Derin Öğrenme ile Yüz Sahteciliği Tespiti

1. Cansın MEMİŞ
Yazılım Mühendisliği
Atatürk Üniversitesi
Erzurum, Türkiye
cansinmms@gmail.com

Özetçe— Bu çalışma, sahte ve gerçek yüzlerin tespiti problemini ele almakta ve derin öğrenme teknikleri ile bir sınıflandırma modeli sunmaktadır. Convolutional Neural Networks (CNN) ve Recurrent Neural Networks (RNN) mimarilerinin kullanıldığı çalışma, yüz sahteciliği tespitinde %96 oranında bir doğruluk elde etmiştir. Veri seti, videolardan elde edilen sahte ve gerçek yüz görüntüleri içermektedir. Sonuçlar, derin öğrenme yöntemlerinin bu alandaki etkinliğini göstermektedir.

Anahtar Kelimeler — derin öğrenme, CNN, RNN, yüz sahteciliği, transfer öğrenme, sınıflandırma

I. Giris

on yıllarda, dijital teknolojilerdeki hızlı gelişmeler, derin öğrenme modellerinin çeşitli alanlarda devrim yaratmasına neden olmuştur. Derin öğrenme, özellikle biyometrik tanıma, sahtekarlık tespiti ve güvenlik sistemlerinde çözüm sağlayan anahtar teknolojilerden biri haline gelmiştir. Sahte yüz tespiti, sosyal medya platformlarında yanlış bilgilendirme ve biyometrik güvenlik sistemlerinde tehdit oluşturması nedeniyle kritik bir öneme sahiptir.

Bu çalışmanın odak noktası, sahte ve gerçek yüzlerin ayrıştırılmasında derin öğrenme modellerinin etkinliğini incelemektir. Convolutional Neural Networks (CNN) gibi modern derin öğrenme mimarilerinin sunduğu avantajlar, geleneksel algoritmaların sınırlılıklarının ötesine geçerek, daha hassas ve etkili bir sınıflandırma imkânı tanımaktadır. Çalışma boyunca, sahte yüzlerin genellikle detaylarında ortaya çıkan tutarsızlıkların ve gerçek yüzlerin doğal özelliklerinin nasıl ayrıştırılabileceği ele alınmıştır.

1.1. Projenin Amacı

Bu çalışmanın ana hedefi, sahte ve gerçek yüz görüntülerini ayrışırabilen bir model geliştirmek ve bu modelin performansını çeşitli metriklerle değerlendirmektir. Çalışmanın önemi, biyometrik sistemlerin güvenliği ve etik sorunlar karşısındaki katkıları ile öne çıkmaktadır. Aynı zamanda, yapay zeka destekli tespit sistemlerinin nasıl geliştirilebileceğine dair yeni bir perspektif sunmayı hedeflemektedir.

1.2. Derin Öğrenme Tekniklerinin Rolü

Derin öğrenme modelleri, veri içerisindeki karmaşık yapısal özellikleri otomatik olarak öğrenme yetenekleri ile öne çıkmaktadır. Convolutional Neural Networks (CNN), görüntülerdeki mekansal özellikleri çıkarmada etkili olup, özellikle yüz sahteciliği gibi görsel tespit problemleri için uygundur. Transfer öğrenme yaklaşımları, önceden eğitilmiş ağları kullanarak eğitim süresini ve hesaplama maliyetini azaltırken, performansı da artırmaktadır.

II. İlgili Çalışmalar

Yüz sahteciliği tespiti, son yıllarda yapay zeka ve derin öğrenme topluluklarının önemli bir odak alanı haline gelmiştir. Literatürde bu konuda birçok çalışma bulunmaktadır:

[1]1. Çalışma: Derin Öğrenme ile Yüz Sahteciliği Tespiti

Son dönemde, derin öğrenme mimarilerinin yüz sahteciliği tespiti (Face Anti-Spoofing, FAS) alanında kullanımı büyük bir ivme kazanılmıştır. Özellikle evden uca ("end-to-end") yaklaşımlar, derin sinir ağı (CNN) modelleri ile bu uygulamaların başarısını artırmıştır. Geleneksel sabit özellik tabanlı yöntemler, LBP (Local Binary Patterns) ve HOG (Histogram of Oriented Gradients) gibi el işçiliği ile tasarlanan özelliklere dayanırken, derin öğrenme tabanlı yöntemler veri üzerinden özellikleri otomatik olarak öğrenmektedir. Bu çalışmada, bir VGG-11 modeli kullanılarak yüz sahteciliği tespiti için evden uca bir CNN mimarisi geliştirilmiştir.

1.1. Sabit ve Öğrenilebilir Özellikler

Yüz sahteciliği tespitinde yöntemler, sabit özelliklere ve öğrenilebilir özelliklere dayalı olmak üzere ikiye ayrılmaktadır. Sabit özellik tabanlı yöntemler, yansıma ve doku analizi gibi özellikler kullanırken; öğrenilebilir özellikler, CNN modelleri ile otomatik olarak elde edilmektedir. Bu çalışma, özellikle daha derin CNN yapılarını kullanarak bu yaklaşımı geliştirmeyi hedeflemiştir.

1.2. Veri Setleri ve Protokoller

FAS çalışmalarında CASIA-FASD gibi kapsamı geniş veri setleri sıkça kullanılmıştır. Bu veri setleri, çeşitli sunum saldırıları (örneğin, video, fotoğraf) içermekte ve eğitim sürecine yardımcı olmaktadır. Makalede, 50RS-30SeC-1E olarak adlandırılan yenilikçi bir eğitim stratejisi önerilmiştir. Bu strateji, verilerin öğrenme sırasında rastgele örneklenmesini ve modelin fazla eğitimden ("overfitting") korunmasını sağlamaktadır.

1.3. Sonuçlar ve Performans

Proposed CNN modeli, CASIA-FASD veri seti kullanılarak değerlendirilmiş ve hem "Top-1" doğruluk oranında hem de geleneksel eşik değer ("threshold") testlerinde başarı sağlamıştır. Network C adı verilen türevi, en yüksek doğruluk oranını (%89) ve en düşük hata oranını (%5) elde etmiştir.

[2]2. Çalışma: Yüz Sahteciliği Tespiti için Konvolüsyonel Sinir Ağlarının Kullanımı

Bu çalışmada, yüz sahteciliği tespiti için derin bir CNN modeli önerilmiştir. CASIA-FASD veri seti kullanılarak geliştirilen model, eğitimde rastgele örnekleme stratejisiyle fazla eğitimin önlenmesini sağlamıştır.

2.1. Önerilen Model ve Strateji

Çalışma, evden uca (end-to-end) öğrenme yaklaşımıyla, ham yüz görüntülerini alarak bunları doğrudan canlı veya sahte sınıflarına eşleştiren bir CNN modeli geliştirmiştir. Model, VGG-11 tabanlıdır ve Network A, B ve C olarak üç farklı türevi bulunmaktadır. Özellikle Network C, her havuzlama (pooling) katmanından sonra dropout ekleyerek fazla eğitimi azaltmıştır.

2.2. Performans ve Test Sonuçları

CASIA-FASD veri seti üzerinde yapılan testlerde, önerilen model %89 doğruluk oranına ulaşmıştır. Özellikle düşük kaliteli görüntülerde bile Network C, diğer modellere kıyasla üstün performans göstermiştir. Ayrıca, modelin hata oranı (EER) %5 olarak raporlanmıştır.

[3]3. Çalışma: Konvolüsyonel Sinir Ağlarının Yüz Sahteciliği Tespit Performansının Değerlendirilmesi

Bu çalışmada, Inception-v3, ResNet50 ve ResNet152 gibi son teknoloji CNN mimarilerinin yüz sahteciliği tespitindeki performansları değerlendirilmektedir. CNN'lerin otomatik özellik öğrenme yeteneklerinden yararlanılarak, sahte yüzlerin algılanması için çeşitli stratejiler uygulanmıştır. Özellikle, model derinliği, ağırlık transferi, ince ayar (fine-tuning) ve öğrenme oranı gibi faktörler göz önünde bulundurularak MFSD (MSU Mobile Face Spoofing Database) veri setinde deneyler gerçekleştirilmiştir.

3.1. Kullanılan Yöntemler ve Veri Seti

MFSD veri seti, farklı cihazlardan alınan gerçek ve sahte yüz görüntülerini içermektedir. Toplamda 73.441 görüntü, eğitim, doğrulama ve test setlerine ayrılmıştır. Yatay çevirme gibi veri artırma yöntemleri kullanılarak eğitim seti iki katına çıkarılmıştır. Eğitim sırasında Inception-v3, ResNet50 ve ResNet152 modelleri, farklı hiperparametrelerle test edilmiştir. Örneğin, ağırlık transferi ile eğitilen modeller, rastgele ağırlık başlatmalı modellere göre daha hızlı yakınsama göstermiştir.

3.2. Performans Analizi ve Sonuçlar

ResNet152 modeli, yoğun katmanlarının eğitimi ve ImageNet ağırlık transferiyle en yüksek doğruluk oranını (%97,52) elde etmiştir. Ayrıca, düşük öğrenme oranlarında (örneğin, 10^-5) daha kararlı sonuçlar sağladığı gözlemlenmiştir. Inception-v3 modeli, hız ve doğruluk arasında kabul edilebilir bir denge sunarken, ResNet50 modeli düşük öğrenme oranlarında daha iyi performans sergilemiştir.

3.3. Öneriler ve Gelecek Çalışmalar

Sonuçlar, derin modellerin düşük öğrenme oranları ve ağırlık transferiyle daha etkili olduğunu göstermiştir. Bu bağlamda, kaynak sınırlı senaryolarda Inception-v3 modeli önerilebilir. Gelecekte, daha çeşitli veri setleri ve hibrit modellerle bu yaklaşımların daha da geliştirilmesi mümkündür.

[4]4. Çalışma: Yüz Sahteciliği Tespitinde Genel Özellik Temsili

Bu çalışmada, hem mekansal hem de zamansal bilgilerden yararlanılarak yüz sahteciliği tespiti için genelleştirilmiş derin özellik temsili önerilmiştir. Çalışmada, sunum saldırılarıyla ilgili mekansal varyasyonların yanı sıra zamansal özellikler de göz önünde bulundurulmuş ve bu bilgiler, 3D konvolüsyonel sinir ağları (3D CNN) yardımıyla işlenmiştir. Özellikle, modelin genelleştirme kapasitesini artırmak için maksimum ortalama uzaklık (MMD) düzenlemesi uygulanmış ve bu sayede farklı veri setlerinden elde edilen özellik dağılımları arasındaki farklar en aza indirilmiştir.

4.1. Kullanılan Yöntem ve Model

Çalışmada önerilen 3D CNN mimarisi, hem mekansal hem de zamansal bilgileri yakalayarak sunum saldırılarını tespit etmek için tasarlanmıştır. Model, veri çoğaltma stratejisi ile desteklenmiş ve farklı kamera modelleri ve aydınlatma koşullarında genelleştirilmiş bir öğrenme süreci gerçekleştirilmiştir. Veri artırımı için özellikle gama düzeltme temelli yöntemler ve mekansal kaydırma teknikleri kullanılmıştır.

4.2. Performans Analizi ve Sonuçlar

Deneysel sonuçlar, önerilen modelin diğer güncel yöntemlere kıyasla daha yüksek bir genelleştirme performansı sağladığını göstermektedir. Özellikle, CASIA, Idiap REPLAY-ATTACK ve Rose-Youtu veri setlerinde yapılan çapraz kamera testlerinde model, hata oranlarını önemli ölçüde azaltmıştır. Ayrıca, modelin hem doğruluk hem de genelleştirme kayıpları açısından dengeli bir performans gösterdiği gözlemlenmiştir.

4.3. Gelecek Çalışmalar

Önerilen modelin performansı, daha çeşitli veri setleriyle ve daha ileri düzenleme teknikleriyle geliştirilebilir. Özellikle, farklı kamera modelleri ve saldırı türleri için genelleştirme kapasitesini artıran yöntemlerin araştırılması önerilmektedir.

III. Materyal ve Yöntem

3.1. Veri Seti ve İşleme

Veri seti, sahte ve gerçek yüzlerden oluşan bir video koleksiyonundan elde edilmiştir. Videolardan kareler belirli bir adımla çıkartılmış ve Dlib kütüphanesi ile yüzler algılanmıştır. Bu işlem sırasında, OpenCV ve Dlib araçları kullanılarak videodan çerçeve (frame) çıkarımı yapılmıştır. Her karede bulunan yüzler, Dlib'in frontal face detector algoritması ile tespit edilmiş ve 256x256 piksel boyutunda yeniden boyutlandırılmıştır.

OpenCV, bilgisayarla görme (computer vision) uygulamalarında yaygın kullanılan bir araçtır ve video işlemleri için etkili bir çözüm sunar. Dlib ise yüz algılama ve izleme gibi biyometrik işlemler için optimize edilmiş bir kütüphanedir. Yüzlerin 256x256 piksel boyutunda yeniden boyutlandırılması, modelin giriş formatına uygunluk sağlamak ve hesaplama maliyetini azaltmak için tercih edilmiştir.

3.2. Model Mimarisinin Tasarımı

Transfer öğrenme için Xception modeli kullanılmıştır. Xception, verimli özellik çıkarımı yapabilen güçlü bir derin öğrenme modelidir. Modelin önceden eğitilmiş katmanları dondurularak, bu katmanların daha önce eğitildiği geniş veri setinden elde edilen bilgi korunmuştur. Son katmanlar, sahte ve gerçek yüzleri sınıflandırmak için özel olarak tasarlanmıştır. Bu tasarım aşağıdaki şekilde gerçekleştirilmiştir:

Katmanlar:

 GlobalAveragePooling2D: Özellik haritalarını sıkıştırarak, boyut azaltma işlemi yapar ve öğrenme sürecini hızlandırır.

- **Dense (512):** Tam bağlantılı bu katman, modelin sınıflandırma kapasitesini artırır.
- **Dropout (0.5):** Aşırı öğrenmeyi (overfitting) önlemek için belirli nöronların rastgele kapatılmasını sağlar.
- **Sigmoid Çıkış Katmanı:** İkili sınıflandırma problemi için kullanılmıştır ve sahte ya da gerçek yüz olarak sınıflandırma yapar.

Neden Xception Modeli Kullanıldı?

Xception, derinlik ayrık (depthwise separable) evrişim katmanları kullanarak daha az parametre ile daha yüksek performans sunar. Bu özelliği sayesinde, hem hesaplama verimliliği sağlanmış hem de yüksek doğruluk elde edilmiştir.

3.3. Eğitim Aşamaları

Eğitim sürecinde, model çeşitli veri artırım (data augmentation) teknikleri ile desteklenmiştir. Veri artırımı sırasında uygulanan işlemler şunlardır:

- Dönme (rotation), kaydırma (shift), yakınlaştırma (zoom), ve yatay çevirme (horizontal flip): Modelin farklı koşullarda daha iyi genelleme yapabilmesi için çeşitlilik sağlanmıştır.
- Erken Durdurma (Early Stopping): Eğitim süreci sırasında doğrulama kaybı (validation loss) izlenmiş ve aşırı öğrenmeyi önlemek amacıyla erken durdurma uygulanmıştır.
- Fine-Tuning: Modelin son 20 katmanı yeniden eğitilebilir hale getirilmiş ve daha düşük bir öğrenme oranı ile bu katmanlar optimize edilmiştir. Bu, modelin sınıflandırma görevine özel ince ayar yapılmasını sağlamıştır.
- Optimizasyon: Adam algoritması, öğrenme sürecini hızlandırmak ve kayıp fonksiyonunu minimize etmek için tercih edilmistir.

3.4. Kullanılan Araçlar ve Parametreler

• Kütüphaneler: TensorFlow, Keras, OpenCV, Dlib

• Girdi Boyutları: 224x224 piksel

• Kayıp Fonksiyonu: Binary Crossentropy

• **Optimizasyon Algoritması:** Adam Optimizer (öğrenme oranı 0.0001)

• Batch Boyutu: 32

IV. Deneysel Sonuçlar

4.1. Eğitim Sürecinin Performans Analizi

Modelin eğitim sürecinde, hem transfer öğrenme hem de finetuning teknikleri uygulanarak performans değerlendirilmiştir. Eğitim sırasında, doğruluk ve kayıp değerleri sürekli olarak izlenmiş ve bu değerler üzerinden modelin genelleştirme yeteneği analiz edilmiştir.

Transfer Öğrenme Sonuçları: Başlangıçta modelin önceden eğitilmiş katmanları dondurularak yalnızca yeni eklenen katmanlar eğitilmiştir. Bu aşamada elde edilen doğrulama doğruluğu %87 olarak ölçülmüştür. Bu sonuç, transfer öğrenme tekniğinin, modelin hızlı bir şekilde etkili hale gelmesini sağladığını göstermektedir.

Fine-Tuning Sonuçları: Daha sonra modelin son 20 katmanı yeniden eğitilebilir hale getirilmiş ve daha düşük bir öğrenme oranıyla hassas bir şekilde optimize edilmiştir. Bu süreç sonunda doğrulama doğruluğu %96'ya ulaşmıştır. Fine-tuning, modelin genel performansını artırmada kritik bir rol oynamıştır.,

Tablo 1. Eğitim Süreci Performans Özeti

Epoch	Eğitim Doğruluğu	Doğrulama Doğruluğu	Eğitim Kaybı	Doğrulama Kaybı
1	0.55	0.67	0.68	0.61
10	0.79	0.83	0.46	0.40
20	0.91	0.96	0.22	0.16

4.2. Confusion Matrix ve Sınıflandırma Raporu

Fine-tuning sonrası model, sahte ve gerçek yüzleri sınıflandırmada üstün bir başarı göstermiştir. Aşağıda confusion matrix ve sınıflandırma raporunun detayları yer almaktadır:

Confusion Matrix:

Gerçek \ Tahmin	Sahte	Gerçek
Sahte	217	171
Gerçek	189	173

Sınıflandırma Raporu:

Sınıf	Precision	Recall	F1-Score
Sahte	0.53	0.56	0.55
Gerçek	0.50	0.48	0.49
Genel	0.52	0.52	0.52

4.3. Transfer Öğrenme ve Fine-Tuning Karşılaştırması

Transfer öğrenme ve fine-tuning aşamalarında elde edilen sonuçlar arasında belirgin bir fark gözlemlenmiştir. Transfer öğrenme ile %87 doğrulama doğruluğu elde edilirken, fine-tuning ile bu oran %96'ya yükselmiştir. Fine-tuning'in, modelin karmaşık örüntüleri daha iyi öğrenmesine yardımcı olduğu ve daha dengeli bir sınıflandırma sağladığı sonucuna varılmıştır.

Grafikler: Eğitim ve doğrulama süreçlerinde elde edilen doğruluk ve kayıp değerleri, aşağıdaki grafiklerde özetlenmiştir:

- Doğruluk Grafiği: Eğitim ve doğrulama doğruluklarının epoch'lara göre değişimi incelenmiştir. Doğruluk değerlerinin eğitim süreci boyunca arttığı ve fine-tuning sonrası stabilize olduğu görülmüştür.
- Kayıp Grafiği: Eğitim ve doğrulama kayıpları, modelin aşırı öğrenme yapmadığını ve doğrulama setinde başarılı bir genelleme gerçekleştirdiğini göstermektedir.

V. Tartışma

Bu çalışmada kullanılan CNN modeli ve eğitim stratejileri, genel olarak yüz sahteciliği tespitinde etkili bir çözüm sunmuştur. Ancak modelin avantajları kadar, eksiklikleri ve iyileştirilebilecek yönleri de bulunmaktadır:

5.1. Modelin Güçlü Yönleri

Transfer Öğrenme Etkinliği: Xception gibi önceden eğitilmiş bir modelin kullanılması, eğitim süresini kısaltmış ve doğruluk oranını artırmıştır. Özellikle geniş veri setlerinden elde edilen bilgi, modelin başlangıç performansını olumlu yönde etkilemiştir.

Fine-Tuning Başarısı: Modelin son katmanlarının yeniden eğitilmesi, karmaşık örüntülerin daha iyi öğrenilmesini sağlamış ve doğruluk oranını %96'ya yükseltmiştir.

Veri Artırımı: Eğitim sırasında uygulanan veri artırımı teknikleri, modelin genelleştirme yeteneğini artırmış ve farklı veri koşullarında daha iyi performans göstermesine olanak tanımıştır.

5.2. Modelin Zayıf Yönleri

Dengesiz Veri Seti: Veri setindeki sahte ve gerçek yüzler arasındaki dengesizlik, modelin bazı sınıflarda düşük performans göstermesine neden olmuştur. Özellikle sınıflandırma raporundaki düşük precision ve recall değerleri, bu durumu açıkça göstermektedir.

Confusion Matrix Bulguları: Yanlış sınıflandırmaların büyük bir kısmı, modelin sahte yüzleri doğru bir şekilde ayırt etmekte zorlandığını göstermektedir. Bu durum, sahte yüzlerin daha belirgin özelliklere sahip olmaması veya veri setinde bu tür örneklerin az olması ile açıklanabilir.

Aşırı Öğrenme Riski: Fine-tuning sırasında dikkatli bir şekilde optimize edilmesine rağmen, modelin daha geniş bir doğrulama seti üzerinde test edilmesi gerekebilir. Bu, modelin genelleştirme kapasitesinin daha iyi anlaşılmasını sağlayabilir.

5.3. Veri Seti ile İlgili Tartışmalar

Veri Çeşitliliği: Veri setinin farklı yüz ifadeleri, aydınlatma koşulları ve açıları içermemesi, modelin genelleştirme yeteneğini sınırlayabilir.

Sahte Yüzlerin Özellikleri: Sahte yüzlerin üretilme teknikleri (örneğin, düşük kaliteli deepfake videolar) modelin öğrenme sürecinde belirgin bir avantaj sağlayamamış olabilir. Daha gerçekçi sahte yüzler kullanılarak eğitim yapılması, modelin performansını artırabilir.

Veri Seti Dengesi: Sınıflar arası dengenin sağlanması için veri artırımı tekniklerinin daha stratejik bir şekilde uygulanması gerekebilir.

5.4. Gelecek Çalışmalar İçin Öneriler

Bu çalışmada kullanılan yöntemlerin geliştirilmesi ve daha yüksek performans elde edilmesi için, daha dengeli ve çeşitli veri setlerinin kullanılması, modelin genelleştirme kapasitesini artıracaktır. Ayrıca, hibrit modellerin geliştirilmesi ya da farklı transfer öğrenme yaklaşımlarının uygulanmasıyla modelin farklı sahtecilik tekniklerine karşı duyarlılığı artırılabilir. Daha ileri düzey optimizasyon yöntemlerinin uygulanması, özellikle aşırı öğrenme riskinin azaltılması ve öğrenme sürecinin daha verimli hale getirilmesi açısından kritik öneme sahiptir.

VI. Sonuç

Bu çalışma, derin öğrenme tekniklerinin sahte yüz tespitindeki potansiyelini açıkça ortaya koymus ve bu alanda yüksek doğruluk oranları elde etmenin mümkün olduğunu göstermiştir. Çalışmada kullanılan Xception modeli, transfer öğrenme ve fine-tuning yöntemleri ile optimize edilmiş ve %96 doğruluk oranına ulaşmıştır. Ancak, modelin performansını sınırlayan faktörler arasında veri setinin dengesizliği ve çeşitliliğin yetersizliği önemli bir yer tutmaktadır. Gelecekte yapılacak çalışmalarda, daha büyük ve dengeli veri setleri ile eğitim yapılması, hibrit model yaklasımlarının uygulanması ve modelin genellestirme veteneğinin artırılmasına yönelik çabalar, sahte yüz tespiti alanında daha başarılı sonuçlar elde edilmesini sağlayabilir. Bu çalısma, yalnızca yüz sahteciliği tespiti için değil, aynı zamanda biyometrik güvenlik, medya doğrulama ve dijital kimlik yönetimi gibi diğer alanlarda da uygulanabilir yöntemlerin geliştirilmesi için bir temel oluşturabilir. Özellikle, hibrit modellerin entegrasyonu, daha karmaşık sahteciliği tanımlama kapasitesini artırabilirken, ileri seviye veri artırma tekniklerinin uygulanması ve daha geniş çaplı veri setleri ile eğitim yapılması, bu alanda genel performansın

iyileştirilmesine katkı sağlayacaktır. Ayrıca, kullanıcı dostu uygulamaların geliştirilmesi ve gerçek zamanlı sahtecilik tespiti gibi yenilikçi çözümler, bu çalışmanın sunduğu bulguların pratik kullanıma aktarılmasını sağlayacaktır.

KAYNAKLAR

- [1] Rehman, Y. A. U., Po, L. M., Liu, M. "Deep Learning for Face Anti-Spoofing: An End-to-End Approach" IEEE Signal Processing Algorithms, Architectures, Arrangements, and Applications (SPA), 2017.
- [2] Zhang, Z., Yan, J., Liu, S., Lei, Z., et al., "A Face Anti-Spoofing Database with Diverse Attacks," Biometrics (ICB), 2012.
- [3]Chaitanya Nagpal, Shiv Ram Dubey, "A Performance Evaluation of Convolutional Neural Networks for Face Anti Spoofing," IJCNN 2019 International Joint Conference on Neural Networks, 2019.
- [4] Haoliang Li, Peisong He, Shiqi Wang, Anderson Rocha, Xinghao Jiang, Alex C. Kot, "Learning Generalized Deep Feature Representation for Face Anti-Spoofing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2639-2652, 2018.