# Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme

**Bilgehan ARSLAN, Şeref SAĞIROĞLU**

Gazi Üniversitesi, Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü 06500 Ankara, TÜRKİYE

(Geliş / Received : 10.04.2015 ; Kabul / Accepted : 08.12.2015)

**ÖZ**

Mobil cihazların kullanımlarındaki artış, bu cihazların farklı kullanım alanlarının oluşmasına sebep olmuştur. Bu alanlarından biri de mobil cihazlarda kullanılan biyometrik sistemler ve yöntemlerdir. Biyometrik sistemler, mobil cihazlar üzerinde uzaktan erişim modeli oluşturmak, kişisel veri gizliliğini sağlamak, erişim güvenliğini kişiselleştirmek ve kolaylaştırmak amacıyla kullanılabilmektedir. Bu çalışmada, mobil cihazlarda kullanılan biyometrik sistemler, metotlar, teknolojiler araştırılmış ve bunların sağladığı üstünlükler ile dezavantajlar verilmiştir. Literatürde yapılan çalışmalar, kullanılan algoritmalar, teknolojiler, metrikler, kullanıldığı alanlar, mobil yüz, avuç izi, iris, ses, parmak izi tanıma gibi farklı biyometrik sistemler için araştırılmış ve yapılan çalışmalar değerlendirilmiştir.

**Anathar Kelimeler: Mobil, biyometri, tanıma, güvenlik, iris, parmak izi, ses, avuç izi, yüz, uzak erişim, veri gizliliği.**

# A Review on Biometric Systems Used in Mobile Devices

**ABSTRACT**

Rise of using mobile devices has led to different usage areas for these devices. One of them is biometric systems and methods used in mobile devices. They create a remote access model on mobile devices, ensure confidentiality of personal data on mobile devices and these are used in order to personalize and facilitate access security. In this study, biometric systems used in mobile devices, methods and technologies have been investigated. Advantage and disadvantages of them are given. The studies in the literature such as algorithms, technologies, metrics, usage, are investigated for different biometric systems. Mobile face, palm print, iris, voice, fingerprint recognition and studies are evaluated.

**Keywords: Mobile, biometrics recognition, security, iris, fingerprint, voice, palm print, face, remote access, data privacy**

## 1. GİRİŞ (INTRODUCTION)

Mobil ortamlar, rahat kullanım alanı ve kullanıcının isteklerini temel alan uygulamalar sebebiyle rağbet görmektedir. Mobil teknolojilerin günlük hayatın vazgeçilmez bir parçası olarak yer edinmeye başlaması, dikkatlerin bu noktada sunulan mobil hizmetlere yoğunlaşmasını sağlamıştır. Bilgi teknolojisi çağında, mobil cihazların temel haberleşme cihazları olarak kullanılmasının dışında kişisel birçok alanda da hizmet vermektedir. Kablosuz telefon iletişim gücündeki büyük artış, mobil cihazlarda çalışabilen spesifik uygulama çeşitliliği ve bununla birlikte bu alandaki üretimin artması sebebiyle çok sayıda kullanıcı tarafından tercih edilmesindeki en büyük etkendir.

Bu çalışmada mobil biyometrik sistemler üzerine genel bir bakış açısı sunmak amaçlanmıştır. Mobil biyometrik sistemler ile alakalı yapılan literatür araştırması sonucunda, bu alanda yapılan çalışmaların kısıtlı sayıda olduğu görülmüştür. Yapılan çalışma doğrultusunda, mobil cihazlar üzerinde biyometri teknikleri kullanmak isteyen araştırmacılara yeni bir bakış açısı oluşturmak ve geliştireceği uygulamalar için yol göstermek amaçlanmıştır. Şimdiye kadar yapılan çalışmalar incelenerek, mobil biyometrik tekniklerden hangisinin en yaygın olduğu, kullanılan tekniklerin avantaj ve dezavantajları, uygulama esnasında oluşabilecek sorunlar incelenmiş ve kullanılan yöntemler kıyaslanarak hangi alanda eksikliklerin olduğunun tespit edilmesi amaçlanmıştır.

Literatür araştırmasında incelenen her çalışmada belirli bir biyometrik tekniğin kullanıldığı bir mobil sistem geliştirilmiş, bu sistemin çalışması için gerekli platformun tasarımı ve geliştirilen uygulamada kullanılan teknikler üzerinde durulmuştur. Bu çalışmada farklı biyometrik teknikler kullanarak geliştirilen uygulamalar birbirleri ile kıyaslanmış ve hangi tekniklerin kullanımının diğerlerine oranla yüksek olduğu tespit edilmiştir.

Yapılan bu çalışmanın, biyometrik yöntemlerin mobil cihazlarda ana hatlarıyla uygulanabilirliği konusunda yol gösterici olması beklenmektedir.

## 2. MOBİL BİYOMETRİK SİSTEMLER (MOBILE BIOMETRIC SYSTEMS)

Mobil cihaz kullanımındaki oran gün geçtikçe artmakla birlikte, artık mobil cihazlar günlük hayatın vazgeçilmez bir parçası haline gelmektedir. BTK verilerine

* *Sorumlu Yazar (Corresponding Author)*
*e-posta:bilgehanarslan@gazi.edu.tr*
*Digital Object Identifier (DOI) : 10.2339/2016.19.2 101-114*

göre, 2014 yılı ocak ayında 69 milyon 797 mobil telefon kullanan abone bulunmaktayken bu sayının 2014 yılı sonu itibariyle 71 milyon 888 bine yükseldiği görülmektedir [1].

Mobil teknolojilerin sürekli gelişimi ve artan talep de göstermektedir ki gün geçtikçe mobil sistemler kullanılan tekniklerin yerini alacaktır. Kullanıcıya ait bir mobil cihaz üzerinden, kişinin kimlik bilgileri, kredi kartı numaraları ve şifreleri, adresi, telefonu, kişisel resim ve videoları, Facebook, WhatsApp, Twitter, Linkedin, Google+ vb. sosyal ağlara giriş için kullandığı şifre ve kullanıcı adı bilgileri gibi birçok veriye erişilebilmektedir. Bu sebeple mobil cihazlarda güvenliği artırabilmek amacı ile PIN (Personal Identification Number) veya token gibi yöntemlere başvurulmuştur. Fakat bu tip yöntemlerde kullanıcı tarafından belirlenen şifrenin kalitesine göre güvenlik seviyesi belirlenmektedir. Kullanıcı basit bir şifre kullandığında kötü niyetli kişilerce ele geçirilen mobil cihazın şifresi çözülebilir. Noktalama işaretleri, rakam ve harfin kombinasyonları, ASCII karakterlerinden oluşan şifreler daha spesifik olduğundan tahmin edilemezler fakat karmaşıklıklarından dolayı kullanıcı tarafından unutulabilir, kullanım açısından elverişli olmayabilir [2]. Bu sebeple kullanıcı tarafından hatırlanmaya ihtiyaç duyulmayan ve aynı zamanda bireyi ayırt edebilecek kadar spesifik bir yöntem arayışı içine girilmiştir. Görülmektedir ki biyometrik teknikler, genellikle güvenlik seviyelerini artırmak için, önceki kimlik doğrulama yöntemlerine ek olarak kullanılan yöntemlerdir ve iyi bir çözüm olarak görülmektedir.

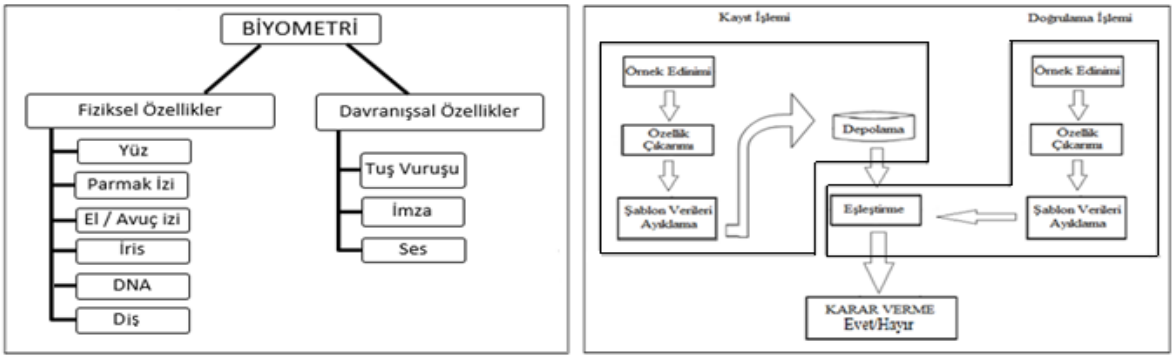
Biyometrik tanıma işlemi gerçekleştirilirken eşsiz olarak belirlenen insan özellikleri kullanılmakta olup biyometrik sistemler temelde 2 farklı grup üzerinden incelenir [3]. Bunlar fizyolojik ve davranışsal özelliklerdir. Parmak izi, DNA, retina, iris vb. gibi insan vücudunun bir bölümünün doğrudan ölçümlenmesi ile uygulanan sistemler fiziksel özellikler kullanılarak tasarlanan biyometrik sistemlerdir. İmza, yürüyüş, konuşma vb. özellikler üzerinden dolaylı olarak kullanıcı tarafından gerçekleştirilen bir işlemi ölçüp elde edilen verilere dayanan sistemler ise davranışsal özellikler kullanılarak tasarlanan biyometrik sistemler olarak adlandırılır. Biyometrik tanıma işlemi iki aşamada gerçekleşmektedir. Bunlar tanımlama ve doğrulama işlemleridir. Tanımlama işlemi, büyük miktarda işlem gücü gerektirir ve kullanılan veritabanı çok büyük ise, çok zaman alır. Doğrulama işleminde ise depolanmış örnek şablon verisi ile kontrol için elde edilen veri, karşılaştırma işlemine tabi tutulduğundan daha az işlem gücü gerektirmektedir.

Biyometrik sistemler önceden depolanmış görüntülerin (veritabanı görüntüleri) tanıma işlemi için anlık elde edilen görüntülerle (prob görüntüler) belirgin ya da ayırıcı özellikleri dikkate alarak eşleştirilmesini sağlar. Tanıma sürecinde tüm biyometrik sistemler belirli adımlar dâhilinde hareket ederler. Her yöntemde ayırt etmek amacı ile kullanılacak karakteristik özellik ve buna bağlı sınıflandırma, analiz etme ve doğrulama işlemleri gerçekleşir [4]. Biyometrik tanıma işlemini basit olarak dört ayrı basamakta incelenmektedir [5-10]:

- Görüntü Elde Etme: Öncelikle kullanılacak yönteme ait donanımlar ile analog veri ortamından dijital veri ortamına gerekli karakteristik özellik (parmak izi, iris retina ağ yapısı vb.) aktarılır.
- Özellik Çıkarma: Analog ortamdan dijital ortama aktarılan veri bir takım işleme tabi tutulur. Aktarılan veriden, tanıma işleminde doğru sonucu alabilecek oranda gerekli parametreler ayırılır.
- Veri tabanı Depolama: Elde edilen bu parametre değerleri güvenlik seviyeleri yüksek veri tabanlarında depolanır. Kontrol işleminin gerçekleşeceği sırada mevcut depolanan parametreler ile anlık ölçülen parametre değerleri karşılaştırılır.
- Eşleştirme: Karşılaştırma işleminin yapılması için gerekli olan verileri tutacak veri tabanı, doğruluğu kontrol edecek algoritmalar ve yöntemlere tabi tutulan ilk ve son verinin, kesişme oranlarına göre tanıma işlemi gerçekleşir.

Şekil 1'de biyometrik sistemler ve bu sistemlerin çalışma basamakları gösterilmektedir

Günümüzde, mobil cihazlardaki işlem gücünün artışı, bu cihazlarda kullanılan kablosuz ağ teknolojilerinde görülen hızlı gelişim ve bu cihazların kullanıcıya sunduğu (kullanıcıya yönelik e-bankacılık, e-ticaret, güvenli mobil ödeme uygulamaları ve ulusal kullanım için e-ticaret, sınır kontrolü, pasaport kontrolü, suçluya ait araştırma, ceset kimlik tespiti, anne ve babalık tespiti




Şekil 1. (a) Biyometrik Sistemler ve Çalışma Şeması (Biometric Systems and Recognition Process Scheme)

gibi uygulamalar) farklı hizmetlerin çeşitliliği sebebiyle mobil cihazlar biyometrik tekniklerle birlikte anılmaktadır. Biyometrik sistemlerin mobil cihazlarda 2 farklı kullanım amacı bulunmaktadır. Bunlar:

- Biyometrik sistemler pahalı teknolojilerdir. Çünkü bu sistemlerde kullanılan yöntemler pahalıdır ve kullanım alanları bakımından kısıtlamalar vardır. Yüksek güvenlik bölgelerine erişim ve giriş çıkış kontrolü gereken noktalarda (hava alanı, teknik merkezler ve laboratuvar, banka, hastane, sınır kontrolü noktaları) kullanılan bu sistemlerin çalışması için gerekli donanımsal ekipmanlar çok fazla yer kaplamaktadırlar ve taşınabilir özelliğe sahip değildirler. Bu sebeple düşük maliyetli, mobil sistem tasarımı biyometrik yöntemler için elzem görülmüştür. Mobil teknolojiler, biyometrik sistemlerin mobil ortamlarda uygulanması taşınabilirlik ve gereğinden fazla alan kaplama gibi dezavantajlarının çözümü olmuştur.
- Mobil cihazlarda kişisel veriler tutulduğundan bu kritik bilgilerin korunması, kötü niyetli kişilerce elde edilmemesi gerekmektedir. Bu kapsamda mobil cihazlarda kullanılan biyometrik teknikler, açığa çıkan güvenlik zafiyetini en aza indirmektedir.

## 3. İLGİLİ ARAŞTIRMALAR (RELATED WORKS)

Biyometrik sistemler geniş kullanım alanına sahiptir. Mobil cihazlarda biyometrik tanıma, güvenli ve akıllı bilgilendirme sistemleri aktif olan araştırma alanlarından biridir. Bugüne kadar farklı araştırmalar, mobil / akıllı telefonlar için kullanılabilir farklı biyometrik teknikler üzerinde yapılmıştır. Bu teknikler, parmak izi tanıma, yüz tanıma, el geometrisi, iris tanıma, ses tanıma, imza vb. yöntemlerdir. Bu çalışmada, mobil biyometrik sistemlerde yapılan uygulamalar akademik ve sektörel (ticari) olarak ikiye ayrılıp incelenmiş ve alt başlıklarda açıklanmıştır.

### 3.1. Akademik Çalışmalar (Academic Researches)

Tablo 1'de mobil biyometrik sistemler üzerine yapılan akademik çalışmalar, bu çalışmada kullanılan teknikler, biyometrik özelliklerin kullanım oranları ve veri tabanları ile çalışmaların avantajları ve dezavantajları verilmiştir. Mobil biyometrik sistemler üzerine yapılan literatür çalışması sonucu yaygın olarak kullanılan mobil tekniklerin; parmak izi tanıma [11]-[15], ses tanıma [16]-[22], iris tanıma [23]-[31], yüz tanıma [32]-[36], avuç izi tanıma [37]-[40], diş tanıma [41] [42], yürüyüş tanıma [43] ve imza tanıma [44] olduğu tespit edilmiştir. Biyometrik tekniklerin kullanılabilirliği, uygulama alanları, gerekli cihaz ve ekipmanlar,

Çizelge 1. Biyometrik Yöntemler, Kullanılan Teknikler, Veri setleri, Kullanım Oranları (Biometric Methods, Utilized Techniques, Data Sets, Usage Rates)

| Özellik | Kullanım Oranları | Kullanılan Teknikler | Veri Tabanları | Avantajlar-Dezavantajlar |
|---|---|---|---|---|
| Parmak İzi | %15 [75] | - | Atmel Fingerprint [2] | • Mobil cihazlarda uygulamanın gerçekleşmesi için harici donanım gerektirmektedir.<br>• Karakteristik olarak ayırt edici özelliği yüksektir. |
| Ses | %13 [75] | MFCC [16] [17] [20], GMM [16] [20], HMMs [17], ASR [19], SVM[19], UBM [20] | AURORA 2.0 [16] | • Uygulaması kolay fakat kolay taklit edilme özelliğine sahiptir.<br>• Ses teline zarar verebilecek hastalık vb. durumlardan etkilenmektedir. |
| İris | %16 [75] | Circular Edge Detection [25], Hough Transform [25], AGF [26], SRs [27], AdaBoost [27], SVM [28], LBP [28], Gabor Filter [28][29] | Chungbuk Iris database [23], Casia [25] [26] [27], MOBIOFake Database [28], MOBIO Multimodal Database [28], MICHE dataset [31] | • Dış etkenlerden neredeyse hiç etkilenmeyecek bir özelliktir.<br>• Karakteristik özelliği ve ayırt edicilik oranı çok yüksektir.<br>• Hassas çekim tekniği ve yüksek çözünürlüğe sahip görüntü gerektirir.<br>• Bazı mobil cihazlardaki düşük kapasiteli kamera yeterli olmadığından harici donanım gerektirmektedir. |
| Yüz | %15 [75] | PCA [32], Okao Vision [33], LBP [20] [36], SVM [35], AdaBoost [35] [36], HaarLike [36], Viola Jones Algorithm [30] | The Color FERET Database, Surveillance Cameras Face Database, The Yale Face Database, Multi-PIE [71] | • Yüksek referans noktası gerektirmesinden dolayı performans oranını düşürmektedir.<br>• Parmak izi gibi kolay taklit edilemezler.<br>• Yara izi, zamana bağlı yaşlanma gibi durumlardan etkilenir. |
| Avuç İzi | %10 [75] | ROI [38] , Gauss Filtreleme [37] [40] | IIT Delhi Database [39], Knuckle Database [39], PolyU palmprint database [40] | • Uygulanacak kişi sayısı belirli bir sınırın altında olan alanlar için kullanımı mümkündür.<br>• Harici donanım gerekmektirmektedir. |
| Diş | - | PCA[41], LDA [41], EHMM[41] [42], HaarLike [41] [42], AdaBoost [41] [42] | - | • Zamana bağlı olarak değişiklik gösterebilmektedir. Dış etkenlerden etkilenme oranı yüksektir. |
| Yürüyüş (Silüet) | - | DTW [43], FastDTW [43] | - | • Doğruluk oranları ve çalışma prensibi üzerine halen araştırmalar yapılmaktadır.<br>• Harici donanım gerektirmektedir. |
| İmza | %10 [75] | HMMs [44], FDR [44] | - | • Kolay taklit edilebilir. |

istikrarlı çalışma oranı ve doğruluk değerleri birbirlerine göre farklılık göstermektedir. Bu sebeple kullanıcı için yüksek tanıma performansı, uygulamaya müdahaleci, kolay ve güvenilirliği yüksek olan, pratik uygulama tekniğine sahip biyometrik tekniği bulmak zordur.

Mobil avuç izi tanımada literatürde farklı çalışmalarda farklı algoritmalar ve metotlar kullanılsa da elde edilen başarıların uygulama için belirli seviyeye geldiği, bundan sonraki süreçlerde üzerinde daha fazla durulan konuların başında geleceği değerlendirilmektedir. Özellikle güvenlik alanında farklı çözümler sunabileceği düşünül-mektedir.

Literatürde en fazla uygulamanın bulunduğu alanların başında mobil yüz tanıma teknikleri gelmektedir. Kullanılan algoritmaların çoğunlukla standart algoritmalar olduğu ve son dönemlerde ise yapay zeka yaklaşımlarının da başladığı, başarı kriterlerinin gittikçe yükseldiği görülmektedir. Özellikle mevcut teknolojilerde başarılı entegrasyonların başlaması sebebiyle bu konunun daha çok çalışılacağı ve özellikle güvenlik alanında farklı uygulama alanları için pek çok fırsatı üzerinde barındıracağı değerlendirilmektedir.

Literatürde incelenen çalışmalar da göstermektedir ki, iris tanıma sistemleri, yüz tanıma sistemlerini kullanım oranı olarak geçmiş ve en çok tercih edilen biyometrik yöntem haline gelmiştir. Kullanılan teknikler olarak değerlendirildiğinde yüz tanıma tekniklerinde kullanılan yapay zekâ yöntemleri iris tanıma sistemlerinde de kullanılmaktadır. Bunun dışında yüz tanıma tekniklerinde kullanılan algoritmalar ve yöntemler, daha hassas ölçüm parametreleri alarak düzenlenmiş ve iris tanıma sistemlerinde kullanılmıştır. İrisin karakteristik özelliği ve değişim gösterme olasılığının düşük olması sebebiyle yüksek güvenlik seviyesine sahip sistemler üzerinde kullanım alanı bulduğu gözlenmektedir. Özellikle mobil uygulamalarda parmak izi ve yüz tanıma sistemlerinden daha hassas bir yöntem seçilmesi gereken durumlarda, iris tanıma uygulamalarına başvurul-maktadır.

Mobil ses ve imza tanıma sistemlerinde incelenen literatür doğrultusunda, uygulamalarda genellikle aynı yöntemlerin kullanıldığı tespit edilmiştir. Kullanılan bu tekniklerde yapılan küçük parametre değişiklikleri ve kullanılan cihaz kalitesi, bu çalışmalardaki farklı sonuçların elde edilmesindeki en büyük etkendir. Bunun dışında özellikle ses ve imza tanıma sistemlerinin kolay taklit edilebilir olmasından dolayı, bu yöntemin beraberinde kullanılan harici tekniklerle çoklu biyometrik yöntemlerin kullanıldığı uygulamaların geliştirildiği gözlenmektedir. Özellikle bankacılık hizmetlerinde ses tanıma sistemlerinin tercih edildiği gözlemlenmektedir.

Parmak izi ile kimlik tespiti yöntemi en fazla kullanılan biyometrik yöntemlerden olmasına rağmen, mobil cihazlarda iris tanıma sistemleri ile kıyasla daha düşük kullanım oranına sahiptir. Parmak izi tespiti üzerine doğru sonuçların elde edilebildiği çok sayıda yöntemin olması sebebiyle, son dönemlerde yapılan çalışmalarda doğru tanımlama işlemi dışında hızlı sonuç üretimi, taşınabilir ortamlar kullanarak güvenli giriş çıkış hizmetleri gibi daha spesifik alanlar üzerinde yoğunlaşıl-dığı, bu tekniğin özellikle güvenlik konusunda pek çok farklı uygulama alanında yer edindiği görülmektedir.

Diş ve yürüyüş analizi gibi biyometrik teknikler, zamanla değişim göstermeleri ve farklı bireylerdeki benzerlik oranlarının yüksek olabilme ihtimali sebebiyle güvenlik zafiyeti oluşturacak ortamlarda çok fazla kullanılma-maktadır. Fakat literatürde yapılan çalışmalar, bu tarz biyometrik teknikler üzerinde halen yoğun araştırmaların yapılmaya devam ettiğini göstermektedir.

**3.1.1. Parmak İzi Tanıma** (Fingerprint Recognition)

Biyometrik yöntemlerden parmak izi tanıma, Faulds ve Herschel adında iki İngiliz bilim adamının çalışmalarıyla başlamıştır [72]. Parmak izi büyüme, yaşlanma gibi zamana bağlı faktörlerle değişmeyen ve ayırıcı özelliğini yitirmeyen bir özelliktir. Biyometrik sistemlerle analiz konusunda parmak izi en eski yöntemlerin arasında yer aldığı için, bu yöntem hakkında çok fazla donanımsal altyapı ve yöntem mevcuttur. Biyometrik sistemler içinde erişimi ve uygulanması en kolay yöntemdir ve oldukça geniş kullanım alanına sahiptir [45]. Mobil parmak izi tanıma üzerine yapılmış bazı çalışmalar aşağıdaki Tablo 2'de listelenmektedir.

Parmak izi tanıma sistemlerinin ilk kullanıldığı zamandan beri, bu sistemi tersine zorlamak adına birçok yönteme başvurulmuştur. Bunlardan biri de parmak izini kopyalama adı altında yapılan işlemlerdir. Bunun üzerine parmak izi okumak dışında, vücut ısısı veya parmak üzerindeki damarlarda bulunan oksijen miktarı gibi ayırt edici ve canlı örnekten alındığına dair sınırlayıcı özellikler eklenerek güvenlik seviyesini arttırıcı uygulamalar geliştirilmiştir [46] .

Bu sistemin avantajları ve dezavantajları [47] :

- Parmak izi bireyden kolay ve maliyetsiz bir biçimde alınabilir.
- Parmak izi de retina gibi ikizlerde bile farklılık gösterir.
- Parmak izi üzerinde değiştirme işlemi oldukça zordur. Bu sebeple taklit ve değiştirme işlemi oldukça zordur.
- Parmak izi ayırt edici belli başlı unsurların farklı kombinasyonlarından oluşur. Bu sebeple kıyaslanacak parmak izinde mevcut olan ayırt edici yapılar belirlenip arama işlemi yapıldığında hızlı sonuç elde edilebilir.
- Örnek alınan parmağın yıpranması sonucu aynı izin tekrar elde edilemeyebilir.
- Kişinin fiziksel değişimi alınan parmak izinin depolanmış örnekle örtüşmemesine sebep verebilir.
- Parmak izinin kalıbının kendisi yerine kullanılma ihtimali vardır.

Parmak izi tespiti yapılırken farklı yöntemler kullanılabilir. Fakat en yaygın olarak öznitelik çıkarımı ve filtreleme yöntemleri kullanılmaktadır. Yapılan çalışmalar incelendiğinde öznitelik çıkarımı için;

inceltilmiş parmak izi görüntüsünden özellik çıkartma, zincir (chain code) kuralı ile özellik çıkartma, bölgesel analiz yaparak özellik çıkartma gibi algoritmaların kullanıldığı görülmüştür [48]. Öznitelik tekniği ile parmak izi tanıma işlemi gerçekleştirilirken, parmak izi okuyucu ile elde edilen veri, bahsettiğimiz öznitelik çıkartma algoritmaları ile işlenir [13]. Elde edilen özellik vektörü veri tabanına kaydedilir ve daha sonra tanıma işleminin gerçekleşmesi sırasında elde edilen yeni parmak izi verisi ile veri tabanındaki özellik vektörü karşılaştırılır [13]. Filtreleme işleminde ise genel olarak gabor filtreleme kullanılmaktadır. Bu filtre sayesinde elde edilen parmak izi verisinden gerekli veri süzülebilmektedir ve özellik vektörü oluşturulmaktadır [49]

**3.1.2. Ses Tanıma** (Speech Recognition)

Ses analizi 20. yüzyılda Dudley ve Fletcher tarafından ortaya çıkmıştır [73]. Konuşma sürecinde oluşan sesin tanıma işleminde sinyal aralığının önemli olduğunu keşfedildiği için ses tanıma algoritmalarının temeli bu çalışmaya dayanmaktadır. Ses tanıma sistemin çalışma prensibinde ayırt edici olarak kullanılan akustik ses verisi dijital formatta veri tabanına kaydedilir. Sistem çalışma sürecinde şifre niteliğinde kullanılan belirli bir kelime grubu, kullanıcıya okutularak kaydedilir. Bu işlem ile kullanıcının ses verisi sisteme öğretilmiş olunur [74]. Kaydedilen ses spektral analizler kullanılarak dijitalleştirilir. Sonrasında ise kontrol işlemini sağlanması gereken durumlarda kullanıcı aynı kelime grubunu okuyarak sisteme erişebilir. Genel olarak ses analizi ile biyometrik tanıma işlemi bu şekilde gerçekleştirilir. Fakat bu işlem sırasında kullanılan teknik ve yöntemler çeşitlilik gösterebilmektedir. Biyometrik ses tanıma yöntemleri göç, vatandaşlık hizmetleri, ordu, uluslararası bankalar ve sağlık örgütleri, hassas bilgi korunumu, kişisel bilgi güvenliği, e-ticaret, internet bankacılığı gibi alanlarda kullanılmaktadır [16]

[17] [18] [22]. Mobil ses tanıma üzerine yapılmış bazı çalışmalar aşağıdaki Tablo 3'de listelenmektedir.

Ses tanıma sistemleri telefon üzerinden bir sisteme ulaşım için daha uygun bir yapıdadır. Fakat sesin çok fazla yer kaplaması, hastalık veya başka dış etkenlerden etkilenmesi, parazit oluşturan dış ortamdan gelen gürültüler sistem çalışmasını engelleyici faktörlerdir [50].

Ses tanıma işleminin dezavantajları [51]:

- Kamuya açık alanlarda veya yankılı telefon hatları gibi gürültülü çevre şartlarında ses tanıma sistemleri güvenilir değildir.
- Soğuk algınlığı nedeni ile meydana gelen ses kısılmalarına karşı çok hassastır.
- Ses tanıma sistemi, geçiş/erişim hakkına sahip bir kişinin ses kaydı kullanılarak kolayca aldatılabilir.

Çizelge 2. Mobil Parmak İzi Tanıma Üzerine Yapılan Akademik Çalışmaların Yöntem, Metrik Değerleri ve Kullanılan Teknolojilere Göre Sınıflandırılması (Classification of academic studies on mobile fingerprint recoginition based on utilized methods,metrics and technologies)

| Kaynak | Algoritmalar/ Metotlar | Başarı Kriterleri | Teknolojiler / Donanımlar |
|---|---|---|---|
| [11] | • Parmak izi tanıma sürecinde Luo ve Chen' in metotları | • EER- %4,16<br>• FNMR- %5,85<br>• FMR- %1 | • Parmak izi yakalamak için AT77C101B<br>• Arm-Core Processor LPC2106 ile parmak izini yakalayıp yakalamadığı kontrolü<br>• Bird Smart Phone E868 mobil cihaz |
| [12] | • FingerprintUser Interface (FpUI) | • Özellik eşleşimi- 0,03 sn<br>• Görüntü yakalama 2 sn<br>• Elde edilen bu değerler FRR ve FAR değerlerine uygundur. | • IC Card<br>• Pocket-PID |
| [13] | • Local Binary Pattern (LBP) | • EER- % 0,081 | • VGN-UX17LP SONY<br>• QuickCam Logitec Camera<br>• Infra-red Illuminators (NIR)<br>• Charge Coupled Device (CCD) |
| [14] | • Transient Evoked Otoacoustic Emission (TEOAE)<br>• Autoencoder Neural Network<br>• Continuous wavelet transform (CWT) | • EER- %2,41 | - |
| [15] | • Discrete Fourier Transform (DFT)<br>• OpenCL 1.1<br>• Android Native Development Kit (NDK) | • Ortalama Zaman-107,07<br>• Ortalama Güç-1217,13<br>• Ortalama Enerji-137,27 | • Google Nexus 4 Smartphone |

Mobil biyometrik yöntemlerden ses analizine dayalı tanıma işleminde HMMs, MFCC, GMM ve SVM modelleri kullanılmaktadır. Mobil ses tanıma işleminde Kounoudes ve arkadaşlarının [17] kullandığı HMMs (Hidden Markov models- Gizli Markov Modeli) istatistiksel bir tekniktir. Bu teknik ile kişinin nasıl ses ürettiğine dair istatistiksel bir model oluşturulur. Ses tanıma yönteminde, kişi tarafından oluşturulan ses dalgaları, ses vektörlerine dönüştürülmektedir. Bu diziler Markov modeli ile işleme sürecine girmektedir. Markov modeli sonlu bir grafa benzetilebilir. Bu graf modeli her hangi bir konumda iken belirli rastlantısal dağılımlara bağlı olarak konumunu koruyabilir veya farklı konuma geçebilir. Ortaya çıkan bu rastlantısal

durumlar incelenerek tanıma işlemi gerçekleşir. HMMS modelinde durum dizisine erişebilmek için İleri, Viterbi ve Baum-Welch algoritmaları kullanılmaktadır [52].

Chen ve Huang [16], Marcel ve arkadaşları [20], Khoury ve arkadaşlarının [22] kullandığı GMM (Gaussian Mixture Model- Gauss Karışım Modeli) , birden fazla gauss yoğunluk eşitlikleriyle kişiye ait ses bilgisinden elde edilen öznitelik vektörünün işlenip, vektörlerinden kişinin akustik niteliklerini temsil eden olasılık yoğunluk fonksiyonunun bulunması prensibine göre çalışmaktadır [53]. GMM sayesinde elde edilen yoğunluk değeri, örnek sayısı artırılarak daha yüksek hassasiyet değerine eriştirilebilir [54].

Çizelge 3. Mobil Sistemlerde Ses Tanıma Üzerine Yapılan Akademik Çalışmaların Yöntem, Metrik Değerleri, Kullanılan Teknolojiler ve Uygulama Alanlarına Göre Sınıflandırılması (Classification of academic studies on mobile speech recoginition based on utilized methods,metrics and technologies)

| Kaynak | Algoritmalar/ Metotlar | Başarı Kriterleri | Teknolojiler / Donanımlar | Kullanıldığı Alanlar |
|---|---|---|---|---|
| [16] | • SD (Spectral Dimension)<br>• MFCC (Mel Frequency Cepstral Coefficients)<br>• GMM (Gaussian Mixture Models) | - | - | • Mobil cihazlarda arayan kişileri seslerinden tanıma |
| [17] | • MFCC (Mel Frequency Cepstral Coefficients)<br>• HMMS (Hidden Markov Models) | • EER- %5 | - | • Çevrimiçi Bankacılık<br>• E-Ticaret<br>• Göçmenlik İşlemleri<br>• Vatandaşlık Hizmetleri<br>• Askeri Hizmetler (Ordu, Donanma)<br>• Sağlık Kuruluşları ve Organizsyonları |
| [18] | • Non-Intrusive and Continuous Authentication (NICA) | • Kullanıcıların %92 daha güvenli oturum erişimi | • Samsung Q45<br>• Sony Vaio UX1<br>• HPMini-Note 2133 | • Hassas Hizmetler ve Bilgiler<br>• Otomatik Erişim Sistemleri |
| [19] | • Automatic Speech Recognition (ASR)<br>• Support vector machine (SVM)<br>• Minimum classification error (MCE) training | • EER -%0,31 | • iPAQ handheld | • Kişisel Bilgi Güvenliği |
| [20] | • Local Binary Patterns<br>• MFCC<br>• GMM<br>• UBM(Universal Backround Model) | - | • Nokia N900 | - |
| [21] | • Universal Backround Model<br>• Probablistic Linear Discriminant Analysis<br>• LBPs (Local Binary Patterns)<br>• MCT (Modified Census Transform) | EER- %18 bay %15,1 bayan | • Nokia N93i | - |
| [22] | • Gaussian Mixture Model | EER-%6,3 bayan %1,9 bayan | - | • Kişisel Bilgi Güvenliği |

Hazen ve arkadaşlarının [19] uyguladığı SVM (Support Vector Machine- Destek Vektör Makinesi) modelinde pozitif ve negatif örnekler mevcuttur. Bilinen bu örneklerle uzay ikiye bölünür ve en iyi hiper-düzlem bulunmaya çalışılır. Bilinen bu pozitif ve negatif örnekler arasındaki mesafeyi en uzak yapan destek vektörleri ile sınıflandırma işlemi yapılır. SVM önceden var olan örneklere göre, yeni durumunun belirli bir sınıfta olmasını belirleme sürecidir [55].

Kounoudes ve arkadaşları [17] ile Marcel ve arkadaşlarının [20] kullandıkları MFCC (Mel Frequency Cepstral Coefficient-Mel-Frequency Cepstrum Katsayıları), algı temelli sesi temsil eden katsayılardır. İnsan kulağı ses frekanslarını doğrusal olmayan bir formda algılar. Yapılan araştırmalar ses frekansının 1 kHz'e kadar doğrusal, daha yüksek frekans değerlerinde ise logaritmik olarak arttığını göstermektedir [56]. İnsan kulağının algılayabildiği frekans değerini Mel Ölçütü sınıflandırmaktadır. Bu ölçüt, Band Geçiren Filtre (band pass filter) olarak kullanılır. Öznitelik aşamasında, Ters Fourier Transformasyonu ve frekans uzayından tekrar zaman uzayına döndürülme işlemine tabi tutulur. Bu işlemin sonucu olarak MFCC elde edilir [57].

### 3.1.3. İris Tanıma (Iris Recognition)

Gözde bulunan iris tabakası insandan insana farklılık gösteren bir yapıdır. İris kişinin hayatı boyunca değişmeden kalan karakteristik bir özellik olduğundan biyometrik sistemlerde ayırt edici bir özellik olarak kullanılmaktadır.1985 yılında Flom ve Safir tüm irislerin eşsiz olduğunu ispatlayarak 1987 iris tanıma ile ilgili patent almışlardır [58]. Bu yöntem gözün rengini veren kısım ve kaslardan oluşan tabakanın görüntüsünün kopyalanarak bir takım görüntü işleme tekniklerinin uygulanması ilkesi ile çalışır. Alınan görüntüden tanıma işlemini doğru gerçekleştirebilecek

sayıda örnek referans noktası alınır ve depolanır. Bu işlem sırasında yüksek çözünürlük değerine sahip sensörler iris tabakası üzerindeki farklılıkları taramaya yönelik çalışır. Sonraki işlemde alınan örnekle mevcut olarak taranan iris karşılaştırma işlemine sokulur [59].

Mobil biyometrik sistemlerde kullanılan iris tanıma yöntemi en yüksek başarıyı elde etmektedir. İris tanıma yönteminin avantajları ve dezavantajları aşağıda belirtilmiştir [58] [59]. Bunlar:

- İris vücutta zor zarar görebilecek bir organdır.
- Yüz, retina vb. tanıma sistemlerinde tek yumurta ikizlerinde fark ayırt edilemezken iris tabakası bu konuda ayrımı sağlayabilecek bir özelliktir. Yani iris dokusu tamamen kişiye özel bir yapıdadır.
- Doğumdan sonra oluşan iris yapısı dıştan bir etkiye maruz kalmadığı sürece değişiklik göstermez.
- Yüksek çözünürlüklü iris resimleri ve üzerine iris deseni basılmış lensler ile var olan sistemleri aşmak mümkün olabilir.
- Bu sistemlerin işleyişi sırasında göz her daim aynı açı ile bakmayacaktır. Veri depolama sürecindeki bakış yönündeki açı değişikliği sebebiyle tanıma işlemi sırasında sorun yaşanabilir. Bu da sistemin dezavantajı olarak görülmektedir.
- İris tanıma işleminde parametrelerin ölçümü için örnek alınırken direkt olarak temas sağlanamaz. Fiziksel temasın sağlanamaması sebebiyle alınan örneklerde yanlışlık olabilir.

İris taramada karşılaştırma için kullanılan referans noktası parmak izi sistemlerindeki karşılaştırma noktasına göre çok fazla sayıdadır. Bu da ölçüm hassasiyetini arttırmaktadır. Bunun dışında irisin bireyde eşsiz oluşu sebebiyle, güvenlik kriteri bakımından hassas olan çevrimiçi bankacılık işlemleri,

Çizelge 4. Mobil Sistemlerde İris Tanıma Üzerine Yapılan Akademik Çalışmaların Yöntem, Metrik Değerleri, Kullanılan Teknolojiler ve Uygulama Alanlarına Göre Sınıflandırılması (Classification of academic studies on mobile iris recoginition based on utilized methods,metrics and technologies)

| Kaynak | Algoritmalar/ Metotlar | Başarı Kriterleri | Teknolojiler / Donanım | Kullanıldığı Alanlar |
|---|---|---|---|---|
| [23] | • BHC encoder Fuzzy Vault Encoder | • Gözlüksüz ve lenssiz %99,5<br>• Gözlüklü ve lensli %99<br>• Genel ortalama %98 | • Panasonic BM ET100US iris tanıma cihazı<br>• Samsung SPH-2300 | - |
| [24] | • Kendi yöntemlerini geliştirmişler ve mevcut yöntemlerle kıyaslamışlar. | - | • IR-LED (Infrared Light Emitting Diode)<br>• Samsung SPH-2300 | • Banka İşlem Hizmeti<br>• Telefon Güvenliği |
| [25] | • Circular edge detection Hough Transform Specular reflection | - | • Samsung SPH-s2300 | • Yüksek güvenlik girişi gerektiren sistemler<br>• Bankacılık işlemleri<br>• Güvenli oturum oluşturma |
| [26] | • AGF (Adaptive Gabor Filter)<br>• IR Pass Filter and Illiminator<br>• ICA<br>• HD (Hamming Distance) | • EER-%0,14 | • Xenon Flash Lamp<br>• SPH-S2300 Samsung | • Erişim Kontrolü<br>• Banka İşlem Hizmeti |
| [27] | • SRs<br>• Adabost Eye Dedector<br>• IR Pass Filter and Illiminator | • EER-%0,05 | • Quickcam Pro-4000 CCD camera<br>• AlphaCam-I CMOS camera<br>• SPH-S2300 Samsung | • Trafik Kontrol ve Takip Hizmetş<br>• Mobil Bankacılık Uygulamaları |
| [28] | • Local Binary Patterns<br>• Linear SVM<br>• Gabor Filter | - | • Asus Transformer Pad TF300T (andriod)<br>• Samsung Galaxy S4<br>• iPhone 5 | • e-Ticaret<br>• e-Sağlık<br>• Çevrimiçi Bankacılık |
| [29] | • Circular Hough Transform<br>• Gabor Filter | • EER-% 3,5 | - | • e-Alışveriş<br>• Güvenli Web Oturumu |
| [30] | • IR Illiminator ve IR Pass Filter<br>• Haar Detection<br>• Viola Jones Algorithm<br>• CSUM<br>• Java Native Interface (JVI) | • FAR-%0,15 | • Samsung Galaxy Tab 2.0 | • Ordu Güvenliği<br>• Güvenli Erişim<br>• Sağlık Kayıtları<br>• Bankacılık İşlemleri |
| [31] | • Gaussian Filter<br>• Canny Filter | - | • Samsung Galaxy Tablet<br>• iPhone 5<br>• Samsung Galaxy S4 | - |

- Tanıma işlemi gerçekleşmesi için alınan örnek resim yüksek görüntü kalitesine sahip ve iyi çözünürlük değerine sahip olmalıdır.

telefon güvenliği, uzaktan erişim kontrolü, güvenli oturum oluşturma, yüksek güvenlik girişi gerektiren sistemler, çevrimiçi sağlık sistemleri, çevrimiçi alışveriş, askeri güvenlik ve sağlık kayıtları gibi alanlarda kullanım yeri elde etmektedir [24] [27] [28] [30]. Mobil iris tanıma üzerine yapılmış çalışmalar Tablo 4'de listelenmektedir.

Mobil cihazlar üzerinde uygulanan iris tanıma sistemleri genel olarak aynı mantıkla çalışmaktadır. İlk önce mobil cihazın kamerası veya cihaz kamerası yetersiz çözünürlük kalitesine sahipse harici bir görüntü yakalama ekipmanı kullanılarak, gözün iris kısmına ait siyah beyaz formatta bir resim çekilir. Bu resim kızılötesi aydınlatıcısı (IR Illiminator) ve kızılötesi filtreleme (IR Pass Filter) teknikleri ile elde edilir [26] [30]. İşlenen fotoğrafta iris haricindeki kısımlar, veritabanında aşırı yüklenme olmaması adına çıkartılarak gerekli kısımların kayıt işlemi gerçekleşir. İris tabakasına ait resimden DNA koduna benzeyen bir kod dizisi üretilir ve üretilen bu kod veritabanında saklanır.

İris tanıma işlemi kaydedilen resim analizine dayalı bir yöntem olması sebebiyle filtreleme, yapay sinir ağları ve istatistiksel algoritmaların birçoğu ile beraber kullanılabilir. Fakat kullanılan bu tekniklerden farklı çalışma mekanizmasına sahip Haar-Benzeri Öznitelik Çıkarımı (Haar-like Features) iris tanıma uygulamalarında yaygın olarak kullanılmaktadır [27] [30]. Haar benzeri öznitelik çıkarımı, çalışmanın yüz tanıma yöntemleri kısmında ayrıntılı olarak açıklanmaktadır.

### 3.1.4. Yüz Tanıma (Face Recognition)

Biyometrik sistemlerin uygulama alanlarına bakarak, en yaygın biyometrik tekniğin parmak izi gösterilmesine karşın, mobil cihazlarda uygulanabilirliği açısından parmak izinin kullanımı için alternatif özel sensörlü donanımlar gerekmektedir. Bu sebeple yüz tanıma sistemleri neredeyse her mobil cihazda kamera bulunması sebebiyle, mobil ortamlarda daha yaygın olarak kullanılan sistemler haline dönüşmüştür. Mobil yüz tanıma üzerine yapılmış çalışmalar Tablo 5'de listelenmektedir.

Yüz tanıma probleminde iki temel yöntem bulunmaktadır. Birinci yöntem temel bileşen analizi olarak adlandırılır. Bu yaklaşımda, bir yüzü en iyi tanımlayan en yakın bilgi tüm yüz görüntüsünden elde edilir [62]. İkinci yöntem bir yüzün gözler, burun, ağız ve çene gibi temel kısımlarından öz nitelik vektörleri çıkarmaya dayalıdır [61]. Bu yöntemde biçim değiştirebilen şablonlar ve geniş matematik yardımıyla bir yüzün temel kısımlarından önemli bilgiler toplanır ve sonra bir öz nitelik vektörüne dönüştürülür [61]. Yüz tanıma işleminde kullanılan en çok bilinen algoritmalar aşağıda sıralanmıştır [60] [61] [62]:

- Temel Bileşenler Analizi (Principal Component Analysis)
- Bağımsız Bileşenler Analizi (Independent Component Analysis)
- Doğrusal Diskriminant Analizi (Linear Discriminant Analysis)
- Evrimsel Takip (Evolutionary Pursuit)
- Elastik Demet Grafik İşleme (Elastic Bunch Graph Matching)
- Kernel Yöntemi (Kernel Methods)
- İz Dönüşümü (Trace Transform)
- Aktif Görünüm Modeli (Active Appearance Model)
- 3 Boyutlu Model Dönüştürme (3-D Morphable

Çizelge 5. Mobil Yüz Tanıma Üzerine Yapılan Akademik Çalışmaların Yöntem, Metrik Değerleri, Kullanılan Teknolojiler ve Uygulama Alanlarına Göre Sınıflandırılması (Classification of academic studies on mobile face recoginition based on utilized methods,metrics and technologies)

| Kaynak | Algoritmalar/ Methodlar | Başarı Kriterleri | Teknolojiler / Donanımlar | Kullanıldığı Alanlar |
|---|---|---|---|---|
| [32] | • Hidden Markov Models<br>Score fusion<br>Fisher Discriminant Ratio (FDR) | • EER- Equal Error Rate %4 | • NIR (NearInfra-Red) light | • e-Ticaret<br>• Erişim Kontrolü |
| [33] | • OKAO Vision | • Threshold- 0,2 | • Symbian OS<br>Embedded Linux<br>ITRON<br>BREW | • Borç Ödeme İşlemleri<br>• Kişisel Bilgi Güvenliği |
| [20] | • Local Binary Patterns<br>• MFCC<br>GMM<br>UBM (Universal Backround Model) | - | • Nokia N900 mobile device linux işletim sistemli | - |
| [34] | • KNN<br>Fisher Classifier<br>Gaussian Classifier | • %5,09 | • Hp iPAQ rw6100 | - |
| [35] | • SVM<br>Ada Boosting | • Modül işlemi tamamlama süresü- 1,4 sn<br>• Threshold- 0,28 | • Symbian OS 60 Series<br>Nokia 6680 | • Telefon Güvenliği |
| [36] | • Haarlike Features<br>• AdaBoost<br>• Local Binary Patterns | - | • Nokia N90 | • Çevrimiçi Bankacılık |
| [30] | • IR Illiminator ve IR Pass Filter<br>• Haar Detection<br>• Viola Jones Algorithm<br>• CSUM<br>• Java Native Interface (JVI) | • FAR-%0,01 | • Samsung Galaxy Tab 2,0 | • Askeri Hizmetler (ordu)<br>• Erişim Kontrolü<br>• Sağlık Kayıtları<br>• Bankacılık İşlemleri |

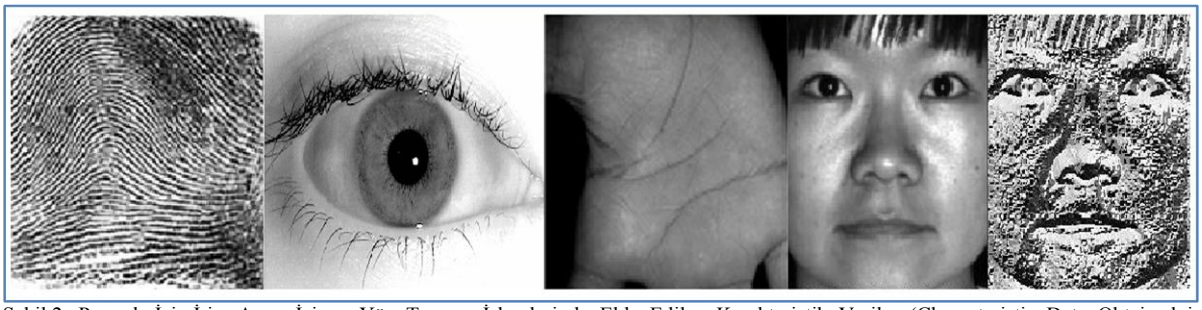
Model)

- 3 boyutlu yüz eşleştirme (3-D Face Recognition)
- Hidden Markov Model (HMM)

Yüz tanıma sürecinde yapılacak ilk işlem yüze ait resimlerden ayırt edici çeşitli özelliklerin ayrılması işlemidir. Bu işlemin yapılma sebebi aynı kişiye ait yüz resimlerinin özelliklerinin benzer, farklı kişilerin yüzüne ait resimlerin ise farklı özelliklere sahip olmasıdır. Bugüne kadar yapılan çalışmalarda yer alan yüz tanıma tekniklerini 2 gruba ayırmak mümkündür. Bu gruplar [61]:

- Geometrik özellik tabanlı, şablon eşlemeli, elastik demet grafı eşleme, yapısal eşleme, gizli Markov model ve dalgacık dönüşüm tabanlı tekniklerin gruplandırıldığı Özellik Kaynaklı Yüz Tanıma teknikleridir.
- Özyüz yaklaşımı ile yüz tanıma, Fisher yüz yaklaşımı ile yüz tanıma ve yapay sinir ağı tabanlı yöntemler Görünüm Tabanlı Yüz Tanıma sistemleridir.

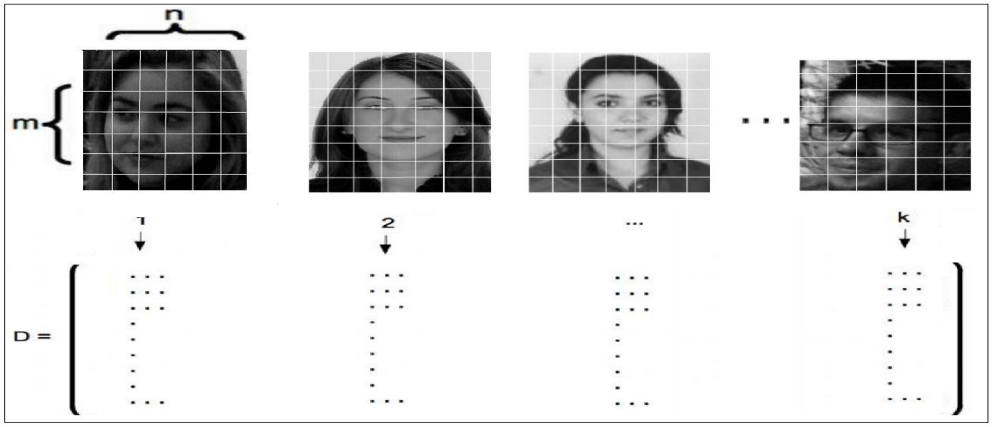
Mobil yüz tanıma teknikleri arasında en çok kullanılanı Haar benzeri özellikler ve özyüzler yöntemleridir. Kameradan alınan görüntülerde yalnızca bireyin yüzü olmayacaktır. Tanıma işlemi için gereken yüz resmi incelendiğinde, resmin burun, göz, kaş, ağız gibi bölümleri renk olarak yüzün geri kalanına göre göre farklılık göstermektedir. Viola ve Jones [32] tarafından geliştirilen Haar benzeri özellik çıkarım yöntemiyle yüzün bu bölgeleri tespit edilir. Yüz resmi çok küçük alt parçalara bölünür. Elde edilen bu küçük dikdörtgen parçalarda piksel yoğunluklarını hesaplanır, komşu bölgelerle arasındaki farklar hesaplanır. Bu sayede görüntüde gölgede kalan kısımlar hesaplanır. Buna göre gözlerin veya burnun kenar kısımları gölgelenmeden dolayı kolay kalacaktır ve bu bölgeler tespit edilecektir [63].



Şekil 2. Parmak İzi, İris, Avuç İzi ve Yüz Tanıma İşlemlerinde Elde Edilen Karakteristik Veriler (Characteristic Data Obtained in Face,Fingerprint, Iris and Palmprint Recognition Process)

Mobil cihazlarda görünüm tabanlı yüz tanıma tekniklerinden en sık kullanılanı ise özyüzler yöntemidir [64]. Yüz tanımada ayırt edebilme işlemini yapabilmek için yüz üzerinde belirleyici noktalar seçilmektedir. Bu noktalar uygulama geliştirici tarafından seçilebilir veya özyüzler yöntemi ile temel bileşenler analizi kullanılarak uygulamanın kendisi bu noktaları belirleyebilir. Her bireyin gri renkte, aynı boy ve en oranına sahip görüntüleri vektörlere dönüştürülür. Bireydeki belirleyici olarak düşünülen karakteristik özellikler dizilere aktarılmaktadır. Birden fazla bireyin mevcut olduğu durumda her birey birer sütunlara karakteristik özellikler ise satırlara yerleşecek biçimde bir matris oluşturulmaktadır. Şekil 2'de bu matrise bir örnek gösterilmiştir.

Yüz tanıma sistemleri uygulama alanı, doğruluk değeri ve uygulanışı yönüyle değerlendirildiğinde avantaj ve dezavantajları mevcuttur [65]. Bunlar:




Şekil 3. Özyüzler Matrisi Oluşturumu (Creating an EigenFaces Matrix)

- İnsan yüzü her bireyde farklıdır. Bu sebeple tanıma sistemlerinde kullanılan bir özelliktir.
- Parmak izi gibi kolay taklit edilememektir.

- Tanıma sistemini işletebilmek için alınan parametreler basit bir kamera kullanılarak elde edilebilmektedir.
- Uygulanması, kullanılan algoritmalar ve analiz yöntemleri diğer yöntemlere göre oldukça zordur.
- Alınan görüntü örnekleri ortam koşullarından çok fazla etkilenmektedir.
- Yüzün tamamı her kontrol işleminde karşılaştırılmaz. Alınan belirli parametreler doğrultusunda kontrole tabi tutulur. Bu sebeple bireyin yüzündeki mimik değişikliği, yara, iz veya estetik sebebiyle yanlış sonuçlar elde edilebilir.

### 3.1.5. Avuç İzi Tanıma (Palm Print Recognition)

Mobil biyometrik tanıma yöntemlerinde avuç izi kullanımı çok yaygın olmamakla birlikte kullanılmaktadır. Bunun sebebi parmak izi tanıma sistemlerinde de olduğu gibi mobil cihaza harici bir donanım eklenmeden bu tanıma işleminin gerçekleşememesidir. Mobil cihaza entegre edilen donanımlar sayesinde avuç içine ait görüntü mobil cihaza aktarılır ve görüntü işleme teknikleri ile elde edilen veri sayısal formata dönüştürülür [66].

Avuç izi tanıması, çalışma prensibi olarak parmak izi tanıma işlemi ile aynı basamaklara sahiptir. Bu iki karakteristik özellik de uygulandığı bölgede yer alan çizgilerin analizine dayanarak çalışmaktadır. Parmak izinde de olduğu gibi avuç içi izi tanınması ve doğrulanması ayırt edici özelliğe sahip öznitelik noktalarının tespitine dayanmaktadır. Fakat avuç içinde yer alan çizgiler daha kalın ve belirgin olduklarından parmak izindeki gibi yüksek çözünürlüğe sahip bir görüntüye ihtiyaç olmadan da tespit edilebilmektedir [66].

Avuç izi tanıma tekniklerinde öznitelik ve işlenmemiş görüntü tabanlı olmak üzere iki farklı yaklaşım mevcuttur. İşlenmemiş görüntüye dayalı analizde avuç izi görüntüsünden direkt olarak elde edilen veriler doğrultusunda tanıma işlemi gerçekleşmektedir. Öznitelik tabanlı yaklaşımda ise avuç içi bölgesinde tanıma için kullanılacak çalışma bölgesi verisi çıkartılarak, tanıma işlemi bu alan üzerinden yapılmaktadır [38]. Mobil avuç izi tanıma üzerine yapılmış çalışmalar Tablo 6'da listelenmektedir.

Avuç izi tanıma sistemlerinde yapay sinir ağları, KNN ve Dalgacık Analizi en sık kullanılan tekniklerdir [39],[40],[67].

Son olarak Şekil 1'de verilen fiziksel ve davranışsal özelliklerle ilgili literatürde yeteri kadar kaynak bulunmadığından burada yorumlanamamıştır.

## 3.2. Sektörel Çalışmalar

### 3.2.1. MOBIO

MOBIO mobil biyometri konsepti ile yeni mobil hizmetler geliştirmektedir. Aydınlanmaya karşı dayanıklı yüz tanıma sistemi, gürültüye dayanıklı ses tanıma sistemi, uygulama modeli adaptasyon ve ölçeklenebilirlik, çoklu biyometrik tanıma gibi bilimsel ve teknik hedefler alanında hizmet vermektedir. MOBIO mobil cihazlar dâhil olmak üzere birçok yenilikçi yönleri ele almaktadır. Bu alanlar [68]:

- Geliştirilen yeni istatistiksel yöntemler sayesinde, ileri düzey teknolojiler bi-modal olarak adlandırılan çoklu biyometrik yöntemlerle birleştirmeyi amaçlamaktadır.
- Biyometrik tanıma modellerinin zamanla tanıma oranlarındaki azalmayı giderebilmek için modellerin yeni versiyonlara uyarlanmasını sağlamaktadır.
- Kullanılan model üzerinde teknik incelemeler yaparak sistem performansı ve işlem gücünü analiz ederek kullanım alanlarına göre biyometrik tanıma sistemlerini düzenlemektedir.
- Geliştirilen teknolojileri değerlendirmek ve karşılaştırmak amacıyla araştırma topluluklarının

Çizelge 6. Mobil Sstemlerde Avuç İzi Tanıma Üzerine Yapılan Akademik Çalışmaların Yöntem, Metrik Değerleri, Kullanılan Teknolojiler ve Uygulama Alanlarına Göre Sınıflandırılması (Classification of academic studies on mobile palmprint recoginition based on utilized methods,metrics and technologies)

| Kaynak | Algoritmalar/ Metotlar | Başarı Kriterleri | Teknolojiler / Donanımlar | Kullanıldığı Alanlar |
|---|---|---|---|---|
| [37] | • Gaussian Filtreleme | • EER- %2,04 | • Motorola Droid X | - |
| [38] | • ROI (region of interest) | • Threshold seviyesi 0,46<br>• ROI çıkarımı 0,433 sn<br>• Kodun çalışması 0,116 sn<br>• Hızlandırılmış eşleştirme 5msn | • I- Phone 4 | - |
| [39] | • Probablistic Hough Transform<br>• Speeded Up Robust Features<br>• Hough Transform<br>• Eigenpalms<br>• KNN | • FAR= %3,4<br>• FRR= %1,7 | • Canon<br>• HTC<br>• Motorola | • Uzaktan Erişim<br>• Doğrulama Sistemi |
| [40] | • Orthogonal Line Ordinal Feature<br>• 2D Gaussian Filter | • Fusion Code EER=% 0,21<br>• Competitive Code EER=% 0,06<br>• Ordinal Code EER=% 0,07<br>• Sum Difference Ordinal Code EER=% 0,07 | • HP iPAQ<br>• HP rx3715 | • Mobil Bankacılık<br>• Mobil Ticaret<br>• Mobil Ofis Sistemleri<br>• Mobil Eğlence |

ortak değerlendirme araçları kullanarak sistemin çalışması üzerine sonuçlar elde edebilmektedir.

#### 3.2.2. Biyometrik Değerlendirme ve Test Projesi (Biometrics Evaluation and Testing - BEAT)

BEAT projesi, Avrupa Birliği tarafından desteklenen teknolojik gelişmeler ve sonuçlarının sergilenmesi üzerine yapılmış bir çalışmadır. BEAT'in amacı biyometrik teknolojiler için standart operasyonel değerlendirme çerçeveleri önermektir [69]. Buna ulaşmak amacıyla [69];

- Biyometrik sistemlerin geçerli kıstaslarla değerlendirilmesi için şeffaf ve bağımsız bir şekilde çevrimiçi ve açık bir platform geliştirilmekte,
- Zafiyet analizi için protokoller ve araçlar tasarlanmakta,
- Genel kriter değerlendirmeleri için standardizasyon belgeleri hazırlanmaktadır.

Bu projede üç çıktının olması beklenmektedir. İlk olarak biyometrik sistemlerin güvenirliliği ölçülebilir olacak ve bu durum performansta anlamlı bir artış görülmesini sağlayacaktır. Bu alanda yapılan araştırmalar sonucu elde edilen veriler ve geliştirilen teknikler, sektör çalışmalarına transfer edilerek birbirleriyle uyum içerisinde çalışan bir çatı oluşturmak amaçlanmıştır. Sonuçlar standartlar üzerinde etki göstermeye başladıkça karar mercileri ve yetkili kişiler biyometri alanındaki gelişmeler konusunda bilgilendirilecektir [69].

#### 3.2.3. OKAO

Yüz yüze iletişimde görsel bilgi önemli bir rol oynamaktadır. Geliştirilen cihazda tanıma işlemi, insan algılaması seviyesindeki kadar hassas olduğu takdirde tanıma süreci çok rahat olacaktır. Japoncada yüz görme anlamına gelen "OKAO" biyometrik sistem geliştirme ortamıdır. OKAO biyometrik tanıma sistemlerini teknolojik gelişimlerle birleştirip bir üst seviyeye taşıyarak akıllı sistemler tasarlamıştır. Güvenlik bakımından hassas olan merkezlerde giriş çıkış işlemleri için ta tasarlanmış özel tanıma hizmetleri, hasta takip sistemleri, uzaktan takip sistemleri için elektronik bileşenler üretimini sağlamaktadır [70].

## 4. SONUÇ VE ÇIKARIMLAR (RESULTS AND CONCLUSIONS)

Bu çalışma; mobil cihazlarla birlikte çalışabilen biyometrik sistemler, kullanılan teknikler ve uygulama alanları üzerine odaklanmıştır. Mobil cihazlar, insan tanımlama ve kimlik doğrulama gibi geleneksel biyometrik arenalarda başarılı çözümler sunmaktadır. Yapılan çalışmada biyometrik sistemler ve mobil ortamda kullanılan biyometrik yöntemler, uygulama için teknik ve sistem gereksinimleri incelenmiştir.

Literatür çalışması esnasında, yapılan uygulamalar incelendiğinde:

- Bu makale kapsamında incelenen literatürde, mobil cihazlarda harici donanım entegresi olmadan çalışabilen, mobil cihaz kamerası aracılığı ile elde edilen görüntüden tanıma işlemi yapılan yüz ve iris tanıma tekniklerinin en yüksek kullanım oranlarına sahip oldukları görülmüştür.
- İncelenen çalışmalarda, geliştirilen mobil biyometrik tanıma sistemlerinde doğrulama işlemini gerçekleştirebilmek için birden fazla biyometrik karakteristik özelliğin bir arada kullanıldığı görülmüştür.
- Tercih edilme oranına bakarak değerlendirildiğinde, parmak izine dayalı tanıma sistemleri biyometrik yöntemler içinde en yaygın kullanım alanına sahip olmasına rağmen, mobil cihazlarda bu yöntemin, harici donanım gerektirdiği için geniş kullanım alanına sahip olmadığı yapılan literatür çalışması sonucu tespit edilmiştir.
- Mobil cihazlarda uygulama performansı, cihaz kapasitesi, mobil uygulama geliştirme süreci, hız dezavantaj olarak görülmektedir. Fakat bunun yanı sıra yerleşik çalışan, büyük ve taşınabilir özelliği olmayan sistemlerle kıyaslandığında, bahsettiğimiz dezavantajlar göz ardı edilebilmektedir.
- Mobil cihazlarda kişisel birçok bilginin yer aldığı, bu bilgilerin özel olduğu ve korunması gerektiği düşünülen bir ortamda, güvenlik katsayısını artıracak düzeydeki uygulamaların talep göreceği düşünülmektedir.
- Güvenlik düzeyini arttırmak isteyen kurumsal kullanıcıların, mobil platform üzerinde uygulanan biyometrik yöntemleri tercih etmeleri yeni fırsatları da beraberinde getirmektedir.

Bugüne kadar yapılan uygulamaların incelenmesi sonucu belirlenen problemler ve bu problemlere getirilen çözüm önerileri tespit edilmiştir [15]-[40]. Bu başlıklar:

- Mobil cihazlarda elde edilen düşük kalitedeki görüntü sebebiyle, yüksek hassasiyet gerektiren iris, retina gibi ayırt ediciliği yüksek tanıma sistemleri için kullanım güçleşmiştir. Bu sebeple görüntü kalitesini arttırmak amacıyla harici kameralar entegre edilerek elde edilen görüntü kalitesi artırılmıştır. Günümüz telefonlarında bu hususun azaldığı değerlendirilmektedir.
- Mobil cihazların karmaşık biyometrik sistem altyapılarına kıyasla sahip olduğu sınırlı işlem gücü ve sınırlı hafızası sebebiyle, uygulama sürecindeki performans düşüklüğünü gidermek için, karmaşık işlemler mobil cihazlar yerine sunucu görevi üstlenen bilgisayarlar üzerinde yapılarak, mobil cihazlar sadece "uzaktan kontrol" işlevini yerine getirmiştir. Bu yöntemle mobil cihaz üzerine düşen yük miktarı azaltılarak performans kriterinde artış elde edilmiştir. 3G'nin yanında 4G'ninde bugünlerde hizmete girmeye başlayacağı değerlendirildiğinde, performansın daha da artacağı düşünülmektedir.
- Mobil cihazlarda görülen bir başka sorun ise yöntem çeşitliliğidir. Mobil cihazlarda kamera ile tanıma

işlemi yapan yüz, iris, retina vb. biyometrik tanıma işlemlerini sağlayacak uygulamalar geliştirilebilirken parmak izi gibi yöntemler harici donanımlar takılmadan gerçekleşmeyebilir. Bu sebeple biyometrik sisteme uygun donanımsal eklemeler yaparak mobil cihazlarda kullanılan farklı biyometrik tekniklerin geliştirilebileceği düşünülmektedir.

- Mobil ortamlarda yaşanan sıkıntılar haricinde problemlerle de karşılaşılmaktadır. Biyometrik sistemlerde kullanılan karakteristik özelliklerle de alakalı sorunlar mevcuttur. El damar ağı, ses gibi tanıma sistemleri aldatılması kolay yöntemler olduğundan güvenlik tehdidi oluşturur. Bu sebeple bu karakteristik özellikler çok sayıda kişinin kullanacağı alanlarda kullanılmamaktadır. Bunun dışında iris, retina gibi karakteristik özelliklerde kullanılan görüntü yüksek çözünürlüğe sahip olmadığından etkin sonuç veremeyebilir ya da parmak izi kopyalama veya işlenmiş lens yöntemleri ile uygulamalar yanıltılabileceğinden bunlara çözümler geliştirilmektedir.

Mobil cihazlarda görüntü veya video işleme işlemleri yapılabilmektedir. Fakat bu cihazların, karmaşık biyometrik sistem altyapılarına kıyasla sahip olduğu sınırlı işlem gücü ve sınırlı hafızası sebebiyle, uygulama sürecindeki performans düşüklüğü görülmektedir [38].

Bu tez çalışmasında yapılan tespitler, sunulan tablolar, tartışılan hususlar, önerilen konular genel olarak değerlendirildiğinde, biyometrik sistemlerin mobil cihazlar üzerinde son yıllarda daha çok kullanılmaya başlandığı, bundan sonraki süreçlerde uygulamaların daha da artacağı görülmektedir.

Yapılan bu çalışmanın bundan sonra, mobil ortamlarda yapılacak olan çalışmaların artışına ve yeni yöntemlerin geliştirilmesine katkılar sağlayacağı değerlendirilmektedir. Tespit edilen bu başlıklar, geliştirilecek uygulamalarda tercih edilmesi, dikkat edilmesi ve iyileştirilmesi gereken unsurları ortaya koymuştur.

## **KAYNAKLAR** (REFERENCES)


[1] İnternet: Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2015). Mobil telefon abone sayısı 72 milyona yaklaştı. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.udhb.gov.tr%2Fhaber-64-mobil-telefon-abone-sayisi-72-milyonayaklasti.html&date=2015-03-21,Son Erişim Tarihi: 21.03.2015.

[2] Clarke, N., Furnell, S. Authentication of users on mobile telephones - A survey of attitudes and practices. ***Computers & Security***, 24(7): 519-527, (2005).

[3] Çınar S. Mobil Android Ortamında Parmak İzi Tanıma ve Kimlik Doğrulama Sisteminin Geliştirilmesi, ***Yüksek Lisans Tezi***, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 13, (2014).

[4] Khan, S., Akbar, M., Shahzad, F., Farooq, M., Khan, Z. Secure biometric template generation for multi-factor authentication. ***Pattern Recognition***, 48(2): 458-472, (2015).

[5] Luis-Garcia, R., Alberola-Lopez, C., Aghzout, O., Ruiz-Alzola, J. Biometric identication systems. ***Signal Processing***, 83(2): 2539-2557, (2003).

[6] Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., Khan, Z. Secure biometric template generation for multi-factor authentication. ***Pattern Recognition***, 48(2): 458-472, (2015).

[7] Filiz S. Siber Güvenlikte Biyometrik Sistemler ve Yüz Tanıma, ***Yüksek Lisans Tezi***, Gazi Üniversitesi Bilişim Enstitüsü, Ankara, 15-17, (2012).

[8] İnternet: Kakıcı, A., Biyometrik Tanıma Sistemleri. URL: http://www.ahmetkakici.com/genel/biyometrik-tanima-sistemleri/ Son Erişim Tarihi: 03.09.2014.

[9] Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., Ben-David, S. (2012). Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption. ***Computing Classification System***, 1-10.

[10] İnternet: Yılmaz A. Biyometrik Tanıma Sistemleri. URL: http:// www.guvenlikdanismanlik.com/biyometrik-tanimasistemleri.htm. Son Erişim Tarihi: 15.09.2014.

[11] Chen, X., Tian, J., Su, Q., Yang, X. Wang, F. A Secured Mobile Phone Based on Embedded Fingerprint Recognition Systems. ***Intelligence and Security Informatics***, 3495: 549-553, (2005).

[12] Uchida, K. Fingerprint-based user-friendly interface and pocket-PID for mobile authentication. ***Pattern Recognition***, 4: 205-209, (2000).

[13] Lee, H. C., Park, K. R., Kang, B. J., Park, S. J. A New Mobile Multimodal Biometric Device Integrating Finger Vein and Fingerprint Recognition. ***Ubiquitous Information Technologies & Applications***, 20-22, (2009).

[14] Liu, Y., Edward, S., Roger, Sr. Human acoustic fingerprints: A novel biometric modality for mobile security. ***Acoustics, Speech and Signal Processing***, 3784-3788, (2014).

[15] Qi, Z., Wen, W., Meng, W., Zhang, Y., Shi, L. An energy efficient OpenCL implementation of a fingerprint verification system on heterogeneous mobile device. ***Embedded and Real-Time Computing Systems and Applications***, 1-8, (2014).

[16] Chen, W., Huang, J. Speaker Recognition Using Spectral Dimension Features. ***Computing in the Global Information Technology***, 132-137, (2009).

[17] Kounoudes, A., Kekatos, V. ; Mavromoustakos, S. Voice Biometric Authentication for Enhancing Internet Service Security. ***Information and Communication Technologies***, 1: 1020-1025, (2006).

[18] Clarke, N., Karatzouni, S., Furnell, S. Flexible and Transparent User Authentication for Mobile Devices. ***Computer Communication Networks***, 1-12, (2009).

[19] Hazen, T. J., Weinstein, E., Park, A. Towards Robust Person Recognition On Handheld Devices Using Face and Speaker Identification Technologies. ***Pattern Recognition***, 289-292, (2003).

[20] İnternet: Marcel, S., McCool, C., Atanasoaei, C., Tarsetti, F., Pesan, J., Matejka, P., Cernocky, J. (2010). MOBIO: Mobile Biometric Face and Speaker Authentication. URL:http://www.webcitation.org/query?url =http%3A%2F%2Fvisidon.fi%2Fpublications%2Fmobiodemo.pdf&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[21] McCool, C., Marcel, S., Hadid, A., Pietikainen, M., Matejka, P., Cernocky, J., Poh, N., Kittler, J., Larcher, A., Levy, C., Matrouf, D., Bonastre, J.-F., Tresadern, P., Cootes, T. Bi-Modal Person Recognition on a Mobile

Phone: Using Mobile Phone Data. ***Multimedia and Expo Workshops***, 635 – 640, (2012).

[22] Khoury, E., Shafey, L., McCool, C., Günther, M., Marcel, S. Bi-modal biometric authentication on mobile phones in challenging conditions. ***Image and Vision Computing***, 32(12): 1147–1160, (2014).

[23] Kang, J. Mobile iris recognition systems: An emerging biometric technology. ***Procedia Computer Science***, 1(1): 475-484, (2010).

[24] Cho, D. H., Park, K. R., Rhee, D. W. Real-time iris localization for iris recognition in cellular phone. ***Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing***, 254-259, (2005).

[25] Cho, D. H., Park, K. R., Rhee, D. W., Kim, Y., Yang, J. Pupil and Iris Localization for Iris Recognition in Mobile Phones. ***Software Engineering, Artificial Intelligence, Networking, and Parallel/ Distributed Computing***, 197-201, (2006).

[26] Jeong, D. S., Park, H., Park, K. R., Kim, J. Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter. ***Image Processing and Computer Vision***, 457-463, (2005).

[27] Park, K. R., Park, H., Kang, B. J., Lee, E. C., Jeong, D. S. A Study on Iris Localization and Recognition on Mobile Phones. ***EURASIP Journal on Advances in Signal Processing***, 1-12, (2007).

[28] Gragnaniello, D., Sansone, C.,Verdoliva, L. Iris liveness detection for mobile devices based on local descriptors. ***Pattern Recognition Letters***, 57: 1-6, (2014).

[29] Kurkovsky, S., Carpenter, T., MacDonald, C. Experiments with Simple Iris Recognition for Mobile Phones. ***Information Technology: New Generations***, 1293 -1294, (2010).

[30] Marsico, M., Galdi, C., Nappi, M., Riccio, D. Face and Iris Recognition for Mobile Engagement. ***Image and Vision Computing***, 32(12): 1161-1172, (2014).

[31] Abate, A. F., Frucci, M., Galdi, C., Riccio, D. BIRD: Watershed Based IRis Detection for mobile devices. ***Pattern Recognition Letters***, 57: 1-9, (2014).

[32] Han, S., Park, H., Cho, D., Park, K., Lee, S. Face Recognition Based on Near-Infrared Light Using Mobile Phone. ***Adaptive and Natural Computing Algorithms***. 4432: 440-448, (2007).

[33] Ijiri, Y., Sakuragi, M., Lao, S. Security Management for Mobile Devices by Face Recognition. ***Mobile Data Management***, 49, (2006).

[34] Kim, D., Chung, K., Hong, K. Person Authentication using face, teeth and voice modalities for mobile device security. ***Biometrics Compendium***, 56(4): 2678-2685, (2011).

[35] Abeni, P., Baltatu, M., D'Alessandro, R. NIS03-4: Implementing Biometrics-Based Authentication for Mobile Devices. ***Global Telecommunications Conference***, 1-5.

[36] Hadid, A., Heikkila, J.Y., Silven, O., Pietikainen, M. Face and Eye Detection for Person Authentication in Mobile Phones. ***Distributed Smart Cameras***, 101-108, (2007).

[37] İnternet: Brown, N. Mobile Verification by Palmprint Bio metrics. URL: http://www.webcitation.org/query?url= https%3A%2F%2Fstacks.stanford.edu%2Ffile%2Fdruid%3Amy512gb2187%2FBrown_Mobile_Identification_by_Palmprint_Biometrics.pdf&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[38] Franzgrote, M., Borg, C., Tobias, B.J., Bussemaker, S., Jiang, X., Fieleser, M., Zhang, D. Palmprint Verification on Mobile Phones Using Accelerated Competitive Code. ***Hand-Based Biometrics***, 1-6, (2011).

[39] Choraś, M., Kozik, R. Contactless palmprint and knuckle biometrics for mobile devices. ***Pattern Analysis and Applications***, 73-85, (2012).

[40] Han, Y., Tan, T., Sun, Z., Hao, Y. Embedded Palmprint Recognition System on Mobile Devices. ***Image Processing and Computer Vision***, 4642: 1184-1193, (2007).

[41] Kima, D., Shinb, J., Hong, K. Teeth recognition based on multiple attempts in mobile devices. ***Journal of Network and Computer Applications***, 33(3): 283-292, (2010).

[42] Kim, D., Hong, K. Multimodal biometric authentication using teeth image and voice in mobile enviroment. ***Consumer Electronics***, 54(4): 1790 – 1797, (2008).

[43] Tanviruzzaman, M., Ahamed, S. I., Hasan, C.S., O'Brien, C. ePet: When Cellular Phone Learns to Recognize Its Owner. ***Computer and Communications Security***, 13-18, (2009).

[44] Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J. Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation. ***Pattern Recognition***, 1-5, (2008).

[45] İnternet: Rüya Şamlı, R., Kurt, M. (2009) Biyometrik Tanıma Sistemleri. URL: http://www.webcitation.org/query?url=http%3A%2F %2Fab.org .tr%2Fab09%2Fkitap%2Fsamli_yu+ksel_AB09.pdf&date=2015-03-21. Son Erişim Tarihi:22.03.2015.

[46] Yıldız H. Avuç içi Esaslı Biyometrik Kimlik Tanıma ve Doğrulama, ***Yüksek Lisans Tezi***, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2, (2010).

[47] Çınar S. Mobil Android Ortamında Parmak İzi Tanıma ve Kimlik Doğrulama Sisteminin Geliştirilmesi, ***Yüksek Lisans Tezi***, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 13, (2014).

[48] İnternet: Görgünoğlu, S., Çavuşoğlu, A. (2009). Parmakizi Tanıma Sistemlerinde Kullanılan Özellik Çıkartma Algoritmalarının Performans Analizi. URL: http://www.webcitation.org/query?url=http%3A%2F %2Fiats09.karabuk.edu.tr%2Fpres%2Fbildiriler_pdf%2FIATS09_01-03_1578.pdf&date=2015-03-21. Son Erişim Tarihi:22.03.2015.

[49] Varlık, A., Çorumluoğlu, Ö. Dijital Fotogrametri Teknikleri İle Kişi Tanıma. ***Harita Teknolojileri Elektronik Dergisi***, 3(2), 1-24, (2011).

[50] Aydın Ö. Yapay Sinir Ağlarını Kullanarak Bir Ses Tanıma Sistemi Geliştirilmesi, ***Yüksek Lisans Tezi***, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, 6-22, (2005).

[51] İnternet: Yılmaz A. Biyometrik Tanıma Sistemleri. URL: http:// www.guvenlikdanismanlik.com/biyometrik-tanima-sistemleri.htm. Son Erişim Tarihi: 15.09.2014.

[52] Abdallah, S. J., Osman, M.İ., Mustafa, M. E. Text-Independent Speaker Identification Using Hidden Markov Model. ***World of Computer Science and Information Technology Journal***, 2(6), 203-208, (2012).

[53] Reynolds, D., Rose, R. Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models. ***Speech and Audio Processing***, 3: 72-83, (1995).

[54] Reynolds, D. A. A Gaussian mixture modeling approach to text independent speaker identification, ***Ph.D. Thesis***, Georgia Institute of Technology, (1992).

[55] Campbell, W. M., Campbell, J. P., Gleason, T. P., Reynolds, D. A., Shen, W. Speaker Verification Using Support Vector Machines and High- Level Features. ***Speech and Language Processing***, 15(7): 2080-2095, (2007).

[56] İnternet: Quatieri, F. (2002). Discrete-Time Speech Signal Processing: Principles and Practice. URL: http://www.webcitation.org/query?url= http%3A%2F%2Fwww.pearson.ch%2Fdownload%2Fmedia%2F9780132429429.pdf&date=2015-03-22. Son Erişim Tarihi: 23.03.2015.

[57] İnternet: Tunalı, V. Konuşmacı Tanıma Sistemi.(2007). URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.vtunali.com%2Ffiles%2FOzan_MUT_Tez.pdf&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[58] Daugman, J. How Iris Recognition Works, ***Image Proccessing***, 14(1): 1-3, (2002).

[59] Femila M.D., Irudhayaraj A.A. Biometric system, ***Electronics Computer Technology (ICECT)***, 152-156, (2011).

[60] İnternet: Kakıcı, A., Biyometrik Tanıma Sistemleri. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.ahmetkakici.com%2Fgenel%2Fbiyometrik-tanima-sistemleri%2F&date=2015-03-22. Son Erişim Tarihi: 23.03.2015.

[61] Erdoğan, A. Yüz Tanımada Özyüz ve Fisher Yüz Algoritmalarının İncelenmesi, ***Yüksek Lisans Tezi***, Ankara Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 16-54, (2010).

[62] İnternet: Çevikalp, H., Neamtu, M., Wilkes, M., Barkana, A. Kişi Yüzlerinin Ayırt edilmesi İçin Yeni Bir Yöntem. URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.math.vanderbilt.edu%2F~neamtu%2Fpapers%2Fcevikalp.pdf+&date=2015-03-22. Son Erişim Tarihi: 23.03.2015.

[63] Viola, P., Jones, M. Rapid object detection using a boosted cascade of simple features, in. ***Computer Vision and Pattern Recognition***, 1: 511-518, (2001).

[64] Turk, M.A., Pentland, A.P. Face recognition using eigenfaces. ***Computer Vision and Pattern Recognition***, 586 –591, (1991).

[65] Yaman, B. Özyüz Kullanarak Yüz Tanıma, ***Yüksek Lisans Tezi***, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Adapazarı, 15-18, (2006).

[66] İnternet: Sönmez, E.B., Özbek N.Ö., Özbek Ö.. (2000). Dalgacık Dönüşümüne Dayalı Çoklu Model Biyometrik Sistem. URL: ab.org.tr/ab08/bildiri/37.doc. Son Erişim Tarihi: 23.03.2015.

[67] Çelik, E. Görüntü İşlemeye Dayalı Avuç İçi İzininYapay Sinir Ağı İle Tanınması, ***Yüksek Lisans Tezi***, Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 32-58, (2011).

[68] İnternet: Welcome to MOBIO. (2008). URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.mobioproject.org%2F&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[69] İnternet: Biometrics Evaluation and Testing. (2011). http://www.webcitation.org/query?url=https%3A%2F%2Fwww.beat-eu.org&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[70] İnternet: OMRON. URL: http://www.webcitation.org/query?url =http%3A%2F%2Fwww.omron.com%2Fr_d%2Fcoretech%2Fvision%2Fokao.html&date=2015-03-21. Son Erişim Tarihi: 21.03.2015.

[71] İnternet: Face Recognıtıon Homepage.(2015). URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.face-rec.org%2Fdataba ses%2F&date=2015-03-24. Son Erişim Tarihi: 24.03.2015.

[72] İnternet: Indian Journal of History of Science. (2001). URL: http://insaindia.org/journals. Son Erişim Tarihi: 07.04.2015.

[73] İnternet: ODTÜ Bilgisayar Topluluğu Elektronik Dergisi. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fe-bergi.com %2Fy%2FSes-Tanima&date=2015-03-24. Son Erişim Tarihi: 24.03.2015.

[74] İnternet: Ses tanıma URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.cclub.org.tr%2Fbergi_yeni%2Fe-bergi%2F2008%2FKasim%2FSesTanima&date=2015-03-24. Son Erişim Tarihi: 24.03.2015.

[75] İnternet: Biometric Market Developments. (2007). URL: http://www.acuity-mi.com/hdfsjosg/euyotjtub/Biometrics% 202007%20 London.pdf.