

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PARMAK DAMAR TANIMA TEKNOLOJİSİ

YÜKSEK LİSANS TEZİ

Songül ŞAN

Tez Danışmanı: Prof. Dr. Asaf VAROL

Anabilim Dalı: Elektronik ve Bilgisayar Eğitimi

Programı: Bilgisayar Sistemleri

ELAZIĞ, 2013

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PARMAK DAMAR TANIMA TEKNOLOJİSİ

YÜKSEK LİSANS TEZİ

Songül ŞAN
(092131103)

Tezin Enstitüye Verildiği Tarih: 28.01.2013

Tezin Savunulduğu Tarih: 15.02.2013

Tez Danışmanı : Prof. Dr. Asaf VAROL

Diğer Jüri Üyeleri : Yrd. Doç. Dr. Resul DAŞ

Yrd. Doç. Dr. Ferhat BAHÇECİ

ELAZIĞ, 2013

ÖNSÖZ

Parmak içindeki damarların dağılım görüntüsü, her insan için farklıdır. Parmak Damar Tanıma Sistemi bu temel üzerinden hareket ederek, parmak damar görüntüsünü elde eden ve bu görüntüyü kullanarak kimlik doğrulama ve tanıma yapan bir biyometrik sistem olarak gün geçtikçe hızla gelişmektedir. Günümüzde parmak damar tanıma sistemi için geliştirilmiş birçok cihaz mevcuttur. Bu çalışmadaki genel amaç biyometrik sistemlerin araştırılıp, bu sistemler için tasarlanan cihazların çalışma mekanizmaları hakkında fikir sahibi olabilmektir.

Songül ŞAN
ELAZIĞ-2013

TEŞEKKÜR

Yüksek lisans çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından desteklenen ve “**Parmak Damar Tanıma Teknolojisi**” adını taşıyan TEKF.11.03 nolu proje kapsamında tamamlanmıştır. FÜBAP'a sağladığı finansal katkıdan ötürü teşekkür ederim.

Ayrıca çalışmam esnasında her türlü bilgiyi, desteği ve yardımlarını esirgemeyen değerli hocam Prof. Dr. Asaf VAROL'a teşekkürü bir borç bilirim.

İÇİNDEKİLER

	<u>Sayfa No</u>
ÖNSÖZ.....	II
TEŞEKKÜR.....	III
İÇİNDEKİLER.....	IV
ÖZET	VI
SUMMARY.....	VII
ŞEKİLLER LİSTESİ.....	VIII
TABLolar LİSTESİ.....	X
KISALTMALAR LİSTESİ.....	XI
1. GİRİŞ	1
1.1. Tez Çalışmasının Amacı	2
1.2. Tez Çalışmasının Kapsamı.....	2
2. BİYOMETRİK SİSTEMLER	3
2.1. Biyometrinin Tarihi.....	3
2.2. Biyometrinin Amacı.....	4
2.3. Biyometrik Sistemlerin Özellikleri	4
2.4. Biyometrik Sistem Çeşitleri	6
2.4.1. Parmak İzi Tanıma	6
2.4.2. El Geometrisi Tanıma	7
2.4.3. DNA Tanıma.....	8
2.4.4. Retina Tanıma	9
2.4.5. Yüz Tanıma.....	9
2.4.6. Ses Tanıma	16
2.4.7. Yüz Termogramı	17
2.4.8. İris Tanıma	17
2.4.9. Damar Tanıma.....	18
2.4.10. İmza Atımı	19
2.4.11. Yürüyüş.....	20
2.4.12. Tuş Vuruşu.....	20
2.5. Biyometrik Sistemlerin Çalışma Mekanizması.....	21
2.6. Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması	22

2.7.	Biyometrik Sistemlerin Kullanım Alanları	24
2.8.	Literatür ve İlgili Çalışmalar	24
2.9.	Çoklu Biyometrik Sistemler	26
2.9.1.	Parmak İzi İle Tümlleşik Parmak Damar Çoklu Biyometrik Sistem	27
3.	PARMAK DAMAR TANIMA SİSTEMİ	29
3.1.	Parmak Damar Görüntülerinin Toplama Süreci	31
3.2.	KFV-100 Parmak Damar Tanıma Cihazı	32
3.2.1.	KFV-100 ve RFID Modül (FeliCa veya MIFARE) Özellikleri	33
3.3.	Parmak Damar Uzman Sistemin Hazırlanması	34
4.	SONUÇ VE ÖNERİLER	37
	KAYNAKLAR	39
	EKLER	41
	ÖZGEÇMİŞ	50

ÖZET

Teknolojideki hızlı gelişmeler, insanlığı hem olumlu hem de olumsuz yönde etkileyebilmektedir. Özellikle siber ortamlarda işlenen suçların artmasıyla dünyada bilgi güvenliği konusunda önemli güvenlik çalışmalarının yapılmasına itmiştir. Bu nedenle günümüzde birçok şirket ve kurum güvenliklerini korumak amacıyla biyometrik tanıma sistemlerinden yararlanmakta ve bu cihazları kullanmaktadır.

Literatürdeki çalışmalara göre parmak içerisindeki damarların dağılım görüntüsü, her insan için farklıdır. Parmak Damar Tanıma Sistemi bu temel özellik üzerinden hareket ederek, parmak damar görüntüsünü elde eden ve bu görüntüyü kullanarak kimlik doğrulaması ve tanınması yapabilen bir biyometrik sistem olarak gün geçtikçe hızla gelişmektedir.

Bu tez çalışmasının genel amacı, geliştirilen bir uzman sistem yazılımı sayesinde, otomasyona girilen her parmak damar görüntüsünün sistemde kayıtlı bulunan diğer parmak damar görüntüleriyle karşılaştırılarak, güvenliği sağlamaktır.

Anahtar Kelimeler: Biyometri, Parmak Damar, Parmak Damar Tanıma Sistemi

SUMMARY

FINGER VEIN IDENTIFICATION TECHNOLOGY

Rapid advances in technology can affect the humanity both positively and negatively. Especially crimes occurred in cyber environment raise concern about information security. For this reason, many companies and institutions around the world utilize and use of biometric recognition systems and tools.

According to the studies in the literature, distribution of blood vessels in the fingers is unique for each person. Therefore, Finger Vein Recognition System, which uses the image of the obtained images of finger vein to authenticate and recognize as a biometric system, is rapidly evolving day by day.

The general purpose of this study is to generate a user authentication expert system to compare each input by the user with the stored finger vein images in the repository to provide secure access to a system.

Keywords: Biometrics, Finger Vein, Finger Vein Recognition System

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 1. Bir Parmak İzi Örneği.....	7
Şekil 2. El Geometrisi ve Görüntünün Alınması	8
Şekil 3. Yüz Tanıma Sistemi.....	10
Şekil 4. Biyometrik Fotoğraf Şablonu	11
Şekil 5. ICAO Standartlarına Göre Biyometrik Fotoğrafın Yüz Hatları	12
Şekil 6. ICAO Standartlarına Göre Biyometrik Fotoğrafın Resim Kalitesi	12
Şekil 7. ICAO Standartlarına Göre Biyometrik Fotoğrafın Yüz Hatları	12
Şekil 8. ICAO Standartlarına Göre Biyometrik Fotoğrafın Saçlar ve Bakışın Yönü	13
Şekil 9. ICAO Standartlarına Göre Biyometrik Fotoğrafta Başın Pozisyonu ve Yüz İfadesi	13
Şekil 10. ICAO Standartlarına Göre Biyometrik Fotoğrafta Fon	13
Şekil 11. ICAO Standartlarına Göre Biyometrik Fotoğrafta Işık	14
Şekil 12. ICAO Standartlarına Göre Biyometrik Fotoğrafta Gözlükler	14
Şekil 13. ICAO Standartlarına Göre Biyometrik Fotoğrafta Küçük Çocuklar	14
Şekil 14. ICAO Standartlarına Göre Biyometrik Fotoğrafta Şapka vb. Aksesuarlar	15
Şekil 15. ICAO Standartlarına Göre Biyometrik Fotoğrafta Baş Örtüsü	15
Şekil 16. Ses Tanıma.....	16
Şekil 17. Yüz Termogramı.....	17
Şekil 18. Gözün Yapısı	17
Şekil 19. El Damar Görüntüsü	19
Şekil 20. Bir İmza Örneği	20
Şekil 21. Stephenson Kelimesinin Yazılış Ritmine Ait Gösterim	21
Şekil 22. Kullanılan Teknolojiye Göre Market Yüzdeleri.....	23
Şekil 23. Parmak İzi İle Tümüleşik Parmak Damar Kimlik Doğrulama Sistemi Blok Diyagramı....	28
Şekil 24. Parmak Damar Tanıma Sistemi ve Çalışma Mekanizması.....	29
Şekil 25. Parmak Damar Modelinin Görüntüsü.....	30
Şekil 26. Uygulamada Kullanılan Bazı Parmak Damar Görüntüler	31
Şekil 27. KfV-100 Cihazı.....	32
Şekil 28. KfV-100 Cihazına Parmağın Yerleştirilmesi.....	34
Şekil 29. KfV-100 Cihazının Parmak Damar Haritasına Göre Şifre Oluşturma Süreci	34
Şekil 30. Parmak Damar Görüntüsü	35

Şekil 31. Parmak Damar Görüntüsünün İskeleti.....	35
Şekil 32. Uygulamanın Matlab Arayüzü.....	36

TABLÖLAR LİSTESİ

	<u>Sayfa No</u>
Tablo 1. Biyometrik Tanıma Sistemlerinin Çeşitlerinin Taradıkları Özellikler.....	5
Tablo 2. Biyometrik Teknolojilerin Karşılaştırılması	5
Tablo 3. Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması.....	23
Tablo 4. KfV-100 Cihazının Özellikleri	33

KISALTMALAR LİSTESİ

INCITS	: International Committee for Information Technology Standards (Uluslararası Bilgi Teknolojileri Standartları Komitesi)
OPTS	: Otomatik Parmak İzi Tanıma Sistemi
ICAO	: International Civil Aviation Organization (Uluslararası Sivil Havacılık Organizasyonu)
DNA	: Deoksiribonükleik Asit
PCR	: Polymerase Chain Reaction (Polimeraz Zincirleme Tepkimesi)
CCD	: Charge-Coupled Device (Şarj Kuplajlı Cihaz)
ATM	: Automatic Teller Machine (Otomatik Vezne Makinesi/Bankamatik)
LED	: Light Emitting Diode (Işık Yayan Diyot)

1. GİRİŞ

Herhangi bir bilginin gizliliğinden, dolayısıyla 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 çıkabilir. Özellikle tıp ya da savunma sanayi gibi sektörlerde çok önemli boyutlarda kayıptan bahsedilmek zorunda kalınabilir.

Bilgi güvenliği için kullanılan kimlik doğrulama işlemi genel olarak bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç farklı şekilde incelenebilir. Bu çalışmanın konusu biyometrik temelli güvenlik sistemleridir [1].

Bilgi temelli kimliklendirme, kullanıcıların ve söz konusu sistemi yöneten kişi veya kişilerin belirli bilgilere sahip olmasını gerektirir. Bu bilgiler, kullanıcı adı ve şifre olabileceği gibi, pin olarak ifade edilen numara dizileri de olabilir. Bu tür sistemlerde kullanıcılar ve kullanıcılara karşılık gelen bilgiler (şifre, pin vs) bir veritabanında tutulur. Kullanıcılar bilgilerini sisteme girdiklerinde veritabanında karşılaştırma yapılır. Eğer karşılaştırma sonucu birbirini tutuyorsa, doğru kullanıcı olduğu anlaşılır ve söz konusu kullanıcının sisteme giriş yapmasına ve sistemde yetkisi dâhilindeki işlemleri gerçekleştirmesine izin verilir. Bu tip sistemlerin en önemli dezavantajı, kullanıcının şifre-pin bilgilerini unutmasının ya da bu bilgilerin bir başkası tarafından elde edilmesinin kolay oluşudur.

Kimlik doğrulamanın diğer bir çeşidi olan aidiyet temelli kimliklendirmede; kullanıcılar kendileri ile eşleşen bir objeye sahiptirler. Bu obje genelde manyetik kart, rozet veya anahtardır. Söz konusu sisteme giriş, kullanıcılar tarafından bu objeler kullanılarak yapılır. Objenin içerisinde sisteme giriş yapanın kim olduğunu belli edecek ve kimlik doğrulaması yapacak bilgiler mevcuttur. Bu çeşit sistemlerde de kişinin söz konusu objeyi unutması, kaybetmesi, çaldırması ihtimali bir dezavantaj oluşturmaktadır.

Biyometrik temelli kimliklendirme sistemlerinde kullanıcı sisteme kendisine ait olan ve üzerinde her daim taşıdığı parmak izi, iris, ses, el geometrisi, yüz gibi bir fizyolojik özelliğini veya imza atış, yürüyüş gibi bir davranışsal özelliğini kullanarak giriş yapar. Kullanıcı bu şekildeki bir sisteme giriş yapmak istediğinde, sistem tarafından kullanıcının uygun biyometrik bilgisi (parmak izi, retina, ses retina) alınır. Alınan bu bilgi aynı kişiden

alınıp veritabanına kaydedilmiş biyometrik bilgi ile karşılaştırılır. Karşılaştırma sonucu doğru ise kişinin kimlik doğrulanması gerçekleştirilmiş olur [1].

1.1. Tez Çalışmasının Amacı

Bu tez çalışmasında bilgi güvenliği için kullanılan kimlik doğrulama yöntemlerinden olan biyometrik sistemlerden biri olan Parmak Damar Tanıma Sistemi ele alınmıştır. Literatürde yapılan araştırmalar sonucunda insanlardaki bazı biyolojik özelliklerin eşsiz olduğu ortaya çıkmıştır. Bu özellikler DNA, retina, iris, parmak izi, damar görüntüleri, yüz şekli gibi. Parmak Damar Tanıma Sistemi de kişilerin parmak damar görüntülerinin birbirinden farklı olması baz alınarak kimlik doğrulama yöntemlerinden biri olarak güvenlik sistemlerinde kullanılmaktadır.

1.2. Tez Çalışmasının Kapsamı

Tezin ilk bölümünde teze genel bir bakış kazandırmak amacıyla, tezin amacı ve kapsamından bahsedilmektedir. İkinci bölümde literatür araştırmaları sonucunda biyometrik sistemlerin tarihi, amacı ve biyometrik sistemlerin çeşitleri hakkında detaylı teorik bilgi verilecek, üçüncü bölümde literatürde var olan parmak damar tanıma yöntemleri incelenmiştir. Ayrıca, Hong Kong Politeknik Üniversitesi Parmak Görüntüleri veritabanından indirilen parmak damar görüntüleri incelenmiştir. Dördüncü bölümde ise yapılan çalışmalar neticesinde sonuç ve öneriler tartışılmıştır.

2. BİYOMETRİK SİSTEMLER

Biyometri, biyolojik verileri, yani bireyin kişisel bir nitelik ya da davranışını analiz ederek kimliğini doğrulama bilimidir. Hayatımızda büyük önem taşıyan biyometrik tabanlı doğrulama güvenilir kimlik doğrulaması için güçlü bir yöntemdir. Günümüzde biyometri giderek daha popüler hale gelmektedir.

Biyometrik sistem, bireyin bir niteliğini ya da davranışını tarayarak daha önce oluşturulan kayıt ile karşılaştırır. Bu sistem, bireyin parmak izini, elini, avuç içini, retinasını ya da sesini incelediğinden, aşırı hassas olmalıdır. Bireyin anatomik ya da fizyolojik niteliklerini ölçerken doğru ve birbirini tekrar eden ölçümler yapılmalıdır [4].

2.1. Biyometrinin Tarihi

Yüzyılımıza damgasını vurmuş olan bilgi teknolojilerinin bir ürünü olan biyometrik sistemlerin temel prensiplerinin anlaşılması ve uygulanması aslında çok öncelere dayanmaktadır. Binlerce yıl önce Nil Vadisi'nde yaşayan insanlar biyometrik tanımlamayı birçok günlük iş süresince rutin bir şekilde kullanmışlardır.

19. yüzyılda kriminoloji araştırmacılarının fiziksel özellikler ve karakteristiklerin kriminal eğilimlerle bir ilgisinin olup olmadığını araştırmaları, bu alana olan ilgiyi arttırmıştır. Bu araştırmalar sonucunda birçok ölçüm aleti üretilmiş ve birçok veri toplanmıştır. Sonuçlar her ne kadar kesin olmasa da bireylerin fiziksel özelliklerinin ölçülmesi kabul görmüş ve parmak izi uygulaması polis tarafından kimlik tespitinde kullanılan uluslararası bir yöntem olmuştur [2].

2.2. Biyometrinin Amacı

Biyometri uygulayıcılarının genel amacı kişilerin kimliklerini doğrulayabilmeleri için, akıllarında tutmaları gereken herhangi bir bilgi ya da yanlarında taşımak, kaybetmemek ya da unutmamak zorunda oldukları kart, anahtar gibi araçların yerine; kopyalanması ya da taklit edilmesi imkansız olan özelliklerini kullanmalarını sağlamaktır. Biyometrik sistemlerde, kimlik belirleme işlemi, kişilerin fiziksel ya da davranışsal özelliklerine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir. Diğer yöntemlere göre çok daha az riske sahiptir. Ancak biyometrik sistemlerin oluşturulabilmesi için bazı standart ölçüler kullanılmalıdır. Biyometrik ölçüler olarak adlandırılan bu ölçülerin şifrelerde kullanımı için INCITS (International Committee for Information Technology Standards-Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur [3].

2.3. Biyometrik Sistemlerin Özellikleri

Birçok yeni teknolojinin geliştirilmesinde olduğu gibi biyometrinin de gelişiminde güvenlik unsuru öncülük etmiştir. Tüm biyometrik sistemler aşağıda açıklanmış olan beş özelliğe sahip olmalıdır [4]:

1. Evrensellik: Tüm bireylerin biyometrik özelliklere sahip olmasıdır.
2. Eşsiz olma: Biyometrik karakteristiğin her insanda farklı bir şekilde yer almasıdır.
3. Süreklilik: Karakteristiğin zamanla değişmemesidir.
4. Elde edilebilirlik: Biyometrik özelliklerin bazı pratik cihazlarla ölçülebilir olmasıdır.
5. Kabul edilebilirlik: Bireylerin biyometrinin ölçüm ve toplanmasında itirazları olmamalıdır.

Biyometrik tanıma sistemlerinin çeşitlerinin taradıkları özellikler Tablo 2.3.1’de, biyometrik teknolojilerin karşılaştırılması Tablo 2.3.2’de verilmiştir [4].

Tablo 1. Biyometrik Tanıma Sistemlerinin Çeşitlerinin Taradıkları Özellikler

Biyometrik karakteristik	Özelliklerin açıklaması
Parmak İzi	Parmak satırları, gözenek yapısı
İmza Tanıma	Basınç ve hız ile yazma farkları
Yüz geometrisi	Göz, burun vs arası uzaklıklar
İris Tanıma	İris deseni
Retina	Retina yapısına (desenine) göre
El Geometrisi	Parmak ve avuç içi ölçülerine göre
Parmak geometri	Parmak ölçme
El Damar yapısı	Elin arkası, parmak veya avuç içi damar yapısı
Kulak formu	Kulağın belirgin boyutları
Ses	Ton ya da ses rengi
DNA	Kalıtsal bir taşıyıcı olan DNA
Koku	Kokunun kimyasal bileşimi
Klavye vuruş	Klavye vuruşlarının ritmi (PC veya diğer klavye)

Tablo 2. Biyometrik Teknolojilerin Karşılaştırılması

Biyometrik Karakteristikler	Evrensellik	Eşsizlik	Süreklilik	Elde Edilebilirlik	Performans	Kabul Edilebilirlik	Yaygınlık
DNA	Yüksek	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük
Kulak	Orta	Orta	Yüksek	Orta	Orta	Yüksek	Orta
Yüz	Yüksek	Düşük	Orta	Yüksek	Düşük	Yüksek	Yüksek
Yüz Termogramı	Yüksek	Yüksek	Düşük	Yüksek	Orta	Yüksek	Düşük
Parmak İzi	Orta	Yüksek	Yüksek	Orta	Yüksek	Orta	Orta
El Geometrisi	Orta	Orta	Orta	Yüksek	Orta	Orta	Orta
İris	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Düşük
Retina	Yüksek	Yüksek	Orta	Düşük	Yüksek	Düşük	Düşük
İmza	Düşük	Düşük	Düşük	Yüksek	Düşük	Yüksek	Yüksek
Ses	Orta	Düşük	Düşük	Orta	Düşük	Yüksek	Yüksek
Damar	Yüksek	Orta	Orta	Orta	Yüksek	Orta	Düşük

2.4. Biyometrik Sistem Çeşitleri

Biyometrik yöntemler, insanların fiziksel veya davranışsal özelliklerini kullanarak kimlik tespiti yapmayı sağlayan yöntemlerdir. Günümüzdeki mevcut biyometrik tanıma yöntemleri şunlardır [5]:

Fizyolojik özelliklere dayalı olan biyometrik tanıma sistemleri:

1. Parmak İzi Tanıma
2. El Geometrisi Tanıma
3. DNA Tanıma
4. Retina Tanıma
5. Yüz Tanıma
6. Ses Tanıma
7. Yüz Termogramı
8. İris Tanıma
9. Damar Tanıma

Davranışsal özelliklere dayalı olan biyometrik tanıma sistemleri:

1. İmza Atımı
2. Yürüyüş
3. Tuş Vuruşu
4. Konuşma

2.4.1. Parmak İzi Tanıma

Parmak izi yüz yılı aşkın süredir kullanılan, taklit edilemeyen bir kimlik belirleme tekniğidir. Tek yumurta ikizleri de dahil olmak üzere; her insanın parmak izinin farklı oluşu, yıllarca değişmemesi, kolay kullanımı ve gelişen yeni teknolojiler bu tekniğin yaygın kullanımını sağlamıştır [19]. İlk kullanılmaya başlandığı yıllardan bu yana gerek yazılım gerekse donanım alanında parmak izi sistemlerinde önemli ilerlemeler kaydedilmiştir. Bir otomatik parmak izi tanıma sisteminde (OPTS) parmak izi tanıma genellikle parmak izinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır.

Bir OPTS’de gerçekleştirilen işlemler aşağıda verildiği şekilde sıralanabilir [20]:

1. Parmak izlerinin alınıp sayısalaya çevrilmesi,
2. Parmak izinde bilgi taşıyan, üzerinde işlem yapılacak kısmın arka plandan

ayrılması,

3. Referans noktaların elde edilmesi,
4. Parmak izinin temizlenip iyileştirilmesi,
5. Resmin ikili resme çevrilmesi,
6. İkili resmin inceltilmesi,
7. Özellik noktalarının ve bu noktaların parametrelerinin bulunması,
8. Yalancı özellik noktalarının elimine edilmesi,
9. Karşılaştırma işleminin gerçekleştirilmesi,
10. Sistemin başarısının değerlendirilmesi.



Şekil 1. Bir Parmak İzi Örneği

Bu sistemlerin en önemli dezavantajı, parmak izinin taklit edilmesi durumunda sistemin yanılabilmesidir. Diğer bir dezavantaj bazı kişilerin pek çok sebepten ötürü (organ eksikliği, yanma, deri hastalıkları) parmak izlerinin bulunmamasıdır. Parmak izi taklit problemi, parmak izinin alındığı parmağın canlılığını test edecek gelişmiş algılayıcıların (sensörlerin) kullanılması ile giderilebilir. Kişide parmak izinin bulunmaması durumunda (örneğin bir yangın sonrasında el derisinin soyulması ve izlerin kaybolması hali), parmak izi tespiti yapılamaz [6].

2.4.2. El Geometrisi Tanıma

El geometrisi tanıma Amerika’da 20 yıldan beri kullanılan, özellikle havaalanları ve nükleer güç istasyonlarında tercih edilen bir yöntemdir. Şekil 2’de gösterildiği gibi bu yöntemde kişilerin elinin veya iki parmağının geometrik yapısı analiz edilir. Parmakların uzunluğu, genişliği, eni ve büküm yerleri ayırt edici özellikler olarak kullanılmaktadır.

El geometrisi tanıma yüksek doğruluk oranına sahip bir yöntem olmakla birlikte büyük ve ağır okuma cihazı nedeniyle maliyet ve kullanım açısından dezavantajlara sahiptir.



Şekil 2. El Geometrisi ve Görüntünün Alınması

Resmin alınma süresinin uzun oluşu da sistemi yavaş yapan bir etmendir. Ayrıca yüzük, yara bandı gibi araçlar, yaralanma ve parmakların kaybedilmesi, gut veya kireçlenme gibi bir takım hastalıklar nedeniyle sistem performansı düşmekte, çocuklarda ise ellerin çok hızlı büyüyüp gelişmesinden dolayı sistem hemen hemen hiç kullanılamamaktadır [6].

2.4.3. DNA Tanıma

Deoksiribonükleik Asit yapısının kişiye özgü bir karakteristik olduğu ilk olarak 1985 yılında keşfedilmiştir. DNA tanıma günümüzde en güvenilir kimlik doğrulama yaklaşımlarından biridir ve en çok babalık testleri ve adli işlemlerde kullanılmaktadır. DNA tanıma saç, kan ve diğer biyolojik materyaller incelenmektedir. Yöntemde hücre nükleuslarındaki kromozomlarda saklanan DNA molekülleri kullanılmaktadır. Her bir DNA molekülü 4 kimyasal birim içerir. Bunlar: Adenin (A), Guanin (G), Sitozin (C) ve Timin (T) olarak sıralanabilir. Bu yapılar şeker molekülleri ve fosfat grupları ile birlikte pozisyon ve diziliş açısından genetik bilginin kodlandığı çatıyı oluştururlar. Tandem tekrarlama olarak bilinen A, G, C, T yapılarının aynı ardışık dizilişlerinin oluşturduğu tekrar yapısı, tekrar sayısı ve miktarının değişimi kişiye özgüdür. Tek yumurta ikizleri buna istisnadır. DNA tanıma gerçekleştirilen işlemler aşağıda verildiği şekilde sıralanabilir:

1. DNA örneğinin alınması.
2. DNA'nın izole edilmesi.

3. Polimeraz zincir tepkimesi (PCR) kullanılarak enzimatik sınırlama ve yükseltmenin gerçekleştirilmesi.
4. Parçaların ayrılması.
5. Tekrar yapılarının vs. bulunması.
6. Elde edilen sonuçların analiz edilmesi.

Doğruluğu çok yüksek bir yöntem olmasına rağmen diğer biyokimyasal ve kimyasal analizlerde olduğu gibi DNA analizinde de yöntemin doğruluğu örnek kalitesine bağlıdır. Örneklerin karışması, kirletilmesi, kemik iliği nakli gibi durumlarda yöntemin başarısı düşmektedir. DNA analizi diğer biyometrik teknikler ile karşılaştırıldığında maliyeti yüksektir. Ayrıca işlem süresinin 24 saat gibi bir zaman gerektirmesi de bu yöntemi gerçek zamanlı kimlik kontrolünün gerektiği durumlarda elverişsiz hale getirmektedir. Son yıllarda gündeme gelen DNA çipler ve mikro diziler ile bu yöntemin elverişsiz özellikleri ortadan kaldırılacaktır [7].

2.4.4. Retina Tanıma

Bir optik alıcı vasıtası ile retinanın benzersiz şablonlarının düşük yoğunluklu bir ışık kaynağı ile taranmasına dayalı yerleşmiş bir teknolojidir. Kararlılığı kanıtlanmış bir teknik olmasına rağmen, kullanıcının bir noktaya sabit bakmasını gerektirmektedir. Eğer gözlük kullanıyorsa ya da okuyucu ile göz temasına girmekten endişe duyuluyorsa, pek güvenilir bir yöntem değildir. Bu nedenlerden ötürü retina taramasının kullanıcılar tarafından kabullenilmesi zor olmakla birlikte teknoloji oldukça verimli çalışmaktadır. Doksanlı yılların ortalarında yeniden tasarımı son haline gelmiş olup gelişmiş bağlanılabilirlik ve kullanıcı arabirimi sağlamaktadır, ama yinede marjinal bir biyometrik teknoloji olarak görülmektedir [13].

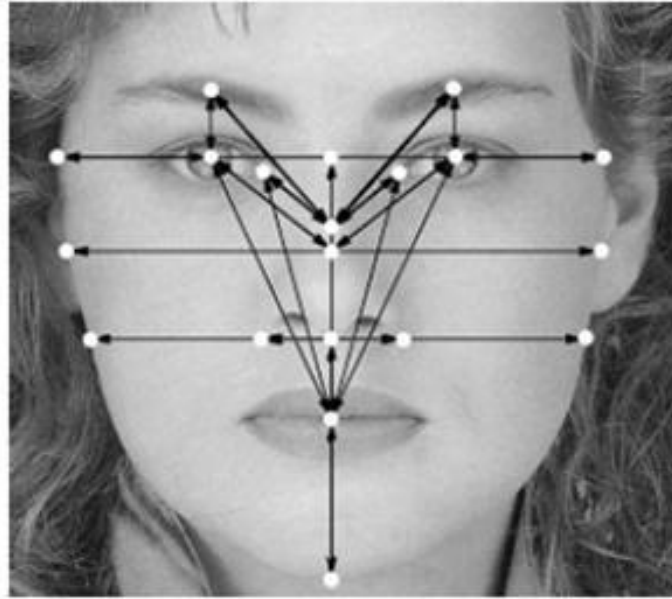
2.4.5. Yüz Tanıma

Yüz tanıma sistemi aslında en doğal biyometrik ayırt edici yöntemdir. İnsanlar birbirlerini ayırt etmede yüzlerinden faydalanırlar. Bu sebeple bu yöntem neredeyse insanlık tarihiyle yaşıt bir biyometrik ayırt etme yöntemidir. Buna rağmen bu yöntemin bilimsel olarak incelenerek bir ayırt edici özellik olarak bilgisayarlarda kullanılması oldukça yeni sayılabilecek bir konudur. Bir suçluyu tanımlamada polis tarafından

kullanılan yöntem örnek verilebilir. Suçluyu anlatan insana suçlu hakkında sorular sorup yüz şeklinin belirlenmesine çalışmaktır. Bu konuda polis ressamlarının standart olarak daha önce çizdikleri bazı yüz parçaları vardır. Verilen tarife göre bu parçalar bir araya getirilerek suçlunun yüz şekline yakın bir yüz şekli bulunmaya çalışılır. Bilgisayarların hayatın içerisindeki hızlı kullanımı yüz tanıma yöntemleri konusunda da oldukça ilerlemeler sağlanmasına neden olmuştur. Günümüzde yüz tanımlama konusunda kullanılan iki yöntem vardır. Bunlar;

1. Yüz Metriği Yöntemi
2. Eigenfaces Yöntemi (Yüz Parçaları)

Yüz Metriği Yönteminde, Şekil 3'teki gibi yüz üzerinde yerleşik olan organlar arasındaki mesafeler ölçülerek bunlardan bir matematik ifade çıkarılmaya çalışılır. Örneğin gözler arasındaki mesafe ağız ve burun arasındaki mesafe vb.

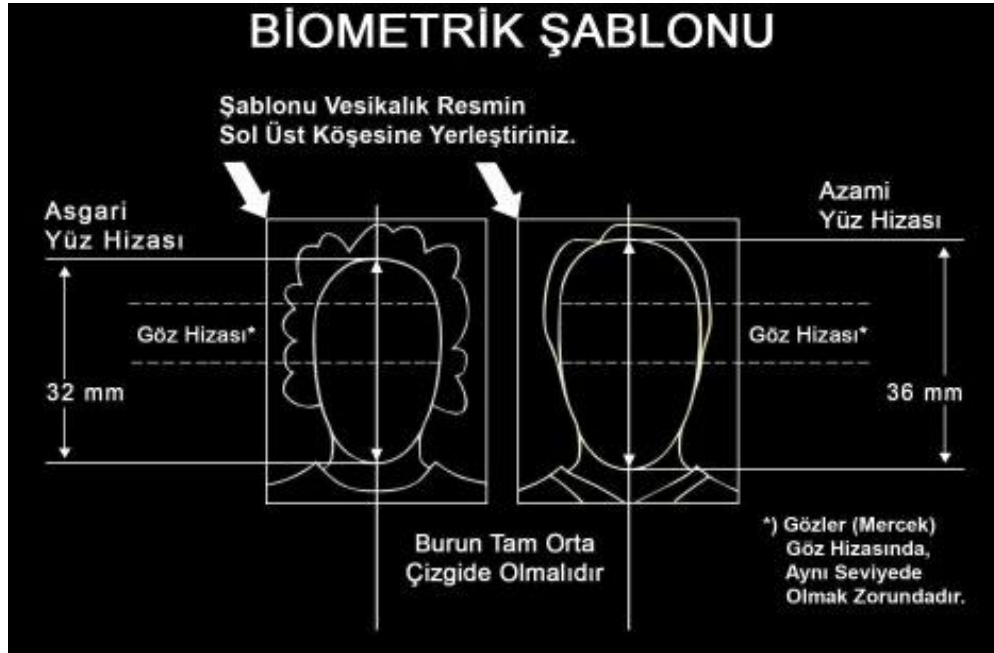


Şekil 3. Yüz Tanıma Sistemi

Eigenfaces Yönteminde ise polis ressamının yaptığına benzer bir yöntem uygulanır. Yüz 150 parçaya bölünür. Bu 150 parçadan 40 tanesinin belirleyiciliği diğer parçalardan daha fazladır. İlk etapta bu 40 parçadan başlayarak yüz tanımlama işlemine geçilir. Böylece yüz tanımlanmaya çalışılır. Bu yöntem yüz metriği yöntemine göre yeni bir yöntemdir ve hala test aşamasındadır. Araştırmacılar tarafından geliştirilmektedir [10].

2.4.5.1. Biyometrik Fotoğraf

Biyometrik fotoğraf, ülkerin vize başvuruları ve pasaportlar için büyükelçilikler, konsolosluklar veya başkonsolosluklar tarafından istenen, standartları ICAO tarafından belirlenen ve Makinede Okunabilen Seyahat Belgelerinde kullanılan yüksek kaliteli, belli ölçüleri ve özellikleri olan vesikalık fotoğraftır [23]. Biyometrik fotoğraf, Şekil 4'te yer alan, ebatları 3,5 cm x 4,5 cm olarak belirlenmiştir. Hemen hemen tüm fotoğrafçılarda biyometrik vesikalık çekirmek mümkündür. e-Pasaportlarda yüz, parmak izi ve göz bebeği olmak üzere üç tür biyometrik veri kullanılmaktadır. Biyometrik özelliklere sahip pasaportlarda kan grubundan parmak izine ve surat yapısına kadar birçok bilgi chip ile kodlanmıştır.



Şekil 4. Biyometrik Fotoğraf Şablonu [22].

ICAO Standartlarındaki Biyometrik Vesikalık Fotoğraflar İçin Aranılan Özellikler [23]:

1. Yüz Hatları

Yüz, fotoğraf üzerinde ortalanmış olarak saç modeliyle birlikte tamamen görünür olmalıdır.



Şekil 5. ICAO Standartlarına Göre Biyometrik Fotoğrafın Yüz Hatları

2. Resim Kalitesi

Fotoğrafta leke ve bükülmeler olmamalıdır. Renkler nötr olmalı ve yüzün doğal renklerini yansıtmalıdır.



Şekil 6. ICAO Standartlarına Göre Biyometrik Fotoğrafın Resim Kalitesi

3. Keskinlik ve Kontrast

Kontrast iyi ayarlanmalı, ayrıntılar yeterince keskin ve net olmalıdır.



Şekil 7. ICAO Standartlarına Göre Biyometrik Fotoğrafın Yüz Hatları

4. Saçlar ve Bakışın Yönü

Gözler açık konumda olmalı ve net olarak görünmelidir. Saçlar gözleri kapatmamalı ve fotoğraf çekilirken doğrudan kameraya bakılmalıdır.



Şekil 8 . ICAO Standartlarına Göre Biyometrik Fotoğrafın Saçlar ve Bakışın Yönü

5. Başın Pozisyonu ve Yüz İfadesi

Başın konumu dik olmalı, baş herhangi bir yöne dönük olmamalıdır. Fotoğraf gülme vb. mimikler olmadan, ağız kapalı olarak çekilmelidir.



Şekil 9. ICAO Standartlarına Göre Biyometrik Fotoğrafta Başın Pozisyonu ve Yüz İfadesi

6. Fon

Fon beyaz ve desensiz olmalıdır. Fonda gölgeler oluşmamalıdır.



Şekil 10. ICAO Standartlarına Göre Biyometrik Fotoğrafta Fon

7. Işık

Işık yüze eşit ölçüde yansıtılmalı, yansıma veya gölgeler bulunmamalıdır. Fotoğrafta "kırmızı-göz" bulunmamalıdır.



Şekil 11. ICAO Standartlarına Göre Biyometrik Fotoğrafta Işık

8. Gözlükler

Gözler net bir şekilde görünmeli, gözlük camı üzerinde yansımalar bulunmamalı, renkli cam veya güneş gözlüğü kullanılmamalıdır. Gözlük camının kenarı veya çerçevesi gözleri kapatmamalı ya da gözleri kapatacak ölçüde kalın olmamalıdır.



Şekil 12. ICAO Standartlarına Göre Biyometrik Fotoğrafta Gözlükler

9. Küçük Çocuklar

Küçük çocukların fotoğraflarında başka kişi veya nesneler bulunmamalıdır.



Şekil 13. ICAO Standartlarına Göre Biyometrik Fotoğrafta Küçük Çocuklar

10. Şapka vb. Aksesuarlar

Kişinin zorunlu olarak kullandığı gözlük ve benzeri aksesuarlar dışında fotoğrafta şapka, başlık, pipo, vb. nesneler bulunmamalıdır.



Şekil 14. ICAO Standartlarına Göre Biyometrik Fotoğrafta Şapka vb. Aksesuarlar

11. Baş Örtüsü

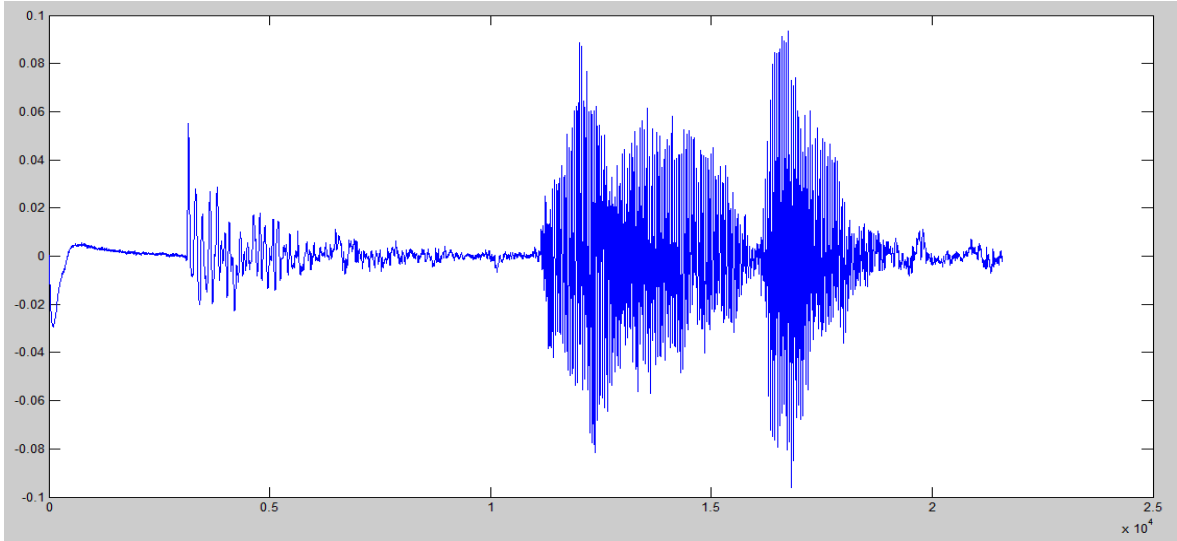
Başörtülü fotoğraflarda yüz çene ucundan alına kadar görünür olmalı, yüzün üzerinde gölgeler oluşmamalıdır.



Şekil 15. ICAO Standartlarına Göre Biyometrik Fotoğrafta Baş Örtüsü

2.4.6. Ses Tanıma

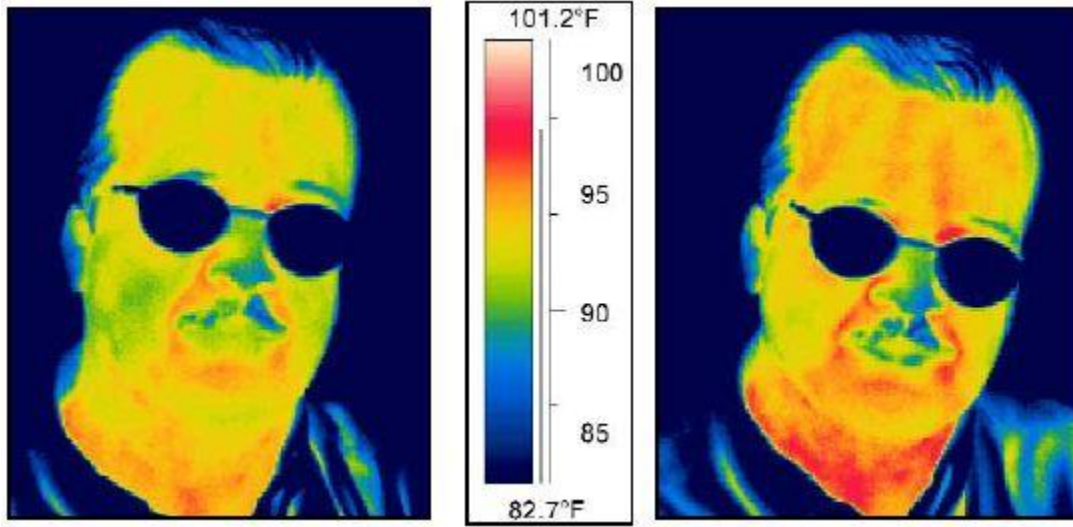
Bir ses tanıma uygulamasında, sinyallerin tanınabilmesi için öncelikle doğru şekilde ifade edilmeleri gereklidir. Diğer bir deyişle, incelenen ses sinyalinin içinde barındırdığı ve yalnızca tanınması hedeflenen sese ait unsurlar, çeşitli sayısal sinyal işleme teknikleri peş peşe uygulanarak belirlenir. Daha sonra belirlenen unsurların bir öznitelik vektörü ile ifade edilmesi gerekir. Bu öznitelikler ile ses tanıma veri tabanı oluşturulur. Veri talebi sırasında kullanıcı tarafından sisteme sunulan örüntü, veri tabanındaki kayıtlardan birisi ile eşleştirilmeye çalışılır. Eşleştirme işleminin sonucu, sistemin nihai karar mekanizmasına aktarılır ve yetki talebi olumlu ya da olumsuz olarak belirlenir [11].



Şekil 16. Ses Tanıma

2.4.7. Yüz Termogramı

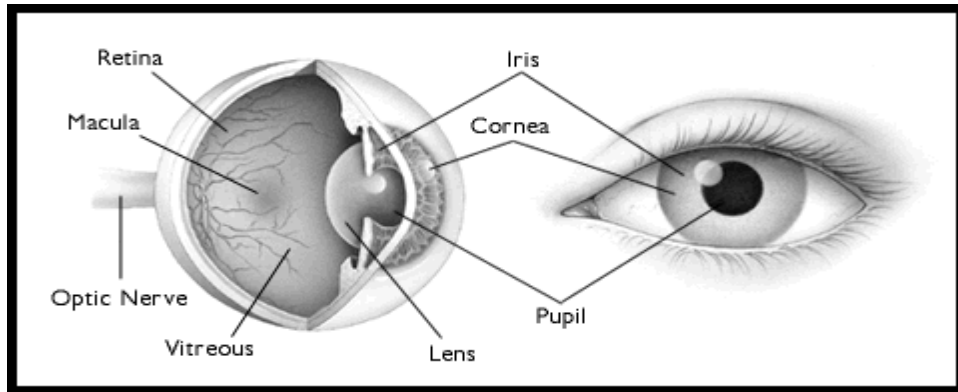
Yüzün ısı haritasının analizi yapılarak kimlik tespiti ve doğrulama işlemlerinde kullanılan biyometrik yöntemlerden biridir. Bu konuda araştırmalar hala devam etmektedir.



Şekil 17. Yüz Termogramı

2.4.8. İris Tanıma

İris tarama, biyometrik taramalar içerisinde en basit olanlarından biridir. Sıradan bir CCD kamera kullanılarak yaklaşık 15-20 cm uzaklıktan tarama yapılabilmektedir. Kullanıcı ile tarayıcı arasında fiziksel temas olmasına gerek yoktur. Gözlükle bile kullanılabilmesi, sistemlere kolay entegre olabilmesi ve iris deseninin en güvenilir desenlerden biri olması, iris tarama sistemlerini daha çok tercih edilir hale getirmektedir. Şekil 18'de insan gözünün anatomik yapısı görülmektedir.



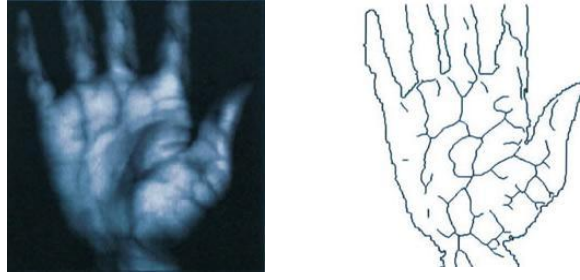
Şekil 18. Gözün Yapısı [12].

Son yıllarda iris tanıma sistemi, diğer sistemlere göre daha güvenilir, uygulaması kolay ve güncelliği her geçen gün artan bir sistem olma özelliğindedir. Bunun sebepleri:

- İris yapısal olarak anne karnında 3. ayda oluşmaya başlamakta, 8. ayda oluşumunu tamamlamakta ve doğumdan sonra 2-3 yıl içinde de tam gelişimini bitirmektedir. Bundan sonra iris, yapı olarak değişikliğe uğramamaktadır.
- Son yıllardaki araştırmalar göstermiştir ki, iris de parmak izi gibi kişi tanımlamada kullanılabilecek ayırt edici özelliğe sahiptir.
- İrisin oluşumu embriyonun gelişimine bağlı olduğu için, genetik yapıya bağlı değildir. İris yapısı, ikizler de bile değişiklik gösterdiği gibi aynı kişinin sağ ve sol gözündeki iris yapıları bile farklı olduğundan dolayı, tanıma için daha ayırt edici özelliğe sahiptir. Bu nedenle, iris tanıma sistemlerinde kişiler sistemin çalışma prensibine göre, ya hep aynı gözle sisteme tanıtılmakta ya da kişinin her iki gözü de sisteme kayıt edilmektedir.
- Gözde bulunan iris, kornea, gözkapığı ve gözbebeği tarafından korunmaktadır. Bu nedenle dış etkilere en az etkilenebilecek özelliktedir.
- İrisin yapısı cerrahi müdahaleyle bile değiştirilememektedir.
- İris tanıma sistemi kişiye zarar vermez. Lazer ya da benzeri görüntü alma tekniklerine ihtiyaç duymadan basit bir CCD kamera ile görüntü alınabilmektedir [12].

2.4.9. Damar Tanıma

Avuç içi damar tanıma teknolojisi, avuç içinde bulunan kan damarlarının her insanda farklı olmasından yola çıkılarak keşfedilmiş bir teknolojidir. Bu teknolojiye ilk olarak algılayıcı (sensör) tarafından kan damarlarına infrared ışık gönderilerek damar yapısı ortaya çıkarılır. Damar yapısının ortaya çıkmasında, kanda bulunan hemoglobinin gönderilen kızılötesi (infrared) ışığı soğurması ilke edinilmiştir. Damar tanıma teknolojisinde kandaki hemoglobin kullanıldığından dolayı tanımlama yapılan uzvun canlı olması, damar içinde kan bulunması önem kazanmakta ve teknolojiye katma değer katmaktadır. Algılayıcı görevi gören IR kamera sayesinde elde edilen görüntü, biyometrik api sayesinde yine algılayıcı üzerinde sayısal bir değere dönüştürülür. Sonrasında bu sayısal değer, 256 bit AES (Advanced Encryption Standart) algoritmasıyla şifrelenerek güvenli veri iletişimi için sunucu/istemci bilgisayarlara iletilir.



Şekil 19. El Damar Görüntüsü

Palm (Avuçici) Damar tanıma teknolojisinin, diğer teknolojilere göre en büyük avantajı elin kesilmesi, zedelenmesi durumlarında damar yapısı etkilenmeyeceği için çalışmaya devam etmesidir [14].

Avuçici damar teknolojisinin başlıca kullanım alanları aşağıdaki gibidir:

- ATM Cihazları
- Medikal Tanımlama (SGK, Hastane, Eczane...)
- Geçiş Kontrolü
- Personel Devam Kontrolü
- Web Tabanlı Kimlik Uygulamaları
- Sistem Oturum Açma İşlemleri
- Bankacılık İşlemleri

2.4.10. İmza Atımı

Bir kişinin, herhangi bir yazının altına söz konusu bu yazıyı yazdığını, okuduğunu veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işaretler olarak tanımlanabilen imza kişiler tarafından yaşamları boyunca pek çok kez kullanılmaktadır. Özellikle hukuksal açıdan büyük yaptırımlarının bulunması ve taklit edilmesi sonucunda kişiyi borç altına sokabilmesi, tüm malvarlığını başka bir kimseye bağışlamasına sebep olması, işlemediği suçların üzerine kalmasına neden olması gibi sebeplerle hayatı önem taşımaktadır. Dolayısıyla kimlik doğrulamasında belki de en sık kullanılan yöntem olan imzanın gerçekten o kişi tarafından atılıp atılmadığının belirlenmesi önemli bir sorun olarak karşımıza çıkmaktadır. Bu sebeple kullanılan imza tanıma sistemlerinde imzayı tanımak için iki tip bilgi kullanılmaktadır. Bunlardan ilki imzalama süresi, hızı, ivmesi, kalemin basım şiddeti gibi kişinin imzalama işlemi ile ilgili özellikler, diğeri ise bir desen

olarak imzaya ait özelliklerdir. Bir imzayı taklit eden herhangi bir kişi desen olarak imzayı taklit edebilse bile imza atış şeklini (süre, ivme, kalemi yerden kaldırma miktarı vs) tekrarlaması güçtür.



Şekil 20. Bir İmza Örneği

İmza tanıma sistemlerinin dezavantajları, sistemin kullanıcının hızını ve imza atma davranışını öğrenebilmesi için uygun sayıda örneğe ihtiyaç duyması ve imza atımının kullanıcının o anki ruh haline, özellikle de acelesi olup olmadığına bağlı olarak değişmesidir [6].

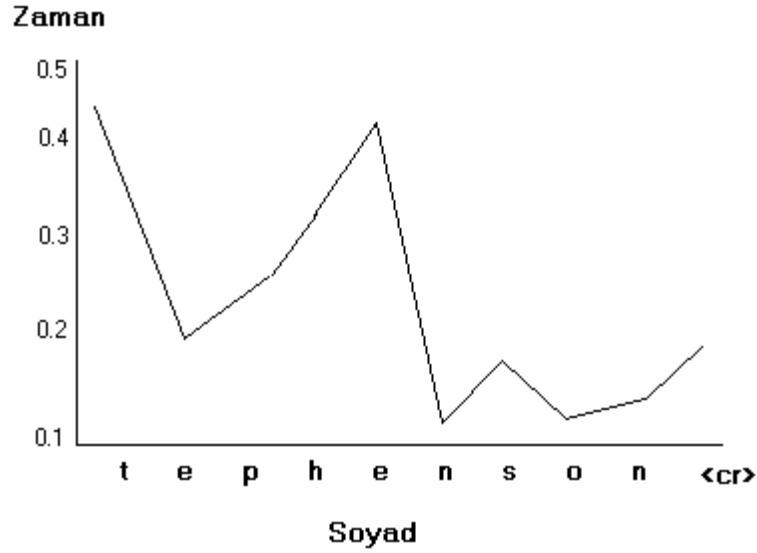
2.4.11. Yürüyüş

Kişilerin yürüyüş şekline göre kimlik doğrulamasında kullanılan biyometrik yöntemlerden biridir. Literatürde bu konuda yapılmış çalışmalara pek yer verilmemiştir.

2.4.12. Tuş Vuruşu

Diğer biyometrik sistemlerin en büyük dezavantajlarından birinin bütün terminallerde kullanılmak üzere ekstra donanım gereksinimi olmalarının yanı sıra, yazma ritmi sistemlerini diğer biyometrik sistemlerden ayıran en temel özellik kendisine has özel bir donanıma ihtiyaç duymamasıdır. Bir Yazma Ritmi sistemi tasarlamak için ihtiyaç duyulan tek girdi aygıtı sadece klavyedir. Böyle bir avantaja sahip bir biyometrik sistemin gerçek hayatta kullanılmaması için hiç bir sebep yoktur. Özellikle üniversiteler gibi pek çok yerde bu tür bir sistem hem bilimsel hem de teknik manada rahatlıkla kullanılabilir. Çünkü insanların el yazıları gibi klavye yazış şekilleri arasında büyük bir benzerlik vardır. Gerçekten de bir insan klavye üzerinde bir şeyler yazmaya başladığında klavyede doğal olarak bilgisayar üzerinde bir iz bırakır. Yani kullanıcının klavyede karakterler üzerinde gezinmesi aslında onun gayet düzenli olarak yapmış olduğu bir yazma ritmi hareketine tekabül eder. Teorik olarak klavyeyi kullanarak bilgisayarda bir editöre bir kelime yazmak

istenildiğinde, kelime içerisinde yer alan harfleri yazarken geçen süre birbirine eşittir. Bir kullanıcıdan soyadı yazılması istenmiş ve yazılma aşamasında geçen süreler tespit edilmiştir. Stephenson kelimesi için geçen süreler ölçülmüş ve bu süreler için grafiği Şekil 21 'de gösterilmiştir.



Şekil 21. Stephenson Kelimesinin Yazılış Ritmine Ait Gösterim

Şekil 21'de kullanıcının yazma ritmi sistemine ait bulgular verilmektedir. Kullanıcı, t ve e karakterleri arasında oldukça zaman kaybederken n ve s ya da s ve o karakterleri arasında geçişi oldukça hızlı yapabilmektedir. Klavyeden girilen iki karakter arasında geçen zamanı ölçerek kullanıcıların yazma ritimlerini tespit etmeye çalışılmaktadır. Aslında yazma ritmiyle ilgili olarak birçok çalışmada ölçülen ve değerlendirilmeye çalışılan değer budur.

Yazma ritmi sistemlerinin en önemli dezavantajlarından birisi karar vermek için gerekli olan verilerin ancak tek bir parametreden, yani iki tuş arasındaki gecikme süresinden elde edilmesinden kaynaklanmaktadır. Sadece tuş aralıklarını değil, tuşlara basılırken geçen sürenin tespiti yazma ritmi çalışmalarında güvenilirlik oranını arttıracaktır [10].

2.5. Biyometrik Sistemlerin Çalışma Mekanizması

Bütün biyometrik teknolojiler, bilgi elde etme, özellik çıkartma, karşılaştırma ve uyuşma/uyuşmama olmak üzere dört adım olarak benzer şekilde çalışırlar. Bilgi elde etme aşamasında, sistem uygun teknik ile bir görüntü veya bilgi elde eder. Bilgi veya görüntü elde edildikten sonra, işleme aşamasıyla yerleştirilmelidir.

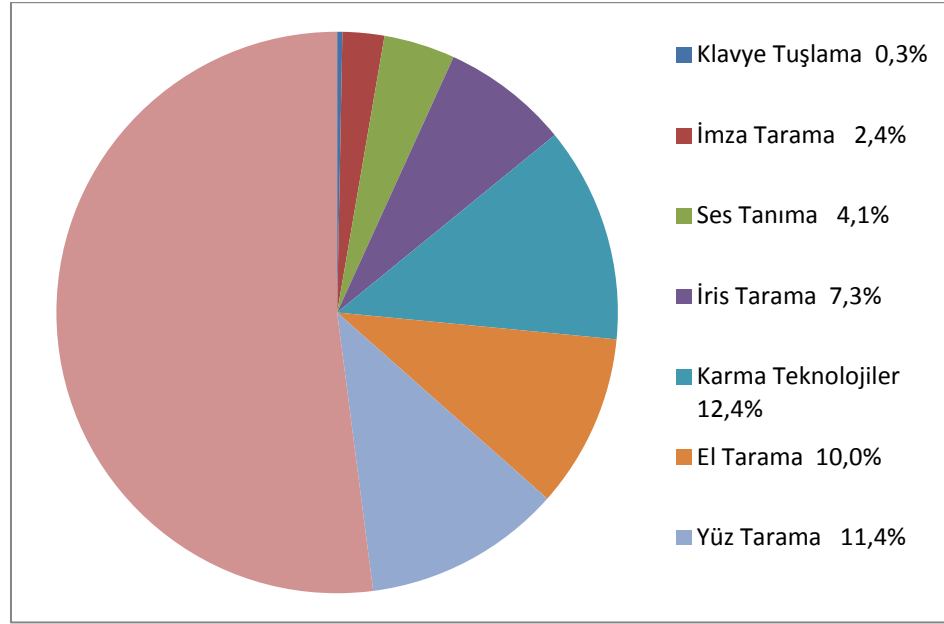
Yerelleştirme, özellik çıkartma aşamasında olur. Özellik çıkartma aşamasında, konuyla ilgisi olmayan enformasyon atılır ve ilgili olan enformasyon alınarak biyometrik şablon şeklinde saklanır. Bu tanıma işleminde, bir yeni bilgi/görüntü alınarak saklanan biyometrik şablon ile karşılaştırılır. Bu karşılaştırmanın sonucu, eğer yeni alınan bilgi şablon ile aynı ise uyuşma var, değil ise uyuşma yoktur sonucuna varılır [3].

2.6. Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

Kullanıcı kimliğini belirleyen diğer sistemler (bilgi temelli ya da aidiyet temelli) ile biyometrik sistemler benzer yönlelere sahip olmakla beraber birbirlerinden ayrıldıkları noktalar da oldukça çoktur. Biyometrik yöntemler dışındaki yöntemlerin biyometrik yöntemlere göre en önemli dezavantajı kullanıcıya bazı bilgileri bilme ve hatırında tutma ya da bazı araçları sürekli olarak yanında taşıma, çaldırmama, unutmama gibi sorumluluklar vermesidir. Biyometrik sistemlerde böyle bir durum söz konusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, nesneye vs ihtiyacı yoktur. Biyometrik sistemlerin diğer sistemlere göre avantajları, dezavantajları, benzer ve farklı yönleri kısaca aşağıdaki gibi ifade edilir [6].

- Diğer kimlik doğrulama yöntemlerinde kullanılan veri her kullanıcı için kesinlikle farklı ve eşsiz iken biyometrik veriler farklı olmakla beraber benzerliklere sahip olabilir.
- Diğer yöntemlerde kullanılan veri, kullanıcı tarafından değiştirilebilir (sistem yöneticisinin isteği üzerine, güncelleme amacıyla veya başka herhangi bir sebepten ötürü). Buna karşın biyometrik veri kişinin istemesi ile değiştirebileceği bir veri değildir, ancak kaza, hastalık vs geçirilmesi durumunda değişir.
- Biyometrik sistemler genelde ek bir donanım, yazılım gerektirdiğinden ek bir maliyet getirir iken, diğer yöntemler genelde kullanılan mevcut sistemlerle uyumludur.
- Diğer yöntemler çalındığı veya benzeri bir duruma uğradığı zaman yenisi ile değiştirilebilir, oysaki biyometrik veriler herhangi bir şekilde elde edildiğinde, geçerliliği kalmaz.
- Biyometrik veriler zaman içerisinde deformasyona uğrayabilir, buna karşın diğer yöntemler için böyle bir durum söz konusu değildir.

Biyometrik sistemler dışındaki tanıma sistemlerinde verinin unutulması, çalınması, kaybedilmesi riski oldukça fazladır. Ancak biyometrik sistemlerde kullanılan veri kişinin fiziksel ya da davranışsal bir özelliği olduğundan bu tarz bir tehlike ile karşı karşıya kalma ihtimali yok denecek kadar azdır. Şekil 22' de kullanılan biyometrik sistemlerin yüzdelik oranları yer almaktadır.



Şekil 22. Kullanılan Teknolojiye Göre Market Yüzdeleri [27].

Tablo 3. Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

Diğer Kimlik Doğrulama Yöntemleri	Biyometrik Yöntemler
Veri kaybı, çalınma, kaybetme tehlikesi büyüktür.	Veri kaybı, çalınma, kaybetme tehlikesi hemen hemen hiç yoktur.
Kullanıcı veriyi kişini istemesi halinde rahatlıkla değiştirebilir.	Biyometrik veri kaza, uzuv kaybı dışında değiştirilemez.
Herkes için kullanılabilir.	Herhangi bir biyometrik tarama sisteminde biyometrik özelliklere sahip olmayan (parmağı, gözü olmayan vb.) kişiler bu sisteme dahil edilmezler.
Zaman içinde değişiklik göstermesine sebep olacak bir durum söz konusu değildir.	Zaman içinde biyometrik veriler deformasyona, değişime uğrayabilir.
Genellikle mevcut sistemlere uyumludur.	Ek bir donanım maliyeti getirir.

2.7. Biyometrik Sistemlerin Kullanım Alanları

Günümüzde biyometrik sistemler aşağıda belirtilen alanlarda kullanılmaktadır:

- Personel devam ve takibi
- Otomatik para çekme makinelerinde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik saptama
- Havalimanlarında check-in ve boarding işlemleri
- On-line bankacılık kullanıcı tanımlama
- Sınır kontrolü ve sınır kapılarından girişlerin kontrolü
- İnternet bankacılığında kullanıcı tanımlama
- Elektronik para transferlerinde kullanıcı tanımlama
- Kredi kartı uygulamaları
- Kurumsal ağ
- Bilgisayar güvenliği
- Kiralık kasalara erişim güvenliği
- Satış noktası terminallerinde (POS) kullanıcı tanımlama
- Askeri kaynakların etkin takibi
- Çek onaylama işlemlerinde kullanıcı güvenliği
- Hastane ve sigorta kuruluşlarında hasta takibi ve kimlik saptama
- Kamu hizmetlerine yönelik kayıt takibi (SSK, vergi, trafik)
- Hesap açma işlemlerinde kimlik tespiti
- Binalara, tesislere ve ofislere erişim güvenliği
- Elektronik ticarete kullanıcı tanımlama
- Şube bankacılığı işlemlerinde kullanıcı tanımlama

2.8. Literatürde Biyometrik Sistemler

Teknolojinin gelişmesiyle beraber güvenlik vazgeçilmez unsurlar arasında yer almaya başlamıştır. Her türlü sistemin güvenliğini artırıcı yöntemler kullanılmakta ve alternatif çözüm arayışları devam etmektedir. Kişinin fiziksel özelliklerinin kimlik tespitinde kullanılması esasına dayanan biyometri teknolojileri, son yıllarda oldukça sık karşılaşılan güvenlik yaklaşımlarındandır [28].

Parmak izinin oldukça eski bir tarihi vardır. Nehemiah Grew (1684), Marcello Malpighi (1686) ve J. E. Purkinje (1823) adlı bilim adamları parmak izlerinin birtakım özellikler barındırdığına dikkat çekmiş olmalarına rağmen bu özelliklerin kişi tespitinde kullanacak kadar benzersiz olduğunu ortaya sürecektir herhangi bir çalışma yapmamışlardır. Günümüzde kullanılan yöntemlerin temeli olarak kullanılan parmak izi tanıma sistemlerinin temeli ise Henry Faulds ve Wiliam James Herschel adında iki İngilizin bilim adamının çalışmalarıyla başlamıştır. Bu iki bilim adamı kişilerin parmak izlerini alma yöntemleri üzerine çalışmışlar ve temel olarak mürekkep kullanımının üzerine gitmişlerdir.

Sir Francis Galton (1822-1911) istatistik üzerine yaptığı çalışmalar sonucunda iki bağımsız değişken arasındaki doğrusal ilişkinin yönünü ve kuvvetini belirten korelasyon (correlation) yöntemini ileri sürmüştür. Bu sayede iki örüntü (pattern) arasında karşılaştırma yapacak bir yöntem elde etmiştir. Çalışmalarının devamında insanların parmak izleri arasındaki farkı sınıflandırıp ayırt edecek yöntemler ortaya çıkarmıştır. Galton parmak izinin kalıtsal olmadığını ve her insanın parmak izinin birbirinden farklı olacağını çalışmalarıyla ortaya çıkarmıştır.

Galton'un çalışmalarını takiben Dr. Henry Faulds (1883-1930) parmak izinin sınıflandırılmasına tam olarak açıklık getirmiştir. Farklı sınıflandırma olsa bile Galton ve Henry'nin yaptığı çalışmaların ürünü olan sınıflandırma sistemi yaygın olarak kullanılmaktadır.

Günümüzdeki sistemlerde bu sınıflandırma genelde iki parmaktan alınan örnekler üzerinde gerçekleştirilmektedir. Tek parmaktan alınan bilgi ile de aynı işlem yapılabilir olmasına rağmen güvenlik ve stabil çalışma açısından en az iki parmak izi alınmaktadır. 25 Haziran 2007'de ABD'de sınır kapılarında bundan sonra iki değil on parmak izinin birden alınacağı bir sisteme geçileceğini açıklamıştır.

Ülkemizde parmak izinin incelenmesi ve biyometrik tanıma olarak kullanılması 1910 yılında Macar asıllı Yusuf Cemil tarafından başlatılmıştır. Daha sonra ise polis teşkilatı tarafından kullanılmıştır [21]. Kullanılan biyometrik sistemlerin belki de en önemlisi polis merkezlerinde, pasaport ve vize başvurularında (İngiltere 2007 yılından beri vize başvurularında, başvuran kişiden biyometrik veriler almaktadır. Keza Amerika Birleşik Devletlerine giriş yapıldığında da parmak izleri alınmaktadır) kullanılan parmak izi sistemleridir.

Kişi tanımlaması için iris kullanma düşüncesini ilk olarak ortaya atan Fransız göz doktoru Alphonse Bertillon'dur. 1981'de iki göz doktoru, Aran Safir ve Leonard Flom,

irisin, biyometrik sistemlerde kullanılabileceğini savunmuşlardır. 1989'da Cambridge Üniversitesi'nden Dr. John Daugman'ın öncülüğünde bir grupla birlikte Safir ve Flom, iris tanıma sisteminin algoritmasını geliştirerek, 1987'de bu düşüncenin patentini almışlardır. Grup, 1992'de iris tanıma üzerine ilk umut verici çalışmayı İngiltere'de gerçekleştirmişlerdir. Daugman dışında daha sonraları R.Wildes, W.Boles ve R.Sanchez-Reillo gibi bilim adamları da benzer sistemler üzerinde çalışmışlardır. 2000'li yıllardan sonra pek çok araştırmacı iris tanıma üzerine farklı çalışmalar yapmışlardır. Özellikle Çin'de çalışmalar artmıştır ve kurulan laboratuvarlar ile çalışmalarda kullanılabilecek hazır bir iris veritabanı oluşturmuşlardır. Yapılan bu sistemlerin tek farkı iris özelliklerini ayırt etmede kullanılan algoritmaların farklılığıdır [29].

El geometrisi tanıma, geliştirilen ilk biyometrik tanıma sistemidir ve ilk kez 20 yıl kadar önce Wall Street'te bulunan Shearson Hamill bankasında kullanılmıştır [30]. Günümüzde el geometrisi sistemleri geniş olarak kullanılmaktadır. 1996 yılında Atlanta Olimpiyat Köyü'ne giriş çıkışlarda bu sistem kullanılmıştır. San Francisco uluslararası havaalanında, Amerikan ordusunda, Amerika'daki nükleer santrallerin %90'ında, Kolombiya Meclisi'nde, hatta Georgia Üniversitesi'nin yurt yemek sisteminde el geometrisi sistemi kullanılmaktadır [30].

2.9. Çoklu Biyometrik Sistemler

Son yıllarda kişilerin yetkilendirilmesi için biyometrik özelliklerin birleştirilerek kullanıldığı çalışmalar revaçtadır [25]. Biyometrik özelliklerin birleştirilmesi, sistemin bozucu etkilere karşı daha güçlü olmasını, doğruluğunun ve güvenilirliğinin artmasını sağlamak ve kullanıcılara biyometrik sistemler bünyesindeki dezavantajları en aza indirgeyerek avantajları kullanma imkanı sunmaktadır. Tekli biyometrik sistemlere göre daha iyi performans, hız ve doğruluk sağlıyor olması bu konuda çalışan teknoloji üreticilerinin, algoritma geliştiricilerin ve bilim adamlarının dikkatini bu yöne yöneltmiştir. Çoklu biyometrik sistemlerin avantajları literatürde sıkça belirtilmektedir. Çoklu biyometrik sistemler incelendiğinde iki biyometrik özellik karar seviyesi, benzeşme oranları seviyesi ve özellik çıkarım seviyesi olmak üzere temelde 3 seviyede birleştirilmektedir [25].

1. Özellik çıkarım seviyesindeki birleştirmede her iki biyometrik özelliğin özellik seti farklı farklı elde edilip bu özellik setleri birleştirilmektedir.

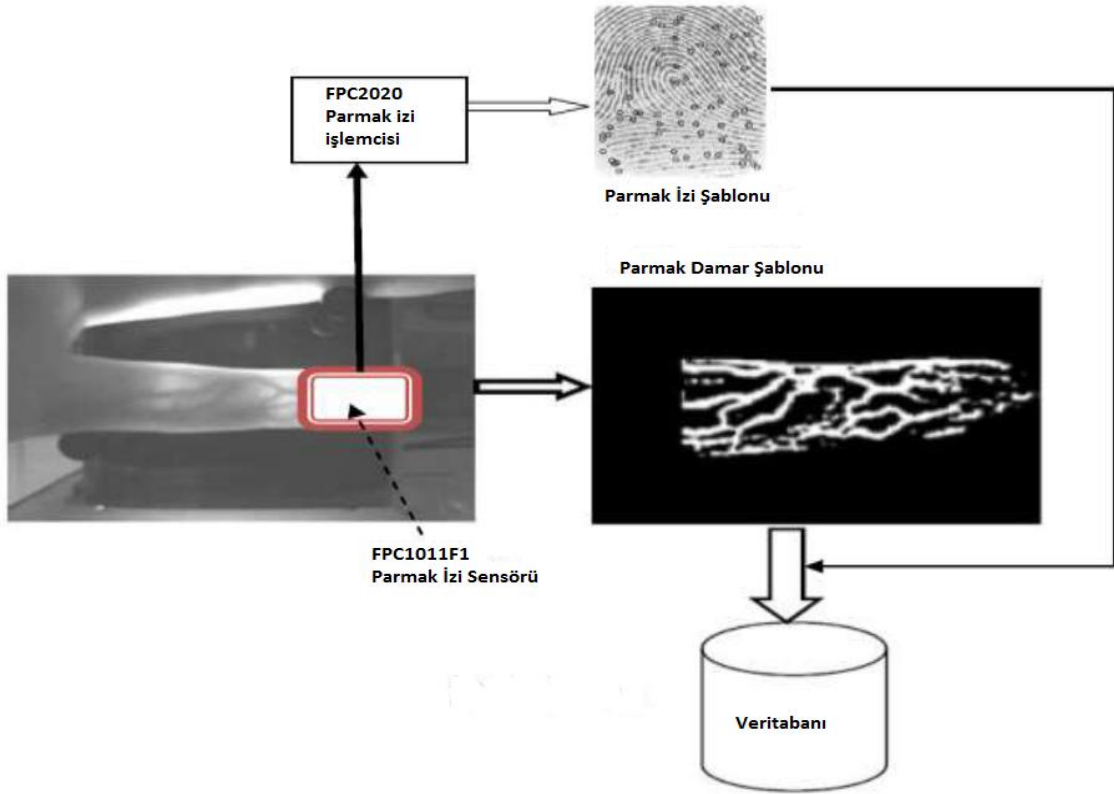
2. Benzeşme oranları seviyesindeki çoklu sistemde biyometrik özelliklerin ayrı ayrı özellik seti çıkarılıp benzeşme oranları hesaplanmakta ve bu aşamada birleştirme işlemi gerçekleştirilmektedir.
3. Karar seviyesinde ise her iki biyometrik özellik birbirinden bağımsız olarak işlemlere tabi tutulmakta sonuçta bir karar vermekte ve sonra bu kararlar birleştirilerek sistem sonucu oluşturulmaktadır.

2.9.1. Parmak İzi İle Tümlleşik Parmak Damar Çoklu Biyometrik Sistem

Sistemin tasarımı iki biyometrik tanımlayıcılar; parmak izi ve damar desenlerini içermektedir. Şekil 23'teki sistemde, FPC1011F1 parmak damar şablonu sensörü, FPC2020 parmak izi sensörü, şablonları depolama için bir harici bilgisayar gibi doğrudan bir arayüz ile bağlanmıştır [17].

LED'den yayılan Yakın Kızılötesi ışınım, parmak içine geçerek kandaki hemoglobin tarafından kısmen emilir. Işımların emildiği bölgeler (yani parmak içindeki kan damarları), parmağın diğer yüzünde konumlanmış kamera tarafından saptanan görüntüde karanlık bölgeler olarak görülür. Bu görüntü üzerinde görüntü işleme yöntemleri uygulanır ve bir parmak damarı motifi çıkarılır.

Parmak izi çukurcuklar ve tepeciklerden oluşmuştur. Bu oluşum genel olarak 5 ayrı şekilde sınıflandırılır. Bu sınıflandırma yapılırken parmak izi deseninde bulunan "core" ve "delta" adı verilen şekiller kullanılır. Parmak izi analizi yapılırken bu ayırıştırıcı noktaların X-Y koordinatları ile yönlerini belirtir açıları belirleyici rol oynar [26].



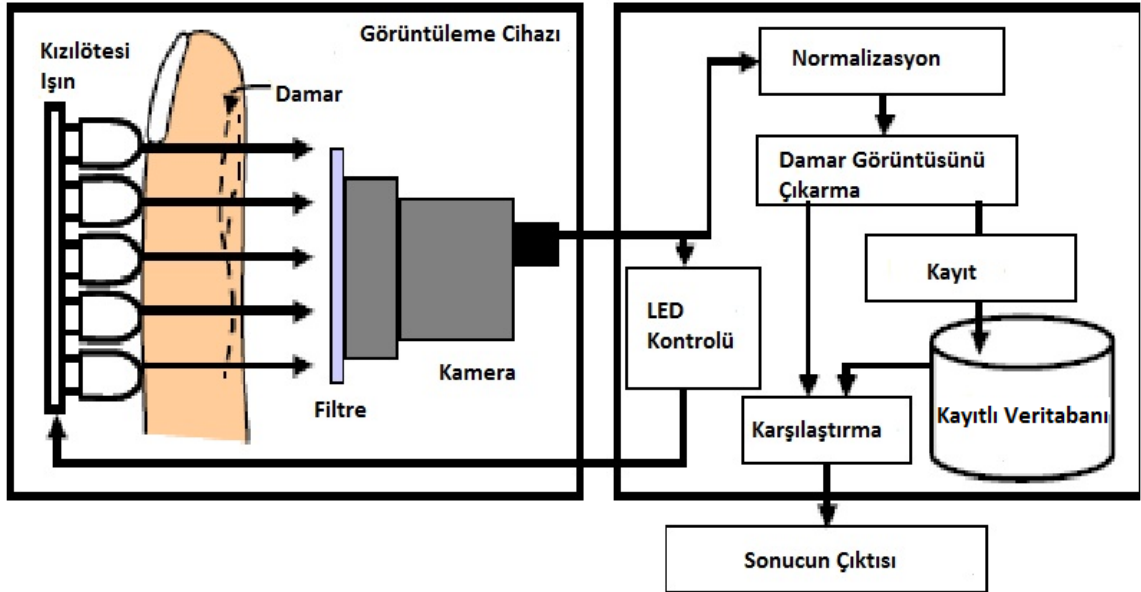
Şekil 23. Parmak İzi İle Tümüleşik Parmak Damar Kimlik Doğrulama Sistemi Blok Diyagramı [17].

Bu çoklu biyometrik sistemde FPC2020 işlemcisi ile parmak izi şablonu elde edilir. FPC1011F1 sensörü ile de parmağın damar şablonu elde edilir. Elde edilen bu şablonlar çeşitli algoritmalar ile sayısallaştırarak bir veritabanına kaydedilir. Sisteme giriş yapmak isteyen kişinin hem parmak izi hem de parmak damar deseni verileri alınıp veritabanındaki veriler ile karşılaştırılarak kişiye yetki verilmektedir. Böylece parmak izi veya parmak damar tanıma biyometrik sistemlerine göre daha iyi performans, hız ve doğruluk sağlanmış olur.

3. PARMAK DAMAR TANIMA SİSTEMİ

Parmak içindeki damarların dağılım görüntüsü, her insan için farklıdır. Parmak Damar Tanıma Sistemi bu temel üzerinden hareket ederek, parmak damar görüntüsünü elde eden ve bu görüntüyü kullanarak kimlik doğrulaması ve tanınması yapan bir biyometrik sistemdir. Bu teknoloji parmağın içini görüntülediği için kir, parmaktaki küçük kesikler, yara izleri ve nemden etkilenmez.

Sistemin çalışma prensibi; yan yana konulmuş bir dizi LED'den yayılan yakın kızılötesi ışınım, parmak içine geçerek kandaki hemoglobin tarafından kısmen emilir. Işınlardan emildiği bölgeler (yani parmak içindeki kan damarları), parmağın diğer yüzünde konumlanmış kamera tarafından saptanan görüntüde karanlık bölgeler olarak görülür. Bu görüntü üzerinde görüntü işleme yöntemleri uygulanır ve bir parmak damarı motifi çıkarılır. Bu motif sayısallaştırılır ve sisteme önceden kayıt edilmiş motif şablonlarıyla karşılaştırılarak kullanıcının kimliği doğrulanır [8].



Şekil 24. Parmak Damar Tanıma Sistemi ve Çalışma Mekanizması [24].



Şekil 25. Parmak Damar Modelinin Görüntüsü [18].

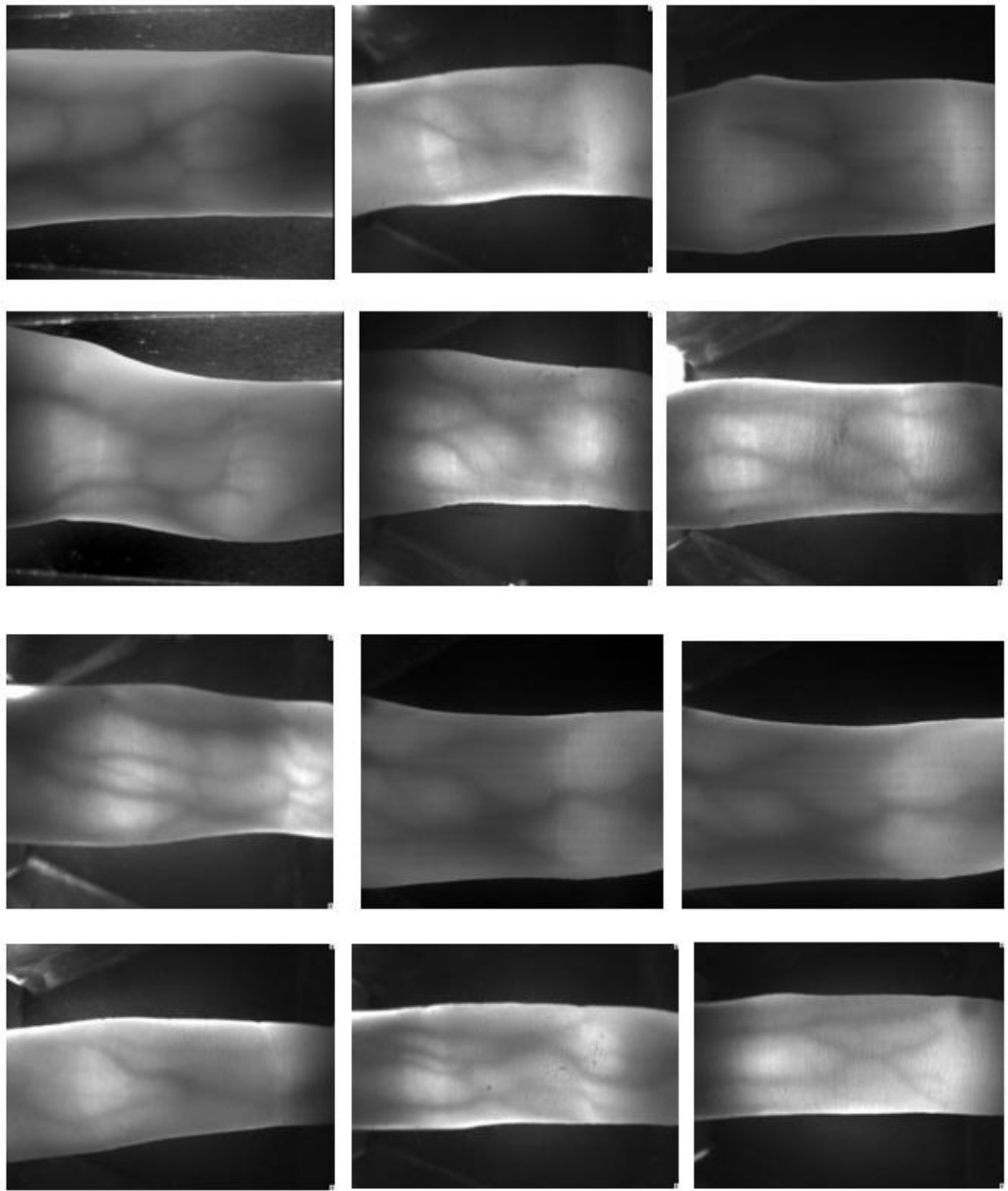
Parmak damar tanıma teknolojisini diğer biyometrik yöntemlerden ayıran özellikler şunlardır [9]:

- Parmak damar yapısı, insan yaşamı boyunca değişime uğramaz.
- Tek yumurta ikizlerinin bile parmak damar yapıları birbirinden farklıdır.
- Her bireyin kendine özgü parmak damar yapısı olduğundan kimlik doğrulama sırasında güvenilir sonuç verir.
- Hızlıdır, kimlik doğrulama işlemini bir kaç saniyede tamamlar.
- Kimlik doğrulama işlemi için akılda şifre tutulmasına gerek kalmaz.
- Parmak damar haritası çalınıp, kopyalanamadığından ATM sahtekârlığı riski en aza indirilmiş olur.
- Parmak izinden farklıdır. Çünkü parmak izi, parmağın dış yüzeyinin izi olduğundan kopyalanması kolaydır. Ancak; damar haritası dış yüzeyden etkilenmeyen bir yapıdadır.
- Sadece canlı parmak kullanılabilir, çünkü işlem sırasındaki kan akışı önemlidir.
- Sistemi kullanırken sadece hizalama amaçlı olarak parmağın ucu okuyucuya dokunur. Dolayısıyla parmak izine göre çok daha hijyeniktir.
- Okuyucunun kullandığı ışınlar insan sağlığına zararlı değildir.
- Parmağın derisinde meydana gelen kesik, ezik vb. deformasyonlardan etkilenmez.

- Müşterilerden alınan parmak damar haritası örneğinden üretilen veri kimlik tespiti için kullanılmaz, kimlik doğrulama için kullanılır. Böylece müşteri, kişisel gizlilik endişesi olmadan cihazı kullanabilir.

3.1. Parmak Damar Görüntülerinin Toplama Süreci

Aşağıdaki şekilde görülen parmak damar görüntüleri Hong Kong Üniversitesinin veritabanından internet üzerinden elde edilmiştir. Parmak damar tanıma sistemi için geliştirilen cihazların çalışma mantığını kavramak için KfV-100 cihazı kullanılmıştır.



Şekil 26. Uygulamada Kullanılan Bazı Parmak Damar Görüntüleri [15].

3.2. KfV-100 Parmak Damar Tanıma Cihazı

Bu cihaz, Parmak Damar Tanıma sistemi için geliştirilmiştir. Parmak damar okuyucu olarak da piyasada bulunur. Teknolojinin hızlı gelişmeler kaydetmesine bağlı olarak sadece biyometrik özelliklerin güvenlik konusunda yetersiz kaldığı anlaşılmış ve bunun sonucunda üretilen cihazlara ya birden fazla biyometrik özellik tanıyabilen sistemler eklenmiş ya da aidiyet temelli kimliklendirme için kullanılan manyetik kartları okuyabilen sistemler dahil edilmiştir. Bu ürün hem parmak damarları tanıyan hem de kullanıcılar için hazırlanan manyetik kartları okuyabilen bir üründür.



Şekil 27. KfV-100 Cihazı

3.2.1. KVV-100 ve RFID Modül (FeliCa veya MIFARE) Özellikleri

Aşağıdaki tabloda kullanılan parmak damar okuyucu cihazın özellikleri yer almaktadır.

Tablo 4. KVV-100 Cihazının Özellikleri

Cihaz Özellikleri	
CPU	S3C2440 400MHz 32Bit RISC,
OS	Linux
Flash Bellek	128 MByte
RAM	64 MByte
LCD	2.8", TFT Renkli, Dokunma Paneli,
Çözünürlük	320 x 240(262K Renk)
Arayüz	TCP/IP, USB, RS232/422/485, Wiegand 26/34Bit
Relay Input	2 port
Output	2 port
Storage for vein pattern	300,000 Max.
Storage for log	1,000,000 Max.
RFID(Optional)	13.56MHz, 125MHz, 900MHz
Boyut	92 x 214 x 84(mm)
Çalışma Sıcaklığı	0~40°C
Nem	20~80%RH
Parmak Damar Modeli Boyutu	Approx 500 byte
Identification method	1:1 or 1:N (N : up to 1,000)
FRR(False Reject Rate)	0.01% under(JIS based testing)
FAR(False Accept Rate)	0.0001% under(JIS based testing)
FTER(Failure to Enroll Rate)	0.08%(IBG Test 2006)

KVV-100 Cihazını kullanabilmek için öncelikle el parmaklarından biri aşağıdaki şekilde (düzgün bir şekilde), tırnak ucu sensörün bulunduğu bölgenin ucunda bulunan ve yanıp sönen led'in üzerine temas edecek şekilde yerleştirilir. Bu aşamada parmağın iç yüzeyi sensöre bakacak konumda, parmak düzgün olarak sensörün bulunduğu kısma yerleştirilir.



Şekil 28. KfV-100 Cihazına Parmağın Yerleştirilmesi

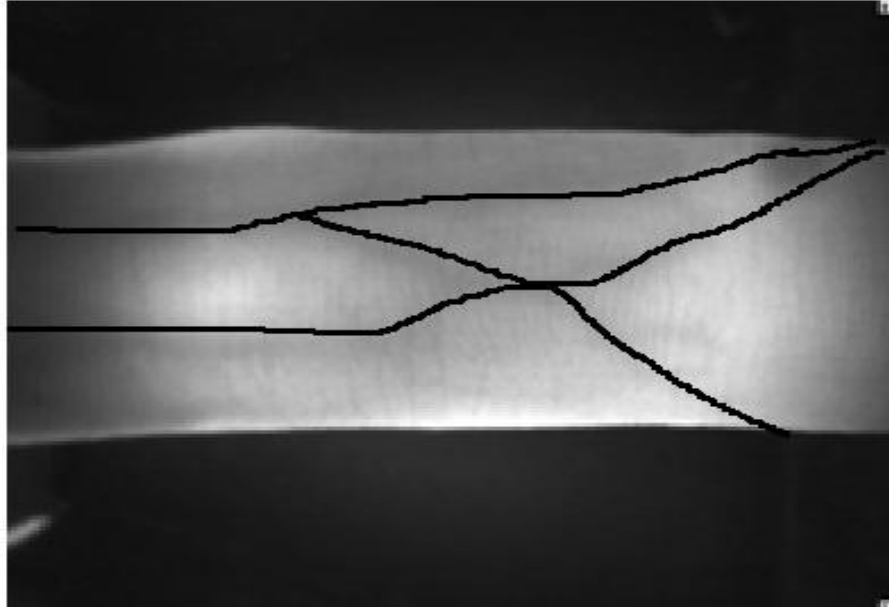
Parmak düzgün yerleştirildikten sonra cihaz aşağıdaki şekildeki gibi 4 kez bu işlemi tekrarlanması gerekir. Eğer parmak düzgün yerleştirilmişse led in ışığı yeşilden maviye dönecektir. Bu işlemin sonunda cihaza parmağı yerleştirirken bir hata olmamışsa cihaz rakamlardan oluşan 10 basamaklı bir şifre üretecektir.(Örnek: 2147483645, 2147483641 gibi).



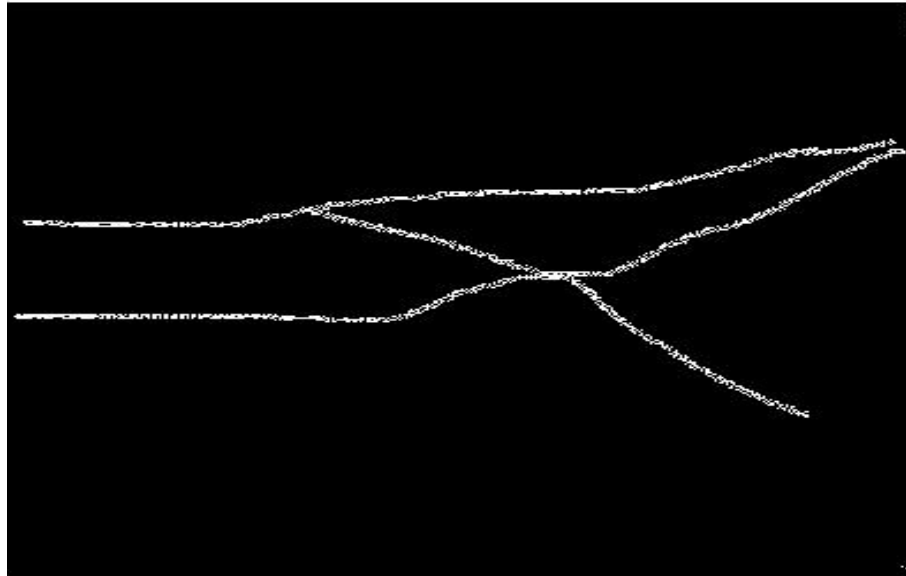
Şekil 29. KfV-100 Cihazının Parmak Damar Haritasına Göre Şifre Oluşturma Süreci

3.3. Parmak Damar Uzman Sistemin Hazırlanması

Elde edilen parmak damar görüntülerinin Matlab programında görüntü işleme komutları kullanılarak iskeleti çıkarılmıştır. Elde edilen görüntüdeki damarlar net olmadığı için bir başka program yardımıyla damarlar üzerinden geçilerek belirgin hale getirilmiştir.



Şekil 30. Parmak Damar Görüntüsü



Şekil 31. Parmak Damar Görüntüsünün İskeleti

Görüntü iskeletinin elde edilmesi için Matlab programı kullanılmıştır. Bu programın komutları aşağıdaki gibidir.

```
>> I=imread('sonn.jpg');  
>> imshow(I)  
>> m=rgb2gray(I);  
>> imshow(m)
```

```
>> x=bwmorph(m,'thin',inf);  
>> imshow(x)  
>> bw=~m;  
>> imshow(bw)
```

Aşağıda Şekil 32'de uzman sistemin Matlab programında hazırlanan arayüzü yer almaktadır. Bu uygulamanın komutları IJESR/April 2012/ Volume-2/Issue-4/Article No-4/158-175 makalesinden alınmıştır [16].



Şekil 32. Uygulamanın Matlab Arayüzü

4. SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin hızlı gelişmesi sonucunda birçok yeni araç ve cihazlar yaşantımızın birer parçası haline gelmiştir. Cihazların sunduğu konfora çabuk alışan insanlar, otomasyon sistemlerine bağımlı hale gelebilmektedir. Örneğin, bazı işyerlerinde girişlerdeki otomatik açılıp kapanan kapılar, bir konfor aracı olarak değerlendirilebilir. Özellikle ülke sınırlarını geçerken, güvenlik unsurlarının oldukça fazlaştırıldığı görülmektedir. Parmak izlerinin alınması, daha sonraki girişlere parmak izlerini karşılaştırarak, ülkeye daha rahat girmeyi sağlayabilmektedir. Güvenlik uygulamaları ile birlikte sahtecilik de gündeme gelmekte ve pek çok sistem ciddi ataklara maruz kalmaktadır. Bu kapsamda ilk akla gelen güvenlik ihlallerinden olan kart, anahtar vb. çalınması, yetkisiz şifre paylaşımı gibi pek çok sorunu ortadan kaldıran biyometrik yöntemlerin gelişmesine neden olmuştur.

Güvenilir kimlik doğrulama günümüzde çok önemlidir. Üç kimlik denetimi yöntemi arasında; yani bilgi temelli kimlik doğrulama, aidiyet temelli kimlik doğrulama ve biyometri temelli kimlik doğrulama; biyometriğe dayalı kimlik doğrulama en güvenilir yöntem olarak bilinir. Araştırmacılar, yüksek doğruluk sağlamak için yeni biyometrik sistemler üzerine araştırmalarını yoğunlaştırmaktadırlar. Ancak bu teknolojinin yaygınlaşabilmesi için maliyetlerin daha uygun hale getirilmesi gerekmektedir.

Biyometrik sistemlerin önemi, kişiye has özellikler tabanlı geliştirilmesidir. Kişiye has özellikler ise, transferlerinin mümkün olmayışı noktasında yüksek güvenlik sağlamaktadır. Dolayısıyla bu özellikleri ile biyometrik sistemler, pasaport kontrollerinden bankacılık işlemlerine kadar geniş bir yelpazede uygulama bulmakta ve önemli bir araştırma konusu olarak ortaya çıkmaktadır.

Biyometrik sistemin en temel avantajı, kişilerin hiçbir zaman hiçbir yerde unutma veya kaybetme olanakları bulunmayan bir uzuvları ile kendilerini tanıtabilmeleridir. Bu yüzden gelecek için planlanmakta olan güvenlik sistemlerinin en temel amacı, insanların hiçbir kart veya anahtar taşımadan veya şifre ezberlemeden kolaylıkla tanınabilmeleridir.

Parmak damar tanıma cihazları mevcut olup son yıllarda kullanımı artmıştır. Örneğin hastanelerde parmak damar okuyucuları sayesinde personelin devamları otomatik olarak belirlenebilmektedir. Parmak damar okuyucularına bağlı olarak açılan gizli kapılar, sistemler veya bir otomasyon sistemine girişler artık James Bond filmlerinde rastlanmayıp, kullanımları günden güne artmaktadır.

Bu çalışmada parmak damarları sayesinde otomasyon sistemlerinin kullanımının temelinin anlaşılması ve basitleştirilmesi amaçlanmıştır. Parmak damar okuyucu cihazlarının nasıl bir yöntemler kod ürettikleri konusunda daha detaylı bilgi sağlanabilmesi için FÜBAP desteği ile bir parmak damar okuyucusu alınmış ve bu cihazın teori ile pratiği nasıl kombine ettiği üzerinde çalışmalar sürdürülmüştür.

Matematiksel modellemede MATLAB yazılım araçları kullanılmıştır. Alınan cihazın şifreleme yönteminin bazen sıkıntılar ortaya çıkardığı görülmüştür. Özellikle parmak damar tanıtımı sürecinde bazen defalarca yeni kayıt alınması gereği doğmuştur. Bu tür sorunların başında parmağın konulduğu platforma tam oturtulmamasının önemli rol oynadığı görülmüştür. Bunun haricinde Matlab'taki kodlamanın da daha hassas hale getirilmesi gereği fark edilmiştir. Bu amaçla Matlab program üzerine bazı modüller eklenerek, okunan damar izlerinin daha hassas değerlendirilmesi yapılabilmektedir. Bunun için özellikle referans alınan nokta sayılarının çoğaltılmasının olumlu sonuç verdiği belirlenmiştir.

Biyometrik sistemler içerisinde parmak damar tanıtımı ile güvenlik amacıyla yapılan ya da geliştirilen otomasyon sistemlerinin bazen kifayetsiz kalacağı, bu nedenle de kombine biyometrik sistemlerin kullanılmasının bir çözüm olacağı sonucuna varılmıştır. Parmak damar okuyucusu ile parmak izi okuyucusunun aynı cihaz üzerinde kombine edilerek, aynı anda çifte kontrol yapılabilmesi durumunda, güvenlik çok daha fazla artırılabilir.

Bu tez çalışması sonucunda, biyometrik güvenlik sistemleri için çifte kontrolü bir arada yapacak bir kombine sistem çalışması yapılması önerilmektedir. Bu kombine sistemin aynı anda hem parmak damarlarını hem de parmak izini tanıyan modüler bir özellik taşıması halinde, sistem güvenliğinin çok fazla artırılacağı sonucuna varılmıştır. Bu tür bir çalışma doktora çalışması özelliğinde olup, bu alanda bir prototip geliştirilmesi ile sağlanabilir. Son yıllarda literatürde parmak damar ve parmak izi ile çalışan biyometrik sistemler üzerine çalışmaların yapıldığı görülmektedir [17]. Yapılacak çalışmada özellikle farklı füzyon aşamalarının ve farklı eşikleri tanıtmak ve bunları kıyaslamak, çalışmanın esasını oluşturabilir.

KAYNAKLAR

- [1]. <http://www.bilisimdergi.com/Biyometrik-Guvenlik-Sistemleri-21-3.html>
(19.05.2011)
- [2]. <http://www.turkeyforum.com/satforum/archive/index.php/t-202.html>
(21.05.2011)
- [3]. http://www.slidefinder.net/b/biyometri_bektas/13993600 (21.05.2011)
- [4]. Ergen, B. ve Çalışkan, A., 2011. Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri, 6th International Advanced Technologies Symposium (IATS'11), Fırat Üniversitesi, Elazığ, Turkey, 16-18 May.
- [5]. <http://alper-ozen.blogcu.com/bilgisayar-destekli-kimlik-tespit-sistemlerinde-biyometrik-yonte/9553687> (14.05.2011)
- [6]. Şamlı, R. ve Yüksel, M. E., 2009. Biyometrik Güvenlik Sistemleri , Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa, 11-13 Şubat, s. 691-697.
- [7]. www.iscturkey.org/2010/2008/2006/pdf/poster/78.pdf (21.05.2011)
- [8]. <http://www.nanobiz.com.tr/images/products/mobiyosys%20brosuru.pdf>
(22.05.2011)
- [9]. www.internethaberoku.com/Biyokimlik-biyometrik-tanima-sistemi-wordh-3251.html (22.05.2011)
- [10]. http://k.domaindlx.com/kirbas/e_is/Veri_ve_Ag_Guvenligi.pdf (22.05.2011)
- [11]. Dede, G. ve Sazlı, M. H., 2009. Biyometrik Sistemlerin Örüntü Tanıma Perspektifinden İncelenmesi ve Ses Tanıma Modülü Simülasyonu, EEBBM Ulusal Kongresi (Elektrik – Elektronik-Bilgisayar ve Biyomedikal Mühendisliği 13. Ulusal Kongresi ve Fuarı), 'Teknolojide Buluşuyoruz', ODTÜ, Ankara, 23-26 Aralık.
- [12]. Yıldız, F. ve Baykan, N. A., 2011. Çapraz İlişki Metoduyla İris Tanıma, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi, 10, 19-37.
- [13]. <http://ab.org.tr/ab03/tammetin/46.pdf> (23.05.2011)
- [14]. <http://www.ergosis.com.tr/avucici-damar-tanima-teknolojisi.html> (20.10.2012)
- [15]. <http://www4.comp.polyu.edu.hk/~csajaykr/fvdatabase.htm> (18.10.2011)

- [16]. Venkatesh D. , Balaji S. ve Chakravarthy A. S .N. Security Evaluation Of Fingerprint Based Authentication Systems. IJESR/April 2012/ Volume-2/ Issue-4/Article No-4/158-175.
- [17]. Aboalsamh, H., A. A Multi Biometric System Using Combined Vein and Fingerprint Identification, International Journal Of Circuits, Systems And Signal Processing, Issue 1, Volume 5, 2011, pp. 29-36.
- [18]. <http://www.appliedbiometrics.com/technology/finger-vein-recognition> (18.05.2011)
- [19]. <http://www.pitsteknoloji.com/biyometrik-sistemler.php> (21.05.2011)
- [20]. <http://www.iscturkey.org/2010/2008/2006/pdf/poster/78.pdf> (25.05.2011)
- [21]. <http://www.ahmetkakici.com/genel/biyometrik-tanima-sistemleri> (23.01.2013)
- [22]. <http://www.canonturk.com/vbulletin/konu-disi/328-biyometrik-fotograf-nedir.html> (22.01.2013)
- [23]. <http://www.epasaport.gov.tr/hakkinda/biyometrikfoto.aspx> (27.01.2013)
- [24]. Miura N., Nagasaka, A., Miyatake, T. “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification”, Machine Vision and Applications ,2004 ,pp 194–203.
- [25]. Indovina, M., Uludag, U., Snelick, R., Mink, A. and Jain, A. Multimodal biometric authentication methods: a cots approach, Proc. MMUA 2003, Workshop on Multimodal User Authentication, (2003), pp. 99-106.
- [26]. <http://www.infomet.com.tr/fingerprint.aspx> (26.01.2013)
- [27]. Varol, A., Cebe B. "Yüz Tanıma Algoritmaları", 5th International Computer & Instructional Technologies Symposium, 22-24 September 2011, Fırat University, ELAZIĞ- TURKEY
- [28]. Varlık, A., Çorumluoğlu, Ö. Dijital Fotogrametri Teknikleri İle Kişi Tanıma , Harita Teknolojileri Elektronik Dergisi Cilt: 3, No: 2, 2011 (1-24).
- [29]. Yıldız, F., Baykan, N. A., Çapraz İlişki Metoduyla İris Tanıma, Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Volume Teknik-Online Dergi Cilt 10, Sayı:1-2011
- [30]. <http://www.elektrik.gen.tr/teknik-i%C3%A7erik/fiziksel-C3%B6zelliklerden-yararlanarak-kimlik-tespit-etme> (20.02.2013)

EKLER

Ek : Matlab Uygulaması

Aşağıda uzman sistemin Matlab komutları yer almaktadır. Bu komutlar IJESR/April 2012/ Volume-2/Issue-4/Article No-4/158-175 makalesinden alınmıştır [16].



Şekil 32. Uygulamanın Matlab Arayüzü

```
function u()
```

```
clear;
```

```
clc;
```

```
close all;
```

```
global imagine n_bands h_bands n_arcs h_radius h_lato n_sectors matrice
```

```
num_disk
```

```
n_bands=4;
```

```
h_bands=20;
```

```
n_arcs=16;
```

```
h_radius=12;
```

```
h_lato=h_radius+(n_bands*h_bands*2)+16;
```

```
if mod(h_lato,2)==0
```

```
h_lato=h_lato-1;
```

```

end
n_sectors=n_bands*n_arcs;
matrice=zeros(h_lato);
for ii=1:(h_lato*h_lato)
matrice(ii)=whichsector(ii,h_radius);
end
num_disk=8;
choix=0;
possibility=6;
messaggio='Insert the number of set: each set determines a class. This set should
include a number of images for each person, with some variations in expression and
in the lighting.';
while choix~=possibility,
choix=menu(' ','Resim seç ve Veritabanına Ekle','Parmak Damar Tanıma için
Resim Seç','Veritabanını Sil',...
'Parmak Damar Görüntüleme','Gabor Filtresi Görüntüleme', 'Çıkış');
%=====

if choix==1,
clc;
close all;
selezionato=0;
while selezionato==0
[namefile,pathname]=uigetfile({'*.bmp;*.tif;*.tiff;*.jpg;*.fig;*.jpeg;*.gif','IMAGE
Files (*.bmp,*.tif,*.tiff,*.jpg,*.jpeg,*.gif)'),'Chose GrayScale Image');
if namefile~=0
[img,map]=imread(strcat(pathname,namefile));
selezionato=1;
else
disp('Select a grayscale image');
end
if (any(namefile~=0) && (~isgray(img)))
disp('Select a grayscale image');

```

```

selezionato=0;
end
end
immagine=double(img);
if isa(img,'uint8')
graylevmax=2^8-1;
end
if isa(img,'uint16')
graylevmax=2^16-1;
end
if isa(img,'uint32')
graylevmax=2^32-1;
end
fingerprint = immagine;
N=h_lato;
[BinarizedPrint,XofCenter,YofCenter]=centralizing(fingerprint,0);
[CroppedPrint]=cropping(XofCenter,YofCenter,fingerprint);
[NormalizedPrint,vector]=sector_norm(CroppedPrint,0);
for (angle=0:1:num_disk-1)gabor=gabor2d_sub(angle,num_disk);
ComponentPrint=conv2fft(NormalizedPrint,gabor,'same');
[disk,vector]=sector_norm(ComponentPrint,1);
finger_code1{angle+1}=vector(1:n_sectors);
end
img=imrotate(img,180/(num_disk*2));
fingerprint=double(img);
[BinarizedPrint,XofCenter,YofCenter]=centralizing(fingerprint,0);
[CroppedPrint]=cropping(XofCenter,YofCenter,fingerprint);
[NormalizedPrint,vector]=sector_norm(CroppedPrint,0);
for (angle=0:1:num_disk-1)
gabor=gabor2d_sub(angle,num_disk);
ComponentPrint=conv2fft(NormalizedPrint,gabor,'same');
[disk,vector]=sector_norm(ComponentPrint,1);
finger_code2{angle+1}=vector(1:n_sectors);

```

```

end
% FingerCode added to database
if (exist('fp_database.dat')==2)
load('fp_database.dat','-mat');
fp_number=fp_number+1;
data{fp_number,1}=finger_code1;
data{fp_number,2}=finger_code2;
save('fp_database.dat','data','fp_number','-append');
else
fp_number=1;
data{fp_number,1}=finger_code1;
data{fp_number,2}=finger_code2;
save('fp_database.dat','data','fp_number');
end
message=strcat('FingerCode was succesfully added to database. Fingerprint
no.',num2str(fp_number));
msgbox(message,'FingerCode DataBase','help');
end
%=====

if choix==2,
clc;
close all;
selezionato=0;
while selezionato==0
[namefile,pathname]=uigetfile({'*.bmp;*.tif;*.tiff;*.jpg;*.jpeg;*.gif','IMAGE Files
(*.bmp,*.tif,*.tiff,*.jpg,*.jpeg,*.gif)'),'Chose GrayScale Image');
if namefile~=0
[img,map]=imread(strcat(pathname,namefile));
selezionato=1;
else
disp('Select a grayscale image');
end

```



```

if (any(namefile~=0) && (~isgray(img)))
disp('Select a grayscale image');
selezionato=0;
end
end
immagine=double(img);
if isa(img,'uint8')
graylevmax=2^8-1;
end
if isa(img,'uint16')
graylevmax=2^16-1;
end
if isa(img,'uint32')
graylevmax=2^32-1;
end
fingerprint = immagine;
N=h_lato;
[BinarizedPrint,XofCenter,YofCenter]=centralizing(fingerprint,0);
[CroppedPrint]=cropping(XofCenter,YofCenter,fingerprint);
[NormalizedPrint,vector]=sector_norm(CroppedPrint,0);
vettore_in=zeros(num_disk*n_sectors,1);
for (angle=0:1:num_disk-1)
gabor=gabor2d_sub(angle,num_disk);
ComponentPrint=conv2fft(NormalizedPrint,gabor,'same');
[disk,vector]=sector_norm(ComponentPrint,1);
finger_code{angle+1}=vector(1:n_sectors);
vettore_in(angle*n_sectors+1:(angle+1)*n_sectors)=finger_code{angle+1};
end
if (exist('fp_database.dat')==2)
load('fp_database.dat','-mat');
vettore_a=zeros(num_disk*n_sectors,1);
vettore_b=zeros(num_disk*n_sectors,1);
best_matching=zeros(fp_number,1);

```

```

valori_rotazione=zeros(n_arcs,1);
for scanning=1:fp_number
fcode1=data{scanning,1};
fcode2=data{scanning,2};
for rotazione=0:(n_arcs-1)
p1=fcode1;
p2=fcode2;
% ruoto i valori dentro disco
for conta_disco=1:num_disk
disco1=p1{conta_disco};
disco2=p2{conta_disco};
for old_pos=1:n_arcs
new_pos=mod(old_pos+rotazione,n_arcs);
if new_pos==0
new_pos=n_arcs;
end
for conta_bande=0:1:(n_bands-1)
disco1r(new_pos+conta_bande*n_arcs)=disco1(old_pos+conta_bande*n_arcs);
disco2r(new_pos+conta_bande*n_arcs)=disco2(old_pos+conta_bande*n_arcs);
end
end
p1{conta_disco}=disco1r;
p2{conta_disco}=disco2r;
end
% ruoto i dischi circolarmente
for old_disk=1:num_disk
new_disk=mod(old_disk+rotazione,num_disk);
if new_disk==0
new_disk=num_disk;
end
pos=old_disk-1;
vettore_a(pos*n_sectors+1:(pos+1)*n_sectors)=p1{new_disk};
vettore_b(pos*n_sectors+1:(pos+1)*n_sectors)=p2{new_disk};

```

```

end
d1=norm(vettore_a-vettore_in);
d2=norm(vettore_b-vettore_in);
if d1<d2
val_minimo=d1;
else
val_minimo=d2;
end
valori_rotazione(rotazione+1)=val_minimo;
end
[minimo,posizione_minimo]=min(valori_rotazione);
best_matching(scanning)=minimo;
end
[distanza_minima,posizione_minimo]=min(best_matching);
beep;
message=strcat('The nearest fingerprint present in DataBase which matchs input
fingerprint is : ',num2str(posizione_minimo),...
' with a distance of : ',num2str(distanza_minima));
msgbox(message,'DataBase Info','help');
else
message='DataBase is empty. No check is possible.';
msgbox(message,'FingerCode DataBase Error','warn');
end
end
%=====

if choix==3,
clc;
close all;
if (exist('fp_database.dat')==2)
button = questdlg('Do you really want to remove the Database?');
if strcmp(button,'Yes')
delete('fp_database.dat');

```

```

msgbox('Database was succesfully removed from the current directory.','Database
removed','help');
end
else
warndlg('Database is empty.',' Warning ');
end
end
%=====

if choix==4,
clc;
close all
selezionato=0;
while selezionato==0
[namefile,pathname]=uigetfile({'*.bmp;*.tif;*.tiff;*.jpg;*.jpeg;*.gif','IMAGE Files
(*.bmp,*.tif,*.tiff,*.jpg,*.jpeg,*.gif)'),'Chose GrayScale Image');
if namefile~=0
[img,map]=imread(strcat(pathname,namefile));
selezionato=1
else
disp('Select a grayscale image');
end
if (any(namefile~=0) && (~isgray(img)));
disp('Select a grayscale image');
selezionato=0;
end
end
figure('Name','Selected image');
imshow(img);
end
%=====

```

```
if choix==5,  
    clc;  
    close all;  
    figure('Name','Gabor Filter');  
    mesh(gabor2d_sub(0,num_disk));  
end  
end [16]
```

ÖZGEÇMİŞ

Songül ŞAN, 1983 yılında Tunceli’de doğdu. İlk, orta ve lise öğrenimini Elazığ ’da tamamladıktan sonra 2005 yılında Fırat Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Öğretmenliği Bölümü’nü kazandı ve 2009 yılında mezun oldu. 2010 yılının başında Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektronik-Bilgisayar Eğitimi Anabilim Dalı’nda yüksek lisans eğitimine başladı. 2011 yılında Diyarbakır Kayapınar Türk Telekom Teknik ve Endüstri Meslek Lisesine Bilişim Teknolojileri Öğretmeni olarak atandı. Halen Meb' de Bilişim Teknolojileri Öğretmeni olarak görev yapmaktadır. Yabancı dili İngilizcedir.