GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

BM495 BİTİRME PROJESİ I

SRS DOKÜMANI

181180030 - İsmail ERTAYLAN

181180006 - Büşra ARIK

Dr. Öğr. Üyesi Çağrı ŞAHİN

2022

Kelime Sayısı :1219

İNTİHAL BEYANI

Bu çalışmadaki tüm bilgilerin akademik kurallara ve etik davranışa uygun olarak alındığını ve sunulduğunu ve bu belgede alıntı yaptığımı belirttiğim yerler dışında sunduğum çalışmanın kendi çalışmam olduğunu, Yükseköğretim Kurumları Bilimsel Araştırma Ve Yayın Etiği Yönergesinde belirtilen bilimsel araştırma ve yayın etiği ilkelerine uygun olduğunu beyan ederim.

Numara	: 181180006	Numara	: 181180030
Ad Soyad	: Büşra Arık	Ad Soyad	: İsmail Ertaylan
Tarih	: 27.11.2022	Tarih	: 27.11.2022
İmza	: 	İmza	: 

İÇİNDEKİLER

SAHTE FOTOĞRAF ANALİZİ

1. GİRİŞ

Günümüzde teknolojinin ilerlemesi ve yapay zekanın yaygınlaşması sürmektedir. Derin sahte fotoğraflar yapay zekanın konularındandır ve bu görsellerin oluşturulması için gerekli modeller yapay zeka ile yapılmaktadır. Her geçen gün algoritmaların gelişimi ile gerçekçiliği artan derin sahte içerikler tehlikeli bir hal almaktadır. Bilinen kişilerin sahte içeriklerinin yayınlanabilmesi oldukça riskli ihtimallerdir. Bu teknoloji ileride ciddi sorunlar oluşturabilir hale gelmektedir. Bu da teknolojinin yarattığı problemleri teknolojinin çözmesine yol açmaktadır. Derin sahte içeriklerin tespiti yapılabilmektedir. Bu tespitlerin yapılabilmesi hukuki anlamda siber güvenlik konularında önemli bir rol oynar. Bu konu, güncel bir teknoloji olmakla birlikte gelişmeye hali hazırda devam etmektedir. Sahte içeriklerin üretiminde çeşitli algoritmalar kullanılırken tespitinde de durum aynıdır. Tanımlamak gerekirse sahte fotoğraf analizi, yapay zekaya dayalı yöntemler ve derin öğrenme teknikleri ile üzerinde değişiklik yapılan fotoğraf ve görsellerin tespitini sağlamaktır. Sahte fotoğraf analizini gerçekleştirilecek ilgili sistemde derin öğrenme teknikleri, hata seviye analizi, meta veri analizi ve evrişimli sinir ağı algoritmaları kullanılacaktır.

1.1. Amaç

Projede amaç; belli veri setleri üstünde bir modele sahte fotoğraf ile gerçek fotoğrafı ayırt etmeyi öğreterek uygulamaya yüklenen fotoğrafın sahte mi yoksa gerçek mi olduğunun tespit edilmesidir. Derin öğrenme teknikleri kullanılarak yapay zekadan destek alınacaktır. Sistem bu tespiti yaptıktan sonra fotoğrafın sahte yada gerçek olduğuna dair bir çıktı üretir.

1.2. Hedef Kitle

Projede hedef kitle, bir görselin sahteliğini analiz etmek isteyen herhangi bir kişi yada kurumu kapsayabileceği gibi, siber konulu davalarda yargı yetkisine sahip kişileri de kapsayabilir. Projenin toplumda bireye kadar ulaşabilmesi sayesinde insanların sorgulama yetenekleri artacaktır ve bu şekilde genellikle toplumda göz önünde olan insanlara karşı olası saldırıların önemini yitirmesine sebep olacaktır.

1.3. Kısaltmalar ve Tanımlar

Kısaltmalar	Açıklamalar
CNN	Convolutional Neural Networks
ELA	Error Level Analysis
JPG	Joint Photographic Group
KVKK	Kişisel Verileri Koruma Kurumu
PNG	Portable Network Graphic

RAM	Random Access Memory

Tanımlar	Açıklamalar
CNN(Evrişimli Sinir Ağı)	CNN genellikle görüntü işlemede kullanılan ve girdi olarak görselleri alan bir derin öğrenme algoritmasıdır. Farklı operasyonlarla görsellerdeki featureları (özellikleri) yakalayan ve onları sınıflandıran bu algoritma farklı katmanlardan oluşmaktadır [1].
Derin Öğrenme	Derin öğrenme, verilen bir veri seti ile sonuçları tahmin eden birden fazla katmandan oluşan bir makine öğrenme yöntemidir [2].
ELA(Hata Seviye Analizi)	Dosyasının belli bir görüntü kalitesi seviyesinde kaydedilmesi ile ortaya çıkan hataların, kaydedilmeden önceki hali ile kıyaslamasını gerçekleştirmek için kullanılan bir algoritmadır [3].
Meta veri	Bir kaynağın ya da verinin öğelerini tanımlayan bilgilerdir. Meta veriler, dosyanın oluşturulması ve işlenmesi ile ilgili bilgiler vermektedir. Bu bilgilerin analizi sayesinde fotoğraf veya görsellerde değişim gerçekleşip gerçekleşmediği tespit edilebilir [4].
Use-Case	Use Case, bir sistem aracılığı ile sunulan veya sunulacak tek bir fonksiyonu tanımlamaktadır [5].

1.4. Referanslar

[1] Doğan, Ö. (2020). CNN (Convolutional Neural Networks) Nedir? Teknoloji.org. https://teknoloji.org/cnn-convolutional-neural-networks-nedir/

[2] Derin Öğrenme (Deep Learning) Nedir? (2020). https://www.beyaz.net/tr/yazilim/makaleler/derin_ogrenme_deep_learning_nedir.html

[3] Sarica, M. (2013). Manipüle Edilmiş Fotoğraf Analizi. Siber Güvenlik Günlüğü. https://www.mertsarica.com/fotograf-analizi/

[4] Wikipedia contributors. (2015). *Metadata*. Vikipedi. https://tr.wikipedia.org/wiki/Metadata

[5] Güneş, V. (2021). Use Case (Kullanım Şekli) Diyagramları ile Resmin Bütününü Görmek! Medium. https://medium.com/@veysel.gunes36/use-case-kullan%C4%B1m-%C5%9Fekli-diyagramlar%C4%B1-ile-resmin-b%C3%BCt%C3%BCn%C3%BCn%C3%BC-g%C3%B6rmek-fbe4f49494f0

1.5. Genel Bakış (Overview)

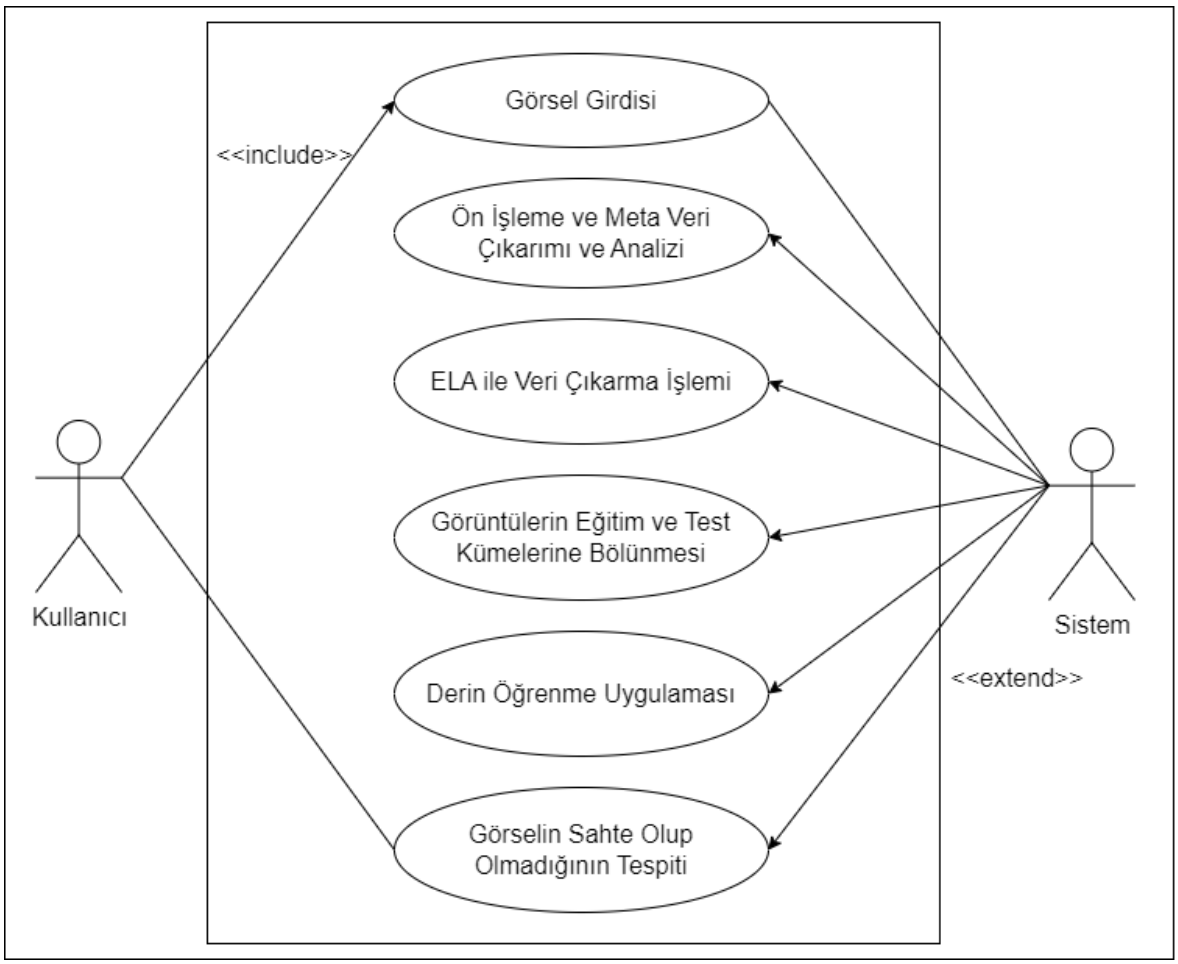
SRS (Software Requirements Specifications), iş gereksinimleri, özellikler, performans ve davranışları dahil olmak üzere geliştirilecek bir yazılım projesinin kapsamlı tanım ve özelliklerini açıklamayı hedefleyen bir belgedir. Kullanıcı ve sistem gereksinimlerini içeren bu belge yazılım gereksinim özelliklerini ifade etmektedir.

2. GENEL TANIMLAMA

2.1. Ürün Perspektifi

Sahte fotoğraf analizinde sistem tek bir kullanıcı tipine sahiptir. Bu sebeple ilgili aşamalar değişkenlik göstermez. Akış kullanıcıdan sisteme ve sistemden kullanıcıya doğrudur. Akış kullanıcının sonucu elde etmesiyle son bulur.

2.1.1. Sistem Arayüzü



Şekil 1 - Sistem Use-Case Diyagramı

2.2 Ürün İşlevleri

- Uygulama açıldığında kullanıcı görsel yükleme butonuna tıklar.
- Kullanıcı tespit yapmak istediği görseli bilgisayarından seçer.
- Kullanıcı görseli seçtikten sonra “tespit et” butonuna tıklar ve görseli sisteme yükler.
- Sistem, ilgili algoritmaları yaptıktan sonra sonuçları ekrana yansıtır.
- Kullanıcı fotoğrafın sahte olup olmadığı bilgisine erişir.
- Kullanıcı sonucun doğruluk analizini ekranda pasta grafiği biçiminde görüntüler.

3.GEREKSİNİMLER SPESİFİKASYONU

3.1 Gerekli Durum ve Modlar

Sistemin değişken herhangi bir modu bulunmamaktadır. Sistem her an tek bir çalışma modundadır ve yüklenen görselin tespitini yapmaya hazır haldedir. Her tespit sonrasında tekrar tespit yapabilir duruma gelmektedir.

3.2 Fonksiyonel Gereksinimleri

Fonksiyonel olarak sistem, yüklenen görselin belirli aşamalardan geçmesiyle hata seviyelerini analiz etmelidir. Bu analiz sonuçlarında görseller eğitim ve test aşamalarından geçmelidir. Ardından görseller, sahteliğin tespit edilebilmesi için derin öğrenme modellerine iletilmelidir. Sistem başarı oranlarını sonuç olarak vermelidir.

3.2.1. Sistem kullanıcının fotoğrafları veya görselleri JPG ve PNG formatında yüklemesine izin vermelidir.
3.2.2. Sistem veri kümesini ön işleme(pre-processing) aşamasından geçirmelidir.
3.2.3. Sistem hata seviye analizi(ELA) tekniğiyle çıkarma işlemi gerçekleştirmelidir.
3.2.4. Sistem hata seviye analizinden geçen görüntüleri eğitim ve test kümelerine bölmelidir.
3.2.5. Sistem görüntülerin derin öğrenme teknikleri aracılığıyla sahte olup olmadığını analiz edebilmelidir.
3.2.6. Sistem sonuç olarak başarı oranını ve sahte olup olmadığını kullanıcıya çıktı halinde sunmalıdır.

3.3 Arayüz Gereksinimleri

3.3.1. Program arayüzü basit ve tek tasarımlı sayfadan oluşmalıdır. Bu ekranda tespiti yapılacak görselin programa yüklenmesi için gerekli bölümler ve sonuçların ekrana yansıyacağı bölümler yer almalıdır.
3.3.2. Arayüz her kullanıcının kolayca kullanabileceği şekilde tasarlanmalıdır. Basit bir görsel yükleme aracı ve anlaşılır bir sonuç ekranı içermelidir.

3.4 Veri Seti Gereksinimleri

3.4.1. Sistem, eğitim ve test aşamalarında kullanılmak üzere uygun veri setini barındırmalıdır.
3.4.2. Kullanıcının yüklediği görseller, sistem tarafından tek seferlik kullanılacak olup veri setine dahil edilmeyecektir.
3.4.3. Sistem, veri seti elemanlarını önceden belirlenmiş ölçüde yeniden boyutlandırarak algoritmalarda kullanılmak üzere sabit boyutlu hale getirmelidir.

3.5 Tasarım ve Uygulama Kısıtlamaları

Sistemin kullanılacağı bilgisayar, yazılım ve donanım olmak üzere bazı gereksinimleri içerir.

3.5.1 Yazılım Kısıtları

3.5.1.1. Sistem geliştirme ortamı olarak Jupyter Notebook çatısı altında Python programlama dili ile gerçekleştirilmelidir. Veri seti üzerinde değişiklik yapılmayacağından bir veri tabanı yönetim sistemine ihtiyaç duyulmamaktadır.

3.5.1.2. Sistemin çıktıları pasta grafiği üzerinde gösterilmelidir.

3.5.2 Donanım Kısıtları

3.5.2.1. Sistemde gerekli işlemlerin yapılacağı bir bilgisayar ve müşterinin çıktıları görebileceği bir monitör olmalıdır.

3.5.2.2. Bilgisayarın çalışacağı sistemde 1.8 GHz ve üzeri işlemci hızına sahip olmalıdır.

3.5.2.3. Bilgisayarın çalışacağı sistem, en az 2 GB RAM'e sahip olmalıdır.

3.5.2.4. Bilgisayarın çalışacağı sistem, ilgili görselleri de barındıracağından en az 10 GB depolama alanına sahip olmalıdır.

3.6 Yazılım Kalite Faktörleri

Sistem aşağıdaki yazılım kalite faktörlerini gerçekleştirecek şekilde geliştirilmelidir.

3.6.1 Sayısal Gereksinimler

3.6.1.1. Sistem, fotoğrafın yüklenmesi işlemini kullanıcının da internet hızına ve yüklediği fotoğrafın boyutuna göre 15 saniyeden kısa bir süre içerisinde tamamlamalıdır.

3.6.1.2. Sistem, yüklenen fotoğrafın analizini 15 saniyeden kısa bir süre içerisinde gerçekleştirmelidir.

3.6.1.3. Sistem, 3 megabayttan daha fazla boyutta bir fotoğrafı kabul etmemelidir.

3.6.2 Kullanılabilirlik

Sistem, her kullanıcı tarafından kolayca kullanılma yeteneğine sahip olmalıdır.

3.6.3 Güvenilirlik

Sistem tarafından üretilen çıktı algoritmanın sonuçlarına göre doğru ve tutarlı olmalıdır.

3.6.4 Erişilebilirlik

Sistem, her an kullanıcı tarafından kullanıma açık halde olmalıdır.

3.6.5 Esneklik

Sistem, olası güncellemelere kolayca adapte olmalıdır.

3.6.6 Test Edilebilirlik

Sistem, veri setinden elde ettiği sonuçlara dayanarak çıktıyı test edebilmelidir.

3.6.7 Taşınabilirlik

Sistem, gereksinimleri karşılayan her mobil cihazda kullanılabilir durumda olmalıdır.