



**T.C.
HALIÇ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI**

BİYOMETRİK KİMLİK TANIMLAMA SİSTEM TASARIMI

YÜKSEK LİSANS TEZİ

**Hazırlayan
Zeynep İNEL ÖZKİPER**

**Danışman
Dr. Öğr. Üyesi Zeynep TURGUT**

İstanbul – 2019

**T.C.
HALIÇ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI**

**BİYOMETRİK KİMLİK TANIMLAMA SİSTEM
TASARIMI**

YÜKSEK LİSANS TEZİ

**Hazırlayan
Zeynep İNEL ÖZKİPER**

**Danışman
Dr. Öğr. Üyesi Zeynep TURGUT**

İstanbul – 2019

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Programı Öğrencisi Zeynep İNEL ÖZKİPER tarafından hazırlanan “*Biyometrik Kimlik Tanımlama Sistem Tasarımı*” konulu çalışması jürimizce Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 05.07.2019

(Jüri Üyesinin Ünvanı, Adı, Soyadı ve Kurumu):

İmzası

Jüri Üyesi : Dr. Öğretim Üyesi Zeynep TURGUT
: Haliç Üniversitesi (Danışman)

Jüri Üyesi : Prof.Dr. Mübariz EMİNLİ
: Haliç Üniversitesi

Jüri Üyesi : Dr.Öğr. Üyesi Selçuk SEVGİN
: İstanbul-Cerrahpaşa Üniversitesi

Bu tez Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulunun kararıyla kabul edilmiştir.

Prof.Dr. Nur TUNALI
Vekil Müdür

Zeynep İnel Özkiper

ORIJINALLIK RAPORU

%8

BENZERLİK ENDEKSİ

%4

İNTERNET
KAYNAKLARI

%2

YAYINLAR

%7

ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

- 1 Submitted to TechKnowledge Turkey** %1
Öğrenci Ödevi
- 2 Submitted to Haliç Üniversitesi** %1
Öğrenci Ödevi
- 3 Submitted to Eskisehir Osmangazi University** <%1
Öğrenci Ödevi
- 4 Submitted to Batman University** <%1
Öğrenci Ödevi
- 5 www.halic.edu.tr** <%1
İnternet Kaynağı
- 6 www.fbedergi.duzce.edu.tr** <%1
İnternet Kaynağı
- 7 Submitted to The Scientific & Technological
Research Council of Turkey (TUBITAK)** <%1
Öğrenci Ödevi
- 8 Submitted to Kocaeli Üniversitesi** <%1
Öğrenci Ödevi

600105
Dr. Öğretim Üyesi
Zeynep TURGUT

TEZ ETİK BEYANI

Yüksek Lisans Tezi olarak sunduğum “Biyometrik Kimlik Tanımlama Sistem Tasarımı” başlıklı bu çalışmayı baştan sona kadar danışmanım Dr. Öğr. Üyesi Zeynep TURGUT’un sorumluluğunda tamamladığımı, hazır veri seti kullandığımı, deneyleri/analizleri ilgili laboratuvarlarda yaptığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim.



Zeynep İNEL ÖZKİPER

ÖNSÖZ

Bu çalışma 2018 – 2019 yılları arasında T.C. Haliç Üniversitesi Bilgisayar Mühendisliği Bölümü'nün bilimsel araştırma ve uygulama çalışmalarına verdiği destek ile hazırlanmıştır.

Tez çalışmamda konunun belirlenmesi ve tamamlanması süresince büyük bir gayret ve özveriyle çalışmamı takip eden, gösterdiği sabır ve hoşgörüsüyle bana destek olan tez danışmanım Sayın Dr. Öğr. Üyesi Zeynep Turgut'a çok teşekkür ederim. Yüksek lisans eğitimim süresince yardımlarını benden esirgemeyen Prof. Dr. Mübariz Eminli'ye ayrıca teşekkürlerimi sunarım. Yüksek lisans tezi çalışmalarım sırasında desteğinden dolayı iş arkadaşım Fatih Çırak'a teşekkür ederim.

Son olarak eğitim hayatım boyunca maddi ve manevi olarak bana destek olan tecrübeleriyle yol gösteren teyzem Dr. Öğr. Üyesi Melek Ertogan'a ve her zaman yanımda olduğunu hissettiren eşim Kadir Özkiper'e, verdiğim her kararın arkasında durarak beni bu günlere getiren sevgili annem Hayriye İnel ve sevgili babam Erdal İnel'e sonsuz teşekkür ederim.

İstanbul, 2019

Zeynep İNEL ÖZKİPER

İÇİNDEKİLER

	Sayfa No.
TEZ ETİK BEYANI	iii
ÖNSÖZ	iv
İÇİNDEKİLER	I
KISALTMALAR	III
ŞEKİLLER	IV
ÇİZELGELER	VI
ÖZET	VII
ABSTRACT	VIII
1. GİRİŞ	1
2. BİYOMETRİK SİSTEMLER	3
2.1. Kimlik Tanıma Amacıyla Kullanılan Biyometrik Özellikler	3
2.1.1. Parmak İzi Tanıma	4
2.1.2. Yüz Tanıma	4
2.1.3. İris Tanıma	5
2.1.4. Retina Tanıma	5
2.1.5. El Geometrisi Tanıma	6
2.1.6. Ses Tanıma	6
2.1.7. Damar Tanıma	7
2.1.8. İmza Tanıma	7
3. LİTERATÜR ÇALIŞMASI	9
4. PARMAK İZİ GÖRÜNTÜ İŞLEME AŞAMALARI	13
4.1. Görüntü Edinme	13
4.1.1. Parmak İzi Çeşitleri	14
4.1.2. Parmak İzi Özellikleri	15
4.2. Görüntü Ön İşleme	16
4.3. Görüntü Zenginleştirme.....	16
4.3.1. Canny Kenar Belirleme Operatörü	17
4.4. Dönüştürme.....	18
4.5. Özellik Çıkarma	19

4.6. Sınıflandırma	20
4.6.1. Geleneksel Yapay Sinir Ağları	20
4.6.1.1. İleri Beslemeli Yapay Sinir Ağları	23
4.6.1.2. Geri Beslemeli Yapay Sinir Ağları	23
4.6.2. Destek Vektör Makinaları.....	24
4.6.3. Evrimsel Sinir Ağı	25
4.6.4. Hibrit Yaklaşım - CNN+SVM	26
5. ARAÇLAR VE YÖNTEMLER.....	28
5.1. Veri Analizi	28
5.2. Performans Metrikleri	31
6. BULGULAR.....	34
7. TARTIŞMA.....	44
8. SONUÇLAR.....	47
9. KAYNAKLAR	48
10. ÖZGEÇMİŞ	51

KISALTMALAR

CNN	: Convolutional Neural Network (Evrşimsel Sinir Ađı)
DCNN	: Deep Convolutional Neural Network (Derin Evrşimsel Sinir Ađı)
FN	: False Negative (Yanlıř Negatif)
FP	: False Positive (Yanlıř Pozitif)
LBP	: Local Binary Pattern (Yerel İkili Desen)
MCC	: Matthews Correlation Coefficient (Matthews Korelasyon Katsayısı)
PCA	: Principal Component Analysis (Temel Bileřen Analizi)
SVM	: Support Vector Machine (Destek Vektör Makinesi)
TN	: True Negative (Dođru Negatif)
TP	: True Positive (Dođru Pozitif)

ŞEKİLLER

Sayfa No.

Şekil 2.1. İris yapısı	5
Şekil 2.2. Retina	6
Şekil 4.1. Görüntü işleme aşamaları	13
Şekil 4.2. Spiral (Loop) tipi parmak izi	14
Şekil 4.3. Helezon (Whorl) tipi parmak izi	15
Şekil 4.4. Kemer (Arch) tipi parmak izi	15
Şekil 4.5. Ayrıntı yapıları	17
Şekil 4.6. Parmak izi görüntüsüne Canny algoritması uygulandıktan sonraki parmak izi görüntüsü	18
Şekil 4.7. Örnek parmak izi dönüşüm görüntüleri	18
Şekil 4.8. Yapay sinir ağı yapısı	21
Şekil 4.9. Yapay sinir ağı nöron yapısı	21
Şekil 4.10. A, B ve C verilerinin sınıflandırma işleminin düzlemsel gösterimi	24
Şekil 4.11. Evrişimsel ağ	25
Şekil 4.12. Hibrit CNN-SVM modelinin yapısı	27
Şekil 5.1. Parmak izi görüntülerinin elde edildiği cihazlar	29
Şekil 5.2. Karışıklık matrisi	31
Şekil 6.1. Crossmatch veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	35
Şekil 6.2. Crossmatch veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	35
Şekil 6.3. Crossmatch veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi	36
Şekil 6.4. Crossmatch veri seti hibrit yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	36
Şekil 6.5. Crossmatch veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi	37
Şekil 6.6. Digital Persona veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	37
Şekil 6.7. Digital Persona veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	38

Şekil 6.8. Digital Persona veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi.....	38
Şekil 6.9. Digital Persona veri seti hibrit yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi.....	39
Şekil 6.10. Digital Persona veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi	39
Şekil 6.11. Green Bit veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	40
Şekil 6.12. Green Bit veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	40
Şekil 6.13. Green Bit veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi..41	
Şekil 6.14. Green Bit veri seti hibrit yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi	41
Şekil 6.15. Green Bit veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi.....	42

ÇİZELGELER

Sayfa No.

Çizelge 4.1. Aktivasyon Fonksiyonları ve Denklemleri.....	22
Çizelge 5.1. LivDet2015 gerçek ve sahte parmak izi görüntü sayıları.....	29
Çizelge 5.2. LivDet2015 parmak izi görüntülerinin elde edildiği cihazların özellikleri.....	30
Çizelge 5.3. LivDet2015 çalışmada kullanılan gerçek ve sahte parmak izi görüntü sayıları.....	30
Çizelge 6.1. Parmak izi görüntülerinin SVM yöntemi ile sınıflandırılarak elde edilen sonuçları.....	42
Çizelge 6.2. Parmak izi görüntülerinin CNN yöntemi ile sınıflandırılarak elde edilen sonuçları.....	43
Çizelge 6.3. Parmak izi görüntülerinin CNN+SVM yöntemi ile sınıflandırılarak elde edilen sonuçları.....	43
Çizelge 7.1. Green Bit veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları.....	44
Çizelge 7.2. Digital Persona veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları.....	44
Çizelge 7.3. Crossmatch veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları.....	45

ÖZET

BİYOMETRİK KİMLİK TANIMLAMA SİSTEM TASARIMI

Dünyada kimlik tanımlama açısından en geniş kabul ile en büyük kullanım oranına sahip biyometrik özelliklerden biri olan parmak izi tanımlama ve doğrulama sistemlerinin yüksek doğruluk sağlaması büyük önem arz etmektedir. Parmak izi tanıma sistemleri kriminal sistemlerden, devlet dairelerine, laboratuvarlardan ve sınır geçişlerine kadar kimlik tanımlamanın gerekli olduğu hemen her yerde diğer biyometrik özellik tanıma sistemlerinden daha yaygın olarak kullanılmaktadır. Bu nedenle parmak izi tanıma sisteminin sahte ve gerçek parmak izinin ayrımını gerçekleştirmede hızlı ve güvenilir olması, daha yüksek hassasiyet sağlaması gerekmektedir.

Bu çalışmada, lateks, ahşap tutkalı, jelatin ve silikon türevlerinden üretilmiş sahte parmak izleri, gerçek parmak izleri karşılaştırılarak sistemin elde ettiği sonuçlara ait performans metrikleri değerlendirilmiş ve bulunan sonuçlar diğer sistemler ile karşılaştırılmıştır. Sahte ve gerçek parmak izini karşılaştırması için uygun makine öğrenmesi yöntemleri LivDet2015 veri setinde bulunan sahte ve gerçek parmak izleri üzerinde çalıştırılmış ve elde edilen sonuçlar kıyaslanarak tartışılmıştır.

Anahtar Kelimeler: Biyometrik kimlik tanımlama, makine öğrenmesi, parmak izi tanıma, SVM, CNN

ABSTRACT

BIOMETRIC IDENTIFICATION SYSTEM DESIGN

It is of great importance to provide the highest accuracy of fingerprint identification and verification systems, which is one of the largest biometric features with the largest acceptance rate in terms of identity identification in the world. Fingerprint recognition systems are more widely used than any other biometric feature recognition system, from criminal systems, government departments, laboratories, border crossings, etc., wherever identification is required. For this reason, the fingerprint recognition system must be fast and reliable in order to realize the separation of the false and live fingerprints, and provide higher sensitivity.

In this study, the performance metrics of the results of the system were evaluated by comparing the false fingerprints produced by latex, wood glue, gelatine and silicon derivatives and live fingerprints and the results were compared with the other systems. Appropriate machine learning methods for comparing fake and live fingerprints were run on fake and live fingerprints in the LivDet2015 dataset and the results obtained were compared and discussed.

Keywords: Biometric identification, machine learning, fingerprint recognition, SVM, CNN

1. GİRİŞ

Toplumlar için en önemli olgu güvenlidir. Kişiler kendilerini güvende hissetmesi adına kimliklerin belirlenmesi önem arz etmektedir. Hukuk gereği suçluya ceza verebilmek için maddi delillerin toplanması gerekmektedir. Kimlik tespiti için kullanılan nüfus cüzdanı ve pasaport gibi belgeler sahte evrak düzenlenebilmesi, evrakların üzerinde değişiklik yapılabilmesi gibi nedenlerle yüksek güvenlik sağlamamaktadır. Bu nedenle evraklardan bağımsız olarak kişiye özgü eşsiz bir kimlik denetim sistemi tasarlanması günümüzün temel gerekliliklerinden biridir. Kimlik tespitinde güvenilir, benzersiz ve değişmez yöntemler bulmak için çalışmalar yapılmıştır. Çalışmalar sonucunda kişiye özgü ve benzersiz olan biyometrik özelliklerin kullanılabilmesi sonucuna varılmıştır.

İnsan vücudunda benzersiz olan birçok özellik mevcuttur. Bu özellikleri tespit ederek diğer insanlardan ayırma yeteneğine sahip sistemler bulunmaktadır. İnsanların fiziksel veya davranışsal özelliklerine göre kimliklendirme yapan sistemlere biyometrik sistemler denir. Biyometrik sistemler yaygın olarak parmak izi, yüz, iris, retina, el geometrisi, imza ve ses gibi kişiye ait özelliklerde kullanılmaktadır.

Herhangi bir suç durumunda olay yerinde delil olarak suç işleyen kişiye ait saç teli, deri döküntüsü, tükürük, kan izi ve parmak izi gibi özellikler veya güvenlik kameraları kullanılmaktadır. Bazen suçun işlendiği yerde güvenlik kamerası olmayabilir ya da kameradan sağlıklı görüntü elde edilemeyebilir. DNA eşleştirmelerinin zaman gereksiniminin yüksek olması ve parmak izi tanıma sistemlerinden daha maliyetli olması sebebiyle en çok kullanılan özellik parmak izidir. 19.yy'dan beri kriminal kimlik tespit sistemlerinde sıklıkla kullanılan parmak izi verileri teknolojik gelişmeler ile birlikte farklı maddeler ile üretilebilir hale gelmiştir. Parmak izine benzer veriler farklı maddeler kullanılarak kolaylıkla oluşturulmaktadır. Ev, iş yeri, banka, laboratuvar vb. alanlarda sıklıkla kullanılan parmak izi verilerinin bir insandan elde edilip edilmediğine ait ayrımın yapılması parmak izi kullanılarak yapılabilecek sahtekarlıkların önüne geçecektir. Bu çalışma içerisinde insanlardan toplanmış canlı parmak izleri ile jelatin, lateks, ahşap tutkalı (woodglue), ekofleks

(ecoflex), body double ve oyun hamuru gibi silikon türevi maddeler ile oluşturulmuş sahte parmak izleri içeren LivDet2015 veri kümesi üzerinde çalışılmıştır. İlgili veri kümesi üzerinde destek vektör makineleri, derin öğrenme – evrişimsel sinir ağları ve hibrit yöntem: evrişimsel sinir ağı – destek vektör makinesi kullanılarak sahte ve canlılara ait olarak etiketlenilmiş parmak izi verileri sınıflandırılmış, böylelikle parmak izi sahtekarlığının önüne geçebilecek bir sistem oluşturulmuştur. LivDet2015 veri kümesinin yapısı incelenerek ilgili veri kümesinin içerisinde yer alan verilere en uygun makine öğrenmesi yöntemleri seçilerek kıyaslanmış ve performans analizleri gerçekleştirilmiştir.

Bu çalışmanın birinci bölüm olan giriş bölümünde neden parmak izi tanıma sisteminin seçildiği ve nerelerde kullanıldığı, ikinci bölüm olan biyometrik sistemler bölümünde kimlik tanıma amacıyla kullanılan parmak izi, yüz, iris, retina, el geometrisi, ses, damar ve imza tanıma sistemleri hakkında kısa bilgiler verilmiştir. Üçüncü bölümde literatür araştırması sonucunda parmak izi görüntüleri üzerinde yapılan çalışmalar ile ilgili özet bilgi verilmiştir. Dördüncü bölümde parmak izi görüntü işleme aşamaları olan görüntü edinme, görüntü ön işleme, özellik çıkarma ve sınıflandırma yöntemlerinden bahsedilmiştir. Beşinci bölümde çalışmada kullanılan bilgisayarın özelliklerinden, LivDet 2015 veri setinden bahsedilmiş ve çalışma sonucunun değerlendirilmesinde kullanılan performans metrikleri anlatılmıştır. Altıncı bölümde veri setinin Matlab ortamında SVM, CNN ve CNN-SVM ile sınıflandırılması sonucu elde edilen sonuçların ekran görüntüleri verilmiştir. Yedinci bölümde gerçek ve sahte parmak izi görüntülerinin SVM, CNN ve hibrit CNN-SVM yöntemleri ile sınıflandırılması sonucu elde edilen sonuçların ölçüm metrikleri üzerinde etkileri tartışılmıştır. Sekizinci bölümde çalışma sonucu yer almaktadır.

2. BİYOMETRİK SİSTEMLER

Biyometrik sistemler kimlik doğrulamada kullanılan, insanların benzersiz olan fiziksel ve davranışsal özelliklerinin ölçümü ve istatistiksel analizleri içermektedir. İki tür biyometrik özellik vardır. Bunlar; fiziksel özellikler ve davranışsal özelliklerdir. Kimlik tanımlamada kullanılan fiziksel özellikler, yüz tanıma, parmak izi tanıma, el geometrisi, iris tanıma, retina taraması, damar tanıma, ses tanıma ve DNA eşleşmesidir. Davranışsal özellikler ise yazım kalıplarının tanınması, imza tanıma, yürüyüş tarzı ve bireyin diğer hareketlerinden oluşur.

Kimlik doğrulaması günümüzde giderek yaygınlaşmaya başlamış, kurumsal ve kamu güvenlik sistemlerinde, sağlık kuruluşlarında ve kişisel elektronik cihazları gibi birçok alanda kullanılmaktadır. Güvenliğin yanı sıra çoğu insanın hatırlamakta güçlük çektiği şifrelerin ve yanında bulundurulması gereken kimlik kartlarının yerine geçmesi ile büyük kolaylık sağlamaktadır.

Emniyet güçlerinin suçlu kimlik çözümleri için kullandıkları otomatik parmak izi tanımlama sistemleri (AFIS) gibi sistemler parmak izi görüntülerini işler, depolar, arar ve eşleştirir. Otomatik biyometrik tanımlama sistemleri (ABIS) gerçek zamanlı veya olay sonrası yüz veya diğer biyometrik özellikleri tanıma kabiliyetine sahip olduğundan, şehir güvenliğinde, hava alanlarında ve sınırlarda kullanılmaktadır. Sınır kontrolünde yaygın olarak kullanılan uygulama elektronik pasaporttur. Bu pasaportlar biyometrik pasaport olarak da bilinen üzerinde biyometrik fotoğrafa ek olarak iki parmağın izi bulunan belgelerdir. Pasaportun içinde bulunan mikro denetleyicisindeki parmak izi ile okunan parmak izinin karşılaştırmasıyla kimlik doğrulaması yapılır.

2.1. Kimlik Tanıma Amacıyla Kullanılan Biyometrik Özellikler

Biyometrik sistemler ilk olarak kişilerin biyometrik özelliklerini sisteme aktarma ikinci olarak da kimlik doğrulama için kişinin bilgilerinin sisteme sorulması adımlarından oluşur (Kakıcı, 2008). Bu bölümde kimlik tanımlama amacıyla

kullanılan parmak izi, yüz, iris, retina, el geometrisi, ses, damar ve imza tanıma sistemleri anlatılmıştır.

2.1.1. Parmak İzi Tanıma

Parmak izi tanıma kimlik doğrulama için kullanılan en yaygın yöntemdir. Parmak izi tanıma iki parmak izinin karşılaştırmasına dayanan biyometrik sistemdir. Parmak izleri sırtlar ve vadilerden oluşan grafiksel desenlerdir. Parmak izinde bulunan bu sırtların bitimi ve çatallanmalarına ayrıntı (minutia) denir. Her insan birbirinden farklı parmak izine sahiptir. İnsan ömrü boyunca değişmeyen biyometrik özelliktir. İlk parmak izi tanıma konusundaki çalışma 1980'lerde Henry Faulds ve Wiliam James Herschel tarafından yazılan bir makalede yapılmıştır. Parmak izi konusunda çalışan Galton 1890'da parmak izlerinin insanlar yaşlandıkça değişmediğini ve bir bireyi tanımlamada eşsiz bir yol olduğunu doğrulamıştır. Galton bu konuda çalışan ilk kişi olmasa da bilimsel kaynaklara dayandıran ilk kişidir. Ülkemizde parmak izinin ilk kimlik tanıma olarak kullanılması 1910 yılında başlamıştır. Bu çalışma içerisinde parmak izi kullanılarak bir biyometrik kimlik tanımlama sistemi önerilmiştir.

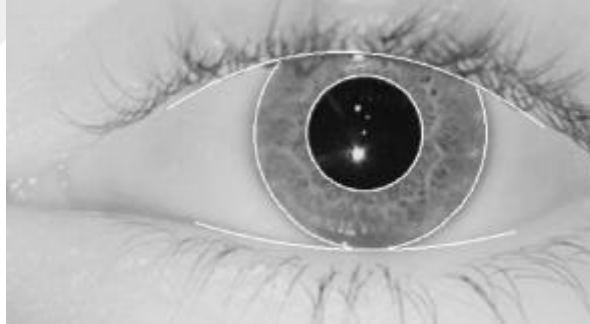
2.1.2. Yüz Tanıma

Yüz tanıma, fotoğraf ya da videodaki bireyin yüz özelliklerinin matematiksel olarak haritalanarak depolanması ve bir yazılım aracılığı ile karşılaştırma işleminin yapılmasıdır. Bilim insanları 1960'lı yıllarda insan yüzlerini tanımak için bilgisayarı kullanmaya başladılar. Daha sonra bu alanda yapılan çalışmalar gelişerek devam etmiştir. Yüz tanıma yüzün çeşitli özelliklerinin çıkarılması ile yapılmaktadır. Bu özellikler burun uzunluğu, elmacık kemiği çıkıntısı, kaş, gözler ve çenedir. İnsan yüzünde 80 düğüm noktası bulunmaktadır (<http://www.turksan.com>, Erişim tarihi: 24 Kasım 2018). Tanıma amaçlı kullanılan yazılım gözler arasındaki mesafe, burun genişliği, göz yuvalarının derinliği, elmacık kemikleri şekli, çene çizgisinin uzunluğu gibi düğüm noktalarını ölçer. Işıklandırma gibi diğer etkenlerden etkilenmeyen Üç boyutlu görüntüden kimlik doğrulama yapan yazılımların adımları; görüntünün elde edildiği bulma (Detection), algılanan yüzün konumunu, boyutunu ve pozunu belirleyen hizalanma (Alignment), yüz eğrilerinin ölçülerek bir şablon oluşturulan ölçüm (Measurement), oluşturulan şablonların koda çevrilerek bunlara bir numara verildiği temsil (Representation), görüntünün veri tabanındaki görüntü ile eşleştirildiği

eşleştirme (Matching), bir görüntünün veri tabanındaki sadece bir görüntü ile eşleşmesi doğrulama veya tanımlama (Verification or Identification) şeklindedir.

2.1.3. İris Tanıma

İris tanıma gözün içindeki renkli çemberde bulunan benzersiz desenleri ölçer. İris tanıma için ilk algoritmayı geliştiren John Daugman'dır (Daugman, 2009). İris tanıma diğer biyometrik tanıma sistemleri gibi yazılımın yanında belirli bir donanıma da ihtiyaç duyduğundan daha az kullanılmaktadır. İris tanımda irisin dışarıdan görülen ayrıntılarının yakın kızılötesi aydınlatmaya sahip video kamera teknolojisi kullanılır. İris görüntüsünün veri tabanındaki iris desenleriyle karşılaştırılması sonucu kimlik doğrulama işlemi gerçekleştirilir. İris tanımanın önemli avantajlarından birisi eşleşme hızının ve yanlış eşleşmelere karşı aşırı dirençli olmasıdır. Dezavantajlarından biri ise kontak lens ve gözlük kullanımları iris tanımda yanlış sonuçlar çıkartabilmektedir. İris tanıma bazı ülkelerde havaalanlarının giriş çıkışlarında, kişisel bilgisayarlarda ve mobil cihazlarda kullanılmaktadır. Gözbebeğinde bulunan irisin sınırları çizilerek gösterilmiş hali Şekil 2.1' de görülmektedir.

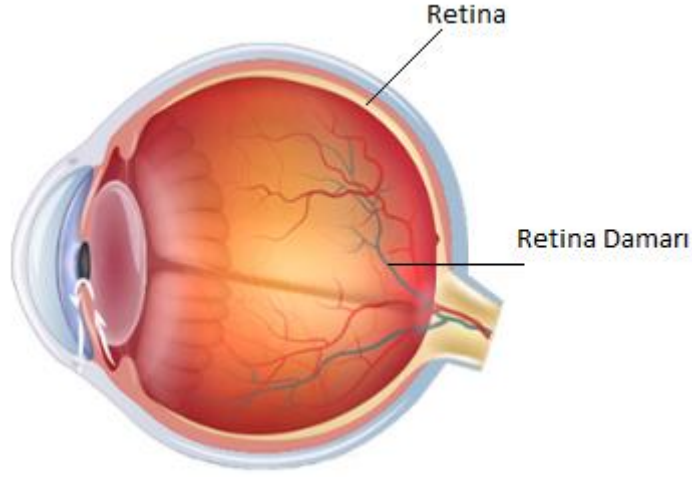


Şekil 2.1. İris Yapısı (Daugman, 2009)

2.1.4. Retina Tanıma

Retina tanıma gözün arkasında bulunan kan damarlarından oluşan benzersiz tabakanın yakalanmasıyla tanıma işleminin gerçekleştirildiği bir biyometrik tekniktir. Retina tanımda kan damarlarının kişiye ait bir düzene sahip olması kullanılır. Göz içerisinde retina kısmı Şekil 2.2' de gösterilmiştir. Retina tanıma, kullanılan uygulamanın maliyeti açısından en az kullanılan biyometrik yöntemlerden biridir. Ancak doğruluğu ve güvenilirliği nedeniyle yüksek güvenlik gerektiren devlet daireleri ve askeri alanlarda kullanılan örnekleri vardır. Retina desenini tanımak için kızılötesi ışını kullanılır. Kızılötesi ışığını kan damarları emerken etrafındaki dokuların yansması sağlanır. Sistem tarafından yansıma tespit edilerek desenin

görüntüsü yakalanır. Yakalanan görüntünün algoritma sayesinde şablonu oluşturulur ve saklanır. Daha sonra yeni bir retina örneği sisteme sunulduğunda veri tabanında bulunan şablonlarla eşleştirilerek kimlik doğrulama gerçekleştirilir.



Şekil 2.2. Retina (Gözebak.com, 2019)

2.1.5. El Geometrisi

El geometrisi tanıma değil doğrulama için kullanılmaktadır. El geometrisi sistemleri en uzun uygulama geçmişine sahiptir. El geometrisi sistemleri elin görüntüsünü yakalamak için bir kamera kullanır. Bu görüntüden elin mesafe ölçüleri alınır. Elin ve parmakların uzunluğu ve kalınlığı parmak eklemleri arasındaki mesafe ölçüleri alınır. Kayıt altına alınan el ölçüleri saklanır ve yeni okutulan el geometrisi ile karşılaştırılarak eşleşme yapılır. El geometrisi eşsiz olmadığından biyometrik tanımda kullanılmamaktadır. Günümüzde sağlık kuruluşlarında, hava alanlarında, fabrikalarda, hapishanelerde kimlik doğrulama işlemlerinde kullanılmaktadır.

2.1.6. Ses Tanıma

Ses tanıma, analog sesin dijital sinyallere dönüştürülerek kelimelerin ve hecelerin sayısal olarak veri tabanına kaydedilmesiyle yapılır. Ses tanıma işlemi sesin karakteristik özelliğine göre analiz edilmesi tekniklerine dayanır. Ses tanıma teknolojileri 1970'lerde yalnızca 1000 kelimeye kadar anlayabilirken 1980'lerde 20.000 kelimeye ulaşmıştır. Sürekli konuşmayı tanıyabilen ilk ses tanıma ürünü 1996 yılında IBM tarafından piyasaya sürülmüştür. Ses tanıma mobil cihazlar, bilgisayarlar ve ev teknolojilerinde (akıllı ev sistemleri gibi) kullanılmaktadır. Nesnelerin interneti kavramı giderek yaygınlaşmaya başladığı için ses tanıma amacıyla çoğu teknolojik

üründe kullanılmaya başlamıştır. İnsanlar sesin metne dönüştürülmesiyle hatırlatıcıların ayarlanması, internette arama yapılması gibi birçok alanda kullanılmaktadırlar. Yapay zeka algoritmaları ve makine öğrenmesi kullanılarak ses tanıma teknolojisi hızla gelişmektedir. Ses tanıma sistemleri, farklı anlamlar taşıyan benzer iki sözcük veya arka plan gürültüleri sistemi olumsuz yönde etkilediğinden daha hızlı çalışan işlemciler kullanılmasını gerektirir. Kısacası ses tanıma teknolojisi yazmak ya da bir tuşa basmak zorunda kalmadan istenilen komutların yapılmasını sağlayan, hayatı kolaylaştıran bir teknolojidir.

2.1.7. Damar Tanıma

İnsan vücudunun damar düzeninin kişiye özgü olduğu ve yaşlandıkça değişmemesi damar tanımanın biyometrik tanıma olarak kullanılmasının nedenidir. Kan damarlarının görüntülerinin alınması için yakın kızılötesi ışık kullanılır (<https://www.bilim.org>, Erişim tarihi: 24 Kasım 2018). Çıkan görüntülerden damar dallanma noktaları ve damar kalınlıkları gibi çeşitli özellikte veriler elde edilir ve veri tabanında saklanır. Damar tanıma, damar yapısı dışarıdan gözle görünür olmadığından ve cilt üzerindeki herhangi bir değişiklik okumanın doğruluğunu etkilemediğinden güvenilir bir biyometrik tanıma yöntemidir. Ayrıca damar tanıma cihazları temassız okuma yaptıkları için daha hijyenik bulunmaktadır. Bazı ülkelerde damar tanıma teknolojisi, ATM'lerde, hastanelerde ve üniversitelerde kullanılmaktadır.

2.1.8. İmza Tanıma

İmza tanıma davranışsal bir biyometrik özelliktir. İmza tanıma eşleştirme aşamasında diğer yöntemlerin aksine iki imzayı yan yana koyup benzerliğine bakmaz, iki görüntünün hareketini ve davranışlarını inceler. Çevrimiçi ve çevrimdışı olmak üzere iki farklı şekilde tanımlama işlemi yapılır. Çevrimiçi sistemlerde birey imzasını gerçek zamanlı olarak dijital bir ortama yazar ve kalemin hareketlerinden yola çıkarak imzanın özellikleri çıkarılır. Çevrimdışı sistemlerde birey imzasını bir kağıda yazar, optik tarayıcılar veya kameralar ile dijitalleştirilen imza sistem tarafından tanınır. İmza tanıma yaygın olarak kullanılan bir yöntemdir. Nagel ve Rosenfeld (1977) tarafından ilk çevrimdışı imza tanıma algoritması, Herbst ve Liu (1978) tarafından ilk çevrimiçi imza tanıma algoritması yayınlanmıştır. İmza atılırken uygulanan hız ve baskının taklit edilmesi imkansız olduğundan güvenilir bir yöntem olarak kullanılmaktadır. Fakat

çeşitli sebeplerde dolayı imzanın deęişmesi tanıma aşamasında sorunlar çıkarabilmektedir.



3. LİTERATÜR ÇALIŞMASI

Gao et al. (2001) parmak izi tanıma amacıyla CNN (Convolutional Neural Network – Evrimsel Sinir Ağı) kullanılmasını önermişlerdir. Çalışmada orijinal, basit ve sürekli zaman CNN'leri kullanmışlardır. Kullanılan tüm görüntüler 256 x 256 pikseldir. Gürültü azaltma ve kontrast geliştirme, sırt geliştirme, ikilileştirme ve inceltme ön işlemlerini içeren algoritma orijinal gri seviyede bir parmak izindeki yüksek frekanslı gürültüyü azaltır, sırtlardaki tahrip olan bağlantıyı kurtarır ve orijinal parmak izi görüntüsünü ikili görüntüye dönüştürür. Elde edilen siyah çizgiler orijinal görüntüdeki tüm özellikleri içerir.

Bhattacharya and Mali (2011) parmak izi görüntüsünün belirli bir veri tabanına ait olup olmadığını kontrol eden tanımlama ve belirli bir kişinin parmak izi olduğunu onaylayan doğrulama olmak üzere iki tür eşleştirme yöntemi ile parmak izi tanıma sistemi üzerinde çalışmışlardır. Önerilen yöntem piksel piksel eşleştirme yapar. Bu yöntemde göre parmak izi görüntüsünün belirli bir noktasına göre görüntü kırılır. Referans noktasını bulmak için ortalama gradyan hesabını kullanmışlar fakat gradyan yaklaşımının her parmak izi için uygun olmadığını eşleştirme için başka özelliklerinde gerekli olduğunu söylemişlerdir. En iyi sonucu ise 4x4 piksel blokları görüntüden almışlardır. Sonuç olarak parmak izi tanıma sisteminin güvenilirliğinin artırma işleminde elde edilen hassasiyete bağlı olduğunu vurgulamışlardır.

Wang et al. (2014) parmak izi görüntülerini sınıflandırmak için parmak izi yönlendirme alanı giriş alanı olarak seçilmiş derin sinir ağına dayalı tek gizli katmanlı oto kodlayıcı kullanmışlardır. Sınıflandırmanın doğruluğunu artırmak için Softmax regresyon modeline dayanan bulanık sınıflandırıcı kullanılmıştır. NIST-DB4 veri tabanını üç gizli katman ile sınıflandırmışlar ve %1.8 reddetme ile doğruluğu %93.1 bulmuşlardır.

Li et al. (2018) gizli parmak izi geliştirme yöntemi olarak derin evrimsel sinir ağı (CNN) kullanan FingerNet'i önermişlerdir. Üç ana bölümü olan FingerNet kodlanan kısmı konvolüsyon parçası ve iki kod çözme yapan parçalama ve yönlendirme işini yapan dekonvolüsyon parçasından oluşur. Konvolüsyon kısmı,

parmak izi özelliklerini çıkarmak içindir. Dekonvolüsyon geliştirme kısmı yapılandırılmış gürültüyü kaldırmak ve parmak izlerini geliştirmek için kullanılır. Dekonvolüsyonun oryantasyon kısmında geliştirme sürecini yönlendirmek için çoklu görev öğrenme stratejisini kullanır. Çok görevli öğrenmeyi performansı iyileştirmek için kullanmışlardır. NIST SD27 veri tabanı ile FingerNet sistemini test etmişlerdir. Önceden tanımlanmış görüntü önceliklerini kullanmak yerine, derin öğrenme yöntemi olan uçtan uca öğrenme stili ile pikselden piksele doğrudan öğrenme yöntemini kullanmışlardır.

Darlow and Rosman (2017) derin evrişimsel sinir ağını kullanan önemsiz ayrıntıları çıkarma yöntemi ile çalışan MENet ağını önermişlerdir. MENet 1024 nodüllü iki tam bağlı katmandan oluşan beş evrişimsel katmandan ve softmax çıkış katmanından oluşur. Softmax normalizasyon fonksiyonu ayrıntı noktasının varlığını veya yokluğunu tahmin etmek için kullanılmıştır. Çıkış katmanı dışındaki diğer tüm birimlerde ReLU aktivasyon fonksiyonu kullanılmıştır. MENet karşılaştırılan diğer ticari yazılımlara (NIST, DP, SG, NT, GL) göre %14.2 kayıpla en iyi olmasa da iyi sonuç vermiştir. FVC veri setinin %80'i eğitim %20'si test amaçlı kullanılmıştır. Yazarlar parmak izi geliştirme, özellik tespiti ve sınıflandırmayı içeren parmak izi tanıma sürecini açıklamışlardır.

Baştürk ve ark. (2018) parmak izi tanımda derin sinir ağlarını kullanmayı önermişlerdir. Derin sinir ağının yapısı iki adet özdevinimli kodlayıcı ve bir adet esnek eşikleyici sınıflandırıcı katmanlarından oluşmaktadır. Ağ yapısının eğitiminde ölçeklenmiş kodları Gabor filtresi ile elde etmişlerdir. Önerdikleri derin sinir ağının ortalama her 532 örneğin 9'unu yanlış tanıdığı anlaşılacak sistemin test doğruluğu %98.31 olarak ölçmüşlerdir. Eğitim işlemi süreyi kısaltmak için grafik işlemci üzerinde gerçekleştirmişlerdir.

Yuan et al. (2017) evrişimsel sinir ağı (CNN)'ni kullanarak gerçek parmak izlerini sahte olanlardan ayırmak için çalışmışlardır. CNN'i kullanmalarının sebebi derin öğrenme temelli öznetelik çıkarma yöntemleri, kendi kendine öğrenme yeteneği, bilgisayarla görme ve görüntü sınıflandırması dahil örüntü tanımda başarılı olmasıdır. Özellik çıkarımı için konvolüsyon işlemi kullandıktan sonra CNN'e dayanan öğrenilmiş özellikler sınıflandırma için destek vektör makineleri (SVM) ile beslenir. Her bir konvolüsyon ve havuzlama işlemi arasında öğrenilmiş özelliklerin boyutlarını azaltmak için temel bileşen analizi (PCA) uygulanmıştır. Metodun performansını ölçmek için gerçek ve sahte olmak üzere toplamda 16056 parmak izi içeren LivDet

2011 veri seti ve 16853 parmak izinden oluşan LivDet 2013 veri setini kullanmışlardır. LivDet 2013 veri setine uygulanan metodun hata oranı sıfıra yakın sonuçlar vermiştir. LivDet 2011 veri setinde ise hata oranının sıfıra yakın değerleri daha azdır.

Song et al. (2019) parmak izi benzerliği hesaplamasında oluşan sorunları ele almak için derin evrişimsel sinir ağı (DCNN) kullanmışlardır. Parmak izi indekslemesi için yaygın olarak kullanılan Minutia Cylinder Code (MCC) tanımlayıcısını ve DCNN'i eğitmek için halka açık olan Peking University and Founder (PUF) veri tabanını kullanmışlardır. Önerilen yöntemin indeksleme doğruluğu FVC2000 DB2a, FVC2000 DB3a, NIST 4, NIST 4 natural ve NIST 14 veri tabanları ile değerlendirmişlerdir. Düşük özellik boyutuna sahip önerilen yöntem diğer önde gelen yöntemlerden çok daha iyi performans gösterdiğini kanıtlamışlardır. Ayrıca ayrıtı özellik çıkarımı sırasında harcanan süre bakımından diğer yöntemlere göre MCC'nin iki kat daha hızlı olduğunu söylemişlerdir.

Noor et al. (2018) parmak izi tanıma sisteminin performans geliştirilmesi için Karar Ağacı, Doğrusal Ayrımcı Analizi (Linear Discriminant Analysis), Orta Gauss Destek Vektör Makinesi (MG-SVM), K-En Yakın Komşu, Bagged Tree Ensemble (Torbalanmış Ağaç Topluluğu) sınıflandırıcıları karşılaştırılmıştır. FV2002 veri seti üzerinde yapılan karşılaştırmada performans ölçütü olarak minHTER, EER, FRR-0,1 FAR ve FRR-10FAR kullanılmıştır. Karar ağacı kullanılarak yapılan sınıflandırmada %98,60 doğruluk, Linear Discriminant Analysis sınıflandırmada %98,80 doğruluk, MG-SVM sınıflandırmada en iyi doğrulama oranı olan %98,90 doğruluk, K-En Yakın Komşu sınıflandırmada %98,80 doğruluk, Bagged Tree Ensemble sınıflandırmada %98,80 doğrulama oranlarını elde etmişlerdir.

Marasco et al. (2019) sensör kullanılmadan suç mahallinden elde edilen sahte parmak izlerinin tespitinde kullanılan mevcut yöntemlerin avantajlarını ve dezavantajlarını ortaya koyan bir çalışma yapmışlardır. Otomatik parmak izi sistemleri ve evrişimsel sinir ağları için geliştirilen doku bazlı detektörleri değerlendirmek için LivDet2013 veri setini eğitmişler ve testler için NISTSD27 veri setini kullanmışlardır. Parmak izi görüntülerinin özelliklerini Local Binary Pattern (LBP), Local Phase Quantification (LPQ), Binarized Statistical Image Features (BSIF) algoritmalarını kullanarak çıkarıp One-Class SVM'yi eğitmek için kullanmışlardır. Yapılan deneyler evrişimsel sinir ağları (CNNs), CaffeNet (%96.5), GoogLeNet (%96.6), Siamese (%93.1), good material robustness (%5.6) için dikkate değer bir hassasiyet gösterdiğini söylemişlerdir.

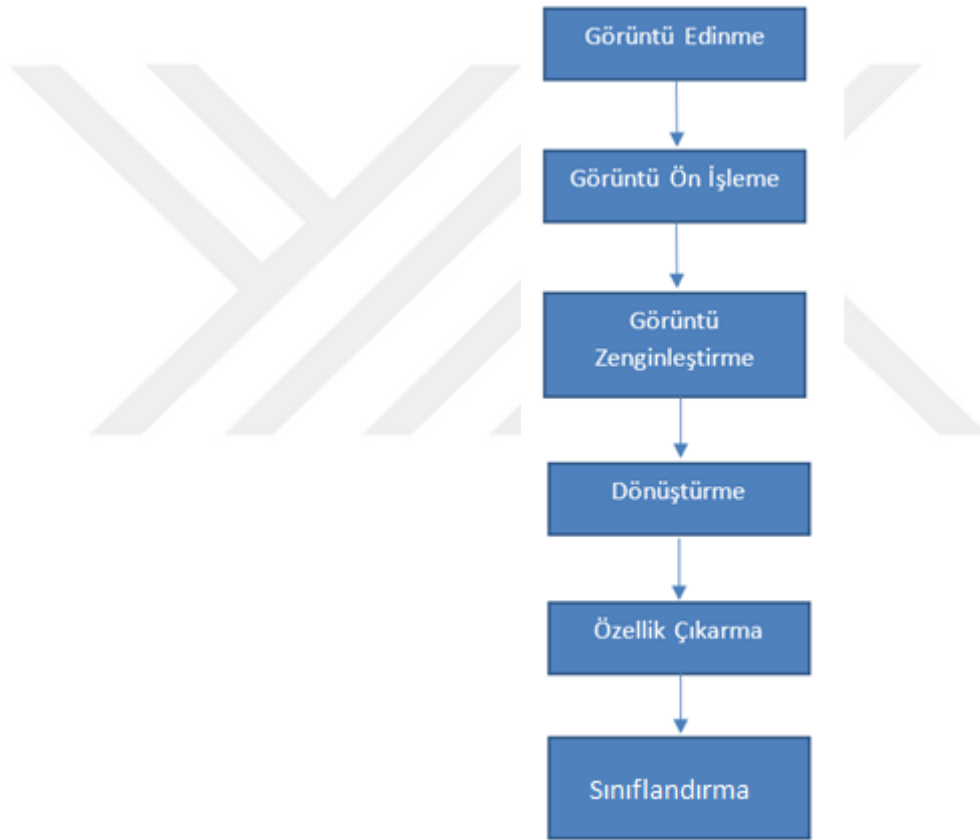
Nogueira et al. (2014) sahte parmak izi tespiti için özellik çıkarma yöntemlerinden Convolutional Networks with random weights (rasgele ağırlıklara sahip konvolüsyon ağları) ve Local Binary Patterns (LBP) tekniklerini kullanmışlardır. Veri seti olarak canlılık tespiti yarışmasında kullanılan LivDet 2009, 2011, 2013 veri setleri kullanılmıştır. Veri kümesi büyütme uygulanarak testleri yapmışlardır. Eğitim aşamasında yavaş ve tasarım açısından LBP'den daha karmaşık olan CN (konvolüsyon ağları) ortalama %4.71 ile en iyi performansa sahip olduğunu sunmuşlardır.

Marasco et al. (2016) sensörler üzerinde sahte parmak izi saldırılarına (Presentation Attack Detection (PAD)) karşı evrimsel sinir ağlarının performanslarını karşılaştırmışlardır. LivDet 2009, 2011 ve 2013 veri tabanlarında bulunan farklı sensörlerden alınmış ecoflex, gelatin, latex, modasil woodglue ile yapılmış ve canlı parmak izi görüntüleri üzerinde sunum saldırılarını değerlendirmek için ISO/IEC 30107 ölçümlerini kullanmışlardır. Karşılaştırdıkları CNN ağları GoogLeNet'in diğer CaffeNet ve Siamese'e göre daha iyi performans gösterdiğini ancak ağların adil olarak değerlendirilebilmesi için aynı kimliğe sahip canlı çiftleri dikkate alındığında oranların yükselebileceğini belirtmişlerdir.

Topcu ve Erdoğan (2019) güvenli parmak izi doğrulama sistemlerinde kullanılabilecek GMM (Generalized Method of Moments)-SVM (Support Vector Machine) tabanlı çözümler sunmuşlardır. GMM-SVM özellik vektörünü bir ikili bit dizisine dönüştürerek ikili vektörler arasında mesafe hesaplaması ile parmak izi eşleştirmesini hızlandırmışlardır. Bu çalışmada asimetrik bölgeye duyarlı asymmetric locality sensitive hashing (ALSH) yöntemini kullanmışlardır. Kullanılan yöntemin doğrulama performansı FVC2002 DB1A ve FVC2002 DB2A veri tabanlarında değerlendirerek parmak izi doğrulamada yaklaşımlarının yüksek bir doğruluğa sahip olduğunu ve mevcut sabit uzunlukta ayrıntı temsillerine göre avantajlarının olduğunu söylemişlerdir.

4. PARMAK İZİ GÖRÜNTÜ İŞLEME AŞAMALARI

Parmak izi tanıma sisteminde görüntünün kalitesi önemli olduğundan görüntünün iyileştirilmesi için sırasıyla görüntü edinme, görüntü ön işleme, özellik çıkarma ve sınıflandırma aracılığı ile eşleştirme yolları izlenir (Parvathy and Patil, 2018). İlgili aşamalar Şekil 4.1’de görülmektedir.



Şekil 4.1. Görüntü işleme aşamaları

4.1. Görüntü Edinme

Parmak izini elde etmede optik parmak izi yakalama cihazları, mürekkep baskı yöntemi, katı hal sensörleri ve ultrasonik tarama yöntemleri kullanılmaktadır. Optik cihazlar bir cam yüzeyden geçen lazer ışını ile alınan görüntünün sayısal olarak çevrilerek parmak izindeki girinti ve çıkıntıların ölçülmesine dayalı bir sistemdir. Katı hal

cihazlarında elektrik teknolojisi kullanılır. Kapasitif sensörlerin kullanıldığı bu sistemde algılama yüzeyinde oluşan değişken voltaj sayesinde görüntü elde edilir. Kapasitörde depolanan yük parmakla yüzeye uygulanan baskı ile değişir ve bu değişimin sonucu analog-dijital dönüştürücü tarafından kaydedilir. Ultrasonik taramada tarayıcıya yerleştirilen parmağa karşılık ultrasonik bir darbe üretilir bu darbenin bir kısmı emilir bir kısmı ise sensöre geri döner. Sensöre geri dönen parmak izinin detaylarıdır. Ultrasonik tarama sistemleri daha uzun süre tarama yaparak parmak izinin ayrıntılı üç boyutlu görüntüsünü çıkardığından kapasitif tarayıcılara göre daha güvenlidir. Diğer sistemlere göre kirli, çok kuru veya nemli parmaklarda daha iyi sonuç vermektedir. Ancak donanımın pahalı olması nedeni ile daha az kullanılmaktadır.

4.1.1. Parmak İzi Çeşitleri

Birbirinden bağımsız üç sırtın bir araya geldiği duruma triradius denir. Buluştukları noktaya ise üç nokta adı verilir. Triradius parmak izi incelemelerinde önemli bir kalıptır. Parmak izi kalıpları genel olarak spiral (Loop), helezon (Whorl), kemer (Arch) olmak üzere üç ana gruba ayrılır. En sık rastlanan parmak izi kalıpları spiral ve helezon tipleridir, kemer tipi ise daha az rastlanan parmak izi kalıbıdır.

Spiral Loop parmak izi bir triradius ve bir merkeze sahip parmak izi tipidir. Şekil 4.2’ de görüldüğü gibi sırt hatları sağdan ya da soldan yatık bir şekilde gelir ve merkez üstünden kıvrılarak aşağı doğru iner.



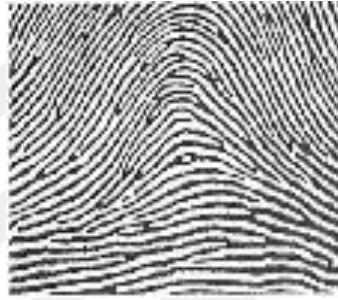
Şekil 4.2. Spiral (Loop) tipi parmak izi

Helezon (Whorl) parmak izi, genelde iki triradius ve bir merkez bulunan parmak izi tipidir. Helezon, parmak izi sırtlarının iç tarafında bulunan dairesel alandır (Parlakyıldız, 2014: 28). Şekil 4.3’ de görüldüğü gibi sırtlar merkez etrafında dairesel şekildedir (Baltacı, 2011: 9).



Şekil 4.3. Helezon (Whorl) tipi parmak izi

Kemer (Arch) tipi parmak izi az rastlanılan parmak izidir. Bu tipteki parmak izinde triradius bulunmaz. Şekil 4.4’ de görüldüğü gibi sırt hatları kemere benzer bir şekil oluşturur.



Şekil 4.4. Kemer (Arch) tipi parmak izi

4.1.2. Parmak İzi Özellikleri

Parmak izinin kimlik tespitinde kullanılmasının ana sebepleri değişmez ve değiştirilemez özelliği, benzemez ve benzetilemez özelliği ve tasnif edilebilir özelliğinin bulunmasıdır. Bu özellikler aşağıda açıklanmıştır.

- Değişmez ve Değiştirilemez Olma Özelliği: Anne karnında oluşan parmak izi değişmeden varlığını korur. Üst derideki herhangi bir bozulma parmak izi hatlarının değişmesine neden olmaz. Alt derideki hatlar tekrardan oluşan üst deride aynı hatların oluşmasını sağlar (Parlakyıldız, 2014: 31).
- Benzemez ve Benzetilemez Olma Özelliği: Tek yumurta ikizlerinin parmak izleri ve hatta bir kişinin her bir parmağına ait parmak izi birbirinden farklıdır. Dışardan yapılacak herhangi bir müdahale ile parmak izi başka bir parmak izine benzetilemez (Baltacı, 2011: 8).

- **Tasnif Edilebilir Özelliği:** Parmak izleri benzersiz olsa da sınıflandırılabilir özelliğe sahiptirler. Parmak izleri kendine ait özellikleri sayesinde sınıflandırılabilir ve saklanabilir. Sınıflandırılabilir özellikleri sayesinde karşılaştırmaya olanak sağlar.

4.2. Görüntü Ön İşleme

Parmak izi görüntüsünde bulunan gürültülerden kurtulmak için yapılan bir işlemdir. Parmak izi görüntüsünde, lekelere bağlı oluşan sırtlarda kopmalara, cildin esnekliği nedeniyle parmak izinin konumsal özelliğinin değişmesi sonucu düşük kontrastlı sırtlar görüntünün kalitesini bozar. Parmaktaki yaralar sırtlarda kopmalara neden olur ve bunların dışında terleme sonucunda paralel sırtların birbirine bitişik görünmesi de görüntünün düzgün işlenmesini engeller. Gürültü azaltma ve görüntü kalitesinin artırılması ile sonraki işlemler kolaylaştırılır. Ön işlemede geliştirme, referans noktası bulma, ikilileştirme (binarizasyon), inceltme ve ayrıntı çıkarımı teknikleri uygulanır.

4.3. Görüntü Zenginleştirme

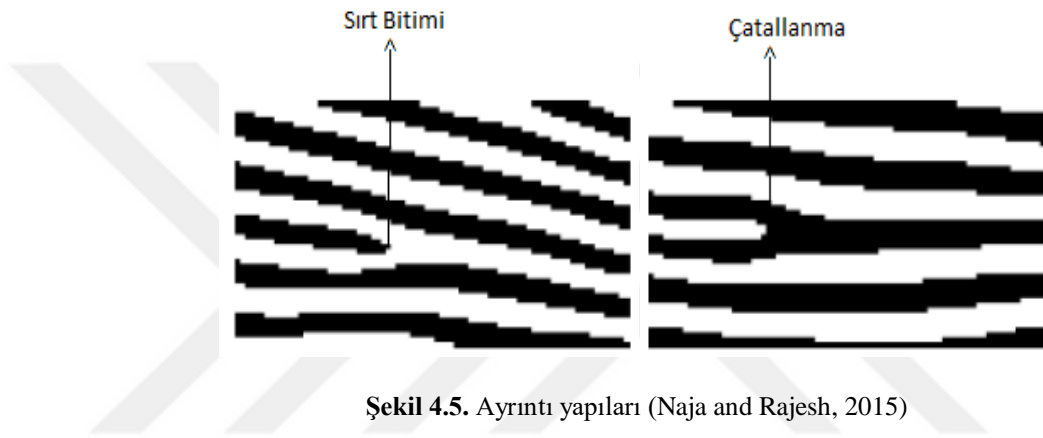
Histogram eşitleme, medyan filtreleme, geçiş filtreleme, Wiener filtreleme, Gabor filtreleme ve yön filtresidir. Ön işlemede görüntü öncelikle gri seviyeye dönüştürülür. Histogram eşitlemede çeşitli gri seviye değerlerinde düşük kontrastlı alanlarda yüksek kontrastlar üretilerek kaliteli görüntü elde edilir. Medyan filtreleme doğrusal olmayan bir filtrelemedir. Görüntüdeki piksel değerlerinin ortalaması alınarak merkez piksel değeri bulunur. Geçiş filtrelemede, parmak izi görüntüsünün kenarları keskinleştirilerek, bulanık görüntünün çıkarılmasıyla yüksek geçişli görüntü elde edilir. Wiener filtreleme görüntüdeki gürültü ve bulanıklığın giderilmesi için kullanılır. Gabor filtresi doğrusal bir filtredir. Ayarlanan frekans bilgisine göre istenilen sırt bilgisine ulaşılmasını sağlar. Yön filtresi görüntüyü frekans bantlarına bölen kenar algılama filtresidir.

Referans noktası bulma işlemi arka planda oluşan gürültülerden kurtulmak için yapılan bir işlemdir. Bu gürültüler sahte ayrıntı noktaları oluşturabileceğinden yanlış sonuç çıkarımlarına yol açar. Görüntü bölümlere ayrılarak her bölümün gradyanı bulunur. Sıralı iki bölümün gradyan değerlerinin ortalaması alınarak görüntünün konumu belirlenir. Bulunan bu referans noktasının etrafındaki uygun bölge kesilir.

İkileleştirmede görüntü gri seviyeden siyah beyaz görüntüye çevrilir. Belirlenen bir gri seviye eşik değerinin üzerindeki piksel değerleri için siyah altındaki piksel değerleri için beyaz olur.

İnceltme ikili görüntüdeki çıkıntıların genişliği tek bir piksele düşürmek için yapılır. Çıktı yine ikili bir görüntüdür. İnceltme işlemi sırasında dikkat edilmesi gereken önemli konu orijinal sırt yapısının değiştirilmemesidir.

Ayrıntı çıkarımında inceltilmiş görüntüden gelen ayrıntının sırt olup olmadığı, bir çatallanmanın olup olmadığı ve bu sırtların başlangıç ve bitiş noktalarının olup olmadığı belirlenir. Şekil 4.5’ de sırt bitimi ve çatallanma örnekleri verilmiştir. Görüntüdeki sahte ayrıntı noktaları iptal edilir.



Şekil 4.5. Ayrıntı yapıları (Naja and Rajesh, 2015)

4.3.1. Canny Kenar Belirleme Operatörü

Canny kenar bulma operatörü 1986 yılında John F. Canny tarafından bulunmuştur. Görüntülerde çeşitli kenarları tespit etmek için kullanılan Canny algoritması görüntüdeki güçlü ve zayıf kenarları birbirine bağlar. Diğer kenar bulma yöntemleri ile karşılaştırıldığında algoritmanın güçlü ve zayıf kenarlar arasında bir köprü kurması gürültülü görüntülerde en iyi sonucu vermekte ve daha az kandırılmaktadır (Jagadeesan and Duraiswamy, 2010).

Canny kenar bulma algoritmasında öncelikle Gauss filtresi kullanarak gürültü azaltma yapılır. Daha sonra güçlü ve zayıf kenarların tespiti için sobel maskeleri uygulanarak görüntü üzerindeki piksellerin kenar yönü ve gradyan büyüklüğü hesaplanır. Bu kenar bulma algoritması sonucu beyaz piksellerin orijinal görüntünün gerçek kenarlarına yakın olduğu ikili bir görüntü elde edilir. Canny operatörü, bitişik pikseller arasında devamlılık sağlayarak tek bir piksellik görüntüler oluşturur. Şekil 4.6’da parmak izi görüntüsünün canny algoritması uygulandıktan sonra kenarları belirlenmiş parmak izi görüntüsü verilmiştir.



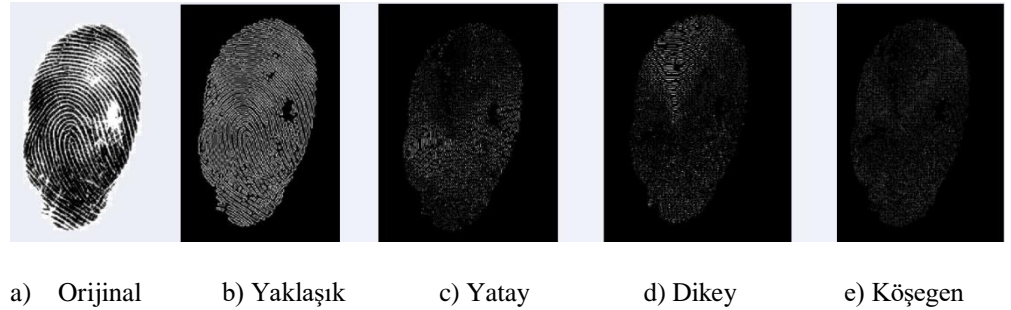
Şekil 4.6. Parmak izi görüntüsüne Canny algoritması uygulandıktan sonraki parmak izi görüntüsü

4.4. Dönüştürme

Dalgacık dönüşümü verileri tam olarak analiz etmek için kullanılan, bir sinyale ait zaman-frekans analizini, dalgacıklar yardımıyla gerçekleştirilen yöntemdir. Dalgacık dönüşümü, sinyali uzamsal alandaki sonlu enerjiyle, ortogonal modüler uzamsal alandaki standart olarak bir fonksiyon kümesine ayırır. Sonra, modüler uzaysal domeninde ki sinyalin özellikleri analiz edilir. Dalgacık dönüşümü, frekans ve zamanın daha iyi yerel kapasitesine sahip modüler uzaysal alan ve zamanlama alanlarındaki işlevi analiz edebilir.

Böylelikle görüntü ayrışabilir dört alt resme indirgenmektedir ve Şekil 4.7’de bir örneği verilmiştir.

Dalgacık dönüşümü, görüntüyü piksel bloklarından daha verimli şekilde depolanabilen bir dizi dalgacığa dönüştürür yani bir sinyali bir dizi temel fonksiyona ayrıştırır (Gupta and Choubey, 2015).



Şekil 4.7 Örnek parmak izi dönüşüm görüntüleri

Çalışmada tek seviyeli 2-D dalgacık ayrışması hesaplanarak sıkıştırma tekniği kullanılmıştır. Matlab ortamında kullanılan dwt2 fonksiyonu ile yatay, dikey ve diyagonal matrisleri hesaplanmıştır. Kullanılan 2 boyutlu dalgacık dönüşüm fonksiyonu, tek boyutlu dalgacık ve ölçekleme fonksiyonlarının tensörü alınarak elde edilmiştir. Önerilen teknik ile görüntü önce alt bantlara ayrılır yani katsayılara ayrılır. Daha sonra bu katsayılar bir eşik değeri ile karşılaştırılır. Eşik altındaki katsayılar sifıra ayarlanır ve eşik değerinin üzerindeki katsayılar sıkıştırılarak kodlanır.

4.5. Özellik Çıkarma

Özellik çıkarımı ikilileştirilmiş ve inceltilmiş görüntü üzerinde yapılır. Çeşitli algoritmalar kullanılarak ayrıntı özelliklerinin çıkarılması işlemidir. Ayrıntı noktaları parmak izinde bulunan sırtlar ve vadilerden oluşur. Parmak izi özellik çıkarımında global ve lokal yapılar belirlenir. Global seviyedeki yapılar kemerler, halkalar ve döngülerdir. Lokal seviyedeki yapılar çıkıntı sonları ve çatallanmalardır. Parmak izi tanıma ve sınıflandırma algoritmaları genelde özellik çıkarma aşamasına ihtiyaç duyar. Özellik çıkarımında kullanılan teknikler: çekirdek matrisiyle yatayda ve dikeyde kenar yakalama tekniği olan Sobel tekniği, çekirdek matrisi 90 derece döndürülerek kenar bulma işlemi yapan Robert tekniği, sobel filtresi gibi davranan Prewitt tekniği, hataları azaltmak için en iyi kenar detektörünü kullanan Canny tekniği'dir.

Bu çalışmada ayırt edici özellikleri elde edebilmek için entropi ve varyans hesaplamaları ile özellik çıkarma teknikleri kullanılmıştır.

Entropi gri tonlamalı görüntüyü sayısal bir dizi olarak belirtir. Görüntülerde piksellerin olasılık değerlerini hesaplarken entropi kullanılır Giriş görüntüsünü karakterize etmek için kullanılabilir istatistiksel bir rastgele ölçümdür yani entropi görüntü bilgilerinin niceliksel bir ölçüsüdür. Eğer görüntümüz iki boyuttan fazla ise bunu renkli bir görüntü olarak değil, çok boyutlu gri tonlamalı bir görüntü olarak kabul eder. Bu çalışmada parmak izi görüntüsünün dalgacık dönüşümü ile piksel değerlerinin dağılımı hesaplandıktan sonra entropi olasılığı hesaplanmıştır. Entropi filtresi gri tonlamalı görüntüdeki piksel değerlerinin dağılımındaki küçük değişimleri tespit edebilir.

Varyans bir sayı kümesinin ne kadar yayıldığıнын bir ölçüsüdür. Görüntü işlemede kenar konumunu belirlemek için kullanılır. Sayıların hesaplanan ortalamadan

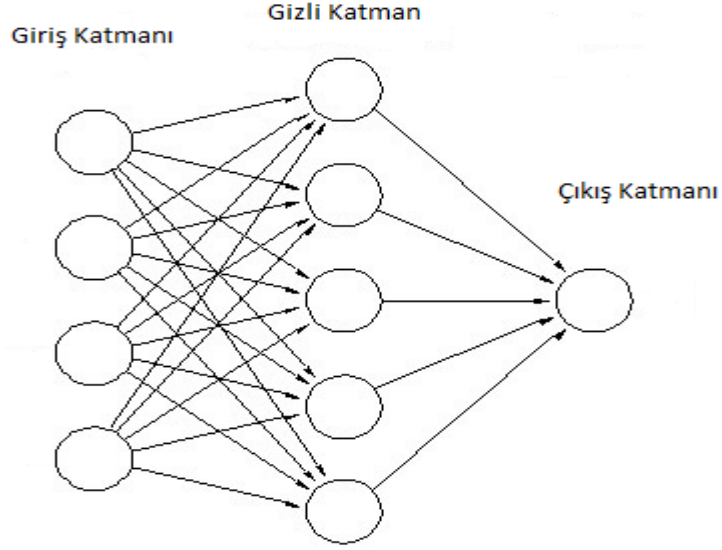
ne kadar uzak olduğunu verir ve sayıların olasılık dağılımını tanımlar. Aslında varyans, piksel değerlerinin yayılımı hakkında bilgi verir. Elde edilen varyans görüntüsü, standart sapmaların kareleri olan giriş veya çıkış görüntülerindeki varyansların bir görüntüsüdür. Bu çalışmada görüntülerin varyansı, iki görüntü arasındaki yapısal benzerliğin bir kalite ölçüsü olarak kullanılmıştır.

4.6. Sınıflandırma

Parmak izi görüntüsünün veri tabanına göre karşılaştırma işleminin yapılmasıdır. Sınıflandırma sırasında ayrıntı'ya göre ya da desene göre iki farklı teknik kullanılır. Desen eşleştirmede iki görüntü karşılaştırılır ve benzerliklerine bakılır. Ayrıntı'ya dayalı eşleştirmede her bir noktanın konumuna ve yönüne bakılır. Parmağın farklı şekillerde görüntüsünün yakalanması, değişen cilt durumu gibi durumlara karşı ayrıntı'ya dayalı eşleştirme daha güvenilirdir. Bu çalışma içerisinde ön işlem aşamasında nitelik çıkarılmasını gerektiren SVM tekniği ve nitelik çıkarımını kendi içinde gerçekleştiren CNN makine öğrenmesi tekniği kullanılarak karşılaştırılmıştır. SVM tekniğinin sınıflandırma başarımının ölçülmesi adına aynı zamanda CNN sınıflandırıcısı ile elde edilen nitelikler SVM ile sınıflandırılarak hibrit yaklaşım incelenmiştir. Aşağıda sınıflandırma teknikleri anlatılmıştır.

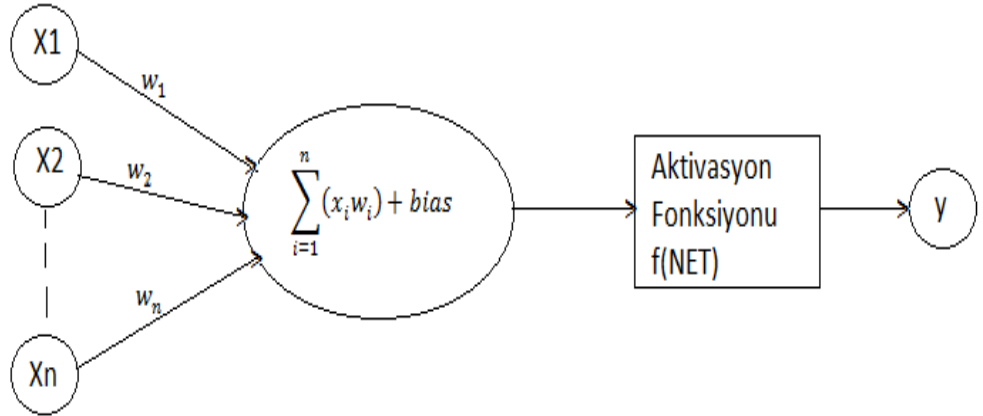
4.6.1. Geleneksel Yapay Sinir Ağları

Yapay sinir ağları, makine öğrenmesinde kullanılan temel araçlardan biridir. İnsan beyin yapısına benzer. Sinir ağları girdi katmanı, gizli katman ve çıkış katmanından oluşur. Bu katmanlar birbirine bazı ağırlık değerleri ile bağlıdır. Giriş katmanından gelen veriler bu ağırlıklarla çarpılıp transfer fonksiyonunda toplamları alınarak ağırlık performansına etkisi olan bir aktivasyon fonksiyonundan geçerek çıkış katmanına verilir. Paralellik, öğrenilebilirlik, hata toleransı, uyarlanabilirlik, genelleme, doğrusal olmama yapay sinir ağlarının özelliklerindedir. Yapay sinir ağları görüntü işlemede, ses tanıma, elle yazılmış karakterlerin tanınması, yüz tanıma, ses tanıma, parmak izi, imza analizi, borsa tahmini gibi uygulamalarda kullanılır. Şekil 4.8'de ileri beslemeli yapay sinir ağı yapısı görülmektedir.



Şekil 4.8. Yapay Sinir Ağı Yapısı

Şekil 4.9’de yapay sinir ağı nöron yapısı içerisinde yer alan: X_1, X_2, \dots, X_n sisteme giriş değerleri, w_1, w_2, \dots, w_n ilgili girişlere atanan ağırlık değerleri olmak üzere her bir giriş kendisine atanan ağırlık değeri ile transfer fonksiyonunda değerlendirilerek aktivasyon fonksiyonundan geçirilir.



Şekil 4.9. Yapay Sinir Ağı Nöron Yapısı

Bir Yapay Sinir Ağları içerisinde problemin doğasına göre farklı transfer fonksiyonlarını kullanmak mümkündür. Sıklıkla kullanılan birkaç aktivasyon fonksiyonuna ait denklemler, grafikler ve değer aralıkları Çizelge 4.1 içerisinde yer almaktadır (Sharma S, 2017).

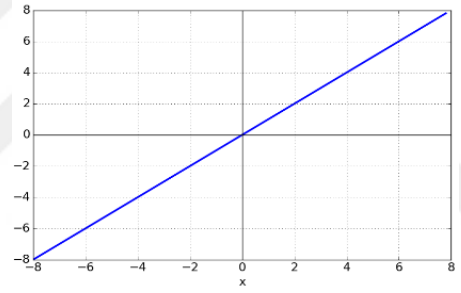
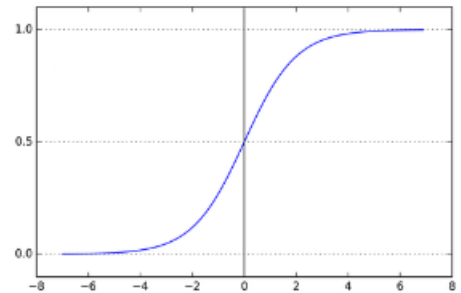
Bir yapay sinir ağı içerisine atanan ağırlıklar o yapay sinir ağı sonucunda elde edilecek çıkış değerlerini doğrudan etkiler. Yapay sinir ağı eğitim algoritmalarının

çoğu ağırlıkları rastgele küçük aralıklarda olacak biçimde atar. Bu aralıklara örnek olarak $[-1, 1]$, $[-3, 3]$ aralıkları verilebilir (Arı ve Berberler, 2017). Çeşitli iterasyonlar sonucunda ağırlık değerleri en iyi sonucu elde edecek biçimde güncellenir.

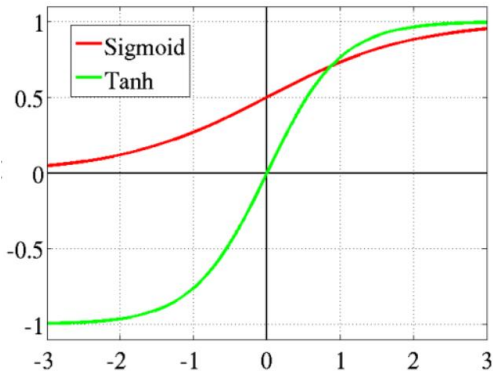
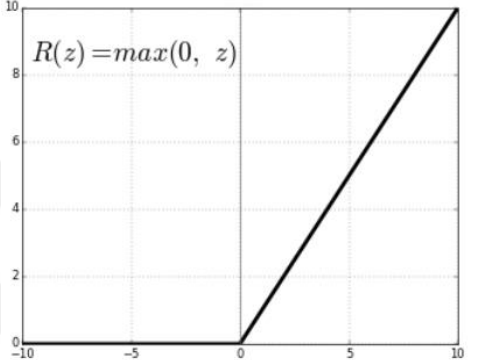
Global minimum elde edilmek istenirken elde edilen sonuç ile önerilen sonuç arasındaki kıyaslamada yanlış sonuçlar elde edilebileceği gibi yerel minimumda takılma da olabilir. Gerçek çıkış değeri y , tahmin edilen çıkış değeri \hat{y} olmak üzere; gerçek çıkış değeri ve tahmin edilen çıkış değeri arasındaki farkın hesaplanmasında genellikle Ortalama Karesel Hata (Mean Square Error) yöntemi kullanılır. İlgili yöntem Denklem 4.1’de yer almaktadır.

$$MSE = \frac{1}{N} \sum_{i=1}^N (\hat{y}_i - y_i) \quad (4.1)$$

Çizelge 4.1. Aktivasyon Fonksiyonları ve Denklemleri

Fonksiyon Adı	Denklem	Grafik	Değer Aralığı
Lineer Fonksiyon	$f(x) = x$		$(-\infty, \infty)$
Sigmoid Fonksiyonu	$f(x) = \frac{1}{1 + e^{-x}}$		$(0,1)$

Çizelge 4.1. (devam)Aktivasyon Fonksiyonları ve Denklemleri

Hiperbolik Tanjant Fonksiyonu	$f(x)$ $= \tanh(x)$ $= \frac{2}{1 + e^{-x}}$ $- 1$		$(-1,1)$
ReLU	$f(x)$ $= \max(0, x)$		$(-\infty, \infty)$

4.6.1.1. İleri Beslemeli Yapay Sinir Ağları

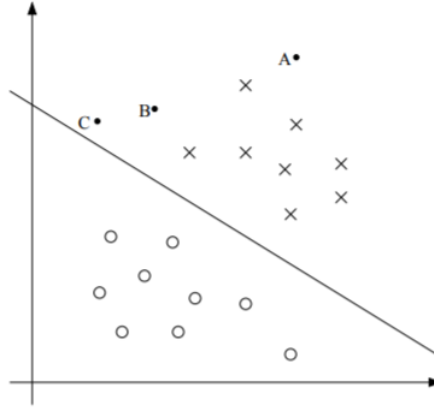
İleri besleme terimi bir yapay sinir ağının nasıl işlediğini açıklar. İleri beslemeli yapay sinir ağları, birimler arasındaki bağlantıların bir döngü oluşturmadığı sinir ağlarıdır. Tek yönlü bir akış vardır. Çıkış katmanı hariç her bir katman bir sonraki katmanla bağlantı gerçekleştirirken, geriye yönelik bağlantıya sahip değildir. Bilgi önce giriş katmanından, sonra gizli katmandan son olarak çıkış katmanından geçerek ilerler.

4.6.1.2. Geri Beslemeli Yapay Sinir Ağları

Geri beslemeli yapay sinir ağlarında hem ileri hem de geri yönde bir akış söz konusudur. Çok fazla giriş ve çıkış verisi varsa ve bunların çıkış verisiyle nasıl ilişkilendirilmesi gerektiği bilinmiyorsa, problem çok karmaşıksa, girdi ve çıktı parametreleri zamana bağlı olarak değişiyorsa geri beslemeli yapay sinir ağı kullanılır. İstenilen çıkışı elde edebilmek için giriş verilerinin iç ağırlıklarını değiştirerek bir fonksiyon modeli oluşturulur. Sistem denetimli öğrenme ile eğitilir.

4.6.2. Destek Vektör Makinaları

Destek Vektör Makinaları (Support Vector Machines) (DVM - SVM) hem sınıflandırma hem de regresyon için kullanılan denetimli makine öğrenme algoritmasıdır. SVM genelde sınıflandırma için kullanılır. Veri setinde her bir ögenin özelliklerine göre n boyutlu uzayda bir koordinat düzleminde gösterimi yapıldıktan sonra bu noktaların iki gruba ayırma işleminin nasıl yapılacağını belirler. SVM iki sınıfı en iyi şekilde ayıran bir sınır çizer. Kısaca farklı sınıf üyeliklerine sahip nesnelere kümesi arasında ayırım yapan bir düzlemdir. Farklı sınıf etiketlerinin durumlarını ayıran çok boyutlu bir alanda aşırı düzlem (hyperplanes) oluşturularak sınıflandırma yapan bir yöntemdir. A, B ve C verilerinin yer aldığı ve Destek Vektör Makinaları kullanılarak gerçekleştirilecek bir sınıflandırma işlemine ait çizim Şekil 4.10'de yer almaktadır.



Şekil 4.10. A, B ve C verilerinin sınıflandırma işleminin düzlemsel gösterimi

Buna göre sınıflar aralarında bir aşırı düzlem oluşturulmasına imkan verecek biçimde ayrıştırılmıştır. Destek Vektör Makinası kullanılarak gerçekleştirilen sınıflandırma işlemine ait denklemler Denklem 4.2, Denklem 4.3 ve Denklem 4.4'te yer almaktadır. İlgili denklemlerde yer alan n: eğitim amaçlı kullanılan veriyi, c: eşleştirme yapılacak sınıf sayısını, göstermektedir. Buna göre herhangi bir sınıf içerisine atama yapmak amacıyla atama yapılacak sınıfın içerisinde yer alan veriler pozitif değerlere taşınırken diğer değerler negatif ağırlığa yığılanırlar.

$$\min_{w_j, b_j} \frac{1}{2} \|w_j\|_2^2 + C \sum_{i=1}^n \xi_i^j \quad (4.2)$$

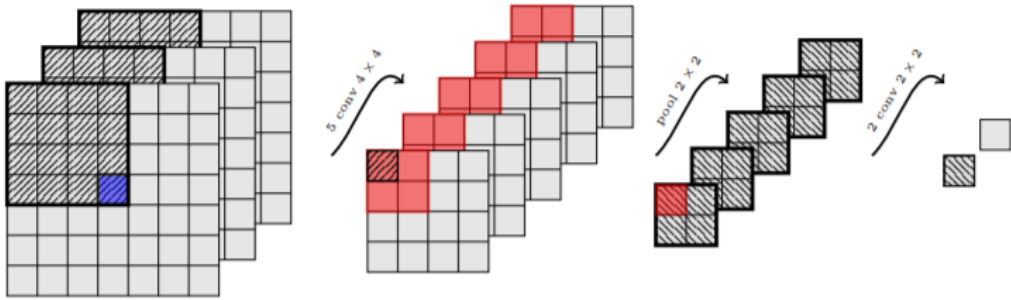
$$s. t. \quad w_j^T x_i + b_j \geq 1 - \xi_i^j, \quad \text{if } y_i = j \quad (4.3)$$

$$w_j^T x_i + b_j \leq -1 \xi_i^j, \text{ if } y_i \neq j \quad \xi_i^{jk} \geq 0 \quad (4.4)$$

Böylelikle pozitif ve negatif değerlerden oluşan iki farklı değer kümesi oluşturularak sınıflandırma işlemi gerçekleştirilir. Anlatılan biçimde ikili sınıflandırma amacıyla kullanılan Destek Vektör Makinaları olduğu gibi çoklu sınıflandırma amacıyla kullanılan Destek Vektör Makinaları da mevcuttur.

4.6.3. Evrişimsel Sinir Ağı

Evrişimsel Sinir Ağı (Convolutional Neural Networks - CNNs), ileri beslemeli yapay sinir ağları gibidir. Girdi ve çıktı verileri arasındaki doğrusal olmayan ilişkiyi modelleyebilirler. Evrişimsel Sinir Ağları, yapay sinir ağlarının resim düzenleme amacıyla oluşturulmuş geliştirilmiş halidir. Katmanları genişlik, yükseklik ve derinlik olmak üzere üç boyutlu nöronlara sahiptir. Evrişimsel Sinir Ağları mimarisinde üç ana katman kullanılır. Bu katmanlar; konvolüsyon katmanı, ortaklama (pooling) katmanı ve tam bağlı katman'dır. Her bir birime ait çıkışlar 2 boyutlu nitelik haritaları oluşturur. Her bir nitelik haritası resmin tümüne bir konvolüsyon (veya ortaklama) filtresi uygulanması sonucu oluşmaktadır. Ortaklama katmanından sonra daima bir lineer olmayan aktivasyon fonksiyonu kullanılmaktadır (Pinheiro and Collobert, 2014). Şekil 4.11' de basit bir evrişimsel ağ görülmektedir. Verilen resimde mavi ile gösterilen alanın sınıflandırılması amacıyla gerçekleştirilen bir dizi konvolüsyon ve ortaklama işlemi görülmektedir. Buna göre 5 adet 4x4 konvolüsyon, 1 adet 2x2 ortaklama ve son olarak tekrar 1 adet 2x2 konvolüsyon işlemi gerçekleştirilerek sınıflandırma işlemi gerçekleştirilmiştir.



Şekil 4.11. Evrişimsel Ağ

- **Konvolüsyon Katmanı (Convolution Layer):** Parametreleri öğrenen filtrelerden oluşur. Her bir filtre giriş hacminin genişliği ve yüksekliği boyunca kaydırılır ve her bir nokta filtrede denk geldiği noktadaki değerle çarpılarak

hesaplanır. Her konvolüsyon katmanda kullanılan filtrelerin her biri 2 boyutlu aktivasyon haritası üretir. Bu aktivasyon haritaları ile derinlik oluşturup çıkış hacmi üretilir. Denklem 4.5'te m çekirdek genişliği ve yüksekliği, h evrişim çıkışı, x giriş, w evrişim çekirdeğini göstermektedir (Ganegedana, 2018).

$$h_{i,j} = \sum_{k=1}^m \sum_{l=1}^m w_{k,l} x_{i+k-1,j+l-1} \quad (4.5)$$

- **Ortaklama Katmanı (Pooling Layer):** Alt örnekleme katmanı olarak da adlandırılır. Kullanılan filtre ile aynı boyuttadır ve giriş hacmine uygulanan filtrenin dolaştığı her bölgedeki maksimum sayıyı çıkarır. Bu katman giriş hacminin uzamsal boyutunu yani derinliğini değiştirerek büyük ölçüde azaltılır. Böylece parametrelerin ya da ağırlıkların miktarı azaltılarak maliyet azaltılır. Matematiksel formülü Denklem 4.6'da verilmiştir (Ganegedana, 2018).

$$h_{i,j} = \{x_{i+k-1,j+l-1} \forall 1 \leq k \leq m \text{ and } 1 \leq l \leq m \quad (4.6)$$

- **Tam Bağlı Katman:** Bu katman girdi hacmini alır ve sınıf sayısı boyutlu bir vektör oluşturur. Belirli bir sınıfa en güçlü şekilde bağlı olan ve belirli ağırlıklara sahip olan yüksek düzey özelliklere bakarak girdinin farklı sınıflar için olasılığı hesaplanır.

CNN görüntüler üzerinde doğru tahminler yaptığından genellikle görüntü tanımada kullanılır. CNN, standart ileri beslemeli yapay sinir ağlarına kıyasla küçük ve ucuz bir mimariye sahip olsa da, eğitiminde çok fazla hesaplama ve büyük etiketli veri seti gerektirir.

4.6.4. Hibrit Yaklaşım – CNN+SVM

Bu çalışmada iki denetimli sınıflandırma tekniği olan CNN ve SVM yöntemi birlikte kullanılarak parmak izi görüntülerinden sahte parmak izlerinin tespiti yapılmıştır. Evrişimsel sinir ağı sınıflandırma görevini icra ederken aynı zamanda özellik çıkarma görevini de yerine getirir. Bu hibrit modelde, CNN eğitilebilir bir özellik çıkarıcı olarak çalışır ve SVM tanıyabilen sınıflandırıcı olarak çalışır. Özellik çıkarma tanıma sistemlerinde önemli bir başarı faktörüdür. SVM sınıflandırıcısı için CNN ağının çıkış değeri bir özellik olarak değerlendirilir. Şekil 4.12 hibrit CNN-SVM modelinin yapısını gösterir. CNN ağı birkaç periyod eğitilir ve daha sonra SVM sınıflandırıcısı çıkış katmanını değiştirir. SVM, CNN ağının çıkış katmanını özellik vektörü olarak alır ve sınıflandırma işlemini gerçekleştirir. Burada CNN

sınıflandırıcısının kullanılma amacı giriş görüntüsünün belirgin özelliklerini otomatik olarak çıkarmasıdır.



Şekil 4.12. Hibrit CNN-SVM modelinin yapısı



5. ARAÇLAR VE YÖNTEMLER

Çalışmada kullanılan bilgisayar Intel (R) Core (TM) i5-3317U işlemciye ve 1.70 GHz işlemci hızına, 4 GB ön belleğe sahiptir. Çalışmanın yürütüldüğü bilgisayar da CPU (Merkezi İşlem Birimi) kullanıldığından görüntülerin işlenmesi sırasında zaman bakımından donanımında GPU (Grafik İşleme Ünitesi) bulunan bilgisayara göre daha uzun sürede sonuç alınmıştır. Sınıflandırma Matlab ortamında hazır fonksiyonlar kullanılarak yapılmıştır.

5.1. Veri Analizi

Bu çalışma içerisinde canlılardan alınan parmak izi ile üretilen sahte parmak izlerinin ayrıştırılması hedeflenmiştir. Bu amaçla içerisinde gerçek ve sahte parmak izleri içeren LivDet2015 veri kümesi kullanılmıştır. İlgili veri kümesi 2 yıl aralıkla gerçekleştirilen “Canlılık Tespiti – Liveness Detection” veri kümeleri oluşturma yarışmaları sonucunda 2015 yılında oluşturulmuştur. Canlılık tespiti veri kümesi oluşturma yarışmaları 2 yıl aralıklarla gerçekleştirilmektedir (Marcialis et al., 2009; Yambay et al., 2011; Ghiani et al., 2013; 2017). Bu çalışmanın gerçekleştirilebilmesi için kullanıma açık olan en yeni veri kümesi LivDet2015 tercih edilmiştir. LivDet2015 veri seti, eğitim ve test olmak üzere iki parçadan oluşmaktadır. Ancak 2019 yılı itibarı ile veri kümesinin yalnızca eğitim kısmı araştırmacılara açılmıştır. Bu nedenle bu çalışma içerisinde LivDet2015 veri seti içerisinde yer alan eğitim kümesi kullanılmış; eğitim kümesinin bir kısmı bölünerek test işlemleri için ayrılmıştır.

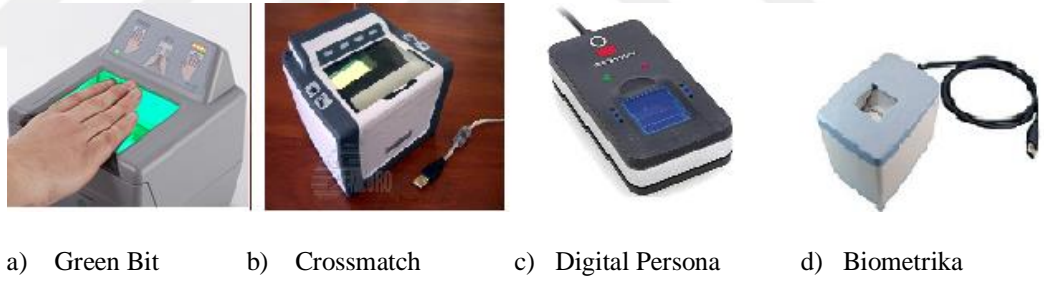
LivDet2015 eğitim kümesi gerçek ve sahte parmak izleri olmak üzere iki temel kısımdan oluşmaktadır. Sahte ve gerçek parmak izleri Green Bit, Biometrika, Digital Persona ve Crossmatch olmak üzere dört farklı şekillerde toplanmış, dört farklı kategoride yer almaktadır. İlgili veri kümeleri içerisinde yer alan veri sayıları Çizelge 5.1’de yer almaktadır. Parmak izi görüntüsü toplamada kullanılan cihazlar optik sensör yöntemini kullanmaktadır. Optik sensör yöntemini kullanan tarayıcıya yerleştirilen

parmak bir ışık kaynağı ile aydınlatılarak parmak izi ayrıntılarının daha net görünmesini sağlar.

Çizelge 5.1. LivDet2015 gerçek ve sahte parmak izi görüntü sayıları

Veri Kümesi	Gerçek parmak izi	Body Double	Ecoflex	Oyun Hamuru	Gelatine	Latex	WoodGlue
Green Bit	1000	-	250	-	250	250	250
Digital Persona	1000	-	250	-	250	250	250
Crossmatch	1510	494	498	481	-	-	-
Biometrika	1000	-	250	-	250	250	250

Parmak izi görüntülerinin elde edildiği cihazlar Şekil 5.1’de verilmiştir. Kullanılan parmak izi okuyucu cihazlarından “a” green bit cihazının görüntüsünü “b” crossmatch cihazının görüntüsünü “c” digital persona cihazının görüntüsünü “d” biometrika cihazının görüntüsünü göstermektedir.



a) Green Bit b) Crossmatch c) Digital Persona d) Biometrika

Şekil 5.1. Parmak izi görüntülerinin elde edildiği cihazlar

LivDet2015 içerisinde yer alan parmak izleri gerçekle uyumlu olması adına parmakların ıslak, kuru olduğu durumlarda ve farklı basınç ortamlarında kaydedilmiştir (Mura et al., 2015). LivDet 2015 veri seti içerisinde green bit, crossmatch, digital persona ve biometrika cihazlarından elde edilen gerçek ve sahte parmak izi görüntü boyutları sırasıyla 500x500 px, 749x799 px, 324x252 px ve 1000x1000 px’dir. Parmak izi görüntülerinin elde edildiği cihazların modelleri, elde edilen görüntü boyutları, cihazın çalışma sıcaklık aralığı ve nem toleransı Çizelge 5.2 ‘de verilmiştir.

Çizelge 5.2. LivDet2015 parmak izi görüntülerinin elde edildiği cihazların özellikleri

Cihaz	Model	Görüntü Boyutu (px)	Sıcaklık Değeri	Nem Toleransı
Green Bit	DactyScan26	500x500	+5 - +40 °C	% 10 - %90
Crossmatch	L Scan Guardian	749x799	+2 - +49 °C	% 10 - %90
Digital Persona	U.are.U 5160	324x252	-10 - +60 °C	% 20 - %90
Biometrika	HiScan-PRO	1000x1000	+5 - +45 °C	% 10 - %90

Bu çalışmada donanım yetersizliği ve görüntülerin bir kısmında bulunan bozukluklar nedeniyle LivDet2015 veri seti içerisinde bulunan parmak izi görüntüleri SVM, CNN ve CNN+SVM algoritmalarında sınıflandırılmadan önce düzenlenmiştir. Kullanılan veri seti Çizelge 5.3’de yer almaktadır. Görüntü boyutu olarak büyük olması nedeniyle Biometrika veri seti çalışma içerisinde kullanılmamıştır.

Çizelge 5.3. LivDet2015 çalışmada kullanılan gerçek ve sahte parmak izi görüntü sayıları

Veri Kümesi	Gerçek parmak izi	Body Double	Ecoflex	Oyun Hamuru	Gelatine	Latex	WoodGlue
Green Bit	997	-	250	-	250	250	250
Digital Persona	1000	-	250	-	250	250	250
Crossmatch	250	30	30	190	-	-	-

Çalışma içerisinde parmak izlerinin doğal niteliklerini ön işlem aşamasında analiz etmeden sınıflandırma yapılması hedeflenmiştir. Bu amaçla ön işlem aşaması kullanılmaksızın yüksek performans ile ham parmak izi görüntülerinden sahte olanların ayrıştırılması amaçlanmıştır. Ham parmak izi görüntüsünden sahte olan parmak izinin yakalanması adına SVM, CNN ve her iki makine öğrenmesi tekniğini birleştirerek hibrit bir yaklaşım CNN+SVM kullanılmış, performans analizleri gerçekleştirilmiştir.

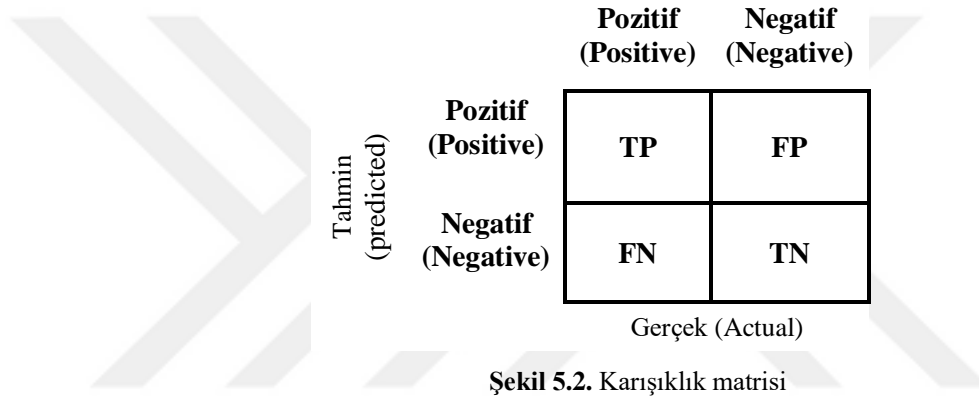
Çalışmada kullanılan CNN yapısında 3x3 konvolüsyon katmanından oluşur ve sırasıyla 8x8, 16x16, 32x32’lik filtreler kullanılmıştır. Her bir konvolüsyon katmanından sonra ReLu (Rectified Linear Unit) aktivasyon fonksiyonu kullanılmıştır.

ReLU katmanı giriş verisindeki negatif değerleri sıfır yapar. Matematiksel olarak Denklem 5.1’de ifade edilmiştir. Maksimum havuzlama katmanı 2x2 boyutunda ve aralık 2’dir.

$$f(x) = \begin{cases} 0, & x < 0 \\ x, & x \geq 0 \end{cases} \quad (5.1)$$

5.2. Performans Metrikleri

Kullanılan makine öğrenmesi sınıflandırıcılarının performans analizi karışıklık matrisinde yer alan metrikler analiz edilerek değerlendirilmiştir. Şekil 5.2’de karışıklık matrisini açıklayan şekil verilmiştir.



Karışıklık matrisi makine öğrenmesi yöntemlerinin performans değerlendirmelerinin yapılmasını sağlayan doğru pozitif, yanlış pozitif, doğru negatif ve yanlış negatif olmak üzere dört temel metriği içermektedir:

- Doğru Pozitif (True Positive – TP): Sahte parmak izinin sahte olarak sınıflandırıldığı durum.
- Yanlış Pozitif (False Positive – FP): Gerçek parmak izinin sahte olarak sınıflandırıldığı durum.
- Doğru Negatif (True Negative – TN): Sahte parmak izinin gerçek olmadığını tespit edildiği durum.
- Yanlış Negatif (False Negative – FN): Sahte parmak izinin gerçek olarak sınıflandırıldığı durum.

Karışıklık matrisindeki metrikler kullanılarak SVM, CNN ile hibrit model CNN ve SVM'e ait kesinlik (precision), recall (sensitivity), doğruluk (accuracy), özgüllük (specificity), F1 skor (F1 score), Matthews korelasyon katsayısı (Matthews correlation coefficient) ve kappa değerleri hesaplanmıştır. İlgili değerler:

- Kesinlik (Precision): Sahte parmak izi olarak tespit edilen verilerin yüzde kaçının sahte parmak izi olduğunun ölçülmesini sağlar. Denklem 5.2'de precision hesaplama formülü verilmiştir.

$$\text{Kesinlik (Precision)} = \frac{TP}{TP+FP} \quad (5.2)$$

- Duyarlılık (Recall – Sensitivity): Sahte parmak izi olarak gerçekleştirilen başarılı tespitlerin oranının bulunmasını sağlayan ölçüttür. Denklem 5.3'de recall hesaplama formülü verilmiştir.

$$\text{Duyarlılık (Recall – Sensitivity)} = \frac{TP}{TP+FN} \quad (5.3)$$

- Doğruluk (Accuracy): Tüm değerlerin yüzde kaçının ait olduğu sınıfa uygun bir biçimde sınıflandırıldığını gösterir. Denklem 5.4'de accuracy hesaplama formülü verilmiştir.

$$\text{Doğruluk (Accuracy)} = \frac{TP+TN}{TP+FP+TN+FN} \quad (5.4)$$

- Özgüllük (Specificity): Yanlış sınıfa ait olduğu belirtilen değerlerin yüzde kaçının doğru olarak yanlış olarak sınıflandırıldığını gösteren ölçüttür. Denklem 5.5'de specificity hesaplama formülü verilmiştir.

$$\text{Özgüllük (Specificity)} = \frac{TN}{TN+FP} \quad (5.5)$$

- F1 Skor (F1 Score): kesinlik ve duyarlılığın harmonik ortalamasıdır. Denklem 5.6'de F1 skor hesaplama formülü verilmiştir.

$$\text{F1 Skor (F1 Score)} = \frac{2(\text{Precision}+\text{Sensitivity})}{(\text{Precision}+\text{Sensitivity})} \quad (5.6)$$

- Matthews Korelasyon Katsayısı (Matthews Correlation Coefficient - MCC): Makine öğreniminde ikili sınıflandırmaların kalitesinin bir ölçüsü olarak kullanılır. -1 ile +1 arasında değerler döndürür. Sonuç

+1'e yaklaştıkça tahminin iyi olduğu anlamına gelir. Denklem 5.7'da MCC hesaplama formülü verilmiştir.

$$MCC = \frac{TP*TN-FP*FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (5.7)$$

- Cohen's Kappa: Cohen'in Kappa modeli ilk olarak sosyal bilimler, biyoloji ve tıp bilimlerinde kullanılmıştır. Asıl amacı aynı olayı gözlemleyen iki veya daha fazla insanın anlaşma veya anlaşmazlık derecesini ölçmektir. Daha sonra uzman sistemler, makine öğrenmesi ve veri madenciliği alanlarında kullanılmaya başlanmıştır. Kullanılan modelin öngörülleri ve gerçekliği arasındaki anlaşma derecesini ölçer (Ben-David A, 2008). Karışıklık matrisinden elde edilen sonucun doğruluğunu ve gerçekliği belirleyen bir ölçüdür. Cohen'nin Kappa modeli iki model arasındaki anlaşma derecesini tahmin eder. Cohen'nin Kappa katsayısı [-1, 1] arasında değer alır. Kappa değeri ne kadar yüksekse, doğruluğun o kadar iyi olduğu anlamına gelir. Denklem 5.8'de kapa hesaplama formülü verilmiştir.

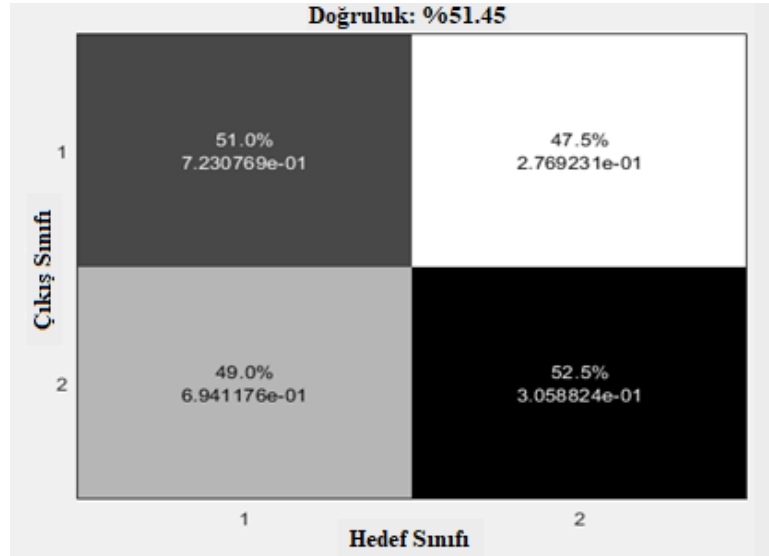
$$Kappa = \frac{\frac{(TP+TN)}{(TP+TN+FP+FN)} - \left[\frac{(TN+FP)(TN+FN)+(FN+TP)(FP+TP)}{(TP+TN+FP+FN)^2} \right]}{1 - \left[\frac{(TN+FP)(TN+FN)+(FN+TP)(FP+TP)}{(TP+TN+FP+FN)^2} \right]} \quad (5.8)$$

6. BULGULAR

Bu tez çalışması içerisinde gerçek ve gerçek olmayan parmak izlerinin ayrıştırılabilmesi adına gerçek olmayan parmak izlerini tespit eden bir biyometrik tanımlama sistemi oluşturulmuştur. Önerilen yöntemin sınanabilmesi adına içerisinde gerçek ve sahte parmak izlerini barındıran LivDet2015 veri kümesi kullanılmıştır. LivDet2015 veri kümesi içerisinde bulunan veriler; gerçek parmak izi verileri ve Crossmatch, Green Bit ve Digital Persona olmak üzere üç farklı kümede yer almaktadır. Veriler gerçek ve sahte olarak iki kümeye bölünmüş böylelikle gerçek ve sahte parmak izleri ayrıştırılmıştır. Bu amaçla ilk olarak veriler ön işlem aşamasında ikilileştirilmiştir. İkileştirilen parmak izi görüntülerine görüntüyü zenginleştirmek adına canny kenar belirleme operatörü ile işlem yapılmış, elde edilen görüntülere dalgacık dönüşümü uygulanmıştır. Görüntülerden niteliklerin çıkarılması amacıyla görüntülere ait entropi ve varyans değerleri hesaplanarak, nitelik matrisi oluşturulmuştur.

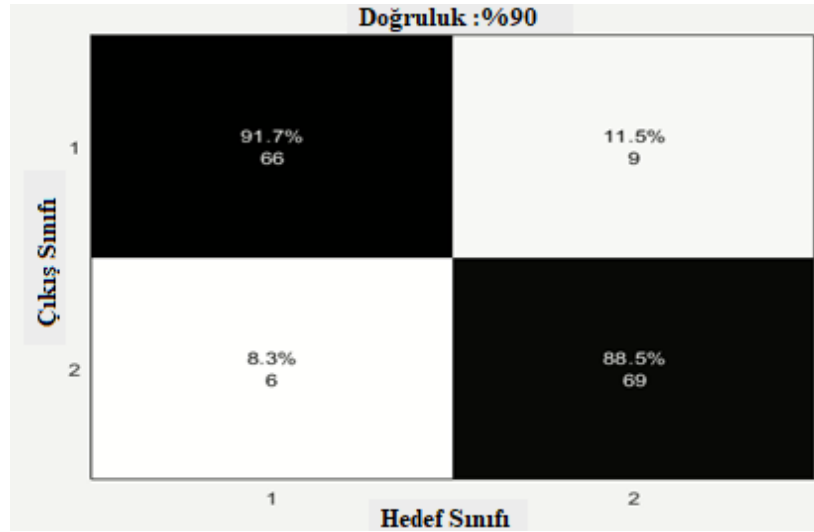
Nitelik matrisleri kullanılarak gerçekleştirilen eşleştirme aşamasında makine öğrenmesi tekniklerinden SVM, CNN ile CNN ve SVM yöntemlerinin birlikte kullanıldığı hibrit model çalıştırılmıştır. Sistemin tekrarlı çalıştırmalar sonucu elde edilen değerlerin ortalaması ve doğruluk – loss eğrileri tüm veri setleri için aşağıda verilmiştir.

Crossmatch veri seti SVM sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.1' de verilmiştir. Karışıklık matrisi kullanılarak hesaplanan değerler şöyledir; doğruluk : 0.5145, hata : 0.4855, duyarlılık : 0.7231, özgüllük : 0.3059, doğru pozitif : 0.7231, yanlış pozitif : 0.6941, yanlış negatif : 0.2769, doğru negatif : 0.3059, kesinlik : 0.5102, F1-score : 0.5983, MCC : 0.0319, kappa : 0.0290.



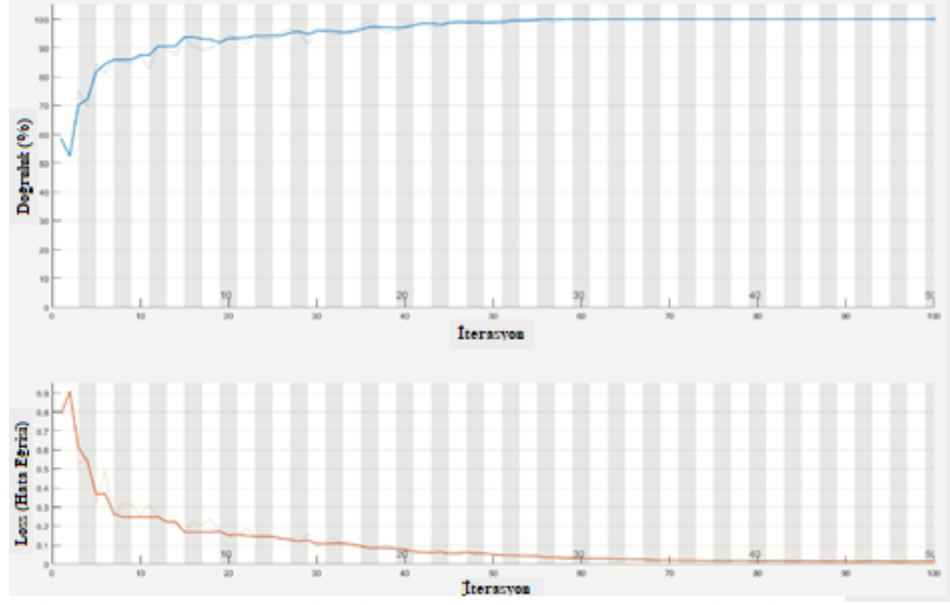
Şekil 6.1. Crossmatch veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

Crossmatch veri seti CNN sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.2’de verilmiştir. Sınıflandırma sonucu elde edilen performans değerleri; doğruluk : 0.90, hata : 0.10, duyarlılık : 0.88, özgüllük : 0.92, doğru pozitif : 66, yanlış pozitif : 6, yanlış negatif : 9, doğru negatif : 69, kesinlik : 0.9167, F1-score : 0.8980, MCC : 0.8006, kappa : 0.80 olarak hesaplanmıştır.



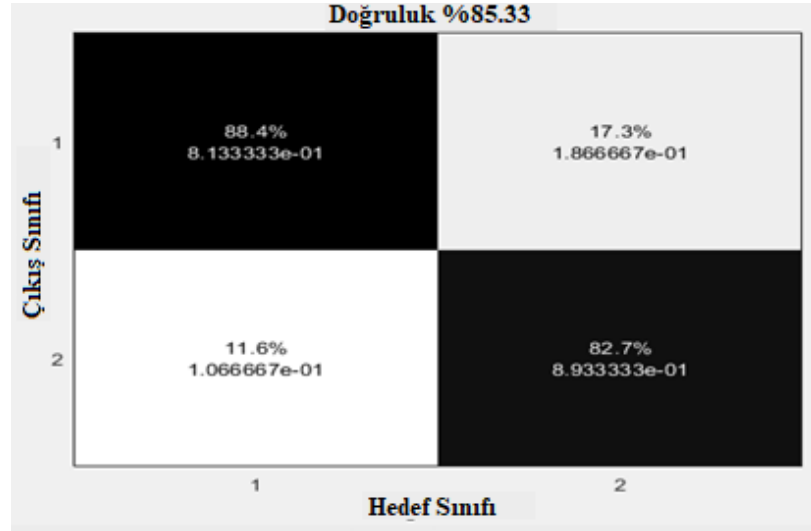
Şekil 6.2. Crossmatch veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

CNN sınıflandırıcısı ile sistemin tekrarlı çalışmaları sonucu elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.3’de gösterilmiştir. Burada loss eğrisi gerçek değerle tahmin edilen değer arasındaki farkı göstermektedir.



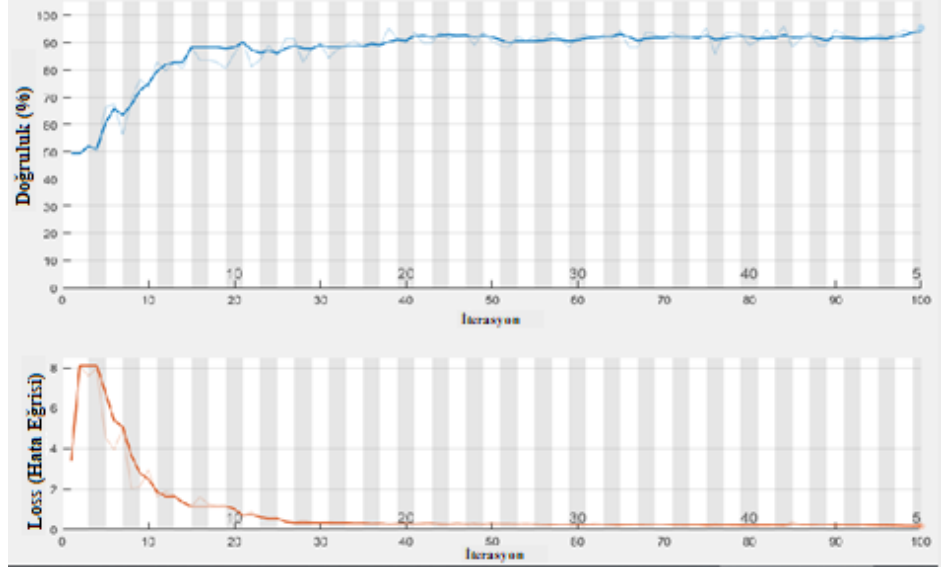
Şekil 6.3. Crossmatch veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi

Crossmatch veri setinin hibrit yöntem CNN+SVM ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.4’de verilmiştir ve performans değerleri; doğruluk : 0.8533, hata : 0.1467, duyarlılık : 0.8133, özgüllük : 0.8933, doğru pozitif : 0.8133, yanlış pozitif : 0.1067, yanlış negatif : 0.1867, doğru negatif : 0.8933, kesinlik : 0.8841, F1-score : 0.8472, MCC : 0.7089, kappa : 0.7067 olarak hesaplanmıştır.



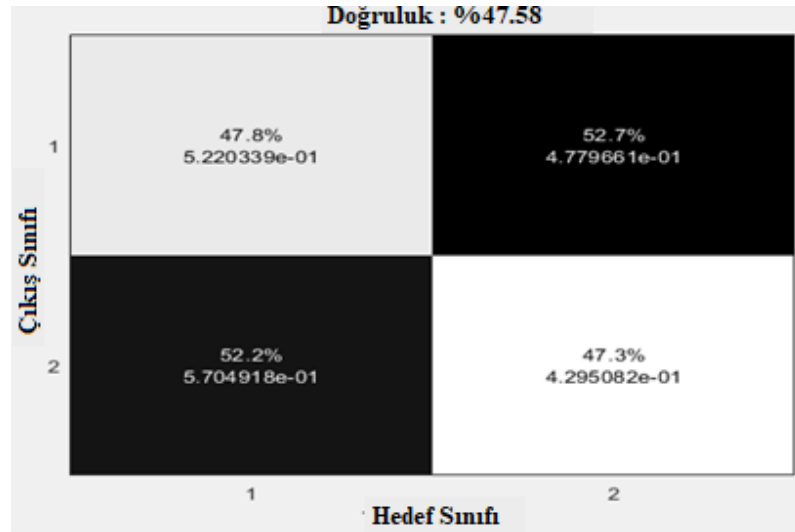
Şekil 6.4. Crossmatch veri seti hibrit yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

CNN+SVM sınıflandırıcısı ile eğitim sürecinde elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.5’de gösterilmiştir.



Şekil 6.5. Crossmatch veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi

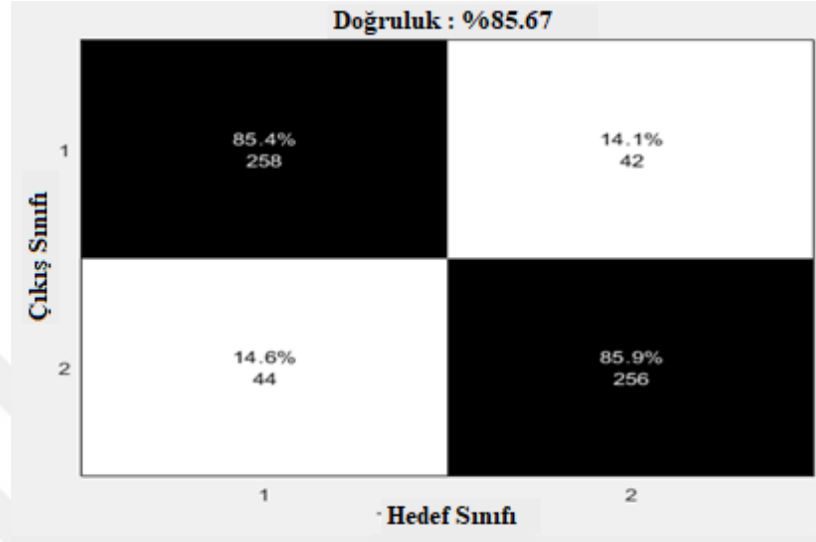
Digital persona veri seti SVM sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.6' de verilmiştir. Karışıklık matrisi kullanılarak hesaplanan değerler şöyledir; doğruluk : 0.4758, hata : 0.5242, duyarlılık : 0.5220, özgüllük : 0.4295, doğru pozitif : 0.5220, yanlış pozitif : 0.5705, yanlış negatif : 0.4780, doğru negatif : 0.4295, kesinlik : 0.4778, F1-score : 0.4990, MCC : 0.0487, kappa : 0.0462.



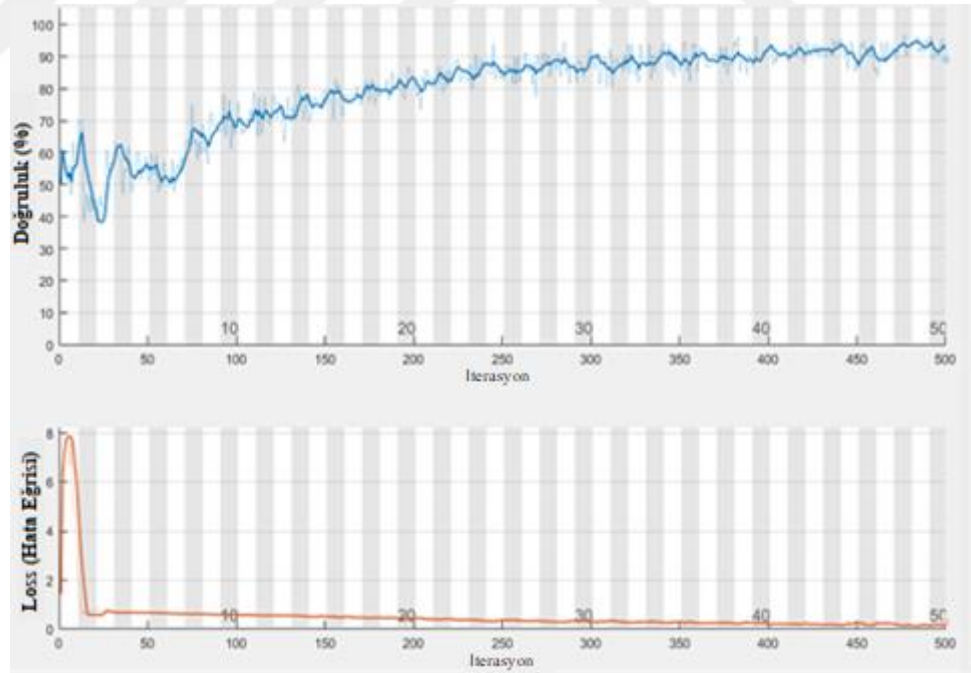
Şekil 6.6. Digital Persona veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

Digital persona veri seti CNN sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.7'de verilmiştir. Sınıflandırma sonucu elde edilen performans değerleri; doğruluk : 0.8567, hata : 0.1433, duyarlılık : 0.86, özgüllük :

0.8533, doğru pozitif : 258, yanlış pozitif : 44, yanlış negatif : 42, doğru negatif : 256, kesinlik : 0.8543, F1-score : 0.8571, MCC : 0.7133, kappa : 0.7133 olarak hesaplanmıştır. CNN sınıflandırıcısı ile eğitim sürecinde elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.8’de gösterilmiştir.



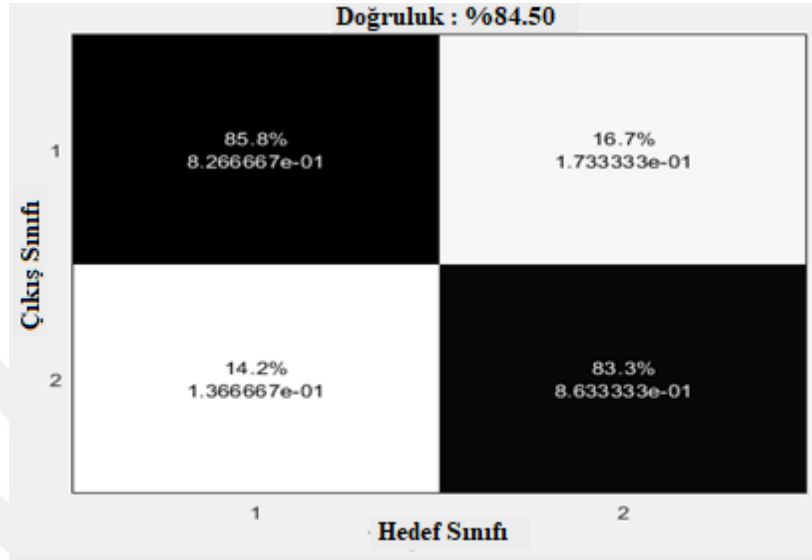
Şekil 6.7. Digital Persona veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi



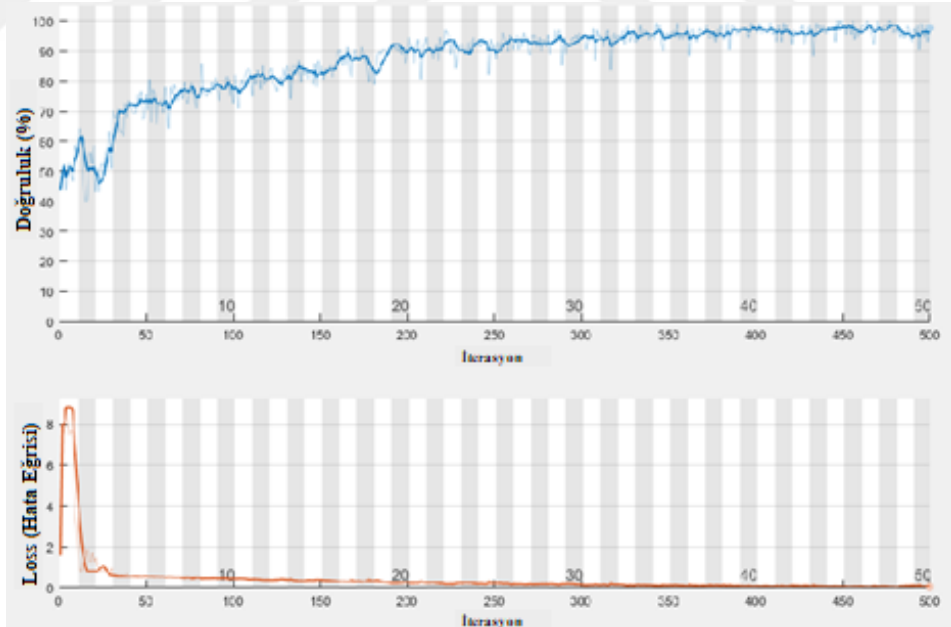
Şekil 6.8. Digital Persona veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi

Digital persona veri setinin hibrit yöntem CNN+SVM ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.9’de verilmiştir ve performans değerleri; doğruluk : 0.8450, hata : 0.1550, duyarlılık : 0.8267, özgüllük : 0.8633, doğru pozitif

: 0.8267, yanlış pozitif: 0.1367, yanlış negatif: 0.1733, doğru negatif: 0.1733, kesinlik : 0.8581, F1-score : 0.8421, MCC : 0.6905, kappa : 0.69 olarak hesaplanmıştır. CNN+SVM sınıflandırıcısı ile eğitim sürecinde elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.10'de gösterilmiştir.



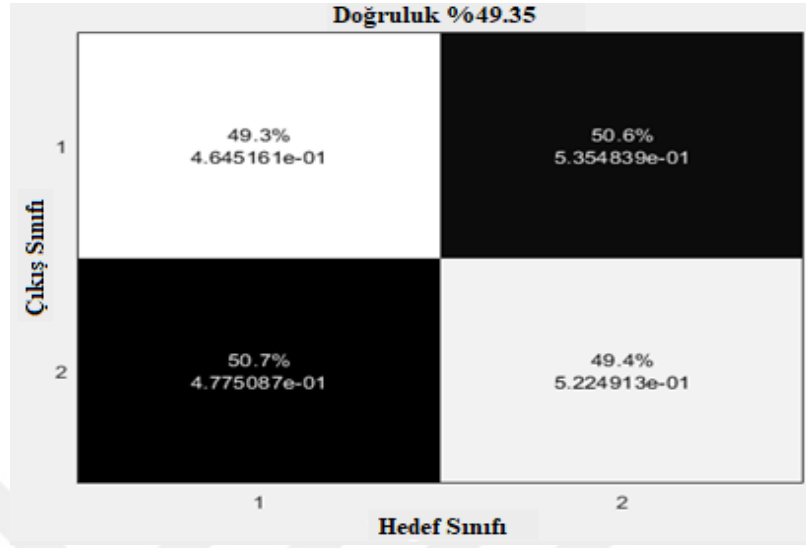
Şekil 6.9. Digital Persona veri seti hibrit yöntem ile sınıflandırılması sonucu elde edilen karışıklık matrisi



Şekil 6.10. Digital Persona veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi

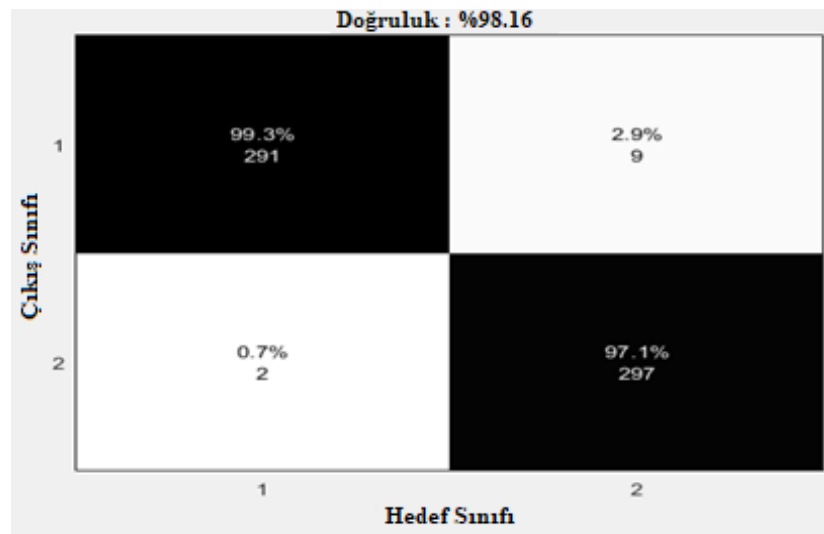
Green bit veri seti SVM sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.11' de verilmiştir. Karışıklık matrisi kullanılarak hesaplanan değerler şöyledir; doğruluk : 0.4935, hata : 0.5065, duyarlılık : 0.4645, özgüllük :

0.5225, doğru pozitif : 0.4645, yanlış pozitif : 0.4775, yanlış negatif : 0.5355, doğru negatif : 0.5225, kesinlik : 0.4931, F1-score : 0.4784, MCC : 0.0130, kapa : 0.0128.

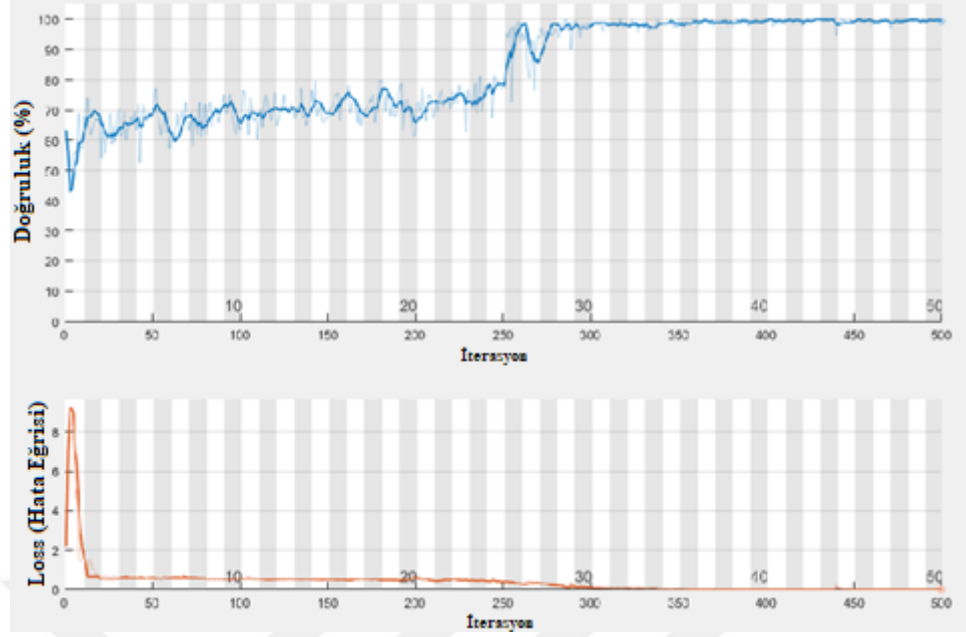


Şekil 6.11. Green Bit veri seti SVM yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

Green bit veri seti CNN sınıflandırıcısı ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.12'de verilmiştir. Sınıflandırma sonucu elde edilen performans değerleri; doğruluk : 0.9816, hata : 0.0184, duyarlılık : 0.97, özgüllük : 0.9933, doğru pozitif : 291, yanlış pozitif : 2, yanlış negatif : 9, doğru negatif : 297, kesinlik : 0.9932, F1-score : 0.9815, MCC : 0.9635, kapa : 0.9633 olarak hesaplanmıştır. CNN sınıflandırıcısı ile eğitim sürecinde elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.13'de gösterilmiştir.

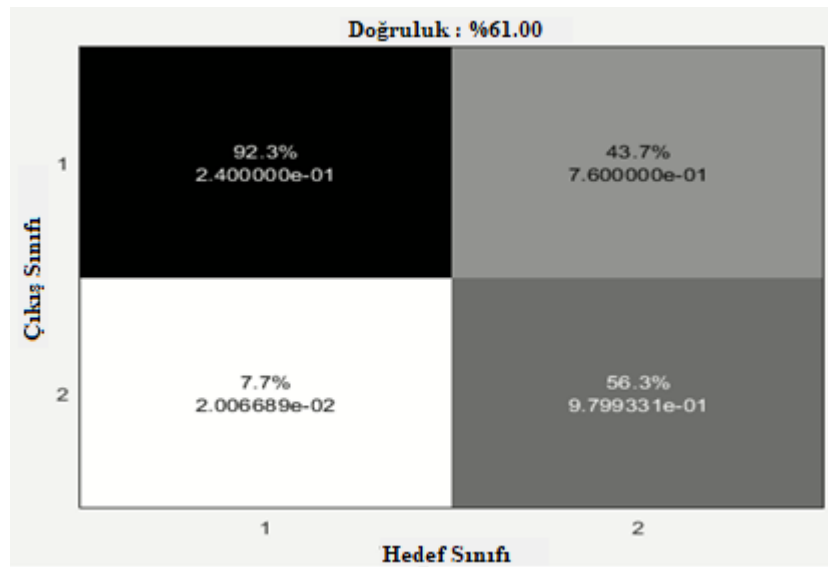


Şekil 6.12. Green Bit veri seti CNN yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi

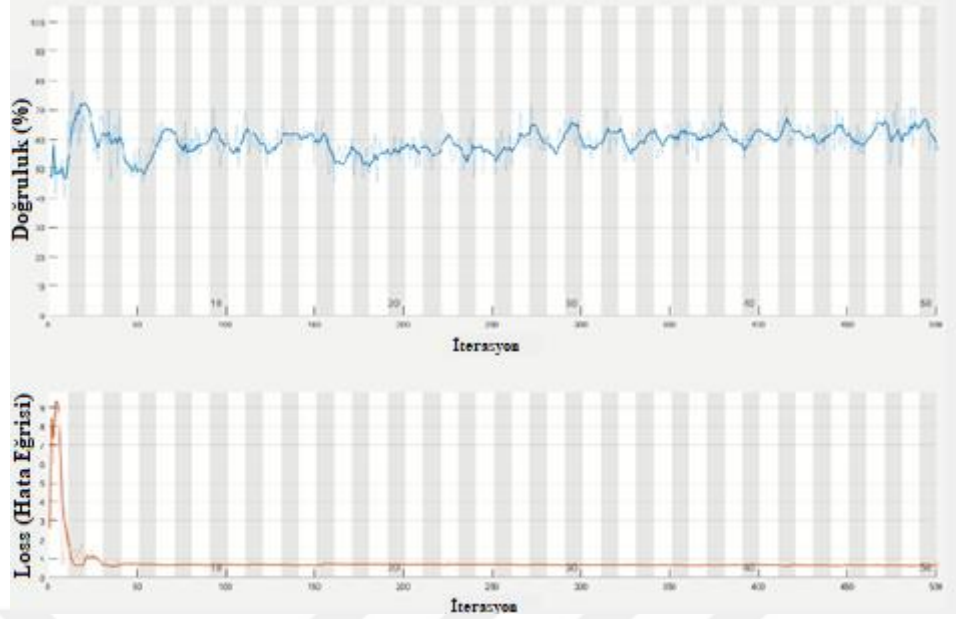


Şekil 6.13. Green Bit veri seti CNN sınıflandırıcısı sonrası doğruluk ve hata eğrisi

Green bit veri setinin hibrit yöntem CNN+SVM ile sınıflandırıldıktan sonra elde edilen karışıklık matrisi Şekil 6.14’de verilmiştir ve performans değerleri; doğruluk : 0.61, hata : 0.39, duyarlılık : 0.24, özgüllük : 0.9799, doğru pozitif : 0.24, yanlış pozitif : 0.0201, yanlış negatif : 0.76, doğru negatif : 0.9799, kesinlik : 0.9228, F1-score : 0.3809, MCC : 0.3270, kappa : 0.2199 olarak hesaplanmıştır. CNN+SVM sınıflandırıcısı ile eğitim sürecinde elde edilen accuracy (doğruluk) ve loss (kayıp) eğrilerinin görüntüleri Şekil 6.15’de gösterilmiştir.



Şekil 6.14. Green Bit veri seti hibrit yöntemi ile sınıflandırılması sonucu elde edilen karışıklık matrisi



Şekil 6.15. Green Bit veri seti hibrit yöntem sınıflandırıcısı sonrası doğruluk ve hata eğrisi

Parmak izi görüntülerinin sınıflandırılarak sahte parmak izlerinin ayrıştırılmasında SVM yöntemi kullanılarak elde edilen sonuçlar Çizelge 6.1’de yer almaktadır. Doğruluk değeri ele alındığında %51.45 ile en yüksek doğruluk oranına Crossmatch veri kümesi üzerinde erişildiği görülmektedir. SVM sınıflandırıcısı kullanıldığında üç veri kümesinde elde edilen doğruluk oranları %48 - %51 aralığında salınmaktadır. Veri kümesi üzerinde ayrıntı vb. özellikler kullanılmadan gerçekleştirilen sınıflandırma işleminde SVM sınıflandırıcısının güçlü bir ayırım sergileyemediği görülmektedir.

Çizelge 6.1. Parmak izi görüntülerinin SVM yöntemi ile sınıflandırılarak elde edilen sonuçlar

Veri Kümesi	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	49.35	49.31	46.45	52.25	47.84	01.30	01.28
Digital Persona	47.58	47.78	52.20	42.95	49.90	04.87	04.62
Crossmatch	51.45	51.02	72.31	30.59	59.83	03.19	02.90

Parmak izi görüntülerinin sınıflandırılarak sahte parmak izlerinin ayrıştırılmasında CNN yöntemi kullanılarak elde edilen sonuçlar Çizelge 6.2’de yer almaktadır. Doğruluk değeri ele alındığında %98.16 ile en yüksek doğruluk oranına Green Bit veri kümesi üzerinde erişildiği görülmektedir. CNN yönteminin nitelik çıkarma ve sınıflandırma amacıyla kullanıldığı durumda üç veri kümesinde doğruluk oranlarının %86 - %98 aralığında salındığı görülmektedir. CNN sınıflandırıcısının

SVM sınıflandırıcısına oranla oldukça güçlü ve kabul edilebilir bir sınıflandırma performansı sergilediği görülmektedir.

Çizelge 6.2. Parmak izi görüntülerinin CNN yöntemi ile sınıflandırılarak elde edilen sonuçlar

Veri Kümesi	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	98.16	99.32	97.00	99.33	98.15	96.35	96.33
Digital Persona	85.67	85.43	86.00	85.33	85.71	71.33	71.33
Crossmatch	90.00	91.67	88.00	92.00	89.80	80.06	80.00

Parmak izi görüntülerinin sınıflandırılarak sahte parmak izlerinin ayrıştırılmasında CNN+SVM yöntemi kullanılarak elde edilen sonuçlar Çizelge 6.3'de yer almaktadır. Doğruluk değeri ele alındığında %85.33 ile en yüksek doğruluk oranına Crossmatch veri kümesi üzerinde erişildiği görülmektedir. CNN+SVM hibrit yönteminde elde edilen sınıflandırmanın sonucunda CNN yönteminden elde edilen sonuçtan daha iyi bir sonuç elde edilememiştir.

Çizelge 6.3. Parmak izi görüntülerinin CNN+SVM yöntemi ile sınıflandırılarak elde edilen sonuçlar

Veri Kümesi	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	61.00	92.28	24.00	97.99	38.09	32.70	21.99
Digital Persona	84.50	85.81	82.67	86.33	84.21	69.05	69.00
Crossmatch	85.33	88.41	81.33	89.33	84.72	70.89	70.67

7. TARTIŞMA

Bu tez çalışması içerisinde üç farklı sınıflandırma tekniği kullanılarak örnek veri kümesi LivDet2015 içerisinde yer alan sahte ve gerçek parmak izleri tespit edilmiştir. SVM, CNN, CNN+SVM sınıflandırma teknikleri kıyaslanarak bir derin öğrenme sınıflandırıcısı (CNN), sınır değeri belirleyerek sınıflandırma yapan geleneksel bir sınıflandırıcı (SVM) ve hibrit yaklaşımların görüntü sınıflandırma üzerindeki performansları analiz edilmiştir.

Çizelge 7.1 içerisinde Green Bit veri kümesi üzerinde üç farklı sınıflandırma tekniği : CNN, SVM, CNN+SVM kullanılarak gerçekleştirilen sınıflandırmaya ait performans metriklerinin sonuçları yer almaktadır.

Çizelge 7.1. Green Bit veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları

Sınıflandırıcı	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
SVM	49.35	49.31	46.45	52.25	47.84	01.30	01.28
CNN	98.16	99.32	97.00	99.33	98.15	96.35	96.33
CNN+SVM	61.00	92.28	24.00	97.99	38.09	32.70	21.99

Çizelge 7.2 içerisinde Digital Persona veri kümesi üzerinde üç farklı sınıflandırma tekniği : CNN, SVM, CNN+SVM kullanılarak gerçekleştirilen sınıflandırmaya ait performans metriklerinin sonuçları yer almaktadır.

Çizelge 7.2. Digital Persona veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları

Sınıflandırıcı	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
SVM	47.58	47.78	52.20	42.95	49.90	04.87	04.62
CNN	85.67	85.43	86.00	85.33	85.71	71.33	71.33
CNN+SVM	84.50	85.81	82.67	86.33	84.21	69.05	69.00

Çizelge 7.3 içerisinde Crossmatch veri kümesi üzerinde üç farklı sınıflandırma tekniği: CNN, SVM, CNN+SVM kullanılarak gerçekleştirilen sınıflandırmaya ait performans metriklerinin sonuçları yer almaktadır.

Çizelge 7.3. Crossmatch veri seti SVM, CNN ve CNN+SVM sınıflandırma performans metrikleri sonuçları

Sınıflandırıcı	Doğruluk (Accuracy) (%)	Kesinlik (Precision) (%)	Duyarlılık (Recall) (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
SVM	51.45	51.02	72.31	30.59	59.83	03.19	02.90
CNN	90.00	91.67	88.00	92.00	89.80	80.06	80.00
CNN+SVM	85.33	88.41	81.33	89.33	84.72	70.89	70.67

2015 parmak izi canlılık tespit yarışmasında %95,5 doğruluk oranı ile birincilik ödülünü kazanan Nogueira ve arkadaşları LivDet 2009, 2011 ve 2013 veri seti üzerinde CNN yöntemini ve yerel ikili desen yöntemini kullanmışlardır (Nogueira et al. 2016). Fire ve Garm-K modüllerinden oluşan fPADnet (parmak izi sunum saldırı tespit ağı) adlı Evrişimsel Sinir Ağlarını (CNN) kullanan sunum saldırı tespit yöntemini öneren çalışmada gerçek ve sahte parmak izlerini ayırt etmede önemli özellikleri elde etmek için Gram-K modülleri doku bilgisi çıkarmada kullanılmıştır. LivDet 2011, 2013 ve 2015 veri seti üzerinde yapılan deneyler sonucu %2,61'lik ortalama algılama hatası oranına ulaşabileceğini göstermişlerdir (Nguyen et al. 2018). Sharma and Dey (2018) parmak izi canlılık tespiti çalışmalarında çıkarılan özelliklerden sequential forward floating selection (SFFS) ve random forest feature selection (RFFS) gibi özellik seçim birimleri kullanarak kaliteli özellikleri ayırmışlar ve SVM sınıflandırıcısı ile LivDet 2015 veri seti üzerinde ortalama sınıflandırma hata oranı %4,3 ile iyi bir performans elde etmişlerdir. Chugh et al. (2017) çalışmalarında parmak izi saldırılarını tespit etmek için, parmak izi ayrıntılarını kullanarak merkezlenmiş derin evrişimsel sinir ağı tabanlı bir yaklaşım önermişlerdir. LivDet 2011, 2013 ve 2015 veri seti üzerinde yapılan deneysel sonuçlarda ortalama %99,03 doğruluk elde etmişlerdir.

Literatür araştırmaları sonucu LivDet veri seti üzerinde gerçek ve sahte parmak izi ayırımını yapmada en çok CNN ve yine bu yöntemi takip eden SVM yönteminin kullanıldığı görülmüştür. Bu nedenle literatürden farklı özellik çıkarma yöntemleri kullanılarak CNN ve SVM sınıflandırıcıları kullanılmıştır.

CNN, evrişim katmanları (convolution layers), havuz katmanları (pooling layers) ve tamamen bağlı katmanlar (fully connected layers) gibi birden fazla yapı bloğu kullanarak geri yayılım yoluyla üzerinde çalıştığı resimlerde özelliklerin hiyerarşilerini otomatik ve adaptif bir biçimde öğrenmektedir (Yamashita et al., 2018). Çizelge 7.1, Çizelge 7.2 ve Çizelge 7.3 içerisindeki sonuçlar incelenecek olursa her üç veri kümesinde, bir sınır değere göre sınıflandırma işlemi gerçekleştiren SVM

sınıflandırıcısının CNN sınıflandırıcısından çok daha düşük bir performans sergilediği görülmektedir. Nitelikleri elde etmek amacıyla gerçekleştirilen konvolüsyon işlemi nedeniyle CNN sınıflandırıcısı nitelikleri ayırtmada SVM sınıflandırıcısına göre yüksek başarı elde etmektedir. CNN ile SVM sınıflandırıcılarının birlikte kullanıldığı hibrit yaklaşımın da CNN sınıflandırıcısı kadar başarılı olmadığı görülmüştür.



8. SONUÇLAR

Bu çalışma içerisinde günlük yaşamların önemli bir parçası olan kimlik tanımlama sistemlerinde biyometrik yaklaşımlar incelenmiş, ilgili yaklaşımlardan parmak izi tanıma, iris tanıma, retina tanıma, el geometrisi tanıma, ses tanıma, damar tanıma, imza tanıma anlatılmıştır. 1800'lü yıllardan beri etkin olarak kullanılan parmak izi tanıma, çalışma içerisinde ana kimlik tanımlama yöntemi olarak seçilmiş, parmak izinin ayrıntıları ve ayırıcı özellikleri ele alınmıştır. Parmak izinin ayırıcı olarak kullanılmasında bilgisayar sistemleri büyük kolaylık sağlamanın yanı sıra aynı zamanda sahte parmak izi ayrımı konusunda da oldukça yardımcıdır. Sahte parmak izlerini canlılara ait parmak izlerinden ayırmak amacıyla makine öğrenme teknikleri kullanılmıştır. Bu amaçla sahte parmak izi verilerini ve kişilere ait verileri içeren örnek bir veri kümesi olan LivDet 2015 seçilmiştir. İlgili veri kümesi insanlara ait parmak izlerinin yanı sıra; lateks, silikon, ekofleks, oyun hamuru vb. maddelerle üretilen parmak izlerini barındırmaktadır. Sahte parmak izlerinin kişisel parmak izlerinden ayrılmasında makine öğrenmesi tekniklerinin kullanılması amacıyla destek vektör makineleri, derin öğrenme yöntemlerinden evrişimsel sinir ağları ve hibrit evrişimsel sinir ağı ardından destek vektör makinesi kullanılmıştır.

Çalışmada veri kümesine en uygun makine öğrenmesi yönteminin seçilmesi en yüksek performansı sağlayan makine öğrenmesi tekniklerinin kıyaslanması hedeflenmiştir. Bu amaçla SVM, CNN ve CNN+SVM teknikleri kullanılarak gerçek ve sahte parmak izlerini içeren LivDet2015 veri kümesi üzerinde sınıflandırma işlemi yapılmıştır.

SVM ile gerçekleştirilen sınıflandırma işleminde ön işlem aşamasında kenar zenginleştirme ve entropi, varyans hesaplamaları ile nitelik matrisleri elde edilmiştir.

Elde edilen sonuçlar incelendiğinde en yüksek doğruluk oranına CNN sınıflandırıcısı kullanılarak erişildiği görülmüştür. CNN sınıflandırıcısı nitelikleri otomatik ve adaptif olarak öğrenebilme yetisi nedeniyle kullanılan veri kümeleri üzerinde en yüksek doğruluğa erişmiştir.

9. KAYNAKLAR

Arı A, Berberler M. (2017) Yapay Sinir Ağları ile Tahmin ve Sınıflandırma Problemleri Çözümü için Arayüz Tasarımı. *Acta Infologica*, 55-73.

Baltacı Ö. (2011) Yapay Sinir Ağları ve Parmak İzi Analizi Yöntemi İle Kimlik Tayini. Yüksek Lisans Tezi. DEÜ. Fen Bilimleri Enstitüsü, İzmir.

Baştürk A, Baştürk Sarıkaya N, Qurbanov O. (2018) Fingerprint Recognition by Deep Neural Networks and Fingercodes. *IEEE 26th Signal Processing and Communications Applications Conference (SIU)*, 1-4.

Ben-David A. (2008) Comparison of Classification Accuracy Using Cohen's Weighted Kappa. *Expert Systems with Applications*, 34:2, 825-832.

Bhattacharya S, Mali K. (2011) Fingerprint Recognition Using Minutiae Extraction Method. *Proc. of International Conference on Emerging Technologies (ICET-2011): International Journal of Electrical Engineering and Embedded Systems*, 0975-4830.

Chugh T, Cao K, Jain AK. (2017) Fingerprint spoof buster. *arXiv preprint arXiv:1712.04489*.

Darlow LN, Rosman B. (2017) Fingerprint Minutiae Extraction Using Deep Learning. *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 22-30.

Daugman J. (2009) How Iris Recognition Works. *The Essential Guide to Image Processing*, 715-739.

Gao Q, Förster P, Möbus RK, Moschytz SG. (2001) Fingerprint Recognition Using CNN: Fingerprint Preprocessing. *Circuits and Systems 2001. ISCAS 2001. The 2001 IEEE International Symposium*, 3: 433-436.

Ghiani L, Yambay D, Mura V, Tocco S, Marcialis GL, Roli F, Schuckers S. (2013) LivDet2013 Fingerprint Liveness Detection Competition 2013. *2013 International Conference on Biometrics (ICB)/IEEE*, 1-6.

Ghiani L, Yambay D, Mura V, Marcialis GL, Roli F, Schuckers S. (2017) Review of the Fingerprint Liveness Detection (LivDet) competition series:2009 to 2015. *Image and Vision Computing*. 58: 110-128.

Gupta D, Choubey S. (2015) Discrete Wavelet Transform for Image Processing. *International Journal of Emerging Technology and Advanced Engineering*, 4(3), 598-602.

Herbst NM, Liu CN. (1978) Signature verification method and apparatus utilizing both acceleration and pressure characteristics. U.S. Patent, No: 4,128,829.

Jagadeesan A, Duraiswamy K. (2010) Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris. *arXiv preprint arXiv:1003.1458*.

- Karakuş O. (2006) Parmakizi Porlarının Bir Kimlik Tespit Yöntemi Olarak Değerlendirilmesi: Poroskopi. Yüksek Lisans Tezi. AÜ. Sağlık Bilimleri Enstitüsü, Ankara.
- Kaygısız M. (1995) Kriminalistikte Parmak İzi İncelemesi. Yüksek Lisans Tezi. İÜ. Adli Tıp Enstitüsü, İstanbul.
- Li J, Feng J, Kuo C. C. J (2018) Deep Convolutional Neural Network for Latent Fingerprint Enhancement. *Signal Processing: Image Communication*. 60: 52-63.
- Maltoni D, Maio D, Jain K. A, Prabhakar S. (2009) *Handbook of Fingerprint Recognition*. Springer-Verlag, London.
- Marasco E, Wild P, Cukic B. (2016) Robust and Interoperable Fingerprint Spoof Detection via Convolutional Neural Networks. 2016 IEEE Symposium on Technologies for Homeland Security (HST), 1-6.
- Marasco E, Cando S, Tang L. (2019) Can Liveness Be Automatically Detected from Latent Fingerprint. 2019 IEEE Winter Applications of Computer Vision Workshops (WACVW), 93-99.
- Marcialis GL, Lewicke A, Tan B, Coli P, Grimberg D, Congiu A, Tidu A, Roli F, Schuckers S, the LivDet 2009 Group (2009) First International Fingerprint Liveness Detection Competition-LivDet2009. *International Conference on Image Analysis and Processing (Springer)*, 12-23.
- Mura V, Ghiani L, Marcialis GL, Roli F, Yambay DA, Schuckers SA. (2015) LivDet2015 Fingerprint Liveness Detection Competition 2015. 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS).
- Nagel RN, Rosenfeld A. (1977) Computer Detection of Freehand Forgeries. *IEEE Transactions on Computers*, 9: 895-905.
- Naja MI, Rajesh R. (2015) Fingerprint Image Enhancement Algorithm and Performance Evaluation. *International Journal of Innovative Research in Computer and Communication Engineering*, 3(1): 441-446.
- Nguyen T, Park E, Cui X, Nguyen VH, Kim H. (2018) fPADnet: Small and Efficient Convolutional Neural Network for Presentation Attack Detection. *Sensor*, 18(8):2532.
- Nogueira FR, De Alencar Lotufa R, Machado CR. (2014) Evaluating software-based fingerprint liveness detection using Convolutional Networks and Local Binary Patterns. 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings, 22-29.
- Nogueira FR, De Alencar Lotufa R, Machado CR. (2016) Fingerprint liveness detection using convolutional neural networks. *IEEE Transactions on Information Forensics and Security*, 11(6): 1206-1213.
- Noor K, Jan T, Basher M, Ali A, Kihalil RA, Zafar MH, Ashraf M, Babar Mİ, Shah SW. (2018) Performances Enhancement of Fingerprint Recognition System Using Classifiers. *IEEE Access*, 5760-5768.
- Parlakıyıldız Ş. (2014) Yapay Sinir Ağları Kullanılarak Parmak İzi Tanıma ve Sınıflandırma. Yüksek Lisans Tezi. GÜ. Fen Bilimleri Üniversitesi, Ankara.
- Parvathy J, Patil GP. (2018) A Survey on Fingerprint Identification Techniques. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 6(1): 1744-1751.

- Pinheiro PO, Collobert R, (2014) Recurrent Convolutional Neural Networks for Scene Labeling. 31st International Conference on Machine Learning, 82-90.
- Sharma RP, Dey S. (2018) Fingerprint liveness detection using local quality features. The Visual Computer, 1-18.
- Song D, Tang Y, Feng J. (2019) Aggregating minutia-centred deep convolutional features for fingerprint indexing. Pattern Recognition, 397-408.
- Topcu B, Erdoğan H. (2019) Fixed-Length Asymmetric Binary Hashing for Fingerprint Verification Through GMM-SVM based Representations. Pattern Recognition, 88:409-420.
- Yamashita R, Nishio M, Do RKG, Togashi K. (2018) Convolutional neural networks: an overview and application in radiology. Insights into imaging. 9(4): 611-629.
- Yambay D, Ghiani L, Denti P, Marcialis GL, Roli F, Schuckers S. (2012) LivDet2011 Fingerprint Liveness Detection Competition 2011. 2012 5th IAPR International Conference on Biometrics (ICB)/IEEE, 208-215.
- Yuan C, Li X, Wu Jonathan QM, Li J, Sun X. (2017) Fingerprint Liveness Detection from Different Fingerprint Materials Using Convolutional Neural Network and Principal Component Analysis. Computers, Materials & Continua, 53(3): 357-371.
- Wang R, Han C, Wu Y, Guo T. (2014) Fingerprint Classification Based on Depth Neural Network, arXiv preprint. arXiv: 1409.5188.
- Bilim.org. (2014) Erişim Tarihi: 24 Kasım 2018, <https://www.bilim.org/dunyanin-ilk-damar-goruntuleme-teknolojisi-gelistirildi/>
- Ganegedana T. (2018) Intuitive Guide to Convolution Neural Networks. Erişim Tarihi: 19 Ocak 2019, <https://towardsdatascience.com>
- Gözebak.com (2019) Erişim Tarihi: 12 Ocak 2019, <https://gozebak.com/retina-dekolmani-ameliyati-sonrasi-nelere-dikkat-edilmeli.html>.
- Kakıcı A. (2008) Biyometrik Tanıma Sistemleri. Erişim Tarihi: 20 Kasım 2018, <https://ahmetkakici.github.io/genel/biyometrik-tanima-sistemleri/>
- Sharma S. (2017) Activation Functions: Neural Networks. Erişim Tarihi: 10 Mayıs 2018, <https://towardsdatascience.com/activation-functions-neural-networks-1cbd9f8d91d6>.
- Türksan Yüksek Teknolojiler Ltd. Şti. (2008) Yüz tanıma. Erişim Tarihi: 24 Kasım 2018, <http://www.turksan.com>

10. ÖZGEÇMİŞ

Zeynep İNEL ÖZKİPER

Zeynep İNEL ÖZKİPER, 1988 yılında doğdu. İlk ve Orta öğrenimini İstanbul'da tamamladı. 2009 yılında Hitit Üniversitesi Bilgisayar teknolojisi ve programlama programında ön lisans öğrenimini tamamladı. 2010'da Haliç Üniversitesi Bilgisayar Mühendisliği bölümünde başladığı lisans öğrenimini 2014 yılında tamamladı. Haliç Üniversitesi Bilgisayar Mühendisliği programında tezli yüksek lisans öğrenimine 2017 yılında başladı. 2014 yılında öğrenci asistan olarak başladığı Haliç Üniversitesi'nde 2018 yılı itibari ile yazılım ve akademik planlama koordinatörlüğü bölümünde uzman olarak çalışmaktadır.