T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ÇEVRİMİÇİ BİYOMETRİK İMZA TANIMA

Muhammet AKSAKAL

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

Danışman
Prof. Dr. Banu DİRİ

Ocak, 2020

T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ÇEVRİMİÇİ BİYOMETRİK İMZA TANIMA

Muhammet AKSAKAL tarafından hazırlanan tez çalışması 28.01.2020 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programı **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Prof. Dr. Banu DİRİ
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Prof. Dr. Banu DİRİ, Danışman
Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi Göksel BİRİCİK, Üye
Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi Tuğba YILDIZ, Üye
Bilgi Üniversitesi _____

Danışmanım Prof. Dr. Banu DİRİ sorumluluğunda tarafımca hazırlanan Çevrimiçi Biyometrik İmza Tanıma başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Muhammet AKSAKAL

İmza

Değerli aileme...

TEŞEKKÜR

Bu tez çalışmamda, bilgi ve tecrübeleriyle çalışmalarıma yön veren, çalışmamın her anında desteğini hiç esirgemeyen kıymetli danışmanım Prof. Dr. Banu DİRİ ve tezime büyük katkı sağlayan değerli Reha DİRİ'ye sonsuz teşekkürlerimi sunarım.

İmza verilerinin toplanması ve oluşturulmasında katkısı değerli arkadaşlarıma, tez çalışmamda fikir alış verişinde bulunduğum Mahmut Can SÖZERİ'ye, yüksek lisans teşviği ile maddi ve manevi destekleriyle Kuveyt Türk AR-GE Merkezi'ne teşekkürlerimi sunarım.

Tez aşamasında her daim beni cesaretlendiren, teşvik eden, maddi ve manevi destekleyen eşime ve aileme şükranlarımı sunuyorum.

Muhammet AKSAKAL

İÇİNDEKİLER

SİMGE LİSTESİ vii

KISALTMA LİSTESİ viii

ŞEKİL LİSTESİ ix

TABLO LİSTESİ xi

ÖZET xii

ABSTRACT xiii

1 Giriş 1

1.1 Literatür Özeti 1

1.2 Tezin Amacı 6

1.3 Hipotez 6

2 Materyaller 8

2.1 Veri Kümeleri 8

2.1.1 Kullanıcılardan Toplanan İmzalar AKSKL-42 8

2.1.2 SVC2004 9

2.2 Programlama Dilleri 9

2.2.1 C# 9

2.2.2 Python 10

2.3 Metodlar ve Algoritmalar 10

2.3.1 Naive Bayes 10

2.3.2 Destek Vektör Makineleri 11

2.3.3 K-En Yakın Komşuluk 12

2.3.4 K-Katlı Çaprazlı Doğrulama 13

2.4 Derin Öğrenme 14

2.4.1 Evrişimsel Sinir Ağı (CNN) 15

2.4.2 Sigmoid Aktivasyon Fonksiyonu 17

3 Sistem Tasarımı ve Uygulanması 19

3.1 Veri Ön İşleme 19
3.1.1 İmza Konumlarının Ötelenmesi 19
3.1.2 Basıncın Sıfır Olduğu Satırların Atılması 20
3.2 Özellik Çıkartma 21
3.2.1 Çevrimdışı Özellikler 21
3.2.2 Çevrimiçi Özellikler 22
3.2.3 Yön Bilgisinden Çıkarılan Özellikler 24
3.2.4 Zaman, Hız ve İvme Bilgisinden Çıkarılan Özellikler 25
3.2.5 İmza Verilerinin Normalize Edilmesi 25
3.2.6 İmza Verisinden Örnekleme Alınması 26
3.2.7 İmza Vektörlerinin Elde Edilmesi 26
3.3 Sistem Tasarımı 28

4 Deneysel Sonuçlar **31**
4.1 Başarım Ölçütleri 31
4.2 İmza Tanıma Test Sonuçları 33
4.3 İmza Doğrulama Test Sonuçları 33

5 Sonuç ve Öneriler **38**

Kaynakça **40**

A İmza Şekilleri **43**

Tezden Üretilmiş Yayınlar **46**

SİMGE LİSTESİ

ω	Açısal Hız
p	Basınç
V	Hız
θ	Kutupsal Koordinatlardaki Açı
μ	Ortalama
σ	Standart Sapma
V_x	X Yörüngesindeki Hız
r	Yarıçap
V_y	Y Yörüngesindeki Hız

KISALTMA LİSTESİ

CNN	Convolution Neurol Network
ÇD	Çapraz Doğrulama
ÇKYSA	Çok Katmanlı Yapay Sinir Ağı
DN	Doğru Negatif
DP	Doğru Pozitif
DVM	Destek Vektör Makinesi
DWT	Dynamic Time Wrapping
DZB	Dinamik Zaman Bükme
EER	Equal Error Rate
EHO	Eşit Hata Oranı
ESA	Evrişimsel Sinir Ağı
FAR	False Accepted Rate
FRR	False Rejection Rate
GMM	Gaussian Mixture Model
KKÇD	K-Katlı Çapraz Doğrulama
KNN	K-Nearest Neighborhood
NB	Naive Bayes
SVC2004	Signature Verification Competition 2004
SVM	Support Vector Machine
YKO	Yanlış Kabul Oranı
YP	Yanlış Pozitif
YRO	Yanlış Reddetme Oranı
YSA	Yapay Sinir Ağları
YN	Yanlış Negatif

ŞEKİL LİSTESİ

Şekil 1.1 Kalemin Yatay ve Dikey ile Yaptığı Açı [13] 4
Şekil 1.2 İmzanın Önemli ve Örnekleme Noktaları [15] 5
Şekil 1.3 X ve Y Koordinatlarındaki Yerel Maksimum, Yerel Minimum ve Pen-up Bilgileri [16] 5
Şekil 2.1 İmza Örnekleri 8
Şekil 2.2 Destek Vektör Makineleri Hiper Düzlemin Belirlenmesi [21] 12
Şekil 2.3 K-Katlı Çapraz Doğrulama Çalışma Yapısı [25] 13
Şekil 2.4 Sinir Hücre Yapısı [28] 14
Şekil 2.5 Yapay Sinir Ağı Yapısı [28] 15
Şekil 2.6 CNN Mimarisi [31] 16
Şekil 2.7 Konvolüsyon İşlemi [31] 16
Şekil 2.8 ReLu Fonksiyon Grafiği 16
Şekil 2.9 Max Pooling İşlemi [32] 17
Şekil 2.10 Sigmoid Aktivasyon Fonksiyonu 18
Şekil 3.1 Sistem Tasarımı 19
Şekil 3.2 Ham İmza Veri Örneği 20
Şekil 3.3 Orijinal İmza ve Ötelenmiş İmza 20
Şekil 3.4 Öteleme ve Sıfır Basınç Değerleri Atıldıktan Sonra Veri İçeriği 21
Şekil 3.5 Bir Kişiye Ait 5 İmza Örneğinin Basınç Grafiği 23
Şekil 3.6 İmzalardan Çıkarılan Bazı Özelliklerin Normalizasyon Sonrası Değerleri 27
Şekil 3.7 İmzanın X ve Y Yörüngesinden Alınan Örnekler 27
Şekil 3.8 İmzanın Basıncından Alınan Örnekler 27
Şekil 3.9 Çok Katmanlı Yapay Sinir Ağı Modeli 29
Şekil 3.10 Evrişimsel Yapay Sinir Ağı Modeli 30
Şekil A.1 Bir Kişiye Ait 5 İmza Örneğinin X Yörüngesindeki Grafiği 43
Şekil A.2 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası X Yörüngesindeki Grafiği 43
Şekil A.3 Bir Kişiye Ait 5 İmza Örneğinin Y Yörüngesindeki Grafiği 44
Şekil A.4 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası Y Yörüngesindeki Grafiği 44

Şekil A.5 Bir Kişiye Ait 5 İmza Örneğinin Basınç Grafiği 44
Şekil A.6 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası Basınç Grafiği 45
Şekil A.7 SVC2004 Veri Setinde Bulunan Orijinal İmza Örneği 45
Şekil A.8 SVC2004 Veri Setinde Bulunan Sahte İmza Örneği 45

TABLO LİSTESİ

Tablo 2.1 AKSKL-42 İmza Veri Seti Kullanıcı Dağılımı 9
Tablo 3.1 İmzalar Üzerinden Çıkarılan Temel ve Ekstra Özellikler 26
Tablo 4.1 Hata Matrisi 32
Tablo 4.2 İmza Tanıma Sınıflama Başarımları 33
Tablo 4.3 Destek Vektör Makineleri Hata Matrisi 34
Tablo 4.4 Evrişimli Sinir Ağı Hata Matrisi 34
Tablo 4.5 K-En Yakın Komşuluk Hata Matrisi 35
Tablo 4.6 Çok Katmanlı Yapay Sinir Ağı Hata Matrisi 35
Tablo 4.7 Naive Bayes Hata Matrisi 35
Tablo 4.8 İmza Doğrulama Başarım Sonuçları 36
Tablo 4.9 SVC2004 Task 2 Yarışması Performans Sonuçları [19] 36
Tablo 4.10 SVC2004 Task 2 Veri Seti Kullanılarak Geliştirilen İlgili Çalışmaların Başarımları [35] 37

ÖZET

Çevrimiçi Biyometrik İmza Tanıma

Muhammet AKSAKAL

Bilgisayar Mühendisliği Anabilim Dalı
Yüksek Lisans Tezi

Danışman: Prof. Dr. Banu DİRİ

Gelişen teknoloji beraberinde biyometrik çalışmalara olan ilgiyi arttırmıştır. Artan güvenlik ihtiyaçları da biyometrik bilgi tabanlı sistemlerin kullanımını zorunlu kılmıştır. İris, parmak izi gibi statik biyometrikler de yerini imza, ses gibi kişinin davranışsal bilgilerini içeren biyometriklere bırakmıştır. Bu çalışmada, kişilerden bir tablet ve kalem aracılığı ile elde edilen imzalar ve SVC2004 imza veri tabanı kulllanılarak imza tanıma ve doğrulama sistemi geliştirilmiştir. İmzalar üzerinden vuruş sayısı, basınç, hız, ivme vs. gibi çevrimiçi özellikler çıkarılmıştır. Çıkarılan özellikler ve imzalardan alınan örneklemelerle imzaları temsil eden vektörler elde edilmiştir. Bu temsili imza vektörleri, Destek Vektör Makinesi, Naive Bayes, K-En Yakın Komşuluk, Çok Katmanlı Yapay Sinir Ağı ve Evrişimsel Sinir Ağı modelleri ile eğitilerek sistemin başarısı ölçülmüştür.

Anahtar Kelimeler: Biyometri, biyometrik imza, çevrimiçi imza, imza tanıma, imza doğrulama

ABSTRACT

Online Biometric Signature Recognition

Muhammet AKSAKAL

Department of Computer Engineering
Master of Science Thesis

Advisor: Prof. Dr. Banu DİRİ

Developing technology has increased interest in biometric studies. Increased security requirements also necessitated the use of biometric information-based systems. Static biometrics, such as iris and fingerprints, have been replaced by biometrics that include behavioral information such as signature and voice. In this study, the signature recognition and verification system has been developed by using the signatures obtained from individuals by means of a tablet and pen and the signature database SVC2004. Online features such as the number of strokes, pressure, velocity, acceleration, etc. were extracted from the signatures. The vectors representing the signatures were obtained with the extracted features and the samples taken from the signatures. The success of the system was measured by training these representative signature vectors with Support Vector Machine, Naive Bayes, K-Nearest Neighborhood, Multilayer Artificial Neural Network and Convolutional Neural Network models.

Keywords: Biometric, biometric signature, online signature, signature recognition, signature verification

1
Giriş

Günümüzde biyometrik kimlik tanıma hızla artış gösteren trend haline gelmiştir. Gelişen teknoloji ve biyometrik çalışmaların artması sebebiyle kullanım alanları da genişlemiştir. Son zamanlarda bankalarda, finans kurumlarında ve diğer ticari kuruluşlarda artan güvenlik ihtiyacı biyometrik sistemlerin kullanımını da çarpıcı bir biçimde arttırmıştır. Kimlik tanımada kullanılan biyometrikler kişinin fiziksel ve davranışsal özelliklerini yansıtmaktadır. Yüz, parmak izi, iris kimlik tanımada kullanılan fiziksel özellikler iken; el yazısı, imza, ses ise kimlik tanımada kullanılan davranışsal özelliklerdir. Yüz, parmak izi, iris gibi statik biyometrikler gün geçtikçe yerini kişinin karakteristik ve hareket bilgilerini içeren davranışsal biyometriklere bırakmaktadır. İmzanın günlük yaşamda yoğun bir şekilde kullanılması imza tanıma çalışmalarına olan ilgiyi de artırmıştır. İmza tanıma veya doğrulama ile imzanın gerçek veya sahte olduğu belirlenerek sahtecilik ve dolandırıcılık gibi suçların önlenmesi de sağlanmaktadır.

Davranışsal bir biyometrik olan imzanın bir özelliği de kişinin imzalama anındaki psikolojik durumunun imza üzerine yansıma etkisinin fazla olmasıdır. Bu da imzanın tanınmasını zorlaştıran bir durumdur. Bu yüzden güvenilir doğrulama sistemlerine ihtiyaç vardır [1].

1.1 Literatür Özeti

Literatürde imza tanıma ve doğrulamaya yönelik birçok sayıda çalışma vardır. İmza tanımada genel olarak çevrimiçi ve çevrimdışı olmak üzere iki teknik kullanılmaktadır [1, 2]. Çevrimdışı imza tanımada, imzanın görüntüsü üzerinden görüntü işleme algoritmaları kullanılarak imzanın sadece yapısal özellikleriyle tanıma işlemi yapılır. Çevrimiçi imza tanımada ise atılan imzanın hızı, basıncı, ivmesi, x ve y yörüngeleri ve süresi gibi dinamik özellikler statik özelliklerle birlikte kullanılarak tanıma işlemi gerçeklenir. Burada imzanın davranışsal detayını yakalamak için özel bir cihaz ve kalem kullanılır [3, 4]. Ayrıca, imzalar arasındaki farklılığı veya benzerliği bulmada

parametrik ve işlevsel olmak üzere iki yaklaşım kullanılır. Bir imzanın parametrik özellikleri imzanın genel özelliklerini tarif eder. Bu özellikler imzanın atılma süresi, en boy oranı, imzanın uzunluğu, vuruş sayısı vb. parametrik özellikleridir. İmzanın işlevsel özellikleri de hız, ivme, kalemin basıncı, kalem eğim açısıdır [5]. Çevrimiçi imzadan türetilen birçok özellik olabilir. Fierrez-Anguilar ve arkadaşları [6] daki çalışmasında imza verisi üzerinden türetilen 100 özellikten oluşan bir set önermiştir. Çevrimdışı bir sisteme göre çevrimiçi sistemlerde, kullanıcının imzası x ve y koordinatlarının sırası ve basınç gibi ilişkili nitelikler ile birlikte değerlendirilir. Orijinal ve sahte imzalar arasında bu değerler farklılık göstereceğinden çevrimiçi imza doğrulama sistemi genellikle çevrimdışı bir sistemden daha iyi doğruluk sağlar [7]. Ayrıca, biyometrik imzalar kişinin duygusal ve fiziksel durumundan da etkilenir [8].

Genel olarak imza sahteciliğinde tanımlanabilecek üç sahtecilik türü vardır [9]. Bunlar rasgele sahtecilik, basit sahtecilik ve yetenekli sahteciliktir.

- Rastgele sahtecilik: İmzanın şekli veya imzalayanın adı hakkında hiçbir bilgi veya ayrıntıya sahip olan kişidir.
- Basit sahtecilik: İmza sahibinin ismini ve imzasının temel şeklini bilen kişidir.
- Yetenekli sahtecilik: İmzalayanın veritabanına erişebilen ve aynı zamanda imza üzerinde biraz pratik yapmış olan kişidir.

Sistem içindeki biyometrik verilerin güvenliği her zaman büyük bir endişe kaynağı olmuştur. Meşru olmayan kimlik doğrulama girişimlerinde, herhangi bir başka dijital sistemlerdeki gibi bir bireyin biyometrik bilgileri kopyalanabilir ve yeniden kullanılabilir. Bu nedenle, hem iletişim kanallarının hem de biyometrik şablonların, şifreleme teknikleriyle korunması ve güvenli bir ortam oluşturulması gerekmektedir.

Kholmatov ve Yanıkoğlu [10] imza tanıma çalışmasıyla etkili bir yöntem geliştirmiştir. Bu yöntemde imzanın koordinat bilgileri kullanılarak 3 boyutlu bir özellik vektörü elde edilmektedir. Kullanıcıdan alınan imza örnekleri ilk olarak ikişerli olarak Dinamik Zaman Bükme (DZB) algoritması ile imzaların birbirine benzememezlik puanları elde edilmiştir. Elde edilen minimum skora sahip imza örneği referans imzası olarak seçilmektedir. Giriş değerleri olarak, verilen imzanın kendine en yakın, en uzak ve referans imzaya olan uzaklığı ile 3 boyutlu imza vektörü elde edilmektedir [11]. Sınıflama safhasında Bayes sınıflama, Destek Vektör Makineleri (DVM) ve doğrusal sınıflayıcı kullanılmıştır. Deney sonuçları olarak toplamda %2,8 oranında EER (Equal Error Rate) elde edilmiştir.

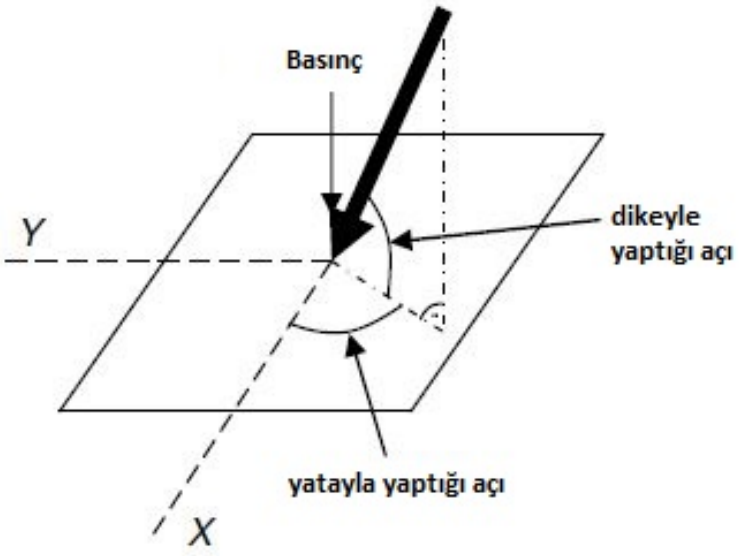
Guru ve Prakash [5] yaptıkları çalışmada çevrimiçi imzaları sembolik olarak aralıklı

bir özellik vektörü halinde temsil etmişlerdir. Her bir imza verisinden dinamik özellikler çıkartılmıştır. Burada bahsedilen sembolik aralıkları hesaplarken özelliklerin ayrı ayrı standart sapmalarından yararlanılmıştır. İmzanın orijinal özellik değerine standart sapma eklenerek üst sınır, çıkarılarak alt sınır belirlenmiştir. Bir imzanın referans imzasına benzerliği bulunurken, bakılan özelliğin değeri referans aralığında olup olmamasına göre bir eklenir. Bu benzerlik değeri toplam özellik sayısına bölünerek benzerlik oranı bulunur. Ayrıca, çalışmanın başarısını arttırmaya yönelik eğitim kümesi üzerinden ortak eşik değeri hesaplanmıştır. Hem kullanıcı tarafından belirlenen eşik değer hem de ortak eşik değere göre imzaların gerçek veya sahte olup olmadığının tespiti yapılmıştır. Çalışmada %3,8 EER elde edilmiştir.

Hurtado ve Jimenez [12] çalışmasında DZB ve GMM (Gausian Mixture Model) algoritmasını birlikte kullanmışlardır. Çalışmadaki ön işlemenin en son adımında DZB algoritması ile imzaların hizalama işlemi yapılmaktadır. Bu geliştirilen yöntem ile GMM algoritmasının performansının iyileştirildiğini göstermişlerdir. DZB doğası gereği imzadaki her örnek arasındaki doğal farkı en aza indirir. Ancak bu yöntemin nitelikli sahte imzalar üzerinde kullanılması sahte imzaların kalitesini artıracağından sahte imzaların tespitini zorlaştıracaktır. Sonuç olarak GMM için otomatik imza tanıma için bir algoritma geliştirilmiştir.

Adamski ve Saeed [13] çevrimiçi imza tanıma ve doğrulama üzerine bir çalışma yapmışlardır. Çalışmada SVC2004 [11] imza veritabanını kullanmışlardır. X ve y yörüngeleri, hız, kalemin basıncı, kalemin yatay ile yaptığı açı (azimuth) ve kalemin dikey ile yaptığı açı (altitude) gibi dinamik özellikleri kullanmışlardır. Şekil 1.1'de azimuth ve altitude gösterilmiştir. Bu özellikler farklı farklı kombinasyonlarla seçilerek DWT (Dynamic Time Wrapping) algoritması kullanılarak sınıflama işlemi gerçekleştirilmiştir. Y, azimuth, basınç, altitude kombinasyonu ile %99,6 ile en iyi başarıyı elde etmişlerdir. Sunulan sistem test edildiğinde %7 EER elde edilmiştir.

Sae Bae ve diğerleri [14] imza doğrulama çalışmasında basit ve etkili bir çevrimiçi imza doğrulama sistemi önermiştir. Önerdikleri sistemde, bir imza verisi basit bir şekilde hesaplanarak elde edilen bir kaç histogramdan oluşan bir özellik setine dayanmaktadır. Bu oluşturulan histogramların, Manhattan mesafesi kullanılarak doğrulaması yapılmıştır. Önerilen sistemin bir özelliği kullanıcıdan çok sayıda imza örneği gerektirmeden sadece bir kaç imza örneği ile kullanıcı bazlı eğitilebilmesidir. Diğer bir özelliği de önerilen sistemde orijinal imzalardan çıkarılan özellik vektörü türetilmiş istatistiksel bilgileri temsil ettiğinden imzanın ham verisi tekrardan elde edilemez. Böylece orijinal biyometrik verilerin gizliliği korunur. Kısacası çalışmalarında biyometrik imza verisinin güvenliği de düşünülmüştür. Çalışmada MCYT-100 ve SUSIG imza veri tabanları kullanılmıştır. Diğer önerilen sistemlerle

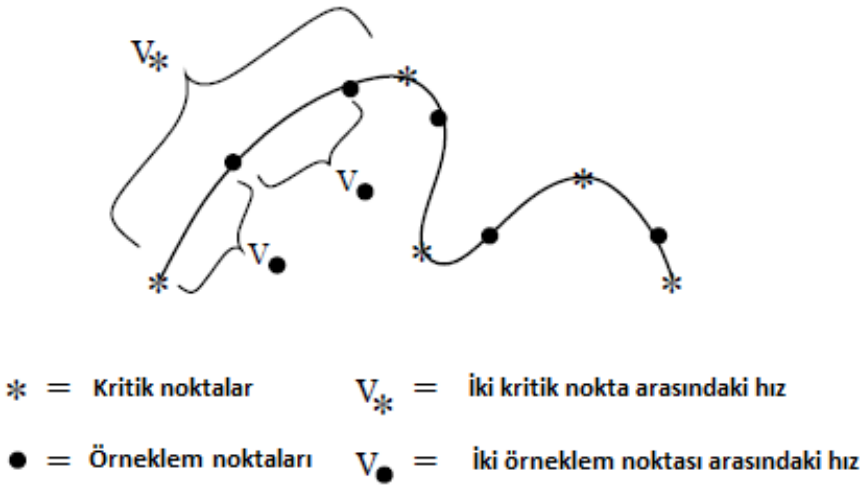


Şekil 1.1 Kalemin Yatay ve Dikey ile Yaptığı Açı [13]

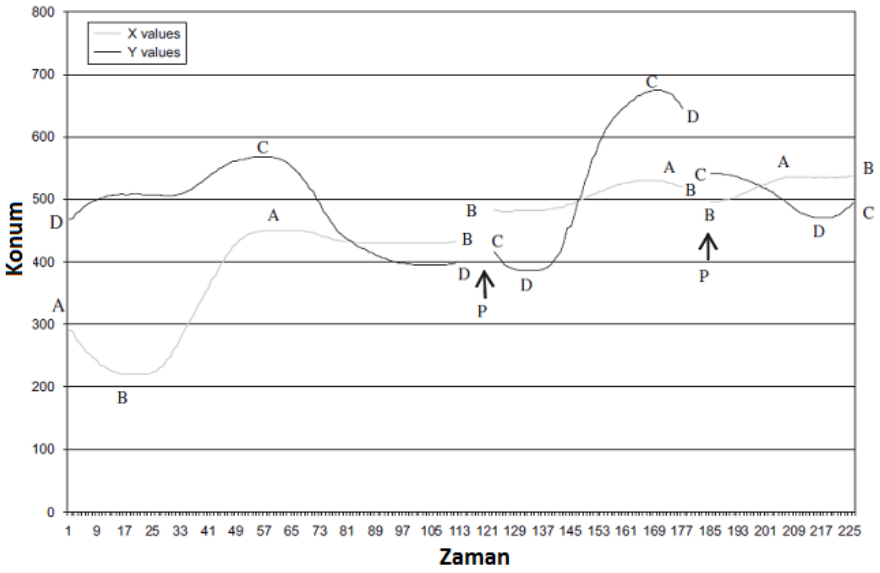
karşılaştırıldığında rekabetçi bir performans sunmaktadır. Sonuçlar, önerilen tekniğin basitliğine rağmen çoğu önerilen sistemlerden daha üstün olduğunu göstermektedir.

Jain ve diğerleri [15] çalışmasında, imzaları bir string dizisi ile temsil etmişlerdir. Bu temsili dizi, Şekil 1.2'de gösterilen imzanın önemli kıvrım noktaları ve örnekleme noktaları ile oluşturulmuştur. Önemli kıvrım noktaları ve eşit zaman aralıkları ile belirlenen örneklem noktaları arasındaki hızlar ayrı ayrı hesaplanmıştır. İmza üzerinde belirlenen bu noktalar ile imzaları temsil eden diziler elde edilmiştir. Elde edilen bu temsil dizileri birbirleri ile karşılaştırılarak benzerlikleri belirlenmiştir. Bu çalışmada kıvrım noktalarının kullanılması imzalardan oluşturulan dizilerin özgün bir hal alması sağlanmıştır. Gupta ve Joyce [16] benzer bir çalışmada, imzanın yerel maksimum ve minimum noktalarını kullarak imzanın şeklini bir string dizisine dönüştürerek güvenilir bir biyometrik imza doğrulama tekniği geliştirmeyi düşünmüşlerdir. Sunulan teknik temel olarak imzanın x ve y yönlerini kullanarak basit bir şekilde string dizisi ile temsil edilmiştir. Çalışmada imzanın x ve y bilgisi ve pen-up bilgisi kullanılmıştır. Çalışmanın en önemli özelliği imzanın pen-up noktalarına göre parçalarına ayrılmasıdır. X ve y yörüngelerindeki yerel max ve yerel min değerleri ve pen-up beş farklı harf ile temsil edilmiştir. Bu değerler Şekil 1.3'de bir imza örneği üzerinden gösterilmiştir. Zaman ekseninde soldan sağa doğru harfler eklenerek imzanın temsili dizisi oluşturulmuştur. Dizilerin benzerlikleri karşılaştırılarak belirlenen eşik değerlerine göre imzanın gerçek veya sahte imza tespiti yapılmıştır. Çalışmadan elde edilen sonuçlara göre imza verisindeki pen-up bilgisinin ayırt edici özelliğinin güçlü olduğu görülmektedir. Pen-up bilgisi az olan imza verilerinde iyi sonuçlar alınamamıştır. Uzman kişilerin atmış olduğu sahte imza

kümesinde %4,8 EER, rastgele kişiler tarafından atılan sahte imzalarda ise %2,25 EER elde edilmiştir.



Şekil 1.2 İmzanın Önemli ve Örnekleme Noktaları [15]



Şekil 1.3 X ve Y Koordinatlarındaki Yerel Maksimum, Yerel Minimum ve Pen-up Bilgileri [16]

Mailah ve Han [17] ileri beslemeli sinir ağı içeren imza doğrulama sistemi geliştirmiştir. Ön işleme aşamasında imza verisini normalleştirme ve DZB algoritması kullanılarak ortak zaman eksenleri oluşturmuşlardır. Ayrıca, imzalar üzerinde birkaç döndürme işlemi yapılarak imzanın çeşitliliği arttırılmıştır. Ardından imzanın anlık hızları hesaplanmıştır. İki farklı yapay sinir ağı tasarlanarak modellenmiş ve giriş değerleri x ve y koordinatları alınmıştır. Çıkış değerleri olarak birinci YSA da basınç değerleri, ikincisinde ise hız büyüklükleri kullanılmıştır. Sistemde rastgele sahte imzalar kullanılarak doğrulama yapılmış ve %1.33 FRR (False Rejection Rate) olarak

sonucu alınmıştır. Seungsoo Nam ve diğerleri [18] (2018) çalışmalarında dinamik imza doğrulama için Evrişimsel Sinir Ağı (ESA) kullanan bir özellik çıkarma yöntemi önermiştir. ESA, otomatik kodlayacıya girdi olarak bir vektör üretmektedir. Deneysel sonuçlar, sahte ve orijinal imzalarla eğitilmiş olan ESA 'nın, sahte imzaları ayırt etmede iyi bir doğruluk vermiştir.

1.2 Tezin Amacı

İmza genellikle bir kağıt ve bir kalem aracılığı ile atılan, kişi doğurlamak için kullanılan yöntemlerden biridir. Gelişen teknolojinin beraberinde getirdiği yeniliklerden imza süreçleri de etkilenmiştir. Bu yöntemlerin başında elektronik ortamda atılan ve kişinin imza atma karakteristiğini tespit etmeye yarayan biyometrik imzalama yöntemi gelmektedir. Biyometrik özellikler fiziksel ve davranışsal olmak üzere iki başlıkta incelenir. Parmak izi, kulak izi, iris fiziksel biyometrik özelliklerdendir. Yürüme temposu, klavyeyi kullanım tarzı ve imzalama şekli de davranışsal biyometrik özelliklerdendir. Biyometrik imzalama yönteminde genellikle imzalama hızı, ivmesi, basıncı ve süresi gibi bilgiler kullanılmaktadır.

Bu tez çalışması ile bir biyometrik imza; hız, ivme, basınç ve süre gibi bilgilerden türetilmiş toplam 27 farklı nitelik ve imza bilgisinin içerisinden seçilen örnekler ile 267 boyutlu bir vektörle temsil edilmiştir. Bu imza vektörleri ile farklı makine öğrenmesi yöntemleri imza tanıma ve doğrulama işlemlerinde kullanılmıştır. Bu çalışmanın birinci bölümünde 82 farklı kişiye ait imza setinden oluşturulmuş özellik vektörleri Destek Vektör Makinesi, k-En Yakın Komşuluk, Naive Bayes ve Çok Katmanlı Yapay Sinir Ağı yöntemleri ile eğitilerek imza tanıma işlemi gerçekleştirilmiş ve başarımları karşılaştırılmıştır. Çalışmanın ikinci bölümde ise DVM, KNN, NB, ÇKYSA ve ESA yöntemleri ile eğitilerek imza doğrulama işlemi yapılmış ve başarımları karşılaştırılmıştır.

1.3 Hipotez

Son yıllarda teknolojideki gelişmeler sayesinde biyometrik doğrulama sistemlerinin çeşitliliği artmıştır. Bu gelişmelerin beraberinde getirdiği yeniliklerden biri de biyometrik imza yöntemidir. Biyometrik imza modellerinin ön plana çıkmasının en önemli nedeni, kişinin davranışsal özelliklerini de göstermesidir. Yani, iki kişinin atmış olduğu imza görüntüsel olarak aynı olsalar bile, imzanın biyometrik bilgileri kullanılarak geliştirilen sistemler ile bu imzaların farklı olduğu ortaya çıkarılabilir.

Bir biyomerik imza verisi içerisinden bir imzayı diğer imzalardan ayırt edebilecek

birçok öznitelik çıkarılabilir. Örneğin imzanın hızı, atılma süresi, vuruş sayısı, basıncı gibi bir çok ayrıt edici özellik elde edilebilir. Bu çıkarılan özellikler ile imza tanıma ve doğrulama sistemleri geliştirilmektedir. Ayrıca, literatürdeki gelişmeler biyometrik imza verilerinin analizinde kullanılacak makine öğrenmesi ve yapay sinir ağı modellerinde çeşitlilik sunmaktadır. Bu tez çalışmasında biyometrik imzaya ait öznitelikler ile makine öğrenme yöntemleri ve yapay sinir ağı kullanılarak tanıma ve doğrulama işleminin yapılabileceği varsayılmıştır.

2
Materyaller

2.1 Veri Kümeleri

Bu çalışmada biri bizim tarafımızdan diğeri literatürde kullanılan iki veri seti kullanılmıştır.

2.1.1 Kullanıcılardan Toplanan İmzalar AKSKL-42

Bu veri seti, 42 kişiden 10 farklı imza örneği alınarak oluşturulmuştur (AKSKL-42[1]). İmzalar Wacom marka bir tablet ve kalem kullanılarak temin edilmiştir. İmza örnekleri erkek, kadın ve farklı yaş gruplarından, 100 Hz frekansı ile 10ms aralıklarla alınmıştır. Alınan bu bilgiler içerisinde tabletin x ve y koordinatları, kalemin yüzeye yapmış olduğu basınç ve süre bilgisi yer almaktadır. Her imza, atılma süresine bağlı olarak farklı büyüklükte bilgiden oluşmaktadır. Alınan imzaların basınç değerleri 0 – 1024 seviye aralığındadır. Şekil 2.1 'de kişilerden alınmış veri setimiz içerisinde yer alan bazı imza örnekleri gösterilmiştir.



Şekil 2.1 İmza Örnekleri

[1]Wacom tablet ve kalem kullanılarak alınmıştır.

Tablo 2.1 AKSKL-42 İmza Veri Seti Kullanıcı Dağılımı

Cinsiyet	Yaş aralığı	Kişi sayısı	Dağılım yüzdesi (%)
E	<25	8	62
	25-50	15	
	50<	3	
K	<25	6	38
	25-50	9	
	50<	1	

2.1.2 SVC2004

Çalışmada kullanılan ikinci veri seti internet ortamından temin edilen SVC2004 biyometrik imza veritabanıdır. SVC2004, 2004 yılında yapılan bir imza doğrulama yarışmasıdır. SVC2004 Task 1 ve Task 2 adında iki ayrı imza veritabanını içermektedir [19]. Task 1 veri tabanı imzanın koordinat bilgilerini, zaman ve kalem vuruş bilgisini içerir. Task2 veri tabanı, Task1 veritabanı bilgilerinin yanı sıra kalemin yatay ile yaptığı açı, dikey ile yaptığı açı ve basınç bilgisini de içermektedir. Task 2, birinci veri kümesindeki imza verisi ile ortak bilgilere sahip olduğundan çalışmada sadece bu veritabanı kullanılmıştır. Bu veri tabanlarında 40 kullanıcıya ait 40 imza örneği bulunmaktadır. Bu imzaların 20 tanesi gerçek, 20 tanesi de sahte imzadır. Sahte imzalar usta kişiler tarafından atılmıştır. Bu veri tabanındaki imza verisi Wacom Intuos tablet kullanılarak elde edilmiştir. Bu veri kümesi çalışmada hem imza tanıma hem de doğrulama için kullanılmıştır.

2.2 Programlama Dilleri

Bu tez kapsamında iki farklı programlama dili kullanılmıştır.

2.2.1 C#

C#[2], Microsoft şirketinin geliştirmiş olduğu bir programlama dilidir. C ve C++ programlama dili etkileşimi ile türetilen C# 'ın en önemli özelliği tamamen nesne yönelimli bir programlama dilidir. Wacom'un geliştiricilere sağladığı C# Wacom SDK'sı da indirilerek, C# kütüphanesine eklenmiştir. Bu kütüphane yardımıyla Wacom kalemi ile anlık tablet üzerindeki x, y, basınç ve zaman bilgileri elde edilmiştir. Ayrıca, C# ile hem tablet ile alınan imzaların hem de SUV2004 veri tabanından elde edilen .txt uzantılı imza verileri düzenlenmiş ve Python programlama dilinde kullanılmak üzere .csv uzantılı dosyaya çevirmek için kullanılmak üzere kullanılmıştır.

[2]https://en.0wikipedia.org/wiki/C_Sharp_(programming_language)

2.2.2 Python

Python[3], üst düzeyde yorumlanan, etkileşimli ve nesne yönelimli bir programlama dilidir. Python oldukça okunabilir şekilde tasarlanmıştır. Diğer dillerden daha az sözdizimsel yapıya sahiptir. İşlevsel ve yapılandırılmış programlama yöntemlerinin yanı sıra nesneye dayalı programlamayı de destekler. Geniş kapsamlı standart kütüphaneye sahiptir. Birçok işletim sisteminde yorumlayıcısı mevcuttur.

Tezde, Python arayüzü, makine öğrenmesi kütüphaneleri ve derin öğrenme için Keras kütüphanesi kullanılarak geliştirilmiştir. Bu arayüzde verilerin dosyadan okunması, ön işleme, makine öğrenmesi algoritmaları ve derin öğrenme ile eğitme, başarım sonuçları, grafiklerin çıkarılması gibi birçok işlem Python arayüzü ile yazılmıştır.

2.3 Metodlar ve Algoritmalar

Bu bölümde test kapsamındaki metod ve algoritmalar anlatılacaktır.

2.3.1 Naive Bayes

Naive Bayes algoritmasının temeli Bayes teoremine dayanır. Verilen bir veri setindeki değerlerin sıklığını ve birleşimini sayarak olasılık kümesini hesaplayan basit bir olasılık sınıflandırıcısıdır. Naive Bayes sınıflandırıcısı, bir sınıftaki belirli bir özelliğin varlığını diğer herhangi bir özelliğin varlığından bağımsız olduğunu varsayar. Bu şartlı bağımsızlık varsayımı, gerçek dünya uygulamalarında nadiren geçerlidir, dolayısıyla Naive olarak nitelendirilir. Ancak, algoritma iyi denetlenmiş çeşitli denetimli sınıflandırma problemlerinde hızlıca öğrenme eğilimindedir [20]. Ayrıca, Naive Bayes sınıflandırıcısı karmaşık yinelemeli parametre tahmin şemalarına başvurmaz. Özellikle büyük veri setlerinde kullanılır.

NB sınıflandırıcısı, Bayes teoremine ve toplam olasılık teoremine dayanır. $X = (x_1, x_2, x_3, ..., x_k)$ k özellik içeren bir öğe olsun. X öğesinin, sınıfının c_i'de olma olasığı (2.1) ' deki gibi ifade edilmektedir.

$$P(c_i|x_k) = \frac{P(x_k|c_i) * P(c_i)}{P(x_k)} \tag{2.1}$$

$P(c_i)$, c_i sınıfının olasılığı, c_i sınıfındaki örnek sayısına bölünmesiyle hesaplanır. $P(x_k)$ sınıfa bağımlı olmadığından paydadan atılabilir. Zincir kuralı kullanılarak tekrardan yazıldığında, sınıf göz önüne alındığında bir özelik, diğer özelliklerden

[3]https://en.0wikipedia.org/wiki/Python_(programming_language)

bağımsız olduğu varsayımına sahip olur. (2.2) ile test örneğinin her sınıf için olasılığı hesaplanmaktadır. En yüksek değere sahip sınıf (2.3)'deki gibi ilgili sınıf atanır.

$$P(c_i|x_k) = P(c_i)\prod_{i=1}^{n} P(x_k|c_i)) \tag{2.2}$$

$$\widehat{y} = argmaxP(y|x) \tag{2.3}$$

2.3.2 Destek Vektör Makineleri

Destek Vektör Makinaları (DVM), verileri sınıflandırmak için kullanılan istatistiksel öğrenme teorisine dayanan denetimli makine öğrenmesi algoritmasıdır. DVM' nin çalışma prensibi iki sınıfı birbirinden ayıran en uygun karar fonkisyonunun tahmin edilmesi, başka bir değişle sınıfları birbirinden ayıran hiper düzlemin tanımlanmasıdır [21]. Basit problemler için düzlemler kolayca sınıfları birbirinden ayırmaktadır. Karmaşık problemler veya çok boyutlu düzlemlerde sınıflar birbirinden tamamen ayrılamamaktadır.

$$h(x) = w^T x \tag{2.4}$$

Çok boyutlu düzlem olmak üzere (2.4) denkleminde $x \epsilon R^N$ N boyutlu bir uzay elemanıdır. $\{-1, 1\}$ ise sınıf etiketleri, w ağırlık vektörünü göstermektedir.

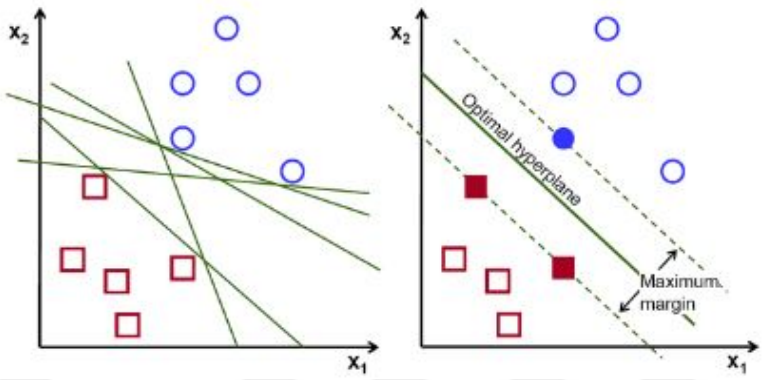
$$min_{w,\varepsilon} = \frac{1}{2} w^T w + c\sum_i \varepsilon_i \tag{2.5}$$

$$y_i(w^T \varphi x_i) \geq 1 - \varepsilon_i, \varepsilon_i \geq 0 \tag{2.6}$$

Denklemde, c sınıfın maksimum hale getirilmesi ve yanlış sınıflandırma hatalarını minimum hale getirilmesini kontrol eden bir maliyet parametresidir. ε sınıflandırma hatası ve gürültülü örnekler için doğru kenara olan mesafeyi temsil eden slack değişkenidir. φ , bir kernel fonksiyonu ile tanımlanan girdi verisinin yüksek boyutlu haritalanmasıdır. (2.7)'de dogrusal olmayan çok boyutlu düzlem ile ayrılamayan ve yaygın olarak kullanılan çekirdek fonksiyonlarından biri olan radyal taban fonksiyonu gösterilmiştir [22].

$$k(x, x') = exp(e^{-\gamma||x-x'||^2}) \tag{2.7}$$

Bir düzlemde bulunan iki sınıfı ayırmak için bir çok sınır çizilebilir. Çizilecek bu sınır iki sınıfın üyelerine en uzak yer olmalıdır. DVM de bu sınırın nasıl çizileceğini belirler (Şekil 2.2). DVM, hem doğrusal hem de doğrusal olmayan verilere uygulanabilmektedir. Yüksek doğruluk oranına sahiptir ve çok sayıda bağımsız değişkenle çalışabilmektedir.



Şekil 2.2 Destek Vektör Makineleri Hiper Düzlemin Belirlenmesi [21]

2.3.3 K-En Yakın Komşuluk

K-En Yakın Komşuluk (K-Nearest Neighbors, KNN) algoritması hem sınıflama hem de regresyon tahmin problemleri için kullanılabilen basit ve çok kullanılan bir tür denetimli makine öğrenmesi algoritmasıdır. KNN tembel bir öğrenme algoritmasıdır. Çünkü özel bir eğitim aşamasına sahip değildir ve tüm veriler sınıflandırma sırasında eğitim için kullanır. KNN parametrik olmayan bir öğrenme algoritmadır. Çünkü temel veriler hakkında hiçbir şey varsaymaz [23]. Algoritmanın çalışmasında tek sayı olmak şartıyla bir k değeri belirlenir. K değerinin anlamı bakılacak komşuluk sayısıdır. Bir test elemanı verildiğinde ilk olarak bütün elemanlara olan uzaklığı hesaplanır. k kadar en yakın elaman alınır. Bu seçilen elemanlar içinde hangi sınıftan daha fazla eleman var ise test elemanı o sınıfa ait olur. Uzaklık hesaplama işlemlerinde genellikle (2.8)'de gösterilen öklid mesafe fonksiyonu kullanılır. Bu fonksiyona alternatif olarak Manhattan (2.9), Minkowski (2.10) fonksiyonları da tercih edilebilir.

$$\sqrt{\sum_{i=1}^{k}(x_i - y_i)^2} \tag{2.8}$$

$$\sum_{i=1}^{k}|x_i - y_i| \tag{2.9}$$

$$\left(\sum_{i=1}^{k}(|x_i - y_i|)^q\right)^{\frac{1}{q}} \tag{2.10}$$

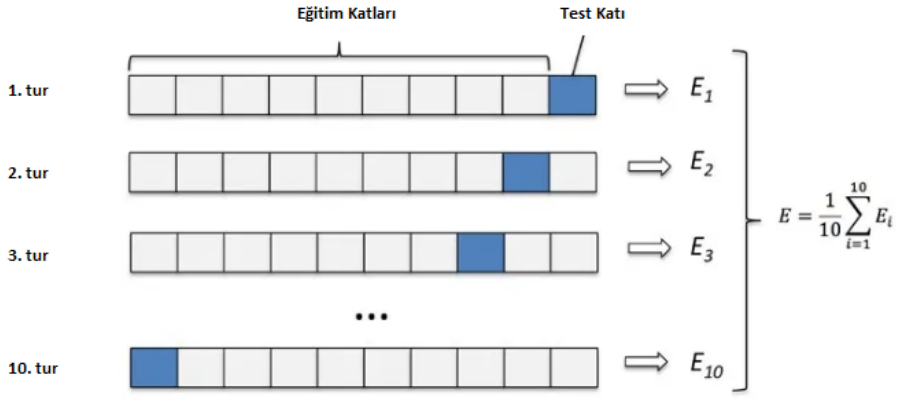
2.3.4 K-Katlı Çaprazlı Doğrulama

Çapraz doğrulama (ÇD), veri bilimi çalışmalarında modelin başarısının sınanması için kullanılan kullanışlı bir tekniktir. Bu teknikle bağımsız veri setleri elde edilerek tahmin başarımı genelleştirilir. Bir makine öğrenimi probleminde veri seti, eğitim ve test olmak üzere iki veri setine ayrılır. Bu ayırmanın amacı olası aşırı öğrenmeden (overfitting) kaçınmak ve modelin daha önceden görmediği veri seti üzerinde nasıl bir performans gösterildiğini anlamak için kullanılır.

K-Katlı Çapraz Doğrulama (KKÇD), makine öğrenimi modellerinde sıkça kullanılan bir tekniktir. KKÇD aşamalı olarak belirtilirse;

- Eğitim verisi rasgele k eşit parçaya $f_1, f_2, f_3 ... f_k$ olmak üzere bölünür.
- i=1 den k ya kadar

  f_i katında k-1 parça eğitim ve kalan bir parça da test için kullanılır. ÇD, eğitim setini kullanarak makine öğrenmesi modelini eğitir. Daha sonra eğitilen model üzerinden test verisi sınanarak işlemin doğruluğu hesaplanır.
- Tüm k çapraz doğrulama sonuçlarının ortalaması hesaplanarak modelin performansı değerlendirilir [24].

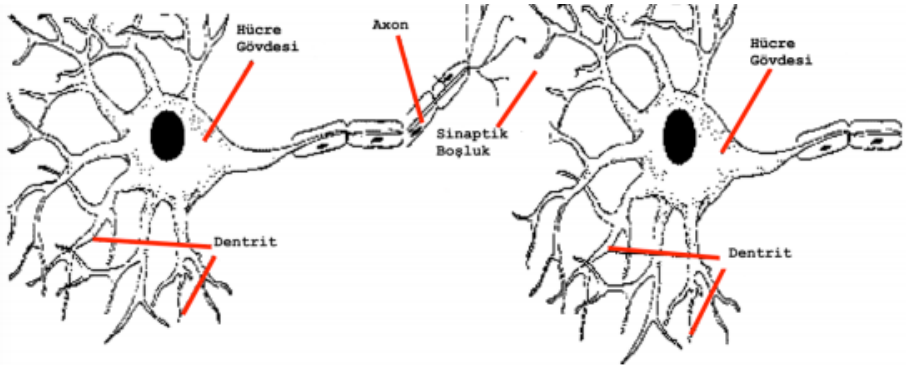


Şekil 2.3 K-Katlı Çapraz Doğrulama Çalışma Yapısı [25]

Şekil 2.3'deki veri seti 10 eşit parçaya ayrılmıştır. Her turda, mavi renkli alan test setine ayrılırken kalan parçalar eğitim için ayrılmıştır. Her turun sonunda, sınıflandırıcıdan gelen doğrulama skorları E_i değişkenine kaydedilmiştir. Tüm katlardaki performans skorlarının ortalaması yani E modelin performansını göstermektedir [25].

2.4 Derin Öğrenme

Yapay Sinir Ağları (YSA), insan beyninin çalışma prensiblerinin bilgisayar ortamına aktarılmış bir makine öğrenimi yöntemidir. McCulloch ve Walter Pitts tarafından eşik mantığı adı verilen ilk YSA 1943'de geliştirilmiştir [26, 27]. Eşik mantığı, matematik ve algoritmalara dayalı sinir ağları için hesaplamalı bir model oluşturulmuştur. Bu model ile birlikte beyindeki biyolojik süreçlere ve yapay sinir ağlarının uygulanmasına odaklanan bir yaklaşım ortaya çıkmıştır.

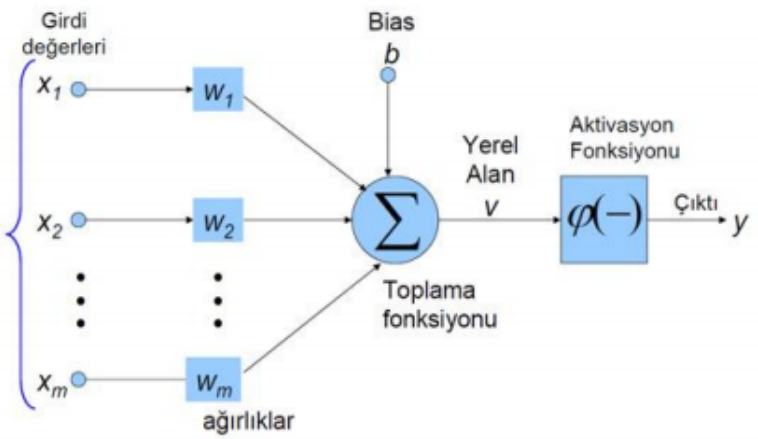


Şekil 2.4 Sinir Hücre Yapısı [28]

Bir sinir hücresinin yapısı Şekil 2.4 'deki gibidir. Dentritlerin uçlarından elde edilen sinyaller çekirdekte ağırlıklandırılarak bir akson boyunca iletilir. Bu iletim akson uçlarında sinapslar yardımıyla bir başka sinir hücresinin dentritlerine iletilir. Bu şekilde sinirler arası iletişim sağlanmaktadır [29]. Bu matematiksel olarak modellendiğinde, dentritlere gelen giriş değerleri ağırlıklar ile çarpıldıktan sonra sinir hücresine iletilir. Sinir hücresinde tüm dentritlerden gelen girişler ile ağırlık çarpımları toplanır. Ardından bir bias (ön yargı) ile toplanır [30]. Bu toplam değeri üzerinde aktivasyon fonksiyonu kullanılır. Sonrasında elde edilen bu değer çıkışa aktarılır. Bu çıkış değeri nihai çıkış veya bir başka sinir hücresinin girişi değeri olabilir. Şekil 2.5 'de tek katmalı bir YSA örneği gösterilmiştir.

YSA 'da öğrenme iki aşamada gerçekleşir. İlk aşama girdinin doğrusal olmayan bir dönüşümünü uygulamak ve çıktı olarak istatistiksel bir model oluşturmaktan ibarettir. İkinci aşama, modeli türev olarak bilinen matematiksel bir yöntemle geliştirmeyi amaçlar. Sinir ağı bu iki fazı hassasiyet seviyesine ulaşıncaya kadar yüzlerce veya binlerce tekrarlayabilir.

Yapay Sinir Ağı temel olarak denetimli eğitim ve denetimsiz eğitim olarak ikiye ayrılabilir. Bu iki yöntemi birbirinden ayıran en belirgin özellik sinapslar üzerinde bulunan ağırlıkların insanlar tarafından belirlenip belirlenmemesidir. Bu durum bir YSA 'nın sonuçta ulaşacağı değeri bulması başladığı değere göre değişmektedir. Yani eğitim sırasında sürekli olarak sinaps üzerindeki ağırlıkları güncelleyen bir



Şekil 2.5 Yapay Sinir Ağı Yapısı [28]

YSA sonuçta ulaşacağı değere yakın bir değerden başlarsa eğitim daha kısa sürede tamamlananacaktır.

Geleneksel makine öğrenme yöntemlerinin aksine önceden çıkarılmış bilgiye ihtiyaç duymaz. Önemli olan özellikleri kendisinin otomatik olarak çıkarmasıdır. Yapay Sinir Ağları yeteneklerinin fazla olması nedeniyle çeşitli problemler üzerinde uygulanabilmektedir. Derin öğrenme algoritmaları, artan işlemci gücü ve grafik işlemcilerinin kullanımıyla, büyük verilerin sınıflandırılması, yüz tanıma, kanser teşisi, otonom sürüş, görüntü işleme ve örüntü tanıma gibi birçok çalışmanın temel kaynağı olmuştur.

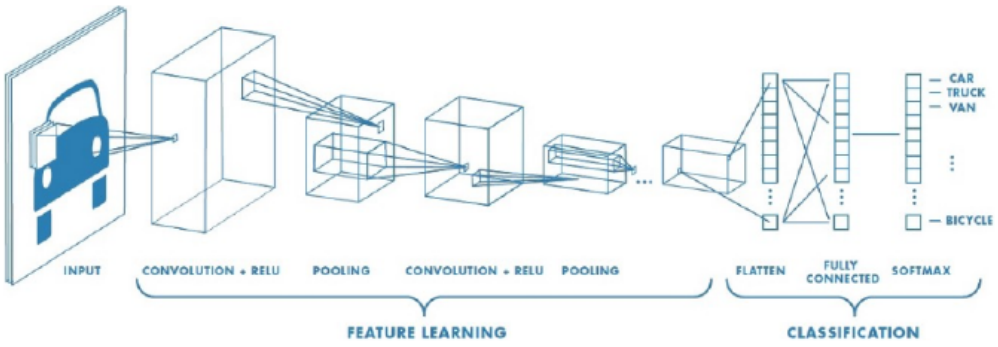
2.4.1 Evrişimsel Sinir Ağı (CNN)

Evrişimsel Sinir Ağı (ESA), geleneksel çok katmanlı algılayıcı mimarilerin aksine, bir görüntüyü temel özelliklerine indirgemek için evrişim ve havuzlama adı verilen iki işlem adımı kullanır [29]. CNN mimarisi Şekil 2.6'da gösterilmiştir. CNN 'lerin görüntü sınıflandırma, video tanıma, öneri sistemleri, otonom araçlar, doğal dil işleme gibi birçok alanda uygulamaları vardır.

Konvolüsyon katmanı (convolution), aktivasyon (activation) katmanı, havuzlama (pooling) ve tam bağlantılı (fully connected) katmanları CNN'nin temel yapı taşlarıdır.

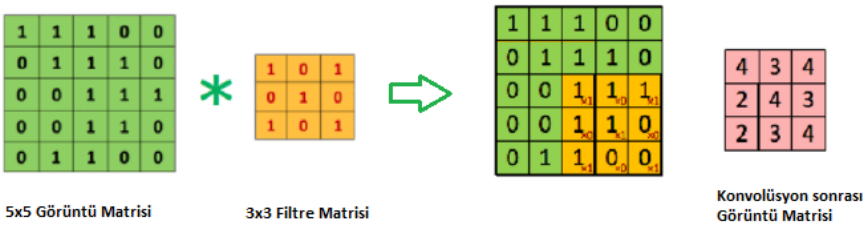
2.4.1.1 Konvolüsyon Katmanı

Konvolüsyon katmanı girişten özellikleri alan ilk katmandır. Bu katmanda görüntü üzerindeki piksellere bazı filtreler uygulanarak görüntünün özellikleri çıkartılır. Evrişim işlemi, filtrede tanımlanan ağırlıklarla orijinal piksel nokta çarpımı ile yapılır. Tüm pikseldeki çarpım değerleri toplanarak sonuç çıktı matrisinde depolanır [29]. Bu



Şekil 2.6 CNN Mimarisi [31]

işlem tüm piksellere uygulanır. Şekil 2.7'de konvolüsyon örneği gösterilmektedir.

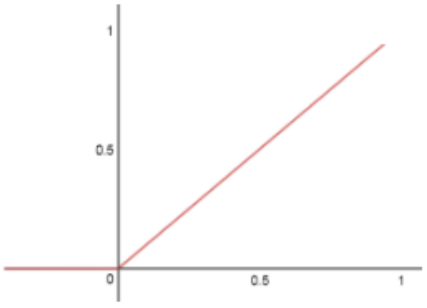


Şekil 2.7 Konvolüsyon İşlemi [31]

2.4.1.2 Aktivasyon Katmanı

Konvolüsyon katmanı, orijinal görüntüden çok daha küçük boyutta bir matris oluşturur. Bu matris, ağın kendisini geri yayılım yoluyla eğitmesine izin vermek için doğrusal olmayan bir tanıma sahip olan bir aktivasyon katmanından geçirilir. Aktivasyon işlevi genellikle ReLu'dur [30]. (2.11)'de ReLu fonkisyonunu temsil edilmektedir.

$$f(x) = max(0, x) \tag{2.11}$$



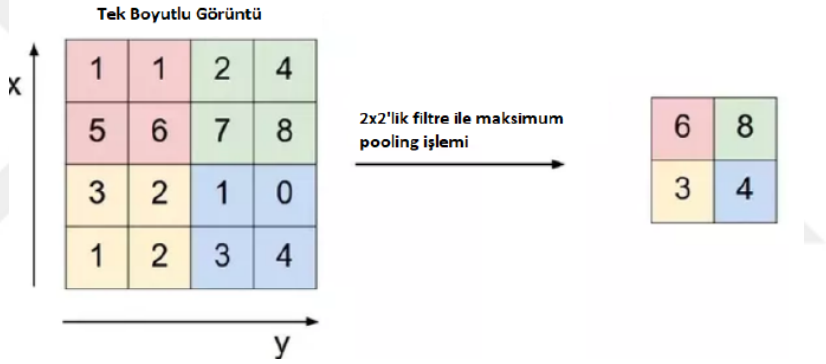
Şekil 2.8 ReLu Fonksiyon Grafiği

2.4.1.3 Havuzlama (pooling) Katmanı

Matrisin boyutunu daha da küçültme işlemidir. Bir önceki katmanın sonuçları üzerinden bir süzgeç geçirilir ve her değer grubundan bir sayı seçilir. Bu ağın, görüntünün her özelliğindeki en önemli bilgilere odaklanarak daha hızlı çalışmasını sağlar [30]. Pooling üç farklı şekilde yapılabilir;

- Max Pooling
- Avarage Pooling
- Sum Pooling

Max pooling, konvolüsyon çıktısındaki maksimum değeri; Avarage pooling, ortalama değeri; Sum pooling de çıktıdaki tüm değerlerin toplamı alınır. Şekil 2.9 'da max pooling örnegi gösterilmektedir.



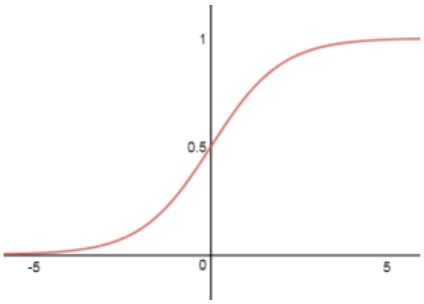
Şekil 2.9 Max Pooling İşlemi [32]

2.4.1.4 Tam Bağlı (Fully Connected) Katman

Girişi, önceki katmanların çıktısını temsil eden tek boyutlu bir vektördür. Tüm nöronların birbirine bağlı olduğu katmandır. Çıktı, resme iliştirilmiş farklı olası etiketler için olasılıkların bir listesidir. En yüksek olasılığı alan etiket, sınıflandırma kararıdır [30].

2.4.2 Sigmoid Aktivasyon Fonksiyonu

Sigmoid fonksiyonu 0 ile 1 arasında değerler almaktadır. Şekil 2.10'da görüleceği üzere türevi x=0 dan önce ise sıfıra, sonra ise 1'e yakınsamaktadır [33]. Fonksiyonun değerinin 0 olması verinin kaybolması, 1 olması da hatırlanmaya devam etmesi anlamına gelir [34]. Sigmoid fonksiyonu (2.12)'de formülize edilmektedir.

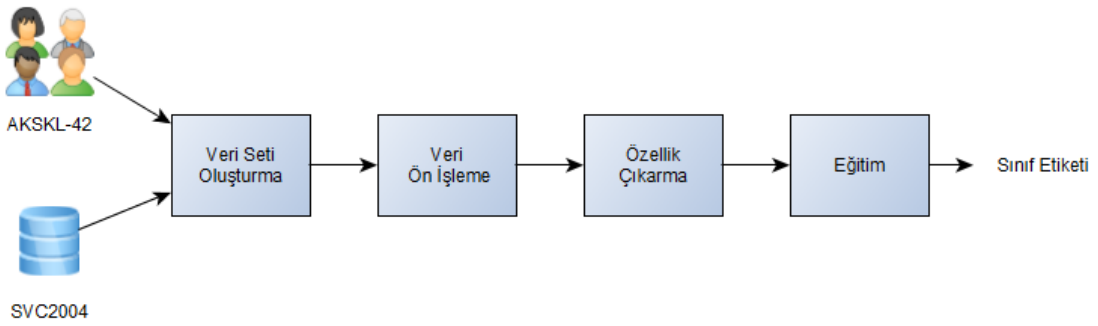


Şekil 2.10 Sigmoid Aktivasyon Fonksiyonu

$$f(x) = \frac{1}{1 + e^{-1}} \tag{2.12}$$

3
Sistem Tasarımı ve Uygulanması

Tez kapsamında geliştirilen sistemin işlem adımları bu bölümde anlatılmaktadır. Sistem veri setinin oluşturulması ve üzerinde ön işleme adımlarının yapılması, devamında özelliklerin çıkarılması ve modelin eğitilip başarısının ölçülmesinde oluşmaktadır (Şekil 3.1).



Şekil 3.1 Sistem Tasarımı

3.1 Veri Ön İşleme

Bu bölümde veri ön işleme aşamasında yapılan işlem adımlarından açıklanacaktır. Şekil 3.2'de atılan bir imzadan elde edilen ham veri gösterilmektedir. Tablodaki ilk ilki kolon imzanın x ve y pikselini, diğer kolonlarda sırasıyla imzanın atılma zamanı ve basınç değerini göstermektedir.

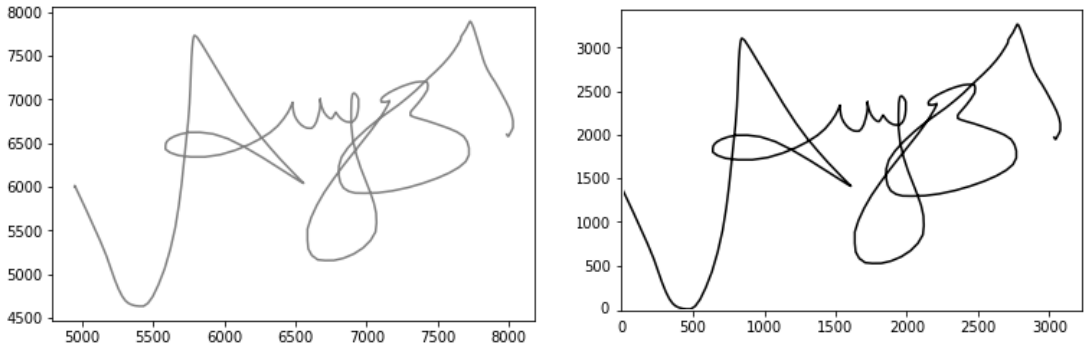
3.1.1 İmza Konumlarının Ötelenmesi

Bir kişiden alınan imza örneklerinin konumları farklı olabileceğinden özellik vektörüne eklenmeden önce imzanları bir referans noktasına kaydırıp eşitliğin sağlanması gerekmektedir. Buradaki problemin çözümü için iki yöntem kullanılabilir. Birincisi tüm koordinat değerlerinden ilk x ve y değerleri çıkartılarak imzaları $(0, 0)$ başlangıç noktasına ötelemek, ikinci olarak da tüm x ve y değerleri minimun x ve y değerinden çıkartılarak imzaların sola ve tabana dayalı duruma getirilerek eşitlik

X	Y	Zaman	Basınç
5434	6501	0	295
5434	6522	10	366
5433	6546	20	383
5428	6571	30	416
5425	6595	40	468
5423	6611	50	521
5423	6621	60	564
5423	6621	70	580
5423	6610	80	595
5437	6549	90	606
5460	6434	100	629
5489	6286	110	680
5519	6120	120	703
5547	5966	130	719
5572	5843	140	740
5598	5736	150	744
5625	5650	160	755
5649	5588	170	758
5670	5547	180	760
5686	5523	190	763
5702	5509	200	763
5722	5500	210	758
5746	5500	220	753
5777	5512	230	734

Şekil 3.2 Ham İmza Veri Örneği

sağlanabilir. Çalışmada ikinci yöntem tercih edilmiştir. Şekil 3.3'de görüldüğü gibi ötelenen imza sola ve tabana dayanır durumdadır. Bütün imzalara bu işlem uygulanarak farklı konumlanma sorunu ortadan kaldırılmıştır.



Şekil 3.3 Orijinal İmza ve Ötelenmiş İmza

3.1.2 Basıncın Sıfır Olduğu Satırların Atılması

İmza basıncının sıfır olduğu kısımlar (kalemin havada olma durumu) imza verisinden silinmiştir. Bunun yapılmasındaki amaç, basınç üzerinden hesaplanacak ortalama, standart sapma gibi ölçüm değerlerini sıfır olan satırların bozmasıdır. Ayrıca, bu satırları silerken kalemin kaldırılma bilgisinin kaybolmaması için pen-up adında

bir kolon daha eklenmiştir. Şekil 3.4'de yapılan işlemler sonrası verinin içeriği gösterilmiştir.

X	Y	Zaman	Basınç	Pen-up
11	1001	0	295	0
11	1022	10	366	0
10	1046	20	383	0
5	1071	30	416	0
2	1095	40	468	0
0	1111	50	521	0
0	1121	60	564	0
0	1121	70	580	0
0	1110	80	595	0
14	1049	90	606	0
37	934	100	629	0
66	786	110	680	0
96	620	120	703	0
124	466	130	719	0
149	343	140	740	0
175	236	150	744	0
202	150	160	755	0

Şekil 3.4 Öteleme ve Sıfır Basınç Değerleri Atıldıktan Sonra Veri İçeriği

3.2 Özellik Çıkartma

Özellik seçimi, sistemin performansında önemli bir rol oynar. Çekinik özelliklerin sisteme dahil edilmesi sistem performansını iyileştirmeyebilir. Özellik vektörünü oluşturan özellikler sınıflandırma doğruluğunu en üst düzeye çıkaracak şekilde seçilmelidir. Bir biyometrik imzanın çevrimdışı ve çevrimiçi özelliklerden oluştuğundan imzalardan çıkarılan özellikler bu başlıklar altında açıklanmıştır. Çalışmada imza verisinden 27 farklı özellik çıkarılmıştır. Tablo 3.1'de çıkarılan özellikler gösterilmiştir.

3.2.1 Çevrimdışı Özellikler

İmzanın statik bilgileri olup, bir imza attıktan sonra da elde edilebilecek özellikleridir. Bu çalışmadaki çevrimdışı özelliklerimiz bir imza örneğinin düzlemdeki x ve y koordinat bilgileridir. Düzlemde bir nokta kartezyen veya kutupsal koordinat sistemi üzerinde temsil edilebilir.

Kartezyen koordinat sisteminde bir nokta, düzlemdeki bir referans noktasından uzaklığı ile temsil edilir. Tez çalışmasında tabletin sol alt noktası referans noktası olarak alınmıştır.

Kartezyen koordinat sistemindeki bir nokta (x, y) kolayca kutupsal koordinat sistemine (r, θ) dönüştürülebilinir. (3.1), (3.2) ve (3.3)'deki formüller kullanılarak r ve θ değerleri hesaplanmıştır.

$$r = \sqrt{x^2 + y^2} \tag{3.1}$$

$$x = rcos\theta \tag{3.2}$$

$$y = rsin\theta \tag{3.3}$$

3.2.2 Çevrimiçi Özellikler

Biyometrik imza davranışsal özellikler içerdiğinden, imza verisi içerisinden bir çok karakteristik özellikler çıkarılabilir. Örneğin hız, ivme, basınç, kalemin vuruş sayısı, kalemin temas süresi gibidir. İki imza dışarıdan aynı görünse bile türetilen çevrimiçi özelliklerle orijinal bir imza ile sahte imza arasındaki ayrım yapılabilir.

3.2.2.1 Hız

Bir imzanın hızının kopyalanması kolay değildir. Hız, orijinal imza ile sahte imza arasındaki farkı ayırt etmek için kullanılan önemli bir özelliktir. Yetenekli bir kişi imzayı kopyalasa dahi imzanın keskin eğrilerinde yavaşlarken, imza sahibi neredeyse sabit hıza sahip olacaktır. Bu nedenle, sisteme hız gibi dinamik özelliğin dahil edilmesi, sahte imzanın ayırt edilebilmesine imkan sağlar. İmzanın x yörüngesindeki hızı, y yörüngesindeki hızı ve açısal hız niteliği (3.4), (3.5) ve (3.6) denklemleri yardımıyla hesaplanmıştır.

$$V_{x_{i-1}} = \frac{x_i - x_{i-1}}{t_i - t_{i-1}} \tag{3.4}$$

$$V_{y_{i-1}} = \frac{y_i - y_{i-1}}{t_i - t_{i-1}} \tag{3.5}$$

$$\omega_{i-1} = \frac{\Theta_i - \Theta_{i-1}}{t_i - t_{i-1}} \tag{3.6}$$

3.2.2.2 İvme

İvme dinamik özelliği de orijinal imza ile sahte imza ayrımını güçlendiren bir niteliktir. Ayrıca, hız gibi bu özellik de kullanıcıdan kullanıcıya farklılık göstereceğinden imza tanıma için önemli bir rol oynamaktadır. Hız değerleri bulunduktan sonra (3.7) ile anlık ivme değerleri de hesaplanmıştır.

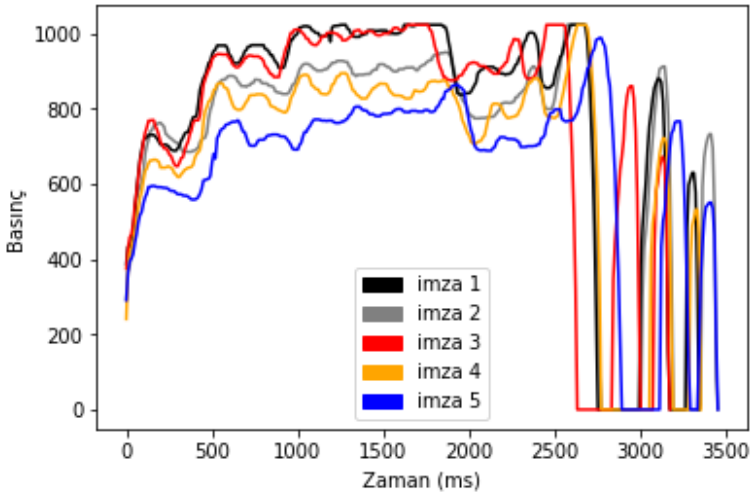
$$a_{i-1} = \frac{V_i - V_{i-1}}{t_i - t_{i-1}} \tag{3.7}$$

3.2.2.3 Basınç

Kalem ucuna uygulanan basınç imza sahteciliği yapan kişi tarafından taklit edilemez bir özelliktir. Bu nedenle orijinal imza ile sahte imza arasında ayrımı kuvvetlendiren önemli bir niteliktir. Şekil 3.5'de bir kişiye ait beş imzanın zamana bağlı basınç grafiği gösterilmiştir. Basıncın ortalama ve standart sapma gibi istatistiksel bilgileri de hesaplanarak özellik vektörüne eklenmiştir. (3.8) kullanılarak ortalama ve (3.9) kullanarak standart sapmalar hesaplanmıştır.

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \tag{3.8}$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \mu)^2}{n-1}} \tag{3.9}$$



Şekil 3.5 Bir Kişiye Ait 5 İmza Örneğinin Basınç Grafiği

3.2.2.4 Kalemin Vuruş Sayısı

Kalemin pen-up bilgisi, kalemin temas halinde mi yoksa havada mı olduğu bilgisini verir. Değeri 1 ise kalemin yukarıda olduğunu, 0 ise tablete temas halinde olduğunu gösterir. Bir kişinin imzalama sırasında kalemi kaldırma sayısı, aynı kullanıcının iki imza örneği için yüksek ihtimalle aynıdır. Bunun nedeni, her insanın kendine özgü bir yazı stiline sahip olmasıdır. Bazı kişiler imza atarken ellerini birkaç kez kaldırırken, imzalarında el yazısı kullanan kişilerin bir kısmı da ellerini kaldırmayabilirler. Ayrıca, el yazısıyla atılan bir imzayı taklit eden kişiler imzayı doğru atabilmek için kalemi birkaç kez kaldırabilir. Böylece orijinal imzada tek vuruş olurken kopyalayan kişide birkaç kalem vuruşu olacaktır. Bu yüzden kalemin vuruş sayısı imza sahteciliğini tespit etmede kullanılan önemli bir niteliktir. İmzanın vuruş sayısını hesaplamak için $0-1$ geçişleri sayılmıştır.

3.2.3 Yön Bilgisinden Çıkarılan Özellikler

İmzanın x ve y koordinatları üzerinden imza vektöründe kullanılmak üzere bazı özellikler türetilmiştir. Türetilen özellikler;

- x değerlerinin standart sapması
- x değerlerinin ortalaması
- x yörüngesindeki işaret değişim sayısı
- y değerlerinin standart sapması
- y değerlerinin ortalaması
- y yörüngesindeki işaret değişim sayısı
- r'nin medyanı
- r'nin ortalaması
- r'nin standart sapması
- θ'nın medyanı
- θ'nın ortalaması
- θ'nın standart sapması
- İmzanın genişliği
- İmzanın yüksekliği

- En/Boy oranı

(3.7) ve (3.8) denklemleri kullanılarak x ve y yörüngesinin hem kartezyen hem de kutupsal koordinatlardaki değerlerinin ortalama ve standart sapmaları hesaplanmıştır. Yörüngelerdeki işaret değişimlerinin sayısını bulmak için x ve y yörüngesinin türevleri alınmıştır. Türevi alınan x ve y'nin işaret değişim sayıları sayılmıştır. Yukarıda bahsedilen özellikler imza vektöründe kullanılmıştır.

3.2.4 Zaman, Hız ve İvme Bilgisinden Çıkarılan Özellikler

Önceden hesaplanan hız, açısal hız ve ivme değerlerinden özellikler türetilerek kullanılan özelliklerin sayısı arttırılmalıdır. Türetilen özellikler;

- Hızın ortalaması
- Açısal hızın ortalaması
- İvmenin ortalaması
- Kalemin havada kalma süresi
- Kalemin temas süresi
- $Vx > 0$ olduğu süre
- $Vx < 0$ olduğu süre
- $Vy > 0$ olduğu süre
- $Vy < 0$ olduğu süre

Yukarıda bahsedilen değerler hesaplanarak özellik vektörüne eklenmiştir.

3.2.5 İmza Verilerinin Normalize Edilmesi

İmzanın x, y, basınç ve diğer üretilen öz niteliklerinin makine öğrenmesi algoritmalarında ve derin öğrenme modelinde eğitilebilmesi için değerlerini normalleştirmek gerekmektedir. Bu değerlerin her biri için (3.10)'daki min-max normalizasyon formülü uygulanarak normalleştirilmiştir. Şekil 3.6'da örnek imzadan çıkarılan normalize edilmiş bazı özelliklerin değerleri gösterilmiştir. Ek A'da Şekil A.2, Şekil A.4 ve Şekil A.6'de normaleştirme sonrası basınç, x ve y grafikleri gösterilmiştir.

$$x_i = \frac{x_i - min(x)}{max(x) - min(x)} \tag{3.10}$$

Tablo 3.1 İmzalar Üzerinden Çıkarılan Temel ve Ekstra Özellikler

No	Özellikler	
1	İmzanın ortalama hızı	Temel özellikler (9)
2	İmzanın ortalama ivmesi	
3	P'nin ortalaması	
4	Vuruş sayısı	
5	Kalemin Temas süresi	
6	Kalemin havadaki süresi	
7	En/boy oranı	
8	Genişlik	
9	Yükseklik	
10	X'in standard sapması	Ekstra özellikler (18)
11	Y'in standard sapması	
12	X'in ortalaması	
13	Y'nin ortalaması	
14	P'nin standar sapması	
15	Ortalama Açısal hızı	
16	Ortalama Theta	
17	Medyan Theta	
18	Standart sapma Theta	
19	Ortalama r	
20	Median r	
21	Standart sapma r	
22	X yönündeki işaret değişim sayısı	
23	Y yönündeki işaret değişim sayısı	
24	$Vx > 0$ olduğu süre	
25	$Vx < 0$ olduğu süre	
26	$Vy > 0$ olduğu süre	
27	$Vy < 0$ olduğu süre	

3.2.6 İmza Verisinden Örnekleme Alınması

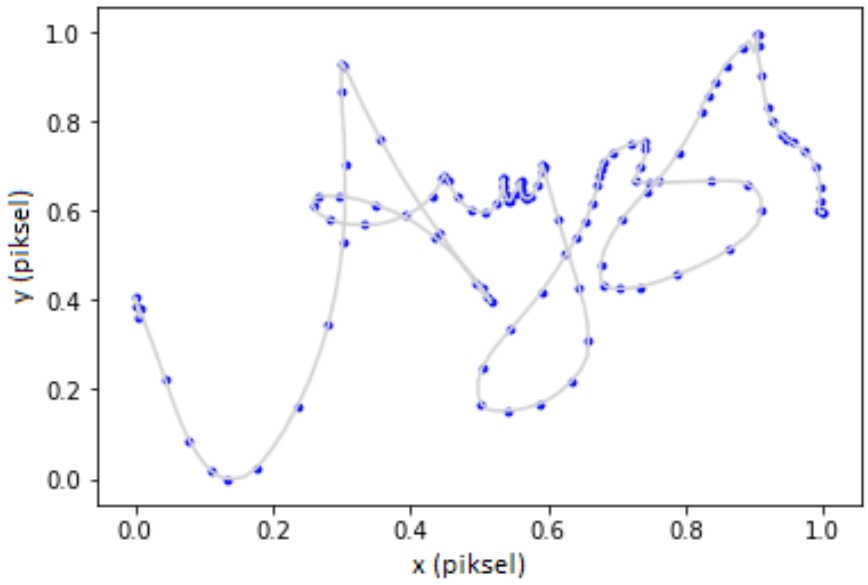
Bu adımda imza vektörüne eklemek üzere imza verilerinden örneklemeler alınmıştır. Bu örneklemeler imzanın 30 ms. de bir, toplamda 2 sn.'e olacak şekilde alınmıştır. İmzanın atılma süresi 2 sn.'den kısa ise vektör boyutlarını eşitlemek için 0 ile beslenerek tamamlanmıştır. Böylece her imzadan 80 örnek x, y ve basınç bilgisi toplamda 240 adet özellik olarak elde edilmiştir. Şekil 3.7 ve 3.8'de örnekleme grafiği gösterilmiştir. Bu örnekler imza vektörünün son kısmına eklenmiştir.

3.2.7 İmza Vektörlerinin Elde Edilmesi

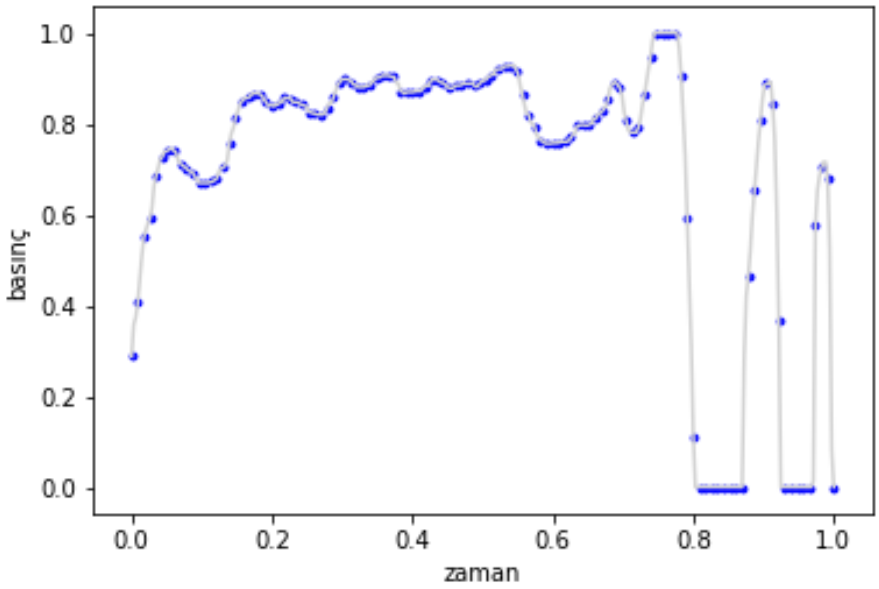
Bu adımda sınıflandırma yöntemlerinde kullanılacak imza vektörleri oluşturulmuştur. Daha önceden elde edilen özelliklerle birlikte imzadan alınan örnemkleme verisi birleştirilerek imzayı temsil eden vektör elde edilmiştir. İmza verisinden 27 ayrı özelliğe ek olarak 240 ayrı nitelik daha eklenerek imzayı temsil eden 268 uzunluğunda

Idx	Class	AvgX	SdX	AvgY	SdY	AvgP	SdP	AvgV	AvgA	AvgW
0	1	0.730328	0.853456	0.635057	0.897114	0.976113	0.74125	0.693843	0.676196	0.223949
1	1	0.739753	0.719771	0.754751	0.944757	0.952506	0.83592	0.725853	0.536674	0.787938
2	1	0.893708	0.787414	0.998396	0.959805	0.865392	0.7923	0.691187	0.648992	0.572565
3	1	1	1	1	0.924729	1	0.475344	0.633854	0.877165	0.23024
4	0	0.562806	0.743994	0.483953	0.44655	0.0738222	0.0692171	0.300677	0.890578	0.640065
5	0	0.318856	0.383718	0.579862	0.418047	0.170399	0.0603141	0.275569	0.999708	0.59577
6	0	0.277546	0.443148	0.531525	0.531792	0	0.0264252	0.381657	0.827243	0.629865
7	0	0.384806	0.567504	0.501923	0.595718	0.173109	0	0.341461	0.913917	0.436304

Şekil 3.6 İmzalardan Çıkarılan Bazı Özelliklerin Normalizasyon Sonrası Değerleri



Şekil 3.7 İmzanın X ve Y Yörüngesinden Alınan Örnekler



Şekil 3.8 İmzanın Basıncından Alınan Örnekler

vektör elde edilmiştir.

$$\overrightarrow{Sign_v} = \langle Class, F_1, F_2, .., F_{27}, x_1, y_1, p_1, .., x_{80}, y_{80}, p_{80} \rangle \tag{3.11}$$

(3.11) ile temsil edilen imza vektörü ile, topladığım AKSKL-42 ve SVC2004 veri setindeki imzalar tanıma işleminde kullanılmak üzere birleştirilmiştir. Ayrıca, sadece SVC2004 veri seti kullanılarak oluşturulan imza vektörleri, tasarlanan modeller yardımı ile imza doğrulama da kullanılmıştır.

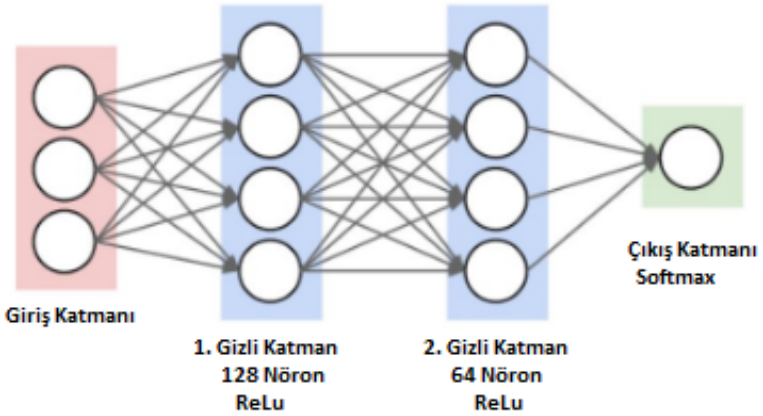
3.3 Sistem Tasarımı

Tez kapsamında deneysel çalışmalar iki başlık altında sunulmuştur. İlk aşamada bizim hazırladığımız AKSKL-42 ve literatürde yer alan SVC2004 imza verileri birleştirilerek oluşturulan veri seti üzerinde gerçekleştirilen imza tanıma işlemi gerçekleştirilmiştir. İkinci aşamada ise sadece SVC2004 veri seti kullanılarak imza doğrulama işlemi gerçekleştirilmiştir. İmza doğrulama adımında imzası alınmış her kişi ayrı ayrı modellenmiş ve başarımları ölçülmüştür.

İmza tanıma çalışmasında veri setinin eğitiminde Destek Vektör Makinesi, K-En Yakın Komşuluk, Naive Bayes ve Çok Katmanlı Yapay Sinir Ağı kullanılmıştır. İmza doğrulamada ise DVM, KNN, Naive Bayes, ÇKYSA ve derin öğrenme modellerinden Evrişimli Sinir Ağıları kullanılarak sistem eğitilmiş ve 5-KÇD kullanılarak sistemin başarısı ölçülmüştür. Sistemlerin eğitilmesinde kullanılan makine öğrenmesi yöntemlerinden Destek Vektör Makinelerinde doğrusal çekirdek (kernel) ve KNN algoritmasında k değeri 3 seçilmiş diğer parametreler değiştirilmemiştir.

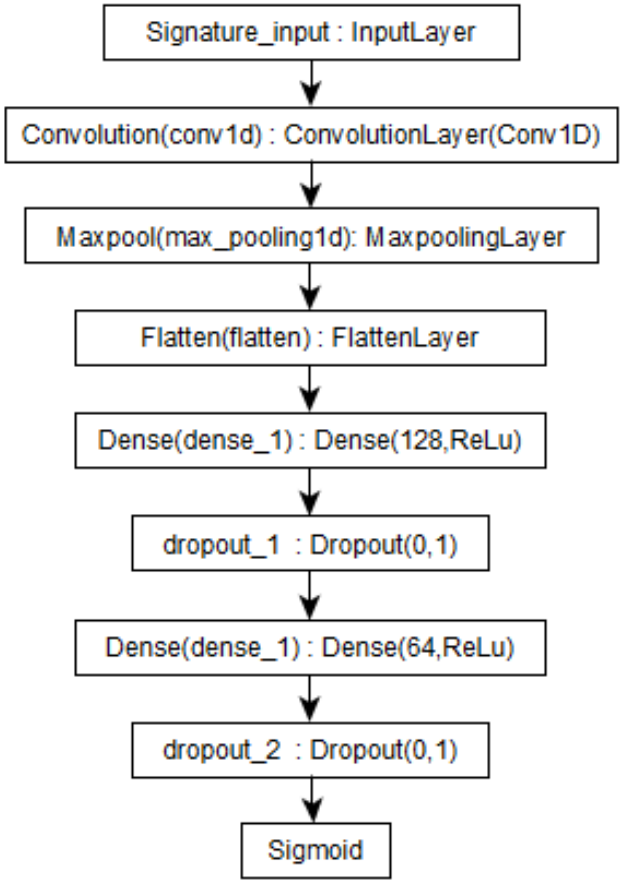
İmza tanıma çalışmasında kullanılan Çok Katmanlı Yapay Sinir Ağı modeli Şekil 3.9'da gösterilmiştir. Bu model giriş, 2 gizli ve çıkış katmanından oluşmaktadır. Birinci gizli katmanda 128 (yaklaşık giriş sayısı ve çıkış sayısının ortalaması), ikinci gizli katmanında 64 nöron ve aktivasyon fonksiyonu olarak ReLu kullanılmıştır. Çıkış katmanında aktivasyon fonksiyonu olarak sınıf etiketi sayısının fazla olmasından dolayı Softmax aktivasyon fonksiyonu kullanılmıştır. Epoch değeri 30 olarak ayarlanmıştır.

Sahte imzaların tespiti için kullanılan Evrişimsel Yapay Sinir ağı modeli de Şekil 3.10'da gösterilmiştir. Bu model giriş, evrişim katmanı, maksimum havuzlama (max pooling), düzleştirme (flatten), 2 tam bağlı gizli katman ve çıkış katmanından oluşmaktadır. Birinci gizli katmanda 128, ikinci gizli katmanda 64 nöron ve aktivasyon fonksiyonu olarak ReLu kullanılmıştır. Tasarlanan bu ESA'da evrişim



Şekil 3.9 Çok Katmanlı Yapay Sinir Ağı Modeli

boyutu 1D (boyut) olarak tanımlanmış olup, epoch 30, kernel 2 ve filtre ise 5 olarak ayarlanmıştır. Modelde her adımda 267 giriş değeri sisteme alınmaktadır. Konvolüsyon katmanı tamamlandıktan sonra filtrelerin etkisiyle girişi verisi 266x5 boyutunda matrise dönüştürülür. Maksimum havuzlama adımında veri 133x5 boyutuna indirilir. Düzleştirme katmanı çıkışında 665 uzunlukta tek boyutlu bir vektöre dönüştürülür. Ardından tam bağlı 2 gizli katman ve son olarak da çıkışa aktarılır.



Şekil 3.10 Evrişimsel Yapay Sinir Ağı Modeli

4
Deneysel Sonuçlar

Çalışmada imza tanıma ve doğrulama olmak üzere iki ayrı deney yapılmıştır. Bu deneylerde 2 farklı veri setinden elde edilen imza vektörleri ile sistemler eğitilerek başarımları ölçülmüştür.

Çalışmanın birinci deneyinde, AKSKL-42 ve SVC2004 imza veri seti birlikte kullanılmıştır. SVC2004 veri setinde 40 kişiye ait 40 imza örnegi bulunmaktadır. Bu 40 imza örneğinin 20 tanesi orijinal, 20 tanesi de uzman kişiler tarafından atılan sahte imzalardır. AKSKL-42 veri tabanına SVC2004 deki sadece orijinal imzalar eklenmiştir. Toplamda 82 kişinin ortalama 15 imzasının bulunduğu veri setiyle imza tanıma işlemleri, Destek Vektör Makineleri, Naive Bayes, K-En Yakın Komşuluk ve Çok Katmanlı Yapay Sinir Ağı modeliyle eğitilerek sistem test edilmiş ve başarımları ölçülmüştür.

İkinci deneyde ise literatürde kullanılan SVC2004 imza veri seti kullanılmıştır. Bu veri seti ile imzaların doğrulama işlemi gerçekleştirilmiştir. Burada sistem Destek Vektör Makinası, Naive Bayes, K-En Yakın Komşuluk, Çok Katmanlı Yapay Sinir Ağı ve Evrişimli Yapay Sinir Ağı modelleriyle eğitilerek başarımları ölçülmüştür.

4.1 Başarım Ölçütleri

Sistemlerin başarımını ölçmede hata matrisi (Confusion Matrix) kullanılmıştır. Hata matrisi çoğu zaman gerçek değerlerinin bilindiği bir dizi test verisi üzerinde bir sınıflama modelinin performansını tanımlamak için kullanılan bir tablodur. Bir algoritmanın performansının görselleştirilmesine izin verir. Sınıflar arasındaki karışıklığın kolayca tespit edilmesini sağlar. Çoğu performans ölçüsü, hata matrisi kullanılarak hesaplanır. Bize sadece bir sınıflandırıcı tarafından yapılan hatalar hakkında değil, daha da önemlisi yapılan hata türleri hakkında da bilgi verir (Tablo 4.1).

- Doğru Pozitif (DP): Gerçek imzanın sistem tarafından gerçek tahmin edilmesi

- Yanlış Pozitif (YP): Sahte imzanın sistem tarafından gerçek tahmin edilmesi
- Doğru Negatif (DN): Sahte imzanın sistem tarafından sahte tahmin edilmesi
- Yanlış Negatif (YN): Gerçek imzanın sistem tarafından sahte tahmin edilmesi

Tablo 4.1 Hata Matrisi

		Tahmin edilen	
		Evet	Hayır
Gerçek veri	Evet	DP	YN
	Hayır	YP	DN

Doğruluk (Accuacry) toplam doğru eşleştirmelerin toplam veri setine bölümüyle bulunur (4.1). Duyarlılık (Recall) sistemin tanıdığı gerçek imzaların toplam gerçek imzaların yüzdesini ölçerken (4.2), Hassasiyet (Precision) sistem tarafından tanınan gerçek imzaların doğru olarak tanınmış imzalar oranını vermektedir (4.3). F-ölçüsü (F-measure) duyarlılık ve hassasiyet değerlerinin ağırlıklı harmonik ortalamasıdır (4.4). Yanlış Kabul Oranı (YKO), biyometrik güvenlik sisteminin yetkisiz bir kullanıcı tarafından erişim girişimini hatalı bir şekilde kabul etme ihtimalinin bir ölçüsüdür. YKO tipik olarak, sahte kabul sayısının, tanıma girişimi sayısına oranı olarak ifade edilir (4.5). Yanlış Reddetme Oranı (YRO), biyometrik güvenlik sisteminin yetkili bir kullanıcı tarafından erişim girişimini hatalı bir şekilde reddetme ihtimalinin bir ölçüsüdür. Bir sistemin FRR'si tipik olarak, yanlış tanıma sayısının, tanıma girişimlerinin sayısına bölünmesiyle bulunur (4.6). Eşit Hata Oranı (EHO), biyometrik sistemlerin performansının değerlendirimesinde kullanılan bir ölçümdür. Sistemin YKO'nın YRO'ya eşit olduğu noktayı temsil eden değerdir (4.7). EER değerinin küçük olması biyometrik sistemin daha başarılı olduğunu gösterir.

$$Dogruluk = \frac{DP + DN}{DP + DN + YP + YN} \tag{4.1}$$

$$Duyarlilik = \frac{DP}{DP + YN} \tag{4.2}$$

$$Hassasiyet = \frac{DP}{DP + YP} \tag{4.3}$$

$$F - olcusu = \frac{2 * Duyarlilik * Hassasiyet}{Duyarlilik + Hassasiyet} \tag{4.4}$$

$$YKO = \frac{YP}{DN + YP} \tag{4.5}$$

$$YRO = \frac{YN}{DP + YN} \tag{4.6}$$

$$EHO = \frac{YKO + YRO}{2} \tag{4.7}$$

4.2 İmza Tanıma Test Sonuçları

Bu deneyde kullanılacak imzaların tamamından oluşmaktadır. AKSKL-42 ve SVC2004 Task 2 veri tabanındaki imzalar birleştirilerek kullanılmıştır. Toplamda 82 kullanıcının ortalama 15 gerçek imzasının bulunduğu bir veri seti elde edilmiştir. Bu veri seti Destek Vektör Makinesi, KNN, Naive Bayes ve Şekil 3.9'da verilmiş olan Çok Katmanlı Yapay Sinir Ağı ile eğitilerek performansları karşılaştırılmıştır. Ayrıca, imzada kullanılan özelliklerin sınıflama başarımlarına etkisi AKSKL-42, birleştirilen AKSKL-42 ve SVC2004 imzaları üzerinde incelenmiştir. İlk olarak iki veri setinin imza vektörleri temel özellikler kullanılarak çıkarılmıştır. DVM, KNN, NB ve ÇKYSA ile eğitilerek başarımları ölçülmüştür. Daha sonra aynı iki imza seti çıkarılan tüm özellikler kullanılarak imza vektörleri oluşturulup yine aynı modellerle eğitilip sınıflama başarımları elde edilmiştir. İmza tanıma snıflama başarımları Tablo 4.2'de gösterilmiştir. Bu tabloya göre en başarılı sınıflandırma %95 ile Destek Vektör Makinesidir. Tablo incelendiğinde imza vektörleri oluşturulurken kullanılan özelliklerin arttırılması sınıflama başarımlarını arttırmıştır. Tablo 4.2 'den rahatça görülebileceği gibi imza vektörlerinde kullanılan 9 temel özellikliğin 27'e çıkarılması modellerin başarımını %2 - %5 oranında iyileştirdiğini göstermektedir.

Tablo 4.2 İmza Tanıma Sınıflama Başarımları

Özellik	**Veri Setleri**	**KNN**	**NB**	**ÇKYSA**	**DVM**
Temel Özellikler (9)	AKSKL-42	0,83	0,81	0,87	0,88
	AKSKL-42 + SVC2004	0,86	0,82	**0,92**	**0,92**
Toplam Özellikler (27)	AKSKL-42	0,86	0,84	0,91	0,93
	AKSKL-42 + SVC2004	0,88	0,84	0,94	**0,95**

4.3 İmza Doğrulama Test Sonuçları

Bu deneyde SVC2004 veri seti kullanılmıştır. Gerçek ve sahte imzaların bulunduğu veri setleri kullanıcı bazlı eğitilerek sınıflama başarımları ölçülmüştür. Eğitim setinde 40 kulanıcıdan alınmış 20 gerçek imza ve 20 tane de uzman kişiler tarafından atılmış 20 sahte imza bulunmaktadır. Sistem 5 Katlı Çapraz Doğrulama ile modellenmiştir.

Sistem modellenirken Destek Vektör Makinesi, Evrişimli Sinir Ağı, K-En Yakın Komşuluk, Çok Katmanlı Yapay Sinir Ağı ve Naive Bayes algoritmaları 5 Katlı Çapraz Doğrulama ile modellenmiştir. Her kullanıcı için sistem ayrı modellendiğinden 40 farklı Hata Matrisi oluşturulmuştur. Ancak, sistemin genel başarısı için tüm kullanıcıların Hata Matrisleri toplanarak yöntem bazında dört farklı hata matrisi çıkarılmıştır. Hata matrisi üzerinde doğruluk, duyarlılık, hassasiyet, F-ölçüsü, YKO, YRO ve EHO değerleri hesaplanmıştır.

Tablo 4.3 Destek Vektör Makineleri Hata Matrisi

		Tahmin edilen	
		Gerçek İmza	Sahte İmza
Gerçek veri	Gerçek İmza	780	20
	Sahte İmza	24	776

Sistemin DVM yöntemi ile alınan başarı sonuçları Tablo 4.3'deki hata matrisinde gösterilmiştir. DVM'de doğrusal kernel kullanılmıştır. Tablo 4.3'ü incelediğimizde YN değerinin (20) diğer yöntemlere göre en düşük değeri verdiğini görmekteyiz. YN değeri veri setinde gerçek olan imzaların sistem tarafından sahte imza olarak kabul edildiğini göstermektedir. YN değerinin yüksek olması kullanıcı tarafından maddi bir kayıba neden olmadığı için tolere edilebilir. Sistemde YP değerinin düşük olması çok daha önemlidir. Çünkü YP değeri sahte olan imzaların sistem tarafından gerçek algılandığını göstermektedir. Bu da sistemin güvenliğinin kötü olduğunu göstermektedir. Hata matrisinde görüldüğü üzere YP değerleri düşük değer vermiştir. DVM'nin hata matrisinde elde edilen verilere göre DVM ile doğrulama oldukça başarılı bir sonuç alınmıştır. DVM ile eğitilen sistemin doğruluğu %97,2 ve EHO değeri %2,75 dir.

Tablo 4.4 Evrişimli Sinir Ağı Hata Matrisi

		Tahmin edilen	
		Gerçek İmza	Sahte İmza
Gerçek veri	Gerçek İmza	758	42
	Sahte İmza	17	783

Sistemin Evrişimli Sinir Ağı modeli (Şekil 3.10) ile alınan başarı sonuçları Tablo 4.4'deki hata matrisinde gösterilmiştir. Tablo 4.4 incelendiğinde YP değerinin (17) diğer yöntemlere göre en düşük değeri verdiğini görmekteyiz. Sistemin başarımı

DVM'a göre düşük olsa da YP değerinin düşük olması sistemin daha güvenilir olduğunu göstermektedir. ESA modelinin başarım sonuçları Tablo 4.7'de gösterilmiştir. Sistemin doğruluğu %96,3 ve EHO değeri %3,68 dir.

Tablo 4.5 K-En Yakın Komşuluk Hata Matrisi

		Tahmin edilen	
		Gerçek İmza	Sahte İmza
Gerçek veri	Gerçek İmza	775	25
	Sahte İmza	58	742

K-En Yakın Komşuluk algoritmasında k değeri 3 seçilerek eğitim yapılmıştır. KNN ile eğitilen sistemin hata matrisi Tablo 4.5'de verilmiştir. Hata matrisi incelendiğinde YP değerinin (58) yüksek olduğu görülmektedir. Sistemin doğruluk değeri %94,8 ve EHO değeri %5,18 dir.

Tablo 4.6 Çok Katmanlı Yapay Sinir Ağı Hata Matrisi

		Tahmin edilen	
		Gerçek İmza	Sahte İmza
Gerçek veri	Gerçek İmza	736	64
	Sahte İmza	31	749

Sistemin Çok Katmanlı Yapay Sinir Ağı ile alınan başarı sonuçları Tablo 4.6'da verilmiştir. Hata matrisi incelendiğinde YP değerinin (64) yüksek olduğu görülmektedir. Sistemin doğruluk değeri %92,8 ve EHO değeri %5,98 dir.

Tablo 4.7 Naive Bayes Hata Matrisi

		Tahmin edilen	
		Gerçek İmza	Sahte İmza
Gerçek veri	Gerçek İmza	732	68
	Sahte İmza	90	710

Sistemin Navie Bayes algoritması ile alınan başarı sonuçları hata Tablo 4.7'deki hata matrisi ile gösterilmiştir. Tablo 4.7 incelendiğinde YP değerinin (90) diğer yöntemlere göre en yüksek değeri verdiğini görmekteyiz. Sınıflama modellerine göre en kötü sınıflama değerleri Naive Bayes ile elde edilmiştir. Sistemin doğruluk değeri %90

ve ERR değeri %9,8 dir. NB ile eğitilen sistemin, imza vektörleri için kötü sınıflama modeli olduğu görülmektedir.

Sistemde kullanılan yöntemlerin imza doğrulama başarım sonuçları Tablo 4.8'de gösterilmektedir. Bu tabloya göre kullanılan eğitim modellerinde en iyi başarı DVM ile alınmıştır. DVM ile %2,75 EHO elde edilmiştir.

Tablo 4.8 İmza Doğrulama Başarım Sonuçları

Yöntem	**Doğruluk**	**Duyarlılık**	**Hassaslık**	**F-ölçüsü**	**YKO(%)**	**YRO(%)**	**EHO(%)**
DVM	0,972	0,975	0,97	0,972	3,0	2,5	2,75
CNN	0,963	0,947	0,978	0,962	2,12	5,25	3,68
KNN	0,948	0,968	0,93	0,949	7,25	3,12	5,18
ÇKYSA	0,928	0,92	0,95	0,939	3,97	8	5,98
NB	0,90	0,915	0,89	0,902	11,25	8,5	9,8

Tablo 4.9 SVC2004 Task 2 Yarışması Performans Sonuçları [19]

Takım Numarası	**Ortalama EHO(%)**
1	3,02
2	3,47
3	4,23
4	4,45
5	3,08
6	4,41
7	6,39
8	4,29
9	5,07
10	8,75
Önerilen Yöntem	DVM:**2,75** ESA: 3,68 KNN: 5,18, ÇKYSA: 5,98 NB: 9,8

SVC2004 yarışmasında 10 farklı takımının Task 2 veritabanı kullanılarak imza doğrulama performans sonuçları Tablo 4.9'de gösterilmiştir. Bu yarışmada bir kullanıcının gerçek imzalarının %25'i referans olarak seçilmiştir. Seçilen bu referans imzaları rasgele seçilmiştir. Tutarlı sonuçlar elde edilebilmesi için 10 kez hesaplama yapılarak ortalama sonuçlar elde edilmiştir. Tablo incelendiğinde takımların EHO değerleri ile önerdiğimiz sistemin DVM ile elde edilen EHO değeri karşılaştırıldığında en başarılı olduğunu görülmektedir. Ayrıca, ESA ile modellenen sistemde kayda değer başarı elde ettiği görülmektedir.

Tablo 4.10'da daha önceden yapılan bazı biyometrik imza doğrulama çalışmalarından elde edilen sonuçlar gösterilmiştir. Bu çalışmalarda, imza doğrulamada kullandığımız SVC2004 Task 2 veri tabanı kullanılmıştır. Tablo incelendiğinde önerdiğimiz sistemin başarımı en iyi ikinci olduğu görülmektedir.

Tablo 4.10 SVC2004 Task 2 Veri Seti Kullanılarak Geliştirilen İlgili Çalışmaların Başarımları [35]

Referans	**Ortalama EHO(%)**
SVC2004 competition,2004	3,02
Fierrez-Agular et al. 2005	DWT: 14,26 HMM:15,04 Fusion :10,91
Fierrez-Aguilar et al. 2005)	7,14
Hu & Wang,2007	Local Feature: 4 Global Feature:16,38 Fusion :3,02
Adamski & Saeed ,2008	7
Gruber et al.2010)	SVM-Euclid: 13,84 SVM-DTW: 16,06 SVM-LCSS: 6,84
S. Rashidi & A. Fallah,2012	**2,04**
Önerilen Yöntem	DVM:**2,75** ESA: 3,68 KNN: 5,18, ÇKYSA: 5,98 NB: 9,8

5
Sonuç ve Öneriler

İmzalar, toplumumuzda yüzlerce yıldır bir kimlik doğrulama şekli olarak kabul edilmiştir. Gelişen teknolojinin beraberinde getirdiği yeniliklerden imza süreçleri de iyi yönde etkilenmiştir. Bu yeniliklerin başında elektronik ortamda atılan ve kişinin imza karakteristiğini de tespit etmeye yarayan biyometrik imzalama yöntemi gelmektedir.

Biyometrik imza doğrulama en çok kabul edilen tekniklerden biridir. Biyometrik imza teknikleri, iris gibi diğer biyometrik tekniklerden daha az doğru olmasına rağmen günlük yaşamın bir parçası haline gelmiştir. Bir imza doğrulama sistemi, imza sahteciliğini tespit edebilmeli ve aynı zamanda orijinal imzaların reddedilmesini azaltabilmelidir.

Bu tez çalışmasında biyometrik imza tanıma ve imza doğrulama olarak iki ayrı deney yapılmıştır. Gerçekleştirilen biyometrik imza tanıma ve doğrulama çalışmasında elde edilen sonuçlar tasarlanan sistemin başarılı olduğunu göstermiştir. Çalışmada toplanan biyometrik imza veri seti AKSKL-42 ve SVC2004 Task 2 veri seti kullanılarak, her imza örneğini temsil eden birer imza vektörleri oluşturulmuştur. Bu imza vektörlerinin oluşturulması iki adımda gerçekleştirilmiştir. İlk olarak, biyometrik imzaların dinamik bilgilerinden 27 özellik çıkarılmış, ikinci olarak da imzalar üzerinde bir zaman serisi boyunca alınan örnekler imza vektörüne eklenmiştir. Bu ekleme işlemi ile imza daha da özelleştirilmiştir.

Tezin imza tanıma bölümünde AKSKL-42 ve SVC2004 deki orijinal imza verileri birleştirilerek toplamda 82 kullanıcıdan oluşan imza veri seti oluşturulmuştur. Bu veri seti ile çeşitli makine öğrenmesi ve yapay sinir ağı modelleriyle sistem çalıştırılmış ve başarımları ölçülmüştür. Sistemin en iyi başarımı Destek Vektör Makinasi ile 2,75 EHO alınmıştır. İmzadan çıkarılan doğru özelliklerin arttırılması imzanın ayırt edici özelliğini arttırmıştır. İmza vektörleri ilk olarak 9 temel özellik ile oluşturulmuş ve sistem modellenerek başarımları ölçülmüştür. Daha sonra özellik sayısı 27'e çıkarılarak aynı işlemler gerçekleştirilerek başarımlar elde edildi. İmza vektörlerinde

özellik sayısının arttırılması sistemde %2 - %5 aralığında iyileştirme yapmıştır. Yani, imza verisinden türetilen ve imzanın karakteristiğini güçlendirecek niteliklerin belirlenmesi önemlidir.

İmza doğrulama bölümünde SVC2004 Task 2 verisi kullanılmıştır. Bu veri seti Destek Vektör Makinesi, k-En Yakın Komşuluk, Naive Bayes, Çok Katmanlı Yapay Sinir Ağı ve Evrişimsel Yapay Sinir Ağı ile modelenerek sistemin başarısı ölçülmüştür. Çalışmadaki biyometrik doğrulama sonuçları aynı veri setiyle yapılan diğer çalışmalarla karşılaştırıldığında sistemin kayda değer sonuçlar aldığı görülmüştür.

Bu sistemin biyometrik imza tanıma ve doğrulama için ticari bir ürün olarak geliştirildiği düşünülürse, Destek Vektör Makinası veya Evrişimli Sinir Ağı modelinden biri seçilebilir. Sistemde sahte imzaların gerçek imza olarak kabul edilmesi kullanıcılar için maddi bir kayba neden olabilir. Sistemin doğruluğunun yanı sıra bu Yanlış Kabul Oranının değerinin de minimum olması beklenilir. Her iki modelde de hem doğruluk değeri yüksek hem de bu YKO değerinin düşük olduğu görülmüştür.

Sonuç olarak, çalışmada biyomektrik imzaları temsil etmek için oluşturulan vektörün sınıflama başarımları test edilmiştir. Bu çalışmada yaygın olarak kullanılan SVC2004 imza veri tabanı kullanılmıştır. Yapılan çalışmada başarılı sonuçlar alınmasına rağmen sistemde bazı geliştirmeler yapılarak daha iyi sonuçlar alınabilmesi sağlanabilir. Gelişen teknolojiyle üretilen imza tabletlerinden alınan bilgilerin çeşitliliği, türetilecek özelliklerin arttırılması ile imza vektörlerinin ayırt edici özellikleri güçlendirilebilir. Gelecek çalışmalarda türetilen parametrik özelliklerin çeşitliliği artırılarak sistemin sınıflandırma başarımı üzerindeki etkileri de araştırılabilinir.

Kaynakça

[1] I. Bhattacharya, P. Ghosh, S. Biswas, "Offline signature verification using pixel matching technique," in *Conference on Computational Intelligence: Modeling Techniques and Applications*, vol. 10, 2013, pp. 970–977.

[2] R. A. Mohammed, R. M. Nabi, S. M-Raouf, R. M. Nabi, "State-of-the-art in handwritten signature verification system," in *International Conference on Computational Science and Computational Intelligence*, 2015.

[3] I. V. Anikin E. S. Anisimova, "Handwritten signature recognition method based on fuzzy logic," in *Dynamics of Systems, Mechanisms and Machines (Dynamics)*, IEEE, 2016.

[4] M. Bashir J. Kempf, "Area bound dynamic time warping based fast and accurate person authentication using a biometric pen," *Conference on Computational Intelligence: Modeling Techniques and Applications*, 2013.

[5] D. Guru H. N. Prakash, "Online signature verification and recognition:an approach based on symbolic representaion," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2009.

[6] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, j. Ortega-Garcia, D. Maltoni, "An on-line signature verification system based on fusion of local and global ınformation," *Audio- and Video-Based Biometric Person Authentication*, vol. 3546, pp. 523–532, 2005.

[7] J. Suraiya Z. Farhana Javed, "Biometric signature verification," *International Journal of Biometrics*, vol. 7, pp. 97–118, 2015.

[8] G. Taherzadeh, R. Karimi, A. Ghobadi, H. Modaberan, "Evaluation of online signature verification features. in advanced communication technology," *13th International Conference on Advanced Communication Technology (ICACT2011)*, 2011.

[9] P. Kumar, S. Singh, A. Garg, Prabhat, "Hand written signature recognition and verification using neural network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 558–565, 2013.

[10] K. Alisher Y. Berrin, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters*, vol. 26, pp. 2400–2408, 2005.

[11] E. Karagedikli, "Sınırlı dokunmatik ekran verileri kullanarak el yazısı imzası doğrulamak için geliştirilmiş bir yöntem," *Yüksek Lisans Tezi*, 2015.

[12] H. Oscar Miguel, P. Luis Mengibar, L. Michael G., L.-J. Judith, "On-line signature verification by dynamic time warping and gaussian mixture models," *2007 41st Annual IEEE International Carnahan Conference on Security Technology*, 2006.

[13] A. Marcin S. Khalid, "Online signature classification and its verification system," *7th Computer Information Systems and Industrial Management Applications*, 2008.

[14] S.-B. Napa M. Nasir, "A simple and effective method for online signature verification," *2013 International Conference of the BIOSIG Special Interest Group (BIOSIG)*, 2013.

[15] J. Anil K., D. G. Friederike, D. C. Scott, "On-line signature verification," *Pattern Recognition*, vol. 35, pp. 2963–2972, 2002.

[16] G. K. Gupta R. C. Joyce, "Using position extrema points to capture shape in on-line handwritten signature verification," vol. 40, 2007, pp. 2811–2817.

[17] M. Musa H. Lim Boon, "Biometric signature verification using pen position, time, velocity and pressure parameters," 2012.

[18] N. Seungsoo, P. Hosung, S. Changho, C. Daeseon, "Forged signature distinction using convolutionan neural network for feature extraction," *Applied Sciences*, 2018.

[19] Y. Dit-Yan, C. Hong, X. Yimin, G. Susan, K. Ramanujan, M. Takashi, R. Gerhard, "Svc2004: First ınternational signature verification competition," 2004.

[20] R. P. Tina S. S. Sherekar, "Performance analysis of naive bayes and j48 classification algorithm for data classification," *International Journal Of Computer Science And Applications*, vol. 6, 2013.

[21] G. Rohith, "Support vector machine — ıntroduction to machine learning algorithms," 2018. [Online]. Available: `https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47` (visited on 11/22/2019).

[22] K. Alexandros, M. David, H. Kurt, "Support vector machines in r," *Journal of Statistical Software*, vol. 15, 2006.

[23] B. Adi, "A quick ıntroduction to k-nearest neighbors algorithm," 2017. [Online]. Available: `https://blog.usejournal.com/a-quick-introduction-to-k-nearest-neighbors-algorithm-62214cea29c7` (visited on 11/18/2019).

[24] S. Harshita, "What ıs k-fold cross validation," 2017. [Online]. Available: `https://magoosh.com/data-science/k-fold-cross-validation/` (visited on 11/30/2019).

[25] E. A. Cagri, "K-fold cross validation," 2017. [Online]. Available: `http://cagriemreakin.com/veri-bilimi/k-fold-cross-validation-1.html` (visited on 11/30/2019).

[26] I. A. Basheera M. Hajmeerb, "Artificial neural networks: Fundamentals, computing, design, and application," *Journal of Microbiological Methods*, vol. 43, pp. 3–31, 2000. DOI: `https://doi.org/10.1016/S0167-7012(00)00201-3`.

[27] W. Mcculloch W. Pitts, "A logical calculus of the ideas immanent in nervous activity," *Bulletin Of Mathematical Biophysics*, vol. 5, pp. 115–133, 1943.

[28] A. Seker, "Derin öğrenme yöntemleri ve uygulamaları hakkında bir inceleme," *Doktora Semineri*, 2017. [Online]. Available: http://www.hasanbalik.com/projeler/doktora_seminer/10.pdf (visited on 11/30/2019).

[29] S. L. Brunton J. Nathan Kutz, "Neural networks and deep learning," *Data Driven Science Engineering Machine Learning, Dynamical Systems, and Control*, pp. 195–226, 2019. DOI: https://doi.org/10.1017/9781108380690.007.

[30] "Convolutional neural network tutorial: From basic to advanced," [Online]. Available: https://missinglink.ai/guides/convolutional-neural-networks/convolutional-neural-network-tutorial-basic-advanced/ (visited on 12/04/2019).

[31] Prabhu, "Understanding of convolutional neural network (cnn) — deep learning," 2018. [Online]. Available: https://medium.com/@RaghavPrabhu/understanding-of-convolutional-neural-network-cnn-deep-learning-99760835f148 (visited on 11/22/2019).

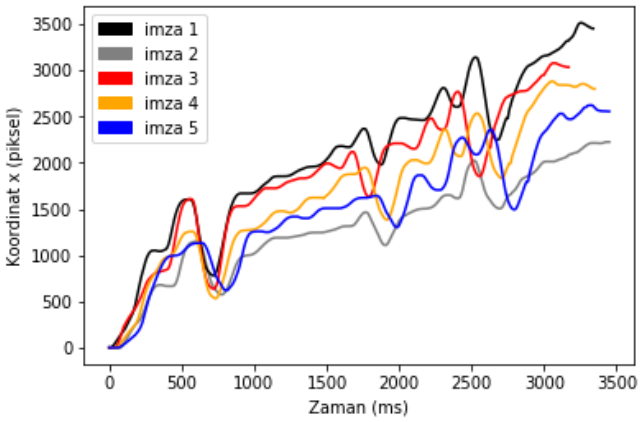
[32] "File:max pooling.png - wikimedia commons," [Online]. Available: https://commons.wikimedia.org/wiki/File:Max_pooling.png (visited on 11/18/2019).

[33] E. S. Sadi, "Sigmoid fonksiyon," 2008. [Online]. Available: http://bilgisayarkavramlari.sadievrenseker.com/2008/11/02/sigmoid-fonksiyon (visited on 11/18/2019).

[34] A. K. Merve, "Derin öğrenme için aktivasyon fonksiyonlarının karşılaştırılması," 2019. [Online]. Available: https://medium.com/@ayyucekizrak/derin-%C3%B6%C4%9Frenme-i%C3%A7in-aktivasyon-fonksiyonlar%C4%B1n%C4%B1n-kar%C5%9F%C4%B1la%C5%9Ft%C4%B1r%C4%B1lmas%C4%B1-cee17fd1d9cd (visited on 11/18/2019).

[35] S. Rashidi, A. Fallah, F. Towhidkhah, "Feature extraction based dct on dynamic signature verification," *Scientia Iranica*, vol. 19, pp. 1810–1819, 2012.

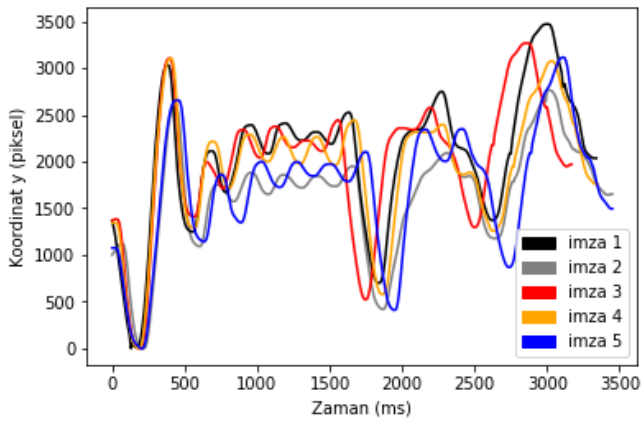
A
İmza Şekilleri



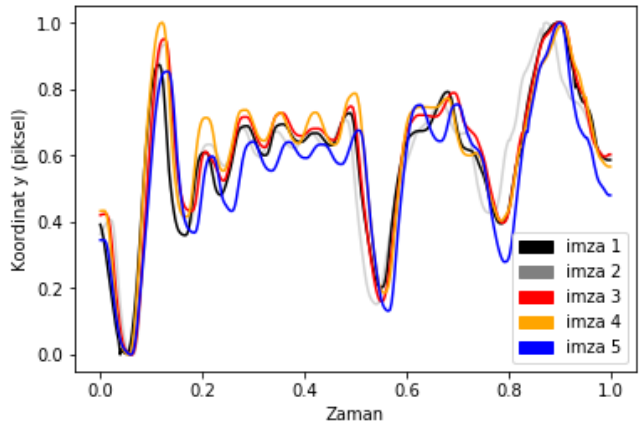
Şekil A.1 Bir Kişiye Ait 5 İmza Örneğinin X Yörüngesindeki Grafiği



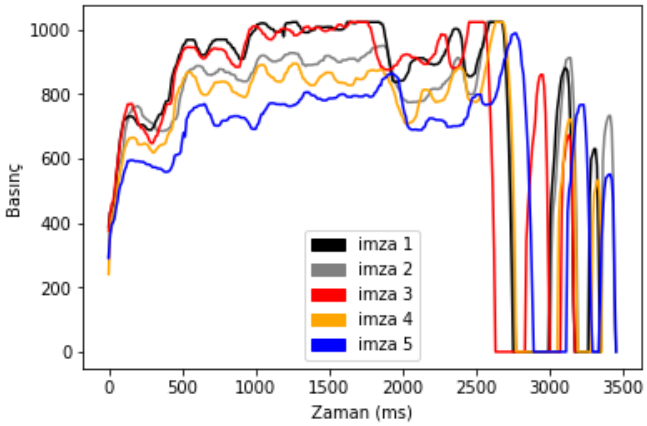
Şekil A.2 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası X Yörüngesindeki Grafiği



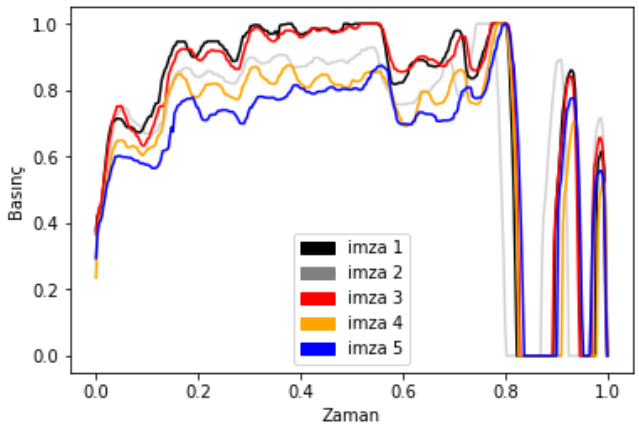
Şekil A.3 Bir Kişiye Ait 5 İmza Örneğinin Y Yörüngesindeki Grafiği



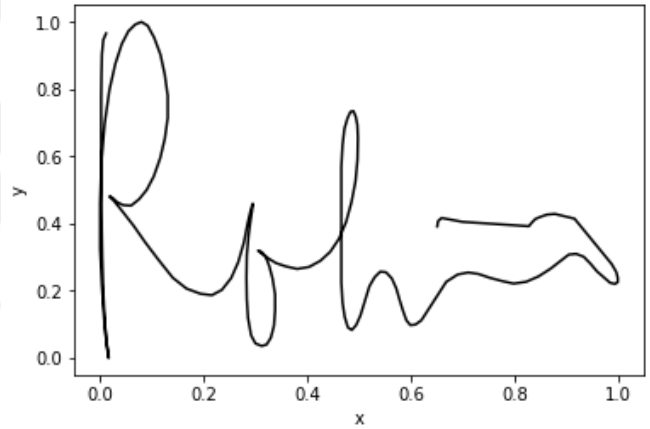
Şekil A.4 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası Y Yörüngesindeki Grafiği



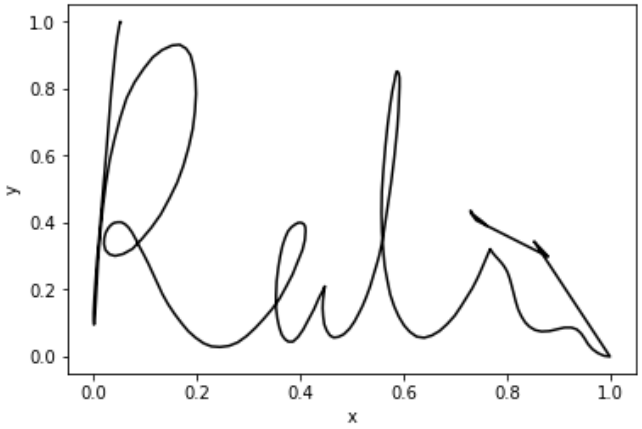
Şekil A.5 Bir Kişiye Ait 5 İmza Örneğinin Basınç Grafiği



Şekil A.6 Bir Kişiye Ait 5 İmza Örneğinin Normalleştirme Sonrası Basınç Grafiği



Şekil A.7 SVC2004 Veri Setinde Bulunan Orijinal İmza Örneği



Şekil A.8 SVC2004 Veri Setinde Bulunan Sahte İmza Örneği

Tezden Üretilmiş Yayınlar

İletişim Bilgileri: mhmmt.aksakal@gmail.com

Konferans Bildirisi

1. Aksakal M., Diri B. “Çevrimiçi Biyometrik İmza Tanıma,” - Hezarfen Uluslararası Fen Matematik ve Mühendislik Bilimleri Kongresi, pp. 37-44, 2019