



ÖZET

Sahte Fotoğraf Analizi projesi, analiz ve yapay zeka teknikleri kullanılarak sahte fotoğrafların tespitine odaklanmaktadır. Günümüzün dijital ortamında manipüle edilmiş görüntülerin yaygınlığı, bu tür örnekleri tanımlamak ve işaretlemek için etkili yöntemler gerektirmektedir. Sahte fotoğraf algılama için kapsamlı bir çözüm sunmayı amaçlayan bu proje, kullandığı metodolojilerle yüksek doğrulukta sonuçlar vermek için gerçekleştirilmiştir. Bu metodolojilerin entegrasyonu, hata seviyelerindeki tutarsızlıkları tespit ederek ve manipülasyonları gösteren kalıpları öğrenmek için derin bir sinir ağını eğiterek manipüle edilmiş görüntülerin tanımlanmasını sağlar. Kapsamlı deneyler ve değerlendirmeler yoluyla bu proje, yanlış bilgilerin yayılmasıyla mücadele etmek ve görsel içeriğin bütünlüğünü korumak için güvenilir ve sağlam bir yaklaşım sunarak sahte fotoğraf tespitinin ilerlemesine katkıda bulunmayı amaçlamaktadır.

GİRİŞ

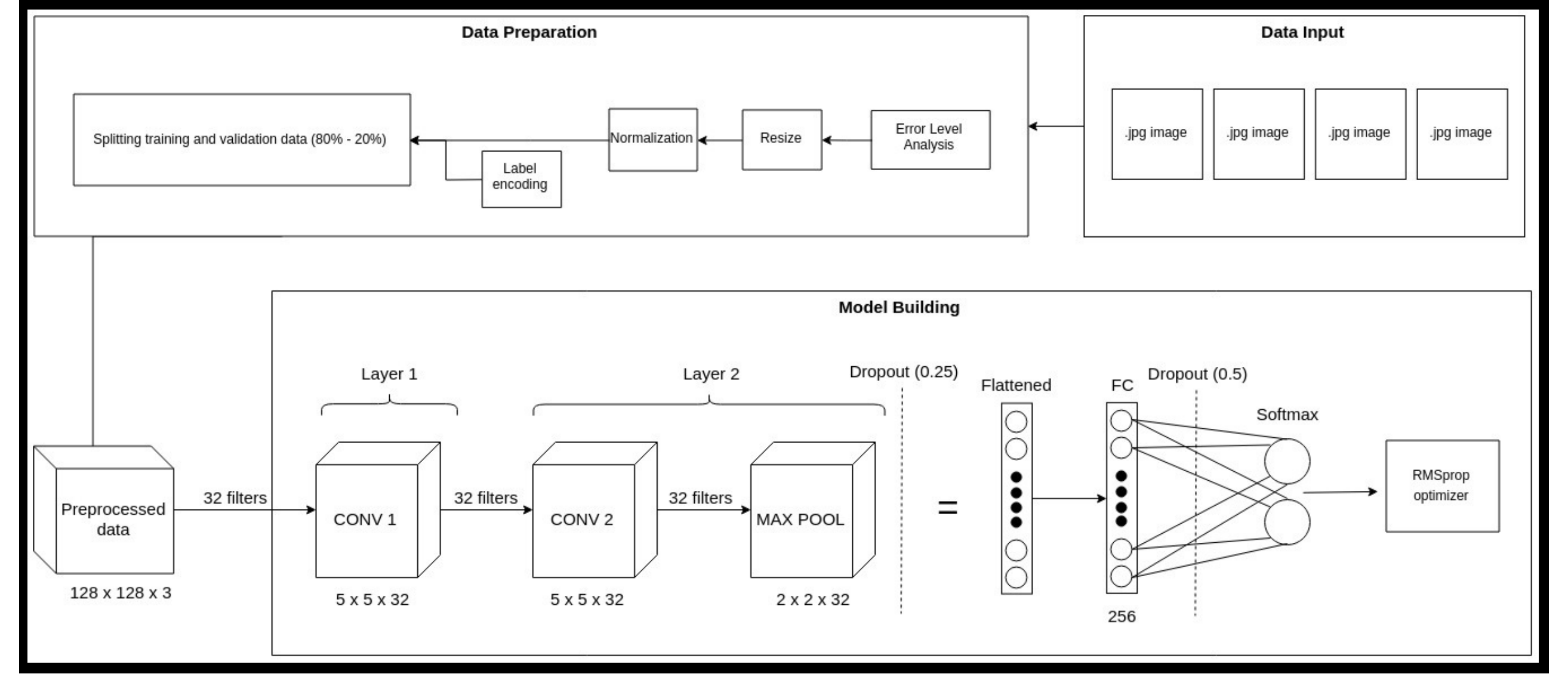
Yapay zekanın ve makine öğrenmesi algoritmalarının gelişmesi ile daha gerçekçi hale gelen derin sahte içerikler tehlikeli hale gelmektedir. Büyük öneme sahip olan bu teknoloji aynı zamanda hukuki anlamda siber güvenlik sorunlarında da ciddi bir role sahiptir. Sahte Fotoğraf Analizi projesi, kullanıcıların programa yüklediği görsellerin meta veri analizi, Hata Seviyesi Analizi (ELA) ve Derin Öğrenme teknikleri kullanılarak sahte olup olmadığının analizini gerçekleştiren bir uygulama olarak geliştirilmiştir. Daha önce yapılan çalışmalar sahte fotoğrafların analizlerine ciddi katkılarda bulunmuştur. "Forged Face Detection using ELA and Deep Learning Techniques"[1] çalışmasında ELA ve CNN bazlı bir model kullanılarak fotoğrafların sahtelik analizinde yüksek doğrulukta sonuçlar elde edilmiştir. Fakat dosya bilgileri göz önüne alınmadığından hızlıca analiz edilebilecek durumlar göz ardı edilmiştir. "Fake Image Detection Using Machine Learning" çalışmasında ise meta veriler ve dosya bilgilerine de yer verilmiştir. Fakat bu projede de Whatsapp, Google+ gibi önemli platformlardaki görsellerde hatalı sonuçlar söz konusudur. Bu projede, daha önceki eksiklikleri gidermek için meta veri analizi, hata seviyesi analizi, ve yapay zeka modeliyle birlikte 3 farklı analiz tekniği kullanılmıştır. Bu da kullanıcıların yöntem seçimindeki hata payına taviz vermeden doğru sonuçlara erişebilmelerine olanak sağlayacaktır.

YÖNTEM

Proje kapsamında sahteliği ölçmek amacıyla 3 yöntem kullanılmıştır. Bu yöntemler sırasıyla;

- Metadata Analizi: Metadata analizi, bir fotoğrafın içerdiği teknik bilgilerin incelenmesidir ve manipülasyon belirtilerini tespit etmek için kullanılır. Fotoğraflar üzerinde yapılan değişiklikler metadata analizi ile ortaya çıkarılabildiğinden, sahte fotoğrafların tespitinde önemli bir rol oynar.
- ELA Analizi: Error Level Analysis (ELA) analizi, fotoğrafların manipülasyon izlerini tespit etmek için kullanılan bir yöntemdir ve fotoğrafların sıkıştırma seviyeleri arasındaki hata düzeylerini karşılaştırır.
- Yapay Zeka Analizi: Yapay zeka analizi, önceden eğitilmiş sinir ağı modelleri kullanarak fotoğrafların sahte olup olmadığını tespit etmek için kullanılan bir yöntemdir. Derin öğrenme tekniklerinin uygulandığı yapay zeka analizi, fotoğraflardaki sahtecilik belirtilerini algılayarak yüksek doğruluk oranlarına ulaşabilmektedir.

Bu yapılan uygulamalar, proje kapsamında kullanılan yöntemlerin teorik temellerini oluştururken, her bir yöntemin sahte fotoğrafların tespit etme amacı farklıdır.



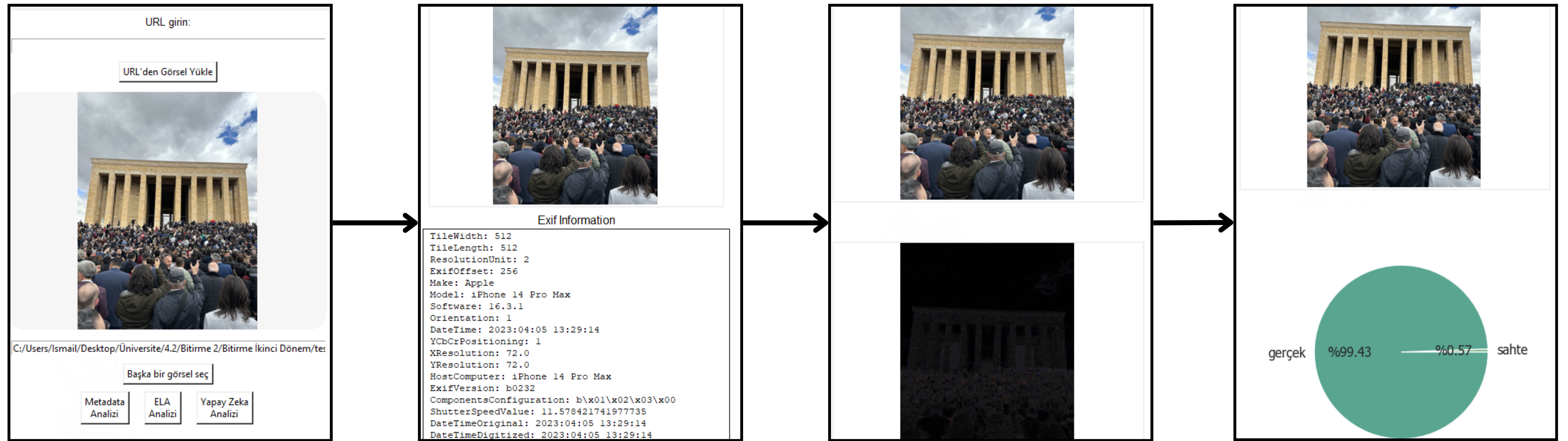
GERÇEKLEŞTİRİLEN ÇALIŞMA

Sahte fotoğraf analizi projesinde seçilen görselin sahtelik analizi gerçekleştirilir. Proje temel olarak Python dilinde programlanmıştır. Arayüz Tkinter kütüphanesi ile kodlanırken Image kütüphanesi ile görsel işlemleri gerçekleştirilmiştir. Yapay zeka aşamasında ise Keras ve TensorFlow kütüphanesi ile eğitimler gerçekleştirilmiştir. 7492 adet gerçek, 5124 adet üzerinde değişiklik yapılmış fotoğrafların bulunduğu CASIA2 veri seti ile modellerin eğitimi gerçekleştirilmiştir. Daha sonrasında test edilmesi amacıyla rastgele 200 adet görsel ilgili veri setinden çıkarılmıştır.

Program kullanıcının seçtiği görselin seçtiği yönteme göre sahtelik analizini gerçekleştirir. Metadata analizi seçtiğinde görselin EXIF bilgilerine erişilir ve bir yazılım aracılığıyla değiştirilip değiştirilmediği ekrana yansıtılır. ELA analizinde görselde değişiklik yapılmış kısımların diğer alanlardan farklı şekilde görünmesi sağlanacak bir filtre uygulanır. Yapay zeka analizinde ise CNN bazlı modelin görselle uygulanmasıyla sahtelik olasılığı yüzde olarak ekrana yansıtılır.

Programın kullanım aşamaları aşağıdaki gibidir:

- Uygulama açıldığında kullanıcı URL kısmına ilgili görselin URL'ini girer ya da istediği görseli bilgisayardan seçer.
- Kullanıcı görseli seçtikten sonra görsel ekranda görünür.
- Kullanıcı analiz yapmak istediği metodun (Metadata-ELA-Yapay Zeka) butonuna tıklar.
- Sistem, ilgili metodun algoritmalarını gerçekleştirdikten sonra sonuçları ekrana yansıtır.
- Kullanıcı fotoğrafın sahte olup olmadığı sonucuna erişir.



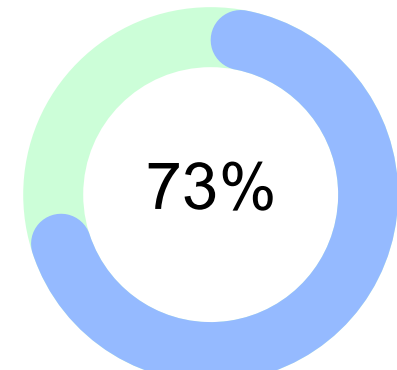
SONUÇ

Testler/Sonuçlar	Sonuç	Başarı Durumu
Çoklu Görsel Testi	Gerçek: %73 Sahte: %86 Genel: %79,5	Başarılı
Öz Çekim Testi	Gerçek: %98,31 Sahte: %0	Başarısız
Photoshop Bulanıklık Testi	Gerçek: %99,43 Sahte: %90,57	Başarılı
Photoshop/Renk Manipülasyonu Testi	Gerçek: %98,86 Sahte: %78,14	Başarılı
Photoshop/Işık Manipülasyonu Testi	Gerçek: %97,59 Sahte: %98,71	Başarılı
İnternette Alınan Görsel Testi	Gerçek: %98,44	Başarılı
Telefondan Kaydedilen ve Üzerine Metin Eklenen Görsel Testi	Sahte: %99,67	Başarılı
Birleştirilen Görsel Testi	Sahte: %95,77	Başarılı
Video Alıntısı Testi	Gerçek: %92,95	Belirsiz
Gizli Ekleme Testi	Sahte: %9	Başarısız

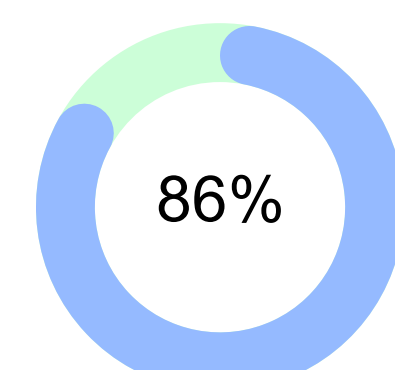
Şekil 7. Test Senaryoları ve Sonuçları Tablosu

- Geliştirilen programın farklı kullanım senaryolarında değişken başarı oranlarına sahip olduğu saptanmıştır.
- Yapay zeka modeli görsellere eklenen cisimlerin, yazıların ve filtrelerin saptanmasında yüksek başarı oranlarına sahiptir.
- Yapay zeka modeli gözle ayırt edilemeyecek değişikliklerde düşük başarı oranlarına sahip olduğundan bu gibi görsellerde metadata analizi ya da ELA analizi kullanılması daha başarılı sonuçlar verecektir.
- Yapay zeka eğitiminde kullanılan verilerin miktarı ve kalitesi yükseldikçe model daha iyi eğitildiğinden daha yüksek başarı oranları elde edilmektedir.
- Proje kendisine yakın "Forged Face Detection using ELA and Deep Learning Techniques" çalışmasına alternatif teknikler sunduğundan daha başarılı olmuştur.
- Proje günlük hayatta, sosyal medyada, iş yaşamında veya habercilik alanında test edilen senaryolarda iyi sonuçlar verdiği için günlük kullanıcıya hitap edebilmektedir.

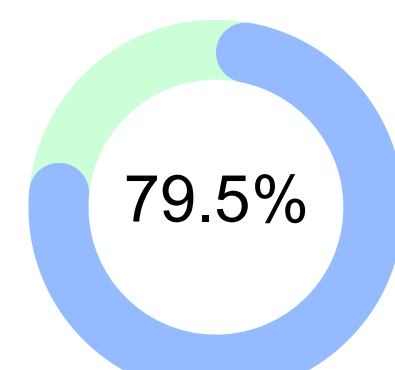
Sonuç olarak elde edilen sonuçlar göz önüne alındığında, bu projenin, gelecek çalışmalara ilgili metotlar yönünde rehberlik etmesi ve mevcut yapay zeka modelinin hem veri seti hem de model açısından iyileştirildiğinde daha başarılı sonuçlar elde etmesi beklenmektedir. Bu proje, gelecekteki sahte fotoğraf analizi projeleri için önemli bir temel oluşturan sonuçlara ve tekniklere sahiptir.



CASIA veri setinden rastgele seçilen 100 gerçek fotoğrafın doğru tahmin edilme oranı



CASIA veri setinden rastgele seçilen 100 sahte fotoğrafın doğru tahmin edilme oranı



Rastgele 200 fotoğraflık testin ortalama doğru tahmin etme oranı