YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AKILLI KART TEKNOLOJİSİYLE GELİŞTİRİLMİŞ ELEKTRONİK PASAPORT VE VİZE SİSTEMİ

Bilgisayar Mühendisi Mehmet Semih UZUN

FBE Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Yrd. Doç. Dr. Banu DİRİ (YTÜ)

İSTANBUL, 2006

İÇİNDEKİLER

SİMGE LİSTESİ

n	Şifrelemede kullanılan çok büyük iki asal sayının çarpımı sonunda elde edilen sayı
e	Şifreleme için belirlenen çok büyük asal sayı
d	Şifre çözmek için belirlenen çok büyük asal sayı
P	Kullanıcıdan daha önceden elde edilmiş özellik şablonu
P'	Kullanıcıdan o an elde edilen özellik şablonu
H_0	Önceki ve o anki şablonların eşit olma durumu (orijinal kullanıcı)
H_1	Önceki ve o anki şablonların eşit olmaması durumu (sahte kullanıcı)

KISALTMA LİSTESİ

PIN – Kişisel kimlik numarası (Personal Idenfication Number)

ATM – Otomatik para çekme makinesi (Automated Teller Machine)

LOC – Koddaki satır sayısı (Lines Of Code)

KLOC – Koddaki satır sayısı / 1000 (Kilo Lines Of Code)

BTS – Biyometrik Tanıma Sistemleri

FAR – Yanlış Kabul Oranı (False Accept Rate)

FRR – Yanlış Reddetme Oranı (False Reject Rate)

CCD – Işığa duyarlı görüntü algılayıcılı kamera (Coupled-Charged Device)

XOR – Ayrıcalı veya (exclusive OR)

HD – Hamming Mesafesi (Hamming Distance)

NC – normalleştirilmiş ilişki (Normalized Correlation)

LVQ – lineer vektör niceleme (linear vector quantisation)

FTIR – engellenmiş toplam iç yansıma

SVM – Destek vektör makineleri (Support Vector Machines)

HMM – Gizli Markov Modeli (Hidden Markov Modal)

PC/SC – Bilgisayar – Akıllı Kart İletişim Protokolü

ATR – Akıllı kartın güç kesiminden sonra verdiği cevap (Answer to Reset)

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Günümüzün küresel sahteciliğini önleyebilmek için mevcut kağıt tabanlı pasaport ve vizelerin artık terk edilmesi gerekmektedir. Bunun yerine, daha karmaşık, mümkün olduğu kadar daha uzun süre dayanabilecek ve kırılması zor olan bir teknoloji kullanılmalıdır.

Akıllı kartlar, sağladıkları güvenlik prensiplerinden ve dışarıdan gelebilecek olan tehditlere karşı güvenli olmalarından dolayı elektronik pasaport ve vize uygulamalarında gelecekte kullanılması muhtemel en yaygın teknolojilerden biri olarak karşımıza çıkmaktadır.

Güvenli bir elektronik pasaport uygulaması için sadece bir teknolojiden yararlanmak, sistemin geleceğe dönük kullanışlılığı ve tam güvenlik seviyesinin sağlanması için uygun olmayabilir. Bu nedenle güvenlik artırımı konusunda sisteme yardımcı olacak biyometrik tanıma teknolojisi de bu tür uygulamaların içerisinde yer almalıdır.

Bu tezde gerçekleştirilen çalışmanın amacı akıllı kart ve biyometrik tanıma teknolojileri kullanılarak güvenli ve uygulanabilir bir elektronik pasaport ve vize uygulaması geliştirmektir.

ÖZET

Teknolojideki hızlı gelişim süreci ve onun bizlere sağladığı kullanım kolaylığı, günlük hayatta bizler için önemli olan yerlere hızla girmesini sağlamıştır. Önceleri kredi kartı işlemlerimiz için kullandığımız elle çalıştırılan POS (point of sale) makinelerinin yerini tam otomatik, aynı anda birçok kontrolü içinde barındıran cihazlar almış; tıpkı bunun gibi, yaygınlaşmaya başladığında sadece arama yapmak ve mesajlaşmak için kullanılan cep telefonları bugün fotoğraf çekmekten radyo dinlemeye kadar birçok özelliği bünyesinde barındıran teknolojik aletler haline gelmişlerdir.

Teknolojik gelişmelere paralel olarak önceleri yüzbinlerce dolara satılan yüksek kapasiteli bilgisayarlar yüz dolarlar seviyesinde evlere girmeyi başarmış, sadece bilgisayarlarla kalmayan bu yayılma süreci yüksek çözünürlüklü tarayıcılara ve kaliteli yazıcılara da yansımıştır. Böyle olunca da, kâğıt üzerinde yapılmakta olan işlemler kopyalanabilir ya da üzerinde tahrifat yapılabilir hale gelmiş, tüm bunlar da bu tür işlemlerin güvenirliği sorgulanır hale getirmiştir.

Ülkeler (ki buna ülkemiz de dahildir) kendi iç işlerinde birçok kademede bilgisayarlı sisteme geçmelerine rağmen, henüz farklı teşkilatlar arasında tam anlamıyla bir bütünleşme sağlanmadığından ve daha da önemlisi vatandaşlara bu sisteme geçiş tamamen yansıtılamadığından, kurumlar ve insanlar arasında kullanılan evraklar üzerinde değişiklik yapılabilmekte, bu durum da ülkelerin karşılaştığı önemli sorunlardan biri olmaktadır.

Ülkeleri en çok zorlayan problemlerin başında o ülkeye yapılan girişlerin ve çıkışların kontrol edilmesinin geldiği de açıktır. Pasaport ve vize, ülkelere giriş çıkışların kontrol edilebilmesi amacıyla kullanılan mekanizmalardır. Bu evraklar üzerindeki sahtecilik de öteden beri devletlerin ciddi biçimde engellemeye çalıştığı işlemlerdir. Ancak günümüz gelişen teknolojisinde de bunu önlemenin yolu, sahteciliğe dayanıklı bir mekanizma kullanmak ve kâğıt evrakları tamamen terk etmekten geçmektedir. Bu tez, böyle bir sistemi altyapısıyla birlikte incelemek, örnek bir sistem ortaya çıkarıp, avantajlarını ve geliştirilme yollarını sunmak amacıyla yazılmıştır.

Tez çalışmasında kullanılacak teknolojiler hakkında hem teorik hem de uygulamaya yönelik kapsamlı bir araştırma yapılmış, kullanılacak teknolojiler sonucunda ortaya çıkması muhtemel olan sorunlardan bahsedilerek, bu sorunlar üzerine yorumlar yapılmıştır.

Anahtar Kelimeler: Pasaport, vize, elektronik pasaport, akıllı kart, güvenlik

ABSTRACT

Fast improvement process and the ease to use of the technology has increased the usage of it in common and important places for us in daliy life. In the past, we were using the manual pos terminals for our credit card process but after then they have been replaced with the fully automated ones. Likewise in the time of the becoming widespread the cellphones were only providing us to talk to or to messaging with other people but nowadays they have megapixel cameras as well as built-in fm radios.

Besides the technological improvements, the cost of high capacity computers which was about hundred thousand US dollars in the past has decreased dramatically to few hundred US dollars. These changes did not occur only in PC prices, they also can be seen in high resolution scanners as well as high quality printers. All of these changes caused the processes those were being made on the paper can be copied or changed easily and this made us to question the security of these kinds of document processes in deep.

From the past to now, the most popular places, where the paper based processes have being executed, are belonging to government. Countries (which Turkey is also one of them) developed their computer systems and changed the existing paper based systems with these new ones but among the different departments there is still lack of digital communication. That short of interaction causes paper traffic inside the departments and also between government and people. This is one of the most difficult problems that governments were being faced.

To control the migration and security in a country, government has to take several actions against them. Passports and visas are the mechanisms for controlling the borders and also their citizens abroad. The fraud on these paper based documents has been done since the past and several things has being tried to avoid these trials. However by the help of the technological improvements, it become easier to take control of these illegal actions. In order to avoid forgeries or global fraud, document based passports/visas need to be replaced. Instead, a sophisticated token with high security features, not easy to forge, should be used.

The aim of this thesis is to provide a securely strong and easy to apply electronic passport and visa solution by using smartcard and biometrics technology.

Keywords: Passport, visa, electronic passport, smartcard, security

1. Giriş

Her ülkenin kendi giriş ve çıkışlarını kontrol etmek için geliştirdiği birtakım yasaları ve düzenlemeleri mevcuttur. Suçluların ya da teroristlerin ülkeye giriş-çıkışını önlemek veya göçleri kontrol etmek ülkeler için son derece büyük önem taşımaktadır.

Ülkeler bu giriş-çıkış kontrollerini pasaport ya da vize denilen kontrol mekanizmalarıyla gerçekleştirmektedirler. Bu nedenle pasaport ve vize ülkelerarası seyahat eden insanları belirlemek için önemli bir kontrol mekanizması olmaktadır. Bunun yanında büyük ülkelerde, pasaport ve vize sahteciliği, yasadışı yollardan ülkeye girme ve ülkeden ayrılma gibi birtakım eylemler için kullanılmaktadır.

Teknoloji ilerledikçe, kağıt üzerindeki tahrifatlar da kolaylaşmakta; tarayıcı, yazıcı ve renkli kopyalayıcı aygıtların gelişmesiyle, belgelerin sahteleri kısa sürede ve gerçeğinden ayırt edilmesi çok zor (kimi zaman imkansız) şekilde yapılmaktadır. Sonuç olarak hükümetler, bu gibi durumların önüne geçmek için değişik tedbirler almaya çalışmaktadırlar, bunun için bazen birçok güvenlik mekanizmasını birlikte kullanmak gerekmektedir.

Bu çalışmanın konusu olan elektronik pasaport , vize sistemi ve uygulaması uzun zamandır birçok ülke ve kurumun üzerinde çalıştığı bir alandır. Sistemin amacı güvenli ve ileriye dönük bir çözüm üretmek olduğundan çalışma yapan kurumlar detaylı ayrıntı vermekten kaçınmaktadırlar. Örneğin, Finlandiya Ekonomi Bakanlığı 1996 yılından itibaren vatandaşlarının akıllı kart sistemini kullanan kimlik kartları için çalışma yapmaya başlamış ve yine Amerika Birleşik Devletleri 2001 yılından itibaren vatandaşlarının pasaportlarına akıllı kart teknolojisini entegre etmek üzere çeşitli yatırımlar gerçekleştirmiştir.

Bu tez çalışmasında kullanılacak teknolojiler hakkında hem teorik hem de uygulamaya yönelik kapsamlı bir araştırma yapılmış, kullanılacak teknolojiler sonucu ortaya çıkması muhtemel olan sorunlardan bahsedilerek üzerinde yorumlar yapılmıştır.

Tezin ikinci bölümünde elektronik pasaport ve vize uygulamasına temel olan teknolojiler anlatılmıştır. Güvenli kimlik sistemleri açıklanmış, bu sistemin parçaları olan akıllı kart teknolojisi ve biyometrik tanıma sistemleri sırasıyla ayrıntılı olarak incelenmiş, akıllı kart ve biyometrik tanıma teknolojilerinin birlikte kullanımının sağlayacağı yararlara değinilmiştir. Üçüncü bölümde uygulama için oluşturulacak olan sistemin yapısı hakkında temel bilgiler verilmiş, dördüncü bölümde ise sistem hakkında ayrıntılı tasarım ortaya konmuştur. Bu bölümde, akıllı kart okuyucuları, biyometrik okuyucuları, kapı ve alarm modülleri, güvenlik

memurları gibi sistem elemanları teker teker ele alınmıştır. Uygulama Beşinci bölümde sistemin yararları açıklanmış, altıncı bölümde de ileride yapılabilinecek olan çalışmalar eklemeler belirtilmiştir. Yedinci bölümde bahsedilen güvenlik ve gizlilik konuları sistemin bugün kullanılan sistemlerle güvenlik açısından karşılaştırılmasını içermekte, kullanıcıların ya da hükümetlerin olası sorularını yanıtlamaya çalışmaktadır. Sekizinci ve son bölümde ise tezin ulaştığı sonuç olarak sistemin bütün olarak sağladığı yararlar ve öngörülen uygulama sorunları vurgulanmaktadır.

2. Elektronik Pasaport / Vize

Geleneksel pasaport ve vizelerin, gelişen teknolojiyle birlikte, sahteciliğe daha dayanıklı hale getirilmesi fikri, birçok bilim adamı ve yetkililerce dile getirilmiş, sağlayacağı faydalar da göz önünde bulundurulduğunda oldukça mantıklı bulunmuştur. Eskisinin yerini alacak sistem şüphesiz üzerinde tahrif ve kopyalama işlemlerinin gerçekleştirilmesi zor olduğu ve mümkün olan en uzun süre bu özelliğini koruması beklenen sistemdir. Küresel sahteciliği önlemek için, kağıt tabanlı pasaport ve vizelerin terk edilmesi gerekmektedir. Bunun yerine daha karmaşık, sahteciliğe mümkün olabilecek en uzun zaman dayanabilecek ve kırılması zor olan bir teknoloji kullanılmalıdır. Böyle bir sistem kullanmanın ön koşulu da güvenli kimlik sistemlerinin incelenmesidir.

2.1 Güvenli Kimlik (Secure ID) Sistemleri

Güvenli bir kimlik sistemi oluşturmanın birkaç anahtar özelliği bulunmaktadır. Öncelikle ve en başta ele alınması gereken kişisel kimliğin şu karakteristiklere sahip olması gerçeğidir:

Fiziksel güvenlik – kimlik kartlarının geçerliliğini kontrol eden bireyler genelde bu kartları denetleme işlemine çok az dikkat ederler. Bu nedenle bu kartların yanlış kullanımını engellemek için öncelikle görsel birtakım koruma özellikleri kartlarda bulundurulmalıdır.

Veri güvenliği – Saklanan verinin gizlilik, doğruluk ve bütünlük özellikleri güvenli bir kimlik denetim sisteminin vazgeçilmez unsurlarıdır. Önemli veriler, istenmeyen bilgi paylaşımlarının önüne geçebilmek için hem karta yazılmaları sırasında, hem de kartın üzerinde bulundukları anda güvenliklerinin korunabilmesi amacıyla şifrelenmelidirler.

Kimlik doğrulama – Kimlik kartı, kullanıcının doğruluğunu teyit edecek biyometrik ya da diğer verilere sahip olmalıdır. Birçok durumda kimlik kartı, içindeki verileri okuyup işleme yeteneğine sahip olan okuyucusuyla birlikte bir doğrulama gerçekleştirebilir.

Gizlilik – En yüksek düzeydeki güvenlik ve gizlilik için, güvenli kimlik sistemi iletişim içinde olduğu sistemin diğer bileşenlerinin de doğruluğunu ve kimliğini kontrol etmek zorundadır.

Güvenli bir göstergenin yanı sıra, eksiksiz sistem güvenlik politikaları ve prosedürleri de önceden belirlenmiş olmalıdır. Güvenlik politikaları ve prosedürleri sistemi kullanacak kurum ya da kuruluşlar tarafından önceden, ki burada pasaport ve vizeyi kullanacak olan devlettir, belirlenen yönetimsel dokümanlardır. Güçlü, anlaşılır ve iyi tasarlanmış politikalar ve prosedürler, sistemin içindeki tüm bileşenlerin görevlerini de açıkça ortaya koyar.

Sistem ne kadar güçlü tasarlanmış olursa olsun, bütün uzmanların ortak görüşü, kimlik doğrulama sistemlerinde en zayıf halkanın "insan" olduğudur. Sistem yöneticileri, güvenlik memurları ve sistemin işleyişini uzaktan izleyen personel şu konularda eğitilmelidirler:

Dolandırıcılık, sahtekarlık ve daha birçok maddenin yazılı olduğu itimatnamenin oluşturulması, sınanması ve kullanımı.

İlişkilendirilmiş önemli bilginin korunmasını sağlayacak olan sistemin güvenlik politikaları ve prosedürleri.

Aynı zamanda, kullanıcıların da kimlik kartının ve okuyucunun arayüzünün kullanımı hakkında açık talimatlarla bilgilendirilmeleri gerekir.

Gerçek ya da düşünülen sistemi etkileyecek faktörlerden birkaçı şu şekilde sıralanabilir:

Kimlik doğrulama sistemi tarafından bilinen ve kullanılacak olan bilginin türü ve miktarı;

Özel verinin nerede saklandığını içeren güvenli kimlik doğrulama sisteminin mimarisi ve teknolojisi, kullanıcılarının kimliklerinin nasıl doğrulandığı ve kart sahibi bireylerin kişisel bilgilere nasıl eriştikleri;

Kimlik doğrulama sisteminin kişisel bilgilere erişimi önlemek için kullanacağı politikalar ve eylemler.

2.2 Akıllı Kart Teknolojisi

Akıllı Kart, içerisinde gömülü bir mikroçip bulunan, kredi kartı büyüklüğünde bir plastik karttır. Bu mikroçip, bugüne kadar manyetik kartların sağladığı hafıza büyüklüğünden daha yüksek bir alan sunmakla kalmaz, aynı zamanda kendi üzerinde güvenlik özelliklerini de

barındırır. Böylelikle kartlar ve terminaller birbirilerinin doğruluğunu aktif şekilde kanıtlarlar.

Akıllı kartların içindeki merkezi işlem ünitesi orjinal IBM PC'nin işlemci gücü olan 8 bitlik bir mikrodenetleyiciden ibarettir. Akıllı kartların bilgisayarlarla iletişim kurabilmeleri için kart okuyucu denen bir aygıta gereksinim vardır.

Akıllı kartların geliştirilme süreci 20 seneden daha fazladır. Bu zaman sonunda kullanımı daha yaygınlaşmış, günümüzde hemen herkesin cüzdanına kadar girmiştir. Bu yaygınlaşmanın sonunda mimari de 8 bitlikten, 16 ve 32 bite doğru kaymıştır. Ancak bu tezde kullanılacak olan akıllı kart 8 bit mimaride olduğu için bundan sonraki açıklama ve bilgiler de bu mimariye göre yapılacaktır.

Akıllı kart yazılımı genellikle karta entegre biçimde bulunan ve kendi dosya sistemi, iletişim, kimlik doğrulama, şifreleme ve erişim kontrolü protokolleri olan bir işletim sistemidir. Akıllı kartlar veri güvenliği, kişisel gizlilik ve taşınabilirlik gerekliliğine haiz olan bilgisayar sistemlerinin kullanışlı elemanlarıdır.

Akıllı kartların programlanması iki önemli sistem gereksiniminin karşılanmasıyla özetlenebilir. Bunlar veri güvenliği ve veri tutarlılığıdır. Veri güvenliği, verinin değerinin ya da hesaplanma yeteneğinin sadece ona bu işlemleri yapmasına izin verilen bir sistem elemanı varlık (entity) tarafından erişilmesi, izin verilmeyen durumlarda erişimin engellenmesi demektir. Veri tutarlılığı ise, kartın üzerinde depolanan verinin, bütün durumlarda depolandığı şekilde kalmasıdır. Herhangi bir yazım sırasında (elektriğin kesilmesi durumunda bile) verinin doğru bir şekilde kartta bulunuyor olması tutarlılığın en önemli gereksinimidir.

Akıllı kart uygulamalarında kullanılan veri miktarı genellikle az, yapılan işlemler de buna paralel olarak oldukça basittir. Örneğin, geliştirilen bir elektronik cüzdan sisteminde, bir ürün alınmak istediğinde yapılacak şey akıllı kartın içindeki değeri okuyup ürünün ücretini bu değerden çıkarmak ve sonucu tekrar karta yazmaktır. Bununla birlikte gerçekleştirilen bu az işlemde satıcının da kullanıcının da tüm beklentileri eksiksiz karşılanmalıdır. Az önceki örnekte işlem sonunda satıcı sattığı ürün kadar kendisine para eklenmesini, kullanıcı da aynı şekilde kartından para çekilmesini bekler. Aynı zamanda bu işlem sonucunda kartının tekrar sorunsuz şekilde çalışmasını ve içindeki bilgilere başkaları tarafından erişilmemesini ister. Akıllı kartlarla oluşturulan sistemlerde bu konulara özen göstermek sistemin en önde gelen yapılacaklar listesinde yer almalıdır.

Akıllı Kart Yazılımı

Temel olarak iki türlü akıllı kart yazılımı mevcuttur. Bunlar:

Sunucu Yazılımı : Bu yazılım akıllı karta bağlı olan bilgisayarda çalışır. Okuyucu taraflı yazılım olarak da bilinir.

Kart Yazılımı : Akıllı kart üzerinde çalışan yazılımdır. İlk türdeki yazılımın aksine kart üzerinde çalışmasından ötürü, bu tür yazılımlara da kart taraflı yazılım denmektedir.

2.2.1 Sunucu Yazılımı

Birçok akıllı kart yazılımı sunucu yazılımıdır. Kişisel bilgisayarları ve iş istasyonlarını halen kullanımda olan akıllı kartlara ve bu kartları daha büyük sistemlere entegre etmek için kullanılırlar. Sunucu yazılımı, son kullanıcı uygulama yazılımı ve akıllı kartların ana platformla entegrasyonunu sağlayan sistem seviyesinde yazılımdan oluşur. Buna ek olarak akıllı karta yapısal erişim için kullanılan çeşitli yardımcı yazılımlar da sunucu yazılımı grubuna girmektedir.

Sunucu yazılımları genellikle C, C++, Java, Visual Basic gibi yeni nesil programlama dilleri kullanılarak yazılırlar ve üreticiler tarafından sunulan kütüphanelerle kart okuyucularıyla iletişim kurabilirler. Bunun yanında kart yazılımı ise güvenli yazılım dillerinden Java ya da makine düzeyindeki Assembly dilinde yazılır.

2.2.2 Kart Yazılımı

Kart yazılımı akıllı kartın üzerinde çalışan yazılımdır. Genellikle bir işletim sistemi ve uygulama programından oluşur. Birçok uygulama için akıllı kartların üzerinde bulunan yazılım, başka bir yazılıma ihtiyaç duyulmadan istenilenlerin yapılabilmesi için yeterlidir. Ancak uygulamaya özel bir yazılım yapımı gerektiğinde, çiplerin mimarisine bağlı ve buna uygun makine dilinde program yazılır ve akıllı karta yüklenir.

Akıllı kart yazılımlarını da uygulama yazılımı ve sistem yazılımı olarak kategorilere ayırmak faydalı olacaktır. Uygulama yazılımı akıllı kartın hesaplama gücünü ve veri depolama yeteneklerini tıpkı başka bir bilgisayar üzerinde çalışıyormuş gibi güvenlik ve tutarlılık ayrıntılarıyla ilgilenmeden kullanır. Diğer yandan sistem yazılımı ise veri tutarlılığı ve güvenliğin tamamen sağlanmasından sorumlu kısımdır ve bütün kontrolü elinde tutar.

Sunucu yazılımı, akıllı karttaki mevcut bir özelliğin farklı bir uygulaması için de kullanılabilir. Örneğin bir şifreleme anahtarı veya bir kişi hakkındaki sağlık kayıtları merkezi bir bilgisayarın diskinde ya da veritabanında tutulmak yerine akıllı kartın üzerinde saklanabilir. Sunucu yazılımı kartın hesaplama ve veri saklama yetilerini ona veri gönderip karşılığında veri ve cevap alarak etkin bir şekilde kullanır.

Kart uygulama yazılımı, klasik akıllı kartları özel bir uygulamada kullanmak için tercih edilir. (bkz. Çizelge 2.1) Bunu yaparken sunucu yazılımının özelliklerini kartın kendisine taşır. Bu da, sunucu ve kart arasındaki iletişimin hızı açısından verimlilik ya da sistemin bir bölümünün korunumu açısından güvenlik özelliklerinin kullanımı sayesinde gerçekleşir. Kart sistem yazılımı, kartın üzerinde bulunan çipin mimarisine özgü olarak kartın sahip olduğu temel fonksiyonları zenginleştirmek üzere alt seviye makine dilinde yazılmıştır.

Çizelge 2.1 Örnek uygulamalarıyla akıllı kart yazılım çeşitleri

Yazılım Türü	**Uygulama**	**Sistem**
Sunucu	Sayısal imza	Elektronik cüzdan
Kart	Piyango	Şifreleme algoritması

2.3 Sunucu ve Kart Yazılımı Entegrasyonu

Kart yazılımı belirli bir kartın üzerine yoğunlaşmış, o kartın içindekilerle ilgilenmektedir. Bu yazılım, uygulama yazılımlarına, önceden belirlenmiş kurallara göre kartın içindeki veriye erişim izni verir ve bunun tersi olarak da uygunsuz şekilde içeriğe ulaşmaya çalışılmasına da engel olur. Bunun yanında sunucu yazılımı ise pekçok kart için ortak özellikler taşımaktadır. Sunucu yazılımı birçok kart taşıyıcısı, birçok kart üreticisi ve aynı zamanda çok sayıda kart için ortaktır.

Kart yazılımı veri ve işlem güvenlik özelliklerini ve kurallarını belirli bir akıllı kart için gerçekleştirir. Örneğin, kartta çalışan program, doğru kişisel kimlik numarası (PIN-Personal Idenfication Number) girilmeden kart üzerinde saklanan hesap numarası bilgisine erişime izin vermemelidir. Ya da kartta çalışan program, kartın içindeki anahtarla sayısal bir imza hesaplaması yapabilmeli ancak her ne koşulda olursa olsun bu anahtarı dışarı vermemelidir. Yazılım kart üzerindeki veriye güvenli ve yetkilendirilmiş erişim sağlar.

Sunucu yazılımı akıllı kartları ve dolayısıyla onları kullanan kişileri daha büyük sistemlere bağlamakta kullanılır. Örneğin, bir bankanın ATM (Automated Teller Machine) cihazındaki yazılım akıllı kartın sahibiyle onun banka hesap bilgileri arasındaki iletişimi sağlar ve bilgilerin tutarlılığını kontrol eder. Benzer bir şekilde, metro istasyonlarında, meşrubat makinelerindeki yazılım da kartın içerisindeki kredi miktarını kontrol eder ve bu krediden alınan ürün kadar eksiltip, kullanıcıya istediği ürünü vermekle görevlidir. Bu nedenle sunucu yazılımı birçok akıllı kart çeşidinden haberdardır ve onlara göre, onların anlayacağı türden cevap verme yeteneği bulunur.

Birçok bilgisayar yazılımının aksine akıllı kart yazılımları başlangıçta bulunduğu ortamı güvenilmez olarak var sayar. Tam anlamıyla tersi kanıtlanana kadar akıllı kartlar iletişime geçtikleri sunucu yazılımlarına güvenmezler. Bir akıllı kart programı yalnızca üzerindeki yazılımına güvenir. Bunun dışındaki bütün programlar onunla etkileşime geçmeden önce güvenilir olduklarını akıllı kartlara bir şekilde kanıtlamak zorundadırlar.

Sunucu Programları

Bugüne kadar genellikle tüm akıllı kart programları, önceden standart özelliklerde üretilip hazırda satılmakta olan ya da üreticilerin özel istekleri doğrultusunda, belli özelliklere sahip olarak bankalar, telekominikasyon şirketleri ve devletler için ürettikleri akıllı kartlar için yazılmış sunucu yazılımlarıdır. Bu geniş kullanımlı kartların işletim sistemleri, akıllı kartın tepki verebileceği 20 ya da 30 komutluk karakteristik bir komut setine sahiplerdir. Sunucu yazılımları komutları karta, kart işletim sistemi de bu komutları işleyip sonuçları tekrar sunucu yazılımına geri gönderir. Bunlar, “Kullanıcının PIN’inin 1234 olduğunu doğrula”, “Beşinci dosyanın ikinci kayıtını oku ve bunu bana döndür” ya da “Elektronik cüzdandaki 15 YTL’den 2 YTL azalt” gibi komutlar olabilir.

Günümüz akıllı kartlarında kullanmak isteyeceğimiz daha özel fonksiyonlar ve bunlara bağlı olarak komutlar olabilir. Şu anda her işleme uygun bir kart ve yine her projeye uyacak bir işletim sistemi mevcut değildir. Örneğin bir kısım kartlar ödeme için gerekli özellikleri taşırken, diğerleri ağ ve şifreleme sistemleri için uygun, bir diğer tür kartlar da taşınabilir uygulamalar için gerekli özellik ve işletim sistemlerine sahiptir. Aynı zamanda birtakım kartlar da genel amaçlı kullanıma yönelik düşük seviye fonksiyonlara sahiptir. Bu bağlamda sunucu yazılım programcısının yapacağı ilk şey, oluşturacağı sistemde, bu sistem için kendine en uygun kartı seçmek olmalıdır.

Akıllı kart sunucu yazılımı kartla ilgili bir işe başlamadan önce özellikle iki görevi yerine getirmelidir. Bunlardan ilki iletişime geçeceği kartın doğrulanması, ikincisi ise kendi doğruluğunun karta kanıtlanmasıdır. Bu gerekli güven sağlanmadan iki parti arasında hiçbir işlem başlatılmamalıdır. Aslında akıllı kartın gerçek görevini yapmak için üstleneceği rol, kredi düşülmesi, sayısal imza oluşturulması gibi, sunucu yazılımı ile kart işletim sistemi arasındaki toplam etkileşim içersinde oldukça küçük bir bölümü oluşturmaktadır.

Yeni Nesil Dillerde Kart Programlama

1996'nın sonlarında, bir akıllı kart üreticisi olan Schlumberger, yeni nesil dillerinin en önemlilerinden Java programlarını çalıştırabilen ilk satışa hazır akıllı kartlarını duyurdu [52]. Java Card ortaya çıkana kadar akıllı kartlar yalnızca kendi üreticilerinin yazıp yüklediği yazılımları çalıştırabilmekteydiler. Bu da oldukça uzun, sıkıcı ve hataya açık bir süreçti. Aynı zamanda çok miktarda kart kullanan büyük şirketler dışında oldukça pahalı bir işlemdi. Bazı üreticiler Fortran, C gibi yeni nesil diller kullanmışlar ancak bu araçların kullanımı kartın sahibine uygun şekilde yansıyamamıştı [53].

Java programlamanın en önemli özelliklerinden biri, sunucu yazılımına kartla daha verimli iletişim kurabilmek için ekstra komutlar sağlayabilmesidir. Java programı sunucu yazılımından komutları alır, onları kart üzerinde çalıştırır ve onları tıpkı kartın üzerindeki işletim sisteminin yaptığı gibi cevaplandırabilir. Bu sayede bir Java Card, kendisinden önceki kartları da taklit edebiliyor ve sağladığı yeni komutlar ile hem yeni bir teknoloji ortaya çıkarıyor, hem de geriye dönük uyumluluk sağlıyor.

Teorik olarak Java akıllı kart programları akla gelebilecek tüm komut setlerini oluşturabilir ve uygulayabilir. Ancak, hem kart üzerindeki programın hafıza kısıtları hem de işlemler için harcanan süre ile ilgili olarak zaman kısıtları nedeniyle ve üzerinde çalıştığı işletim sisteminin fonksiyonelliği Java kartlarının da limitlerini etkileyen en önemli faktörlerdendir. Örneğin şifrelemenin çok güvenli anahtarlar kullanılarak kart üzerindeki Java tarafından yapılması, karta yükleme esnasında çok fazla hesaplama zamanı gerektirdiğinden ötürü istenmeyebilir. Bunun yerine işletim sistemi üzerinde şifreleme fonksiyonları yerine üretici tarafından karta sadece şifreleme işlemlerini yapan ikinci bir denetleyici entegre edilebilinir.

Akıllı kart üzerinde depolanıp çalıştırılan Java programları aynı zamanda klasik ana/bağımlı bağlantıyı kaldırmış, bu da ortaya yeni akıllı kart uygulama sınıflarının çıkmasını sağlamıştır. Her ne kadar altta çalışan sistem halen yarı çift yönlü kanala sahip olsa da, ki bu kanal iki

tarafın da diğer tarafa bilgi gönderebilmesine ve ancak bunu aynı anda sadece bir tarafın yapabilmesine izin vermektedir, programcı kartın sunucu yazılımına bilgileri ne şekilde göndereceğini ayarlayabilmekte ve bunun üzerinde tam kontrol sağlayabilmektedir.

Makine Dilinde Yazılan Kart Programları

Bazı durumlarda sistem tasarımcısı akıllı kart üzerindeki işletim sistemini geliştirmeyi ya da yeni ve kendine özgü bir akıllı kart oluşturmayı isteyebilir. Örneğin, yeni bir şifreleme algoritması eklemeyi ya da kartla yeni bir iletişim şekli oluşturmayı düşünebilir.

Özelleştirilmiş bir akıllı kart oluşturabilmek için, uygulama yazılımcısı, Schlumberger ya da Gemplus gibi bir akıllı kart ve muhtemelen Motorola, Siemens ya da Philips gibi bir çip üreticisiyle birlikte çalışmak zorundadır. Tamamen farklı bir kart oluşturmak için var olan işletim sistemini geliştirmek, yeni kütüphaneler eklemek de bu sayede mümkün olabilir. Kartlarda bulunan iletişim ve kart dosya servisleri gibi birtakım fonksiyonlar genellikle bütün akıllı kartlar için ortaktır. Özgün bir kart tasarımcısı bunları tekrar üretmek istemeyecektir. Şu anda çok az sayıda bağımsız geliştirilmiş akıllı kart işletim sistemi kullanıma hazır olarak bulunmaktadır.

Özelleştirilmiş bir akıllı kart oluşturmak hem zaman hem de maddi açıdan oldukça pahalıdır. Çizelge 2.2'de bazı varsayımlar verilmiştrir. Oluşturulacak olan yeni kart kullanılmakta olan sistemle, sunucu yazılımıyla ve diğer sistemlerle sorunsuz olarak çalışabilmelidir, bu da sunucu tarafında da para ve zaman harcamasına neden olacaktır. Genellikle bu özelleştirme işlemi kritik öneme sahip ve uyumluluğun birinci derecede gerekliliği bulunmayan durumlarda yapılır.

Çizelge 2.2 Akıllı kart projeleri karşılaştırılması

Yazılım Türü	Uygulama Geliştirme Süresi	Yazılım Boyutu	Kullanılan Kart Tipi	Zorluk Derecesi	Yapılacak Harcama
Sunucu	6 Ay	10 KLOC	Satışta Olan	Orta	Düşük
Uygulama Kart	1 Sene	1 KLOC	Java Card	Orta	Orta
Sistem Kart	2 Sene	4 KLOC	Özelleştirilmiş	Yüksek	Yüksek

2.4 Akıllı Kart Yazılım Güvenliği

Akıllı kart yazılım güvenliği, şifreleme teknikleri kullanılarak gerçekleştirilmektedir. Anahtarlar karttaki dosyalarda saklanmakta, algoritma ve protokoller ise kartta bulunan

yazılımlara entegre edilmiştir. Şifreleme teknikleri, kullanıcılar, kartlar ve terminaller gibi sistem elemanlarını yetkilendirmek ve akıllı kartla dış dünya arasındaki iletişimi şifrelemek için kullanılır. Kendi güvenlik gereksinimleri nedeniyle akıllı kartların içine gömülü bulunan şifreleme fonksiyonları aynı zamanda başka sistemlerdeki güvenlik özellikleri için de kullanılabilir. Üretici tarafından sağlanan korumalar sistemin daha sonraki güvenliğini arttırıcı niteliktedir.

Akıllı kart, kaynaklara erişim izni vermeden önce kiminle iletişim kurduğunu anlamak zorundadır. Benzer şekilde, diğer elemanlar tarafından kabul edilmeden önce de kendisinin kim olduğunu ispatlaması gerekir. Bu sebepledir ki akıllı kartın aktif hale getirildikten sonra öncelikli olarak gerçekleştireceği görevlerden biri diğer sistem elemanlarına kendini doğrulamasıdır. Bunlar öncelikli olarak kartı terminale yerleştiren insanla terminal arasındaki doğrulama, daha sonra ise kartın diğer tüm varlıklarla arasındaki tanımlama ve doğrulama işlemleridir.

Kimlik denetimi, kimi zaman önceden belirlenmiş bir 4 haneli PIN gösterimi olabileceği gibi karşı taraftan gelen şifrelenmiş bir mesajı, belli bir anahtar, algoritma ya da önceden tanımlanmış işlem protokolü kullanıp anlayabileceği hale getirme gibi karmaşık bir işlem de olabilir. Bu kimlik denetimi sırasında herhangi bir noktada, bir varlık olması gerekenden farklı davranışlar sergilerse, o varlıkla o aşamadan sonra yapılacak olan tüm iletişimler engellenir. Bu başarısız girişimleri her biri, belli bir sayıya ulaştığında kaynaklara erişimin kısıtlanması ya da sonraki tüm işlemlerin engellenmesi amacıyla akıllı kartta depolanabilir.

Şifreleme akıllı karttan dışarıya ya da dışarıdan karta doğru yapılacak olan tüm mesaj trafiğine uygulanabileceği gibi sadece belli mesajlara da uygulanabilir. Eğer akıllı kart aynı anda iki uygulamayla iletişim içerisindeyse, bu uygulamaların her ikisi için ayrı şifreleme anahtarları kullanabilir.

Akıllı kart uygulama geliştiricileri yeni kimlik denetim ya da şifreleme algoritmaları tasarlamak zorunda değillerdir. Bunun yerine, akıllı kartın üzerinde hali hazırda bulunan fonksiyonları kullanabilirler. Bunlar, önceden denetlenmiş ve belli bir doğruluk seviyesinde çalıştığı ispatlanmış olanaklardır. Yeni algoritmaların tasarlanması kolay olmadığı gibi, doğruluklarının ispatı da uygulama geliştiricileri tarafından tercih edilmemektedir. Çizelge 2.3'te bazı akıllı kartların üzerinde bulunan şifreleme algoritmalarının listesi verilmektedir.

Çizelge 2.3 Akıllı kart şifreleme algoritmaları örnekleri

Algoritma	Örnek Kullanımı
DES	İletişim kanalları
A3 ve A8	GSM telefonları
Elliptic Curve	Sayısal imza
RSA	Sayısal imza

2.4.1 DES Veri Şifreleme Standartı (Data Encryption Standard)

Veri Şifreleme Standartı (Data Encryption Standard - DES), IBM tarafından geliştirilmiştir. DES şu ana kadar üzerinde en çok çalışma yapılan algoritmadır ve içerisinde önemli sayılabilecek zayıf bir noktaya henüz raslanmamıştır.

Orjinal DES algoritmasında, DES anahtarı adı verilen, rastlantısal olarak 1'ler ve 0'lar kullanılarak üretilmiş 56 bit uzunluğunda bir veri kullanılır. Bu dizi asıl veriyle karıştırılır ve daha sonra kendisine eklenir (toplama işlemi), sonuçta ortaya karıştırılmış bir veri çıkar. Anahtarı değiştirme işlemi yeni ve farklı bir veri dizisiyle başlar.

Şifre çözme işlemi de göndericiyle aynı noktadan başlayarak, aynı rastlantısal örgüyü elde edebilmek için tasarlanmıştır. Tam olarak şifreleme işleminin tersi uygulanır, tekrarlı çıkarma işlemi yapılarak orjinal veriye ulaşılır.

Bu algoritma şimdilerde geliştirilmiş ve Triple-DES adı verilen, anahtar uzunluğunun üç katına çıkarıldığı yeni bir algoritma haline getirilmiştir.

Bu algoritmada hem göndericinin, hem de alıcının aynı anahtara sahip olması gereklidir. Böylece her iki tarafında birbirini tanıma işlemi otomatik olarak sağlanır. Şifreyi çözmek için saldırıya nerden başlaması gerektiği hakkında bir bilgiye sahip değildir.

2.4.2 RSA Açık Anahtar Tekniği (Public Key Technique)

RSA'nın mantığı, şifreleme için e, şifre çözme için d olarak belirlenen çok büyük iki asal sayıyı çarptığımızda elde edilen n sayısını, kendisini oluşturan orjinal iki sayıya dönüştürme prensibine dayanmaktadır.

$$n = e\ d$$

RSA asimetrik şifreleme sistemi olarak adlandırılır. Çünkü, şifre çözme anahtarı olan d ile şifreleme anahtarı olan e birbirlerinden farklıdır. RSA, çift anahtarlı bir sistemdir, e ya da

d'den herhangi biri ele geçirildiğinde sistem çözülebilir.

n herkese açık olarak yayınlanabileceği için, şifreleme konusunun en büyük sorunlarından olan anahtar iletimi için genel anahtar dosyası oluşturmaya imkan verecektir. Herkese açık olan n özel değeri, kimlik denetimi gerçekleştirilmesi için bir bireye ya da firmaya verilebilir. Bu, tasdikleme otoritesinin (certification authority) görevidir.

Açık anahtar şifreleme sistemleri, kimlik denetleme işlemlerine sayısal imza özelliği eklemede kolayca uygulanabilir. Sayısal imza kullanımı alıcının önceden gerçekleşen iletişimi inkar etme (repudiation) ihtimalini ortadan kaldırır.

2.4.3 A3 ve A8 Şifreleme Teknikleri

Bu teknikler GSM telefon sistemlerinde kullanılmaktadırlar ve sağlama toplamı (cheksum) işlemine dayanmaktadır. Kullanılmakta olan ve ticari uygulama olduklarından haklarında çok fazla ayrıntı bilinmemektedir.

2.4.4 ECC Eliptik Eğri Şifreleme Algoritması (Elliptic Curve Cryptosystem)

Eliptik eğri şifreleme ayrık logaritma şifreleme sistemidir. Ayrık logaritma sistemi (discrete logarithm system), açık anahtarı, gizli anahtarların yerine kullanma işlemini engellemek üzere geliştirilen ve çözümü zor olan diskrit logaritma problemine dayanmaktadır.

ECC aygıtları diğer sistemlerden daha az saklama alanı, daha az güç, hafıza ve veriyolu genişliği gerektirir. Bu da bu şifreleme teknolojisinin birçok alanda uygulanabilirliğini arttırmaktadır. Bunların arasında kablosuz cihazlar, el bilgisayarları, akıllı kartlar ve küçük istemciler vardır. Verimliliğin önemli olduğu durumlarda bu teknik çok önemli avantajlara sahiptir [13]

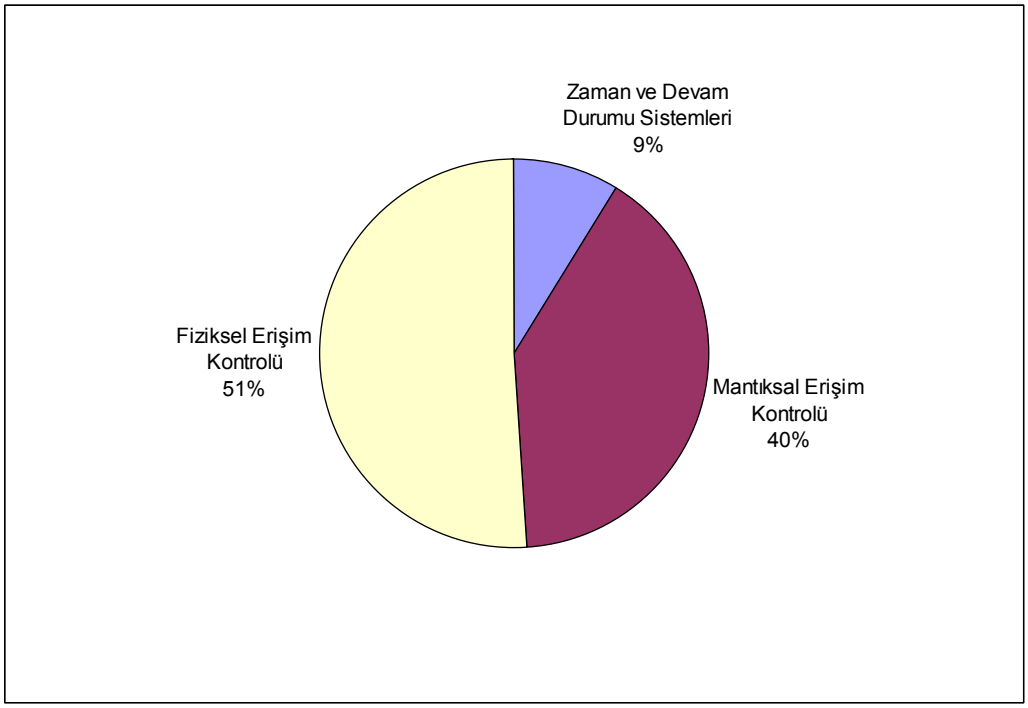
İçerdiği gömülü mikroçip kopyalanamadığından ve bilgi erişim korumalı (protected access) kontrol içerdiğinden günümüz kart teknolojisinde akıllı (smart) kartlar en güvenilir ortamı oluşturmaktadır. Tüm bu nedenlerden dolayı akıllı kartlar geleneksel kağıt tabanlı pasaport ve vizelerin yerini almaya aday en iyi teknolojilerden biridir.

2.5 Biyometrik Tanıma (Biometrics) Nedir?

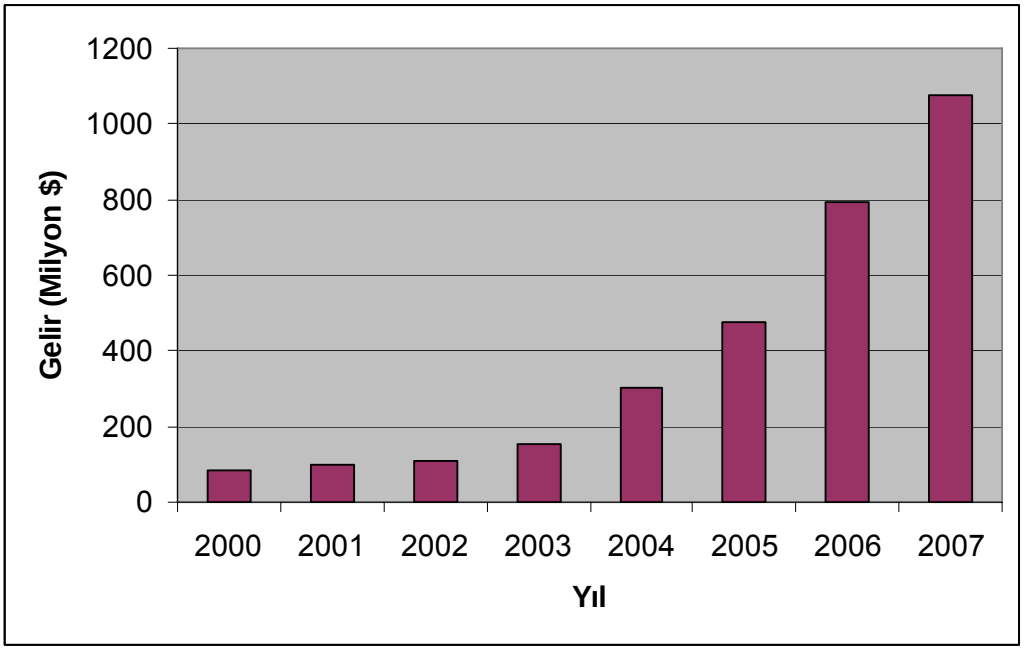
Geçmişten günümüze kadar kullanılan geleneksek kimlik saptama yöntemleri genellikle şifre, PIN gibi kişinin bildiği ya da kart, anahtar gibi kişinin sahip olduğu varlıklar üzerinden gerçekleştirilmiştir (Miller, 1994). Ancak bu şifreler unutulabilir, başka bir kişi tarafından tahmin edilebilir ya da kart çalınabilir veya kaybedilebilir.

Biyometri, kişileri fiziksel özelliklerinden yararlanarak tanıma bilimidir (Ratha,1995). Biyometrik Tanıma Sistemlerinin (BTS) fiziksel ya da sanal kaynaklara erişimi sağlamada yakın gelecekte kullanılacak en önemli teknoloji olması beklenmektedir. Bu teknoloji elde ya da akılda tutulan şifre, kart gibi varlıklar yerine, kişinin bireysel olarak sahip olduğu kendine özgü özellikler üzerinde çalışmaktadır. Teoride kişinin sahip olduğu hemen hemen bütün fiziksel özellikleri bu teknolojide kullanılabilir, ancak en seri ve verimli biyometrik tanıma işlemleri parmak izi, yüz, iris (göz), retina, el geometrisi, ses ve imza üzerinde gerçekleştirilmektedir (Pankanti, 2000; Liu, 2001; Greene, 2001).

Son zamanlarda (özellikle 11 Eylül 2001 tarihinden sonra) artan yüksek güvenlik gereksinimleri beraberinde biyometrik teknolojinin güvenlik sistemlerinde kullanımını da artırmıştır. 2001 yılı itibariyle biyometrik teknolojinin kullanıldığı en önemli üç kol olan fiziksel erişim, mantıksal erişim kontrolü, zaman ve devam sektörleri şekil 2.1'de görülmektedir (Norton, 2002). Endüstrinin ulaşacağı büyüklük 2007 yılı itibariyle 1 milyar USD olarak gösterilmektedir (BSWD, 2002) (bkz. Şekil 2.2).

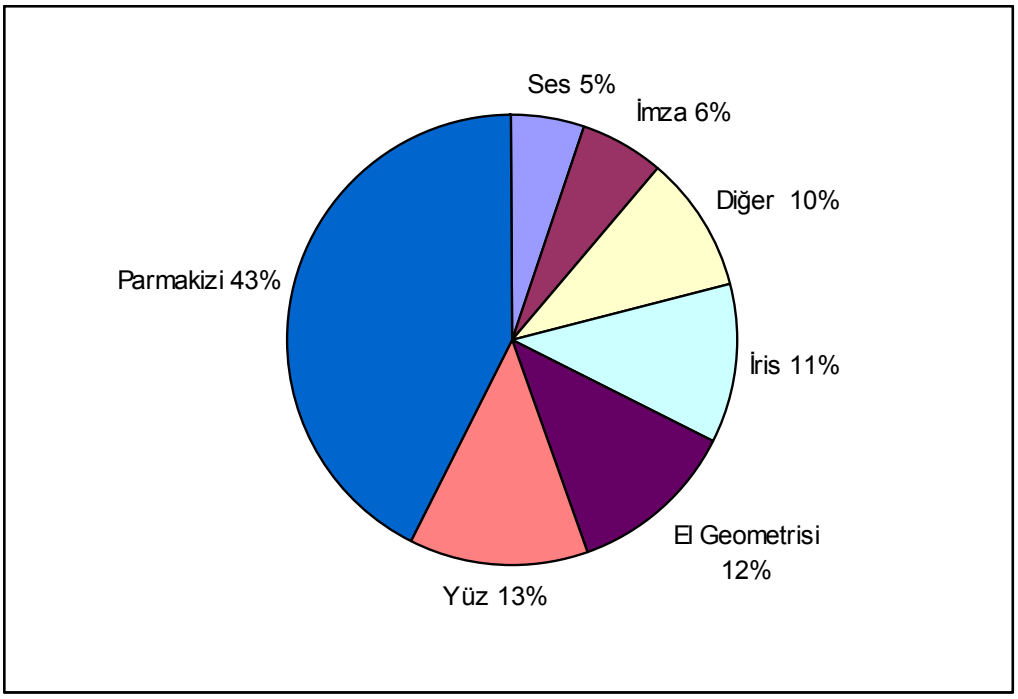


Şekil 2.1 2001 Yılı biyometri pazar payı dağılımı



Şekil 2.2 2000-2007 Yılları arasındaki biyometrik teknoloji pazar büyüklüğü

Kullanılmakta olan biyometrik teknolojiler içerisinde parmak izi tanıma bu pazarda en yüksek yaygınlığa sahiptir (BTT, 2003) (bkz. Şekil 2.3).



Şekil 2.3 2002 Yılına ait biyometrik teknolojileri pazar dağılımı

Biyometrik Tanıma Sistemi (BTS), bir kullanıcıdan alınan bilginin fiziksel ya da davranışsal özelliklerinin analiz edildiği şekil tanıma sistemidir (Pankanti, 2000). İlk aşamada (sistemin eğitimi); sistem, vektör şablonları ya da prototipler şeklinde sayısallaştırılmış olan kişiye özgü bilgileri alır. Genellikle bu bölüm sistemin genel yaşam süresini oluşturur. Daha sonra kullanıcılardan alınan biyometrik özellikler daha önceden hazırlanmış olan veritabanındaki biyometrik bilgilerle karşılaştırılır. Böylelikle sistem, kişinin gerçekten istenilen kişi olup olmadığına karar verir. BTS iki farklı şekilde çalışabilir. Bunlardan ilki kimlik doğrulama, diğeri ise kimlik saptaması yani özdeşleşmedir. Kimlik doğrulamada sistem, kişinin olduğunu iddia ettiği kimlik bilgisini veritabanından alır ve önceden kendisine uyması istenen hassaslık ölçüsünde bu doğrulama işlemini gerçekleştirir, sonuçta kullanıcıyı kabul ya da reddeder. Teşhis işleminde ise BTS biyometrik özellikleri çıkarıp veritabanındakilerle karşılaştırıp, veritabanındaki kullanıcılardan hangisi olduğuna karar verir.

Bu yöntemler arasında şüphesiz teşhis işlemi çok daha fazla dikkat gerektiren bir yöntemdir. Bunun birkaç nedeni vardır; birincisi, doğrulamaya göre çok daha fazla karşılaştırma işlemi yapılması, ikinicisi de bu karşılaştırma işlemleri arttıkça hata olasılığının da buna paralel olarak artmasıdır (Daugman, 1999).

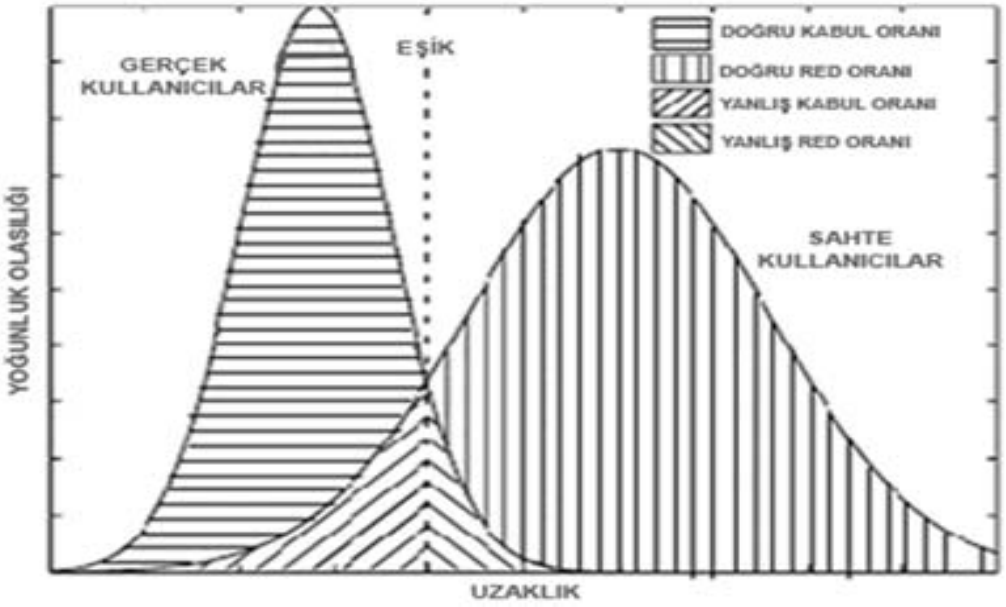
Örüntü tanımanın geleneksel yöntemleri BTS için de kullanılabilir. Kullanıcı erişim

sisteminin P kişisinden alınan belirleyici özellik vektörü şablonunun P′ duğunu farzadelim ve iki durumu da inceleyelim (Bolle, 2000).

H_0 : $P=P'$, kullanıcı orjinal

H_1 : $P\neq P'$, kullanıcı sahte

Yanlış kabul oranı (FAR-False Accept Rate) sistemde olmayan bir kişiyi sistem içerisinde yer alan bir kişi olarak algılama, sahte bir kullanıcının sistemdeki varlığı hipotezinin gerçekleşme olasılığıdır. Yanlış reddetme oranı (FRR-False Reject Rate) ise sistem içerisinde yer alan birini sahte bir kullanıcı olarak algılama, orjinal kullanıcının sistemde olması durumunda diğer hipotezin gerçekleşme durumudur. Şekil 2.4'te iki parametrenin de birbiriyle oldukça ilişkili olduğu görülmektedir.



Şekil 2.4 Biyometrik sistem karar grafiği

2.5.1 BTS Gereksinimleri

Kabul edilebilir bir BTS'nin geliştirilmesi bir taraftan operasyonel, teknik ve üretim karakteristiklerine, diğer taraftan da son uygulamadaki başarısına ve finansal uygunluğuna bağlıdır. Bu bölümde birbirinden farklı BTS'ler için değişik karakteristik kriterler ve onların uygun olabileceği alanlar verilmektedir.

Güvenilirlik – Şifre tabanlı bir güvenlik sisteminde doğru şifrenin girilmesi herzaman kullanıcının kabul edilmesine, yanlış şifrenin girilmesi ise kullanıcının reddine neden

olmaktadır. Ancak %100 başarılı bir kimlik doğrulama BTS tarafından garanti edilemez. Algılayıcı gürültüsü, işleme metotlarındaki sınırlamalar ve daha da önemlisi biyometrik özellikler ve onların gösterimi örnek verilebilinecek en önemli nedenler olabilir. Uygulanacak biyometrinin hassasiyeti de üzerinde çalışılan veri sayısına bağlı olarak değişmektedir. Başarılı bir BTS için kullanılacak teknolojinin ve bu teknolojinin üzerinde çalışacağı uygulamanın ve insanların çok iyi analiz edilmesi gerekir (Wayman, 1999). Büyük ölçekli projelerde güvenilirlik kritik bir gereksinimdir. Dikkat edilmediği takdirde elde edilen hassasiyet yetersiz hale gelebilir.

Kullanım kolaylığı – Kullanımdaki zorluk ile sağlanan güvenlik seviyesi arasında ters orantı bulunmaktadır. BTS'nin kullanım açısından pratik olabilmesi için sistemde kullanılacak uygulamanın eğitiminin kullanıcılara detaylı bir şekilde önceden verilmesi gerekmektedir. Uygulamanın uyumuyla kullanıcılarının bu sistemi kabulu herzaman önceden tahmin edildiği şekilde olmayabilir.

Kullanıcı kabulü – Çoğu kullanıcı hantal, kullanımı zor sistemleri sevmez ve bunları kullanmayı zor bulur. Ancak yüksek güvenlik gerektiren uygulamarda, BTS genelde kullanımı karmaşık bir sistemdir Daha da önemlisi biyometrik teknoloji hakkında akla şu soruyu getiren birkaç önyargı bulunmaktadır: İnsanları izlemek için kullanılan biyometrik veri, gizlilik haklarına tecavüz anlamına gelir. Biyometrik teknoloji aslında böyle bir durumun olmasını en az diğer doğrulama yöntemleri kadar engellemektedir. Birçok biyometrik teknoloji tek yönlü mantık ile çalışmaktadır. Göz tanıma örneğini ele alırsak, bir iris resminden ilgili özellik vektörü çıkarılır ve iris veritabanında saklanmış olan vektörler ile elde edilen bu canlı şablon karşılaştırılır. Bir iris resminden bu özelik vektörünü elde etmek mümkündür ancak bunun tersi yani karakteristik vektörden resmin kendisini elde etmek, birkaç rastlantısal istisnai durum haricinde imkansızdır. Bu durumda doğrulama için kullanılan veri göz resmi değil, bu resim kullanılarak elde edilen özellik vektörüdür. Bunun yanında biyometrik verinin iletişimi sırasında değişik şifreleme teknikleri de uygulanmakta, bu da veri iletişiminin maksimum güvenlikle yapılmasını sağlamaktadır. Bu durumda biyometrik teknolojinin bugüne kadar kullanılan şifre, kart gibi birçok teknolojiden daha güvenli olduğu tartışılmaz bir gerçek olarak karşımıza çıkmaktadır.

Gerçekleştirme kolaylığı – Gelişmeleri teşvik etmek ve uygulamayı yaygınlaştırabilmek için biyometrik teknoloji sistem entegrasyonu ve uygulaması için kullanımı kolay hale getirilmelidir. Biyometrik teknolojiden yararlanmak ve sistemlere entegre etmek, endüstri

standartlarının tam oturmamış olması sebebiyle kolay değildir (Wayman, 1997). Biyometrik teknolojinin kimlik doğrulama pazarına girebilmesi için gerçekleştirilen ve verimli çalışan sistemlerin sayısının arttırılması, ucuz, kullanıcı dostu uygulamalarının içerisine bu teknolojinin doğru bir şekilde yerleştirilmesi gerekmektedir.

- Maliyet - BTS maliyet fayda analizi sonucunda uygunluğu ortaya çıkan pek çok iş çözümünde kullanılmaktadır. BTS uygulamasında maliyet açısından göz önünde bulundurulması gereken birçok önemli nokta bulunmaktadır. Bunlardan bir kısmı ekipmanlarla ilgili maliyetler, kurulum ve eğitim maliyetleridir. Yazılım ve sistem bakım ve operasyon maliyetleri de eklenebilecek diğer maddeleri oluşturmaktadır. Hızla artan ucuz işlem gücü ve yüksek miktarlarda üretilen algılayıcılar biyometrik teknolojinin yakın gelecekte maliyet açısından daha da uygun yerlere gelmesini sağlayacaktır.

Çizelge 2.4'de en sık kullanılan biyometrik teknolojiler, bunların performansları ve pratik kullanım yerleri gösterilmektedir [23].

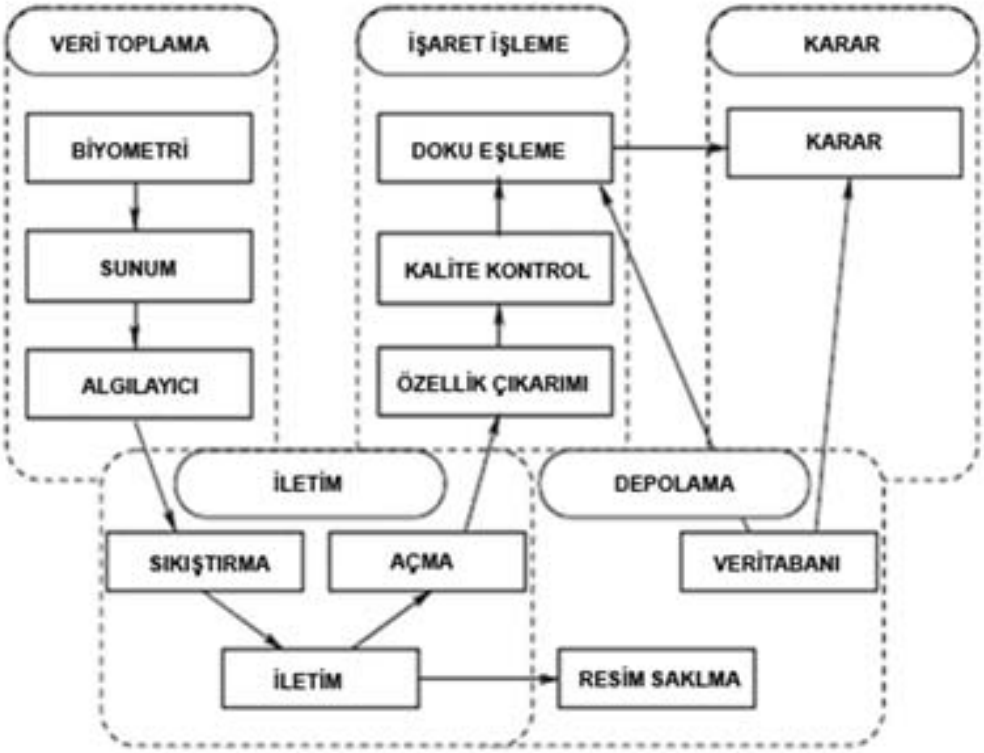
Çizelge 2.4 En önemli biyometrik teknolojilerinin karakteristik özellikleri

Biyometri Tipi	Doğruluk	Kullanım Kolaylığı	Kullanıcı Kabulu	Uygulama Kolaylığı	Maliyet
Parmakizi	Yüksek	Orta	Düşük	Yüksek	Orta
El Geometrisi	Orta	Yüksek	Orta	Orta	Yüksek
Ses	Orta	Yüksek	Yüksek	Yüksek	Düşük
Retina	Yüksek	Düşük	Düşük	Düşük	Orta
İris	Orta	Orta	Orta	Orta	Yüksek
İmza	Orta	Orta	Yüksek	Düşük	Orta
Yüz	Düşük	Yüksek	Yüksek	Orta	Düşük

2.5.2 Genel bir BTS Modeli

Biyometrik tanıma sistemlerinin daha iyi anlaşılabilmesi için sistemleri değişik bölümlere ayırmak, böylelikle de gerçek bir modelin ortaya konması gerekir (Jain, 2000; Pankanti, 2000). Böyle bir model James L. Wayman tarafından birbirinden bağımsız beş alt sistem

ortaya konarak sunulmuştur (Wayman, 1997) (bkz. Şekil 2.5). Alt sistemleri ayrı ayrı incelenmesi aşağıda verilmiştir:



Şekil 2.5 Biyometrik sistem genel modeli

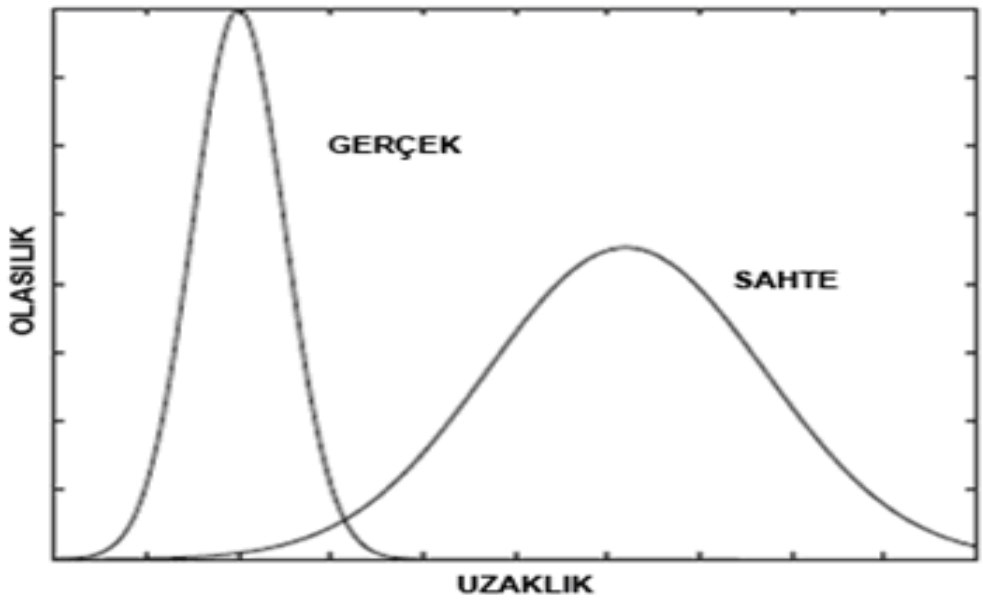
- Veri toplama alt sistemi – Bu alt sistem analiz edilecek biyometrik özelliklerin alınmasıyla görevlidir. Biyometrik karakteristikler farklı ve kararlı olmalıdır. Veri toplama için biyometrik özellik algılayıcıya iletilir. Sıklıkla daha önceden belirlenmiş bir iletim kullanılır (örneğin kişinin parmağını algılayıcının üzerine belli bir şekilde, belli bir basınç uygulayarak yerleştirmesi). Bu aşamada verinin toplanacağı yerde, kullanıcıyla sistemin gireceği etkileşim, BTS tasarlanırken önceden göz önünde bulundurulmalıdır (Wayman, 2000).

- İletim alt sistemi – Birçok durumda, biyometrik veri alma ve işleme değişik yerlerde gerçekleşir. Bu nedenle bir çeşit iletim gerekli olmaktadır. Ayrıca, bant genişliğini verimli kullanmak için verinin sıkıştırılması da gerekli olabilir. Veri iletimiyle ilgili birçok farklı senaryo düşünülebilir.

- Veri bir yerde toplanır ve işlemin (özellik çıkarımı, depolanma, karar... vs.) gerçekleşeceği başka bir yere iletim yapılır. Parmak izi, yüz tanıma, ses tanıma gibi teknikler için sıkıştırma standartları mevcuttur (Wayman, 1997).

- Veri toplama ve özellik çıkarımı belli bir yerde, depolama ve karar işlemleri de başka bir yerde yapılır. Bu durumda veri sıkıştırması gerekli olmayabilir.

- İşaret işleme alt sistemi – Bu alt sistem orjinal veriyi (ya da sıkıştırma veya açma işleminden sonra elde edilen indirgenmiş veriyi) bireylerin birbirinden ayırt edilmesini sağlayacak olan bilgileri içeren bütün farklı özelliklerini korumaya çalışarak ve gereksiz bilgileri atarak özellik vektörüne çevirir. Özellik çıkarımının amacı örüntü tanımada kullanılacak olan, diğerleriyle karşılaştırılıp sonucun sayısal olarak elde edilebileceği, buna göre karar verilebilinecek olan ve az yer kaplayan biyometrik bilginin elde edilmesidir. Şekil 2.6'de karar kriterinde kullanılan uzaklık dağılım eğrisi görülmektedir. Özellik çıkarımı ve örüntü eşleştirme tüm biyometrik teknolojilerinin çekirdeğini oluşturmaktadır ve bu işlemler orjinal ve sahte örnekler arasında olabildiğince fazla farklılık elde edebilmek amacıyla tasarlanmışlardır. Bu da daha düşük hata oranı yakalanmasını kolaylaştırmaktadır.



Şekil 2.6 Orjinal ve sahte uzaklık dağılımı

- Depolama alt sistemi – sistemle ilişki halinde bulunan kullanıcılara ait şablonları içeren alt sistemdir. Bu veritabanı merkezi olabildiği gibi bir şekilde dağıtık halde de bulunabilir.

- Karar alt sistemi – Çıkarılan özellik vektörlerinin veritabanındakilerle karşılaştırılması sonucunda sayısal değerler elde edilir. Bu durumda iki vektörün aynı olup olmadığının saptanması için bir karar işlemi gerçekleştirilmek zorundadır. Karar işlemi uzaklığın belli bir eşik değeri de göz önünde bulundurularak ölçülmesi gibi basit bir işlem olabilir. Eşleşme ya da eşleşememe sonucunda uygulanacak eylem doğrulama sistemine göre farklılık arzetmektedir. Karar işlemi sonunda, eşleşme durumunda sınırlı erişim bölgelerine ya da kaynaklarına izin verilebilir.

2.5.3 Biyometrik Tanıma Çeşitleri

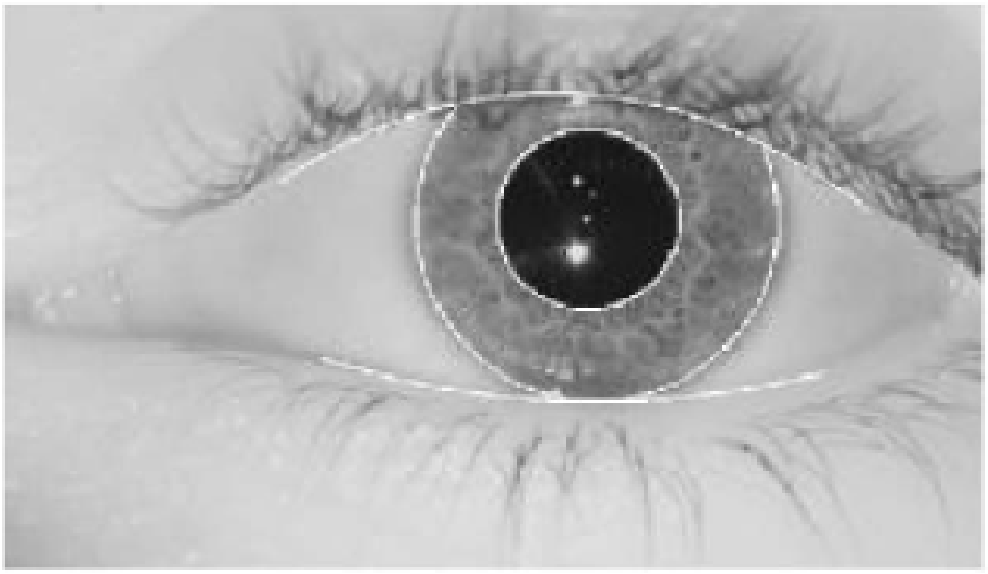
Biyometrik tanımada kullanılan göz, parmak izi, yüz ve diğer tanıma sistemleri hakkında bilgi verilecektir.

2.5.3.1 Göz (Iris) Tanıma

İnsan gözü sahip olduğu eşsiz karmaşık yapı nedeniyle biyometrik bilgi için son derece değerli bir kaynaktır (Adler, 1965). İris'in görünüşü onun sahip olduğu katmanlı yapının bir sonucudur (Wildes, 1997) ve genetik olarak belirlenmektedir. Karmaşıklığı ve doğruluğu arttırmak üzere çok sayıda göz örneğiyle çalışılarak birçok göz tanıma sistemi geliştirilmiştir (Daugman, 1993; Negin, 2000).

Böylesine küçük bir bölgenin resminin alınmasının çok kolay olmaması veri toplamayı göz tanıma sisteminin en kritik bölümü haline getirmiştir. Kullanıcıdan sistemin önüne oturması istenildikten sonra, steryo kamera gibi yapay görüntüleme teknikleri önce gözün yerini belirler daha sonra da sahip olduğu CCD (Işığa Hassas - Charge-Coupled Device) kamera sayesinde resmin elde edilmesini sağlar (Negin, 2000). Bu resimleme işleminin karmaşıklığı kullanıcıdan gözünü kameranın önüne getirmesinin istenilmesiyle azaltılabilir. Bu durumda, kullanıcıya pozisyon almada yardımcı olmak için bir geri besleme gereklidir (Wildes, 1997).

Veri toplandıktan sonra elde edilen resimde irisin yeri saptanır. İris, gözbebeğinin etrafında bir daire formunda yer alır. Bazen iris, göz kapakları veya kirpikler tarafından saklanmış olabilir. Bu durumda iris sınırları değişik yöntemler kullanılarak bulunur. Sınır integralleri (Daugman, 1997) ya da Hough çevrimleri (Wildes, 1997) bu yöntemlerden bazılarıdır. Şekil 2.7 irisin belirlendiği bir resmi göstermektedir.



Şekil 2.7 Çekilen resimde belirlenen iris

Önişleme aynı zamanda iris resmini normalleştirilmiş forma çevirmek için kullanılan bir kayıt adımını da içerir.

Önişleme adımı yapıldıktan sonra resimdeki değerli ve farklı bilgilerin uygun boyutta içerileceği ve sayısal değerlerin elde edileceği özellik çıkarım gerçekleştirilebilir. Her irisin birbirinden farklılığı çeşitli ölçeklerde sahip olduğu detaylara bağlıdır. Bu da değişik ölçeklerde yapılacak olan sınıflandırmalar için istenilen bir özelliktir. J.Daugman (1997) tarafından önerilen sistem ticari olarak kabul görmüş ve ilgi gösterilmiş bir sistemdir.

- Wildes (1997) de yine çok ölçekli analize dayanan bir sistem önermiştir. Daugman'ınkinden daha detaylı bir işlemle iris resim üzerinde belirlendikten sonra, özellik çıkarımı Gaus filtrelerinin Laplace dönüşümü uygulamasından elde edilen isotropik bant geçişli ayırma yapılarak gerçekleştirilir.

- Boles ve Boashash (1998)'ın önerdiği sistem ise farklı bir yaklaşım sergilemektedir. İristeki farklılık bilgisini göstermek için eşmerkezli daireler çizilir (iris çapı

normalleştirildikten sonra) ve karşılığı olan tek boyutlu işaretler elde edilir. Bu dairesel bölgeler diyadik wavelet dönüşü kullanılarak analiz edilir. Son olarak, iki ayrı benzerlik fonksiyonundan eşleşme algoritması meydana getirilir.

- Lim et al. Sistemlerinde iris bölgesini belirlemiş ve onu sabit boyutlu bir dörtgen içine aktarmıştır (Lim, 2001). Özellik çıkarımı, birçok alt resim elde edebilmek için Haar waveletlerini dört kere kullanılmasıyla sağlanmıştır. Özellik vektörü, alt resimden yüksek geçirgen filtreyle dördüncü adımın sonunda, önceki üç adımın ortalama değerleriyle tekrar yüksek geçirgen filtre kullanılarak elde edilen 84 özellikten oluşmuştur. Bu yolla, sonuç vektörünün boyutu 87 olmuş, her bir değer iris resminin temsil edilebilmesi için ikili bir değere kuantalanmıştır. Eşleşme ve karar adımları, eğitim işleminden sonra, iki gösterimin karşılaştırılması ve aynı irise ait olup olmadığının belirlenmesi amacıyla LVQ yapay sinir ağları kullanılarak gerçekleştirilmiştir.

- İris tanımayla ilgili diğer metotlar iris örüntüsünü ve renklerini tanıma (Flom, 1987), normalleştirme adımından sonra diğer iki boyutlu wavelet dönüşümlerinin kullanımı (Zhu, 2000) işlemlerini içermektedir.

Bu bölümde anlatıldığı üzere, iris tanıma için birden fazla algoritma geliştirilmiştir. İris resminden elde edilen bilginin çok ölçekli oluşu sebebiyle, bu algoritmaların hepsi çok ölçekli özellik çıkarım metotlarını kullanmaktadırlar. Eşleşme ve karar verme yaklaşımları birbirlerinden farklı olsa da hepsi oldukça iyi sonuçlar vermektedirler. Ancak, iris tanımadaki en önemli sorun, üzerinde çalışılacak olan iris resminin kullanıcı yardımsız elde edilmesindeki zorluktur. Bu da iris tanımanın, yüksek tutarlılığına rağmen ticari uygulamalar içindeki kullanımını önemli ölçüde azaltmaktadır.

2.5.3.2 Parmak İzi Tanıma

Parmak izi tanıma, yaygın kullanımından ötürü en iyi bilinen biyometri tekniğidir. 1893 yılında İngiltere'de Home Ministry Office iki farklı bireyin aynı parmak izine sahip olamayacağını kabul etmiştir (Jain, 2001). O günden beri, parmak izinin bireylerin tanımlanması için biyometrik bir kaynak olmaya uygunluğu üzerine araştırmalar yapılmış (Pankanti, 2001) ve ikizlerin dahi aynı parmak izine sahip olmadıkları ispatlanmıştır (Jain, 2001).

Parmak izleri her bir bireyde farklı olan tümsek ve çukurlardan oluşan bir desene sahiptir.

Daha da ayrıntıya girersek, her bir parmağın izi birbirinden farklıdır ve bu izler kişinin hayatı boyunca ona özgü olarak sabit kalır. Parmak izi tanıma için veri elde edilmesi işlemi, parmağın bir tarama aygıtına yerleştirilmesiyle yapılır. En popüler canlı parmak izi tarama teknolojisi (parmak izi canlı olarak değil, bir resimden de elde edilebilir ancak bu doğrulama işlemi mantığına aykırıdır) engellenmiş toplam iç yansıma (FTIR) konseptidir (Hartman, 1996). Diğer canlı tarama metotları ultrason toplam iç yansıma, kapasite farkı algılaması, dokunmasız üç boyutlu taramadır. Taranmış bir parmak izi şekil 2.8'da görülmektedir.

Şekil 2.8 Tanımlama işleminde kullanılan bir parmak izi

Parmak izi tanıma sisteminin işaret işleme bloğu bölüm 2.2.2'deki genel modelde olduğu gibi, elde edilen biyometrik bilginin her bir desenin farklılığını ortaya koyacak uygun gösterim haline getirilmesini amaçlar. Bu durumda akla gelen soru şudur: Hangi gösterim parmak izi resminden değişmez ve farklı bilgileri içerebilir? Birçok parmak izi tanıma sistemi parmak izindeki bölgesel yükseltilerin ve onların dağılımlarının farklılığı üzerine kurulmuştur. Yaklaşık yüzelli farklı yükselti yapısı tanımlanmış olmasına rağmen (Lee, 1991), iki belirgin yapı kullanılmaktadır: Yükselti bitimleri ve yükselti çatallanmaları. Bu iki yapı, birbirlerinin arka plan-ön plan çiftidir ve basınç çeşitlilikleri bir türdeki yapıyı diğer türe çevirebilir. Birçok durumda bu iki yapı arasındaki fark anlaşılmaz ve bu durum önemsiz ayrıntı olarak

görülür (Jain, 1997). Şekil 2.9, yükselti bitimlerini ve yükselti çatallanmalarının örneğini göstermektedir. Önceden belirtildiği gibi, birçok parmak izi tanıma sistemi parmak izinin önemsiz görünen ayrıntılarından yararlanıp, iki iz arasındaki farklılığı ortaya çıkarma esasına dayanır. Açıklanacak ve daha sonra literatürdeki diğer önerilen sistemlerle karşılaştırılacak olan tanıma sistemi, Jain (1997) tarafından önerilen sistem olup, gerek bütünlüğüyle ve gerekse sağlanan dokümanlarla anlatım için son derece uygundur. Parmak izi resminden başlayarak sistem, önce son derece önemli olan az önce bahsedilen ayrıntıların pozisyonlarını saptar. Birçok adımdan oluşan bu metot şu şekilde işler:

1. İlk olarak, bir yönlendirme alanı hesaplanır. Bu alan, resmin her bölgesindeki yükseltilerin ve çukurların yönlerini gösterir. Bu hesaplama, resimdeki (daha önceden alanların bölgesel komşuluğunun kararlılığını sağlayacak şekilde bloklara ayrılmış olan) bütün görüntü noktalarının dikey ve yatay eğimleri göz önünde bulundurularak yapılır.

2. Daha sonra yükseltiler ortaya çıkartılır ve inceltilir.

3. Bu adımda, kritik noktalar kolaylıkla bulunabilir. Her bir kritik nokta için, pozisyon, yönelim alanı ve diğer ilgili yükselti bölüm bilgisi saklanır.

Kritik noktalar bulunduktan sonra, eşleştirme stratejisi geliştirilmelidir. Kritik noktaların gösterim planı, aynı parmaktan alınan birden çok parmak izi resmi arasındaki farklılığı dikkate almayacağı için bu problem eşleştirme adımında ele alınmalıdır. Aynı kişiden elde edilmiş olsa bile iki gösterimin birbirinden farklı olmasına neden olan faktörler, rotasyon, parmağın algılayıcının üzerinde oluşturduğu baskı nedeniyle oluşan lineer olmayan deformasyonlar ya da kritik noktaların elde edilmesi sırasındaki hatalı çıkarım işlemi olabilir. Ayrıca, eşleştirme işlemi iki kritik nokta deseni arasında elastik bir karşılaştırmaya dayanmalıdır. Jain'in sistemi iki bölümde incelenen bir eşleştirme stratejisi kullanmaktadır:

1. Nokta deseni hizalaması, özellikle gürültü ve deformasyonun olduğu durumlarda genelde zor bir işlemdir. Kritik noktalardaki yükseltilerden yararlanma ve karşılık gelen eğri alanlarını kullanma problemi basitleştirir ve sonuçları kesinleştirir.

2. Mükemmel bir hizalamada, her bir karşılık gelen nokta çifti rastlantısal olmalıdır. Ancak, pratikte bu olmaz (hizalama algoritmasının aslında parmak izi özelliği sayılmayan lineer olmayan deformasyonları modelleyemeyeceği göz önünde bulundurulmalıdır). Bu nedenle, öncelikle kritik desenleri gösteren bir elastik

algoritma ve daha sonra eşleştirme sonucunu elde etmek için dinamik programlama algoritması oluşturulmalıdır.

Şekil 2.9 Yükselti bitimi ve yükselti çatallanması

Literatürde benzer yaklaşımlar bulunabilir (Duc, 1997; Furui, 1997). Sıklıkla, resim kalitesi değişkenlik gösterdiğinden, bir önişlem adımı bu kaliteyi arttırmak için yardımcı olabilir. Literatürde rastlanılan araştırmaların çoğunun kritik noktaların elde edilimi ve analizine dayanmasına rağmen, bu konuda değişik yaklaşımlar da bulunmaktadır. Bazı yazarlar geleneksel (kritik noktalara dayanan) parmak izi tanıma sistemlerinin birtakım sorunları olduğunu düşünürler. Bunların ilki, ticari uygulamalardaki yüksek örnek sayısı için yükselti yapılarının otomatik olarak elde edilmesindeki zorluktur. Bunun yanında, birbirinden farklı sayıda kritik nokta içeren iki parmak izinin karşılaştırılması da çözülmesi zor bir problemdir (Wayman, 1997). Bu eksiklikler parmak izi tanımanın yaygınlaşmasını sağlamakta kullanılacak olan yeni stratejiler geliştirilmesinin temellerini oluşturmaktadır. Coetzee çalışmasında özelliklerden yararlanmamış, bunun yerine ikili sisteme çevrilmiş parmak izi resmindeki frekans alanlarının bağıntıları üzerinde çalışmıştır (ABI, 2002). Prabhakar (2002)'ın çalışması da bu yönde oldukça ilginçtir, parmak izindeki hem bölgesel, hem de genel bilgileri kullanmak yerine geleneksel kritik nokta yaklaşımından oldukça farklı dokuma tabanlı bir yaklaşım sergilemiştir. Bu metotta, önce resimdeki nadir referans noktası yönelim alanı yardımıyla bulunur.

2.5.3.3 Yüz Tanıma

İnsan olarak bizler, diğer insanların yüzlerini tanıma kabiliyetine sahibizdir. Bu nedenle bilgisayarların da bizim yüzlerimizi tanımaları bize doğal gelmektedir. Otomatik yüz tanımanın en önemli avantajı, güvenli bölgelere girişin sağlanmasından, video gözetimlerine kadar birçok alanı kapsamaktadır. Uygulamaların birbirlerinden bu kadar farklı olmaları teknik gereksinimlerin de birbirlerinden farklı olmasını ve birçok yüz tanıma tekniğinin

geliştirilmiş olmasını da beraberinde getirmektedir. İnsanların birbirlerini tanıma şekli üzerinde çalışılmış ve otomatik yüz tanıma sistemlerinin temelleri bu sonuçlar üzerine atılmıştır (Chellappa, 1995). Yüz tanıma durağan resimler üzerinden, video karelerinden, steryo resim dizileri üzerinden yapılabilir. Bu bölümde iki boyutlu resimler üzerinden insanların tanınması konusuna değinilecektir. Bu konu hem bilimsel araştırmalarda, hem de ticari uygulamalarda en çok önem verilen konudur.

Bilgisayar yardımıyla yüz tanıma konusunda yapılan ilk araştırmaların biri Bledsoe (2001) tarafından sunulmuştur. Çalışmasında, yüze birkaç nokta yerleştirmiş daha sonra tanınmayan bir insan için verilen özellik noktaları kümesinin uzaklığı, en yakın komşu veya diğer sınıflandırma yöntemleri yardımıyla o insanın tanınması için kullanılmıştır. Benzer yaklaşımlar birçok araştırmada uygulanmış, değişik yöntemler kullanılarak göz köşeleri, ağız kenarları gibi noktalar arasındaki uzaklık ve açı cinsinden yüz karakterize edilmiştir.

Daha yakın zamanlarda ise istatistiksel yaklaşımlar ağırlık kazanmıştır. Turk ve Pentland (2000) Karhunen – Loeve (KL) yayılımını kullanarak özel yüzlerin özel vektör kümelerini saptamışlardır. Daha sonra, seçilen herhangi bir resim özel yüzlerin ağırlıklı kombinasyonu cinsinden yazılabilir hale gelmiştir. Ağırlıklar, resmin iç çarpım operasyonuyla özel yüz bileşenlerine dönüştürülmesiyle elde edilmektedir. Sınama resminin tanınması veritabanındaki resimlerden en yakın ağırlığa (Euclidian uzaklığı cinsinden) sahip olanın bulunmasıyla sağlanır. Burada kullanılan uzaklık tipindeki çeşitliliğin sistemin performansını büyük ölçüde etkilediğini belirtmek gerekir (1995).

Destek vektör makineleri (SVM) (Phillips, 1993) bu alanda kullanılmıştır. Yüz tanıma K sınıfı bir problem olarak alınırsa, K burada bilinen birey sayısıdır, SVM'ler ikili sınıflandırma metotudur. Sınıflardan biri, bir kişinin resimleri arasındaki farklılık, diğeri ise iki farklı kişinin resimleri arasındaki farklılıktır. Yüz resmi, orjinal görüntü noktaları vektörize edilip, ölçüm özellikleri veya özel yüz kombinasyonu şeklinde gösterilebileceği için N boyutlu bir vektör haline getirilebilir.

Yüz tanıma için yapay sinir ağlarının kullanımı daha çok tercih edilir. Çok sayıda sistem yapay sinir ağlarını sadece yüz tanıma için değil, aynı zamanda cinsiyet sınıflandırması ve yüz ifadelerinin sınıflandırılmasında da kullanmaktadır. Bu tip sistemlerin incelenmesi kaynaklarda bulunabilir (Miller, 1994).

Gabor filtrelemesinden genetik algoritmalara kadar diğer birçok özellik çıkarım ve eşleştirme

teknikleri yüz tanıma için kullanılmaktadır.

2.5.3.4 Diğer BTS'ler

Parmak izi tanıma muhtemelen en iyi bilinen biyometrik tanıma teknolojisidir ve çok sayıda uygulamada kullanılmaktadır. İris tanıma popüler olmasa da bugüne kadar geliştirilen doğruluk oranı en yüksek biyometrik tanıma teknolojilerinden biridir. Biyometrik tanımadaki çalışmalar halen devam etmektedir. Kaydadeğer çok daha fazla teknoloji gümünüzde kullanılmaktadır. Bunlardan bazıları şunlardır:

- Ses tanıma – Yüz tanımayla birlikte ya da tek başına çalışmaktadır. Konuşmacı (speaker) doğrulama konusuna iyi bir giriş kaynaklarda bulunabilir (Daugman, 1999). Konuşmacı doğrulama teknolojileri iki ana kategoride incelenir (Jain, 2001):
    - Yazı bağımlı uygulamalar, burada sistem her kullanıcıya farklı bir yazı verir. Yazı bağımlı sunucunun bir durumunda sistem potansiyel kullanıcıya her erişim için farklı olması gereken bir cümle verir. Yazı bağımlı konuşmacı tanımlamasında kullanılan ana metotlar, telaffuzu ardışık ses vektörleri olarak gösteren ve daha sonra sistemde tanımlı olan telaffuz ile kullanıcınınki arasındaki uzaklığı dinamik programlama yöntemleriyle hesaplayan dinamik zaman saptırımı ve gizli Markov modelleridir.
    - Yazı bağımsız uygulamalar, burada kullanıcı her girişte aynı cümleyi söylemek zorunda değildir. Bu nedenle, sistem tarafından kullanılan tek bilgi kullanıcının akustik katakteristiğidir. Bu yöntemde vektör kuantalama, küresel uzaklık ve Gaussian karışım modeli kullanılmıştır (Jain, 2001).
- El Şekli Tanıma – Bu biyometrik teknik, her insanın elinin farklı bir şekle sahip olmasına ve bu şeklin belli bir yaştan sonra dahi değişmemesi esasına dayanır. El şekli tanıma biyometrik teknikleri elin şeklini, parmakların uzunlukları, genişlikleri ve avcun belli bölgelerdeki genişliği bilgilerini kullanarak tanımlar (Wayman, 1997).
- Retina tanıma – Retina bazlı bir BTS, gözün arka kısmındaki kan damarı katmanlarını inceler. Çok üstün bir tanıma teknoloji olsa da, bu bölgenin resmini elde etmekteki zorluk, bu yöntemin en büyük dezavantajlarından biridir. Resimleri elde edebilmek

için kızılötesi ışık kaynağı gereklidir, bu sayede, farklılık bilgilerine sahip karakteristik noktaların analizi için kullanılacak olan doku resmi alınır.

- İmza onaylama – Bu biyometri teknolojisi oldukça eski bir tarihe sahiptir ve doküman tanımlama ve ilişkilendirmede yaygın kullanıma sahiptir. (Bolle, 2000) Çevrim içi ve çevrim dışı tanıma olarak iki kısımda incelenir. Çevrim dışı tanıma, imzaların kağıttan taranması ve analiz edilmesine dayanırken çevrim içi tanıma ise imza henüz atılırken (kalem ucunun kağıda değerkenki basıncını zamana bağlı olarak kaydedip) gerekli bilgiyi alan sistemlerdir (Turk, 1991). Özel donanım gerektirdiğinden, çevrim içi sistemlerin hali hazırda kullanıldıkları alanlardan daha öteye yayılma ihtimalleri az görünmektedir.

- Diğer biyometrik tanıma teknolojilerine, tuş darbesi tanıma, avuç izi özellikleri (Daugman, 1997) ve kulak tanıma örnek verilebilir.

2.5.4 Günümüzdeki Durum

Günümüzde, biyometrik ürünler sistemlerinin fiyatları, teknolojinin gelişmesine ve piyasaya birçok yeni üreticinin girişine paralel olarak hızla düşmektedir (Zhu, 1997; Rhia, 2000). Aslında biyometri endüstrisi, sektördeki güçleri ortak bir platformda birleştirmiştir. The BioAPI Konsorsiyumu, Compaq Computer Corp., IBM Corp., Identicator Technology, Microsoft Corp., Miros Inc. ve Novell Inc. şirketleri tarafından değişik üreticilerin yazılımlarında kullanılmak üzere ortak bir kullanıcı arabirimi tasarlamak üzere kurulmuştur ve desteklenmektedir (Rhia, 2000). Bir biyometrik kullanıcı arabirimi, yazılım uygulamalarının biyometrik teknolojilerle iletişim kurmasını sağlayan açık bir sistemi tanımlar. Biyometrik teknolojileri sağlayan ve üreten şirketler hakkındaki bilgiye [1, 3, 4] erişebilinir. Buna ek olarak bir takım biyometri şirketleri ve ürünleri [5, 7, 9] yayınlarda bulunabilir. Günümüzde bu şirketlerin çoğu yüz, parmak izi, iris, imza, ses ve dudak hareketi tanıma çözümleri sunmaktadırlar. AcSys Biometrics Corp. [10] pazardaki en yüksek yüz tanıma sistemine sahiptir.[11] AcSys'nin partner listesi CHUBB PLC, Litton Industries' PRC Inc., the US State Department, Consular Services Branch gibi şirket ve kurumları içermekte, halen de gelişimini sürdürmektedir. Rekabetçi firmalar olarak Nexus ve Group International Inc. [13], Graphco Technologies Inc. sayılabilir. G-TEC [14], TouchChip parmak izi biyometrisi üzerinde çalışmalar yapmaktadır ve ürünler sunmaktadır [15]. IBG biyometri endüstrisine liderlik eden ve danışmanlık yapan teknoloji servis şirketidir [12]. IBG aynı zamanda Amerika Birleşik Devletlerinde finansal enstitülere, devlet kurumlarına, sistem

entegratörlerine ve yüksek teknoloji şirketlerine 1996 yılından bu yana teknoloji tarafsız ve satıcı bağımsız çözümler sunmaktadır. IBG gerçek yaşam uygulamalarını parmak içi, yüz, iris tanıma sistemlerini kullanarak gerçekleştirmekte ve bu teknolojileri IT güvenliği, taşımacılık, akıllı kart ve tanıma sistemleri çözümlerinde kullanmaktadır.

Dünyadaki akademik ortama baktığımızda ise, Güney Carolina Üniversitesi (USC) [28], Biyometri Programı, Maryland Üniversitesi (UMD) [29] ve Massachusetts Teknoloji Enstitüsü (MIT) Medya Laboratuvarı [30] gibi birkaç laboratuvar ve araştırma gruplarının yukarıda bahsedilen şirketler için algoritma geliştirdiği görülmektedir. MIT ve USC algoritmaları ticari uygulamalar için aynı zamanda temel oluşturmaktadır. Örneğin, sektördeki en bilinen yüz tanıma şirketlerinden biri olan Viisage [31], MIT Medya laboratuvarında geliştirilen özel yüz bazlı tanıma algoritmasını kullanmaktadır.

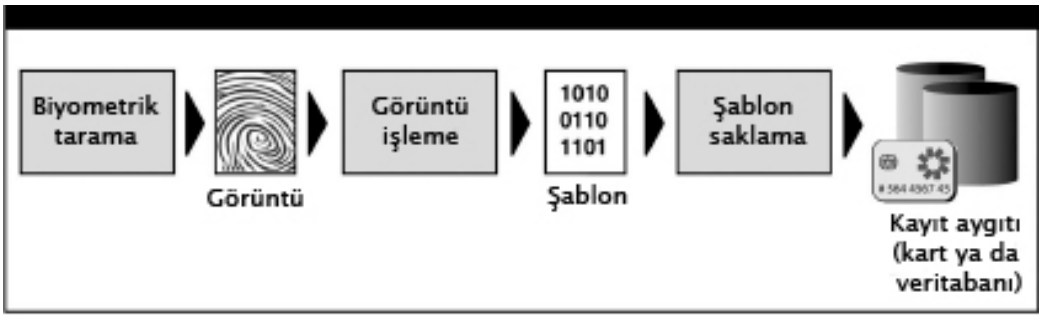
Yüksek tutarlılık seviyesine sahip büyük veritabanına sahip olan birkaç biyometri sunucusu da bulunmaktadır. Bunların en önemlileri, tanıma için biyometri teknolojilerini kullanan ve bir erişim kontrol sistemi olan BioAccess sunucusu [21], istemci-sunucu uygulamaları sağlayan ve yüksek tutarlılık, güvenlik, geliştirilebilirlik ve performans sağlayan Oss Nakalva[103]'dır. Cyber- SIGN da lisanslı teknolojiye sahip bir istemci-sunucu uygulamasıdır (TCP/IP istemci-sunucu) [24].

Biyometrik teknolojiler, kişinin kendine özgü fiziksel özelliklerinden ya da davranışlarından yararlanarak onun kimliğini tespit etmede kullanılan metotlardır.

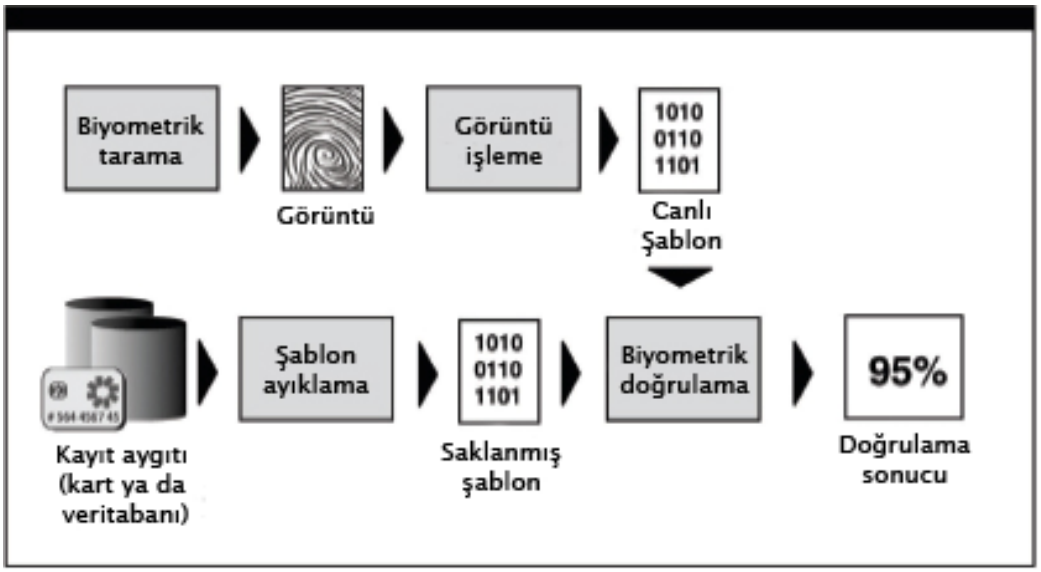
Biyometrik tanıma, çalınma ya da unutma riski taşımadığı ya da kopyalanması çok zor olduğu için güvenli ve geçerli bir doğrulama çeşididir.

Biyometrik tanıma kimlik sistemlerinde iki amaç ile kullanılmaktadır: Birincisi bireylerin kimliklerini doğrulama, ikincisi de bireyleri tanımadır. Kimlik doğrulama bireyin istenilen nüfusta olup olmadığını kontrol etme işlemidir. Tasarlanan sistemde ise kullanım amacı kartı kullanan bireyin gerçekte kartın sahibi olan kişi olup olmadığının tespit edilmesidir.

Akıllı kartlar, doğalarında olan özellikleri sayesinde yüksek güvenlikli sistemler sağlamak konusunda başarılıdırlar. Bu nedenle biyometrik tanımayla birlikte kullanılacak olan akıllı kart sistemi, tasarımı istenen güvenli kimlik tanıma sistemi için çok iyi bir altyapı oluşturma kabiliyetine sahiptir.



Şekil 2.10 Biyometrik bilginin saklanması



Şekil 2.11 Biyometrik bilgi doğrulama işlemi

Biyometrik tanıma sistemlerinde mevcut olan üç önemli bileşen şunlardır (bkz. Şekil 2.10 ve 2.11) (Uzun, 2005).

Bir insanın biyometrik karakteristiğini analog ya da dijital bir resimden tarayıp kaydedecek bir mekanizma.

Saklama, işleme ve "gerçek" resimle kaydedilmiş olanı karşılaştırmada kullanılacak bir yazılım.

Bireyin kimlik doğrulaması için uygulama sistemiyle kullanılacak olan bir arayüz.

Kullanıma uygun olan biyometrik teknolojiyi seçmek göz önüne alınmak zorunda olan birçok faktöre bağlıdır. Bunlar; çevre, kullanıcı profili, doğrulamanın kesinlik oranı, toplam sistem maliyeti ve kullanıcı kabulünü etkileyebilecek kültürel yaklaşım gibi konulardır.

2.6 Akıllı Kart / Biyometrik Kimlik

Bütünleştirilmiş bir akıllı kart / biyometrik kimlik sistemine bakıldığında şu sorulara öncelikle cevap aranmalıdır:

Biyometrik sistem kimlik doğrulama mı yoksa tanıma işlemi mi yapıyor;

Hangi tür biyometrik bilgi saklanmalı – Bütün biyometrik bilgiyi saklamak daha çok hafıza gerektireceğinden kimlik kartının maliyeti, olası gizlilik ve güvenlik tehlikelerinin sayısı artacaktır;

• Biyometrik bilgi nerede saklanacak – Biyometrik bilgi akıllı kartta, yerel okuyucuda ya da merkezi bir veritabanında saklanabilir. Akıllı kart kullanan bir kimlik sistemi için normal olarak biyometrik şablon, gizliliği ve güvenliği arttırmak için kart sahibiyle her zaman birlikte olması gereken kartın içinde saklanır;

• biyometrik işlem nerede gerçekleştirilecek – Biyometrik işlem iki birbirinden farklı ve sıralı işlemden oluşur. İlk olarak kullanıcının "canlı" biyometrik şablonu alınır ve işlenir. İkinci olarak ise çıkarılan bu canlı şablon, güvenilen ve daha önceden saklanmış olan şablonla karşılaştırılır.

Bu işlemlerin ikisi de akıllı kartın üzerinde, yerel okuyucuda, ya da merkezi sunucuda yapılabilir, ancak yüksek güvenlik gerektiren sistemlerde canlı şablon okuyucuda çıkartılıp, çıkarılan şablon karşılaştırma için akıllı karta gönderilir.

2.7 Yararlar

Bütünleştirilmiş bir akıllı kart ve biyometrik tanıma sisteminin çok sayıda yararı vardır. Biyometrik tanıma sistemlerinde akıllı kart teknolojisinin kullanımı, güvenlik seviyesini azımsanmayacak şekilde arttırmaktadır. Bu güvenlik artırımı kullanıcıya üç önemli gizlilik yararı sunmaktadır, bunlar kişisel bir veritabanı, kişisel bir ateşduvarı ve kişisel bir terminaldir.

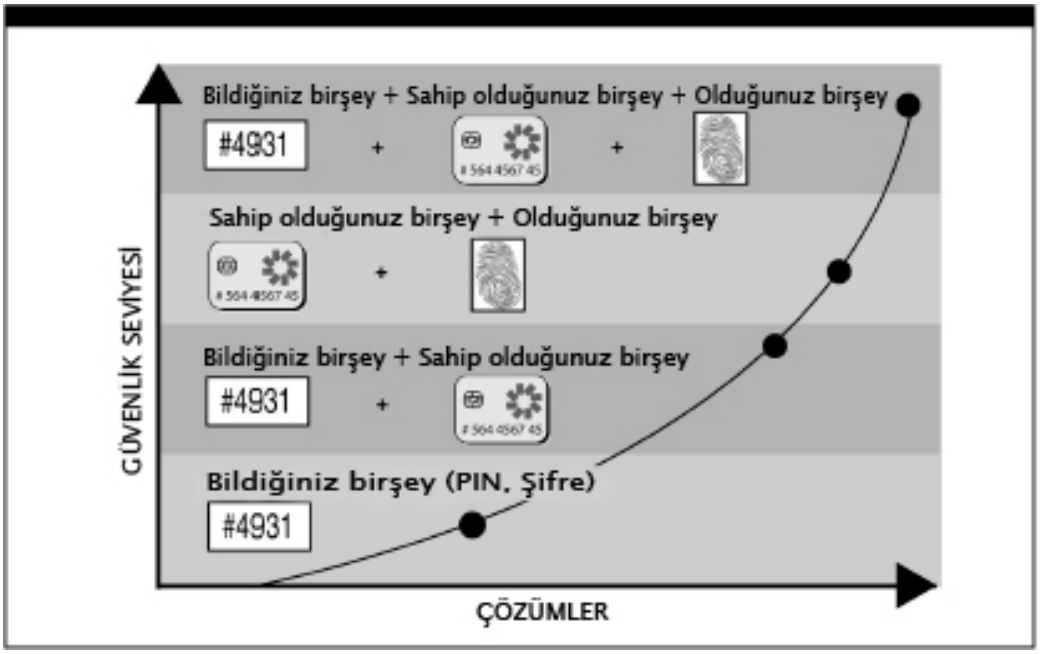
Kişisel Veritabanı

Kimlik doğrulama sistemlerinin çoğu, tüm sistem kullanıcılarının kişisel bilgilerini merkezi bir veritabanında tutmaktadır. Bu merkezileştirme bilgilerin daha az korunduğunu ya da erişilmeye açık olduğunu akla getirmektedir. Akıllı kartlar bu problemi çözmektedir. Kişisel

verileri doğrudan kendi üzerinde sakladığı ve koruduğu için verilerin korunmasını otomatik olarak arttırmaktadır. Veriler bir merkez yerine, her zaman için kullanıcının kendine ait gizli bilgilerin sahibi olduğu akıllı kart üzerinde depolanmaktadır.

Kişisel Ateşduvarı

Veri deposu olma özelliğinin yanında buna ek olarak akıllı kart aynı zamanda kullanıcının bilgileri için bir ateşduvarı özelliğine sahiptir. Kimlik kartından bilgi istendiğinde, akıllı kart bu bilgiyi isteyen kişinin buna yetkili olup olmadığını kontrol edebilecek yeteneğe sahiptir. Kart, bilgi isteyen kişinin kimliğine göre ona sınırlaması dahilinde bilgi gösterme kabiliyetini de içinde barındırmaktadır.



Şekil 2.12 Sistemin genel yapısı

Kişisel Terminal

Günümüzün elektronik dünyasında, insanlar sıkça dağıtık ya da taşınabilir terminaller vasıtasıyla sistemlerle ilişkiye girmektedirler. Sahip oldukları şifreleme işlem kabiliyetleri sayesinde akıllı kartlar bu terminallerin güvenilirliğini arttırmaktadır. Bu, bireylere arttırılmış güvenlik şekline çevrilebilir ve kart sahiplerini sıradan aygıtları kişisel terminaller şeklinde kullanımına izin verebilir.

Terminal güvenilirliğindeki artış özellikle biyometrik sistemler için çok önemlidir. Biyometrik kimlik sistemleri, biyometrik bilgileri anında tarama özelliğine sahip olan

terminallere doğrudan bağlantılıdır.

Kimlik sistemi bu tanımayı gerçekleştirecek olan okuyucuya güvenmelidir. Eğer böyle olmazsa, kimlik doğrulama işleminin bütünlüğü zarar görecektir. Akıllı kartlar bu konuya da çözüm sunmaktadırlar. İyi uygulanmış güvenlik protokollerinin kullanımı, akıllı kartları okuyucularla sayısal sertifika değişimi sayesinde anlaştırmakta, bu sayede de yüksek güvenlikli bir tanışma gerçekleştirilmiş olmaktadır.

Bütünleştirilmiş olan akıllı kart ve biyometrik tanıma işleminin bir diğer avantajı da yüksek güvenlik derecesidir. Kimlik doğrulama sistemlerinde akıllı kartlarla birlikte kullanılan biyometrik teknoloji, kullanıcıları minimum belirsizlikle tanıma işlemini gerçekleştirmektedir. Biyometrik tabanlı kimlik doğrulama, PIN numarası gibi bilmeniz gereken şeyleri kontrol etmek yerine, kim olduğunuzdan yola çıkarak kim olmanız gerektiği sonucuna varır.

Şekil 2.12 bütün sistemdeki arttırılmış güvenliği, geliştirilmiş etkinliği ve kimlik doğrulama süresinin hızını göstermektedir.

Akıllı kartları, kriptografik fonksiyonları ve biyometrik tanımayı kullanan bir kimlik sisteminin birçok önemli avantajı vardır:

Kartın her kullanım anında, biyometrik şablon sayısal olarak alınıp saklanır ve kullanım zamanları da bu bilgilerle kaydedilir;

Şablon ve diğer kişisel bilgiler güçlü bir şifreleme algoritmasıyla kartın üzerinde şifrelenmiş şekilde saklanır;

Akıllı kart, sahibinin doğru kişi olduğunu denetler. Biyometrik şablon asla kartı terketmez, üzerindeki bilgilerin korunmasını sağlar ve kullanıcının gizlilikle ilgili konularını içerir;

Akıllı kart kimliği aynı zamanda bilgi paylaşımı öncesinde kartla okuyucu arasında bağımsız kriptografik özelliklere sahip bir doğrulama işlemi gerçekleştirir. Bu da kart sahibinin önemli ve hassas bilgilerinin güvenliğini daha fazla sağlamaktadır. Bu sayede kart, istenmeyen kişilerin eline geçse bile içindeki bilgilerin okunması engellenebilmektedir;

Akıllı kartlar, programlar, birden çok biyometrik şablon, verinin değiştirilmesini, silinmesini ya da kopyalanmasını engellemek üzere kullanılacak olan birden çok kriptografik anahtar gibi günden güne fazlalaşan veri için yeterli kapasiteye sahiplerdir;

Akıllı kart aynı zamanda kart sahibinin dijital kimliğini doğrulamak için kriptografik anahtarların ve algoritmaların saklandığı korumalı hafızaya sahiptir. Bu özelliği de akıllı kartları hem fiziksel hem de mantıksal doğrulama için ideal bir ortam haline getirmektedir.

Biyometrik şablonun akıllı kartlarda saklanmasının sağladığı diğer getiriler de genel sistem performansını arttırması ve yerel kimlik doğrulamasıyla kart sahibinin rahatını sağlamasıdır.

Hızlı ve seri kullanım gerekli olduğunda, ki bu projede kullanılacak olan havaalanı ya da sınır kapısındaki gümrük çıkışları bu iş için gayet uygundur, kart okuyucusuna temas gerektirmeyen akıllı kartlar, hem gerekli güvenlik önlemlerini tıpkı diğer akıllı kartlar gibi içinde barındırmakta, bunun yanı sıra fiziksel teması da ortadan kaldırmaktadır.

Bütünleşik akıllı kart ve biyometrik tanımanın bahsedilecek en son özelliği de yüksek güncellenebilir ve esnek bir çözüm olduğudur. Aynı zamanda bu sistem maliyeti göz önüne alındığında oldukça etkileyici sonuçları olacak bir sistemdir.

Kimlik doğrulama sistemlerinde genel olarak anahtar gereksinim güncellemenin yüksek bir harcama yapılmadan gerçekleştirilebilmesidir. Akıllı kartlar, veriler ve kimi zaman da programlar bazında yeniden yazılabilir oluşları nedeniyle esnek bir şekilde kart verilerinin ya da kartla sistem etkileşimini sağlayan algoritmaların güncellemesine izin vermektedirler.

3. Sistemin Yapısı

Bu sistemdeki en önemli noktalardan biri de kartı taşıyan ve kullanan kişinin gerçekten doğru kişi olup olmadığının denetlenmesidir. Geçmişte ve hatta günümüzde, bu tanıma işlemi insan duyuları yardımıyla yapılmaktadır. Ancak, teknolojik ilerlemeler, bu tanıma işleminin daha güvenilir bir şekilde yapılmasını mümkün hale getirmiştir.

Bununla birlikte, biyometrik teşhis işlemi gün geçtikçe daha da güvenli ve önemli hale gelmektedir. Bu teknik, insanları kişiye özel olan el şekli ve boyutu, parmak izi, ses ve göz (iris) özelliklerini kullanarak ayırt etmeyi sağlıyor. Bunların her biri kişiye özgü birer özellik olduğundan, teşhis işlemini daha güvenilir hale getiriyor.

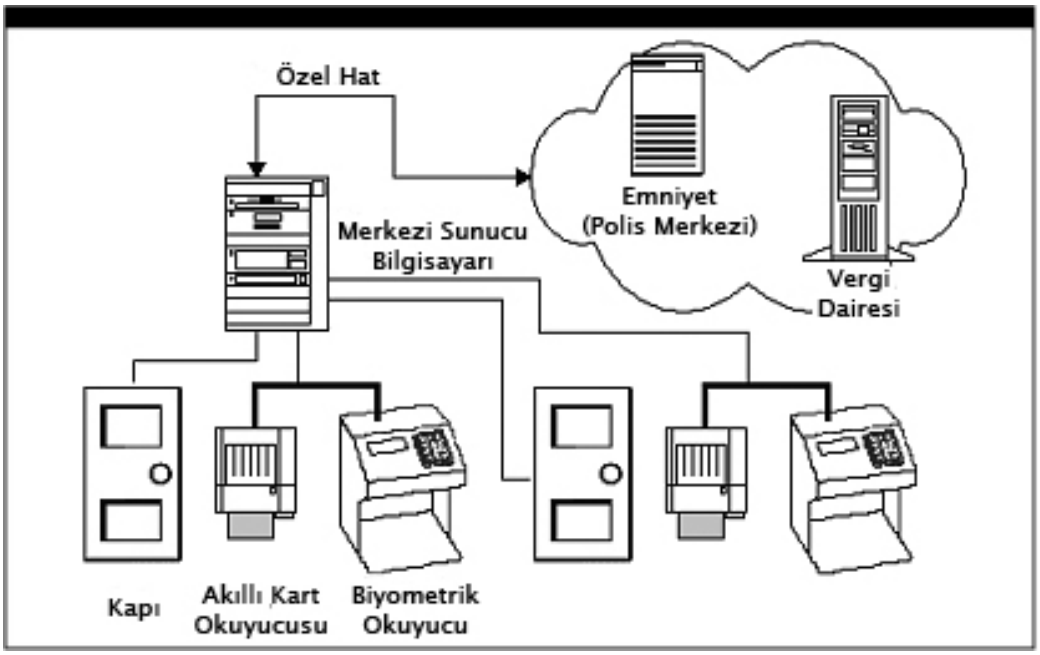
Son yıllarda mikroişlemci ve gelişmiş görüntü işleme elektronik cihazlarının fiyatlarının düşmesiyle, biyometrik teşhisi sağlayan sistemlerin maliyetleri de hızla makul düzeylere gerilemiştir. Böylelikle, biyometri giriş kontrol sistemlerinde popüler bir yere kavuşmuştur.

Sonuç olarak, biyometrik teşhisle birlikte kullanılacak olan akıllı kart teknolojisi, yeni nesil pasaport / vize uygulaması olarak ülkeye giriş kontrollerinde ana unsur olacaktır.

Tüm sistemde, geleneksel doküman tabanlı pasaport/vize, kişisel bilgilerin ve kart sahibinin biyometrik bilgilerinin bulunduğu akıllı kartla değiştirilecektir.

Kullanıcı havaalanındaki gümrük kapısına geldiğinde, kartını (pasaportunu) okuyucuya yerleştirecek ve kendi de tanımlama işlemi için biyometrik teşhis cihazının başına geçecek. Kontrol işleminden sonra, gerçek kişinin özel bilgileri ana makineye gönderilip bir sonraki onay işlemi gerçekleştirilecek, böylelikle kullanıcının suçlu listesinde bulunup bulunmadığı ya da vergi borcunun olup olmadığı anında kontrol edilecektir.

Her şey onaylandıktan sonra, merkezi makine geçişin açılması için bir sinyal yollayacak ve kullanıcının ülkeyi terk etmesi sağlanacaktır. Diğer durumda, bir uyarı sinyali gönderilecek ve görevli memur durumdan haberdar edilecektir. Şekil 3.1'de sistemin genel yapısı gösterilmektedir.



Şekil 3.1 Sistemin genel yapısı

4. Detaylı Tasarım ve Açıklama

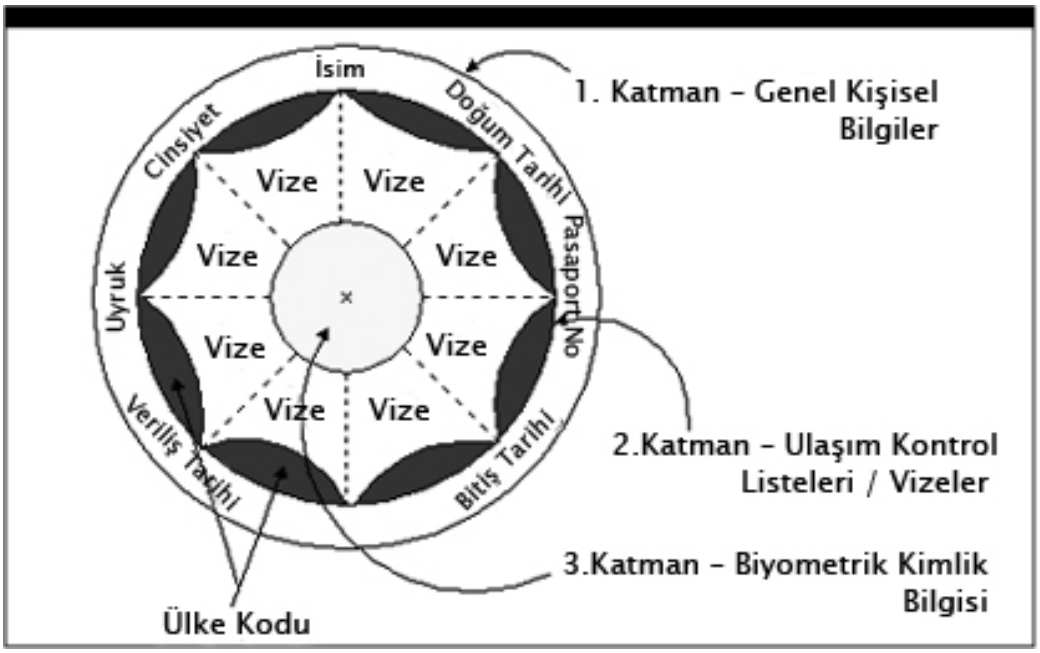
Sistem akıllı kart, biyometrik tanıma, akıllı kart okuyucu, biyometrik okuyucu, kapı ve uyarı modülü, gümrük memuru gibi birçok parçadan oluştuğu için, bundan sonraki bölümde bu parçalar teker teker ele alınacaktır.

4.1 Akıllı Kart

Akıllı kart bu sistemde en önemli rollerden birini oynamaktadır. Kart, sadece kullanıcı hakkındaki bilgileri içermekle kalmaz, aynı zamanda kartı kullanan kişinin gerçekten olması gereken kişi olup olmadığını da, denetleme işini de yapar.

Fiziksel olarak, kartın yüzeyinde kart sahibiyle ilgili bilgiler (resim, ad – soyad, cinsiyet, uyruk, verildiği tarih, geçerlilik süresi ve imza gibi) bulunacaktır. Bu bilgilerin tümü genel bilgi edinme amaçlı kullanılacaktır.

Kartın içinde yer alan mikroçip daha detaylı bir bilgiye sahip olacaktır. Mantıksal olarak mimari incelendiğinde üç katmandan oluşan bir yapı karşımıza çıkacaktır. Her katman alt katmanda olan bilgileri içeren ve koruyan bir yapıya sahiptir. Şekil 4.1 bu yapıyı genel olarak göstermektedir.



Şekil 4.1 Akıllı Kart Yapısı

1. Katman – Genel Kişisel Bilgiler

Bu katman, kişi hakkındaki genel bilgileri içerir. Bunlara örnek olarak, isim, cinsiyet, doğum tarihi, uyruk ve pasaport no verilebilir. Bu alanın amacı, ülkenin gümrük bölgesini kullanmak isteyen kişiyle ilgili bilgilere erişmek ve bunları kendi veritabanına kaydetmektir. Buradaki bilgilerin bir kısmı merkezi ana makineye de gönderilecektir. Bu katmandaki bilgi tek yazımlık ancak çok okumalı bir yapıda olmalıdır, aynı zamanda şifrelenmiş halde saklanmalıdır ve kart sahibi gerektiğinde PIN kodunu girerek bilgileri görebilmelidir.

2.Katman – Ulaşım Kontrol Listeleri / Vizeler

Geleneksek vizeler dijital ortama aktarılacak ve bu bölümde tutulacaktır. Farklı ülkelere ait farklı vizeler sıralı şekilde bu bölüme yazılacaktır. Her kayıttaki bilgi, ülke kodu, vize tipi/sınıfı, veriliş tarihi, bitiş tarihi, şartlar gibi verilerden oluşur. Belli bir vizenin süresi dolduğunda, kayıt orada kalacak, bir sonraki yenilemede bu kaydın üzerinde gerekli değişiklikler gerçekleştirilecektir. Bu nedenle, kayıttaki her veri alanı dikkatli bir şekilde doldurulmalı ve böylelikle kullanıcının aynı anda çok sayıda vizesi olma durumu gerçekleştirilmelidir. Ayrıca, her bir vize kaydı ülkelere özel algoritmalar kullanılarak şifrelenmeli ve kartın üzerinde o şekilde kayıtlı tutulmalıdır, böylelikle her ülke kendi vizesiyle ilgili bilgileri çözmeli ve ona göre değerlendirme yapmalıdır.

3.Katman – Biyometrik Kimlik Bilgisi

Bu katman olabildiğince güvenli bir alan olarak saklanmalıdır, çünkü kullanıcının biyometrik teşhis bilgilerini içeren katman burasıdır. Buradaki veri kesinlikle şifrelenmiş olmalı ve anahtar sadece havaalanında bulunan biyometrik teşhis üniteleri tarafından bilinmelidir.

Genel olarak, kartta kullanıcı tarafından değiştirilebilecek bir bölge olmamalıdır. Her katman kendisine yapılan atak işlemlerine karşı belli bir denemeden sonra kendini geçersiz hale getirmelidir.

4.2 Biyometrik Tanıma

Günümüzde çok sayıda biyometrik teşhis sistemi bulunmaktadır. Bunlara örnek olarak ses, parmak izi, iris, el geometrisi, damar, dudak, kulak izi ve DNA tanıma sistemlerini verebiliriz. Bu projede kullanıma konu olan metot ise halihazırda polis teşkilatında kullanılmakta olan ve bu durumun oldukça fazla miktarda veriye sahip olduğu parmak ve el izi tanıma sistemidir.

4.3 Akıllı Kart Okuyucuları

Daha önce de belirtildiği üzere, karttan biyometrik bilgilerin okunabilmesi için kullanılacak akıllı kart okuyucuların belli izinleri almış ve güvenli aygıtlar olması gerekmektedir. Bu okuyucular karmaşık yapıda tasarlanmış olmalı ve her üç katmana da erişebilecek düzeyde kriptografik güvenlik modüllere sahip olmalıdır.

Güvenlik Modülü – Genel Amaçlı Okumalar

Bu modül kartta kişiyle ilgili genel bilgilerin bulunduğu katmandaki bilgileri okumak için kullanılacaktır. Bu nedenle daha önceden belirlenmiş bir anahtarla ulaşmak bu bölüm için yeterli güvenliği sağlamış olacaktır.

Güvenlik Modülü - Vize Onaylanması

Bu modül içerisinde vize bilgilerini barındıran ikinci katmandan okuma yapacaktır. Bu katman üzerine kendi vizeleriyle işlem yapmak isteyen her ülkeye açık bir bölüm olmalıdır. Ülke kodu şifrelenmiş olmayan bir veri olduğundan (ya da ilk katmandaki anahtarla şifrelenmiş olduğundan), okuyucu ilgili kayıta ulaşıp, o ülke için geçerli vize kontrolünü yapabilecektir.

Güvenlik Modülü - Biyometrik Eşleme

Bu modül, kendi içerisinde kapalı bir tasarıma sahip olmalı, ve kimlik tespit işlemi son derece gizli yapılmalıdır. Dışarıdan alınacak bir anahtar bu modüle ulaşmak için kullanılabilir.

4.4 Biyometrik Okuyucu

Burada kullanılacak olan biyometrik okuyucu şu anda polis teşkilatında da kullanılmakta olan parmak izi tanıma sistemi olabilir. Bu aygıtın olabildiğinde kullanıcı dostu olmasında yarar vardır, bu sayede kullanıcılar herhangi bir karışıklığa imkan tanımadan gerekli olan kontrolü kısa sürede gerçekleştireceklerdir. Teknik olarak, doğruluğu yüksek bir cihaz olmalı, ve yüksek güvenlikli hatlardan haberleşme yapabilmeleri için akıllı kart okuyucusuna yakın bir yere yerleştirilmelidir. En yüksek güvenliği sağlayabilmek için, akıllı kart okuyucusuyla biyometrik okuyucu bütün kontrolleri kendi içersinde yapan tek bir cihaz olarak üretilmelidir. Bu durumda verilerin dışarı sızma ihtimali en aza indirilebilinir.

4.5 Kapı Modülü ve Alarm

Otomatik açılıp kapanan bir kapı bu sistem için gerekli olan bir diğer cihazdır. Merkezi bir bilgisayardan alacağı işaretle bu kapının açılıp kapanması sağlanacaktır. Kapıya entegre edilmiş ya da dışarıda ayrık duran bir uyarı sistemi de güvenlik sisteminin bir parçası olacaktır. Kapıyla bilgisayar arasındaki iletişim hattı da her türlü saldırıya karşı korunmalı olmalıdır.

4.6 Gümrük Memuru – Arka plan Onaylama Sistemi

Şu anda görev yapmakta olan gümrük memurları, bu sistemden sonra yaptıkları iş bakımından pek bir değişikliğe uğramayacaklardır. Kullanıcının parmak izi, kart sahibiyle karşılaştırıldıktan ve onay alındıktan sonra gümrük memurunun görevi devletten devlete farklı olmakla birlikte önceki sistemle aynı şekilde yürüyebilmektedir.

5. Sistemin Yararları

Daha önce de belirtildiği gibi, elektronik pasaportların ve vizelerin kullanımı, kağıtlar üzerinde daha kolay yapılabilen sahteciliğin önüne geçecektir. Bununla birlikte bu sistem daha başka yararlar da sağlar. Bunlar:

Yüksek güvenlik: Kartın üzerindeki tüm bilgiler fazlasıyla korunmaktadır. Sahibinin kartı kaybetme durumunda, bulan kişinin kartın üzerinde işlem yapsa dahi kartı kullanma ihtimali yoktur.

Kolay uygulama ve güvenilir yapı: Kullanıcının tanınması sadece parmak izinin aygıt tarafından kolaylıkla analiz edilmesiyle sağlanmaktadır. Biyometrik teşhis sistemini daha da güvenilir bir hale getirmektedir.

Taşımada kolaylık: Elektronik pasaportun boyu normal bir kredi kartının aynısıdır. Bu nedenle taşımada herhangi bir zorluk olmayacaktır.

Dışardan gelen ataklara karşı dayanıklılık: Geleneksel kağıt tabanlı dokümanlara göre hasar görme olasılığı çok azdır.

İşlem kolaylığı: İşlemlerin tamamlanması için geçen süre geleneksel sistemlerdeki bilgilerin elle girilmesi için harcanan zamandan daha kısadır.

İnsan kaynaklarından tasarruf: Tüm işlemler otomatik olarak yapılmaktadır. İnsan unsuru yalnızca oluşan bir hata nedeniyle işin içine girmektedir.

6. Geliştirilen Örnek Sistem

Önerilen sisteme ait bir prototipin geliştirilmesi de bu tezin konusudur. Geliştirilen prototipte gerçek hayattaki pasaport ve vize bilgileri basite indirgenmiş ve sistemin çalışmasının gösterimi amaçlanmıştır.

Sistemin genel bir simülasyonu oluşturulduğundan, görselliğe çok fazla önem verilmemiş, genel sistem için en gerekli noktalar prototipe dahil edilmiştir. Ana menüde (bkz. Şekil 6.1) yapılabilecek olan işlemler kayıt ve kontrol olarak sınıflandırılmıştır. Bunları ele alacak olursak:

Şekil 6.1 Ana menü

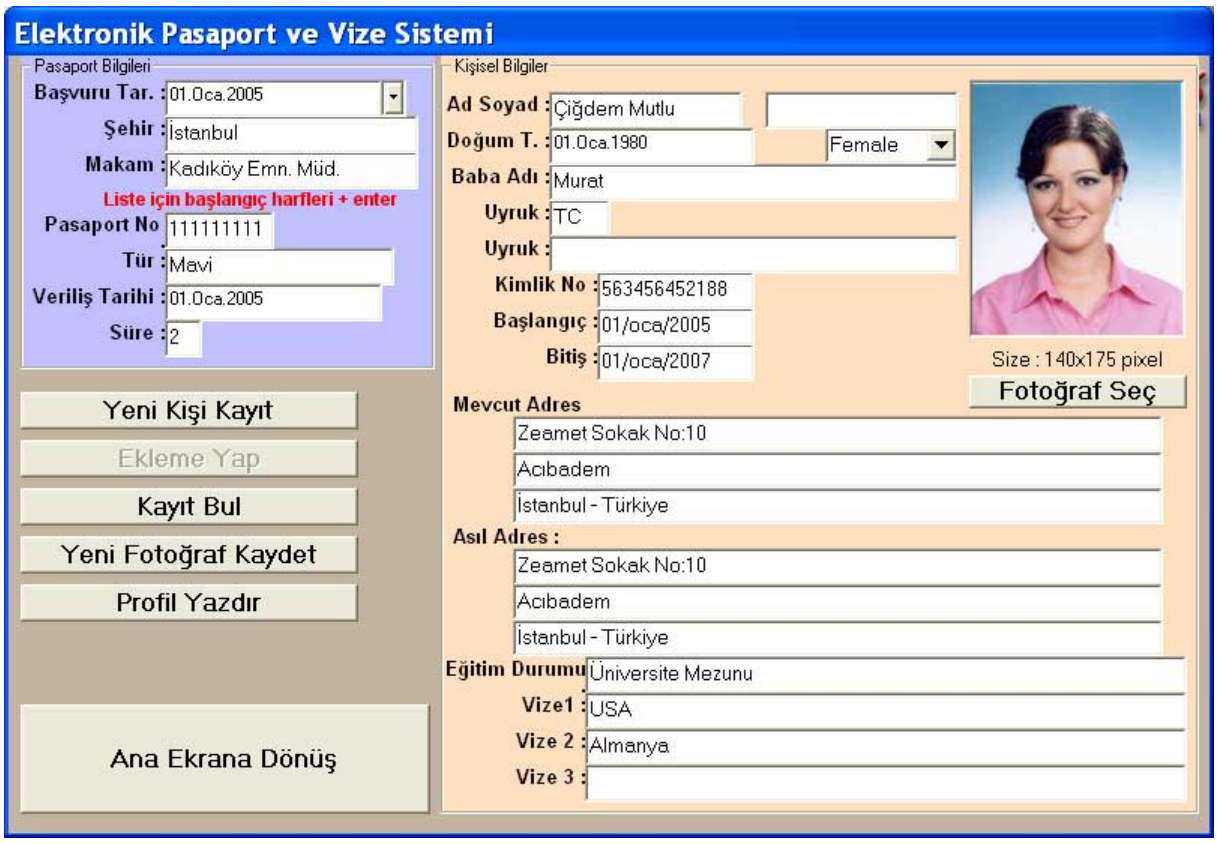
- Kayıt İşlemleri
    - Pasaport Oluştur : Yeni pasaport bilgisinin girildiği bölümdür.
    - Vize Bilgisi Gir : Daha önceden oluşturulan pasaportun üzerinde vize işlemleri yapmak için kullanılır.

- Biyometrik Bilgi Giriş ve Doğrulama : Pasaport sahibine ait biyometrik bilginin sisteme girilmesi ve bu bilginin doğrulanması amacıyla kullanılan bölüm.

- Kontrol İşlemleri
  - Pasaport Kontrol : Önceden tanımlanmış pasaport (akıllı kart) ve biyometrik kimlik bilgisinin eşlenirliğini kontrol eden bölüm
  - Vize Kontrol : Pasaport sahibinin gitmek istediği ülkenin vizesine sahip olup olmadığının kontrol edildiği bölüm
  - Çıkış

Bundan sonraki bölümde ana menüdeki öğeler ayrıntılı olarak ele alınacaktır.

6.1 Pasaport Oluşturma



Şekil 6.2 Pasaport oluşturma

Ekranın sağ tarafında kişinin ayrıntılı nüfus ve adres bilgileri görülmektedir. Klasik pasaport

yapraklarındaki bilgilerden farklı olmayan bu bilgilerin benzerleri tüm bireylerin kimliklerinde de aynen bulunmaktadır. Her bireyin vesikalık fotoğrafı ya daha önce sisteme tanıtılmıştır ya da kayıt esnasında sayısal fotoğraf makinesiyle çekilmektedir. Vesikalık fotoğraf görüntüsünün altındaki fotoğraf seç düğmesiyle sistemdeki fotoğraflardan biri kişi fotoğrafı olarak belirlenir. Fotoğraf veritabanında tutulmak istenirse kodda yapılacak değişiklikle sistem buna uyumlu hale getirilebilinir.

Ekranın ikiye ayrılmasındaki amaç, önerilen sistemde savunulduğu üzere, kişisinin kendisine verilecek ya da erişimi kısıtlanacak bilgilerin daha açık şekilde gösterilmesidir. Burada solda kalan mavi zeminli bölüm emniyet kayıtlarında tutulacak ve kişinin bu bölgedeki bilgilere erişimi kısıtlanacaktır. Her iki bölümdeki alanlara eklemeler yapılabilinir.

Sol alt tarafta kalan düğmeler yardımıyla da arama yapılması, yeni fotoğraf kaydı ya da görüntülenmekte olan kişinin profil bilgilerinin yazdırılması sağlanabilir.

Çıkış tuşuyla ana menüye dönülür.

6.2 Vize Bilgisi Girme

Sistemde vize bilgileri pasaport oluşturma ekranında girilmektedir. Bunun dışında her ülke vize bilgilerinde değişik veriler saklamak isteyebilir, kişiler hakkında notlar tutabilir. Bu gibi durumlarda bu ekrandan vize bilgileri girilebilinir. İlerisi için kullanılabilecek bir bölümdür.

6.3 Biyometrik Bilgi Giriş ve Doğrulama

Bu bölüm iki aşamadan oluşmaktadır. Bunların ilki kişilerin ilk biyometrik bilgilerini alma (bkz. Şekil 6.3) diğeri isi önceden alınmış biyometrik bilginin kontrolüdür (bkz. Şekil 6.4).

Kayıt sırasında parmak izinin görüntüsü alındığında ekranda resmi görüntülenir. Sistem kararlı bir halde resmi onayladığında (ki bu sistemde algılayıcıya üç kez yerleştirip çekildiğinde kararlı bir resim elde edilir) sol taraftaki düğmeleri kullanarak kayıt, tanıma, silme işlemleri yapılabilinir. Parmak izini veritabanındaki kayıtla eşleştirmek için hem kimlik numarası hem de isim bilgileri sorulmaktadır. Bu alanlar istenildiği gibi değiştirilebilinir.

Şekil 6.3 Biyometrik bilgi kayıt

Şekil 6.4 Biyometrik bilgi kontrol

İkinci aşama olan kontrol bölgesinde ise girilen biyometrik bilginin kontrolü yapılmaktadır. Parmak algılayıcıya yerleştirilip kontrol düğmesine basıldığında, sistem resmin ait olduğu kişiyi veritabanından bulup ekrana çıkarmaktadır.

6.4 Pasaport Kontrol

Şekil 6.5 Pasaport kontrol

Pasaport kontrol ekranında kullanıcıdan pasaportunu (akıllı kartını) okuyucuya yerleştirmesi ve ardından da parmağını algılayıcıya koyması istenir. Bunların ardından kontrol tuşuna basıldığında sistem kartın içindeki veriyle kullanıcıdan gelen biyometrik veriyi karşılaştırır ve sonucu ekranda gösterir. Burada yapılan kontrol, kullanıcının olduğu iddia ettiği kişiyle yani pasaport sahibiyle aynı kişi olup olmadığıdır.

Önerilen sistemde bu kontrol sonucunda sonuç pozitif yani veriler eşleşiyorsa kapı açılır, negatifse yani biyometrik veriyle kartın içindeki veri birbirinden farklıysa alarm modülü devreye girerek kontrol mekanizmasını uyarır.

6.5 Vize Kontrol

Şekil 6.6 Vize kontrol

Vize kontrol ekranı da pasaport kontrol ekranına oldukça benzemektedir. Farkı ise akıllı kart yerleştirildiğinde kartın içinde bulunan vize bilgilerinin ekrana basılmasıdır. Böylelikle kullanıcının o an hangi ülkelere seyahat edebileceği ekranda görüntülenmiş olur.

Tüm bu işlemler son kullanıcı odaklı olduğundan kartın içindeki bilgilerin görüntülenmesi gereksiz olmaktadır. Bu bilgilerin görüntülenmesi için sistem geliştiricilerinin kullanacağı basit bir program da yazılmıştır.

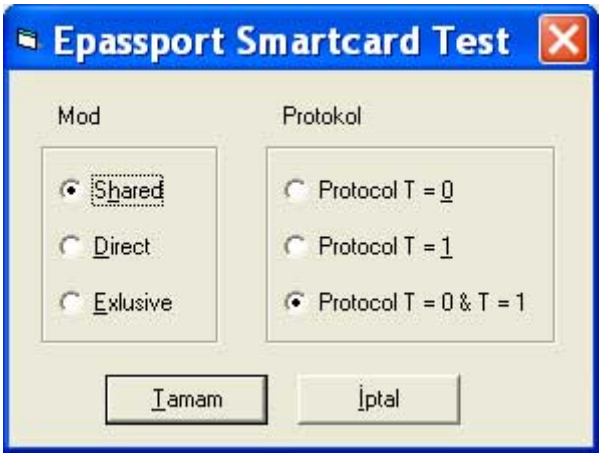
Akıllı kartla iletişimde PC/SC protokolünü kullanan bu programın ekran görüntüleri de aşağıda verilmiştir.

Şekil 6.7' de programın genel şekli görülmektedir. Sisteme bağlı olan okuyucular "okuyucuyu seçin" yazısının hemen yanında yer alan kutuda görülmekte, seçim yapıldıktan sonra hemen altındaki bağlan tuşuyla ilgili okuyucuya bağlanılmakta ve işlemlerin sonucu alttaki büyük yazı kutusunda görülmektedir.

Bağlantı için mod ve tür seçilmesi gerekmektedir (bkz. Şekil 6.8). Bunlar pc/sc protokolünün

özelliği olan ayarlardır. Seçilen akıllı kart türüne göre bunlar da ayarlanabilir.

Şekil 6.7 Akıllı kart test programı



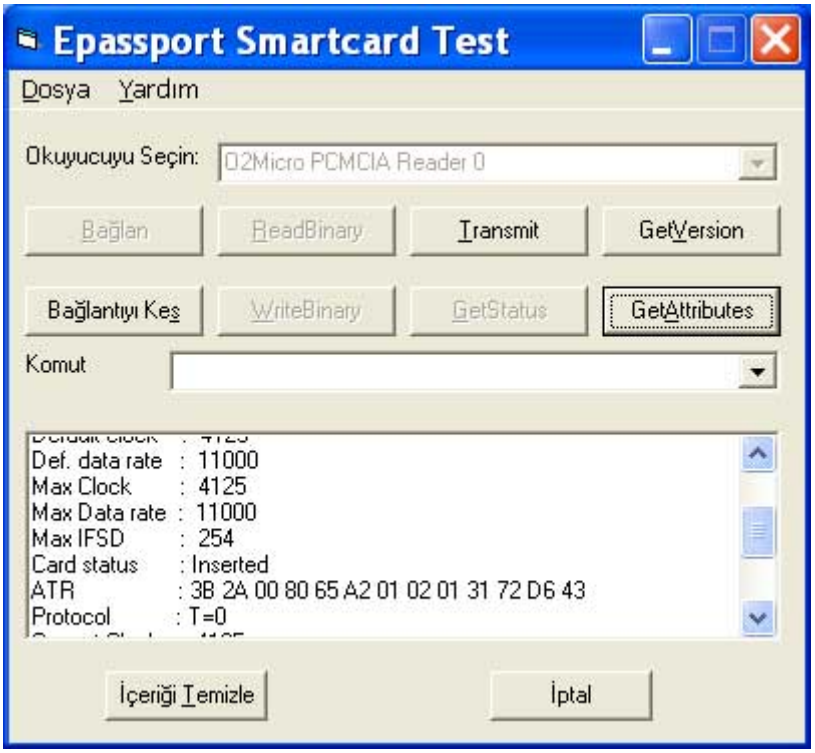
Şekil 6.8 Bağlantı türü seçimi

Ayarlar doğru seçildiğinde okuyucudaki kartla sorunsuz bir bağlantı kurulmuş olur (bkz. Şekil 6.9). Bağlantı gerçekleştikten sonra kartın ATR bilgisi yazı kutusunda belirir ve kartla ilgili son durum da bu bilgiyi takip eder.

Programa bazı hazır komutlar da dahil edilmiştir. Bunlar kartın sürümünü denetleyen "GetVersion" ve kartın özelliklerini görüntüleyen "GetAttributes" komutlarıdır. Standartlaşan

komutlar olduklarından orijinal dillerinde kullanılmışlardır (bkz. Şekil 6.10).

Şekil 6.9 Kurulmuş bağlantı



Şekil 6.10 Hazır komutlar

7. Güvenlik ve Gizlilik Konuları

Akıllı kartların ve biyometrik teşhis teknolojilerinin tanımlama işleminde kullanılacak olması beraberinde güvenlik ve gizlilikle ilgili pek çok soruyu da akıllara getirmektedir. Örnek olarak, "Will smart card know too much about you" [54] ve "Touching big brother - How biometric technology will fuse flesh and machine" [52] makaleleri bu konuda yazılmış makalelerden sadece ikisidir. Bu nedenle güvenlik, bu sistemin en fazla üzerinde durulması gereken konusudur.

Kartta depolanan bilgi her biri üç farklı güvenlik sistemi içeren üç katmanda bulunmaktadır. Bu mekanizma sadece güvenliği en yüksek seviyede tutmakla kalmaz, aynı zamanda veriyi istek dışı ortaya çıkarma ihtimalini de en aza indirmektedir.

Kullanılacak olan okuyucular (akıllı kart ve biyometrik teşhis edici aygıtlar) tamamen özel kontrollerden geçmiş ve her türlü saldırıya karşı korunmalı olarak üretilmeli ve olabildiğince kapalı şekilde çalıştırılmalıdır.

Aynı şekilde, bütün kapılar, okuyucular, ana makine ve diğer onaylama makineleri arasındaki iletişim hatları birbirilerine güvenliği yüksek bir şekilde bağlanmalı ve bu bağlantılarda özel kriptografik algoritmalar kullanılıp sisteme entegre edilmelidir. Bu durumda, bütün sistemin çok sıkı bir şekilde güvenli ve korumalı olması sağlanmalıdır.

Önerilen teknoloji, kişisel bilgileri tıpkı daha önce kullanılmakta olan pasaport gibi taşıdığından ve şüphesiz ki ondan çok daha güvenli olduğundan, kullanıcı bu yeni teknolojiyi kullanmak için herhangi bir tedirginlik duymayacaktır. Beklenen, onların bunu rahatlıkla kabul edip, yeni seyahat kartları olarak biran önce kullanıma geçmeleridir.

8. Sonuç ve Öneriler

Akıllı kartların ve biyometrik okumanın bütünleştirildiği bir kimlik doğrulama sistemi kullanıcıların ve devletin hayatını hissedilir derecede kolaylaştıracaktır. Kart sahibinin kişisel ve gizli bilgilerini kartın üzerinde tutmak ve bu bilgilere erişimin biyometrik özellikler kullanılarak sağlanması sistemin güvenliği konusunda herkesi tatmin edebilecek gerçeklerdir. Akıllı kartlar bugünlerde değişik türdeki banka kartlarından, personel takip kartlarına, ön-ödemeli uygulamalardan iletişim alanlarına kadar pekçok sektörde kullanılan teknoloji haline gelmiştir.

8.1 Bundan Sonra Neler Yapılabilir?

Sistemin genişletilmesi ve geliştirilmesi, kartın farklı katmanlarla zenginleştirilmesiyle mümkün olabilir. Şöyle ki, bugün birçok havayolu şirketi elektronik bilet sistemini devreye sokmuştur ya da sokmak istemektedir [40]. Akıllı kart bu gibi bilgilerin eklenmesi için çok elverişli bir yapıya sahiptir. Ayrıca yüksek kapasiteli havaalanlarında bagaj kontrolü de böyle bir sisteme rahatlıkla entegre edilebilir

Kartın ilk katmanı genel amaçlı bilgi depolama bölümü olduğundan, bu genişletmede düşünülen bilgiler için de bu katman rahatlıkla kullanılabilir. Bu bölüme yazılacak bilet ve bagaj bilgileri her türlü uygulamayla rahatlıkla okunup işlenebilir. Yine tanıma ve onaylama işlemleri üçüncü katmandaki biyometrik bilgilerin teşhisiyle yapılabilir.

Diğer taraftan, bu kart aynı zamanda bir seyahat kimlik kartıdır bu nedenle bunun bir kimlik kartı olmasında bir sorun olamaz. Üzerinde kan grubu, kullanıcının olası alerjileri ya da bunun gibi sağlık bilgilerinin bulunmasında çok yarar olabilir.

Günümüz teknolojisi ve küresel ekonomi göz önüne alındığında bu ya da benzeri bir sistemin kısa sürede uygulamaya konacağı şüphe götürmez bir gerçektir. Aynı zamanda, akıllı kartın bu kadar yaygın oluşu ve herkes tarafından az çok bilinen bir teknoloji olması, onun bu sistem için uygunluğunu ortaya koymaktadır. Akıllı kartların uzmanlarından biri olan Jerome Sviglas şöyle diyor, “Smart kart gerçekten de yüksek taşınabilirliğe, yüksek teknolojiye ve yüksek otomatikleştirilmiş günlük hayat uygulamalarına giriş anahtarıdır.” (The 700 Club Newswatch, 1995). Gelişmiş biyometrik tanıma teknolojisiyle birlikte, “bundan böyle bu gibi cihazları sadece James Bond ya da Star Trek fimlerinde görmeyeceğiz.” (Spence, Recognition Systems Inc.).

Kaynaklar

2002 market review, Biometric Technol. Today, 11 (January 2003) 9–11.

A. Jain, L. Hong, S. Pankanti, (2000), Biometric identi cation, Comm. ACM 43 (2) (February 2000) 91–98.

A. Jain, L. Hong, S. Pankanti, R. Bolle, (1997), An identity authentication system using ngerprints, Proc. IEEE 85 (9) 1365–1388.

A. Jain, R.M. Bolle, S. Pankanti, (1999), Biometrics: Personal Identi cation in Networked Society, Kluwer Academic Publishers, Dordrecht.

A. Jain, S. Pankanti, (2001), Biometrics systems: anatomy of performance, IEICE Trans. Fund. E84-D (7) 788– 799.

A. Ross, L. Hong, S. Pankanti, R. Bolle, (2001), Information fusion in biometrics, in: Proceedings AVBPA'01, Halmstad, Sweden, pp. 354–359.

A.K. Jain, A. Ross, S. Pankanti, (1999), A prototype hand geometry-based veri cation system, Second International Conference on Audio and Video-based Biometric Person Authentication, Washington DC, USA, March 1999.

A.K. Jain, S. Pankanti, S. Prabhakar, A. Ross, (2001), Recent advances in ngerprint veri cation, Lecture Notes Comput. Sci. 2091 182–190.

A.K. Jain, S. Prabhakar, L. Hong, (1999), A multichannel approach to ngerprint classi cation, IEEE Trans. Pattern Anal. Mach. Intell. 21 (4) 348–359.

A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, (2000), Filterbank-based ngerprint matching, IEEE Trans. Image Process. 9 (5) (May 2000) 846–859.

A.K. Jain, S. Prabhakar, S. Pankanti, (2001), Twin test: on discriminability of ngerprints, Lecture Notes Comput. Sci. 2091 211–216.

B. Duc, E.S. Bigun, J. Bigun, G. Maitre, S. Fischer, (1997), Fusion of audio and video information for multimodal person authentication, Pattern Recogn. Lett. 18 835–843.

B. Miller, (1994), Vital signs of identity, IEEE Spectrum 31 (2) pp22–30.

Biometric Systems: Worldwide Deployments, (2002), Market Drivers, and Major Players, Allied Business Intelligence, Oyster Bay, NY.

C. Sanderson, (2002), Information fusion and person verification using speech and face information. Technical Report IDIAP-RR 02-33, Dalle Molle Institute for Perceptual Artificial Intelligence. September 2002.

C.-C. Han, H.-L. Cheng, C.-L. Lin, K.-C. Fan, (2003), Personal authentication using palm-print features, Pattern Recogn. 36 371–381.

Clarke, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues, Information Technology & People, 7, 4, pp 6-37.

D. Gabor, Theory of communication, J. Inst. Electr. Eng. 93 (1946) 429–457.

D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, (2002), Fingerprint verification competition, IEEE Trans. Pattern Anal. Mach. Intell. 24 (3) (March 2002) 402–412.

D.L. Hall, J.L. Llinas, (2001), Multisensor data fusion, in: D.L. Hall, J. Llinas (Eds.), Handbook of Multisensor Data Fusion, CRC Press, USA, 2001, pp. 1–10.

F.H. Adler, (1965), Physiology of the Eye, St. Louis, MO, United States, Mosby.

G. Tomko, (1998), Privacy implications of biometrics—a solution in biometric encryption, in: Proceedings of the English Annual Conference on Computers, Austin, TX, August 1998, pp. 1309–1312.

L G.M. Candea, M.C. Moy, (1997), Sureid a ngerprint-based authentication system for insecure networks, Class project paper for 6857: Network and Computer Security, Massachussetts Institute of Technology, April 1997.

H.C. Lee, E.R.E. Gaensslen, (1991), Advances in Fingerprint Technology, Elsevier, New York, 1991.

J. Daugman, (1999), Biometric decision landscapes, Technical Report TR482, University of Cambridge Computer Laboratory.

J. Daugman, C. Downing, (2001), Epigenetic randomness, complexity, and singularity of human iris patterns, Proc. Roy. Soc. 268 1737–1740.

J. Daugman, (1988), Complete discrete 2d gabor transforms by neural networks for image analysis and compression, Trans. Acoust. Speech and Signal Process. 36 (7) 1169– 1179.

J. Daugman, (1993), High con dence recognition of persons by a test of statistical independence, IEEE Trans. Pattern Anal. Mach. Intell. 15 (11) 1148–1161.

J. Daugman, (1997), How iris recognition works, URL:www.cl.cam.ac.uk/users/jgdl000/irisrecog.pdf.

J. Daugman, (1985), Uncertainty relation for resolution in space, spacial frequency, and orientation optimized by two-dimensional visual cortical lters, J. Opt. Soc. Amer. A 2 (7) 1160–1169.

J. Kittler, J. Matas, K. Jonsson, (1997), M.U. Ramos-Sanchez, Combining evidence in personal identity veri cation systems, Pattern Recogn. Lett. 18 845–852.

J. Kittler, M. Hatef, R.P.W. Duin, J. Matas, (1998), On combining classi ers, IEEE Trans. Pattern Anal. Mach. Intell. 20 (3) 226–239.

J. Phillips, H. Moon, S.A. Rizvi, P.J. Rauss, (2000), The feret evaluation methodology for face-recognition algorithms, IEEE Trans. Pattern Anal. Mach. Intell. 22 (10) 1090–1104.

J.D. Stosz, L.A. Alyea, (1993), Automated system for fingerprint authentication using pores and ridge structure, Department of Defense.

J.G.A. Dol ng, E.H.L. Aarts, (1998), On-line signature veri cation with hidden markov models, in: Proceedings of the International Conference on Pattern Recognition, August 1998, pp. 1309–1312.

J.L. Wayman, (2000), A de nition of biometrics, National Biometric Test Center Collected Works 1997–2000, San Jose State University, pp. 21–23.

J.L. Wayman, (1997), Biometric identi cation standards research, Technical Report, Final Report, San Jose State University, San Jose, CA.

J.L. Wayman, (2000), Fundamentals of biometric authentication technologies, National Biometric Test Center Collected Works 1997–2000, San Jose State University,, pp. 1–19.

J.L. Wayman, (1997), Generalized biometric identi cation system model, in: Proceedings of 31st IEEE Asilomar Conference on Signals, Systems and Computing, Paci c Grove, CA.

J.L. Wayman, (1999), Technical testing and evaluation of biometric identification devices, in: Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, Dordrecht.

L. Coetzee, (1992), Fingerprint recognition, M.S. Dissertation, Faculty of Electronic and Computer Engineering. University of Pretoria.

M. Hartman, (1996), Compact ngerprint scanner techniques, in: Proceedings of the Biometric Consortium Eighth Meeting, San Jose, CA, June 1996.

M. Negin, (2000), T.A.C. Jr., M. Salganico8, T.A. Camus, U.M.C. von Seelen, P.L. Venetianer, G.G. Zhang, An iris biometric system for public and personal use, Computer 33 (2) 70–75.

M. S. Uzun, B. Diri, (2005) "Developing Electronic Passport And VISA System Using Smart Card Technology", INISTA Innovations in Intelligent Systems and Applications, 2005, Yildiz Technical University, Istanbul

M.A. Turk, A.P. Pentland, (1991), Face recognition using eigenfaces, in: Proc. Internat. Conf. Pattern Recognition, Hawaii, pp. 586–591.

N. Ratha, S. Chen, A.K. Jain, (1995), Adaptive Row orientation based feature extraction in ngerprint images, Pattern Recogn. 28 (8) 799–813.

N.K. Ratha, A. Senior, R.M. Bolle, (2001), Tutorial on automated biometrics, in: Proceedings of International Conference on Advances in Pattern Recognition, Rio de Janeiro, Brazil, March 2001.

S. N.P.H. Thian, S. Bengio, J. Korczak, (2002), A multi-sample multi-source model for biometric authentication, Technical Report IDIAP-RR 02-14, Dalle Molle Institute for Perceptual Arti cial Intelligence, April 2002.

P. Verlinde, P. Druyts, G. Chollet, M. Acheroy, (1999), A multi-level data fusion approach for gradually upgrading the performances of identity veri cation systems, Proc. SPIE 3719 14–25.

P.J. Phillips, A. Martin, C.L. Wilson, M. Przybocki, (2000), An introduction to evaluating biometric systems, Computer 33 (2) 56–63.

P.J. Phillips, A.J. O'Toole, Y. Cheng, B. Ross, H.A. Wild, (1999), Assessing algorithms as computational models for human face recognition, Technical Report, Technical Report NISTIR 6348, National Institute of Standards and Technology.

P.J. Phillips, (1999), Support vector machines applied to face recognition, Technical Report, NISTIR 6241, National Institute of Standards and Technology.

R. Chellappa, C.L. Wilson, S. Sirohey, (1995), Human and machine recognition of faces: a survey, Proc. IEEE 83 (5) 705–740.

R. Norton, (2002), The evolving biometric marketplace to 2006, Biometric Technol. Today 11 7–8.

R.M. Bolle, S. Pankanti, N.K. Ratha, (2000), Evaluation techniques for biometrics-based authentication systems (frr), in: Int. Conf. Pattern Recognition (ICPR), Vol. 2, Barcelona.

R.P. Wildes, (1997), Iris recognition: an emerging biometric technology, Proc. IEEE 85 1348–1363.

S. Furui, (1997), Recent advances in speaker recognition, in: J. BigXun, G. Chollet, G. Borgeford (Eds.), Audio and Video-based Biometric Person Authentication, Springer, Berlin, pp. 237–252.

S. Lim, K. Lee, O. Byeon, T. Kim, (2001), Efficient iris recognition through improvement of feature vector and classi er, ETRI J. 23 (2) 61–70.

S. Liu, M. Silverman, (2001), A practical guide to biometric security technology, IT Professional 3 (1) 27–32.

S. Pankanti, R.M. Bolle, A. Jain, (2000), Biometrics: the future of identification, Computer 33 (2) 46–49.

S. Pankanti, S. Prabhakar, A.K. Jain, (2001), On the individuality of fingerprints, in: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), Hawaii, US.

S. Prabhakar, (2001), Fingerprint classi cation and matching using a lterbank, Ph.D. Dissertation, Department of Computer Science and Engineering, Michigan State University.

T. Greene, (2001), Biometric security—practical and adordable! Information Security Regarding Room, Sans Institute.

T. Poggio, F. Girosi, (1990), Regularization algorithms for learning that are equivalent to multilayer networks, Science 247 978–982.

Y. Zhu, T. Tan, Y. Wang, (1999), Biometric personal identification based on iris patterns, National Laboratory of Pattern Recognition (NLPR), Institute of Automation, Chinese Academy of Sciences.

Z. Rhia, (2000), V. Matya's, Biometric authentication systems, Technical Report, FIMU-RS-2000-08, Faculty of Informatics, Masaryk University.

Davies S., (1994), Touching Big Brother, Information Technology & People, 7, 4.

INTERNET KAYNAKLARI

[1] Finnish Ministry of Finance (1996). Electronic Identification Finnish Electronic Citizen Card Smart Chipcard Finland, Internet WWW page, at URL: <http://www.tietotie.fi/vahti/eid.html> (24 Mar. 1997)

[2] Gemplus Limited (1995). Which Smart Card Technologies will you need to ride the Information Highway Safely?, Internet WWW page, at URL: <http://www.dice.ucl.ac.be/~dhem/cascade/scard95.html> (24 Mar. 1997)

[3] http://amp.ece.cmu.edu

[4] http://attrasoft.com

[5] http://biometrics.ag.uq.edu.au

[6] http://biometrics.cse.msu.edu

[7] http://euro.ecom.cmu.edu/resources/elibrary/ectlinks.shtml

[8] http://lebox.vt.edu/users/teastman/pages/otherlinks.htm

[9] http://mambo.ucsc.edu/psl/fanl.html

[10] http://www.acsysbiometricscorp.com

[11] http://www.all-internet-security.com/authentication

[12] http://www.authentec.com

[13] http://www.bioapi.org

[14] http://www.biodigest.com

[15] http://www.bioid.com

[16] http://www.biometricgroup.com/index.html

[17] http://www.biometrics.co.za

[18] http://www.biometrics.org

[19] http://www.biometricsmi.com

[20] http://www.biometrics-today.com

[21] http://www.business.com/directory/computers and software/hardware and accessories/security products/authentication/biometrics/

[22] http://www.cadix.com

[23] http://www.certicom.com/index.php?action=res,ecc_faq

[24] http://www.cybersign.com

[25] http://www.engr.sjsu.edu/biometrics

[26] http://www.findbiometrics.com

[27] http://www.graphcotech.com

[28] http://www.gslis.utexas.edu/palmquis/courses/project98/comvision/facerec.htm

[29] http://www.hh.se/ide/islab/isprojekt.htm

[30] http://www.ibia.org/apibull.htm

[31] http://www.imagistechnologies.com/?source=googleadwords

[32] http://www.infineon.com

[33] http://www.keyware.com

[34] http://www.klm.com, http://www.flypgs.com, http://www.thy.com.tr

[35] http://www.media.mit.edu

[36] http://www.nxsgrp.com

[37] http://www.oss.com/products/biometrics/biosupport.html

[38] http://www.purchasingresearchservice.com

[39] http://www.st.com/stonline/products/support/touchip/index.htm

[40] http://www.tech.purdue.edu/it/resources/biometrics

[41] http://www.umd.edu

[42] http://www.usc.edu

[43] http://www.veridicom.com

[44] http://www.viisage.com

[45] http://www-white.media.mit.edu/vismod

[46] IriScan Inc. (1997). IriScan Inc. Home Page, Internet WWW page, at URL: <http://www.Iriscan.com> (24 Mar. 1997)

[47] Medical Records Systems (1997). Medical Card System, Internet WWW page, at URL: <http://www.sni.net/talos/medical.htm> (24 Mar. 1997)

[48] Recognition System Inc. (1991). The 1991 Sandia Report: A Performance Evaluation of Biometric Identification Devices, Internet WWW page, at URL: <http://www.recogsys.com/articles> (24 Mar. 1997)

[49] Recognition System Inc. (1996). Biometrics In Physical Access Control: Issues, Status and Trends, Internet WWW page, at URL: <http://www.recogsys.com/articles> (24 Mar. 1997)

[50] Recognition System Inc. (1997). Recognition System Inc. Home Page, Internet WWW page, at URL: <http://www.recogsys.com> (24 Mar. 1997)

[51] Rice J. (1997). Veincheck Biometric Home Page, Internet WWW page, at URL: <http://innotts.co.uk/~joerice> (24 Mar. 1997)

[52] Schumberger Limited (1996). Advantages, Smart Cards: Inherent advantages, Internet WWW page, at URL: <http://www.slb.com/et/inherent_advantage.html> (24 Mar. 1997)

[53] Smart Card Forum (1997). Smart Card Forum Home Page, Internet WWW page, at URL: <http://www.smartcrd.com> (24 Mar. 1997)

[54] The 700 Club Newswatch (1995). Biometrics Fact Sheet, Internet WWW page, at URL: <http://www.cbn.org/factsheets/biometrics.html> (24 Mar. 1997)

ÖZGEÇMİŞ

Doğum tarihi	23.02.1981	
Doğum yeri	İstanbul	
Lise	1994-1998	Şişli Yunus Emre Lisesi
Lisans	1998-2002	Doğuş Üniversitesi Mühendislik Fak. Bilgisayar Mühendisliği Bölümü
Yüksek Lisans	2002-2005	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Müh. Anabilim Dalı, Bilgisayar Müh. Programı

Çalıştığı kurumlar

	2002-2005	Doğuş Üni. Bilgisayar Mühendisliği Araştırma Gör.