
GAZİ ÜNİVERSİTESİ
Gazi
1926

ADLİ BİLİŞİM İNCELEME SÜREÇLERİNDE YAPAY ZEKA KULLANIMI

İsrafil DİLBER

YÜKSEK LİSANS TEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2022

İsrafil DİLBER tarafından hazırlanan "…ADLİ BİLİŞİM İNCELEME SÜREÇLERİNDE YAPAY ZEKA KULLANIMI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Aydın ÇETİN

Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ..……

Başkan: Doç. Dr. Sinan TOKLU

Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

Üye: Doç. Dr. A. Talha KABAKUŞ

Bilgisayar Mühendisliği Bölümü, Düzce Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum. ……...

Tez Savunma Tarihi: 27/06/2022

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..……

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

İmza
İsrafil DİLBER
...../……/……

ADLİ BİLİŞİM İNCELEME SÜREÇLERİNDE YAPAY ZEKA KULLANIMI

(Yüksek Lisans Tezi)

İsrafil DİLBER

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2022

ÖZET

Son dönemde teknolojide meydana gelen gelişmeler neticesinde başta internet, akıllı telefon ve bulut bilişim hizmetleri olmak üzere, bilgiyi depolayan ve kullanan bilişim cihazları ve yazılımsal uygulamaların kullanım oranları artmıştır. İnternet ağı ve söz konusu teknolojik cihazların yoğun olarak kullanımı, paralelinde farklı ortamlarda aktarılan veya depolanan veri kapasitesini arttırmış ve söz konusu artış aynı zamanda dijital dünya ile ilişkilendirilen suç oranının da artmasına sebebiyet vermiştir. İşlenen farklı suçlara ilişkin dijital delil miktarı da bu gelişmeler neticesinde artış göstermiş ve bu durum, uzmanların veriyi doğru analiz edebilme etkinliğini olumsuz yönde etkilemiştir. Veri inceleme ve analiz süreçlerinde karşılaşılan zorluklar, nihai olarak ise hukuki yargılama süreçlerini olumsuz etkilemiştir. Hem adli bilişim hem de hukuk alanında yaşanan sorunların giderilmesi adına tezde, adli olay kapsamında elde edilen dijital görüntü verilerinin yüksek doğruluk oranında analiz edilmesini mümkün kılan bir model önerilmiştir. Model, sınıflandırma için özel tasarlanan ağ yapısı ile VGG16'ya ait evrişimsel ağ katmanlarının birleşmesinden oluşmaktadır. Çalısma kapsamında 300*300 VPI çözünürlükte veri seti oluşturmak maksadıyla, Kaggle platformundan 3085, diğer dijital kaynaklardan ise 915 adet görüntü derlenmiştir. Model, TensorFlow ve Keras kütüphaneleri yardımı ile FloydHub geliştirme ortamında test edilmiştir. Elde edilen sonuçlara göre model ile %97.8 oranında doğruluk elde edilmiştir. Nihai olarak ise elde edilen sonuç, derin öğrenme alanda gerçekleştirilen benzer sınıflandırma çalışmaları ile karşılaştırılmıştır.

Bilim Kodu	:	92401
Anahtar Kelimeler	:	Adli bilişim, yapay zeka, derin öğrenme, evrişimsel sinir ağları, ESA
Sayfa Adedi	:	49
Danışman	:	Prof. Dr. Aydın ÇETİN

ARTIFICIAL INTELLIGENCE IN DIGITAL FORENSICS INVESTIGATION PROCESSES

(M. Sc. Thesis)

İsrafil DİLBER

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

June 2022

ABSTRACT

As a result of the recent developments in technology, the usage rates of IT devices and software applications that store and use data, especially internet, smart phone and cloud computing services, have increased. The extensive use of the internet network and technological devices has increased the data capacity that is transferred or stored in different environments, and this increase has also caused an uprising in the crime rate associated with the digital world. The amount of digital evidence has also increased and has negatively affected the efficiency of the experts to analyze the data correctly. The difficulties in the data analysis and processes, ultimately adversely affected the legal proceedings. In order to eliminate the problems in the field of forensic and law, a model that enables the analysis of digital image data with high accuracy has been proposed. The model consists of a specially designed network structure and the convolutional network layers of VGG16. Within the scope of the study, 3085 images from the Kaggle platform and 915 images from other digital sources were compiled in order to create a data set with 300*300 VPI resolution. The model has been tested in the FloydHub development environment with the help of TensorFlow and Keras libraries. According to the results, 97.8% accuracy was obtained with the model. Finally, the results were compared with similar classification studies carried out in the field of deep learning and forensics.

Science Code	:	92401
Key Words	:	Digital forensics, artificial intelligence, deep learning, convolutional neural networks, CNN
Page Number	:	49
Supervisor	:	Prof. Dr. Aydın ÇETİN

TEŞEKKÜR

Bu tezin hazırlanmasında tecrübelerinden istifade ettiğim, tez hazırlık süreçlerinde akademik bilgisi ile her zaman yanımda olan ve zaman ayırarak yönlendirme, girdi, düzeltme, öneri ve yorumlarını esirgemeyen değerli tez danışmanım Prof. Dr. Aydın ÇETİN'e, hem ders günlerinde hem de tez hazırlık süreçlerinde çalışmalarıma devam edebilmem için gerekli fedakarlığı, destek ve esnekliği sağlayan başta amirlerim ve mesai arkadaşlarıma, maddi ve manevi desteklerini her zaman yanımda hissettiğim eşim Duygu DİLBER'e, tecrübeleri ile bana destek olan kardeşim Sinan DİLBER'e ve aileme teşekkürlerimi sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ADAM	Uyarlanabilir moment tahmini (Adaptive moment estimation)
ASSS	Avrupa siber suç sözleşmasi
CART	Bilgisayar analizi ve müdahale ekibi (Computer analysis and response team)
CPU	Merkez işlem birimi (Central processing unit)
DLCF	Derin öğrenme siber adli bilişim (Deep learning cyber forensics)
DSFD	Çift çekim yüz dedektörü (Dual shot face detector)
ESA	Evrişimsel sinir ağları
FBI	Federal soruşturma bürosu (Federal bureau of investigation)
FN	Yanlış negatif (False negative)
FP	Yanlış pozitif (False positive)
GPU	Grafik işlem birimi (Graphics processing unit)
ILSVRC	ImageNet büyük ölçekli görsel tanıma yarışması (ImageNet large scale visual recognition challenge)
IOCE	Uluslararası bilgisayar kanıtı organizasyonu (International organization on computer evidence)
MOV	Film dijital video (Movie digital video)
MP4	MPEG-4 Part 14
MTCNN	Çok görevli basamaklı evrişimli sinir ağları Multi-task cascaded convolutional neural networks
NIJ	Ulusal Adalet Enstitüsü (National Institute of Justice)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)

Kısaltmalar	Açıklamalar
RMSProp	Kök ortalama kare yayılımı (Root mean square propagation)
SGD	Stokastik gradyan iniş (Stochastic gradient descent)
SWGDE	Dijital kanıt üzerine bilimsel çalışma grubu (Scientific working group on digital evidence)
TN	Doğru negatif (True negative)
TP	Doğru pozitif **(**True positive)
TWGDE	Teknik dijital kanıt çalışma grubu (Technical digital evidence working group)
URL	Tek tip kaynak bulucu (Uniform resource locators)
VGG	Görsel geometri grubu (Visual geometry group)
VPI	Görüntü programlama arayüzü (Vision programming interface)

1. GİRİŞ

Dijital cihaz ve bu cihazlara ait bellek boyutlarının durmaksızın artışı ile söz konusu teknoloji cihazlarının bireyler tarafından günlük rutin işlemlerde yoğun kullanımı, dijital cihazların analiz edilmesine duyulan ihtiyacı ve aynı zamanda incelenerek değerlendirlecek veri boyutunu da artırmıştır. Veri boyutu problemi yanı sıra, halihazırda kullanılan adli bilişim cihaz ve uygulamaları yüksek boyutlara ulaşan verilerin özellikle de görsel verilerin analizi yapma ve elde edilen bulguların birbiri ile ilişkilendirilmesi gibi durumlarda arzulanan performansı sergileme noktasında yetersiz kalmaktadırlar. Bahsi geçen sorunlar neticesinde, uzmanlar tarafından verilerin analizine ayrılan zaman olması gerekenden çok fazla olmaktadır [1]. Adli bilişim veri analiz işlemlerine sıkı sıkıya bağlı olan ve bu çalışmalara paralel sürdürülen hukuki yargılama süreçleri uzamakta ve meydana gelen aksamalar hukuki süreçlerin güvenirliliğini zedelemektedir.

Elde edilen verilerin gerçek değeri ortaya konulurken esas alınan nokta, bu verilerin karar verme aşamalarında ne derece etkili olduğu ve kararı etkileyecek yararlı bilgiler üretme noktasında ki becerisidir. Genel olarak, adli bilişi inceleme ve analiz süreçleri, suç analiz uzmanlarının toparlanan veriye ait anlamlı sonucu açıklamak için bir takım araçlardan faydalanmak sureti ile rapor ve özet çıkardıkları geleneksel bir çalışmadır. Analiz yapan uzmanların verilere ilişkin faydalı bilgileri doğru olarak algılaması ve kavraması her zaman mümkün olmayabilir. Bu sorunun üstesinden gelmek için söz konusu veriler Last Activity View, Sleuth Kit, SANS SFIT gibi farklı cihaz ve yazılımlar kullanılarak anlaşılması kolay uygun bir formata dönüştürülebilir [2].

Mevcut kullanımda bulunan adli bilişim yazılım ve cihazları her ne kadar veriye ait hash karşılaştırmaları veya metin formatında bulunan verilerin aranması ve analizi konularında iyi sonuçlar ortaya koysa da söz konusu görsel verilerin incelenerek doğru şekilde yorumlanması olduğunda, bahsi geçen adli bilişim uygulamaları çoğu zaman yetersiz performans sergilemektedirler. Performans açığının giderilmesi maksadı ile görsel verilerin manuel olarak uzmanlar tarafından incelenmeye çalışılması ise nihai olarak analiz süreçlerinde harcanan birim zamanı artırmakta ve olası hata payı riskini katlamaktadır. Bununla birlikte olası görüntü manipülasyonunun tespit edilmesi amacı ile son dönemde derin öğrenme metodları etkin olarak kullanılmış ve tatminkar neticeler elde edilmiştir[3].

Tezde, uzmanlar tarafından veri analiz süreçlerinde kullanılmak üzere, derin öğrenme algoritmalarını kullanan ve elde edilen görüntü verilerini hem hızlı hem de doğru olarak sınıflandırabilen bir model ortaya konulmuştur. Tez çalışması boyunca kullanılan metod ve yöntemler ile elde edilen sonuçlar bu alanda gerçekleştirilen diğer çalışmalarda kullanılan yöntem ve sonuçları ile karşılaştırılarak değrlendirilmeye tabi tutulmuştur.

Bilişim suçları ve bilişim yoluyla işlenen suçlar ile daha etkin bir şekilde mücadele edilebilmesi için, suçların aydınlatılması ve suçluların adli makamlara teslim edilmesi sürecinde fiziksel delillerden çok, elektronik veya manyetik bir ortam üzerinden iletilen veya bu ortamlara kaydedilen delil niteliği taşıyan veri ve bilgiler olarak tanımlanan dijital delillere ihtiyaç duyulmaktadır [4]. Hukuki soruşturma ve yargılama süreçlerinde dijital cihaz ve ortamlardan elde edilen veriler her zamankinden çok daha fazla önemli hale gelmiştir. Dolayısı ile hukuki yargılama süreçlerinin aksamadan yapılabilmesi ancak toplanan dijital verilerin arzulanan zaman içerisinde doğru analiz edilebilmesi ve mahkemelere sunulabilmesi ile mümkündür. Veri inceleme süreçlerinde ki aksaklıkların giderilmesi ve hukuki süreçlerde hata payının en aza indirgenmesi ve bu süreçlerin mağduriyete sebebiyet vermeyecek şekilde en kısa zaman içerisinde tamamlanabilmesi adına tezde ortaya konulan çalışma önem arz etmektedir.

Dosya gizleme, format değiştirme, veri şifreleme, steganografi vb. işlemler tez çalışmasının kapsamı dışına çıktığı ve tezde elde edilen sonuçların karşılaştırıldığı diğer çalışmalarda bu işlemler yer almadıklarından dolayı veri setlerinde bulunan görüntülerde söz konusu kriptografik işlemlerin olmadığı varsayılmıştır. Adli bilişim veri inceleme süreçlerinde görüntü verileri diğer veri formatlarına oranla hem boyut olarak daha fazla alan işgal etmektedir hem de görüntü verileri bir çok vakada manuel incelendiğinden dolayı daha fazla zaman almaktadır. Dolayısı ile görüntü verilerinin incelenmesi ve analizine ilişkin mevcut sorunlar sebebi ile tez çalışmasının kapsamı görüntü veri formatı ile sınırlı tutulmuştur.

Veri setleri derin öğrenme ağ yapısına yedirilmeden önce 300*300 VPI çözünürlükte standart hale getirilmiş ve ağ yapısının doğruluk oranını arttırmak maksadı ile görüntü verileri üzerinde veri çoğaltma işlemleri uygulanmıştır. Tezde veri türü olarak birincil ve ikincil veri toplama yöntemlerinden faydalanılmıştır. Verilerin elde edilmesi süreçlerinde ise örnekleme, deney ve alan araştırması yöntemleri kullanılmıştır.

Bu çalışma altı bölümden oluşmaktadır. Çalışmanın ilk bölümü olan giriş bölümünde, ele alınan problemin tanımı, araştırmanın amacı, kullanılan yöntemler kısaca açıklanmıştır. Çalışmanın ikinci bölümünde, adli bilişim kavramı, adli bilişim türleri, veri inceleme süreçleri ve diğer hususlar açıklanmıştır. Çalışmamızın üçüncü bölümünde ise adli bilişim kapsamında yapay zekâ ve derin öğrenme alanında yapılan önceki çalışmalara yer verilerek bu alanda kapsamlı literatür araştırması ortaya konmuştur. Çalışmanın dördüncü bölümünde ise kullanılan veri seti ve modelinin oluşturulması ve bu kapsamda faydalanılan hiper parametre türleri ve parametreye ait değerler hakkında bilgi verilerek, izlenen yol ve yöntemler hakkında detaylı bilgi sunulmuştur. Çalışmanın beşinci bölümde ise çalışma boyunca teste tabi tutulan parametreler ile ilgili parametre sonuçları ortaya konulmuş, söz konusu sonuçlarda elde edilen veriler bu alanda gerçekleştirilen farklı çalışmalar ile karşılaştırılmak suretiyle değrlendirilmeye alınmıştır. Çalışmanın sonucu ve önemine ilişkin olarak yapılan sonuç değerlendirmesi ise tezin son bölümde ortaya konulmuş, müteakip yıllarda bu alanda ne gibi çalışmaların yapılabileceğine dair bir ön görüde bulunulmuştur.

2. ADLİ BİLİŞİM VE TARİHİ

Adli bilişim inceleme süreçleri bilimsel prensip, metodoloji ve teknik hususları bünyesinde barındıran bir bilim dalıdır. Adli bilişim inceleme süreçlerinde elde edilecek dijital verilerin, mahkemelerde delil niteliği taşıyabilmesi için adli bilişim uzmanlarının iyi eğitim almaları ve gerekli yetenekleri kazanmaları önem arz etmektedir.

Adli bilişim kavram olarak hem hukuk hem de bilişim alanları ile yakından ilişkilidir. Bununla beraber tezde ortaya koyulan çalışma kapsamı gereği, adli bilişim kavramının daha çok teknik boyutu üzerinde durulmuştur. Diğer bir ifade ile çalışmanın kapsamı, adli bilişim süreçlerinde suça ilişkin verilerin elde edilmesinden incelenmesine, analiz edilmesinden yorumlanmasına kadar olan teknik süreci içine almaktadır.

Adli bilişim, bilgisayar ve bilgisayar sistemlerinin suç nedeni veya suç aleti olarak kullanımı ile işlenen suçların çoğalmasına tepki olarak ortaya çıkmıştır. Adli bilişim kavramının geçmişi, dijital verilerin incelenebilmesi için FBI ve diğer kolluk güçlerinin laboratuvar kurarak bilgisayar suçlarını inceleyecek programları geliştirmeye başladığı 1984 ve öncesi yıllara kadar dayanmaktadır. Bilgisayar Analiz ve Müdahale Ekibi (CART), Dijital Kanıt Üzerine Çalışma Grubu (SWGDE), Teknik Dijital Kanıt Çalışma Grubu (TWGDE), Ulusal Adalet Enstitüsü (NIJ) gibi araştırma kuruluşları bir disiplin olarak adli bilişim bilimini tartışmak ve inceleme süreçlerinde standardı sağlamak maksadıyla bu döneme müteakip kurulmuşlardır.

Adli bilişim uygulamaları her ne kadar 1980'li hatta bazı kaynaklara göre daha önceki yıllarda ortaya çıkmaya başlasada, bu kavramın akademik alanda kullanılmaya başlaması 1990'lı yılları bulmuştur. Adli bilişim kavramının uluslararası alanda kabul görmesi ile birlikte ise hem adli bilişim alanında bilgi paylaşımını desteklemek hem de farklı ülkelerde bu alanda çalışmalar yürüten birimler arasında koordinasyonun sağlanması maksadı ile 1995 yılında Uluslararası Dijital Delil Örgütü (IOCE) kurulmuştur.

Türkiye'de adli bilişim kavramının bir disiplin olarak kabul görmeye başlaması ve müteakiben yasalarda yer alması ise 1990 yılı ve sonrası döneme denk gelmektedir. Bu kapsamda bilişim suçları Türk Ceza Kanunu (TCK)'na 1991 yılında ilk defa girmiştir. Bilişim suçları ile daha etkin mücadele edilebilmesi maksadı ile 2001 yılında imzalanan Avrupa Siber Suç Sözleşmasi (ASSS) maddeleri iç hukukumuza aktarılmış ve TCK'nın 243

ve 244'ncü maddelerinde sırası ile bilişim sistemine girme suçu ile bilişim sistemini yok etme, bozma ve verileri yok etme suçları tanımlanmıştır.

Adli bilişimin Türkiye'de gelişmeye başlaması ve bu kapsamda ilk olarak adli bilişim laboratuvarlarının kurulması Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı gibi kolluk kuvvetleri aracılığı ile gerçekleşmiştir. Müteakip yıllarda adli bilişim uygulamalarının büyük şirketler dahil toplumun hemen hemen her alanında ihtiyaç haline gelmesi, kolluk kuvvetleri haricinde bu alanda hizmet veren özel firmaların da kurulmasını zorunlu hale getirmiştir.

2.1. Adli Bilişim ve Dijital Delil Kavramı

Adli bilişim kavramının ortaya çıkması ve uygulamalarının yaygınlaşması ile özellikle akademik alanda adli bilişim kavramının ne olduğuna dair bir çok tanımlama yapılmıştır. Örneğin, G.L. Palmer, ABD'de düzenlenen bir konferansta adli bilişimi şu şekilde tanımlamaktadır; Suça ilişkin olayların ortaya çıkarılmasını kolaylaştırmak veya yıkıcı ve yasal olmayan olası planlı eylemlerin tahmin edilmesine yardım etmek amacıyla dijital kaynaklardan elde edilen dijital delillerin; bilimsel olarak kanıtlanmış teknikler kullanılarak muhafaza edilmesi, toplanması, doğrulanması, tanımlanması, analiz edilmesi, yorumlanması, raporlanması ve sunulmasıdır[5].

Bir diğer tanımlamaya göre ise adli bilişim, "Elektromanyetik ve optik ortamlarda tutulmakta olan veya bu ortamlar arasında iletilen veri, bilgi, görüntü, ses veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal delil özelligi taşıyacak şekilde tanımlanması, elde edilmesi, muhafazası, incelenmesi ve mahkemeye sunulmasıdır"[6].

Adli bilişimi en genel haliyle, bilişim cihazları aracılığı ile işlenen siber suçlarda suçun aydınlatılmasına yardımcı olacak dijital delillerin önceden belirlenmiş standart prosedürler çerçevesinde uzman kişiler tarafından bilişim cihazlarından elde edilmesi, saklanması, analizinin yapılması ve yorumlanarak raporlanması olarak tanımlayabiliriz.

Adli bilişim veri inceleme süreçlerinin doğru anlaşılması için öncelikle dijital delil kavramının anlaşılması ile mümkündür. Dijital delil mahkemede kanıt değeri taşıyabilen, ikili sistemde kaydedilen veya iletilen bilgidir. Dijital delil, bilgisayar sabit diskinde, akılı telefonlarda ve diğer bir çok bilişim alanında bulunabilirler. Dijital delil çoğunlukla bilişim

suçları, çocuk pornosu veya kredi kart hırsızlıkları ile ilişkilendirilsede aslında her türlü suça ilişkin soruşturmalarda kullanılabilmektedir [7].

2.2. Adli Bilişim Türleri

Adli bilişim veri inceleme süreçleri genellikle bilgisayar, telefon gibi bilişim cihazları ile ilişkilendirilmekle beraber, esasında adli bilişim alanında yapılan dijital veri incelemeleri bir çok farklı dijital cihaz ve ortamı kapsamaktadır. Dolayısı ile farklı alanları kapsayacak şekilde yapılan özel çalışmalar adli bilişim türleri olarak ortaya çıkmıştır. "Söz konusu adli bilişim türleri, genel olarak bilgisayar adli bilişimi, ağ ve İnternet adli bilişimi ve gömülü cihazlara ait adli bilişimdir. Ancak son dönemlerde dördüncü bir alt dal olarak sosyal ağ adli bilişimi de kabul edilmektedir"[8].

Bilgisayar

Adli bilişim uzmanlarının, suç kapsamında yaptıkları çalışmalarda, bilgisayar en çok incelenen cihaz olarak ön plana çıkmaktadır. Bilgisayar adli bilişimi, suç kapsamında direkt veya dolaylı olarak kullanılan ve içerisinde suça ilişkin dijital delil barındığı değerlendirilen masaüstü bilgisayar, dizüstü bilgisayar, notebook veya benzeri cihazlardan önceden belirlenen standart yöntemler ile veri elde edilmesini kapsamaktadır.

Resim 2.1. Adli bilişim cihazları [6]

Ağ ve internet

Ağ ve internet adli bilişimi, temelde ağ bağlantıları üzerinde bulunan ve bir kullanıcıdan diğer kullanıcıya giden paket trafiğinin giriş ve çıkışında yer alan veriler ile ilgilenir. Ağ ve internet adli bilişim uzmanları çoğunlukla, güvenlik duvarları, saldırı tespit sistemleri veya ağ yönlendirici cihazlar tarafından kayıt altına alınan veri trafiğini analiz ederler. Amaç, saldırı kaynağına kadar takip ederek siber suç işleyen kişinin yargılanmasıdır [9].

Ağ ve internet adli bilişimi, hem önceden kaydedilmiş hem de canlı veri trafiğinin standart yöntemler ile incelenmesini ve analiz edilmesini kapsamaktadır.

Gömülü cihazlar

Gömülü cihaz, bir veya bir kaç işlemi gerçekleştirmek için tasarlanmış, taşınabilir MP3 çalar, cep telefonu, akıllı telefonlar ve araba navigasyon sistemleri gibi özel maksatlı bilgisayar sistemidir [10].

Resim 2.2. Adli bilişim alanında incelenen gömülü cihazlar [10]

Gömülü cihaz adli bilişimi, diğer adli bilişim türlerine oranla çok farklı bilişim cihazının/ortamının incelenmesini konu alır. Bu alanda incelenen bilişim cihazları, akılı telefonlar başta olmak üzere dijital veri saklayan kredi kartları, GPS cihazları, araba ve akıllı sistem yazılımları olmak üzere bir çok bilişim ortamını kapsamaktadır.

Sosyal ağ

Sosyal medya platformları, tıpkı e-mail ve anlık mesajlaşma ortamları gibi günümüzde

yaygın olarak kullanılan önemli iletişim araçlarındandır. Sosyal medya platformları, hem şirketler hem işletmeler hem de hükümetler açısından toplumla veya müşterilerle iletişim kurmak için ideal kanallardır. Dolayısı ile sosyal medya platformları bir çok organizasyon, kurum ve birey için önemli iletişim aracı haline gelmiştir.

Yapılan araştırmalarda son zamanlarda işlenen bir çok suçun bir şekilde sosyal ağ platformları ile ilişkisi olduğu veya bu platformların kişiler tarafından bizzat suç aracı olarak kullanıldığı bilinmektedir. Sosyal ağ adli bilişimi, hem bilişim camiası için hem de adli makamlar için yeni bir alan olduğundan dolayı literatürde bu kavramın tanımlanmasına ilişkin önemli eksiklikler söz konusudur.

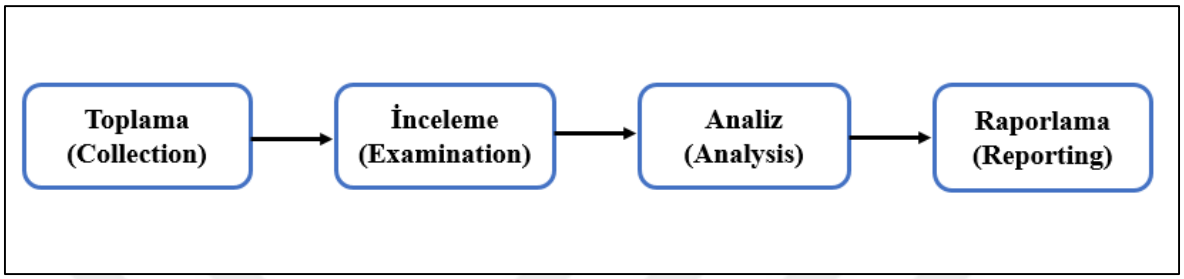
Bununla birlikte adli bilişim kavramı bir çok kesim tarafından yaygın olarak bilinmekte ve mahkeme süreçlerinde kullanılmaktadır. Google arama motoru 2021 yılı için "digital forensics" kavramı için 3 milyon üzerinde sonuç üretirken, "sosyal ağ adli bilişimi (social network forensics)" kavramı için sadece 25 bin civarı sonuç üretmektedir. Bu sonuçlar bile günümüzde sosyal ağ adli bilişiminin, adli bilişim terimi kadar sık kullanılmadığını ortaya koymaktadır. Bu kavram, her nekadar sosyal ağ platformlarının hızlı yaygınlaşması ve gelişmesi sonucunda ortaya çıksa da bu alanda henüz kabul görmüş net bir tanımlama söz konusu değildir. Aslına bakılırsa, sosyal ağ adli bilişimi gelecekte adli bilişiminin ana odak noktalarından birisi haline gelecek ve bu alan hem günümüzde hem de geleceğin dijital dünyasında önemli bir yer işgal edecektir [11].

Günümüzde yeni yeni önem kazanmaya başlayan ve gelecektede önemi daha fazla artacak olan sosyal ağ adli bilişimi, en basit tanımı ile halihazırda kullanılan adli bilişim veri inceleme süreçlerinin sosyal medya olarak bilinen Facebook, Twitter, Instagram, Linkedin gibi sosyal ağ platformlarına veya buralardan elde edilen dijital verilere uygulanmasından ibarettir.

2.3. Adli Bilişim Delil İnceleme Süreçleri

Adli bilişim delil inceleme süreçlerinde elde edilen delillerin yasal bir çerçeve kazanması ve delillerin sunulacağı mahkemeler tarafından kabul görebilmesi için delil elde etme ve inceleme süreçlerin bazı standart prosedürlerle gerçekleştirilmesi gerekir. Adli bilişim delil elde etme ve inceleme süreçlerinde kullanılan yöntemler hakkında bütün dünyada genel kabul gören bir uygulama söz konusu değildir.

Bir çok kaynak delil inceleme süreçlerinde kullanılan aşamaları farklı olarak ele almaktadır. Bununla beraber Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yapılan üst düzey tanımlamaya göre delil inceleme süreçleri, Toplama (Collection), İnceleme (Examination), Analiz (Analysis) ve Raporlama (Reporting) aşamalarından oluşmaktadır [12]. NIST tarafından tanımlanan süreçler Şekil 2.1.'de sunulmuştur.



Şekil 2.1. Adli Bilişim Delil İnceleme Süreçleri [12]

2.3.1. Delil toplama

Dijital delillerin toplama aşaması, ilgili bilişim cihaz veya ortamından delil olması muhtemel verilerin belli standart prosedürler ile elde edilmesi sürecidir. Dijital deliller doğası gereği zarar görmeye ve dış etkenlerden kolayca etkilejmeye oldukça müsait yapıdadırlar. Dolayısı ile delil toplama aşaması aynı zamanda verilerin zarar görmemesi için gerekli planlamanın yapıldığı aşamadır.Toplanacak verinin elde edilmesi esnasında değişmediğinden emin olunması gerekir. Bu maksatla yazmaya korumalı adli bilişim cihazları ile veri elde etme işleminin gerçekleştirilmesi önemlidir.

Veri toplama işleminin alanında uzman ve yetkili personel tarafından gerçekleştirilmesi hem doğru verilerin kısa zamanda toplanmasını hem de olası veri kaybının en aza indirgenmesini sağlayacaktır. Delil toplama işlemine başlamadan önce, sürecinin strateji ve yöntemini doğru belirlemek için;

- Nasıl bir suç veya saldırının meydana geldiğini anlamak,
- Verilerin hangi cihaz veya lokasyonda bulunabileceğini tespit etmek,
- Süreç boyunca kullanılacak veri inceleme cihaz ve yazılımlara karar vermek,
- Yapılan her türlü işlemi kayıt altında tutmak,

Veri toplama aşamasında adli bilişim uzmanının yükünü hafifletecek ve inceleme başında takip edebileceği bir yol haritasının oluşmasını sağlayacaktır. Delil toplama aşamasında genel olarak tercih edilen üç yöntem mevcuttur.

Manuel Veri Elde Etme

Manuel veri elde etme yöntemi, daha çok bilişim cihazlarının belleğinde yer alan verilerin elde edilmesinde tercih edilen bir yoldur. Bu yöntemde, açık olan cihazın dosya sistemine ve belleğine girilerek gerekli görülen dosya ve loglarda inceleme yapılır. Bu yöntemin en büyük dezavantajı, inceleme yapılırken adli bilişim uzmanının mevcut verileri silme, değiştirme veya bu verilere ekleme yapma olasılığının bulunmasıdır. Bu yöntem ile dijital veri elde etmek ancak sınırlı ölçüde gerçekleşmektedir. Çünkü uzman kişi, ancak cihazın işletim sisteminin ona sunduğu dosyalama sistemi üzerinde çalışabilir. Kısıtlı yapısı nedeniyle çok tercih edilen bir yöntem değildir ve genellikle son çare olarak uygulanır.

Mantıksal Veri Elde Etme

Mantıksal veri elde etme yöntemi, bilişim cihazına erişelerek cihaz içerisinde bulunan dosyalama sisteminin bire bir kopyasının çıkarıldığı yöntemdir. Bu yöntemde bilişim cihazının bit bit kopyası alınmadığından dolayı ihtiyaç duyulması halinde ilerleyen süreçlerde bazı verilere ulaşma imkanı ortadan kalkmaktadır.

Fiziksel Veri Elde Etme

Bu yöntemde üzerinde delil barındırdığı düşünülen cihazın kopyalama biriminin dosyalama sisteminden bağımsız olarak bit bit ve bayt bayt kopyalanmasıdır. Diğer bir ifade ile bilişim cihazının fiziksel olarak birebir kopyasının çıkarıldığı veri elde etme yöntemidir. Adli bilişim uzmanına veri inceleme aşamasında daha fazla delil bulma imkanı tanımakla beraber, cihazın tamamı ile kopyalanması boyut olarak fazla alan gereksinimini ortaya çıkarmakta ve bu durum yöntemin her zaman kullanışlı olmasını engellemektedir.

2.3.2. İnceleme

Veri inceleme aşaması, olayın meydana çıkarılması kapsamında dijital verilerin sistematik ve kapsamlı olarak irdelendiği safhadır. İnceleme aşamasının neticesinde toplanan imajlardan delilin bulunması olası bölgeler ortaya çıkarılır. Bu alanlar log dosyaları, veri dosyaları, zaman damgası veya diğer alanlar olabilir [13].

İnceleme aşaması, ayrıca veri toplama aşamasında elde edilen cihaz ve dokümanların hangileri üzerinde çalışma yapılacağının ve hangi formatta verilerin elde edileceğinin belirlendiği aşamadır. Bu aşamada toplanan imaj dosyaları içerisinde suç unsuru oluşturması muhtemel delillerin ortaya çıkarılması hedeflenir. İnceleme aşamasında ayrıca önceden silinen, gizlenen veya şifrelenen veri veya dosyaların bilişim cihazlarından elde edilmesi amaçlanır. Özellikle bu aşamada, olay yerinden elde edilen veriler incelenirken bu verilerin bütünlüğünün bozulmaması için özel dikkatin gösterildiği ve bu maksat ile veri inceleme cihazlarının tecrübeli personel tarafından kullanılmasının zorunlu olduğu aşamadır.

2.3.3. Analiz

Analiz aşaması, hem uzun sürmesi hem de adli bilişim uzmanının kendi tecrübesini ve yorumunu bu aşamada kullanması nedeni ile diğer aşamalara oranla daha fazla zamana ihtiyaç duyulan ve insan hatasının ortaya çıkma olasılığının daha fazla olduğu aşamadır. Elde edilen delillerin, maddi olayın aydınlatılması maksadı ile anlamlandırıldığı aşama olduğundan dolayı adli bilişim veri inceleme süreçlerinde yer alan en kritik aşamadır.

Analiz aşamasında, önceden toplanan ve müteakiben incelenen veriler değerlendirilmeye tabi tutularak delil niteliği taşıyan bilgi elde edilmeye çalışılır. Elde edilen delillerin yasal zeminde anlam kazanması için uygun yöntem ve standart prosedürlerin mutlak takip edilmesi gerekir. Çoğunlukla adli bilişim uzmanının kendi tecrübe ve yorum yeteneğinin ön planda olduğu aşama olmasıyla beraber bazı durumlarda silinen dosya veya klasörlerin ortaya çıkarılması gibi bazı özel uygulamaların gerçekleştirilebilmesi için ek yazılım veya cihazlar kullanılabilir. İhtiyaç duyulması halinde kullanılacak cihazlar mutlaka güvenilir olmalı ve ilgili kurumlar tarafından onayının verilmiş olması gerekir.

Analiz aşamasında, genellikle adli bilişim uzmanının kullandığı iki yöntem vardır. Birinci yaklaşımda, adli bilişim uzmanı bildiği veri içerisinde bilmediği bir bilgiyi elde etmeye çalışır. İkinci yaklaşımda ise bilmediği bir şey içinde bildiği bir bilgiyi elde etmeye çalışır. İlk yöntem kapsamında, zarar görmüş yazılımlar, kullanılmış programlar, silinen dökümanlar veya internet geçmişi gibi hususlar örnek verilebilir. İkinci yöntem için ise URL adresleri, e-mail adresleri veya kullanıcı hesap bilgileri örnek verilebilir. Bu aşamada aamaç, elde edilen deliller tek tek bir araya getirilerek suça ilişkin gerçekler ortaya çıkarılmaya çalışılır. Elde edilen deliller; saldırı zamanı, saldırı yöntemi, saldırgan kimliği, saldırı konumu veya buna benzer diğer hususların ortaya çıkarılmasında kritik rol oynar.

Bu aşamada incelemeyi gerçekleştirecek personelin bu alanda yeterli eğitimi almış ve yeterli tecrübeye sahip olması suça ilişkin delillerin doğru yorumlanması ve olayın doğru çözümlenebilmesi adına hayati öneme sahiptir.

2.3.4. Raporlama

Adli bilişim sürecinde ortaya konulan tüm çalışmaların neticesini ifade etmesi açısından raporlama aşaması en az diğer aşamalar kadar önemlidir. Dolayısı ile yapılan çalışmada elde edilen sonuçların doğru anlaşılması adına, bu bölümde oluşturulan raporun; anlaşılır, yalın, açık, kısa ve öz olmalıdır. Raporlama işlemi;

- Veri toplama,
- Elde edilen sonuçların analiz edilmesi,
- Rapora dair bir taslağın oluşturulması,
- Rapora son şeklinin verilmesi,
- Raporun en son halinin gözden geçirilmesiolmak üzere belirli safhalardan meydana gelen bir süreçtir.

Hazırlanan raporun hazırlanma aşamaları kadar, maddi olaya ilişkin barındırdığı bilgiler de önemlidir. Mahkemenin talepleri, maddi olayın cinsi vb. hususlara bağlı olarak raporun formatı değişmekle beraber, bir raporda genel olarak;

- Suça konu olay hakkında bilgiler,
- İncelemenin özeti,
- Üzerinde inceleme yapılan delillere ilişkin bilgiler,
- İstifade edilen kaynaklar,
- Elde edilen delillerin ne zaman ve kime verildiği bilgisi,
- İnceleme neticesinde hangi bulgulara ulaşıldığı,
- Hash değerleri hesaplamaları gibi bilgilere yer verilmesi gerekir.

Raporların eklerinde incelenmesi talep edilen video, resim ya da programlara ve işletim sistemine ilişkin olay günlükleri de muhakkak yer almalıdır. Ayrıca rapor teknik açıdan doğru ve bilimsel hazırlanmalı, adli bilişime özel tanım ve terimler sade, herkesin anlayacağı şekilde açıklanmış olmalıdır [14].

Raporlama aşamasından ortaya konan deliller mutlaka belgelendirilmeli ve bu aşamada ortaya konulan sonuçlar yoruma imkan vermeyecek şekilde kesin ve net olmalıdır. Kesin sonuç belirtmeyen raporlar, adli vakanın ortaya çıkarılmasını enegelleyeceği gibi mahkeme süreçlerinin de sekteye uğrayarak uzamasına veya hatalı kararların çıkmasına neden olacaktır.

Ortaya konan rapor sonucunun mahkeme tarafından geçerli olarak kabul edilmesi, ancak bütün raporlama sürecinde standart bir yöntem izlenmesi ile mümkündür. Rapor oluşturulurken raporu hazırlayacak uzmanın takip etmesi gereken prosedür ve bu prosedüre ilişkin adımlar müteakip maddelerde sıralandığı gibidir.

1. Raporu hazırlayan kurum ve kişi bilgileri,
2. Maddi olaya ilişkin tarih, saat ve diğer bilgiler,
3. İnceleme ve raporlama süreçlerine dair başlangıç ve bitiş tarih bilgileri,
4. Yapılan incelemenin ne maksatla ve hangi kapsam çerçevesinde yapıldığı,
5. Toplanan verilere ve elde edilen delillere ilşkin ayrıntılı kayıt bilgileri,
6. İşlemler esnasında kullanılan cihaz, yazılım ve program bilgileri ile inceleme esnasında kullanılan metod ve yöntem bilgileri.

3. LİTERATÜR ARAŞTIRMASI

Birçok alanda ortaya konulan çalışmalarda olduğu gibi adli bilişim alanında gerçekleştirilen çalışmalarda da derin öğrenme algoritma ve yöntemlerinden yaygın olarak faydalanılmaktadır. Bu bilgiye paralel olarak özellikle geçmiş son beş yıl içerisinde adli bilişim kapsamında derin öğrenme metod ve yöntemlerinin kullanıldığı çalışmalar ve bu çalışmalarda derin öğrenme metodlarının kullanım şekli araştırılarak ortaya konulmuştur. Yapılan incelemeler sonucunda, adli bilişime alanında derin öğrenme metodlarının yaygın olarak metin [15], ses [16], video [17-19] ve resim/görsel [3],[20-29] formatında ki verilerinin incelemesinde kullanıldığı gözlemlenmiştir. Belirtilen ana çalışma alanları yanı sıra derin öğrenme metodlarının; Yöntem iyileştirme [30,31], süreç iyileştirme ve otomasyon [32,33], saldırı tespit ve güvenlik log analizi [2],[34-35], gibi alanlarda da yoğun olarak kullanıldığı tespit edilmiştir.

Metin formatının incelemesine ilişkin olarak, Kansagara ve Singh [15] günümüzde dijital suçların önceye oranla çok daha hızlı arttığı belirtmiş ve bunun temel sebebinin bütün verilerin dijital cihazlarda tutulması olduğunu ileri sürmüşlerdir. Bu verileri incelerken, adli bişim uzmanlarının bilişim cihazlarında metin araması yaparken, yapılan işleme ilişkin beklenen sonuçların bütününü alamadıklarını ileri sürmüş ve sonuçların tamamını getirebilecek bir model ortaya koymuşlardır. İleri sürülen modelde dosyaların toparlanabilmesi maksadı ile kohenen kendi kendine organizasyon haritası gibi tekniklerden yararlanılmış ve tekst aramasının geliştirilmesi kapsamında iyi sonuçlar elde etmişlerdir.

Ses formatında bulunan verilerin incelenmesi kapsamında, ses formatında bulunan verilerin analizi maksadı ile kullanılan temel konuşma işleme metodları ile adli bilişim alanında ses verisinin analizinde kullanılan programlar ve uygulamalar, performans odaklı olacak şekilde karşılaştırılmıştır [16]. Tablolar yardımı ile çalışma neticesinde ortaya konulan sonuçlar ayrıntılı gösterilmiş ve bu alanda çalışma yürütecek bireylere, yapacakları analiz kapsamında doğru uygulamayı seçmeleri konusunda destek vermek ve süreçlerin doğru ve güvenilir olmasını sağlamak hedeflenmiştir.

Video analizi kapsamında, özellikle sosyal medyada yer alan ve mahkemelerde delil olarak kullanılması muhtemel 3GP, MOV ve MP4 formata sahip görsellerin, orjinal görsel bozularak manipüle edildiğini ortaya koyabilen bir yöntem önerilmiştir [17]. Ortaya konulan model, görsel/video düzenleme uygulamalarının arkada bıraktığı izleri makine öğrenmesi

algoritmaları ile analiz ederek hangi program ile hangi dijital platformda düzenlemenin yapıldığının ortaya çıkarılması mantığına dayanmaktadır. Birbirinden farklı beş ölçüt ile değerlendirilmeye tutulan modelde, 4979 adet orjinali ile oynanmış video görüntüsü kullanılmıştır. Sonuçların değerlendirilmesinde rastgele orman (random forest) modelinin en iyi başarıyı gösterdiği tespit edilmiştir. Önerilen model, aynı zamanda Sosyal medya platformunun tespit edilmesi kapsamında kullanılmış ve modelin farklı sosyal medya platformlarını (12) yüzde yüz doğruluk oranı ile tespit ettiği gözlemlenmiştir.

Ortaya konulan bir diğer çalışmada derin öğrenme algoritmalarından faydalanan yüz tanımlama dedektörleri (MTCNN, PyramidBox ve DSFD) hem doğruluk hem de hız açısından farklı veri setleri ile test edilmiştir [18]. Çalışma sonuçları değerlendirildiğinde, görüntü verilerinin boyutlandırılarak işleme sokulmasının, doğruluğu azalttığı fakat yüz tanıma süreçlerini hızlandırığı tespit edilmiştir. Özellikle yüzde 50 ve 25 oranında yeniden boyutlandırılan görüntülerde Dual Face Shot Detector (DSFD) detektörünün en yüksek hız ve doğruluk oranı ortaya koyduğu kanıtlanmıştır.

Sreenu ve Durai [19] ortaya koydukları çalışma kapsamında ise nüfus yoğunluğunun fazla olduğu ortamlarda meydana gelen olaylara ilişkin olarak olay tespitinden nesne tespitine, şiddetin tespit edilmesinden kalabalık analizine kadar farklı birçok alanı incelemeye tabi tutmuşlardır. Tespit aşamalarında derin öğrenme teknolojisinden faydalanılmış ve kullanılan algoritma türleri performans odaklı karşılaştırılmıştır. Çalışma neticesinde, halihazırda kullanılan video tespit ve analiz uygulamalarının, nesnelerin birbirini engellemsi, olusuz hava şartları gibi dinamikler göz önünde bulundurulduğunda işlemlerin büyük bir bölümünde görüntü verisini analiz etme noktasında yetersiz kaldığı ileri sürülmüştür. Video analiz uygulamalarının belirttilen gerçek dünya şartlarının tek tek ele alınması durumunda çözüm üretebildiği bunun yanında söz konusu olumsuz durumların tamamının vuku bulması durumunda çözüm sunacak bir analiz uygulamasının mevcut olmadığı belirtilmiş, çalışma neticesinde video analiz uygulamalarında daha etkin sonuçlara ulaşılabilmesi için halihazırda kullanılan derin öğrenme yöntemleri ile geleneksel video analiz tekniklerinin birleştirilerek kullanılması önerilmiştir.

Derin öğrenme uygulamaları ile görüntü verilerinin analizi kapsamında Fernandes, Cardoso ve Astrup [20] hem hukuki süreçler hem de adli bilişim aşamalarında kullanılmak üzere cinsel saldırı olaylarına ait verilerinin otomatik, doğru ve objektif değerlendirilmesine imkan sağlayan bir model ortaya koymuşlardır. Çalışma boyunca bilgisayar görmesi ve aynı

zamanda makine öğrenmesi yöntemlerinden faydalanılmış, çalışma kapsamı içerisine, delil yorumlanması, cinsel bölge yara tespiti ve kararın görsel teknikler ile açıklanması gibi birçok husus dahil edilmiştir. Cinsel saldırı izlerinin tespit edilebilmesi açısından geleneksel uygulamalar ile derin öğrenme yöntemleri karşılaştırılmış, gerçekleştirilen testlerin tamamında derin öğrenme yöntemlerinin klasik yöntemlere oranla daha yüksek başarı gösterdiği tespit edilmiştir.

Görüntü verilerinin incelenmesi kapsamında başka bir çalışmada ise Evrişimsel Sinir Ağları (ESA) algoritması kullanan bir adli bişim modeli önerilmiştir [21]. İleri sürülen modelde, görsel verilere ait gri düzey eş oluşum matrisleri ESA algoritmasını beslemek maksadı ile girdi olarak kullanılmıştır. Karşı adli bilişim saldırılarının ortaya çıkarılması ve sahteciliğin etkin olarak tespiti açısından geleneksel yöntemlerle karşılaştırılan model, yüksek başarı ortaya koymuştur.

Dijital verilerin hem bütünlüğünün hem de orjinalliğinin tespitine ilişkin kullanılan aktif ve pasif yöntemler ile derin öğrenme mimarisi ile geliştirilen yöntemler, bu alanda ortaya konulan bir diğer çalışmada birbiri ile karşılaştırılmıştır[3]. Çalışmada, manipüle edilmiş görsel verilerinin tespiti kapsamında ESA temelli metotlar başarılı sonuçlar vermiş olsa bile, söz konusu alanda karşı adli bilişim tekniklerinden de yaygın olarak faydalanıldığı ve bu yöntemlerin de tatminkar neticeler ortaya koyduğu gözlemlenmiştir.

Bu alanda gerçekleştirilen diğer bir derin öğrenme temelli uygulamada, insanlara ait elbiselerden oluşturulmuş görüntü verilerine dayanarak kimlik tespitinde bulunabilen bir model ortaya konulmuştur[22]. Çalışma neticesinde klasik kıyafet veri seti ile görüntü sınıflandırma işlemi gerçekleştirildiğinde ileri sürülen modelin istenilen performansı sergilemediği, bununla beraber veri seti maksadı ile yaygın kullanılan ve popüler marka ismi ile logolar kullanıldığında söz konusu derin öğrenme modelinin %75 seviyesine yakın başarı ortaya koyduğu gözlemlenmiştir.

Görsel verilerin incelenmesine ilişkin olarak Olmos, Tabik, ve Herrera [23] mevcut güvenlik ve kontrol sistemlerinin otomatik olarak görüntü sınıflandırma işlemi gerçekleştirmediğini belirtmiş ve manuel işlem yapılmasına ihtiyaç duyulmadan silah görüntü verilerini otomatik olarak tespit edebilen bir derin öğrenme modeli önermişlerdir. Çalışmada, havaalanları ve adliye binaları gibi güvenlik kontrolünün ön planda olduğu alanlarda, halihazırda kullanılan silah tespit yöntemlerinin çoğunlukla metal cisimleri algılamaya odaklı olduğu, bunun

yanında bu sistemlerin X-ray cihazı ve yürüyen bant gibi maliyeti yüksek parçalar ile birlikte ancak etkin kullanılabildiği, bununla beraber söz konusu maliyetlerin bu sistemlerin kullanımını sınırlandırdığı belirtilmiş ve ortaya konulan handikabın aşılmasına yönelik olarak VGG16 ağ modeli farklı veri setleri ile test edilmiştir. Çalışmaların neticesinde Faster RCNN algoritmasının en iyi görüntü sınıflandırma algoritması olduğu tespit edilmiş bunun yanında söz konusu algoritma yaygın olarak bilinen yedi film kullanılarak elde edilen görsel veri setinde de test edilmiş ve iyi sonuçlar elde edilmiştir.

Görüntü verilerinin incelenmesi ve sınıflandırılması kapsamında ortaya konulan bir diğer çalışmada, adli bilişim analiz süreçlerinde derin öğrenme tabanlı OpenFace uygulamaları farklı veri setleri ile test edilmiştir[24]. Çalışmada adli bilişim inceleme süreçlerinde kullanılmak üzere toplanan yüz görsellerinin benzerlik ve farklılıklarının hangi doğruluk ile bulunabildiğine odaklanılmıştır. Bu kapsamda OpenFace uygulamalarının tatmin edici bir başarı oranı ortaya çıkardığı, bununla beraber yüz verilerine ait görsellerin kalitesinin düşmesi, beraberinde modelin etkinliğini de düşürdüğü tespit edilmiştir. Çalışma neticesinde eğer geliştirilmez ise OpenFace derin öğrenme uygulamalarının görüntü veri analizi kapsamında yetersiz seviyede kalacağı, ancak söz konusu algoritmaların geliştirilmesi durumunda iyi sonuçlar elde edilebileceği vurgulanmıştır.

Mayer ve Stamm [25] iki görsel veriye ait adli izlerin biribiri ile benzer olup olmadığını ortaya koyan ve "Adli benzerlik" adıyla tanımlanan bir görüntü yaklaşım modeli önermişlerdir. Çalışmada, modelin adli izlerin benzer olup olmadığını ortaya koyarken diğer ağ yapılarından farklı olarak başka veriler ile önceden eğitilmeye ihtiyaç duymadığı ve bunun önemli bir avantaj olduğu ileri sürülmüştür. Model, görüntü eşlerinin aynı uygulama ile yapılıp yapılmadığının tespit edilebilmesi noktasında test edilmiştir. Çalışma neticesinde, modelin önceden benzer veri setleri ile eğitilmediği görüntü setlerin de bile doğru sonuçlar verdiği ve bu alanda gerçekleştirilen diğer çalışmalara oranla hata payını yaklaşık yüzde 50 oranında azalttığı gözlemlenmiştir.

Görüntü verilerinin incelenmesine ilişkin olarak gerçekleştirilen bir başka çalışmada, iki farklı makine öğrenmesi algoritması ile hiperspektral kamera yöntemleri olaya ilişkin elbise parçasında yer alan barut kalıntısını insan müdahalesine ihtiyaç duymadan otomatik olarak tespit edebilme noktasında test edilerek incelenmiştir[26]. Çalışmada, farklı kumaşlar üzerinde yer alan barut izi örneklerini içeren hiperspektral kamera görüntüleri ile veri seti oluşturulmuş ve iki farklı mesafeden iki tür mühimmat kullanılarak gerekli barut kalıntıları

elde edilmiştir. Çalışma neticesinde, olay yerinde barut kalıntısının olup olmadığının ortaya konulabilmesi için ikincil bir tanımlama metodunun kullanılması gerektiği ileri sürülmüş, bunun yanında görüntü işleme algoritmaları teknolojisinden faydalanan hiperspektral kamera uygulamalarının, delil toplama ve analiz süreçlerini destekler nitelikte olduğu vurgulanmıştır.

Eriş [27] yaptığı çalışma ile farklı alanlarda etkin olarak kullanılan derin öğrenme algoritmalarından, adli bilişim görüntü analiz aşamalarında da yardımcı bir estrüman olarak faydalanılmasını amaçlamıştır. Çalışma neticesinde, derin öğrenme algoritmaları kullanılarak veri sınıflandırma modeli oluşturmuş, görüntü veri setleri ile yapılan denemelerde yüzde 90 üzerinde doğruluk oranına ulaşılmıştır.

Bu kapsamda yapılan diğer bir çalışmada görüntü üzerinde gerçekleştirilen olası manipülasyon ve sahtecilik işlemlerini ve bu süreçlerde kullanılan görüntü manipülasyon yöntemlerini incelemek üzere çalışmalar gerçekleştirilmiştir[28]. Çalışma kapsamında ImageNet ile farklı derin öğrenme modellerinden faydalanılırken, pratik olarak manipülasyon ve sahtecilik tespit mekanizmasının oluşturulmasının zor olduğu, ancak bununla beraber transfer öğrenme tekniği ve farklı yöntemlerin birleştirilmesi ile manipülasyon/sahtecilik tespit sistemi geliştirilebildiği ileri sürülmüş ve manipülasyon yöntemlerinin sürekli geliştiği, bu gelişmeye paralel olarak ise manipülasyon tespit sitemlerinin de geliştirilmesi gerektiği vurgulanmıştır.

Bu alana dair ortaya konulan son çalışmada ise adli bilişim analiz aşamalarında derin öğrenme teknikleri ile görsel verilerinin doğru ve hızlı sınıflandırılabilmesi konusu üzerinde durulmuştur[29]. Çalışmada, görüntü veri analizi süreçlerinde insan müdahalesinin en aza indirgenmesi hedeflenmiştir. Yüzde 93 oranında başarının elde edildiği çalışmada, ağ yapısının eğitilmesi ve doğrulama işlemleri için 30 bin görsel veri kullanılmıştır.

Yöntem iyileştirme kapsamında ortaya konulan çalışmada ise web sitesi saldırılarına dair analiz ve inceleme aşamalarında makine öğrenimi algoritmalarından etkin bir şekilde faydalanılabileceği ileri sürülmüştür[30]. Özellik seçim işleminin makine öğrenmesi aşamalarında hayati öneme sahip olduğu vurgulanan çalışmada, modelin başarı ve performansının artması ancak söz konusu parametrelerin doğru seçilmesine bağlı olduğu belirtilmiştir. Halihazırda web sitesi saldırıları çerçevesinde delil elde edebilmek için optimal bir seçim parametresinin henüz uygulanmadığı belirtilen çalışmada, wrapper ve

filter yöntemlerine dayanan hibrit bir metot ortaya atılmıştır. İleri sürülen modelin başarılı olduğunun kanıtlanması için birbirinden farklı üç web site saldırı senaryosu kullanılmıştır. Sonuç olarak makine öğrenimi ve veri madenciliği modeli oluştururken hibrit yaklaşımı kullanmak, internet site saldırıları kapsamında inceleme yapan ve adli bişimi için tasarlanmış akıllı otomasyon sistemlere yardımcı olabileceği vurgulanmıştır.

Yöntem iyileştirmeye ilişkin bir diğer çalışmada ise adli bilişim çerçevesinde verinin analiz edilmesini sağlayan ve toplamda 3 farklı aşamadan meydana gelen bir çalışma yöntemi ortaya konulmuştur[31]. Çalışmanın birinci aşamasında android tabanlı telefonlar kapsamında veri incelemesi gerçekleştirilerek aynı zamanda adli bilişim alanında yaygın kullanılan Autopsy ve Paraben E3 cihazlarının karşılaştırılması yapılmıştır. Yapılan işlemler neticesinde android tabanlı telefonlar üzerinde gerçekleştirilen değişikliklere ait izlerin, söz konusu telefonların dahili hafızasında tespit edilebileceği kanıtlanmıştır. Çalışmanın bir sonraki aşamasında android tabanlı cihazlar üzerinde snapchat yazılımına ait veriler, incelenerek snapchat uygulamasında yapılan bazı işlem ve kullanıcı verilerinin Paraben E3 aracılığı ile elde edilebileceği tespit edilmiştir. Üçüncü aşama olan son aşamada ise IBM Watson ve Microsoft Azure yapısında yer alan makine öğrenmesi servisleri performansları açısından birbiri ile karşılaştırılarak teste tabi tutulmuştur. Çalışmada, Microsoft Azure makina öğrenimi stüdyosunun kullanıcı deneyimi açısından daha başarılı olduğu ve ilgili modelleri IBM Watson uygulamasına oranla daha hızlı oluşturduğu gözlemlenmiştir.

Rughani [32] süreç iyileştirme ve otomasyon kapsamına giren çalışmasında, adli bilişim analiz aşamalarında rutin ve sıradan uygulamaların insan müdahalesini en aza indirecek şekilde yapay zeka teknolojileri kullanılarak yapılması gerektiği anlayışına dayanan bir model ileri sürmüştür. Çalışmada, adli bişlişim süreçleri; Delil toplama, analiz ve sunum basamaklarına indirgenmiş ve bu üç basamakta yapay zeka ve makina öğrenimi algoritmaları kullanılarak insan eli ile yapılması gereken ve uzun zaman alan süreçlerin hızlandırılması amaçlanmıştır. Çalışma neticesinde, kullanılması planlanan yapay zeka ve makina öğrenimi algoritmalarının benzer vakalar ile önceden cok iyi eğitilmesi şartı ile, ileri sürülen modelin veri analiz aşamalarında gerekli duyulan zaman ve işlemci gücü ihtiyacını azaltacağı, buna ek olarak iş gücünü de asgari seviyeye çekeceği belirtilmiştir.

Bu alana ilişkin ortaya konulan diğer bir çalışmada ise delil analizine dair otomasyonun yapılabilmesi maksadı ile sayısal mantık ve yapay zekâ teknolojilerinin ne oranda kullanılabileceği test edilmeye çalışılmıştır[33]. Çalışmada, insan müdahalesi ile yapılması

zor olan veri analiz süreçlerinin, optimizasyon problemi gibi ifade edilebileceği önerilmiş ve kanıt olarak ise sayısal mantık programları ile gerçek soruşturma vakalarının formalize edilebildiği ve bir metodolojinin somut inceleme hipotezini nasıl formüle ettiği gösterilmiştir.

Saldırı tespiti ve log güvenlik analizine ilişkin olarak yapılan çalışmada delillerin tespit edilebilmesi adına, sistem dosyalarında yer alan güvenlik kayıtlarının makina öğrenmesi algoritmaları yardımı ile analiz edilerek söz konusu kayıtların başka uygulamalar aracılığı ile manipüle edilip edilmediği ortaya konulmaya çalışılmıştır[2]. Çalışma süresince MS Excel, MS Word veya MS PP gibi birbirinden farklı 10 bilgisayar uygulamasının loglarda bıraktığı izlerden faydalanılarak 42 bin civarında veri oluşturulmuş ve yedi derin öğrenme algoritması oluşturulan bu veri seti yardımı ile eğitilerek test edilmiştir. Yapılan testin sonucunda ise en iyi doğruluk oranı YSA ve rastgele orman (random forest) algoritmaları ile elde edilmiştir.

Pandey, Mujmer, Gyarsiya ve Kanungo [34] log analizine ilişkin yaptıkları çalışmalarında adli bilişim açısından zararlı yazılımların gerçek zamanlı olarak tespit edilmesinin zor olduğunu, bununla beraber bu yazılımların bazı ortak özellikler gösterdiğini ve bu özelliklerin zararlı yazılımların tespitinde ve analizinde kullanılabileceğini ileri sürmüşlerdir. Adli bilişim alanında halihazırda mevcut sorun sahaları ayrıca çalışmada ortaya konulmuştur. Zararlı yazılım ve uygulamaların tespit edilebilmesine ilişkin olarak çalışmada, makine öğrenmesi algoritmaları değerlendirilmeye tabi tutulmuş ve sistem dosyaları içerisinde zararlı yazılımların tespit edilebilmesi adına rastgele orman algoritmasının en etkin algoritma olduğu ileri sürülmüştür. Zararlı yazılımların tespit edilebilmesi kapsamında mevcut olan uygulamalar incelenerek tespit süreçlerinin daha iyi nasıl yapılabileceği ve kullanılan sistemlerin nasıl daha güvenli olabileceği ve bu maksatla ne gibi güvenlik modifikasyonlarının yapılması gerektiği de ayrıca çalışmada vurgulanmıştır.

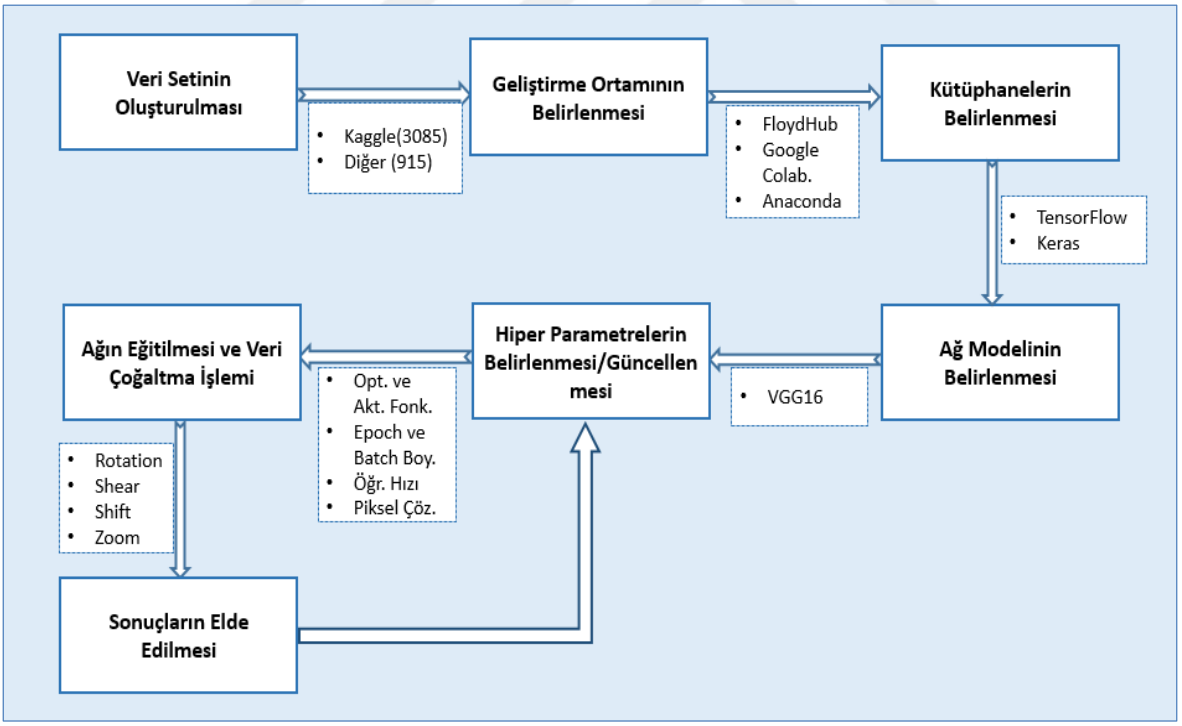
Söz konusu alan dair gerçekleştirilen son çalışmada, öncelikle siber saldırılara karşı, derin öğrenme algoritmalarının etkin olarak kullanılabileceği belirtilmiş ve bu maksata uygun şekilde derin öğrenme ve akıllı hesaplama tekniklerinden faydalanan ve Deep Learning Cyber Forensics (DLCF) olarak isimlendirilen jenerik bir yapı ileri sürülmüştür[35]. Yapılan çalışmanın neticesinde, sadece adli bilişim alanında değil derin öğrenme teknolojilerinin farklı birçok alanda kullanıldığı, dolayısı ile siber adli bilişim alanında da veri boyutunun

en aza indirgenmesi, vakaların tespit edilmesi ve elde edilen sonuçların doğru ve objektif yorumlanması aşamalarında derin öğrenme yöntemlerinden faydalanılabileceği ileri sürülmüştür.

4. ARAÇLAR VE YÖNTEM

Halihazırda kullanımda olan adli bilişim veri analiz yazılım, cihaz ve uygulamaları görsel verilerin analiz edilmesi, değerlendirilmesi ve yorumlanması söz konusu olduğunda, bu işlemleri insan müdahalesi olmaksızın otomatik olarak gerçekleştirme noktasında yetersiz kalmaktadır. Bununla beraber özellikle son yıllarda teknolojinin gelişmesine paralel olarak veri kaydeden, gönderen ve alan bilişim cihaz ve ortamlarının çoğalması, suça ilişkin incelenmesi gereken veri miktarını artırmıştır. Artan iş yükü karşısında, veri inceleme aşamalarında özellikle görüntü verilerinin doğru ve hızlı analiz edilmesi noktasında adli bilişim uzmanlarına yardımcı olacağı değerlendirilen bir görüntü sınıflandırma modeli önerilmiştir.

Tezin bu bölümünde çalışma kapsamında oluşturulan veri seti, kullanılan ağ modeli ve test edilen hiper parametreler hakkında ayrıntılı bilgi verilmiş ve çalışma boyunca takip edilen aşamalar ana hatları ile Şekil 4.1.'de gösterilmiştir.



Şekil 4.1. Önerilen modele ait süreç akış diyagramı

4.1. Veri Setinin Oluşturulması

ImageNet, MNIST ve MS-COCO gibi veri setleri derin öğrenme çalışmalarında modellerin eğitilmesi maksadı ile yaygın tercih edilen veri setlerinden bazılarıdır. Veri seti oluştururken tercih edilecek birçok kaynak mevcut olmakla beraber, elde edilen sonuçların karşılaştırıldığı diğer çalışmalarda kullanılan veri setleri de dikkate alınarak, tezde önerilen modelin eğitilmesi maksadı ile ana kaynak olarak Kaggle veri seti platformundan faydalanılmıştır.

Kaggle platformu, hem açık kaynak hem de binlerce kategoride kapsamlı veri seti yelpazesine sahip olmasından dolayı da ayrıca tercih edilmiştir. Her ne kadar veri seti oluşturma aşamasında ana kaynak olarak Kaggle platformu kullanılsa da bunun yanında yaygın kullanılan arama motorlarından elde edilen görsel verilerden de çalışma boyunca faydalanılmıştır.

Tezde toplamda 4000 bin veri seti kullanılırken bu rakamın 2000 adedini tabanca görüntüleri geriye kalan 2000 adedini ise bıçak görüntüleri oluşturmuştur. Oluşturulan 4000 adet görüntü verisinin 1000 adedi test, 1000 adedi doğrulama (validation), geriye kalan 2000 adet görüntü ise modelin eğitilmesi amacı ile kullanılmıştır.

Modelin eğitilmesi ve doğrulaması için kullanılan tabanca cisimine ait görüntülerin [36-38] tamamı, bıçak cismine ait görüntülerin [39-40] ise sadece 585 adedi Kaggle veri seti platformundan faydalanılarak oluşturulurken, geriye kalan 915 adet bıçak görüntüsünün oluşturulmasında kaynak olarak yaygın bilinen arama motorları kullanılmıştır. Test görüntülerinin elde edilmesinde ise yine Kaggle platformu kulanılmıştır. Tezde kullanılan veri setine ilişkin örnek görseller Resim 4.1.'de sunulmuştur.

Resim 4.1 Veri seti örnekleri

Veri çoğaltma işlemi, ağ yapılarının kullanıldığı çalışmalarda ilgilenilen alana ilişkin yeterli sayıda orjinal görüntünün mevcut olmadığı durumlarda tercih edilir. Veri çoğaltma işlemi, temelde modelin az sayıdaki veri ile etkin olarak eğitilebilmesi için mevcut görsellerin döndürmek, daraltmak, büyütmek veya uzatmak gibi farklı işlemlerden geçirilmesi ve bu işlemlerden geçen görsellerin tekrardan ağın eğitilmesinde kullanılmasıdır.

Tezde ağ modelinin etkin olarak eğitilmesi adına horizontal flip, shift, rotation ve zoom gibi farklı veri çoğaltma yöntemlerinden faydalanılmış ve bu işlemler gerçekleştirilirken yaygın tercih edilen %20 oranı benimsenmiştir.

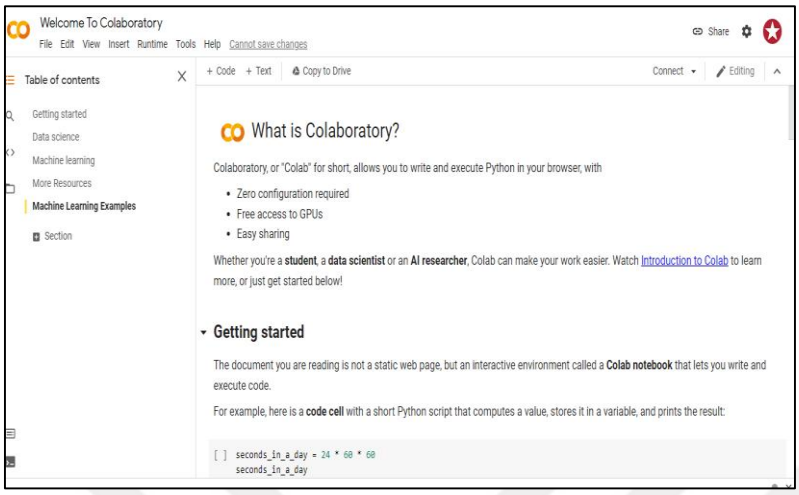
4.2. Geliştirme Ortamı ve Kullanılan Kütüphaneler

Derin öğrenme alanında yapılan çalışmalarda araştırmacıların yaygın olarak tercih ettiği geliştirme ortamlarından bazıları maddelerde sıralandığı gibidir;

- Deep Learning Studio,
- FloydHub,
- Anaconda,
- Deep Learning Kit,
- Google Colaboratory,
- Neural Disegner

Farklı programlama dilleri kullanılarak yazılan geliştirme ortamlarını hem açık kaynak hem de ücretli olarak temin edebilmek mümkündür. Tez boyunca Anaconda, Google

Colaboratory geliştirme ortamları yanı sıra FloydHub'ın ücretli ve ücretsiz versiyonları da denenerek test edilmiştir.



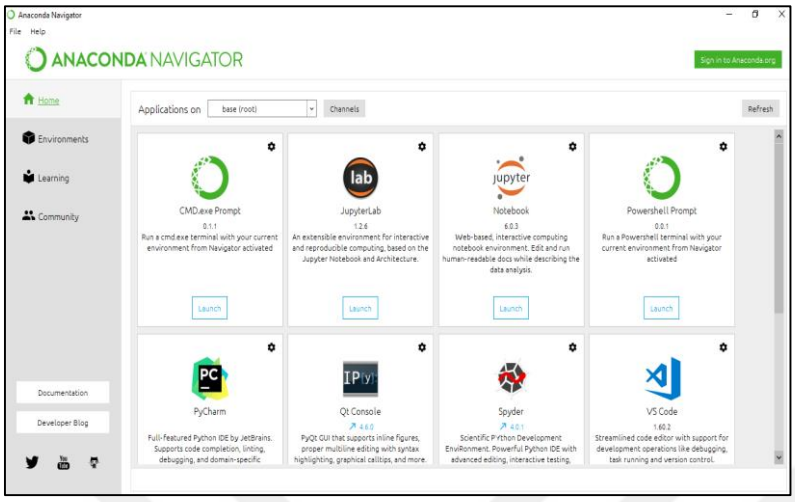
Resim 4.2. Google Colaboratory geliştirme ortamı

Google Colaboratory geliştirme ortamı, araştırmacılar için CPU ve GPU desteği sunan, Python programlama dili ile kod yazılmasına imkan tanıyan, derin öğrenme uygulamaları geliştirirken bu alanda yaygın olarak kullanılan TensorFlow, Keras ve OpenCV gibi kütüphanelerindan faydalanabilmenizi sağlayan, Google şirketinin sunduğu derin öğrenme alanında uygulama geliştirecek ve çok yüksek sistem gereksinimine ihtiyaç duymayacak araştırmacıların sıklıkla tercih ettiği ücretsiz bir bulut hizmetidir. Google Colaboratory geliştirme ortamı başta derin öğrenme alanında kullanılan kütüphaneler olmak üzere bir çok özelliği bünyesinde hazır bulundurmaktadır. Dolayısı ile bu uygulama, yapılandırmaya ihtiyaç duymadan araştırmacılara etkileşimli bir çalışma ortamı sunmaktadır.

Anaconda derin öğrenme platformu ise dünya üzerinde 7 milyondan fazla kullanıcı ile dünyanın en popüler derin öğrenme platformlarının başında gelmektedir. Anaconda derin öğrenme platformu farklı programlama dillerinde yazılmış projelerin çalıştırmakla beraber esas olarak Python programlama dilini kullanmaktadır. Anaconda derin öğrenme platformu, Google Colaboratory platformundan farklı olarak kurulacak sistemin özelliklerine bağlı olarak yapılandırmaya ihtiyaç duyar.

FloydHub geliştirme ortamı ise tıpkı Google Colaboratory geliştirme ortamında olduğu gibi başta TensorFlow ve Keras kütüphaneleri olmak üzere bir çok derin öğrenme kütüphanelerini bünyesinde barındırmaktadır. FloydHub ücretli derin öğrenme platformu, hem sağladığı performans değerleri hem işlem süresi hem de kullanıcı odaklı olması açısından avantaj sağladığından dolayı tezde çoğunlukla FloydHub (GPU-62) geliştirme

ortamı tercih edilmiştir. Tezde görüntü sınıflandırmaya ilişkin ortaya konulan sonuçlar FloydHub'ın ücretli bulut bilişim servisleri ile elde edilen doğruluk oranlarıdır.



Resim 4.3. Anaconda geliştirme ortamı

TensorFlow, Keras, Pytorch veya Theano gibi kütüphaneler derin öğrenme alanına ilişkin uygulamalarda, araştırmacılar tarafından yoğun olarak tercih edilmektedir. Hata vermemesi, birbiri ile uyumu, yaygın kullanım alanı ve birçok platform ile sorunsuz çalışabilmesi gibi avantajlar nedeni ile TensorFlow ve Teras tez çalışmasında faydalanılan derin öğrenme kütüphaneleri olmuşlardır.

Keras kütüphanesi, optimizasyon ve hata fonksiyonunun belirlenmesi ile ağ katman sayısı gibi parametrelerin belirlenmesinde bilgi desteği sağlayan ve çoğunlukla düşük seviye operasyonları desteklemek maksadı ile tercih edilen çatı bir kütüphanedir.

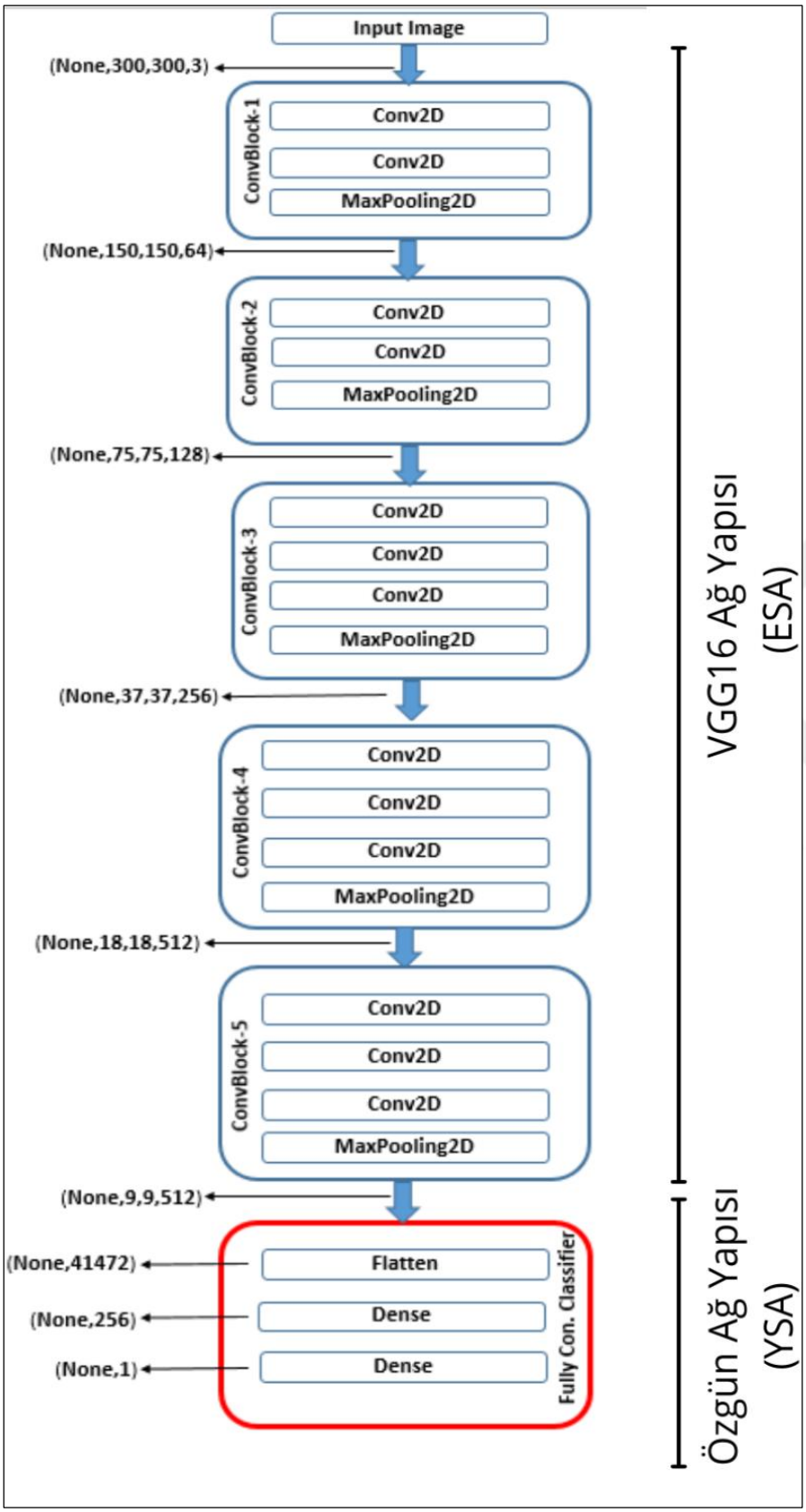
Keras, bu avantajlarına ek olarak önemli bir kod düzenlemesine ihtiyaç duymadan Theano, TensorFlow veya CNTK benzeri düşük seviye derin öğrenme kütüphaneleriyle uyum içerisinde çalışabilir. TensorFlow kütüphanesi ise Google tarafından geliştirilmiş, hızlı işlem gücüne sahip, ölçülebilmesi kolay ve farklı projelere rahatça adapte olabilen yapıya sahip açık kaynak kodlu bir derin öğrenme kütüphanesi statüsündedir.

4.3. Ağ Modelinin Eğitilmesi

Zaman kıstasını ve işlem gücünü etkin kullanarak daha iyi başarı oranına ulaşabilmek adına derin öğrenme çalışmalarında önceden binlerce/milyonlarca farklı veri setleri ile defalarca eğitilmiş ağ yapılarından faydalanmak, araştırmacılar tarafından kullanılan yaygın bir yöntemdir.

Transfer öğrenmesi (Transfer learning) olarak bilinen bu yöntemde çoğunlukla ILSVRC, LeNet veya VGG16 gibi performans ve başarısı kanıtlanmış ağ modelleri tercih edilmektedir. Bahsi geçen modeller, ESA ve tam bağlı (fully connected) YSA olmak üzere iki farklı katmandan oluşurlar. Bu katmanların ilkinde veri setine ait öznitelik (features) çıkarımı yapılırken, ikinci katman olan YSA'da ise sınıflandırma yani classification işlemi gerçekleştirilir. Yüksek başarı oranının yanı sıra görüntü sınıflandırma kapsamında birçok çalışmada yaygın olarak tercih edilen VGG16 ağ yapısı tezde, transfer öğrenmesi maksadı ile kullanılan ağ modeli olmuştur.

VGG16 yapısında yer alan ESA katmanı eğitilmeye ihtiyaç duymadan mevcut hali ile önerilen modele aktarılırken, görüntü sınıflandırma aşaması için üç katmandan oluşan bir ağ yapısı tasarlanmıştır. 14 milyondan fazla değişkenin bulunduğu VGG16 ağ yapısı ile bu ağ yapısının sonuna eklenen 3 özgün katmandan oluşan model yapısı Şekil 4.2.'de sunulduğu gibidir.



Şekil 4.2. VGG16 ağ yapısına dayanan önerilen model

Derin öğrenme çalışmaları maksadı ile ağ yapısı tasarlanırken doğru olarak seçilmesi gereken birçok hiper parametre söz konusudur. Karar kılınacak bu parametrelerin fonksiyonu önemlidir, çünkü bu parametreler modelin başarısının arttırılması adına model yapısının tamamı ile değiştirilmesi ihtiyacını ortadan kaldırmaktadırlar. Parametrelerin mevcut avantaj ve esnekliğine karşın, araştırmacıların bütün parametre türüne ve parametre değerine özellikle deneme yanılma yöntemi ile karar verecek olması ise önemli bir dezavantaj olarak değerlendirilebilir.

Hiper parametrelerin kapsamı oldukça geniştir. Oluşturulacak en basit ağ modellerinde bile fonksiyon türünden, katman sayısına kadar, eğitilecek ağırlık sayısından evre sayısına kadar birçok konuya araştırmacıların karar vermesi gerekir. Dolayısı ile belirlenmesi gereken parametrelerin kapsamı oldukça geniştir.

Parametre türü ve değeri hem çalışma hem de modelin başarısı için kritiktir. Çünkü parametreler üzerinde yapılacak ufak düzenlemeler modelin doğruluk oranını ve devamında bütün çalışmanın başarısını önemli ölçüde değiştirebilir.

Bununla beraber araştırmacılar için hangi parametrenin model kapsamında daha iyi sonuç vereceğini tahmin etmek ve seçilecek parametreye karar vermek kolay değildir. Çünkü, aynı parametre değerlerinin farklı modellerde ortaya çıkaracağı sonuçlar farklı olacağından dolayı parametre tür ve değerleri ancak deneme yanılma yöntemi ile belirlenebilmektedir.

Tezde en iyi doğruluk oranına ulşılabilmesi adına farklı hiper parametre bileşenleri ve bu bileşenlere ait değerler teste tabi tutulmuş ve alınan sonuçlar kapsamında hangi parametrenin kullanılması gerektiğine karar verilmiştir.

4.4. Hiper Parametrelerin Seçimi

Önerilen modelin arzulanan doğruluk oranını elde edebilmesi maksadı ile aktivasyon fonksiyonu, optimizasyon fonksiyonu, kayıp fonksiyonu, öğrenme hızı, evre sayısı, yığın boyutu ve piksel çözünürlüğü olmak üzere toplamda 7 hiper parametre dikkate alınmıştır.

4.4.1. Aktivasyon fonksiyonu

Aktivasyon fonksiyonunun ağ yapıları açısından ana işlevi, nöronlarda bulunana ağırlıkların toplamını hesaplamak ve bu değere eşik (bias) değerinide ekleyerek ağırlık değerlerinin

hesaplanması sağlamak ve ortaya konulan hesabın sonucunda söz konusu nöronun aktif olup olmayacağına karar vermektir. Bu fonksiyonun üstlendiği rol oldukça önemlidir. Çünkü aktivasyon fonksiyonu, doğrusal olmayan gerçek dünya problemlerinin yapay sinir ağları açısından çözülebilmesini mümkün kılmıştır. Aktivasyon fonksiyonun doğru seçilmesi, çalışmada ortaya konulan modelin başarısını doğrudan etkilemektedir. Aktivasyon fonksiyonunun doğru belirlenmesi adına hem gizli katman hem de çıktı katmanında yoğun olarak tercih edilen birçok fonksiyon model üzerinde test edilmiş ve sonuçlar Bölüm 5'te gösterilmiştir.

4.4.2. Optimizasyon fonksiyonu

Optimizasyon fonksiyonu, çalışmada kullanılan ağ yapısının eğitilmesi, ağırlık değerlerinin back propagation (geri yayılım) tekniği ile güncellenmesi ve işlem sonucunda hata değerinin bulunması gibi birçok etkenin belirlenmesinden sorumludur. Bu fonksiyonun ağ yapılarında ki asıl görevi ise hata değerinin minimum seviyeye indirgenmesidir. Optimizasyon foksiyonunun belirlenmesi kadar hata fonksiyonunun seçimi de oldukça önemlidir. Şöyle ki, eğer lokal minimum içeren hata fonksiyonu seçilir ise, bu durumda optimizasyon fonksiyonunun yanılma payı her zaman söz konusudur. ADAM, Ada Delta, SGD, AdaGrad ve OLSİ gibi fonksiyonlar günümüzde derin öğrenme alanında gerçekleştirilen çalışmalarda yaygın olarak tercih edilen optimizasyon fonksiyonlarıdır. Bu kapsamda, Bölüm 5'te önerilen model üzerinde test edilen optimizasyon fonksiyonları ve elde edilen sonuçlar gösterilmiştir.

4.4.3. Kayıp fonksiyonu (Loss fonksiyonu)

Kayıp fonksiyonu oluşturulan model sonucunda elde edilmesi beklenen sonuç ile elde edilen sonucun arasındaki farkı ortaya koyan fonksiyondur. Diğer bir ifade ile, modelin doğruluğunu ortaya koyan fonksiyon türüdür. Bunu elde edilen sonuç ile tahmin edilen sonuç farkını ortaya koyarak gerçekleştirmektedir. Başlangıç aşamasında tahminen belirlenen, müteakip aşamalarda ise elde edilen sonuçlara bağlı olarak güncellenen, katmanlarda yer alan ağırlık değerlerinin belirlenmesinde önemli etkiye sahiptir. Cost fonksiyonu şeklinde de adlandırılan bu fonksiyonun doğru seçimi, geri yayılım (back propagation) yönteminin doğru ve etkin uygulanabilmesi adına oldukça önemlidir. Cross Entropy, Categorical Hinge veya Mean Squared Error gibi fonksiyonlar derin öğrenme

alanında çalışma yapan araştırmacıların yoğun olarak tercih ettiği kayıp fonksiyonu türleridir. Tez çalışması boyunca test edilen kayıp fonksiyonları ve söz konusu test sonuçlarına ilişkin sonuçlar Bölüm 5'te sunulmuştur.

4.4.4. Öğrenme hızı (Learning rate)

Öğrenme hızı, oluşturulan model ağ yapısı beslenirken, doğru sonuçların alınabilemesi adına ayarlanması gereken önemli parametrelerden biridir. Bu hiper parametrenin temel görevi, ağ modeline ait katmanlarda yer alan ağırlıkların geri yayılım işlemine müteakip ne oranda güncelleneceğini ortaya koymasıdır. Öğrenme hızının doğru belirlenmesi oldukça önemlidir, çünkü belirlenecek değer ideal değerden küçük ise bu durumda modelin eğitilme süreci uzayacak ve model verimsiz hale gelecektir. Bunun yanında belirlenen değerin ideal değerden büyük olması durumunda ise model en iyi çözüm noktasından sapacaktır. Tez çalışması boyunca test edilen öğrenme hızı değerleri ve söz konusu test sonuçlarına ilişkin sonuçlar Bölüm 5'te sunulmuştur.

4.4.5. Evre sayısı (Epoch sayısı)

Evre sayısı ile ifade edilen, veri setinde bulunan tüm görsellerin modelde kullanılan ağ katmanlarından bir defa geçmesi işlemidir. Evre değeri, derin öğrenme çalışmalarında önemli bir yer işgal eder, çünkü modelin yeterli oranda eğitilmesi ancak bu değerin artırılması ile mümkündür. Söz konusu değer, ideal noktadan düşük olarak hesaplanır ise ağın yetersiz eğitilmesi durumu oluşmakta, ideal noktadan yüksek belirlenir ise bu durumda da ağın aşırı ezberlemesine (overfitting) neden olmaktadır. Tez çalışması boyunca test edilen evre sayısı değerleri, değerlere ait test sonuçları ve bu sonuçların grafik gösterimleri Bölüm 5'te sunulmuştur.

4.4.6. Yığın boyutu (Batch boyutu)

Derin öğrenme çalışmalarında oluşturulan veri setinin tamamının aynı anda ağa yedirilmesi hem ağın kapasitesi açısından hem de kullanılan geliştirme ortamının işlem gücü açısından mümkün değildir. Dolayısı ile veri setlerinin belli sayı veya paketler halinde ağa yedirilmesi gerekir. Yığın boyutu ile ifade edilen model eğitilirken her seferinde modele gönderilen veri setlerinden oluşan paket sayısıdır. Bütün parametrelerde olduğu gibi yığın boyutunun ideal

olarak hesaplanabilmesi de modelin başarı oranını belirleyen önemli hususlardandır. Dolayısı ile yığın sayısının artırılması modelin doğruluk oranının artması ile doğrudan ilişkilidir. Tez çalışması boyunca test edilen yığın boyutu değerleri ve söz konusu test sonuçlarına ilişkin sonuçlar Bölüm 5'te sunulmuştur

4.4.7. Piksel çözünürlüğü

Oluşturulan ağ modellerinin standart bir piksel çözünürlüğü formatına kavuşturularak eğitilmesi, modelin başarılı olması adına bir gerekliliktir. Bu noktadan hareketle veri setinde yer alan bütün görsellerin boyutları standart piksel çözünürlüğüne getirilmiştir. Tez çalışması boyunca test edilen piksel çözünürlüğü değerleri ve söz konusu test sonuçlarına ilişkin sonuçlar Bölüm 5'te sunulmuştur

5. BULGULAR VE DEĞERLENDİRME

Önerilen model ile en iyi başarı oranının yakalanabilmesi adına Bölüm 4.4'te ayrıntılı açıklanan bütün hiper parametre türleri hem farklı fonksiyonlar ile hem de bu fonksiyonlara ait farklı değerler ile test edilmiştir. Test esnasında her bir denemede sadece bir parametre üzerinde değişikliğe gidilmiş diğer parametre türleri ve bu türlere ait değerler ise sabit tutulmuştur. Sonuçların yer aldığı çizelge ve tablolarda doğruluk oranı (accuracy) olarak ifade edilen değer, Eş. 5.1.'de görüldüğü üzere doğru olarak sınıflandırılan veri seti görsellerinin, toplam veri seti sayısına oranıdır.

$$Doğruluk\ Oranı\ = \frac{(TP + TN)}{(TP + FP + FN + TN)} \tag{5.1}$$

Aktivasyon fonksiyonunun doğru belirlenmesi adına model üzerinde Sigmoid, ReLu, Softmax, Linear ve Tanjant fonksiyonları test edilmiştir. Test süresince çıktı katmanında ideal değerin tespit edildiği Sigmoid fonksiyonu sabit tutulmuş, gizli ağ katmanlarında ise ReLu, Softmax, Linear ve Tanjant fonksiyonları farklı değerler ile test edilmiş elde edilen sonuçlar Çizelge 5.1.'de sunulmuşur.

Çizelge 5.1. Aktivasyon fonksiyon ve değerleri

Aktivasyon Fonksiyonu	**Gizli Katman ve Çıktı Katmanı**			
	Linear ve Sigmoid	**Tanjantve Sigmoid**	**Softmax ve Sigmoid**	**Relu ve Sigmoid**
Doğruluk Oranı	%89.6	%89.4	%85.7	**%97.8**
Kayıp Oranı	0.25	0.25	0.63	**0.17**

Aktivasyon fonksiyonları kapsamında test edilen fonksiyon çeşitleri arasında ReLu ile en yüksek doğruluk oranı yakalanırken, Softmax ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir.

Optimizasyon fonksiyonunun doğru tespit edilmesi maksadı ile RMSProp, AdaGrad, AdaDelta, Adam ve SGD fonksiyonları model üzerinde teste tabi tutulmuştur. Bu kapsamda elde edilen doğruluk oranları Çizelge 5.2.'de sunulmuştur.

Çizelge 5.2. Optimizasyon fonksiyonları ve değerleri

Optimizasyon fonksiyonu	**AdaDelta**	**SGD**	**AdaGrad**	**Adam**	**RMSProp**
Doğruluk Oranı	%60.5	%70.5	%76.5	%89.7	**%97.8**
Kayıp Oranı	0.66	0.60	0.53	0.24	**0.17**

Optimizasyon fonksiyonları kapsamında test edilen fonksiyon çeşitleri arasında RMSProp ile en yüksek doğruluk oranı yakalanırken, AdaDelta ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir.

Kayıp fonksiyonunun doğru tespit edilmesi adına Binary Crossentropy (BC), Sparse Categorical Crossentropy (SCC), Categorical Hinge (CH), Kullback Leibler Divergence (KLD), Mean Squared Error (MSE), Mean Absolute Error (MAE) ve Mean Squared Logarithmic Error (MSLE) fonksiyon türleri test edilmiştir. Bu kapsamda ulaşılan doğruluk oranı değerleri Çizelge 5.3.'te sunulmuştur.

Çizelge 5.3. Kayıp fonksiyonları ve değerleri

Kayıp Fonksiyonu	**CH**	**MSE**	**MSLE**	**MAE**	**SCC**	**KLD**	**BC**
Doğruluk Oranı	%89.0	%89.8	%89.6	%86.2	Anlamlı sonuç elde edilemiştir	Anlamlı sonuç elde edilmemiştir	**%97.8**
Kayıp Oranı	0.62	0.07	0.03	0.14			**0.17**

Kayıp fonksiyonu kapsamında test edilen fonksiyon çeşitleri arasında Binary Crossentropy ile en yüksek doğruluk oranı yakalanırken, Mean Absolute Error ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir. Bunun yanında KLD ve SCC fonksiyon türleri ile gerçekleştirilen testlerde anlamlı sonuçlara ulaşılamamıştır.

Öğrenme hızının doğru tespit edilmesi maksadı ile farklı değerler model üzerinde denenmiş bu kapsamda elde edilen sonuçlar Çizelge 5.4.'de sunulmuştur.

Çizelge 5.4. Öğrenme hızı ve değerleri

Öğrenme Hızı Değeri	**0.001**	**0.0001**	**0.00001**	**0.00002**	**0.00003**
Doğruluk Oranı	%50	%93,4	%94.8	**%97,8**	%95.9
Kayıp Oranı	7.71	0.21	0.24	**0.17**	0.13

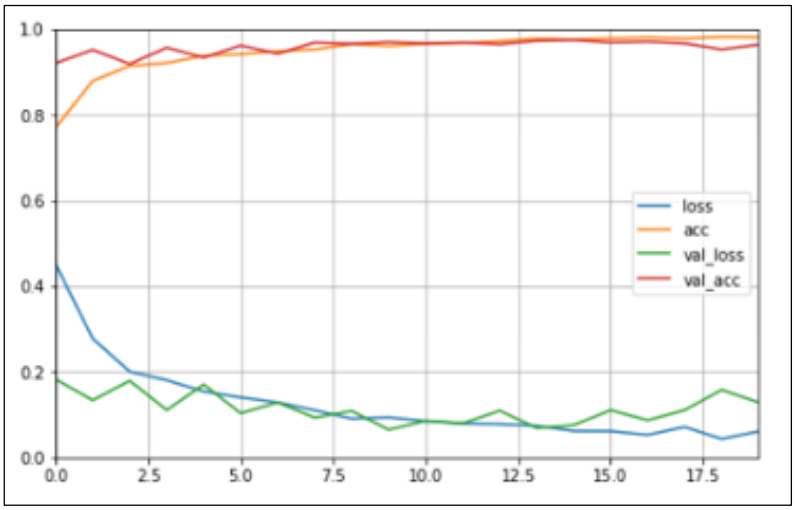
Öğrenme hızı kapsamında test edilen değerlerden 0.00002 değeri ile en yüksek doğruluk oranı yakalanırken, 0.001 değeri ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir.

Evre sayısının doğru tespit edilmesi maksadı ile farklı değerler model üzerinde denenmiş bu kapsamda elde edilen sonuçlar Çizelge 5.5.'de sunulmuştur.

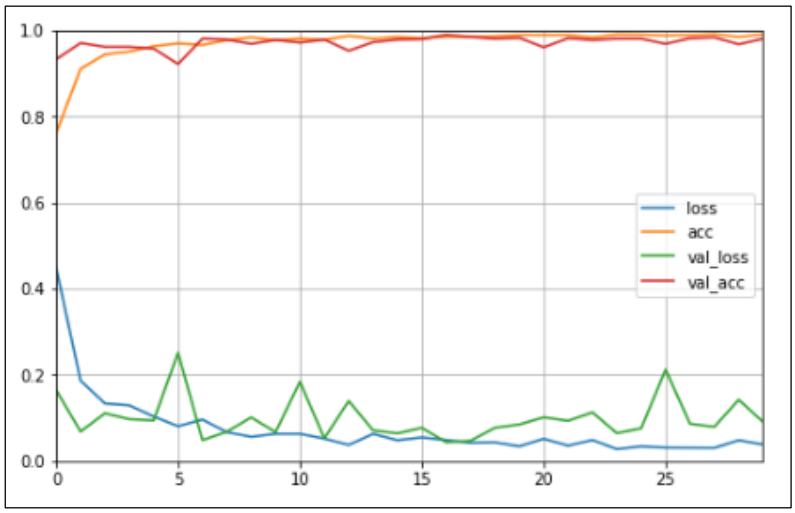
Çizelge 5.5. Evre sayısı ve değerleri

Evre Sayısı	**20**	**30**	**45**	**60**
Doğruluk Oranı	%96,5	%97,8	%97,1	%97.2
Kayıp Oranı	0.15	0.17	0.20	0.25

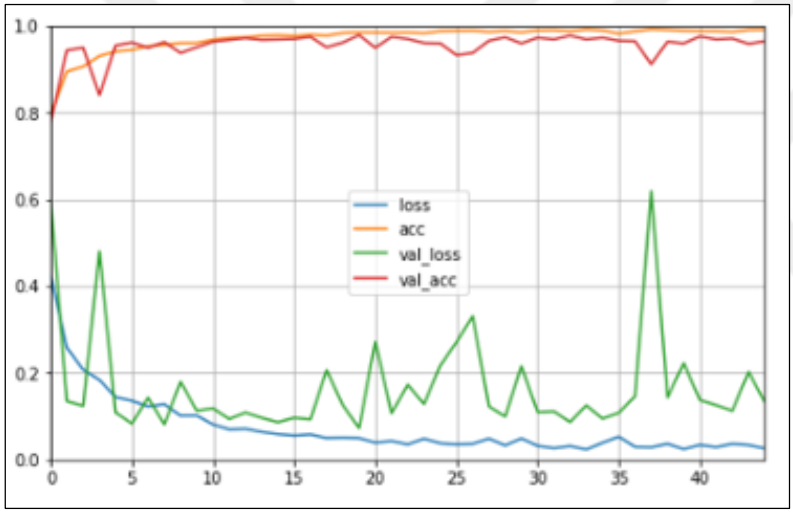
Evre sayısı kapsamında test edilen değerlerden 30 değeri ile en yüksek doğruluk oranı yakalanırken, 20 değeri ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir. Test edilen evre sayılarına ilişkin doğruluk oranı grafikleri Şekil 5.2., 5.3, 5.4 ve 5.5'da gösterilmiştir.



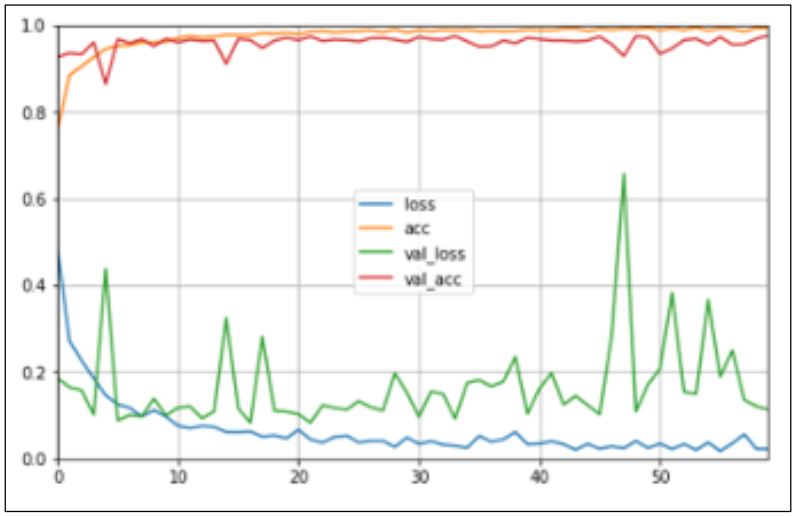
Şekil 5.2. 20 değeri ile elde edilen doğruluk oranı



Şekil 5.3. 30 değeri ile elde edilen doğruluk oranı



Şekil 5.4. 45 değeri ile elde edilen doğruluk oranı



Şekil 5.5. 60 değeri ile elde edilen doğruluk oranı

Yığın boyutunun doğru tespit edilmesi maksadı ile farklı değerler model üzerinde denenmiş bu kapsamda elde edilen sonuçlar Çizelge 5.6.'da sunulmuştur.

Çizelge 5.6. Yığın boyutu ve değerleri

Yığın Boyutu	**10**	**20**	**30**	**40**
Doğruluk Oranı	%95.2	**%97.8**	%95.3	%94.9
Kayıp Oranı	0.18	**0.17**	0.28	0.30

Yığın boyutu kapsamında test edilen değerlerden 20 değeri ile en yüksek doğruluk oranı yakalanırken, 40 değeri ile ise en düşük doğruluk oranına ulaşıldığı gözlemlenmiştir.

Piksel çözünürlüğünün doğru tespit edilmesi maksadı ile farklı değerler model üzerinde denenmiş bu kapsamda elde edilen sonuçlar Çizelge 5.7.'de sunulmuştur.

Çizelge 5.7. Piksel çözünürlüğü ve değerleri

Piksel Çözn.	**100*100**	**150*150**	**200*200**	**300*300**	**400*400**
Doğruluk Oranı	%87	%97.1	%50	**%97.8**	Anlamlı sonuç elde edilememiştir
Kayıp Oranı	7.66	0.15	0.69	**0.17**	

Piksel çözünürlüğü kapsamında test edilen değerlerden 300*300 değeri ile en yüksek doğruluk oranı yakalanırken, 200*200 değeri ile ise en düşük doğruluk oranına ulaşılmış, 400*400 değerinde ise anlamlı sonuçların elde edilemediği gözlemlenmiştir.

Literatür araştırması boyunca incelenen çalışmalarda, delil/veri inceleme süreçlerinin insan müdahalesinden kurtarılması ve bu süreçlerinin otomasyonunun sağlanması maksadı ile hız ve doğruluk faktörlerinin geliştirilmesi üzerinde durulduğu ve söz konusu geliştirmenin sağlanabilmesi adına video, görüntü, log dosyası, ses ve metin gibi farklı veri formatlarının önerilen modeller aracılığı ile sınıflandırılarak analiz edildiği veya edilmeye çalışıldığı tespit edilmiştir.

Son yıllarda ortaya konulan çalışmalar arasında özellikle [23,27,29] ile adli bilişim süreçlerinde elde edilen görüntülerin doğru sınıflandırılması ve analiz edilmesi sureti ile bu süreçlerde mevcut insan müdahalesinin minimum seviyelere çekilmesi ve söz konusu veri

inceleme süreçlerinin hızlandırılarak bu alanda çalışma yapan uzmanların iş yükünün düşürülmesi hedeflenmiştir.

[23,27,29] ile ortaya konulan çalışmalarda kullanılan hiper parametre türleri ile elde edilen doğruluk oranları, tezde önerilen ağ modeline ait parametre türleri ve doğruluk oranları ile karşılaştırılmış, her bir çalışma neticesinde ulaşılan sonuçlar Çizelge 5.8.'de ayrıntılı olarak sunulmuştur.

Çizelge 5.8. Çalışmalara ait ana değişken ve hiper parametreler

Referans Numarası	**Veri Seti Türü**	**Veri Seti Görüntü Sayısı**	**Veri Çoğaltma Yöntemi**	**Ağ Modeli**	**Hiper Parametreler**			**Doğruluk Oranı**
					Opt. Fonk.	**Akt. Fonk.**	**Kayıp Fonk.**	
23	ImageNet	3000	N/A*	VGG-16	SGD	ReLU	N/A*	%91,43
27	ImageNet ve Diğer Kaynaklar	6660	Mevcut	Faster RCNN	N/A	N/A	N/A*	%95,00
29	ImageNet	25000	Mevcut	Özgün	ADAM	Sigmoid	MAPE	%93,58
Önerilen Model	Kaggle Platformu ve Diğer Kaynaklar	4000	Mevcut	VGG-16	RMSprop	ReLU	Binary Cross Entropy	%97,80

**: Bilinmiyor*

Tezde, farklı parametre türleri ve değerlerleri ile yapılan çalışma ve testler neticesinde ağ katmanlarında yer alan hiper parametrelerin modelin başarısı üzerinde önemli etkiye sahip oldukları ve bu parametrelere ait değerlerin ancak deneme yanılma yolu ile nihai olarak belirlenebileceği önerilen model üzerinde gerçekleştirilen test ve denemeler ile ortaya konulmuştur.

Ağ katmanlarında tercih edilen fonksiyon türleri, ağda bulunan katman ve değişken sayıları veya model eğitilirken kullanılan yığın ve evre değerleri üzerinde gerçekleştirilen hassas düzenleme ve güncellemelerin (fine tuning) önerilen modelin performansına doğrudan etki ettiği yapılan test ve denemeler neticesinde gözlemlenmiştir. Önerilen modele ait hiper parametreler üzerinde yapılan hassas değişiklikler sonucunda ulaşılan doğruluk oranının diğer çalışmalara kıyasla yükseldiği Bölüm 5'te yer alan çizelge ve tablolar ile ortaya konulmuştur.

Teknolojinin her alanında meydana gelen gelişmelere paralel olarak hem ülkemizde hem de dünyada hukuki işlem ve süreçlerde dijital verilere atfedilen değer ve önem arttığı gibi aynı zamanda bu verilerin hukuksal zeminde doğru kararların alınabilmesi adına kullanım oranı da katlanarak artmıştır. Teknolojini imkanlarının yaygın olarak kullanılması ile beraber ise suç soruşturmaları kapsamında farklı dijital kaynaklardan toparlanan veri ve delil kapasitesinde önceki dönemlere kıyasla eksponansiyel artış meydana gelmiştir.

Geldiğimiz noktada eksponansiyel artış gösteren veri boyutu manuel olarak yapılan analiz aşamalarının etkinliğinin sorgulanmasına neden olmaktadır. Dolayısı ile bahsi geçen olumsuz durumun giderilmesi ve hem analiz hem de hukuki süreçlerde artan veri miktarına paralel olarak verimliliğin artması ancak verilerin doğru, hızlı ve otomasyon ile yapılması ile mümkün olabilecektir.

Söz konusu otomasyon ve doğruluk adımlarının yapılabilmesi için tezde önerilen görüntü sınıflandırma modelinin, adli bilişim analiz süreçlerinin verimliliğinin artırılarak işlemlerin makul zaman aralığında ve arzulanan doğruluk oranında tamamlaması, nihai olarak ise hukuki süreçlerde meydana gelen aksaklıkların minimum seviyeye indirgenmesi adına önemli olduğu değerlendirilmektedir.

6. SONUÇ VE ÖNERİLER

Bu tezde, adli bilişim analiz aşamalarında hız ve doğruluk unsurlarının artırılması, manuel inceleme adımlarının ve insan müdahalesi süreçlerinin en aza indirgenmesi adına görsel verileri yüksek doğruluk oranı ile sınıflandırmayı sağlayan VGG16 ağ tabanlı bir model önerilmiştir.

Suç kapsamında elde edildiği varsayılan veriler, TensorFlow ve Keras derin öğrenme kütüphaneleri desteği ile FloydHub geliştirme ortamında önerilen model ile teste tabi tutulmuş ve söz konusu veriler üzerinde sınıflandırma işlemleri gerçekleştirilmiştir. FloydHub geliştirme ortamında gerçekleştirilen testler sonucunda elde edilen doğruluk oranları ile model üzerinde kullanılan hiper parametre türleri ve bu parametrelere ait değerler görüntü sınıflandırma ve adli bilişim alanında ortaya konulan farklı çalışmalar ile karşılaştırılmıştır.

Önerilen modelin adli bilişim analiz aşamalarında insan hatalarının minimum seviyelere indirgenmesi ve bunun neticesinde ise bütün olarak analiz doğruluk oranlarınının artırılması adına veri inceleme süreçlerinde adli bilişim uzmanları tarafından yardıcı bir metod olarak kulanılabileceği değerlendirilmektedir.

Tezde ortaya konan görüntü sınıflandırma çalışmasının kapsamı sadece görüntü formatında yer alan veri setleri ile sınırlandırılmıştır. Mevcut modelin geliştirilerek farklı modeller oluştrulması şartı ile sadece görüntü formatında ki veriler değil aynı zamanda ses, log, video veya başka formatta bulunan verilerde de adli bilişim analiz aşamalarında yardımvcı bir yöntem olarak kullanılabileceği değerlendirilmektedir. Modelin, yardımcı bir eleman olarak değerlendirilmesine ek olarak veri analiz aşamalarının tam otomasyonunun yapılabilmesi adına farklı derin öğrenme modellerinin ileride yapılacak çalışmalarda kullanılabileceği değerlendirilmektedir.

KAYNAKLAR

1. Ganesh, V. (2017). Artificial intelligence applied to computer. *International Journal of Advance Research in Computer Science and Management Studies*, 5(5), 21-29.

2. Mohammad, R.M.A., Alqahtani, M. (2019). A comparison of machine learning techniques for file system forensics analysis. *Journal of Information Security and Applications*, 46, 53-61.

3. Ferreire, W.D., Ferreire, C.B.R., Junior, G.C., and Soares, F. (2020). A review of digital image forensics. *Computers and Electrical Engineering*, 85, 106685.

4. Başar, Y. (2015). Siber suç soruşturmalarında adli bilişim incelemeleri. Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

5. Palmer, G.L.(2001). A road map for digital forensic research. *Digital Forensic Research Conference*, August 7-8, New York, United States of America, 23.

6. Gül M.(2018). Adli Bilişim Atlatma Teknikleri ve Karşı Tedbirler, Yüksek Lisans Tezi, Milli Savunma Üniversitesi Hezarfen Havacılık ve Uzay Teknolojileri Enstitüsü, 19.

7. İnternet: National Instıtude of Justice (NIJ) , URL: https://nij.ojp.gov/digital-evidence-and-forensics, Son erişim tarihi 11.08.2020

8. Özen M.,Özocak G. (2015) Adli bilişim, elektronik deliller ve bilgisayarlarda arama ve el koyma tedbirlerinin hukuki rejimi. *Ankara Barosu Dergisi*, 45-46.

9. Pilli E.S.,Joshi R.C., Niyogi R. (2010) A generic framework for network forensics. *International Journal of Computer Applications*, 1, 11, 1.

10. Lim K.,Lee S. (2008) A methodology for forensic analysis of embedded systems. *International Conference on Future Generation Communication and Networking*, December 13-15, Hainan Island, China.

11. Son J. (2012), Social network forensics: Evidence extraction tool capabilities, School of Computing and Mathematical Sciences, Auckland, New Zealand

12. Dimitriadis A., Ivezic N.,Kulvatunyou B., Mavridis I. (2019) Digital forensics framework for reviewing and investigating cyber attacks, Array, 5.

13. Kaur R., Kaur A. (2012) Digital forensics. *International Journal of Computer Applications*, 50, 5.

14. Bucak Y. (2019) Adli bilişim ve Türk Ceza Muhakemesi hukukunda bilgisayarlarda arama, Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü, İstanbul, 32.

15. Kansagara, N., and Singh, S. (2017). Thematically clustering in digital forensics text string searching: A survey. *International Journal of Advanced Research in Computer Science*, 8(3), 1128-1130.

16. Korkmaz, Y. ve Aytuğ, B. (2018). Adli bilişim açısından ses incelemeleri. *Science and Engineering Journel of Fırat University*, 30(1), 329-343.

17. Orozco, A.L.S., Huaman, C.Q., Alvarez, D.P., and Villalba, L.J.G. (2020). A machine learning forensics technique to detect post-processing in digital videos. *Future Generation Computer Systems*, 111, 199–212.

18. Chaves, D., Fidalgo, E., Alegre, E., Rodriguez, R.A., Martino, F.J., and Azzopardi, G. (2019). Assessment and estimation of face detection performance based on deep learning for forensic applications. *Sensors*, 20, 16, 4491.

19. Sreenu, G., and Durai, M.A.S. (2019). Intelligent video surveillance: A review through deep learning techniques for crowd analysis. *J Big Data*, 6, 48.

20. Fernandes, K., Cardoso, J.S., and Astrup, B.S. (2018). A deep learning approach for the forensic evaluation of sexual assault. *Pattern Analysis and Applications*, 21 629–640.

21. Sun, J.Y., Kim, S.W., Lee, S.W., and Ko, S.J. (2018). A novel contrast enhancement forensics based on convolutional neural networks. *Signal Processing: Image Communication*, 63, 149–160.

22. Bedeli, M., Geradts, Z., and Eijk, E. (2018). Clothing identification via deep learning : Forensic applications. *Forensic Sciences Research*, 3(3), 219–229.

23. Olmos, R., Tabik, S., and Herrera, F. (2018). Automatic handgun detection alarm in videos using deep learning. *Neurocomputing*, 275, 66–72.

24. Fydanaki, A., and Geradts, Z. (2018). Evaluating OpenFace: An open-source automatic facial comparison algorithm for forensics. *Forensic Sciences Research*, 3(3), 202–209.

25. Mayer, O., and Stamm, M.C. (2020). Forensic similarity for digital images. *IEEE Transactions On Information Forensics And Security*, 15, 1331-1346.

26. Glomb, P., Romaszewski, M., Cholewa, M., and Domino, K. (2018). Application of hyperspectral imaging and machine learning methods for the detection of gunshot residue patterns. *Forensic Science International*, 290, 227–237.

27. Eriş, M. (2018). Derin öğrenme yöntemleri kullanarak adli bilişim incelemelerinde delil çıkarımının gerçekleştirilmesi, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.

28. Thakur, R., and Rohilla, R. (2020). Recent advances in digital image manipulation detection techniques: A brief review. *Forensic Science International*, 312, 110311.

29. Karakuş, S. (2018). Derin öğrenme yöntemleri kullanarak dijital deliller üzerinde adli bilişim incelemesi, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.

30. Babiker, M., Kararslan, E., and Hoşcan, Y. (2019). A hybrid feature-selection approach for finding the digital evidence of web application attacks. *Turkish Journal of Electrical Engineering & Computer Sciences*, 27, 4102 – 4117.

31. Raji, M.K. (2018). Digital forensic tools & cloud-based machine learning for analyzing crime data, M. Sc. Thesis, Georgia Southern University Department of Information Technology, Georgia, United States of America.

32. Rughani, P.H. (2017). Artificial intelligence based digital forensics framework. *International Journal of Advanced Research in Computer Science*, 8(8), 10-14.

33. Costantini, S., Gasperis, G., and Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence*, 86, 193–229.

34. Pandey, A., Mujmer, S., Gyarsiya, P., and Kanungo, S. (2018). A study on digital forensics using various algorithms for malware detection. *International Journal of Advanced Research in Computer Science*, 9(3), 85-89.

35. Karie, N.M., Kebande, V.R., and Venter, H.S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. *Forensic Science International: Synergy*, 1, 61-67.

36. İnternet: Sasank, S. Guns Dataset. *Cipec*.URL: https://www.kaggle.com/issaisasank/guns-object-detection, Son Erişim Tarihi: 02.02.2022.

37. İnternet: Kumar, A. Guns Detection Dataset (2nd ver.). *Cipec*.URL: https://www.kaggle.com/atulyakumar98/gundetection, Son Erişim Tarihi: 02.02.2022.

38. İnternet: Khatri, Y. Guns Dataset (1th ver.). *Cipec*.URL: https://www.kaggle.com/khatriyash/csgo-guns-dataset, Son Erişim Tarihi: 02.02.2022.

39. İnternet: Shekhar, S. Knife Dataset (1th ver.). *Cipec*.URL: https://www.kaggle.com/shank885/knife-dataset, Son Erişim Tarihi: 02.02.2022.

40. İnternet: Singh, V. Knife Detection Dataset (1th ver.). *Cipec*.URL: https://www.kaggle.com/vijaysingh888/knife-detection, Son Erişim Tarihi: 02.02.2022.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : Dilber, İsrafil
Uyruğu : T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilişim Enstitüsü	2022
Lisans	Kara Harp Okulu	2008
Lise	Kuleli Askeri Lisesi	2004

İş Deneyimi

Yıl	Yer	Görev
2022-Halen	TSK	Subay

Yabancı Dil

İngilizce

Tezden Üretilen Yayın

Dilber, İ. ve Çetin, B. (2021). Adli bilişim incelenme süreçlerinde yapay zeka kullanımı: VGG16 ile görüntü sınıflandırma. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 9(5), 1695-1706.

Hobiler

Tenis, fizik, kitap, yabancı dil

GAZİLİ OLMAK AYRICALIKTIR...