ANKARA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BİYOMETRİK SİSTEMLERİN BİLGİ GÜVENLİĞİ

Abubakr RAKHIMOV

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2017

TEZ ONAYI

Abubakr RAKHIMOV tarafından hazırlanan **"Biyometrik Sistemlerin Bilgi Güvenliği"** adlı tez çalışması 26/05/2017 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Semra GÜNDÜÇ
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri :

Başkan : Doç. Dr. Süleyman TOSUN
Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü

Üye : Doç. Dr. Semra GÜNDÜÇ
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Üye : Yrd. Doç. Dr. Bülent TUĞRUL
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Yukarıdaki sonucu onaylarım.

Prof. Dr. Atila YETİŞEMİYEN
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

26.05.2017

Abubakr RAKHIMOV

ÖZET

Yüksek Lisans Tezi

BİYOMETRİK SİSTEMLERİN BİLGİ GÜVENLİĞİ

Abubakr RAKHIMOV

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Semra GÜNDÜÇ

Günümüzde teknoloji dünyasında Bilgi Güvenliği en önemli problemlerden biri olarak kabul edilmektedir. Biyometrik Tanıma Sistemleri bu alanda yeni bir endüstrinin ortaya çıkmasına sebep olmuştur. Bu teknolojilerin geleneksel yaklaşımlara göre çok güvenli oldukları kabul edilmiştir. Bireysel ve kurumsal bilgileri güvenli bir ortamda tutabilmek ve korumak için büyük çaba harcanmaktadır. Biyometrik Sistemleri bazı matematiksel algoritmalardan geçirilmesi ile kişilerin kendine has kimlik doğrulaması sağlanabilir. Bu çalışmada kamu kurumlarında bir başkasının yerine binaya giriş ve çıkışların önlenmesi amacıyla Yüz kimlik tespiti yapan BİPEKS (Biyometrik Personel Kontrol Sistemi) adlı bir uygulama geliştirilmiştir. Öncelikle kişisel bilgileri, Ad, Soyad, Doğum Tarihi, Cinsiyet, Kimlik No gibi verilerden oluşan kullanıcı bilgileri veri tabanına kayıt edilmektedir. Kişisel veriler kayıt edildikten sonra kişiyi seçip ona ait biyometrik bilgileri veri tabanına eklemektedir. Giriş ve Çıkış zamanında kullanıcıdan biyometrik sensör veya kamera yoluyla alınan biyometrik veriye veya yüz görüntüsünü veri tabanına daha önceden kaydedilen veriler ile karşılaştırılmaktadır. Karşılaştırma sonucuna göre kişi Giris-Çıkış yapabilecek ya da yapamayacak. Bu çalışmada, insan yüzünün otomatik ve gerçek zamanlı tanınması için Haar Cascade metodu kullanılmış ve oldukça yüksek başarı elde edilmiştir.

Mayıs 2017, 41 sayfa

Anahtar Kelimeler: Biyometri, Mültimodal, Sorgulama, Doğrulama, Onaylama

ABSTRACT

Master Thesis

INFORMATION SECURITY OF BIOMETRIC SYSTEMS

Abubakr RAKHIMOV

Ankara University
Graduate School of Natural and Applied Sciences
Computer Engineering Department

Supervisor: Assoc. Prof. Dr. Semra GÜNDÜÇ

In today's world of technology, Information Security is considered as one of the most important problems. Biometric Recognition Systems have led to the emergence of a new industry in this area. It is recognized that these technologies are very secure compared to traditional approaches. Great efforts are being made to keep and protect individual and corporate information in a safe environment. Biometric systems can be authenticated by passing them through some mathematical algorithms. In this study, a application called "BİPEKS (Biometric Personnel Control System)" which detects facial identities has been developed in public institutions in order to prevent entrance and exit to the building instead of someone else. Firstly, user information consisting of personal information, name, surname, date of birth, gender, identity number is recorded in the database. After the personal data has been recorded, the person is selected and added to the database of his / her biometric data. The biometric data or facial image taken by the user through the biometric sensor or camera at the Input and Output time is compared with the data previously stored in the database. According to the comparison result, the person will be able to enter or exit. In this study, Haar Cascade method have been used to recognize the automatic real-time human face and achieved quite high success.

May 2017, 41 pages

Key Words: Biometrics, Multimodal, Identification, Recognition, Verification

ÖNSÖZ ve TEŞEKKÜR

Çalışmalarımı yönlendiren, araştırmalarımın her aşamasında bilgi, öneri ve yardımlarını esirgemeyerek akademik ortamda olduğu kadar beşeri ilişkilerde de engin fikirleriyle yetişme ve gelişmeme katkıda bulunan danışman hocam sayın Doç. Dr. Semra GÜNDÜÇ, çalışmalarım süresince manevi desteklerini esirgemeyen Sayın Prof. Dr. İman ASKERBEYLİ, sevgisi ve bilimsel yaklaşımı kendisinden öğrenmeye çalıştığım değerli hocam Doç. Dr. Recep ERYİĞİT, Doç. Dr. Refik SAMET, Yrd. Doç. Özgür TANRIÖVER, Yrd. Doç. Dr. Mehmet Serdar GÜZEL, Yrd. Doç. Dr. Gazi Erkan BOSTANCI, çalışmalarım sırasında önemli katkılarda bulunan ve yönlendiren Yrd. Doç. Dr. Bülent TUĞRUL, Bilgi Güvenliği konusunda kendilerinden çok şeyler öğrendiğim Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü Sayın Prof. Dr. Şeref SAĞIROĞLU ve bilimsel çalışmaların yanında her aşamada pratik çözümleriyle destek veren Dr. Yılmaz AR, Arş. Gör. Zeynep YILDIRIM, Arş. Gör. Özge MERCANOĞLU SİNCAN, Arş. Gör. Sevgi YİĞİT SERT ve Arg. Gör. Pınar KÜLLÜ en derin duygularla teşekkür ederim.

"MIA Teknoloji" şirketinde staj yapmama imkan sağlayan sayın Genel Müdür Ali Gökhan BELTEKİN'e teşekkür etmeyi borç bilirim. Ayrıca AR-GE ve Yazılım Birim Başkanı Osman ÇEBİN, arkadaşlarım yazılım mühendisleri Osman ORHAN, Bedrettin SUMER, Mehmet BAHAR, Fatoş ŞİMŞEK ve Barış BEKMEZ'e projelerimin yazılım sırasında ve tez çalışmasında yardımcı oldukları için müteşekkirim. "MIA Teknoloji" şirketi AR-GE ve Yazılım Birimi çalışanları sayesinde edindiğim bilgiler, kendi projelerimi (TOBIS, KOBIS) ve "Biyometrik Personel Kontrol Sistemi" adlı yüksek lisans tezimi yazmamı mümkün kılmıştır.

Abubakr RAKHIMOV

Ankara, Mayıs 2017

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AAM	Aktif Görünüm Modeli
ATM	Otomatik Vezne Makinesi
BİPEKS	Biyometrik Personel Kontrol Sistemi
CPU	Merkezi İşlem Birimi
CRM	Müşteri İlişkileri Yöntemi
CSV	Virgülle Ayrılmış Veriler (Değişkenler)
DNA	Deoksiribo Nükleik asit
EBGM	Elastik Demet Grafik Eşleştirme
EP	Evrimsel Takip
EER	Eşit Hata Oranı
FAR	Yanlış Kabul Oranı
FRR	Yanlış Reddetme Oranı
FTE	Kayıt İçin Arıza Oranı
HTML	Metin İşaretleme Dili
ICA	Bağımsız Bileşen Analizi
ICAO	Uluslararası Sivil Havacılık Organizasyonu
LDA	Doğrusal Diskriminant Analizi
PCA	Temel Bileşenler Analizi
PDF	Taşınabilir Belge Biçimi
PDKS	Personel Devam Kontrol Sistemleri
POS	Satış Noktası
RTF	Gelişmiş Yazı Dosyası Türü
SGK	Sosyal Güvenlik Kurumu
XLS, XLSX	Excel Programının Dosya Uzantısı

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Veri veya bilgi konusunda bahsetiğiimiz an aklımıza bilgi gizliliği ve bilgi güvenliği kavramları gelir, ancak unutmayalım ki bu kavramların yanında kimlik doğrulama kavramı da çok önemlidir. Bu teknoloji dünyasında bilgiyi istenen kişiye veya her hangi bir kamu kurumuna gönderdiğimiz zaman eğer tesadüfen başka bir kişiye veya kuruma giderse mutlaka ortaya istenmeyen sonuçlar çıkabilir. Gizli bilgileri üçüncü kişi ile paylaşmak, (tesadüfen olsa bile...) bu tür problemleri bankalar, tıp ve savunma sanayi gibi sektörlerde ciddi boyutlarda ortaya çıkarabilir.

Sektörler tarafından özel sektör, kamu kurumları, savunma sanayi vs. sektörler tarafından bilgi temelli olarak sistemi yöneten kişilerin ve kullanıcıların belirli bilgilere sahip olmasını gerektirir. Örnek olarak bu bilgiler kişilerin adı, soyadı, cinsiyeti, doğum günü, şifreler ve pin kodlar gibi bilgiler olabilir. Bu tip sistemlerde kullanıcıların ve kullanıcılara karşılık gelen bilgiler (şifreler, pin kodlar) bir veri tabanında kaydedilip saklanır. Kullanıcılar bilgilerini sisteme girdiği zaman veri tabanında karşılarştırmalar yapılır. Karşılaştırma sonucunda bilgiler (giren bilgiler ve veri tabanında var olan bilgiler) birbirini tutuyorsa doğru kullanıcı olduğunu tespit eder ve kullanıcının sisteme giriş yampasına ve sistemde yetkilerini kontrol ederek işlemlerini gerçeklerştirmesine izin verilir. Bu tür sistemlerde kullanıcının şifresini (pin kodu) unutması ya da bu bilgileri üçüncü taraftan elde edilmesi bu sistemin en önemli dezavantajlardandır.

Başka türlü kimlik doğrulama sistemlerde kullanıcılar kendileri ile eşleşen bir objeye sahiptirler ki, bu obje genelde manyetik kart, akıllı kart (smart card) veya anahtardır ve bu objeler kullanılarak sisteme giriş yaparlar. Objenin içerisinde sisteme giriş yapabilmek için kim olduğunu belli edecek bilgiler mevcuttur, ama bu tip sistemlerde objeyi (manyetik kart veya smart card) kaybetmesi, unutması ya da çaldırması ihtimali bir dezavantaj yaratmaktadır.

Biyometrik kimliklendirme teknolojilerde kullanıcı sisteme kendisine ait olan ve başka insana da ait olmayan üzerinde daim taşındığı parmak izi, yüz, göz, iris ve retina gibi bir

fizyolojik özelliğini kullanarak giriş yapar. Bu şekilde kullanıcı sisteme giriş yapmak istediğinde, sistem tarafından kullanıcının uygun biyometrik bilgileri alınır ve bu alınan bilgiler aynı kişiden veri tabanında (daha önceden) kaydedilmiş biyometrik bilgi ile karşılaştırılır. İşi yapıldıktan sonra kişinin biyometrik bilgileri doğru olduğu durumda kimlik tespiti gerçekleştirilmiş olur (Varol ve Cebe 2011).

Tezin Amacı

Bu Tez çalışmasında bilgi güvenliği için Biyometrik Teknolojilerin gelişmiş özeliklerini ve yöntemlerini bir araya getirip uygulamalı şekilde kullanılmaktadır. Biliyoruz ki her insanda biyolojik Parmak İzi, Parmak Damar, Avuç İçi ve Yüz gibi özellikleri eşsiz ve benzersizdir. Buna rağmen bu özelikleri kullanarak kamu kurumlarında ve özel sektörde Giriş ve Çıkışlarda, bigisayara biyometrik giriş yapmak ve bilgi güvenliği sayısını arttırmak için yeni fikirler ortaya çıkmıştır. Bu fikirleri bir araya getirip kişinin biyometrik özeliklerini faydalı bir şekilde kullanarak bir uygulama ortaya çıkmasına sebep olmuştur. Ortaya çıkan uygulamanın ismi Biyometrik Personel Kontrol Sistemi (BİPEKS) olarak adlandırılmıştır. Aşağıdaki bölümlerde BİPEKS uygulaması hakkında detaylı bilgi verilmiştir. Yazmış olduğum uygulama farklı alanlarda faaliyet gösteren farklı kurumlarda kullanılabilir.

Tezin Kapsamı

Tez kapsamında biyometrik teknolojileri ve tez amacı üzerinde kısaca genel anlamda bahsedilmektedir. İkinci bölümde ise literatürler üzerinde yaptığım araştırmaların sonunda biyometrik teknolojilere genel bakış, biyometrik nedir, yöntemler, çalışma prensibi, sınıflandırma ve kullanımları teori olarak detaylı bilgi verilecektir. Üçüncü bölümde yüz tanıma yöntemleri incelenmiştir. Dördüncü bölümde ise yazmış olduğum uygulama Biyometrik Personel Kontrol Sistemi (BİPEKS) hakkında bahsedilmektedir. Beşinci bölümde ise bütün yapmış olduğum çalışmaların neticesinde sonuç ve değerlendirme tartışılmıştır.

2. BİYOMETRİK SISTEMLERE GENEL BAKIŞ

Günümüzde dünya çapında giriş ve çıkış yerlerde erişim kontrol sistemlerin yöntemi olarak şifre, manyetik kart, çipli kart (smart card) ve pin kodu gibi araçları kullanılmaktadır. Bu tip yöntemlerin çoğunun yaygınlaşmış olmalarına rağmen, tüm dünyada bu sistelerin yetkili olmayan kişiler tarafından çıkar amaçlı kullanılmasından kaynaklanan büyük maddi (maliyetli) ve manevi kayıpları önleyememektedir. Aslında bu tür sebepler kişiye özel olmamalıdır ki, bir alana erişimi engelleyebilmekte, ancak kimin eriştiğini kontrol edememektedirler.

Bu tip problemli yöntemlerde örnek olarak banka kartları veya metro ve otobüs kartları olabilir. Bir örnek: banka kartınızın şifresini bilen kişi, kart kendisine ait olmasa bile hesabınızdan istediği işlemleri yapabilmektedir. Buna benzer kaçak girişler askeri alanlarda çok tehlikeli sonuçlar doğurulabilir. Bu tür problemlerin çözümünün bulunabilmesi için yaklaşık 20 yıllık geçmişe sahip ve halihazırda geliştirmekte olan biyometrik teknolojiler faaliyet göstermektedir (Ergen ve Çalışkan 2011).

Bu problemli yöntemleri ortadan kaldırmak için sadece bir kart yada şifre kullanmak yeterli olmuyor, bunun yanında insanın (kullanıcının) gerçekten beyan edilen kişi olup olmadığı da tespit edilmektedir ki, bu konuda biyometrik sistemler yardımcı olabilir. Biyometrik teknolojilerin temel avantajı, giriş-çıkış veya her hangi başka bir işi yapmak isteyen insanın şahsen fiziksel olarak sisteme tanıtmak zorunda olmasıdır. Bundan başka çoğu biyometrik teknolojiler kontrol ettiği objenin canlı olup olmadığını da anlayabilir, dolaysıyla kopya yada protez kullanma ihtimali ortadan kaldırılır.

Biyometrik sistemlerinin günümüzde farklı alanlarda kullanılmaya başlamasıyla birlikte altyapının mantığı nasıl olacağına dair çeşitli fikirler ortaya koyulmuştur. Bu fikirlerden en fazla tercih edilen yöntemlerden iki yöntem olmuştur.

Birinci yöntemde kullanıcı başta bir seferlik olarak örnek biyometrik verileri merkezi veri tabanına kayıt edecek. Bundan sonra sistemi kullandığı zaman, biyometrik veriler daha önce veri tabanındaki örnek bilgilerle karsılaştırılarak değerlendirilir.

İkinci yöntemde ise kullanıcının bilgileri kendisine verilen bir akıllı kart (smart card) içerisinde tutulur, çünkü bu yöntemde merkezi veri tabanı yoktur. Kullanıcı biyometrik sistemden giriş ve çıkış yapacağı zaman kartı makineden (kart okuyucu) geçirir ve fiziksel örneğini sensora verir ve sistem tarafından karttaki örnek verilen örnekle (daha önceden biyometrik veriler ile) karşılaştırır ve buna göre geçiş için izin verilir ya da geçişi rededilir. Bu yöntemde ortada herhangi bir network erişimi olmadığı için işlem daha hızlı çalışmaktadır, ancak bunun dezavantajı da var ki, erişim kartı kaybolursa ya da bozulursa giriş yapmak mümkün olmayacak (http://elektroteknoloji.com 2010).

2.1 Biyometrik Nedir

“Bio” (yaşam) ve “Metron” (ölçüm), kelimelerinden oluşan biyolojik ve biyometrik verileri ölçme ve analiz etme birimidir. Yaşadığımız bilişim dünyasında biyometrik teknolojiler genel olarak insan vücudundaki parmak izi, el geometrisi, avuç içi, yüz, göz, retina, iris ve ses şekilleri gibi özelliklerle ilgilenilir ve bunlar güvenli kimlik tespiti için kullanılır.

Biyometri: İnsanları birbirinden ayıran ve ölçülebilir şekilde psikilojik ve davranışsal olarak iki kısma ayrılmaktadır. Bu iki özelliği kimlik tespitinde kullanan sistemler biyometrik kontrol ve tanıma sistemleri olarak adlandırılmıştır. Biyometrik teknolojiler insanın fiziksel ve davranışsal özelliklerini diğer insanlardan ayıran ve fark edebilecek şekilde çalışmaktadır. Araştırdığım literatürlere göre kişinin biyometrik özellikleri fiziksel, davranışsal ve biyokimyasal olmak üzere üçe ayrılmıştır ki bu özellikler biyometrik teknolojilerde otomatik tespit edilebilmek için kullanılan bir terimdir. Biyometri kelimesi özet olarak “biyolojik izleri ölçülebilir bireyler” olarak tanımlanabilir (http://www.ispozelguvenlik.com.tr 2014).

2.2 Biyometrik Sistemler

Bütün Biyometrik Teknolojiler fiziksel ve davranışlar olarak iki gruba ayrılmaktadır. Fizyolojik özeliklerde: parmak izi, parmak damar, el geometrisi, avuç içi,kulak şekli,yüz, göz, iris, retina ve cilt ele alınmaktadır. Davranışsal özelliklerde ise: ses, konuşma tarzı, tuş vuruşları/yazma ritmi, imza tarzı gibi özelikler yer alır. Bazı kaynaklarda ise biyometrik sistemlerin özellikleri biyokimyasal, fizyolojik ve davranışsal olarak üçe ayrılmaktadır.İnsan gözü ile görülen insan bedenine ait veriler fizyolojik özelikler olarak tanımlanmaktadır.

Literatürlere göre biyometrik sistemler "tek model ve çoklu model" sistemler olarak adlandırılmaktadır. İki biyometrik sistemi bir arada kullandığınız halde o sistemin ismi "çoklu model biyometrik sistem" anlamına geliyor. Yüz tanıma ve Parmak Damar tamına bir arada yapıldığı sistem, çoklu model biyometrik sistemi olarak betimlenmektedir. Çizelge 2.2 farklı biyometrik sistemlerin doğruluk, kullanım kolaylığı ve kullanıcı kabul oranı karşılaştırılmıştır.

2.3 Biyometrik Yöntemler

Biyometrik teknolojilerde uygulanabildiği yöntemler oldukça çok fazladır. Yöntemi seçerken en önemli olarak yöntemin aldığı fiziksel özelliğin yeterince ayırdedici olabilmesidir. Güvenli bir biyometrik sistem seçtiğiniz yöntemde aynı özelliklerin iki insanda bulunması olasılığı en düşük yani birkaç milyonda bir ihtimaldir. Bu yöntemlerin sonucunda bazı teknikler ön palana çıkmıştır. Ortaya çıkan tekniklerin arasında yüz tanıma, göz, iris ve retina analizi, ses analizi, parmak izi tanıma, el meometrisi, parmak damar tanıma ve imza analizi gibi yöntemler bulunmaktadır. Bu yöntemler farklı donanım ve algoritmalar kullanırlar, ama her birisi temelde aynı mantıkla çalışmaktadırlar. Ayrıca bu yöntemlerin arasında berlirli farklıkları, maliyet, güvenilirlik seviyesi, kullanım kolaylıkları, teknik desteği gibi bazı etkenler ortaya koymaktadır. Çizelge 2.3 biyometrik teknolojilerin kullanılan veya araştırılan yöntemlerin karşılaştırılmaları bulunmaktadır.

2.4 Çalışma Prensibi

Dünyadki bütün biyometrik teknolojilerde hemen hemen aynı çalışma mantığı vardır. Bu çalışma mantığına göre, biyometrik sistemi kullanacak kişi ilk adımda kendi biyometrik bilgilerini (parmak izi, yüz veya avuç içi olabilir) sistemin veri tabanına kaydeder. Bu kaydettiği yer, lokal veri tabanı, network üzerinden bağlanan host üzerinden veri tabanı ya da her kullanıcıya özel bir çipli kart (smart card) üzerinde bulunabilir.

Daha sonra kaydettiğiniz kişi biyometrik sistemini kullanmak istediği zaman her seferde biyometrik bilgisini bir sensör (yüz tanıma sistemler için kamera ile) aracılığıyla bilgisayara (biyometrik sisteme) aktarır ve şifresini girer. Verilen örneği alan sistem (veya bilgisayar) girilen şifreyi indeks olarak kullandığı için bir hash fonksiyonuyla tek seferde (tek adımda) kayıtlı olan kişinin bilgisini veri tabanında bulur ve bulunan verileri karşılaştırır. Karşılaştırma sonucunda erişim isteği kabul edilir ya da rededilir.

Başka bir çalışma prensibi ise bilgi akıllı kart üzerinde saklandığı takdirde herhangi bir şifre ya da hash fonksiyonuna gerek kalmayacak, çünkü veri, anında kart (smart card-akıllı kart) üzerinden çekilerek veri tabanındaki örnek veriler ile karşılaştırılır. Bu tip durumlarda zaman tasarrufu olur, ancak smart kart okuyucusu için ekstra harcamalar lazımdır.

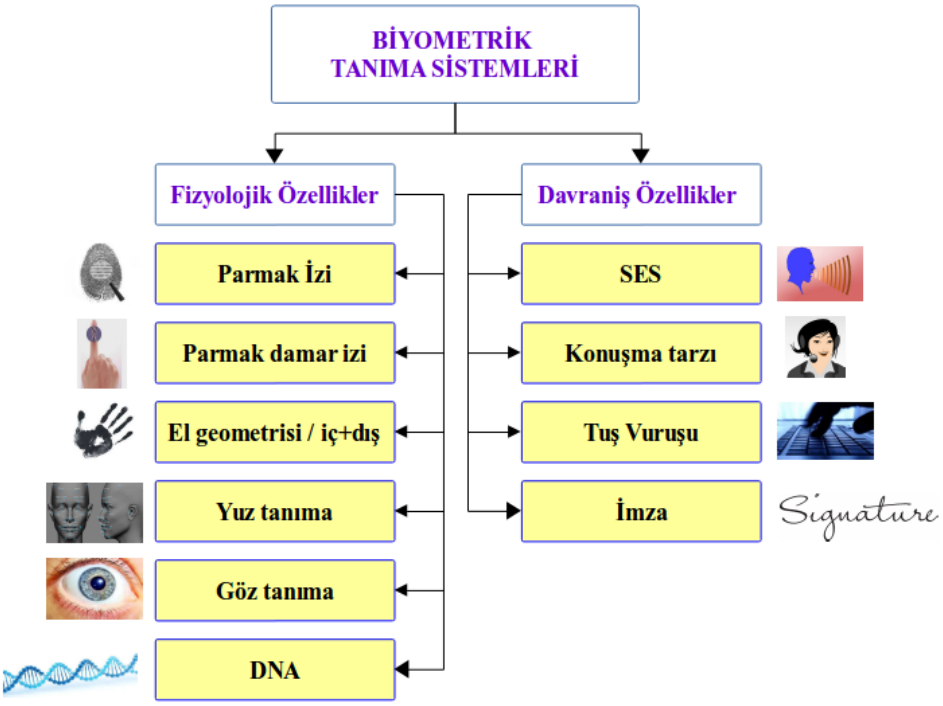
Bütün biyometrik tanıma teknoljiler için iki temel kullanım amacı vardır. Bu amaçlardan birincisi giriş izni isteyen kişinin isteğine cevap vermek, ikinci amaç ise kimliği girilen kişinin kayıtlarına ulaşıp kullacının kimliğini tespit etmektir. Bu iki işlem, birinci işlem kimlik doğrulama (ID verification), ikinci işlem ise kimlik tespiti (ID identification) olarak adlanmaktadır, ki bu iki yöntem temelde birbirinden çok farklıdır.

Kimlik sorgulama (ID identification) işleminde ise kişinin verileri veri tabanında var olup olmadığını sorgulanır ve eğer kişinin verileri sistemde varsa kullanıcnıya bilgileri

sunulur. Bu verilerin veri tabanında kesinlikle olup olmadığını bilmediği için sıralı butün veri tabanı üzerinde arama yapmaktadır ki bu işlem milyonlarca kayıt bulunan bir veri tabanında çok uzun süre gerektiren bir işlemdir. Bundan dolayı pahalı bir sistemin kurulması gerekir, bu tip gelişmiş sistem bir saniye içinde 100,000 kaydı sıralı olarak arayabilmektedir. Biyometrik tanıma sistemlerin yanlış kabul oranı, yanlış reddetme oranı ve çapraz hata oranı çizelge 2.4'de değerlendirilmiştir.

Kimlik onaylama (ID verification) işlemlerinde ise onaylanması istenen kimlik verileri veri tabanında mutlaka olmalıdır. Sorgulama işleminde ise önemli olan izin isteyen kişinin gerçekten veri tabanında kayıtlı olan kişi olup olmadığını belirlemektir. Bu tip işlem hashing fonksiyonu yardımıyla veri tabanına bir tek erişimi gerektirir, bundan dolayı çok hızlıdır, günlük yatımızda kullanılan çoğu biyometrik teknolijiler bu şekilde çalışmaktadır. Uluslararası Biyometrik Grubun 2007-2012, 2009-2014 ve 2010-2015 Biyometri pazar ve sanayi değişimleri şekil 2.2-2.4'te bulunmaktadır.

2.5 Biyometrik SınıflandırmaTürleri



Şekil 2.1 Biyometrik sistemlerin diğer yöntemler

2.6 Biyometrik Sistemlerin Karşılaştırılması

Çizelge 2.1 Farklı biyometrik teknolojilerin bir araya getirilip kullanılabilirlik özellikleri sınıflandırılmıştır.

Çizelge 2.1 Biyometrik sistemlerin kullanılabilirlik özelliklerinin sınıflandırılması (Gad and El-Sayed)

Boyometrik Sistemler	Evrensellik	Eşsizlik	Süreklilik	Elde Edilebilirlik	Perfonmans	Kabul Edilebilirlik	Yaygınlık
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
Tuş dinamikleri	Düşük	Düşük	Düşük	Orta	Düşük	Orta	Orta
El ven	Orta	Orta	Orta	Orta	Orta	Orta	Yüksek
DNA	Yüksek	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük
SES	Orta	Düşük	Düşük	Orta	Düşük	Yüksek	Düşük
İmza	Düşük	Düşük	Düşük	Yüksek	Düşük	Yüksek	Düşük
Kulak	Orta	Orta	Yüksek	Orta	Orta	Yüksek	Orta
Yüz Termogrami	Yüksek	Yüksek	Düşük	Yüksek	Orta	Yüksek	Yüksek
Iris	Yüksek	Yüksek	Yüksek	Orta	Yüksek	Düşük	Yüksek
Retina	Yüksek	Yüksek	Orta	Düşük	Yüksek	Düşük	Yüksek
Koku	Yüksek	Yüksek	Yüksek	Düşük	Düşük	Orta	Düşük
Yürüyüş	Orta	Düşük	Düşük	Yüksek	Düşük	Yüksek	Orta

Hemen hemen çoğu biyometrik teknolojilerde kullanılan bazı istatistiksel ölçümleri aşağıda sıralanmıştır.

FRR (FalseRejection Rate) - Yanlış reddetme oranıdır, ve yetkili kullanıcıyı reddeder, iyi biyometrik tanıma teknolojisi için bu değer düşük olmalıdır.

FAR (FalseAcceptence Rate) - Yanlış kabul etme oranıdır ve yetkili olmayan kişiyi kabul eder ki, iyi bir biyometrik tanıma teknolojisi için bu değer düşük olmalıdır.

FTE (FailuretoEnroll) - Biyometrik sisteme yeni kullanıcı kimliği oluşturmak istediğinizde başarısız olduğunda bu durum kayıt için arıza oranıdır. İyi bir biyometrik tanıma teknolojisi için budurum azaltılmış olmalıdır.

EER (EqualError Rate) - FRR ve FAR hesaplanarak bulunur. Eşit hata oranıdır ve iyi biyometrik sistemlerde bu oran düşük olmalıdır. (http://elektroteknoloji.com 2010)

Çizelge 2.2 Biyometrik sistemlerin karşılaştırılması (Yalçın ve Gürbüz 2015)

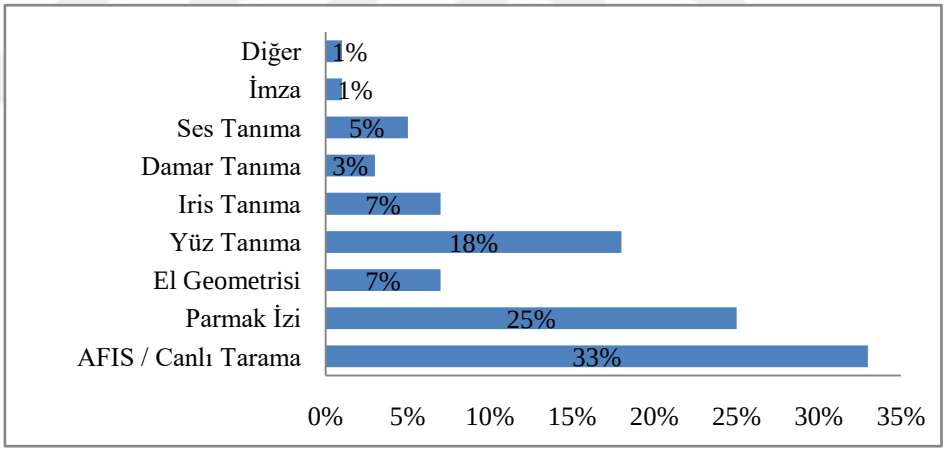
Faktörler	**Doğruluk**	**Kulanım Kolaylığı**	**Kulanıcı Kabul Oranı**
Parmak İzi	Yüksek	Orta	Düşük
El geometrisi	Orta	Yüksek	Orta
Yüz	Düşük	Yüksek	Yüksek
İris	Orta	Orta	Orta
Retina	Yüksek	Düşük	Düşük
Ses	Orta	Yüksek	Yüksek
İmza	Orta	Orta	Yüksek

Çizelge 2.3 Biyometrik yöntemlerinin karşılaştırılması (http://elektroteknoloji.com 2010)

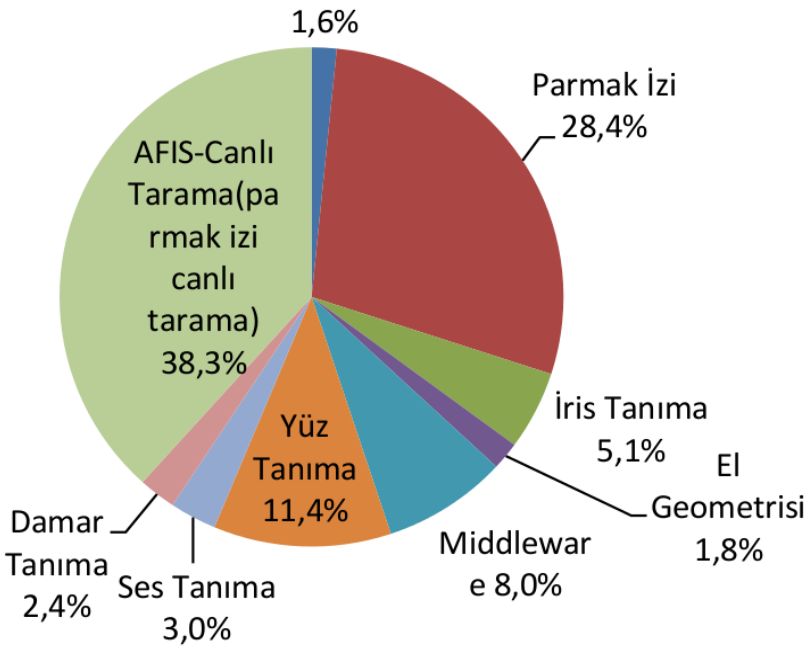
Yöntem	**Olumlu Taraflar**	**Olumsuz Taraflar**
Parmak İzi Tanıma	- güvenilir, çok yaygın, ucuz - küçük sensoru var	- insanların %3-7'sinin parmak izi kullanılamıyor
El Geometrisi Analizi	- hızlı, veri boyutu düşük - kullanımı kolay	- güvenilirliği tam değil - sensoru çok büyük
Yüz Tanıma	- ucuz	- güvenilirliği tam değil
Yüz Termografisi	- çok güvenilir	- henüz ticari kullanıma geçmedi - infrared kamera çok pahalı
İris Analizi	- çok güvenilir, resim hiç değişmiyor	- kameralar çok pahalı
Retina Analizi	- en güvenilir yöntem	- tarama yapılırken kafa sabit durmalı
Ses Tanıma	- kullanımı kolay - telefonlarda kullanılabiliyor	- güvenilirliği oldukça az
İmza Tanıma	- ticari anlaşmalarda çok kullanışlı	- güvenilirliği az - birden fazla örnek gerekiyor

Çizelge 2.4 Biyometrik sistemlerin değerlendirilmesi (Srivastava 2013)

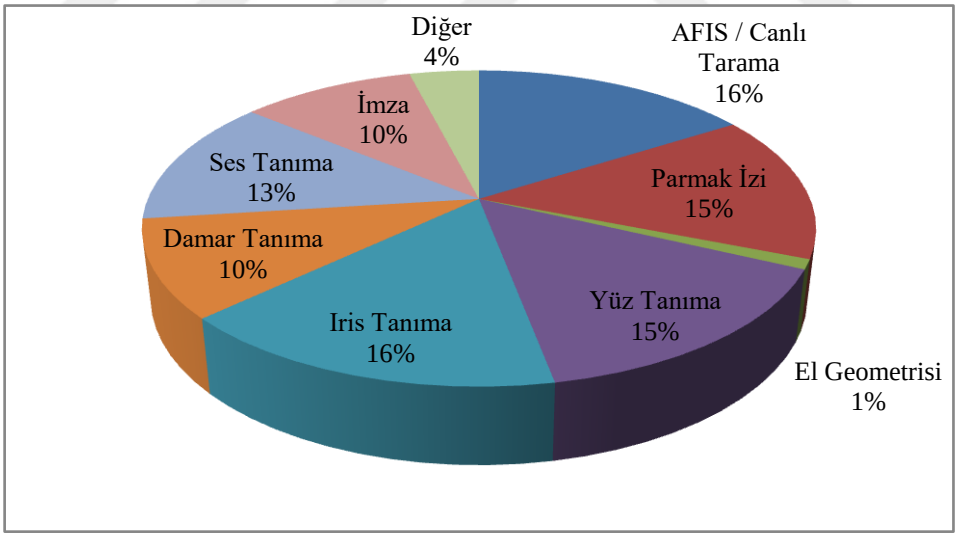
Boyometrik Sistemler	Yanlış Kabul Oranı	Yanlış Reddetme Oranı	Çapraz Hata Oranı	Kayıt için başarısızlık	Yakalama başarısızlık Oranı	Algılayıcının mesafesi
Parmak İzi	2.00%	2.00%	2.00%	1.00%	-	Sıfır
Yüz Tanıma	1.00%	20.00%	-	NA	NA	~ 20 m
El geometrisi	2.00%	2.00%	1.00%	NA	NA	10 cm
Avuç içi	-	-	-	-	-	Sıfır
DNA	-	-	-	-	-	Sıfır
SES	2.00%	10.00%	6.00%	-	-	20 cm
İmza	-	-	-	-	-	Sıfır
Kulak	-	-	-	NA	NA	~ 5 m
Iris	0.94%	0.99%	0.01%	0.50%	-	30 cm
Retina	0.99	1.00%	0.04%	0.80%	-	2 cm
Yazma ritimi	7.00%	0.10%	1.80%	-	-	Sıfır



Şekil 2.2 Uluslararası Biyometrik Grubun 2007-2012 Biyometri pazar ve sanayi



Şekil 2.3 Uluslararası Biyometrik Grubun 2009-2014 Biyometri pazar ve sanayi



Şekil 2.4 Uluslararası Biyometrik Grubun 2010-2015 Biyometri pazar ve sanayi

2.7 Biyometrik Sistemlerin Kullanım Alanları

Banka ATM'lerinde kullanıcı tanımlama, kredi kartı güvenliği,

Binalara, tesislere ve ofislere erişim güvenliği,

CRM uygulamaları,

Çağrı merkezlerinde kimlik tespiti,

Çek onaylama işlemlerinde kullanıcı güvenliği,

Elektronik öeme, elektronik bilet satışı,

E-ticaret işlemleri

Gemi ve Limanlarında güvenliği için,

Hastanelerde hasta kayıt ve kimlik tespitleri,

Havalimanlarında check-in ve boarding işlemleri,

İnternet bankacılığında kullanıcı tanımlama,

Kamu hizmetlerine yöelik kayıt takibi (SGK, vergi, trafik) sayılabilir.

Kiosk'larda kullanıcı tanımlama,

Kiralık kasalara erişim güvenliği,

Kombine bilet uygulamaları,

Kurumsal ağ, kişisel bilgisayar ve taşınabilir bilgisayar güvenliği,

Maçarda kombine bilet uygulamaları,

Okullarda öğrenci devam takip ve erişim kontrol, veli kontrolü

Personel devam ve takip kontrolü

Satış noktası terminallerinde (POS) kullanıcı tanımlama,

Sınır kontrolüve sınır kapılarından girişlerin kontrolü

Ulusal kimlik uygulamaları, sürücü ehliyeti ve pasaportlarda kimlik tespiti,

Üyelik gerektiren spor salonu uygulamaları,

Yüsek güvenlik bögelerine erişim kontrolü (http://www.ispozelguvenlik.com.tr 2014).

3. YÜZ TANIMA SİSTEMİ

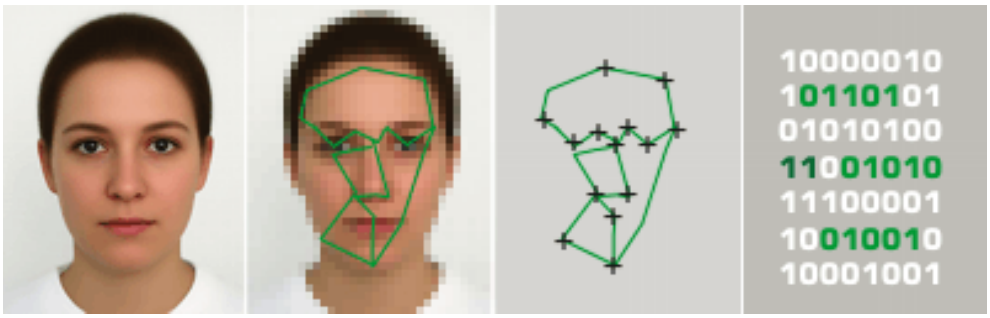
3.1 Yüz tanıma tarihçesi

İlk resim yüz sınıflama metodu 25 Mayıs 1888 yılında Sir Francis Galton tarafından bulunmuştur. 1990'dan itibaren yüz tanıma sistemine ihtiyaclardan dolayı ilgi artmıştır. Bunun sebebi ar-ge çalışmaların artması, suçlu tanıma, suçlu ve teröristlerin hareketleri, veri merkezlerine giriş, suçlu insanların kimlik tespiti, akıllı kartlarda, havaalanlarında ve sınır kontrollerinde kullanabileceği için önem kazanmıştır.

Her yüz farklı karakteristik özelliklere sahiptir. Her insan yüzü yaklaşık 80 düğüm noktasına sahiptir. Yüz tanıma teknolojisiyle yüzdeki yaklaşık 50-80 noktayı inceleyerek, gözler arasındaki mesafe, burun genişliği, göz çukurlarının derinliği, elmacık kemiklerinin şekli, çene hattının uzunlukları vs. ölçülür.

Bu verilerden şablon oluşturarak sonucunda bir teknoloji oluşturulur ki bu teknolji bilgisayar yazılımlarında kullanılarak uygulanmaktadır. Yüz tanıma sistemleri günümüzde günden güne bir çok alanda yer almaktadır.

Örnek olarak pasaport kontollerinde kullanılan biyometrik fotoğraflar ICAO (International Civil Aviation Organization – Uluslararası Sivil Havacılık Organizasyonu) tarafından bir standart fotoğraf olarak belirlenmişler. Bu tip fotoğraflar makinede okunabilen uluslararası pasaportlarında (kimliklerinde) kullanılan yüksek kaliteli, belirli ölçü ve özelliklere sahip olan fotoğraftır ki insanın yüz biyometrisini tespit edilebilmesi için kullanılmaktadır. Uluslararası pasaportlarında (e-pasaport, çipli kimlikler) parmak izi, yüz ve göz bebeği olmak üzere üç çeşit biyometrik verilerin kullanılması mümkündür, ama ICAO uyulamalarında göz bebeği biyometrisine henüz geçilmemiştir, ancak bazı ülkeler tarafından bu konudaki çalışmalar halen devam etmektedir (http://ispozelguvenlik.com.tr 2014).



Şekil 3.1 Yüz tanıma sistemini çalışma şekli (http://personel-takip.com 2015)

Biyometrik sistem olarak hayatımızın içinde yer alan yüz tanıma sistemleri ile kişinin fiziksel özellikleri anında araştırılmakta ve güvenlik açısından tedbirler alınmaktadır. Yüz tanıma sistemleri geniş bir alana yayılmış ve bu sayede güvenlik açıkları kapatılmaya çalışılmıştır. Tıpkı parmak izi gibi yüz tanıma sisteminde de kişilerin farklı yüz yapıları kolaylıkla teşhis edilebilmektedir.

3.2 Yüz tanıma sistemi nasıl çalışır

Yüz tanıma sisteminin sağlıklı çalışabilmesi için video ve termal görüntüleme tekniklerinin kullanılması gerekir. Video ile yüzün belli alan görüntüleri alınır ve yüzün fotoğrafı çekilerek sisteme kaydedilir. Bu fotoğraf çekildiğinde sistem yüzün ayırt edici tüm özelliklerini hafızasında tutar. Yüz tanıma sisteminde kullanılan termal kamera ise veya 3D kamera ile yüzün altında oluşan kan akışını analiz ederek kişinin belirleyici özelliğine göre kod oluşturur ve bu şekilde kişinin kimlik bilgileri de girilerek işlem tamamlanmış olur. Yüz tanıma sistemleri herhangi bir cerrahi operasyonun geçirilmesinde dahi çalışır. Ancak yüz doğrulama sistemi çalışırken karar verilmesi zorlaşır. Karanlıktan etkilenmeyen termal kameralar yüz tanıma programında oldukça etkin şekilde çalışmaktadır.

3.3 Yüz tanıma sistemleri nerelerde kullanılır

En çok kullanıldığı alanlar içinde özellikle güvenlik birimleridir. Suçlu ve terörist taramalarında oldukça sık kullanılır. Son zamanlarda kimlik, sürücü belgesi ve pasaportlarda da kullanılmaya başlanmıştır.Bunların yanında güvenlik alanlarında personelin giriş çıkışlarını tespit etmek için kullanılmaktadır. Bu sayede özellikle güvenlik şirketleri personelin kontrol edilmesinde oldukça etkili olduğu bilinmektedir. Bariyer veya turnike olan bölgelerde kişilerin yüz analizleri yapılarak giriş çıkışı engelli olan kişileri tanımada oldukça güvenli ve yararlı bir sistemdir.

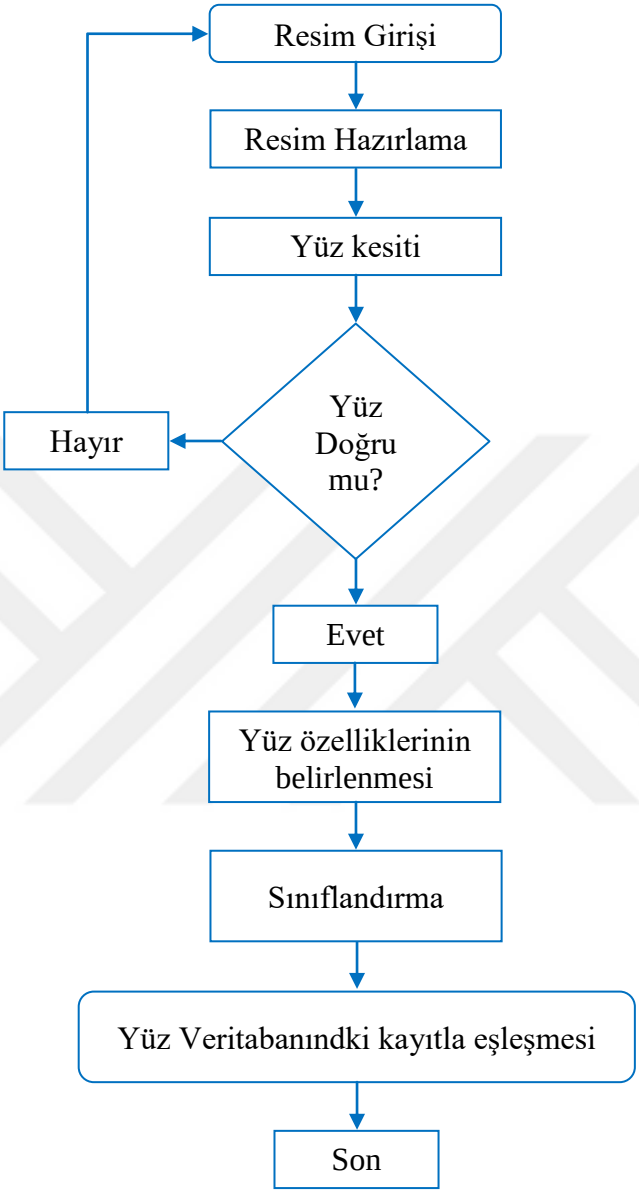
3.4 Yüz tanıma algoritmaları

Yüz tanıma algoritmaları genelde iki gruba ayrılabilir. Bu iki gruptan birincisi "resimler üzerinden yüz tanıma tekniğidir" ikincisi ise "hareketli bir görüntü üzerinde yüz tanıma tekniğidir". Bu iki teknoloji günümüzde onlarca yüz tanıma sistemlerinde kullanılmaktadır. Bu teknolojileri örnek olarak mobese kameralarında, sınır ve gümrük kapılarında, pasaport kontrollerinde ve şirketlerin giriş-çıkış uyulamarında kameralarda yüz tanıma sistemleri rastlanabilir.

Sınırlarda passaport kontrollerinde insanın yüzündeki biyometrik detayları kişi ile eşleştiriyor ve bir sonraki geçişleride aynı kişi olup omadığını tespit eder. Bu yöntemde insanın yüzündeki biyometrik özellikleri ağız ve burun ile arasındaki uzaklık, gözlerin uzaklığı ve ağız genişliği oranı gibi özellikleri tanıyarak sistemdeki veri tabanına kayıt eder.

Sonra yeni geçişlerinde kişi sadece geçişteki kameraya baktığı durumda eski ve yeni biyometrik veriler sistem tarafından karşılaştırarak giriş veya çıkış yapabilir. Mobese kameralarında kullanılan uygulama daha önceden veri tabanına kaydedilmemiş bir görüntünün anlık yakalanan görüntülerle karşılaştırılması mantığına dayanmaktadır.
Böylece suçlu veya başka bir aranan kişinin resmi veri tabanında kayıt edilip diğer kontrol edilen kişilerin resimleri veri tabanında tutulmamaktadır. Bu tip yöntemin en

büyük dezavantajı işlenecek verilerin çok olmasından dolayı iyi donanıma sahip olunması gerekmektedir.



Şekil 3.2 Yüz tanıma algoritması

3.5 Yüztanıma algoritmaların işlemleri

- Video kameradan, web kameradan, trafik kameradan kaynak olarak resim girişi,
- Resmin tamamının alınmasından sadece bir bölümünün alınması için hazırlanması,

- Aldığı kesitli resimden veri tabanında var olan kesit ile karşılaştırılması,
- Başarısız durumda resim girişinden itibaren adımların tekrar edilmesi,
- Yeni bir yüz kaydının alınması veya veri tabanındaki kayıtla eşleşmesi,
- Yüzün biyometrik özellikleri belirlenerek veri tabanına kaydedilmesi.

Hemen hemen çoğu yüz tanıma sistemlerinde kullanılan algoritmalar:
PCA (Principal Component Analysis) - Görüntüdeki kısımları tespit etikten sonra spesifik kısımlar kalacak bu algoritma o görüntünün sıkıştırılıp karşılaştırılması esasına dayanır. PCA yöntemini kullanmak için tanıma işleminin gerçekleştirilmesi için yeni alınan yüzün resimleri veri tabanında bulunan resimler ile aynı boyutta olması gerekir. Bu yöntemde kullandığınız resimler veri tabanında sıkıştırılmış ve küçültülmüş şekilde bulunur, bu durumda veri tabanın yükünü azaltmış ve yüz tanıma hızını arttırmış olacaktır.

ICA (Independent Component Analysis) - Bu algoritma görüntüdeki temel bir bileşeni tespit ediyor ve diger bileşenlerin fonksiyonların çıkarılmasına dayanır. Görüntünün yaklaşık değerlerini çıkarıp bu değerler üzerinden işlem yapılabilmesini sağlar.

LDA (Linear Discriminant Analysis) - Bu algoritmanın amaçı verilerin sınıflandırması için gerekli ayırt edici öznitelikleri seçmektir, ayırt edici olmayan öznitelikleri elemektir. Bu şekilde resimleri analiz ederken görüntülerin içerikleri değil özniteliklerine göre analiz edebilen bir yöntemdir.

EP (Evolutionary Pursuit) - Bu algoritma görüntüleri analiz etmektedir, kişinin karakteristik ve evremsel özelliklerine göre sınıflandırma ve tanıma yapılmaktadır.

EBGM (Elastic Bunch Graph Matching) – Bu yöntem insan yüz üzerindeki kritik noktaların işaretlenmesini sağlıyor ve bu noktaları kullanarak bir özellik vektörü belirliyor, ondan sonra grafik şablonları kullanarak eşleştirilmesini yapıyor.

Trace Transform Radon - İz Radon Dönüşümü - Yüz tanıma sistemlerinde radon dönüşümü iki boyutlu uzayda düz çizgileri uygulanan integral dönüşümüdür. Radon ters radon ile yüz görüntülerinin tekrar oluşturmasını sağlıyor. Radon algoritma iz dönüşüm yaparken cisimleri tanırken rotasyon boyutlandırma gibi transformasyonların etkileri ortadan kaldırılıyor ki, bu durumda farklı açılardan görüntüsü alınan cisimlerde tanımlama yapabilir.

AAM (Active Appearance Model) - Bu algorıtmayüz tanıma sistemlerde gri resimler veya görüntülerin üstünde hatmin ve hedef noktaları arasındaki farkların hesaplanmasını (leastsquares) sağlar.

3D Morphable Model – Bu algoritma ile görüntüyü veri tabanındaki diğer görüntülerle birleştirerek ortaya çıkan yeni görüntüye olan uyumluluğunu kontrol etmektedir. Bu şekilde ortam şartlarına bağlı kalınmadan yüksek seviyede uygun olan görüntü elde edilmektedir.

3D Face Recognition – Bu yöntem yüz tanıma sistemlerinde insanların yüz üzgünlüğü, mutluluğu, heyacanlığı ve sinirliği gibi durumları ortaya çıkarır. Ortaya çıkan durumları kullanarak birleştirme takdirinde bu durumları kontrol ederek uyumun en yüksek seviyede olmasını sağlamaktadır (Varol ve Cebe 2011).

3.6 Tanımlanan görüntü kalitesi parametreleri

- Farkedilebilir deri yapısı
- Fluluk/Odak
- Gözlük ya da diğer engellerin varlığı
- Hız
- Kafa ebatları ve çözünürlüğü
- Kafa kırpma
- Kontrast

- Parlaklık
- Parlama varlığı/yokluğu
- Poz
- Yüzle ilgili olmayan objelerin otomatik eliminasyonu
- Yüzün görüntüdeki konumu (örn. ortalanmış) (http://www.ergosis.com.tr 2016).

3.7 Yüz tanıma sistemlerin uygulanabileceği alanlar

- Araştırma ve geliştirme ortamaları
- Casinolar ve eğlence parkları
- Fabrikalar
- Finans sektörü
- Hapishaneler
- Havaalanları ve sınır geçişleri
- Perakendeciler
- Polis ve emniyet uygulamaları
- Spor tesisleri, spor karşılaşmaları (http://www.ergosis.com.tr 2016).

3.8 İki boyutlu görüntülerde poz doğrultma

Yüzdeki poz değişimi yüz tanıma sistemlerinin performanslarını etkileyen en büyük problemlerden biridir. Bu çalışmada tam karşıdan çekilmiş, tek bir giriş görüntüsünden, o kişinin farklı pozlara sahip görüntülerini sentezleyen bir yöntem tanıtılmaktadır. Genellikle yüz tanıma sistemleri ya tam karşıdan çekilmiş yüz görüntülerinde çalışmakta ya da belirli pozlara sahip yüz görüntülerinde çalışabilmektedir. Fakat gerçek hayatta varsayılan yüz pozlardan farklı bir yüz sisteme giriş olarak gelebilmekte bu ise tanıma başarımını çok büyük oranda etkilemektedir.

Poz sentezi için oluşturulan eğitim kümesinde tam karşıdan bakan bir kişinin farklı pozlarına ait tüm resimlerdeki doku ve bu resimlerdeki yüze ait şekil bilgisi

kullanılmıştır. Yüz şekil bilgisinin oluşturulmasında 73 adet nokta kullanılmıştır. Bu çalışmadaki amaç var olan karmaşık yüz poz sentezi yöntemleri yerine oldukça basit ve örnek tabanlı çalışan bir yöntemi tanıtmaktır. Var olan yüz poz sentezi yöntemleri incelendiğinde genellikle 3B(3 Boyutlu) bilgisine ihtiyaç duyulduğu görülecektir. Oysaki +45/-45 düzlem içi ve düzlem dışı yüz pozlarının sentezlenmesinde 3B bilgisi kullanmaksızın,sadece basit doğrusal bükme ve yüz şekil bilgisini oluşturan noktaların uyarlanır olarak deforme edilmesiyle farklı poza sahip yüzler belirli bir yakınsamayla sentezlenebilir. Yüz belirli bir açıyla sağa/sola veya yukarı/aşağı baktığında, yüz şeklinden bağımsız olarak yüzü oluşturan doku üçgenleri yaklaşık olarak aynı açısal yolu alırlar. Bu ise yüzü oluşturan doku üçgenlerinin belirli bir kurala göre deforme olması, ölçek değiştirmesi ve/veya konum değiştirmesi anlamına gelir. Eğitim kümemizdeki yüzlere ait doku üçgenlerinin poza göre nasıl bir değişim yaptığı şekil bilgisini oluşturan noktaların hareketi referans alınarak modellenebilir. Bu noktalar üzerine Delaunay üçgenleri oluşturulduğunda poz değişimi modellenebilmektedir.

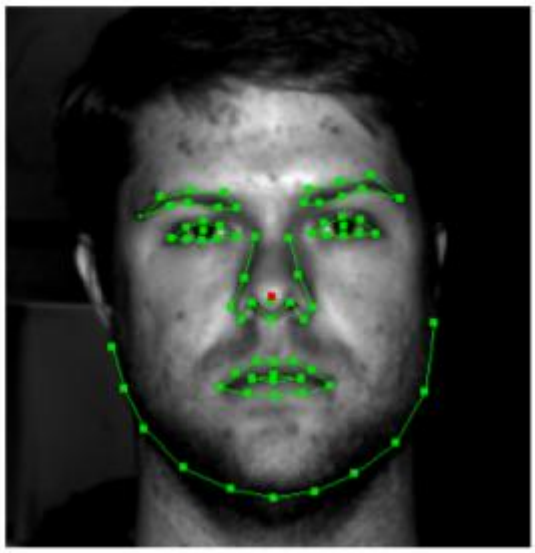
Poz sentezindeki en büyük zorluk yüzün poz değişimi neticesinde yüze ait bazı bölgelerin bir kısmı veya tamamının görünmez (self-occlusion) hale gelmesidir. O bölgelerdeki üçgenler her ne kadar ihmal edilecek kadar küçültülmüş olsa da, bu gibi durumlarda sentezlenen yüzde sentetik çıkıntı/kenarların oluşmasına sebebiyet verebilmektedir.

Bilgisayarla görü teorisine göre herhangi bir nesnenin hassas 3B geometri bilgisini elde edebilmek için en az üç adet o nesneye ait görüntüye ihtiyacımız var. Bunun yanında tek bir görüntüde 3B geometriyi kuracak yeterli bilgi bulunmamaktadır. Fakat gerçek hayatta, her kişinin üç adet görüntüsüne sahip değiliz. Blanz ve Vetter'in önerdiği bozulabilir model uydurma yöntemiyle, 3B yüz verilerinden oluşan eğitim kümesiyle kurulan model yardımıyla 2B tek bir görüntüden özgün pozlar elde edilebilmektedir. Fakat bu ve benzeri 3B yaklaşımların en büyük problemi hesaplama maliyetlerinin çok yüksek olması. Blanz ve Vetter'in yönteminde 3B uydurması için gerekli süre yaklaşık olarak 5 dakika civarıdır. Bu tür bir hesaplama maliyeti gerçek zamanlı sistemlerde benzer yaklaşımların kullanılmasını zorlaştırmaktadır. Bunun yanında 3B yüz tarama için özelleşmiş 3B tarayıcılara ihtiyaç olması ve bu tür donanımların hem çok maliyetli

hem de yeterli çözünürlükteki 3B veri için tarama süresinin mevcut teknolojiyle oldukça uzun sürmesi 3B yaklaşımların olumsuz taraflarıdır.

Bu çalışmada tanıtılan ve oldukça yüksek maliyetli olan 3B bozulabilir model benzeri bir yaklaşım için uydurma (fitting) modelini 2B verideki poz değişimlerinin basit bir modeli çıkartılarak çok daha hızlı ve etkin bir yakınsamanın sağlanabileceği gösterilmeye çalışılmıştır. Yönetimin oluşturulmasındaki temel düşünce poz değişiminde asıl değişimin doku değil şekil olduğu düşüncesidir. Vetter ve Poggio'nun tanıtılan doğrusal-nesne-sınıfı yöntemi ve bu yöntemin daha sonraki versiyonlarının 45-90 derece gibi poz değişimlerinde oldukça kötü sonuçlar ürettiği görülmektedir. Ayrıca 0-45 derecelik poz değişimlerinde derinlik bilgisi fazlaca hissedilmediği için sadece 2B görüntüler modellenerek yeni bakış açıları ve eğitim kümesindekilerden farklı pozlar sentezlemek mümkün olduğu görülecektir.

Yale B veri kümesinde yer alan resimlerin yüze ait 73 adet önemli noktaları işaretlenmiştir. 73 adet yüz önemli noktalarının yüz bileşenlerine göre dağılımı şu şekildedir: 14 nokta ağız, 12 nokta burun, 9 nokta sağ göz, 9 nokta sol göz, 8 nokta sol kaş, 8 nokta sağ kaş ve 11 nokta çene yayı (Şekil 3.3) (Gökmen ve Kahraman 2007).



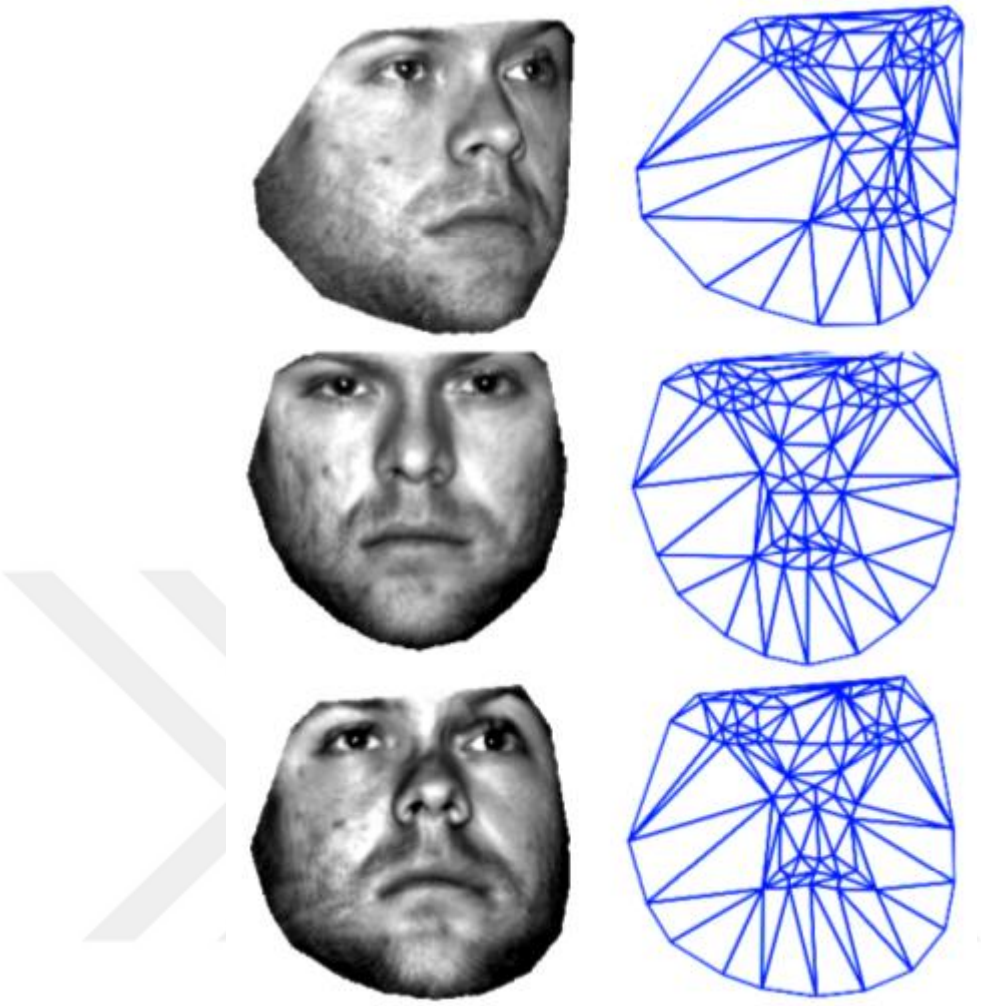
Şekil 3.3 73 nokta ile işaretlenmiş yüz görüntüsü (Gökmen ve Kahraman 2007)

Eğitim kümesindeki tüm insan yüzlerinin önemli noktaları elle belirlenmiştir. Eğitim kümesindeki tüm yüzleri { (S0 , T0) } şeklinde ifade edebiliriz:

$$S\,0 = ((x1, y\,1) , (x2, y\,2) ,..., (xK, y\,K)) \in R\,2\,K \quad (3.1)$$

S0 yüze ait K adet önemli noktadan oluşan Şekil vektörü, T0 ise S 0 ile belirlenen alandaki yüze ait doku bilgisidir. Şekil 3.3'de yüz şekil bilgisi ve bu şekle göre eğilip kesilen (warp+crop) yüz dokusu gösterilmektedir. Ayrıca şekil 3.4'de aynı kişinin farklı pozlardaki yüz doku ve şekil değişimlerini gösterilmiştir.

Farklı pozlarda yüz şekil ve doku bilgisinin nasıl değiştiğini şekil 3.4.a, b'ye bakarak anlayabiliriz. Dikkat edilirse üç farklı pozdaki en büyük değişim yüz Şekil bilgisini oluşturan tel-örgü üçgenlerinde olduğu görülecektir. Her üç pozda da yüzü oluşturan üçgen sayısı eşittir, çünkü yüz üzerindeki önemli noktaların sayısı sabittir. Pozdaki değişimle üçgenler ölçek ve şekil değiştirmekte ve buna bağlı olarak dokuyu oluşturan beneklerde enterpolasyon yöntemi ile değişmektedir. Her bir pozdaki doku bilgisi alınıp referans bir yüze, tam karşıdan bakan yüze ait tel-örgünün üzerine yeniden kurulursa yaklaşık olarak benzer ve tam karşıdan bakan bir yüz görüntüsü oluşturduğu görülecektir. Bunun anlamı iki boyutlu bir yüz görüntüsü üzerinde şekil deformasyonu yapılarak farklı pozlar elde edilebileceğidir.



Şekil 3.4 Yüz poz değişimi: a. Yüz dokusu, b. Yüz önemli noktaları üzerine (Gökmen ve Kahraman 2007)

2B görüntülerden doğrusal bükme ve hizalama yardımıyla yüz poz doğrultmaktaki birincil amacımız, yüz saptama aşamasında önemli noktaları belirli bir doğrulukla bulunan yüzlerden tanıma amaçlı öznitelikler çıkartmadan önce kurulan poz deformasyon modeli yardımıyla eğitim kümesindeki bakış açısına yüzü doğrultmaktır. Bu işlemi ön-işlem olarak kabul edebiliriz. Eğitim kümesindeki yüksek karşıtlığa sahip görüntüler kullanılarak kurulan yüz uzayına, test görüntüsü olarak aynı özelliklere sahip, fakat düşük karşıtlığa sahip bir yüz iz-düşürüldüğünde, modelimiz doğru olmasına rağmen tamamen hatalı öznitelikler elde ederiz. Bu problemin çözümünde yapılması gereken yüz uzayına iz-düşürülecek görüntülerin mümkün olduğunca eğitim kümesindeki yüzlere benzer hale getirmektir. Aynı şekilde sadece karşıdan bakan

yüzlerden oluşturulmuş yüz uzayına, farklı pozdaki bir yüz iz-düşürülüp, elde edilen öznitelik vektörlerle yüzü geri-çattığımızda tümüyle hatalı bir yüz elde edilecektir (Gökmen ve Kahraman 2007).

3.9 "Bio Access Terminal" Uygulamada Kullanılan Önemli Fonksiyonlar

Yüz Bölgesinin Tespiti

1. public HaarCascade face = newHaarCascade("haarcascade_frontalface_default.xml")

Yüz tespiti yapan metoddur.Bu metot yüz bulma işlemini haarcascade sınıflandırıcısını kullanarak gerçekleştirir.

2. MCvFont font = new MCvFont(FONT.CV_FONT_HERSHEY_COMPLEX, 0.5d, 0.5d)

Yüz bulma ve tanıma video kameradan yapılıyorsa, bulunan kişi bilgileri hemen yüz bölgesinin altına yazılmaktadır. Yukarıdaki ifade kullanılan yazıya ait tanımlamayı gösterir.

3. Capture grabber

Video kameradan kare (frame) kare görüntüleri yakalayan ve bunları kendinde saklayan Emgu CV sınıfından oluşturulmuş bir değişkendir.

4. facesDetected = gray.DetectHaarCascade(face, 1.2, 10, new Size(80, 80))

Verilen görüntüde dikdörtgen bölgeleri bulur ve bir dizi olarak bu bölgeleri saklar.Görüntüdeki yüz bölgesinin koordinatlarını hesaplar.

5. currentFrame.Convert<Gray, Byte>();

Video kameradan yakalanan anlık görüntünün rengini gri olarak değiştiren fonksiyondur.

6. currentFrame.Copy(facesDetected[0]).Convert<Gray, byte>().Resize(100, 100, Emgu.CV.CvEnum.INTER.CV_INTER_CUBIC)

Görüntüdeki yüz bölgesini tespit ettikten sonra bu bölgeyi kopyalayan fonksiyondur.

7. currentFrame.Draw(facesDetected[0], new Bgr(Color.Green), 2)

Görüntü üzerinde yüz bölgesini çerçeve olarak çizen fonksiyondur (çizginin rengi ve kalınlığıdır).

Gerekli EmguCV Kütüphaneleri

1. Emgu.CV.dll

OpenCV resim işleme aşağıdaki fonksiyonlarını içerir, bunlara:

- Capture
- EigenFaceRecognizer
- EigenObjectRecognizer
- EigenObjectRecognizer.RecognitionResult
- FisherFaceRecognizer
- HaarCascade
- Retina

örnek olarak verilebilir.

2. Emgu.CV.UI.dll

Resim görüntülemek için kullanıcı arayüzü sağlar, ve bu arayüzlerden bazıları şunlardır:

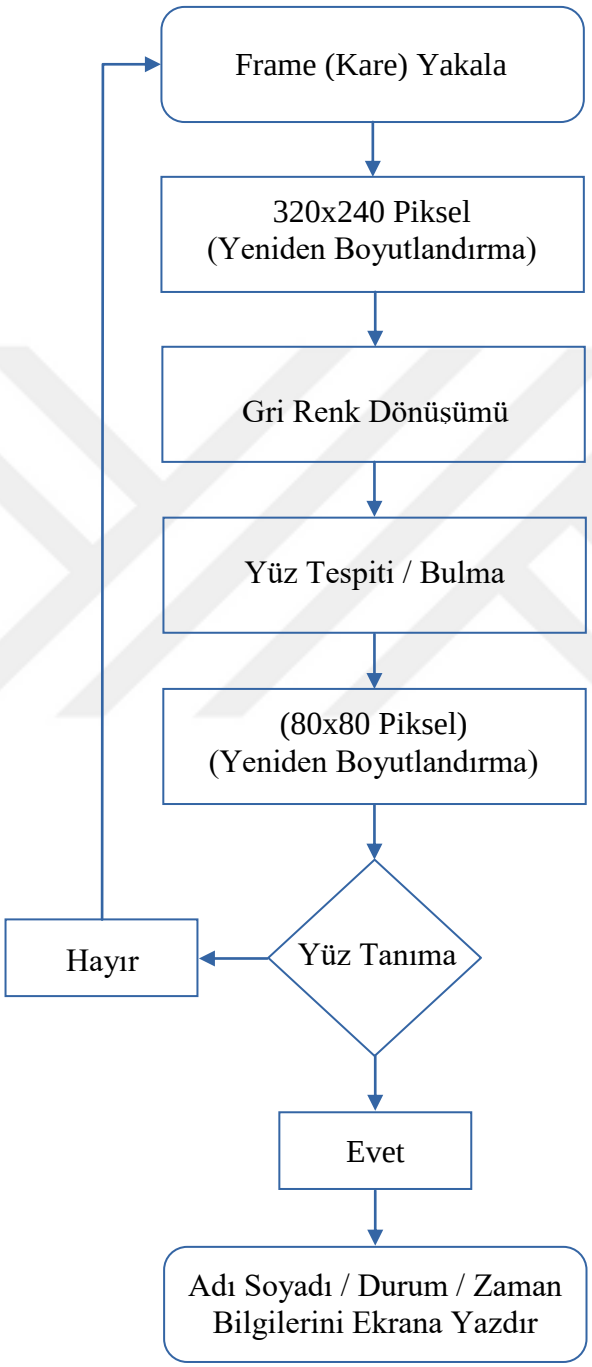
- HistogramBox
- HistogramViewer
- ImageBox
- ImageViewer
- MatrixViewer

3. Emgu.Util.dll

Emgu.CV projeleri tarafından kullanılan araçlar kolleksiyonudur, bunlara örnek olarak:

- CvException
- CvToolbox

- DataLogger
- TbbTaskScheduler
- VectorOfDataMatrixCode, verilebilir.



Şekil 3.5 “Bio Access Terminal” uygulamanın yüz bulma modülü

4. BİYOMETRİK PERSONEL KONTROL SİSTEMİ (BİPEKS)

4.1 Tanımı ve Yapısı

Biyometrik sistem olarak hayatımızın içinde yer alan parmak izi tanıma, parmak damar tanıma ve avuç tanıma sistemleri gibi yüz tanıma sistemleri ile kişinin fiziksel özellikleri anında araştırılmakta ve güvenlik açısından tedbirler alınmaktadır. Biyometrik sistemleri geniş bir alana yayılmış ve bu sayede güvenlik açıkları kapatılmaya çalışılmıştır. Yazmış olduğum uygulama Biyometrik Personel Kontrol Sistemi (BİPEKS) diğer biyometrik sistemler gibi merkezi veritabanından algılama ve tanımlama özelliklerine sahiptir.

Biyometrik Personel Kontrol Sistemi (BİPEKS)'inher bir yöntemin ayrı ayrı çalışabileceği şekilde tasarlanmıştır. Bu da kullanıcıya geniş bir seçim olanağı sunmakta, farklı yöntemlerin performanslarını izleme ve değerlendirme imkanı vermektedir.

Biyometrik Personel Kontrol Sistemi (BİPEKS) uygulama Microsoft Visual Studio 2012 C#.Net programı kullanılarak geliştirilmiştir. Görüntü işleme algoritmaları için Emgu CV ve OpenCV kütüphaneler, veritabanı işlemleri için MS SQL Server 2012 kullanılmıştır.

Tasarımı, Arayüzü, Alt Yapısı ve Yazılımı %100 tarafımca geliştirilmiş olup, sistemin kod içinde herhangi başka bir uygulamadan yabancı kod kullanılmamıştır. Bundan dolayı müşterilerin özel sektor veya kamu kuruluşlarında değişiklikler ve güncellemeler yazılım alanında kolaylıkla yapılabilmektedir.

Sistem tasarımında aşağıdaki özelliğe dikkat edilmiştir:
Biyometrik Personel Kontrol Sistemi (BİPEKS)sistemi geliştirilmeye açık bir yapıya sahiptir. Gerek duyulan ihtiyaçlara göre sistem fonksiyonları geliştirilebilir veya

değiştirilebilir. Biyometrik Personel Kontrol Sistemi (BİPEKS) sistem birbirinden bağımsız birçok fonksiyonun birleşimiyle meydana gelmiştir, böylece sistemdeki karmaşıklığın önüne geçilmiştir.

Biyometrik Personel Kontrol Sistemi (BİPEKS) uygulamasının çeşitli kurumlarda kullanılabilmesi için gereken bilgisayar bilgilerini sunulmuştur.

4.2 Sistem Gereksinimleri

CPU:

- Intel Core i3, i5, i7 2.0GHz veya üzeri

Bellek (RAM):

- 2 GB sistem belleği veya üzeri

İletişim Sistemi:

- Windows 7, 8, 8.1, 10
- Windows Server 2008 R2
- Windows Server 2012 R2

Ek programlar:

- Microsoft .NET Framework 4.0 veya daha yeni bir sürüm
- MS SQL Server 2012 / 2014 / 2016

Gerkli Disk Alanı:

- Windows – 7 Gb maksimum
- BİPEKS uygulama için – 250 MB
- Microsoft .NET Framework – 100 MB
- MS SQL Server – 20 Gb minimum

Yönlendirici:

- Minimum: 802.11 a/g yönlendirici
- Önerilen: 8.02.11n 5Ghz yönlendirici veya Ethernet

4.3 Arayüzü ve Ayarlar

Günümüzde piyasada en yaygın olarak PDKS (Personel Devam Kontrol Sistemler)' inden kartlı sistemler yer almışlartır. Bunun sebebi ise kartlı sistemlerin kolay kulanımı, uzun ömürlü olması, arıza ve dektek oranı düşük ve maliyeti gibi önemli avantajlara sahip olması. Bu avantajların yanında kartlı sistemlerin dezavantajlarıda vardır. Bu dezavantajlar; bireysel kartınızı başka kişi tarafından kullanabilme olasılığı yüksek, sistemin güvenlik açığı, kart bozulması gibi dezavantajları var ki, şirketler ve kamu kuruluşları tarafından PDKS (Personel Devam Kontrol Sistemi) olan Biyometrik Sisteme ilgi ve tercihleri arttırmıştır.

4.4 Fonksiyonlar ve Özellikleri

Fonksiyonlar

- Yeni kullanıcı ekleme, güncelleme ve listeleme (sınırsız)
- Var olan kullanıcılara rol verme (Admin, User veya İnsan Kaynakları gibi...)
- Yeni kullanıcının hesabını otomatik olarak oluşturabilmesi
- Kullanıcının bilgileri güncelleyebilmesi ve şifre değiştirebilmesi
- Şirketin bilgileri: Şube, Bölüm, Birim, Pozisyon vb. gibi ekleyebilmesi
- Terminal listesine yeni terminal eklenebilinmesi
- Personel listesininrapor veya çıktısının alınabilinmesi
- Personele birden fazla terminalden izin verilebilinmesi
- Personelin giriş ve çıkış raporununalınabilinmesi
- İstenilen zamanda Veritabanının yedekleme yapılabilinmesi
- Kullanıcının sisteme giriş ve çıkış saatlerinin Log yapılabilinmesi
- Kullanıcınınfonksiyonları kullanabilmesi için rol verilmesi
- Yeni personelin kaydedilmesi ve güncellenebilmesi (sınırsız)
- Rapor alınabilen formatlar: PDF, HTML, MHT, RTF, XLS, XLSX, CSV, Text
- Image şekilde rapor alınabilen formatlar: BMP, EMF, WMF, GIF, JPEG, PNG

Özellikleri

- Biyometrik veriyi Veritabanına sayısal veri olarak kaydedilebilmesi
- Geçiş noktalarında kullanıcı yüzünüokuttuğu zaman anlık gösterilmesi
- İstenilen zamanda ve istenilen yerde veri yedekleme imkanı
- İnsan Kaynakları Sistemi ile entegrasyonu
- Kurum veya şirketteki turnikelere ve kameralara entegre edilebilmesi
- Kayıt kapasitesi gibi bir kısıtlama bulunmamaktadır
- Kolayca sistemi geliştirebilme ve yönetebilme imkanı
- Kurumun isteğinegöre özel modül ve raporların geliştirilebilmesi
- Mevcut sistem (Active Directory) ile entegrasyon edilebilinmesi
- Mevcut sistem (İnsan Kaynakları Bilgi Sistem) ile entegrasyon edilebilinmesi
- Giriş-Çıkış raporlarını oluşturma ve çıktıları almak için esnek özelliklere sahiptir
- Yazılım kurum ihtiyaçlarına uygun olarak %100 tarafımca geliştirilmiştir

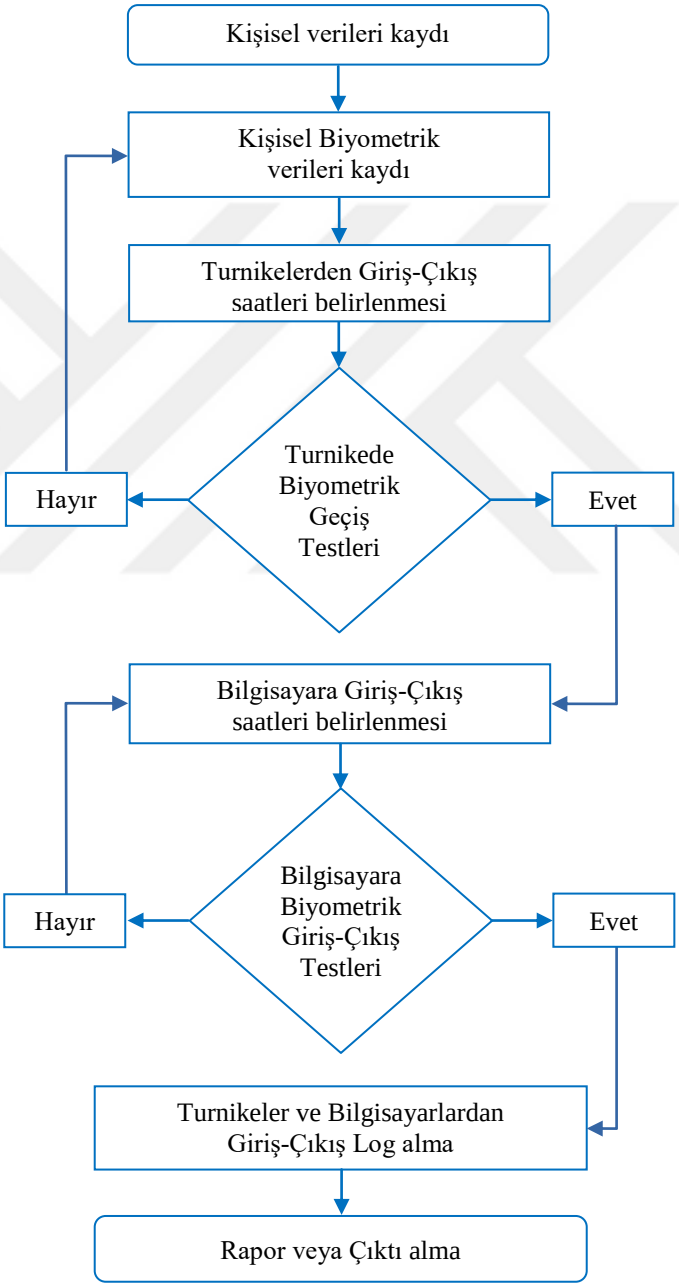
4.5 Avantaj ve Dezavantaj

Avantajlar

- Piyasaya yeni bir uygulama çıkarabilme imkanı
- İngilizce, Tacikçe, Türkçe ve Rusça kullanma imkanı mevcuttur
- Başka var olan sistemler ile entegrasyon edilebilme imkanına sahiptir
- Kurum veya müşteri istediği şekilde rapor alabilme imkanına sahiptir
- Var olan biyometrik uygulamalara göre fiyatı düşüktür
- Biyometrik sistemler pazarına farklılık ve genişlik kazandırması
- Var olan fonksiyonların yanına diğer fonksiyonları eklenilebilmesi mümkündür
- Kurumlar için yeni bir biyometrik teknolojiye sahip olabilme ve kullanılabilme imkanı
- Yazılım kodları %100 tarafımca yazılmış olup başka var olan sistemlerle entegrasyon edilebilme imkanına sahiptir

Dezavantajlar

- Uygulamayı tek başıma yazdığım için oldukça fazla zamanımı aldı
- Yeterli zamanım olmadığından yazmış olduğum kodların güvenlik testlerini yapamadım
- Uygulamayı tek başıma yazdığım için piyasadaki uygulamalarla rekabet edemeyebilir



Şekil 4.1 BİPEKS'in çalışma tarzı

5. SONUÇ VE DEĞERLENDİRME

Biyometrik teknolojilerin gelişmesiyle birlikte kişinin şifre unutma, giriş-çıkış raktı kaybolma veya şifre ve anahtar kaybedilebilecek gibi avantajları ile gelecekte daha çok yer edinecek gibi görülmektedir. Sonuç olarak bu tez çalışmasında Yüz tanıması bir sistem meydana getirme hedeflenmiştir.

Gerçek zamanlı yüz tanıma sisteminde kamera ile yakalanan görüntülerden yüz bölgesinin bulunması, bulunan bu bölgelerin tanıma işleminin gerçekleştirilmesi sağlanmıştır. Böylece önerilen yöntem ortaya çıkmıştır. Yüz tanıma sistemlerinde poz ve aydınlık gibi degişimler yüz tanıma oranını olumsuz yönde etkilemektedir. Bu tip sıkıntılar çoğu yüz tanıma sistemlerinde mevcuttur. Bu tip sıkıntıların sayısını azaltmak için geniş kapsamlı sistemlerde filtreler kullanılarak ışığın ayarlanması gibi önlemler ile bu sorunların etkileri azaltılmaktadır.

Yapılan deneylerde aynı kişiden alınan birden fazla resim olması durumunda performansın arttığı ve veritabanındaki farklı kişi sayısı azaltıldığı takdirde de performansın arttığı gözlemlenmiştir. Tanıma işlemi için geçen süre, veritabanında bulunan görüntü boyutlarına ve toplam görüntü sayısına bağlı olarak değişmektedir, çünkü, görüntülerin boyutları büyüdükçe veya toplam görüntü sayısı arttıkça, tanıma hızını doğrudan etkilemektedir.

“Bio Access Terminal” uygulamanın geliştirilmesinde hazır EmguCV ve OpenCV kütüphaneleri kullanılmıştım, aynı zamanda çalışmada, tanıma başarım oranını artırmaya yönelik kodlama teknikleri uygulanmıştım ve kütüphane kullanımı beraberinde bazı kısıtlamaları da getirmiştim.

Web camera ve yüz arasındaki mesafe	Sisteme kayıtlı kişi sayısı	Kişi başı resim sayısı	Yanlış kabul etme oranı	Minimum ve maksimum yüz tanıma oranı
10-40 cm.	50 kişi.	5-15 resim.	5%	64% - 98%

Buna rağmen ortalama yüz tanıma oranı %86,64 'e ulaşan başarımlar elde edilmiştir. Literatürdeki yöntemlere göre Tez çalışmasının başarılı olduğu görülmektedir.

“Bio Access Terminal” uygulamanın sonunda, tanıma başarı oranını ve performansını artırmaya yönelik şunları yapılabiliriz:

- Yüz tanıma algoritmalarını anlayan iyi bir yazılımcı tarafından fonksiyonlar ve kütüphaneler uzerinde çalışma ve sistem testleri yapılması
- Yüz tanıma sisteminin gerçek zamanlı çalışma hızını arttırmak için kod üzerinde ve veritabanı bağlantıları üzerinde çalışmalrı yapmak gerekmektedir
- Gerçek zamanlı yüz tanıma performansını artırmak için ışıklandırma ve poz durumları üzerinde optimizasyonları yapılması gerekmektedir

Bu çalışma esnasında biyometrik sistemler üzerine araştırmaları yaparken ilginç fikirler ortaya çıkmıştır ki gelecekte sunulacaktır, umarım ki bu hedeflere kısa zamanda ulaşırım.

KAYNAKLAR

Anonim. 2010. Web Sitesi: http://elektroteknoloji.com/Elektrik_Elektronik/Teknik_Yazilar/Biyometrik_Sistemler_Fiziksel_Ozelliklerden_Yararlanarak_Kimlik_Tespit_Etme_bilgisayar_destekli.html, Erişim Tarihi: 11/10/2016

Anonim. 2014. Web Sitesi: http://www.ispozelguvenlik.com.tr/teknoloji/biyometrik-guvenlik-teknolojileri/, Erişim Tarihi: 25/10/2016.

Anonim. 2015. Web Site: http://www.personel-takip.com/yuz-tanima-sistemleri.html, Erişim Tarihi: 10/11/2015.

Anonim. 2015. Web Sitesi: http://www.vahitgumus.com/it/biyometrik-tanima/ Erişim Tarihi: 27/10/2016.

Anonim. 2016. Web Sitesi: http://www.ergosis.com.tr/yuz-tanima-sistemi.html, Erişim Tarihi: 12/10/2016.

Aygün S., Akçay M., ve Güneş E. 2015. "Bulut Sistemler için Önerilen Biyometri Tabanlı Güvenlik Sistemine Genel Bakış", International Symposium On Digıtal Forensics And Security 2015, Ankara/Turkey.

Elumalai, K. and Kannan, M. 2011. "Multimodal Authentication For High End Security", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 2 Feb 2011.

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

Gad, R., El-Sayed A., El-Fishawy N. and Zorkany M. 2015. "Multi-Biometric Systems: A State of the Art Surveyand Research Directions", (IJACSA) International Journal of Advanced Computer Science and Applications Vol. 6, No. 6, 2015.

Gökmen, M., Kahraman, F., Kurt, B. ve Çapar, A. 2007. "Çok Amaçlı Gürbüz Yüz Tanıma", İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Bilgisayar Mühendisliği Bölümü, 1/9/2005 – 31/8/2007.

Görgünoğlu, S. ve Çavuşoğlu, A. 2009. "Parmakizi Tanıma Sistemlerinde Kullanılan Özellik Çıkartma Algoritmalarının Performans Analizi", 5. Uluslararası İleri Teknolojiler Sempozyumu (IATS'09), 13-15 Mayıs 2009, Karabük, Türkiye.

Miura, N. and Nagasaka, A. 2004. Takafumi Miyatake “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification”, Machine Vision and Applications (2004) 15: 194–203.

Nabiyev, V. 2009. “Kulak Biyometrisine Göre Kimlik Tespiti”, 2. Mühendislik ve Teknoloji Sempozyumu, 30 Nisan - 1 Mayıs 2009, Çankaya Üniversitesi/Ankara.

Srivastava, H. 2013. “A Comparison BasedStudy on Biometricsfor Human Recognition”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 15, Issue 1 (Sep. - Oct. 2013), PP 22-29.

Şamlı, R. ve Yüksel, M. 2009. “Biyometrik Güvenlik Sistemleri”, Akademik Bilişim09 - XI. Akademik Bilişim Konferansı Bildirileri, 11-13 Şubat 2009, Harran Üniversitesi, Şanlıurfa.

Varol, A. ve Cebe, B. 2011. “Yüz TanimaAlgoritmalari”, 5th International Computer&Instructional Technologies Symposium, 22-24 September 2011, Fırat University, Elazığ/Turkey.

Yalçın, N. ve Gürbüz, F. 2015. “Biyometrik Güvenlik Sistemlerinin İncelenmesi” - Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3 (2015) 398-413.

EK 1 Biyometrik Personel Kontrol Sistemi

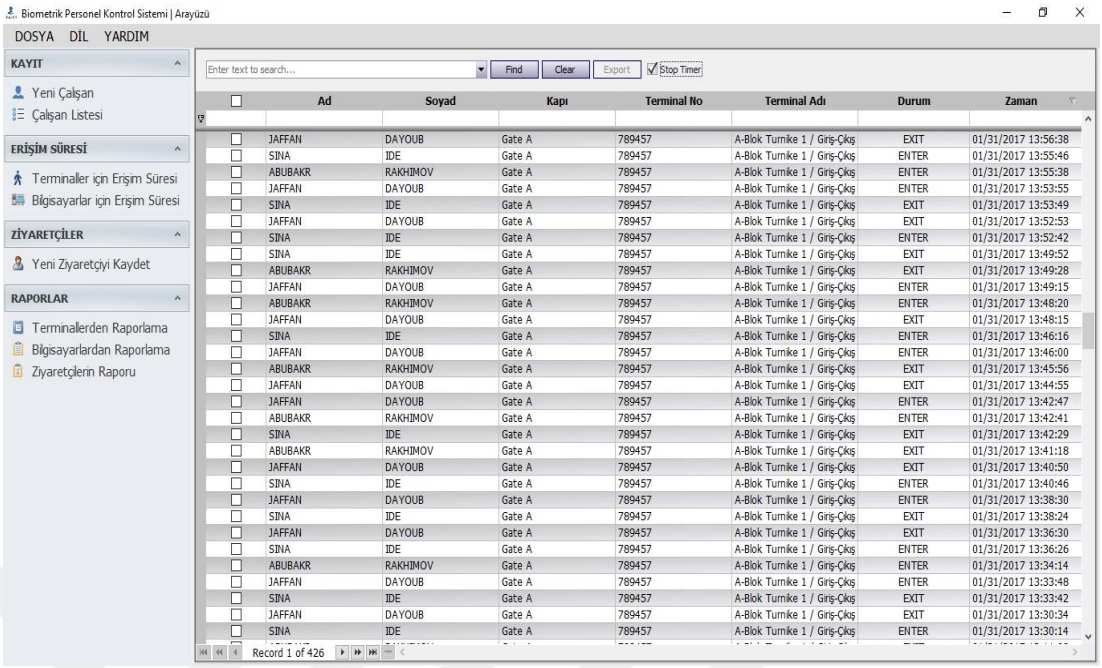
Şekil 1 Sisteme Giriş

Şekil 2 Şifre Yenileme

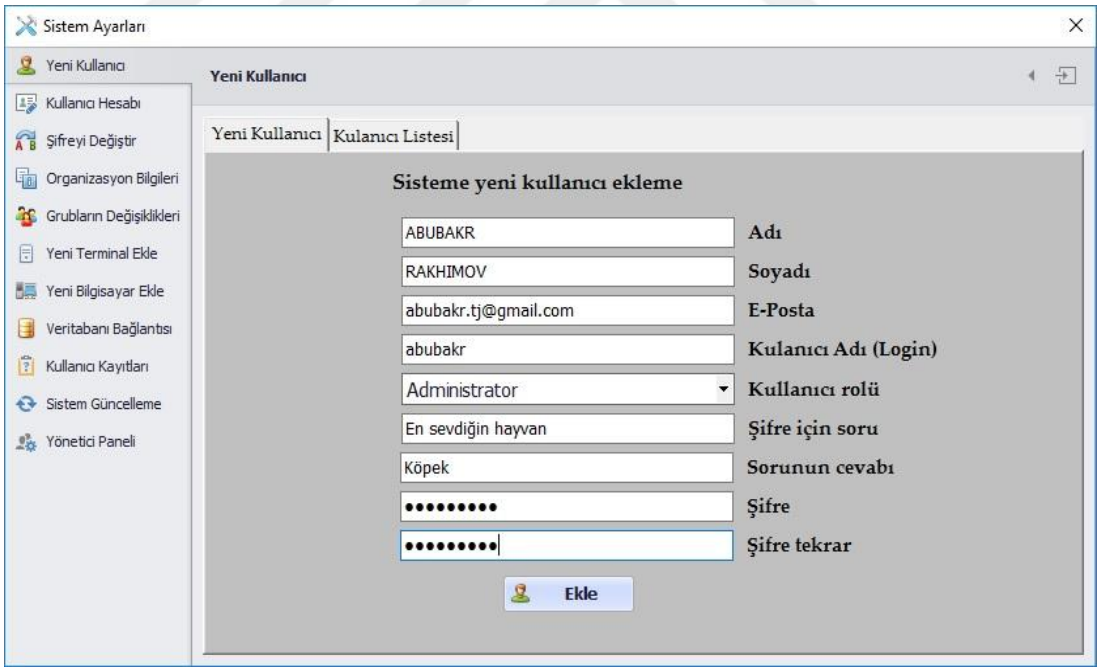
Şekil 3 Yeni Personelin Bilgi Girişi

Selection	Fotoğraf	Adı	Soyadı	Doğum Tarihi	Cinsiyet	Pasaport No	Cep Telefon	E-Posta	Adres	Kayıt Tarihi
☑		TEST	TEST	25.03.1992	Bay	MO885236941	(505) 666-99-97	test@yahoo.com	Ankara	25.02.2017 13:41
☑		ABDULLAH	KHALIL	20.02.1995	Bay	7879878	(778) 878-78-97	abdullah@ya.ru	Ankara	20.02.2017 21:36
☑		TEST	USER	18.02.2017	Bay	12345678	(111) 111-11-11	user@hotmail.com	Ankara	18.02.2017 14:29

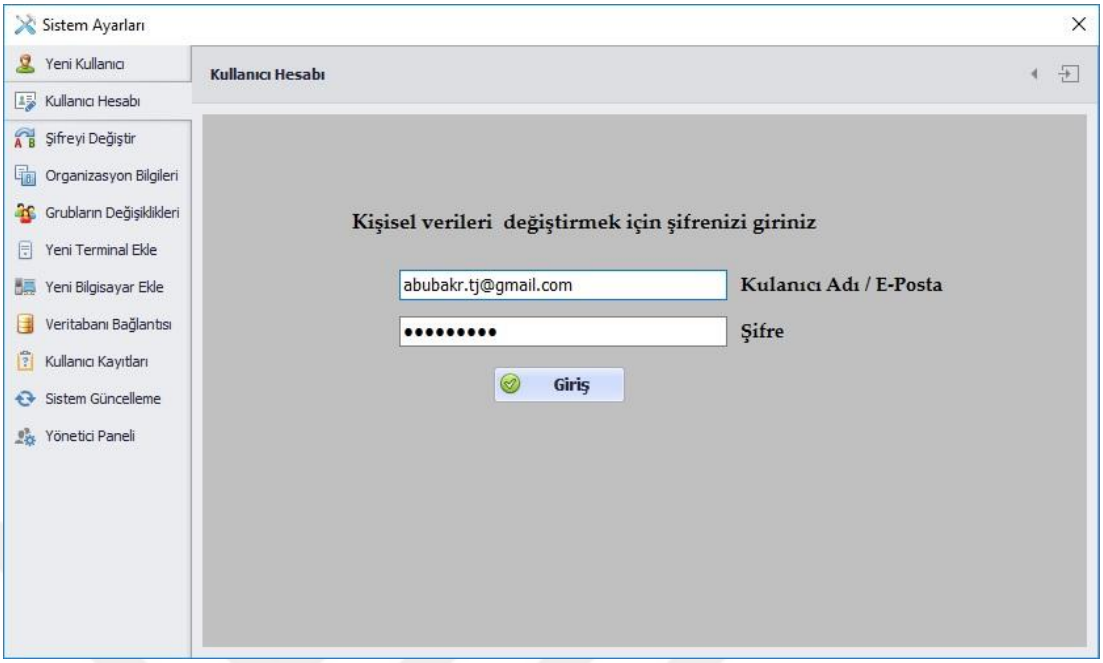
Şekil 4 Kayıtlı Kişilerin Rapor Listesi



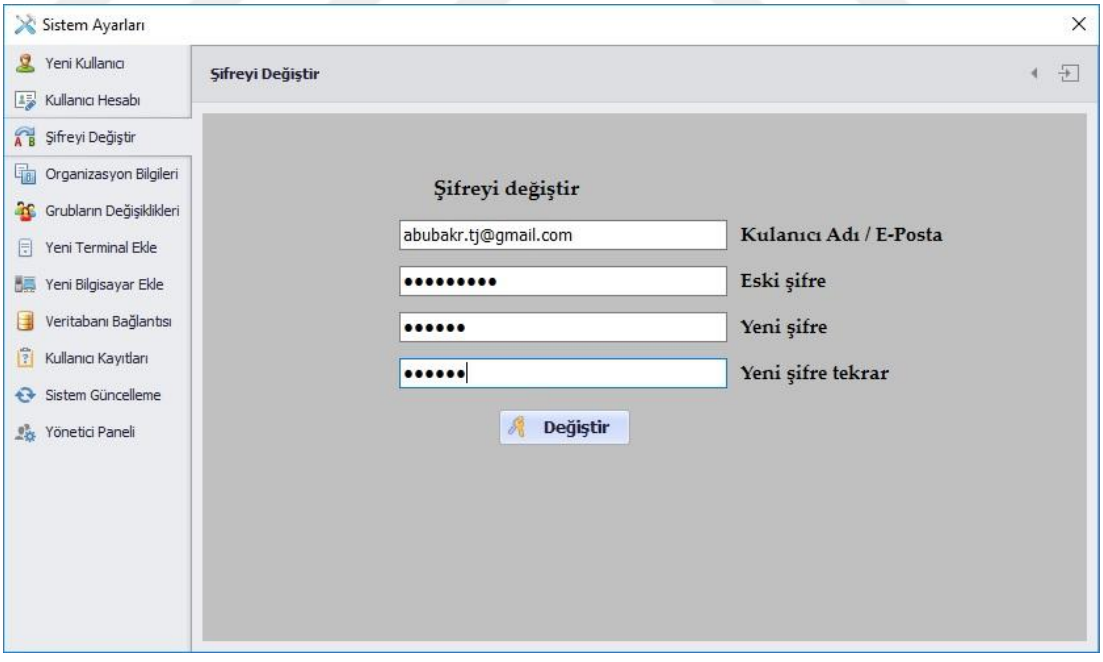
Şekil 5 Tuernikelerden Giriş-Çıkış Raporu



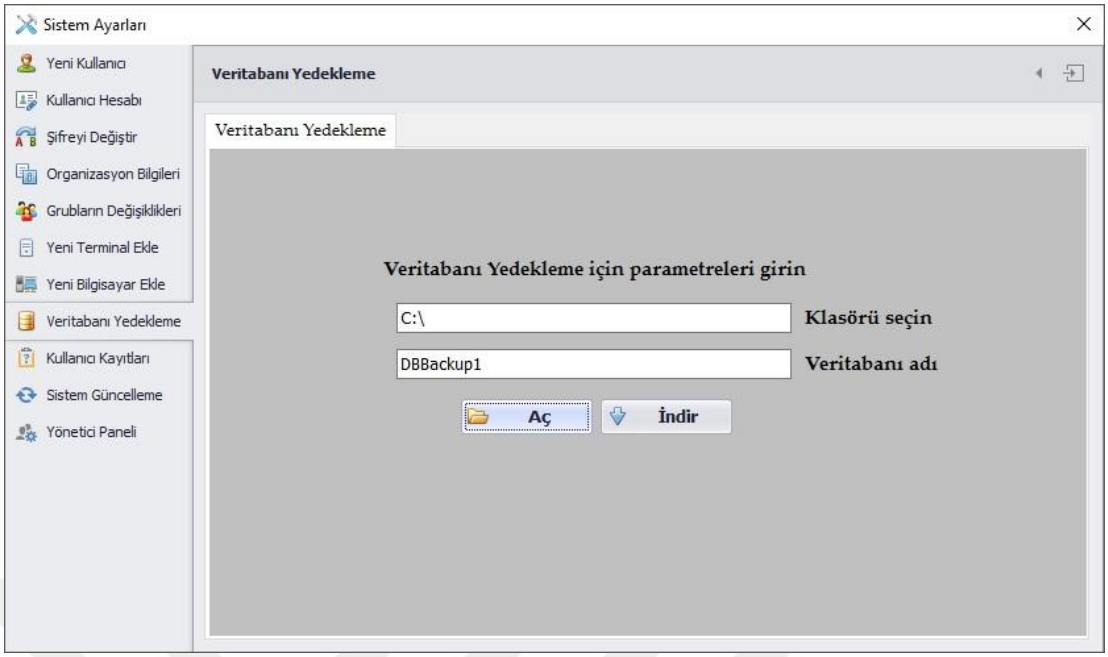
Şekil 6 Sistem Kullanıcı Ekleme Formu



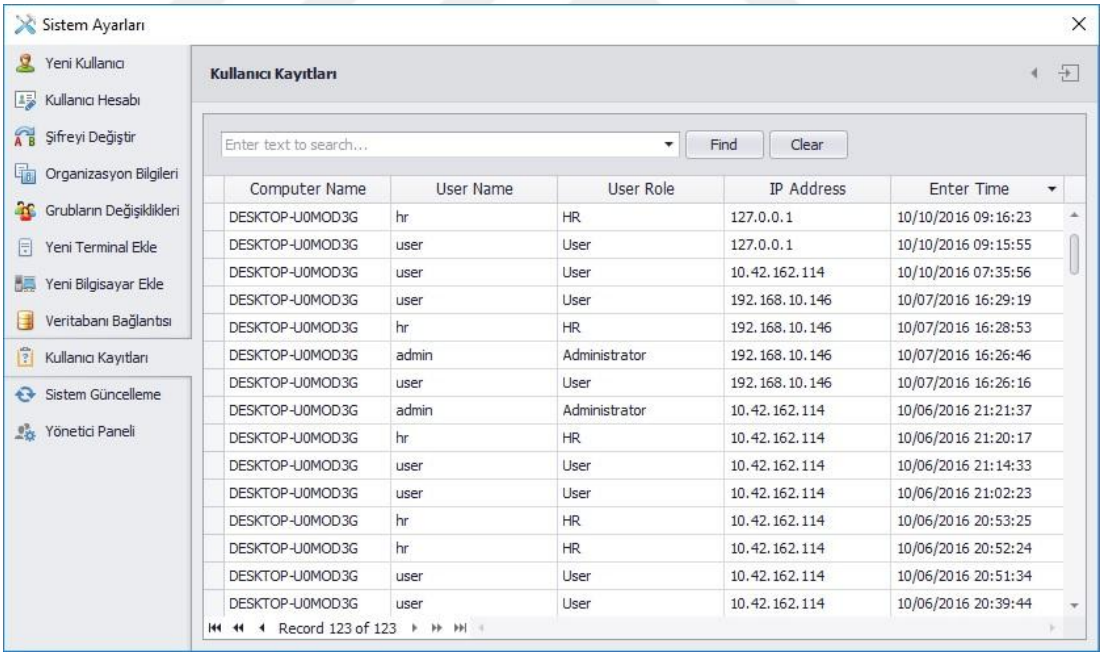
Şekil 7 Sistem Kullanıcı Hesaba Giriş



Şekil 8 Sifre Deiğiştirme Formu



Şekil 9 Veritabanı Yedekleme Formu



Şekil 10 Sistem Kullanıcıların Sisteme Giriş Log Listesi

ÖZGEÇMİŞ

Adı Soyadı : Abubakr RAKHIMOV

Doğum Yeri : Tacikistan

Doğum Tarihi : 25/02/1986

Medeni Hali : Bekar

Yabancı Dili : Tacikçe, Rusça, Türkçe, İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise **:** Tacikistan Maliye ve Ekonomi Enstitüsü Lisesi (09/2001 – 06/2003)

Lisans **:** Tacikistan Milli Üniversitesi, Fizik Fakültesi,
Bilgisayar Mühendisliği Bölümü (09/2003 – 06/2008)

Yüksek Lisans: Ankara Üniversitesi, Fen Bilimleri Enstitüsü,
Bilgisayar Mühendisliği Anabilim Dalı (Eylül 2013 – Mayıs 2017)

Çalıştığı Kurum/Kurumlar ve Yıl

07/2015-10/2016 "MIA Teknoloji", AR-GE ve Yazılım Birimi (Stajer)

01/2009-10/2012 "Kazkommertsbank Tacikistan", Bilgi Teknolojileri Yönetimi

09/2008-01/2009 "Agroinvestbank", Bilgi Teknolojileri Departmanı,
Telekomünikasyon Birimi

05/2005-09/2008 "Milli Eğitim Bakanlığı", Bilgi Teknolojileri Birimi

01/2005-08/2007 Kamu Vakfı "Sivil Girişim İnternet Politikası",
Bilgi Teknolojileri Birimi

02/2004-02/2008 "Tacikistan Milli Üniversitesi", Bilgi Teknolojileri Birimi