



T.C.
KAHRAMANMARAŞ ST İMAM NİVERSİTESİ
FEN BİLİMLERİ ENSTİTS

MAHREMİYET DUYARLI YAPAY ZEKÂ SİSTEMİ İLE COVID-19 HASTALIĞININ TESPİT EDİLMESİ

ABDULLAH İSMETOĞLU

YKSEK LİSANS TEZİ
ENFORMATİK ANABİLİM DALI

KAHRAMANMARAŞ 2022

T.C.
KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

**MAHREMİYET DUYARLI YAPAY ZEKÂ SİSTEMİ
İLE COVID-19 HASTALIĞININ TESPİT EDİLMESİ**

ABDULLAH İSMETOĞLU

YÜKSEK LİSANS TEZİ
Enformatik Anabilim Dalı

KAHRAMANMARAŞ 2022

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin akademik kural ve etik davranışlar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

ABDULLAH İSMETOĞLU



Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bilgilerin çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

MAHREMİYET DUYARLI YAPAY ZEKÂ SİSTEMİ İLE COVID-19 HASTALIĞININ TESPİT EDİLMESİ

(YÜKSEK LİSANS TEZİ)

ABDULLAH İSMETOĞLU

ÖZET

Covid-19 hastalığı; ilk olarak Çin'in Hubei eyaleti Wuhan kentinde görülen solunum yoluyla insandan insana hızlı bir şekilde bulaştığı bilinen ve DSÖ tarafından pandemi ilan edilen bir hastalıktır. Bu hastalığın teşhisinde PCR testleri haricinde akciğerden çekilen CT ve CXR görüntüleri kullanılır. Ancak yeterli sayıda hekimin olmaması, çok sayıda kişinin muayene sırası beklemesi gibi sebepler dolayısıyla hastalık teşhisi geç yapılabilmektedir. Günümüzde yapay zekâ ve derin öğrenme tıp ve sağlık alanında yüksek başarılı ve hızlı çözümler sunmaktadır. Ancak hastalık verileri hassas veri olduğu için yapılan yapay zekâ temelli çalışmalarda mahremiyet, önemli bir problem haline gelmiştir. Bu tez çalışmasında Covid-19 hastalığının mahremiyet duyarlı bir şekilde tespit edilebilmesi için yeni bir sistem geliştirilmiştir. Geliştirilen bu sistemde derin öğrenme mimarilerinden olan evrişimli sinir ağlarından (CNN) faydalanılmış mahremiyet koruyucu önlem olarak ise diferansiyel mahremiyet ile gradyanlara gürültü ekleme yöntemi tercih edilmiştir. Yapılan deneylerde geliştirilen sistemin başarısı, 5 farklı veri kümesi kullanılarak test edilmiş ve maksimum %97 başarıya ulaşıldığı görülmüştür.

Anahtar Kelimeler: Yapay Zekâ, Derin Öğrenme, Covid-19, Veri Mahremiyeti, Diferansiyel Mahremiyet

Kahramanmaraş Sütçü İmam Üniversitesi

Fen Bilimler Enstitüsü

Enformatik Anabilim Dalı Ekim/2022

Danışman: Dr. Öğr. Üyesi Yavuz CANBAY

Sayfa Sayısı: 89

**DETECTING COVID-19 DISEASE BY USING PRIVACY AWARE ARTIFICIAL
INTELLIGENCE SYSTEM
(M.Sc. THESIS)**

ABDULLAH İSMETOĞLU

ABSTRACT

Covid 19, emerging in the Wuhan city of the Hubei State of China, is a serious disease that is known to spread from person to person quickly by the respiratory tract and is declared a pandemic by WHO. Except for PCR tests, CT and CXR images scanned from the lungs are used to diagnose this disease. However, the diagnosis may be made late due to some reasons, such as the lack of enough doctors or the high number of patients waiting in line for examination. In today's world, artificial intelligence and deep learning provide quick and highly successful solutions in the medical and healthcare fields. Nevertheless, as the disease data is personal, privacy can be a big problem in medical studies based on artificial intelligence. This thesis has developed a new system to diagnose Covid-19 in a privacy-aware way. In this developed system, Convolutional Neural Networks (CNN), one of the bases of deep learning, is used. Adding noise to gradients with differential privacy is preferred as a prevention mechanism for privacy protection. In the experiments, the success of this developed system was tested by using five different data sets, and it has been observed that a maximum of 97 successes have been achieved.

Keywords: Artificial Intelligence, Deep Learning, Covid-19, Data Privacy, Differential Privacy

Kahramanmaraş Sütçü Imam University
Graduate School of Natural and Applied Sciences
Department of Informatics, October/2022

Supervisor: Asst. Prof. Dr. Yavuz CANBAY

Page number: 89

TEŞEKKÜR

Yüksek lisans eğitimim süresi içerisinde bilgi ve birikimlerini benden esirgemeyen, tez çalışmamın her aşamasında bilimsel konulardaki desteğinin yanında anlayış ve sabır ile çalışmamın etkin bir şekilde ilerlemesini sağlayan kendisiyle çalışmaktan onur duyduğum tez danışmanım kıymetli hocam Sayın **Dr. Öğr. Üyesi Yavuz CANBAY’a** sonsuz saygı ve teşekkürlerimi sunarım.

Tez çalışmamın başından itibaren başta uygulama, araştırma ve makale olmak üzere her aşamasında mesleki deneyimlerini paylaşarak çalışmama katkıda bulunan Sayın hocam **Dr. Öğr. Üyesi Pelin CANBAY’a** saygı ve teşekkürlerimi sunarım.

Yüksek lisans eğitimi süresince bilgi, birikim ve desteklerini esirgemeyen ve bu alanda gelişmeye katkıda bulunan **KSÜ Bilgisayar Mühendisliği Bölümü ve Enformatik Ana Bilim Dalı hocalarıma** saygı ve teşekkürlerimi sunarım.

Yüksek lisans eğitimimin başından sonuna kadar manevi desteklerini her an hissettiğim ve her koşulda yanımda olan **eşime, aileme, çalışma arkadaşlarıma ve dostlarıma** sonsuz teşekkür ederim.

ABDULLAH İSMETOĞLU

İÇİNDEKİLER

Sayfa No

ÖZET	I
ABSTRACT	II
TEŞEKKÜR	III
SİMGELER VE KISALTMALAR DİZİNİ	VI
ŞEKİLLER DİZİNİ	VII
TABLOLAR DİZİNİ	IX
1. GİRİŞ	10
1.1. Covid-19 Hastalığı	11
1.2. Yapay Zekâ	11
1.3. Makine Öğrenmesi	12
1.4. Derin Öğrenme	13
1.4.1. CNN Mimarisi	14
1.4.2. DNN mimarisi	18
1.4.3. RNN Mimarisi	19
1.4.4. LSTM Mimarisi	21
1.5. Veri Mahremiyeti	24
1.5.1. Veri Mahremiyetinin Korunması	25
1.5.2. Mahremiyet Korumalı Veri Yayınlama	25
1.5.3. Mahremiyet Korumalı Veri Analizi	27
1.5.3.1. Diferansiyel Mahremiyet	28
1.5.3.2. Diferansiyel Mahremiyette Kullanılan Mekanizmalar	30
1.5.4. Derin Öğrenmede Diferansiyel Mahremiyet	32
1.5.4. Derin Öğrenme Modelleri Kullanılan Sistemlere Yapılan Saldırıları	33
1.5.4.1. Üyelik Çıkarım Saldırısı	34
1.5.4.2. Eğitim Verisine Saldırı	37
1.5.4.3. Model Çıkarma Saldırısı	37
1.5.5. Derin Öğrenme Modelleri Kullanılan Sistemlerde Diferansiyel Mahremiyet Mekanizmasının Uygulanması	38
2. ÖNCEKİ ÇALIŞMALAR	47
2.1. Diferansiyel Mahremiyet Mekanizmasını Kullanan Çalışmalar	47
2.2. Covid-19 Tespitinde Derin Öğrenme Tekniklerini Kullanan Çalışmalar	48
2.3. Covid-19 Tespitinde Veri Mahremiyetini Dikkate Alarak Derin Öğrenme Tekniklerini Kullanan Çalışmalar	51
2.4. Derin Öğrenme Mimarileri Kullanılarak Covid-19 Hastalık Teşhisi Yapılan Çalışmaların Karşılaştırılması	52
2.5. Açık Veri Setleri	54
3. MATERYAL VE METOT	56
3.1. Materyal	56

3.1.1. Kullanılan Verisetleri	56
3.2. Metot.....	57
3.2.1. Programlama	59
3.2.2. Uygulamada Kullanılan Hiper parametreler	59
4. BULGULAR VE TARTIŞMA	60
4.1. Geleneksel Sınıflandırma Sonuçları.....	60
4.2. Mahremiyet Duyarlı Sınıflandırma Sonuçları	65
5. SONUÇ VE ÖNERİLER.....	71
KAYNAKLAR.....	72
ÖZGEÇMİŞ.....	HATA! YER İŞARETİ TANIMLANMAMIŞ.



SİMGELER VE KISALTMALAR DİZİNİ

DP	: Differential Privacy – Diferansiyel Mahremiyet
CNN	: Convolutional Neural Network – Evrişimli Sinir Ağları
DNN	: Deep Neural Network – Derin Sinir Ağları
RNN	: Recurrent Neural Network – Tekrarlayan Sinir Ağları
LSTM	: Long Short Term Memory – Uzun Kısa Süreli Bellek
CT	: Computed Tomography – Bilgisayarlı Tomografi
CXR	: Chest X-Ray – Göğüs Röntgeni
PCR	: Polymerase Chain Reaction- Polimeraz Zincir Reaksiyonu
EKG	: Elektrokardiyografi
DSÖ	: Dünya Sağlık Örgütü
WHO	: World Health Organization
RNA	: Ribonükleik Asid
KVKK	: Kişisel Verileri Koruma Kurumu
SVM	: Support Vector Machine – Destek Vektör Makineleri
SGİY	: Stokastik Gradyan İniş Yöntemi
SMPC	: Güvenli Çok Partili Hesaplama
SGD	: Stochastic Gradient Descent

ŞEKİLLER DİZİNİ

Şekil 1.1 Covid-19 hastalığının teşhisi için çekilen dört farklı hastanın CXR görüntüleri .	10
Şekil 1.2 Yapay zekâ, makine öğrenmesi ve derin öğrenme arasındaki	13
Şekil 1.3 CNN mimari yapısı ve çalışma prensibi.....	14
Şekil 1.4 Evrişim işlemi örneği	16
Şekil 1.5 Ortaklama işlemi örneği	17
Şekil 1.6 Düzleme işlemi örneği.....	17
Şekil 1.7 Tam bağlantı katmanı	18
Şekil 1.8 Bir yapay sinir hücresi örneği	18
Şekil 1.9 DNN mimari yapısı örneği	19
Şekil 1.10 RNN mimarisi yapısının çalışma mantığı	20
Şekil 1.11 Örnek bir RNN mimarisi	21
Şekil 1.12 Tek katmanlı RNN'deki yinelenen modül yapısı.....	22
Şekil 1.13 Dört katmanlı LSTM'deki yinelenen modül yapısı	22
Şekil 1.14 Tek yönlü LSTM yapısı.....	23
Şekil 1.15 Çift yönlü LSTM yapısı.....	23
Şekil 1.16 Kapıları olan LSTM yapısı	23
Şekil 1.17 Veri toplama ve veri yayınlama süreci	26
Şekil 1.18 Diferansiyel mahremiyet süreci.....	29
Şekil 1.19 Diferansiyel mahremiyetin ilgili olduğu temel bileşenler	30
Şekil 1.20 Derin öğrenmede mahremiyet koruma planlarının sınıflandırılması	33
Şekil 1.21 Üyelik çıkarım saldırısının gösterimi	34
Şekil 1.22 Gölge modelinin şematik gösterimi.....	35
Şekil 1.23 Diferansiyel mahremiyet mekanizmasının olmadığı bir sisteme yapılan sızma girişimi.....	36
Şekil 1.24 Diferansiyel mahremiyet mekanizmasının olduğu bir sisteme yapılan sızma girişimi.....	36
Şekil 1.25 Eğitim verisine saldırı yöntemi kullanılarak elde edilen görüntü	37

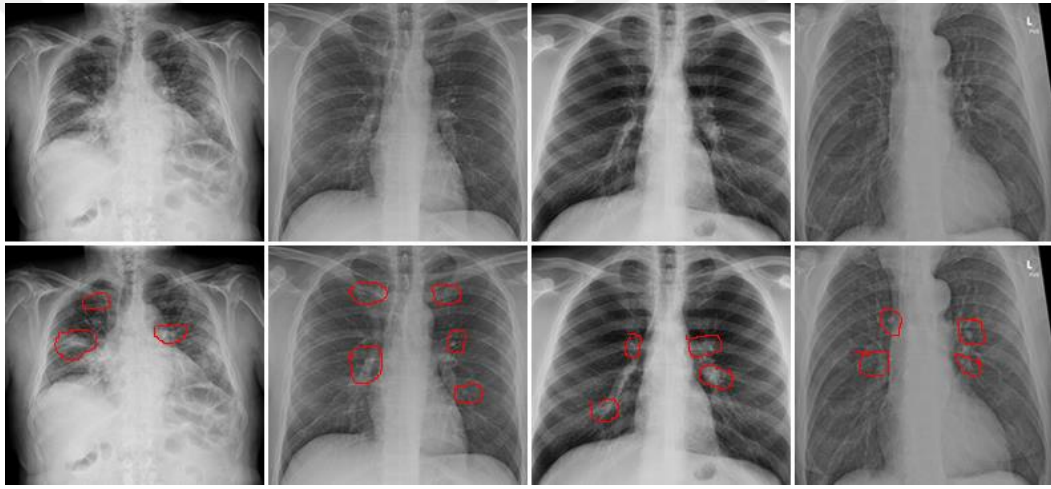
Şekil 1.26 Model çıkarma saldırısının gösterimi	38
Şekil 1.27 Derin öğrenme modelleri kullanılan sistemin farklı bölümlerine diferansiyel mahremiyet mekanizmasının uygulanması.....	39
Şekil 1.28 Gradyan hesabında kullanılan dış bükey düzlem	41
Şekil 1.29 SGD algoritmasıyla gradyanlara gürültü eklenerek diferansiyel mahremiyetin sürece dâhil edilmesi.....	44
Şekil 1.30 SGD optimizasyon algoritması ile diferansiyel mahremiyet sürecinin sisteme dahil edilmesine ait işlem adımları	44
Şekil 1.31 Gradyan bilgilerinin ele geçirilmesine yönelik yapılan saldırılar ve sonuçları ..	45
Şekil 3.1 Tez çalışması kapsamında yapılan işlemlere ait diyagram.....	58
Şekil 4.1 DS1 veri kümesi kullanılarak gerçekleştirilen hastalık teşhisinde elde edilen sonuçlara ait grafik	61
Şekil 4.2 DS2 veri kümesi kullanılarak gerçekleştirilen hastalık teşhis işleminde edilen test ve eğitim sonuçlara ait grafik	62
Şekil 4.3 DS3 veri kümesi kullanılarak gerçekleştirilen hastalık teşhisinde elde edilen sonuçlara ait grafik	63
Şekil 4.4 DS4 veri kümesi kullanılarak gerçekleştirilen hastalık teşhisinde elde edilen sonuçlara ait grafik	64
Şekil 4.5 DS5 veri kümesi kullanılarak gerçekleştirilen hastalık teşhisinde elde edilen sonuçlara ait grafik	65
Şekil 4.6 DS1 veri kümesi kullanılarak elde edilen sonuçlara ait grafik.....	66
Şekil 4.7 DS2 veri kümesi kullanılarak elde edilen sonuçlara ait grafik.....	67
Şekil 4.8 DS3 veri kümesi kullanılarak elde edilen sonuçlara ait grafik.....	68
Şekil 4.9 DS4 veri kümesi kullanılarak elde edilen sonuçlara ait grafik.....	69
Şekil 4.10 DS5 veri kümesi kullanılarak elde edilen sonuçlara ait grafik.....	70

TABLÖLAR DİZİNİ

Tablo 2.1 Derin öğrenme ile Covid-19 hastalığını tespit eden çalışmalar	53
Tablo 2.2 Literatürde Covid-19 hastalığının teşhisinde yaygın olarak kullanılan verisetleri	55
Tablo 3.1 Tez çalışmasında kullanılan verisetleri	56
Tablo 3.2 Çalışmada kullanılan verisetlerine ait görüntülerin özellikleri	56
Tablo 3.3 CNN mimari yapısına ait katmanlar	57
Tablo 3.4 Uygulamada kullanılan hiper parametreler	59
Tablo 4.1 DS1 veri kümesine ait sınıflandırma sonuçları	60
Tablo 4.2 DS2 veri kümesine ait sınıflandırma sonuçları	61
Tablo 4.3 DS3 veri kümesine ait sınıflandırma sonuçları	62
Tablo 4.4 DS4 veri kümesine ait sınıflandırma sonuçları	63
Tablo 4.5 DS5 veri kümesine ait sınıflandırma sonuçları	64
Tablo 4.6 DS1 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları	66
Tablo 4.7 DS2 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları	67
Tablo 4.8 DS3 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları	68
Tablo 4.9 DS4 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları	69
Tablo 4.10 DS5 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları	70

1. GİRİŞ

Covid-19 hastalığı solunum yoluyla insandan insana hızlı bir şekilde bulaştığı bilinen bir hastalıktır. (Long ve ark., 2020). Kalabalık ortamlarda hasta kişilerle aynı ortamlarda bulunulmasının yanı sıra öksürme, hapşıрма ve konuşma ile oluşabilecek damlacıkların iletimi hastalığın bulaş riskini arttırmaktadır (Abbasi-Oshaghi ve ark., 2020). Covid-19 hastalığının teşhisinde PCR testleri ve PCR testlerine ek olarak CT ve CXR görüntüleri de kullanılmaktadır. Şekil 1.1'de Covid-19 hastalığına yakalanan 4 kişinin çekilmiş CXR görüntüleri verilmektedir. İlgili görüntülerde kırmızı renk ile işaretlenen bölümler, Covid-19 virüsünün akciğerde neden olduğu hasarları göstermektedir (Long ve ark., 2020).



Şekil 1.1 Covid-19 hastalığının teşhisi için çekilen dört farklı hastanın CXR görüntüleri (Mooney, 2020)

Yapay zekâ ve derin öğrenme son zamanlarda pek çok alanda kullanılmakta olup özellikle tıp alanında sunduğu çözümlerle yüksek başarılı sonuçlar verdiği görülmektedir. Yapay zekâ, insan zekâsını bir makinede kopyalamaya veya simüle etmeye çalışan bir bilgisayar bilimi teknolojisidir. Yapay zekâ sayesinde makineler genellikle insanların yapabildiği öğrenme, akıl yürütme, karar verme ve problem çözme gibi tamamen zekâ gerektiren görevleri gerçekleştirebilmektedir (Alafi, 2019).

Derin öğrenme, makine öğreniminin bir alt dalıdır ve beynin sinirsel aktivitelerini oluşturulan yapay sinir ağları aracılığıyla taklit eder. Derin öğrenme algoritmaları, görüntü işleme başta olmak üzere ses, görüntü, metin vb. verilerin işlenip anlamlandırılmasında sıklıkla kullanılmaktadır (Yapıcı ve Topaloğlu, 2021). Derin öğrenme ayrıca karmaşık ve zor problemlere çözüm bulma yeteneğine sahiptir. Sağlık alanında çalışanlar ve

araştırmacılar derin öğrenme algoritmalarını kullanarak CT, CXR, EKG vb. görüntüler üzerinde sınıflandırma, nesne ve lezyon tespiti gibi görevleri başarıyla gerçekleştirmektedir (Aslan, 2019).

Covid-19 hastalığının teşhisinde üst solunum yolu örnekleri alınarak yapılan PCR tabanlı testlerin maliyetinin yüksek olması ve bu testlerin sonuçlarının 6-9 saat arasında alınabilmesi sebebiyle alternatif bir hastalık tanı sistemine ihtiyaç duyulmaktadır (Minaee ve ark., 2020). Bu çalışmada Covid-19 hastalığının teşhisinde veri mahremiyetini de dikkate alan bir yapay zekâ sistemi geliştirilmiştir. Literatürde sıklıkla kullanılan 5 veri kümesi ile yapılan testlerde en yüksek %97 başarı elde edildiği görülmüştür. Gözlemlenen sonuçlar dikkate alındığında mahremiyet duyarlı yapay zekâ sistemi ile Covid-19 hastalığının kabul edilebilir seviyelerde tespit edilebildiği görülmüştür.

1.1. Covid-19 Hastalığı

Covid-19 hastalığı, yedinci insan koranavirüsü olarak şiddetli akut solunum yolu enfeksiyonu koranavirüs-2 (SARS-Cov-2) adıyla 2020 yılı ocak ayındaki son zatürre salgını sırasında, ilk olarak Çin'in Hubei eyaleti Wuhan kentinde keşfedilmiştir (Ciotti ve ark., 2020).

DSÖ Acil Durum Komitesi tarafından uluslararası lokasyonlardan artan vaka bildirim oranlarına dayanarak Covid-19 hastalığı, salgın hastalık olarak ilan edilmiştir. Covid-19 virüsü, hayvanlara ve insanlara bulaşabilen pozitif tek sarmallı büyük RNA virüsleridir (Velavan ve Meyer, 2020). Dünyada toplam vaka sayısı 617 milyona ulaşmış, ülkemizde ise bu sayı 17 milyonu geçmiş olup bu rakamlar halen hızlı bir şekilde artmaya da devam etmektedir. Covid-19 hastalığına bağlı olarak vefat edenlerin sayısı dünyada 6,5 milyona ulaşmış olup ülkemizde 100 bin rakamını geçmiştir (WHO, 2021).

1.2. Yapay Zekâ

Yapay Zekâ kelimesi ilk olarak 1956 yılında Dortmund konferansında John McCarty tarafından kullanılmıştır. Tıp, mühendislik ve endüstri alanları başta olmak üzere bilişim teknolojilerinde artan verilerin büyüklüklerinin hesaplanması, depolanması gibi ihtiyaçlar için tasarlanmış gelişmiş algoritmalar sayesinde oldukça popüler hale gelmiştir (Alpaydın, 2013). Günümüzde yapay zekâdan; sağlık, bankacılık, moda, eğitim vb. birçok sektör ciddi anlamda yararlanmaktadır. Yapay zekâ'nın temel amacı makinelerle insan zekâsı kazandırmaktır. Başka bir deyişle yapay zekâ, makineleri akıllı hale getirmeye ve

insanlar gibi davranmanın yanı sıra düşünmeye odaklanarak zeki insan davranışını taklit etmeye çalışır. Yani bilgi temelleri yoluyla insan biliş kabiliyetini simüle etmeye çalışır (Elmas ve Babayev, 2021). Bu makineler; analiz, teşhis ve problem çözme konularında insanlardan daha iyi ve hızlı düşünceleri için eğitilmektedir. Yapay zekânın en popüler ve en iyi örneği kendi kendine hareket eden arabalar ve robotlardır (Alafi, 2019).

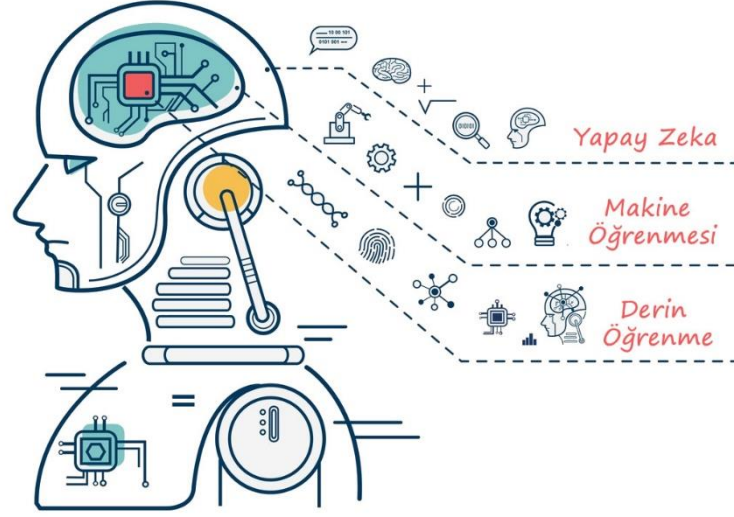
Yapay zekânın amacı doğadaki canlı varlıkların zekâ ile gerçekleştirdikleri davranışlarını yapay olarak üreterek bir kuram oluşturmaktır (Charniak ve McDermott, 1985). Ayrıca insan zekâsıyla yapılabilecek işlerin makineler tarafından yapılmasını sağlamaktır. Bu amaçların gerçekleştirilebilmesi için öncelikle insan düşünce yapısının anlaşılması gerekir. Yapay zekâ, insanoğlunun hayatını kolaylaştırmak için kullanılmaktadır. İnsanın birçok davranışı zekâ belirtisi olarak kabul edilmektedir (Alkan, 2019). Bunun sebebi insanın düşünen bir varlık olması ve dolayısıyla eylemleri düşünme ve bunun sonucunda karar vermesiyle gerçekleştirmesidir.

1.3. Makine Öğrenmesi

Makine öğrenmesi, yalnızca deneyimlere dayalı tahminler yapmaya odaklanan yapay zekânın bir alt dalıdır. Makinenin belirli bir görevi yerine getirmek için açık bir program yerine bilgi ve verilere dayalı olarak karar vermesine olanak tanır. Makine öğrenmesi, derin öğrenme ve ilgili kurallar gibi teknikler aracılığıyla yapay zekâ sistemlerini destekler ve onları istatistiksel tekniklerle eğitir (Alafi, 2019). Algoritmalar, zaman içinde öğrenmek ve geliştirmek ve kullanıcının daha iyi bir seçim yapmasına yardımcı olmak için özel olarak tasarlanmıştır. Özellikle veriler ile ilgili olarak verilerin toplanması, filtrelenebilmesi, analiz edilmesi, algoritmaların eğitilmesi ve test edilmesi ile algoritmalar kullanılarak gelecek durumlarla ilgili tahminlerde bulunulması makine öğrenimi ile gerçekleştirilir. Bu metodolojilerin uygulanmasına örnek olarak görüntü tanıma verilebilir. Görüntü tanımayla ilgili literatürde birçok araştırma ve çalışma mevcuttur. Çalışmalar genellikle verilen görüntüye belirli filtreler uygulayarak görüntüde bulunan nesneler; insan, araç, mekân, hayvan vb. şekilde sınıflandırılarak tespiti üzerinedir. Örneğin Daş ve arkadaşları çalışmalarında (Daş ve ark., 2019) sabit ve hareketli görüntülere belirli filtreler uygulayarak görüntülerde bulunan insan, çocuk, araç, saat vb. nesneleri tanıma işlemi gerçekleştirmişlerdir.

Derin Öğrenme, makine öğrenimi tekniklerinden biridir. Derin öğrenme, yapay zekâ ve makine öğrenmesi arasındaki ilişkiye bakıldığında makine öğrenmesinin derin

öğrenmeyi kapsadığı, yapay zekânın da makine öğrenmesini kapsadığı görülmektedir (Alafi, 2019). Şekil 1.2’de yapay zekâ, makine öğrenmesi ve derin öğrenme arasındaki ilişki gösterilmektedir.



Şekil 1.2 Yapay zekâ, makine öğrenmesi ve derin öğrenme arasındaki (Şimşek, 2019)

1.4. Derin Öğrenme

Derin öğrenme, temeli yapay sinir ağı olan makine öğrenmesi tekniklerinden birisidir. Son yıllarda yapay zekânın yeniden şekillenmesine neden olmuştur (Ravî ve ark., 2016). Derin öğrenmenin ana ilham kaynağı, devam eden bilgi, gözlem, deneyim ve geçici keşiften etkilenen sinirbilimdir (Rusk, 2016). Derin öğrenme, karmaşık nöron katmanlarını kullanarak üst düzey veri soyutlamalarını modellemeye çalışır. Verilerin büyüklüklerinin hızlı bir şekilde artması ve buna bağlı olarak hesaplamanın zorlaşması problemi, karmaşık yapılara sahip sinir ağları sayesinde başarılı bir şekilde çözülebildiği için yoğun ilgi görmüş ve çeşitli alanlarda kullanılmıştır (Hao ve ark., 2016). Derin yapay sinir ağları gibi derin öğrenme yöntemleri, çok büyük veri kümelerindeki kalıpları ve yapıyı keşfetmek için birden çok işlem katmanı kullanır. Her katman, sonraki katmanların üzerine inşa ettiği verilerden bir kavram öğrenir. Katmanların seviyesi ne kadar yüksekse, öğrenilen kavramlar o kadar soyut olur (Rusk, 2016).

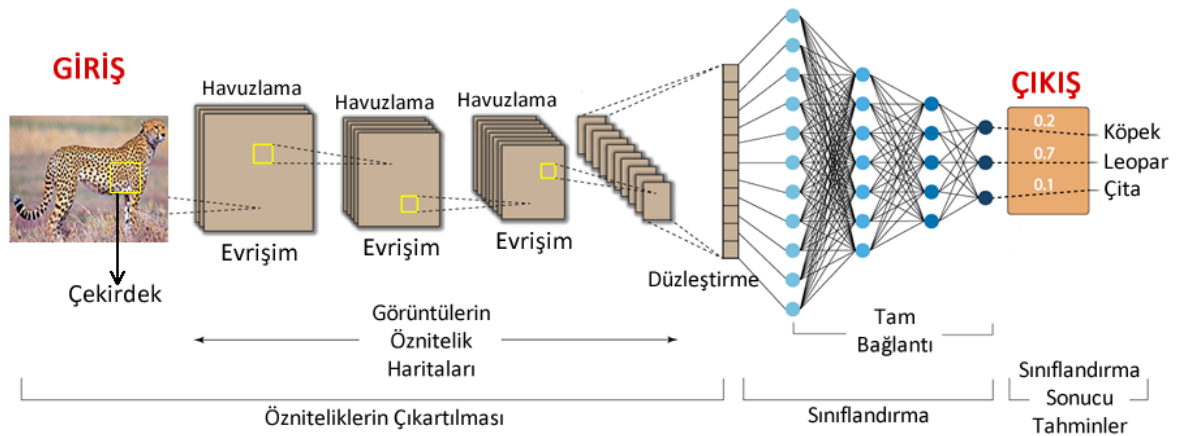
Derin öğrenme algoritmaları, sağlık alanında analitik veriye dayalı modellerin oluşturulmasına olan ilgiyi de artırmıştır. Temeli yapay sinir ağlarına dayanan bir teknik olan derin öğrenme, son yıllarda yapay zekânın geleceğini yeniden şekillendiren güçlü bir makine öğrenimi tekniği olarak karşımıza çıkmaktadır (Ravî ve ark., 2016). Derin

öğrenme, çok büyük hacimli verilerden üst düzey bilgileri çıkardığı için büyük veri bağlamında çok değerlidir.

Derin öğrenme, Evrişimli Sinir Ağları (Convolutional Neural Network-CNN), Tekrarlayan Sinir Ağları (Recurrent Neural Network-RNN), Derin Sinir Ağları (Deep Neural Network-DNN) ve Uzun Kısa Süreli Bellek (Long Short Term Memory-LSTM) olmak üzere 4 temel mimariden oluşmaktadır. Bu mimariler alt bölümlerde açıklanmıştır.

1.4.1. CNN Mimarisi

Yapay zekâ temelli görüntü işlemede sıklıkla kullanılan CNN ilk olarak Kunihiko Fukushima tarafından 1980 yılında tanıtılmış, kullanımı ise ilk olarak Yann LeCun ve arkadaşları tarafından gerçekleştirilmiştir (Lecun ve ark., 1998). CNN mimarisinden önce görüntü işleme ve sınıflandırma işlemlerinde geleneksel yapay sinir ağları kullanılmaktaydı. Bu ağların kapasiteleri genellikle sınırlı olduğu için veriler büyüdükçe geleneksel ağlar yeterli olmayıp yeni bir ağa ihtiyaç duyulmuştur ve CNN mimarisi bu ihtiyacı karşılamak için ortaya çıkmıştır. CNN mimarisinin en önemli özelliği katmanlı bir yapıya sahip olmasıdır (Yıldız ve ark., 2021). Bu mimaride algoritma, insan nöronlarının yapısına benzer şekilde modellenmiştir. CNN mimarisi çoğu durumda geleneksel mimarilerden daha iyi sonuçlar vermektedir (Luo ve ark., 2020). Ancak bu mimarinin en büyük dezavantajı düşük çözünürlüklü görüntülerde performansın önemli ölçüde düşmesidir (Aghdam ve ark., 2019). Şekil 1.3'te CNN mimari yapısı ve çalışma prensibi verilmiştir.



Şekil 1.3 CNN mimari yapısı ve çalışma prensibi (Swapna, 2021)

CNN mimarisi filtreler üzerinde çalışır. Mimari yapıdaki ilk filtreler görüntüdeki kenarları öğrenir, sonraki filtreler görüntünün karmaşık şekillerini öğrenir ve son filtreler

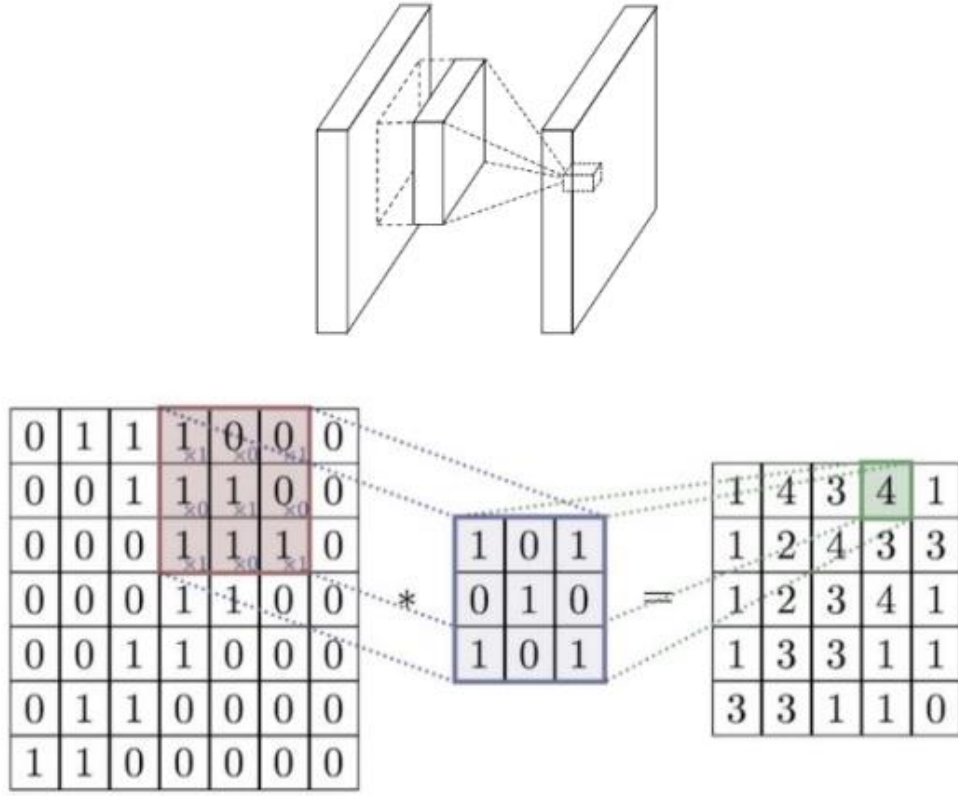
ise renkleri ve karmaşık yapıları çıkarır. CNN mimarisinde giriş görüntüsü üzerinde filtre işlemi uygulanarak matris şeklinde çıkış verisi oluşturulur. Ardından öznitelik haritası elde edilir. Öznitelik haritası modelin karmaşıklığını azaltmak için girdi olarak verilen görüntülerin özniteliklerinin çıkarıldığı haritalardır. Ayrıca bu haritalar ağı eğitimi de kolaylaştırmaktadır. Kullanılan filtrelere ait değerlerin görüntüye uygulanması sonucunda yeni oluşan katsayı değerleri her işlem adımında yinelenir (Tan, 2019).

Evrişim katmanı, girdi olarak verilen görüntü üzerinde filtreler uygulayarak girdinin öznitelik haritalarına dönüştürülmesini sağlar. Havuzlama katmanı, filtre uygulandıktan sonra ağı artmış olan parametre sayısı ile boyutunu azaltmaktadır. Bu azaltma aynı zamanda hesaplama yükünün azaltılmasını ve ezberlemenin minimuma inmesini sağlamaktadır (Pervan ve Keleş, 2019). Düzleştirme katmanında, havuzlama katmanında elde edilen öznitelik haritalarına düzleme işlemi uygulanarak bir vektöre dönüştürülür. Tam bağlantı katmanında ise gelen veriler belirli değerlere göre ağırlandırılarak birleştirilmektedir. Kayıp fonksiyonu kullanılarak eğitim süresince ağırlık değerleri elde edilmektedir. Sınıflandırma yapılabilmesi için son katman olan tam bağlantı katmanında softmax, sigmoid vb. aktivasyon fonksiyonlarının çıktıları kullanılarak olasılık değerleri hesaplanmaktadır. CNN mimarisinin görüntü verileri üzerindeki başarısından dolayı tıbbi görüntülerin sınıflandırmasında yoğun olarak tercih edilmektedir (Eker ve Nevcihan, 2021).

Bu çalışmada CNN mimarisinin tercih edilmesinin ana nedeni, görüntü verilerinde yüksek başarı vermesinden dolayı CXR ve CT görüntülerinden Covid-19 hastalığının teşhisini yüksek başarıyla elde edebilmektir. CNN mimarisinde tüm işlemler katmanlarda gerçekleşir. Her katmanın kendine özgü görevleri vardır.

1.4.1.1. Evrişim Katmanı

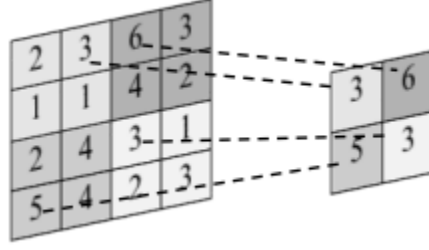
Evrişim katmanı, girdi olarak verilen görüntü üzerinde filtreler uygulayarak girdinin öznitelik haritalarına dönüştürülmesini sağlar. Başka bir ifadeyle verinin önemli özniteliklerinin daha belirginleştiği farklı bir veriye dönüştürülmesi veya evrilmesi sağlanır. Bunu sağlamak için de filtreler girdi verisinin üzerinde gezdirilerek eşleşen anlamlı kısımlardan yeni öznitelik haritaları oluşturulur (O'Shea ve Nash, 2015). Şekil 1.4'te girdi olarak alınan 7x7'lik bir görüntü matrisine 3x3'lük bir filtre uygulanarak elde edilen öznitelik haritası görülmektedir. Girdi olarak verilen görüntü matrisine farklı filtrelerin uygulanması sonucunda birçok farklı öznitelik haritaları elde edilebilmektedir.



Şekil 1.4 Evrişim işlemi örneği (Doğan ve Türkoğlu, 2019)

1.4.1.2. Ortaklama Katmanı

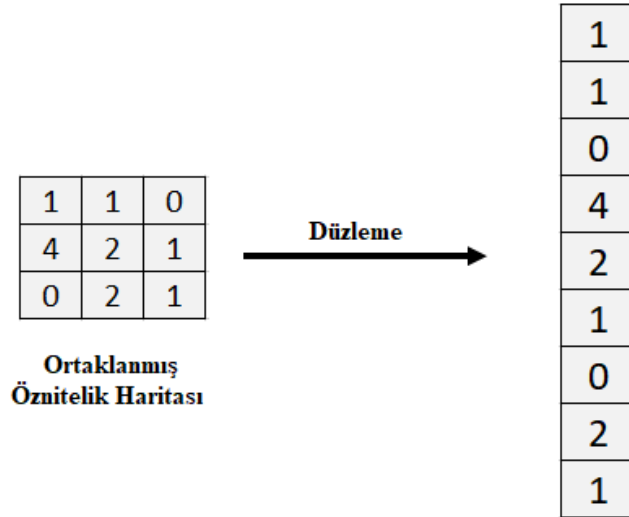
Ortaklama katmanı, verideki boyutsallığı kademeli olarak azaltmayı ve böylece modelin parametre sayısını ve hesaplama karmaşıklığını azaltmayı amaçlamaktadır. Ortaklama, evrişim katmanı sonrası elde edilen öznitelik haritalarındaki örüntüleri ve bu örüntülerin bağlantısını ortaya çıkarmak için kullanılır. Ortaklama işleminde öncelikle bir çerçeve belirlenir. Belirlenen bu çerçeve evrişim katmanı sonucu elde edilen öznitelik haritalarının üzerinde gezerek ortaklama işlemini gerçekleştirir ve her öznitelik haritası için bir ortaklanmış öznitelik haritası üretir (O'Shea ve Nash, 2015). Ortaklama işlemlerinde çıktının boyutunu düşürmek için maksimum değer alma veya ortalama gibi bazı fonksiyonlar kullanılmaktadır. Bu fonksiyonlar ile belirli bir alan içindeki değerler hesaplanarak yeni değer üretilir (Kurt, 2018). Şekil 1.5'te girdi olarak alınan 4x4'lük görüntü matrisine 2x2'lik bir çerçeve ile maksimum ortaklama işlemi yapılması sonucu elde edilen ortaklanmış öznitelik haritası örnek olarak gösterilmiştir.



Şekil 1.5 Ortaklama işlemi örneği (Doğan ve Türkoğlu, 2019)

1.4.1.3. Düzleme Katmanı

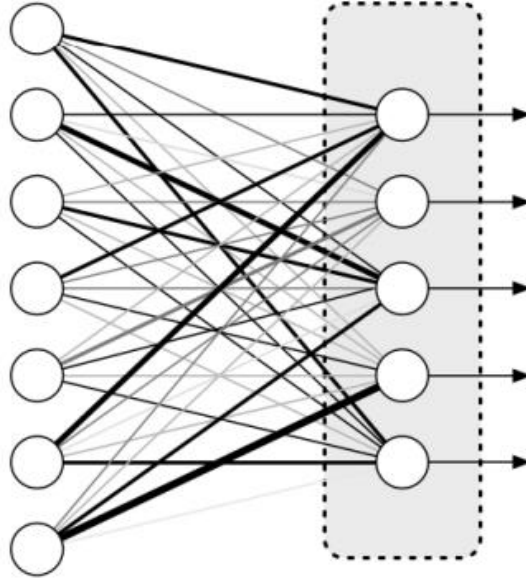
Ortaklama katmanında elde edilen ortaklanmış öznitelik haritalarına düzleme işlemi uygulanarak bir vektöre dönüştürülür. Bu işlem yapılırken verilerin sırası korunur. Bu işlemin temel amacı veriyi sinir ağları ile işlemeye hazır hale getirmektir. Özetle, tam bağlantı aşaması için verilerin hazırlandığı aşamadır (Tan, 2019). Şekil 1.6'da girdi olarak alınan 3x3'lük ortaklanmış öznitelik haritasının düzleme sonrası yapısı görülmektedir.



Şekil 1.6 Düzleme işlemi örneği (Canbay, 2020)

1.4.1.4. Tam Bağlantı Katmanı

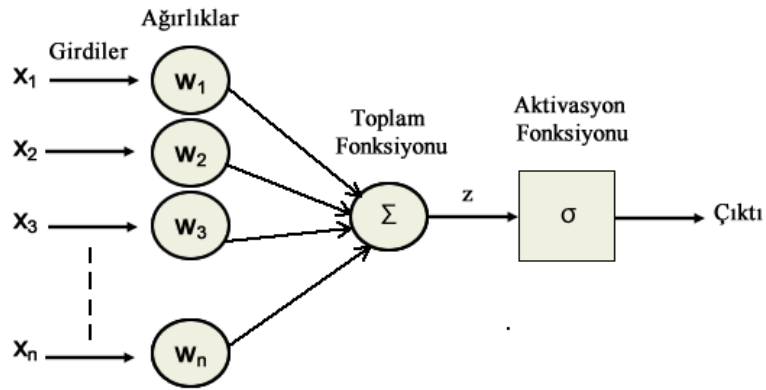
CNN mimarisinin en son katmanı olan tam bağlantı katmanında evrişim ve ortaklama işlemleri sonucunda elde edilen değerler girdi olarak alınmaktadır. Bu değerlerle aktivasyon fonksiyonları kullanarak olasılık değerleri hesaplanmakta ve bu değerlere göre sınıflandırma yapılmaktadır. Bu katman çalışma prensibi olarak yapay sinir ağına benzetilmektedir. (Kurt, 2018). Şekil 1.7'de tam bağlantı katmanı için bir örnek gösterilmektedir.



Şekil 1.7 Tam bağlantı katmanı (Doğan ve Türkoğlu, 2019)

1.4.2. DNN mimarisi

DNN, insanın beyin yapısının ve fonksiyonlarının makinelerce öğrenilmesi ve taklit yoluyla işlemlerin gerçekleştirilebilmeleri için geliştirilmiş işlem birimlerinden oluşan mimaridir (Canbay, 2020). Bir DNN mimarisi, girdi ve çıktılar arasında birden fazla gizli birim katmanlarına sahip, ileri beslemeli yapay bir sinir ağıdır (Hinton ve ark., 2012). Şekil 1.8’de tek sinir hücreli ve tek katmanlı olan sinir ağı örneği verilmiştir.

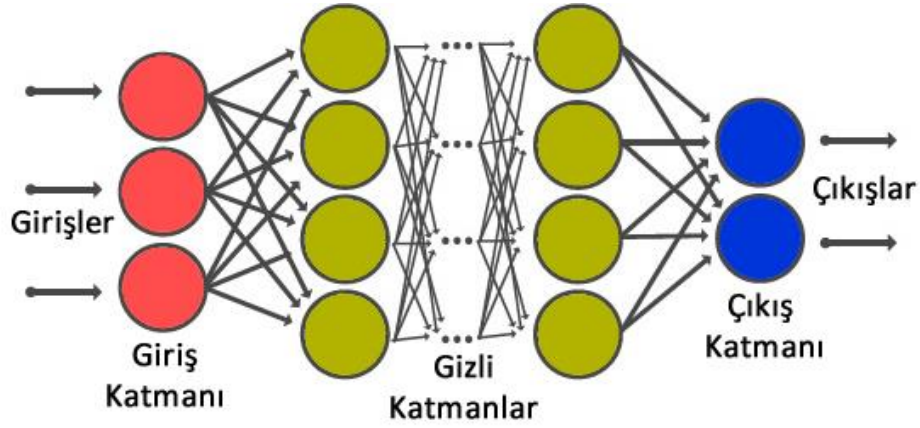


Şekil 1.8 Bir yapay sinir hücresi örneği (Canbay, 2020)

Çok sayıda gizli katmana ve katman başına çok sayıda birime sahip DNN'ler, çok sayıda parametreye sahip çok esnek modellerdir. Bu esneklik onlara girdiler ve çıktılar arasındaki çok karmaşık ve oldukça doğrusal olmayan ilişkileri modelleme yeteneği sağlar. Bu yetenek, yüksek kalitede modelleme için önemlidir. Ancak, bu durum aynı zamanda

eğitim setindeki belirli örneklerin tesadüfi olarak alınması sebebiyle fazla tahminlemeye yol açabilen gereksiz verilerin de modellemelerine sebep olabilmektedir.

Çok büyük eğitim setleri, modelleme gücünü korurken, eğitimi hesaplama açısından çok büyük değerler elde edeceğinden çalışmanın performansını azaltabilir (Ciresan ve ark., 2010). Şekil 1.9’da DNN mimari yapısı örneği verilmiştir.



Şekil 1.9 DNN mimari yapısı örneği (Mathworks, 2022)

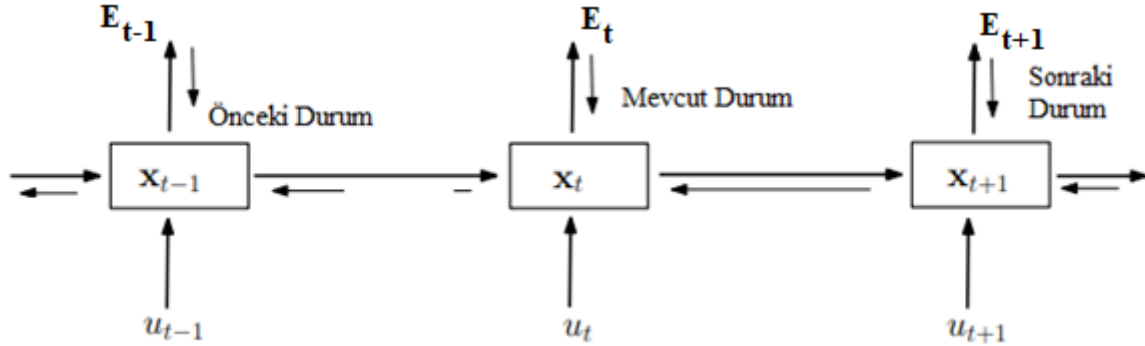
DNN mimari yapısında, birbirine bağlı nöronlar katmanlar halinde bulunmaktadır. Bu mimari yapı, gizli katman, giriş katmanı ve çıkış katmanı olmak üzere üç katmandan oluşmaktadır. DNN mimari yapısının Derin Sinir Ağı olarak adlandırılmasının nedeni birden fazla gizli katmana sahip olmasıdır. (Kimanuka ve Büyük, 2018). DNN mimarisindeki gizli katmanlarda bulunan nöronların sayısı, sınıflandırmada önemli bir yere sahiptir. DNN mimarisinin diğer mimarilerden ayrılmasının sebebi, bu mimaride çok katman olması ve bu katmanlarda çok sayıda nöron bulunmasıdır (Aydoğan ve Karci, 2020).

1.4.3. RNN Mimarisi

RNN mimarisi, düğümler arasındaki bağlantıların bir döngü oluşturabildiği ve bazı düğümlerden gelen çıktıların, diğer düğümlerde girdi olarak kullanılmasına imkân verildiği yapay sinir ağı sınıfıdır (Graves, 2013). RNN mimarisinin temelinde sıralı bilgilerin kullanılması vardır (Şeker ve ark., 2017). Bu mimaride önceki giriş bilgileri, mevcut giriş bilgileri ile beraber değerlendirilir. Yani RNN mimarisinde sistem, önceki bilgiler ile yeni öğrenmiş olduğu bilgileri birlikte ele alır. Örneğin; bir konum uygulamasında t-1 anındaki konum, t anındaki konum ile t anındaki konum ise t+1 anındaki konum ile bağlantılıdır.

İstenilen anda mevcut konum bilgisi gerekirse, bir önceki konuma göre belirlenir (Canbay, 2020). Bu mimarinin tekrarlayan olarak ifade edilmesinin sebebi bir dizinin her ögesi için değerin önceki çıktılara bağlı olmasıdır (Şeker ve ark., 2017).

Şekil 1.10'da RNN mimarisinin çalışma mantığı gösterilmiştir. E_t , çıktıdan t anında ortaya çıkan hatayı, U_t ağıın girdi değerini, X_t ise ağıın t anındaki gizli durumunu ifade etmektedir.

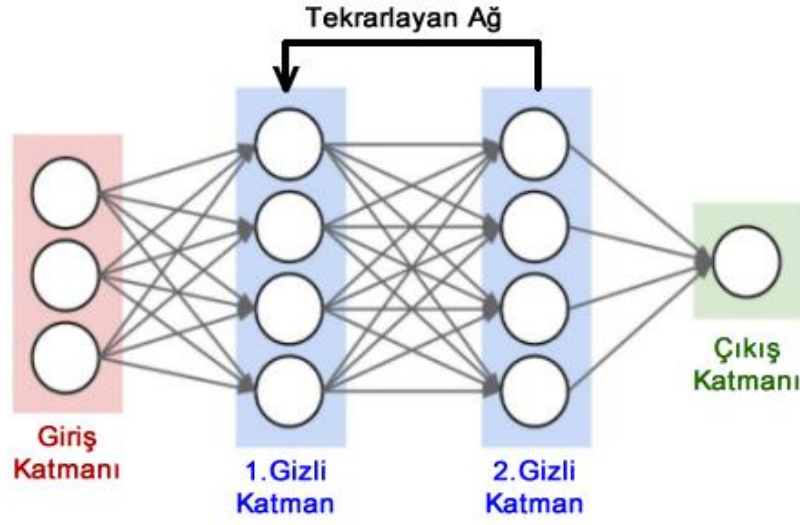


Şekil 1.10 RNN mimarisi yapısının çalışma mantığı (Pascanu ve ark., 2013)

RNN mimari yapısında, bir zaman gecikmesi ile ilişkili olarak gizli katmanlar arasındaki bağlantılara izin verilmesi durumunda model, geçmişle ilgili bilgileri saklayabilir ve verilerin zamansal olarak birbirinden çok uzakta olan olaylar arasındaki bağlantıları keşfetmesini sağlar. Prensipde RNN basit ve güçlü bir model olsa da pratikte doğru şekilde eğitilmesi zordur (Pascanu ve ark., 2013). RNN mimari yapısında girişten alınan veriler katmanlardan geçirilerek bir çıkış elde edilir. Bu çıkış değeri doğru değer ile karşılaştırılır. Karşılaştırılan bu değerler arasında farka ait hata ölçümü yapılır. Bu ölçüme göre katman üzerindeki ölçülen değerler değiştirilir. Bu şekilde işlemler en doğru sonuca ulaşılan kadar devam eder ve çıktı verebilen bir model oluşturulmuş olur. RNN mimari yapısında, girdi verileri işleme alınırken bu yapıda bulunan hafızalar kullanılmaktadır (Metin ve Karasulu, 2015). Şekil 1.11'de örnek bir RNN modeli verilmiştir.

RNN mimari yapısı, giriş, çıkış ve iki gizli katman olmak üzere dört katmandan oluşur. Bu katmanlar işlev yönünden birbirlerinden bağımsız olarak çalışmaktadır. (Britz, 2015). RNN mimarisinin temelini oluşturan tekrarlı aşamalar sonucunda bir önceki girişin değeri saklanır. Bu saklanan değer ile yeni elde edilen giriş değeri birleştirilir. Bu sayede yeni elde edilen giriş değerinin bir önceki giriş değeri ile olan ilişkisi sağlanmış olur. RNN mimarisi, doğal dil işleme, metin tanıma, ses tanıma gibi önceki girdi değerlerinin

kullanıldığı çeşitli işlemler için faydalı olduğu için kullanılmaktadır (Canbay ve ark., 2021).



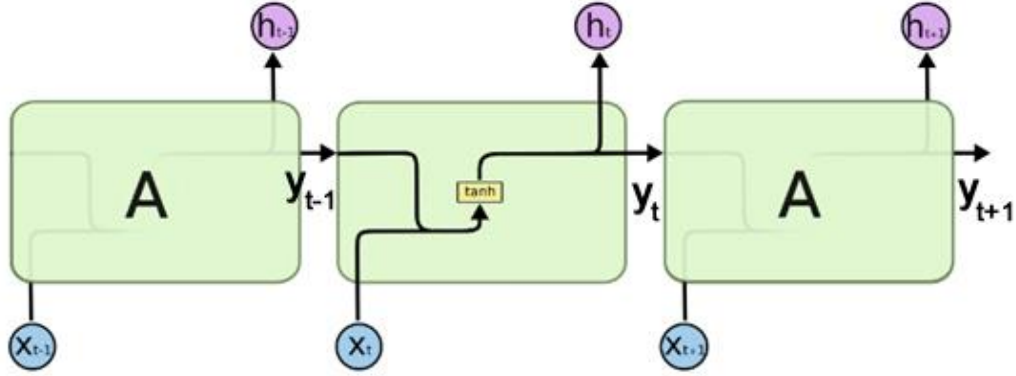
Şekil 1.11 Örnek bir RNN mimarisi (Gurari, 2021)

1.4.4. LSTM Mimarisi

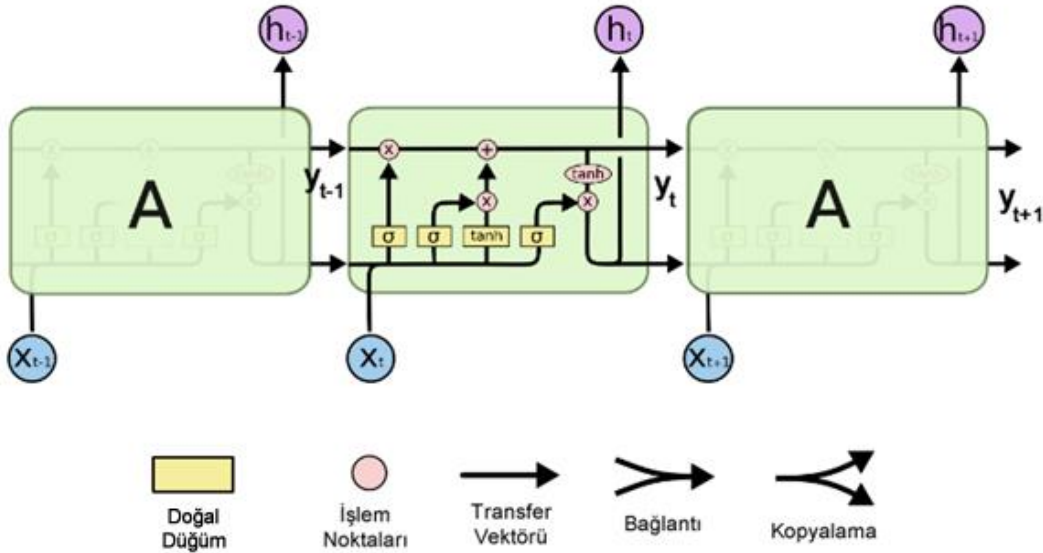
Sıralı verilerin modellenmesi için ilk olarak Hochreiter ve Schmidhuber tarafından tanıtılan LSTM, RNN mimarisinin farklı bir türüdür. Klasik RNN mimari yapısında öğrenmenin önceki zaman dilimlerindeki bilgilerin girdi olarak kullanılmasıyla gerçekleştiği kabul edilmektedir (Kara, 2019). Ancak bu klasik yapıda gradyan kaybolması sorunu vardır (Karim ve ark., 2019). Bu sorunun çözümü için Hochreiter ve Schmidhuber çalışmalarında (Hochreiter ve Schmidhuber, 1997) LSTM mimarisini önermişlerdir. LSTM mimari yapısında bilgi akışını kontrol edebilmek için RNN katmanlarına bir kapı mekanizması eklenir. Bu sayede RNN'lerin kısa süreli bellek sorunu ortadan kaldırılmaktadır (Yurtsever, 2021). LSTM ayrıca bilgilerin daha iyi depolanması için tasarlanmıştır (Gunduz, 2021). LSTM mimarisinde, uzun zaman önce girdi olarak gelen herhangi bir bilgiyi hatırlamak için özel katmanlar bulunmaktadır (Latifoğlu ve Nuralan, 2020).

LSTM modelinin yapısı bir zincirin yapısına benzemektedir. Standart RNN mimari yapısında bir $\tanh$ sinir ağı katmanı bulunmaktadır. Fakat tekrar eden modülün ise farklı bir yapısı vardır. Bu yapıda tek bir $\tanh$ sinir ağı yerine, benzersiz bir iletişim özelliklerine sahip dört $\tanh$ sinir ağı katmanına sahiptir. Standart bir LSTM ağı, hücre olarak adlandırılan bellek bloklarından meydana gelir. Hücrelerin mevcut durumları bir sonraki hücreye aktarılarak işlemler yapılır. Şekil 1.12'de tek katmanı bulunan RNN'deki

yenilenen modül yapısı, Şekil 1.13'te ise dört katmanlı bulunan LSTM'deki yenilenen modül yapısı verilmiştir. Şekildeki x ile girdi katmanını, y ile çıktı katmanını ve h ile gösterilenler ise gizli katmanları ifade etmektedir.

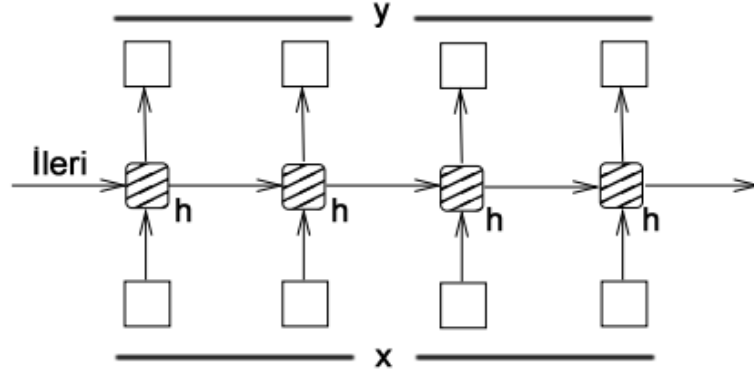


Şekil 1.12 Tek katmanlı RNN'deki yenilenen modül yapısı (Olah, 2015)

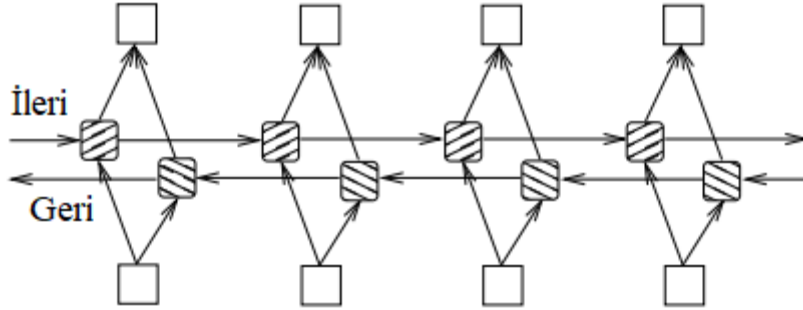


Şekil 1.13 Dört katmanlı LSTM'deki yenilenen modül yapısı (Olah, 2015)

Standart RNN'ler, metin, ses ve video gibi sıralı verilerle ilgili araştırma alanlarında yaygın olarak kullanılmaktadır. Ancak RNN'ler girdi ile çıktı arasında uzun zaman olduğu durumlarda girdi verilerinin ilgili bilgilerini öğrenmede yetersiz kalmaktadır. Bunun için çift yönlü bir LSTM ağı kullanılması gerekmektedir. Bu durum LSTM'nin derin öğrenmede odak noktası haline gelmesini sağlamıştır (Yu ve ark., 2019). Şekil 1.14'te tek yönlü, Şekil 1.15'te ise çift yönlü LSTM yapısı verilmiştir. Şekilde verilen kutucuklardan, x ile gösterilen kutucuklar girdi katmanını, y ile gösterilenler çıktı katmanını, h ile gösterilenler ise gizli katmanları ifade etmektedir.

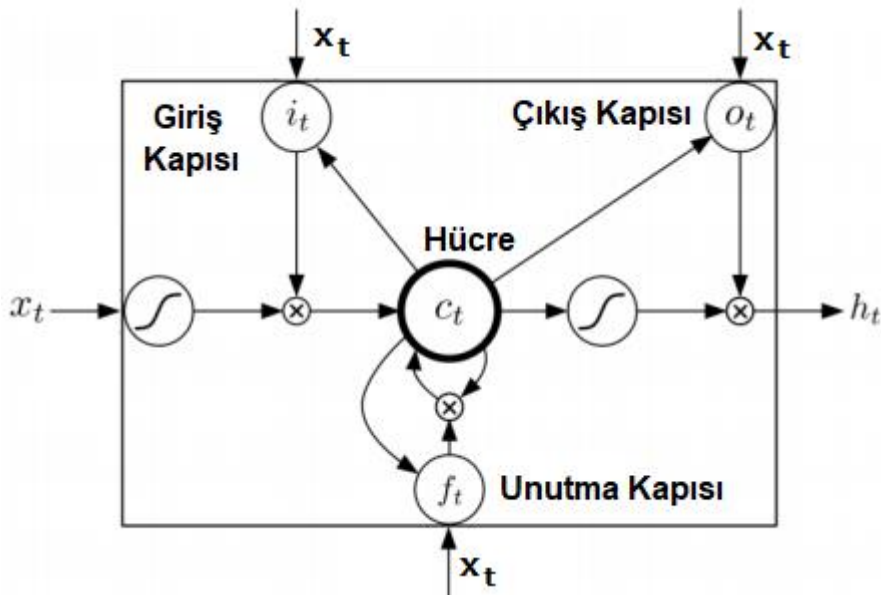


Şekil 1.14 Tek yönlü LSTM yapısı (Huang ve ark., 2015)



Şekil 1.15 Çift yönlü LSTM yapısı (Huang ve ark., 2015)

Şekil 1.16’da ise kapıları olan bir LSTM’nin genel yapısı verilmiştir. Burada X_t veriyi, i_t giriş kapısını, o_t çıkış kapısını, f_t unutma kapısını, h_t gizli vektör ve c_t hücre aktivasyon vektörünü ifade etmektedir.



Şekil 1.16 Kapıları olan LSTM yapısı (Huang ve ark., 2015)

1.5. Veri Mahremiyeti

Mahremiyet kavramı ilk olarak 1890 yılında Amerikalı yargıç Brandeis tarafından kullanılmış olup “Mahremiyet Hakkı” adlı makalesi ile literatüre girmiştir (Warren ve Brandeis, 1890). Günümüzde ise mahremiyet konusu kanunlarla korunan bireylerin temel hak ve özgürlüğüdür (Canbay, 2019). Mahremiyet, bir bireyin kendisi hakkındaki her bir olgu üzerinde dışarıdan bir müdahaleye izin vermeksizin karar ve kontrol yetkisine sahip olmasıdır. Veri mahremiyeti ise kişinin verilerinin mahremiyet seviyesi ile bu verinin kişiye faydası arasındaki dengeyi korumaya çalışan ve verinin paylaşım veya yayınlanması konusundaki sınırlarının verinin sahibine ait olmasıdır (Canbay, 2019). Başka bir deyişle bireylerin kendilerine ait bilgilerinin hangi ortamda nasıl elde edildiği, ne kadarının ne zaman paylaşılacağı veya kullanılacağı üzerinde karar ve kontrol sahibi olmasıdır (Jain ve ark., 2016).

Günümüzde, yasal düzenlemeler tek başına kişisel veri mahremiyetini korumakta yetersiz kalmaktadır. Örneğin; e-ticaret platformlarına gün geçtikçe artan ilgi nedeniyle web siteleri üzerinden alışveriş yaygınlaşmış ve bunun sonucunda e-ticaret hacmi, toplam ticaret hacminin önemli bir kısmını oluşturmuştur. Bu durum kullanıcılara ait kişisel verilerin üçüncü şahıslar tarafından genellikle kullanıcıların bilgisi ve kontrolü olmaksızın önbellege alınmasına, kopyalanmasına ve arşivlenmesine neden olmaktadır. Yasal düzenlemeler belirli seviyelerde koruma sağlasa da teknik yönden pek çok yapıya ihtiyaç gün geçtikçe artmaktadır (Geambasu ve ark., 2009).

Bilgi ve iletişim teknolojilerinin hızlı bir şekilde gelişmesi ve güçlenmesi sonucunda bireylerin mahremiyetlerinin korunması ciddi bir şekilde önem arz etmektedir (Tataroğlu, 2013). Ülkemizde her türlü kişisel verilerin işlenmesinde, bireylerin temel hak ve özgürlüklerinin korunması, kişisel verileri işleyen tarafların sorumlulukları ile uyacakları usul ve esaslar, “Kişisel Verilerin Korunması Kanunu” kapsamındadır (KVKK, 2020). Kanunda kişisel veri, “kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi” olarak ifade edilmektedir. Kişinin kimlik numarası, pasaport numarası, sosyal güvenlik numarası, telefon numarası, özgeçmiş, parmak izleri, ses kayıtları, görüntüleri, resim ve genetik bilgileri gibi veriler kişiyi belirlenebilir yapması sebebiyle kişisel veri olarak kabul edilmektedir. Bu verilerin dışında kişiye ait sosyal medya hesabı, mail adresi, web sitesi vb. verilerin kişiyi sanal ortamda belirlenebilir yapacağından bu verilerde kişisel veri olarak tanımlanabilmektedir (KVKK, 2021).

1.5.1. Veri Mahremiyetinin Korunması

Verinin elde edilmesi süreci, aktif veri üretimi ve pasif veri üretimi olarak sınıflandırılabilir. Aktif veri üretimi, veri sahibinin verileri üçüncü bir taraf ile paylaşmaya istekli olduğu anlamına gelirken pasif veri üretimi ise verilerin sahibinin çevrimiçi etkinliği sebebiyle istekli olup olmadığına bakılmaksızın elde edilmesidir (Mehmood ve ark., 2016). Bu bağlamda veri sahibi için en büyük tehlike, verilerinin isteği ve izni dışında üçüncü şahıslar tarafından kullanılmasıdır.

Veri sahibi, kişisel ve hassas bilgilerini mümkün olduğunca gizlemek ister ve bu bilgiler üzerinde ne kadar kontrol sahibi olabileceği konusunda endişelenir. Bu endişelerin ortadan kalkması için erişimi kısıtlar veya veriler üzerinde değişiklik yaparak verilerin üretimi sırasında mahremiyet ihlali riskini en aza indirebilir (Mehmood ve ark., 2016). Ancak bu yöntemler günümüzde yetersiz kalmaktadır.

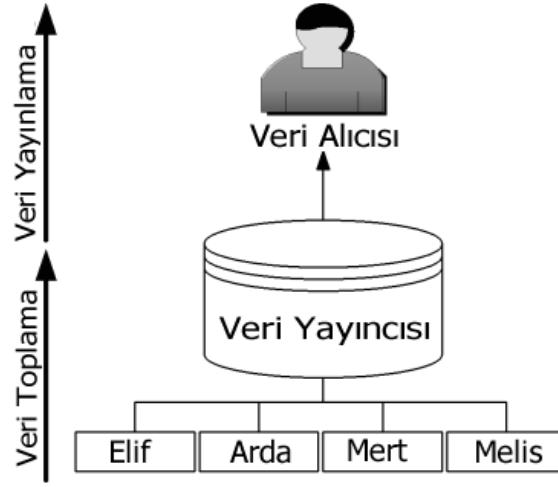
Verilerin elde edilmesi ile yaşam döngüsünün farklı aşamalarında (veri oluşturma, veri depolama ve veri işleme gibi) mahremiyetin korunması için geliştirilmiş bazı mahremiyet koruyucu modeller vardır (Mehmood ve ark., 2016). Literatürde yaygın olarak kullanılan modeller: *k*-Anonimlik, *l*-Çeşitlilik ve *t*-Yakınlıktır (Canbay ve ark., 2020).

1.5.2. Mahremiyet Korumalı Veri Yayınlama

Veri yayınlama, veriden fayda elde etmek isteyen araştırmacılara verilerin çeşitli platformlar aracılığıyla paylaşılmasıdır. Mahremiyet korumalı veri yayınlama ise kişisel verilerin yayınlanmadan önce mahremiyeti koruyucu önlemler alarak veri sahibinin gerçek kimliğinin açığa çıkmasının engellenmesidir. Mahremiyet korumalı veri yayınlama sürecinde tarafların hangi verilerin paylaşılacağı, hangi verilerin toplanacağı, verilerin nerede ve nasıl depolanacağı gibi önemli tüm gereksinimlerinin karşılanması gerekmektedir (Canbay ve ark., 2020).

Veri toplayıcıları tarafından dijital bilgilerin toplanması, bilgiye dayalı karar verme için muazzam fırsatlar sunmaktadır. Karşılıklı anlaşmalar veya belirli verilerin yayınlanmasını gerektiren düzenlemeler nedeniyle, taraflar arasında verilerin karşılıklı transferine ve yayınlanmasına yönelik bir talep vardır. Veri yayıncılığındaki mevcut uygulama, esas olarak ne tür verilerin yayınlanabileceğine ilişkin politikalara, yönergelere ve yayınlanan verilerin kullanımına ilişkin yasal düzenleme ve anlaşmalara dayanmaktadır. Bu yaklaşım tek başına verinin zarar görmesine veya yetersiz korumaya yol açabilir.

Mahremiyet koruyucu mekanizmalar, veri mahremiyetini korurken faydalı bilgilerin yayınlanması için yöntemler ve araçlar sağlar (Fung ve ark., 2010).



Şekil 1.17 Veri toplama ve veri yayınlama süreci (Fung ve ark., 2010)

Verinin toplama ve yayınlanması süreci Şekil 1.17’de verilmiştir. Veri toplama aşamasında, veri yayıncısı kayıt sahiplerinden (örneğin, Elif ve Arda) verileri toplar. Veri yayınlama aşamasında veri yayıncısı, toplanan verileri bir veri madencisine paylaşır veya bu platform üzerinden araştırmacılara açık yayınlar. Örneğin, bir hastane hastalardan veri toplar ve hasta kayıtlarını harici bir tıp merkezine gönderebilir. Bu örnekte hastane veri yayıncısıdır. Hastalar kayıt sahipleridir ve tıp merkezi ise veri alıcısıdır (Fung ve ark., 2010).

Veri yayınlama sürecinde mahremiyetin korunması için yaygın olarak kullanılan yöntem verilerin anonimleştirilmesidir. Verileri anonimleştirme, verinin biçiminin ve tipinin korunarak mahremiyet koruyucu işlemlerin veriye uygulanmasıdır. Veri anonimleştirme ilk olarak Chaum tarafından önerilmiştir (Chaum, 1981). Verilerin anonimleştirilmesi sürecinde, mahremiyeti korumak için kullanıcıyı tanımlayan tüm kişisel bilgiler kaldırılarak veriler anonimleştirilir. Sadece anonimleştirilmiş verilerden bir bireyi tanımlamanın mümkün olmayacağı varsayılır. Ancak, büyük hacimli verilerin ve güçlü veri analizi araçlarının mevcudiyeti nedeniyle, mevcut anonimleştirme teknikleri giderek etkisiz hale gelmektedir. Büyük verilerin olduğu alanlarda anonimleştirmenin, belirli alanları maskeleyemekten veya genelleştirmekten daha fazlasını yapması gerekmektedir. Anonimleştirilmiş verilerin herhangi bir saldırıya açık olup olmadığı dikkatlice analiz edilmelidir. Bunun için özellikle büyük verilerle ilgili farklı mahremiyet koruyucu

önlemlere ihtiyaç vardır. (Mehmood ve ark., 2016). Bu çerçevede veri yayınlamada kullanılan literatürdeki mahremiyet koruma modellerinden bazıları şunlardır:

k-Anonimlik Modeli: Veri sahibinin mahremiyetini korumayı amaçlayan k-anonimlik modeli, ilk defa Sweeney tarafından önerilmiştir (Sweeney, 2002). Sweeney, her kaydın yarı tanımlayıcıya göre en az k-1 diğer kayıtla ayırt edilemez özelliği olması gerektiği belirtmiştir. Başka bir deyişle, k-anonimlik, her eşdeğerlik sınıfının birbirine benzer en az k kayıt içermesini gerektirmektedir. k-anonimliğinin sağladığı koruma basit ve anlaşılması kolaydır. Bireyin kimliğinin ifşasına karşı koruma sağlamaktadır.

l-Çeşitlilik Modeli: k-anonimlik kimlik ifşasına karşı koruma sağlarken, öznitelik ifşasını önlemek için yetersiz kalmaktadır. Bu problemi çözmek adına Machanavajhala ve arkadaşları çalışmalarında her eşlenik sınıfındaki hassas bir niteliğin dağılımının en az l kadar “iyi temsil edilen” değere sahip olmasını gerektiren, l-çeşitlilik adı verilen yeni bir mahremiyet modelini ortaya koymuşlardır (Machanavajhala ve ark., 2007).

t-Yakınlık Modeli: k-anonimlik, öznitelik ifşasını önlemede yetersiz kaldığı, l-çeşitlilik modelinin ise çarpık veri dağılımı saldırısına karşı yeterli korumayı sağlayamamasından dolayı, Li ve arkadaşları çalışmalarında (Li ve ark., 2007) t-yakınlık modelini önermişlerdir. Bu modelde, oransal ve sayısal olarak eş olan herhangi bir sınıftaki öznitelik dağılımının, genel tablodaki öznitelik dağılımına yakın olması gerekmektedir. Başka bir deyişle iki dağılım arasındaki mesafe t eşiğinden fazla olmamalıdır (Rebollo-Monedero ve ark., 2010).

1.5.3. Mahremiyet Korumalı Veri Analizi

Teknolojinin hızla gelişmesi ve buna bağlı internet platformlarının ve teknolojik aletlerin yoğun bir şekilde kullanılması sonucunda dijital bilgilerin toplanması ve toplanan verilerin analiz edilmesi gün geçtikçe daha fazla önem kazanmakla birlikte çeşitli sorunları da beraberinde getirebilmektedir. Orijinal halde bulunan veriler, genellikle bireyler hakkında hassas bilgiler içerir ve bu tür verilerin analizi sırasında mahremiyet koruyucu önlemler alınmaması durumunda bireyin mahremiyeti ihlal edilebilir. Mahremiyet koruyucu yaklaşımlar tek başına yeterli gelmediğinden doğru mahremiyet koruyucu mekanizmanın kullanılmaması durumunda bu durum verinin zarar görmesine veya yetersiz korumaya yol açabilir. Doğru mahremiyet koruyucu mekanizmayı kullanmak veri mahremiyetini korurken aynı zamanda verinin de bozulmasını engeller. (Fung ve ark., 2010).

Verilerin analiz edilmesi sürecinde kullanılan mahremiyet koruma modellerinin (k -Anonimlik, l -Çeşitlilik, t -Yakınlık vb.) arka plan saldırılarına karşı yetersiz kalması sebebiyle güçlü bir mahremiyet koruyucu mekanizmaya ihtiyaç duyulmuştur. Diferansiyel mahremiyet bu korumayı sağlayarak mahremiyet garantisi sunar.

1.5.3.1. Diferansiyel Mahremiyet

Diferansiyel mahremiyet, Dwork tarafından önerilen ve günümüzde sıklıkla kullanılan, matematiksel gürültü ekleme işlemine dayanarak olası saldırılara karşı koruma sağlamayı amaçlayan, sağlam ve güvenilir bir mahremiyet koruma yöntemidir (Dwork, 2006). Diferansiyel mahremiyet, istatistiksel veritabanları üzerinden mahremiyeti koruyan gürültülü sorgu yanıtları sağlamak için güçlü bir araçtır. Gürültülü sorgu yanıtlarının dağılımının herhangi bir tanımlama grubunun eklenmesi veya silinmesiyle çok az değişmesini garanti eder. Veriler hakkında herhangi bir varsayımda bulunmadan mahremiyeti sağladığı ve bir kayıt dışında geriye kalan tüm kayıtları bilen saldırganlara karşı bile koruma sağladığı belirtilmektedir (Kifer ve Machanavajjhala, 2011).

Diferansiyel Mahremiyet, sorguların bir veri kümesine verdiği yanıtla hareket eder. Böylece anonimleştirme işlemi orijinal veri kümesini değiştirmeyecektir. Bunun yerine, diferansiyel mahremiyet mekanizması gürültülü yanıtları dönderir ve saldırganın cevaptan herhangi bir bilgi çıkarmasını engeller. Yayımlanan bilgilere göre bir kişinin veri kümesinde olup olmadığının ayırt edilemezliğini zorunlu kılarak güçlü mahremiyet garantisi sağlar. Diferansiyel mahremiyetin temelindeki fikir, veritabanında herhangi bir bireysel verinin varlığının veya yokluğunun, yayımlanan nihai istatistiksel bilgiyi önemli ölçüde etkilememesi gerektiğidir ve bu nedenle, bazı yardımcı bilgilere sahip saldırganlara karşı güçlü mahremiyet garantisi verir. (Geng ve Viswanath, 2014). Aşağıda diferansiyel mahremiyet için ilgili tanımlar verilmiştir.

ϵ -Diferansiyel Mahremiyet; K mekanizması, her S çıktısı için, komşu olan herhangi D_1 ve D_2 veri kümeleri için Denklem 1.1'de verilen şartı sağlaması durumunda, mekanizmanın ϵ -diferansiyel mahremiyeti sağladığı kabul edilmektedir (Dwork, 2006).

$$\Pr[K[(D_1) \in S] \leq e^\epsilon \times \Pr[K[(D_2) \in S] \quad (1.1)$$

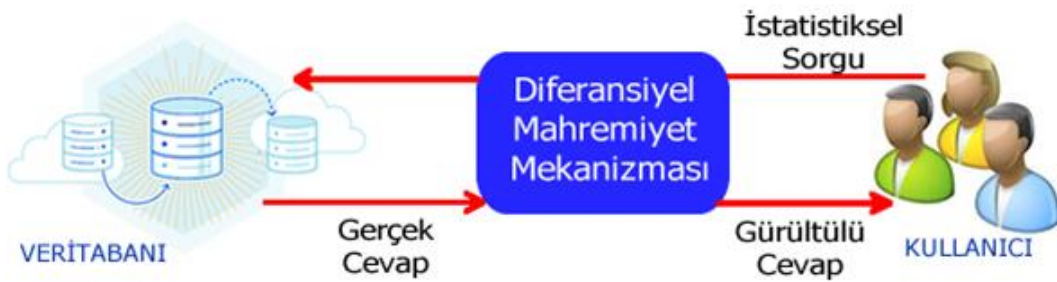
(ϵ, δ) – Diferansiyel Mahremiyet; K mekanizması, her S çıktısı için, komşu olan herhangi D_1 ve D_2 veri kümeleri için Denklem 1.2'de verilen şartı sağlaması durumunda,

mekanizmanın (ϵ, δ) – diferansiyel mahremiyeti sağladığı kabul edilmektedir. ϵ ile δ mahremiyetin seviyesini kontrol eden iki parametredir. En basit haliyle ifade etmek gerekirse, ϵ gürültülü sorgu yanıtlarının dağılımının herhangi bir tanımlama grubunun eklenmesi veya silinmesiyle oluşabilecek etkinin üst sınırıdır, δ ise bu sınırın tutmama olasılığıdır. δ , mahremiyeti tam olarak sağlanmış bir sistemde ihlal olma olasılığını sınırladığından, δ 'nın 0'a yaklaşarak çok küçük olması gerekmektedir (Steinke ve Ullman, 2015). Denklemlerde, K diferansiyel mahremiyet mekanizmasını, S çıktıyı, D_1 ve D_2 , veritabanındaki komşu veri kümelerini, ϵ mahremiyet bütçesini, δ deltayı, Pr ise olasılığı ifade etmektedir.

$$Pr[K[(D_1) \in S] \leq e^\epsilon x Pr[K[(D_2) \in S] + \delta \quad (1.2)$$

Verilen formüllerden anlaşılacağı üzere, ϵ -Diferansiyel Mahremiyet, diferansiyel mahremiyetin temeli olarak ifade edilirken, (ϵ, δ) -Diferansiyel Mahremiyet ise $\delta > 0$ değeri için yaklaşık diferansiyel mahremiyet olarak ifade edilmektedir (Beimel ve ark., 2013).

Şekil 1.18'de diferansiyel mahremiyet süreci gösterilmiştir. Diferansiyel mahremiyet sürecinde ilk olarak, kullanıcı veri tabanına sorgu göndererek bilgi talep eder. Veri tabanı gerçek cevabı diferansiyel mahremiyet mekanizmasına gönderir. Diferansiyel mahremiyet mekanizması da cevaba gürültü eklemesi ile yeni oluşan gürültülü cevabı kullanıcıya gönderir. Bu şekilde kullanıcının gerçek cevaba erişmesi engellenmiş olur. Bu işlem için diferansiyel mahremiyet süreci tamamlanmış olur (Canbay ve Sağiroğlu, 2020).



Şekil 1.18 Diferansiyel mahremiyet süreci (Canbay ve Sağiroğlu, 2020)

Diferansiyel mahremiyetin ilgili olduğu temel bileşenler Şekil 1.19'da verilmiştir. Farklı mahremiyet yaklaşımları ile ilgili ilk araştırmalar 2003 yılında yapılmıştır. Ancak Dwork ve arkadaşlarının 2006 yılında yayınlamış oldukları çalışmadan sonra dünya

çapındaki bilim adamları tarafından önemli çalışma grupları oluşturularak bu alanda araştırmalar yapılmaya başlanmıştır (Dwork ve ark., 2006).



Şekil 1.19 Diferansiyel mahremiyetin ilgili olduğu temel bileşenler (Zhu ve ark., 2017)

Diferansiyel mahremiyet son zamanlarda mahremiyeti korumada güçlü ve gelecek için umut verici bir mahremiyet modeli olarak kabul edilmiştir. Diferansiyel mahremiyetin en yaygın çalışma alanları makine öğrenimi, derin öğrenme, veri madenciliği, istatistik ve öğretim teknolojileridir (Zhu ve ark., 2017).

1.5.3.2. Diferansiyel Mahremiyette Kullanılan Mekanizmalar

Derin öğrenme modelleri kullanılan sistemdeki eğitim verilerinin mahremiyetini sızıntılara karşı korumanın yolu, öğrenme algoritmasının oluşturduğu eğitim parametrelerine gürültü eklemektir. Bununla birlikte, bu yaklaşımı kullanırken çok fazla gürültü eklemek, öğrenme algoritmasının performansını düşürecektir (Zhu ve ark., 2017). Bu bağlamda, literatürde, eğitim süreci sırasında eğitim verilerinin mahremiyetini sağlamak amacıyla bazı mekanizmalar kullanılmaktadır. Bunlar; Laplace Mekanizması, Gauss Mekanizması ve Eksponansiyel Mekanizma olup bunlar aşağıda açıklanmıştır.

1.5.3.2.1. Laplace Mekanizması

Laplace mekanizması, sorgu sonucunu kullanıcıya geri göndermeden önce sorguya Laplace gürültüsünün eklenmesi mantığına dayanır (Zhu ve ark., 2017). D veri kümesi için f sorgusunu yanıtlayan mekanizma Denklem 1.3'teki gibi oluşturulur.

$$M(D) = f(D) + \text{lap}(0, \Delta f / \varepsilon) \quad (1.3)$$

Denklem 3'te verilen f sorgu fonksiyonunu, $\text{lap}(0, \Delta f / \varepsilon)$ laplace dağılımını, D verikümesini, Δf ise maksimumum sorgu değerini yani hassasiyeti ifade etmektedir.

1.5.3.2.2. Gauss Mekanizması

Diferansiyel mahremiyetin sağlanması için kullanılan diğer bir mekanizma Gauss mekanizmasıdır. Komşu veritabanlarında gerçekleştirilen f sorgu fonksiyonu için sorgunun hassasiyeti Denklem 1.4'te verilmiştir (Sun ve ark., 2019).

$$\Delta f^2 = \max_{D_1, D_2} \| f(D_1) - f(D_2) \|_2 \quad (1.4)$$

N normal dağılım olmak üzere Gauss mekanizması Denklem 1.5'te verilmiştir. Denklemde bulunan M mekanizmayı, x sorgudaki herhangi bir veriyi, σ ise gauss gürültüsünün standart sapmasını ifade etmektedir.

$$M(D) = f(D) + N(0, \Delta f^2 x \sigma^2) \quad (1.5)$$

Tez çalışmasında DP-SGD algoritmasında diferansiyel mahremiyeti sağlamak için Gauss mekanizmasından faydalanılmıştır.

1.5.3.2.3. Eksponansiyel Mekanizma

Sayısal olmayan sorgularda diferansiyel mahremiyeti sağlamak için üstel bir fonksiyon kullanılan mekanizmadır (Zhu ve ark., 2017). Skor fonksiyonu $q(D, \phi)$, D veri kümesi için elde edilen $\phi \in \Phi$ çıktısını değerlendirmek için kullanılır. Δ_q , q fonksiyonunun hassasiyeti varsayıldığında D veri kümesi için Denklem 1.6'da ε -diferansiyel mahremiyet sağlanmış olur.

$$M(D) = \{\emptyset \text{ olasılıkla geri dön} \propto \exp\left(\frac{\varepsilon q(D, \emptyset)}{2\Delta_q}\right) \quad (1.6)$$

Sayısal özniteliklerden farklı olarak kategorize edilmiş özniteliklerin kullanıldığı yapılarda değerlerinin bir tahminine izin vermez. Bu nedenle, kategorize edilmiş öznitelikler üzerinden sorguları yanıtlamak için Laplace mekanizmasını uygulamak iyi bir strateji değildir. Bu yapılarda eksponansiyel mekanizma kullanmak daha uygundur. Yanıta

rastgele gürültü ekleyen Laplace mekanizmasının aksine eksponansiyel mekanizma, sorgu için olası yanıtlar kümesinden rastgele bir yanıt seçmeye çalışır (Filho ve ark., 2021).

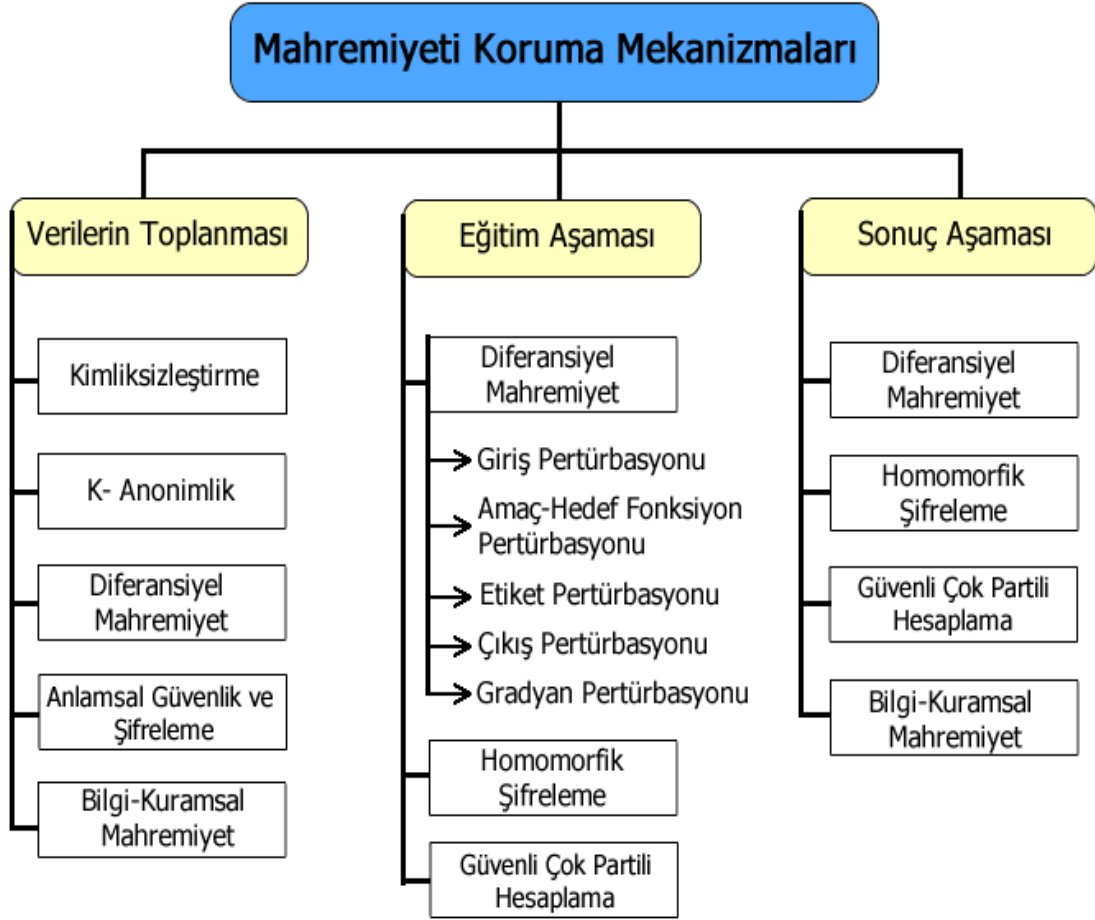
1.5.4. Derin Öğrenmede Diferansiyel Mahremiyet

Derin öğrenme, tıp, finans, enerji gibi birçok alanda başarılı bir şekilde kullanılmaktadır. Yapılan araştırma çalışmalarında kullanılan eğitim veri kümesi ile ilgili parametreleri ve veri ile ilgili diğer bilgileri öğrenmede başarılı sonuçlar elde edilmektedir. Bu parametreler ve ayrıntılı bilgiler kullanılırken bu bilgilerin mahremiyetinin ifşa edilmesi riski ortaya çıkmaktadır (Parmaar, 2020).

Derin öğrenme modelleri kullanılan sistemlerde, tarafların ortak çıkarları doğrultusunda eğitim veri kümeleri ve eğitim parametrelerinin mahremiyetinin korunması önemli bir konudur. Mahremiyetin korunması diferansiyel mahremiyet sayesinde sağlanabilmektedir. Derin öğrenmede diferansiyel mahremiyeti koruma hedefleri, öncelikle eğitim veri kümeleri ile eğitim parametrelerinin korunmasını içermektedir. Derin öğrenme modellerinde mahremiyeti sağlamak için mahremiyet koruma mekanizmaları Şekil 1.24'te gösterildiği gibi verilerin işlenmesi sürecinde üç aşamada uygulanır. Bu aşamalardan en güvenli olanı mahremiyet koruma mekanizmalarının eğitim aşamasına uygulanmasıdır. Bu uygulamada genelde iki yöntem kullanılır. Bunlar, mevcut bir algoritmanın yürütme sürecine gürültü eklemek ve verilen optimizasyon probleminin amaç fonksiyonlarını değiştirmektir (Zhu ve ark., 2017). Bu iki yöntemin dışında veriye gürültü eklemek ve çıktıya gürültü ekleme yöntemleri de yoğun olmamakla beraber kullanılmaktadır.

Derin öğrenme mimarileri kullanılan modellerde en büyük mahremiyet riski modelin eğitim aşamasında, eğitim parametrelerinin ele geçirilme ihtimalidir. Diferansiyel mahremiyet mekanizması kullanılarak eğitim aşamasında kullanılan kişilere özgü bilgiler dışarıdan gelebilecek saldırılara karşı korunabilmektedir. Diferansiyel mahremiyet ile verilere doğrudan erişim engellenerek mahremiyeti korumaya yönelik çalışmalar literatürde yaygın bir şekilde bulunmaktadır. Bu çalışmalara önceki çalışmalar bölümünde yer verilmiştir.

Literatürdeki genel kabul görmüş çalışmalara bakıldığında homomorfik şifreleme, SGİY, SMPC, DSGİ vb. yöntemlerin tek başına kullanılmadığı bu yöntemlerle birlikte diferansiyel mahremiyet mekanizmasının kullanıldığı görülmüştür. Bunun sebebi diğer yöntemlerin mahremiyeti korumada tek başlarına yeterli olmamasıdır.



Şekil 1.20 Derin öğrenmede mahremiyet koruma planlarının sınıflandırılması (Mireshghallah ve ark., 2020)

Şekil 1.20’de derin öğrenmede mahremiyeti sağlamak için koruma planlarının sınıflandırılmasına ait şema verilmiştir. Birinci kısımda verilerin toplanması aşamasındaki mahremiyet koruma yöntemlerini içermektedir. İkinci kısımda eğitim veri kümesinde bulunan kişiler hakkında hassas bilgilerin açığa çıkmaması için özel mekanizmalar verilmiştir. Son kısımda ise derin öğrenme sürecinin sonuç aşamasında kullanılabilecek mahremiyet koruyucu mekanizmalar verilmiştir.

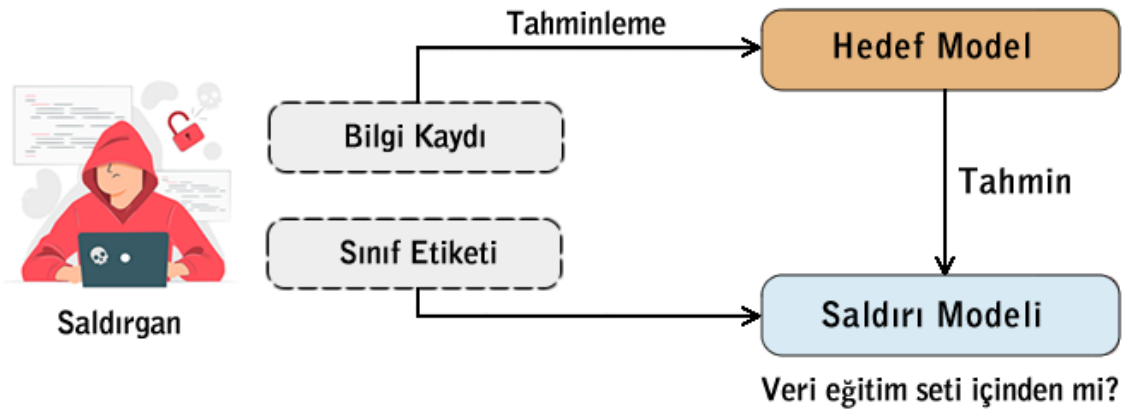
1.5.4. Derin Öğrenme Modelleri Kullanılan Sistemlere Yapılan Saldırıları

Derin öğrenme modelleri kullanılarak tasarlanan sistemlerde, mahrem bilgileri elde etmek için çeşitli saldırılar düzenlenmektedir. Bunlardan en yaygın olarak gerçekleşenler, üyelik çıkarım saldırısı, eğitim verisine saldırı ve model çıkarma saldırısıdır.

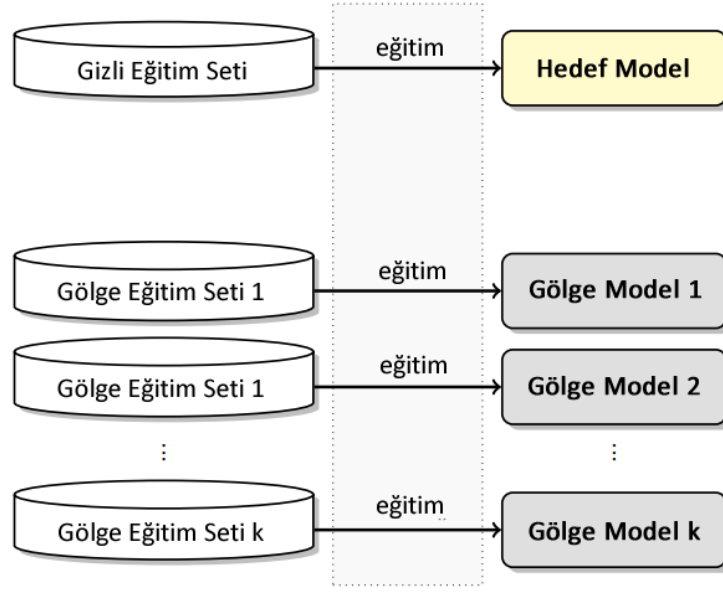
1.5.4.1. Üyelik Çıkarım Saldırısı

Üyelik çıkarım saldırısı ilk olarak Goodfellow ve arkadaşları tarafından önerilmiştir (Goodfellow ve ark., 2014). Saldırgan, bilgilerin bir makine öğrenme modeli veya eğitim veri kümesinde bulunup bulunmadığını öğrenmeye çalışır (Zhao ve ark., 2019). Saldırgan, bir veri kaydı ile hedef modeli sorgular ve modelin tahmini bilgilerini o kayıt üzerinden elde eder. Elde edilen bilgi, kaydın hangi sınıfa ait olduğunu belirten sınıf bazlı bir olasılık vektörüdür. Bu tahmin vektörü, hedef kaydın etiketiyle birlikte bu kaydın hedef modelin eğitim veri kümesinde mi yoksa dışında mı olduğu sonucuna varan saldırı modeline iletilir (Shokri ve ark., 2017). Bu şekilde verinin eğitim seti içinde olup olmadığı belirlenir.

Üyelik çıkarım saldırısı için bir örnek gösterim Şekil 1.21’de verilmiştir. Bu saldırıdan korunma için ise Şekil 1.22’de gösterilen gölge modeli kullanılmaktadır. Sistemin mahremiyetini test etmek için yapay bir saldırı planlanır. Bu saldırı sistem tasarımcısı tarafından daha önce oluşturulmuş gölge model olarak adlandırılan sentetik modellere yönlendirilip yönlendirilmediği kontrol edilir. Eğer saldırılar gölge modellere yönlendirilebiliyorsa bu model kullanılarak saldırganın asıl veri kümesi yerine asıl veri kümesine benzer bir şekilde üretilmiş sentetik veri kümesine yönlendirilmesi sağlanarak verinin mahremiyeti sağlanmış olur (Fredrikson ve ark., 2014).



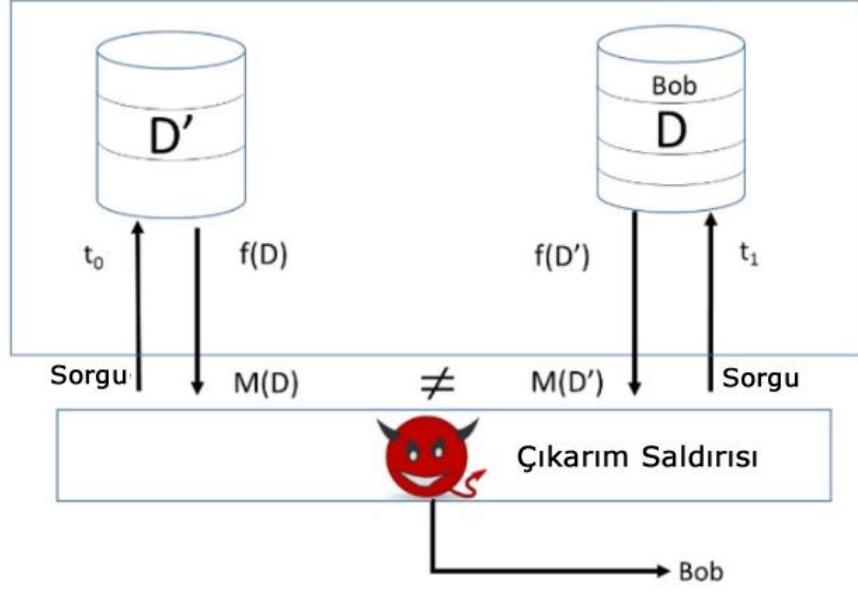
Şekil 1.21 Üyelik çıkarım saldırısının gösterimi (Zhao ve ark., 2019)



Şekil 1.22 Gölge modelinin şematik gösterimi (Shokri ve ark., 2017)

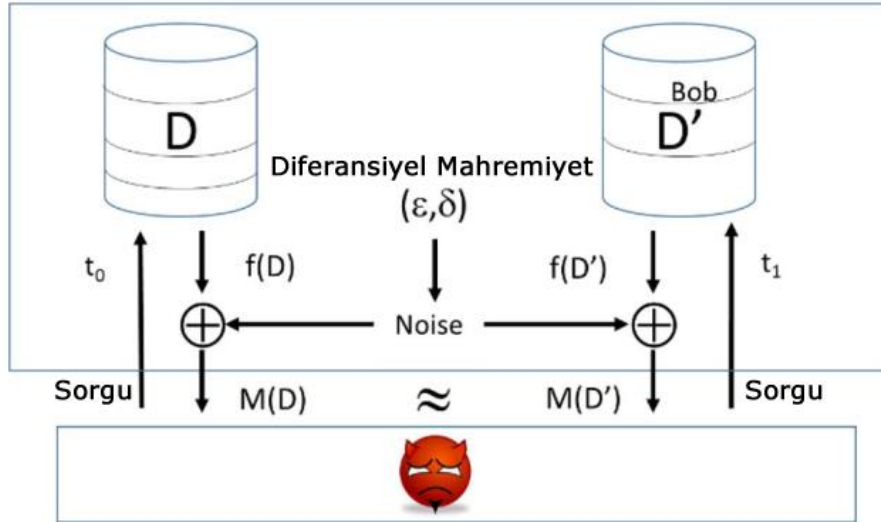
Şekil 1.22’de verilen gölge modelinin uygulanması sürecine örnek vermek gerekirse 100 kullanıcıdan oluşan DB1 adında bir veritabanı olduğu, bu kayıtlardan bir kısmı ile birlikte gerçek olmayan kayıtlardan oluşan 10 tane daha sentetik veritabanının üretildiği varsayılmış olsun. Saldırgan, “zeus” adlı kullanıcının veritabanında olup olmadığını kontrol ederek sisteme sızmaya çalışır. Sızmayı tespit eden sistem saldırganı zeus adlı kullanıcının olduğu sentetik olarak üretilen DB5 veri tabanına yönlendirir. Saldırgan gizli veritabanına eriştiğini düşünür ancak sentetik olarak üretilen veritabanına ulaşmış olur. Bu şekilde saldırganın tüm verilere erişmesi engellenir.

Şekil 1.23 ve Şekil 1.24’te sisteme üyelik çıkarım saldırısı gösterimleri verilmiştir. ϵ ve δ ne kadar küçük belirlenirse, $M(D)$ ve $M(D')$ Şekil 1.23 ve Şekil 1.24’te gösterildiği gibi o kadar benzer olur. Sistem, sorgulama sırasında normal verilere gürültü eklemektedir. Saldırgan bu verileri benzer örnekler oluşturmak için kullanmaktadır. Saldırgan tarafından, oluşturmuş olduğu örneklerle benzer tekrar sorgulama yaparak modelin sınıflandırma sistemi çözülmeye çalışılır. Bu saldırılar modelin sınıflandırma sistemi öğrenilene kadar sürdürülür. Diferansiyel mahremiyet mekanizmasının devrede olmadığı sistemde Şekil 1.23’te olduğu gibi sızma girişimi başarılı olur. Ancak diferansiyel mahremiyet mekanizmasının aktif olduğu sistemde ise Şekil 1.24’te olduğu gibi sızma girişimi başarısız olur. Bu tip saldırılar, görüntü işleme, ses tanıma ve kötü amaçlı yazılım algılama vb. uygulamaları içeren alanlarda kullanılmaktadır. Bu saldırılar özellikle görüntü işleme uygulamalarının kullanıldığı derin öğrenme modellerini aldatabilmektedir (Ha ve ark., 2020).



Şekil 1.23 Diferansiyel mahremiyet mekanizmasının olmadığı bir sisteme yapılan sızma girişimi (Ha ve ark., 2019)

Şekil 1.23'te diferansiyel mahremiyet mekanizmasının olmadığı bir sisteme yapılan çıkarım saldırısı gösterimi verilmiştir. Herhangi bir koruma mekanizması olmadığı için saldırgan veritabanında bulunan bob adlı kayıta ulaşmıştır.



Şekil 1.24 Diferansiyel mahremiyet mekanizmasının olduğu bir sisteme yapılan sızma girişimi (Ha ve ark., 2019)

Şekil 1.24'te diferansiyel mahremiyet mekanizmasının olduğu bir sisteme yapılan çıkarım saldırısı gösterimi verilmiştir. Diferansiyel mahremiyet mekanizması olduğu için saldırgan herhangi bir veriye ulaşamamıştır.

1.5.4.2. Eğitim Verisine Saldırı

Bu saldırı yönteminin temel mantığı eğitim setinin belirli kısmı kullanılarak elde edilen modelin çıktısı ile saldırılar düzenlenip diğer verilere erişilmesidir. Bu saldırıların en yoğun gerçekleştiği sistemler yüz tanıma sistemleridir. Saldırganlar bu sisteme girerek görüntü verilerinden kişilerin tanınabilir yüz görüntülerini elde etmeye çalışmaktadırlar (Zhao ve ark., 2019). Şekil 1.25'te model çıkarma saldırısının gösterimi verilmiştir.



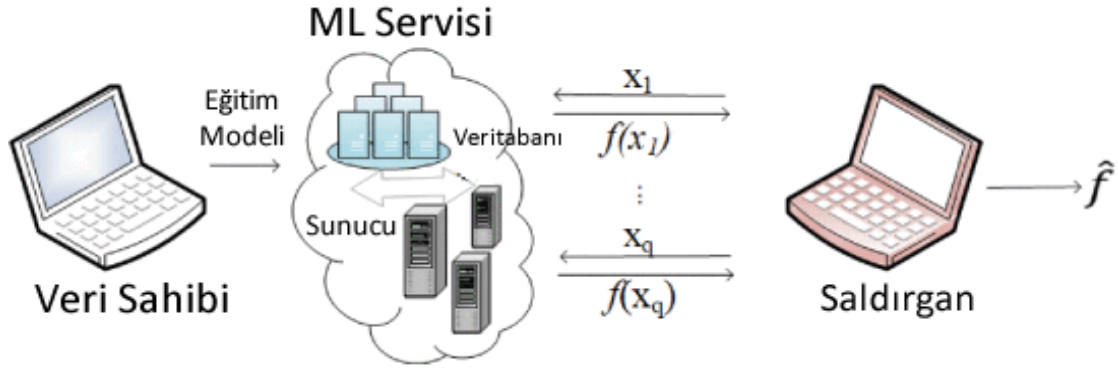
Şekil 1.25 Eğitim verisine saldırı yöntemi kullanılarak elde edilen görüntü (Fredrikson ve ark., 2015)

Şekil 1.25'te model çıkarma saldırısının gösterimi verilmiştir. Bu modelde aynı veri kümesinde uçak, otomobil, kuş, kedi, geyik, köpek, at, gemi, kamyon vb. görüntüler varsa bu görüntüler, eğitim veri kümesindeki belirli bir örneğe karşılık gelemmez ve model bir örneğin eğitim kümesinde olup olmadığına karar veremez. Saldırı etkisi çok sınırlıdır, bu saldırı yalnızca belirli model türleri için kullanılmaktadır (Zhao ve ark., 2019).

1.5.4.3. Model Çıkarma Saldırısı

Model çıkarma saldırısı, kişiye özel veriler üzerinde eğitilen modelin parametrelerini elde etmek için tasarlanmıştır. Saldırgan, eğitim verisi çıktılarından modelin parametrelerine ulaşabilmek için benzer olan modelin işlevselliğini arttırmayı amaçlar. Model parametreleri ve eğitim seti arasındaki yakın bağlantı sebebiyle parametrelerin sızdırılması söz konusu olabilmektedir. Parametrelerin sızdırılması durumunda eğitim verilerinin mahremiyeti tehlikeye düşecektir (Tramèr ve ark., 2016). Şekil 1.26'da model çıkarma saldırısının gösterimi verilmiştir. X veritabanında bulunan herhangi bir veriyi ifade etmektedir. Saldırgan f modelini hedef alarak ona benzer olan $\hat{f}$ modelini oluşturabilir. Bu model ile hedef modelin algoritmalarını ve denklemlerini

çözebilmektedir. Model çıkarma saldırıları model ters çevirme gibi diğer mahremiyet saldırıları için bir basamak işlevi görebilmektedir (Zhao ve ark., 2019). Bununla birlikte, model ters çevirme saldırısı yalnızca aynı tür girdinin bulanık özelliklerini elde eder yani farklı türdeki veriler aynı yerde var ise sonucun neredeyse hiçbir etkisi olmaz (Goodfellow ve ark., 2014).



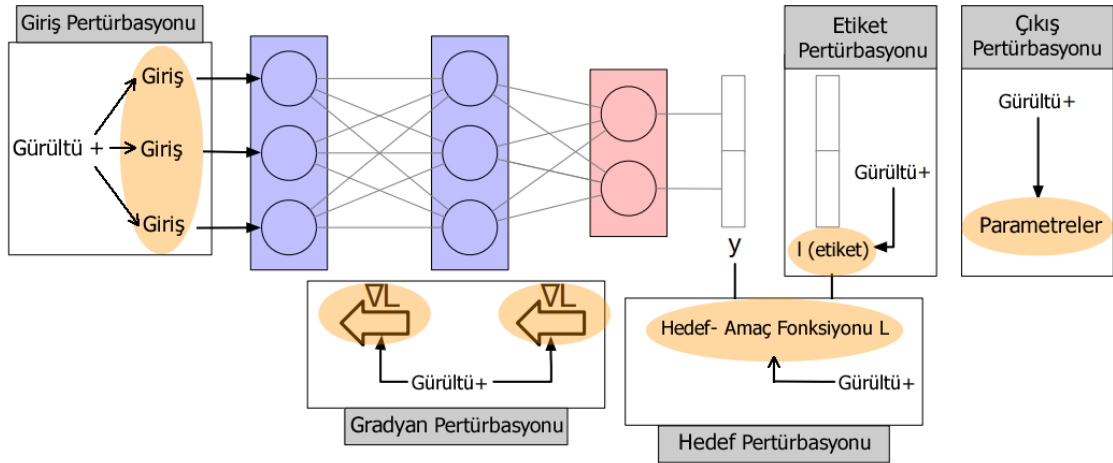
Şekil 1.26 Model çıkarma saldırısının gösterimi (Zhao ve ark., 2019)

1.5.5. Derin Öğrenme Modelleri Kullanılan Sistemlerde Diferansiyel Mahremiyet Mekanizmasının Uygulanması

Derin öğrenmede veri mahremiyeti genel olarak diferansiyel mahremiyet yöntemi ile sağlanır. (Parmaar, 2020).

Şekil 1.27’de derin öğrenme modelleri kullanılan sisteme diferansiyel mahremiyet mekanizmasının uygulanmasına ait şema verilmiştir. Mahremiyet mekanizması giriş, gradyan, hedef, etiket ve çıkış pertürbasyonu olmak üzere 5 yere eklenebilmektedir. Yaygın olarak çıktı, gradyan ve hedef pertürbasyonuna yöntemleri tercih edilmektedir.

Çıktı pertürbasyonunda Laplace ve Gauss mekanizması kullanılır (Zhang ve ark., 2017). Bu yöntemde yapılan işlem sonrası elde edilen çıktı parametresine gürültü eklenerek verinin mahremiyetinin korunması amaçlanır (Yu ve ark., 2019).



Şekil 1.27 Derin öğrenme modelleri kullanılan sistemin farklı bölümlerine diferansiyel mahremiyet mekanizmasının uygulanması (Mireshghallah ve ark., 2020)

Hedef pertürbasyonunda mahremiyet korumasının sağlanması için hedef-amaç fonksiyonuna gürültü eklenir (Wu ve ark., 2017). Bu pertürbasyon, veriye değil hedef-amaç fonksiyonuna gürültü ekleyerek fonksiyonun sonucunu değiştirir. Gürültü eklenmiş ve sonucunda değiştirilmiş olan amaç fonksiyon değerleri orijinal fonksiyon değerleri gibi optimizasyon algoritmalarına iletilir (Nozari ve ark., 2016).

Gradyan pertürbasyonu ise her döngüde oluşan ara sonuç değerlerini değiştirir (Yu ve ark., 2019). Diferansiyel mahremiyet, verilerin sonradan işlenmesine izin verdiğinden gradyan pertürbasyonu, mahremiyet garantisine zarar vermeden her döngüde gürültülü gradyanı serbest bırakarak sonuç elde edilir (Dwork ve Roth, 2014). Gradyan pertürbasyonun, çıktı ve hedef pertürbasyonlara göre çeşitli avantajları vardır. Gradyan pertürbasyonu, hedef üzerinde güçlü bir varsayım gerektirmez çünkü tüm öğrenme sürecinden ziyade yalnızca her gradyan güncellemesinin hassasiyetini sınırlaması gerekir. Bu nedenle gradyana gürültü ekleme yöntemi, dağıtılmış optimizasyon ve birleşik öğrenme ortamında uygun bir seçimdir (Konečný ve ark., 2015), (Agarwal ve ark., 2018), (Jayaraman ve ark., 2018).

Tez çalışmasında gradyan pertürbasyonu yöntemi kullanılmıştır. Sistemin başarı oranının hesaplandığı bölümde SGD optimizasyon algoritması sürecine diferansiyel mahremiyet entegre edilmiştir. Mahremiyet korumalı SGD optimizasyon algoritmasında, tüm gradyanlar yerine rastgele seçilen bazı gradyanların ağırlıkları öğrenme katsayısı ile çarpılarak güncellenmektedir (Seyarer ve ark., 2020). Eğitim parametrelerinin dâhil edildiği her döngüde gradyanlar kırılarak, bu gradyanlara büyüklüğü kontrol edilen

gürültü eklenmiştir. Bu eklenen gürültü sayesinde yetkisiz kullanıcıların gerçek eğitim parametreleri yerine gürültü eklenmiş eğitim parametrelerine erişmeleri sağlanmış olur. Mahremiyetin seviyesi ϵ ile ölçülür, δ ise mahremiyet garantisinin tutmama ihtimalini sınırlar. Mahremiyet ile verilerin koruma derecesi ters orantılıdır. Epsilon ne kadar yüksek olursa, verilerin koruma derecesinin o kadar az olduğu ve kullanıcı bilgilerinin ortaya çıkma ihtimalinin o kadar yüksek olduğu anlamına gelir (Parmaar, 2020).

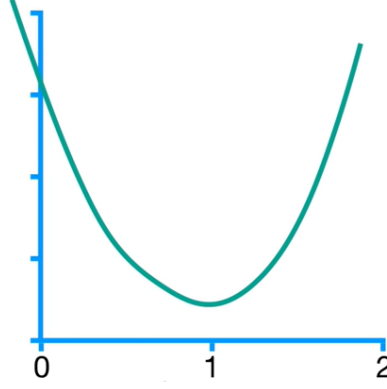
1.5.5.1. Diferansiyel Mahremiyet Korumalı SGD Optimizasyonu

SGD (Stochastic Gradient Descent), derin öğrenme mimarisi temelli modellerde kullanılan popüler bir optimizasyon algoritmasıdır. SGD'de model ile ilgili değerlerin optimize edilmesi sürecinde gradyan hesabı yapılırken adımlar arasından kademeli olarak düşüş gerçekleştirerek, en uygun değer elde edilmeye çalışılmaktadır (Ruder, 2016). Normal gradyan inişte minimum işlem adımına ulaşmak çok fazla hesaplama yapabileceğinden bu büyük zaman kaybına neden olur. SGD bunun yerine, ağırlık güncellemelerinin yalnızca rastgele seçilen tek bir noktanın gradyan hesaplamasını yaptığı için bu zaman kaybını önlemektedir (Carpenter ve ark., 2018). SGD'nin temel mantığı, tüm gradyanlar yerine rastgele seçilen bir kısım gradyanlarla ağırlıkların güncellenmesidir.

1.5.5.2. Gradyan Hesabı

Gradyan çok boyutlu bir türev gibidir. Çok boyutlu girdileri olan bir fonksiyon düşünüldüğünde gradyan, fonksiyon çıktısının girdinin her boyutuna göre ne kadar hızlı değiştiğini gösterir. SGD optimizasyon algoritması ile gradyanlara ait değerler optimize edilerek diferansiyel mahremiyet sürecine dahil edilmektedir.

SGD algoritması kullanılan modellerde gradyanlar verilerin belirli özelliklerine göre Şekil 1.28'de verilen dış bükey düzleme yerleştirilmektedir. Normal gradyan iniş hesabında tek tek tüm noktaların düzlemdeki yerlerine göre uzaklıkları alınarak kesişim noktaları karelerinin artanlarının toplamı yöntemi kullanılarak dış bükey düzleme yerleştirilir. Gradyan hesabı buna göre yapılır. SGD algoritması kullanılan modellerde ise başlangıç, iniş ve bitiş noktaları belirlenerek optimum sonuca yakın hesaplama sayısı artırılarak gradyan hesabı yapılmaktadır.



Şekil 1.28 Gradyan hesabında kullanılan dış bükey düzlem (Starmer, 2019)

Gradyan hesabında kullanılan kayıp fonksiyonu Denklem 1.7’de verilmiştir. Denklemde y ara güncellemeler sırasında oluşan değişken güncelleme değerini, X veri kümesini, w ağırlığı, b ise eklenecek gürültüyü ifade etmektedir (Wang, 2018).

$$C(y, w, X, b) = \frac{1}{N_0} \sum_{i=1}^N (y_i - \max(0, w \cdot X_i + b))^2 \quad (1.7)$$

Her iterasyondaki gradyan (neuron) hesabı ise ilgili formül Denklem 1.8’de verilmiştir. Bu denklemde x girdi verisini, w ağırlığı b ise eklenecek gürültüyü ifade etmektedir (Wang, 2018). Her iterasyonda yinelemenin, yalnızca bir eğitim örneğini analiz etmesi sebebiyle, sadece tek örneğin değerlendirildiği bir döngüden sonra bile parametreler güncellenir.

$$neoron(x) = \max(0, w \cdot x + b) \quad (1.8)$$

SGD optimizasyon algoritmasına dahil edilen diferansiyel mahremiyet mekanizması, mahremiyet maliyetlerini eğitim adımları arasında eşit şekilde dağıtarak eğitim verilerinin mahremiyetini sağlar ve mahremiyet koruması sağlanan sistemin, mahremiyeti ne düzeyde sağladığını ölçer (Du ve ark., 2021). Verilerin analizinde mahremiyetin sağlanmasının yanında veriden de yüksek düzeyde fayda elde edilmesi amaçlandığından bu işlemler yapılırken verilerin bozulmaması gerekmektedir. Diğer yöntemlerde veriye veya çıktıya gürültü eklenerek gerçek veriler korunmaya çalışılmaktadır. Ancak verilerin miktarı ve eklenen gürültülerin büyüklüğü arttıkça veride bozulma olacağından veriden elde edilecek fayda da azalacaktır. Diferansiyel mahremiyet mekanizması, mahremiyeti sağlamak için veriye değil ilgili sorgu fonksiyonun sonucuna

gürültü ekleyerek verinin miktarı ve büyüklüğü ne kadar fazla olursa olsun veriden elde edilecek faydayı azaltmamaktadır.

Derin öğrenme mimarilerinde öğrenme süreci içerisindeki gradyanların hesaplanması aşamasında veriler kullanıldığı için gradyan değerini bilen saldırganların veriyede ulaşma ihtimali yüksektir. Dolayısıyla gradyan hesabında veri kullanıldığı için bu alanda mahremiyetin sağlanması gerekmektedir. Diferansiyel mahremiyet mekanizması burada devreye girerek her gradyanın hesaplanması sırasında Denklem 1.7’de de görüleceği üzere gradyan hesabına gürültü çarpanında belirlenmiş olan değer eklenmektedir. Bu işlem sonucunda hesaplanan gradyan değeri gerçek değer olmadığı için bu gradyan değerini ele geçiren saldırganların gerçek gradyan bilgisine yani verilere ulaşmaları engellenmiş olur.

Çalışma kapsamında eğitim veri kümesinden elde edilen parametreler ile sistem eğitilmektedir. Eğitim sürecinde diferansiyel mahremiyet burada devreye girerek gradyan hesabından elde edilen değere gürültü çarpanı ile belirlenmiş değer kadar gürültü eklemektedir. Ardından test veri kümesindeki görüntülerin parametreleri eğitim veri kümesinden elde edilen parametreler ile karşılaştırılarak hastalık teşhisi gerçekleştirilmektedir. Eğitim ve test parametrelerinin birbirlerine göre farklılıklarına göre kayıp fonksiyon değerleri elde edilmektedir. Daha sonra bu kayıp değerlerinin ortalaması alınarak her iterasyon için ortalama kayıp fonksiyon değeri ve aynı şekilde ortalama başarı oranı da elde edilmektedir. En son gürültü eklenmiş ortalamalar toplanarak bu değerlerin ağırlıklarına göre aritmetik ortalaması hesaplanmaktadır. Bu hesap ile birlikte sistemin başarı oranı, duyarlılığı vb. değerleri elde edilmektedir.

Algoritma 1, deneysel olarak elde edilen kayıp fonksiyonu $\mathcal{L}(\theta)$ 'yi en aza indirerek θ parametreleriyle bir modeli eğitmek için kullanılan temel yöntemi özetlemektedir (Abadi ve ark., 2016). Algoritmada eğitim verilerinin kullanıldığı tek kısım gradyan hesaplamasının yapıldığı kısımdır (Abadi ve ark., 2016). Dolayısıyla saldırganların eğitim verilerini elde etmek için saldırı düzenleyecekleri kısımda burasıdır. Mahremiyetin sağlanabilmesi için modelin güncellenmesinden önce her iterasyonda gradyanın kendisine $g_t[x_i] \leftarrow g_t[x_i] + X_{i,t}$ fonksiyonu ile gürültü eklenmektedir. Gürültü doğrudan gradyana eklendiği için bu yaklaşıma genellikle gürültülü gradyan inişi denir.

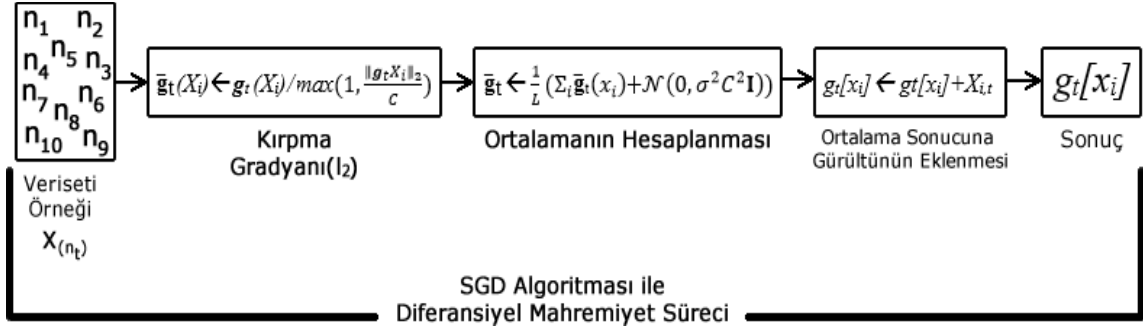
Algoritma – 1: Diferansiyel Mahremiyet Uygulanmış SGD algoritması**Giriş:** Örnekler($X_1 \dots X_n$), Kayıp Fonksiyonu $\mathcal{L}(\theta) = \frac{1}{N} \sum_i \mathcal{L}(\theta, x_i)$

Parametreler: η_t = Öğrenme oranı, σ = Gürültü ölççeği, L = Grup boyutu, C = gradyan model sınırı, X = Veri kümesi(Veriler), T = Orjinal veri kümesi t = Orjinal veri kümesi içerisinde seçilmiş veri

 $t \in [T]$ (Seçilen her veri, veri kümesinden olmalı) L/N örnekleme olasılığı için rastgele L_t örneği alınır. $(X_i) \leftarrow \nabla_{\theta_t} \mathcal{L}(\theta_t, X_i)$ (her L_t nin i elemanı için $g_t(X_i)$ in hesaplanması)**Kırpma Gradyanı** $\bar{g}_t(X_i) \leftarrow g_t(X_i) / \max(1, \frac{\|g_t X_i\|_2}{C})$ (her gradyanın büyüklüğünün kırılması)**Ortalamanın Hesaplanması ve Gürültü Ekleme** $\bar{g}_t \leftarrow \frac{1}{L} (\sum_i \bar{g}_t(x_i) + \mathcal{N}(0, \sigma^2 C^2 \mathbf{I}))$ (kırılmış gradyanların ortalamasının hesaplanması) $g_t[x_i] \leftarrow g_t[x_i] + X_{i,t}$ (gürültünün eklenmesi)**Gradyan İniş** $\theta_{t+1} \leftarrow \theta_t - \eta_t \bar{g}_t$ (iniş yönünde bir adım atılması)

SGD'nin her adımında, rastgele bir örnek alt kümesi için $\nabla_{\theta_t} \mathcal{L}(\theta_t, X_i)$ gradyanı hesaplanmaktadır. Yüksek mahremiyet garantisinin sağlanması için her bir örneğin g_t üzerindeki etkisinin sınırlandırılması gerekmektedir. Gradyanların boyutlarında standart bir ölçü olmadığı için her gradyan, l_2 normu ile kırılmaktadır. Gradyan vektörü (g), kırpma sınırı C için $g / \max(1, \frac{\|g\|_2}{C})$ fonksiyonu ile değiştirilmektedir. Kırpma işlemi sırasında, $\|g\|_2 \leq C$ durumunda g 'nin korunması sağlanırken, $\|g\|_2 > C$ durumunda ise kırpma değeri C nin değeri kadar yapılır (Abadi ve ark., 2016). Her döngüde yapılan bu işlem kırpma gradyanı olarak tanımlanmaktadır.

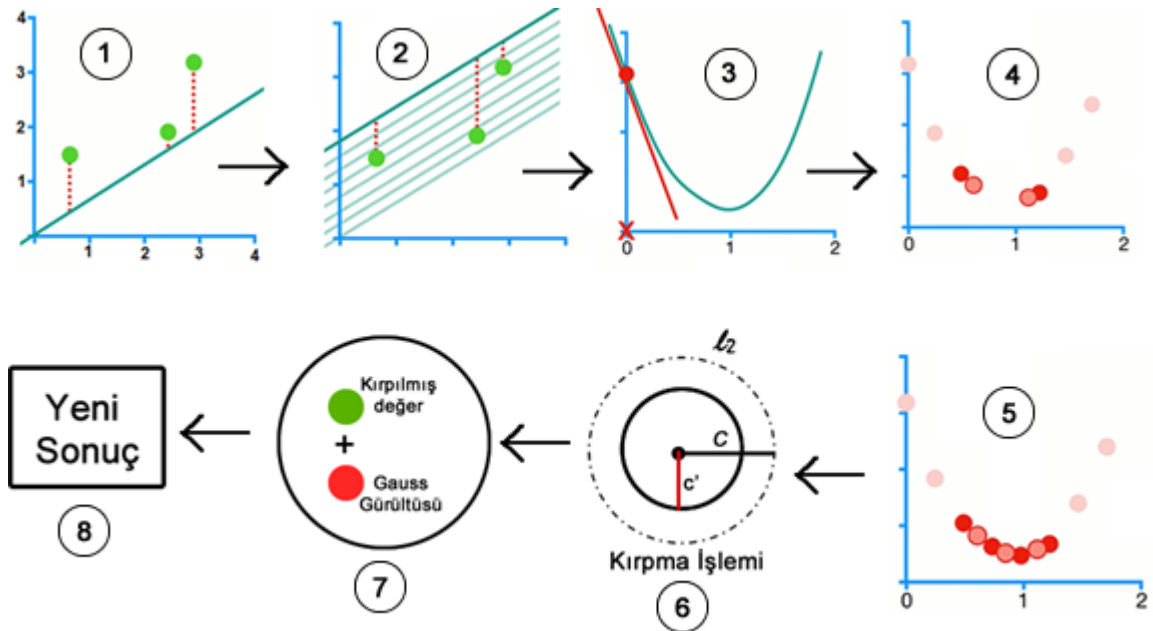
Şekil 1.29'da SGD algoritmasıyla gradyanlara gürültü eklenerek diferansiyel mahremiyetin mahremiyetin sürece nasıl dâhil edildiği gösterilmektedir. Şekil 1.30'da ise SGD optimizasyon algortması ile Diferansiyel mahremiyet sürecinin sisteme dahil edilmesine ait işlem adımları görsel olarak verilmiştir.



Şekil 1.29 SGD algoritmasıyla gradyanlara gürültü eklenerek diferansiyel mahremiyetin sürece dâhil edilmesi

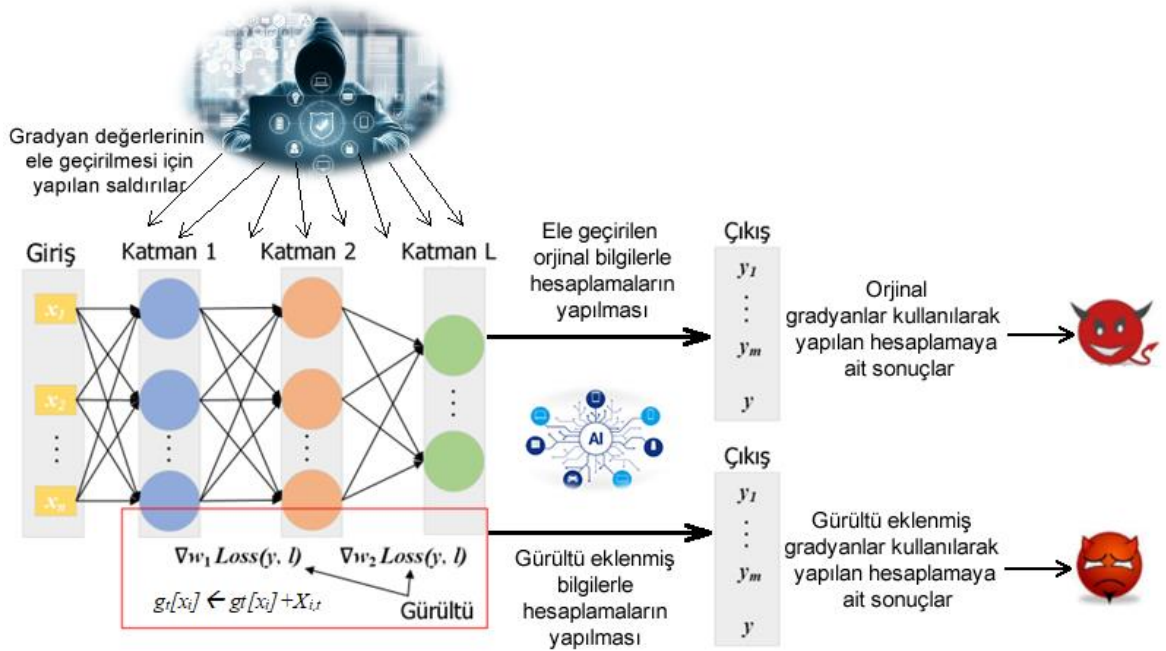
İşlem Adımları:

1. Veri kümesinden rastgele veri seçilmesi
2. Gradyan hesabı için verilerden özelliklerinin elde edilme süreci
3. Gradyan hesabında kullanılacak iniş noktasının belirlenmesi
4. Gradyan hesabı için verilerin istenilen düzleme taşınması
5. Seçilen verilerin özelliklerine göre gradyanın hesaplanması
6. Hesaplanan değerin l_2 normunda belirlenen C kadar kırılması
7. Yeni oluşan değere Gauss gürültüsünün eklenmesi
8. İterasyon için gürültü eklenmiş sonucun elde edilmesi



Şekil 1.30 SGD optimizasyon algoritması ile diferansiyel mahremiyet sürecinin sisteme dahil edilmesine ait işlem adımları

Gerçekleşen hastalık teşhisi ve mahremiyet koruma işleminin sonunda, modelin çıktısına ek olarak tutulan bilgilere göre, mahremiyet mekanizmasının başarı oranı hesaplanmaktadır. Elde edilen sonuçlara bakıldığında, çıktı değerlerinin ϵ ile batch_size'dan çok gürültü ile veri kümesine bağlı olduğu görülmüştür. DP-SGD algoritması kullanılan modellerde gradyan hesabı birçok kez yapıldığından dolayısıyla veri kümesindeki eğitim parametrelerine de erişim yoğun bir şekilde yapılmaktadır. İterasyon sayısının az olması başarı ve doğruluk değerlerinin düşük çıkmasına sebep olacağı gibi iterasyon sayısının çok olması da toplam ϵ değerinin çok büyük değerlere ulaşmasına sebep olabilmektedir. Bu durumlarda istenen mahremiyet seviyesine ulaşılamamaktadır. Bu gibi durumlarda mahremiyet kayıplarının kontrol edilmesi gerekmektedir. Abadi çalışmasında toplam ϵ her iterasyonda kontrol edilip eklenen gürültü sınırlandırılmıştır. Bu şekilde mahremiyeti korumaya çalışmıştır (Abadi ve ark., 2016).



Şekil 1.31 Gradyan bilgilerinin ele geçirilmesine yönelik yapılan saldırılar ve sonuçları (X. Liu ve ark., 2020)

Derin öğrenme modeli kullanılarak tasarlanmış bir sistemde hesaplanan ara değerlere diferansiyel mahremiyet mekanizması ile gürültü eklenmesi ve yapılan saldırıların gösterimi Şekil 1.31’de verilmiştir. Saldırganlar eğitim sonunda elde edilen gradyan değerlerine ulaşmaya çalışmaktadır. Gerçek gradyan değerlerinin saldırganlar tarafından ele geçirilmesi durumunda gradyan değerleri için tersine bir işlem yürütülerek gerçek veriye ulaşılabileceğinden, gradyan değerlerinin korunması mahremiyet açısından

önem arz etmektedir Saldırganlar, eğitim sürecinde gradyanlara eklenen gürültü sayesinde gerçek gradyan değerleri yerine gürültülü gradyan değerlerine erişim sağlamış olur ve bu şekilde orijinal verilerin mahremiyeti korunur.

Bu tez çalışmasında gradyan pertürbasyonu ile diferansiyel mahremiyeti sağlayan DP-SGD algoritması tercih edilmiştir. Bu algoritmanın tercih edilmesinin sebebi ise kolay uygulanabilir olması ve algoritmadaki ifadelerin matematiksel olarak kanıtlanmış olmasıdır.



2. ÖNCEKİ ÇALIŞMALAR

Bu bölümde literatürdeki, diferansiyel mahremiyet mekanizmasını kullanan çalışmalar, Covid-19 tespitinde derin öğrenme tekniklerini kullanan çalışmalar ve Covid-19 tespitinde veri mahremiyetini dikkate alan derin öğrenme temelli çalışmalar hakkında bilgi verilmiştir.

2.1. Diferansiyel Mahremiyet Mekanizmasını Kullanan Çalışmalar

Shokri ve arkadaşları çalışmalarında (Shokri ve Shmatikov, 2015), çok sayıda kullanıcıdan oluşan büyük bir gruba ait hassas verilerin başka kişilere sızdırılmadan bir sinir ağı modeli tasarlayacak sistem geliştirdiler. Geliştirdikleri sistem ile gruptaki her bir kullanıcının hassas verileri birbirlerinden bağımsız olarak eğitilmiştir. Verilerin mahremiyetini korumak ve güvenlik riskini en aza indirmek için diferansiyel mahremiyet mekanizması kullanılmış olup parametrelere gürültü eklenerek parametreler güncellenmiştir.

Abadi ve arkadaşları çalışmalarında (Abadi ve ark., 2016), diferansiyel mahremiyet mekanizması ve SGİY kullanarak yeni bir yöntem geliştirmişlerdir. Verinin mahremiyetini korumak için her eğitim döngüsü sonrasında ağ parametrelerini güncellemeden önce gradyana gürültü eklenmiştir.

Chase ve arkadaşları çalışmalarında (Chase ve ark., 2017) tasarladıkları model ile ilgili çalışmalarında verilerin mahremiyetini korumak için diferansiyel mahremiyet mekanizmasını SMPC yöntemi ile birlikte kullanmışlardır.

Brett ve arkadaşları ise biyomedikal bilgiler içeren verilerin mahremiyetini korumak için çalışmalarında (Jones ve ark., 2019) verilere rastgele gürültü ekleyerek diferansiyel mahremiyet mekanizmasını kullanmışlardır.

Gong ve arkadaşları yayınladıkları çalışmalarında (Gong ve ark., 2020), merkezi bir sunucu ile kullanıcıların verilerinin mahremiyetini korumak için diferansiyel mahremiyet mekanizması ile homomorfik şifrelemenin beraber kullanıldığı bir sistem tasarlamışlardır.

Chaudhuri ve arkadaşları çalışmalarında (Chaudhuri ve ark., 2011) hassas bilgiler içeren eğitim verilerinin sınıflandırması üzerinde çalışmış olup bu sınıflandırmaya ait hassas verilerin mahremiyetini korumak için diferansiyel mahremiyet mekanizmasını kullanmışlardır.

Filho ve arkadaşları çalışmalarında (Filho ve ark., 2021) Covid-19 hastalık teşhisini gerçekleştirmeyip sadece Covid-19 hastalarına ait ad, cinsiyet ve adres bilgilerini diferansiyel mekanizması kullanarak gizlemeyi amaçlamışlardır. Bu çalışmada %70 e yakın başarı oranı elde etmişlerdir.

2.2. Covid-19 Tespitinde Derin Öğrenme Tekniklerini Kullanan Çalışmalar

CNN mimarisini kullanarak Covid-19 hastalık teşhisi gerçekleştiren literatürdeki güncel bazı çalışmalar aşağıda özetlenmiştir.

Javaheri ve arkadaşları çalışmalarında (Javaheri ve ark., 2020), 287 hastadan 89.145 adet CT görüntüsünden oluşan veri kümesi ile Covid-19 hastalığını teşhis eden ve diğer akciğer hastalıklarından ayırt eden CovidCTNet adlı CNN tabanlı açık kaynak bir algoritma seti geliştirmişlerdir. Bu çalışma ile hastalık teşhisinde %90 başarı oranı elde etmişlerdir.

Runwen Hu ve arkadaşları 1042 CT görüntüsü kullanarak yaptıkları çalışmalarında (Hu ve ark., 2020) hem Covid-19 hastalığını teşhis etmiş hemde bu hastalığı diğer solunum yolu hastalıklarından ayırmayı başarmışlardır. Bu çalışmada gürültü olmayan veri kümesinde %96,89, %10 gürültü bulunan görüntüler kullanılarak ise %92,23 başarı oranı elde etmişlerdir.

Federe öğrenme ile Covid-19 hastalığını teşhis eden Liu ve arkadaşları çalışmalarında (Liu ve ark., 2020), 15.282 adet CXR görüntüsünden oluşturdukları özel veri kümesi kullanmışlardır. Bu veri kümesini kullanarak CovidNET modelinde %90,06, MobileNet-V2 modelinde %88,98, ResNet18 modelinde %91,07 ve ResNeXt modelinde ise %91,26 başarı oranı elde etmişlerdir.

Mondal ve arkadaşları çalışmalarında (Mondal ve ark., 2020) Amerika'daki Johns Hopkins Üniversitesi ile Brezilya'daki Albert Einstein İsrail Hastanesinden alınan 5644 adet CT görüntüsü ile oluşturdukları veri kümesi ile Covid-19 hastalığını diğer solunum yolu hastalıklarından ayırarak sınıflandırma çalışması yapmışlardır. Bu çalışma sonunda %93,13 başarı oranı elde etmişlerdir.

Mohammed ve Hussain çalışmalarında (Muhammad ve Hossain, 2021), 12.210 adet CT görüntüsü ile oluşturdukları veri kümesini kullanarak Covid-19 hastalığını teşhis etmeye çalışmış ve bu çalışma ile hastalık teşhisinde %97,1 başarı oranı elde etmişlerdir.

Buonsenso ve arkadaşları 500 den fazla CT ve CXR görüntüsü kullanarak yaptıkları çalışmalarında (Buonsenso ve ark., 2020), Covid-19 virüsünün hacmini ölçen bir sistem tasarlamış ve %91,6 başarı oranı elde etmişlerdir.

Covid-19 hastalığını teşhis etmek için COVID-Net adlı bir derin öğrenme modeli geliştiren Loey ve arkadaşları çalışmalarında (Loey ve ark., 2020), 612 CXR görüntüsü kullanarak gerçekleştirdikleri deneylerde farklı modeller kullanarak %99,6 başarı oranına ulaşmışlardır.

Abbas ve arkadaşları çalışmalarında (Abbas ve ark., 2021), normal hastalara, Covid-19 hastalarına ve Sars hastalarına ait CXR görüntülerini kullanarak CNN tabanlı DeTraC adlı bir model geliştirmişlerdir. 196 adet görüntü ile geliştirdikleri bu sistem ile %95,1 başarı oranı elde etmişlerdir.

Solunumsesi ve CXR görüntüsü kullanarak Covid-19 hastalığını teşhis eden CNN tabanlı, çok modlu bir model öneren Sait ve arkadaşları çalışmalarında (Sait ve ark., 2021), geliştirdikleri bu model ile solunum yolu sesi kullanılarak hastalık teşhisinde %80, CXR görüntüsü kullanarak gerçekleştirilen hastalık teşhisinde %99,66 başarı oranı elde etmişlerdir.

3487 CT görüntüsünden (1579 normal, 1485 zatüre ve 423 Covid-19 hastası görüntüsü) oluşan veri kümesi ile AlexNet, ResNet-18, DenseNet201, ve SqueezeNet modelleri kullanarak Covid-19 hastalık teşhisi gerçekleştiren Chowdhury ve arkadaşları çalışmalarında (Chowdhury ve ark., 2020), %99,7 başarı oranı elde etmişlerdir.

Maghdid ve arkadaşları çalışmalarında (Maghdid ve ark., 2021), CNN tabanlı AlexNet modeli kullanarak, Covid-19 hastalığına yakalanmış hastalara ait 170 CXR görüntüsü, 361 CT görüntüsünden oluşan veri kümesi ile Covid-19 hastalık teşhisi gerçekleştirmişlerdir. Çalışma ile CXR görüntüsü kullanarak gerçekleştirdikleri hastalık teşhisinde %98, CT görüntüsü kullanarak gerçekleştirdikleri hastalık teşhisinde ise %94,1 başarı oranı elde etmişlerdir.

1428 CXR görüntüsünden (224 Covid-19, 700 solunum yolu hastası ve 504 normal hasta görüntüsü) oluşan veri kümesi ile CNN tabanlı MobileNet-V2 modeli kullanılarak Covid-19 hastalığının teşhisini gerçekleştiren Apostolopoulos ve Mpesiana çalışmalarında (Apostolopoulos ve Mpesiana, 2020), %98,66 duyarlılık, %96,46 özgüllük ve %96,78 başarı oranı elde etmişlerdir.

Linda Wang ve arkadaşları çalışmalarında (Wang ve ark., 2020), Covid-19 virüsünü tespit etmek için CNN tabanlı VGG-19, ResNet50 ve COVID-Net modellerini kullanmışlardır. 16.756 CXR görüntüsünden oluşan yeni veri kümesi kullanılarak hastalık teşhisinde en yüksek oranı COVID-Net ile %91 duyarlılık ve %93,3 başarı oranı elde etmişlerdir.

Ghoshal ve Tucker çalışmalarında (Ghoshal ve Tucker, 2020), 5941 CXR görüntüsünden oluşan veri kümesi ile Covid-19 hastalığını teşhis etmişlerdir. CNN tabanlı ResNet50V2 modeli kullanarak yapmış oldukları teşhis işleminde %89,82 başarı oranı elde etmişlerdir.

Covid-19 hastalığını zatüre gibi solunum yolu hastalığından ayıran ve hastalığı teşhis ederek bir sınıflandırma modeli öneren Öztürk ve arkadaşları çalışmalarında (Ozturk ve ark., 2020) %98,08 başarı oranı elde etmişlerdir. Bu çalışmada 120 hastaya ait 1000 CXR görüntüsü kullanarak oluşturdukları veri kümesi kullanmışlardır.

Uçar ve Korkmaz çalışmalarında (Ucar ve Korkmaz, 2020), Covid-19 hastalığını CXR görüntülerinden teşhis eden SqueezeNet tabanlı yeni bir model önermişlerdir. Önerdikleri bu model ile Covid-19 hastalığını teşhis etmiş ve onu zatüre hastalığından ayırmışlardır. Bu çalışma ile %98,3 başarı oranı elde etmişlerdir.

Xu ve arkadaşları çalışmalarında (Xu ve ark., 2020), 618 CT görüntüsü kullanarak Covid-19 hastalığını teşhis etmişlerdir. Noisy-OR Bayesian olasılık fonksiyonu ile hesaplanarak gerçekleştirilen hastalık teşhisinde %86,7 başarı oranı elde etmişlerdir.

CT ve CXR görüntülerinden oluşan 3 farklı veri kümesi kullanarak Covid-19 hastalığının teşhisini gerçekleştiren Narin ve arkadaşları çalışmalarında (Narin ve ark., 2020), veri setlerinde sırasıyla %96,1, %99,5 ve %99,7 başarı oranları elde etmişlerdir.

Toğaçar ve arkadaşları çalışmalarında (Toğaçar ve ark., 2020), Covid-19 tespitinde CNN mimari temelli bir model geliştirmiş olup Covid-19 hastalığını diğer pnömoni hastalıklarından ayırarak doğru bir şekilde sınıflandırmışlardır. Çalışma sonunda %99,27 başarı oranı elde etmişlerdir.

Farooq ve Hafeez çalışmalarında (Farooq ve Hafeez, 2020), Covid-19 hastalığını diğer solunum yolu hastalıklarından ayırmayı amaçlamışlardır. Çalışma kapsamında CNN tabanlı CovidResNet50 adlı yeni bir yaklaşım modeli sunmuşlardır. Bu model ile Covid-19 hastalığının teşhisinde %96,23 başarı oranına ulaşmışlardır.

CT görüntülerinden Covid-19 hastalığını tespit etmek isteyen Ko ve arkadaşları (Ko ve ark., 2020) çalışmalarında CNN tabanlı bir sistem tasarlayarak Covid-19 hastalığını diğer solunum yolu hastalıklarından ayırmayı başarmışlardır. İtalyan Tıbbi ve Girişimsel Radyoloji Derneği, Wonkwang Üniversite Hastanesi ve Chonnam Ulusal Üniversite Hastanesinden elde ettikleri CT görüntülerinden oluşan veri kümesi ile %100,00 özgüllük, %99,58 duyarlılık ve %99,87 başarı oranlarına ulaşmışlardır.

Zhang ve arkadaşları çalışmalarında (Zhang ve ark., 2020) 43.370 adet CT ve CXR görüntüsü ile oluşturulan veri kümesini kullanarak hem Covid-19 hastalığını teşhis etmiş hemde bu hastalığı diğer solunum yolu hastalıklarından ayıran CNN tabanlı bir sistem tasarlamışlardır. Tasarladıkları bu sistem ile hastalığın teşhisinde %83,61 başarı oranı elde etmişlerdir.

Shou Wang ve arkadaşları (Wang ve ark., 2020) çalışmalarında, 4106 hastaya ait 5372 CT görüntüsü kullanarak Covid-19 hastalığının teşhisinde %90 başarı oranına ulaşmışlardır.

Hemdan ve arkadaşları (Hemdan ve ark., 2020) çalışmalarında CT görüntülerinden oluşan veri kümesi ile hastalığın çeşitleri ile ilgili sınıflandırma yapan CNN tabanlı Derin Öğrenme Sınıflandırıcıları Çerçeve Modeli oluşturmuşlardır. Çalışma ile Covid-19 hastalarının sınıflandırmasında ise %91, Covid-19 dışındaki solunum yolu hastalıklarının sınıflandırmasında ise %89 başarı oranına ulaşmışlardır.

2.3. Covid-19 Tespitinde Veri Mahremiyetini Dikkate Alarak Derin Öğrenme Tekniklerini Kullanan Çalışmalar

Müftüoğlu ve arkadaşları çalışmalarında (Müftüoğlu ve ark., 2020), Covid-19 hastalığına yakalınmış 139 hastaya ait 373 CXR görüntüsünden veri kümesi kullanmışlardır. Çalışmada Covid-19 hastalığının teşhisi için CNN tabanlı derin öğrenme modeli olan EfficientNet-B0 kullanılarak %94,7 başarı oranı elde etmişlerdir. Daha sonra diferansiyel mahremiyet uyguladıktan sonra ise başarı oranının %71'e düştüğü ifade edilmiştir.

Literatürde diferansiyel mahremiyet kullanılarak Covid-19 hastalık teşhisinin yapıldığı tek çalışma Müftüoğlu ve arkadaşlarının yapmış olduğu çalışmadır (Müftüoğlu ve ark., 2020). Bu çalışmada %71 başarı oranı elde etmişlerdir.

2.4. Derin Öğrenme Mimarileri Kullanılarak Covid-19 Hastalık Teşhisi Yapılan Çalışmaların Karşılaştırılması

Derin öğrenme mimarilerinin tıp alanında büyük başarılar elde etmesi neticesinde Covid-19 hastalığının teşhisinde de yoğun olarak kullanılmaktadır. Hastalığın teşhisi için hastanın CT veya CXR görüntüsü kullanılmaktadır. Derin öğrenme mimarisi kullanılarak Covid-19 hastalığının teşhisini gerçekleştiren literatürde genel kabul görmüş çalışmaların detaylı karşılaştırılması Tablo 2.1’de verilmiştir. Tablodan da görüleceği üzere literatürdeki çalışmalar genellikle, Github ve Kaggle platformlarında halka açık olarak yayınlanan CT ve CXR görüntülerini kullanmaktadır.

Hastalık teşhisinde CT ve CXR görüntüleri yaygın bir şekilde kullanılmaktadır. Bu görüntülerden hastanın cinsiyeti, kemik yaşı, hastalığı ve hastaya ait bazı bilgiler elde edilebilmektedir (Chhikara ve ark., 2020). Son yirmi yıla bakıldığında CT, CXR ve ultrason görüntüleri kullanılarak hastalığın erken teşhis çalışmalarına yönelik gün geçtikçe artan bir eğilim görülmektedir. Bunun sebebi radyolojik cihazlardan elde edilen tıbbi görüntülerin sınıflandırılmasında derin öğrenme mimarilerinin başarılı sonuçlar elde etmesidir (Horry ve ark., 2020).

Literatürdeki genel kabul görmüş çalışmalara bakıldığında bu çalışmaların tamamında CNN mimarisi kullandığı görülmektedir. Bunun sebebi CNN mimarisinin katmanlı yapısı sayesinde öğrenme ve sınıflandırma işleminin başarılı şekilde yapılmasıdır. Bu çalışmalardan en yüksek başarıyı, %99,87 başarı oranı ile Ko ve arkadaşları (Ko ve ark., 2020) elde etmiştir. Daha sonra %99,66 başarı oranı ile Sait ve arkadaşları (Sait ve ark., 2020), %99,6 başarı oranı ile de Loey ve arkadaşları (Loey ve ark., 2020) elde etmiştir. Literatürde CT ve CXR görüntüsü kullanılarak Covid-19 hastalık teşhisinde diferansiyel mahremiyet kullanan tek çalışma Müftüoğlu ve arkadaşlarının yapmış olduğu çalışma olup, bu çalışmada %71 başarı oranı elde etmişlerdir (Müftüoğlu ve ark., 2020).

Tablo 2.1 Derin öğrenme ile Covid-19 hastalığını tespit eden çalışmalar

Çalışma	Görüntü Türü	Mimari	Veri kümesi	Veri Sayısı (Adet)	Mahremiyet Odaklı	Doğruluk / Başarı Oranı
(Javaheri ve ark., 2020)	CT	CNN	Çalışmaya Özgü	89.145	Hayır	%90
(Hu ve ark., 2020)	CT	CNN	Çalışmaya Özgü	1042	Hayır	%96,89- %92,23
(Liu ve ark., 2020)	CXR	CNN	COVIDx	15.282	Hayır	%91,26
(Muhammad ve Hossain, 2021)	CT ve CXR	CNN	IEEE 8023	12.210	Hayır	%97,5
(Loey ve ark., 2020)	CXR	CNN	IEEE 8023	612	Hayır	%99,6
(Abbas ve ark., 2021)	CT ve CXR	CNN	Çalışmaya Özgü	196	Hayır	%93,1
(Sait ve ark., 2021)	Ses ve CXR	CNN	Çalışmaya Özgü	36.285	Hayır	%80- %99,66
(Chowdhury ve ark., 2020)	CXR	CNN	Novel Dataset, Italian Society of Medical and Interventional Covid-19 Database	3487	Hayır	%99,70
(Maghdid ve ark., 2021)	CT ve CXR	CNN	IEEE 8023	531	Hayır	%94,1- %98
(Apostolopoulos ve Mpesiana, 2020)	CXR	CNN	COVID-19 Image Data Collection, Covid-19 X-Rays(Kaggle)	1428	Hayır	%96,78
(Wang ve ark., 2020)	CXR	CNN	IEEE8023, RSNA Pneumonia Detection Challenge Dataset, COVID-19 Image Data Collection	16.756	Hayır	%93,3
(Ghoshal ve Tucker, 2020)	CXR	CNN	Çalışmaya Özgü	5941	Hayır	%89,82
(Ozturk ve ark., 2020)	CXR	CNN	COVID-19 Image Data Collection	1000	Hayır	%87,02- %98,08
(Ucar ve Korkmaz, 2020)	CXR	CNN	Kaggle chest X-ray dataset, COVID-19 Image Data Collection, COVIDx dataset	15.903	Hayır	%98,3
(Xu ve ark., 2020)	CT	CNN	Çalışmaya Özgü	618	Hayır	%86,7
(Ko ve ark., 2020)	CT	CNN	Çalışmaya Özgü	3993	Hayır	%99,87
(Narin ve ark., 2020)	CT ve CXR	CNN	Kaggle Chest X-Ray	7406	Hayır	%98,43
(Toğaçar ve ark., 2020)	CT ve CXR	CNN	IEEE 8023	590	Hayır	%99,27
(Farooq ve Hafeez, 2020)	CT ve CXR	CNN	COVIDx	2839	Hayır	%96,23
(Zhang ve ark., 2020)	CT ve CXR	CNN	Çalışmaya Özgü	43.370	Hayır	%83,61
(Wang ve ark., 2020)	CT ve CXR	CNN	CT-EGFR	5372	Hayır	%90,00
(Hemdan ve ark., 2020)	CT ve CXR	CNN	IEEE 8023	50	Hayır	%91,00
(Müftüoğlu ve ark., 2020)	CT ve CXR	CNN	Çalışmaya Özgü	373	Evet	%71,00

2.5. Açık Veri Setleri

Radyoloji uzmanları, Covid-19 dâhil akciğerde oluşan her türlü enefeksiyonu tespit etmek için sıklıkla CT ve CXR görüntülerini kullanmaktadırlar. Covid-19 virüsü vücuda girdiğinde, akciğeri kaplayan epitel hücreleri enfekte etmeye başlar. Sonrasında akciğerde lekeler oluşmaya başlar. Bu lekeler bakılarak hastalık teşhisi yapabilmek için uzman bilgisi ve ciddi bir zaman gerekmektedir. Özellikle Covid-19 salgının yoğun olduğu bölgelerde bulunan hastanelerin temel sağlık sisteminin aksamadan devam ettirilmesi ve hastaların hızlı bir şekilde teşhisini yapabilmek için derin öğrenme mimarileri kullanılmaktadır (Ghoshal ve Tucker, 2020). Bu hastalıklarla ilgili araştırma ve deneysel çalışma yapılabilmesi için halka açık platformlarda Covid-19, Zatüre ve normal hastalara ait CT ve CXR görüntüleri paylaşılmaktadır.

Tablo 2.2’de literatürde Covid-19 hastalığının teşhisi için yaygın olarak kullanılan CT ve CXR görüntülerinin bulunduğu veri setleri ile ilgili bilgiler verilmektedir. Bu tablodan da görüleceği üzere çalışmalarda en çok Joseph Paul Cohen tarafından oluşturulan ve github platformunda paylaşılan veri kümesi kullanılmaktadır. Bunun en önemli sebebi veri kümesinde bulunan görüntülerde gürültü olmaması ve görüntü kalitesinin iyi olmasıdır. Farklı platformlarda incelenen CT ve CXR görüntülerine bakıldığında, bazılarında gürültü olarak adlandırılacak lekeler ve yazılar bulunmaktadır. Bu gürültüler, derin öğrenme mimarilerinin öğrenme ve teşhis işlemlerini güçleştirmekte ve teşhis işleminde başarı oranını ciddi anlamda düşürmektedir.

Tablo 2.2 Literatürde Covid-19 hastalığının teşhisinde yaygın olarak kullanılan verisetleri

Referans	Veri kümesi	Veri Türü	Yayınlandığı Platform	Kullanan Çalışmalar
(Dandil ve Serin, 2020)	Chest X-ray Image Kaggle	Görüntü	Kaggle	(Rabbah ve ark., 2020)
(Cohen, 2020)	Covid-19 X-ray Image dataset (IEEE8023)	Görüntü	Github	(Loey ve ark., 2020) (Hemdan ve ark., 2020) (Muhammad ve Hossain, 2021) (Abbas ve ark., 2021) (Maghdid ve ark., 2021)
(Data, 2018)	Covid-19 X-ray Chest Data	Görüntü	Mendeley Data	(Narin ve ark., 2020)
(Pengtao Xie, 2020)	UCSD-AI4H / Covid-19 CT Image	Tablo	Github	(Sharma, 2020)
(Rahman, 2021)	Covid-19 Radiography Database	Görüntü	Kaggle	(Sait ve ark., 2021)
(Chung, 2020)	Covid-19 Chest X-ray Datasets	Görüntü	Github	(Wong ve ark., 2020) (L.Wang ve ark., 2020)
(Ali, 2019)	Covid-19 Radiography Image Datasets (X-Rays)	Görüntü	Mendeley Data	(Soomro ve ark., 2021)
(Lisphilar, 2020)	Covid-19 Dataset In Japan	Tablo	Kaggle	(Kobayashi ve ark., 2020)
(Tails, 2020)	Covid-19 Dataset in Germany	Tablo	Kaggle	(Mavragani, 2020)
(Mooney, 2020)	Covid-19 Dataset in San Francisco	Tablo	Kaggle	(Gianfrancesco ve ark., 2020)
(Institute, 2020)	Covid-19 Open Research Dataset Challenge	Görüntü ve Tablo	Kaggle	(L. L.Wang ve ark., 2020)
(Zhao, 2020)	Covid-19 X-ray Datasets	Görüntü	Kaggle	(B. Liu ve ark., 2020)
(Rajkumar, 2020b)	Coronavirus Novel Dataset	Tablo	Kaggle	(Levitt ve ark., 2020)
(Sun, 2020)	Covid-19 Dataset in USA	Tablo	Github	(Alamo ve ark., 2020)
(Hu, 2020)	Covid-19 Image Dataset	Görüntü	Github	(Hu ve ark., 2020)
(Goldbloom, 2020)	Covid-19 Data From John Hopkins University Dataset	Tablo	Kaggle	(Zarikas ve ark., 2020)
(Rajkumar, 2020a)	Covid-19 Dataset in India	Tablo	Kaggle	(Prakash ve ark., 2020)
(Data4u, 2020)	Covid-19 and clinical spectrum dataset	Tablo	Kaggle	(Mondal ve ark., 2020)
(Union, 2020)	Covid-19 European Union Open Dataset	Tablo	Data.europa.eu	(Di Pietro ve ark., 2020)
(Larxel, 2020)	Covid-19 Dataset	Tablo ve Görüntü	Kaggle	(Apostolopoulos ve Mpesiana, 2020)
(Badr, 2020)	Covid -19 Unified Dataset	Tablo	Github	(Kerr ve ark., 2021)
(Lira, 2020)	Covid-19 Dataset in Mexico	Tablo	Kaggle	(Medel-Ramírez ve Medel-Lopez, 2020)

3. MATERYAL VE METOT

3.1. Materyal

Bu bölümde Covid-19 hastalık teşhis çalışmasında kullanılan veri kümeleri, araç-gereçler ve geliştirilen sistem ile ilgili bilgiler verilmektedir.

3.1.1. Kullanılan Verisetleri

Covid-19 hastalığının teşhisinde Tablo 2.2’de gösterildiği gibi birçok veri kümesi bulunmaktadır. Ancak görüntü kalitesi ve bu görüntüler ile ilgili yapılan çalışmalarda yüksek başarı ve doğruluk oranları elde edilebildiği için Tablo 3.1’de verilen verisetleri kullanılmıştır. Bu tez çalışmasında, toplamda 3530 adet CT ve CXR görüntülerinden oluşan 5 farklı veri kümesi ayrı ayrı kullanılmıştır. Veri kümeleri ile ilgili bilgiler Tablo 3.1’de verilmiştir.

Tablo 3.1 Tez çalışmasında kullanılan verisetleri

Veri kümesi	Veritürü	Sayısı	Referans	Yayımlandığı platform
Dataset1 (DS1)	CXR	150	(Kaggle, 2020)	Kaggle
Dataset2 (DS2)	CXR	270	(Ali, 2019)-(164 görüntü) (Cohen, 2020)-(106 görüntü)	Kaggle Github
Dataset3 (DS3)	CXR	500	(Tawsifur Rahman, 2021)	Kaggle
Dataset4 (DS4)	CXR	1000	(Mooney, 2020)	Kaggle
Dataset5 (DS5)	CT ve CXR	1610	(Data, 2018)	Mendeley Data

Tez çalışmasında kullanılan verisetlerinde Covid-19 ve Normal hastalara ait CT ve CXR görüntüleri bulunmaktadır. Her veri kümesi ile ilgili sayısal bilgiler Tablo 3.2’de verilmiştir.

Tablo 3.2 Çalışmada kullanılan verisetlerine ait görüntülerin özellikleri

Verisetleri	Covid-19 Bulaşan Hastalara Ait Görüntü Sayısı	Normal Hastalara Ait Görüntü Sayısı	Toplam Görüntü Sayısı
Dataset1 (DS1)	60	90	150
Dataset2 (DS2)	150	120	270
Dataset3 (DS3)	219	281	500
Dataset4 (DS4)	500	500	1000
Dataset5 (DS5)	900	710	1610

3.2. Metot

Bu çalışmada CT ve CXR görüntüsünden oluşan 5 farklı veri kümesi kullanılmıştır. Bu görüntüler ön işlem olarak 200x200 çözünürlüğe dönüştürülmektedir. İlk evrişim katmanının parametrelerinden, girdi boyutu 200x200x2, ağda kullanılan filtrelerin boyutları ise 3x3 şeklindedir.

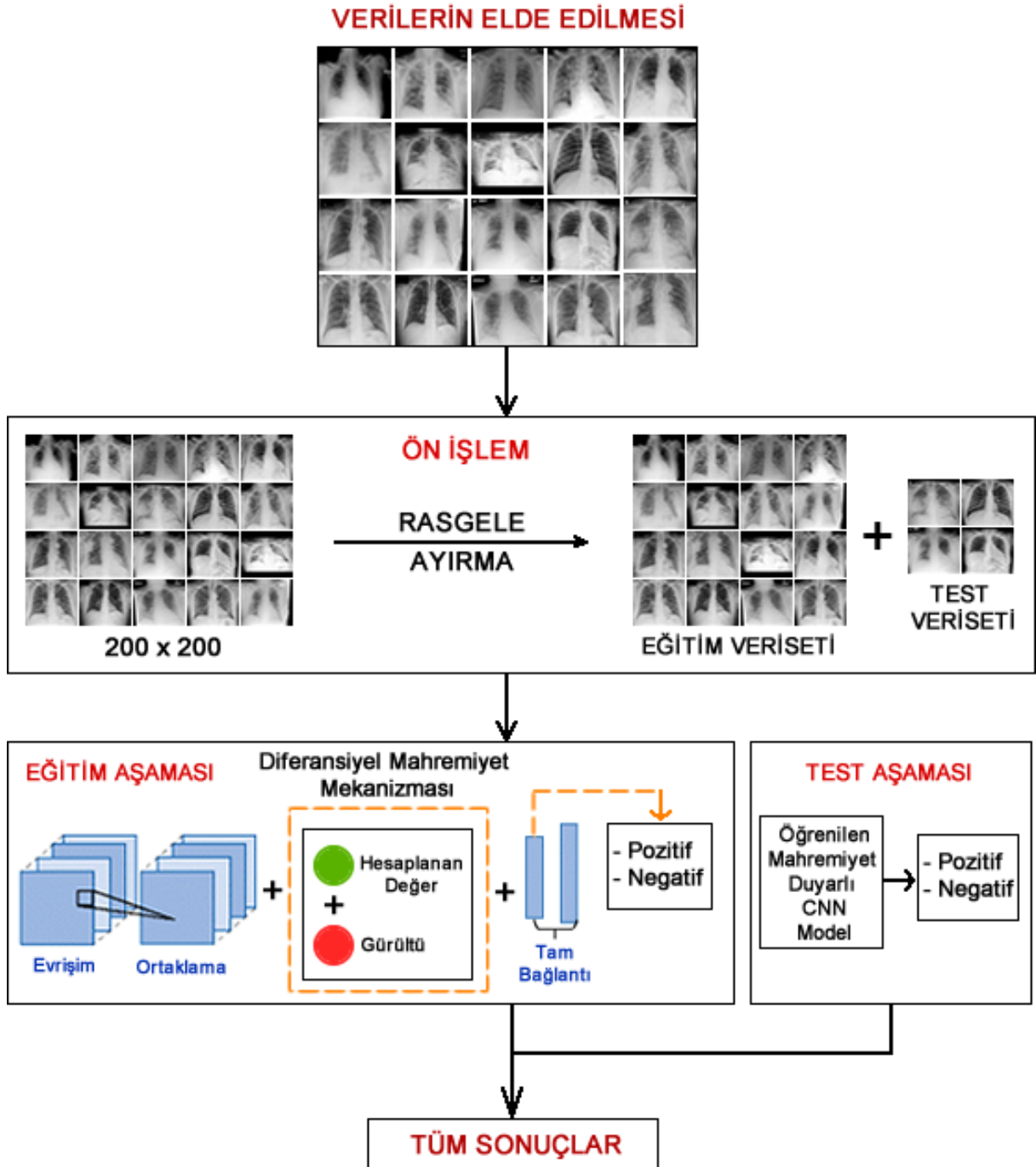
Çalışma kapsamında tasarlanan Covid-19 hastalığını tespit eden sistem python programlama dilinde hazırlanmıştır. Veri kümesinin %80'i eğitim, %20'si test verisi olarak belirlenerek eğitim ve test çalışması yapılmıştır. Çalışmada her veri kümesi için ayrı ayrı farklı epoch ve batch size değerleri test edilerek en doğru sonuca ulaşmaya çalışılmıştır. Yapılan testler sonucunda en doğru ve en geçerli sonuçları veren epoch ve batch size değerleri kullanılarak işlemlere devam edilmiştir. Çalışmada kullanılan 5 veri kümesi literatürde yaygın olarak kullanılan ve genel kabul görmüş veri kümeleridir. Bu veri kümeleri python programlama dilinde hazırlanan CNN mimari tabanlı, DP-SGD optimizasyon algoritması ile her bir veri kümesi için ayrı ayrı olmak üzere hastalık teşhis işlemi gerçekleştirilip başarı ve doğruluk oranları elde edilmiştir. Sistemde epoch ve batch_size değerleri için belirli değerler verilerken denemeler yapılmış olup bu denemeler sonucunda en anlamlı ve en yüksek başarı oranlarının epoch=50, batch_size=8 olduğu durumda elde edildiği görülmüştür. Bu bağlamda tüm deneylerde epoch ve batch size için bu değerler kullanılmıştır. Sisteme farklı δ değerleri manuel olarak girilerek sistemin ε ve doğruluk değerlerinin hesaplanması gerçekleştirilmiştir. En yüksek başarı oranının $\delta=1e-2$ olduğu durumda elde edilmiştir.

Bu tez çalışmasında geliştirilen CNN mimarisi Tablo 3.3.'te verilmiştir.

Tablo 3.3 CNN mimari yapısına ait katmanlar

CNN Mimari Yapısında Katmanlar	Kernel	Çıktının Yapısı
Conv2 + Relu	3*3*32	198*198*32
MaxPooling	3*3*32	99*99*32
Conv2d_1 + Relu	3*3*64	97*97*64
MaxPooling2d_1	3*3*64	48*48*64
Conv2d_2 + Relu	3*3*128	46*46*128
MaxPooling2d_2	3*3*128	23*23*128
Dense + Relu	-	64
Dense + sigmoid	-	1

Ayrıca geliştirilen sistem akış diyagramı olarak Şekil 3.1’de verilmiştir. Çalışma kapsamında literatür taraması yapılarak lüteratürde yaygın olarak kullanılan veri kümelerinden 5 tanesi giriş verisi olarak alınmıştır. Daha sonra veriler ön işleme tabi tutulduktan sonra %80’i eğitim, %20’si test olacak şekilde ayrılmıştır. Eğitim aşamasında diferansiyel mahremiyet mekanizması sisteme dâhil edilerek verilerin mahremiyeti sağlanmıştır.



Şekil 3.1 Tez çalışması kapsamında yapılan işlemlere ait diyagram

3.2.1. Programlama

Çalışmada, Python programlama dilinin 3.9 sürümü ve Anaconda program seti ile birlikte gelen Spider ve Jupyter Notebook programları kullanılmıştır. Teşhis işleminin yapılabilmesi için python programlamada kullanılan Keras ve Tensorflow kütüphaneleri eklenmiştir.

Uygulamada 3 evrişim katmanı, 3 havuzlama katmanı ve 2 tam bağlantı katmanı bulunmaktadır. İlk üç katmanda verilere ait temel öznitelikler çıkarılmış, sonrasında elde edilen değerlere göre ortaklama işlemi uygulanmış ve son olarak tam bağlantı katmanında sınıflandırma işlemi yapılmıştır. Tez çalışmasında CNN ağları kullanılmış olup evrişim katmanında veri kümesine çeşitli filtreler uygulanmıştır.

3.2.2. Uygulamada Kullanılan Hiper parametreler

Model eğitiminde kullanılan parametreler mahremiyet duyarlı ve geleneksel olmak üzere 2 ayrı şekilde farklı değerler verilerek uygulanmıştır. Uygulama sonucunda alınan en yüksek başarı oranlarına bakılarak çalışmada kullanılacak en uygun değerler seçilmiştir. Uygulamada her yığın için hesaplanan hassasiyet 'l2_norm_clip' parametresi ile sınırlandırılmaktadır. Gradyanlara eklenen gürültü miktarı ise 'noise_multiplier' parametresi belirlenmektedir. Uygulamada kullanılan parametrelere ait değerler Tablo 3.5'te verilmiştir.

Tablo 3.4 Uygulamada kullanılan hiper parametreler

Hiper Parametre	Değeri
Görüntünün Girdi boyutu	200 x 200
Öğrenme Katsayısı (learning_rate)	0.15
Kırpma Normu (l2_norm_clip)	1
Gürültü Parametresi (noise_multiplier)	0.1
Epoch	50
Batch_size	8

Tez çalışması kapsamında yapılan iş ve işlemleri gösteren diyagram Şekil 3.1'de verilmiştir. CNN tabanlı sistemde diferansiyel mahremiyet mekanizması eğitim bölümünde devreye girerek gradyanlara gürültü eklenmektedir. Gürültü eklenmiş verilere göre uygulamanın sonuç değerleri elde edilmektedir. Diferansiyel mahremiyetin sürece dâhil edilmesi ile uygulamanın eğitim aşamasında gradyanlara gürültü eklenerek verilerin mahremiyeti sağlanmıştır.

4. BULGULAR VE TARTIŞMA

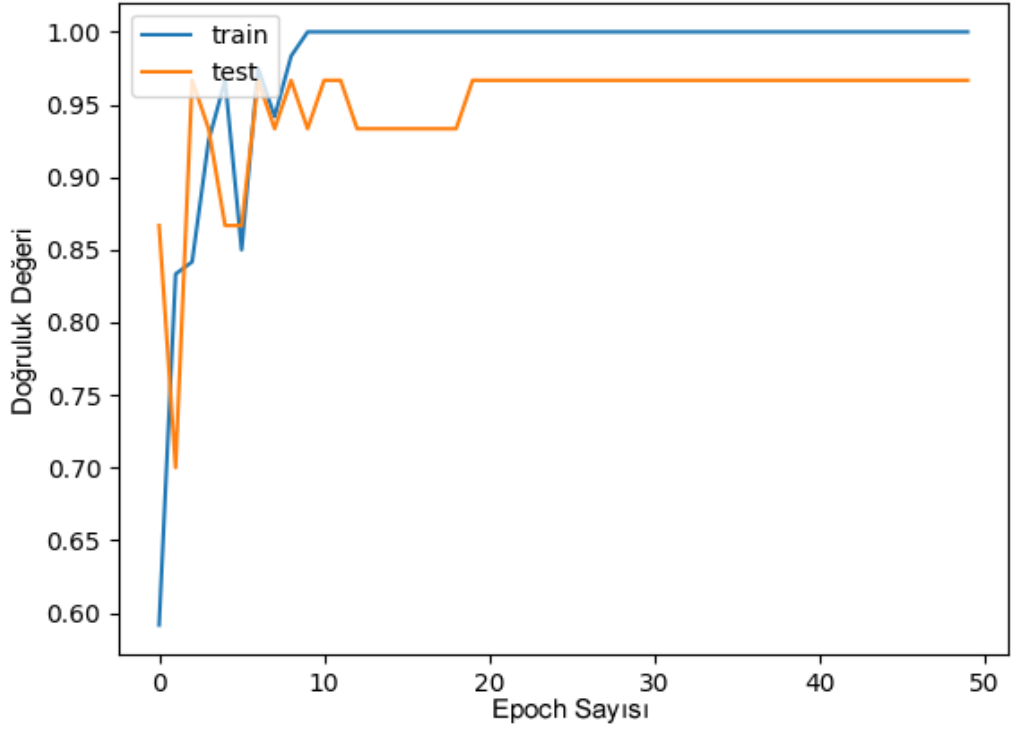
Bu bölümde deneysel çalışmalara ve elde edilen sonuçlara yer verilmiştir. Covid-19 hastalığının teşhisi geleneksel CNN yapısı ve mahremiyet duyarlı CNN yapısı için ayrı ayrı sonuçlar elde edilmiştir. Bu çalışmalar Python programlama dilinin keras ve tensorflow kütüphaneleri kullanılarak gerçekleştirilmiştir.

4.1. Geleneksel Sınıflandırma Sonuçları

Bu deneyde, geleneksel CNN modeli kullanılarak Covid-19 hastalık tespiti 5 farklı veri kümesi için gerçekleştirilmiştir. Her bir veri kümesi için elde edilen sonuçlar epoch=50 ve batch_size=8 için ayrı ayrı olarak Tablo 4.1, 4.2, 4.3, 4.4 ve 4.5'te verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.1, 4.2, 4.3, 4.4 ve 4.5'te sunulmuştur.

Tablo 4.1 DS1 veri kümesine ait sınıflandırma sonuçları

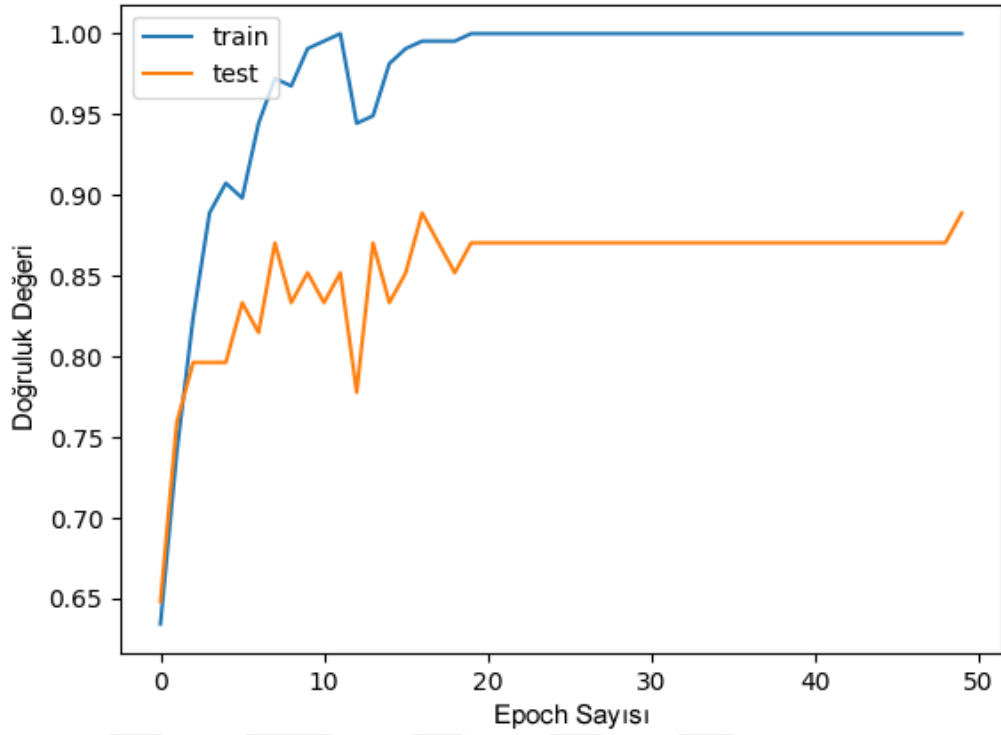
Normal Sınıflandırma (TRAIN)						
Epoch	Batch_Size	Durum	Accuracy	Precision	Recall	F1
50	8	1	1,00	1,00	1,00	1,00
		0		1,00	1,00	1,00
		macro avg		1,00	1,00	1,00
Normal Sınıflandırma (TEST)						
Epoch	Batch_Size	Durum	Accuracy	Precision	Recall	F1
50	8	1	0,97	0,92	1,00	0,96
		0		1,00	0,95	0,97
		macro avg		0,97	0,96	0,97



Şekil 4.1 DS1 veri kümesi için epoch sayısına göre elde edilen doğruluk değerleri grafiği

Tablo 4.2 DS2 veri kümesine ait sınıflandırma sonuçları

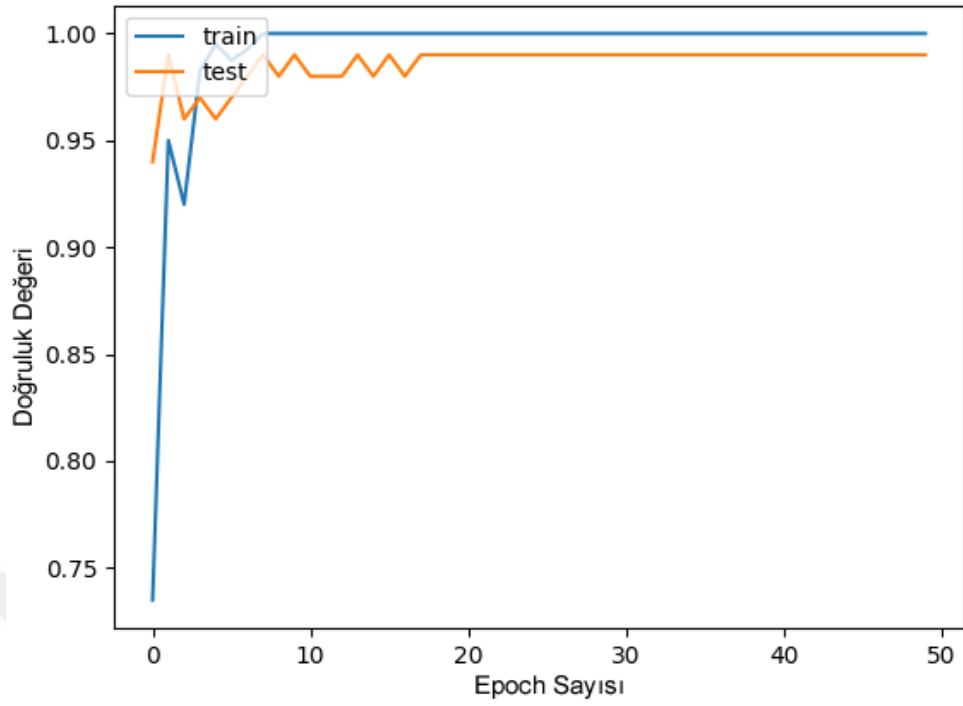
Eğitim Sonuçlar (TRAIN)						
Epoch	Batch_Size	Durum	Accuracy	Precision	Recall	F1
50	8	1	1,00	1,00	1,00	1,00
		0		1,00	1,00	1,00
		macro avg		1,00	1,00	1,00
Test Sonuçları (TEST)						
Epoch	Batch_Size		Accuracy	Precision	Recall	F1
50	8	1	0,89	0,87	0,93	0,90
		0		0,91	0,84	0,87
		macro avg		0,89	0,89	0,89



Şekil 4.2 DS2 veri kümesi için epoch sayısına göre elde edilen doğruluk değerleri grafiği

Tablo 4.3 DS3 veri kümesine ait sınıflandırma sonuçları

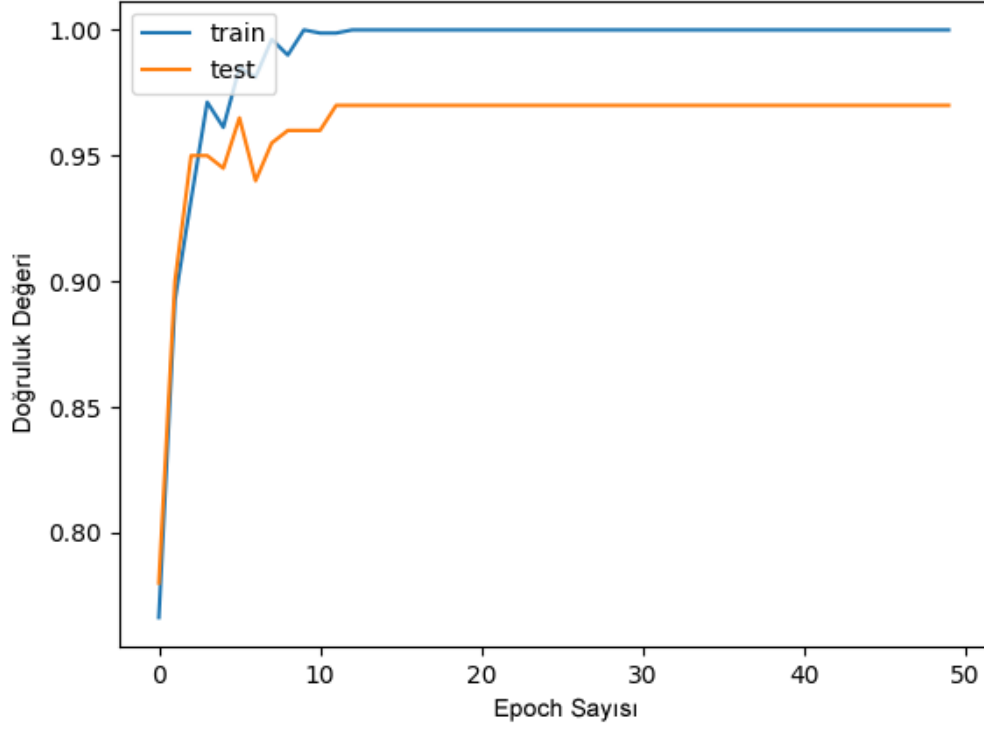
Normal Sınıflandırma (TRAIN)						
Epoch	Batch_Size		Accuracy	Precision	Recall	F1
50	8	1	1,00	1,00	1,00	1,00
		0		1,00	1,00	1,00
		macro avg		1,00	1,00	1,00
Normal Sınıflandırma (TEST)						
Epoch	Batch_Size		Accuracy	Precision	Recall	F1
50	8	1	0,99	1,00	0,98	0,99
		0		0,98	1,00	0,99
		macro avg		0,99	0,99	0,99



Şekil 4.3 DS3 veri kümesi için epoch sayısına göre elde edilen doğruluk değerleri grafiği

Tablo 4.4 DS4 veri kümesine ait sınıflandırma sonuçları

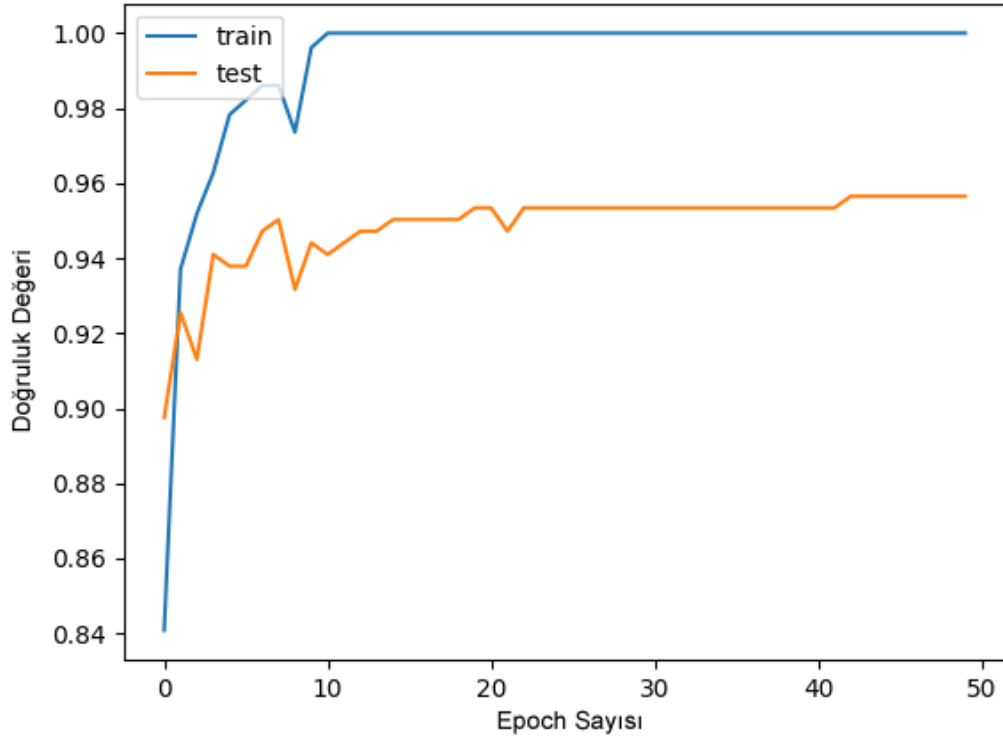
Eğitim Sonuçları (TRAIN)						
Epoch	Batch Size	Değer	Accuracy	Precision	Recall	F1
50	8	1	1,00	1,00	1,00	1,00
		0		1,00	1,00	1,00
		macro avg			1,00	1,00
Test Sonuçları (TEST)						
Epoch	Batch Size	Değer	Accuracy	Precision	Recall	F1
50	8	1	0,97	0,98	0,96	0,97
		0		0,96	0,98	0,97
		macro avg			0,97	0,97



Şekil 4.4 DS4 veri kümesi için epoch sayısına göre elde edilen doğruluk değerleri grafiği

Tablo 4.5 DS5 veri kümesine ait sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)						
Epoch	Batch_Size	Durum	Accuracy	Precision	Recall	F1
50	8	1	1,00	1,00	1,00	1,00
		0		1,00	1,00	1,00
		macro avg			1,00	1,00
Test Sonuçları (TEST)						
Epoch	Batch_Size	Durum	Accuracy	Precision	Recall	F1
50	8	1	0,96	0,95	0,97	0,96
		0		0,97	0,94	0,95
		macro avg			0,96	0,96



Şekil 4.5 DS5 veri kümesi için epoch sayısına göre elde edilen doğruluk değerleri grafiği

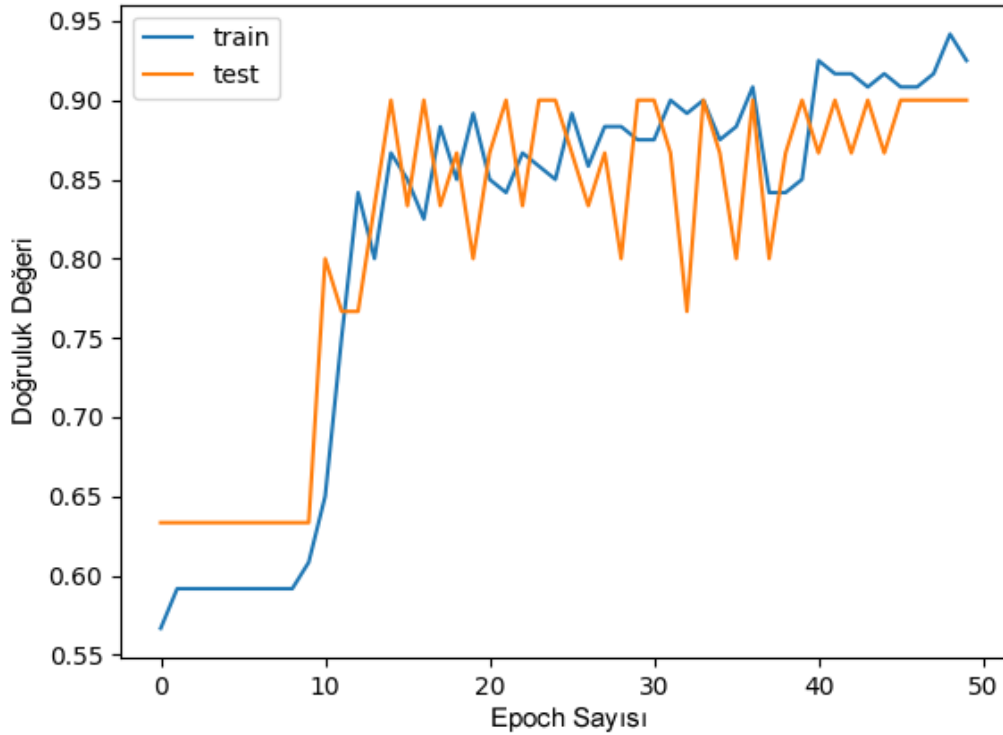
4.2. Mahremiyet Duyarlı Sınıflandırma Sonuçları

Bu deneyde, mahremiyet duyarlı CNN modeli kullanılarak Covid-19 hastalık tespiti 5 farklı veri kümesi için gerçekleştirilmiştir. Her bir veri kümesi için elde edilen sonuçlar epoch=50, batch_size=8 ve $\delta=1e-2$ için hesaplamalar yapılmış ve bu hesaplama sonucunda oluşan değerlere ait tablo ve grafikler aşağıda verilmiştir.

DS1 veri kümesine ait $\delta=1e-2$ olduğu durumda elde edilen değerler Tablo 4.6'da verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.6'da sunulmuştur.

Tablo 4.6 DS1 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Durum	Accuracy	Precision	Recall	F1
50	8	1e-2	22230,93	1	0,92	0,88	0,92	0,90
				0		0,94	0,92	0,93
				macro avg		0,91	0,92	0,91
Test Sonuçları (TEST)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Durum	Accuracy	Precision	Recall	F1
50	8	1e-2	22230,93	1	0,90	0,79	1,00	0,88
				0		1,00	0,84	0,91
				macro avg		0,89	0,92	0,90

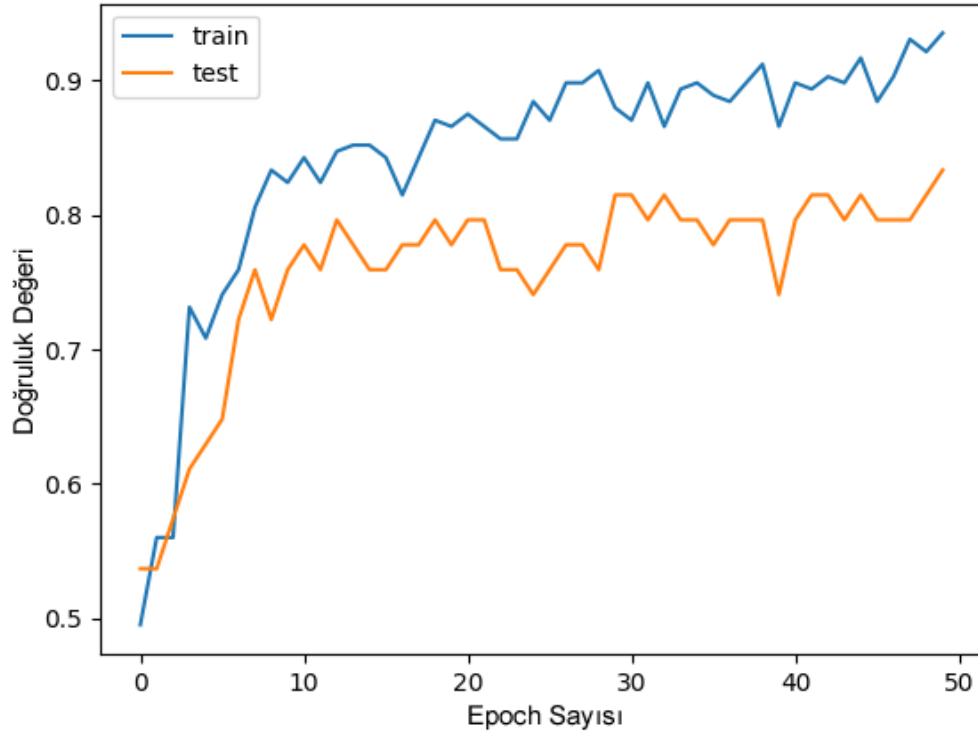


Şekil 4.6 DS1 veri kümesi üzerinde mahremiyet duyarlı sistem için epoch sayısına göre elde edilen doğruluk değerleri grafiği

DS2 veri kümesine ait $\delta=1e-2$ olduğu durumda elde edilen değerler Tablo 4.7’de verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.7’de sunulmuştur.

Tablo 4.7 DS2 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	30456,6	1	0,94	0,93	0,95	0,94
				0		0,94	0,92	0,93
				macro avg		0,94	0,93	0,93
Test Sonuçları (TEST)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	30456,6	1	0,83	0,86	0,83	0,84
				0		0,81	0,84	0,82
				macro avg		0,83	0,83	0,83

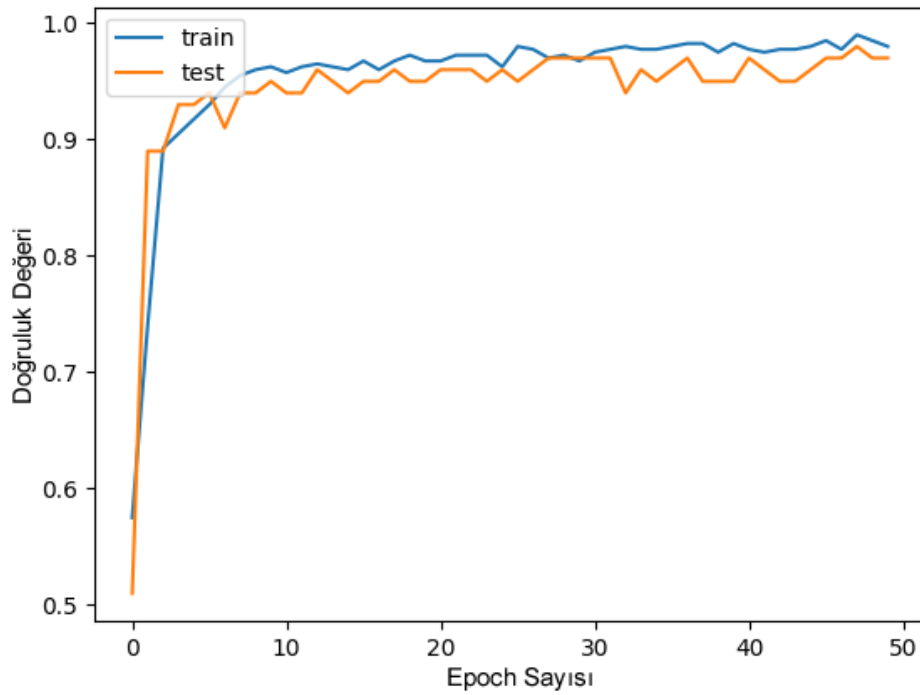


Şekil 4.7 DS2 veri kümesi üzerinde mahremiyet duyarlı sistem için epoch sayısına göre elde edilen doğruluk değerleri grafiği

DS3 veri kümesine ait $\delta=1e-2$ olduğu durumda elde edilen değerler Tablo 4.8’de verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.8’de sunulmuştur.

Tablo 4.8 DS3 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)								
Epoch	Batch_Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	39823,77	1	0,99	0,98	0,99	0,99
				0		1,00	0,99	0,99
				macro avg		0,99	0,99	0,99
Test Sonuçları (TEST)								
Epoch	Batch_Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	39823,77	1	0,97	0,98	0,96	0,97
				0		0,96	0,98	0,97
				macro avg		0,98	0,97	0,96

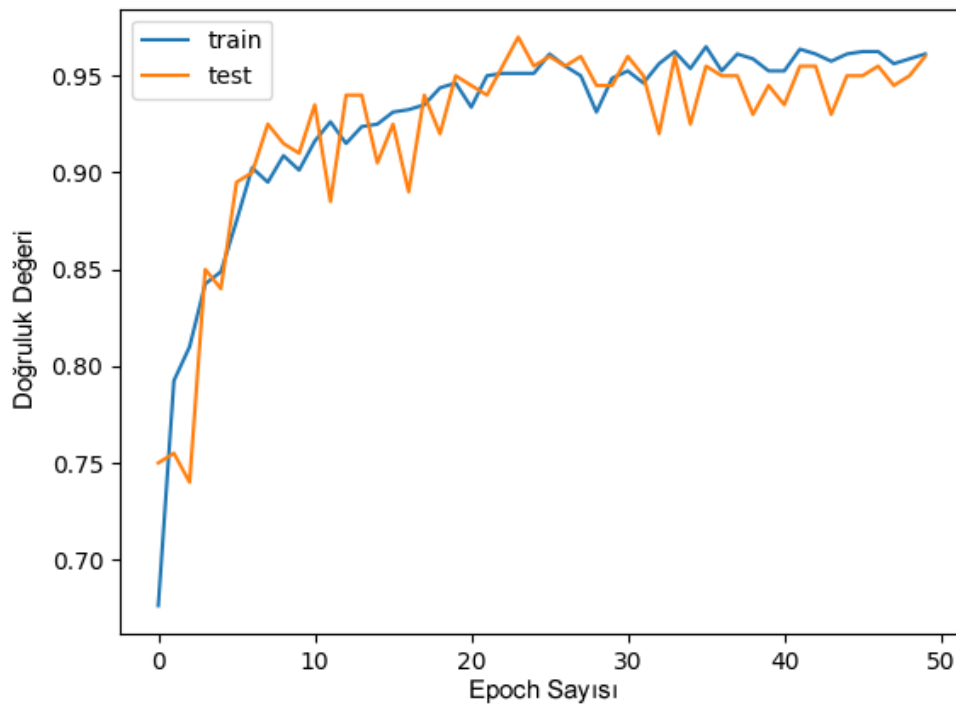


Şekil 4.8 DS3 veri kümesi üzerinde mahremiyet duyarlı sistem için epoch sayısına göre elde edilen doğruluk değerleri grafiği

DS4 veri kümesine ait $\delta=1e-2$ olduğu durumda elde edilen değerler Tablo 4.9' da verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.9'da sunulmuştur.

Tablo 4.9 DS4 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)								
Epoch	Batch_Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	39823,77	1	0,97	0,68	0,96	0,97
				0		0,97	0,98	0,97
				macro avg		0,97	0,97	0,97
Test Sonuçları (TEST)								
Epoch	Batch_Size	Delta	Elde edilen Epsilon	Değer	Accuracy	Precision	Recall	F1
50	8	1e-2	39823,77	1	0,96	0,97	0,95	0,96
				0		0,95	0,97	0,96
				macro avg		0,96	0,96	0,96

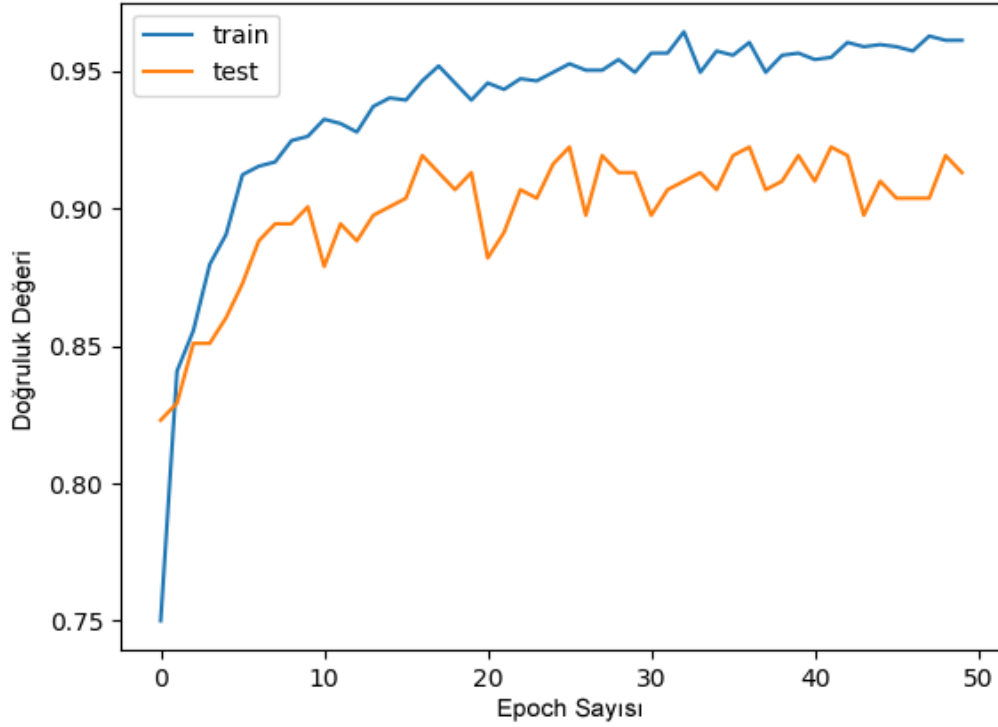


Şekil 4.9 DS4 veri kümesi üzerinde mahremiyet duyarlı sistem için epoch sayısına göre elde edilen doğruluk değerleri grafiği

DS5 veri kümesine ait $\delta=1e-2$ olduğu durumda elde edilen değerler Tablo 4.10'da verilmiştir. Ayrıca bu sonuçlar epoch bazlı grafiksel olarak Şekil 4.10' da sunulmuştur.

Tablo 4.10 DS5 veri kümesine ait mahremiyet duyarlı sınıflandırma sonuçları

Eğitim Sonuçları (TRAIN)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Durum	Accuracy	Precision	Recall	F1
50	8	1e-2	54017,11	1	0,95	1,00	0,91	0,95
				0		0,89	0,99	0,94
				macro avg		0,94	0,95	0,95
Test Sonuçları (TEST)								
Epoch	Batch Size	Delta	Elde edilen Epsilon	Durum	Accuracy	Precision	Recall	F1
50	8	1e-2	54017,11	1	0,91	0,96	0,87	0,91
				0		0,87	0,96	0,92
				macro avg		0,92	0,91	0,91



Şekil 4.10 DS5 veri kümesi üzerinde mahremiyet duyarlı sistem için epoch sayısına göre elde edilen doğruluk değerleri grafiği

5. SONUÇ VE ÖNERİLER

Literatürde derin öğrenme yaklaşımları kullanılarak hastalık teşhisi, yaygın bir şekilde kullanılmakta olup bu alandaki araştırmaların ve çalışmaların sayısı gün geçtikçe artmaya devam etmektedir. Bu çalışmalarda çoğunlukla CNN mimarisinin kullanıldığı görülmüştür. CNN mimarisinin kullanılma sebebi görüntünün işlenmesi sürecinde, görüntüden istenilen özniteliklerin çıkarılması ve bu özniteliklere göre sınıflandırma işlemi yapıldığında CNN mimarisinin diğer mimarilerden daha yüksek başarı oranı elde etmesidir.

Bu tez çalışmasında öncelikle bu alanda yapılan çalışmalar ile ilgili literatür taraması yapılmış ve bu çalışmalar ile ilgili özet bilgiler bir arada derlenerek verilmiştir. Çalışma kapsamında hem Covid-19 hastalığının teşhisi gerçekleştirilmiş hem de veri mahremiyeti sağlanmıştır. Çalışmamızda farklı δ değerleri verilerek en iyi başarı oranı elde edilmeye çalışılmış ve yapılan deneylerde tüm veri setleri için en yüksek başarı oranı $\delta=1e-2$ olduğu durumda elde edilmiştir. Bu δ değerine göre deney sonucunda ε değeri elde edilmiştir. Çalışmamızda en yüksek başarı oranı 500 CXR görüntüsünden oluşan DS3 veri kümesi kullanılarak $\varepsilon=39823,77$ ve %97 başarı oranı elde edilmiştir.

Çalışma kapsamında beş ayrı veri kümesi kullanılarak geliştirilen mahremiyet duyarlı sistem test edilmiş ve deneysel sonuçlar elde edilmiştir. Her veri kümesi için ayrı ayrı doğruluk, f1-score ve hassasiyet değerleri elde edilmiştir. Mahremiyet duyarlı yapay zekâ sisteminin tüm deneylerde en yüksek DS1 için %90, DS2 için %83, DS3 için %97 ve DS4 için %96 ve DS5 için %91 başarı verdiği görülmüştür. Bu çalışma kapsamında farklı veri kümeleri için bile geliştirilen sistemin yüksek başarı verdiği görülmüştür. Ayrıca literatürdeki mahremiyet duyarlı benzer çalışmalara bakıldığından %70 gibi bir başarı oranının elde edildiği görülmektedir. Ancak bu tez kapsamında geliştirilen sistem başarı oranının en düşük %83 en yüksek ise %97 olduğu görülmektedir. İleriki çalışmalarda farklı ön işlem adımlarının uygulanarak sistemin başarısının artırılması, açıklanabilir yapay zekâ ile mahremiyet duyarlı hastalık tespiti gibi çalışmalar yapılması planlanmaktadır.

KAYNAKLAR

- Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., ve Zhang, L. (2016). *Deep Learning With Differential Privacy*. Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.
- Abbas, A., Abdelsamea, M. M., ve Gaber, M. M. (2021). Classification of COVID-19 in chest X-ray images using DeTraC deep convolutional neural network. *Applied Intelligence*, 51(2), 854-864.
- Abbasi-Oshaghi, E., Mirzaei, F., Farahani, F., Khodadadi, I., ve Tayebinia, H. (2020). Diagnosis and treatment of coronavirus disease 2019 (COVID-19): Laboratory, PCR, and chest CT imaging findings. *International Journal of Surgery*, 79, 143-153.
- Agarwal, N., Suresh, A. T., Yu, F. X. X., Kumar, S., ve McMahan, B. (2018). cpSGD: Communication-efficient and differentially-private distributed SGD. *Advances in Neural Information Processing Systems*, 31.
- Aghdam, O. A., Bozorgtabar, B., Ekenel, H. K., ve Thiran, J.-P. (2019). *Exploring Factors for Improving Low Resolution Face Recognition*. Paper presented at the CVPR Workshops.
- Akar, H., ve Akar, F. (2021). Sosyal Medyada Mahremiyet Algısı: Üniversite Öğrencileri Araştırması. *İnönü Üniversitesi İletişim Fakültesi Elektronik Dergisi (İNİF E-Dergi)*, 6(1), 285-297.
- Akkaya, Ş. (2021). *Derin Öğrenme Yöntemi İle Diferansiyel Mahremiyetli Medikal Görüntü Sınıflandırma*. Gazi Üniversitesi,
- Alafi, B. (2019). Artificial Intelligence And Deep Learning Methodologies. *The Journal of Cognitive Systems*, 4(2), 57-61.
- Alamo, T., Reina, D. G., Mammarella, M., ve Abella, A. (2020). Covid-19: Open-data resources for monitoring, modeling, and forecasting the epidemic. *Electronics*, 9(5), 827.
- Albert Sun, N. (2020, Erişim Tarihi: 05.12.2020). NY-Times Covid-19 USA Dataset. İnternet Sayfası: <https://github.com/nytimes/covid-19-data>
- Ali, A. (2019, Erişim Tarihi: 16.08.2022). Pneumonia sample XRays. İnternet Sayfası: <https://www.kaggle.com/datasets/ahmedali2019/pneumonia-sample-xrays>
- Alkan, O. (2019). *Parkinson Hastalığının Teşhisinde Derin Öğrenme Yöntemi İle Spect Görüntü Analizi*. (Yüksek Lisans Tezi), Ağrı İbrahim Çeçen Üniversitesi, Fen Bilimleri Enstitüsü,
- Alpaydın, E. (2013). *Yapay Öğrenme*: İstanbul: Boğaziçi Üniversitesi Yayınevi.

- Apostolopoulos, I. D., ve Mpesiana, T. A. (2020). Covid-19: Automatic detection from X-ray images utilizing transfer learning with convolutional neural networks. *Physical and Engineering Sciences in Medicine*, 43(2), 635-640.
- Aslan, Z. (2019). On the use of deep learning methods on medical images. *The International Journal of Energy and Engineering Sciences*, 3(2), 1-15.
- Aydoğan, M., ve Karci, A. (2020). Spelling Correction with the Dictionary Method for the Turkish Language Using Word Embeddings. *Avrupa Bilim ve Teknoloji Dergisi*, 57-63.
- Badr, H. S. (2020, Erişim Tarihi: 04.12.2020). Covid-19 Unified-Dataset. İnternet Sayfası: https://github.com/CSSEGISandData/COVID-19_Unified-Dataset
- Beaulieu-Jones, B. K., Wu, Z. S., Williams, C., Lee, R., Bhavnani, S. P., Byrd, J. B., ve Greene, C. S. (2019). Privacy-preserving generative deep neural networks support clinical data sharing. *Circulation: Cardiovascular Quality and Outcomes*, 12(7), e005122.
- Beimel, A., Nissim, K., ve Stemmer, U. (2013). Private Learning And Sanitization: Pure vs. Approximate Differential Privacy. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques* (pp. 363-378): Springer.
- Britz, D. (2015, Erişim Tarihi: 28.12.2020). Recurrent Neural Networks Tutorial, Part 1 – Introduction To RNNs. İnternet Sayfası: <http://www.wildml.com/2015/09/recurrent-neural-networks-tutorial-part-1-introduction-to-rnns/>
- Buonsenso, D., Piano, A., Raffaelli, F., Bonadia, N., Donati, K. D. G., ve Franceschi, F. (2020). Novel coronavirus disease-19 pnemoniae: a case report and potential applications during COVID-19 outbreak. *Eur Rev Med Pharmacol Sci*, 24(5), 2776-2780.
- Canbay, P. (2020). Sağlıkta Yapay Zekâ: Derin Öğrenme Teknikleri ve Uygulamaları. In K. D. Ahmet Rıza Şahin, Süleyman Sivri (Ed.), *Sağlık Bilimlerinde Yapay Zekâ* (pp. 25-39): Akademisyen Kitabevi.
- Canbay, Y. (2019). Aykırı veri yönelimli fayda temelli büyük veri anonimleştirme modeli. *Mühendislik Mimarlık Fakültesi Dergisi*, 35(1), 355-368.
- Canbay, Y., İsmetoğlu, A., ve Canbay, P. (2021). Covid-19 Hastalığının Teşhisinde Derin Öğrenme ve Veri Mahremiyeti. *Mühendislik Bilimleri ve Tasarım Dergisi*, 9(2), 701-715.
- Canbay, Y., ve Sağiroğlu, Ş. (2020). Derin Öğrenmede Diferansiyel Mahremiyet. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 6(1), 1-16.
- Canbay, Y., Vural, Y., ve Sağiroğlu, Ş. (2020). Mahremiyet Korumalı Büyük Veri Yayınlama İçin Kavramsal Model Önerileri. *Politeknik Dergisi*, 23(3), 785-798.
- Carpenter, K. A., Cohen, D. S., Jarrell, J. T., ve Huang, X. (2018). Deep learning and virtual drug screening. *Future medicinal chemistry*, 10(21), 2557-2567.

- Charniak, E., ve McDermott, D. (1985). *Introduction to Artificial Intelligence*. Boston: Addison-Wesley Pub.Company.
- Chase, M., Gilad-Bachrach, R., Laine, K., Lauter, K., ve Rindal, P. (2017). Private collaborative neural network learning. *Cryptology ePrint Archive*.
- Chaudhuri, K., Monteleoni, C., ve Sarwate, A. D. (2011). Differentially private empirical risk minimization. *Journal of Machine Learning Research*, 12(3).
- Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2), 84-90.
- Chhikara, P., Singh, P., Gupta, P., ve Bhatia, T. (2020). Deep convolutional neural network with transfer learning for detecting pneumonia on chest X-rays. In *Advances in Bioinformatics, Multimedia, and Electronics Circuits and Signals* (pp. 155-168): Springer.
- Chowdhury, M. E., Rahman, T., Khandakar, A., Mazhar, R., Kadir, M. A., Mahbub, Z. B., . . . Al Emadi, N. (2020). Can AI help in screening viral and COVID-19 pneumonia? *IEEE Access*, 8, 132665-132676.
- Chung, A. G. (2020, Eriřim Tarihi: 04.02.2022). Actualmed Covid-19 Chest X-ray Dataset Initiative. İnternet Sayfası: <https://github.com/agchung/Actualmed-COVID-chestxray-dataset>
- Chung, A. G. (2020, Eriřim Tarihi: 20.12.2020). Figure1-Covid-Chestxray-Dataset. İnternet Sayfası: <https://github.com/agchung/Figure1-COVID-chestxray-dataset>
- Ciotti, M., Ciccozzi, M., Terrinoni, A., Jiang, W.-C., Wang, C.-B., ve Bernardini, S. (2020). The COVID-19 pandemic. *Critical reviews in clinical laboratory sciences*, 57(6), 365-388.
- Ciresan, D. C., Meier, U., Gambardella, L. M., ve Schmidhuber, J. (2010). Deep, big, simple neural nets for handwritten digit recognition. *Neural computation*, 22(12), 3207-3220.
- Cohen, J. P. (2020, Eriřim Tarihi: 05.12.2020). IEEE8023 Covid-19 Chest X-ray. İnternet Sayfası: <https://github.com/ieee8023/covid-chestxray-dataset>
- Dandıl, E., ve Serin, Z. (2020). Derin Sinir Ağları Kullanarak Histopatolojik Görüntülerde Meme Kanseri Tespiti. *Avrupa Bilim ve Teknoloji Dergisi*, 451-463.
- Dař, R., Polat, B., ve Tuna, G. (2019). Derin öğrenme ile resim ve videolarda nesnelerin tanınması ve takibi. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 31(2), 571-581.
- Data4u, E. (2020, Eriřim Tarihi: 04.02.2022). Diagnosis of Covid-19 and its clinical spectrum. İnternet Sayfası: <https://www.kaggle.com/einsteindata4u/covid19>
- Data, M. (2018, erişim Tarihi: 07.07.2022). Labeled Optical Coherence Tomography (OCT) and Chest X-Ray Images for Classification. İnternet Sayfası: <https://data.mendeley.com/datasets/rscbjbr9sj/2>

- Di Pietro, G., Biagi, F., Costa, P., Karpiński, Z., ve Mazza, J. (2020). *The likely impact of COVID-19 on education: Reflections based on the existing literature and recent international datasets* (Vol. 30275): Publications Office of the European Union.
- Doğan, F., ve Türkoğlu, İ. (2019). Derin Öğrenme Modelleri ve Uygulama Alanlarına İlişkin Bir Derleme. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 10(2), 409-445.
- Du, J., Li, S., Feng, M., ve Chen, S. (2021). Dynamic differential-privacy preserving sg. *arXiv preprint arXiv:2111.00173*.
- Dwork, C. (2006). *Differential Privacy*. Paper presented at the International Colloquium on Automata, Languages and Programming, Berlin, Heidelberg.
- Dwork, C., Kenthapadi, K., McSherry, F., Mironov, I., ve Naor, M. (2006). *Our Data, Ourselves: Privacy Via Distributed Noise Generation*. Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques.
- Dwork, C., ve Roth, A. (2014). The Algorithmic Foundations Of Differential Privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4), 211-407.
- Eker, A. G., ve Nevcihan, D. (2021). Medikal Görüntü İşlemede Derin Öğrenme Uygulamaları. *Acta Infologica*, 5(2), 459-474.
- Elmas, Ç., ve Babayev, J. (2021). Artificial Intelligence Techniques Used in Project Management. *Advances in Artificial Intelligence Research*, 1(1), 1-5.
- Farooq, M., ve Hafeez, A. (2020). Covid-Resnet: A deep Learning Framework For Screening Of Covid19 From Radiographs. *arXiv preprint arXiv:2003.14395*.
- Fredrikson, M., Jha, S., ve Ristenpart, T. (2015). *Model inversion attacks that exploit confidence information and basic countermeasures*. Paper presented at the Proceedings of the 22nd ACM SIGSAC conference on computer and communications security.
- Fredrikson, M., Lantz, E., Jha, S., Lin, S., Page, D., ve Ristenpart, T. (2014). *Privacy in Pharmacogenetics: An {End-to-End} Case Study of Personalized Warfarin Dosing*. Paper presented at the 23rd USENIX Security Symposium (USENIX Security 14).
- Fung, B. C., Wang, K., Chen, R., ve Yu, P. S. (2010). Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (Csur)*, 42(4), 1-53.
- Geambasu, R., Kohno, T., Levy, A. A., ve Levy, H. M. (2009). *Vanish: Increasing Data Privacy with Self-Destructing Data*. Paper presented at the USENIX security symposium.
- Geng, Q., ve Viswanath, P. (2014). *The optimal mechanism in differential privacy*. Paper presented at the 2014 IEEE international symposium on information theory.
- Ghoshal, B., ve Tucker, A. (2020). Estimating uncertainty and interpretability in deep learning for coronavirus (COVID-19) detection. *arXiv preprint arXiv:2003.10769*.

- Gianfrancesco, M. A., Hyrich, K. L., Gossec, L., Strangfeld, A., Carmona, L., Mateus, E. F., . . . Bhana, S. (2020). Rheumatic disease and COVID-19: initial data from the COVID-19 global rheumatology alliance provider registries. *The Lancet Rheumatology*, 2(5), e250-e253.
- Goldbloom, A. (2020, Erişim Tarihi: 20.12.2020). Covid-19 Data From John Hopkins University Dataset. İnternet Sayfası: <https://www.kaggle.com/antgoldbloom/covid19-data-from-john-hopkins-university>
- Gong, M., Feng, J., ve Xie, Y. (2020). Privacy-enhanced multi-party deep learning. *Neural Networks*, 121, 484-496.
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., . . . Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27.
- Graves, A. (2013). Generating sequences with recurrent neural networks. *arXiv preprint arXiv:1308.0850*.
- Gunduz, H. (2021). An efficient stock market prediction model using hybrid feature reduction method based on variational autoencoders and recursive feature elimination. *Financial Innovation*, 7(1), 1-24.
- Gurari, D. (2021, Erişim Tarihi: 03.08.2022). Recurrent Neural Networks. İnternet Sayfası: https://home.cs.colorado.edu/~DrG/Courses/IntroToMachineLearning/Lectures/10_RecurrentNeuralNetworks.pdf
- Ha, T., Dang, T. K., Dang, T. T., Truong, T. A., ve Nguyen, M. T. (2019). *Differential privacy in deep learning: an overview*. Paper presented at the 2019 International Conference on Advanced Computing and Applications (ACOMP).
- Ha, T., Dang, T. K., Le, H., ve Truong, T. A. (2020). Security and privacy issues in deep learning: a brief review. *SN Computer Science*, 1(5), 1-15.
- Hao, X., Zhang, G., ve Ma, S. (2016). Deep learning. *International Journal of Semantic Computing*, 10(03), 417-439.
- Hemdan, E. E.-D., Shouman, M. A., ve Karar, M. E. (2020). Covidx-Net: A Framework Of Deep Learning Classifiers To Diagnose Covid-19 In X-Ray Images. *arXiv preprint arXiv:2003.11055*.
- Hinton, G., Deng, L., Yu, D., Dahl, G. E., Mohamed, A.-r., Jaitly, N., . . . Sainath, T. N. (2012). Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. *IEEE Signal processing magazine*, 29(6), 82-97.
- Hochreiter, S., ve Schmidhuber, J. (1997). Long Short-Term Memory. *Neural computation*, 9(8), 1735-1780.
- Horry, M. J., Chakraborty, S., Paul, M., Ulhaq, A., Pradhan, B., Saha, M., ve Shukla, N. (2020). COVID-19 detection through transfer learning using multimodal imaging data. *IEEE Access*, 8, 149808-149824.

- Hu, R. (2020, erişim Tarihi: 04.02.2022). Covid-19 Dataset. İnternet Sayfası: <https://github.com/RunwenHu/COVID-19>
- Hu, R., Ruan, G., Xiang, S., Huang, M., Liang, Q., ve Li, J. (2020). Automated diagnosis of covid-19 using deep learning and data augmentation on chest ct. *MedRxiv*.
- Huang, Z., Xu, W., ve Yu, K. (2015). Bidirectional LSTM-CRF models for sequence tagging. *arXiv preprint arXiv:1508.01991*.
- Institute, A. (2020, Erişim Tarihi: 05.12.2020). Covid-19 Open Research Dataset Challenge (CORD-19). İnternet Sayfası: <https://www.kaggle.com/allen-institute-for-ai/CORD-19-research-challenge?select=metadata.csv>
- Jain, P., Gyanchandani, M., ve Khare, N. (2016). Big Data Privacy: A Technological Perspective And Review. *Journal of Big Data*, 3(1), 25.
- Javaheri, T., Homayounfar, M., Amoozgar, Z., Reiazi, R., Homayounieh, F., Abbas, E., . . . Mousavi, S. A. J. (2020). Covidctnet: An open-source deep learning approach to identify covid-19 using ct image. *arXiv preprint arXiv:2005.03059*.
- Jayaraman, B., Wang, L., Evans, D., ve Gu, Q. (2018). Distributed learning without distress: Privacy-preserving empirical risk minimization. *Advances in Neural Information Processing Systems*, 31.
- Kaggle. (2020, Erişim Tarihi: 08.07.2022). SARS-COV-2 Ct-Scan Dataset. İnternet Sayfası: <https://www.kaggle.com/datasets/plameneduardo/sarscov2-ctscan-dataset>
- Kara, A. (2019). Uzun-Kısa Süreli Bellek Ağı Kullanarak Global Güneş Işınımı Zaman Serileri Tahmini. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 7(4), 882-892.
- Karim, F., Majumdar, S., Darabi, H., ve Harford, S. (2019). Multivariate LSTM-FCNs for time series classification. *Neural Networks*, 116, 237-245.
- Kerr, G. H., Badr, H. S., Gardner, L. M., Perez-Saez, J., ve Zaitchik, B. F. (2021). Associations between meteorology and COVID-19 in early studies: Inconsistencies, uncertainties, and recommendations. *One Health*, 12, 100225.
- Kifer, D., ve Machanavajjhala, A. (2011). *No free lunch in data privacy*. Paper presented at the Proceedings of the 2011 ACM SIGMOD International Conference on Management of data.
- Kimanuka, U. A., ve Büyük, O. (2018). Turkish Speech Recognition Based On Deep Neural Networks. *Journal of Natural ve Applied Sciences*.
- Ko, H., Chung, H., Kang, W. S., Kim, K. W., Shin, Y., Kang, S. J., . . . Jung, H. (2020). Covid-19 pneumonia Diagnosis Using A Simple 2D Deep Learning Framework With A Single Chest CT Image: Model Development And Validation. *Journal of Medical Internet Research*, 22(6), e19569.
- Kobayashi, G., Sugawara, S., Tamae, H., ve Ozu, T. (2020). Predicting intervention effect for COVID-19 in Japan: state space modeling approach. *BioScience Trends*.

- Konečný, J., McMahan, B., ve Ramage, D. (2015). Federated optimization: Distributed optimization beyond the datacenter. *arXiv preprint arXiv:1511.03575*.
- Kurt, F. (2018). *Analysis Of The Effects Of Hyperparameters In Convolutional Neural Networks*. (Yüksek Lisans Tezi), Hacettepe Üniversitesi,
- KVKK, (2020, Erişim Tarihi: 23.11.2020). Kamuoyu Duyurusu (Covid-19 İle Mücadelede Konum Verisinin İşlenmesi ve Kişilerin Hareketliliklerinin İzlenmesi Hakkında Bilinmesi Gerekenler). İnternet Sayfası: <https://www.kvkk.gov.tr/Icerik/6726/COVID-19-ILE-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2->
- KVKK, (2021). Kişisel Verilerin Korunması Kanunu ve Uygulaması. *Ankara: Kişisel Verileri Koruma Kurumu*.
- Larxel. (2020, Erişim Tarihi: 04.02.2022). Covid-19 X rays. İnternet Sayfası: <https://www.kaggle.com/andrewmvd/convid19-X-rays>
- Latifoğlu, L., ve Nuralan, K. B. (2020). Tekil Spektrum Analizi ve Uzun-Kısa Süreli Bellek Ağları ile Nehir Akım Tahmini. *Avrupa Bilim ve Teknoloji Dergisi*, 376-381.
- Lecun, Y., Bottou, L., Bengio, Y., ve Haffner, P. (1998). Gradient-Based Learning Applied To Document Recognition. *Proceedings of the IEEE*, 86(11), 2278-2324.
- Levitt, M., Scaiewicz, A., ve Zonta, F. (2020). Predicting the trajectory of any COVID19 epidemic from the best straight line. *MedRxiv*.
- Li, N., Li, T., ve Venkatasubramanian, S. (2007). *t-Closeness: Privacy Beyond k-Anonymity And l-Diversity*. Paper presented at the 2007 IEEE 23rd International Conference on Data Engineering.
- Lira, C. (2020, Erişim Tarihi: 05.12.2020). Covid-19 Mexico Dataset. İnternet Sayfası: <https://www.kaggle.com/carloslira/covid19-mexico>
- Lisphilar. (2020, Erişim Tarihi: 10.12.2020). Covid-19 Dataset In Japan. İnternet Sayfası: <https://www.kaggle.com/lisphilar/covid19-dataset-in-japan>
- Liu, B., Yan, B., Zhou, Y., Yang, Y., ve Zhang, Y. (2020). Experiments of federated learning for covid-19 chest x-ray images. *arXiv preprint arXiv:2007.05592*.
- Liu, X., Xie, L., Wang, Y., Zou, J., Xiong, J., Ying, Z., ve Vasilakos, A. V. (2020). Privacy and security issues in deep learning: A survey. *IEEE Access*, 9, 4566-4593.
- Loey, M., Smarandache, F., ve Khalifa, N. E. M. (2020). Within the lack of COVID-19 benchmark dataset: a novel gan with deep transfer learning for corona-virus detection in chest x-ray images. *Symmetry*, 12(4), 1-19.
- Loey, M., Smarandache, F., ve M Khalifa, N. E. (2020). Within the lack of chest COVID-19 X-ray dataset: a novel detection model based on GAN and deep transfer learning. *Symmetry*, 12(4), 651.

- Long, C., Xu, H., Shen, Q., Zhang, X., Fan, B., Wang, C., . . . Li, H. (2020). Diagnosis of the Coronavirus disease (Covid-19): rRT-PCR or CT? *European journal of radiology*, 126, 108961.
- Luo, Y., Shao, Y., Chu, H., Wu, B., Huang, M., ve Rao, Y. (2020). *CNN-based blade tip vortex region detection in flow field*. Paper presented at the Eleventh International Conference on Graphics and Image Processing (ICGIP 2019).
- Machanavajjhala, A., Kifer, D., Gehrke, J., ve Venkitasubramaniam, M. (2007). 1-Diversity: Privacy Beyond k-Anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1), 3-es.
- Maghdid, H. S., Asaad, A. T., Ghafoor, K. Z., Sadiq, A. S., Mirjalili, S., ve Khan, M. K. (2021). *Diagnosing COVID-19 pneumonia from X-ray and CT images using deep learning and transfer learning algorithms*. Paper presented at the Multimodal Image Exploitation and Learning 2021.
- Manuel Filho, E., Neto, E. R. D., ve Machado, J. C. (2021). Privacy-preserving of patients with Differential Privacy: an experimental evaluation in Covid-19 dataset. *Journal of Information and Data Management*, 12(5).
- Mathworks. (2022, 05.01.2022). Introducing Deep Learning with MATLAB. İnternet Sayfası: <https://www.mathworks.com/campaigns/offers/next/deep-learning-ebook.html#3>
- Mavragani, A. (2020). Tracking COVID-19 in Europe: infodemiology approach. *JMIR public health and surveillance*, 6(2), e18941.
- Medel-Ramírez, C., ve Medel-Lopez, H. (2020). Data Mining for the Study of the Epidemic (SARS-CoV-2) COVID-19: Algorithm for the Identification of Patients (SARS-CoV-2) COVID 19 in Mexico. *Available at SSRN 3619549*.
- Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G., ve Guo, S. (2016). Protection of big data privacy. *IEEE Access*, 4, 1821-1834.
- Metin, İ. A., ve Karasulu, B. (2015). İnsan Aktivitelerinin Sınıflandırılmasında Tekrarlayan Sinir Ağı Kullanan Derin Öğrenme Tabanlı Yaklaşım. *Veri Bilimi*, 2(2), 1-10.
- Minaee, S., Kafieh, R., Sonka, M., Yazdani, S., ve Soufi, G. J. (2020). Deep-Covid: Predicting Covid-19 From Chest X-Ray Images Using Deep Transfer Learning. *arXiv preprint arXiv:2004.09363*.
- Mireshghallah, F., Taram, M., Vepakomma, P., Singh, A., Raskar, R., ve Esmailzadeh, H. (2020). Privacy in deep learning: A survey. *arXiv preprint arXiv:2004.12254*.
- Mondal, M. R. H., Bharati, S., Podder, P., ve Podder, P. (2020). Data analytics for novel coronavirus disease. *Informatics in Medicine Unlocked*, 20, 100374.
- Mooney, P. (2020a, Erişim Tarihi: 08.12.2020). Kaggle, Pneumonia Sample X-Rays. İnternet Sayfası: <https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia>

- Mooney, P. (2020b, Eriřim Tarihi: 06.12.2020). San Francisco Covid-19 Data. İnternet Sayfası: <https://www.kaggle.com/paultimothymooney/san-francisco-covid19-data>
- Muhammad, G., ve Hossain, M. S. (2021). A Deep-Learning-Based Edge-Centric COVID-19-Like Pandemic Screening and Diagnosis System within a B5G Framework Using Blockchain. *IEEE Network*, 35(2), 74-81.
- Müftüoğlu, Z., Kizrak, M. A., ve Yıldırım, T. (2020). *Differential Privacy Practice On Diagnosis of Covid-19 Radiology Imaging Using EfficientNet*. Paper presented at the 2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA).
- Narin, A., Kaya, C., ve Pamuk, Z. (2020). Automatic Detection Of Coronavirus Disease (Covid-19) Using X-Ray Images And Deep Convolutional Neural Networks. *arXiv preprint arXiv:2003.10849*.
- Nozari, E., Tallapragada, P., ve Cortés, J. (2016). *Differentially private distributed convex optimization via objective perturbation*. Paper presented at the 2016 American Control Conference (ACC).
- O'Shea, K., ve Nash, R. (2015). An Introduction To Convolutional Neukral Networks. *arXiv preprint arXiv:1511.08458*.
- Olah, C. (2015, Eriřim Tarihi: 06.12.2020). Understanding LSTM Networks. İnternet Sayfası: <http://colah.github.io/posts/2015-08-Understanding-LSTMs>
- Ozturk, T., Talo, M., Yildirim, E. A., Baloglu, U. B., Yildirim, O., ve Acharya, U. R. (2020). Automated detection of COVID-19 cases using deep neural networks with X-ray images. *Computers in Biology and Medicine*, 121, 103792.
- Parmaar, N. R. (2020, Eriřim Tarihi: 29.02.2022). Differential Privacy in Deep Learning. İnternet Sayfası: <https://towardsdatascience.com/differential-privacy-in-deep-learning-cf9cc3591d28>
- Pascanu, R., Mikolov, T., ve Bengio, Y. (2013). *On the difficulty of training recurrent neural networks*. Paper presented at the International conference on machine learning.
- Pengtao Xie, J. S., Jinyu Zhao. (2020, Eriřim Tarihi: 28.11.2020). GitHub UCSD-AI4H / Covid-CT. İnternet Sayfası: <https://github.com/UCSD-AI4H/COVID-CT>
- Pervan, N., ve Keleş, Y. (2019). Derin öğrenme yaklaşımları kullanarak Türkçe metinlerden anlamsal çıkarım yapma. *Ankara Üniversitesi, Ankara, Türkiye*.
- Prakash, K. B., Imambi, S. S., Ismail, M., Kumar, T. P., ve Pawan, Y. (2020). Analysis, prediction and evaluation of covid-19 datasets using machine learning algorithms. *International Journal*, 8(5).
- Rabbah, J., Ridouani, M., ve Hassouni, L. (2020). *A New Classification Model Based on Stacknet and Deep Learning for Fast Detection of COVID 19 Through X Rays Images*. Paper presented at the 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS).

- Rajkumar, S. (2020a, Eriřim Tarihi: 20.12.2020). Covid-19 India Dataset. İnternet Sayfası: <https://www.kaggle.com/sudalairajkumar/covid19-in-india>
- Rajkumar, S. (2020b, Eriřim Tarihi: 05.12.2020). Novel Coronavirus 2019 Dataset. İnternet Sayfası: <https://www.kaggle.com/sudalairajkumar/novel-corona-virus-2019-dataset>
- Ravi, D., Wong, C., Deligianni, F., Berthelot, M., Andreu-Perez, J., Lo, B., ve Yang, G.-Z. (2016). Deep learning for health informatics. *IEEE journal of biomedical and health informatics*, 21(1), 4-21.
- Rebollo-Monedero, D., Forne, J., ve Domingo-Ferrer, J. (2010). From t-closeness-like privacy to postrandomization via information theory. *IEEE Transactions on Knowledge and Data Engineering*, 22(11), 1623-1636.
- Rodrigues, P. (2020, Eriřim Tarihi: 04.12.2020). Covid-19 – Kaggle: Chest X-Ray (normal). İnternet Sayfası: <https://data.mendeley.com/datasets/rscbjbr9sj/2>
- Ruder, S. (2016). An overview of gradient descent optimization algorithms. *arXiv preprint arXiv:1609.04747*.
- Rusk, N. (2016). Deep learning. *Nature Methods*, 13(1), 35-35.
- Sait, U., KV, G. L., Shivakumar, S., Kumar, T., Bhaumik, R., Prajapati, S., . . . Chakrapani, A. (2021). A deep-learning based multimodal system for Covid-19 diagnosis using breathing sounds and chest X-ray images. *Applied Soft Computing*, 107522.
- Sait, U., KV, G. L., Sunny Prajapati, Rahul Bhaumik, Tarun Kumar, Sanjana S, ve Bhalla, K. (2020, Eriřim Tarihi: 02.02.2022). Curated Dataset for COVID-19 Posterior-Anterior Chest Radiography Images (X-Rays). İnternet Sayfası: <https://data.mendeley.com/datasets/9xkhgts2s6/1>
- Seyarer, E., Ayata, F., Uçkan, T., ve Karci, A. (2020). Derin Öğrenmede Kullanılan Optimizasyon Algoritmalarının Uygulanması Ve Kiyaslanması. *Computer Science*, 5(2), 90-98.
- Sharma, S. (2020). Drawing insights from COVID-19-infected patients using CT scan images and machine learning techniques: a study on 200 patients. *Environmental Science and Pollution Research*, 27(29), 37155-37163.
- Shokri, R., ve Shmatikov, V. (2015). *Privacy-preserving deep learning*. Paper presented at the Proceedings of the 22nd ACM SIGSAC conference on computer and communications security.
- Shokri, R., Stronati, M., Song, C., ve Shmatikov, V. (2017). *Membership inference attacks against machine learning models*. Paper presented at the 2017 IEEE symposium on security and privacy (SP).
- Soomro, T. A., Zheng, L., Afifi, A. J., Ali, A., Yin, M., & Gao, J. (2021). Artificial intelligence (AI) for medical imaging to combat coronavirus disease (COVID-19):

- a detailed review with direction for future research. *Artificial Intelligence Review*, 1-31.
- Starmer, J. (2019, Eriřim Tarihi 27.07.2022). Gradient Descent, Step-by-Step. İnternet Sayfası: <https://www.youtube.com/watch?v=sDv4f4s2SB8>
- Steinke, T., ve Ullman, J. (2015). Between pure and approximate differential privacy. *arXiv preprint arXiv:1501.06095*.
- Sun, Z., Wang, Y., Shu, M., Liu, R., ve Zhao, H. (2019). Differential privacy for data and model publishing of medical data. *IEEE Access*, 7, 152103-152114.
- Swapna. (2021, 14.12.2021). Convolution Neural Networks(CNN). İnternet Sayfası: <https://developersbreach.com/convolution-neural-network-deep-learning/>
- Sweeney, L. (2002). k-Anonymity: A Model For Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05), 557-570.
- Şeker, A., Diri, B., ve Balık, H. H. (2017). Derin öğrenme yöntemleri ve uygulamaları hakkında bir inceleme. *Gazi Mühendislik Bilimleri Dergisi (GMBD)*, 3(3), 47-64.
- Şimşek, N. Y. (2019, 15.12.2021). Derin Öğrenme(Deep Learning) Nedir ve Nasıl Çalışır? İnternet Sayfası: <https://nyilmazsimsek.medium.com/derin-%C3%B6%C4%9Frenme-deep-learning-nedir-ve-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-2d7f5850782>
- Tails, H. o. (2020, Eriřim Tarihi: 06.12.2020). Covid-19 Tracking Germany Dataset. İnternet Sayfası: <https://www.kaggle.com/headsortails/covid19-tracking-germany>
- Tan, Z. (2019). *Derin Öğrenme Yardımıyla Araç Sınıflandırma*. (Yüksek Lisans Tezi), Fırat Üniversitesi,
- Tataroğlu, M. (2013). Mahremiyet sorunlarının önlenmesinde mahremiyet etki değerlendirmesi (MED). *Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 20(1), 263-289.
- Tawsifur Rahman, M. C., Amith Khandakar. (2021, Eriřim Tarihi: 02.02.2022). Covid-19 Radiography Database. İnternet Sayfası: <https://www.kaggle.com/tawsifurrahman/covid19-radiography-database>
- Toğaçar, M., Ergen, B., ve Cömert, Z. (2020). Covid-19 Detection Using Deep Learning Models To Exploit Social Mimic Optimization And Structured Chest X-Ray Images Using Fuzzy Color And Stacking Approaches. *Computers in Biology and Medicine*, 103805.
- Tramèr, F., Zhang, F., Juels, A., Reiter, M. K., ve Ristenpart, T. (2016). *Stealing Machine Learning Models via Prediction {APIs}*. Paper presented at the 25th USENIX security symposium (USENIX Security 16).
- Ucar, F., ve Korkmaz, D. (2020). COVIDiagnosis-Net: Deep Bayes-SqueezeNet based diagnosis of the coronavirus disease 2019 (COVID-19) from X-ray images. *Medical Hypotheses*, 140, 109761.

- Union, E. (2020, Eriřim Tarihi: 20.12.2020). European Union Open Covid-19 Coronavirus Dataset. İnternet Sayfası: <https://data.europa.eu/euodp/en/data/dataset/covid-19-coronavirus-data>
- Velavan, T. P., ve Meyer, C. G. (2020). The COVID-19 epidemic. *Tropical medicine ve international health*, 25(3), 278.
- Wang, K.-F. (2018, Eriřim Tarihi: 12.08.2022). Calculating Gradient Descent Manually. İnternet Sayfası: <https://towardsdatascience.com/calculating-gradient-descent-manually-6d9bee09aa0b>
- Wang, L., Lin, Z. Q., ve Wong, A. (2020). Covid-Net: A Tailored deep Convolutional Neural Network Design For Detection Of Covid-19 Cases From Chest X-Ray Images. *Scientific Reports*, 10(1), 1-12.
- Wang, L. L., Lo, K., Chandrasekhar, Y., Reas, R., Yang, J., Eide, D., . . . Merrill, W. (2020). Cord-19: The covid-19 open research dataset. *ArXiv*.
- Wang, S., Zha, Y., Li, W., Wu, Q., Li, X., Niu, M., . . . Yu, H. (2020). A Fully Automatic Deep Learning System For Covid-19 Diagnostic And Prognostic Analysis. *European Respiratory Journal*.
- Warren, S., & Brandeis, L. D. (1890). *The Right to Privacy* (Vol. 4(5)): Harvard Law Review.
- WHO. (2021, 14.12.2021). WHO Coronavirus (COVID-19) Dashboard. İnternet Sayfası: <https://covid19.who.int/>
- Wong, A., Qiu Lin, Z., Wang, L., Chung, A. G., Shen, B., Abbasi, A., . . . Duong, T. Q. (2020). COVIDNet-S: Towards computer-aided severity assessment via training and validation of deep neural networks for geographic extent and opacity extent scoring of chest X-rays for SARS-CoV-2 lung disease severity. *arXiv e-prints*, arXiv: 2005.12855.
- Wu, X., Li, F., Kumar, A., Chaudhuri, K., Jha, S., ve Naughton, J. (2017). *Bolt-on differential privacy for scalable stochastic gradient descent-based analytics*. Paper presented at the Proceedings of the 2017 ACM International Conference on Management of Data.
- Xu, X., Jiang, X., Ma, C., Du, P., Li, X., Lv, S., . . . Su, J. (2020). A deep learning system to screen novel coronavirus disease 2019 pneumonia. *Engineering*, 6(10), 1122-1129.
- Yapıcı, M. M., ve Topaloğlu, N. (2021). Performance comparison of deep learning frameworks. *Computers and Informatics*, 1(1), 1-11.
- Yıldız, K., Güneř, E., ve Bas, A. (2021). CNN-based Gender Prediction in Uncontrolled Environments. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 9(2), 890-898.
- Yu, D., Zhang, H., Chen, W., Liu, T.-Y., ve Yin, J. (2019). Gradient perturbation is underrated for differentially private convex optimization. *arXiv preprint arXiv:1911.11363*.

- Yu, Y., Si, X., Hu, C., ve Zhang, J. (2019). A review of recurrent neural networks: LSTM cells and network architectures. *Neural computation*, 31(7), 1235-1270.
- Yurtsever, M. (2021). Gold price forecasting using LSTM, Bi-LSTM and GRU. *Avrupa Bilim ve Teknoloji Dergisi*(31), 341-347.
- Zarikas, V., Pouloupoulos, S. G., Gareiou, Z., ve Zervas, E. (2020). Clustering analysis of countries using the COVID-19 cases dataset. *Data in brief*, 31, 105787.
- Zhang, J., Xie, Y., Liao, Z., Pang, G., Verjans, J., Li, W., . . . Shen, C. (2020). Viral Pneumonia Screening On Chest X-Ray Images Using Confidence-Aware Anomaly Detection. *arXiv preprint arXiv:2003.12338*.
- Zhang, J., Zheng, K., Mou, W., ve Wang, L. (2017). Efficient private ERM for smooth objectives. *arXiv preprint arXiv:1703.09947*.
- Zhao, A. (2020, Eriřim Tarihi: 04.02.2022). COVIDx CXR-2 Dataset. İnternet Sayfası: https://www.kaggle.com/andyczhao/covidx-cxr2?select=competition_test
- Zhao, J., Chen, Y., ve Zhang, W. (2019). Differential privacy preservation in deep learning: Challenges, opportunities and solutions. *IEEE Access*, 7, 48901-48911.
- Zhu, T., Li, G., Zhou, W., ve Philip, S. Y. (2017). *Differential privacy and applications*: Springer.