TC

İSTANBUL AYDIN ÜNİVERSİTESİ

FEN BİLİMLER ENSTİTÜSÜ

ONLİNE SINAV SİSTEMLERİNDE GÜVENLİK SORUNLARI VE BİR ÖRNEK UYGULAMA

YÜKSEK LİSANS TEZİ

KADİR KESKİN

Y1213.010030

Bilgisayar Mühendisliği Ana Bilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Ali GÜNEŞ

HAZİRAN 2015

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1213.010030** numaralı öğrencisi **Kadir KESKİN** 'in **"ONLİNE SINAV SİSTEMLERİNDE GÜVENLİK SORUNLARI VE BİR ÖRNEK UYGULAMA"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 10.06.2015 tarih ve 2015/12 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul edilmiştir.

Öğretim Üyesi Adı Soyadı	İmzası
Tez Savunma Tarihi :30/06/2015	
1)Tez Danışmanı: Prof. Dr. Ali GÜNEŞ	.....
2) Jüri Üyesi : Yrd. Doç. Dr. Duygu ÇELİK	.....
3) Jüri Üyesi : Yrd. Doç. Dr. M. Ahmed SHAH	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans / Doktora tezi olarak sunduğum "……..……

…….
……" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve

geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (…/…/20…)

Aday / İmza

ÖNSÖZ

Online eğitim sistemleri hızla gelişmekte ve yaygınlaşmaktadır. Yine bu eğitim sistemine bağlı olarak online sınavlar da artış göstermektedir. Gelişen her sistemde olduğu gibi online sınav sistemlerinde de bazı sorunlar ortaya çıkmaktadır. Bu sorunların en önemlisi ise güvenliktir. Bu çalışmada maksat online sınav sistemlerinde oluşan güvenlik sorununun çözümüne yönelik olarak güvenli sınav giriş uygulaması geliştirmektir. Bu bağlamda yapılacak en etkin yöntemler araştırılmış ve biyometrik sistemlerden Parmak İzi Tanıma Teknolojisi kullanılarak Güvenli online sınav giriş uygulaması gerçekleştirilmiştir.

HAZİRAN-2015 **Kadir KESKİN**

Öğretim Görevlisi

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **V**
İÇİNDEKİLER ..... **VII**
KISALTMALAR LİSTESİ ..... **IX**
ÇİZELGE LİSTESİ ..... **XI**
ŞEKİL LİSTESİ ..... **XIII**
ÖZET ..... **XV**
ABSTRACT ..... **XVII**
1 GİRİŞ **1**
1.1 Tez Çalışmasının Amacı 2
1.2 Tez Çalışmasının Kapsamı 2
2 ONLİNE EĞİTİM SİSTEMLERİ **3**
2.1 Online Eğitim Nedir? 3
3 ONLİNE EĞİTİMDE SINAV SİSTEMLERİ **5**
3.1 Online Sınavlarda Güvenlik Sorunları 5
4 OTOMATİK KİMLİK TANİMA SİSTEMLERİ **7**
4.1 OCR (Optik Karakter Tanıma Sistemleri) 8
4.2 Akıllı Kart Sistemi 9
4.3 Barkod Sistemleri 10
4.4 Radyo Frekansı İle Kimlik Tanıma(RFID) 12
4.5 Biyometrik Kimlik Tanıma Sistemleri 12
5 BİYOMETRİK KİMLİK TANIMA SİSTEMLERİ **13**
5.1 Biyometrik Sistemlerin Özellikleri 14
6 MATERYAL VE YÖNTEM **21**
6.1 Tarihçesi 21
6.2 Parmak İzi Teknolojisinin Çalışma Mantığı 22
6.3 Parmak İzi Teknolojisinin Temel Özellikleri ve Bileşenleri 23
6.4 Parmak İzi Tanıma Teknolojisinin Dezavantajları 23

6.5 Parmak İzi Tanıma Teknolojisinin Avantajları 24
6.6 Parmak İzi Teknolojisinin Kullanıldığı ve Kullanılabileceği Alanları 25
6.7 Parmak İzi ve Güvenlik 25
7 PARMAK İZİ TANIMA ALGORİTMASI 29
8 YÖNTEM 31
8.1 Parmak İzi Tanıma Teknolojisi ile Güvenli Online Sınav Giriş Projesi 31
8.2 PİTT ile Güvenli Sınav Giriş Uygulamasında Kullanılan Yazılım Yapısı 31
8.3 Kullanıcı Giriş Ekranı 32
8.4 Yönetici Ana Ekranı 43
8.5 Yeni Kullanıcı Ekleme Ekranı 45
8.6 Kullanıcı Düzenleme Ekranı 52
8.7 Sınav Giriş Sistemi Uygulamasında Kullanılan Donanım Yapısı 62
8.8 Sınav Sisteminin Veri Tabanı Yapısı 64
9 SONUÇ VE ÖNERİLER 65
KAYNAKLAR 67
ÖZGEÇMİŞ 69

KISALTMALAR LİSTESİ

C#	Csharp
DNA	Deoksiribonükleik asit
RFID	Radio Frequency Identification (Radyo Frekanslı Tanımlama)
USB	Universal Serial Bus
SQL	Structured Query Language
BLOB	Binary Large Object
PİTT	Parmak İzi Tanıma Teknolojisi

ÇİZELGE LİSTESİ

Sayfa

Çizelge 1: Birey Ayırt Etme Karşılaştırma Tablosu 20

ŞEKİL LİSTESİ

Sayfa

Şekil 4.1: Otomatik Kimlik Tanıma Sistemleri 8
Şekil 4.2: Optik Karakter Tanıma Sistemi 9
Şekil 4.3: Barkod Örneği 10
Şekil 4.4: Barkotlama Aşamaları 11
Şekil 4.5: RFID Bileşenleri 12
Şekil 5.1: Ses Tanıma Sistemleri 15
Şekil 5.2:İris Tanıma Sistemi 16
Şekil 5.3: Yüz Tanıma Sistemi 17
Şekil 5.4: El Geometrisi Tanımlama Aleti 18
Şekil 5.5: DNA Örneği 19
Şekil 5.6: Parmak İzi Örneği 19
Şekil 6.1: Parmak İzi Görüntüsü 25
Şekil 7.1: Parmak İzi Tanıma Algoritması 30
Şekil 8.1: Kullanıcı Giriş Ekranı 32
Şekil 8.2: Kullanıcı Giriş Ekranı Başarısız Durum 33
Şekil 8.3: Kullanıcı Giriş Ekranı Başarılı Durum 34
Şekil 8.4: Kullanıcı adı ve Parola Doğrulama 34
Şekil 8.5: Sınav Ekranı 35
Şekil 8.6: Yönetici ekran görüntüsü 43
Şekil 8.7: Yeni Yullanıcı Ekleme Ekranı 45
Şekil 8.8: Kullanıcı Güncelleme Ekranı 53
Şekil 8.9: Kullanıcı Parmak İzi Güncllleme 54
Şekil 8.10: Uygulamada kullanılan Parmak İzi Okuyucu Cihaz 63
Şekil 8.11 : Veri Tabanı Görüntüsü 64

ONLİNE SINAV SİSTEMLERİNDE GÜVENLİK SORUNLARI VE BİR ÖRNEK UYGULAMA

ÖZET

Bu proje üç ana bölümden oluşmaktadır. Bu bölümler sırasıyla şöyledir;

- Online sınav sistemleri ve otomatik tanıma teknolojileri,
- Biyometrik tanıma teknolojileri ve parmak izi tanıma teknolojisinin(PİTT) teorik olarak ele alındığı bölüm,
- Parmak izi uygulamasında kullanılan yazılımın sunulduğu uygulama bölümü.

Teorik bölümde online sınav sistemleri ile otomatik ve biyometrik tanıma teknolojilerinden bahsedildikten sonra parmak izi uygulamalarının geçmişten günümüze kadar ki uygulama alanları ele alınmış. Ve geliştirme sürecinde PİTT 'nin gelecekte nerelerde kullanılacağından bahsedilirken, uygulama bölümünde yapılan çalışma için gerekli yazılım ve donanım gereksinimleri ve uygulamanın şekline göre oluşturulacak sistemden bahsedilmiştir.

Bu tez çalışmasında " güvenli online sınav giriş" uygulaması yapılmıştır. Projede Visual Studio 2010.NET platformuna C# dilinde PİTT teknolojisi ile parmak izi okuyucu kullanarak güvenli giriş yapmayı sağlayan yazılım geliştirilmiştir.

Bu yazılıma göre, kullanıcılar parmak izi okuyucuya parmak izlerini okuttuktan sonra sınav ekranına geçiş yapılır ve bu ekranda kullanıcı adı ile parolası onaylanarak güvenli bir şekilde sınav ekranı açılır. Kullanıcı buradan sınavlarını kontrol eder. Eğer kullanıcının tanımlı bir sınavı varsa sınavını tamamlar ve sınavdan çıkış yapar. Eğer giriş yapan kullanıcı, yönetici ise bu ekrandan sınav ataması, sınav tarihlerinin belirlenmesi ve soru düzenleme/ekleme vb. işlemler gerçekleştirir.

PİTT' ni tercih etmemizdeki faktörler; öncelikle en güvenli sistemlerden biri olması ve biyometrik sistemler içinde kullanımı en kolay olanı olmuştur. Ayrıca PİTT' in yakaladığı hızlı gelişim sayesinde geleceğin teknolojileri arasındadır.

Anahtar Kelimeler: PİTT, Online Sınav Sistemi, Biyometrik Sistemler, Visual Studio 2010.NET, C#.

SAFETY PROBLEMS IN ONLINE TEST SYSTEM AND A CASE STUDY

ABSTRACT

This project consists of three main sections. These sections are as follows respectively;

- Online test systems and automatic identification technologies,
- Biometric recognition technology and fingerprint recognition technology (PİTT) section were discussed theoretically,
- Application section is about fingerprint application software

In the theoretical section, automatic and biometric recognition technologies with online exam system are mentioned, after that applications of fingerprint applications from the past to the present day were discussed. And in the development process, PITT was mentioned where it will be used in the future. Necessary software and hardware requirements for studies in the application section and system to be established according to the type of the application were explained. In this thesis "secure online exam entry" application is made. The project has been developed in the C # language in Visual Studio platform 2010.NET . Application software allows logging in securely with using fingerprint reader with PITT technology. According to this software, users swipe a fingerprint through fingerprint reader, then the examination screen appears. In this screen, user have to login with username and password to access the test screen. The user controls the test from here. If there is a user-defined test, user complete this test and then log out of the exam. If user is a administrator, user can perform a lot of operations such as assign a exam, determining the exam date, adding/editing questions, etc.

PITT's first reason for preference are that it is an one of the most secure systems and it is the easiest to use in biometric systems. Additionally, due to the rapid development of PITT , it is among the technologies of the future.

Keywords: Pitt, Online Examination System, Biometric Systems, 2010.NET Visual Studio, C #.

1 GİRİŞ

Teknolojinin hızla ilerlediği günümüzde online ve uzaktan eğitim sistemleri de hızla yaygınlaşmaktadır. Dolayısıyla online eğitim sistemlerinde farklı ölçme ve değerlendirme yöntemleri kullanılmakla birlikte en yaygın olarak çevrimiçi sınavlardır kullanılmaktadır. Bu sınav sistemlerinde yaşanacak en büyük güvenlik sorunu ise sınavlarda başkasının yerine sınava girme olasılıklarıdır.

Bu sorunun çözümü ise online sınavlara güvenli giriş sisteminin geliştirilmesidir. Çalışmada bu sorunun çözümüne yönelik olarak otomatik kimlik tanıma sistemleri ve biyometrik kimlik tanıma sistemleri incelenmiştir.

Otomatik kimlik tanıma sistemleri, özellikle kurumsal uygulamalarda hata riskini ve güvenlik sorunlarını en aza indirmek için insan faktörünün aradan çıkarılarak toplanacak verilerin iş akışı süreci içinde kesintiye uğramadan otomatik ve hatasız olarak alınması şeklinde tanımlanır.

Biyometrik kimlik tanıma sistemlerinde ise, kullanıcı sisteme kendisine ait olan ve üzerinde her daim taşıdığı parmak izi, iris, ses, el geometrisi, yüz gibi bir fizyolojik 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 veri tabanına kaydedilmiş biyometrik bilgi ile karşılaştırılır. Karşılaştırma sonucu doğru ise kişinin kimlik doğrulanması gerçekleştirilmiş olur.

Bu çalışmada online sınavlarda karşılaşılacak güvenlik sorununa en etkin çözüm olarak biyometrik kimlik tanıma sistemlerinden parmak izi tanıma teknolojisi kabul edilmiş ve güvenli online sınav giriş uygulaması geliştirilmiştir.

Parmak izi teknolojisi, parmak izi okuma cihazından aldığı veriler ile veri tabanında kayıtlı verilerin karşılaştırılması sonucu istenilen işlemleri gerçekleştirme mantığına dayalı çalışma sistemine sahiptir.

Bu sistemin çalışması;

İlk olarak,

- Parmak izini okuma ve sayısal formata çevirme

- Okunan parmak izinden bilgi üretme
- Üretilen bilginin saklanması

Daha sonra,

- Saklanan bilgi ile giriş bilgilerin karşılaştırılması
- Sistemin kontrolü ve sisteme giriş şeklinde gerçekleşir.

1.1 Tez Çalışmasının Amacı

Bu tez çalışmasında sınav güvenliğini artırmak ve online sınavlarda başkasının yerine sınava girmek şeklinde gerçekleştirilen kopya sorunun önüne geçmek için kimlik doğrulama yöntemlerinden biri olan Parmak İzi Tanıma Sistemi ele alınmıştır. Literatür araştırmaları sonucunda online sınavlarda gerçekleşebilecek en büyük kopya sorunu başkasının yerine sınava girmek olduğu ve insanlardaki bazı biyolojik özelliklerin eşsiz olduğu ortaya çıkmıştır. Bunlar DNA, retina, iris, parmak izi, yüz şekli vb. Parmak İzi Tanıma Sistemi kişilerin parmak izi görüntülerinin birbirinden farklı olması referans alınarak sınav güvenliği için kimlik doğrulama yöntemi olarak kullanılmaktadır.

1.2 Tez Çalışmasının Kapsamı

Çalışmanın ilk bölümünde teze genel bir bakış kazandırmak amacıyla, tezin amacı ve kapsamından bahsedilmektedir. İkinci bölümde literatür araştırmaları sonucunda online eğitim, online eğitimde sınav sistemleri ve güvenlik problemlerinden bahsedilerek otomatik geçiş sistemlerinden teorik bilgiler verilmiştir. Daha sonra çalışmanın amacı kapsamında biyometrik sistemlerin çeşitleri hakkında detaylı teorik bilgi verilerek, üçüncü bölümde literatürde var olan parmak izi tanıma sistemleri incelenmiştir. Ayrıca, tezin amacının en önemli bileşeni olan parmak izi tanıma sistemlerinin tarihi, kullanım yerleri, çalışma mantığı, avantajları/dezavantajları ve güvenliği incelenerek bir uygulama geliştirilmiştir. Dördüncü bölümde ise yapılan çalışmalar neticesinde sonuç ve öneriler tartışılmıştır.

2 ONLİNE EĞİTİM SİSTEMLERİ

2.1 Online Eğitim Nedir?

Online eğitim öğrenciyle öğretmenin aynı mekânda olmaksızın aynı sanal ortamda bulundukları bir eğitim türüdür. Yani fiziksel bir sınıf ortamında bulunmadan sanal sınıf ortamlarıyla bir arada oldukları eğitim türüdür. Bu model eğitimlerde öğrenci ile öğretmen arasında sanal yollarla bir iletişim kurulur. Eğitimci(öğretmen) bir uçta ders verirken, öğrenciler konum ve mekân fark etmeden istedikleri ülkeden ve istedikleri yerden derse katılabilirler.

Uzaktan eğitim, ders veren kişi ile öğrencinin aynı ortamda bulunmadığı eğitim sistemini anlatan bir terimdir. Öğrenci bir bilgisayar yardımıyla derslerini takip edebilir. United States Distance Learning Association 2004 yılında yapmış olduğu uzaktan eğitim tanımı şu şekildedir:

"Uzaktan eğitim uydu, video, ses, grafik, bilgisayar, çoklu ortam teknolojisi gibi araçların yardımıyla, eğitimin uzaktaki öğrencilere ulaştırılmasıdır. USDLA, öğretmen ve öğrencinin birbirlerinden coğrafi olarak uzak olduğunu belirterek bu eğitim programında elektronik araçların ya da yazılı materyal ve matbu malzemelerinin kullanılması gerektiğinin altını çizer." (mezun.com, 2014)

Online eğitim sekron ve asekron olmak üzere iki türlü gerçekleşir.

2.1.1 Sekron Eğitim

Bu tür online eğitimlerde öğrenci ile öğretmen aynı anda aynı sanal ortamda bulunurlar. Öğretmen ders anlatırken öğrenciler canlı olarak sesli, görüntülü ve varsa materyal paylaşımı veya belge paylaşımları hepsini aynı anda takip edebilirler.

İstediklerinde mesaj yoluyla soru sorabilir ve cevap verebilirler. Eğer yönetici konumunda olan öğretmen söz hakkı verirse, donanımsal imkânı olan öğrenciler sesli olarak da derse katılıp söylemek istediklerini söyleyebilirler.

2.1.2 Asekron Eğitim

Bu tür online eğitim sistemlerinde öğrenci ile öğretmen aynı anda aynı sanal ortamda bulunmazlar. Öğretmenler tarafından yapılan dersler görsel ve/veya sesli olarak

kaydedilip sisteme eklenir. Öğrenciler istedikleri zaman bu dersleri izleme ve dinleme imkânına sahiptirler. Asekron online eğitim sistemlerinde sekron eğitim sistemlerinde olduğu gibi soru sorma ve cevaplama şansı yoktur.

3 ONLİNE EĞİTİMDE SINAV SİSTEMLERİ

Online eğitim sistemlerinde farklı ölçme ve değerlendirme yöntemleri kullanılmakla birlikte en yaygın kullanılan yöntem çevrimiçi sınavlardır.

Çevrimiçi sınavlar, öğrencilerin belirtilen tarih ve saatte internete bağlı herhangi bir bilgisayar üzerinden sisteme giriş yaparak cevapladıkları sorulardan oluşan sınav türüdür. Sistem sorumluları tarafından öğrencilerin sınav süreleri ve sınava giriş hakkı sayıları sınav oluşturulurken tanımlanmaktadır. Sınava giriş saatleri esnetilebilmektedir. Herhangi bir saat yerine belirlenen saatler arasında öğrencilerin sınava giriş yapmaları mümkündür. Fakat sınav süresinden bir esneklik olmamaktadır. (Kınalıoğlu & Güven, 2011)

Çevrimiçi sınavlarda sorular çoktan tek seçmeli, çoktan çok seçmeli boşluk doldurma, eşleştirme, kısa cevap, numaralı, doğru yanlış vb. soru türleri bulunmaktadır. Sınav değerlendirmesi sistemde belirtilen kriterlerde otomatik olarak sistem tarafından yapılmaktadır. Değerlendirme sonucu oluşturulan raporları, öğretim elemanları(sadece kendi verdiği dersleri), sistem sorumluları(tüm dersleri) ve öğrenciler(sadece kendi notlarını) kendi yetkileri kapsamındaki kısıtlılıklar doğrultusunda görebilmektedir.

3.1 Online Sınavlarda Güvenlik Sorunları

Online sınavlar çevrim içi olarak belirtilen saat ve sürede gerçekleşir. Özellikle sonuca etkisi yüzdelik olarak fazla olan sınavların(üniversitelerde final sınavları gibi) uygulanması laboratuvarlar ortamında gözetmenler eşliğinde yapılmaktadır. Her ne kadar sınavlar gözetmen eşliğinde olsa da sınav katılımcıları gözetmenler tarafından tanınmamaktadır. Özellikle fazla katılımlı sınav ve laboratuvarlarda öğrencilerin birbirleri yerine sınava girme olasılığı yüksektir. Bu çalışmada bu sorunun giderilmesi için katılımcıların(öğrencilerin) otomatik olarak tanınacağı sistemler araştırılmış ve parmak izi tanıma teknolojisi ile bir sınav giriş sistemi uygulaması geliştirilmiştir.

4 OTOMATİK KİMLİK TANİMA SİSTEMLERİ

Otomatik tanıma ve veri toplama sistemleri, özellikle kurumsal uygulamalarda hata riskini ve güvenlik sorunlarını en aza indirmek için insan faktörünün aradan çıkarılarak toplanacak verilerin iş akışı süreci içinde kesintiye uğramadan otomatik ve hatasız olarak alınması şeklinde tanımlanır.

Sistem tanıma projelerinde ise, insan faktörünü aradan çıkartarak insan gücüne olan ihtiyacı en aza indirmek ve zamandan kazanç sağlamak ve daha az hata payı elde etmek amaçlanmıştır.

Otomatik tanıma sistemlerinden beklenen genel özellikler;

Tanımlanacak birey veya nesnenin kimliğini sıfır hata ile vermesi,

Tanımlama işleminin mesafe, ortam, hava şartları gibi fiziksel sınırlarının olabildiğince az olması,

Tanımlama işleminde, insan faktörünün olabildiğince az olması, mümkün olduğu kadar otomasyona açık olması,

Değişken şartlara göre kendini güncelleyebilecek bir altyapıya sahip olması,

Esnek ve diğer uygulamalar ile kolaylıkla entegre edilebilir bir tanımlama sistemi olması ve güncellemelere açık olması,

Maliyetinin özellikle birim maliyetinin otomatik tanımlamaya geçilmesi durumunda elde edilebilecek olan verimlilik ve kalite yükselmesinin getirisi ile kendisini amorti edebilecek düzey de olması,

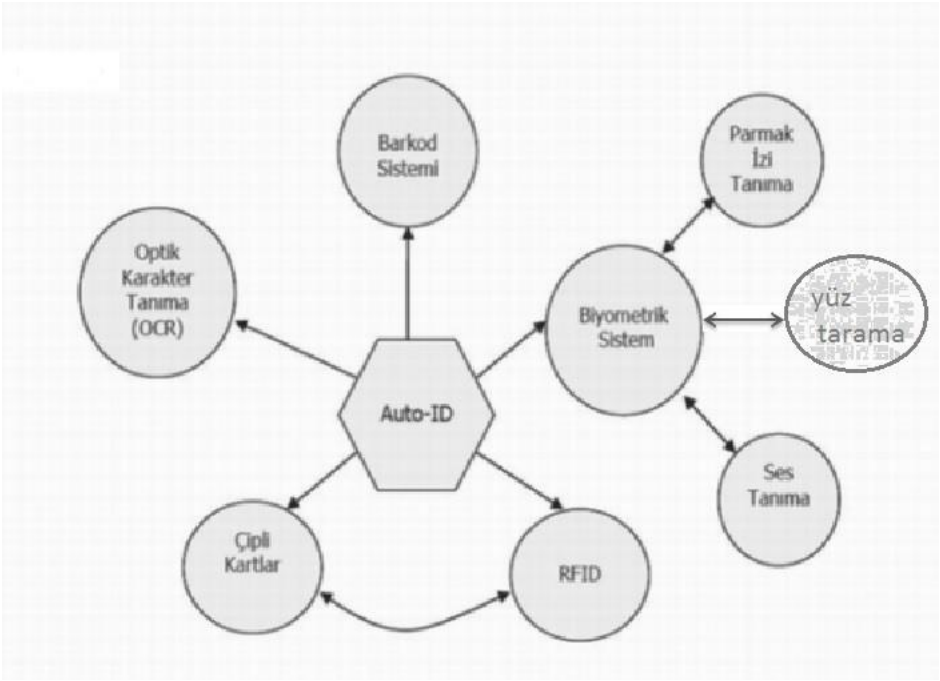
Gelişen teknoloji ile otomatik tanımlamanın otomatik olarak aldatılabilmesine yönelik uygulamalara karşı korunaklı olması,

Yapay zekâ uygulamaları ile birlikte çalışabilecek donanım ve yazılım altyapısına sahip olarak, gereken yerlerde kurallardan kararlara geçiş aşamasında insan gibi karar verebilmesi ama yanlış kullanım veya hataya izin vermemesi amaçlanmaktadır.

Otomatik tanımlama sistemleri günümüzde neredeyse her alanda(basit bir market sisteminden eğitim, e-devlet ve sağlık sistemlerine kadar birçok alanda) kullanılmakta ve kullanıldığı alana göre tür ve yöntemde farklılık/çeşitlilik göstermektedir. Bu türler arasında RFID sistemler ile en çok kıyaslanan barkod okuma sistemleri dâhil olmak

üzere, biyometrik sistemler (yüz tanıma sistemleri, parmak izi tanıma sistemi, ses tanıma sistemi, iris tanıma sistemi, el geometrisi tanıma sistemi) bulunmaktadır.

- Otomatik tanıma sistemleri temel olarak 5 grupta toplanabilir:
- OCR (optik karakter tanıma sistemleri)
- Akıllı Kart Sistemi
- Barkod Sistemleri
- RFID (Radyo Frekansı ile kimlik tanıma)
- Biyometrik Kimlik Tanıma Sistemleri (Yüz Tanıma, Parmak İzi Tanıma… vb.)



Şekil 4. 1: Otomatik Kimlik Tanıma Sistemleri

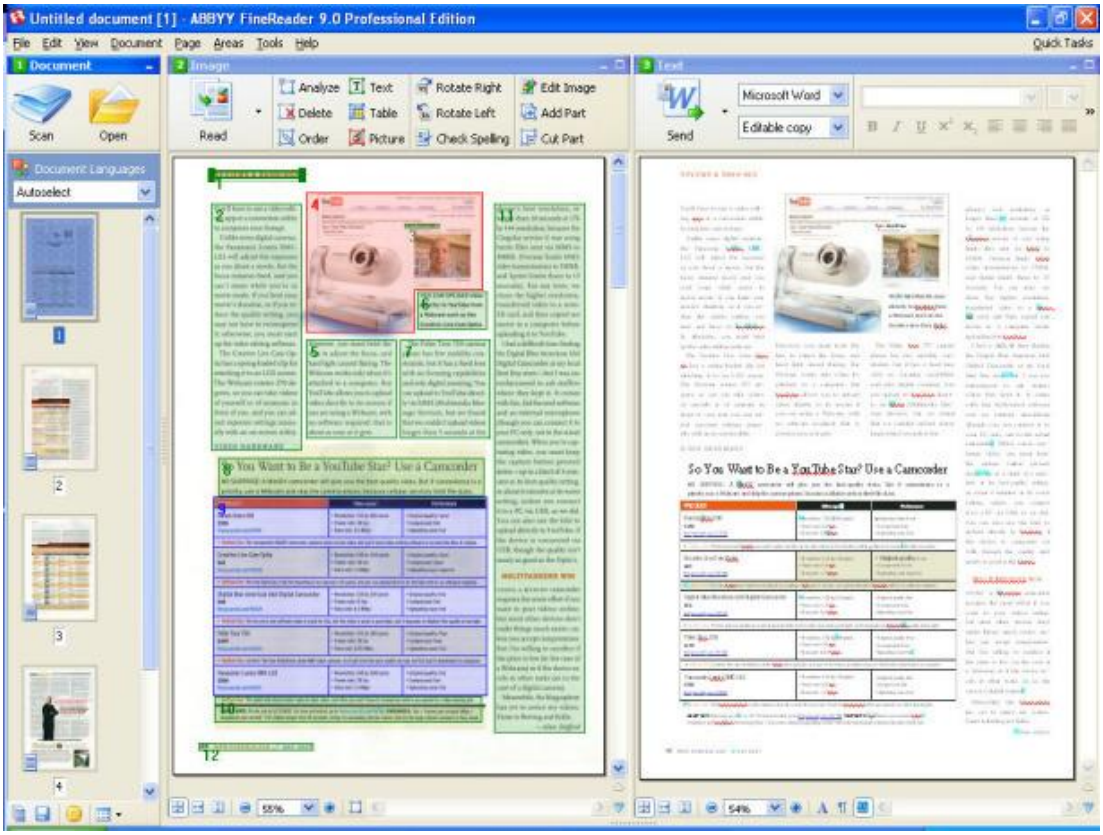
4.1 OCR (Optik Karakter Tanıma Sistemleri)

Optik Karakter Tanıma işlemi, basılı belgelerin okunarak bilgisayar metinlerine dönüştürülmesi işlemidir. Optik bir cihaz aracılığı ile taranan basılı veya el yazısı

dokümana ait karakterler kümesi sayısal görüntüye dönüştürülür. (Kır, Öz, & Gülbağ, 2011)

Kısaca OCR, taranmış kâğıt evrakları, PDF dosyaları veya dijital bir kamerayla çekilen resimler gibi değişik belge türlerini düzenlenebilir ve aranabilir verilere dönüştürülmesine olanak sağlayan bir teknolojidir. Örneğin günümüzde en sık kullandığımız tarayıcılar hatta akıllı telefon uygulamaları bu tür işlemlerin bir kısmını halledebilse de bir kitap, makale ya da bir PDF dosyasının çıkarılması siyah beyaz nokta topluluğundan başka bir şey değildir. Üzerinde düzenleme, ekleme, çıkarma gibi işlemler yapılamamaktadır. OCR sistemleri tüm bu işlemleri yapmasına olanak sağlamaktadır.

OCR belge yapısını incelemektedir. Sayfayı metin, resim ve tablo şeklinde parçalara bölmektedir. Satırları önce kelimelere sonrada karakterlere bölen bu sistemin zaman ve iş gücünden tasarruf yapma avantajını sağlamaktadır.



Şekil 4. 2: Optik Karakter Tanıma Sistemi

4.2 Akıllı Kart Sistemi

Akıllı kartlar bir plastik kart içine bir mikro kontrolör gömme kavramı içermektedir. Akıllı kartlar, kredi kartı boyutlarında içerisinde işlemci, ROM ve RAM belleği

bulunan ve bir mikroçipe sahip donanımdır. Üzerinde manyetik şerit veya barkod gibi çeşitli teknolojileri de içinde barındırmaktadır. Günümüzde kimlik doğrulama başta olmak üzere birçok gizlilik gerektiren uygulamada kullanılmaktadır.

Akıllı kartlar veri tiplerine göre;

- Bellek kartları
- Güvenlik donanımlı
- Güvenlik donanımı olmayan
- İşlemcili kartlar
- Kripto işlemcili
- Kripto işlemcili olmayan şeklinde sınıflandırılırlar.

Üzerindeki mikroçiplere göre temaslı ve temassız olarak iki çeşittir. Bu tür kartlar hiprit kartlardır. Toplu taşıma araçları temassız kartların en çok kullanıldığı alandır.
Açık anahtar yapısı ve e-imza sistemlerinde kullanan akıllı kartlar kripto işlemcili sınıfa girmektedir. Kripto işlemcili akıllı kartlar üzerinde şifreleme-şifre çözme, imzalama-imza onaylama, kart içinde bilgi yazabilme, kartın şifre ile korunması gibi hizmetler sunar. (ŞAN, 2013)

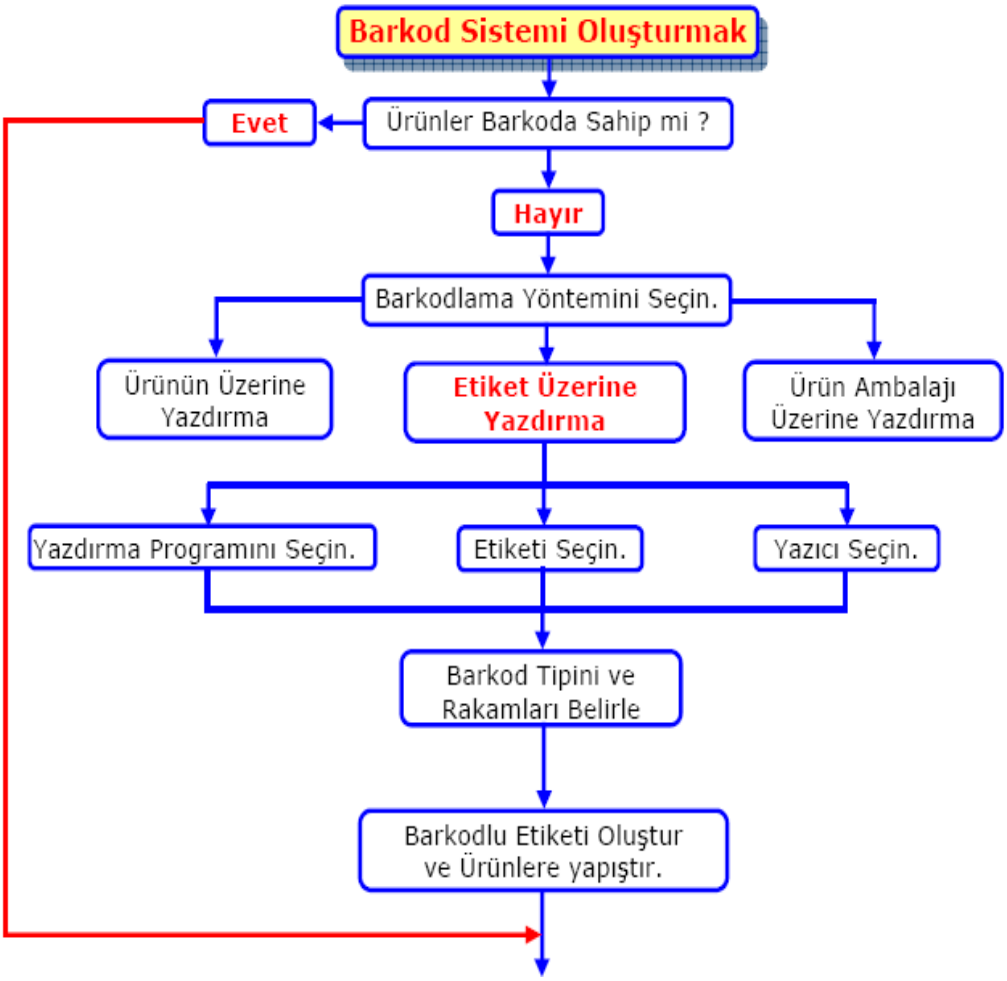
4.3 Barkod Sistemleri

Şekil 4. 3: Barkod Örneği

İngilizce 'de çubuk-çizgi anlamına gelen bar ve kod kelimelerinin birleşiminden ortaya çıkmış olan barkod kelimesi makineler tarafından okunabilen bir dildir. Farklı kalınlıktaki dik çizgi ve boşluklar makineler tarafından okunarak, verinin otomatik

olarak ve hatasız bir şekilde başka bir ortama aktarılması için kullanılan bir yöntemdir. Barkod alfabesi denilen boşluk ve çizgilerin hangi sıraya göre dizileceğine karar veren sistemi oluşturur. Birçok barkod alfabesi vardır bazısı sadece rakam içerirken bazıları rakam ve özel karakterleri içermektedir.

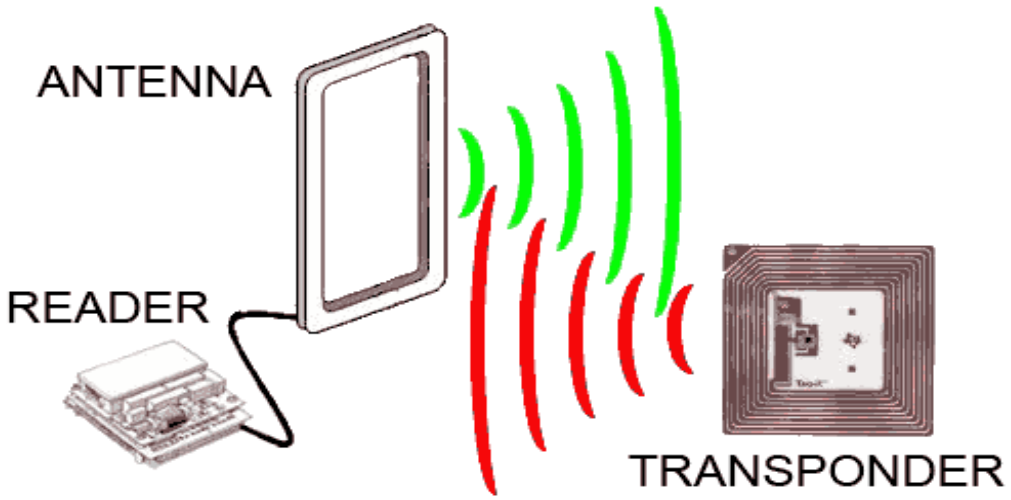
Barkod sisteminin faydalarından bahsedecek olursak benzer ürünler arasındaki karışıklığı önler, doğruluğun artması veri girişlerinin hızındaki artış maliyeti düşürecek ve karı artıracaktır, bu sistemin işlenmesi yazıcılar, okuyucular ve tüm yazılım- donanım ürünlerinin kullanım-kurulum kolaylığından dolayı basittir. (Reid, 2003)



Şekil 4. 4: Barkotlama Aşamaları

4.4 Radyo Frekansı İle Kimlik Tanıma(RFID)

Radyo frekans tanımlama (RFID) sistemleri radyo frekanslarını kullanarak duran ya da hareket halinde bulunan canlıları ya da nesneleri tek veya çok ayırt etmeksizin tanımlamakta kullanılan teknolojidir. RFID, temel olarak bir etiket ve okuyucudan meydana gelir. RFID etiketleri Elektronik Ürün Kodu (EPC) gibi nesne bilgilerini almak, saklamak ve göndermek için programlanabilirler. Ürün üzerine yerleştirilen etiketlerin okuyucu tarafından okunmasıyla bilgiler otomatik olarak kaydedilebilir veya değiştirilebilir. (Zaim, 2009)



Şekil 4. 5: RFID Bileşenleri

4.5 Biyometrik Kimlik Tanıma Sistemleri

Biyometrik kimlik tanıma sistemleri bir sonraki aşamada detaylı bir şekilde anlatılacaktır.

5 BİYOMETRİK KİMLİK TANIMA SİSTEMLERİ

Biyometri, kişileri fizyolojik ve davranışsal özelliklerine bağlı olarak tanımlayan bir bilim dalıdır. Biyometrik tanımlamalarda kriptoloji biliminden ya da bir güvenlik sisteminden bahsedilirken aslında bilgi güvenliğinden bahsedilmektedir. Bilgi, insanlarla paylaştıkça anlam kazandığına göre bilginin gizliliği sorumlu kimseler haricindeki kişilerle paylaşılmaması gerekmektedir. Bunun anlamı, bilginin bozulmadan, değiştirilmeden, başka birinin eline geçmeden sağlıklı bir şekilde ulaşması olarak düşünebilir. Bilgi sorumlu kişiler tarafından gizli değilken üçüncü şahıslar tarafından gizlidir.

Biyometrik sistemler yıllar öncesinden kullanılmakta iken yakın zamanlarda araştırmacıların kişiler hakkında fiziksel ve karakteristik özelliklerinin suça eğilimlerini araştırması ile hız kazanmıştır. Biyometrik sistemlerin uygulama alanları günümüzde oldukça geniştir. Özellikle kriminal amaçlı teşhis ve tespit uygulamaları, kredi kartı uygulamaları, elektronik imza bunların başında gelmektedir.

Biyometrik sistemlerde bireylerden alınan parmak izi, iris, yüz tarama gibi örnekler, refarans olarak belirlenen bölümleri ve göstergeleri vasıtasıyla elektronik sistemlerin anlayacağı sayısal verilere dönüştürülüp şifrelenerek veri tabanına/depo aygıtlarına kaydedilmektedir. Daha sonra sisteme girmek isteyen bu kullanıcıların önceden vermiş oldukları örneklerdeki referans noktaları ile giriş esnasındaki örneklerin referans noktaları karşılaştırılarak her iki kayıtın uyumluluğu kontrol edilir. Sistemin güvenirliliğini belirleyen en önemli etken ise, belirlenen referans noktalarının fazlalığıdır. Ama maksimum seviyede alınacak referans noktasından daha fazla referans noktası belirlenmesi sisteme ekstra yük olacağından sistem geliştiricileri tarafından tercih edilmemektedir. (Varol & Cebe, Yüz Tanıma Algoritmaları, 2011)

Şifreleme yönteminin hızla artan güvenlik ihtiyacını karşılamayacağı anlaşıldığından biyometrik sistemlerin(parmak izi, iris, yüz tarama vb.) geliştirilmesi kaçınılmaz hale gelmiş ve hız kazanmıştır.

Biyometri bir diğer ifadeyle fertleri ayırt eden ölçeklendirilebilen davranışsal ve psikolojik karakterlerin kimliklerini tespit etmede kullanılabilen bilgisayar kontrollü

sistemlerdir. Biyometrik sistemler ferdin bir tek kendinin sahip olduğu ve başkalarından ayıran fiziki veya davranış özelliklerinin bilinmesi prensibiyle çalışır. Bu sistemde el geometrisi ve parmak izinin incelenmesi, konuşma ve ses analizleri, iris tanınması, yüz özelliklerinin karşılaştırılması gibi süreçler mevcuttur. Biyometrik teknolojiler çalışma yapısı olarak benzerlik gösterirler ve hepsi aynı mantık üzerinde çalışırlar. İlk olarak veriler alınır ve bu veriler sayısal formata çevrilerek ilgili alanda saklanır. İstenildiği zaman alınan bu veriler ile ilgili birey hızlıca eşleştirilir ve bir sonuca varılır. Bu sistemler çok yüksek hıza sahip olduklarından çok kısa sürede birçok eşleştirme yapabilirler.

5.1 Biyometrik Sistemlerin Özellikleri

Güvenlik unsuru birçok teknolojide olduğu gibi biyometrik sistemlerin gelişmesinde de en önemli unsur olmuştur. Bütün biyometrik sistemlerin beş ana özelliğe sahip olması gerekmektedir. (Ergen & Çalışkan, Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri, 2011)

Bunlar;

Evrensellik: Yeryüzünde yaşayan herkes biyometrik özelliklere sahiptir.
Eşsiz olma: Her bireyde biyometrik karakteristik farklı bir şekildedir.
Süreklilik: Var olan karakteristik zamanla değişmemektedir.
Elde edilebilirlik: Biyometrik özellikler bazı pratik cihazlarla ölçülebilirdir.
Kabul edilebilirlik: Fertler cihazlar tarafından ölçülen biyometrik özelliklerine itiraz edemezler.

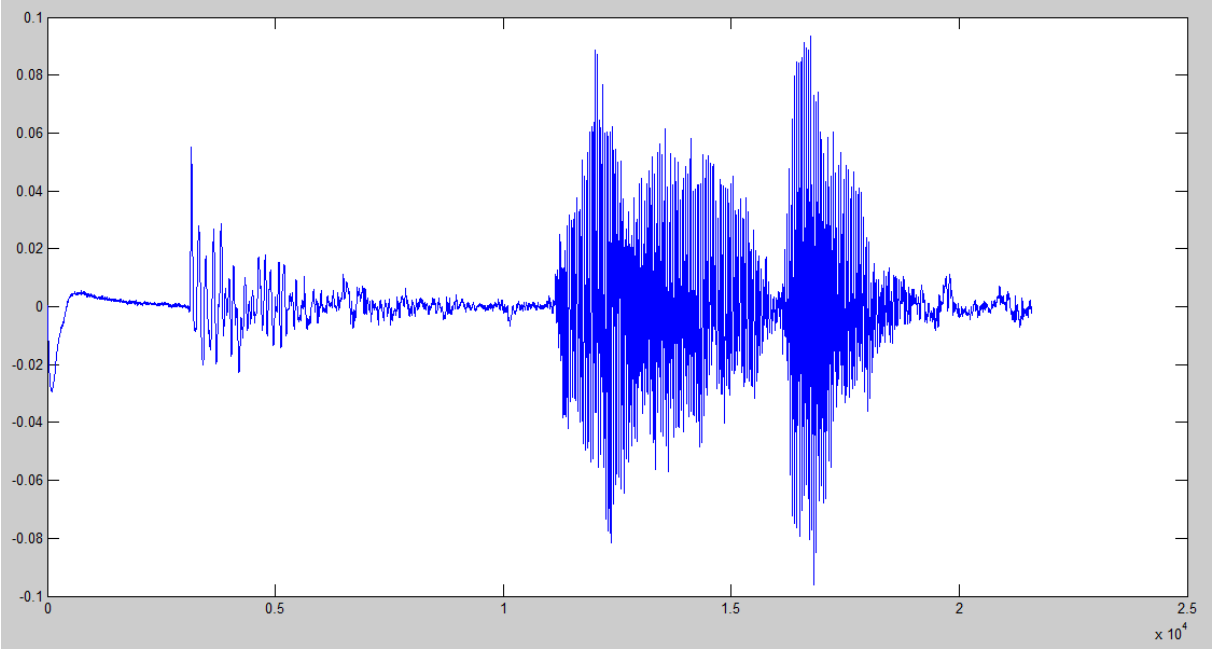
5.2 Biyometrik Tanıma Sistem Çeşitleri

5.2.1 Ses tanıma

1950'li yılların sonlarından bu yana üzerinde çalışılan ses tanıma sistemi Microsoft tarafından teknolojik bir devrim olarak nitelendirilmiştir. Bu alanda, temelde ses tanıma sistemi tarafından yapılan iş ses/konuşma alarak ne söylendiğini tahmin etmektir. Yani test edilen ses sinyallerinde bulunan ve tanınması istenilen ses sinyallerine ait unsurlar, farklı sayısal ses işleme yöntemleri uygulanılarak belirlenir.

Ses tanıma sistemleri birbirinden farklı birçok alt problem içerir.

Konuşmacının tanınması, konuşmacının belirlenmesi, konuşmacıya bağımlı/bağımsız tanıma, ayrık kelime tanıyabilme, anahtar kelime bulma ve sürekli ses tanıma. Konuşmanın analiz edilmesinde ya da tanınmasında ses olarak girilen verinin metne çevrilmesi üzerinde çalışılmaktadır. Sayısal veriye çevirme işlemi sırasıyla örnekleme, nicelendirme ve kodlama aşamalarıdır. (Yalçın, 2008)



Şekil 5. 1: Ses Tanıma Sistemleri

5.2.2 Retina ve iris tanıma

Bu teknoloji 1980' li yıllardan bu yana kullanılmaktadır. Bu teknolojiyi diğer biyometrik teknolojilerin önüne geçiren en önemli özellik, gözün yapısında diğer biyometrik özelliklere göre daha az deforme olması ve ömür boyunca göz yapısının değişmiyor olmasıdır. Hata oranı yok denilecek kadar az olan bu teknoloji gümrük gibi ülke girişlerinde ve kimlik doğrulamasının hata kabul etmez olduğu alanlarda uygulanmaktadır.

Göz yuvarlağının arkasında bulunan ve damarlarla kaplı olan ağ yapısı retinadır. Görme ise bu ağ yapısına gelen ışınların beyne ilettiği sinyaller ile gerçekleşir. Retina taramasında parmak damar tanıma ve el geometrisinde olduğu gibi harita şeklinde

görüntüsü alınır ve sayısal verilere çevrilerek kaydedilir. Ve istenildiği zaman eşleştirme ve karşılaştırma işlemi yapılır. Fakat parmak izi tanıma teknolojisinde olduğu gibi kızılötesi ışınlar kullanarak canlı-cansız varlıkları test edemediği için canlı olmayan varlıkları denetleme yeteneği yeterli güvenlik sağlayamamaktadır. (Aktaran: (Varol & Cebe, Yüz Tanıma Algoritmaları, 2011))

Göz tarama yöntemiyle yapılan farklı bir tarama ise iris taramasıdır. İris tarama yönteminde kaslardan oluşan ve gözdeki renkli kısım olan iris tabakasının fotoğrafı çekilir ve bu şekilde görüntü işlenmesine tabi tutulan bir yöntemle çalışır. Alınan bu görüntü kaydında yaklaşık 200 tane referans noktası seçilir. Daha sonra bütün biyometrik tanıma sistemlerinin çalışma yapısında olduğu gibi var olan kayıtlar ile yeni görüntülerin referans noktaları eşleştirilerek onay işlemi sağlanır. (Varol & Cebe, Yüz Tanıma Algoritmaları, 2011)

Bu sistemin dezavantajları;

- Kurulum ve bakım maliyetlerinin yüksek olması,
- Gözlük ya da lens kullananlarda hatalı okuma yapma,
- Odaklanma sorunu sebebiyle doğru açının tutturulamaması,
- Gözleri görmeyen bireylerde tanımlama yapılamaması şeklinde sıralanabilir.

Şekil 5. 2:İris Tanıma Sistemi

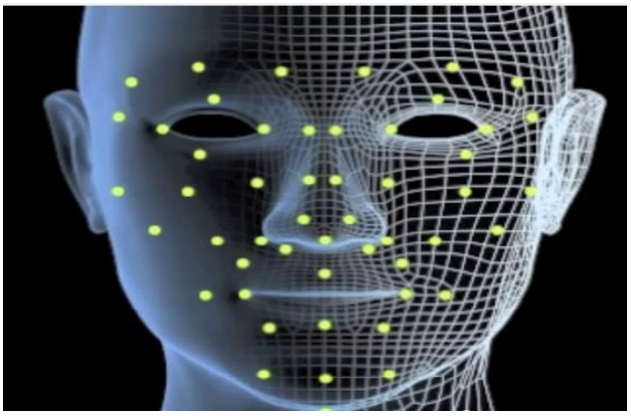
5.2.3 Yüz Tanıma

Biyometrik teknolojiler arasında devrim niteliğinde sayılabilecek olan bu teknoloji ilk olarak askeriyede kullanılmıştır. Uydu, kamera gibi görüntü araçlarından gelen görüntüleri suçlu yakalamak ya da takip gibi işlerde kullanılmaktadır.

Yüz tanıma sistemi, son zamanlarda talep oranına bağlı olarak çok popüler bir tanıma sistemi haline gelmiştir. Öyle ki günümüzde neredeyse tüm bilgisayarlarda kullanıcı girişi yapılabilmesi amacıyla yüz tarama sistemi kullanılmaktadır.

Yüz tarama sisteminde de tıpkı iris taramadaki gibi yüzün belirli referans noktaları alınıp saklanıp daha sonra karşılaştırılması esasına dayanır. Yüz taramanın dezavantajları, yüzün geometrik şeklindeki bozulma (kilo alma – verme…) sonucunda okumanın imkânsızlaşmasıdır. Ayrıca taranan kısmın irise oranla çok büyük olduğundan, depolama ve kontrol işlemlerinin hem çok uzun hem de maliyetli olması olarak tanımlanabilir.

Buna rağmen yüz tarama sistemi; askeri ve istihbarat birimleri, polis merkezleri, hava alanları ve kasalar gibi yüksek güvenlik gerektiren alanlarda etkin olarak kullanımı armaktadır.



Şekil 5. 3: Yüz Tanıma Sistemi

5.2.4 El Geometrisi

Bu sistemde kişinin elinin ya da kullanılan sisteme göre iki parmağının geometrik yapısı analiz edilir. Belirleyici özellikleri parmağın uzunluğu, genişliği ve büküm noktalarıdır. El geometrisi doğruluk oranı yüksek olmasına karşın dezavantajlarının

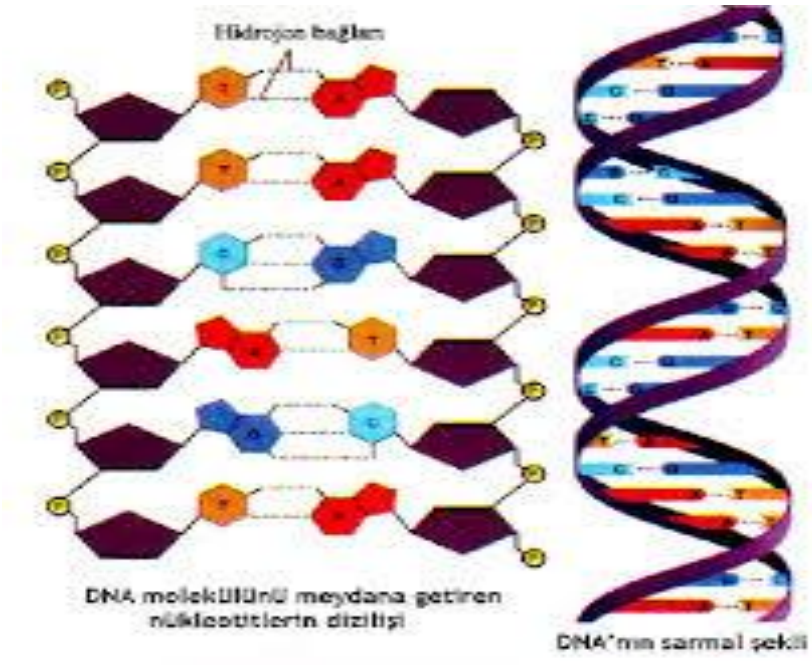
çok olmasından dolayı pek tercih edilmemektedir. Bunlar arasında el geometrisi alım sırasında işlemin uzun sürmesi ve büyük ve maliyetli cihazları en baş sebepleri arsında gelmektedir.

El geometrisi, kişi tanımada kişilerin el şekillerini kullanan bir biyometrik özelliktir. Bir biyometrik sistem de, el geometrisine dayanarak ana hat oluşturulur ve gerçekleştirilir. İşlem önceliği (siyah-beyaz içindeki renk görüntüsünü değiştirdiği gibi, ayrıt sezimi ve dış hatları çıkarma) ve ölçüm algoritmaları el görüntüsüne uygulanır. (Ergen & Çalışkan, Biyometrik Sistemler ve El tabanlı Biyometrik Tanıma Karakteristilkleri, 2011)

Şekil 5. 4: El Geometrisi Tanımlama Aleti

5.2.5 DNA tanıma

Kişinin saç, tırnak, deri, kan veya herhangi bir biyolojik materyali incelenerek ele alınarak içerisindeki DNA moleküllerinin dizilimine göre incelenir. Parmak okuma sistemine destek olarak yanık, kesik benzeri sebeplerden ötürü tanımlanamayan durumlarda kullanılan bu sistem aynı zamanda birçok dezavantaja da sahiptir. Bu dezavantajlar arasında DNA' nın elde edildiği doku örneği temel alındığı için dokunun kirlenmesinden kaynaklı kalitesinin düşmesi, 24 saatte gerçekleştirme zorunluluğundan kaynaklı yüksek maliyet gibi sebepler sayılabilir.



Şekil 5. 5: DNA Örneği

5.2.6 Parmak İzi Tanıma

Şekil 5. 6: Parmak İzi Örneği

Biyometrik uygulamalar da belki de en önemlisi olarak tanımlayabileceğimiz parmak izi uygulaması, taklit edilemez bir bilgi kaynağıdır. Tez konum olan parmak izi tanıma sistemleri ve bu sistemlerle oluşturacağım on-line sınav giriş sistemi bir sonraki bölümde ayrıntılı bir şekilde bahsedilecektir.

Çizelge 1: Birey Ayırt Etme Karşılaştırma Tablosu

Biyometrik Kaynak	Yaygınlık	Ayırt Ediciliği	Dayanaklılık	Bulunabilirlik	Performans	Kabul Edilebilirlik	Sistemi Yanıltma
Parmak İzi	Orta	Yüksek	Yüksek	Orta	Yüksek	Orta	Yüksek
Yüz Tanıma	Yüksek	Düşük	Orta	Yüksek	Düşük	Yüksek	Düşük
El Geometrisi	Orta	Orta	Orta	Yüksek	Orta	Orta	Orta
İris	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Yüksek
Retina	Yüksek	Yüksek	Orta	Düşük	Yüksek	Düşük	Yüksek
Ses	Orta	Düşük	Düşük	Orta	Düşük	Yüksek	Düşük
DNA	Yüksek	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük

Yukarıdaki tabloda;

Yaygınlık; her biyometri kaynağının insanlarda bulunma yaygınlığını gösterir.

Ayırt Edicilik; bu kaynakların bireyleri ayırt edebilme başarısını işaret eder.

Dayanıklılık; bu elemanların zamana ve yaşlanmaya karşı direncini ifade eder.

Bulunabilirlik; bu kaynakların elde edilip işlemesinin kolaylığını gösterir.

Performans; biyometri elemanlarının doğruluk yüzdesi, hızı ve sağlamlığını anlatır.
Kabul Edilebilirlik; gündelik hayatta kabul edilme derecesini gösterir.
Sistemi Yanıltma; sütunu ise bu kaynakları kullanarak sistemi aldatabilme ihtimalini belirtir.

Yukarıdaki tabloda bireylerin birbirinden ayırt edilmesinde kullanılan biyometrik sistemlerin karşılaştırılması yapılmıştır.

6 MATERYAL VE YÖNTEM

6.1 Tarihçesi

İlk olarak, Nehemiah Grew (1684), Marcello Malpighi (1686) ve J. E. Purkinje (1823) gibi anatomistler insanların parmaklarındaki kıvrımların bazı özellikleri bulunduğuna dikkat çekmekle beraber, bu izlerden faydalanma metotlarını belirtmemişlerdir.
Modern manada parmak izi tespiti ve faydalanma 1880'de Henry Faulds ve Wiliam James Herschel adlı iki İngiliz bilim adamı, Nature adlı bir ilmi mecmuada parmak izi hakkında makale yazmışlardır. Bu bilginler önceleri pişmiş çömleklerdeki parmak izleriyle ve matbaa mürekkebiyle parmak izi alma metoduyla uğraştılar. Günümüzde kullanılan parmak izi metodu da aynı esasa göre yapılmaktadır.
İlerleyen dönemlerde parmak izi üzerine çalışan Galton, parmak izinin ebeveynden kalıtımsal olarak geçmediğini açıkladı. Dolayısıyla her bireyin parmak izinin birbirinden farklı olduğu ve her bireye ait parmak izinin de öznel, tek ve değişmez olduğu ilkesi o zamandan kaydedilmiştir.
Sir Francis Galton parmak izleri hakkındaki bilimsel incelemelerini tamamlamış ve 1892 de yayınlamıştır. Genel itibariyle parmak izleri tanımlamalarında Galton' un çalışması kullanıldı. Sir Francis Galton kendi sınıflandırmasını oluştururken Punkinje' nin dokuzlu sınıflandırma modeline ait örnekleri de alarak bu alanda yeni terimler oluşturdu. Genetik olarak birbirinden alakasız bireylerden başlayarak çift yumurta ikizlerinin de karşılaştırmasını yaparak parmak izlerinin kalıtsal yönlerinde çalışmalar yapmıştır.

Parmak izinin kişiyi tanıma ve kimlik belirleme amacıyla kullanma düşüncesi, 1890´lı yıllarda, İngiliz polis şefi olan ve Hindistan´da görev yapan Sir Edward Henry tarafından ortaya atılmıştır. Bu biyometrik kimlik belirleme yöntemi günümüzde en yaygın olarak kullanılan yöntemdir.

6.2 Parmak İzi Teknolojisinin Çalışma Mantığı

Bütün biyometrik ve akıllı sistemlerde olduğu gibi parmak izi tanıma sistemlerinde de ilk olarak parmak izinin sisteme kaydedilmesi gerekir. Kullanıcının yapmak istediği işlemde kullanacağı parmak izini referans olarak sisteme kaydetmesi ve daha sonra sistemi kullanacağı zaman sisteme kaydetmiş olduğu parmak izini sisteme tanıtması(cihaza okutması) gerekir.

Parmak izi sistemleri, parmak ucu derisinde olan çıkıntıların parmak izi okuyucu cihazlar aracılığıyla okunması sonucu, parmak ucu çıkıntılarının resmini alıp sayısal verilere dönüştürmesi sonucunda bu veriler üzerinden işlem yapmayı sağlayan sistemlerdir.

Parmak izi okuma cihazı kurulduktan sonra sistem için hazırlanmış olan yazılım aracılığı ile iletişim sağlanır. Parmak izi okuma cihazı okuma üzerindeki sensör, parmak izini elektrik dalgaları aracılığıyla tanılar(parmak ucu çıkıntılarını resmedip sayısal formata çevirir.).

Cihaz tarafından tanımlanan parmak izi (resmedilip sayısal formata dönüştürülen veri) ile veri tabanında kayıtlı olan parmak izleri(veri tabanında kayıtlı sayısal format veriler) karşılaştırılıp eşleşen parmak izi bulunur.

Cihazdan gelen parmak izi ile veri tabanında kayıtlı olan parmak izi eşleştikten sonra istenilen işlemler gerçekleşir.

Bu sistemin çalışması;

İlk olarak,

- Parmak izini okuma ve sayısal formata çevirme
- Okunan parmak izinden bilgi üretme
- Üretilen bilginin saklanması

Daha sonra

- Saklanan bilgi ile giriş bilgilerin karşılaştırılması
- Sistemin kontrolü ve sisteme giriş

Şeklinde gerçekleşir.

6.3 Parmak İzi Teknolojisinin Temel Özellikleri ve Bileşenleri

Parmak izi teknolojisi, parmak izi okuma cihazından aldığı veriler ile veri tabanında kayıtlı verilerin karşılaştırılması sonucu istenilen işlemleri gerçekleştirme mantığına dayalı çalışma sistemine sahiptir.

Bu sistemde iki temel bileşen mevcuttur.

Bunlar;

Yazılım ve donanımdır.

6.3.1 Yazılım

Parmak izi tanıma sisteminin yazılımı parmak izi okuma cihazından gelen parmak izlerini(sayısal formata dönüştürülmüş verileri) işlemeye yarar. Yazılım aracılığıyla cihazdan gelen bilgiler hazırlanan sistemin ihtiyaç ve özelliklerine göre işlenir.

6.3.2 Donanım

Parmak izi teknolojisi ile oluşturulan sistemlerin temel donanımı parmak izi okuma cihazıdır. Parmak izi cihazları kullanıcıların parmak izi kayıtlarını alır ve kullanım anında veri tabanında kayıtlı olan parmak izleri ile eşleştirerek yapılacak işlemi otomatik olarak gerçekleştirir.

6.4 Parmak İzi Tanıma Teknolojisinin Dezavantajları

Parmak izi tanıma sisteminin en büyük dezavantajı parmak izi taklit problemidir. Bu problem parmak izinin alındığı parmağın canlılığını test edecek gelişmiş sensörlerin kullanılması ile giderilebilir.

Parmak izi tanıma sisteminde RFID sistemlere göre yüksek teknoloji kullandığından üretim maliyetleri de bu bağlamda yükselmektedir. Dolayısı ile donanım fiyatı diğer sistemlere göre yüksektir.

Islak ve pürüzlü zeminlerde parmak izi alınamamaktadır. Dolayısıyla parmak izi alma işlemi daima kuru, pürüzsüz ve dış etkenlerden korumalı bir alanda yapılması gerekmektedir.
Yağlı veya kirli parmaklardan parmak izi alma zorluğunun yaşanması bir diğer dezavantajdır. Fakat bu problem doğru algoritmalar ve yüksek kaliteli sensörler en düşük seviyeye indirilebilir.

6.5 Parmak İzi Tanıma Teknolojisinin Avantajları

Otomatik kimlik tanıma sistemlerinde ve özellikle kartlı geçiş sistemlerinde olduğu gibi kişiler yanlarında kart, barkot vb materyal taşımazlar. Ya da kullanıcı adı ve şifrelerini akıllarında tutmak zorunda kalmazlar. Tüm biyometrik sistemlerde olduğu gibi parmak izi tanıma teknolojisinde de gerekli giriş bilgileri bireyin kendisindedir. Parmak izi tanıma teknolojisinde kullanıcılara ait bilgiler, kişinin parmak uçlarına tanımlanır. Dolayısıyla kartı unuttum, kaybettim gibi mazeretler tamamen ortadan kalkar. Parmak izi tercihinde kayıp, unutma, çaldırma gibi mazeretler sona erer.
Başkasının kimliğini kullanma gibi sorunların çözümü için %100 güvenlidir.
Geleneksel sınav sistemlerinde yapılan kimlik kontrolü için ayrılan zaman kaybı ortadan kalkar.
Parmak izinin başkasına transfer edileme, kaybedilme, çalınma ve kopyalanma gibi riskleri yoktur.

Parmak izi okuma teknolojisinin teknik avantajları;

- Hızlı Tanıma
- Bağımsız (standalone) ve/veya network üzerinden eş zamanlı çalışma
- Tümleşik ve/veya RFID Desteği
- Web & Network desteği
- Yüksek parmak izi kapasitesi
- Yüksek hareket kaydı
- Tek ve/veya çoklu geçiş kontrolü
- Çoklu iletişim seçeneği (TCP/IP, RS-232, Rs485, USB)
- Sarfı olmayan ekonomik çözüm
- Maksimum güvenlik ve güvenilirlik

6.6 Parmak İzi Teknolojisinin Kullanıldığı ve Kullanılabileceği Alanları

Parmak izi tanıma teknolojisi günümüzde birçok alanda kullanılmaya başlanmıştır. Özellikle kartlı personel takip sistemleri parmak izi tanıma sistemlerine dönüştürülmeye başlanmaktadır.

- Hasta kimliklendirilmesi (hastanelerde hasta takiplerinde)
- Personel Kimliklendirilmesi(Fabrika vb. personel takiplerinde)
- Öğrenci Kimliklendirilmesi(Üniversiteler ve okullarda öğrenci takip)
- Gümrük noktaları Yurda giriş ve çıkış kontrollerinde
- Kamusal alanlar
- Bilgi işlem vb. alanlarda yoğun olarak kullanılabilmektedir.

6.7 Parmak İzi ve Güvenlik

Şekil 6. 1: Parmak İzi Görüntüsü

Parmak izi, parmak ucu derisinde, göz ile görülebilen çıkıntıların meydana getirdiği şekillerdir. Dış deriye ait bu çıkıntılara hat (papilla) denir. Parmaklar dikkatlice incelendiğinde, parmak izlerinin, birçok hattın farklı biçimlerde bir araya gelmesiyle oluştuğu görülmektedir.

Çocuğun anne karnında gelişmeye başlamasından itibaren parmağın değişmeyen ve aynı kalan izlerin bulunduğu bölgeye papilla denmektedir. Bu bölgenin üzerinde

bulunan epidermis olarak isimlendirilen derinin tahrip olduğu durumlarda kendini yeniden oluşturabilme özelliği vardır.

Amerikan Federal Araştırma Bürosu(AFAB) tarafından yalpan araştırmada 250 Milyondan fazla kişiden parmak izi alınmış ve bunların içinde birbirinin aynı olan hiçbir parmak izine rastlanılmamıştır. Bu araştırma sonucu parmak izlerinin benzemezliğini kanıtlayan bir bulgudur.

Yaşayan, doğacak veya ölmüş hiçbir insanın parmak izi aynı değildir. Her ferdin parmak izi farklıdır, ferde özeldir ve tekrarı da yoktur. Bunun yanında her kişinin tüm parmaklarının izleri de birbirinden farklıdır.

Tek yumurta ikizleri de dâhil olmak üzere her bireyin parmak izleri farklıdır. Dolayısıyla, insanlara kimlik oluşturulurken gen olarak DNA sarmalı fiziki olarak ise parmak izleri ile kodlanır. Bu dokusal kodlama sistemi, günümüzde teknolojik olarak kullanılan barkod sistemine benzetilebilir. Deri üzerindeki yanıklar, derin kesikler ve yaralar gibi olağan dışı durumlar olmadığı müddetçe, parmak izlerindeki bu hatlar, insan hayatı boyunca değişmez. Parmak izlerinin bu değişmez ve herkes için farklı özellikleri (tek yumurta ikizlerinde bile bu farklılık mevcuttur), parmak izlerini kimlik tespiti konusunda çok kullanılan bir özellik haline getirmiştir. Doğru tanımlama için parmak izinin küçük bir parçası bile yeterli olmaktadır.

Parmak izleri, tanımlamanın doğruluğu bakımından yeterinde verimli bir şablon oluşturmak için oldukça karmaşık yapıya sahiptir. Daha verimli bir güvenlik sistemi oluşturulmak istenirse, birkaç parmak izi(aynı kişiye ait farklı parmaklar) aynı anda tanımlanabilir. Çünkü her parmağın izi birbirinden farklıdır. Günümüzde bazı ülkelerde sağ ve sol ellerin işaret parmaklarının tanıtılması yeterli görülmektedir. Parmak izi taraması, hızlıdır ve bireyleri rahatsız edecek herhangi bir unsuru yoktur. Parmak izi tarayıcı cihazlar, kolay bir şekilde küçültülebilir. Aynı zamanda düşük maliyetle çok sayıda üretilebilirler. Bunun yanında bazı insanların parmak izlerini görüntülemek zordur. Yeni teknolojilerde, parmak izlerini sadece görüntü olarak değil de, hem görüntü hem kod veya sadece kodlayarak saklamak da tercih edilmektedir.

Parmak izi okuyucularının bir kısım güvenlik özellikleri aşağıdaki gibidir.

Hatalı Red Oranı: Kabul edilmesi gereken bir parmak izinin reddedilme olasılığıdır. Bu oran, yaklaşık % 1,4’ dür.

Hatalı Kabul Oranı: Kabul edilmemesi gereken bir parmak izinin kabul edilme olasılığıdır. Bu oran % 0,001' dir.

Çözünürlük: Birim yüzey alanında kaç noktanın taranabildiğini ifade eder. Dot Per Inch (dpi) olarak tanımlanır.

Parmak İzi Kaydolma Süresi: Kabul edilmesi gereken bir parmak izinin algılayıcıya tanıtılma süresidir. Ortalama parmak izi okuma süresi 3 saniyeden kısadır(<3 sn).

Parmak İzi Doğrulama Süresi: Okutulan bir parmak izinin onaylanma süresidir. Bu süre ortalama 1 saniyedir(<=1).

Tolere Edilebilen Parmak Hareketi: Parmak izinin parmak izi okuyucusuna okutma açısıdır. Ortalama 18 derecelik sapmalar tolere edilebilir(+/- 18 derece).

Çalışma Sıcaklığı: Parmak izi okuyucu cihazın çalışma sıcaklığıdır. Ortalama -10/+50 °C.

Güç Tüketimi: Operasyon ve uyku modu olarak iki ayrı şekildedir. Operasyon modunda 35 miliA, uyku modunda 20 mikroA.

G/Ç Desteği: Sensörün hangi G/Ç arabirimlerini desteklediğini belirtir. USB, Paralel, SPI (Serial Peripheral Interface) gibi.

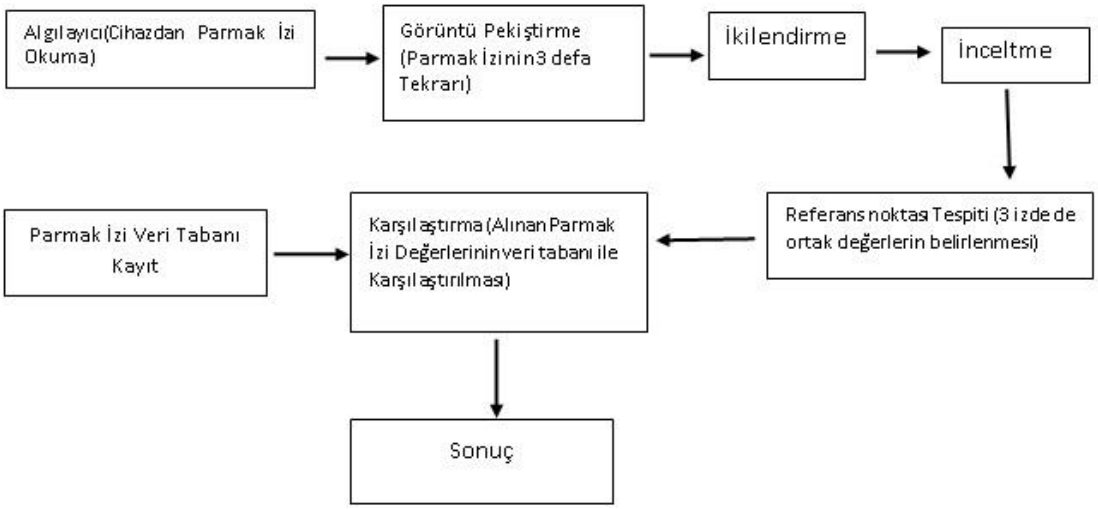
7 PARMAK İZİ TANIMA ALGORİTMASI

Parmak izi tanıma yöntemiyle kimliklendirme tekniği 100 yılı aşkın süredir kullanılmaktadır. İlk olarak Amerika ve Avusturalya' da 1980'lerin ortasında otomatik parmak izi tanıma teknolojisi tanıtılmıştır. İlerleyen zamanlarda birçok ülkede geliştirilen farklı algoritmalar ve teknolojik sistemlerle kullanılmaya başlanmıştır. Genel itibariyle parmak izi tanıma teknolojisi, parmak izinde bulunan referans noktalarının ve bu referans noktalarına ait parametrelerin eşleştirilmesi/karşılaştırılması yöntemine dayalı çalışır. Parmak izi tanıma teknolojisinde gerçekleştirilen işlemler aşağıda verildiği şekilde sıralanabilir:

- Parmak izi alınır ve sayısal verilere dönüştürülür,
- Parmak izi üzerinde bilgi taşıyan, üzerinden işlem gerçekleştirilecek olan bölüm arka planda ayrılır.
- Parmak izi temizlenir ve iyileştirilir,
- Resin ikili resme çevrilir,
- İkili resim inceltilir,
- Referans noktaları bulunur ve bu referans noktaların parametreleri belirlenir,
- Sadece referans noktaları elimine edilir,
- Son olarak sistemin başarısı değerlendirilir,

Parmak izi eşleştirmenin özel metotları başlıca 5 evreye bağlıdır.

- Görüntü pekiştirme
- Sırt algılama
- İkilendirme
- İnceltme
- Referans noktalarının tespiti



Şekil 7.1: Parmak İzi Tanıma Algoritması

8 YÖNTEM

8.1 Parmak İzi Tanıma Teknolojisi ile Güvenli Online Sınav Giriş Projesi

Bu çalışmada Parmak İzi Tanıma Teknolojisi(PİTT) İle Online sınav girişi uygulaması gerçekleştirilmiştir.

Çalışmada merkezi bir veri tabanı ve parmak izi tanıma sistemiyle güvenli bir şekilde otomatik olarak sınav girişinin işletilmesi ve kontrol edilmesi amaçlanmıştır. Donanım olarak kullanılan parmak izi okuyucu ile de her bilgisayarda ayrı ayrı olmak üzere sınav giriş kontrolü yapılmıştır. Böylece klasik olarak yapılan kimlik kontrol sistemine alternatif olarak, çevrim içi işletilebilen, kontrol edilebilen ve otomatik olarak öğrenciyi tanıyabilen, parmak izi ile kimlik oluşturma ve öğrenci tanıma uygulaması gerçekleştirilmiştir. Bu sistemle tüm işlemler internet üzerinden veya yerel ağ üzerinden otomatik olarak yapılacağından, kimlik kontrolü esnasında zaman kazandıracaktır. Ayrıca sınav güvenliği de artırılacaktır. Özellikle çok katılımlı sınavlarda gözetmenler tarafından tanınmayan öğrenciler sistem tarafından tanınacaktır. Biyometrik tanıma vasıtasıyla parmak izi kullanılarak oluşturulan kimlikler ile öğrenciler sisteme kaydedilecek ve bu merkezi yönetim sayesinde öğrenci girişleri otomatik yapılacaktır. Böylece başkasının yerine sınava girmek isteyenler, sistem tarafından otomatik olarak tanınacak ve veri tabanında kimlik bilgileri olmayan kişilere sınav ekranı açılmayacaktır. Öğrenciler gözetmenler tarafından kabul edilip öğrenci kimliklerindeki hileler fark edilmese bile bu öğrenciler sınav giriş sistemi tarafından fark edilecek ve sınav ekranın açılması sistem tarafından engellenecektir.

8.2 PİTT ile Güvenli Sınav Giriş Uygulamasında Kullanılan Yazılım Yapısı

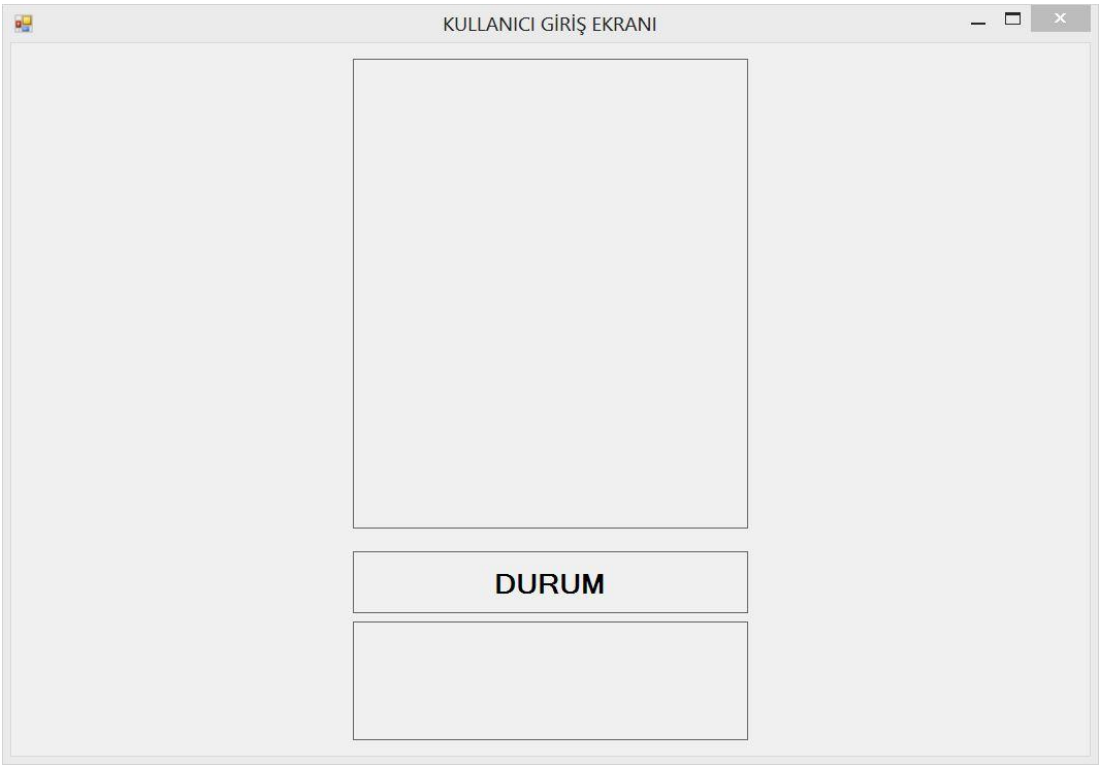
Php dili ile geliştirilmiş olan ve dematrasyonda kullandığımız sınav ekranına Microsoft Visual Studio ortamında C# dili kullanılarak cihaz ile iletişime geçip

doğrulama işlemi sonrası php dili ile geliştirilmiş olan sınav ekranına geçiş işlemi için geliştirilmiştir. Veri tabanı olarak MySql Server seçilmiştir.

Bu projede C# dili kullanılarak cihazdan gelen parmak izi bilgileri ile web tabanlı sınav sisteminde kayıtlı kullanıcı bilgilerini yöneten bir sistem geliştirilmiştir.
Proje yönetici ve kullanıcı ekranı olmak üzere iki görevlidir.

8.3 Kullanıcı Giriş Ekranı

Yönetici tarafından kayıt işlemi yapılmış olan kullanıcıların sınava giriş işlemi yapma durumlarında kullandıkları ara yüzdür. Bu ara yüz cihazdan gelen parmak izi ile veri tabanında kayıtlı parmak izlerini karşılaştırıp eşleştirmekte ve kullanıcının sınava girişini onaylamakta veya onayı engellemektedir.



Şekil 8.1: Kullanıcı Giriş Ekranı

Kullanıcı Application ekranı iki ara yüzden meydana gelir. Bunlardan birisi parmak izi bekleme ekranı diğeri ise doğrulama sonrası web tabanlı sınavın gösterileceği ekrandır.

Şekil 8.1’ de kullanıcı bekleme ekranı görülmektedir.

Parmak izi bekleme ekranı kullanıcıların parmak izlerini okutmasını beklediği ekrandır. Bu ekranda kullanıcıların parmak izlerini cihaza okutması sonrası doğrulamak için veri tabanında karşılaştırmaları yapar.

Kullanıcı parmak izini cihaza okuttuktan sonra şekil 8.2' de olduğu gibi durum kısmının üst tarafındaki kutucukta parmak izi görüntüsü alt tarafındaki kutucukta ise başarılı veya başarısız olma durumları belirtilmektedir.

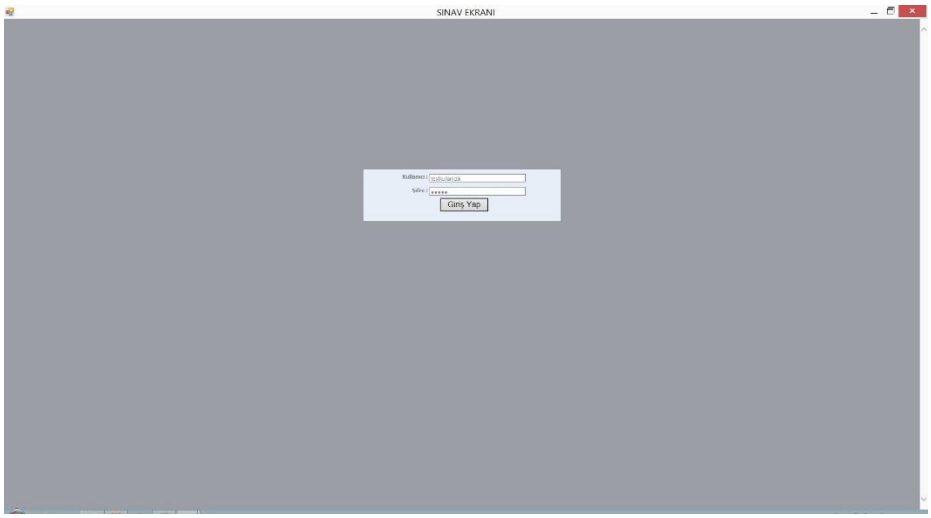
Parmak izi cihazından gelen parmak izi ile veri tabanındaki parmak izlerinin karşılaştırılması olumsuz olduğu durumlarda şekil 8.2' deki gibi doğrulama başarısız mesajı verecektir.

Şekil 8.2: Kullanıcı Giriş Ekranı Başarısız Durum

Parmak izi cihazından gelen parmak izi ile veri tabanındaki parmak izlerinin karşılaştırılması olumlu olduğu durumlarda şekil 8.3' de olduğu gibi doğrulama başarılı mesajı verilecek ve sınav ekranına geçiş sağlanacaktır.

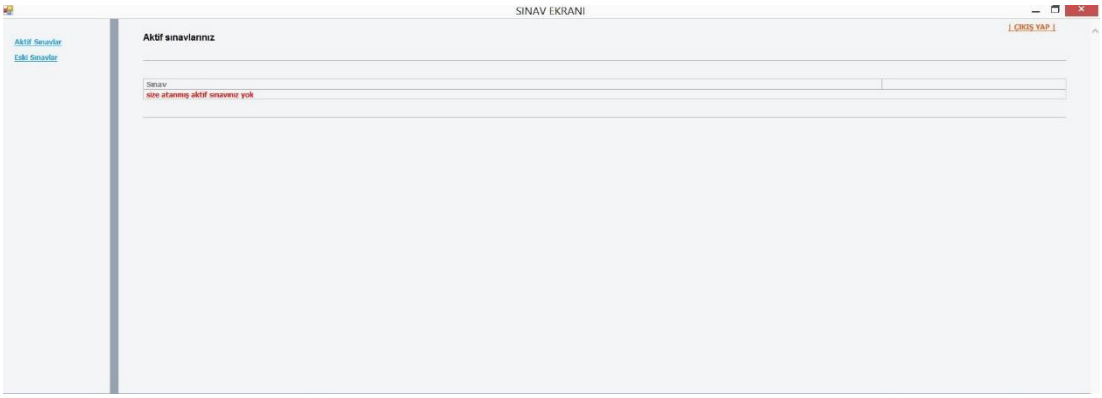
Şekil 8.3: Kullanıcı Giriş Ekranı Başarılı Durum

Karşılaştırma olumlu sonuçlandığında sınav sisteminin gösterileceği ekranın o kullanıcı için açılması işlemlerini gerçekleştirir. Ve şekil 8.4' de olduğu gibi sınav ekranında o kullanıcıya ait kullanıcı adı ve parola görüntülenir. Kullanıcı tarafından onaylandıktan sonra sınav ekranına geçiş sağlanır.



Şekil 8.4: Kullanıcı adı ve Parola Doğrulama

Kullanıcı adı ve parola onayı sonrası açılan sınav ekranı şekil 8.5' de olduğu gibidir.



Şekil 8.5: Sınav Ekranı

Sınav giriş ekranı ve doğrulama işlemini gerçekleştiren kodlar;

```
using MySql.Data.MySqlClient;

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace ParmakIziSistemi

{

    public partial class MainForm : Form
```

```
{
    MySqlConnection mysqlConnection = null;
    MySqlCommand mysqlCommand = null;
    MySqlDataReader mysqlDataReader = null;
    Object parmakIzi;
    public MainForm()
    {
        InitializeComponent();
    }
    private void Form1_Load(object sender, EventArgs e)
    {
        if (axZKFPEngX1.InitEngine() != 0) //-->Parmak izi cihazının bağlı olup olmadığının kontrolü gerçekleştirilir.
        {
            MessageBox.Show("Parmak izi cihazına algılanamadı!", "Hata");
            Application.Exit();
        }
        else
        {
            mysqlConnection = new MySqlConnection();
```

```
            mysqlConnection.ConnectionString                                    =
"Server=localhost;Database=parmakizi;Uid=root;Pwd=";";

            mysqlCommand = new MySqlCommand();

            mysqlConnection.Open();

            mysqlCommand.Connection = mysqlConnection;

            mysqlCommand.CommandText = "SELECT * FROM users";



            axZKFPEngX1.BeginCapture(); //--> Parmak izi okuma işleminin
başlatılması işlemini gerçekleştirir.

        }

    }
```

Okunan parmak izini ekranda gösteren method aşağıdaki gibidir

```
    private void axZKFPEngX1_OnImageReceived(object sender,
AxZKFPEngXControl.IZKFPEngXEvents_OnImageReceivedEvent e)

    {

        Graphics canvas = pnlParmakiziResmi.CreateGraphics();

        axZKFPEngX1.PrintImageAt(canvas.GetHdc().ToInt32(), 0, 0,
pnlParmakiziResmi.Width, pnlParmakiziResmi.Height);

        canvas.Dispose();

    }
```

```
//--> Parmak izi okuma işlemi

private void axZKFPEngX1_OnCapture(object sender, AxZKFPEngXControl.IZKFPEngXEvents_OnCaptureEvent e)

{

   try

   {

      mysqlDataReader = mysqlCommand.ExecuteReader();

      while (mysqlDataReader.Read())

      {

         parmakIzi = mysqlDataReader.GetValue(8); //veri tabanından geleni 'parmakIzi' isimli değişkenin içine atıyor.

         bool b = false;

         if (axZKFPEngX1.VerFinger(ref parmakIzi, e.aTemplate, false, ref b)) //veri tabanından gelen parmak izi ile cihazdan gelen parmak izinin karşılaştırılmasını yapar.

         {

            axZKFPEngX1.EndInit(); //--> Okuma işlemi bitiriliyor

            System.Threading.Thread.Sleep(3000);

            SinavEkrani qf = new SinavEkrani(mysqlDataReader.GetString(1), mysqlDataReader.GetString(2));

            qf.ShowDialog();

            lblDurum.Text = "";
```

```
                panel1.Refresh();
                break;
            }
            else
            {
                lblDurum.Text = "Doğrulama başarısız !";
                lblDurum.ForeColor = System.Drawing.Color.Red;
            }
        }

    }
    catch (MySql.Data.MySqlClient.MySqlException ex)
    {
        MessageBox.Show("Hata Kodu : " + ex.Number + " , Hata Mesajı : " + ex.Message,
            "Veritabanı hatası", MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
    mysqlDataReader.Close();
}
```

```
//işlem sırasında yada sonunda kullanıcıya geri dönüş bildirimleri yapan method.
private void axZKFPEngX1_OnFeatureInfo(object sender, AxZKFPEngXControl.IZKFPEngXEvents_OnFeatureInfoEvent e)
{
   lblDurum.Text = "Doğrulama başarılı !";
   lblDurum.ForeColor = System.Drawing.Color.Green;
}
```

Sınav ekranında ise Web tabanlı sınav sisteminin gösterilmesi ve sınavın uygulaması sağlanır. Ayrıca kullanıcının sınavı bitirdikten sonra sistemden çıkış yapması halinde tekrar bekleme ekranına geçiş sağlanır.

Sınav ekranının açılmasını sağlayan kodlar;

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
```

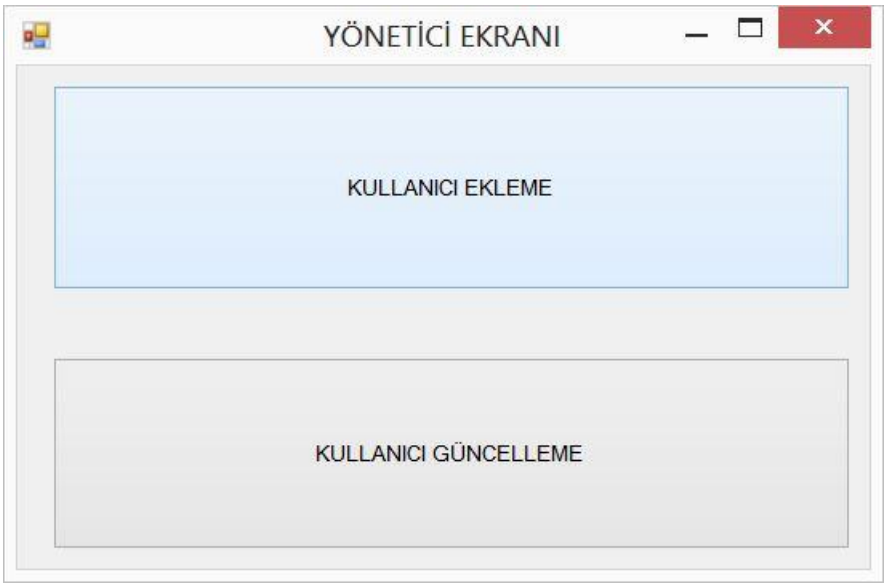
```
using System.Windows.Forms;


namespace ParmakIziSistemi
{
    public partial class SinavEkrani : Form
    {
        private int repeater = 0;
        private String html, usernames, passwords;
        public SinavEkrani(String usernames, String passwords)
        {
            InitializeComponent();
            this.usernames = usernames;
            this.passwords = passwords;
        }
        private void SinavEkrani_Load(object sender, EventArgs e)
        {
            webBrowser1.Navigate("http://localhost/sinavekrani");      // Sınav ekranının açılması işlemi gerçekleştirirlir.
        }
```

```
    private void webBrowser1_DocumentCompleted(object sender,
WebBrowserDocumentCompletedEventArgs e)

    {

        //--> açılan sayfaya parmak izi doğrulaması ile elde edilen şifrelerin yazılması
işlemleri gerçekleştirirlir.

        html = ((WebBrowser)sender).Document.Body.InnerHtml;

        if (repeater == 0)

        {

            Application.DoEvents();


webBrowser1.Document.GetElementById("txtLogin").SetAttribute("value",
usernames);

            webBrowser1.Document.GetElementById("txtPass").SetAttribute("value",
passwords);


//webBrowser1.Document.GetElementById("btnSubmit").InvokeMember("click");
//--> Otomatik giriş yapmak için kullanılır

            repeater++;

        }

        if
(webBrowser1.Document.Url.ToString().Contains("http://localhost/sinavekrani/logo
ut.php")) //--> çıkış işlemi kontrolü yapılır.

        {
```

```
            this.Close();
        }


    }
```

8.4 Yönetici Ana Ekranı

Kullanıcı ekleme ve kullanıcı düzenleme seçiminin gerçekleştirilmesini sağlayan ana ekrandır. Burada açılan seçimler kullanılarak ya yeni bir kullanıcı eklenir ya da var olan kullanıcı üzerinde düzenleme ve değişiklik işlemleri gerçekleştirilir. Yönetici ana ekranı şekil 8.6' da görüntülenmektedir.



Şekil 8.6: Yönetici ekran görüntüsü

Yönetici ana ekranı ve tercihe göre yönlendirme işlemini gerçekleştiren kodlar;

```
using System;

using System.Collections.Generic;

using System.ComponentModel;
```

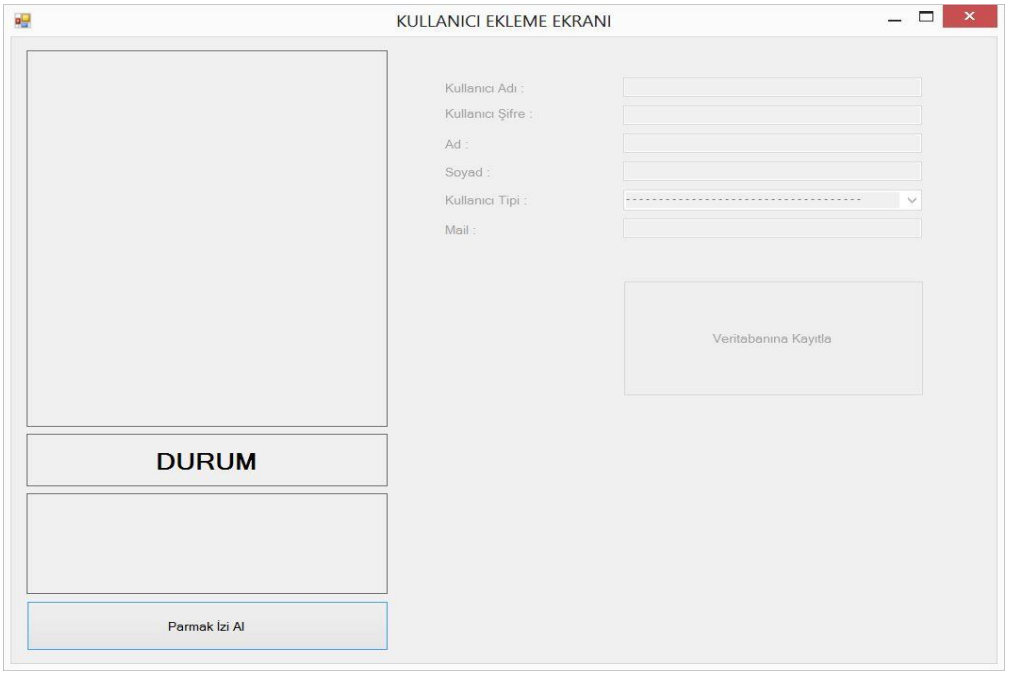
```
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
namespace ParmakIziYoneticiSistemi
{
    public partial class Yonetim : Form
    {
        public Yonetim()
        {
            InitializeComponent();
        }
        private void button1_Click(object sender, EventArgs e)
        {
            new AdminForm().Show();
        }
        private void button2_Click(object sender, EventArgs e)
        {
```

```
            new KullaniciDuzenle().Show();
        }
    }
}
```

8.5 Yeni Kullanıcı Ekleme Ekranı

Sisteme yeni kullanıcı kaydetme işlemi yönetici tarafından gerçekleştirilir. Yeni kaydolan öğrencilerin parmak izlerini sisteme tanımlanır ve öğrencilere ait kimlik bilgileri girilerek kimliklerini oluşturulur.

Yeni kayıt ekleme ekranı şekil 8.7'de görüntülenmektedir. Şekilde 8.7' de görüldüğü gibi önce eklenecek olan kullanıcının parmak izi alınır ve daha sonra parmak izine göre kimlik bilgileri oluşturulur. Parmak izi alınmadan kimlik oluşturma bilgileri aktif hale gelmez. Parmak izi tanılama işlemleri başarılı olduğu durumda kimlik oluşturma alanı aktifleşir ve kullanıcı bilgileri girilerek kullanıcı kimliği oluşturulur. Böylece yeni kullanıcı eklenir.



Şekil 8.7: Yeni Yullanıcı Ekleme Ekranı

Yeni kayıt ekleme işlemini gerçekleştiren kodlar;

```
using MySql.Data.MySqlClient;
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;

namespace ParmakIziYoneticiSistemi
{
    public partial class AdminForm : Form
    {
        private MySqlConnection mysqlConnection = null;
        private MySqlCommand mysqlCommand = null;
        private MySqlDataReader mysqlDataReader = null;

        Object RegTemplate;
```

```
public AdminForm()
{
    InitializeComponent();
}
private void Form1_Load(object sender, EventArgs e)
{
    if (axZKFPEngX1.InitEngine() != 0) //--> parmak izi cihazının bağlı olup olmadığı kontrolü
    {
        MessageBox.Show("Parmak izi cihazına algılanamadı!", "Hata");
        Application.Exit();
    }
    else
    {
        mysqlConnection = new MySqlConnection();
        mysqlConnection.ConnectionString = "Server=localhost;Database=parmakizi;Uid=root;Pwd=";";
        mysqlCommand = new MySqlCommand();
        mysqlConnection.Open();
```

```
            mysqlCommand.Connection = mysqlConnection;
        }
    }
    //--> parmak izinden okunan her izi ekranda gösteren method
    private void axZKFPEngX1_OnImageReceived(object sender,
AxZKFPEngXControl.IZKFPEngXEvents_OnImageReceivedEvent e)
    {
        Graphics canvas = pnlParmakiziResmi.CreateGraphics();
        axZKFPEngX1.PrintImageAt(canvas.GetHdc().ToInt32(), 0, 0,
pnlParmakiziResmi.Width, pnlParmakiziResmi.Height);
        canvas.Dispose();
    }
    //--> parmak alma işlemini object içine atan method
    private void axZKFPEngX1_OnEnroll(object sender,
AxZKFPEngXControl.IZKFPEngXEvents_OnEnrollEvent e)
    {
        if(e.actionResult)
        {
            RegTemplate = e.aTemplate;
            lblDurum.Text = "Parmak izi alımı başarılı!";
            infoPanel.Enabled = true;
```

```
    }
}
//--> Parmak izini bir Object nesnesinde tutulmasını sağlıyoruz
private void btnParmakIziAl_Click(object sender, EventArgs e)
{
    if (axZKFPEngX1.IsRegister) //--> cihazdan register alırken 3 defa aynı algoritmayı yakalasın diye kullanılan register methodu
    {                   //--> eğer doğrulanırsa enroll(kayıtlanma) işlemi bitiriliyor
        axZKFPEngX1.CancelEnroll();

    }
    axZKFPEngX1.BeginEnroll();
    lblDurum.Text = "Doğrulama için 3 defa okutunuz.";

}
//--> Kayıtlanma esnasında uyarıların verildiği ekran
private void axZKFPEngX1_OnFeatureInfo(object sender, AxZKFPEngXControl.IZKFPEngXEvents_OnFeatureInfoEvent e)
{
    if (e.aQuality != 0)
```

```
        {
            MessageBox.Show("Parmak izi kalitesi düşüktü tekrar okutunuz.");
        }else
        {
            if (axZKFPEngX1.IsRegister)
            {
                lblDurum.Text = "Doğrulama için " + (axZKFPEngX1.EnrollIndex - 1).ToString() + " defa okutunuz.";
            }
        }
    }
    //--> tüm bilgileri topladıktan sonra veri tabanına bastırıyoruz.
    private void button1_Click(object sender, EventArgs e)
    {
        try
        {
            mysqlCommand.CommandText = "INSERT INTO `users`(`UserID`, `UserName`, `Password`, `Name`, `Surname`, `added_date`, `user_type`, `email`, `fingerprint`) VALUES (NULL,@username,@password,@name,@surname,@addeddate,@usertype,@email,@fingerprint)";
            mysqlCommand.Prepare();
```

```
            mysqlCommand.Parameters.AddWithValue("@username",
txtUserName.Text.ToString());

            mysqlCommand.Parameters.AddWithValue("@password",
txtPassword.Text.ToString());

            mysqlCommand.Parameters.AddWithValue("@name",
txtName.Text.ToString());

            mysqlCommand.Parameters.AddWithValue("@surname",
txtSurname.Text.ToString());

            mysqlCommand.Parameters.AddWithValue("@addeddate",
DateTime.Now.ToString("yyyy-MM-dd HH:mm:ss"));

            mysqlCommand.Parameters.AddWithValue("@usertype",
(cmbxUserType.SelectedIndex+1));

            mysqlCommand.Parameters.AddWithValue("@email",
txtMail.Text.ToString());

            mysqlCommand.Parameters.AddWithValue("@fingerprint",
RegTemplate);

            mysqlCommand.ExecuteNonQuery();

            MessageBox.Show("Veritabanına Kayıtlama işlemi başarılı..!","İŞLEM
SONUCU : ");

        }

        catch (MySql.Data.MySqlClient.MySqlException ex)

        {

            MessageBox.Show("Hata kodu : " + ex.Number + " Hata mesajı : " +
ex.Message,
```

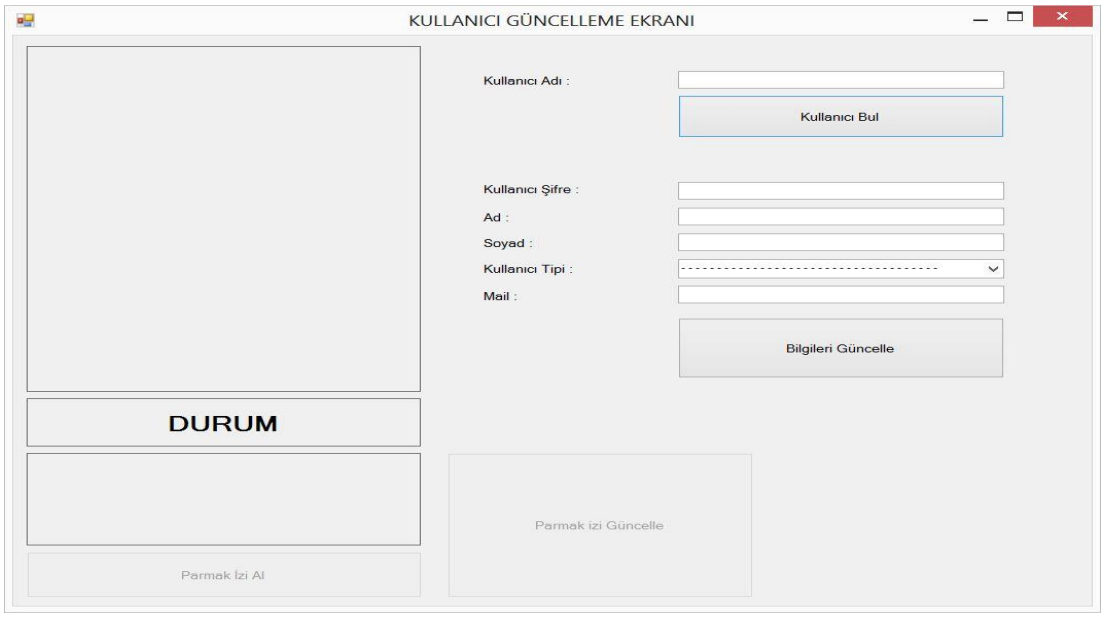
```
                "Veritabanı hatası", MessageBoxButtons.OK, MessageBoxIcon.Error);
        }
        finally
        {
            mysqlConnection.Close();
        }
    }
}
```

8.6 Kullanıcı Düzenleme Ekranı

Aynı zamanda kayıtlı kullanıcılara ait güncelleme işlemleri yine yönetici tarafından yapılır. Veri tabanında kayıtlı kullanıcılara ait bilgilerin güncellenme işlemleri, parmak izi de dâhil olmak üzere buradan gerçekleştirilir. Güncelleme işlemleri iki türlü yapılır.

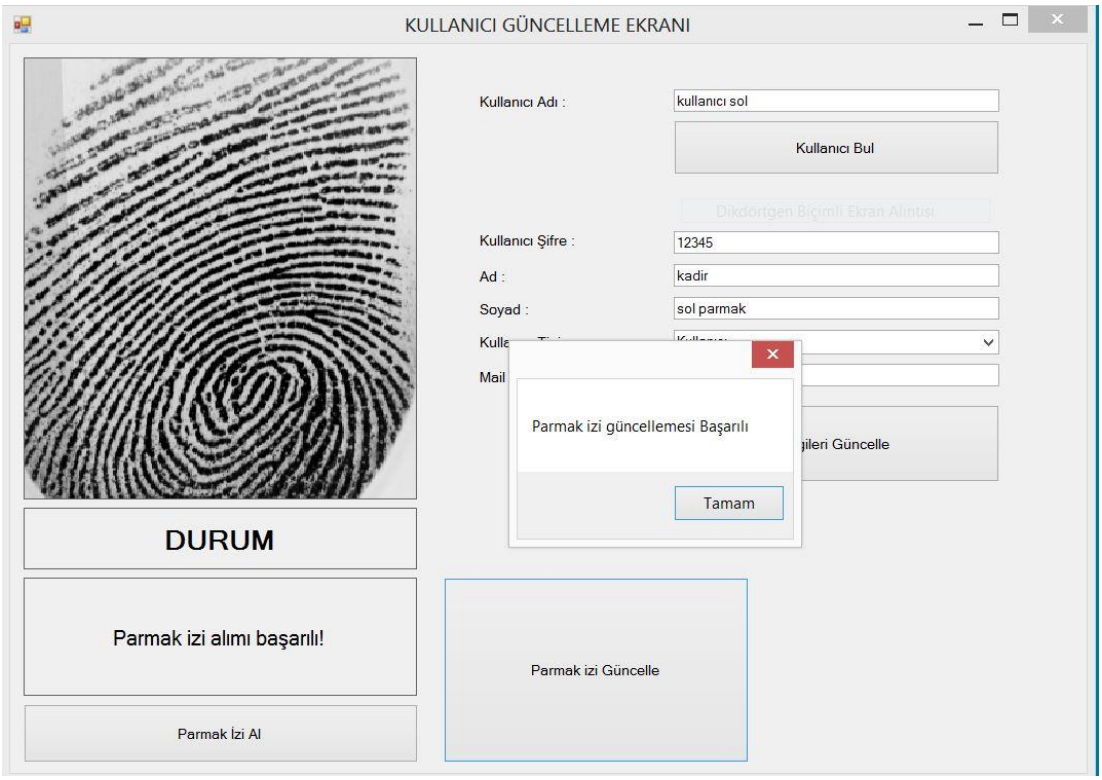
- Kimlik bilgileri güncellemesi
- Parmak izi güncellemesi

Şekil 8.8’ e olduğu gibi kullanıcı adı girilerek kullanıcı bulunur ve kullanıcı bilgileri güncellenir. Kullanıcı bilgileri güncellendikten sonra parmak izi güncelleme işlemi gerçekleştirilir.



Şekil 8.8: Kullanıcı Güncelleme Ekranı

Kullanıcı bilgileri güncellendikten sonra kullanıcıya ait istediği parmak izi(isteğe bağlı var olan parmak izi dışında da olabilir) tekrar tanımlanır. Ve parmak izi alımı başarılı mesajı görüldükten sonra parmak izini güncelle butonu tıklanarak güncelleme işlemi tamamlanır. Şekil 8.9' da görüldüğü gibi kullanıcı bilgileri güncelleme işlemi tamamlandıktan sonra parmak izinin tekrar okutulup tanımlanmasıyla parmak izi güncellemesi de yapılır.



Şekil 8.9: Kullanıcı Parmak İzi Güncllleme

Güncelleme işlemlerinin yapılmasını sağlayan kodlar;

```
using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;
```

```
using MySql.Data.MySqlClient;


namespace ParmakIziYoneticiSistemi
{
    public partial class KullaniciDuzenle : Form
    {
        MySqlConnection mysqlConnection = null;
        MySqlCommand mysqlCommand = null;
        MySqlDataReader mysqlDataReader = null;
        Object parmakIzi;
        int useridd;


        public KullaniciDuzenle()
        {
            InitializeComponent();
        }
        private void KullaniciDuzenle_Load(object sender, EventArgs e)
        {
            if (axZKFPEngX1.InitEngine() != 0) //--> parmak izi cihazının bağlı olup olmadığı kontrolü
```

```
        {
            MessageBox.Show("Parmak izi cihazına algılanamadı!", "Hata");
            Application.Exit();
        }
        else
        {
            mysqlConnection = new MySqlConnection();
            mysqlConnection.ConnectionString =
"Server=localhost;Database=parmakizi;Uid=root;Pwd=";";
            mysqlCommand = new MySqlCommand();
            mysqlConnection.Open();
            mysqlCommand.Connection = mysqlConnection;
        }
    }

    private void axZKFPEngX1_OnImageReceived(object sender,
AxZKFPEngXControl.IZKFPEngXEvents_OnImageReceivedEvent e)
    {
        Graphics canvas = pnlParmakiziResmi.CreateGraphics();
        axZKFPEngX1.PrintImageAt(canvas.GetHdc().ToInt32(), 0, 0,
pnlParmakiziResmi.Width, pnlParmakiziResmi.Height);
```

```
            canvas.Dispose();
        }
        private void button1_Click(object sender, EventArgs e)
        {
            mysqlCommand.CommandText = "select * from users where UserName='" +
txtUserName.Text + "';";
            mysqlDataReader = mysqlCommand.ExecuteReader();
            while (mysqlDataReader.Read())
            {
                txtName.Text = mysqlDataReader.GetString("Name");
                txtSurname.Text = mysqlDataReader.GetString("Surname");
                txtMail.Text = mysqlDataReader.GetString("email");
                txtPassword.Text = mysqlDataReader.GetString("Password");
                if (mysqlDataReader.GetInt32("user_type") == 1)
                {
                    cmbxUserType.SelectedIndex = 0;
                }
                else
                {
                    cmbxUserType.SelectedIndex = 1;
```

```
            }
            useridd = mysqlDataReader.GetInt32("UserID");
            btnParmakIziAl.Enabled = true;
        }
        mysqlDataReader.Close();

    }

    private void button2_Click(object sender, EventArgs e)
    {
        mysqlCommand.CommandText = "UPDATE users SET UserName = '"+txtUserName.Text+"', Password = '"
            +txtPassword.Text+"', Name = '"+txtName.Text+"', `Surname` = '"+txtSurname.Text+
            "', user_type = "+(cmbxUserType.SelectedIndex+1)+", email = '"+txtMail.Text+"' WHERE UserID = "+useridd+";";
        try
        {
            if (mysqlCommand.ExecuteNonQuery() == 1)
            {
                MessageBox.Show("Güncelleme Başarılı");
```

```
            }
            else
            {
                MessageBox.Show("Güncelleme Başarısız...!");
            }
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message.ToString());
        }

    }

    private void btnParmakIziAl_Click(object sender, EventArgs e)
    {
        if (axZKFPEngX1.IsRegister) //--> cihazdan register alırken 3 defa aynı algoritmayı yakalasın diye kullanılan register methodu
        {                           //--> eğer doğrulanırsa enroll(kayıtlanma) işlemi bitiriliyor
            axZKFPEngX1.CancelEnroll();
```

```
        }
        axZKFPEngX1.BeginEnroll();
        lblDurum.Text = "Doğrulama için 3 defa okutunuz.";
    }

    private void axZKFPEngX1_OnFeatureInfo(object sender,
AxZKFPEngXControl.IZKFPEngXEvents_OnFeatureInfoEvent e)
    {
        if (e.aQuality != 0)
        {
            MessageBox.Show("Parmak izi kalitesi düşüktü tekrar okutunuz.");
        }
        else
        {
            if (axZKFPEngX1.IsRegister)
            {
                lblDurum.Text = "Doğrulama için " + (axZKFPEngX1.EnrollIndex -
1).ToString() + " defa okutunuz.";
            }
        }
```

```
}

private void axZKFPEngX1_OnEnroll(object sender, AxZKFPEngXControl.IZKFPEngXEvents_OnEnrollEvent e)
{
    if (e.actionResult)
    {
        parmakIzi = e.aTemplate;
        lblDurum.Text = "Parmak izi alımı başarılı!";
        button3.Enabled = true;
    }
}

private void button3_Click(object sender, EventArgs e)
{
    mysqlCommand.CommandText = "UPDATE users SET fingerprint = @fingerprint WHERE UserID = " + useridd + ";";
    mysqlCommand.Parameters.AddWithValue("@fingerprint", parmakIzi);
    try
    {
```

```
    if (mysqlCommand.ExecuteNonQuery() == 1)
    {
        MessageBox.Show("Parmak izi güncellemesi Başarılı");
    }
    else
    {
        MessageBox.Show("Parmak izi güncellemesi Başarısız...!");
    }
}
catch (Exception ex)
{
    MessageBox.Show(ex.Message.ToString());
}       }
```

8.7 Sınav Giriş Sistemi Uygulamasında Kullanılan Donanım Yapısı

Sınav giriş sisteminde proje donanım bileşenleri olarak USB port ile çalışan Parmak izi okuyucu kullanılmıştır.

Şekil 8.10: Uygulamada kullanılan Parmak İzi Okuyucu Cihaz

Projede kullanılabilen parmak izi okuyucu cihazı şekil 23'de görüntülenmektedir. Ayrıca projenin çalışması için windows işletim sistemi üzerinde MySql Microsoft visual studio bulunan bir bilgisayar kullanılmıştır. Parmak izi okuyucu cihazı usb port ile bağlanmaktadır ve bağlantının ardından veri aktarımı parmak izi okuyucu cihaz tarafından gerçekleştirilir ve C# ile cihazdan gelen veriler yönetilir.

Sınav giriş sisteminde kullanılan cihazın özellikleri;

Parmak izi algoritmasının kriterleri;

Kullanılan cihaz (ZK4500) okuma işlemine resmedilen parmak izi minimum 300DPI veya daha fazla kaliteye sahiptir(300DPI<=)

Parmak izi kayıtlanması ya da okunması esnasına parmak izi üstündeki çizgilerin okunma kalitesi %35 veya daha fazla olması cihazın yazılıma olumlu cevap döndürmesini sağlar. Aksi durumlarda SDK'nın geliştiricilere sunduğu method ya da eventlar çalışmaya olumsuz cevap döndürür ve yapılmak istenen işlem(kayıt yada doğrulama) tamamlanmaz.

Okunan bir parmak izi 310 yada 1153Byte olur. SDK içinde buna Template denilmekte.

Cihazın parmak izi doğrulama kalitesi 90%

Yanılma payı %0,1' dir

SDK(STANDART DEVELOPMENT KİT) Mimarisi

SDK geliştiricilere VC++, C++,VB gibi dillerde activex sunar ve bir yada birden fazla cihaz kontrol edilebilir.

SDK'nın başarılı bir şekide çalışması için cihaz sürücüleri cihazın bağlanılacağı sistem üzerinde kurulu olmalı.

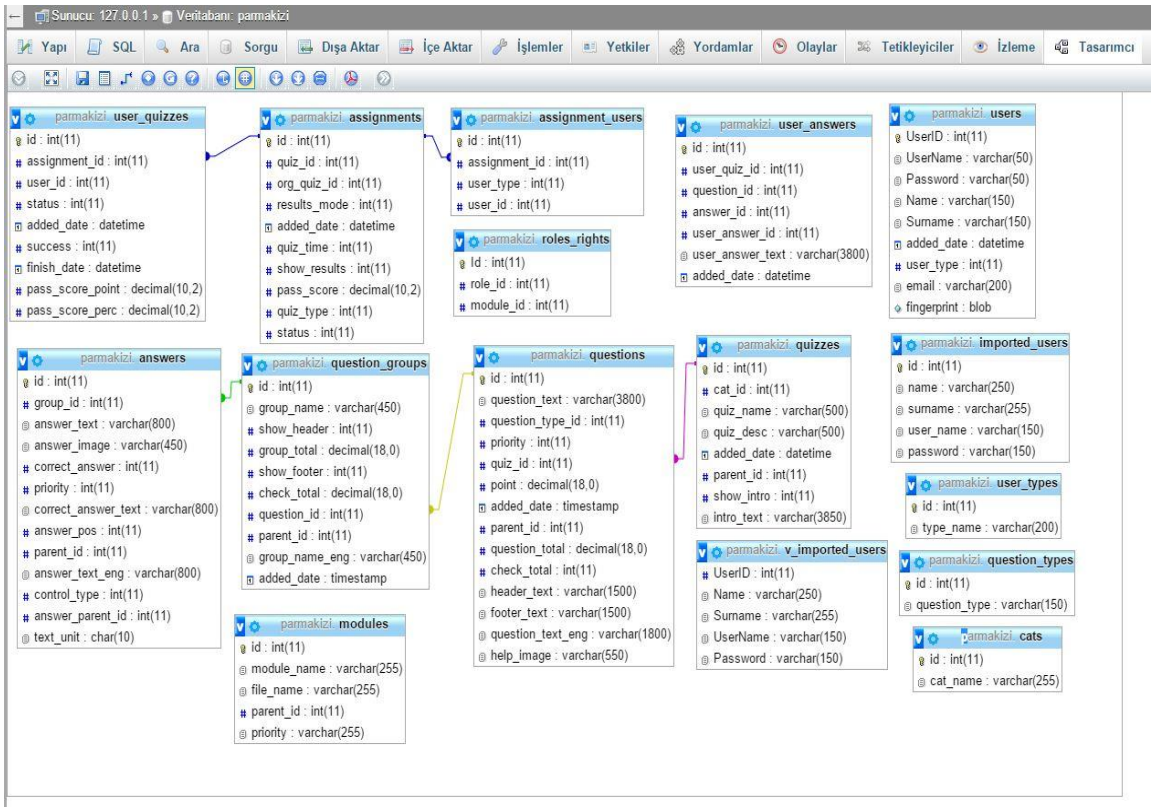
Cihaz ISO 9001:2000 standartlarına ve FCC Class B, CE, ICES, BSMI, MIC USB, WHQL onaylarına uygundur.

8.8 Sınav Sisteminin Veri Tabanı Yapısı

Var olan sınav sisteminin veri tabanında kullanıcılar tablosu içinde parmak izlerinin kaydedilmesi için yeni bir alan eklenmiştir.

Eklenen yeni alanın özellikleri parmak izi cihazından gelen binary verileri tutacak BLOB(Binary Large Object) tipinde eklenmiştir.

Veri tabanı ve ilişkileri şekil 8.11'de görüntülenmektedir.



Şekil 8.11: Veri Tabanı Görüntüsü

9 SONUÇ VE ÖNERİLER

Biyometrik Sistemler ve Parmak İzi Tanıma Teknolojisi araştırılmış, birçok kullanım alanı tespit edilmiştir. Parmak İzi Tanıma Teknolojisi bir çok takip sistemi için kullanılabileceği gibi online sınavlarda giriş için kullanılabileceği de bu çalışma ile kanıtlanmıştır.

Bu tez çalışmasında, bir öğretim kurumunda özellikle uzaktan eğitim gören ve öğretim görevlileri(sınav gözetmenleri) tarafından tanınmayan öğrencilerin sınav girişlerinin kontrollerinin sağlıklı şekilde yapılmasında sorunlar yaşanmaktadır. Bu çalışmada yapılan uygulamayla güvenli sınav girişinin yapılması sağlanmış ve başkasının yerine sınava girmenin önüne geçilmiştir.

Uygulamada, var olan web tabanlı sınavlara parmak izi tanıma teknolojisi ile giriş yapılabileceği kanıtlanmış. Ve parmak izi okuyucu cihaz ile web tabanlı sınav sisteminin login kısmının entegrasyonu sağlanmıştır.

Sisteme giriş yapacak olan her kullanıcının(yöneticiler de dâhil) parmak izi tanımlanıp parmak izlerini okutarak sisteme giriş yamaları sayesinde yöneticinin kullanıcı adı, parolası gibi bilgiler kullanılarak sorular üzerinde yapılacak tahribatın da önüne geçilmiştir.

Hata ve güvenliği üst seviyede olan sistem %0.01'lik bir hata payı ile çalışmaktadır. Bu hata payı, parmak izi okutma kalitesiyle 0' a kadar düşmektedir. Ayrıca parmak damar algılayıcı parmak izi okuyucu cihaz seçimiyle parmak izi kopyalama gibi sorunun da önüne geçilmiştir.

Bu tez çalışmasında, her bilgisayarda bir tane parmak izi okuyucu cihazı varsayılmıştır. Fakat her bilgisayarda bir parmak izi okuyucu cihaz konması maliyet açısından yüksek olduğu düşünülerek, parmak izi doğrulaması işlemi gerçekleştikten sonra login ile kullanıcı adı ve parola da doğrulanarak sınav girişi tamamen sağlanmıştır.

Dolayısıyla laboratuvar ortamlarında gözetmenler eşliğinde yapılan sınavlarda salon girişine bir parmak izi okuyucu konularak giriş sağlanabilir. Sınava girecek kullanıcı salon girişinde parmak izini okutur ve burada random olarak bir bilgisayar atanır ve kullanıcı sadece o bilgisayarda sınava giriş yapabilir. Belirtilen bilgisayarda ise login

ile kullanıcı adı ve parolası ile ikinci güvenlik işleminden geçerek sınav girişi sağlanabilir.

KAYNAKLAR

Ergen, B., & Çalışkan, A. (2011). Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri. 6th International Advanced Tecnologies Symposium(IATS'2011). Fırat Üniversitesi, Elazığ, Türkiye,16-18 Mayıs.

Ergen, B., & Çalışkan, A. (2011). Biyometrik Sistemler ve El tabanlı Biyometrik Tanıma Karakteristilkleri. 6 th İnternational Advanced Technologies Symposium(IATS'11). Elazığ.

Kınalıoğlu, İ. H., & Güven, Ş. (2011). Uzaktan Eğitim Sisteminde Öğrenci Başarısını Ölçülmesinde. XIII. Akaddemik Bilişim Konferansı. Malatya.

Kır, B., Öz, C., & Gülbağ, A. (2011). Yapay Sinir Ağlarında Negative Correlation Learning. Sakarya,Kocaeli.

M.Erkan Yüksel, a. Z. (2009, şubat 11-13). otomatik nesne tanımlama ,takibi ve yönetiminde RFID'nin yeni nesil kablosuz iletişim teknolojileri ile kullanımı. akademik bilişim konferansı bildirileri, s. 111-120.

Pala, Z. (2008, şubat). e-Sınav. akademik bilişim, s. 4-6.

Reid, K. (2003, eylül). The Barcode of the 21st. National Petroleum News, s. 36-42.

ŞAN, S. (2013). Yüksek Lisans Tezi. Parmak Damar Tanıma Teknolojisi, 6-17.

Varol, A., & Cebe, B. (2011, September 22-24). Yüz Tanıma Algoritmaları. ELAZIĞ, TURKEY.

Varol, A., & Cebe, B. (2011). Yüz Tanıma Algoritmaları. 5 th International Computer & Instructional Technologies Symposium . Elazığ.

Yalçın, N. (2008, Mart). Konuşma Tanıma Teorisi ve Teknikleri. Kastamonu Eğitim Dergisi, s. 249-266.

Zaim, M. ,. (2009, Mayıs 13-15). YENİ NESİL TEKNOLOJİ OLARAK RFID, RFID SİSTEM YAPILARI VE BİR RFID SİSTEM TASARIM

YAKLAŞIMI. 5. Uluslararası İleri Teknolojiler Sempozyumu (IATS'09),, s. 2-3.

İnternet Kaynakları:

Url-1 <http://mezun.com/online-egitim/online-egitim-genel/uzaktan-online-egitim-nedir.html>, alındığı tarih:6/01/2015.

Url-2 <http://www.artelektronik.com/parmak-izi.html#biyometri>, alındığı tarih: 10/12/2014.

Url-3 <http://www.artelektronik.com/yuz-tanima-sistemleri.html >, alındığı tarih: 8/02/2015.

Url-4
<https://www.google.com.tr/search?hl=tr&biw=1280&bih=575&q=y%C3%BCz%20tarama%20sistemleri%20&um=1&ie=UTF-8&tbm=isch&source=og&sa=N&tab=wi&ei=D9RIVbu9M4ac7gbVgoHQBg#um=1&hl=tr&tbm=isch&q=el+geometrisi > alındığı tarih: 8/1/2015.

Url-5 < http://tr.wikipedia.org/wiki/Parmak_izi>, alındığı tarih: 8/1/2015.

ÖZGEÇMİŞ

Ad-Soyad **:** Kadir KESKİN

Doğum Tarihi ve Yeri: 1987/Hatay.

ÖĞRENİM DURUMU

Lisans **:** 2007, Marmara Üniversitesi, Atatürk Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojileri Bölümü

Yüksek Lisans **:** 2015, İstanbul Aydın Üniversitesi ,Fen Bilimler Enstitüsü, Bilgisayar Müh. Anabilim Dalı, Bilgisayar Müh. Programı

MESLEKİ DENEYİM

2013-… Öğretim Görevlisi, İstanbul Aydın Üniversitesi