Fırat Üniv. Müh. Bil. Dergisi
30 (1), 345-364, 2018

Science and Eng. J of Fırat Univ.
30 (1), 345-364, 2018

Davranışsal Biyometrinin 5 Yılı: Kimlik Doğrulama ve Anomali Tespit Uygulamaları

Fatma GÜMÜŞ[1], Oğuz ATA[2], Hasan Hüseyin BALIK[1,3]
[1]Bilgisayar Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, İstanbul, Türkiye
[2]Yazılım Mühendisliği Bölümü, İstanbul Altınbaş Üniversitesi, İstanbul, Türkiye
[3]Hava Harp Okulu, Milli Savunma Üniversitesi, İstanbul, Türkiye
hasanbalik@gmail.com

(Geliş/Received: 05.07.2017; Kabul/Accepted: 13.11.2017)

Özet

Mevcut biyometrik kullanıcı doğrulama teknikleri ikiye 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 çalışmada son beş yılda en yaygın olarak incelenen davranışsal biyometri yöntemlerinin kimlik doğrulama ve anomali tespit uygulamalarında kullanılan öznitelikler 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, 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.

5 Years Of Behavioral Biometrics: Authentication And Anomaly Detection Applications

Abstract

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 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, 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.

1. Giriş

1.1. Motivasyon

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 güvenliğinin kontrol altında tutulması 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 dâhilinde olan bir anahtar bilgi (şifre, PIN) ile doğrulamayı gerçekleştirir. Ancak kart ve şifrenin çalınması ya da sahtesinin üretilmesi önüne geçilmesi zorlu senaryolardır. Kişinin bireyselliğini ayırt edici olarak belirleyen,

fiziksel ya da davranışsal olarak üzerinde taşıdığı biyometrik veri ise çalınma ve sahtecilik senaryolarına karşı oldukça dirençlidir.

Mevcut biyometrik kullanıcı doğrulama teknikleri ikiye 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 doğrulamaya yardımcı olabilmesidir. Sonuç olarak, davranışsal kimlik doğrulamanın fizyolojik biyometri kullanmaktan daha ucuz olmasının 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 güvenlikli 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 ya da belli şartlar gerçekleştiğinde model güncellenebilir. Kullanıcı sistemde işlem yapar hâldeyken 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 aksamlarının 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. Araştırmanın gerekçesi ve katkısı

Bu çalışmada davranışsal biyometri alanında, kimlik doğrulama ve anomali tespit uygulamalarını konu alan son beş yılı içeren güncel çalışmaları incelenmesi ve bu süre zarfında en çok kullanılan yöntemlerin ve açık problemlerin belirlenmesi amaçlanmıştır. Davranışsal biyometri yöntemleri kategorize edilirken literatürdeki mevcut bölümlendirilmeden yararlanılmış ancak nihai şema son 5 yılda öne çıkan çalışmaların gruplandırılmasıyla oluşturulmuştur.

Biyometrik doğrulama ve anomali tespit uygulamalarının genel mimarisi benzerlik göstermektedir. Bu nedenle, incelemenin kapsamı son beş yılda öne çıkan çalışmalarda davranışsal biyometride kimlik modeli oluşturmanın ana fonksiyonu olan öznitelik çıkarımı prosedürlerini tanıtmak ve raporlanan başarılarını bildirmek olarak tanımlanmıştır. Doğrulama ve anomali tespit aşamasında kullanılan yöntemler 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 motor becerilere dayandırılmıştır. Son grupta ise

saf davranışsal biyometri olduğu belirtilmiştir. Bu grup, 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 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 koşular 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 biyometride son 5 yıllık literatürün incelendiği bu çalışmada son yıllarda öne çıkan konulara geniş yer vermek için yöntemler üç ana bölüme ayrılmıştır: Vücut Dinamiklerine Dayalı Davranışsal Biyometri, Bilgisayar Çevre Bileşenleri ve Taşınabilir Cihaz Etkileşimine Dayalı Davranışsal Biyometri, İmza ve Davranış Dinamikleri. Bu çalışmanın devamı şu şekilde düzenlenmiştir: Bölüm 2'de biyometrik kimlik doğrulama, anomali tespiti ve değerlendirme metriklerini içeren arka plan kavramları, Bölüm 3'te üç ana başlığa ayrılmış literatür incelemesi, Bölüm 4'te ise yapılan incelemeye ilişkin genel değerlendirme ve açık sorulara yer verilmiştir.

2. Arka Plan Kavramları

2.1. Biyometrik kimlik doğrulama ve anomali tespiti

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 modelle karşılaştırılır ve doğrulama sonucu hesaplanır. Sistemde tanımlı eşleme skoru sağlanıyorsa erişim izni verilir, aksi halde erişim engellenir.

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].

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

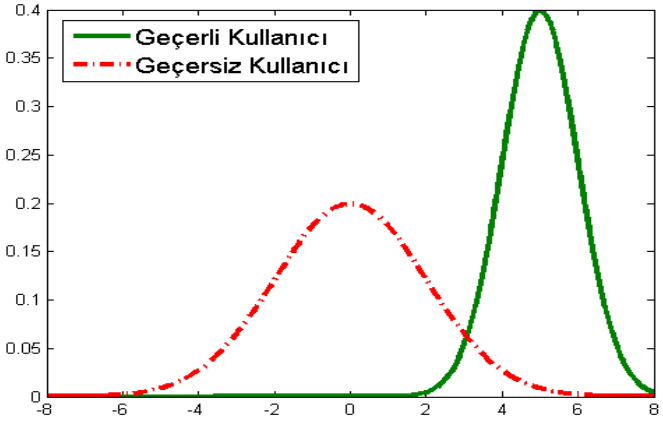
dışı aktivite olduğu tespit edildiğinde, sistemde tanımlı uyarı mekanizmaları devreye girer.

Biyometrik tanıma ve anomali tespit sistemlerindeki öncelik, tanıma hatalarını en aza indirgemek olduğu için uygun sensör, öznitelik seçim/çıkarım prosedürü ve benzerlik ölçümünün tasarlanması önemlidir. Öznitelikler bireyi yeterince açıklamalı ve diğer bireylerden mümkün olduğunca ayırabilecek niteliğe sahip olmalıdır. Bu nedenle algılayıcıdan toplanan biyometrik veri nicelleştirildikten 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.

2.2. Değerlendirme metrikleri

Biyometrik sistemlerin değerlendirilmesinde en sık kullanılan iki metrik doğruluk (accuracy) ve Eş Hata Oranı'dır (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 ret (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'deörnek dağılımlar görülmektedir. 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 sisteme daha çok 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. Örnek olasılık yoğunluk dağılımları.

3. Davranışsal Biyometri Çalışmaları

3.1. Vücut dinamiklerine dayalı davranışsal biyometri

3.1.1. Yürüyüş ve üst vücut hareketi

Yürüyüş biyometriğinde amaç, insanları yürüme biçimlerinden tanımaktır. Yürüme ölçümü dikkat çekmeden, uzaktan görsel izleme yoluyla yapılabileceği gibi taşınabilir sensörden alınan değerlerin analiziyle de gerçekleştirilebilmektedir. Görsel izleme yoluyla alınan yürüyüş biyometrisi düşük çözünürlüklü görüntüden bile çıkarılabilmektedir. Model tabanlı olan ve olmayan şeklinde iki alt grupta incelenebilir[16].

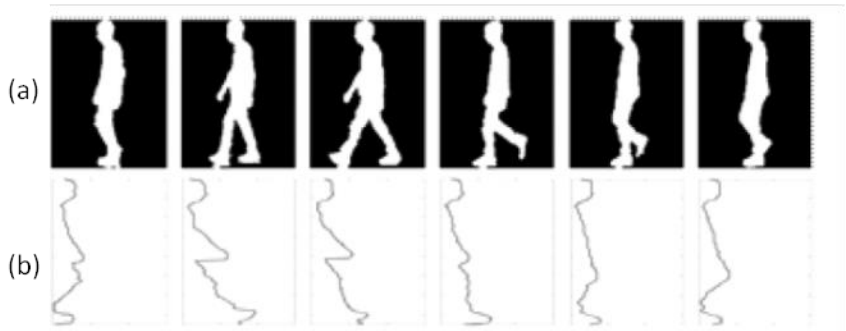
Model tabanlı yaklaşım insan vücudunu temel alır. Görüntüyü insan modeli üzerinde haritalandırır. İyi doğrulama performansı elde edebilmek için bu haritalamanın yüksek isabetle yapılması gerekir. Burada arka plan görüntüsünün ne kadar iyi ayırt edilebildiği ve kıyafet değişikliklerinin modeli ne kadar etkilediği büyük önem göstermektedir. Vücut hareket aksamlarını işaretleyici araçların kullanılması, özniteliklerin 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.

Galajdová ve diğ. [17] 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. 5 kadın ve 5 erkekten oluşan örnek kümesinde, en çok değişim gösteren parametrelerin 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 öznitelikler ayrıca manuel olarak belirlenmiştir. Çalışmadaki başarı %95.92 olarak raporlanmıştır, ancak veri setinin 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.

Kim ve diğ. [16] yürüyüş videosunda insan siluetine dayalı iki yöntemi birleştirerek doğrulama yapmıştır. Deneyler, 20 denekten oluşan CASIA-A [35] veritabanında gerçekleştirilmiştir. Füzyonda kullanılan ilk yöntemde bir silüet resmi en ve boydan ikiye bölünmek suretiyle dört parçaya ayrılır. Böylece t zamanında H×W boyutuna sahip bir siluet görüntüsü için dört şablon tanımlanmıştır: Sol genişlik vektörü, sağ genişlik vektörü, yukarı genişlik vektörü ve aşağı genişlik vektörü.

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. Şekil 2'de dikey izdüşümü çıkarılmış 6 karelik bir video parçası örneği verilmiştir.



Şekil 2. Silüetlerin çıkarılması. a. Tüm silüet, b. sol silüet [16].

Füzyonun etkisinin izlenmesi için silüet yöntemleri ayrı ayrı, ardından öznitelik seviyesinde birleştirme ve daha sonra doğrulama skoru seviyesinde birleştirme yapılarak başarı ölçümü yapılmıştır.

Tekil siluet yöntemlerinin sonuçları izlendiğinde genişlik ölçümlerine dayanan yöntemde sağ ve sol genişliğe ilişkin özniteliklerin %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. [18], kıyafetin yanıltıcı etkisinin azaltılması için altın oranına dayalı bölütleme yöntemini önermiştir. Yürüyüş Enerji Görüntüsü (Gait Energy Image, GEI) yürüyüş modellemede kullanılan defacto bir yöntemdir[19]. Bütün bir yürüyüş silküsünde 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 [36] verisetinde, farklı kıyafet senaryoları için elde edilen en düşük doğrulama sonucu %91.53 ve en yüksek %99.6 sonucu elde edilmiştir.

Liu ve diğ.[20] izleme (survellience) ortamında bir kamera yakalanan kişinin modellenip, başka kamerada doğrulanması senaryosu ele almıştır. Hem görünüş profili hem de GEI özellikleri birlikte kullanılmıştır. Skor ve öznitelik seviyesinde füzyon sonuçları değerlendirilmiştir.

Deneyler CASIA verisetinde gerçekleştirilmiştir. Kişilerin kıyafet (ceket, çanta, normal) değişimi yapmadığı senaryoda öznitelik seviyesinde füzyon, çantalı örnekler dışında, en iyi performansı göstermiştir. 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 kişinin doğrulanması için uygun bir yöntem olduğunu gösterdiği söylenmiştir.

Bouchrika ve diğ.[21] güvenlik kameraları ile izleme senaryosunu ele almıştır. Senaryoda, izleme koşulları gözetimsizdir; arka planda 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. 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 çıkartılması gerçekleştirilmiştir. İnsan yürüyüş özelliğinin çıkarımı için, hareket modelleri, yürüme türünün farklı evrelerinde diz ve kalça için açısal hareketi tanımlayan tıbbi verilere dayanarak türetilmiştir. 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 [36] 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 uygun görülebilmektedir.

Ngo ve diğ. [22], 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 telefondan elde edilmiş olması, ve 3 farklı zemin eğim koşulunu değerlendirmiş olması olarak sıralanmıştır.

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 veri setlerinde denekler yetişkindir (20-40 yaş) ancak çalışmanın veri setinde 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 veri setinin farklı yürüyüş eğimi koşullarındaki % 15.8,% 14.3 ve% 14.3 EER sonucunu birbiriyle kıyaslamanın çok doğru olmadığı belirtilmiştir.

3.1.2. Ses ve konuşma

Konuşmacı doğrulama işlemi, diğer biyometrik özelliklerde olduğu gibi önce öznitelik çıkarımı işlemine tabı tutulur, modellenir ve doğrulama yapılır. Sistem metine bağımlı yada metinden bağımsız olarak gerçeklenebilir. 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[23]. Her iki yöntemde ses sinyalini kısa süreli (genellikle 25 ms) bölütler halindeolarak incelenir.

Metin bağımlı doğrulama sistemlerinde doğrulama aşamasında genel olarak Saklı Markov Modeli (HMM) ve Vektör Nicelleme (VQ) kullanılırken, metinden bağımsız sistemlerde Gauss Karışım 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 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 arka plan modelini (UBM) oluşturur ve pozitif örnekler ise ilgili konuşmacının modelini, yani öz-sesini, oluşturmak için kullanılır[24].

Konuşma ve konuşmacı doğrulama yöntemleriyle ilgili inceleme yapan Hansen ve Hasan'ın güncel çalışmasında [25] yöntemler ve değerlendirme kriterleri ayrıntılı olarak anlatılmaktadır.

Sarkar ve diğ.[26] uzun süreli akustik özellikler elde edip, kısa süreli özelliklerle karşılaştırmış ve ikisinin birleşiminin performansını incelemiştir. Kısa süreli özellikler fonemleri modeller, uzun süreli özellikler ile ise hece ve kelimeleri modelleyebilmek mümkündür. Çalışmada uzun süreli konuşma özelliklerinin çıkarılması için Çok Katmanlı Perceptron (Multi-layer Perceptron, MLP) kullanılmıştır. Biri olasılık doğrusal regresyona (Maximum Likelihood Linear Regression, MLLR)[37] 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. 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 sistem yalnız cepstal özellikleri kullanan i-vector yöntemiyle kıyaslandığında EER ölçümünde yaklaşık %50 azalma izlenmiştir.

Konuşma ve konuşmacı modellemede son yıllarda izlenen diğer bir gelişme derin öğrenmenin uygulanması olmuştur. Liu ve diğ.

[27] konuşma sinyalinden 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 (j-vektör). DNN'den öznitelikler elde edildikten sonra GMM yada i-vector sistemlerine verilmiş ve başarı ölçümü yapılmıştır.

Derin öznitelikler elde edildikten sonra PCA ile projeksiyon yapılmış, ardından GMM ve i-vector konuşmacı sınıflandırma prosedürüne verilmiştir. Deneylerde j-vektör'den elde edilen öznitelik üzerinde en iyi konuşmacı ve konuşma sınıflandırma başarısı (%0.1 EER) gözlemlenmiştir.

Metin bağımlı ve metinden bağımsız konuşmacı doğrulama yöntemlerinin birlikte kullanıldığı bir çalışma yapan Cai ve diğ. [28] 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.

3.1.3. Göz hareketleri ve bakış

Rigas ve diğ. [29] 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 noktalarının oluşturduğu örüntüler doğrulama safhasında ele alınırken, örüntüler üst üste örtüştürülür ve noktalar arası mesafe ölçülür. KNN (k=1), KNN (k=3) ve SVM sınıflandırıcılarla elde edilen doğrulama sonuçları incelenmiştir. Deney sonuçlarına göre KNN (k=3) sınıflandırıcıyla en yüksek başarı olan %70.2 değerine ulaşmıştır.

Cantoni ve diğ.[30] de benzer bir deney düzeneği üzerinde çalışmıştır. Yüz resimleri 17 ilgi bölgesine bölünmüş ve bireysel bakış bilgileri için her bölgeye düşen dikkat noktası yoğunluğu 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 yol ve dikkat süresinin birlikte kullanıldığı düzenek en düşük EER sonucunu göstermiştir.

Juhola ve diğ.[31] 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 oto-neurolojik 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.

Kasprowski ve Harezlak[32] bakış ve fare dinamiklerini birleştiren bir doğrulama sistemi önermiştir. Deneklere ekrandaki noktaları fare ile birleştirmeleri söylenmiş, ve deneyler sırasında hem fare harekeleri hem de göz hareketleri kayıt altına alınmıştır. Statik ölçümlere dayalı öznitelikler, histogram'dan 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.

3.1.4. Dudak hareketleri

Wang ve diğ. [33] 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. Diğer bir davranışsal özellik dudak dokusunda oluşan zamansal değişimdir. Dudak görüntüsünde meydana gelen değişimler dudak çevresi bilgisiyle, dokuda meydana gelen değişiklikler ise parlaklık değeri bilgisiyle ölçülmüştür. Belirlenen bu dört özellik içinde analizler yapılarak her biri 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 altkümeyi oluşturan öznitelikler, davranışsal özellikler içinden belirlenen optimal altkümeyi oluşturan 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. [34] 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. 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.

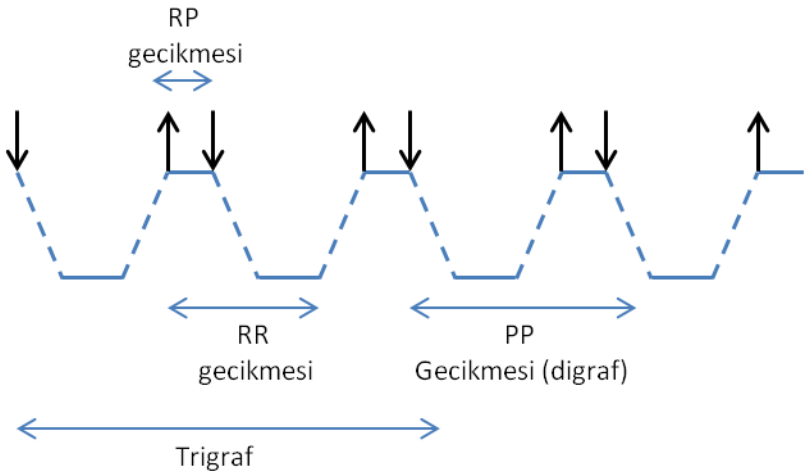
3.2. Bilgisayar Çevre Bileşenleri Ve Taşınabilir Cihaz Etkileşimine Dayalı Davranışsal Biyometri

3.2.1. 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[38][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[38].

Şekil 3'te tuşlama biyometrisinde kullanılan gecikmeye ilişkin öznitelikler görülmektedir.



Şekil 3. Tuşlama öznitelikleri [38].

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[38][12].

Chandrasekar ve Kumar [39] statik şifre tuşlamaları senaryosunda çalışmıştır. Öznitelik olarak PP ve RR gecikmesi kullanılmıştır. Ortalama medyan, standart sapma ve Hausdorff zamanlaması hesaplamaları kullanılarak önişleme yapılmış, sonuçta her örnek için 4 öznitelik üretilmiştir. Hausdorff zamanlaması, iki nokta arasındaki maksimum izometrik mesafe olarak tanımlanmıştır ve mesafe ölçümü olarak Öklid kullanılmıştır[40].

Deneylerde bağışıklık sisteminden esinlenerek modellenen bir Yapay Sinir Ağı (Artificial Immune System, AIS) 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. 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. [40] 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 Hausdroff 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.

Fare ve tuş vuruş dinamikleri gibi davranışsal biyometri yöntemleri kullanılarak insan ve bot arasında ayrım yapmak için bir algılama yaklaşımı sunan Chu ve diğ. [41] bir tuşun basılıp serbest bırakılması, farenin tıklanması 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 tekrarcı) veri üretmiştir. C4.5 karar ağacı algoritması kullanılmıştır. Bot/insan ayrımının 96 aksiyonda %98 TPR ve %99 TNR ile sağlandığı görülmüştür.

Deutschmann ve diğ. [42] tuşlama ve fare dinamikleriyle davranışsal kimlik doğrulamanın sürekli, online olarak yapılmasını ele alınmıştır. Bir güven değeri hesaplanarak tuş girişleri kayıt altına alınmış ve belli aralıklarla kullanıcı modelinde oluşan değişiklikler izlenmiştir.

Veri haftada 20 saat boyunca 99 kişiden 10 hafta boyunca toplanmıştır. 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 [15] dokunmatik klavye ile giriş PIN'inin girilmesinde anomali tespiti senaryosu üzerine çalışmıştır. Çalışmada tuşta bekleme 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 tabletten ayrıldığı noktayı birleştiren doğru) gibi beş özellik ele alınmıştır. Veri toplama işlemi 50 kullanıcı için yapılmıştır ve her kullanıcının elli örneği kaydedilmiştir.

Normal/anormal sınıflandırmasında mesafeye dayalı sınıflandırma ve meta bilişsel yapay sinir ağı (MCNN) performansı karşılaştırılmıştır. %0.2 EER ile MCNN'nin en iyi performansı sergilediği görülmüştür.

Schclar ve diğ. [43] eğitim kümesindeki eleman sayısının azaltılarak modelin fazla örtüşmesinin (overfitting) önüne geçmeyi hedeflemiştir..817 kullanıcıdan aynı şifrenin on kere girilmesi istenmiştir. Öznitelik olarak tuşta 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.

3.2.2. Fare etkileşimi dinamikleri

Sayed ve diğ. [46] deneylerinde katılımcılara ekran üzerinde örüntüler çizdirmiştir. Çizim alanından toplanan ham veriler, yatay koordinat (x ekseni), dikey koordinat (y ekseni) ve geçen her pikseldeki milisaniye cinsinden geçen süreyi içermektedir. Deneydeki 39 katılımcıya, her hareketi 30 kez çizdirilerek beş farklı tür hareketin tekrarlanması sağlanmıştır.

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. Dört hareket kombine edildiğinde FAR % 5.26, ve FRR =% 4,59 değerleri elde edilmiştir.

Shen ve diğ. [44] fare dinamiklerinde anomali tespiti çalışması yapmıştır. 17.400 örnekten oluşan veri seti oluşturulmuş, öznitelikler çıkarılmış ve 17 farklı anomali tespit algoritmasının performansı değerlendirilmiştir. Hareket yönü, hareket mesafesi ve tıklama tipi verisi toplanmıştır.

Öznitelikler iki gruba ayrılmıştır: bütünsel özellikler ve işlemsel özellikler. Bütünsel özellikler, hareket hali ve hareket süresi gibi fare davranışlarının genel özelliklerini tanımlar, işlemsel özellikler ise hız eğrileri gibi fare davranışlarının ayrıntılı dinamik süreçlerini ifade etmektedir.

Feher ve diğ. [45] 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. Tuşlama Dinamikleri başlığında değinildiği üzere Chu ve diğ. [41] tuşlama ve fare dinamiklerini birlikte kullanmıştır. Fare dinamiklerinde öznitelikler, fare tuşlarının tıklanması arasında geçen süre, işaret edip tıklama ve tıklayıp sürükleme verilerinden elde edilmiştir.

Yine tuşlama ve fare dinamiklerini birleştiren Deutschmann ve diğ. [42] 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 [32]'ın çalışmasında ise, fare ve göz hareketi dinamikleri birlikte kullanılmıştır. Tek başlarına yüksek doğrulama performansı sağlamayan bu iki yöntem birlikte kullanıldığında doğrulamanın %6.82 EER ile sağlandığı görülmüştür.

3.2.3. 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].

Robertson ve Guest [47], 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 (hareketin başlangıç-bitiş mesafesi), ve hareketin başlangıç ve bitişi arasında geçen süredir.

Peng ve diğ. [48] giyilebilir gözlüklerde dokunma ve ses biyometsi 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 en önemli öznitelikler tespit edilmiştir. Maksimum basınç tek parmak dokunmatiği için, iki parmak arasındaki mesafe iki parmaklı etkileşim için en önemli öznitelikler olduğu görülmüştür. Önemli olduğu belirtilen bir diğer bulgu, ivmeölçer özellikleri ve manyetometre özelliklerinin genellikle jiroskop özelliklerinden daha ayırt edici olmasıdır.

Öznitelik çıkarımı yapılmasının ardından, 7 SVM sınıflandırıcıdan alınan sonuçlar birleştirilmiştir. 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 [49] 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. Başparmak uzunluğu ve hızlıca kaydırma hareketlerinin üç özelliği arasında bir ilişki olduğunu gösterilmiştir.

Zhou ve diğ. [50] akıllı telefonlara hem girişte hem de giriş sonrasında ekrana dokunma dinamiklerinin birlikte kullanıldığı bir kimlik doğruma yöntemi önermiştir. 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) oluşan doğrulama düzeneklerine verilip, performans izlenmiştir. En yüksek başarı ANN ve rastgele ormanlarda sağlanmıştır. Yalnız tuşlama dinamikleri kullanıldığında başarı ~%40 iken, dokunma ve şifre ile birlikte kullanıldığında başarı %70+ olmuştur.

Kambourakis ve diğ. [51], 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. 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 özniteliğin bir vektör olarak kullanılması ve her öznitelik için ortalama alınması.

Sınıflandırma için rastgele orman ve KNN kullanılmıştır.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. [52] 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, kullanıcılardan 22 farklı çok parmaklı şifre örüntüsü alınmıştır. 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. [53] 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.

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 biyometrik özniteliği çıkarmış ve doğrulama yapmıştır. İlgilenilen senaryo, kullanıcının cihazı kullanması esnasında arkaplanda sürekli kimlik doğrulamadır.

Özniteliklerin ilgililikleri ölçülmüş, KNN ve SVM ile sınıflandırma yapılıp performansları incelenmiştir. Karşılıklı bilgi ölçümü kullanıldığında özniteliklerde ilk 6 öneme sahip olan özelliklerin SenthilPrabha ve diğ. [14]'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 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.

3.2.4. Taşınabilir cihaz etkileşimine dayalı diğer yöntemler

Sitová ve diğ. [54] 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.

HMOG özelliklerinin kimlik doğrulama performansı, dokunmatik ekran dokunma (dokunma süresi, temas büyüklüğü, hız) ve tuş vuruşu dinamik öznitelikleri (tuşta bekleme süresi ve PP gecikmesi (bkz. Bölüm 3.1) ile birleştirilmiştir. Öznitelik seçimi HMOG özelliklerinde Fisher skoru ile, dokunma özniteliklerinde mRMR[55] 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. Deneyler oturma ve yürüme senaryolarında gerçekleştirilmiştir.

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.

3.3. İmza ve davranış dinamikleri

3.3.1. İmza dinamikleri

Literatürde imza analizine iki ana yaklaşım vardır: dinamik ve statik 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 daha önce verilmiş olup, bu bölümün konusu statik imza doğrulamadır. Statik imza şekil ve oran gibi imzanın geometrik özelliklerini temel almaktadır.

Khan ve Dhole [56], Saikia ve Sarma [57], ve Hafemann ve diğ.[58] 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.

Neamah ve diğ. [59] 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 binary görüntü üzerinden hesaplanır[60]. Hesaplanan ağırlık merkezi referans noktası alınarak açısal aralık ve aralık mesafesi hesaplanmıştır. Her bireyin imzası için "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.

Batista ve diğ.'nin [61] 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 ayrık 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 veri seti kullanılmış, bu örnekleri üreten kişilerin doğrulama sistemine asla kayıtlı olmayacakları belirtilmiştir. Ayırt etme aşamasında her eğitim imzası Rastgele Altuzay Yöntemi [62] 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 [63] ve [64]'e dayalı dinamik iki sınıflandırıcı seçme algoritmasıyla (OP-ELIMINATE ve OP-UNION) en uygun sınıflandırıcı altkümesi seçilmiştir. OP-ELIMINATE algoritmasında sınıfllandırıcı 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 altkümesi ilgili test örneği için sınıflandırıcı topluluğunu (EoC, ensemble of classifiers) oluşturmuştur.

Deneylerde Brezilya statik imza veriseti [65] ve GPDS veriseti [66] kullanılmıştır. İlk senaryoda her kullanıcı için 20 imza örneği kullanılırken, ikinci senaryoda 4, 8 ve 12'şer imza örnekleri ile deneme yapılmıştır. Kullanılan verisetlerinde negatif örnekler ya rastgele yada uzman taklitlerden oluşmaktadır. Deneylerde performans değerlendirmesi yapılırken her negatif örnek grubu için ayrı ayrı FAR hesaplanıp ortalaması alınmıştır (average error rate, AER). Baseline olarak [65]'teki doğrulama yöntemi kullanılmış, farklı sınıflandırıcı seçme algoritma kombinasyonlarının performansı değerlendirilmiştir. Her iki veriseti ve senaryo için de baseline sınıflandırıcı en kötü performası sergilemiştir.

Kumar ve diğ. [67] YSA ve SVM sınıflandırıcıların performansını çevrelenmiş olma (surroundness) öznitelik kümesi için karşılaştırmıştır. Görüntüler üzerinde önişleme yapılıp binary görüntü haline getirildikten sonra, her siyah piksel için çevrelenme farklı mesafelerde ölçülmüştür. r mesafesinde çevrelenme ölçmek için, ölçülmek istenen pikseli ortalayan r yarıçaplı dairede bulunan siyah piksel sayısı sayılmıştır. Deneyler CEDAR[68] ve GPDS[66] verisetlerinde gerçekleştirilmiştir. 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.[69] 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.

Öznitelikler [70]'teki prosedürle elde edilmiştir. Deneyler CEDAR[68] ve GPDS[66] verisetlerinde gerçekleştirilmiştir. Eğitim sırasında çeşitli hiper-parametreler için destek vektörlerinin sayısını ve tanıma oranını maksimum yapan hiper-parametre değerleri sınıflandırıcıda kullanılmıştır. Eşik değeri için FAR ve FRR değerlerinin ortalaması kullanılmıştır. Her iki veriseti için de eşik değerleri sıfıra yakın çıkmıştır. Sistemin 4, 8, 12'şer imza ile eğitildiği durumda örnek sayısı arttıkça başarının iyileştiği görülmüştür. GPDS veri kümesinde [67]'nin en iyi başarıyı verdiği ve ardından sırayla [69] ve [61]'in performansının geldiği görülmüştür.

3.3.2. Davranış dinamikleri

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

Sultana ve diğ. [71] 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 alınabileceği belirtilmiştir. Çalışmada bu dört çeşit etkileşim öznitelikleri kullanılmıştır.

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

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.

4. Genel Değerlendirme Ve Açık Problemler

4.1. Genel değerlendirme

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. 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.

4.2. Açık problemler

4.2.1. Veri güvenliği

Davranışsal biyometri modellerinin tesis ve sistem erişimi, finansal işlemler ve çevrimiçi sosyal ağlar gibi alanlarda daha fazla yararlanılacağı öngörülmektedir. 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 öznitelik transformasyonu[72], sahtekar girişi önleyici prosedürler[4][73][74] 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[75].

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.

4.3. Davranışsal Biyometrik Doğrulama Performansı

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

4.3.1. 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].

4.3.2. Saha Koşullarına Uygun Çalışmanın Yetersizliği

Deneysel 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.

4.3.3. Kaynakların Etkin Kullanımı

Biyometrik uygulamaların öncül gereksinimi doğruluk performansının yükseltilmesidir. Sistemlere he 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 bulunsa da, 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.

4.3.4. Erişime Açık Verisetinin Oluşturulması

Davranışsal biyometri ile ilgili çalışmalarda açık veri setlerinin 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.

5. 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://goo.gl/AbirLE, 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. Salakhutdinov, R., ve Hinton, G., (2009). "Deep boltzmann machines", Artificial Intelligence and Statistics, 448-455.

15. Prabha, R. S., ve Vidhyapriya, R., (2017). "Intruder Detection System Based on Behavioral Biometric Security", Journal Of Scıentıfic & Industrıal Research, 76: 90-94.

16. Kim, E., Hong, S., ve Lee, H. (2012). "Human Identıfication By Fusion Of Multiple Gait Representations", Advanced Topics in Biometrics, 229.

17. 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.

18. 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.

19. Man, J., ve Bhanu, B. (2006). "Individual recognition using gait energy image", IEEE transactions on pattern analysis and machine intelligence, 28(2): 316-322.

20. Liu, Z., Zhang, Z., Wu, Q., ve Wang, Y., (2015). "Enhancing person re-identification by integrating gait biometric", Neurocomputing, 168: 1144-1156.

21. 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.

22. 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.

23. 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.

24. 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).

25. Hansen, J. H., ve Hasan, T., (2015). "Speaker recognition by machines and humans: A tutorial review", IEEE Signal processing magazine, 32(6): 74-99.

26. 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.

27. 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.

28. Cai, Y., Li, X., Gong, Z., ve Codina, T. R., (2014). "Speaker verification for multi-task interactions", Interacting with Computers, 26(2): 135-144.

29. 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.

30. 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.

31. 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.

32. Kasprowski, P., ve Harezlak, K., (2016). "Fusion of eye movement and mouse dynamics for reliable behavioral biometrics", Pattern Analysis and Applications, 1-13.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. Deutschmann, I., Nordström, P., ve Nilsson, L., (2013). "Continuous authentication using behavioral biometrics", IT Professional, 15(4): 12-15.

43. 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.

44. Shen, C., Cai, Z., Guan, X., ve Maxion, R., (2014). "Performance evaluation of anomaly-detection algorithms for mouse dynamics", Computers & Security, 45: 156-171.

45. Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., ve Schclar, A., (2012). "User identity verification via mouse dynamics", Information Sciences, 201: 19-36.

46. Sayed, B., Traore, I., Woungang, I., ve Obaidat, M. S., (2013). "Biometric authentication using mouse gesture dynamics", IEEE Systems Journal, 7(2): 262-274.

47. Robertson, J., ve Guest, R., (2015), "A feature based comparison of pen and swipe based signature characteristics", Human Movement Science, 43, 169-182.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. Saikia, H., ve Sarma, K. C. (2012). "Approaches and issues in offline signature verification system", International Journal of Computer Applications, 42(16): 45-52.

58. Hafemann, L. G., Sabourin, R., ve Oliveira, L. S. (2015). "Offline handwritten signature verification-literature review", arXiv preprint arXiv:1507.07909.

59. Neamah, K., Mohamad, D., Saba, T., & Rehman, A. (2014). "Discriminative features mining for offline handwritten signature verification", 3D Research: 5(1), 2.

60. 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.

61. 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.

62. Skurichina, M., ve Duin, R. P. (2002). "Bagging, boosting and the random subspace method for linear classifiers", Pattern Analysis & Applications, 5(2): 121-135.

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. Donoho, D. L., ve Duncan, M. R., (2000). "Digital curvelet transform: strategy, implementation, and experiments", Wavelet Applications VII, 5 Nisan 2000, Orlando, FL.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.