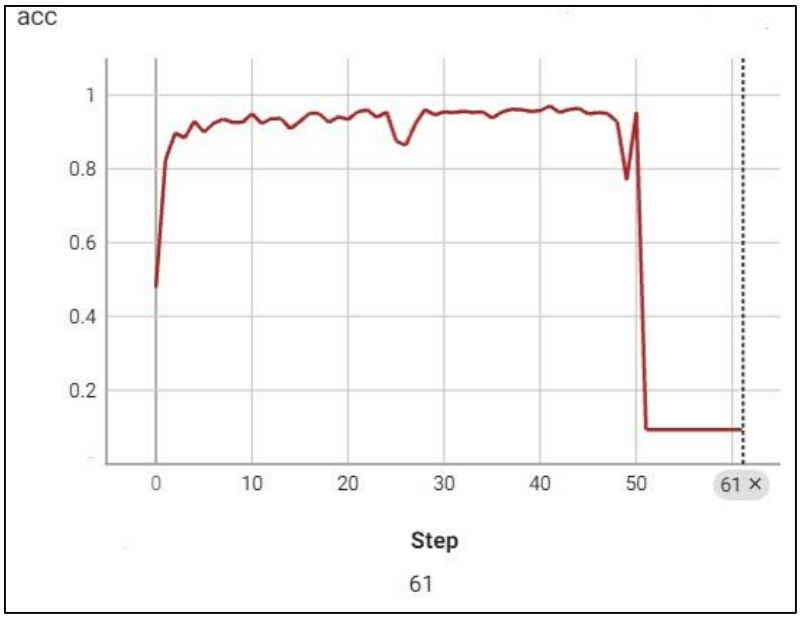
Çizelge 5.15. sonuçlarına ait test domain doğruluk oranı, precision, recall, F1-score metriklerinde en başarılı sonuçlar Dumpware10 RGB EfficientNet-b6 modeline aittir.

Çizelge 5.15. CORAL kayıplı Dynamic Distribution Adaptation Network test sonuçları

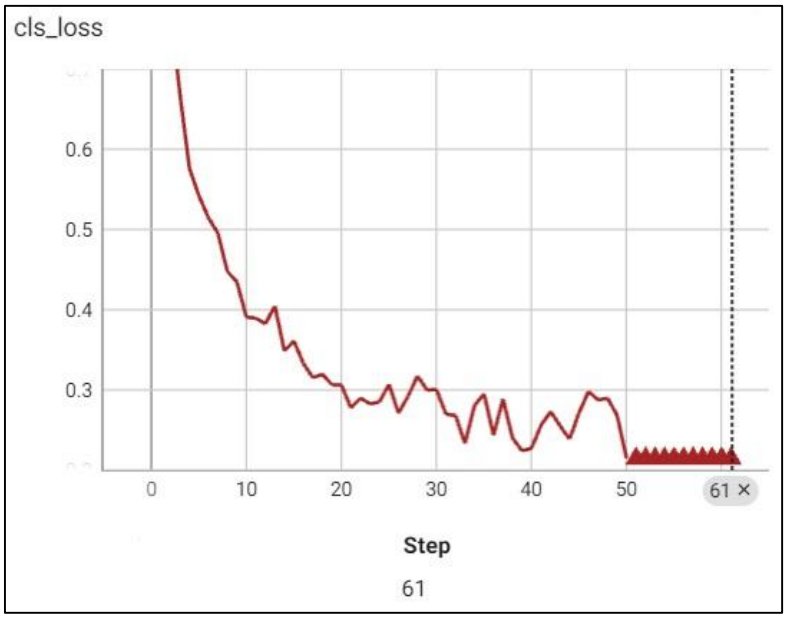
Malware veri kümesi	Malware görüntü türü	Backbone model	Test doğruluk oranı	Precision	Recall	F1-score
Microsoft Malware Classification Challenge	Gri tonlamalı	EfficientNet-b6	0,95854	0,9009	0,8554	0,8647
Microsoft Malware Classification Challenge	RGB	EfficientNet-b5	0,95257	0,9484	0,8478	0,8596
Dumpware10	RGB	EfficientNet-b6	0,96064	0,9460	0,9556	0,9491

Şekil 5.19. grafiğinde CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 validasyon

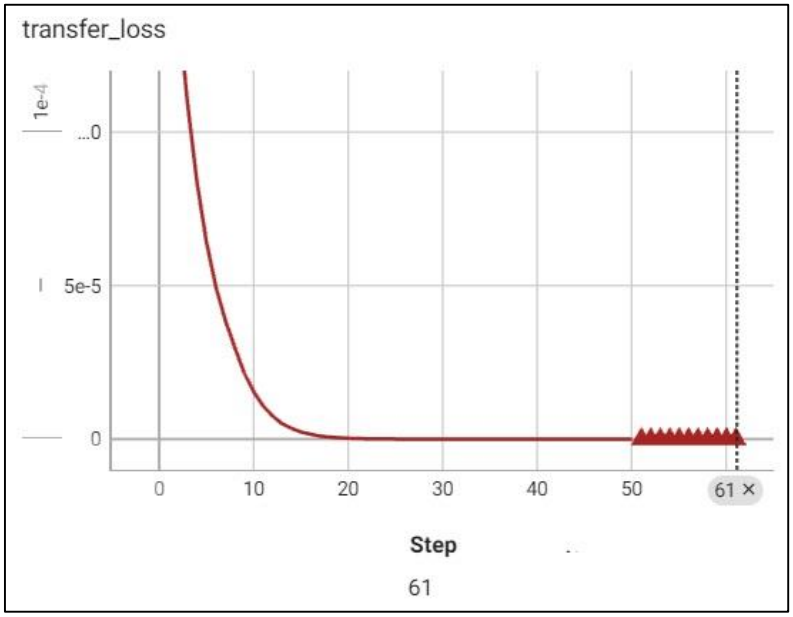
doğruluk oranı gösterilirken şekil 5.20. grafiğinde CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 classification kaybı gösterilmektedir. Şekil 5.21 ve şekil 5.22. grafiklerinde sırasıyla CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 transfer kayıp oranı ve total kayıp oranını göstermektedir. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 grafikleri incelendiğinde validasyon doğruluk oranı grafiklerinin daha düşük dereceli zikzak değişimlerine sahip olduğu görülmektedir. Bu durum eğitim tutarlılığını göstermektedir. Yalnız anında düşen doğruluk oranı çizgisi, model anomalisine işaret etmektedir. EarlyStopping mekanizması, ilgili model anomalisini aşarak en yüksek doğruluk oranlı noktada model ağırlıklarını önceden kaydetmektedir. Model ağırlığı, ani doğruluk oranı düşüşlerinden etkilenmemektedir.



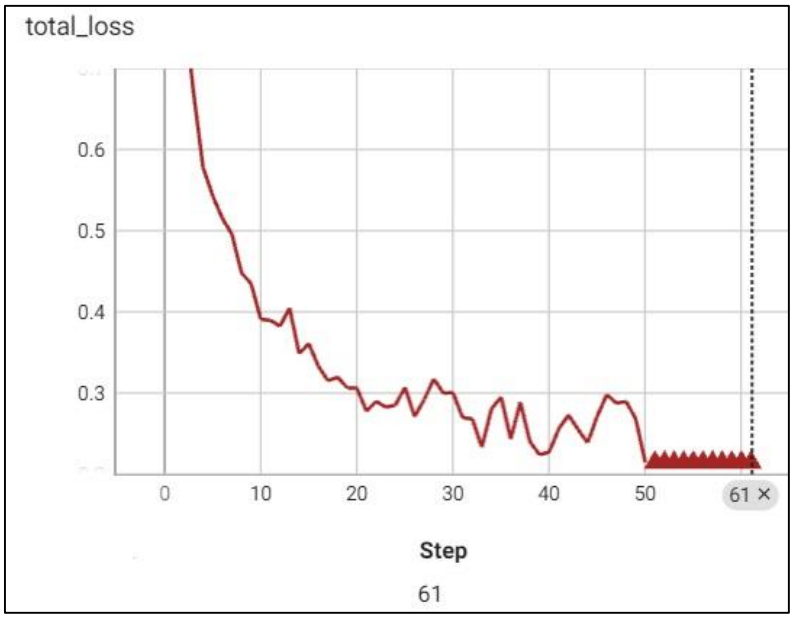
Şekil 5.19. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 validasyon doğruluk oranı



Şekil 5.20. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 classification kayıp oranı

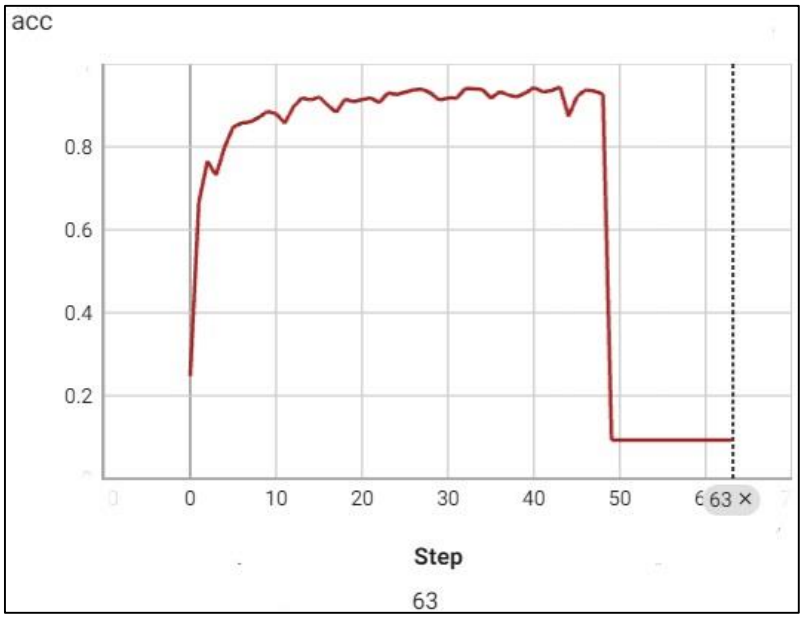


Şekil 5.21. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 transfer kayıp oranı

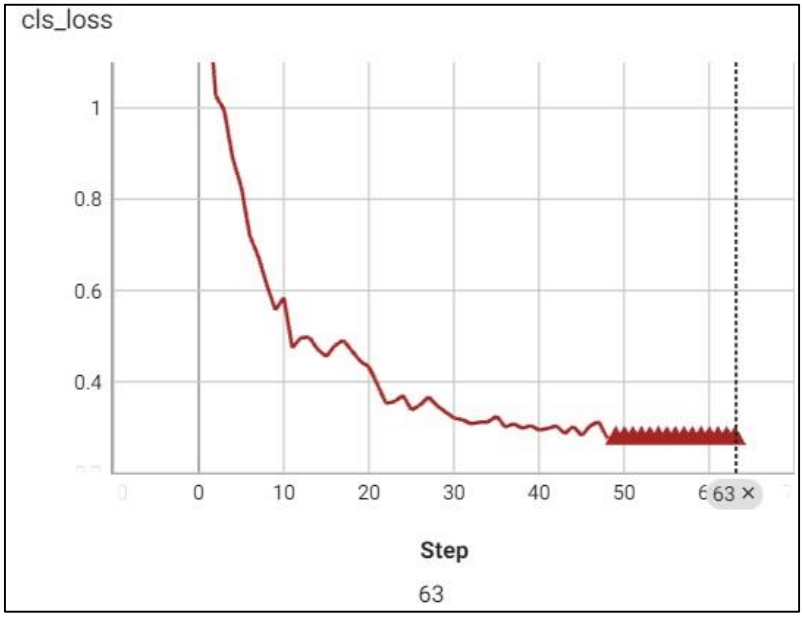


Şekil 5.22. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 total kayıp oranı

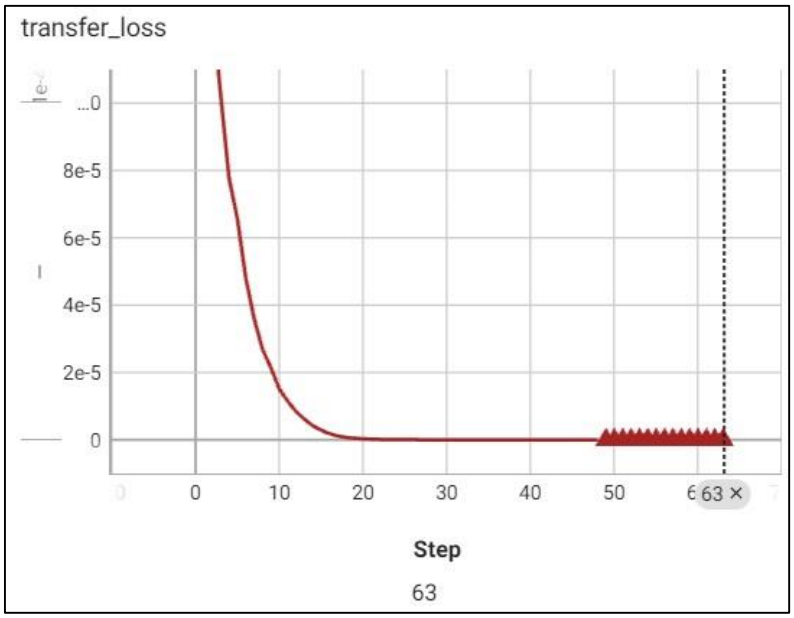
Şekil 5.23. grafiğinde CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 validasyon doğruluk oranı gösterilirken şekil 5.24. grafiğinde CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 classification kaybı gösterilmektedir. Şekil 5.25. ve şekil 5.26. grafiğinde sırasıyla CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 transfer kayıp oranı ve total kayıp oranı gösterilmiştir. CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 grafikleri incelendiğinde validasyon doğruluk oranındaki zikzak dalgalanmalarının geçmiş deneylere kıyasla azaldığı görülmektedir. Ayrıca ani validasyon doğruluk oranı düşüşü model anomalisidir. Yalnız EarlyStopping mekanizması en yüksek validasyon doğruluk oranına sahip model ağırlıklarını önceden kaydetmektedir. Model ağırlıkları ani validasyon doğruluk oranı düşüşlerinden etkilenmemektedir.



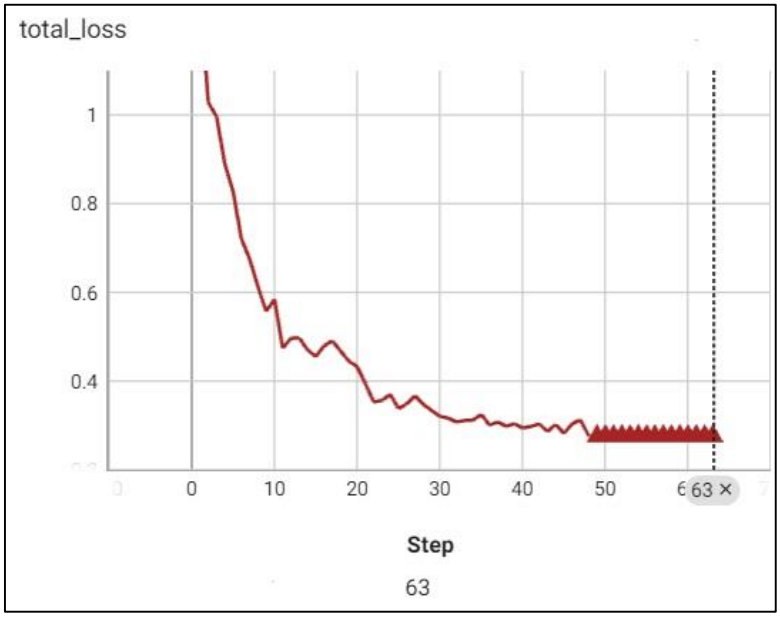
Şekil 5.23. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 validasyon doğruluk oranı



Şekil 5.24. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 classification kayıp oranı



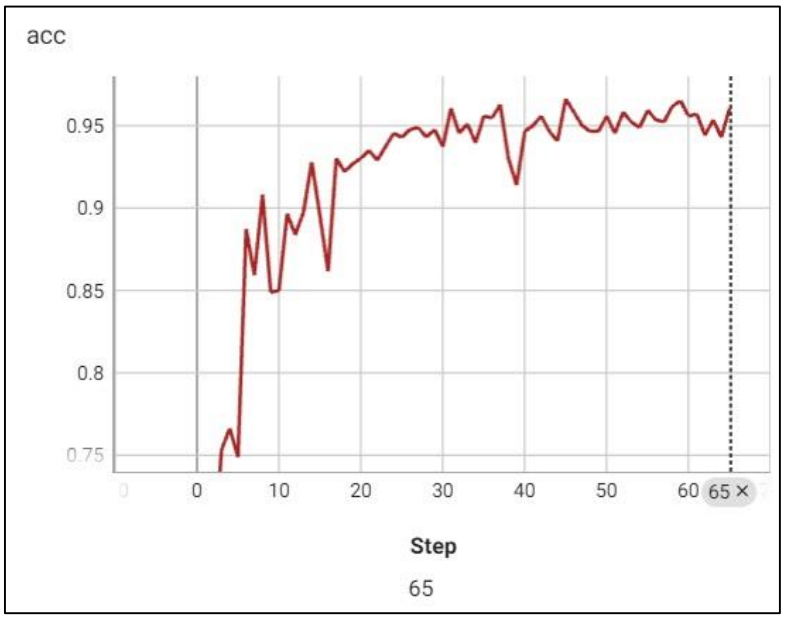
Şekil 5.25. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 transfer kayıp oranı



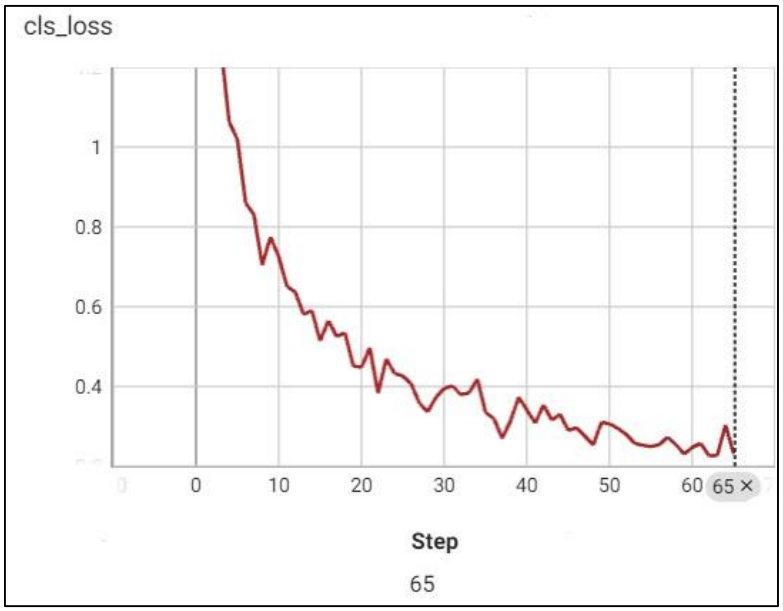
Şekil 5.26. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 total kayıp oranı

Şekil 5.27. grafiğinde CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Dumpware10 EfficientNet-b6 validasyon doğruluk oranı gösterilirken şekil 5.28. grafiğinde Dynamic Distribution Adaptation Network deneyinin Dumpware10 EfficientNet-b6 classification kaybı gösterilmektedir. Şekil 5.29. ve şekil 5.30. grafiğinde sırasıyla CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Dumpware10 EfficientNet-b6

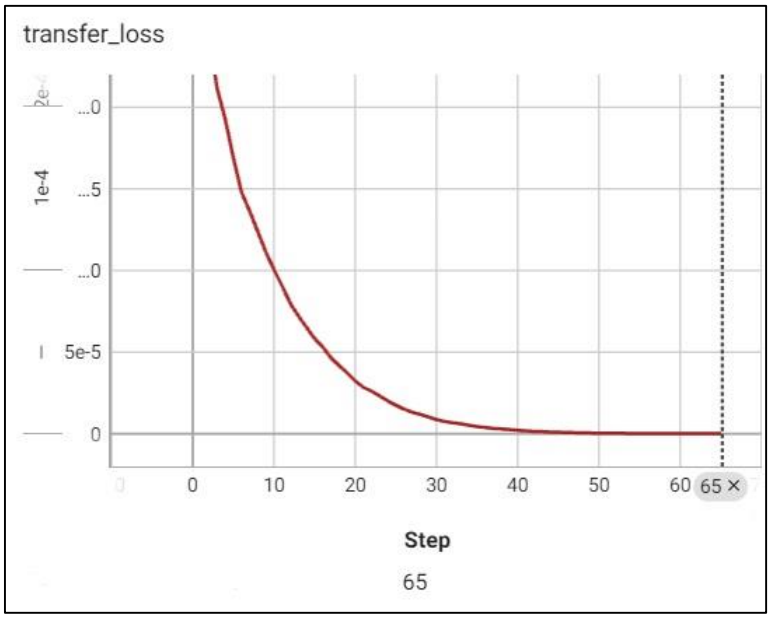
transfer kaybı ve total kaybı gösterilmiştir. CORAL kayıplı Dynamic Distribution Adaptation Network deneyinin Dumpware10 grafikleri incelendiğinde validasyon doğruluk oranlarında daha az dalgalanmalara -CORAL kayıplı Dynamic Distribution Adaptation Network deneyleri hariç- rastlanmaktadır. CORAL kayıplı Dynamic Distribution Adaptation Network Dumpware10 EfficientNet-b6 deneyinde ani doğruluk oranı düşüşü yaşanmamıştır.



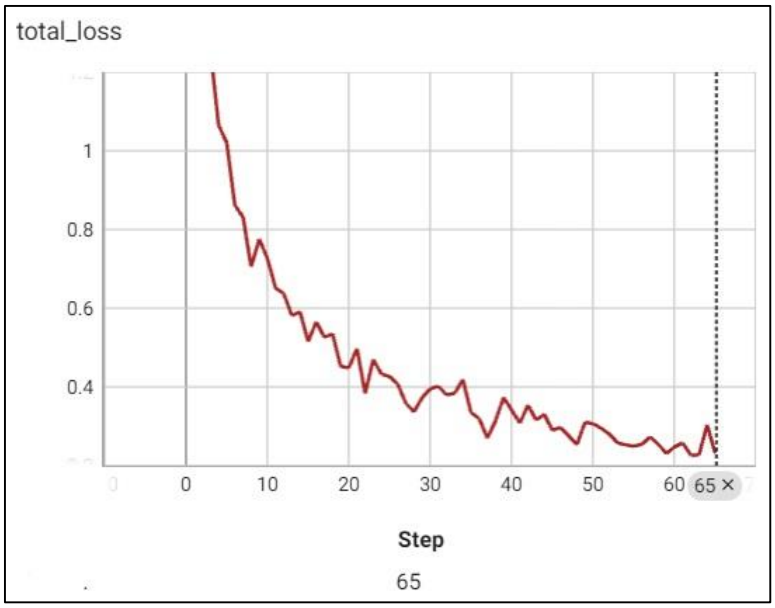
Şekil 5.27. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 validasyon doğruluk oranı



Şekil 5.28. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 classification kayıp oranı

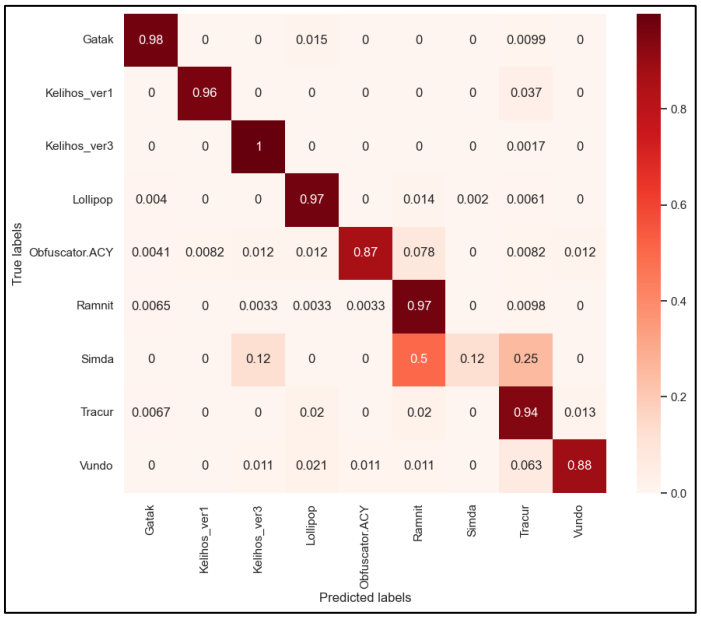


Şekil 5.29. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 transfer kayıp oranı



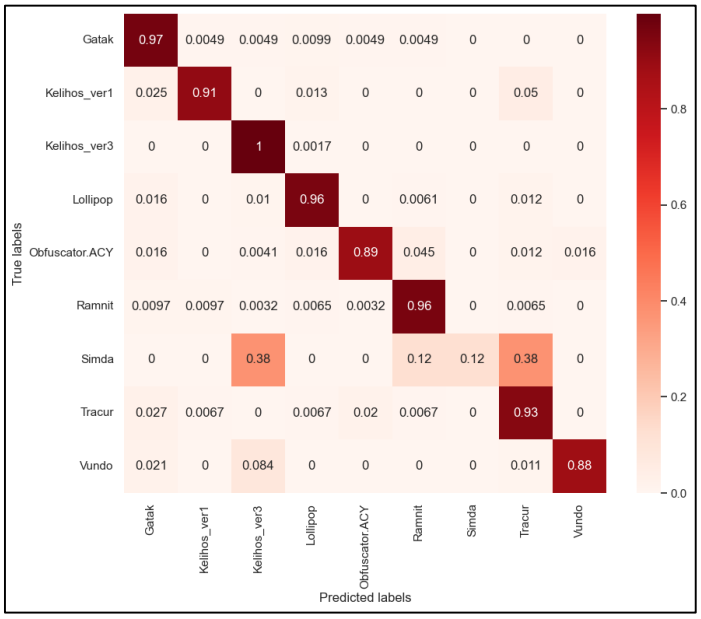
Şekil 5.30. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 total kayıp oranı

Şekil 5.31. gösteriminin CORAL kayıplı Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 konfüzyon matrisi incelendiğinde en yüksek doğruluk oranı Kelihos_ver3 ve en düşük doğruluk oranı Simda sınıfındadır.



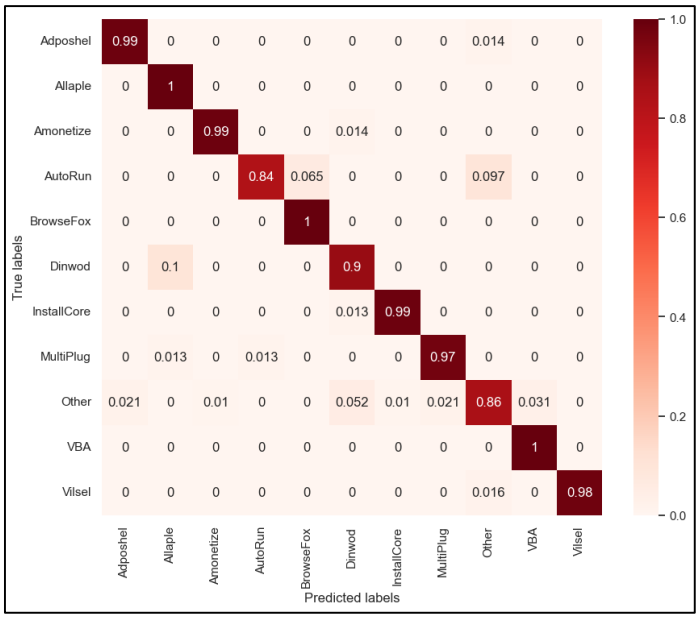
Şekil 5.31. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (Gri tonlamalı) EfficientNet-b6 konfüzyon matrisi

Şekil 5.32. gösteriminin CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisinde Kelihos_ver3 en yüksek doğruluk oranına sahipken Simda en düşük doğruluk oranına sahiptir.



Şekil 5.32. CORAL kayıplı DDAN Microsoft Malware Classification Challenge (RGB) EfficientNet-b5 konfüzyon matrisi

Şekil 5.33. gösterimine ait CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 konfüzyon matrisi incelendiğinde Allaple, BrowseFox ve VBA sınıflarının en yüksek doğruluk oranlarına sahip olduğu görülürken AutoRun sınıfının en düşük doğruluk oranına sahip olduğu görülmektedir.



Şekil 5.33. CORAL kayıplı DDAN Dumpware10 EfficientNet-b6 konfüzyon matrisi

Çizelge 5.16. araştırmada yürütülen Transfer Learning ve MaxPooling deneylerinin en yüksek performans metrikleri özetlenmektedir. Deneylerde EfficientNet modellerinin (EfficientNet-b5, b6 ve b7) gri tonlamalı ve RGB malware görüntülerine uygulanarak malware sınıflandırmasına odaklanılmıştır. Değerlendirme için Microsoft Malware Classification Challenge (MMCC) ve Dumpware10 veri kümeleri kullanılmıştır. Çizelge test doğruluk oranı, F1-score, recall, precision ve validasyon doğruluk oranı metriklerine sahiptir. Transfer learning deneyinde EfficientNet-b7 (Gri tonlamalı) en yüksek validasyon değerlendirme doğruluk oranına (95,27%) sahiptir, güçlü test doğruluk oranı (93%) ve precision değeri (88,15%) yanındadır. Dumpware10 veri kümesinde EfficientNet-b6 (RGB), transfer learning ve DDAN deneylerinde en başarılı test doğruluk oranı (96%) ve güçlü precision değeri (94,60%) yakalamıştır, ek olarak 96,63% validasyon doğruluk oranı mevcuttur. MaxPooling deneyleri, EfficientNet-b7 (Gri tonlamalı) modelinde 90% test doğruluk oranıyla transfer learning deneylerine kıyasla daha düşük sonuç göstermiştir. DDAN yaklaşımı, test ve validasyon doğruluk metriklerini RGB ve gri tonlamalı malware

görüntülerinde iyileştirmiştir, özellikle Dumpware10 veri kümesinde gözle görülür gelişme sergilemiştir.

Çizelge 5.16. Transfer Learning, MaxPooling ve DDAN deneylerinin en başarılı sonuçları

Transfer Learning	Model	Görüntü Türü	Test doğruluk	F1 Score	Recall	Precision	Validasyon doğruluk
MS	EfficientNet-b7	Gri tonlamalı	0,93	0,8963	0,9163	0,8815	0,952792
	EfficientNet-b5	RGB	0,91	0,8646	0,8777	0,8550	0,9447796
Dumpware10	EfficientNet-b6	RGB	0,91	0,8786	0,8843	0,8811	0,934498
MaxPooling							
MS	EfficientNet-b7	Gri tonlamalı	0,90	0,8529	0,8434	0,8893	0,918250
	EfficientNet-b5	RGB	0,89	0,8288	0,8407	0,8207	0,926394
Dumpware10	EfficientNet-b6	RGB	0,88	0,8299	0,8275	0,8469	0,903930
DDAN							
MS	EfficientNet-b6	Gri tonlamalı	0,95854	0,8647	0,8554	0,9009	0,9706
	EfficientNet-b5	RGB	0,95257	0,8596	0,8478	0,9484	0,9442
Dumpware10	EfficientNet-b6	RGB	0,96064	0,9491	0,9556	0,9460	0,9663

Çizelge 5.17. birtakım deneysel araştırma sonuçlarını Transfer learning, MaxPooling ve Dynamic Distribution Adaptation Network (DDAN) deneylerini ekleyerek karşılaştırmaktadır. Transfer learning deneyinde EfficientNet-b7 (Gri tonlamalı) modeli, Microsoft Malware Classification Challenge veri kümesi için en yüksek validasyon doğruluk oranını (95,27%) sağlamaktadır. EfficientNet-b5 (RGB) nispeten daha düşük doğruluk oranı (94,48%) göstermektedir. MaxPooling tekniği, Transfer Learning deneyine göre daha başarılı sonuçlar çıkaramamaktadır. Gri tonlamalı malware görüntüleri için EfficientNet-b7 91,82% validasyon doğruluk oranı ve RGB malware görüntüleri için 92,63% doğruluk oranı çıkmaktadır. DDAN yaklaşımı, çizelgede en yüksek değerlere sahiptir. EfficientNet-b6 (Gri tonlamalı) modeli, 97,06% validasyon doğruluk oranına sahipken EfficientNet-b5 (RGB) ve EfficientNet-b6 (RGB) sırasıyla 94,42% ve 96,63% validasyon doğruluk oranlarına sahiptir.

Bu tezin akademik literatüre katkısı, genel çalışmaların dışına çıkarak seyrek yararlanılan ve özgün kantman yapılandırmalı EfficientNet mimarisini Dynamic Distribution Adaptation Network (DDAN) modellemesine etkin şekilde dahil etmesidir ve malware sınıflandırmasını gerçekleştirmesidir. Özellikle Dumpware10 veri kümesini işleyen comparison of transfer

learning performance in image - based malware file classification on the Dumpware10 dataset -çizelge 5.17'de 21 kaynak numaralı çalışma- çalışması, Xception ve Inception gibi transfer learning modellerini uygulamaktadır. Bu tez çalışması ise EfficientNet mimarisi ve Dynamic Distribution Adaptation Network donanımını daha özgün bir transfer learning modellemesinde birleştirmektedir. Yalnız bu tez çalışmasının deney sonuçları irdelendiğinde daha kapsamlı hiperparametre optimizasyonuyla daha başarılı validasyon doğruluk oranı, test doğruluk oranı, recall, precision, f1-score test sonuçlarını elde etmek mümkündür. Örneğin Adam ve SGD optimizasyon fonksiyonlarının farklı öğrenme oranları ve epoch döngü sayılarıyla denenmesi ve hiperparametre yapılandırmalarının yürütülmesiyle malware görüntülerinin eğitim döngüsü geliştirilebilmektedir.

Çizelge 5.17. DDAN deney sonuçlarıyla akademik çalışmaların karşılaştırması

Çalışmalar	Veri kümesi	Doğruluk oranı	DDAN EfficientNet-b6 (Gri tonlamalı) doğruluk oranı
[11]	MMCC	99,63% (eğitim)	97% (validasyon) 95% (test)
[2]	MMCC	99,06% (eğitim)	97% (validasyon) 95% (test)
[1]	MMCC	99,44%	97% (validasyon) 95% (test)
[4]	MMCC	99,58%	97% (validasyon) 95% (test)
			DDAN EfficientNet-b6 (RGB) doğruluk oranı
[19]	Dumpware10	99,60%	96% (validasyon) 96% (test)
[21]	Dumpware10	97%	96% (validasyon) 96% (test)

6. SONUÇLAR VE ÖNERİLER

EfficientNet sinir ağı mimarisi, Microsoft Malware Classification Challenge benchmark veri kümesi ile özel Dumpware10 veri kümesinde başarılı doğruluk oranları göstermiştir. Optimizasyon algoritmalarından 0.01 öğrenme oranlı SGD, paralel öğrenme oranında Adam algoritmasına göre nispeten daha başarılı sonuçlar elde etmiştir. EfficientNet-b0 sinir ağı mimarisinden EfficientNet-b7 sinir ağı mimarisine kadar irdelenen eğitim döngülerinde derinlik arttıkça doğruluk oranının arttığı, yalnız EfficientNet-b4 sinir ağı mimarisinin düşük performans gösterdiği görülmüştür. Dumpware10 veri kümesine ait malware görüntüleri, Microsoft Malware Classification Challenge veri kümesine ait RGB üç kanallı malware görüntüleri ve iki kanallı gri tonlamalı malware görüntülerinde farklı EfficientNet mimarileri başarılı performans göstermiştir. Microsoft Malware Classification Challenge veri kümesine ait iki kanallı gri tonlamalı malware görüntüleri, en yüksek katman derinlikli EfficientNet-b7 mimarisinde başarılı performans kaydederken Microsoft Malware Classification Challenge veri kümesine ait RGB üç kanallı malware görüntüleri daha düşük katman derinlikli EfficientNet-b5 mimarisinde başarılı performans kaydetmiştir. Malware verileri, görüntü dönüşüm metodu ve veri kümesine göre değişken performans sonuçları çıkarmıştır. Bu çalışmada EfficientNet derin öğrenme mimarisi modeline bağlı malware sınıflandırması ve görselleştirmesi tamamlayıcı bir araştırmasıyla yürütülmüştür. EfficientNet mimarisine ait inverse residual blok yapılandırmasıyla yaratılan derin öğrenme modeli, malware sınıflandırmasında yüksek doğruluk oranları başarmıştır. Microsoft Malware Classification Challenge ve Dumpware10 veri kümelerinde derin öğrenme modeli başarılı sonuçlar kaydetmiştir. Microsoft Malware Classification Challenge veri kümesinde 97% değerlendirme (validasyon) doğruluk oranı ve 95% test doğruluk oranı yakalanırken Dumpware10 veri kümesinde 96% değerlendirme doğruluk oranı ve test doğruluk oranı yakalanmıştır. EfficientNet derin öğrenme mimarisi, malware sınıflandırma deney çalışmalarında yüksek performans çıkarmıştır. Özellikle veri ön işleme ve eğitim döngüsündeki görüntü dönüşümleri, model başarısına gözle görülür katkıda bulunmuştur. EfficientNet mimarisinin derinlik, genişlik ve çözünürlük boyutlarında dengeli ölçeklendirmesi, derin öğrenme modelinin doğruluk oranını arttırmıştır. Bu çalışma siber güvenlik alanında derin öğrenme tekniklerinin etkin malware sınıflandırma kapasitesini ortaya çıkarmıştır. EfficientNet mimarisinin esnekliği ve transfer learning metotlarının kullanımı modelin doğruluk ve genelleme yatkınlığını arttırmıştır. Gelecek çalışmalarda model performansı farklı veri kümelerinde ve daha karmaşık malware tespit metotlarıyla

geliştirilebilmektedir. Sonuç olarak bu çalışma EfficientNet mimarisinin siber güvenlikte malware sınıflandırması için çözüm sağlayabileceğini irdelemiştir.

KAYNAKLAR

1. Deng, H., Guo, C., Shen, G., Cui, Y., Ping, Y. (2023). MCTVD: A malware classification method based on three-channel visualization and deep learning, *Computers & Security*, 126(7), 103084.

2. Ahmed, M., Afreen, N., Ahmed, M., Sameer, M., Ahamed, J. (2023). An inception V3 approach for malware classification using machine learning and transfer learning, *International Journal of Intelligent Networks*, 4, 11-18.

3. Kumar, S., Panda, K. (2023). SDIF-CNN: Stacking deep image features using fine-tuned convolution neural network models for real-world malware detection and classification, *Applied Soft Computing*, 146, 110676.

4. Bu, S.-J., Cho, S.-B. (2023). Malware classification with disentangled representation learning of evolutionary triplet network, *Neurocomputing*, 552, 126534.

5. Chaganti, R., Ravi, V., Pham, T. D. (2023). A multi-view feature fusion approach for effective malware classification using Deep learning, *Journal of Information Security and Applications*, 72(21), 103402.

6. Baek, S., Jeon, J., Jeong, B., Jeong, Y.-S. (2021). Two-stage hybrid malware detection using Deep learning, *Human-centric Computing and Information Sciences*, 11(27), 1-15.

7. Kumar, M. (2022). Scalable Malware Detection System Using Distributed Deep Learning, *Cybernetics and Systems*, 54(5), 619-647.

8. Xing, X., Jin, X., Elahi, H., Jiang, H., Wang, G. (2022). A malware detection approach using autoencoder in deep learning, *IEEE Access*, 10, 25696-25706.

9. Alomari, E. S., Nuiaa, R. R., Alyasseri, Z. A. A., Mohammed, H. J., Sani, N. S., Esa M. I., Musawi, B. A. (2023). Malware detection using deep learning and correlation-based feature selection, *Symmetry*, 15(1), 123.

10. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Venkatraman, S. (2019). Robust intelligent malware detection using deep learning, *IEEE Access*, 7, 46717-46738.

11. Pratama, H. Y., Sidabutar, J. (2022). *Malware classification and visualization using EfficientNet and B2IMG algorithm.* 2022 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Depok, 75-80.

12. Oyucu, S., Polat, O., Türkoğlu, M., Polat, H., Aksöz, A., Ağdaş, M. T. (2024). Ensemble Learning Framework for DDoS Detection in SDN-Based SCADA Systems, *Sensors*, 24(1), 155.

13. Polat, O., Türkoğlu, M., Polat, H., Oyucu, S., Üzen, H., Yardımcı, F., Aksöz, A. (2024). Multi-Stage learning framework using convolutional neural network and decision Tree-Based classification for detection of DDoS Pandemic Attacks in SDN-Based SCADA Systems, Sensors, 24(3), 1040.

14. Iman, M., Arabnia, H. R., Rasheed, K. (2023). A review of deep transfer learning and recent advancements, *Technologies*, 11(2), 40.

15. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L.-C. (2018). *Mobilenetv2: Inverted residuals and linear bottlenecks*. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Salt Lake City, 4510-4520.

16. Tan, M., Le, Q. (2019). *EfficientNet: Rethinking model scaling for convolutional neural networks*. International Conference on Machine Learning, California, 6105-6114.

17. Escudero García, D., DeCastro-García, N., Muñoz Castañeda, A. L. (2023). An effectiveness analysis of transfer learning for the concept drift problem in malware detection, *Expert Systems with Applications*, 212(3), 118724.

18. Wang, J., Chen, Y., Feng, W., Yu, H., Huang, M., Yang, Q. (2020). Transfer learning with dynamic distribution adaptation, *ACM Transactions on Intelligent Systems and Technology*, 11(1), 1-25.

19. Tekerek, A., Yapici, M. M. (2022). A novel malware classification and augmentation model based on convolutional neural network, *Computers & Security*, 112(2), 102515.

20. Bala, Z., Zambuk, F. U., Imam, B. Y., Gital, A. Y., Shittu, F., Aliyu, M., Abdulrahman, M. L. (2022). Transfer learning approach for malware images classification on Android devices using deep convolutional neural network, *Procedia Computer Science*, 212(4), 429-440.

21. Prawiranata, F. P. S., Hadiprakoso, R. B. (2023). *Comparison of transfer learning performance in image-based malware file classification on the Dumpware10 dataset*. 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, 252-257.



Gazili olmak ayrıcalıktır