T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜZ TANIMA SİSTEMLERİNDE CANLILIK ANALİZİ

Tugay BOZİK

YÜKSEK LİSANS TEZİ

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektonik Mühendisliği Programı

Danışman

Dr. Öğretim Üyesi Nihan Kahraman

Haziran, 2019

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜZ TANIMA SİSTEMLERİNDE CANLILIK ANALİZİ

Tugay BOZİK tarafından hazırlanan tez çalışması çalışması 28.06.2019 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı, Elektronik Mühendisliği Programı **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üyesi Nihan KAHRAMAN

Yıldız Teknik Üniversitesi

Danışman

Jüri Üyeleri

Dr. Öğr. Üyesi Nihan KAHRAMAN, Danışman
Yıldız Teknik Üniversitesi _____

Doç. Dr. Burcu ERKMEN, Üye
Yıldız Teknik Üniversitesi _____

Prof. Dr. Zümray DOKUR, Üye
İstanbul Teknik Üniversitesi _____

Danışmanım Dr. Öğretim Üyesi Nihan Kahraman sorumluluğunda tarafımca hazırlanan Yüz Tanıma Sistemlerinde Canlılık Analizi başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim

Tugay BOZİK

İmza

Aileme

ve

biricik eşime

TEŞEKKÜR

Yüksek lisans eğitimim boyunca bana öğrettikleri ile katkıda bulunan tüm değerli hocalarıma, özellikle tezin hazırlanma aşamasında benden yardımlarını esirgemeyen ve beni sürekli olarak aydınlatan Dr. Öğretim Üyesi Nihan KAHRAMAN'a çok teşekkür ederim. Yüksek lisans eğitimim boyunca ders aldığım veya bir şekilde bilgi alışverişinde bulunduğum tüm hocalarıma sonsuz saygılarımı sunarım.

Çalışmalarımda beni lisans eğitimimden itibaren destekleyen sevgili hocam ve ağabeyim Güray GÜRKAN'a da ayrıca teşekkür ederim.

Hayatım boyunca beni her zaman destekleyen, beni en güzel şekilde yetiştiren, bugüne kadar her türlü fedakârlığı yapan ve sahip olduğum için onur duyduğum aileme sonsuz sevgilerimi, son olarak her zaman yanımda olduğu için en değerli parçam olan eşim Dilara'ya sonsuz teşekkürlerimi sunarım.

Tugay Bozik

İÇİNDEKİLER

KISALTMA LİSTESİ vii

ŞEKİL LİSTESİ viii

TABLO LİSTESİ ix

ÖZET x

ABSTRACT xii

1 Giriş 1

1.1 Literatür Özeti 1

1.2 Tezin Amacı 7

1.3 Hipotez 7

2 Görüntü İşleme Yöntemleri ile Kullanıcıların Yüzdeki Biyometrik Verilerinin Tespit Edilmesi 9

2.1 Önerilen Yöntem 9

2.2 Görüntünün Elde Edilmesi 13

2.3 Resmin Gri Tonlama Uzayında Elde Edilmesi 13

2.4 Yüz Tespit Etme 15

2.5 Göz Alanı Tespit Etme 17

2.6 İris Bölgesi Tespit Etme 19

3 Canlılık Kararını Vermek için Doğrulama Yapılması 22

3.1 Ekran yazılarının Dinamik olarak çıkarılması 22

3.2 İris Konumunu ile Ekran Metinlerinin Konumlarını Eşleştirerek Canlılık Tespiti 24

4 Sonuç ve Öneriler 29

Kaynakça **32**

Tezden Üretilmiş Yayınlar **36**

KISALTMA LİSTESİ

3B	3 Boyutlu
BGR	Blue – Green - Red
CNN	Convolutional Neural Network
DNA	Deoksiribo Nükleik Asit
FL	Facial Landmarks
FPS	Frame Per Second
HOG	Histogram Of Gradient
HSI	Hue Saturation Intensity
HSV	Hue Saturation Value
IR	Infrared
Kb	Kilobyte
LBP	Local Binary Pattern
LED	Light Emitting Diode
Mb	Megabyte
Mp	Megapiksel
ms	milisaniye
OpenCV	Open Source Computer Vision
RBF	Radial Basis Function
RGB	Red- Green - Blue
ROI	Region of Interest
WLBP	Weber Local Binary Pattern
WLD	Weber Local Descriptor
YCbCr	Luminance – Chroma Blue – Chroma Red

ŞEKİL LİSTESİ

Şekil 1.1 Biyometrik Sistem Blok Diyagramı……3
Şekil 1.2 Biyometrik Sistemlere Atak Noktaları [12] ……4
Şekil 2.1 Önerilen Algoritmanın Blok Diyagramı……12
Şekil 2.2 RGB Renk Uzayı Renk Kübü……14
Şekil 2.3 Gri Ton Renk Uzayı……15
Şekil 2.4 Dlib 68 Nokta Yüz İşaretleyicisi [51]……17
Şekil 2.5 Dlib 68 Yüz Noktası Maskesi……18
Şekil 2.6 Dlib ile Gözlerin Ayrı Ayrı Belirlenmesi……19
Şekil 2.7 Gri Tonlama Seviyesinde İris Görüntüleri ……21
Şekil 3.1 Ekran Metinlerinin Yerleşim Bölgeleri ……23
Şekil 3.2 Canlılık Analizi Ret Kararı Görseli-1……25
Şekil 3.3 Canlılık Analizi Ret Kararı Görseli-2……26
Şekil 3.4 Canlılık Analizi Kabul Kararı Görseli-1……26
Şekil 3.5 Canlılık Analizi Kabul Kararı Görseli-2……27
Şekil 3.6 Gözlüklü Kişilerde Canlılık Analizi Kabul Kararı Görseli……28
Şekil 3.7 Gözlüklü Kişilerde Canlılık Analizi Ret Kararı Görseli……28

TABLO LİSTESİ

Tablo 1.1 Biyometrik Karakteristikler……2
Tablo 1.2 Biyometrik Karakteristiklerin Karşılaştırılması [2]……2

ÖZET

Yüz Tanıma Sistemlerinde Canlılık Analizi

Tugay BOZİK

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Danışman: Dr. Öğretim Görevlisi Nihan Kahraman

Günümüzde bilgisayarların gündelik yaşantımızın önemli bir parçası olması ile birlikte insan-bilgisayar etkileşimi oldukça fazla artmıştır. Teknolojinin sürekli olarak gelişmesiyle bu etkileşim her alanda oldukça önemli bir rol almaktadır. Son zamanlarda bu etkileşimin güvenlik alanında da önemli bir rol aldığını görüyoruz. Geleneksel güvenlik sistemlerinde şifreler, kartlar ve anahtarlar kullanılırken bunların kopyalanması, çalınması veya unutulması sürekli karşılaşılan bir konudur. Güvenlik gerektiren uygulamalar; mobil bankacılık, banka uygulamaları, erişim kontrol sistemleri gibi uygulamalarda önemini çok net anladığımız alanlarda geleneksel güvenlik yöntemlerinin yerine biyometrik veriler üzerinden kişilerin sistemlere daha güvenli ve pratik olarak erişimi sağlanmaya başlamıştır. Biyometrik veriler, kişilere ait ölçülebilir fiziksel ve davranışsal özellikleri tanıyarak, kimlik belirlemek üzere geliştirilmiş otomatik sistemler için kullanılan bir terimdir. Biyometrik veriler içerisinde en çok kullanılan özellik yüz ve göz biyometriğidir. Bu verileri kullanarak erişilen sistemler çok daha güvenilirdir. Ancak, biyometrik kimlik doğrulama sistemlerinin dolandırıcılık, sahtekarlık saldırılarına karşı olan

zafiyeti yaygın olarak bilinen bir konudur. Sistemleri, biyometrik verileri taklit ederek kandırmaya çalışmak bilinen en yaygın dolandırıcılık saldırılarıdır.

Bu çalışmada yüz tanıma sistemlerine yapılan dolandırıcılık saldırılarına karşı canlılık analizi yapılarak bir çözüm önerilmiştir. Kişilerin sisteme girmek için bir kamera karşısına geçmesiyle birlikte çalışan bir algoritma sayesinde canlılık kararı verilerek sistemlere sahte girişlerin önüne geçilmesi amaçlanmıştır. Geleneksel biyometrik doğrulama sistemlerinin üzerinde az maliyetli bir donanım değişikliği ile mevcut güvenlik seviyelerini arttırmak mümkündür.

Python programlama dilini kullanarak, OpenCV görüntü işleme kütüphanesinin yetkinlerinden faydalanılmıştır. Aynı zamanda görüntü işleme algoritması olarak Dlib kütüphanesinden de faydalanılmıştır. Donanım olarak Intel i5 2.3GHz işlemciye sahip bilgisayar ve 1024x768 çözünürlüklü 5MP standart web kamerası kullanımıştır. Aynı zamanda bu yazılım Raspberry Pi 3 Model B donanımı üzerinde de test edilmiş olup aynı başarıya ulaşmıştır. Ekran karşısına geçen bir kişinin şekil dedektörü algoritması ile yüz bölgesi tespit edilmiştir. Ardından bilateral filter, aşındırma ve eşik değeri karşılaştırması yöntemleri ile de iris bölgeleri bulunduktan sonra ekran üzerinde dinamik olarak farklı zamanlarda ve farklı koordinatlarda çıkan yazıların takip edilmesi beklenmektedir. Bu sayede güvenlik açığı olan sistemlere girişlerde biyometrik verileri kullanarak canlılık analizi yapılıp dolandırıcılık saldırıları önlenmiştir. Bu çalışmanın yapılmasında ki temel amaç mevcut güvenlik sistemlerine ucuz ve hızlı bir çözüm sunmaktır.

Biyometrik sisteme girişleri simüle etmek için gönüllüler üzerinde test edilmiş, canlılık veya dolandırıcılık atağı kararını vermeyi sağlayan %97 başarı oranına sahip bir algoritma geliştirilmiştir.

Anahtar Kelimeler: Biyometrik, sahtecilik, canlılık analizi, Dlib, yüz işaretleyicileri

ABSTRACT

Liveness Detection in Face Recognition Systems

Tugay BOZİK

Department of Electronics and Communication Engineering

Master of Science Thesis

Advisor: Assist. Prof. Dr.Nihan Kahraman

Nowadays, as computers are an important part of our daily life, human-computer interaction has increased considerably. With the continuous development of technology, this interaction plays a very important role in all areas. Recently, we see that this interaction also plays an important role in security. When using passwords, cards and keys in traditional security systems, copying, stealing or forgetting is a common issue. Applications requiring security; In areas where we understand the importance of mobile banking, bank applications and access control systems in a very clear way, it has been started to provide safer and more practical access of people to systems by replacing traditional security methods with biometric data. Biometric data is a term used for automated systems developed for identification by recognizing measurable physical and behavioral characteristics of individuals. The most commonly used feature in biometric data is face and eye biometrics. Systems accessed using this data are much more reliable. However, the vulnerability of biometric authentication systems to fraud and spoofing attacks is widely known. Trying to trick systems by simulating biometric data is the most common fraud attack.

In this study, a solution has been proposed by analyzing vitality against fraud attacks against facial recognition systems. Thanks to an algorithm running with the passing of a person against a camera to enter the system is intended to prevent the fake login to the system by giving the viability decision. It is possible to increase existing security levels with a low cost change over traditional biometric verification systems.

Using the Python programming language, it has benefited from the authority of the OpenCV image processing library. Dlib library is also used as image processing algorithm. A computer with an Intel i5 2.3GHz processor and 5MP standard webcam with 1024x768 resolution was used as hardware. At the same time, this software has been tested on the Raspberry Pi 3 Model B hardware and has achieved the same success. The face detector was detected by a figure detector algorithm. Afterwards, after the iris regions are found with bilateral filter, abrasion and threshold value comparison methods, it is expected to follow the texts dynamically at different times and at different coordinates on the screen. In this way, by using biometric data to access the vulnerable systems, vitality analysis was conducted and fraud attacks were prevented. The main purpose of this study is to provide a cheap and fast solution to the existing security systems.

An algorithm with a 97% success rate has been developed to simulate inputs to the biometric system, which has been tested on volunteers, allowing the decision of liveness or the attack of fraud.

Keywords: Biometrics, spoofing, liveness detection, Dlib, facial landmarks

1
Giriş

1.1 Literatür Özeti

Günümüzde teknolojinin gelişmesiyle birlikte güvenlik gerektiren sistemlerde birçok yenilikler olmuştur. Özellikle görüntü işleme konusunda yapılan yeni çalışmalar sayesinde biyometrik verilerin bilgisayar görüsüne uygun haline getirilmeleri kolay hale getirilmiştir. Biyometri, biyolojik verileri, yani bireyin kişisel bir nitelik ya da davranışını analiz ederek kimliğini doğrulama bilimidir [1].

Tüm biyometrik sistemler aşağıda açıklanmış olan beş özelliğe sahip olmalıdır [2]:

- Evrensellik: Tüm bireyler biyometrik özelliklere sahip olmalıdır.
- Eşsiz olma: Biyometrik karakteristiğin her insanda farklı bir şekilde yer alması.
- Süreklilik: Karakteristiğin zamanla değişmemesi.
- Elde edilebilirlik: Biyometrik özelliklerin bazı pratik cihazlarla ölçülebilir olması.
- Kabul edilebilirlik: Bireylerin biyometriğin ölçüm ve toplanmasında itirazları olmamalı.

Biyometrik tanıma sistemlerinin çeşitlerinin taradıkları özellikler aşağıdaki tabloda verilmiştir [2].

Biyometri, vücut ölçüleri ve hesaplamaları için kullanılan teknik terimdir. İnsan özellikleriyle ilgili ölçüleri işaret eder. Biyometrik kimlik doğrulama bilgisayar bilimlerinde bir tanımlama ve erişim kontrolü olarak kullanılır [3-4]. Ayrıca, gözetim altındaki gruplardaki bireyleri tanımlamak için kullanılır.

Tablo 1.1 Biyometrik Karakteristikler

Biyometrik karakteristik	**Özelliklerin açıklaması**
Parmak İzi	Parmak satırları, gözenek yapısı
İmza Tanıma	Basınç ve hız ile yazma farkları
Yüz geometrisi	Göz, burun vs arası uzaklıklar
İris Tanıma	İris deseni
Retina	Retina yapısına (desenine) göre
El Geometrisi	Parmak ve avuç içi ölçülerine göre
Parmak geometri	Parmak ölçme
El Damar yapısı	Elin arkası, parmak veya avuç içi damar yapısı
Kulak formu	Kulağın belirgin boyutları
Ses	Ton ya da ses rengi
DNA	Kalıtsal bir taşıyıcı olan DNA
Koku	Kokunun kimyasal bileşimi
Klavye vuruş	Klavye vuruşlarının ritmi (PC veya diğer klavye)

Tablo 2'de bazı biyometrik karakteristiklerin karşılaştırılması verilmiştir [2].

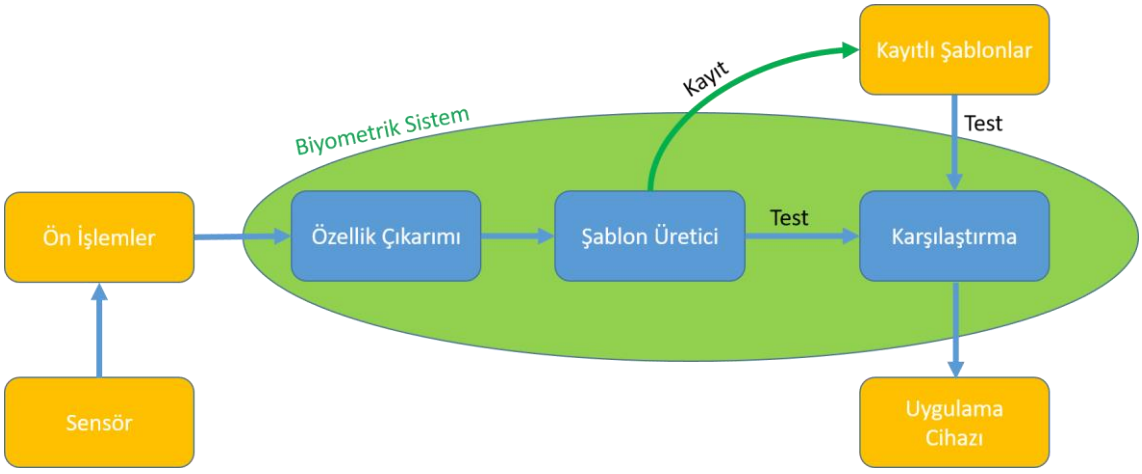
Tablo 1.2 Biyometrik Karakteristiklerin Karşılaştırılması [2]

Biyometrik Karakteristik	**Evrensellik**	**Eşsizlik**	**Süreklilik**	**Elde Edilebilirlik**	**Performans**	**Kabul Edilebilirlik**	**Yaygınlık**
DNA	Y	Y	Y	D	Y	D	D
Kulak	O	O	Y	O	O	Y	O
Yüz	Y	D	O	Y	D	Y	Y
Yüz Termogramı	Y	Y	D	Y	O	Y	D
Parmak İzi	O	Y	Y	O	Y	O	O
El Geometrisi	O	O	O	Y	O	O	O
İris	Y	Y	Y	O	Y	D	D
Retina	Y	Y	O	D	Y	D	D
İmza	D	D	D	Y	D	Y	Y
Ses	O	D	D	O	D	Y	Y
Y:Yüksek O:Orta D:Düşük							

Biyometrik tanımlayıcılar, bireyleri etiketlemek ve tanımlamak için kullanılan ayırt edici, ölçülebilir özelliklerdir [5]. Biyometrik tanımlayıcılar sıklıkla fiziksel ve davranışsal özellikler olarak sınıflandırılır [6]. Fiziksel özellikler vücudun şekli ile ilgilidir. Örnekler arasında, parmak izi, avuç içi damarları, yüz tanıma, DNA, avuç içi izi, el geometrisi, iris tanıma, retina bulunur, ancak bunlarla sınırlı değildir. Davranış özellikleri imza, yazı yazma şekli, bireyin yürüyüşü ve bireyin sesi olarak düşünülebilir ancak bunlarla sınırlı değildir [7]. Bazı araştırmacılar davranışsal ölçüt terimini, biyometrinin alt sınıfı olarak tanımlamak için ortaya atmıştır [8].

Daha geleneksel erişim kontrolü araçları arasında ehliyet veya pasaport gibi belirteç tabanlı kimlik sistemleri ve şifre veya kişisel kimlik numarası gibi bilgi tabanlı kimlik sistemleri yer almaktadır [5]. Biyometrik tanımlayıcılar bireylere özgü olduğundan, kimlik doğrulamada belirteç ve bilgi tabanlı yöntemlerden daha güvenilirdirler; Bununla birlikte, biyometrik tanımlayıcıların toplanması, bu bilgilerin nihai kullanımıyla ilgili gizlilik kaygılarını arttırmaktadır [5] [9-10].

Biyometrik sistemlerin genel çalışma mekanizması Görüntü Yakalama > Özellik Çıkarma > Şablon Oluşturma > Karşılaştırma şeklindedir ve Şekil 1'deki gibi ifade edilebilir.



Şekil 1.1 Biyometrik Sistem Blok Diyagramı

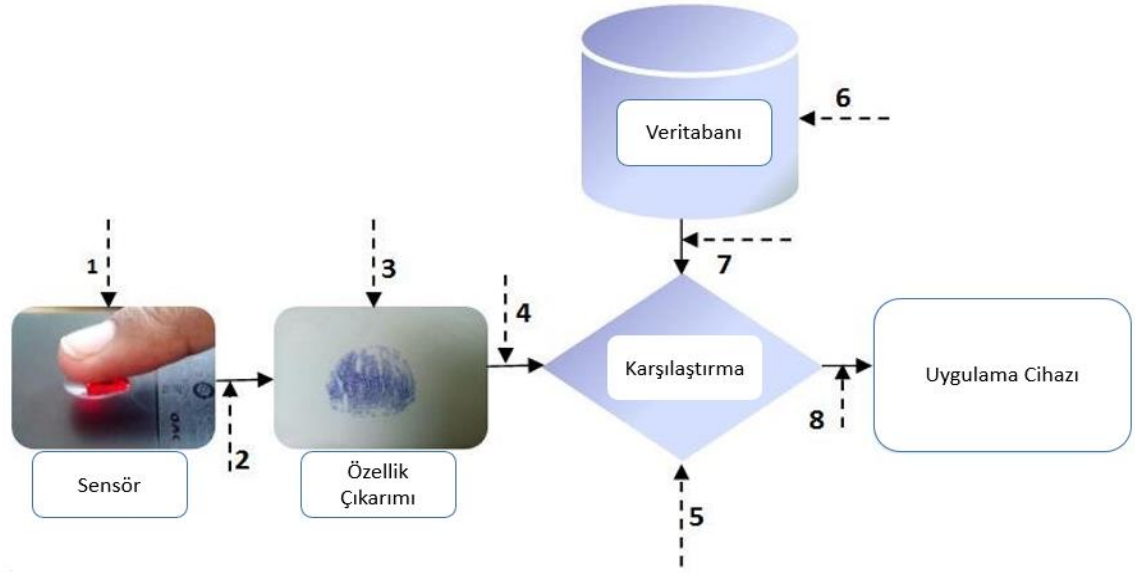
Biyometrik sistemler, fiziksel (pasif) ve davranışsal (aktif) biyometrik sistemler olmak üzere temelde 2 gruba ayrılır. Fiziksel biyometrik sistemler; parmakizi, el

geometrisi, yüz, ses, iris ve retina gibi kişide bulunan, diğer kişilerden ayrılmasını sağlayan sabit fiziksel özellikler üzerine kurulmuştur [11]. Davranışsal biyometrik sistemler ise; imza, yazı dinamiği, konuşma esnasındaki dudak hareketleri, yürüyüş şekli tanıma gibi belli bir zamanda belli amaçlar için gerçekleştirilmiş ve gene herkesin birbirinden farklı olarak gerçekleştirdiği davranışlar üzerine kurulmuştur.

Fiziksel (yüz, iris vb.) ve davranışsal özellikleri (ses, imza vb.) kullanan biyometrik tabanlı kimlik doğrulama sistemleri, gün geçtikçe daha popüler hale gelmekte ve sistemlerin güvenliğini artırmak için birçok uygulamada kullanılmaktadır. Geleneksel sistemler, yetkili bir kişi ile sisteme sahtekarlıkla erişebilecek izinsiz giriş yapan kişileri ayırt edememektedir. Biyometrik sistemler daha kullanışlıdır 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 savunmasızdırlar [12]. Biyometrik sistemde, Şekil 2'de gösterildiği gibi saldırıya uğrayabilecek sekiz saldırı noktası vardır. Bu saldırı noktaları doğrudan saldırılar ve dolaylı saldırılar olmak üzere iki kategoriye ayrılır.

Doğrudan saldırılar: Kullanılan işlem algoritması, özellik vektör formatı, vb. gibi sistem çalışması hakkında özel bilgi gerektirmeyen saldırıları işaret eder.

Dolaylı saldırılar: Doğrudan saldırıların aksine, bunlar saldırıyı başarılı kılmak için kimlik doğrulama sisteminin iç işleyişi hakkında bilginin gerekli olduğu saldırılardır. Biyometrik tabanlı bir kimlik doğrulama sisteminde bir sahtekâr tarafından saldırıya uğrayabilecek olan tüm yedi saldırı noktasını (2, 3, 4, 5, 6, 7, 8.) içerir.



Şekil 1.2 Biyometrik Sistemlere Atak Noktaları [12]

Bir sahtekarlık saldırısı, bir kişi verileri tahrif ederek ve dolayısıyla meşru olmayan erişim ve avantajlar elde ederek başka biri olarak maskelenmeye çalıştığında meydana gelir [13]. Örneğin; yüz tanıma sistemlerine karşı sahtekarlık saldırıları genellikle geçerli kullanıcının fotoğrafı, videosu veya 3D modelinden oluşur [14].

Sahtekarlık ataklarını önlemek için literatürde birçok çalışma bulunmaktadır. Bunlara örnek vermek gerekirse, multi-biyometrik verileri kullanarak, canlılık analizinde mimik taraması yaparak, göz kırpmaları sayarak, soru cevap tarzı ile kullanıcılardan bilgi alarak, yüz ifadelerinin değiştirilmesini kontrol ederek, ağız hareketlerini takip ederek sahtekarlık atakları önlenmeye çalışılmıştır [15].

Schwartz ve ark. [16], yayınladığı metotta yüz bilgisini tanımlamak için birkaç özellik tanımlayıcısı birleştirilmiştir. Bu yöntem şekil, renk ve doku gibi yüz bilgilerini açıklamak için, yüz bölgelerine ve çıkarılmış bütünsel özellik tanımlayıcılarına odaklanır. Gragnaniello ve diğerleri [17], anti-spoofing sistemlerinde canlılık tespit görevi için Weber Local Descriptor (WLD) dahil olmak üzere birçok tanımlayıcının potansiyelini değerlendirmektedir. LBP ve WLD'nin ayırt edilebilirliğini birleştiren Weber Local Binary Pattern (WLBP) [18] adlı diğer bir yerel tanımlayıcı, göz kırpma (canlılık) tespiti için etkili bir şekilde kullanılmaktadır [19]. Bazen, [20-22] gibi özellik öğrenme yöntemleri de,

boyutluluk sorununun lanetini önlemek için bu özellik çıkarma yöntemleriyle birlikte kullanılır.

Sahtekârlık saldırılarını önlemek için kullanılan yöntemler kendi arasında da farklılık göstermektedir. Örneğin; göz kırpma sayarak canlılık analizini birkaç farklı yöntem ile yapmak mümkündür. Moriyama'nın göz açıp kapama algılama yöntemi [23], göz bölgesindeki ortalama yoğunluktaki değişimin, aydınlatma koşullarına ve gürültüye karşı hassas olmasına dayanır. Ji ve arkadaşları [24], sürücü yorgunluğunun tahmin etmek için göz açıp kapamalarını tespit etmek için aktif bir IR kamera kullanmaya çalışmışlardır. Pan ve arkadaşları [25], adaptif güçlendirme algoritmasından türetilen ayırt edici bir ölçüm olan göz yakınlığını, hesaplama etkinliği ve algılama doğruluğu değerlendirmişlerdir.

Sonuç olarak kullanıcılara ait kişisel verilerin korunması, çeşitli yerlere erişim kontrolü, banka işlemleri, tesis veya bina giriş kontrolü gibi birçok alanda güvenliğin sağlanması gerekmektedir. Yalnızca yetkili kişiye erişim izni verilmesi gereken bu ve benzeri durumlarda, çeşitli şifreleme yöntemleri (kimlik kartı, parola, manyetik kart vb.) kullanılmaktadır. Geleneksel şifreleme yöntemlerinin kolay aldatılabilmesi, yavaş çalışması, maliyetli olması, çalınmasının kolay olması veya kolay unutulması gibi kullanıcıyı zor durumunda bırakabilecek dezavantajlar, alternatif şifreleme yöntemleri arayışını doğurmuştur. Bu arayışın doğal bir sonucu olarak, biyometrik doğrulama sistemleri günlük hayatta daha fazla yer almaya başlamıştır [26]. Bu nedenle, bu tez çalışmasında yüz tanıma sistemlerini kandırmaya yönelik saldırılara karşı önlem almak için canlılık analizi yapılmıştır.

1.2 Tezin Amacı

Bu tez çalışması çerçevesinde geliştirilmiş olan yöntemin öncelikli hedefi, biyometrik erişim kontrolü gerektiren uygulamalarda sahtekarlık yöntemleri ile sistemleri kandırmaya yönelik spoofing ataklarını önlemektir. Özellikle banka uygulamaları, mobil uygulamalar, şifreler ile açılan uygulamalar bu yöntemin kullanımı için uygun birer alandır. Bu amaçla seçilen yöntem, kullanıcıların görüntüleri gerçek zamanlı bir sistemden elde edildikten sonra bu görüntülere gerekli morfolojik işlemlerin uygulanması, kullanıcının yüz tespiti edilmesi, kernel matrislerinin oluşturulup, yüz içerisinden göz bölgelerinin çıkarılması, göz bölgeleri içerisindeki irislerin belirlenip, bulunan irislerin merkez noktalarının takibinin yapılmasını sağlar. Bu yöntem sayesinde yüz tanıma sistemlerinde canlılık analizi problemlerine çözüm bulmak amacıyla kişilere takip edildiklerini hissettirmeden ekranda çeşitli yerlerde farklı zamanlarda ekran yazıları çıkartılarak kullanıcıların bu yazıları okumaları esnalarındaki iris hareketleri takip edilip, ardından sistemin ekrandaki yazının konumu ile kullanıcıların baktıkları yönlerin eşleşip eşleşmediğini onlara fark ettirmeden kontrol etmektir.

1.3 Hipotez

Günümüzde güvenlik konusundaki yüz tanıma sistemlerinde yapılan çalışmalarda performans ve maliyet konularına dikkat edilmiş ancak biyometrik verilerin elde edilmesi konusundaki zorluklar ihmal edilmiştir. Erişim kontrolü sağlayan sistemlerde fotoğraf çekerek yüz tanıma yapanlar, video çekerek yüz tanıma yapanlar var. Fotoğraf çekerek yüz tanıma yapan sistemleri kandırmak kolay, ancak video çekerek yüz tanıma yapan sistemlerde biraz canlılık analizine bakma durumu var. Ama bu canlılık analizine bakma durumu son yıllarda gerçekleştiği için eski kurulan sistemlerle çalışan güvenlik önlemleri alan yerler yüz tanıma sistemlerinde aynı anda canlılık analizine bakmıyorlar. Yapılan literatür araştırmalarında bir çok farklı kandırma yöntemi incelenmiştir. Bu çalışmada amacımız portatif bir taşınabilir, ucuz maliyetli bir sistem üretip eski yüz tanıma sistemlerini kullanan yerlere çözüm üretmektir. Bunun içinde hızlı çalışan bir algoritmayı düşük maliyetli bir board üzerinde tasarladık. Bu çalışmada kullanıcılara hissettirmeden onların iris

pozisyonlarını ekran yazılarını okurken takip edilmesi konusundaki problemler ve bunun ardından oluşturulan algoritma ile gerçek zamanlı olarak yüz tanıma sistemlerini kandırmaya yönelik problemler giderilmiştir. Ayrıca günümüzde kullanılan güvenlik gerektiren uygulamalarda mevcut sistemler üzerinde çok fazla değişiklik yapmadan basit bir donanım ve yazılım değişikliği ile sistemlerin güvenlik seviyeleri biraz daha arttırılabilir hale getirilmiştir.

2
Görüntü İşleme Yöntemleri ile Kullanıcıların Yüzdeki Biyometrik Verilerinin Tespit Edilmesi

Biyometrik erişim kontrolü isteyen uygulamalarda kullanılmak üzere canlılık analizi problemlerine çözüm sunan yöntemden bahsedilmiştir. Bu önerilen yöntemin ilk adımı olan kullanıcıların standart bir web kamerası üzerinden görüntülerinin elde edilmesi kısmında hangi görüntü işleme algoritmaları kullanıldığından bahsedilmiştir.

2.1 Önerilen Yöntem

Yüz tanıma sistemlerini kandırmaya yönelik atakları önlemek için canlılık analizi yöntemi temel olarak iki aşamadan oluşmaktadır;

- Görüntü işleme ve yüz biyometrik verilerinin belirlenmesi
- Sistemin gösterdiği noktalarla ile kullanıcıların baktığı yön arasında doğrulama yapılıp canlılık kararının verilmesi

Algoritma ilk olarak kamera açıldığı anda görüntü üzerindeki yüzleri tespit etmek ile işe başlar. Bulunan yüz içerisinden ilgi bölgesi (ROI) çıkarılır. Bu çalışmadaki amaç iris merkezi ile koordinat takibi olduğu için ROI göz bölgesidir. ROI'nin yüz bölgesinden yola çıkılarak basit hesaplamalarla elde edilmesi yerine daha hassas belirleme yapmak adına yüzdeki belli noktalar referans alınabilir. Birçok amaç için kullanılmak üzere yüzdeki belli noktaları çıkartan algoritmalar önerilmiştir. Bunlardan en geçerli olanı günümüzde yüz tanıma uygulamalarında aktif şekilde kullanılan yüz işaret yerleridir (Facilal Landmarks-FL) [27]. FL noktaları yüzde burun, kaşlar, gözler ve dudak gibi önemli bölgeleri işaret etmek adına geliştirilmiştir. Bu FL noktaları mimik tanıma, duygu durum tespiti, cinsiyet ve yaş tespiti gibi uygulamalar tarafından kullanılmaktadır. Bu çalışmada, ROI'nin daha sabit ve her görüntü karesinde olabildiğince aynı bölgenin belirlenmesi için

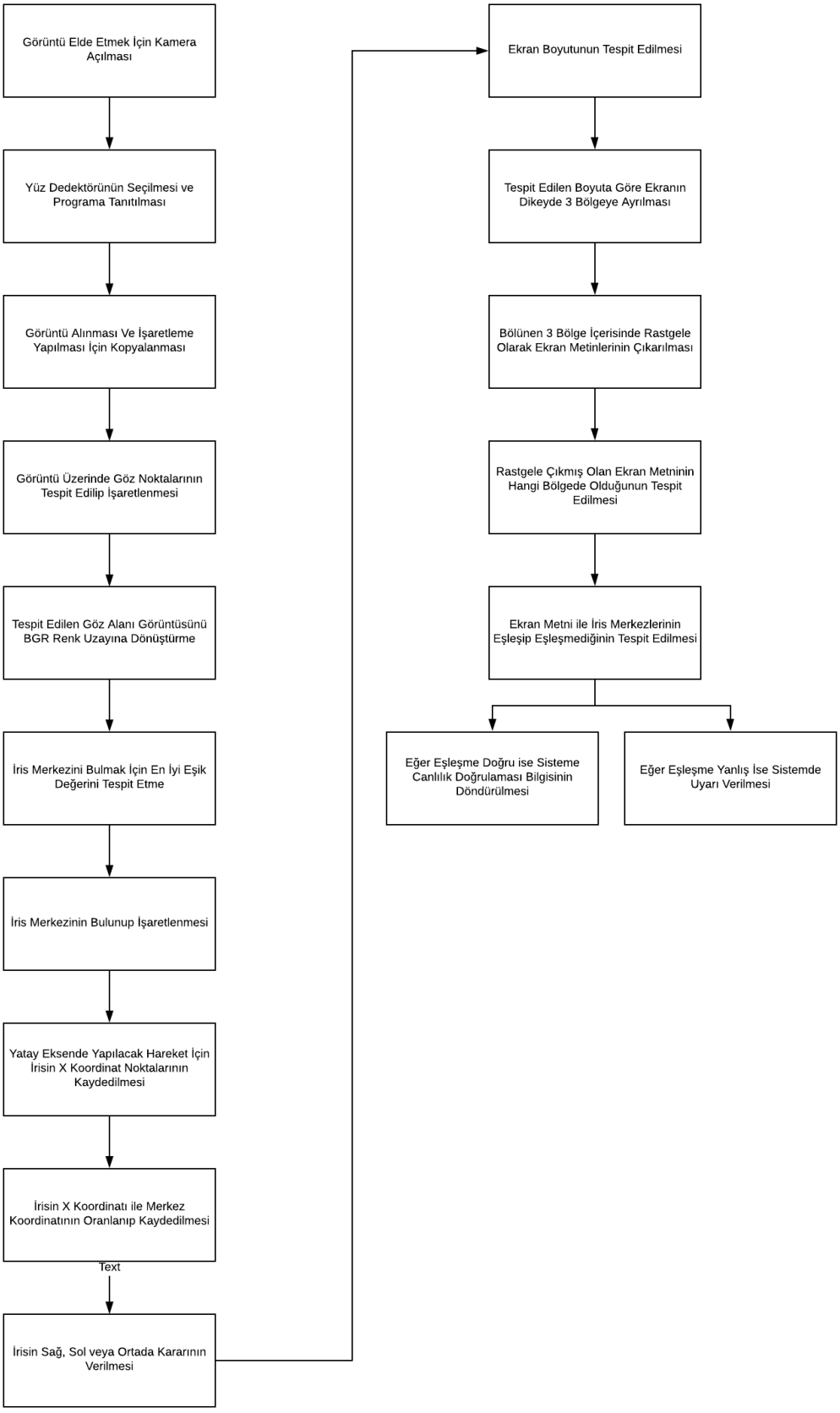
FL'lerden faydalanılmıştır. FL'ler içerisindeki sağ gözü ve sol gözü işaret eden koordinatlar belirlidir. Göz bölgesi tespit edilip çıkarıldıktan sonra elde edilen bu görüntü üzerinde morfolojik işlemler yapılır. Bunun yapılmasındaki amaç görüntü içerisindeki öznitelik verilerini daha anlaşılır hale getirmektir. Bu yapılan işlemler Bölüm 2.2'de detaylı olarak anlatılacaktır. Elde edilen görüntü üzerinden OpenCV kütüphanesini kullanarak kapalı kontur bulma işlemi yaparak iris bölgesinin tespit edilmesi ve pozisyonunun tahmin edilmesi sağlanır. OpenCV (Açık Kaynak Bilgisayarlı Görme Kitaplığı) açık kaynaklı bir bilgisayar görme ve makine öğrenimi yazılım kütüphanesidir. OpenCV, bilgisayarlı görüntü uygulamaları için ortak bir altyapı sağlamak ve ticari ürünlerde makine algı kullanımını hızlandırmak için inşa edilmiştir. BSD lisanslı bir ürün olan OpenCV, işletmelerin kodu kullanmasını ve değiştirmesini kolaylaştırır. Kütüphane, hem klasik hem de modern bilgisayar görmesi ve makine öğrenmesi algoritmalarının kapsamlı bir setini içeren 2500'den fazla optimize edilmiş algoritmaya sahiptir. Bu algoritmalar, yüzleri algılamak ve tanımak, nesneleri tanımlamak, videolarda insan hareketlerini sınıflandırmak, kamera hareketlerini izlemek, hareketli nesneleri izlemek, nesnelerin 3B modellerini çıkarmak, stereo kameralardan 3B nokta bulutları üretmek, görüntüleri yüksek çözünürlükte üretmek için kullanılabilir[28].

İkinci aşamada ise iris pozisyonu görüntü işleme algoritmaları sayesinde belirlendikten sonra canlılık analizi yapmak için ekran üzerinde farklı yerlerde metinler yazdırmaktır. Bunun için yine OpenCV Kütüphanesi ve Python programlama dilinde matematiksel işlemler yapmaya yarayan kütüphanesi Numpy kullanılmıştır. Ekran boyutlarını OpenCV kütüphanesinin fonksiyonları ile elde ettikten sonra Numpy Kütüphanesi yardımı ile bu değerleri dikeyde üç bölgeye ayrılacak şekilde programa komutlar veririz.

Üçüncü aşama ise canlılık bilgisinin sisteme geri döndürülmesidir. Bunun için önerilen algoritmada kullanıcıların ekran üzerinde baktığı yöne tespit edildikten sonra, ekranda farklı zaman aralıklarında farklı bölgelerde dinamik olarak çıkan yazıları takip etmesi sağlanmıştır. Aynı zamanda ekranda ilk yüz tespit edildiği zamandan canlılık kararı verilen zamana kadar geçen süre içerisinde insan gözünün kırpma miktarı hesaplanır. Bu canlılık kararı vermekte destekleyici bir unsur olarak

kullanılır. Eğer kullanıcıların baktığı yön ile ekranda çıkan metinlerin koordinatları belirlediğimiz eşik değeri kadar deneme sonrasında birbiri ile eşleşiyorsa sisteme canlılık bilgisi döndürülür. Aksi halde ise, yani belirlenen eşik değeri kadar deneme sonrasında kullanıcıların bakış yönü ile ekran metinlerinin koordinatları eşleşmiyorsa sisteme sahtekarlık atağı bilgisi döndürülür.

Şekil 3'te, yukarıda bahsedilen aşamaları içeren tezde önerilen sisteme ait blok diyagramı görülmektedir.



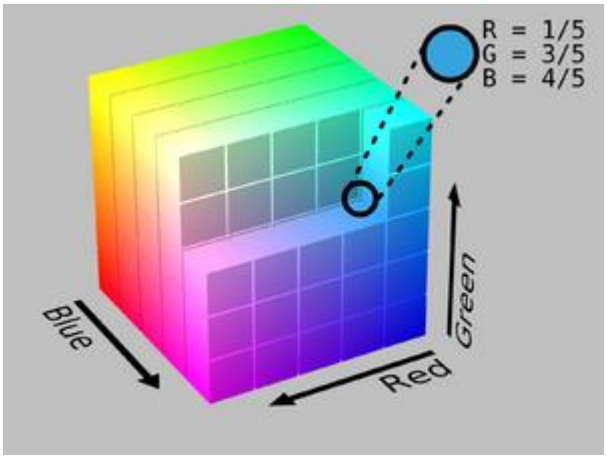
Şekil 2.1 Önerilen Algoritmanın Blok Diyagramı

2.2 Görüntünün Elde Edilmesi

Yüz tanıma sistemlerinde canlılık analizi yapılması amacı ile oluşturulacak olan sistemde ilk olarak görüntünün elde edilmesi işlemi gerçekleştirilmiştir. Gerçek zamanlı bir sistem oluşturulması nedeniyle görüntüler kameranın sürekli şekilde çalıştırılmasıyla elde edilmiştir. Kameradan elde edilen görüntülerden belli aralıklarla tek bir resim karesi çekilerek gerekli işlemler bu resim üzerinden gerçekleştirilmiştir. Kullanılacak sistemde maliyetin ve işlem hızının önemli olması nedeniyle çözünürlük 640x480 piksel olarak belirlenmiştir. Aynı zamanda Logitech C170 markalı 5 MP çözünürlükle standart web kamerası kullanılarak görüntüler elde edilmiştir. Bu kameranın görüntü yakalama hızı 640x480 çözünürlükte 30 FPS'dir. Yani bu kamera ile yaklaşık 33 ms'de bir görüntü elde edilir. Bu çalışmada 60 ms'de bir görüntü alınmıştır. Yani yaklaşık olarak saniyede 15-16 görüntü elde edilmiştir. Görüntülerin bu şekilde alınması hem sistemin maliyetinde hem de işlem hızında kazanç sağlamıştır. Elde edilen görüntüden yüz tanıma sistemlerinde canlılık kararını amacıyla öncelikle yüz bölgesinin tespiti işlemi gerçekleştirilmiştir.

2.3 Resmin Gri Tonlama Uzayında Elde Edilmesi

Elde edilen görüntünün bilgisayar tarafından işlenebilmesi amacıyla bilgisayarların da anlayacağı bir uzayda yorumlanması gerekmektedir. Bu amaçla elde edilen görüntü BGR uzayında iken gri tonlama uzayına dönüştürülmüştür. Görüntü işleme kütüphanesi olan OpenCV'nin standart kameralardan görüntü almak için kullandığı fonksiyonu olan VideoCapture.read() fonksiyonu giriş görüntüsünü varsayılan olarak BGR formatında kaydeder. BGR, Mavi, Yeşil, ve Kırmızı ana renklerinin oluşturduğu bir renk uzayıdır. BGR renk uzayı en çok bilinen RGB renk uzayından türetilmiş bir renk uzayıdır. Örnek vermek gerekirse, her bir renk kanalı 8 bitten oluştuğu için RGB renk uzayında 24 bitlik bir renk bilgisi bulunmaktadır. Bunların içerisinde en az önemli bitleri olarak Mavi renklerin bulunduğu bitler temsil ederken, en önemli bitleri Kırmızı renklerin bitleri temsil eder. BGR renk uzayında ise durum tam tersidir. En önemli bitleri Mavi renklerin bitleri oluştururken, Kırmızı renklerin olduğu bitler en az önemli bitlerdir.



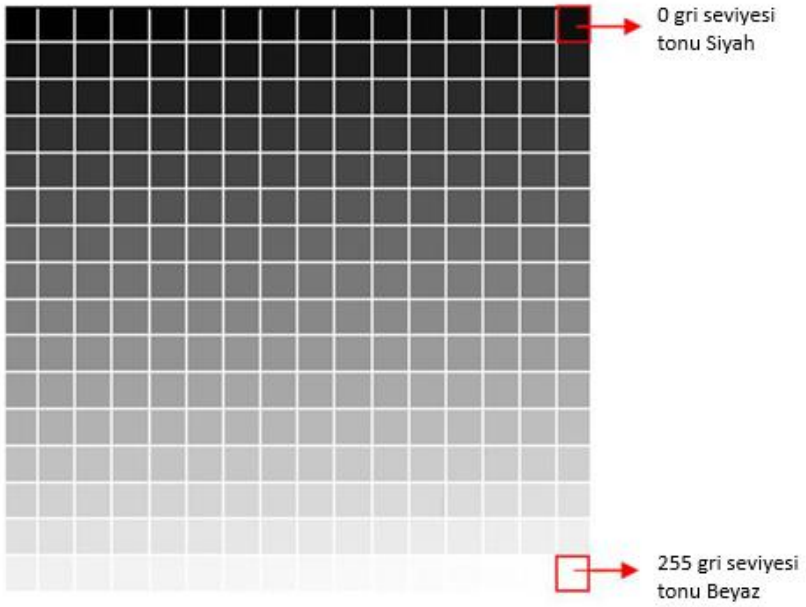
Şekil 2.2 RGB Renk Uzayı Renk Kübü

Dijital görüntünün her bir pikselinin sahip olduğu parlaklık değeri gri seviyeler olarak adlandırılır. Her bir pikseldeki parlaklık değerinin kodlandığı bit sayısına göre gri seviye aralığı belirlenir. Gri seviyeni sınırlarında iki renk vardır, siyah ve beyaz. Bu ikisi arasında kodlanan görüntülere ise gri-ton (gray scale, monochromatic) görüntüler adı verilir. Bu resimler bilgisayarda 8 bit formatında saklanır. Bunun anlamı her piksel 8 bit ikili kod ile saklanır. Yani 2^8=256 olarak gösterilirse 0-255 arasında değer alır. 0 siyah rengi gösterirken, 255 beyaz rengi göstermektedir.

Bir griton resim 800x600 piksel boyutlarında olursa içerisinde 480.000 piksel olacaktır. Her piksel 8 bit=1 byte hafızada yer alacağına göre resmin tamamı 480 kByte=0,48 MByte yer kaplayacaktır. Aynı resim renkli olsayda, her renk (RGB-RedGreenBlue) benzer şekilde 256 ton renk alarak 2^8*3=2^{24} yani 24 bit yer kaplar. Bu durumda aynı resim bu sefer 3 katı yer kaplar. Bu nedenle görüntü işleme algoritmalarını RGB resimler üzerinde değilde Gri ton resimler üzerinde yapmak daha hızlı bir sonuç almamıza yardımcı olmaktadır. Renkli dijital bir görüntüyü gri-ton bir görüntüye dönüştürme işlemi aslında RGB renk modelinde belirtilen her bir renk bandına karşı düşen gri-ton görüntülerin ölçeklendirilmesinden başka bir şey değildir. Normalde üç rengin değerini toplayıp üçe bölerek gri tonu elde edebiliriz. Fakat bu gözümüzün farklı renkleri farklı algılama hassasiyetini tam yansıtmaz. Bu nedenle aşağıdaki formüllerde verildiği gibi ölçekleme yapılmalıdır. İlk verilen formül en gerçekçi olanıdır.

$$Gri\_Degeri = 0.299 \times R + 0.587 \times G + 0.114 \times B \quad (2.1)$$

Şekil de 16 × 16 'lık bir ızgara üzerinde 256 farklı gri seviyenin gösterimi verilmiştir.



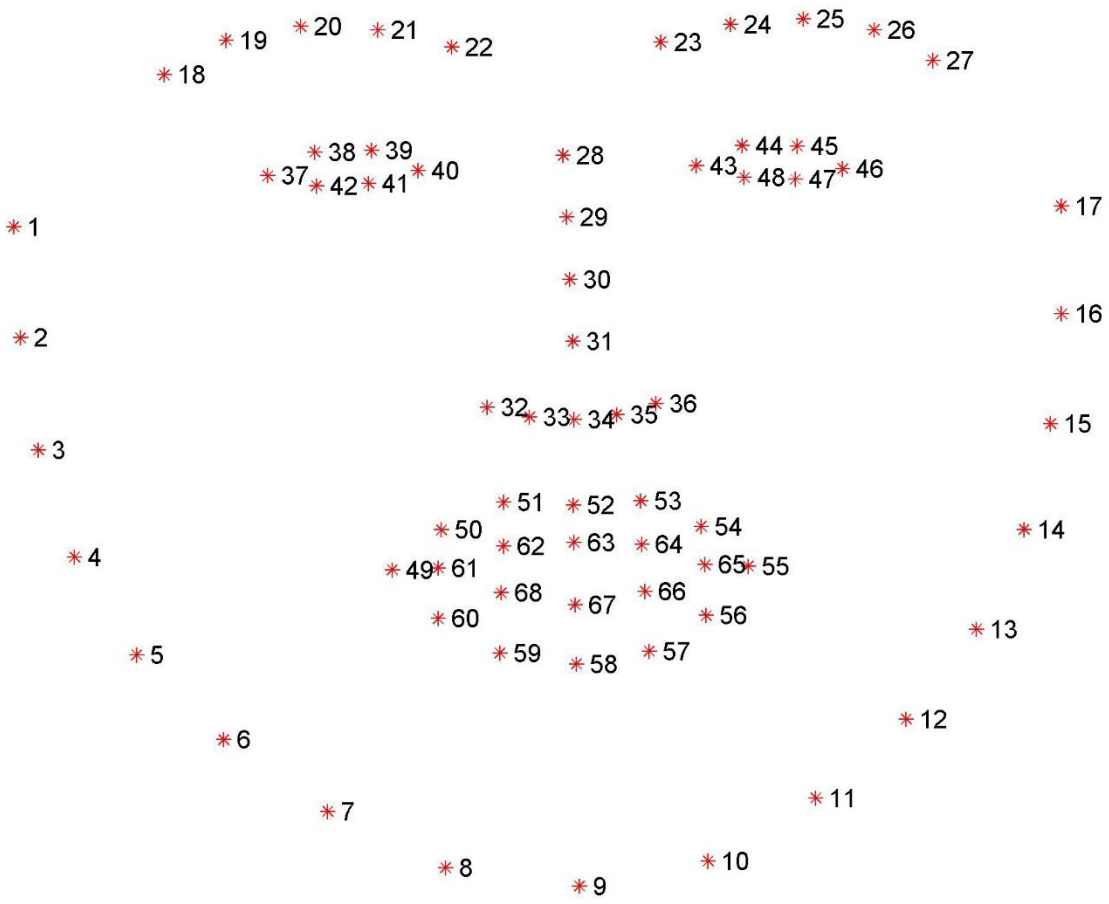
Şekil 2.3 Gri Ton Renk Uzayı

2.4 Yüz Tespit Etme

Yüz tespiti, yüz tanımanın ilk önemli adımıdır. Temel olarak, görüntüyü biri yüz içeren diğeri yüz olmayan bölgeleri temsil eden olarak iki parçaya böleceği için aslında görüntü bölümleme problemidir. Yüz algılama performansı, tüm tanıma sisteminin performansını etkiler.

İlk olarak kamera çalıştığı anda görüntü üzerindeki kişilerin yüzlerinin tespit edilmesi işlemi yapılır. Bu işlemi başarılı bir şekilde yapabilmek için kameradan gelen görüntü öncelikle çeşitli morfolojik işlemlerden geçer. Yukarıda bahsedildiği gibi kameradan gelen görüntü varsayılan olarak BGR renk uzayından Gri ton görüntüye dönüştürülür. Ardından görüntü içerisinde yüz bulma algoritması için Dlib kütüphanesinin yüz bulma dedektörü tercih edilmiştir [29]. Yüz bölgesinin bulunması ve istenilen analiz bölgesinin belirlenmesi aşaması sinyalin kalitesi ve

devamlılığı için ciddi önem arz ediyor olmasından dolayı, yüz bulma başarısı gayet yüksek olan bu kütüphane tercih edilmiştir. Sharma ve diğerlerinin [30] çalışması, Dlib kütüphanesinin CNN tabanlı yüz bulma algoritmasını diğer algotirmalarla farklı ortam koşullarında karşılaştırmış ve %96 yüz bulma başarısı ile diğerlerinin içinde en iyi sonucu veren algoritma olduğunu belirtmiştir. Singh ve diğerleri, Ten Rengi" esas alınarak yüz algılama algoritmalarının detaylı bir deneysel çalışmasını yapılmıştır. Bu çalışma için üç renk uzayı, RGB, YCbCr ve HSI ana odak noktaları olmuştur [31]. Bir diğer çalışmada Zangana ve arkadaşları [32], yüz tanıma sistemlerindeki problemlere çözüm olması amacıyla RGB renk uzayında görüntüler ile çalışmayı değil de YCbCr ve HSV renk uzaylarını kullanmışlardır. Chow ve arkadaşları [33], yüz hatlarını bulmak için çeşitli deforme olabilir şablonlar kullanırken Jeng ve arkadaşları [34] geometrik ilişkilere dayanarak yüz özelliklerinin tespiti ve doğrulanması üzerinde çalışılmıştır. Bu çalışmada, yüz tespit etme algoritması olarak Dlib kütüphanesinin yüz dedektörü kullanılmış olup diğer çalışmalarla karşılaştırıldığında hem istenilen bölgenin analiz edilmesine kolaylık sağlamasından hem de %96 başarı oranına ulaşmasından dolayı seçilmiştir. Dlib kütüphanesinin dezavantajı olarak yüzün kamera karşısında öne doğru eğilmesi anlarında yüz bölgesi tespiti zorlaşmaktadır. Bu nedenle kamera karşısında düz bir bakış ile bakılması doğruluğu arttıracaktır.

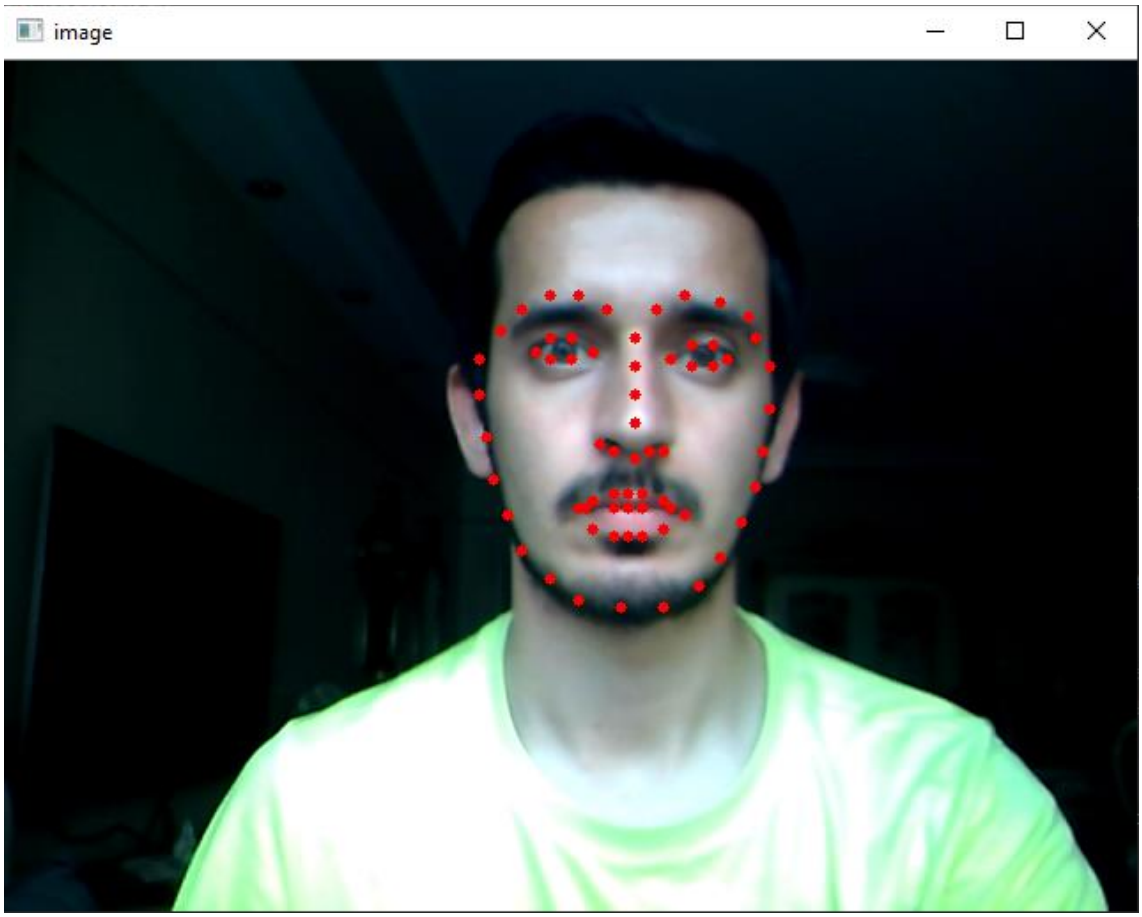


Şekil 2.4 Dlib 68 Nokta Yüz İşaretleyicisi [51]

2.5 Göz Alanı Tespit Etme

Mevcut göz algılama yöntemleri iki kategoriye ayrılabilir: aktif ve pasif göz algılama [35]. Aktif algılama yöntemleri, göz bebeği merkezlerini hızlıca bulmak için özel aydınlatma ve IR kameraları kullanır. Dezavantajları, özel aydınlatma kaynaklarına ihtiyaç duymaları ve dış ortamlarda daha fazla yanlış algılamaya sahip olmalarıdır. Pasif yöntemler doğrudan görsel spektrumdaki ve normal aydınlatma koşulundaki görüntülerden gözleri algılar. Bazı geçmiş çalışmalar, gözlerin görüntü gradyanları [36] ve projeksiyon [37] gibi farklı göz özelliklerine dayanarak lokalize olmasını sağlar. Ancak, bu özellikler görüntü gürültüsüne duyarlıdır. Huang ve Wechsler optimal Dalgacık paketlerini seçer ve gözü ve gözü olmayan Radyal Temel Fonksiyonlar (RBF'ler) ile sınıflandırır [38]. Yong ve diğerleri [39] 'da, AdaBoost yöntemi Haar özellikli hem yüz hem de göz dedektörü eğitmek için kullanılır.

Görüntüde yüz bölgesi bulunduktan sonra yüzün belli bir alanının analiz edilmesi gerekmektedir. Canlılık analizi yapılması için önerilen algoritmada kullanıcıların iris merkezlerinin tespitinin yapılması kritiktir. Bu nedenle, tespit edilen yüz alanı içerisinde göz alanını tespit etmek için Dlib kütüphanesinin yüz dedektöründe ilgili işaretleyici noktalarını programa iletiriz.



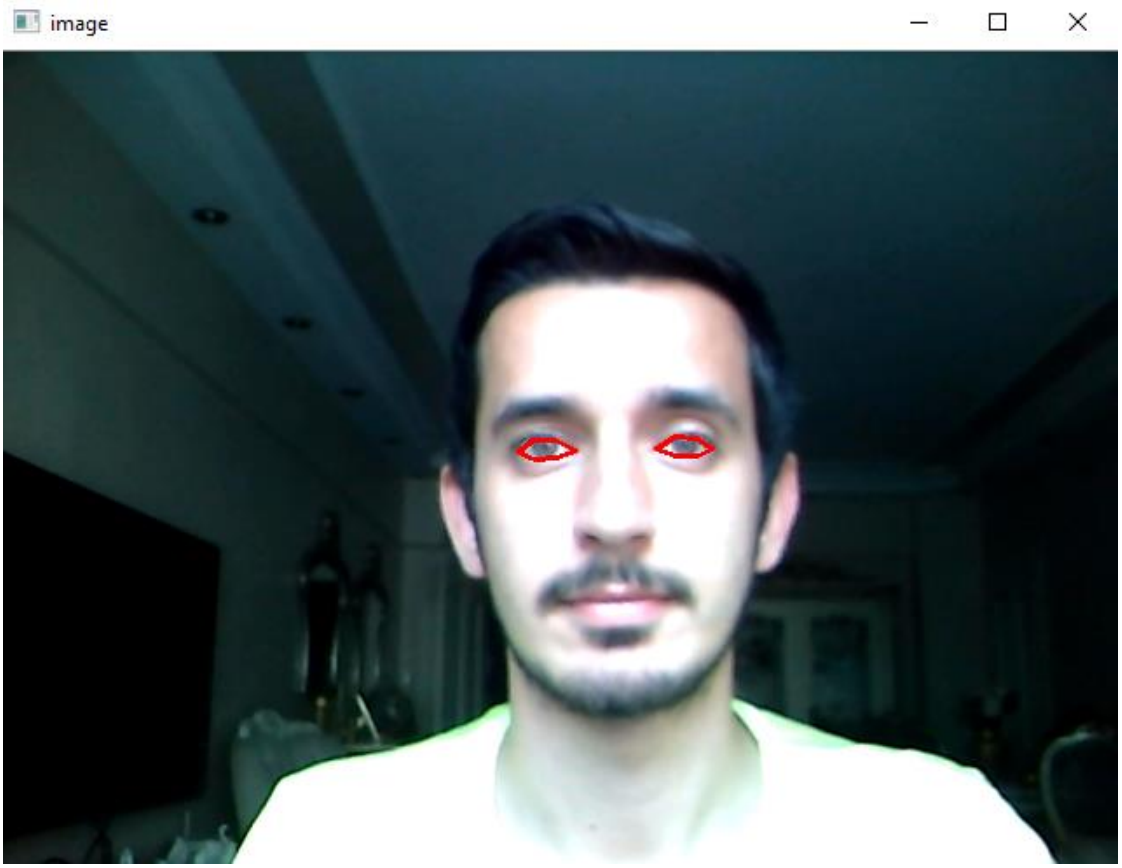
Şekil 2.5 Dlib 68 Yüz Noktası Maskesi

Yukarıdaki şekilde FL'ler ile gösterilen noktalar yüzdeki her bir özelliği belirtmektedir.

Görüntü üzerinden kullanıcıların gözlerine erişmek için aşağıdaki koordinatları kullanırız;

- Sağ Göz Noktaları : [37, 38, 39, 40, 41, 42]
- Sol Göz Noktaları: [43, 44, 45, 46, 47, 48].

Bu işaretleme koordinatları sayesinde canlı görüntü üzerinden yüz bölgesi tespit edilmiş olan kullanıcının göz bölgeleri ayrı ayrı bulunmuş olur. Bu çalışmada kullanılan göz bölgesini tespit edilmesi algoritması bazen ortam ışığından ve yansımalardan etkilenebilmektedir. Ancak, homojen aydınlatma olan bir sistem kurulursa bu sorun büyük ölçüde çözülmüş olacaktır.



Şekil 2.6 Dlib ile Gözlerin Ayrı Ayrı Belirlenmesi

2.6 İris Bölgesi Tespit Etme

Canlılık analizi yapılmak üzere kullanılacak olan algoritmanın temel prensibi kullanıcıların bakış yönlerini takip etmektir. Kullanıcıların bakış yönlerini, Bölüm 2.5'te anlatıldığı üzere göz bölgeleri tespit edildikten sonra takip ederiz. İris, kişiden kişiye göre değişken olmasından dolayı güvenlik için kullanılan en önemli

biyometriklerden biridir. Bu çalışmada göz bölgesi içerisinden iris alanını tespit ederek, iris merkezinin koordinatlarını takip etmek amaçlanmıştır.

İris bölgesinin tespiti için literatürde çok sayıda yöntem önerilmiştir. Bazı algoritmalar her iki gözün irislerini tespit etmek için kenar tespiti ve sonrasında Hough dönüşümü yöntemlerini kullanır [40-44]. Daugman ve arkadaşlarının [45] yaptığı çalışmada, irisin iç ve dış çemberlerinin sınırlarını belirlemek için integro-farksal (integro-differential) operatör önerilmektedir. Bazı çalışmalarda ise irisin yansıtma özelliğinden yararlanılarak IR kamera ile alınan görüntülerden iris tespiti yapılmaktadır [46]. Bununla birlikte, iris yüze kıyasla oldukça küçük olduğu için irisin Hough dönüşümünün tüm yüz bölgesine doğrudan uygulayarak doğru şekilde tespit edilmesi zordur. Chow ve Li [43] bu sorunu çözmek için bir algoritma önermiştir. Bu algoritma, yoğunluk görüntüsündeki vadilerden göz pencerelerini seçer.

Bu çalışmada, iris bölgesini tespit etmek için Dlib kütüphanesinin yüzdeki özellik işaretleyicilerinden yararlanarak elde ettiğimiz göz bölgeleri içerisinde öncelikle morfolojik işlemler yapılmıştır. İlk olarak giriş görüntüsüne Bilateral filtre uygulanmıştır. Bilateral Filtre, görüntüler için doğrusal olmayan, kenar koruyucu ve gürültü azaltıcı bir düzeltme filtresidir. Her pikselin yoğunluğunu, yakınındaki diğer piksellerden gelen yoğunluklarının ağırlıklı ortalaması değerleriyle değiştirir. Bu ağırlıklı ortalama bir Gauss dağılımına şeklinde olabilir. Önemli olarak, ağırlıklı ortalamalar sadece öklid piksel mesafesine değil, aynı zamanda radyometrik farklılıklara da (örneğin, renk yoğunluğu, derinlik mesafesi vb.) bağlıdır. Bu sayede görüntüdeki keskin kenarlar korunur. Bilateral Filtrenin matematiksel ifadesi şöyledir;

$$I_{filtre}(x) = \frac{1}{W_p} \sum_{x_i \in \Omega} I(x_i)\, f_r(\|I(x_i) - I(x)\|) g_s(\|x_i - x\|) \tag{2.2}$$

ve normalleşme terimi, W_p , olarak tanımlanır

$$W_p = \sum_{x_i \in \Omega} f_r(\|I(x_i) - I(x)\|) g_s(\|x_i - x\|) \tag{2.3}$$

Burada,

I_{filtre}, filtrelenmiş görüntü,

I, filtrelenecek görüntü,

x, filtrelenecek mevcut pikselin koordinatları,

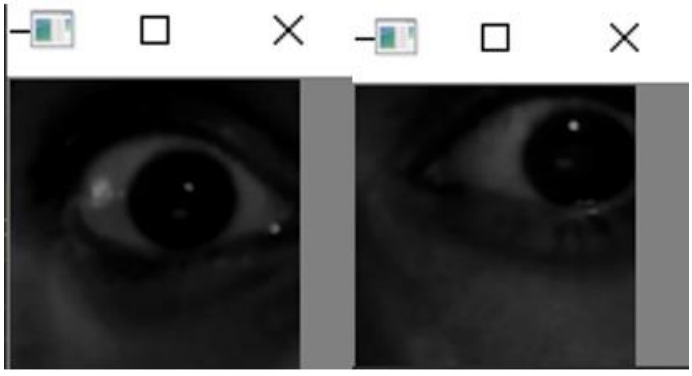
Ω, x'de ortalanan pencere,

f_r, yoğunluklardaki farklılıkları yumuşatmak için kullanılan aralık çekirdeğidir,

g_s, koordinatlardaki farklılıkları yumuşatmak için kullanılan uzaysal çekirdeğidir.

Görüntüyü bilateral filtreden geçirdikten sonra 3x3 boyutundaki Kernel matrisi ile aşındırma (Erosion) işlemi yapılır. Aşındırma işlemi görüntü işlemedeki en temel operatörlerden biridir. Aşındırma ikili bir görüntüde bulunan nesnelerin boyutunu seçilen yapısal elemente bağlı olarak küçültme işlemidir ve birbirine ince bir gürültü ile bağlanmış iki veya daha fazla nesneyi birbirinden ayırmak için kullanılır.

Gri tonlamalı olarak dönüştürülen giriş görüntüsüne aşındırma işlemi uygulayarak görüntünün içerisindeki kenarları belirleme işlemi sağlanmış olur. Bu kenar belirlemeden sonra eşik değeri yöntemini uygulayarak yeni görüntünün üzerinde kenarların daha net ortaya çıkması sağlanmıştır.



Şekil 2.7 Gri Tonlama Seviyesinde İris Görüntüleri

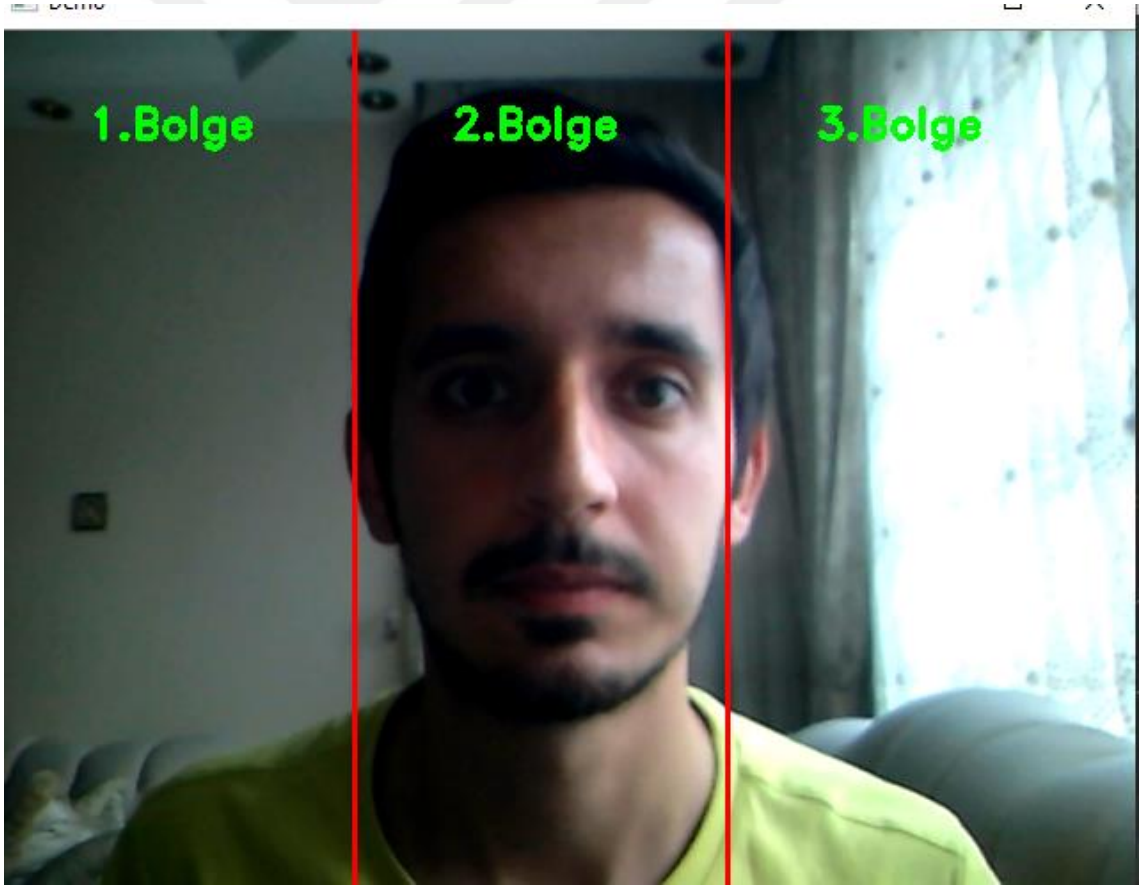
3
Canlılık Kararını Vermek için Doğrulama Yapılması

Canlılık analizini yapmak için literatürde farklı olarak birçok metot önerilmiştir. Bazı çalışmalarda göz kırpmalarını sayarak [47], kullanıcılara soru sorup cevap bekleyerek, ya da birden fazla biyometrik özelliği birleştirerek canlılık analizi yapılmaktadır. Bu çalışmada, ilk aşamada kamera çalıştığı andan itibaren kullanıcıların göz kırpmaları sayılmaya başlanır. Göz açıp kapama, göz kapaklarının hızlı bir şekilde kapanması ve açılmasının fizyolojik bir aktivitesidir; bu, gözyaşlarının kornea ve konjonktivanın yüzeyinden tahriş edici maddeleri uzaklaştırmasına yardımcı olan gözlerin temel bir işlevidir. Göz kırpma hızı, yorgunluk, duygusal stres, davranış kategorisi, uyku miktarı, göz yaralanması, ilaç ve hastalık gibi unsurlarla değişebilse de, araştırmacılar, bir insanın dinlenme halinde göz kırpma oranını dakikada yaklaşık 15 ila 30 göz kırpma olduğunu bildirmektedir. Yani, bir kişi yaklaşık olarak her 2 ila 4 saniyede bir göz kırpar ve göz kırpma ortalama olarak 250 milisaniye sürer. Ancak araştırmacılara göre göz bir nesneye odaklandığı zaman göz kırpma oranı belirgin ölçüde düşer. Örnek vermek gerekirse, okuma esnasında insanların göz kırpma oranı yaklaşık olarak dakikade 3 veya 4 adettir [48].Bu bilgilerden yola çıkarak algoritma, göz kırpma sayısı belirlenen zaman aralığı içerisinde eşik değerine ulaşırsa canlılık analizi için ekran yazılarının dinamik olarak çıkarılmasını sağlar.

3.1 Ekran yazılarının Dinamik olarak çıkarılması

Canlılık kararını vermek için doğrulama yapılması sırasında kullanıcıların bakış yönleri ile ekran yazılarının takibi amaçlanmıştır. Python programlama dilini kullanarak geliştirilen bu algoritma da ilk olarak ekran boyutunun tespit edilmesi gerekir. Burada ekran boyutundan kastımız aslında kullanıcıdan görüntü almak için kullandığımız kameranın pencere boyutudur. 640x480 çözünürlük denildiği zaman 640 piksel genişlikte, 480 piksel yükseklikte bir pencere içerisinde çalışma alanımız

vardır. Bu çalışmada ekranın yükseklik ile ilgili olan piksellerinin takibi yerine genişlik belirten piksellerini kullanarak farklı zamanlarda farklı bölümlerde yazılar çıkartılmıştır. Ekran genişlik boyutunda 3 parçaya bölünerek, kullanıcıların sol, orta veya sağ tarafa bakma durumları tespit edilmeye çalışılmıştır. Python programlama dilinin matematiksel işlemler için kullanılan kütüphanesi olan Numpy Kütüphanesi ve rastgele sayı oluşturma modülü olan Random modülü kullanılarak ekranda dinamik olarak bir metnin çıkarılması sağlanmıştır. Ekran üzerinde yazı çıkarma süresi olarak 10 saniyede bir olmak üzere genişlik pikselini temsil eden değer Random modülü tarafından oluşturulduktan sonra ekran metninin çıkarılacağı yer belirlenmiş olur. Fakat programın daha hızlı çalışması istenildiği takdirde 1 saniyede bir olmak üzere de ekran yazıları çıkarmak mümkündür. Ancak bu durumda ekrandaki yazıların okunması zorlaşacağından iris merkezinin takip edilmesi de zorlaşacaktır.



Şekil 3.1 Ekran Metinlerinin Yerleşim Bölgeleri

Şekil 10'da görülen 3 bölgenin birisinde rastgele ekran yazıları çıkarak kamera karşısındaki kullanıcının bu bölgelerden hangisine baktığı analiz edilmiştir. Random kütüphanesinin yardımı ile ekran genişliği limiti sınırları içerisinde kalmak koşulu ile her yeni üretilen x koordinatı değerinde kullanıcıların bakış yönleri takip edilmiştir.

3.2 İris Konumunu ile Ekran Metinlerinin Konumlarını Eşleştirerek Canlılık Tespiti

Yüz tanıma sistemlerinde canlılık tespiti için önerilen algoritmada ilk olarak kullanıcıların bakış yönlerini iris merkezleri sayesinde bulunmuştur. Ardından ikinci olarak, ekranda farklı zamanlarda farklı konumlarda ekran metinleri çıkarılarak kullanıcıların bu metinleri okumaları beklenmiştir. Üçüncü olarak ise kullanıcıların bakış yönleri ile ekrandaki metinlerinin konumlarının eşleşip eşleşmediğini tespit ederek biyometrik sistemlere giriş için canlılık kararının bildirimi sağlanmıştır.

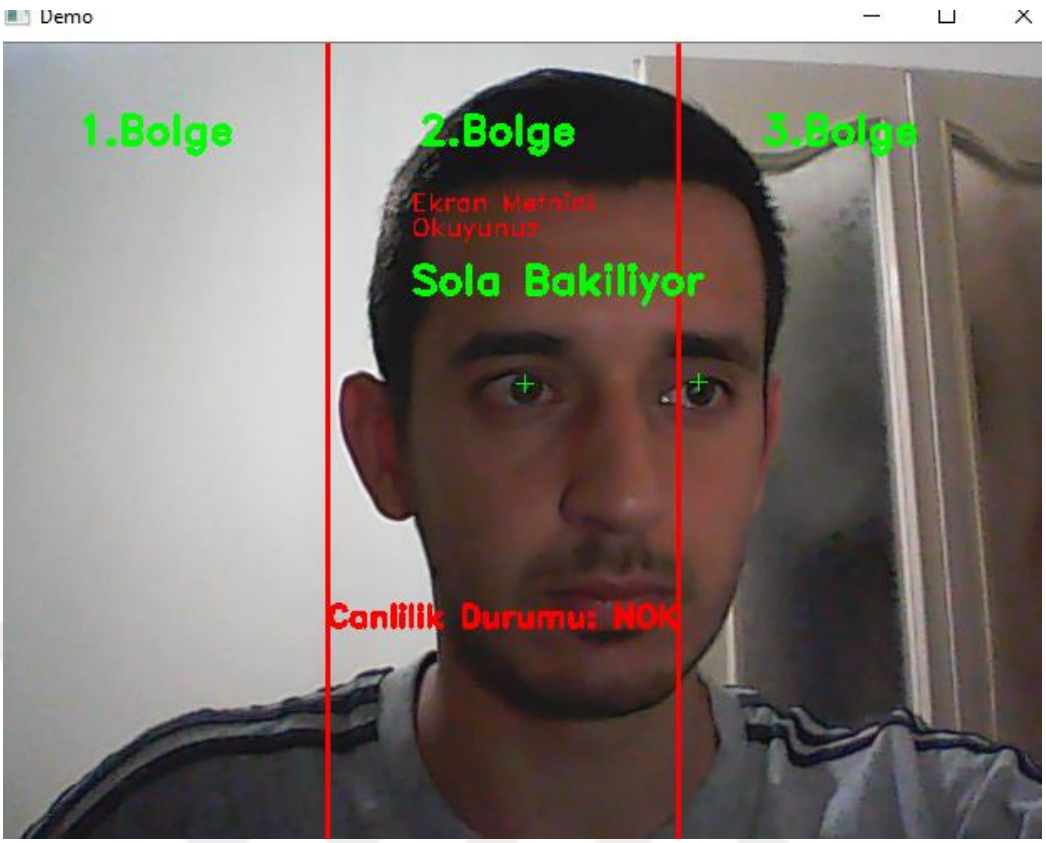
Literatürde yüz tanıma sistemlerinde canlılık tespiti için kullanılan yöntemler şöyle sıralanabilir;

- Sıklık ve Doku Tabanlı Analiz
- Değişken Odaklama Tabanlı Analiz
- Gözlerin Hareketli Bazlı Analiz
- Optik Akış Bazlı Analiz
- Göz Kırpma Tabanlı Analiz
- Eleman Bağımlı Tamamlayıcı Tabanlı Analiz
- 3D Yüz Şekli Tabanlı Analiz
- İkili Sınıflandırma Tabanlı Analiz
- Doğal İpuçlarına Dayalı Analiz
- Dudak Hareketi Bazlı Analiz

- Standard Tekniklerin Kombinasyonu Bazlı Analiz olmak üzere birkaç farklı durum olarak incelenmektedir [49].

Bu çalışmada, kullanıcılara takip edildiklerinin farkına vardırılmadan canlılık tespiti işlemini yapmak için onları ekranda çıkan yazıları okudukları anlarda takip ederek, sisteme canlılık kararını döndürmek amaçlanmıştır. Bu yöntemin avantajı diğer sistemlerde olduğu gibi ek olarak bir donanıma ihtiyaç duymadan mevcut sistemlerde küçük bir modifikasyon ile daha güvenilir hale getirmesidir. Ayrıca algoritmanın görüntüleri yakalama başarı oranı %97 olmasından dolayı ve kullanıcıların göz hareketlerini tespit ve takip etmedeki kararlılığı nedeni ile birçok avantaj sağlamaktadır.

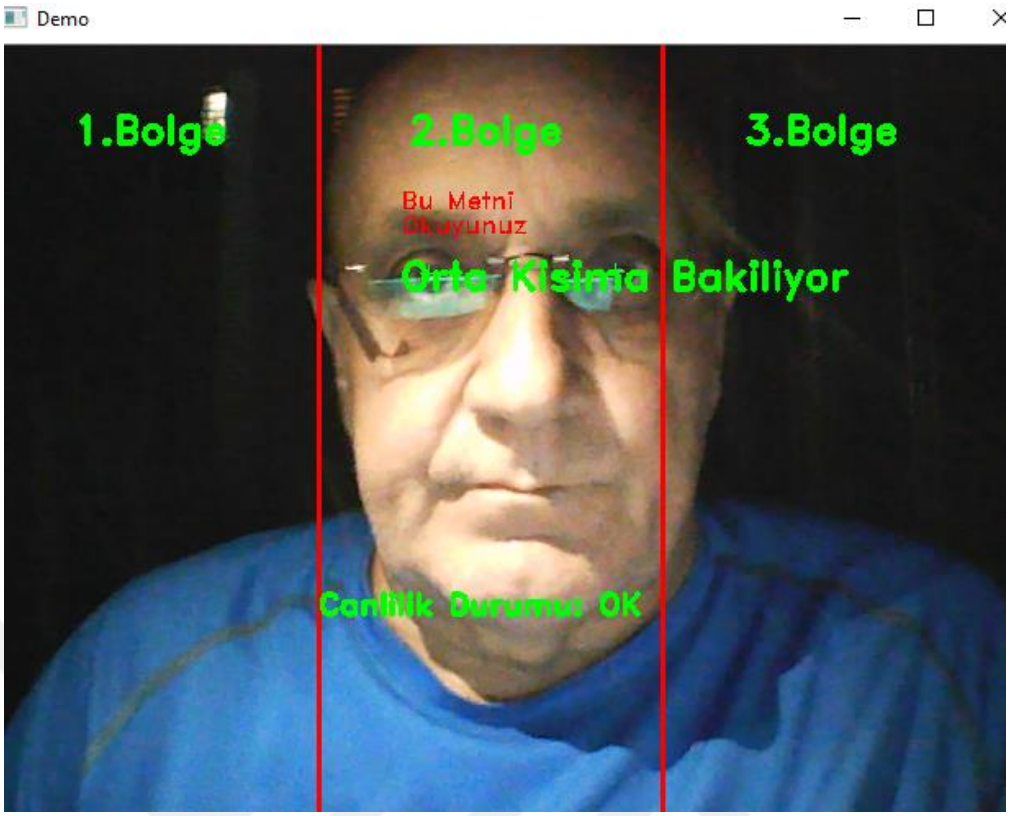
Şekil 3.2 Canlılık Analizi Ret Kararı Görseli-1



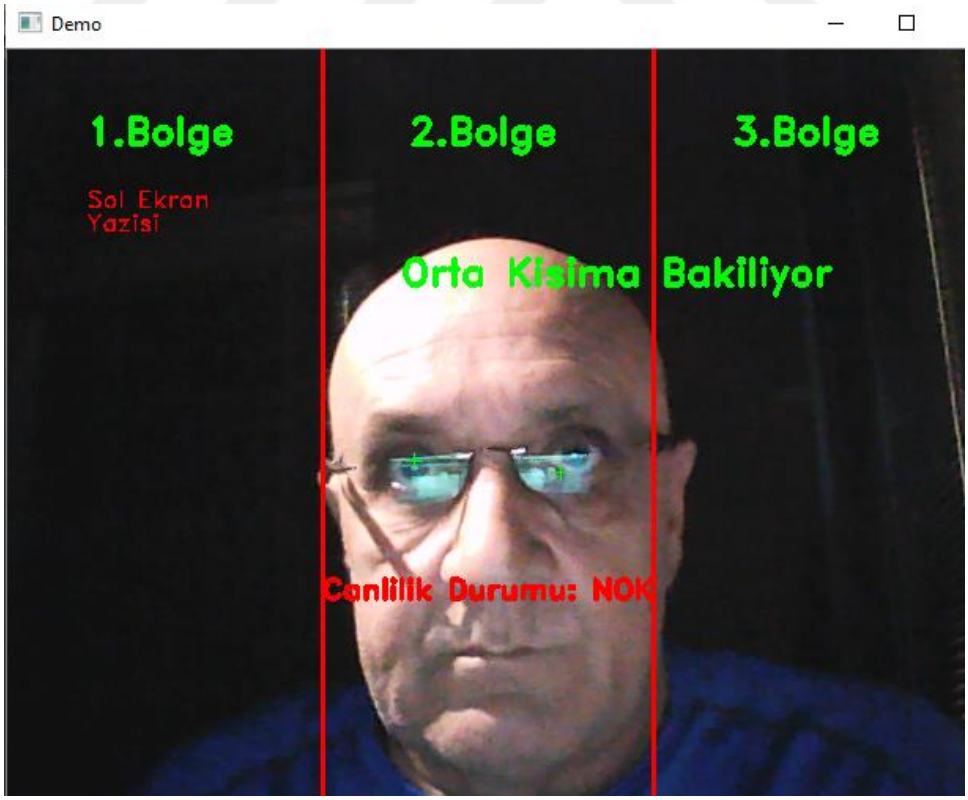
Şekil 3.3 Canlılık Analizi Ret Kararı Görseli-2

Şekil 3.4 Canlılık Analizi Kabul Kararı Görseli-1

Şekil 3.5 Canlılık Analizi Kabul Kararı Görseli-2



Şekil 3.6 Gözlüklü Kişilerde Canlılık Analizi Kabul Kararı Görseli



Şekil 3.7 Gözlüklü Kişilerde Canlılık Analizi Ret Kararı Görseli

4
Sonuç ve Öneriler

Bu tezde yüz tanıma sistemlerinde canlılık analizi yapmak amacı ile literatürde bulunan örnekleri çoğunlukla ek maliyet ve değişiklik isteyen sistemlere karşın düşük maliyetli, ek bir donanım ihtiyacı olmayan, hızlı çalışan bir algoritma önerilmiştir. Bu algoritma temel olarak iki aşamadan oluşmaktadır. Bu aşamalar öncelikle kullanıcıların sırası ile yüz bölgesi, göz alanı ve iris bölgeleri bulunmasından sonra ikinci aşama, bulunan iris noktalarının ekranda farklı zamanda farklı koordinatlarda çıkan yazıları takip etmesi ile canlılık kararının sisteme geri bildirim olarak verilmesidir.

Literatürde yüz ve yüz içerisindeki bileşenleri tespit etmek için birçok yöntem önerilmiştir. Bunlara örnek olarak yüz tespit ederken çoğunlukla kullanılan yöntemler;

- Yönlü Gradyanlar Histogramı Algoritması (HoG)
- Viola-Jones Algoritması
- Yapay Sinir Ağı Tabanlı Algoritmalar
- Destek Vektör Makineleri Tabanlı Algoritmalar
- Dlib yöntemi
- Yerel İkili Desenler Histogramlarıdır.

Bu yöntemlerin hepsinin birbirine göre üstün olduğu durumlar vardır. Kullanılacak olan yöntem ve algoritmayı belirlerken, uygulamadaki ihtiyaçları net olarak belirledikten sonra hangi özelliğin yapılacak uygulamadaki etkisi daha fazla ise o yöntemin tercih edilmesi daha doğru olur. Örneğin, Yönlü Gradyanlar Histogramı yöntemi ile Viola Jones Algoritması en çok kullanılan iki yüz tespit yöntemidir. Yönlü Gradyanlar Histogramı algoritması aynı zamanda nesne algılama amacıyla bir

özellik çıkarıcıdır. Viola Jones metodu gibi piksel yoğunluklarını göz önüne almak yerine, teknik, gradyan vektörlerin oluşumunu sayar, görüntü bölümlerini sınırlandırmak için ışık yönünü temsil eder. Bu yöntem, doğruluğu artırmak için çakışan yerel kontrast normalizasyonu kullanır. HoG algoritmasının doğruluğu Viola Jones algoritmasına göre çok fazladır. Ayrıca HoG ile daha zorlu şartlarda bulunan, eğik yüz, gözlük takılan yüz gibi, tespitler Viola Jones algoritmasına göre daha kolay bulunabilir. Ancak, doğruluğunun yüksek olması ve birçok şart altında yüz tespit etmesinin yanında HoG algoritması Viola Jones algoritmasına göre hız bakımından yavaştır.

Bir başka örnek olarak Dlib %99 oranında doğruluğa sahip bir önceden eğitilmiş yüz modeli kütüphanesi verilebilir. Derin öğrenme algoritmaları kullanılarak eğitilen bu model zaman olarak karşılaştırıldığında doğruluğunun yüksek olmasından dolayı diğer yöntemlere göre biraz yavaş kaldığı durumlar vardır. Bu tez çalışmasında HoG yönteminin geliştirilmiş versiyonu olan Dlib yöntemi kullanılmıştır. Gerçek zamanlı çalışmalarda daha kullanışlı olmasından ve doğruluğunun güvenlik sistemleri için yeterli olmasından dolayı bu yöntem seçilmiştir. Dlib yöntemi hız ve süre bakımından diğer algoritmalara göre bu tür uygulamalar için başarılı sonuçlar vermiştir.

Bu tezde ikinci aşama olarak canlılık kararını vermek için kullanıcıların iris hareketlerinin takip edilmesini sağlayan ve canlılık kararını sisteme geri bildiren algoritma yeterli başarımı sağlamıştır. Benzer yöntem olarak, Killioğlu ve arkadaşları [50], kamera etrafına LED çerçevesi yerleştirilip, rastgele sıra ile yanan LED'leri takip etmesini isteyen bir yöntem önermiştir. Mevcut sistemlere uygulanabilirlik açısından karşılaştırıldığında ekstra bir donanım gerektirmemesinden ve kullanılan yazılım dili ve kütüphanelerinin başarılı olmasından dolayı bu tezde önerilen sistem daha hızlı, ve uygulanabilir bir çözümdür. Aynı zamanda, güvenlik sistemlerine giriş için bu tarz bir uygulamada kullanıcıların takip edildiklerini anlamaması en önemli etkendir. Bu tez çalışmasında kullanıcılara bir yönlendirme doğrudan yapılmadan sadece ekrana baktıkları zaman çıkan yazıları takip etmeleri beklenmektedir. Bu şekilde

oluşturulan yöntemin kullanıcılara takip edildiklerini hissettiremeden bir sahte yöntemlerle giriş yapmaya çalışıp çalışmadıklarının takibi yapılmıştır.

Bu tez özelinde gelecekte planlanan çalışmalar ise sistemin her türlü atak türünde bir çözüm olmasını sağlamaktır. Önerilen algoritmanın daha hızlı ve doğruluğunu daha da arttırmak için literatürde bulunan diğer çalışmalardan da faydalanılarak yeni bir yöntem geliştirilebilir. Kullanılan kamera ve bilgisayarın modellerinin yükseltilmesi ile işlem hızının artması sağlanabilir. Yüz tespiti için kullanılan Dlib yönteminin en büyük dezavantajı minimum 80x80 boyutundan küçük boyutlarda yüz tespiti yapamamaktadır. Bunun üstesinden gelmek için daha küçük boyutlarda yüz fotoğrafları ile algoritmayı eğiterek bu dezavantajın çözülmesi planlanmıştır. Önerilen algoritmanın şu andaki durumu mevcut güvenlik geçiş sistemlerine ait bir çözüm olarak sunulmuştur. Yani kullanıcıların bir ekran karşısına geçip giriş için onay almalarını bekledikten sonra canlılık analizi yapılarak sisteme giriş izni verilmesi amaçlanmıştır. Ancak, teknolojinin gelişmesi ile birlikte mevcut güvenlik sistemleri de oldukça gelişmiştir. Örneğin, bankacılık uygulamaları artık şubelere gitmeden mobil telefonlar aracılığı ile her yerde her zaman yapılabilmektedir. Bu ve bu tarz uygulamalara karşı bir çözüm olması amacı ile mobil uygulamaları bu algoritmanın mobil sürümü yazılarak adapte edilebilir. Böylelikle mobil saldırılarında önüne geçmek için bir yöntem sağlanmış olacaktır.

Kaynakça

[1] J. G. Daugman, High confidence visual recognition of persons by a test of statistical independence, *IEEE Trans. Pattern Analysis and MachineIntelligence*, vol. 15, No. 11, pp. 1148 -1161, 1993

[2] Ergen, B., and A. Çalışkan. "Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri." 6th International Advanced Technologies Symposium (IATS'11). 2011.

[3] "Biometrics: Overview". Biometrics.cse.msu.edu. 6 September 2007. Archived from the original on 7 January 2012. Retrieved 2012-06-10.

[4] "What is Biometrics?". Biometrics Research Group. Michigan State University. Archived from the original on 27 August 2017. Retrieved 10 November 2017.

[5] Jain, Anil, Lin Hong, and Sharath Pankanti. "Biometric identification." Communications of the ACM 43.2 (2000): 90-98.

[6] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A (eds.). Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[7] Poddar, Arnab; Sahidullah, Md; Saha, Goutam (March 2018). "Speaker Verification with Short Utterances: A Review of Challenges, Trends and Opportunities". IET Biometrics. 7(2): 91–101. doi: 10.1049/iet-bmt.2017.0065.

[8] "Biometrics for Secure Authentication" (PDF). Archived from the original (PDF) on 25 March 2012. Retrieved 29 July 2012.

[9] Weaver, A. C. (2006). "Biometric Authentication". Computer, 39 (2), p. 96–97. DOI 10.1109/MC.2006.47

[10] Marciano, Avi (2018). "Reframing biometric surveillance: From a means of inspection to a form of control". Ethics and Information Technology. doi:10.1007/s10676-018-9493-1. ISSN 1572-8439.

[11] Halici U.; Jain L. C.; Hayashi, I.; Lee, S.B.; Tsutsui T., Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC press, USA, 1999

[12] R. Jain and C. Kant, "Attacks on Biometric Systems: An Overview", IJASR, vol. 1, no. 7, pp. 283-288, Sep. 2015.

[13] de Freitas Pereira, Tiago, et al. "Can face anti-spoofing countermeasures work in a real world scenario?." 2013 international conference on biometrics (ICB). IEEE, 2013.

[14] S. G. Pan, Z. Wu, and L. Sun. "Liveness detection for face recognition". In K. Delac, M. Grgic, and M. S. Bartlett, editors, Recent Advances in Face Recognition, Chapter 9. IN-TECH, (2008)

[15] Määttä, Jukka, Abdenour Hadid, and Matti Pietikäinen. "Face spoofing detection from single images using micro-texture analysis." 2011 international joint conference on Biometrics (IJCB). IEEE, 2011.

[16] W. R. Schwartz, A. Rocha and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in Proc. of IEEE International Joint Conference on Biometrics (IJCB), pp. 1-8, 2011.

[17] D. Gragnaniello, G. Poggi, C. Sansone and L. Verdoliva, "An investigation of local descriptors for biometric spoofing detection," IEEE T INF FOREN SEC, vol. 10, no. 4, pp. 849-863, April 2015.

[18] F. Liu, Z.Tang, and J. Tang, "WLBP: weber local binary pattern for local image description," Neurocomputing, vol. 120, pp. 325-335, November 2013.

[19] F. Liu, J. Tang, and Z. Tang, "An eye states detection method by using WLBP," in Proc. of 7th IEEE Int. Conf. on Semantic Computing, CA, pp. 198-201, 2013.

[20] X. Shu et al., "Image classification with tailored fine-grained dictionaries," IEEE Trans. on Circuits and Systems for Video Technology, vol. 28, no. 2, pp. 454-467, Feb. 2018.

[21] Z. Li and J. Tang, "Unsupervised feature selection via nonnegative spectral analysis and redundancy control," IEEE Trans Image Process., vol. 24, no. 12, pp. 5343-5355, Dec. 2015.

[22] Z. Li, J. Tang and X. He, "Robust structured nonnegative matrix factorization for image representation," IEEE Trans on Neural Netw. and Learning Syst., vol. 29, no. 5, pp. 1947-1960, May 2018.

[23] Moriyama, Tsuyoshi, et al. "Automatic recognition of eye blinking in spontaneously occurring behavior." Object recognition supported by user interaction for service robots. vol. 4. IEEE, 2002.

[24] Ji, Qiang, Zhiwei Zhu, and Peilin Lan. "Real-time nonintrusive monitoring and prediction of driver fatigue." IEEE transactions on vehicular technology 53.4 (2004): 1052-1068.

[25] Pan, Gang, et al. "Eyeblink-based anti-spoofing in face recognition from a generic webcamera." 2007 IEEE 11th International Conference on Computer Vision. IEEE, 2007.

[26] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14 (1), 4-20.

[27] Kazemi, Vahid, and Josephine Sullivan. "One millisecond face alignment with an ensemble of regression trees." Proceedings of the IEEE conference on computer vision and pattern recognition. 2014.

[28] OpenCV Library – www.opencv.org

[29] King, Davis E. "Dlib-ml: A machine learning toolkit." Journal of Machine Learning Research 10.Jul (2009): 1755-1758.

[30] Sharma, S., Karthikeyan Shanmugasundaram, and Sathees Kumar Ramasamy. "FAREC—CNN based efficient face recognition technique using Dlib." 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT). IEEE, 2016.

[31] Singh, Sanjay Kr, et al. "A robust skin color based face detection algorithm." 淡江理工學刊 6.4 (2003): 227-234.

[32] Zangana, Hewa Majeed, and Imad Fakhri Al-Shaikhli. "A new algorithm for human face detection using skin color tone." IOSR Journal of Computer Engineering 11.6 (2013): 31-38.

[33] Chow, Gloria, and Xiaobo Li. "Towards a system for automatic facial feature detection." Pattern Recognition 26.12 (1993): 1739-1755.

[34] Jeng, Shi-Hong, et al. "An efficient approach for facial feature detection using geometrical face model." Proceedings of 13th International Conference on Pattern Recognition. vol. 3. IEEE, 1996.

[35] Ji, Qiang, et al. "Special issue: eye detection and tracking." Computer Vision and Image Understanding 98.1 (2005): 1-3.

[36] Kothari, Ravi, and Jason L. Mitchell. "Detection of eye locations in unconstrained visual images." Proceedings of 3rd IEEE International Conference on Image Processing. vol. 3. IEEE, 1996.

[37] Waring, Christopher A., and Xiuwen Liu. "Face detection using spectral histograms and SVMs." IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 35.3 (2005): 467-476.

[38] Huang, Jeffrey, and Harry Wechsler. "Eye detection using optimal wavelet packets and radial basis functions (rbfs)." International Journal of Pattern Recognition and Artificial Intelligence 13.07 (1999): 1009-1025.

[39] Ma, Yong, et al. "Robust precise eye location under probabilistic framework." Sixth IEEE International Conference on Automatic Face and Gesture Recognition, 2004. Proceedings.. IEEE, 2004.

[40] Bhatia, Nitin, and Megha Chhabra. "Improved hough transform for fast iris detection." 2010 2nd International Conference on Signal Processing Systems. vol. 1. IEEE, 2010.

[41] Wildes, Richard P., et al. "A machine-vision system for iris recognition." Machine vision and Applications 9.1 (1996): 1-8.

[42] Liu, Xiaomei, Kevin W. Bowyer, and Patrick J. Flynn. "Experiments with an improved iris segmentation algorithm." Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05). IEEE, 2005.

[43] Chow, Gloria, and Xiaobo Li. "Towards a system for automatic facial feature detection." Pattern Recognition 26.12 (1993): 1739-1755.

[44] Tian, Ying-li, T. Kanada, and Jeffrey F. Cohn. "Recognizing upper face action units for facial expression analysis." Proceedings IEEE Conference on Computer Vision and Pattern Recognition. CVPR 2000 (Cat. No. PR00662). vol. 1. IEEE, 2000.

[45] Daugman, John G. "High confidence visual recognition of persons by a test of statistical independence." IEEE transactions on pattern analysis and machine intelligence15.11 (1993): 1148-1161.

[46] Tekyıldız, Ahmet, et al. "Iris recognition system based on fast iris localization and phase correlation mathching." 2012 20th Signal Processing and Communications Applications Conference (SIU). IEEE, 2012.

[47] Pan, Gang, et al. "Monocular camera-based face liveness detection by combining eyeblink and scene context." Telecommunication Systems 47.3-4 (2011): 215-225.

[48] Bentivoglio, Anna Rita, et al. "Analysis of blink rate patterns in normal subjects." Movement disorders 12.6 (1997): 1028-1034.

[49] Chakraborty, Saptarshi, and Dhrubajyoti Das. "An overview of face liveness detection." arXiv preprint arXiv:1405.2227 (2014).

[50] Killioğlu, M., M. Taşkiran, and N. Kahraman. "Anti-spoofing in face recognition with liveness detection using pupil tracking." 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, 2017.

[51] C. Sagonas, E. Antonakos, G, Tzimiropoulos, S. Zafeiriou, M. Pantic. 300 faces In-the-wild challenge: Database and results. Image and Vision Computing (IMAVIS), Special Issue on Facial Landmark Localisation "In-The-Wild". 2016.

Tezden Üretilmiş Yayınlar

İletişim Bilgisi: tugaybozik @gmail.com

Konferans Bildirileri

1. T. Bozik, N. Kahraman (2019, Haziran). “An Improved Methodology for Fraud Detection in Face Recognition Systems.” Proceedings of ISSRD International Conference (s. 1-4). Istanbul, Turkey 04 June 2019.