T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

AKILLI TELEFONLARDA KULLANICILARIN TERCİH ETTİKLERİ KİMLİK DOĞRULAMA YÖNTEMLERİ

Yüksek Lisans Tezi

Tezi Hazırlayan:

Miray İREN

İstanbul, 2018

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

AKILLI TELEFONLARDA KULLANICILARIN TERCİH ETTİKLERİ KİMLİK DOĞRULAMA YÖNTEMLERİ

Yüksek Lisans Tezi

Tezi Hazırlayan:

Miray İREN

Öğrenci No:
160820806

Danışman:
Dr. Ediz ŞAYKOL

İstanbul, 2018

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "**Akıllı Telefonlarda Kullanıcıların Tercih Ettikleri Kimlik Doğrulama Yöntemleri** " başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım.15.08.2018

Miray İREN

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi ..160820806 no'lu .....MİRAY İREN.....'in 15/8/18 tarihinde yapılan tez savunma sınavı[1] sonucunda ..45. dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle, ...KABUL.. kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ

Programı : BİLGİSAYAR MÜHENDİSLİĞİ

Tez Başlığı[3] : Akıllı Telefonlarda Kullanıcıların Tercih Ettikleri Kimlik Doğrulama Yöntemleri

---

Tez Sınav Jürisi	Öğretim Üyesi	İmza
Danışman :	Dr. Ediz Şaykol	
Üye :	Prof. Dr. Gökhan Sağlamoğlu	
Üye :	Dr. Turhan Karaçoban	

[1]Jüri üyeleri, söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tezsınavına alır. Tez savunma sınav süres ienaz 45, ençok 90 dakikadır. Jüri üyeleri, sınavöncesiyapılacaktoplantıda, kendiaralarından danışmandışındabirüyeyibaşkanseçer. Tezsınavı, tezçalışmasınınsunulmasıve bunuizleyen soru-cevap bölümünden oluşur. Tezsınavı, öğretim elemanları, lisansüstü öğrenciler vealanın uzmanlarındanoluşandinleyicilerinkatılımınaaçıkortamlardagerçekleştirilir.Belirlenengündeyapılamayanjüritoplantısı, katılanlarınhazırladığıbirtutanaklaenstitüyönetiminebildirilir. Bu durumda, jüriengeç on beşgüniçindetoplanarakadayıtezsavunmasınavınaalır. (05 Ağustos 2017 tarihli 30145 sayılıResmiGazetedeYayınlananDeğişiklik-Madde 29-3)

[2]Tezsınavınıntamamlanmasındansonrajüri, tezhakkında salt çoğunlukla "kabul", "düzeltme" veya "ret" kararıverir. Jüribaşkanı, jüriüyelerinceimzalanmışkarartutanağını, tezsınavınıizleyenüçgüniçindeilgilienstitüyönetimineteslimeder. Tezihakkındadüzeltmekararıverilenöğrenciengeçüç ay içindegereklidüzeltmeleriyaparakvebirincifıkradakiusulegöreteziniaynıjüriönündeyenidensavunur.Süresiiçerisinde "düzeltme" savunmasınagirmeyenöğrencininenstitüileilişiğikesilir. (BeykentÜniversitesiLisansüstüEğitimveÖğretimYönetmeliği-Madde 29-4)

[3]İleridedoğabilecekaksaklıklarınengellenmesiiçintezinbaşlığınınyazılmasıgerekmektedir.

Adı ve Soyadı : Miray İREN
Danışmanı : Dr. Ediz Şaykol
Türü ve Tarihi : Yüksek Lisans Tezi, 2018
Alanı : Bilgisayar Mühendisliği
Anahtar Kelimeler : Göz Takibi, Kimlik Doğrulama, Akıllı Android İşletim Sistemli Cep Telefonları

ÖZ

AKILLI TELEFONLARDA KULLANICILARIN TERCİH ETTİKLERİ KİMLİK DOĞRULAMA YÖNTEMLERİ

Göz takibi günümüzde hala gelişmekte olan büyük bir teknoloji icadıdır. Özellikle sağlık sektörü, oyun sektörü ve satış sektöründe. Aynı zamanda akıllı telefonlarımız da gün geçtikçe daha güçlü donanıma sahip olmaktadırlar. Asıl amaç göz takibi ile kimlik doğrulanması tekniğiyle akıllı telefonlarının güvenliğinin arttırılması. Tezin içeriğinde akıllı telefonlarının ön kamerasından göz bebeklerinin takip edilerek kimlik doğrulanması incelenmiştir. Akıllı telefonlarda, bunun başarılması için göz takip algoritmaları ve göz bebeği eşleşme taslakları uygulanmıştır. Kullanıcıların güvenilir bir şekilde kimlik doğrulamalarını mobil cihazları ile güvenli bir şekilde yapabilmeleri için göz bebeği segmentasyon algoritması, gözün algılanması ve gözün bakış estimasyon algoritmasını kapsamaktadır.

Name and Surname : Miray İREN
Supervisor : Assist. Prof. Ediz Şaykol
Degree and Date : Master with Thesis, 2018
Major : Computer Engineering
Key Words : Eye Tracking, Authentication, Android Based Smartphone

ABSTRACT

CHOOSING THEIR OPTIMIZATION IDENTIFIERS OF OPERATORS IN INTELLIGENT TELEPHONES

Eye tracking is a marvelous technology that is still a developing invention. Even today, especially in the grand sectors of marketing, gaming and health. In addition, smartphones are improving each passing day, at the same rate. The main purpose of this thesis is to greatly increase the security of smart phones through the usage of eye tracking with authentication technique. The thesis delves into the details of authentication through eye tracking by using the front camera of a smartphone. In order to achieve this goal, numerous eye and pupil tracking algorithms were utilized. On top of that, widely used methods of our time such as fingerprint, password, pattern, voice and face recognition were also observed in detail. Secure authentication methods preferred by users for them to safely operate their smartphones were researched. Lastly, this thesis also covers eye and gaze detection algorithms.

İÇİNDEKİLER

Sayfa No.

ÖZ i
ABSTRACT ii
TABLOLAR LİSTESİ vi
ŞEKİLLER LİSTESİ viii
KISALTMALAR x
1.GİRİŞ 1
1.1 Tez Özeti 1
2. KULLANILAN TEKNOLOJİLER VE ALAKALI ÇALIŞMALAR 3
2.1. Göz Takibi 3
2.2. İlgili Çalışmalar 4
2.3. Gözü Takip Eden Cihazlar 4
2.4. Kimlik Doğrulama 6
2.5. Tek Faktörlü Kimlik Doğrulaması 6
2.6. Kimlik Doğrulaması İçin Geliştirilen Teknoloji 7
2.7. Çok Faktörlü Kimlik Doğrulaması 8
2.8. Viola-Jones Özellik Tespiti 10
2.9. Yüz Tespiti Ve Göz Takibi 13
3. DİZAYN VE ARAÇLAR 14
3.1. Giriş 14
3.2. Eye Localization 15
3.3. Gaze Tabanlı Kimlik Doğrulama 15
3.4. Android 17
3.5. Göz Takibi İçin Android Applicatıon Lifecycle 17
3.6. Multi Factor Authentication (MFA) 19
3.7. Gaze Estimation Algoritması 19
4. TAKİP ALGORİTMALARI 21
4.1. Haar Cascade 21
4.2 Template Eşleşme Algoritması 23
4.3 Timm ve Barth Algoritması 23

5. IMPLEMENTATION 25
5.1 Android Eye Localization Uygulama Sonuçları 25
5.2. Gözün Görüntüsünün Veritabanı 25
5.3. Gözün Görüntüsünün İşlenmesi 26
5.3.1. K Means 26
5.3.2. Morfolojik Segmentasyon 28
5.4. Kullanıcı-Cihaz Arasındaki Kimlik Doğrulama İçin Uygulama 31
5.4.1. Mesafeye Ve Projeksiyona Bağlı Gaze Estimation 31
5.4.2. Parolanın Belirlenmesi 32
5.4.3. Parolanın Girilmesi 33
5.5. Templata Eşleşme Implementation 33
5.6. Timm ve Barth Algoritmasının Implementasyonu 34
5.7. Kalibrasyon 35
5.8. Özet 36
6. ÖNERİLER 37
6.1. İris Taraması 38
6.2 İris Taraması İçin Gerekli Donanım 39
6.2.1 Kızılötesi Gücü 39
6.3 İris Taramasında Sağlık Sorunlarının Etkisi 40
6.4. Göz Takibi Tabanlı Webcam'in Artıları Ve Eksileri 40
6.5. İris Taraması Hakkında Yapılan Açıklamalar 41
6.5.1.Sistem İhlallerinden Kaçınmak 42
6.6. Eye Gesture 42
6.6.1 Akıllı Telefonlar İçin Kimlik Doğrulama Methodları Ve Eye Gesture 43
6.7. Eye Gesture Avantajları 43
6.7.1. Framework Modülleri 44
7. SONUÇ 47
7.1 Giriş 47
7.2 Tanımlayıcı İstatistikler 47
7.3 Anket Soruları ve Analiz Tablo Sonuçları 48
7.3.1 Nominal Ve Ordinal Ataması 51
7.4 Test Sonuçları 51
7.4.1 Mann-Whıtney-U Analizi 55
7.4.2 Kruskall-Wallıs Analizi 55

7.4.3 Johnckere-Terspra Analizi 56
7.5 SONUÇ VE ÖNERİLER 57
KAYNAKLAR 61

TABLOLAR LİSTESİ

Tablo No. **Sayfa No**

Tablo 2.1: Multi Factors 8
Tablo 2.2: MIT Admissions Training Data 13
Tablo 5.1: İrisin Renk Etkileri 30
Tablo 7.1: Cinsiyet 48
Tablo 7.2: Yaş 49
Tablo 7.3: Eğitim 49
Tablo 7.4: Departman 49
Tablo 7.5: Bilgisayar Bilgisi 49
Tablo 7.6: İşletim Sistemi (Önceki) 49
Tablo 7.7: İşletim Sistemi (Şuan) 50
Tablo 7.8: Parola Tercih Sebebi 50
Tablo 7.9: Kullandığı Parola (Önceki) 50
Tablo 7.10: Kullandığı Parola (Şuan) 50
Tablo 7.11: Test Statistics Cinsiyet 51
Tablo 7.12: Jonckheere-Terpstra Test Yaş 51
Tablo 7.13: Jonckheere-Terpstra Eğitim 52
Tablo 7.14: Test Statistics ve Jonckheere-Terpstra Test Bilgisayar Bilgisi 52
Tablo 7.15: Test Statistics İşletim Sistemi Önce 53
Tablo 7.16: Ranks 53
Tablo 7.17: Test Statistics İşletim Sistemi Şuan 53
Tablo 7.18: Ranks 53
Tablo 7.19: Test Statistics Şifre Tercihi ve Ranks 54
Tablo 7.20: Test Statistics Şifre Tercihi 54
Tablo 7.21: Şifre Tercihi Ranks 54
Tablo 7.22: Kruskal Wallis Test ve Gelecek Şifre 54
Tablo 7.23: Jonckheere-Terpstra Test[a] Ekran Kilidi Önce 55
Tablo 7.24: Mann Whitney-U Analizi 55
Tablo 7.25: Kruskall-Wallis Analizi 56
Tablo 7.26: Jonckheere-Terpstra Test Eğitim ve Bilgisayar Bilgisi 56
Tablo 7.27: Önceki Ekran Kilidi İçin Mann Whitney U Test Sonuçları 57
Tablo 7.28: Şu anki Ekran Kilidi İçin Mann-Whitney-U Test Sonuçları 57

Tablo 7.29: Şu Anki Ekran Kilidi İçin Kruskall-Wallis Test Sonuçları 58
Tablo 7.30: Önceki Ekran Kilidi İçin Kruskall-Wallis Test Sonuçları 58
Tablo 7.31: Şu anki Ekran Kilidi Johnckere-Terspra Test Sonuçları..... 59
Tablo 7.32: Önceki Ekran Kilidi Johnckere-Terspra Test Sonuçları 59

ŞEKİLLER LİSTESİ

Şekil No. **Sayfa No**

Şekil 2.1: Tobii Göz Takibi Ürünleri 5
Şekil 2.2: Eye Tribe Ürünü 5
Şekil 2.3: Monitör Çeşitleri 5
Şekil 2.4: Smart Eye Ürünleri 6
Şekil 2.5: Akıllı Telefonlardaki Parmak Okuyucu 7
Şekil 2.6: Kullanıcı Deneyiminin Kimlik Doğrulamasının Protokol Akışı 9
Şekil 2.7: Göz Takibi Kimlik Doğrulaması 9
Şekil 2.8: Viola-Jones, Haar Feature Tekniği 11
Şekil 2.9: Viola-Jones, Haar Feature tekniği 11
Şekil 2.10: Viola-Jones, İntegral resmi 11
Şekil 2.11: Viola-Jones, Dört İntegral Değerinin Hesaplanması 11
Şekil 2.12: Viola-Jones, İntegral Görüntülerin Haar Feature Dikdörtgenleri 12
Şekil 2.13: Viola-Jones, İki Haar feature Dikdörtgeninin Hesaplanması 12
Şekil 3.1: Eye Localization Uygulaması 15
Şekil 3.2: Gaze-Based Grafiksel Parolama Örneği 16
Şekil 3.3: Saliency Masks 17
Şekil 3.4: Android Activity Lifecycle 18
Şekil 3.5: MFA'nın En Doğru Özeti 19
Şekil 3.6: Gaze Estimation Algoritması 19
Şekil 4.1: Viola-Jones, Haar Feature Tekniği 21
Şekil 4.2: Haar Feature Tekniğinin Etapları 22
Şekil 4.3: Haar Feature Sorgulaması 22
Şekil 4.4: Template Eşleşmesi 23
Şekil 5.1: Gözün Görüntüsünün Veritabanındaki Kaydedilmiş Hali 26
Şekil 5.2: K Means Örneği ve Akış Şeması 27
Şekil 5.3: Orijinal Resim ve Threshold Görüntüsü 29
Şekil 5.4: Threshold ve Morfolojik Görüntü 29
Şekil 5.5: Morfolojik İşlem Sonrası 30
Şekil 5.6: Parola Ekranı 31
Şekil 5.7: Yatay ve Dikey Kalibre 32
Şekil 5.8: Gözün Ekran ile Arasındaki Mesafesi 34
Şekil 5.9: Kalibrasyon Testi Örneği 35

Şekil 6.1: Kızıl Ötesi 39
Şekil 6.2: Eye Gesture Kimlik Doğrulaması 43
Şekil 6.3: Framework Modülleri 44
Şekil 6.4: Fruit Row (FR) 44
Şekil 6.5: Corner Gif (CG) 45
Şekil 6.6: Illusion Image (II) 45
Şekil 6.7: Simple Dot (SD) 46

KISALTMALAR

2FA **:** Two Factor Authentication

CG **:** Corner Gif

FR **:** Fruit Row

II **:** Illusion Image

IT **:** Information Technology

LAB : Lightness-Alpha-Beta

MFA **:** Multifactor Authentication

NFL **:** National Football League

RGB **:** Kırmızı – Yeşil – Mavi

SD **:** Simple Dot

1.GİRİŞ

1.1 Tez Özeti

Akıllı telefonlarda işletim sistemleri ve donanımları gün geçtikçe gelişmektedir ve kullanıcı sayısı artmaktadır. Aynı zamanda gözün gerçek zamanlı olarak takip etmek, insanların dünyayı nasıl etkilediğini ve algıladıklarını anlamak önemlidir. Göz takibi; pazarlama, oyun endüstrisi ve sağlık sektöründe yararlıdır. Mobil uygulamalar yardımıyla akıllı telefonlar internete erişimleri sayesinde dinamik platformlara ulaşabilir. Sağlanan erişim yüzünden güvenlik açıkları ortaya çıkmaktadır. Ancak parolama sistemleri birçok açıdan bu sorunla mücadele etmekte ve parolama sistemi güvenli oldukça parolayı kullanmaya devam etmektedir. Bu şekilde, akıllı telefon kullanıcıları banka, kişisel, sağlık ve benzeri işlemlere kolaylıkla erişebilirler.

Problemin en büyük temeli parola uygulamalarındaki insan faktörüdür. Kullanıcı sisteme parola girmekten sorumlu, herhangi bir hata sonrası parola sistemi girilen parolayı aynı olmadığında problem çıkabilir. Bu nedenle güçlü parola tercihleri mümkün oldukça karmaşık olmak zorundadır. Ancak bazı parola sistemleri basit, zayıf girilen parolaları da kabul etmektedir. Bu da onların bir güvenlik açığıdır.

Akıllı telefonlarda depolanan bilgilerini ve web sunucularını korumak için geliştirilmiş kimlik doğrulama adımlarına ihtiyaç duyulmaktadır. Çok faktörlü şemalar genellikle ek donanım gerektirir ve pahalıdır. İki adımlı yaklaşımlar güvenliği yeterince geliştirmemekte ve çoğu için nadiren kullanılmaktadırlar. Tezim, bunların dezavantajlarını gidermeyi amaçlamaktadır. Akıllı telefonlarda parolaların kullanışlılığını ve çoklu iletişim ağının sağladığı güvenliği birleştirerek; bakış açısı, model algılama ve tahmin kullanan bir sistem aracılığıyla faktör doğrulama uygulanmaktadır. Amaç göz takibi sayesinde insan-cihaz etkileşimi için gözleri kullanmaktır. Göz bebekleri ve diğer tanımlayıcı biyometrik bilgiler kullanılmaktadır. Bu çalışmanın amacı, akıllı telefonların bilgilerine ulaşarak güvenliği arttırmak.

Akıllı telefonların gelişimiyle algılama teknolojisi sayesinde, mobil cihazlarda göz izleme uygulamaları büyük bir potansiyele sahiptir. Geliştirilen göz takibi uygulamaları ile kullanıcının göz hareketleri takip edilir. Aynı zamanda bu tezde, mobil cihazlarda göz izleme sonuçlarının ne kadar doğru ve istikrarlı olduğunu araştırılır.

IOS ve Android işletim sistemini kullanan 46 kullanıcıda kullanıcı analizi yapılmış olup, kullanıcılara hangi şifreleme yöntemlerini kullandıklarını ve gelecekte hangi şifreleme yöntemini kullanmak istedikleri sorularak anket sonucu elde edilip, sonuçlar incelenerek ortaya veriler çıkartılmıştır. Kullanıcıların yanıtlarından elde edilen cinsiyet, yaş, eğitim seviyesi, departman bilgisi, bilgisayar bilgi seviyesi ve kullandıkları şuan ki ve önceki cep telefonlarının işletim sistemleri bilgilerine dayanılarak belli sonuçlar elde edilmiştir. Elde edilen sonuçlara dayanılarak hangi işletim sistemini kullanan kullanıcıların daha güçlü parolalar kullandıkların sonuçları elde edilmiştir.

2. KULLANILAN TEKNOLOJİLER VE ALAKALI ÇALIŞMALAR

2.1. Göz Takibi

Göz takibi, yüzyıla aşkın süredir üzerinde çalışılmış bir bilimdir. Muayeneler için araçlar başta doğrudan gözlem ve optik aletler kullanılmıştır. Günümüzde ise dijital çağda izleme yapılmakta ve daha Sofistike sistemler kullanılarak gerçekleştirilmektedir. 1990'da Gallup Applied Science göz izleme sistemini NFL analisti Joe Theismann kullandı ve insanların Amerikan futbolu maçını izlerken oyunun hangi bölümlerinin kaçırdıklarını, belirleyebilmek için taraftarlara bu teknolojiyi kullandırttı. Bu cihazlar sayesinde kullanıcının göz hareketleri izlendi, bir bilgisayar aracılığıyla da gözlerinin nerelere odaklandığını ve nerelere bakmadığını izleyecekti. En sonunda da, izleyicilerin ne tarafları izlediğini bir cursor mark ile işaretledi [1].

Günümüzde göz takibi yapan göz takibi alıcılarının çoğu kızılötesi kameralarla takip edilmektedir. Bunun için kornea yansımalarını hesaplaması kızılötesi veya yakın kızıl ötesi ışığın göz bebeği üzerindeki yansıması hesaplanır [2].

Göz takibi metodolojisine göre 3 yöntem vardır [3];

- Gözün kısa ve hızlı hareketi (saccade)
- Pürüzsüz takip
- Tespit

Gözün kısa ve hızlı hareketi, gözün yeniden pozisyon almasına neden olur. Bu hareket yansıma ve tekrar görüş odaklanmasına neden olur.

Pürüzsüz takip ise gözün hareket eden bir nesneye odaklanmasıdır. Göz, üzerine odaklanmış nesnenin hızına bağlı olarak hareket hızını ayarlar.

Fixation metodu gözün sabit bir noktaya odaklanmasıdır. Pürüzsüz takip ve Fixation en popüler metottur medikal araştırmalarda. Tezde üzerinde duracağım Fixation yani odaklanma modelidir.

2.2. İlgili Çalışmalar

Yüzü izleyebilen çok aşamalı bir algoritma var Cristinacce'e göre [4]. Bu yaklaşımın birinci aşamasında yüzü tespit etmek vardır. İkinci aşama, yanıtların güçlendirilmesi olarak bilinen bir algoritmayı kullanarak bire uygulamak ve birleştirmektir. Son aşamada, aktif görünüm modeli kullanılarak tahmin edilen noktaları hassaslaştırmaktır.

Bir diğer metot ise Asteriadis [5]. Amaç yüzdeki gözleri geometrik olarak bulmaktır. Bu yöntemde suratın sınırlarını belirlemek ve yüzü kapsayan bir kenar haritası çıkarılır. Daha sonra her piksele bir vektör atanır ve en yakın kenar pikseli gösterir. Bu vektörler göz takibinin eğim ve uzunluğunu bulmakta kullanılırlar. Türkan [6] kenar yansıtması kullanarak göz lokalizasyonunu başlatıyor. Bu algoritmada yüzü süzmek için bir dalgacık dönüşümü sağlayan high pass filtreleme kullanılır. Sonuç olarak yüzün kenarları vurgulanır ve karikatür benzeri bir temsili elde edilir. Yeni filtrelenmiş resimde, her göz için aday noktalar sağlamak için kenar bölgenin yatay yansıtmaları ve profilleri analiz edilir.

Göz izleme çözümlerinin çoğu donanımlarında kızılötesi kameralar kullanır; kesin izleme için. Valenti ve Gevers kızılötesi olmayan bir çözüm bulmaya çalışıyorlardı ve düşük çözünürlüklü web kamera kullandılar [7].

Bir diğer metot Timm ve Barth tarafından tanıtılan göz takibinin düşük çözünürlüklü kameralar ile takip edilmesi. Algoritma, noktalar kullanılarak gözün takip edilmesidir [8]. Son olarak ilk metotlardan biri olan Kothari ve Mitchell metodu, Timm ve Barth algoritmasını kullanarak kaş, göz kapakları ve gözlüklerden kaynaklanan sorunlarını ortadan kaldırmaktadır [9].

2.3. Gözü Takip Eden Cihazlar

Tobii [şekil 2.1], The Eye Tribe[15], Interactive Minds[16] ve Smart Eye[17] firmaları birçok alanı hedef almıştır. Bunlar; oyun, ulaşım, pazarlama ve sağlık sektörüdür. Ürünler olarak; gözlük, küçük bir donanım parçası veya bir aygıta gömülü olabilirler.

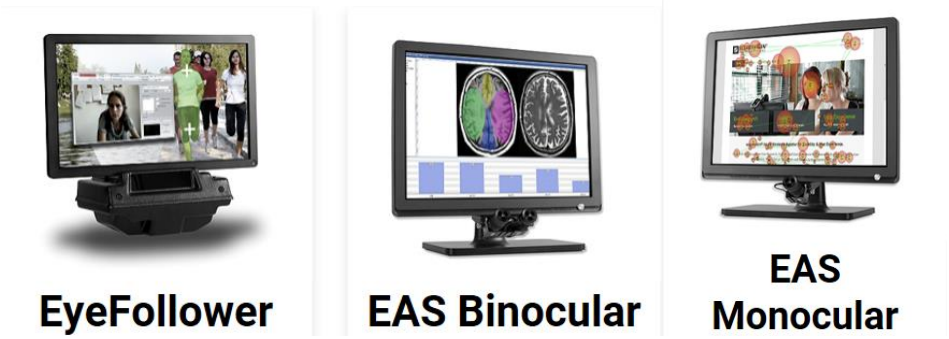
1. Gözlük 2. Tobi Pro Spectrum 3. Tobi Pro Lab

Şekil 2.1: Tobii Göz Takibi Ürünleri

The Eye Tribe şirketi de, Danimarkalı tabanlı bir şirkettir. Kopenhag'da uygun fiyatlı taşınabilir aygıt üretiyorlar bilgisayarlar, tabletler ve akıllı telefonlar için [şekil 2.2].

Şekil 2.2: Eye Tribe Ürünü

Interactive-minds firması göz takibi konusunda uzmanlaşmış şirketlerden biridir. Çoğunlukla ALS hastaları ve Locked-in sendromu olan kişiler gibi tıbbi nedenlerden ötürü. Ürünler monitörlere ayarlanabilir ve taşınabilir. Bunlar aşağıdaki resimlerdekiler gibidir [şekil 2.3].



Şekil 2.3: Monitör Çeşitleri

Eye Follower: 4 Kamera ile hedef doğruluğu ve kafa hareketlerinin takibi

EAS Binocular: Araştırma ve analizler için

EAS Monocular: Monoküler göz takibi

Smart Eye, kafa hareketleri ve göz takibinde dünyada bir lider olarak kabul edilen bir İsveçli şirkettir otomotiv, havacılık ve uzay alanında yapılan araştırmaları ile [şekil 2.4].

1-Smart Eye Aurora | 2- Smart Eye DR120 | 3- Smart Eye Antisleep | 4- Smart Eye Blackbird

Şekil 2.4: Smart Eye Ürünleri

2.4. Kimlik Doğrulama

Kullanıcı kimlik doğrulamasında kullanıcıya bazı sorular sorulmalıdır. Bunlar;

- Kullanıcı ne biliyor?
- Kullanıcı neye sahip?
- Kullanıcı nedir?

2.5. Tek Faktörlü Kimlik Doğrulaması

Tek faktörlü kimlik doğrulama, kimlik doğrulama yöntemlerinin en basit biçimidir. Tek faktörlü kimlik doğrulama ile bir kişi kendini doğrulamak için bir kimlik bilgisiyle eşleşmelidir. Bunun en popüler örneği, bir kullanıcı adına ait bir parola (kimlik bilgisi) olacaktır. Günümüzde bu kimlik doğrulama yöntemini kullanmaktadır.

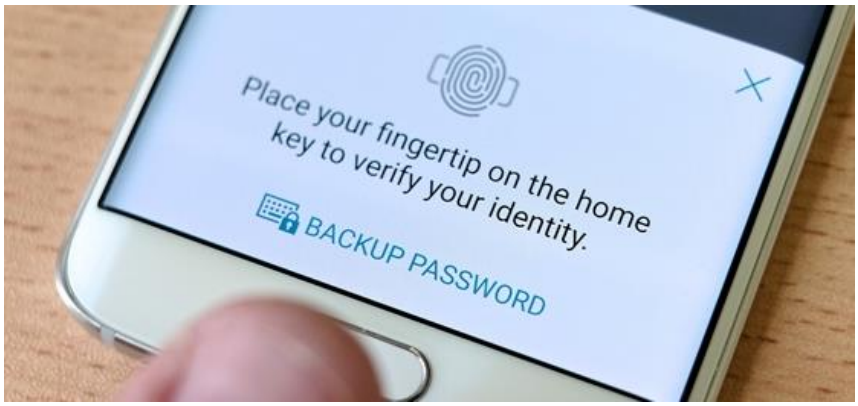
Parolalarla ilgili temel sorunlardan biri, çoğu kullanıcı güçlü ve unutulmaz parolalar oluşturmaları gerektiklerini yeteri kadar bilmemektedirler. Karmaşıklığı artıran ek kuralların, parolayla ilgili konularla ilgili sorular ortaya çıkarmakta. Bu sorun, IT ve yönetimin, parolama standartlarının kaymasına neden olmasına ve bunun sonucu olarak basit yedi karakter içeren

parolalar ve daha kısa, karmaşıklığa sahip parolaların ortaya çıkmasına neden olabilir. Bu parolalar, kısa sürede kırılabilir. Sonuç etkili olmaz.

Parolaların daha az öngörülebilir olabilmesi için daha fazla entropiye ihtiyaç duyduğu açık olsa da, çalışanların entropi ile aslında hatırlayabilecekleri parolalar yaratmaları için eğitilmeleri gerekir. Uzunluk belki de entropi yaratmada daha önemlidir. Kullanıcıların uzun ama unutulmaz cümleler oluşturmaları teşvik edilmelidir. Başkentler, rakamlar ve belki birkaç özel karakterin eklenmesi ve büyük karakterler entropiyi büyük ölçüde arttırır. Parola güvenirliliği ölçümünde, kullanıcıları daha güçlü parolalar oluşturmaya motive etmekte. Özellikle güncel güncellenmiş sayısal derecelendirmelerde etkili oldukları gösterilmiştir. Yine de, bir saldırgan korunan bilgisayarda bulunan parola veritabanını yakaladığında brute force, dictionary ve rainbow table saldırılarıyla parolalar kırılabilir [10].

2.6. Kimlik Doğrulaması İçin Geliştirilen Teknoloji

Günümüzde, Google ve Apple Inc. gömülü sensörler geliştirerek bilgi erişimini sağlayan güvenli donanım geliştirdi. Güvenlik geliştirilerek özel hat aracılığıyla önbellek öğesi ve aygıttaki alıcıyla ile iletişime geçer. Google'ın geliştirdiği bu teknoloji ile güvenli veri yoluna sahip yakın alan iletişimi çipi ile teknoloji hatlarını kullanarak CPU'dan güvenli bilgi iletmek için kullanılır.



Şekil 2.5: Akıllı Telefonlardaki Parmak Okuyucu

Bütün akıllı telefonlarda 4 haneli dijit PIN kodu kullanılmaktadır. Kullanılan bu metot en güvenli yoldur. Aynı zamanda kullanışsız ve tatmin edici değildir. Her gün bu parolayı cep telefonunuza yüzlerce kez girdiğinizde, artık kullanıcılar bundan yorulmaya başlar. Bu bütün parolalar için geçerlidir.

PIN'nin dışında pattern de bir başka parolama metodudur. Bu genel anlamda en çok kullanılan parolama tekniğidir. PIN'e göre biraz daha güvensizdir ancak yine de kullanıcılar bunu göz önünde bulundurmaktadırlar.

Parmak okuyucu telefonun modeline bağlı olarak; telefonun önünde ya da arkasında konumlandırılmıştır. Kullanışı oldukça kolaydır. Ancak bazen parmak izi okumada sorunlar ortaya çıkabilmektedir. Parmağınızı okuyucunun üstüne koyduğunuzda okuyucu üzerinde bulanıklık olabilir sizin parmağınız yağlanmasından ötürü. Birçok insan parola girerken cep telefonlarına zorlanmaktadırlar.

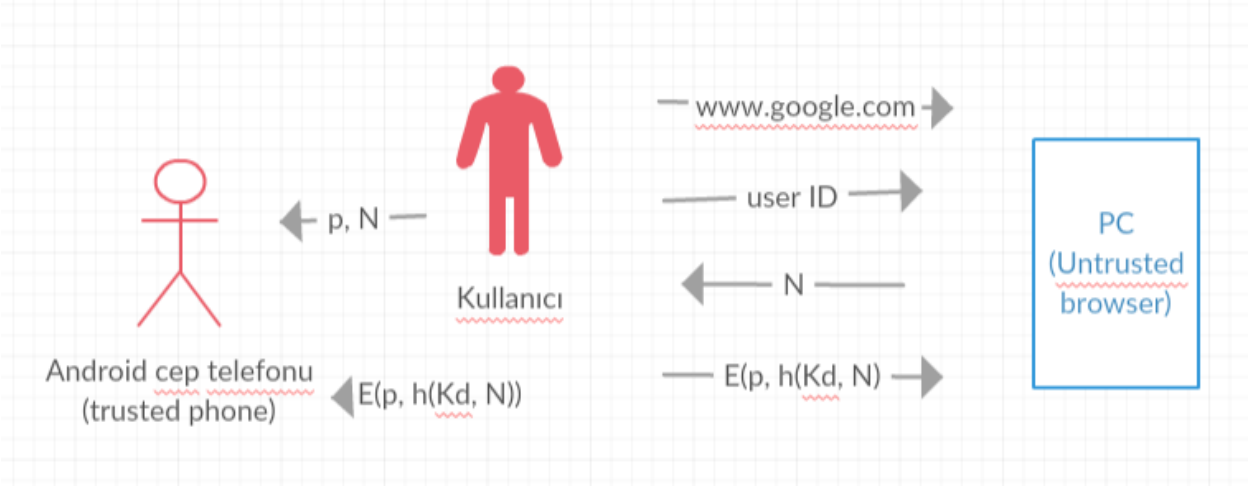
Günümüzde teknoloji artık farklı bir boyuta taşınmıştır. Bütün bu parola girme zorunluluklarından kurtulup ve aynı zamanda telefonlarımızı da güvenli bir şekilde kullanabiliriz. Bunu da akıllı telefonlarının, göz takibi ile kimlik doğrulanmasının yapılmasıyla gerçekleştirebiliriz.

2.7. Çok Faktörlü Kimlik Doğrulaması

Çok faktörlü kimlik doğrulanmasında en az iki kimlik doğrulanması yapılmaktadır. Bu yöntem güvenlik seviyesini arttırmaktadır. İki faktörün birleştirilip güvenliğe eklenmesi yüksek maliyete neden olmaktadır.

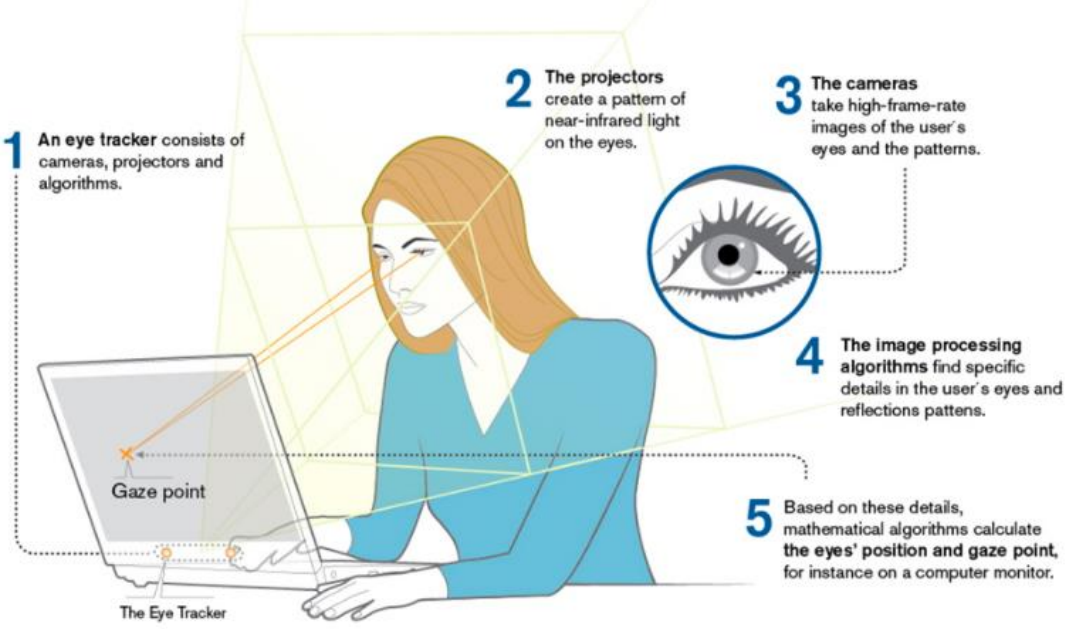
Faktörler	Açıklama	Uygulamalar
Bilgi	Sadece kullanıcının bildiği	Parola, PIN
Kişisel	Sadece kullanıcının sahip olduğu	ID kart, anahtar
Duyu Organları	Sadece kullanıcının	Biyometrik (Parmak izi, iris, ses)

Tablo 2.1: Multi Factors



Şekil 2.6: Kullanıcı Deneyiminin Kimlik Doğrulamasının Protokol Akışı

Bu sistem çok faktörlü kimlik doğrulma ile trusted device'a yani android işletim sistemli cep telefonlarına güvenerek iki adımda kimlik doğrulaması yapmaktadır.



Şekil 2.7: Göz Takibi Kimlik Doğrulaması

Tiwari, Sud. Sanyal, Abraham, Knapskog ve Sug. Sanyal cep telefonlarının identification kod ve kısa mesaj servisi çoklu faktör kullanmaktadır. Sistem mobil aygıtların işlemlerini desteklemekte, oldukça güvenlidir bankaların serverları arasındaki iletişimini, mobil cihazları ve POS makinelerini [11].

Huang, Xiang, Chonka, Zhou ve Deng tarafından kapsamlı bir şema tanımlanmıştır; kullanıcıların doğrulanmış parolaları ile kimlik doğrulamaları, smart card possession ve biyometrik karakterler. Birçok endişe üç faktöre yanaşmıştır sonucunda. Biyometrik datalar ile ilgili olarak [12]. Fan ve Lin ise üç faktör sistemi olarak parolanın smart kart ve parmak izi ile birleştirilmesini öne sürmüştür [13].

Milan, Perez-Cable ve Javidi bir sistemin retina görüntüsünü kullanarak cevap olarak spesifik görüntünün ID üstünde veya kartta kimlik doğrulaması olarak saklanmasını öne sürmüştür [14]. Görüntü ise kullanıcının retinası. Bu yaklaşım yüksek güvenlik gerektirmektedir ve external olarak görüntü ekipmanları lazımdır. Hiçbir kimlik doğrulama teknolojisi yeterince iyi bir şekilde birleştirememiştir kimlik doğrulama faktörlerini, ki kullanıcıların parolalarını aktif eden. Bu çalışma kullanıcı ile cep telefonları arasındaki kimlik doğrulama metodunun uygulanabilirliğini arttırmaya yöneliktir. Metot, kullanıcının göz bebeklerinin baktığı noktaya dayalıdır. Aynı anda da kullanıcının suratı, gözleri tespit edilmelidir.

2.8. Viola-Jones Özellik Tespiti

Kullanıcının suratının önüne bir kamera konulmalı ve kişinin biyometrik bilgileri toplanabilir kimlik doğrulama sayesinde. Biyometrik bilgiler özel görüntü karakterlerinden çıkarılabilir. Bu bölüm kullanıcının yüz özelliklerinin tespitiyle ilgilidir. Bu algoritma dört adımdan oluşmaktadır;

- Haar Feature Selection
- İntegral Görüntü Yaratılması
- Adaboost Training
- Cascading Classifiers

Haar Features: Bütün insanların suratları benzer özellik gösterebilir. Bunları da Haar features şu şekilde ayırt edebilir;

1- Göz karartılı olabilir üst yanakların üstünde kalan kısmı.
2- Burun köprüsü daha aydınlık olabilir gözlere oranla.
3- Gözlerin ve ağızın konumu ve büyüklüğü
4-Piksel büyüklüğü

Şekil 2.8: Viola-Jones, Haar Feature Tekniği

İntegral Görüntü Yaratılması:

$$ii(x, y) = \sum_{x' \leq x, y' \leq y} i(x', y'),$$

Şekil 2.9: Viola-Jones, Haar Feature tekniği

1	1	1
1	1	1
1	1	1

Input image

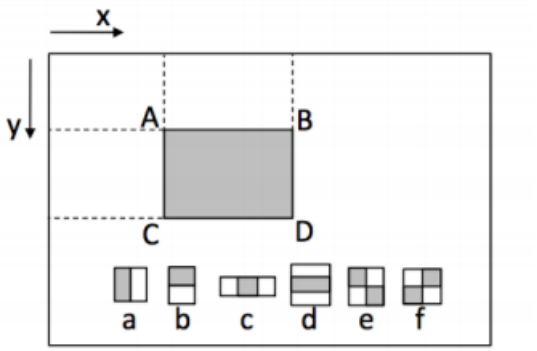
1	2	3
2	4	6
3	6	9

Integral image

Şekil 2.10: Viola-Jones, İntegral resmi

$$\sum_{(x,y) \in ABCD} i(x, y) = ii(D) + ii(A) - ii(B) - ii(C).$$

Şekil 2.11: Viola-Jones, Dört İntegral Değerinin Hesaplanması



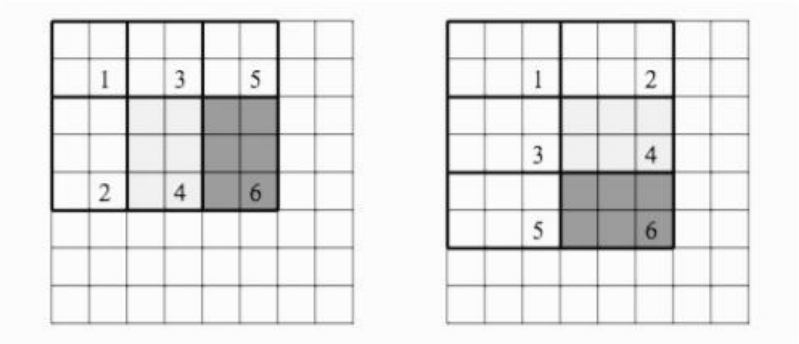
Şekil 2.12: Viola-Jones, İntegral Görüntülerin Haar Feature Dikdörtgenleri

Bu örnek 19*19 pikseldir.

Görüntü input'u olarak => $(18 + 16 + ... + 2) * (19 + 18 + ... + 1) * 2 = 34200$

İntegral görüntü ise 20*20 pikseldir. Satır ve sütunlar sıfırdan başlatılmıştır. Haar feature değeri koyu renkli dikdörtgenin piksel toplamıdır. Aşağıda 6 değer toplanır.

$$f = -I(x_1, y_1) + I(x_2, y_2) + 2I(x_3, y_3) - 2I(x_4, y_4) - I(x_5, y_5) + I(x_6, y_6).$$



Şekil 2.13: Viola-Jones, İki Haar feature Dikdörtgeninin Hesaplanması

Adaboost Training: Amaç kazananı ve kaybedeni bulmaktır. Amaç en çok tercih edilen oranı bulmak, en hızlı kaydedilen tur süresini son bir aydaki yapılan en büyük kazanç [15].

ID	Name	**Admit/Deny**	Region	Gender	GoodAtMath	Athlete	SAT
1	Andrew	Admit	East	M	Y	N	2280
2	Burt	Deny	East	M	N	N	2180
3	Charlie	Deny	East	M	N	Y	2400
4	Derek	Admit	West	M	Y	N	2260
5	Erica	Admit	Deep South	F	N	N	2360
6	Faye	Admit	Midwest	F	Y	N	2350
7	Greg	Admit	West	M	N	Y	2290
8	Helga	Deny	Midwest	F	N	Y	2380
9	Ivana	Admit	International	F	Y	N	2310
10	Jan	Deny	International	M	N	Y	2150

Tablo 2.2: MIT Admissions Training Data

İki sınıf sistemi vardır şekil 2.14'e göre. Bunlar admit/deny, y/n şeklindedir.

Örnek olarak eğer "matematikte başarılı ise"==Y sonra tahmin edilir "Admit" olarak.

Weak learner olarak genel gerçekleşen hata rastgele tahminden daha iyidir. Adaboost zor veri noktalarına odaklanır. Elde edilen veri noktaları en zayıf sınıflandırıcı tarafından yanlış sınıflandırılmıştır.

AdaBoost zayıf sınıflandırıcıları şu şekilde kapsamlı tahmin eder: Optimal derece ağırlığı kullanılır zayıf sınıflandırıcılar için.

2.9. Yüz Tespiti Ve Göz Takibi

Gaze takibi, insan bilgisayar etkileşiminde (HCI) ve biyometrikte dikkat çekmeye başlamıştır. Güvenilir gaze sonuçlarının elde edilmesinde yüz tespiti, göz region tespiti, göz bebekleri ve iris tespiti sayesindedir. Yaratılan Haar cascade, Viola-Jones metodu ile yüz ve göz tespiti yapılabilir.

3. DİZAYN VE ARAÇLAR

3.1. Giriş

Gün geçtikçe teknoloji çığır açmakta ve insanlar artık yanlarında ufak taşınabilir cep telefonlarını rahatlıkla kullanabilmektedirler. Bununla beraber hayatın getirisi olarak bir çok datayı tek bir cihaz içinde bulundurabilmekteyiz. Bu yüzden gün geçtikçe güvenlik açıkları ortaya çıkmaktadır. Aynı zamanda saldırı düzenleyecek insanlar tarafından kurar ihlalleri artmaktadır. Güvenlik, kullanılabilir aygıt üzerine entegre edilir. Bu yüzden kullanıcılar daha komplike parolalar oluşturmak zorundadırlar.

Bilgisayarlarda da güvenlik koruması vardır ve onlarında donanımlarında arızalar çıkabilir. Bu yüzden insanlar her an bir hata alma durumuna karşı olarak durumu kabullenmektedirler ve backup alırlar. Benzer olarak insanlar sitelere bağlandıklarında kullanıcı adı ve parolalarıyla giriş yaparlar ve kayıt aşamasında gerekli belli başlı ilgileri doldururlar. Teknolojinin ilerlemesiyle bu güvenlik işlemleri yetersiz kalmakta ve yeni koruma sistemlerinin geliştirilmesi gerekmektedir.

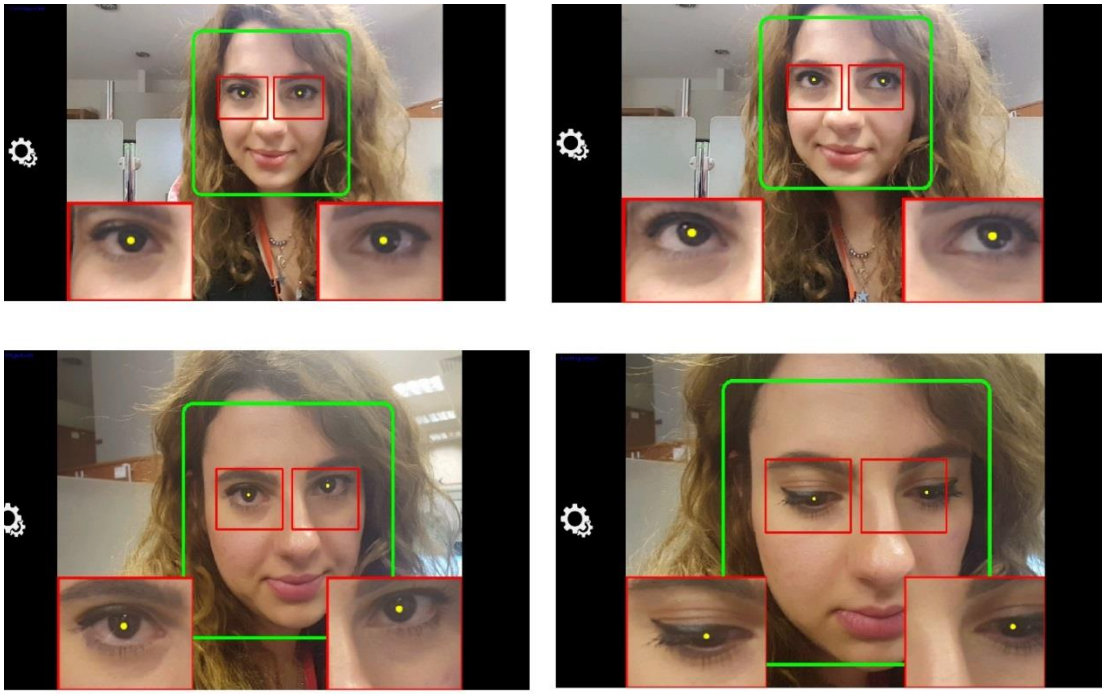
Günümüzde insanlar hızlı bir şekilde kimlik doğrulaması yapmak istiyorlar. Örnek olarak; parolanın el ile girilmesi, şekil çizilmesi, parmak okutulması ve geliştirilmekte olan göz takibi ile doğrulama yapılması.

Karakteristik parametrelere göre kimlik doğrulama işlemi yavaş olmalıdır ve ne kadar yavaş ise bu işlem o kadar güvenlidir. Bu sayede kullanıcılar bilgilendirilir. En basit parolamada de parola direk yazdırılır. Bu işlem verilerinizi en basit düzeyde korur. İlerleyen teknoloji ile cep telefonları, laptoplar ve ipad'ler ile medikal alanlarda tutulan hasta verilerinin, finansal veriler vb. şemaları kimlik doğrulama şemalarına oranla daha komplikedir. Cep telefonlarında ise kullanıcılar hem güvenli hem de kullanılabilirliğinin daha kolay olmasına dikkat çekmektedirler.

Son noktada asıl amaç arka plan server'ını ve veri deposunu korumaktır. Cihaz authentication'ı, kimlik doğrulama etkileşimini talep eder. Sistem kullanıcı etkilişimi için orta düzey MFA güvenliği ister. MFA ile birden fazla method kullanır.

3.2. Eye Localization

Akıllı telefonlar için geliştirilmiş olan ‘Eye Localization’ uygulaması ile yüz tespiti ve göz bebeklerinin tespiti yapılmaktadır. Kamera önünde bulunan kişinin göz hareketleri sürekli takip altındadır. Nereye bakarsa baksın geliştirilen uygulama sayesinde göz bebekleri sarı noktalar ile takip edilir. Kırmızı çerçeveler ise gözleri takip etmektedir. Yeşil çerçeve olanlar da kişinin yüzünü hedef almaktadır.



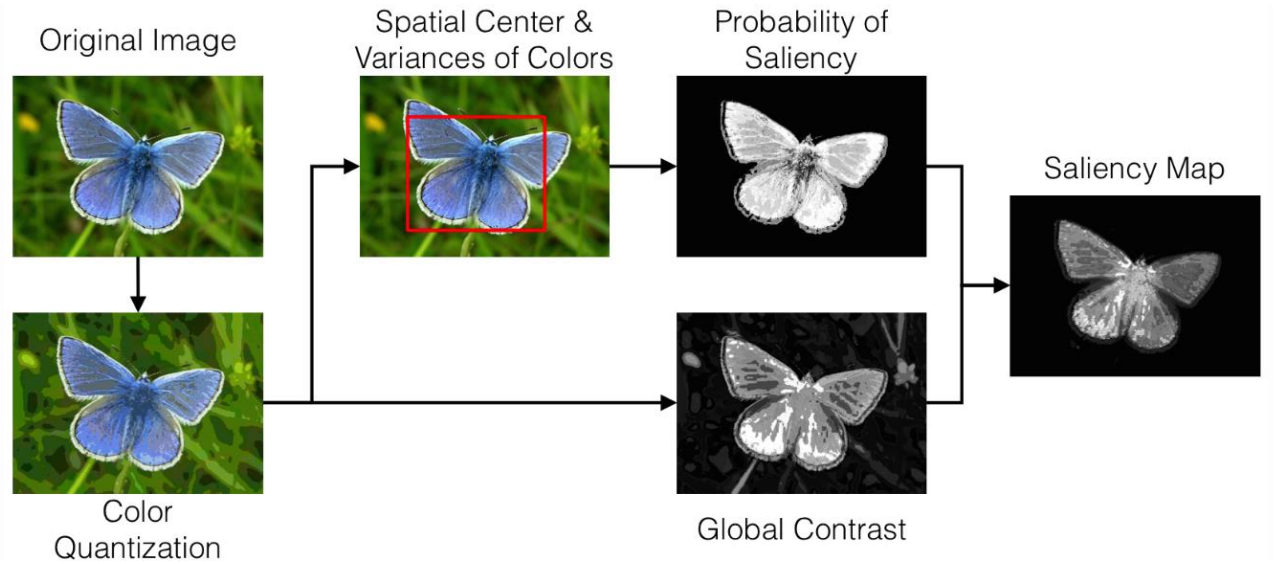
Şekil 3.1: Eye Localization Uygulaması

3.3. Gaze Tabanlı Kimlik Doğrulama

Gaze tabanlı parolamada shoulder surfing resistant kimlik doğrulaması kullanılır. Ancak bu aşamada parola oluşturmak zorlu olabilir. Florian.alt bu aşamada ‘Novel Authentication’ kullanmıştır. Amaç tek bir resim çerçevesinde grafiksel olarak parola oluşturmaktır. Parola zorluğuna bağlı olarak kullanıcı görsele bakarken görsel dikkatine bağlı olarak bir parola oluşturur. Bu işlem sonucu standart olan resim kimlik doğrulamasına oranla girilen 4 karakterli PIN parolasına göre daha güvenli olur. Göze çarpan kalıplar parolayı daha da güçlendirmektedir [15].

Sonuç olarak, görsel olarak parolama PIN ile girilen parolaya göre daha güvenlidir ve bunu ‘Florian.alt’ görsel parolamayı iki kişi üzerinde denemiştir. Deneme süresinde ön bir eğitim verilmiştir ve iki gün sonra bu iki kişiden parolalarını girmeleri istemişlerdir. Ayrıca parolalarını hatırlamamaları sorun teşkil etmemektedir. Deneme sonucunda 40 paroladan 14’ü doğru hatırlanmıştır. Onay verilen şekilde kullanıcılar istedikleri grafiksel parolalarını belirleyebilirler. İhtimallere karşı her iki parolada en başta kullanıcı hesapları yaratılırken belirlenmelidir.

Şekil 3.2: Gaze-Based Grafiksel Parolama Örneği



Şekil 3.3: Saliency Masks

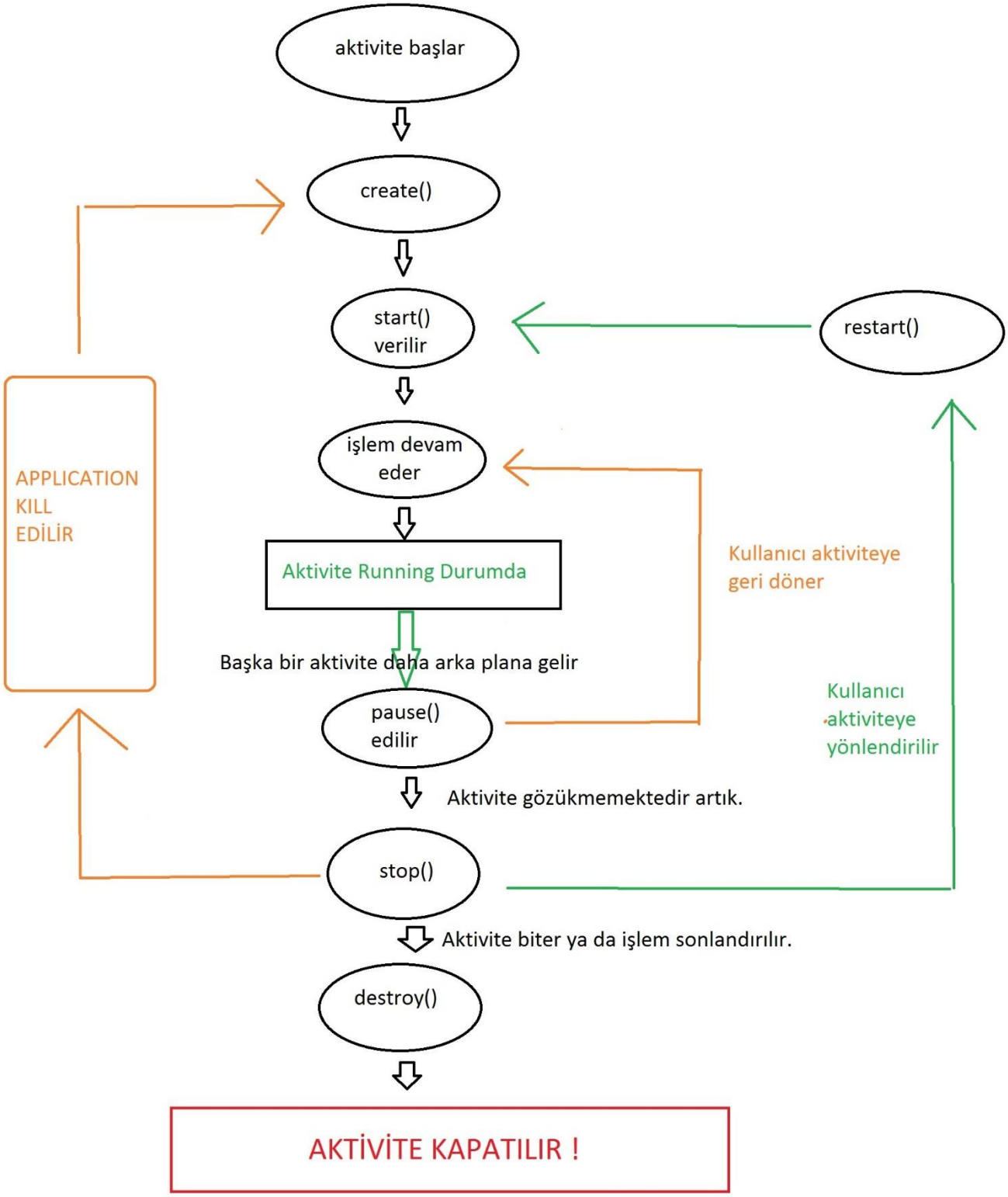
3.4. Android

Android işletim sistemi diğer işletim sistemlerine göre open source'dur. Gerekli tool'lar sayesinde application'lar geliştirilebilir. 'Eclipse' ve 'Android Studio' bunlara örnektir. Kullanıcı kimlik doğrulaması çoklu faktör sonrasında bu işlemi arşivler.

Sistem birden fazla algoritma yürütür. Asıl amaç çoklu faöktör özelliğini sağlayabilmektir. Algoritma kalibre edilmelidir göz takibi için. Bunun sonucunda sadece kullanıcının bilgisi sisteme alınmış olmalıdır. Bu işlem sonucunda güvenlik sağlanmış olur ancak MFA için değildir. Ekstra güvenlik için geliştirilmiş olan bu işlem sistemin çalışması ve parolanın girilip kabul olmasıyla ilgilidir.

3.5. Göz Takibi İçin Android Applicatıon Lifecycle

İlk olarak create() fonksiyonu çağırılır. Ardından start() fonksiyonu ile aktivite çalışmaya başlatılır. İşlem aynı zamanda pause ve resume olarakta devam ettirilir ya da durdurulur. Eğer kullanıcı application'ı kill ederse (örneğin, geri tuşuna basarsa) application pause() durumuna getirilir. Kullanıcı tekrar uygulamaya girdiğinde bu aktivite kaldığı yerden devam eder. Bu anda devreye resume() fonksiyonu girmiş olur. Geri tuşuna basıldığında 2 fonksiyon çağırılır aktivitede. Bunlar; destroy() ve stop() fonksiyonlarıdır. Altivite lifecycle'ı şekil 3.4'te gösterildiği gibidir.



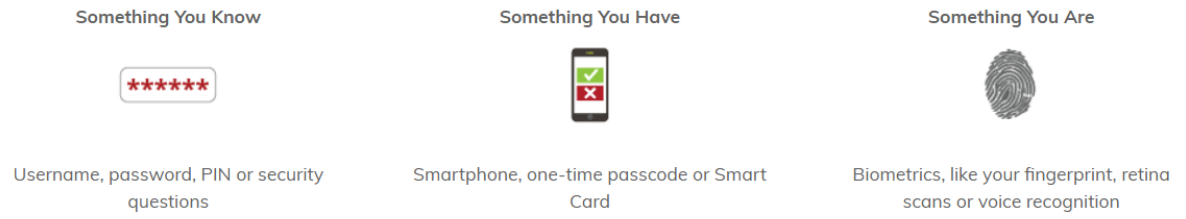
Şekil 3.4: Android Activity Lifecycle

3.6. Multi Factor Authentication (MFA)

Multi factor kimlik doğrulamayı farkında olmadan hemen hemen herkes günümüzde kullanmaktadır. Bunlara örnek olarak;

- Banka kartınızı ATM'de swipe etmek
- Bir websiteye girerken login olduktan sonra autherise için ceb telefonunuza gelen parolayı tekrar websitesine girmek

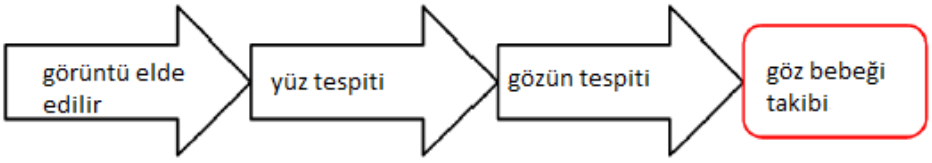
MFA bazen 2FA kullanmakta, güvenlik delili olarak göstermek için. MFA'nın en doğru olarak anlatılmış hali şekil 3.5'te gösterilmiştir [16].



Şekil 3.5: MFA'nın En Doğru Özeti

3.7. Gaze Estimation Algoritması

Kameranın sağladığı video görüntüsü ile gözün görüntüsü extract edilir. Gaza estimation ve gözün tanınması sağlanır. Bu olay şekil 3.6' da adım adım gösterildiği gibi gerçekleşmektedir.



Şekil 3.6: Gaze Estimation Algoritması

Bu algoritmanın ilerleyen akışını etkileyen en önemli faktör, kameranın çözünürlüğüdür. Ancak video chat için tasarlanmış olan akıllı telefonlardaki ön kameranın çözünürlüğü daha düşük kalitedir.

Haar cacscade denemelerinde yüz ve göz tespit edilir. Bu işlemi 100 kere, 1000 kere tekrar edilirse işlem daha güvenilir olur. Haar'ı kullanırken tespit süresi direkt olarak piksel sayısını, resim büyüklüğünü belirler. Görüntü büyüklüğünü küçültmek tespit algoritmasında yer alan tespit süresini azaltır. Dikey yüz tanımlama işlemi, özellik tanımada kolaylık sağlar. İşlem başlatıldıktan sonra en iyi olan match seçilir ve onun tespit edilmiş halini görürsünüz. Eğer karede birden fazla yüz var ise en büyüğü seçilir. Göz takibini hızlandırabilmek için ilk işlem yüz tanımlaması yapılır ve çerçeve içine alınır. Bu maske hem yatay hem de dikey olarak yerleştirilir. Bu yarım resimleme işleminden sonra göz takibi algoritmasına geçilir. İnsan anatomini optimize etmek için dikey yönde orta hizalarda göz tespiti yapılır. Bir göz tespiti yapıldıktan sonra aynı göz eşit hizada diğer tarafta olmak üzere tespiti gerçekleştirilir.

Yüz tespit algoritmasına benzeri olarak, sol üst taraf önemlidir. Çünkü gaze estimation algoritması için de kullanılır. Algoritma göz tespiti yaparken aynı zamanda yüz tespiti gerçekleştirilir. Bu işlem görüntü yakalama ve video frame'i belirlemede ki geçen süreyi kısaltır. Bu kısımda görüntü kesilir ve göz bebeği takip algoritmasına geçilir.

Göz bebeğini takip etmeden önce bütün pikseller işlem görülür, segmentlere ayrılır. Bu işlemin amacı işlem süresini azaltmaktır mümkün oldukça.

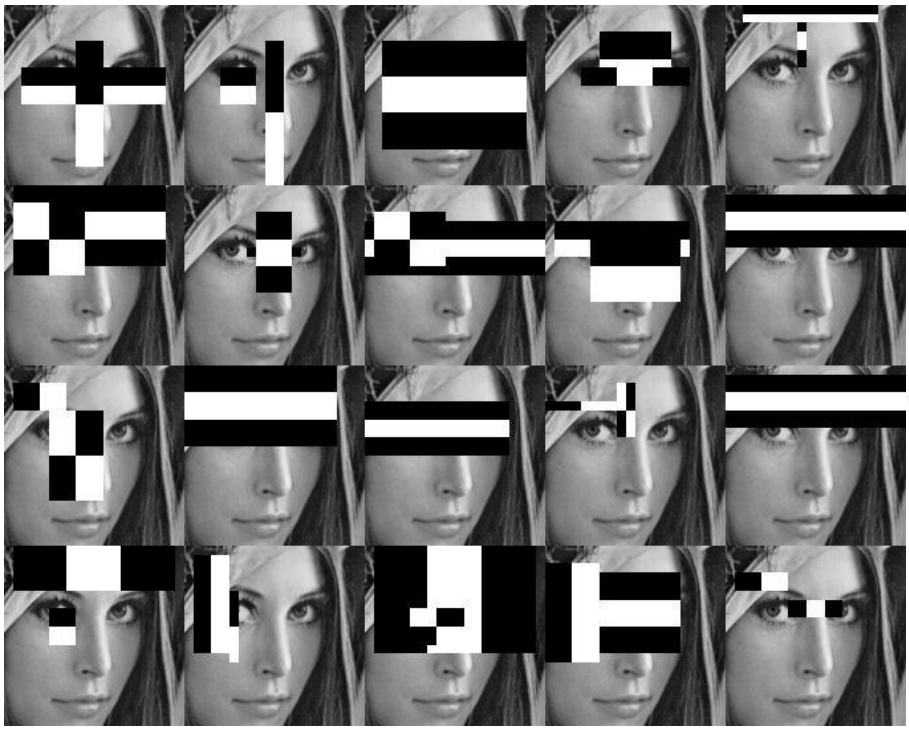
Sonuç olarak MFA sayesinde olabilecek olan saldırılar azaltılmış olur. Algoritma kullanıcıya göre kalibre edilmeli ve tasarlanmalıdır.

4. TAKİP ALGORİTMALARI

Bu bölümde göz takibiyle ilgili algoritmalar bulunmaktadır. Göz takibinin işleyişi, nasıl uygulandığı, göz bebeğinin nasıl merkezlendiği ve bütün teoriler ile ilgilidir.

4.1. Haar Cascade

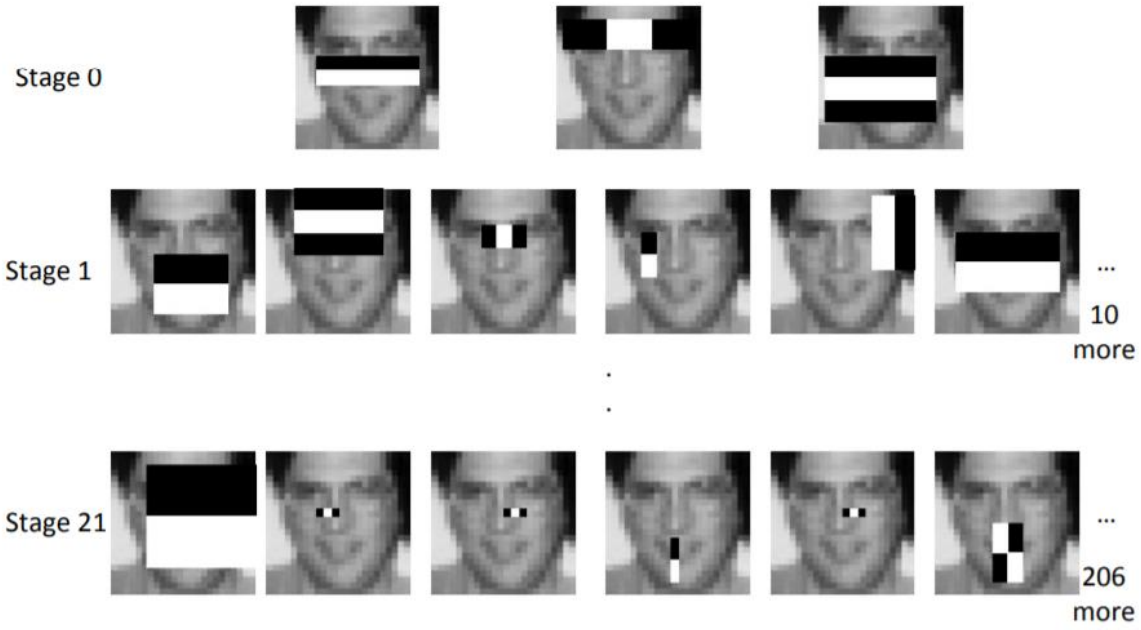
Günümüzde iyi ya da kötü bütün cep telefonları insan yüzünü tespit edebilmektedir. Basit bir kod ve akıllı telefonlar için yazılan bir uygulama aracılığıyla basit bir görünüm yakalayabilirsiniz. Bu işlem Viola – Jones algoritmasının Haar cascade sınıfı sayesinde gerçekleşir. Bu algoritmada daha önceden bahsettiğim gibi yüz tespiti yapılmaktadır.



Şekil 4.1: Viola-Jones, Haar Feature Tekniği

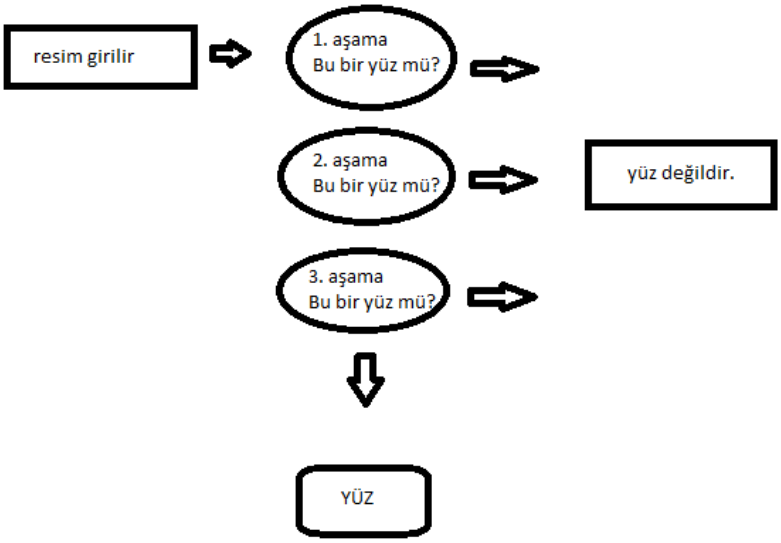
Temel olarak makine öğrenmesi algoritmasıdır. Bir çok yüzü ve yüz olmayan kareleri seçer ve bunları Haar cascade özelliği kullanılarak realtime görüntüsü elde edilir [17]. Training verilerde işlem yavaştır ancak tespit daha hızlıdır.

Aşama aşama dikdörtgenlerle aşağıdaki gibi yüz şeçme işlemleri gerçekleşmektedir Haar sınıfında



Şekil 4.2: Haar Feature Tekniğinin Etapları

Yüz tespitinde Haar cascade kullanımını input olarak resim girildiğinde, ilk iş olarak input görüntüye girilen görüntünün yüz mü olduğunu sorgular. Bunu birkaç kez tekrarlar. Eğer sonuç yüz değil ise yüz değildir sonucunu girer. Şekil 4.3'te sorgulama tekniği gösterilmiştir.



Şekil 4.3: Haar Feature Sorgulaması

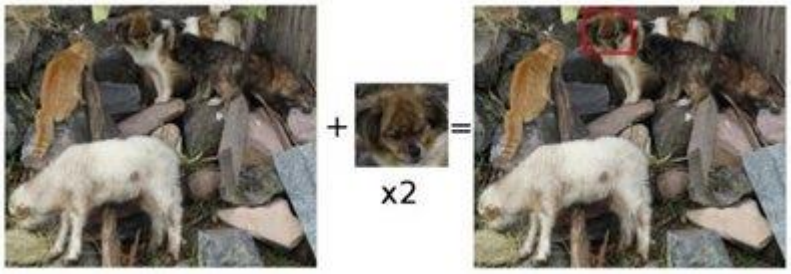
Kompleks resimlerde yüz tespiti zor olabilmektedir, ancak çekilen resimdeki arka plan sade, düz olursa yüz tespiti başarı oranı artmaktadır.

4.2 Template Eşleşme Algoritması

Bilgisayar görüşünde template eşleşmesi demek, görüntünün benzeri olan template ile eşleşmesidir. İki tane bileşen vardır;

- Kaynak resim
- Template resim

Kaynak resmin (K) içinde template resim belirlenmiştir ki aranılan template resim bulunabilsin diye. Template resim (T), kaynak resim ile karşılaştırılıp ortaya en iyi eşleşmenin çıkmasını sağlamaktadır. Eşleşen bölgeler her piksel ile hesaplanır, bir den fazla hesaplama ile de en iyi eşleşme ortaya konulur.



Şekil 4.4: Template Eşleşmesi

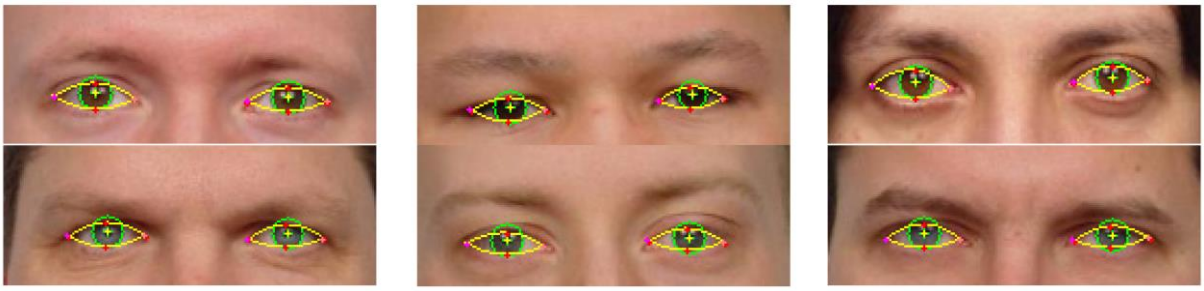
4.3 Timm ve Barth Algoritması

Timm ve Barth göz bebeği merkezini bulmak için kullanılır. Algoritma tüm input resim üzerinde çalışır ve iris merkezini bulma odaklı olarak. Genelde göz bebeği karanlık çıkar. Ek faktör olarak Timm ve Barth algoritması göz bebeğinin ters çevirilmiş görüntüsünü alır. Algoritma sistem analizi ve tespitte kullanılır. Kullanıcının istemsiz gözünü kırmasına bağlıdır. Hareket analiz tekniği kullanılır, template oluşturulurken gözün.

İlk adım olarak gözün konumu tespit edilir. Bir çok görüntü ve önceki görüntüler thresholded işlemi ile binary görüntüye ulaşılır. İki farklı görüntüde gözün hareketinden ötürü bozulan resimler elde edilir. Görüntü kirliliği de giderildikten sonra ortam ışığı, kamera

çözünürlülüğü de görüntüde etkilidir. Ortaya çıkan görüntüde en mümkün görüntü elde edilmeye çalışır hem sol hem de sağ göz için. Eğer yükseklik ve en de büyük bir fark var ise bu kullanıcının gözü değildir.

Template yaratılırken, kullanıcı gözünü kırptığı andaki görüntüsü asla çekilmemelidir. Göz tespit edildiğinde zamanlama ayarlanır. Template elde edildikten sonra zamanlayıcı sayesinde kullanıcının göz kırpma süresi hesaplanır.



Şekil 4.5: Göz Template

Template eşleşmesinde kullanıcının gözünü kırpmasının doğruluğu önemlidir.

Bu hesaplamanın sonucunda korelasyon ortaya çıkar. Ortaya çıkan değer ile açık veya kapalı bir göz şablonu olup olmadığını anlaşılabilir. Hassasiyet kaybı vardır. Ortam aydınlatma koşulları sürekli değişir. Bu yöntem saniyede 30 kez gerçekleştirilir. Arama yapılan bölge kullanıcının gözünün etrafındaki küçük bir alanla sınırlandırılmıştır. Bu azaltılmış arama alanı, sistemin smooth olarak gerçek zamanlı çalışmasını sağlar.

- Kamera çözünürlüğü; maliyet ve etki kamera çözünürlüğüne bağlıdır.
- Kameranın konumu; gözün kameraya olan uzaklığı önemlidir ve ne kadar yakın olursa o kadar başarılı sonuç elde edilir.
- Sabitlik; yatay olarak performans %30 oranında daha başarılı olmaktadır ve olabildiğince stabil kalınırsa test daha güvenilir olmaktadır.
- Özne; farklı insanlar farklı göz yapılarına ve dolaylı olarak farklı göz tespitlerine neden olmaktadırlar. Bu gözlüğe, test sırasında başlarını oynatmalarına ve göz kırpmalarına bağlı olarak değişmektedir. Hedef bu sorunları minimum düzeyde tutarak başarılı bir model oluşturmaktır.
- Ortam ışığı; bu sadece görüntü çözünürlüğünün dışında da kamera frame oranını da etkilemektedir.

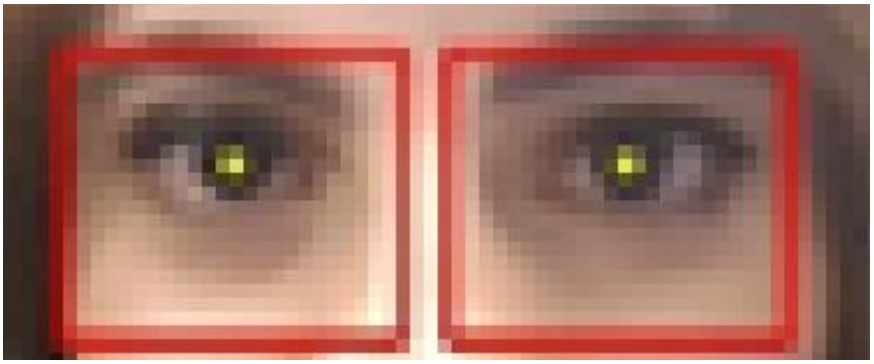
5. IMPLEMENTATION

5.1 Android Eye Localization Uygulama Sonuçları

En iyi durumlar ekrandaki kişinin static durması ve ortam ışık kontrastının ideal olması göz tespitinde ve gaze işleminde önemlidir. Algılama algoritması nispeten kesin sonuçlar verir, ancak uygulama aydınlatma ve mobil cihaz konumundaki küçük değişikliklere karşı duyarlıdır. Dahası, basit olarak yüz özelliklerini tespit ederken küçük bir kesit ile tespit edilmiş olan göz bebekleri gösterilir. Gözün nerede olduğunu bulmak için gerçek zamanlı göz işleme gereklidir. Uygulama gereği kullanılan ön kamera yüksek performanslı değildir. Göz tespit edildiğinde direk olarak kırmızı bir çerçeve içine alınır. Gözün tespiti ile ortaya güvenilir bir gerçek zamanlı sonuç çıkar. Kamera kalitesinin düşük olmasından kaynaklı olarak bir sonuç elde edilemez ve bunun için daha başka bir şey yapılamaz. Ayrıca telefon dünyasına bakıldığında doğal ortam static olmadığı gibi cep telefonlarınında işlemcilerinin yavaş olmasıyla kaliteli bir gerçek zamanlı görüntü ortaya çıkmamış olabilir. Akıllı telefonlarında gerçekleşen büyük gelişimler sayesinde artık sadece gözlere odaklanılıp, daha detaylı bilgiler edinilmeye başlanıldı. Aynı zamanda bu işlem laptop'ların webcam'lerinde de gerçekleşmektedir.

5.2. Gözün Görüntüsünün Veritabanı

Asıl amaç gözün detaylarını işlemek ve gaze yönünü ve sizisini yeterli bir şekilde kimlik doğrulamk için bilgilerini toplamaktır. Göz tespit algoritmaları ve scriptler ile gözün görüntüsü kaydedilir. Bunu yapan programlar OpenCV ve SimpleCV'dir. SimpleCV uygulamasında webcam desteği de bulunmaktadır. Ancak bu işlem görüntü kalitesinden ve yakalanan gözün görüntüsü çözünürlüğünden dolayı .masraflı olabilir. Ancak video frame oranları bu scriptler tarafından optimize edilebilir. Akıllı cep telefonlarında kırpılmış görüntüler tespit edilir. Bunlar gözlerin ve yüzün dosya olarak kaydedilmesiyle oluşur. Gözün görüntüsü veritabanına yüklenir. Görüntünün organizasyonuna göre amaç segmentasyonların sonucuna ulaşmaktır. Aşağıdaki resminde gözün veritabanında saklandığı kalitesi ve çözünürlüğü verilmiştir.



Şekil 5.1: Gözün Görüntüsünün Veritabanındaki Kaydedilmiş Hali

Görüntüler ışığın durumuna ve diğer etkenlere bağlı olarak veritabanına o anki görüntü kaliteleriyle kayıt edilirler.

5.3. Gözün Görüntüsünün İşlenmesi

Göz bebeğinin tespit edilmesiyle elde edilen gözün görüntüsünde iris te tespit edilmiş olur. Bir önceki konuda paylaşılmış olan şekil 4.5'te göz bebekleri daireler içerisine alınır. Doğru bir implementasyon yapılabilmesi için uygulama tarafından çözünürlük olarak 960*1280 seçilir. Bu sayede algoritmalar etkili olarak göz bebeği takibi ve yüz takibi yapabilmektedir. Çözünürlük dikkate alınması gereken bir unsurdur. ???????Bunun en önemli nedeni resme bakıldığında göz bebeklerinin ne kadar küçük olduğunu herkes görebillir ve buna ayırılan pikselde küçüklüğüne bağlı olarak az olmaktadır. ???????

Frame'in maksimuma çekilmesi tespit aşamasını hızlandırır. Bu çalışmada, veritabanına bakıldığında gözün tespit edilen kimlik bilgileri ile amaç göz bebeği segmentasyonlarına ulaşmaktır. Bunu;

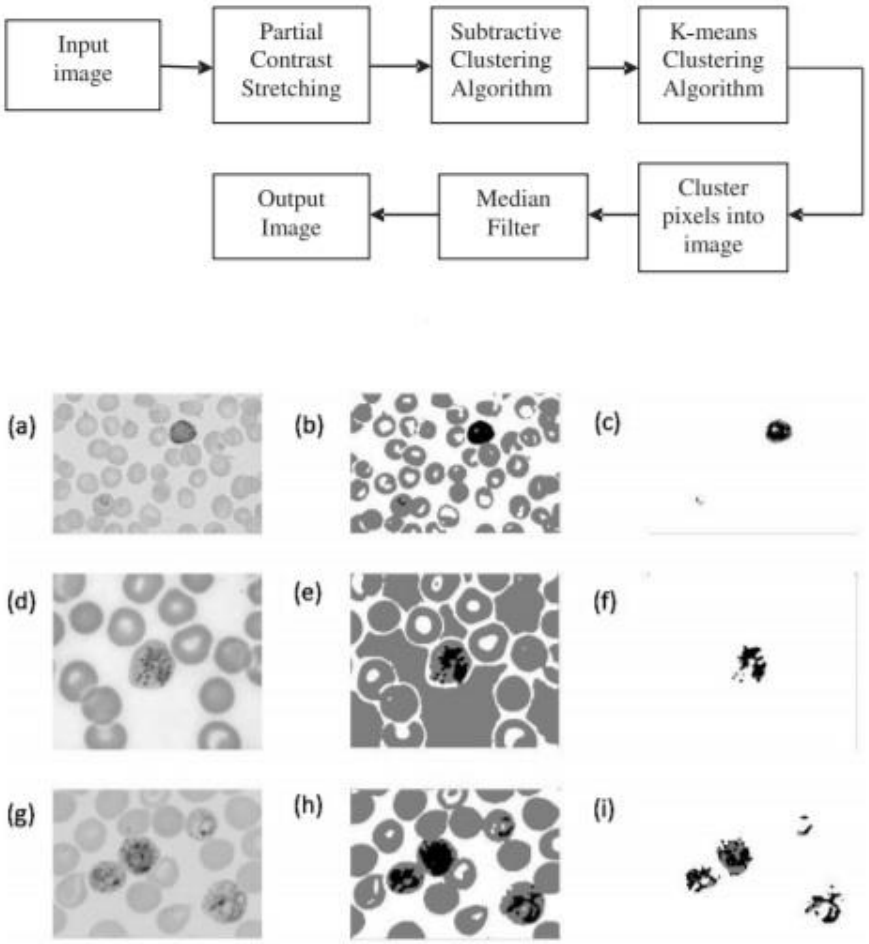
- K means
- Daugman's Integrodi Erential Operator
- Morphological Processing

ile elde ederiz.

5.3.1. K Means

Sınıflandırma tekniği genel olarak görüntü işleme ve bilgisayar görü uygulamasında benzer özellikte olan piksellerin sınıflandırılmasında kullanılır yoğunluğuna ya da rengine göre. K means sınıflandırması, k optimal sınıflandırma sonucu ve bütün piksellerinin minimum renk

uzaklığına göre ayrılıp sınıflandırılmışlardır. Bu işlem herkesin farklı irisi, ten rengi, farklı gözbebeği ve beyazlığına göre yapılmıştır. K means sınıflandırmasının asıl amacı renk seğmenleri methoduna göre, iris rengine göre aynı zamanda irisin dışında yakalanan göz resminde gözbebeğine göre seğmenlere ayırmaktır. K means'i uygulamadan önce yakalanan görüntü kırmızı-yeşil-mavi' den (RGB) lightness-alpha-beta'ya (LAB) çevrilir, alpha kanalının kayıpsız benzerlik kırmızı-yeşil ekseninde ve beta kanalının kayıpsız mavi-sarı ekseninde.



Şekil 5.2: K Means Örneği ve Akış Şeması

Görüntü segment olarak yüklenir. Kontrast uygulanır. Sınıf numaraları oluşturulur k sayıları olmak üzere. Denklem oluşturulur bütün piksellerin değerleri için. 3 Adımda maksimum potansiyel oluşturulur, orta merkez sınıflandırma olarak en uyumlu olan. Potansiyel verilerin denklem kullanarak update yapılır ilk olan merkezi sınıflandırmaya göre. Maksimum değer bulunur dördüncü adımda. Bu işlem k değerini bulana kadar devam eder. Öklid uzaklığıyla her pikselin merkeziyle alakalı olan resimde. Minimum uzaklığa bağlı olarak yeni piksel atanır. Tekrar yeni merkez hesaplanır. Bunu 10-12 kere tekrarla yaparak hata toleransı

azalacak şekilde olmalıdır. Sınıflar tekrar şekillendirilir resim olarak. Medyan filtreleme uygulanır resim segmentlerine ki istenmeyen kirlilik yok edilmek üzere.

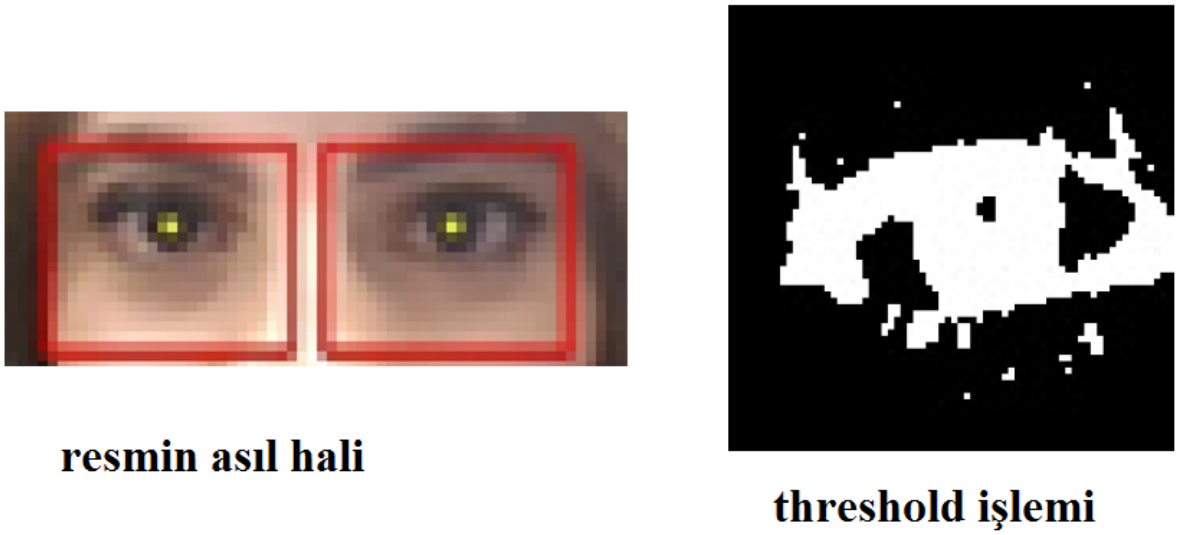
Şekil 4.6'da yayılmış olan mikrop görüntüsü vardır ve bu resimde istenilen algoritma uygulanmıştır matlab ortamında. K=3 seçilmiştir. K means uygulandığındaki ilk görüntü orta sütündakidir. Diğer uygulamada ise en son hali sağdaki sütundur.

Sonuç olarak bu algoritmada gözün görntüsünün pikselini oluşturan grup ile k'ye aktarılır Öklid uzaklığı pikseller arasında. Bu metot 3 renk ile yapılır. Bunlar; ten, iris/göz bebeği beyazlıktır. Buna bağlı olarak gözün görüntüsü sınıflandırılır k denklemi kullanılarak ve piksellerde iris ve gözbebeği tespit edilir. İnsan teni piksellerde dikkat edilebilir şekildeir. Çünkü açık renkte piksellerdir. Bazı durumlar vardır ki gözbebeği ve irisin de renginin açık olduğu pikseller biyolojik sebeplerden ötürü.

5.3.2. Morfolojik Segmentasyon

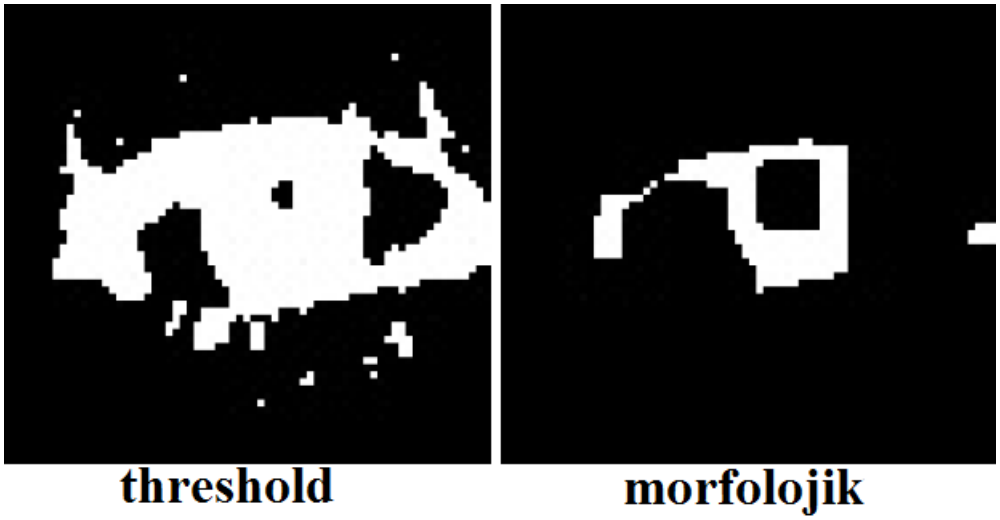
Biyometrik bilgi çıkarılırken belirlirli performans gerekliliğine bakıldığında,başlangıçta güçlü analitik bütünlüğe sahip bir yöntem araştırılmıştır. gelişmekte olan gerçek zamanlı bir segmentasyon yaklaşımı ana öncelik haline geldi. Morfolojik segmentasyon, thresholding, dilation ve erezyon gibi doğrusal olmayan görüntü filtrelemesi kullanır.

Bu uygulama için, filtreler seçilir; resimde iris ve gözbebeğini temsil eden pikseller haricindeki görüntüler silinir. Bu metot 3 basit işleme tekniğiyle göreseller üzerinde implemente edilmiştir. Genellikle kullanıcının gözbebeği merkezini son derece doğru bir şekilde ortalıyarak sırayla gerçekleştirilir. SimpleCV kullanılarak tekniklerin uygulanması ile bütün iris segmentasyonu işlem görür, irisin merkezi tespit edilir.



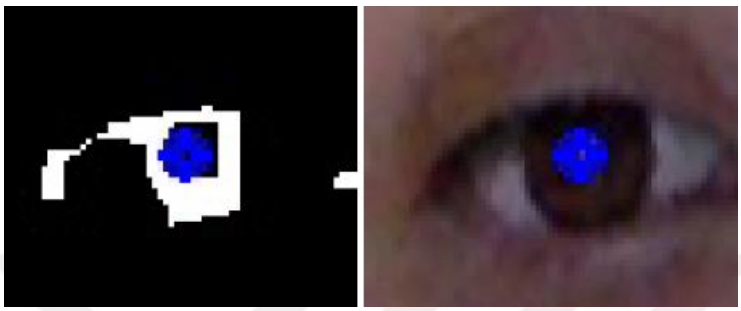
Şekil 5.3: Orijinal Resim ve Threshold Görüntüsü

Iris alanını segmentlere ayırmada ilk adım olarak, göz görüntüsünü binary olarak threshold yapılır. Gözbebeğinin en karanlık olması gerektiği için görüntüdeki bu bölge, görüntüyü iki kategoriye ayırır: (1) eşik değerinin üstünde threshold ve (2) eşik değerinin altında threshold. Threshold, kullanıcı tarafından gözlemlenen aydınlatması kalibre edilmelidir, ayarlanmalıdır. Amaç belirli ortamdaki koşulların doğru sonuçları sağlaması için. Binary gösterimde, threshold altındaki pikseller 1 değeriyle sınıflandırılır ve diğer tüm pikseller yok sayılır ve 0 değeri ile sınıflandırılır. Threshold çıktısı şekil 4.8'de gösterilmiştir.



Şekil 5.4: Threshold ve Morfolojik Görüntü

Bir çok gürültü irisin etrafından silinmiştir. Geriye kalan gürültüler ise morfolojik erezyonlar ile silinmiştir. Erezyon işleminde binary görüntüdeki pikseller silinir. Erezyon işleminde 3*3 maskesi işlenir. İris bölgesi minimum 9 kareden büyük olmalıdır. Erezyon işlemi sonucunda iris etrafındaki kenarlar silindi ancak dilation işlemi ile tekrar büyüyecektir. Morfolojik işlemde ise binary resimde iris seçilir ve işlemler sonrasında gözün orijinal ve irisin seçili hali karşımıza gelir.



Şekil 5.5: Morfolojik İşlem Sonrası

Şekil 4.9'daki işlemde iris merkezi bulunmuş ve mavi olarak seçilmiştir. Aynı zamanda blob işlemi yapılmıştır burada. Blob ile aynı seçilmiş bölgeler bir arada bulunur. SimpleCV blob tespit operatörü ile resmin merkezi hesaplanır.

Variable	k-Means	DIDO	Morphological
Dark Iris	Good	Best	Best
Light Iris	Poor	Poor	Good
Dark Skin	Poor	Good	Good
Light Skin	Good	Good	Best
Overhead	Good	Poor	Best
Sunlight	Poor	Good	Good
Lamp	Poor	Poor	Good
Bright Directed	Poor	Good	Good
Dim Light	Poor	Poor	Good

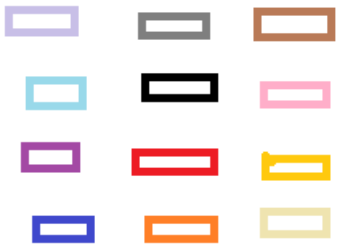
Tablo 5.1: İrisin Renk Etkileri

Konunun içerisinde de renklerin etkisinden bahsedilmişti ve bununla ilgili olarak yukarıdaki şekil 4.10'da bütün detaylar verilmiştir etkileri ile. Şekil 4.10'daki tablonun özeti olarak değerlere bakıldığında açık renk endişe yaratmaktadır database'de. Bütün performans hesaplamaları 10-15 göz örneği üzerinden yapılmıştır.3'ün altında başarı oranına sahip olanlar 'poor' olarak belirlenmiştir. 5'ten fazla başarılı olanlar ise 'good' olarak nitelendirilmiş ve son olarak 8'den fazla başarılı olanlar ise 'best' olarak seçilmiştir.

Tabloya bakıldığında morfolojik işlem daha başarılı bulunmuştur. Thresholding işlemi ışık durumunu uyarlar. Lamba aydınlatması en zor durumdur. En iyi kullanıcı çevresi açık ten, koyu iris rengi ve tepeden ışıklandırmadır.

5.4. Kullanıcı-Cihaz Arasındaki Kimlik Doğrulama İçin Uygulama

İlk adımda iyi bir performans elde edilebilmesi için calibre edilmelidir uygulama. İkinci adımda kullanıcının seçtiği uzunlukda ve komplekste bir PIN girilmelidir. Üçüncü adımda ise çoklu faktör uygulanmalıdır PIN'nin dışında. Parolanın girilmesiyle göz gaze'i uygulanmalıdır.



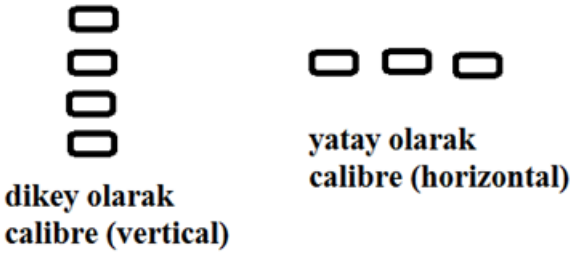
Şekil 5.6: Parola Ekranı

Kullanıcı şekil 4.11'de bulunan 12 adet tuşu kullanarak bir parola girerken, her bir tuşa bastığında renkler değişir her seferinde. Amaç güvenliği artırmaktır. Her bir sembolün bir anlamı vardır ve random olarak değişmektedir.

5.4.1. Mesafeye Ve Projeksiyona Bağlı Gaze Estimation

Implementation yapmadan önce gözün konumu belirlenir ve ardından referans noktası belirlenir. Bu referans noktası belirlenince kimlik doğrulama için kullanıcının bakış doğrusunda ilerlenir. Kullanıcı akıllı cep telefonuna baktığında gözünün konumu ve gözbebekleri aşağı yukarı aynı hizada olmak zorundadır. Uzayda, özne nerede ise bakış açısı oraya doğrudur. İki boyutun birbirinden farkı gözün konumu ve göz bebeğinin nerede merkez olduğudur (Δx, Δy). Unutmamak gerekir ki gözbebeğinin ve gözün konumunun hedef noktalaları aynı değildir. Bu sebepten ötürü, gözün konumunun merkezinin referans noktası gözün doğal bakışı olarak alınmıştır ve bu cihazın memory'sinde tutulmaktadır. Çoğu özne için, iki merkez mükemmel bir şekilde uyum sağlayamaz. Bu nedenle bir çeviriReferans noktasını veya göz bölgesi merkezini ayarlamak için sabit hesaplanmalıdır. Eğer özne gözün merkezinden uzaklaşır göz bebeği artık aynı pozisyonda değil ise, bu noktalar arasındaki mesafe ölçülür.

Uzaklık ölçümü yatay (Δx) ve dikey (Δy) olarak yapılır. İki boyuttaki vektörler gaze vektör olarak adlandırılır.



Şekil 5.7: Yatay ve Dikey Kalibre

Kalibrasyon adımları şu şekildedir; şekil 4.12'de gösterilen bütün blokların hepsi bağımsız olarak kalibre edilir. Birinci adım, dört Dikey merkez noktaları, kullanıcıya dört merkezi bloğun her birine bakmasını isteyerek dikey eksen boyunca uzatılmış ve bakış vektörlerinin dikey bileşenlerinin ortalaması alınmıştır Şekil 4.12'de soldaki gösterilen bloklar gibi çoklu örnekler arasında. İkinci adımda şekil 4.12'de sağda gösterildiği gibi, yatay eksen boyunca üç merkez noktası vardır ve aynı yöntem kullanılır. Bu sonuç 12 aşama yerine 7 aşamada gerçekleşen kalibrasyon işlemi ile kalibre süresi azaltılmış olur. Kalibrasyon tamamlandıktan sonra, örneklenen her bakış vektörü her yönden en yakın merkeze göre sınıflandırılmıştır. Bakış vektörünün bu şekilde sınıflandırılması, bakış açısı tahminini gerçekleştirir ve Android kimlik doğulama uygulamasında bu olayın biyometrik bölümde gerçekleştirmesini sağlar. Bilgi faktörü belirlenmeye devam etmektedir. İşlem tamamlandığında, bir sonraki aşamaya geçilir.

5.4.2. Parolanın Belirlenmesi

Uygulamanın ikinci aşamasında, kullanıcı belirli bir uzunluktaki PIN parolasını girer. PIN bütün kimlik doğrulama işlemlerinde kullanılır. Kullanıcı tarafından PIN yaratılırken kompleks olmalıdır ve uzunluk arttıkça güvenlik artar. PIN seçildikten sonra kullanıcı arayüzünde arşivlenir.

PIN seçildikten sonra cihazda depolanması önemlidir ve encrypt olarak memory de tutulur olası memory saldırılarından korunmak için. Bu PIN'nin 3rd party uygulamalarda güvenli bir şekilde kullanılmasını sağlamaktadır kullanıcının manuel olrak tekrar PIN yaratmak istemesine karar verdiği ana kadar.

5.4.3. Parolanın Girilmesi

Uygulama bu etapta çoklu faktör kimlik doğrulamasında eye gaze sorunsuz gibi gözükebilir. İkinci etapta kullanıcı kimlik doğrulama ekranında gerekli yerlere gözünü diktiğinde sıralı bloklar geçerli değerleri bulundurur ve PIN bu aşamada girilir. Eğer kullanıcının biyometrik özellikleri eşleşmez ve kalibrasyona cevap vermez ise ilk etapta, kimlik doğrulama başarı ile gerçekleşmemiş olur. Benzeri olarak uygulama kullanıcının input'unu tanır ancak PIN'i memory'de yedeklendiği parolanın aynı değil ise kimlik doğrulama başarılı olmaz. Sadece her iki işlemde yani hem biyometrik ve PIN doğru şekilde girilirse başarılı bir şekilde log in olunur kullanıcı hesabına.

Teknoloji ilerledikçe yüksek hassasiyet ile biyometrik parolalarda ileri boyuta taşınmaktadır. Buda geleceğin projesidir. Morfolojik segmentasyon algoritmasına göre bazı kısıtlamalar vardır. Bu da ortam ışığı ile ilgilidir. Sonuç olarak kimlik doğrulama işlemlerinde ışık altında başarılı sonuç elde edilmektedir. Aynı kalibrasyon dünyasındaki gibi. Uygulamaların gelişmesiyle ışık ortamında performans artacaktır algoritma ile.

5.5. Templata Eşleşme Implementation

Dördüncü bölümde bahsedilen template eşleşme algoritması Java veya istediğiniz bir yazılım dili kullanılarak OpenCV'de yazılır. İlk adım olarak yüz tespiti Haar cascade ile yapılıyordu. Haar makine öğrenmesi tabanlı cascade fonksiyonu bir çok pozitif ve negatif görüntülere odaklanmıştır. Sınıflandırıcı bütün yüz özellikleri extract eder.

OpenCV'de k detectMultiScale () fonksiyonuda yüzü tespit eden sınıflandırıcı haarcascade_frontalface_alt_xml'dir. Aranması gereken alanın boyutu fonksiyonda import edilebilir.

Ardından, tespit edilen yüzün boyutlarına ve koordinatlarına göre, iki kare göz alanını temsil edecek şekilde hesaplanır.

Son adımda da gözlerin şablonunu ilk beş karede elde etmektir ve gözleri bulmak için kullanılır bu şablon. Fonksiyon aşağıdakilerden sorumludur;

- Get_template()
- Match_eye()

Get_template() fonksiyonunun input sınıflandırıcı vardır ve bu gözleri tespit eder. haarcascade_frontalface_alt_xml'i kullanarak. DetectMultiScale() fonksiyonu ile. Göz bölgesini bulma algoritması en karanlık bölgeyi bulmayı yani irisi bulmaya çalışır.

Match_eye() fonksiyonu input girişi vardır göz alanı ve ilk resim frame'i yaratıldığının görüntüsünün. Tüm bunlar onCameraFrame() fonsiyonunda çağırılır.

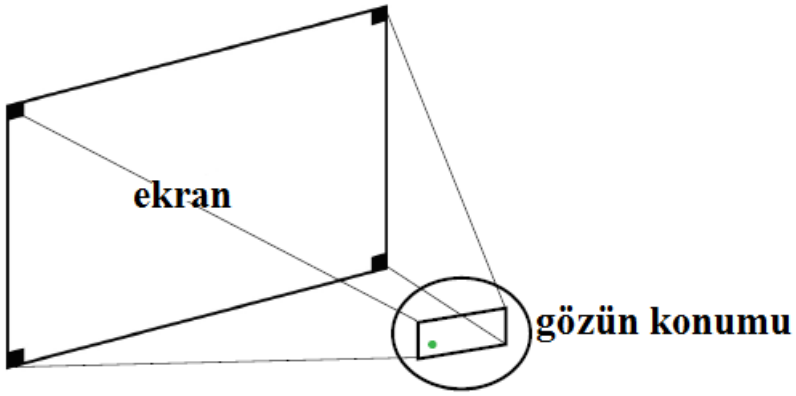
5.6. Timm ve Barth Algoritmasının Implementasyonu

Timm ve Barth algoritması göz bebeğinin merkezinin bulunmasını sağlar. Vektörler kullanılır. Olası vektörlerin oryantasyonu sonucu merkez bulunur. Bazen olası merkez yanlış çıkabilir. Kullanıcının okuma gözlüğünden ve ya gözkapağından ötürü. Bunu düzeltmek içinde ağırlık ortalaması uygulanır karaltının ortasına. Asla aydınlık merkeze uygulanmaz. Gussian filtresi kullanılır gözlük parlaması ve aydınlatmadan kaçınılmak için.

Bazen saç gözlük ve kaşlar farklı yönde görünmesine neden olabilir. Threshold uygulanır ki gürültüyü azaltabilmek için görüntüdeki. Maksimum değerler göz bebeğini kullanmada kullanılır.

Implementasyon'da ki işlem aynı template eşleşme algoritmasındaki gibidir. Bundan sonra bir fonksiyon ile gözler çerçve içine alınır. Bu etapta minMaxLoc() fonksiyonu ile maksimum nokta bulunur ve o nokta göz bebeğinin merkezi olarak seçilir.

Koordinatların verilmesi ile kullanıcı ekrana baktığında gözün ekran ile arasındaki mesafe bulunur ve boyutu hesaplanır şekil 5.8'deki gibi.



Şekil 5.8: Gözün Ekran ile Arasındaki Mesafesi

Ekranın dört köşeside belirlenir ve göz bunu hafızada tutar. Herhangi bir etkinlik ve değişiklikte otomatik olarak göz bu alana bakıyor olacaktır ve değişikliği görmektedir. Ekran boyutu tekrar boyutlandırılabilir.

5.7. Kalibrasyon

Kalibrasyon işlemi gözler tarafından bir öznenin geometrik özelliklerinin tam olarak özelleştirilmiş ve doğru bir bakış açısı ile hesaplanması için olan bir süreçtir. Göz takibi işleminin kaydı başlamadan önce kullanıcı kalibrasyon prosedürü için alınır. Bu prosedür boyunca göz takibini gerçekleştiren aygıt kullanıcının gözlerinin karakteristik olarak 3D göz modelini hesaplar. Bu işlem gaze verileriyle sağlanır. Bu model şeklini, kırılmayı ve ışığın kırılmasının bir diğer göz açısından detaylarını içerir. Kalibrasyon boyunca kullanıcı belli bir noktaya bakması istenir ekranda. Aynı zamanda bu işlem kalibrasyon noktaları olarak bilinmektedir. Bu işlem boyunca birden çok görüntü alınır ve gözün bilgileri tutularak analiz edilir. Sonuç bilgisi entegre edilir göz modeline ve her görüntünün bakış açısı hesaplanır. Prosedür bittiğinde kalibrasyon kalitesi değişik uzunluktaki yeşil çizgilerle gösterilir. Her bir çizginin uzunluğu kalibrasyon noktasının merkezi arasındaki offset'i temsil eder. Büyük offset'ler belli bir noktaya bakarken dikkat dağınıklığına neden olabililir veya eye tracker doğru kurulmamış olabilir. Ayrıca kullanıcı kalibrasyon sırasında başını sabit tutamayabilir. Kalibrasyon işlemi sırasında hem açık hemde koyu göz bebeği metotları test edilir ki az olan ortam ışığına uyumlu olabilmesi için. Kullanıcın göz karakteri önemlidir.

Şekil 5.9: Kalibrasyon Testi Örneği

5.8. Özet

Göz bebeği segmentasyonu ve kullanıcı bileşenleriyle başarılı bir entegre oluşur. Kullanıcılar kendi parolasını belirleyebilir be kimlik doğrulaması ile eye gaze ile minimum geribildirim yapılır arayüze. Çoklu faktör kullanılarak akıllı cep telefonlarının güvenlik açıkları azaltılmış ve daha güvenli hale getirilmiş olur biyolojik parolama desteğiyle. Gaze estimasyonu webcam kullanıldığında ortam ışığı probleminden ötürü bazı zorluklar ortaya çıkar. Bu zorluğun dışında gelişmiş olan uygulamada Bu zorluğa rağmen, geliştirilen uygulama başarıyla gözbebeğinin segmentasyon algoritması ve bakış gaze estimasyonu ile kullanıcının bakış açısını etkileşim ortamı olarak kullanıp kimlik doğrulamasına izin verir. Arka planda da görüntü kirlilikleri azaltarak ve görüntünün işlenmesiyle ilerleyen adımlarda da kimlik doğrulama teknolojisi kullanılarak bu teknoloji ileri boyutlara taşınabilir.

6. ÖNERİLER

Kimlik doğrulama işlemine göz gaze özelliği uygulanarak akıllı telefonların güvenliği arttırılmıştır. Kullanıcı bu işleme başladığında ilk olarak cep telefonunun ön kamerasından kullanıcının yüzünün görüntüsü yakalanır. Bu görüntüde yüz ve gözün konumu teslim edilmiş olur. Ardından göz bebeklerinin yerleri tespit edilir. Sonra kullanıcının gaze'i tespit edilir ve morfolojik segmentasyon algoritması ile. Kimlik doğrulama uygulaması cep telefonunda çalışır durumdayken karşısına renkli bloklar gelir ve burada kullanıcı gözleriyle belirlediği parolama ne ise ona göre şekil çizer ve işlemi başlatır aynı zamanda dijital parola da girerek. Input olarak girildiği anda parola, işlem otomatik olarak başlar. Bu işlemin başarısı aynı zamanda ortam ışığına bağlıdır. Aynı zamanda sonuca bakıldığında çözünürlüğün büyük bir önemi vardır. Doğal ışık etkiyi azaltmaktadır irisin tespiti yapıldığı anda. Laptoplarda gaze tabanlı kimlik doğrulama uygulandığında ise sonuç cep telefonlarına oranla daha başarılıdır. Çünkü laptoplarda ki web cam çözünürlüğü daha yüksektir.

Kimlik doğrulama uygulaması mobil dünyasında zorlayıcı alternatif bir parola modeli deneyimi sunmaktadır. 3rd parti kullanıcılara uygulama belirsiz bir feedback yollar. Göz takibi sayesinde mobil-kullanıcı arasında interaktif bir algoritma vardır. Android dünyasındaki dizayn onaylanmıştır ve gerçek zamanlı tespit yapılır yüz özelliklerine dair Haar cascade ile. Gözün merkezi tespit edilir ve görüntü işleme tekniği ile göz bebeği extract edilir. Bu ölçümler sayesinde gaze point tahmin edilir. Otomatik düzeltme metodu ihtiyaç duyulur. Bunun nedenleri de; ortam ışığı, gölgeler, kullanıcının başının pozisyonu, aygıt hareketi ve göz rengidir. Bütün bu faktörler gaze estimation'nın performansını etkileyen faktörlerdir. Bu sorunlar doğal sebepler olarak sonuçlandırılmıştır. Ek olarak giyilebilen teknolojilerde bu alanda gelişmektedir. Levi's ilk teknolojik kot ceketini icat etmiştir.

Kalibrasyonun ana fikri, göz orta noktasını piksel olarak almaktı ve kullanıcının bakışına göre ekranına dikdörtgen ölçek oluşturulur. Ayrıca, Timm ve Barth algoritması ile göz bebeklerinin merkezinin bulunmasıyla vektörler tanımlanır ve her pikseldeki göz bebeği merkezini daha öncekinden farklı piksellerde algılar. Bunun nedeni, algoritmanın merkez olarak uygun bulabileceği diğer olası merkezlerde bu algoritmada açıklanmıştır. Başka bir sorun ise başın hareketi. Her ne kadar cihaz ve kafa sabit olsa da, yüzü yakınlaştırdıkça kafanın sallandığı görülür ve bu sorun piksel pozisyonunun değişmesine neden olmaktadır. Yüz tanıma işlemi sırasında sabit bir konumda durulmalı. Sonuç olarak kalibrasyon uygulanabilir değil.

Pikseller üzerindeki bu sapmalar, sonuçta beklenen dikdörtgenin çökmesine veya hatta farklı yönlenmesine neden olabilir. Sonucunda düzensiz şekiller ve belki üçgenler ortaya çıkabilir.

Tezde ki asıl amaç akıllı telefonlarında göz takibini kullanarak ve retina ile tanımayı uygulayarak güvenliği arttırmaktır. Haar cascade sınıflandırmasıyla bu hedef gerçekleştirilir. İki gözün de merkezinin takip edilmesi ve belirlenmesi ile çerçeveler yerleştirilir. Template eşleşme algoritması ve Timm ve Barth algoritması uygulanır. Kalibrasyon tespit sırasında bazen başarılı olamayabiliyor. Göz bebeklerinin küçük olmasından kaynaklı. Algoritmalar az sayıda pikseller tarafından yürütülmekte. Sonuç olarak kalibrasyon işlemi gözün boyutunun küçük olduğundan ötürü başarısız olabilmektedir. Başarılı olabilmesi için daha büyük ekranlar kullanılmalıdır. Küçük ekranlı cihazlardan uzak durulmalı bu hatadan kaçınılmak için. Daha geniş açı her zaman daha iyi sonuç verir.

Gelecekte daha farklı olarak farklı açılardan göz takibi yapılabilir. İleride geliştirilecek algoritmalar ile dar açılardan bile başarılı sonuçlar elde edilip göz bebeği tespitleri yapılabilir. Kullanıcının başının 3 boyutlu modeli çıkarılabilir. Sadece kullanıcı suratından ziyade tüm resim extract edilebilir ve daha detaylı araştırmalar yapılabilir. Kıvrımların hesaplamaları da hesaplanabilir. Böylece aktif kullancının tarama sonucu sistem tarafından yanıltılmamış olur. Daha iyi bir performans için. Günümüzün ilerleyen teknoloji sayesinde insanlar araçlarının kapısını da multi factör parola ile anahtarlarına ihtiyaç duymadan açabilirler.

6.1. İris Taraması

İristeki patternler eşsizdir ve sanal olarak kopyası elde edilemez. Bunun anlamı iris kimlik doğrulama işlemi, en güvenli yollardan biridir telefonunuzun ekranını kilitlemektir istediğinizde.

Sadece göz takibi ile akıllı telefonlarımızı kilitlemek aslında çok yeteri değildir. Hazır bir resim çıktısı ile bu aldatılabilir ya da kafanızı biraz sağa veya sola çevirdiğinizde karşılaşacağınız sorun ekran kilidinizi başarılı bir şekilde açamayacağınız bir durum olacaktır. Bu tür sorunlar hem güvenlik açığıdır hem de gün içerisinde vakit kaybına neden olacaktır. Aynı zamanda Eye Locking ile gözlük kullananlar problem yaşayabilir. Aynı zamanda, gün ışığı da büyük bir dezavantajdır.

Son teknoloji göz izleme özelliği, yakın kızıl ötesi spektrum ışığını algılayan ve aynı zamanda bu spektrumdaki aktif aydınlatmadan faydalanan yüksek performanslı endüstri

kameralarını kullanır. Bu özellikler, göz takibi için son derece hassas bir sistem oluşturmak için birlikte çalışır.

6.2 İris Taraması İçin Gerekli Donanım

6.2.1 Kızılötesi Gücü

Tipik göz takip cihazı, her türlü ışık koşulunda göz hareketini yakalamak için tasarlanmış ve optimize edilmiştir ve kafa hareketini, göz bölgesinin geniş kapsamlı fizyolojik varyasyonunu telafi edebilen özel bir kamera donanımının parçasıdır.

Şekil 6.1: Kızıl Ötesi

Web cam göz izleme;

Başlamak için, web kamerası göz izleme esas olarak, gözle görülebilir spektrumdaki ışığı algılayan normal bir kamera kameradan göz izleme verileri almak anlamına gelir. Bunun nedeni, sadece görünür spektrum ışığı ile çalışan bir web kamerasına gerçekten ihtiyaç duymamız ya da istememizdir. Yakın kızıl ötesi spektrum ışığında video konferansı ilginç bir deneyim olabilir.

Görsel spektrum, çözünürlük ve kontrast;

Web kameraları veya tüketici uygulama kameraları görsel spektrum için ayarlanmıştır ve bu bazı sınırlamalar getirmişlerdir:

• Sadece görsel spektrum: yakın kızıl ötesi spektrum ışığından yarar sağlama (algoritmanın gözbebeğini çevreleyen ve irise karşı doğru şekilde algılamasını sağlar). Göz, muhtemelen hem gözbebeği hem de iristen oluşan büyük bir bulanıklık olarak görünecektir.

• Çözünürlük: Tipik bir web kamerası maksimum HD kayıt yapabilir. Ancak genellikle gecikme ve kare hızında bir farklılık kaydedebilir. Daha düşük bir çözünürlük bunu çözebilir. Daha az pikselin bulunması sonuçta daha az doğruluk ve güvenilirlik demektir.

• Kontrast: web kamerasının tamamen ortam ışığına bağlı olması nedeniyle, gözün hareketlerini yüzün arka planına karşı daha az kontrast olduğundan, düşük ışıklandırma daha az hassasiyetle sonuçlanabilir.

6.3 İris Taramasında Sağlık Sorunlarının Etkisi

Göz takibi ile kilitleme, iris taramasına geçilmeli. Bunun nedenleri ise aşağıdaki sağlık sorunlarından ötürüdür;

Lazer göz ameliyatı olacak olan kişi iris taramasında gözümü tanıtabilecek midir?

- Lazer destekli göz ameliyatı geçirdiyseniz, gözdeki ışığın yansıması, korneadaki değişiklikten dolayı değişecektir. Bunun için gözünüzü tekrar taratmanız gerekmektedir.

Gözlerde bir sağlık problem varsa, iris scanner hala çalışır mı?

- Göz hastalıkları ciddi şekilde şişmediği sürece, göz hastalıklarından ötürü scanner etkilenmez.

Son teknoloji göz izleme özelliği, yakın kızıl ötesi spektrum ışığını algılayan ve aynı zamanda bu spektrumdaki aktif aydınlatmadan faydalanan yüksek performanslı endüstri kameralarını kullanır. Bu özellikler, göz takibi için son derece hassas bir sistem oluşturmak için birlikte çalışır.

6.4. Göz Takibi Tabanlı Webcam'in Artıları Ve Eksileri

Artıları:

- Ucuz webcam le çalışır.
- Bir çok insan kitlesine hitap edebilir.
- Evde kurulabilir ve test edeilebilir.

Eksileri:

- Düşük ortaama kalitesi göz takibine oranla.
- Hareket sırasında hassas oluşu,
- Düşük çözünürlük ve frame.

- Düşük ışıkta yeterli performan gösteremez.

Bunun artısı her yerde göz takibi yapma ortamını sağlar. Gömülü kameralara sahip tüm cihazların destekleyebileceği bir teknolojidir. Bu günlerde neredeyse tüm kişisel bilgisayarlar ve mobil cihazlarda kamera mevcuttur.

Ancak, olumsuzluklar, araştırmanın türünün ve kalitesinin, web kamerası kullanımı ile ciddi şekilde sınırlı olduğunu göstermektedir. Dahası, araştırma kullanılan araçların kalitesini yansıtmaktadır. Bu da web kamerası tabanlı yöntemlerin gözden geçirilmesinin mümkün olmadığı anlamına gelmektedir.

6.5. İris Taraması Hakkında Yapılan Açıklamalar

Ne Samsung ne de Apple, kendi iris tekniğiyle ilgili söylentileri doğrulamamıştır. Apple'ın kaynakları, şirketin 2014 yılında iris taramasını araştırdığını ve KGI güvenlik analisti Ming-Chi Kuo'nun Mart ayında Apple'ın 2017 iPhone modelinin yüz tanıma teknolojisini kullanabileceğini öngördüğünü bildirdi. Şirket, artan doğruluk için 3D render'e dayanan bir yüz tanıma sistemi de dahil olmak üzere, bu teknolojiyi içeren bir dizi patente sahiptir.

Çoğu akıllı telefon, bu özelliği eklemek için ek donanım gerektirmez, daha doğrusu mevcut ön yüz kameralarını kullanabilir ve iris taraması için bir algoritma oluşturulmuştur. İris tanıma sistemi, görüntü sinyalini yakalamak için üç lens kullanır ve daha sonra üretilen görüntüye bağlı olarak kullanıcının irisini kontrol eder.

Bank of America, JPMorgan Chase ve Wells Fargo bankalarındaki milyonlarca müşteri artık kendi hesaplarını cep telefonları aracılığıyla girişlerini için parmak izlerini okutarak yapabilmektedirler. Wells Fargo ayrıca bazı müşterilerin kurumsal hesaplara giriş yapmak için gözlerini telefon kameralarıyla taramasına izin veriyor. Jain, özellikle tanımanın parmak izi ile daha doğru olduğunu ve popülerlik kazandığını belirtti. Bununla birlikte, kimlik doğrulama için iris taramalarını kullanan mevcut teknolojilrede vardır. Tipik olarak kontak veya gözlük takan kişilerle, değişen ışık koşullarıyla ve kameranın doğru konumlandırılmasıyla ilgili sorunlarla karşılaşırlar. Ancak Litan, bu sorunun zamanla çözüleceğini belirtti.

6.5.1.Sistem İhlallerinden Kaçınmak

Biyometrik sistemler elbette kusursuz değildir: Bilgisayar korsanları, biyometrik bir sahtekarlık ya da bir sistemi erişimin sağlanmasına kandırabilen bir tool (silikondan yapılmış bir parmak izi kalıbı gibi) oluşturabilir. Satıcılar, kişinin göz kırpması, gözdeki kan akışını ölçmesi veya tarih ve saati okumak için sesli kimlik doğrulamasını kullanmak gibi, canlılığı kontrol etmek için farklı teknikler kullanabilir. Litan, bununla birlikte, bu önlemlerin teknik bir kitlesel ölçekte ortaya çıkana kadar ne kadar doğru olduğunu kanıtlamanın zor olacağını belirtmiştir.

Bu sistemler bir başkasının kimliğine bürünmeyi zorlaştırırken, bir başka kişinin adı altında kendi irislerini veya parmak izlerini kaydettirebilmek için güçlü bir kayıt işlemine sahip olmaları gerekir. Bu, Apple Pay için önemli bir sorundu. Güvenlik sistemleri güçlü iken, suçlular başka bir kişi olarak kaydolabilirlerdi.

Sonuç olarak, teoride birisinin telefonunuza fiziksel erişimi varsa, tek ihtiyacınız olan şey, telefonunuzun kilidini açmak için bir fotoğrafınızdır. Bu yüzden iris taraması daha güvenli bir yöntemdir. Çünkü daha fazla veri noktasını okur ve depolar, bu da teknolojiyi aldatmayı zorlaştırır.

Business Insider hikayesine göre, parmak izi teknolojisi 13 referans noktası kullanıyor. Bir iris taraması, 200 referans noktasına kadar gidebilir. bunun anlamı sadece telefonunuzun kilidini açmak için 400 referans noktası vardır.

6.6. Eye Gesture

Mobil teknoloji hızla büyüyor, akıllı telefon, özel kullanıcı verilerini iletmek, hassas kurumsal dosyaları depolamak ve güvenli ödeme işlemleri yapmak için kaçınılmaz hale geldi. Ancak akıllı telefonlar, kimliği doğrulanmamış erişime karşı son derece savunmasızdır EyeVeri, akıllı telefon güvenlik koruması için yeni bir göz hareketi tabanlı kimlik doğrulama sistemi. Son zamanlarda akıllı telefon çok yaygın hale geldi. Dünyada kullanılan 1,5 milyardan fazla akıllı telefon vardır.

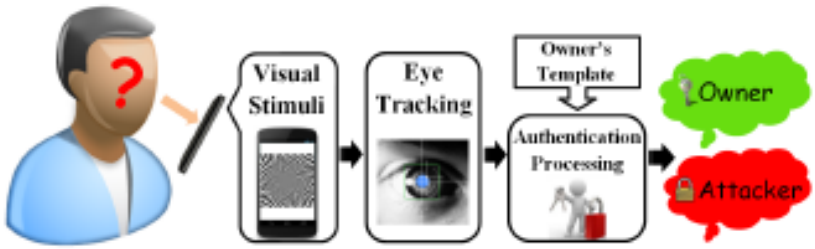
6.6.1 Akıllı Telefonlar İçin Kimlik Doğrulama Methodları Ve Eye Gesture

- Parmak okuyucu
- Pass-Code
- Yüz tanıma
- Konuşma analizi
- Iris taraması

Hassas noktaları;

Örneğin, birileri fotoğrafını çekerken veya parmaklarını gösterdiğinde, insanlar başka bir yüksek çözünürlüklü kamera kullanarak parmak izini basabiliyorlar. Potansiyel risk, bu biyo-özelliklerin çoğunun elde edilebileceği veya çoğaltılabileceğidir.

Göz hareketi, istemli ve istemsiz hareket olarak kategorize edilebilir.



Şekil 6.2: Eye Gesture Kimlik Doğrulaması

6.7. Eye Gesture Avantajları

1- Güvenli

2- Benzersiz

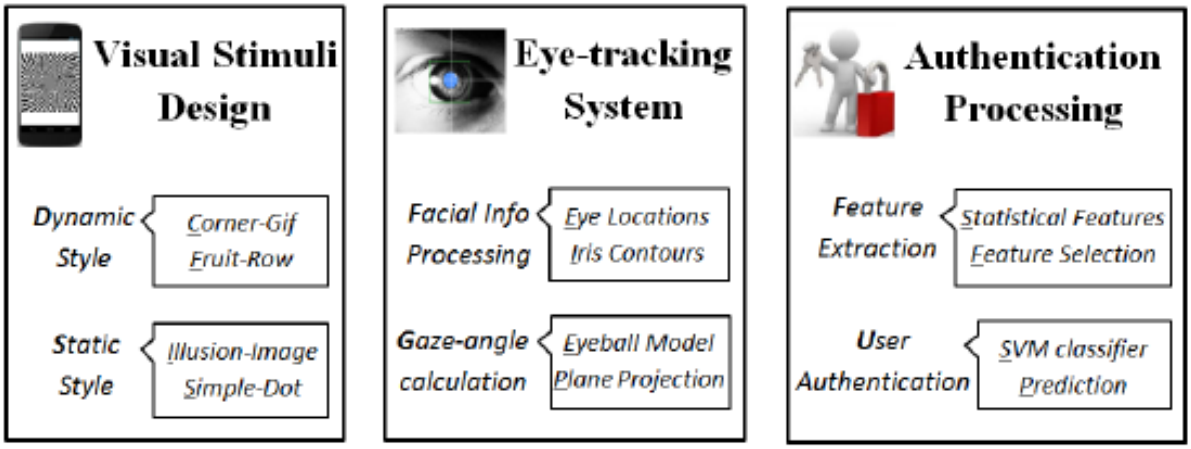
3- Değişmez (sabit)

Göz doğrulama sistemi, bir kimlik doğrulama yaklaşımı olarak bazı avantajları vardır;

- Eşsiz: Ekstraoküler biyoyapı ve göz hareketi davranışlarının yüksek oranda bireysel bağımlılıklarını uyarır;

- Sabit: Uzun vadeli çalışmada görüldüğü gibi, fizibilitesini artıran oldukça istikrarlı bir performans elde eder.

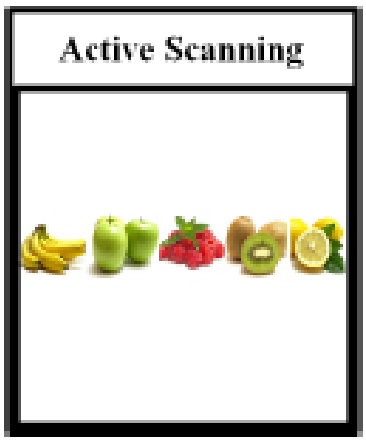
6.7.1. Framework Modülleri



Şekil 6.3: Framework Modülleri

Birisi akıllı telefona erişmeyi denediğinde, önceden tasarlanmış görsel uyaranlar ekranda gösterilir. Platform arka planda çalışan göz izleme sistemi, aynı anda nesnenin göz hareketini yakalar ve odak noktasının konum bilgisini kaydeder. Kullanıcının verileri kaydedildikten sonra, verilerden belirli özellikler çıkarılır. Ardından önceden depolanmış sahip şablonunu temel alan bir sınıflandırıcı, kullanıcının gerçek sahibi olup olmadığını belirlemek için gelen verileri işler.

Fruit-Row(FR)



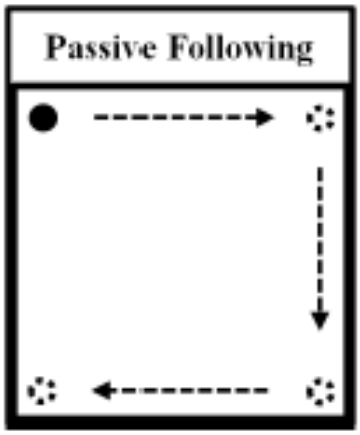
(a) Fruit-Row (FR);

Şekil 6.4: Fruit Row (FR)

FR bir satırda bir meyve dizisi içerir ve özne kendi sırasına göre soldan sağa doğru sırayla tarar.

Corner-Gif(CG)

CG, bir siyah çemberin dört köşeden saat yönünde döndüğü bir gif içerir. Konu, kimlik doğrulama işlemi sırasında siyah daireyi tam olarak takip etmelidir.

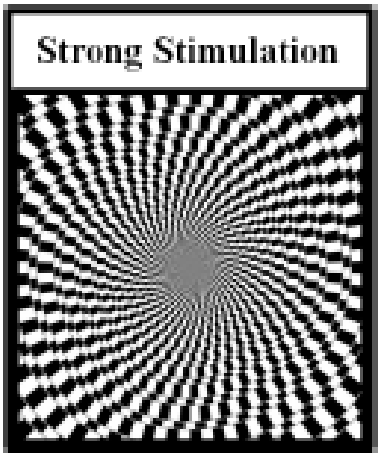


(b) Corner-Gif (CG);

Şekil 6.5: Corner Gif (CG)

Illusion-Image (II)

Göz küresinin bilinçsiz titreşimini kuvvetle uyaran tipik bir illusion görüntüsüdür.

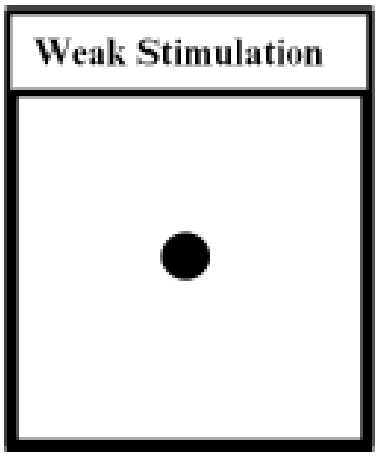


(c) Illusion-Image (II);

Şekil 6.6: Illusion Image (II)

Simple-Dot(SD)

SD ekranın ortasına yerleştirilmiş basit bir noktaya sahiptir ve kişi ayrıca işlem sırasında noktaya bakmalıdır. Bu uyaranları izlerken kişi, yüz ve akıllı telefonun pozisyonuna göre baş hareketini minimumda tutmalıdır.



(d) Simple-Dot (SD).

Şekil 6.7: Simple Dot (SD)

Kimlik Doğrulama İşlemi

1- Özellik Çıkarımı;
   - Fizyolojik Bilgi
   - Davranışsal Bilgi
2- Kimlik Doğrulama Algoritması

Bakış verileri toplandıktan sonra, kimlik doğrulama işlemi kullanıcının yasal sahip olup olmadığını doğrulamak için yapılır.

Fizyolojik ve davranışsal bilgiler içeren bir dizi göz hareketi özellikleri önerir ve geliştirir.

7. SONUÇ

7.1 Giriş

Bu bölümde akıllı telefon kullanan insanlara yönelik oluşturulmuş anket sorularının değerlendirilmesi ve sonuçları yer almaktadır. Elde edilerin bilgiler analiz edilmiştir. Analiz edilen sonuçlar ile kullanıcıların hangi ekran kilidi parolalarını tercih ettiklerinin sonuçları belirtilmiştir.

7.2 Tanımlayıcı İstatistikler

Bu bölümde tanımlayıcı istatistikler ortaya konulmaktadır. Anket ortalama olarak 50 kişiye sorulmuş olup, hedef kitlenin seçimi ise tekneolojiyi yakından takip eden genç kitle olarak belirlenmiştir. Bunun dışında ek olarak aynı şirkette olup farklı departmanlarda çalışan insanlarda bu anket sorularını yanıtlamışlardır.

Ankete katılan kişilerin ilgili oldukları departmanlar;

- IT
- Marketing
- Human Resources

Yukarıdaki depatmanlarda çalışan kişilerin hepsi üniversite mezunu olmakla birlikte aralarında yüksek lisans yapmış olanlarda bulunmaktadır.

Cinsiyet:

İdeal bir araştırma için yüzde 50'lik bir ayrım olması gerekmektedir ve araştırmada mümkün oldukça kadın ve erkek sayısı eşitleniştir. Amaç doğru bir istatistik ortaya çıkarmaktır.

Yaş:

Yaş unsuru sorulan sorular arasında en önemli yerini korumaktadır. Bunun nedeni, genç kitlenin okur yazar oranın yüksek olması ve teknolojiyi yakından takip etmeleri verilen cevaplarda büyük bir önem taşımaktadır. Genç olan hedef kitle günümüzün gelişen teknolojisini yakından takip etmektedirler ve kullandıkları teknolojinin eksiklerini saptayarak bunların geliştirilmesini talep etmektedir. Buna bağlı olarak her zaman yapılan testlerde hedef kitlenin

büyük ölçüsü genç kitle olmaktadır. Büyük firmaların ürünleri satışa çıkarmadan önce yaptıkları tesler ve deneyimlerin sonuçları genelde 14-35 yaş arası olarak belirtilmiştir.

Okur Yazarlık Oranı:

Ankete katılan kişilerin eğitim seviyeleri minimum üniversite seviyesidir. Bu kriter sayesinde kullanıcıların verdikleri yanıtların ne kadar güvenilir ve kendilerine özgün oldukları anlaşılmaktadır.

Kullanılmış ve Kullanılmakta Olan Cep Telefonu Modelleri:

Yapılan anket sonuçlarına göre çalışanlar ikiye ayrılmaktadır. Bunlar; android ve IOS'tur. Günümüzde de bu iki işletim sistemi çok popüler ve öne çıkmaktadır. Anket sonucuna bakıldığında hemen hemen bütün kullanıcılar yarı yarı olmak üzere eşit bir dağılım gözlenmektedir.

7.3 Anket Soruları ve Analiz Tablo Sonuçları

Akıllı telefonlarda parola tercihiyle ilgili 46 kişiyle yapılan ankette katılımcılara cinsiyet, yaş, eğitim, çalıştığı departman, bilgisayar bilgi düzeyi, telefonunun işletim sistemi (önceki ve şuan) ve kullanılan parolanın tercih sebebi olmak üzere 8 adet bağımsız değişken sorusu ile daha önce ve şuan telefonunda kullandığı parola olmak üzere 2 adet bağımlı değişken sorusu sorulmuştur. Katılımcıların kullandığı parolaların güvenlik düzeylerinin katılımcıların cinsiyetine, yaşına, eğitim durumuna, çalıştığı departmana, bilgisayar bilgisi düzeyine, telefonunda kullandığı işletim sistemine ve Kullanılan parolanın tercih sebebine göre değişip değişmediği ölçülmüştür. Bağımlı ve bağımsız değişkenlere ilişkin detayların yer aldığı tablolar (Tablo 7.1-7.10) aşağıda gösterilmiştir [19].

Katılımcıların 16 tanesi kadın, 30 tanesi erkektir. Kadın katılımcıların oranı %35 iken, erkek katılımcıların oranı %65'tir.

Değişken	Türü	Kategoriler	Sayı	Yüzde
Cinsiyet	Nominal	Kadın	16	0,35
		Erkek	30	0,65

Tablo 7.1: Cinsiyet

Katılımcıların 22 tanesi 25 yaşın altındayken 17 tanesi 25 ile 35 yaşları arasında, 7 tanesi ise 35 yaşından büyüktür. 25 yaş altı katılımcıların sayısı %48, 25 ile 35 yaş arası

katılımcıların sayısı %37, 35 yaş üstü katılımcıların sayısı ise %15'tir. Katılımcıların %85'inin 35 yaşın altında olduğu yani genç bir katılımcı kitlesiyle anket yapıldığı görülmüştür.

Değişken	Türü	Kategoriler	Sayı	Yüzde
Yaş	Ordinal (Sıralı)	<25 yaş	22	0,48
		25-35 yaş	17	0,37
		>35 yaş	7	0,15

Tablo 7.2: Yaş

Değişken	Türü	Kategoriler	Sayı	Yüzde
Eğitim	Ordinal (Sıralı)	Lisans	39	0,85
		Lisansüstü	7	0,15

Tablo 7.3: Eğitim

Değişken	Türü	Kategoriler	Sayı	Yüzde
Departman	Nominal	Sigorta	7	0,18
		Denetim	7	0,17
		IT	25	0,62
		Pazarlama	7	0,03

Tablo 7.4: Departman

Değişken	Türü	Kategoriler	Sayı	Yüzde
Bilgisayar Bilgisi	Ordinal (Sıralı)	Orta	10	0,22
		İyi	15	0,32
		Yüksek	21	0,46

Tablo 7.5: Bilgisayar Bilgisi

Değişken	Türü	Kategoriler	Sayı	Yüzde
İşletim Sistemi (Önceki)	Nominal	Android	20	0,43
		IOS	26	0,57

Tablo 7.6: İşletim Sistemi (Önceki)

Değişken	Türü	Kategoriler	Sayı	Yüzde
İşletim Sistemi (Şuan)	Nominal	Android	15	0,33
		IOS	31	0,67

Tablo 7.7: İşletim Sistemi (Şuan)

Değişken	Türü	Kategoriler	Sayı	Yüzde
Şifre		Kolaylık	22	0,25
Tercih	Nominal	Güvenlik	15	0,47
Sebebi		Kolaylık + Güvenlik	9	0,28

Tablo 7.8: Parola Tercih Sebebi

Değişken	Türü	Kategoriler	Sayı	Yüzde
Kullandığı Şifre (Önceki)	Ordinal	Hiçbiri	14	0,31
		Şifre	19	0,41
		Parmak İzi	13	0,28
		Parmak İzi +Şifre		

Tablo 7.9: Kullandığı Parola (Önceki)

Değişken	Türü	Kategoriler	Sayı	Yüzde
Kullandığı Şifre (Şuan)	Ordinal	Hiçbiri	5	0,11
		Şifre	10	0,22
		Parmak İzi	8	0,17
		Parmak İzi +Şifre	23	0,50

Tablo 7.10: Kullandığı Parola (Şuan)

2 kategorili nominal değişkenlerle, 2 veya daha fazla kategorili ordinal değişkenlerin testinde Mann-Whitney-U; 2'den fazla kategorili nominal değişkenlerle, 2 veya daha fazla kategorili ordinal değişkenlerin testinde Kruskall-Wallis ve 2 veya daha fazla kategorili ordinal değişkenlerle yine 2 veya daha fazla kategorili ordinal değişkenlerin testinde Jonckheere-Terpstra testi kullanılmalıdır (Çilan, 2009). Analiz edilen değişken tiplerine uygun testler SPSS 20. kullanılarak analiz edilmiştir. Analiz sonucunda elde edilen bulgular aşağıdaki gibidir.

7.3.1 Nominal Ve Ordinal Ataması

Cinsiyet, çalışılan departman bilgisi, önceki ve şuan ki telefon bilgisi, şuanda kullanılan güvenlik yönteminin nedeni ve gelecekte kullanılmak istenilen parolama yöntemi nominal olarak belirlenmiştir analizler yapılırken.

Yaş bilgisi, eğitim seviyesi, bilgisayar bilgi seviyesi, akıllı telefonlarda şu anda kullanılmakta olan güvenlik yöntemi ve bir önce ki telefonda kullanılan güvenlik yöntemi ise ordinal olarak belirlenmiştir.

7.4 Test Sonuçları

SPSS ile veri analizleri yapılmış olup aşağıdaki sonuçlar elde edilmiştir.

Test Statistics[a]

	ekran_kilidi_once
Mann-Whitney U	204.000
Wilcoxon W	340.000
Z	-.958
Asymp. Sig. (2-tailed)	.338

a. Grouping Variable: Cinsiyet

Test Statistics[a]

	ekran_kilidi_suan
Mann-Whitney U	182.000
Wilcoxon W	318.000
Z	-1.444
Asymp. Sig. (2-tailed)	.149

a. Grouping Variable: Cinsiyet

Tablo 7.11: Test Statistics Cinsiyet

Jonckheere-Terpstra Test[a]

	ekran_kilidi_once
Number of Levels in yas	3
N	46
Observed J-T Statistic	371.500
Mean J-T Statistic	323.500
Std. Deviation of J-T Statistic	41.668
Std. J-T Statistic	1.152
Asymp. Sig. (2-tailed)	.249

a. Grouping Variable: yas

Jonckheere-Terpstra Test[a]

	ekran_kilidi_suan
Number of Levels in yas	3
N	46
Observed J-T Statistic	359.500
Mean J-T Statistic	323.500
Std. Deviation of J-T Statistic	44.561
Std. J-T Statistic	.808
Asymp. Sig. (2-tailed)	.419

a. Grouping Variable: yas

Tablo 7.12: Jonckheere-Terpstra Test Yaş

Jonckheere-Terpstra Test[a]

	ekran_kilidi_once
Number of Levels in egitim	2
N	46
Observed J-T Statistic	201.000
Mean J-T Statistic	136.500
Std. Deviation of J-T Statistic	28.337
Std. J-T Statistic	2.276
Asymp. Sig. (2-tailed)	.023

a. Grouping Variable: egitim

Jonckheere-Terpstra Test[a]

	ekran_kilidi_suan
Number of Levels in egitim	2
N	46
Observed J-T Statistic	160.500
Mean J-T Statistic	136.500
Std. Deviation of J-T Statistic	30.299
Std. J-T Statistic	.792
Asymp. Sig. (2-tailed)	.428

a. Grouping Variable: egitim

Tablo 7.13: Jonckheere-Terpstra Eğitim

Test Statistics[a,b]

	ekran_kilidi_once
Chi-Square	.070
Df	3
Asymp. Sig.	.995

a. Kruskal Wallis Test

b. Grouping Variable: departman

Test Statistics[a,b]

	ekran_kilidi_suan
Chi-Square	.416
df	3
Asymp. Sig.	.937

a. Kruskal Wallis Test

b. Grouping Variable: departman

Jonckheere-Terpstra Test[a]

	ekran_kilidi_once
Number of Levels in bilgisayar_bilgisi	3
N	46
Observed J-T Statistic	394.000
Mean J-T Statistic	337.500
Std. Deviation of J-T Statistic	42.245
Std. J-T Statistic	1.337
Asymp. Sig. (2-tailed)	.181

a. Grouping Variable: bilgisayar_bilgisi

Jonckheere-Terpstra Test[a]

	ekran_kilidi_suan
Number of Levels in bilgisayar_bilgisi	3
N	46
Observed J-T Statistic	371.500
Mean J-T Statistic	337.500
Std. Deviation of J-T Statistic	45.180
Std. J-T Statistic	.753
Asymp. Sig. (2-tailed)	.452

a. Grouping Variable: bilgisayar_bilgisi

Tablo 7.14: Test Statistics ve Jonckheere-Terpstra Test Bilgisayar Bilgisi

Test Statistics[a]

	ekran_kilidi_once
Mann-Whitney U	138.500
Wilcoxon W	348.500
Z	-3.107
Asymp. Sig. (2-tailed)	.002

a. Grouping Variable: İşletim_Sistemi_once

Test Statistics[a]

	ekran_kilidi_suan
Mann-Whitney U	176.000
Wilcoxon W	386.000
Z	-2.009
Asymp. Sig. (2-tailed)	.045

a. Grouping Variable: isletim_sistemi_once

Tablo 7.15: Test Statistics İşletim Sistemi Önce

Ranks

isletim_sistemi_once		N	Mean Rank	Sum of Ranks
ekran_kilidi_once	android	20	17.43	348.50
	IOS	26	28.17	732.50
	Total	46		

Tablo 7.16: Ranks

Test Statistics[a]

	ekran_kilidi_once
Mann-Whitney U	156.500
Wilcoxon W	261.500
Z	-1.859
Asymp. Sig. (2-tailed)	.063

a. Grouping Variable: isletim_sistemi_suan

Test Statistics[a]

	ekran_kilidi_suan
Mann-Whitney U	85.500
Wilcoxon W	190.500
Z	-3.568
Asymp. Sig. (2-tailed)	.000

a. Grouping Variable: isletim_sistemi_suan

Tablo 7.17: Test Statistics İşletim Sistemi Şuan

Ranks

isletim_sistemi_suan		N	Mean Rank	Sum of Ranks
ekran_kilidi_suan	android	14	13.61	190.50
	IOS	32	27.83	890.50
	Total	46		

Tablo 7.18: Ranks

Test Statistics[a,b]

	ekran_kilidi_once
Chi-Square	6.509
df	2
Asymp. Sig.	.039

a. Kruskal Wallis Test

b. Grouping Variable: sifre_tercihi

Ranks

sifre_tercihi		N	Mean Rank
ekran_kilidi_once	kolaylık	22	23.30
	güvenlik	15	19.00
	kolaylık+güvenlik	9	31.50
	Total	46	

Tablo 7.19: Test Statistics Şifre Tercihi ve Ranks

Test Statistics[a,b]

	ekran_kilidi_suan
Chi-Square	7.461
df	2
Asymp. Sig.	.024

a. Kruskal Wallis Test

b. Grouping Variable: sifre_tercihi

Tablo 7.20: Test Statistics Şifre Tercihi

Ranks

sifre_tercihi		N	Mean Rank
ekran_kilidi_suan	kolaylık	22	19.05
	güvenlik	15	24.77
	kolaylık+güvenlik	9	32.28
	Total	46	

Tablo 7.21: Şifre Tercihi Ranks

Test Statistics[a,b]

	ekran_kilidi_once
Chi-Square	2.512
df	3
Asymp. Sig.	.473

a. Kruskal Wallis Test

b. Grouping Variable: gelecek_sifre

Test Statistics[a,b]

	ekran_kilidi_suan
Chi-Square	1.065
df	3
Asymp. Sig.	.786

a. Kruskal Wallis Test

b. Grouping Variable: gelecek_sifre

Tablo 7.22: Kruskal Wallis Test ve Gelecek Şifre

Jonckheere-Terpstra Test[a]

	ekran_kilidi_suan
Number of Levels in ekran_kilidi_once	3
N	46
Observed J-T Statistic	401.000
Mean J-T Statistic	284.500
Std. Deviation of J-T Statistic	42.206
Std. J-T Statistic	2.760
Asymp. Sig. (2-tailed)	.006

a. Grouping Variable: Ekran_Kilidi_Once

Tablo 7.23: Jonckheere-Terpstra Test[a] Ekran Kilidi Önce

7.4.1 Mann-Whıtney-U Analizi

Test Statistics[a]		
ekran_kilidi_once	Cinsiyet	isletim_sistemi_suan
Mann-Whitney U	204.000	156.500
Wilcoxon W	340.000	261.500
Z	-.958	-1.859
Asymp. Sig. (2-tailed)	.338	.063

ekran_kilidi_şuan	Cinsiyet	isletim_sistemi_suan
Mann-Whitney U	176.000	85.500
Wilcoxon W	386.000	190.500
Z	-2.009	-3.568
Asymp. Sig. (2-tailed)	.045	.000

Tablo 7.24: Mann Whitney-U Analizi

7.4.2 Kruskall-Wallıs Analizi

Test Statistics[a,b]			
	ekran_kilidi_once	ekran_kilidi_once	ekran_kilidi_once
Chi-Square	.070	6.509	2.512
df	3	2	3
Asymp. Sig.	.995	.039	.473
a. Kruskal Wallis Test			
b. Grouping Variable: departman			

Test Statistics[a,b]			
	ekran_kilidi_suan	ekran_kilidi_suan	ekran_kilidi_suan
Chi-Square	.416	7.461	1.065
df	3	2	3
Asymp. Sig.	.937	.024	.786
a. Kruskal Wallis Test			
b. Grouping Variable: departman			

Tablo 7.25: Kruskall-Wallis Analizi

7.4.3 Johnckere-Terspra Analizi

Jonckheere-Terpstra Test[a]

	ekran_kilidi_once
Number of Levels in egitim	2
N	46
Observed J-T Statistic	201.000
Mean J-T Statistic	136.500
Std. Deviation of J-T Statistic	28.337
Std. J-T Statistic	2.276
Asymp. Sig. (2-tailed)	.023
a. Grouping Variable: Egitim	

Jonckheere-Terpstra Test[a]

	ekran_kilidi_once
Number of Levels in bilgisayar_bilgisi	3
N	46
Observed J-T Statistic	394.000
Mean J-T Statistic	337.500
Std. Deviation of J-T Statistic	42.245
Std. J-T Statistic	1.337
Asymp. Sig. (2-tailed)	.181
a. Grouping Variable: Bilgisayar_Bilgisi	

Tablo 7.26: Jonckheere-Terpstra Test Eğitim ve Bilgisayar Bilgisi

7.5 SONUÇ VE ÖNERİLER

Mann-Whitney-U Test Sonuçları

2 kategorili nominal değişkenlerle, 2 veya daha fazla kategorili ordinal değişkenlerin testinde Mann-Whitney-U testi kullanılır. Bu durumda daha önce ve şuan kullanılan ekran kilidinin 2 kategorili olan "Telefonda Kullanılan İşletim Sistemi" ve "Cinsiyet"e göre farklılık gösterip göstermediği test edilmiştir. Tablo.11'de görüleceği üzere daha önce kullanılan ekran kilidi cinsiyete göre *(Z=-,958, p=0,338)* farklılaşmazken, kullanılan işletim sistemine göre *(Z=-3,107, p=0,002)* farklılaşmaktadır. Veriye bakıldığı zaman IOS kullanıcılarının Android kullanıcılarına göre daha güçlü şifreler kullandığı görülmüştür.

Ekran_Kilidi_Once	İsletim_Sistemi_Once	Cinsiyet
Mann-Whitney U	138,500	204,000
Wilcoxon W	348,500	340,000
Z	-3,107	-,958
Asymp. Sig. (2-tailed)	**,002**	,338

Tablo 7.27: Önceki Ekran Kilidi İçin Mann Whitney U Test Sonuçları

Tablo 7.27'de görüleceği üzere daha önce kullanılan ekran kilidi cinsiyete göre *(Z=-1,444, p=0,149)* farklılaşmazken, kullanılan işletim sistemine göre *(Z=-3,568, p=0,000)* farklılaşmaktadır. Veriye bakıldığı zaman IOS kullanıcılarının Android kullanıcılarına göre daha güçlü şifreler kullandığı görülmüştür.

Ekran_Kilidi_Şuan	Cinsiyet	İsletim_Sistemi_Suan
Mann-Whitney U	182,000	85,500
Wilcoxon W	318,000	190,500
Z	-1,444	-3,568
Asymp. Sig. (2-tailed)	,149	**,000**

Tablo 7.28: Şu anki Ekran Kilidi İçin Mann-Whitney-U Test Sonuçları

Kruskall-Wallis Test Sonuçları

2'den fazla kategorili nominal değişkenlerle, 2 veya daha fazla kategorili ordinal değişkenlerin testinde Kruskall-Wallis testi kullanılır. Bu durumda daha önce ve şuan kullanılan ekran kilidinin 2'den fazla kategorili olan "Çalıştığı Departman" ve "Kullandığı Şifre Tercihinin Sebebi" ve "Gelecekte İçin Hayal Ettiği Şifre"ye göre farklılık gösterip göstermediği

test edilmiştir. Tablo 7.28'de görüleceği üzere şu an kullanılan ekran kilidi Departman *(*Chi-Square *=0,416, p=0,937)* ve Gelecekteki Şifre Tercihine göre *(*Chi-Square *=1,065, p=0,786)* farklılaşmazken, Şifre Tercih Sebebine göre *(*Chi-Square *=7,461, p=0,024)* farklılaşmaktadır. Veriye bakıldığı zaman şifre tercih sebebi kolaylık + güvenlik olanların sadece güvenlik olanlara göre, güvenlik olanların da kolaylık olanlara göre daha güçlü şifreler kullandığı görülmüştür.

Ekran_Kilidi_Suan	Departman	Şifre Tercihi	Gelecekte Şifre
Chi-Square	,416	7,461	1,065
df	3	2	3
Asymp. Sig.	,937	**,024**	,786

Tablo 7.29: Şu Anki Ekran Kilidi İçin Kruskall-Wallis Test Sonuçları

Tablo 7.29'de görüleceği üzere daha önce kullanılan ekran kilidi Departman *(*Chi-Square *=0,070, p=0,995)* ve Gelecekteki Şifre Tercihine göre *(*Chi-Square *=2,512, p=0,473)* farklılaşmazken, Şifre Tercih Sebebine göre *(*Chi-Square *=6,509, p=0,039)* farklılaşmaktadır. Veriye bakıldığı zaman şifre tercih sebebi kolaylık + güvenlik olanların sadece kolaylık olanlara göre, kolaylık olanların da güvenlik olanlara göre daha güçlü şifreler kullandığı görülmüştür.

Ekran_Kilidi_Once	Departman	Şifre Tercih Sebebi	Gelecekte Şifre
Chi-Square	,070	6,509	2,512
df	3	2	3
Asymp. Sig.	,995	**,039**	,473

Tablo 7.30: Önceki Ekran Kilidi İçin Kruskall-Wallis Test Sonuçları

Johnckere-Terspra Test Sonuçları

2 veya daha fazla kategorili ordinal (sıralı) değişkenlerle yine 2 veya daha fazla kategorili ordinal değişkenlerin testinde Johnckere-Terspra testi kullanılır. Bu durumda daha önce ve şuan kullanılan ekran kilidinin Yaşa, Eğitime ve Bilgisayar Bilgisine göre farklılık gösterip göstermediği test edilmiştir. Tablo 7.31'de görüleceği üzere şu an kullanılan ekran kilidi Yaş *(*J-T *=359,500, p=0,419)*, Eğitim *(*J-T *=160,500, p=0,428)* ve Bilgisayar Bilgisi *(*J-T *=371,500, p=0,452)* gruplarından hiçbiri için farklılaşmamaktadır. Bu durumda kullanılan ekran kilidinin kullanıcıların yaşına, aldıkları eğitime veya sahip oldukları bilgisayar bilgisi düzeyine göre farklılık göstermediği görülür.

Ekran_Kilidi_Once	Yaş	Eğitim	Bilgisayar Bilgisi
Number of Levels in yas	3	2	3
N	46	46	46
Observed J-T Statistic	359,500	160,500	371,500
Mean J-T Statistic	323,500	136,500	337,500
Std. Deviation of J-T Statistic	44,561	30,299	45,180
Std. J-T Statistic	,808	,792	,753
Asymp. Sig. (2-tailed)	,419	,428	,452

Tablo 7.31: Şu anki Ekran Kilidi Johnckere-Terspra Test Sonuçları

Tablo 7.32'de ise şu an kullanılan ekran kilidinin Yaş, Eğitim ve Bilgisayar Bilgisi gruplarına göre farklılık gösterip göstermediğine dair test sonuçları görülebilir. Şu an kullanılan ekran kilidinin sadece eğitim gruplarına göre *(J-T =201,000, p=0,023)* farklılık gösterdiği, yaş *(J-T =371,500, p=0,249)* ve bilgisayar bilgisi gruplarına göre *(J-T =394,000, p=0,181)* farklılık göstermediği görülür. Bu durumda eğitim düzeyi arttıkça daha önce kullanılan ekran kilidinin güvenlik seviyesinin de arttığı söylenebilir. Kullanıcıların şu an kullanılan ekran kilitleri için eğitim düzeyleri farklılık göstermezken daha önce kullandıkları şifreler için farklılık göstermesi, kullanılan şifrelerin artık eğitim düzeyinden bağımsız hale geldiği yorumu yapılabilir. Yani eskiden kullanıcıların eğitim düzeyi arttıkça kullandıkları şifreler daha güvenli hale gelmekteyken, şuan eğitim düzeyleri farketmeksizin daha güvenli veya daha az güvenli şifreler kullanabilmekteler.

Ekran_Kilidi_Once	Yaş	Eğitim	Bilgisayar Bilgisi
Number of Levels in yas	3	2	3
N	46	46	46
Observed J-T Statistic	371,500	201,000	394,000
Mean J-T Statistic	323,500	136,500	337,500
Std. Deviation of J-T Statistic	41,668	28,337	42,245
Std. J-T Statistic	1,152	2,276	1,337
Asymp. Sig. (2-tailed)	,249	**,023**	,181

Tablo 7.32: Önceki Ekran Kilidi Johnckere-Terspra Test Sonuçları

Sonuç olarak 46 kişide yapılan anket sonuçlarına göre, genç ve eğitim seviyesi yüksek olan bir kitle hedef alınmıştır. Kullanıcıların yanıtlarından elde edilen cinsiyet, yaş, eğitim seviyesi, departman bilgisi, bilgisayar bilgi seviyesi ve kullandıkları şuan ki ve önceki cep telefonlarının işletim sistemleri bilgilerine dayanılarak belli sonuçlar elde edilmiştir. Bu sonuçlara dayanılarak IOS işletim sistemini kullanan kullanıcıların Android işletim sistemini kullanan kullanıcılara oranla daha güçlü parolalar kullandıkları sonuçlar elde edilmiştir. Bu sonuç Mann Whitney-U testinin sonucuna dayanılarak elde edilmiştir. Kullanıcıların önceki telefonlarıyla şu anki telefonları karşılaştırıldığında IOS kullananların sayısı artmıştır.

Android işletim sistemine sahip akıllı telefonların bazılarında ekran kilitleme zorunluluğu bulunmamaktadır. Bu sebepten ötürü bazı kullanıcılar ekran kilitleme özelliğini seçmemektedirler. Bu durum güvenlik açığıdır. Bu sonuca dayanarak IOS işletim sistemini kullanan kullanıcılarda parola zorunluluğu olduğundan ötürü daha IOS işletim sisteminin kullanılması daha güvenlidir.

Araştırma sonucuna göre eye tracking yöntemi büyük oranda kullanıcıların gelecekte kullanmayı tercih ettikleri bir yöntem olarak ortaya çıkmıştır. Eye tracking ile IOS ve Android işletim sistemli telefonlarda daha güçlü bir şifreleme yöntemi olarak geliştirilebilir ve kullanıcıların sonuçlarına dayanarak bu yöntemin ileride daha çok kullanılabileceğ sonucu ortaya çıkarılır.

KAYNAKLAR

[1] Technavio, Technavio's Tech Tuesday: Eye Tracking Is One of the Hottest Things in Tech Right Now, https://www.technavio.com/blog/technavios-tech-tuesday-eye-tracking-one-hottest-things-tech-right-now, 13 Kasım 2017

[2] Sigut, J., & Sidha, S. A. (2011). Iris center corneal reflection method for gaze tracking using visible light. *IEEE Transactions on Biomedical Engineering*, *58*(2), 411-419.14/10/2010. ISSN 0018-9294. doi: 10.1109/TBME.2010.2087330

[3] Duchowski, A. T. (2007). Eye tracking methodology. *Theory and practice*, *328*.

[4] Cristinacce, D., Cootes, T. F., & Scott, I. M. (2004, September). A multi-stage approach to facial feature detection. In *BMVC* (Vol. 1, pp. 277-286). [5] Asteriadis, S., Nikolaidis, N., Hajdu, A., & Pitas, I. (2006, March). An eye detection algorithm using pixel to edge information. In *Int. Symp. on Control, Commun. and Sign. Proc*.

[5] Asteriadis, S., Nikolaidis, N., Hajdu, A., & Pitas, I. (2006, March). An eye detection algorithm using pixel to edge information. In *Int. Symp. on Control, Commun. and Sign. Proc*.

[6] Türkan, M., Pardas, M., & Cetin, A. E. (2007, March). Human eye localization using edge projections. In *VISAPP (1)* (pp. 410-415). [7] Valenti, R., & Gevers, T. (2008). Accurate eye center location and tracking using isophote curvature.

[7] Valenti, R., & Gevers, T. (2008). Accurate eye center location and tracking using isophote curvature.

[8] Timm, F., & Barth, E. (2011). Accurate Eye Centre Localisation by Means of Gradients. *Visapp*, *11*, 125-130.

[9] Kothari, R., & Mitchell, J. L. (1996, September). Detection of eye locations in unconstrained visual images. In *Image Processing, 1996. Proceedings., International Conference on*(Vol. 3, pp. 519-522). IEEE.

[10] Rouse, M. (2015). What is single-factor authentication (SFA) - Definition from WhatIs.com. Retrieved from http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA

[11] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S. J., & Sanyal, S. (2011). A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. *arXiv preprint arXiv:1111.3010*.

[12] Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems*, *22*(8), 1390-1397.

[13] Fan, C. I., & Lin, Y. H. (2009). Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. *IEEE Transactions on Information Forensics and Security*, *4*(4), 933.

[14] Millán, M. S., Pérez-Cabré, E., & Javidi, B. (2006). Multifactor authentication reinforces optical security. *Optics letters*, *31*(6), 721-723.

[15] Florian.alt, Gaze Authentication, http://www.florian-alt.org/academic/project/gaze-based-authentication/, 15 Ocak 2018

[16] Rouse, M. , What is single-factor authentication (SFA)? http://searchsecurity.techtarget.com/definition/single-factor-authentication-SFA, 15 Ocak 2018

[17] Ajna, R. , Training Haar Cascades https://memememememememe.me/post/training-haar-cascades/, 17 Ocak 2018

[18] Dhanachandra, N., Manglem, K., & Chanu, Y. J. (2015). Image segmentation using K-means clustering algorithm and subtractive clustering algorithm. *Procedia Computer Science*, *54*, 764-771.

[19] Çilan, Ç. A. (2009). *Sosyal bilimlerde kategorik verilerle ilişki analizi*. Pegem Akademi.

ÖZGEÇMİŞ

11 Kasım 1992 tarihli İstanbul İli FATİH ilçesi doğumluyum. İlk ve orta okulu Oğuzkaan Kolejinin de okuduktan sonra ve liseyi BAKIRKÖY ilçesinde bulunan Florya Final Okullarında tamamladıktan sonra 2011 yılında Beykent Üniversitesi Bilgisayar Mühendisliği bölümüne kaydoldum. Bu bölümden 2016 yılında mezun olduktan sonra da Beykent Üniversitesinde Bilgisayar Mühendisliği yüksek lisansına başladım. Ardından 2017 yılında PriceWaterhouse Coopers firmasında işe başladım ve şuan System&Network departmaında System Administarator olarak çalışmaktayım.

Miray İREN