T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MOBİL SİSTEMLER ÜZERİNDE, BİYOMETRİK, NFC VE KONUM BİLGİLERİNİ KULLANARAK KİŞİ TANIMA

Zeynel Erdi KARABULUT

Danışman
Yrd. Doç. Dr. Mustafa Cem KASAPBAŞI

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL - 2018

KABUL VE ONAY SAYFASI

Zeynel Erdi KARABULUT tarafından hazırlanan **"Mobil Sistemler Üzerinde, Biyometrik, NFC ve Konum Bilgilerini Kullanarak Kişi Tanıma"** adlı tez çalışması 09/02/2018 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Bilgisayar Mühendisliği AnaBilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman	**Yrd. Doç. Dr. Mustafa Cem KASAPBAŞI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Doç. Dr. Serhat ÖZEKES** Üsküdar Üniversitesi	.....
Jüri Üyesi	**Yrd. Doç. Dr. Alper ÖZPINAR** İstanbul Ticaret Üniversitesi	.....

Onay Tarihi : 9./2./2018

Prof. Dr. **Necip ŞİMŞEK**
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

Tarih
09/02/2018

İmza

Zeynel Erdi KARABULUT

İÇİNDEKİLER

Sayfa

ÖZET

Yüksek Lisans Tezi

MOBİL SİSTEMLER ÜZERİNDE, BİYOMETRİK, NFC VE KONUM BİLGİLERİNİ KULLANARAK KİŞİ TANIMA

Zeynel Erdi KARABULUT

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Ana Bilim Dalı

Danışman: Yrd. Doç. Dr. Mustafa Cem KASAPBAŞI

2018, 45 sayfa

Mobil uygulamalar günümüzde oldukça popülerdir ve günlük hayatta önemli rol almaktadır. Bu çalışmada bulut tabanlı bir etkinlik davetli kontrol (kişi tanıma) mobil uygulaması gerçekleştirilmiştir. Bu geliştirilen uygulamada NFC, biyometrik sistemlerden yüz tanıma ve konum bilgilerini kullanarak kişi tanıma sistemi geliştirilmiştir. Geliştirilen mobil uygulamanın 4 modülü vardır. Bu modüller, Yüz tanıma modülü, NFC modülü, Konum modülü ve Tarih ve Saat modülüdür. Yüz tanıma modülünde Microsoft yüz API (Application Programming Interface), (SAAS(software as a service)) olarak kullanılmıştır. NFC modülünde ise her kullanıcıya ait sadakat kartı bilgileri uygulama tarafından okunarak kişi tanınır. Konum modülünde ise kontrolü yapan kullanıcı gerçekten etkinliğin yapıldığı mekânda mı değil mi bunun kontrolü yapılır. Tarih ve Saat modülünde ise etkinlik kontrolü doğru zamanda mı yapılıyor bunun kontrolü yapılır. Mobil uygulamasının yüz tanıma modülü Yale yüz veri tabanı ile test edilmiştir. Yale yüz veri tabanında 15 farklı kişinin 11'er fotoğrafı vardır. Bu çalışmadaki test için kullanılan resimler normal, normal ve merkez ışıklı, normal sol ışıklı ve sağ ışıklı, normal ve mutludur. Bu çeşitli resimleri geliştirilen uygulamanın yüz tanıma modülü ile test edilip confusion (karışıklık) matrisleri oluşturulmuştur. Yüz tanıma modülü'nün testinden sonra ortaya çıkan karışıklık matrisinde doğruluk oranı %100 çıkmıştır. Diğer çalışmalar da yapılan yüz tanıma algoritmalarıyla (Eigen Face, Fisher Face gibi) tez kapsamında geliştirilen yüz tanıma modülü karşılaştırılmıştır. Eigen Face, Fisher Face gibi algoritmalar ile geliştirilen uygulamalarda doğruluk oranı maksimum %97-%99 arasında değişmektedir.

Anahtar Kelimeler: Biyometrik, kişi tanıma, NFC, yüz tanıma.

ABSTRACT

M.Sc. Thesis

RECOGNIZE PERSON USING BIOMETRIC, NFC AND LOCATION INFORMATION ON MOBILE SYSTEMS

Zeynel Erdi KARABULUT

İstanbul Commerce University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Mustafa Cem KASAPBAŞI

2018, 45 pages

Mobile applications are very popular nowadays and play an important role in daily life. In this study, cloud based mobile application for invitee control (person recognition) application is implemented. In the developed application, NFC, face recognition from biometric systems and using location information a person recognition system has been developed. The developed mobile application has 4 modules. These modules are Face recognition module, NFC module, Location module and Date and Time module. Microsoft face API (Application Programming Interface), (SAAS (software as a service)) has been used in face recognition module. In the NFC module, the loyalty card information of the user is read by the application and the person is recognized. In the location module, the user who performs the control is checked whether it is in the place where the activity is actually performed. In the Date and Time module, the effectiveness check is done at the right time and it is checked. The face recognition module of the mobile application has been tested with the Yale face database. There are 11 photographs of 15 different people in Yale face database. In this study the pictures used for testing are normal, normal and center light, normal left and right lights, normal and happy. These various images were tested with the face recognition module of the developed application and confusion matrices were calculated. The accuracy of the confusion matrix after the facial recognition module test is 100%. Other facial recognition algorithms implemented in other studies (such as Eigen Face, Fisher Face) have been compared with the face recognition module developed in this thesis. In applications developed with algorithms such as Eigen Face, Fisher Face, the accuracy rate ranges from 97% to 99% at maximum.

Keywords: Biometric, face recognition, NFC, person recognition.

TEŞEKKÜR

Bu tez çalışmasının gerçekleşmesinde verdiği katkılardan dolayı ve danışmanım olarak tezin yazılmasında yol gösteren değerli hocam Yrd. Doç. Dr. Mustafa Cem KASAPBAŞI'na çok teşekkür ederim.

Zeynel Erdi KARABULUT

İSTANBUL, 2018

ŞEKİLLER

Sayfa

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR

API	Uygulama Programlama Arayüzü (Application programming interface)
ECMA	Avrupa bilgisayar üreticiler birliği (European computer manufacturers association)
EGM	Esnek grafik uyumu (Elastic graph matching)
FAR	Yanlış kabul oranı (False Accept Rate)
FN	Yanlış tahmin edile negative değer (False negative)
FP	Yanlış tahmin edilen pozitif değer (True positive)
FRR	Yanlış reddetme oranı (False reject rate)
ICA	Bağımsız bileşen analizi (Independent component analysis)
ID	Kimlik numarası (Unique id number, identity)
ISO/IEC	Uluslararası standartlar örgütü (international organization for standardization/ international electrotechnical commission)
JSON	Javascript nesne notasyonu (Javascript object notation)
LLCP	Mantıksal bağlantı protokolü (Logical link control protocol)
MCC	Matthews korelasyon katsayısı (Matthews correlation coefficient)
MRF	Markov rastgele alanı (Markov random field)
NDEF	NFC veri alışveriş formatı (NFC data exchange format)
NFC	Yakın alan iletişimi (Near field communication)
NFCIP-1	Yakın saha iletişimi arayüzü protokol-1 (near field communication interface and protocol-1)
NFCIP-2	Yakın saha iletişimi arayüzü protokol-2 (Near field communication interface and protocol-2)
PCA	Prensip bileşen analizi (Principle component analysis)
PIN	Kişi kimlik numarası (Personal identification number)
RFID	Radyo frekans tanımlama (Radio frequency Identification)
ROM	Sadece okunabilir bellek (Read only memory)
SAAS	Servis olarak yazılımı kullanma (Software as a service)
SNEP	Basit NFC alışveriş format protokolü (simple NDEF exchange protocol)
SVM	Destek vektörü makinesi(Support vector machine)
TN	Doğru tahmin edilen negatif değer (True negative)
TP	Doğru tahmin edilen pozitif değer (True positive)

1. GİRİŞ

Mobil cihaz kullanımındaki oran gün geçtikçe artmakla birlikte, artık mobil cihazlar günlük hayatın vazgeçilmez bir parçası haline gelmektedir. Mobil teknolojilerin hızlı gelişim içinde olması ve artan yoğun ilgi de göstermektedir ki her geçen gün mobil uygulama ve sistemleri kullanılan tekniklerin yerini alacaktır.

Bu tez çalışmasında, ilk iki bölüm de biyometrik sistemler ve NFC (Near field communication) teknolojisinden bahsedilmiştir. Bu bölümler de biyometrik sistemler ve NFC teknolojisi kısaca anlatılmıştır.

Bu tez kapsamında bir mobil Android uygulaması geliştirilmiştir, bu uygulama etkinlik davetli kontrol uygulaması olarak düşünülse de birçok farklı alanda uygulana bilinecek bir alt yapı oluşturulmuştur. Hatta lojistik uygulaması için senaryolar üretilmiştir. İlerleyen bölümler de lojistik sektörü için, geliştirilen mobil uygulama üzerinden üretilen senaryolara detaylı değinilmiştir. Etkinlik davetli kontrol uygulaması özellikleri, biyometrik sistemlerden yüz tanıma, akıllı kart sistemlerinden NFC kart bilgisini okuma ve yazma, etkinliğin yapıldığı mekânın konum bilgisi ile kontrol işlemini yapan mobil uygulama kullanıcısının konum bilgilerini karşılaştırma (gerçekten kullanıcı bu etkinliğin yapıldığı yerde mi etkinlik kontrol işlemini yapıyor diye). Son olarak da etkinlik kontrol işlemi etkinliğin yapılacağı tarihte mi yapılıyor onun kontrolü yapılır ve kişi tanıma işlemi başarıyla tamamlanmış olur. Bu uygulama da, öncelikle kullanıcı sisteme e-mail ve şifresiyle kayıt olur, sonra sisteme giriş yapar, kullanıcı giriş yaptıktan sonra etkinlik davetli kontrolü yapmak için bir etkinlik oluşturur ve bu etkinliğe davet edeceği kişilerin adlarını, en az 1 tane fotoğrafını ve etkinlik tarihini mobil uygulamadan kaydeder. Böylece etkinliğe katılacak kişiler mobil uygulama üzerinden kontrol edilebilir. Ayrıca, bu uygulamada yapılan etkinlik davetli kontrol işlemi, yüz tanıma ile yapıldığı gibi NFC kartlar üzerinden de yapılabilir. Kullanıcı etkinlik oluşturduktan sonra etkinliğe katılacak kişilerin bilgilerini uygulama üzerinden NFC teknolojisini kullanarak NFC kartlara yazar, böylece davetli kişileri NFC kartlar ile de kontrol edebilir. Etkinliğin yapıldığı yer ve etkinliğin yapılacağı zaman dışında uygulama üzerinden kontrol yapılamaz, etkinliğin yapılacağı konum ve tarihinde, davetli kişi kontrol sistemi gerçekleştirilir.

Tezin son bölümünde, araştırmalar ve bulgular bölümünde testler yapılmış ve bazı sonuçlar elde edilip bu sonuçlar değerlendirilmiştir.

2. LİTERATÜR ÖZETİ

Günümüzde NFC teknolojisinin kullanıldığı MiFare kartları ve NFC özellikli cep telefonları ile çeşitli uygulamalar geliştirilmiştir. Bu uygulamalara örnek olarak giriş/çıkış işlemlerinin kontrolü, toplu taşımada ücret ödemesi, takvim senkronizasyonu ve elektronik kartvizit sistemleri verilebilir. Bu bölümde konu ile ilgili yapılan diğer çalışmalar incelenmiştir.

Deniz vd. (2003), bağımsız bileşen analizi ve destek vektör makineleri kullanılarak yüz tanıma çalışması yapılmıştır, yapılan bu çalışmada SVM+ PCA (Principle component analysis), SVM (Support vector machine)+ ICA (Independent component analysis) yöntemlerini kullanarak yüz tanıma sistemi gerçekleştirilmiştir. Bu geliştirilen yüz modülü, popüler Yale yüz veri tabanı ile test edilip yüz tanıma sisteminin doğruluk oranları elde edilmiştir.

Tang vd. (2003), yüz tanıma yapan makine adlı tez çalışması yapılmıştır, yapılan bu çalışmada geliştirilen yüz tanıma modülünde, Eigen face, Fisher face, EGM (Elastic graph matching) SVM ve yapay sinir ağları algoritmaları kullanılmıştır. Yüz tanıma yapan makine çalışmasında geliştirilen yüz tanıma modülünde bu tez kapsamında geliştirilen yüz tanıma modülü gibi Yale yüz veri tabanı ile test edilmiştir.

Huang vd. (2004), Markov random field algoritmasını kullanarak bir hibrit yüz tanıma sistemi yapılmıştır. Bu geliştirilen sistem de yüz tanıma algoritmalarından olan MRF (Markov random field) algoritmasını kullanarak, resimleri küçük parçalara ayırarak yüz tanıma sistemine tanıtmıştır. Ayrılan her parçaya daha sonra kolaylıkla kişi yüzü tanımak için bir ID (Unique id number, identity) vermiştir. Bu ID'lere göre yüz tanıma işlemi gerçekleştirmiştir. Bu geliştirilen uygulamanın yüz tanıma modülünde, yüz tanıma doğruluk oranı elde etmek için çeşitli yüz veri tabanları (Yale yüz veri tabanı gibi) kullanılarak test işlemleri yapılmıştır.

Antonia Rana ve Andrea Ciardulli (2013), Android akıllı telefonlarından NFC ve biyometrik sistemlerden yüz tanıma bilgilerini kullanarak kimlik doğrulama adlı çalışma yapılmıştır. Bu tez çalışmasında, NFC ve yüz tanıma ile kişi tanıma ve doğrulama yapılmıştır. Yapılan bu çalışmada kısıtlı sayıda test yapılmıştır, yani popüler güçlü yüz veri tabanlarından biriyle bu çalışma test edilmemiştir. Bu testlerin yapılmaması da uygulamanın güvenilirliğini bilinmez kılmaktadır.

Bir diğer NFC tez çalışması Narol (2014), bu çalışmada NFC teknolojisinin toplu ulaşımda uygulanması üzerine çalışma yapılmıştır. Toplu ulaşımda yüksek kaliteli, kolay erişilebilir ve kullanıcıların gereksinimlerini karşılayan, güvenli uygulamalar sunmak amacıyla temassız haberleşme, dijital, mobil teknolojiler ile temassız ödeme sistemi geliştirilmesi amaçlanmıştır. Toplu Ulaşım sektöründe, NFC uygulamalarının kullanılabilmesi için akıllı şehir uygulamalarına farklı bir bakış açısı sunulmaktadır. Temassız ödemeyi destekleyen akıllı kartlar, trenlerde, otobüslerde ve diğer bütün toplu ulaşım araçlarında elektronik bilet olarak kullanılması, kullanıcıları bilet almak için satış makinelerinde veya satış gişelerinde akbil kuyruğundan kurtarmaktadır. Bu sayede zamandan kazanç sağlanmaktadır. Aynı zamanda sistem üzerinde eş zamanlı veri girişi yaparak giriş-çıkış yapan araç bilgileri ve araçların ödeyecekleri miktar kayıt altında tutulmaktadır.

Adalan (2017), bu çalışma da yüz tanıma, NFC kart ve ses komutlarını kullanarak kapı kilidi açma sistemi için bir mobil Android uygulaması geliştirilmiştir. Bu uygulamada yeterli kullanıcı testleri yapılmamıştır, yüz tanıma modülünde fotoğrafı çekilen kişinin çeşitli tipte fotoğraflarına yönelik test çalışması yapılmamıştır (Örneğin; sol ışıklı veya sağ ışıklı fotoğraf gibi). Bu sebepten dolayı, ortam koşullarına bağlı olarak arka planın koyu renkte olması ve arka plandan alınan ters ışık ile birlikte referans noktaların yanlış koordinatları göstermesine yol açmaktadır.

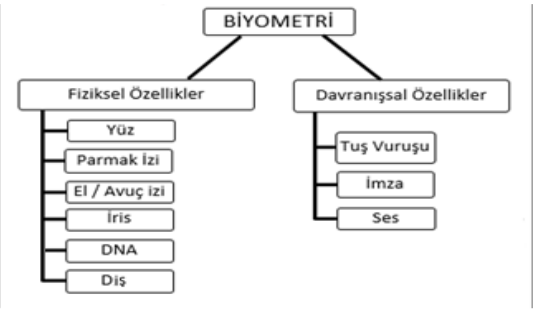
Bir diğer çalışma da, Assarasee vd. (2017), bu tez çalışmasında da Microsoft yüz API kullanılarak, kişilerin varlığını yüz tanıma ile izleyebilecek bir uygulama çatısı geliştirilmiştir. Bu çalışmada Microsoft'un yüz API'si kullanılarak sadece yüz tanıma işlemi üzerinden bir uygulama çatısı yapılmıştır. Bu çalışma da kişi tanıma sistemi için, NFC, konum ve tarih gibi önemli bilgiler kullanılmamıştır, basitçe sadece yüz tanıma uygulama çatısı geliştirilmiştir.

Yapılan literatür taramasında çoğunlukla NFC teknolojisini kullanarak temassız veri okuma sistemleri ve klasik yüz tanıma algoritmaları (Eigen face, Fisher face, EGM gibi) kullanarak kişi tanıma sistemleri üzerine çalışmalar yapılmıştır. Bu çalışmalarda geliştirilen uygulamaların sadece belirli bir alan üzerine odaklandığı gözlemlenmiştir.

3. BİYOMETRİK SİSTEMLER

Kullanıcının bir mobil cihazı üzerinden, kişinin kimlik bilgileri, kredi kartı numaraları ve şifreleri, adresi, telefonu, kişisel resim ve videoları, WhatsApp, Facebook, Twitter, İnstagram vb. sosyal ağlara giriş için kullandığı şifre ve kullanıcı adı bilgileri gibi birçok veriye erişilebilmektedir. Bu sebeple mobil cihazlarda güvenliği artırabilmek amacı ile şekilsel işaretli şifreler veya PIN (Personal Identification Number) kodu gibi basit yöntemlere başvurulmuştur. Ancak, güvenlik seviyesi bu basit yöntemlerde kullanıcı tarafından seçilen şifrenin zorluğuna göre belirlenmektedir. Kullanıcı çok basit bir şifre kullandığında kötü niyetli kişilerce ele geçirilen mobil cihazın şifresi çözülebilir. Rakam, noktalama işaretleri (nokta, virgül gibi) ve harf kombinasyonları ile ASCII karakterlerinden oluşturulan şifreler daha özellikli olduğundan tahmin edilmesi çok zordur ancak karmaşıklıklarından dolayı kullanıcı tarafından unutulabilir, kullanım açısından kullanışlı olmayabilir. Bu nedendir ki kullanıcı tarafından hatırlanması zorunlu olmayan ve aynı zamanda kişiyi ayırabilecek kadar belirli bir yöntem arayışı içine girilmiştir. Görülmektedir ki biyometrik sistemler, çoğunlukla güvenlik seviyelerini artırmak için, diğer kimlik doğrulama yöntemlerini geliştirmek için kullanılan tekniklerdir ve başarılı bir çözüm olarak gözükmektedir.

Biyometrik tanıma işlemi gerçekleştirilirken benzersiz olarak belirlenen insan özellikleri kullanılmakta olup biyometrik sistemler temelde 2 farklı grup üzerinden incelenmektedir. Bunlar fiziksel ve davranışsal özelliklerdir. Parmak izi, DNA, retina, iris vb. gibi insan vücudunun bir bölümünün doğrudan ölçümlenmesi ile uygulanan sistemler fiziksel özellikler kullanılarak tasarlanan biyometrik sistemlerdir. İmza, konuşma, yürüyüş vb. özellikler üzerinden dolaylı olarak doğrulama işlemleridir (Arslan ve Sağıroğlu, 2016).



Şekil 3.1. Biyometrik sistemler (Arslan ve Sağıroğlu, 2016)

3.1. Biyometri

Biyometrik sistemlerin kullanılmaya başlamasıyla kimlik doğrulama işlemlerinde büyük kolaylıklar sağlanmıştır. Kişiler herhangi bir bilgi ezberlemeden veya bir kartı yanında bulundurmadan kimlik doğrulayabilmektedirler (Şamlı ve Yüksel, 2009). Biyometrik sistemlerde kimlik doğrulama işlemleri kişinin biyometrik özellikleri kullanılarak yapılmaktadır. Bu nedenle başkasına verilmesi veya kaybolması gibi olaylar gerçekleşmemektedir.

Biyometrik tanıma sistemleri bireyleri birbirinden ayırabilme olanağı sunarak bireyin kim olduğunu doğrulamasına olanak sağlamaktadırlar Biyometrik sistemlerle daha güvenli sistemler geliştirilmektedir. Biyometrik sistemlerin çalışma prensibi; her yöntemin kendine özel cihazıyla alınan verilerin incelenip daha önceden kaydedilmiş verilerle karşılaştırılıp onaylanmasından oluşmaktadır (Kakıcı, 2008). Biyometrik sistemler de güvenlik çok önemli olduğu için geliştirilmiştir. Örneğin bir biyometrik tanıma sistemiyle DNA örneğinden suçlu kişi tespiti yapılabilmektedir.

3.2. Biyometrik Sistemlerde Kullanılan Yöntemler

Biyometrik sistemlerin yöntemleri iki kademeden oluşmaktadır. İlk kademede bireyin kimliğini belirleyen bilgiler sisteme ait araçlar kullanılarak alınmaktadır. Alınan bu bilgiler, yönteme ait kullanılan çeşitli algoritmalarla incelenmekte ve kişiyi tanımlayacak özellikler çıkarılarak veri tabanına kaydedilmektedir. Diğer kısım da ise bireyin sisteme ait aynı cihazla alınan bilgileri, sistemde kullanılan yönteme ait aynı algoritmalarla incelenmekte ve kimliğinin özellikleri elde edildikten sonra veri tabanında ki bilgilerle karşılaştırılmaktadır. Eğer eşleşme meydana gelirse bireyin kimliği doğrulanarak kimliği tespit edilmektedir. Biyometrik sistemler, algoritmalar, kullanılan çeşitli yöntemler ve cihazlar nedeniyle birbirinden çok farklılık göstermektedir (Kakıcı, 2008).

Biyometrik sistemler, bireyin fiziksel veya davranışsal özelliklerini (örneğin yüz, parmak izi, ses, imza, tuş darbesi ritimleri) analiz ederek kimliğinin benzersizliğini doğrulamaktadırlar. Günümüzde geçerli olan biyometrik tanıma sistemleri temel olarak iki grupta incelenmektedirler. Bunlardan birincisi; Fizyolojik Özellikler (Retina, Parmak İzi, Damar, El Geometrisi, Yüz, Ses, DNA) olarak bilinmektedir. Diğer grupta ise; Davranışsal Özellikler (Konuşma, Yürüyüş, İmza Atımı, Tuş Vuruşu) yer

almaktadır (Şamlı ve Yüksel, 2009).

3.2.1. Parmak izi tanıma

Parmak izi, insanlarda çok sıklıkla kullanılan taklit edilmesi imkânsız bir bilgidir. Parmak izi tanıma sistemleri için yazılım ve donanım alanlarında çok büyük gelişmelerin olması, bu sistemlerin hızlı ve kolay bir biçimce kullanılmasına sebep olmuştur. En temel parmak izi tanıma algoritmaları ayrıntı (Minutiae), korelasyon ve çizgi (ridge) tabanlı eşleştirme yöntemleridir. Korelasyon tabanlı eşleştirme yöntemleri, iki farklı çizgi modeli karşılaştırıldığından dolayı kayıt noktalarının yer bilgisini gerektirirler ve resmin döndürülmesinden etkilenmektedirler. Ayrıntı (Minutiae) tabanlı eşleştirme tekniğinde ise parmak izinin ayrıntı noktaları belirlenip ve bu belirlenmiş ayrıntı noktaları oluş sırasına göre karşılaştırılmaktadır. Çizgi tabanlı eşleştirme yönteminde ise çizgiye ait şekil ve yön özellikleri kullanılmaktadır. Ayrıntı ve çizgi tabanlı sistem teknikleri çok düşük çözünürlükteki parmak izi görüntülerinden ayrıntı ve çizgi özelliklerini çıkaramamaktadırlar. Bu sorundan dolayı ayrıntı ve çizgi tabanlı eşleştirme yöntemlerinde görüntü iyileştirme ve temizleme yöntemleri kullanılmaktadır (Sönmez ve diğer 2007).

Galton, insanlardaki parmak izinin genetik özellikte olamadığını ve herkesin parmak izlerinin birbirlerinden çok farklı olduğunu yapmış olduğu çalışmalarla belirtmiştir. Henry Faulds ise başka bir açıdan bakarak parmak izinin sınıflandırılmasına kesin olarak açıklık getirmiştir. Galton ve Henry'nin yapmış olduğu çalışmalar farklı türden sınıflandırmalar olsa bile sınıflandırma sistemlerinden ürünü olan yaygın olarak kullanılmaktadır (Kakıcı, 2008). Otomatik parmak izi tanıma sistemlerinde (OPTS) parmak izi tanıma işlemi, parmak izinden elde edilen özellik noktalarının ve bunlara ait verilerin karşılaştırılması ile gerçekleştirilmektedir (Şamlı ve Yüksel, 2009).

3.2.2. Yüz tanıma

Yüz tanıma sistemi en önemli biyometrik buluşlardan biridir. İlk olarak askeriye alanlarında kullanılarak geliştirilmiştir. İleri teknoloji silahlarında, caddelere yerleştirilen güvenlik kameralarıyla aranmakta olan bir suçlunun tespiti ve yakalanması gibi uygulamalarda kullanılmaktadır. Güvenlik amaçlı olarak yüz görüntülerinin otomatik olarak tanınması yaygın bir biçimde kullanılmaktadır (Şamlı ve Yüksel, 2009). Yüz tanıma işlemi kullanımı kolay olan bir yöntemdir. Yüz nitelikleri insanların birbirlerini tanımak için insanlar tarafından kullanılan en yaygın biyometrik

özelliklerdendir. Kimlik doğrulama işlemlerinde vesikalık fotoğraflar bile kontrol edilmekte ve yüz tanıma yöntemiyle kimlik tespiti gerçekleştirilmektedir. Yüz tanıma işlemleri iki metottan birine göre yapılmaktadır. İlk metotta gözler kaşlar, burun, dudak, çene ve yüz boşluklarının ilişkileri, ya da yüz niteliklerinin yeri ve şekline göre gerçekleştirilmektedir. İkinci metotta ise yüzü temsil eden yüz niteliklerinin analiz edilmesiyle yapılmaktadır (Jain vd., 2007). Otomatik bir yüz tanıma sisteminin doğru çalışabilmesi için, bir kişiden alınan görüntüde yüzün mevcut olup olmadığının tespit edilmesi, eğer varsa yüzün bulunması ve farklı koşullar altında (alınan herhangi bir çeşit resimden) genel bir bakışla yüzün tanınması gerekmektedir.

3.2.3. İris tanıma

İris tanıma sistemlerinin kullanım amacı, iris şeklinin bir ömür değişmemesi ve başka biyometrik sistemlere göre çok daha az zarar ve bozulacak bir özelliğe sahip olmasıdır. İris tanıma sistemi gözleri görmeyen, gözleri olmayan, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan insanlarda uygulanamamaktadır. Bu insanlar haricinde havalimanları gibi kişi kontrolünün çok önemli olduğu yerlerde çok yüksek bir başarı yüzdesi ile kullanılmaktadır (Şamlı ve Yüksel, 2009).

İris tarama biyometrik sistemleri bir kişinin kimliğini doğrulamak amacıyla, kişinin tüm yaşamı boyunca değişmeden kalan insan irisinin karakteristik özelliklerini kullanmaktadır. İris gözün renkli dairesinin veya pigmentli alanıdır, genellikle kahverengi, yeşil, gri veya mavi halkalar irisi oluşturmaktadır. İrisin insan bünyesinde çok iyi korunan ve yaralanmalardan çok az etkilenen bir yapısı vardır. Genellikle iris tarama işlemleri irise yakın özel güçlü özellikli bir kamerayla çekilen bir fotoğrafla başlamaktadır. Kullanıcı iris okuma cihazına ortalama bir metre mesafede durmak zorundadır. Kamera gözü aydınlatarak çok yüksek çözünürlükle bir fotoğraf çekmek için kızılötesi bir yansıtıcı kullanmaktadır. İrisin iç yüzeyindeki desenlerin karakteristik özelliklerinin haritasını çıkaran bir iris tarama algoritması kullanılmaktadır. İris desen bilgileri karmaşık ve birbirinden farklı 200'ün üzerinde özellik noktalarından oluşmaktadır (Femila ve Irudhayaraj, 2011). Bu eşsiz noktaları oluşturan halkalar radyal bir modda iris bölgesinin görüntüsünü veren doku içinde sınıflandırılmaktadır. Bir bireyin sağ ve sol göz yapıları da farklı olduğundan, iris tanıma teknolojileri bu özelliği de kullanarak yanlış biyometrik tanımaların önüne geçmektedirler.

3.2.4. Retina tanıma

Kişilerde retina tanıma işlemi, kişilerin göz bebeği arkasındaki damar tabakanın doğrulanarak kişinin tanınmasıdır. Kişilerin damar yapıları birbirlerinden farklı olmasına rağmen çeşitli hastalıklar sonucu damar ve göz yapısı değişerek damarları etkilediğinden çok fazla yaygınlaşmış bir yöntem değildir. Retina tanıma işleminde özelliklerin belirlenmesi esnasında kişinin belirli bir noktaya bakmaya zorunlu olması bu yöntemin çok az kullanılmasına neden olmaktadır (Kakıcı, 2008). İris tanıma teknolojisi ile birlikte, retina tarama teknolojisiyle çok güvenilir ve doğru bir biyometrik teknolojiyi oluşturmaktadır. Kullanılması en zor olan biyometrik tanıma sistemlerinden biridir. Kullanıcıdan bir başarı elde edilmesi için sabırlı olması gerekmektedir. Biyometrik sistemlerde kullanılan retina damarlarının desenleri kişiden kişiye ve tek yumurta ikizleri arasında bile benzersiz olduğu ispatlanmıştır. Kişi retina yapısı bir ömür boyunca değişmemektedir (Femila ve Irudhayaraj, 2011). Retina tarayıcı cihazı ile iyi bir görüntünün elde edilmesi için bir noktaya sürekli bakılması gerekmektedir.

Bu teknolojide eşsiz retina desenlerinin taranması için optik yansıtıcı yoluyla düşük yoğunluklu kızılötesi ışık kaynağı kullanılmaktadır. Damarlarla ilgili elde edilen bilgiler kaydedilmektedir. Retina tanıma sistemi, kişi kimlik tespiti ve doğrulaması işlemlerinde başarıyla uygulanmaktadır.

3.2.5. El yazısı tanıma

El yazısını oluşturan harflerin konum ve şekillerinin biçimleri birbirinden farklılıklar göstermektedir. Harflerin oluşturulma sırası, çizgi ve noktaların oluşturulma şekli de belirlenecek özellikleri oluşturmaktadır. Önceki yazılmış yazılardan kimlik tanıma işlemi yapıldığında bazı özellikler değiştiğinden, yazı yazılırken yapılan tespit işlemi daha doğru sonuçlar vermektedir. Diğer tanıma yönteminde kullanılan cihazlar farklı işler içinde kullanılabildiği halde el yazısı tanıma için üretilen cihazlar sadece bu amaçla kullanılmaktadırlar. Bu nedenle diğer cihazlara göre maliyetleri daha fazla olmaktadır (Kakıcı, 2008).

3.2.6. DNA tanıma

Bu tanıma sisteminde bireyin tırnak, deri parçası, saç, kan, sperm veya herhangi bir biyolojik özelliği elde edilerek hücre içerisindeki DNA molekülleri incelenmektedir.

Devletin güvenlik güçleri tarafından suçlu tespiti işlemlerinde kullanılmaktadır. Doğruluğu çok yüksek ve geçerli bir yöntemdir. Bununla birlikte kişinin biyolojik yapısında değişikliğin olması sonucu alınan DNA örneğinin kalitesi çok azalacağından inceleme yapılması zorlaşmaktadır (Şamlı ve Yüksel, 2009).

3.2.7. El geometrisi tanıma

El geometrisi tanıma işlemleri elin şekli, avuç içi boyutu, parmakların genişlikleri ve uzunlukları gibi insan elinden alınan ölçümlere göre yapılmaktadır. El geometrisi tabanlı kimlik doğrulama sistemleri çok yaygın olarak kullanılmaktadır. Bu teknolojiyi kullanmak çok kolay ve ucuzdur. Elleri kötü etkileyen kuru havalar gibi çevresel faktörlerden el geometrisi tabanlı kimlik doğrulama sistemleri etkilenmemektedirler. Ancak el geometrisi çok fazla ayırt edici olmadığından büyük nüfuslu kişi kimlik tespiti sistemlerinde tercih edilmemektedir. Çocukların büyüme döneminde el geometrisi bilgileri değişebilmektedir. Bununla birlikte, kişilerin ellerine yüzük veya metal eşyalar takması sonucu el geometrisinin özelliklerinin belirlenmesi zorlaşmaktadır. El geometrisi kişi tanıma sistemleri, büyük bir nüfusa sahip olan yerlerde, kişinin kimliğinin belirlenmesi gereken yerlerde çok fazla kullanılmamaktadır (Jain vd., 2007). El geometrisi tabanlı sistemin fiziksel boyutu çok büyüktür. Sadece birkaç parmak yerine tüm elin (genellikle orta ve işaret parmak) ölçümlerine dayanan kimlik doğrulama sistemleri mevcuttur. Bu sistemlerde kullanılan cihazlar el geometrisi için kullanılan cihazlardan daha küçük, ancak diğer bazı özellikleri (örneğin, yüz, parmak izi, ses gibi) çıkarmak için kullanılan cihazlardan daha büyüktür.

3.2.8. İmza tanıma

Bir kişinin, bir belgedeki yazının altına bu yazıyı yazdığını veya onayladığını belirtmek için her zaman aynı formatta yazdığı işaretler veya isimlerinden oluşmaktadır. İmzalar kişiler tarafından tüm hayatları boyunca çok sık kullanılmaktadır. Hukuksal açıdan çok büyük sorumlulukları bulunmaktadır. Sahte imzalar atılması sonucu kişi borç altına girebilmekte ve tüm mal varlığını tanımadığı başka kişilere devretmesi gibi olaylar gerçekleşebilmektedir. Kimlik doğrulamada imzanın kim tarafından atıldığının tespit edilmesi öncelikli bir işlemdir. İmzayı tespit etmek için iki tip bilgi kullanılmaktadır. İlki bir imzanın kolay taklit edilebilen desen biçiminden oluşmasıdır. Diğer yöntem ise imza atarken geçen süre, kalemin basım şiddeti, ivmesi gibi taklit edilmesi zor olan özelliklerdir (Şamlı ve Yüksel, 2009).

3.3. Biyometrik Sistemlerin Uygulama Alanları

Yüksek güvenlik gerektiren sistemlerde bir kişinin kimliğinin tespit edilmesi çok önemli bir olaydır. Kullanılan sistemde, "Kimliği iddia edilen kişi gerçekten mevcut mu? Bu binayı kullanmaya yetkili bu kişi mi? Hükümet tarafından belirlenmiş izin listesinde ismi var mı?" biçiminde değişik güvenlik olayları görülmektedir. Günlük hayatta ulaşım ve iletişimde oluşan hızlı gelişmeler, güvenlik konusunda çoğalan kaygılar nedeniyle güvenilir kullanıcı kimlik doğrulama tekniklerine duyulan gereksinimi artırmıştır. Bu nedenlerle biyometrik sistemler geliştirilerek çok farklı uygulamalarda kullanılmaktadırlar. Bu uygulamalar üç ana grup altında kategorize edilmektedir.

Birincisi, fiziksel erişim kontrolü, elektronik veri güvenliği, bilgisayar sistemlerine giriş, e-ticaret, internet erişimi, ATM veya kredi kartı kullanımı, cep telefonu, tıbbi kayıt yönetimi, uzaktan eğitim gibi ticari uygulamalar. İkincisi, ceza evleri, ulusal kimlik kartı, ehliyet, pasaport kontrolü, fiziksel erişim kontrolü, sınır kontrolü gibi devlet uygulamaları. Üçüncüsü, ceset kimlik tespiti, suçluya ait araştırma, anne ve babalık tespiti gibi adli uygulamalar (Akın vd., 2002).

3.4. Biyometrik Sistemlerin Performansı

Parola tabanlı sistemlerde, farklı iki biyometrik sistem arasında doğru bir karşılaştırmanın yapılabilmesi için, bir kişinin kimliğinin tespit edilmesi gerekmektedir. Bir biyometrik sistemde, iki biyometrik özelliğin karşılaştırılması sonucu bir kullanıcının biyometrik özelliği, azda olsa benzerleriyle eşleştirilebilmektedir. Bunlar; kullanıcının biyometrik karakteristiğinde oluşan değişiklikler (örneğin, konuşma tanımayı etkileyen solunum rahatsızlıkları), kusurlu algılama sonuçları (örneğin, arızalı sensörler nedeniyle parmak izinin gürültülü olması), çevre koşullarında oluşan değişiklikler (örneğin, yüz tanımada tutarsız aydınlatma seviyeleri) ve algılayıcı sensörler ile kullanıcı etkileşimindeki değişiklikler (örneğin, kapanmış iris veya kısmi parmak izi) sonucu oluşmaktadır (Jain vd., 2007). Bir kişinin biyometrik özellikli veri setinde belirlenen değişiklikler sınıf-içi değişim olarak adlandırılmakta ve iki farklı kişiden alınan özellik veri setleri arasında oluşan değişim ise sınıflar arası değişim olarak ifade edilmektedir. Biyometrik özellikli verilerde, sınıflar arası büyük değişimler ve sınıf içi küçük değişimler görülebilmektedir.

İki biyometrik özellik arasındaki benzerlik oranı, bir benzerlik puanı ile

belirtilmektedir. Benzerlik karşılaştırma puanı; bir kullanıcıya ait alınan iki biyometrik özellikli örneğin karşılaştırılıp aynı gerçek puan sonuçlarının elde edilmesiyle oluşmaktadır. Sahte bir puan; sınır değerini aştığında yanlış kabul (false accept) veya yanlış karşılaştırma, gerçek bir puan; sınır değerinin altına düştüğünde yanlış reddetme (false reject) veya yanlış olmayan karşılaştırma olarak ifade edilmektedir. Yanlış kabul oranı; (False Accept Rate - FAR) bir biyometrik sistemde, sınır değerin aşılması sonucu oluşan sahte puan olarak tanımlanmaktadır. Benzer şekilde, Yanlış reddetme oranı; (False Reject Rate - FRR) bir biyometrik sistemde, sınır değerin altına düşülmesi sonucu oluşan gerçek puan olarak tanımlanmaktadır. FAR ve FRR oranları biyometrik sistemlerin yaptığı karşılaştırmaların ne kadar doğru olduğunu ölçmek için kullanılmaktadırlar. Yanlış kabul oranı veya yüzdesi, yetkisiz kişilerin sisteme giriş izni, yanlış reddetme oranı ise yetkili bir kişiye sisteme giriş izni verilmemesi olasılığıdır. Biyometrik sistemlerde, karşılaştırılan özelliklerin sayısı bir sınır (threshold) değeriyle kıyaslanmaktadır. FAR ve FRR ölçüm değerleri, bir biyometrik sistemin güvenirliliği hakkındaki en doğru bilgiyi vermektedir (Kakıcı, 2008). FAR ve FRR değerleri ters orantılı olarak çalışmaktadır. FAR değeri artarken FRR değeri ise azalmaktadır. Sınır değeri ayarlanarak FAR ve FRR değerleri değiştirilebilmektedir (Jain vd., 2007).

4. NFC TEKNOLOJİSİ

4.1. NFC

NFC yakın saha iletişimi de denilen yeni nesil bir kablosuz iletişim teknolojisidir. Kullanıcıların temassız olarak işlemlerini kolay basit ve güvenilir olarak gerçekleştirmelerini, temassız ödeme yapabilmelerini, tek bir tuşla dijital cihazlara bağlanabilmesini sağlayan bir teknolojidir. NFC teknolojisi, 13,56 MHz (yüksek frekansta) ve en çok 424 Kbit/s (düşük bant genişliğinde) veri haberleşmesini güvenli bir şekilde sağlamaktadır (Grassie, 2007). NFC teknolojisinin günümüzdeki kullanımının çok hızlı artacağı öngörülmektedir. Şekil 4.1'de NFC teknolojisine sahip iki cep telefonun karşılıklı etkileşimi görülmektedir.

Şekil 4.1 NFC teknolojisi etkileşimi (NearFieldCommunication.org, 2017)

NFC çift yönlü ve tek yönlü veri iletişim yeteneği ve temassız kullanımı sayesinde kullanıcılarına büyük kolaylıklar sunmakta ve diğer teknolojiler ile kablosuz iletişim kurmak için en ideal ortamı sunmaktadır. Kullanıcılar bir filmin posterine cep telefonunu yaklaştırdığında o filmin fragmanını izleyebilecek, filmin konusunu okuyabilecek ve isterlerse filmin biletini interaktif satış yapan siteye bağlanabileceklerdir. Ayrıca evinize, aracınıza, çalışma masanıza birer NFC etiketi yapıştırarak, telefonunuzu üstüne koyar koymaz ses, wifi, bluetooth gibi özellikleri açıp kapatma, seçtiğiniz bir uygulama ya da görevi çalıştırma işlemleri kolaylıkla yapılabilecektir. Toplantı yapılacak salonun girişine telefonu sessize alan NFC etiket konulduğunda toplantıya katılanlar NFC etiketini okuttuklarında telefonları otomatik olarak sessize alınacak veya bir dergiye reklam amacıyla yerleştirilmiş bir NFC etiketi mobil cihazımızı yaklaştırdığınızda bizi o ürünün doğrudan internet sayfasına yönlendirebilecektir. Kısacası, NFC özellikli cep telefonunuz ile internet sitesini, iletişim bilgilerini, telefon numarasını, müzik dosyasını, videoları ve fotoğrafları

paylaşabilir, evimizdeki kapının kilidini açabilir ve telefonunuzu alışverişlerinizde mobil cüzdan olarak güvenle ve kolaylıkla kullanabilirsiniz.

NFC teknolojisinin yararlarını şu şekilde sıralayabiliriz;
-Kullanmak için iki cihazı birbirine yakın mesafede yaklaştırmak yeterlidir.
-Çok çeşitli kullanım özelliği sayesinde büyük bir kullanıcı topluluğuna ve sanayiye hitap etmektedir.
- NFC teknolojisinin yapısını oluşturan katman, ISO, ECMA (european computer manufacturers association) standartlarını uygulamaktadırlar.
- NFC, kablosuz teknolojilerin (bluetooth, wifi gibi) hızlı ve basit bir şekilde kurulumunu kolaylaştırmaktadır.
- Yakın temas özelliğini kullanarak çalıştığı için son derece güvenli kullanıma sahiptir.
- Yerleşik güvenlik uygulamalarına sahiptir.
- NFC, kullanılan temassız kart sistemleri ile uyumlu çalışabilmektedir (NearFieldCommunication.org, 2017).

4.2. NFC'nin Tarihçesi

Sony ve Philips ile birlikte geliştirilmiş olan NFC teknolojisi 2002 yılının sonlarında, ECMA Standartlar Birliği(Avrupa) tarafından kabul görmüştür. Yaklaşık bir yıl sonra 2003 yılı sonlarında, ISO/IEC (international organization for standardization/ international electrotechnical commission) tarafından bir standart olarak kabul edilmiştir. ECMA ve ISO/IEC tarafından NFC için ISO/IEC 18092/ECMA–340 NFCIP–1 ve ISO/IEC 21481/ECMA–352 NFClP–2 olmak üzere iki ayrı standart geliştirilmiştir. 2004 yılında Philips, Nokia ve Sony firmaları NFC Forum'u oluşturmuşlardır. NFC standartları, kar amaçlı olmayan bu organizasyon tarafından geliştirilmektedir. İş ve eğitim sektöründe NFC teknolojisinin bilinirliğinin, güvenilirliğinin ve kullanımının arttırılması amaçlamaktadır. Standartlar kamuya açık olup isteyen herkes tarafından erişilebilmektedir. NFC'nin taşıdığı iş potansiyeli ve popülaritesinin artması sonucunda NFC Forum'a zaman içinde Microsoft, Visa, Nokia, MasterCard, NEC, Inside Secure, Innovision, Renesas, NTT-Docomo ve ST gibi dev firmalar katılarak bu Forumu daha büyütmüştürler. NFC Forumun günümüzde çeşitli iş ve hizmet sektöründen oluşan 170 üyesi bulunmaktadır. Üye kuruluşlar bu teknolojinin mobil cihazlarda ve kişisel bilgisayarlarda kullanımını arttırmak istemektedir. NFC Forum yayınlamış olduğu 16 şartname ile tüm tarafları ilgilendiren, yeni, güçlü, tüketici odaklı ürünler oluşturulması için yol haritası sağlamaktadır. NFC içerikli

servislerin kullanıldıkları yerlerin belirlenmesi ve kullanıcılar tarafından kolaylıkla far edilebilmesi amacıyla evrensel bir NFC sembolü olan N-Mark geliştirilmiştir (NFC World, 2017).

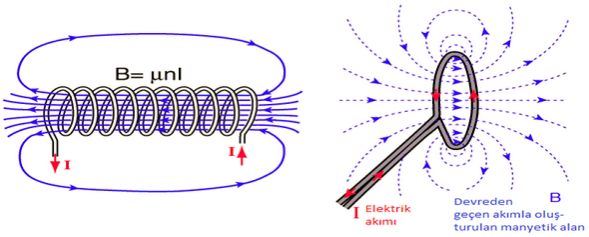
Şekil 4.2'de NFC sembolü olan N-Mark görülmektedir.

Şekil 4.2. NFC sembolü (NFC World, 2016)

4.3. NFC Çalışma Prensibi

NFC teknolojisi; wifi, bluetooth gibi çeşitli kablosuz iletişim teknolojilerinde olduğu gibi radyo dalgaları üzerinden veri gönderme sistemiyle çalışır. NFC'de kullanılan teknoloji, RFID (Radio frequency identification) temeline dayanmaktadır. Yani veri transferi elektromanyetik indüklemeyle yapılır. Manyetik alan altına giren kapalı devrelerde bir akım oluşur. Oluşan bu akımla radyo dalgaları yayılır. Manyetik alan yardımıyla kapalı devreden akım geçirme işlemine indükleme denilir.

Şekil 4.3'te NFC cihazlarda oluşan manyetik alan görülmektedir. Eğer kapalı devreden bir akım geçerse, bu akımın etkisiyle bir manyetik alan oluşur. Aynı şekilde eğer kapalı bir devre manyetik alana yaklaştırılırsa içerisinden akım geçer. Bu geçen akım vasıtasıyla pasif NFC cihazları güç kaynağına ihtiyaç duymadan çalışırlar.



Şekil 4.3. NFC cihazlarda olan manyetik alan (NFC World, 2016)

NFC teknolojisini wifi, bluetooh'dan ayıran en belirgin özelliği veri transferinin iki cihazın birbirini tetiklemesiyle başlatılabiliyor olmasıdır. NFC aktif cihaz, NFC pasif cihaza yaklaştırıldığında, veri göndermenin yanı sıra NFC aktif cihazdan yayılan manyetik dalgalar NFC pasif cihazda elektrik akımı oluşmasına sebep oluyor. Bu sebeple NFC pasif cihazın kendine ait bir güç kaynağı bulundurması gerekmez. Şekil 4.4'te NFC mobil cihazın arka kapağındaki NFC anten bağlantısı görülmektedir.

Şekil 4.4. Bir mobil cihazın NFC anteni (NFC World, 2016)

Bir mobil cihazda NFC özelliğinin olup olmadığını cihazın arka kapağındaki etiketten anlamak mümkündür. NFC aktif cihaz aracılığı ile NFC pasif cihazın enerji ihtiyacı karşılanmaktadır. Bu sebeple NFC pasif cihazlar dışarıdan ekstra enerji güç kaynağına ihtiyaç duymamaktadır. Piyasada bulunan kablosuz şarj özelliği olan cihazlar NFC teknolojisinin kullandığı enerji aktarım yöntemini kullanmaktadırlar. Ancak bu teknoloji aracılığı ile oluşturulan akım düşük seviyelerde olduğu için kısa sürede yüksek miktarlarda güç gerçekleştirilemez (NFC World, 2016).

4.4. NFC ve RFID

Temel olarak NFC ve RFID teknolojileri aynı standartlar üzerine kurulmuştur. RFID teknolojisinde etiketten okuyucuya tek yönlü veri taşınır. NFC teknolojisinde ise hem çift yönlü hem de tek yönlü veri iletimi gerçekleştirilir. Ancak NFC iki aktif cihazın birbirleriyle haberleşmesini sağlamaktadır. Bu yüzden NFC hem RFID Etiketlerin okunup yazılmasını hem de iki elektronik cihazın veri paylaşımını sağlar. RFID etiketlerinin aktif, pasif ve yarı aktif olmak üzere üç çalışma modu vardır. NFC teknolojisinde aktif etiket kullanılmamaktadır. NFC etiketler kısa mesafede çalıştıklarından ve iletişimin sağlanması için cihazların birbirine çok yakın tutulması gerektiğinden, kullanıcıların bilgisi olmadan çalışma olanakları yoktur. RFID teknolojisi 125-134 KHz (Düşük Frekans), 13,56 MHz (Yüksek Frekans), 40-930 MHz (Ultra Yükse Frekans) kredi kartı, kimlik kartı, giriş kartı gibi uygulamalarda özellikle tercih edilmektedir ve 2,5-5 GHz hızlarında çalışırken NFC sadece 13,56 MHz frekansında çalışmaktadır (Narol, 2014).

4.5. NFC Standartları

NFC teknolojisinin kullanılabilmesi ve yaygınlaşabilmesi için NFC kullanan kurumların veya bireylerin işbirliği içinde çalışması gerekmektedir. Bu amaçla çeşitli standartlara ihtiyaç duyulmaktadır. Mobil ödeme standartları olmadan şirketlerin yatırım yapmak için uygun pazarlara ulaşmaları mümkün olmayacağından bu platformlara daha az yatırım yapılacaktır. NFC bir standarttır. Dünyadaki NFC Forum kabul görülen iki tane standart vardır. Bunlar: ISO/IEC 18092/ECMA-340: Near Field Communication Interface and Protocol-1 (NFCIP-1) ve ISO/IEC 21481/ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2) (Narol, 2014).

4.6. NFC Çalışma Modları

Veri iletişimi, NFC teknolojisinde üç farklı modda gerçekleşmektedir. Bu modlar Kart Emülasyon Modu (card emulation mode), Okuyucu/Yazıcı Modu (reader/writer mode) ve Birebir İletişim Modudur (peer-to-peer mode, p2p mode) (NFC Research Lab, 2016).

4.6.1. Kart emülasyon modu

NFC özelliğine sahip mobil cihaz, Kart emülasyon modunda, normal bir akıllı kart gibi davranır ve bu amaçla kullanılarak içinde birçok önemli bilgi saklayabilir. NFC okuyucu tarafından oluşturulan manyetik alan sayesinde NFC etiket gibi davranan mobil cihazın yaklaştırılmasıyla, cihaz içindeki tüm bilgilerin okuyucuya transferi gerçekleştirilir, bu mod ödemenin cep telefonundan yapılabildiği elektronik ödeme sistemleri için oluşturulmuştur. Kart emülasyon modu, Şekil 4.5'de gözükmektedir. Temassız ödeme sistemlerinin birçoğunda, elektronik bilet ve erişim kontrolü sistemlerinde kullanılmaktadır. Bu modda NFC cihazları, toplu taşıma kartı veya ödeme yapabilmek için kredi kartı olarak kullanılabilmektedir (NFC Research Lab, 2016).

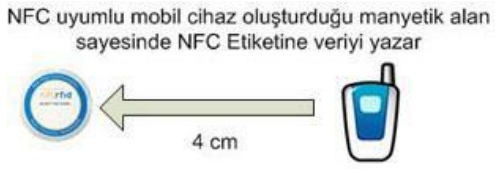
Şekil 4.5. Kart emülasyon modu (NFC Research Lab, 2016)

Şekil 4.6. Kart emülasyonu modu kullanımı (NFC World, 2016)

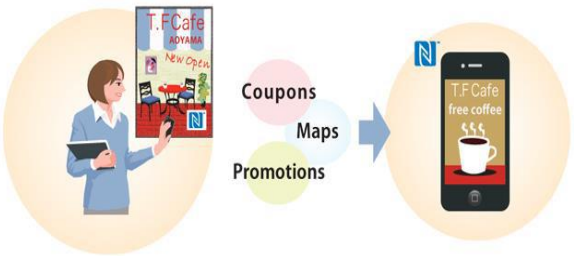
4.6.2. Okuyucu yazıcı modu

Okuyucu/yazıcı modunda, NFC teknolojisine sahip mobil cihaz 4 cm gibi kısa mesafede güçlü bir manyetik alan oluşturur. Pasif etiketin (NFC etiketi) mobil cihaza dokundurulmasıyla okuma işlemi başlar. Sonunda NFC teknolojisine sahip mobil cihaz NFC etiketinde depolanan veriyi okuyabilir, bu veriyi değiştirebilir, ya da NFC etikete yeni veri yazabilir. Şekil 4.7'de görüldüğü gibi NFC cihazın NFC etikete yaklaştırılmasıyla haberleşme başlar ve NFC etikette yer alan bilgiler NFC cihaza aktarılır. NFC etikete veri yazma Şekil 4.8'de görüldüğü gibi tek yönlü olarak NFC cihaz tarafından gerçekleştirilir. Şekil 4.9'da okuyucu/yazıcı modunu kullanan akıllı poster, harita, ürün bilgileri gibi örnek NFC uygulamaları görülmektedir (NFC Research Lab, 2016).

Şekil 4.7. Okuyucu modu



Şekil 4.8. Yazıcı modu
(NFC Research Lab, 2016)



Şekil 4.9. Okuyucu modu kullanımı (NFC World, 2016)

4.6.3. Birebir iletişim modu

Birebir iletişim modunda, iki NFC cihazı Şekil 4.14'de görüldüğü gibi birbiriyle karşılıklı haberleşerek bilgi alışverişinde bulunabilirler. İki NFC uyumlu cihazdan bir mobil cihaz öteki mobil cihaza yaklaştırıldığında veri transferi gerçekleşir. Birebir İletişim Modunda bir cihaz aktif durumda iken öteki cihaz pasif durumdadır. İki cihaz arasında yapılan etkileşime en iyi örnek bluetooth eşleştirmesi gösterilebilir. Birebir İletişim Modunda NFC cihazları iletişim kurarken NFC Forumun LLCP (logical link control protocol, mantıksal bağlantı kontrol protokolü)'nü kullanır. SNEP (simple NDEF exchange protocol), basit NDEF (NFC data exchange protocol) veri taşıma protokol ile cihazlar arasında NDEF mesajlaşması sağlanır (NFC Research Lab, 2016).

Şekil 4.10. Birebir iletişim modu (NFC Research Lab, 2016)

4.7. NFC Etiket Tipleri

NFC forumun desteklediği dört tip etiket bulunmaktadır. Şekil 4.12'te bu etiket tipleri görülmektedir.

- Tip 1 Etiket: Topaz, (broadcom)
- Tip 2 Etiket: Mifare UL, (nxp)
- Tip 3 Etiket: Felica, (sony)
- Tip 4 Etiket: DESFire, (nxp)

Şekil 4.11. NFC cihaz etiketleri (NFC World, 2016)

4.7.1. Tip 1 etiket

Tip 1 Etiket, ISO 14443A standardına dayanmaktadır. NFC etiketler kullanıcının isteğine göre okumak ve yazmak için kullanılabilir. Hafıza kapasiteleri 96 byte'tır. İstenmesi halinde 2 KByte'a kadar yükseltilebilir. Haberleşme hızı 106 Kbit/s'dir. Örnek olarak Topaz, Broadcom BCM20203 verilebilir (NFC World, 2016).

4.7.2. Tip 2 etiket

Tip 1 Etiket'e benzemektedir. ISO 14443A standardına dayanmaktadır. NFC etiketler kullanıcının isteğine göre okumak ve yazmak için kullanılabilir. Hafıza kapasiteleri 48 Byte'tır. İstenmesi halinde 2 KByte'a kadar yükseltilebilir. Haberleşme hızı 106 Kbit/s'dir. Örneğin NXP MiFare Ultralight (NFC World, 2016). İstanbul Ticaret Üniversitesi 2017 öğrenci kartları Tip 2 Etikete girmektedir (NXP MiFare Classic 1k).

4.7.3. Tip 3 etiket

Tip 3 etiket, ISO 18092 standardı ve FeliCa olarak bilinen Japon Sanayi Standardı esas almaktadır. Hafıza durumu değişkendir, 1 MB'a kadar genişletilebilir. Haberleşme hızı 212 veya 424 Kbit/s'dir. Örnek olarak Sony Felica verilebilir (NFC World, 2016).

4.7.4. Tip 4 etiket

Tip 4 etiket, ISO 14443A standardı ve NXP DESFire veri çarpışma koruma özelliğine sahip etiket tipidir. 32 KByte hafıza kapasitesine sahiptir. Haberleşme hızı 106, 212 veya 424 Kbit/s'dir. Örnek olarak NXP DESFire, SmartMX-JCOP verilebilir (NFC World, 2016) (NFC World, 2017).

4.8. NFC Teknolojisinin Uygulama Alanları

NFC teknolojisinin kullanım alanlarını aşağıdaki gibi sıralamak mümkündür. Müşteriler alışveriş yaparken satın almak istedikleri ürün hakkında bilgiye ürün üzerine yerleştirilmiş NFC etiketini mobil cihazları ile okutarak erişebilirler. Bu etiketler sayesinin de ürünün fiyatı özellikleri gibi bilgiler elde edilebilir. Müşteriler ile etkileşimli sanal mağazacılık oluşturmak mümkün olmaktadır. NFC ödeme mobil uygulamalarında banka kartı ya da kredi kartı bilgileri cep telefonunda depolanır ve mobil ödeme işlemi yapılırken, içinde kart bilgilerini saklayan cep telefonu NFC okuyucuya yaklaştırılarak ödeme gerçekleştirilir. NFC bilet mobil uygulamalarında alınan bilet akıllı telefonunda depolanır ve turnikeden geçiş esnasında akıllı telefonu

okuyucuya dokundurularak, bilet doğrulaması yapılır. Sağlık sisteminde uzaktan hasta takibi, hastaların hayatını kolaylaştıran bir sistemdir. İnsan faktöründen kaynaklanan ölçüm hatalarının önüne geçerek daha gerçekçi değerler elde edilmesini sağlar. Aynı zamanda hastanın doktora gitme gereksinimini ortadan kaldırarak hem zamandan hem de maddi olarak kazanç sağlar. Örneğin NFC özellikli şeker ölçüm cihazı ile ölçülen şeker değerleri yine NFC özellikli mobil cihazlar aracılığıyla okunarak doktorun ekranına yansıtılır ve kayıt altına alınır. Böylelikle doktora gitmeye gerek kalmaz. Eğer müdahale edilmesi gereken bir durum var ise anında ilgili yerlere bilgi aktarım sağlanarak hiç zaman kaybetmeden gerekli tıbbi müdahalenin başlatılması sağlanır. Fabrikalarda veya işyerlerinde çalışan insanların işe giriş ve çıkışları NFC kartlar sayesinde çok hızlı bir şekilde turnikelerde veya kapılarda kayıt altına alınır. Böylelikle sıra bekleme derdi olmadan personel devam takip işlemleri kolay bir şekilde kontrol edilebilir ve ayrıca detaylı raporlamada yapılabilir.

Ücretli geçiş yapılan otoyollar ve köprülerde, araçların duraklama yapmadan ve trafiği aksatmadan üzerlerinde bulunan NFC kartlar sayesinde ödeme noktalarından geçiş yaparken karta bağlı hesaplarındaki bakiyeden ücretlerini ödemeleri sağlanır. Bireyler otoparklarda araçların konaklama yaptıkları süre oranında ücret ödenmesi işlemini herhangi bir personele ihtiyaç duymadan rahatlıkla yapabilirler.

Mobil ödeme sistemi ile toplu ulaşımda yaptığımız her türlü ödemeler mobil cihazlarımız aracılığıyla yapılabilir. Mobil ödeme uygulamalarında kullanıcının yapacağı bir ödeme işlemi basit görünse de, karmaşık bir yazılım altyapısı arka planda bulunmaktadır.

Elektronik anahtar uygulamaları ile mobil cihazımız araba, ev ve işyeri anahtarı olarak kullanılabilir. NFC cihazımızla sinema afişini okutturarak film hakkında bilgi alabilir, filmin fragmanını izleyebilir ve bize yakın olan hangi sinema salonlarında gösterimde olduğunu öğrenebiliriz. İki NFC mobil cihazın birbirine yakın teması sayesinde bağlantı kurulmasına ihtiyaç olmadan NFC özelliğinin açık olması sayesinde çok hızlı bir şekilde dosya transferi başlatılabilir. Kişiler bu sayede fotoğraflarını, müzik ve video dosyalarını birbirleriyle paylaşma imkânına sahip olmaktadırlar.

Dünyanın en büyük kargo firması FedEx, günde yaklaşık 3 milyon kargo taşımakta ve dünya çapında 42500'den fazla araca sahiptir. FedEx kuryelerinin çözüm üretmek istediği bir konu ise araç anahtarların kaybolmasını engellemektir. 200 araçta pilot

olarak denenen yeni sistemde anahtar yerine kuryelerin bileklerine RFID etiket takılmaktadır. FedEx kuryeleri her gün kilometrelerce yol kat etmektedir. Kurye her teslimatı gerçekleştirdiğinde anahtarları aramak için zaman harcamaktadır. Kuryenin anahtarını kaybettiğinde ise yedek anahtarın gelmesi zaman alabilmektedir. Anahtarın kaybolması durumunda ise yeniden anahtar yapılmasının maliyeti ise 200$'dır. FedEx kuryeleri RFID kullanımıyla birçok paketi taşırken anahtarlarla uğraşma zorluğundan kurtulmuş ve kargo teslimatı daha verimli olmuştur (Narol, 2014).

5. ETKİNLİK DAVETLİ KONTROL MOBİL UYGULAMASI

Etkinlik davetli kontrol mobil uygulaması, tez kapsamında geliştirilen bir Android mobil uygulamadır. Bu uygulamada kullanıcı öncelikle sisteme bir kullanıcı adı (e-mail) ve şifre ile kayıt olur. Kayıt olduktan sonra sisteme giriş yapar, giriş yaptıktan sonra kendi etkinliklerini oluşturup bu etkinliğe davetli kişilerin isimlerini, yüzlerini ve etkinliğin tarihi ve saatini seçip sisteme kaydeder, böylece kayıt ettiği kişileri düzenleyeceği etkinlikte rahatlıkla kontrol edebilir. Davetli kontrol etme işlemi 4 modül üzerinden yapılabilir. Birincisi, davetlinin NFC kartını okutarak (NFC modülü), ikincisi, davetlinin fotoğrafını çekerek yüz tanıma sistemi ile davetli kontrolü yapabilir (Yüz tanıma modülü), üçüncüsü, etkinliğin yapıldığı yerde mi yapılıyor kontrol işlemi bunun kontrolü yapılır (Konum modülü), dördüncü ve son modül ise, kullanıcının oluşturduğu etkinlik tarihi ve saati doğru mu değil mi, etkinlik kontrolü doğru zamanda mı yapılıyor bunun kontrolü yapılır (Tarih ve Saat modülü). Bu tez kapsamında, etkinlik konumları için, İstanbul Ticaret Üniversitesinin kampüslerinin konumları ölçü alınmıştır. Mobil uygulamayı kullanan kullanıcının konum bilgileri, İstanbul Ticaret Üniversitesinin kampüslerine göre uzaklık bilgileri mobil uygulama da gösterilmiştir. Ayrıca, NFC kartlara veri yazabilme işlemi geliştirilen mobil uygulama üzerinden yapılabilmektedir. Geliştirilen mobil uygulamanın NFC modülünde, test olarak İstanbul Ticaret Üniversitesi öğrenci kartları kullanılmıştır.

5.1. Uygulamada Kullanılan Teknolojiler

Geliştirilen mobil uygulamada kullanılan teknolojiler, Microsoft yüz API, Android işletim sistemi, JSON (Javascript Object Notation) veri formatı teknolojisi, Picasso kütüphanesi, PHP ve MYSQL ve Google Play konum servisleridir.

5.1.1. Microsoft bilişsel yüz API

Microsoft yüz API, bulut tabanlı bir servistir. Bu tez kapsamında geliştirilen etkinlik davetli kontrol uygulamasında yüz tanıma için kullanılan yüz API'sidir. Bu yüz API'sinde iki temel fonksiyon vardır. Bu fonksiyonlar, yüz algılama ve yüz tanımadır.

Yüz algılama işleminde, bir veya daha fazla insan yüzünün resimler içinde tanınmasından sonra ve dikdörtgen içindeki yüzlerin bulunduğu noktaları ile birlikte, yüz ifadeleri üzerinden makine öğrenimi tabanlı tahminler içeren yüz öznitelikleri görüntülenir. Yaş, Cinsiyet, Duygu, Poz, Gülümseme, Bıyık ve Sakalın yanı sıra

resimdeki her yüz için 27 yer işareti. Kullanılabilen yüz özniteliği özellikleridir. (Microsoft Yüz API Dokümantasyon, 2017).

Şekil 5.1. Yüz algılama

Şekil 5.2. Yüz algılama sonucu JSON (Microsoft Yüz API Dokümantasyon, 2017)

Bu yüz API'sinde, bir resimde 64 resim'e kadar yüz algılama yapılabilir. Microsoft yüz API'de yüz tanıma, önceden kaydedilen kişi yüzü veri tabanına göre yapılır.

Şekil 5.3. Yüz tanıma sonucu (Microsoft Yüz API Dokümantasyon, 2017)

Bu yüz API'sinde, kişi grupları oluşturarak bu gruptaki kişilere yüzler tanımlanarak, yüz tanıması yapılabilir. Etkinlik davetli kontrol uygulamasında bu modül kullanılmıştır. Microsoft yüz API'de ayda 30.000 işlem (yüz ekleme, yüz silme, yüz tanıma gibi işlemler) ücretsizdir, bir ayda 30.000 yüz tanıma işleminden daha fazla işlem yapmak için (kurumsal kullanımlar için) her fazladan 1.000 işlem için ücret 1.5$'dır (Microsoft Yüz API Dokümantasyon, 2017).

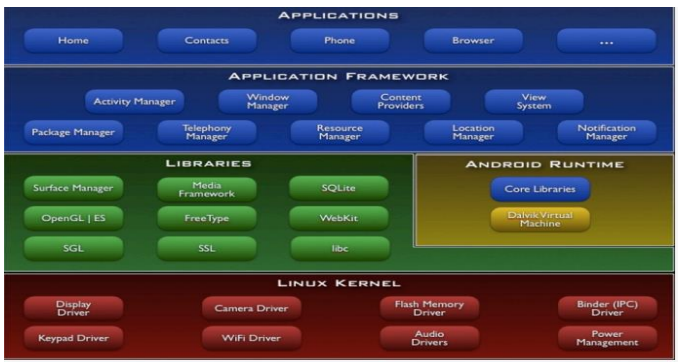
Şekil 5.4. Kişi ve yüzlerini gruplandırma (Microsoft Yüz API Dokümantasyon, 2017)

5.1.2. Android işletim sistemi

Android işletim sistemi, Linux çekirdeğini kullanan bir işletim sistemidir. Etkinlik davetli kontrol mobil uygulamasında kullanılan işletim sistemidir. Android işletim sistemi, Google, Open Handset Alliance ve özgür yazılım grupları tarafından geliştirilmektedir. İlk düşünce olarak dokunmatik ekranlar için tasarlanan Android, düşük maliyetli ve kişiselleştirilebilen işletim sistemi arayan yüksek teknolojiye sahip tüm cihazlar arasında da popülerdi. İlk dönemlerde Android işletim sistemi yalnız tablet ve akıllı telefonları kapsasa da, günümüzde arabalar, televizyonlar, oyun konsolları, dijital kameralar ve saatler gibi çeşitli cihazlarda da kullanılmaya başlamıştır.

Birçok yazılım, donanım, telekomünikasyon firmasının katkıda bulunduğu Open Handset Alliance adı verilen şirketler grubu sayesinde ortaya çıkan Android'in kaynak kodları iki farklı tipte lisans kullanır. Kullandığı Linux çekirdeği GPL, diğer dış bileşenler ise Apache Lisansı ile dağıtılmaktadır. Bu yapı yazılımcıları Android'e katkıda bulunmaları için teşvik ettiğinden, sürekli gelişmesini ve yeni özelliklerin eklenmesini sağlar. Aynı zamanda telefon üreticilerinin koyduğu çeşitli yasakları sevmeyen kullanıcıların tercih ettiği veya yazılım güncelleştirme desteği erken kesilmiş eski modellerin en yeni sürümleri kullanmasını sağlayan CyanogenMod veya Miui gibi Android sürümlerinin de (Custom ROM) ekosisteme dâhil olmasını sağlamaktadır.

Android mimarisi, Linux çekirdeği, kütüphaneler, Android çalışma zamanı (runtime), uygulama geliştirme çatısı ve uygulamalar katmanlarından oluşur.



Şekil 5.5. Android işletim sistemi mimarisi (Geleceği Yazanlar Turkcell, 2011)

Android, Linux çekirdeğini (kernel) kullanır. Linux çekirdeğine Android için eklenen kod parçaları ve kütüphaneler lisansına sahipken, diğer bileşenler üretici firmalarına kendilerine ait kapalı ROM (Read only memory) üretmelerine izin verecek ama yine

özgür bir şekilde Apache Lisansı ile dağıtılacaktır.

Linux çekirdeğinin yapısı, memory ve process (hafıza ve süreç) kontrolü, security (güvenlik), dosyalama ve bağlantı için I/O işlemleri ve cihaz sürücüleridir. Çekirdekte Android için özelleştirilmiş başlıca alanlar ise güç kontrolü, paylaşılan hafıza, low memory killer ve süreçler arası iletişim içindir.

Mimarinin diğer önemli yapısı olan kütüphaneler (libraries) bölümünde, C ile yazılmış sistem kütüphaneleri, internet tarayıcısı (browser) motorlarının çalışması için Webkit, görüntüleme kontrolünü yapan Surface Manager, grafik işlemleri için OpenGL, ses ve video işlemleri için gereken Media Framework, veri yapıları kontrolü ve düzenlenmesi için SQLite gibi kütüphaneler bulunur (Geleceği Yazanlar Turkcell, 2011).

5.1.3. JSON veri formatı

JSON, kısaca bir veri değişim formatıdır. Javascript uygulamaları için geliştirilmiştir. JSON, Javascript Object Notation'ın kısaltılmasıdır. JSON'ın çıkış amacı, XML dosyalarının veri transferlerinde çok büyük olması, bu sebeple XML'den daha az yer kaplayacak bir veri formatına ihtiyaç duyulmasıdır. Günümüzde sadece Javascript uygulamalarında değil, yazılım geliştirmede kullanılan birçok teknolojide JSON formatındaki veriler tercih edilmektedir. JSON, geliştirilen etkinlik davetli kontrol mobil uygulamasında PHP ile yazılmış web servis ile veri transferi için kullanılmıştır.

PHP uygulamaları, Java uygulamaları, Web servis uygulamaları, Mobil uygulamaların veri transferleri gibi birçok noktada veriler JSON formatında kullanılmaktadır. JSON Veri Formatı, JSON türündeki veriler iki parçadan oluşur: key (anahtar) ve value (değer). Anahtar'da nesnenin hangi özelliğinin olduğu (kodlamadaki değişken ismi gibi) tanımlanırken değerde ise anahtar özelliğinin değeri (kodlamadaki değişkenin değeri gibi) tanımlanır. Bu anahtar ve değerler string türünde tanımlanır. Aşağıda bir JSON nesnesi örneği bulunmaktadır (JSON, 2017).

```
{
  "Isim": "Zeynel Erdi",
  "Soyad": "Karabulut"
}
```

Yukarıdaki JSON nesnesinde 2 tane anahtar ve 2 tane değer vardır: "Isim" anahtarının

değeri “Zeynel Erdi” , “Soyad” anahtarını değeri ise “Karabulut” olarak tanımlanmıştır.

Her JSON nesnesi, süslü parantez ile başlar ve içinde sonsuz sayıda key-value ikilileri bulunabilir.

```
{
  "Isim": "Zeynel Erdi",
  "Soyad": "Karabulut"
}
```

JSON Dizi yapısı, her JSON dizisi köşeli parantez ile başlar ve içinde sonsuz sayıda değer bulunabilir. Key-value ikilileri JSON dizilerde yoktur. Sadece string değer alabileceği gibi JSON nesnesi de tanımlanabilir.

```
[
  "Zeynel Erdi",
   "Karabulut"
]
```

İki JSON nesnesine sahip JSON dizisi;

```
[ {
      "Isim": " Zeynel Erdi ",
      "Soyad": "Karabulut",
      "Bolum": "Bilgisayar Mühendisliği",
      "Il": "İstanbul",
      "Telefon": "05380270922"
 },
 {
      "Isim": "Burcu",
      "Soyad": "Kara",
      "Bolum": "Makine Mühendisliği",
      "Il": "Bursa",
      "Telefon": "05345678799"
  } ]
```

5.1.4. Picasso kütüphanesi

Tez kapsamında geliştirilen mobil uygulama da kişilerin yüz resimlerini sunucudan çekip uygulamada göstermek için, Picasso kütüphanesi kullanılmıştır. Her uygulamada ihtiyaç duyulmamakla birlikte birçok uygulama içerisinde İnternet üzerinden resim indirmek istenilebilir. Bunun için kesinlikle en iyi çözüm Picasso kütüphanesidir. Standart Android API'ler ile bir resmi indirmek için yapılması gereken adımlar en azından şunlardır:

Resim URL'si alınır. Resmi indirmek için AsyncTask oluşturulur. AsyncTask çalıştırılır. Sonucu Bitmap olarak saklanır. Bu Bitmap kaynak olarak ayarlanır. Cache (Önbellek) görüntü saklanır. Gördüğünüz gibi burada bir sürü iş var ama Picasso Kütüphanesi sayesinde sadece ImageView için bir resim URL sağlamanız yeterli olacaktır. Picasso kullanıyorsanız yukarıdaki adımları unutabilirsiniz. Yapmanız gerekenler sadece resim URL'si alınır ve tek bir satır kod yazarak, ImageView komponenti içerisine resim başarıyla yüklenir.

"Picasso. with(this).load(imageUrl).into(ImageView);"

Bu kolaylıklar için Android Studio içindeki uygulama dosyasında bulunan build.gradle dosyası içerisinde dependencies kısmına aşağıdaki satırı eklemeniz yeterli olacaktır.

compile 'com.squareup.picasso:picasso:2.4.0' (Picasso, 2017).

5.1.5. PHP ve MYSQL

Etkinlik davetli kontrol uygulamasında kullanılan sunucu tarafı (PHP) ve veri tabanı teknolojileridir (MYSQL). MYSQL, hızlı ve güçlü bir veri tabanı sunucusudur. Bir web tabanlı takip ve otomasyon sistemi için gerekli olan kayıt işlemi MYSQL ile çok kolay bir şekilde yapılabilir. PHP ise, dinamik web siteleri, web servisleri geliştirmek için oluşturulmuş web tabanlı bir programlama dilidir. Etkinlik davetli kontrol mobil uygulamasının MYSQL veri tabanı tablolarının fonksiyonel yapısı şu şekildedir.

Kullanıcılar -> Users (unique_id, name, email, encrypted_password)
Etkinlik -> KisiGrup (KisiGrupIdd, KisiGrupAdi, KullaniciAdi, Tarih)
Davetli -> Kisi (KisiIdd, KisiAdi, KisiGrupIdd)
Davetli Yüzü -> KisiYuzu (YuzIdd, ResimUrl, KisiIdd)

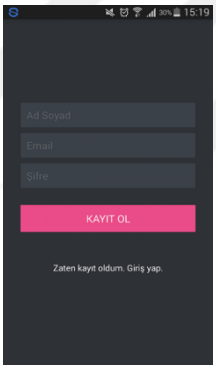
5.1.6. Google Play konum servisleri

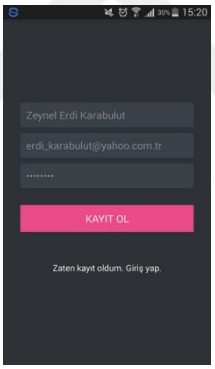
Tez kapsamında yapılan uygulamada kullanıcıların konumlarını algılamak için kullanılan kütüphanedir. Bu kütüphane de kullanıcıların konumlarını pil tüketimini en aza indirerek kolayca alınabilir.

Google, Google Haritalar servisini Android ortamında kullanabilmesi için Google Maps Android API'yi aracı kılar. Google Maps Android API v2, Google Play Servislerinin bir parçasıdır. Dolayısıyla geliştiriciler, Google Haritalar ve benzeri Google servislerini kullanan uygulamaları geliştirebilmek için ilk önce Google Play Servisler' i elde etmesi gerekmektedir.

5.2. Etkinlik Davetli Kontrol Android Uygulaması Kullanıcı Kayıt Ekranı

Uygulamayı kullanabilmek için kullanıcının sisteme kayıt olduğu bir ekrandır. Kullanıcı, ad soyadını, e-mail adresini ve şifresini girerek bir kullanıcı oluşturur.





Şekil 5.6. Kullanıcı kayıt ekranı Şekil 5.7. Kullanıcı bilgilerini girdi

5.3. Etkinlik Davetli Kontrol Android Uygulaması Kullanıcı Giriş Ekranı

Uygulamayı kullanabilmek için kullanıcının sisteme giriş yaptığı ekrandır. Bu ekranda kullanıcı kayıt olduğu e-mail (kullanıcı adı) ve şifre ile uygulamaya giriş yapar.

Şekil 5.8. Kullanıcı giriş ekranı Şekil 5.9. Kullanıcı giriş bilgilerini girdi

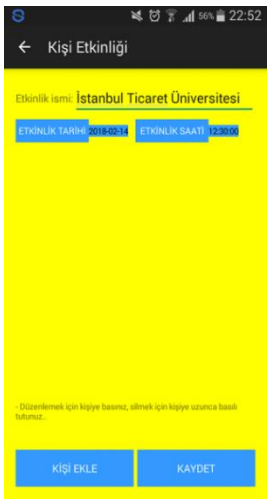
5.4. Etkinlik Davetli Kontrol Android Uygulama Ana Ekranı

Bu ekran kullanıcının uygulamaya giriş yaptıktan sonra karşılaştığı ana ekrandır. Bu ekranda kullanıcı etkinlik oluşturup bu etkinliğe katılacak kişilerin isimlerini ve yüzlerini tanıtabilir, NFC karta etkinliğe katılacak kişilerin bilgilerini yazabilir ve etkinliğe katılacak kişileri yüz tanıma ve NFC kart ile mobil uygulama üzerinden bu etkinliğe gerçekten davetli olup olmadıklarını kontrol edebilir. Ana ekranın üst menüsünde 3 tane menü seçeneği vardır, bunlardan ilki yenileme seçeneğidir. Bu yenileme tuşunun görevi etkinlikleri ve bu etkinliğe katılacak kişilerin tüm bilgilerini çekmektir, bu özellikle mobil uygulamanın veri tüketimi en az seviyelere indirilmiş olunur ve uygulama çoğu zaman offline çalışır, buda kullanıcının internet paketinin daha az kullanmasına neden olur. Bu ana ekranda ikinci menü seçeneği konum kontrol seçeneğidir, etkinliğin yapıldığı mekâna kullanıcının uzaklığı üst menüdeki konum ikonundan kontrol edilebilir. Son olarak kullanıcı uygulamadan çıkış yapmak için üst menüden çıkış menü ikonuna basıp çıkış işlemini gerçekleştirebilir.

Şekil 5.10. Uygulama ana ekranı

5.5. Etkinlik Oluşturma Ekranı

Etkinlik oluşturma ekranında, kullanıcı bir etkinlik oluşturmak için, etkinliğin adı yazılır, etkinliğin tarihi ve saati seçilir ve etkinlik oluşturma işlemi Şekil 5.11'deki kaydetme tuşuna basılarak tamamlanır. Oluşturulabilecek etkinlikler, toplantı, düğün veya bir üniversite etkinliği olabilir. Örneğin bu tez kapsamında İstanbul Ticaret Üniversitesi etkinliği oluşturuldu.

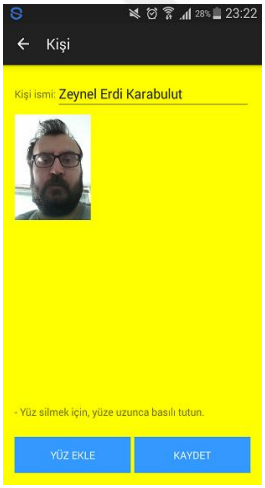


Şekil 5.11. Etkinlik oluşturma ekranı

5.6. Etkinlik Davetli Kişileri Kaydetme Ekranı

Bu ekranda, İstanbul Ticaret Üniversitesi için oluşturulan etkinliğe, davetli kişilerin adlarını ve akıllı telefonların kameraları kullanarak davetli kişi yüzleri eklenir. Akıllı telefonun kamerasını kullanarak etkinliğe davetli kişinin fotosu çekilir ve uygulamanın veri tabanına (MYSQL) ve Microsoft Bulut'a kaydedilir (Şekil 5.12).

Şekil 5.12. Etkinliğe kişi yüzü ekleme



Şekil 5.13. Etkinliğe kişi yüzü eklendi

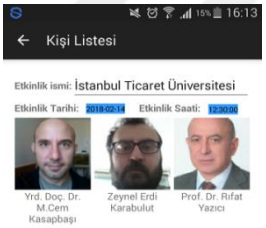
5.7. NFC Karta Veri Yazma Ekranı

Bu ekran etkinliğe katılacak davetliler eğer NFC kart ile kontrol edilecekse, o davetliye ait bilgiler bu ekranda NFC kartlarına yazılabilir (Şekil 5.14).

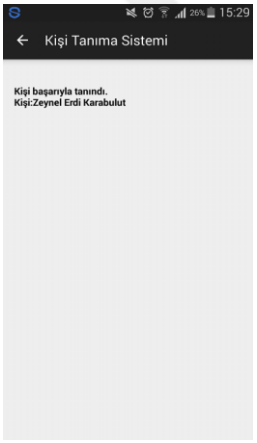
Şekil 5.14. NFC karta veri yazma

5.8. NFC Kart İle Etkinlik Davetli Kişileri Kontrol Etme Ekranı

NFC kart ile etkinlik davetli kişileri kontrol etme modülü, ana ekrandan NFC ile kişi tanıma butonundan seçilir. Aşağıdaki şekillerden 5.15'de, kontrol edilecek etkinlik (grup) gözükmektedir. Daha önceden İstanbul Ticaret Üniversitesi etkinliği oluşturulmuştu bu oluşturulan etkinliğe şekil 5.15'de görüldüğü gibi 3 kişi eklenir. Şekil 5.16'da ise NFC kart ile davetli kişi kontrol işleminin sonucu gözükmektedir.



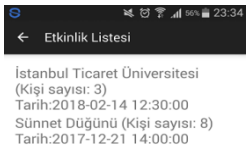
Şekil 5.15. Seçilen etkinlikteki kişiler



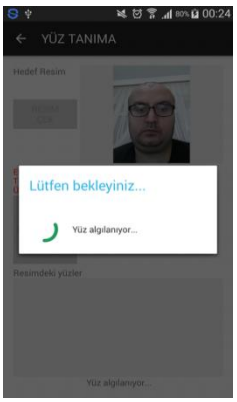
Şekil 5.16. NFC ile davetli kontrol sonucu

5.9. Yüz Tanıma İle Etkinlik Davetli Kişileri Kontrol Etme Ekranı

Etkinlik davetli kontrol uygulamasında yüz tanıma ile kişi tanıma ekranında, önceden oluşturulan etkinlik ve bu etkinliğe kaydedilen kişi yüzlerine göre davetli kontrolü yapılır. Ana ekrandan yüz tanıma ile kişi tanıma seçeneği seçilir ve davetli kontrolü yapılacak etkinlik seçilir.



Şekil 5.17. Etkinlik seçimi



Şekil 5.18. Yüz tanıma ile davetli kontrol

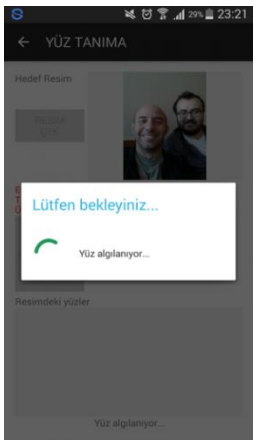
Şekil 5.17'de etkinlik davetli kontrolü yapılacak etkinlik seçilir ardından, etkinlikteki kişileri kontrol etme işlemi başlar. Yukardaki Şekil 5.18'de ise telefonun kamerasıyla davetlinin fotoğrafı çekilir ve yüz algılama işlemi başlar ve bu yüze ait kişi etkinliğe davetliyse aşağıdaki şekil 5.19'da ki gibi bir ekran ile karşılaşılır. Şekil 5.19'da eğer kişi başarılıyla tanınırsa, tanınan kişinin bulut ve MYSQL sunucudaki kayıtlı fotoğrafı da tanınan kişinin isminin sağ tarafında gözükmektedir. Eğer fotoğrafı çekilen kişi etkinliğe davetli değilse şekil 5.20'deki gibi olumsuz ekranla karşılaşılır. Bu olumsuz ekranda tanınmayan kişi veya kişiler vardır.

Şekil 5.19. Etkinliğe davetli kişi başarıyla tanındı

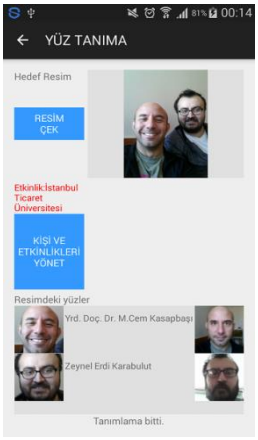
Şekil 5.20. Etkinliğe davetli olmayanlar.

Şekil 5.20'de görüldüğü üzere toplu fotoğraf çekilerek de etkinlik davetli kontrol işlemi yapılır, bu geliştirilen uygulamada yüz tanıma için Microsoft yüz API kullanılmıştır, bu API'de bir fotoğrafta 10 kişiye kadar kişilere ait benzer yüz araması yapılabilir.

Örneğin; İstanbul Ticaret Üniversitesi etkinliğine kayıtlı Zeynel Erdi KARABULUT ve Yrd. Doç. Dr. Mustafa Cem KASAPBAŞI'nın aynı fotoğrafta olduğu bir davetli kontrol işlemi yapılır sonuçlarını görülür.



Şekil 5.21. Toplu davetli kişi kontrol işlemi yapılıyor



Şekil 5.22. Bir resimden davetliler tanındı

Şekil 5.21 ve şekil 5.22'den anlaşılacağı üzere, tez kapsamında geliştirilen mobil uygulamada çekilen bir fotoğrafta bir davetli olmasına gerek yoktur birden fazla davetliler aynı fotoğrafta tanınabilir. Bir fotoğrafta 10 kişiye kadar davetli yüz taraması yapılabilir.

5.10. Etkinlik Davetli Uygulamasının Konum Modülü

Etkinlik davetli kontrol uygulamasında, etkinliğin yapılacağı konum ile mobil uygulamayı kullanan kullanıcının konum bilgileri karşılaştırarak (kullanıcı gerçekten etkinliğin yapıldığı yerde mi değil mi) konum kontrolü yapılır. Bu uygulamada etkinlik konumları için İstanbul Ticaret Üniversitesinin kampüslerinin konum bilgileri kullanılmıştır. Şekil 5.23'de, mobil uygulamayı kullanan kullanıcının İstanbul Ticaret Üniversitesinin kampüslerine olan uzaklıkları görülür.

Şekil 5.23. Kullanıcının konum bilgisi

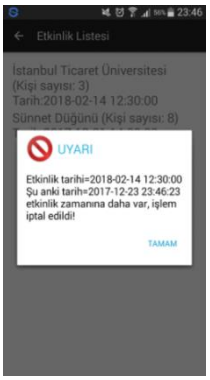
Şekil 5.23'de görüldüğü gibi, kullanıcının Küçükyalı, Sütlüce ve Bursa kampüslerine olan uzaklığı gözükmektedir.

Böylece etkinlik davetli kontrol uygulamasını kullanan kullanıcı gerçekten İstanbul Ticaret Üniversitesinde mi değil mi anlanmış olunur. Eğer davetli kontrolünü yapan kullanıcı gerçekten o mekânda değilse şekil 5.24'de ki gibi bir ekran ile karşılaşılır. Uygulamada etkinlik konum modülünde kullanıcı İstanbul Ticaret Üniversitesi kampüslerine uzaklığı en fazla 200 metre ise etkinlik davetli kontrolü yapmasına izin verilmiştir. Kullanıcı İstanbul Ticaret Üniversitesinde değilse şekil 5.24'de ki gibi uyarı ekranıyla karşılaşılır ve davetli kontrol işlemi iptal edilir.

Şekil 5.24. Kullanıcı etkinliğin yapılacağı yerde değil

5.11. Etkinlik Davetli Uygulamasının Tarih ve Saat Modülü

Etkinlik davetli kontrol uygulamasında, tarih ve saat modülü de vardır, bu modülde, kullanıcı etkinliği oluştururken etkinlik tarihi ve saati seçer, kullanıcı o seçilen tarih dışında davetli kişi kontrolü işlemini yapamaz, geliştirilen uygulama da kullanıcı etkinliğin tarihi dışında davetli kontrolü yapmaya çalıştığında şekil 5.25'de ki gibi bir uyarı ekranıyla karşılaşır.



Şekil 5.25. Kullanıcı etkinlik tarihi dışında davetli kontrolü yapmaya çalışırsa

5.12. Lojistik Sektöründe Üretilen Örnek Senaryolar

Temel lojistik işlemleri, outbound lojistik (dışa yönelik lojistik), inbound lojistik (içe yönelik lojistik) ve reverse lojistiktir (tersine lojistik).

Outbound lojistik (dışa yönelik lojistik), üretilen mal ve hizmetlerin dağıtım kanallarına iletilmesinde nihai tüketiciye teslim edilmesine karada gerçekleşen tüm faaliyetleri içerir (Christopher, 1998).

Inbound lojistik, işletmenin üretim faaliyetlerinde kullanacağı girdilerin elde edilmesi, üretim sürecine alınması, stoklanması gibi faaliyetleri içerir (Christopher, 1998).

Reverse lojistik, yarı mamul, hammadde, nihai ürün ve bunlarla ilişkili bilgilerin bitirildiği noktadan başlangıç noktasına doğru, değer kazanmak ya da sözü edilen şeylerin uygun şekilde yok edilmesini sağlamak amacıyla etkin bir biçimde akışı planlama, yürütme, uygulama ve kontrol etme faaliyetleridir (Bowersox vd., 2002).

Kargo kaybı, şirket işinde ve lojistik yönetiminde büyük sorun yaratan olumsuz bir etkiye sahiptir, ancak sektörde az sayıdaki çalışma kargo kaybını ele almıştır. Kargo kaybının en önemli unsurlarından bazıları, transit tipleri, ürün kategorileri ve nakliye hedefleridir (Pei-Ju vd., 2017).

Bu tez kapsamında geliştirilen mobil uygulama ile lojistik bilgi sisteminde kimlik doğrulama ve yetkilendirme süreci arasında bir köprü oluşturulması için senaryolar üretilmiştir. Ayrıca, kargo hasar, kargo hırsızlığı ve kargo sorumluluk sigortasında kargo kaybı konularını gerçek kargo kaybı verilerinden istifade ederek yardımcı olacak ve tanımlayacak bir örnek sistem senaryoları yapılmıştır.

Lojistik Bilgi Sistemi'nde, binlerce günlük gelen, giden veya ters lojistik işlemi vardır ve bunların çoğunda, kimliği doğrulanmış ve güvenli bir şekilde ele alınması gereken hassas bilgiler bulunmaktadır.

Lojistik sektörü için, uygulanan güvenli kimlik doğrulama yüz modeli, SaaS olarak bulut tabanlı Microsoft yüz API'den ve veri tabanı olarak kullanılan bir MYSQL'den oluşur. Modül adları, Şekil 5.26'da gösterildiği gibi Yüz Modülü, NFC Modülü, Konum Modülü, Tarih ve Saat Modülü‘dür. Bu modüllerin tamamı Android mobil uygulamasında uygulanmaktadır. Lojistik şirketin bilgilerini saklamak için harici bir

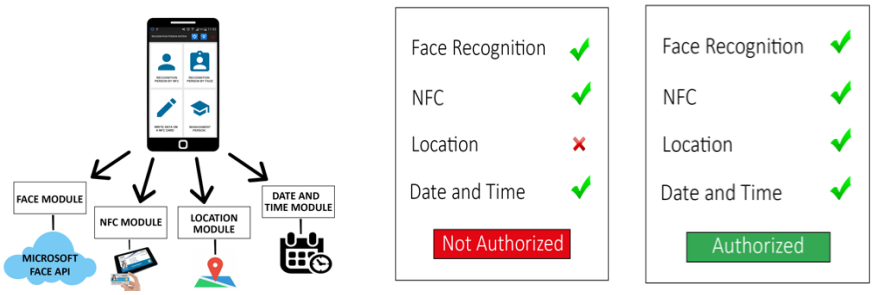
MYSQL veri tabanı vardır. Lojistik sektörünü daha iyi tanımlamak için aşağıda bazı senaryolar verilmiştir.

Senaryo 1: Sistem Yöneticisi, bir outbound lojistik olayı kaydeder ve müşteri bilgilerini kargo bilgileriyle ilişkilendirir (yüz bilgileri, sadakat kartı bilgileri NFC, alımın yapılacağı mekânın yeri ve alınması gereken tarih ve saat). Kargo adamı, mobil uygulamayı kullanarak, müşteriyi, teslim tarihini ve yerini doğrulamak için kullanır. İşlem tamamlandığında hiçbir parti kargo devrini inkâr edemez.

Senaryo 2: Müşteri lojistik bilgi sisteminde ters Lojistik olayını kayıt eder, (Kullanıcı bilgilerini, konumu ve tarih saat bilgilerini girer). Sistem bir yük kullanıcısını bu olayla ilişkilendirir. Müşteri, yük adamını doğrulamak için mobil uygulamayı kullanır; ayrıca, kargo adamı, müşterinin kimliğini doğrulamak için kendi mobil cihazı üzerinden mobil uygulamayı kullanır.

Senaryo 3: Şirket müşterinin yüklediği yüz imajını pakette kullanır ve pakete müşteriye aktarılır. Müşteri, kargo paketini özel bir şekilde doğrulamak için mobil uygulamayı kullanır.

Senaryo 4: Tedarikçi firma, tedarik kargosunu tam yer ve zamanla gönderir, bu nedenle kargo doğru kişiye doğru yerde ve doğru zamanda teslim edilir.



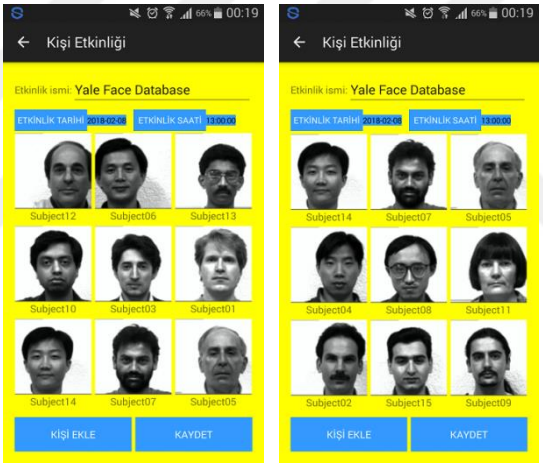
Şekil 5.26. Uygulama modülleri ve etkileşim sonuçları

Üretilen lojistik senaryolar da kişi tanıma işlemi şu şekildedir. Eğer tanıma işleminin yapıldığı yer doğru ise konum modülü başarıyla geçilir, tarih ve saat verileri kontrol edilir eğer doğru zamanda doğru yerde kişi doğrulama işlemi yapılıyorsa bir sonraki adıma geçilir, son olarak NFC modülü ve/veya yüz modülü, etkinliğin geçerliliğini teyit ederse uygulamanın kişi tanıma işlemi başarıyla tamamlanmış olur. Sembolik gösterim Şekil 5.26 'da verilmektedir.

6. ARAŞTIRMA VE BULGULAR

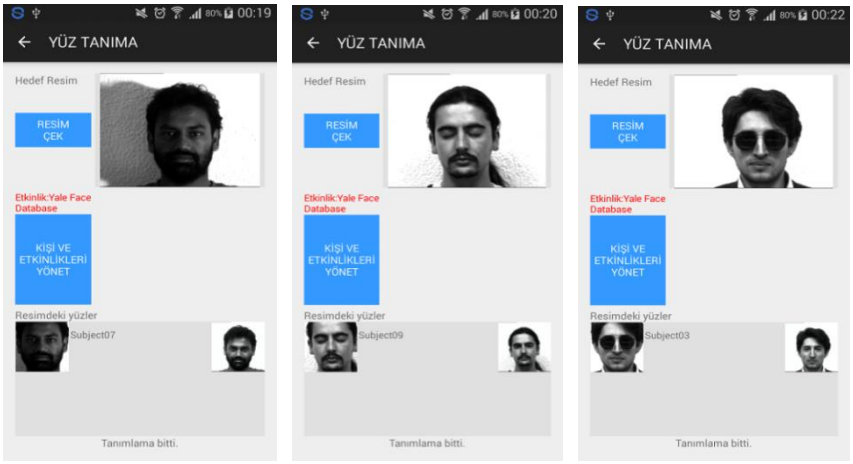
Tez kapsamında geliştirilen bulut tabanlı davetli kişi kontrol mobil uygulaması, Yale yüz veri tabanı ile test edilip, confusion (karışıklık) matrisleri oluşturuldu.

Yale yüz veri tabanı, GIF formatında 165 gri tonlamalı resim içerir. Bu popüler yüz veri tabanında kişi başına 11 resim düşmekte ve 15 kişiden oluşmaktadır. Bu resimler kategorize edilir ve farklı yüz ifadeleri veya farklı resim kategorileri teker teker her bir kişi için alınıp test edilir. Bu test edilen resim kategorileri şunlardır; merkez ışık, gözlüklü, mutlu, sol ışık, gözlüksüz normal, sağ ışık, üzgün, uykulu, şaşkın ve göz kırpması. Veri kümesinin boyutu 6.4 MB'tır (Yale Face Database, 2016). Sonuç olarak tez kapsamında geliştirilen mobil uygulamasına öncelikle Yale yüz veri tabanındaki 15 kişiden her birinin birer normal fotosu kaydedilir (Şekil 6.1).



Şekil 6.1. Yale yüz veri tabanı etkinliği oluşturuldu

Mobil uygulaması üzerinden oluşturulan Yale yüz veri tabanı etkinliği ve bu etkinlikteki kişilerin testleri şekil 6.2'deki gibi yapılır. Şekil 6.2'de ki Yale yüz veri tabanı test edilme ekranına dikkatli bakılırsa her bir kişinin bir çok özellikli resimleri test edilmiştir. Bu çeşitli özellikteki resimler, normal, gözlüklü-gözlüksüz, merkez ışıklı, sağ ışıklı, sol ışıklı, mutlu, üzgün, uykulu, göz kırpma gibi birçok fonksiyonlu kategoriden oluşmaktadır. Bu çeşitli resimler her bir kişi için ayrı ayrı test edilmiştir. Bu kadar güçlü bir yüz veri tabanı üzerinden yüz tanıma modülü'nün test edilmesi önemlidir. Şekil 6.2'de tez kapsamında geliştirilen mobil uygulamadaki yüz tanıma modülü'nün Yale yüz veri tabanındaki kişilerin farklı kategorideki resimlerinin test işlemleri sonuçlarından bazı örnekler gözükmektedir.



Şekil 6.2. Yale yüz veri tabanı etkinliğinin test edilmesi

Bu testler sonucunda, confusion (karışıklık) matrisinin sonuç değerleri aşağıdaki formüller ile oluşturulmuştur. True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN), etkinlik(Sensitivity), doğruluk(Accuracy), hata oranı(Miss Rate), seçicilik(specificity), F1 Score, Matthews Correlation Coefficient (MCC), denklemleri 1-6 aşağıdaki gibidir.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Miss\ Rate = \frac{FN}{FN+TP} \quad (2)$$

$$Sensitivity = \frac{TP}{FN+TP} \quad (3)$$

$$Specificity = \frac{TN}{FP+TN} \quad (4)$$

$$F1-score = \frac{2TP}{2TP+FP+FN} \quad (5)$$

$$MCC = \frac{TP*TN-FP*FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TP+FN)}} \quad (6)$$

		Predicted															
		01.	02.	03.	04.	05.	06.	07.	08.	09.	10.	11.	12.	13.	14.	15.	Null
Actual	01.	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	02.	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	03.	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0	0
	04.	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0	0
	05.	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0	0
	06.	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0	0
	07.	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0	0
	08.	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0	0
	09.	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0	0
	10.	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0	0
	11.	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0	0
	12.	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0	0
	13.	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0	0
	14.	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0	0
	15.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10	0

Şekil 6.3. Yüz tanıma modülü'nün confusion (karışıklık) matris sonucu

Bu matrisinin sonuçlarına göre yukardaki (1), (2), (3), (4), (5), (6) formüllerini kullanarak elde edilen sonuçlar çizelge 6.1'deki gibidir.

Çizelge 6.1. Bulut tabanlı yüz tanıma modülü'nün doğruluk sonuçları

BULUT	Ortalama Doğruluk	Ortalama F1 değeri	Ortalama MCC	Ortalama Etkinlik
Normal	%100	%100	%100	%100
Normal – Merkez Işıklı	%100	%100	%100	%100
Normal-Mutlu	%100	%100	%100	%100
Normal- Sol ve Sağ Işıklı	%100	%100	%100	%100
Ortalama	%100	%100	%100	%100

Tez kapsamında geliştirilen uygulamanın yüz tanıma modülü'nün doğruluk oranları çizelge 6.1'de verilmiştir.

Çizelge 6.1'deki sonuçlara bakılırsa, Yale yüz veri tabanı ile bulut tabanlı davetli kişi tanıma uygulamasına toplam 165 fotoğraf üzerinden doğruluk testi yapılmıştır. Bu testlerin sonucunda %100'e yakın başarı elde edilmiştir.

Uygulamanın yüz tanıma modülünde, 15 kişinin 11'er değişik 165 resmi tek tek test edilip, tüm resimler yüz modülü tarafından başarıyla tanınmıştır. Çizelge 6.1 de görüldüğü üzere doğruluk oranları %100 çıkmıştır.

Tez kapsamında geliştirilen mobil uygulamanın yüz tanıma modülü'nün doğruluk testleri çizelge 6.1'de incelenmişti.

Şimdi literatürdeki Tang vd. (2003), yüz tanıma makinesi adlı tez çalışmasındaki yüz tanıma modülü'nün doğruluk sonuçlarını inceleyelim.

Çizelge 6.2 ve 6.3'de literatürdeki Tang vd. (2003), çalışmasıyla, tez kapsamında geliştirilen uygulamanın yüz tanıma modüllerinin doğruluk oranları karşılaştırılmıştır.

Bu karşılaştırma işleminde Yale yüz veri tabanında ki fotoğraflar kullanılmıştır, Tang vd. (2003), çalışmasında ki yüz tanıma modülünü Yale yüz veri tabanı ile test edildiğinde çizelge 6.2 ve 6.3'deki sonuçlar ortaya çıkmıştır. Bu sonuçlar incelendiğinde Tang vd. (2003), çalışmasında Yale yüz veri tabanındaki kişilerin, normal, normal-merkez ışıklı, normal-mutlu, normal-sol ve sağ ışıklı fotoğrafları üzerinden yapılan test sonuçlarından elde edilen yüz tanıma başarı oranı %81-%97 arasında çıkmıştır.

Tez kapsamında geliştirilen bulut tabanlı yüz tanıma modülünde ki başarı oranı daha yüksek çıkmıştır.

Çizelge 6.2. Literatürdeki bir Eigen face yüz tanıma modülü doğruluk sonuçları (Tang vd., 2003)

Eigen face	Ortalama Doğruluk	Ortalama F1 değeri	Ortalama MCC	Ortalama Etkinlik
Normal	0,97	0,71	0,73	0,59
Normal – Merkez Işıklı	0,97	0,72	0,74	0,59
Normal-Mutlu	0,97	0,72	0,74	0,58
Normal- Sol ve Sağ Işıklı	0,97	0,73	0,75	0,6
Ortalama	0,97	0,72	0,74	0,59

Çizelge 6.3. Literatürdeki bir Fisher face yüz tanıma modülü doğruluk sonuçları (Tang vd., 2003)

Fisher face	Ortalama Doğruluk	Ortalama F1 değeri	Ortalama MCC	Ortalama Etkinlik
Normal	0,96	0,65	0,68	0,56
Normal – Merkez Işıklı	0,97	0,79	0,79	0,74
Normal-Mutlu	0,97	0,76	0,77	0,67
Normal- Sol ve Sağ Işıklı	0,99	0,88	0,89	0,89
Ortalama	0,97	0,77	0,78	0,72

Tang vd. (2003), adlı çalışmadaki Eigen face, Fisher face gibi popüler yüz tanıma algoritmalarını kullanarak geliştirilen yüz tanıma modülü'nün confusion (karışıklık) matrisinden elde edilip hesaplanan doğruluk sonuçları çizelge 6.2 ve 6.3'de gözükmektedir. Tez kapsamında geliştirilen yüz tanıma modülü ile doğruluk sonuçları karşılaştırıldığında, Tang vd. (2003) çalışmasında, 86.1% ile 97.8% arasında doğruluk sonuçlarının alındığı görülmüştür. Tez kapsamında geliştirilen yüz tanıma modülünde bu başarı oranı %100 çıkmıştır.

7. SONUÇ VE ÖNERİLER

Günlük binlerce öğrenci, akademik personel üniversite kampüslerine giriş yaparak kampüs içinde yemekhane, kütüphane ve dersliklerden faydalanmaktadır. Ayrıca günlük hayatta binlerce toplantı, davet gibi etkinlikler düzenlenmektedir.

Bu tez kapsamında geliştirilen uygulamayla, ister NFC kart kullanılsın, ister davetlinin yüzü kontrol edilsin, her hangi bir etkinlik örneğin; bir toplantı, düğün gibi etkinlikteki davetliler bu sistem ile çok rahatlıkla kontrol edilebilir.

Tez kapsamında geliştirilen uygulamanın yüz tanıma modülü'nün, Yale yüz veri tabanı ile test edilip karışıklık matrislerini çıkarılıp doğruluk sonuçlarının %100'e yakın başarı sağlaması çok büyük bir avantajdır. Diğer birçok yüz tanıma modülünde örneğin, popüler fisher faces, eigen faces gibi algoritmaları kullanarak geliştirilen yüz tanıma sistemlerinde, testlerin doğruluk başarı oranları maksimum %97-%99 oranlarında gözükmektedir. Tez kapsamında kullanılan SAAS(Software as a service) yüz tanıma modülünde bu başarı oranı Yale yüz veri tabanı testleri sonucunda %100'e yakın doğruluk göstermiştir. Çizelge 7.1'de, literatürdeki çalışmalardan Yale yüz veri tabanı ile test edilen yüz tanıma sistemlerin bu tez kapsamında geliştirilen uygulamadaki yüz tanıma modülü ile doğruluk sonuçları karşılaştırılması vardır.

Çizelge 7.1. Literatürdeki yüz tanıma çalışmalarıyla karşılaştırma sonuçları

Refs.	**Uygulanan Methodlar**	**Doğruluk %**	**Not**
(Deniz vd., 2003)	SVM+PCA SVM+ICA	99.39% 99.39%	Sadece doğruluk karşılaştırıldı
(Tang vd., 2003)	Face recognition committee machine (FRCM) includes Eigen face, Fisher face, Elastic Graph Matching (EGM), SVM, and Neural network	86.1% ile 97.8% arasında	Sadece doğruluk karşılaştırıldı
(Huang vd., 2004)	Markov random field (MRF)	96.11	Sadece doğruluk karşılaştırıldı
Uygulanan Çalışma	Cloud (Bulut), Saas	100%	Doğruluk ve diğer metrikler karşılaştırıldı

Çizelge 7.1'de görüldüğü gibi diğer yapılan çalışmalarla karşılaştırma yapıldığında, uygulanan çalışma yani bu tez kapsamında geliştirilen cloud (bulut) tabanlı çalışmanın sonuçları daha başarılıdır.

Çizelge 7.1'de literatür bölümünde de bahsedildiği üzere Deniz vd. (2003), bağımsız

bileşen analizi ve destek vektör makineleri kullanılarak yüz tanıma çalışmasının yüz tanıma modülü'nün başarı oranı %99.39. Tang vd. (2003), yüz tanıma yapan makine çalışmasındaki yüz tanıma başarı oranı %86.1 ile %97.8 arasında değişmektedir. Huang vd. (2004), Markov random field algoritmasını kullanarak yapılan hibrit yüz tanıma çalışmasında, yapılan yüz tanıma modülü'nün yüz tanıma başarı oranı maksimum %96.11'dir.

Literatürdeki benzer çalışmalarda, NFC ve yüz bilgileri dışında tez kapsamında geliştirilen uygulama da kullanılan konum, tarih ve saat gibi önemli bilgiler kullanılmıyor. Etkinlik davetli kontrol uygulamasında, uygulamayı kullanan kullanıcının konum bilgisi ve etkinliğin yapılacağı tarih ve saat bilgisi kullanılmaktadır. Böylece uygulamayı kullanan kullanıcı gerçekten o etkinlik mekânında mı, doğru zamanda mı, kişi tanıma kontrol işlemi yapıyor rahatlıkla bilinebilir.

Tez kapsamında geliştirilen uygulamanın kullanımı oldukça kolaydır. Günümüzde hemen hemen herkes mobil uygulamaları çok sıklıkla kullanmaktır. Geliştirilen uygulamanın ucuz, kolay ve anlaşılır olması çok büyük avantajdır. Geliştirilen etkinlik davetli kontrol uygulamasını kullanmak için, bir tane akıllı Android telefon, Microsoft yüz API key, bu API key'in ayda 30.000 işlemden daha fazla işlem yapacak kurumsal firmalar için aylık yaklaşık 5-10 dolar ücreti olacaktır. Bu API'nin normal kullanım da her hangi bir ücreti yoktur, son olarak uygulamayı kullanmak için PHP sunucu olması yeterlidir. Birçok bedava PHP sunucuları olması ve Microsoft yüz API'nin ücretsiz seçeneğinin olması sadece bir akıllı telefon ve geliştirilen mobil uygulama ile toplantı, düğün, ders gibi çeşitli etkinlikler kolaylıkla kontrol edilebilir. Üstelik geliştirilen mobil uygulamanın sunucu bazlı olması, kullanıcının sadece kendi telefonuna bağımlı kalmasını ortadan kaldırıyor, kullanıcı herhangi bir akıllı Android telefon ile kendi kullanıcı adı ve şifresiyle önceden oluşturduğu etkinlik ve davetlileri kontrol edebilir. Uygulamada NFC kart bilgisi kullanarak da kişi tanıma yapılıyor fakat kişilerin kartları unutması bazen problemler oluşturabiliyor, yüz tanıma sisteminin biyometrik bir sistem olması ve benzersiz bir sistem olması büyük avantajdır.

Sonuç olarak, bu tez çalışmasında, yüz tanıma modülü, NFC kartlar modülü, konum modülü ve tarih ve saat modülü kullanılarak etkinlik davetli kontrol (kişi tanıma) sistemi geliştirilmiştir. Böylece etkinliğe gerçekten davetli olan kişileri kolaylıkla mobil cihazlardan tanınarak kontrolü sağlanmıştır.

KAYNAKLAR

Akın H., Karaçam B., Gürpınar K., 2002. Kimliklendirmede Biyometrik Yöntemlerin Kullanım Alanları. Yıllık Adli Tıp Toplantıları, Antalya, 16-19 Mayıs, 48-51.

Adalan K., 2017. Yüz Tanıma, NFC ve Ses Kontrollü Kapı Kilidi Açma Sistemi. Yıldız Teknik Üniversitesi, Elektrik Elektronik Fakültesi, Yüksek Lisans Tezi, 53, İstanbul.

A. K. Jain, A. Ross ve J. Shah, 2007. From template to image: reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4), 544–560.

Antonia R., Andrea C., 2013. Identity verification through face recognition, Android smartphones and NFC. World Congress on Internet Security (WorldCIS-2013), Italy, 22 March, 162-163.

Arslan B., Sağıroğlu Ş., 2016. Mobil Cihazlarda Biyometrik Sistemler Üzerine Bir İnceleme. Politeknik Dergisi, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, 19(2), Ankara, 101-114.

Battini Sönmez E, Özbek N. Ö, Özbek Ö., 2007. Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi, Akademik Bilişim 2007.

Bowersox, D.J., Closs, D.J., ve Cooper, B.M. 2002. Supply Chain Logistics Management. McGraw Hill, Burr Ridge, Boston.

Christopher, M. 1998. Logistics and Supply Chain Management: Strategies for reducing cost and improving service, (2nd Ed.), Prentice Hall, New York.

Femila M.D., Irudhayaraj A.A., 2011. Biometric system. 3rd International Conference on Electronics Computer Technology, Kanyakumari, 8-10 April, 152-156.

Geleceği Yazanlar Turkcell, Android İşletim Sistemi Üzerine Genel Bilgiler, 2011. Erişim Tarihi: 10.08.2017. https://gelecegiyazanlar.turkcell.com.tr/konu/android/egitim/android-201/android-cihazlar-ve-android-isletim-sistemi-uzerine-genel-bilgiler

Grassie K., 2007. Easy handling and security make NFC a success, Card Technology Today, 19(10), 12–13.

Huang R., Pavlovic V., and Metaxas D.N., 2004. A hybrid face recognition method using Markov random fields. Proceedings of the 17th International Conference on Pattern Recognition ICPR 2004, Cambridge, 23-26 August, 157-160.

JSON, 2017. JSON'a Giriş. Erişim Tarihi: 15.08.2017. https://www.json.org/json-tr.html

Kakıcı, A., 2008. Biyometrik Tanıma Sistemleri. Erişim Tarihi: 15.09.2017. https://ahmetkakici.github.io/genel/biyometrik-tanima-sistemleri

Microsoft Yüz API Dokümantasyon, 2017. Erişim Tarihi: 20.10.2017. https://docs.microsoft.com/tr-tr/azure/cognitive-services/face/overview

NearFieldCommunication.org, 2017. Erişim Tarihi: 23.05.2017. http://www.nearfieldcommunication.org/how-it-works.html

NFC World, 2016. Erişim Tarihi: 12.08.2017. http://www.nfc-world.com/en/about/03.html

NFC Research Lab, 2016. Erişim Tarihi: 22.08.2017. https://nfclab.com/tr/aboutnfc.html

Narol T., 2014. NFC teknolojisinin toplu ulaşımda uygulanması. Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 69, İstanbul.

O. Deniz, M. Castrillon, M. Hernandez, 2003. Face recognition using independent component analysis and support vector machines. Pattern Recognition Letters, 24(1), 2153-2157.

Assarasee P., W. Krathu, T. Triyason, V. Vanijja and C. Arpnikanondt, 2017. Meerkat: A Framework for Developing Presence Monitoring Software based on Face Recognition. 2017 10th International Conference on Ubi-media Computing and Workshops (Ubi-Media 2017), Thailand, 1-4 August, 171-177.

Pei-Ju Wu, Mu-Chen Chen, Chih-Kai Tsau, 2017. The data-driven analytics for investigating cargo loss in logistics systems. International Journal of Physical Distribution and Logistics Management, 47(1), 68-83.

Picasso, 2017. Picasso Android Kütüphanesine Giriş. Erişim Tarihi: 10.05.2017. http://square.github.io/picasso/

Şamlı, R. ve Yüksel M.E., 2009. Biyometrik Güvenlik Sistemleri, Akademik Bilişim'09

Tang H., Lyu M., and King I, 2003. Face recognition committee machine. In Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2003), 2(1), 837- 840.

Yale Face Database, 2016. Erişim Tarihi: 17.03.2017. http://vismod.media.mit.edu/vismod/classes/mas622-00/datasets/

ÖZGEÇMİŞ

Adı Soyadı	: Zeynel Erdi KARABULUT
Doğum Yeri ve Yılı	: Kadıköy, 24/04/1989
Medeni Hali	: Evli
Yabancı Dili	: İngilizce
E-posta	: erdi_karabulut@yahoo.com.tr

EĞİTİM DURUMU

Lise	: Beykoz Fevzi Çakmak Anadolu Lisesi, 2006
Lisans	: İstanbul Ticaret Üniversitesi, Mühendislik ve Tasarım Fakültesi, Bilgisayar Mühendisliği Bölümü
Yüksek Lisans	: İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, 2015-...(devam ediyor)

MESLEKİ DENEYİM

Erk Teknoloji Hizmetleri A.Ş 2013-...(devam ediyor)