# ELECTRIC DOOR LOCK ACCESS WITH VISUAL PASSWORD USING RASPBERRY PI

**Alperen ŞENYİĞİT**
Eskişehir Osmangazi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü
ORCID: 0009-0007-9039-2237

**Mustafa Can SEÇGİN**
Eskişehir Osmangazi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü
ORCID: 0009-0003-2129-7157

**Reşat ÇAYHAN**
Eskişehir Osmangazi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü
ORCID: 0009-0006-5940-2946

**Doç. Dr. Hasan Serhan YAVUZ**
Eskişehir Osmangazi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü
ORCID: 0000-0002-4944-1013

## ABSTRACT
Smart door locks can be used as a component of home automation or in enterprises to provide enhanced entrance security. Door security is essential for ensuring personal safety, protection of valuables, and privacy. In this paper, we present an application that detects facial expressions and hand gestures to provide access to an electric automatic door lock. The implementation involves using a visual camera connected to a Raspberry Pi. The designed algorithm identifies access authorization through a generic visual password. The system operates in two authorization modes: administrator and user. The administrator can create visual passwords based on consecutive mimic movements and store the password in the device. In user mode, the system analyzes facial and hand movements of individuals in front of the door and verifies their authenticity by matching the detected movements with the predefined visual passwords. The system aims to provide touchless access to the door, eliminating the need for physical keys or contact with the lock. For real-time data processing from the camera, we used popular computer vision libraries including OpenCV, Mediapipe, and CVZone. We also developed a user-friendly graphical interface that allows administrators to modify their visual passwords and monitor system activity. Administrators can edit or change visual passwords and check log records to identify people who attempt access. The system also takes a screenshot upon incorrect entry and locks the door for a certain period of time after multiple failed attempts to increase security. We tested the performance of the system with mixed visual passwords under different illumination conditions and obtained satisfactory visual password identification results.
**Keywords:** Visual object detection, authentication, gesture recognition, visual password door lock, Raspberry Pi

# RASPBERRY Pİ KULLANARAK GÖRSEL ŞİFRE İLE ELEKTRİKLİ KAPI KİLİDİ ERİŞİMİ

## ÖZET
Akıllı kapı kilitleri, gelişmiş giriş güvenliği sağlamak için işletmelerde veya ev otomasyonunun bir bileşeni olarak konutlarda kullanılmaktadır. Kapı güvenliği, kişisel güvenliğin, değerli eşyaların korunmasının ve mahremiyetin sağlanması için gereklidir. Bu çalışmada, elektrikli otomatik kapı kilidine erişim sağlamak için yüz mimiklerini ve el hareketlerini algılayan bir uygulama tasarlanmıştır. Raspberry Pi platformunda çalıştırılan uygulama, görsel kameradan gerçek zamanlı olarak yakaladığı imgeleri kullanarak mimik hareketlerini izlemektedir. Tasarlanan algoritmada, erişim yetkilendirmesi (kilidin açılması) görsel parolanın doğru olarak gerçekleştirilmesi sonrasında verilmektedir. Sistem, yönetici ve kullanıcı olmak üzere iki yetki seviyesinde çalışmaktadır. Yönetici, ardışık mimik hareketlerine göre görsel şifreler oluşturabilmekte ve şifreyi cihazda saklayabilmektedir. Kullanıcı modunda sistem, kapı önündeki kişilerin yüz ve el hareketlerini analiz eder ve tespit edilen hareketleri önceden tanımlanmış görsel şifrelerle karşılaştırarak ilgili hareketlerin giriş yetkisi olup olmadığını sorgular. Çalışmada, kapıya temassız erişim sağlayarak fiziksel olarak anahtar veya kilide temas ihtiyacının ortadan kaldırılması amaçlanmıştır. Kameradan gerçek zamanlı veri işleme için OpenCV, Mediapipe ve CVZone gibi popüler bilgisayarla görü yazılım kütüphaneleri kullanılmıştır. Ayrıca, yöneticilerin görsel parolaları değiştirebilmesi ve sistem etkinliğini izlemelerine olanak tanıyan, kullanıcı dostu bir grafik arayüz geliştirilmiştir. Yöneticiler, erişim girişiminde bulunan kişileri izlemek için günlük kayıtlarını da kontrol edebilir. Sistem ayrıca hatalı girişlerde ekran görüntüsü almaktadır ve güvenliği artırmak için birden fazla başarısız girişimden sonra kapıyı belirli bir süre kilitlemektedir. Sistemin performansını farklı aydınlatma koşullarında karışık görsel şifrelerle test ettiğimizde, tatmin edici seviyelerde görsel şifre tanımlama sonuçları elde edilmiştir.
**Anahtar kelimeler:** Görsel nesne algılama, kimlik doğrulama, mimik tanıma, görsel şifreli kapı kilidi, Raspberry Pi

## GİRİŞ
Akıllı kapı kilitleri, ev sahiplerine çeşitli kimlik doğrulama yöntemleri aracılığıyla evlerine erişimi uzaktan kontrol etme yeteneği sağlayan, gelişmekte olan bir teknolojidir (Dawn vd., 2023). Bu kilitler, belirli kişilere belirli zamanlarda erişim izni verecek şekilde programlanabilir ve hatta birisi içeriye giriş veya çıkış yaptığında ev sahiplerine bildirim gönderebilir (Chakraborty ve Sultana, 2022). Kullanılan donanım ve yazılım çeşitlerine göre tuş takımı şifrelemesi, biyometrik tanımlama, bluetooth, RFID (radio frequency identification) veya NFC (near-field communication) gibi teknolojiler üzerinden kimlik doğrulama yaparak, içeriye yalnızca yetkili kişilerin erişimini sağlar (Govindraj vd., 2020). Bazı modellerde, birisi yanlış bir kod veya parola kullanarak kapıyı açmaya çalıştığında ev sahiplerine uyarı gönderme özelliği de vardır (Dawn vd., 2023). Akıllı kapı kilitleri, evlerine kimin girdiği konusunda ek bir güvenlik ve kontrol katmanı sağlayarak, ev sahiplerinin iç huzurunu ve güvenlik sistemlerinden genel memnuniyetlerini artırma potansiyeline sahiptir. Yenilikçi teknolojiler içeren son kullanıcı ürünlerinin fiyatları ise genelde yüksektir.
Son yıllarda, özellikle parmak izi veya yüz tanıma gibi biyometrik tanıma kullanan akıllı kapı kilitleri popülaritesini arttırmaktadır (Saroha vd., 2022). Bu kilitler, bireylerin benzersiz fiziksel özelliklerine dayandığından yüksek düzeyde güvenlik sağlamaktadır (Venkata vd., 2021). Ayrıca biyometrik tabanlı kilitler, fiziksel anahtarlara veya kaybolabilecek, çalınabilecek veya paylaşılabilecek kodlara olan ihtiyacı ortadan kaldırdıkları için ek kolaylık sunmaktadır (Motwani vd., 2021).

Biyometrik tabanlı akıllı kilitlerin önemli aleyhte durumları olarak, bireylerin mahremiyet endişeleri, potansiyel güvenlik ihlalleri veya teknik sınırlamalar sıralanabilir. Bu durumlara rağmen akıllı kilitler, en yeni teknoloji ve tasarımı birleştiren güvenli ve kullanışlı bir çözümler sunması sayesinde bireylerin evlerine erişimi kontrol etme şeklini değiştirme potansiyeline sahiptir.

Akıllı kapı kilitlerinde yaygın olarak giriş erişimi için kimlik kontrolü yapılmaktadır. Erişim izni olan benzersiz kimlik, kullanıcının kilide erişmek için özel sensörler tarafından algılanıp doğrulanması gereken bir kod veya nümerik girişi yapılan bir şifre olabilir (Huang vd., 2022). Kimlik doğrulama yöntemi, ev otomasyon sistemlerinde en yaygın olarak kullanılan yöntemdir ve kullanıcıların fiziksel anahtarlara ihtiyaç duymadan aile üyelerine, arkadaşlara veya hizmet sağlayıcılara erişim izni vermesine olanak tanır (Huang vd., 2022). Bununla birlikte, bu kimlik doğrulama yöntemi, erişim yetkisi olmayan bir bireyin veya potansiyel bir saldırganın erişim kodunu gözlemleyebilmesi veya kırabilmesi durumlarında saldırılara karşı savunmasızdır (Pierrou ve Lantz, 2022). Bu riskleri azaltmak için akıllı kapı kilidi üreticileri, ek bir güvenlik katmanı sağlamak için biyometrik tanımlama veya 2FA (two-factor authentication) gibi daha gelişmiş kimlik doğrulama yöntemlerini kullanmaya başlamıştır (Wang vd., 2022).

Bilgisayarlı görü içeren teknolojilerin akıllı kilitlerde kullanımı görsel kameralar ile mümkündür. Görsel kameralar, kullanıcıların yüzü gibi biyometrik tanımlayıcıların görüntülerini yakalamak için kullanılır. Uygulamaya özel geliştirilen bilgisayarlı görü algoritmaları, kamera ile yakalanan görüntüleri önceden var olan bir veritabanıyla karşılaştırmak için kullanabilir. Akıllı kapı kilitleri için kimlik tanımlamaya dayalı kimlik doğrulama yöntemleri çeşitli avantajlar sunarken dezavantajları da vardır (Paul vd., 2019). Örneğin, tanımlama tabanlı kimlik doğrulama yöntemleri, parola tahmin etme, sosyal mühendislik ve kimlik avı gibi çeşitli saldırı türlerine karşı savunmasız olabilir (Mathew ve Divya, 2017). Ek olarak, birçok kullanıcı, biyometrik verilerinin veya kişisel bilgilerinin bilgisayar korsanları veya diğer yetkisiz taraflarca erişilebilecek bir veritabanında saklanmasından rahatsız olabilir (Jain ve diğerleri, 2016). Ayrıca, özellikle yüz tanıma veya parmak izi taraması gibi biyometrik tanımlama yöntemleri kullanılırken, tanıma dayalı kimlik doğrulama yöntemleri her zaman doğru olmayabilir (Arora ve Bhatia, 2022). Yetersiz aydınlatma, görünümdeki değişiklikler veya fiziksel yaralanmalar gibi faktörler bu yöntemlerin doğruluğunu etkileyerek yanlış negatiflere veya yanlış pozitiflere yol açabilir. Son olarak, akıllı kapı kilitleri için tanımlamaya dayalı kimlik doğrulama yöntemleri, geleneksel kilit ve anahtar sistemlerinden çok daha pahalı olabilir.

Görsel parolalar, kullanıcının biyometrik tanımlama yerine belirli bir görüntü veya renk dizisi girmesine dayanan akıllı kilitler için alternatif bir kimlik doğrulama yöntemidir (Renaud ve De Angeli, 2009). Görsel parolaların potansiyel avantajlarından biri, kullanıcıların hatırlamalarının daha kolay olabilmesidir. Görsel parola kimlik doğrulamasını kullanan akıllı kapı kilitleri, geleneksel kilit sistemlerine popüler bir alternatif haline gelmektedir. Grafik kriptografiye dayalı güvenli bir görsel şifre şeması, akıllı kilit sistemlerinde güvenliği artırmanın etkili bir yoludur (Vivek vd., 2020). Bu kimlik doğrulama yöntemi, kullanıcının kapının kilidini açmak için bir dizi görüntü seçmesine dayanmakta ve yetkisiz kişilerin erişimini zorlaştırmaktadır. Ayrıca olası şifre kombinasyonlarının sayısının çoğaltılarak güvenliğin arttırılması mümkündür (Andriotis vd., 2022). Akıllı kapı kilitlerinde görsel parola doğrulamanın kullanılması, ev güvenliğini iyileştirmek için umut verici bir yaklaşımdır.

Bu çalışmada düşük maliyetli standart bir elektrikli kapı kilidinin giriş erişimi için çeşitli yüz ifadeleri ve el hareketlerinin görsel şifre olarak kullanıldığı bir uygulama gerçekleştirilmiştir.

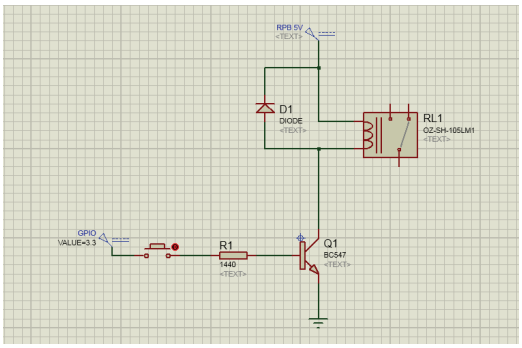
Gerçek zamanlı görüntü işleme ve mimik tespiti için OpenCV (Bradski, 2000), Mediapipe (Lugaresi vd., 2019) ve CVZone (CVZone, 2022) kütüphaneleri kullanılmış, bu kapsamda geliştirilen bir mimik sıralama algoritması ile görsel şifre tespiti yapılmıştır. Geliştirilen algoritmalar Raspberry Pi platformu üzerinde çalıştırılmış ve uygun görsel şifre tespit edildiğinde kapı kilidine erişim sağlandığı farklı ortamlarda yapılan testlerle doğrulanmıştır.

## METODOLOJİ

Çalışmamızda yüz ve el hareketleri görsel şifre olarak kullanılmaktadır. Bir elektrikli kapı kilidi erişiminin görsel şifrelerle sağlanabilmesi için görüntülerin algılanıp işlenmesi, yüz ve el hareketlerinin gelişmiş bilgisayarlı görü algoritmaları ile izlenip kategorize edilmesi ve son olarak doğru şifre tespit edildiğinde elektrikli kapı kilidinin tetiklenmesi gerekmektedir. Bu süreçlerin gerçek zamanlı olarak işletilebilmesi için donanım platformu olarak Raspberry Pi-4 8GB - Model 4B; yazılım araçları olarak da Python programlama dili, Mediapipe, OpenCV ve CVZone kütüphaneleri kullanılmıştır. Yazılım araçları ile kameradan yakalanan görüntüler gelişmiş görsel nesne sezimi algoritmalarıyla gerçek zamanlı olarak değerlendirilmekte ve uygun parola girişi olup olmadığı tespit edilmektedir. Doğru parola girişi yapıldığında kapı kilidi tetikleme devresi ile kilidin açılması sağlanmaktadır. Uygulama için tasarlanan yöntemin detayları ilerleyen alt başlıklarda özetlenmiştir.

### Elektrikli Kapı Kilit Sistemi Tetikleme Mekanizması

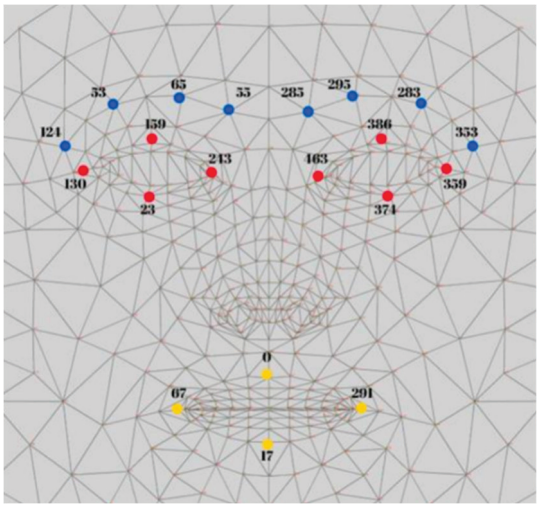
Görsel şifrenin başarılı olduğu durumlarda kapı kilidinin tetiklenmesi Şekil 1'de verilen devre ile gerçekleştirilmektedir. Bu devre Raspberry Pi'in çıkış pinlerine bağlı olup, kapıyı açtıktan bir süre sonra tetikleme devresine verilen gerilimi kesmektedir. Tetikleme işlemi, devrede *RL1* olarak gösterilen 16A minyatür güç rölesi tarafından gerçekleştirilir.




**Şekil 1.** Elektrikli kapı kilidi tetikleme devresi şeması

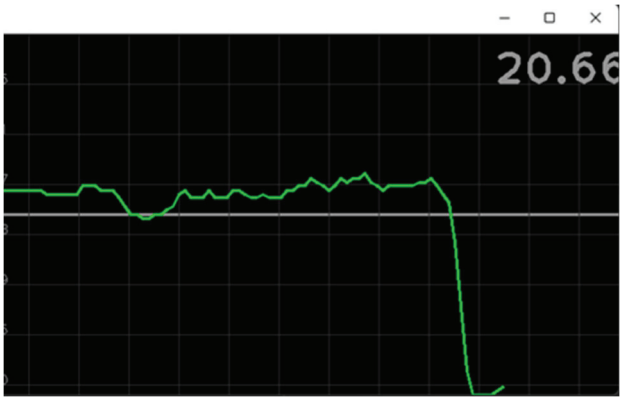
### Mimik Tanıma ve Hedef Mimiklerin Tespiti

Hedef mimiklerin ve el hareketlerinin tespit edilme süreci çalışmanın en önemli bileşenidir. Kameradan alınan gerçek zamanlı görüntüden yüz mimiklerin tespiti için Mediapipe kütüphanesi tarafından sağlanan FaceMesh modeli kullanılmıştır (Kartynnik vd., 2019). Modelde yüze ait 468 adet döndürülen noktadan Şekil 2'de gösterilen 20 nokta, yüz nirengi noktaları olarak seçilmiş ve bu noktalar kullanılarak hazırlanan algoritma ile kullanıcının kameraya gösterdiği mimiklerin tespiti yapılmıştır.




**Şekil 2**. Yüz mesh haritasında mimik tespiti için seçilen nirengi noktaları

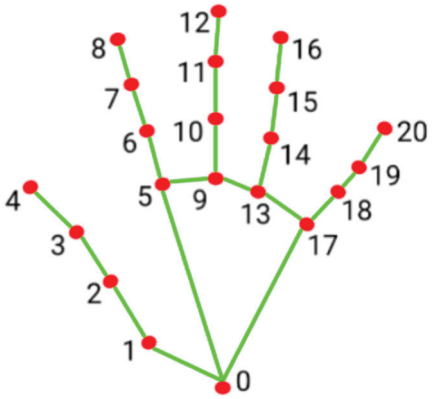
Yüz mimiklerinden kaş kaldırma, göz kırpma, gülümseme ve ağız açma hareketleri parola hareketleri olarak seçilmiştir. Göz kırpma hareketinin tespitinde Kuwahara vd. (2022) önerdiği Eye Aspect Ratio (EAR) özniteliği kullanılmıştır. Şekil 3'te özetlenen bu öznitelik göz yüksekliği ve genişliği ile ilgili bir oran değeridir. Açık bir göz yüksek bir EAR oranı verir, göz kapatıldığında EAR oranı düşmektedir. Bu yöntem hedeflediğimiz diğer mimiklerin tespitinde de kullanılmıştır. Her mimik için bu oranlar ayrı ayrı hesaplanmıştır ve ilgili aralıklarda hedef mimiklerin gerçekleştiği tespit edilmiştir.




**Şekil 3.** Göz kırpma anında değişen EAR oranı

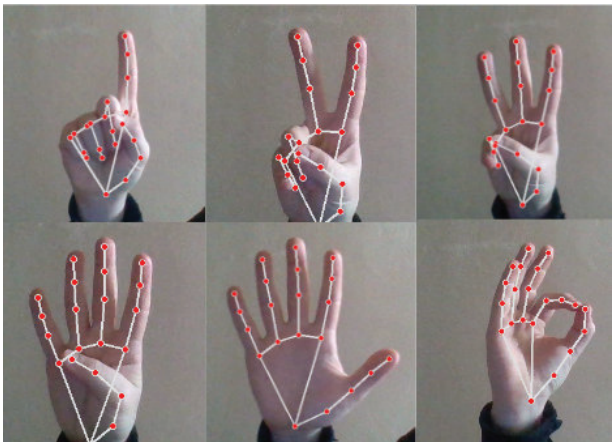
**El Hareketlerinin Tespiti**

Bu çalışmada tasarlanan akıllı kapı kilidi sistemine görsel şifre çeşitliliğini ve güvenliği arttırmak amacı ile görsel şifre olarak yüz mimiklerine ilave olarak el hareketleri de eklenmiştir. Bu amaç doğrultusunda MediaPipe Hands kütüphanesi kullanılmıştır (Zhang vd., 2020). Şekil 4'de çalışmada el tespiti sonucunda kullanılan noktalar gösterilmektedir.




**Şekil 4.** El hareket tespiti için kullanılan nirengi noktaları

El nirengi noktalarının konumları kullanılarak, EAR özniteliklerine benzer biçimde çok sayıda el hareketi tespit edilebilir. Bu çalışmada tek el ile yapılabilen ve Şekil 5'de gerçek görseli gösterilen 0-1-2-3-4-5 rakam el hareketleri görsel şifre olarak seçilmiştir. Bu görsel şifreler sağ el veya sol el hareketi olarak ayrıştırılarak kullanılabileceği gibi, sağ elle yapılan bir rakamı veya sol elle yapılan bir rakamı "aynı görsel şifre: bir rakamı" olarak da algılanabilir. Bu çalışmanın yazılım tasarımında, hareketler için el ayrımı yapılmamıştır; sağ el veya sol el için aynı rakam işareti aynı şifre olarak tasarlanmıştır. Daha yüksek güvenlik sağlamak için hareketin hangi elle yapıldığı ayrıştırılarak, örneğin "sağ elle gösterilen bir rakamı" veya "sol elle gösterilen bir rakamı" biçiminde kullanılabilir.

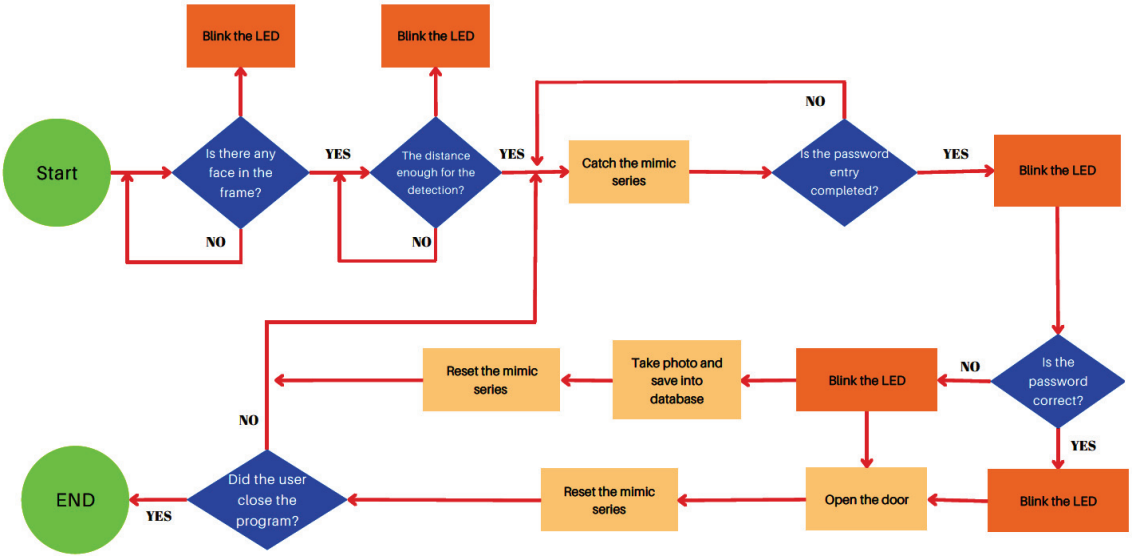


**Şekil 5.** Gerçek ortamda el hareketlerinin tespiti

## Yazılım Tasarımı

Görsel şifre tespitine dayalı elektrikli kapı kilidi erişiminde tasarladığımız yazılım süreci, akış diyagramı Şekil 6'da özetlenen temel algoritma ile gerçekleştirilmiştir. Algoritma çalışmaya başladığında kamera kadrajında herhangi bir insan olup olmadığını kontrol eder. Bu kontrol bize herhangi bir kullanıcının kameraya erişmeye çalışıp çalışmadığı bilgisini verir. Eğer kullanıcı kameraya yeterince yaklaşırsa kamera kullanıcının mimiklerini yakalamaya başlar. Kameranın yakaladığı mimikler ve hareketler depolanır ve ardışıl tekrar etmeyen hareketler ile şifre basamakları oluşturulmaya başlanır. Sonuç doğru olduğunda Rapsberry Pi tarafından tetikleme devresi çalıştırılır ve kapı açılır. Eğer sonuç yanlış olursa akıllı kilit sisteminin güvenilirlik ve sürekliliğini sağlamak için hazırlanan kontrol çalışır.

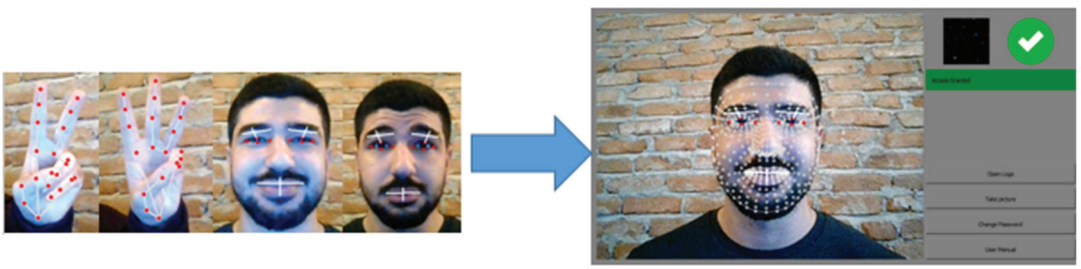
Bu kontrol ile şifreyi yanlış giren kullanıcının fotoğrafı veritabanına tarih ve saat bilgileri ile kaydedilir. Kullanıcı istediği zaman arayüzü kullanarak şifreyi güncelleyebilir.




**Şekil 6.** Tasarlanan algoritma ve ana program akış diyagramı

## Görsel Şifreler

Kameradan alınan gerçek zamanlı yakalanan kullanıcı görüntüleri ile yöneticinin arayüz üzerinden istediği zaman değiştirebildiği güncel görsel şifre karşılaştırılmaktadır. Güvenlik açısından aynı görselin ardışıl olarak tekrar edilmediği görsel el hareketleri veya yüz mimikleri kombinasyonundan oluşan bir görsel hareket grubu, aktif görsel parola olarak kullanılabilir. Görsel hareketlerin parola olabilmesi için en az bir görsel hareket kullanılmalıdır. Yönetici, görsel şifre olarak ikiden daha büyük basamaklı şifreler için yan komşuluğunda farklı bir görsel mimik içeren bir hareket serisini atayabilir. Şekil 7'de, 4 ardışıl mimik hareketi içeren 4 basamaklı bir görsel şifre gösterilmiştir. Algoritma her adımda basamak kontrolü yapıp sonucunda gelen veriyi ilgili basamağa eklemesi ve sonrasında diğer basamağa şifre yerleştirmek için beklemesi prensibine göre kodlanmıştır. Kullanıcının kamera karşısında gösterdiği mimikler, yöneticinin önceden belirlediği görsel şifreyle, gelen akış zincirine göre basamak basamak karşılaştırılmaktadır. Kullanıcının kamera karşısındaki görsel hareketleri akış zinciri, şifre olarak atanan seriye eşdeğer olacak sıralamayla yakalandığında erişim yetkisi verilmektedir.



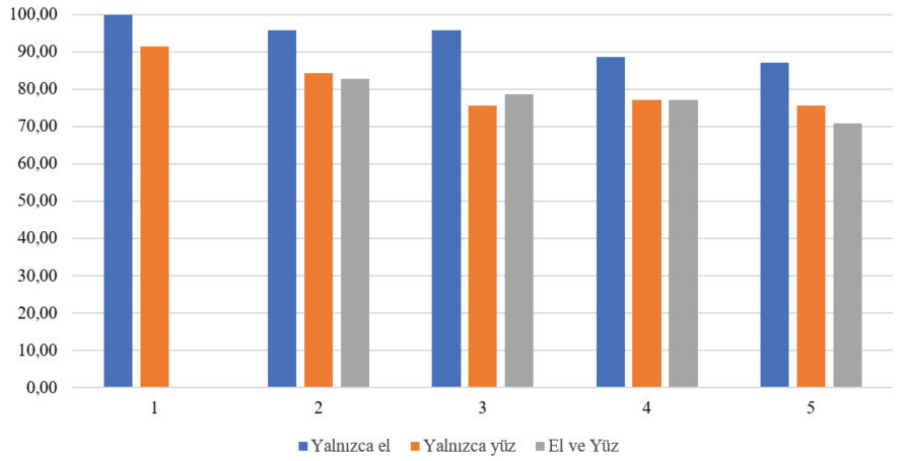
**Şekil 7.** Dört basamaklı olarak tanımlanan ve arayüzde doğrulanan örnek bir görsel şifre

## BULGULAR

Çalışmada önerilen yöntemin gerçek ortamda verimliliğini tespit etmek için çeşitli testler yapılmıştır. Bu testler, katılımı gönüllülük esasına dayalı 14 farklı bireyin farklı zamanlarda, iç mekân-dış mekân karışık olarak farklı ortamlarda, her bir bireyin farklı zamanlar için çok sayıda denemeleri üzerinden, farklı sayıda görsel şifre basamakları için yapılmıştır. Katılımcılar farklı zaman ve ortamlarda testler alabilmek için kolayca ulaşabileceğimiz yakın çevremizdeki farklı yaş ve cinsiyetlerdeki aile bireyleri ve arkadaşlardan seçilmiştir. Her bir test öncesi uygulama bireylere anlatılmış, deneklerin ilk denemeleri danışman eşliğinde yaptırılmıştır. Bireyler hazır olduklarını söylediklerinde, danışman müdahalesi olmadan erişim yapmaya çalışmışlardır. Bu aşamada danışman deneme sonucunu deney tablosuna not almaktadır. Deneylerde 1, 2, 3, 4 ve 5 ardışık hareket için farklı görsel şifreler (a) sadece el hareketleri; (b) sadece yüz mimikleri; (c) el-yüz karışık olacak biçimde test edilmiştir. Her şifre basamağı için en az 5 farklı görsel şifre kombinasyonu denenmiştir. Denemeler sonucu ilgili bireyin doğru erişim başarı oranları tablolaştırılmıştır. Deneyler sonucunda elde edilen başarı değerlerinin ortalamaları özet olarak Tablo'da verilmektedir. Tablodaki değerler yüzde cinsinden doğru başarı oranlarını göstermektedir. Tablonun ilk üç satırında verilen değerler, Şekil 8'de sütun grafiği olarak özetlenmiştir.

**Tablo.** Uygulamayı test eden bireylerin ortalama başarım oranları

| Görsel şifre uzunluğu (ardışıl mimik sayısı) | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|
| Yalnızca el hareketleri içeren parolada ortalama başarım değeri (%) | 100,00 | 95,71 | 95,71 | 88,57 | 87,15 |
| Yalnızca yüz mimikleri içeren parolada ortalama başarım değeri (%) | 91,43 | 84,29 | 75,71 | 77,14 | 75,71 |
| El-yüz karışık mimik içeren parolada ortalama başarım değeri (%) | ----- | 82,86 | 78,57 | 77,15 | 70,77 |
| **Ortalama** | **95,72** | **87,62** | **83,33** | **80,95** | **77,88** |




**Şekil 8.** Kullanıcıların farklı uzunluktaki görsel şifre doğru giriş ortalama değerleri (%)

Tablo incelediğinde göze çarpan ilk sonucun, yalnızca el kombinasyonları içeren görsel şifreler için başarım değerlerinin, yalnızca yüz mimikleri içeren durumdan ve el-yüz karışık olarak kullanıldığı durumdan daha yüksek değerlerde olduğudur. Bunun en önemli nedeni olarak insan elinin karakteristiğinin insan yüzünden daha düşük seviyede farklılık göstermesidir. Farklı insanların sergilediği Şekil 5'de verilen el hareketleri, birbirinden daha kolay ayrıştırılabilmiştir. Sadece bir el hareketi olarak belirlenen görsel şifrede %100 doğruluk oranı ile görsel şifre başarılı bir biçimde algılanmıştır. Bu oran bir yüz mimiği için %91,43'e düşmektedir. Yüz mimiklerinin tespiti EAR oranı eşik değeri üzerinden belirlenmektedir ve bu oran örneğin fazla çekik gözlü veya gözlerini kısarak bakan bireyler için gözün kapalı/açık olduğu durumlarda çelişkili çıktılar üretebilmektedir. Başarım oranındaki düşüş, yüz mimiklerin ayrıştırılabilirliğinin daha zor olmasıyla açıklanabilir. El hareketlerinin ve yüz mimiklerinin karışık olarak tanımlandığı parola doğrulaması başarımının yalnızca el ve yalnızca yüz içeren parola durumu arasındaki değerlerde olması beklenirken, sonuçlar şaşırtıcı biçimde sadece el hareketleri veya sadece yüz mimikleri kullanıldığı durumdan biraz daha düşük çıkmıştır. Deneyler sırasında bunun bir nedeni olarak deneklerin bu karışık hareketleri yapmaya çalışırken sadece el veya sadece yüz kullanılan duruma göre daha zorlanmaları, bir diğer nedeni ise el ve yüz aynı anda kadraja girdiğinde, özellikle el hareketi gerçekleştirmeye çalışırken farkında olmadan gülümseme ve göz kırpma mimiklerini de sergilemesi sonucunda şifre serisinin bozulması olarak gözlenmiştir. Bir diğer önemli genel çıkarım ise şifre basamak sayısının arttığında tüm durumlar için başarım oranlarının düşmesidir. Test edilen üç durum için ortalama başarım değerleri bir basamaklı şifre için %95,72 iken, iki basamaklı şifre için %87,62'ye, üç basamaklı şifre için %83,33'e, dört basamaklı şifre için %80,95'e, beş basamaklı şifre için %77,88'e gerilemektedir. Deneysel ortamda, görsel şifre uzunluğu arttıkça, bireylerin ardışıl olarak bu görsel şifreyi sergilerken zorlandıkları gözlenmiştir. Ayrıca az önce ifade edildiği gibi nadir de olsa bireylerin geçerli şifreyi sergilerken farkında olmadan aralarda göz kırpma ve gülümseme mimikleri yaptıkları gözlenmiştir. Bu mimikler şifre serisini bozduğu için yanlış tanıma olarak etiketlenerekbaşarım oranını düşürmektedir. Beş basamaktan daha uzun şifreler tanımlandığında, deneklerin bu şifre serilerini hatırlamada zorlanmaya başladıkları, sıralamada da insan hataları nedeniyle karışıklık yaşadıkları gözlenmiştir. Bu yüzden altı veya daha büyük uzunluklardaki şifre testleri yapılmamıştır. Bu uygulama için de tavsiye edilmemektedir. Beş basamak için yalnızca el hareketleri içeren parolada başarım oranları ortalaması %87,15; yalnızca yüz mimikleri içeren parolada başarım oranları ortalaması %75,71; karışık mimikler içeren parolada başarım oranları ortalaması %70,77; genel başarım ortalaması ise %77,88 olarak hesaplanmıştır. Bu değerler, tüm kategorilerde %75 üzerinde olması sebebiyle genel anlamda yeterli başarım olarak kabul edilebilir. Yalnızca el mimikleri kullanılması durumu ise beş basamak uzunluğundaki bir parola için bile %85'in üzerindedir.

## TARTIŞMA VE SONUÇ

Bu çalışmada, Raspberry Pi üzerinde gerçek zamanlı olarak çalıştırılabilen görsel şifre doğrulama özelliğine sahip bir elektrikli kapı kilidi giriş sistemi tasarlanmıştır. Tasarımda kullanılan görsel şifreler el hareketleri ve yüz mimiklerinden oluşmaktadır. Görsel şifreler, kullanıcı kimliğinden bağımsız olduğu için yeni üyelerin gelmesi veya mevcut üyelerin ayrılması gibi durumlarda veri tabanı güncellemesi, yeniden eğitim yapılması gibi karmaşık süreçler içermemektedir. Bireyler anahtardan bağımsız, klavye veya tuş takımı gibi ekipmanlara temas etmek zorunda olmadan, yalnızca kamera karşısında önceden tanımlanan görsel parolayı el hareketleri veya yüz mimikleriyle sergileyerek kapı kilidini açabilmektedir. Raspberry Pi 4 Model B üzerinde çalıştırılan sistem kolayca taşınabilmekte ve ucuz maliyetli herhangi bir elektrikli kapı kilidine monte edilebilmektedir.

Görsel şifreler üzerinden erişim başarımı farklı bireylerin katılımıyla farklı ortam koşullarında ve farklı uzunluklarda olan görsel şifrelerle test edilmiştir. Yapılan testler sonucunda, sadece el hareketlerinin görsel şifre olarak kullanılması durumunda, sadece yüz hareketlerinin görsel şifre olarak kullanıldığı durumdan ve el-yüz mimikleri karışık olarak kullanıldığı durumdan daha başarılı sonuçlar verdiği gözlenmiştir. En düşük başarım ise yüz ve el hareketlerini karışık olarak içeren şifrelerde gözlenmiştir. Buradan, sadece el hareketleri içeren görsel şifrelerin, diğer görsel şifrelere göre daha kolay ayrıştırılabilir olduğu söylenebilir. Şifre uzunluğunun artmasıyla birlikte görsel şifrelerin doğru tespit edilebilme başarımlarında bir miktar azalma görülmüştür. Bunun bir nedeni insan kaynaklı uzun şifreleri doğru sıralamayla hatırlayabilme hatasının artması, bir başka nedeni bireylerin farkında olmadan şifre serisini bozacak bir yüz mimiği sergilemeleri, bir diğer nedeni ise bireylerin fiziksel özelliklerinin farklı olması sebebiyle özellikle yüz mimiklerinin doğru ayrıştırılamaması olarak özetlenebilir. Tüm bu olumsuzluklara rağmen doğru tanıma başarımları genel ortalamalar üzerinden değerlendirildiğinde en iyi sonuç olarak tek basamaklı görsel şifre tespiti başarım oranı %95,72; en kötü sonuç olarak da beş basamaklı görsel şifre tespiti başarım oranı %77,88 olarak elde edilmiştir. Bu değerler, yeterli başarım oranları olarak kabul edilebilir. Daha yoğun giriş çıkışların yaşandığı ortamlar için veya yüksek oranlarda erişim ihtiyacı mevcut olduğu durumlarda uzun olmayan ve yalnızca el hareketleri içeren görsel şifrelerin tercih edilmesi daha uygun olacaktır.

## BİLGİLENDİRME

Bu çalışma 2209-A Üniversite Öğrencileri Araştırma Projeleri Destekleme Programı kapsamında TÜBİTAK tarafından desteklenmiştir.

## KAYNAKÇA

Andriotis, P., Kirby, M., & Takasu, A. (2022). Bu-Dash: a universal and dynamic graphical password scheme (extended version). International Journal of Information Security, 1-21.

Arora, S., & Bhatia, M. P. S. (2022). Challenges and opportunities in biometric security: A survey. Information Security Journal: A Global Perspective, 31(1), 28-48.

Bradski, G. (2000). The OpenCV Library. Dr. Dobb's Journal of Software Tools.

Chakraborty, P., & Sultana, S. (2022). IoT-based smart home security and automation system. In Micro-Electronics and Telecommunication Engineering: Proceedings of 5th ICMETE 2021 (pp. 497-505). Singapore: Springer Nature Singapore.

CVZone (2022), https://github.com/cvzone/cvzone.

Dawn, S., Bhowmick, A., Bhowmik, S., & Mandal, S. (2023). Smart Door: A Modern Approach to Control Door using Artificial Intelligence. American Journal of Electronics & Communication, 3(3), 6-10.

Govindraj, V. J., Yashwanth, P. V., Bhat, S. V., & Ramesh, T. K. (2020, June). Smart door using biometric NFC band and OTP based methods. In 2020 International Conference for Emerging Technology (INCET) (pp. 1-4).

Huang, H. Y., Fanjiang, Y. Y., Hung, C. H., & Lee, C. A. (2022, November). Design and Implementation of a Smart Intercom System through Web Services on Web of Things. In Telecom (Vol. 3, No. 4, pp. 675-691).

Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.

Kartynnik, Y., Ablavatski, A., Grishchenko, I., & Grundmann, M. (2019). Real-time facial surface geometry from monocular video on mobile GPUs. arXiv preprint arXiv:1907.06724.

Kuwahara, A., Nishikawa, K., Hirakawa, R., Kawano, H., & Nakatoh, Y. (2022). Eye fatigue estimation using blink detection based on Eye Aspect Ratio Mapping (EARM). Cognitive Robotics, 2, 50-59.

Lugaresi, C., Tang, J., Nash, H., McClanahan, C., Uboweja, E., Hays, M., ... & Grundmann, M. (2019). Mediapipe: A framework for building perception pipelines. arXiv preprint arXiv:1906.08172.

Mathew, M., & Divya, R. S. (2017, July). Super secure door lock system for critical zones. In 2017 International Conference on Networks & Advances in Computational Technologies (NetACT) (pp. 242-245).

Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multifactor door locking systems: A review. Materials Today: Proceedings, 46, 7973-7979.

Paul, P., Al Achib, M. A., Hossain, H. S., & Hossain, M. K. (2019). Smart Door Lock Using Fingerprint Sensor. BRAC University, 1-13.

Pierrou, T., & Lantz, E. (2022). Security evaluation of a smart door lock system.

Renaud, K., & De Angeli, A. (2009). Visual passwords: cure-all or snake-oil?. Communications of the ACM, 52(12), 135-140.

Saroha, A., Gupta, A., Bhargava, A., Mandpura, A. K., & Singh, H. (2022, July). Biometric Authentication Based Automated, Secure, and Smart IOT Door Lock System. In 2022 IEEE India Council International Subsections Conference (INDISCON) (pp. 1-5).

Venkata, N. Y. L., Rupa, C., Dharmika, B., Nithin, T. G., & Vineela, N. (2021, August). Intelligent Secure Smart Locking System using Face Biometrics. In 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) (pp. 268-273). IEEE.

Vivek, T. V. S., Rajavarman, V. N., & Madala, S. R. (2020). Advanced graphical-based security approach to handle hard AI problems based on visual security. International Journal of Intelligent Enterprise, 7(1-3), 250-266.

Wang, Z., Liu, D., Sun, Y., Pang, X., Sun, P., Lin, F., ... & Ren, K. (2022). A Survey on IoT-enabled Home Automation Systems: Attacks and Defenses. IEEE Communications Surveys & Tutorials.

Zhang, F., Bazarevsky, V., Vakunov, A., Tkachenka, A., Sung, G., Chang, C. L., & Grundmann, M. (2020). Mediapipe hands: On-device real-time hand tracking. arXiv preprint arXiv:2006.10214.