



**TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ**



BİYOMETRİK KİMLİKLENDİRMEDE YÜZ TANIMANIN ADLİ BİLİŞİM SÜREÇLERİNE ETKİSİ VE ANALİZİ

Aqeel Shihab Ahmed JOLAQ

**DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ**

DANIŞMAN

Doç. Dr. Recep ERYİĞİT

ANKARA

2023

**TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ**

**BİYOMETRİK KİMLİKLENDİRMEDE YÜZ TANIMANIN
ADLİ BİLİŞİM SÜREÇLERİNE ETKİSİ VE ANALİZİ**

Aqeel Shihab Ahmed JOLAQ

**DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
YÜKSEK LİSANS TEZİ**

**DANIŞMAN
Doç. Dr. Recep ERYİĞİT**

**ANKARA
2023**

ETİK BEYAN

Ankara Üniversitesi

Adli Bilimler Enstitüsü Müdürlüğü'ne,

Yüksek Lisans tezi olarak hazırlayıp sunduğum “Biyometrik Kimliklendirmede Yüz Tanımanın Adli Bilişim Süreçlerine Etkisi ve Analizi” başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Aqeel Shihab Ahmed JOLAQ

Tarih: 25.01.2023

İmza:

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Disiplinlerarası Adli Bilimler Anabilim Dalı
Adli Bilişim İkinci Öğretim Tezli Yüksek Lisans Programında

Aqeel Shihab Ahmed JOLAQ tarafından hazırlanan

“Biyometrik Kimliklendirmede Yüz Tanımanın Adli Bilişim Süreçlerine Etkisi ve Analizi”

adlı tez çalışması

aşağıdaki jüri tarafından **YÜKSEK LİSANS TEZİ** olarak

OY BİRLİĞİ ile kabul edilmiştir.

25.01.2023

Prof. Dr. Fatih Vehbi ÇELEBİ

Ankara Yıldırım Beyazıt Üniversitesi Mühendislik ve Doğa Bilimleri Fakültesi

Jüri Başkanı

Doç. Dr. Recep ERYİĞİT

Dr. Öğr. Üyesi Bülent TUĞRUL

Ankara Ü. Mühendislik Fakültesi
Üye

Ankara Ü. Mühendislik Fakültesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

Prof. Dr. Fügen AKTAN

Sağlık Bilimleri Enstitüsü Müdürü

İÇİNDEKİLER

Etik Beyan	ii
Kabul ve Onay	iii
İçindekiler	iv
Önsöz	vii
Simgeler ve Kısaltmalar	viii
Şekiller	ix
Çizelgeler	xiii
1. GİRİŞ	1
1.1. Adli Bilişim	6
1.1.1. Sistematik Adli Bilişim Soruşturma Modelinin Aşamaları	14
1.1.1.1. Hazırlık Aşaması	14
1.1.1.2. Olay Yeri Güvenliğinin Sağlanması Aşaması	14
1.1.1.3. Delillerin Belirlenmesi / Tanımlanması Aşaması	15
1.1.1.4. Olay Yeri Belgelenmesi Aşaması	16
1.1.1.5. İletişim Koruması Aşaması	17
1.1.1.6. Kanıt Toplama Aşaması	17
1.1.1.6.1. Geçici Kanıt Toplama	18
1.1.1.6.2. Kalıcı Kanıt Toplama	18
1.1.1.7. Olay Yerindeki Delillerin Korunması Aşaması	19
1.1.1.8. Delil İnceleme Aşaması	20
1.1.1.9. Delil Analiz Yapma Aşaması	21
1.1.1.10. Delillerin Sunulması Aşaması	21
1.1.1.11. Sonuç ve Raporlama Aşaması	22
1.2. Biyometrik Kimliklendirme	24
1.2.1. Biyometrinin Fikir ve Tarihsel Gelişimi	25
1.2.2. Biyometrinin İşlevselliği	30
1.2.3. Biyometrinin Avantajları ve Dezavantajları	31
1.2.4. Biyometrik Sistemlerin Göstergeleri	32
1.2.5. Biyometrik Sistemlerin Tanımlayıcı Türleri	33

1.2.5.1. Biyometrinin Fizyolojik Türleri:	36
1.2.5.1.1. Parmak İzleri	36
1.2.5.1.2. Avuç İçi İzi	39
1.2.5.1.3. DNA Tanıma	41
1.2.5.1.4. Retina Tanıma	43
1.2.5.1.5. İris Tanıma	44
1.2.5.1.6. Yüz Tanıma	46
1.2.5.1.7. El Geometrisi	48
1.2.5.1.8. Parmak Damarı (Parmak Deseni)	50
1.2.5.2. Biyometrinin Davranışsal Türleri:	52
1.2.5.2.1. Ses Tanıma	52
1.2.5.2.2. Dudak Hareketi	54
1.2.5.2.3. El Yazısı (İmza Atımı)	57
1.2.5.2.4. Yazma Ritmi	58
1.2.5.2.5. Yürüyüş Tanıma	61
1.2.6. Biyometrik Tanıma Yöntemlerinin Karşılaştırma (Evrensellik, Eşsizlik, Süreklilik, Elde edilebilirlik, Performans; Kabul Edilebilirlik ve Yaygınlık).	62
2. GEREÇ ve YÖNTEM	65
2.1. Veri Seti Açıklaması	65
2.2. Veri Ön İşleme	67
2.3. Yüz Algılamada Kullanılan Kodlama Yöntemi	69
2.3.1. Referans Noktaları (Fiducial Points)	69
2.4. Yüz Tanımda Kullanılan Yöntemler ve Algoritmalar	72
2.4.1. Özellik Tabanlı Yüz Tanıma Sistemleri:	73
2.4.1.1. Yapısal Eşleme	73
2.4.1.2. Elastik Demet Grafi Eşleme	74
2.4.1.3. Gizli Markov Modeli	75
2.4.2. Görünüm Tabanlı Yüz Tanıma Sistemleri:	76
2.4.2.1. Temel Bileşen Analizi	76
2.4.2.2. Üç Boyutlu (3D) Yüz Tanıma Modelleri (3D Morphable Model)	78
2.4.3. Karma Yüz Tanıma Sistemleri	79
2.4.3.1. Aktif İstatistiksel Yüz Modelleri	79

2.4.3.2. Diğer Karma Yöntemler ve Çeşitli Kombinasyonlar.	80
2.5. Yapay Zeka ve Derin Öğrenme Algoritmaları	81
3. BULGULAR	85
3.1. Yüz Tanıma Sistemleri	85
3.1.1. Kriminal İnceleme Amaçlı Fotoğraftan Fotoğrafa Sorgulama Yöntemi	86
3.1.2. Kent Güvenlik Yönetim Sisteminde Kullanılan Canlı Yüz Tanıma Yöntemi	93
3.2. Gerçekleştirilen Testler ve Yapılan Analizler	95
3.2.1. Fotoğraftan Fotoğrafa Yapılan Sorgu Analizleri	95
3.2.2. Canlı Yüz Tanımadan Yapılan Sorgu Analizleri	119
3.3. Test Sonuçlarının Değerlendirilmesi ve Yorumlanması	122
4. TARTIŞMA	127
5. SONUÇ ve ÖNERİLER	133
ÖZET	136
SUMMARY	137
KAYNAKLAR	138

ÖNSÖZ

Biyometrik Kimliklendirme Sistemleri (BKS); kimlik doğrulamanın temel dayanağıdır. Her insanın fiziksel veya davranışsal özellikleri doğru bir şekilde tanımlanabilmesi gerekmektedir. Biyometri terimi, Antik Yunan'dan gelmektedir. Yunanca yaşam anlamına gelen bio, ölçmek anlamına gelen metric kelimelerinden türetilmiştir.

Biyometri, insanların benzersiz fiziksel (örneğin parmak izi, avuç içi izi, yüz tanıma gibi) ve davranışsal (el yazısı-imza atımı, yürüyüş, tuş vuruşu gibi) özelliklerinin ölçümü ve istatistiksel analizidir. Dolayısıyla biyometri, esas olarak kişileri tanımlamak veya doğrulamak için gelişmekte ve hâlihazırda kullanılmakta olan teknolojik bir sistemdir.

Gelişmiş teknolojilerde Biyometrik Sistemler, kişileri tanıma ve doğrulamak için günümüzde yaygın bir şekilde kullanılmaktadır. Yüz, kullanılan en temel biyometrik özelliklerden birtanesidir. Kişilerin yüz fotoğrafları sayesinde, bireylerin kimliği, cinsiyeti, yaşı, ırkı vb. nitelikleri hakkında elde edilen bilgiler aracılığı ile kişinin profilini ve kimliğini tespit etmek mümkün olacaktır.

Böylelikle olay yerinden elde edilen yüz görüntülerini hibrit algoritmalar sayesinde sayısallaştırıp, veri tabanındaki mevcut olan ve daha önceden sayısallaştırılmış yüz verileri ile karşılaştırma yaparak saniyeler içerisinde fotoğraf karesindeki kişilerin kim olduğunu belirlemek mümkün olabilmektedir.

Bu aşamada; tez çalışmamın planlanmasında, araştırılmasında, yürütülmesinde ve oluşturulmasının yanı sıra çalışmamı bilimsel temeller ışığında yöneterek şekillendiren ve tezimin gerçekleştirilmesinde her türlü katkı ve yardımda bulunarak çalışmalarım boyunca karşılaştığım bütün sorunlarda engin bilgi, birikim, tecrübe ve deneyimlerine başvurduğum, rehberliğinden yararlandığım danışmanım saygıdeğer hocam Sayın Doç. Dr. Recep ERYİĞİT'e,

Başta biricik oğlum Ali ve minicik kızım Zehra olmak üzere her zaman ve her anlamda maddi ve manevi açıdan yanımda olan ve bana her türlü imkân ve desteği sağlayıp sunan değerli aileme, sonsuz minnet duyacağımı ifade eder, en kalbi şükranlarımı sunar,

Bu araştırma ve çalışmamı vatanımız uğruna kahramanca savaşarak şehit olan bütün şehitlerimizin o kutsal ve aziz ruhlarına itfah eder, onları daima saygıyla, hasretle, rahmetle; minnetle kutsar, yar ederim.

Son olarak ülkemizin bilimin ışığında kalkınmasını, ülkemizde de uygarlık ve insanlık için gerekli bilimsel araştırmalar yapılmasının altyapısını sağlayan Başöğretmenimiz Ulu Önder Gazi Mustafa Kemal ATATÜRK'ü her zaman özlem ve minnetle yar eder, sevgi ve saygıyla anarım.

SİMGELER VE KISALTMALAR

SABSA	Sistematik Adli Bilişim Soruşturma Aşamaları
BK	Biyometrik Kimliklendirme
BKS	Biyometrik Kimliklendirme Sistemleri
BKY	Biyometrik Kimliklendirme Yöntemleri
BKYTS	Biyometrik Kimliklendirme Yüz Tanıma Sistemi
CCTV	Kapalı Devre Televizyon Sistemi
GPS	Küresel Konumlama Sistemleri
KGYS	Kent Güvenlik Yönetim Sistemi
OY	Olay Yeri
YT	Yüz Tanıma
YTS	Yüz Tanıma Sistemleri
APFIS	Otomatik Parmak ve Avuç İzi Tespit Sistemi

ŞEKİLLER

Şekil 1.1. Sistematik Adli Bilişim Soruşturma Modelinin (SABSM) Aşamaları	13
Şekil 1.2. Biyometri Yöntemlerini Seçerken İnsanların Tercihleri	31
Şekil 1.3. Biyometrik Kimlik Doğrulama Yöntemleri	34
Şekil 1.4. A) Farklı Parmak İzleri, B) Bir Örnek Parmak İzi Görüntüsü	37
Şekil 1.5. Avuç İzi Kategorisi	40
Şekil 1.6. Avuç İçi İzi 5. Kategori ve Bölünmesi	41
Şekil 1.7. DNA İkili Sarmal Yapısı	42
Şekil 1.8. Örnek İnsan Retina Şeması Temsili	43
Şekil 1.9. İris Örneği (Sol Üst Köşede İris Kodu Bulunan Bölünmüş İris Örneği)	44
Şekil 1.10. Yüz Tanıma Tekniği Örnekleri	47
Şekil 1.11. El Geometrisi Ölçüsü	49
Şekil 1.12. Tipik Bir El Geometrisinin Ölçülmesi	49
Şekil 1.13. Parmak Damarı Tanıma İçin Görüntü Örneği	50
Şekil 1.14. Ses Tanıma İçin Görüntü Örneği	52
Şekil 1.15. Ses Üretim Mekanizması	53
Şekil 1.16. Dudak Hareketleri Şeması Temsili	56
Şekil 1.17. Örnek İmza Görüntüsü	58
Şekil 1.18. A. Kayıt, B. Kimlik Doğrulama Akış Şeması	60
Şekil 1.19. Sağ Ayak Hareketine Dayalı İnsan Yürüyüş Döngüsü	61
Şekil 2.1. Temizleme İşlemi Uygulama Öncesi Görüntüler	68
Şekil 2.2. Temizleme İşlemi Uygulandıktan Sonraki Görüntüler	68
Şekil 2.3. Ön Profil Referans Nokta Lokasyonu	70

Şekil 2.4. Göz Bebeklerin Referans Nokta Lokasyonu	71
Şekil 2.5. Yüz Tanımada Kullanılan Çizgisel Kenar Haritası İllüstrasyonu	74
Şekil 2.6. Elastik Demet Grafi Eşleme Yöntemi	75
Şekil 2.7. Seri Haldeki Yüz Resimlerinin Modellendiği Gizli Markov Model İllüzyonu	76
Şekil 2.8. Mona Lisa'nın Yeniden Yapılandırılmış 3 Boyutlu Yüzü	79
Şekil 3.1. Papiyon Polyface Sistemin Giriş Ekran Görüntüsü	88
Şekil 3.2. Demografik Veri ve Fotoğraf Giriş Modül Ekranı	89
Şekil 3.3. Örnek Demografik Veri ve Fotoğraf Giriş Modül Ekranı	89
Şekil 3.4. Veri Görüntüleme Modülü	90
Şekil 3.5. A. Antropolojik Noktaların Kodlama Şablonu, B. Polyface Kodlama Modülü, C. Antropolojik Olarak Göz bebeklerin Sistem Tarafından Otomatik Kodlanması; D. Antropolojik Olarak Diğer Noktaların Sistem Tarafından Otomatik Kodlanması	91
Şekil 3.6. Sorgulama Modülü	92
Şekil: 3.7. Aday Listesi Kontrolü	92
Şekil 3.8. Sorgu Sonuçların Mukayesesi ve Kimlik Tespit Ekranı	93
Şekil 3.9. Canlı Yüz Tanıma Sistemleri Aracılığıyla Aranılan Kişilerin Tespiti	94
Şekil 3.10. Ön Profil – Ön Profil Sorgu Sonucu	97
Şekil 3.11. Ön Profil - 45 Derecelik Sol Açılış Sorgu Sonucu	97
Şekil 3.12. Ön Profil - 45 Dereceden Düşük Sol Açılış Sorgu Sonucu	98
Şekil 3.13. Ön Profil – 45 Derecelik Sağ Açılış Sorgu Sonucu	98
Şekil 3.14. Ön Profil - 45 Dereceden Düşük Sağ Açılış Sorgu Sonucu	99
Şekil 3.15. 45 Derecelik Sağ Açılış - 45 Derecelik Sol Açılış Sorgu Sonucu	100
Şekil 3.16. 45 Derecelik Sol Açılış - 45 Derecelik Sağ Açılış Sorgu Sonucu	100
Şekil 3.17. Ön Profil (Gözlüklü) - Ön Profil (Gözlüksüz) Sorgu Sonucu	101

Şekil 3.18. Ön Profil (Gözlüksüz) - Ön Profil (Gözlüklü) Sorgu Sonucu	102
Şekil 3.19. Ön Profil - 45 Derecelik Sol Aç (Gözlüklü) Sorgu Sonucu	102
Şekil 3.20. Ön Profil - 45 Derecelik Sağ Aç (Gözlüklü) Sorgu Sonucu	103
Şekil 3.21. Farklı Duygudurum Profili Sorgu Sonucu	104
Şekil 3.22. Ön Profil - Ön Profil (Karanlık Görüntülü) Sorgu Sonucu	104
Şekil 3.23. Farklı Yaş Profili Sorgu Sonucu	105
Şekil 3.24. Ön Profil (Sakalsız) – Ön Profil (Sakallı) Sorgu Sonucu	106
Şekil 3.25. Ön Profil – Ön Profil (Düşük Çözünürlüklü Görüntü) Sorgu Sonucu	106
Şekil 3.26. Ön Profil (Maskeli) – Ön Profil (Maskesiz) Sorgu Sonucu	107
Şekil 3.27. Ön Profil (Maskeli & Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Sonucu	108
Şekil 3.28. Ön Profil (Maskeli & Güneş Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Sonucu	108
Şekil 3.29. Ön Profil (Maskeli & Gözlüklü & Şapkalı) – Ön Profil (Maskesiz & Gözlüksüz & Şapkasız) Sorgu Sonucu	109
Şekil 3.30 Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Gözlüksüz & Şapkasız) Sorgu Sonucu	110
Şekil 3.31. 45 Derecelik Sağ Aç (Maskeli & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Şapkasız) Sorgu Sonucu	110
Şekil 3.32. Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Maskeli & Gözlüklü & Şapkasız) Sorgu Sonucu	111
Şekil 3.33. Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - 45 Derecelik Sağ Aç (Maskeli & Gözlüksüz & Şapkalı) Sorgu Sonucu	112
Şekil 3.34. Otomatik Kodlama Sorgu Sonuç Aday Listesi	113
Şekil 3.35. Otomatik Kodlamanın Sorgu Sonuç Görselleri	114
Şekil 3.36. Manuel Kodlama Sorgu Sonuç Aday Listesi	115
Şekil 3.37. Manuel Kodlamanın Sorgu Sonuç Görselleri	116

Şekil 3.38. Canlı Kameradan Alınan Anlık Yüz Algılanma Görüntüsü	120
Şekil 3.39. Tanımlama ve Tespit Görselleri	121
Şekil 3.40. Canlı Yüz Tanımada Yapılan Sorgu Sonuçları	122



ÇİZELGELER

Çizelge 1.1. Biyometrik Güvenlik Sistemlerinin Kullanılabilirlik Özelliklerine Göre Sınıflandırılması	63
Çizelge 3.1. Fotoğraftan Fotoğrafa Yapılan Sorgu Sonuçları	95
Çizelge 3.2. Otomatik Kodlama İşlemi ile Manuel Kodlama İşlemi Karşılaştırması	117



1. GİRİŞ

Adli Bilişim gerek Türkiye’de gerekse diğer dünya ülkeleri için gelişimini tamamlamış bir disiplin değildir. Ancak adaletin gerçekleşmesi amacına hizmet eden bu bilim dalı, teknik gelişmelere bağlı olarak kendini yenilemekte ve değişen ihtiyaçlara göre cevap aramaktadır.

Bu araştırma, Adli Bilişim disiplinine bir giriş sağlar. Onun için Biyometrik Kimliklerdirme Sistemleri (BKS); kişilerin artan sayıda ve türde suça karışması ile birlikte, işlenen suçlara yönelik Olay Yerinden (OY) toplanan verilerin incelenmesinde ve analiz edilmesinde, Adli Bilişim uzmanlarının hızlı ve doğru bir şekilde suçlunun kimliğini belirlemede yardımcı olacaktır. Nitekim Biyometrik Teknolojisi; adli uygulamalarda çağdaş gelişmelerle birlikte ortaya çıkan yeni teknolojik olanakların sağladığı görüntü kayıtlarının çözülmesi, teknik olarak suçun aydınlatılması ve suçlunun tespit edilmesinde önemli bir rol oynamaktadır.

Ayrıca geçmişte fiziksel araçlar ve yollarla işlenen suçlar dijitalleşmenin artmasıyla birlikte giderek yerini elektronik araçlarla işlenen suçlara bırakmaktadır. Dijital ortamda işlenen suçların başında, elektronik cihazlar gelmektedir. Bu cihazlar, masaüstü ve dizüstü bilgisayarlar olmak üzere tabletler, akıllı telefonlar, depolama cihazları gibi elektronik cihazları örnek göstermek mümkündür.

Dijital Deliller; pek çok tipte karşımıza çıkmaktadır, bunlar: dijital fotoğraflar, videolar, ses dosyaları, veri dosyaları, kurtarılmış ve silinmiş dosyalar, kayıp alanlardan

kurtarılmış veriler, sunucu kayıt dosyaları, e-posta, chat kayıtları, internet geçmişi, web sayfaları, log kayıtlar ve abone kayıtları vb. şeklinde sıralanması mümkündür.

Böylelikle dijital delillerin elde edilmesi ve analizi son derece önemli hale gelmiş ve klasik yöntemlerin yerine daha modern tekniklerin kullanım zorunluluğu doğmuştur. Gerek güvenliğin sağlanması için önleyici tedbirlerin alınmasında gerekse suçluların kimliklerinin tespit edilmesinde Biyometrik Sistemler kullanılmaya başlanmıştır.

Biyometri, insanların fiziksel ve davranışsal niteliklerini inceleme sonucunda bireyleri birbirinden ayıran bir bilim dalıdır. Biyometrik sistemler, insanların kimliklerini belirlemek için, biyometrik özelliklerinden yararlanılarak oluşturulmuş sistemlerdir. Dolayısı ile Yüz Tanıma (YT), biyometrik sistemlerden biridir. Bu sistemler, kişilerin kimliklerini tespit etmek için kullanılmaktadır. Bu yüzden, Yüz Tanıma Sistemlerinin (YTS) güvenlik açısından önemi son yıllarda giderek artmaktadır. YTS'leri örneğin adli ve kriminal vakalarda, pasaport kontrol noktalarında, güvenlik ve personel devam kontrolünde, Kent Güvenlik Yönetim Sisteminde (KGYS), çevrimiçi (online) sınavlarda yani bir başkasının yerine sınava girişin önlenmesi amacı ile kullanılmaktadır. Bu nedenle Biyometrik Yüz Tanıma Teknolojisi adli uygulamalarda önemli bir rol oynamaktadır.

Yüz özellikleri incelendiğinde, her bir yüz birçok farklı, ayırt edilebilir özellikler taşır. Nitekim yüz kendine has özelliklere, girinti ve çıkıntılara sahiptir. Yüz Tanıma Yazılımları bu noktaları düğüm noktaları olarak adlandırır. Bu düğüm noktalarına göre YT işlemi gerçekleştirilir. İnsan yüzünde yaklaşık 80 tane düğüm noktası vardır. Yazılımlar tarafından işlenen bu noktaların bazıları; gözlerin birbirine olan uzaklığı, burun genişliği, göz çukurunun derinliği, elmacık kemiğinin şekli ve çene kemiğinin uzunluğu gibi özellikleri sıralamak mümkündür.

Düğüm noktaları rakamsal bir değerle kodlanır ve bu kodlara yüz izi denir. Bu değerler yüz tanıma yazılımlarının veri tabanında saklanır. Geçmişte yüz tanıma yazılımları sadece 2 boyutlu görüntüleri karşılaştırma imkanına sahip iken, günümüzde yeni teknolojik yazılımlar sayesinde 3 boyutlu modeller kullanılmaktadır. Bu da sonuçların doğruluğunu attırmaktadır.

Bu çalışmada iki çeşit Yüz Tanıma Yöntemi ele alınmıştır. Birincisi; adli incelemelerde yüze dayalı Kimlik Tespiti (fotoğraftan - fotoğrafa sorgulama), ikincisi ise; kent güvenlik yönetim sisteminden (KGYS) canlı yüz tanıma yöntemidir.

Görsel bilgi, nitelik ve nicelikleri itibari ile somut bilgidir. Adli Bilimler alanında meydana gelen bir vakanın aydınlatılmasında fotoğrafik görsel bilginin kullanılması ve mahkemelere suçun ve suçlunun tespitine yönelik delil olarak sunulması çevirmen ve yorum gerektirmeyen bilgi varlığı olmasındaki özelliğinden kaynaklanmaktadır.

Yüz tanıma sistemleri, günümüzde yaşanan bilişim suçları, terör olayları, kara listeye dayalı güvenlik amaçlı kişi tespitleri, sınır güvenliği gibi olaylarda en sık kullanılan yöntemlerden biri olmuştur. Nitekim şahıs her yere parmak izini bırakıp gitmediği için ve teknoloji sayesinde pek çok yerde kameralar ve KGYS'leri halihazırda kullanıldığı için Yüz tanıma sistemleri bu gibi durumlarda en iyi alternatif çözüm olmaktadır.

Adli Bilişim Uzmanları, Biyometrik Yüz Tanıma Sistemlerini kullanarak OY'den elde edilen video kayıtlarını ve dijital fotoğrafları veritabanında kayıtlı milyonlarca yüz görüntüsü ile otomatik olarak 1:1 ve 1:N karşılaştırma yaparak, eşleşme durumunda saniyeler içerisinde suçlunun kimliğine ulaşılır.

En nihayetinde; Biyomektik Kimliklendirme Yüz Tanıma Sistemi (BKYTS) Adli Vakalarda, delil toplama sürecinde elde edilen veriler, biyometrik yöntemlerle analiz edilip, işlenen suçların çözümüne büyük ölçü de katkı sağlamaktadır. Bu nedenle adli bilişim sürecinde elde edilen deliller, biyometrik yöntemlerle incelenerek analiz işlemleri yapıp OY'den toplanan fotoğraf, video vb. materyaller hızlı ve doğru bir şekilde teşhis edilir. Dolayısıyla adli bilişim uzmanları, biyometrik yöntemlerle suçluya yönelik kimlik tespit etme olanağını sağlar. Biyometrik yöntemler kullanarak teknik açıdan suçun aydınlatılması, suçlunun kimliğinin tespit edilmesi, suçlunun bulunması, ve adaletin tecelli etmesine yardımcı olarak önemli bir rol oynamaktadır.

Bu bağlamda; tez çalışmamızın kapsamı, adli vakaların incelenmesinde yer alan Sistematik Adli Bilişim Soruşturma Aşamalarına (SABSA) doğrudan bir genel bakış sunmakla birlikte Biyometrik Kimliklendirme Yöntemlerine (BKY) değinilmiş olup her aşama kendi içerisinde kapsamlı bir biçimde ele alınmış ve biyometrik sistemlerin karşılaştırması yapılmıştır. Ayrıca çalışmamızın ana konusu olan Biyometrik Kimliklendirmede Yüz Tanımanın Adli Bilişim Süreçlerine Etkisi ve Analizi kapsamı doğrultusunda YT ile ilgili analiz ve testler laboratuvar ortamında yapılmış olup elde edilen sonuçlar bulgular bölümünde yorumlanarak değerlendirilmiştir.

Son olarak bu bölümde, araştırmamızın amacından bahsedecek olursak, yüz tanıma sistemleri, insanların yüz görsellerini, videolardan alınan görüntülerini ya da gerçek zamanlı CCTV kameralardan alınan görüntüleri analiz eden sistemler olarak tanımlamak mümkündür. Bu nedenle adli vakaların aydınlatılmasına yönelik olarak işlenen suçların yüz tanıma sistemleri aracılığıyla kimliği belirsiz kişi ve/veya kişilerin tespit edilmesi sağlanmaktadır. Bu işlem OY'den toplanan görsellerin veri tabanında kayıtlı olup kimlikleri belli olan bütün yüzlerle sorgulama ve karşılaştırılması yapılır, analiz sonucunda eşleşme durumu söz konusu olduğu takdirde suçlunun kimliği tespit edilmiş olur ve söz konusu olayın aydınlatılması gerçekleşir.

Yüz tanıma sistemleri, genellikle gözler, burun, ağız ve çene kenarlarındaki mesafeler de dahil olmak üzere bütün yüz yapısını ölçer. Bu ölçümler bir veritabanında saklanır ve kullanıcı kamera önüne geldiği zaman yapılacak karşılaştırmalar için kullanılır. Sonuç olarak; bütün bu bilgiler göz önüne alındığında dünyada ve ülkemizde, kurum ve kuruluşlar açısından yüz tanıma ve kimlik tespit sistemleri çok önemlidir.

Bu Yüksek Lisans tez çalışmasının amacı, yüz tanıma sistemleri kullanılan Kimlik Tespit Sistemi için etkili ve başarımlı oranı yüksek yeni yaklaşımları analiz etmektir. Bu amacı gerçekleştirmek için belirlenen hedefler;

- Literatür taramasının yapılması,
- Analiz için veri seti araştırılması,
- Veri seti açıklaması ve veri ön işleme,
- Görsellerin açısal yönden incelenmesi,
- Yazılım kullanarak veri setinin analizi,
- Yüz tanımada kullanılan kodlama yöntemleri,
- Analiz metodlarının karşılaştırılması ve başarısı yüksek olan metodun belirlenmesi,

Biyometrik Kimliklendirmede Yüz Tanımanın Adli Bilişim Süreçlerine Etkisi ve Analizi kapsamında yürüttüğümüz tez çalışmamızın amacı, yaşanan adli bilişim olaylar sonucunda OY'den elde edilen ve toplanan görsellerin, fotoğrafların yanı sıra videoların otomatik yüz tanıma sistemlerini kullanarak, bu sistemler aracılığıyla biyometrik kimliklendirme işlemi adli bilişim uzmanlarına nasıl bir fayda sağlayacağını, adli vakaların aydınlatılmasına yönelik olarak işlenen suçların yüz tanıma sistemleri sayesinde henüz kimliği belirlenmemiş olan kişi ve/veya kişilerin teknik açıdan

suçlunun kimliğinin hızlı, doğru ve kesin bir biçimde tespit edilmesini yapılan test ve analizler sonucunda gösterilmesi amaçlanmış, biyometrik kimliklendirmede yüz tanıma sistemlerinin önemine vurgu yapılmıştır.

1.1. Adli Bilişim

Bilgi teknolojisinin yaygınlaştığı bu çağda, Siber Suçların kurbanı olma ihtimalimiz de artmaktadır. Teknolojinin ve modern iletişim araçlarının yayılması ile birlikte bu araçlar dünya çapında iletişimi kolaylaştırmak için kullanılabilecek iki ucu keskin bir kılıç gibidir. Bu aynı zamanda, ülkeler ve farklı medeniyetler arasındaki mesafeleri yakınlaştırmak için farklı kültürlerin dünya üzerindeki en önemli aktarım aracıdır, ancak kişisel, siyasi veya maddi amaçlara hizmet etmek için belirli kişilere veya kurumlara ciddi zarar vermek için de kullanılabilirler (Başlar, 2019).

Son yıllarda dünya çapındaki toplumlar, bilgi toplumu olma yolunda muazzam ilerlemeler kaydetmektedirler. Bilgi ve iletişim teknolojisi, artık neredeyse yer yüzündeki insanların tüm yaşam alanlarına nüfuz etmiştir. Bu bilgilere ek olarak, bilgi ve iletişim teknolojisine artan merak ve beraberinde gelen bağımlılık, toplumları, veri ve bilgisayar sistemlerine karşı veya bunlar aracılığıyla işlenen siber suçlar gibi tehditlere karşı savunmasız hale getirmektedir. Bilgi ve iletişim teknolojisine karşı veya bilgi ve iletişim teknolojisi aracılığı ile işlenen çok sayıda suça müteakip olarak, bir bilgisayar sisteminde veya diğer elektronik cihazlarda saklanan Dijital Deliller ilgili mahkemelere kanıt olarak sunulabilir (Holtgrewe, 2014).

Ancak öte yandan insanoğlunun geliştirdiği her türlü araç, şu veya bu şekilde hukuka aykırı eylemlerin işlenmesinde de kullanılmaktadır. Bu bilgisayarlar için de geçerlidir. Bilgisayarlar, mali suçlar, bilgisayar dolandırıcılığı, casusluk ve sabotaj, veri

iletiřim ađı, terörizm, cinayet, uyuřturucu, cep telefonu dolandırıcılığı, çocuk pornografisi ve hemen hemen tüm diđer soruřturma sınıflandırmalarında kullanılmaktadır. Adli Bilgisayar inceleme süreci, bilgisayar güvenlik planlarının kırılması, hasarlı donanım yahut depolama ortamının onarımı veya deđiřtirilmesi, gizli veya bozuk verileri almak için karmařık veri kurtarma tekniklerinin kullanılması vb. gibi teknik olarak karmařık sorunlarla uđrařmayı ierir. Standart yazılım ve donanım cihazları, bir bilgisayar sistemini dođru bir řekilde analiz etmek için yetersiz kaldıđı durumlarda özel amalı cihazlara ihtiya olabilir (Henkođlu, 2020, s: 1-24).

Bilgisayarlar, dikkatli bir řekilde ele alınmasını gerektiren nispeten yeni bir kanıt türüdür. Verilerin küçük kısımlarının bile bozulması, delili kabul edilemez hale getirebilir. Adli Bilim Laboratuvarları, personelin, kanıtları ve bununla ilgili yasal kaygıları ele alma konusunda deneyimli olduđu bir ortam sađlar. Bu nedenle delil olarak ele geirilen bilgisayarların incelenmesi için adli laboratuvarlarda uzman kiřilerin geliřtirilmesi ve yetiřtirilmesi arzu edilir (Küme ve Ark., 2009).

Bilgisayar Suu, verilerin otomatik olarak iřlenmesini veya veri iletimini ieren her türlü yasa dıřı, etik olmayan veya yetkisiz davranıř olarak tanımlanmaktadır. Sular ve su iletiřimi günümüzde giderek daha fazla bilgisayar ve telekomünikasyona dayalı hale gelmekte bu da bilgisayar sularını artırmaktadır. Bilgisayar sularındaki artıřla birlikte, bilgisayarın delil olarak incelenmesi için hızla artan bir talep var. Çünkü Bilgisayar ve İnternet tabanlı sular, dünya apında ok sayıda insanı etkileyen küresel bir sorun haline gelmiřtir (Hatipođlu, 2017).

Yapılan pek ok anket arařtırması, birok bilgisayar suun rapor edilmediđini (bilgisayar sularının polis tarafından kayıt altına alınmadıđından deđil), řirketlerin mađdur olduklarını aıklamak konusunda isteksiz olduklarını ortaya koymaktadır.

Bunun da nedeni ise şirket sahiplerinin, şirketlerinin negatif tanıtımdan ya da olumsuz anlamda etkileneceğinden endişe duymaları, korkmalarından ileri gelmektedir. Onun için bu sayede de pek çok bilgisayar suçu ve dolandırıcılık tespit edilmiyor (CSO Online).

Bilgisayarların çoğalması, telekomünikasyonun yayılması ve internetin beraberinde getirdiği sözde bilgi ekonomisinin yükselişi, insanların iş yapma, yönetme, kendilerini eğlendirme, aile ve arkadaşlarla sohbet etme biçimlerini kökten değiştirdi. Bu da, çeşitli siber suç tehditlerine yol açmaktadır. Onun için tam bu noktada adli bilişiminin önemi ve gerekliliği öne çıkmaktadır (Doğanay, 2019).

Bu noktada adli bilişiminin, modern çalışmalarda öne çıkan bir araştırma konusu olmasının nedeni, önemli veri kaynakları genellikle üzerinde araştırma çalışmalarının yürütüldüğü cihazlarda bulunan bilgilerden oluşmaktadır (Hatipoğlu, 2017).

Günümüzde, kolluk kuvvetleri tarafından gerçekleştirilen soruşturmaların çoğu, Dijital Kanıt, yani bir dijital cihazda depolanan, cihaz tarafından iletilen veya cihazdan alınan ve araştırma değeri olan bilgi ve verileri içermektedir. Ancak bu bilgilere, verilere veya kanıtlara; OY'deki elektronik cihazlara el konulduğu zaman ulaşılır. 'Adli Bilişim' olarak adlandırılan bu alanda, sorgulama faaliyetinin karmaşıklığı ve yığın depolama cihazlarının artan kapasitesi nedeniyle, araştırmacılar büyük miktarda bilgiyi analiz etme sorunuyla karşı karşıya kalmakla birlikte araştırmalar için kullanılan dijital araçlar, merkezi bir endişe kaynağıdır (Taylor ve Ark., 2010).

Burada araştırma faaliyetlerinin kilit yönleri ise, mevcut verilerin toplanması ve analizidir. Bu bakış açısıyla Dijital Veri Analizi, işlenen suçların aydınlatılması açısından daha net bir vizyonunu tasvir etmede önemli bir rol oynar (Eriş, 2018).

Adli Bilişim, bilgisayarlarda, dijital cihazlarda veya diğer dijital depolama ortamlarında depolanan verilerin belirlenmesi, elde edilmesi, işlenmesi, analiz edilmesi ve raporlanmasına odaklanan bir bilim dalıdır (Henkoğlu, 2020, s: 17-38).

Araştırmalar için değerli verileri tutan bilgisayar, dijital cihaz veya diğer dijital depolama sistemleri elektronik delil olarak bilinir. Örneğin dizüstü bilgisayarlar, akıllı telefonlar, sunucular, dijital video kaydediciler, Kapalı Devre Televizyon Sistemleri (CCTV), dronlar, Küresel Konumlama Sistemleri (GPS) ve oyun konsolları vb. elektronik aletlerden ileri gelmektedir (Göksu, 2011).

Adli Bilişimin temel hedefi, elektronik delillerden veri çıkarmak, verileri yararlı bilgilere dönüştürmek ve bulguları kovuşturmaya sunmaktır. Bu nedenle, ilgili tüm süreçler, bulguların mahkemede kabul edilebilir olmasını sağlamak için sağlam adli tekniklerden yararlanmalıdır (Göksu, 2011).

Adli bilişim, bilgisayar ortamlarını (sabit diskler, disketler, teypler vb.) kanıt için metodik olarak inceleme sürecidir. Başka bir deyişle, adli bilişim, bilgisayarla ilgili kanıtların toplanması, korunması, analizi ve sunulmasıdır. Adli bilişim, adli bilişim analizi, elektronik keşif, elektronik kanıt keşfi, dijital keşif, veri kurtarma, veri keşfi, bilgisayar analizi ve bilgisayar incelemesi olarak da adlandırılır. Bilgisayar kanıtları ceza davalarında, hukuk uyuşmazlıklarında ve insan kaynakları/iş davalarında faydalı olabilir (Say, 2006).

Adli bilim, genel olarak, hukuk sistemini ilgilendiren soruları yanıtlamak için bilimin bir uygulaması olarak tanımlanır (Say, 2006). Tez çalışmamızın bu bölümü adli bilişim sürecini anlatmaktadır. Bu yüzden Adli Bilişim'de karşılaşılan tüm aşamalar (Delillerin toplanması, incelenmesi, analiz edilmesi; raporlanması vb.) kapsamlı bir biçimde ele alınmıştır (Göksu, 2011).

Netice itibarıyla Adli bilişim aslında, OY'den elde edilen dijital kanıtların toplanması, korunması, analizi, tanımlanması, doğrulanması, yorumlanması, belgelenmesi ve raporlanıp sunulmasına (işlem süreci şekil 1.1'de şematik olarak gösterilmiştir) yönelik bilimsel olarak türetilmiş ve kanıtlanmış yöntemlerin kullanımı sayesinde suç teşkil ettiği tespit edilen kanıtların teşhis edilmesine yardımcı olmak amacıyla olayların aydınlatılması için bilişim teknolojisinin resmileştirilmiş önemli bir bilim dalıdır. Dolayısıyla bu tanım, adli bilişimin ana görevlerini vurgulamaktadır. Genel olarak adli bilişim, bilginin bütünlüğünü korumakla beraber veriler için katı bir gözetim zinciri sürdürüp OY'den toplanan verilerin incelenmesi, tanımlanması ve analiz uygulamalarını kapsar. Bu yüzden de Adli bilişim, kanıt sağlamada çok kritik bir rol oynamaktadır (Arslan 2015).

Veri terimi, belirli bir şekilde biçimlendirilmiş farklı dijital bilgi parçalarını ifade eder. İletişim ve veri işleme yöntemlerine uygulanan teknolojik medyanın evrimi, içinde bulunduğumuz çağın temel özellikleridir. Bilgisayarlar artık hayatımızda yavaş yavaş temel ev eşyaları haline gelmektedir. Dolayısı ile son zamanlarda bilgisayarların, profesyonel ve kişisel kullanımının genişlemesi ve ağ oluşturma'nın yaygınlığı, birçok kaynaktan sürekli artan miktarda veriyi kaydedebilen ve analiz edebilen araçlara olan ihtiyacı da artırdı. Bu nedenle bilgisayarların günümüzde suç işlerinde kullanılması doğal bir sonuç olarak karşımıza çıkmaktadır. Zira standart bilgisayar sistemleri (örn. masaüstü bilgisayarlar, dizüstü bilgisayarlar, sunucular), ağ ekipmanı (örn. güvenlik duvarları, yönlendiriciler), bilgi işlem çevre birimleri (örn. yazıcılar), kişisel dijital

yardımcılar (PDA), CD'ler, DVD'ler, çıkarılabilir sabit sürücüler, yedekleme bantları, flash bellek gibi birçok tüketici elektronik cihaz (örneğin cep telefonları, video oyun konsolları, dijital müzik çalarlar, dijital video kaydediciler) verileri depolamak için kullanılabilir. Bu artan çeşitlilikteki veri kaynakları, olayları aydınlatmak üzere adli bilişimde kullanılan araç ve tekniklerinin geliştirilmesini ve de iyileştirilmesini teşvik etmiştir. Bu aynı zamanda bu tür araç ve tekniklerin, suçları araştırmak, bilgisayar güvenlik olaylarını yeniden yapılandırmak, operasyonel sorunları gidermek ve kaza sonucu oluşan sistem hasarlarını onarmak gibi birçok amaç için kullanılabileceği anlaşılmıştır (Kızmaz ve Küçükçolak, 2021).

Son on yılda, bilgisayarların dahil olduğu suçların sayısı giderek artmakta olduğu görülmektedir, bu da suçların kim, ne, nerede, ne zaman ve nasıl olduğu sorularına yanıt aramak için kolluk kuvvetlerine yardımcı olmayı amaçlar (Başlar, 2019).

Sonuç olarak adli bilişim, dijital delillerin ve verilerin ilgili mahkemelere uygun bir şekilde sunulmasını sağlamak üzere bir bilim dalıdır. Adli araçlar ve teknikler, genellikle şüpheli sistemleri araştırarak, kanıt toplayarak ve koruyarak, olayları yeniden yapılandırarak ve bir olayın mevcut durumunu değerlendirerek olaya dair yanıt bulmak üzere yürütülen adli soruşturmalar adli bilimle bir bütünleşik olarak düşünülür. Bununla birlikte, adli araçlar ve teknikler, diğer birçok görev türü için de yararlıdır. Örneğin operasyonel sorun gidermede, günlük izlemede, veri kurtarmada ve veri toplamada, durum tespiti gibi konularda adli bilişim araçlarını kullanır (Göksu, 2011).

Adli bilişim prosesi, OY'i inceleme temeline benzemektedir. Bu proses nihayetinde görünmeyen vasıfta olan elektronik kanıt, görünebilir ve anlaşılabilir duruma gelmektedir. Proses içerisinde bir elektronik kanıtın tahribata uğrayıp

uğramadığı veya sonradan değiştirilip değiştirilmediği de tespit edilmektedir (Göksu, 2011).

Adli bilişim, bilimsel yöntemler kullanılarak suçun aydınlatılabilmesi için farklı türdeki sayısal medyalar üstünde bulunan, suç ile alakalı dijital delillerin değişmeden, bozulmadan ve hasar görmeden anlaşılabilir bir biçimde adalete sunulmak üzere hazır durumuna getirilmesine zemin sağlayan ve bütün yönleri ile bilimsel teknik ilkelerin uygulandığı bir kanıt inceleme prosesinin tümüdür (Küme ve Ark., 2009).

1.1.1. Sistematik Adli Bilişim Soruşturma Modelinin Aşamaları

1.1.1.1. Hazırlık Aşaması

Hazırlık Aşaması, bu aşama gerçek araştırmadan önce gerçekleşir. Bu aşamada, işlenen suçun ve suç teşkil eden faaliyetlerin doğası hakkında bir ön bilgi edinmek, delil kaynaklarını paketlemek için OY’de biriken kanıt niteliği taşıyan materyalleri hazırlamada, toplamada vb. stratejilerin planlamasını içermektedir. Suç mahalline gitmeden önce suçla ilgili koşulların mümkün olan en iyi değerlendirmesini elde etmek çok önemlidir. Dijital cihazlarla ilgili soruşturmalardaki en kritik konu, delil toplama bitmeden elektronik cihazlardaki gücün bitmesidir. Soruşturmanın sağlıklı bir süreç içerisinde yürütülmesi açısından yasal olan gerekli tüm kısıtlamaların izni için ilgili mercilerden gerekli izinlerin alınması sağlanmalıdır. Bu yüzden bu aşama OY’e gitmeden önce arama izni, yönetimden destek ve gerekli diğer yasal bütün izinlerin alınmasının yanı sıra şüphelilerin de mahremiyet haklarını dikkate alınmasını kapsamaktadır. Ayrıca adli soruşturma hakkında bilgi veren tüm ilgili taraflara yasal uyarı sağlanmalıdır. Zira olayın doğası ve çeşitli teknik, yasal ve diğer faktörler dikkate alınarak uygun bir soruşturma stratejisi geliştirilmelidir. Nitekim kapsamlı bir hazırlık aşamasına sahip olmak, kanıt kalitesini artırır ve soruşturma ile ilişkili riskleri ve tehditleri en aza indirir. Ayrıca OY’i incelemelerinde kullanılan ekipmanların tam ve eksizlik olması durumunda olayın aydınlatılmasında oldukça önem arz etmektedir (Bucak, 2019 ve Özbek, 2013).

1.1.1.2. Olay Yeri Güvenliğinin Sağlanması Aşaması

Olay Yeri Güvenliğinin Sağlanması Aşaması, bu aşama öncelikle suç mahallinin hem yetkisiz erişime karşı korunması hem de delillerin kirlenmesine karşı muhafaza edilmesi ile ilgilidir. Gözaltı zincirinin gerektiği gibi takip edildiğinden emin olmak ve

suç mahallini ilgili merciler tarafından görevlendirilmiş olan yetkili kişilere teslim etmek için resmi bir protokol olmalıdır. Kanıtların gerçekte ne kadar suç mahallinde olduğuna dair karar vermek zor olsa da yetkilendirilmiş Olay Yeri Uzmanları, suçun kapsamını belirlemeli ve bir çevre oluşturmalıdır. Ayrıca OY'deki bütün kişilerin güvenliğinin sağlanması ve tüm delillerin bütünlüğünün korunması da bu aşamada hedef olmalıdır. Olay yeri uzmanları, olay yerinin mutlak kontrolüne sahip olmalı ve istenmeyen yetkisiz kişilerin olay yerine müdahalesine engel olmalıdır. Olay mahallindeki kişi sayısı arttıkça delillerin bulaşma riski ve yok edilme olasılıkları da artmaktadır. Bu aşamada kanıt yolsuzluğunun en aza indirilmesinde en yüksek öncelik verilmelidir. Kanıt olabilecek herhangi bir öge tahrif edilmemelidir. Bu aşama, kanıt kalitesini belirlediği için genel araştırma sürecinde önemli bir rol oynamaktadır (Agarwal ve ark., 2011).

1.1.1.3. Delillerin Belirlenmesi / Tanımlanması Aşaması

Delillerin Belirlenmesi Tanımlanması Aşaması; bu aşama, OY'ni değerlendirmek, potansiyel kanıt kaynaklarını belirlemek ve uygun bir arama planı formüle etmek için olay yeri uzmanları tarafından yürütülen ilk araştırmayı kapsar. Ancak bu her ne kadar basit gibi görünse de karmaşık bir ortamda basit olmayabilir. Örneğin Windows, mobil aygıtları söz konusu olduğunda, aygıtın kendisi dışındaki başlıca kanıt kaynakları, bilgisayar kasası, güç adaptörü, harici bellek kartları, kablolar ve diğer aksesuarlarda vb. cihazlarda bulunan bilgiler bilgisayarlarla kolaylıkla senkronize edilebildiği için OY'deki herhangi bir kişisel bilgisayar veya dizüstü bilgisayar da delil içerebilir. Ayrıca OY'nin işlenmesinde herhangi bir uzman yardımının gerekli olup olmadığını belirlemek için OY'deki elektronik ekipmanlar değerlendirilir. Bu bilgilere ek olarak OY'deki kişileri tespit etmek ve ön görüşmeleri yapmak son derece önemlidir. İşlenen suçun aydınlatılmasında OY'den toplanan elektronik cihazlar, cihazlarda bulunan çeşitli uygulamalar, kullanıcı adları ve şifreleri, şifreleme bilgileri, güvenlik şemaları, sistem yöneticileri vb. gibi değerli bilgileri yargı kanunlarına aykırı olmaksızın usulüne göre belirlenmesi ve tanımlanmasını yapar. Bu işlemlere müteakip olarak olay yeri

uzmanları olayla ilişkili, suç mahallinde bulunan farklı kişilerden maksimum bilgi elde etmeye çalışmalıdır. Ayrıca arama emrinde yer almayan maddelerin aranması gerekirse, mevcut arama emrinde uygun değişiklikler yapılmalı veya ek maddeleri içeren yeni bir arama emri çıkarılmalıdır. Son olarak araştırma ve tanıma aşamasının sonunda kanıt toplamak ve analiz etmek için uzmanlar tarafından bir başlangıç planı geliştirilmelidir (Elveren, 2018)

1.1.1.4. Olay Yeri Belgelenmesi Aşaması

Olay Yerinin Belgelenmesi Aşaması; bu aşama suç mahallini fotoğraflama, OY'nin kroki çizimi ve haritalanması ile birlikte OY'nin uygun şekilde belgelenmesini kapsar. OY'deki tüm elektronik cihazlar ve çevre birimleri ve diğer tüm aksesuarlarla birlikte OY'nin fotoğraflanması gerekir. Ayrıca dijital veya mobil cihazlar açık durumda ise ekranda görünenler de belgelenmelidir. Ek olarak sahne yeniden canlandırılmak ve gözden geçirilmek istendiğinde OY'de bulunan ve uzmanlara yardımcı olan tüm görünür verilerin bir kaydı oluşturulmalıdır. Nitekim bu, özellikle adli tıp uzmanının, soruşturmadan birkaç ay sonra olabilecek bir mahkemede ifade vermesi gerektiğinde önem arz etmektedir. Olayı ilk olarak kim hangi tarih ve saat diliminde bildiren dahil olmak üzere olayı çevreyelen koşul ve şartlarda dikkate alınmalıdır çünkü OY'de bulunanların, gelenlerin, gidenlerin vb. OY'deyken yaptıkları faaliyetlerin özeti ile birlikte kayıtlarının tutulması gerekir. Kişiler, mağdurlar, şüpheliler, görgü tanıkları, tanıklar, diğer yardımcı personeller vb. gibi ayrı gruplara ayırmak ve giriş anında konumlarını kaydetmek gerekir. Son olarak OY'ni belgelemek, soruşturmanın tüm aşamaları için önemlidir ve gerekli görüldüğü durumlarda OY'ni yeniden canlandırmak suçun aydınlatılmasında büyük rol oynamaktadır. Sonuç olarak uygun gözetim zincirini sürdürmek için olay yerinin belgelenmesi aşaması sürekli bir geri döngü faaliyetini içerdiğinden dolayı mutlak surette gereklidir (Crime Scene Investigator).

1.1.1.5. İletişim Koruması Aşaması

İletişim Koruması Aşaması, bu adım kanıt toplamadan önce gerçekleşir. İletişim koruması aşamasında, cihazların olası tüm iletişim seçenekleri engellenmelidir. Cihaz kapalı durumda görünse bile kablosuz veya Bluetooth gibi bazı iletişim özellikleri ile etkinleştirilebilir. Dolayısıyla bu, mevcut bilgilerin üzerine yazılmasına neden olabilir. Bu nedenle bu tür olasılıklardan kaçınılmalıdır. Ek olarak, cihazın bir bilgisayara bağlı kızıakta olduğu diğer durumlarda ise, ActiveSync kullanan senkronizasyon mekanizmaları etkinleştirilebilir bu da delillerin bozulmasına yol açabilir. Bu yüzden bir cihaz ele geçirildikten sonra en iyi seçenek, tüm iletişim yeteneklerini devre dışı bırakarak onu izole etmektir. Son olarak kanıtların sağlığı, güvenliği ve muhafaza edilmesi açısından aygıt yuvadaysa, onu bilgisayara bağlayan tüm USB veya seri kabloları devre dışı bırakılmalıdır (Agarwal ve Ark., 2011).

1.1.1.6. Kanıt Toplama Aşaması

Kanıt Toplama Aşaması; dijital veya mobil cihazlar gibi kanıtların toplanması önemli bir adımdır ve bunların çalışması için uygun bir prosedür veya kılavuz gerekir. Dijital cihazlar gibi kanıtların toplanmasını iki sınıflandırma kategorisine ayırabiliriz (Shinder ve Cross, 2008, s: 623-652). Bunlar;

- Geçici Kanıt Toplama
- Kalıcı Kanıt Toplama

1.1.1.6.1. Geçici Kanıt Toplama

Geçici Kanıt Toplama; kanıt niteliği taşıyan geçici verilerin çoğu, RAM'da mevcut olduğu için uçucu nitelikte olacaktır. Bu nedenle cihaz durumu ve bellek içeriği değişebileceğinden, geçici kanıt toplama her zaman sorun teşkil eder. Onun için uçucu nitelikteki verilerin suç mahallinde toplanması mümkün değilse şayet daha sonra güvenli bir yerde delillerin toplanıp toplanmayacağına karar vererek ve mevcut gücün yeterli olup olmadığını da hesaba katarak şayet cihazın pil gücü yetersizse tüm bu bilgiler kısa sürede kaybolacaktır. Dolayısıyla bu durumda mümkünse güç adaptörü kullanılarak veya değiştirilerek yeterli gücün sağlanması gerekir. Ancak pil gücünü korumak şüpheli görünüyorsa, belleğin içeriğini mümkün olan en kısa sürede uygun araçlar kullanılarak görüntülenmesi sağlanmalıdır. Daha sonra elverişli ve daha iyi sonuçlar elde etmek açısından uygun araç kombinasyonları kullanarak yeterli bir güç kaynağı sağlanmalıdır. Ayrıca kullanıcı tarafından yüklenen herhangi bir kötü amaçlı yazılımın varlığı da bu noktada kontrol edilmelidir. Sonuç olarak bu aşama da diğer bütün aşamalar gibi suçun aydınlatılmasında büyük öneme sahiptir (Daniel, 2011. s: 25-32 ve Liu, 2009, s: 305-389).

1.1.1.6.2. Kalıcı Kanıt Toplama

Kalıcı Kanıt Toplama; bu aşama elektronik cihazlar tarafından desteklenen hem harici hem de dahili depolama ortamlarından kanıt toplama işlemini amaçlar. Kalıcı kanıt toplama aşamasında MMC kartları (Multimedia Card), kompakt flaş (Compact Flash (CF)) kartları, bellek çubukları, güvenli dijital (SD) kartlar, USB gibi bellek çubukları vb. bu cihazlarla senkronize edilen bilgisayarlardan alınan kanıtlar toplanacaktır. Mahkeme tarafından kabul edilebilir kanıt toplamak için uygun adli araçlar kullanılmalıdır. Toplanan kanıtların bütünlüğü ve gerçekliği, hash değeri, yazma koruması vb. mekanizmalarla sağlanmalıdır. Nitekim suç mahallinde bulunan tüm güç kabloları, adaptörler ve diğer aksesuarlar da toplanarak aramaya özen gösterilmelidir.

Yazılı şifreler, donanım ve yazılım kılavuzları gibi elektronik olmayan nitelikteki kanıtlar ve ilgili belgeler, bilgisayar çıktıları vb. metaryellerinde toplanması gerekir. Ayrıca kanıtların bütünlüğünü sağlamak için OY’de bulunan fiziksel delillerinde var olabileceğini göz önünde bulundurarak (Örneğin parmak izleri) bu delillerin alınmasını da unutulmamalıdır (Okuyucu, 2020).

1.1.1.7. Olay Yerindeki Delillerin Korunması Aşaması

Olay Yerindeki Delillerin Korunması Aşaması; Bu aşama, OY’den toplanan delillerin muhafazası, paketlenmesini, nakliyesini ve depolama işlemini içerir. Toplanan elektronik kanıtların değiştirilmemesini veya yok edilmemesini sağlamak için uygun prosedürler izlenmeli ve belgelenmelidir. Paketlemeden önce tüm potansiyel kanıt kaynakları tanımlanmalı ve uygun şekilde etiketlenmelidir. Sıradan plastik torbaların kullanılması statik elektriğe neden olabilir. Bu nedenle, kanıtların anti-statik paketlenmesi esastır. Cihaz ve aksesuarlar, delil torbasına konulmadan önce bir zarfa konulmalı ve mühürlenmelidir. Kanıt torbaların, başka herhangi bir cihazla temas kurmamasını engellemek için bir radyo frekans izolasyon kabında tutulmalıdır. Bu kanıt torbalarını tutan tüm kaplar da uygun şekilde etiketlenmelidir. Kanıt kaynakları nakliye sırasında şok, aşırı basınç, nem, ısı veya sıcaklık nedeniyle kolayca zarar görebileceğinden yeterli önlemlerin alınması gereklidir. Daha sonra OY’den toplanan delil niteliğindeki kanıtlar, uygun bir gözetim zincirinin sağlanabileceği ve delillerin incelenmesi, analiz edilmesi ve işlenmesinin başlatılabileceği güvenli bir yere taşınarak korunması sağlanmalıdır. Kanıtlar sağlıklı bir yere taşınınca güvenli bir alanda saklanmalı ve elektromanyetik radyasyon, toz, ısı ve nemden korunmalıdır. Kanıtların tutulduğu yere yetkisiz kişiler depolama alanına girmemelidir. (Karakuş, 2018, Shinder ve Cross, 2008, s: 623-652).

1.1.1.8. Delil İnceleme Aşaması

Delil İnceleme Aşaması; Bu aşama, toplanan kanıtların içeriğinin adli bilişim uzmanları tarafından incelenmesini, davanın kanıtlanması ve olayın aydınlatılması için kritik olan bilgilerin çıkarılmasını içerir. İncelemeye geçmeden önce uygun sayıda kanıt yedeği oluşturulmalıdır. Bu aşama olayın gerçekliğini, delillerin orijinalliğini ve önemini açıklarken kanıtları görünür kılmayı amaçlar. Geçici ve kalıcı kanıt toplama aşamaları sırasında toplanan büyük hacimli verilerin, gelecekteki analizleri için yönetilebilir bir boyuta ve forma dönüştürülmesi gerekir. Veri filtreleme, doğrulama, örüntü eşleştirme ve suçun veya şüpheli olayın niteliğine göre belirli anahtar kelimelerin aranması, ilgili ASCII kodun yanı sıra ASCII kodu olmayan verilerin kurtarılması vb. bu aşamada gerçekleştirilen önemli adımların bir kısmıdır. Adres defteri, randevular, takvim, planlayıcı vb. gibi kişisel ajanda bilgileri, metin mesajları, sesli mesajlar, fotoğraflar, videolar, belgeler ve e-postalar ayrıntılı olarak incelenmesi gereken yaygın kanıt kaynaklarının bir diğer kısmıdır. Gizli veya gizlenmiş bilgileri tespit etmek ve kurtarmak her ne kadar meşakkatli bir iş olsa da bu verilerde olayın aydınlatılmasında genellikle hayati önem arz etmektedir. Parolaları kurtarmak, olağandışı gizli dosya veya dizinleri bulmak, dosya uzantısı ve imza uyumsuzlukları vb. için veriler kapsamlı bir şekilde araştırılmalıdır. İncelemeyi yapan kişi tarafından kullanılan Adli Bilişim araçlarının yetenekleri, inceleme aşamasında önemli bir rol oynar. Ayrıca kanıtlar inceleme için teslim alınırken ve check-in yapılırken tarih, saat, araştırmacının adı ve diğer ayrıntılar belgelenmelidir. Delillerin uzmanlar tarafından ele geçirildikten sonra değiştirilmediğinin kanıtlanması ve dolayısıyla verilerin matematiksel olarak doğrulanması için md5 şifreleme gibi karma tekniklerin kullanılması gerekir (Agarwal ve ark., 2011, Aydoğan, 2009).

1.1.1.9. Delil Analiz Yapma Aşaması

Delil Analiz Yapma Aşaması; bu aşama daha çok, araştırma ekibi tarafından kanıtların incelenmesinin sonuçlarına dayalı olarak yürütülen teknik bir incelemedir (Agarwal ve ark., 2011). Delil analiz yapma aşamasındaki temel faktör, analiz işleminin kriminal laboratuvarında adli bilişim yazılım ve donanımlarını kullanarak yürütülmesini esas almaktadır (Barbaros, 2016). Analiz sırasında her olayın önemine göre incelenecek olan veri parçaları arasındaki ilişkilerin belirlenmesi, gizli verilerin analiz edilmesi, inceleme aşamasından elde edilen bilgilerin öneminin belirlenmesi, olay verilerinin çıkartılan verilere dayanarak yeniden yapılandırılması, detaylandırılması ve uygun sonuçlara varılması vb. bu kapsamda yapılacak faaliyetler arasındadır. Ayrıca çıkarılan verilerin zaman çerçevesi analizini, gizli veri analizini, uygulama analizini ve dosya analizini içermektedir. Analiz aşamasının sonuçları, analiz süreçlerinde ek adımlara ihtiyaç olduğunu gösterebilir. Kanıt zincirinin ve olayların zaman çizelgesinin tutarlı olup olmadığı belirlenmelidir. Analiz için bir araç kombinasyonu kullanmak daha iyi sonuçlar verecektir. Analiz sonuçları eksiksiz ve doğru bir şekilde belgelendirilmelidir (Agarwal ve ark., 2011). Son olarak kanıt inceleme işlemi ve delil analiz faaliyetleri adli makamların arzu edeceği doğrultuda analiz işlemleri gerçekleştirilecektir (Oğuz, 2018).

1.1.1.10. Delillerin Sunulması Aşaması

Delillerin Sunulması Aşaması; bu aşamada toplanan kanıtların ayıklanması ve analiz edilmesinden sonra, sonuçların adli makam ve mahkemeler, kolluk kuvvetleri, teknik uzmanlar, hukuk uzmanları vb. dahil olmak üzere çok çeşitli kitlelere sunulması gerekebilir. Öncelikle olayın veya suçun niteliğine bağlı olarak, bulguların doğrulanması gerekir. Örneğin soruşturma türü bir polis soruşturması ise veya şirket içi bir soruşturma ise uzmanlarca OY'den toplanıp incelenerek analiz edilen kanıt ve deliller mahkemeye sunulur. Ancak bu aşamanın bir sonucu olarak, belirli suç veya şüpheli olayla ilgili şahısların, iddiaları teyit etmek veya reddetmek mümkün olmalıdır. Önceki aşamaların

her birinin bireysel sonuçları, suç hakkında uygun bir sonuca varmak için yeterli olmayabilir. Dolayısıyla tam bir resim elde etmek için inceleme ve analiz sonuçları bütünüyle gözden geçirilmelidir bunun için soruşturma sürecindeki çeşitli adımların ayrıntılı bir özetini ve ulaşılan sonuçları içeren bir rapor sunulmalıdır. Çoğu durumda, adli bilişim uzmanlarının mahkemede bilirkişi ifadesi vermesi gerekebilir. Ayrıca soruşturma sürecinin çeşitli aşamalarında yer alan teknik terimlerin ve mesleki terminolojilerin açık, anlaşılır ve net bir biçimde açıklanması gerekir. Adli bilişim denetçisinin uzmanlığı ve bilgisi, benimsenen metodoloji, kullanılan araç ve teknikler vb. gibi tüm hususlara mahkeme heyeti önünde itiraz edilmesi muhtemeldir. Bu yüzden raporla birlikte dijital delillerin kopyaları, gözetim zinciri belgesi, çeşitli delillerin çıktıları vb. destekleyici materyaller de dahil olmak üzere hepsi ilgili mercilere sunulmalıdır (Akarslan, 2011).

1.1.1.11. Sonuç ve Raporlama Aşaması

Sonuç ve Raporlama Aşaması; SABSM'deki son aşama olan gözden geçirme ve raporlama aşamasıdır. Bu aşamada delil niteliği olan kanıtların bilgilendirilmesi yapılır. Bu amaçla araştırmadaki tüm adımların gözden geçirilmesi, kanıt üzerinde yapılmış olan bütün işlemlerin yanı sıra olaya ilişkili yapılan analizler mutlaka raporlanmalıdır çünkü olayın aydınlatılmasında delil bütünlüğü oldukça önem teşkil eder. Ancak alternatif olarak bir olayın iki veya daha fazla açıklaması varsa, raporlama sürecinde her birine gereken önem verilmelidir. Analistler, önerilen her olası açıklamayı kanıtlamaya veya çürütmeye çalışmak için metodik bir yaklaşım kullanmalıdır (Okuyucu, 2020). Ayrıca raporlama aşamasının bir diğer parçası olan sonuç ve yorumlar da aynı şekilde olayın aydınlatılmasında büyük bir önem arz etmektedir. Zira titiz bir şekilde raporlanmamış bir adli vaka çalışmasından elverişli, yararlı ve de gerçek bir verime ulaşmak mümkün olmayabilir. Bu yüzden de çoğu durumda, bir olayın veya suçun bütüncül resmini elde etmek için çok fazla inceleme ve analiz aşaması tekrarı gerekir. İnceleme sürecinin net bir şekilde anlaşılması açısından gerekli görüldüğü hallerde bilirkişi raporu görsellerle

de desteklenebilir. Bu da raporu incelemek üzere olayla ilişkin karar verecek olan mercilerin işini kolaylaştıracaktır. (Eriş, 2018).

Son olarak olayla ilgili adli bilişim uzmanları tarafından yapılan çalışmalar sonucunda, ilgili makamlara sunulmak üzere bilirkişi aracılığıyla hazırlanan rapor içeriği kısa cümlelerin yanı sıra net ve anlaşılır ifadelerle yazılmalıdır, teknik bilgi ve kavramlar çok fazla kullanılmamalıdır. Yer verilen teknik terimler açıklamaları ile birlikte yazılmalıdır. Konunun bütünlüğü açısından rapor akışında, olayla ilişkili malumatlar (Örneğin araştırmanın ve incelemenin başlangıç ve bitiş tarihi, zaman dilimi gibi), OY'den toplanan yahut el konulan ve üzerinde inceleme ve analiz yapılan elektronik kanıtlara yönelik gerekli bilgiler, araştırmada kullanılan ekipmanlarla (Donanım ve yazılımlar gibi) ilgili bilgiler, araştırmaya dair takip edilen yol, kullanılan yöntem, izlenen taktikler, suçta kullanılan teknolojik imkanlar, toplanan kanıtlarla ilgili yapılan işlemler sırasıyla kapsamlı ve detaylı bir şekilde yazıldıktan ve gerekli mercilere sunulduktan sonra dijital delil inceleme aşaması tamamlanmış olacaktır. Ancak gerekli görüldüğü durumlara karşı dijital deliller olası yeni bir inceleme ve tekrar analiz aşaması için hazır vaziyette muhafaza edilerek saklanmalıdır (Düden, 2019, Kaya 2016, Ukşal, 2015).

Bu maksatla bu tez çalışmasının yapılış amacı günden güne oldukça zor bir hal alan adli bilişim aşamalarını BKY'leri ile bağlantılı bir şekilde sistematik bir süreç içerisinde yürütmek, sığ ve yetersiz kalan alanların iyileştirme noktalarının belirlenmesini sağlamak adına kapsamlı bir adli bilişim ve Biyometrik Kimliklendirme süreci tasarlamaktır.

1.2. Biyometrik Kimliklendirme

Biyometri kelimesi Yunanca'dan gelmektedir ve iki köke ayrılmaktadır. Dolayısı ile biyometri terimi, Yunanca yaşam anlamına gelen bio ve ölçmek anlamına gelen metric kelimelerinden türetilmiştir (Akkan, 2013). Biyometri kısaca; kişilerin biyolojik iz ve verilerini ölçmekte, istatistiksel olarak analiz etmektedir (Alharbi ve Alahrbi, 2020).

Biyometrik doğrulama ya da yalnızca biyometri, bireyin ileri sürdüğü kişi olduğunu doğrulama prosesidir. Kişinin kimliğinin doğrulanması üç şekilde yapılabilir, birincisi kişinin bildiği bir şey (şifre gibi), ikincisi kişinin sahip olduğu bir şey (anahtar, özel kart gibi) üçüncüsü ise; kişinin olduğu bir şey (parmak izi, avuç içi izi gibi) (Wikipedia).

Biyometri, bireylerin anatomik yönden eşsiz olmasına dayanır ve bireylerin biyometrik açıdan tanımlanması için kullanılır. Eşsiz fizyolojik özellikleri veya davranış özelliklerini kontrol ederek kişiyi tanımlayan otomatikleştirilmiş bir sistemdir (Wikipedia).

Dolayısıyla biyometri, akıllı teknoloji ve cihazlarda giderek daha fazla kullanılmaktadır. Çeşitli uygulamalarda farklı biyometrik özellikler bulunmaktadır. Biyometrik tanıma sistemleri, örneğin pasaport doğrulama, havaalanları, binalar, cep telefonları ve kimlik kartları gibi birçok alanda yaygın olarak kullanılmaktadır (Saday ve Akhan, 2003).

Son zamanlarda birçok alanda kullanılan güvenilir tanıma sistemlerine yönelik artan talep, biyometrik sistemlere daha fazla önem verilmesi gerektiğinin açık kanıtıdır.

Biyometrik sistemler, benzersiz ve kaybolmayan veya unutulamayan fizyolojik özelliklere (parmak izi, iris ve yüz tanıma, avuç içi izi gibi) veya davranışsal özelliklere (yürüyüş, imza ve yazma gibi) dayalı doğru otomatik kişisel tanıma araçlarını temsil eder. Ortak bir biyometrik tanıma sistemi, algılama, özellik çıkarma ve eşleştirme modüllerinden oluşup kimlik doğrulama ve tanımlama için biyometrik sistemler ile ilgili literatürde çeşitli açılardan incelenme mevcuttur (Koç, 2019).

Günümüzde yüz tanıma sistemleri, giderek daha popüler bir hale gelmiştir. Birkaç farklı alanda bu tür bir teknolojiye duyulan ihtiyaç, araştırmaları her yıl daha ileriye taşımaya devam ediyor. Yüz tanıma sistemleri, yaygın olarak kişi tanımlama amacı ile kolluk kuvvetleri tarafından kullanılmaktadır. Buna ek olarak, bilgisayarda oturum açmak gibi daha önemsiz görevler için evde de kullanılabilir. Örneğin sanal gerçeklik ve insan-robot etkileşiminde gelişen bazı eğlence uygulamaları da vardır, ancak bunlar şimdilik yaygın olmaktan uzaktır (Çoban ve Özyurt, 2022, Çetinkaya ve Akçay, 2012).

Sonuç olarak, son teknolojik gelişmeler, yüz tanımayı çok geçerli bir tanımlama ve doğrulama tekniği haline getirdi ve popüleritesinin arkasındaki sebeplerden biri, görüntü alımının müdahaleci olmayan doğasıdır. Yani kişi sürecin farkında bile olmadan kolayca fotoğrafı çekilip ardından bu yöntemler sayesinde sistemler aracılığı ile kişinin kimliğinin tespiti gerçekleşir (Temiz, 2022).

1.2.1. Biyometrinin Fikir ve Tarihsel Gelişimi

Biyometrinin ilk fikri yıllar önce ortaya çıkmıştır. Ancak ne zaman ve nerede ortaya çıktığını belirtmek zordur. Lakin insan vücudunun parçalarını kullanma fikirleri ve hatta bu fikirleri kullanma yolları tüm dünyada ortaya çıktığı görülmüştür. Biyometrinin ilk kanıtları, MÖ 29000'de mağara adamlarının çizimlerini imzalamak için

parmak izlerini kullandıkları görülmüştür. Ayrıca Babillilerde yaşadıkları dönemde, kil tablet şeklindeki ticari işlemleri imzalamak için her yöntemi kullanmışlardır.

Biyometrik kimlik doğrulama ilk olarak eski Mısır döneminde kullanılmaya başlanmıştır. Dolayısı ile yöneticilerden biri, Khufu'nun büyük piramidinin inşası sırasında, işçilere yiyecek sağlama sürecini sistemleştirmeye çalışmıştır. Bu sebeple çalışan işçilerle ilgili (isim-soyisim, yaş, çalıştığı birim ve pozisyonu, meslek vb.) bilgileri kayıt altına almıştır. Ancak yönetici, bir çok çalışan işçiden şüphelenerek kendisini aldattığını düşünmüş olup daha sonra işçilerin fiziksel ve davranışsal niteliklerini de kayıt altına almaya başlamıştır.

14. yüzyılda Çin'de biyometrik kimlik doğrulama, tüccarlar arasında oldukça popülermiş. O dönemlerde biyometri teknolojisinin oldukça basit olduğu ve çocukları diğerlerinden ayırt etmek için mürekkepli kağıt kullanarak avuç içi izi ve ayak izlerinin alınmasına izin verilmiştir. Ancak bu denli basitliğine rağmen biyometrik kimlik doğrulama yönteminin hala kullanımda olduğunu ve hatta en popüler olduğunu belirtmek ilginçtir.

1823 yılında Çek fizyolog ve biyolog Jaonnes Evangelista Purkinje, el ve ayaklardaki papiller çıkıntıları inceleyerek bilimsel çalışmasını yayınlamıştır. Nitekim parmak izi modellerini sınıflandırmaya çalışan ilk kişi olmuştur.

1858'de Hindistan'da bir İngiliz subayı olan William James Herschel, kimlik tespiti için parmak izlerini kullanan ilk Avrupalı bilim insanı olmuştur. Parmak izlerinin eşsiz olduğuna güvenen Herschel, belge imzalamak için kullanmıştır.

1870'li yılında antropolog Alphonse Bertillon hüküm giymiş suçluları belirlemenin yolunu ararken sadece el ve ayak izlerini değil, vücut hareketlerini ve vücuttaki her türlü izi de kullanmıştır. Bertillonage olarak bilinen bilim adamının fikirleri, Amerikan ve İngiliz polis güçleri tarafından benimsenerek popüler hale gelmiş ve şüpheli çemberini en aza indirmeye yardımcı olmuştur. En ilginç gerçek ise; günümüzde biyometrinin en popüler yolu olan parmak izleri Bertillon'un sistemine dahil edilmiş, ancak Bertillon bunu önemli görmemiştir.

1880'de Henry Fauld, Sir Charles Darwin'e parmak izlerini sınıflandırmak üzere sistemi açıklamaya çalıştığı bir mektup yazmış ve yardım istemiştir. Darwin, Fauld'a yardım edememiş, ancak mektubunu Sir Francis Galton'a iletmiştir. Faulds ve Galton arasında geçen yazışmalar çok yoğun olmamasına rağmen yine de çok benzer sınıflandırma sistemleri üretmişler. Faulds'un, suçluların kimliğinin belirlenmesinde parmak izlerinin anlamı üzerinde durulmasında ısrar eden ilk Avrupalı bilim adamı olduğu düşünülmektedir.

1892'de Sir Francis Galton, üç ana (döngüler, kıvrımlar, kemerler) parmak izi kalıbının tanımlamış ve “Parmak İzleri” kitabını yayınlamıştır. Sir Francis Galton, 10 parmağın hepsinden parmak izi alınması gerektiğini teklif eden ilk kişi olmuştur.

Mark Twain, eserlerinde biyometriyi kullanan ilk yazar olarak kabul edilir. “Pud'un Başlı Wilson'ın Taklidi”, hobisi parmak izi toplamak olan genç bir avukatın öyküsüdür. Çevresindeki insanlarla ilişkileri oldukça yoğun olmasına rağmen insanlar hobisini anlamamış onu eksantrik olarak görmüşler. Ancak genç avukatın bilgisi, haksız yere cinayetle suçlanan bir kişinin hayatını ve özgürlüğünü kurtarmaya yardımcı olmuştur. Böylece, biyometri giderek daha popüler hale gelmiştir.

1903 yılında ABD'de New York Eyalet Hapishanesinde, suçlular için sistematik parmak izi kullanmaya başlanmıştır. Bertillon sisteminin bazı kusurları, iki erkek, tek yumurta ikizi nedeniyle Bertillon sistemine göre aynı ölçülere sahip olma durumu ve bu durumun birbirinden ayırt edilemiyor olması gözlenmiştir.

1904 yılında Kansas ve St. Louis Polis Departmanları, 1905 yılında ABD Ordusu, 1906 yılında ABD Donanması ve 1908 yılında ABD Deniz Piyadeleri parmak izi kullanmaya başlamıştır.

1960'larda Otomatik parmak izi tanıma sistemi oluşturulmuştur. Bu da aynı zamanda yüz tanımanın başlangıç noktası olarak bilinmektedir. W. Bledsoe, yüz tanımanın babası olarak kabul edilmektedir. Hatta bir fotoğrafçıya kulak, göz, burun ve ağzı bulmakta ısrar eden ilk kişi olarak tarihe geçmiştir.

1965'ler otomatik imza tanıma araştırmasının başlangıcı olmuştur. 1969 yılında FBI (Federal Soruşturma Bürosu) tarafından parmak izi tanımlama süreci otomatikleştirilmeye çalışılmıştır.

1974 yılında ilk olarak elden geometri sistemi tanımlanmıştır. Böylece Stanford Araştırma Enstitüsü ve Ulusal Fizik Laboratuvarı bir imza tanıma üzerinde çalışmaya başlamıştır.

1980'lerde biyometri terimi (otomatik insan/kişi tanımlama yöntemlerini tanımlamak için) kullanılmaya başlanmıştır. Ayrıca 1980'lerin başlarında Goldstein, Harmon ve Lesk tarafından yüz tanıma fikri geliştirilmiştir. Yüz tanımayı

otomatikleştirmek için 21 spesifik sübjektif oluşturuu (saç rengi, dudak kalınlığı vb.) kullanmışlar. Ayrıca, Dr. Joseph Perkell tarafından konuşmanın davranışsal bileşenlerinin ilk modeli üretilip oluşturulmuş ve çalışmalarında röntgen kullanmıştır.

1983'te hem ABD Enerji Bakanlığı (Sandia Ulusal Laboratuvarı'nda) hem de Savunma Bakanlığı (Deniz Yüksek Lisans Okulu'nda) biyometriyi test etmeye başlamıştır.

1985'te ilk retina taraması yapılmış ve ABD Savunma Bakanlığı'nda (Deniz Yüksek Lisans Okulu'nda) güvenli erişim için kullanılmıştır.

1986 yılında ilk biyometrik derneğin temeli atılmış ve Uluslararası Biyometrik Derneği kurulmuştur.

1990 yılında iris tanıma teknolojisi Cambridge Üniversitesi'nden Daugman tarafından oluşturulmuştur.

1991 yılında Birleşik Krallık'ta Biyometrik Derneği kurulmuştur. 1992 yılında göç sisteminde ilk kez parmak izi kullanılmıştır. 1994 yılında ABD el geometrisine dayalı biniş sistemini kurulmuştur.

1997 yılında ilk Biyometrik Test Merkezi kurulmuştur. Son olarak 2002 yılında ilk biyometrik standartların kabulü gerçekleşmiştir (Filiz, 2012, Babich, 2012).

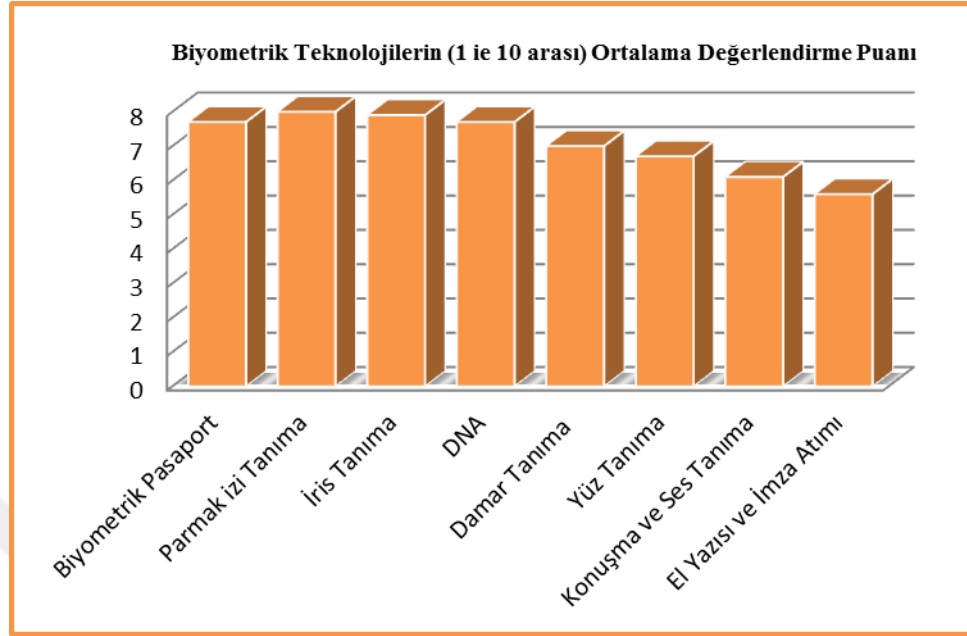
1.2.2. Biyometrinin İşlevselliği

Teknolojinin ilerlemesi neticesinde biyometrinin gelişmesi dolayısı ile güvenilirlik faktörü öncü bir faktördür. Onun için bütün biyometrik sistemler aşağıdaki özelliklere sahip olmalıdır. Bu özellikler;

1. Evrensellik: Her insanın sahip olması gereken bir biyometrik özelliktir.
2. Benzersizlik: Kişileri birbirinden ayıran bir biyometrik özelliktir.
3. Kalıcılık: Kişilerin biyometrik ölçüm ve özellikleri zaman içerisinde değişmemelidir.
4. Ölçülebilirlik (Toplanabilirlik): Kolay ölçümlü ve ekonomik olmalı, zaman alıcı olmamalı.
5. Performans: Biyometrik sistemlerin sağlam, hızlı ve doğru olmasıdır.
6. Elde edilebilirlik: Biyometrik özelliklerin teknolojik cihazlarla ölçülebilir ve kaydedilebilir olmasıdır.
7. Kabul edilebilirlik: Kişilerin biyometrik sistemlere karşı ne kadar güvendiğini tanımlamasıdır (Şan, 2013).

George Washington Üniversitesi öğrencileri, insanların biyometrik teknolojilere ve bunun farklı yöntemlerine karşı tutumları hakkında bir anket düzenlemişlerdir. Yapılan bu çalışmada ilginç olan şey, ankete katılan tüm insanların yarısından fazlasının (%77) biyometrinin kimlik doğrulama için oldukça yararlı bir araç olarak görmesi dikkat çekicidir. Ankete katılan katılımcıların %16'sı biyometrinin sunduğu bazı avantajları beğendiklerini söylerken, ankete katılanların sadece %7'si biyometriye karşı olduğunu belirtmiş (Babich, 2012).

Biyometrik yöntemlerle ilgili olarak, birinci sırada parmak izi tanıma, ikinci sırada ise iris tanıma yer almaktadır. Aşağıdaki Şekil 1.2'de, biyometri yöntemlerini seçerken sıradan insanların tercihlerini göstermektedir (Babich, 2012).



Şekil 1.2. Biyometri Yöntemlerini Seçerken İnsanların Tercihleri

1.2.3. Biyometrinin Avantajları ve Dezavantajları

Biyometrinin en büyük avantajı, gelişmiş güvenlik teknolojisine ve doğruluk oranının yüksek olmasına sahiptir. Kullanışlı olması, kopyalanamaz ve paylaşılamaz olması, unutulamaz veya kaybedilemez olması, düşük maliyetli olmasıdır (Babich, 2012).

Biyometrinin en büyük dezavantajları, kişisel mahremiyet ihlali, doğruluk oranının çok yüksek olmasına rağmen sistemden sisteme değişkenlik söz konusu olduğu için her sistem %100 kesin sonuç vermeyebilir, ölçeklenebilir veya toplanabilir olması, her hangi bir güvenlik ihlali söz konusu olduğu takdirde sıfırlanamaz olmasıdır (Babich, 2012).

1.2.4. Biyometrik Sistemlerin Göstergeleri

Biyometrik sistemlerin göstergeleri: Her biyometrik sistem, göstergelerine göre değişkenlik göstermektedir;

1. Geçiş kapasitesi: Bu her hangi bir kullanıcıya hizmet vermek için gereken süre ile karakterize edilir ve iş durumuna bağlıdır (kimlik doğrulama mı yoksa tanımlama işlemi mi yapılmak istenmektedir). Sistemin veritabanındaki tüm örnekleri karşılaştırması gerektiğinden, kimlik tanımlama kimlik doğrulamadan daha fazla zaman alacaktır. Kimlik doğrulamada, 1:1 karşılaştırma yapılırken, kimlik tanımada 1:N karşılaştırma yapılmaktadır.
2. Maliyet: Biyometrik sistemlerin en önemli parametrelerinden biridir.
3. Tanımlamanın güvenilirliği: Burada iki olasılık söz konusudur. Birinci olasılık; sistem kullanıcıyı tanımadığında “Yanlış Red Oranı” ikinci olasılık ise; sistem yanlış kişiyi kullanıcı olarak tanıdığına “Yanlış Kabul Oranı”. “Yanlış kabul” hatası güvenlik açısından “Yanlış ret”ten daha tehlikelidir, ancak “Yanlış ret” hatası, kullanıcıyı ilk andan itibaren tanımadığı için sistemi kullanmayı rahatsız eder. Bu iki olasılık birbiriyle bağlantılıdır ve birini en aza indirmeye çalışmak ikincisini artırır. Bu nedenle pratikte sistem uzlaşmaya varmalıdır. Sistemin görevi daha az yanlış insanları tanımak ve daha az doğru kullanıcıları reddetmek olduğundan, bu alan biyometrinin en zor olanıdır.
4. Kullanım Basitliği ve Rahatlığı: Bu parametreler sistemin ilgi çekiciliğini artırır.
5. Psikolojik Rahatlık Ölçeği: Değişik yöntem ve sistemlerin kullanıcı bakımından ne denli negatif tepki, şüphe veya korku yarattığını ifade eder.
6. Sistemle Oyun Oynama Yeteneği: Yayınlar, teyp kaydı, vb. gibi farklı “kopyaları” kullanma yeteneğini ifade eder. Burada en savunmasız sistemler olarak kabul edilenler: Ses tanıma ve yüz tanıma sistemleri.
7. Harmanlama Yöntemi: Burada iki yolu vardır; temaslı ve temassız. Yani kullanıcının parmak izi mi? Ses mi? Yoksa yüz tanıma mı? Kullanması

gerektiğini ifade eder. Ya da bu aşamada kişinin sadece özel bir cümle söylemesi veya kameraya bakması yeterli olacak mıdır sorusunu yanıtlar.

8. Kimlik Doğrulama Doğruluğu: Bu sistemden sisteme farklılık gösterir.
9. Verimlilik: Fiyat performansı, doğruluk oranı ve kullanım kolaylığı gibi parametrelerle ilişkilidir.
10. Entegrasyon: Birden fazla sistemin tek bir cihaza entegrasyonudur. Bu da sistemi daha nitelikli kılacaktır.
11. Gizlilik: Burada kullanıcılar tarafından endişe edilen en önemli faktörlerden birisi, kişisel mahremiyet ihlalinin söz konusu olup olmadığıdır. Yani biyometrik veriler, veritabanında (parmak izi, avuç içi izi vb.) resim olarak mı tutulmaktadır? Yoksa sayısallaştırılmış veri olarak mı? Saklanmaktadır sorusuna yanıt aranmaktadır (Babich, 2012).

1.2.5. Biyometrik Sistemlerin Tanımlayıcı Türleri

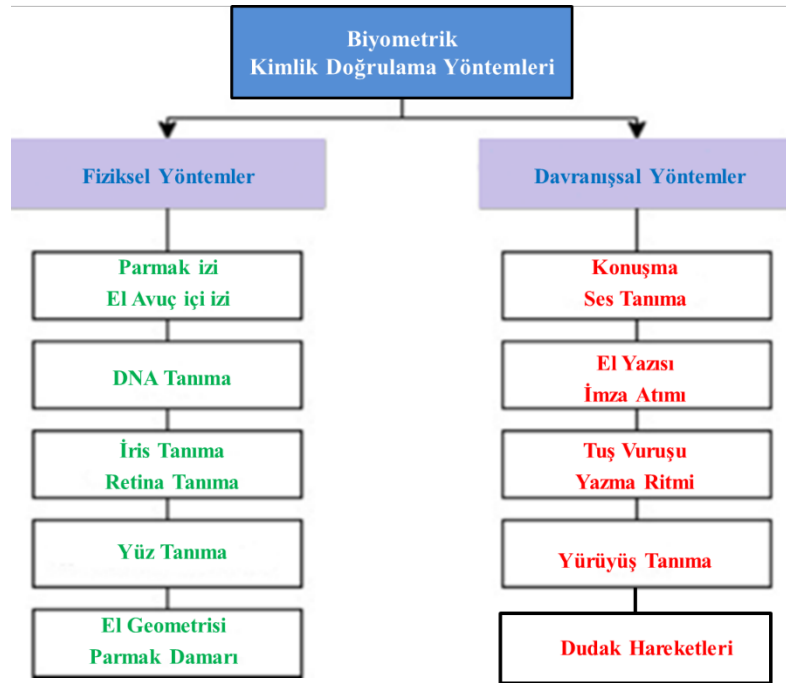
Biyometrik, bir bireyin fizyolojik (yüz, iris, parmak izi, el geometrisi, retina vb.) ve davranışsal (yürüyüş, ses, imza, tuş vuruşu vb.) özelliklerine göre sistemin bir bireyi benzersiz bir şekilde tanımlayabildiği bir bilimdir.

Dolayısıyla bir kişinin biyometrik özellikleri benzersizdir. Bu tür anahtarların neredeyse çoğunun kopyalanması ve tam olarak üretilmesi imkansızdır. Kuramsal olarak bunlar ideal anahtarlardır. Ancak biyometrik tanımlamanın kullanılmasıyla birçok spesifik problem ortaya çıkmaktadır (Alharbi ve Alahrbi, 2020).

Fizyolojik (yüz, iris vb.) ve davranışsal özelliklerin (ses, imza vb.) kullanıldığı biyometrik tabanlı kimlik doğrulama sistemleri giderek daha popüler hale gelmekte ve sistem güvenliğini artırmak için birçok uygulamada kullanılmaktadır. Geleneksel

sistemler, yetkili bir kişi ile sisteme hileli bir şekilde erişebilen davetsiz misafir arasında ayırım yapamaz. Biyometrik sistemlerin kullanımı daha uygundur çünkü herhangi bir şifreyi hatırlamaya gerek yoktur ve tek bir biyometrik özellik ile şifreleri hatırlama yükü olmadan farklı hesaplar güvence altına alınabilir. Biyometrik sistemler, geleneksel sistemlere göre büyük avantajlar sunar ancak saldırılara karşı savunmasızdır (Yalçın ve Gürbüz, 2015).

Dolayısıyla tüm biyometrik tanımlayıcılar iki büyük gruba ayrılabilir: Fizyolojik (İris Taraması, Parmak ve Avuç İçi İzleri, El/Parmak Geometrisi, Damar Görüntüleme, Yüz tanıma, Ses Kalıbı, Retina Taraması, DNA, Koku, Kulak memesi, Ter, Gözenek, Dudaklar) Davranışsal (İmza, Tuş vuruşu, Konuşma, Yürüyüş vb.). Aşağıda şekil 1.3'te, biyometrik kimlik doğrulama yöntemlerinin sınıflandırması şematik olarak sunulmuştur (Alharbi ve Alahrbi, 2020).



Şekil 1.3. Biyometrik Kimlik Doğrulama Yöntemleri

Davranış biyometrisi kullanıcı için daha az pahalı ve daha az tehlikeli olsa da, fizyolojik özellikler bir kişinin son derece kesin bir şekilde tanımlanmasını sağlar. Biyometrik yöntemler, geleneksel yöntemlerde kullanılan kart ve şifrelere göre daha yüksek seviyede doğrulama sağlamaktadır (Alharbi ve Alahrbi, 2020, Yalçın ve Gürbüz, 2015).

Kullanım alanları; biyometrik sistemler günümüzde pek çok alanda kullanılmaktadır. Bu alanlardan bazıları aşağıda belirtilmiştir.

1. Kriminalistikte, biyometrik tanımlayıcısı olarak, adli vakaların çözümünde yardımcı olup faillerin kimliklerinin tespit edilmesini sağlar, kimliği belirsiz cesetlerin belirlenmesinde,
2. Havalimanlarında mevcut olan E-gate sistemlerinde ve check-in ve boarding işlemlerinde,
3. İş yerlerinde, okullarda, giriş çıkış noktalarında, personel devam ve takip kontrollerinde,
4. Güvenlik sistemlerinde, yüksek güvenlik gerektiren yerlere giriş çıkış kontrolleri alanlarında,
5. Oylama sistemlerinde, oy kullanan kişilerin kimliklerinin doğrulanması işleminde,
6. Pasaport, ehliyet, yeni nesil kimlik kartlarında, biyometrik verilerin kaydedilmesinde,
7. Kent güvenlik yönetim sistemlerinde,
8. Sosyal yardım dağıtım organizasyonlarında,
9. Göçmenlerin ve yabancıların kayıt altına alınmasında,
10. İnternet bankacılık işlemlerinde kullanıcı tanımlanmasında ve online hesap açma işlemlerinde kullanılır (Şan, 2013).

Sonu olarak, biyometrik doęrulama yntemleri (DNA, İris tanıma, Parmak izi, Yüz tanıma, Ses, Yazma Ritmi vb.) güvenlik derecelerine gre farklılık gsterir.

1.2.5.1. Biyometrinin Fizyolojik Trleri:

Bir kişinin sistemler tarafından kullanılan bireysel ve fiziksel zellikleri psiko-duygusal durumun etkisiyle deęiřmedięi iin fizyolojik sistemler daha gereki olarak kabul edilmektedir. Biyometrik tanımlama sistemlerinin alt bařlıęı olarak bilinen fizyolojik tanımlama, bireylerin istatistiksel zellikleri ile ilgilenir. Bu fizyolojik trler, parmak ve avu ii izleri, DNS, iris ve yz tanıma gibi parametreler fizyolojik yntemlerden birkaçı olup ařaęıda en nemlileri kapsamlı bir řekilde anlatılmıřtır (Gmř ve Ark., 2018).

1.2.5.1.1. Parmak İzleri

Parmak izi, en eski biyometrik yntem olmasıyla birlikte kimlik doęrulamada nc bir metottur. Dolayısıyla bugn parmak izleri, dięer biyometrik teknolojiler arasında en eski ve popler olanlardan biri olarak kabul edilmektedir. Parmak izleri; 1896'dan beri zellikle su tespitinde kullanılmaktadır. Burada ana fikir, parmaęın bir tarafından dięerine akan izgi, benzeri ıkıntılarla oluklu cilde sahip parmak ularına dayanmaktadır. Bu sırtların akıřı srekli deęildir ve bir desen oluřturur. Akıř rnts, kemerler, ilmekler ve sarmallar gibi bir sınıflandırma dzenine yol aarken, sırt akıřındaki sreksizlik, ařaęıdaki (řekil 1.4'te) grldę gibi minutiae adı verilen zellik noktalarına yol aar (Arslan ve Saęıroęlu, 2016).



Şekil 1.4. A) Farklı Parmak İzleri, B) Bir Örnek Parmak İzi Görüntüsü

Parmak izi tanıma daktiloskopi olarak da bilinir veya elle tanımlama, insan parmaklarından, avuçlarından veya ayak parmaklarından alınan iki sürtünme çıkıntısı cilt izlenimi örneğini karşılaştırma işlemidir (Aygün, 2016).

Parmak izi alma yöntemi, güvenlik güçleri, kolluk kuvvetleri (Polis, Kriminal kurumlar vb.) gibi adli vakalarla ilgilenen kurum ve kuruluşlar açısından suçların araştırmasına ve aydınlatılmasına yardımcı olur. En şaşırtıcı gerçek, sadece parmak izleri kullanılarak bir kişi hakkında ne kadar çok detayın bilinebileceğidir (Aygün, 2016).

İnsan derisinin üç katmanı vardır: epidermis, dermis ve hipodermis. Dermis ayrıca iki katmana sahiptir: papiller ve ağsı katman. Papiller tabakada kendilerini papiller denilen çift piramidal oluşumlar halinde bulurlar. Her bir papiller çifti, ter bezlerinin kanallarıyla bölünmüştür. Bu tür çiftler bir sıra oluşturur ve epidermis tabakası ile kaplanır ve papiller çizgilerden oluşan bir tarak oluşturur. Papiller çizgiler düzensiz fakat akıntılar şeklinde yerleştirilmiştir. Üç akarsu birbirine yakın olduğunda delta denilen üçgen oluştururlar (Babich, 2012).

Papiller desenin (örüntü) esnek olduğundan kaynaklı, dünyada benzer iki desenin (örüntü) olmadığı anlamına gelmektedir. Her insanın kendine özgü papiller paterni vardır. Her papiller desenin kendine özgü yapı detayları vardır. Çizgilerin başlangıcı ve sonu, çizgilerin birleşmesi ve ayrılması, kıvrımlar ve kırılmalar, sırtlar, gözler ve kancalar, papiller çizgilerin kırılmaları ve başlangıç ve bitişlerinin yaklaşan yerleri gibi. Ayrıca benzersizliğin yanı sıra papiller patern stabildir. Yaş değişiklikleri papiller paterni etkilemez ve papiller paternin tüm yaşam dönemi boyunca sabit kaldığı kabul edilir (Babich, 2012).

Papiller patern yansıtılır. Kişi istese de istemese de her şeyde parmak izini bırakabilir. Bu, insan derisinin fizyolojik özelliği nedeniyle olur ayrıca insan cildi her zaman ter ve yağ salgılarıyla kaplıdır. Papiller örüntünün geri yükleme özelliği vardır. Parmağa çok zarar verilmemişse, papiller patern zaman içerisinde değişiklik olmaksızın tamamen eski haline döner (Babich, 2012).

Kriminalistikte parmak izi almanın yeri ayrı bir anlam ifade etmektedir. Parmak izleri bir kişinin masumiyetini kanıtlamak için suçlu olup olmadığı ispatlar. Yapılan araştırmalar ışığında, parmak izinin tek yumurta ikizleri de dâhil olmak üzere her insanda farklı olduğu kanıtlanmıştır (Öztürk, 2006).

Günümüzdeki teknolojik gelişmeler ışığında, teknoloji ilerledikçe suç işleme yöntemleri ve çözümleri de gelişmiştir. 19. yüzyılda adli anlamda kullanılan ve en önemli delil kaynağı olarak kabul edilen parmak izi günümüzde de çok yaygın olarak kullanılmaktadır (Hıdımoğlu, 2010). Günümüz teknolojisiyle AFIS/APFIS sistemi kullanılmakta olup olay yerinden alınan kimliği belirsiz kişi ve/veya kişilere ait parmak ve avuç izleri bu sistem sayesinde kimlik tespit işlemleri yapılmaktadır (Moses ve Ark., 2011).

Dünya ülkelerinde uygulanmakta olan parmak izi eşleştirmelerine baktığımızda, İngiltere ve İtalya'da 16 nokta, Türkiye, Belçika, Finlandiya, Fransa, İsrail, İrlanda, Yunanistan, Polonya, Portekiz, Romanya, Slovenya, İspanya Japonya ve Güney Amerika ülkelerinde 12 nokta, Almanya, İsveç, Hollanda, İsviçre'de 8-12 nokta, Güney Afrika'da 7 nokta incelemesi uygulanmaktadır (Filiz, 2012).

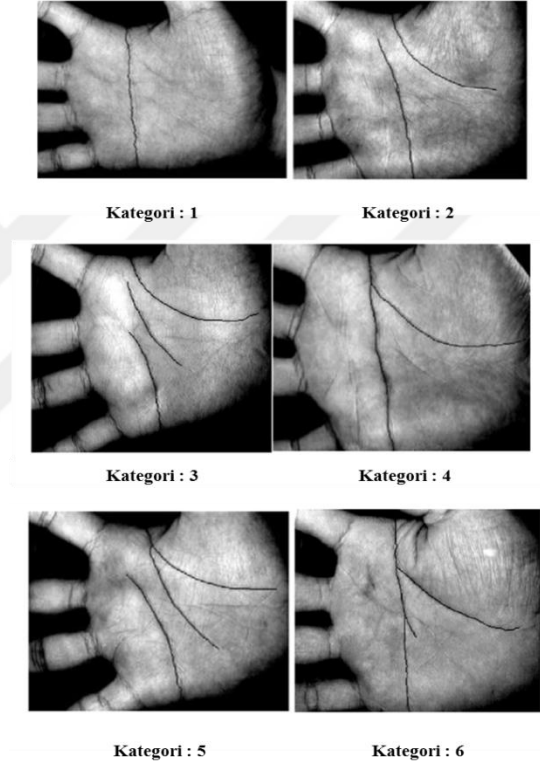
Dünyadaki hemen her ülkenin, suçlulara yönelik parmak izlerinin depolandığı bir veri havuzu mevcuttur. Onun için bu tür veri havuzlarının olması, adli vakalarda hem iş yükünü minimize eder hem de soruşturmaların zamanını en aza indirmeye yardımcı olur (Ceyhan Ve Ark., 2014).

Sonuç olarak AFIS/APFIS otomatik parmak ve avuç izi tespit sistemi, hem doğrulama hem de tanımlama açısından oldukça yüksek doğruluk oranına sahip bir teknolojidir (Moses ve Ark., 2011).

1.2.5.1.2. Avuç İçi İzi

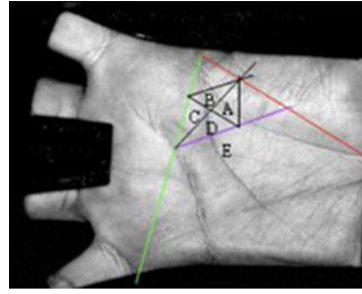
Biyometri yöntemi olarak ifade edilen avuç içi izi, parmak izi ve iris tanıma gibi yöntemlerle sıklıkla anılır. Ellerin avuç içi kısımlarını temsil eden avuç içi izi biyometri açısından ayırt edici özelliklere sahip olup, avuç içi izi tarayıcılar aracılığı ile kolayca alınabilir. Avuç içi izi cihazların, parmak izi için kullanılanlara benzerdir ancak boyutları daha büyüktür ve bu da mobil cihazlara kullanım sınırlamasını getirmektedir. İnsanların avuç içi izleri, temel çizgi, kırıksıklık, ikincil çizgi ve sırtlardan oluşmaktadır. Ayrıca avuç içi aynı zamanda bir avuç içi ile diğerini karşılaştırırken kullanılan doku, girintiler ve işaretler gibi bilgileri de içerir (Almezoghı, 2019).

Avuç içi izlerini farklı avuç içi çizgilere ve kesişme sayılarına göre sınıflandırmak mümkündür. Aşağıdaki (Şekil 1.5'te) gösterilen sınıflandırma X. Wu, D. Zhang, K. Wanfg ve B. Huang tarafından “İlke çizgilerini kullanarak Palmprint sınıflandırması” olarak sunulmuştur. Bu sınıflandırma grubuna göre 6 avuç izi kategorisi vardır.

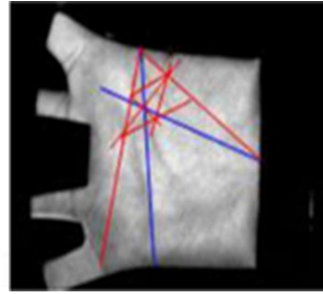


Şekil 1.5. Avuç İzi Kategorisi

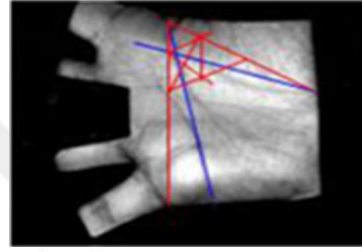
X. Wu, D. Zhang, K. Wanfg ve B. Huang tarafından “İlke çizgilerini kullanarak Palmprint sınıflandırmasına göre kategori 5 en yaygın olanıdır. Bu kategori de ayrıca 5 alt kategoriye ayrılmaktadır Şekil 1.6’da (Fang ve Ark., 2006).



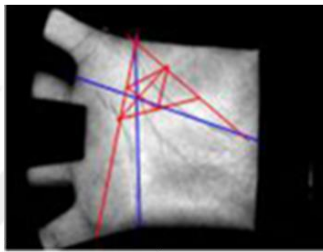
Kategori : 5



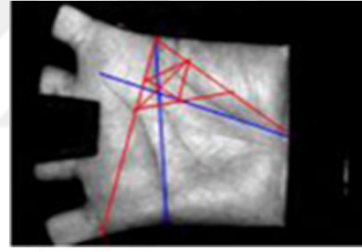
Kategori : 5 A



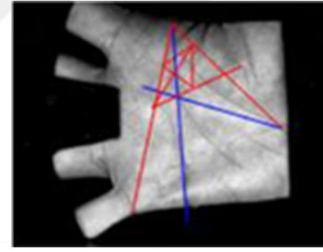
Kategori : 5 B



Kategori : 5 C



Kategori : 5 D

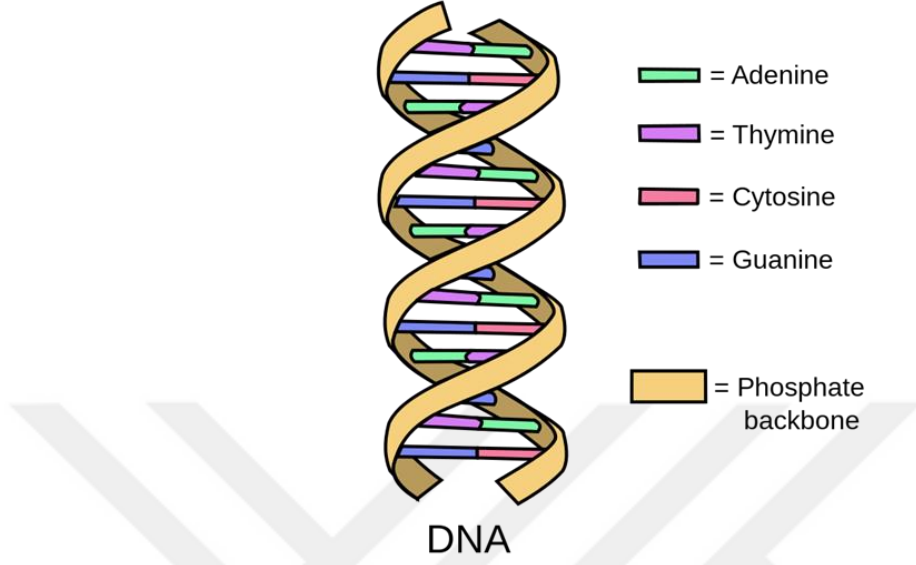


Kategori : 5 E

Şekil 1.6. Avuç İçi İzi 5. Kategori ve Bölünmesi

1.2.5.1.3. DNA Tanıma

DNA, hücrelerde bulunan, her canlı da farklı yapıya sahip olan, genetik bilgileri taşıyan bir nükleik asittir. DNA dört bazdan oluşur bunlar, Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) bazlarıdır. Bu bazların hepsi birlikte DNA kodunu oluşturur. Aşağıdaki şekil 1.7’de DNA ikili sarmal yapısı gösterilmiştir. İnsan genomu 6 milyar baz çiftinden oluşmaktadır. Bunların % 99’u her insanda aynı olup yalnızca %1’i her insanda farklıdır, dolayısı ile DNA’yı bir biyometri yöntemi yapan da sadece bu %1’lik kısımdır. (Kurtoğlu ve Tekedereli, 2015).



Şekil 1.7. DNA İkili Sarmal Yapısı

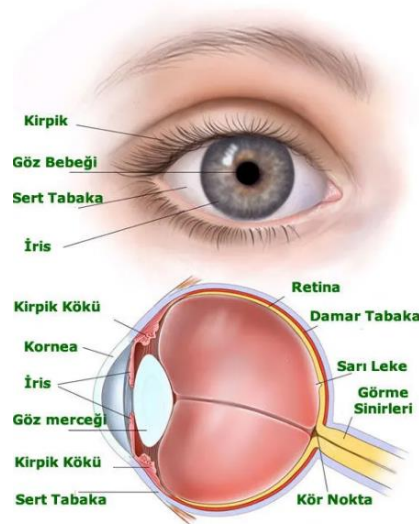
DNA, kriminalistikte yaygın olarak kullanılan popüler bir biyometrik yöntemdir çünkü DNA tanıma, biyometrik yöntemler arasında en güvenilir yöntemlerin başında gelmekte olup bir çok faili meçhul suçu aydınlatıp çözülmesine yardımcı olmaktadır. Fakat DNA tanıma, otomatik olmayan tek biyometrik yöntemdir (Özkaya ve Sağıroğlu, 2022). Bu nedenle DNA testlerinin sonuçlanması bazen saatler, bazen de günler sonra çıkmaktadır (Yalçın ve Gürbüz, 2015).

DNA, sadece vücut sıvısı değil, aynı zamanda tırnak, saç teli, tükürük, idrar, kan, ve kullanılmış tıraş bıçakları gibi çeşitli biyolojik kaynaklardan kolaylıkla elde edilebilir (Yalçın ve Gürbüz, 2015). Biyometrik uygulamalar için bukkal sürüntü en basit, kullanışlı ve ağrısız numune toplama yöntemidir. DNA'nın çıkarılması için birçok yöntem mevcuttur. Hangi yöntemin kullanılacağını seçimi, özellikle numune sayısı ve miktarı, maliyet ve hız gibi çeşitli faktörlere bağlıdır. Onun için adli vakalarda DNA miktar tayini önemli bir adımdır (Zeybek, 2012).

DNA tanıma yöntemini diğer biyometrik yöntemlerden farklı kılan bir istisna vardır; ikizlerin DNA'sı aynı olabilir. DNA tanıma, tıpkı bir parmak izi yöntemi gibi benzersizdir ve zamanla değişmez (Hashiyada, 2011).

1.2.5.1.4. Retina Tanıma

Retina; gözün en içteki, ışığa duyarlı doku tabakası olarak tanımlanır. Ayrıca gözün arkasındaki ışığa duyarlı sinir dokusu katmanları olarak da ifade edilmektedir. Göz küresinin arka planında yer alır ve görmemizi sağlar. Retina dıştan içe doğru 10 tabakaya ayrılmaktadır. Retinin en önemli avantajlarından biri, retina biçimlerinin çok farklı olması ve her gözün benzersiz bir kan damarı şekline sahip olmasıdır. Bu, tek yumurta ikizlerinin gözlerinde bile farklıdır (Şekil 1.8'de). Biyometrik yönden oldukça doğru ve zor olarak kabul edilen, yüksek güvenilirlik gerektiren alanlarda kullanılan ancak nispeten sınırlı bir uygulama alanına sahiptir. Bu da yaygın bir şekilde benimsenmesini kısıtlamakta ve sınırlamaktadır (Sadıkoğlu ve Üzelaltınbulat, 2018).



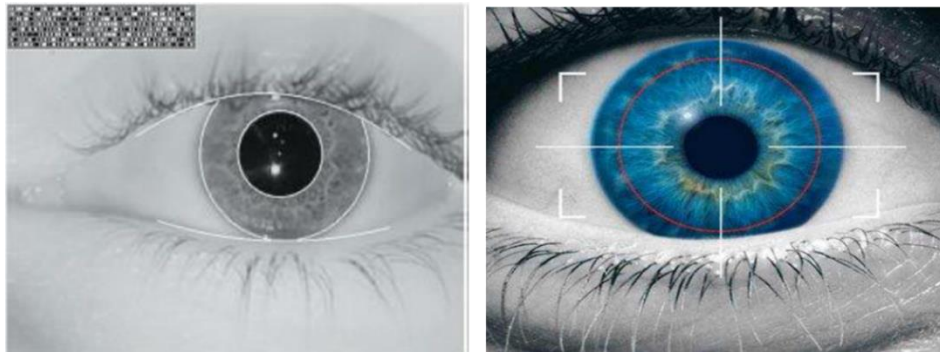
Şekil 1.8. Örnek İnsan Retina Şeması Temsili

1.2.5.1.5. İris Tanıma

İris tanıma, her kişi için benzersiz özelliklere sahip olan iris, gözün ön kısmında bulunur ve hamilelik döneminin sekizinci ayında oluşur. Renkli ve stabil bir yapısı vardır. Hayat boyu değişmemektedir. Bunlara ek olarak, iris 400'den fazla ayırt edici karakteristik özelliğe sahiptir (Akkan, 2013).

İris görüntüsü, genellikle görünür ve yakın kızıl ötesi ışıkları (700 - 900 nm) monokrom bir kamera kullanılarak elde edilir. Gözün renkli kısmı olan iris, trabeküler ağ adı verilen bir doku tipinden oluşur. İris yakından incelendiğinde katmanlı radyal çizgiler veya ağ görünümündedir. Görünür ağ, halkalar, çizgiler, oluklar, kriptler vb. özelliklerden oluşur ve irise benzersiz bir desen sağlar. Burada ana nokta, iris deseninin yaşam boyu aynı kalması ve desenin genetik yapıdan bağımsız olması nedeniyle ikizler, hatta tek yumurta ikizleri arasında da farklı olmasıdır (Şekil 1.9'da).

İris tanıma yöntemi, biyometrik yöntemler arasında doğruluğu kesin olarak kabul edilmektedir. İris, parmak izinden farklı olarak göz kapağı, kornea ve sulu mizah tarafından korunur.



Şekil 1.9. İris Örneği (Sol Üst Köşede İris Kodu Bulunan Bölünmüş İris Örneği)

İris tanıma süreci: İris tanıma sürecini bazı kaynaklar iki gruba bazıları ise üç gruba ayırmaktadır; bu gruplar: görüntünün yakalanması, iris konumunu tanımlama ve görüntüyü optimize etme, görüntü saklama ve karşılaştırma olarak ifade etmek mümkündür.

İris tanıma sisteminde kayıt işlemi; iris tarayıcısı aracılığı ile yapılmaktadır. Gözlük kullanan kişiler, yansımayı önlemek için ilk kayıt sırasında gözlüklerini çıkarmalıdır. Kontakt lens kullanan kişiler ise, sürece etki etmeyecekleri için lenslerini çıkarmamalıdır, çünkü lensler herhangi bir yansıma yapmazlar. Yapılan iris görüntü kayıtları karşılaştırma ve doğrulama için veritabanına kaydedilmektedir.

İris Tanımanın Avantajı ve Dezavantajı:

Avantajı: İris tanıma yönteminin avantajları arasında ilk sırada irisin tüm yaşam boyunca sabit kalması gelmektedir. Kullanıcı ve iris tarayıcısı arasında herhangi bir temas gerektirmez. Lazer kullanılmaz, sadece video teknolojisi kullanılır. Yüksek doğruluk seviyesi sahiptir bu da yöntemi parmak izi ile tek sıraya koymaktadır. Ayrıca bu yöntem, hızlı ve ölçeklenebilirdir.

Dezavantajı: Yöntemin büyük avantajlarına rağmen bazı dezavantajları da vardır. İrisin küçük bir organ olması sebebiyle tarama işlemini uzaktan yapmak imkansızdır. Körlük ve katarakt gibi göz problemleri olan kişiler için irisi okumak çok zor olduğu için tanıma sürecine katılmak çok zor olacaktır. Dolayısıyla doğru miktarda aydınlatma olmadan görüntü yakalamak zordur.

Sonuç olarak iris tanıma, çok düşük yanlış kabul oranı ile iris tanıma doğruluğu yüksektir. Hem doğrulama hem de tanımlama için uygulanabilir bir tekniktir. Tanımlama hızı çok hızlıdır. Ayrıca zayıf aydınlatma, yansıma ve muhtemelen camlardan etkilenir, bebeklerde ve kataraktlı kişiler için uygun bir yöntem değildir. Bu yöntemde görüntüyü yakalayabilmek için, kullanıcının kısa bir süre hareketsiz kalmasını gerektirir. Ek olarak, sistem maliyetinin nispeten yüksek olması ve sistemin kompakt olmaması nedeni ile yöntemi parmak izi ile tek sıraya koymaktadır (Saleh, 2022).

1.2.5.1.6. Yüz Tanıma

Tüm insanlık tarihi boyunca insanlar bir kişiyi diğerinden ayırt etmek için yüz kullanmışlardır. Yüz ve/veya yüz tanıma, bir video kaynağından alınan dijital bir görüntü veya video karesi yardımıyla bir kişiyi otomatik olarak tanımlayan veya doğrulayan bir bilgisayar uygulamasıdır. Buna en iyi örnek, elde edilen verileri veritabanında kayıtlı olan verilerle karşılaştırmaktır (Akgül ve Akar, 2022).

Normal bir kamera kullanılarak bir yüz görüntüsü alınabilir. Bu da kimlik doğrulamak için kullanılan en yaygın biyometrik örnektir. Yüz tanımayı gerçekleştirmek için kullanılan iki ana yaklaşım vardır, bunlar bütünsel veya küresel yaklaşım ve öznitelik tabanlı yaklaşımdır.

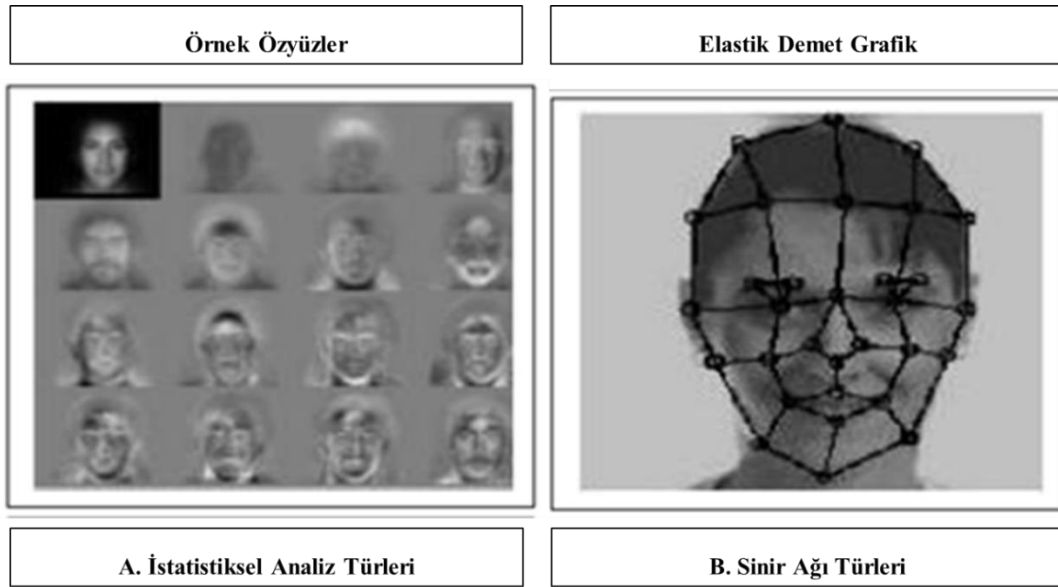
Özellik Tabanlı Yaklaşım:

Öznitelik tabanlı yaklaşım, kişinin elmacık kemiklerini çevreleyen noktalar, burun ve ağız kenarı, gözlerdeki noktalar vb. dahil olmak üzere yüzdeki değişime daha az duyarlı olan sabit referans noktalarının belirlenmesine dayanır. Bu noktaların yerleri, noktalar arasındaki geometrik ilişkileri hesaplamak için belli noktalar kullanılır.

Noktaları çevreleyen bölgeler yerel olarak da analiz edilebilir. Referans noktalarındaki tüm yerel işlemlerden elde edilen sonuçlar daha sonra toplanır ve genel yüz tanımayı elde etmek için birleştirilir. Özellik noktalarının tespiti analizden önce geldiğinden, sistem görüntüdeki konum varyasyonlarına karşı dayanıklıdır. Ancak referans noktalarının otomatik tespiti, yüz tanıma için yüksek bir doğruluk oranı sağlayacak kadar tutarlı ve doğru değildir.

Bütüncül Yaklaşım:

Bütünsel yaklaşım, şekil 1.10'da görüldüğü gibi tek tek noktaları yerelleştirmeden tüm yüz görüntüsünü aynı anda işler. Bu yaklaşımın kullanılan teknoloji türünde sinir ağları, istatistiksel analiz veya dönüşümler gibi bazı çeşitleri vardır. Bütünsel yaklaşımın avantajı, yüzü bir bütün olarak kullanmasıdır. Bu genel olarak daha doğru tanıma sonuçları verir. Bununla birlikte, bu teknik, ölçek ve konumdaki değişikliklere karşı hassastır ve bu nedenle büyük eğitim veri setleri gerektirir.



Şekil 1.10. Yüz Tanıma Tekniği Örnekleri.

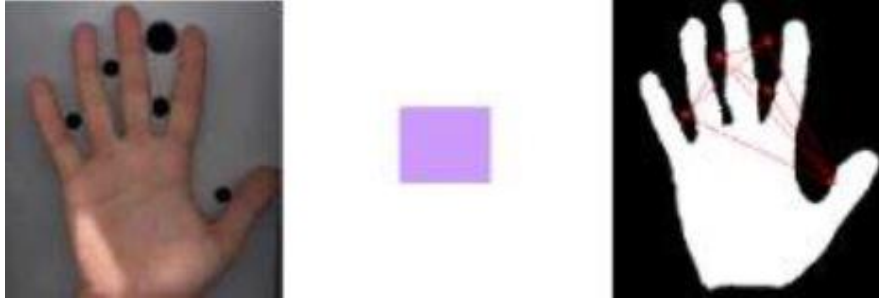
Bir kişinin yüzü sayısız ayırt edici özelliğe sahiptir. insan yüzünde yaklaşık 80 tane düğüm noktası mevcuttur. Bu düğüm noktalarından bazıları yazılımlar tarafından ölçülebilir örneğin;

1. iki göz arasındaki uzaklık
2. Burun genişliği
3. Göz yuvalarının derinliği
4. Elmacık kemiklerinin şekli
5. Çene hattının uzunluğu gibi bu düğüm noktaları ölçülerek özel bir sayısal kod oluşturulur. Bu kod yüz baskısı olarak ifade edilir ve bu kodlar veritabanında yüzü temsil eder.

Sonuç olarak, yüz tanıma, parmak izi tanımadan sonra kullanılan en popüler biyometrik sistemdir. Hızlı, kompakt ve kullanımı kolay olduğu için benimsenmektedir (Turhal, 2008).

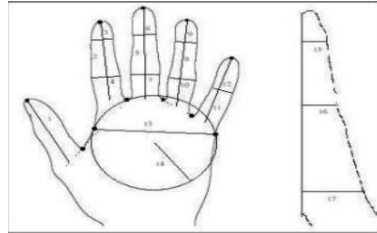
1.2.5.1.7. El Geometrisi

El geometrisi, elin geometrik şeklini tanıma amacıyla kullanılmakta olan bir yöntemdir. Ancak bu yöntem geçmişte kullanıldığı kadar günümüzde popüler bir şekilde kullanılmamaktadır. Yöntem, bir kişinin elinin şeklinin başka bir kişinin elinin şeklinden farklı olmasına ve belirli bir yaştan sonra değişmemesine dayanmaktadır. Bu biyometri yönteminin temel özelliği, el parmak boylarını, parmak uzunluklarını, eklemler arasındaki mesafeleri, eklemlerin şeklini, elin yüzey alanını ölçer ve kaydeder Şekil 1.11’de (Iula ve Micucci 2022).



Şekil 1.11. El Geometrisi Ölçüsü

El görüntüsü, kullanıcı elini istenilen bir yüzeye koyduğunda üstten yakalayan bir kamera kullanılarak elde edilir. Kullanıcı eli, referans işaretleri veya mandallar kullanılarak hizalanabilir. Genellikle tek bir görüntüde, yandan görünüm ve üstten görünüm olmak üzere iki görünüm alınır. Yan görünüm genellikle bir yan ayna kullanılarak üst kamera tarafından yakalanır. El görüntüsü ve parmaklar yerleştirilir, genişlik, uzunluk, kalınlık, eğrilikler ve bunların göreceli geometrileri ölçülür şekil 1.12’de (Almossawy ve George, 2022).

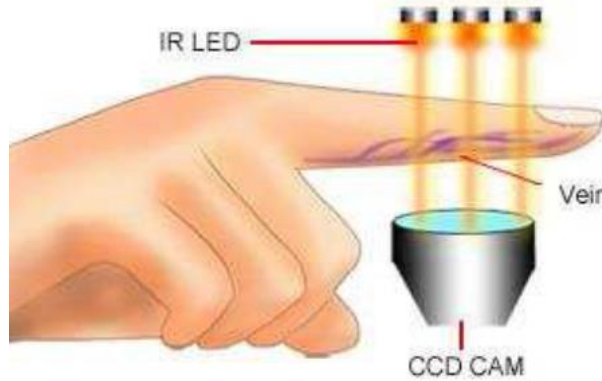


Şekil 1.12. Tipik Bir El Geometrisinin Ölçülmesi

Bazı durumlarda el geometrisi şablon boyutu çok küçük olabilir. Bu durumda, doğrulama için kabul edilebilir doğruluğa sahiptir, ancak en iyi tanımlama için yeterli değildir. Bu biyometrik yönteminin ana avantajı, çoğu insanın kolaylıkla kullanabilmesi ve kabul oranının iyi olmasıdır. Ancak olumsuz yanı, sistemin oldukça hantal olması, günümüzde nadiren kullanılıyor olması ve artrit gibi sağlık sorunları ile karşılaşabilmesidir (Wang ve Ark., 2022).

1.2.5.1.8. Parmak Damarı (Parmak Deseni)

Parmak damarı kimlik doğrulaması, genellikle kişilerin parmakları içindeki damar desenini kullanarak belirleyen biyometrik bir teknolojidir (Şekil 1.13'te). Damarlar genellikle kanı vücudun farklı bölümlerine taşımakla görevli borucuk veya kanallardır (Koç, 2019). Damarlar her insanda, kendine özgü fiziksel ve davranışsal özelliklere sahiptir. Bu nedenle kişisel bilgileri ve erişim kontrolünü çok daha iyi koruyarak oldukça yüksek bir güvenlik derecesi sağlar (Akkan, 2013). Kandaki deoksihemoglobin kızılötesi ışıkları emdiği için damar desenleri birkaç koyu ana hat olarak görülmektedir. Kızılötesi ışıklar, parmak damar modelinin bir görüntüsünü yakalayan özel kamera ile birleşir. Bu görüntü daha sonra herhangi bir kişinin biyometrik doğrulama verilerinin bir şablonu olarak kaydedilmekle birlikte kalıp verilerine dönüştürülür. Kimlik doğrulama sırasında, belirli parmak damarı görüntüsü alınır ve kişinin kayıtlı şablonuyla karşılaştırılır (Al-Ogaili Ve Shadhar, 2022).



Şekil 1.13. Parmak Damarı Tanıma İçin Görüntü Örneği

Parmak Damarı Biyometrisinin Avantaj ve Dezavantajları: Parmak Damarı Biyometrisinin bir çok avantajı olduğu gibi birden çok dezavantajı da vardır.

Avantajlar:

- Parmak damar desenleri genellikle her insanda farklıdır; tek yumurta ikizleri arasında bile her bireye özgüdür, bu nedenle gerçek yanlış kabul oranı oldukça düşüktür.
- Bir el veya parmak yerleştirmek işlemi, diğer biyometrik teknolojilere kıyasla aslında daha az müdahalecidir.
- Kan damarları insan vücudunun içinde yer aldığı için okunması veya çalınması oldukça zordur.
- Parmak damarları, kimlik doğrulama işlemi sırasında herhangi bir iz bırakmadığını için çoğaltılamaz.
- Parmak damar kalıpları, benzersiz ve değişmezdir. Bu nedenle damar kalıbının bir kez kaydedilmesi halinde tekrardan ve yeniden kayıt alınmasına gerek yoktur.
- Parmak damarlarının çevresel faktörlerden veya sağlık koşullardan kaynaklı meydana gelen değişikliklerden etkilenme olasılığı daha düşüktür.
- Pürüzlü epidermis, döküntülerden ve çatlaklardan kaynaklı olası sorunların, kimlik doğrulamanın sonucu üzerinde bir etkisi yoktur.
- Damar tanıma sistemlerinin doğruluk seviyesi oldukça yüksek.
- Doğrulama prosesi hızlıdır.

Dezavantajları:

- Olası bir kaza durumunda, kullanıcı parmaklarını kaybeder ise, doğrulama işlemi yapılamaz.
- Toplu tanıma için uygun değil.
- Bu teknoloji henüz test edilmemiştir, çünkü yalnızca satıcı şirketler doğruluk seviyelerini onaylamaktadır. Hükümetler ve standart şirketler veya kurum kuruluşlar tarafından henüz test edilmemiştir (Kauba ve Ark., 2022, Saini ve Rana, 2014).

1.2.5.2. Biyometrinin Davranışsal Türleri:

Davranış tanımlama yöntemleri, bir kişinin eylemlerine dikkat ederek, kullanıcıya eylemlerini kontrol etme fırsatı verir. Bu yöntemlere dayanan biyometri, yüksek düzeyde iç değişkenleri (ruh hali, sağlık durumu vb.) dikkate alır, bu nedenle bu tür yöntemler yalnızca sürekli kullanımda faydalıdır. Ses, yürüyüş, yazım ritmi gibi davranış veya bazen psikolojik olarak adlandırılan özellikler psikolojik faktörlerden etkilenir. Zaman içerisinde değişebilme özelliğinden dolayı bu özelliklerin sürekli yenilenmesi gerekmektedir. Kişinin davranışsal özellikleri, hem kontrollü eylemlerden hem de kontrollü psikolojik faktörlerden etkilenmektedir. Dolayısıyla davranış özellikleri zamanla değişebileceğinden, kayıtlı biyometrik numune her kullanımda yenilenmelidir (Deniz ve Özer, 2022).

1.2.5.2.1. Ses Tanıma

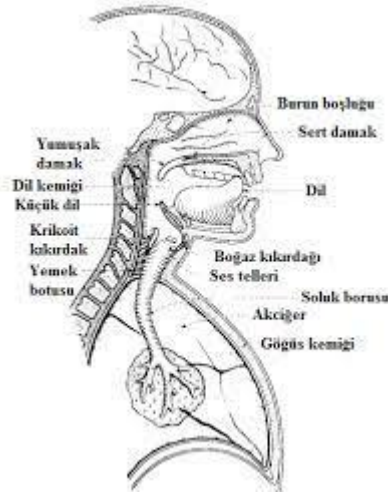
Ses tanıma, bir biyometri yöntemidir. Biyometrik tanımda kullanılan diğer birçok yöntem gibi ses de benzersizdir (Şekil 1.14'te). Ses tanıma sistemlerini kullanarak, ses analizi yapmak ve kişileri tanımlamak artık günümüz teknolojisi ile çok kolaydır. Biyometrideki ses veya “ses baskısı”, sesin sayısal bir modeli olarak sunulur. Ses biyometrisini güvenilir kılan, pek çok ayrı özelliğe sahip olmasıdır (Babich, 2012).



Şekil 1.14. Ses Tanıma İçin Görüntü Örneği

Ses, genellikle diğer biyometrik yöntemler gibi benzersiz özelliklere sahiptir. Bu nedenle benzersiz özellikleri sayesinde biyometrik kimlik doğrulamaya hizmet eder. Sesin benzersizliği, insan boğazının ve ağzının farklı fiziksel bileşenleri nedeniyle elde edilir. Ses üretmek için hava, insan vücudunu rezonatörler aracılığıyla terk eder. Seslerin biçimi, tonu, akışı, boyutu, gırtlak, ağız boşluğu (ağız) ve burun boşluğu gibi (burun) engellere bağlıdır. Ayrıca bu engeller arasında dil, diş etleri, dişler, dudaklar, bunların konumu ve boyutu yer alabilir Şekil 1.15'te (Asha ve Chellappan, 2012).

Ses tanıma aracılığı ile kimlik doğrulama; ses kaydı yardımıyla kişinin kimliğinin tespit edilebilmesi için kişiden konuşma örneği alınmalıdır. Ardından alınan örnek analiz edilerek veritabanında kayıtlı olan örneklerle karşılaştırılır, eşleşme durumunda kimlik doğrulaması yapılmış olur (Korkmaz Ve Boyacı, 2018).



Şekil 1.15. Ses Üretim Mekanizması

Ses doğrulama prensibi: Ses doğrulama için iki tür sistem kullanılabilir, bunlar:

1. Metne bağlı konuşma
2. Metinden bağımsız konuşma (Babich, 2012).

Sonu olarak ses, yaygın bir iletiřim aracı olduėundan, geniř bir telefon aėı ve mikrofonlarla birlikte ses doėrulamanın maliyeti ok dūřuk olması ile beraber sistemin kendisi de ok kompakttır. Ayrıca, kullanımı nispeten kolaydır. Diėer taraftan sesin yařa gre deėiřkenlik gstermesi ve ocukluktan ergenliėe geiř dneminde ciddi bir deėiřim yařanabilmektedir. Bunlara ek olarak; duygudurum bozukluėu, hastalık durumu, oda akustiėi ve evresel grlt gibi faktrler sesi olumsuz etkileyebilir. Kanal uyumsuzluėu (farklı tip ve kalitede mikrofon kullanımı) ve mikrofonlardaki eřitlilik de bu biyometrik teknolojinin yaygın kullanımı iin nemli bir sorun teřitil etmektedir (Saini ve Rana, 2014).

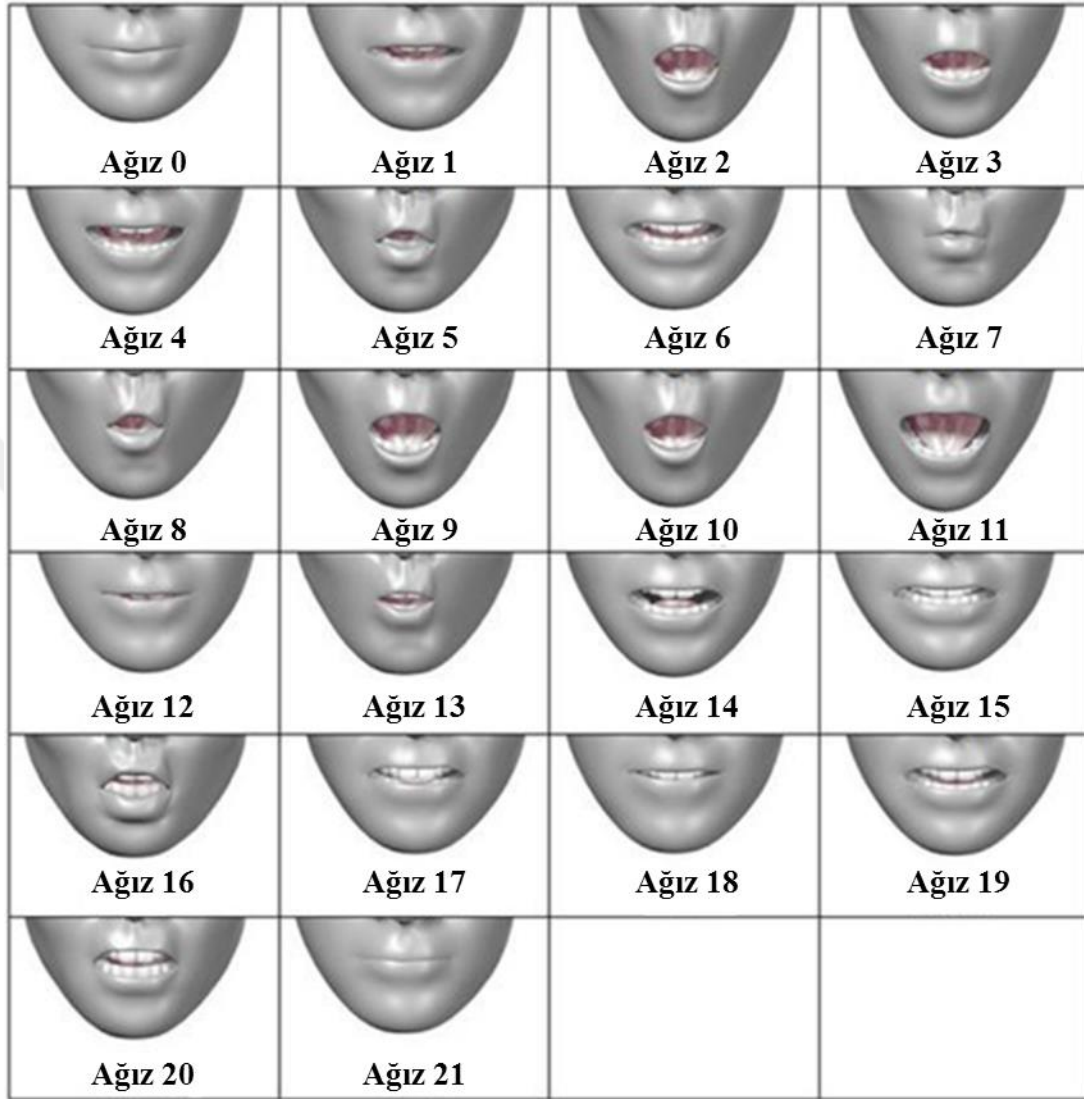
1.2.5.2.2. Dudak Hareketi

Su ve adli srelerden kaynaklanan en byk insan tanıma tekniėi, genellikle insan dudakları ile tanımlamadır. Biyometrik, geleneksel tanımlamanın birok zorluėu ile uėrařtıėı iin son zamanlarda nemli bir odak noktası oluřturmuřtur. İnsan kimliėini tanıyabilmek iin dudakların řekli ve renk zellikleri dikkate alınır. Dudak biyometrisi, yz ve ses tanıma gibi biyometrinin gcn artırmak iin kullanılabilir (Jeon ve Kim, 2022).

Dudak hareketleri konuřma dneminde karmařık kas ve kemik senkronizasyonu gerektirir. Seste belirli nller oluřtururken, (řekil 1.16'da) gsterildiėi gibi st ve alt dudaklar eřitli biimler geliřtirir. Konuřurken dudak oluřumu deėiřir, bu da aėzın hareket etmesine neden olur. Dudakla ilgili kasların ve kemiklerin bileřimi, bireye baėlıdır ve dudak řeklindeki bireyler arasında kk farklılıklara katkıda bulunur. Ek olarak, bireylerin zel konuřma biimleri genellikle eřitli dudak hareketi biimleri retir. Bu nedenle dudak hareketlerinin benzersiz zellikleri, kullanıcı kimlik doėrulaması iin biyometrik olarak kullanılabilir.

Dudak ve konuşma hareketlerinin faydalarını dahil ederek ilk şemaların eksikliklerini gideren cihazlarda multimodal biyometri doğrulaması yapılmıştır. Aynı anda, Multimodal biyometri doğrulama, yerleşik ses araçlarıyla akıllı telefonlarda bu iki biyometriyi algılar ve bunları veri noktasıyla birleştirir. Daha sonra güvenli ve verimli kimlik doğrulama özellikleri birleştirilmiş verilerden çıkarılır. Dudak, güçlü evrensellik, güvenilirlik, uzun ömür ve ölçülebilirliğe sahip biyometrik özelliklerden biridir ve biyometrik bir özellik olarak etkinliği ve kabul edilebilirliği arttırabilir, dolayısıyla bu alanda daha fazla çalışma yapıldıkça geliştirilmelidir (Alharbi ve Alahrbi, 2020).





Şekil 1.16. Dudak Hareketleri Şeması Temsili

1.2.5.2.3. El Yazısı (İmza Atımı)

Bir kişinin adını imzalama şekli, o kişinin karakteristiği olarak kabul edilir. Bu da uygulanabilir bir biyometrik tanıma modu sağlayabilir. Dinamik imza tanıma, bir kişinin imzasını incelemek için otomatik bir yöntemdir (Şamlı ve Yüksel, 2009).

İmza doğrulama, öncelikle işleme ve doğrulama için bilgisayara bağlanan özel bir kalem (ekran kalemi) ve yazı tabletinden oluşur. Kayıt işleminin veri toplama aşamasına başlamak için, kişi adını yazı tabletine birkaç kez imzalaması gerekir (Kaymaz, 2010).

Veriler elde edildikten sonra, imza doğrulama sistemi, kişinin adını imzalamasının ne kadar sürdüğü de dahil olmak üzere yazarın davranışsal özelliklerini çıkarır; uygulanan basınç; imzayı imzalama hızı; imzanın genel boyutu; imzadaki vuruşların miktarı ve çeşitli yönleri gibi bilgileri, kayıt taleplerinin doğrulanması için canlı imzanın kayıt şablonuyla gelecekteki karşılaştırmasında kullanır (Şan, 2013).

El yazısı doğrulaması, kalem, tablet veya dokunmatik ekran gibi dijital ürünlerle sağlanabilir. Aslında, bir el yazısı imzası bir Biyoteknolojik (BT) cihazları sembolüne dönüşmüştür. Günümüzde, dokunmatik paneller yaygın ve ucuz hale geldiğinden, parmak hareketini yakalamak kolaydır.

Biyometrik detayları olan kişisel tanımda, sistemde kişisel tanımlama, frekans ve basınç özellikleri kullanılmaktadır. Aynı kişi aynı mesajı yazdığında bu özellikler değiştirilemez. Nitekim örnek bir imza, aynı zamanda bir el yazısı işaretidir Şekil 1.17'de (Kaymaz, 2010).



Şekil 1.17. Örnek İmza Görüntüsü

1.2.5.2.4. Yazma Ritmi

Biyometrik tuş tanıma, insanları yazı yazma biçiminden tanımaya yarayan bir tekniktir. Bu teknik “ne” yazıldığı ile değil “nasıl” yazıldığı ile ilgilenen bir teknolojidir.

Günümüz dünyası tamamen bilgisayarlaştırılmış durumda. Bu nedenle teknolojik cihazlar, hemen hemen her insanın çok önemli bir parçası, vazgeçilmez bir aracı haline gelmiş durumdadır. Onun için bilgisayar sadece iş için değil aynı zamanda eğlence, iletişim ve eğitim aracı vb. amaçlarla da kullanılmaktadır. Örneğin keyboard, bilgisayarlardan ayrılmaz bir parçadır. Bu parça ayrı bir aparat halinde olduğu gibi dizüstü bilgisayarların veya akıllı telefonların içine gömülü bir şekilde de olabilir.

Keyboard, bilgisayarda yapılan işlemlerimizi sağlamaktadır. Bu nedenle her insanın kendine özgü keyboard kullanım şekli vardır. Kimi insanlar hızlı yazma yeteneğine sahipken kimi insanlarda yavaş yazma becerisine haizdir. Onun için her insanın klavye kullanma yöntemi ve şekli farklıdır. Ayrıca yazma ritmi insanların günlük ruh halini yansıtmaktadır.

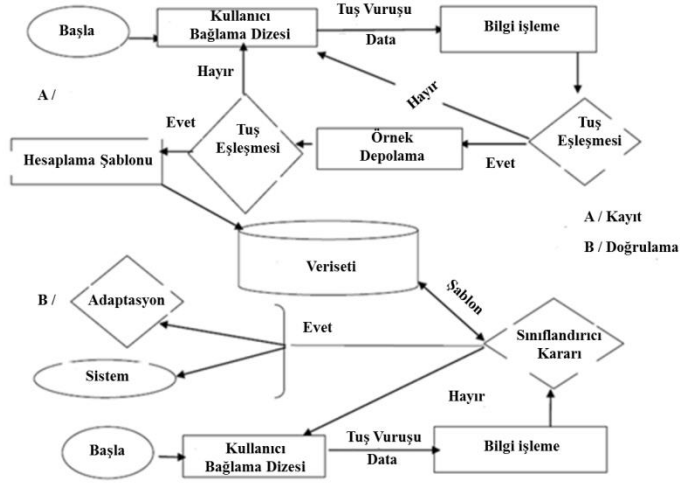
Bir kullanıcının yazma düzenini tanımlamak için kullanılan ana özellikler vardır, bu özellikleri,

- Ardışık tuş vuruşları arasındaki gecikmeler, ilk tuşun serbest bırakılması ile ikinci tuşun basılması arasındaki süredir,
- Her tuş vuruşunun süresi, kullanıcının tuşu basılı tuttuğu süredir,
- Parmak yerleştirme,
- Tuşlara uygulanan basınç;
- Genel yazma hızı şeklinde sıralamak mümkündür.

Birde dört tuşa basma gecikmesi olayı vardır;

1. P-P (Bas - Bas): tuşlara peş peşe basma arasındaki zaman aralığını ifade eder ve yazma hızını gösterir.
2. P-R (Bas - Bırak): Tuşa basılması ve bırakılması arasındaki zaman aralığı ifade eder, kullanıcının yazmak için ne kadar çaba sarf etmesi gerektiği gösterir.
3. R-P (Bırakma - Basma): Bir tuşun bırakılması ile diğerine basılması arasındaki geçen zamanı ifade eder.
4. R-R (Bırakma - Bırakma): Peş peşe iki tuşun serbest bırakılması için geçen zamanı ifade eder.

Kullanıcılar, sisteme erişmek istediği takdirde, hesap bilgileri (giriş adı ve kullanıcı şifresi) ile giriş yapar. Burada bir tuş vuruşu verisi yakalanarak, örnek bir tuş verisi oluşturulur. Oluşturulan bu örnek, veriler kullanılarak hesaplanan özellikleri (tuş süresi ve tuş vuruşu, gecikme süresi gibi) içerecektir. Yeni bir hesap için, bir şablon oluşturulur. Anahtar kod özelliklerinin eşleşmesi durumunda bu örnek saklanacaktır. Kimlik doğrulama durumunda, örnek sınıflandırıcı tarafından analiz edilecek ve şablon ile karşılaştırılacaktır (Şekil 1.18’de).



Şekil 1.18. A. Kayıt, B. Kimlik Doğrulama Akış Şeması

iki tür tuş vuruş dinamiği vardır. Statik dinamik ve sürekli dinamik. Statik dinamikte, tuş vuruşları sadece belli bir zaman aralığında, örneğin oturum açma sırasında analiz edilebilir. Statik dinamikler, basit şifrelere kıyasla daha sağlam kullanıcı doğrulaması sağlayabilir. Ancak bu yöntem sürekli güvenlik sağlayamamaktadır. Sürekli dinamikteyse, tuş vuruşları tüm oturum açma prosedürü boyunca analiz edilebilir.

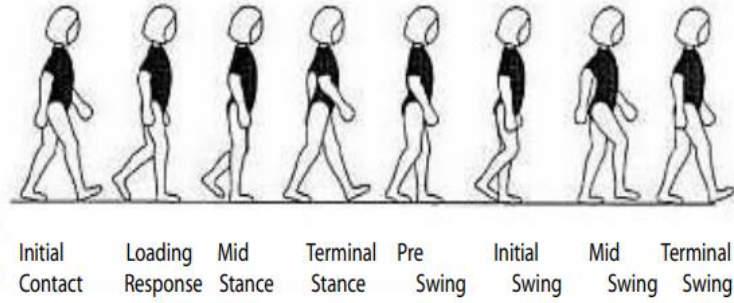
Yazma Ritminin Avantaj ve Dezavantajları:

Avantajı: Bu yöntemin ana avantajları, müdahaleci olmaması, geniş çapta kabul görmesi, minimum eğitim ve ek donanım gerekliliğidir.

Dezavantajı: Bu yöntemin ana dezavantajları, yüksek düzeyde yanlış reddetme oranı, kullanıcının fiziksel durumuna bağlı olma, dar aralıklı uygulamalarıdır (Babich, 2012).

1.2.5.2.5. Yürüyüş Tanıma

Yürüyüş biyometrisi, bireylerin yürüme biçimine dayanan bir biyometri yöntemidir. Bu tanıma yöntemi, kişilerin yürüme hızından etkilenmemektedir (Şekil 1.19'da). Ancak yürüyüş analizinin ortak faktörleri vardır. Bu faktörler; diz ve ayak bileği hareketleri ve açıları gibi kinematik faktörlerdir. Ayrıca adımların uzunluğu ve genişliği, yürüme hızı gibi uzamsal ve zamansal faktörlerdir. Bunlara ek olarak faktörler arasındaki korelasyondur. Nitekim asırlar önce Psikologlar, insanların yürüyüş ölçütlerini incelemişlerdir. Bu sebeple de, bir insanın başka bir insanı bir saniyeden daha kısa bir sürede tanımlayabileceğini keşfetmişlerdir (Santos ve Ark., 2022).



Şekil 1.19. Sağ ayak hareketine dayalı insan yürüyüş döngüsü

Bertenthal ve Pinto, insan yürüyüş algısının üç önemli özelliğini ortaya koymuşlardır. Bu özellikler;

1. Yürüyüş Frekansı: çeşitli yürüyüş komponentleri ortak bir frekansı paylaşır.
2. Faz kilitleme: yürüyüş komponentleri arasındaki bağlantı sabittir.
3. Fiziksel akla yatkınlık.

Yukarıda Bertenthal ve Pintonun ortaya koymuş oldukları yürüyüş algılarından yola çıkarak, bireylerin yürüyüş özelliklerini analiz etme sonucunda bir bireyin kimliğini doğrulamak ve bireyin kim olduğunu teşhis etmek açısından önemlidir.

Ayrıca yürüyüş tanıma yaklaşımlarına baktığımızda; üç tip yürüyüş tanıma yaklaşımı vardır. Bunlar; yapay görme tabanlı, zemin sensörü ve giyilebilir sensör tabanlı yaklaşımlardır (Mogan ve Ark., 2022).

Yürüyüş Tanımanın Avantaj ve Dezavantajı:

Avantaj: Bu yöntemin ana avantajları arasında, düşük çözünürlük ve aydınlatmanın yeterli olmaması halinde bile yürüyüş analizi yapılabilir. Ayrıca kişileri yakın bir mesafeden, saniyeler gibi kısa bir süre içerisinde tanıma yeteneği vardır.

Dezavantaj: Yürüyüş tanımanın dezavantajları arasında bazen yüzeye, yokuş aşağı, yokuş yukarı ve kişinin yürüyüş tarzını etkileyebilecek bir şey giyip giymediğine bağlı olmasıdır (Gafurov, 2008).

1.2.6. Biyometrik Tanıma Yöntemlerinin Karşılaştırma (Evrensellik, Eşsizlik, Süreklilik, Elde edilebilirlik, Performans; Kabul Edilebilirlik ve Yaygınlık).

Biyometrik sistem, genel olarak kişilerin fizyolojik ve davranışsal verilerinden faydalanarak kimlik tespiti veya doğrulaması yapabilen ve bu ölçümleri daha sonra güvenlik maksatlı kullanılmasını sağlayan sistemlere verilen addır.

Biyometrik sistemleri iki gruba ayırmak mümkündür. Bu sistemler, Fizyolojik biyometrik sistemler (parmak izi, retina tanıma, dudak hareketi, yüz tanıma, DNA, avuç içi izi, el geometrisi, parmak damarı (parmak deseni) ve iris tanım) ve Davranışsal biyometrik sistemler (yazma ritmi (tuş vuruşu), el yazısı, imza atımı, yürüyüş ve ses tanıma) olmak üzere bir kişinin diğer kişiden ayırt edilmesini sağlayan değişmez özelliklerdir (Musayeva ve Yahyayev, 2014).

Aşağıdaki çizelge 1.1.'de biyometrik güvenlik sistemlerinin kullanılabilirlik özellikleri yüksek, orta ve düşük olarak sınıflandırılarak karşılaştırılmıştır. Bu çizelgede; Y=Yüksek, O=Orta, D=Düşük olarak ifade edilmektedir.

Çizelge 1.1. Biyometrik Güvenlik Sistemlerinin Kullanılabilirlik Özelliklerine Göre Sınıflandırılması

Biyometri	Evrensellik	Eşsizlik	Süreklilik	Elde edilebilirlik	Performans	Kabul edilebilirlik	Yaygınlık
Parmak izi	O	Y	Y	O	Y	O	O
DNA	Y	Y	Y	D	Y	D	D
İris Tanıma	Y	Y	Y	O	Y	D	D
Ses Tanıma	O	D	D	O	D	Y	Y
Yüz Tanıma	Y	D	O	Y	D	Y	Y
Retina	Y	Y	O	D	Y	D	D
El Geometrisi	O	O	O	Y	O	O	O
İmza Atımı	D	D	D	Y	D	Y	Y

Yukarıdaki çizelge 1.1.'de, evrensellik biyometrinin her insanda ne kadar yaygın olduğunu gösterir; eşsizlik, biyometrinin bir kişiyi diğerinden ne kadar iyi ayırdığını gösterir; süreklilik, biyometrinin yaşlanmanın etkisine ne kadar iyi direndiğini gösterir; elde edilebilirlik ise işleme için biyometriyi edinmenin ne kadar kolay olduğunu ölçer. Performans, biyometrinin ulaşılabilir doğruluğunu, hızını ve sağlamlığını gösterirken, kabul edilebilirlik, teknolojinin halk tarafından günlük yaşamlarında kabul edilme

derecesini, yaygınlık ise, biyometrinin kullanımı bakımından ne derece kullanıldığını gösterir (Kaya ve Güneş, 2016).



2. GEREÇ ve YÖNTEM

Bu bölümde, kullanılan yöntem açıklamasıyla beraber tez çalışmamız esnasında kullanılacak yöntem ve deneyler ele alınıp veri seti üzerinde uygulanarak analiz edilecektir. İlk olarak veri seti içerisinde mevcut olan karşılaştırma açısından elverişsiz görüntülerin temizlenmesi sağlanır. Ardından elde edilen veriler yüz tanıma sistemi (Polyface) içerisinde bulunan yapay zeka derin öğrenme yöntemi aracılığı ile analiz ve testler yapılacaktır.

2.1. Veri Seti Açıklaması

Bu çalışmada iki tür veri seti kullanılmıştır. Birinci veri seti MIT-CBCL (2003-2005). Bu veri seti Massachusetts Institute of Technology (MIT Professional Education) tarafından oluşturulmuştur. MIT-CBCL yüz tanıma veritabanı, 10 deneğin yüz görüntülerini içerir. Yani Test seti, 200 görüntüden oluşmaktadır. Birinci veri seti iki eğitim setinden oluşmaktadır. Bu setler;

- Ön, yarı profil ve profil görünümü dahil olmak üzere yüksek çözünürlüklü resimleri kapsar,
- 10 deneğin 3D kafa modellerinden oluşturulmuş sentetik görüntüler (324/nesne). Kafa modelleri, yüksek çözünürlüklü, eğitim görüntülerine dönüştürülebilir bir model yerleştirilerek oluşturulmuştur. 3D modeller veritabanına dahil değildir.

Bu veri seti lisanslı olup aşağıdaki nitelikleri taşıyan araştırmacıların kullanımına sunulmuştur.

MIT-CBCL veri seti Lisans şartları,

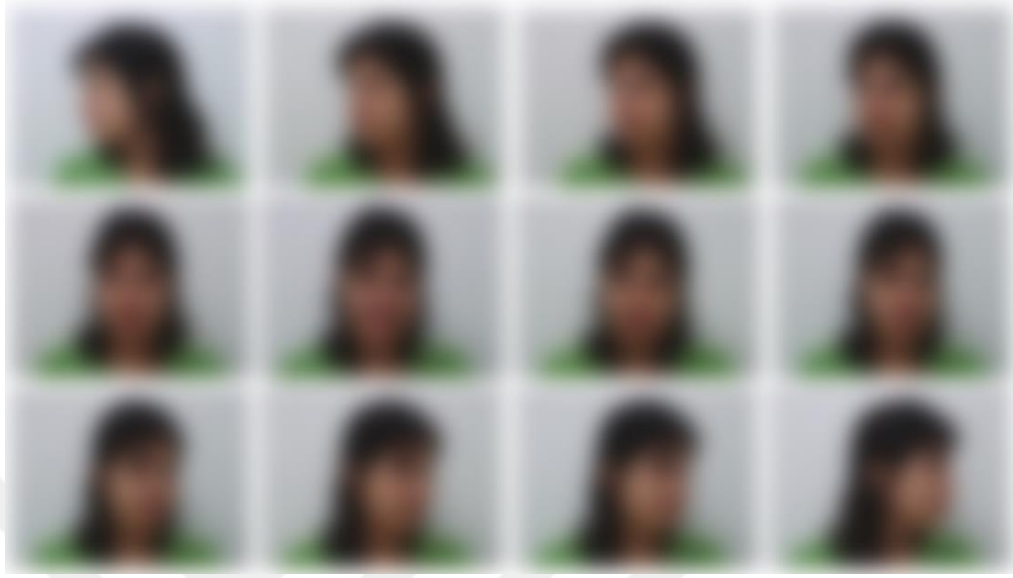
1. Bu veri tabanındaki görüntüleri kullanabilir ve çoğaltabilirsiniz, ancak bu veritabanı yalnızca araştırma amaçlıdır. Bu nedenle, bu görseller, 2. maddede açıklandığı şekilde atıfta bulunulması koşuluyla, akademik dergilerde, bilimsel konferans bildirilerinde yayınlanabilir ve/veya sunulabilir veya sınıf ortamlarında ve diğer benzer akademik ortamlarda kullanılabilir.
2. MIT'nin (Massachusetts Institute of Technology) telif hakkı bildirimi, veritabanındaki mevcut herhangi bir görüntünün herhangi bir kullanımına, yayınlanmasına veya sunumuna dahildir. Ek olarak, teşekkür ve alıntı uygun şekilde kullanılacaktır.
3. Veri seti içerisinde bulunan görüntülerin tamamı veya bir kısmı dahil başkaları ile paylaşıp dağıtılamaz.
4. Veri setinde bulunan görüntüleri yeni görüntüler oluşturmak için kullanabilirsiniz, ancak indirilen görüntüler değiştirilmemelidir.
5. Görseller herhangi bir ticari kullanım, satış veya herhangi bir dağıtım için kullanılamaz.
6. Görüntü veritabanının telif hakkı her zaman MIT'e aittir. MIT'nin adı ve ticari markaları MIT'nin önceden özel yazılı izni olmadan, veri setinde bulunan görüntülerle ilgili reklam yapmak, onaylamak, tanıtmak veya herhangi bir tanıtımla bağlantılı olarak kullanılamaz. Ek olarak 2. maddedeki telif hakkı bildirimi ve kabulü dışında "Massachusetts Institute of Technology"nin adını veya onun herhangi bir varyasyonunu, uyarlamasını, kısaltmasını veya herhangi bir mütevellî heyeti, memurları, öğretim üyeleri, fakülte öğrencilerini, çalışanları veya acentelerinin veya MIT'nin sahip olduğu herhangi bir ticari markanın herhangi bir tanıtım materyalinde, adlandırma kuralında veya diğer kamu duyurularında veya ifşasında MIT'nin önceden yazılı izni ve onayı olmadan kullanılamaz.
7. Veri tabanında bulunan görüntüleri "olduğu gibi" ve açık veya zımni garantiler ve satılabilirlik olmaksızın, sınırlar olmaksızın, ihlal etmeme ve uygunluk garantileri de dahil olmak üzere kabul edilir.

MIT, mütevellileri, müdürleri, yetkilileri, çalışanları ve iştirakleri hiçbir durumda ekonomik zararlar ve yararlar dahil olmak üzere herhangi bir arızı veya dolaylı hararlardan sorumlu olmayacaktır (MIT-CBCL Face Recognition Database).

İkinci veri seti ise FEI Face Database, bu veri seti Haziran 2005 ile Mart 2006 yılları arasında São Bernardo do Campo, São Paulo Brezilya'daki FEI Yapay Zeka Laboratuvarında hazırlanmış bir takım yüz görüntüsünü içeren bir Brezilya yüz veritabanıdır. Bu veri setinde farklı açılardan çekilmiş 200 kişilik bir yüz görüntüsünden oluşmaktadır. Her kişi için 14 görüntü çekilmiş olup veri seti toplam 2800 görüntü içermektedir. Bu veri seti veri ön işlemeye tabii tutularak elverişsiz görüntüler ayıklanacaktır. Çekilen tüm görüntüler renklidir. Bu görüntülerin arka planı homojendir ve beyaz renkli bir arka planda çekilmiştir. Bu veri seti içerisinde ölçek yaklaşık %10 değişkenlik göstermekle birlikte her görüntü farklı boyutlardadır. Kullanılan tüm denek yüzler, belirgin görünümlü, farklı saç modeli ve değişik süslemelerle birlikte 19 ila 40 yaşları arasındaki FEI öğrenci ve personeline aittir (FEI Face Database Disclaimer).

2.2. Veri Ön İşleme

Bu çalışmada kullanılan veri setleri, ön profil olmak üzere farklı açılardan çekilmiş görüntüler içermektedir. Ancak sistemin verimli bir şekilde çalışması açısından görüntülerin ayıklanması ve temizlenmesi gerekir. Buradaki amaç, kişilerin doğru bir şekilde tespit edilmesi için kullanılan görüntülerin sistemin analiz edebilme açlarına uygun olması gerekmektedir. Sistem 45 derecelik açıya kadar kesin tespit edici özelliğine sahiptir ancak 45 ile 90 derece arasındaki çekilen görüntülerin tespiti için sistemin önleyici tespit edici niteliğinden de faydalanılabilir. Veri seti, sistem içerisine aktarılırken yüzlerin doğru kodlanması ve kimlik tespiti için veri setinde bulunan 45 derecelik açıdan fazla olan görüntülerin temizleme işlemi yapılmıştır. Aşağıdaki şekil 2.1'de temizleme işlemi uygulanmadan önceki görüntüler, şekil 2.2'de temizlenme işlemi uygulandıktan sonraki görüntüler gösterilmektedir (Oğuzlar, 2003).



Şekil 2.1. Temizleme İşlemi Uygulama Öncesi Görüntüler



Şekil 2.2. Temizleme İşlemi uygulandıktan Sonraki Görüntüler

Yukarıda kullandığımız görüntüler veri seti içerisinde bulunan görüntülerden rastgele seçilmiş olup örnek amaçlı gösterilmiştir. Veri setinde kullandığımız diğer tüm görüntüler de aynı ayıklama işlemlerine tabii tutularak temizlenecektir (Oğuzlar, 2003).

2.3. Yüz Algılamada Kullanılan Kodlama Yöntemi

Hareketsiz (fotoğraf), video veya canlı kameralarından alınan görüntüler yüz tanıma popülaritesini, özel sektörden güvenlik alanına kadar uzanan geniş uygulama alanı nedeniyle son on yılda büyük ölçüde araştırılmıştır (Avcı ve Ark., 2017). Tüm bu uygulamalar, kişileri doğrulama veya tespit etme sürecine ilişkin yüz fotoğraflarının doğru kodlanması neticesinde etkin ve verimli bir eşleştirme ve karşılaştırma imkanı sağlar. Çalışmamızda kodlama yöntemi olarak Fiducial Points kullanılmıştır (Mitra ve Ark., 2020).

2.3.1. Referans Noktaları (Fiducial Points)

Referans noktaları (Fiducial Points); genellikle kaş, göz, burun, dudak ve çene köşesinin yanı sıra dudak ucunda ve burun ucunda ayrıca yüzdeki diğer dış ortam organlarında bulunan ve yüz ifadesini temsil eden bir dizi belirgin noktalardır (Hani ve Ark., 2011).

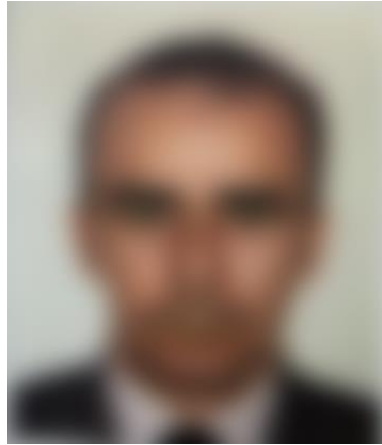
Referans noktalarının otomatik olarak algılanması, noktalar arasındaki mesafeler ve yüz bileşenlerinin göreceli boyutları ile yüz ifadelerinin belirgin özelliklerini çıkarabilir ve özellik vektörünü oluşturabilir. Ek olarak, özellik noktalarının seçilmesi, yüzdeki en önemli özellikleri temsil etmeli ve kolayca çıkarılmalıdır. Başka bir deyişle, özellik noktalarının sayısı yeterli bilgiyi temsil etmeli ve çok fazla olmamalıdır (Arca ve Ark., 2006).

İlk temel adım, görüntüdeki yüzü ve buna karşılık gelen yüz özelliklerini (gözler, burun, ağız ve çene) lokalize etmekten oluşur. Göz köşeleri veya burun ucu gibi nispeten

sabit veya sağlam yüz işaretleri, yüz işleme literatüründe referans noktaları olarak adlandırılır. Bu yüzden gözler tespit edildikten sonra ağız, kendine özgü anatomik şeklinden yararlanılarak lokalize edilir. Daha sonra göz ve ağız pozisyonlarına göre burun, kaşlar ve çene tespit edilir (Kusban, 2021).

Bu çalışmada kodlama yöntemi olarak (fotoğrafların kodlanması için) Fiducial Points (Referans Noktaları) metodu kullanılmıştır. Kodlama işlemi hem otomatik hem de manuel olarak gerçekleştirilmiştir. Ayrıca yöntem hem renkli hem de renksiz (Siyah-Beyaz) görüntüler üzerinde kodlama yapabilme kabiliyetine sahiptir (Salmam ve Ark., 2018).

Yüz ve yüz özelliklerini lokalize ettikten sonra, ön profilde belirlenen referans nokta sayısı, 66 düğüm noktası olarak tanımlanır (Şekil 2.3'te). Tanımlanan bu noktalara Gabor filtresi uygulayarak karakterize edilir. Tanıma, farklı jetler arasındaki benzerlikleri ölçerek karşılaştırma işlemi gerçekleştirilir (Campadelli ve Lanzarotti, 2004).



Şekil 2.3. Ön Profil Referans Nokta Lokasyonu

Otomatik ile manuel kodlama arasındaki en önemli fark, otomatik kodlama işleminde tüm referans noktalar otomatik olarak kodlanır. Bununla birlikte, bir yüz görüntüsü verildiğinde, bazı özelliklerinin yanlış bir şekilde lokalize edilmesi veya tanımlanması nadiren görülür, bu da hem özellik lokalizasyonu belirlemede hem de referans noktası tahmi etmede bazı hatalara neden olur. Bu durumda manuel kodlama işleminde; sistem göz bebeklerinin referans noktalarını, yeniden yapılandırılmasına imkan tanır şekil 2.4'te (Arca ve Ark., 2006).



Şekil 2.4. Göz Bebeklerin Referans Nokta Lokasyonu

Referans noktalarının fotoğraf veya video görüntüleri üzerinde başarılı bir şekilde algılanması, yüz algılama ve tanımlama (duygu ve yüz ifadeleri tanımı) gibi çok sayıda yüz görüntü yorumlama görevinde önemli bir rol oynamaktadır (Yun ve Guan, 2009).

Sonuç olarak yüz algılama, otomatik referans algılama ve izleme sistemi için önemlidir ve genel sistem performanslarını etkiler. Bu nedenle kişilerin yüksek doğruluk oranıyla tespit edilmesi, referans noktaların doğru kodlamasından geçer. Dolayısıyla referans noktaları ne kadar iyi ve doğru kodlanırsa, eşleşme skor sonuçları da o kadar iyi, doğru ve yüksek olacaktır (Çeliktutan, 2013).

2.4. Yüz Tanımada Kullanılan Yöntemler ve Algoritmalar

Akıllı davranışların yapay olarak üretmeyi amaçlayan, canlı sistemlerin ve insan beynini model alan yapay zeka çalışmaları; farklı alanlarda sistemler geliştirilmesine, ürünler üretilmesine bunun yanı sıra tahmin, sınıflandırma, kümeleme gibi amaçlar için de kullanımı yaygınlaşmıştır. Yapay zeka; insan zekasının, sinir sistemi, gen yapısı gibi fizyolojik ve nörolojik yapısının ve doğal olayların modellenerek bilgisayar ve yazılımlara aktarılması olarak adlandırılmaktadır.

Biyometrik sistemlerde, insanların yüz gibi diğer vücut özellikleri kullanılmaktadır. Nitekim birini tanımak için yüzlerce yıldır ses ve davranış analizleri yapılmaktadır. Ayrıca onlarca yıldır da bilişim ve teknoloji alanındaki gelişmeler, biyometrik tanıma sistemlerinin ilerlemesinde de önemli katkıda bulunmuştur. Dolayısı ile son on beş yıldaki büyük ilerleme, özel sektörün yanı sıra akademik yönden de yüz tanıma sisteminin ilgi çeken bir konu olmasını sağlamıştır. Bunun nedeni yüz tanıma sistem doğrulama ve tanımlama olarak bilinen bilgisayar, tablet ve mobil cihazlarda geliştirilen ve kullanılabilir uygulama olmasıdır. Dijital bir cihaz kullanarak bir kişinin kimliğinin belirlenmesine veya doğrulanmasına izin veren görüntü, resim veya video; dijital bir görüntüdeki yüz özelliklerini veritabanındaki bulunan yüz özelliklerine göre karşılaştırılmasıdır. Yapay sinir ağları geliştirilmiş bir bilgi işleme modelidir. Sinir sisteminin çalışma prensibine göre insan beyni Yapay sinir ağlarının sorunları çözebilecek bilgi farklı yöntemler kullanılarak elde edilebilir. Backpropagation (geri yayılım) ve yaygın olarak kullanılan radial basis function (radyal tabanlı fonksiyon) sinir ağı algoritmalarıdır. Yüz tanıma sistemlerinde elde edilecek başarımların artırılmasına yönelik farklı sinir ağı algoritmalarından hibrid çalışmalar yapılarak özelleştirilmiş algoritma paplion yüz tanıma sisteminin engineine yerleştirilmiştir.

Papillon yüz tanıma sisteminde farklı aşamalar bulunmaktadır. Yüz resimlerinden çeşitli özelliklerin çıkarılması ilk aşama olarak değerlendirilmektedir. Aynı insana ait farklı resimler arasındaki benzerlik aranırken farklı insanlara ait resimlerdeki çıkarılan özelliklerin farklı olması ve karşılaştırılırken bu farklardan dolayı eşleşmemesi ve ayırt edici olması yüz tanıma sisteminin temel özelliğidir (Parwani, 2022). Bu bağlamda yüz tanımda kullanılan yöntemler üç temel gruba ayrılır. Bu gruplar;

2.4.1. Özellik Tabanlı Yüz Tanıma Sistemleri:

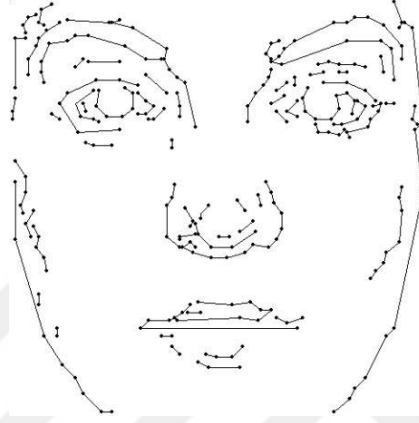
Bu sistemlerde ekseriyetle ilk olarak göz, burun ve ağız noktaları lokalize edilir. Daha sonra lokalize edilen bu noktalar birbirlerine göre geometrik pozisyonlarından ve/veya biçimlerinden yüzü sınıflandıran yapısal veriler elde edilir (Turhal, 2008). Özellik tabanlı yöntemleri esas olarak 3 farklı başlık altında incelemek mümkündür

2.4.1.1. Yapısal Eşleme

Bu yöntemin temel prensibi kaş, göz, burun; ağız gibi yüz özelliklerini ifade eden organların yüz üzerindeki lokasyonlarını tespit etme esasına dayanmaktadır. Bu organların birbirine göre lokasyonları, nitelikleri, birbiri arasındaki açı, mesafe ve uzaklık gibi parametreler yüz tanıma sırasında belirleyici özelliklerdir. Dolayısı ile bu algoritmaların başarı performansı yüz özelliklerinin kalitesi ile doğru orantılıdır.

Başka bir yaklaşımda şablon eşleme ve geometrik özellik seti eşleme yöntemleri ile yüz özelliklerinin çizgisel kenar haritası olarak türeyiştir. Bu metotta ekseriyetle sobel kenar analizi algoritması kullanılarak yüzlerin ikili kenar haritalarını oluşturur. Yüz görselleri arasındaki benzerlikleri yüz nitelik şeması kullanılarak bulmak

mümkündür. Aşağıdaki şekil 2.5'te çizgisel kenar haritası örneği verilmiştir (Gao ve Leung, 2002).



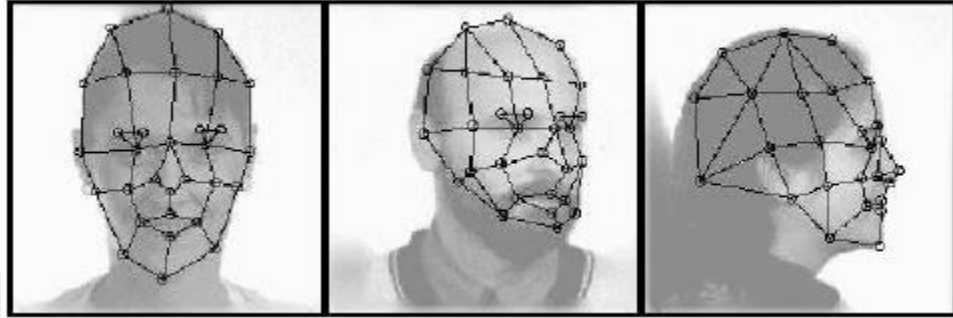
Şekil 2.5. Yüz Tanımda Kullanılan Çizgisel Kenar Haritası İllüstrasyonu

2.4.1.2. Elastik Demet Grafi Eşleme

Elastik demet grafi eşleme - Elastic Bunch Graph Matching (EBGM) olarak bilinen bu yöntemde geniş çaplı bir dikdörtgen ızgara, insan yüzüne maske şeklinde örtülerek yüzdeki kritik düğüm noktalarının işaretlenmesini sağlar. Aşağıdaki şekil 2.6'da elastik demet grafi örneği verilmiştir. Elastik demet grafi eşleme metodunun ehemmiyet arz eden aşamalarından biri, yüzdeki kritik düğüm noktalarının dikdörtgen ızgarası içerisine tam ve doğru bir şekilde yerleştirilmesi gerekir.

2004 yılında Gonzales-Jimenez ve Albo-Castro tarafından yüzdeki çukurlukları ve çıkıntıları bulan bir algoritma geliştirilmiştir. Geliştirilen bu algoritma yüzde görülen aydınlanma değişimlerini kontrol altında tutabilmektedir. Onun için bu yöntem ekseriyetle yüksek performansla çalışan yöntemler arasında yer almaktadır. Fakat bu yöntemler genellikle $128 * 128$ gibi büyük ebatlarda yüz görüntülerine gereksinim

duyarlar. Bu yüzden bu yöntemin yalnızca büyük ebatlı resimlerle çalışması mümkündür (Bolme, 2003).

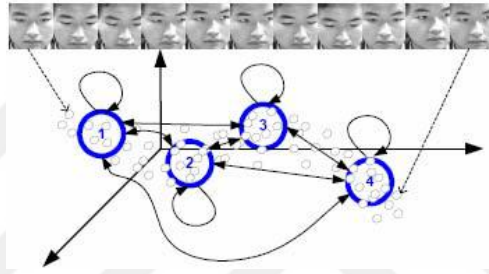


Şekil 2.6. Elastik Demet Grafi Eşleme Yöntemi

2.4.1.3. Gizli Markov Modeli

Gizli Markov Modeli - Hidden Markov Model (HMM) olarak bilinen bu yöntem, genellikle makine öğrenimi algoritmaları verilere yönelik istatistiksel parametreleri dikkate alarak öğrenme ve tahmin etme esasına dayanarak çalışır. Dolayısıyla istatistiksel verileri dikkate alan metotların başında Gizli Markov Modeli gelmektedir. Gizli Markov Modeli ilk olarak Baum ve ark. tarafından önerilmiştir (Ali ve Ark., 2022). Bu model 1970’lerde görüntü işleme ve tanımda yaygın olarak kullanılmıştır. Onun için bu yöntem ilk olarak yüz modelleme çalışmalarında uygulanmıştır. Daha sonra bilgisayar ağlarına da uygulanan bu model, internet ağ trafiğine yapılan saldırıları algılayabilmek ve tespit etmek için kullanılmıştır (Biswas ve Ark., 2022). Genel olarak Gizli Markov Modelleri bir sınıflandırma aracı olarak bilinmektedir. Bu model başta zaman serileri olmak üzere bir çok problemin çözümünün de sınıflandırma aracı olarak kullanılmıştır (Auguste, 2022). Bu modeller, özellik vektörüne dayalı matematiksel kosinüs uygulaması ile elde edilir. Gizli Markov modellerinin, yüz tanıma ile ilgili kapsamlı uygulaması olan ve her yerde bulunan bir stokastik model sınıfıdır. Gizli Markov modelleri yeni gözlemlenen verinin sınıflandırılmasını sağlamaktadır. Gizli Markov

modellerinin, gözlem durumu ve gizli durum olmak üzere iki durumu vardır. Örneğin Biyoinformatikte, eğer DNA dizisi ACAATGGT olarak verilirse, DNA dizisi bir gözlem durumu olarak kabul edilirken, gizli durum hangi bilginin elde edileceğine bağlı olarak değişir. Nitekim Markov Zincirinde genellikle doğrudan gözlem yapılamaz onun için adından da anlaşılacağı üzere buna gizli Markov modeli denilmektedir (Samaria, 1994). Aşağıdaki şekil 2.7’de üç boyutlu bir durum geçiş uzayı örneği yer almaktadır.



Şekil 2.7. Seri Haldeki Yüz Eesimlerinin Modellendiği Gizli Markov Model İllüzyonu

2.4.2. Görünüm Tabanlı Yüz Tanıma Sistemleri:

Bu sistemler aracılığı ile yüz özelliklerinin tamamı kullanılarak yüzü biçimlendirecek ham veri elde edilmeye çalışılır. Görünüm tabanlı yöntemlerini başlıca iki ayrı grupta ele almak mümkündür (Turhal, 2008).

2.4.2.1. Temel Bileşen Analizi

Son yıllarda yüz tanıma sistemleri, bilgisayarla görü alanının ve görüntü analizin hem popüler bir araştırma alanı hem de en başarılı uygulamalardan biri olarak karşımıza çıkmaktadır. Yüz tanıma sistemlerinde kullanılan en basit ve en etkili Temel Bileşen Analizi (PCA) yaklaşımlarından biri olan özyüz yaklaşımı olarak adlandırılan

yaklaşımıdır. Bu yaklaşım, yüzleri, ilk öğrenme görüntü setinin (eğitim seti) ana bileşenleri olan küçük temel özellikli özyüzlere dönüştürür. Bu da özyüz alt uzayına yeni bir görüntü yansıtılarak yapılır, ardından kişi özyüz uzayındaki konumu bilinen bireylerin konumuyla karşılaştırılarak minimum öklid mesafesi ölçülerek sınıflandırılır (Chang ve Ark., 2022).

Temel Bileşen Analizi (PCA), yüz tanımadaki değişken sayısını azaltmak için kullanılan istatistiksel bir yaklaşımdır. Bu da n sayı sütun ile m sayı satırdan meydana gelen bir yüz görseli $n * m$ ebatında bir vektörle ifade edilebilir. PCA'da, eğitim setindeki her görüntü, özyüzler adı verilen ağırlıklı özvektörlerin doğrusal bir kombinasyonu olarak kabul edilmektedir. Bu özvektörler, bir eğitim görüntü setinin kovaryans matrisinden elde edilir. Ağırlıklar, en alakalı Özyüzler kümesi seçildikten sonra bulunur (Han Ve Ark., 2022).

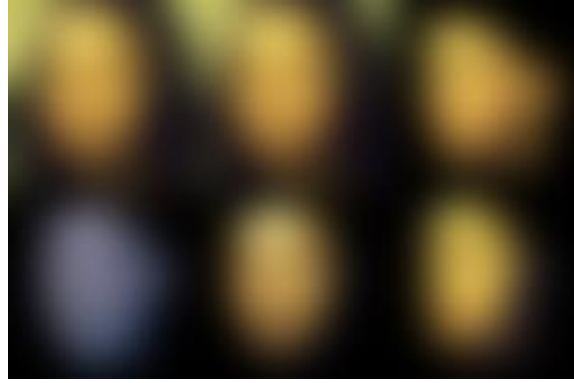
Bu yaklaşımın (Temel Bileşen Analizi Yönteminin) diğer yüz tanıma sistemlerine göre avantajlarına baktığımızda, basitliği, düşük hassasiyete sahip olması, kapasite ve bellek ihtiyaçlarının azaltılması, hızı ve yüzdeki küçük veya kademeli değişikliklere karşı duyarsızlığıdır. Ek olarak, düşük ebatlı uzaylarda etkin indekslemelerin yapılmasına olarak tanınmasıdır (Boudou ve Viguier-Pla, 2022).

Bu yöntemin en önemli kriterleri, yüz görsellerinin tam ve düzgün olmasının yanı sıra sabit aydınlanma şartlarına bağlıdır. Eğer bu şartlar sağlanmazsa, ilk özvektörler yüz pozları ve aydınlanma şartlarındaki değişiklikleri yansıtacaklardır. Bu sebeple Temel Bileşen Analizi (PCA) tabanlı yöntemler, aydınlanma ve poz gibi farklı ön şartlarla sınırlandırılmamış ortamlar açısından elverişli değildir (Ronda, 2022).

2.4.2.2. Üç Boyutlu (3D) Yüz Tanıma Modelleri (3D Morphable Model)

Yüz tanıma oldukça meşakkatli fakat üzerinde çok çalışma ve araştırma yapılmış bir Pattern tanıma problemidir. Aslında insan yüzü üç boyutlu (3B) düzlemde yer alan bir yüzeydir. Bu sebepler 3DMM'ler geçmişten günümüze uzanan bilgisayarla görme, insan davranış analizi, bilgisayar grafikleri ve kraniyofasiyal cerrahi gibi pek çok alanda yaygın olarak uygulanmaktadır (Göze ve Yıldız, 2022).

Üç boyutlu (3B) yüz tanıma modelleri (3DMM'ler): insan yüzünü şekil ve doku açısından istatistiksel olarak 3D modelleyebilen bir yöntemdir. Bu yöntemin temel prensibi, 3B yüzlerden oluşan bir veri kümesine dayanır. Yüzler arası geçişte, tüm yüzler arasında tam bir uyumluluk gerektirir. Onun için eğitim setinde bulunan denek yüzlerin düşük kalite ve çözünürlükte olsa bile uyumlu olmaları gerekir. Ayrıca yararlı bir yüz sentez sistemi için, sonuçların yüz olma olasılıkları açısından nicelleştirilebilmesi önemlidir. Dolayısı ile üç boyutlu yüz tanıma sistemi temel olarak iki bölümden meydana gelmektedir. İlk bölümde 3B görselde yüz ve yüzde bulunan bazı önemli noktalar bulunur. Daha sonra belirlenen yüz çerçevesi standart bir poz ve boya getirilir. Ardından farklı metotlar aracılığı ile 3B yüz tasarlanması gerçekleştirildikten sonra yüz tanıma aşamasına geçilir (Blanz ve Vetter, 1999). Yalnız buradaki en önemli nokta, yüz üzerindeki bazı önemli düğüm noktalarının (göz ve dudak kenarları gibi) doğru bir şekilde lokalize edilmesi gerekir. Yüz üzerinde bulunan düğüm noktalarının tespit edilmesi yüz tanıma sistemleri açısından daha sonraki aşamalar için (ör. çakıştırma için yüzlerin kabaca hizalanması için) gereklidir. Düğüm noktaları, genellikle göz ve ağız kenarları, burun kanatları, burun ucu, burun ile alnın birleştiği yer ve çene ucudur. Bu noktaları genel olarak manual (Elle) bir şekilde işaretlemek mümkündür, dolayısı ile bu özellik sayesinde yüz tanıma sistemleri tamamen otomatik olmaktan çıkmaktadır (Kusban, 2021, Çeliktutan, 2013, Yun ve Guan, 2009). Aşağıdaki şekil 2.8'de yeniden yapılandırılmış bir üç boyutlu resim örneği yer almaktadır.



Şekil 2.8. Mona Lisa'nın Yeniden Yapılandırılmış 3 Boyutlu Yüzü

2.4.3. Karma Yüz Tanıma Sistemleri

Kalite olarak en iyi ve yüksek oranda sonuçların elde edilmesi bakımından karma yöntemlerin aynı anda kullanılarak uygulanmasıdır. Bu metodlar, özellik tabanlı ile görünüm tabanlı yüz tanıma sistemlerinin farklı kombinasyonlarından oluşan yöntemlerdir (Turhal, 2008).

2.4.3.1. Aktif İstatistiksel Yüz Modelleri

Aktif istatistiksel yüz modelleri, 1995 yılında Cootes tarafından aktif şekil modelleri olarak ifade edilen ve aşağıda belirtilen istatistiksel şekil modellerini birleştirirler.

A. PDM - Point Distribution Model (Nokta dağılım modeli): Bir nesnenin şekil ve şekil değişimlerini nokta topluluğu olarak saptar. Başka bir ifadeyle, bir dizi örnek şekillerden istatistiksel bir şekil ve şekil varyasyon modeli oluşturur. Ortalama şekil ve bir dizi varyasyon modu bu kümeden hesaplanabilir. Her mod, eğitim kümesindeki

şekillerin ortalamadan farklılık gösterme eğiliminde olduğu bir yolu tanımlar. Gerçek örnek kümelerini analiz ederek, şekil değişiminin kompakt bir açıklaması oluşturulabilir. Bu tür modeller, çok sayıda örnek mevcut olduğunda, ilgilenilen şekiller sınıfını en iyi şekilde temsil eder. Ancak, böyle bir seti elde etmek zor olabilir ve küçük bir küme üzerinde eğitilmiş bir PDM, makul şekillerin uzayını yeterince genişletmek için yeterli varyasyona izin vermeyebilir.

B. LGL - Local Gray-Level (Yerel gri düzeyi modeli): Noktalardaki değişimleri gri seviyesindeki değişimler olarak belirler (Cootes ve Taylor 2004).

2.4.3.2. Diğer Karma Yöntemler ve Çeşitli Kombinasyonlar.

2005 yılında Chev ve diğerleri tarafından, yüz görsellerin sınıflarını modellemek üzere gizli markov modelini kullanmıştır. Daha sonra gizli markov modelinde tahmin edilen her değişken için cüzi türev analizi yapılmış ve Fisher özdeğerleri hesaplanmıştır (Ali ve Ark., 2022). Daha sonra Fisher özdeğerleri geleneksel logaritmik olasılıklar ve görünüm tabanlı özellik setleri ile birleştirilmiştir. En nihayetinde elde edilen özellik vektörleri bir yüz modelinde barındırması gereken tüm lokal nicelikleri taşıyabilmektedir (Biswas ve Ark., 2022). Bu özellik vektörlerini yüz tanıma sistemlerinde kullanabilmek için LDA yöntemi uygulanır. Bu yöntem ile, tek başına HMM ya da yalnızca görünüm tabanlı özellik (Fisher) özvektörlerini kullanıldığında daha başarılı sonuçlar elde edilmiştir (Samaria, 1994).

Sonuç olarak bu çalışmada kullanılan yüz tanıma sistemleri, çeşitli kullanım senaryolarına göre farklı algoritmaları hibrit bir şekilde kullanılarak özelleştirilmiştir. Örnek vermek gerekirse gerçek zamanlı yüz tanıma, resim ve videodan yüz tanıma, kriminal bazlı yüz tanıma bu kullanım senaryolarından bazılarıdır. Özniteliklerin

ıkarılmasında kullanılan teknikler, teknolojik yenilikler bakımından, bu modellerin kullanılmasına dair artırıcı bir etki yapacaktır. zellikle, mobil grntleme cihazlarının yazılım ve teknolojilerindeki geliřmeler ile grntlerden gerek zamanlı olarak zniteliklerin elde edilebilmesi saėlanabilir noktaya gelir ve kullanılan modelin bařarımına katkıda bulunarak kullanım kolaylıėı saėlanacaktır. Ek olarak, grnt iřleme, yapay zeka ve makine ėrenim alanında yapılan alıřmaların etkisi; hem yz grntsn hem de z niteliklerini aynı anda elde edilebilmesinin yanı sıra tm yz grntsn kullanan grnm tabanlı model ve znitelik tabanlı sistemlerinin birlikte alıřmasıyla oluřturulan hibrit bir model gerek zamanlı ve ideal olmayan kořullarda sistemin daha bařarılı olmasını saėlamaktadır (Yıldız, 2021).

2.5. Yapay Zeka ve Derin ėrenme Algoritmaları

Yapay zeka terminolojisi; en basit ve yalın ifade ile yapay zeka (YZ), problem zme ve ėrenme gibi insan zihninin yaptığı iřlevleri taklit eden bir makine tarafından gsterilen zekadır. Bařka bir deyiřle YZ; grevleri yerine getirmek iin insan zekasını taklit eden ve toplanan verilere gre kendilerini geliřtirebilen sistem veya cihazları ifade eder.

Yapay zekanın temeli, Amerika Birleřik Devletlerinde 1956 yılında Dartmouth Kolejinde yapılan ve pek ok arařtırmacının katıldığı bilimsel bir kongre de atılmıştır. Yapay zeka; makine ėrenimi ve derin ėrenme olmak zere iki ayrı ana bařlıkta sınıflandırılmıştır (Doėan ve Trkoėlu, 2019).

Yapay zeka, makine ėrenme yntemlerine baėlı olup olmaksızın tahmin etmek ve karar vermek gibi faaliyetleri yapabilme kabiliyetine sahip olan teknolojiye verilen genel isimdir. Bu nedenle yapay zeka kendini farklı uygulama alanlarında eřitli řekillerde

gösterir. Örneğin, chatbotlar, müşteri sorunlarını daha hızlı anlamak ve daha verimli cevaplar sağlamak için yapay zeka kullanır. Ayrıca YZ, yüz tanıma sistemlerinde, büyük veri analizlerinde, sağlık ve bankacılık sektörlerinde, otonom araçlar (kendi kendini süren arabalar) gibi alanlarda kritik bilgi ve verilerin analiz edilmesinde kullanılmaktadır. Ek olarak YZ; arama motorları (Google arama motoru), öneri sistemleri gibi alanlarda da sıkça rastlanmaktadır (Karaküçük ve Eker, 2020, Bozüyük ve Ark., 2005).

Yapay zeka teknolojisi, bir zamanlar insan gücü gerektiren süreçleri veya görevleri otomatikleştirerek kurumsal performansı ve üretkenliği artırmaktadır. Onun için yapay zeka, belirli bir form veya işlevden ziyade verileri yüksek performansla analiz etme yeteneği ile ilgilidir. Bununla birlikte; YZ, dünyayı ele geçiren insan benzeri robotların görüntülerini sunsa da, insanların yerini alması amaçlanmamıştır. Fakat YZ; yalnızca insan yeteneklerini ve katkılarını önemli ölçüde artırmayı amaçlamaktadır (Kutucu, 2020).

Yüz tanımada; yapay zeka modelleri ve algoritmaları kullanılarak, olay yerinden alınan görüntülerin veritabanında kayıtlı olan görüntülerle sorgulanması yapılır. Sorgu sonucunda önerilen adaylarla ilgili adli bilişim uzmanlarına gerekli kararı vermede yardımcı olabilecektir.

Yapay zeka ve derin öğrenme algoritmaları günümüzde yüz tanıma teknolojisi alanında oldukça popüler bir araştırma alanı olarak karşımıza çıkmaktadır. Derin öğrenme algoritması, yüz tanıma uygulamaları içerisinde en sık kullanılan algoritmalarından biridir. Günümüz dünyasında suçların aydınlatılmasında ve teknik olarak suçluların tespit edilmesinde sıkça kullanılan yüz tanıma sistemleri sayesinde biyometrik kimliklendirme yapabilmek mümkün hale gelmiştir. Ayrıca suçlunun

kimliğinin ivedilikle tespit edilmesi ve doğru olan en erken zamanda çabucak ortaya çıkarılması, olası başka suçların işlenmesi önlenabilir veya önüne geçilmesi hedeflenebilir (Süzen ve Kayaalp, 2018).

Yapay zeka, bazı yüz tanıma işlemlerini derin öğrenme algoritmaları aracılığı ile gerçekleştirmektedir. Derin öğrenme, gizli katmanlardan meydana gelen, nicelik olarak değişebilen ve makine öğrenim algoritmalarını konu alan bir çalışma alanıdır. Derin öğrenme, komplike durumlar açısından gözlem yapabilen, analiz edebilen ve karar verme noktalarında insan zekası gibi davranabilme yeteneğine sahiptir. Derin öğrenme; aynı zamanda makine öğrenmesi olarak da adlandırılabilir (Pirim, 2006).

Derin öğrenme, öğrenme kabiliyeti sayesinde ham verileri işler, işlenen verileri anlamlı verilere dönüştürür. Örneğin, yüz tanıma, ses tanıma gibi bunlara benzer pek çok alan için örnek vermek mümkündür. Derin öğrenme, makine öğrenmenin bir alt çeşididir. Bu nedenle makine öğrenme algoritmalarını da kapsamaktadır. Derin öğrenme, yapay zekanın gelişiminde, pek çok şeyi algılamasında ve anlamasında yardımcı olan popüler bir yaklaşımdır. Nitekim bu alanda sosyal medya platformları (Facebook, Twitter vb.), Microsoft, Google gibi firmalar pek çok çalışma yapmaktadır (Bahar, 2021).

Derin öğrenme algoritmaları, yapısal yönden yapay sinir ağlarına benzediği için nöronların birbiri ile iletişim kurmasını sağlamaktadır. Nitekim yapay sinir ağları sistemlerinde nörona benzer yapılar, birbiri ile ilişki içerisinde. Bu da algoritmaların, bu şekilde öğrenmesini, bilgileri belleğe atmasını ve depolamasını, ilişkilendirme kapasitesine sahip olmasını düşündürmektedir (Gündüz ve Cedimoğlu, 2019).

Derin öğrenme algoritmaları, ham verileri ayırma özelliğine sahip olmasından dolayı işlenmemiş verileri işleme yeteneğinden yararlanarak öğrenir. Fakat bu konuda sistemin eğitilmiş olması elzemdir. Bunun içinde katmanlardan oluşan verilerin sınıflandırılması ve işlenmesi açısından bir hiyerarşi oluşumu gerekir. Bu da yararlı bilgilerden soyut verileri, somut hale dönüştürmede kullanılır (İnik ve Ülker, 2017).

Yüz tanıma, ses tanıma ve plaka tanıma sistemleri, iris ve parmak izi okuyucular, insansız araç kullanımı gibi alanlarda derin öğrenmenin kullanıldığını örnek göstermek mümkündür (Şeker ve Ark., 2017).

Sonuç olarak; yapay zeka, makine öğrenmesi ve derin öğrenme algoritmaları yüz tanıma sistemleri açısından gelecek için umut vaadeden, biyometrik kimliklendirme bakımından suçluların kimliğinin hızlı bir şekilde tespit edilmesinin yanısıra olayların çözümünde ve aydınlatılmasında yararlı ve faydalı olabilecek ileri teknolojik gelişmelere ışık olabilme yeteneğine sahiptir. Ancak bu konuda bir takım çalışmalara gereksinim vardır. Onun için yüz tanıma sistemleri bakımından; doğruluk, sensitivite, spesifisite, duyarlılık, güvenilirlik ve validite çalışmalarının arttırılması gerekmektedir (Bulut, 2020, Kaya ve Yıldız, 2014).

3. BULGULAR

3.1. Yüz Tanıma Sistemleri

Otomatik yüz tanıma sistemlerinin esası 1970’li yıllarda atılmış olsa da genel olarak yüz tanıma sistemlerinin geçmişı 1950’li yıllara dayanmaktadır. Papilon yüz tanıma sistemleri ise 2012 yılında Papilon Savunma Teknoloji ve Ticaret A. Ş. tarafından geliştirilen ticari bir yüz tanıma yazılımıdır (Mengüç ve Acır, 2022).

Günümüzde, teknolojinin ilerlemesi ve gelişmesi ile birlikte biyometrik sistemlerin özellikle de yüz tanıma sistemlerinin kullanımı üzerindeki araştırmaların hızla arttığı görülmektedir. Hatta öyle ki yüz verilerinin kullanımı üzerinde pek çok çalışma yapılmış ve yapılmaktadır. Bu da son zamanlarda yüz tanıma en çok çalışılan alanlardan biri haline gelmiştir (Aksoy, 2019).

Yüz ve yüz özellikleri en temel biyometrik özelliklerdendir. Nitekim bu özellikler aracılığı ile yüz tanıma sistemlerini kullanarak kişilerin kimliği ve cinsiyet tespiti, yaş aralık tahmini, duygudurumu hakkında fikir sahibi olmak artık çok kolaydır (Mamak ve Ark., 2020).

Yüz tanıma sistemleri, görüntü ve video tabanlı olmak üzere iki temel sınıfa ayrılmaktadır. Görüntü tabanlı sistemlere baktığımızda, bireylerin anlık fiziki görünümelerini kullanmak üzere bir tanımlama yaparken, video tabanlı sistemler ise;

görüntü tabanlı özelliğın yanında birde görünümledeki değışikliklerden ve yüz hareketlerinden de faydalanmak mümkündür.

Yüz tanımanın yaygın kullanımına bakıldığında, yüz tanımanın güvenlik amaçlı olarak kullanımının en etkin olduđu karşımıza çıkmaktadır. Onun için araştırmamızda iki çeşit yüz tanıma yöntemi benimsenmiştir; bu yöntemler, kriminal inceleme amaçlı fotoğraftan fotoğrafa sorgulama yöntemi ve kent güvenlik yönetim sisteminde kullanılan canlı yüz tanıma yöntemidir (Yılmazer ve Solak, 2021).

Bu çalışmada her iki kullanım yönteminin de seçili uygulamalar üzerinden sahadaki kullanımlarının sonuçları ve yapılan testlerden elde edilen verilerin analizleri paylaşılacaktır. Birinci yöntemde, kriminal inceleme amaçlı filtreleme yöntemi ile sayısallaştırılmış verilerin hem otomatik hem de kullanıcı tarafından işaretlenmesine bağılı görüntü kalitesinden bağımsız bir şekilde suç ve suçlunun tespitini kapsar. İkinci yöntemde ise, canlı kamera görüntüleri üzerinden bir kara listede aranan kişilerin veya tespitine ihtiyaç duyulan kişilerin anlık olarak kameradan görüntü analizini kapsar. Dolayısı ile etkin bir kamu güvenliği projesinde bu iki yöntemin ayrı ayrı veya bir arada kullanılmasına yönelik tavsiye ve öneriler de bulunulacaktır (Ebrahimpour ve Ark., 2022).

3.1.1. Kriminal İnceleme Amaçlı Fotoğraftan Fotoğrafa Sorgulama Yöntemi

Çalışmayı oluşturmak amacıyla piyasada bulunan bir uygulama seçilmesi ve analizin bu uygulama üzerinden yapılması gerekmektedir. Bu amaçla incelemede Papiion yüz tanıma sistemi kullanılmıştır. Bu sistem öncelikle bir fotoğraf havuzu oluşturur, tespit edilmiş ve tespit edilmemiş fotoğrafları bir arada arşivler ve sorgulama yapar. Sistemin çalışma prensibini daha açık bir ifade ile vurgulamak gerekirse;

herhangi bir fotoğrafın diğer fotoğraflar içerisinde sorgulamasını yapma esasına dayanmaktadır. Ek olarak, bu uygulama kullanıcıya, tanımlayıcı özellik noktalarına ve tanımlayıcı bilgilerine müdahale etmesine imkân sağlar.

Sistemin genel prensip özelliklerinden ve işleyiş mekanizmasından bahsetmemiz gerekirse; yüz tanıma sistemi veri analizi kapsamında yürütülen bu çalışma, Massachusetts Institute of Technology (MIT) ve FEI Face Database veri setleri kullanılmıştır. Linux İşletim Sistemi, Intel (R) Core (TM) i7-4790 CPU @ 3.60 GHz., ön bellek boyutu 8192 KB, 500 Gigabyte SSD nitelikli belleği olan masaüstü bilgisayarda kurulu Papilon yüz tanıma (fotoğraftan fotoğrafa sorgulama) sistemi, sürüm 3.1.0 – 3.20.1 uygulaması sayesinde yapılan deneyler sonucunda yüz tanıma (özellik tabanlı, görünüm tabanlı ve karma) yöntemleri, yapay zeka ve derin öğrenme algoritmaları kullanılarak yapılan analiz ve test sonuçları değerlendirilmiş olup performans ölçümleri incelenmiştir.

Test çalışmalarına başlamadan önce kullandığımız uygulama olan Papilon yüz tanıma sistemin genel işleyişine ve tasarım materyaline baktığımızda, demografik veri ve fotoğraf girişi, veri görüntüleme, kodlama, sorgulama, aday listesi kontrolü ve kimlik tespiti aşamalarından oluşmaktadır.

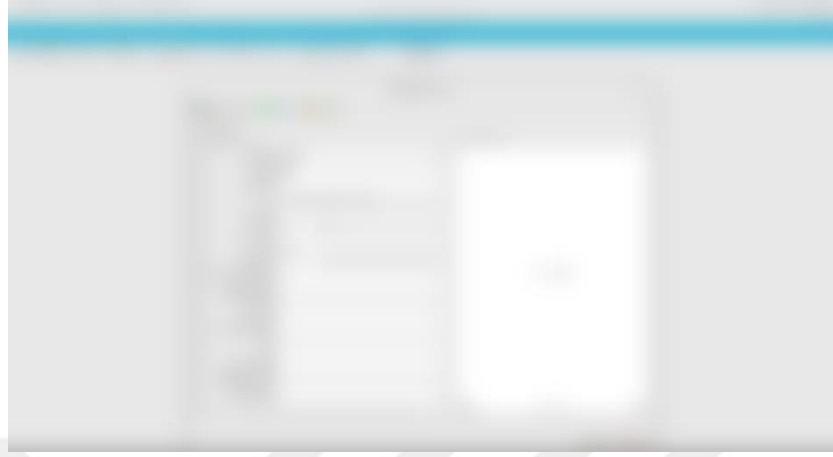
Bu sistem, Papilon Savunma Teknoloji ve Ticaret A. Ş. tarafından geliştirilen ticari bir yüz tanıma yazılımıdır. Papilon yüz tanıma sistemi, yapay zeka ve derin öğrenme algoritmalarını kullanarak kimlik tespiti için verilere doğrudan uygulanabilen bir yüz tanıma sistemidir.

Bu sistem, dosya yönetim sistemi formatına sahiptir. Veriler uc birimlerde sayısallaştırılıp veri tabanına gönderilmektedir. Adli bilişim uzmanları tarafından kimlik tespiti yapılan şahış ve/veya şahısların mahkemelere delil olarak sunulması için sistemden görsel olarak Ekspertiz Raporu almakta mümkündür. Aşağıdaki şekil 3.1’de Papilon yüz tanıma sistemin giriş ekranı gösterilmiştir.



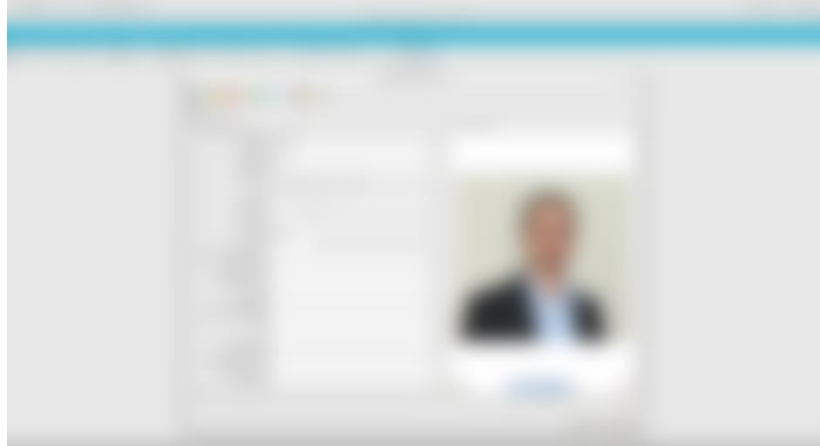
Şekil 3.1. Papilon Polyface Sistemin Giriş Ekran Görüntüsü

Demografik veri ve fotoğraf giriş modülü: Bu modülde kimliği belli olan kişilerin adı-soyadı, kimlik numarası, profil fotoğrafı ve diğer kişisel bilgileri yer alırken, kimliği belli olmayan kişilerinse, fotoğrafı, olay yeri, olay tarihi, varsa tanık bilgileri gibi bilgiler yer almaktadır. Şekil 3.2’de Demografik veri ve fotoğraf giriş modülün şematizası gösterilmiştir.



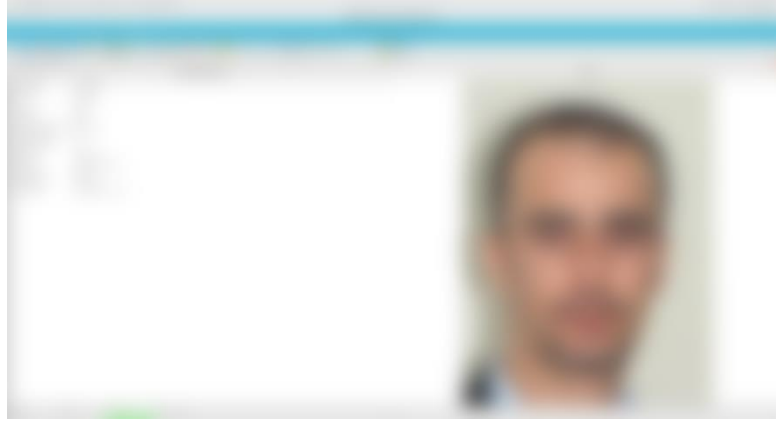
Şekil 3.2. Demografik Veri ve Fotoğraf Giriş Modül Ekranı

Yukarıdaki şekil 3.2’de görüldüğü üzere sağ tarafta demografik veriler yer alırken, programın sol tarafında ise kişinin fotoğrafı yer almaktadır. Örnek şekil 3.3’te gösterilmiştir.



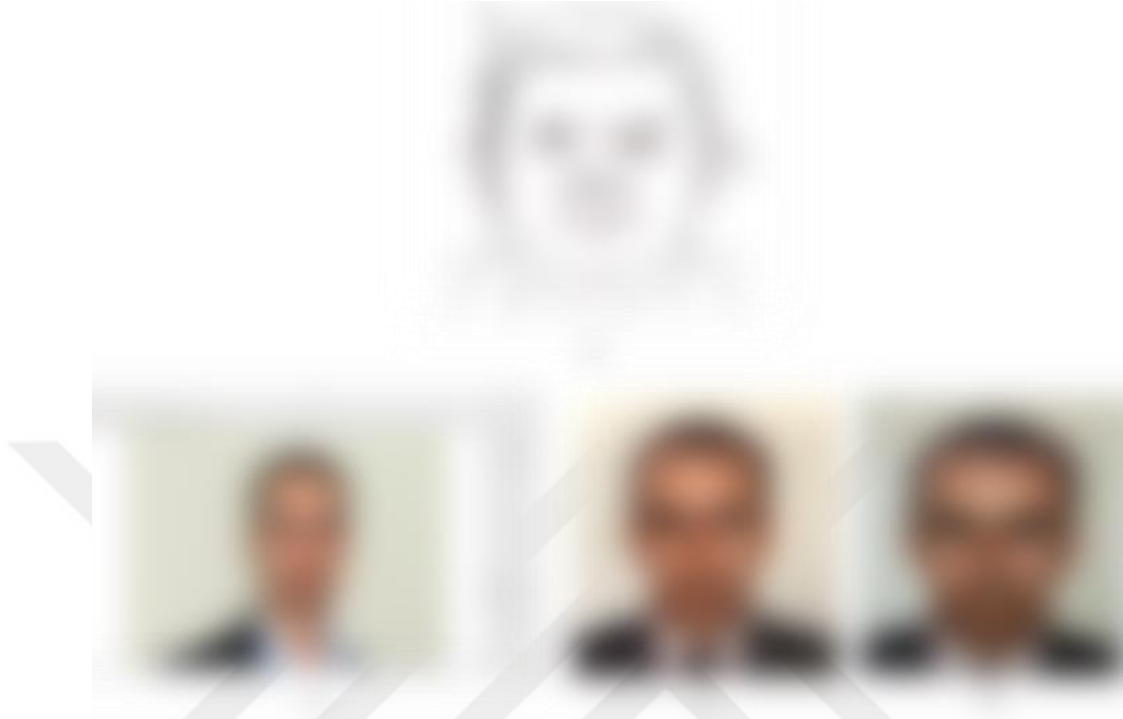
Şekil 3.3. Örnek Demografik Veri ve Fotoğraf Giriş Modül Ekranı

Veri görüntüleme Modülü: Veriseti içerisinde bulunan şahısların fotoğrafı varsa demografik bilgileri sistemde sorgulama yapıldığında görüntülenir. Aşağıdaki şekil 3.4’te olduğu gibi.



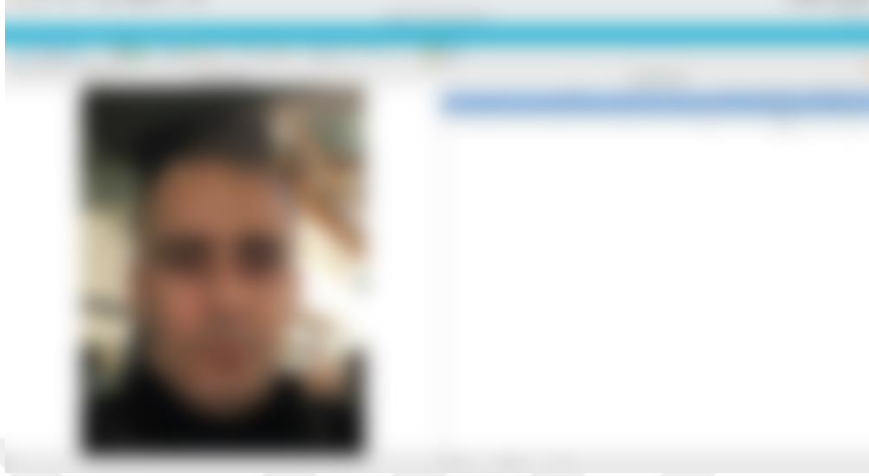
Şekil 3.4. Veri Görüntüleme Modülü

Kodlama Modülü: Bu modülde kişi veya kişilerin antropolojik olarak adlandırılan noktaları fiducial points (referans noktaları) metodu kullanılarak kodlama işlemi yapılır. Burada dikkat edilmesi gereken en önemli husus, göz bebekleri sistem tarafından otomatik olarak kodlandırılrsa da uzman kişiler tarafından manual olarak kontrol edilmesi gerekmektedir, çünkü göz bebeği noktaları; yaşa, estetik gibi operasyonel işlemlere bakmaksızın stabilitesini yüksek ölçüde korumaktadır. Diğer noktalar (örneğin gözlerin birbirine olan uzaklığı, burun genişliği, göz çukurunun derinliği, elmacık kemiğinin şekli, çene kemiğinin uzunluğu vb. noktalar) sistematik olarak kodlanır. Aşağıdaki şekil 3.5’te olduğu gibi bu noktalar sayısal ölçütlerle kodlanır, bu kodlara da yüz izi denir.



Şekil 3.5. A. Antropolojik Noktaların Kodlama Şablonu, B. Polyface Kodlama Modülü, C. Antropolojik Olarak Göz bebeklerin Sistem Tarafından Otomatik Kodlanması; D. Antropolojik Olarak Diğer Noktaların Sistem Tarafından Otomatik Kodlanması

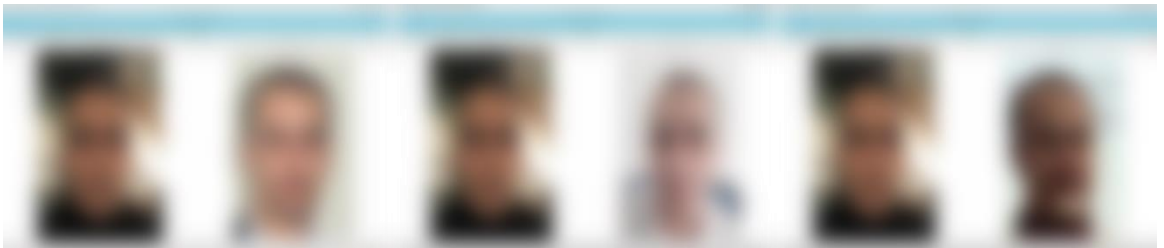
Sorgulama Modülü: kimlik tespiti için demografik veri girişi ve fotoğraf eklenip kodlama işlemi gerçekleştirildikten sonra dosya uç birimlerde sayısallaştırılıp veri setine gönderilir. Burada sayısallaştırma işlemindeki temel amaç, hem veri güvenliğini sağlamak hem de veri tabanındaki işlem yükünü hafifleterek sorgu sonuçlarını saniyeler içerisinde getirmeyi sağlamaktır. Sorgu sonucunda aday listesi oluşturulup potansiyel adayların eşleşmesi en yüksek puandan en düşük puana doğru sıralanmış olur. Aşağıdaki şekil 3.6’da olduğu gibi.



Şekil 3.6. Sorgulama Modülü

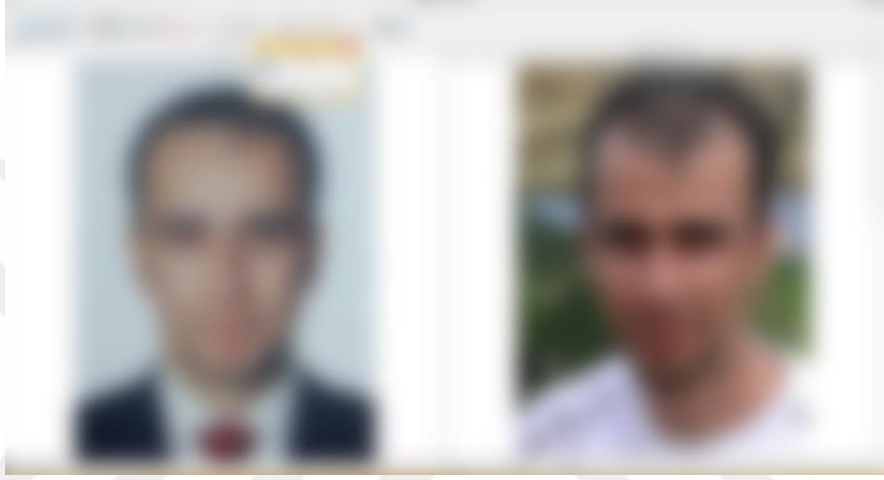
Aday listesi kontrolü: veritabanına yeni bir görsel eklendikten sonra sistem potansiyel eşler için (yüz görüntüsündeki sayısallaştırılmış özellikleri karşılaştırarak verinin benzerliğine göre) otomatik veritabanı araması başlatır ve aday listelerini oluşturur. Potansiyel adaylar sorgu sonucunda eşleşme skoruna göre listelenir.

Eşleşme skoru, iki görsel arasındaki benzerliğin sayısal ölçümüdür. Sayısal değerler, 1'den 10,000'e kadar değişmektedir. Eşleşme skoru ne kadar yüksek olursa, eşleşme olasılığı da o dererece yüksek olur. Adaylar, aday listesinde eşleşme skorlarına göre azalan şekilde sıralanırlar. Şekil 3.7'de olduğu gibi.



Şekil: 3.7. Aday Listesi Kontrolü

Kimlik Tespiti: sistem tarafından otomatik olarak getirilen potansiyel adaylar, uzmanlar tarafından kontrol edilir. Daha sonra benzerlik durumuna göre aynı (hit) kararı verilerek kimlik tespiti yapılmış olur. Aşağıdaki şekil 3.8’de olduğu gibi.



Şekil 3.8. Sorgu Sonuçların Mukayesesi ve Kimlik Tespit Ekranı

3.1.2. Kent Güvenlik Yönetim Sisteminde Kullanılan Canlı Yüz Tanıma Yöntemi

Canlı yüz tanıma teknolojisi; kontrolsüz dış ortamda ve kapalı kontrollü alanlarda kullanılmakta olan bir yüz tanıma ve tespit sistemidir. Bu teknolojinin; kontrolsüz dış ortam kullanımına bakıldığında; kent güvenlik yönetim sisteminde ve akıllı şehirlerde kullanılmaktadır. Kapalı kontrollü alanlardaki kullanımına örnek vermek gerekirse, havalimanlarından metro istasyonlarına, özel işletmelerden kamu kuruluşlarına kadar pek çok yerde kullanılmaktadır (Kün ve Ark., 2014).

Canlı yüz tanıma sistemlerinin kullanılabilirliğini değerlendirmek amacıyla kontrollü iç ortamda (kapalı kontrollü alanda) Papilyon yüz tanıma sisteminin

performans ölçümü yapılmıştır. Bu da kameradan alınan anlık görüntüler üzerinde gerçekleştirilmiştir (Ebrahimpour ve Ark., 2022).

Ancak bu noktada hayati öneme sahip olan bir kriter söz konusudur. Bu kriter; canlı yüz tanıma sistemlerin kapalı kontrollü alanlardaki başarı oranı, kontrolsüz dış ortamlara göre daha yüksek olmasıdır. Bunun temel nedeni; canlı yüz tanımanın kontrolsüz dış ortam kullanımını etkileyecek pek çok faktörden kaynaklı ileri gelmektedir. Bu faktörler; çevresel (güneş ışığı, olumsuz hava şartları vb.) faktörler, kameranın konumu ve yüksekliği gibi faktörlerden olumsuz etkilenmektedir.

Canlı yüz tanıma sistemleri aracılığı ile aranmakta olan hedef kişilerin tespiti, sistem tarafından otomatik olarak yapılmaktadır (şekil 3.9). Ek olarak canlı yüz tanıma sistemleri, hem kapalı kontrollü alanlarda hem de kontrolsüz dış ortamda 90 derecelik açıya kadar yüz tespiti yapma kabiliyetine sahiptir.



Şekil 3.9. Canlı Yüz Tanıma Sistemleri Aracılığıyla Aranılan Kişilerin Tespiti

Sonuç olarak; yüz tanıma sistemini kent güvenlik yönetim sistemine veya havalimanı kamera izleme sistemine entegre edilmesi halinde istihbarat amaçlı olarak

kesin tespit edici özelliğinden, kriminal inceleme ve Adli bilişimde ise kameradan yüz tanıma önleyici tespit edici faktöründen yararlanmakta fayda vardır (Şeker, 2009).

3.2. Gerçekleştirilen Testler ve Yapılan Analizler

3.2.1. Fotoğraftan Fotoğrafa Yapılan Sorgu Analizleri

Çalışmamızda kullanılmak üzere 20 bin denek yüz görüntüsü toplandı. Analiz ve test için toplanan bu görüntüler önce sisteme yüklendi, ardından sistem tarafından otomatik kodlama ve sorgulama işlemi yapıldı. Analizler için çeşitli senaryolar oluşturuldu. Bu senaryolar aşağıdaki çizelge 3.1’de özetlenmiştir. Ayrıca otomatik kodlamaya karşı elverişsiz görüntülerin manuel kodlama işlemi de yapıldı.

Çizelge 3.1. Fotoğraftan Fotoğrafa Yapılan Sorgu Sonuçları

Yapılan Testler	Yapılan Sorgu Senaryoları	Eşleşme Skoru	Aday Listesindeki Sıralama
Test 1	Ön Profil - Ön Profil	9910	Birinci Sırada
Test 2	Ön Profil - 45 Derecelik Sol Aç	9057	İkinci Sırada
Test 3	Ön Profil - 45 Derecelik Sağ Aç	9920	İkinci Sırada
Test 4	45 Derecelik Sağ Aç - 45 Derecelik Sol Aç	9968	Birinci Sırada
Test 5	45 Derecelik Sol Aç - 45 Derecelik Sağ Aç	9897	Birinci Sırada
Test 6	Ön Profil (Gözlüklü) - Ön Profil (Gözlüksüz)	9576	Birinci Sırada
Test 7	Ön Profil (Gözlüksüz) - Ön Profil (Gözlüklü)	9931	Birinci Sırada
Test 8	Ön Profil - 45 Derecelik Sol Aç (Gözlüklü)	9677	Birinci Sırada
Test 9	Ön Profil - 45 Derecelik Sağ Aç (Gözlüklü)	9636	Birinci Sırada
Test 10	Farklı Duygudurum Profili	9691	Birinci Sırada
Test 11	Ön Profil - Ön Profil (Karanlık Görüntülü)	8822	Birinci Sırada
Test 12	Farklı Yaş Profili	6736	Birinci Sırada
Test 13	Ön Profil Sakalsız - Ön Profil Sakallı (Ancak Düşük Çözünürlüklü Kalitesiz Görüntü İle Farklı Yaş Profili)	5844	Birinci Sırada
Test 14	Ön Profil – Ön Profil (Ancak Düşük Çözünürlüklü Görüntü)	5107	Beşinci Sırada
Test 15	Ön Profil (Maskeli) – Ön Profil (Maskesiz)	6414	Birinci Sırada

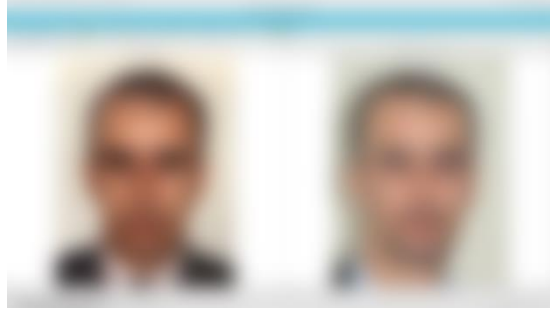
Çizelge 3.1. (devam) Fotoğraftan Fotoğrafa Yapılan Sorgu Sonuçları

Test 16	Ön Profil (Maskeli & Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz)	5588	Birinci Sırada
Test 17	Ön Profil (Maskeli & Güneş Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz)	5111	Birinci Sırada
Test 18	Ön Profil (Maskeli & Gözlüklü & Şapkalı) – Ön Profil (Maskesiz & Gözlüksüz & Şapkasız)	5310	Birinci Sırada
Test 19	Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Gözlüksüz & Şapkasız)	5024	Üçüncü Sırada
Test 20	45 Derecelik Sağ Aç (Maskeli & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Şapkasız)	5719	Birinci Sırada
Test 21	Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Maskeli & Gözlüklü & Şapkasız)	5173	Üçüncü Sırada
Test 22	Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - 45 Derecelik Sağ Aç (Maskeli & Gözlüksüz & Şapkalı)	5080	Beşinci Sırada
Test 23	Diğer Test ve Senaryo Analizleri: Otomatik Kodlama İşlemi ile Manuel Kodlama İşlemi Karşılaştırması		

Yukarıdaki çizelge 3.1’de yapılan testlerin ve kurgulanan senaryoların veri analizleri açıklamaları ile birlikte aşağıda kapsamlı bir şekilde ele alınmıştır.

1. Test: Ön Profil – Ön Profil Sorgu Senaryosu

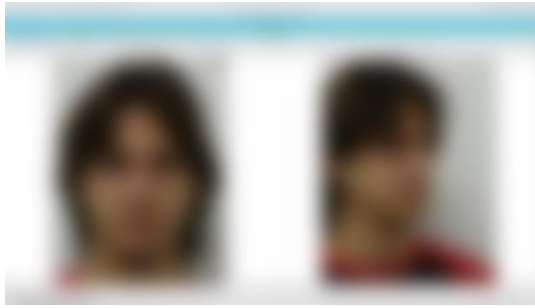
Bu test ve senaryo analizinde ön profil – ön profil sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9910 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.10’da) birinci sırada gelmiştir.



Şekil 3.10. Ön Profil – Ön Profil Sorgu Sonucu

2. Test: Ön Profil - 45 Derecelik Sol Açılış Sorgu Senaryosu

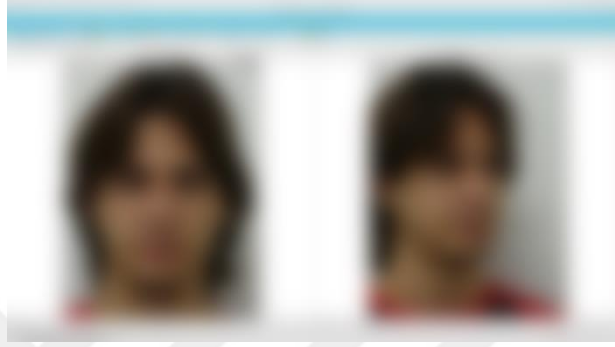
Bu test ve senaryo analizinde ön profil – 45 derecelik sol açılış sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9057 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.11’de) ikinci sırada gelmiştir.



Şekil 3.11. Ön Profil - 45 Derecelik Sol Açılış Sorgu Sonucu

Buradaki en önemli husus; yapılan test ve senaryo analizi sonucunda birinci sırada gelen aday da yine aynı aday olup ancak fotoğraf açısının (45 dereceden düşük) farklı olması nedeniyle aday birinci sırada gelmiştir. Çünkü sistemin çalışma özelliklerinden birisi açısal bakımdan adayların sıralamasını ön profilden hareketle 90 derecelik açıya doğru sıralamaktadır. Bu nedenle de sistem adayın aşağıdaki (şekil 3.12’de) görselini

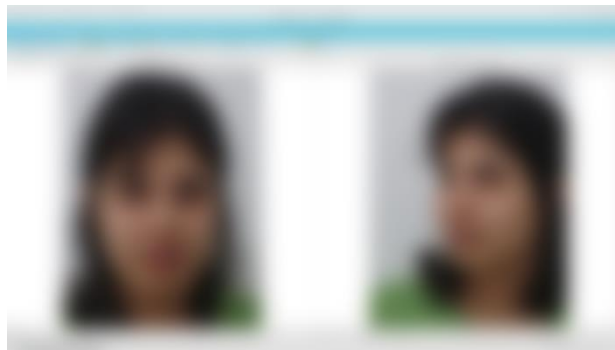
eşleşme skoru olarak 10.000 puan üzerinden 9883 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru adayı birinci sırada gelmiştir.



Şekil 3.12. Ön Profil - 45 Dereceden Düşük Sol Açılış Sorgu Sonucu

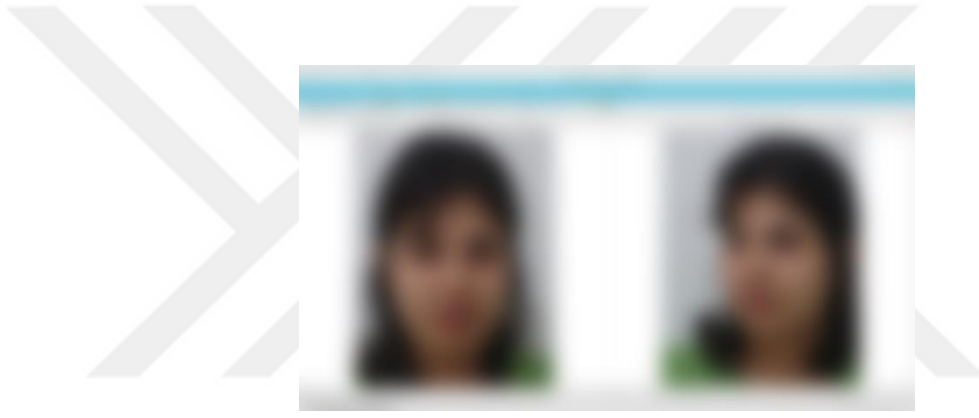
3. Test: Ön Profil – 45 Derecelik Sağ Açılış Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil – 45 derecelik sağ açılış sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9920 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.13'te) ikinci sırada gelmiştir.



Şekil 3.13. Ön Profil – 45 Derecelik Sağ Açılış Sorgu Sonucu

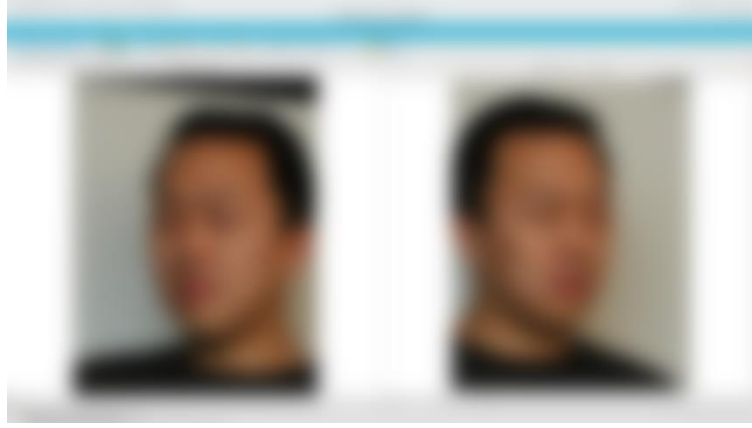
Buradaki en önemli husus; yapılan test ve senaryo analizi sonucunda birinci sırada gelen aday da yine aynı aday olup ancak fotoğraf açısının (45 dereceden düşük) farklı olması nedeniyle aday birinci sırada gelmiştir. Çünkü sistemin çalışma özelliklerinden birisi açısal bakımdan adayların sıralamasını ön profilden hareketle 90 derecelik açıya doğru sıralamaktadır. Bu nedenle de sistem adayın aşağıdaki (şekil 3.14'te) görselini eşleşme skoru olarak 10.000 puan üzerinden 9981 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru adayı birinci sırada gelmiştir.



Şekil 3.14. Ön Profil - 45 Dereceden Düşük Sağ Açılı Soru Sonucu

4. Test: 45 Derecelik Sağ Açılı - 45 Derecelik Sol Açılı Soru Senaryosu

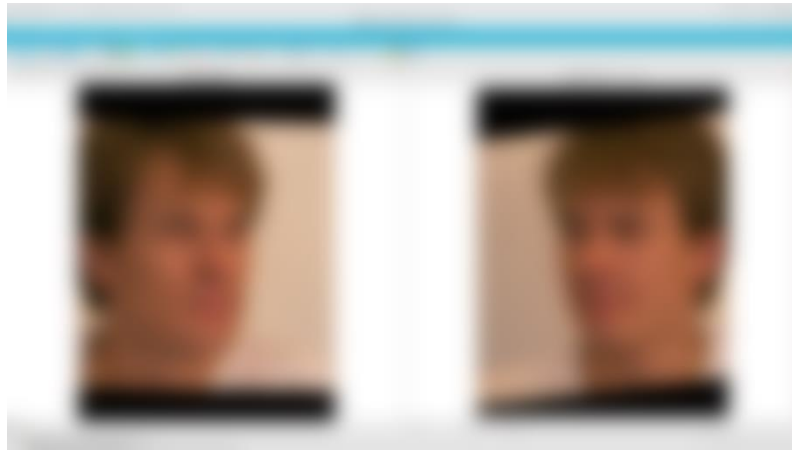
Bu test ve senaryo analizinde 45 derecelik sağ açılı - 45 derecelik sol açılı sorgulaması yapılmıştır. Soru sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9968 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.15'te) birinci sırada gelmiştir.



Şekil 3.15. 45 Derecelik Sağ Aç - 45 Derecelik Sol Aç Sorgu Sonucu

5. Test: 45 Derecelik Sol Aç - 45 Derecelik Sağ Aç Sorgu Senaryosu

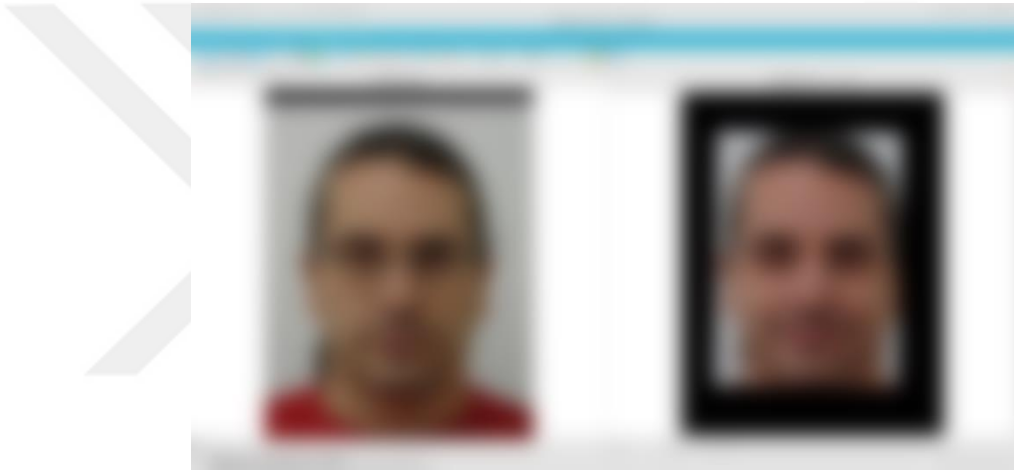
Bu test ve senaryo analizinde 45 derecelik sol aç - 45 derecelik sağ aç sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9897 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.16'da) birinci sırada gelmiştir.



Şekil 3.16. 45 Derecelik Sol Aç - 45 Derecelik Sağ Aç Sorgu Sonucu

6. Test: Ön Profil (Gözlüklü) - Ön Profil (Gözlüksüz) Sorgu Senaryosu

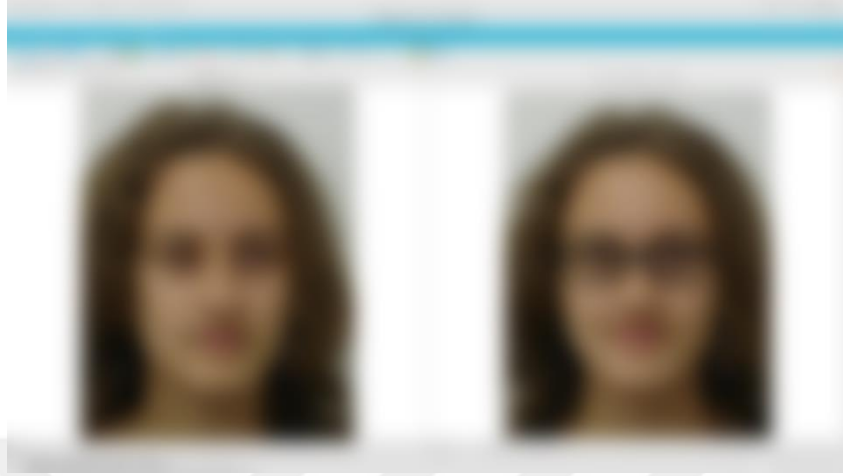
Bu test ve senaryo analizinde ön profil (gözlüklü) - ön profil (gözlüksüz) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9576 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.17’de) birinci sırada gelmiştir.



Şekil 3.17. Ön Profil (Gözlüklü) - Ön Profil (Gözlüksüz) Sorgu Sonucu

7. Test: Ön Profil (Gözlüksüz) - Ön Profil (Gözlüklü) Sorgu Senaryosu

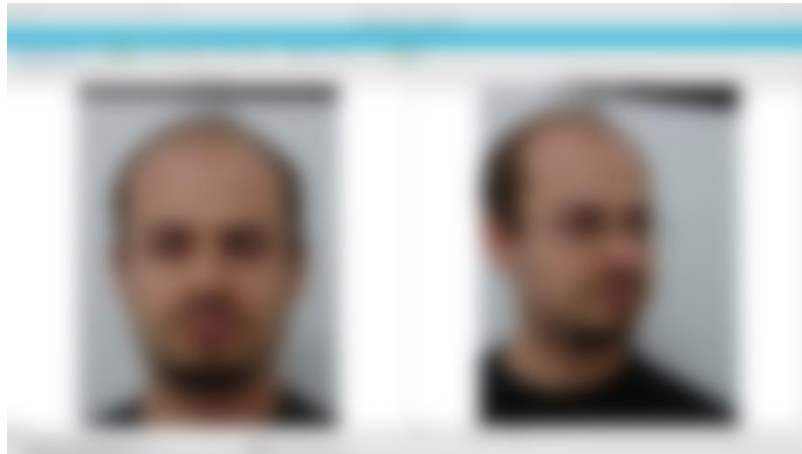
Bu test ve senaryo analizinde ön profil (gözlüksüz) - ön profil (gözlüklü) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 9931 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.18’de) birinci sırada gelmiştir.



Şekil 3.18. Ön Profil (Gözlüksüz) - Ön Profil (Gözlüklü) Sorgu Sonucu

8. Test: Ön Profil - 45 Derecelik Sol Aç ı (Gözlüklü) Sorgu Senaryosu

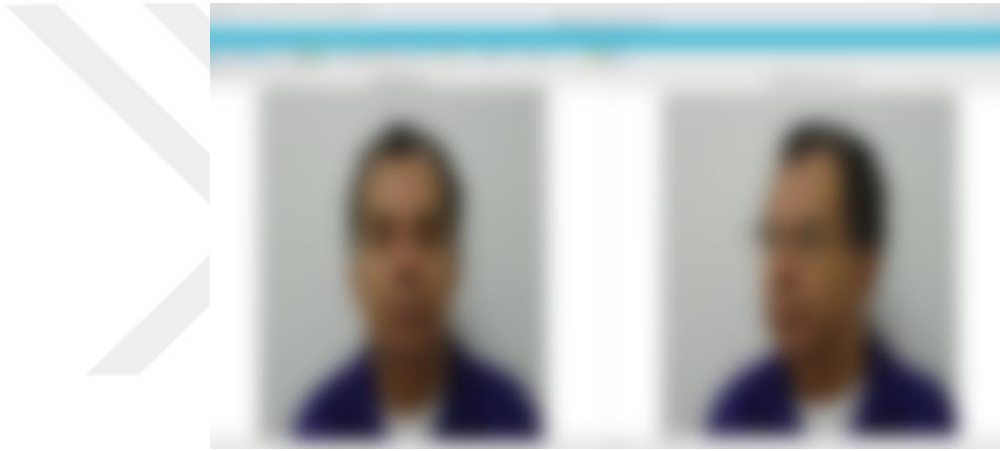
Bu test ve senaryo analizinde ön profil - 45 derecelik sol aç ı (gözlüklü) sorgulamas ı yapılmı ştır. Sorgu sonucuna bakıldı ğında eşleşme skoru 10.000 puan üzerinden 9677 puan benzerli ği ile aday listesindeki sıralama sonucuna göre do ğru aday (Şekil 3.19’da) birinci sırada gelmi ştir.



Şekil 3.19. Ön Profil - 45 Derecelik Sol Aç ı (Gözlüklü) Sorgu Sonucu

9. Test: Ön Profil - 45 Derecelik Sağ Aç ı (Gözlüklü) Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil - 45 derecelik sağ aç ı (gözlüklü) sorgulamas ı yapılmıřtır. Sorgu sonucuna bakıldıđında eşleşme skoru 10.000 puan üzerinden 9636 puan benzerliđi ile aday listesindeki sıralama sonucuna göre dođru aday (Şekil 3.20’de) birinci sırada gelmiřtir.



Şekil 3.20. Ön Profil - 45 Derecelik Sağ Aç ı (Gözlüklü) Sorgu Sonucu

10. Test: Farklı Duygudurum Profili Sorgu Senaryosu

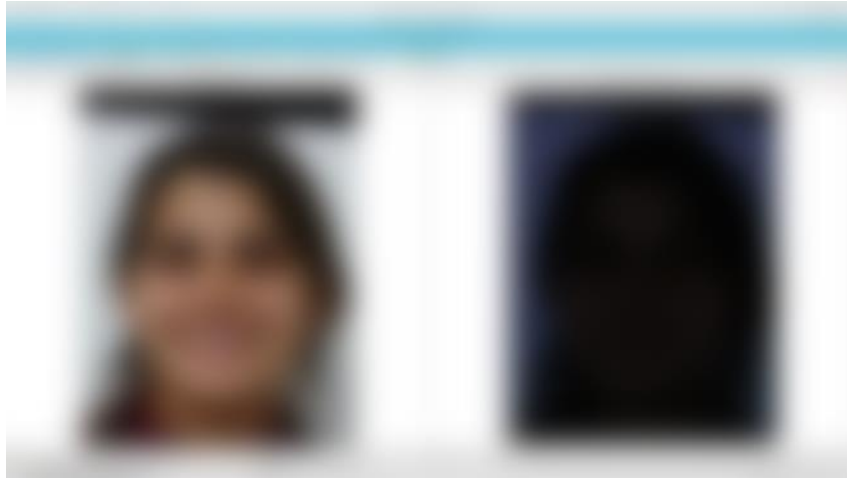
Bu test ve senaryo analizinde farklı duygudurum profili sorgulamas ı yapılmıřtır. Sorgu sonucuna bakıldıđında eşleşme skoru 10.000 puan üzerinden 9691 puan benzerliđi ile aday listesindeki sıralama sonucuna göre dođru aday (Şekil 3.21’de) birinci sırada gelmiřtir.



Şekil 3.21. Farklı Duygudurum Profili Sorgu Sonucu

11. Test: Ön Profil - Ön Profil (Karanlık Görüntülü) Sorgu Senaryosu

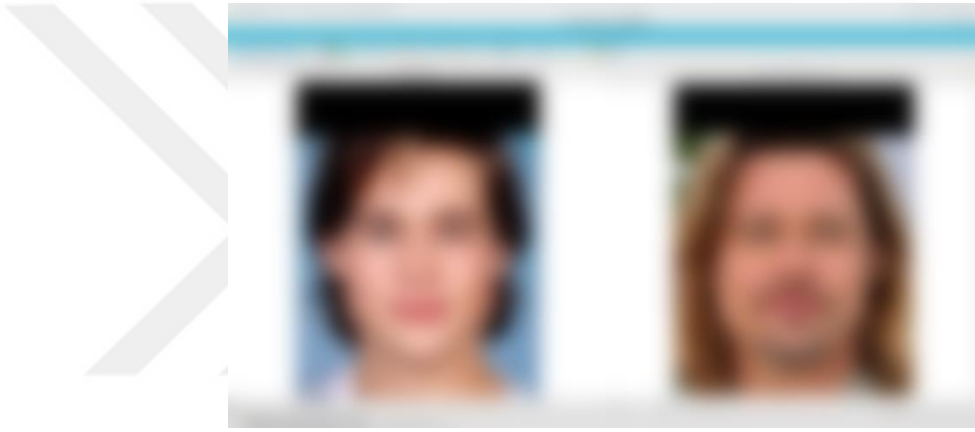
Bu test ve senaryo analizinde ön profil - ön profil (karanlık görüntülü) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 8822 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.22’de) birinci sırada gelmiştir.



Şekil 3.22. Ön Profil - Ön Profil (Karanlık Görüntülü) Sorgu Sonucu

12. Test: Farklı Yaş Profili Sorgu Senaryosu

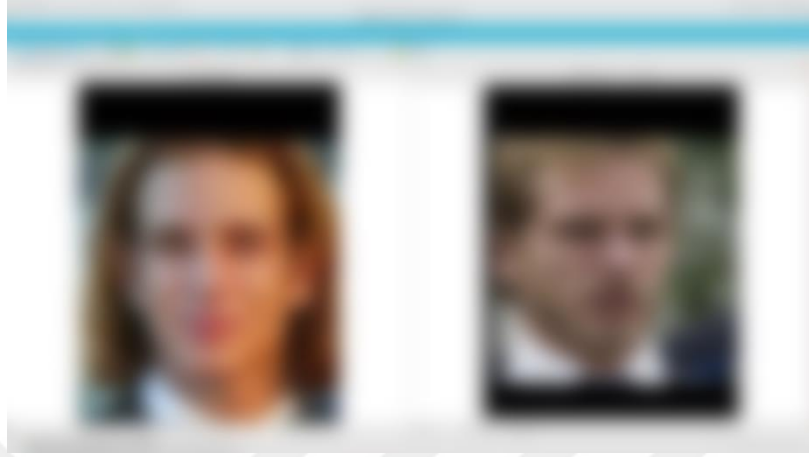
Bu test ve senaryo analizinde farklı yaş profili sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 6736 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.23'te) birinci sırada gelmiştir.



Şekil 3.23. Farklı Yaş Profili Sorgu Sonucu

13. Test: Ön Profil (Sakalsız) – Ön Profil (Sakallı) Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil (sakalsız) – ön profil (sakallı) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5844 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.24'te) birinci sırada gelmiştir. Buradaki benzerlik puanının düşük olmasının sebebi, görsellerin düşük çözünürlüğe sahip kalitesiz görüntü ile iki fotoğraf arasındaki farklı yaş profilinden ileri gelmektedir.

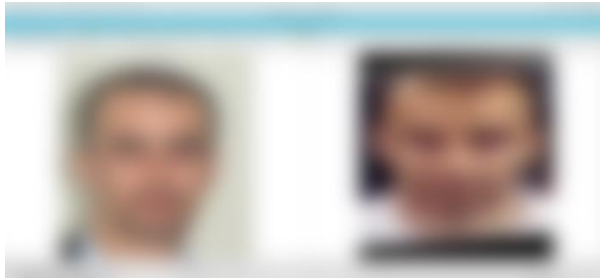


Şekil 3.24. Ön Profil (Sakalsız) – Ön Profil (Sakallı) Sorgu Sonucu

14. Test: Ön Profil – Ön Profil (Düşük Çözünürlüklü Görüntü) Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil – ön profil (düşük çözünürlüklü görüntü) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5107 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.25'te) beşinci sırada gelmiştir.

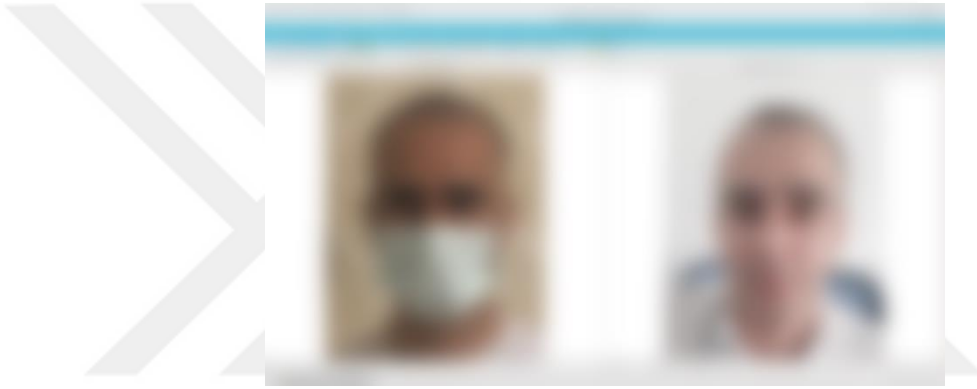
Burada benzerlik puanının düşük olması ve adayın beşinci sırada gelmesinin nedeni karşılaştırılan fotoğrafın hem düşük çözünürlüğe sahip olması hem de bu adayın sistemde kayıtlı olan daha kaliteli görsellerin olmasından kaynaklı ileri gelmektedir.



Şekil 3.25. Ön Profil – Ön Profil (Düşük Çözünürlüklü Görüntü) Sorgu Sonucu

15. Test: Ön Profil (Maskeli) – Ön Profil (Maskesiz) Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil (maskeli) – ön profil (maskesiz) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 6414 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.26'da) birinci sırada gelmiştir.



Şekil 3.26. Ön Profil (Maskeli) – Ön Profil (Maskesiz) Sorgu Sonucu

16. Test: Ön Profil (Maskeli & Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Senaryosu

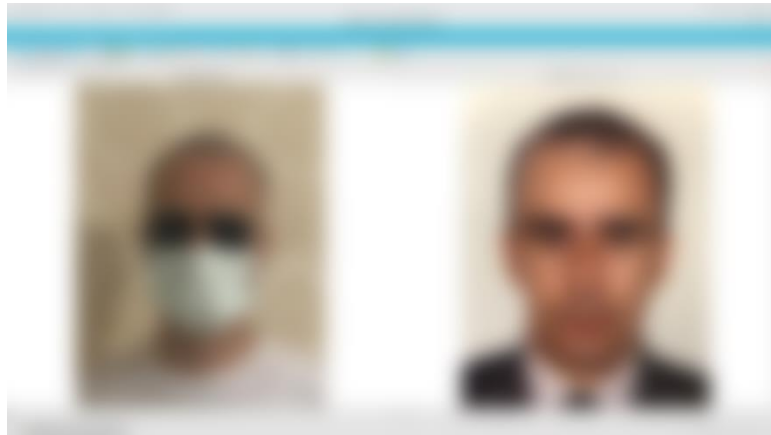
Bu test ve senaryo analizinde ön profil (maskeli & gözlüklü) – ön profil (maskesiz & gözlüksüz) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5588 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.27'de) birinci sırada gelmiştir.



Şekil 3.27. Ön Profil (Maskeli & Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Sonucu

17. Test: Ön Profil (Maskeli & Güneş Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Senaryosu

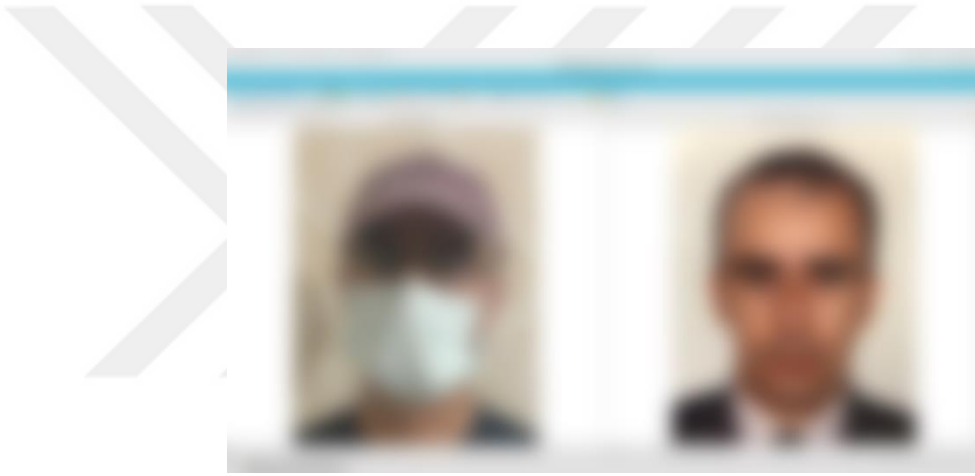
Bu test ve senaryo analizinde ön profil (maskeli & güneş gözlüklü) – ön profil (maskesiz & gözlüksüz) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5111 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.28’de) birinci sırada gelmiştir.



Şekil 3.28. Ön Profil (Maskeli & Güneş Gözlüklü) – Ön Profil (Maskesiz & Gözlüksüz) Sorgu Sonucu

18. Test: Ön Profil (Maskeli & Gözlüklü & Şapkalı) – Ön Profil (Maskesiz & Gözlüksüz & Şapkasız) Sorgu Senaryosu

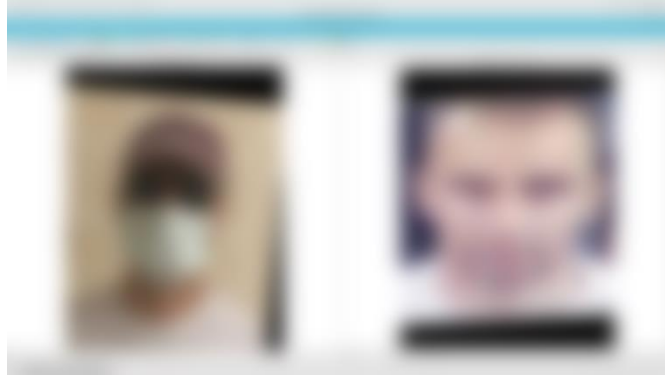
Bu test ve senaryo analizinde ön profil (maskeli & gözlüklü & şapkalı) – ön profil (maskesiz & gözlüksüz & şapkasız) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5310 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.29’da) birinci sırada gelmiştir.



Şekil 3.29. Ön Profil (Maskeli & Gözlüklü & Şapkalı) – Ön Profil (Maskesiz & Gözlüksüz & Şapkasız) Sorgu Sonucu

19. Test: Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Gözlüksüz & Şapkasız) Sorgu Senaryosu

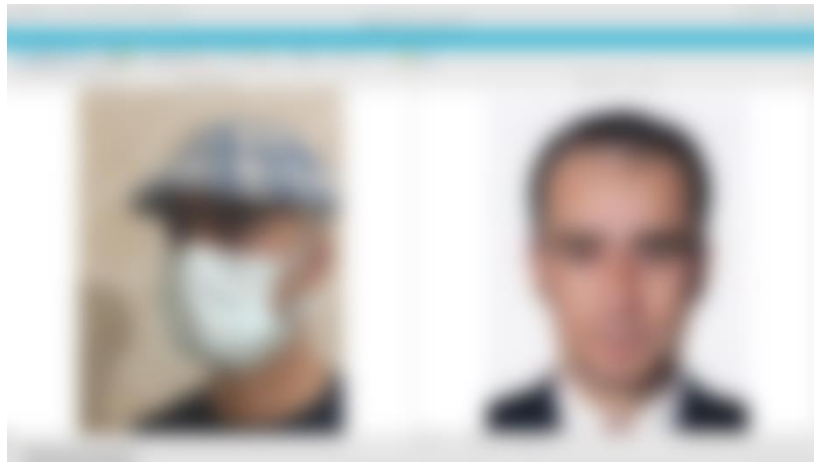
Bu test ve senaryo analizinde ön profil (maskeli & güneş gözlüklü & şapkalı) - ön profil (düşük çözünürlüklü görüntü: maskesiz & gözlüksüz & şapkasız) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5024 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.30’da) üçüncü sırada gelmiştir.



Şekil 3.30 Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Gözlüksüz & Şapkasız) Sorgu Sonucu

20. Test: 45 Derecelik Sağ Açılı (Maskeli & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Şapkasız) Sorgu Senaryosu

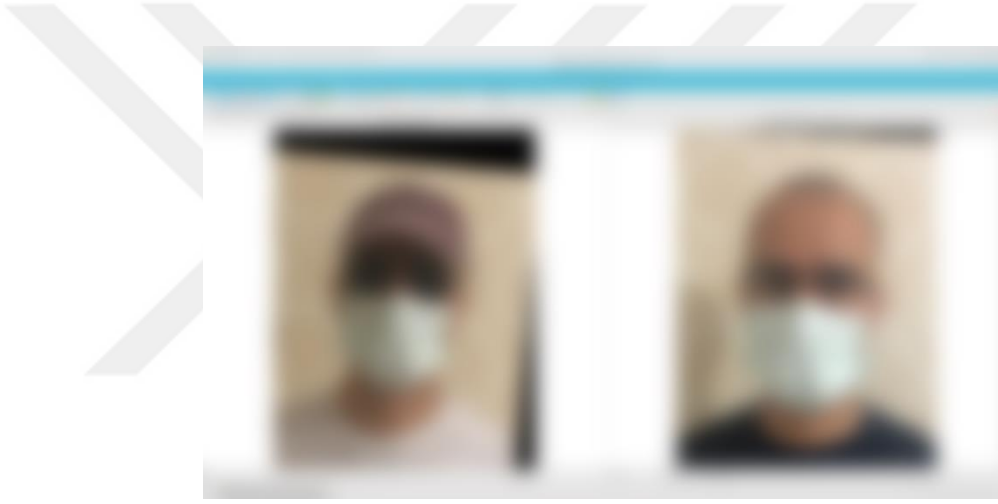
Bu test ve senaryo analizinde 45 derecelik sağ açılı (maskeli & şapkalı) - ön profil (düşük çözünürlüklü görüntü: maskesiz & şapkasız) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5719 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.31’de) birinci sırada gelmiştir.



Şekil 3.31. 45 Derecelik Sağ Açılı (Maskeli & Şapkalı) - Ön Profil (Düşük Çözünürlüklü Görüntü: Maskesiz & Şapkasız) Sorgu Sonucu

21. Test: Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Maskeli & Gözlüklü & Şapkasız) Sorgu Senaryosu

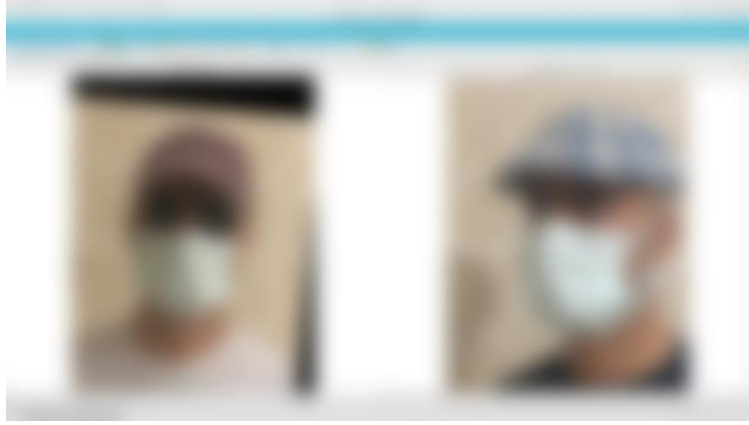
Bu test ve senaryo analizinde ön profil (maskeli & güneş gözlüklü & şapkalı) - ön profil (maskeli & gözlüklü & şapkasız) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5173 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.32’de) üçüncü sırada gelmiştir.



Şekil 3.32. Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - Ön Profil (Maskeli & Gözlüklü & Şapkasız) Sorgu Sonucu

22. Test: Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - 45 Derecelik Sağ Açılı (Maskeli & Gözlüksüz & Şapkalı) Sorgu Senaryosu

Bu test ve senaryo analizinde ön profil (maskeli & güneş gözlüklü & şapkalı) - 45 derecelik sağ açılı (maskeli & gözlüksüz & şapkalı) sorgulaması yapılmıştır. Sorgu sonucuna bakıldığında eşleşme skoru 10.000 puan üzerinden 5080 puan benzerliği ile aday listesindeki sıralama sonucuna göre doğru aday (Şekil 3.33’te) beşinci sırada gelmiştir.



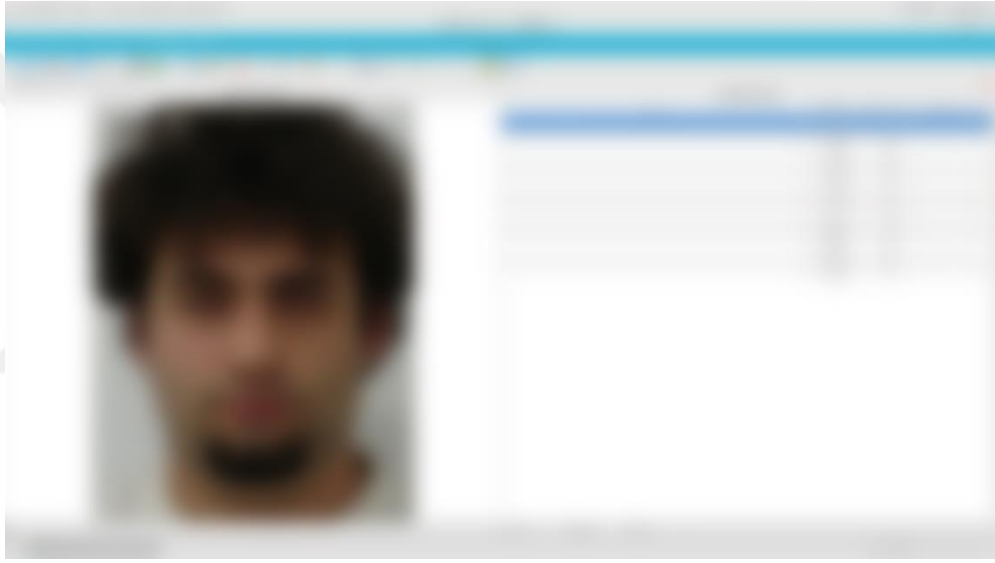
Şekil 3.33. Ön Profil (Maskeli & Güneş Gözlüklü & Şapkalı) - 45 Derecelik Sağ Açı (Maskeli & Gözlüksüz & Şapkalı) Sorgu Sonucu

23. Diğer (Otomatik Kodlama ile Manuel Kodlama) Sorgu Senaryoları

Aşağıdaki çizelge 3.2’de denek bir kişiye ait 14 adet farklı açılardan çekilmiş görüntüler, otomatik ve manuel kodlama işlemine tabii tutularak elde edilen tespit sonuçlarının mukayesesi yer almaktadır. Otomatik kodlama işleminde 90 derecelik açı ile çekilen bir görüntünün tespit imkanını sağlamazken, manuel kodlama işlemi yaparak 90 derecelik açılardan çekilmiş görüntülerin tespit imkanı sağlandığı görülmüştür. Örneğin çizelge 3.2’de yer alan kart numaraları 52-10 ve 52-01 olan verilerine ait sorgu sonuçları verilmiştir. Otomatik ve manuel kodlama işlemi aşağıda ele alınmıştır.

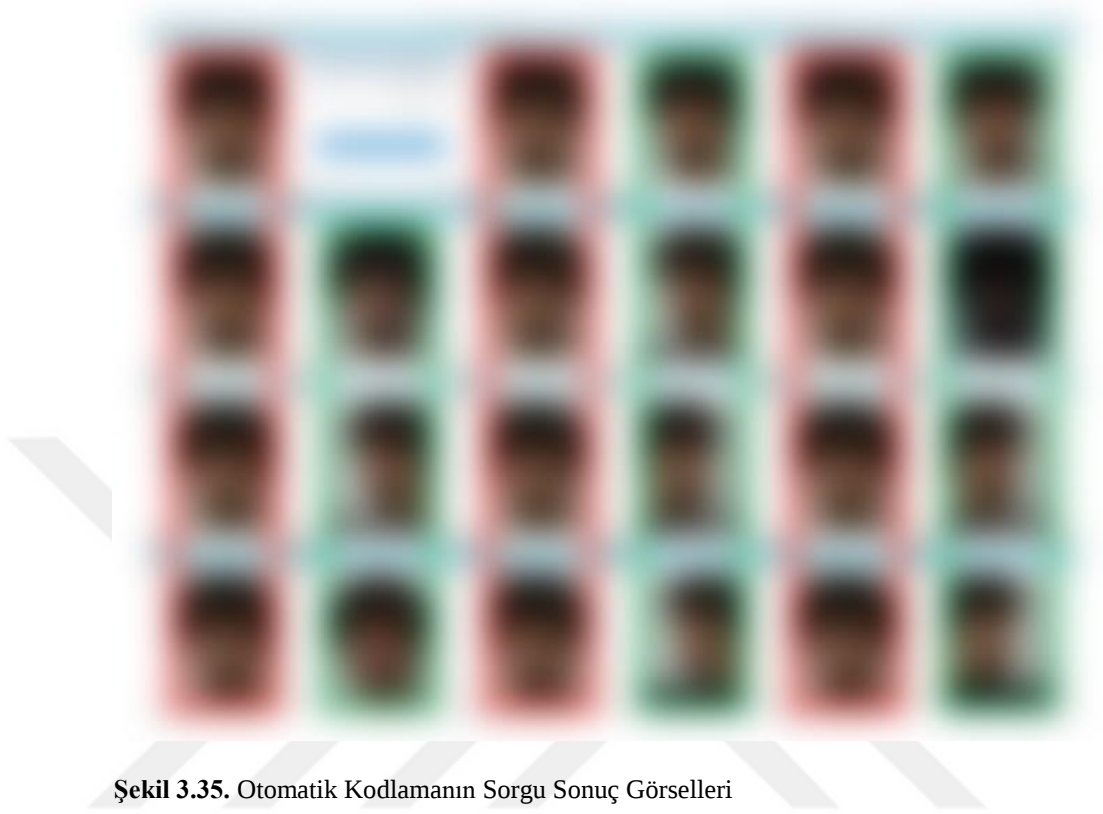
1. Otomatik Kodlama

Denek bir kişiye ait 14 adet farklı açılardan çekilmiş görüntüler sisteme yüklendi. Daha sonra otomatik kodlama ve sorgulama yapıldı. Yapılan otomatik kodlama ve sorgu sonucuna bakıldığında aday listesinde 11 doğru aday geldiği görülmüştür (çizelge 3.2’de, şekil 3.34’te).



Şekil 3.34. Otomatik Kodlama Sorgu Sonuç Aday Listesi

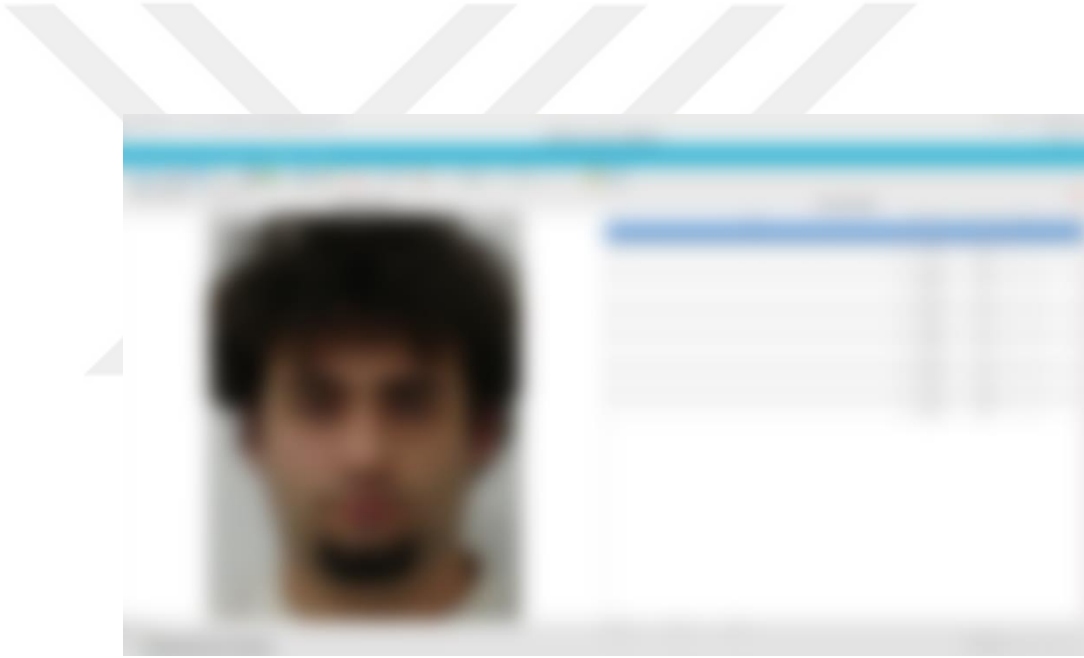
Otomatik kodlama yaparak aday listesinde 11 doğru aday gelmiştir. Doğru adayların eşleşme skoru 10.000 puan üzerinden farklı puan benzerlikleri ile sıralama sonucuna bakıldığında görsellerin çözünürlüğüne, kalitesine ve çekilen açılara göre yüksek puandan düşük puana doğru sıralanmıştır (şekil 3.35’te).



Şekil 3.35. Otomatik Kodlamanın Sorgu Sonuç Görselleri

2. Manuel Kodlama

Araştırmacı tarafından manuel kodlama yapıp sorgu sonucuna bakıldığından aday listesinde 13 doğru adayın geldiği görülmüştür (çizelge 3.2’de). Burada otomatik kodlama ile manuel kodlama arasındaki en önemli fark, manuel kodlama adayların 90 derecelik açıdan çekilmiş görüntülerini bile getirme kabiliyetine sahiptir. Aynı zaman olay yerinden elde edilen düşük çözünürlüğe sahip kalitesiz görüntüleri de aynı şekilde manuel kodlama yaparak doğru sonuç elde etmek mümkündür (şekil 3.36’da).



Şekil 3.36. Manuel Kodlama Sorgu Sonuç Aday Listesi

Manuel kodlama yaparak aday listesinde 13 doğru aday gelmiştir. Doğru adayların eşleşme skoru 10.000 puan üzerinden farklı puan benzerlikleri ile sıralama sonucuna bakıldığında görsellerin çözünürlüğüne, kalitesine ve çekilen açılara göre yüksek puandan düşük puana doğru sıralanmıştır (şekil 3.37’de).



Şekil 3.37. Manuel Kodlamanın Sorgu Sonuç Görselleri

Sonuç olarak hem otomatik hemde manuel kodlamada, kırmızı kutucuk içerisindeki fotoğraf sorgulanmıştır. Sorgulama sonucunda yeşil kutucuk içerisindeki fotoğraflar aday listesinde aday olarak gelmiştir. Otomatik kodlamada 11 aday gelirken manuel kodlamada 13 adayın geldiği görülmüştür.

Çizelge 3.2. Otomatik Kodlama İşlemi ile Manuel Kodlama İşlemi Karşılaştırması

Otomatik Kodlama işlemi			Manuel Kodlama işlemi		
Kart Numarası	Eşleşme Skoru	Aday Listesindeki Sıralama	Kart Numarası	Eşleşme Skoru	Aday Listesindeki Sıralama
52-05.jpg	9999	1. Sıra	52-05.jpg	9999	1. Sıra
52-06.jpg	9997	2. Sıra	52-06.jpg	9997	2. Sıra
52-13.jpg	9994	3. Sıra	52-13.jpg	9994	3. Sıra
52-04.jpg	9986	4. Sıra	52-04.jpg	9984	4. Sıra
52-14.jpg	9972	5. Sıra	52-14.jpg	9972	5. Sıra
52-03.jpg	9950	6. Sıra	52-03.jpg	9947	6. Sıra
52-07.jpg	9921	7. Sıra	52-07.jpg	9921	7. Sıra
52-08.jpg	9433	8. Sıra	52-08.jpg	9964	8. Sıra
52-09.jpg	9278	9. Sıra	52-12.jpg	9200	9. Sıra
52-12.jpg	9200	10. Sıra	52-02.jpg	9151	10. Sıra
52-02.jpg	9154	11. Sıra	52-09.jpg	9089	11. Sıra
			52-10.jpg	6181	12. Sıra
			52-01.jpg	5925	13. Sıra

52-05 numaralı kartın sorgu sonucu hem otomatik kodlamada hemde Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9999 puan benzerliğiyle doğru aday, aday listesinde birinci sırada gelmiştir.

52-06 numaralı kartın sorgu sonucu hem otomatik kodlamada hemde Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9997 puan benzerliğiyle doğru aday, aday listesinde ikinci sırada gelmiştir.

52-13 numaralı kartın sorgu sonucu hem otomatik kodlamada hemde Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9994 puan benzerliğiyle doğru aday, aday listesinde üçüncü sırada gelmiştir.

52-04 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9984 puan benzerliğiyle gelirken, Manuel kodlamada eşleşme skoru

10.000 puan üzerinden 9986 puan benzerliđiyle her iki aday da sorgu sonucu aday listesinde dördüncü sırada gelmiştir.

52-14 numaralı kartın sorgu sonucu hem otomatik kodlamada hemde Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9972 puan benzerliđiyle doğru aday, aday listesinde beşinci sırada gelmiştir.

52-03 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9950 puan benzerliđiyle gelirken, Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9947 puan benzerliđiyle her iki aday da sorgu sonucu aday listesinde altıncı sırada gelmiştir.

52-07 numaralı kartın sorgu sonucu hem Otomatik kodlamada hemde Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9921 puan benzerliđiyle doğru aday, aday listesinde yedinci sırada gelmiştir.

52-08 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9433 puan benzerliđiyle gelirken, Manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9964 puan benzerliđiyle her iki aday da sorgu sonucu aday listesinde sekizinci sırada gelmiştir.

52-09 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9278 puan benzerliđiyle dokuzuncu sıra da gelirken, manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9089 puan benzerliđiyle on birincil sırada gelmiştir.

52-12 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9200 puan benzerliğiyle onuncu sıra da gelirken, manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9200 puan benzerliğiyle dokuzuncu sırada gelmiştir.

52-02 numaralı kartın sorgu sonucu otomatik kodlamada eşleşme skoru 10.000 puan üzerinden 9154 puan benzerliğiyle on birinci sıra da gelirken, manuel kodlamada eşleşme skoru 10.000 puan üzerinden 9151 puan benzerliğiyle onuncu sırada gelmiştir.

52-02 numaralı kartın sorgu sonucu otomatik kodlama işlemi yapıldığında aday listesinde aday gelmez iken, manuel kodlama işlemi yapıldığında eşleşme skoru 10.000 puan üzerinden 6181 puan benzerliğiyle on ikinci sırada gelmiştir.

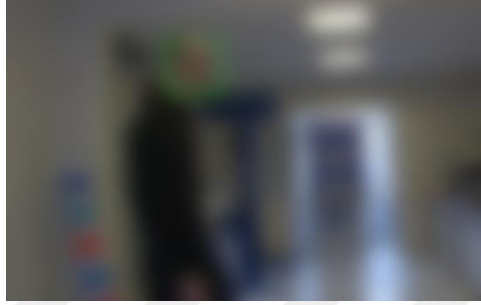
52-01 numaralı kartın sorgu sonucu otomatik kodlama işlemi yapıldığında aday listesinde aday gelmez iken, manuel kodlama işlemi yapıldığında eşleşme skoru 10.000 puan üzerinden 5925 puan benzerliğiyle on üçüncü sırada gelmiştir.

3.2.2. Canlı Yüz Tanımadan Yapılan Sorgu Analizleri

Canlı yüz tanıma sisteminin önceliği, tanıma ve tespit edilmesi istenilen kişi ve/veya kişilerin fotoğrafları, sistemin verisetine kaydedilmesi gerekmektedir.

Canlı yüz tanıma sistemi, KGYS veya havalimanı güvenlik kameralarına entegre edilmesi halinde, aranan kişi ve/veya kişilerin canlı kameralar karşısından geçmesi

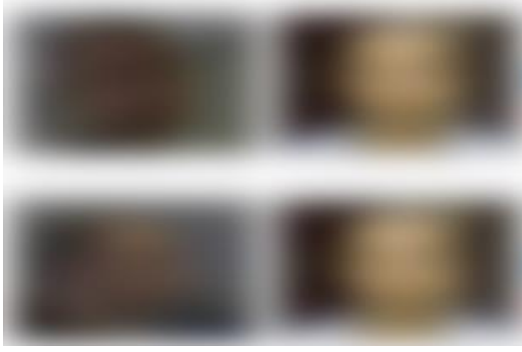
durumunda öncelikle aranan kişilerin yüzün algılanması yapılır. Aşağıdaki şekil 3.38’de olduğu gibi (Şeker, 2009).



Şekil 3.38. Canlı Kameradan Alınan Anlık Yüz Algılanma Görüntüsü

Algılanan bu yüzler sistemin verisetinde kayıtlı olan mevcut tüm fotoğraflar ile karşılaştırması yapılır. Bu işlem karmaşık algoritmalar aracılığı ile saniyeler içerisinde gerçekleşmektedir.

Karşılaştırma sonucunda bir eşleşme söz konusu olduğunda kişinin tanımlanması ve tespiti yapılmış olur aşağıdaki şekil 3.39’da olduğu gibi sol taraftaki fotoğraflar canlı kameradan anlık alınmış görüntüler olup sağ taraftaki fotoğraflar ise, sistemin verisetinde kayıtlı olan mevcut görsellerdir. Tespit edilen kişi ile ilgili sistem tarafından anlık olarak güvenlik güçlerine kırmızı kod aranma alarmı gönderilir.



Şekil 3.39. Tanımlama ve Tespit Görselleri

Canlı yüz tanıma sistemin özelliklerinden bir tanesi, sisteme yüklenen görsellerin kodlanması sistem tarafından otomatik olarak yapıldığı için kullanıcılara herhangi bir manuel kodlama imkanı vermez (Ebrahimpour ve Ark., 2022).

Sonuç olarak; anlık bir şekilde canlı kameradan alınan görüntüler ile sistemin verisetine kayıtlı görsellerin karşılaştırılması yapıp herhangi bir eşleşme söz konusu olduğu takdirde, aranan kişilerin tanımlanması ve tespit edilmesi yapılır. Örnek test sonuçları yüzde eşleşme oranları ile birlikte aşağıdaki şekil 3.40'ta gösterilmiştir.



Şekil 3.40. Canlı Yüz Tanımada Yapılan Sorgu Sonuçları

3.3. Test Sonuçlarının Değerlendirilmesi ve Yorumlanması

Yüz tanıma teknolojisi, en yaygın kullanılan biyometrik yöntemlerden biridir. Temassız biyometrik analiz sunmakla birlikte kolay erişilebilirdir. Ayrıca ek donanım gerektirmez (Vazquez-Fernandez ve Gonzalez-Jimenez, 2016). Bu nedenle bu teknoloji son yıllarda kullanım açısından oldukça yaygın bir şekilde kullanılmaktadır (Adjabi ve Ark., 2020).

Yüz tanıma sistemi, bir kişinin kimliğini, yüzün fizyolojik özelliklerine dayalı olarak tanımlamak veya doğrulamak için akıllı yöntemler kullanan bir tür biyometrik sistemdir.

Yüz tanıma sistemleri, görüntü tanıma ve karşılaştırma algoritmalarından oluşur. Bu algoritmaların temeli, bireylerde göz, burun, yanak gibi yüz organlarının boyutu, şekli ve konumu ile ilgili özelliklerin analizine dayanmaktadır (Vazquez-Fernandez ve Gonzalez-Jimenez, 2016).

Yüz tanıma sistemlerinin, suçluların tespiti, kimlik kartları, pasaport ve kredi kartı sahiplerinin doğrulanması, bankalar, mağazalar ve havaalanlarında biyometrik kontrol gibi birçok uygulaması bulunmaktadır (Adamek ve Ark., 2015).

Yüz tanıma sistemlerinde fotoğraftan fotoğrafa sorgulama yapıldığında; yaş farkı, farklı açılardan çekilmiş görüntüler, çözünürlüğü düşük görüntü, saç, sakal, güneş ve tıbbi gözlük kullanımı, şapka ve maske kullanımı gibi faktörler sorgu sonuçlarını etkilemediğini yapılan analizler sonucunda görülmüştür.

Kriminal incelemelerde ve adli bilişim vakalarında her zaman olay yerinden alınan görüntüler biyometrik veya ön profil fotoğrafları olmayabilir. Nitekim yüz fotoğraflarının güvenlik kameralarından, kamu veya özel kurum veya kuruluşlardaki ya da sokaklardaki kameralardan veya KGYS kameralardan elde edilmiş olması muhtemeldir. Bu da görüntü kalitesinin çok düşük olması anlamına gelmektedir. Dolayısıyla bu tip fotoğrafları, manuel kodlama yeteneğini kullanarak tespit yüzdesi arttırılır, bu da olayların çözülmesine yönelik büyük katkı sunmaktadır.

Yapılan test senaryolarına ve sorgu sonuçlarına baktığımızda; ilk olarak dikkat edilmesi gerekli ve öncelikli olan hususiyet, ilk veritabanı oluşturma aşamasında kimliği bilinen kişilerin fotoğraflarını sisteme kaydederken ön profil ve biyometrik fotoğraf olmasına dikkat edilmelidir. Bunun esas nedeni; sisteme ne kadar yüksek kalitede ve çözünürlükte bir fotoğraf kaydedilirse, adli vakalarda olay yerinden elde edilen fotoğrafla sorgulaması yapıldığı zaman, sorgu sonuçlarının yüksek eşleşme skoru ile adayın birinci sırada gelmesi söz konusu olduğu gibi yüksek başarı oranıyla da neticelenmesinde rol oynar. Bunu da bulgular bölümünde gerçekleştirdiğimiz test sonuçlarında görmek mümkün.

Bu noktada, ön profil (normal) - ön profil (normal), ön profil - 45 derecelik (sağ - sol) açılardan çekilmiş fotoğraflar, 45 derecelik sağ açı - 45 derecelik sol açı veya bunların tersi, ön profil (gözlüklü) - ön profil (gözlüksüz) veya bunların tersi, ön profil - 45 derecelik sağ açı (gözlüklü), ön profil - 45 derecelik sol açı (gözlüklü) ve farklı duygudurum profilli (gülmek - somurtmak gibi) gibi görsellerin sorgu sonuçları ve eşleşme skorları 10.000 puan üzerinden 9000 puan skala dolayısı ve üzerinde bir benzerlikle doğru adayın aday listesinde birinci sırada geldiği açıkça görülmüştür.

Ön profil (aydınlık görüntü) - ön profil (karanlık görüntü), farklı yaş profilleri (gençlikte çekilen fotoğraf ile ileri yaşta çekilen fotoğraf gibi), ön profil (maskeli) - ön profil (maskesiz), ön profil (sakalsız) – ön profil (sakallı) fakat burada düşük çözünürlüklü, kalitesiz görüntü ile farklı yaş profil söz konusu, ön profil (normal) - ön profil (normal) ancak düşük çözünürlüklü görüntü, ön profil (maskeli - gözlüklü) - ön profil (maskesiz - gözlüksüz), ön profil (maskeli - güneş gözlüklü) - ön profil (maskesiz - gözlüksüz), ön profil (maskeli - gözlüklü - şapkalı) - ön profil (maskesiz - gözlüksüz - şapkasız), ön profil (maskeli - güneş gözlüklü - şapkalı) - ön profil (maskesiz - gözlüksüz - şapkasız), ön profil (maskeli - güneş gözlüklü - şapkalı) - ön profil (düşük çözünürlüklü görüntü: maskesiz - gözlüksüz - şapkasız), 45 derecelik sağ açı (maskeli -

şapkalı) - ön profil (düşük çözünürlüklü görüntü: maskesiz - şapkasız), ön profil (maskeli - güneş gözlüklü - şapkalı) – ön profil (maskeli - gözlüklü - şapkasız), ön profil (maskeli - güneş gözlüklü - şapkalı) – 45 derecelik sağ açısı (maskeli - gözlüksüz - şapkalı) gibi görsellerin sorgu sonuçları ve eşleşme skorları 10.000 puan üzerinden 5000 ile 8999 eşleşme skoru arasında bir benzerlikle doğru adayın aday listesinde ilk beşinci sırada geldiği görülmektedir.

Yüz tanıma sistemi tarafından fotoğrafların otomatik kodlaması yapılarak 45 derecelik açısı kadar sistemin kesin tespit edici kabiliyetinden, 45 ile 90 derece arasında çekilen görüntülerin uzmanlar tarafından manuel kodlaması yapılarak sistemin önleyici tespit edici özelliğinden faydalanmak gerekir.

Benzer şekilde olay yerinden elde edilen düşük çözünürlüklü görüntülerin yanı sıra fotoğrafların güneş gözlüğü ve maskeli olması durumunda sistemin manuel kodlama yeteneğini kullanarak önleyici tespit edici özelliğinden yararlanmak gerekir.

Yüz tanıma sistemlerini kullanarak olay yerinden elde edilen bir fotoğrafın milyonlarca fotoğraf arasından sorgulanması yapıldığında, doğru adayın ilk onuncu sırada gelme ihtimali oldukça yüksektir ancak olay yerinden elde edilen fotoğrafların pek çok değişik faktöre bağlı olmasından kaynaklı olarak (görselin kalitesiz ve düşük çözünürlüklü olması, açısal parametreler, maske ve gözlük kullanımı, farklı yaş profili vb.) bazen doğru aday ilk onuncu sırada gelmekten ziyade daha yüksek sıralarda gelme ihtimalin mevcudiyetini de göz ardı etmemek gerekir.

Diğer yandan adli vakalarda elde edilen görsellerin sorgulama ve karşılaştırma için belirlenen kriterlere göre elverişsiz ve bozuk olması sebebi ile doğru adayın gelmeme ihtimali de söz konusu olabilmektedir.

Canlı yüz tanıma biyometrisi; hem kontrolsüz dış ortamda hem de kapalı kontrollü alanlarda kullanılan bir sistemdir. Bu sistemin kapalı kontrollü alanlardaki başarımları, kontrolsüz dış ortamlara göre daha yüksektir çünkü kontrolsüz dış ortam kullanımına etki edecek birden fazla faktör vardır. Ancak sistem, 90 derecelik açıya kadar teşhis ve tespit etme özelliğine sahiptir. Ayrıca sistemin çalışma mekanizmasına baktığımızda, aranan şahısların kameralar karşısına geçmesi durumunda aranan kişilerin kimliklerinin tanımlanması ve tespit edilmesi yapıp sistem tarafından anlık olarak ilgili mercilere kırmızı kod alarmı gönderilir.

Sonuç olarak, kurgulanan farklı senaryolar üzerinde gerçekleştirdiğimiz çeşitli analizler ve uygulamalar, kriminal ve adli bilişim vakalarına yönelik olay yerinden elde edilecek olan görüntülerin yüz tanıma sistemleri aracılığı ile olayların çözülmesine ve aydınlatılmasına etkili katkılar sunmaktadır. Tüm bunlara ek olarak, yüz tanıma sistemleri, adli bilişim uzmanlarına zamandan ve emekten tasarruf sağlarken, sonuçların da yüksek hız ve doğruluk oranı ile karakterize olmasını sağlar. Bu da yüz tanımanın, olayların aydınlatılmasında ne kadar etkili ve önemli olduğunu gösterir.

4. TARTIŞMA

Adli bilişim, dijital delillerin ve verilerin ilgili mahkemelere uygun bir şekilde sunulmasını sağlamakla yükümlüdür. Adli bilişim; özellikle ceza mahkemesinde delil değeri ve niteliği taşıyabilen bir hadisenin adli vaka sürecine evrildiği durumlarda, ilgili hadisenin neticelendirilmesi bakımından kullanılan kanıtların, sistematik adli bilişim soruşturma aşamaları ile doğrudan ilintili olduğunu vurgulamak gerekir. Nitekim adli bilişim sürecinin her bir aşaması, olayların aydınlatılması ve çözülmesi bakımından oldukça önemlidir. Bu sebeple, bütün bu süreç boyunca azami dikkat edilmesinin yanı sıra araştırma sürecini titizlikle yürütmek ve bilimsel yöntem ve tekniklere dayandırarak yapılması elzemdir.

Ayrıca adli bilişim sürecinin araştırma faaliyetlerinin kilit noktası, olay yerindeki mevcut verilerin uygun bir şekilde toplanması ve analizidir. Bu analizlerin biyometrik yöntem ve teknikler aracılığı ile yapılması durumunda, teknik olarak suçun aydınlatılması ve suçlunun tespit edilmesinde önemli bir rol oynamaktadır. Bu da adli bilişim uzmanlarına zamandan ve emekten tasarruf sağlar.

Biyometri; antik çağlardan günümüze kadar süregelen, yaygın ve etkin bir şekilde kullanılan, upuzun bir geçmişe sahiptir. Bazı insanlar, biyometrinin bir bilim dalı olduğunu kabul etmekle beraber spesifik olarak yalnızca kriminalistikte kullanıldığını düşünmektedir. Oysa ki günümüz dünyasında artık biyometri pek çok farklı uygulama alanına sahiptir. Örneğin, yeni nesil kimlik kartlarında, pasaportlarda, giriş çıkış kontrol noktalarında, havalimanında kullanılan E-gate sistemlerinde, bankacılık uygulamalarında; yüksek güvenlik gerektiren binaların giriş çıkışlarında ve kent güvenlik yönetim sistemi gibi alanlarda geniş bir kullanım alanına sahiptir.

Biyometrinin; evrensellik, Eşsizlik, süreklilik, elde edilebilirlik, performans; kabul edilebilirlik ve yaygınlık gibi birden fazla fonksiyonu vardır. Biyometrinin en büyük avantajlarından bir tanesi, gelişmiş güvenlik teknolojisine ve doğruluk oranının yüksek olmasına sahip olmasıdır. Biyometrinin en yaygın ve etkili yöntemlerinden biri yüz tanımadır.

Her biyometrik sistem, geçiş kapasitesi, maliyet, tanımlamanın güvenilirliği, kullanım basitliği ve rahatlığı, psikolojik rahatlık ölçeği, sistemle oyun oynama yeteneği, harmanlama yöntemi, kimlik doğrulama doğruluğu, verimlilik; entegrasyon ve gizlilik gibi göstergelere göre değişkenlik göstermektedir.

İki tür biyometrik tanımlayıcı tür vardır; bunları fiziksel ve davranışlar olarak iki ana grup altında toplamak mümkündür. Fiziksel grup; parmak ve avuç içi izi, yüz, iris ve retina tanıma, el geometrisi ve DNA gibi yöntemleri içerir. Davranışsal grup; yazma ritmi, el yazısı (imza atımı), yürüyüş ve ses tanıma gibi yöntemleri kapsar. Herbir biyometri yöntemi de, insan anatomisinin benzersiz özelliklerine dayanmaktadır.

Parmak izi; kriminalistikte en yaygın kullanılan biyometrik yöntemlerin başında gelmektedir. En eski ve en popüler olan bu yöntemin ana fikri; papiller paternin tek yumurtalı ikizlerinde bile farklı ve benzersiz olmasıdır. Papiller patern örneği, bireylerin dokunduğu herhangi bir yüzeyden kolaylıkla alınabilir. Ayrıca parmak izlerinin suç mahallerinde bırakılan en popüler delil olduğu düşünülmektedir.

İris tanıma yöntemi; biyometrik yöntemler arasında doğruluğu kesin olarak kabul edilmektedir. Bu yöntem iris tarama prensibine dayanmaktadır. Her kişi için benzersiz bir özelliğe sahiptir olmasının yanı sıra stabildir ve hayat boyu değişmemektedir. İris,

parmak izinden farklı olarak göz kapağı, kornea ve sulu mizah tarafından korunmaktadır.

Avuç içi izi; biyometri yöntemi olarak ifade edilen avuç içi izi, parmak izi ve iris tanıma gibi yöntemlerle sıklıkla anılır ancak daha çok kriminalistik vakalarda kullanılmakta olup bazı ülkelerin mevzuatı gereği mahkumların avuç içi izleri alınmaktadır. Bu yöntemin, 6 palmiye kategorisi vardır. Kategori 5 en yaygın olanıdır. Ayrıca kategori 5'inde kendi alt bölümleri vardır.

DNA; ekseriyetle parmak izi gibi kriminalistik olaylarda kullanılmaktadır. Bu yöntemin en büyük dezavantajı otomatik olmaması ve zaman alıcı olmasıdır. Ancak bu yöntemi diğer bütün yöntemlerden ayırın en önemli özellik, kesinliği nedeni ile pek çok insan tarafından güvenilir olması hesabıyla tercih edilmektedir.

El geometrisi; elin geometrik biçimini tanımak amacı ile kullanılmakta olan bir biyometrik yöntemdir. Ancak bu yöntem geçmişte kullanıldığı kadar günümüzde popüler bir şekilde kullanılmamaktadır. Bu biyometrik yönteminin ana avantajı, çoğu insanın kolaylıkla kullanabilmesi ve kabul oranının iyi olmasıdır. Ancak olumsuz yanı, sistemin oldukça hantal olmasıdır.

Yüz tanıma; geçmişten günümüze süregelen süreçte insanlar bir kişiyi diğerinden ayırt etmek için yüz ve yüz özelliklerini kullanmışlardır. Bir kişinin yüzü sayısız ayırt edici özelliğe sahiptir. İnsan yüzünde yaklaşık 80 tane düğüm noktası vardır. Bu düğüm noktalarına da yüz izi denilmektedir. Yüz tanımayı gerçekleştirmek için kullanılan iki ana yaklaşım vardır, bunlar bütünsel veya küresel yaklaşım bir diğer yaklaşım ise öznitelik tabanlı yaklaşımdır. Hızlı ve kompakt olması nedeni ile kullanımı

benimsenmektedir. iki tür yüz tanıma teknolojisi vardır. Bunlar; 2D ve 3D teknolojileridir.

Ses; kişi ve/veya kişileri tanımlamak için kullanılan en hızlı biyometrik yollardan biridir. Her kişi farklı ses dalga boylarına ve benzersiz frekanslara sahiptir. Ses doğrulama için iki tür sistem kullanılabilir, bunlar; metne bağlı konuşma yöntemi ile metinden bağımsız konuşma yöntemidir.

El Yazısı (imza atımı); Islak imza ve biyometrik imza “biyometrik”tir. Dolayısıyla kişiler, teknolojik (cep telefonu, tablet; bilgisayar vb.) araçlar sayesinde, tıpkı normal bir kalem kullanılarak kağıda atılan ıslak imzada olduğu gibi, biyometrik imzalarını da söz konusu araçları kullanarak oluşturabilirler. Biyometrik imza da elle atılmaktadır ve ıslak imzadan bu noktada hiçbir farkı mevcut değildir.

Her biyometri yöntemin kendine göre üstünlükleri ve sınırlılıkları mevcut. Ayrıca her yöntemin diğer biyometrik yöntemlere göre de hem avantajları hem de dezavantajları vardır. Günümüz dünyasında teknoloji hızlı gelişmekte ve de ilerlemektedir. Onun için bu yöntemlerde her gün gelişmekte ve ilerlemektedir. Ek olarak bu konudaki araştırmalar ve çalışmalar yoğun bir şekilde devam etmektedir. Nitekim üretici firmalar, sistemlerin kullanımını kolaylaştırmak, güvenilirliğini arttırmak, doğruluğunu yükseltmek, genel olarak kullanışlı ve ekonomik bir hale getirmek için AR-GE faaliyetlerini her geçen gün daha da yoğunlaştırmaktadırlar. Bu da hem alıcıların seçimini hem de üreticilerin sürdürülebilir rekabet etme yeteneğini etkilemektedir.

Biyometrik kimliklendirmede yüz tanımanın adli bilişim süreçlerine etkisi ve analizi adlı tez çalışmamızda, araştırmacılara açık erişimli [MIT CBCL Face

Recognition Database (2003-2005) ve FEI Face Database Disclaimer (2005-2006)] olan iki ayrı veriseti kullanılmıştır. Çalışmamızın ilk aşamasında, kullandığımız verisetleri içerisinde bulunan ve karşılaştırma bakımından elverişsiz olan görsel ve görüntüler veri ön işleme işlemine tabii tutularak temizlenmiştir. Yapılan ayıklama işleminden sonra analiz için hazır hale gelen verisetleri Papilon yüz tanıma sistemine yüklenmiş olup bilimsel veriler doğrultusunda kurgulanan bir dizi senaryolar için gerekli testler yapılmıştır.

Yüz algılamada kullanılan kodlama metodu olarak Fiducial Points metodolojisi kullanılmıştır. Kodlama işlemi hem otomatik hem de manuel olarak gerçekleştirilmiştir. Kodlama işlemi sırasında dikkat edilmesi gereken en önemli kriter; yüz özellik noktalarının sayısı, yeterli düğüm noktalarını temsil etmeli ve çok fazla olmamalıdır. Ek olarak; aranan kişilerin yüksek doğruluk oranı ile tespit edilmesi, referans noktaların doğru kodlamasından geçer.

Yüz tanımada üç ayrı yöntemin yanı sıra birde yapay zeka ve derin öğrenme algoritması kullanılmıştır. Bu yöntemler genel olarak; özellik tabanlı yüz tanıma yöntemi, görünüm tabanlı yüz tanıma yöntemi ve karma yüz tanıma yöntemidir. Ayrıca yüz tanıma ve biyometrik kimliklendirme bakımından, yapay zeka ve derin öğrenme algoritması önemli bir noktaya gelecek gibi gözükmemektedir.

Yüz ve yüz özellikleri en temel biyometrik özelliklerden biridir. Son zamanlar biyometrik yüz tanıma ile ilgili yapılan çalışmalar giderek artmaktadır. Bu da yüz tanıma sistemlerini popüler bir hale getirmektedir. Ayrıca yüz tanıma sistemlerini, görüntü ve video tabanlı olmak üzere iki temel başlık altında toplamak mümkündür.

Yaptığımız çalışmada iki temel yüz tanıma yöntemi benimsenmiştir. Bu yöntemler, kriminal inceleme amaçlı fotoğraftan fotoğrafa sorgulama yöntemi ve kent güvenlik yönetim sisteminde kullanılan canlı yüz tanıma yöntemidir.

Sonuç olarak; yüz tanıma biyometrisi, son zamanlarda en yaygın ve etkin kullanıma sahip olan bir biyometrik teknolojidir. Bu teknoloji kişilerin kimliğini, yüzün fizyolojik özelliklerine dayalı olarak tespit etme kabiliyetine sahiptir. Bu biyometrik teknoloji aracılığı ile kişileri tespit etme sırasında karşılaşılan yaş farkı, farklı açılardan çekilmiş görüntüler, kalitesiz ve çözünürlüğü düşük olan görüntüler, aranan kişilerin tıbbi ve/veya güneş gözlüğü kullanımı, şapka ve maske kullanımı gibi yüz tanıma ve tespit etme açısından engel teşkil eden parametrelere rağmen sorgu sonuçlarını etkilememektedir. Bu da bulgular kısmında gerçekleştirdiğimiz testlerde ve yaptığımız analizler sonucunda açıkça görülmüştür.

5. SONUÇ ve ÖNERİLER

Yüz tanıma; biyometri, gözetim, güvenlik, yüz tanımlamadan kimlik doğrulamaya kadar çeşitli uygulamalarda hayati bir rol oynamaktadır. Bu nedenle yüz tanıma, bir kişinin yüzünü kullanarak kimliğini tanımlamanın veya doğrulamanın bir yolu olarak tanımlanır. Yüz tanıma sistemleri ise, kişileri fotoğraflarda, videolarda ya da gerçek zamanlı olarak tanımlamak için kullanılan sistemlerdir. Bu sistemler; suçların çözülmesi, durdurması, önlenmesi ve engellenmesi ile birlikte, suçluları adalete teslim etme noktasında büyük bir potansiyele sahiptir. Yüz eşleştirmede ve yüz tanımada kullanılan pek çok farklı yöntem vardır. Dolayısıyla polislerin, güvenlik güçlerin ve kolluk kuvvetlerinin güvenlik açısından karşılaştıkları sorunların minimize edilmesi ve hataların ortadan kaldırılması noktasında yüz tanıma teknolojisinin devrede olması oldukça pratik ve sorun gidermede yararlı bir çözüm sunmaktadır. Bunun yanı sıra toplum güvenliğine yönelik geniş talepler, güvenlik ve emniyet amacını yerine getirmedeki verimlilik biyometrik yüz kullanımının yaygınlaşmasına neden olmuştur.

Covid-19 ile birlikte devam eden daha az temas eğilimi Yüz Tanıma teknolojisi açısından önemli gelişmelere yol açmıştır. Yapay zeka tarafından desteklenen bu yenilikçi çalışmalar; suçları önlemede, tespit etmede, belgelerin doğrulanması noktasında kullanılması başarımlarının yükseltilmesinde büyük rol oynarken demografik bilgiler ile biyometrik verilerin senkronizasyon sonucunda, yürütülen soruşturmalar, suç ve suç takibinin adil ve hızlı olarak yapılmasını sağlayacaktır. Bu aşamada hataların sınırlandırılması ve zorlukların ortadan kaldırılması noktasında yüz tanıma sistemlerinde kullanılan algoritmaların doğruluk oranlarını arttırarak standardını korumak önemlidir. Bu da yargı hatalarının önüne geçilmesi önleyecektir.

Teknolojinin süregelen gelişimi ile birlikte bugün, pasaport, ehliyet ve yeni nesil kimlik kart başvurularında vatandaşların fotoğrafları, kolluk kuvvetleri tarafından biyometrik yüz verilerinin ICAO standartları gereğince alınmasına etken olmaktadır. Toplanan bu veriler daha sonra olası adli vakalarda kullanılmak üzere depolanmaktadır. Ancak bu işlem yalnızca ilgili merciler tarafından yüz tanıma sistemleri kullanılarak yapılmaktadır. Bu da işlenen suçların aydınlatılmasının yanı sıra suçlunun kimliğini tespit etmesini sağlamaktadır. Özellikle kriminal veya adli bilişim vakalarında, olayın çözümüne yönelik büyük katkı sunacağını ve önemli etki sağlayacağını gerçekleştirdiğimiz testlerden elde ettiğimiz sonuçlar aracılığı ile değerlendirmek mümkündür.

Yüz tanıma sistemlerini, kent güvenlik yönetim sistemine veya havalimanı kamera izleme sistemine entegre edilmesi halinde istihbarat amaçlı olarak sistemin kesin tespit edici özelliğinden faydalanmak mümkün olduğu gibi kriminal inceleme ve adli bilişim alanında ise; kameradan yüz tanıma sisteminin önleyici tespit edici yeteneğinden faydalanmak gerekir.

Kriminal inceleme amaçlı fotoğraftan fotoğrafa sorgulama sisteminde kalitesiz ve çözünürlüğü düşük görsellerin, farklı açılardan çekilmiş görüntülerin, videolardan alınan resimlerin bile doğru kodlanması halinde kimlik tespit etme imkanı sağlandığı saptanmıştır. Ancak kodlama işlemi uzun ve meşakkatli bir iştir. Özellikle kayıt zamanında kodlama işlemi yüksek emek harcatır. KGYS’de ise operatöre herhangi bir kodlama imkânı verilmez. Bu durumda kötü ve farklı açıdan çekilmiş görüntülerde tespit kaybı yaşanır. Etkin bir KGYS’de, kişilerin yüze dayalı tespit sistemlerinde bizim öngörümüz, hem kriminal inceleme amaçlı kritik kişilerin ve aranmakta olan kişilerin yüzlerinin kodlanması hem de veri havuzunun sayısını yüksek tutmak için FRS dediğimiz kent güvenlik sistemlerinde kullanılan yöntemin füzyon olarak kullanılmasıdır.

Yapay zeka ve makine öğrenimi uygulamalarda doğruluk oranların artmasına destek olmuş olsa da her türlü ortamdan elde edilen görüntülerin analiz edilmesinde sadece teknolojinin bu alanındaki gelişmeler yeterli olmamakta görüntü füzyonu, bilgisayarla görme ve makine öğrenme gibi farklı alanları içeren çok disiplinli bir konudur. Piksel seviyesinde füzyon, tek tek her bir piksele uygulanarak gerçekleştirilen orijinal girdi görüntülerini iyileştirerek çıktı görüntüsünün her iki girdi görüntüsünden daha yararlı bilgilere sahip olmasını amaçlamaktadır. Füzyon işlemi sırasında orijinal görüntülerde göze çarpan tüm yüz bilgileri korunmakta, füzyon sonrasında yüz görüntüsünde yapay ve tutarsız veriler bulunmaması sağlanmaktadır. Bunun temel nedeni kullanılan füzyon işleminin piksel seviyesinde yapılmasıdır. Özellik seviyesinde füzyon, birçok farklı görüntü analizi uygulamasında kullanılmaktadır. Yüz tanıma sisteminde kullanılan füzyon algoritması, yanlış geometrik kayıt ve gürültü gibi görüntüde oluşabilecek bazı olumsuz etkenleri telafi edebilme özelliğine sahip olması görüntü kalitesi düşük kameralardan elde edilen görüntülerin füzyonu ile başarımlarının yükselmesine yapay zeka ve makine öğrenimi ile yüksek teknolojinin becerilerinden faydalanması sağlanmıştır.

Bu sayede veri setinin oluşum hızı yüksek tutulurken diğer yandan tespit için aranan kişilerin de kötü görüntülerinin kodlama imkânı ile sorgulama fırsatı olur. En nihayetinde amacımız kişilerin doğru tespitinin yapılması ve bu sebepten her ikisinde de aynı algoritmik metodolojinin kullanıldığında ve birbirini anlayan iki sistem halinde ortaya çıkarıldığı zaman füzyon modelin etkin bir şekilde çalışacağı öngörülmektedir. Araştırmacılara ve bu konuda ilgisi olan uzmanlara ilerleyen aşamalardaki önerimiz, bu füzyon metodolojisinin ayrı ayrı sistemlerdeki başarısının mukayese edilerek literatüre kriminal amaçlı ve kent güvenlik amaçlı sistemlerin daha etkin bir şekilde nasıl dahil edilebileceğine yönelik çalışmamız referans alınarak gerekli bilimsel çalışmaların yapılması tavsiyemizdir.

ÖZET

Biyometrik Kimliklendirmede Yüz Tanımanın Adli Bilişim Süreçlerine Etkisi ve Analizi

Son yıllarda, bilgi ve iletişim teknolojisinin yaygınlaştığı görmekteyiz. Bu da siber suçların kurbanı olma olasılığımızı arttırmaktadır. Teknolojinin ve modern iletişim araçlarının yayılıp çoğaldığı bu çağda, her ne kadar dünya çapında iletişimi kolaylaştırmak için kullanılıyor olsa da, bu araçların iki ucunun keskin bir kılıç gibi olduğunu unutmamak gerekir. Fakat buna rağmen bilgi ve iletişim teknolojisi, artık neredeyse yer yüzündeki insanların tüm yaşam alanlarına nüfuz etmiş durumdadır. Ek olarak, insanlar tarafından bilgi ve iletişim teknolojisine artan merak ve beraberinde gelen bağımlılık, toplumları, veri ve bilgisayar sistemlerine karşı veya bunlar aracılığıyla işlenen siber suçlar gibi tehditlere karşı savunmasız hale getirmektedir. Dolayısıyla bu tehditlere karşı mücadele etme konusunda da karşımıza Adli Bilimler kapsamında yer alan Adli Bilişim Bilimi çıkmaktadır. Adli bilişim; gerek Türkiye’de gerekse diğer dünya ülkelerinde gelişimini henüz tamamlamış bir disiplin değildir. Fakat adaletin tecelli etmesi amacıyla hizmet eden bir bilim dalı olarak karşımıza çıkmaktadır. Teknolojik gelişmelere bağlı olarak kendini her geçen gün yenilemekte ve ilerletmekte, hizmet alanını genişletmekte olan, adli bilişim süreçlerini dikkatli ve titiz bir şekilde yürütmekle ve sonuçlandırmakla mükellef olan, süreç sonucunu ilgili mercilere sunmak üzere olayları araştırma odaklı, şeffaf ve tarafsız bir şekilde belgeleme ve raporlama sorumluluğu olan bir disiplindir. Bu araştırma, adli bilişim disiplinine bağlı olarak biyometri teknolojisine bilhassa biyometrik yüz tanıma sistemlerine bir giriş sağlar. Biyometri, insanların fiziksel ve davranışsal özelliklerinden yararlanarak kişileri birbirinden ayırma yeteneğine sahip olmakla birlikte geniş bir uygulama alanı olan bir teknolojidir. Ayrıca biyometrinin en büyük avantajı, gelişmiş güvenlik teknolojilerine ve doğruluk oranının yüksek olmasına sahip olmasıdır. Bu nedenle biyometrik kimliklendirme sistemleri, kişilerin artan sayıda ve türde suça karışması ile beraber, işlenen suçlara dair olay yerinden toplanan verilerin incelenmesinde ve analizinde, adli bilişim uzmanlarına hızlı ve doğru bir şekilde suçun aydınlatılması ve suçlunun kimliğinin tespit edilmesinde önemli katkılar sunmaktadır. Ek olarak, biyometrinin pek çok işlevselliği mevcut olup, her biyometrik sistemin, göstergelerine göre farklı değişkenlikleri vardır. Buna karşın her biyometri yöntemin kendine göre avantajları ve dezavantajları olduğunu da ifade etmek gerekir. Biyometrinin en yaygın ve etkili yöntemlerinden biri yüz tanımadır. Yüz kendine has özelliklere, girinti ve çıkıntılara sahiptir. Nitekim yüz özellikleri incelendiğinde, her bir yüz farklı pek çok ayırt edici referans noktası taşımaktadır. İnsan yüzünde yaklaşık 80 tane düğüm noktası olarak ifade edilen referans noktası vardır. Bu düğüm noktaları rakamsal bir değerle kodlanır ve bu kodlara yüz izi denir. Yüz tanıma sistemleri aracılığı ile düğüm noktası olarak adlandırılan bu özellikler çıkarıldığında, suçlunun kimliğinin tespit edilmesi yapay zeka ve derin öğrenme algoritmaları ile kolay ve mümkün olacaktır. Bu çalışmada, araştırmacılara açık erişimli [MIT CBCL Face Recognition Database (2003-2005) ve FEI Face Database Disclaimer (2005-2006)] olan iki ayrı veriseti kullanılmıştır. Ek olarak bu çalışmada, iki temel yüz tanıma yöntemi ele alınmıştır. Bu yöntemler, kriminal inceleme amaçlı fotoğraftan fotoğrafa sorgulama yöntemi ve kent güvenlik yönetim sisteminde kullanılan canlı yüz tanıma yöntemidir. Sonuç olarak; biyometrik kimliklendirme de yüz tanıma sistemlerinin performansını değerlendirmek üzere bir takım senaryo kurgulanmış ve gerekli testler yapılmıştır. Yapılan testlerin analiz sonuçları bulgular bölümünde kapsamlı bir şekilde sunulmuştur.

Anahtar Kelimeler: Adli Bilişim, Adli Bilişim Süreçleri, Biyometri, Biyometrik Yöntemler, Biyometrik Kimliklendirme, Yüz Tanıma; Yüz Tanıma Sistemleri.

SUMMARY

The Effect and Analysis of Face Recognition on Forensic Information Processes in Biometric Identification

In recent years, we see that information and communication technology has become widespread. This increases our probability of being a victim of cybercrime. In this age where technology and modern communication tools are spreading and multiplying, it should not be forgotten that these tools are like a sharp sword, although they are used to facilitate communication around the world. However, despite this, information and communication technology has now penetrated almost all living spaces of people on earth. In addition, the growing curiosity and accompanying dependence on information and communication technology by humans makes societies vulnerable to threats such as cybercrime committed against or through data and computer systems. Therefore, in the fight against these threats, we come across Forensic Information Science, which is included in Forensic Sciences. forensic informatics; It is not a discipline that has not yet completed its development both in Turkey and in other world countries. However, it appears as a branch of science that serves the purpose of the manifestation of justice. Responsibility for documenting and reporting incidents in a research-oriented, transparent and impartial manner in order to present the result of the process to the relevant authorities, which renews and advances itself day by day depending on technological developments, expands its service area, is obliged to carry out and finalize the forensic processes carefully and meticulously. It is a discipline. This research provides an introduction to biometric technology, especially biometric facial recognition systems, depending on the forensic discipline. Biometrics is a technology with a wide range of applications, although it has the ability to distinguish people from each other by taking advantage of their physical and behavioral characteristics. In addition, the biggest advantage of biometrics is that it has advanced security technology and high accuracy. For this reason, biometric identification systems provide important contributions to forensic informatics experts in the examination and analysis of the data collected from the crime scene, with the increasing number and type of crime involved, in clarifying the crime and identifying the criminal in a fast and accurate manner. In addition, biometrics has many functionalities and each biometric system has different variability according to its indicators. On the other hand, it should be noted that each biometric method has its own advantages and disadvantages. One of the most common and effective methods of biometrics is facial recognition. The face has unique features, indentations and protrusions. As a matter of fact, when facial features are examined, each face carries many distinctive reference points. There are about 80 reference points on the human face, expressed as nodes. These nodes are encoded with a numerical value and these codes are called face traces. When these features, called node points, are removed through face recognition systems, the identification of the criminal will be easy and possible with artificial intelligence and deep learning algorithms. In this study, two separate datasets that are open to researchers [MIT CBCL Face Recognition Database (2003-2005) and FEI Face Database Disclaimer (2005-2006)] were used. In addition, in this study, two basic face recognition methods are discussed. These methods are the photo-to-photo interrogation method for criminal investigation and the live face recognition method used in the city security management system. As a result; In order to evaluate the performance of face recognition systems in biometric identification, a number of scenarios were designed and necessary tests were carried out. The results of the analysis of the tests are presented in a comprehensive way in the findings section.

Keywords: Forensic Informatics, Forensic Information Processes, Biometrics, Biometric Methods, Biometric Identification, Face Recognition; Face Recognition Systems.

KAYNAKLAR

- ADÁMEK M, MATÝSEK M, NEUMANN P (2015). Security of Biometric Systems. *Procedia Engineering*. **100**: 169-176.
- ADJABİ İ, OUAHABİ A, BENZAOUİ A, TALEB-AHMED A (2020). Past, Present, and Future of Face Recognition: A Review. *Electronics*. **9**: 1-52.
- AGARWAL A, GUPTA M, GUPTA S, GUPTA SC (2011). Systematic Digital Forensic Investigation Model. *International Journal of Computer Science and Security (IJCSS)*. **5**: 118-131.
- AKARSLAN H (2011). Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı. *Yüksek Lisans Tezi, T.C. Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Türkiye*.
- AKGÜL İ, AKAR F (2022). Derin Öğrenme Modeli ile Yüz İfadelerinden Duygu Tanıma. *Journal of the Institute of Science and Technology*. **12**: 69-79.
- AKKAN G (2013). Parmak İzi ve Ses Tanıma Sayısal Kanıt İşlemlerinin Analizi. *Yüksek Lisans Tezi, Fırat Üniversitesi, Türkiye*.
- AKSOY B (2019). Yüz Tanıma Sistemlerinde Doğruluk Performanslarının Değerlendirilmesi. *Mühendislik Bilimleri ve Tasarım Dergisi*. **7**: 835-842.
- ALHARBİ EH, ALAHRBİ MM (2020). Biometric Authentication Systems Towards Secure And Privacy Identification: A Review. Erişim Adresi: [<https://www.semanticscholar.org/paper/BIOMETRIC-AUTHENTICATION-SYSTEMS-TOWARDS-SECURE-AND-Alharbi-Alahrbi/b46cef11c95b83bc25eaea0e655b5ebe7b52cae4>]. Erişim Tarihi: [17.06.2022].
- ALİ D, TOUQİR İ, SİDDİQUİ AM, MALİK J, IMRAN M (2022). Face Recognition System Based on Four State Hidden Markov Model. *IEEE Access*. **10**: 74436-74448.
- ALMEZOGHI HHA (2019). Yerel İkili Sisteme Dayalı Palm Baskı İle İnsan Tanımlama Metodu. *Doktora Tezi, Kastamonu Üniversitesi, Türkiye*.
- ALMOSSAWY MMT, GEORGE LE (2022). A Digital Signature System Based On Hand Geometry-Survey: Basic Components of Hand-Based Biometric System. *Wasit Journal of Computer and Mathematics Science*. **1**: 1-14.

- AL-OGAİLİ H, SHADHAR AM (2022). The Finger Vein Recognition Using Deep Learning Technique. *Wasit Journal of Computer and Mathematics Sciences*. **1**: 1-11.
- ARCA S, CAMPADELLİ P, LANZAROTTİ R (2006). A Face Recognition System Based On Automatically Determined Facial Fiducial Points. *Pattern Recognition*. **39**: 432-443.
- ARSLAN B, SAĞIROĞLU Ş (2016). Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme. *Politeknik Dergisi*. **19**: 101-114.
- ARSLAN Ç (2015). Dijital Delil ve İletişimin Denetlenmesi. *Ceza Hukuku ve Kriminoloji Dergisi (CHKD)*. **3**: 253-266.
- ASHA S, CHELLAPPAN C (2012). Biometrics: An Overview of the Technology, Issues and Applications. *International Journal of Computer Applications*. **39**: 35-52.
- AUGUSTE MEB (2022). Face Recognition in Databases of Images with Hidden Markov's Models. *Pan-African Artificial Intelligence And Smart Systems*. **405**: 55-73.
- AVCI E, KARAKUŞ S, TUNCER T, VAROL A (2017). Biyometrik Güvenlik Sistemlerinin Performans Analizi. Erişim Adresi: [<https://silo.tips/download/byometrk-gvenlk-sstemlernn-performans-analz-performance-analysis-of-biometric-se>]. Erişim Tarihi: [17.03.2022].
- AYDOĞAN H (2009). Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri. *Yüksek Lisans Tezi, T.C. Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Türkiye*.
- AYGÜN S (2016). Çoklu Biyometrik Sistem Tasarımı. *Yüksek Lisans Tezi, Anadolu Üniversitesi, Türkiye*.
- BABIÇ A (2012). Biometric Authentication. Types of Biometric Identifiers. *Bachelor's Thesis, Haaga-Helia University of Applied Sciences, Finlandiya*.
- BAHAR MS (2021). Yapay Zeka ve Derin Öğrenme Teknikleri Kullanılarak Yüz Fotoğrafları İçeren Sahte Fotoğraf ve Video Sentezi. *Yüksek Lisans Tezi, Tekirdağ Namık Kemal Üniversitesi, Türkiye*.
- BARBAROS İ (2016). Bulut Depolama Uygulamalarını Kullanan Bilgisayarların Adli Bilişim Açısından İncelenmesi. *Yüksek Lisans Tezi, İstanbul Üniversitesi, Türkiye*.
- BAŞLAR Y (2020). Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri. *TBB Dergisi*. **148**: 47-76.

- BİSWAS D, JAYAN S, NADİPALLİ S, SNEHA B, SUBRAMANİ R (2022). Attendance Tracking with Face Recognition Through Hidden Markov Models. *IEEE International Conference on Electronics and Renewable Systems (ICEARS)*. **978**: 1640-1645.
- BLANZ V, VETTER T (1999). A Morphable Model For The Synthesis of 3D Faces. In *Proceedings of The 26th Annual Conference on Computer Graphics and Interactive Techniques*. 187-194.
- BOLME DS (2003). Elastic Bunch Graph Matching. *Master Thesis, Colorado State University, United States of America*.
- BOUDOU A, VİGUIER-PLA S (2022). Principal Components Analysis and Cyclostationarity. *Journal of Multivariate Analysis*. **189**: 1-17.
- BOZÜYÜK T, YAĞCI C, GÖKÇE İ, AKAR G (2005). Yapay Zeka Teknolojilerinin Endüstrideki Uygulamaları. Erişim Adresi: [<http://tektasi.net/wp-content/uploads/2014/01/yapay-zeka-teknolojilerinin-end%C3%BCstrideki-uygulamaları.pdf>]. Erişim Tarihi: [26.03.2022].
- BUCAK Y (2019). Adli Bilişim ve Türk Ceza Muhakemesi Hukukunda Bilgisayarda Arama. *Yüksek Lisans Tezi, Üsküdar Üniversitesi, Türkiye*.
- BULUT S (2020). Dijital Çağda Medya: Makine Öğrenmesi, Algoritmik Habercilik ve Gazetecilikte İşlevsiz İnsan Sorunsalı. *Selçuk İletişim*. **13**: 294-313.
- CAMPADELLİ P, LANZAROTTİ R (2004). Fiducial point localization in color images of face foregrounds. *Image and Vision Computing*. **22**: 863-872.
- CEYHAN E, SAĞIROĞLU Ş, AKYIL E (2014). Parmak İzi Öznitelik Vektörleri Kullanılarak Ysa Tabanlı Cinsiyet Sınıflandırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*. **29**: 201-207.
- CHANG LC, LİOU JY, CHANG FJ (2022). Spatial-Temporal Flood İnundation Nowcasts by Fusing Machine Learning Methods and Principal Component Analysis. *Journal of Hydrology*. **612**: 1-16.
- COOTES TF, TAYLOR CJ (2004). Statistical Models Of Appearance For Computer Vision. Erişim Adresi: [https://www.face-rec.org/algorithms/AAM/app_models.pdf]. Erişim Tarihi: [24.03.2022].
- Crime Scene Investigator. Erişim Adresi: [<https://www.crime-scene-investigator.net/evidenc2.html>]. Erişim Tarihi: [13.06.2022].
- CSO Online. Erişim Adresi: [<https://www.csoononline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html>]. Erişim Tarihi: [09.06.2022]

- ÇELİKTUTAN O, ULUKAYA S, SANKUR B (2013). A Comparative Study of Face Landmarking Techniques. *EURASIP Journal on Image and Video Processing*. **2013**: 1-27.
- ÇETİNKAYA HH, AKÇAY M (2012). Yüz Tanıma Sistemleri Ve Uygulama Alanları. Erişim Adresi: [https://ab.org.tr/ab12/kitap/cetinkaya_akcay_AB12.pdf]. Erişim Tarihi: [24.06.2022].
- ÇOBAN A, ÖZYURT F (2022). Kapsül Ağları ile Yüz Verilerinin Sınıflandırılması. *Avrupa Bilim ve Teknoloji Dergisi*. **33**: 176-183.
- DANIEL L (2011). DIGITAL FORENSICS FOR LEGAL PROFESSIONALS: UNDERSTANDING DIGITAL EVIDENCE FROM THE WARRANT TO THE COURTROOM. *Elsevier*.
- DENİZ MÖ, ÖZER MT (2022). Biyometrik Verilerin İşlenmesinin Yargı Kararları Işığında Değerlendirilmesi. *Çukurova Üniversitesi Hukuk Araştırmaları Dergisi*. **1**: 92-110.
- DOĞAN F, TÜRKOĞLU İ (2019). Derin Öğrenme Modelleri ve Uygulama Alanlarına İlişkin Bir Derleme. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*. **10**: 409-445.
- DOĞANAY HA (2019). Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi. *Yüksek Lisans Tezi, Ankara Üniversitesi, Türkiye*.
- DÜDEN S (2019). Türkiye'de Adli Bilişimin Gelişimi ve Dijital Delil İncelemeleri. *Yüksek Lisans Tezi, Gebze Teknik Üniversitesi, Türkiye*.
- EBRAHİMPOUR N, AYDEN MA, ALTAY B (2022). Liveness Control İn Face Recognition With Deep Learning Methods. *The European Journal of Research and Development*. **2**: 92-101.
- ELVEREN Ş (2018). Dünyada ve Türkiye'de Adli Bilişim Eğitim Uygulamalarının İncelenmesi ve Türkiye İçin Uygulamaya Yönelik Öneriler. *Yüksek Lisans Tezi, Gazi Üniversitesi, Türkiye*.
- ERİŞ FG (2018). Mobil Cihazlarda Sosyal Medya Uygulamalarının Adli Bilişim Açısından Analizi. *Yüksek Lisans Tezi, Fırat Üniversitesi, Türkiye*.
- ERİŞ M (2018). Derin Öğrenme Yöntemleri Kullanarak Adli Bilişim İncelemelerinde Delil Çıkarımının Gerçekleştirilmesi. *Yüksek Lisans Tezi, Fırat Üniversitesi, Türkiye*.

- FANG L, LEUNG MKH, SHIKHARE T, CHAN V, CHOON KF (2006). Palmprint Classification. Erişim Adresi: Erişim Adresi: [<https://docplayer.net/17210907-Palmprint-classification.html>]. Erişim Tarihi: [03.07.2022].
- FEI Face Database Disclaimer. Erişim Adresi: [<https://fei.edu.br/~cet/facedatabase.html>]. Erişim Tarihi: [17.03.2022].
- FİLİZ S (2012). Siber Güvenlikte Biyometrik Sistemler ve Yüz Tanıma. *Yüksek Lisans Tezi, Gazi Üniversitesi, Türkiye*.
- GAFUROV D (2008). Performance and Security Analysis of Gait-Based User Authentication. *Doctoral Dissertation, University of Oslo, Norway*.
- GAO Y, LEUNG MK (2002). Face Recognition Using Line Edge Map. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. **24**: 764-779.
- GÖKSU M (2011). Hukuk Yargılamasında Elektronik Delil. *Doktora Tezi, Ankara Üniversitesi, Türkiye*.
- GÖZE H, YILDIZ O (2022). Video Görüntülerinde Gerçek Zamanlı Yüz Tanıma ve Zaman İşaretleme için Yeni Bir Derin Öğrenme Modeli. *Bilişim Teknolojileri Dergisi*. **15**: 167-175.
- GÜMÜŞ F, OĞUZ A, BALIK HH (2018). Davranışsal Biyometrinin 5 Yılı: Kimlik Doğrulama ve Anomali Tespit Uygulamaları. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*. **30**: 345-364.
- GÜNDÜZ G, CEDİMOĞLU İH (2019). Derin Öğrenme Algoritmalarını Kullanarak Görüntüden Cinsiyet Tahmini. *Sakarya University Journal of Computer and Information Sciences*. **2**: 9-17.
- HAN Y, SONG G, LIU F, GENG Z, MA B, XU W (2022). Fault Monitoring Using Novel Adaptive Kernel Principal Component Analysis Integrating Grey Relational Analysis. *Process Safety and Environmental Protection*. **157**: 397-410.
- HANİ SM, KESHK H, EL-ADAWY M, EL-TOBELY T (2011). Face Profile Recognition And Identification. *Journal of Engineering Sciences (JES)*. **39**: 1043-1054.
- HASHİYADA M (2011). DNA biometrics. In Biometrics. IntechOpen. Erişim Adresi: [<https://www.intechopen.com/chapters/16506>]. Erişim Tarihi: [07.07.2022].
- HATİPOĞLU C (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri. *International Congress on Politic, Economic and Social Studies (ICPESS)*. **3**: 157-168.

- HENKOĞLU T (2020). ADLİ BİLİŞİM: DİJİTAL DELİLLERİN ELDE EDİLMESİ VE ANALİZİ. *Pusula*.
- HIDIMOĞLU K (2010). Web Kamera Kullanımı ile Parmak İzi Tanıma ve Kimlik Tespiti Doğrulama. *Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Türkiye*.
- HOLTGREWE U (2014). New New Technologies: The Future And The Present Of Work İn Information And Communication Technology. *New technology, work and employment*. **29**: 9-24.
- IULA A, MİCUCCI M (2022). Multimodal Biometric Recognition Based on 3D Ultrasound Palmprint-Hand Geometry Fusion. *IEEE Access*. **10**: 7914-7925.
- İNİK Ö, ÜLKER E (2017). Derin Öğrenme ve Görüntü Analizinde Kullanılan Derin Öğrenme Modelleri. *Gaziosmanpaşa Bilimsel Araştırma Dergisi*. **6**: 85-104.
- JEON S, KİM MS (2022). End-to-End Lip-Reading Open Cloud-Based Speech Architecture. *Sensors*. **22**: 1-21.
- KARAKUŞ S (2018). Derin Öğrenme Yöntemlerinin Kullanılarak Dijital Deliller Üzerinde Adli Bilişim İncelemesi. *Yüksek Lisans Tezi, Fırat Üniversitesi, Türkiye*.
- KARAKÜÇÜK Y, EKER S (2020). Oftalmolojide Yapay Zeka Ve Derin Öğrenme Uygulamaları. Erişim Adresi: [https://www.researchgate.net/profile/Yalcin-Karakucuk-2/publication/342438070_OFTALMOLOJIDE_YAPAY_ZEKA_VE_DERIN_OGRENME_UYGULAMALARI/links/5f8e7fcd92851c14bcd550c0/OFTALMOLOJIDE-YAPAY-ZEKA-VE-DERIN-OeGRENME-UYGULAMALARI.pdf]. Erişim Tarihi: [26.03.2022].
- KAUBA C, DRAHANSKÝ M, NOVÁKOVÁ M, UHL A, RYDLO Š (2022). Three-Dimensional Finger Vein Recognition: A Novel Mirror-Based Imaging Device. *Journal of Imaging*. **8**: 1-24.
- KAYA Ç, YILDIZ O (2014). Makine Öğrenmesi Teknikleriyle Saldırı Tespiti: Karşılaştırmalı Analiz. *Marmara University Journal of Science*. **26**: 89-104.
- KAYA Y (2016). Bulut Temelli Adli Bilişim. *Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Türkiye*.
- KAYA Z, GÜNEŞ A (2016). Biyometrik Güvenlik Sistemleri ve Yüz Tanımaya Dayalı Çevrimiçi Sınav Sistemi. *Eğitim ve Öğretim Araştırmaları Dergisi*. **5**: 87-97.
- KAYMAZ S (2010). Çevrimdışı İmza Tanıma. *Yüksek Lisans Tezi, Marmara Üniversitesi, Türkiye*.

- KIZMAZ MH, KÜÇÜKÇOLAK RA (2021). Büyük Veri Teriminin Kökeni ve Büyük Verinin V'leri. *Working Paper Series*. **2**: 19-31.
- KOÇ HK (2019). Biyometrik Tanı Yöntemlerinde Kişisel Veri Güvenliği Arttırılmış Sistem Tasarımı. *Yüksek Lisans Tezi, Mersin Üniversitesi, Türkiye*.
- KORKMAZ Y, BOYACI A (2018). Adli Bilişim Açısından Ses İncelemeleri. *Fırat Üniv. Müh. Bil. Dergisi*. **30**: 329-343.
- KURTOĞLU EL, TEKEDERELİ İ (2015). DNA Onarım Mekanizmaları. *Balıkesir Sağlık Bilimleri Dergisi*. **4**: 169-177.
- KUSBAN M (2021). Improvement Palmprint Recognition System by Adjusting Image Data Reference Points. Erişim Adresi: [<https://iopscience.iop.org/article/10.1088/1742-6596/1858/1/012077/pdf>]. Erişim Tarihi: [18.03.2022].
- KUTUCU H (2020). Derin Öğrenme Algoritmaları Kullanarak Bir Konuşma Tanıma Uygulaması. *Yüksek Lisans Tezi, Sakarya Uygulamalı Bilimler Üniversitesi, Türkiye*.
- KÜME T, CAN İÖ, ŞİŞMAN AR (2009). Medicolegal Sample Procedures in Clinical Laboratories. *Türk Klinik Biyokimya Dergisi*. **7**: 101-113.
- KÜN U, BAYRAM L, ÖZHAN MZ (2014). Kent Güvenlik Yönetim Sistemleri. Erişim Adresi: [https://d1wqtxts1xzle7.cloudfront.net/65040126/Bolum_12_Kent_Guvenlik_Yonetim_Sistemleri_2_-with-cover-page-v2.pdf?Expires=1665523458&Signature=a~FcIn5yk~O2Hx2MQXHLHj02pd7okyK68-ikLQIkYjAbBfF4WLJno-O6ohcimJl6YQNpMn1--nxoD~VGLudopMvO2Qk12n8scUr6knikoVHamwjVQQYw6KEGJWKP5HQeQqgBC5ooL8zAM2KEXziNyqBwaMDoNaYDHfzKtndYuuCPwdvpEk01A5hR4duAqAIyScOUgPUUOmVaepf9xTPSmwAkN-b~-xjFYPM56UTf0bERcu8plWO-mleYzeEeVXUUoQOK3iNutVu35y1K-w90cgUiqGrjfUyLtffYXY8Gz~fS7KFJnpBDob5seKHb~m36M-CgxZvRS0XVWniREgppJw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA]. Erişim Tarihi: [26.05.2022].
- LİU D (2009). CISCO ROUTER AND SWITCH FORENSİCS: INVESTİGATING AND ANALYZİNG MALİCİOUS NETWORK ACTİVİTY. *Syngress*.
- MAMAK U, KONYAR MZ, SOLAK S, UÇAR MH (2020). Gerçek Zamanlı Yüz Tanıma Tabanlı Personel Kontrol ve Takip Sistemi Tasarımı. *Avrupa Bilim ve Teknoloji Dergisi*. **19**: 497-504.

- MENGÜÇ EC, ACIR N (2022). Yeni Bir Otomatik Yüz Tanıma Sistemi. *Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi*. **11**: 574-583.
- MIT-CBCL face recognition database. Erişim Adresi: [<http://cbcl.mit.edu/software-datasets/heisele/facerecognition-database.html>]. Erişim Tarihi: [16.03.2022].
- MİTRA R, KADDOUM G, DAHMAN G, POİTAU G (2020). Error Analysis Of Localization Based On Minimum-Error Entropy With Fiducial Points. *IEEE Communications Letters*. **25**: 1187-1191.
- MOGAN JN, LEE CP, LİM KM (2022). Advances in Vision-Based Gait Recognition: From Handcrafted to Deep Learning. *Sensors*. **22**: 1-24.
- MOSES KR, HİGGİNS P, MCCABE M, PRABHAKAR S, SWANN S (2011). Automated Fingerprint İdentification System (Afis). Erişim Adresi: [https://lkouniv.ac.in/site/writereaddata/siteContent/202003241550009003kamyani_vajpayee_Automated_fingerprint_identification.pdf]. Erişim Tarihi: [27.06.2022].
- MUSAYEVA G, YAHYAYEV M (2014). Biyometrik Güvenlik Sistemleri. Erişim Adresi: [https://www.researchgate.net/profile/Gunay-Musayeva-2/publication/271210599_Biyometrik_Guvenlik/links/54c2362c0cf256ed5a8c5f89/Biyometrik-Guevenlik]. Erişim Tarihi: [22.08.2022].
- OĞUZ R (2018). Adli Bilişimde İnceleme Süreçleri. *Yüksek Lisans Tezi, Ankara Üniversitesi, Türkiye*.
- OĞUZLAR A (2003). Veri Ön İşleme. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*. **21**: 67-76.
- OKUYUCU HH (2020). Hash Fonksiyonlarının Adli Bilişimde Uygulamaları ve C++ ile Şifreleme Algoritması Tasarımı. *Yüksek Lisans Tezi, Karabük Üniversitesi, Türkiye*.
- ÖZBEK M (2013). Adli Bilişimde Delillerin Toplanması ve İncelenmesi. *Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Türkiye*.
- ÖZKAYA N, SAĞIROĞLU Ş (2022). Açık Anahtar Altyapısı ve Biyometrik Teknikler. Erişim Adresi: [https://www.researchgate.net/profile/Necla-Ozkaya/publication/251743851_ACIK_ANAHTAR_ALTYAPISI_VE_BIYOMETRIK_TEKNIKLER/links/542e819f0cf277d58e8ebd4d/ACIK-ANAHTAR-ALTYAPISI-VE-BIYOMETRIK-TEKNIKLER.pdf]. Erişim Tarihi: [06.07.2022].
- ÖZTÜRK C (2006). Kriminalistğe Farklı Bir Bakış-İz Ve İz Bilimi. *Polis Bilimleri Dergisi (PBD)*. **8**: 59-72.

- PARWANI RP (2022). Artificial Intelligence. Erişim Adresi: [https://www.researchgate.net/profile/Ritwik-Parwani/publication/358292421_Artificial_Intelligence/links/61fbd6cb1e98d168d7eb79d4/Artificial-Intelligence.pdf]. Erişim Tarihi: [21.03.2022].
- PİRİM H. (2006). *Yapay Zeka. Yaşar Üniversitesi E-Dergisi*. **1**: 81-93.
- RONDA V, AGERBO E, BLESES D, MORTENSEN PB, BØRGLUM A, MORS O, WERGE T (2022). Family Disadvantage, Gender, and The Returns To Genetic Human Capital. *The Scandinavian Journal of Economics*. **124**: 550-578.
- SADAY T, AKHAN N (2003). Bilgisayar Destekli Kimlik Tespit Sistemlerinde Biometrik Yöntemlerin Değerlendirilmesi. *Akademik Bilişim Konferansları*. Erişim Adresi: [<https://ab.org.tr/ab03/tammetin/46.pdf>]. Erişim Tarihi: [21.06.2022].
- SADIKOĞLU F, ÜZELALTINBULAT S (2018). Sinirsel Ağlara Dayanarak Biyometrik Retina Tanıması. *Yangın Güvenlik ve Koruma Sistemleri Dergisi*. **24**: 24-34.
- SAİNİ R, RANA N (2014). Comparison of Various Biometric Methods. *International Journal of Advances in Science and Technology (IJAST)*. **2**: 24-30.
- SALEH AH (2022). Iris Segmentation and Recognition Based on Deep Learning In The Presence of Diseases. *Yüksek Lisans Tezi, Karabük Üniversitesi, Türkiye*.
- SALMAM FZ, MADANİ A, KİSSİ M (2018). Emotion Recognition From Facial Expression Based on Fiducial Points Detection and Using Neural Network. *International Journal of Electrical and Computer Engineering*. **8**: 52-59.
- SAMARİA FS (1994). Face Recognition Using Hidden Markov Models. *PhD Thesis, University of Cambridge, England*.
- SANTOS CFGD, OLIVEIRA D de S, PASSOS LA, PİRES RG, SANTOS DFS, VALEM LP, MOREİRA TP, SANTANA MCS, RODER M, PAPA JP, COLOMBO D (2022). Gait Recognition Based on Deep Learning: A Survey. *ACM Computing Surveys (CSUR)*. **55**: 1-34. Erişim Adresi: [<https://dl.acm.org/doi/pdf/10.1145/3490235>]. Erişim Tarihi: [13.07.2022].
- SAY K (2006). Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarında İncelenmesi. *Yüksek Lisans Tezi, Ankara Üniversitesi, Türkiye*.
- SHİNDER DL, CROSS M (2008). SCENE OF THE CYBERCRİME. Elsevier.

- SÜZEN AA, KAYAALP K (2018). Derin Öğrenme ve Türkiye’de ki Uygulamaları. Erişim Adresi: [https://www.researchgate.net/profile/Ahmet-Suezen/publication/327666072_Derin_Ogrenme_ve_Turkiye'deki_Uygulamaları/inks/5b9cc16d45851574f7cb5fd0/Derin-Oegrenme-ve-Tuerkiyedeki-Uygulamaları.pdf]. Erişim Tarihi: [27.03.2022].
- ŞAMLI R, YÜKSEL ME (2009). Biyometrik Güvenlik Sistemleri. Erişim Adresi: [<https://ab.org.tr/ab09/bildiri/102.pdf>]. Erişim Tarihi: [11.07.2022].
- ŞAN S (2013). Parmak Damar Tanıma Teknolojisi. *Yüksek Lisans Tezi, Fırat Üniversitesi, Türkiye.*
- ŞEKER A, DİRİ B, BALIK HH (2017). Derin Öğrenme Yöntemleri ve Uygulamaları Hakkında Bir İnceleme. *Gazi Mühendislik Bilimleri Dergisi*. **3**: 47-64.
- ŞEKER G (2009). Polisin Kent Güvenlik Uygulaması ve Yönetim Modeli. Doktora Tezi, Dokuz Eylül Üniversitesi, Türkiye.
- TAYLOR M, HAGGERTY J, GRESTDY D, HEGARTY R (2010). Digital Evidence İn Cloud Computing Systems. *Computer law & security review*. **26**: 304-308.
- TEMİZ H (2022). Rapid Marking Attendance with Face Recognition. *Avrupa Bilim ve Teknoloji Dergisi*. **36**: 78-86.
- TURHAL ÜÇ (2008). İki Boyutlu Yüz Tanıma Metodlarına Yeni Yaklaşımlar; Satır ve Sütun Vektörleri Arasındaki Değişimlerin Kullanılması. *Doktora Tezi, Eskişehir Osmangazi Üniversitesi, Türkiye.*
- UKŞAL M (2015). Mobile Forensic. *Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, Türkiye.*
- VAZQUEZ-FERNANDEZ E, GONZALEZ-JIMENEZ D (2016). Face Recognition For Authentication On Mobile Devices. *Image and Vision Computing*. **55**: 31-33.
- WANG R, MADDEN K, WANG C (2022). Low-effort User Authentication for Kiosk Systems based on Smartphone User’s Gripping Hand Geometry. *In CHI Conference on Human Factors in Computing Systems Extended Abstracts*. **22**: 1-6.
- Wikipedia. Erişim Adresi: [<http://en.wikipedia.org/wiki/Biometrics>]. Erişim Tarihi: [21.06.2022].
- Wikipedia. Erişim Adresi: [https://tr.wikipedia.org/wiki/Kimlik_do%C4%9Frulama]. Erişim Tarihi: 19.06.2022].
- YALÇIN N, GÜRBÜZ F (2015). Biyometrik Güvenlik Sistemlerinin İncelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*. **3**: 398-413.

YILDIZ K (2021). Deep Learning-Based Face Recognition With Raspberry P1 and Usb Accelerator For Iot Environments. *Yüksek Lisans Tezi, Atılım Üniversitesi, Türkiye.*

YILMAZER B, SOLAK S (2021). YÜZ TANIMA TABANLI DUYURU SİSTEMİ TASARIMI ve KULLANILABİLİRLİĞİ. *Euroasia Journal of Mathematics, Engineering, Natural and Medical Sciences.* **8:** 21-35.

YUN T, GUAN L (2009). Automatic Fiducial Points Detection For Facial Expressions Using Scale Invariant Feature. *IEEE International Workshop on Multimedia Signal Processing.* 1-6.

ZEYBEK V (2012). Transplantasyon Sonrası Hastaların Kan, Saç Ve Bukkal Sürüntü Örneklerinin DNA Profilleri. *Doktora Tezi, Dokuz Eylül Üniversitesi, Türkiye.*