T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

KAMUDA GÜVENLİK AMAÇLI KULLANILAN BİYOMETRİK SİSTEMLERİN KARŞILAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Tanyel YÜCEL

Danışman
Yrd. Doç.Dr. Hüseyin ÇAKIR

Ankara – 2015

T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

KAMUDA GÜVENLİK AMAÇLI KULLANILAN BİYOMETRİK SİSTEMLERİN KARŞILAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Tanyel YÜCEL

Danışman

Yrd. Doç.Dr. Hüseyin ÇAKIR

Ankara – 2015

ONAY

Tanyel YÜCEL tarafından hazırlanan "Kamuda Güvenlik Amaçlı Kullanılan Biyometrik Sistemlerin Karşılaştırılması" başlıklı bu çalışma, 2.../03/2015 tarihinde yapılan savunma sınavı sonucunda (oybirliği / ~~oyçokluğu~~) ile başarılı bulunarak jürimiz tarafından Adli Bilimler Anabilim dalında Yüksek Lisans tezi olarak kabul edilmiştir.

.....

Doç. Dr. Mehmet Akif OCAK (Başkan)

.....

Doç. Dr. Şenol YAPRAK

.....

Yrd. Doç. Dr. Hüseyin ÇAKIR (Danışman)

TELİF HAKLARI BEYANNAMESİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yüksek lisans tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir; bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir mercii tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

Tarih 02/.03/.2015

Tanyel YÜCEL

III

ÖNSÖZ

Bu araştırmanın gerçekleşmesinde yardım ve katkıları olan herkese teşekkürü bir borç bilirim. Tez konusunun belirlenmesinde ve araştırma sürecinde beni yönlendiren aramızda uzun mesafeler olsa da bir telefon yakınımda olan kıymetli hocam Yrd.Doç. Dr. Hüseyin ÇAKIR'a, araştırma sürecinde bilgi ve birikimlerini benden esirgemeyerek bana yol gösteren Yrd.Doç.Dr. Ahmet GÜNEYLİ ve Yrd.Doç.Dr. Özhan ÖZTUĞ'a ayrıca bu süreçte çalışmalarımda bana destek olan arkadaşlarım Fehim YELTEKİN ve Hasan UMUR'a sonsuz teşekkürler.

ÖZET

T.C.

Polis Akademisi

Güvenlik Bilimleri Enstitüsü

Adli Bilimler Anabilim Dalı

Kamuda Güvenlik Amaçlı Kullanılan Biyometrik Sistemlerin Karşılaştırılması

Hazırlayan: Tanyel YÜCEL

Yüksek Lisans Tezi

Tez Danışmanı: Yrd.Doç.Dr.Hüseyin ÇAKIR

2015 - 79 Sayfa (Ekler hariç)

Günümüzde geçmişe göre bir bölgeye izinsiz girme gibi konuların oldukça güç bir hale gelmesinde güvenlik sistemlerinin katkısı büyüktür. Güvenlik sistemlerinin tarihsel süreçteki gelişimi incelendiğinde, en önemli değişimin bilgisayar teknolojilerinin gelişimi ile birlikte yaşandığı görülmektedir. Bundan önceki dönemde daha çok mekanik yöntemlerle yapılan güvenlik kontrolleri, bu dönemden sonra daha dijital sistemlerle, bilgisayar üzerinden ve daha yüksek kesinlikle yapılmaktadır. Bu noktada biyometrik sistemler devreye girmektedir. Biyometrik Sistemlerde kullanılan biyometrik veri, biyolojik olarak sahip olduğumuz veri olup, insan biyolojisinin değişmesi çok zor olan özelliklerini içermektedir.

Bu Çalışmada Biyometrik sistemlerin avantajları ve dezavantajları ortaya çıkarılarak karşılaştırılması amaçlanmıştır. Biyometrik sistemleri karşılaştırmak için çalışma 17 alt başlık altında incelenmiştir. Çalışmanın amacına uygun olarak kamu kurumunda biyometrik sistem kullanan toplam 82 personel ile anket gerçekleştirilmiştir. Araştırmada nicel ve nitel veriler toplanmış ve araştırma deseni "genel tarama modeli" olarak belirlenmiştir. Ayrıca, biyometrik sistemlerle ilgili yerli ve yabancı kaynaklar incelenmiştir. Verilerin çözümlenmesinde, yüzde, frekans, aritmetik ortalama, standart sapma ve ki kare hesaplaması kullanılmıştır.

Biyometrik sistemlerin güvenilir sistemler oldukları ve irdelenen biyometrik sistemlerin kendilerine göre eksileri ver artıları olduğu saptanmıştır.

Anahtar Kelimeler: Biyometrik Sistemler, Güvenlik Sistemleri, Biyolojik Ölçüm, Biyometrik Veri, Kamu.

ABSTRACT

Police Academy

Institute of Security Sciences

Department of Forensic Science

The Comparison of Biometric Systems Used for Security Purposes in Public

Tanyel YÜCEL

Master's Thesis

Supervisor: Asst.Prof.Dr.Hüseyin ÇAKIR

2015 - 79 Pages (Excluding appendices)

Security systems have a great impact on reducing unauthorized enterances when compared to the past. When we analyse the development of security systems through history, it is evident that the greatest difference has been maintaned with the development of computer technology. Before computer technology, security control was maintained withmechanical methods, however with computer technology security is maintained with digital systems, through computers and with higher reliability. Biometrics Systems come into action at this point. Biometric data which is used in biometric systems are the biological data which we have and it includes features of human biology which are very hard to change.

This study aims to ıdentify the advantages and disadvantages of Biometric Systems and make a comparison of the Biometric Systems. In order to compare the Biometric Systems, the study has used 17 sub headings. A questionaire has been administered to 82 staff members who are working with Biometric Systems in public offices. Quantitative and qualitative data has been collected through out the research. The analysis design/method used is general searching method. Local and international resources have been analyzed about Biometric Systems. Percentage, frequency, arithmetic mean, standart deviation and chi-square calculation has been used in data analysis.

The research results show that Biometric System are reliable systems and the analyzed Biometric Systems each have their own advantages and disadvantages.

Key Words: Biometric Systems, Security Systems, Biological measurements, Biometric Data, Public.

KAMUDA GÜVENLİK AMAÇLI KULLANILAN BİYOMETRİK SİSTEMLERİN KARŞILAŞTIRILMASI

İÇİNDEKİLER

Sayfa

BİRİNCİ BÖLÜM

KURAMSAL ÇERÇVE, İLGİLİ ARAŞTIRMALAR VE LİTERATÜR TARAMASI

İKİNCİ BÖLÜM

KAMUDA GÜVENLİK AMAÇLI KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN KARŞILAŞTIRILMASI

ÜÇÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri

Ar&Ge : Araştırma Ve Geliştirme

ATM : Automated Teller Machine

CASIA : Chinese Academy of Sciences' Institute of Automation

CRM : Customer Relationship Management

DNA : Deoksiribo Nükleik Asit

IBG : International Biometric Group

ID : Identification

OPTS : Otomatik Parmak İzi Tanıma Sistemleri

POS : Point Of Sale

SSK **:** Sosyal Sigortalar Kurumu

SSO : Single Sign On

UCSB : Uni-Characteristic Biometric Systems

UYAP : Ulusal Yargı Ağı Projesi

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

EKLER LİSTESİ

GİRİŞ

Teknolojinin ilerlemesi her alanda olduğu gibi kuşkusuz suç olaylarında da etkisini göstermiştir. Bir yaklaşıma göre geçmişe kıyasla suç olaylarında artış var gibi görünse de bir diğer yaklaşıma göre suçun tespiti ve ortaya çıkmasındaki olanakların artması nedeniyle, suç olayları daha fazla ön plana çıkmaktadır. Teknolojik yenilikler bir yandan suç işleme olanaklarını arttırırken, bir yandan da güvenlik sistemlerinde ciddi ve önemli gelişmelere yol açmıştır. Suçun önlenmesinde ve suç olaylarına karıştıkları tespit edilen kişilerin yakalanmasında güvenlik sistemlerinin büyük önemi vardır. Her geçen gün kullanım oranı, alternatifleri ve imkânları artan güvenlik sistemleri, özellikle kamusal alanlarda önemli katkılara sahiptir.

Kamu ve özel kurumlardaki güvenlik anlayışı arasında her ne kadar ortak noktalar olsa da, ufak farklılıklar vardır. Özel kurumlarda ya da daha doğru ifadeyle özel işletmelerde, güvenlik konusu daha sınırlı olup, işletme sorumluları güvenliği sağlamakla görevlidir. Öte yandan kamu kurumlarında ise güvenlik sadece o kurumu değil, aynı zamanda tüm kamuyu da ilgilendiren bir konudur. Bu noktada, kamu yararı ve kamusal değerlerin korunması kavramları ön plana çıkmaktadır. Dolayısıyla kamusal görev yapan kurumların güvenlikleri sağlanırken, sadece kurum içerisindeki korunması gereken değerlerin değil, aynı zamanda kamusal yarar sağlayan iç ve dış değerlerin de korunması gerekir.

Esasen güvenlik konusu ve belli bir bölgenin izole edilerek korunma altına alınması, gerek evrensel insan hakları, gerekse evrensel hümanizma düşüncesine aykırıdır. Diğer yandan günlük yaşamımızdaki pratik bilgiler ve uygulamalar, güvenlik hususunun gerekli olduğunu ve teori ile uygulama arasında ciddi farklılık olduğunu göstermektedir. Bu nedenle, kamuya ait olan bir kurum dahi olsa, o kurumun yine kamunun genelinden ayrılması ve ayrı bir güvenlik sistemi ile korunması gerekmektedir. Söz gelimi bir garnizon komutanlığı aslında tüm ülkenin ortak malı olsa da, herkesin buralara girmeye hakkı yoktur. Dolayısıyla kamu kurumlarında güvenlik konusunun sadece kriminal ve teknolojik anlamda değil, sosyolojik anlamda da ele alınması gereken konuları ve sorunları vardır.

Bu çalışmada ise güvenlik sistemlerinin teknik ve kullanım açısından incelenmesine yer verilmiştir.

Güvenlik sistemlerinin tarihsel süreçteki gelişimi incelendiğinde en önemli değişimin kuşkusuz bilgisayar teknolojilerinin gelişimi ile birlikte yaşandığı ifade edilebilir. Bundan önceki dönemde daha çok mekanik yöntemlerle yapılan güvenlik kontrolleri, bu dönemden sonra daha dijital sistemlerle, bilgisayar üzerinden ve daha yüksek kesinlikle yapılmaktadır.

Günümüzde geçmişe göre suç işleme ya da bir bölgeye izinsiz girme gibi konuların oldukça güç bir hale gelmesinde de güvenlik sistemlerinin katkısı vardır. Her ne kadar bilgisayar ve programları insan tarafından geliştirilmiş olsa da hiçbir insanın yapamayacağı hassasiyette güvenlik kontrolü yapabilmektedir. Bu nedenle güvenlik sistemlerinin bilgisayar destekli olması ve bu sistemlerin yaygınlaşması kaçınılmazdır.

Güvenlik sistemlerinde biyometrik sistemlerin kullanımının temel mantığı, biyometrik değerlerin değiştirilememesinden kaynaklanmaktadır. Bir güvenlik sistemini yapay olan verilerle değiştirmek mümkündür. Ancak biyometrik veri, biyolojik olarak sahip olduğumuz veri olup, insan biyolojisinin iris, ses, parmak izi gibi değişmesi çok zor olan özelliklerinin ölçümü üzerinden işlemektedir. Bu nedenle, biyometre parametreleri ölçümü üzerinde kurulmuş olan sistemler, hata payı sıfıra yakın bir kesinlikte görevlerini yerine getirmektedir.

Güvenlik sistemleri; sistemin maliyeti, kullanılabilirliği, güvenlik sağlanacak yerin ve güvenliği korunacak kitlenin yapısına göre değişiklik gösterebilmektedir. Örneğin deoksiribo nükleik asit **(**DNA**)** yöntemi çok kesin bir yöntem olsa da bir maç girişinde ya da bir kamu kurumu girişinde kullanımı çok mantıklı değildir. Her ne kadar DNA yöntemine göre daha düşük kesinliği olsa da parmak izi ya da iris, bu yerler için daha idealdir. Benzer şekilde, farklı sistemlerin farklı güvenlik amaçlarına göre avantajları ve dezavantajları vardır. Bu nedenle en uygun yöntemin seçilmesi için öncelikle güvenlik sisteminin temel amaç ve yöntemlerinin iyi bir şekilde analiz edilmesi gerekir. Bu çalışmada bu amaçlanmış olup, farklı güvenlik sistemlerinin analizine yer verilmiştir.

BİRİNCİ BÖLÜM
KURAMSAL ÇERÇEVE, İLGİLİ ARAŞTIRMALAR VE LİTERATÜR TARAMASI

1.1. KURAMSAL ÇERÇEVE

Bu bölümde araştırma ile doğrudan ilgili konuları içeren kuramsal bilgiler verilmeye çalışılmıştır. Bu amaçla Kamuda, güvenlik amaçlı kullanılan biyometrik sistemler üzerine görüşlerin alınması ve bu sistemlerin karşılaştırılması için öncelikle biyometrik sistemlerin neler olduğu, bunların temelinde yatan bilgi ve bilgi toplumuna geçiş süreci, bu sürecin sonucunda ön plana çıkan bilgi güvenliği ve genel olarak güvenlik hususları gibi konuların bilinmesi gerekir. Çalışmanın bu bölümünde bu amaçla, bilgi ve bilgi toplumuna geçiş süreci, bilgi güvenliği, biyometrik sistemlerin tanımı, çeşitleri, kullanım yararları, sakıncaları, kamuda biyometrik sistemlerin kullanımı ve biyometrik olmayan kartlı sistemler gibi konulara kısaca değinilmiştir.

1.2. İLGİLİ ARAŞTIRMALAR

Biyometrik sistemler, gerek kullanım alanları gerekse teknik açıdan teknolojik gelişmelerle ilgili konulara odaklanmış birçok çalışmada ele alınmaktadır. Bu çalışmalardan bir bölümü mevcut sistemlerin güvenilirliğini ve kesinliğini arttırmaya yönelik mühendislik çalışmaları olup, daha çok elektronik ve bilgisayar mühendisliği ilgi alanlarındadır. Diğer bir bölüm çalışma ise bu sistemlerin kullanımındaki etik değerler, bilgi güvenliği gibi sosyal konulara yoğunlaşmaktadır.

Singleton 2003 yılındaki çalışmasında, biyometrik güvenlik sistemlerinin bilgi güvenliğinde en iyi seçeneğinin hangisi olduğu sorusuna yanıt aramıştır. Daha önce dış saldırılara karşı bilgi güvenliği ve saldırılara karşı bilgi güvenliği konularını inceleyen serinin üçüncüsü olan çalışmada, bilgi güvenliğinde daha çok iç tehditler üzerinden biyometrik sistemler değerlendirilmiştir. Çalışmada yaygın olarak kullanılan biyometrik sistemler kıyaslanmış ve farklı bilgi güvenliği amaçlarına göre

en uygun seçeneğin ne olacağı sorunu üzerinde durulmuştur. Bu çalışmada da, en uygun biyometrik sistemin, istenilen güvenliğe göre değiştiği rapor edilmiştir.

Yöneticilerin, biyometrik sistemleri kullanmalarındaki, planlı davranış teorisini inceleyen Seyal ve Turner'in 2013 yılındaki çalışmasında, Brunei Darussalam hükümetinin e-devlet projesinin konusu olan, 10 bakanlıktan 155 yönetici üzerinde araştırma yapmıştır. Araştırma sonuçlarına göre biyometrik kullanımı davranış eğiliminin bir tahmin edicisi olarak rapor edilmiştir.

2004 yılındaki çalışmasında, biyometrik sistemlerde tanıma problemi üzerinde duran Rukhin, farklı biyometrik sistemlerin ortak noktası olan tanıma aşamasının matematiksel ifadesinin kesinliği nümerik olarak incelenmiştir. Çalışma sonuçlarına göre, formülde ayrık noktaların çokluğu, tanımlamanın keskinliği ile ilişkilidir.

Biyometrik tanımlama konusunu inceleyen Richards, çalışmanın ele alındığı 1997 yılında oldukça sınırlı olan bu sistemlerin türlerinden çok, genel olarak geçerlilik ve güvenilirlikleri, tutarlılıkları, verilerin kaydedilmesi ve derlenmesi gibi konulara değinilmiştir.

Robb 2002 yılında yaptığı çalışmada, biyometrik teknolojinin o dönemki güncel durumunu değerlendirmiştir. Çalışmada, bu çalışmada da değinilen biyometrik yöntemler hakkında bilgi verilerek, bunların kesinliği üzerinde durulmuştur. Daha sonra bu sistemlerin bilgisayar teknolojileri ile ilişkisi incelenerek, günümüz teknolojileri ile ilgili çıkarımlarda bulunulmuştur.

Biyometrik sistemler ve gizlilik konusunu inceleyen Ploeg (2003) çalışmasında, teknolojinin teorileşmesi konusuna değinmiştir. Çalışmada, biyometrik sistemler ilk olarak bir gizlilik sorunu olup olmadığı şeklinde ele alınmış, daha sonra ise teknolojik determinizm açısından ele alınmıştır. Çalışmada daha çok sosyolojik açıdan değerlendirilen biyometrik sistemlerle ilgili genel yargılardan kaçınıldığı görülmektedir.

Palombo 2011 yılında, Biyometri: Yapılar, Teknolojiler, Biyopolitikalar isimli, Joseph Pugliese tarafından yazılan kitabın özetini ve yorumunu yapmıştır. Çalışmada konuya ilişkin diğer çalışmalara paralel olarak, bu sistemlerin bir özel yaşam gizliliği sorunu olup olmadığı ve teknolojik yeri incelenmiştir.

Biyometrik teknolojilerin fonksiyonelliği, yeni trendler ve güvenlik açıklarını inceleyen Nardo (2008) yaptığı çalışmada, bu sistemlerin günlük yaşamımızdaki mevcut yeri ve geleceği incelenmiştir. Yazara göre bu sistemler günümüzde her ne kadar yetişkinler için geçerli sistemler olsa da gelecekte gündelik yaşamın bir parçası olacaktır.

Laux ve diğerleri 2011 yılındaki çalışmalarında, biyometrik otorizasyon sistemlerinin adaptasyonunu ve son kullanıcılara güvenlik sistemlerinin açılmasında kullanımını incelemişlerdir. Çalışmada, bu sistemlerin entegrasyonunda yönetimin desteğinin olmasının, sisteme adaptasyon üzerinde ciddi bir etkisinin olmadığı rapor edilmiştir. Diğer bir ifadeyle sisteme adaptasyonda yöneticinin yaklaşımının istatistiksel olarak anlamlı bir etkisi yoktur.

Biyometrik sistemler ve geniş çaptaki sivil tanımlamada kullanımını hukuki açıdan inceleyen Hopkins, 1999 yılında yapmış olduğu bu çalışmada, sistemlerin sınırları, geçerliliği, güvenilirliği gibi konulara yer verilmiş, daha sonra ise bu sistemlerin geleceği ile ilgili öngörülerde bulunulmuştur.

Jali ve diğerleri 2014 yılında yapmış oldukları çalışmalarında, çok faktörlü grafiksel şifrelemenin, kullanıcı otorizasyonunda kullanılabilirliğini incelemişlerdir. Çalışmada yazarların üniversitelerinden rastgele seçilen 30 kişi üzerinde uygulama yapılarak, bir imajın şifre olarak kullanımı ile otorizasyon arasındaki ilişki araştırılmıştır. Biyometrik sistemlerde de grafiksel şifre bir anlamda söz konusu olduğundan, sistemin başarısının, biyometrik sistemlerin başarısı ile ilişkili olduğu ifade edilmiştir.

Federal e-devlet uygulamalarında otorizasyon ve gizlilik kavramlarını inceleyen Holden ve Millett, yapmış oldukları 2005 yılındaki çalışmalarında, kamu hukuku çerçevesinde, politikalar ve uygulamaların hukuki ve sosyal açıdan değerlendirilmesine yer verilmiştir.

Gough 2008 yılında yapmış olduğu araştırmada, biyometrik sistemlerin üniversitelerde kullanımını, Davenport üniversitesi örneği ile göstermiştir. Çalışmada, biyometrik sistemlerin üniversite öğrencileri üzerinde uygulanmasının, öğrencilerin biyometrik teknolojiye daha kolay adapte olmalarını sağladığı rapor edilmiştir.

Biyometrik sistemler, kanıt ve kişisel gizlilik kavramlarını 2003 yılındaki çalışmasında inceleyen Freeman, biyometrik sistemler, kişilerin özel yaşamının gizliliği ve kişisel verilerin korunması gibi hukuki normlarla değerlendirilmiştir.

Yağcıoğlu (2008) çalışmasında, kontrollü insan giriş çıkışlarının otomatik olarak yapıldığı durumlarda en yaygın uygulamanın kimlik kartı kullanımının olduğunu ancak bu tür sistemlerin hırsızlık ve kartın farklı kişilerce kullanılması gibi pek çok problemini incelemiştir. Son yıllarda biyometrik tabanlı sistemlerin hem kontrollü otomatik giriş çıkışlarda hem de güvenlik amacıyla yaygın olarak kullanıldığını, iris veya parmak izinden tanımayı sağlayan sistemlerin yakın temas gerektirdiği için genelde tercih edilmediği konusuna değinmiştir. Yüz tanıma tabanlı sistemlerin ise insanlar tarafından rahatsız edici bulunduğunu ve yaygın olan yüz tanıma sistemlerinin iki boyutlu fotoğraflardan tanıma amaçlı olduklarını, iki boyutlu sistemlerin başarılarının bulundukları ortama bağlı olduklarından bahsetmiştir. Yüz tanıma sistemlerinde değişen ışıklandırma, karmaşık arka plan ve değişen poz tanımayı doğrudan ve çok ciddi şekilde etkileyebilen değişkenlerin başında geldiğine değinmiş. Bu noktada üç boyutlu yüz tanıma sistemlerini ve önemini anlatmıştır.

1.3. BİLGİ VE BİLGİ TOPLUMUNA GEÇİŞ

Sanayi devriminden sonra artan üretim ve tüketim, ürünlerin ön plana çıkmasına, hizmet ve bilginin ikinci planda tutulmasına neden olmuştur. Öte yandan tüketimin artmasıyla birlikte, daha fazla üretim gerekmiş ve bunun için ise akıllı teknolojilerin geliştirilmesi ihtiyacı doğmuştur. İşte bu amaçla başlayan araştırma ve geliştirme (Ar&Ge) çalışmaları, günümüzde bilginin önemini giderek arttırmıştır. Özellikle internet ve bilgisayarlı teknolojiler sayesinde, bilgi toplumuna geçiş sağlanmıştır. Çalışmanın bu bölümünde, biyometrik sistemlerin yapı taşı olan bilgi ve bilgi toplumuna geçiş süreci hakkında bilgi verilmiştir.

1.3.1. Bilgi Kavramı

Bilgi kavramı, insanlık evriminin temelini oluşturmuştur. İnsanlık tarihinin; geçmişten günümüze kadar üç önemli aşamadan geçtiği, üç önemli devrim yaşadığı ve dönüşüme uğradığı kabul edilmektedir. Birinci dalga tarım toplumu olarak nitelenir ve milattan önce başlayan bu süreci sanayi devrimine kadar gelir. Günümüzde işletmelerin en değerli varlıklarından birisi haline gelen bilgi, aşağıdaki özelliklere sahiptir (Yıldız ve Tenekecioğlu, 2004:579-590):

- Kıt bir kaynak değildir. Bu nedenle azalan verimler değil, artan verimler yasası geçerlidir.
- Kendi kendini sürekli kümülatif olarak yenileyen sınırsız bir üretim unsurudur.
- Bilgi; sermaye ve toprak gibi birbirine tamamlayan üretim faktörleri değil; aksine onların yerine ikame edilebilen bir üretim faktörüdür.
- Bilgi; sermaye ve toprağa göre çok daha akışkandır, yer değiştirebilir, taşınabilir.
- Bilgi paylaşılabilir ve bölünebilir.
- Toprak ve sermaye gibi özel mülkiyet konusu olup diğer insanları dışlamaz." (H.Erkan ve C.Erkan, 2014:7).

Buckland "bilgi" (information) terimini üç ayrı anlamda ele alarak tanımlamaktadır: (Buckland, 1991)

1- Süreç olarak bilgi: Verilerin bir araya getirilmesi ile oluşturulan anlamlı semboller enformasyon olarak tanımlanmaktadır. Enformasyon genellikle, bireyler veya kurumlar tarafından bir sorunun çözümü, herhangi bir çalışmanın başlatılması ya da bitirilmesi gibi faaliyetler sonucunda ortaya çıkarılan verilerin bütününü ifade etmektedir. İşte bu öğrenme eylemi, birisine bir şeyler aktarma ya da söyleme süreci "süreç olarak bilgi" olarak adlandırılmaktadır.

2- Bilgi olarak bilgi: İngilizce'de "knowledge" kelimesi, değişmez bilgileri ifade eder. Bu süreçte karşı tarafa aktarılan şeye ise "bilgi olarak bilgi" adı verilir.

3- Nesne olarak bilgi: Bilgi terimi, bilgilendirici, bilgi taşıyıcı nesneler için de kullanılmaktadır. Bu anlamda ise "nesne olarak bilgi"den söz etmek mümkündür.

Bilginin üretimi, paylaşımı ve kullanımı konularında araştırma yapan, bilgi üretiminin her aşamasında, bilgi üretimini destekleyici koşulların sağlanması gerektiğini ifade eden, özellikle örtülü bilgiye vakıf olma, bunun açık bilgiye dönüştürülmesi ve bu bilginin paylaşılmasının sağlanması üzerinde duran Von Krogh'a göre, bunların yapılabilmesi için, organizasyon içinde, metaforlar aracılığıyla ortak bir dilin kullanılması gerektiğini ifade etmektedir (akt. Geyik ve Barca, 2004:409-418).

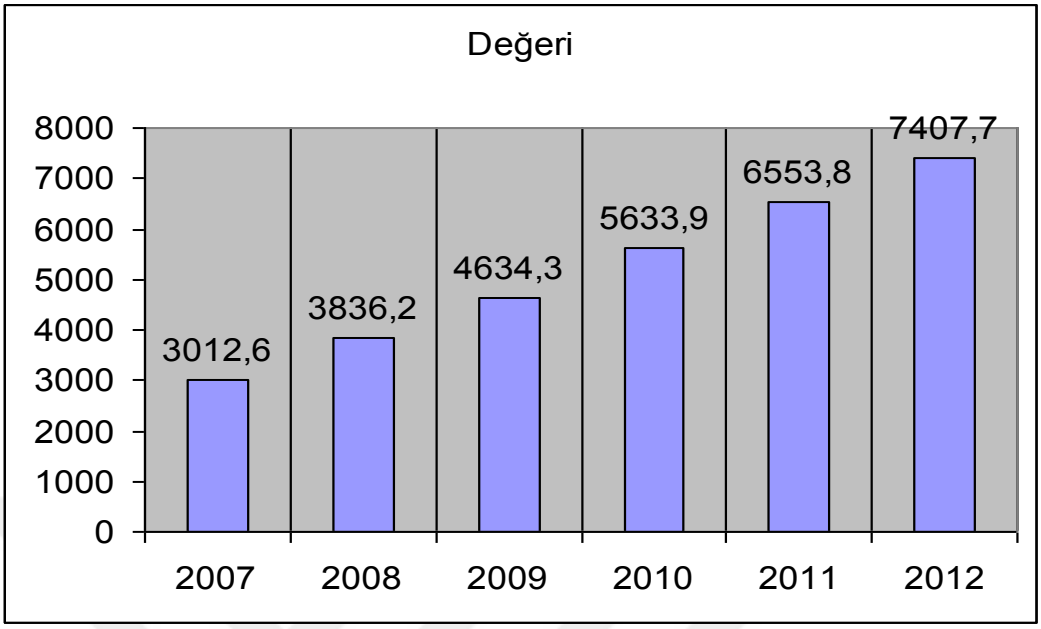
1.3.2. Bilgi Teknolojileri ve Bilgi Toplumu

Bilişim teknolojileri, yönetim kararları alınmasında temel veri kaynağıdır. Ayrıca firma stratejilerini gerçekleştirme ve rekabet üstünlüğünü sağlamada en önemli araçtır. Bilişim teknolojilerinin düzeyi ve kullanabilme kapasitesi işletmelerin "başarı ya da başarısızlığını" belirler. Bilişim teknolojilerinin bütün işletme fonksiyonlarına değer katacak biçimde kullanılması firmaların performansını arttırmakta ve rekabet üstünlüğü sağlamaktadır (Geyik ve Barca, 2004:409-418).

1.3.3. Bilgi Güvenliği

Bilgi güvenliği, son yıllarda bilgi toplumuna geçişle birlikte önemi artan bir konudur. Bilgilerin dijital ortamda saklanmaları, bunlara birden fazla bölgeden erişim imkânlarının bulunması ve toplanan bilgilerin çok kısa sürede, maliyeti çok düşük olan programlar aracılığıyla analiz edilmesi, bu analiz neticesinde de bireylerin sınıflandırılmaları ya da kişisel bilgilerin korunmasının ihlali gibi konular gündeme gelmiştir. Biyometrik sistemlerde ise bilgi güvenliği, kişisel verilerin de ötesine giderek, biyolojik verilerin sınıflanmasını ve kullanımını gündeme getirmektedir. Uluslararası Biyometri Grubu (IBG) tarafından yayınlanan rapora göre, 2007 yılından itibaren biyometrik sistemlerin kullanımı giderek daha yaygınlaşmış olup, günümüzde oldukça ciddi bir sektör haline gelmiştir. 2007 yılından 2012 yılına kadarki süreçte bu değişim, Şekil 1.1'de gösterilmiştir.

Şekil 1.1: Bilgi Güvenliği İçerisinde Biyometrik Sistemlerin Payı



Kaynak: Nabiev, (2009:277).

Şekil 1.1'de görüleceği gibi, 2007 yılından 2012 yılına gelindiğinde, biyometrik sistemlere harcanan bütçenin iki katından fazla arttığı görülmektedir. Bu durum, alınan verilerin ya da toplanan kişisel bilgilerin de arttığı anlamına gelmektedir. Buna ilave olarak, bu artışın iki katın çok üstünde olduğunu ifade etmek mümkündür. Zira 2007 yılında kurulan bir biyometrik sistemin maliyeti, 2012 yılında yaklaşık 8-10 kat azalmıştır. Teknolojinin ilerlemesi ve biyometrik sistem ekipmanlarının ucuzlamasıyla, daha fazla sistemin yaygın hale geldiği ifade edilebilir. Dolayısıyla çok ciddi bir bilgi kümülâtifliği söz konusu olup, bu bilgilerin güvenliği de ciddi önem taşımaktadır.

1.4. BİYOMETRİK SİSTEMLER

Bir biyometrik sistemi en genel haliyle biyolojik ölçüm (biyo-metri) şeklinde tanımlamak mümkündür. Buna göre biyometrik sistemler, biyolojik verilerin ölçümüne dayalı olan ölçüm sistemleri olup, bu verilerin daha sonra güvenlik amaçlı kullanımı konusunu içermektedir.

Buna göre her biyolojik verinin ölçümü biyometrik sistemlere konu olabilmektedir. Diğer yandan, her biyolojik veri biyometrik sistemlerin üretilme ya

da geliştirilme amacına uygun olmayabilir. Örneğin parmak sayısı, kollarda kemik oranları gibi biyolojik veriler, biyometrik sistemlerin konusu olamazlar. Her ne kadar tanımına göre bunlar biyolojik veri olup, bunların ölçümü biyometrik kavramına denk gelse de temelde bir biyometrik sistemin, aynı zamanda ayırt edici özelliğinin de olması gerektiği ifade edilebilir. Buna göre biyometrik sistemleri, bireylerin biyolojik açıdan ayırt edici özelliklerini bir araya getirerek, güvenlik amaçlı kullanan sistemler olarak tanımlamak daha doğru olacaktır. Çalışmanın devam eden bölümünde, literatürde biyometrik sistemlerle ilgili yapılan tanımlar ve biyometrik sistemlerin yaygın olarak kullanılan türlerine yer verilmiştir.

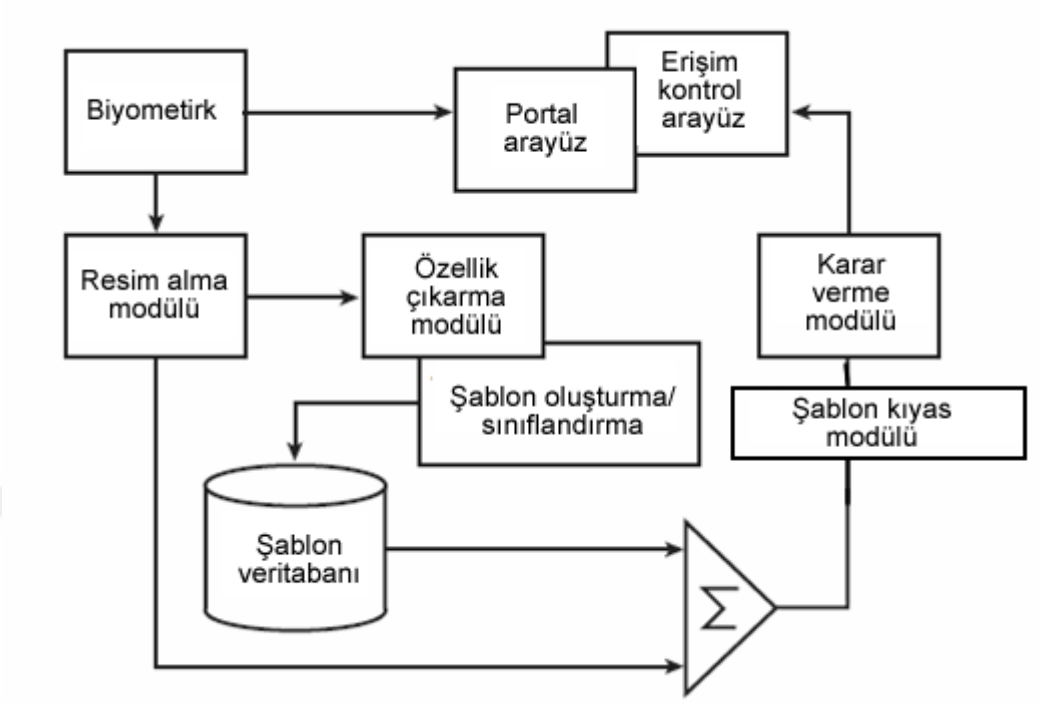
1.4.1. Biyometrik Sistemlerin Tanımı

Biyometrik ya da biyometri, literatürde "yaşam ölçümü" olarak geçmekte olup, parmak izi, göz retinası, iris, yüz hatları, el geometrisi ve vücut kokusu gibi fiziksel özellikleri analiz eden biyolojik verinin ölçülmesi, analiz edilmesi ve işlenerek dijital sunumunu içeren bir terimdir (Ajana, 2012:852).

Biyometrik sistemlerde, kimlik belirleme işlemi, kişilerin fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir. Diğer sistemlere göre çok daha az riske sahiptir (Eren, 2009:18).

Dhameja (2005) ise biyometrik kavramını, fiziksel data ve davranışsal karakteristikler sayesinde bireylerin tanınması süreci olarak tanımlamaktadır. Bu sistemler, genellikle belli bir karaktere bağlı olarak gerçekleştiğinden, en yaygın türünü standart-karakteristik biyometrik sistemler (UCBS-Uni-characteristic biometric systems) olarak nitelendirmek mümkündür. Bir UCBS bileşenlerini aşağıdaki gibi göstermek mümkündür (Dhameja, 2005:46-47).

Şekil 1.2: Bir UCBS'nin Alt Yapı Görünümü



Kaynak: Dhameja, (2005:47).

Şekilde de görüldüğü gibi, standart bir biyometrik sistemde, genel olarak bir veri tabanı bulunup, bu veri tabanındaki mevcut verilerin, alınan ya da sınanacak verilerle karşılaştırıldığı bir ara yüz bulunur. Bu ara yüz sayesinde, sınanacak olan kişiden alınan bilgiler, veri tabanına erişilerek oradaki verilerle kıyaslanmakta ve kıyaslama sonucu yeniden ara yüze verilmektedir. Bir biyometrik sistem temel olarak aşağıdaki bileşenlerden meydana gelmektedir (Dhameja, 2005:47):

i. Biyometrik sensor,
ii. Özellik çıkarma ve geçici dosya oluşturma modülü,
iii. Biyometrik karakteristik dosyası kayıt veri tabanı,
iv. Biyometrik şablon kıyaslama modülü,
v. Karar verme ya da çıktı modülü.

Bu aşamaları yerine getirirken, bir biyometrik sistemde temelde iki ana fonksiyon kullanılır: (1) bireyin teşhisi ve (2) tanınması. Her bir aşamadaki eylemleri özetlemek mümkündür (Dhameja, 2005:48). Bunlar;

Teşhis Aşaması:

1. Bireyin biyometrik karakterinin görüntüsünün alınması,
2. Özellik çıkarma modülüyle, kıyaslanacak olan özelliğin elde edilmesi,
3. Yerel bir sürücüye, elde edilen görüntünün daha sonra kıyaslanma amaçlı kaydedilmesi.

Tanıma Aşaması:

4. Bireyin biyometrik karakteristiğinin canlı imajının alınması,
5. Özellik çıkarma modülü ile kıyaslanacak biyometrik özelliğin işlenmesi,
6. Elde edilen görüntünün, 3. aşamada elde edilen veri tabanı ile karşılaştırılması,
7. Kıyaslama modülünden elde edilen sonuçların skorlanması,
8. Elde edilen sonuçların veri tabanına işlenmesi.

Biyometrik sistemler temelde, kişinin biyometrik özelliğinin elde ederek bu özelliği bir giriş verisi olarak kullanılırlar. Biyometrik sistemler elde edilen bu veriden anlamlı bölümün çıkarılması daha sonra bu anlamlı bölüm kullanılarak oluşturulan şablonun veritabanındaki diğer şablonlarla karşılaştırılması işlemlerini gerçekleştiren örüntü tanıma sistemleridir. Bu sistemler, elde edilen giriş verisini sayısal koda çevirirler ve söz konusu özelliğin bir örneğini elde ederek çalışmaktadırlar. Alınan örnek daha sonra, çeşitli matematiksel işlevler kullanılarak, özelliğin etkin ve yüksek derecede ayırt edici bir örneğini içeren biyometrik bir şablona dönüştürülmektedir. Biyometrik şablon, veritabanına daha önceden aynı yöntem kullanılarak oluşturulup depolanmış şablonlarla karşılaştırılmaktadır (Durmuş, 2010:1).

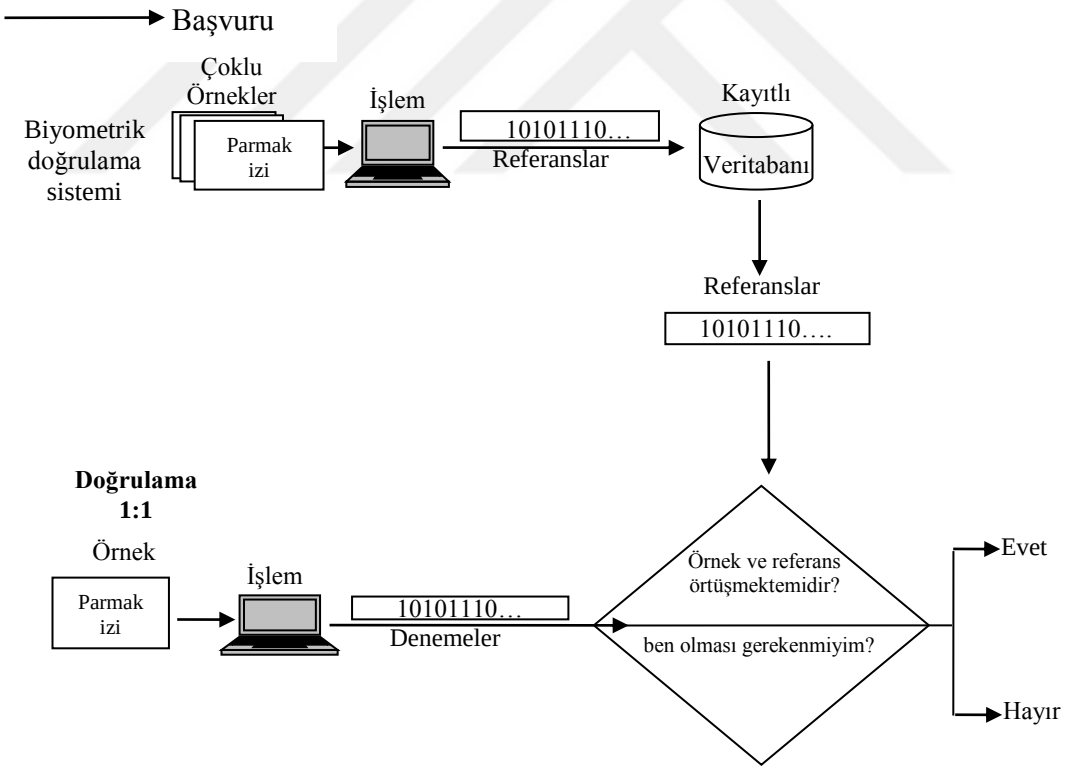
Biyometrik sistemler bir insan beyni gibi çalışmakta daha önceden gördüğü bir kişiyi tanıyıp ayırt etmektedir. Biyometrik sistemlerde tanıma amaçlı kullanılan ekipmanlar, her insanda farklı olan fiziksel özellikleri analiz ederek herhangi bir şifreye ihtiyaç duymadan veritabanı, bankalar ve bilgisayar sistemleri gibi ortamlara giriş için kimlik doğrulaması yaparlar (Koçer, 2007:16).

Biyometrik sistemlerde ayırt etme, doğrulama ve tanılama olarak iki yöntemle gerçekleşmektedir. Doğrulama modunda çalışan sistemlerde kullanıcı kendisine daha önceden sağlanmış bir kullanıcı adı veya ID numarası ile sisteme giriş yapar. Sistem, kullanıcının biyometrik verisiyle kayıtlı olan veriyi karşılaştırır,

akabinde biyometrik sistem doğrulanmış veya doğrulanmamış şeklinde bir cevap verir. Genellikle doğrulama sistemi tercih edilmektedir bunun nedeni ise kullanıcıdan elde edilen veri sadece kullanıcının talep ettiği kayıtlı biyometrik veriyle karşılaştırılmaktadır. (Ergen ve Çalışkan, 2011:456).

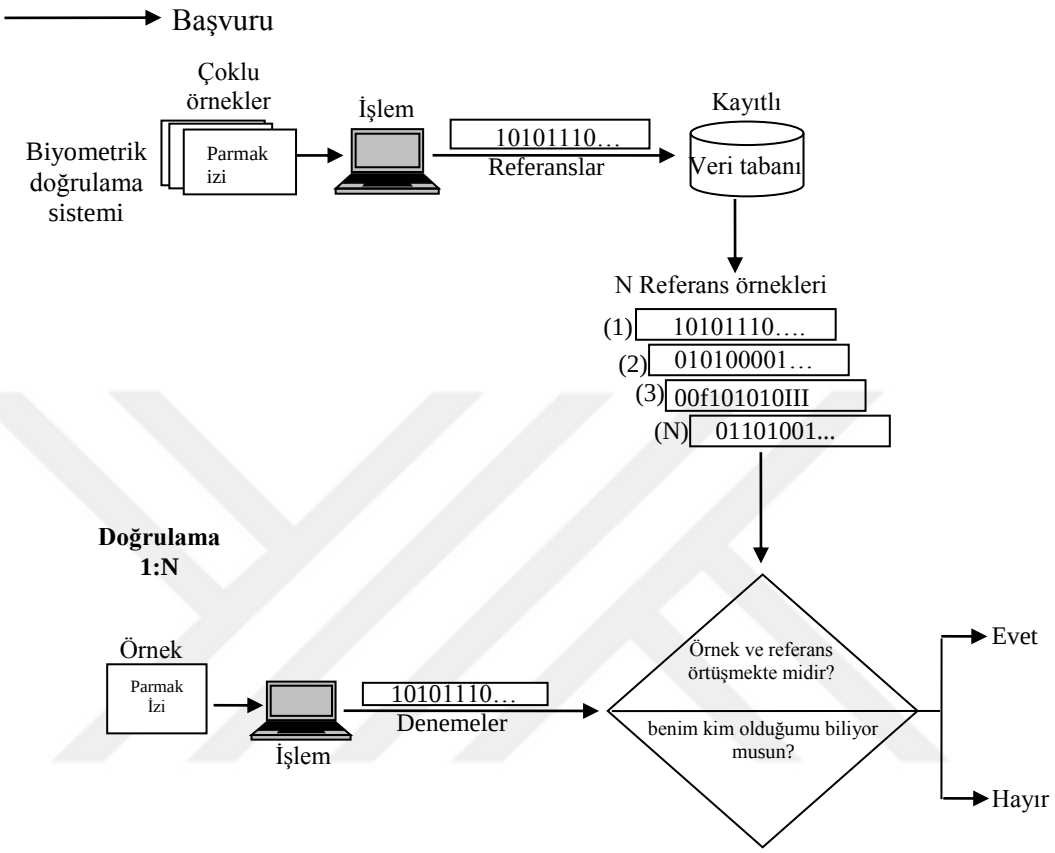
Tanıma modunda çalışan sistemlerde, kişinin kimlik belirtmesine gerek yoktur. Burada yeni elde edilen biyometrik veri ile veritabanındaki diğer bütün şablonlar arasında bire bir karşılaştırma yapılmak suretiyle kişi aranarak tanınmaktadır. Bu tür sistemler sadece "Bu biyometrik veri kimindir?" sorusuna yanıt arayacak şekilde çalışmaktadır (Durmuş, 2010:2).

Şekil 1.3: Doğrulama Modunda Çalışan Biyometrik Sistemlerdeki Süreç



Kaynak: Vacca, (2007:25).

Şekil 1.4 Devamı Tanıma Modunda Çalışan Biyometrik Sistemlerdeki Süreç



Kaynak: Vacca, (2007:26).

1.4.2. Biyometrik Sistem Türleri

Biyometrik sistem türleri, biyometrik ölçümün yapılacağı ya da diğer ifadeyle, değerlendirmeye konu olan biyometrik özelliğe göre değişmektedir. Fiziksel ve biyolojik karakterler sınırlı olmamakla birlikte (Dhameja, 2005:46), en yaygın kullanılan biyometrik sistem türleri aşağıdaki gibi özetlenebilir:

i. Parmak İzi Tanıma
ii. Yüz Tanıma
iii. El Geometrisi Tanıma
iv. İris Tanıma
v. Retina Tanıma

vi. Ses Tanıma

vii. DNA Tanıma

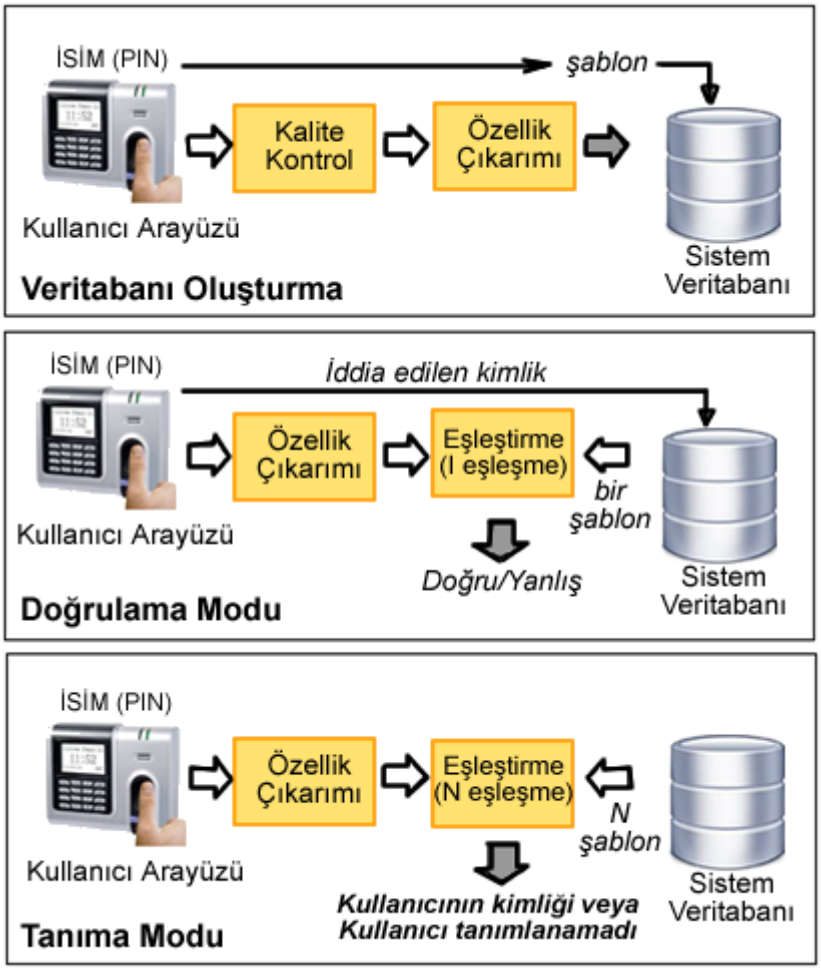
1.4.2.1. Parmak İzi Tanıma

İnsanlar ilk olarak parmak izlerini imza şeklinde kullanmıştı. Bugün ise adli soruşturmalarda, kaza hallerinde kimlik tespiti yaparken, endüstride erişim kontrol noktalarında güvenliği sağlama ve düzenli erişim için kullanılmaktadır. Bir insanın kendisini belirleyen pek çok biyometrik özelliği (DNA, retina, ses ve el geometrisi vb.) olmakla birlikte, parmak izi kişinin kimliğinin tespit edilmesinde ilk sırada kullanılmaktadır (Karakülah vd., 2004:13).

Biyometrik kimliklendirme tekniklerinden olan parmak izi tanıma 100 yılı aşkın bir süredir kullanılmaktadır. İlk otomatik parmak izi tanıma sistemleri (OPTS) 1980'lerin ortasında Amerika ve Avustralya'da tanıtılmış daha sonra çeşitli algoritmalarla geliştirilen bu sistemler dünyanın birçok yerinde kullanılmaya başlanmıştır. Bir OPTS'de parmak izi tanıma sisteminde parmak izinde bulunan özellik noktalarının çıkarılması ve bunlara ait parametrelerin karşılaştırılması temeline dayanmaktadır (Özkaya ve Sağıroğlu, 2012:3). Bu sistemlerin dezavantajları arasında, parmak izinin taklit edilmesi ve bazı kişilerin pek çok sebepten ötürü (organ eksikliği, yanma, deri hastalıkları) parmak izlerinin bulunmamasıdır (Eren, 2009:21).

Yapılan çalışmalara bakıldığında parmak izinin en yaygın olarak kullanılan ve güvenilir bir ayırt ediciliğe sahip olduğu görülmektedir. Parmak izi, biyometrik güvenlik sistemi türünde, bireylerin parmak izlerinin farklılığından yararlanılarak, kişilerin ayırt edilmesi sağlanmaktadır. Genel olarak biyometrik sistemlerin çalışma prensipleri benzer olup, standart bir parmak izi kontrol sisteminin çalışma prensibi, Şekil 1.5'deki gibidir.

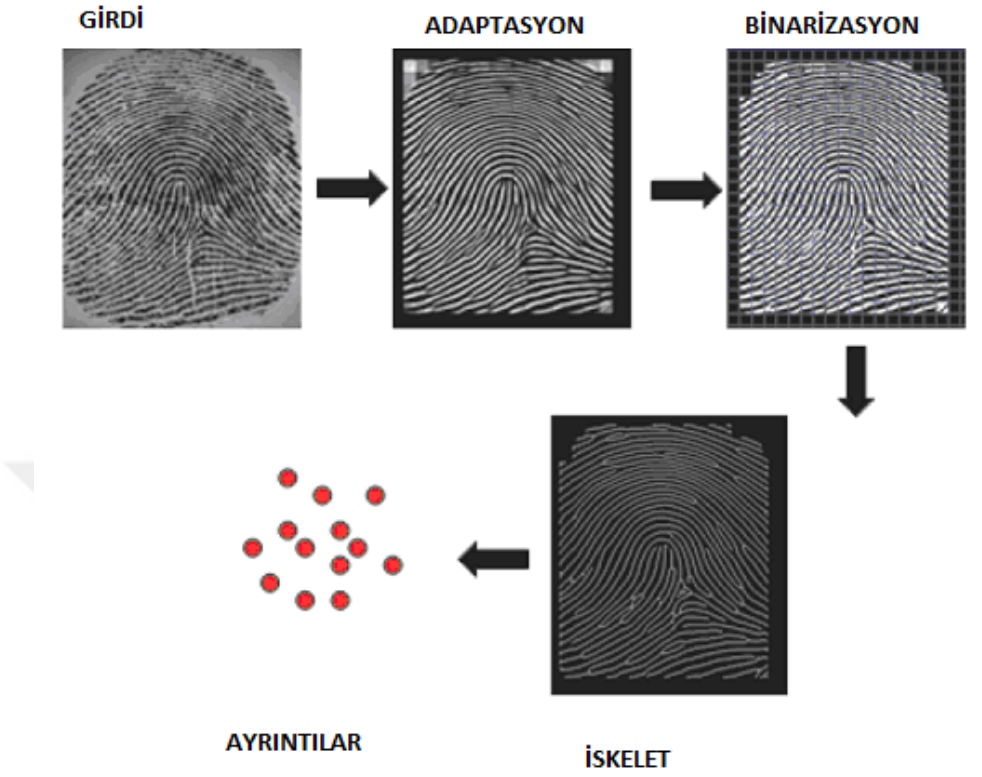
Şekil 1.5: Standart Bir Parmak İzi Tanımlama Süreci



Kaynak: Jain vd., (2004:5).

Şekil 1.5'de görüldüğü gibi sistem üç aşamadan oluşmaktadır. Bunlar veri tabanı oluşturma, doğrulama ve tanıma modudur. Veri tabanı oluşturmada, sistemi kullanacak olan kişilerin parmak izi bilgileri elde edilip, veri tabanına girilmektedir. Doğrulama modunda çalışan sistem, kullanıcı ara yüzü üzerinden gelen kişinin kimliğini veri tabanı bilgilerine göre kontrol etmektedir. Doğrulama modunda çalışan sistem ise kullanıcı ara yüzü üzerinden gelen şablonun doğruluğunu kontrol etmektedir. Günümüzde bazı parmak izi sistemlerinde, veri tabanında olmayan kişilerin de bilgileri veri tabanına eklenerek, dinamik bir yapıda veri tabanları yazılmaktadır. Bu şekildeki sistemlerde, gelen kişilerin bir anlamda kayıtlarının tutulması sağlanmaktadır. Bir parmak izi teşhis sisteminin analitik yapısı Şekil 1.6'daki gibidir.

Şekil 1.6: Parmak İzi Tanımlamada Verilerin Dijitalleştirilmesi



Kaynak: Kholmatov, (2008:21).

Şekilde de görüleceği gibi, parmak izi girişinin ardından alınan parmak izi resmi ön işleme teknikleri ile gürültüden arındırılıp filtrelenmekte, bilahare siyah tonlarında imaja çevrilmekte (grayscale), ardından piksellerine ayrılarak, bölge haritası çıkarılmaktadır (binarization). Daha sonra, parmak izinin iskeleti (skeletonizing), son aşamada ise parmak izine özgü set (minutiae set) çıkarılmakta ve veri tabanına işlenmektedir. Kıyaslama ve teşhis aşamasında bu son aşamada elde edilen set sonuçları kıyaslanmaktadır.

1.4.2.2. Yüz Tanıma

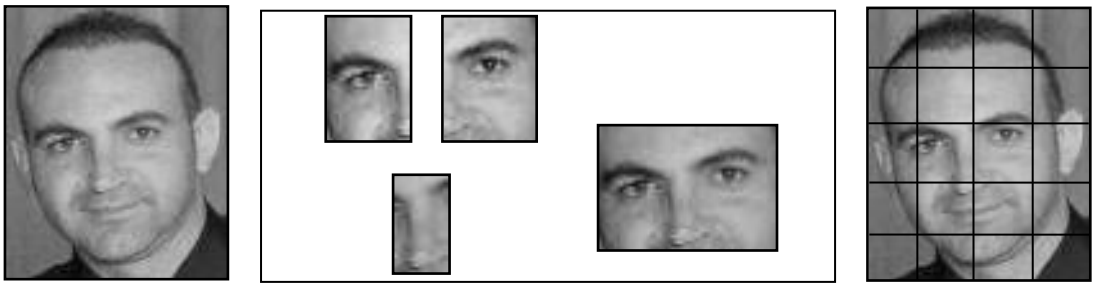
Yüz tanımlama sistemlerinin temeli mevcut yüz/yüzlerin görüntülerinden o yüzle ilgili karakteristik özelliklerin çıkartılmasına dayanmaktadır. Bu sistemler geliştirme aşamasında olup özellikle geometrik eşleştirme yöntemiyle çalışan sistemler bazı ATM makinelerinde deneme amaçlı kullanılmaktadır (Varlık, 2008:14).

Yüz tanıma sistemlerinde yüz bölgesinde bulunan gözler, kaşlar, burun, dudaklar, çene şekilleri ve bunlar arasındaki ilişkilere dayalı analizler yer almaktadır. Yüz tanıma sistemlerinde görüntü yakalama cihazı(kamera) ile herhangi bir fiziksel temas gerektirmemesi bu yöntemin bir avantajıdır (Gürbüz, 2014:20).

İnsanoğlunun yaradılışı gereği yüz bölgesinde yer alan tüm organların, kendi aralarında altın oran dediğimiz müthiş bir oran yer almaktadır, bu oran dışarıdan yapay bir müdahale olmadığı sürece değişmez. İnsan yüzündeki bu özellikler, değişik yöntemler uygulanarak belirlenir ve farklı eşleştirme yöntemleri ile yüz tanıma gerçekleştirilir (Filiz, 2012:1-2).

Yüz tanıma sistemleri, uygulamalarda sınırlı başarı sağlamışlardır. Ama çalışmalar halen devam etmektedir. Teknik zorluklar aşılabilirse, yüz tanımanın en iyi biyometrik sistem haline geldiğini görebiliriz. Bununla birlikte günlük hayatta pek kullanılabilir olarak değerlendirilmemektedirler. Sima, kulak memesi ya da birçok farklı parametreyi kullanan yüz tanıma sistemleri bulunmaktadır (Eren, 2009:24). Bir yüz tanıma sisteminde, yüzün farklı bölgeleri Şekil 1.7'teki gibi ele alınmaktadır.

Şekil 1.7: Yüz Tanıma Sistemlerinde Parça Yaklaşımı



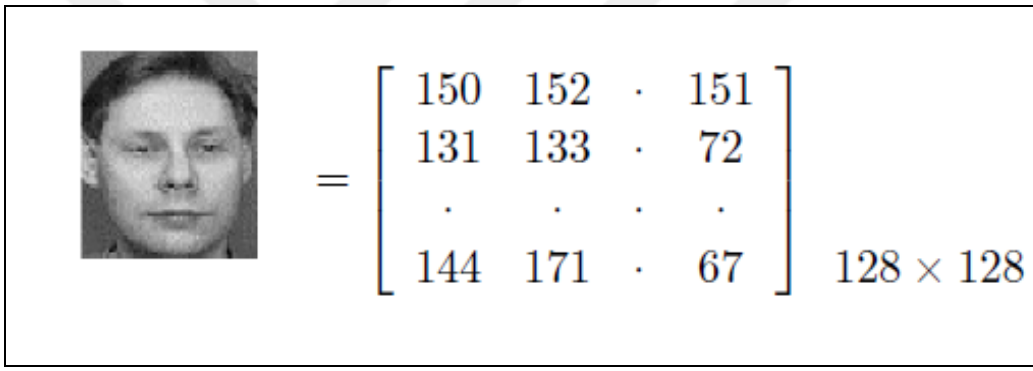
Kaynak: Arar, (2010:9).

Yüz tanıma sistemlerinde, parmak izi ya da diğer biyometrik sistemlerde olduğu gibi, ilk olarak imaj alınmakta ve veri tabanına kaydedilmekte daha sonra gelen kişinin imajı alınarak benzer dijital veriler türetilmekte, en sonunda ise türetilen dijital imaj ile veri tabanındaki imajların kıyaslaması yapılmaktadır.

Bir yüz tanıma sürecinde, ilk olarak resim yine siyah tonlu bir hale (grayscale) getirilmekte ve renk tonlarının 256 milyon renkten, iki tonlu (binary) renkli bir şekle gelmesi sağlanmaktadır. Daha sonra her bir bölge kendi içerisinde değerlendirilerek, resmin bilgisayar koduna uygun bir şekilde dijital veriye dönüştürülmesi gerçekleşmektedir.

Dijital veriye dönüştürme sürecinde, bilgisayar verilerinin matematiksel ya da nümerik veri olması nedeniyle imaj içerisindeki renk tonları sayısal değerlere karşılık gelecek şekilde sayılandırılmaktadır. Şekil 1.8'de, bu şekilde dönüştürülmüş bir imaj görülmektedir.

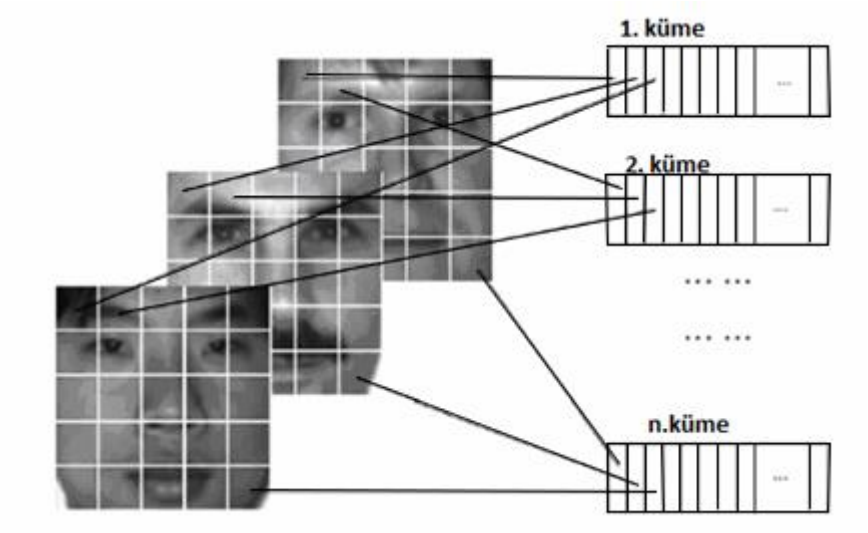
Şekil 1.8: Bilgisayar Verilerine(dijital) Dönüştürülmüş Bir İmaj Örneği



Kaynak: Tilki, (2014:8).

Burada, resmin bir matris oluşturduğu görülmektedir. Bilgisayar dilinde matrisler, tek boyutlu düzenden, iki boyutlu düzene geçişin göstergesidir. Bilgisayar programları sayesinde matrisin herhangi bir noktasını, (n x j) şeklinde koordinatlarını belirterek seçmek ve kıyaslamak mümkündür. Buna göre her bir veri tabanı nesnesi için bir girdi oluşturularak, Şekil 1.9'daki gibi veri tabanına depolanmaktadır.

Şekil 1.9: Yüz Farklı İmajlarla Oluşturulan Veri Seti



Kaynak: Tilki, (2014:8).

Veri seti oluşturulurken her bir imajın bütün bölgeleri yerine farklı bölgelerin veri setleri oluşturulmaktadır. Diğer bir ifadeyle bütün yüz verileri değil, sadece sağ kaş grubu, sol kaş grubu, burun bölgesi grubu gibi gruplar oluşturulmaktadır. Bu sayede kıyaslama yapılırken, her bir bölgenin ne derece örtüştüğü de ortaya konulmuş olmaktadır.

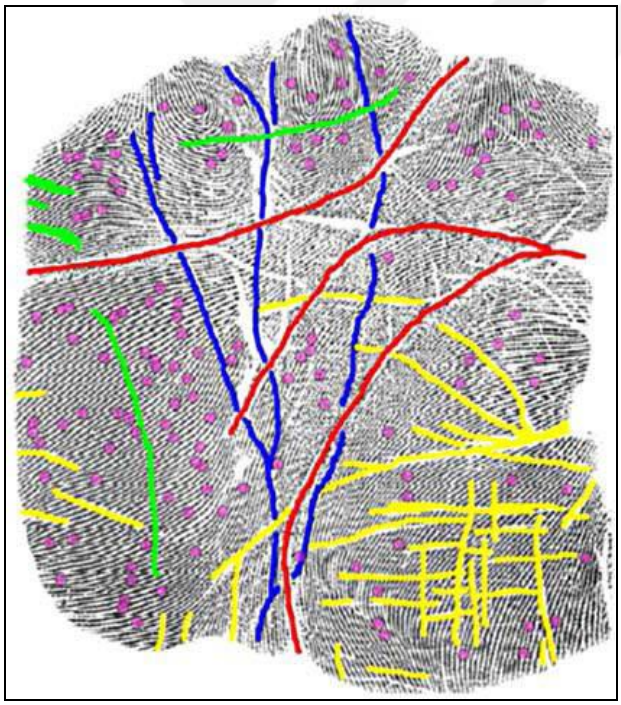
Yüz tanıma sisteminin dezavantajları arasında kullanıcının kilo alması ve taranan kısmın büyük olması bulunmaktadır. Taranan kısmın büyük olması işlem süresini uzatmakta bununla birlikte daha büyük depolanma alanlarına ihtiyaç duymaktadır. Bu da yüksek maliyeti beraberinde getirtmektedir. Teknolojinin gelişmesiyle küçük bir algoritma sistemi yazılarak yüzdeki belirli oranların ve referans noktalarının depolanması sağlanarak hem maliyet düşürülmüş hem de işlem süresi azaltılmıştır (Varol ve Cebe, 2011:3).

Kişilerin yüzündeki ufak mimik değişimlerinden bile sistem yanılabilmektedir. Ayrıca yüzdeki sakal ve tüyler, makyaj ve gözlük kullanımında hatalar oluşmakta ve bu sistemlerde hala geliştirilmesi gereken sorunlar olduğunu ortaya koymaktadır (Hıdımoğlu, 2010:10-11).

1.4.2.3. El Geometrisi Tanıma

Palmar(avuç içi) yüzeyinde görünen fleksiyon(bükülen) kırışıklıklar üç kategori altında toplanabilir. Bunlar: Majör fleksiyon, minör fleksiyon ve ikincil kırışıklıklardır. Major fleksiyon kırışıklıkları en geniş kırışıklıklar olmakla birlikte merkezden uzak çapraz şekilde kalp hattında, radyal çapraz şeklinde yaşam hattında ve proksimal çaprazlar biçiminde kafa hattında bulunurlar. Bu majör fleksiyon kırışıklıklar, iki avuç içi izini biyometrik tanımlamada referans olarak dizerken kullanılan yüksek derecede görünür geniş çizgilerdir. Küçük fleksiyon kırışıklıklar, ikincil kırışıklıklar ve önemsiz ayrıntı yerleri ile birlikte, adli ve sivil uygulamalar için avuç içi izi tanımlamada güvenilir özellikler olarak hizmet vermektedir (Jain ve Demirkus, 2008:4-5). Palmar yüzeydeki kırışıklıklar şekil 1.10'da gösterilmiştir.

Şekil 1.10: Elin Anatomisi



Kaynak: Kumar vd., (2009:32).

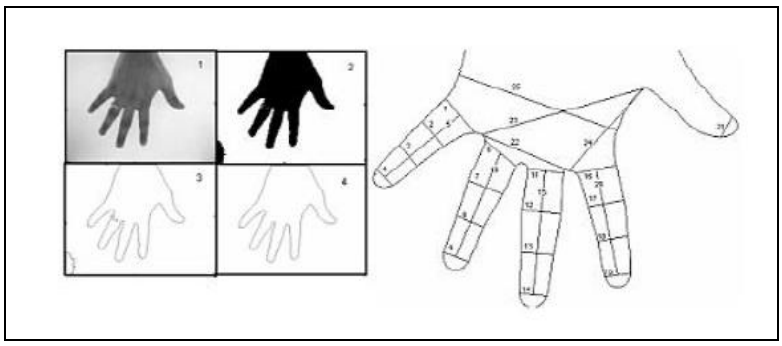
El geometrisi tanıma da diğer biyometrik sistemler gibi yüksek doğruluk oranına sahip bir sistem olmakla birlikte büyük ve ağır okuma cihazı nedeniyle maliyet ve kullanım açısından dezavantajlara sahiptir. Resmin alınma süresinin uzun olusu da sistemi yavaş yapan bir etmendir (Şamlı ve Yüksel, 2009:686).

El Geometrisi tanıma sistemi her insanda el şeklinin farklı olduğu ve değişmediği mantığından hareket ederek karşılaştırma yapan bir sistemdir. El, tarayıcıya yerleştirildiği zaman parmakların uzunluğu ile birlikte şekli, elin kalınlığı, kapladığı yüzey alanı gibi bilgiler analiz edilerek sonuca varılır. Bu analizler sonucunda 90 civarında değer elde edilir ve elde edilen bu değerler sayesinde kişiler birbirlerinden kolayca ayırt edilebilir. Ayrıca sistem sadece geometrik özelliklerle ilgilendiği için karşılaştırmayı etkileyen olumsuzluklardan olan yara ve kir gibi etmenler bu sistemde etkili değillerdir.(Varlık, 2008:14).

El, tıpkı göz irisi, parmak izi ve yüzdeki bazı hatlar gibi kişiye özel bir takım karakteristikler içermektedir. Esasen tüm bu biyometrik kıyaslama kıstaslarında benzer şablonlar görülse de bunların farklı kombinasyonları ve bu kombinasyonların bir araya geldiği farklı permutasyon değerleri nedeniyle biyometrik kıyaslayıcılar farklılık göstermektedir. Örneğin insan genomunu oluşturan DNA, beş karbonlu şeker içerip, sadece dört nükleotitten oluşmaktadır. Öte yandan bu dört nükleotitin dizilimi her insanda farklılık gösterdiğinden, DNA insanlar arasında seçici bir değer görmektedir. Yine el izinde de her insana özgü bir el geometrisi yoktur. Sadece benzer şablonların farklı geometride bir araya gelmesi söz konusudur.

Bu geometrik oran matematiksel olarak o kadar yüksektir ki her bir kişinin el geometrisi kendisine özgüdür. Bu nedenle el geometrisi, günümüzde kullanılan biyometrik sistemlerden birisidir. El geometrisi örnekleri Şekil 1.11'de gösterilmiştir.

Şekil 1.11: Farklı El Geometrisi Örnekleri

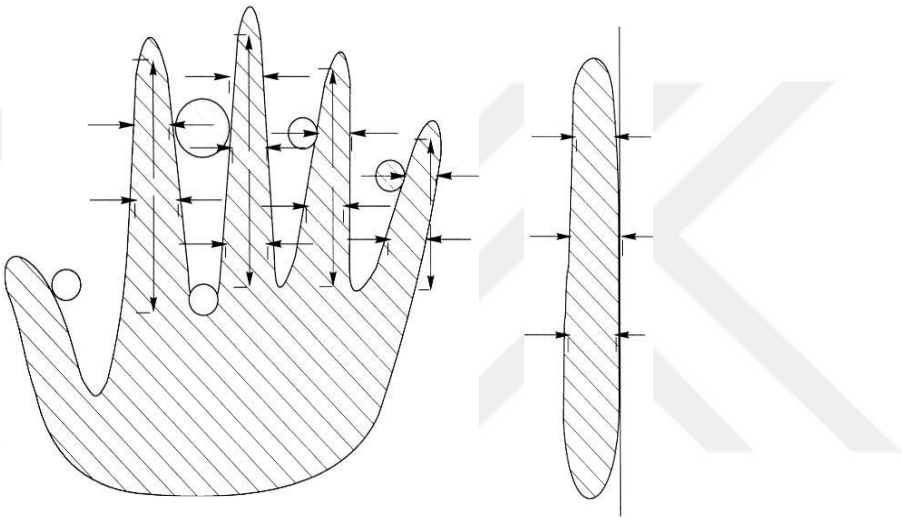


Kaynak: Doğan, (2011:11).

Şekilde de görüldüğü gibi el geometrisinde de yukarıda değinilen durum söz konusu olup, el içerisindeki farklı geometrik şablonların ne derece örtüştüğü ve bunun derecesi, eşleştirmenin sonucunu vermektedir.

Altta Şekil 1.12'de görüldüğü gibi parmak uzunluğu, genişliği, kalınlığı, elin kıvrımları ve fiziki özellikleri her insanı birbirinden ayırt etmeyi sağlar.

Şekil 1.12: Tipik El Geometrisi Ölçümleri



Kaynak: Zunkel, (2002:89).

El geometrisinin biyometrik sistemler içerisinde yaygın olarak kullanımı zor görünmektedir. Elin deforme olması, boyutundaki değişiklikler ve okuma cihazlarının entegrasyonundaki güçlükler bu sistemin yaygın kullanımına engel olan nedenlerdendir, bu sistem yerine parmak izi veya iris tanıma sistemlerinin tercih edilmesi daha makbul olacağı görüşü egemendir (Şahin, 2012:21).

Avuç içi tanıma biyometride yeni bir alan kabul edilmektedir. Farklı algoritmaların performansını karşılaştırabilmek ve değerlendirebilmek için ortak avuç içi veri tabanından faydalanmaya ihtiyaç duyulmakta ve bununla ilgili olarak bir problem meydana çıkmaktadır. Hong Kong Polytechnic üniversitesi avuç içi veritabanı en yaygın kullanılan veri tabanıdır (Ergen ve Çalışkan, 2011:458).

Avuç izi ve parmak izi tanıma eşleme yapmak için benzer algoritmalar kullanmaktadırlar. Her iki sistem de çizgilerde beliren etkilerin temsil ettiği

karakteristiklere, kişiye has bilgilere dayanır. İşlemedeki yetersizlikler ve canlı tarama teknolojilerindeki eksiklikler nedeniyle avuç izi tanıma algoritmaları, parmak izi tanıma algoritmalarıyla kıyaslandığı zaman daha yavaş çalıştıkları görülmektedir (Şahin, 2012:22).

1.4.2.4. İris Tanıma

İrisin, bebek embriyo olarak anne karnındayken oluşması ve insanın ölümüne kadar değişmemesi iris tanıma sistemlerinin güvenirliğinin ne kadar yüksek olduğunu göstermektedir (Koçer, 2007:27). İris, gözün içindeki dairesel renkli bölgedir ve yaşamı süresince değişmediği gerçeğinden yola çıkılarak İris tanıma sistemleri geliştirilmiştir (Gürbüz, 2014:20).

Üzerinde Çukurlar, kara noktalar, damarlar gibi fiziksel özellikleri içeren 400'den fazla ayırt edici karakteristik taşımaktadırlar ve bu karakteristikler her insanda farklıdırlar. Fiziksel özellikleri içeren bu karakteristikler, parmak izinden altı kat daha ayırt edici sayılmaktadır (Varlık, 2008:15). İris deseni o kadar bir ayırt edicidir ki aynı insan da bile iki gözün iris desenleri farklılık göstermektedir. Bu sistemde de diğer biyometrik sistemlerde olduğu gibi iris deseni sayısal hale dönüştürülüp veri tabanında saklanarak gerektiğinde karşılaştırma için kullanılmaktadır (Filiz, 2012:15).

Gözün daha az deforme olacak ve dış etkenlerden daha az zarar görecek bir yapıya sahip olması, iris tanıma sistemlerinin kullanılmasında temel faktörlerdendir. Diğer biyometrik sistemlere göre daha az etkilenmelerine rağmen uykusuzluk, gözyaşı ve diğer bazı hastalıklar iris tanıma sistemlerini etkilemektedir. Bu sistem gözü olmayan, gözleri görmeyen, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan kişilerde uygulanamaz. Söz konusu sistemler havaalanı gibi kimlik doğrulamanın çok önemli olduğu yerlerde yüksek bir doğruluk oranı ile uygulanmaktadır (Şamlı ve Yüksel, 2009:686). Güvenilirliği ve doğruluğu bayağı yüksek olan iris tanıma sistemleri kurulum ve bakım maliyeti yüksek olan biyometrik sistemler arasındadır.

Bu sistemde de diğer sistemlerde olduğu gibi kişinin kimliğini saptamak için öncelikle kişinin gözünün görüntüsü alınarak kullanılan algoritmalar sayesinde iris

bölgesinin şablonu oluşturulur. Daha sonra bu şablon, bir eşleşme bulunup kişinin kimliği saptanana veya eşleşme bulunamayıp kişi kimliği saptanmamış olarak tanımlanana kadar şablonların depolandığı bir veritabanıyla karşılaştırılır (Durmuş, 2010:8). Bir iris tanıma sisteminin genel algoritması Şekil 1.13'de gösterilmiştir.

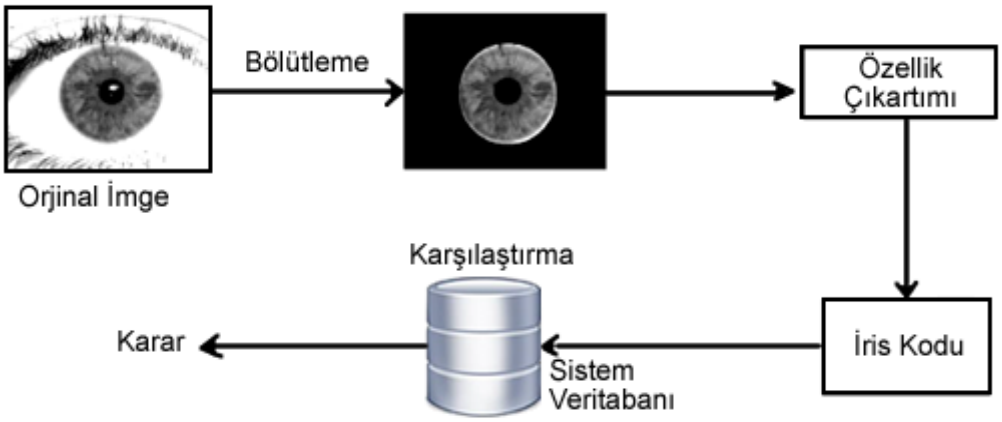
Şekil 1.13: (a) CASIA-V1 Veri Tabanından Bir imge Örneği (b) Bu İmgeye Karşılık Gelen Kenar Haritası (c) Yatay Değişimin Kenar haritası (d) Dikey Değişimin Kenar Haritası

Kaynak: Durmuş, (2010:15).

Şekil 1.13'de de görüldüğü gibi ilk olarak imge seçilmekte, ardından imgeye karşılık gelen kenar haritası çıkarılmaktadır. Daha sonrasında ise yatayda ve dikeyde değişim haritaları çıkarılarak, kıyaslama için dijital veri elde edilmektedir.

Üç aşamadan oluşan basit bir iris tanıma sistemi Şekil 1.14'de gösterilmektedir. İlk aşamada asıl imgeden iris bölgesi bölütlenir, ikinci kısımda bölütlenen imgeye algoritma uygulanarak özellik çıkartımı yapılır, son aşamada ise elde edilen özellik vektörü eldeki veritabanı ile kıyaslanarak bir sonuca varılır (Çelebi, 2008:26).

Şekil 1.14: Basit Bir İris Tanıma Sistemi



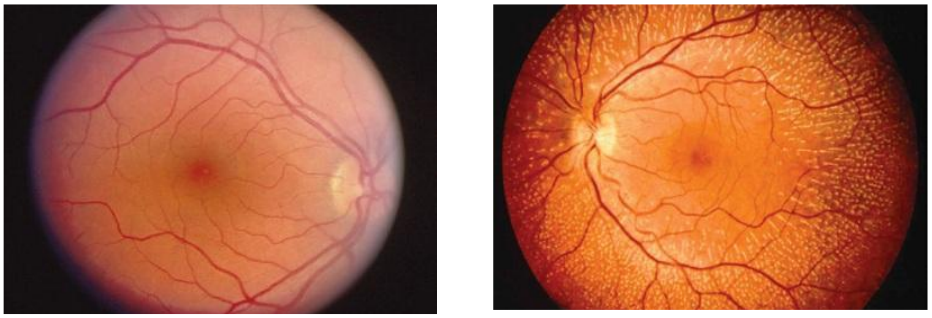
Kaynak: Çelebi, (2008:27).

1.4.2.5. Retina Tanıma

Retina tanıma her gözde kendine has olan optik yapıyı dikkate alarak geliştirilen sistemlerdir. Bu optik yapı taranırken kullanıcının belirli bir noktaya bakma mecburiyetinde kalması kullanımını oldukça güçleştirmektedir. Bu yüzden güvenlik seviyesi iyi durumda olmasına rağmen fazla yaygınlaşmamıştır (Filiz, 2012:17).

Retina tanımanın iris tanımadan farkı, iris tanımada gözün iris bölgesindeki yatay ve dikey alanlar kıyaslanırken, retina tanımada ise retina içerisindeki kılcal damarların topolojisi önemlidir. Bir retinanın kılcal damar haritası aşağıdaki gibi örneklendirilebilir.

Şekil 1.15: Retina Örnekleri



Kaynak: Doğan, (2011:12).

Retina damarları yapısal açıdan zengin ve her bireye ve her göze özgü bir karakteristik yapıdadır. Retinal damarı değişmek veya çoğaltmak kolay olmadığından dolayı bu yöntemin en güvenli biyometrik yöntem olduğu iddia edilmektedir. Retina taramaları, filmlerde ve askeri tesislerde kullanılmaktadır. Retina, biyometrik teknolojinin, 'En Yüksek Ve Pahalı Teknolojisi' olarak yüceltilmektedir. Önceden belirlenmiş retinal damar parçasının görüntülenebilmesi için bir kişinin bir göz parçacığını dikkatle gözetlemesi ve görsel alanda belirli bir noktaya odaklanması gerekmektedir. Görüntü elde etme işlemi, işbirliği, göz parçacığı ile temas ve kullanıcının bilinçli çabasını gerektirmektedir. Tüm bu faktörler retinal biyometriğin kamusal kabulünü olumsuz yönde etkilemektedir. Günümüzde bir dizi retina tarama-tabanlı kimlik doğrulama tesisi sıfır yanlış ile pozitif olarak işlem yapmaktadır. Retinal biyometriği olumsuz etkileyen bir diğer faktör de hipertansiyon gibi tıbbi durumlarda ortaya çıkar (jain vd., 2002:14).

Tarama yapılırken gözün bir müddet hareket ettirilememesi ve kırpılmamasından dolayı zahmetli olması, gözün bir lazer ile tarama yapılmasından ötürü gözlük veya lens gibi engellemeler sonucu sorun çıkmasına bağlı olarak çoğu kez tercih edilmeyen bir biyometrik tanımlama sistemidir (Varol ve Cebe, 2011:3).

1.4.2.6. Ses Tanıma

Konuşma organlarının aksamadan çalışması sonucunda ağızdan anlamlı bir şekilde sözcükler ve tümceler üretmek için çıkarılan birimlere ses denir. Ağız, burun ve boğaz boşluğundaki organlar aracılığıyla ciğerlerimizden çıkan hava bir takım sessel birimlere dönüşerek şekillenir (Yosuntaş, 2008:88). İnsan sesinin günlük hayatımızda ne kadar kullanıldığı göz önüne alındığı zaman, etkili bir yöntem olduğu düşünülse de seslerin kolay taklit edilebilir olması nedeniyle güvenlik zafiyetleri vardır (Filiz, 2012:17).

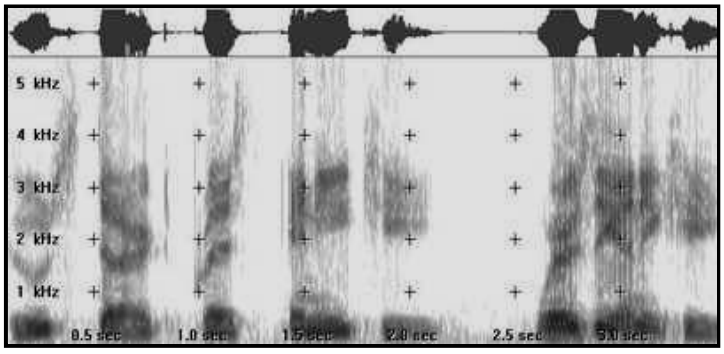
Sesin dijital bir veriye dönüştürülüp saklanması ve daha sonra veritabanında depolanmış olan diğer örneklerle karşılaştırılması mantığına dayanarak çalışan ses tanıma sistemlerini kullanacak kişiler öncelikle kullanacakları kelimeyi veya kelime grubunu birkaç defa sisteme tanıtmalıdırlar (Varlık, 2008:15).

Ses tanıma sistemlerinde kullanılan teknikte ses frekansları üç boyutlu görüntüleri oluşturmakta ve sesin en küçük birimleri, özel bir takım şekillere çevrilip karakterize edilmektedir. Bu sistemlerden bir takım ürünler piyasaya sürülse de yerel akustiğin değişebilir olması, telefon cihazlarının ve kullanıcı ortamlarının sabit olmaması nedeniyle güvenilir olarak görülmemektedirler (Karadaş, 2014:16). Ses tanıma sistemleri telefon üzerinden bir sisteme ulaşım için daha uygun bir yapıda görünüyor olsa da bu tür bir sistemde kişinin ses dalgaları telefonda iletilirken bozulmalara uğrayabilmektedir (Koçer, 2007:24).

Sesin hastalık veya psikolojik durumlarına bağlı olarak değişmesi, arka plandaki gürültülerle birlikte hem kayıt sırasında hem de sisteme giriş sırasında okunan metinde yanlış sözcük kullanılması gibi ses tanıma sistemlerini daha kullanışsız ve güvensiz hale getiren dezavantajlar bulunmaktadır (Hıdımoğlu, 2010:13-14).

İnsanların ağız yapılarına göre sesleri de farklılıklar göstermektedir. Ses karakteristiği ses spektrogramına göre belirlenmektedir. Farklı konuşma tonları grafikte farklı şekillerin oluşmasını sağlamaktadır (Şen, 2012:23). şekil 1.15'de örnek bir ses spektrogramı bulunmaktadır.

Şekil 1.16: Ses Spektrogramı



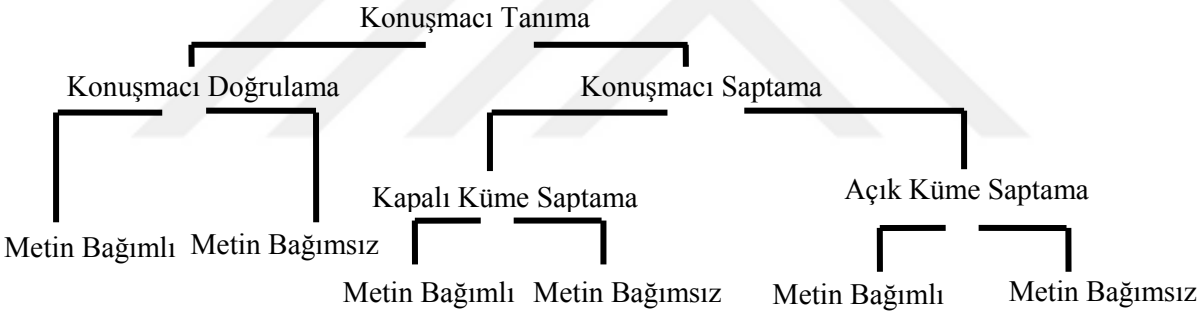
Kaynak: Şen, (2012:24)

Konuşmacı tanıma işlemi, konuşmacı doğrulama ve konuşmacı saptama olmak üzere iki ana şekilde gerçekleştirilir. Her iki yöntemde de konuşmacılara ait bir veritabanı bulunmakta analiz yapmak ve karar vermek için benzer teknikler kullanmaktadırlar. Konuşmacı belirlemede sistemde kayıtlı tüm konuşmacılarla

karşılaştırma yapılarak hangisinin konuştuğunun belirlenirken, konuşmacı doğrulama ise kim olduğunu iddia eden kişinin kabul veya reddedilmesidir (Hanilçi, 2007:1).

Metin bağımlı ve bağımsız olarak ele alınırken, Metnin bağımlı olduğu sistemlerde konuşulan metin, sistem tarafından önceden kayıt altına alınmıştır. Metinden bağımsız sistemlerde ise metin rastgele bir sözdizimi olabilmektedir. Bununla birlikte konuşmacı tanıma, açık küme ya da kapalı küme olabilir. Kapalı kümede eşleştirilmek istenen ses örneği, veritabanındaki konuşmacılardan birisine aittir. Açık kümede ise ses örneği veritabanındaki konuşmacılardan birine ait olduğu gibi olmayabilir de, bu yüzden açık küme konuşmacı tanıma sistemlerinde, ret sonucunu da içeren fazladan bir olasılık daha bulunmaktadır halbuki bu durum kapalı küme sisteminde söz konusu değildir (Karasartova, 2011:4-5).

Şekil 1.17: Konuşmacı Tanıma Sınıflandırma



Kaynak: Rençber, (2011:2).

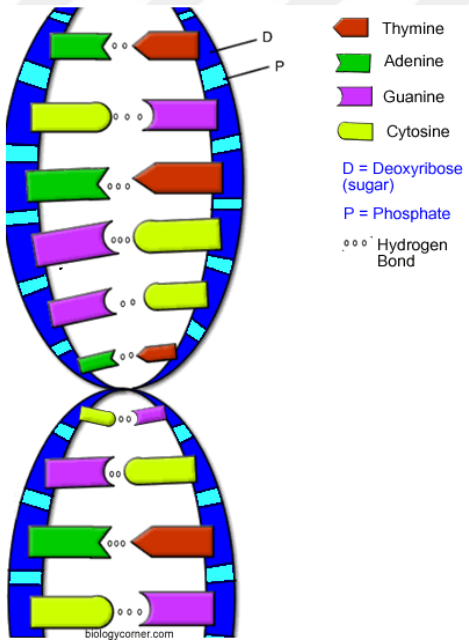
1.4.2.7. DNA Tanıma

Deoksiribonükleik asit (DNA) biyometriği herhangi bir bireyi tanımlamanın en kesin yöntemidir. Her insan her bir hücresinde kişisel bir harita vardır. Blueprint olarak bilinen bu harita her vücut hücresinde bulunabilmektedir. Doğruluğu çok yüksek bir yöntemdir. Genellikle Emniyet güçleri tarafından olay yeri inceleme sonucunda olay yerinde bulunan biyolojik materyallerin incelenmesiyle suçluların bulunmasında kullanılır. Bununla birlikte hukuki olaylarda babalık davalarında kullanılmaktadır (Gürbüz, 2014:22).

Kişinin saç, tırnak, deri parçası, kan, sperm veya herhangi diğer bir biyolojik materyali ele alınarak hücre içerisinde bulunan DNA moleküllerindeki dizilim incelenir. DNA'nın elde edileceği biyolojik dokunun kirlenmesi gibi durumlarda örnek kalitesi düşeceğinden analiz yapmak zorlaşır (Şamlı ve Yüksel, 2009:686).

DNA yapısının elde edilmesi oldukça güç ve günler, hatta haftalar alan uzun süren bir süreçken aynı zamanda oldukça maliyetli ve karmaşık bir uygulamadır. Hiç kimse biyometrik bir sisteme giriş için kendi DNA yapısını vermek istemez. Bunlar, DNA yapısının biyometrik tanıma amacıyla kullanılmasına engel teşkil eden nedenlerdendir (Koçer, 2007:26). Bir DNA dizilimi aşağıdaki gibidir;

Şekil 1.18: Bir DNA Dizilimi Ve Nükleotitler



Kaynak: http://www.biologycorner.com/bio1/DNA.html

Bir DNA diziliminde, toplam Adenozin, Guanin, Sitozin ve Timin olmak üzere dört nükleotit olmasına rağmen, bu dizilim sarmal yapıda olup, her insanda farklıdır. Saç, kıl, tüy, tükrük gibi birçok kriminal kanıtta, DNA %99,99 tutarlılıkta sonuç vermektedir.

1.5. BİYOMETRİK SİSTEMLERİN GEREKLİLİĞİ

Yetkili kişilerin erişebildiği alanlarda bu erişiminin denetlenmesi, hukuksal alanda suçla ilgili, diğer bazı gizlilik gerektiren ve gerektirmeyen alanlarda kimliklendirmeye ihtiyaç duyulması, insanlık tarihiyle birlikte ortaya çıkmıştır (Karakülah vd., 2004:14). Günümüzde ise kişiyi, kendisine özgü bir özelliğini kullanarak tanımaya dayanan ve biyometri olarak bilinen bir bilim dalı gelişmiştir. Biyometrik tanımanın temel avantajı, bir kart ya da şifre kullanmak yerine, giriş izni isteyen kişinin kendisini fiziksel olarak sisteme tanıtmak zorunda olmasıdır (Durmuş, 2010:1). Biyometrik sistemlerde kullanılan fiziksel özelliklerin unutulması, kaybedilmesi, çalınması gibi kötü durumların olmaması sistemin güvenliği için çok önemli bir avantajdır. Bununla beraber biyometrik sistemlerde kullanılan tanımlama özellikleri kişiye özel ve tektir (Varlık, 2008:10).

Biyometrik sistemler kişinin her insanda farklı olan fiziksel veya davranış özelliklerini kullanarak, alınan bilgilerin bilgisayar teknolojileriyle kimliğin tespit edilmesi yoludur. Fiziksel özellikler genelde hep aynı kalırlar ve değişmezler. Bireysel kimliklendirme için fiziksel özelliklerden yararlanan sistemler arasında DNA, yüz izi, dişlerin yapısı, retina, iris, el geometrisi, el damarları, parmak izi bulunmaktadır. Davranış özellikleri ise ortama ve ruhsal duruma göre değişmektedir. Bu özelliklerinden yararlanan sistemler arasında ses, imza ve konuşma bulunmaktadır (Karakülah vd., 2004:14).

Biyometrik sistemlerin en önemli özelliği, kişilerin biyolojik özelliklerini saklayamamaları nedeniyle, kişilerin teşhisi ve güvenlik sistemlerinin sağlanmasında tarafsız veriler türetmesi ve güvenilir sonuçlar vermesidir. Bu sistemler güvenlik denetimi amaçlı olarak birçok kurum ya da kuruluşta kullanılabilmektedir.

Uluslararası Biyometrik Grup raporuna göre 2004 yılında toplam biyometrik gelir 1440.6 milyon dolarken, 2005 yılında 1905.4 milyon dolara yükselmiştir (Dhameja, 2005:47). Kişilerin kendilerine özgü fizyolojik özelliklerini kullanarak otomatik kimliklendirme yapan biyometrik sistemler, güvenliğin her gün daha da iyi olması gereken modern dünyada gelişen teknolojinin sayesinde geniş kullanım alanları bulmaktadır. Bu sistemler aşağıdaki gibi birçok sistemde kullanılmaktadır (Karadaş, 2014:14-15):

- Yüksek güvenlik bölgelerine erişim kontrolü,
- Binalara, tesislere ve ofislere erişim güvenliği,
- Ulusal kimlik uygulamaları, sürücü ehliyeti ve pasaportlarda kimlik tespiti,
- Bilgisayar güvenliği,
- Kurumsal ağ güvenliği,
- Personel devam ve takip uygulamaları,
- Hastanelerde yeni doğan ünitelerine erişim kontrolü,
- Okullarda öğrenci devam, takip ve erişim kontrol, veli kontrolü,
- Elektronik ödeme, loyalty işlemleri,
- Kredi kartı güvenliği,
- Banka ATM'lerinde kullanıcı tanımlama,
- Kiralık kasalara erişim güvenliği,
- Satış noktası terminallerinde (POS) kullanıcı tanımlama,
- İnternet bankacılığında kullanıcı tanımlama,
- Çağrı merkezlerinde kimlik tespiti,
- Havalimanlarında check-in ve boarding işlemleri,
- Gemi ve Liman güvenliği,
- Sınır kontrolü ve sınır kapılarından girişlerin kontrolü,
- Kurumsal ağ, kişisel bilgisayar ve taşınabilir bilgisayar güvenliği, SSO,
- Çek onaylama işlemlerinde kullanıcı güvenliği,
- Maçlarda kombine bilet uygulamaları,
- Elektronik bilet satışı,
- Hastane ve sigorta kuruluşlarında hasta takibi ve kimlik saptama,
- Kamu hizmetlerine yönelik kayıt takibi (SSK, vergi, trafik),
- CRM uygulamaları (Customer Relationship Management) Müşteri İlişkileri Yönetimi,
- Kiosk'larda kullanıcı tanımlama,
- Ulusal yargı ağı (UYAP) güvenliği,
- E-ticaret işlemlerinde.

Uçak bileti, otel odası, araç kiralama gibi çeşitli turizm hizmetlerinde ve giriş kontrol sistemlerinde kullanılabilecek biyometrik işlevleri olan bir akıllı kart tasarlanması önerisi biyometri endüstrisinde en çok tartışılan konulardan birisidir.

Teknik olarak bu fikrin icra edilmesi mümkün olmasına rağmen, politik ve ticari açıdan bakıldığında çözülmesi gereken birçok sorun ortaya çıkarmaktadır. Bu kartlara kimlerin sahip olacağı sorusu bir yana, bu uygulamanın kimler tarafından ve nasıl yönetileceği de önem arz etmektedir. Uzmanlar, bu alanda kullanılacak biyometrik akıllı kartların bir pilot uygulamasının yapılarak kullanıcılara cazip gösterilmesini önermektedirler. Biyometrik sistemlerin ve akıllı kart teknolojisinin birleştirilmesi ile oluşan biyometrik tanımlama ve doğrulama sistemleri hem kullanıcıları hem de devletin güvenlik ihtiyacını karşılar durumdadır (Uzun, 2006:52).

1.6. BİYOMETRİK SİSTEMLERİN SAKINCALARI

Biyometrik sistemlerin sakıncaları, sistemin kendisinden ya da kullandığı yöntemden ziyade, kullanılma şekli ile yakından ilişkilidir. Dixon (2008) kütüphanelerde biyometrik sistemlerin kullanımını incelediği çalışmasında, bu sistemlerin kütüphanelerde erişim ve yetki amaçlı kullanımının kamu yararı sağladığını ifade ederken, başka amaçlarla kullanımın ya da kütüphane içerisindeki diğer aktivitelerin gözlemlenmesi amacıyla kullanımının özel hayatın gizliliği ya da kişisel özel mülkiyeti ihlal edeceğini rapor etmiştir (Dixon, 2008:141).

Bir başka çalışmada, Freeman (2003) biyometrik sistemler ile kanıt ve kişisel gizliliği incelemiştir. Bu çalışmada yer verilen pek çok uzman görüşünün, aslında bu sistemlerin güvenilirliğinin yüksek olduğu ancak oluşturulan veri tabanlarının bir anlamda fişleme ifade edebileceği, kişisel verilerin korunması ve özel hayatın gizliliği gibi konularda biyometrik sistemlerin sakıncalar içerebileceğine işaret etmiştir (Freeman, 2003:4-7).

Holden ve Millet (2005), ABD'de federal ajanslarda kullanılan biyometrik sistemlerde erişim, güvenlik, otorizasyon ve gizlilik konuları arasında önemli bir ilişki olduğunu ve bu gizliliğin korunması için gerekli önlemlerin alınması gerektiğini bildirmiştir.

Biyometrik şablon koruma yöntemleri, bir yandan güvenliği arttırmak için güvenilir öznitelikler ve eşleştirme/karşılaştırma algoritmaları yaratmaya çalışırken diğer taraftan ise biyometrikleri gizleyerek mahremiyeti sağlamaya çalışır. Biyolojik veri olan biyometriklerin mahriemiyeti oldukça önemlidir. Yemek yemeyi çok seven birinin şişmanlamayı göze almıştır, sağlam bir yuvaya sahip olmayı hedefleyen bir kuşun çok fazla enerji tüketmek zorunda kalması gibi veya büyüyüp daha fazla kazanmayı hedefleyen bir şirketin yönetimde zaaflar yaşaması gibi ödünleşim, mahremiyet ve güvenlik arasında da görülmektedir. Biyometrik şablon korumada güvenliği arttıran özniteliklerin temel amacı kişiyi en iyi şekilde tanımlayacak vektörler üretmektir. Biyometrik olmayan sistemlerde çalınan bir şifreyi değiştirmek mümkünken biyometrik şablonların bir şekilde başka birinin eline geçmesi aslında teorik anlamda hiçbir zaman değişmeyecek biyolojik bir bilginin kaybolması demektir. Bu mahrem bilginin gizliliğini sağlamak için çeşitli kriptografik kıyım fonksiyonları ve biyometrik anahtarlar kullanılabilinir. Ancak kullanılan bu yöntemler genelde salt biyometriklerin sunduğu ayırt ediciliği azaltmakta ve tanıma başarımını düşürerek güvenlik risklerine yol açabilmektedir (Kanak, 2013:3).

1.7. BİYOMETRİK SİSTEMLERİN KIYASLANMASI

Biyometrik sistemler dışındaki sistemler, kullanıcıya bazı bilgileri bilme ve hatırında tutma bununla birlikte kullanılan araçları sürekli olarak yanında taşıma, çaldırmama, unutmama gibi sorumluluklar vermektedir.

Biyometrik sistemlerde, kimlik belirleme işlemi, kişilerin fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir. Diğer yöntemlere göre çok daha az riske sahiptir (Eren, 2009:18). Kısacası biyometrik sistemlerde kişinin kimliğini doğrulayabilmesi için kendisinden başka herhangi bir bilgiye, nesneye vs ihtiyacı yoktur.

Her biyometrik sistemin kendi artıları ve eksileri vardır. Üzerinde çok fazla araştırma yapılmış olmasına ve bazı olumsuz yanlarının üstesinden gelinebilse bile bir yöntemin kendi doğasında eksiklikleri olabilir.

Jain ve ark'a göre biyometrik sistemlerin karşılaştırılmasında aşağıdaki yedi faktör dikkate alınmıştır.

- Evrensellik: Uygulamaya ulaşan her bir birey o özelliği sahiplenmelidir.
- Teklik: Verilen özellik nüfusun üyeleri arasında yeteri kadar farklı olmalıdır.
- Kalıcılık: Bir bireyin biyometrik özelliği, belirli bir eşleme algoritması ile ilgili olarak zaman içinde yeterince değişmeyen olmalıdır. Önemli ölçüde değişen bir özellik kullanışlı bir biyometrik değildir.
- Ölçülebilirlik: Bireysel rahatsızlık yaratmadan, uygun cihazlar kullanılarak biyometrik özelliği kazanmak ve dijitalize etmek mümkün olmalıdır. Ayrıca, edinilen ham veri temsili özelliklerini çıkarmak için işleme mükellef olmalıdır.
- Performans: Tanıma doğruluğu ve hassasiyeti elde etmek için gerekli olan kaynaklar, uygulamanın ihtiyaçlarını karşılamalıdır.
- Kabul Edilebilirlik: Uygulamayı kullanacak hedef nüfustaki bireyler sisteme kendi biyometrik özelliklerini sunmak için istekli olmalıdır.
- Tuzağa Düşürme: Bir biyometrik özelliğin yapay doku kullanılarak taklit edilebilme kolaylığı- davranışsal özellikler durumunda fiziksel özellikleri ve taklit durumunda sahte parmaklar kullanarak- o uygulamanın güvenlik ihtiyaçlarına uygun olmalıdır.(Whither Biometrics Comittee, 2010:34-35)

Esasen her birinin görevi aynı olsa da, temelde küçük farklılıklar gösteren biyometrik sistemlerin, birbirlerine göre üstün ya da düşük özellikleri vardır. Biyometrik sistemlerin kullanım alanlarına göre özelliklerinin kıyaslanması Tablo 1.1'de verilmiştir.

Tablo 1.1: Yaygın Kullanılan Biyometrik Sistemlerin Kıyaslanması

Biyometrik Karakteristik	**Evrensellik**	**Eşsizlik**	**Süreklilik**	**Elde Edilebilirlik**	**Pcrfonnans**	**Kabul Edilebilirlik**	**Yaygınlık**
DNA	Y	Y	Y	D	Y	D	D
Kulak	O	O	Y	O	O	Y	O
Yüz	Y	D	O	Y	D	Y	Y
Yüz Termogramı	Y	Y	D	Y	O	Y	D
Parmak izi	O	Y	Y	O	Y	O	O
El Geometrisi	O	O	O	Y	O	O	O
Îris	Y	Y	Y	O	Y	D	D
Retina	Y	Y	O	D	Y	D	D
Imza	D	D	D	Y	D	Y	Y
Ses	O	D	D	O	D	Y	Y
Y:Yüksek O: Orta D:Düşük							

Kaynak: Ergen ve Çalışkan, (2011:456).

Tablodan da görüleceği gibi, imza ve ses gibi dış ortamlardan daha fazla etkilenen ya da daha fazla müdahale edilebilen sistemler dışında şu yöntem şu yöntemden daha üstündür gibi bir genelleme yapmak mümkün değildir. Burada önemli olan nokta, ihtiyacın ne olduğunun belirlenmesi ve uygun yönteme buna göre karar verilmesidir. Örneğin hem yaygınlık, hem de elde edilebilirlik önemli olduğunda, yüz tanıma sistemleri, imza ve sese göre daha etkilidir. Ancak yaygın ve kabul edilebilirliği yüksek bir yöntem istendiğinde, daha güvenilir olmasına rağmen, DNA yöntemi ses ve imzadan daha az cazip hale gelebilir. Sesle ya da retinayla elde edilen güvenlik sistemi, bir DNA sistemi kadar kesinliğe sahip değildir. Ancak bir kamu kurumuna girişte, ya da ortak kullanım alanlarında, DNA sistemi hem erişilebilir değildir, hem de uygulanabilirliği yok denilecek kadar sınırlıdır. Sistem özelliklerine göre ise biyometrik sistemleri Tablo 1.2'deki gibi kıyaslamak mümkündür.

Tablo 1.2: Biyometrik Sistemlerin İşlevselliklerine Göre Kıyaslanması

Biyometrik Tür	Doğrulama	Tanıma	Yanlış kabul	Yanlış ret	Kişiye Etkisi	Masrafı
Yüz	Evet	Hayır	Zor	Kolay	Çok düşük	Düşük
Parmak izi	Evet	Evet	Çok zor	Çok zor	Orta	Düşük
El geometrisi	Evet	Hayır	Çok zor	Orta	Düşük	Orta
İris	Evet	Evet	Çok zor	Çok zor	Orta	Yüksek
Retina	Evet	Evet	Çok zor	Çok zor	Yüksek	Yüksek
Ses	Bazen	Hayır	Orta	Kolay	Çok düşük	Düşük
İmza	Bazen	Hayır	Orta	Kolay	Düşük	Orta

Kaynak: Şen, (2012:16).

Tablo 1.2'de benzer bir durum söz konusudur. Bir yöntem bir amaç için çok uygunken, diğeri için çok uygun olmayabilir. Örneğin yanlışı kabul oranının çok zor olmasının istendiği bir güvenlik sisteminde, ses ya da imza sistemleri kullanışlı değildir.

1.8. KAMUDA BİYOMETRİK SİSTEMLER

Kamu kurumları, hitap ettikleri kesimin büyüklüğü ve aynı zamanda tüm kamuya mal olan bir hizmeti verdiği için, bu alanlarda güvenlik oldukça önemlidir. Kamu kurumlarında güvenliğin genel olarak iki aşamada gerçekleştiği ifade edilebilir. Birincisi, bu kurumlara giren kişilerin önceden seçimi ile ilgilidir. Örneğin bir askeri tesise, bu alana sadece girme yetkisi olanların girebildiği durumlarda (Gough, 2008), biyometrik sistemler otorizasyon ve tanımlama açısından önemlidir. Bir diğer yaklaşım ise suç unsurunun yüksek olduğu adliye gibi kriminal vaka alanlarında, suç işlenmesi durumunda gelen kişilerin kimliklerinin belirlenmesinde önem arz eder. İkincisi, daha az kullanıma sahip olsa da ulusal düzeyde güvenlik gerektiren durumlarda, bu güvenlik unsurundan da söz etmek mümkündür. Ancak biyometrik sistemler daha çok kimlik doğrulama ve otorizasyon alanlarında kullanılmaktadır (Akram vd., 2012:169-170).

Bilgi güvenliği için kullanılan kimlik doğrulama işlemi genel olarak bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç farklı şekilde incelenebilir Herhangi bir bilginin gizliliğinden buna bağlı olarak da güvenliğinden bahsedebilmek için kimlik doğrulama kavramı oldukça önemlidir. Bilgi,

gönderilmek istenen kişiye veya kuruma değil de başka kişi veya kuruma gönderilirse istenmeyen sonuçlar ortaya çıkar. Yanlış ellere gönderilen bu bilgi tıp ya da askerîye gibi kritik alanlarda daha fazla kaybın yaşanmasına neden olabilir (Şamlı ve Yüksel, 2009:684).

Kamuda biyometrik sistemlerin çeşitli kullanım alanları vardır. Dixon (2008) çalışmasında, kütüphanelerde yetki ve erişim sistemlerinde biyometrik sistemlerin kullanımını incelemiştir. Yazar çalışmada bu sistemin kamu kurumlarında yüksek güvenilirliğe sahip olduğunu ve bu sayede bu kurumlarda yüksek güvenilirliğin sağlanabildiğini rapor etmiştir (Dixon, 2008:141).

1.9. KARTLI SİSTEMLER-AKILLI KARTLAR

Kartlı Sistemler, giriş kontrolü yapılmak istenen birimin, personel-ziyaretçi giriş, kontrol ve denetiminin yapılmasını sağlamakta olup, personel devam kontrol sistemleri ile uyumlu olacak şekilde çeşitli fabrikalar, hastaneler, okullar gibi pek çok bina giriş sistemlerinde kullanım alanına sahiptir. Kartlı sistemlerde ana öğe kart olup, mifare kart, yakınlık kartı, plastik kart gibi kartlar geliştirilmiştir. Bunlardan en yaygın olanları olan mifare kartlar, içinde yazılım yüklü olan elektronik çipli kartlardır. Tüm donanım, mifare kartın içine gömülü olarak yerleştirildiğinden diğer manyetik araçlardan ya da su dökülmesi veya güneşe maruz kalma gibi koşullardan etkilenmemektedir. Mifare karttaki bilgiler çalınamamakta ve kopyalanamamaktadır. Dolayısıyla bilgilerin bozulması da mümkün değildir ve güvenlik yüksek düzeyde sağlanmaktadır (Akınlar, 2012:49).

Şekil 1.19: Öncelikli(Proximity) Kart Ve Kartlı Sistem Örneği

Kaynak: Akınlar, (2012:49).

Akıllı kartların güvenlik uygulamalarında kullanılması eski tarihlere dayanmakta olup, özellikle Java Card (Chen, 2000) gibi kullanımı daha da kolay akıllı kart uygulama geliştirme ortamlarının ve yazılım çerçevelerinin ortaya çıkması sonucunda bu uygulamalarda akıllı kartların kullanılması giderek yaygınlaşmaktadır (Kardaş vd., 2008:32).

İKİNCİ BÖLÜM
KAMUDA GÜVENLİK AMAÇLI KULLANILAN BİYOMETRİK SİSTEMLERİN KARŞILAŞTIRILMASI

2.1. ARAŞTIRMANIN KONUSU VE KAPSAMI

Nitelikli bir biyometrik sistemi kullanmak için biyometrik sistemleri değerlendirerek sistemleri karşılaştırmak gerekmektedir. Binalardaki güvenlik sistemleri personel tarafından kullanılmaktadır bu nedenledir ki karşılaştırmanın başarılı olabilmesi için personelin görüş ve düşünceleri değerlidir. Personelin onay vermediği, personel tarafından uygun görülmeyen ya da benimsenmeyen uygulamaları yürütmek kolay değildir. Bu noktada personelin kullanmış olduğu biyometrik sistemlere ilişkin görüşleri incelenmiştir. Ankara'nın başkent olmasından ötürü daha fazla kamu kurumu olduğu düşünülerek anket Ankara ilinde yapılmıştır. Bu doğrultuda Ankara ilinde, A1 ve A2 olarak nitelendirilen bir kurumun iki farklı şubesi ile B olarak nitelendirilen kurumda olmak üzere toplam iki kurumda görev yapan 82 personele anket yapılmıştır. Yöneltilen sorulara doğru ve samimi cevaplar alabilmek için anket yapılan personele ait ad ve soyadı gibi bilgileri alınmamıştır.

2.2. ARAŞTIRMANIN AMACI

Bu tez çalışmasında güvenlik amaçlı kullanılan kimlik doğrulama yöntemlerinden olan biyometrik veya kart tanıma sistemini kullanan personelin sistem ile ilgili görüşlerini belirlemek ve var olan durumu olduğu gibi betimlemek için bu görüşlere dayanarak biyometrik ve kart tanıma sistemlerinin karşılaştırılması amaçlanmıştır. Literatürde yapılan araştırmalar sonucunda insanlardaki bazı biyolojik özelliklerin eşsiz olduğu ortaya çıkmıştır. Araştırma sonucu ortaya çıkan durum araştırmacılara öneriler sunma açısından önemlidir.

2.3. ALT AMAÇLAR

1) Araştırmaya katılan personelin kullandığı sistemlere ilişkin görüşlerinde
    a. Güvenirlik,
    b. Harcanan vakit yönünden verimlilik,
    c. Kişinin kendini güvende hissetmesi,
    d. Binanın güvenliğini sağlaması,
    e. Öğrenilebilirlik,
    f. Şifre hatırlama zorunluluğunu ortadan kaldırma,
    g. Kart taşıma zorunluluğunu ortadan kaldırma,
    h. Kullanılabilirlik,
    i. Kurumda ne derece gerekli olduğu,
    j. Kamuda ne derece gerekli olduğu, konusunda personel görüşleri farklılaşmakta mıdır?

2) Personelin görev yaptığı süre içerisinde kurumunda kullanılan biyometrik sistem farklı bir sistemle değiştirildi mi? Değiştirildiyse sebebi/sebepleri nedir?

3) Personelin herhangi bir zamanda başka bir güvenlik sistemi ile ilgili deneyimi oldu mu? Olduysa bu sistem ile mevcut sistemi kullanılabilirlik yönünden karşılaştırması nasıldır?

4) Personelin herhangi bir zamanda başka bir güvenlik sistemi ile ilgili deneyimi oldu mu? Olduysa bu sistem ile mevcut sistemi güvenlik yönünden karşılaştırması nasıldır?

5) Personelin, çalıştığı kurumda kullanılan sistemin güvenlik yararları konusunda düşünceleri nelerdir?

6) Personele göre çalıştığı kurumda kullandığı sistemin olumlu yanları nelerdir?

7) Personele göre çalıştığı kurumda kullandığı sistemin olumsuz yanları nelerdir?

8) Personel Kurumunda kullanılan sistemin güvenlik dışında başka hangi amaçlar için kullanıldığını düşünüyor?

2.4. SAYILTILAR

i. Kurumlardaki personel anketi cevaplarken gerçek düşüncelerini yansıtmışlardır.
ii. Araştırmada kullanılan anket formu geçerli ve güvenilirdir.
iii. Araştırmada kullanılan anketin geçerliği ve güvenirliği ile ilgili başvurulan uzman görüşleri yeterlidir.
iv. Kaynak tarama sonucunda elde edilen bilgilerin doğruluğu kabul edilmiştir.

Örneklem evreni temsil edici niteliktedir.

2.5. SINIRLILIKLAR

Türkiye'de gelişmekte olan bir teknoloji olması sebebiyle hâlihazırda kamu kurumlarında çok sayıda güvenlik amaçlı kullanılan biyometrik sistem bulunmamaktadır. Çalışmanın amacı doğrultusunda biyometrik sistemler incelenirken, parmak izi, el geometrisi, yüz tanıma sistemi ve biyometrik sistem olmayan kartlı sistemlere ilişkin görüşlere yer verilmiştir.

Ayrıca bu araştırma,

i. Türkiye'deki Ankara İlindeki iki kurum ile sınırlıdır.
ii. Kurumlardaki personel görüşleri ile sınırlıdır.
iii. Veri toplama aracı olarak anket ile sınırlıdır.

Araştırma yapılan kurumların isimleri, tez genelinde kurumların güvenliği gerekçesi ile verilmemiştir.

2.6. ARAŞTIRMANIN MODELİ

Araştırma verileri iki farklı yöntemle toplanmıştır. Sağlıklı bununla birlikte gerçekçi bulgular elde etmek ve güvenlik sistemlerini karşılaştırabilmek için; nicel ve nitel yöntemden yararlanılmıştır.

Araştırma tarama modeli olarak seçilmiştir. Tarama modelleri; geçmişte veya hâlen var olan bir durumu, var olduğu şekli ile betimlemeyi amaçlayan araştırma yaklaşımıdır. Araştırmaya konu olan olay, birey ya da nesne, kendi koşulları içinde

ve olduğu gibi tanımlanmaya çalışılır. Onları herhangi bir şekilde değiştirme, etkileme çabası gösterilmez (Karasar, 2009:77).

2.7. EVREN VE ÖRNEKLEM

Araştırmanın evreni Ankara ilinde iki farklı kamu kurumunda görev yapıp kurumlarına giriş-çıkışlarda biyometrik veya kart tanıma sistemini kullanan ve ankete katılan 82 personel oluşturmaktadır.

Tablo 2.1: Biyometrik Ve Kart Tanıma Sistemi Dağılımı

Biyometrik ve Kart Tanıma Sistemi	**f**
Parmak izi	30
El Geometrisi	30
Kart Tanıma	22
Toplam	82

Ele alınan örneklem grubunda kurumunda parmak izi , el geometrisi (biyometrik) ve kart tanıma sisteminin kullanımına dair dağılım Tablo 2.1' de görülmektedir.

2.8. PERSONELİN DEMOGRAFİK YAPISI

Tablo 2.1'den 2.5'e kadar araştırmaya katılan personelin demografik bilgileri sunulmuştur.

Tablo 2.2: Araştırmaya Katılan Personelin Cinsiyetlerine Göre Dağılımı

Cinsiyet	**f**	**%**
Kadın	26	32
Erkek	56	68
Toplam	82	100

Tablo 2.2'de görüldüğü gibi % 32 oranında (26) kadın ve % 68 oranında (56) erkek personel araştırmaya katılmıştır.

Tablo 2.3: Araştırmaya Katılan personelin Yaşlarına Göre Dağılımı

Yaş	f	%
20-25	14	18
26-30	39	48
31-35	16	19
36-40	2	2
41-45	1	1
46-50	6	6
51-55	2	2
56-60	2	2
Toplam	82	100

Tablo 2.3'e göre ankete katılan personelin yaklaşık üçte ikisinin 30 yaş ve altı olduğu görülmektedir. Buna göre katılımcıların genç bireyler olduğu söylenebilir.

Tablo 2.4: Araştırmaya Katılan Personelin Çalışma Sürelerine Göre Dağılımı

Çalışma Yılı	f	%
1-5	70	85
6-10	4	4
11-15	4	4
16-20	-	-
21-25	-	-
26-30	3	3
31-35	1	1
Toplam	82	100

Tablo 2.4' e göre personelin yarıdan fazlası bir yıldır görev yaparken, yine 2 ve 3 yıllık çalışma süresi olanların oranı da yüksektir. Dolayısıyla katılımcıların büyük çoğunluğunun (yaklaşık %83) görev süresi açısından oldukça yeni oldukları söylenebilir.

Tablo 2.5: Araştırmaya Katılan Personelin Öğrenim Düzeyi Dağılımı

Öğrenim Durumu	f	%
Ortaokul	1	1
Lise	19	23
Üniversite	49	60
Lisansüstü	13	16
Toplam	82	100

Tablo 2.5'te göre katılımcıların yalnızca biri ortaokul mezunu iken 19' u lise; 49' u üniversite ve son olarak da 13' ünün lisansüstü mezunu olduğu görülmektedir. Buna göre katılımcıların fazlasının (yaklaşık dörtte üçü) üniversite ve üstü öğrenim kurumundan mezun olduğu söylenebilir.

Araştırmaya Katılan Personelin Bilgi Düzeyi Dağılımı ölçekte yer alan 6. Soru olan "Biyometrik sistemlerle ilgili bilgi düzeyinizi nasıl değerlendiriyorsunuz" sorusuna katılımcıların verdikleri cevaplar ele alındığında, ortalamanın 3,79 olduğu ve bunun orta düzeye yakın olduğu söylenebilir.

2.9. VERİLERİN TOPLANMASI

Posta, e-posta veya telefon ile yapılacak anket çalışmalarına katılımın az olabileceği ve gerekli özenin gösterilemeyebileceği öngörülerek tüm anketler, araştırmacı tarafından bizzat kurumlara gidip yetkili personele gerekli bilgiler verildikten sonra yetkili personel tarafından, kendi personeline edindiği bilgilerle dağıtılmak suretiyle tamamlanmıştır. Katılımcılara Ek-1'de bulunan toplam 24 adet açık ve kapalı uçlu soru yöneltilmiştir.

Çalışmanın amacı doğrultusunda biyometrik sistemler incelenirken, parmak izi, el geometrisi, yüz tanıma sistemi ve biyometrik sistem olmayan kartlı sistemlere ilişkin görüşlere yer verilmiştir.

Ayrıca bu araştırma,

i. Türkiye'deki Ankara İlindeki iki kurum ile sınırlıdır.

ii. Kurumlardaki personel görüşleri ile sınırlıdır.

iii. Veri toplama aracı olarak anket ile sınırlıdır.

Anket çalışması yapılan kurumların güvenlik sistemleri ile ilgili olumsuz yanlarının ortaya çıkmaması ve herhangi bir güvenlik zaafına sebebiyet vermemek için kurumların isimleri açıklanmamıştır.

Anket soruları hazırlanırken beş akademik personelden uzman görüşü alınmıştır. Ayrıca sorular yazım, dilbilgisi ve ifade eksiklikleri yönünden kontrol ettirilmiştir.

Ankete 150 kişi katılmış fakat 82 kişi anketi doğru ve eksiksiz olarak doldurduğu için değerlendirme 82 kişiye göre yapılmıştır. Görüşü alınan 82 kişiye ait veriler, istatistikî yöntemlerle [frekans (f), yüzde (%)] çözümlenerek değerlendirilmiş ve yorumlanmıştır. Bununla birlikte ki kare hesaplaması kullanılmıştır. Değerlendirme SPSS 17.0 programı kullanılarak yapılmıştır.

2.10. VERİLERİN ANALİZİ

Anket aracılığı ile toplanan veriler araştırmacılar tarafından bilgisayarda SPSS 17.0 for Windows paket programına kaydedilmiş ve veriler analiz edilmiştir. Araştırmada anlamlılık düzeyi p=0,05 olarak alınmıştır. p değerinin 0,05' ten küçük olduğu durumlarda anlamlı farklılık olduğu kabul edilmiştir. Personelin kullandığı biyometrik veya kart sistemine ait görüşlerini belirlemek için, her bir ifadeye ilişkin yüzde, frekans, aritmetik ortalama, standart sapma kullanılmış ve ki kare hesaplaması yapılmıştır. Anket yedi dereceli likert tipi ölçme aracı olarak geliştirilmiştir. Ayrıca verilen cevaplar da 1-3 için düşük, 4 için orta ve 5-7 için ise yüksek olacak şekilde düzenlenmiştir.

ÜÇÜNCÜ BÖLÜM
ARAŞTIRMA BULGULARI

3.1. BİYOMETRİK VE DİĞER SİSTEMLERİN GÜVENİRLİK YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemi güvenilir bulup bulmadıklarına ilişkin analiz tablo 3.1, 3.2, 3.3 ve 3.4'te gösterilmiştir.

Tablo 3.1 Biyometrik Ve Kart Tanıma Sistemi Güvenirlik Dağılımı

Biyometrik Ve Kart Tanıma Sistemi	Güvenirlik Düzeyi	f
Parmak izi	Düşük	3
	Orta	1
	Yüksek	26
	Toplam	30
El Geometrisi	Düşük	1
	Orta	3
	Yüksek	26
	Toplam	30
Kart Tanıma	Düşük	3
	Orta	6
	Yüksek	13
	Toplam	22

Tablo 3.2 Parmak İzi Güvenirlik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Güvenirlik Düzeyi
Chi-Square	38,600[a]
df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = **Parmak izi**	

Tablo 3.2'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre personel parmak izi sistemini yüksek düzeyde güvenilir bulmaktadır. Parmak izi: χ^2 (2) = 38,6, p < 0,05.

Tablo 3.3 El Geometrisi Güvenirlik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Güvenirlik Düzeyi
Chi-Square	38,600[a]
df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = **El geometri**	

Tablo 3.3'deki p değeri (Asymp. Sig.= ,000) ve χ2 hesabına göre, personel el geometri sistemini yüksek düzeyde güvenilir bulmaktadır. El geometri: χ2 (2) = 38,6, p < 0,05.

Tablo 3.4 Kart Tanıma Güvenirlik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Güvenirlik Düzeyi
Chi-Square	7,182[a]
df	2
Asymp. Sig.	,028
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,3.	
b. Kurumunuzda kullanılan biyometrik sistem = **Diğer(kart tanıma)**	

Tablo 3.4'deki p değeri (Asymp. Sig.= ,028) ve yapılan χ^2 hesabına göre personel, kart tanıma sistemini yüksek düzeyde güvenilir bulmaktadır. Kart Tanıma: χ^2 (2) = 7,18, p < 0,05.

3.2. BİYOMETRİK VE DİĞER SİSTEMLERİN HARCANAN VAKİT YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin giriş ve çıkışlarda harcanan vakit yönünden verimliliğini nasıl bulduklarına ilişkin analiz tablo 3.5, 3.6, 3.7 ve 3.8'de gösterilmiştir.

Tablo 3.5. Biyometrik Ve Kart Tanıma Sistemi Vakit Yönünden Verimlilik Dağılımı

Vakit Yönünden Verimlilik	Verimlilik Düzeyi	f
Parmak izi	Düşük	11
	Orta	5
	Yüksek	14
	Toplam	30
El Geometrisi	Düşük	17
	Orta	4
	Yüksek	9
	Toplam	30
Kart Tanıma	Düşük	4
	Orta	3
	Yüksek	15
	Toplam	22

Tablo 3.6 Parmak İzi Harcanan Vakit Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Harcanan Vakit Düzeyi
Chi-Square	4,200[a]
df	2
Asymp. Sig.	,122
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullamılan biyometrik sistem = Parmak izi	

Tablo 3.6'daki p değeri (Asymp. Sig.= ,122), yapılan χ^2 hesabına göre, personel parmak izi sisteminin vakit yönünden verimlilik düzeylerini farklı şekilde

algılamışlardır. Buna göre parmak izi sistemi kullanan personel, anlamlı bir şekilde lehte veya aleyhte cevap vermemişleridir. Parmak izi: χ^2 (2) = 4,2, p > 0,05.

Tablo 3.7 El Geometri Harcanan Vakit Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Harcanan Vakit Düzeyi
Chi-Square	8,600[a]
df	2
Asymp. Sig.	,014
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.7'deki p değeri (Asymp. Sig.= ,014), el geometrisi aleyhine anlamlı bir fark elde edilmiştir. Diğer bir deyişle kurumunda el geometrisi kullanan personelin fazlası bu sistemin vakitten kayıp yarattığını düşünmektedirler. El geometrisi: χ^2 (2) = 8,6, p < 0,05.

Tablo 3.8 Kart Tanıma Harcanan Vakit Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Harcanan Vakit Düzeyi
Chi-Square	12,091[a]
Df	2
Asymp. Sig.	,002
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,3.	
b. Kurumunuzda kullanılan biyometrik sistem = Diğer(kart tanıma)	

Tablo3.8'deki p değeri (Asymp. Sig.= ,002), kurumunda kart tanıma sistemi kullanan personelin fazlası bu sistemin kullanımının zaman kaybı yaratmadığını düşünmektedirler. Kart tanıma: χ^2 (2) = 12,09, p < 0,05.

3.3. BİYOMETRİK VE DİĞER SİSTEMLERİN KİŞİNİN KENDİNİ GÜVENDE HİSSETMESİ YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin varlığının kendilerini güvende hissetmelerine ne derece etkilidir sorusuna ilişkin analiz tablo 3.9, 3.10, 3.11 ve 3.12'de sunulmuştur.

Tablo 3.9. Biyometrik Ve Kart Tanıma Sistemi Varlığının Kendilerini Güvende Hissetmelerine Etki Derecesi

Biyometrik Ve Kart Tanıma Sistemi Varlığının Kendilerini Güvende Hissetmelerine Etki Derecesi	Etki Derecesi Düzeyi	f
Parmak izi	Düşük	4
	Orta	6
	Yüksek	20
	Toplam	30
El Geometrisi	Düşük	2
	Orta	11
	Yüksek	17
	Toplam	30
Kart Tanıma	Düşük	11
	Orta	5
	Yüksek	6
	Toplam	22

Tablo 3.10 Parmak İzi Güvende Hissetme Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Güvende Hissetme Düzeyi
Chi-Square	15,200[a]
df	2
Asymp. Sig.	,001
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.10'daki p değeri (Asymp. Sig.= ,001) ve yapılan χ^2 hesabına göre parmak izi sistemi için personel anlamlı bir şekilde lehte cevap vererek kendilerini güvende hissettiklerini belirtmişlerdir. Parmak izi: χ^2 (2) = 15,2, p < 0,05.

Tablo 3.11 El Geometrisi Güvende Hissetme Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statisticsb	
	Güvende Hissetme Düzeyi
Chi-Square	11,400[a]
df	2
Asymp. Sig.	,003
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.11'daki p değeri (Asymp. Sig.= ,003) ve yapılan χ^2 hesabına göre el geometrisi lehine anlamlı bir fark elde edilmiştir. Diğer bir deyişle kurumunda el geometrisi kullanan personelin fazlası bu sistemin varlığının, kendilerini orta ve yüksek düzeyde güvende hissetmelerine etki ettiğini düşünmektedirler. El geometrisi: χ^2 (2) = 11,4, P < 0,05.

Tablo 3.12 Kart Tanıma Güvende Hissetme Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Güvende Hissetme Düzeyi
Chi-Square	2,818[a]
Df	2
Asymp. Sig.	,244
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,3.	
b. Kurumunuzda kullanılan biyometrik sistem = Diğer(kart tanıma)	

Tablo 3.12'deki p değeri (Asymp. Sig.= ,244), yapılan χ^2 hesabına göre kurumunda kart tanıma sistemi kullanan personelin görüşlerinin anlamlı farklılık yaratmadığı ortaya çıkmıştır. Kart Tanıma: χ^2 (2) = 2,82, p > 0,05.

3.4. BİYOMETRİK VE DİĞER SİSTEMLERİN BİNANIN GÜVENLİĞİNİ SAĞLAMASI YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin binanın güvenliği sağlamaya ne derece yeterlidir sorusuna ilişkin analiz tablo 3.13, 3.14, 3.15 ve 3.16'da gösterilmiştir.

Tablo 3.13 Biyometrik Ve Kart Tanıma Sistemi Binanın Güvenliği Sağlamaya Ne Derece Yeterli

Kurumlarında Kullanılan Biyometrik Ve Kart Tanıma Sisteminin Binanın Güvenliği Sağlamaya Derecesi	**Güvenliği Sağlama Düzeyi**	**f**
Parmak izi	Düşük	3
	Orta	5
	Yüksek	22
	Toplam	30
El Geometrisi	Düşük	2
	Orta	6
	Yüksek	22
	Toplam	30
Kart Tanıma	Düşük	6
	Orta	5
	Yüksek	11
	Toplam	22

Tablo 3.14 Parmak İzi Bina Güvenliği Sağlama Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Bina Güvenliğini Sağlama Düzeyi
Chi-Square	21,800[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.14'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre parmak izi sistemi için personel, anlamlı bir şekilde lehte cevap vererek bulundukları binanın güvenliğini sağlamasında etkili olduğu görüşündedir. Parmak izi: (2) = 21,8, p< 0,05.

Tablo 3.15 El Geometrisi Bina Güvenliği Sağlama Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Bina Güvenliğini Sağlama Düzeyi
Chi-Square	22,400[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.15'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre el geometrisi lehine anlamlı bir fark elde edilmiştir. Başka bir deyişle el geometri sistemini kullanan personel, sistemin bulundukları binanın güvenliğini sağlamasında etkili olduğu görüşündedir. El geometrisi: χ^2 (2) = 22,4, P < 0,05.

Tablo 3.16 Kart Tanıma Bina Güvenliği Sağlama Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Bina Güvenliğini Sağlama Düzeyi
Chi-Square	2,818[a]
Df	2
Asymp. Sig.	,244
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,3.	
b. Kurumunuzda kullanılan biyometrik sistem = Diğer(kart tanıma)	

Tablo 3.16'daki p değeri (Asymp. Sig.= ,244) ve χ^2 hesabına göre kurumunda kart tanıma sistemi kullanan personelin görüşlerinin anlamlı farklılık yaratmadığı ortaya çıkmıştır. Kart tanıma: χ^2 (2) = 2,82, p > 0,05.

3.5. BİYOMETRİK VE DİĞER SİSTEMLERİN ÖĞRENİLEBİLİRLİK YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin öğrenilebilirlik düzeyi sorusuna ilişkin analiz tablo 3.17, 3.18 ve 3.19'da sunulmuştur.

Tablo 3.17 Biyometrik Ve Kart Tanıma Sistemi Öğrenilebilirliği

Kurumlarında Kullanılan Biyometrik Ve Kart Tanıma Sisteminin Öğrenilebilirlik Derecesi	Öğrenilebilirlik Düzeyi	f
Parmak izi	Düşük	5
	Orta	3
	Yüksek	22
	Toplam	30
El Geometrisi	Düşük	1
	Orta	2
	Yüksek	27
	Toplam	30
Kart Tanıma	Düşük	0
	Orta	0
	Yüksek	22
	Toplam	22

Tablo 3.18 Parmak İzi Öğrenme Düzeyi Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Öğrenme Düzeyi
Chi-Square	21,800[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.18'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre parmak izi sistemi için personel anlamlı bir şekilde lehte cevap vermişleridir. Parmak izi: χ^2 (2) = 21,8, p < 0,05.

Tablo 3.19 El Geometrisi Öğrenme Düzeyi Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Öğrenme Düzeyi
Chi-Square	43,400[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.19'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre el geometrisi lehine anlamlı bir fark elde edilmiştir. El geometrisi: χ^2 (2) = 43,4, P < 0,05.

Diğer taraftan, kurumunda Kart tanıma sisteminin öğrenilebilirliğinin tüm personel (22 kişi) tarafından yüksek düzeyde olarak işaretlenmiş olması dikkat çekicidir.

3.6. BİYOMETRİK VE DİĞER SİSTEMLERİN ŞİFRE HATIRLAMA ZORUNLULUĞUNU ORTADAN KALDIRMASI YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin şifre hatırlama zorunluluğunu ortadan kaldırma düzeyi sorusuna ilişkin analiz Tablo 3,20, 3.21 ve 3.22'de gösterilmiştir.

Tablo 3.20. Biyometrik Ve Kart Tanıma Sisteminin Şifre Hatırlama Zorunluluğunu Ortadan Kaldırması

Kurumlarında Kullanılan Biyometrik Ve Kart Tanıma Sisteminin Şifre Hatırlama Zorunluluğunu Ortadan Kaldırması	Şifre Hatırlama Zorunluluğunu Ortadan Kaldırma Düzeyi	f
Parmak izi	Düşük	1
	Orta	2
	Yüksek	27
	Toplam	30
El Geometrisi	Düşük	0
	Orta	2
	Yüksek	28
	Toplam	30
Kart Tanıma	Düşük	0
	Orta	0
	Yüksek	22
	Toplam	22

Tablo 3.21 Parmak İzi Şifre Hatırlama Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Şifre Hatırlama Düzeyi
Chi-Square	43,400[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.21'deki p değeri (Asymp. Sig.= ,000), yapılan χ^2 hesabına göre parmak izi sistemi kullanan personel, şifre hatırlama zorunluluğunu ortadan kaldırmasına anlamlı bir şekilde lehte cevap vermişleridir. Parmak izi: χ^2 (2) = 43,4, $p < 0,05$.

Tablo 3.22 El Geometrisi Şifre Hatırlama Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Şifre Hatırlama Düzeyi
Chi-Square	22,533[a]
Df	1
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 15,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.22'deki p değeri (Asymp. Sig.= ,000). Yapılan χ^2 hesabına göre el geometri sistemi kullanan personel, şifre hatırlama zorunluluğunu ortadan kaldırmasına anlamlı bir şekilde lehte cevap vermişleridir. El geometrisi: χ^2 (2) = 22,5, $p < 0,05$.

Diğer taraftan, kurumunda Kart tanıma sisteminin şifre hatırlama zorunluluğunu ortadan kaldırması, tüm personel (22 kişi) tarafından yüksek düzeyde olarak işaretlenmiştir.

3.7. BİYOMETRİK VE DİĞER SİSTEMLERİN KART TAŞIMA ZORUNLULUĞUNU ORTADAN KALDIRMASI YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin kart taşıma zorunluluğunu ortadan kaldırma düzeyi sorusuna ilişkin analiz tablo 3.23 ve 3.24'te sunulmuştur.

Tablo 3.23. Biyometrik Ve Kart Tanıma Sisteminin Kart Taşıma Zorunluluğunu Ortadan Kaldırması

Kurumlarında Kullanılan Biyometrik Ve Kart Tanıma Sisteminin Kart Taşıma Zorunluluğunu Ortadan Kaldırması	Kart Taşıma Zorunluluğunu Ortadan Kaldırma Düzeyi	f
Parmak izi	Düşük	1
	Orta	2
	Yüksek	27
	Toplam	30
El Geometrisi	Düşük	0
	Orta	0
	Yüksek	30
	Toplam	30
Kart Tanıma	Düşük	22
	Orta	0
	Yüksek	0
	Toplam	22

Tablo 3.24 Parmak İzi Kart Taşıma Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Kart Taşıma Zorunluluk Düzeyi
Chi-Square	43,400[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Buna göre parmak izi sistemi için personel anlamlı bir şekilde lehte cevap vermiştir. Parmak izi: χ^2 (2) = 43,4, $p < 0,05$.

Yine tüm katılımcılar (30) el geometrisi lehine cevap vermişlerdir. Bunların aksine kurumunda kart tanıma sistemi kullanan personelin tümü (22 kişi) kart taşıma zorunluluğunu ortadan kaldırma düzeyini düşük olarak işaretlemişlerdir.

3.8. BİYOMETRİK VE DİĞER SİSTEMLERİN KULLANILABİLİRLİK YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin kullanılabilirlik düzeyi sorusuna ilişkin analiz Tablo 3.25, 3.26 ve 3.27'de verilmektedir.

Tablo 3.25. Biyometrik Ve Kart Tanıma Sisteminin Kullanılabilirliği

Kurumlarında Kullanılan Biyometrik ve Kart Tanıma Sisteminin Kullanılabilirliği	**Kullanılabilirlik Düzeyi**	**f**
Parmak izi	Düşük	5
	Orta	6
	Yüksek	19
	Toplam	30
El Geometrisi	Düşük	2
	Orta	8
	Yüksek	20
	Toplam	30
Kart Tanıma	Düşük	0
	Orta	0
	Yüksek	22
	Toplam	22

Tablo 3.26 Parmak İzi Kullanılabilirlik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Kullanılabilirlik Düzeyi
Chi-Square	12,200[a]
Df	2
Asymp. Sig.	,002
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.26'daki p değeri (Asymp. Sig.= ,002) ve yapılan χ^2 hesabına göre parmak izi sistemi kullanan personel sistemin kullanılabilir olduğuna dair lehte cevaplar vermişlerdir. Parmak izi: χ^2 (2) = 12,2, $p < 0,05$.

Tablo 3.27 El Geometrisi Kullanılabilirlik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Kullanılabilirlik Düzeyi
Chi-Square	16,800[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.27'daki p değeri (Asymp. Sig.= ,000) ve χ^2 hesabına göre el geometri sistemi kullanan personel sistemin kullanılabilirliği lehine cevap vermişlerdir. El geometrisi: χ^2 (2) = 16,8, $p < 0,05$.

Diğer taraftan kart tanıma sisteminin kullanılabilirliği tüm katılımcılar (22 kişi) tarafından yüksek düzeyde olarak işaretlenmiştir.

3.9. BİYOMETRİK VE DİĞER SİSTEMLERİN KURUMDA NE DERECE GEREKLİ OLDUĞU YÖNÜNDEN DEĞERLENDİRİLMESİ

Kurumda bulunan biyometrik ve kart tanıma sisteminden herhangi birini kullanan personelin, kullandığı sistemin gereklilik düzeyi sorusuna ilişkin analiz tablo 3,28, 3.29, 3.30 ve 3.31'de gösterilmektedir.

Tablo 3.28 Biyometrik Ve Kart Tanıma Sisteminin Gerekliliği

Kurumlarında Kullanılan Biyometrik Ve Kart Tanıma Sisteminin Gerekliliği	Gereklilik Düzeyi	f
Parmak izi	Düşük	10
	Orta	4
	Yüksek	16
	Toplam	30
El Geometrisi	Düşük	6
	Orta	2
	Yüksek	22
	Toplam	30
Kart Tanıma	Düşük	1
	Orta	5
	Yüksek	16
	Toplam	22

Tablo 3.29 Parmak İzi Gereklilik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Gereklilik Düzeyi
Chi-Square	7,200[a]
df	2
Asymp. Sig.	,027
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = Parmak izi	

Tablo 3.29'daki p değeri (Asymp. Sig.= ,027), yapılan χ^2 hesabına göre parmak izi sistemi için personel anlamlı bir şekilde lehte cevap vererek bu sistemin gerekli olduğunu söylemişlerdir. Parmak izi: χ^2 (2) = 7,2, $p < 0,05$.

Tablo 3.30 El Geometrisi Gereklilik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Gereklilik Düzeyi
Chi-Square	22,400[a]
df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 10,0.	
b. Kurumunuzda kullanılan biyometrik sistem = El geometrisi	

Tablo 3.30'daki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre el geometri sistemi için personel anlamlı bir şekilde lehte cevap vererek bu sistemin gerekli olduğunu söylemişlerdir. El geometrisi: χ^2 (2) = 22,4, $p < 0,05$.

Tablo 3.31 Kart Tanıma Gereklilik Ki-Kare(Chi-Square (χ^2)) Hesabı

Test Statistics[b]	
	Gereklilik Düzeyi
Chi-Square	16,455[a]
Df	2
Asymp. Sig.	,000
a. 0 cells (,0%) have expected frequencies less than 5. The minimum expected cell frequency is 7,3.	
b. Kurumunuzda kullanılan biyometrik sistem = Diğer(kart tanıma)	

Tablo 3.31'deki p değeri (Asymp. Sig.= ,000) ve yapılan χ^2 hesabına göre kart tanıma sistemini kullanan personel anlamlı bir şekilde lehte cevap vererek bu sistemi yüksek düzeyde gerekli olarak işaretlemiştir. Kart tanıma: χ^2 (2) = 16,5, $p < 0,05$.

3.10. BİYOMETRİK VE DİĞER SİSTEMLERİN KAMUDA NE DERECE GEREKLİ OLDUĞU YÖNÜNDEN DEĞERLENDİRİLMESİ

Ölçekte yer alan 7. Soru olan "Kamuda, biyometrik sistemlerin kullanılmasını ne derece gerekli görüyorsunuz?" sorusuna personelin verdikleri cevaplar ele

alındığında, ortalamanın 5,17 olduğu ve bunun ortanın üzerinde bir düzey olduğu söylenebilir.

3.11. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN DEĞİŞTİRİLME SEBEBİ/SEBEBLERİNE İLİŞKİN BULGULAR

Kurum A1'de veri toplama amacıyla ulaşılan ve parmak izi sistemini kullanan personel bu soruya hayır yanıtını vererek görev yaptığı süre içerisinde farklı bir sistemi kullanmadığını belirtmiştir. Dolayısıyla herhangi bir değiştirme nedeni açıklanmamıştır.

Kurum A2'de görevli personelden bu soruya yanıt veren personel, daha önceden kartlı sistem kullandıklarını belirtmiş, şu anda kurumda kullanılan el geometrisinin daha önce kullanılan kartlı sisteme oranla daha güvenli olduğunu ve bu yüzden değiştirildiğini kendi ifadeleriyle; *"Kartı başka birisi alıp kullanabilmektedir bu yüzden kartla geçiş sistemi el geometrisine göre daha zayıf güvenlik sağlamaktadır, biyometrik sistem(el geometrisi) kendine özgü olduğundan kartlı sisteme göre daha güvenlidir."*

Kurum B'de görevli personel, kurumda daha önce yüz tanıma sistemini kullanıldığının şu andaki mevcut sistemin ise kartlı sistem olduğunu belirtmiştir. Bu soruya yanıt verenlerin cevaplarından en öne çıkanı giriş-çıkışlarda ortaya çıkan sorunlar olduğu *"Giriş-çıkışlarda sorunlar yaşanıyordu özellikle bayanlarda(makyaj gibi), zaman kaybı oluyordu, performans eksikliği vardı ve verimsizlik oldu."* şeklinde ifade edilmiştir.

3.12. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN KULLANILABİLİRLİĞİNE İLİŞKİN BULGULAR

Kurum A1'de görevli ve parmak izi sistemi kullanan personelden bu soruya yanıt veren personel herhangi bir zamanda kartlı sistemi kullandıklarını ortaya koymuşlardır. Dolayısıyla parmak izi ile kartlı sistemin kullanılabilirliğini karşılaştırmışlardır. Yapılan bu karşılaştırmada kartlı sistemin kullanılırlığının daha

iyi olduğunu personel ifadeleriyle; *"kartlı sistemin kullanmak daha kolay ve hızlı, binaya daha seri girip çıkılıyor"* şeklinde ifade edilmektedir.

Kurum A2'de görevli el geometri sistemi kullanan personelden bu soruya yanıt veren personel herhangi bir zamanda kartlı sistemi kullandıklarını söylemiştir. Herhangi bir zamanda kartlı sistem kullandığını belirten personelden birçoğu kartlı sistemin kullanılırlığının daha iyi olduğunu ortaya koymuştur. Ortaya konulan nedenler *"kartlı sistemin kullanımı daha hızlı, kolay ve pratiktir"* biçimindedir.

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt veren personel kurumdaki kartlı sistemle yüz tanıma sisteminin karşılaştırmıştır. Yapılan karşılaştırmada genel olarak, kartlı sistemin kullanılırlığının, yüz sistemine göre daha iyi olduğunu ortaya koyan personelin nedenleri *"Kartlı sitem daha kolay ve hızlı, Yüz tanıma sistemi zaman alıcı, daha zor, yüz tanıma sisteminde giriş –çıkış süresi daha uzun ve yüz tanıma sisteminde tanıma sorunu(mimikler, makyaj gibi)"* biçimindedir.

3.13. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN GÜVENLİK YÖNLERİNE İLİŞKİN BULGULAR

Kurum A1'de görevli ve parmak izi sistemi kullanan personelden bu soruya yanıt veren personel herhangi bir zamanda kartlı sistemi kullandıklarını ortaya koymuşlar ve parmak izi ile kartlı sistemi güvenlik yönünden karşılaştırmışlardır. Bu soruya personelin vermiş olduğu cevaplar kendi ifadeleriyle şu şekildedir; *"Biyometrik sistem olan parmak izi daha güvenlidir, kişi kendi uzvunu(parmağını) kullanarak geçiş yapar bu yüzden daha güvenli, kart çalınabilir veya kaybolabilir bu yüzden güvenlik zaafları mevcuttur."*

Kurum A2'de görevli el geometri sistemi kullanan personelden bu soruya yanıt veren personel herhangi bir zamanda kartlı sistemi kullandıklarını söylemiştir. Herhangi bir zamanda kartlı sistem kullandığını belirten personel el geometrisi ve kartlı sistemi güvenlik yönünden karşılaştırmış el geometrisinin daha güvenli olduğunu ortaya koymuştur. Ortaya konulan nedenler *"El geometrisi kendine özgü olduğundan kartlı sisteme göre daha güvenli, kartla geçiş sistemi daha az güvenlikli*

çünkü kartı başka biri alıp kullanabilir, kartı eline geçiren herkes giriş yapabilir bu yüzden güvenli değil" biçimindedir.

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt veren personel herhangi bir zamanda yüz tanıma sistemini kullandıklarını ortaya koymuşlardır. Kısacası kurumdaki kartlı sistemle yüz tanıma sistemini karşılaştırmıştır. Yapılan karşılaştırmada Yüz tanıma sisteminin kartlı sisteme göre daha güvenlikli olduğunu belirtmişlerdir Bu soruya personelin vermiş olduğu cevaplar kendi ifadeleriyle özetle; *"Yüz tanıma sistemi daha güvenli herkes kendi yüzünü kullanmaktadır. Yüz tanıma sisteminin daha güvenli olduğunu düşünüyorum çünkü kişi kendi orada olmadıkça giriş yapılamaz. Yüz tanıma sistemi daha güvenli zira başkası adına sistemden geçiş şansı yoktur. Kartlı sistemde başkası adına kart kullanılabilir veya kaybolabilir."*şeklindedir.

3.14. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN GÜVENLİK YARARLARINA İLİŞKİN BULGULAR

Kurum A1'de görevli parmak izi sistemini kullanan personelden soruya cevap verenler sistemin güvenlik açısından yararlı olduğu üzerinde durmuş ve kendi ifadeleriyle genel olarak şunları ifade etmişlerdir; *"Güvenlik açısından yararlıdır, giriş-çıkışlar kontrol altındadır."*

Kurum A2'de görevli el geometri sistemini kullanan personelden soruya cevap veren personele göre; *"Kişiye özel olduğu için güvenlik bakımından oldukça yararlıdır, giriş-çıkışlar tamamen kontrol altındadır, insan hatalarından oluşabilecek güvenlik açıklarını ortadan kaldırmaktadır(şifre unutma, kart kaybetme gibi)."*

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt verenler farklı görüşler ortaya koymuşlardır. Bir grup personel kartlı sistemin güvenlik açısından yararlı olduğunu ifade etmiş *"Personel ve misafir takibi yapar, vukuat anında binada kimlerin olduğu tespit edilebilir, kart başkalarının eline geçmediği sürece güvenlik açısından yararlıdır, güvelik konusunda yararlı olduğunu düşünüyorum, caydırıcıdır, giriş-çıkışları kontrol altında tutar.*" olarak görüşlerini belirtmiştir. Diğer grup personel ise, kartlı sistemin güvenlik açısından yararlı

olmadığını ortaya koymuş ve "*mevcut sistemin güvenlik konusunda yetersiz olduğunu düşünüyorum.*"olarak görüşlerini belirtmiştir. Son olarak diğer bir grup personel ise kartlı sistemin tek başına güvenlik için yeterli olmadığından bahsetmiş, ve ana hatlarıyla şunları söylemiştir "*çok güvenli olmasa da yararı vardır*, yararı muhakkak vardır, hiç yoktan iyidir, *tam anlamıyla güvenli değil* " şeklinde görüş belirtmiştir.

3.15. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN OLUMLU YANLARINA İLİŞKİN BULGULAR

Kurum A1'de görevli parmak izi sistemini kullanan personelden bu soruya yanıt veren personelin cevapları genel olarak kendi ifadeleriyle özetle şu şekildedir; "*Güvende hissettirmektedir, giriş-çıkışlar denetim altındadır, kart taşıma ve şifre hatırlama zorunluluğu yoktur, giriş-çıkışlarda personeli denetlemede faydalıdır."*

Kurum A2'de görevli el geometri sistemini kullanan personelden soruya yanıt veren personel cevaplarında ana hatlarıyla şunları ifade etmişlerdir; *"Güvenilirdir, güvende hissettirir, şifre hatırlama ve kart taşıma zorunluluğu yoktur."*

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt veren personelin cevapları özetle; *"Güvenilir ve hızlı olması, personelin ve binaya giriş yapan misafirlerin takibinin yapılması, şifre hatırlama zorunluluğunun olmaması"* şeklindedir.

3.16. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN OLUMSUZ YANLARINA İLİŞKİN BULGULAR

Kurum A1'de görevli parmak izi sistemini kullanan personelden bu soruya yanıt veren personelin cevapları genel olarak kendi ifadeleriyle özetle şu şekildedir; *"Zaman kaybına yol açmaktadır, fişlenme duygusu vardır, zaman kaybı ve hijyenik(sağlıklı) değildir."*

Kurum A2'de görevli el geometri sistemini kullanan personelden soruya yanıt veren personel cevaplarında ana hatlarıyla şunları ifade etmişlerdir; *"Zaman kaybına*

yol açmaktadır, İnsanların özellikleri kayıt altına alınmaktadır ve hijyenik(sağlıklı) değildir."

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt veren personele göre sistemin olumsuz yanları; "*Kart taşıma zorunluluğu, kartın kaybolması veya çalınması, kartın yetkisiz kişilerin eline geçmesi."*şeklindedir.

3.17. KULLANILAN BİYOMETRİK VE DİĞER SİSTEMLERİN BAŞKA HANGİ AMAÇLAR İÇİN KULLANILDIĞINA İLİŞKİN BULGULAR

Kurum A1'de görevli parmak izi sistemini kullanan personelden soruya yanıt veren personel sistemin güvenlik dışında personeli denetlediğini belirmiş ve kendi ifadeleriyle genel olarak şunları ifade etmişlerdir; *"Personelin mesai saatlerinde giriş-çıkış kontrolünü yapar, iş takibi yapar."*

Kurum A2'de görevli el geometri sistemini kullanan personelden bu soruya yanıt veren personelin sistemin güvenlik dışında personeli denetlediğini ortaya koymuşlardır. Ortaya konulan nedenler; *"Giriş ve çıkışlarda personelin kaydını tutuyor ve personeli denetler"* biçimindedir.

Kurum B'de görevli kartlı sistemi kullanan personelden bu soruya yanıt veren personel sistemin güvenlik dışında personeli denetlemek amacında olduğunu belirterek özetle şunları ifade emişlerdir *; "Personel devam takibi, mesai dışında kimlerin kurumda çalıştığı, bizim işe geliş ve gidişimizi kontrol eder."*

SONUÇ VE ÖNERİLER

Bu tez çalışması kapsamında yaygın olan biyometrik sistemler tanıtılmış, kamuda güvenlik amaçlı kullanılan biyometrik sistemlerin çalışma prensipleri temel alınarak söz konusu biyometrik sistemleri karşılaştırmak amaçlanmıştır. Bu doğrultuda herhangi bir zamanda herhangi bir yerde veya kamuda biyometrik sistemleri kullanan personelin kullandıkları sistem veya sistemleri değerlendirmeleri irdelenmiştir. Kurum A1, A2 ve B olarak adlandırılan iki kamu kurumda yapılan anket çalışmasında; Kurum A1'deki personel parmak izi sistemini, kurum A2'deki personel el geometrisi ve Kurum B'deki personel biyometrik olmayan kartlı sistemi kullanmıştır. Kartlı sistemi kullanan B kurumunda daha önce yüz tanıma sistemi kullanılmıştır.

Kurumlarında biyometrik ve kart tanıma sistemini kullanan personel, sistemini güvenilir bulup bulmadıklarına ilişkin yapılan analizlerde kendi kullandıkları güvenlik sistemlerini güvenilir bulmuşlardır.

Personel kullandıkları sistemleri vakit yönünden değerlendirmiş, kartlı sistemi kullanan personel, sistemin zaman kaybı yaratmadığına dair görüş belirtmiştir. Bununla birlikte kartlı sistemi kullanan personel daha önce kurumda yüz tanıma sistemini kullandıklarını ve zaman kaybı nedeniyle kartlı sisteme geçtiklerini ifade etmişlerdir. Parmak izi tanıma sistemi ile ilgili vakit yününden yapılan değerlendirmede lehte veya aleyhte bir görüş belirtilmezken, el geometrisi kullanan personel bu sistemin vakit kaybına yol açtığı görüşündedir.

Tüm bu görüşler neticesinde yüz tanıma sisteminin diğer sistemlere göre daha zaman alıcı olduğu ve yüzde yapılan değişiklikler (makyaj, mimikler) gibi sorunlara henüz çözüm bulunamadığı sonucuna varılmıştır. Yapılan literatür taramasında da yüz tanıma tabanlı sistemlerin insanlar tarafından rahatsız edici bulunduğu, yüz tanıma sistemlerinde değişen poz, ışıklandırma ve karmaşık arka planın tanımayı doğrudan çok ciddi şekilde etkileyebilen değişkenlerin başında geldiğine değinilmiştir.

El geometrisinin ise yüz tanıma sisteminden sonra en çok vakit kaybına neden olan sistem olduğu, bu sistemleri sırasıyla parmak izi ve kartlı sistemlerin izlediği sonucuna varılmıştır. Daha önceki çalışmalara bakıldığı zaman yüz

tanıma sisteminin yanlış reddi kolay kabul etmesi, el geometri sisteminin yanlış ret oranının orta düzeyde olması, parmak izi sisteminde ise yanlış ret oranının çok zor düzeyde olması bunun bir göstergesidir.

Yapılan anket çalışmasında yüz tanıma sisteminin performans eksikliğinden bahsedilmiş ve değiştirilme sebeplerinden gösterilmiştir. Daha önceki çalışmalardan yapılan literatür taramasında da performans yönünden yüz tanıma sisteminin düşük seviyede, el geometrisinin orta düzeyde ve parmak izi sisteminin yüksek düzeyde olduğu belirtilmiştir. Yüz, parmak izi ve el geometri sistemi doğrulama modunda düzgün çalışırken, tanıma modunda ise parmak izi sistemi dışında kalan yüz ve el geometrisi sistemlerinde verimin düştüğünden bahsedilmiştir.

Parmak izi ve el geometrisi sistemi kullanan personelden bir kısmı herhangi bir zamanda kartlı sistemi kullandıklarını ortaya koymuşlar, parmak izi ve el geometrisi ile kartlı sistemi güvenlik yönünden karşılaştırmışlardır. Yapılan karşılaştırma sonucunda parmak izi ve el geometrisi sistemlerinin, kartlı sisteme göre daha güvenli olduğu belirtilmiştir. Parmak izi ve el geometrisi sistemini kullanan personel bu sistemlerin kendilerini orta ve yüksek düzeyde güvende hissetmelerine etki ettiklerini düşünmektedirler. Yine daha önceden yüz tanıma sistemi kullanıp şu anda kartlı sistemi kullanan personel, yüz tanıma sisteminin daha güvenli olduğunu belirmiştir. Ayrıca parmak izi ve el geometrisi tanıma sistemini kullanan personel, güvenlik yönünden bu sistemlerin yararlı olduğunu düşünürken, kart tanıma sistemini kullanan personel görüş ayrılığına düşerek yararlı, yararsız ve kısmen yararlı olduğunu düşünen guruplara bölünmüştür. Yapılan tüm bu analizlerin sonucunda biyometrik sistemler olan parmak izi, el geometrisi ve yüz tanıma sisteminin, kartlı sisteme göre daha güvenlikli olduğu sonucuna varılmıştır.

Personel, biyometrik sistem olan parmak izi, el geometrisi ve yüz tanıma sistemlerinin kişiye özgü ve insan hatalarını ortadan kaldıracak nitelikte olduğunu belirtmiştir. Parmak izi, el geometrisi ve kartlı sistemi kullanan personelin şifre hatırlama zorunluluğunun olmadığı ortaya çıkmıştır.

Parmak izi ve el geometrisi sisteminde başka bir deyişle biyometrik sistemlerde kart taşıma zorunluluğunun olmadığı bunun aksine kartlı sistemlerde kart taşıma zorunluluğunun olduğu ortaya konmuştur.

Biyometrik sistemlerde kullanılan biyometrik veri, biyolojik olarak sahip olduğumuz veri olup, insan biyolojisinin değişmesi çok zor olan özelliklerinin ölçümünü içermektedir. Bu nedenle, bu ölçümler üzerinde kurulmuş olan sistemler, hata payı sıfıra yakın bir kesinlikte görevlerini yerine getirmektedir.

Biyometrik olmayan bir sistemde şifreyi unutmak, yapay olan verilerle değiştirmek, kullandığı objeyi ele geçirmek mümkündür bu da güvenlik zafiyeti anlamına gelmektedir. Bu yüzden bu sistem kullanıcıya bazı bilgileri bilme ve hatırda tutma bazı objeleri sürekli olarak yanında taşıma, unutmama gibi sorumluluklar yüklemektedir. Tüm bunları biyometrik olmayan sistemlerin dezavantajı olarak sayabiliriz.

Biyometrik sistemlerde böyle bir durum söz konusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, objeye vs ihtiyacı yoktur.

Biyometrik sistemleri kullanan personel fişlenmek duygusu algılamaktadır. Daha önce yapılan çalışmalarda, bu sistemlerin bir özel yaşam gizliliği sorunu olup olmadığı ve bu sistemlerin kullanımındaki etik değerler irdelenmiştir. Bu çalışma biyometrik sistemlerin çalışma prensipleri üzerine olup sosyolojik açıdan değerlendirilmeden kaçınılmıştır.

Yapılan anket çalışmasında personel; parmak izi ve el geometrisi sistemlerini sağlık açısından değerlendirmiş ve hijyenik olmadığı ortaya konmuştur.

Parmak izi ve el geometrisi tanıma sisteminin yani biyometrik sistemlerin kullanılabilir ve öğrenilebilir olmasına karşın kartlı sistemin kullanılabilirliğinin ve öğrenilebilirliğin daha yüksek olduğu belirtilmiştir. Bununla birlikte personelin, kendi kurumlarında ve kamuda biyometrik ve kartlı sistemler kullanılmasının gerekli olduğu ortaya çıkmıştır.

Kurum A1, A2 ve B'deki parmak izi, el geometrisi ve kart tanıma sistemleri, güvenlik dışında sistemi kullanan personelin mesai saatlerine riayet edip etmedikleri ile ilgili olarak giriş-çıkışlarını denetlenmekte kullanılmaktadır.

Araştırmada örneklem olarak kullanıcı personel temel alınmıştır. İleriki araştırmalarda güvenlik sistemlerine ilişkin görüşler konusunda sistemi kuran uzmanların ve üst düzey yöneticilerin görüşleri de alınabilir. Böylelikle biyometrik sistemlerin maliyeti ve çalışma prensipleri daha detaylı bir şekilde irdelenecektir.

Araştırmanın evreni Ankara olarak belirlenmiştir. İleriki araştırmalar Türkiye'nin diğer bölgelerinde veya genelinde gerçekleştirilebilir.

Araştırmada parmak izi, el geometrisi, kart tanıma ve dolaylı yoldan yüz tanıma sistemi ele alınmıştır. İleriki araştırmalarda bunlar dışındaki biyometrik sistemler de ele alınarak daha fazla biyometrik sistemin karşılaştırılması yapılabilinir.

Anketin yapıldığı kurumlardaki personel tek güvenlik sistemi kullanmaktadır. Daha sonra yapılacak çalışmalarda birden çok biyometrik sistem kullanan kurumlarda birden çok sistemi aynı anda kullanarak giriş yapan personel ele alınabilinir.

KAYNAKÇA

Ajana, Btihaj, (2012), "Biometric citizenship", *Citizenship Studies*, 16:7, pp.851-870.

Akınlar, Cüneyt, (2012), "Bina Giriş Kontrol Sistemleri", Yusuf Oysal (Ed.), *Güvenlik Sistemleri*, T.C. Anadolu Üniversitesi Yayını no: 2489, Açıköğretim Fakültesi Yayını No:1460, ss.44-64.

Akram, Syed; Mohammed, Misbahuddin ve Varaprasad, G., (2012), "A Usable and Secure Two-Factor Authentication Scheme", *Information Security Journal*: A Global Perspective, 21:4, pp.169-182.

Arar, Nuri Murat, (2010), *Fusing Local Appearance Models For Face Recognition*, Bilkent University B.S Computer Engineering Master Thesis.

Buckland, Michael, (1991), "Information as Thing*.", Journal of the American Society for Information Science*, pp.351-360.

Çelebi, Aysun Taşyapı, (2008), *Biyometrik Tanıma*, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Kocaeli.

Dhameja, Sandeep CISSP, NSA IAM, (2005), "Multi-Characteristic Biometric Systems: Who Are You?", *Information Systems Security, March/April*.

Dixon, Pam, (2008), Ethical Issues Implicit in Library Authentication and Access Management: "Risks and Best Practices", *Journal of Library Administration*, 47:3-4, pp.141-162.

Doğan, Şengül, (2011), *Yeni Bir Sayısal Damgalama Tekniği ile Biyometrik Uygulamalar*, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Yayınlanmamış Doktora Tezi.

Durmuş, Sinem Özer, (2010), *İristen Kimlik Tanıma*, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kocaeli.

Eren, Bilal, (2009), *Biyometrik Teknolojilerin Etkili Tasarlanması Ve uygulanmasında Yeni bir öneri: Multimodel teknoloji*, Mimar Sinan Güzel Sanatlar Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi.

Ergen, Burhan ve Çalışkan, Abidin, (2011), "Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri", *6th International Advanced Technologies Symposium* (IATS'11), 16-18 May 2011, Elazığ, Turkey.

Erkan, Hüsnü ve Erkan, Canan, *Bilgi Ekonomisinde Teori ve Politika*, kisi.deu.edu.tr/selim.sanlisoy/bilgiekonomisinde_teori_politika.doc (Erişim Tarihi: 22.07.2014)

Filiz, Süleyman, (2012), *Siber Güvenlikte Biyometrik Sistemler ve Yüz Tanıma*, Gazi Üniversitesi Bilişim Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

Freeman, Edward H. J.D, (2003), Biometrics, Evidence, and Personal Privacy, *Information Systems Security*, 12:3, pp.4-8.

Geyik, M. ve Barca, M. (2004), "Etkin Bilgi Üretimi İçin Örgütler Nasıl Tasarlanmalıdır?", *İII. Ulusal Bilgi, Ekonomi Ve Yönetim Kongresi*, ss. 409-418, Eskişehir.

Gough, Reid, (2008), "Biometric Studies at Davenport University", *Journal of Applied Security Research*, 3:2, pp.269-282.

Gürbüz, Filiz, (2014), *Serbest Taklit Yöntemi İle Atılan Sahte İmzaların Grafometrik Özelliklerine Dayalı Biyometrik İmzadoğrulama Sistemi Ve Analizi*, Gazi Üniversitesi Bilişim Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Hanilçi, Cemal, (2007), *Konuşmacı Tanıma Yöntemlerinin Karşılaştırmalı Analizi*, Uludağ Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Bursa.

Hıdımoğlu, Kadir, (2010), *Web Kamera Kullanımı ile Parmak İzi Tanıma Ve Kimlik Tespiti Doğrulama*, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, İstanbul.

Holden, Stephen H. ve Millet, Lynette I., (2005), "Authentication, Privacy, and the Federal E-Government", *The Information Society: An International Journal*, 21:5, pp.367-377.

Hopkins, Richard, (1999), "An Introduction to Biometrics and Large Scale Civilian Identification", *International Review of Law, Computers and Technology*, 13:3, pp.337-363.

Jain, Anil; Bolle, Ruud and Pankant, Sarath (2002), "Introduction To Biometrics", Anıl, Jain; Ruud, Bolle and Sarath, Pankanti (Ed.), *Biometrics Personal Identification in Newyork Society*, Kluwer Academic Publishers, pp.1-41.

Jain, Anil K., Ross, Arun, Prabhakar, Salil, (2004), "An Introduction to Biometric Recognition" Invited Paperformation, *IEEE Transactions on Circuits and Systems for Video Technolog*, Vol.14, No.1, pp.4-20.

Jain, Anil K. and Demirkus, Meltem, (2008), "On Latent Palmprint Matching", *MSU Technical Report.*

Jali, Mohd, Zalisham; Steven M. Furnell, and Paul, S. Dowland, (2014), "Investigating the Viability of Multifactor Graphical Passwords for User Authentication", *Information Security Journal: A Global Perspective.*

Kanak, Alper, (2013), *Biyometrik Güvenlik Sistemlerinde Mahremiyet, Güvenlik ve Güven İlişkisinin Modellenmesi,* Gebze İleri teknoloji Enstitüsü, Mühendislik ve Fen Bilimleri Enstitüsü Yayınlanmamış Doktora Tezi, Gebze.

Karadaş, Kürşat, (2014), *Biyometrik Sistem İle İnsan Profil Resmi Üzerinden Kulak Bölgesinin Tespiti Ve Cinsiyet Belirleme*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Karakülah, Makbule; Danacı, Mustafa ve Ciritci, İbrahim Hakkı, (2004), "Biyometrik Parmak İzinin Akıllı Kartlarla Kullanımı ve Uygulaması", *Pamukkale Üniversitesi Mühendislik Fakültesi, Mühendislik Bilimleri Dergisi*, Cilt: 10, Sayı: Özel; ss.13-16.

Karasar, Niyazi, (2009), *Bilimsel Araştırma Yöntemi*. Ankara: Nobel Yayın Dağıtım.

Karasartova, Suikum, (2011*), Metinden Bağımsız Konuşmacı Tanıma Sistemlerinin İncelenmesi Ve Gerçekleştirilmesi,* Ankara Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Kardaş, Geylani, Çelikel, Ebru ve Alaybeyoğlu Ayşegül, (2008), "Bilgisayar Ağlarında Güvenli Mesajlaşma İçin Akıllı Kart Destekli Bir Sistem Mimarisi", *Pamukkale Üniversitesi Mühendislik Fakültesi, Mühendislik Bilimleri Dergisi*, Cilt: 14, Sayı: 1; ss.31-40.

Kholmatov, Alisher, (2008), *Privacy Protecting Biometric Authentication Systems*, Sabanci University, Doctora of Phylosophy.

Koçer, Hasan Erdinç, (2007), *İris Deseninin Yapay Zeka Yöntemleri ile Tanınması*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Yayınlanmamış Doktora Tezi, Konya.

Kumar, Amıoy ve Ajay, Mundra, Tanvır, Singh, (2009), "Anatomy Of Hand" Stan Z.Li (ed.), (2009), *Encyclopedia Of Biometrics*, Springer Publishers, pp.28-35.

Laux, Dawn, Andy, Luse, Brian, Mennecke and Anthony, M. Townsend, (2011), Adoption of Biometric Authentication Systems: Implications for Research and Practice in the Deployment of End-User Security Systems, *Journal of Organizational Computing and Electronic Commerce,* 21:3,pp. 221-245.

Nabiev, Vasif V., (2009), "Kulak Biyometrisine Göre Kimlik Tespiti", *2. Mühendislik ve Teknoloji Sempozyumu*, 30 Nisan - 1 Mayıs 2009 / Çankaya Üniversitesi / Ankara.

Nardo, Joseph V. Di, (2008), Biometric Technologies: Functionality, Emerging Trends, and Vulnerabilities, *Journal of Applied Security Research*, 4:1-2, pp.194-216.

Özkaya, Necla ve Sağıroğlu, Şeref, (2012), *Açık Anahtar Yapısı ve Biyometrik Teknikler,* ueimzas.gazi.edu.tr/pdf/poster/78.pdf.

Palombo, Lara, (2011), Biometrics: Bodies, technologies, biopolitics, Social Identities: *Journal for the Study of Race, Nation and Culture*, 17:5, pp.717-720.

Ploeg, Irma van der, (2003), "Biometrics and Privacy A note on the politics of theorizing technology", *Information, Communication and Society*, 6:1, pp.85-104.

Rençber, Eda, (2011), *Akıllı Yöntemler İle Konuşmacı Tanıma*, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

Richards, Donald R., (1997), "Biometric Identification", *Information Systems Security*, 6:2, pp.28-44.

Robb, Drew, (2002), Biometrics Technology Comes of Age, *EDPACS: The EDP Audit, Control, and Security Newsletter,* 29:12, pp.12-20.

Rukhin, Andrew L., (2004), "The Recognition Problem of Biometrics", *CHANCE*, 17:1, pp.30-34.

Seyal, Afzaal H. ve Rodney, Turner, (2013), A study of executives' use of biometrics: an application of theory of planned behaviour, *Behaviour and Information Technology*, 32:12, pp.1242-1256.

Singleton, Tommie, (2003), Biometric Security Systems: The Best Infosec Solution?, *EDPACS: The EDP Audit, Control, and Security Newsletter*, 30:9, pp.1-24.

Şahin, Bahattin, (2012), *Biyometrik Verilerin Pasaport Ve Sınır Kapılarında Uygulanması Ve Bir Model Önerisi*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Şamlı, Rüya ve Yüksel, M. Erkan, (2009), "Biyometrik Güvenlik Sistemleri", *Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri* 11-13 Şubat 2009 Harran Üniversitesi, Şanlıurfa.

Şen, Osman Nihat, (2012), *Göç Kontrol Mekanizması Olarak Biyometrik Sistemlerin Etkinliği: Avrupa Birliği Ve Amerika Birleşik Devletleri Uygulamalarının Türkiye'ye Etkisi*, Polis Akademisi Güvenlik Bilimleri Enstitüsü Uluslararası Güvenlik Anabilim Dalı Yayınlanmamış Doktora Tezi.

Tilki, Özcan, (2014), *Pca Based Face Recognition: An Application*, Çankaya University Graduate School Of Natural And Applied Sciences Computer Engineering, Master Thesis.

Uzun, Mehmet, Semih, (2006), *Akıllı Kart Teknolojisiyle Geliştirilmiş Elektronik Pasaport ve Vize Sistemi*, Yıldız Teknik Üniversitesi Fen Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Vacca, John R., (2007), *Biometric Technologiesand Verification System.*, Elsevier İnc.

Varlık, Abdullah, (2008), *Dijital Fotogrametri Teknikleri İle Kişi Tanıma*, Selçuk Üniversitesi Fen Bilimleri Enstitüsü Doktora Tezi, Konya.

Varol, Asaf ve Cebe, Betül, (2011), "Yüz Tanıma Algoritmaları", *5th International Computer and Instructional Technologies Symposium*, 22-24 September 2011, Fırat University, Elazığ

Whiter Biometrics Comittee (2010), *Biometrics Recognition*::Challenges and Opportunities, National Academies Press.

Yağcıoğlu, Mustafa, (2008), *Comparıson Of 3D Facial Anchor Point Localization Methods*, Master Degree Department of Electrical and Electronics Engineering, Middle East Technical University

Yıldız, B. ve Tenekecioğlu, B., (2004), Entelektüel Sermayenin İşletmelerin Piyasa Değeri Üzerindeki Etkisi ve İMKB100 İşletmelerinde Görgül Bir Çalışma., *3. Ulusal 17 Bilgi, Ekonomi ve Yönetim Kongresi*, ss. 579-590, Eskişehir.

Yosuntaş, Çiğdem, (2008), *Sahte Kimlik*, Beykent Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Zunkel Richard L., (2002), "Hand Geometry Based Verification", Anıl Jain, Ruud Bolle and Sarath Pankanti (Ed.), *Biometrics Personal Identification in Newyork Society*, Kluwer Academic Publishers, pp.87-101

EKLER

EK-1. Kamuda Güvenlik Amaçlı Kullanılan Biyometrik Sistemlere İlişkin Görüşleri İçeren Anket Formu.

Sayın,

Bu anket bir yüksek lisans tez çalışması olarak güvenliği sağlamaya yönelik kullanılan biyometrik sistemlerin karşılaştırılması amacıyla hazırlanmıştır. Bu çalışma sonucunda elde edilecek bulgular, birey ve kurumları deşifre etmeden bilimsel yayınların hazırlanmasında kullanılacaktır. Lütfen her maddeyi dikkatlice okuduktan sonra, düşüncelerinizi en doğru biçimde yansıtacak cevaplar veriniz ve yanıtsız ifade bırakmayınız.

Yardımlarınızdan dolayı teşekkür ederim.

Tanyel YÜCEL
Polis Akademisi
Güvenlik Bilimleri Enstitüsü
Yüksek Lisans Öğrencisi

A) KİŞİSEL BİLGİLER

1.) Göreviniz (iş yerindeki pozisyonunuz) : …….

2.) Cinsiyetiniz:

☐ Kadın ☐ Erkek

3.) Yaşınız:……

4.) Kaç yıldır bu kurumda çalışıyorsunuz?…….

5.) Eğitim düzeyiniz:

☐ İlkokul ☐ Ortaokul ☐ Lise ☐ Üniversite ☐ Lisans Üstü

6.) Biyometrik sistemlerle ilgili bilgi düzeyinizi nasıl değerlendiriyorsunuz?

Bilgim yoktur							Bilgiliyim
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

7.) Kamuda, biyometrik sistemlerin kullanılmasını ne derece gerekli görüyorsunuz?

Gerekli değil							Gerekli
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

B) KULLANILAN BİYOMETRİK SİSTEM HAKKINDA GENEL BİLGİLER

8.) Kurumunuzda hangi biyometrik sistem kullanılmaktadır?

☐ Parmak izi ☐ Yüz tanıma ☐ İris tanıma ☐ El geometrisi ☐ Diğer (……)

9.) Kurumunuzda kullandığınız biyometrik sistemi güvenirlik bakımından nasıl değerlendirirsiniz?

Güvenilir değil							Güvenilir
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

10.) Kurumunuzda kullanılan biyometrik sistemin giriş ve çıkışlarda harcanan vakit yönünden verimliliğini nasıl değerlendirirsiniz?

Verimsiz							Verimli
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

11.) Kurumunuzda kullanılan biyometrik sisteminin varlığı kendinizi güvende hissetmenizde ne derece etkilidir?

Etkisiz							Etkili
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

12.) Görev yaptığınız süre içerisinde kurumunuzda kullanılan biyometrik sistem daha önce farklı bir sistemle değiştirildi mi?

☐ Evet ☐ Hayır

13.) 12. Soruya cevabınız **Evet** ise değiştirilme sebebini açıklayınız.

……
……
……
……
……
……
……

14.) Sizce Biyometrik Sistem binanın güvenliği sağlamaya ne derece yeterlidir?

Yeterlsiz							Yeterli
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

15.) Kurumunuzdaki mevcut sistemin kullanımını, öğrenilebilirlik bakımından nasıl değerlendirirsiniz?

Zor							Kolay
☐	☐	☐	☐	☐	☐	☐	
1	2	3	4	5	6	7	

16.) Mevcut sistem şifre hatırlama zorunluluğunu ortadan kaldırmaya ne derece etkilidir?

Etkisiz ☐ ☐ ☐ ☐ ☐ ☐ ☐ Etkili
1 2 3 4 5 6 7

17.) Mevcut sistem kart taşıma zorunluluğunu ortadan kaldırmaya ne derece etkilidir?

Etkisiz ☐ ☐ ☐ ☐ ☐ ☐ ☐ Etkili
1 2 3 4 5 6 7

18.) Kurumunuzdaki biyometrik sistemi, kullanılabilirlik yönünden nasıl değerlendirirsiniz?

Zor ☐ ☐ ☐ ☐ ☐ ☐ ☐ Kolay
1 2 3 4 5 6 7

19.) Kurumunuzda, biyometrik sistemin kullanılmasını ne derece gerekli görüyorsunuz?

Gerekli değil ☐ ☐ ☐ ☐ ☐ ☐ ☐ Gerekli
1 2 3 4 5 6 7

20.) Herhangi bir zamanda başka bir güvenlik sistemi ile ilgili deneyiminiz oldu mu? Olduysa bu sistem ile mevcut sistemi;

A) Kullanılabilirlik yönünden karşılaştırabilir misiniz?
……
……
……
……
……
.....

B) Güvenlik yönünden karşılaştırabilir misiniz?
……
……
……
……
……
.....
.....
.....

21.) Kurumunuzda kullanılan biyometrik sisteminin güvenlik yararları konusunda düşünceleriniz nelerdir?

……
……
……
……
……
……
……
……
.

22.) Sizce biyometrik sistemin **<u>olumlu yanları</u>** nelerdir?

……
……
……
……
……
……
……
……
……
……
……
……
……

23.) Sizce biyometrik sistemin **<u>olumsuz yanları</u>** nelerdir?

……
……
……
……
……
……
……
……
……
……
……
……
……

24.) Kurumunuzdaki biyometrik sistemin güvenlik dışında başka hangi amaçlar için kullanıldığını düşünüyorsunuz?

……
……
……
……
……
……
……

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	**:**Tanyel YÜCEL
Doğum Yeri	**:**Lefkoşa
Mesleği	**:**Polis Mensubu/Kriminalistik Uzman

Eğitim Durumu

Lisans Öğrenimi	**:**Doğu Akdeniz Üniversitesi
Bildiği Yabancı Diller	**:**İngilizce

İş Deneyimi

Stajlar	**:**Ankara Kriminal Polis Laboratuarı
Çalıştığı Kurumlar	**:**Polis Genel Müdürlüğü(KKTC)

İletişim

E-Posta	**:**tanyel_yucel@hotmail.com
Tel.	**:**03927143836
Tarih	**:**