

**T.C.  
PAMUKKALE ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ  
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**KULAK BİYOMETRİSİ KULLANARAK  
GÖRÜNTÜ İŞLEM TABANLI  
KİMLİK TESPİTİ**

**YÜKSEK LİSANS TEZİ**

**ESMA YENİSARI**

**DENİZLİ, MAYIS - 2015**

**T.C.  
PAMUKKALE ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ  
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**



**KULAK BİYOMETRİSİ KULLANARAK GÖRÜNTÜ İŞLEM  
TABANLI KİMLİK TESPİTİ**

**YÜKSEK LİSANS TEZİ**

**ESMA YENİSARI**

**DENİZLİ, MAYIS - 2015**

## KABUL VE ONAY SAYFASI

**Esma YENİSARI** tarafından hazırlanan “**KULAK BİYOMETRİSİ KULLANARAK GÖRÜNTÜ İŞLEM TABANLI KİMLİK TESPİTİ**” adlı tez çalışmasının savunma sınavı 04.05.2015 tarihinde yapılmış olup aşağıda verilen jüri tarafından oy birliği ile Pamukkale Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Danışman

Doç. Dr. Emre ÇOMAK

.....

Üye

Doç. Dr. Sezai TOKAT

Pamukkale Üniversitesi

.....

Üye

Doç. Dr. Aydın KIZILKAYA

Pamukkale Üniversitesi

.....

Pamukkale Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun  
..... tarih ve ..... sayılı kararıyla onaylanmıştır.

.....

Prof. Dr. Orhan KARABULUT

Fen Bilimleri Enstitüsü Müdürü

**Bu tezin tasarımı, hazırlanması, yürütülmesi, arařtırmalarının yapılması ve bulgularının analizlerinde bilimsel etięe ve akademik kurallara özenle riayet edildiđini; bu alıřmanın dođrudan birincil ürünü olmayan bulguların, verilerin ve materyallerin bilimsel etięe uygun olarak kaynak gösterildiđini ve alıntı yapılan alıřmalara atfedildiđine beyan ederim.**

**ESMA YENİSARI**

## ÖZET

**KULAK BİYOMETRİSİ KULLANARAK GÖRÜNTÜ İŞLEM TABANLI  
KİMLİK TESPİTİ  
YÜKSEK LİSANS TEZİ  
ESMA YENİSARI  
PAMUKKALE ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ  
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI  
(TEZ DANIŞMANI:DOÇ. DR. EMRE ÇOMAK)**

**DENİZLİ, MAYIS – 2015**

Küreselleşme ve teknoloji ile dünya üzerindeki sınırların ortadan kalkmasıyla insan etkileşiminin de sınırları değişmiştir. Gerek fiziki gerek sanal olarak dünyanın herhangi bir noktası ile etkileşim kurma hızı artmıştır. Birbiriyle ilişki içinde olan kişi sayısı bir hayli fazla olduğundan kişileri tanıma büyük bir problem haline gelmiştir. Kimlik tanıma ve kimlik doğrulama işlemlerini hem kullanışlı hem de güvenli hale getirmek çoğu sistem için öncelik oluşturmaktadır. Çoğu sistemde kullanılan şifre, parola, güvenlik kartı gibi bilinen ya da sahip olunan bir nesne kullanarak güvenlik sağlamak yerine doğrudan kişinin kendisini kullanma fikri gelişmiştir. Biyometri adı verilen ve kişinin kendisini oluşturan, bireye özgü davranışsal ya da karakteristik birtakım özellikler vardır. Biyometrik sistemlerde retina, iris, parmak izi, kulak, imza gibi karakteristik özellikler ile kimlik doğrulama ve kimlik tanıma işlemleri yapılmaktadır. Her bir biyometrik veri kullanılma amacına, güvenlik seviyesine ya da elde edilebilme şartına göre farklı sistemlerde kullanılmaktadır. Bu tezde kulak biyometrisi ile kimlik tanıma işlemi gerçekleştirilmiştir. Kullanılan kulak görüntüsü görüntü işleme yöntemleri ile istenen forma getirilmiştir. Literatürde var olan standart yöntemlerin aksine pek çok görüntü işleme ve iyileştirme yöntemi aynı anda kullanılarak kulak görüntüsünden kontur bilgisine ulaşılmıştır. Verilerde bir standart sağlamak için normalize edildikten sonra kayıt edilmiştir. Kimlik doğrulama ve kimlik tanımlama işlemlerini gerçekleştirmek içinde Hu momentleri baz alınarak eşleştirme yapılmıştır. Sistemde kullanılan AMI kulak veri tabanındaki farklı kişilere ait kulak görüntüleri kullanılarak, kimlik tanımda umut vaat eden sonuçlara ulaşılmıştır.

**ANAHTAR KELİMELELER:** Biyometri, Biyometrik Sistem, Kulak Biyometrisi, Görüntü İşleme, Kimlik Tanımlama, Kimlik Doğrulama

## **ABSTRACT**

### **IMAGE PROCESSING BASED IDENTIFICATION BY USING EAR BIOMETRY**

**MSC THESIS**

**ESMA YENİSARI**

**PAMUKKALE UNIVERSITY INSTITUTE OF SCIENCE**

**COMPUTER ENGINEERING**

**(SUPERVISOR:ASSOC. PROFESSOR DR. EMRE ÇOMAK)**

**DENİZLİ, MAY 2015**

With the elimination of borders in the world by globalization and technology the boundaries of the human interaction has also changed. Both the physical and the virtually interaction speed of any point in the world has increased. The number of people who are in relationships with each other is considerable so recognizing people has become a major problem. To make identification and authentication procedures both convenient and secure is a priority for most systems. Instead of using something that own like security card or something that known like password, the idea of using the persons himself/herself improved. There are set of behavioral and characteristic features that are individual called biometrics. In biometric systems, authentication and identification procedures are performed by the features such as retina, iris, fingerprint, ear, signature. Each biometric data can be used in different systems according to the security level, obtaining condition or using ambition .In this thesis, identification procedure was carried out with ear biometrics. Ear images that are used convert to the desired form by image processing methods. Unlike standard methods in the literature many image processing and enhancement methods used simultaneously to reach ear contour from the ear image. To provide a standard for data, normalization process is done before recording. To perform authentication and identification, matching process is done by Hu moments. Using ear images belong to different people in AMI database, promising results have been achieved in recognition of identity

**KEYWORDS:** Biometric, Biometric System, Ear Biometry, Image Processing, Identification, Authentication

# İÇİNDEKİLER

Sayfa

<b>ÖZET</b> .....	<b>i</b>
<b>ABSTRACT</b> .....	<b>ii</b>
<b>İÇİNDEKİLER</b> .....	<b>iii</b>
<b>ŞEKİL LİSTESİ</b> .....	<b>v</b>
<b>TABLO LİSTESİ</b> .....	<b>vi</b>
<b>KISALTMALAR LİSTESİ</b> .....	<b>vii</b>
<b>ÖNSÖZ</b> .....	<b>viii</b>
<b>1. GİRİŞ</b> .....	<b>1</b>
1.1 Tezin Amacı ve Literatüre Katkısı .....	1
<b>2. LİTERATÜR ÇALIŞMASI</b> .....	<b>5</b>
<b>3. BİYOMETRİ</b> .....	<b>9</b>
3.1 Biyometri Nedir.....	9
3.2 Fiziksel ve Davranışsal Biyometrik Karakteristikler .....	10
3.2.1 Beyin.....	10
3.2.2 Diş.....	12
3.2.3 DNA.....	12
3.2.4 El Geometrisi .....	12
3.2.5 İris .....	13
3.2.6 Parmak İzi .....	13
3.2.7 Retina.....	14
3.2.8 Yüz.....	14
3.2.9 Dudak Şekli ve Hareketi .....	14
3.2.10 İmza .....	15
3.2.11 Kalp Atışı.....	15
3.2.12 Klavye Kullanımı.....	15
3.2.13 Ses .....	16
3.2.14 Yürüyüş Biçimi.....	16
<b>4. KİMLİK TESPİTİ VE GÜVENLİK</b> .....	<b>17</b>
<b>5. GÖRÜNTÜ İŞLEME</b> .....	<b>18</b>
5.1 Görüntü İşleme Nedir .....	18
5.2 Görüntü İşlemenin Temel Adımları .....	18
<b>6. BİYOMETRİK SİTEMLERDE GÖRÜNTÜ İŞLEME İLE KİMLİK TESPİTİ VE GÜVENLİK</b> .....	<b>23</b>
6.1 Biyometrik Sistem Nedir .....	23
6.1.1 Kayıt (Enrollment).....	23
6.1.2 Doğrulama (Verification) .....	23
6.1.3 Tanımlama / Kimlik Belirleme (Identification).....	24
6.2 Biyometrik Sistem Çalışma Prensipleri.....	25
6.3 Biyometrik Sistemlerin Karşılaştırılması .....	25
6.4 Biyometrik Sistemlerin Uygulama Alanları .....	27
6.5 Biyometrik Sistemlerin Avantaj ve Dezavantajları.....	29
<b>7. BİYOMETRİK SİSTEM BAŞARIM ÖLÇÜMÜ OLARAK HATA ORANLARI</b> .....	<b>31</b>
7.1 Yanlış Eşleşme(FMR) , Yanlış Reddetme (FNMR) ve Eşit Hata Oranı (EER).....	31

7.2	Edinim Başarısızlığı (FTC) ve Kayıt Başarısızlığı (FTE) .....	32
7.3	Yanlış Red Oranı (FRR) ve Yanlış Kabul Oranı (FAR) .....	33
<b>8.</b>	<b>BİYOMETRİK VERİ OLARAK KULAK.....</b>	<b>35</b>
<b>9.</b>	<b>YAPILAN ÇALIŞMALAR VE UYGULAMA SONUÇLARI.....</b>	<b>40</b>
<b>10.</b>	<b>SONUÇ VE ÖNERİLER.....</b>	<b>57</b>
<b>11.</b>	<b>KAYNAKLAR.....</b>	<b>59</b>
<b>12.</b>	<b>ÖZGEÇMİŞ.....</b>	<b>65</b>



## ŞEKİL LİSTESİ

### Sayfa

Şekil 3.1: İnsana ait fiziksel ve davranışsal biyometrik karakteristikler.....	11
Şekil 5.2: Görüntü işleme temel adımları .....	19
Şekil 6.3: Biyometrik sistemde genel kullanımda olan üç uygulama; .....	24
Şekil 6.4: Biyometrik sistem çalışma prensibi .....	26
Şekil 7.5: Biyometrik sistem hata oranları .....	32
Şekil 7.6: Yanlış eşleşme ve yanlış reddetme oranları.....	34
Şekil 8.7: Dış kulak yapısı ve bölümleri .....	37
Şekil 9.8: AMI kulak veri tabanında 5 numaralı kayıta ait, kulak örnekleri.....	41
Şekil 9.9: AMI kulak veri tabanında 28 numaralı kayıta saç, küpe gibi faktörlerden kaynaklanan tıkanıklıklar.....	41
Şekil 9.10: AMI kulak veri tabanından yapılan testler için kırılan kulak görüntüleri. ....	41
Şekil 9.11: Giriş sayfası ekran görüntüsü .....	42
Şekil 9.12: Giriş sayfasında kayıt bilgisi.....	42
Şekil 9.13: Giriş sayfasında kimlik doğrulama bilgisi .....	43
Şekil 9.14: Giriş sayfasında kimlik sorgula bilgisi .....	43
Şekil 9.15: Kayıt sayfası görünümü .....	44
Şekil 9.16: Kayıt sayfasında kulak foto yükleme.....	45
Şekil 9.17: Kayıt sayfasında yüklenen kulak görüntüsünü rengini parlatma....	45
Şekil 9.18: Kayıt sayfasında kulak görüntüsünü grileştirme .....	45
Şekil 9.19: Kayıt sayfasında kulak görüntüsünü ikili görüntü haline getirme..	46
Şekil 9.20: Canny Kenar Bulma algoritması uygulama.....	46
Şekil 9.21: Kulak görüntüsünün konturunu bulma .....	46
Şekil 9.22: Kulak görüntüsünü normalleştirdikten sonra, özellik çıkartımı yapılıp veri tabanına kaydedilmesi.....	47
Şekil 9.23: Temsili verilen piksellere medyan filtre uygulanma örneği .....	48
Şekil 9.24: Genleşme uygulanmış temsili piksel örneği .....	49
Şekil 9.25: Kimlik sorgula sayfası ekran görüntüsü .....	52
Şekil 9.26: Yüklenen kulak görüntüsünün özelliğini çıkartıp veri tabanında sorgulama .....	52
Şekil 9.27: Kimlik doğrula sayfası ekran görüntüsü.....	52

## TABLO LİSTESİ

### Sayfa

Tablo 6.1: Biyometrik sistemlerin karşılaştırılması (Y: yüksek, O: orta, D: düşük) (Jain ve diğ. 2004).....	27
Tablo 9.2: Çalışmanın eşleşme doğruluğu oranları.....	55
Tablo 9.3: Aynı açılardan oluşan kulak görüntüleri kullanılmasıyla belirlenen parametrelere göre yapılan test ve sonucu. ....	55
Tablo 9.4: Farklı açılardan oluşan kulak görüntüleri kullanılmasıyla belirlenen parametrelere göre yapılan test ve sonucu. ....	56

## KISALTMALAR LİSTESİ

<b>EEG</b>	: Elektroensefalogram (Beyin Dalgaları Aktivitesini Elektriksel Yöntemle Ölçme)
<b>MR</b>	: Manyetik Rezonans
<b>DNA</b>	: Deoksiribonükleik Asit
<b>FMR</b>	: Yanlış Eşleştirme Oranı False Match Rate )
<b>FNMR</b>	: Yanlış Reddetme Oranı (False non-Match Rate)
<b>EER</b>	: Eşit Hata Oranı (Equal Error Rate)
<b>FTC</b>	: Yakalama Hatası ( Failure To Capture)
<b>FTE</b>	: Kayıt Hatası (Failure To Enroll)
<b>FAR</b>	: Yanlış Kabul Oranı (False Acceptance Rate)
<b>FRR</b>	: Yanlış Red Oranı (False Rejection Rate)
<b>USTB</b>	: Pekin Bilim ve Teknoloji Üniversitesi (University of Science and Technology Beijing)
<b>UND</b>	: Notre Dame Üniversitesi (University Of Notre Dame)
<b>ITT</b>	: Tallaght Teknoloji Enstitüsü (Institute Of Technology Tallaght)
<b>AMI</b>	: Atlas Meta Verileri Arayüzleri (Atlas Metadata Interfaces)
<b>GMA</b>	: Market Ürünleri Derneği (Grocery Manufactures Association)
<b>XM2VTS</b>	: Teleservisler İçin Çoklu Mod Doğrulama Ve Güvenlik Uygulamaları (Multi Modal Verification For Teleservices And Security Applications)
<b>UCR</b>	: Kaliforniya Üniversitesi ( University Of California Riverside)
<b>UMIST</b>	: Manchester Üniversitesi Bilim Ve Teknoloji Enstitüsü (The University Of Manchester Institute Of Science And Technology)
<b>NIST</b>	: Standart Ve Teknoloji Milli Enstitüsü (National Institute Of Standards And Technology)
<b>FERET</b>	: Yüz Tanıma Teknolojisi (The Face Recognition Technology)
<b>UBEAR</b>	: Beira İç Üniversitesi, Portekiz (University of Beira Interior)
<b>OpenCV</b>	: Açık Kaynak Kodlu Bilgisayar Görüşü (Open Source Computer Vision)
<b>SQL</b>	: Yapısal Sorgulama Dili (Structured Query Language)
<b>VB</b>	: Visual Basic

## ÖNSÖZ

Bu çalışmada biyometrik yöntemler hakkında gerekli bilgi elde edilerek biyometrik yöntemlerden biri olan kulak biyometrisi ile görüntü işlem tabanlı kimlik tanıma işlemi gerçekleştirilmiştir.

Tez çalışmasını hazırlama aşamasında katkıda bulunan tez danışman hocam Doç. Dr. Emre ÇOMAK'a teşekkürü bir borç bilirim.

Tezim ve hayatımın her alanındaki elde ettiğim başarılarda mutlaka katkısı bulunan, umutsuzluğa kapıldığım her an yanımda olup beni olumlu bir şekilde yönlendiren kardeşim Betül YENİSARI'ya sonsuz teşekkür ederim.

Tüm eğitim hayatımda yanımda olup beni destekleyen ve teşvik eden annem Ayşe YENİSARI ve babam Ahmet YENİSARI'ya teşekkür ederim..

Tezimi hazırlama sürecinde maddi manevi yardımlarını esirgemeyen Çanakkale Onsekiz Mart Üniversitesi öğretim elemanı hocalarıma ve mesai arkadaşlarıma şükranlarımı sunarım.

# 1. GİRİŞ

## 1.1 Tezin Amacı ve Literatüre Katkısı

Günümüz dünyasında teknoloji, eğitim, yönetim, güvenlik, bilişim, mobil gibi farklı birçok alanda en geçerli değer bilgidir. Bilgi bu kadar önemli bir konumda kendine yer edinirken onun korunması saklanması ihtiyacı da ortaya çıkmıştır. Hayatımızın her alanında olan bilgiye ulaşmak için kimi zaman bankamatikte şifre gireriz, kimi zaman bir binaya güvenlik kartıyla gireriz, kimi zaman da cep telefonlarından parmak izimizi okuturuz.

Bilginin güvenliğini sağlarken 3 farklı yöntem kullanılır. Bunlar; parola, giriş kodu gibi bilinen bir şey, akıllı kart, güvenlik kartı gibi sahip olunan bir şey ya da biyometrik gibi hali hazırda olunan bir şeydir (Liu ve Silverman 2001). Parola, şifre, güvenlik kartı birer nesneyken, biyometri kişinin kendisi, yani öznedir.

Bilgi tabanlı ya da kart tabanlı sistemlerle karşılaştırıldığında, biyometri daha doğru, hassas sonuç verir ve kopyalaması zordur. Biyometride parola hatırlama gerekmez, kimlik taşımaya gerek olmaz (Ngugi ve diğ 2011; O’Gorman 2004).

Biyometri; yaşama ve insana dair özelliklerle ilgili ölçümlerdir. Biyometrik; tanımak veya kimlik doğrulaması yapmak için bireylerin benzersiz fiziksel ve davranışsal özelliklerini ölçmektir (Liu ve Silverman 2001). İnsanlar zaten binlerce yıldır birbirlerini tanımak için yüz, ses, yürüyüş gibi vücut özelliklerini kullanmışlardır (Jain ve diğ. 2004). Günümüzde ise bu biyometrik özellikler otomatik sistemlere entegre edilerek kimlik tanıma ve kimlik doğrulama işlemleri teknolojik yöntemlerle yapılabilmektedir.

Bireye ait her özellik biyometrik veri olarak kullanılmaz. İnsana ait bir özelliğin biyometrik olarak adlandırılabilmesi için sahip olması gereken bazı şartlar vardır. Bunlar; evrensellik, ayırt edicilik, devamlılık ve elde edilebilirliktir. Bu

şartların yanı sıra bir biyometrik sistemin, tanımlama başarımı, kabul edilebilirlik, ve atlatılamaz olması gibi özelliklere de sahip olması gerekir.

Yukarıda sayılan şartları sağlayan biyometrik özellikler fiziksel ve davranışsal olarak iki ayrı grupta değerlendirilebilir. Beyin, DNA, kulak, yüz, parmak izi, kan damarları, el geometrisi, iris ve retina fiziksel özelliklere örnek olarak verilebilir. Davranışsal özelliklere imza, kalp atış ritmi, klavye kullanımı ve yürüyüş biçimi örnek olarak verilebilir.

Bir biyometrik sistem, bir bireyden biyometrik veriyi elde etme, elde edilen veriden özellik seti çıkarma ve veri tabanındaki örnek küme ile bu özellik kümesini karşılaştırma işlemlerini yöneten bir görüntü tanıma sistemidir (Jain ve diğ 2004). Tasarımlarında farklılıklar mevcut olsa da bir biyometrik sistemin genel olarak üç önemli işlevi vardır:

- Kayıt aşaması: Tanımlama veya doğrulama yapılacak kişiye ait biyometrik verinin sisteme girişinin yapılması.
- Kimlik doğrulama: Biyometrik verisi alınan kişideki veri ile söz konusu kişiye ait sistem veri tabanına daha önceden kaydedilen biyometrik veri örneği bire bir karşılaştırılır. Karşılaştırma sonunda biyometrik verilerin uyuşması durumunda doğrulama yapılır.
- Kimlik belirleme: Sistem bireyin kimliğini tanıyabilmek için veri tabanındaki tüm kullanıcı örnekleriyle bireyin biyometrik verisini eşleştirmeye çalışır. Birey sisteme herhangi bir kimlik iddia etmez bu yüzden birçok karşılaştırma yapılır.

Tasarlanan sistemde kullanılacak biyometrik veriye göre kayıt, doğrulama ve tanımlama işlemleri şekillenir. Kayıt aşamasında elde edilen veri kimi zaman algılayıcılarla elde edilen parmak iziyken, kimi zaman ses verisini tutan ses dalgaları olabilir.

Kullanılacak veri kişinin sahip olduğu biyometrik özelliğinin sayısal görüntüsüyse bunun uygun formata getirilmesi için görüntü işleme teknikleri kullanılır. İlk önce kullanılacak görüntü yakalanır. Elde edilen görüntü üzerinde işlem yapabilmek için öncelikle filtreleme ve iyileştirme uygulanır. Görüntüyü gri

tonlamalı veya iki renkten (siyah ve beyaz) oluşan biçime dönüştürmek de görüntü üzerinde yapılabilecek işlemlerdendir. Tanımlama ve kimlik belirleme işlemlerinde nasıl bir eşleştirme yöntemi kullanılacaksa ona uygun olarak görüntü işleme adımları da farklılık gösterebilir. Elde edilen veride belli bir standarda ulaşılması hedeflenmektedir. Belirlenen standartlara göre uygun forma getirilmiş veri kaydedilir.

Genel bir biyometrik sistem yedi parçadan oluşmaktadır. Bunlar biyometrik okuyucu ihtiva eden bir kullanıcı ara yüzü veya sensör, kalite kontrol modülü, biyometrik sinyal kalitesini geliştirmek için bir donanım modülü, kişi tanıma görevi için uygun olan biyometrik örnekten sadece gerekli bilgiyi ayıklayan bir özellik çıkarıcı, kullanıcının biyografik bilgileriyle birlikte çıkartılan özellikleri depolayan bir veri tabanı, tanıma ve benzerlik oranını belirlemek için iki özellik kümesini karşılaştıran bir eşleyici, eşleyici tarafından belirlenen benzerlik çıktısına dayanarak kişinin kimliğini belirleyen karar modülüdür (Jain ve Nandakumar 2009).

Günümüz dünyasında teknoloji ve küreselleşme neticesinde fiziksel olarak sadece aynı ortamda bulunan insanlarla değil, çevrimiçi olarak dünyanın herhangi bir noktasıyla dahi ilişkili olunabilmektedir. Bu durumda kişinin gerçekte kim olduğu, iddia ettiği veya olduğunu reddettiği kişi olup olmadığı konusu önemli hale gelmektedir. Tüm bu bilgiler ışığında bu çalışmada, kimlik tanıma ve kimlik doğrulama yaparak güvenli giriş sağlayacak bir sistem tasarlanmış ve bunu yaparken de veri olarak kulak biyometrisi kullanılmıştır.

Bu çalışmada öncelikle biyometrinin ne olduğu, hangi karakteristiklerin biyometrik veri olduğu, biyometrik yöntemlerin farklılığı, üstünlükleri ve eksik yönleri yapılan literatür çalışması neticesinde ortaya konulmuştur. Sistemde kullanılacak olan biyometrik veriye karar verildikten sonra kullanıcı ara yüzü olan bir program tasarlanmıştır. Biyometrik veriyi kayıt altına almak ve eşleştirme işlemlerini gerçekleştirmek için gerekli olan görüntü işleme teknikleri incelenmiştir. Tezin amacı çalışmanın birinci bölümünde, tez konusu hakkında literatür çalışmaları neticesinde yapılan benzer çalışmalar ikinci bölümde anlatılmıştır. Daha sonra incelenen literatür neticesinde ortaya çıkan tanım, kural, teoremler gibi bilinmesi gereken kavramları açıklanmıştır. Üçüncü bölümde biyometrinin ne olduğu, hangi özelliklerin biyometrik veri olduğu kapsamlı bir biçimde incelenmiştir. Dördüncü

bölümde güvenliđin önemi, güvenliđi sađlamak için kullanılan yöntemlere yer verilmiştir. Sistem tasarımı için gerekli olacak görüntü işleme teknikleri ve temel adımları beşinci bölümde incelenmiştir. Altıncı bölümde ise iki, üç, dört ve beşinci bölümler neticesinde elde edilen bilgiler harmanlanıp biyometrik sistem tasarımı için görüntü işleme yöntemleri kullanılarak kimlik tespiti gerçekleştirme hakkında bilgi verilmiştir. Yedinci bölümde biyometrik sistem tasarımı sonrasında ortaya çıkan hata oranları anlatılmıştır. Sekizinci bölümde kullanılacak biyometrik veri olan kulak tanıtılmış, avantaj ve dezavantajlarına yer verilmiştir. Dokuzuncu bölümde tasarlanan sistem, kullanıcı arayüzü ekran çıktıları ile verilmiş, yapılan işlem ve kullanılan yöntemler anlatılmış, çalışmanın test sonucu ortaya çıkan oranları verilmiştir. Son olarak onuncu bölümde varılan sonuçlar ve geleceđe yönelik yapılacak çalışmalara ve önerilere yer verilmiştir.



## 2. LİTERATÜR ÇALIŞMASI

Biyometrik kimlik tanımlamada kulak biyometrisinin kullanılması 1900'lü yılların başlarına dayansa da, her geçen gün yeni bir yöntem kullanarak veya mevcut yöntemleri birleştirerek daha verimli sonuçlara ulaşma amacı hala günceldir. Bu amaç doğrultusunda son yıllarda kulak biyometrisi ile yapılan çalışmaların sayısı bir hayli artmıştır. Bu bölümde incelenen literatür neticesinde son iki yılda yapılan çalışmalarla ilgili bilgiler verilecektir.

Susmitha ve Reddy (2014) yaptıkları çalışmada kulak biyometrisi için giriş verisi olarak IIT Delhi Kulak Veri tabanındaki örnekleri kullanmışlardır. Alınan örneklere, ön işlem olarak iyileştirme tekniklerinden olan gürültü azaltımı işlemi uygulanmıştır. Gürültü azaltımı için Medyan filtre kullanılmıştır. Kulak görüntüsünden gerekli olan bölümlerin elde edilmesi için otomatikleştirilmiş kırpma işlemi gerçekleştirilmiştir. Görüntüde kenar tespiti için sıfır-karşıt yöntemi kullanılmıştır. Özellik çıkartımı aşamasında kulağın concha bölümü yerel özellik, dış heliks bölümü global bölüm olarak alınmıştır. Kulak görüntüsünden alınan bu yerel ve global bölümlerin başarılı biçimde birleştirilmesi için global bölümün boyutları yerel bölüme göre tekrar düzenlenmiştir. Elde edilen bu yeni birleştirilmiş haldeki özellikler veri tabanında saklanmıştır. Son olarak herhangi bir görüntünün veri tabanındaki diğer örneklerle karşılaştırma işlemi Hamming mesafe eşleştirme yöntemi ile yapılmıştır. Yapılan eşleştirme işlemi sonrası %100 doğruluk elde edilmiştir. Çalışmada kullanılan kulak görüntülerinin açıları ve görüntü kaliteleri aynı olduğundan başarılı bir sonuç elde edilmiştir.

Kurniawan ve diğ. (2014) yaptıkları çalışmada kulak tanımlama için 2 özellik kullanmışlardır. Bu özellikler, geometrik özellikler ve öz vektör özellikler adını almaktadır. Sisteme girdi olarak yüz bölgesinden çıkartılmış kulak görüntüsü kullanılmıştır. Yapılan çalışmada Pekin Bilim ve Teknoloji Üniversitesi veri tabanı (USTB) kullanılmıştır. Veri tabanındaki tüm örnekler 300x400 piksel boyutunda olduğundan normalize etmeye gerek olmamıştır. Girdi görüntülerindeki yüksek aydınlatmadan dolayı görüntü çok parlak olacağından ve dolayısıyla kenar tespitinde yeteri kadar güçlü ve temiz kenarlar elde edilemeyeceğinden, kontrast değişkeni

sabitlenmiştir. CHLAE yöntemi kullanılarak histogram eşitleme yapılmıştır. Kulak şekli geometrik özellik yöntemi ile ölçülmüştür. Bunun yanı sıra Üçgen Oran Yöntemi (TRM) ve Şekil Oran Yöntemi de başarıyı artırmak adına çalışmaya dahil edilmiştir. Geometrik özellik yöntemi ile kulağın geometrik bilgisinin tek başına yeterli olamayacağı ve verilen poz değişkeninden dolayı bazı kısıtlar ortaya çıkacağı görülmüştür. Bu yüzden bu çalışmada geometrik özellik yanı sıra öz vektör özelliği kullanılmıştır. Öz vektör özelliği, bölümlere ayrılan kulak görüntüsünden özellik çıkartmaya dayanır. Kulak öncelikle altı bölüme ayrılır ve her biri için öz vektör ile özellik çıkartımı yapılır. Son olarak elde edilen özellikler sınıflandırma için kullanılmıştır. Yapay sinir ağları benimsenen çalışmada, sistemin eğitimi için farklı poz değerlerindeki kulak görüntüleri kullanılmıştır. Test verisi olarak bazı kulak olmayan görüntüler sisteme girdi olarak verilmiştir. Yapay sinir ağlarından çıkan iki sonuca göre kulak, belirlendi ya da belirlenemedi olarak karar verilmiştir. Yapılan çalışmada 25 bireye ait farklı pozlardaki 104 kulak görüntüsü kullanılmıştır. Geometrik özellik yöntemi ile çıkartılan 64 özellikte %82,76 başarıya ulaşılırken, Geometrik yöntem ile öz vektör yönteminin bir arada kullanılmasıyla elde edilen 100 özellik ile başarı oranı %93,10 a ulaşmıştır. Ulaşılan performans sonucuna göre geometrik özelliklerin tek başına poz değişkeni ile başa çıkamadığı görülmüştür. Bu sebepten birleştirilen geometrik yöntem ve öz vektörler yöntemi ile daha iyi sonuçlara ulaşılmıştır.

Anwar ve diğ. (2015) yaptıkları çalışmada 272x204 piksel boyutunda görüntüleri kullanmışlardır. Görüntüyü düzgünleştirmek için Gaussian filtre kullanılmıştır. Daha sonra görüntüdeki kulağı tespit etmek için Yılan (snake) yöntemi kullanılmıştır. Yılan yönteminde görüntüye tıklamak suretiyle el ile başlangıç pozisyonu ve kontrol noktaları seçilmiştir. Kontur pozisyonunu hesaplamak için yapılacak yineleme sayısı belirlenmiştir. Kenar tespiti aşamasında, gürültü azaltımı yapmak için 5x5 boyutunda medyan filtre uygulanmıştır. Daha sonra görüntü Global Eşik değeri kullanarak ikili (binary) görüntü haline getirilmiştir. Bu ikili görüntü üzerinde Canny Kenar tespit yöntemi kullanarak kenar tespiti yapılmıştır. Son işlem olarak da morfolojik işlemlerden olan genişletme uygulanarak ayrı duran kenarlar birbirine bağlanmıştır. İstenmeyen piksellerde, örneğin 50 den az olanlar silinip konturlar birbirine bağlanmıştır. Sınıflandırmada üç farklı yöntem kullanılmıştır. Bu yöntemler; Saf (naive) sınıflandırma, Öklit uzaklığını kullanan en

yakın komşuluk sınıflandırması (nearest neighbourhood) ve en küçük mutlak fark uzaklığını kullanan K-en yakın komşuluk (K-nearest neighbourhood) sınıflandırmasıdır. Çalışmada test aşamasında IIT veri tabanındaki 50 kişiye ait 3'er kulak görüntüsü kullanılmıştır. Sonuç olarak saf sınıflandırmada %88'lik, en yakın komşulukta %94'lük ve K-en yakın komşuluk sınıflandırmasında ise %98'lik bir doğruluğa ulaşılmıştır.

Jamil ve diğ. (2015) kulak biyometrisi ile kimlik doğrulama çalışmalarında beş ana adımı uygulamışlardır. Bu adımlar; görüntüyü yakalama, görüntü üzerinde ön hazırlık işlemleri uygulama, kulak bölümlene, özellik çıkartımı ve kulak eşleştirmedir. Kulak görüntülerini elde etmek için hazır bir veri tabanı kullanmak yerine sayısal bir fotoğraf makinesi kullanmışlardır. Alınan kulak görüntüleri iç mekanda beyaz florasan ışığında, dış mekanda ise standart güneş ışığı altında gerçekleşmiştir. Söz konusu örnekler kişilerin yüzleri sola dönük haldeyken, ayakta duran pozisyonda alınmıştır. Kamera ile kişi arasındaki açı dikkate alınmayıp, mesafe olarak genelde birkaç metre uzaklıktan çekim yapılmıştır. 17 ile 50 yaş arasında 50 gönüllüden farklı açılarda dörder fotoğraf alınarak toplamda 200 fotoğraf elde edilmiştir. Ön hazırlık adımında alınan görüntüler otomatik olarak yeniden boyutlandırılmış ve 8-bitlik gri tonlamalı görüntü haline getirilmiştir. Her birey için çekilen üçer fotoğraf veri tabanına kaydedilmiş, dördüncü fotoğraf ise test için kullanılmıştır. Kulak bölümlene aşaması başarılı bir doğrulamanın ön şartı olduğundan bu adımda kulak bölgesindeki gerekli olmayan bilgilerden arındırma işlemi yapılmıştır. İstenmeyen gürültüyü önlemek için Taraflı Normalleştirilmiş Kesim algoritması (Bianced normalized cut - BNC) kullanılmıştır. BNC uygulandıktan sonra hala istenmeyen bağımsız pikseller kaldıysa bunları yok etmek için de Entropi fonksiyonu kullanılmıştır. Kulak sınırlarını arka planından bölmek için de genel eşikleme yapılmıştır. Kulak bölümlenenin son aşamasındaki morfolojik işlemler adımı; iskeletleştirme (skeletonization), doldurma (filling), açma (opening) işlemleri yapılmıştır. Log-Gabor dalgacıkları kullanarak kulak görüntüsü istenen formda kodlanmış hale getirilmiştir. Elde edilen kodlanmış haldeki kulakları eşleştirmek için Hamming uzaklığı kullanılmıştır. Tüm bu adımlardan sonra yapılan çalışma ile kulak görüntüsünden kimlik doğrulama işleminde ortalama % 92.66'lık bir başarıya ulaşılmıştır.

Alay-ay ve diğ (2015) yaptıkları çalışmada Temel bileşen analizi (PCA) yöntemi ile kulak görüntüsünden kimlik belirleme işlemi yapmışlardır. Sistemin ara yüzü Visual C# ve MatLap'da geliştirilirken, arka planda MS-SQL kullanılmıştır. Çalışmada kullanılan kulak görüntüleri fotoğraf makinesi ile kullanıcıların sağ kulağından alınmış, JPEG formatındaki görüntülerdir. Normalizasyon adımımda tüm görüntülerin boyutu standart bir hale ölçeklenmiştir. Kulak olmayan bölümler ve saç gibi arka plan görüntüleri maskelenmiştir. Daha sonra Canny Kenar Tespit etme ile özellik çıkartılmıştır. Eğitim aşamasında öz değer ve öz vektörler çıkartılmıştır. Bu işlemden sonra çıktı olarak JPEG formatında öz vektörlerden oluşan görüntü elde edilmiştir. Veri tabanına kaydedilen bu görüntüler daha sonra kimlik doğrulama aşamasında eşleştirildiğinde farklı ışık kaynağı, poz açısı ve kameradan uzaklığa göre başarı oranının da değiştiği görülmüştür. Çalışma ortalama % 85.66'lık tanılama başarımına sahiptir.

Galdemez ve diğ. (2014) yaptıkları çalışmada test aşamasındaki başarıyı artırmak için ön işlem olarak Hausdorf uzaklığını kullanmışlardır. Özellik çıkartımı aşamasında Temel bileşenler Analizi (Principal Component Analysis - PCA) ile Lineer Diskriminant Analizi (Linear Discriminant Analysis - LDA) birlikte uygulamışlardır. Daha sonra rotasyondan bağımsız bir ölçek ile anahtar noktalar olarak adlandırılan ilgili noktaları tespit etmek için SURF (Speeded Up Robust Features) algoritmasını kullanmışlardır. Farklı bireylere ait 300 denemede ortalama % 97 başarıya ulaşmışlardır.

## 3. BİYOMETRİ

### 3.1 Biyometri Nedir

Biyometri; kelime kökeni olarak Yunanca yaşam anlamına gelen ön ek biyo (*bios*) ile yine yunanca ölçüm anlamına gelen son ek metri (*-metria*) kelimelerinin birleştirilmesiyle oluşmuştur. Bu durumda biyometri; yaşama ve insana dair özellikler ile ilgili ölçümlerdir.

İnsanlar binlerce yıldır birbirlerini tanımak için yüz, ses, yürüyüş gibi vücut özelliklerini kullanmışlardır (Jain ve diğ. 2004).

İnsan etkileşiminin sadece aynı ortamda bulunan kişilerle sınırlı olduğu dönemlerin aksine, günümüzde etkileşimde olduğumuz kişilerin sınırı belirsizleşmiştir. Kişiler arası bu sınırın belirsizleşmesinde en öneml, rol internet ve teknoloji alanındaki gelişmelerdir. İnternet, küresel ve yerel olan arasındaki sınırları belirsizleştirerek iletişim ve etkileşimde yeni kanallar açmıştır (Denizci 2009).

Çağdaş toplumlarda, otomatikleştirilmiş insan tanıma için kullanılan makine tanıma sistemlerinin geliştirilmesine yönelik artan bir ilgi söz konusudur. Adli tıptan milli güvenliğe kadar çeşitli uygulamalar ile biyometri, modern toplumun ayrılmaz bir parçası haline gelmiştir. (Singh ve diğ. 2014).

Biyometrik; tanımak veya kimlik doğrulaması yapmak için bireylerin benzersiz fiziksel ve davranışsal özelliklerini ölçmektir (Liu ve Silverman 2001).

Bireye ait her karakteristik özellik biyometri değildir. İnsana ait herhangi bir karakteristik özelliğin biyometrik olarak değerlendirilebilmesi için aşağıdaki şartları sağlaması gerekmektedir.

- Evrensellik : Her insan bu karakteristiğe sahip olmalıdır.
- Ayırt edicilik : Herhangi iki kişi sahip olduğu bu karakteristik açısından yeterince farklı olmalıdır.

- Devamlılık : İlgili karakteristik belli bir zaman süresi zarfında yeteri kadar değişmeyen olmalıdır.
- Elde edilebilirlik : Karakteristik nicel olarak ölçülebilir olmalıdır.

Bununla birlikte, pratik bir biyometrik sisteme (örneğin, kişisel biyometrik tanıma için kullanan bir sistemde) dahil edilmesi gereken bir takım maddeler de vardır. Bu maddeler aşağıda verilmiştir.

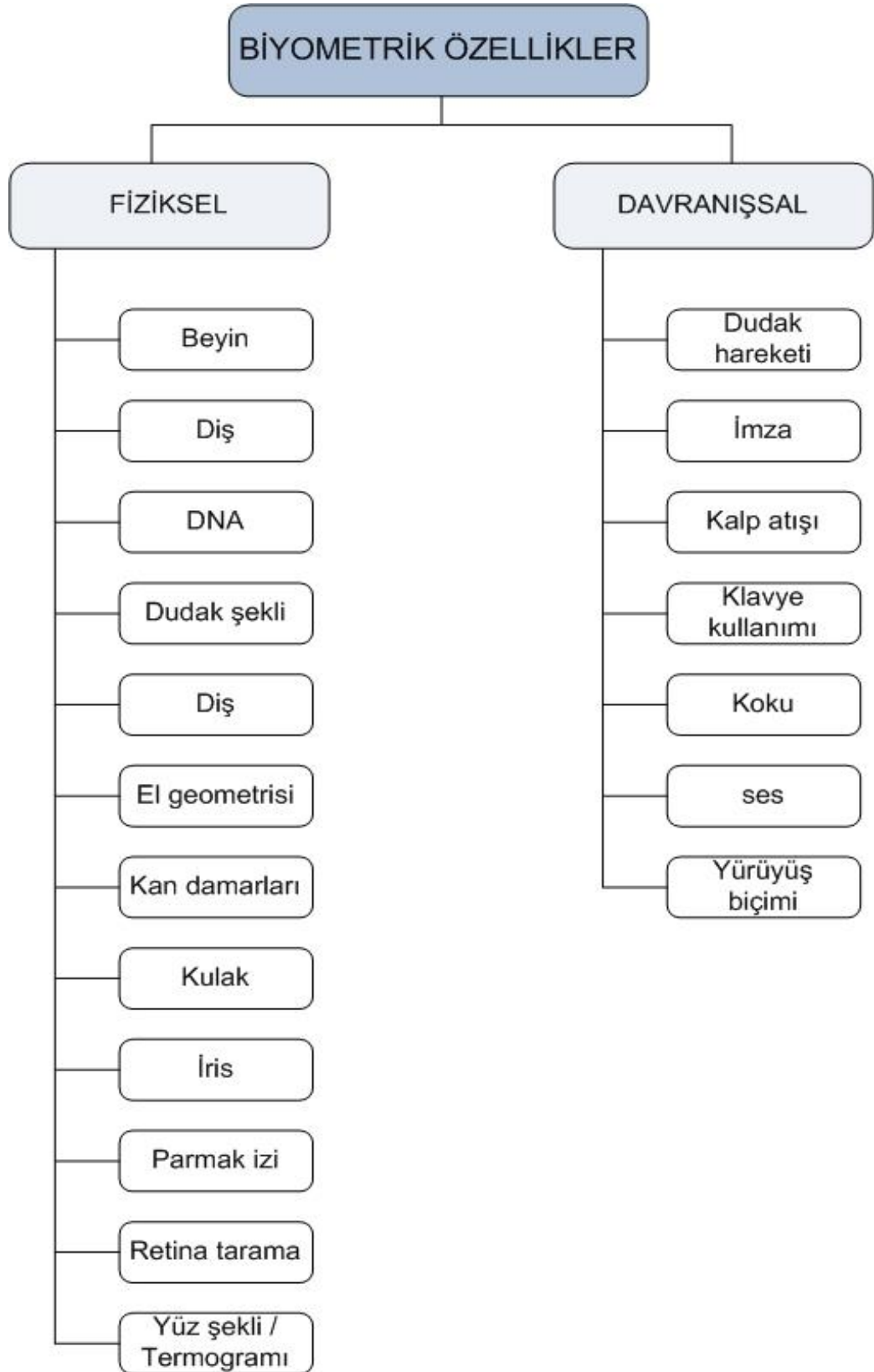
- Başarım : Operasyonel ve çevresel faktörlerin etkisinde dahi beklenen tanımlama doğruluğunu ve hızını sağlamalıdır.
- Kabul edilebilirlik : İnsanların günlük yaşamlarında belirli bir biyometrik tanımlayıcıyı kullanmayı kabul etmeleridir.
- Atlatılabilirlik : Hileli yöntemler kullanarak sistemin kandırılmamasıdır (Jain ve diğ. 2004).

### **3.2 Fiziksel ve Davranışsal Biyometrik Karakteristikler**

Biyometrik veri olarak kabul edilen, evrensellik, ayırt edicilik, devamlılık, elde edilebilirlik gibi özellikleri taşıyan fiziksel ve karakteristik bazı özellikler Şekil 3.1’de gösterilmiştir.

#### **3.2.1 Beyin**

Beyin dalga örüntüleri oldukça bireyseldir. Tamamıyla aynı şekilde düşünen iki insan yoktur. Beyinden gerekli biyometrik imzayı elde etmenin iki yolu var. Bu yollardan ilki kullanıcıya elektrotlarla kaplı bir şapka giydirilerek birçok noktadan EEG verisi toplamaktadır. Diğeri ise MR görüntülemedir. MR görüntüleme yöntemi büyük cihazlar gerektirir ve istenen özelliğin elde edilmesi uzun zaman alır. Beyin ile biyometrik tanımlama yapmak zor ve maliyetli olduğundan pratikte ilk başvurulacak yöntem değildir. Örneğin banka hesabına ulaşmak için beyin dalgaları kullanılmaz fakat üst düzey bir askeri komutanı tanımlamak için kullanılabilir (Bodhani 2013).



**Şekil 3.1:** İnsana ait fiziksel ve davranışsal biyometrik karakteristikler

### 3.2.2 Diş

Emniyet ve kolluk kuvvetlerinde ölmeden hemen önceki (Antemortem )adli tanımlama kadar ölümden sonraki (Postmortem) kişi tanımlama da yapılabilir (Fahmy ve diğ. 2005).

Yangın veya çarpışma gibi kitlesel felaketlerde veya yumuşak dokuların çürümesi sonucunda kurban postmortem tanımlama yapabilmek için davranışsal ve fiziksel özellikleri uygun değildir. Bu durumda vücudun en zor hasar alan parçası olarak dişler postmortem tanımlama için en uygun aday haline gelmektedir (Lin ve diğ. 2010).

### 3.2.3 DNA

Deoksiribo Nükleik Asit kişinin bireyselliğini gösteren mükemmel olarak tanımlanabilecek benzersiz bir koddur. Ancak günümüzde kişi tanımlama için çoğunlukla adli uygulamalar alanında kullanılmaktadır. Farklı uygulamalarda bu biyometriyi kullanmayı kısıtlayan bazı konular vardır. Bunlar:

- Duyarlılık sorunu: Gizli bir amaç için hiç kuşulanılmayacak bir vücut parçasından bir parça DNA örneği çalmak kolaydır.
- Otomatik gerçek zamanlı tanımlama sorunu: Günümüz şartlarında DNA eşleştirme birtakım kimyasal yöntemlere ve uzmanlık bilgisine ihtiyaç duymaktadır.
- Gizlilik sorunları: Kişinin mahremiyetinde kalmasını istediği bazı hastalıklar DNA örneği ile anlaşılabilir. Ayrıca genetik kod bilgisi istenmeyen ayrımcılığa neden olabilir (Jain ve diğ. 2004).

### 3.2.4 El Geometrisi

El geometrisi sistemi insan elinden, şeklinden, avuç içi ve parmakların boyutundan alınan bir dizi ölçüme dayanmaktadır. Ticari el geometrisi tabanlı doğrulama sistemleri dünyanın yüzlerce farklı yerinde kurulmuştur. Bu yöntem diğerlerine nispeten uygulaması kolay ve ucuzdur. Islak hava, kuru cilt gibi kişisel anomaliler gibi çevresel faktörlerin de el geometrisini elde etmeye olumsuz bir



katkısı yoktur. Fakat parmağa takılan yüzük gibi takılar ve doğru el geometrisini almadaki becerinin sınırlamaları bu yöntemin olumsuzlukları arasındadır. Ayrıca el geometrisi tabanlı bir sistemin fiziksel boyutu büyük olduğundan dizüstü bilgisayarlar gibi bazı cihazlarda gömülü olamaz (Jain ve diğ. 2004).

### **3.2.5 İris**

İçten göz bebeği (pupil) ve dıştan gözün beyaz kısmı (sclera) tarafından sınırlanan, halka şeklindeki damarlı bölgedir. İrisin görsel dokusu fetus gelişimi sırasında meydana gelir ve yaşamın ilk iki yılında stabilize olur. Karmaşık iris dokusu kişisel tanıma için yararlı ve farklı bilgiler taşır. Tek yumurta ikizleri de dahil her iris kişiye özel ve ayırt edicidir. Ayrıca, yapay irisleri (örneğin, kontakt lensler) tespit etmek oldukça kolaydır. İlk iris tabanlı tanıma sistemlerinde kullanıcı katılımı zor ve maliyeti yüksek olmasına rağmen, yeni sistemler daha kullanıcı dostu ve uygun maliyetli hale gelmiştir (Jain ve diğ. 2004).

### **3.2.6 Parmak İzi**

Parmak izleri kişi tanımlama ve doğrulama için en yaygın olarak kullanılan biyometrik özelliktir (Kamble ve Gawali 2012). İnsanlar yüzyıllar boyunca kimlik tanıma amaçlı parmak izlerini kullanmışlar ve parmak izi ile sağlanan eşleşme doğruluğunun çok yüksek olduğu gösterilmiştir (Maio ve diğ. 2002).

Bir parmak izi parmak ucu yüzeyindeki kabartılar ve girintilerin şekliyle oluşmaktadır ve cenin gelişiminin ilk yedi ayında belirlenir. Günümüz itibari ile ABD’de bir parmak izi tarayıcısının maliyeti yaklaşık 20 dolardır. Bu yüzden kişisel diz üstü bilgisayarlar gibi pek çok alanda parmak izi tarama tabanlı uygulamalar kolay karşılanabilir maliyettedir. Bir kaç yüz kişiyi kapsayan küçük ve orta ölçekli doğrulama sistemleri için parmak izi tanıma sistemleri yeterlidir. Bir kişiye ait birden fazla parmak izi örneği alınması ise milyonları kapsayan geniş ölçekli kimlik tanıma işlemi için ek bilgi sağlamaktadır. Parmak izi biyometrisinin dezavantajı ise genetik faktörler, yaşlılık, kesik ve yaralar gibi durumlardan etkilenmesidir (Jain ve diğ. 2004).

### **3.2.7 Retina**

Gözbebeğine gelen ışığı ayarlayan göz küresinin arkasındaki ağ üzerindeki kan damarlarının görüntüsünü alır ve analiz eder. Retina şekli yüksek ayırt edici özelliklere sahiptir. Tek yumurta ikizleri dahil her göz kendine has bireysel bir şekle sahiptir. Her bir retina şekli insan hayatı boyunca sabit kalır. Fakat ciddi fiziksel yaralanmalar, yüksek kan basıncı ve diyabet gibi bazı hastalıklardan olumsuz etkilenebilir. Retinanın ufak bir alanı olması ve vücudun iç kısmında bulunması sebebiyle diğer çoğu biyometriye göre görüntü yakalamayı zorlaştırır. Ayrıca retina taraması sırasındaki ufak hareketler bile bu taramanın tekrar tekrar yapılmasına neden olabilir (Ashokkumar ve Thyagarajan 2013).

### **3.2.8 Yüz**

Yüz tanıma yanıtılması güç bir yöntemdir ve yüz görüntüleri muhtemelen kişisel bir tanıma yapmak için insanlar tarafından kullanılan en yaygın biyometrik özelliktir. Yüz tanımlama hareketsiz olarak çekilen sabıka kaydı fotoğraflarından, havaalanı gibi kalabalık ve karmaşık arka planlı hareketli ortamlardan alınan görüntülere kadara geniş bir alanda kullanımı mevcuttur (Jain ve diğ. 2004). Yüz tanıma sistemleri son 20 yılda aktif bir araştırma konusu olmuştur ve erişim kontrol sistemlerinde günümüzde yerini almış durumdadır. Bu biyometrik, kimlik tanımlamadaki en doğal yöntemdir. Parmak izi ya da iris görüntüsü elde etmedeki gibi dışarıdan müdahaleye gerek olmaması bir avantajıdır. Yüz tanıma sistemleri suç önleme, video gözetimi, kişi doğrulama gibi benzer güvenlik alanlarında kullanılabilir. Fakat yine de bazı saldırılara karşı savunmasızdır. Bunlar; sensöre biyometrik örneğin taklidinin sunulması gibi sistemi atlatmaya çalışan saldırılar veya biyometrik örneğin biçimini bozmaya yönelik yapılan saldırılardır (Hemalatha ve Wahi 2014).

### **3.2.9 Dudak Şekli ve Hareketi**

Konuşmacı tanımlama ve doğrulama için dudak biyometrisi kullanma son yıllarda pek çok araştırmacı tarafından büyük ilgi çekmiştir. Parmak izi, yüz, ya da

ses gibi bazı geleneksel biyometriklerden farklı olarak, dudak biyometrisi hem fizyolojik hem de davranışsal yönleri içerir. Fizyolojik olarak farklı insanlar farklı dudaklara sahiptir. Öte yandan, insanlar genellikle konuşma stilleri ile diğer insanlardan ayırt edilebilirlerdir. Dudak hareketleri bir video kamera tarafından kolayca elde edilebilir. Yüz tanıma, ses tanıma gibi kişi tanımlama sistemlerine doğrudan entegre edilebilir olması avantajlarından (Wang ve Liew 2012).

### **3.2.10 İmza**

İnsanın imza atış şekli bireyin karakteristik bir özelliği olarak bilinir. İmzalar yazma aracı ile temas ve az da olsa kullanıcı çabası gerektirse de, devlet işlerinde, yasal ve ticari işlemlerde kişisel tanımlama yöntemi olarak kabul görmüştür. İmza belli zaman dilimlerinde değişebilen, fiziksel ve duygusal durumlardan etkilenebilen davranışsal bir biyometriktir. Bazı insanların ardışık attıkları imzalar arasında bile fark olabilir. Ayrıca sistemi atlatmak için imza kopyalayan profesyonel sahtekarlar da olabilir (Jain ve diğ. 2004).

### **3.2.11 Kalp Atışı**

Bir kişinin kalp atışı sahte kimlikle kopyalanamaz ya da kimlik gizleme için kalp atışı değiştirilemez. Kalp atışı elektrokardiogram kaydı formunda elde edilir. Bir kişinin ECG'si kalbin anatomisi, boyut ve pozisyonuna göre, göğüs kafesi yapısına ya da diğer sebeplere bağlı olarak kişiden kişiye farklılık gösterir (Simon ve Eswaran 1997 ; Hegde ve diğ. 2011).

### **3.2.12 Klavye Kullanımı**

Her insanın klavyede karakteristik bir şekilde yazdığı varsayılmaktadır. Bu biyometrinin her insanda tam anlamıyla farklılık göstermesi beklenmiyor fakat yine de kimlik tanımlama için bazı ayırt edici bilgiler elde etmemize izin verir. Örneğin bir sistemde kişi herhangi bir bilgiyi anahtarlarırken tuş vuruş biçimi gözlenebilir (Jain ve diğ. 2004).

Tuş vuruş biyometrisi bazı nedenlerden dolayı cazip gelebilir. Öncelikle tuş vuruşu hem işi hem de şahsi işi gereği klavye kullanan bilgisayar kullanıcıları için müdahaleci bir yöntem değildir. Ayrıca tek gerekli donanımı bilgisayar ve klavye olduğundan oldukça ucuz maliyetlidir (Gunetti ve Picardi 2005).

### **3.2.13 Ses**

Fizyolojik ve davranışsal biyometrinin bir kombinasyonudur. Bireyin ses özelliği; ses yolları, ağız ve burun deliği, dudak yapısı gibi sesi oluşturan unsurların boyut ve şekline bağlıdır. İnsan konuşmasının bu fizyolojik özellikleri değişmezdir fakat sesin davranışsal bölümü yaş, tıbbi durumlar, grip ya da duygu durumuna bağlı olarak değişkenlik gösterebilir. Büyük ölçekli tanımlamalar için pek uygun değildir (Jain ve diğ. 2004).

Ticari alanda ses biyometrisine yapılan harcamalar son yıllarda yatay bir seyir izlemiş olsa dahi, ses biyometrisinin yükselen değerini ve gelir artışını gören endüstri bu yönde bir değişikliğe gitmektedir. Teknoloji şirketlerinin katılımı, uygulama geliştiriciler ve fırsatçı çözüm sağlayıcıları bu değişimin anahtarıdır. (Golden 2012).

Parola teknolojisi olarak ses biyometrisine güvenmemizin bir sebebi, onun basitliğindedir. Neticede hepimiz her an konuşuruz. Bir insanın kimliğini onaylaması için gerekli olan tek şey adını ya da telefonunu söylemek gibi doğal durumlardandır. Teknik ve piyasa açısından da durum basittir. Ses kolayca kayıt edilebilir ve ses tanımlama için temel basit donanımlar yeterlidir (Khitrov 2013).

### **3.2.14 Yürüyüş Biçimi**

Bir kişinin kendine özgü şekilde yürümesinin biyometrisidir ve karmaşık bir uzay-zaman biyometrisidir. Yürüme biçimi davranışsal bir biyometridir ve zaman içinde değişmeyen bir özellik değildir. Özellikle uzun zaman dilimleri içerisindeki vücudun kilo dalgalanmaları beyindeki hasarlar yaşlılık veya sarhoşluk gibi nedenlerden dolayı değişim gösterebilir. Yürüme biçiminin edinimi yüz resmini elde etmeye benzer olduğundan kabul edilebilir bir biyometridir (Jain ve diğ. 2004).

## 4. KİMLİK TESPİTİ VE GÜVENLİK

Günümüz modern organizasyonları için bilginin çok önemli bir etken olduğu inkar edilemez. O yüzden bilginin güvenliğini sağlamak çoğu organizasyon için ilk öncelik sırasındadır. Fakat bilgi güvenliğini tamamen garanti altına alabilecek tek bir formül mevcut değildir. Bu yüzden gerekli güvenliği sağlamak için bir dizi uygulama ve bir takım standartlara ihtiyaç var.

Bilgi kuruluşların can damarı ve günümüz etkin dünyasında önemli bir ticari varlıktır. Sağlam kararlar alabilmek için, yönetsel karar alma sürecini destekleyen kaliteli, doğru, tam ve güncel bilgiye ulaşmak hayati önem taşır. Kaynakların iyi korunmasını sağlamak için bilgi sistemleri kaynaklarının güvenliğini sağlamak son derece önemlidir. Bilgi güvenliği, kullanıcı adı ve bir parolaya sahip olmak kadar basit bir olay değildir (Solms ve Solms 2004).

Zararlı yazılımlar, kimlik avcıları ve sosyal mühendisler bir kuruluşu her yönden tehdit eden unsurlardır (Susanto ve diğ. 2011).

Güvenlik alanı üç farklı kimlik doğrulama kullanır.

- Kodlanabilir bilgi : Parola, pin kodu, ya da kişiye özel bir bilgi (Örneğin annenin kızlık soyadı).
- Fiziksel bir araç : Kart anahtar, akıllı kart, güvenlik kartı
- Doğal bir özellik : Biyometri

Bu üçünden en kapsamlı ve en güvenli kimlik doğrulama aracı biyometridir (Liu ve Silverman 2001).

Biyometrik teknolojiler geleneksel kimlik doğrulama yöntemlerine göre daha fazla avantaj sunar. Bilgi tabanlı ya da kart tabanlı sistemlerle karşılaştırıldığında, biyometri daha doğru, hassas sonuç verir, kopyalaması zordur. Biyometride parola hatırlama gerekmez, kimlik taşımaya gerek olmaz (Ngugi ve diğ. 2011; O’Gorman 2004).

## 5. GÖRÜNTÜ İŞLEME

### 5.1 Görüntü İşleme Nedir

Görüntü, iki-boyutlu ışık şiddeti fonksiyonudur. Bir görüntü  $f(x,y)$  şeklinde iki-boyutlu bir fonksiyon olarak ifade edilirse; burada  $x$  ve  $y$  uzaysal (düzlemsel) koordinatlarıdır. Herhangi bir  $(x,y)$  koordinat çiftindeki  $f$  sayısal değeri, görüntünün o noktadaki rengini temsil eder.

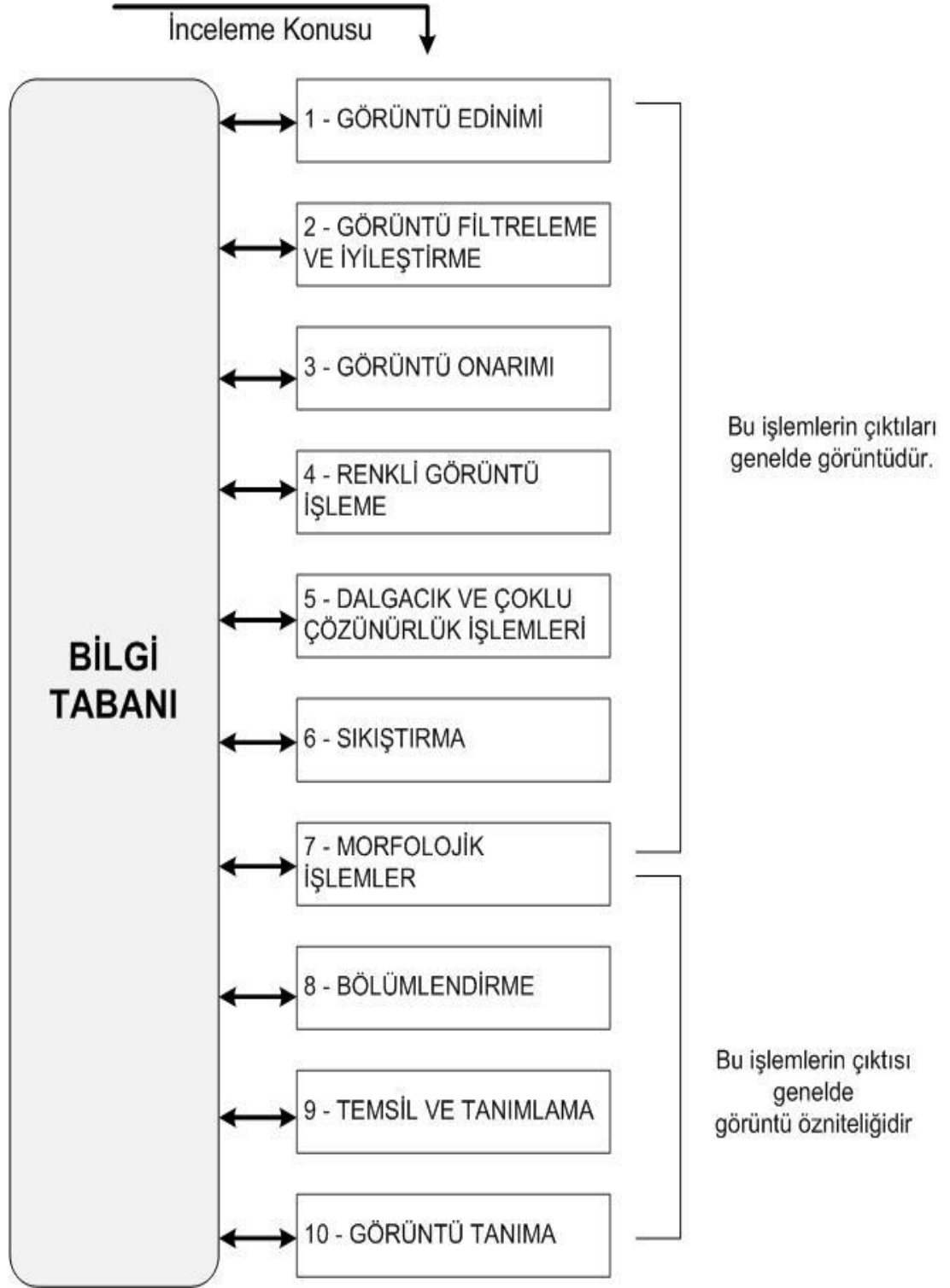
$f$  fonksiyonunun değeri ile  $x$  ve  $y$  değerlerinin tümü sonlu olduğunda, görüntü sayısal görüntü olarak adlandırılır. Sayısal görüntü işleme, belirli bir amaç için bilgisayarlar vasıtasıyla görüntü üzerinde gerçekleştirilecek olan işlemleri kapsar. Bir sayısal görüntü; her biri belli bir konum ve değere sahip sonlu sayıda elemandan oluşmuştur. Görüntüyü oluşturan bu en küçük resim parçalarına piksel adı verilir.

### 5.2 Görüntü İşlemenin Temel Adımları

Görüntü işlemenin temel adımları Şekil 5.2 'de gösterilmiştir.

#### I. Görüntü Edinimi(Image Acquisition)

Görüntü elde etmedeki ilk süreçtir. Genel olarak bu adımda görüntü ölçekleme gibi ön işlemler yapılır. Bir görüntüyü almak için çok farklı yöntemler (fotoğraflama, MR çekimi, ultrason) olsa da asıl amaç algılanan veriden sayısal görüntüler elde etmektir. Algılanan görüntüyü sayısal forma çevirmek iki işlem gerektirir. Bunlar, koordinat değerlerini sayısallaştırma anlamına gelen örnekleme ve genlik değerlerini sayısallaştırma anlamına gelen nicemleme işlemleridir (Gonzales ve Woods 1992).



Şekil 5.2: Görüntü işleme temel adımları

## II. Görüntü Filtreleme ve İyileştirme (Image Enhancement)

Burada amaç özel bir uygulamada kullanabilmek için görüntünün orijinal halinden daha uygun bir hale çevirme işlemidir. Genel bir görüntü iyileştirme teorisi yoktur. Görüntü üzerinde gerçekleştirilecek olan iyileştirme işlemleri uygulamadan uygulamaya değişiklik arz eder. Belirli bir yöntem için hangi iyileştirmenin yapılması gerektiği konusunda karar verici gözlemcidir (Gonzales ve Woods 1992). Başlıca görüntü iyileştirme yöntemlerine örnek olarak: parlaklık ve kontrast düzeltme, görüntü negatifleştirme, logaritmik dönüşüm, gri seviye dönüşümleri, histogram işlemleri, eşikleme dönüşümü, yoğunluk dönüşümü verilebilir (Maini ve Aggarwal 2010).

## III. Görüntü Onarımı(Image Restoration)

Görüntü onarımı yöntemi de görüntünün görünümünü iyileştirme ile ilgilenen bir alandır fakat öznel olan görüntü iyileştirme adımının aksine bu adım nesnedir. Bu adım matematiksel ve olasılık modele dayalı olarak görüntüyü düzeltme eğilimindedir. Restorasyon yönteminde eldeki görüntünün orijinal halinin düzgün olduğu kabul edilir. Görüntüde oluşan bozulmayı modelleyip, orijinal görüntüyü kurtarmak için ters işlem uygular. Gürültü giderme, bulanıklık giderme ve odak kusurlarını düzeltme gibi işlemler görüntü onarım tekniklerindedir.

## IV. Renkli Görüntü İşleme (Color Image Processing)

Renkli görüntü her bir pikselinde renk bilgisi barındıran bir sayısal görüntüdür. Renkli görüntü işleme, internetteki sayısal görüntülerin kullanılmasındaki gözle görülür artış ile gittikçe önem kazanan bir adımdır. Görüntü işlemede renk kullanımının iki temel sebebi vardır. İlki obje tanımayı kolaylaştırmada renk güçlü bir tanımlayıcıdır, ikincisi insanlar gri renk tonuna kıyasla binlerce tonda ve yoğunlukta renk algılayabilir. Renk dönüştürme, ton düzeltme, keskinleştirme işlemleri renkli görüntü işlemeye örnek olarak verilebilir.

## V. Dalgacık ve Çoklu Çözünürlük İşlemleri (Wavelets and Multiresolution Processing)



Dalgacıklar çözünürlüğün farklı derecelerindeki görüntüleri temsil eder. Çoklu çözünürlük teorisi, bir görüntünün birden fazla farklı çözünürlükte analiz eder.

#### VI. Sıkıştırma (Compression)

Adından da anlaşılacağı üzere sıkıştırma adımı, bir görüntüyü kaydetmek için gereken depolama alanını azaltmak ya da o görüntüyü iletmek için gerekli olan bant genişliğini azaltmak işleminin yapıldığı adımdır. Son yıllarda depolama teknolojisinde belirgin bir artış olsa da aynı durumun iletim kapasitesinde geçerli olduğu söylenemez. Belki de bu yüzden sayısal görüntü işleminin en gerekli ve ticari olarak en önemli alanlarından.

#### VII. Morfolojik İşlemler (Morphological Processing)

Morfoloji kelimesi genelde biyolojinin bir dalı olarak bilinse de burada bahsedilen matematiksel morfolojidir. Matematiksel morfoloji, şekil alanının tanıtımı ve sunumu için gerekli olan görüntü bileşenlerini ayıklamak için gerekli olan araçlardır. Görüntü işlemede genelde filtreleme, inceltme, budama gibi ön veya son işlem olarak kullanılan morfolojik tekniklerin olduğu adımdır. Ayrıca aşındırma, genişletme, açma ve kapama önemli morfolojik işlemlerdir.

#### VIII. Bölümlendirme (Segmentation)

Bölümlendirme bir görüntünün, kendisini oluşturan parçalara bölünme prosedürüdür. Genel olarak özerk çalışan otonom bir bölümlendirme görüntü işleminin en zor görevlerindedir. Sağlam bir bölümlendirme prosedürü, görüntüleme problemlerinin çözümünde başarılı bir yol sunar. Başka bir deyişle; görüntü tanımlamanın başarılı bir şekilde olması, bölümlenmenin doğruluğuna bağlıdır.

#### IX. Temsil ve Tanımlama (Representation and Description)

Çoğu zaman bölümlendirme adımından sonra gelir. Bir görüntü alanlara bölümlendikten sonra, bölümlenen piksellerden oluşan küme bilgisayar işlemesi için uygun formdadır. Belli bir alanın “temsili” onun sınırlarını

belirtir, “tanımlaması” ise sınırları belirlenen o alandaki söz konusu piksellerin ayırt edici özelliğini verir

#### X. Görüntü Tanıma (Object Recognition)

Son olarak da görüntü tanıma, kendi tanımlayıcılarının verdiği bilgilere dayanarak bir nesneye etiket atama işlemidir.

Bir problemin etki alanı hakkındaki bilgi, görüntü işleme sisteminde bilgi tabanı formunda temsil edilir. Bilgi tabanı, her bir işlem modulünün yönetimine klavuzluk ederken veyodüller arası etkileşimi de kontrol altında tutar (Gonzales ve Woods 1992).

## **6. BİYOMETRİK SİTEMLERDE GÖRÜNTÜ İŞLEME İLE KİMLİK TESPİTİ VE GÜVENLİK**

### **6.1 Biyometrik Sistem Nedir**

Bir biyometrik sistem, bir bireyden biyometrik veriyi elde etme, elde edilen veriden özellik seti çıkarma ve veri tabanındaki örnek küme ile bu özellik kümesini karşılaştırma işlemlerini yöneten bir görüntü tanıma sistemidir (Jain ve diğ. 2004). Biyometrik sistem uygulama kapsamına bağlı olarak farklılık gösterse de genelde üç temel işlem adımını içerisinde barındırır. Bunlar; kayıt, doğrulama ve tanımlamadır.

#### **6.1.1 Kayıt (Enrollment)**

Görüntüsü alınacak nesneden biyometrik referansların toplanması ve bu verilerin depolanması ile ilgilidir. Bu işlem için sistem yöneticisinin kullanıcı bilgilerini sisteme sunması ve fonksiyonu çalıştırması gerekmektedir. Bunun yanı sıra biyometrik verisi alınacak kullanıcı biyometrisini sisteme sunmalıdır. Her şey yolunda gittiği takdirde, görüntüsü alınacak nesneden referans bilgileri alınır ve depolanır (Saavedra ve diğ. 2013).

#### **6.1.2 Doğrulama (Verification)**

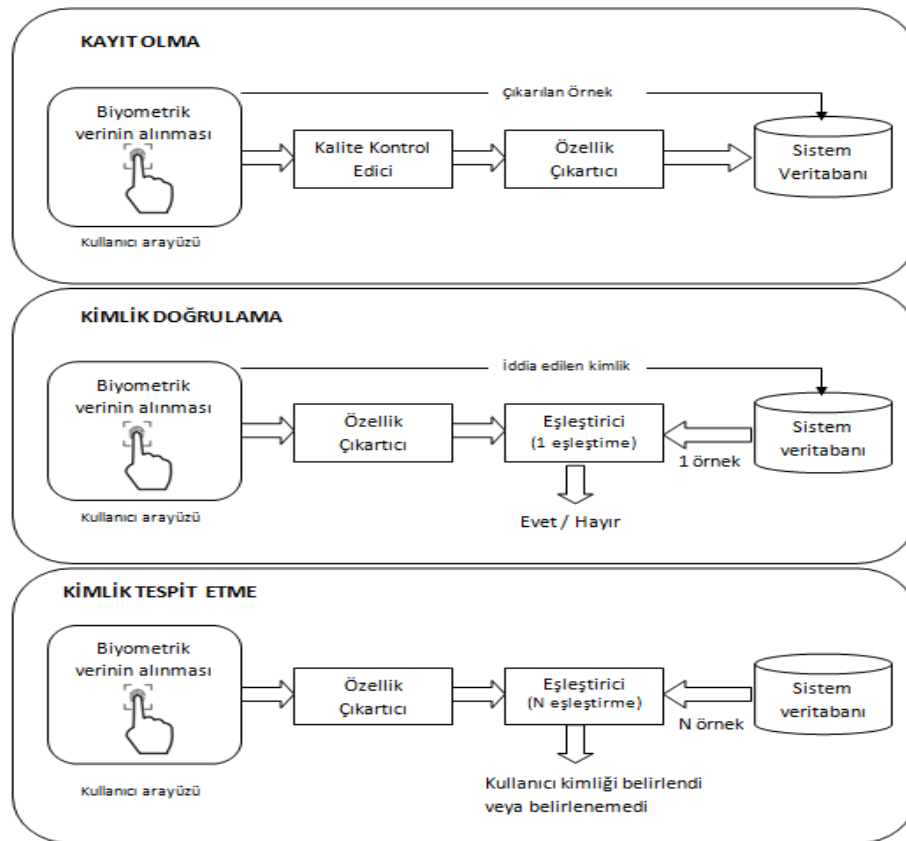
Sistem, görüntüsü alınan kişideki biyometrik veriyle, yine söz konusu kişiye ait daha önceden sistem veri tabanında kaydedilen biyometrik veri örneğini karşılaştırır. Bu gibi sistemlerde tanınmak isteyen kişi bir kimlik iddia eder. Sistemde birebir bir karşılaştırma yaparak, iddia edilen kişi gerçekten iddia ettiği kişi mi değil mi diye bakar. Doğrulama sistemleri genelde, birden çok insanın tek bir kimlik kullanmasını engellemeyi amaç edinen “pozitif tanıma” yöntemi için kullanılır (Jain ve diğ. 2004; Wayman 2001; Faundez-Zanuy 2006).

### 6.1.3 Tanımlama / Kimlik Belirleme (Identification)

Sistem bireyin kimliğini tanıyabilmek için veri tabanındaki tüm kullanıcı örnekleriyle bireyin biyometrik verisini eşleştirmeye çalışır. Birey sisteme herhangi bir kimlik iddia etmez. Bu nedenle sistem bireyin kimliğini tanımlayabilmek için bire- çok karşılaştırma yürütür. Kimlik belirleme negatif tanıma yöntemi için önemli bir bileşendir. Negatif tanımda amaç bir kişinin birden çok kimlik kullanmasına engel olmaktır. Kimlik belirleme pozitif tanıma için de kullanılabilir. Burada kolaylık olarak kullanıcının herhangi bir kimlik iddia etmesine gerek olmaz.

Geleneksel şifre, pin, anahtar, jeton ve kart gibi geleneksel yöntemler pozitif tanıma için geçerli olsa da negatif tanıma sadece biyometrik veri aracılığıyla yapılabilir (Jain ve diğ 2004; Saavedra ve diğ. 2013; Zanuy 2006).

Şekil 6.3’de biyometrik sistemlerde genel kullanımda olan kayıt, kimlik doğrulama, kimlik tespit etme uygulamalarının işleyişi gösterilmiştir.



Şekil 6.3: Biyometrik sistemde genel kullanımda olan üç uygulama; kayıt, kimlik doğrulama ve kimlik tespit etme.

## 6.2 Biyometrik Sistem Çalışma Prensibi

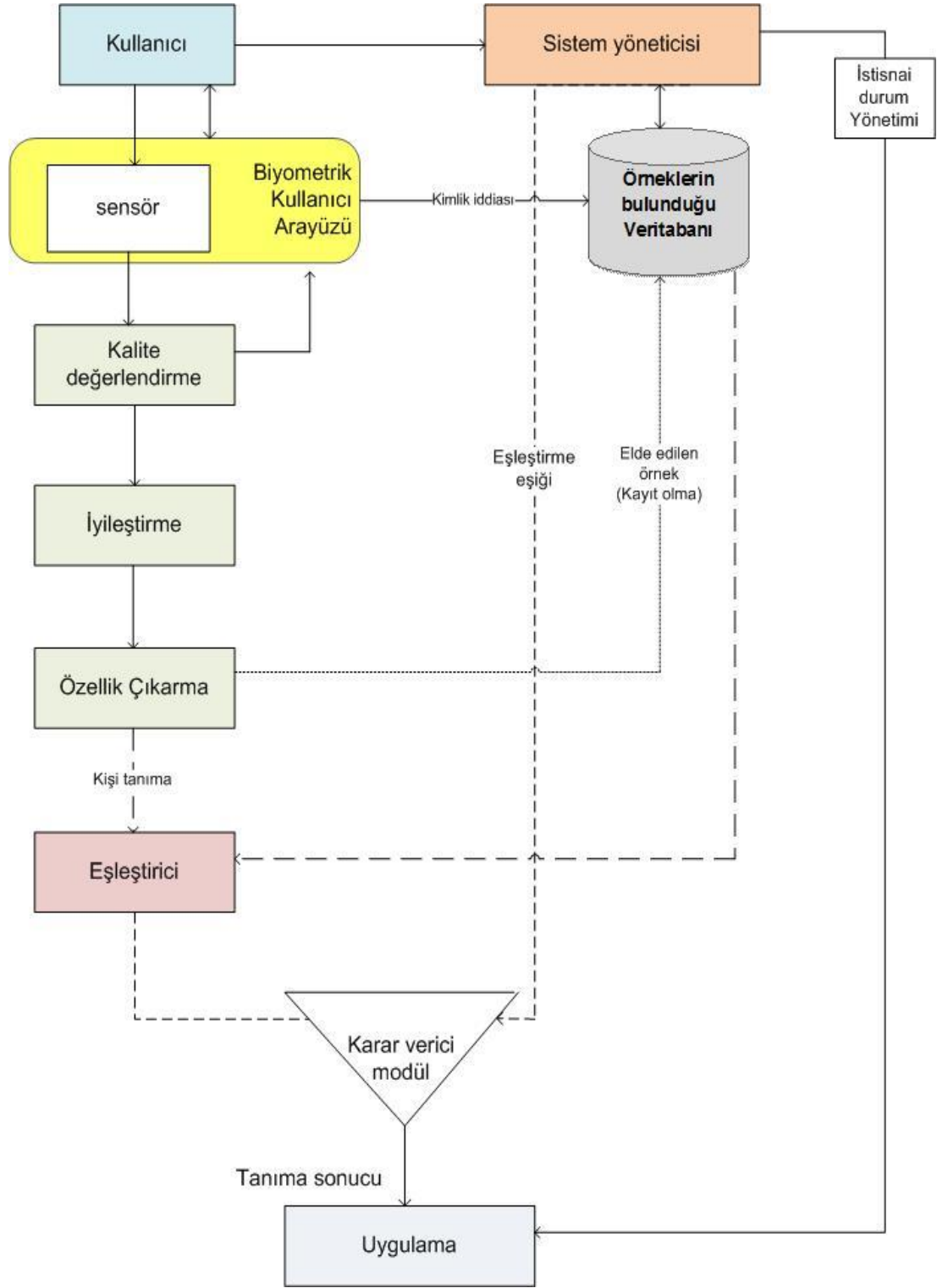
Genel itibari ile biyometrik sistemler ardışık olarak Şekil 6.4’de gösterildiği gibi yedi temel modülden oluşmaktadır. Bunlar

- Biyometrik okuyucu ihtiva eden bir kullanıcı ara yüzü veya sensör,
- Elde edilen biyometrik örneğin diğer işlemler için yeterli kaliteye sahip olup olmadığını belirleyen bir kalite kontrol modülü,
- Biyometrik sinyal kalitesini geliştirmek için bir donanım modülü,
- Kişi tanıma görevi için uygun olan biyometrik örnekten sadece gerekli bilgiyi ayıklayan bir özellik çıkarıcı,
- Kullanıcının biyografik bilgileriyle birlikte çıkartılan özellikleri depolayan bir veri tabanı,
- Tanıma ve benzerlik oranını belirlemek için iki özellik kümesini karşılaştıran bir eşleyici,
- Eşleyici tarafından belirlenen benzerlik çıktısına dayanarak kişinin kimliğini belirleyen karar modülüdür.

Genelde bütün biyometrik sistemler benzer temel modüllerden oluşur ve bu sistemi kurmak için üç ana adım vardır. İlki tasarımcı biyometrik sistem için en uygun mimariyi seçer. Daha sonra seçilen mimariye uygun olarak gerekli yazılım ve donanım bileşenleri seçilir. Son olarak da biyometrik sistemin etkin verimli bir biçimde uygulanabilmesi için uygun kurallar tanımlanır.

## 6.3 Biyometrik Sistemlerin Karşılaştırılması

Bir biyometrik sistemde kullanılacak biyometrik veri sistemin gereksinimlerine göre seçilir. Bazı biyometrik verilerin ayıricılığı yüksekken bazılarının kullanıcılar tarafından kabul edilebilirliği yüksektir. Kimisi daha kolay atlatılabilirken, kimisinin kalıcılığı daha azdır. Tüm biyometrik veriler biyometrik özellik şartlarını sağlar fakat her birinin güçlü ya da zayıf yönleri vardır. Tablo 6.1’de farklı biyometrik veriler kullanan sistemlerin zayıf ya da güçlü olduğu özellikleri karşılaştırılmaktadır.



Şekil 6.4: Biyometrik sistem çalışma prensibi

**Tablo 6.1:** Biyometrik sistemlerin karşılaştırılması (Y: yüksek, O: orta, D: düşük) (Jain ve diğ. 2004)

	Evrensellik	Ayrırcılık	Devamlılık	Elde Edilebilirlik	Başarım	Kabul Edilebilirlik	Atlatılabilirlik
DNA	Y	Y	Y	D	Y	D	D
Yüz	Y	D	O	Y	D	Y	Y
Parmak İzi	O	Y	Y	O	Y	O	O
El Geometrisi	O	O	O	Y	O	O	O
İris	Y	Y	Y	O	Y	D	D
Retina	Y	Y	O	D	Y	D	D
İmza	D	D	D	Y	D	Y	Y
Ses	O	D	D	O	D	Y	Y
Kulak	O	O	Y	O	O	Y	O
Yüz Termogramı	Y	Y	D	Y	O	Y	D
Tuş Vuruş Hızı	D	D	D	O	D	O	O
Yürüyüş	O	D	D	Y	D	Y	O
Koku	Y	Y	Y	D	D	O	D
El Damarları	O	O	O	O	O	O	D

#### 6.4 Biyometrik Sistemlerin Uygulama Alanları

- **Hukuk, emniyet alanı** : Biyometrik teknolojiler suçlu olduğu iddia edilen kişilerin tespitinde güvenli bir araç olarak uzun zamandır kullanılmaktadır. Örneğin parmak izi kullanılarak bireyin suç kaydı olup olmadığı ya da gerçekleşen bir olaydaki parmak izinin kime ait olduğunu bulmak için merkezi kayıtlardaki depolanan parmak izleri karşılaştırılır. Mevcut durumda FBI sivil ve suçlulara ait elinde tuttuğu 10 milyonlarca parmak izi kaydı ile en büyük biyometrik veritabanlarından birine sahiptir.
- **Özgeçmiş Denetimleri** : Biyometrik teknolojiler gerek devlet gerekse ticari alanda çalışan istihdamında özgeçmiş kontrolünde kullanılır. Özgeçmiş ya da sabıka kaydı kontrolleri suçlu aramalarındakiyle aynı veri tabanı

kullanılır. Fakat suçlu tespitindeki gibi alınan biyometrik veri kayıt altına alınmaz ve kontrol sonrası silinir.

- Gözetim : Biyometrik teknolojiler herhangi bir görüş alanındaki veya belli bir alandaki bir kişiyi tespit etmek, izlemek ya da kimlik tespiti yapmak için kullanılır. Tarihsel olarak bakıldığında gözetim uygulamaları oldukça zahmetli, vakit alıcıydı. Kamera görüntülemesi için monoton olarak izleme yapmak gerekiyordu. Otomatik yüz tanıma sistemi ile bu işlem tamamen otomatikleştirilmiştir. Biyometrik gözetim sistemi sayesinde takip edilmesi gereken söz konusu birey bulunduğu anda yetkilileri uyaran bir uygulama geliştirilebilir.
- Sınır kontrolü : Giderek artan uluslararası seyahat hacmi ile daha hızlı, otomatikleştirilmiş, kolay sınır geçiş teknolojisine ihtiyaç olmuştur. Uluslararası standartlara uygun biyometrik özellikli pasaportlar kullanılmaya başlanmıştır. Sınır kontrolü uygulamaları için parmak izi, iris, ve yüz tanıma teknolojileri kullanılmaktadır.
- Dolandırıcılık azaltma : Biyometrik teknolojiler kamu sektöründe sahte kimlik kullanarak kar elde etmeye çalışan bireyleri engellemek için kullanılabilir.
- Fiziksel Erişim Kontrolü : Bireyin belli bir alana erişimine izin vermeden önce tanımlamak ya da kimlik tespiti yapmak için kullanılır. Bazı şirketler ve kamu kurumları belirli alanlara girişte iris tanıma, el geometrisi, parmak izi gibi yöntemlerle kimlik tespiti yapmaktadır.
- Zaman ve Katılım : Biyometri çalışan yönetimine yardımcı olmak için ticari uygulamalara hizmet eder. Bu uygulamada çalışanın giriş çıkış saati kolaylıkla kontrol edilebilir. Yüzlerce ticari işyeri çalışma saati ve maaş düzenlemeleri için biyometrik tanıma ile çalışan mesai saati kontrolü yapabilmektedir.
- Tüketici Tanıma : Bu uygulama ile ticari bir işlem yürütürken kişinin kimliğini doğrulamak için kullanılabilir. Şu sıralar ülkemizde de bazı bankaların ATM'lerinde uygulanan parmak izi tanıma ya da el geometrisi sensörleri buna örnektir.
- Tıp/ Adli tıp : Biyometrik veri tanınmayacak durumda olan cesetlerin teşhisinde kullanılabilir. Ayrıca ebeveyn tespitinde DNA ile kontrol uzun yıllardır yapılan bir uygulamadır.



- Bunların dışında biyometrik veri uzaktan eğitim, kişisel bilgisayarlar, telefonlar, mobil cihazlar, e-ticaret uygulamaları, ev güvenliği gibi daha pek çok alanda kullanılmaktadır.

## 6.5 Biyometrik Sistemlerin Avantaj ve Dezavantajları

Her sistemde olduğu gibi biyometrik sistemin de getirdiği bazı avantajlar ve dezavantajlar vardır. Kimlik doğrulama ya da kimlik tespit uygulamalarında biyometrik veri kullanarak çalınma, kopyalama, paylaşma, kaybetme gibi istenmeyen durumlar ortadan kalkar. Bir kişinin farklı kimlik ya da birden fazla kimlik kullanıp kullanmadığı kolayca anlaşılabilir. Güvenlik konusunda bilgi ya da kart tabanlı sistemlere göre çok daha öndedir. Bilgi tabanlı sistemlerde şifre/PIN tahmin edilme ihtimali, kartlı sistemlerde kopyalama, çalınma ihtimali varken biyometrik sistemde tahmin edilebilecek herhangi bir şifre ya da kopyalanacak bir veri yoktur. Şifre ile giriş yapılan sistemlerde zayıf /kırılabılır parola oluşturma ihtimali varken biyometrik sistemdeki tüm kullanıcılar eşit seviyede güvenliğe sahiptir. Biyometrik sistemin çeşitli alanlarda başarılı bir şekilde uygulanıyor olması, sistemin tüm problemleri çözdüğü anlamına gelmez. Biyometrik sistemlerde geliştirilmesi gereken pek çok alan mevcuttur (Jain ve diğ. 2004).

Günümüz şartlarında biyometrik sistem beraberinde donanım maliyeti de getirir. Sistemin güvenlik seviyesi artırıldıkça karşılanması gereken maliyet de artacaktır. Herhangi bir biyometrik sistemde, biyometrik özelliği olmayan kimseler bu sisteme dahil edilemeyecek olması da dezavantajlar arasındadır. Ayrıca biyometrik ölçüler değiştirilemez olduğundan çalınma gibi durumlarda geçerliliğini kaybeder (Şamlı 2010). Şifre günceller gibi biyometrik veri güncelleme mümkün olmamaktadır. Bunu yanı sıra biyometrik veri zaman için değişim gösterebilir, deforme olabilir, kaza gibi durumlarda zarara uğrayabilir hatta tamamıyla yok olabilir. Biyometrik özelliği ele geçirmek için yapılacak her türlü müdahale, kişinin kendi beden bütünlüğüne zarar verir ölçüde olacağı için hayati tehlikelere neden olan durumlar ortaya çıkabilir. Biyometrik sistemin olumsuz diğer bir yönü de kişilerin biyometrik sisteme özellik vermeyi kabul etmeye karşı duruşlarıdır. Örneğin iris

tarama sisteminin gözde hasarlara neden olabileceği düşüncesi ile bazı bireyler biyometrik özellik vermeyi reddedebilmektedir.

Biyometrik veri ile çalışması planlanan bir sistem tasarlanırken tüm bu avantaj ve dezavantajlar göz önünde bulundurulmalı, istenen güvenlik seviyesine göre bir seçim yapılmalı, bu seçimin kullanıcılar tarafından kabul edilebilir olmasına özen gösterilmelidir.

## 7. BİYOMETRİK SİSTEM BAŞARIM ÖLÇÜMÜ OLARAK HATA ORANLARI

Performans değerlendirme biyometrik sistem algoritmasını sınırlarını ve üstünlükleri anlamak ve ona uygun uygulamalar geliştirmek için gereklidir. Biyometrik sistemlerin başarımı doğruluk, kaynak tüketimi, ölçeklenebilirlik ve sensör çalışılabilirliği açılarından değerlendirilebilir (Tian ve diğ. 2009).

Bir biyometrik tanıma sisteminde doğruluk performansı ölçülmesinde çeşitli hata oranları ortaya çıkar. Bu hata oranları biyometrik sistemin doğruluğunu hakkında bilgi veren oranlardır.

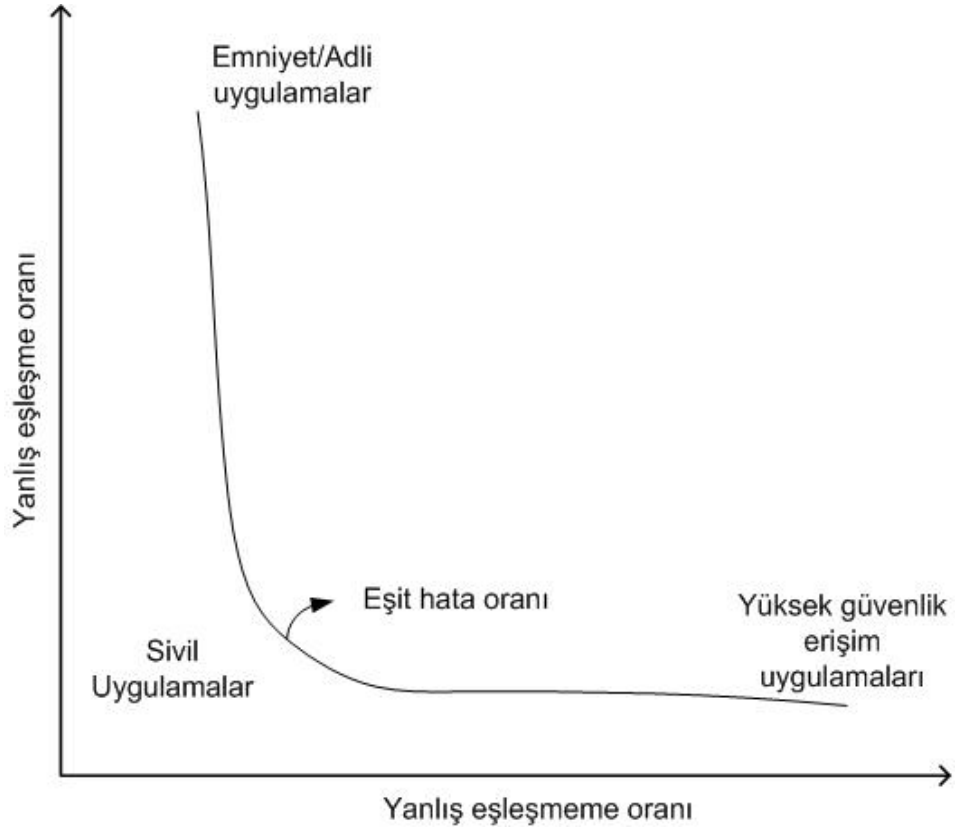
### 7.1 Yanlış Eşleşme(FMR) , Yanlış Reddetme (FNMR) ve Eşit Hata Oranı (EER)

Yanlış Eşleşme (FMR) : İki farklı insandan alınan biyometrik veriyi aynı kişiye aitmiş kabul etme hatası

Yanlış Reddetme (FNMR) : Aynı insandan alınan 2 farklı biyometrik veriyi farklı iki insandan alınmış gibi kabul etme hatası

Her biyometrik sistemde bu iki hata arasında karşılıklı değiş tokuş mevcuttur. Her iki hata oranı da t eşik değerli bir sistemin fonksiyonlarıdır. Burada gürültülü veriye karşı sistemi daha toleranslı hale getirmek için t eşik değerinin azaltılmasıyla Yanlış Eşleşme oranı artar. Diğer yandan sistemi daha güvenilir hale getirmek için t eşik değerinin artırılmasıyla yanlış reddetme oranı artış gösterir (Uludag ve diğ. 2004).

Her iki hata oranının eşit olduğu nokta ise Eşit Hata Oranını verir(EER). Biyometrik sistem hata oranlarının sivil uygulamalar, adli uygulamalar ve yüksek güvenlik erişimli uygulamalar karşısındaki durumu Şekil 7.5’de verilmiştir.



Şekil 7.5: Biyometrik sistem hata oranları

## 7.2 Edinim Başarısızlığı (FTC) ve Kayıt Başarısızlığı (FTE)

Bu iki hata oranının yanı sıra bir biyometrik sistem doğruluğu hakkında bilgi veren diğer başarısızlık oranları; edinim başarısızlığı ve kayıt başarısızlığıdır.

Edinim başarısızlığı sadece otomatik yakalama fonksiyonu olan sistemlerde uygulanabilir ve sisteme sunulan biyometrik özellik örneğinin alınmasındaki hata sayısının yüzdesi olarak ifade edilir. Bu tip hata genelde yeterli kalitedeki biyometrik özelliğin sistem tarafından yerinin belirlenememesinden kaynaklıdır (Jain ve diğ. 2004). Sistem veriyi görmez dolayısıyla elde edemez.

Diğer taraftan kayıt başarısızlığı ise sisteme biyometrik özellik verecek kullanıcıyı kayıt yapamamasından kaynaklanan hataların yüzdesidir. Kayıt başarısızlığı genelde sistemin kalitesiz biyometrik veriyi kayıt etmeyi reddetmesi ile ortaya çıkar (Jain ve diğ. 2004). Burada sistem veriyi yakalar fakat yetersiz bulduğu için kayıt etmez.

Başarısızlık oranları ve yanlışlık oranları arasındaki karşılıklı bağlantı, biyometrik sistemin önemli özellikleridir ve sistemin başarısının hesaplanma sürecinde göz önünde bulundurulması gerekmektedir.

Yukarıda sayılan 4 ölçüm, kullanılan biyometrik sistem uygulamasının özelliğine bakmaksızın tümüne uygulanabilir olduğundan, başlıca ölçüm oranları olarak kabul edebiliriz. Kayıt ve edinim başarısızlığı özellik çıkarma bileşenlerinin performansını ölçerken, yanlış eşleşme ve yanlış reddetme oranları eşleştirme bileşeninin performansını ölçer (Jang ve Kim, 2009) .

### 7.3 Yanlış Red Oranı (FRR) ve Yanlış Kabul Oranı (FAR)

Doğrulama; kişinin bir kimlik iddia ettiği ve iddia edilen bu kimliğe ait veri tabanındaki örnek ile iddiada bulunan kişiden alınan özelliğin karşılaştırılması sonucu sistemin kabul ya da red kararı verdiği, biyometrik sistemin en önemli uygulamalarından biridir. Biyometrik sistem performansı ölçülürken sisteme etkileşimde tek bir teşebbüs olabileceği gibi genelde birden fazla teşebbüs bulunulabilmektedir. Bu açıdan bakıldığında yukarıda sayılan temel ölçümler yeterli olmadığında yanlış kabul oranı (FAR) ve yanlış red oranı (FRR) ölçümlerine bakılır. Başka bir deyişle olumlu ya da olumsuz belirtilen durum hakkına kabul ya da red gibi bir durum söz konusu ise yani doğrulama yapılacaksa FAR ve FRR bakılır (Liu ve Silverman 2001).

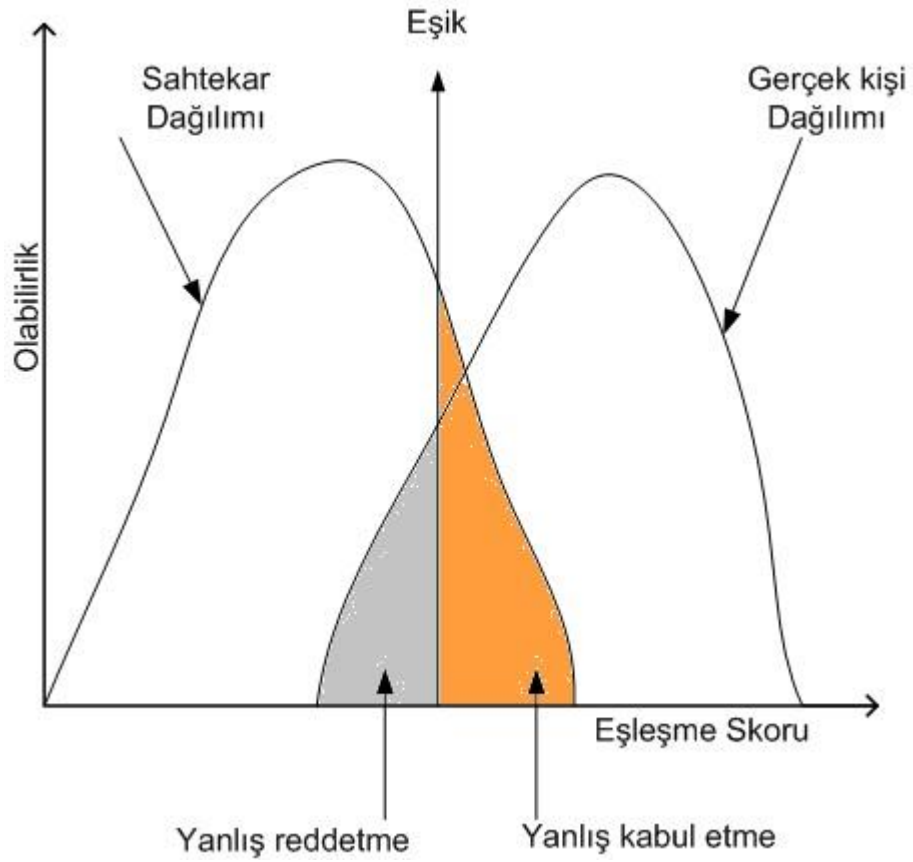
Yanlış red oranı (FRR) : gerçek bir kimlik iddia eden in yanlış olarak kabul edildiği doğrulama işlemlerinin oranıdır. Tek bir girişim olduğunda FTA ve FNMR içeren FRR oranı aşağıdaki gibidir.

$$FRR = FTA + FNMR (1 - FTA) \quad (6.1)$$

Yanlış kabul oranı (FAR) : yanlış kimlik iddia eden birinin yanlışlıkla doğru olarak kabul edildiği doğrulama işlem oranıdır. Tek bir girişim olduğunda FTA ve FNMR içeren FAR oranı aşağıdaki gibidir.

$$FAR = FMR (1 - FTA) \quad (6.2)$$

FRR ve FAR kayıt sırasında ortaya çıkan başarısızlıkları içermez (Jang ve Kim 2009; Shan ve diğ. 2009) . Şekil 7.6'da FAR ve FRR oranları ve birbirleriyle ilişki durumlarını görebiliriz.



Şekil 7.6: Yanlış eşleşme ve yanlış reddetme oranları

## 8. BİYOMETRİK VERİ OLARAK KULAK

Sosyal etkileşimin giderek sayısal hala geldiği, finansal işlemler düzenli olarak internet üzerinden yürütüldüğü bir dünyada bireyin kimliğini güvenli bir şekilde belirlemek büyük önem taşımaktadır. Ayrıca çeşitli emniyet ve askeri uygulamalar, bir bireyin potansiyel bir tehdit ya da cezai suçlu olup olmadığını belirleme ihtiyacı duyar (Ross ve Abaza 2011).

Şifre, parola, kimlik kartı gibi geleneksel yöntemlerin yetersiz kaldığı günümüz şartlarında kişilerin fiziksel ve davranışsal özelliklerini kullanarak kimlik tespit etmeye yarayan biyometrik sistem büyük önem kazanmaktadır.

Her bir biyometrik özelliğin birtakım güçlü yönlerinin olduğu gibi bazı zayıflıkları da mevcuttur. Tek bir biyometrik özellikten tüm uygulamaların gerekliliklerini verimli bir şekilde karşılaması beklenemez (Jain ve diğ. 2004).

İnsanın sahip olduğu özellikler içerisinde bakıldığında evrensellik, benzerlik, kalıcılık gibi biyometrik olma şartlarını sağlayan güçlü bir özellik olarak kulak karşımıza çıkmaktadır.

Kulak özelliğinin biyometrik olup olmadığı hakkındaki soru işaretlerini gidermek için çok sayıda çalışma girişimi olmuştur.

Kulağın kişi tanımlamada kullanılabilecek potansiyelde olduğu, suçluları tespit etmede fiziksel ölçümlerin kullanımına öncülük eden Fransız polis memuru Alphonse Bertillon tarafından 1880'lerin başında fark edilmiştir. Bertillon antropometri adını verdiği çalışma ile kulak da dahil olmak üzere vücudun çeşitli yerlerini tanımlamak için nicel ve nitel özellikleri kombine etmiştir (Ross ve Abaza 2011; Bertillon 1893).

Kulak benzersizliğini belirlemek için ilk deneysel çalışma 1964 yılında yine bir polis memuru olan Inarelli tarafından yapılmıştır (Prakash ve Gupta 2014).

1948-1962 yılları arasında topladığı 10000 kulak fotoğrafı ile yaptığı çalışmada crus of helix'e dayanarak 12 farklı geometrik ölçüm olduğunu ortaya koymuştur (Iannarelli 1989).

Iannarelli'nin (1989) çalışması ile diğer araştırmacıları motive eden kulak biyometrisi hakkında yapılan diğer incelemeler bize kulağın yaşla birlikte değişmediği, farklı yüz ifadelerine göre şekil değiştirmedeği, sarmal ve kıvrım gibi belirleyici özellikler yönünden zengin olduğu bilgisini vermektedir. Ayrıca parmak izine göre daha büyük, yüze göre daha küçük olması sebebiyle belli bir mesafeden görüntü yakalanması daha kolaydır.

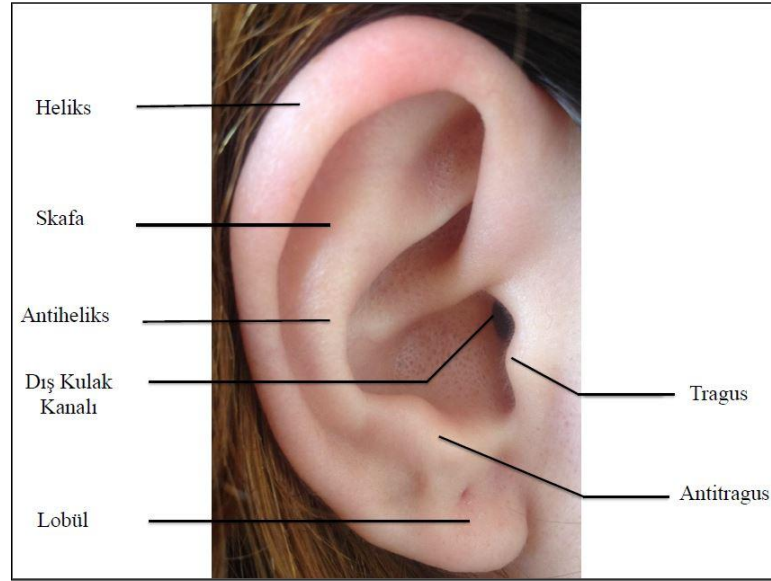
İnsanların kimliklerini kulakları ile tanımlama literatürde son zamanlarda ilgi çeken bir konudur. Bu eğilimin çeşitli sebepleri vardır. İlk olarak yüz tanıma gibi temassız biyometrikleri karşılaştıkları bazı sorunlar kulak için geçerli değil. İkincisi yüz tanıma için verilen çoklu yüz tanıma pozlarında, yandan verilen poz için örneğin, yüz ile birlikte kullanılacak en umut verici adaydır. Üçüncüsü eldeki herhangi bir kişi izleme kaydında yüzün tamamıyla gözükmediği durumlarda kulak özelliği kullanılabilir (Singh ve diğ 2014). Yüz tanımak için gerekli ışığın ya da açının uygun olmadığı durumlarda kulak tanıma devreye girer.

Buna ek olarak başın her iki yanında bulunan konumu gereği, kulak arka planı kolayca tahmin edilebilir yapıdadır (Masaoud ve diğ 2013; Hurley 2007).

Şekil 8.7'de genel terminolojide kulak kepçesinin ayırt edici özellik olarak kullanılan birtakım girinti, çıkıntı ve sarmallardan oluşan yapısı gösterilmiştir.

Pinna	:Kulak kepçesi olarak ifade edilen bölüm.
Auricula	:Dış kulak yolu
Konka auricula	:Kulağın en derin yeri konka aurikula ismini alan çukur bir bölgedir. Konka aurikula; derine doğru, dış kulak yolu ile devam etmektedir.
Helix	:Aurikula'yı çepeçevre saran çıkıntıya heliks adı verilmektedir.
Antiheliks	:Heliks önünde bulunan ikinci bir kabarıklık antihelikstir.
Tragus	:Dış Kulak Yolunun ön kısmında bulunan çıkıntı tragus denir.
Antitragus	:Tragus altındaki ikinci bir çıkıntı antitragus olarak adlandırılır.
Lobül	: Aurikulanın altında lobül kısmı bulunmaktadır.





**Şekil 8.7:** Dış kulak yapısı ve bölümleri

Kulak, yukarıda sayılan farklı bölüm ve bölgelerden oluşmakta olduğu görülmektedir. Bu farklı bölümler tanımlama yapmada veri zenginliğini sağlar. Girinti ve çıkıntıların artması elde edilen özelliklerin artması demektir. Bu sayede kimlik bulma ya da doğrulama işlemi sırasında karşılaştırılacak alanların artmasını dolayısıyla verimliliğin artmasını sağlar.

Sağlam bir kulak tanıma algoritması geliştirmek ve test etmek için ışıklandırma ve poz gibi değişiklik gösterebilen faktörlerin dikkatlice kontrol altına alındığı yeterli büyüklükte veritabanları gerekmektedir. 19 nesne den oluşan küçük bir veri tabanı olsa da, Carrerira Perpınan 1995 veri tabanının kullanımı oldukça yaygındı (Abaza ve diğ. 2013).

Günümüzde pek çok üniversite ve organizasyon yüzlerce kulak görüntüsünden oluşan veritabanları bulunmaktadır. Buradaki temel amaç kulak biyometrisi alanındaki araştırmalara destek sağlamaktır (Narayan ve Dubey 2014).

Bu veritabanlarından bir kısmı halka açık bir kısmı ise gerekli lisanslar alındıktan sonra kullanılabilir durumdadır. Mevcut olan bazı kulak veritabanları şunlardır.

- USTB Kulak Veri tabanı : Pekin Bilim ve Teknoloji Üniversitesi Kulak Tanıma Laboratuvarı tarafından sağlanmaktadır. Farklı uzaklık mesafelerinde,

arka planı belli bir renkte olan veya deęişen açılarda çekimlerin yapıldığı farklı veritabanlarını içermektedir.

- UND Kulak Veri tabanı :Notre Dame Üniversitesi tarafından ücretsiz erişimi olan bir veri tabanıdır. Farklı sayılarda ve farklı ortam durumlarında elde edilmiş koleksiyonlardan oluşmaktadır.
- IIT Delhi Kulak Veri tabanı : 2006- 2007 yılları arasında kampüste bulunan 18 ile 58 yaş arasındaki öğrenci ve personelin kulak görüntüsü alınarak oluşturulmuştur. Görüntülerin jpeg formatında olup çözünürlükleri 272x204 pikseldir (Narayan ve Dubey 2014).
- IIT Kanpur Kulak Veri tabanı : 2 farklı veri kümesinden oluşmaktadır. İlki 190 kişiden alınan 801 yüz profili, ikincisi 89 kişiden alınan 801 yüz profilinden oluşmaktadır. Yan yüz profili alınırken örneklerin farklı açılarda çekilmiş görüntüleri kullanılmaktadır (Narayan ve Dubey 2014; Prakash ve Gupta 2011).
- AMI Kulak Veri tabanı : Görüntülerin Matematiksel Analizi (GMA) kulak veri tabanı kulaktan kimlik tespiti yapılabilmesi için bilimsel uygulamalarda ücretsiz kullanım sunmaktadır. Veri tabanı Esther Gonzales tarafından oluşturulmuş olup kapalı alan çekimlerinden oluşmaktadır. Veri tabanı 19-65 yaş arası 100 farklı kişiden elde edilmiştir. Görüntüler jpeg formatında 492 x 702 piksel çözünürlüktedir (Narayan ve Dubey 2014).
- XM2VTS Veri tabanı : Dört ay aralıklarla, dört ayrı mevsimde 295 kişiye ait dörder adet görüntüden oluşmaktadır.
- UCR Veri tabanı : Kaliforniya Riverside Üniversitesine tarafından oluşturulmuş bu veri tabanı 155 kişiye ait 902 görüntüden oluşmaktadır. Bu veritabanındaki 12 kişinin kulağı kısmen kapalı, 6 kişi de küpelidir. Özel, genel kullanıma açık olmayan bir veri tabanıdır.
- WVU Veri tabanı : Bilgisayar, fotoğraf makinesi ve lineer aktüatör kullanan bir sistem ile oluşturulan bir kulak veri tabanıdır. 402 kişiyte ait 460 videodan oluşur. Her bir video iki dakika boyunca sol taraftan başlayıp sağ tarafta son bulur. Özel kullanıma ait bir veri tabanıdır.

- UMIST / Sheffield Veri tabanı : Sheffield Üniversitesi tarafından oluşturulmuş bir veri tabanıdır. 20 kişiye ait 564 görüntüden oluşmaktadır. Halka ücretsiz açık bir veri tabanıdır.
- FERET Veri tabanı : 1199 tekil ve 365 benzer örüntülerin olduğu toplam 14216 görüntüden oluşmaktadır. Görüntüler çoğunlukla iki boyutlu tanımlama ya uygundur. Genel kullanıma açık fakat ücretli bir veri tabanıdır.
- UBEAR Veri tabanı : 126 kişiye ait 4430 görüntüden oluşmaktadır. Bu veri tabanında kulak görüntüleri kontrolsüz çevre şartları altında elde edilmiştir. Görüntülerde kişilerden bazıları şapka takarken bazılarında küpe bulunmakta, bazılarında ise kulak görüntüsü saçla kapalı haldedir. Halkın kullanımına açık, ücretsiz bir veri tabanıdır. (Kandgaonkar 2015)

## 9. YAPILAN ÇALIŞMALAR VE UYGULAMA SONUÇLARI

Biyometrik sistemlerin üç temel işlevi kayıt, doğrulama ve tanımlamadır. Buradan yola çıkarak bu üç işlev yerine getirilebilecek bir arayüz tasarlanmıştır.

Tasarlanan arayüz için kullanılan dil C# ve geliştirilen ortam Microsoft Visual Studio 2010 dur. Kullanıcı ara yüzü oluşturmak için Form Application kullanılmıştır. Sisteme kayıt edilen biyometrik verinin görüntü, kişi ve diğer gerekli bilgileri SQL Server Veri tabanında tutulmuştur. Görüntü işleme işlemleri için OpenCV (Open Source Computer Vision) kütüphanesi sisteme uyarlanmıştır. OpenCV Intel Rusya araştırma merkezi tarafından geliştirilen ücretsiz kullanımda olan, açık kaynak kodlu bilgisayar görüşü sağlayan programlama işlevlerini içeren bir kütüphanedir. C++, C, Python ve Java dillerine uyumludur. Tasarlanan sistemde kullanılan dil C# olduğundan ara bağdaştırıcı bir platform gereksinimi EmguCV ile sağlanmıştır. EmguCv; C#, VB gibi .NET dillerinden OpenCv işlevlerinin çağrılmasına imkan tanır. Sistemde kullanılan kulak örnekleri Esther Gonzales tarafından oluşturulan AMI kulak veri tabanından sağlanmıştır. Bilimsel kullanıma açık ve ücretsiz olan bu veri tabanına [http://www.ctim.es/research\\_works/ami\\_ear\\_database/](http://www.ctim.es/research_works/ami_ear_database/) adresinden ulaşılabilir. Bu veri tabanında 100 bireye ait toplam 700 kulak kaydı bulunmaktadır. Bu kulak kayıtları başın düz durumdaki ve sağa, sola, yukarı, aşağı gibi farklı pozisyonlarındaki çekimleriyle elde edilmiştir. Her bireye ait yedi farklı kulak görüntüsü bulunmaktadır. Bu veri tabanında biyometrik sistemde tanımlama ve doğrulama işlemleri kulak biyometrisi ile yapıldığından, görüntü edinimi sadece kulak görüntülerinden elde edilmiştir.

Kullanılan AMI veritabanındaki 5 numaralı kayıta ait kulak örnekleri Şekil 9.8'de verilmiştir. Veritabanındaki bazı kulak örnekleri daha belirgen bazıları saç, gözlük ve küpe gibi bazı tıkanıklıklara sahiptir (Şekil 9.9). Çalışmada yapılan bazı denemeler için veritabanındaki kulaklar kırılarak saç ve gözlük gibi faktörlerden kaynaklanan olumsuzluklar en aza indirmeye çalışılmıştır (Şekil 9.10).



**Şekil 9.8:** AMI kulak veri tabanında 5 numaralı kayıta ait, kulak örnekleri.

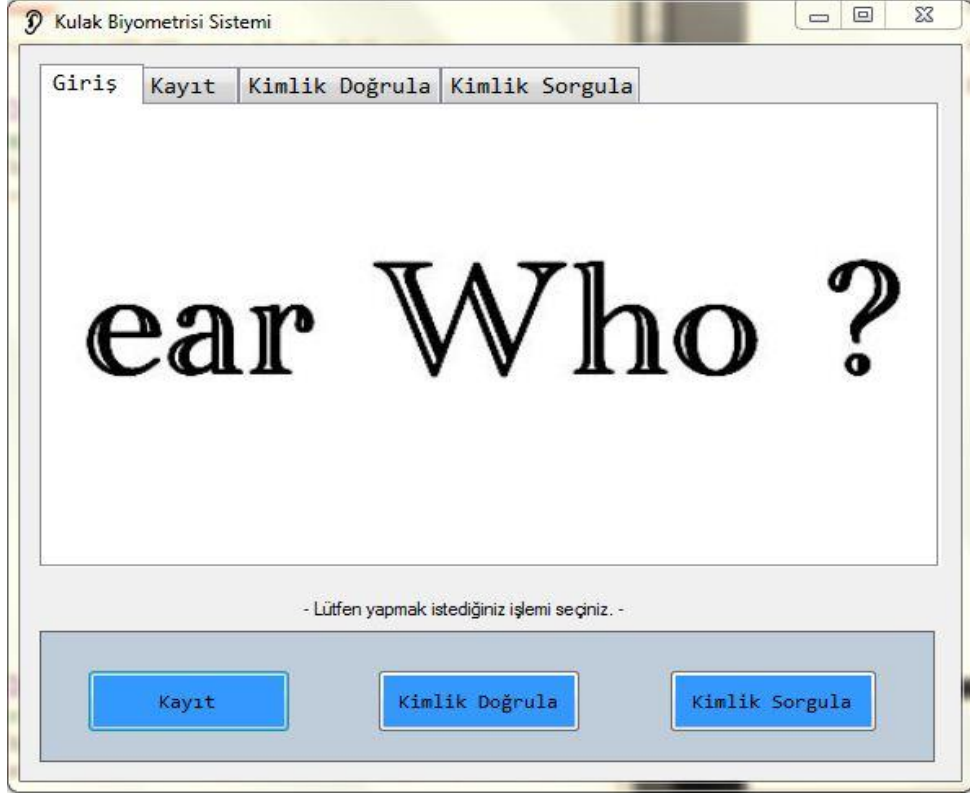


**Şekil 9.9:** AMI kulak veri tabanında 28 numaralı kayıta saç, küpe gibi faktörlerden kaynaklanan tıkanıklıklar.

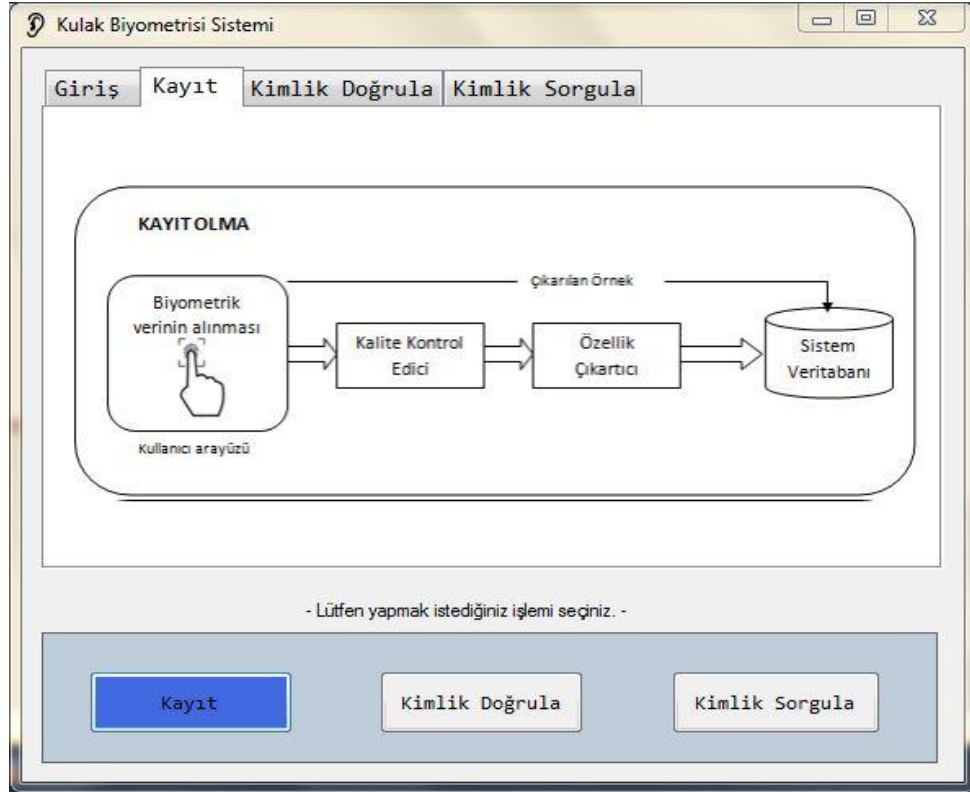


**Şekil 9.10:** AMI kulak veri tabanından yapılan testler için kırılan kulak görüntüleri.

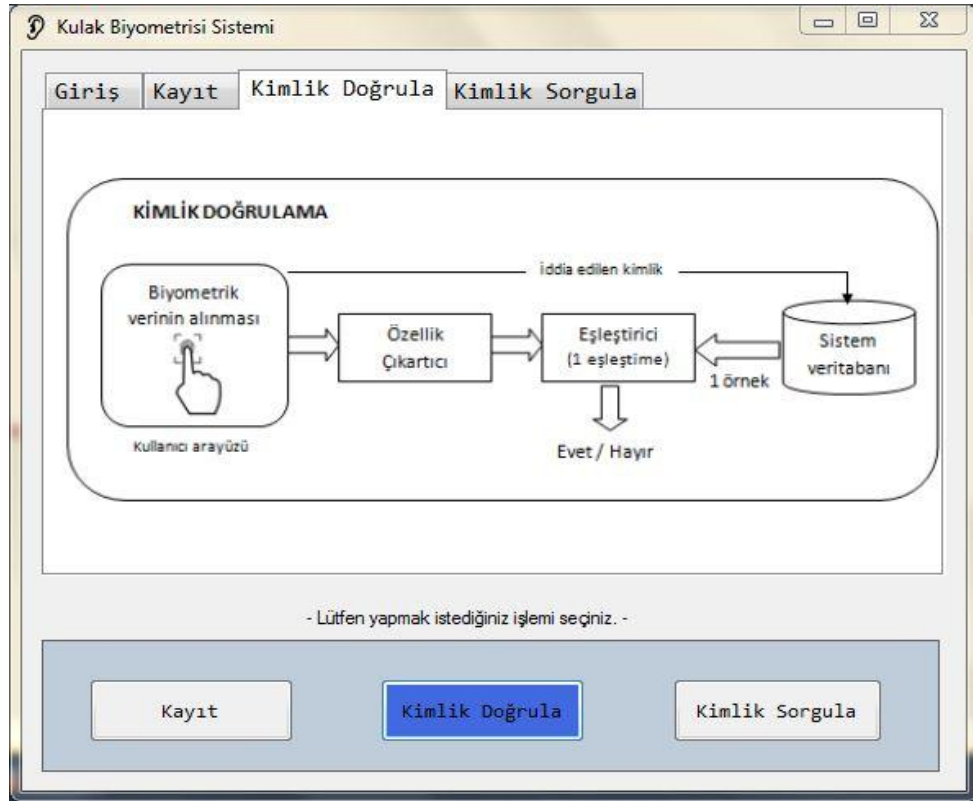
Sistem ilk açılış ekranı Şekil 9.11’de görüldüğü gibidir. Yapılmak istenen her bir işlem için Şekil 9.12, Şekil 9.13 ve Şekil 9.14’de görüldüğü gibi bilgi verir nitelikte yönergeler hazırlanmıştır. Bu yönergeler ışığında yapılmak istenen işlemin seçimine olanak tanımıştır. Yönergelerdeki bilgiler neticesinde yapılmak istenen işleme karar veren kullanıcı kayıt, kimlik doğrulama ve kimlik sorgulama sayfalarından her birine ulaşabilmektedir.



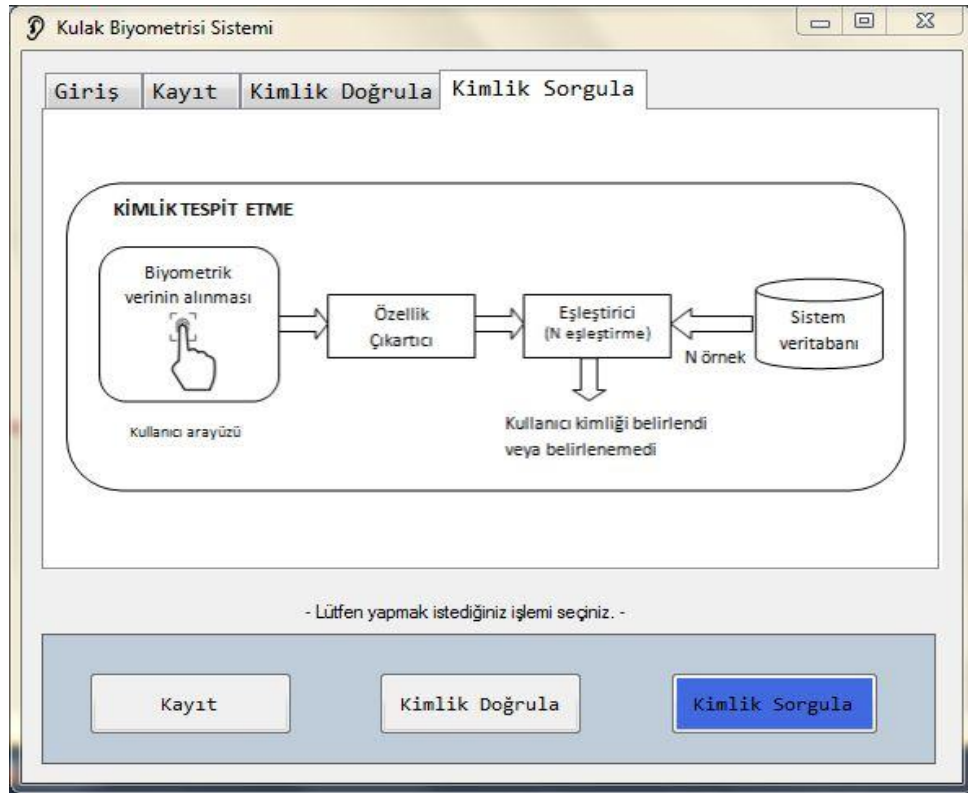
Şekil 9.11: Giriş sayfası ekran görüntüsü



Şekil 9.12: Giriş sayfasında kayıt bilgisi

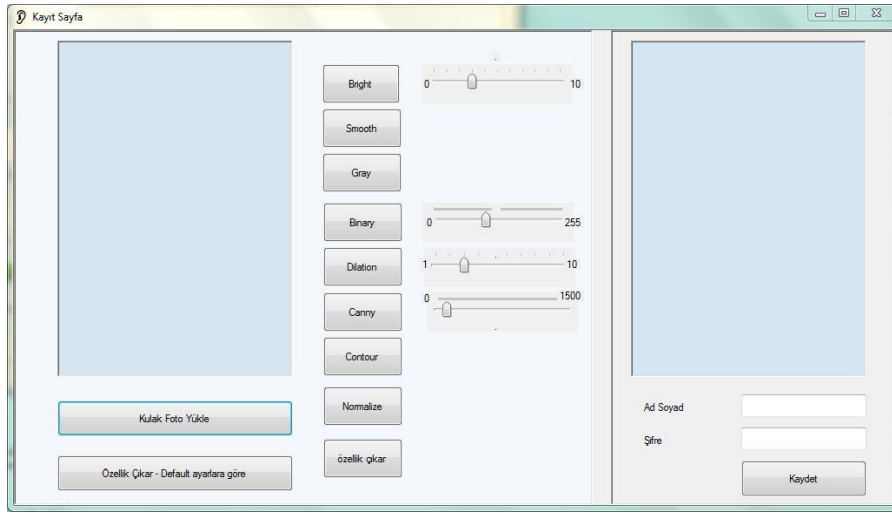


Şekil 9.13: Giriş sayfasında kimlik doğrulama bilgisi



Şekil 9.14: Giriş sayfasında kimlik sorgula bilgisi

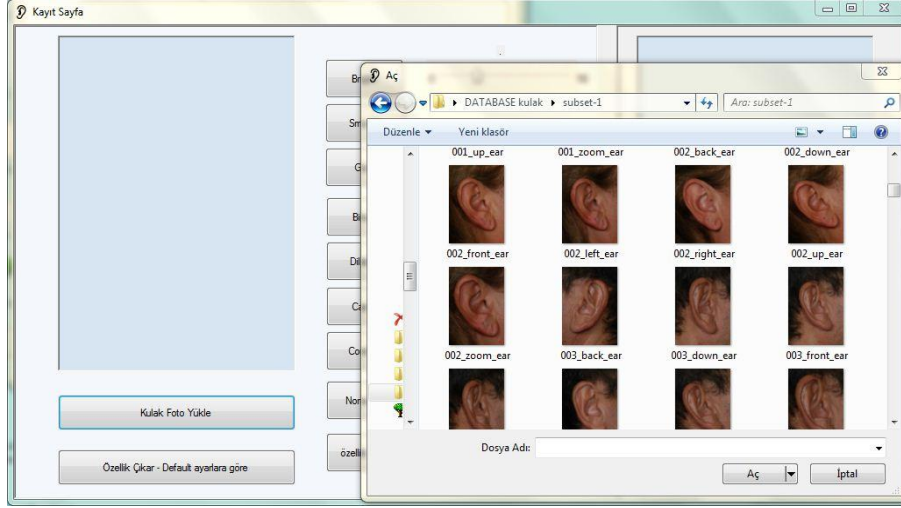
İlk açılan pencerede kayıt seçeneği açıldığında ortaya çıkan ekran görüntüsü Şekil 9.15'deki gibidir. Burada görüntü edinimi sırasında alınan kulak görüntüsü yüklenir ve çeşitli görüntü işleme yöntemleri uygulanır. Şekil 5.2'de listelenen görüntü işlemenin 10 adımından gerekli görülenler gerçekleştirilerek uygun bir özellik çıkartımı işlemi yapılır. Burada görüntüye yapılan her bir uygulama en iyi özellik elde etmek için belli sırada ve belli bir aralıkta yapılmıştır. Bu oranlara ve yapılacak uygulamalara karar verirken sistem pek çok testten geçmiştir. Çıkarılan özellik ad-soyad ve şifre bilgileri ile veri tabanına kaydedilir.



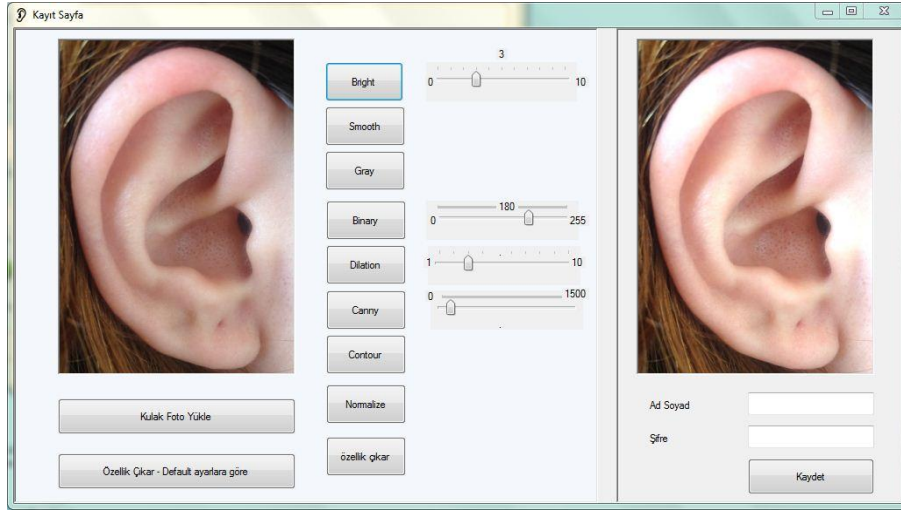
Şekil 9.15: Kayıt sayfası görünümü

Şekil 9.16'da kayıt sayfasında kayıt gerçekleştirmek için kulak yükleme seçeneğine tıklandığında açılan dosya görülmektedir. Burada kayıt edilmek istenen kulak görüntüsü seçilir ve ilk resim kutusu ile ekrana yansıtılır. Bu resim kutusundaki kulak görüntüsüne iyileştirme işlemleri yapmak için öncelikle kulağın parlaklık ayarı değiştirilebilir (Şekil 9.17). Görüntü grileştirilir (Şekil 9.18), ikili-seviye haline getirilir (Şekil 9.19). Daha sonra bu ikili seviye haline gelen görüntüden kenarlarını bulunup (Şekil 9.20), kontur bilgisi elde edilir (Şekil 9.21). Sonra da normalleştirme işlemi ile kulağın açısı ayarlanıp özellik çıkartılır (Şekil 9.22). Yüklenen kulağa yapılan tüm işlemler sırasıyla sağdaki resim kutusunda görülebilmektedir.

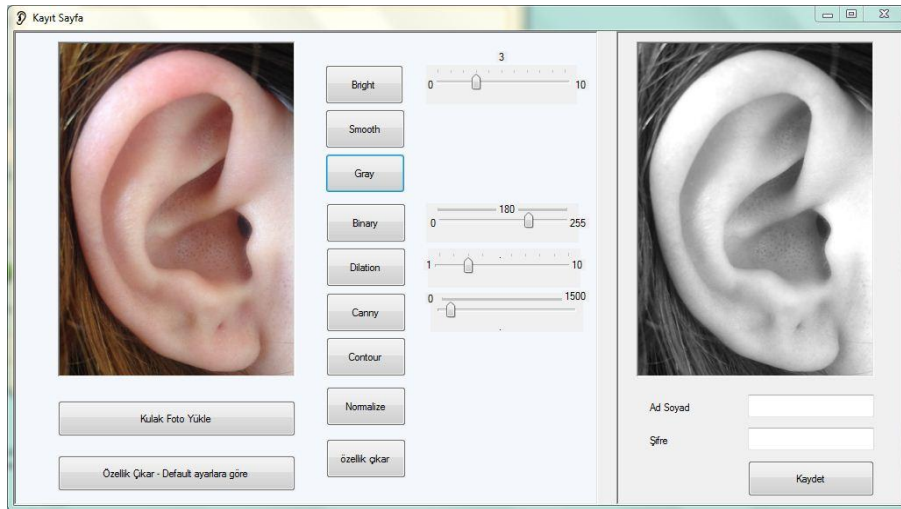




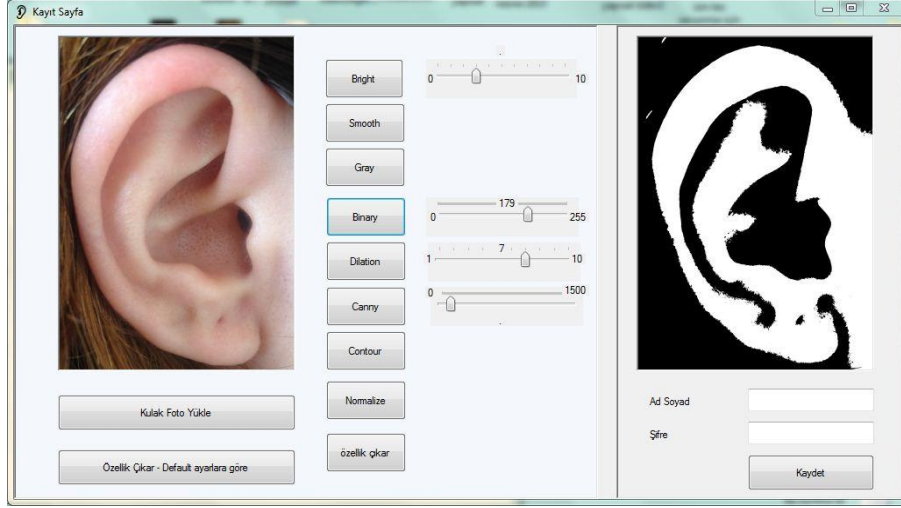
Şekil 9.16: Kayıt sayfasında kulak foto yükleme



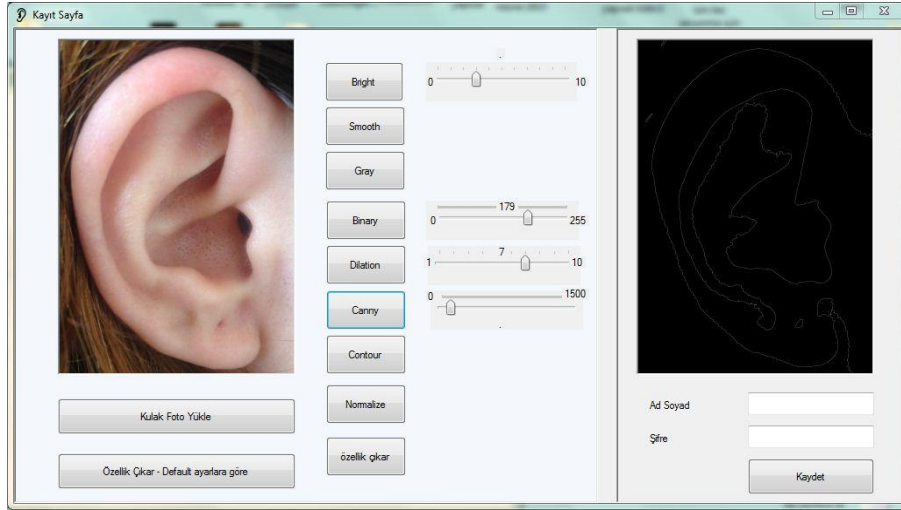
Şekil 9.17: Kayıt sayfasında yüklenen kulak görüntüsünü rengini parlatma



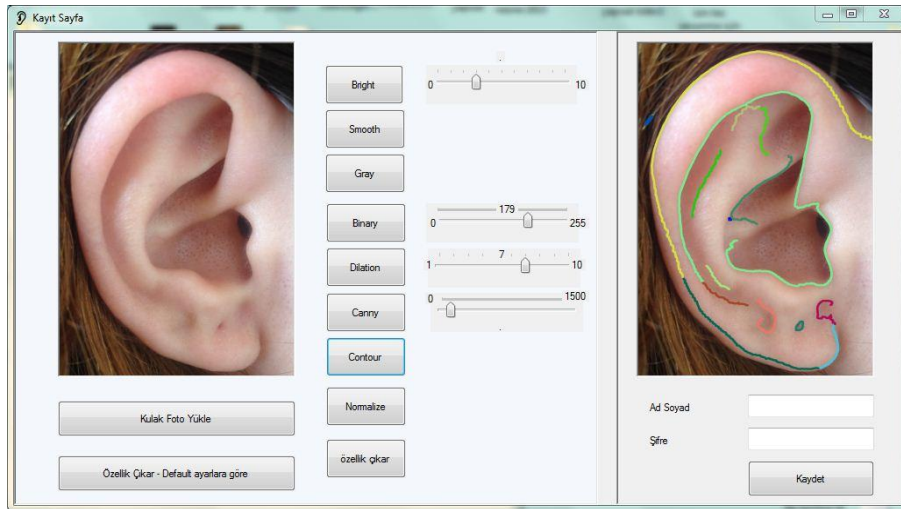
Şekil 9.18: Kayıt sayfasında kulak görüntüsünü grileştirme



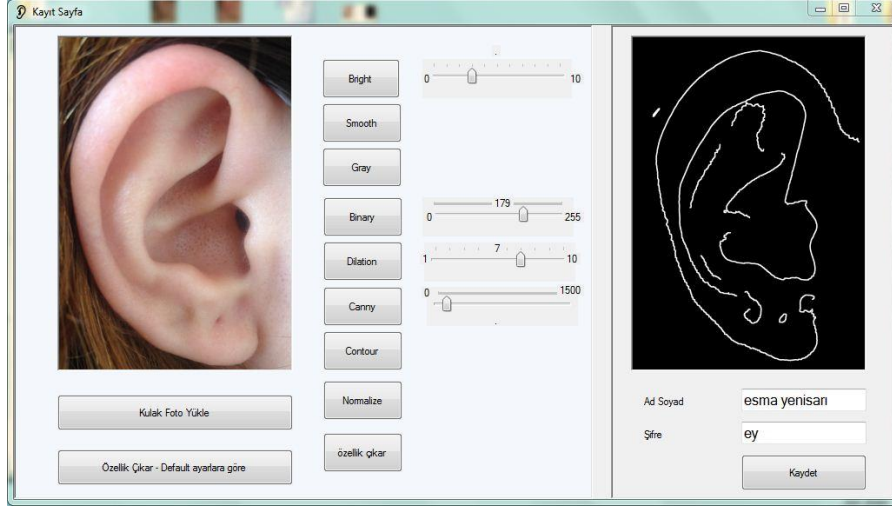
Şekil 9.19: Kayıt sayfasında kulak görüntüsünü ikili görüntü haline getirme



Şekil 9.20: Canny Kenar Bulma algoritması uygulama



Şekil 9.21: Kulak görüntüsünün konturunu bulma



**Şekil 9.22:** Kulak görüntüsünü normalleştirdikten sonra, özellik çıkartımı yapıp veri tabanına kaydedilmesi

Elde edilen görüntüyü sayısal olarak ifade edersek

$$f(x, y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0, M-1) \\ \vdots & \vdots & \ddots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1, M-1) \end{bmatrix} \quad (9.1)$$

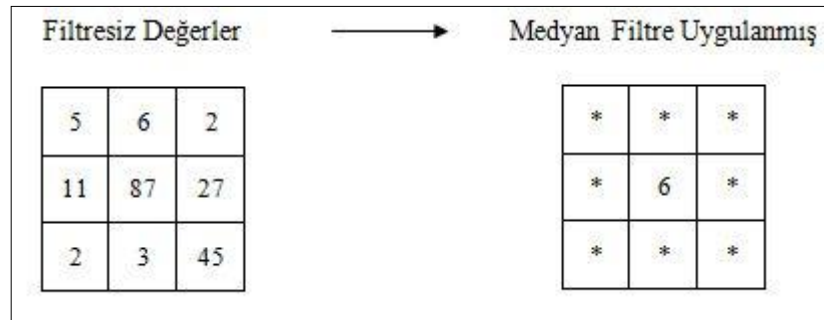
Burada  $f(x, y)$  Sayısal görüntü, matris elemanları ise her bir pikseli ifade eder.

Bulanıklaştırma olarak da bilinen yumuşatma(smoothing) basit ve sık kullanılan bir görüntü işleme işlemidir. Farklı nedenlerle bulanıklaştırma yapılabilir fakat genelde görüntüdeki gürültüyü ve paraziti azaltıp geçişleri yumuşatmak için kullanılır. Bulanıklaştırma işlemi için farklı filtreler kullanılabilir. En genel kullanılan filtreler lineer olanlardır yani işlem sonrası çıktıdaki piksel değerlerin  $g(i, j)$  girdideki piksel değerlerin toplamı olarak temsil edildiği  $f(i + k, j + l)$  filtrelerdir:

$$g(i, j) = \sum_{k,l} f(i + k, j + l)h(k, l) \quad (9.2)$$

Burada  $h(k, l)$  filtre katsayıları anlamına gelen çekirdektir(kernel) (Szeliski 2011).

Bunun dışında Gaussian, Median ve Bilateral gibi pek çok farklı filtre bulunmaktadır. Sistemimizde kullandığımız yumuşatma filtresi Medyan filtredir. Medyan filtre lineer olmayan uzaysal bir filtredir ve genelde tuz-biber olarak bilinen görüntü gürültüsünü azaltmak için kullanılır. Medyan filtre görüntüdeki her bir piksel üzerinde gezerek her bir pikselin yoğunluk değerini hesaplar. Daha sonra söz konusu pikselin komşuluk piksellerinin yoğunluk değerlerinin ortancasını bulur ve bunu çalışılan piksel değeri yerine yazar. Burada komşuluk değerleri önce sıraya konular daha sonra ortadaki değer alınır (Church ve diğ. 2008). Medyan filtreyi görüntü üzerinde kayan bir pencere olarak düşünürsek merkezdeki değer yerine pencere içindeki değerlerin ortancasını yazması beklenir. Şekil 9.23’de temsili olarak verilen piksellere medyan filtre uygulama örneği görülmektedir.



**Şekil 9.23:** Temsili verilen piksellere medyan filtre uygulanma örneği

Gri tonlama (Grayscale) diğer bir görüntü işleme yöntemidir. Bu yöntem ile birçok renk ile uğraşmak yerine gri tonları ile işlem yaparak zamandan ve hızdan tasarruf edilir. Bir görüntüyü gri tonlama ile her bir pikselin değeri tek bir kanaldan oluşur ve her bir piksel sadece yoğunluk bilgisini taşır (Johnson 2006). 256 renk içinde her rengin tonu kadar gri tonlaması oluşturulur. Her bir pikseldeki renk değerinin ortalaması alınarak gri ölçek oluşturulur (Çevik ve Çadır 2011).

$$Gri\ Tonlama = \frac{K(i,j)kırmızı + K(i,j)yeşil + K(i,j)mavi}{3} \quad (9.3)$$

$$K(i,j)kırmızı = Gri\ Tonlama \quad (9.4)$$

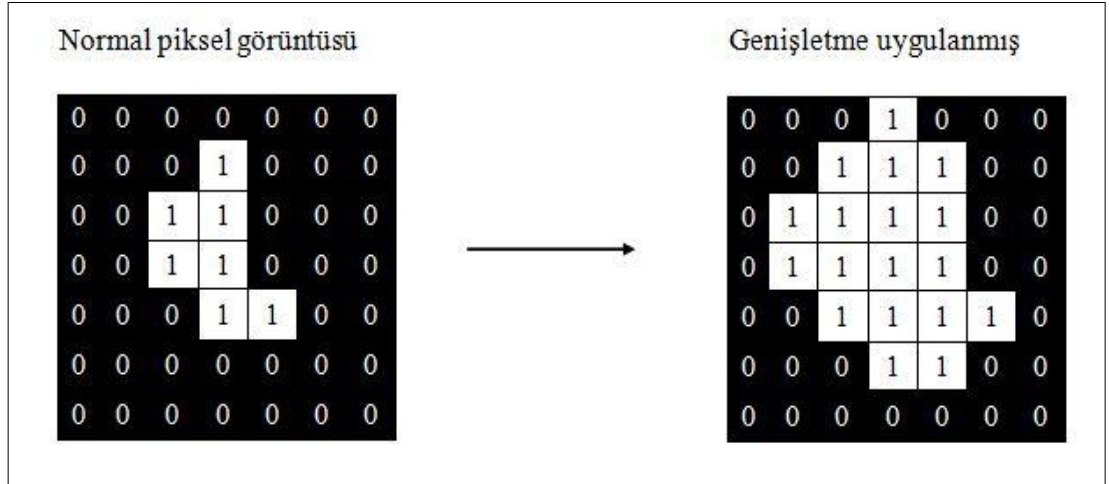
$$K(i,j)_{yeşil} = Gri\ Tonlama \quad (9.5)$$

$$K(i,j)_{mavi} = Gri\ Tonlama \quad (9.6)$$

Her bir piksel değeri için sadece 2 olası değer ihtimalinin olduğu sayısal görüntülere ikili seviye (binary) görüntü denir. Gri tonlamalı hale gelen görüntü belli bir eşik değeri verilerek ikili renk seviyesine indirgenir. Burada belli eşik altındaki pikseller 0, üstündeki değerler 255 değerine sahip olur. İki seviyeli görüntü hafızada bitmap olarak depolanabileceğinden daha az yer kaplar İki seviyeli görüntüde piksel değerleri 1 veya 0 olarak temsil edilir.

$$f(x,y) = \begin{bmatrix} 1 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \dots & 1 \end{bmatrix} \quad (9.7)$$

İki seviyeli hale gelen görüntü, görüntü işlemedeki morfolojik bir işlem olan genişletme(dilation) işleminin tabii tutulur. Genişletme (genleşme) gri tonlamalı görüntü üzerinde de kullanılabileceği gibi genelde iki seviyeli görüntülerde kullanılır. Şekil 9.24'de genleşme uygulanmış piksel örneği görülmektedir.



Şekil 9.24: Genleşme uygulanmış temsili piksel örneği

Morfolojik bir dönüşüm olan genleşme de  $\oplus$ ; vektör toplamını kullanarak iki kümeyi birleştirirsin.  $X \oplus B$  genleşmesi X ile B arasındaki her bir kümenin olası tüm vektör toplamlarının kümesi ise (Sonka ve diğ. 1993) .

$$X \oplus B = \{p \in \varepsilon^2 : p = x + b, x \in X \text{ ve } b \in B\} \quad (9.8)$$

Yapılan morfolojik işlemlerden sonra gürültüsü azaltılmış ve kenarlarının bulunması için ideal hale gelen görüntüye, Canny kenar bulma algoritması uygulanır. 1986 yılında John F. Canny tarafından geliştirilen Canny Kenar tespiti uygulandığında çıktı iki seviyeli ince kenarlardan oluşan bir görüntüdür. Bu çıktıda hangilerin gerçekten kenar hangisinin değil olduğuna karar vermek için eşikleme kullanılır. Canny kenar bulma algoritması güçlü ve zayıf kenarları bulabilmek için 2 eşik değeri kullanır. Bir zayıf kenar ancak güçlü bir kenar ile bağlantılı ise çıktı olarak görülür. Canny işleminin dayandığı temeller aşağıdaki denklemlerde verilmiştir (Ding ve Goshtasby 2001; Latha ve Chaithany 2013).

Gauss filtresi ile gürültü temizleme ve yumuşatma

$$G(x, y) = \exp [-(x^2 + y^2)/2\sigma^2] \quad (9.9)$$

Gradyan büyüklüğü ve gradyan yönünü her bir piksel için belirle.  $n$  yön,  $p$  görüntü ise

$$n = \nabla(g * p) / |\nabla(g * p)| \quad (9.10)$$

$$G_n P = \frac{\partial}{\partial n} [g * p] \quad (9.11)$$

Eğer bir pikseldeki gradyan büyüklük gradyan yönündeki 2 komşuluğundan da büyükse, bu pikseli kenar olarak işaretler.

$$0 = \frac{\partial}{\partial n} G_n P = \frac{\partial^2}{\partial n^2} [g * p] \quad (9.12)$$

Eşikleme yaparak zayıf kenarlar temizlenir.

Canny kenar bulma algoritmasının yanısıra görüntüdeki kenarları bulmanın bir diğer yolu da OpenCV kütüphanesindeki FindContours() fonksiyonudur. Bu fonksiyon basit yaklaşım yöntemiyle görüntü kenarlarını bulur. Canny kenar bulma algoritmasından sonra kullanımı da mevcuttur. Cannyde çıktı iki seviyeli görüntüyken, kontur bulmada çıktı noktalar kümesidir. Kontur bulmada çıktı olarak

elde edilen noktalar kümesi daha sonra amacına uygun farklı işlemlerde de kullanılabilir.

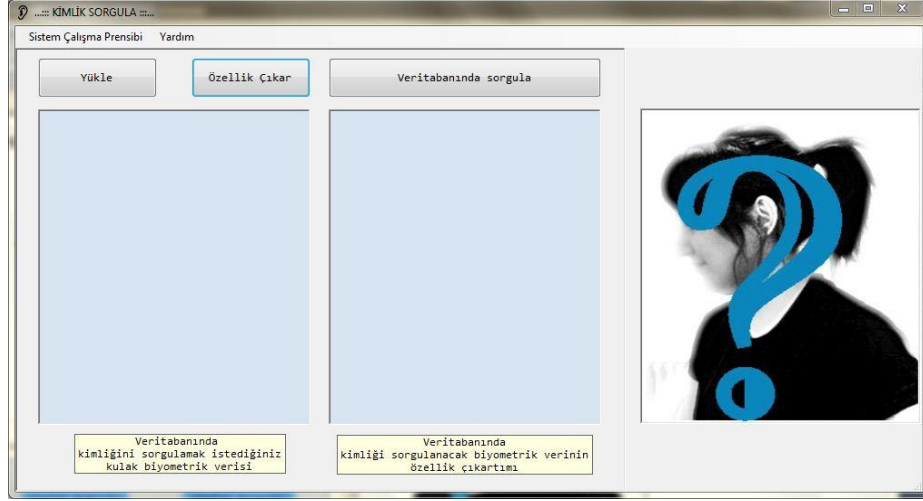
Normalizasyon bir görüntü fonksiyonunun  $g_1(x, y)$  den  $g_2(x, y)$  ye dönüşüm işlemidir. Böylelikle orijinal görüntüdeki ilgili tüm bilgiler korunurken aynı zamanda normalleştirme kriterleri olarak adlandırdığımız koşullar kümesini de karşılamaktadır. Buna bağlı olarak  $g_2(x, y)$  nin orijinal görüntü nün  $g_1(x, y)$  standart bir versiyonudur diyebiliriz (Abu-Mostafa ve Psaltis 1985). Görüntüdeki her bir nesnenin birbirinden farklılık gösteren farklı parametreleri vardır. Bu farklılıklar boyutu, konumu, açısı gibi parametreler olabilir. Normalize işlemi ile bu farklılıklar yok edilerek veri kümesinde belirli bir standart sağlanır. Kulak biyometrisinde alınan örneklerde görülen en büyük fark kulak eğiminin farklı oluşudur. Görüntü normalize edilerek veri kümesindeki kulakların duruş açısına belirli bir standart getirilmiştir. Bu standart için kontur bulma fonksiyonunda elde edilen noktalar kümesinden faydalanılmıştır.

Yapılan tüm görüntü işleme adımlarından sonra elde edilen örnek, ad-soyad ve şifre bilgisi ile veri tabanına kaydedilir.

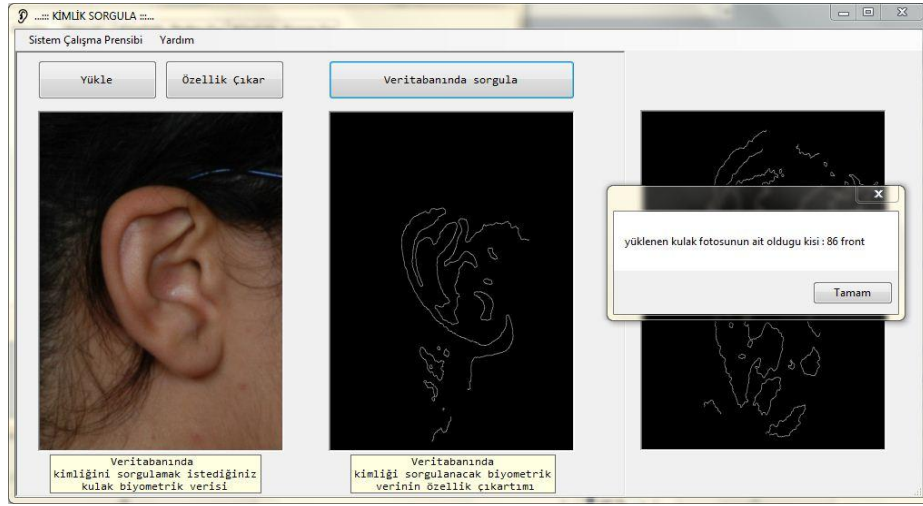
Şekil 9.25’de kimlik sorgulama sayfası görülmektedir. Burada soldaki resim kutusuna sorgulanacak kulak görüntüsü yüklenir ve ikinci resim kutusuna özellik çıkartılır. Daha sonra bire-çok arama yaparak özelliği çıkartılan kulak görüntüsü veri tabanında tüm örneklerle karşılaştırılır. Eşleşme oranı en az çıkan benzerliği en fazla olanıdır. Tüm veri tabanında karşılaştırma yapıp eşleşme oranları hesaplanır. En düşük değere sahip olan örnek aranan kişi olarak tespit edilir ve veri tabanındaki kayıtlı ismi ekrana yansıtılır (şekil 9.26).

Şekil 9.27’de kimlik doğrulama sayfası görülmektedir. Kimlik doğrulamada bir kulak örneği yüklenir, özellik çıkartılır ve kime ait olduğuna dair bir iddiada bulunulur. Bire-bir karşılaştırma yaparak iddia edilen örnek ile veri tabanındaki iddiada bulunulan isimdeki gerçek kayıt karşılaştırılır. Eğer eşleşme oranı belirlenen eşik değerinden küçükse, yüklenen kulak görüntüsünün iddia edilen kişi olduğu kabul edilmektedir.

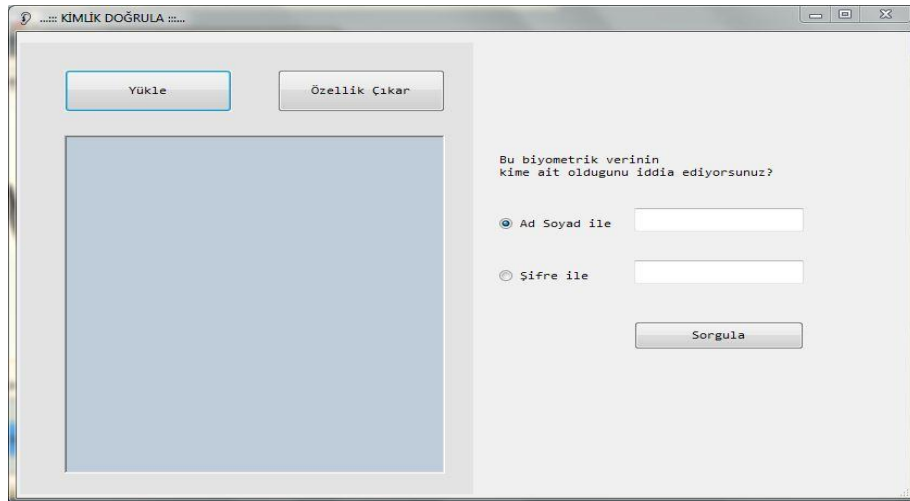




Şekil 9.25: Kimlik sorgula sayfası ekran görüntüsü



Şekil 9.26: Yüklenen kulak görüntüsünün özelliğini çıkartıp veri tabanında sorgulama



Şekil 9.27: Kimlik doğrula sayfası ekran görüntüsü



Örnekleri karşılaştırırken Cosinus benzerliği, surf match, sift match, kontur eşleştirme gibi farklı yöntemler denenmiştir. İstenen verimliliğe ulaşılamamıştır. Karşılaştırma metodu olarak Hu momentlerinin kullanıldığı karşılaştırma işlemi yapılmıştır. Bu karşılaştırma işlemi ile

$$m_i^A = \text{sign}(h_i^A) \cdot \log|h_i^A| \quad (9.13)$$

$$m_i^B = \text{sign}(h_i^B) \cdot \log|h_i^B| \quad (9.14)$$

ve  $h_i^A$  ile  $h_i^B$  sırasıyla A ve B nin Hu momentleri iken 3 farklı karşılaştırma yöntemi

$$I_1(A, B) = \sum_{i=1}^7 \left| \frac{1}{m_i^A} - \frac{1}{m_i^B} \right| \quad (9.15)$$

$$I_2(A, B) = \sum_{i=1}^7 |m_i^A - m_i^B| \quad (9.16)$$

$$I_3(A, B) = \sum_{i=1}^7 \left| \frac{m_i^A - m_i^B}{m_i^A} \right| \quad (9.17)$$

elde edilir. Buradan dönen sonuç ne kadar küçük ise görüntüler o kadar benzerdir. Bire-bir benzeme durumunda sonuç 0 hesaplanır.

Hu (1962) geometrik moment teorisinden 7 değişmez moment geliştirmiştir. Bu yedi moment döndürme, konum, yönelim gibi işlemlere karşı bağımsızdır (Sabhara ve diğ. 2013). Yedi Hu momentleri aşağıda verilmiştir.

$$M_1 = (\eta_{20} + \eta_{02}) \quad (9.18)$$

$$M_2 = (\eta_{20} + \eta_{02})^2 + 4\eta_{11}^2 \quad (9.19)$$

$$M_3 = (\eta_{30} + \eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \quad (9.20)$$

$$M_4 = (\eta_{30} + \eta_{12})^2 + (\eta_{21} + \eta_{03})^2 \quad (9.21)$$

$$M_5 = (\eta_{30} - 3\eta_{12})^2(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - (3\eta_{21} - \eta_{03})^2] \quad (9.22)$$

$$\begin{aligned} M_6 = & (\eta_{20} + \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \\ & + 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \\ & + (3\eta_{21} + \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 \\ & - (3\eta_{21} - \eta_{03})^2] \end{aligned} \quad (9.23)$$

$$\begin{aligned} M_7 = & (3\eta_{21} - \eta_{03})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} - \eta_{03})^2] \\ & - (\eta_{30} + 3\eta_{12})(\eta_{21} + \eta_{03})[(\eta_{30} + \eta_{12})^2 \\ & - (\eta_{21} - \eta_{03})^2] \end{aligned} \quad (9.24)$$

Aynı açılarda ve farklı açılarda kulak görüntüleriyle denenen sistemde elde edilen doğruluk oranı ve ortalaması Tablo 9.2'de verilmiştir.

Yapılan testler neticesinde 100 kişiye ait kulak fotolarının düz bir açıyla alındığı 'front' adlı görüntüler sisteme yüklenmiş ve kimlik tespitinde % 96 doğruluk elde edilmiştir (Tablo 9.3). Farklı kulak açılarına göre kulak tespiti yapmak için de veri tabanındaki 'subset-4' deki 82-106 arasındaki 25 görüntü kullanılmıştır. Sisteme eğitim için kulak görüntülerinden 'front' eklenip farklı açılarda kulak görüntüleri kullanarak sistem test edilmiştir. Test sonucu kontur alanı 10 ve üzeri konturlar için, Gaussian pürüzsüzleştirme işlemi gerçekleştirilip, ikili seviye (binary) oranı 108 olarak alındığında % 72 doğruluk elde edilmiştir (Tablo 9.4). Görüntü iyileştirme aşamasında pürüzsüzleştirme işlemi esnasında medyan yumuşatma kullanılarak test edildiğinde doğruluk oranı % 40 elde edilmiştir. Bu da bize görüntü iyileştirme aşamasındaki parametrelerin sonuçlara ne kadar etki ettiğini göstermektedir. Görüntülerdeki kontur bulma işlemi esnasında kontur alanınının 20 den büyük olduğu konturlar esas alındığında doğruluk oranınının %32 düştüğü görülmüştür. Bu da bize

esas alınan konturların miktarının artmasıyla, ayrıntının arttığını ve daha çok karşılaştırma alanı olduğu için daha iyi sonuçlar elde ettiğimizi göstermektedir. İkili seviye görüntü yapma işleminde oran 104'e düşürüldüğünde % 44 doğruluk elde edilirken, 110' a çıkarıldığında %56 elde edilmiştir. Benzeme sonucu elde edilen değer sıfıra yaklaştıkça eşleşme oranı artmaktadır. Bu durumda %100 eşleşmede benzeme oranı sıfır çıkmaktadır.

**Tablo 9.2:** Çalışmanın eşleşme doğruluğu oranları.

GÖRÜNTÜ TÜRÜ	DOĞRULUK ORANI
Aynı açıdan görüntüler kullanıldığında	% 96
Farklı açılardan görüntüler kullanıldığında	% 72
Ortalama	% 84

**Tablo 9.3:** Aynı açılardan oluşan kulak görüntüleri kullanılmasıyla belirlenen parametrelere göre yapılan test ve sonucu.

	Kullanılan toplam kulak sayısı	100 eğitim-100 test
Veri tabanı işlemleri	Kullanılan kümeler	subset-1,2,3,4
	Kullanılan görüntüler	1-106 arası örnekler
	Veri tabanındaki görüntü(işlemsiz)	evet
Parametreler	Canny kenar algoritması	100
	İkili görüntü yapma (binary)	108
	Aşındırma (dilation)	3
	Parlatma (bright)	3
Normalizasyon	Açı değiştir (rotate process)	evet
Yumuşatma	Gaussianblur	Evet
Sonuc	Doğru eşleşme	96%

**Tablo 9.4:** Farklı açılardan oluşan kulak görüntüleri kullanılmasıyla belirlenen parametrelere göre yapılan test ve sonucu.

	Kullanılan kulak sayısı	25 eğitim-150 test
Veri tabanı işlemleri	Kullanılan kümeler	subset-4
	Kullanılan görüntüler	82-106 arası örnekler
	Veri tabanındaki görüntü(işlemsiz)	Evet
Parametreler	Canny kenar algoritması	100
	İkili görüntü yapma (binary)	108
	Aşındırma (dilation)	3
	Parlatma (bright)	3
Normalizasyon	Açı değiştir (rotate process)	Evet
Yumuşatma	Gaussianblur	Evet
Sonuc	Doğru eşleşme	72%

## 10. SONUÇ VE ÖNERİLER

İnsanların binlerce yıldır birbirini tanımak için kişiye özgü karakteristik özellikleri kullandığını bilinmektedir. Çoğu zaman yüzünden, bazı zaman sesinden, bazen de yürüyüşünden kişinin kim olduğunu rahatlıkla söyleyebilmekteyiz. Bu durumdan yola çıkarak, gözleme dayalı bu tanıma işlemini makine ortamına taşıma fikri ortaya çıkmış ve son zamanlarda gittikçe yaygınlaşmıştır. Literatürde pek çok farklı biyometrik yöntem olup, her birinin diğerinden farklı üstünlükleri ve eksiklikleri bulunmaktadır.

Bu çalışmada kimlik tespiti için kulak biyometrisi kullanılmıştır. Kulak şeklinin yaşa bağlı olarak değişim göstermemesi, yapısında pek çok kıvrıma sahip olup karşılaştırılacak özellik sayısının fazla olması, ülkemizde bu konu hakkında yapılan çalışmaların azlığı kulak biyometrisi yönteminin bu tezde kullanılma nedenini oluşturmaktadır. Parmak izi, yüz tespiti gibi klasik çok bilinen bir yöntem olmaması, retina taraması, beyin dalgaları ölçümü gibi maliyetli olmaması sebepleri de ayrıca kulak biyometrisi seçiminde etkili olmuştur.

Biyometrik yöntemlerle kimlik tespiti yapılabilmesi için gerekli ön bilgi literatür çalışması yaparak elde edilmiştir. Pek çok biyometrik yöntem hakkında bilgi sahibi olunmuştur. Kimlik tanıma ve doğrulama sistemleri incelenmiştir. Sistem için uygun forma getirilmiş görüntü elde edilebilmesi için görüntü işleme teknikleri hakkında bilgi sahibi olunmuştur. Tüm bu hazırlık sürecinden sonra tasarlanan sistem ile kimlik tanıma işlemi gerçekleştirilmiştir.

Çalışmada sistemi test etmek AMI veri tabanındaki 100 bireye ait 700 kulak görüntüsü kullanılmıştır. Renkli kulak görüntüsüne morfolojik işlemler uygulanarak kontur bilgisi elde edilmiş ve Hu momentleri kullanılarak eşleştirme yapılmıştır.

Kullanılan veri tabanındaki kulak görüntüleri kısmen saç ve yüz bölgesinden de alanları içermektedir. Çalışma sadece kulak alanlarına yönelik olduğundan görüntülerin bir kısmındaki bu saç ve yüz alanları eşleştirme başarısına olumsuz etki etmiştir. Ayrıca kullanılan görüntülerin bir kısmında küpe, bir kısmında gözlük, bir kısmında ise saçın kısmen de olsa kulağı kapattığı görülmektedir. Bu kapanan alanlar

da eşleştirmeyi olumsuz etkileyen faktörlerdir. Aynı açıdan kulak görüntülerinde eşleştirme başarısı % 96 gibi gayet umut vaat edici oranlardayken, açının değişmesi ile bu oranın % 72'lere düştüğü görülmektedir. Görüntüsü alınan bireyin baş pozisyonunun sağa, sola, yukarıya ve aşağıya çevrilmiş durumlarında, kulağa etki eden ışık açısının değiştiği gözlemlenmiştir. Bu durumda kontur bilgisi de değişmektedir. Kullanılan veri tabanında elde edilen görüntüler farklı ışık durumlarında, farklı ortamlarda toplandığından, sistem tasarlanırken belirlenen standart parametreler bazıları için çok net özellik çıkartmayı sağlarken, bazıları içinse kötü özellik çıkartılmasına sebep olmuştur. Veri tabanındaki bazı kulaklar aydınlık bir ortamda alınırken, bazıları ise daha karanlık ortamda elde edildiği anlaşılmaktadır. İlerleyen çalışmalarda ortam farklılıklarından kaynaklanan, her görüntünün kendi özel şartlarına göre görüntü iyileştirme yöntemi yapılırsa daha iyi sonuçlar alınacağı düşünülmektedir.

Her bir biyometrik sistemin kullanım amacı farklıdır fakat her durumda tek bir biyometrik yöntemin tek başına yeterli olmadığı görülmektedir. Bu yüzden iki ya da daha fazla yöntemin bir arada kullanıldığı hibrit sistemler her zaman için daha güvenlidir. Sistemde istenen güvenlik düzeyine göre elde bulunan yöntemlerin fazla olması her zaman avantajdır. Özellikle terör saldırıları gibi suçlu tanımda bir çok biyometrik yöntemin halihazırda bulunması, hangi biyometrik veri elde edilirse (parmak izi bilgisi, yüz termogramı, damar haritası) buna uygun yöntemin devreye girerek tanıma yapabilmesi oldukça önemlidir.

Üst düzey askeri bir üsse sadece imza ile girmek, ya da oturduğumuz sitenin güvenliğinden geçebilmek için beyin MR çekirmek ya da kamera görüntülerin de çok da net olmayan bir suçluyu retina taraması yaparak tanıma çalışmak çok da mantıklı olmayacaktır. Bu sebepten tüm biyometrik sistemler geliştirilmeli, hata oranları en aza indirilmeli ve kullanım yerine göre herhangi biri ya da birkaçı arasından seçim yapılmalıdır.

## 11. KAYNAKLAR

Abaza, A., Ross, A., Hebert, C., Harrison, M. A. F. and Nixon, M.S., “A survey on ear biometrics”, *ACM Computing Surveys*, 45(2), (2013).

Abu-Mustafa, Y. and Psaltis, D., “Image normalization by complex moments”, *IEEE Transactions On Pattern Analysis And Machine Intelligence*, 7(1), 46-55, (1985).

Alay-ay, K. M., Meralpis, M. A. L., Romero, D. R., Sison, R.F. and Comendador, B. E.V., “Oto-ID: Ear recognition and shape-based human detection for user identification”, *Journal of Automation and Control Engineering*, 3(2), 146-150, (2015.)

Anwar, A.S., Ghanby, K.K.A. and Elmahdy H., “Human ear recognition using geometrical features extraction”, *International Conference on Communication, Management and Information Technology (ICCMIT)*, Elsevier B.V., (2015).

Ashokkumar, S. and Thyagarajan, K.K., “Retina biometric recognition in moving video stream using visible spectrum approach”, *Green Computing, Communication and Conservation of Energy (ICGCE)*, 2013 International Conference on, Chennai, 180-187, (2013).

Bertillon, A., *Identification anthropométrique*, Melun: Imprimerie Administrative, (1893).

Bodhani, A., “Bodies of evidence”, *Engineering & Technology*, 8(8), 78-81, (2013).

Canny, J., “A computational approach to edge detection”, *IEEE Transactions On Pattern Analysis And Machine Intelligence*, 8(6), 679-698, (1986).

Church, J., Chen, Y. and Rice, S., “A spatial median filter for noise removal in digital images”, *Southeastcon, 2008. IEEE*, Huntsville, AL, 618-623, (2008).

Çevik, K. K., ve Çakır, A., “Görüntü işleme yöntemleriyle araç plakalarının tanınarak kapı kontrolünün gerçekleştirilmesi”, *AKÜ Fen Bilimleri Dergisi*, 31-38, (2010).

Denizci, Ö.M., “Bilişim toplumu bağlamında internet”, *Marmara İletişim Dergisi*, (15), 47-63, (2009).

Ding, L. and Goshtasby, A., “On the Canny edge detector”, *Pattern Recognition*, 34(3), 721-725, (2001).

Fahmy, G., Nassar, D. E. M., Haj-said, E., Chen, H., Nomir, H., Zhou, et al., “Towards an automated dental identification system (ADIS)”, (ed: D. Zhang and A.K. Jain), *International Conference on Biometric Authentication - ICBA*, 3072, Springer-Verlag Berlin Heidelberg, 789-796, (2004).

Faundez-Zanuy, M., “Biometric security technology”, *Aerospace and Electronic Systems Magazine, IEEE*, 21(6), 15-26, (2006).

Galdamez, P. L., Arrieta, A. G., Ramon, M. R., “Ear Recognition using a Hybrid Approach based on Neural Networks”, *17th International Conference on Information Fusion (FUSION)*, Salamanca, 1-6, (2014).

Gonzales, R. C., Woods, R. E., *Digital Image Processing*, Massachusetts, USA: Addison-Wesley, (1992).

Gunetti, D. and Picardi, C., “Keystroke analysis of free text”, *ACM Transactions on Information and System Security (TISSEC)*, 8(3), 312-347, (2005).

Golden P., “Voice biometrics – the Asia Pacific experience”, *Biometric Technology Today*, 2012(4), 10-11, (2012).

Hegde, C., Prabhu, H.R., Sagar, D.S., Shenoy P.D., Venugopal, K R. and Patnaik, L.M., “Heartbeat biometrics for human authentication”, *Signal, Image and Video Processing*, 5(4), 485-493, (2011).

Hemalatha, S., and Wahi, A., “A study of liveness detection in face biometric systems”, *International Journal of Computer Applications*, 91(1), 31-35, (2014).

Hu M.K., “Visual pattern recognition by moment invariants”, *IRE Transactions On Information Theory*, 8(2),179-187, (1962).

Hurley, D.J., Arbab-Zavar, B. and Nixon, M.S., “The ear as a biometric”, (eds: A. Jain, P. Flynn, A.A. Arun), *Handbook of Biometrics*, USA: Springer, 131-150, (2008).



Iannarelli, A., “*Ear identification, Forencis Identification Series*”, Fremont, California: Paramount Publishing Company, (1989).

Jain, A. K., Nandakumar, K., “Biometric system design, overview”, (ed: S. Z. Li), *Encyclopedia of Biometrics*, New York:Springer, 135-140, (2009).

Jain, A. K., Ross, A., Prabhakar, S., “An introduction to biometric recognition”, *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1), 4-20, (2004).

Jamil, N., AlMisreb, A. And Halin A.A., “Illumination-invariant ear authentication”, *Medical and Rehabilitation Robotics and Instrumentation (MRR2013)*, 42, Elsevier B.V., 271-278, (2014).

Jang, J., Kim, H., “Performance measures”, (ed: S. Z. Li), *Encyclopedia of Biometrics*, New York:Springer, 1062-1067, (2009).

Johnson, S., “*Stephen Johnson on Digital Photography*”, O'Reilly Media, (2006).

Kamble, P.D. and Gawali B.W., “Fingerprint verification of atm security system by using biometric and hybridization”, *International Journal of Scientific and Research Publications*, 2(11), 1-3, (2012).

Kandgaonkar, T. V., Mente, R. S., Shinde, A.R. and Raut, S.D., “Ear biometrics: A survey on ear image databases and techniques for ear detection and recognition”, *IBMRD's Journal of Management and Research*, 4(1), 88-103, (2015).

Khitrov, M., “Talking passwords: voice biometrics for data access and security”, *Biometric Technology Today*, 2013(2), 9-11, ( 2013).

Kurniawan, F., Mohd Rahim, M.S. and Khalil, M.S., “Geometrical and eigenvector features for ear recognition”, *International Symposium on Biometrics and Security Technologies (ISBAST)*, Kuala Lumpur, IEEE, 57-62, (2014).

Latha, A.P. and Chaithanya, P.K., “Binary morphology operator to extract binary edge of an image”, *International Journal of Engineering and Advanced Technology (IJEAT)*, 2(6), 26-30, (2013).

Lin, P. L., Lai, Y.H. and Huang, P. W., “An effective classification and numbering system for dental bitewing radiographs using teeth region and contour information”, *Pattern Recognition*, 43(4), 1380-1392, (2010).

Liu, S. and Silverman, M., "A practical guide to biometric security technology", *IT Professional*, 3(1), 27-32, (2001).

Maini, R. and Aggarwal, H. "A comprehensive review of image enhancement techniques", *Journal of Computing*, 2(3), 8-13, (2010).

Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L. and Jain, A.K., "FVC2002: Second fingerprint verification competition", (eds: R. Kasturi, D. Laurendeau and C.Suen), Canada, USA, *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, 3, 811-814, (2002).

Masaoud, K., Algabary, S., Omar, K., Nordin, J. and Abdullah, S.N.H.S., "A review paper on ear recognition techniques: models, algorithms and methods", *Australian Journal of Basic and Applied Sciences*, 7(1), 411-421, (2013).

Narayan, D. and Dubey, S., "A survey paper on human identification using ear biometrics", *International Journal of Innovative Science and Modern Engineering (IJISME)*, 2(10), 9-13, (2014).

Ngugi, B., Kamis, A. and Tremaine, M., "Intention to use biometric systems", *e-Service Journal*, 7(3), 21-46, (2011).

O’Gorman, L., "Securing business’s front door", (eds: S. Ghosh, M. Malek and E. A. Stohr), *Guarding Your Business, A Management Approach to Security*, USA: Springer US, 119-149, (2004).

Prakash, S. and Gupta, P., "An efficient ear recognition technique invariant to illumination and pose", *Telecommunication Systems*, 52(3), 1435-1448, (2001).

Prakash, S. and Gupta, P., "Human recognition using 3D ear images", *Neurocomputing*, 140, 317-325, (2014).

Ross, A. and Abaza, A., "Human ear recognition", *Computer*, 44(11), 79-81, (2011).

Saavedra, B.F., Reillo, R.S., Jimenez, J.L. and Hurtado, O.M., "Evaluation of biometric system performance in the context of Common Criteria", *Information Sciences*, 245,240-254, (2013).

Sabhara, R.K., Lee, C. and Lim, K., “Comparative study of Hu moments and zernike moments in object recognition”, *Smart Computing Review*, 3(3), 166-173, (2013).

Shan, S., Chen, X., Gao,W., “Performance evaluation, overview”, (ed: S. Z. Li), *Encyclopedia of Biometrics*, New York:Springer, 1058-1062, (2009).

Simon, B.P., Eswaran, C., “An ECG classifier designed using modified decision based neural networks”, *The Journal of Biomedical Informatics, Computers And Biomedical Research*, 30, 257-272, (1997).

Singh, B., Kumar, A. And Tomar, P., “A survey on ear biometrics revolution”, 1(7), 333-338, (2014).

Solms, B., Solms, R., “The 10 deadly sins of information security management”, *Computers & Security*, 23(5), 371-376, (2004).

Sonka, M., Hlavac, V. and Boyle, R., *Image processing, analysis, and machine vision*, Springer-Science+Business Media, BV., (1993).

Susanto, H., Almunawar, M.N. and Tuan, Y.C., “Information security management system standards:a comparative study of the big five”, *International Journal of Electrical & Computer Sciences IJECS*, 11(5), 21-27, (2011).

Susmitha, P.N., Reddy, S.S.S., “A review on biometrics and analysis of fusion methods for ear biometrics”, *IJRIT International Journal of Research in Information Technology*, 2(6), 261-272, (2014).

Szeliski, R., *Computer Vision Algorithms and Application*, London, Dordrecht, Heidelberg, New York: Springer- Verlag, (2011).

Şamlı, R. ve Yüksel, M. E., “Biyometrik güvenlik sistemleri”, (eds: M. Akgül, E.Derman, U. Çağlayan, A. Özgüt), *Akademik Bilişim '09*, Şanlıurfa, Ankara, 685-689, (2009).

Tian, J., Zhang, Y. and Cao, K., “Fingerprint matching, automatic”, (ed: S. Z. Li), *Encyclopedia of Biometrics*, New York:Springer, 497-502, (2009).

Uludag, U., Pankanti, S., Prabhakar, S., and Jain, A.K., “Biometric cryptosystems: issues and challenges”, *Proceesings of the IEEE*, 92(6), 948-960, (2004).

Wang, S. and Liew, A.W., “Physiological and behavioral lip biometrics: A comprehensive study of their discriminative power”, (eds: C.Y. Suen, R. Chin, J.Kittler, L.Shapiro, et all.), *Pattern Recognition*, 45(9), 3328-3335, (2012).

Wayman, J.L., “Fundamentals of biometric authentication technologies”, *International Journal of Image and Graphics*, 1(1), 93-113, (2001).

## 12. ÖZGEÇMİŞ

Adı Soyadı : Esmâ YENİSARİ

Doğum Yeri ve Tarihi : İZMİR 06.03.1985

Lisans Üniversite : Celal Bayar Üniversitesi - Matematik

Lisans 2. Üniversite : Anadolu Üniversitesi - İşletme

Y. Lisans Üniversite : Ege Üniversitesi - Matematik Öğretmenliği  
(Tezsiz Yüksek Lisans)

Elektronik posta : esma.yenisari@gmail.com

İletişim Adresi : Barbaros Mah. Çağdaş Sok. No:4 D:4  
ÇANAKKALE

