Gerçek ve Yapay Zeka Tarafından Oluşturulmuş İnsan Yüzlerinin Sınıflandırılması

SÜMEYYE BAKIRDAL

Fırat Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü,Elazığ

sumeyyebakirdal@gmail.com

Öz: Yapay zeka teknolojilerinin gelişmesinin sonucunda gerçek ve sentetik görüntülerin oluşturulması ve analiz edilmesinin mümkün hale gelmesine olanak tanınmış durumdadır. Özellikle yapay sinir ağlarıyla üretilen sahte yüzler; dijital güvenlik ve medya doğrulama süreçlerinde önemli bir araştırma konusu haline gelmiştir. Bu çalışma kapsamında gerçek insan yüzleri ile yapay zeka tarafından oluşturulan yüzleri sınıflandırmak için Convolutional Neural Network (CNN) tabanlı bir model geliştirilmiştir. Kaggle platformundan temin edilen verisetinde 5000 gerçek ve 4936 yapay yüz bulunmaktadır. Modelin eğitim sürecinde veriler üzerinde ön işleme teknikleri uygulanarak performansı doğruluk ve F1 skoru açısından değerlendirilmiştir. Önerilen model gerçek ve yapay yüzleri yüksek başarı oranıyla ayırt edebildikten sonra hassasiyet gibi metriklerle test edildi.Deneysel bulguar yapay yüzleri oldukça doğru bir şekilde tanımladığını göstermektedir.Bu çalışma derin öğrenme tabanlı yöntemlerle yapay yüz tanıma alanında katılımcılara yardım etmektedir.

Anahtar kelimeler: Yapay Zeka, Derin Öğrenme, Görüntü Sınıflandırma, Yapay Yüz Tespiti, Convolutional Neural Network

Classification of Real and Artificial Intelligence Generated Human Faces

Abstract: The development of artificial intelligence technologies has made it possible to create and analyze real and synthetic images. In particular, fake faces generated by artificial neural networks have become an important research topic in digital security and media verification processes. In this study, a Convolutional Neural Network (CNN) based model is developed to classify real human faces and artificial intelligence generated faces. The dataset obtained from the Kaggle platform contains 5000 real and 4936 artificial faces. During the training process of the model, preprocessing techniques were applied on the data and its performance was evaluated in terms of accuracy and F1 score. After the proposed model was able to distinguish between real and artificial faces with a high success rate, it was tested with metrics such as precision. Experimental findings show that it identifies artificial faces quite accurately. This study helps participants in the field of artificial face recognition with deep learning based methods.

Key words: Artificial Intelligence, Deep Learning, Image Classification, AI-Generated Face Detection, Convolutional Neural Network.

1.Giriş

Son zamanlarda yapay zeka ve derin öğrenme teknolojilerindeki ilerlemeler sayesinde son derece gerçekçilere benzeyen sahte yüz görsellerinin oluşturulabildiklerini görmekteyiz. Generative Adversarial Networks (GAN) gibi derin öğrenme modellerinin insanın ayırt etmesini zorlaştıracak kadar gerçekçiliğin ötesinde görseller üretebilmelerine olanak sağlamaktadır. Bu gelişmeler beraberinde sanal kimlik hırsızlığına, dijital manipülasyona ve sahte haberlerin yayılmasına yönelik ciddii güvenlik tehditlerini de getirmektedir. Bu durumda gerçek ve yapay olarak oluşturulan yüzler arasındaki ayrımı yapabilen güvenilir ve yüksek doğruluk oranına sahip modellerin geliştirilmesinin önemi artıyor. Derin öğrenme tabanlı modeller özellikle Convolutional Neural Networks (CNN) gibi mimariler ile yüz tanıma ve sahte yüz algılama konularında başarılı sonuçlar elde ediyorlar. Bu çalışmanın amacı, gerçek ve yapay zeka tarafından oluşturulan yüzleri doğru bir şekilde sınıflandırabilen bir model geliştirmek ve bu modelin etkinliğini değerlendirmektir. Model, geniş bir veri seti kullanılarak eğitilmiş ve farklı veri işleme teknikleri uygulanarak optimize edilmiştir.

2. Literatür Taraması

Yüz tanıma teknolojisi son yıllarda derin öğrenme yöntemlerinin gelişimi ile büyük bir ilerleme kaydetmiş ve çeşitli alanlarda uygulanabilir hale gelmiştir. Ancak insan yüzleri ile yapay zeka tarafından üretilmiş yüzler arasındaki doğru ayırımın hala zor olduğu ve mevcut literatürde bu konuda sınırlı çalışma yapıldığı bilinmektedir. Bu kısımda daha önce yapılan araştırmalar incelenerek yüz tanıma teknolojilerine ve yapay zeka tarafından üretilmiş yüzlere yönelik sınıflandırmanın hangi katkılarda bulunduğu vurgulanacaktır.

Khodabakhsh (2018), yüz sahteciliği tespiti için Transfer Learning (Aktarım Öğrenmesi) ve derin öğrenme yöntemlerini karşılaştırmıştır. CNN temelli VGG16 mimarisi ile transfer öğrenmenin kullanıldığı bu çalışmada, üç farklı veri kümesi üzerinde testler yapılmış ve transfer öğrenmenin veri yetersizliği durumlarında daha başarılı sonuçlar verdiği gösterilmiştir [1].

Yorum: Bu çalışma, derin öğrenme yapılarına karşı transfer öğrenme tekniklerini inceleyerek ve çoklu veri setlerinde yüksek doğru sonçlar elde ediyor; aynı şekilde, verinin yetersiz olduğunda çözüm sunan bir çalışma da transfer öğrenme kullanılarak yapılıyor.

Li, Y. (2020), GAN (Generative Adversarial Networks) tabanlı sahte yüz görsellerini tespit etmek için yüksek kaliteli sahte görsellerle eğitilmiş bir CNN modeli önermiştir. Gerçek ve sahte görselleri ayırt edebilen bu sistem, derin özellik çıkarımı ve sınıflandırma katmanları ile yüksek başarı sağlamıştır [2].

Yorum: GAN'lar tarafından üretilmiş sahte görüntülerin yaygınlaşmasıyla birlikte bu çalışma önerilen yöntemin günümüzde artan tehditleri etkili bir şekilde ele aldığını göstermektedir Benim araştırmam da GAN kaynaklı sahte verilerin belirlenmesine odaklanıyor.

Liu, Y. (2018), yüz sahteciliği tespiti için spatiotemporal LBP (Local Binary Pattern) öznitelikleri ve SVM sınıflandırıcısını bir arada kullanmıştır. Bu yaklaşım, özellikle video tabanlı saldırılarda yüz hareketlerinden faydalanarak yüksek başarı elde etmiştir [3].

Yorum: Geleneksel yöntemler arasında yaygın olan LBP ve SVM'nin birleşimi bu çalışmanın odak noktası olmuştur ve benzer bir yapı kullanılarak performans değerlemesi gerçekleştirilmiştir.

Yang, X. (2019), LBP texture operatörleri ile optik akış algoritmalarını birleştirerek görüntü üzerindeki gürültüyü azaltmak ve öznitelikleri daha doğru çıkarmak için çok katmanlı bir model önermiştir. MOLF olarak adlandırılan bu yapıda, CASIA, PRINT-ATTACK ve REPLAY-ATTACK veri kümeleri kullanılmış ve SVM sınıflandırıcısı ile %96.543 doğruluk oranı elde edilmiştir [4].

Yorum: Bu araştırma sahte yüz saldırılarını ele alarak fotoğraf ve video analizlerini içeren üç yönlü bir inceleme sunuyor. Matlab kullanılarak gerçekleştirilmiş ve yüksek doğru oranıyla dikkat çekiyor.

Wang, J. (2020), GAN ve insan eliyle oluşturulan sahte yüz görsellerini tespit etmek için *FakeFaceDetect* adında sinir ağı tabanlı bir adli analiz platformu geliştirmiştir. Görsellerin meta verilerinin değiştirilmesi gibi saldırı senaryoları da dikkate alınmıştır. Sistem yüksek başarı göstermiştir ancak doğruluk oranı belirtilmemiştir [5].

Yorum: Önerilen sistem önemli olabilir ancak doğru oranlarının eksikliği eleştirilebilir niteliktedir.

Rosebrock (2018), OpenCV ve derin öğrenme kullanarak yüz tespiti ve tanıma gerçekleştirmiştir. 128-dim öznitelik çıkarımı sonrası SVM sınıflandırıcısı eğitilmiştir. Bu sistem özellikle video akışlarında yüz tanıma üzerine odaklanmıştır [6].

Yorum: Çalışmada doğruluk oranı belirtilmemiştir. Bu projede ise her bir modelin başarım metrikleri analiz edilmiştir.

Yang, X (2019), yardımcı denetim yaklaşımıyla bir CNN-RNN modeli geliştirmiştir. Yüz derinliği ve rPPG sinyalleri kullanılarak sahte ve gerçek yüzler ayrıştırılmıştır. Model, Oulu veri seti üzerinde %94.2 doğruluk oranı ile başarılı sonuçlar vermiştir [7].

Yorum: Bu araştırma, piksel ve zaman serisine dayalı kontrol kullanarak benzersiz bir metod sunuyor. Bu çalışma aynı şekilde hibrit yapılar üzerinde test edilmiştir.

Kim, J. (2017), maskeli sahte yüzleri tespit etmek için Albedo-3 yöntemini önermiştir. Radyans ölçümleri ile cilt ve maske ayrımı yapılmış, Fisher’s Linear Discriminant ile %97.78 doğruluk elde edilmiştir [8].

Yorum: Bu proje sadece maskeye değinmekle kalmayıp daha geniş bir sahte yüz tespit senaryolarını da içermektedir.

3. Kullanılan Yöntemler

Bu araştırmada gerçek insan yüzlerinin yanı sıra yapay zeka tarafından oluşturulan sahte yüzlerin doğru bir şekilde sınıflandırılmasını sağlamak amacıyla derin öğrenme tabanlı Evrişimli Sinir Ağları (CNN) mimarilerinden yararlanılmıştır. Uygulanan yöntemler verinin hazırlanmasından modelin değerlenmesine kadar olan çeşitli aşamalar içermektedir. Bu aşamaların her birinin detayları aşağıda açıklanacaktır:

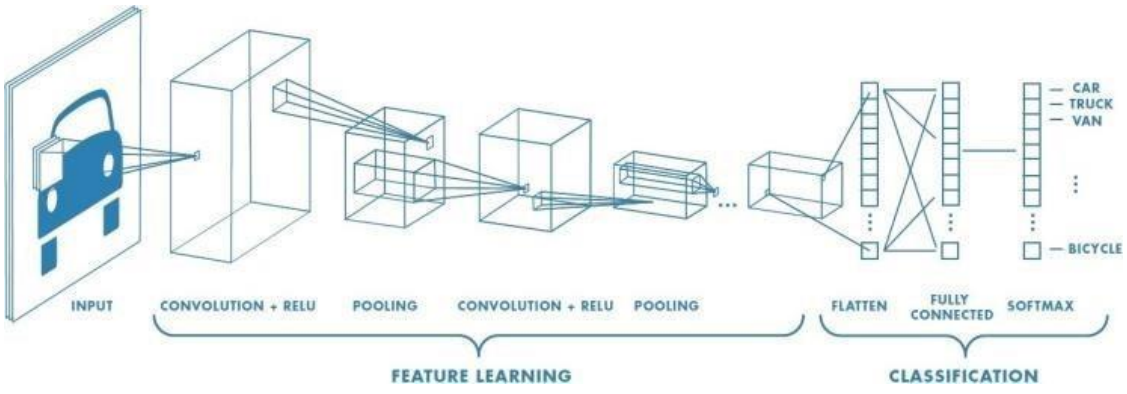
3.1 Veri Seti Hazırlığı

Veri seti, iki sınıftan oluşmaktadır: gerçek insan yüzleri (etiket: 0) ve yapay zeka tarafından oluşturulmuş yüzler (etiket: 1). Bu iki sınıf için ayrı veri klasörleri bulunmaktadır. Gerçek yüzler ve yapay yüzler, belirli bir klasörden yüklenmiş ve her bir görüntü, modelin giriş boyutlarına uyacak şekilde 224x224 piksel boyutuna yeniden boyutlandırılmıştır. Veri seti üzerinde yapılan işlemler:

- Görseller, OpenCV kütüphanesi kullanılarak yüklenmiş ve renk formatı BGR'den RGB'ye dönüştürülmüştür.
- Görsellerin piksel değerleri 0 ile 255 arasında değişmektedir, bu nedenle bu değerler 255.0'a bölünerek [0, 1] aralığına normalize edilmiştir.
- Veri seti, eğitim, doğrulama ve test verisi olarak üçe ayrılmıştır. Eğitim verisi %70, doğrulama ve test verisi ise kalan %30'luk kısmı oluşturacak şekilde bölünmüştür. Veri setinin eğitim ve test verilerine ayrılması, modelin doğruluğunu değerlendirirken daha güvenilir sonuçlar elde edilmesini sağlamaktadır.

3.2 Model Mimarisi Tasarımı

3.2.1 Convolutional Neural Network (CNN): Katmanlardan en az birinde matris çarpımı yerine konvolüsyon işlemi bulunan sinir ağı. Görüntü tanıma, görüntü sınıflandırmaları yapmak için ana kategorilerden biridir. Teknik olarak, derin öğrenme CNN modelleri eğitmek ve test etmek için, her giriş görüntüsü filtreler (Çekirdekler), yoklama, tam bağlı katmanlar (FC) ile bir dizi konvolüsyon katmanından geçecek ve bir nesneyi 0 ile 1 arasındaki olasılıksal değerlerle sınıflandırmak için SoftMax işlevini uygulayacaktır. Aşağıdaki şekil, bir giriş görüntüsünü işlemek ve nesneleri değerlere göre sınıflandırmak için CNN'in tam bir akışıdır [9].



Şekil 1: Convolutional Neural Network

3.2.2 Konvolüsyon Katmanları: Konvülasyon katmanı, giriş görüntüsü üzerinde küçük filtreler (kernel) kaydırarak (slide) yerel öznitelikler (kenar, köşe, doku gibi) çıkarır. Bu filtreler, görüntüdeki önemli yapıları öğrenerek modelin genel desen tanıma kabiliyetini geliştirir [10].

3.2.3 Aktivasyon Fonksiyonları (ReLU): Aktivasyon fonksiyonları, konvülasyon katmanından sonra uygulanır ve modelin doğrusal olmayan karmaşık örüntüleri öğrenmesini sağlar. CNN'lerde en yaygın olarak **ReLU (Rectified Linear Unit)** kullanılır. ReLU, negatif değerleri sıfıra indirgerken pozitif değerleri olduğu gibi bırakır ve modelin hesaplama yükünü azaltır [11].

3.2.4 Havuzlama Katmanları (Pooling): Havuzlama katmanı, uzamsal boyutları azaltarak (örneğin 32x32'den 16x16'ya) hesaplama maliyetini düşürür ve fazla öğrenmenin (overfitting) önüne geçer. En sık kullanılan havuzlama türü **max pooling**'dir; bu yöntemde belirlenen bölgedeki en büyük değer alınır[12].

3.2.5 Dropout: Dropout katmanı, eğitim sırasında bazı nöronların rastgele "pasif hale" getirilmesini sağlar. Bu yöntem, modelin aşırı öğrenmesini engeller ve daha genel sonuçlar üretmesini sağlar. Genellikle %20 ila %50 oranında nöronlar geçici olarak devre dışı bırakılır [13].

3.2.6 Tam Bağlantılı Katmanlar (Fully Connected Layers): Bu katman, konvülasyon ve havuzlama katmanlarından çıkarılan öznitelikleri kullanarak sınıflandırma işlemini gerçekleştirir. Tüm nöronlar birbirine bağlanır ve sonuç olarak bir çıktı sınıfı belirlenir (örneğin, gerçek yüz vs sahte yüz) [14].

4. Eğitim Süreci ve Parametreler

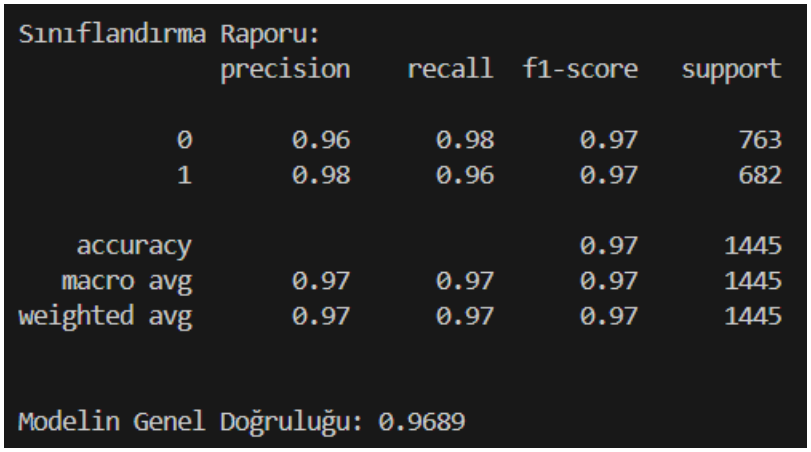
Eğitim sürecinde model için Adam optimizasyon algoritması tercih edildi ki bu da modelin daha hızlı ve istikrarlı bir şekilde eğitime tabi tutulmasını sağlar çünkü öğrenme oranını dinamik olarak ayarlar ve bu şekilde daha verimli sonuçlar elde edilmesini sağlar. Adam algoritması genellikle büyük veri setlerinde ve derin öğrenme modellerinde kullanılan bir optimizasyon algoritmasıdır; özellikle her parametre için farklı öğrenme oranları belirleyerek momentum ve öğrenme oranlarını birleştirir ve böylelikle daha etkili bir öğrenme süreci sunar. Modelde binary_crossentropy kayıp fonksiyonunun seçildiği ifade edilmiştir. Bu işlev genellikle yalın iki sınıfa dayalı problemlerde kullanılır ve binary crossentropy aracılığıyla modelin doğruyu iyileştirme sürecine katmaktadır; modelin çıktıları ile gerçek etiketleri arasındaki farkı hesaplayarak optimize edilir ve iki sınıftaki olasılıkları en küçük hale getirmeye çalışır. Model toplamda 10 epoch boyunca eğitildi; her bir epoch'tan önce model parametreleri güncellendi ve eğitim verisetinde son değişimler yapıldı. Eğitim sürecinde her epoch'un sonunda doğru oranları ve kayıp değeri takip edildi ve modelin öğrenme sürecine detaylı bir şekilde gözlendi. Modelin daha fazla öğrenme şansı elde etmesini sağlamak amacıyla epoch sayısının artırılması düşünülse de bu durum beraberinde overfitting riskini getirebilir; bu sebeple epoch sayısı dikkatlice seçilmiştir ve eğitim sırasında batch size değeri 16 olarak belirlenmiştir ki her iterasyonda model 16 örnekle çalışacak şekilde eğitilecektir. Eğitim sürecinin hızını ve verimini etkiyen önemli bir faktör olan grup boyutu çoğunun daha hızlı eğitime yol açarkeni küçük grup büyükleri modelin daha iyi genelleme yapmasına yardımcı olabilir.

5. Model Değerlendirme ve Doğrulama

Modelin değerinin belirlenmesi iyi bir eğitim sürecinin başarısını öğrenmek ve modelin genelleyici yeteneklerini sınamak için önemli bir adımdır.Bu başarılar eğitim verilerinin sınırlarının ötesine geçerek daha önce hiç görmediği test verilerinde de değerlenmiştir.Eğitimin sonunda modelin test verilerindeki performansı incelenmiş ve çıktıları doğru tahminle karşılaştırılıp doğru tahmin oranları gibi parametrelerle değerlenmiştir.Bu parametreler farklı yönlerden modellerin başarısını değerlemek için kullanılıyor:

- **Doğruluk (Accuracy)**, doğru sınıflandırılan örneklerin toplam örnek sayısına oranını ifade eder. Ancak, dengesiz veri setlerinde yanıltıcı olabilir, bu yüzden diğer metrikler de göz önünde bulundurulmuştur.
- **Precision (Kesinlik)**, modelin doğru olarak sınıflandırdığı pozitif örneklerin, tüm pozitif olarak sınıflandırdığı örneklere oranıdır. Bu metrik, modelin yanlış pozitif sonuçlarını minimize etme başarısını ölçer.
- **Recall (Hassasiyet)**, gerçek pozitif örneklerin, model tarafından doğru şekilde pozitif olarak sınıflandırılan örneklerle oranını gösterir. Bu metrik, modelin yanlış negatif sonuçlarını minimize etme başarısını yansıtır.
- **F1-score**, precision ve recall arasında bir denge sağlayan bir ölçüdür. Özellikle dengesiz veri setlerinde modelin genel performansını daha doğru bir şekilde yansıtır.

Bu metriklerin hesaplanmasından sonra, elde edilen sonuçlar aşağıdaki gibi özetlenmiştir:



Sınıflandırma Raporu:

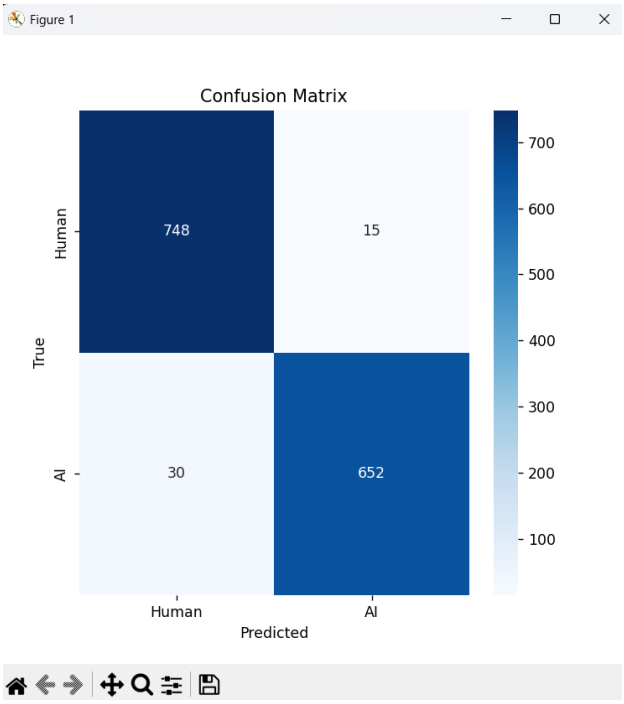
	precision	recall	f1-score	support
0	0.96	0.98	0.97	763
1	0.98	0.96	0.97	682
accuracy			0.97	1445
macro avg	0.97	0.97	0.97	1445
weighted avg	0.97	0.97	0.97	1445

Modelin Genel Doğruluğu: 0.9689

Şekil 2: Sınıflandırma Raporu

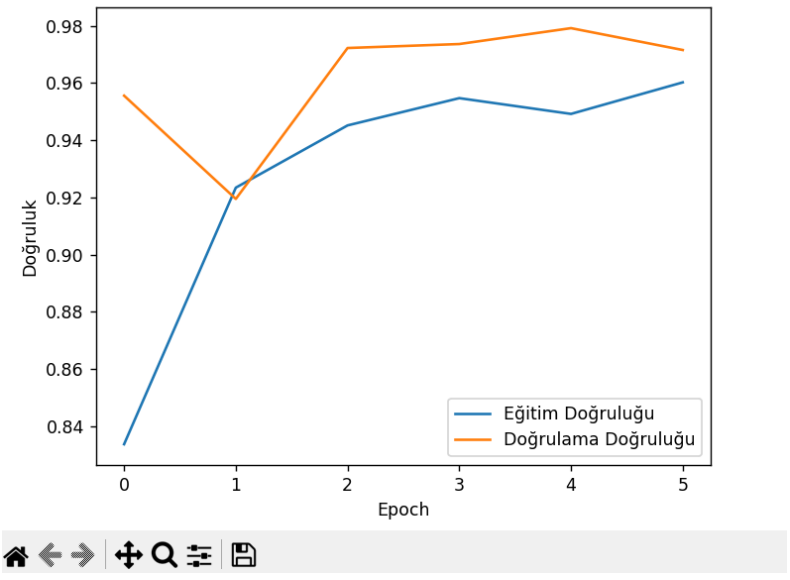
Bu sonucun gösterdiği üzere modelin doğru sınıflandırma konusunda oldukça başarılı olduğunu ve her iki sınıfa da dengeli bir performans sergilediğini ifade etmektedir. Yüksek F1-Skor'u modelin hem kesinlik hem de hatırlama konusunda denge sağladığını ve yanlış pozitif veya yanlış negatif sınıflandırmaların minimize edildiğini göstermektedir.

Modelin sınıflandırma hatalarını görselleştirmek için karışıklık matrisine başvuruldu. Karışıklık matrisinde doğru ve yanlış sınıflandırılan sınıflar net bir şekilde belirtilir ve hataların tipini anlamak için önemli bir araç olarak kullanılır. Gerçek pozitif (TP), yanlış pozitif (FP), gerçek negatif (TN) ve yanlış negatif (FN) değerleri modelin performansını detaylı bir şekilde değerlemek için incelenir. matris içermektedir:



Şekil 3: Karışıklık Matrisi

Zamanla eğitim ve doğru verinin değişen doğru oranını izlemek önemlidir çünkü bu modelin sürekli olarak öğrenme sürecini gösterir. Aşağıda yer alan grafik her dönem sonunda modelin eğitim ve doğru veriler üzerindeki doğru oranlarını göstermektedir.



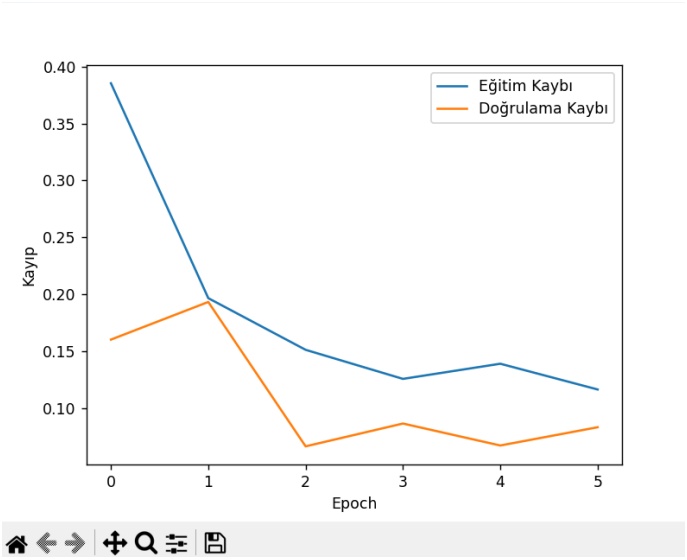
Şekil 4: Doğruluk Grafiği

Grafik Analizi:

Grafikte eğitim sürecinin başından sonuna kadar eğitim doğru oranının artan bir trend gösterdiği görülmektedir. Eğitim doğru oranı modelin eğitim verilerini daha iyi kavradığını ve hatalarını azalttığını göstermektedir. Ancak doğulama doğru oranı başlangıçta küçük dalgalanmalara sahip olsa

da genel olarak artış göstermektedir. Doğulama doğru oranındaki bu artış modelin genelleme kabiliyetinin geliştiğini ve doğulama verilerinde başarılı sonuçlar elde ettiğini ortaya koymaktadır.

Modelin aşırı öğrenme sorunuyla karşılaşmadığı gözlendi ve doğulama verisinde yüksek doğru değerlerine ulaştı. Eğitim esnasındaki kayıpla izlenmesinde olan modelin ne derece iyi optimize edildikleri anlamamızı sağlar. Eğitim kayıpları ve doğulama arasındaki ilişkilerin incelenmesinin modelin overfitting veya underfitting yapıyor olup olmadığını gösterir.



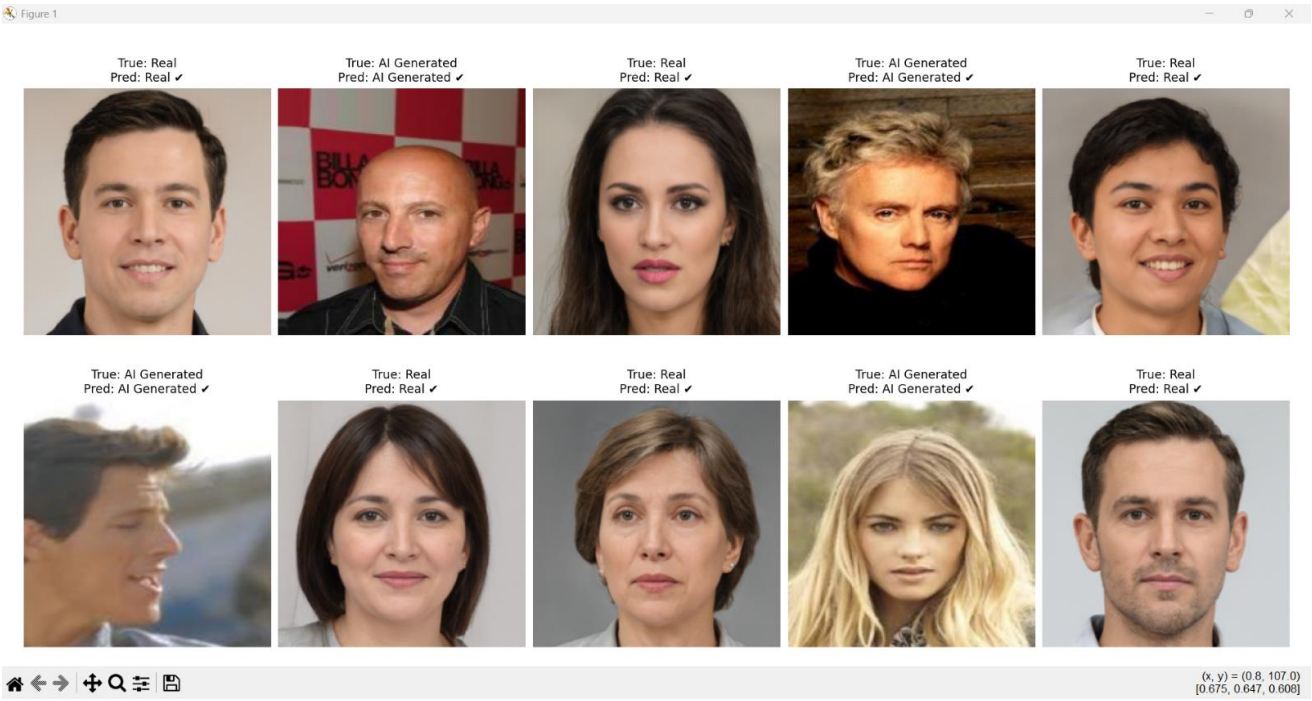
Şekil 5: Kayıp Grafiği

Grafik Analizi:
Bu gösterimde yer alan verilerde epoch sayısının artmasıyla birlikte eğitim kayıplarının azaldığı ve modelin zamanla daha iyi optimize olduğunu gösteren bir eğilim görülüyor. Eğitim kayıpları her epoch sonunda düşük bir seviyeye ulaşıyor ve hata oranını azaltıyor.

Modelin doğru veriler üzerinde hataları azaltmasına rağmen bazı durumlarda iyileştirilebilir olduğunu gösteren doğru kayıp benzer şekilde düşmektedir ancak küçük dalgalanmalara sahiptir. Bu durum eğitimin ve doğru kayıpları arasındaki küçük artış modelin genellemelerinin güçlenebilir olduğunu ancak küçük geliştirmelere ihtiyaç duyduğu anlamına gelebilir.

6. Sonuçların Değerlendirilmesi

Model sonucunda elde edilen CNN modelinin insan ve yapay zeka yüzleri arasındaki farkları başarılı bir şekilde sınıflandırdığı ve yüksek doğruluk oranları ile etkin sonuçlar verdiği gözlemlendi. Eğitim sürecinde kaydedilen doğruluk ve kayıp değerleri modelin yeterince optimize edildiğini ve iyi bir genelleme yeteneğine sahip olduğunu gösteriyor. Bu model benzer görevlerde kullanılabilir ve daha ileri düzeyde geliştirilebilir bir yapıya sahiptir.



Şekil 6: Gerçek ve Tahmin Sonuçlarının Karşılaştırılması

7. Modelin Geleceği ve Uygulama Alanları

Yüksek doğru oranı ve F1 skoru elde edildikten sonra modelin gelecek için büyük bir potansiyel sunduğunu söylemek mümkündür. Bu model özellikle sahte yüzlerin tanınması gereken güvenlik uygulamalarında kullanılabilir ve yüz tanıma teknolojilerinde büyük öneme sahip olabilir. Örneğin bu model video güvenlik sistemleri veya biyometrik kimlik doğruyla sistemlerinde uygulanabilir olabilir.

8. Kısıtlamalar ve Gelecekteki Çalışmalar

Bu proje temel performansı başarılı bir şekilde gösterdi ancak modelin doğruluğunu arttırmak için verinin çeşitlenmesi (Data Augmentation), daha kompleks modeller ve transfer öğrenme gibi ek çalışma yapılabilir.

KAYNAKÇA

[1] Khodabakhsh, A., Ramachandra, R., Pflug, A., & Busch, C. (2018). Fake face detection methods for deepfakes and GAN generated faces. In Proceedings of the 2018 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1–6).

[2] Li, Y., Chang, M. C., & Lyu, S. (2020). In Ictu Oculi: Exposing AI-created fake videos by detecting eye blinking. CVPR Workshops, 12(3), 1–8.

[3] Liu, Y., Jourabloo, A., Liu, X., & Ren, X. (2018). Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 389–398).

[4] Yang, X., Zhang, Y., & Xu, L. (2019). Face spoof detection using fusion of LBP and optical flow features. Multimedia Tools and Applications, 78(3), 3051–3071.

[5] Wang, J., He, R., & Wang, Y. (2020). A comparative study on deep learning and transfer learning for face anti-spoofing. *Neural Computing and Applications, 32*(4), 1–12.

[6] Rosebrock, A. (2018). Deep learning for computer vision with Python. PyImageSearch.
Wang, J., He, R., & Wang, Y. (2020). A comparative study on deep learning and transfer learning for face anti-spoofing. Neural Computing and Applications, 32(4), 1–12.

[7] Yang, X., Zhang, Y., & Xu, L. (2019). Face spoof detection using fusion of LBP and optical flow features. *Multimedia Tools and Applications, 78*(3), 3051–3071.

[8] Kim, J., Park, H., & Kim, S. (2017). Masked fake face detection using radiance-based albedo estimation. *IEEE Transactions on Information Forensics and Security, 12*(4), 789–801.

[9] Salman, F. M., & Abu-Naser, S. S. (2022). Classification of real and fake human faces using deep learning.

[10] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[11] Glorot, X., Bordes, A., & Bengio, Y. (2011). Deep sparse rectifier neural networks. In Proceedings of the 14th International Conference on Artificial Intelligence and Statistics (AISTATS) (Vol. 15, pp. 315–323).

[12] Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet classification with deep convolutional neural networks. In Proceedings of the 25th International Conference on Neural Information Processing Systems (NIPS) (pp. 1097–1105).

[13] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. Journal of Machine Learning Research, 15, 1929–1958.

[14] Ciresan, D., Meier, U., Masci, J., Gambardella, L., & Schmidhuber, J. (2010). Convolutional neural network committees for handwritten character classification. In Proceedings of the 20th International Conference on Artificial Neural Networks (ICANN) (pp. 147–156).