

GAZİ ÜNİVERSİTESİ  
MÜHENDİSLİK FAKÜLTESİ  
BİLGİSAYAR MÜHENDİSLİĞİ



BM496 BİLGİSAYAR PROJESİ II

SOFTWARE REQUIREMENTS SPECIFICATION  
DOCUMENT (SRS)

Sahte Fotoğraf Analizi

Dr. Öğr. Üyesi Çağrı ŞAHİN

181180030 - İsmail ERTAYLAN

181180006 - Büşra ARIK

2023

## İÇİNDEKİLER

1. GİRİŞ .....	1
1.1. Amaç .....	1
1.2. Hedef Kitle .....	1
1.3. Kısaltmalar ve Tanımlar .....	1
1.4. Referanslar .....	2
1.5. Genel Bakış .....	3
2. GENEL TANIMLAMA.....	4
2.1. Ürün Perspektifi .....	4
2.1.1. Sistem Arayüzü .....	4
2.1.2. Kullanıcı Arayüzü .....	4
2.2. Ürün İşlevleri.....	4
2.3. Kullanıcılar ve Özellikleri .....	5
2.4. Varsayımlar ve Bağımlılıklar .....	5
3. GEREKSİNİMLER .....	6
3.1. Gerekli Durum ve Modlar .....	6
3.2. Fonksiyonel Gereksinimleri .....	6
3.3. Dış Arayüz Gereksinimleri.....	6
3.4. Dahili Veri Gereksinimleri.....	6
3.5. Performans Gereksinimleri .....	7
3.6. Diğer Gereksinimler .....	7
3.7. Gereksinimlerin Önceliği ve Kritikliği .....	7
4. YAZILIM KALİTE FAKTÖRLERİ .....	7
4.1. Güvenilirlik .....	7
4.2. Güvenlik .....	7
4.3. Taşınabilirlik .....	7
4.4. Yeniden Kullanılabilirlik.....	7
4.5. Test Edilebilirlik.....	7
4.6. Esneklik.....	7
4.7. Erişilebilirlik.....	8
5. TASARIM VE UYGULAMA KISITLARI .....	9
5.1. Yazılım Kısıtları.....	9
5.2. Donanım Kısıtları.....	9

# 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 zekâ 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 gerçekleştirecek 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 ya da 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

<b>JPG</b>	Joint Photographic Group
<b>KVKK</b>	Kişisel Verileri Koruma Kurumu
<b>PNG</b>	Portable Network Graphic
<b>RAM</b>	Random Access Memory

<b>Tanımlar</b>	<b>Açıklamalar</b>
<b>CNN (Evrışimli Sinir Ağı)</b>	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].
<b>Derin Öğrenme</b>	Derin öğrenme, verilen bir veri seti ile sonuçları tahmin eden birden fazla katmandan oluşan bir makine öğrenme yöntemidir [2].
<b>ELA (Hata Seviye Analizi)</b>	Dosyasının belli bir görüntü kalitesi seviyesinde kaydedilmesi ile ortaya çıkan hataların, kaydedilmeden önceki hali ile kıyaslamasını gerçekleştirmek için kullanılan bir algoritmadır [3].
<b>Meta veri</b>	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].
<b>Use-Case</b>	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](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*. Wikipedi. <https://tr.wikipedia.org/wiki/Metadata>

[5] Güneş, V. (2021). Use Case (Kullanım Şekli) Diyagramları ile Resmin Bütünü 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

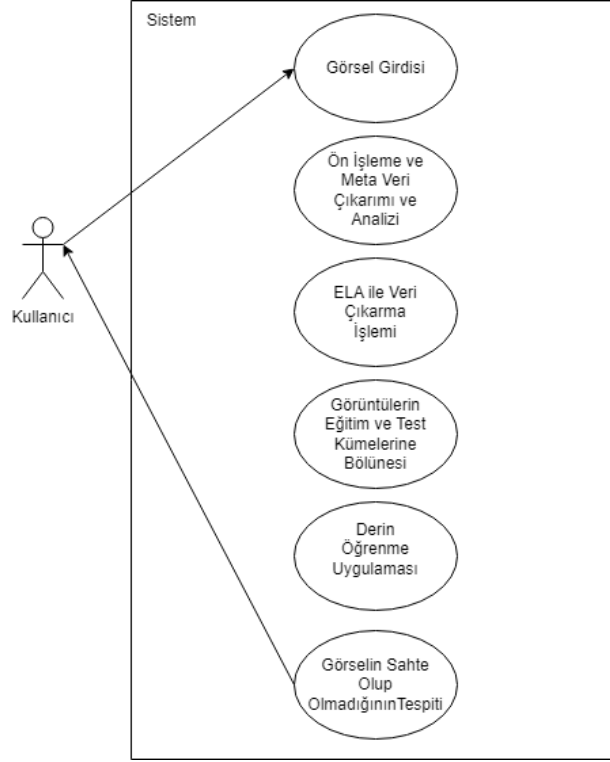
SRS (Software Requirements Specifications), iş gereksinimleri, özellikler, performans ve davranışları dahil olmak üzere geliştirilecek bir yazılım projesinin kapsamlı tanım ve özelliklerini açıklamayı hedefleyen bir belgedir. Kullanıcı ve sistem gereksinimlerini içeren bu belge yazılım gereksinim özelliklerini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

#### 2.1.2. Kullanıcı Arayüzü

- Yazılımın kullanıcı arayüzü, kullanıcının sisteme erişebileceği Google Chrome, Microsoft Edge veya Firefox gibi tarayıcılarla uyumlu olacaktır.

### 2.2. Ürün İşlevleri

- Kullanıcı tespit yapmak istediği görseli bilgisayarından seçer.
- Kullanıcı görseli seçtikten sonra görsel sisteme aktarılır.
- Sistem, ilgili algoritmaları yaptıktan sonra sonuçları ekrana yansıtır.
- Kullanıcı fotoğrafın sahte olup olmadığı bilgisine erişir.
- Kullanıcı sonucun doğruluk analizini ekranda pasta grafiği biçiminde görüntüler.

### 2.3. Kullanıcılar ve Özellikleri

Sistemde tek bir kullanıcı bulunmaktadır. Sistemi kullanan bu kullanıcının yapabilecekleri önceden belirlidir.

- Kullanıcı sisteme bilgisayarında bulunan bir görseli yükler.
- Kullanıcı sistemden bu görselin sahtelik analizini elde eder. Kullanıcı sistemi istediği kadar tekrar kullanabilir.
- Kullanıcı görsellerin herhangi bir yerde depolanmadığını, kopyalanmadığını ve yalnızca kendi bilgisayarında bulunduğunu bilerek programı rahatça kullanır.

### 2.4. Varsayımlar ve Bağımlılıklar

- Kullanıcının sistemi kullandığı bilgisayarın minimum sistem gereksinimlerini karşıladığı varsayılır.
- Kullanıcının sisteme yüklediği görsellerin teknik standartları karşıladığı varsayılır.
- Kullanıcının sistemin çıktısını anlayabilmek için grafik okuyabiliyor olduğu varsayılır.
- Sistemin her bir aşamadan sonraki çıktısı bir öncekine bağımlıdır. Aradaki aşamalardan birinde oluşabilecek farklılık diğer çıktıları da etkiler.
- Sistem yapay zeka aracılığıyla analiz yaparken veri setini eğitir. Dolayısıyla iyi sonuçların çıktısı veri setinin iyi örnekler barındırıyor olmasına bağımlıdır.

### 3. GEREKSİNİMLER

#### 3.1. Gerekli Durum ve Modlar

Sistemin değişken herhangi bir modu bulunmamaktadır. Sistem her an tek bir çalışma modundadır ve yüklenen görselin tespiti yapmaya hazır haldedir. Her tespit sonrasında tekrar tespit yapılabilir 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.

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

#### 3.3. Dış Arayüz Gereksinimleri

- Yüklenen görsel program üzerinde görünür hale gelmelidir.
- Yüklenen görselin belirli aşamalardan sonraki varsa değişimleri ekrana yansıtılmalıdır.
- Görselin analiz sonuçları gerek sayısal oranlarla gerekse grafiklerle kullanıcıya yansıtılmalıdır.

#### 3.4. Dahili Veri Gereksinimleri

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



### 3.5. Performans Gereksinimleri

- Sistem, fotoğrafın yüklenmesi işlemini kullanıcının da internet hızına ve yüklediği fotoğrafın boyutuna göre 15 saniyeden kısa bir süre içerisinde tamamlamalıdır.
- Sistem, yüklenen fotoğrafın analizini 15 saniyeden kısa bir süre içerisinde gerçekleştirmelidir.
- Sistem, 5 megabayttan daha fazla boyutta bir fotoğrafı kabul etmemelidir.
- Sistem 50 kilobyttan daha ufak boyutta bir fotoğrafı kabul etmemelidir.

### 3.6. Diğer Gereksinimler

- Sistem kullanıcının herhangi bir kayıp yaşamaması için herhangi bir verisini barındırmamalıdır.

### 3.7. Gereksinimlerin Önceliği ve Kritikliği

Gereksinimlerin tümü sistemin doğru ve performanslı çalışabilmesi için önceliklidir. Fakat yine de bazı gereksinimler kritik derecede önem arz etmektedir. Bunlardan bazıları şunlardır:

- Fonksiyonel gereksinimler: Programın ağırlıklı öne çıkan özelliği işlevselliğidir. Bu sebeple programın fotoğrafların sahtelik analizlerini yapabilmesi için gerekli fonksiyonel gereksinimler en kritik gereksinimlerdir.
- Dahili veri gereksinimleri: Program yapay zeka algoritmaları aracılığıyla analizi gerçekleştirmektedir. Dolayısıyla modelin eğitilebilmesi için uygun bir veri setinin bulundurulması gerekmektedir.

## 4. YAZILIM KALİTE FAKTÖRLERİ

### 4.1. Güvenilirlik

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

### 4.2. Güvenlik

Sistemin herhangi bir güvenlik açığı sorunu bulunmamaktadır.

### 4.3. Taşınabilirlik

Sistem, gereksinimleri karşılayan her bilgisayarda kullanılabilir durumda olmalıdır.

### 4.4. Yeniden Kullanılabilirlik

Sistem, her kullanıcı tarafından kolayca kullanılma yeteneğine sahip olmalıdır.

### 4.5. Test Edilebilirlik

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

### 4.6. Esneklik

Sistem, olası güncellemelere kolayca adapte olmalıdır.

**4.7. Eriřilebilirlik**

Sistem, her an kullanıcı tarafından kullanıma açık halde olmalıdır.

## **5. TASARIM VE UYGULAMA KISITLARI**

### **5.1. Yazılım Kısıtları**

- 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.
- Sistemin çıktıları pasta grafiği üzerinde gösterilmelidir.

### **5.2. Donanım Kısıtları**

- Sistemde gerekli işlemlerin yapılacağı bir bilgisayar ve müşterinin çıktıları görebileceği bir monitör olmalıdır.
- Bilgisayarın çalıştığı sistemde 1.8 GHz ve üzeri işlemci hızına sahip olmalıdır.
- Bilgisayarın çalıştığı sistem, en az 2 GB RAM'e sahip olmalıdır.
- Bilgisayarın çalıştığı sistem, ilgili görselleri de barındırdığından en az 10 GB depolama alanına sahip olmalıdır.