ÇOKLU BİYOMETRİK SİSTEM TASARIMI

Sercan AYGÜN

Yüksek Lisans Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Şubat - 2016

JÜRİ VE ENSTİTÜ ONAYI

Sercan Aygün'ün "**Çoklu Biyometrik Sistem Tasarımı**" başlıklı **Bilgisayar Mühendisliği** Anabilim Dalındaki, Yüksek Lisans Tezi 04.02.2016 tarihinde, aşağıdaki jüri tarafından Anadolu Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

	Adı-Soyadı	İmza
Üye (Tez Danışmanı)	**: Yrd. Doç. Dr. MUAMMER AKÇAY**	**.....**
Üye	**: Doç. Dr. CÜNEYT AKINLAR**	**.....**
Üye	**: Yrd. Doç. Dr. NİHAN KAHRAMAN**	**.....**

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

Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

ÇOKLU BİYOMETRİK SİSTEM TASARIMI

Sercan AYGÜN

Anadolu Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. Muammer AKÇAY
2016, 99 sayfa

Bu tezde parmak izi ve yüz çoklu biyometrisi kullanılarak elektronik pasaport sistemlerine uyumlu bir biyometrik sistem tasarımı yapılmıştır. Parmak izi verisi için özellik çıkarımı yeni bir yöntem ile *Açıdan Bağımsız Parmak izi Tanıma (ABPT)* kullanılarak sağlanmıştır. Yüz tanıma için önerilen yöntem ise Uluslararası Sivil Havacılık Örgütü (ICAO) standartlarına uygun olan pasaport yüz resimlerini dikkate alarak geliştirilmiştir. Bu yöntem *İlişkisel Bit Operatörü (İBO)* adıyla özellik çıkarımı sırasında kullanılmaktadır. Yüz resminden İBO ile şablon çıkarımı sırasında *dilimle, işle, birleştir* isminde böl ve yönet yaklaşımına benzer bir paralel algoritma yük dengeleme ile çok çekirdekli mimaride çalıştırılmıştır. Biyometrik şablonlar 2 boyutlu kare kod (QR) içine kriptografik olarak gömülmüştür. Şifreleme anahtarı steganografi ile QR resminin içine saklanmıştır. Veri azaltmak için sıkıştırılmış kare kod, parmak izi ve yüz verilerinin karar seviyesi füzyonu için eşleştirme modülüne güvenli bir şekilde transfer edilmiştir. Her adımda gelecek çalışmalarda lojik seviyesi donanım tasarımına uygun algoritma hedefi göz önüne alınarak tamamlanan tez çalışması, analiz ve testler ile bitirilmiştir.

Anahtar Kelimeler: Çoklu Biyometri, Güvenlik, Paralel Hesaplama, Parmak İzi Tanıma, QR Kod, Yüz Tanıma

ABSTRACT

Master of Science Thesis

MULTIBIOMETRIC SYSTEM DESIGN

Sercan AYGÜN

Anadolu University
Graduate School of Sciences
Computer Engineering Program

Supervisor: Assist. Prof. Muammer AKÇAY
2016, 99 pages

In this thesis, e-passport system compliant biometric system modelling has been achieved by using fingerprint and face multibiometrics. Feature extraction for fingerprint data has been done by using a new method, *Angle Invariant Fingerprint Matching (AIFM)*. The method proposed for face recognition has been developed by considering International Civil Aviation Organization (ICAO) standards compatible passport pictures. This method namely *Relational Bit Operator (RBO)* is used during feature extraction. While template has been being extracted via RBO from face pictures, a parallel algorithm named as *slice, process, merge* similar to divide and conquer approach is run on the multicore architecture by using load balancing. Biometric templates are cryptographically embedded into the QR codes. Encryption key is hidden into the QR image via steganography. Compressed QR is transferred into the matcher module in a secure way for decision level fusion of fingerprint and face templates. Thesis has been completed with analysis and tests by considering logic level hardware design appropriateness of every proposed method in each step for future studies.

Keywords: Multibiometrics, Security, Parallel Computing, Fingerprint Recognition, QR Code, Face Recognition

TEŞEKKÜR

Öncelikle bu tez çalışmasının her aşamasında ve ders dönemindeki en büyük desteği sağlayan tez danışmanım Sayın Yrd. Doç. Dr. Muammer Akçay hocama sonsuz teşekkür ve saygılarımı sunarım. Kendisinin sabrı ve desteği olmasa idi, bu tez çalışması ve yüksek lisans araştırma çalışmalarımın bu derece başarılı olması olanaksızdı. Ayrıca değerli hocamın akademik olarak Araştırma Görevliliği mesleğime devam edebilmem adına yayın yapma konusundaki yönlendirmelerinin de beni olumlu olarak ivmelendirdiğini belirtmek isterim.

Ayrıca, eğitim-öğretim hayatım boyunca sırası ile ilköğretimden liseye, lisans eğitimimden daha evvel tamamladığım ilk yüksek lisans dereceme kadar emeği geçen tüm hocalarıma tek tek teşekkürlerimi ve saygılarımı sunarım. Bu kapsamda Eskişehir Osmangazi Üniversitesi Elektrik-Elektronik Mühendisliği ve Bilgisayar Mühendisliği bölümündeki hocalarıma ve ayrıca Sayın Prof. Dr. Ece Olcay Güneş başta olmak üzere İstanbul Teknik Üniversitesi Elektronik Mühendisliği'ndeki hocalarıma ve araştırma görevlisi olarak çalıştığım Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği bölümü akademik ve idari personeline ayrı ayrı saygı ve sevgilerimi sunarım.

Son olarak değerli annem Sayın Filiz Aygün'e ve değerli babam Sayın Tonay Aygün'e hayatımın her anında her konuda destekçi oldukları için sevgilerimi ve hürmetlerimi sunarım.

Sercan Aygün

Şubat 2016

İÇİNDEKİLER

Sayfa

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

SİMGELER ve KISALTMALAR DİZİNİ

AAA : Açık Anahtar Altyapısı

AIFM : Angle Invariant Fingerprint Matching
(Açıdan Bağımsız Parmak izi Tanıma-ABPT)

BAC : Basic Access Control
(Temel Erişim Kontrolü)

CAN : Card Access Number
(Kart Erişim Numarası)

CPU :Central Processing Unit
(Merkezi İşlem Birimi)

CVCA : Country Verifier Certification Authority
(Ülke Doğrulama Sertifikasyon Yetkisi)

DVCA : Document Verifier Certification Authority
(Belge Doğrulama Sertifikasyonu Yetkisi)

DWT : Discrete Wavelet Transform
(Ayrık Dalgacık Dönüşümü)

EAC : Extended Access Control
(Genişletilmiş Erişim Kontrolü)

FAR : False Accept Rate
(Hatalı Kabul Oranı)

FMR : False Match Rate
(Hatalı Eşleştirme Oranı)

FNMR : False Non-Match Rate
(Hatalı Olarak Eşleştirememe Oranı)

FPGA : Field Programmable Gate Array
(Sahada Programlanabilen Kapı Dizileri)

FRR : False Reject Rate
(Hatalı Ret Oranı)

GB :Gigabyte (Gigabayt)

GPU :Graphics Processing Unit
(Grafik İşlem Birimi)

GSEM : Gri Seviyesi Eş-Oluşum Matrisi

HDMI : High Definition Multimedia Interface
(Yüksek Çözünürlüklü Çokluortam Arayüzü)

IC : Integrated Circuit
(Tümdevre)

ICAO : International Civil Aviation Organization
(Uluslararası Sivil Havacılık Örgütü)

JPEG : Joint Photographic Experts Group

kNN : k Nearest Neighbor
(En yakın k komşuluk)

LSB : Least Significant Bit
(En Düşük Anlamlı Bit)

MIMD : Multiple Instruction Multiple Data
(Çok Komutlu Çok Verili)

MRZ : Machine-Readable Zone
(Makine ile Okunabilir Alan)

NFC : Near Field Communication
(Yakın Alan İletişimi)

nm : nanomikron

OCR : Optical Character Recognition
(Optik karakter tanıma)

PCA : Principal Component Analysis
(Temel Bileşen Analizi)

PCT : Parallel Computing Toolbox
(Paralel Hesaplama Araç Kutusu)

RAM : Random Access Memory
(Rastgele Erişimli Bellek)

QR : Quick Response
(Hızlı Cevap; Kare Kod)

RBO : Relational Bit Operator
(İlişkisel Bit Operatörü-İBO)

RFID : Radio Frequency Identification
(Radyo Frekanslı Tanımla)

RSA : Rivest-Shamir-Adleman

SFinGe : Synthetic Fingerprint Generator
(Sentetik Parmak İzi Üreteci)

SIMD : Single Instruction Multiple Data
(Tek Komutlu Çok Verili)

UML : Unified Modelling Language
(Birleşik Modelleme Dili)

VGA : Video Graphics Array
(Video Grafik Dizisi)

VLSI : Very Large Scale Integrated Circuit
(Çok Geniş Ölçekte Tümdevre)

1. GİRİŞ

Bu tez çalışmasında, hedeflenen bir uygulama alanına yönelik olarak akademik zeminde bir sistem tasarımı hedeflenmiştir. Bu sistem biyometrik bir sistemi oluşturacak ve önerilen algoritmayı çalıştıracaktır. Biyometrik uygulamaların kullanım alanları çok çeşitlidir. Bankacılık sektöründen sınırlar arası geçişe, kişisel bilgisayarın güvenliğinden mobil telefonların uygulamalarına kadar pek çok alanda kullanılmaktadır. Bu tez çalışması genel olarak çoklu biyometri kullanarak sınır güvenliğindeki geçişlerde kullanılan elektronik pasaport sistemlerini geliştirmeye yöneliktir. Elektronik pasaportların uymak zorunda oldukları bazı temel standartlar mevcuttur. Örneğin biyometrik yüz resimlerinin uyması gereken bazı temel standartlar vardır. Ayrıca güvenlik ile ilgili bazı alt limit kurallar da mevcuttur. Bu alt kuralların ötesinde bazı ek yenilikler yetkilendirme (*authorization*) ve güvenlik adına ülkelerin kendilerine bırakılmıştır. Örneğin, çoklu modda biyometri kullanmak ve sistem güvenliğini arttırıcı ek çözümler sunmak gibi.

Bu yüksek lisans tezi, çoklu biyometri elemanlarından ilki için parmak izi verisini kullanmaktadır. Önerilen yöntemle parmak izi işlenmesinin ve sınıflandırmanın yapılması tez kapsamında sunulan yeni yöntemlerden biridir. Ayrıca, çoklu biyometrik sistem oluşturabilmek için elektronik pasaport standardındaki yüz biyometrisi de kullanılarak, paralel hesaplama, güvenli veri transferi ve yüz tanıma ile sistem tasarımı modüler düzeyde yapılmaktadır. Yüz biyometrisi için paralel hesaplamayla yüksek başarım hedeflenmiş, biyometrik verilerin paralel hesaplanması da örneklendirilmiştir. Yüz tanıma için kullanılan operatör ve güvenlik detayları da bu tez kapsamında önerilen yeni yaklaşımlardır. Son adımda biyometrik verilerin füzyonu ile sistemin karar modülü de sunulmaktadır. Sistem tasarımının her adımında önerilen yeni yaklaşım, donanım üzerinde gerçeklenebilirlik göz önüne alınarak sağlanmıştır. Bu sebeple olabildiğince basit ve mantık (*lojik*) devre elemanları ile kolayca tasarlanabilir çözümler elde edilmesi hedeftir.

Bu araştırmada, bilgisayar mühendisliğinin 3 temel anabilim dalının bir araya getirilmesi hedeflenmiştir. Tasarlanan algoritmalar bilgisayar bilimleri açısından, önerilen sistemin donanım detayları donanım mühendisliği açısından ve tüm sistemin ayağa kaldırılması ile testlerin uygulanması için kodlamanın yapılması ise yazılım mühendisliği açısından bazı akademik yaklaşımları kullanılmaktadır. Şekil 1.1'de ilgili bu üç bilim dalı kullanılarak hibrit yapı gösterilmektedir.

Şekil 1.1. Bilgisayar Mühendisliği açısından bu tez çalışmasının hibrit yapısı

Güvenlik açıkları her sistem için kaçınılmaz bir sorundur. Ne kadar güvenli olursa olsun her sistemin gözden kaçan zayıf bir noktası mevcuttur ve gelişen teknoloji ile sistemin açığını kullanarak zarar vermek mümkün olabilmektedir. Anlık olarak güvenli nitelendirilen bir yazılım veya donanım sistemi söz konusu bile olsa var olan güvenlik açıkları nedeniyle hesaplama gücü yüksek bilgisayarlar ile bu sisteme sızmak söz konusu olabilir. Teknolojide meydana gelen gelişmeler beraberinde veri güvenliği açısından da bilinçli olma gerekliliğini gerektirir. Hem uygulama geliştiriciler hem de kullanıcılar, güvenliği sağlayan kusursuz bir yol olmadığını bilmelidirler. En temel yöntemle, kaba kuvvet saldırısı (*brute force attack*) kullanılarak, pek çok şifrenin kırılabileceği bir gerçektir. Bu türlü güvenlik saldırıları hesaplama gücü yüksek bilgisayarlarla –örneğin *süper bilgisayarlar*– yapılsa dahi tüm ihtimallerin denenmesi zaman alabilir. Ancak yine de bir şekilde sistemin ele geçirilmesi mümkün olabilmektedir. Kriptografi yardımı ile bir adım daha güvenli sistemler, şifreleme teknikleri kullanarak yazılımsal ve donanımsal çözümler ile sağlanabilmektedir. Performansı yüksek, zaman karmaşıklığı düşük

yeni algoritmalar ve taşınabilir donanımlar kişi güvenliğini arttırıcı çözümler olarak kullanılmaktadır. Bu sebeple bu tez çalışmasında mevcut bir sistemin daha güvenli hale nasıl getirilebileceği üzerine de çalışılmıştır. Biyometrik verilerin kullanılması hedefi ile önerilen sistem, çoklu modda biyometrik veri kullanarak güvenli bir çözüm sunarken, diğer yandan kişiye özel ve değiştirilemeyen verilerin kullanılmasından ileri gelen başka kritik bir durumu da irdelemektedir.

Son zamanlarda görüntü işleme için paralel mimariler de kullanılmaktadır. Biyometrik veriler çok çeşitlidir ancak elde edilebilirlik, hesaplanabilirlik ve elektronik ortamda işlenebilirlik açısından iki veri tipi seçilmiştir: yüz ve parmak izi verisi. Bu tezde önerilen tasarım sırasında uygun formattaki yüz verileri kullanılarak belirli standartlarda çalışılmıştır. Yüz verisinin "*biyometrik fotoğraf*" olarak nitelendirilebilmesi için uyulması gereken arka plan görüntüsü, boyutlar, yüzün tam konumu vb. gibi kurallar vardır. Bu kurallara uygun elde edilen biyometrik verilerden çıkarılan şablonun transferi sırasında güvenlik tehditlerine maruz kalmaması ve verilerin ulaştığı noktada hala kullanılabilir bir formatta örüntü tanıma için anlamlı olması kritiktir. Öte yandan pasaport sistemleri parmak izi verisine de ihtiyaç duymaktadır. Sınır kontrollerinde önceden alınmış olan parmak izi verisi kontrol amaçlı bir kez daha istenerek doğrulama yapılabilir. Önceden kayıtlı parmak izi verisi (veya verileri) ham veri olarak veya bir şablon olarak tutulabilir. Genel olarak pasaport sistemleri biyolojik özetleme (*biohashing*) yöntemi ile özellik çıkarımından elde edilen parmak izi verisinin özet fonksiyonu ile normalize edilmiş halini kullanır. Elektronik pasaport standartlarına uymayı kabul etmiş ülkeler temel bazı teknolojik uygunlukları pasaport defterinde ve sisteminde tümünde sağlamayı kabul etmiş olmalarının yanı sıra ek bazı yenilikler de getirebilirler. Çoklu biyometrinin kullanım biçimi ve kapsamı da bu ek seçenekler arasında sayılabilir.

Sistemin üzerinde çalışacağı donanım da oldukça önemlidir. Sahip olunan mimariye bağlı olarak algoritma geliştirmek performans açısından daha verimli sonuçlar getirecektir. Yapılabilirlik analizinde elde var olan veya satın alınması planlanan donanım bileşenleri de bu kapsamda gözden geçirilmelidir. Bu tez çalışmasında sistem; 4 çekirdekli bir geliştirme kartı, tek çekirdekli verilerin

saklandığı başka bir geliştirme kartı, ileri yönelik olarak geliştirmeye açık kamera ve parmak izi sensörü ile bazı giriş-çıkış birimleri bulundurmaktadır. Donanım bileşenleri, sistem bileşenleri ile aynı olabileceği gibi (örneğin sensör modülü), tek bir kart üzerinde pek çok biyometrik sistem elemanı da gerçeklenebilir (örneğin özellik çıkarıcı, eşleştirici, karar verici modülleri vb.). Hedeflenen bir diğer yaklaşım da donanım tasarımına hizmet etmesi açısından sayısal bir devrenin gelecek çalışmalarda tasarlanabilmesidir. Bu sebeple önerilen algoritmalar, bazı operatörler ve yöntemler Sahada Programlanabilen Kapı Dizilerinde (*Field Programmable Gate Array – FPGA*) tasarlanabilmelidir.

1.1. Elektronik Pasaport Sistemleri

İlk olarak uygulama alanı hakkında bilgi edinmek, algoritma geliştirme ve mevcut eksik yönlerin tespitinde kolaylık sağlayacaktır. Bu bölümde elektronik pasaport sistemleri ve bağlı olarak kullanılan biyometrik sistemler açıklanacaktır. Elektronik pasaport sembolü Şekil 1.2'de verilmiştir.

Şekil 1.2. e-Pasaport sembolü [1]

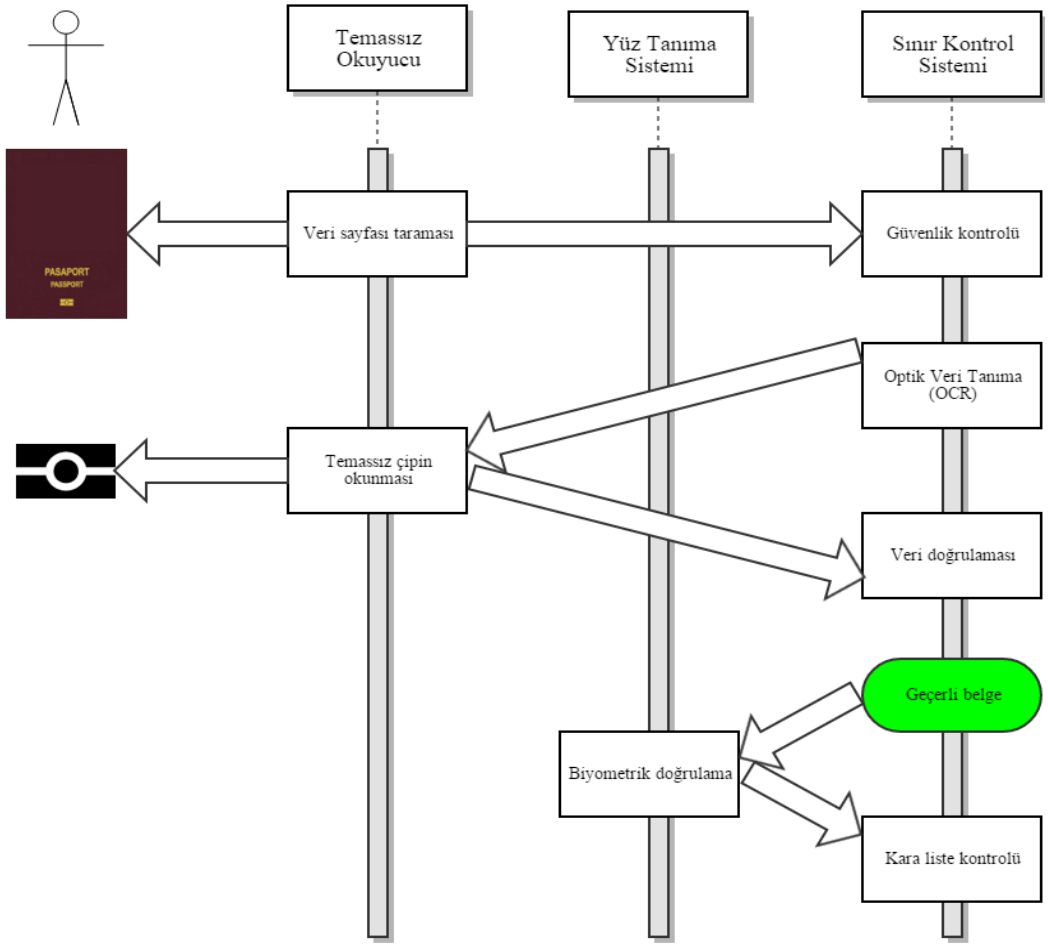
Elektronik pasaportların Uluslararası Sivil Havacılık Örgütü tarafından belirlenen bazı standartlara uyması gerekmektedir. Biyometrik resim bu standartlardan biridir. Şekil 1.3'de Türkiye Cumhuriyeti Emniyet Genel Müdürlüğü'nün resmi sayfasından alınan bazı örnek pasaport resimleri görülmektedir. En sağda verilen olması gereken doğru pasaport fotoğrafı örnekleri için çeşitli koşullarda örnek biyometrik yüz fotoğrafının durumları verilmektedir.

Burada yüz tanıma algoritmalarında işleri kolaylaştıracak bazı hususlardan söz etmek mümkündür. Öncelikle duruş ve yüz verisinin sahip olduğu büyüklük bazı standartlara uymalıdır. Buna ilaveten ışıklandırma netliği bozmadan ve resimdeki verinin homojenliğine zarar vermeden sağlanmalıdır. Diğer önemli nokta olan arka planda kullanılan zeminin beyaz fon olması yüz verisinin koordinatlarını bulmayı kolaylaştırmaktadır. Tüm bu hususlar bir araya gelince mevcut resimde yüzün nerede olduğu aramak için zaman kaybı olabildiğince en aza indirilecektir. Resim üzerinden veri tabanında bir arama söz konusu ise resmin analizi, işlenmesi ve tanınması sırasında geçen zaman oldukça kritik hale gelmektedir. Minimum 32 KB veri taşıyabilen biyometrik pasaportlar ICAO standartları uyarınca JPEG veya JPEG2000 formatında biyometrik veriler saklanmaktadır. Biyometrik veriler yüz veya retina biyometrisi, parmak izi biyometrisi gibi verileri kapsamaktadır.

Şekil 1.3. E-pasaportlarda kullanılmak üzere uygun olan ve olmayan biyometrik yüz resimleri [2]

Tek biyometrik veri kullanan (tekli modda) bir e-pasaport sistemi incelenirse, Şekil 1.4'deki gibi bir akış ile karşılaşılmaktadır. Elektronik pasaportlar bilgisayar tarafından okunabilen bir koda sahiptir. Bilgilerin bulunduğu bilgisayar tarafından okunabilen bu kod (*machine readable code*) ve pasaport içinde bulunan elektronik yonga kişiye ait olan verilere erişim için kullanılmaktadır. Elektronik yonga içinde

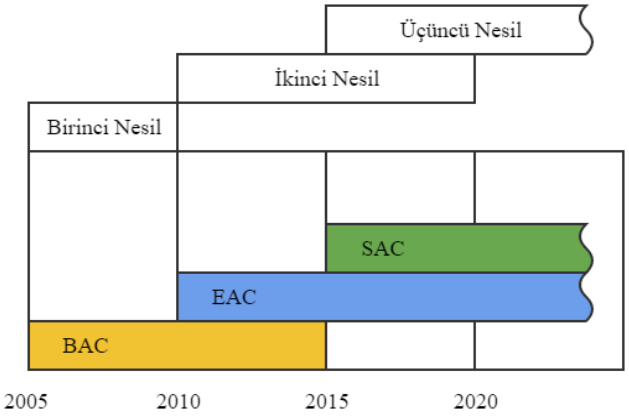
biyometrik verilerin şablon halleri tutulmaktadır. Birçok ülkede doğrulama işlemi yalnızca yüz tanıma ile sağlanmaktadır. Bu tez çalışmasının bir amacı da bu türlü sistemlerde çoklu biyometrinin yaygınlaşmasını sağlamaktır. Pasaport sisteminin akışında veri sayfasının taranıp bilgisayar tarafından anlamlı kodun kullanılmasından sonra güvenlik kontrolü yapılmaktadır. Daha sonra sınır kontrol sistemi üzerinden elektronik yonga içindeki veri doğrulaması ile belgenin geçerliliği kontrol edilmektedir. Yonga içindeki ve taranan pasaport sayfasındaki bilgiler doğru ise ardından biyometrik sistem devreye girerek kontrol sağlamaktadır. Bu tez çalışmasının amacı bu sırada devreye giren biyometrik sistem için çoklu modda bir çözüm sunmaktır. Standart olarak çoğunlukla kullanılan tekli biyometri yerine çoklu biyometri ile daha yenilikçi çözümler sunulacaktır.



Şekil 1.4. e-Pasaportlarda doğrulamaya ilişkin sistem akışı [3]

Elektronik pasaport standartları genel olarak Uluslararası Sivil Havacılık Örgütü (ICAO) tarafından belirlenmektedir. Şekil 1.5'te gösterildiği gibi 3 tip e-pasaport nesli söz konusudur. Birinci nesil BAC (*Basic Access Control*) temel erişim kontrolü olarak taban gereksinimleri kullanmaktadır. Bu nesil, biyometrik yüz resminin saklanmasını sağlasa da biyometrik veri ile çalışmayı desteklemez. BAC protokolü e-pasaporta fiziksel bir erişim olmadan veri okunmasını engeller. Elektronik pasaport kullanmayı kabul eden ülkelerde 2005 ve 2009 yılları arasında bu protokol kullanılmıştır. Elektronik yonga ve okuma terminali arasında haberleşme simetrik bir anahtar ile sağlanmaktadır. Pasaport sayfasında kişisel bilgilerin bulunduğu ve altında da bir kod olan alan mevcuttur. Makine ile okunabilir alan (*Machine-Readable Zone* - MRZ), ismi verilen bu kod ile anahtar üretimi sağlanmaktadır. Optik karakter tanıma (*Optical Character Recognition* - OCR) ile MRZ verisi terminal tarafından okunmaktadır. BAC protokolü elektronik yongayı klonlamaya karşı korumamaktadır. Bu protokolde MRZ değişmediği ve sabit bir anahtar kaynağı söz konusu olduğu için entropinin düşük olması bir dezavantajdır. ICAO, BAC için pasif doğrulamayı (*Passive Authentication*) zorunlu kılmıştır. Buna göre her elektronik pasaportun veri bütünlüğü (gerçekçiliği-*authenticity*), yani veri değişikliği olup olmadığı kontrol edilmektedir. Pasaport içinde veri, her bir ülke tarafından sağlanan dijital imza (*digital signature*) ile tutulmaktadır. Dijital imza doğrulaması ile veri gerçekçiliğinin kontrolü yapılır; ancak bu kontrol pasaportun kopya olup olmadığını anlamaya yetmez. Aktif doğrulama (*Active Authentication*) yöntemi ile veri kopyalaması önlenebilmektedir. Yonga içinde saklı bir gizli anahtar ve yongaya ait terminal ile haberleşmeyi sağlayan açık anahtar ile kontrol sağlanmaktadır. Aktif Doğrulama yönteminin ülkelerce kullanımı opsiyoneldir. Almanya tarafından kullanıma sunulan ikinci nesil güvenlik mekanizmasına bakıldığında genişletilmiş erişim kontrolü (*Extended Access Control* - EAC) ile parmak izi, iris vb. gibi biyometrik verilerin de kullanımı sağlanmıştır. Avrupa Birliği tarafından 2006 yılında onaylanan bu mekanizma ICAO tarafından zorunlu tutulmamıştır. İkinci nesil EAC ile ek olarak biyometrik verilerin güvenli kullanımı söz konusudur ve birinci nesil BAC aynen bırakılmıştır. Ancak bu mekanizmayı kullanmak ülkelerin inisiyatifindedir. Bu mekanizma ile

yonga doğrulaması (*Chip Authentication*) yöntemi RSA anahtar çifti kullanarak biyometrik veri şablonu transferi sağlamaktadır. Öte yandan biyometrik verilere erişim terminal doğrulaması (*Terminal Authentication*) ile daha güvenli hale getirilmiştir. Buna göre yalnızca izin verilen terminallerden veri erişimi sağlanabilmektedir. Elektronik pasaport yongası, ülke doğrulama sertifikasyon yetkisi (*Country Verifier Certification Authority* - CVCA) ile bir sertifika bulundurur. CVCA sertifikası ilgili pasaportun ait olduğu ülke tarafından sağlanmaktadır. Terminalin güvenilirliği belge doğrulama sertifikasyonu yetkisi (*Document Verifier Certification Authority* - DVCA) ile sağlanan sertifika sayesinde anlaşılmaktadır. DVCA terminal sertifikası hiyerarşik olarak diğer sertifikalarla birlikte yongaya erişir. Yonga terminale rastgele bir sayı gönderir ve terminal de bu sayıyı imzalayarak geri gönderir. Ardından yonga üzerinde terminal sertifikasında bulunan açık anahtar ile ilgili imzanın doğruluğu kontrol edilir. Bu yaklaşım AAA, Açık Anahtar Altyapısı (*Public Key Infrastructure*) gerektirir. 2010 yılında ICAO tarafından sunulan 3. nesil e-pasaportların ise 2014 yılından itibaren Avrupa ülkeleri tarafından kullanımı zorunludur. Tanımlayıcı Erişim Kontrolü (*Supplemental Access Control*-SAC), ismindeki bu yeni nesil BAC üzerindeki dezavantajları gidermeye yönelik bir sistemdir. Kullandığı 6 haneli kart erişim numarası (*Card Access Number*-CAN) ile BAC'de bulunan düşük entropi problemini önler. Diffie Hellman anahtar değişimi algoritması ile oturum anahtarı kullanan SAC, anahtar üretimi bakımından kart erişim numarası entropisine bağımlı değildir. SAC gelecek 10 yılın e-pasaport teknolojisini oluşturmaktadır [4].



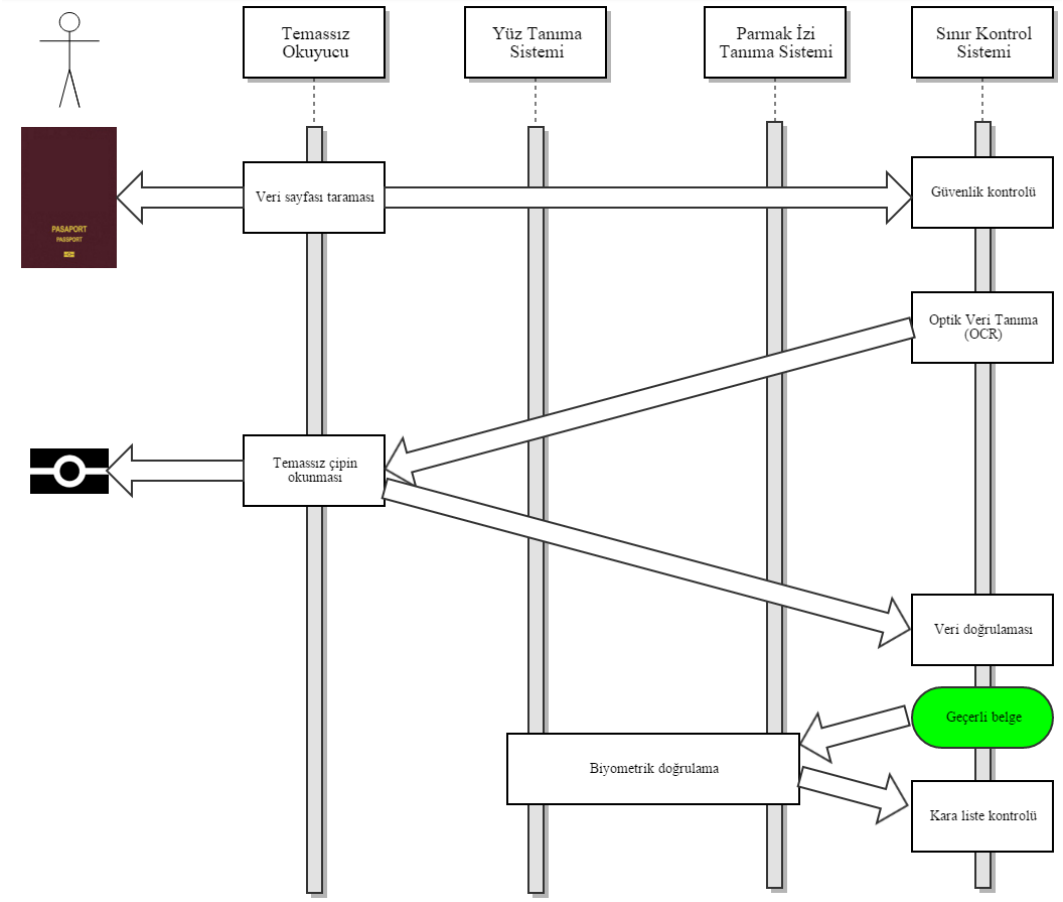
Şekil 1.5. Elektronik pasaportun güvenlik mekanizmalarının gelişimi [4]

1.2. Hipotez

Bu tez çalışması, sunulan bazı yeni teorik yaklaşımlarım gerçek bir uygulama ile hayata geçirilmesi ve bu sayede de ilgili teorinin testini hedeflemektedir. Bu kapsamda ilgili savın tanımı en başta yapılmalıdır. Böylelikle hipotezin ne denli akademik zemine oturtulabileceği de ortaya çıkmış olacaktır. Şekil 1.4'de gösterilen standart sisteme yeni bir ilaveyle parmak izinin de çoklu biyometri alt yapısında performans için paralel hesaplama ve veri güvenliği düşünülmelidir. Düzenlenen yeni çoklu biyometrik tabanlı sistem Şekil 1.6'da gösterilmektedir. Sistem tasarımı yapılırken yalnızca sistemin çalışması değil kullanılan verinin güvenliği ve ilgili sistemin performansı da göz önüne alınmalıdır. Performans için paralel hesaplama, güvenlik için ise kriptografi ile şifreleme söz konusudur. Bu tez çalışmasının bir amacı da olabildiğince yeni yöntem sunmaktır. Bu sebeple biyometrik verilerden özellik çıkarımı standart yöntemlerden farklı yapılmalıdır. Tez hipotezinin öngördüğü; yeni özellik çıkarımı yöntemi ve eşleştirme yöntemi, yeni paralel algoritma ile biyometrik veri işleme ve görsel kriptografide yeni bir fikir ile biyometrik veri güvenliği elde etmektir.

Özetle, bu tez kapsamında savunulan hipotez şu şekildedir:

1. *Parmak izi ve yüz biyometrik verileri için e-pasaport sistemlerine uygun olarak özellik çıkarımının yeni yöntemlerle yapılması.*
2. *Performans artırımı için paralel hesaplama kullanımı.*
3. *Sistem modülleri arası güvenli biyometrik şablon transferinin sağlanması.*
4. *Karar seviyesi biyometrik veri füzyonunda oylama yöntemi ile kullanıcı doğrulamasının uygun sınıflandırmayla yapılması*
5. *Önerilen yöntemlerin donanımda tasarlanabilir olması.*



Şekil 1.6. Standart e-pasaport sistemlerine çoklu biyometri yaklaşımının eklenmesi

1.3. Motivasyon

Mevcut biyometrik sistemlerde ve özellikle elektronik pasaport kullanan pek çok ülkede biyometrik verilerin bir arada kullanılarak füzyon yapılması henüz çok yaygın değildir. 2004 yılında Pakistan'da kullanılan bir sistem ile 7 milyona yakın kişi çoklu biyometri özelliği olan e-pasaport kullanmaktadır. Bu pasaport yüz ve parmak izi verilerini bir arada işlemektedir [5]. Ancak verilerin nasıl füzyon edildiği ile ilgili herhangi bir bilgi bulunamamıştır. Öte yandan Hollanda'da da çoklu moddaki biyometrik verilerin pasaportlar üzerinde kullanımı denenmektedir [6]. Ülkemizde öngörülen kimlik kartı değişikliği ve medyada yer bulan bu kartların pasaport gibi kullanılabilir olacağı haberleri de göz önüne alınırsa, bu konudaki eğilimin biyometrik verilerin elektronik ortamda işlenerek doğrulama sağlanacağı

yönündedir. Parmak izi, yüz, el ayası, parmak damarı ve iris e-devlet uygulamalarında kullanılması öngörülen biyometrik veri çeşitleridir. Bu tez çalışması bu noktadan motivasyon alarak, 2 veri tipini –parmak izi ve yüz– kullanarak sistem tasarımı hedeflemektedir. Parmak izi eşleştirme için de, yüz tanıma için de pek çok metot kullanılmaktadır. Bu yöntemler frekans bazlı Fourier analizinden, *gradient* operatörüne, temel bileşen analizinden (*Principle Component Analysis*-PCA), Haar özelliklerine kadar pek çok örneğe sahiptir. Literatür incelendiğinde başarı oranları çok yüksek, performans cevabı hızlı çözümler bu yöntemlerle elde edilebilir. Ancak donanımda gerçeklenebilirlik ilkesine bakıldığında iki temel sorun ortaya çıkmaktadır: *yonga üzerinde alan ve çalışma hızı* [7]. Analog IC tasarımdan, lojik seviyesi VLSI tasarıma kadar donanım mühendisliğinin tüm kollarında bu iki parametre arasında bir ödünleşim (*trade-off*) söz konusudur. Alandan kayıp ile hız arttırılabilir veya hızdan feragat edilerek alandan kazanç sağlanabilir. Nanomikronlar (nm) seviyesindeki boyutlarda eleman barındıran kırmık için bu iki parametrenin de önemli olduğu açıktır. Bu sebeple bilgisayar bilimlerinde önerilen tüm bu yöntemler, donanım üzerinde bir modül olarak gerçeklenmeye çalışıldığında bazı sorunlar da beraberinde gelmektedir. Erişim sistemlerinde (özellikle biyometrik özelliği olanlarda) akıllı kart, RFID, NFC gibi elektronik araçların (literatürde erişim sistemlerinde genel olarak *token* ismi ile anılmaktadır) kullanıldığı düşünüldüğünde bazı özellik çıkarımı, sınıflandırma, eşleştirme, karar algoritmalarının bu kartlarda gerçeklenebilmesi söz konusu olabilir. Bazı temel algoritmaların kart içinde koştuğu ve eşleştirmenin de kartta yapıldığı bazı akıllı kartlar (*match-on cards)* birer donanım olduklarından yine alan ve hız parametrelerine takılmaktadır. Bu sebeple bu tez çalışmasında önerilen yöntemlerin olabildiği kadar basit lojik devrelerle gerçeklenebilmesi de motivasyonu oluşturan bir etmendir.

Öte yandan biyometrik verilerin gizliliği de sistem tasarımı için oldukça önemlidir. Her erişim sistemi modüller arası (*inter-module*) ve kendi modülü içinde (*intra-module*) haberleşirken bazı ataklara maruz kalabilir. Bu ataklardan en çok risk arz edeni biyometrik verilerin kendisinin veya elde edilen şablonunun ele geçirilmesine yönelik olandır. Bu tez çalışmasında bir diğer uygulanan yöntem ile

biyometrik veriden özellik çıkarımı sonrasında elde edilen anlamlı verinin güvenli olarak modüller arası transferidir. Bu motivasyon noktasından hareketle verilerin görsel kodlama elemanı ile gizlenerek transferi söz konusu olacaktır.

Son olarak güncel bir konu olan görüntü işlemenin paralel olarak hesabı için de tez çalışması kapsamında bir hareket noktası söz konusudur. Yüz tanıma sırasında özellik çıkarımının paralel hale getirilmesi, pasaport resimlerine ait düzgün simetri, beyaz arka plan özelliği, başın pozisyonu ve ışıklandırma gibi avantajlardan dolayı resmin bloklara ayrılarak yapılmasını sağlayacaktır.

1.4. Problemin Tanımı ve Kısıtlar

Doğru problem tanımı ve problemin ait olduğu çalışma alanını doğru belirlemek öncelikle tüm değişkenlerin doğru belirlenmesine yardımcı olacak ve böylece problem çözümüne ulaşmak için izlenen yolda da doğru bir ilk adım atılmış olacaktır. Problem çözümünde kullanılan adımlar Şekil 1.7'de gösterilmektedir.

Problem Tanımı:

- Tekli biyometrik veri kullanımdan ileri gelen güvenlik sorunları, daha kolay atak yapılabilirlik ve biyometrik verisine ait problem sahibi kişiler için doğrulama sıkıntısı (örneğin ellerini kaybetmiş bir kişi için yalnızca parmak izi tanıma kullanılamaz)
- Farklı tipteki biyometrik verinin füzyonu ile ortaya çıkan problem
- Özellik çıkarımının hem parmak izi hem de yüz tanıma için düşük seviye donanımda gerçeklenmesi gerekliliği ve mevcut algoritmaların karmaşık oluşu
- Matris yapısındaki yüz resminin görüntü işlemeden ileri gelen uzun işlem süresi
- Artan sayıda biyometrik veri için çoklu mod söz konusu olduğunda ortaya çıkan gizliliği koruma problemi

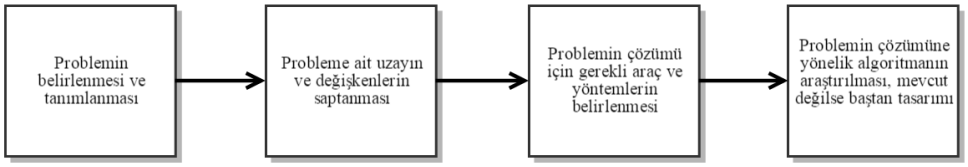
Problem Uzayı:

- Biyometrik sistemin çalıştığı donanım ile kendi içindeki modüler yapısı ve sahip olunan geliştirme ortamına ilişkin yazılım.

- Biyometrik verinin alındığı giriş kısmı, verinin özellik çıkarımı ve eşleştirme ile karar için kullanıldığı modüller ve verilerin saklandığı bir veri tabanı veya hafıza alanı.

Problem Çözümü:

- Biyometrik bir sistem tasarımında kolay, güvenli ve performansı daha yüksek çözümler sunmak ve mümkün olabildiği kadar yeni yöntem ile akademik değeri yüksek çözümler üretmek.
- Biyometrik sistem tasarımının donanımda daha aşağı seviyede tasarlanabilirliği göz önüne alınarak, basit çözümler ile özellik çıkarımının hem parmak izi hem de yüz verisi için yapılması ve teze özgü yöntemin ortaya konulması.
- Yüz biyometrik verisi için paralel hesaplamadan faydalanarak çoklu çekirdekli mimarinin avantajlarını kullanmak. Elde edilen şablonların karar aşaması için güvenli transferinin yeni bir yöntemle sağlanması.



Şekil 1.7. Bir probleme yönelik çözüm adımları [8]

Bu çalışmaya ait bazı kısıtlar da mevcuttur. Bunlar en temel olarak hafıza ve performansla ilgilidir ve esasen önceki kısımda bahsedilen alan ve hız ile ilişkilidir. Kısıtlar problemin kendisini oluşturan değişkenlerdir ve bunlar üzerinden çözüme gidilecektir. Bu sebeple donanım üzerinde algoritma gerçeklendiğinde daha az yer kaplaması açısından tasarımın basit algoritmik çözümlerle yapılması, problem tanımının içindedir. Yine verilerin işlenmesi sırasında paralel hesaplama kullanılması hız problemi ile ilgilidir. Sistemin üzerinde koştuğu hazır donanım bileşenlerinde de çeşitli kısıtlar söz konusu olabilir. Örneğin, parmak izi sensörü çok gürültülü veri okuyup, doğrulama işlemini etkileyici sonuçlara sebep olabilir. Sonuç olarak sensörün kalitesi de başarıyı etkileyen bir faktördür.

2. TEORİK ALTYAPI

Bu bölümde tezin akademik zemine oturtulması ve okuyucuya daha anlaşılır bir bakış açısı sunmak üzere çeşitli teorik bilgiler verilecektir. Bu altyapı sağlayıcı bilgiler 3. Bölüm'de anlatılan sistem tasarımı için de temel oluşturmaktadır. Öncelikle literatür analizi sunulacak ve önceki çalışmalara ilişkin bilgiler verilecektir. Ardından biyometri ile ilgili detaylar hem parmak izi hem de yüz için anlatılacaktır. Bu bölümün ilerleyen kısımlarında, biyometri, yüz ve parmak izi biyometrisi ile çoklu biyometri, QR 2 boyutlu kodlama, Gri Seviyesi Eş-Oluşum Matrisi (GSEM), gibi mevcut var olan bilimsel kavramlar ve yöntemlerden söz edilecektir.

2.1. Kaynak Taraması

Tez çalışması kapsamında farklı tipteki biyometrik verilerin füzyonuna ilişkin örneklere bakıldığında, literatürde bazı çalışmalara rastlamak mümkündür. Farklı teknolojileri bir araya getirmek biyometrik bir sistemin doğruluk oranını yükseltir. Ross, temel olarak çoklu biyometriden bahsettiği makalesinde birden fazla biyometrik veri kullanmanın yararlarına değinmektedir [9]. Biyometrik sistem, bir biyometrik veriye ilişkin herhangi bir sıkıntı yaşadığı takdirde bir diğer biyometrik veri ile bu açığı kapatabilmektedir. Yine Ross'a göre çoklu biyometri çok yoğun veri tabanlarında indeksleme ve filtreleme gibi bazı temel veri tabanı operasyonları için de kolaylık sağlamaktadır. Sensörlerden gelen gürültülü veriler, birden fazla kez veri okuması yardımıyla maskeleme işlemi sayesinde yine çoklu biyometrinin aynı tipteki veri üzerine etkisi ile daha berrak hale getirilebilir. Ross için çok sayıda biyometrik veriyi kullanmak, güvenlik ataklarına karşı da dirençli bir sistemi sunmaktadır. *Imposter* ve *spoofing* ataklarının analizinde çoklu biyometri daha sağlıklı tespitler vermektedir. Ross için çoklu biyometrinin sınıflandırılması çeşitli temel etmenler içerir: i.) çoklu sensör, ii.) çoklu algoritma, iii.) çoklu örnek, iv.) çoklu kopya, v.) çoklu mod gibi. Hibrit kullanımlar da söz konusudur [9]. Bu tez çalışması çoklu modda biyometrik sistem sınıfına dahildir. Tezdeki çalışmaya benzer olarak hem yüz hem de parmak izinin birleştirildiği

uygulamalardan biri Telgad ve ark. tarafından skor seviyesi füzyon kullanılarak sunulmuştur. Eşleşme skorunun farklı biyometrik veriler için benzeşmesini sağlamak ve daraltmak adına normalizasyon tekniği kullanılmıştır. Böylelikle benzerlik oranları farklı tipteki biyometrik veriler için birbiri cinsinden ifade edilebilmektedir. Telgad ve ark.'nın çalışmasında görülmektedir ki çoklu mod kullanıldığında doğruluk oranı tekli moda göre artış göstermektedir. Yüz için PCA ve parmak izi için minutiae özellik noktaları ile Gabor filtresinin sonuçları füzyon yapıldığında %4 bir artış ile toplamdaki genel doğruluk yüzdesi %97.5 olmaktadır [10]. Ali ve ark. yine yüz ve parmak kullanarak sınıflandırma doğruluğunu arttırıcı bir çalışma yapmışlardır. Yüz kenar haritası, Gabor dalga boyu ve parmak izi *minutiae* özellik noktalarını kullanarak ortalama hata değeri azaltılarak sınıflandırma doğruluğu %96.45'e çıkarılmıştır [11]. Çoklu biyometri ve güvenlik konuları bir arada incelendiğinde Nandakumar and Jain her bir kullanıcı için çoklu biyometrik veri saklamanın getirebileceği problemlere değinmektedir. Özellikle biyometri gibi gizli kalması gereken bir veri söz konusu olduğunda verinin çok olmaması veri güvenliğinin sağlanabilmesi açısından daha kolay bir iştir. Ancak çoklu biyometrinin amacı gereği tekli moda göre daha fazla veri saklanacaktır. Nandakumar ve Jain tarafından bulanık tonoz şeması (*fuzzy vault scheme*) kullanılarak özellik çıkarımı seviyesinde füzyon uygulanmış olup, parmak izi ve iris verileri tek bir veri tipiymiş gibi bir uzaya indirgenmiştir. Nandakumar and Jain'in özelllik çıkarımı sırasında kullanılan bir polinom ve tonoz anahtarı yardımıyla elde ettikleri veri tek tipte olması sebebiyle güvenlik açısından daha avantajlıdır [12]. Donanım ve çoklu biyometrik kullanımı arasındaki ilişiki göz önüne alınarak literatür incelendiğinde Wang ve ark. tarafından ARM9 tabanlı gömülü bir sistem üzerinde parmak ve ses verisinin bir arada işlendiği örnek mevcuttur. Bu çalışmada ses verisi ile tekil olarak elde edilen doğrulama sonuçlarının düşük olmasına rağmen, parmak izi ile birleştirildiğinde %1.0067 gibi bir EER'ye (*Equal Error Rate*, Ortak Hata Oranı) sahip olunduğu görülmektedir. Çalışmada ayrıca SVM için farklı *kernel* kullanımı ile füzyon karşılaştırılması yapılmaktadır. *Poly, RBF* ve *Tanh kernel* için yakın sonuçlar elde edilmiştir. Wang ve ark. kullandıkları gömülü sistemin performans sonuçlarını da sunmaktadır.

Masaüstü uygulamasına göre kıyaslanan değerlere için gömülü sistem ortalama 3 kat daha yavaş çalışma zamanı harcamaktadır [13]. Çoklu biyometri kullanan e-pasaport örneklerine bakıldığında bazı ülkelerin hem güvenliği arttırıcı hem de havalimanlarındaki yoğunluğu azaltıcı yönde bazı çözümleri mevcuttur. Örneğin, İspanya Madrid'teki Barajas Havalimanı ile Barselona'daki El Prat Havalimanı Avrupa'nın en yoğun havalimanları arasında gösterilmektedir. Kullanılan yeni teknoloji ile geçiş kontrol gişelerinde çoklu biyometrik çözümler kullanılarak daha hızlı işlem zamanı elde edilmektedir. İris, parmak izi ve yüz biyometrilerini kullanan sistem farklı modülleri için 1:1 veya 1:N doğrulama yapabilmektedir [14]. Öte yandan e-pasaportların çıkışı ile birlikte bazı ülkelerde yine kişi doğrulama işlemlerinin hızını ve güvenliğini arttırıcı çözümler çoklu biyometri ile denenmeye başlanmıştır. 2004 yılında Hollanda e-pasaport haberleri henüz yayılmaya başlamışken, çoklu biyometri için 15.000 deneme pasaportunu gündemine almıştır. E-pasaport standartlarına göre zaten yüz biyometrisi kullanılacak olan yapıya bir de parmak izi eklenerek denemeler yapılmıştır [6]. Pakistan'da ise parmak izi verilerinin hem 1:N hem de 1:1 kontrolünü sağlayan aynı zamanda 1:1 yüz tanıma ile kişi doğrulaması yapan çoklu biyometri desteği bulunan pasaport mevcuttur. Pakistan bu teknolojiyi kullanan ilk ülkelerdendir [5]. Gelişen teknoloji ile birlikte bazı havalimanları akıllı sistemler kullanarak yolcuların kimlik doğrulamasını memur kullanmadan yalnızca kendi başlarına yapmalarını sağlamaktadır. Örneğin Malezya'da Kuala Lumpur Hava Limanında Malezyalı yerli halk pasaport ve parmak izlerini göstererek doğrulama başarılı ise otomatik olarak geçiş yapabilmektedirler (*AutoGate*) [15].

Tezin bir bölümünde görüntünün paralel işlenmesine yönelik *dilimle, işle, birleştir* yönteminden de söz edilecektir. Bu sebeple paralel hesaplamaya ilişkin literatür analizi de yapılmıştır. Verilerin işlenmesi yüzyıllardır süregelen bir uğraş konusu olmuştur. Günümüz teknolojilerinin gelişmesi ile birlikte artan veri miktarı ve verilerin beraberinde getirdiği işlem yükü, taşıdığı çeşitli kritik bilgilerin de varlığı ile paralel hesaplamayla performans artırımı yaklaşımını daha da önemli kılmıştır. Artan veriler, çalışma zamanı ve iş yükü açısından donanım üzerinde çeşitli problemleri beraberinde getirirken, yine gelişen teknoloji sayesinde verilerin

paralel olarak işlenmesi de mümkün olabilmektedir. Özellikle 2000'lerin başından itibaren günlük kişisel bilgisayarları etkilemeye başlayan çok çekirdekli işlemciler günlük kullanımda daha sıklıkla karşılaşılmaya başlanmış ve işlemlerin paralel olarak yapılması mümkün olmuştur. Boru hattı (*pipeline*) yaklaşımı içeren sistemlerin temel olduğu bu yeni nesil teknolojiler, çok çekirdekli bir merkezi işlem birimi veya paralel çalışan uzaktan buluta erişimli hesaplama makinaları olabilmektedir. Ayrıca, GPU teknolojisinin de sahaya girmesi ile görüntüden sorumlu birimlerin bilgisayar mimarisi hiyerarşisinde performans arttırıcı olarak rol oynaması da söz konusudur. Teknolojik gelişmeler ile birlikte artan veri miktarı, verilerin saklanması ve işlenmesi gibi iki temel konuda sıkıntıları da beraberinde getirmektedir. Yüksek başarım amacıyla paralel hesaplama, karmaşıklığı yüksek problemlerin çözümü için disiplinler arası hesaplamalardan, genetik verilerin işlenmesine kadar, hatta yer bilimleri, uzay araştırmaları gibi konuları da kapsayarak çok çeşitli uygulama alanına hitap etmektedir. Verilerin işlenmesi esnasında ortaya çıkabilecek üstel hesaplama zamanı ($2^{polinom(n)}$ vb.) algoritmanın hesaplanması açısından yük getirir. Bu durum, problemlerin yüksek başarımı için hem donanımsal olarak çok çekirdekli mimarilerin, hem de yazılımsal açıdan karmaşıklığı azaltıcı yönde önerilen -böl ve yönet, özyinelemeli algoritmalar vb.- yaklaşımların kullanılmasını gerektirir. Böylelikle paralel hesaplama sağlanarak performansı etkileyen yüksek çalışma zamanı azaltılabilir ve yüksek başarım sağlanır. Bu çalışmada uygulama alanı olarak görüntü işlemede bir resim için paralel hesaplama ve çok çekirdekli mimari kullanarak performans artırımı hedeflenmektedir. Özellikle hızın önemli olduğu erişim sistemlerinde yüz tanıma, parmak izi tanıma vb. görüntü işleme teknikleri gerektiren biyometrik uygulamalar önerilen yaklaşım için kullanılabilir. Örneğin, e-devlet uygulamalarında yüz tanıma ile sistem erişimi özelliği sağlandığında, bir ülkedeki tüm kişilerin biyometrik yüz verileri, ilgili veri tabanında saklanacak ve her bir doğrulama işlemi için hem gelen veriden özellik çıkarma, hem de ilgili veri tabanında arama yapmak için zaman harcanacaktır. O halde yüz verilerinden özellik çıkarma işlemi çok çekirdekli işlemci içinde iş yoğunluğuna göre dağıtılabilir. Ancak resmi hangi parçalara ayırmak ve nasıl dağıtım yapmak en uygun sonucu getirecektir? Bu çalışma ve daha

önceki bazı benzer çalışmalar bu soruya cevap aramaktadır. Görüntü işleme için yüksek başarım sağlamak adına paralel hesaplamanın kullanılması başka araştırmacılar tarafından da güncel olarak takip edilmektedir [16]. Literatür incelendiğinde [17] kaynağında paralel ve ayrık olarak görüntü işlemeye yönelik, konuya yeni başlayan araştırmacılar da göz önüne alınarak bazı temel bilgiler sunulmaktadır. Görüntü işleme için paralel hesaplama olarak bazı yaklaşımlardan bahseden bu çalışma i.) Veri Paralel ii.) Blok Paralel ve iii.) Boru Hattı Paralel olarak 3 tip sunmaktadır. Önerilen tez çalışması da bu sınıflandırmalardan Blok Paralel başlığı altındadır ve resmin parçalara ayrılması ile paralel hesaplanmasına yönelik bir amaç söz konusudur [18].

Grama ve diğerleri bir çalışmalarında donanım mimarileri üzerinden görüntü analizinin paralel hesaplama ile işlenmesinden bahsetmektedirler. SIMD-*Single Instruction Multiple Data* Tek Komutlu Çok Verili mimariler daha aşağı seviye hesaplamalar için kullanılırken, MIMD-*Multiple Instruction Multiple Data* Çok Komutlu Çok Verili mimariler üst seviye süreçler için kullanılır. Grama ve diğerleri paralel hesaplama adına temel sayılabilecek kitaplarında SIMD gibi teknolojilerin görüntü işleme uygulamalarında kullanılabileceğini söylemektedir [19]. Krishnakumar ve diğerleri SIMD-MIMD mimarisi tasarımı yaparak, geliştirilmiş boru hattı mimarisi ile görüntü işleme için kullanılan bir yenilik sunmaktadır. Araç kutusuna bir eklenti şeklindeki kütüphanelerle sunulan yaklaşım ile standart ardışıl sistemlere göre performans açısından 40-65% arası bir iyileşme gözlenmiştir [20] [18]. Görüntü işlemeye yönelik algoritmaların yüksek başarım amacıyla paralel bir platformda gerçeklenmesi ile ilgili bir çalışma da Kaur tarafından sunulmuştur. Görüntü iyileştirme algoritmasının Matlab ortamında analizini öngören çalışma, değişik boyuttaki veriler ile analiz sonuçları elde etmektedir. Zaman performansı ve algoritmanın verimliliği açısından tek çekirdeğe göre iyi sonuçlar elde edilen çalışmada, yüksek başarım için gerekli zaman, hız, verimlilik, verilerin kapsamı gibi değişkenler tanımlanarak sonuçlar sunulmaktadır. Görüntünün parçalara ayrılarak yük dengeleme yapılması da çalışma içinde yer alan yöntemler arasındadır [18].

Biyometrik görüntülerin işlenmesinde olduğu gibi, tıbbi görüntülerin işlenmesinde de verilerin sıkıştırılması, transferi, bazı morfolojik operatörlerin kullanımı, renk dönüşümü, rotasyon işlemleri, görüntünün devriğinin alınması vb. gibi bazı temel görüntü analizi teknikleri kullanılmaktadır. Barry ve diğerleri tarafından zaman karmaşıklığı açısından yük getiren bu operasyonlardan bazılarının analizi sunulmaktadır [21] [22]. Bizim çalışmamızda da biyometrik veriden özellik çıkarımı sırasındaki iş yükünün fazla olduğu gözlenerek belli bir kısmın paralel hale getirilmesi hedeflenmektedir. Bu sebeple de bir görüntü işleme operatörü örnek olarak seçilerek iş yükü işlemcilere dağıtılacaktır.

Literatüre bakıldığında paralel hesaplama için bazı temel algoritmalara rastlamak da mümkündür. Ercan ve diğerleri tarafından derlenen paralel programlamada kullanılan temel algoritmalara bakıldığında [23]:

•Böl ve Yönet (*Divide & Conquer*)
•Paralel İşaretçi Teknikleri
    * İşaretçi Atlama
    * Euler Tur
    * Graf Küçültmesi
    * Kulak Ayrıştırma
•Rastgeleleştirme (*Randomization*)
    * Örnekleme
    * Simetri Kırılması
    * Yük Dengeleme

ile karşılaşılmaktadır. Bunlardan Böl ve Yönet, problemi küçük parçalara ayırıp ayrı ayrı çözmek ve ardından birleştirmek (*merge*) mantığı ile çalışır ve bu çalışmamızda da başvurulan teknik olacaktır.

Bir diğer çalışmada Altıntaş ve Yegenoğlu seri ve paralel yaklaşımlarla görüntü işlemeye ait hız, performans, verimlilik gibi konulara değinmişlerdir [24]. Hız ve verim için dikkat çekilen metriğe göre;

$$Hız = \frac{Seri\ Çalışma\ Süresi}{Paralel\ Çalışma\ Süresi} \tag{2.1}$$

$$Verim = \frac{Hızlanma}{İşlemci\ Çekirdek\ Sayısı} \tag{2.2}$$

denklemleri (2.1) ve (2.2) olarak sunulmaktadır. Akgün tarafından sunulan bir diğer makalede, paralel görüntü filtreleme uygulamasına değinilmektedir. Bu çalışmamıza benzer bir yaklaşımla filtreleme işlemini görüntüyü çeşitli parçalara ayırarak yapan Akgün, piksel sayısını iş yükü olarak kabul etmiş, yük dengeleme işleminin ardından çok çekirdekli bir mimarideki analizleri sunmuştur. Bu analizde iki farklı Intel işlemci mimarisinde test yapılmış, farklı boyutlardaki görüntülerin değişik sayıdaki paralel çalışan parça üzerinde çalışma performansları sunulmuştur [25]. Pande ve diğerleri, yüz için özellik çıkarımı sırasında ve bir kenar bulma yaklaşımı olarak Robert kenar çıkarımı işleminde paralel olarak hesaplama yapmayı öngörmüşlerdir. Bir uygulama iskeleti (*framework*) olarak önerdikleri yaklaşımlarında %92 yüz tanıma başarı oranı sunulmuştur [26].

Bir diğer çalışma da yüzün algılanması ve tanımlamasının yapılması işlemlerinin paralel olarak yapılabileceğini öngörmektedir. Bhutekar ve Manjaramkar GPU kullanarak CUDA yardımı ile paralel hesaplama yöntemiyle yüz tanıma teknolojisine ait bir yaklaşım sunmaktadırlar. Çalışmada yüz algılama ve tanımlama işlemlerinin paralel olarak yürütülmesi önerilmekte ve hem GPU hem de CPU üzerinde testler sunulmaktadır [27]. Çok çekirdekli bir mimaride herhangi bir algoritmanın paralel olarak çalıştırılmasına yönelik ilk çalışmamız olan [8] ise, A* algoritmasının rota planlamaya yönelik Türkiye illeri için hesabının paralel olarak yapılması ve Matlab paralel hesaplama aracı (*Parallel Computing Toolbox*-PCT) yardımı ile analizinin sunulmasına yöneliktir. Bu çalışmamızda sonuçlar performans analizi ile birlikte verilmiştir. Bu yeni çalışmamızda ise bahsedilen literatür taraması da göz önüne alınarak, doğrulama ve sistem erişimi gibi uygulamalarda kullanılabilecek biyometrik yüz verisinin işlenmesi sırasında gerekli olan piksellerin paralel çalışan çekirdekler arasında dağıtımı anlatılacaktır.

Bu yeni çalışmaya benzer olarak ayrıca Saxena ve diğerleri tarafından sunulan tıbbi görüntülerin belirli görüntü işleme teknikleri açısından nasıl paralel hesaplama ile hızlandırılacağına ilişkin bir çalışma da mevcuttur. Tıbbi resimlerin veri miktarı çok fazla olabileceği için paralel hesaplama kullanılması, zaman performansı açısından yarar sağlayacaktır. Resimlerin paralel hesaplanması için bölmelendirilme ihtimallerine değinen bu çalışmada, işlemciye dağılımın nasıl

yapıldığı hakkında çok fazla detay bulunmasa da bizim bu yeni çalışmamızda hem çekirdek iş yükü hem de bölmelendirmeden doğan iş yükünü göz önüne alarak yük dağıtımının nasıl yapılabileceği anlatılacaktır [28].

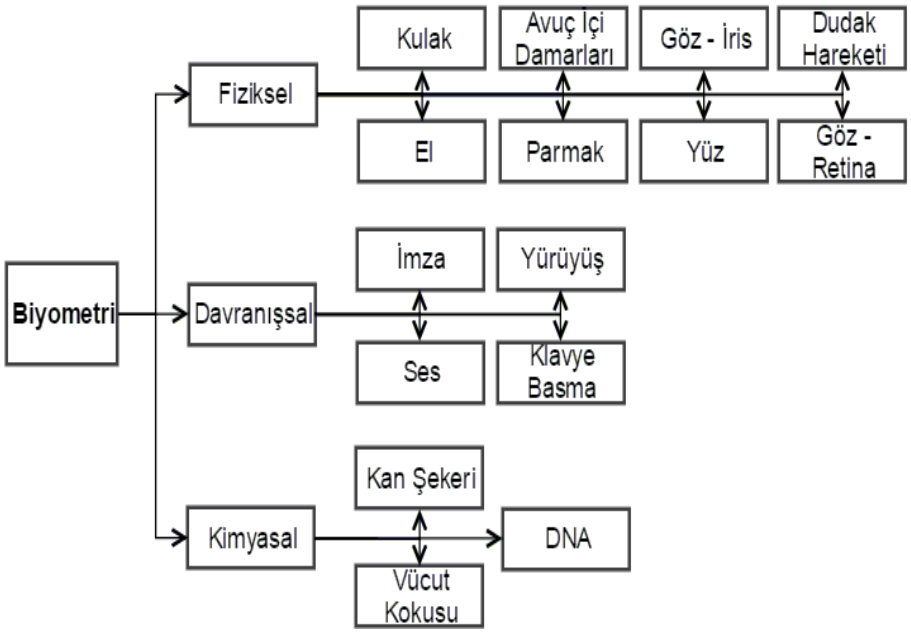
Diğer yandan güvenlik ve kare kod ile ilgili literatür taraması da yapılmıştır. QR kodun güvenlik seviyesini artırıcı bir eleman olarak kullanılmasına örnek teşkil edecek çalışmalara bakıldığında literatürde bir takım örneklerle karşılaşılmaktadır. Chen ve Wang QR kod üzerinde kullanılmayan kısımların dikkate alınarak QR kodu bazı verileri gizlemek için kullanmayı önermişlerdir [29]. Bu çalışmada, verilerin kayıplı ve kayıpsız olma durumlarına göre bir sınıflandırma söz konusudur. QR kod kendi yapısında zaten hatalara karşı dirençli olacak şekilde kodlanmıştır. Bazı durumlarda QR kodun bazı kısımları eksik olabilir ve hata toleransı ile kayıplı kısımlar veri kaybına sebep olmadan ilgili bilginin çıkarılması sağlanabilir. Chen ve Wang'a göre kullanılan QR kodlu yaklaşım ile JPEG ataklarına karşı daha dirençli bir çözüm üretilmektedir. Ayrıca %25 gibi bir oranda hata düzeltmesi söz konusu olabilen QR kod, önerilen güvenlik yaklaşımı için uygundur. Diğer yandan Zigomitros ve Patsakis, tam tersine bir yaklaşım izleyerek kodlanmış QR resmini bir diğer başka resim içine gömerek farklı bir yol sunmaktadır [30]. Zigomitros ve Patsakis'e göre verilerin sıkıştırılması gerektiğinde önerilen yöntem iyi sonuçlar vermektedir. Ayrıca bu türlü bir yöntem ile internet aramaları verinin gömülü olduğu QR'ı kontrol ederek daha hızlı hale getirilebilmektedir. Benzer bir yaklaşım da [29] kaynağında Chung ve ark. tarafından sunulmaktadır. Buna göre, kayıpsız veri gömmek için QR kod kullanılmakta ve bazı sıradan sayılabilecek QR kod bölgeleri boyut azalımı amacıyla kırpılabilmektedir [31]. Literatür analizinden QR ile ilgili çıkarılacak genel bir sonuç; bu türlü 2 boyutlu görsel kodlama kullanıldığında ilgili oluşan resmin her alanı kullanılmaz ve kayıtlar söz konusu olsa dahi kodlamanın ve maske ismi verilen bir işlem gereği veri geri kazanılabilir. Buradan hareketle bu tez çalışmasında bazı alanlar gömülen verinin yanı sıra başka bir verinin saklanması için kullanılabilir (QR'a gömülen veri biyometrik bir veri, saklanan veri de şifrelenmiş veri için bir anahtar olacaktır).

QR kodun daha genel anlamda kullanımına bakıldığında tıbbi alanda da çeşitli uygulamalarına rastlamak mümkündür. Yenilikçi bir fikir ile QR içine gizli tıbbi verileri gömen Chang ve ark. hastane ortamında 2 boyutlu barkod kullanımını medikal çevreye kazandırmıştır [32]. Maheswari ve Hemanth ise çalışmalarında Fresnelet dönüşümü ile steganografinin en düşük anlamlı bit (*Least Significant Bit LSB*) uygulamasına kare kod üzerinden bir örnek sunmaktadır [33]. Ramesh ve ark. ise literatürde genel olarak kare kod uygulamalarında karşımıza çıkacağı üzere metin verisini QR içine gömerek ayrık dalga boyu dönüşümü (*Discrete Wavelet Transform – DWT*) yöntemi ile kodlama ve kod çözme işlemlerini frekans uzayında yapmaktadır [34]. Bu tez çalışmasında da tıpkı genel eğilime benzer bir şekilde QR içine veri gömülecektir ancak bu veri metin değil de biyometrik şablonu içerdiğinden yeni bir yaklaşım sunularak QR kodun daha güvenli hale getirilmesi sağlanacaktır.

2.2. Biyometrinin Temelleri

Tez kapsamında planlanan çoklu biyometrik verilere ilişkin güvenli hale getirme hedefi beraberinde biyometrik verilerle çalışmayı ve bu verileri doğru biçimde kullanmayı da getirmiştir. Peki, biyometrik veri nedir? Çeşitleri nelerdir? Bu verilerin kullanılmasının avantajları, dezavantajları nelerdir? Bu bölümde, temel olarak biyometriden bahsedilecektir. Özellikle yüz tanıma sistemlerinin taşınabilir cihazlarda dahi kullanılabilir hale gelmesi biyometrik verilerin kullanım alanının hangi boyutlara ulaştığını göstermektedir. Biyometrik veriler çok çeşitlidir ve farklı farklı biyolojik ve davranışsal özellikler ayırt edici olarak kullanılabilmektedir.

Bir veri çeşidinin biyometrik veri olarak nitelendirilebilmesi için öncelikle belli bazı özellikleri taşıması gereklidir. Bunlar, i.) Kişiye özel ayırt edici özellikler olması ii.) Yıllar içinde değişken özellikte olmaması olarak sıralanmaktadır. Ayrıca ölçülebilirlik gibi bir özelliğe de sahip olması gereklidir. Ölçülen verilerin sayısal olarak bilgisayar ortamında işlenmesi gerekecektir. Biyometrik verilerin temel olarak sınıflandırıldığı yapı Şekil 2.1'de gösterilmektedir.



Şekil 2.1. Biyometrik verilerin çeşitliliği [35]

Biyometri (Biometrics) köken olarak antik Yunanca "*bios*" yani yaşam ve "*metron*" hesaplama kelimelerinin birleşiminden oluşmaktadır [36]. Doğuştan gelen kişiye özel bu eşsiz özellikler artık günümüzde pek çok mühendislik uygulamasında güvenlik, sınıflandırma, doğrulama, tanımlama gibi amaçlarla ve adli vakalarda kullanılmaktadır. Biyometrik metotların çeşitlerine bakıldığında, bunları 3 ana sınıfta toplamak mümkündür: fiziksel, davranışsal ve kimyasal [35]. Uygulamaya yönelik biyometrik özelliklerin kullanılması durumunda, Şekil 2.1'deki şemadan faydalanarak tasarımı gerçekleştirmek, ortaya konan tasarımın uygulanabilirliği açısından önemlidir. Genel olarak doğrulama sistemlerine bakıldığında ise

i.) Kart vb. gibi aksesuar tabanlı olan

ii.) Biyometrik tabanlı olanlar

iii.) Görüntü veya yazı içerip, bilgi tabanlı olan

sistemlerle karşılaşılmaktadır.

2.2.1 Biyometrik sistemlere ilişkin performans metriği

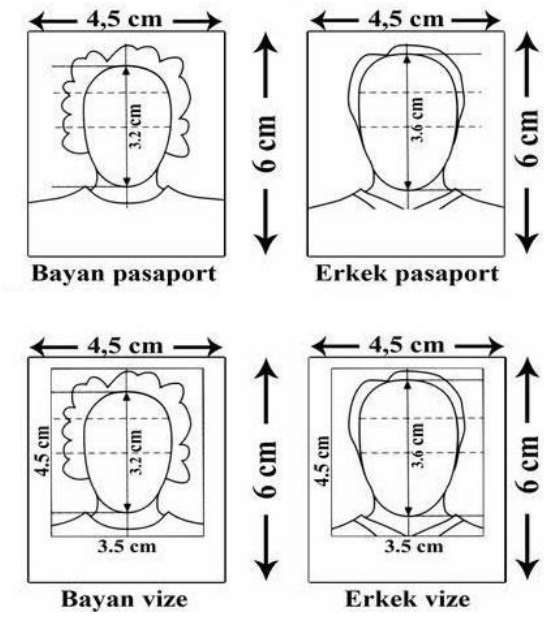
Biyometrinin önemli Profesörlerden biri olan Anil K. Jain'in ve ark. kitabında da yer verdiği çeşitli bilgiler bu bölümde derlenmiştir. Biyometrik sistemler esasen bir erişim sisteminin parçasıdır ve kişilerin biyolojik verilerini kullanarak erişim sağlamalarına olanak tanır. Öncelikle 2 tip erişim yönteminden söz etmek mümkündür: i.) Doğrulama (*Verification*) ii.) Tanımlama (*Identification*). *Doğrulama*, pasaport sistemlerine daha uygun olarak kişinin kim olduğunun iddiası ile sisteme "Bu kişi Ali midir?" şeklinde bir soru sorarak ilgili kişinin eşsiz kimlik numarası yardımıyla saklı olan verisine ulaşılıp karşılaştırılması durumudur. Daha hızlı sonuçlar elde edileceği açıktır. Öte yandan *Tanımlama* kişinin biyometrik bilgisinin varlığında kim olduğuna dair bir fikir/iddia olmadan veri tabanı üzerinden tanımlama yapmaktır. Daha çok adli (*forensics*) uygulamalarında kullanılan bu yöntemin tüm veri tabanını taraması gerekebileceği için performans zamanı daha fazladır. Doğrulama veya tanımlamanın ışığında bu tez çalışmasının çalışma performansı sınıflandırma başarısına göre incelenecektir. Bu sebeple verilerin doğru veya yanlış sınıflanmasına bağlı olarak *False Non-Match Rate (FNMR)* ve *False Match Rate (FMR)* gibi iki temel kavramdan söz etmek gerekir. FNMR yüzdesel olarak aynı kullanıcıdan alınan biyometrik verilerin hatalı olarak non-match yani "eşlenmedi" olarak karar verilmesinden elde edilen bir sonuçtur. Örneğin 100 denemeden 2'si uyuşmamış olarak işaretlenmiş ise %2 olarak belirlenir. FNMR hataları genel olarak sensör kaynaklı sorunlardan ileri gelir ve kişiye ait biyometrik verinin yeniden alınması ile çözülebilir. FMR ise olasılıksal olarak eşleşmemesi gereken iki biyometrik bilginin aynı kullanıcıya aitmiş gibi hatalı olarak eşlenmesi denilebilir. Biyometrik doğrulama sistemlerinde FNMR ve FMR genellikle *False Reject Rate (FRR)* ve *False Accept Rate (FAR)* olarak anılırlar.

Match Score yani Eşleşme Oranı, *Genuine* veya *Authentic* Score olarak isimlendirilir ve iki eş arasındaki benzerliği gösterir. Öte yandan, *Imposter Score* yani Sahtelik Oranı ise eş olmayan iki veri arasındaki benzerliği tanımlar. Benzerlik Skoru s olmak üzere sisteme ilişkin biyometrik doğrulama işlemleri η eşik değeri

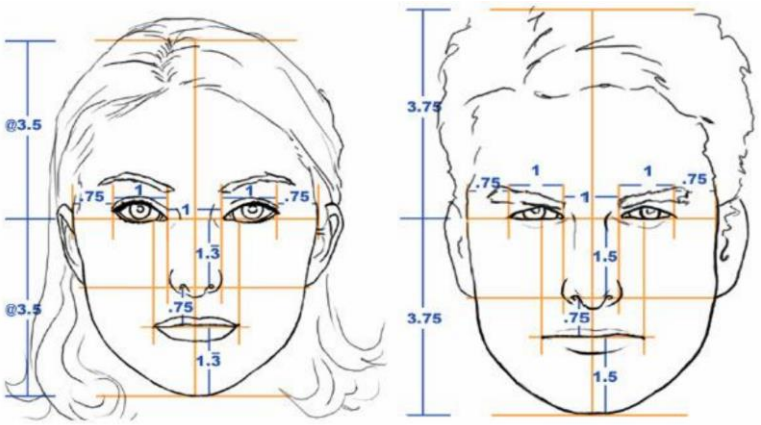
üzerinden yorumlanır. Bu sebeple FRR ve FAR oranları hesaplanırken bu değerler kullanılır [37].

2.3. Yüz Biyometrisi

Yüz resminden elde edilen veri de kişiye özel bir veridir ve son yıllarda pek çok uygulama alanında karşımıza çıkmaktadır. Çeşitli oranlara sahip ve bazı standartlarda olan yüz biyometrisi özellikle pasaport uygulamalarında son derece yaygın olarak kullanılmaktadır. Yakın gelecekte kimlik kartlarında da parmak izi biyometrisi ile bir araya gelerek yer alacağı düşünülmektedir. Şekil 2.2 ve 2.3'de yüz biyometrisine ilişkin detaylar gösterilmektedir. Bayan ve erkeğe ait oranlar farklıdır. Şekil 2.2'de biyometrik pasaport için kullanılan şablonda yüz, göz, çene, kafanın konumu ve büyüklüğü gibi detaylar mevcuttur. Yani bu resimleri kullanarak geliştirilen uygulamada yüzün nerede olduğunu bulmak için ayrıca algoritma geliştirmeye gerek yoktur. Arka plan ve ışık da 1. Bölümde örneklendiği üzere zaten görüntü işleme açısından kolaylık sağlayıcıdır.



Şekil 2.2. Biyometrik bir resim elde edilirken kullanılan şablon örneği [38]



Şekil 2.3. Yüze ilişkin çeşitli oranlar [39]

Şekil 2.3'de gösterildiği gibi yüze ait çeşitli oranlar söz konusudur. Bu oranlar özellikle pasaport biyometrisi resimleri gibi sabit bir şablon kullanan uygulamalar için oldukça önemlidir. Çünkü yüze ait herhangi bir nokta bulunduktan sonra -örneğin Haar filtreleri ile gözün tespiti- yalnızca bu oranlarla yüze ait diğer önemli noktalara ulaşmak mümkündür. Denklem (2.3), (2.4), (2.5), (2.6), (2.7), (2.8) ile yüze ilişkin bazı oranlar sunulmaktadır [39].

$$\frac{Yüz\ Boyu}{Yüz\ Genişliği} \tag{2.3}$$

$$\frac{Dudak - Kaşların\ Birleşim\ Yeri\ Arası}{Burun\ Boyu} \tag{2.4}$$

$$\frac{Yüz\ Boyu}{Çene\ Ucu - Kaşların\ Birleşim\ Yeri\ Arası} \tag{2.5}$$

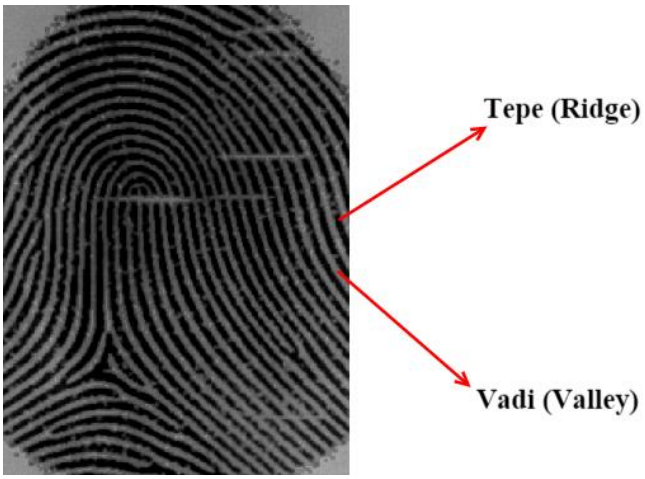
$$\frac{Ağız\ Boyu}{Burun\ Genişliği} \tag{2.6}$$

$$\frac{Burun\ Genişliği}{Burun\ Delikleri\ Arası} \tag{2.7}$$

$$\frac{Göz\ Bebekleri\ Arası}{Kaşlar\ Arası} \tag{2.8}$$

2.4. Parmak İzi Biyometrisi

Parmak izi kişiye özgü olan ve adli uygulamalarda kullanılan çok önemli bir biyometrik veridir. Tek yumurta ikizleri de dâhil olmak üzere dünya üzerinde herhangi iki kişinin parmak izi şekilleri birebir aynı olamaz. Bu tez çalışmasında ikinci bir biyometrik veri olarak da parmak izi biyometrisi kullanılacaktır. Parmak izi gelişimi insan yavrusunun anne karnındaki 10. haftasından sonraki izleyen haftalarda oluşmaya başlar. İnsan vücudunda bulunan ter atımını sağlayan gözenekler aslında parmak izinin bir parçası olan tepe (*ridge*) noktalarının şekillenmesinde etkilidir. Parmak bir yüzeye dokunduğunda çıkan izler bu tümsek noktalardır. İçte kalan boşluklar ise vadi (*valley*) olarak isimlendirilmektedir. İlgili görsel örnek Şekil 2.4'de sunulmaktadır.



Şekil 2.4. Parmak izindeki tepe ve vadi çizgileri

Çoklu biyometri hedefinin diğer elemanını oluşturan parmak izi özellik çıkarımı için temel olarak 3 seviye kullanılmaktadır. Seviye 1, 2 ve 3 (*Level 1, Level 2, Level 3*) olarak isimlendirilen bu yaklaşımlar kullanılan sensör çözünürlüğünden elde edilen özellik noktası tipine kadar çeşitli parametrelerle birbirlerinden ayrılmaktadır. Seviye 1 parmak izine ait tepe yönlerini ve frekans haritasını bulur. Böylece parmak izinin orta noktasını bulmak mümkündür. Seviye 2 ise tepe ucu noktalarını ve çatal noktalarını bulmaktadır. Seviye 3 sensöre daha bağımlı bir yaklaşım olarak en az 500 .ppi çözünürlüğe sahip cihaz gerektirir. Seviye 3 çok

daha detaylı olarak görüntüyü inceler; tepe noktalarının çevresini ve *pore* adı verilen tepe noktalarının esas oluşum sebebi ter atım gözeneklerini inceler.

Bu tez çalışmasında seviye 2 ile çalışılmıştır. Seviye 2 için özellikler çıkarılırken üç temel değişken kullanılmaktadır:

1.) Özellik tipi (uç noktası veya çatal)

2.) Özelliğin ilgili verinin (resmin) üzerindeki xy-koordinatı (x,y)

3.) Açı

Her bir özellik noktası için bu üç parametrenin hesaplanması ve saklanması gerekmektedir. Özellik çıkarımı adı verilen bu işlem biyometrik veriden anlamlı bilginin çıkarılmasına yarar ve sınıflandırma için kullanılır.

Parmak izinin alınmasına ilişkin olarak kullanılan çeşitli tipte sensörler mevcuttur. Bunlar kullanılan donanımsal özelliğe bağlı olarak:

-Kapasitif sensörler

-Optik sensörler

-Termal sensörler

-Basınca göre çalışan sensörler

-RF sensörler

-Ultrasonik sensörler

olabilir.

Kullanılan sensör tipi ve kalitesi sensör üzerinde kullanıcı davranışı ile birlikte oluşan görüntünün kalitesini belirleyecektir. Olası kullanıcı davranışları; sensöre gereğinden çok veya az basınç uygulamak, görüntü elde edildiği sırada parmağı kaydırmak, parmağı sensöre çok az alanı kaplayacak şekilde göstermek olarak sayılabilir. Ortam ışığına ve parmağın kuruluğuna göre de resmin kalitesi

değişmektedir. Tüm bu değişkenler doğrulama oranlarını olumsuz etkilemektedir. Literatürde parmak izi elde etmenin zorluğundan dolayı sentetik parmak izi üretici kullanılmaktadır ve sayılan olumsuz koşullar gerçeğe yakın olarak modellenebilmektedir [40]. Bu değişkenlere bağlı ortaya çıkan gürültü ve diğer problemler, önişlemler ile en aza indirilebilir. Bir sonraki alt bölümde bu işlemler ele alınmıştır.

2.4.2. Örnek bir görüntü üzerinde özellik çıkarımı önişlemleri

Bu kısımda özellik çıkarımına ön hazırlıktan bahsedilecektir. Görüntü işlemede kullanılan bazı temel filtreler ve morfolojik operatörler ile gürültü giderme ve görüntü iyileştirme yapılabilmektedir.

Şekil 2.5. SFinGe sentetik parmak izi üreteci ile üretilmiş parmak izi verisi [40]

Şekil 2.5'de örnek bir parmak izi görüntüsü sunulmaktadır. Kullanılan sentetik veri üretme programı yardımı ile görüntüye bir miktar gürültü eklenmiş, kullanıcının uyguladığı basınç ve parmak kuruluğu gibi parametreler de ayarlanmıştır. Bu görüntünün özellik çıkarımı fazına gitmeden önce uygulanan Wiener Filtresi, açınım, genleşme ve erozyon operatörleri, eşikleme ve ikilileştirme ile inceltme operasyonlarının sonuçları Şekil 2.6 – 2.9 arasında gösterilmektedir.

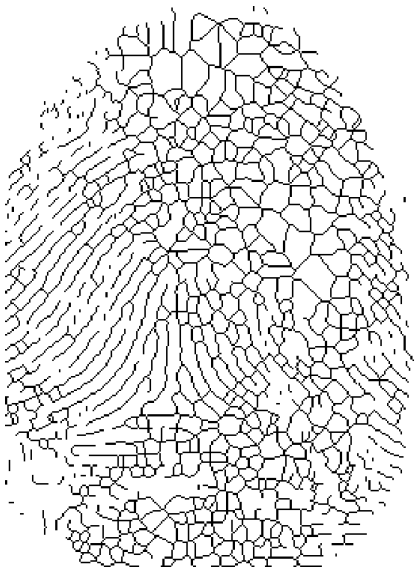
(a) (b)

Şekil 2.6. Esas görüntü (a) ve Wiener Filtresi uygulanmış görüntü (b)

(a) (b) (c)

Şekil 2.7. Açınım (a), Genleşme (b), Erozyon (c) morfolojik operatörlerinden geçirilen resim

Şekil 2.8. Eşikleme (*Thresholding*) ve İkilileştirme (*Binarization*) işlemlerinden sonra parmak izi

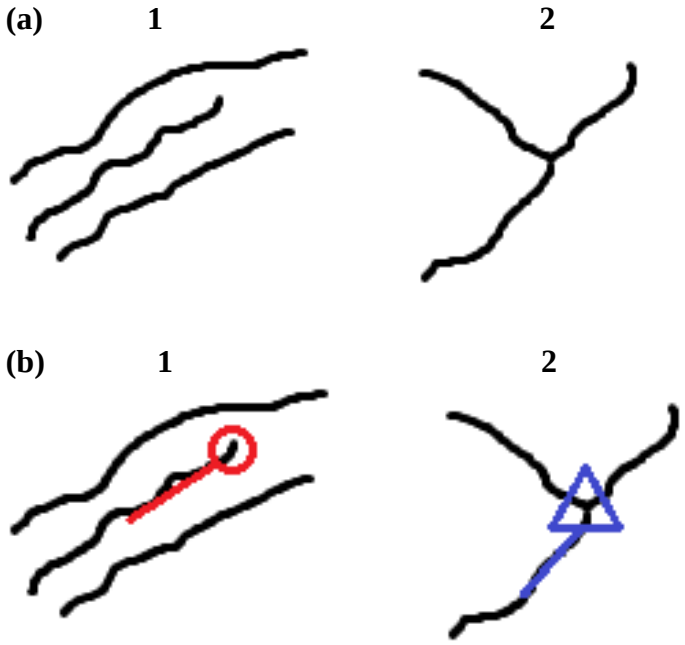


Şekil 2.9. İnceltilmiş (*Thinned*) görüntü (1'er piksel boyutunda)

Şekil 2.9'da ilk parmak izi görüntüsünün gürültülü olmasından ileri gelen sağ üst bölgedeki fazla çatal noktaları gösterilmektedir. Bu durum gürültünün ve eşiklemede seçilen değerin etkisini göstermektedir.

2.4.1. Uç ve çatal noktalarını kullanarak özellik çıkarımı

Seviye 2 kapsamında kullanılan tepe noktalarının bittiği uç noktalar ve "Y" harfine benzer çatal noktalar bu tez çalışması kapsamında elde edilmiştir. Şekil 2.10'da özellik çıkarımından önce ve sonraki parmak izi özellikleri gösterilmiştir. Sonraki 3. Bölümde önerilecek olan yöntemde kullanılacak olan bu özelliklerden esasen açıya ihtiyaç yoktur ancak yine de gelecek çalışmalarda kullanılmak üzere bulunmuştur.



Şekil 2.10. Özellik noktalarının ve açılarının bulunması; 1 ve 2 ile gösterilenler sırasıyla uç nokta ve çatal nokta, (a) özellik bulunmadan önce (b) özellik bulunduktan sonra

Şekil 2.10'da gösterilen parmak izi seviye 2 için önem arz eden özellikleri göstermektedir. Bu özel noktalar, özellik çıkarımı (*feature extraction*) sırasında kullanılacak olup, biyometrik özellik gereği her kişi de farklı bir dağılım gösterecektir. Özellik çıkarımı, 3x3 boyutunda bir operatör ile sağlanmaktadır. Merkez piksel (i,j) koordinatında – i satır ve j sütun – olmak üzere, (i-1,j-1) sol üst, (i-1, j) orta üst, (i-1, j+1) sağ üst, (i, j+1) sağ, (i+1, j+1) sağ alt, (i+1, j) orta alt, (i+1, j-1) sol alt, ve (i, j-1) sol piksel olmak üzere operatör yapısı Şekil 2.11'de görülmektedir. Filtreye benzeyen bir yapı ile tüm resim (kenarlar hariç) taranacak ve özellik çıkarımındaki anlamlı noktaların koordinatları elde edilecektir.

i-1 , j-1	i-1 , j	i -1 , j+1
i , j-1	i , j	i , j+1
i+1 , j-1	i+1 , j	i+1 , j+1

Şekil 2.11. Özellik çıkarımı için piksellerin xy-koordinat düzleminde konumu (bir çeşit operatör)

(a)

1	0	0
0	1	0
0	0	0

(b)

0	1	0
0	1	0
0	0	0

(c)

0	0	1
0	1	0
0	0	0

(d)

0	0	0
0	1	1
0	0	0

(e)

0	0	0
0	1	0
0	0	1

(f)

0	0	0
0	1	0
0	1	0

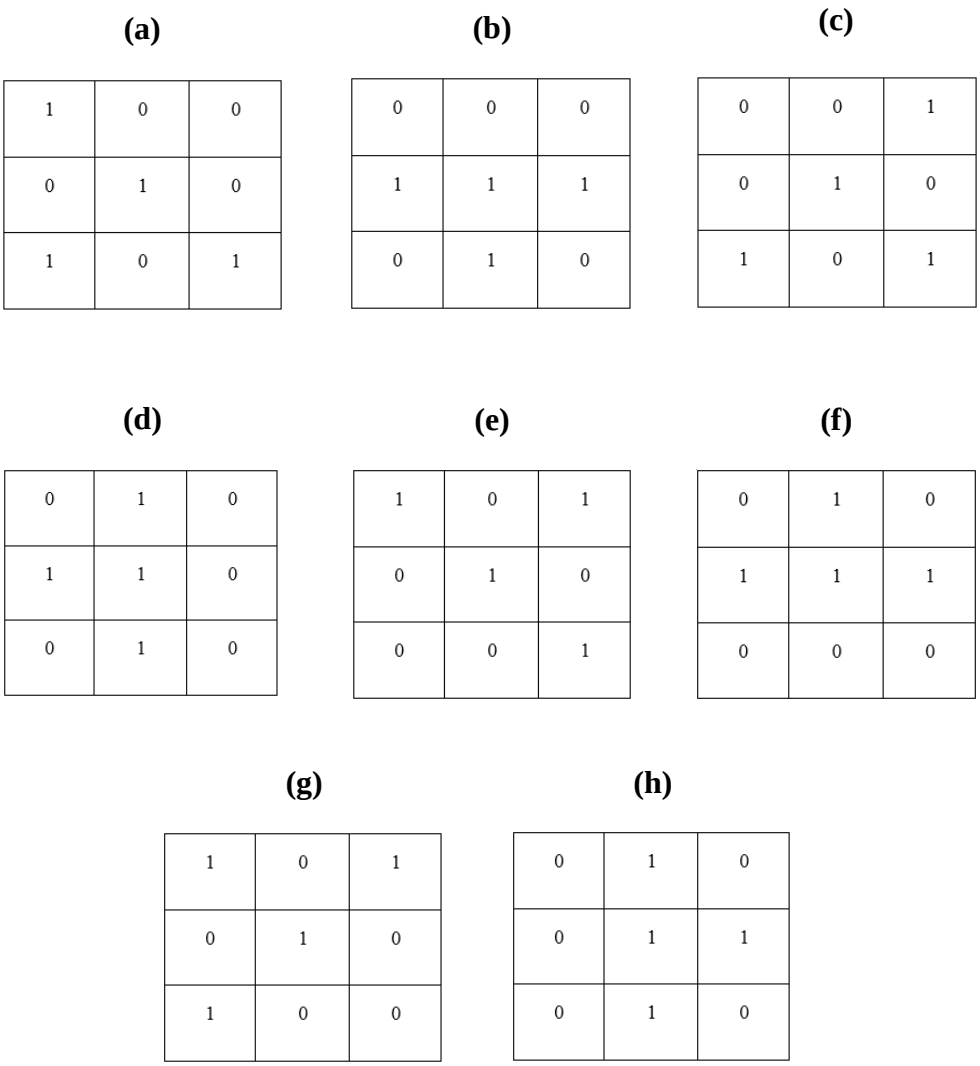
(g)

0	0	0
0	1	0
1	0	0

(h)

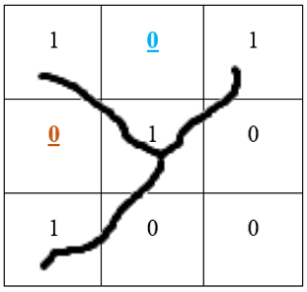
0	0	0
1	1	0
0	0	0

Şekil 2.12. Uç noktası için muhtemel olasılıklar ve filtre benzeri yapının durumları



Şekil 2.13. Çatal noktası için muhtemel olasılıklar ve filtre benzeri yapının durumları

Şekil 2.12'de ve Şekil 2.13'de sırasıyla olası uç noktaların ve çatal noktaların durumları verilmektedir. Oluşturulan algoritma her bir özellik için 8 durumu da göz önüne alarak herhangi bir uç noktası veya çatal noktası olup olmadığını kontrol edecektir. Burada 1 ile gösterilen veri devam eden tepe çizgisi (*ridge*) olduğunu 0 ise bir vadi (*valley*) varlığını göstermektedir. Bu ikili bit değerleri ön işlemlerde anlatılan eşikleme ardından uygulanan ikilileştirme işleminden gelmektedir. İnceltilmiş 1'er piksel boyutundaki yapı ile de devam eden tepe çizgileri komşu olan 1 ikili değeri ile gösterilmektedir. Şekil 2.14'de gösterilen örnek bir çatal noktası bulunmaktadır.

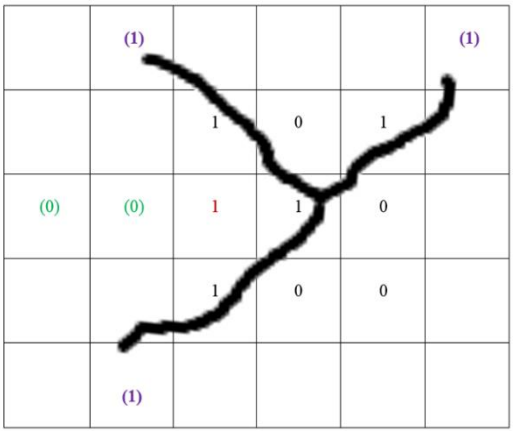


Şekil 2.14. Örnek bir çatal noktası

Ancak 3x3 boyutunda örüntü eşleştirici operatör kullanmak bazı sıkıntılar yaratabilir. Şekil 2.15'da kırmızı ile gösterilen 1 değerinin varlığı sebebiyle örüntü eşleşmez ve bu nokta esasında bir çatal noktası olmasına rağmen listeye alınmaz.

	i-2 , j-2 (1)	i-2 , j-1	i-2 , j	i-2 ,j+1	i-2 , j+2 (1)
	i-1 , j-2	1	0	1	i-1 , j+2
i , j-3 (0)	i , j-2 (0)	1	1	0	i , j+2
	i+1 , j-2	1	0	0	i+1 , j+2
	i+2 , j-2 (1)	i+2 , j-1	i+2 , j	i+2 , j+1	i+2 , j+2

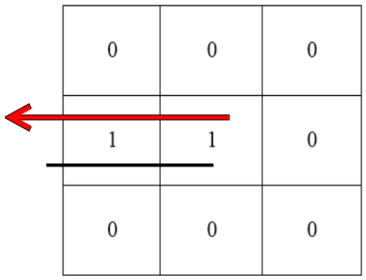
Şekil 2.15. Genişletilmiş filtre ile çatal noktası analizi



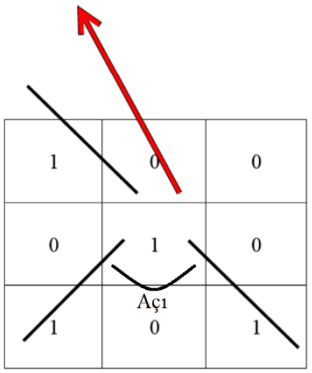
Şekil 2.16. Genişletilmiş filtre ile çatal noktası analizi örneği

Şekil 2.15'de mor ile gösterilen (i-2, j-2), (i-2, j+2), (i+2, j-2), mor renkli değerlerinin 1 olması ve (i, j-2), (i, j-3) yeşil renkli değerlerinin de 0 olması durumunda daha geniş çerçevede bakıldığında mevcut çatal yakalanabilir. Görsel olarak çatalın varlığı Şekil 2.16'da gösterilmektedir. Bu sebeple 5x5 boyutunda genişletilmiş bir filtre ile de özellik çıkarımı bu tez kapsamında yapılmıştır.

Literatürde, özellik çıkarımı sırasında ilgili özelliğin koordinatı yanı sıra açısı da önemlidir. Bu 3 veri (x-eksenindeki koordinatı, y-eksenindeki koordinatı ve açı) Seviye-2 kapsamında elde edilen özelliklerdir. Şekil 2.17'de örnek olarak bir uç noktaya ilişkin açının hesabı gösterilmektedir. Çeşitli açı ihtimalleri mevcuttur. Bunlar Şekil 2.12'de gösterilen durumlara da bağlı olarak: 0, π/4, π/2, 3π/4, π, 5π/4, 3π/2, 7π/4 olarak 45'er derecelik fark ile sıralanabilir. Aynı biçimde açı hesabı Şekil 2.18'deki gibi çatal noktaları için de yapılmaktadır. Çatal noktasına ait 3 adet birbiri ile kesişerek birleşen çizginin birbirleri arasında kalan açılardan en az değere sahip olanı alınarak açı kaydedilir.

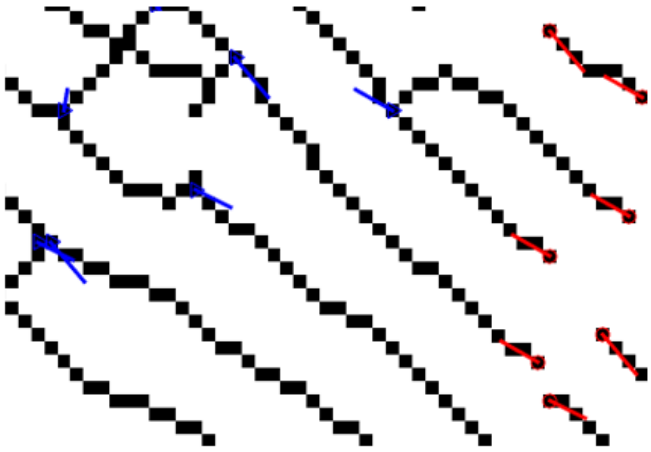


Şekil 2.17. Uç noktası için örnek açı hesabı, π



Şekil 2.18. Çatal noktası için örnek açı hesabı, π/2

Şekil 2.19'da, tasarlanan özellik çıkarma algoritması uygulandıktan sonra elde edilen parmak izi özelliklerine ait bir kesit sonuç olarak sunulmuştur. Burada mavi üçgenler çatal, kırmızı daireler ise uç noktalardır.



Şekil 2.19. Algoritma uygulandıktan sonra uç (kırmızı) ve çatal (mavi) noktaları gösteren bir kesit

2.5. Çoklu Biyometri

Önceki iki kısımda anlatılan yüz ve parmak izi biyometrisine ilişkin detaylar sistem düzeyi tasarım için çoklu biyometri yaklaşımı gereği bir araya getirilebilir. Çoklu biyometri 2 veya daha fazla biyometrik verinin kullanımı ile her bir biyometrik verinin avantajını ayrı ayrı kullanarak performans sağlayan bir yaklaşımdır. Biyometrik sistemlerde pek çok sorunun çözümü çoklu biyometri ile sağlanır. Biyometrik verisini kaybeden kişiler (sonradan veya doğuştan gelen sağlık sorunları) ikinci biyometrik veriyi kullanabilir, çift yumurta ikizlerinde eşik değerine bağlı olarak yüksek benzerlikten meydana gelebilecek sorunlar yine çoklu biyometri ile çözülebilir. Birden çok biyometrik veri kullanıldığında artan veri miktarı ve buna bağlı olarak güvenlik tehditleri söz konusudur. Daha da önemlisi farklı tipteki verileri anlamlı bir şekilde birleştirmek ayrı bir problemdir.

Biyometrik verileri birleştirmek için çeşitli füzyon yöntemleri önerilmiştir. Bunlar uygulamaya bağlı olarak değişebilir. Bir sonraki alt bölümde çoklu biyometriye ilişkin füzyon yöntemlerinden söz edilecektir.

2.5.1. Çoklu biyometri için füzyon yöntemleri

Son yıllarda biyometride yapılan çalışmalar tek bir biyometrik verinin kullanımından başka çoklu modda farklı verileri bir araya toplayarak daha güvenli sistemler kurmayı amaçlamaktadır. Ancak birden fazla verinin bir araya getirilmesi nasıl yapılacaktır? Bunun için çeşitli yöntemler söz konusudur. Temel olarak 4 farklı yaklaşımdan söz etmek mümkündür:

i.) Sensör seviyesi füzyon
ii.) Özellik seviyesi füzyon
iii.) Skor seviyesi füzyon
iv.) Karar seviyesi füzyon

Bu birleştirme tekniklerinden ilki sensör seviyesinde genel olarak veri kayıplarını azaltmak için aynı biyometrik veri tipine ancak birden çok defa veri almak koşuluyla müdahale eden bir yöntemdir. Örneğin, parmak izi sensöründe parmağın eksik kalan kısımlarını ikinci defa veri okumayı talep ederek tamamlayabilmek gibi. Diğer birleştirme yöntemi olan özellik seviyesi füzyon, özellik çıkarımı sırasında birden fazla çeşit verinin bir araya getirilmesi için kullanılır. Birleştirilen veriler tek olarak sınıflandırma/karar modülüne giderler. Bu seviyede birleştirme yaparken esas sıkıntı gelen verilerin farklı tipte olmasıdır. Örneğin, parmak izi için gelen özellikler seviye 2 için koordinat bilgisi ve ilgili özelliğin açı değeri iken, yüz biyometrisi için gelen değer, başka uzayda elde edilmiş yüz verisine ilişkin bir vektör olabilir. Bu iki farklı verinin bir araya getirilmesi Denklem (2.9)'daki gibi bir normalizasyon ile sağlanabilmektedir:

$$\hat{x} = \frac{x - \min(h_x)}{\max(h_x) - \min(h_x)} \tag{2.9}$$

x gelen verinin değeri, ve $\max(h_x)\ ile \min(h_x)$ gelen veriler arasındaki en büyük ve en küçük değerlerdir. Gelen veriler homojen olduğunda aritmetik ortalama almak da bir diğer yöntemdir. Her gelen farklı tipteki biyometrik veri için elde edilen $\hat{x}$ değerleri ardından birbirine bağlama (*concatenation*) işlemine tabi olur. Birleştirilen tüm veriler arasından bir aralık seçilerek sınıflandırma/karar modülüne

gönderilir. Üçüncü sınıflandırma yöntemi olan skor seviyesi birleştirme ise yapay sinir ağları, genetik algoritmalar, karar ağacı, Bayes teorisi gibi yaklaşımlar ile sensörden gelen farklı skorları birleştirir. Bu tez çalışmasında kullanılacak olan karar seviyesi birleştirme gelen verileri lojik AND, OR veya oylama yöntemine tabi tutarak iki veya daha çok farklı biyometrik veriden bir sonuç elde eder. Adından anlaşılacağı gibi biyometrik bir sistemin karar aşamasında rol oynar. Bunlardan başka ayrıca sıra seviyesi füzyonu (*rank level fusion*) da mevcuttur [37].

2.6. Kare Kod, (*Quick Response-QR*) 2 Boyutlu Kodlama

Bir resmin yalnızca siyah ve beyaz renk bilgisi kullanarak 2 boyutlu kare şeklinde bir fiziksel yapıda veri sakladığı kodlar Hızlı Cevap (*Quick Response*) kod, diğer adıyla kare kod olarak isimlendirilir. Alışveriş yaparken ürünlerin üzerinde barkod gibi bir görsel malzemenin içine bazı bilgiler kodlanır. Bu bilgiler ile kasada ödeme sırasında fiyat ve ürün detayları edinilir. Tek boyutlu bu barkod yapısı ilgili her bir çubuğun kalınlığına göre bilgi taşır ve lazer bir okuyucu ile okunur. QR kodda ise 2 boyut söz konusudur. QR kod Japon şirketi Denso Wave tarafından icat edilmiş çoğunlukla siyah ve beyaz renklerden oluşan görsel bir veri kodlama öğesidir. Çoğunluk siyah beyaz denilmesinin sebebi, QR kodun kullanılmayan bazı kısımlarına başka görsel öğeler, logolar konulabilir. Şekil 2.20'de buna bir örnek verilmiştir.

Şekil 2.20. İçine "Anadolu Üniversitesi" metin bilgisi gömülmüş örnek bir kare kod

Bu tez çalışmasında verilerin gömülerek saklanacağı bir görüntü ortamı sağlanacaktır. Bu taşıyıcı görüntü kare kod olduğu içine hem veri gömebilmek, hem de kullanılmayan QR alanları için veri saklamak mümkündür. Kare kod içine internet sitesi linki, metin, sayı, Kanji karakterleri gibi veri tipleri gömülebilir. 40 farklı seviye tipi bulunan QR kod, kodlayabildiği veri miktarına ve dolayısı ile kare kod resmi boyutuna bağlı olarak sınıflandırılmaktadır. Seviye 1 en düşük hafızaya, seviye 40 ise en geniş hafızaya ancak en büyük çözünürlüğe sahip kare kod tipidir. QR kod resminden bazı kısımlar kaybolsa bile hata düzeltme algoritması sayesinde çeşitli yüzdelerde geri kazanım mümkündür. L, M, Q, H olarak isimlendirilen hata düzeltme seviyeleri sırasıyla %7 ,%15, %25, %30 oranında hata düzeltmesi sağlamaktadır. Yüksek hata düzeltme oranı daha az veri kapasitesi demektir. Bu sebeple en fazla veri gömülebilecek seviye 40 tipindeki QR için L seviyesi hata düzeltmesi ile en fazla 2953 bayt veri gömülebilmektedir [41] [42].

2.7. Gri Seviye Eş-Oluşum Matrisi

Gri Seviye Eş-Oluşum Matrisi GSEM (*Gray Level Co-Occurrence Matrix*) istatistiksel bir analiz yöntemi olarak görüntüdeki tekrar eden doku özelliklerini analiz eder. İlk kez Haralik ve ark. tarafından bir görüntünün istatistiksel bilgileri kullanarak dokusal özelliklerini tespit etmek için analizi ile ortaya çıkarılmıştır. N_x x N_y boyutunda bir I matrisi ile temsil edilen bir görüntü olsun. $L_x = \{1,2,..N_x\}$ sütunlar, $L_y = \{1,2,..N_y\}$ satırlar ve her bir elemanın üyesi olduğu $G = \{1,2..N_g\}$ ölçeklendirilmiş gri seviyesi değerleri taşıyan küme olmak üzere I görüntüsü bir fonksiyona bağlı olarak temsil edilebilir. Buna göre $I: L_x \times L_y \rightarrow G$ fonksiyonu her bir L_x x L_y çifti için tanımlanabilir. Buna göre yön ve uzaklık bilgisi ile komşular arası ilişkinin birbirini nasıl takip ettiğinin dağılımı bir fonksiyon olabilir. Gri seviye eş-oluşum matrisi N_g x N_g kare matris olmak üzere I görüntü bilgisindeki komşuların komşu piksellerin tekrarlarının frekans bilgisini içerir. GSEM'deki her bir eleman $p(i,j,d,\Theta)$ ile tanımlanır. Burada i bir piksel değeri olarak, p pikselinin (x,y), konumundaki gri seviyesi değeridir ve j ise p'den d uzaklığında bulunan komşu pikselin gri seviyesi değeridir. Θ değeri iki komşu

piksel arasındaki açı bilgisidir ve bu sebeple p pikselinden komşu piksellere olan yön bilgisini verir. Görüntüye ilişkin kontrast (karşıtlık), homojenlik, enerji, korelasyon gibi özellikler GSEM bilgisinden elde edilebilir. Sınıflandırma için direkt olarak GSEM de kullanılabilir. Gri seviye eş-oluşum matrisi kullanılarak 14 değişik özellik elde etmek mümkündür. Bazıları Çizelge 2.1'de verilmiştir [43] [44] [45] .

Çizelge 2.1. Gri seviye eş-oluşum matrisi kullanılarak elde edilebilecek bazı özellikler [44]

Özellik	**Denklem**
Kontrast (*Contrast*)	$\sum_{i,j} \lvert i-j \rvert^2 p(i,j)$ (2.10)
Homojenlik (*Homogeneity*)	$\sum_{i,j} \frac{p(i,j)}{1+\lvert (i-j) \rvert}$ (2.11)
Enerji (*Energy*)	$\sum_{i,j} \{p(i,j)\}^2$ (2.12)
Korelasyon (*Correlation*)	$\sum_{i,j} \frac{(i-\mu_i)(j-\mu_j)p(i,j)}{\sigma_i \sigma_j}$ (2.13)

Şekil 2.21 4x5'lik bir görüntü için (solda) d = 1 ve Θ = 0 olmak üzere GSEM (sağda) eldesini göstermektedir.

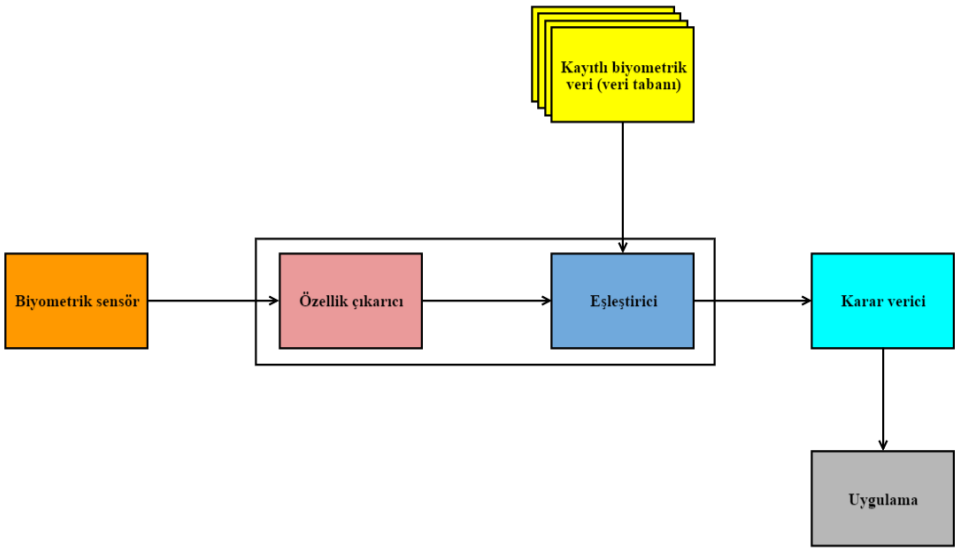
1	1	2	3	1
3	5	7	2	6
4	4	1	1	1
5	7	3	8	4

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	3	1	0	0	0	0	0	0
2	0	0	1	0	0	1	0	0
3	1	0	0	0	1	0	0	1
4	1	0	0	1	0	0	0	0
5	0	0	0	0	0	0	2	0
6	0	0	0	0	0	0	0	0
7	0	1	1	0	0	0	0	0
8	0	0	0	1	0	0	0	0

Şekil 2.21. Gri Seviye Eş-Oluşum Matrisi-GSEM örneği

3. BİYOMETRİK SİSTEM TASARIMI

Sistem düzeyinde bir tasarım hedefleyen bu tez çalışmasında biyometrik bir sistemin çeşitli modülleri tasarlanacaktır. İlgili sistemin bileşenleri temel olarak şu şekilde sıralanabilir: verinin alındığı sensör girişi, özellik çıkarımının yapıldığı modül, kayıtlı önceki biyometrik verileri/şablonları gelen giriş verisine eşleyici kısım ve eşleşme oranına göre karar verici kısım ile sonda uygulama modülü (arayüz, ATM makinası vb.). Şekil 3.1'de temel olarak bir biyometrik sistemin bileşenleri gösterilmiştir [37].



Şekil 3.1. Biyometrik bir sisteme ilişkin modüller

Şekil 3.1.'e göre öncelikle biyometrik veri bir sensör yardımıyla alınır. Bu bir parmak izi sensörü, kamera, mikrofon, hatta kimyasal ölçüm yapan bir sensör olabilir. Ardından elde edilen veriler özellik çıkarımı için ilgili modüle iletilir. Edinilen özellikler önceden kayıtlı veriler ile karşılaştırılmak ve sınıflandırılmak için bazı işlemlere tabi olur. Eldeki sonuca ve mevcut eşik değere göre bir karar verilir ve gelen verinin kim olduğu hakkında veya iddia edilen kişi olup olmadığı hakkında bir sonuca varılır. Eğer sisteme kullanıcı kaydı söz konusu ise, (*enrollment*) o zaman gelen biyometrik veri özellik çıkarımının ardından veri tabanına kaydedilir. Uygulama kısmı kullanıcı ile iletişimde olan kısımdır. Bu tez

çalışmasında benzer bir sistem genel hatları ile ve belirli modüller üzerine yoğunlaşarak hem güvenlik hem de gelen veriyi doğru tanımlayabilme ilkeleri kapsamında tasarlanmaya çalışılmıştır. Bu açıdan Bölüm 2'de anlatılan teorik alt yapı bilgileri kullanılacaktır.

3.1. Sistemi Oluşturan Donanım Bileşenleri

Bu kısımda algoritmanın koştuğu gerçekleme ortamına ilişkin donanım detayları sunulmaktadır. İki temel kart kullanılmıştır: özellik çıkarımı, veri güvenliği, karşılaştırma gibi işlemlerin yapıldığı *4 çekirdekli UDOO* ve veri tabanının tutulacağı *Raspberry Pi* geliştirme kartı.

3.1.1. UDOO 4 çekirdekli geliştirme kartı

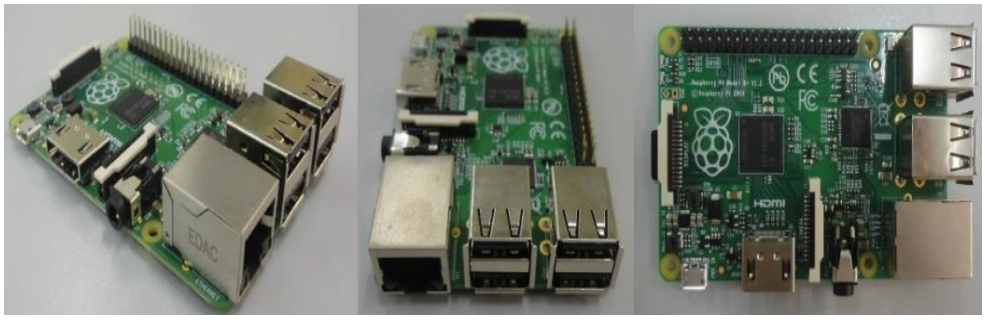
UDOO 4 çekirdekli geliştirme kartı özel olarak çok çekirdekli uygulamalar için kod geliştirmeye de yarayan bir elektronik karttır. Özelliklerine bakıldığında, 1GHz 4 çekirdekli ARM Freescale Cortex-A9 i.MX 6 CPU ve 1GB DDR3 RAM mevcuttur. UDOO kart HDMI çıkışa sahiptir ve VGA'ya dönüştürücü ile bir ekrana bağlanmaktadır.

Şekil 3.2. UDOO 4 çekirdekli geliştirme kartı

Şekil 3.2'de gösterilen karta özel bir işletim sistemi bulunmaktadır ve bu mini bilgisayar Arduino geliştirme kartı ile uyumlu pin yapısına da sahiptir. Böylelikle Arduino ile çalışan sensörler bu kart üzerinde kullanılabilir. Arduino geliştirme kartı kullanarak [46] kaynağında sunulan parmak izi tabanlı bir güvenlik sistemi mevcuttur.

3.1.2. Raspberry pi geliştirme kartı

Bir diğer geliştirme kartı Raspbian işletim sistemi yüklü olarak kullanılan Şekil 3.3'deki Raspberry pi 2 geliştirme kartıdır.



Şekil 3.3. Raspberry pi geliştirme kartı

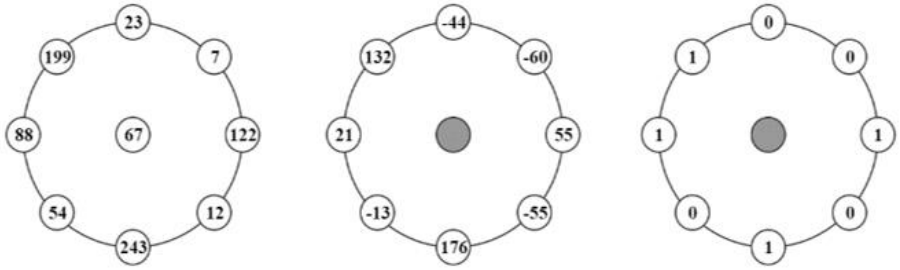
Bu kart ARMv7 4 çekirdek işlemcili 900MHz saat işaretine sahip, 1GB RAM'i olan bir modeldir. Minimum 4 GB hafıza kartı ile çalışan bu sistem, testler sırasında var olan biyometrik verilerin saklanması için kullanılmıştır. Dört adet USB çıkışı bulunan bu kart ile giriş çıkış birimleri –klavye, fare gibi- kolayca bağlanarak uygulama geliştirilmiştir. Ayrıca Raspberry pi, sahip olduğu 40 ek pin ile başka bazı sensörlerin bağlanmasını ve değişik haberleşme protokolleri (I2C, SPI, UART gibi) ile haberleşerek uygulama geliştirmeyi desteklemektedir. Literatür incelendiğinde elektronik sağlık sistemleri, giyilebilir teknolojiler başı çekmektedir. Boyut olarak bu geliştirme kartı neredeyse kredi kartı ile aynıdır. Arunkumar ve Raja Raspberry pi ile parmak izi okuyuculu bir güvenlik sistemi geliştirmişlerdir. Parmak izi resimleri arasında tepe çizgilerinin eşlenmesi üzerine geliştirilen algoritma gömülü sistem üzerinde çalıştırılarak sistem seviyesinden daha üst seviyede -uygulama seviyesinde- bir çalışma sunulmaktadır [47].

3.2. Önerilen Metotlar

3.2.1. İlişkisel Bit Operatörü (İBO)

Yüz tanımada kullanılan pek çok operatör ve yöntem mevcuttur. Bunlardan bazıları arka planı olmayan, yalnızca yüzün olduğu görüntüleri alırken, bazıları yüz üzerinde önemli noktaları çeşitli filtreler yardımı ile belirmeye çalışır. Bu tez çalışmasında önerilen yeni bir yaklaşım arka planı çoğunlukla homojen dokuda olan yüz resmi üzerinde temel elemanları aramadan benzer dağılım gösteren verileri çıkarır. Tek bir gri piksel değeri ile ifade edilen aynı davranıştaki veriler, tekrar eden bu gri seviyesi yeni piksel değerinin dağılımı ile yüz verisi elde edilir.

Literatürde yerel ikili örüntü operatörü (*Local Binary Pattern*) ile görüntüden çeşitli desendeki özellikler elde edilerek veri çıkarımı yapılır. Yüz tanımada da karşımıza çıkan bu yöntem, bu tez çalışmasındaki önerilen operatöre ilham kaynağı olmuştur. Yerel ikili örüntü operatörü, merkez piksele göre komşuların değerini kıyas ederek; büyük olan komşu değeri için 1, küçük olan için 0 ikili değerini yazar. Elde edilen 1 ve 0'lardan oluşan veri yapısı üzerinde bir noktadan başlanarak ikili değerler onluk tabana çevrilir ve yeni değer kaydedilir. Bu analiz ile nokta, *yarım ay, daire* vb. gibi özellikleri elde etmek mümkündür. Merkez pikselden kaç adım ötedeki komşuların seçileceği ve ikili değerlerin hangisinden başlanarak onluk tabana dönüşüm yapılacağı bu yöntemin parametreleridir [48].



Şekil 3.4. Yerel ikili örüntü operatörü örneği

Tez kapsamında önerilen yeni yöntem ile bileşen analizi yapmak yerine tıpkı insan gözünün algısını taklit eder gibi yakın dokudaki görüntü parçalarını tek bir

değere indirgemek ve böylece hem benzer davranışları sınıflamak hem de daha az veri elde etmek mümkün olmuştur. Örneğin,

I

188	45	12	66	78	88	3	255

II

174	42	19	50	67	112	42	243

I ve II ile gösterilen vektör değerleri incelendiğinde soldan sağa her ardışık hücre arasındaki artış azalış ilişkisi, I ve II için aynıdır. Azalan değerler için 0, artan değerler için 1 kullanarak iki vektör içinde elde edilen ikilik tabandaki değer aynı olacaktır.

188 → 45 → 12 → 66 → 78 → 88 → 3 → 255

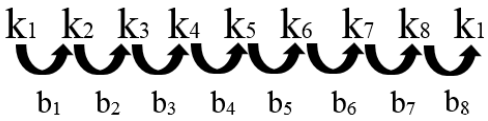
0	0	1	1	1	0	1

Şekil 3.5'de gösterilen c merkez ve tüm k komşuları için yeni bir operatör tanımlaması yapılabilir. Yüz resmi üzerinde çerçeveyi oluşturan piksel değerleri hariç her bir piksel c olacak şekilde, komşuların birbirleri ile olan dağılımına bakılarak tıpkı I ve II vektörlerinde olduğu gibi azalmalar ve artmalar kontrol edilebilir.

k_1	k_2	k_3
k_8	c	k_4
k_7	k_6	k_5

Şekil 3.5. İBO – İlişkisel Bit Operatörü; c merkez piksel ve tüm k_x komşuları

Şekil 3.6 ile gösterilen komşu ilişkilerinden elde edilen $b_1b_2b_3b_4b_5b_6b_7b_8$ ikili sayı değeri komşuların davranışını yeni bir gri seviyesi piksel değeri ile modellemek için kullanılacaktır. Komşu değerleri arasındaki geçişte artmalar 1 ($k_1 < k_2$), azalmalar 0'dır ($k_1 > k_2$).



Şekil 3.6. Komşu piksellerin değişimi ile 2'lik düzende $b_1b_2b_3b_4b_5b_6b_7b_8$ sayısı eldesi

Şekil 3.7'de sayısal bir örnek ile operasyon gösterilmektedir. Buna göre kırmızı renkteki merkezin çevresindeki komşular herhangi birinden başlayarak ve bir yön seçerek sıralanacak olursa:

$$k_1k_2k_3k_4k_5k_6k_7k_8k_1 = 211 \quad 71 \quad 13 \quad 110 \quad 98 \quad 9 \quad 42 \quad 58 \quad 211$$

$$b_1b_2b_3b_4b_5b_6b_7 = (00100111)_2 = (39)_{10}$$

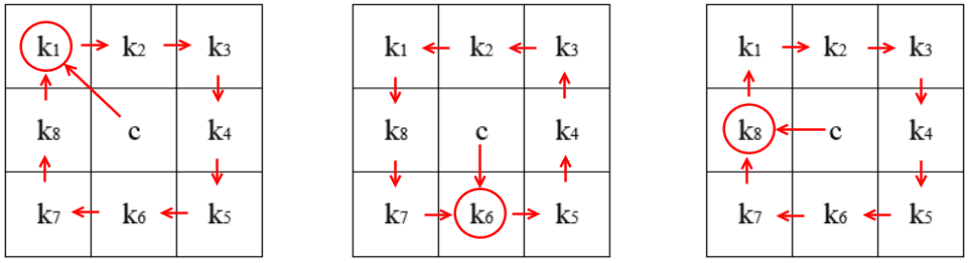
39 sayısı onluk tabanda elde edilir. Bu yeni sayı başka bir matris içinde ilgili merkez piksel pozisyonunda saklanır.

211	71	13
58	67	110
42	9	98

Şekil 3.7. 8-bit gri seviye piksel değerlerine sahip örnek bir görüntü parçası

İlişkisel Bit Operatörü-İBO (Relational Bit Operator-RBO) ismi ile literatüre sunulan bu yaklaşımda elde edilen değerlerin tekrarları tespit edilecektir. Çünkü bazı değerler benzer resim dokusu için aynıdır ve sayıca öne çıkan bu değerler sınıflandırma için kullanılabilir. İBO üç parametreye sahiptir: merkezden

komşulara olan adım sayısı, başlangıç pikseli ve yön. Şekil 3.8 adım boyu 1 olan komşuluktaki durumu farklı başlangıç pikseli ve yönleri için göstermektedir.



Şekil 3.8. Olası başlangıç pikseli ve operasyon yönü

3.2.2. Açıdan Bağımsız Parmak İzi Tanıma (ABPT) Yöntemi

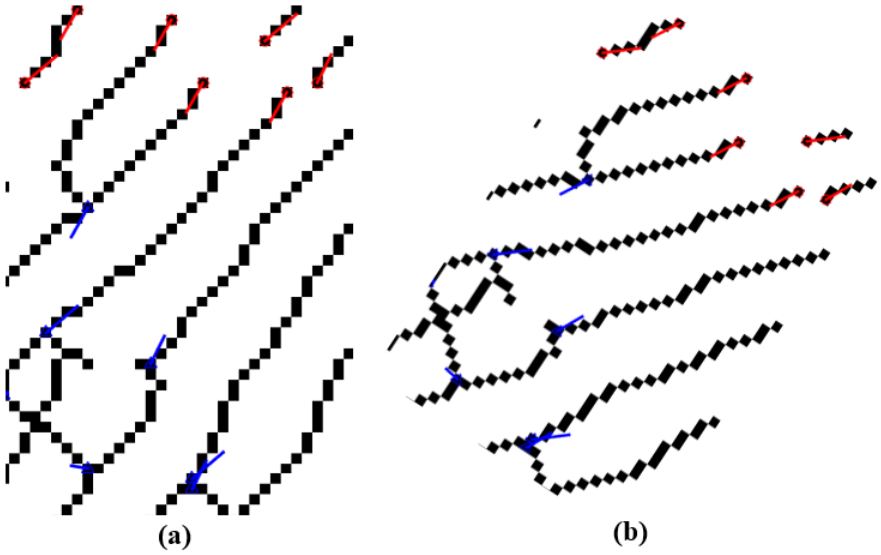
Çoklu biyometri kapsamında diğer biyometrik veri olan parmak izinin özellik noktası çıkarımı Bölüm 2.'de anlatılmıştı. Çıkarılan özelliklerin veri tabanında ait olduğu sınıf ile eşleştirilmesi için literatürde seviye 2 kapsamında özellik tipi, koordinatı ve açı bilgisi kullanılmaktadır. Genel olarak parmak izi eşleştirme için:

1.) Poincaré indeks yöntemi ile seviye 1 özellikleri kullanarak orta nokta tespiti
2.) Seviye 2 ile uç ve çatal noktaları için koordinat ve açı değerlerinin eldesi
3.) Parmak izinin tam orta noktasından dikey olarak geçen sanal çizginin sensör yüzeyine paralel olarak yaptığı açının bulunması

adımları kullanılarak test edilen verinin önceden kayıtlı veri ile açısal olarak farkına bakılır. Böylece parmağın sensör üzerindeki hareketi modellenmiş olur.

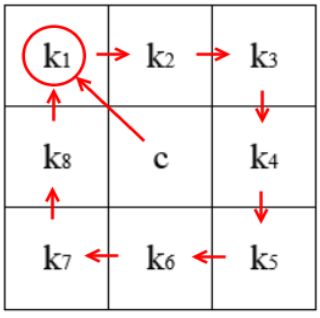
Açıdan Bağımsız Parmak izi Tanıma (ABPT) ve sınıflandırma yöntemi ile seviye 1 ile orta nokta tespiti, seviye 2 için açılar ve sensör üzerindeki açısal yön kullanılmadan yeni bir yöntemle eşleştirme önerilmektedir. Şekil 3.9'da sensör üzerinde meydana gelebilecek olası bir açısal farklılık gösterilmektedir. Mavi ve kırmızı çizgilerle gösterilen özellik noktalarının tepe çizgileri hepsi aynı oranda ve aynı miktar açı kadarlık bir rotasyona sahip olmaktadır. ABPT ile her uç ve çatal noktası özelliğinin açı değeri kullanılmadan, olası tüm rotasyon durumları değerlendirilerek bir model geliştirilmiştir. Parmak izi tanıma teknolojilerinde parmağın sensöre her defasında dokunduğu yön parametresi farklı olacaktır. Bunun

bir şekilde modellenmesi parmak izi eşleştirmedeki *minutiae* özellik noktalarının sayısı göz önüne alınarak sağlanacaktır.



Şekil 3.9. Önceki bölümde elde edilen özellikleri belirli parmak izinin rotasyonu

Önerilen yöntem ile kıyas yapılacak olan test resmi öncelikle tüm rotasyon ihtimalleri için değerlendirilecektir. Bunun için Şekil 3.10'da gösterilen ilişkisel bit operatörü ile aynı yapı kullanılmaktadır. Sistem düzeyinde çoklu biyometri için tasarım yaparken benzer operatörü kullanarak benzer verileri elde etmek adına füzyon kapsamında da oldukça avantajlı bir durum elde edilmiştir. Dahası donanımda gerçeklenebilirlik incelendiğinde aynı operatörün kullanılması ve bu operatörün kıyas edici devre ile (*comparator*) kolayca temsil edilebilirliği tezin başında konulan hedefe de uygundur.



Şekil 3.10. İlişkisel bit operatörüne benzer yapı

Şekil 3.10'da gösterilen merkez piksel c'nin konumu, parmak izi özellik çıkarımı sırasında uç ve çatal noktalar bulunurken elde edilen özellik noktasının koordinatıdır. Yani tüm resmi taramak gibi bir durum söz konusu değildir; yalnızca *minutiae* özellik noktaları ve çevresindeki pikseller dikkate alınacaktır. Her bir özellik noktası için 1 adım uzaklıktaki komşu pikseller k_1 komşusundan başlanarak ve saat yönünde ilerlenerek bir vektör şeklinde bir araya getirilir. Bu defa elde edilen değerler artma veya azalma ile değil, parmak izi 1 ve 0 ikili değerlerinin 8 bit olarak bir araya getirilmesi ile elde edilmiştir. Çizelge 3.1'de özellik çıkarımında kullanılan şablonlara ilişkin elde edilen onluk tabandaki değerler hesaplanmıştır. Bu değerler her $\pi/4$ olası dönüş için elde edilebilecek örüntü değeridir. Böylece her bir özellik noktası için açı yerine geçebilecek bir sayı değeri elde edilmiştir.

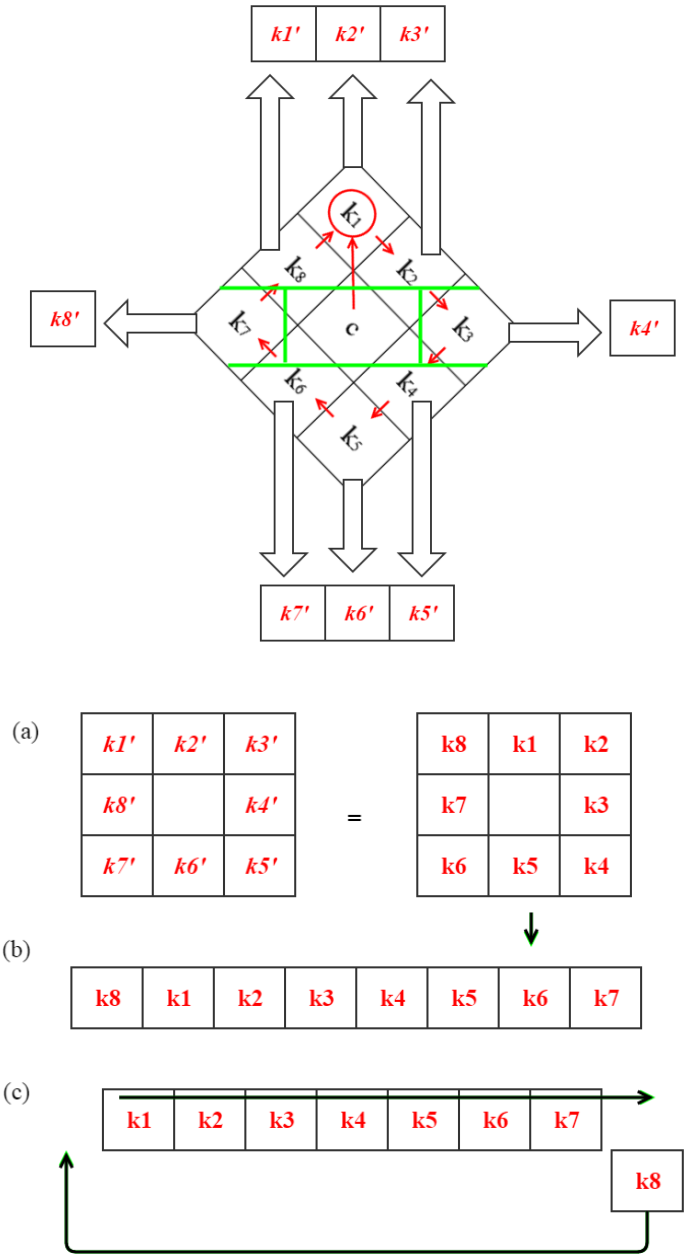
Çizelge 3.1. Özellik tipine göre elde edilen bazı örüntü değerleri

Şekildeki pozisyonu	**Özellik Tipi**	
	Uç nokta, Şekil 2.12	***Çatal, Şekil 2.13***
(a)	$(10000000)_2=(128)_{10}$	$(10001010)_2=(138)_{10}$
(b)	$(01000000)_2=(64)_{10}$	$(00010101)_2=(21)_{10}$
(c)	$(00100000)_2=(32)_{10}$	$(00101010)_2=(42)_{10}$
(d)	$(00010000)_2=(16)_{10}$	$(01000101)_2=(69)_{10}$
(e)	$(00001000)_2=(8)_{10}$	$(10101000)_2=(168)_{10}$
(f)	$(00000100)_2=(4)_{10}$	$(01010001)_2=(81)_{10}$
(g)	$(00000010)_2=(2)_{10}$	$(10100010)_2=(162)_{10}$
(h)	$(00000001)_2=(1)_{10}$	$(01010100)_2=(84)_{10}$

Sınıflandırma yapılırken, kimliklendirme veya doğrulama yapılacak olan test resmi için mevcut pozisyonundan $\pi/4$ rotasyon adımları ile resimdeki her bir özellik noktası için örüntü değeri hesaplanacak ve her bir örüntü sabit değerinin de anlık pozisyondaki resimde kaç adet bulunduğu kaydedilecektir. $8*\pi/4$ yani 2π başlangıç konumuna gelene dek bu operasyon sürdürülecektir. Ardından elde edilen değerler

veri tabanındaki aynı algoritmadan gelen veriler ile kıyaslanarak sınıflandırma yapılacaktır.

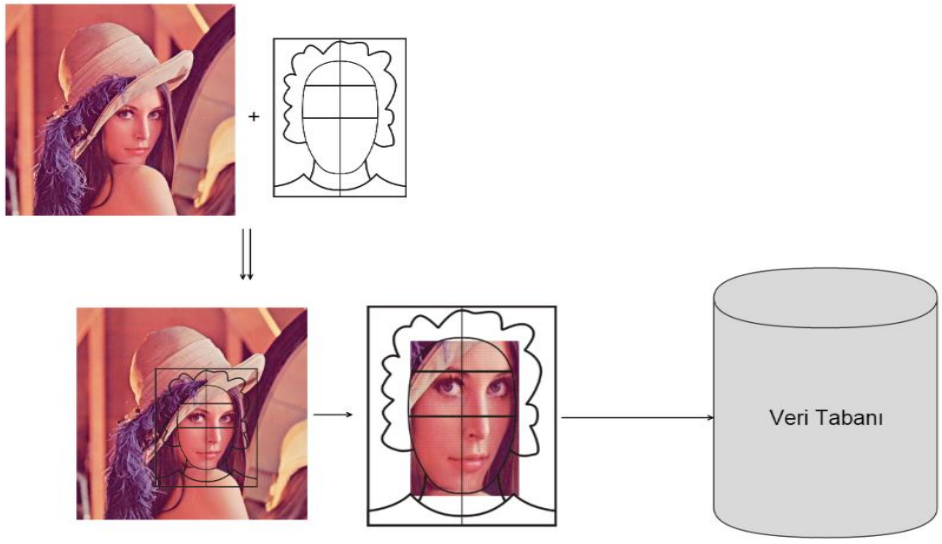
Şekil 3.11'de her bir rotasyon adımı için esasında lojik kaydırma operasyonu yapıldığı vurgulanmaktadır. Bu durum yine lojik seviyesi donanım ile tasarlanabilirlik açısından oldukça avantajlıdır.



Şekil 3.11. Her rotasyonda yapılan kaydırma işlemi

3.2.3. Biyometrik sistemde paralel hesaplama: *dilimle, işle, birleştir*

Resimler görüntü işleme tekniklerine tabi olurken matris yapısında olduklarından dolayı ve bir veri tabanında arama işlemi de söz konusu olabileceği için toplam hesaplama zamanı açısından problemler ortaya çıkabilir. Veri tabanı oluşturulurken diğer resimlerin özellik çıkarımı işlemleri ve ilgili yeni bir resmin arama & yetkilendirme işlemi biyometrik geçiş sistemlerinde zaman ve performansı etkileyen parametrelerdir. Bu sebeple tek bir biyometrik hazır veriden özellik çıkarımı yapılırken gerekli piksellerin bölünerek çok çekirdekli işlemcide dağıtılması mümkündür. Parçalı olarak yapılacak işlemler birbirlerinden bağımsız olarak yapılabilir ve veri kaybı olmaması için sınır pikseller de kendi arasında paylaşılabilir. Nihayetinde en son hesaplanan özellikler bir araya getirilecektir. Böylece, elde var olan tek resmin tümünün baştan sona ve tek bir işlemcide daha uzun sürede işlem görmesinden farklı olarak; parçalı ve çok çekirdekli bir mimaride daha hızlı hesaplanması söz konusu olacaktır [16].

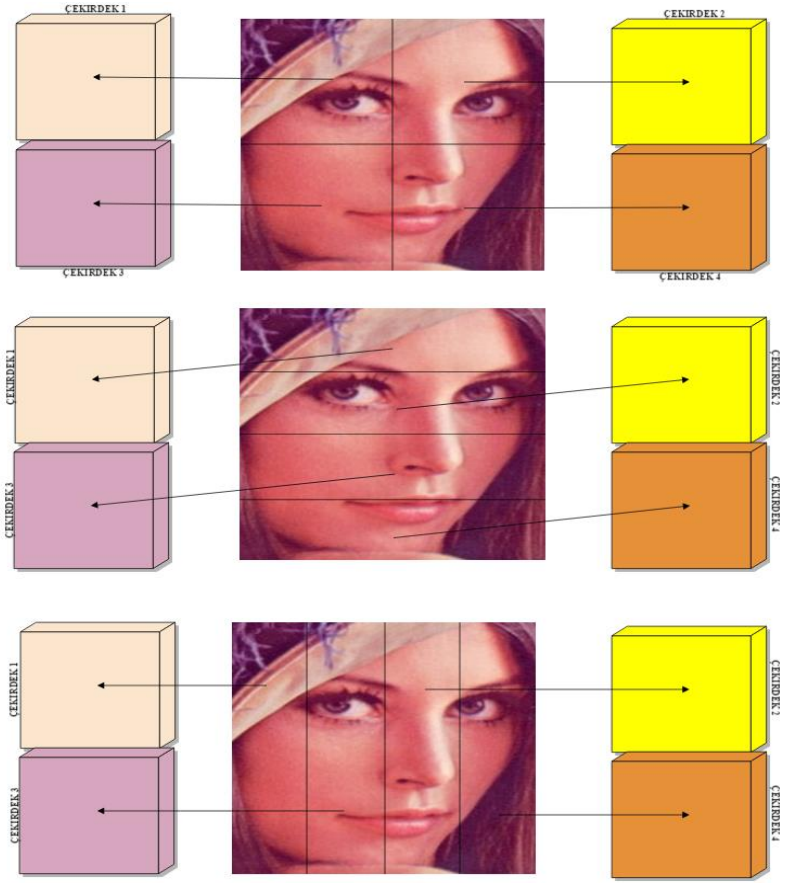


Şekil 3.12. Biyometrik bir yüz görüntüsü ile veri tabanına erişim

Şekil 3.12'de örnek bir biyometrik erişim sistemi için yüz verisinin kullanımı gösterilmektedir. Gelen verinin gerekli kısımları kullanılarak ilgili veri tabanında arama yapılır. Bu türlü biyometrik erişim sistemleri güvenlik artırımı sağlaması sebebiyle son yıllarda yaygınlık kazanmaya başlamıştır. Bu noktada yüz tanıma

sırasında gelen veriden çıkarılacak özellik (*feature extraction*) teknikleri hız açısından paralel hale getirilebilir. Bu çalışmada bir resmin özellik çıkarımı sırasında daha en başta kullanılması öngörülen piksel sayısına bağlı olarak iş yükünün işlemci içinde dağıtılması yaklaşımı sunulacaktır. Pasaport sistemlerinde kullanılan tam bir yüz resminde belirli ölçülerin dışında kalan kısımlar -arka plan vb.- özellik çıkarımı bakımından kullanılmayacağından dikkate alınmaz. Kalan işe yarar veri; yani yüze ait pikseller işlemci içinde bölgesel olarak yüz tanıma algoritması için kullanılmak üzere dağıtılabilir ve yüksek başarım sağlanabilir.

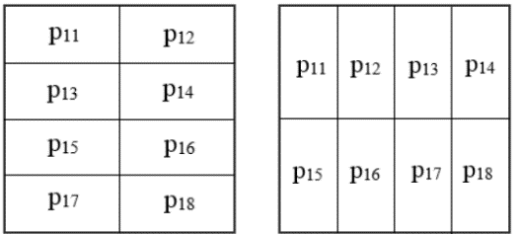
Şekil 3.13'de görsel olarak bir yüz resmine ait 4 çekirdekli bir işlemcide dağıtılma durumları gösterilmektedir. Bir sonraki kısımda ilgili bölmelere ayırma işleminin detayları ve işlemci içinde dağıtılma durumları anlatılacaktır.



Şekil 3.13. Yüz resminin analizi için 4 çekirdekli işlemciye ait örnek iş bölümü ihtimalleri

Yatay olarak, dikey olarak ya da orta noktaları seçerek bölmelendirme işlemi kullanılacak olan bu çalışmada, eşit olarak parçalara ayırma işlemi gelen yüz görüntüsü için yapılacaktır. Ardından biyometrik bir şablon gereği gerekli olmayan pikseller çıkarıldığında kalan işe yarar veriden oluşan parça, bir iş yükü getirecektir ve anlık olarak ilgili çekirdeklerin de iş yüküne göre dağıtım yapılacaktır. Bu sebeple bağımsız her bir bölmeleme ihtimalinin kendi içindeki parçalarının birbiri arasındaki farklılıkları önemlidir. Birbirlerinden çok farklı iş yükü getiren parçalar eşit yoğunluktaki bir işlemcide eş zamanlı bitmeyecek ve en iyi çözümü sunmayacaktır. İşlemcinin durumuna göre en az fark veya çok farka sahip dilimleme seçeneği, işlemcinin durumuna göre seçilip dağıtılacaktır. Yük dengeleme sağlayacak bu yöntem ile yüksek başarımlı sonuçlar hedeflenmektedir.

Bölmelendirmenin yapılabilmesi için çeşitli ihtimaller söz konusudur. Şekil 3.13'de ortaya çıkan 3 seçenek 4 çekirdekli bir mimari için verilmiştir. Diğer bir örnek olarak gösterilen Şekil 3.14'de işlemcideki çekirdek sayısı 8 olduğunda ortadan olarak isimlendirilen bölmelendirme şeklinin 2 farklı ihtimal ile yapılabileceği vurgulanmaktadır. Her bir *p* parçası iş yükünü yani işe yarar piksel sayısını göstermektedir.



Şekil 3.14. 8 çekirdekli bir işlemcinin "ortadan" yaklaşımını kullanarak resmi parçalara ayırması

İşlemcinin mevcut iş yüküne göre olası resim bölmelendirmelerinden hangisinin uygulanıp ilgili parçaların çekirdeklere dağıtılacağına karar vermek oldukça kritiktir. Bu noktada, öncelikle her ihtimal için hesaplanan p parçalarının kendi içinde birbirlerinden ne kadar farklı olduğuna bakılır. Bu noktada k ortalama (*k-means*) algoritmasına benzer yaklaşımdan yola çıkarak, her iş yükünün ortalamaya olan uzaklığı konusunda benzerlik gösteren ancak iteratif olmayan bir algoritma sunulmaktadır. Bunun için gri seviyesindeki piksel sayısı temel alınarak

hesaplanan işe yarar p_{xy}'ler önce ortalama hesabına katılır. Ardından her birinin mutlak değer olarak ilgili ortalamadan ne kadar uzak olduklarına bakılır ve toplamsal bir sonuç elde edilir. Bu değer her bir iş yükünün ilgili bölmelendirme için birbirine ne kadar yakın olduğunun bir göstergesidir ve Fark olarak isimlendirilmiştir. Fark eğer 0 ise tüm parçaların iş yükü aynıdır ve rastgele dağıtılabilir.

$$Ort_o = \frac{p_{11} + p_{12} + p_{13} + \cdots + p_{1n}}{n} \tag{3.1}$$

$$Fark_o = |Ort_o - p_{11}| + |Ort_o - p_{12}| + \cdots + |Ort_o - p_{1n}| \tag{3.2}$$

$$Ort_y = \frac{p_{21} + p_{22} + p_{23} + \cdots + p_{2n}}{n} \tag{3.3}$$

$$Fark_y = |Ort_y - p_{21}| + |Ort_y - p_{22}| + \cdots + |Ort_y - p_{2n}| \tag{3.4}$$

$$Ort_d = \frac{p_{31} + p_{32} + p_{33} + \cdots + p_{3n}}{n} \tag{3.5}$$

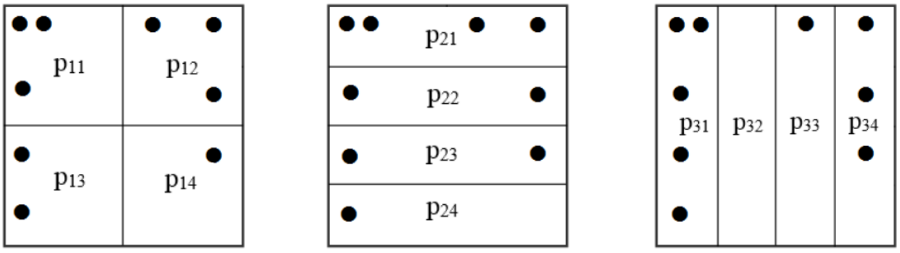
$$Fark_d = |Ort_d - p_{31}| + |Ort_d - p_{32}| + \cdots + |Ort_d - p_{3n}| \tag{3.6}$$

Yukarıdaki (3.1)'den (3.8)'e kadarki denklem grubunda, bir önceki paragrafta anlatılan ifadeler formüllerle verilmiştir. Denklemlerde o, y, d alt indisleri ile gösterilen ortalama ve fark değerleri; sırası ile orta noktaları seçerek, yatay olarak ve dikey olarak bölmelendirme olduğundaki durumları ifade eder. Ortalama değerlerin tümü zaten birbirine eşit olacaktır; çünkü nasıl bölümlendirildiğine bakılmaksızın toplamdaki mevcut piksel sayısı bellidir ve hep aynı çıkacaktır.

İşlemcideki çekirdeklere dağıtılmaya aday resim, *p* ile sembolize edilen olası her bir parçasının sahip olduğu işe yarar piksel sayısı için hesaplamaya tabi olur. İşe yarar piksel, biyometrik veri açısından anlam ifade eden, arka plan görüntüsü vb. kısımların çıkarılması ile elde edilen anlamlı gri seviyesi değerlerdir.

Şekil 3.15'de teorik olarak anlatılan bölmelendirme işlemine ait nümerik bir örnek sunulmaktadır. Her bir siyah nokta, kullanılacak olan bir pikselin varlığını

temsil etmektedir. Basit olması açısından sayılar çok küçüktür. Örneğin, 512x512 boyutundaki bir görüntü için yalnızca bir p_{xy} bölmesi tümüyle anlamlı, işe yarar piksel değerleri taşıyor ise, 65536 adet piksel iş yükü yaratacaktır. İlgili örneğimizde 4 çekirdekli işlemcinin üzerinde çalışan bir yüz tanıma algoritması için işleme alınacak verinin olası bölmelendirilme işleminden bahsedilmektedir. Önce ortalama hesabı, sonra ilgili parçaların arasındaki değişimin kontrolünün ardından güncel olarak işlemcinin iş yüküne göre dağıtım yapılacaktır.



Şekil 3.15. Nokta ile gösterilen, işlem yükünü artıran piksellerin 4 çekirdekli işlemcide dağılımı

$$p_{11} = 3 \quad p_{21} = 4 \quad p_{31} = 5$$

$$p_{12} = 3 \quad p_{22} = 2 \quad p_{32} = 0$$

$$p_{13} = 2 \quad p_{23} = 2 \quad p_{33} = 1$$

$$p_{14} = 1 \quad p_{24} = 1 \quad p_{34} = 3$$

$$Ort_o = (3 + 3 + 2 + 1) / 4 = 2{,}25$$

$$Fark_o = | 2{,}25 - 3 | + | 2{,}25 - 3 | + | 2{,}25 - 2 | + | 2{,}25 - 1 | = 3$$

$$Ort_y = (4 + 2 + 2 + 1) / 4 = 2{,}25$$

$$Fark_y = | 2{,}25 - 4 | + | 2{,}25 - 2 | + | 2{,}25 - 2 | + | 2{,}25 - 1 | = 3{,}5$$

$$Ort_d = (5 + 0 + 1 + 3) / 4 = 2.25$$

$$Fark_d = | 2{,}25 - 5 | + | 2{,}25 - 0 | + | 2{,}25 - 1 | + | 2{,}25 - 3 | = 7$$

Bu sonuçlara bakarak sırası ile en yüksek farklılıktan en düşüğe doğru dikey, yatay ve ortalayarak bölmelendirilen resim adaylarından seçilen uygun bir tanesinin 4 parçası n=4 çekirdek içine dağıtılacak şekilde atanır. Bu sırada anlık olarak işlemcinin her bir çekirdeği için de yük yoğunluğuna bakılacaktır. Eğer homojen bir dağılım yoksa ilgili bölümlendirmelerden parçalar arasında yüksek değişim gösteren seçilir. Tersi durumda, eğer her bir çekirdek birbirine yakın bir iş yüküne sahip ise bu defa en az fark yaratan bölmelendirme biçimi seçilerek her parça çekirdek yükü ile ters orantılı olarak atanır. Yani, diyelim ki seçilen $p_{x1y1}<p_{x1y2}<p_{x1y3}<p_{x1y4}$ için 4 çekirdekli bir işlemciye ait $\ell_1 < \ell_2 < \ell_3 < \ell_4$ gibi bir oranla anlık işlemci yükü söz konusu olsun. Bu durumda ilgili atama

$$p_{x1y1} \rightarrow \ell_4$$
$$p_{x1y2} \rightarrow \ell_3$$
$$p_{x1y3} \rightarrow \ell_2$$
$$p_{x1y4} \rightarrow \ell_1$$

şeklinde olacaktır.

Görüldüğü gibi bu noktada işlemcideki iş yükü farkı da göz önüne alınmaktadır. Hangi bölmelendirmenin seçileceği iş yükü dağılımına bağlıdır. Bu çalışmada önerilen yaklaşıma ait algoritma detayları sözde kod olarak Çizelge 3.4'de sunulmuştur. Algoritmaya ilişkin giriş çıkış değişkenleri ise açıklık kazandırmak adına Çizelge 3.2'de verilmektedir.

Çizelge 3.2. Algoritma için giriş çıkış değişkenleri

Değişken Adı	**Açıklama**
I	Giriş görüntüsü
n	Çekirdek sayısı
M	Resmin satır sayısı
N	Resmin sütun sayısı
$\ell_{1,2,...,n}$	Çekirdeklerin iş yükü
p_{xy}	Resmin her bir parçası
Fark[]	$Fark_o$, $Fark_y$, $Fark_d$
I1, I2, I3,…,Ik	Resmin kopyaları
Boyutlar[]	Biyometrik yüz şablon için vesikalık boyutlar

Algoritmanın içeriğine bakıldığında 2 temel fonksiyon karşımıza çıkmaktadır: Dilimle ve Hesapla. Yüksek başarım hedefi ile hesaplanacak olan resim tüm dilimleme seçeneklerine tabi olarak anlık iş yüküne göre en uygun işlemcide dağıtılacaktır. Hesapla fonksiyonu Dilimle fonksiyonunu çağırarak yatay, dikey ve ortadan dilimleme için tüm durumları ayrı resim kopyaları için hesaplatır. Fark ve işlemci çekirdeklerinin güncel yük sıralamasının ardından algoritmadaki 26. satırdan itibaren en uygun dilimleme seçilerek işlemcide dağıtım gerçekleşir. İş yükü yaratacak dilimlenmiş her bir p_{xy} parçası için x dilimleme çeşidini (1:Ortadan, 2:Yatay, 3:Dikey), y ise dilimlenen hangi parça olduğunu ifade etmektedir. Çizelge 3.3'de satır-sütun sayısının çekirdek sayısına bağlı olarak nasıl dilimlendiği örneklenmiştir.

Çizelge 3.3. Bazı çekirdek sayıları için resmin M-N satır-sütun sayısına göre dilimleme örnekleri ve M-N sayılarının bölme işlemi

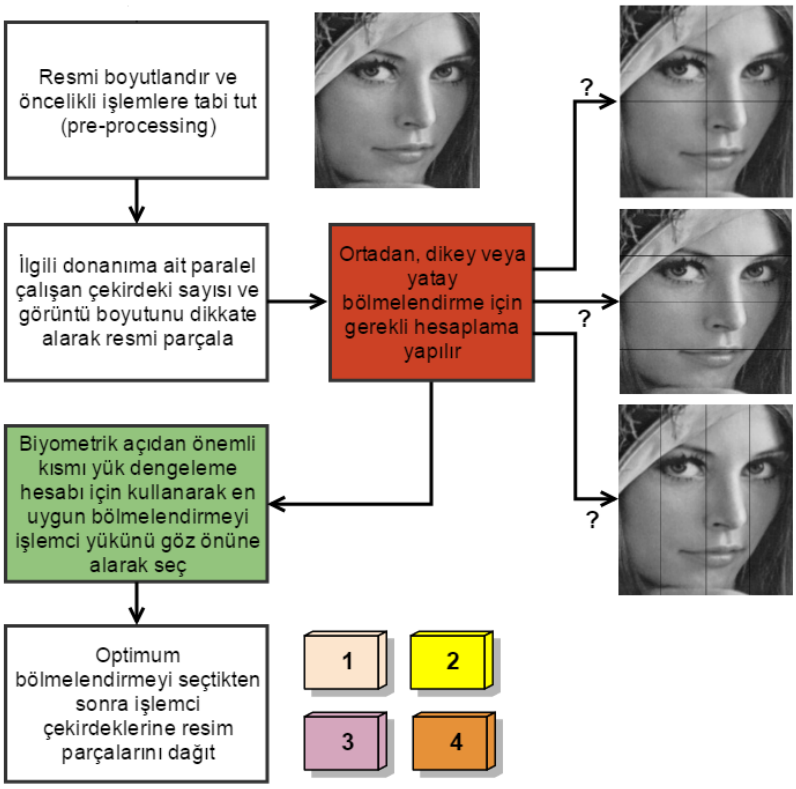
Ortadan *x*=1	**Yatay *x*=2**	**Dikey *x*=3**
n=4 için, M/2 && N/2	*n*=2 için, M/2	*n*=2 için, N/2
n=8 için, (M/2 && N/4) || (M/4 && N/2)	*n*=4 için, M/4	*n*=4 için, N/4

* && →ve, || →veya

Çizelge 3.4. Sözde kod şeklinde ifade edilen algoritma

Algoritma: Biyometrik yüz verisinin yüksek başarım için paralel olarak hesaplanması

```
1:  function Dilimle (I, x, n, çıkış_I, Fark[], pxy[])
2:        I1, I2, I3,…,Ik ← I
3:        ön_işlem(I1, I2, I3,…,Ik);
4:        M, N ← I.satır_sütun
5:        if x==1 then
6:        1.  Ortadan dilimleme yapılır (M, N sayıları
7:        bölünür).
          2. İş yükleri hesaplanır, ortalama ve fark
          bulunur.
8:        end if
9:        if x==2 then
10:       1. Yatay dilimleme yapılır (M, N sayıları
11:       bölünür).
          2. İş yükleri hesaplanır, fark bulunur.
12:       end if
13:       if x==3 then
14:       1.  Dikey dilimleme yapılır (M, N sayıları
15:       bölünür).
          2. İş yükleri hesaplanır, fark bulunur.
16:       end if
17: end function
18:
19: function Hesapla(n, pxy[], M, N)
20:       for x=1 ➔ 3 do
21:             Dilimle(I, x, n, çıkış_I, Fark[],pxy[])
22:       end for
23:       1. Fark[] için ortadan, yatay, dikey değerleri sıranılır.
24:       2. l1,2,...,n anlık çekirdek iş yükleri için sıralama yapılır.
25:       if çekirdekler arası iş yükü farkı çok fazla then
26:             1. Fark[] en fazla olan dilimleme çekirdeklere gider.
27:       else çekirdekler arası iş yükü farkı az then
28:             1. Fark[] en az olan dilimleme çekirdeklere gider.
29:       end if
30: end function
```



Şekil 3.16. Önerilen yönteme ait adımların gösterimi

Şekil 3.16'da bir resmin analizi sırasında işlemciye ait çekirdeklere görev dağılımdaki adımların nasıl yapılacağı açıklanmaktadır. Burada ilk adım *pre-processing* yani resmin ön hazırlığı işlemidir. Aslında bu kısım renkli resmin gri seviyeye çevrilmesinden, gereksiz alanların kırpılmasına kadar önemli alt işlemleri içerir. Şablon olarak kullanılan ICAO standartları, önişlem için önemli ölçüde kolaylık sağlamaktadır. Ardından kullanılan donanıma ait detaylara göre; yani sahip olunan çekirdek sayısına göre bölmelendirme aynı anda ve aynı resmin farklı kopyaları için yapılır. Bu sebeple algoritma içinde birden fazla resim kopyası oluşturulmuştur. Bu önişlemler de işlemciler arasında dağıtılabilir. Hesaplamaların ardından optimum dağıtım yapılır. Şekil 3.16'da özellikle kırmızı ve yeşil ile belirtilen adımlar yaklaşımın en kritik adımlarını oluşturmaktadır

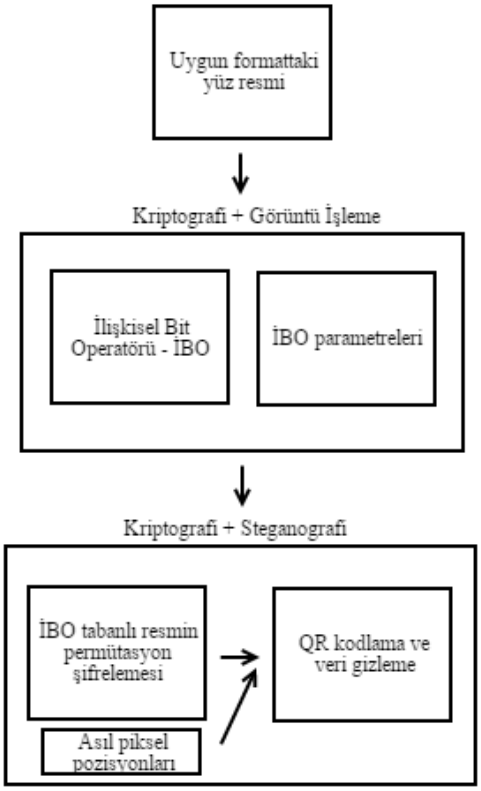
3.2.4. Görsel kriptografi ve biyometrik veri güvenliği

Bu bölümde, elde edilen biyometrik veri şablonlarının sınıflandırılmak üzere gönderileceği modüle transferi sırasında verilerin güvenli hale getirilmesi anlatılacaktır. Biyometrik veriler akıllı bir karttan veya elektronik belge yongasından okuyucu terminale transfer olabileceği gibi bir veri tabanında uzun bir yolculuk ile de kıyaslanmak ve sınıflandırma için seyahat edebilir. Bu veri akışının güvenli bir kanalda olmaması durumda verilerin şifrelenmesi gereklidir. Esasen pasaport sistemleri her adımda güvenli bir kanal üzerinden haberleşmektedir ancak modüller arası sistemi yanıltmaya yönelik ataklar (*reply* atak gibi) mevcuttur.

Bu bölümde öncelikle kriptografi ve steganografi kavramları üzerinde durmakta fayda vardır. Kriptografi bir şifreleme sanatıdır. Bir *E(x)* şifreleyen *encryption* fonksiyonu ve *K* anahtarı ile şifrelenen *x* mesajı *D(x)* kod çözen *decryption* fonksiyonu ile geri elde edilmektedir. Steganografi ise bir medya dosyası kullanarak (örneğin taşıyıcı resim, *stegano image*) saklanmak istenen bilgiyi taşıyıcı medya içine saklamaktadır. Steganografik bir sistemin kırılması görsel veya işitsel olarak gizlenen mesajın atak yapan kişi tarafından fark edilebilirliğine bağlıdır [49].

Şekil. 3.17'de, temel olarak bir yüz görüntüsünün güvenli hale getirilmesi ile ilgili adımlar gösterilmektedir. Burada en genel hali ile önerilen yaklaşımın temel noktalarını gösterilmiştir. Biyometrik yüz resmi biçimsel bir formata sahiptir. Bu giriş görüntüsü arka planı beyaz ve yüzün bazı önemli noktaları belirli bir şablona uygun konumlandırılması ile elde edilir. Önerilen sistemde renk verisinden bağımsız gri seviyesi resimler kullanılmıştır. Önerilen İBO ile paralel işlenen resimden elde edilen veriler birleştirildiğinde 2^n sayıda bayt değeri elde edilmektedir. Örneğin 8-bit gri seviyesinde [0,255] aralığında 256 değer GSEM köşegen değerinden elde edilmektedir. İBO uygulanırken kullanılan başlangıç pikseli, komşuluk adımı ve yön parametresi gibi değişkenlerin de anahtarın bir parçasını oluşturmak üzere saklı tutmak gerekir. Çünkü bu değerler ile veri tabanında aynı algoritmayı uygulamak gereklidir. Elde edilen 2^n adet sayı değeri

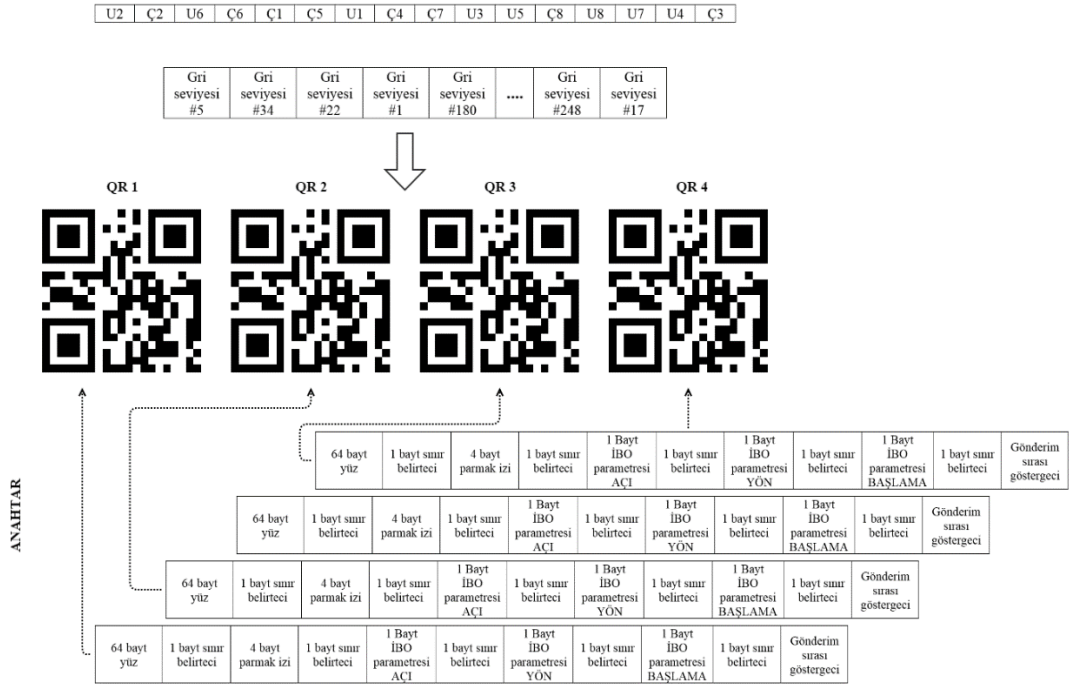
gerçek pozisyonları karıştırılacak şekilde permütasyon şifrelemesine tabi olur. Esas pozisyon değerleri anahtarı oluşturmaktadır.



Şekil 3.17. Yüz şablonu için verilerin güvenliğinin sağlaması adımları [50]

Elde edilen karıştırılmış ancak gerçek pozisyon değerleri anahtar olarak saklanmış veri QR kod içine standart kare kod kodlaması ile gömülmektedir. Elde edilen görüntü resmi bir taşıyıcı medya dosyası olarak kullanılarak steganografi ile içine anahtar saklanmaktadır. QR kodun hataları karşı direnci ve siyah alanların arasında yeni gri seviyesi değerlerin fark edilemezliği ile anahtar gizlemesi yapılmaktadır. Daha güvenli olması açısından tek bir QR taşıyıcı görüntü kullanmak yerine *t* adet kullanmak ataklara karşı daha zor bir senaryo oluşturacaktır. Bu sebeple paralel çalışan *t* görüntü parça sayısı kadar QR görüntüsü elde edilebilir. Öte yandan çoklu biyometri kapsamında, yüz resminin sahibi kullanıcının parmak izi verisi de bu şemaya dahil edilmiştir. Elde edilen her bir uç ve çatal noktalarının komşusundan ABPT ile bulunan örüntü değerleri sayıca kaç tane olduğuna bakılarak (örneğin uç noktası örüntü değerinden biri olan 128 için 16

tane mevcut ise 16 sayısını kayıt etmek şeklinde bir dizi oluşturarak) her örüntü sayısı da QR'a gömülür. Şekil 3.18'de tüm anlatılanlar gösterilmektedir. U ve Ç uç ve çatala ilişkin elde edilen örüntü sayılarını göstermektedir. 16 adet örüntü tipi söz konusudur ve bunları da karıştırarak permütasyon şifrelemesi yapmak mümkündür. Ardından hem yüz hem parmak izinin çıkarılmış özellikleri 4'er parça olarak QR'a gömülür ve her birinin esas pozisyonları İBO parametreleri ile birlikte anahtar şeklinde görüntüye saklanır.



Şekil 3.18. Biyometrik veri güvenliği için önerilen yöntem

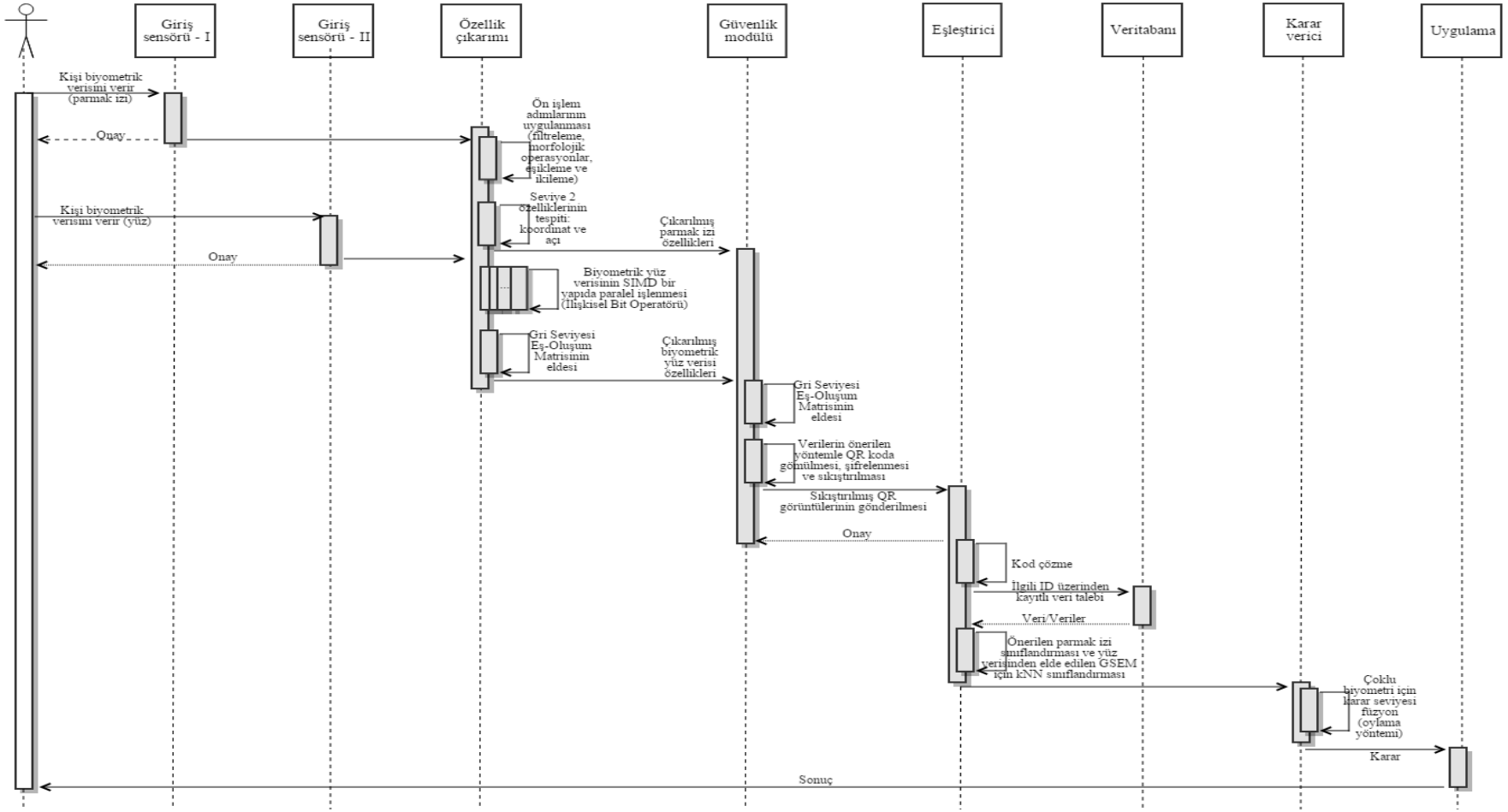
3.3. Yazılım Mühendisliği Açısından Sistem Modelleme

Donanım üzerinde koşacak olan bir algoritmanın yazılım ile gerçeklenecektir. Bu sebeple yazılım mühendisliği temellerinden faydalanarak tasarım yapmak sistemlerin ileride meydana gelecek değişikliklere daha iyi cevap vermesi ve sistemin bakımı açısından oldukça önemlidir. Bu kısımda önerilen sistemin yazılım ile oluşturulurken faydalanılan UML sıralama diyagramından ve geliştirme ortamı detaylarından bahsedilecektir.

Geliştirme ortamı üzerinde Python programlama dilinin sağlamış olduğu avantajdan faydalanarak "*multiprocessing*" kütüphanesi ile teorik olarak açıklanan yaklaşımları uygulamaya dönüştürmek mümkün olmuştur. Bu açıdan Python dili sağladığı dinamik programlama avantajının yanı sıra OpenCV'nin de bir arada kullanılabilirliği dolayısı ile kullanışlı bir geliştirme ortamı sağlanabilmiştir.

3.3.1. UML sıralama diyagramı

Birleşik Modelleme Dili (*Unified Modelling Language-UML*) yazılımın daha anlaşılır ve sistemik olarak farklı tasarımcılar arasında modüler bir yapıda tasarımını kolaylaştıran yapıdır. Yapısal ve davranışsal UML gibi iki temel başlığa ayrılan bu modelleme ile bu tez çalışmasında sistemin davranışsal olarak olay/modül sıralamasına bağlı tasarım detaylarına değinilecektir. Önerilen sistemin sırası ile tüm çalışma detayları Şekil 3.19'de verilmiştir.



Şekil 3.19. Önerilen sistemin tümüyle UML sıralama diyagramı ile gösterimi

3.3.2. Geliştirme ortamı: MatLab ve Python detayları

Gerçekleme ortamının detayları hem algoritmanın geliştirildiği geliştirme ortamı hem de algoritmanın koştuğu donanım olarak sunulacaktır.

Donanım üzerinde kullanılabilirliği ve gömülü sistemlerle uyumu düşünüldüğünde Python geliştirme ortamı bilimsel çalışmalarda kullanılmaya son derece uygundur. Matlab ise yüksek seviyeli bir dil olarak pek çok mühendislik dalında kullanılan çok geniş kapsamlı bir mühendislik programıdır; yazılım ve sistem geliştirme ortamıdır.

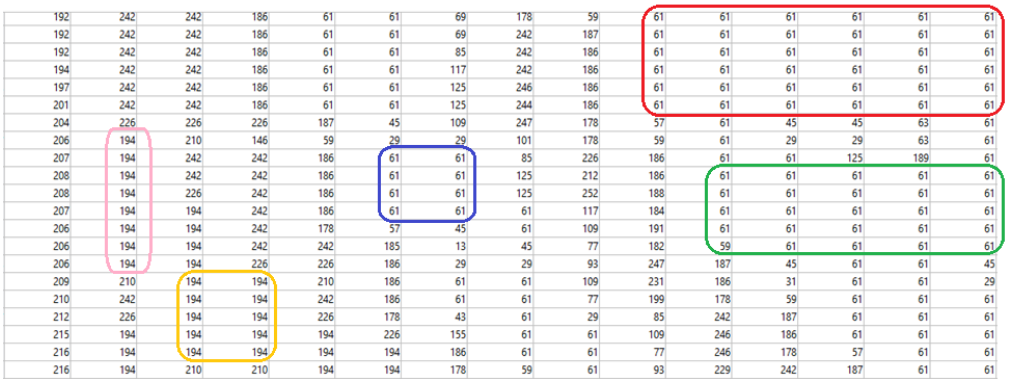
Parmak izi ve yüz tanıma için gerekli kodlar öncelikle Matlab'de yazılmıştır. Bunun sebebi performans açısından masaüstü bir bilgisayar kullanarak, Matlab gibi yüksek seviyeli bir dil kullanabilmek ve böylece algoritma geliştirme açısından daha elverişli bir çalışma ortamı elde etmektir. Ancak kodlar Python diline taşındığında elde edilen doğruluk oranlarına ilişkin sonuçlar neredeyse birbiri ile aynıdır. Böylece çapraz kontrol yapılması sağlanmıştır.

Sistemin tümüne ilişkin kodlama Python 2.7 ile Geany IDE kullanılarak yapılmıştır. Python programlama dilinin seçilmesinin önemli bir sebebi, hemen hemen her geliştirme ortamında yer bulmuş olmasıdır. Raspberry pi geliştirme kartından, Linux işletim sistemi bulunan bir mini bilgisayara kadar, Windows işletim sistemi de dâhil olmak üzere pek çok platformda çalışabilen bir gerçekleme ortamıdır. İşlemcilere dağıtılan (*broadcast*) veri Python'da *multiprocessing* ile kolaylıkla yapılabilmektedir. *Multiprocessing* esasen Python'da paralel hesaplama yapmaya yarayan özel bir pakettir. Programcının paralel çalışabilecek kodlar üretmesini sağlar. Hem Windows, hem Linux gibi farklı işletim sistemleri ortamında çalışabilmektedir. Verinin işlemcilere dağıtılması, işlemcilerin paralel çalıştırılması basitçe halledilir.

4. SİSTEM ANALİZİ VE BULGULAR

4.1. Sisteme Genel Bakış

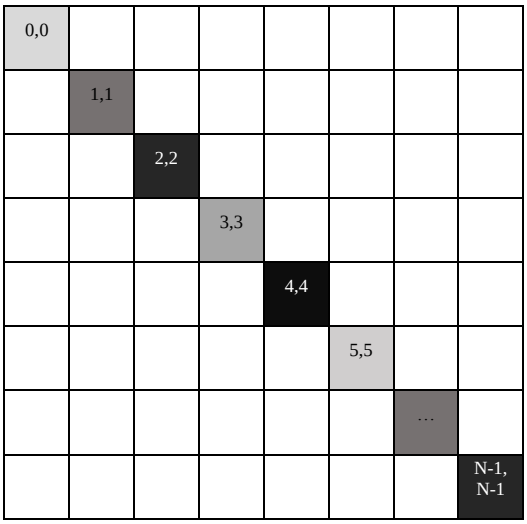
Bu bölümde sisteme genel bir bakış ve bu sırada elde edilen ara analizler sunulacaktır. Öncelikle, önerilen yöntem ile ilişkisel bit operatörü uygulanan bir yüz resmine ilişkin sonuçlar Şekil 4.1'de gösterilmektedir. Elde edilen görüntüsünün gri seviyesi değerlerine bakıldığında vurgulandığı üzere bazı değerlerde orijinal resmin gri seviye değerlerinden farklı olarak tekrarlar gözlenmiştir. Amaçlandığı gibi operatör bazı değerlerde belirginleşmektedir.



Şekil 4.1. İBO uygulanan bir biyometrik yüz resminin gri seviye değerlerinde oluşan tekrarlar

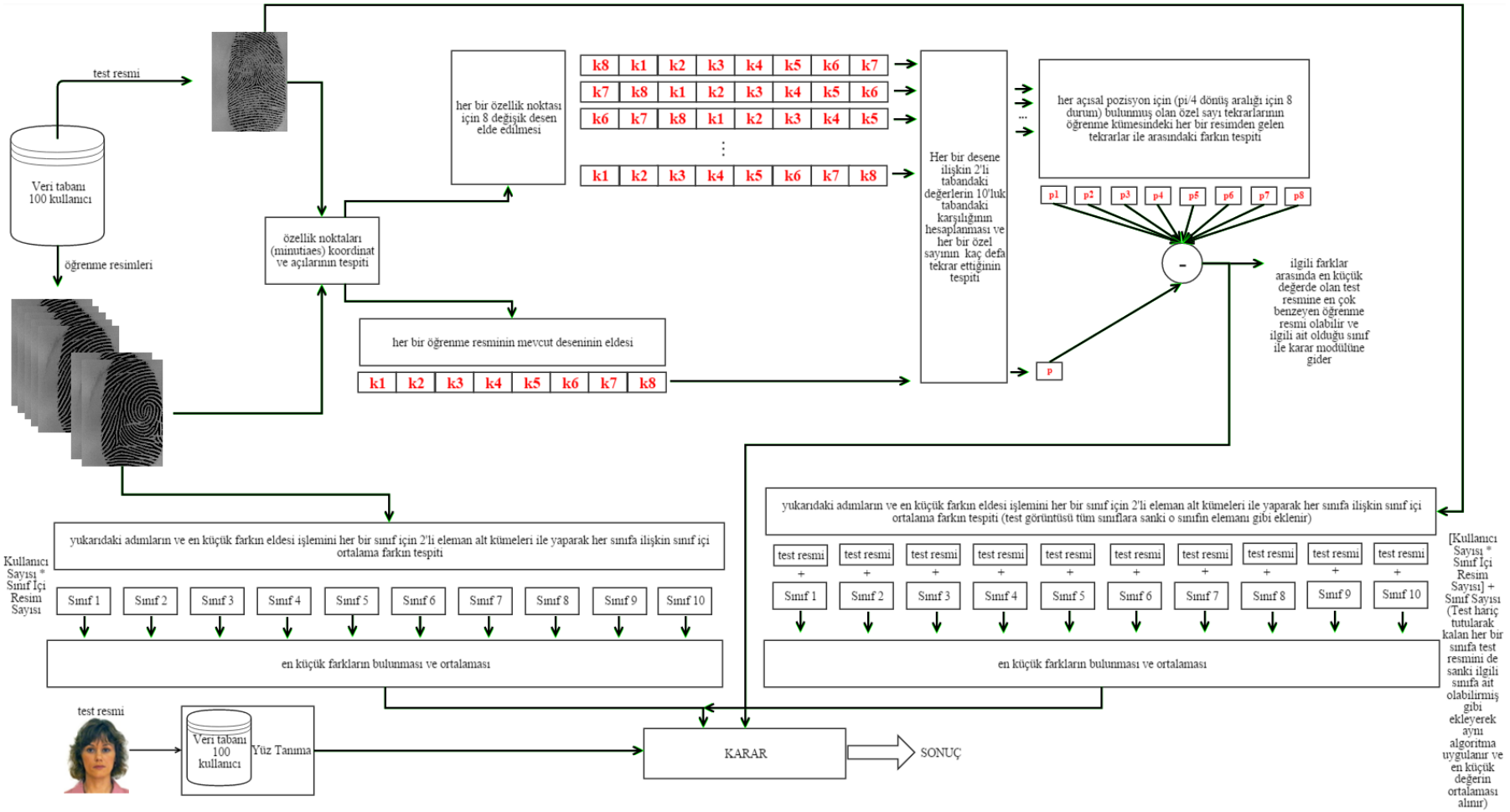
Operatör sonucu olan resimde elde edilen GSEM köşegen üzerindeki elemanlarda bir yığılma göstermektedir. Bu durum ardışık olarak gelen aynı gri seviyesi sayının İBO ile elde edilmesinden ileri gelmektedir. Sınıflandırma için standart yaklaşımlar literatürde GSEM'yi tümüyle kullanırken, İlişkisel Bit Operatörü sayesinde yalnızca köşegendeki elemanlar kullanılarak sınıflandırma yapılmaktadır. Gri seviyesi resim kullanılarak yapılan işlemler renk analizi vb. kullanmamakla birlikte n-bit gri seviyesi için $2^n = N$ adet gri seviye değeri sağlamaktadır. GSEM'yi matrisi NxN boyutundadır. Önerilen metot ile N katlık daha az veri kullanarak işlem gerçekleştirilmektedir. Bu durum, donanım üzerinde gerçeklenebilirlik açısından hem performans hem de hafıza için oldukça önemli bir durumdur.

$$NxN \rightarrow 2^n = N \tag{4.1}$$



Şekil 4.2. [0,N-1] arasında değişen gri seviyesi değerlerinin eş oluşum matrisi şablonu

Yüz tanıma için elde edilen gri seviyesi eş oluşum değerleri kNN sınıflandırıcı ile sınıflandırılmıştır. Öte yandan sistemin parmak izi sınıflandırmasına yönelik olarak gerekli açıklama da Şekil 4.3 üzerinde detaylıca yapılmaktadır.



Şekil 4.3. Sistemin tümüne ilişkin bir şema

Karar mekanizması sistemin sınıflandırmayı yapan son aşamasıdır. Bu modül farklı biyometrik verilerin füzyonu için kullanılmaktadır (karar seviyesi füzyon). Şekil 4.3'de gösterilen parmak izi sınıflandırmasına yönelik şemada karar modülüne gönderilen sonuçlardan biri ABPT yönteminden direkt gelen sonuçtur. Bu sonuç gelen test resmi ve veri tabanındaki diğer tüm verilerin arasındaki özellik sayısı farkına bakan ve ardından varyasyon en az olan sınıfa resmi gönderen sonuçtur. Veri tabanın da her kullanıcıya ait en az 2 resim bulunmalıdır. Buradan hareketle sınıf içi ABPT ile ortalama örüntü sayısı farkı bulunur ve gelen her test parmak izi resmi için, bu resim sanki o sınıfa aitmiş gibi tüm sınıflara ilave edip yeniden ABPT çalıştırarak yeni ortalama değerine bakılır. En az değişimi gösteren sınıfa gelen test verisi atılır ve ikinci kez sınıflandırılır. Burada söz edilen ortalama, sınıflandırma sırasında bir eşik değer olarak da kullanılabilir. Parmak izi dışında üçüncü bir karar parametresi füzyon için kullanılacak olan yüz sınıflandırma sonucudur. kNN sınıflandırıcının sonucuna göre gelen sonuç resmin ait olduğu kişinin sayaç değerini 1 arttırır. Parmak izi karar vericileri de dahil en az 2 karar verici tarafından oyalanan sınıf gelen kullanıcının ait olduğu sınıftır. Böylece oylama yöntemi ile karar seviyesi füzyon sağlanır.

4.2. Testler ve Analiz

Testler ve analiz için kullanılan yüz ve parmak izi veri tabanları çeşitli kaynaklardan toplanarak derlenmiştir. Yüz resimleri için kullanılan veri tabanı Stirling Üniversitesi'nde duygu analizi üzerine çalışan bir grubun oluşturduğu resimlerdir. Bu veri tabanı, incelenen pek çok veri seti içinde pasaport resimlerine en benzer özellik gösteren veri tabanıdır. Parmak izi için ise, parmak izi doğrulama yarışması kapsamında (*Fingerprint Verification Competition-FVC*) oluşturulmuş olan veri tabanı kullanılmıştır. FVC 2002 ve FVC 2004 veri tabanlarının kullanıldığı testlerde ayrıca SFinGe sentetik parmak üreteci ile elde edilen parmak izi verileri de kullanılmıştır. FVC veri tabanı da bu sentetik parmak izi verisine sahiptir [51] [52].

Çoklu biyometri kapsamında her bir yüz verisine atanmış olan parmak izleri mevcuttur. Önerilen parmak izi algoritması için her bir kullanıcıya ilişkin en az m=2 adet veri olmak zorundadır. Bu verilerin kayıt sırasında alındığı varsayılmaktadır. Sınıf içi parmak izi verileri farklı açılarda elde edilmiş olabilir. Yüz veri tabanı için her bir kişiden 1 pasaport formatında kayıt için veri alındığı varsayılmaktadır. Bu açıdan gerçek bir pasaport doğrulama sistemine uygun yaklaşım kullanılmıştır. Kayıt resmi, pasaport standartlarına uygun olan arka planı beyaz ve ölçü olarak belirli standartlara göre hazırlanmıştır. İlgili veri tabanı bu sebeple Adobe PhotoShop 2015 ile uygun hale getirilmiştir. Pasaport resmine dönüştürme işlemi usulüne uygun olarak, profesyonel bir fotoğrafçıdan da biyometrik resimler hakkında yardım alınarak yapılmıştır. Kullanılan ikinci yüz verisi herhangi bir işleme tabi tutulmamış arka planı farklı olan test resimdir. Bu test resminde yüz biraz eğri olabilir ve ışıklandırma da esas biyometrik resim (öğrenme kümesi) kadar kusursuz olmayabilir; tıpkı havalimanında yolculuk eden bir kişinin anlık çekilen bir resminde olabileceği gibi.

4.2.1. Test metodolojisi

Biyometrik sistem için uygulanacak olan test metodolojisi kullanılan uygulamaya bağlı olarak değişmektedir. Doğrulama veya tanımlama amacına göre oluşturulan test yaklaşımı da farklılık göstermektedir. Kaynak taraması kısmında verilen örneklerde ülke bazında kullanılan çoklu biyometrik pasaport örnekleri sunulmuştur. Burada 1:N ve 1:1 gibi iki temel aramadan söz edilmiştir. 1:N bir adet test verisinin veya uygulama alanında sistemden başarı ile onay almaya çalışan gelen verinin, N adet önceden kayıtlı veriler arasında tek tek aranması anlamına gelmektedir. Bu tez çalışmasında hem parmak izi, hem yüz için 1:N sınıflandırma yani tanımlama yapılmaktadır. Bunun için veri tabanında en az 2 parmak izi ve 1 yüz verisi her kullanıcı için kaydedilmiştir. 1 parmak izi ve 1 yüz görüntüsü de test edilmek üzere kullanılmaktadır. Her kullanıcı için saklanan en az iki parmak izi sayısı sınıflandırma sırasında önerilen yöntem sebebiyle gereklidir. 100 kişilik bir veri tabanında öğrenme kümesi en az için 200 parmak izi ve 100 yüz resmi

bulunmaktadır. Tanımlama için gelen 1 parmak izi ve 1 yüz verisi füzyon yöntemi ile bir araya getirilip karar verilmektedir.

4.2.2. Test sonuçları

Tasarlanan sistem doğruluk oranları açısından testlere tabi tutulmuştur. Bu testlerde m parametresi ile gösterilecek olan her kullanıcı için kayıtlı parmak izi resmi sayısı m=2'den 6'ya kadar değiştirilmiş ve test sonuçları kaydedilmiştir. Tekil olarak yalnızca yüz resimleri test edildiğinde başarı oranı %80 değerine kadar ulaşmaktadır. Yüz tanıma, sistemde parmak izi tanıma doğruluk oranından daha iyi sonuçlara sahiptir. Parmak izi tanıma ise değişen m değerlerine bağlı olarak farklı performans göstermektedir. Yüz tanıma için test ve öğrenme resimleri arası ışıklandırma/gölge farkı sınıflandırmayı etkilememiştir. Kullanılan gözlük, şaç modeli, kıyafet farkı, yüz ifadesi gibi değişkenlerden de genel olarak bağımsız çalışmaktadır. Ancak profile ilişkin duruş değiştiğinde yanlış sınıf ile sonuçlandırma eğilimi gözlenmiştir. Şekil 4.4'de bu duruma bir örnek sunulmaktadır. Soldaki ilk iki resim doğru sınıflandırılırken, sağdaki son iki resim yanlış sınıflandırılmıştır.

Şekil 4.4. Profilden görünüşün test sonuçlarına etkisi

Şekil 4.5'da ICAO standartlara uygun oluşturulan öğrenme kümesi gösterilmektedir. Şekil 4.6 ise test kümesini oluşturan resimleri göstermektir ve bu örnek grubu tümüyle doğru sınıflandırılmışlardır.

Şekil 4.5. ICAO standartlarına uyumlu hale getirilmiş öğrenme kümesinden bir örnek

Şekil 4.6. Test kümesine gönderilen bazı resimler

Çizelge 4.1'de parmak izine ilişkin sonuçlar sunulmaktadır. Çizelge 4.2'de ise parmak izi ve yüz biyometrik verilerinin birleşiminden elde edilen sonuçlar verilmektedir. Çoklu biyometrik veri kullanmak doğruluk oranlarında da bir artış göstermektedir.

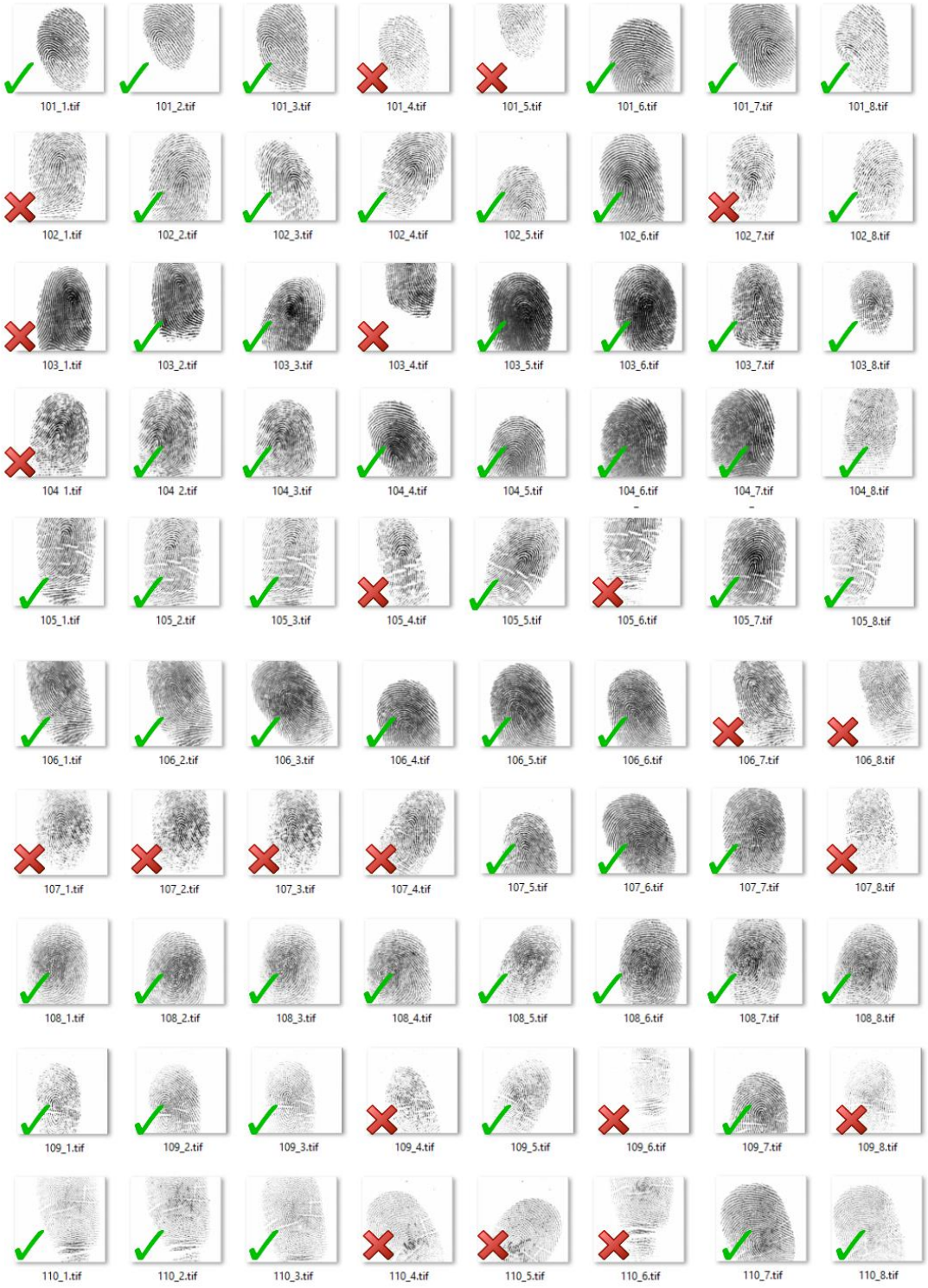
Çizelge 4.1. Her kullanıcı için değişken sayıdaki sınıf içi resim sayısına bağlı doğruluk oranları

Kullanıcıya Ait Parmak İzi Sınıfını Oluşturan Eleman Sayısı				
m=2	**m=3**	**m=4**	**m=5**	**m=6**
Doğruluk Oranları				
%74	%76	%77	%79	%82

Çizelge 4.2. Füzyon yapıldıktan sonraki test sonuçları

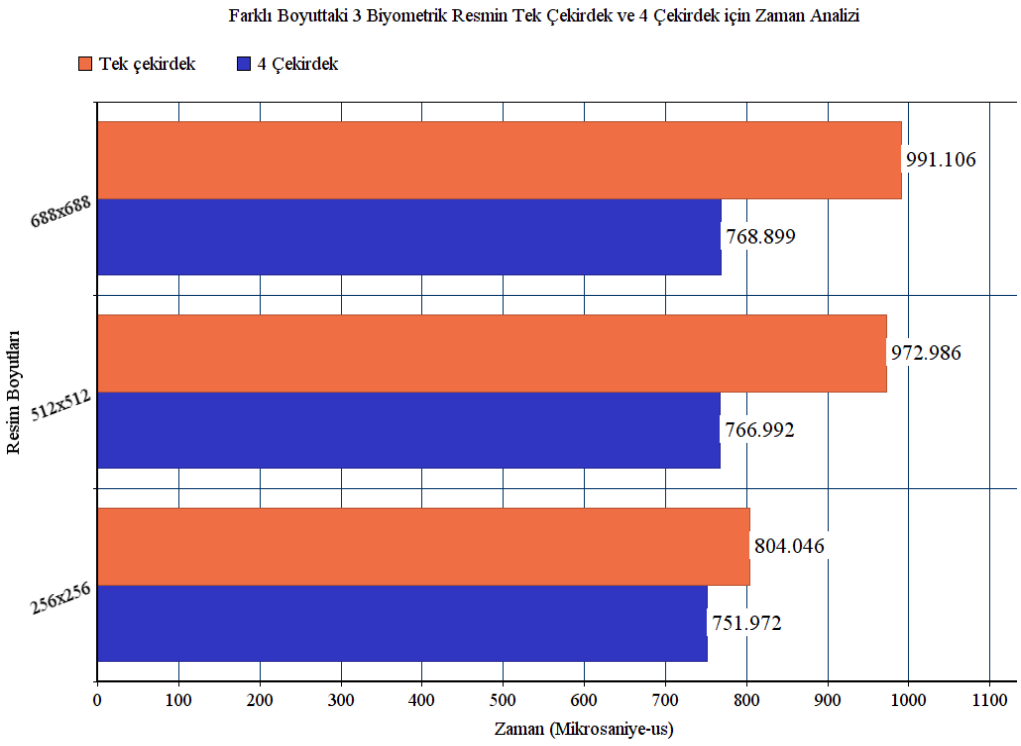
Kullanıcıya Ait Parmak İzi Sınıfını Oluşturan Eleman Sayısı ve Yüz Resmi				
m=2 + Yüz	**m=3 + Yüz**	**m=4 + Yüz**	**m=5 + Yüz**	**m=6 + Yüz**
Doğruluk Oranları				
%81	%82	%84	%84	%87

Şekil 4.7 FVC-DB1 veri tabanından bir kesit sunmaktadır. Sınıf içi 8 veri ile testler genişletildiğinde doğruluk oranı %72.5 olarak belirlenmiştir. Sınıf içi parmak izi resmi sayısı m=6'dan sonra daha kötü sonuçlar üretmeye başlamıştır. Şekil 4.7'de kırmızı çarpı ile gösterilen resimler sınıflandırılamayan veya doğru sınıflandırılamayan resimleri göstermektedir. Sonuçlara göre çıkarılan yorum, parmağın sensörde kapladığı alan ve uygulanan baskı miktarına göre sınıflandırma başarısı değişmektedir.



Şekil 4.7. Test edilen bazı parmak izi resimleri (FVC veri tabanı)

Öte yandan Şekil 4.8'da, bir resmin İBO operatörü ile özellik çıkarımı sırasında bu çalışmadaki paralel algoritma ile 4 çekirdeğe dağılımına ilişkin zaman analizi sunulmuştur. Burada tek çekirdekliye göre çekirdek sayısı arttıkça daha hızlı işlem zamanı elde edilmiştir. Değişik resim boyutları için yapılan testlerin sonuçlarının zaman performansı açısından iyileştirici ve yüksek başarımı destekler olduğu söylenebilir. Testler defalarca çalıştırılıp ortalama değerler elde edilmiştir. Şekil 4.9'a göre 4 çekirdeğe iş yükünü dağıtmak toplam süreyi 1/4'e indirmemektedir. Bu durum anlık işlemci yoğunluğuna ve görüntü işleme sırasındaki kullanılan matris yapısındaki veriye bağlıdır. Resmin piksel sayısı arttıkça elde edilen zaman performansı kazancı da artmaktadır. Gelecek çalışmalarda farklı testlerin yapılması planlanmaktadır.



Şekil 4.8. Tek ve çok çekirdekli mimaride 3 farklı boyuttaki görüntünün İBO için analizi

5. SONUÇ VE ÖNERİLER

Bu tez çalışması ile çoklu modda çalışan bir biyometrik sistem tasarımı tamamlanmıştır. Parmak izi ve yüz biyometrik verileri için özellik çıkarımı ve sınıflandırma yapılmakta, test sonuçlarına istinaden çoklu biyometri ile daha yüksek doğruluklu sonuçlar elde edilmektedir.

Önerilen sınıflandırma yaklaşımı gereği her bir kullanıcı için en az 2 parmak izi resmi kayıt sırasında alınmış olmalıdır. Bu kapsamda aynı veri üzerinden çoklu biyometrinin karar seviyesinde füzyonuna da örnek sunulmuştur. Her bir kullanıcı için kaydedilen parmak izi verisi optimum 4 olduğunda yüz biyometrik verileri ile birlikte %84 başarı göstererek kabul edilebilir bir sonuç sunmaktadır. Esasen en iyi doğruluk oranı %87 ile m=6 adet sınıf içi eleman olduğunda elde edilmiştir. Ancak her kullanıcıdan 6 defa veri taraması yapmak kullanışlı değildir. Yüz resimlerinin sınıflandırılması başın profilden görünüşü ile bozulmaktadır. Parmak izi sınıflandırılması ise görüntünün sensördeki miktarı az ise, gürültü varsa veya sensöre uygulanan baskı kötü ise özellik noktalarının (*minutiae*) kaybından ötürü sonuçlar daha kötü çıkmaktadır. Çünkü önerilen ABPT yöntemi parmakta bulunan özellik miktarı ile doğrudan ilişkilidir.

Öte yandan bu çalışma genel olarak çok çekirdekli donanımlar için görüntü işlemeye yönelik uygulamalarda yüksek başarım sağlamak amacıyla teorik bir yaklaşımı sunmak ve ilgili algoritmayı ortaya koymak üzere hazırlanmıştır. Çalışmanın teoriden uygulamaya geçirilmesi kısmı da donanım olarak kullanılan geliştirme ortamı üzerinde, Linux tabanlı bir işletim sistemi bulunan 4 çekirdekli bir bilgisayar ile sağlanmıştır. Sonuçlara göre resim boyutu arttıkça hızlanma miktarı da artmaktadır.

Biyometrik verilerin gizliliği de kare kod içine şifreli gömülüp parçalı olarak entropinin artırımı ile sağlanmaktadır. Gelecek çalışmalar, önerilen bu güvenlik algoritmasının kriptolojik analizi üzerine olacaktır. Her bir anahtarın farklı QR'a saklanması ve anahtarların da biyometrik verilere bağlı olarak dinamik pozisyon değiştirmesi öneriler arasındadır.

İkiden daha fazla biyometrik veri kullanarak sistem güvenliği ve çoklu biyometri yaklaşımı bu çalışma ile kıyas amacı ile yapılabilir. Örneğin, iris verisi kullanarak üçlü biyometrinin etkisi ölçülebilir.

Tez çalışmasının bir hedefi de önerilen algoritmaların gelecek çalışmalar kapsamında donanımda tasarlanabilir olmasıdır. Özellikle İBO ve ABPT yöntemleri ile bu önemli ölçüde sağlanmıştır. Karşılaştırıcı, kaymalı kaydediciler, toplayıcı, çoklayıcı vb. gibi temel lojik devre elemanları ile özellik çıkarımı, sınıflandırma vb. sağlanabilecektir. Bu durum temaslı / temassız akıllı kart tasarımı için oldukça önemli bir sonuçtur.

Bu tez çalışması gelecek çalışmalar kapsamında sensörden gerçek zamanlı veri alarak çalışabilir. Sistemin kurulu olduğu donanım, Arduino uyumlu bir parmak izi sensörü ile çalışabilir durumdadır. Biyometrik sistem tasarımı kapsamında ayrıca uygulama modülü görsel bir arayüz programı ile tasarlanabilir.

Sonuç olarak bu tez çalışması çoklu biyometrik sistem tasarımını tüm yönleri ile ele alıp başarı ile tamamlanmıştır.

KAYNAKLAR

[1] Anonim, *U.S. Department of Homeland Security*, 2015. http://www.dhs.gov/e-passports

[2] Anonim, *e-Pasaport Bilgi ve Randevu Merkezi* https://epasaport.egm.gov.tr/hakkinda/biyometrikfoto.aspx

[3] Vikipedi, *Biometric passport* https://en.wikipedia.org/wiki/Biometric_passport

[4] Mösenbacher, M., *Preventing fraud in ePassports and eIDs Security protocols for today and tomorrow*, *NXP,* 2013. http://www.nxp.com/documents/other/75017377.pdf

[5] NADRA, *Multi-Biometric e-Passport* https://www.nadra.gov.pk/index.php?option=com_content&view=article&id=42&Itemid=92

[6] Anonim, *The Netherlands plans UK supermarket chain trials biometrics*, Elsevier, 2004. http://ac.els-cdn.com/S0969476504001249/1-s2.0-S0969476504001249-main.pdf?_tid=05c8edae-cbe2-11e5-93a4-00000aacb35e&acdnat=1454660912_0a9d3074e841aa88ca4ecb55cf1a12fc

[7] Kuntman, H.H., Toker, A. ve Özcan, S., *Sayısal Elektronik Devreleri*. Sistem Yayıncılık A.Ş., İstanbul, Türkiye, 1996.

[8] Aygün, S. ve Akçay, M., "Matlab paralel hesaplama aracı ile A* algoritmasının rota planlama için analizi," *Genç Mühendisler Sempozyumu*, İstanbul, Mayıs, 2015.

[9] Ross, A., "An Introduction to multibiometrics," *15th European Signal Processing Conference (EUSIPCO)*, Polonya, Eylül, 2007.

[10] Telgad, R.L., Deshmukh, P.D. ve Siddiqui, A.M.N., "Combination approach

to score level fusion for multimodal biometric system by using face and fingerprint," *Int. Conf. Recent Adv. Innov. Eng. ICRAIE 2014*, 2014.

[11] Ali, A.S.O., Sagayan, V., Malik, A.S. ve Rasheed, W., "A combined face, fingerprint authentication system," *Proc. Int. Symp. Consum. Electron. ISCE*, 5–6, 2014.

[12] Nandakumar, K. ve Jain, A.K., "Multibiometric template security using fuzzy vault," *BTAS*, 2008.

[13] Wang, J., Li, Y., Liang, P., Zhang, G. ve Ao, X., "An effective multi-biometrics solution for embedded device," *Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern.*, Ekim, 917–922, 2009.

[14] Indra, *Mullti-biometric Case Study, NEUROtechnology*, 2010. http://www.neurotechnology.com/download/CaseStudy_Spain_Airports_Border_Control_System.pdf

[15] Juels, A., Molnar, D. ve Wagner, D., "Security and privacy issues in ePassports," *Secur. Priv. Emerg. Areas Commun. Networks, 2005.*, 74–88, 2005.

[16] Aygün, S. ve Akçay, M., "Yüz tanıma teknolojilerinde yüksek başarım için paralel hesaplama," *4. Ulusal Yüksek Başarımlı Hesaplama Konferansı*, ODTÜ, Ankara, Ekim, 2015.

[17] Prajapati, H.B. ve Vij, S.K., "Analytical study of parallel and distributed image processing," *2011 Int. Conf. Image Inf. Process.*, 1–6, 2011.

[18] P. Kaur, "Implementation of image processing algorithms on the parallel platform using Matlab," *Int. J. Comput. Sci. Eng. Technol.*, vol. 4, no: 06, pp. 696–706, 2013.

[19] Grama, A., Gupta, A., Karypis, G. ve Kumar, V., *Introduction to parallel computing*, Addison Wesley, 2003.

[20] Krishnakumar, Y., Prasad, T.D., Kumar, K.V.S., Raju, P. ve Kiranmai, B., "Realization of a parallel operating SIMD-MIMD architecture for image processing application," *2011 Int. Conf. Comput. Commun. Electr. Technol. ICCCET 2011*, 98–102, 2011.

[21] Barry, D., Cluff, R., Duncan, C. ve Kennedy, J.M., "High-performance parallel image processing using SIMD technology," *Proc. SPIE 3658, Medical Imaging 1999: Image Display*, 344–351, 1999.

[22] Bräunl, T., "Tutorial in data parallel image processing, " *Australian Journal of Intelligent Information Processing Systems (AJIIPS)*, vol. 6, pp. 164–174, 2001.

[23] Ercan, U., Akar, H., ve Koçer, A., "Paralel programlamada kullanılan temel algoritmalar", *Akademik Bilişim'13*, 23-25 Ocak, Antalya, Türkiye, 2013.

[24] Altıntaş, V. ve Yegenoğlu, V.D., "Görüntü işlemede seri ve paralel programlamanın performansı", *6th International Advanced Technologies Symposium (IATS'11)*, 16-18 Mayıs, Elazığ, Türkiye, 2011.

[25] Akgün, D., "Paralel görüntü filtreleme için çok çekirdekli bilgisayar üzerinde başarım analizi", *Journal of Advanced Technology Sciences*, vol. 2, no. 1, 76-83, 2013.

[26] Pande, V., Elleithy, K. ve Almazaydeh, L., "Parallel processing for multi face detection and recognition", *Conference: 5th International Conference on Computers and Their Applications in Industry and Engineering (CAINE-2012)*, New Orleans, Louisiana, A.B.D, 2012.

[27] Bhutekar, S.J., ve Manjaramkar A. K., "Parallel face Detection and Recognition on GPU", *International Journal of Computer Science and Information Technologies*, Vol. 5 (2) , 2014.

[28] Saxena, S., Sharma, N. ve Sharma, S., "Image processing tasks using parallel computing in multi core architecture and its applications in medical

imaging", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 4, Nisan, 2013.

[29] Chen, W.Y. ve Wang, J.W., "Nested image steganography scheme using QR-barcode technique," *Optical Engineering* vol. 48(5), Mayıs, 2009.

[30] Zigomitros, A. ve Patsakis, C., "Cross format embedding of metadata in images using QR codes," *Springer-Verlag*, 113–121, 2011.

[31] Chung, C.H., Chen, W.Y. ve Tu, C.M., "Image hidden technique using QR-barcode," *2009 Fifth Int. Conf. Intell. Inf. Hiding Multimed. Signal Process.*, 522–525, 2009.

[32] Chang, Y.Y., Yan, S.L., Lin, P.Z., Zhong, H.B., Marescaux, J., Su, J.L., Wang, M.L.ve Lee, P.Y., "A mobile medical QR-code authentication system and its automatic FICE image evaluation application," *J. Appl. Res. Technol.*, vol. 13, no. 2, 220–229, 2015.

[33] Maheswari, S.U. ve Hemanth, D.J., "Frequency domain QR code based image steganography using Fresnelet transform," *AEU - Int. J. Electron. Commun.*, vol. 69, no. 2, 539–544, 2015.

[34] Ramesh, M., Prabakaran, G. ve Bhavani, R., "QR- DWT code image steganography," *Int. J. Comput. Intell. Informatics*, vol. 3, no. 1, 9–13, 2013.

[35] Banirostam, H., Shamsinezhad, E. ve Banirostam, T., "Functional control of users by biometric behavior features in cloud computing," *Proc. - Int. Conf. Intell. Syst. Model. Simulation, ISMS*, 94–98, 2013.

[36] Soyjaudah, K.M.S., Ramsawock, G. ve Khodabacchus, M.Y., "Cloud computing authentication using cancellable biometrics," *IEEE AFRICON Conf.*, 2013.

[37] Jain, A.K., Ross, A. ve Nandakumar, S., *Introduction to Biometrics*. Springer, 2011.

[38] Anonim, *ISFO* http://www.isfo.org.tr/index.php?isfo=Pasaport&sayfa=CekimTeknik-Pasaport

[39] Özmen, G. ve Kandemir, R., "Haar dalgacıkları ve kübik bezier eğrileri İle yüz ifadesi tespiti," *ELECO 2012*, Bursa, 529–533, 2012.

[40] Anonim. *SFinGe Synthetic Fingerprint Generator* http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111%7C%7C12&

[41] Islam, W. ve Member, S., "A novel QR code guided image stenographic technique," *IEEE International Conference on Consumer Electronics (ICCE)*, no. 1, 586–587, 2013.

[42] Denso Wave, *Information capacity and versions of the QR code* http://www.qrcode.com/en/about/version.html

[43] Castellano, G., Bonilha, L., Li, L.M. ve Cendes F., "Texture analysis of medical images," *Clin. Radiol.*, vol. 59, no. 12, 1061–9, 2004.

[44] Güneş E.O., Aygün, S., Mürvet, K., Kalateh, A. ve Çakır, Y., "Determination of the varieties and characteristics of wheat seeds grown in Turkey using image processing techniques," *Agro-Geoinformatics*, Beijing, China, 2014.

[45] Clausi, D.A., "Texture segmentation of SAR sea ice imagery," *Methods*, vol. 37, no. 2, p. 176, 1996.

[46] Aygün, S., Akçay, M. ve Güneş, E.O., "Bulut sistemler için önerilen biyometri tabanlı güvenlik sistemine genel bakış," *The Third International Symposium on Digital Forensics and Security (ISDFS 2015)*, Ankara, May 2015.

[47] Arunkumar, L., "Biometrics authentication using Raspberry pi," *Int. J. Trends Eng. Technol.*, vol. 5, no. 2, 2349–9303, 2015.

[48] Ojala, T., Pietikäinen, M. ve Harwood, D., "A comparative study of texture measures with classification based on featured distributions," *Pattern Recognit.*, vol. 29, no. 1, pp. 51–59, 1996.

[49] Raphael, A.J. ve V., Sundaram, , "Cryptography and steganography – A survey," *Int. J. Comput. Technol. Appl.*, vol. 2, no. 3, 626–630, 2011.

[50] Aygün, S. ve Akçay, M., "Securing biometric face images via steganography for QR code" *ISCTurkey*, Ekim, Ankara 2015.

[51] University of Stirling, *Psychological Image Collection at Stirling (PICS)* http://pics.stir.ac.uk/2D_face_sets.htm

[52] Anonim. Fingerprint Verification Competition, 2004. http://bias.csr.unibo.it/fvc2004/download.asp

[53] Anonim. Fingerprint Verification Competition, 2002. http://bias.csr.unibo.it/fvc2002/download.asp

Ek: Kullanılan Yüz Verilerinden Örnek