

**T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**DAVRANIŞSAL BİYOMETRİ: KİMLİK DOĞRULAMA VE ANOMALİ TESPİT
UYGULAMALARINDA KULLANILAN YÖNTEMLER**

FATMA GÜMÜŞ

**DOKTORA SEMİNERİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI**

DANIŞMAN

İÇİNDEKİLER

İÇİNDEKİLER	vi
SİMGE LİSTESİ	viii
KISALTMA LİSTESİ	ix
ŞEKİL LİSTESİ.....	xi
ÇİZELGE LİSTESİ	xii
ÖZET	xiii
ABSTRACT	xiv
BÖLÜM 1	1
GİRİŞ	1
1.1 Davranışsal Biyometriye Genel Bakış.....	1
1.2 Biyometrik Kimlik Doğrulama ve Anomali Tespitinin Genel Yapısı.....	3
1.3 Seminerin Amacı ve İçeriği.....	7
BÖLÜM 2	10
VÜCUT DİNAMİKLERİNE DAYALI DAVRANIŞSAL BİYOMETRİ	10
2.1 Yürüyüş ve Üst Vücut Hareketi	10
2.1.1 Model Tabanlı Çalışmalar	11
2.1.2 Bütünsel Yaklaşım Uygulayan Çalışmalar	12
2.1.3 Sensör Ölçümleri Kullanan Çalışmalar	16
2.2 Ses ve Konuşma	17
2.3 Göz Hareketleri ve Bakış	20
2.4 El Mimikleri	22
2.5 Dudak Hareketleri	23
BÖLÜM 3	26

BİLGİSAYAR ÇEVRE BİLEŞENLERİ VE TAŞINABİLİR CİHAZ ETKİLEŞİMİNE DAYALI DAVRANIŞSAL BİYOMETRİ	26
3.1 Tuşlama Dinamikleri	26
3.2 Fare Etkileşimi Dinamikleri	30
3.3 Dokunmatik Ekran Etkileşimi	32
3.4 Taşınabilir Cihaz Etkileşimine Dayalı Diğer Yöntemler	38
BÖLÜM 4.....	40
İMZA ve DAVRANIŞ DİNAMİKLERİ.....	40
4.1 İmza Dinamikleri	40
4.2 Davranış Dinamikleri	45
BÖLÜM 5.....	48
DEĞERLENDİRME VE DAVRANIŞSAL BİYOMETRİ UYGULAMALARININ GELECEĞİ.....	48
KAYNAKLAR.....	51

$x_L^y(t)$	: t zamanında y eksenini boyunca en soldaki sınır pikselinin x-koordinat değerleri
$x_R^y(t)$	: t zamanında y eksenini boyunca en sağdaki sınır pikselinin x-koordinat değerleri
$y_U^x(t)$	: t zamanında x eksenini boyunca en üst sınır pikselinin y-koordinat değerleri
$y_D^x(t)$	: t zamanında x eksenini boyunca en alttaki sınır pikselinin y-koordinat değerleri
m_{UBM}	: UBM parametrelerinden oluşan süper-vektör
θ	: toplam olabilirlik fonksiyonu
$Y_i^{c_k}$	: i'inci örnek için c_k sınıflandırıcısından elde edilen olabilirlik sonucu
x_n, y_n	: n'inci örneğin ekrandaki x,y pozisyonu
t_n	: n'inci örneğe ilişkin zaman vektörü
p_n	: n'inci örnek için ekran üzerine uygulanan basınç
A_n	: n'inci örnek için parmağın ekranda kapladığı alan
o_n^f	: n'inci örnek için f indeksli parmağın yönü
o_n^{ph}	: ph telefonu üzerindeki n'inci örnek için ekranın dikey yada yatay olması

KISALTMA LİSTESİ

AER	Average Error Rate (Ortalama Hata Oranı)
AIS	Artificial Immune System (Yapay Bağışıklık Sistemi)
ANN	Artificial Neural Network (Yapay Sinir Ağı)
COG	Center of Gravity (Ağırlık Merkezi)
DCT	Discrete Cosine transform (Ayrık Cosine Dönüşümü)
DTW	Dynamic Time Warping (Dinamik Zaman Bükmesi)
EER	Equal Error Rate (Eş Hata Oranı)
ELM	Extreme Learning Machine (Aşırı Öğrenme Makinesi)
EM	Expecttation Maximization (Beklentiye Büyütme)
EoC	Ensembles of Classifiers (Sınıflandırıcı Toplulukları)
EOG	Elektro-oculography
FAR	False Acceptance Rate (Hatalı Kabul Oranı)
FNR	False Negative Rate (Hatalı Negatif Oranı)
FPR	False Positive Rate (Hatalı Pozitif Oranı)
FRR	False Reject Rate (Hatalı Ret Oranı)
GEI	Gait Energy Image (Yürüyüş Enerji Görüntüsü)
GMM	Gaussian Mixture Model (Gauss Karışım Modeli)
GSO	Gravitational Search Optimization (Yerçekimi Arama Optimizasyonu)
HMM	Hidden Markov Model (Saklı Markov Modeli)
HMOG	Hand Movement Orientation and Grasp (El Hareketleri Yönlendirmesi ve Kavraması)
HSV	Hue, Saturation, Value (Ton, Doygunluk, Değer) renk uzayı
KNN	K-Nearest Neighbor (K-En Yakın Komşu)
LDA	Linear discriminant Analysis (Doğrusal Diskriminant Analiz)
LPCC	Linear Predictive Coding Coefficients (Doğrusal
MCNN	Meta Cognitive Neural Network (Meta Bilişsel Sinir Ağı)
MD	Mahalanobis Distance (Mahalanobis Mesafesi)
MFCC	Mel-Frequency Cepstral Coefficients (Mel-Frekans Kepstral Katsayıları)
MLLR	Maximum Likelihood Linear Regression (Olasılık Doğrusal Regresyon)
MLP	Multi-Layer Perceptron (Çok Katmanlı Perceptron)
MRAN	Minimal Resource Allocation Network (Minimum Kaynak Ayırma Ağı)
mRMR	Minimum Redundancy Maximum Relevance

NIST	National Institute of Standards and Technology (ABD Ulusal Standartlar ve Teknoloji Enstitüsü)
PCA	Principal Component Analysis (Temel Bileşen Analizi)
PP	Press-to-Press (tuşa basımından sonraki basıma geçen süre)
RGB	Red, Green, Blue (Kırmızı, Yeşil, Mavi) renk uzayı
RP	Release-to-Press (tuşun bırakılmasından basılmasına dek geçen süre)
RR	Release-to-Release (tuşun bırakılmasından bir sonraki bırakmaya geçen süre)
SDS	Stochastic Diffusion Search (Stokastik Difüzyon Arama)
SRAN	Self-adaptive Resource Allocation Network (Kendiliğinden Uyarlanabilir Kaynak Ayırma Ağı)
SURF	Speeded Up Robust Features (Hızlandırılmış Gürbüz Öznitelikler)
SVM	Support Vector Machines (Destek Vektör Makineleri)
TNR	True Negative Rate (Doğru Negatif Oranı)
TPR	True Positive Rate (Doğru Pozitif Oranı)
UBM	Universal Background Model (Genel Arkaplan Modeli)
VQ	Vector Quantization (Vektör Nicemleme)
YSA	Yapay Sinir Ağı

ŞEKİL LİSTESİ

	Sayfa
Şekil 1.1 Bir biyometrik doğrulama sisteminin genel mimarisi.	3
Şekil 1.2. Anomali tespitinde profillerin kategorizasyonu [9].	4
Şekil 1.3. Tipik anomali tespit sistem mimarisi [9].	4
Şekil 1.4. Geçerli ve geçersiz kullanıcı olasılık yoğunluk dağılımları örnekleri.	7
Şekil 2.1. Silüetlerin çıkarılması [29].	13
Şekil 2.2. Resim için yön çizgileri eklenmiş 'p' harfinin el hareket resmi[47].	22
Şekil 2.3. 'p' harfinin el hareket görüntüsünün ilgili Yön Histogramı[47].	23
Şekil 2.4. Dudak öznitelikleri çıkarımı[49].	24
Şekil 3.1. Tuşlama öznitelikleri [53].	27
Şekil 3.2. Saat yönünde döndürme jesti[67].	36
Şekil 3.3. Parmakların eşlenmesi [67].	36
Şekil 4.1. İmza ağırlık merkezine dayalı çıkarılan öznitelikler[76].	41
Şekil 4.2. Cevaplama ağı için örnek benzerlik eşlemesi[88].	46

ÇİZELGE LİSTESİ

Sayfa

Tablo 1.1. Literatürde kullanılan makine öğrenme teknikleri.	5
Tablo 2.1. Görüntüye dayalı yürüyüş modellemede öznelik çıkarım yöntemleri ve özellikleri[30].	11

DAVRANIŞSAL BİYOMETRİ: KİMLİK DOĞRULAMA VE ANOMALİ TESPİT UYGULAMALARINDA KULLANILAN YÖNTEMLER

Fatma GÜMÜŞ

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Semineri

Seminer Danışmanı: Prof. Dr. Hasan Hüseyin BALIK

Mevcut biyometrik kullanıcı doğrulama teknikleri iki tür olarak ayrılabilir: fizyolojik ve davranışsal yaklaşımlar. Fizyolojik biyometri, bir kişinin parmak izi, yüz, iris/retina ve el/avuç içi gibi fiziksel özellikleri ile ilişkili iken davranış biyometrisi, bir kişinin ses, yazılı imzalama, yürüyüş, yazım ritmi (tuş vuruş dinamikleri) ve dokunmatik dinamikleri gibi davranış modeliyle ilgilidir.

Bu seminer çalışmasında son beş yılda en yaygın olarak incelenen davranışsal biyometri yöntemlerinin kimlik doğrulama ve anomali tespit uygulamalarında kullanılan öznelilikler ve çalışmaların performansları incelenmiştir. Davranışsal biyometri yöntemleri üç ana başlıkta incelenmiştir: Vücut dinamiklerine dayalı davranışsal biyometri (yürüyüş ve üst vücut dinamikleri, ses ve konuşma, göz hareketleri ve bakış, el mimikleri, dudak hareketleri), bilgisayar çevre bileşenleri ve taşınabilir cihaz etkileşimine dayalı davranışsal biyometri (tuş vuruş dinamikleri, fare etkileşimi, dokunmatik ekran etkileşimi, diğer taşınabilir cihaz etkileşimi), imza ve davranış dinamikleri.

Anahtar Kelimeler: davranışsal biyometri, biyometrik kimlik doğrulama, biyometrik anomali davranış tespiti.

**DAVRANIŞSAL BİYOMETRİ: KİMLİK DOĞRULAMA VE ANOMALİ TESPİT
UYGULAMALARINDA KULLANILAN YÖNTEMLER**

Fatma GÜMÜŞ

Department of Computer Engineering

PhD Seminar

Seminar Adviser: Prof. Dr. Hasan Hüseyin Balık

Biometric user verification techniques can be divided into two types: physiological and behavioral. While physiological biometry is related to the physical characteristics of a person such as fingerprint, face, iris/retina, and hand/palm, behavior biometrics relate to a behavioral pattern such as a person's voice, written signature, gait, keystroke and touch dynamics.

In this seminar study, the features used and the performances of the studies in authentication and anomaly detection applications of behavioral biometry methods are examined. The study's focus is the methods that have been examined most commonly in the past five years. Behavioral biometry methods are investigated in three main categories: behavioral biometry based on body dynamics (gait and upper body dynamics, voice and speech, eye movements and gaze, hand gestures, lip movements), behavioral biometry based on computer components and mobile device interaction (keystroke, mouse interaction, touch interaction, other portable device interaction), signature and behavior dynamics.

Keywords: Behavioral biometrics, biometric authentication, biometric anomaly behavior detection.

GİRİŞ

1.1 Davranışsal Biyometriye Genel Bakış

Bilgisayar ve internet uygulamalarının modern yaşamın vazgeçilmezleri olması ile birlikte bilgi ve sistemlere erişimde yetkili girişlerin yüksek doğrulukta sağlanması ve yetkisiz giriş teşebbüslerinin hassasiyetle yakalanması daha önemli hale gelmiştir. Bununla birlikte, giriş yapılan bir sistemde gerçekleştirilen işlemlerin yada güvenliği kontrol altında tutulmak amaçlanan bir bölgede meydana gelen normal ve anormal durumların tespit edilmesi de gereklilik olmuştur.

Yetkili giriş sorgulamasında girişi yapanın iddia ettiği kişi olduğunun doğrulanmasında kullanılan klasik yöntemler kişinin sahip olduğu bir eşya (genellikle elektronik kart) ve/veya bilgisi dahilinde olan bir anahtar bilgi (şifre, PIN) ile doğrulamayı gerçekleştirir. Ancak kart ve şifrenin çalınması yada sahtesinin üretilmesi önüne geçilmesi zorlu senaryolardır. Kişinin bireyselliğini ayırt edici olarak belirleyen, fiziksel yada davranışsal olarak üzerinde taşıdığı biyometrik veri ise çalınma ve sahtecilik senaryolarına karşı oldukça dirençlidir.

Mevcut biyometrik kullanıcı doğrulama teknikleri iki tür olarak ayrılabilir: fizyolojik ve davranışsal yaklaşımlar. Fizyolojik biyometri, bir kişinin parmak izi, yüz, iris/retina ve el/avuç içi gibi fiziksel özellikleri ile ilişkili iken davranış biyometrisi, bir kişinin ses, yazılı imzalama, yürüyüş, yazım ritmi ve dokunmatik dinamikleri gibi davranış modeliyle ilgilidir[1].

Davranışsal biyometri için güçlü bir argüman, ek donanım gerektirmeden kimlik doğrulamasına yardımcı olabilmesidir. Sonuç olarak, davranışsal kimlik doğrulama

fizyolojik biyometri kullanmaktan daha ucuz olmasını yanında, ek donanım kullanımı içermediği için, kullanıcı tarafında giriş sisteminin kullanımı daha kolaydır.

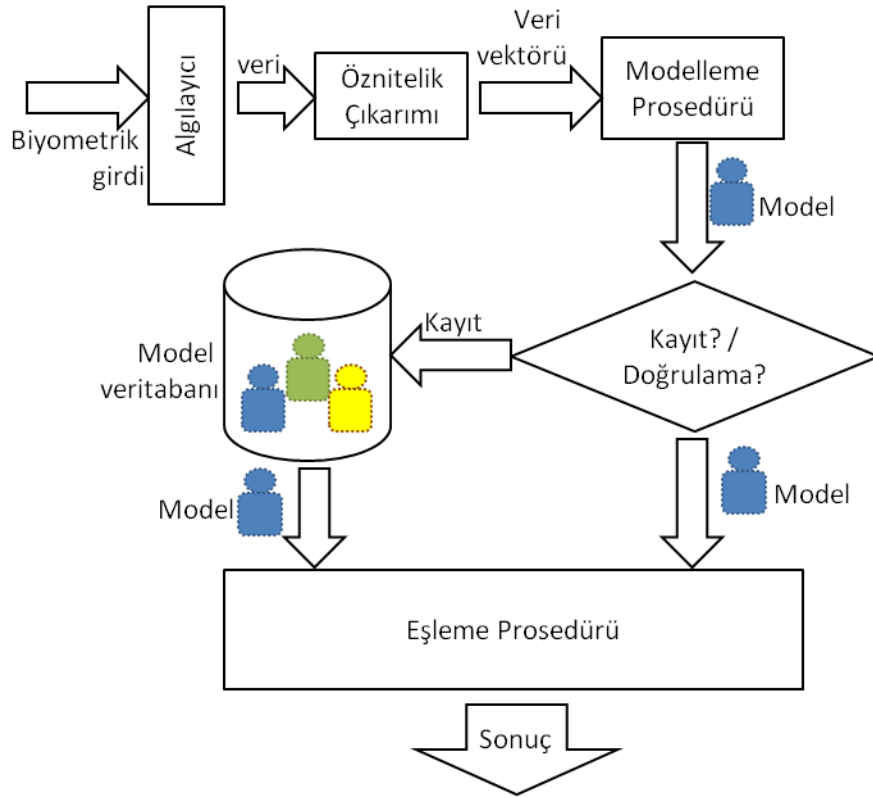
Davranışsal biyometrik özelliklerin kullanıldığı sistemde pasif doğrulama yapmak oldukça elverişlidir. Aktif kimlik doğrulama, bir cihazla uğraşmayı ve bir veya daha fazla geçerli bilgi parçasını girmeyi veya başka türlü bir etkileşim gerektirir. Günümüzde kullanıcılar çok fazla sayıda uygulama veya hizmet kullandığından, her bir uygulama/hizmet için bu tür kimlik doğrulamanın gerekli olması sıkıcı ve sinir bozucu olarak değerlendirilebilir. Bunun bir sonucu olarak kullanıcılar sistem erişiminde daha az güvenli seçenekleri tercih edebilirler. Pasif, yada diğer bir adıyla sürekli doğrulama, sistem arka planında kullanıcıya direkt girdi isteği göndermeden çalışır. Kullanıcı sisteme giriş yaptıktan sonra sistemde tanımlanmış özelliklerin kaydını tutmaya başlar. Yeterli veri toplandığında istatistiksel yöntemler veya makine öğrenimi kullanılarak kullanıcı modeli oluşturulur ve belli süre aralıklarıyla yada belli şartlar gerçekleştiğinde model güncellenebilir. Kullanıcı sistemde işlem yapar haldeyken sürekli veri toplanır ve oluşan davranış modeli kullanıcı modeliyle karşılaştırılır. Anormal davranış tespit edildiğinde sistemde tanımlı güvenlik prosedürü uygulanır.

Fiziksel özelliklerin toplanmasında yüksek kaliteli girdi gerekirken, davranışsal özelliklerde bu hassasiyet şart değildir. Çünkü statik bir ölçümden çok zaman içindeki değişimlerin ifade edilmesi yolu izlenmektedir. Örneğin, güvenlik kameralarından alınan görüntüler, özellikle giriş kontrolü değil gözetim amaçlı kullanılanlar, yüz tanıma ile kimlik doğrulama için yeterli kaliteye sahip değildir. Ancak yürüyüş profilinin çıkarılmasında insan vücudu hareket aksamalarının silüetinin elde edilmesi yeterli olabilmektedir[2].

Tüm bu özelliklerinin yanında bir dezavantaj olarak, birçok davranışsal biyometrik özelliğin fizyolojik özelliklere göre ayırt ediciliğinin daha az olduğu ve başka bir biyometrik özellik yada klasik giriş yöntemi ile birlikte kullanılmasının daha güvenli olduğu literatürde belirtilmiştir[3,4,5].

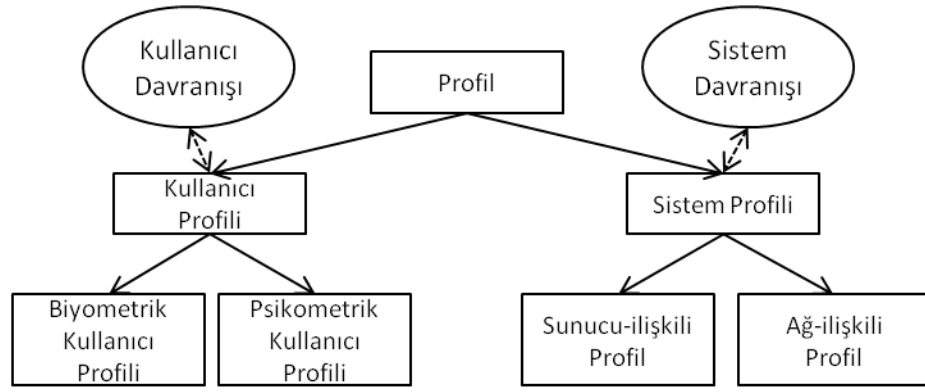
1.2 Biyometrik Kimlik Doğrulama ve Anomali Tespitinin Genel Yapısı

Biyometrik kimlik doğrulama ve anomali tespit uygulamalarının genel mimarisi fizyolojik ve davranışsal biyometri için aynıdır. Kimlik doğrulamada biyometrik özellik girdi olarak alınır, tüm geçerli kullanıcılar için bireysel modeller oluşturulur ve saklanır. Sisteme gelen giriş isteklerinde, istek sahibinden toplanan biyometrik girdi iddia edilen kimliğe ait saklı modellerle karşılaştırılır ve doğrulama sonucu hesaplanır. Sistemde tanımlı eşleme skoru sağlanıyorsa erişim izni verilir, aksi halde erişim engellenir.



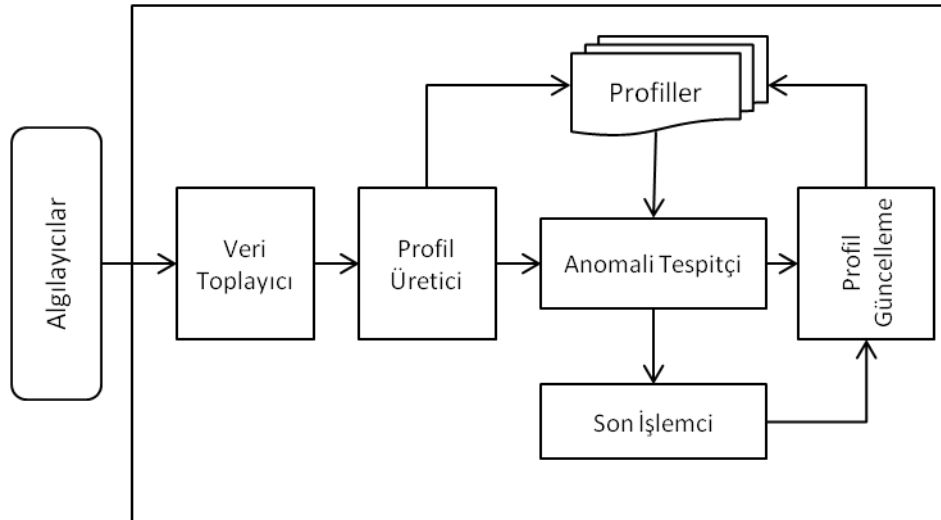
Şekil 1.1 Bir biyometrik doğrulama sisteminin genel mimarisi.

Davranışsal anomali tespit sistemleri sistem ve/veya kullanıcı davranışlarına odaklanmaktadır. Sistem davranışı, cihaz tarafından üretilir, bilgisayar etkinlikleri ve ağ durumuyla ilgilidir. Kullanıcı davranışı, kullanıcının sistemle etkileşimi sırasında üretilmektedir ve bu çalışmada anomali analizinin odağını oluşturmaktadır. Kullanıcı profili biyometrik ve psikometrik olarak incelenebilir[9].



Şekil 1.2. Anomali tespitinde profillerin kategorizasyonu [9].

Anomali tespit sistemleri genel olarak yetkisiz sistem girişlerinin tespiti amacıyla kullanılmaktadır. Sistemde toplanan kullanıcı verisi ile kullanıcının normal davranışının modeli oluşturulur (profil). Profiller statik yada zaman içinde yenilenecek şekilde tasarlanabilir. Aktif bir oturumda kullanıcı aktiviteleri sistemde toplanır, kayıtlı kullanıcı davranışıyla olan benzerliği hesaplanır. Dinamik profil yenilemenin olduğu sistemlerde, anomali analizinde aktif davranışın normal dışı olmadığı sonucuna varılırsa, bu yeni aktiviteler ile kullanıcı profili güncellenir. Normal davranış dışı aktivite olduğu tespit edildiğinde, sistemde tanımlı uyarı mekanizmaları devreye girer.



Şekil 1.3. Tipik anomali tespit sistem mimarisi [9].

Biyometrik tanıma ve anomali tespit sistemlerindeki öncelik, tanıma hatalarını en aza indirmek olduğu için uygun sensör, öznelilik seçim/çıkarım prosedürü ve benzerlik ölçümünün tasarlanması önemlidir. Öznelilikler bireyi yeterince açıklamalı ve diğer bireylerden mümkün olduğunca ayırabilecek niteliğe sahip olmalıdır. Bu nedenle

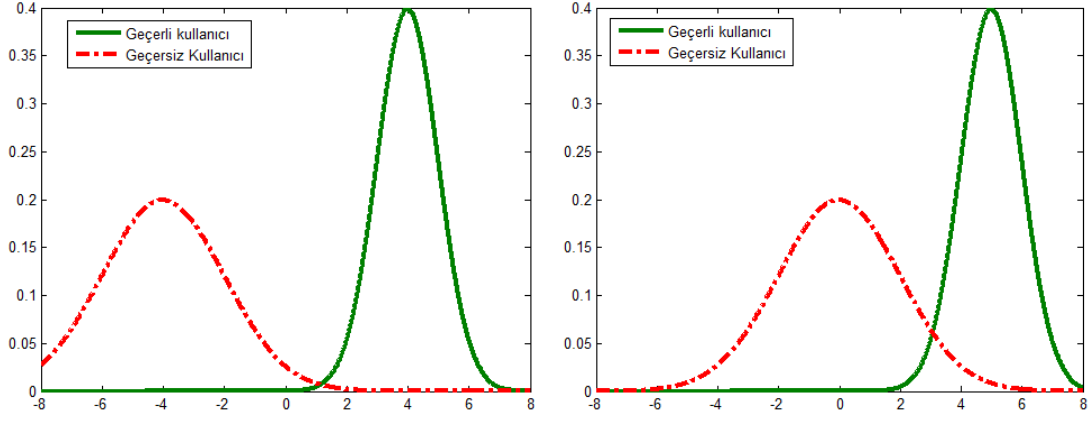
algılayıcıdan toplanan biyometrik veri nicemleştirildikten sonra öznitelik seçimine yada çıkarımına tabi tutulur. Çeşitli biyometrik verinin kaynakları farklı olduğu için özniteliklerinin de farklılık göstereceği açıktır.

Modelleme ve doğrulama prosedüründe istatistiksel yöntemler ve makine öğrenimi yöntemleri kullanılmaktadır. Gözetimli öğrenme yöntemleri kimlik doğrulama için kullanılırken, anomali tespitinde gözetimsiz öğrenme de kullanılabilmektedir. Uzaklık ve benzerlik ölçümlerinin de işlemlerinde kullanıldığı istatistiksel yöntemlerden hem doğrulama hem de anomali tespitinde yararlanılabilmektedir. Aşağıdaki tabloda seminer literatür taramasından elde edilen, öğrenme algoritmaları listesi bulunmaktadır.

Tablo 1.1. Literatürde kullanılan makine öğrenme teknikleri.

GRUP	Teknikler
Sınıflandırma	Destek Vektör Makineleri (Support Vector Machines, SVM)[14], K en yakın komşu (KNN), Karar ağacı(Türevler: J48[15], NBTree[16], C4.5[17]), Naive Bayes[18], Rastgele orman (Random forest)[19].
Yapay Sinir Ağları	Derin Kısıtlanmış Boltzmann Makineleri (Restricted Boltzmann Machines, RBM)[20], BayesNet[21], Perceptron ve Çok Katmanlı Perceptron (Multilayer Perceptron, MLP), Meta Bilişsel Sinir Ağı (Meta Cognitive Neural Network, MCNN)[22], Aşırı Öğrenme Makinesi (Extreme Learning Machine, ELM)[23].
Model Oluşturma	Saklı Markov Modeli (Hidden Markov Model, HMM)[24], Gauss Karışım Modeli (Gaussian Mixture Model, GMM)[25].
Boyut Azaltma / Projeksiyon	Temel Bileşen Analizi (Principal component analysis, PCA)[26], Doğrusal diskriminant analiz (Linear Discriminant Analysis, LDA)[27], Vektör Nicemleme (Vector Quantization, VQ)[28].

Biyometrik sistemlerin değerlendirilmesinde en sık kullanılan iki metrik doğruluk (accuracy) ve Eş Hata Oranıdır (Equal Error Rate, EER) [6]. Doğruluk, geçerli ve geçersiz kullanıcı giriş denemelerinden oluşan bir test kümesinde, geçerli ve geçersiz denemelerin isabetli olarak ayırt edilme sayısının toplam deneme sayısına oranını ifade eder. Giriş denemelerinin hassasiyetle kontrol altında tutulmasını gerektiren biyometrik sistemlerde hatalı kabul (False Positive Rate, FPR) ve hatalı red (False Negative Rate, FNR) oranlarına yüklenen önem uygulama türüne göre değişiklik gösterebilmektedir. Bu oranlar birbirlerine ters orantılıdır, birini azaltmak diğerinin yükselmesiyle sonuçlanır. Bunun nedeni biyometrik sistemlerde eşlemelerin birebir değil, olasılık değerlerine göre yapılmasıdır. Bir giriş denemesinin, iddia edilen kimlik modeline ne kadar çok benzediğini gösteren bir ifadedir. Doğrulamanın olumlu yada olumsuz sonuçlanması, belirlenen bir eşik değerine göre gerçekleştirilir. Pozitif model (yeşil) doğrulanmak istenen kimlik ve negatif model (kırmızı) sistemde saklı sahtekar modelleri olmak üzere aşağıdaki Şekil 1.4'te örnek dağılımlar görülmektedir. Şekilde iki dağılım ele alındığında sağdaki şekli sağlayan sistemin sahtekar girişlerine karşı oldukça dirençli olmasının yanında (düşük FPR), geçerli kullanıcıları da büyük oranda doğru bir şekilde sisteme girişini sağlayabileceği görülmektedir (düşük FNR). Ancak gerçek sistemlerde durum daha çok sol şekildeki gibi olmaktadır. Sahtekar dağılımının bir bölümü geçerli kullanıcı dağılımı alanı ile kesişmektedir. Bu durumda eşik değeri sistemde güvenliğin önemi ve kullanıcıların hatalı olarak reddedilmesinin getirdiği maliyet dikkate alınarak değerlendirme yapılmaktadır. Eşik değeri arttıkça sisteme geçersiz girişler azalacaktır, ancak geçerli kullanıcıların bir bölümü girişte sorun yaşayacaktır (Düşük FPR, yüksek FNR). Eşik değeri düşürüldüğünde geçerli kullanıcılar daha çok sisteme girebilecek ancak sistem sahtekarlara karşı daha korumasız hale gelecektir (Düşük FNR, yüksek FPR). Biyometrik yöntemlerin başarısı değerlendirilirken doğruluktan daha çok bilgi veren, FPR ve FNR değerlerinin birbirine en yakın olduğu değer olan EER daha çok kullanılmaktadır.



Şekil 1.4. Geçerli ve geçersiz kullanıcı olasılık yoğunluk dağılımları örnekleri.

1.3 Seminerin Amacı ve İçeriği

Doktora seminer çalışmasının amacı akademik bir konuda araştırma yapma, bunu raporlama ve yazılı ve sözlü olarak diğer doktora öğrencileri ile paylaşarak akademik alanda yazılı ve sözlü iletişim becerisi geliştirmektir.

Bu çalışmada davranışsal biyometri alanında, kimlik doğrulama ve anomali tespit uygulamalarını konu alan, güncel çalışmaları incelemek ve bunlara ilişkin tez düzeninde rapor oluşturulmuştur. Davranışsal biyometri yöntemleri kategorize edilirken literatürdeki mevcut bölümlendirilmeden yararlanılmış ancak nihai şema son 5 yılda önce çıkan çalışmaların gruplandırılmasıyla oluşturulmuştur.

Bölüm 1.2'de belirtildiği üzere biyometrik doğrulama ve anomali tespit uygulamalarının genel mimarisi benzerlik göstermektedir. Biyometrik yöntemlerde farklılığı oluşturan en önemli nokta öznelitliklerin belirlenmesidir. Bu nedenle, seminer çalışmasının kapsamı son beş yılda önce çıkan davranışsal biyometri yöntemlerinde öznelitlik çıkarımı prosedürlerini tanıtmak ve raporlanan başarılarını bildirmek olarak tanımlanmıştır. Doğrulama aşamasında kullanılan gözetimli öğrenim algoritmaları ve anomali tespitinde kullanılan gözetimsiz tespit algoritmalarını içeren makine öğrenme yöntemleri kapsam dışı olduğu için bunlar hakkında ayrıntılı bilgiye yer verilmemiştir.

Yampolskiy ve Govindaraju[1] davranışsal biyometriyi beş alt grupta incelemektedir. İlk grupta incelenen kaynak tabanlı biyometri, bir kişinin ürettiği bir metin veya bir çizimi incelemeye dayanır. İkinci kategori, insan bilgisayar etkileşimi tabanlı biyometriden

oluşur. Üçüncü kategori, bilgisayar yazılımının gözlemlenebilir düşük seviyeli eylemleri üzerinden kullanıcının davranışını izleyerek elde edilebilen, dolaylı insan bilgisayar etkileşimi tabanlı biyometri kümesidir. Diğer bir kategori, beyin, iskelet, eklemler ve sinir sistemi gibi kullanıcıların motor becerilerine dayandırılmıştır. Son grup ise saf davranışsal biyometri olduğu belirtilmiştir. Bireyin davranışında benzersiz bilgi içeren ancak kalıcı kas hareketleri üzerinde yoğunlaşmayan insan davranışını içerir.

Davranışsal biyometri konusunda son yıllarda yapılan çalışmalar genellikle bu kategorizasyona atıfta bulunmuş olsa da içerik yoğunluğu bakımından mobil teknolojiler ve çevrimiçi kullanıcı davranışı gibi güncel gelişmelere paralel olarak gelişen ihtiyaçlara yönelik olarak özel konulara yoğunlaşmıştır[5,7,8,9,10].

Geçtiğimiz iki yılda davranışsal biyometriyi ele alan inceleme (survey) çalışmalarında da benzer bir trend izlenmektedir. Alzubaidi ve diğ. [11] kullanıcı-akıllı telefon etkileşimine dayalı biyometrik özelliklerin kullanıldığı çalışmaları incelemiştir. Dört tür özellik ayrıntılı olarak incelenmiştir: tuşlama, dokunmatik ekran davranışı, yürüyüş ve el hareket mimikleri. Neves ve diğ. [2] sınırlandırılmamış koşullar ve izleme (surveillance) şartlarında davranışsal biyometri incelemesi, anomali ve eylem tespiti üzerine bir inceleme yapmıştır. Ali ve diğ. [12] Tuş vuruşu dinamik kimlik doğrulaması, kullanılan yöntemler ve algoritmalar, doğruluk oranı ve bu araştırmaların eksikliklerini araştırmıştır. Meng ve diğ. [5] mobil telefonlarda uygulanan 6 davranışsal biyometrik kimlik doğrulama yöntemini (konuşma, imza, yürüyüş, davranış profili, tuşlama, dokunma) içeren bir inceleme yapmıştır.

Jain ve diğ. (2016) biyometrinin akademik çalışmalardaki son 50 yılını değerlendirirken üç ana grup belirlemiştir: Kolluk kuvvetleri ve adli tıp uygulamalarında kullanılan özellikler, çoğunlukla ticari uygulamalarda kullanılan ancak kullanımı sınırlı olan özellikler ve araştırmacılar tarafından incelenmiş ancak yeterli teknolojik olgunluk veya kabul görmemiş özellikler[13]. Parmak izi, yüz, iris, kulak, yürüyüş, el, perioküler ve ses özelliklerine ilişkin akademik çalışmalar incelenmiştir. Fizyolojik ve davranışsal biyometrik özellikleri ele alan kapsamlı bir çalışma olmasına karşın, davranışsal biyometriye ilişkin yalnız ses özellikleri ve yürüyüş dinamiklerine yer vermesi nedeniyle davranışsal biyometri içeriği kısır kalmıştır.

Davranışsal biyometrinin incelendiği bu seminer çalışmasında da son yıllarda öne çıkan konulara geniş yer vermek için yöntemler üç ana bölüme ayrılmıştır: Vücut dinamiklerine Dayalı Davranışsal Biyometri (Bölüm 2), Bilgisayar Çevre Bileşenleri ve Taşınabilir Cihaz Etkileşimine Dayalı Davranışsal Biyometri (Bölüm 3), İmza ve Davranış Dinamikleri (Bölüm 4). Bölüm 5'te yapılan incelemeye ilişkin tartışma ve davranışsal biyometrinin geleceği ile ilgili değerlendirmeye yer verilmiştir.

VÜCUT DİNAMİKLERİNE DAYALI DAVRANIŞSAL BİYOMETRİ

2.1 Yürüyüş ve Üst Vücut Hareketi

Yürüyüş biyometriğinde amaç, insanları yürüme biçimlerinden tanımadır. Yürüme ölçümü dikkat çekmeden, uzaktan görsel izleme yoluyla yapılabileceği gibi taşınabilir sensörden alınan değerlerin analizliyle de gerçekleştirilebilmektedir. Görsel izleme yoluyla alınan yürüyüş biyometrisi düşük çözünürlüklü görüntüden bile çıkarılabilmektedir. Model tabanlı olan ve olmayan şeklinde iki alt grupta incelenebilir[29].

Model tabanlı yaklaşım insan vücudunu temel alır. Görüntüyü insan modeli üzerinde haritalandırır. İyi doğrulama performansı elde edebilmek için bu haritalamanın yüksek isabetle yapılması gerekir. Burada arkaplan görüntüsünün ne kadar iyi ayırt edilebildiği ve kıyafet değişikliklerinin modeli ne kadar etkilediği büyük önem göstermektedir. Vücut hareket aksamalarını işaretleyici araçların kullanılması, özneliliklerin doğru çıkarılması için kullanılan yöntemlerden biridir.

İnsan vücudunu model almayan (bütünsel) yaklaşımlarda ise görüntü içerisinde hareketli cisim tayini yapmak yada silüetler üzerinde enerji hesabı yapılması yöntemleri izlenebilmektedir. Aşağıdaki tabloda model tabanlı ve bütünsel yaklaşımların çıkardığı öznelilikler, ve bunların avantaj/dezavantajları özetlenmektedir.

Tablo 2.1. Görüntüye dayalı yürüyüş modellemede öznitelik çıkarım yöntemleri ve özellikleri[30].

	AVANTAJ	DEZAVANTAJ
MODEL TABANLI YAKLAŞIMLAR		
Statik parametreler	Sabit görünüm, Kompakt gösterim	Kamera kalibrasyonu gerektirir
Elips parametreler	Kompakt gösterim	Düşük gürbüzlük
Kalça açısı	Kompakt gösterim	Düşük gürbüzlük
Şekil parametrelerinin birleşimi	Kompakt gösterim	Düşük gürbüzlük
BÜTÜNSEL YAKLAŞIMLAR		
Kontur	Yapısal farklılıklara karşı hassas	Yüksek karmaşıklık, Düşük gürbüzlük
Genişlik	Yapısal farklılıklara karşı hassas, Düşük karmaşıklık	Düşük gürbüzlük
İzdüşüm	Gürbüz, Düşük karmaşıklık	Kaba yapısal temsil
Açısalılık	Gürbüz	Kaba yapısal temsil
Bağıl aşamalar	Kompakt gösterim, Ölçekten bağımsız	Aşamaların tayin edilmesinin güçlüğü
Silüet	Kayıpsız gösterim	Yüksek karmaşıklık

2.1.1 Model Tabanlı Çalışmalar

Galajdová ve diğ. [31] deneklere uygulanan reflektörler ile vücutta 25 takip noktası belirlemiş ve hareketleri izlemiştir. Kimlik doğrulaması için vücut bölümlerinin açıları ve yörüngelerinden oluşan yürüyüşün kinematik parametreleri değerlendirilmiştir. Bu parametrelerin matematiksel ve istatistiksel analizi yoluyla bireye özgü hareket örüntüsü elde etmek amaçlanmıştır. Reflektörlerin 10'u üst vücutta, 15'i ise vücudun alt bölümüne yerleştirilmiştir.

Ölçümler 10 adımlık yürüme döngüsü için yapılmıştır, her döngü boyunca izlenen aksamaların yatay ekseninde yaptığı açı kaydedilmiştir. 5 kadın ve 5 erkekten oluşan örnek kümesinde, en çok değişim gösteren parametreler sağ dirsek, sağ ve sol bilekler, sağ uyluk, sol ve sağ dizler, sağ ve sol dirsekler ve sağ ve sol ayak bilekleri olmak üzere 10 bölgeden alınan veri olduğu çok kriterli analiz ile belirlenmiştir. Her birey için kimliği tanımlayıcı olan ancak diğer bireyleri ayırt edici olacak öznelilikler ayrıca manuel olarak belirlenmiştir. Çalışmadaki başarı %95.92 olarak raporlanmıştır, ancak verisetinin küçüklüğü göz önüne alındığında, yöntemin genel geçerliliğinin olduğunu söylemek zordur. Ayrıca doğrulamanın manuel olarak yapılmasının hızlı ve güvenilir sistemlerin gereksinim olduğu giriş sistemleri için çok uygun olmadığı söylenebilir.

2.1.2 Bütünsel Yaklaşım Uygulayan Çalışmalar

Kim ve diğ. [29] yürüyüş videosunda insan silüetine dayalı iki yöntemi birleştirerek doğrulama yapmıştır. Deneyler, 20 denekten oluşan CASIA-A [50] veritabanında gerçekleştirilmiştir. Tüm denekler, görüntü düzlemine göre, üç boyutlu olarak, kanonik (0 °), eğik (45 °) ve ön (90 °) görüntülerle, serbest düz bir hat boyunca yürütülmüştür. Veriseti kontrollü koşullarda toplanmıştır, arka plan hepsinde aynı olduğu için yürüyüşü arkaplandan ayırmak için önışlemeye gerek yoktur.

Füzyonda kullanılan ilk yöntemde bir silüet resmi en ve boydan ikiye bölünmek suretiyle dört parçaya ayrılır. Böylece t zamanında H×W boyutuna sahip bir silüet görüntüsü için dört şablon tanımlanmıştır: Sol genişlik vektörü (Eşitlik 2.1), sağ genişlik vektörü (Eşitlik 2.2), yukarı genişlik vektörü (Eşitlik 2.3) ve aşağı genişlik vektörü (Eşitlik 2.4).

$$w_L^y(t) = |x_L^y(t) - W/2|, \quad (2.1)$$

$$w_R^y(t) = |x_R^y(t) - W/2|, \quad (2.2)$$

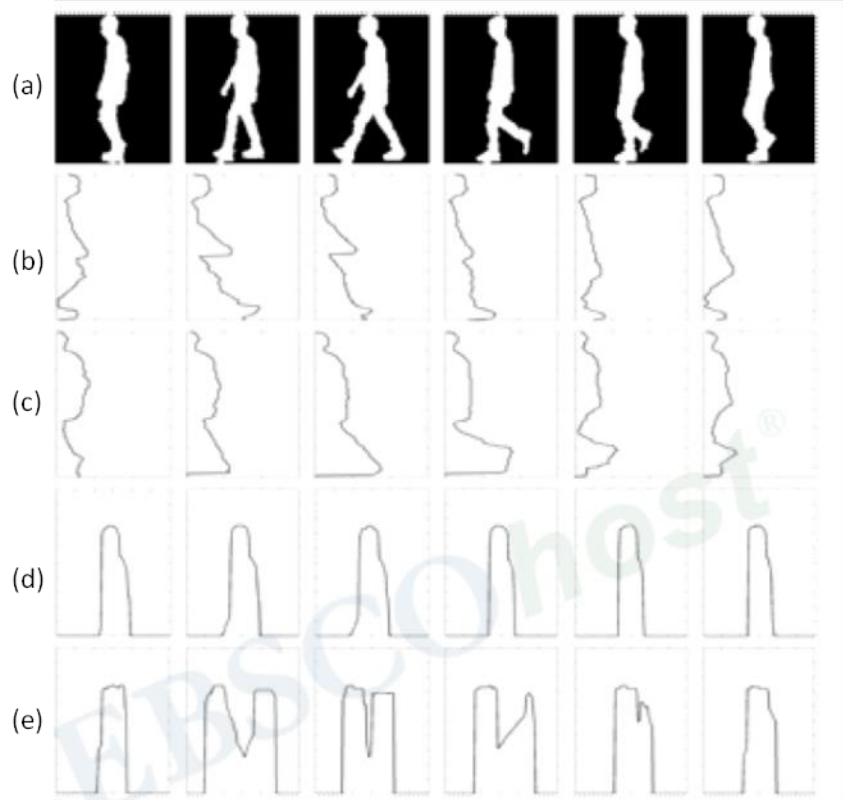
$$w_U^y(t) = |y_U^x(t) - H/2|, \quad (2.3)$$

$$w_D^y(t) = |y_D^x(t) - H/2|, \quad (2.4)$$

$x_L^y(t)$ t zamanındaki belirli bir sıra boyunca en soldaki sınır pikselinin x-koordinat değerlerini, $x_R^y(t)$, y ekseni boyunca en sağdaki sınır pikselini, $y_U^x(t)$, bir sütun x boyunca en üst sınır pikselinin y-koordinat değerlerini, $y_D^x(t)$, t zamanında belirli bir

sütun x boyunca en alttaki sınır pikselinin x-koordinat değerlerini temsil eder. H ve W ise bir silüet görüntüsünün yüksekliği ve genişliğidir.

Füzyona giren ikinci silüet yöntemi dikey izdüşüm vektörüdür. Bir silüet görüntüsünün satırındaki sıfır olmayan piksel sayısı olarak tanımlanmaktadır. Silüet yine 4'e bölünür ve her parça için ayrı ayrı hesaplama yapılır. Aşağıda dikey izdüşümü çıkarılmış 6 karelik bir video parçası örneği verilmiştir.



Şekil 2.1. Silüetlerin çıkarılması. a. Tüm silüet, b. sol silüet, c. sağ silüet, d. tepe silüeti, e. alt vücut silüeti [29].

Füzyonun etkisinin izlenmesi için silüet yöntemleri ayrı ayrı, ardından öznetelik seviyesinde birleştirme ve daha sonra doğrulama sokoru seviyesinde birleştirme yapılarak başarı ölçümü yapılmıştır. Silüet yöntemleri izole olarak değerlendirilirken, modellerin eşlenmesinde L2 norm mesafesi kullanılmıştır. Öznetelik vektörleri birleştirilirken t zamanında hizalama yapılmış, skor seviyesinde ise en yakın model bulunurken çeşitli mesafe ölçümleri kombinasyonlarının performansı izlenmiştir.

Tekil silüet yöntemlerinin sonuçları izlendiğinde genişlik ölçümlerine dayanan yöntemde sağ ve sol genişliğe ilişkin özneteliklerin %81 ve %78 ile en yüksek başarıyı

gösterdiği görülmüştür. Silüet izdüşümü yönteminde ise sağ, sol ve yukarı izdüşüm özniteliklerinde %90 üzeri başarı elde edildiği kaydedilmiştir. Alt bölge izdüşümünün çok iyi sonuç göstermemesinin en muhtemel nedeni kıyafet varyasyonlarının en çok bu bölgeyi etkilemesi olarak görülebilir. Öznitelik seviyesinde füzyonda genişlik vektörleri birleştirildiğinde %83 ve silüet izdüşümünde %95 başarı, skor seviyesinde birleştirmede ise en yüksek %98 başarı elde edilmiştir.

Liang ve diğ. [32], kıyafetin yanıltıcı etkisinin azaltılması için altın oranına dayalı bölütleme yöntemini önermiştir. Farklı kıyafetlerin etkisinin incelenebilmesi için her denek için altısı normal kıyafet, iki çantalı ve 2 kıyafet değişimi senaryosundan oluşan on dizi yürüyüş bilgisi bulunmaktadır.

Yürüyüş Enerji Görüntüsü (Gait Energy Image, GEI) yürüyüş modellemede kullanılan defacto bir yöntemdir[33]. Bütün bir yürüyüş silkesünde ortalama silüeti hesaplar. GEI, vücut bölümlere ayrılarak hesaplanmıştır. Vücut bölümlendirilirken 3 yöntem incelenmiştir: Önceden tanımlı orantıları kullanarak bölümlendirme, eşit oranlı bölümlendirme, altın oranla kıyafet ile görünümü değişen bölümlerin bulunup çıkarılması. Altın oran yöntemi ile CASIA-B [51] verisetinde, farklı kıyafet senaryoları için elde edilen en düşük doğrulama sonucu %91.53 ve en yüksek %99.6 sonucu elde edilmiştir.

Liu ve diğ.[34] izleme (surveillance) ortamında bir kamera yakalanan kişinin modellenip, başka kamerada doğrulanması senaryosu ele almıştır. Hem görünüş profili hem de GEI özellikleri birlikte kullanılmıştır. Görünüş özellikleri için renk bilgisini tanımlamak üzere HSV histogramı, doku bilgileri için Gabor özelliği kullanılmıştır. Skor ve öznitelik seviyesinde füzyon sonuçları değerlendirilmiştir.

Deneyler CASIA verisetinde gerçekleştirilmiştir. Kişilerin kıyafet (ceket, çanta, normal) değişim yapmadığı senaryoda öznitelik seviyesinde füzyon, çantalı örnekler dışında, en iyi performansı göstermiştir. Çantalı örneklerde skor seviyesindeki birleştirmenin daha yüksek doğrulukta tanıma gerçekleştirdiği tespit edilmiştir. Kıyafet değişimlerinin ceketten-normale geçiş ve çantadan-cekete geçiş senaryoları incelendiğinde, her ikisinde de öznitelik seviyesindeki birleşimin en yüksek başarıyı sağladığı görülmüştür.

Sonuçta görünüm ve GEI özniteliklerinin, öznitelik seviyesinde birleştirilmesi ile hem kıyafetin değişmediği durumda hem de çapraz girim koşullarında daha iyi performansa sahip olduğu görülmüştür. Bunun da kişinin bir kamerada yakalanıp modellendikten sonra, diğer kamera görüşüne girdiğinde -kıyafetinde değişim olsa bile- kişinin doğrulanması için uygun bir yöntem olduğunu gösterdiği söylenmiştir.

Bouchrika ve diğ.[35] güvenlik kameraları ile izleme senaryosunu ele almıştır. Senaryoda, izleme koşulları gözetimsizdir; arkaplanda gerçek öğeler bulunmaktadır, kayıtlarda insan dışında hareket eden nesneler de bulunmaktadır. Önerilen yöntem dört ana adımdan oluşmaktadır. Önce noktasal mesafeyi kullanarak yürüyen kişi tespiti yapılmıştır. burada izlenen yöntem silüet çıkarmaya benzemektedir. Videoda art arda gelen çerçevelerin birbirinden çıkarılmasıyla hareket noktaları tespit edilmiştir. Yapılan analizde insan yürüyüşünün oluşturduğu hareket noktalarının örüntülü bir şekilde ilerlediği, taşıt ve diğer objelerin ise daha rastgele hareket noktası kümeleri oluşturduğu görülmüştür.

İkinci aşamada yürüme özelliklerinin işaretsiz olarak çıkartılması gerçekleştirilmiştir. İnsan yürüyüş özelliğinin markörsüz çıkarımı için, hareket modelleri, yürüme türünün farklı evrelerinde diz ve kalça için açısal hareketi tanımlayan tıbbi verilere dayanarak türetilmiştir. Gerçek zamanlı sistemlerde gürbüz ve hızlı performansı nedeniyle yürüme özelliklerinin lokalizasyonu için bir Haar benzeri şablon kullanılmıştır. Sonraki aşamada çıkarılan özelliklerin görüntüleme noktasına göre düzeltilmesi işlemi gerçekleştirilmiştir. Böylece yürüyüş periyodunu ifade eden değerler elde edilmiştir. Son adımda yürüyüş imzası oluşturulmuştur. Bunun için başlangıç noktası sol bacağın topuk vuruşu olarak seçilmiş ve faz bilgisi hizalanmıştır.

Kameraların bakış açısı sabitken yürüyüş doğrulama senaryosunda, CASIA-B [51] verisetinde 6 bakış açısı için inceleme yapılmıştır. KNN ile kimlik doğrulama yapıldığında eklem açılarından elde edilen öznitelikler ile %73.6 başarı elde edilmiştir. Bu sonuç baseline silüet ve GEI yöntemleri sonuçlarına göre düşüktür, ancak kıyafet değişimlerine karşı gürbüz olması nedeniyle gözetimsiz izleme şartlarında daha müsait görülebilmektedir.

2.1.3 Sensör Ölçümleri Kullanan Çalışmalar

Ngo ve diğ. [36], atalet sensörü ile toplanmış yürüyüş biyometrisi verisiyle çalışmıştır. Verisetinde 744 bireyden alınan yürüyüş ölçümleri bulunmaktadır. Oluşturulan verisetinin, literatürdeki örneklerinden farkı örnek sayısının fazla olması, dengeli cinsiyet dağılımına sahip olması, geniş yaş aralığında denekler içermesi, verinin üç atalet sensörü ve taşınabilir telefonda elde edilmiş olması, ve 3 farklı zemin eğim koşulunu değerlendirmiş olması olarak sıralanmıştır.

Yürüyüş periyodunun tespit edilmesinde literatürden dört yöntem seçilmiş ve test edilmiştir: 1) $[-1,1]$ aralığına normalleştirdikten sonra yukarı-aşağı ivmeye dayalı periyotları tespiti, 2) sıfır ortalamaya ayarlandıktan sonra yukarı-aşağı ivmeye dayalı periyotları tespit etme, 3) 3D ivme sinyali genliği kullanılarak periyotların tespiti ve 4) Dinamik Zaman Bükmesi (Dynamic Time Warping, DTW)'ye dayalı faz kayıt tekniği kullanarak periyot saptaması. Veri tabanında her kişi için düz-seviye yürüyüş için ikişer, aşağı ve yukarı eğimli yürüyüşler için ise birer örnek bulunmaktadır. Tüm deneyler, her bir özne için belirlenen eğitim, birinci düz-seviye yürümek sırası olan bir sinyal sekansı içermiştir.

Sonuçlarda iki hususa dikkat çekilmiştir. Birincisi, sensörler, sensör konumları, ayakkabı çeşitliliğini çok fazla olduğu için bu farklılıklardan kaynaklanan etmenlerin etkisinden arındırılmanın zor olduğudur. Burada yaş aralığının genişliğine de dikkat çekilmiştir. Literatürdeki diğer verisetlerinde denekler yetişkindir (20-40 yaş) ancak çalışmanın oluşturduğu verisetinde çocuk ve yaşlılar da bulunmaktadır. Sonuçlar incelendiğinde, yalnız yetişkinler incelendiğinde doğrulama başarısının çok daha yüksek olduğu görülmüştür.

İkinci husus örnek sayısının etkisidir. Sensör ölçümlerinden yararlanan yürüyüş doğrulama sistemleri deneylerinde örnek sayısı çok küçük olduğundan, o sistemlerdeki tek haneli EER değerleri ile bu çalışmanın verisetinin farklı eğim koşullarındaki % 15.8, % 14.3 ve % 14.3 EER sonucunu birbiriyle kıyaslamamanın çok doğru olmadığı belirtilmiştir.

2.2 Ses ve Konuşma

Konuşmacı doğrulama işlemi, diğer biyometrik özelliklerde olduğu gibi önce öznitelik çıkarımı işlemine tabi tutulur, modellenir ve doğrulama yapılır. Otomatik konuşmacı tanıma sistemlerinde bu işlemlerde makine öğrenimi metodolojisinden yararlanılır. Ses sinyali öznitelik çıkarımı işlemine tabi tutulduktan sonra, bu çıktının konuşmacı modelinin oluşturulması ve ardından diğer konuşmacı modellerine olan benzerliğinin hesaplanması, bir otomatik konuşmacı doğrulama sistemindeki makine öğrenmesinin ana sürecini oluşturur. Sistem metine bağımlı yada metinden bağımsız olarak gerçekleştirilebilir. Metine bağımlı sistemde konuşma içeriğinin de eşlenmesi gerekirken, metinsen bağımsız sistemlerde bu kontrol edilmez.

Dijital ses sinyali öznitelik çıkarımında Mel Frekans Katsayıları (MFCC) ve Doğrusal Öngörülü Doğrulama Katsayıları (LPCC) en çok tercih edilen yöntemlerdendir[37]. MFCC, insan işitmesinin bir modellemesidir ve işitme sınırı olan 1000 Hz ile 1 kHz aralığı kabul edilmiştir. Filtreleme ve Fourier transformasyona dayanır. LPCC en güçlü konuşma analiz tekniklerinden biridir ve düşük bit hızda kaliteli konuşma kodlama için en yararlı yöntemlerden biridir. Sesin, periyodik dürtü veya rasgele gürültü ile uyarılan, doğrusal ve zamana göre değişen bir sistemin çıktısı ile modellenebileceği prensibine dayanır. Her iki yöntemde ses sinyalini kısa süreli (genellikle 25 ms) bölütler halinde, takip eden bölütlerin birbiri üzerinde bir miktar (genelde 10 ms) bindirilmiş olarak incelenir.

Metin bağımlı doğrulama sistemlerinde doğrulama aşamasında genel olarak Saklı Markov Modeli (HMM) ve Vektör Nicemleme (VQ) kullanılırken, metinden bağımsız sistemlerde Gauss Karşım Modeli (GMM) kullanılmaktadır.

Metinden bağımsız sistemler için son yıllarda GMM kullanım trendi yerini i-vector'e bırakmıştır. Her konuşma sinyali parçası, konuşmacıya bağlı öz-ses bileşenleri (V) olarak da bilinen alt uzayın bulunduğunu varsaymaktadır. MFCC katsayıları kullanılarak pozitif (kullanıcıdan alınan) ve negatif (farklı konuşmacılardan alınan) örnekler için GMM parametreleri (ortalama ve kovaryans) hesaplanır. Negatif örnekler, genel arkaplan modelini (UBM) oluşturur ve pozitifler ilgili konuşmacının modelini, yani öz-sesini, oluşturmak için girdi alınır[38].

$$M = m_{UBM} + Tx, \quad (2.5)$$

i-vector alt uzayı eşitlikteki gibi modellenir. M , söyleyişe bağlı süper-vektör, m_{UBM} UBM parametrelerinden oluşan süper-vektörü, T sütunları öz-sesleri veren matris (toplam varyasyon matrisi) ve x i-vector'ü ifade eder[38]. i-vector yöntemi ile tüm veri kümesi (pozitif ve negatifler birlikte) aynı i-vector çıkarımı algoritmasından geçirerek modeller. T matrisinin adaptasyonu Beklentiyi Büyütme (Expectation Maximization, EM) algoritması ile yapılarak temel ve alternatif hipotez için konuşmacı modelleri oluşturulur.

Konuşma ve konuşmacı doğrulama yöntemleriyle ilgili inceleme yapan Hansen ve Hasan'ın güncel çalışmasında [39] yöntemler ve değerlendirme kriterleri ayrıntılı olarak anlatılmaktadır.

Konuşmacı tanıma sistemlerinin çoğunda, konuşmacıyla ilgili bilgileri sinyalden ayıklamak için kısa süreli akustik cepstral özelliklerin çıkarıldığı bölüm başında belirtilmiştir. Sarkar ve diğ.[40] uzun süreli akustik özellikler elde edip, kısa süreli özelliklerle karşılaştırmış ve ikisinin birleşiminin performansını incelemiştir. Kısa süreli özellikler fonemleri modeller, uzun süreli özellikler ile hece ve kelimeler modelleyebilmek mümkündür. Çalışmada uzun süreli konuşma özelliklerinin çıkarılması için Çok Katmanlı Perceptron (Multi-layer Perceptron, MLP) kullanılmıştır. MLP'nin mimarisi ortada şişe boynu oluşturacak şekilde tasarlanmıştır, bu nedenle otoencoder ağlarına benzemektedir. Biri olasılık doğrusal regresyona (Maximum Likelihood Linear Regression, MLLR)[52] ve diğeri de i-vektör sistemine dayanan iki konuşmacı tanıma sistemi değerlendirilmiştir.

MLP girdisi, ham dijital ses verisinin 500 ms'lik segmentler halinde Ayrık Cosine Dönüşümü (Discrete Cosine transform, DCT) ile katsayıların elde edilmesi yoluyla elde edilmiştir. MLP dört katmanlıdır, üçüncü katmandaki nöron sayısı, elde edilmek istenen öznitelik sayısı kadardır ve öznitelikler bu katmandan çekilmiştir. Elde edilen öznitelik için konuşmacı adaptasyonu yapılmaz, yalnız Temel Bileşen Analizi (Principal Component Analysis, PCA) veya Doğrusal Diskriminant Analiz (Linear Discriminant Analysis, LDA) ile projeksiyon gerçekleştirilir.

Deneylerde NIST'in 2008 ve 2010 yarışma verisetleri kullanılmış, ve deney sonuçlarında kısa ve uzun süreli özniteliklerin kullanıldığı sistemin yalnız cepstal özellikleri kullanan i-vector'e göre EER ölçümünde yaklaşık %50 azalma izlenmiştir.

Konuşma ve konuşmacı modellemede son yıllarda izlenen diğer bir gelişme derin öğrenmenin uygulanması olmuştur. Liu ve diğ. [41] konuşma sinyalinin öznitelik çıkarmada geleneksel yöntemler ve derin öğrenme yöntemlerinin karşılaştırılması yapılmıştır. Derin yapay sinir ağlarının (DNN) dört tipi incelenmiştir: Derin Kısıtlanmış Boltzmann Makineleri (RBM), konuşma ayırt edici DNN, konuşmacı ayırt edici DNN ve çok görevli ortak öğrenilmiş DNN. DNN'den öznitelikler elde edildikten sonra GMM yada i-vector sistemlerine verilmiş ve başarı ölçümü yapılmıştır.

RBM'ye orijinal cepstal özellikler girdi olarak verilmiş, ağ gözetimsiz olarak eğitilmiştir. Konuşma ayırt edici DNN'de kişileri ayır etme önemli olmadığı için çıkış katmanında fonemler sınıf olarak kullanılmıştır, dolayısıyla eğitim gözetimlidir. Konuşmacı ayırt edici DNN'de de gözetimli öğrenme söz konusudur, çıkış nöronları konuşmacı sınıfları olarak tasarlanmıştır. Çok görevli ortak öğrenilmiş DNN'de hem fonemlerin hem de konuşmacıların ayırt edici özellikleri çıkarılmak hedeflenmiştir. Ağın çıkış katmanında hem fonem, hem de konuşmacı sınıfları bulunur.

Derin öznitelikler elde edildikten sonra PCA ile projeksiyon yapılmış, ardından GMM ve i-vector konuşmacı sınıflandırma prosedürüne verilmiştir. Metinden bağımsız sistemin aksine, metin bağımlı sistemde i-vector sisteminin performansı GMM sisteminden düşüktür. Deneylerde j-vektör olarak adlandırılan çok görevli ortak öğrenilmiş DNN'den elde edilen öznitelik üzerinde en iyi konuşmacı ve konuşma sınıflandırma başarısı (%0.1 EER) gözlemlenmiştir.

Sesli şifre girişinde, konuşma sinyaliyle birlikte dudakların da modellendiği doğrulama sistemi sunulmuştur. Dudakların yerinin tespiti, hareketinin HMM ile modellenmesi üzerinde çalışılmış ve doğrulama bu iki biyometrik özelliğin birlikte kullanılmasıyla oluşan doğrulama sonucu değerlendirilmiştir.

Metin bağımlı ve metinden bağımsız konuşmacı doğrulama yöntemlerinin birlikte kullanıldığı bir çalışma yapan Cai ve diğ. [42] ses perdesi ve MFCC öznitelikleri kullanılmış, Vektör Nicemleme (VQ) ve Mahalanobis mesafesi (MD) ölçümlerinin

performansı incelenmiştir. Deney sonuçlarında MD'nin doğruluk performansının VQ'ya göre üstün olduğu ancak, yöntemlerin çalışma süreleri incelendiğinde VQ'nun daha hızlı hesaplandığı görülmüştür. Yazarlar, bu yöntemlerden birinin seçileceği durumda hız ve doğruluk arasında tercih yapılması gerektiğini vurgulamıştır.

2.3 Göz Hareketleri ve Bakış

Rigas ve diğ. [43] dikkat noktasına dayalı göz hareketi biyometrisi üzerine çalışmıştır. Deneylerde denekler göz hareketleri izlenirken yüz görüntüleri kayıt altına alınmakta ve her katılımcının dikkat noktaları hakkında bilgi toplanmıştır. Deney, 20-30 bir yaş aralığından 15 gönüllü (12 erkek/3 kadın) katılımı ile yürütülmüştür. Dikkat noktalarından oluşturulan graf örüntüsü ile kullanıcılar modellenmiştir. Göz hareketlerinin kaydedilmesi için maliyeti düşük bir göz takip cihazı ve MATLAB'in göz takip araç kutusu kullanılmıştır.

Önerilen yöntemde, göz hareketlerinin pozisyonları, görüntü düzlemindeki x-y koordinatları olarak, her göz yörüngesini temsil eden öznitelik olarak kullanılmıştır. Göz izleme cihazının sağladığı ham göz hareketi kayıtları, gürültülü veya belirsiz numunelerin ortadan kaldırılması gereken bir ön işleme aşamasından geçirilmiştir. Yayılım ağacı (spanning tree) tabanlı yöntemle aykırı noktalar tespit edilmiş ve çıkarılmıştır.

Dikkat noktalarının oluşturduğu örüntüler doğrulama safhasında ele alınırken, örüntüler üstte örtüştürülür ve noktalar arası mesafe ölçülür. Bir test örneği, eğitim kümesinde en düşük uzaklık skoru ile eşleştiği modelin etiketi ile sınıflandırılmıştır. KNN (k=1), KNN (k=3) ve SVM sınıflandırıcılarla elde edilen doğrulama sonuçları incelenmiştir. Deney sonuçlarına göre önerilen yöntem KNN (k=3) sınıflandırıcıyla en yüksek başarı olan %70.2 değerine ulaşmıştır.

Cantoni ve diğ.[44] de benzer bir deney düzeneği üzerinde çalışmıştır; deneklerden yüz resimlerine bakmaları istenmiş ve dikkat noktaları kayıt altına alınmıştır. Yüz resimleri 17 ilgi bölgesine bölünmüş ve bireysel bakış bilgileri için her bölgeye düşen dikkat noktası yoğunluğu (dikkat bulutları) ölçülmüştür. Noktaların koordinatlarının yanında,

bölgedeki yoğunluk ve dikkat süresi de öznitelikler olarak kaydedilmiştir. Koordinat bilgileri kullanılarak göz dikkatinin izlediği yol (arc) belirlenmiştir.

Öznitelikler doğrulama için tek başlarına kullanıldığında, en iyi performansı dikkat süresi özniteliği vermiştir. Öznitelik kombinasyonlarında ise arc ve dikkat süresinin birlikte kullanıldığı düzen en düşük EER sonucunu göstermiştir.

Juhola ve diğ.[45] göz hareketi biyometrisinde medikal bir yaklaşımda bulunmuştur. Düzensiz göz hareketleri kullanılarak, bir doğrulama yöntemi geliştirilmiştir. Göz bir nesneyi takip ederken, istemsiz bir hareket olan odağı doğrultma işlemi yapması özelliğinden yararlanıldığı belirtilmiştir. Elektro-oculography (EOG) ile kaydedilen 19 sağlıklı ve 21 otoneurolojik hastanın düzensiz göz hareketi ve bir video kamera sistemi (VOG) ile kaydedilen 40 sağlıklı ek düzensiz göz hareketi kullanılmıştır.

Doğrulama için genlik, doğruluk, gecikme ve maksimum hız özellikleriyle doğrulama yapılırken, temsil edilen seriler KNN, doğrusal ve kuadratik diskriminant analizi ve naive Bayes sınıflandırması uygulanmıştır. EOG verilerinde en yüksek başarı %90 ile naive Bayes sınıflandırıcıda, VOG'da ise 574 ile ikinci dereceden diskriminant analizinde elde edilmiştir.

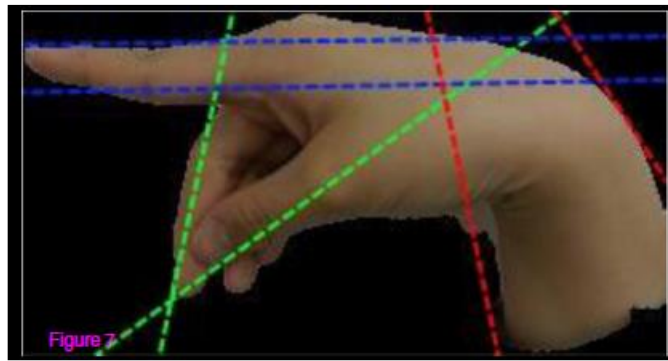
Göz hareketleri ve bakış biyometriği, doğrulamada tek başına yüksek performans göstermese de ancak başka bir biyometrik yöntem e destekleyici olarak kullanıldığında sistem başarısını yükseltecek etkiye sahip olduğu görülmektedir. Kasprowski ve Harezlak[46] bakış ve fare dinamiklerini birleştiren bir doğrulama sistemi önermiştir. Denekleri ekrandaki noktaları fare ile birleştirmeleri söylenmiş, ve deneyler sırasında hem fare hareketleri hem de göz hareketleri kayıt altına alınmıştır. Statik ölçümlere dayalı öznitelikler, histogramdan elde edilen değerler ve DTW ölçümü öznitelikler olarak kullanılmış ve SVM ile sınıflandırma yapılmıştır. Bakış biyometrik verisi kimlik doğrulama için tek başına kullanıldığında %16.79 EER, fare dinamiği ile birlikte kullanıldığında %6.82 EER değeri gözlemlenmiştir.

2.4 El Mimikleri

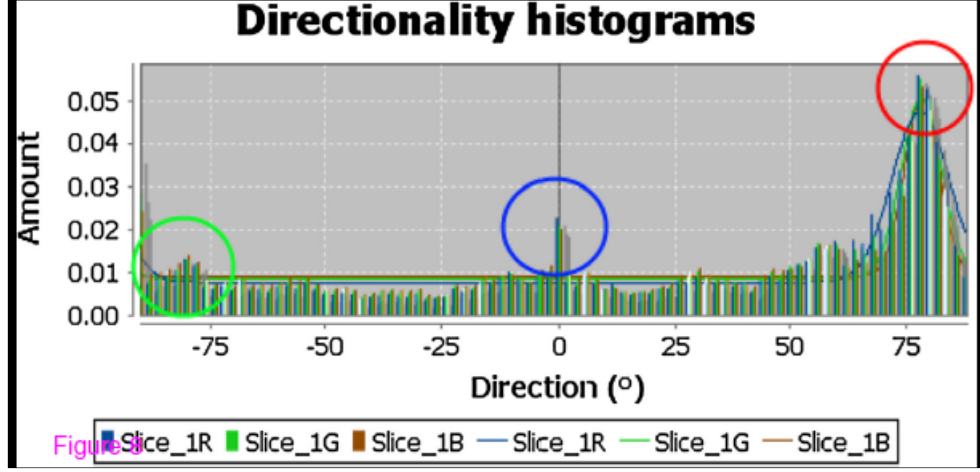
Bu bölümde akıllı telefon etkileşimi ile yakalanan el mimikleri dahil edilmemiş, ilgili özellik Bölüm 3.3'te incelenmiştir. Burada el mimiklerinin bir kamera ile yakalanması senaryosu üzerinde durulmuştur.

Kullanıcının işaret dili el hareketinin ölçümlerine dayanan biyometrik kimlik doğrulama yöntemi geliştiren Fong ve diğ. [47], işaret dili ile şifre girişi yapılmasıdır. Burada el işaretlerinin karşılık geldiği harflerin tespit edilmesinin yanında kimlik doğrulama yapılması da amaçlanmıştır. Çalışmada yoğunluk profili (intensity profiling), renk histogramı ve boyut analizi görüntü işleme algoritmaları kullanılmıştır. El hareket görüntülerinin ön işlemek-sinde için üç adım uygulanmıştır: RGB'den HSV'ye Dönüşüm, Erozyon/Genişletme ve Görüntü Hizalama. Öznitelikler iki farklı görüntü verisi üzerinde uygulanmıştır. Birincisi el görüntüsünün orijinal yoğunluk (intensity) değerleri, diğeri el konturudur. Görüntü haritasının yoğunluğu, el derisinin tonları ve dokusu hakkında zengin bilgi verirken, el konturu, elin anahat şekliyle ilgili bilgi vermiştir.

El konturu çıkarımı Sobel filtresi ile gerçekleştirilmiş, ve yön analizleri Fourier spektrum analizine dayanılarak yapılmıştır. Yön analizi, histogramda bulunan en yüksek zirveye ilişkin istatistikler de üretir. Maksimum zirve, histogramın periyodik doğasını hesaba katarak bir Gauss fonksiyonuyla ilişkilendirilir. Aşağıdaki şekiller de 'p' harfine ilişkin yön belirteçleri ve histogramı görülmektedir.



Şekil 2.2. Resim için yön çizgileri eklenmiş 'p' harfinin el hareket resmi[47].



Şekil 2.3. 'p' harfinin el hareket görüntüsünün ilgili Yön Histogramı[47].

Çıkarılan yön vektörlerinin hisstogramda minimum, medyan ve maksimum noktaları öznitelikler olarak kaydedildikten sonra, korelasyon tabanlı bir öznitelik çıkarım algoritmasıyla zayıf bilgi içeren öznitelikler elenmiştir.

J48, Random Forest, NNge, Perceptron, NBTree, Karar Tablosu, Ortaklık Kuralları, SVM, BayesNet ve Naive Bayes sınıflandırma algoritmaları üzerinde sınanan yöntemde en yüksek kimlik doğrulama performansı %93.75 ile Perceptron'dan elde edilmiştir.

2.5 Dudak Hareketleri

Wang ve diğ. [48] konuşma sırasında dudakların fizyolojik ve davranışsal olarak incelenebilen özniteliklerin ayırt ediciliği üzerine çalışma yapılmıştır. Fizyolojik dudak özellikleri, genellikle statiktir. Zamansal bilgi içermez ve tekil dudak görüntülerinden çıkarılabilirler. Davranışsal dudak özellikleri ise, konuşma sırasındaki dudak hareketine bağlı dudak deformasyonunu ile ilgili zamansal bilgi içeren dinamiktir öznitelikleri belirtir ve bir dudak görüntü dizisinden çıkarılırlar.

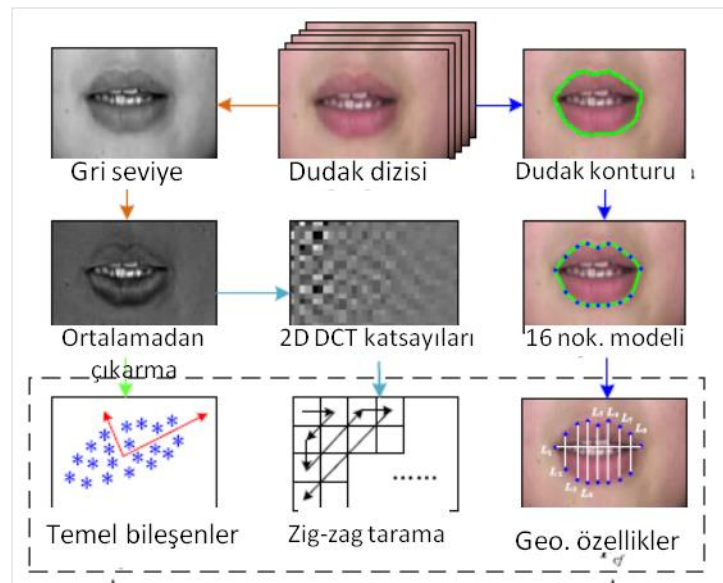
Çalışmada dudağın iki fizyolojik özelliği ile ilgili bilgi çıkarılmıştır. İlki dudak konturudur ve dudağın çerçevesini verir, diğeri de dudak bölgesinin parlaklık yoğunluğu bilgisidir. Çıkarılan davranışsal özelliklerden biri dudak görüntüsünde konuşma sırasında görülen bozulmalardır. Videoda birbirini takip eden çerçeveler üzerinde fark alınmak suretiyle, zaman serisi oluşturulur. Diğer bir davranışsal özellik dudak dokusunda oluşan zamansal değişimdir ve bu da benzer şekilde elde edilir. Dudak görüntüsünde meydana gelen değişimler dudak çevresi bilgisiyle, dokuda meydana gelen değişiklikler ise

parlaklık değeri bilgisiyle ölçülmüştür. Belirlenen bu dört özellik içinde analizler yapılarak herbiri için ayrı öznitelik kümeleri oluşturulmuştur.

Konuşmacıların GMM ile modellendiği doğrulama senaryosunda beş set öznitelik kümesinde test gerçekleştirilmiştir: 4 özelliğin bireysel başarıları, fizyolojik özellikler içinden belirlenen optimal altküme oluşturulan öznitelikler, davranışsal özellikler içinden belirlenen optimal altküme oluşturulan öznitelikler. Fizyolojik öznitelik kümelerinden parlaklık değeri kümesi %0.81 EER ile en iyi performansı gösterirken, davranışsal özelliklerde şekil bilgisi ve optimal altküme deneyleri %0.52 EER ile en iyi doğrulama performansı sergilemiştir.

Liu ve diğ. [49] sesli şifre girişinde, konuşma sinyaliyle birlikte dudakların da modellendiği doğrulama sistemi sunmuştur. Dudakların yerinin tespiti, hareketinin HMM ile modellenmesi üzerinde çalışılmış ve doğrulama ses ve dudak biyometrisinin birlikte kullanılmasıyla oluşan doğrulama deneyleri gerçekleştirilmiştir.

Dudak öznitelikleri olarak konuşma sırasında meydana gelen şekil değişimleri kullanılmıştır. Dudağın alanında meydana gelen değişimler için PCA, dudağı içine alan çerçevedeki değişimlerin ifadesi için DCT dönüşümü ve dudak konturundaki değişim için ise dikey genişlik ölçümleri alınmıştır. Öznitelik çıkarımına ilişkin bir örnek şekilde verilmiştir.



Şekil 2.4. Dudak öznitelikleri çıkarımı[49].

GMM ve HMM yöntemlerinin çeşitli versiyonları ve özniteliklerin farklı kombinasyonları üzerine yapılan deneylerde üç öznitelik türünün de kullanıldığı sistemlerin diğer varyasyonlardan daha yüksek doğruluk gösterdiği belirtilmiştir.

BİLGİSAYAR ÇEVRE BİLEŞENLERİ VE TAŞINABİLİR CİHAZ ETKİLEŞİMİNE DAYALI DAVRANIŞSAL BİYOMETRİ

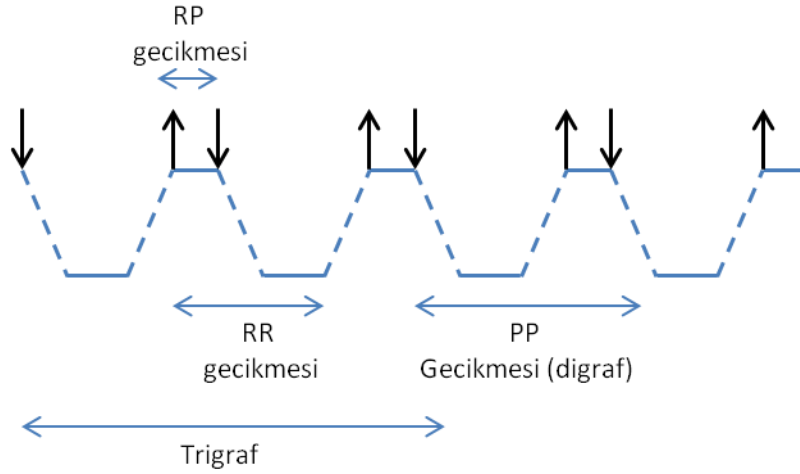
3.1 Tuşlama Dinamikleri

Standart klavye, erişimin sınırlandırıldığı oda girişlerinde bulunan güvenlik tabletleri ve taşınabilir cihazların klavyeleri gibi sistemler kullanılarak kullanıcıların tuşlama davranışları biyometrik ayırt ediciliğe sahiptir. En önemli avantajlardan biri kullanıcıdan pasif olarak toplanabilmesidir. Böylece mevcut güvenlik prosedürlerine ilave bir katman olarak eklenmesinin maliyeti düşüktür.

Genel olarak statik ve dinamik olarak veri toplanabilir[53][11]. Statik veri, belirlenmiş bir dizgenin (örneğin PIN yada alfanumerik şifre) doğruluğunun onaylanmasından sonra giriş sırasında alınan tuşlama davranışının kayıtlı profile ait olup olmadığına bakmayı içerir. Dinamik analiz, tuşlamanın sürekli yada belli aralıklarla izlenmesidir. İki şekilde olabilir. Gözetimli eğitim aşamasının olduğu yapıda, kullanıcıdan sisteme kayıt olurken bir dizgeyi birkaç defa yazması istenerek model oluşturulacak ve toplanan dinamik veri bu model ile karşılaştırılacaktır. Diğer bir yöntemde kullanıcı sisteme giriş yaptıktan sonra tuşlamaları log'lanmaya başlayacak ve öncül bilgi oluştuktan sonra anomaliler belirlenecektir. Tuşlamanın dinamik izlenmesinin gizlilik sorunlarına yol açabileceği göz önünde bulundurulmalıdır[53].

Aşağıdaki şekilde tuşlama biyometrisinde kullanılan gecikmeye ilişkin öznitelikler görülmektedir. Literatür araştırmasında, aynı öznitelikleri kullanan araştırmacıların

bunlara farklı isimler verdiği örneklere rastlanmıştır. Anlaşılabilirliğin artırılması için, araştırma kapsamında incelenen tüm çalışmalardaki öznitelik tanımları buradaki isimlerle belirtilmiştir.



Şekil 3.1. Tuşlama öznitelikleri [53].

Gecikmenin, tuşa basımından sonraki basıma (press-to-press, PP), tuşun bırakılmasın bir sonraki bırakmaya (release-to-release, RR) ve tuşun bırakılmasından basılmasına dek geçen süre (release-to-press, RP) olarak üç ana türü bulunmaktadır. PP gecikmesi "digraf" olarak da sıkça kullanılmaktadır. Trigraf, tuş geçişleri arasındaki zaman aralığıdır. Tuşta bekleme süresi ise, bir tuşun basılı kalma süresini ifade eder[53][12].

Chandrasekar ve Kumar [54] statik şifre tuşlamaları senaryosunda çalışmıştır. Öznitelik olarak PP ve RR gecikmesi kullanılmıştır. Ortalama medyan, standart sapma ve Hausdorff zamanlaması hesaplamaları kullanılarak önışleme yapılmış, sonuçta her örnek için 4 öznitelik üretilmiştir. Hausdorff zamanlaması, iki nokta arasındaki maksimum izometrik mesafe olarak tanımlanmıştır ve mesafe ölçümü olarak Öklid kullanılmıştır[55].

Deneylerde bağışıklı sisteminden esinlenerek modellenen bir Yapay Sinir Ağı (Artificial Immune System, AIS) kullanılmıştır. Giriş katmanını toplanan 4 özniteliğin ortalamalarının beslendiği 4 nöron, 4 nörondan oluşan 1 saklı katman ve çıkış katmanında 1 nöron kullanılmıştır. Sistem, 5 geçerli kullanıcı ve 5 geçersiz kullanıcıyla eğitilmiştir. Tüm geçersiz kullanıcılara geçerli şifreler verilmiştir. Parolanın doğrulanmasından sonra, çıktı (desired output on neuron) ile sabit eşik değeri

karşılaştırılarak tuşlama örüntüsü doğrulanmıştır. Hata değeri 0.001'den düşükse, kullanıcı geçerli kullanıcı olarak kabul edilmiş, aksi halde geçersiz kullanıcı olarak dönüş yapılmıştır. AIS kullanılarak elde edilen sonuçlarda FAR %4.99 olmuştur. Özniteliklerin tanıma başarısındaki öneminin anlaşılması için her öznitelik tek tek doğrulayıcı sistemden geçirilmiştir. Hausdorff zamanlama süresi, %96'nın üzerinde başarıyla bu algoritma için en iyi performansı sağlamıştır.

Chandrasekar ve diğ. [55] diğer bir çalışmada deneylere öznitelik seçim aşaması eklemiştir. Özniteliklerde PP ve RR gecikmesinin yanında RP gecikmesinin ortalama, standart sapma, medyan ve Hausdorff zamanlama değerleri hesaplanmıştır. Stokastik Difüzyon Arama (Stochastic diffusion search, SDS) ve Yerçekimi Arama Optimizasyonu (Gravitational search optimization, GSO) öznitelik alt kümesi seçiminde kullanılmıştır. Kimlik modellerini doğrulamak için, yapay sinir ağı uygulamalarından olan Uyarlanabilir Rezonans Teorisi (Adaptive Resonance Theory, ART) kullanılmıştır. GSO'yu kullanırken Hausdorff zamanlaması, RP ve PP gecikmesi için yanlış sonuç kabul oranı (FAR)% 7.32 ile en iyi sonuca ulaşırken, stokastik difüzyon algoritması, sahte kabul oranı (FAR) %5.16 ile RP ve PP gecikmesi için en iyi sonucu vermiştir.

CAPTCHA imgesi ile gerçek insan doğrulaması sistemi yerine, fare ve tuş vuruş dinamikleri gibi davranışsal biyometri yöntemleri kullanılarak insan ve bot arasında ayırım yapmak için bir algılama yaklaşımı sunan Chu ve diğ. [56] bir tuşun basılıp serbest bırakılması, farenin tıklamaya ve sürükleyip bırakma sürelerinden elde edilen öznitelikler kullanmıştır. Deney, 207 saat insan ve 32 saat bot'dan oluşan 239 saatlik veriyi içermektedir. 1000'den fazla insan kullanıcı ve iki tür blog botu (insan taklit eden ve tekrarıcı) veri üretmiştir. C4.5 karar ağacı algoritması kullanılmıştır. Bot/insan ayırımının 96 aksiyonda %98 TPR ve %99 TNR ile sağlandığı görülmüştür.

Deutschmann ve diğ. [57] tuşlama ve fare dinamikleriyle davranışsal kimlik doğrulamanın sürekli, online olarak yapılmasını ele alınmıştır. Bir güven değeri (Eşitlik 3.1) hesaplanarak tuş girişleri kayıt altına alınmış ve belli aralıklarla kullanıcı modelinde oluşan değişiklikler izlenmiştir. Formülde, C kullanıcının güveni olmak üzere, T tek bir teste dayalı olarak, güvenerek kullanıcıya güvenmeyen arasındaki eşittir. P doğrulama

skorudur (olasılık). Z ise, her sınamada güvenin ne kadar artacağı veya azaltılacağını belirleyen sabittir.

$$C = \begin{cases} 100, \text{ başlangıçta} \\ \text{Max} \left(C - \frac{T-P}{100 \times T/Z}, 0 \right), P < T \\ \text{Min} \left(C + \frac{P-T}{100 \times (1-T)/Z}, 100 \right), P \geq T \end{cases}, \quad (3.1)$$

Veri haftada 20 saat boyunca 99 kişiden 10 hafta boyunca toplanmıştır. bir bulanık ağ ile kullanıcı profilleri oluşturulmuş, ardından profillerin test verisi ile karşılaştırılması için Bayes ağı kullanılmıştır. Deney sonuçlarında tuş vuruş dinamiklerinin, küçük gruplar için kullanıcıların güvenilir sürekli kimlik doğrulamanın mümkün olduğu gözlemlenmiştir. Testlerin hiçbirinde geçerli kullanıcılar yanlışlıkla reddedilmemiş ve 38 etkileşimden sonra geçersiz kullanıcılar tanınmaya başlanmıştır.

Prabha ve Vidhyapriya [22] dokunmatik klavye ile giriş PIN'inin girilmesinde anomali tespiti senaryosu üzerine çalışmıştır. Çalışmada tuşta bekleme süresi, tuşa basılı durma süresi (RP gecikmesi), basınç, yükselen eğim (parmağın temas noktası ve rakama basarken maksimum basıncın bulunduğu nokta arasındaki doğru) ve iniş eğimi (maksimum basınç noktası ile ve parmağın tableten ayrıldığı noktayı birleştiren doğru) gibi beş özellik ele alınmıştır. Her örneği oluşturan 4 rakamlık bir PIN'lerin her rakamı için bu öznelik değerleri kaydedilmiştir. Veri toplama işlemi 50 kullanıcı için yapılmıştır ve her kullanıcının elli örneği kaydedilmiştir.

Normal/anormal sınıflandırmasında mesafeye dayalı yöntemle (Öklid, Manhattan, normalize Manhattan, Pearson korelasyon katsayısı) ve meta bilişsel yapay sinir ağı (meta cognitive neural network, MCNN) performansı karşılaştırılmıştır. %0.2 EER ile MCNN'nin en iyi performansı sergilediği görülmüştür.

Schclar ve diğ. [58] eğitim kümesindeki eleman sayısının azaltılarak modelin fazla örtüşmesinin (overfitting) önüne geçmeyi hedeflemiştir. İlk yöntemde, eğitim kümesi tüm kullanıcılar arasından en genelleyici profillerin eğitim kümesine alınması gerçekleştirilmiştir. İkinci yöntemde ise, kimliği doğrulanmak istenen kullanıcıya en

benzer kullanıcılar belirlenip eğitim kümesine alınmıştır. Üçüncü yöntem rastgele kullanıcı seçimidir.

817 kullanıcıdan aynı şifrenin on kere girilmesi istenmiştir. Öznitelik olarak tuşa bekleme süresi, RP, RP ve RR gecikme süreleri kullanılmıştır. Sınıflandırıcı olarak ise Naive Bayes, en yakın komşu ve Adaboost (C4.5 karar ağaçları ile) algoritmaları kullanılmıştır. Deney sonuçlarına göre, yüksek sayıda kullanıcının olduğu sistemlerde doğrulama yaparken eğitim kümesinin küçültülmesinin performansa olumlu etkisinin olduğu görülmüştür. En iyi doğrulama başarısı Adaboost deneylerinde izlenmiştir. Rastgele seçim yönteminde en iyi başarının 40 kullanıcılık kümede %90.57, benzer kullanıcılar (ikinci yöntem) prosedüründe en iyinin 20 kullanıcıdan oluşan kümede %87.44, genelleyici kullanıcılar (birinci yöntem) prosedüründe ise 50 kullanıcılık kümede %87.33 olduğu belirtilmiştir.

3.2 Fare Etkileşimi Dinamikleri

Fare dinamikleri ile ilgili biyometrik doğrulama çalışmalarında ortak öznitelik prosedürlerine fazla rastlanmamaktadır. Araştırmacılar ilgili olduğunu düşündükleri özellikler üzerinde çalışmışlardır.

Sayed ve diğ. [61] deneylerinde katılımcılara ekran üzerinde örüntüler çizdirmiştir. Çizim alanından toplanan ham veriler, yatay koordinat (x eksen), dikey koordinat (y eksen) ve geçen her pikseldeki milisaniye cinsinden geçen süreyi içermektedir. Deneydeki 39 katılımcıya, her hareketi 30 kez çizdirilerek beş farklı tür hareketin tekrarlanması sağlanmıştır.

Önişleme safhasında gürültü olduğu gözlemlenen veri çıkarılmış, veri merkeze taşınmış ve normalizasyon yapılmıştır. koordinat ve zaman verisinden elde edilen öznitelikler şunlardır: Yatay koordinat , Dikey koordinat , Mutlak zaman, Yatay hız, Dikey hız, Teğet hız, Teğet hızlanma, Teğetsel titreme, piksel cinsinden orijinden izlenen yol, Tanjant eğimi açısı, Eğrilik ve Eğrilik değişim oranı. Yakalanan hareketler bir öğrenme vektör niceleme yapay sinir ağı (learning vector quantization neural network) sınıflandırıcısı kullanılarak analiz edilmiştir.

Deneylerde tek bir hareket uygulandığında FAR % 8.65 ve FRR % 5.17, iki hareket kombine edildiğinde FAR % 8.57 ve FRR 2.29, üç hareket kombine edildiğinde FAR % 6.39 ve FRR % 4.59, dört hareket kombine edildiğinde ise FAR % 5.26, ve FRR =% 4,59 değerleri elde edilmiştir.

Shen ve diğ. [59] fare dinamiklerinde anomali tespiti çalışması yapmıştır. 17.400 örnekten oluşan veriseti oluşturulmuş, öznitelikler çıkarılmış ve 17 farklı anomali tespit algoritmasının performansı değerlendirilmiştir. Hareket yönü, hareket mesafesi ve tıklama tipi verisi toplanmıştır.

Hareket süresi, mesafe, hız ve ivme ayrı ayrı analiz edilmiş ve yeni fare özniteliklerine dönüştürülmüştür. Bu öznitelikler genelde iki gruba ayrılmıştır: bütünsel özellikler ve işlemsel özellikler. Bütünsel özellikler (3 adet), hareket hali ve hareket süresi gibi fare davranışlarının genel özelliklerini tanımlar, işlemsel özellikler (10 adet) ise hız eğrileri gibi fare davranışlarının ayrıntılı dinamik süreçlerini ifade etmektedir. Bir örnekteki her fare hareketi için mesafe ile ilgili özellikler, zamana bağlı özellikler, hızla ilişkili özellikler ve hızlandırmayla ilgili özellikler bulunmuştur. Bu özellikler, her bir fare davranış örneğini karakterize etmek için bir $13 \times 8 = 104$ boyutlu öznitelik vektörü oluşturmuştur.

Fehrer ve diğ. [60] fare hareketi hiyerarşisi (toplam 3 seviye) oluşturmuş, ve öznitelikleri bu hiyerarşiden çıkarmıştır. İlk seviyeyi atomik fare hareketleri (butonlara tıklama ve ana yönlerde hareket etme) oluşturmaktadır. İkinci seviyede fare hareketindeki standart sapma hesaba katılmış ve çift tıklamada tıklamalar arası standart sapma hesaplanmıştır. Üçüncü seviyede ise, farenin hareket edip sol tuşa basılması hesaplanmıştır. Her seviyedeki özniteliklerin hesaplanmasında önceki seviyelerde hesaplanmış öznitelikler kullanılmıştır. Öznitelikler hareket (movement) ve eylem (action) olarak iki sınıfta incelenmiştir. Sınıflandırma Bayesian yaklaşımla gerçekleştirilmiş ve yeni türetilen özniteliklerin doğrulama sonucunu iyileştirdiği belirtilmiştir.

Fare dinamikleri tek başına doğrulama prosedüründe kullanılmak yerine, genel olarak diğer biyometrik yöntemlerle birlikte kullanılır. Bölüm 3.1'de değinildiği üzere Chu ve diğ. [56] tuşlama ve fare dinamiklerini birlikte kullanmıştır. Fare dinamiklerinde

öznitelikler, fare tuşlarının tıklanması arasında geçen süre, işaret edip tıklama ve tıklayıp sürüklenme verilerinden elde edilmiştir. Yine tuşlama ve fare dinamiklerini birleştiren Deutschmann ve diğ. [57] sürekli kimlik doğrulama senaryosunda çalışmıştır. Farenin ekrandaki hareketi monitör çözünürlüğü ile birlikte analiz edilmiştir. FPR'nin tuşlama dinamiklerinden daha fazla olduğu, yetkisiz kullanıcıların ise hızla tespit edilebildiği gözlemlenmiştir. Kasprowski ve Harezlak [46]'ın Bölüm 2.3'te ayrıntılı olarak verilen çalışmasında, fare ve göz hareketi dinamikleri birlikte kullanılmıştır. Tek başlarına yüksek doğrulama performansı sağlamayan yöntemler birlikte kullanıldığında doğrulamanın %6.82 EER ile sağlandığı görülmüştür.

3.3 Dokunmatik Ekran Etkileşimi

Dokunmatik ekranlar özellikle akıllı taşınabilir cihazlarla günlük yaşamın bir parçası haline gelmiştir. Kullanıcıların dokunmatik ekranda kaydırma (swipe), hafifçe dokunma (ThumbStroke) ve çoklu dokunma (multi-touch) davranışlarının ayırt edici kullanıcı modelleri çıkarmak için elverişli olduğu literatür çalışmalarında ortaya koyulmuştur[11]. Veri dokunmatik şifre örüntülerinin girilmesi esnasında yada bir uygulama etkileşimi sırasında toplanabileceği gibi, cihaz etkileşiminin sürdüğü sırada toplanıp kullanıcı davranışlarının anomali tespitinin yapılması gerçekleştirilebilir.

Robertson ve Guest [62], dokunmatik ekranda hem parmak hem ekran kalemi etkileşimini konu almıştır. Deneylere 40 üniversite öğrencisi katılmış ve dokunmatik ekranı parmak (ilk kip) ve kalem (ikinci kip) ile imzalamaları ve sağ-sol yönlerinde kaydırma hareketleri (üçüncü kip) kaydedilmiştir. Çıkarılan 15 öznitelik korelasyon analizi ile incelendiğinde, bazı özniteliklerin her üç kip için de ortak olarak kullanılabileceği sonucu çıkarılmıştır. Bunlar yol uzunluğu (road length, hareketin başlangıç-bitiş mesafesi), ve hareketin başlangıç ve bitişi arasında geçen süredir.

Peng ve diğ. [63] giyilebilir gözlüklerde dokunma ve ses biyometrisi özellikleri kullanılarak, kullanıcıların sürekli doğrulanmasının yapıldığı bir sistem önerilmiştir. Dokunmatik özelliği için çıkarılan öznitelikler süre, mesafe, hız, ve basınç ölçümlerine dayanmaktadır. 32 kullanıcı davranışının oluşturduğu örnek kümesinde, kimlik belirleyici öznitelikler önem sırasına göre sıralanmıştır. Özniteliklerden yalnız küçük bir alt kümesinin her kullanıcının ilk 15 önemli öznitelikleri sırasına girdiği gözlemlenmiştir.

Maksimum basınç tek parmak dokunmatığı için, iki parmak arasındaki mesafe iki parmaklı etkileşim için en önemli öznitelikler olduğu belirlenmiştir. Önemli olduğu belirtilen bir diğer bulgu, ivmeölçer özellikleri ve manyetometre özelliklerinin genellikle jiroskop özelliklerinden daha üst sıralarda yer almış olmasıdır.

7 kip belirlenmiş (tek dokunmalı hareketleri, ileri doğru geçiş jesti, geriye doğru geçiş jesti, aşağı doğru geçiş jesti, iki parmaklı ileri doğru geçiş jesti, iki parmaklı geriye doğru geçiş jesti ve konuşma dinamikleri) ve her biri için ayrı ayrı öznitelik çıkarımı yapılmış ve sınıflandırıcılara verilmiştir. Öznitelik çıkarımı yapılmasının ardından, 7 sınıflandırıcının sonuçları birleştirilmiştir. Tüm sınıflandırıcılar SVM kullanmakta ancak girişte öznitelikler farklılık göstermektedir.

Tüm sınıflandırıcılardan elde edilen olabilirlik sonuçları bir toplama prosedürüne gönderilmiştir. Doğrulamanın online olarak gerçekleştirildiği senaryoda, doğrulama kontrolü yapılan her t anı için tüm kiplerin kullanılmış olmayabileceği de göz önünde bulundurulmalıdır. Toplama prosedürüne düşen olabilirlik sonuçları arasındaki yakınlığın belli bir eşik değerinde olması beklenmektedir. Toplama prosedüründe olabilirlik $Y_i^{c_k}$, c_k kullanıcı sınıflandırıcısının olabilirlik sonucu, n toplama prosedürüne gelen sonuç sayısını, ve H_0 ve H_1 temel hipotez ve alternatif hipotezi göstermek üzere aşağıdaki formül ile hesaplanır:

$$\theta(Y) = \prod_{i=1}^n \frac{P(Y_i^{c_k}|H_0)}{P(Y_i^{c_k}|H_1)} \quad , \quad (3.2)$$

Sistem genel performansı incelendiğinde, dokunma dinamiklerinin bireysel kullanıldığı durumlarda % 90'dan fazla algılama oranı ve % 10'un altında yanlış alarm oranı elde edilmiştir. Yalnızca sesli komutlar kullanıldığında, doğruluk, tek bir dokunmatik hareket türünden daha iyi olduğu görülmüştür. Tüm dokunma tabanlı özellikler birleştirildiği durumda ortalama tespit oranı % 98.7, yanlış alarm oranı % 0.8 olmuştur. Sesli komutlar eklendiğinde ortalama algılama oranı % 99.2'ye yükselmiş ve yanlış alarm oranı % 0.5'e düşmüştür.

Bevan ve Fraser [64] akıllı telefonlarda kaydırma hareketi dinamikleri kullanarak doğrulama yapılması üzerine çalışmıştır. Öznitelik çıkarımı yapılmış, kaydırma hareketinde kullanılan parmağın fiziksel özellikleri ile ilgili çıkarım yapılmıştır.

Kaydırma jestlerini ilişkin şu öznitelikler çıkarılmıştır: Jest uzunluğu, jest tamamlanma süresi, ortalama jest kalınlığı, ortalama uygulanan dokunmatik basınç, ulaşılan maksimum hız, ve ulaşılan maksimum ivme. ANOVA testleri ile parmağın fiziksel özellikleri hakkında çıkarımda bulunmak için özniteliklerin önemi ölçülmüştür. Başparmak uzunluğu ve hızlıca kaydırma hareketlerinin üç özelliği arasında bir ilişki olduğunu gösterilmiştir. Daha uzun başparmaklarına sahip olan kullanıcılar daha kısa başlama zamanı, daha yüksek hız ve daha yüksek ivmelerle kaydırma hareketini tamamlamıştır.

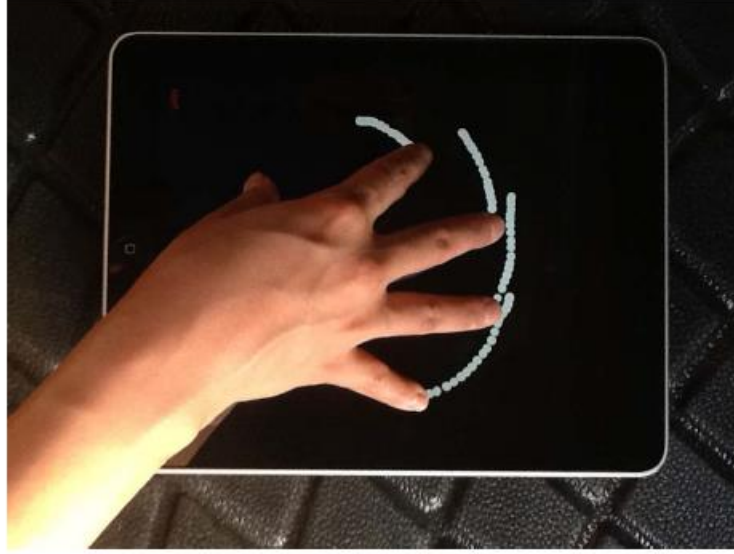
Zhou ve diğ. [65] akıllı telefonlara hem girişte hem de giriş sonrasında ekrana dokunma dinamiklerinin birlikte kullanıldığı bir kimlik doğruma yöntemi önermiştir. Deneylerde araştırmacıların geliştirdiği ThumbStroke adı verilen dokunmatik ekran klavyesi kullanılmış, kullanıcılar kendi şifrelerini oluşturarak sisteme kayıt olmuştur. Doğrulamada şifrenin yanı sıra, tuşlama ve dokunmatik dinamikleri kullanılmıştır. Zamansal, pozisyonel, hareket yönü ve operasyonel olmak üzere 4 öznitelik kümesi elde edilmiştir. Bunlar 7 sınıflandırıcı kombinasyonlarından (karar ağacı, naive Bayes, SVM, ANN, k-en yakın komşu, rastgele orman, AdaBoost) oluşun doğrulama düzeneklerine verilip, performans izlenmiştir. Deneyler büyük ve küçük ekranlarda yapılmıştır. En yüksek başarı ANN ve rastgele ormanlarda sağlanmıştır. Yalnız tuşlama dinamikleri kullanıldığında her iki ekranda başarı ~%40 iken, dokunma ve şifre ile birlikte kullanıldığında başarı %70+ olmuştur.

Kambourakis ve diğ. [66], dokunmatik tuşlara dokunma üzerine çalışma yapmıştır. Klasik tuş vuruş sistemlerinde kullanılan tipik özniteliklerin yanı sıra, hız ve uzaklığın da kullanılması önerilmiştir. Veriseti 20 kişiden alınan veriden oluşmaktadır. İki senaryo incelenmiştir: alfa-nümerik şifre girişinde doğrulama ve yazılı ifadeyi yeniden yazma. Kullanılan klasik tuş vuruş öznitelikleri tuşta bekleme süresi ve RP gecikmesidir (bkz. Bölüm 3.1). Ek olarak kullanılan özniteliklerden uzaklık, dokunmatik klavyede birbiri ardına basılan iki tuşun ekrandaki uzaklığını belirtmektedir. Hız ise, PP gecikmesi ve RP gecikmesinin oranı (PP/RP) olarak hesaplanmıştır. Özniteliklerin kullanılmasında iki metodoloji izlenmiştir: hesaplanan her özneliğin bir vektör olarak kullanılması ve her öznelik için ortalama alınması.

Sınıflandırma için rastgele orman, KNN ve MLP kullanılmış, ancak akıllı telefonun bellek limiti nedeniyle MLP kullanımı iptal edilmiştir. KNN ve rastgele orman algoritmalarının performans karşılaştırması yapılmıştır. Alfa-nümerik şifre doğrulama senaryosunda en iyi başarı, birinci öznitelik metodolojisiyle rastgele orman algoritmasında %26 EER ile sağlanırken; yazılı ifade tekrarlama senaryosunda en iyi başarı ikinci öznitelik metodolojisinde KNN algoritmasında %13.6 EER ile sağlanmıştır.

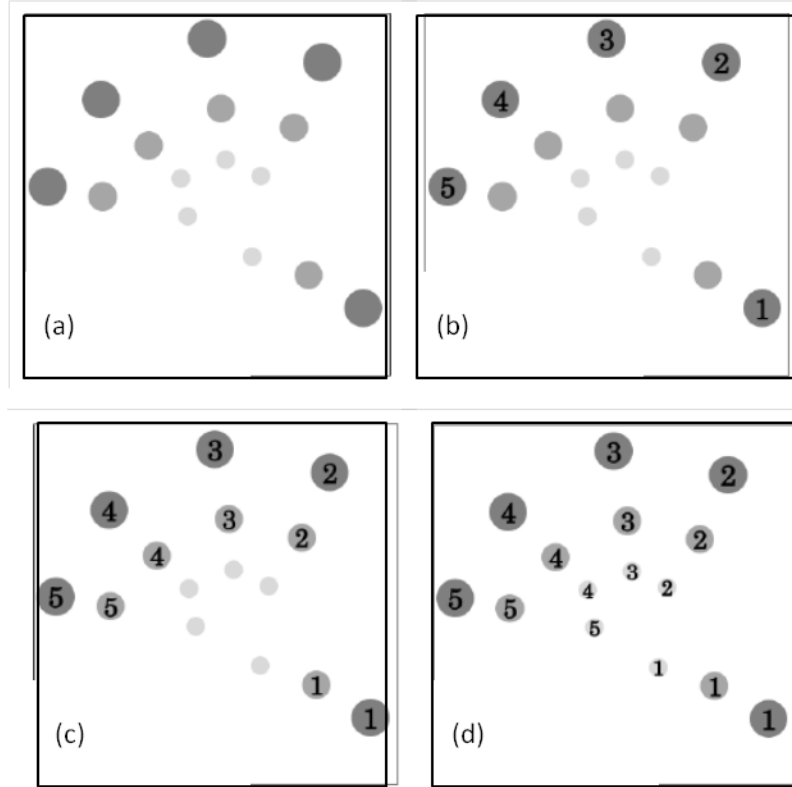
Sae-Bae ve diğ. [67] çoklu dokunuş (multitouch) özelliğine sahip cihazlarda dokunma bilgisini zaman serisi olarak alma, bunu işleyip öznitelik çıkarma, ve sonra modelleme ve test örneğinin doğrulanmasından oluşan prosedür geliştirmiştir.

Çoklu dokunuşta, hareket gerçekleştirilirken yakalanan dokunma noktalarının x-y koordinatlarının bir zaman serisidir. Her örnek birden fazla dokunma noktasını içerir ve her dokunma noktası bir parmak ucuyla oluşturulmaktadır. Ancak, hangi parmak ucunun hangi temas noktasına karşılık geldiği bilinmemektedir. Temas noktaları oluştukları zamana göre sıralanır. Bu yüzden sistemde örnekleri birbiriyle birebir karşılaştırılamamaktadır. Bu nedenle öncelikle parmakların dokunma davranışıyla eşlemesi yapılmıştır. Kullanıcılardan 22 farklı çok parmaklı şifre örüntüsü alınmıştır. Bunlardan bazılarında tüm parmaklar ekran üzerinde yer değiştirirken bazılarında sabit parmaklar bulunmaktadır. Örneğin parmakların öncül tespiti için şekildeki dokunma davranışında (saat yönü döndürme hareketi, CW) tüm parmakların hareket doğrultusu görülmektedir.



Şekil 3.2. Saat yönünde döndürme jesti[67].

Yukarıdaki şekilden elde edilen dokunma izleri ve parmakların eşlenmesi dıştan içe doğru aşamalı olarak aşağıdaki gibi gerçekleştirilmiştir.



Şekil 3.3. Parmakların eşlenmesi [67].

Oluşan zaman serilerinde DTW uzaklığı Manhattan, Öklid ve Cosine fonksiyonlarıyla hesaplanıp, performans karşılaştırması yapılmıştır. 22 hareketin ortalama EER

sonuçlarına göre en iyi performans %7.88 ile Manhattan fonksiyonunda gözlemlenmiştir.

SenthilPrabha ve diğ. [68] kaydırma dinamiklerine bağlı 30 öznitelik çıkarmıştır. 60 kullanıcıdan x ve y koordinatları, basınç, mutlak olay zamanı, cihazın ekran yönü ve kaydırma yönü verisi toplanmıştır. Dokunma hareketi, parmağın ekrana değmesiyle başlar ve ayrılmasıyla son bulur. Bunlardan toplam 30 öznitelik elde edilmiş ve önemli olanların bulunması için karşılıklı bilgi (mutual information) ölçütü kullanılmıştır. Öznitelikler önem sırasına göre listelendiğinde ilk 6 öznitelik: gezilen alan, 20'nci yüzdalik çiftler arası hız (20th percentile pairwise velocity), Basınç, uçtan uca hattın yönü, x eksen başlangıç ve x eksen bitiştir.

Kullanılan sınıflandırıcılar, YSA temellidir. Bunlar meta bilişsel sinir ağı (Meta Cognitive Neural Network, MCNN), aşırı öğrenme makinesi (Extreme Learning Machine, ELM), kendiliğinden uyarlanabilir kaynak ayırma ağı (Self-adaptive Resource Allocation Network, SRAN) ve minimum kaynak ayırma ağı (Minimal Resource Allocation Network, MRAN) 'dir. MCNN sınıflandırıcısı en iyi performansı göstermiştir. 30 öznitelikli MCNN sınıflandırıcısının doğruluğunun yaklaşık % 75 iken en önemli 6 öznitelik kullanıldığında doğruluk yaklaşık % 82 olmuştur.

Frank ve diğ. [7] kullanıcı-dokunmatik ekran etkileşiminde 30 davranışsal biyometri özniteliği çıkarmış ve doğrulama yapmıştır. İlgilenilen senaryo, kullanıcının cihazı kullanması esnasında arkaplanda sürekli kimlik doğrulamadır. Bir dokunma hareketi yörüngesi bir vektörler dizisi olarak aşağıda gösterilmiştir. x_n , y_n pozisyon, t_n zaman vektörü, p_n ekran üzerine uygulanan basınç, A_n parmağın ekranda kapladığı alan, o_n^f parmağın yönü ve o_n^{ph} ekranın dikey yada yatay olmasıdır.

$$s_n = (x_n, y_n, t_n, p_n, A_n, o_n^f, o_n^{ph}), n \in \{1, 2, \dots, N\}, \quad (3.3)$$

Özniteliklerin ilgililikleri ölçülmüş, KNN ve SVM ile sınıflandırma yapıp performansları incelenmiştir. Karşılıklı bilgi ölçümü kullanıldığında özniteliklerde ilk 6 öneme sahip olan özelliklerin SenthilPrabha ve diğ. [20]'nin sonuçlarıyla aynı olduğu görülmüştür. Veri farklı oturumlarda toplanmıştır. Oturum-içi, oturumlar-arası ve bir hafta sonraki oturum ile oluşturulan 3 senaryoda doğrulama yapılmıştır.

Medyan EER, tüm kullanım senaryolarında% 0-% 4 aralığındadır. Medyan oturumlar-
arası hataları % 0 iken, birkaç aykırı örnek % 10 EER olmuştur. Yani oturum içinde
davranış değişmemektedir. Oturumlar arası EER, senaryoya ve sınıflandırıcıya bağlı
olarak% 2-% 3, bir hafta sonrası EER ise % 0-% 4 olmuştur. SVM, KNN yönteminden her
zaman daha düşük bir hata elde etmiştir.

3.4 Taşınabilir Cihaz Etkileşimine Dayalı Diğer Yöntemler

Sitová ve diğ. [69] akıllı telefon kullanıcılarının sürekli doğrulanması için el hareketleri,
yönlendirmesi ve kavramasının (HMOG) kullanıldığı bir yöntem önermiştir. 2 öznitelik
kümesi ve 4 sınıflandırıcı kullanılarak performans karşılaştırılması yapılmıştır.

Öznitelik kümeleri, kavrama direnci ve kavrama istikrarı öznitelikleri olarak ayrılmıştır.
Bu öznitelikler ivmeölçer, jiroskop ve manyetometre ile toplanan veri kullanılarak
hesaplanır. kavrama direnci öznitelikleri, bir el kavramasının direnci dokunma ve
hareket olaylarının ekrana yaptığı başınçla ölçülmüştür. Kavrama istikrarı öznitelikleri,
dokunma olayı tamamlandıktan sonra bir dokunma olayındaki parmak kuvvetinin
neden olduğu dalgalanmaların ne kadar çabuk ortadan kalktığını nicelik olarak belirtir.

HMOG özelliklerinin kimlik doğrulama performansı, dokunmatik ekran dokunma
(dokunma süresi, temas büyüklüğü, hız) ve tuş vuruşu dinamik öznitelikleri (tuşa
bekleme süresi ve PP gecikmesi (bkz. Bölüm 3.1) ile birleştirilmiştir. Öznitelik seçimi
HMOG özelliklerinde Fisher skoru ile, dokunma özniteliklerinde mRMR[70] yöntemi ile
gerçekleştirilmiştir. Ardından PCA ile öznitelik dönüşümü gerçekleştirilmiştir.

Analizlerde manyetometre ile elde edilen HMOG özellikleri, tüm doğrulayıcı ve
koşullarda, ivmeölçer ve jiroskop özelliklerinden daha kötü performans göstermiştir.
Ayrıca, yürüme esnasında dokunma özellikleri ve HMOG özellikleri tuş vuruş
dinamikleri özelliklerinden daha iyi performans göstermiştir. Otururken HMOG daha
kisa örüntüler için tuşlama dinamiklerinden daha iyi performans göstermiştir.

Deneyler dört farklı özellik alt kümesi üzerinde yapılmıştır:

- (1) yalnızca HMOG özellikleri;
- (2) yalnız dokunma öznitelikleri;

(3) 12 oturma ve 8 yürüme senaryosunda yalnız tuşlama öznitelikleri

(4) HMOG ve en iyi performans gösteren 3 dokunma özniteliği.

Oturma senaryosunda HMOG %23.4 EER, HMOG ve 3 dokunma özniteliği %20.1 EER ve dokunma öznitelikleri %25.7 EER gözlemlenmiştir. Buna göre oturma senaryosunda HMOG ve 3 dokunma özniteliğinin daha uygun olduğu söylenebilir. yürüme senaryosunda yine HMOG ve 3 dokunma özniteliği %15.1 EER ile en iyi performansı göstermiştir.

İMZA ve DAVRANIŞ DİNAMİKLERİ

4.1 İmza Dinamikleri

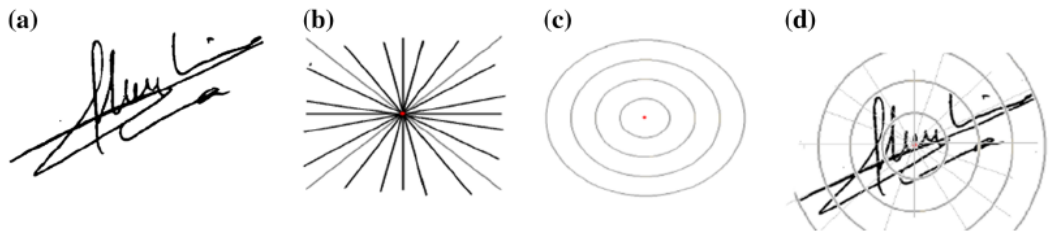
Literatürde imza analizine iki ana yaklaşım vardır: dinamik (çevrimiçi) ve statik (çevrim dışı) imza doğrulama. Dinamik doğrulama, imza sürecinin dinamiklerinin analizine dayanmaktadır. Bunlar dokunmatik cihazlarla etkileşim sürecinden elde edilen hız ve basınç özelliklerini temel almaktadır. Dinamik imza ile ilgili çalışmalar Bölüm 3.3'te verilmiş olup, bu bölümün konusu statik imza doğrulamadır. Statik imza şekil ve oran gibi imzanın geometrik özelliklerini temel almaktadır.

Khan ve Dhole [71], Saikia ve Sarma [72], ve Hafemann ve diğ.[73] çalışmalarında statik imza doğrulama süreçlerini ayrıntılı olarak ele almıştır. Statik imza doğrulama, imza modeli oluşturma ve test örneğinin oluşturulan model ile benzerliğinin tespit edilmesi aşamalarından oluşan tipik bir model tanıma görevi haline gelir. Bu kimlik doğrulama tekniğinde, bir kağıda yazılan imzaların görüntüleri kullanılarak analiz yapılmaktadır. Görüntünün iyileştirilmesi üzere ön işlemler yapıldıktan sonra öznitelik çıkarımı yapılmaktadır. Çıkarılan öznitelikler global, lokal ve geometrik (grid, ızgara) olarak üç temel grupta incelenmektedir. Global öznitelikler imza görüntünün bütünü kullanılarak elde edilirken, lokal öznitelikler görüntünün bir kısmı kullanılarak çıkarılmaktadır. Geometrik özellikler ise döndürme ve ölçekleme gibi görüntü işlemlerine karşı gürbüz öznitelik çıkarma yöntemleri (örneğin SURF[74]) ile elde edilen öznitelikleri ifade etmektedir.

Hafemann ve diğ.[73] statik imza ile kimlik doğrulamada karşılaşılan zorlukları üç madde ile belirtmiştir. Zorluklardan ilki, statik imzanın ayırt ediciliğinin diğer biyometrik özelliklere göre çok daha düşük olmasıdır. Uzman taklitlerin tespit edilmesi çok kolay değildir. ikinci zorluk sistemin eğitim aşaması ile ilgilidir. Statik imza doğrulama çalışmalarının çoğunda yalnız pozitif örnekler ile eğitim yapıp negatiflerin tespit edilmeye çalışılması yine uzman taklitlerin tespitindeki başarıyı düşürmekte olduğu ifade edilmiştir. Sıralanan üçüncü zorluk, sistem eğitiminde kullanıcıdan çok az sayıda örnek alınması nedeniyle oluşturulan modelin yetersiz kalmasıdır.

Shah ve diğ.'nin [75] inceleme çalışmasında 2010-2013 yıllarında statik imza doğrulama üzerine yapılan 15 çalışma incelenmiştir. İlgili çalışmalarda hakim olan doğrulama yöntemlerinin histogram gibi görüntü inceleme yöntemleri, enerji hesaplama ve sinyal dönüşümleri, ve makine öğrenmesi yöntemleri (YSA, SVM, HMM) olduğu görülmüştür.

Neamah ve diğ. [76] ağırlık merkezi (COG, Center of Gravity) ve graf tekniklerine dayalı öznitelik çıkarma yöntemlerini kullanmıştır. Ağırlık merkezi, imza görüntüsünün yatay ve dikey centroid noktaları olarak ifade edilmektedir ve önışlemeden geçirilmiş binary görüntü üzerinden hesaplanır[77]. Hesaplanan ağırlık merkezi referans noktası alınarak şekilde gösterilen açılal aralık ve aralık mesafesi hesaplanmıştır. Her bireyin imzası için benzersiz bir graf oluşturulması öznitelik vektöründeki ilişkilere dayanılarak üretilmiştir. Bu graf yönlü ve ağırlıksızdır. "Yukarı", "aşağı", "sağ" ve "sol" bulanık değişkenleriyle komşuluklar bulunmuş ve graf bu yönler ile oluşturulmuştur. Doğrulama aşamasında HMM kullanılmıştır. Çalışmada kullanılan veriseti ve doğrulama sonuçları hakkında bilgi verilmemiş, yalnız yöntemlerinin sahte imzaların ayırt edilmesinde faydalı olabileceği belirtilmiştir.



Şekil 4.1. İmza ağırlık merkezine dayalı çıkarılan öznitelikler. a. İmza görüntüsü, b. Açılal aralık, c. Aralık mesafesi, d. Öznitelik görüntülerinin imza üzerine oturtulması [76].

Batista ve diğ.'nin [78] çalışmasında az sayıda örnek kullanılarak statik bir imza doğrulama sistemi tasarlanması için, hibrid üretken-ayırt edici (generative-discriminative) sınıflandırıcı toplulukları (EoC, ensembles of classifiers) önerilmiştir. Çalışmada sınıflandırıcıların seçim sürecinin dinamik olarak gerçekleştirilmiştir.

Çalışmanın temel çıkış noktası, devreye alınmış bir doğrulama sisteminde geçerli kullanıcıdan alınacak eğitim örneği sayısının çok az olmasından kaynaklanan sorunun çözülmesi amacıdır. bunun üstesinden gelmek için "üretme" ardından "ayırt etme" işlemi yapılmıştır. Üretme aşamasında birden fazla ayırık HMM farklı durum sayısı ve kod defter (codebook) büyüklüğü ile eğitilmiştir. Bu şekilde bir imza farklı hiper-parametre değerleri ile eğitildiği için o imza için birden fazla model üretilmiştir. Kod defteri için bağımsız negatif örneklerden oluşan bir veriseti kullanılmış, bu örnekleri üreten kişilerin doğrulama sistemine asla kayıtlı olmayacakları belirtilmiştir. Ayırt etme aşamasında her eğitim imzası için HMM olabilirliği hesaplanmaktadır. Bu olabilirlik değerlerinden oluşan vektörler (bir vektörün her elamını farklı hiper-parametreler ile eğitilmiş modellerin olasılıklarını göstermek üzere) Rastgele Altuzay Yöntemi [79] ile iki sınıflı (pozitif ve negatif sınıflar olmak üzere) sınıflandırıcı havuzunda eğitilmiştir. Böylelikle sistemde yalnız tek bir kullanıcı kayıtlı olsa dahi, bağımsız negatif veriseti örnek modelleri ve kullanıcının modeli olabilirliği hesaplanabildiği için, doğrulama gerçekleştirilebileceği belirtilmiştir.

Her bir test örneği için [80] ve [81]'e dayalı dinamik iki sınıflandırıcı seçme algoritmasıyla (OP-ELIMINATE ve OP-UNION) en uygun sınıflandırıcı altkütmesi seçilmiştir. OP-ELIMINATE algoritmasında sınıflandırıcı topluluğu K adet komşu örneğin tamamını doğru sınıflandıran sınıflandırıcılar ile oluşturulurken, OP-UNION algoritmasında bir adet örneği doğru sınıflandıran K en yakın sınıflandırıcı ile oluşturulmuştur. Seçilen sınıflandırıcı altkütmesi ilgili test örneği için sınıflandırıcı topluluğunu (EoC, ensemble of classifiers) oluşturmuştur.

Deneylerde Brezilya statik imza veriseti [82] ve GPDS veriseti [83] kullanılmıştır. Kişi başı örnek sayısının çok fazla ve çok az olduğu iki senaryo gerçekleştirilmiştir. İlk senaryoda her kullanıcı için 20 imza örneği kullanılırken, ikinci senaryoda 4, 8 ve 12'şer imza örnekleri ile deneme yapılmıştır.

Öncelikle sınıflandırıcı hiper-parametreleri belirlenmiştir. Farklı hiper-parametreler ve farklı negatif örnek altkümesiyle eğitilmiş 10 SVM sonucu kullanılmıştır. En düşük hata oranını sağlayan hiper-parametre değerleri tespit edilip, nihai SVM'lerin eğitilmesinde bu değerler kullanılmıştır. Sonuçta, her bir kullanıcı için Rastgele Altuzay Yöntemi ile 100 adet nihai SVM eğitilmiştir. Sisteme bir test örneği ile giriş yapılmak istendiğinde bu 100 SVM'den alınan pozitif/negatif sınıf kararları toplanıp demokrasi usulüyle son karar belirlenmiştir.

Kullanılan verisetlerinde negatif örnekler ya rastgele yada uzman taklitlerden oluşmaktadır. Brezilya verisetinde bunlara ilave olarak "basit taklit" grubu da bulunmaktadır. Deneylerde performans değerlendirmesi yapılırken Her negatif örnek grubu için ayrı ayrı FAR hesaplanıp ortalaması alınmıştır (average error rate, AER). Baseline olarak [82]'deki doğrulama yöntemi kullanılmış, farklı sınıflandırıcı seçme algoritma kombinasyonlarının performansı değerlendirilmiştir. Her iki veriseti ve senaryo için de baseline sınıflandırıcı en kötü performansı sergilemiştir. Birinci senaryoda OP-ELIMINATE yöntemi her iki veriseti için en üstün başarıyı sağlamıştır. İkinci senaryoda az sayıda negatif örnek kullanıldığında OP-UNION yöntemi daha yüksek başarı sağlarken, negatif örnek altkümesi sayısı artırıldıkça OP-ELIMINATE yönteminin başarıda öne geçtiği görülmüştür.

Kumar ve diğ. [84] YSA ve SVM sınıflandırıcıların performansını çevrelenmiş olma (surroundness) öznelilik kümesi için karşılaştırmıştır. Görüntüler üzerinde önileme yapıp binary görüntü haline getirildikten sonra, her siyah piksel için çevrelenme farklı mesafelerde ölçülmüştür. r mesafesinde çevrelenme ölçmek için, ölçülmek istenen pikseli ortalaayan r yarıçaplı dairede bulunan siyah piksel sayısı sayılmıştır. r yarıçapı çember, Chebyshev mesafesi kullanılarak belirlenmiştir. Bu işlem tüm pikseller için yapıldığında, her bir pikselin çevrelenme değeri bulunmuş olur.

Yazarlar $r = 1, 2, \dots, 11$ değerlerinin kullanarak çok sayıda öznelilik değeri elde etmiştir. Daha genel ve temsili özneliliklerin elde edilmesi için dört istatistiksel değer elde edilmiştir: entropi, birinci, ikinci ve üçüncü derece moment. Dolayısıyla, her imza görüntüsünden $11 \times 4 = 44$ öznelilik çıkarılmıştır. Öznelilik seçimi yoluyla öznelilik

sayısı azaltılmıştır. 6 öznitelik seçim algoritmasının performansa etkisi incelenmiştir. Deneyler CEDAR[85] ve GPDS[83] verisetlerinde gerçekleştirilmiştir.

YSA ve SVM hiper-parametrelerinin optimizasyonu için, eğitim verileri üzerinde, gizli çeşitli hiperp-parametre değeri için 10 kat çapraz doğrulama yapılır. Sarıcı (wrapper) öznitelik seçimin en iyi performansı gösterdiği belirtilmiştir. Sınıflandırıcılar karşılaştırıldığında, yüksek öznitelik sayısının olduğu deneylerde YSA, diğerlerinde SVM'in daha iyi performans sergilediği görülmüştür. CEDAR verisetinde elde edilen en yüksek doğruluk oranı %91.67 iken, GPDS verisetinde %86.24 olup, bunlar karşılaştırılan literatür yöntemleri arasında en yüksek değerlerdir.

Guerbai ve diğ.[86] de topluluk öğrenmesinden yararlanmıştır. Tek sınıflı SVM (one-class SVM, OC-SVM) sınıflandırıcı kullanarak statik imza doğrulama gerçekleştirmiştir. OC-SVM eğitimde yalnız pozitif örneklerden oluşan bir veriseti kullanmaktadır. Sisteme giriş yapmaya çalışan bir test örneği için eğitim örnekleriyle benzerliği hesaplanarak kabul yada ret kararı belirlenir. Ancak OC-SVM'in eğitim örnek kümesinin küçük olduğu durumlarda, eğitim kümesi üzerine fazla örtüştüğü ve FNR oranını artırdığı belirtilmiştir. Çalışmada, bunun nedeninin benzerlik hesabında kullanılan katı eşik değeri olduğu ve bunun yumuşatılarak FNR'ın azaltılması önerilmiştir.

Çalışmanın doğrulama sistemi üç aşamadan oluşmaktadır: eğitim kümesine alınacak kullanıcıların seçimi, imza modellerinin oluşturulması ve optimum eşik değerinin seçilmesi. Sisteme kayırlı kullanıcılar arasından rastgele seçimler yapılarak iki kullanıcı altkümesi oluşturulmuştur. İlk alt küme OC-SVM'in parametrelerini ayarlamak için, ikinci altküme ise optimum eşik değerini bulmak için kullanılmıştır. Öznitelikler [87]'teki prosedürle elde edilmiştir. Burada yalnız eğri (curvelet) katsayısının enerji ve standart sapması kullanılmıştır. OC-SVM, örnekleri orijinal uzaydan öznitelik uzayına yansıtmayı sağlar. Bu projeksiyon, karar fonksiyonu $f(x)$ vasıtasıyla bir örneğin orijinden ayrılmasına olanak tanır. $f(x) > 0$ olduğunda, bir model x kabul edilir, aksi halde reddedilir. OC-SVM karar fonksiyonunda 5 mesafe ölçüm yönteminin (Öklid, Manhattan, Chebychev, Korelasyon, Spearman) her biri için deneme yapılmıştır. Deneyler CEDAR[85] ve GPDS[83] verisetlerinde gerçekleştirilmiştir. Eğitim sırasında çeşitli hiper-parametreler için destek vektörlerinin sayısını ve tanıma oranını

maksimum yapan hiper-parametre deęerleri sınıflandırıcıda kullanılmıştır. 5 mesafe ölçümünü kullanan OC-SVM sınıflandırıcılar ikinci veri altkütmesi ile eğitilerek ve sonuçların demokrasi kararı bulunarak optimum eşik deęeri elde edilmiştir. Eşik deęeri için FAR ve FRR deęerlerinin ortalaması kullanılmıştır. Her iki veriseti için de eşik deęerleri sıfıra yakın çıkmıştır. AER deęerlerine bakıldığında CEDAR veriseti için 5 mesafe ölçüm yönteminin kullanıldığı sınıflandırıcı topluluğunun performansının, her bir mesafe ölçüm yönteminin tek tek kullanıldığı sistemlerden daha iyi olduęu gösterilmiştir. Sistemin 4, 8, 12'şer imza ile eğitildięi durumda örnek sayısı arttıkça başarının iyileştięi görölmüştür. GPDS veri kümesinde [84]'ün en iyi başarıyı verdięi ve ardından sırayla [86] ve [78]'in performansının geldięi görölmüştür.

4.2 Davranış Dinamikleri

Dijital davranışsal profillemeye, son yıllarda popülerlik kazanan bir araştırma konusudur ve dijital hizmetler ile etkileşim verisine dayalı doğrulama için kullanılabilir[11].

Sultana ve dię. [88] kişilerin sosyal ağ davranışlarından, sosyal platforma has öznitelikler çıkartılmış ve kullanıcı modelleme yapmıştır.

Twitter'da kullanıcı ile ilgili bilgi üç şekilde edinilebilir: Sosyal profil bilgileri, ağ bilgileri ve etkileşim bilgileri. Sosyal profilden elde edilen bilgi kişisel ve zamansal olarak iki kategoriye ayrılabilir. Kişisel bilgiler biyografi bilgileri iken, zamansal bilgi konum ve profil oluşturma tarihi gibi öğelerden oluşmaktadır. Ağ bilgileri, takip eden ve edilen kullanıcı verisiyle oluşturulan graf'tır. Twitter'da etkileşim bilgileri hashtag, yeniden tivit atma (retweet), tivit cevaplama (reply) ve URL'lerin yanında tivit içerikleri de biyometrik özellik olarak ele alınabileceęi belirtilmiştir. Çalışmada bu dört çeşit etkileşim öznitelikleri kullanılmıştır.

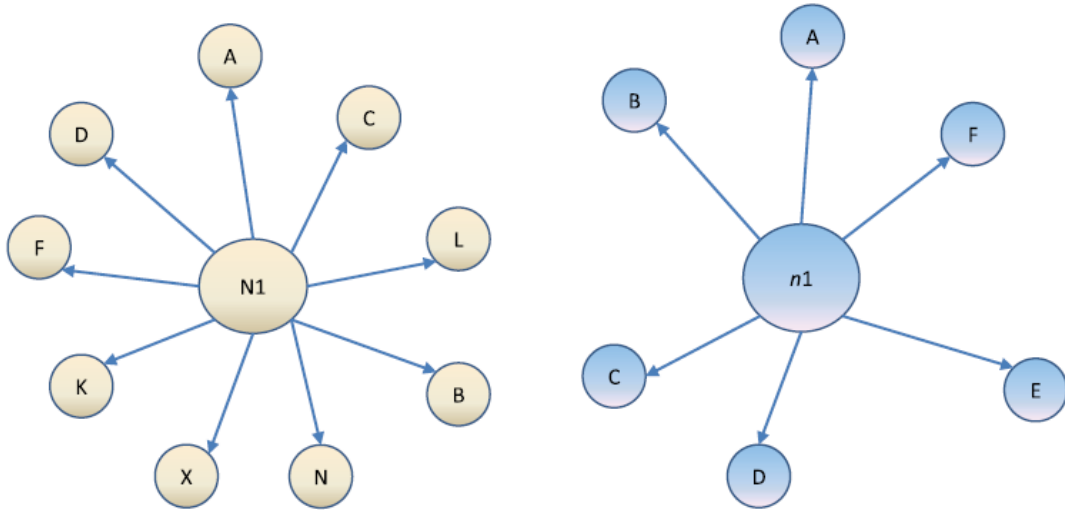
Cevaplama ağı oluşum sürecinde ilgili kişiye ait tüm yanıtların bulunması, bunların sayılması ve bir eşiğin uygulanması bulunmaktadır. Cevaplama ağında kullanıcının sürekli etkileşim kurduęu kişilerin ağı dahil edilmesi amaçlanmıştır. Bir eşik sayısı belirlenmiş ve toplam cevaplar eşikten büyükse cevaplama ağına dahil edilmiştir.

Yeniden tivit atma ağında rastgele davranışların ağı dahil olmaması için karşılıklı davranış ele alınmıştır. Yani bir kullanıcı dięerinin yazdığını yeniden tivit atmış ancak bu

diğer kullanıcı karşıdakinin hiçbir tivit'ini yeniden atmamışsa ağa dahil edilmemiştir. Bu bilgilerden iki ağı ağ oluşturulur. Yeniden tivit atma ve geçerli kullanıcının tivit'inin yeniden atılma ağları.

Bazı hashtag'lar uzun bir süre boyunca bir kullanıcının tweet'lerinde düzenli olarak görünüyorsa, kullanıcının o konuyla ilgili olduğu belirtilmiştir. Belli bir eşiği geçen tüm hashtag'ler hashtag ağına eklenmiştir. Konuların çok hızlı değişebilmesi nedeniyle hashtag ağının sık aralıklarla güncellenmesi gerektiği ifade edilmiştir. URL paylaşımının kullanıcılar arasındaki paylaşma örüntülerini verebileceği belirtilmiştir. Cevaplama ağının oluşturulmasına benzer şekilde oluşturulmuştur.

Şekildeki örnekte n1 ve N1 ağlarının beş eşleşen çifti bulunurken, n1'deki toplam düğüm sayısı 6'dır. Dolayısıyla, n1'in N1'e eşleşme skoru 0.83'tür (5/6).



Şekil 4.2. Cevaplama ağı için örnek benzerlik eşlemesi[88].

Deneyler, 3 aylık izlemeden elde edilen 50 kullanıcıdan oluşan düzenekte gerçekleştirilmiştir. doğrulama aşamasında, tek özellik ve özellik kombinasyonları performansları ölçülmüştür. Doğrulan bir örneğin benzerlik değeri en fazla olan ilk değer doğru model olma olasılığı %20'nin altındadır, ancak ilk 20 değere bakıldığında oran %100'e çıkmıştır. Tüm öznitekler kullanıldığında ilk değerinde doğru tanınma olasılığı %60 üzerine çıkmıştır.

Peng ve diğ. [9] bir sisteme izinsiz girişlerin tespitinde (intrusion detection) sistem ve kullanıcı davranışının modellerinden yararlanıldığı düzenekleri açıklamıştır. Özellikle

kullanıcı davranışının modellenmesi üzerine bir inceleme çalışmasıdır. Kullanıcı davranışı, tuşlama karakteristiği gibi biyometrik özellikler ve metin içeriği gibi psikometrik özellikler ile modellenmektedir. Biyometrik özellikler ile ilgili ayrıntılı bilgi Bölüm 2, 3 ve 4.1'de verilmiştir. Bu bölümün asıl odağını psikometrik özellikler oluşturmaktadır.

Psikometrik kullanıcı profilleri genel olarak kullanıcının özelliklerini içerir. Bu özellikler zekası, bilişsel becerileri, kararları, gereksinimleri ve tercihleri yansıtmaktadır. Psikometrik özellikler diğer davranışsal biyometri özelliklerine göre daha zor modellenirler, sayısallaştırmaları kolay değildir. [9]'da psikometrik özellikleri kullanan 14 çalışma (1994-2013) incelenmiştir. İncelenen çalışmalarda kullanıcı tarafından yazılmış metnin sözdizimsel ve semantik gibi analizlerin yapılmasına olanak sağlar. Oluşturulan profiller, büyük miktarda veriyi işleyerek oluşturulduğu için yüksek maliyetlerle elde edilmektedir. Ancak teknolojinin gelişmesiyle elektronik metinlerin kullanılabilirliği artmakta ve psikometrik profillemeye yazar tespiti, intihal algılaması ve kötü amaçlı yazılım tespiti için kullanıma daha uygun hale gelmektedir.

Davranış tabanlı yaklaşımlar, donanıma daha az bağımlı olarak yeni müdahaleleri algılayabilmesine rağmen, yüksek FPR ana dezavantaj olarak belirtilmektedir. Bunun temel nedeni, davranışın tüm kapsamı eğitim aşamasında elde edilmemiş olması yada meşru davranışların zaman içerisinde değişebilmesi olarak görülmektedir. Bu nedenle sistem, eğitimin periyodik olarak yeniden gerçekleştirilmesine ihtiyaç duyar. Bu şekilde davranış modelleri güncellenebilmektedir. Ancak, burada sisteme bir şekilde giriş yapan saldırganın zaman içinde kullanıcı profilini değiştirebilme riskinin göz önünde bulundurulması gerekmektedir[9].

DEĞERLENDİRME VE DAVRANIŞSAL BİYOMETRİ UYGULAMALARININ GELECEĞİ

Bu çalışmada davranışsal biyometrinin kimlik doğrulama ve anomali tespiti uygulamalarını konu alan son 5 yıla dair literatür analizi yapılmıştır. Analizin büyük kısmını vücut dinamikleri ile ilgili, bilgisayar çevre bileşeni ve taşınabilir cihaz etkileşimi ile ilgili ve imza ve davranış dinamikleri ile ilgili olmak üzere 3 ana başlıkta incelenen yöntemlerin kullandığı öznitelik çıkarım metotları oluşturmaktadır. Analiz sonucunda ses ve yürüyüş biyometrisi gibi yöntemlerin fiziksel biyometriye denk performansı olduğu görülmesine rağmen birçoğunun performansı daha düşüktür. Bunun başlıca nedeni davranışsal biyometrinin zamanla değişen dinamik yapısıdır. Yaş, hastalık ve ortam değişkenlerinden etkilenebilmektedir. Tüm bunlara rağmen düşük kalitede toplanmış verinin bile analizde kullanılabilmesi, kullanıcı verisinin pasif olarak elde edilebilme kolaylığı ve sürekli kimlik doğrulama sistemlerinde yüksek kullanılabilirliği olması nedeniyle, davranışsal biyometrinin kullanımı giderek yaygınlaşmaktadır.

Davranışsal biyometri uygulamalarının geleceği ile ilgili açık problemler aşağıda altı madde ile özetlenmiştir.

1. Veri Güvenliği

Davranışsal biyometri modellerinin tesis ve sistem erişimi, finansal işlemler ve çevrimiçi sosyal ağlar gibi alanlarda daha fazla yararlanılacağı öngörülmektedir [ref. numaraları]. Bu tür uygulamalarda kötü niyetli şahısların izinsiz giriş yapmaları yada geçerli girişleri bloke etmelerinin en kestirme yolu biyometrik veri ile ilgili müdahalede bulunmaktır. Uygulama kullanıcıların mahremiyetinin korunması ve kimlik modeli veri

güvenliğinin sağlanması hakkında öznelik transformasyonu[89], sahtekar girişi önleyici prosedürler[4][90][91] ve diğer biyometrik özelliklerle füzyon[3] gibi yöntemler son yıllarda literatürde incelenmekte ve saha çalışmaları ile ilgili gelişmeler devam etmektedir. Ancak bulut bilişime entegre olan biyometrik sistemlere, işlem gücü hesaba katılarak uygun hale getirilmesi için güvenlik tedbirlerinin yeniden yapılandırılması hâlâ açık bir sorundur[92].

Güvenlikle ilgili diğer bir mesele, üretici (generative) ve çekişmeli öğrenme (adversarial learning) ile ilgili son yıllardaki gelişmelerle ilgilidir. Makine öğrenmesi metodolojisi ile oluşturulan sistemlerin, başka düşman sistemlerin saldırısına maruz kalıp saklı biyometri örüntülerinin bozulması, doğrulama eşiğinden geçebilecek false-positive yapay verinin oluşturulması ile hatalı doğrulamanın gerçekleşmesi gibi tehditlere karşı yapılan çalışmaların az sayıda olduğu görülmektedir.

2. Davranışsal Biyometrik Doğrulama Performansı

Fiziksel biyometrik sistemlerinin kıyaslandığında, davranışsal biyometrik sistemlerin doğruluğunun artırılması gerektiği açıkça görülmektedir[5]. Davranışsal biyometride öznelik çıkarım yöntemleri çeşitlendirmeye açık bir konudur. Daha ayırt edici özneliklerin eklenmesi ve düşük ayırt ediciliğe sahip olanların çıkarılması ile doğrulama performansının artırılması mümkün olduğu söylenebilir.

3. Güvenlik Seviyesi ve Kullanılabilirlik Dengesi Çalışmaları

Biyometrik doğrulamada yanlış kabullerin (false-positive) oranının en aza indirilmesi esas amaçtır. Sistemin doğruluk performansını daha az düşüreceği için yanlış reddetme (false-negative) maliyeti daha düşüktür. Fakat yanlış reddedilmeye maruz kalan bir yetkili kullanıcının uygulama için görüşünü olumsuz etkilemektedir. Uygulama kullanılabilirliği ve yaygınlığını artırmak için yanlış reddedilmeleri düşürücü politikalar sistem güvenliğini azaltacaktır. Bu da dolaylı olarak kullanıcının sistemdeki verisini daha korumasız hale getirecektir. Bu nedenle yanlış giriş / yanlış kabul dengesi ile ilgili kullanılabilirlik ve güvenlik açısından incelemeye adanmış çalışmaların yapılması önemlidir[5].

4. Saha Koşullarına Uygun Çalışmanın Yetersizliği

Deneyisel çalışmalarının büyük çoğunluğunda veri laboratuvar koşullarında toplanıp kaydedilmiştir. Bu koşullar saha şartlarının önemli kısmı göz ardı edilmek üzere düzenlenmiştir. Yeni çalışmalarda gerçek ortamın daha iyi simule edilmesi ve sıklıkla karşılaşılabilecek problemlerin iyi analiz edilip deney ortamına eklenmesi daha gerçekçi sonuçlar elde etmek ve yöntemlerin iyileştirilme çalışması için önemli katkı sağlayabilecektir[12]. Bunun yanında, deneylerin veri toplama cihazlarının (sensör, akıllı telefon gibi) farklı marka ve modelleri ile tekrarlanıp yöntem gürbüzlüğünün kontrol edilmesi de faydalı olabilecektir.

5. Kaynakların Etkin Kullanımı

Biyometrik uygulamaların öncül gereksinimi doğruluk performansının yükseltilmesidir. Sistemlere her an her yerden erişimin bir gereksinim haline geldiği günümüzde, kaynak tüketimi analizi de büyük önem taşımaktadır[5]. İncelenen literatür çalışmaları arasında geliştirilen yöntemlerle ilgili kaynak tüketimi sonuçları bulunsada, üzerinde çalışılan veri ve platform farkından dolayı, çok sağlıklı karşılaştırma yapma imkanı olmamaktadır. Kaynak tüketimi analizinde yalnız çalışma süresi, fiziksel kaynak kullanımı (CPU, bellek, enerji kaynağı vb.) gibi öğelerin yanında yöntem için gerekli öznitelik sayısı ve bunların elde edilme maliyetleri ve eğitim safhasında kullanılan model sayısı gibi kalemlerin de analiz edilmesi yöntem iyileştirilmesi ve geliştirilmesi için yarar sağlayabilecektir.

6. Erişime Açık Verisetinin Oluşturulması

Davranışsal biyometri ile ilgili çalışmalarda açık verisetlerinin yetersizliği yöntemlerin performans karşılaştırılmasının yapılmasının önüne geçebilmektedir. Ayrıca, bazı çalışmalarda kullanılan veri miktarının çok az olduğu görülmektedir. Bunun nedeni özellikle bu türde veri toplamanın özellikle zamansal ve finansal olarak pahalı olmasıdır. Uluslararası çalışmalarda kullanılabilecek, ilgili yasal, gizlilik ve güvenlik protokollerine uyan, veri tabanlarının oluşturulabilmesine olanak tanıyan bir platformun geliştirilmesi bu alandaki çalışmalara büyük katkı sağlayabilecektir.

KAYNAKLAR

-
- [1] Yampolskiy, R. V., ve Govindaraju, V. (2008). "Behavioural biometrics: a survey and classification", *International Journal of Biometrics*, 1(1): 81-113.
- [2] Neves, J., Narducci, F., Barra, S., ve Proença, H., (2016). "Biometric recognition in surveillance scenarios: a survey", *Artificial Intelligence Review*, 46(4): 515-541.
- [3] Gofman, M. I., ve Mitra, S., (2016). "Multimodal biometrics for enhanced mobile device security", *Communications of the ACM*, 59(4): 58-65.
- [4] Šeděnka, J., Govindarajan, S., Gasti, P., ve Balagani, K. S., (2015). "Secure outsourced biometric authentication with performance evaluation on smartphones", *IEEE Transactions on Information Forensics and Security*, 10(2): 384-396.
- [5] Meng, W., Wong, D. S., Furnell, S., ve Zhou, J., (2015). "Surveying the development of biometric user authentication on mobile phones", *IEEE Communications Surveys & Tutorials*, 17(3): 1268-1293.
- [6] Precise Biometrics, Understanding Biometric Performance Evaluation, Teknik Rapor, <https://precisebiometrics.com/wp-content/uploads/2014/11/White-Paper-Understanding-Biometric-Performance-Evaluation.pdf>, Son Erişim: Nisan 2017.
- [7] Frank, M., Biedert, R., Ma, E., Martinovic, I., & Song, D. (2013). "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication", *IEEE transactions on information forensics and security*, 8(1): 136-148.
- [8] Sultana, M., Paul, P. P., ve Gavrilova, M. (2014, October). "A concept of social behavioral biometrics: motivation, current developments, and future trends", In *Cyberworlds (CW), 2014 International Conference on* (pp. 271-278). IEEE.

- [9] Peng, J., Choo, K. K. R., ve Ashman, H. (2016). "User profiling in intrusion detection: A review", *Journal of Network and Computer Applications*, 72: 14-27.
- [10] Murmuria, R., Stavrou, A., Barbará, D., & Fleck, D. (2015, November). "Continuous authentication on mobile devices using power consumption, touch gestures and physical movement of users", In *International Workshop on Recent Advances in Intrusion Detection* (pp. 405-424). Springer International Publishing.
- [11] Alzubaidi, A., ve Kalita, J., (2016). "Authentication of smartphone users using behavioral biometrics", *IEEE Communications Surveys & Tutorials*, 18(3): 1998-2026.
- [12] Ali, M. L., Monaco, J. V., Tappert, C. C., ve Qiu, M., (2016). "Keystroke biometric systems for user authentication", *Journal of Signal Processing Systems*, 86(2): 1-16.
- [13] Jain, A. K., Nandakumar, K., ve Ross, A., (2016). "50 years of biometric research: Accomplishments, challenges, and opportunities", *Pattern Recognition Letters*, 79: 80-10.
- [14] Hearst, M. A., Dumais, S. T., Osuna, E., Platt, J., ve Scholkopf, B., (1998). "Support vector machines", *IEEE Intelligent Systems and their Applications*, 13(4): 18-28.
- [15] Bhargava, N., Sharma, G., Bhargava, R., ve Mathuria, M., (2013). "Decision tree analysis on j48 algorithm for data mining", *Proceedings of International Journal of Advanced Research in Computer Science and Software Engineering*, 3(6).
- [16] Kohavi, R., (1996). "Scaling Up the Accuracy of Naive-Bayes Classifiers: A Decision-Tree Hybrid", In *KDD*, (96):202-207.
- [17] Chawla, N. V., (2003). "C4.5 and imbalanced data sets: investigating the effect of sampling method, probabilistic estimate, and decision tree structure", In *Proceedings of the ICML* (Vol. 3).
- [18] Rish, I., (2001). "An empirical study of the naive Bayes classifier", *IJCAI 2001 workshop on empirical methods in artificial intelligence*, 3, (22): 41-46, New York.
- [19] Liaw, A., ve Wiener, M., (2002). "Classification and regression by randomForest", *R news*, 2(3). 18-22.

- [20] Salakhutdinov, R., ve Hinton, G., (2009). "Deep boltzmann machines", *Artificial Intelligence and Statistics*, 448-455.
- [21] Friedman, N., Geiger, D., ve Goldszmidt, M., (1997). "Bayesian network classifiers", *Machine Learning*, 29(2-3): 131-163.
- [22] Prabha, R. S., ve Vidhyapriya, R., (2017). "Intruder Detection System Based on Behavioral Biometric Security", *Journal Of Scientific & Industrial Research*, 76: 90-94.
- [23] Huang, G. B., Zhu, Q. Y., ve Siew, C. K., (2006). "Extreme learning machine: theory and applications", *Neurocomputing*, 70(1): 489-501.
- [24] Rabiner, L. R., (1989). "A tutorial on hidden Markov models and selected applications in speech recognition", *Proceedings of the IEEE*, 77(2): 257-286.
- [25] Reynolds, D. A., Quatieri, T. F., & Dunn, R. B., (2000). "Speaker verification using adapted Gaussian mixture models", *Digital signal processing*, 10(1-3): 19-41.
- [26] Abdi, H., ve Williams, L. J., (2010). "Principal component analysis", *Wiley interdisciplinary reviews: computational statistics*, 2(4): 433-459.
- [27] Welling, M., (2005). "Fisher linear discriminant analysis", *Department of Computer Science, University of Toronto*, (3): 1-4.
- [28] Makhoul, J., Roucos, S., ve Gish, H., (1985). "Vector quantization in speech coding", *Proceedings of the IEEE*, 73(11): 1551-1588.
- [29] Kim, E., Hong, S., ve Lee, H. (2012). "Human Identification By Fusion Of Multiple Gait Representations", *Advanced Topics in Biometrics*, 229.
- [30] Boulgouris, N. V., Hatzinakos, D., ve Plataniotis, K. N. (2005). "Gait recognition: a challenging signal processing technology for biometric identification", *IEEE Signal Processing Magazine*, 22(6): 78-90.
- [31] Galajdová, A., Šimšík, D., ve Rákay, R., (2016). "An automated procedure for identification of a person using gait analysis", *International Journal of Advanced Robotic Systems*, 13(5): 1-5.
- [32] Liang, Y., Li, C. T., Guan, Y., ve Hu, Y., (2016). "Gait recognition based on the golden ratio", *EURASIP Journal on Image and Video Processing*, 2016(1): 22.

- [33] Man, J., ve Bhanu, B. (2006). "Individual recognition using gait energy image", IEEE transactions on pattern analysis and machine intelligence, 28(2): 316-322.
- [34] Liu, Z., Zhang, Z., Wu, Q., ve Wang, Y., (2015). "Enhancing person re-identification by integrating gait biometric", Neurocomputing, 168: 1144-1156.
- [35] Bouchrika, I., Carter, J. N., ve Nixon, M. S., (2016). "Towards automated visual surveillance using gait for identity recognition and tracking across multiple non-intersecting cameras", Multimedia Tools and Applications, 75(2): 1201-1221.
- [36] Ngo, T. T., Makihara, Y., Nagahara, H., Mukaigawa, Y., ve Yagi, Y., (2014). "The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication", Pattern Recognition, 47(1): 228-237.
- [37] Bimbot, F., Bonastre, J. F., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., ... & Reynolds, D. A. (2004), "A tutorial on text-independent speaker verification. EURASIP journal on applied signal processing", 2004, 430-451.
- [38] Kanagasundaram, A., Vogt, R., Dean, D. B., Sridharan, S., & Mason, M. W. (2011, August). "I-vector based speaker recognition on short utterances", Proceedings of the 12th Annual Conference of the International Speech Communication Association (pp. 2341-2344). International Speech Communication Association (ISCA).
- [39] Hansen, J. H., ve Hasan, T., (2015). "Speaker recognition by machines and humans: A tutorial review", IEEE Signal processing magazine, 32(6): 74-99.
- [40] Sarkar, A. K., Do, C. T., Le, V. B., ve Barras, C., (2014). "Combination of cepstral and phonetically discriminative features for speaker verification", IEEE Signal Processing Letters, 21(9): 1040-1044.
- [41] Liu, Y., Qian, Y., Chen, N., Fu, T., Zhang, Y., ve Yu, K., (2015). "Deep feature for text-dependent speaker verification", Speech Communication, 73: 1-13.
- [42] Cai, Y., Li, X., Gong, Z., ve Codina, T. R., (2014). "Speaker verification for multi-task interactions", Interacting with Computers, 26(2): 135-144.

- [43] Rigas, I., Economou, G., ve Fotopoulos, S., (2012). "Biometric identification based on the eye movements and graph matching techniques", *Pattern Recognition Letters*, 33(6): 786-792.
- [44] Cantoni, V., Galdi, C., Nappi, M., Porta, M., ve Riccio, D., (2015). "GANT: Gaze analysis technique for human identification", *Pattern Recognition*, 48(4): 1027-1038.
- [45] Juhola, M., Zhang, Y., ve Rasku, J., (2013). "Biometric verification of a subject through eye movements", *Computers in biology and medicine*, 43(1): 42-50.
- [46] Kasprowski, P., ve Harezlak, K., (2016). "Fusion of eye movement and mouse dynamics for reliable behavioral biometrics", *Pattern Analysis and Applications*, 1-13.
- [47] Fong, S., Zhuang, Y., ve Fister, I., (2013). "A biometric authentication model using hand gesture images", *Biomedical Engineering OnLine*, 12(1): 111.
- [48] Wang, S. L., ve Liew, A. W. C., (2012). "Physiological and behavioral lip biometrics: A comprehensive study of their discriminative power", *Pattern Recognition*, 45(9): 3328-3335.
- [49] Liu, X., ve Cheung, Y. M., (2014). "Learning multi-boosted HMMs for lip-password based speaker verification", *IEEE Transactions on Information Forensics and Security*, 9(2): 233-246.
- [50] Wang, L., Tan, T., Ning, H., ve Hu, W. (2003). "Silhouette analysis-based gait recognition for human identification", *IEEE transactions on pattern analysis and machine intelligence*, 25(12): 1505-1518.
- [51] Zheng, S., Zhang, J., Huang, K., He, R., ve Tan, T. (2011). "Robust view transformation model for gait recognition", *2011 18th IEEE International Conference on Image Processing (ICIP)*, 2073-2076.
- [52] Stolcke, A., Kajarekar, S. S., Ferrer, L., & Shrinberg, E. (2007)., "Speaker recognition with session variability normalization based on MLLR adaptation transforms", *IEEE Transactions on Audio, Speech, and Language Processing*, 15(7): 1987-1998.

- [53] Banerjee, S. P., & Woodard, D. L. (2012). "Biometric authentication and identification using keystroke dynamics: A survey", *Journal of Pattern Recognition Research*, 7(1): 116-139.
- [54] Chandrasekar, V., ve Suresh Kumar, S., (2016). "A dexterous feature selection artificial immune system algorithm for keystroke dynamics", *Stochastic Analysis and Applications*, 34(1): 147-154.
- [55] Chandrasekar, V., Kumar, S. S., ve Maheswari, T., (2016). "Authentication based on keystroke dynamics using stochastic diffusion algorithm", *Stochastic Analysis and Applications*, 34(1): 155-164.
- [56] Chu, Z., Gianvecchio, S., Koehl, A., Wang, H., ve Jajodia, S., (2013). "Blog or block: Detecting blog bots through behavioral biometrics", *Computer Networks*, 57(3), 634-646.
- [57] Deutschmann, I., Nordström, P., ve Nilsson, L., (2013). "Continuous authentication using behavioral biometrics", *IT Professional*, 15(4): 12-15.
- [58] Schclar, A., Rokach, L., Abramson, A., ve Elovici, Y., (2012). "User authentication based on representative users", *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 42(6): 1669-1678.
- [59] Shen, C., Cai, Z., Guan, X., ve Maxion, R., (2014). "Performance evaluation of anomaly-detection algorithms for mouse dynamics", *Computers & Security*, 45: 156-171.
- [60] Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., ve Schclar, A., (2012). "User identity verification via mouse dynamics", *Information Sciences*, 201: 19-36.
- [61] Sayed, B., Traore, I., Woungang, I., ve Obaidat, M. S., (2013). "Biometric authentication using mouse gesture dynamics", *IEEE Systems Journal*, 7(2): 262-274.
- [62] Robertson, J., ve Guest, R., (2015), "A feature based comparison of pen and swipe based signature characteristics", *Human Movement Science*, 43, 169-182.

- [63] Peng, G., Zhou, G., Nguyen, D. T., Qi, X., Yang, Q., ve Wang, S., (2016). "Continuous Authentication With Touch Behavioral Biometrics and Voice on Wearable Glasses", *IEEE Transactions on Human-Machine Systems*, 99: 1-13.
- [64] Bevan, C., ve Fraser, D. S., (2016). "Different strokes for different folks? Revealing the physical characteristics of smartphone users from their swipe gestures", *International Journal of Human-Computer Studies*, 88: 51-61.
- [65] Zhou, L., Kang, Y., Zhang, D., ve Lai, J., (2016). "Harmonized authentication based on ThumbStroke dynamics on touch screen mobile phones", *Decision Support Systems*, 92: 14-24.
- [66] Kambourakis, G., Damopoulos, D., Papamartzivanos, D., ve Pavlidakis, E., (2014). "Introducing touchstroke: keystroke-based authentication system for smartphones", *Security and Communication Networks*, 9(6): 542–554.
- [67] Sae-Bae, N., Memon, N., Isbister, K., ve Ahmed, K., (2014). "Multitouch gesture-based authentication", *IEEE transactions on information forensics and security*, 9(4): 568-582.
- [68] SenthilPrabha, R., Vidhyapriya, R., ve RavithaRajalakshmi, N., (2016). "Performance analysis for a Touch dynamic authentication system with reduced feature set using neural networks", *IETE Journal of Research*, 62(2): 198-204.
- [69] Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., ve Balagani, K. S., (2016). "HMOG: New behavioral biometric features for continuous authentication of smartphone users", *IEEE Transactions on Information Forensics and Security*, 11(5): 877-892.
- [70] Peng, H., Long, F., & Ding, C. (2005). "Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy", *IEEE Transactions on pattern analysis and machine intelligence*, 27(8): 1226-1238.
- [71] Khan, S., ve Dhole, A. (2014). "A Review on Offline Signature Recognition and Verification Techniques", *International Journal of Advanced Research in Computer and Communication Engineering*, 3(6): 6879-6882.

- [72] Saikia, H., ve Sarma, K. C. (2012). "Approaches and issues in offline signature verification system", *International Journal of Computer Applications*, 42(16): 45-52.
- [73] Hafemann, L. G., Sabourin, R., ve Oliveira, L. S. (2015). "Offline handwritten signature verification-literature review", *arXiv preprint arXiv:1507.07909*.
- [74] Bay, H., Ess, A., Tuytelaars, T., ve Van Gool, L. (2008). "Speeded-up robust features (SURF)", *Computer vision and image understanding*, 110(3): 346-359.
- [75] Shah, A. S., Khan, M. N. A., ve Shah, A. (2015). "An appraisal of off-line signature verification techniques", *International Journal of Modern Education and Computer Science*, 7(4): 67.
- [76] Neamah, K., Mohamad, D., Saba, T., & Rehman, A. (2014). "Discriminative features mining for offline handwritten signature verification", *3D Research*: 5(1), 2.
- [77] Baltzakis, H., ve Papamarkos, N. (2001). "A new signature verification technique based on a two-stage neural network classifier", *Engineering applications of Artificial intelligence*, 14(1): 95-103.
- [78] Batista, L., Granger, E., ve Sabourin, R. (2012). "Dynamic selection of generative–discriminative ensembles for off-line signature verification", *Pattern Recognition*, 45(4): 1326-1340.
- [79] Skurichina, M., ve Duin, R. P. (2002). "Bagging, boosting and the random subspace method for linear classifiers", *Pattern Analysis & Applications*, 5(2): 121-135.
- [80] Ko, A. H., Sabourin, R., ve Britto Jr, A. S. (2008). "From dynamic classifier selection to dynamic ensemble selection", *Pattern Recognition*, 41(5): 1718-1731.
- [81] Cavalin, P. R., Sabourin, R., & Suen, C. Y. (2010). "Dynamic selection of ensembles of classifiers using contextual information", *International Workshop on Multiple Classifier Systems*, 7-9 Nisan 2010, Cairo, 145-154.
- [82] Batista, L., Granger, E., ve Sabourin, R. (2010). "Improving performance of HMM-based off-line signature verification systems through a multi-hypothesis approach", *International Journal on Document Analysis and Recognition (IJDAR)*, 13(1): 33-47.

- [83] Vargas, F., Ferrer, M., Travieso, C., ve Alonso, J. (2007). "Off-line handwritten signature GPDS-960 corpus", Ninth International Conference on Document Analysis and Recognition (ICDAR 2007), 23-26 Eylül 2007, Parana, IEEE, 764-768.
- [84] Kumar, R., Sharma, J. D., ve Chanda, B., (2012). "Writer-independent off-line signature verification using surroundedness feature", Pattern recognition letters, 33(3): 301-308.
- [85] Kalera, M. K., Srihari, S., ve Xu, A., (2004). "Offline signature verification and identification using distance statistics", International Journal of Pattern Recognition and Artificial Intelligence, 18(07), 1339-1360.
- [86] Guerbai, Y., Chibani, Y., ve Hadjadji, B. (2015). "The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters", Pattern Recognition, 48(1): 103-113.
- [87] Donoho, D. L., ve Duncan, M. R., (2000). "Digital curvelet transform: strategy, implementation, and experiments", Wavelet Applications VII, 5 Nisan 2000, Orlando, FL.
- [88] Sultana, M., Paul, P. P., ve Gavrilova, M., (2015). "Social behavioral biometrics: an emerging trend", International Journal of Pattern Recognition and Artificial Intelligence, 29(08): 1556013.
- [89] Lim, M., Teoh, A. B. J., ve Kim, J., (2015). "Biometric feature-type transformation: Making templates compatible for secret protection", IEEE Signal Processing Magazine, 32(5): 77-87.
- [90] Sizov, A., Khoury, E., Kinnunen, T., Wu, Z., ve Marcel, S., (2015). "Joint Speaker Verification and Antispoofing in the i-Vector Space", IEEE Transactions on Information Forensics and Security, 10(4): 821-832.
- [91] Ichino, M., Yamazaki, Y., ve Yoshiura, H., (2015). "Speaker verification method for operation system of consumer electronic devices", IEEE Transactions on Consumer Electronics, 61(1): 96-102.

[92] Al-Rubaie, M., ve Chang, J. M., (2016). "Reconstruction Attacks Against Mobile-Based Continuous Authentication Systems in the Cloud", IEEE Transactions on Information Forensics and Security, 11(12): 2648-2663.