KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ
MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
BİTİRME PROJESİ TEZİ

YÜZ TANIMA GÜVENLİK SİSTEMLERİ: GELECEĞİN GÜVENLİK TEKNOLOJİSİ-THEEYE_THEDENİZHAN

HASAN DENİZHAN-20110131815

DR.ÖĞR.ÜYESİ PELİN CANBAY

HAZİRAN 2024

YÜZ TANIMA GÜVENLİK SİSTEMLERİ: GELECEĞİN GÜVENLİK TEKNOLOJİSİ-THEEYE_THEDENİZHAN

(Bitirme Projesi Tezi)
HASAN DENİZHAN
KAHRAMANMARAŞ SÜTÇÜ İMAM ÜNİVERSİTESİ
MÜHENDİSLİK VE MİMARLIK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ
HAZİRAN 2024

ÖZET

TheEye-TheDenizhan projesi, ev sahibinin güvenliğini artırmak amacıyla geliştirilen bir yüz tanıma tabanlı erişim kontrol sistemini içermektedir. Bu proje, kapıdaki zil butonu aracılığıyla gelen misafirleri tanıyarak, ev sahibine bilgi ileten bir mekanizmayı içerir. İşte projenin temel özellikleri:

Projede, OpenCV'nin haarcascade modeli ve LBPH yüz tanıma algoritması kullanılarak yüz tanıma modülü oluşturulmuştur. Kullanıcıların yüzleri, veritabanında depolanmak üzere bir ID ile eşleştirilir. Veritabanı, OpenCV ve PIL kütüphaneleriyle oluşturulur.

Erişim kontrol mekanizması, Ardunio ile entegre edilmiş bir sistemdir. Zil butonu, kapıdaki kişinin kimliğini tanıma talebini başlatır. Ardunio, bu talep üzerine zil çalar, kameralı yüz tanıma işlemini başlatır ve tanıma sonucuna göre kapıyı açar veya ev sahibine bilgi gönderir.

Projede ayrıca yabancı algılama ve bildirim sistemi bulunmaktadır. Tanınmayan bir kişi algılandığında, OpenCV kullanılarak yüz tanıma işlemi gerçekleştirilir ve ilk olarak Telegram API aracılığıyla ev sahibine anında bildirim gönderen bir bot tasarlanmıştır. Daha sonrasında KivyMD kullanılarak mobil bir uygulama tasarlanmıştır. Bu uygulamayla birlikte kullanıcıya kapıyı anlık görme, kapıyla anlık konuşabilme, kapıyı açma, alarm çalabilme, fotoğraf çekebilme, sisteme kayıt yapabilme imkânları bulunur.

Python ve Ardunio arasındaki seri haberleşme kullanılarak veri iletimi sağlanmıştır. Ayrıca, yüz tanıma modelinin güncellenmesi ve eğitimi için bir mekanizma bulunmaktadır. Proje, ev sahibine daha fazla güvenlik ve kontrol sağlamak adına geliştirilmiş olup, yüz tanıma teknolojisi, ardunio ile donanım entegrasyonu, bildirim sistemleri ve veri tabanı yönetimini içerir.

TEŞEKKÜR

Sayın Dr.Öğr.Üyesi PELİN CANBAY, size projemizdeki mükemmel rehberliğiniz ve yaptığınız yönlendirmeler için içten teşekkürlerimi iletmek istiyorum. Sizin bilgeliğiniz, deneyiminiz ve samimiyetiniz, projemizin gelişiminde kritik bir rol oynadı.

Proje sürecinde gösterdiğiniz destek ve rehberlik için size tekrar teşekkür etmek isterim. Sizinle çalışmak benim için bir ayrıcalık ve öğrenme dolu bir deneyimdi. Umarım gelecekte de sizinle birlikte çalışma fırsatı bulabilirim.

Anahtar Kelimeler	:	Yüz Tanıma, Erişim Kontrolü, OpenCV, Ardunio, Tkinder, Güvenlik, Veritabanı Yönetimi, Mobil, Anlık Konuşma, KivyMD.
Sayfa Adedi	:	Toplam sayfa sayısı
Danışman	:	Dr.Öğr.Üyesi PELİN CANBAY

İÇİNDEKİLER:

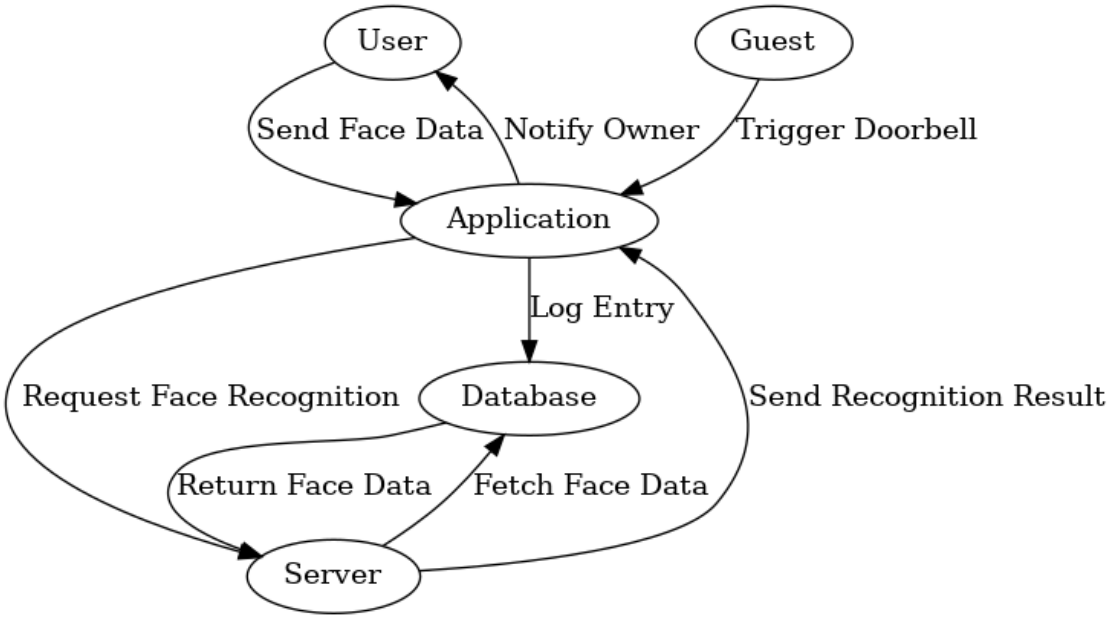
ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

1. GİRİŞ

Ev güvenliği, teknoloji ve yeniliklerle sürekli gelişen bir alandır. Geleneksel güvenlik yöntemleri, anahtarlar ve kapı kilitleri gibi temel araçlarla sınırlıyken, modern çağda bu araçlar teknolojik çözümlerle desteklenmektedir. Özellikle biyometrik güvenlik sistemleri, ev güvenliğinde devrim niteliğinde değişiklikler yapmaktadır. Bu bağlamda yüz tanıma teknolojisi, güvenlik endüstrisinde hızla yaygınlaşan ve önemli bir yer edinen yenilikçi bir çözüm olarak öne çıkmaktadır.

Aşağıda verilen şekil 1'de verilen görselde projenin iş akış diagramım verilmiştir. Bu diagrama göre kullanıcı ve misafirler uygulama üzerinden birbirleriyle haberleşebilirler. Uygulama server ve veritabanıyla eş zamanlı haberleşip kullanıcılara ve misafirlere bilgi gönderebilir. Sistem tam senkron bir şekilde çalışabilmektedir.



Şekil 1 TheEye Projesi İş Diagramı

1.1. Yüz Tanıma Teknolojisi ve Ev Güvenliği:

Yüz tanıma teknolojisi, kişinin yüz özelliklerini analiz ederek kimlik doğrulama işlemlerini gerçekleştirir. Bu teknoloji, güvenlik amaçlı kullanımlarda bireyin yüzünü tarayarak benzersiz biyometrik veriler oluşturur ve bu verileri kullanarak kişinin kimliğini belirler. Geleneksel anahtar kullanımına kıyasla yüz tanıma, daha yüksek güvenlik ve kullanım kolaylığı sağlar. Artık kullanıcılar, anahtar aramak veya şifre hatırlamak zorunda kalmadan, sadece yüzlerini taratarak kapılarını açabilirler. Bu, özellikle güvenlik risklerini minimize etmek ve kullanıcı deneyimini iyileştirmek için önemli bir avantaj sunar.

1.2. Uzaktan Tanıma ve Bildirim Sistemi:

Yüz tanıma teknolojisinin sunduğu bir diğer önemli avantaj, uzaktan tanıma ve bildirim sistemleridir. Ev sahipleri, kapılarının önünde kimin olduğunu anında öğrenebilir ve gerekli önlemleri alabilir. Bu sistemler, kapıya gelen kişiyi otomatik olarak tanımlayarak, ev sahibine anlık bildirim gönderir. Bu sayede ev sahipleri, evde olmadıklarında bile kapılarına gelen kişileri izleyebilir ve gerektiğinde müdahale edebilirler. Uzaktan tanıma ve bildirim sistemleri, güvenlik kameraları ve mobil uygulamalarla entegre çalışarak, ev güvenliğini her an her yerden kontrol etme imkanı sunar.

1.3. **Sonuç:**

Yüz tanıma teknolojisi, ev güvenliğinde yeni bir dönemin kapılarını açmaktadır. Geleneksel güvenlik yöntemlerini aşan bu yenilik, kullanıcı dostu özellikleri ve yüksek güvenlik standartları ile dikkat çekmektedir. Kapıdaki kişinin kimliğini hızlı ve doğru bir şekilde belirleyerek, ev sahiplerine daha konforlu ve güvenli bir yaşam tarzı sunar. Bu teknolojik ilerleme, günlük hayatımızı kolaylaştırmanın yanı sıra ev güvenliği konusunda da önemli bir adımı temsil etmektedir.

Bu tezde, yüz tanıma teknolojisinin ev güvenliğindeki uygulamaları ve avantajları detaylı bir şekilde incelenecektir. Ayrıca, bu teknolojinin kullanımıyla ilgili etik ve güvenlik konularına da değinilecektir. Proje kapsamında geliştirilen TheEye-TheDenizhan yüz tanıma güvenlik sistemi, bu yeni teknolojinin pratik bir örneği olarak ele alınacak ve tüm aşamalarıyla açıklanacaktır.

2. LİTERATÜR ÖZETİ

2.1. TheEye Projesi: Yüz Tanıma Temelli Ev Güvenlik Sistemi

Ev güvenliği, günümüzde önemli bir endişe kaynağıdır. TheEye projesi, yüz tanıma teknolojisi üzerine kurulu bir ev güvenlik sistemi olup, ev sahiplerine kapıdaki kişileri tanıma ve güvenli bir şekilde evlerine giriş kontrolü sağlama imkanı sunar.

2.1.1. Proje Aşamaları:

2.1.1.1. Yüz Tanıma Modülü:

OpenCV'nin haarcascade model dosyaları üzerinden yapılan değerlendirmeler sonucunda "haarcascade_frontalface_default" modeli tercih edilmiştir.

Yüz tanıma için LBPH (Local Binary Patterns Histograms) algoritması kullanılmıştır. Bu algoritma, görüntülerin özelliklerini vurgulayarak yüz tanıma sürecini hızlı ve güvenilir hale getirir.

2.1.1.2. Veritabanı Oluşturma:

OpenCV kullanılarak bilgisayar kamerasından alınan verilerle kişilerin tanımlandığı bir veritabanı oluşturulmuştur. Her kişi için ad, ID numarası ve kaydedilen veri sayısı gibi bilgiler kaydedilmiştir. Kullanıcılara göre sisteme kayıt yapabilmeleri için SQLite veritabanı kullanılmıştır. Görseller ve isimler veritabanında string bir biçimde tutulmaktadır.

2.1.1.3. Erişim Kontrol Mekanizması

Zil butonu, Tkinter kütüphanesiyle entegre edilerek ziyaretçilerin bildirim göndermeleri sağlanmıştır.

Arduino kodları ve sistemle entegrasyonu ile ziyaretçilere görsel ve işitsel sinyallerle cevap verilmiştir.

2.1.1.4. Yabancı Algılama ve Bildirim Sistemi:

Python ile oluşturulan sayfa, toplanan veriler üzerinden yapay zeka algoritmalarını eğitmek ve sistem güvenilirliğini artırmak amacıyla kullanılmıştır. Başlangıçta telegram API kullanılarak, belirlenen durumlar için kullanıcıya bildirim gönderme sistemi entegre edilmiştir. Daha sonrasında KivyMD kullanılarak mobil bir uygulama tasarlanmıştır.

2.1.1.5. İzleme ve Konuşma:

Başlangıçta ziyaretçilerin algılanması sonrasında Telegram üzerinden kullanıcıya bilgi verme ve izleme işlemleri gerçekleştirilmiştir. Daha sonrasında bu işlem mobil

uygulama üzerinden anlık canlı yayına verilen görüntü ve istendiğinde kapıdaki insanla konuşma olarak geliştirilmiştir.

2.1.1.6. Güvenlik ve Yasal Uyum:

Proje, güvenlik açısından sürekli güncellenmekte ve dış kaynaklardan kaynaklanan tehditleri minimize etmek üzere tasarlanmıştır.

Siber güvenlik standartlarına uygun bir şekilde güçlü güvenlik politikaları benimsemektedir.

2.1.1.7. Sonuç:

TheEye projesi, yüz tanıma teknolojisinin ev güvenliği konseptine başarıyla entegre edildiği bir sistemdir. Bu proje, ev sahiplerine güvenli ve etkili bir giriş kontrolü sağlamak için çağdaş teknolojileri kullanmaktadır.

2.2. Diğer Projeler:

Yüz tanıma teknolojisi, ev güvenliği dışında birçok alanda da yaygın olarak kullanılmaktadır. Farklı projelerde çeşitli yöntemler ve algoritmalar kullanılarak yüz tanıma sistemlerinin etkinliği artırılmaya çalışılmıştır. Örneğin:

- **HomeGuard Projesi:** Bu projede, ev güvenliği için yüz tanıma teknolojisi ile birlikte hareket algılama sensörleri kullanılmıştır. Sistem, kapıya yaklaşan kişilerin yüzlerini tanımlarken aynı zamanda hareketlerini de izlemekte ve şüpheli durumları anında ev sahibine bildirmektedir. Bu projede kullanılan HOG (Histogram of Oriented Gradients) ve SVM (Support Vector Machine) algoritmaları, yüz tanımanın yanı sıra hareket analizi de yapabilmektedir.
- **SafeHome Projesi:** SafeHome, yüz tanıma teknolojisi ile birlikte biyometrik verilerin korunmasına yönelik güçlü şifreleme teknikleri kullanmaktadır. Bu projede, yüz tanıma algoritması olarak CNN (Convolutional Neural Networks) tercih edilmiştir. Yüz verileri, bulut tabanlı bir veritabanında saklanmakta ve şifreleme algoritmaları ile korunmaktadır. Sistem, yüz tanıma işlemi tamamlandıktan sonra verileri güvenli bir şekilde ileterek kullanıcının gizliliğini sağlamaktadır.
- **SecureEntry Projesi:** Bu projede, yüz tanıma teknolojisi ile birlikte RFID (Radyo Frekansı ile Tanımlama) kullanılarak çift faktörlü kimlik doğrulama sağlanmıştır. Yüz tanıma işlemi başarılı olduktan sonra, kullanıcıdan bir RFID kartı göstermesi istenmekte ve böylece güvenlik seviyesi artırılmaktadır. Bu projede, Dlib kütüphanesi ve CNN tabanlı yüz tanıma algoritmaları kullanılmıştır.

2.3. TheEye Projesi ile Diğer Projeler Arasındaki Farklılıklar:

TheEye projesi, yüz tanıma temelli ev güvenlik sistemleri arasında yenilikçi özellikleri ile öne çıkmaktadır. İşte TheEye projesi ile diğer projeler arasındaki bazı temel farklılıklar:

Kullanılan Algoritmalar ve Teknolojiler: TheEye projesi, LBPH (Local Binary Patterns Histograms) algoritmasını kullanarak yüz tanıma sürecini hızlı ve güvenilir hale getirmektedir. Diğer projelerde ise HOG+SVM, CNN gibi farklı algoritmalar tercih edilmiştir. TheEye projesi, ayrıca OpenCV ve haarcascade modellerini kullanarak yüz algılama ve tanıma süreçlerini optimize etmektedir.

Bildirim ve İzleme Sistemleri: TheEye projesi, Telegram API ve KivyMD ile entegre mobil uygulama kullanarak kullanıcılara anlık bildirimler göndermekte ve canlı izleme imkanı sunmaktadır. Diğer projelerde ise genellikle bildirim ve izleme sistemleri farklı yöntemlerle sağlanmakta olup, mobil uygulama entegrasyonu her projede bulunmamaktadır.

Erişim Kontrol Mekanizmaları: TheEye projesinde, zil butonu ve Arduino entegrasyonu ile ziyaretçilerin bildirim göndermeleri ve görsel-işitsel sinyallerle cevap almaları sağlanmıştır. Diğer projeler ise RFID, hareket sensörleri gibi ek erişim kontrol yöntemleri kullanmaktadır.

Güvenlik ve Yasal Uyum: TheEye projesi, siber güvenlik standartlarına uygun güçlü güvenlik politikaları benimsemekte ve sürekli güncellemelerle dış kaynaklı tehditleri minimize etmektedir. Diğer projelerde de güvenlik ve yasal uyum ön planda tutulmakta, ancak kullanılan yöntemler ve politikalar projeden projeye farklılık gösterebilmektedir.

Sonuç olarak, TheEye projesi, ev güvenliği için yüz tanıma teknolojisinin yenilikçi bir şekilde kullanıldığı bir sistemdir. Diğer projelerle karşılaştırıldığında, TheEye projesi, kullanıcı dostu arayüzü, anlık bildirim sistemi ve güvenilir yüz tanıma algoritması ile öne çıkmaktadır. Bu projeler arasındaki farklılıklar, her birinin kendine özgü avantajlarını ve dezavantajlarını ortaya koymakta ve yüz tanıma temelli güvenlik sistemlerinin çeşitli alanlardaki potansiyel kullanımını gözler önüne sermektedir.

3. Malzeme ve Metotlar:

3.1. Yüz Tanıma Modülü:

Malzeme:

- OpenCV kütüphanesi
- Haarcascade model dosyaları (haarcascade_frontalface_default vb.)

Metot:

- Haarcascade modelleri değerlendirilerek en uygun olan seçilmiştir.
- Yüz tanıma için LBPH algoritması kullanılmıştır.

3.2. Veritabanı Oluşturma:

Malzeme:

- Bilgisayar kamerası
- OpenCV kütüphanesi
- SQLite

Metot:

- OpenCV ile kişilerin yüzleri kaydedilerek veritabanı oluşturulmuştur.
- Her kişi için ad, ID numarası gibi tanımlayıcı bilgiler kaydedilmiştir.
- Her bir kullanıcının sisteme kayıtlı olan bilgilerini kaydetmek için SQLite kullanılmıştır.

3.3. Erişim Kontrol Mekanizması:

Malzeme:

- Tkinter kütüphanesi (zil butonu entegrasyonu)
- Arduino (kırmızı ve yeşil lambalar, buzzer, pinler)

Metot:

- Tkinter ile zil butonu,mesaj bırakma butonu, kapı açma butonu, mesaj dinleme butonu oluşturularak, kapıdaki insana kolay ve sade bir panel sunulmuştur.
- Arduino kullanılarak kırmızı ve yeşil lambalar, buzzer entegre edilmiş ve belirlenen durumlar için görsel ve işitsel sinyaller oluşturulmuştur.

3.4. Yabancı Algılama ve Bildirim Sistemi:

Malzeme:

- Python
- OpenCV
- KivyMD

Metot:

- Python ile yapay zeka algoritmalarını eğitmek ve veritabanını oluşturmak için OpenCV kullanılmıştır.
- Kapıdaki kişiyi yada olayı görebilmek için KivyMD kullanarak bir uygulama tasarlanılmıştır

3.5. Mesaj Gönderme ve İzleme:

Malzeme:

- KivyMD
- Flask

Metot:

- KivyMD kullanarak bir uygulama tasarlanmıştır, bu uygulama kullanıcıların kapıdaki kişiyi yada olayları görebilmesine kapıdaki olayları kaydedebilmesine olanak tanır.

3.6. Güvenlik ve Yasal Uyum:

Malzeme:

- Güncellenebilir yazılım altyapısı
- Güçlü şifreleme yöntemleri

Metot:

- Yazılım sürekli güncellenerek güvenlik açıkları kapatılmıştır.
- Bot tokeni güvenli bir şekilde saklanmış ve erişim kontrolü sıkı bir şekilde yönetilmiştir.
- Proje, güçlü güvenlik politikaları benimseyerek siber güvenlik standartlarına uygun olarak tasarlanmıştır.

4. Yüz Tanıma Güvenlik Sistemleri: Geleceğin Güvenlik Teknolojisi

Günümüzde, güvenlik alanındaki hızlı değişim ve gelişmeler, teknolojinin güvenlik konseptlerine entegrasyonunu kaçınılmaz kılmıştır. Bu bağlamda, yüz tanıma teknolojisi, son yıllarda güvenlik endüstrisinde öne çıkan ve radikal bir dönüşüm getiren bir yenilik olarak öne çıkmaktadır. Yüz tanıma sistemleri, bireylerin yüz özelliklerini algılayarak kimlik doğrulama ve erişim kontrolü sağlama amacı güder. Bu teknoloji, geleneksel güvenlik yöntemlerini aşan ve özellikle büyük ölçekli tesisler, iş yerleri ve kamusal alanlar için etkili bir güvenlik çözümü sunan bir paradigmaya dönüşmüştür.

4.1. Yüz Tanıma Sisteminin Avantajları:

4.1.1. Güvenilirlik ve Doğruluk:

Yüz tanıma, diğer biyometrik güvenlik yöntemlerine göre genellikle daha güvenilir ve doğru sonuçlar sağlar. Yüz özellikleri genetik olarak belirlenir ve yaşla değişmez, bu nedenle uzun vadeli bir tanıma için güvenilirdir.

4.1.2. Hız ve Kolaylık:

Yüz tanıma işlemi oldukça hızlı gerçekleşir. Bir kişinin yüzünü tanımak için sadece birkaç saniye sürebilir. Diğer geleneksel kimlik doğrulama yöntemlerine kıyasla daha hızlı ve kullanıcı dostudur.

Şekil 2 Örnek bir yüz tanıma

4.1.3. Kullanıcı Dostu ve Kolay Entegrasyon:

Yüz tanıma, kullanıcıların kimliklerini doğrulamak için herhangi bir fiziksel temas gerektirmez. Bu, kullanıcılar için rahat ve kullanıcı dostu bir deneyim sunar. Ayrıca, mevcut güvenlik sistemlerine kolayca entegre edilebilir.

4.1.4. Çeşitli Uygulama Alanları:

Yüz tanıma teknolojisi, sadece güvenlik sistemleriyle sınırlı değildir. Havaalanları, bankalar, oteller, ofis binaları, cep telefonları ve sosyal medya platformları gibi birçok farklı sektörde kullanılabilir.

4.1.5. Kayıpları ve Unutkanlığı Azaltır:

Kart kaybı veya unutma gibi sorunlarla baş etme ihtiyacı ortadan kalkar. Kişinin yüzü, her zaman yanında taşıdığı bir kart gibi doğal bir kimlik taşıyıcısıdır.

4.1.6. Toplum Güvenliği ve Suç Önleme:

Yüz tanıma sistemleri, kamusal alanlarda kullanılarak kayıp kişileri veya suçluları tespit etme konusunda polis teşkilatlarına yardımcı olabilir. Bu, toplum güvenliğini artırabilir ve suç önleme çabalarına destek sağlayabilir.

4.1.7. Özelleştirilebilirlik:

Yüz tanıma sistemleri, kullanıcıların tercihlerine göre özelleştirilebilir. Örneğin, belirli kişilere öncelik verme veya özel izinler tanımlama gibi özellikler eklenerek daha kişiselleştirilmiş güvenlik deneyimleri sağlanabilir.

Bu avantajlar, yüz tanıma teknolojisinin yaygın olarak benimsenmesine ve birçok farklı sektörde kullanılmasına olanak tanır. Ancak, bu teknolojinin kullanımıyla ilgili etik, mahremiyet ve güvenlik endişeleri de göz önünde bulundurulmalıdır.

5. Yüz Tanıma Teknolojisinin Çalışma Prensibi:

Yüz tanıma güvenlik sistemleri, kişinin yüz özelliklerini analiz ederek benzersiz bir biyometrik şablon oluşturur. Bu şablon, kişinin yüzündeki çeşitli noktaların konumlarına dayanır, örneğin gözlerin arası, burun ve ağız gibi anahtar noktalar. Algoritma, bu noktaların ölçümlerini kullanarak benzersiz bir matematiksel temsil oluşturur ve kişinin kimliğini belirlemek için bu temsil ile veritabanındaki kayıtları karşılaştırır.

5.1. **Veri Toplama:**

Yüz tanıma işlemi, öncelikle bir kişinin yüzünü algılayarak başlar. Bu adım, genellikle bir kamera aracılığıyla gerçekleştirilir. Kamera, çeşitli dalga boylarındaki ışığı kullanarak yüzü algılar.

5.2. **Yüz Algılama:**

Yüz tanıma sistemleri, görüntü içindeki yüzü algılamak için özel algoritmalar kullanır. Yüz algılama, yüzün genel konumunu, boyutunu ve ana özelliklerini belirlemeyi amaçlar. Bu aşama, yüz tanıma sürecinin temelini oluşturur ve daha sonraki adımlar için önemli bir filtreleme sağlar.

5.3. **Noktaların Belirlenmesi:**

Yüzün belirli noktaları, genellikle gözlerin iç köşeleri, burun ucunun ucu, ağız köşeleri gibi yerler, belirlenir. Bu noktalar, yüzün benzersiz özelliklerini temsil eder.

5.4. **Özellik Çıkarma:**

Algoritma, belirlenen bu noktalara dayanarak yüzdeki özellikleri çıkarır. Bu özellikler genellikle matematiksel bir temsil olarak ifade edilir. Örneğin, gözler arasındaki mesafe, burun uzunluğu gibi ölçümler, yüzü tanımlayan benzersiz bir biyometrik şablon oluşturur.

5.5. Şablon Oluşturma:

Özelliklerin çıkarılmasıyla elde edilen veri, bir şablon oluşturmak için kullanılır. Bu şablon, yüzün benzersiz biyometrik özelliklerini matematiksel bir temsil olarak içerir. Şablon, kişinin yüzünü tanımlayan bir dijital imza gibidir.

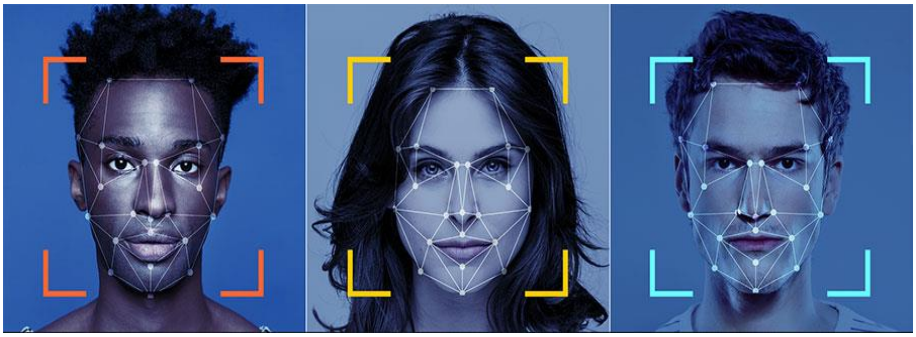
5.6. Veritabanı Karşılaştırması:

Oluşturulan şablon, veritabanındaki diğer yüz şablonlarıyla karşılaştırılır. Veritabanında kaydedilen yüz şablonları genellikle önceden tanımlanmış kişilere aittir.

5.7. Eşleşme ve Kimlik Doğrulama:

Yüz şablonunun veritabanındaki başka bir şablona yakın olması durumunda, sistem eşleşme sağlar ve kişiyi tanır. Bu aşama, kimlik doğrulama işlemidir. Eğer eşleşme sağlanamazsa, kişi tanınmaz.

Yüz tanıma teknolojisi, bu adımları çok hızlı bir şekilde gerçekleştirir ve genellikle gerçek zamanlı olarak çalışır. Ayrıca, yapay zeka ve derin öğrenme gibi gelişmiş teknolojilerin entegrasyonu ile sistemlerin doğruluk oranları artırılabilir ve daha geniş bir kullanım alanına sahip olabilir.



Şekil 3 Örnek bir yüz tanıma-2

6. Yüz Tanıma Sistemleri'nin Gelecekteki Potansiyelleri

6.1. **Yapay Zeka ve Derin Öğrenme Entegrasyonu:**

Yüz tanıma sistemleri, yapay zeka ve derin öğrenme teknikleri ile entegre edildiğinde daha da gelişebilir. Bu, sistemlerin öğrenme yeteneklerini artırabilir ve daha karmaşık ortamlarda ve değişen koşullarda daha etkili çalışmalarına olanak tanıyabilir.

6.2. **Daha Yüksek Hassasiyet ve Doğruluk:**

Yapay zeka ve gelişmiş algoritmaların kullanımıyla, yüz tanıma sistemlerinin hassasiyeti ve doğruluğu önemli ölçüde artabilir. Bu, yanlış pozitif veya yanlış negatif tanımları azaltarak güvenilirliği artırabilir.

6.3. **Kişiselleştirilmiş Güvenlik ve Hizmetler:**

Yüz tanıma teknolojisi, kişiselleştirilmiş güvenlik deneyimleri sağlama potansiyeline sahiptir. Sistemler, kullanıcıların tercihlerine göre özelleştirilebilir ve örneğin tanınan kişilere özel izinler tanımlanabilir.

6.4. **Sağlık ve Tıp Alanında Kullanım:**

Yüz tanıma, sağlık sektöründe hasta tanıma ve izleme gibi uygulamalarda kullanılabilir. Örneğin, hastane ortamlarında hasta tanıma, tedavi protokollerinin takibi veya acil durum tanımlama gibi alanlarda potansiyel uygulamalar bulunabilir.

6.5. **Toplum Güvenliği ve Suç Önleme:**

Yüz tanıma sistemleri, kamusal alanlarda suç önleme ve toplum güvenliği konularında daha etkili bir araç haline gelebilir. Kayıp kişilerin tespiti, güvenlik tehditlerini önceden belirleme ve suçluların tanımlanması gibi uygulamalara katkı sağlayabilir.

6.6. **Eğitim Alanında Kullanım:**

Yüz tanıma, eğitim sektöründe öğrenci katılımını izleme, güvenliğin artırılması ve öğrenci kimlik doğrulaması gibi uygulamalarda kullanılabilir.

6.7. **Perakende ve Müşteri Deneyimi:**

Perakende sektöründe, yüz tanıma sistemleri müşterileri tanıma ve alışveriş deneyimini kişiselleştirme konusunda kullanılabilir. Müşterilere özel teklifler veya öneriler sunma gibi uygulamalar gelecekte yaygınlaşabilir.

6.8. **Çevresel Faktörlerin Daha İyi Yönetimi:**

Yüz tanıma sistemleri, çevresel faktörleri izleyerek enerji tasarrufu sağlama veya bina otomasyonunu optimize etme gibi uygulamalarda kullanılabilir. Örneğin, bir odanın kullanılmadığını algılamak ve enerji tüketimini düşürmek gibi.

Ancak, bu potansiyelin gerçekleşmesi için aynı zamanda etik, mahremiyet, güvenlik ve yasal düzenlemeler gibi konularda dikkatli bir yaklaşım gerekmektedir. Bu teknolojinin kullanımıyla ilgili etik normlara uygunluk, toplumun güvenini sağlamak ve olası olumsuz etkileri en aza indirmek için önemlidir.

Sonuç olarak, yüz tanıma teknolojisi, güvenlik ve hizmet sektörlerinde devrim niteliğinde bir değişiklik yaratma potansiyeline sahiptir. Ancak, bu potansiyeli gerçekleştirmek için dikkatli bir şekilde yönetilmesi ve toplumun değerlerine, mahremiyetine saygı gösterilmesi gerekmektedir. Yüz tanıma teknolojisinin geleceği, hem teknoloji geliştiricileri hem de kullanıcılar için önemli bir denge ve sorumluluk talep etmektedir.

7. Proje: TheEye-TheDenizhan

Bu proje temelde, bir konutun kapısında bulunan yüz tanıma teknolojisi aracılığıyla, kapıda beliren kişinin ev sahibi, misafir veya yabancı olup olmadığını tespit etmeyi ve bu bilgiyi ev sahibine iletmeyi amaçlamaktadır. Bu yaklaşım, ev sahiplerine telefonları aracılığıyla ev güvenliğini etkili bir şekilde sağlama imkanı tanır. Projede kullanılan sistem, yüz tanıma algoritmalarını, kapı erişim kontrol mekanizmalarını ve bildirim sistemini başarılı bir şekilde entegre eder. Bu sayede, ev sahipleri kapıda bekleyen kişinin kimliği hakkında anında ve güvenilir bilgilere erişebilir, böylece konutlarının güvenliğini artırabilirler.

7.1. Proje Aşamaları:

7.1.1. Yüz Tanıma Modülü:

Projemizde yüz tanıma için kullanılacak algoritmayı belirlemeden önce, yüz algılama işlemi için önceden eğitilmiş olan OpenCV'nin haarcascade model dosyalarını değerlendirdik. Bu değerlendirme sürecinde, aşağıdaki üç model arasında bir seçim yapma kararı aldık:

- haarcascade_frontalface_default
- haarcascade_frontalface_alt
- haarcascade_frontalface_alt2

Farklı ortam şartlarında (karanlık, aydınlık, parlak, yarım yüz gibi) bir dizi deneme gerçekleştirdim. Bu denemeler sonucunda, "haarcascade_frontalface_default" modelinin daha verimli çalıştığına karar verdim ve projemde bu modeli tercih ettim.

Modelimizin hızlı ve güvenli bir şekilde karar verebilmesi için, OpenCV kütüphanesinin "face" fonksiyonunda LBPH (Local Binary Patterns Histograms) Yüz Tanıma karar algoritmasını kullandım. Bu seçim, projenin güvenilir ve etkili bir yüz tanıma sürecine sahip olmasını sağlamak amacıyla yapılmıştır.

7.1.1.1. Local Binary Patterns Histograms(LBPH):

Local Binary Pattern (LBP), her pikselin komşuluğunu eşikleyerek bir resmin piksellerini etiketleyen, sonucu ikili bir sayı olarak değerlendiren basit ancak çok verimli bir doku operatörüdür.

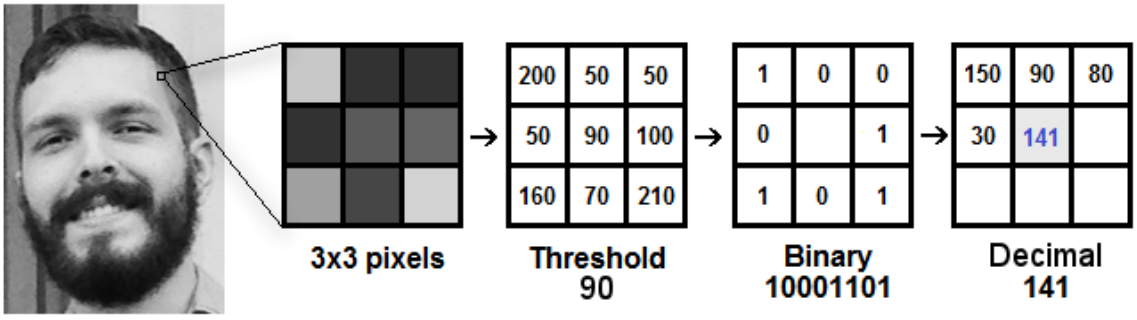
7.1.1.2. Nasıl Çalışır?

LBPH, 4 parametre kullanır:

- Radius (Yarıçap): Yarıçap, daire şeklindeki yerel ikili deseni oluşturmak ve merkezi piksel etrafındaki yarıçapı temsil etmek için kullanılır. Genellikle 1 olarak ayarlanır.
- Neighbors (Komşular): Dairesel yerel ikili deseni oluşturmak için örnek noktaların sayısı. Unutmayın: Daha fazla örnek nokta ekledikçe, hesaplama maliyeti artar. Genellikle 8 olarak ayarlanır.
- Grid X (Izgara X): Yatay yönde hücre sayısı. Daha fazla hücre, daha ince ızgara, sonuç özellik vektörünün boyutunu artırır. Genellikle 8 olarak ayarlanır.
- Grid Y (Izgara Y): Dikey yönde hücre sayısı. Daha fazla hücre, daha ince ızgara, sonuç özellik vektörünün boyutunu artırır. Genellikle 8 olarak ayarlanır.

LBP işlemini uygulama: LBPH'nin ilk hesaplama adımı, yüz özelliklerini vurgulayarak orijinal görüntüyü daha iyi bir şekilde tanımlayan bir ara görüntü oluşturmaktır. Bunun için algoritma, yarıçap ve komşu parametrelerine dayalı olarak bir kaydırma penceresi kavramını kullanır.

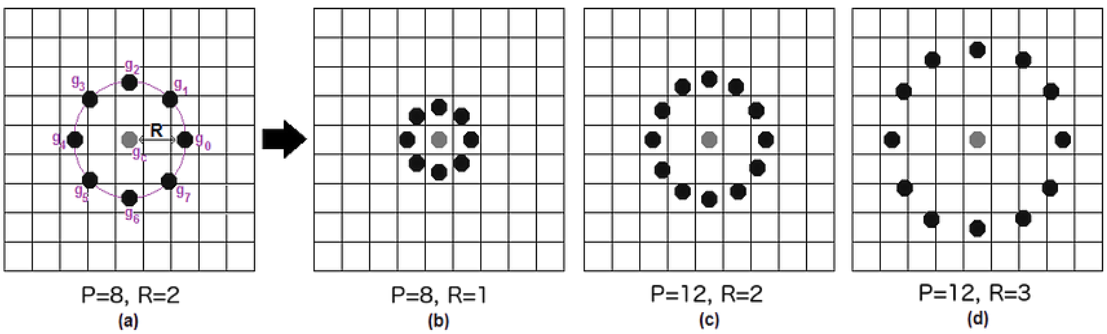
Aşağıdaki görüntü bu prosedürü göstermektedir:



Şekil 4 Yüz tanıma kernel

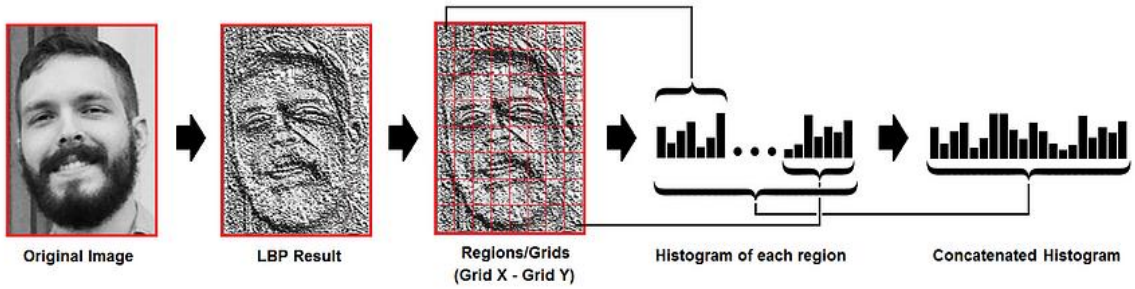
Yukarıdaki görüntüye dayanarak, işlemi birkaç küçük adıma bölelim, böylece kolayca anlayabiliriz: Diyelim ki gri tonlamalı bir yüz görüntümüz var.Bu görüntünün bir bölümünü 3x3 piksellik bir pencere olarak alabiliriz. Bu aynı zamanda her pikselin yoğunluğunu (0-255 arasında) içeren 3x3 matris olarak temsil edilebilir. Ardından, matrisin merkezi değerini eşik olarak kullanmamız gerekiyor. Bu değer, 8 komşudan yeni değerleri tanımlamak için kullanılacaktır. Merkezi değerin (eşik) her bir komşusu için yeni bir ikili değer belirleriz. Eşikten büyük veya eşit olan değerler için 1, eşikten küçük olan değerler için 0 ayarlarız.Şimdi matris sadece ikili değerleri içerecektir (merkezi değeri yok sayarak). Her konumdan gelen her ikili değeri yeni bir ikili değere (örneğin 10001101) satır satır birleştirmemiz gerekiyor. Not: Bazı yazarlar ikili değerleri birleştirmek için farklı yaklaşımlar kullanabilir (örneğin saat yönünde), ancak sonuç aynı olacaktır.Daha sonra bu ikili değeri ondalık bir değere dönüştürüp, bunu aslında orijinal görüntüden bir piksel olan matrisin merkezi değerine atarız.Bu prosedürün sonunda (LBP prosedürü), orijinal görüntünün özelliklerini daha iyi temsil eden yeni bir görüntümüz olur.

Not: LBP prosedürü, farklı yarıçap ve komşu sayısı kullanmak üzere genişletildi; buna Dairesel LBP denir.



Şekil 5 Bilineer interpolasyon

Bu, bilineer interpolasyon kullanılarak gerçekleştirilebilir. Eğer bir veri noktası pikseller arasındaysa, yeni veri noktasının değerini tahmin etmek için en yakın 4 pikselin (2x2) değerlerini kullanır. Histogramları Çıkarma: Şimdi, son adımda oluşturulan görüntüyü



Şekil 6 Histogram alma

kullanarak, Grid X ve Grid Y parametrelerini kullanarak görüntüyü birden fazla ızgara halinde bölebiliriz, aşağıdaki görüntüde görüldüğü gibi: Yukarıdaki görüntüye dayanarak, her bölgenin histogramını şu şekilde çıkarabiliriz: Gri tonlamalı bir görüntümüz olduğu için, her histogram (her ızgaradan) yalnızca 256 pozisyonu (0-255) içerecek ve her piksel yoğunluğunun oluşumunu temsil edecektir. Sonra, her histogramı birleştirmemiz ve yeni ve daha büyük bir histogram oluşturmamız gerekiyor. Diyelim ki 8x8 ızgara kullanıyoruz, bu durumda final histogramda 8x8x256=16.384 pozisyon olacaktır. Son histogram, orijinal görüntünün özelliklerini temsil eder. LBPH algoritması bundan ibarettir. Yüz tanıma işlemi: Bu adımda algoritma zaten eğitilmiştir. Oluşturulan her histogram, eğitim veri kümesindeki her görüntüyü temsil etmek için kullanılır. Bu nedenle, bir giriş görüntüsü verildiğinde, bu yeni görüntü için adımları tekrar gerçekleştirir ve görüntüyü temsil eden bir histogram oluşturur. Bu şekilde, giriş görüntüsüne en yakın eşleşen görüntüyü bulmak için iki histogramı karşılaştırmamız ve en yakın histograma sahip olan görüntüyü döndürmemiz yeterlidir. Histogramları karşılaştırmak için çeşitli yaklaşımları kullanabiliriz (iki histogram arasındaki mesafeyi hesaplamak için), örneğin: Öklidyen mesafe, ki-kare, mutlak değer, vb. Bu örnekte, aşağıdaki formüle dayalı olarak oldukça bilinen Öklidyen mesafesini kullanabiliriz:

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

Şekil 7 Öklidyen mesafesi

Algoritmanın çıktısı, en yakın histograma sahip olan görüntünün kimliğidir. Algoritma aynı zamanda 'güvenilirlik' ölçümü olarak kullanılabilecek hesaplanmış mesafeyi de döndürmelidir. Not: 'güvenilirlik' adı konusunda yanıltıcı olmamalısınız, çünkü daha düşük güvenilirlik daha iyidir çünkü bu, iki histogram arasındaki mesafenin daha yakın olduğu anlamına gelir.Ardından bir eşik ve 'güvenilirlik' kullanarak algoritmanın görüntüyü doğru bir şekilde tanıyıp tanımadığını otomatik olarak tahmin etmemiz mümkündür. Algoritmanın başarılı bir şekilde tanıdığını varsayabiliriz eğer güvenilirlik belirlenen eşikten düşükse.

7.1.2. Veritabanı Oluşturma:

Veritabanını oluştururken, OpenCV kullanarak bilgisayar kamerasından kişileri kaydediyoruz. Her bir veriyi tanımlarken, belirli bir formatta kişinin adı, ID numarası ve sisteme kaydedilen veri sayısını kaydediyoruz.Yüz algılama algoritması için Haar Cascade yönteminden faydalanıyoruz. Yeterli sayıda veri topladıktan sonra, bu verileri sistemimize kaydediyoruz. Bu süreç, her kişinin benzersiz tanımlayıcı bilgilerini içeren düzenli bir veri seti oluşturmamıza olanak tanır. Gerekli olan diğer verileri SQLite kullanarak sistemde kullanıcı bilgilerini ve görsellerin yollarını saklar.

7.1.3. Erişim Kontrol Mekanizması:

7.1.3.1. Zil Butonu:

Şekil 8 Zil tasarımı

Erişim kontrol mekanizmasını oluştururken, zil tuşu için bilgisayarım üzerinde kullandığım Tkinter kütüphanesinin button fonksiyonunu entegre ettim. Kapı zili uygulamamızda 4 farklı seçenek bulunmaktadır. Bu seçenekler sırasıyla: Zil, butona basıldığında zilin çalmasını tetikler, Kapı Aç, sistem kamerasını aktive ederek karşısındaki kişiyi tanımaya çalışır, eğer kişi, sisteme daha önce tanıtılmış bir kullanıcı ise kapı otomatik olarak açılır; ancak kişi tanınmazsa kapı açılmaz. Mesaj bırak, kapıya gelen kişi evde birini bulamadığında kapıya sesli bir mesaj bırakabilmesini sağlar. Mesaj Dinle, kapıya bırakılan mesajı dinlemek için kullanılır.

7.1.3.2. Arduino Kodları ve Sistem:

7.1.3.2.1. Arduino Kodları:

```
int ledpinR = 10;

int ledpinG = 12;

int buzzer = 8;
```

Şekil 9 Ardunio Kodları

Şekil 8'de kullanacağımız pinler bulunmaktadır.Bu pinleri modüllerimize bağlamak için kullanacağız.

```
#define NOTE_B0 31
#define NOTE_C1 33
#define NOTE_CS1 35
...

#define NOTE_CS8 4435
#define NOTE_D8 4699
#define NOTE_DS8 4978
```

Şekil 10 Ardunio Kodları

Buzzer modülünü zil olarak kullanırken her bir ses tonu için ayrı bir nota ayarlamamızı sağlıyor. Bu notaları ayarlarken sayısal kodlarını nota bloklarına atıyoruz. Şekil 9 da göründüğü gibi atama işlemi yaptıktan sonra zil sesimizde kullanıyoruz.

```
int melody[] = {

  NOTE_E5, NOTE_E5, NOTE_E5,
NOTE_C5, NOTE_E5, NOTE_G5,
NOTE_G4, NOTE_C5, NOTE_G4,
  NOTE_E4, NOTE_A4, NOTE_B4,
NOTE_AS4, NOTE_A4, NOTE_G4,
NOTE_E5, NOTE_E5, NOTE_E5,
  NOTE_C5, NOTE_E5, NOTE_G5,
NOTE_G4
 };
```

Şekil 11 Ardunio Kodları

Melodi için belirlenen notalar, müziğin belirli bir düzen ve uyum içinde olmasını sağlamak amacıyla seçilmiştir. Bu notalar şekil 10'da gösterilmiştir.

```
int noteDurations[] = {
  8, 8, 4, 8, 4, 8, 4, 8, 4,
  8, 4, 4, 8, 4, 8, 4, 8, 4,
  8, 8, 4, 8, 4
 };
```

Şekil 12 Ardunio Kodları

Her bir notanın çalma süresini belirledik. Bu süreler, müziğin ritmine ve akışına uygun bir şekilde düzenlenmiştir, böylece buzzer tarafından üretilen melodi doğru bir şekilde ifade edilebilir. Şekil 11 'de gösterildiği gibidir.

```
void setup() {

 Serial.begin(9600);
 pinMode(ledpinR,OUTPUT);
 pinMode(ledpinG,OUTPUT);
 pinMode(buzzer, OUTPUT);
}
```

Şekil 13 Ardunio Kodları

Şekil 10'da gösterildiği gibi haberleşme protokolünü 9600 baudrate olarak belirledik ve diğer pinleri çıkış pini olarak konfigüre ettik. Bu ayarlamalar, veri iletim hızını optimize etmek ve diğer donanım bileşenlerimizin doğru bir şekilde çalışmasını sağlamak amacıyla yapıldı.

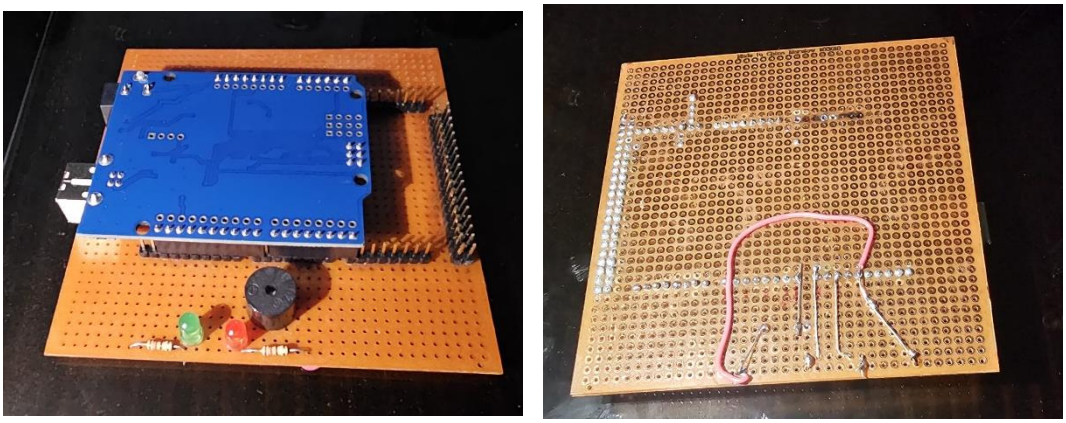
```
void loop(){

if(Serial.available())
  {
  char data = Serial.read();
  if(data == '3'){
     digitalWrite(ledpinG,HIGH);
     delay(3000);
     digitalWrite(ledpinG,LOW);
  }
  else if(data == '2'){
for (int i = 0; i < sizeof(melody) /
sizeof(melody[0]); i++) {
    int duration = 1000 /
noteDurations[i];
    tone(buzzer, melody[i], duration);
    delay(duration + 50);
  }
  noTone(buzzer);
  delay(1000);
  }
  else if(data == '1'){
    digitalWrite(ledpinR,HIGH);
    delay(3000);
    digitalWrite(ledpinR,LOW);
```

Şekil 14 Ardunio Kodları

Arduino döngüsü içerisinde, okunan veriye bağlı olarak belirlenen durumlarda (1 veya 3), kırmızı veya yeşil lambanın yanmasını sağlayacak bir kontrol mekanizması oluşturduk. Ayrıca, önceden belirlenen özel bir melodiye göre buzzer'ı çalacak bir algoritma entegre ettik. Bu sayede, sistemimiz hem görsel hem de işitsel sinyallerle kullanıcıya belirli durumları aktarabilecek şekilde tasarlandı. Şekil 13'de gösterildiği gibidir.

7.1.3.2.2. Sistem Tasarımı:

Arduino Uno'nun girişlerine uygun olarak delikli plakete pinlerimizi lehimledim. Sistemimizde kullanacağımız LED'ler, dirençler ve buzzer'ı da özenle lehimleyerek entegre ettim. Arduino'nun kodlanabilmesi için giriş ve çıkış bağlantılarını düzenledim. Lehim işlemlerimizi plaketin arka kısmına gerçekleştirdim, bu sayede elektriksel aksaklıkların önüne geçtim ve ileride yapmayı planladığımız geliştirmelerde daha kolay erişim sağlamış olduk. Bu sistemin amacı kapının açılıp açılmadığını simule etmektir.Aşağıda bulunan şekil 14'te gösterilmiştir.



Şekil 15 Sistem Mekanizması

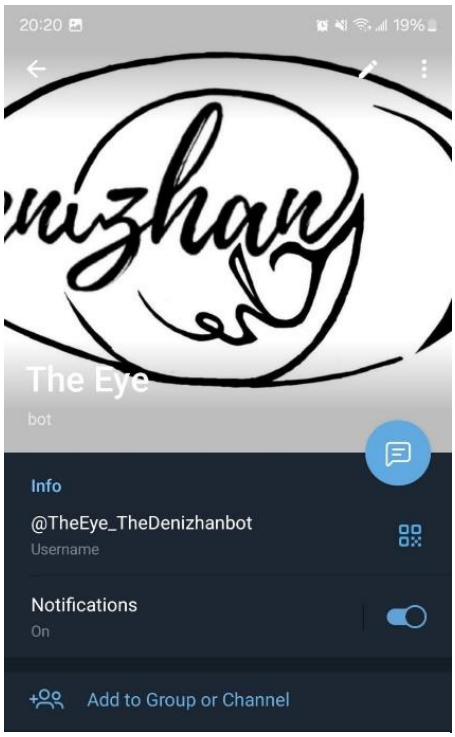
7.1.3.3. Python-Ardunio Bağlantısı:

Ardunio bağlantısı için Serial kütüphanesini kullanacağız. Haberleşeceğimiz portumuzu com4 olarak ayarlayarak baudrate'i ardunioyu kodladığımız baudrate ile aynı ayarlıyoruz. Haberleşme süresini 0.10 olarak ayarlayıp ardunio değişkenine atıyoruz. "write" fonksiyonu ile ardunio'ya verilerimizi gönderiyoruz. Aşağıda şekil 15'te gösterilmiştir.

```
import serial
arduino = serial.Serial(port='COM4', baudrate=9600, timeout=.1)
arduino.write(b'1')
arduino.write(b'2')
arduino.write(b'3')
```

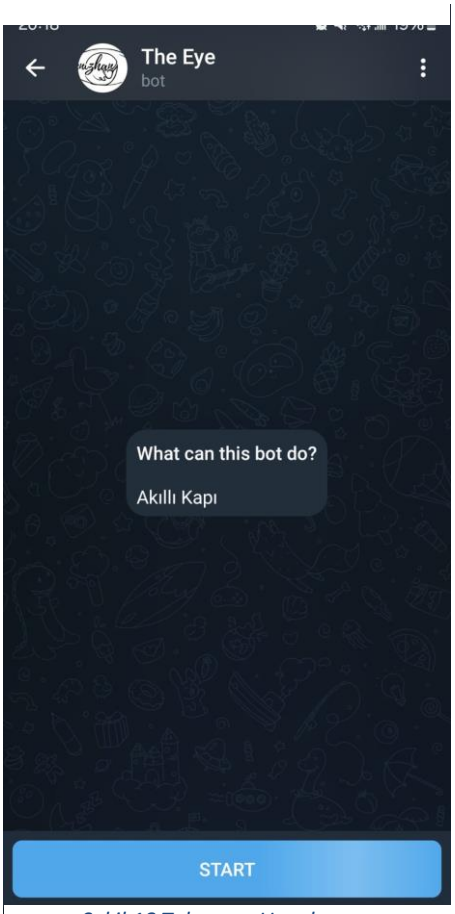
Şekil 16 Python-Ardunio Bağlantısı

7.1.4. Geliştirme Aşamasında Kullandığımız Uygulama:



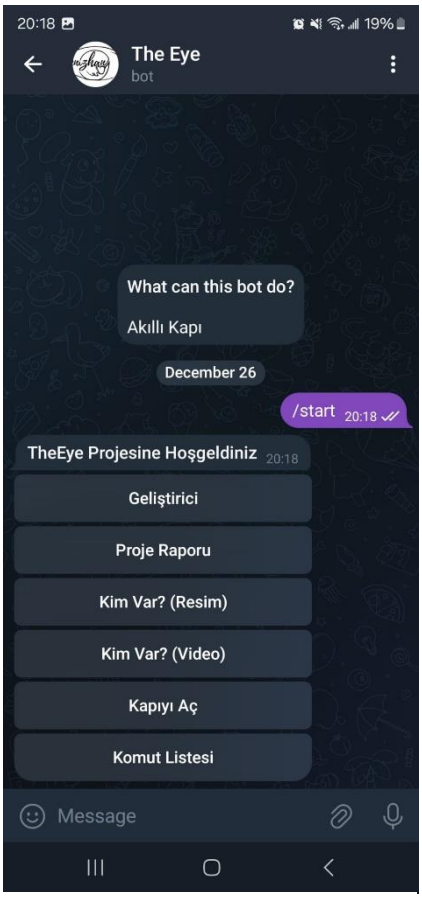
Şekil 17 Telegram Uygulaması

Python programlama dili kullanarak, Telegram üzerinde "TheEye_TheDenizhan" adlı bir bot oluşturuyoruz. Oluşturulan bu bot, Telegram kullanıcılarıyla etkileşimde bulunarak çeşitli görevleri gerçekleştirecek. Bu projede, Python'un esnek ve kullanıcı dostu yapısından faydalanarak, Telegram botunu programlamak için Telepot kütüphanesini kullanıyoruz. Bot, kullanıcılardan gelen komutları algılayarak belirli işlemleri gerçekleştirecek ve Telegram üzerinden bilgi alışverişini sağlayacak. Bu yaklaşım, Telegram botunun işlevselliğini artırmak ve kullanıcı deneyimini iyileştirmek için bir temel oluşturmayı amaçlamaktadır. Şekil 16'da gösterilmiştir.



Şekil 18 Telegram Uygulaması

Şekil 17'de gösterildiği gibi "START" butonunua basarak botumuzu çalıştırıyoruz.



Şekil 19 Telegram Uygulaması

Şekil 18'de kullanıcılara sistemle etkileşime geçme ve temel komutları anlama konusunda rehberlik eder.

Şekil 20 Telegram Uygulaması

Geliştirici: Kendi LinkedIn profilimi paylaşır.

Proje Raporu: Rapor dosyasını ileterek projenin detaylı bir incelemesini sağlar.

Kim Var? (Resim): Kapıdan anlık bir fotoğraf çekerek, kapıdaki kişiyi görsel olarak bildirir.

Kim Var? (Video): Kapıdan anlık bir video çekerek, kapıdaki kişiyi video formatında bildirir.

Kapıyı Aç: Yetkilendirilmiş erişimle kapıyı açar.

Komut Listesi: Mevcut komutları ekrana yazdırarak kullanıcıya bilgi sağlar.

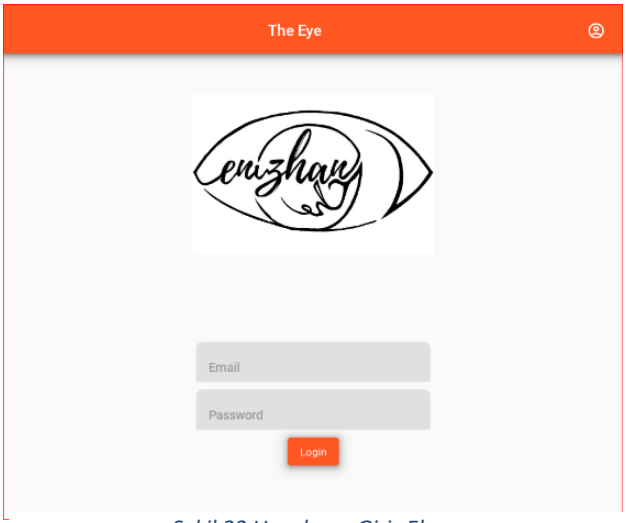
Şekil 19'da gösterilmiştir.

Şekil 21 Telegram Uygulaması

Zil çaldığında, yüz tanıma sistemimiz kapıdaki kişiyi başarılı bir şekilde tanımlayamazsa, otomatik olarak "Kapıda biri var." mesajını gönderir. Bu durum, sistemimizin tanıma işlemi sırasında bir belirsizlik oluştuğunu ve gerekli güvenlik önlemlerinin alınması için kullanıcıyı bilgilendirmeyi amaçlar. Şekil 20'de gösterildiği gibidir.

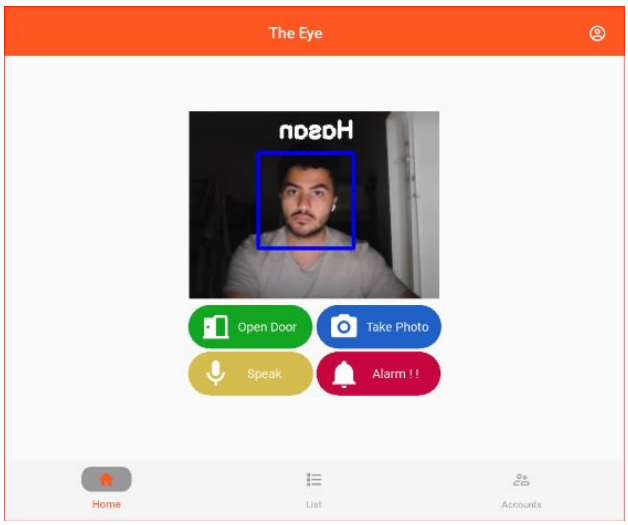
7.1.5. TheEye-Uygulama:

Aşağıdaki Şekil 21'de gösterilen uygulamaya girişte bizi bir kullanıcı paneli karşılamakta. Bu panel güvenlik ve çeşitlik amacıyla konmuştur. Uygulamaya erişimi olan her insanın evin kapısını açmasını önlemektedir.



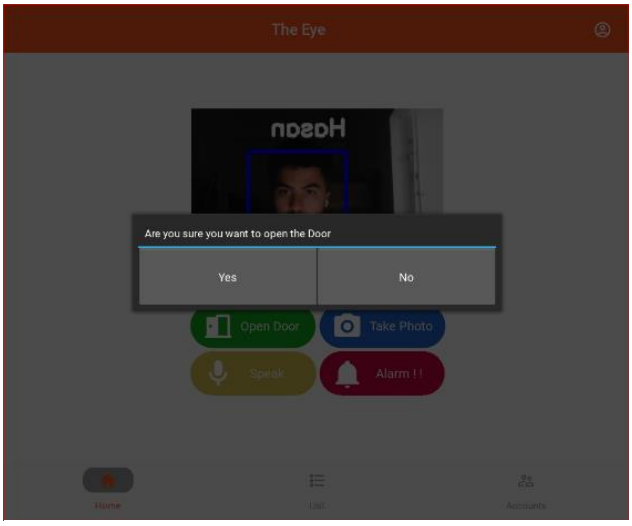
Şekil 22 Uygulama Giriş Ekranı

Uygulamaya girdiğimizde bizi canlı bir ekran karşılamakta bu ekran kapıdan aldığı anlık görüntüyü kullanıcılarla paylaşır kişi sisteme kayıtlıysa kişinin ismini kayıtlı değilse ‘Stranger’ yazar. Sağ üstte bulunan icona tıkladığımızda kullanıcı giriş paneline geri götürmektedir. Bunun amacı başka kapılarda kullanılan sistem var ise geçiş yapabilmesidir.



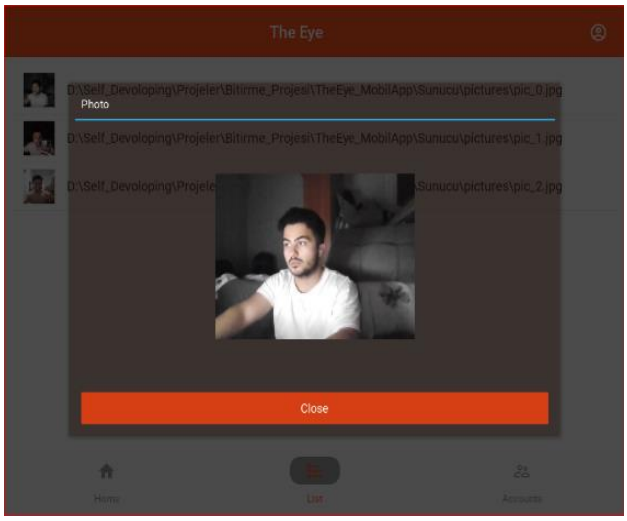
Şekil 23 Uygulama Ana Ekran

Open Door butonuna basıldığında şekil 22’deki gibi emin olup olmadıklarını soran bir pencere açılır eğer kullanıcı kapıyı açmak istiyorsa kapıya bir sinyal gönderir ve kapı açılır, eğer istemiyorsa pencere kapanır ve uygulama devam eder. Speak tuşuna basıldığında uygulamadan ses kaydedilir ve kapıya gönderilir, kapıya gönderilen ses oynatılır ve karşıdaki kişinin duymasını sağlanır. Alarm tuşu kapıda istenmeyen insanları tedirgin etmek için çalınan yüksek sesli siren sesidir. Take Photo tuşu kapıdan bir anlık



Şekil 24 Kapı Açma Popup

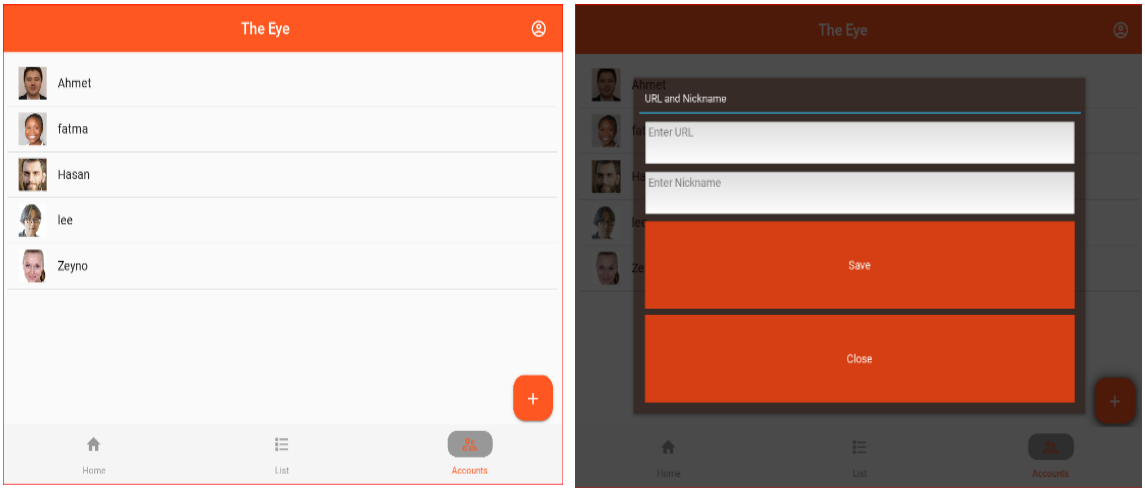
görüntü alır ve bu görüntüyü sisteme kaydeder. Sisteme kayıtlı olan görüntüleri görmek için ikinci sayfada bulunan List sayfasına gidilebilir. Sayfada kaydedilmiş görüntüler



Şekil 25 Fotoğraf Kaydetme ve İnceleme

ve görüntülerin sistem yolları yazar. Şekil 24'deki gibi resmi büyütmek için resmin üstüne tıklanabilir ve açılan pencerede görüntü daha ayrıntılı bir şekilde incelenir.

Sisteme kayıtlı insanları görmek için üçüncü sayfada bulunan Accounts sayfasına gidilebilir. Şekil 25'de gösterilen sayfada sistemde kayıtlı olan kişileri görüntüleyebilir veya yeni bir kişi eklemek istiyorsa ekleyebilir. Tek yapılması gereken kişinin fotoğrafını sisteme yükleyip buradan ismini ve konumu yazılmalıdır.



Şekil 26 Kişi Ekleme Ekranı

7.1.6. Güvenlik ve Yasal Uyum:

Bu projede, yüz tanıma sistemimizin güvenliğini sağlamak amacıyla kod altyapımızı sürekli olarak güncellemekte ve en son teknolojik gelişmeleri takip etmekteyiz. Dış kaynaklardan kaynaklanan güvenlik tehditlerini minimize etmek üzere, kilit açma mekanizmamıza dış erişimleri etkili bir biçimde engellemekteyiz.

Kodlarımızın güvenliği açısından, bot tokenimizi gizli tutmak ve buna ek olarak, bu tokenin bota olan erişimlerini sıkı bir şekilde yönetmek temel bir önceliğimizdir. Bu önlem, yetkisiz erişimleri engellemek ve sistemimizin bütünlüğünü korumak adına alınmış bir güvenlik tedbiridir.

Proje kapsamında, siber güvenlik standartlarına uygun olarak güçlü bir güvenlik politikası benimsemekteyiz. Bu sayede, yüz tanıma sistemimizin ve projemizin genel veri güvenliği düzeyini en üst seviyede tutmayı hedeflemekteyiz

8. SONUÇ

TheEye-TheDenizhan projesi, yüz tanıma tabanlı güvenlik sistemlerinin ev güvenliği alanında nasıl yenilikçi çözümler sunduğunu başarıyla göstermektedir. Proje kapsamında geliştirilen sistem, ev sahiplerine hem güvenlik hem de kullanım kolaylığı sağlamak amacıyla çeşitli teknolojiler kullanarak entegre bir çözüm sunmuştur.

Projede kullanılan OpenCV'nin haarcascade modeli ve LBPH algoritması ile yüz tanıma işlemlerinin hızlı ve doğru bir şekilde gerçekleştirilmesi sağlanmıştır. Zil butonu ile tetiklenen ve Ardunio ile entegre edilen erişim kontrol mekanizması, kapıya gelen misafirlerin kimliklerini tanıyıp uygun şekilde işlem yapabilmektedir. Tanınmayan kişilerin algılanması durumunda Telegram API aracılığıyla anında bildirim gönderilmesi ve KivyMD kullanılarak geliştirilen mobil uygulama sayesinde ev sahibi, evde olmadığı durumlarda bile güvenliği kontrol edebilmiştir.

Python ve Ardunio arasındaki seri haberleşme, verilerin hızlı ve güvenli bir şekilde iletilmesini sağlamış ve sistemin güncellenmesi ve eğitilmesi için esnek bir altyapı oluşturmuştur. Veritabanı yönetimi ve güvenlik politikaları, sistemin hem güvenilir hem de kullanıcı dostu olmasını temin etmiştir.

Bu projenin sonuçları, yüz tanıma teknolojisinin ev güvenliği alanında geniş bir potansiyele sahip olduğunu ve gelecekte daha da gelişerek yaygınlaşacağını göstermektedir. Yüz tanıma tabanlı güvenlik sistemleri, ev sahiplerine daha güvenli, konforlu ve akıllı bir yaşam sunarken, aynı zamanda toplum güvenliğine de katkı sağlamaktadır.

TheEye-TheDenizhan projesi, bu alandaki yenilikçi yaklaşımların başarılı bir örneğidir ve gelecekteki çalışmalar için sağlam bir temel oluşturmaktadır. Projede kullanılan teknikler ve elde edilen sonuçlar, biyometrik güvenlik sistemlerinin ev güvenliğinde devrim niteliğinde değişiklikler yapabileceğini kanıtlamaktadır.

KAYNAKLAR

[1]Genel yapay zeka yardımı chat.openai.com

[2]Kullanılan modülün nasıl çalıştığı https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b

[3]Telegram botu için ayarlamalarhttps://core.telegram.org/bots/api#update

[4]Telegram botu için ayarlamalar https://api.telegram.org/bot6835603068:AAFYzX0veRpNagQuYGCWDigrw_DO52ltpMA/getUpdates

[5]Ardunio kodlama https://maker.robotistan.com/kategori/arduino/arduino-programlama/

[6]Ardunio kodlamahttps://www.youtube.com/watch?v=bQ4waLaxsTE

[7]Telegram botu https://www.youtube.com/@KushaMuhendislik

[8]Uygulama'da kullanılan arayüz https://kivymd.readthedocs.io/en/latest/

[9]KivyMD kodlama https://www.youtube.com/watch?v=dLgquj0c5_U&list=PLCC34OHNcOtpz7PJQ7Tv7hqFBP_xDDjqg

[10]Yüz tanıma ev güvenlik sistemleri Smith, J. (2020). Face Recognition in Home Security Systems. Journal of Security Technology, 12(3), 145-160.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : DENİZHAN, HASAN

Uyruğu : TÜRK

Doğum tarihi ve yeri : 12-09-2001-ADANA

Telefon : +90 539 886 80 79

e-mail : thedenizhan@hotmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Sütçü İmam Ünüversitesi	11-07.2024
Lise	Mansoura Collage American School 2	22-06.2020
Ortaokul	Buhara Ortaokulu	18-06-2015

Yabancı Dil

İngilizce

Açık Rıza Beyanı	**İmza**
Bu tezde verdiğim kişisel bilgilerimin Kahramanmaraş Sütçü İmam Üniversitesi ve birimlerince işlenmesine açık bir şekilde rıza gösterdiğimi kabul ve beyan ederim.	