

**T.C.**

**KARADENİZ TEKNİK ÜNİVERSİTESİ**

Real ve Fake Yüz Görüntülerinin Derin Öğrenme (CNN) ile Sınıflandırılması

**Grup Adı MNY**

Melike Nur YILMAZ

415214

Proje Raporu: Real ve Fake Yüz Görüntülerinin Derin Öğrenme ile Sınıflandırılması

1. Giriş

Bu proje, gerçek ve sahte yüz görüntülerinin derin öğrenme modelleri kullanılarak sınıflandırılmasını amaçlamaktadır. Projede kullanılan veri setleri farklı zorluk seviyelerine sahip iki veri kümesinden oluşmaktadır. Projeye dahil edilen derin öğrenme modelleri arasında MobileNet v3-small, Basit CNN Modeli ve ShuffleNet bulunmaktadır. Bu modellerin performansları her iki veri seti üzerinde değerlendirilmiştir.

2. Veri Setleri

2.1 Veri Seti 1: Fake vs Real Face Classification(REALvsFAKE)

Bu veri seti, sahte ve gerçek yüz görüntülerinin daha kolay ayrıştırılabildiği bir veri setidir.

2.2 Veri Seti 2: HardFake vs Real Faces(HARDfakevsreal)

Bu veri seti, sahte ve gerçek yüz görüntülerinin ayrıştırılmasının daha zor olduğu bir veri setidir.

Veri Setlerinden Örnek Veriler



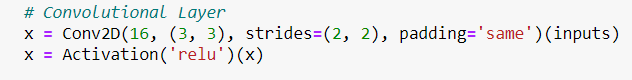
3. Kullanılan Derin Öğrenme Modelleri

3.1 MobileNet v3-small

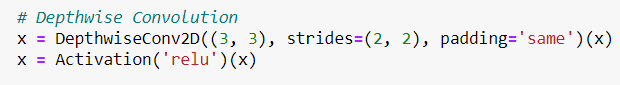
MobileNet v3-small, mobil cihazlar ve gömülü sistemler için optimize edilmiş hafif bir derin öğrenme modelidir. Özellikle sınırlı hesaplama kaynaklarına sahip cihazlar için tasarlanmıştır.

MobileNet v3-small Model Mimarisi

3.1.1 Evrişim Katmanları (Convolutional Layers): Giriş görüntüsündeki özellikleri çıkarmak için kullanılan evrişim katmanları bulunur. Bu katmanlar, görüntü üzerinde filtrelendirme işlemi yaparak özellik haritasını oluşturur.



3.1.2 Derinliksel Evrişim Katmanları (Depthwise Convolutional Layers): MobilNetV3 mimarisinde, evrişim katmanları genellikle derinliksel evrişim katmanları olarak uygulanır. Bu katmanlar, giriş kanallarını tek tek işleyerek hesaplama maliyetini azaltır ve modelin hafif olmasını sağlar.



3.1.3 Küresel Ortalama Havuzlama (Global Average Pooling): Bu katman, özellik haritasındaki her kanalın ortalama değerini alarak bir vektör oluşturur. Bu, özellik haritasının boyutunu azaltır ve modelin çıktılarına beslenmeden önce veri boyutunu azaltır.



3.1.4 Tam Bağlantılı Katmanlar (Fully Connected Layers): MobilNetV3'ün son katmanları tam bağlantılıdır. Bu katmanlar, küresel ortalama havuzlama katmanının çıktılarını alır ve sınıflandırma için kullanılır. Özellik vektörleri, sınıflar arasında ayrım yapmak için bu katmanlara beslenir.



3.1.5 Aktivasyon Fonksiyonları: Evrişim ve tam bağlantılı katmanların ardından genellikle ReLU (Rectified Linear Activation) gibi aktivasyon fonksiyonları kullanılır. Bu fonksiyonlar, modelin öğrenme kapasitesini artırır ve ağın doğrusallığı kırarak daha kompleks karar sınırları öğrenmesini sağlar.

3.1.6 Modelin Sonu (Output Layer): Modelin sonunda, genellikle softmax aktivasyon fonksiyonuyla donatılmış bir çıktı katmanı bulunur. Bu katman, modelin verilen görüntüyü belirli sınıflara sınıflandırmasını sağlar.

MobilNetV3 mimarisi, hesaplama gücü kısıtlı cihazlar için optimize edilmiş olup, hafif ve verimli bir yapıya sahiptir. Bu bileşenler, modelin yüksek performanslı sınıflandırma yapmasını sağlar, aynı zamanda modelin boyutunu küçük tutarak depolama ve bellek gereksinimlerini azaltır. Bu özellikler, mobil ve gömülü sistemlerde uygulama geliştirmek için ideal bir seçenek sunar.

3.1.7 Model Sonuç

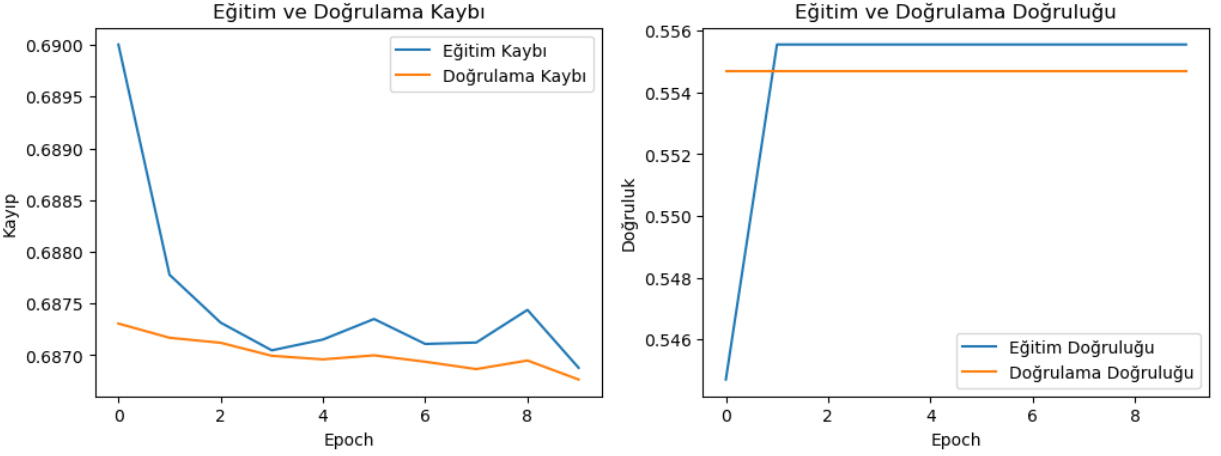
Veri Seti 1 için:

Eğitim setinde %51.41 doğruluk elde edildi.

Doğrulama setinde %55.47 doğruluk elde edildi.

Eğitim ve doğrulama kayıp değerleri yaklaşık olarak 0.69 seviyesinde sabit kaldı.





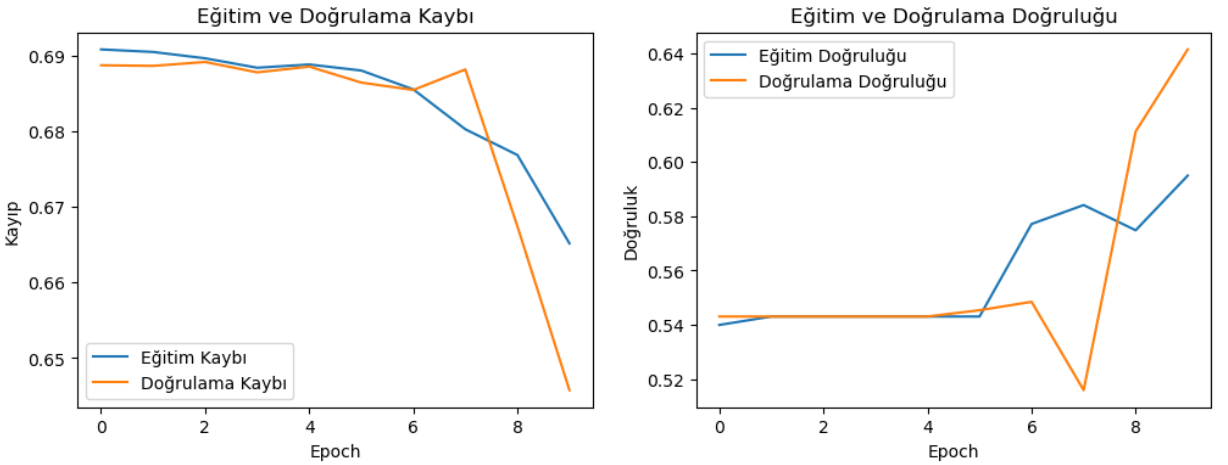
Veri Seti 2 için:

Eğitim setinde %59.52 doğruluk elde edildi.

Doğrulama setinde %64.16 doğruluk elde edildi.

Eğitim kaybı 0.6662, doğrulama kaybı ise 0.6458 olarak belirlendi.





3.2 Basit Evrişimli Sinir Ağı Modeli

Basit CNN Model Mimarisi

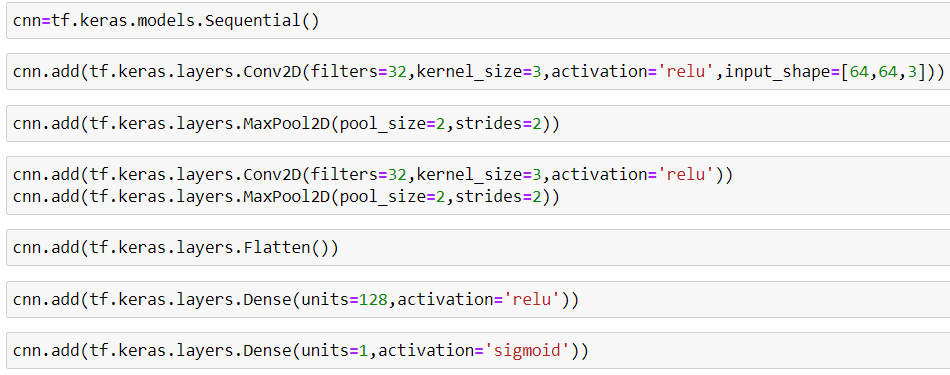
Bu çalışma, gerçek ve sahte görüntüler arasındaki farkı belirlemek için basit bir evrişimli sinir ağı (CNN) modeli geliştirmeyi amaçlamaktadır.

3.2.1 Veri Yüklemesi ve Ön İşleme:

Proje için kullanılan veri seti, gerçek ve sahte görüntüler içeren iki sınıftan oluşmaktadır. Eğitim veri seti, gerçek ve sahte görüntülerin bulunduğu klasörlerden yüklenmiş ve ön işleme adımları uygulanmıştır. Veri artırma teknikleri kullanılarak, eğitim veri seti çeşitlendirilmiş ve modelin daha genelleştirilmiş özellikler öğrenmesi sağlanmıştır.

3.2.2 Model Mimarisi:

Geliştirilen model, iki evrişim katmanı (Conv2D) ve ardından bir dizi tam bağlı katman içermektedir. Evrişim katmanları, görüntülerdeki özellikleri çıkarmak için kullanılırken, tam bağlı katmanlar bu özellikleri sınıflandırmak için kullanılmıştır. Modelin çıkış katmanında, ikili sınıflandırma için sigmoid aktivasyon fonksiyonu kullanılmıştır.



3.2.3 Model Eğitimi ve Değerlendirme:

Model, eğitim ve doğrulama veri setleri üzerinde 10 epoch boyunca eğitilmiştir. Eğitim sırasında, adam optimizerı ve ikili çapraz entropi kaybı kullanılmıştır. Ayrıca, modelin performansını değerlendirmek için doğruluk metriği kullanılmıştır.

3.2.4 Model Sonuç

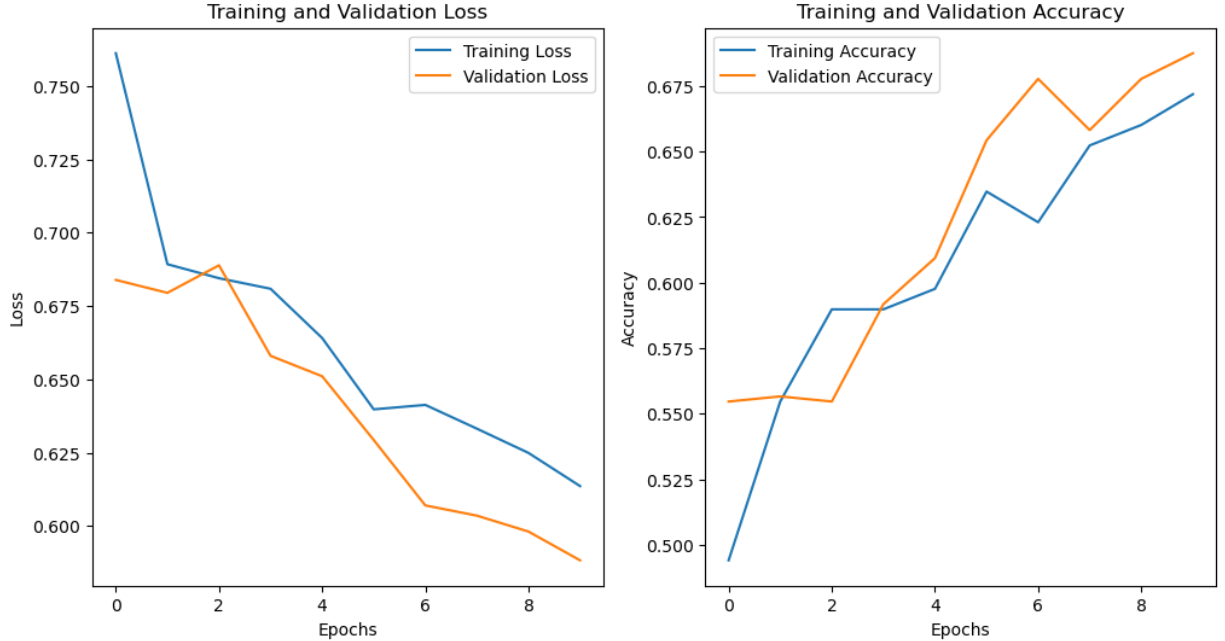
Veri Seti 1 için :

Eğitim setinde %69.56 doğruluk elde edildi.

Doğrulama setinde %68.75 doğruluk elde edildi.

Eğitim kaybı 0.5917, doğrulama kaybı ise 0.5883 olarak belirlendi.





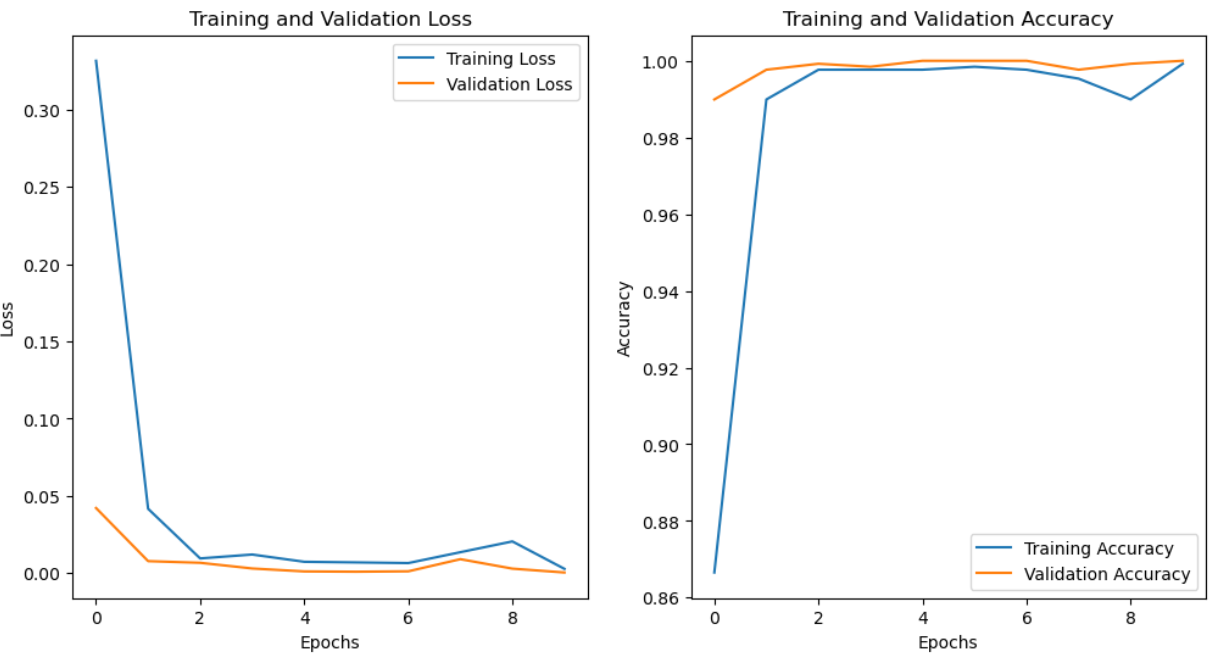
Veri Seti 2 için :

Eğitim setinde %99.88 doğruluk elde edildi.

Doğrulama setinde %100.00 doğruluk elde edildi.

Eğitim kaybı 0.0100, doğrulama kaybı ise 0.0045 olarak belirlendi.





3.3 ShuffleNet

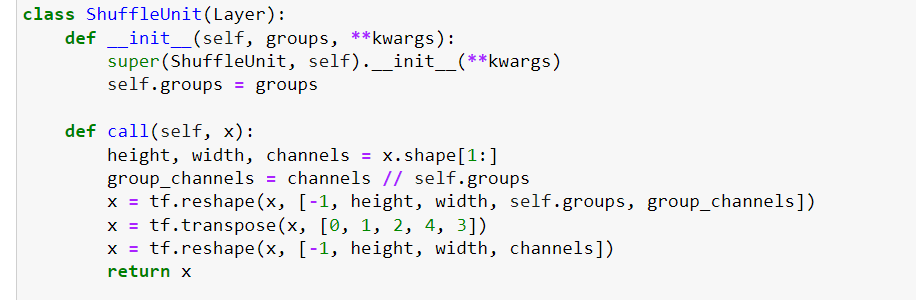
Bu çalışmada, ikili görüntü sınıflandırma amacıyla TensorFlow ve Keras kullanılarak bir ShuffleNet V2 modeli geliştirildi. ShuffleNet V2, özellikle mobil ve gömülü cihazlar gibi hesaplama gücü kısıtlı ortamlarda verimlilik sağlamak üzere tasarlanmış hafif bir konvolüsyonel sinir ağı (CNN) mimarisidir.

Bu modelin temel yeniliklerinden biri, hesaplama maliyetini azaltırken yüksek doğruluğu korumak için kanal karıştırma ve grup konvolüsyonları kullanmasıdır.

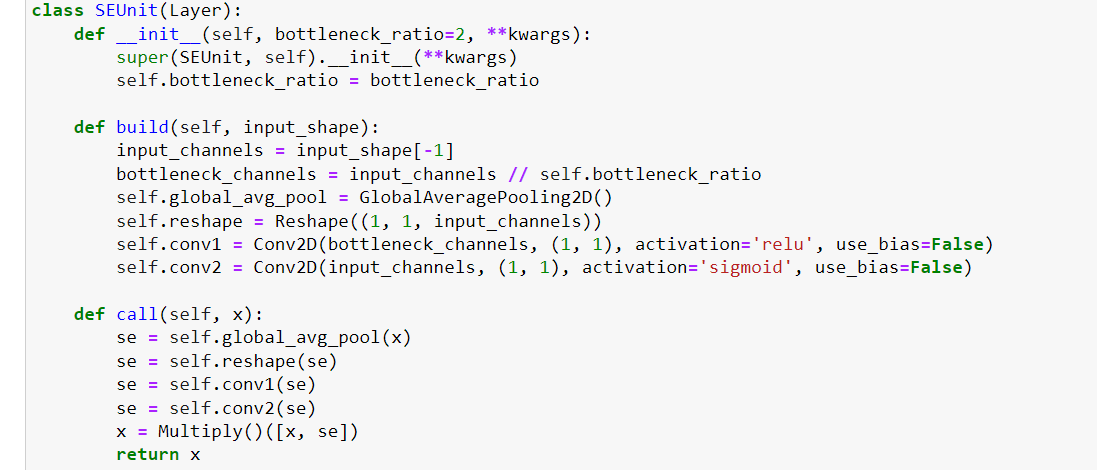
ShuffleNet Model Mimarisi

ShuffleNet V2 mimarisi, aşağıdaki ana bileşenlerden oluşur:

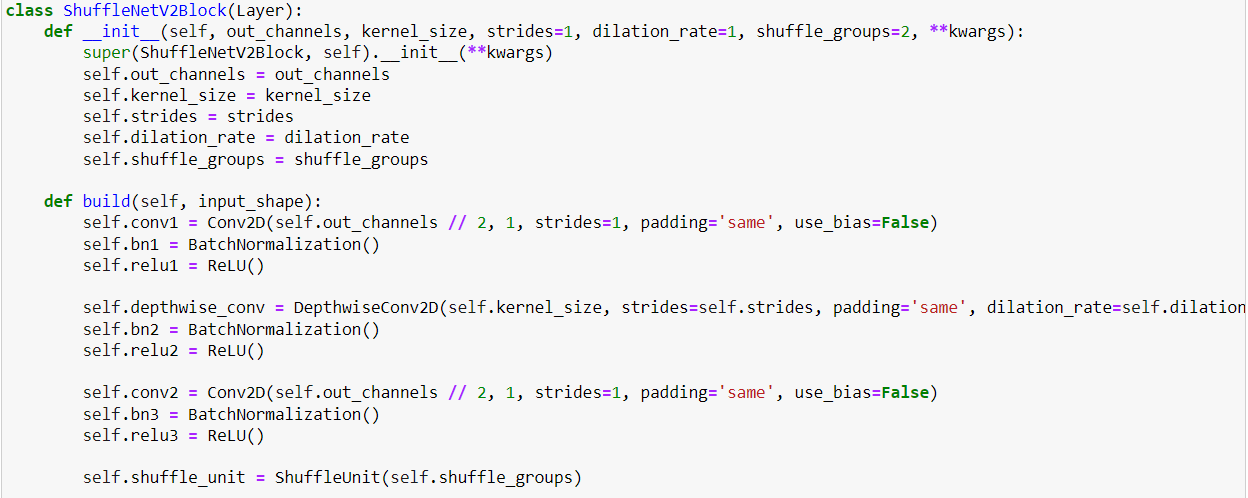
3.3.1 ShuffleUnit Katmanı: Bu katman, kanal karıştırma mekanizmasını uygular. Kanal karıştırma, farklı özellik haritası grupları arasındaki bilgi akışını iyileştirerek, ağın temsil kapasitesini artırır. Aşağıdaki kod parçası, bu katmanın nasıl çalıştığını göstermektedir:

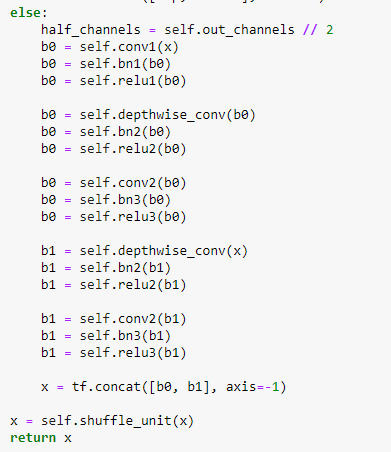
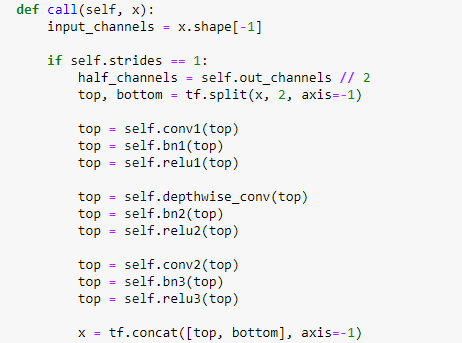


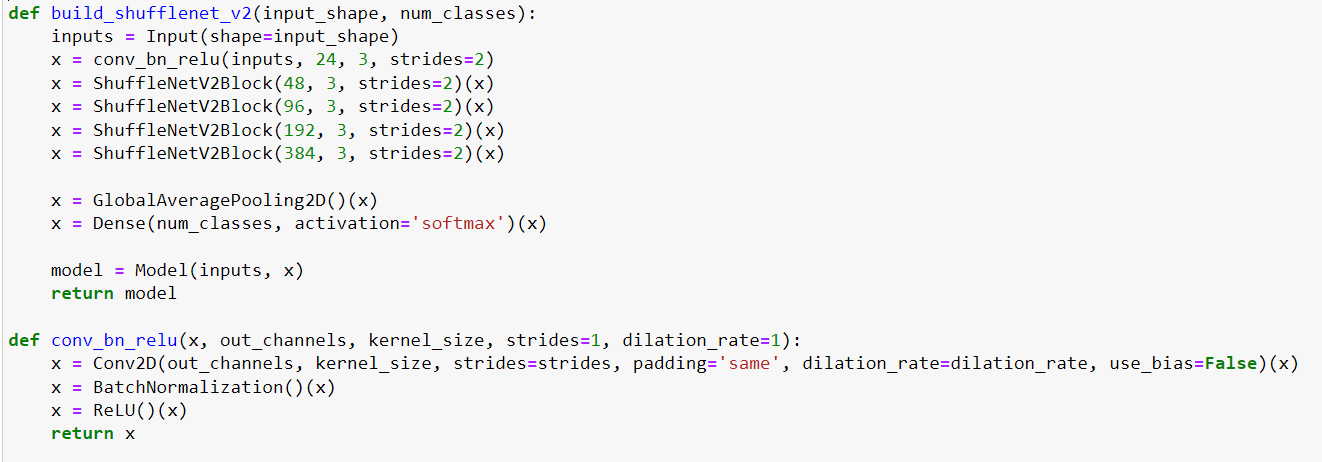
3.3.2 SEUnit Katmanı: Sıkıştırma ve Uyarma (SE) bloğu, kanallar arasındaki bağımlılıkları modelleyerek ağın temsil gücünü artırır. Bu katman, global ortalama havuzlama, iki tam bağlantılı katman ve sigmoid aktivasyon kullanarak kanal bazında özellik yanıtlarını yeniden kalibre eder:



3.3.3 ShuffleNetV2Block Katmanı: Bu katman, ShuffleNet V2'nin temel yapı taşıdır. Kanal karıştırma ile birlikte derinlik-wise ayrılabilir konvolüsyonları kullanarak hesaplama açısından verimli ve güçlü bir özellik çıkarıcı oluşturur:





3.3.4 Modelin Kurulumu: ShuffleNet V2 modeli, bir dizi ShuffleNetV2Block katmanını, ardından bir global ortalama havuzlama katmanını ve sınıflandırma için yoğun bir çıkış katmanını kullanarak oluşturulur:

3.3.5 Veri Hazırlama ve Eğitim

Model, "REALvsFAKE" veri setindeki görüntüler kullanılarak eğitildi. Eğitim ve doğrulama setleri için veri artırma teknikleri uygulandı. Eğitim setinde görüntüler yeniden ölçeklendirme, kesme, yakınlaştırma ve yatay çevirme gibi işlemlerden geçirildi:



Bu modelde Kanal karıştırma ve SE blokları gibi yenilikçi teknikler kullanarak, modelin düşük hesaplama gücü ile yüksek doğruluk elde edebildiği görülmüştür. Bu, özellikle mobil ve gömülü sistemler için önemli bir avantaj sağlar.

3.3.6 Model Sonuç

Eğitim Sonuçları Veri Seti 1 için:

Model, eğitim veri setinde %64.90 doğruluk oranına ulaşmıştır.

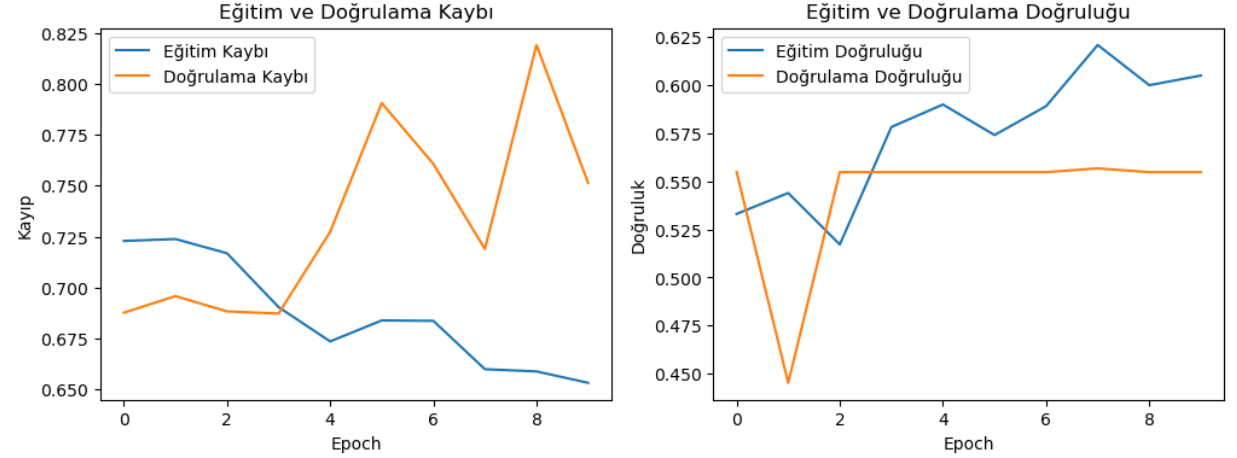
Eğitim kaybı, epochlar ilerledikçe azalmış ve son epochta 0.6430 olarak kaydedilmiştir.



Doğrulama Sonuçları:

Doğrulama veri setinde model %57.81 doğruluk oranına ulaşmıştır.

Doğrulama kaybı ise 0.6935 olarak kaydedilmiştir.



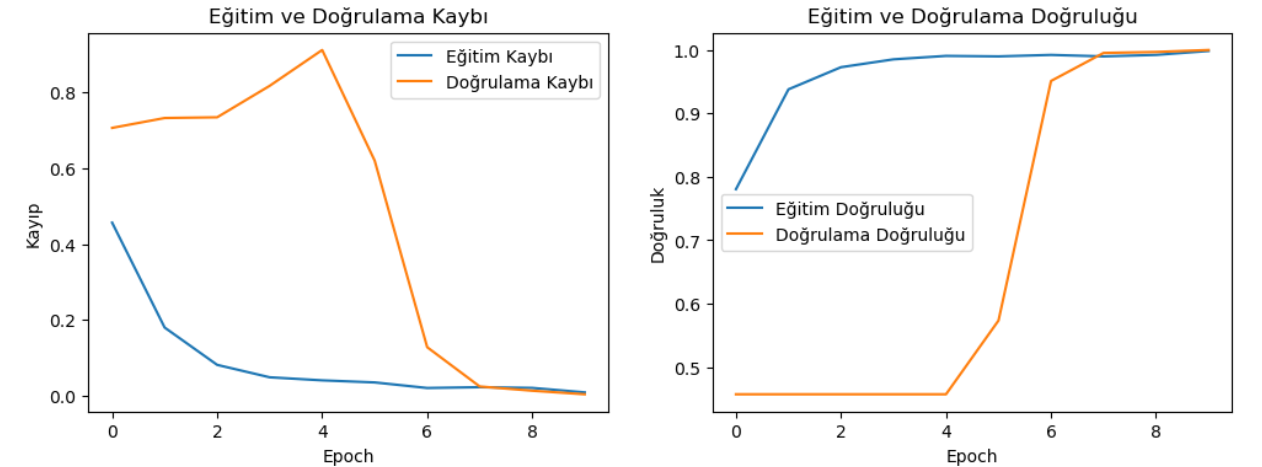
Eğitim Sonuçları Veri Seti 2 için:

Model eğitiminde, son epoch'ta %99.88 doğruluk elde edilmiş ve kayıp 0.0100 olarak ölçülmüştür.



Doğrulama Sonuçları:

Model, doğrulama veri setinde %100.00 doğruluk oranına ulaşmış ve doğrulama kaybı 0.0045 olarak hesaplanmıştır.



4. Sonuç

Bu çalışmada, gerçek ve sahte yüz görüntülerini sınıflandırmak için üç farklı derin öğrenme modeli olan MobilNetV3 Small, Basit CNN ve ShuffleNet kullanılmıştır. Her bir modelin performansı, eğitim doğruluğu, doğrulama doğruluğu, eğitim kaybı ve doğrulama kaybı gibi metriklerle değerlendirilmiştir. Sonuçlar aşağıdaki gibidir:

MobilNetV3 Small modeli, eğitim veri setinde %51.41 doğruluk ve doğrulama veri setinde %55.47 doğruluk elde etmiştir. Eğitim ve doğrulama kayıp değerleri yaklaşık olarak 0.69 seviyesinde sabit kalmıştır. Bu sonuçlar, modelin veri setine yeterince iyi uyum sağlamadığını ve hem eğitim hem de doğrulama setlerinde düşük performans sergilediğini göstermektedir.

MobilNetV3 Small modeli, hafif ve düşük bellek gereksinimleri olan bir modeldir. Ancak, bu çalışma özelinde modelin düşük doğruluk oranları, veri setinin karmaşıklığını öğrenmede yetersiz kaldığını veya daha fazla eğitim verisine ihtiyaç duyduğunu göstermektedir. Bu durum, modelin daha fazla veri ile eğitilmesi veya modelin hiperparametrelerinin optimize edilmesi gerektiğini düşündürebilir..

Basit CNN modeli, MobilNetV3 Small modeline göre daha yüksek doğruluk ve daha düşük kayıp değerleri elde etmiştir. Eğitim ve doğrulama setlerinde benzer performans göstermiştir. Bu durum, modelin veri setindeki desenleri öğrenmede daha başarılı olduğunu ve aşırı uyum problemi yaşamadığını göstermektedir. Ancak, doğruluk oranının daha da iyileştirilmesi için modelin karmaşıklığı artırılabilir veya daha fazla veri kullanılabilir.

ShuffleNet modeli, eğitim setinde makul bir doğruluk oranına ulaşmış ancak doğrulama setinde daha düşük bir performans sergilemiştir. Eğitim kaybı epochlar ilerledikçe azalmış, ancak doğrulama kaybı yüksek kalmıştır Bu sonuçlar, modelin eğitim sürecinde öğrenme kapasitesini artırdığını ve belirli bir doğruluk oranına ulaştığını göstermektedir.