YMH321 Bilgi Sistemleri ve Güvenliği

Biyometrik Güvenlik Araçları

Bölüm - 10

Prof. Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıkları

- Güvenlik Araçları
- Bilişim Suçları
- Bilgi ve Bilgi Güvenliği
- Sonuç
- Sorular
- Kaynaklar

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Biyometrik tanıma, datayı kodlama veya şifreleme /deşifreleme için vücut özelliklerini kullanan bir süreçtir. Parmak izi, retina ve iris, avuç içi izi,yüz yapısı ve ses tanıma günümüzde sıkça araştırılan biyometrik tanıma teknikleridir. Bu özellikler her şahsa özel olduğu için biyometrik yöntemler hırsızlık ve dolandırıcılığa kısmen de internet üzerinde ticarete cevap olabilecektir.Bu yeni teknolojinin özelliği parola veya PIN numarası yerine çalınamayan kaybolmayan veya yeniden oluşturulamayan biyometrik özelliğin kullanılmasıdır. Bir endüstri uzmanına göre, Kullanıcının erişim haklarına sahip olabilmek için onun parmağını kesmedikçe, biyometrik tanıma erişim kontrolü için mükemmel bir yöntemdir.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

- Tablo 8.1 ‘de ifade edildiği üzere biyometrik yöntemleri kullanmak için oldukça fazla seçenek bulunmaktadır.Tablo 8.1 ‘de verilmiş olan biyometrik yöntemler bugüne kadar kararlılığı test ve kabul edilmiş olan yöntemlerdir.Bunlar için daha doğru bir ifade kullanılması gerekirse bu yöntemler bilinen biyometrik yöntemlerdir.Bu yöntemlerin ötesinde halihazırda araştırma aşamasında olan bir çok biyometrik yöntemde bulunmaktadır.Bunlar arasında en dikkat çekici olanlarından birisi insanların kulak yapılarını algılayıp tanıyan sistemlerdir.Bu da göstermektedir ki insanların kendilerine has olan bütün uzuvları biyometrik tanımlayıcı olarak kullanılabilir. Bu da biyometrik sistemlerin ana amacını oluşturmaktadır.

BİYOMETRİK GÜVENLİK SİSTEMLERİ

Biyometrik Yöntem	Hata Oranı
Retina Tarama(ışığı ileten damarlar)	1:10.000.000
İris Tarama(göz rengini veren bölge)	1:131.000
Parmak İzi Tarama	1:500
El Geometrisi Tarama	1:500
İmza(Yazı Yazma) Tarama	1:50
Ses Tarama	1:50
Yüz Tarama	Veri Yok
Vascular Patterns	Veri Yok

Tablo 8.1. Biyometrik Yöntemlerin hata oranları

Biyometriğin Tarihçesi

- Bugünün biyometrik tanıma süreçleri geçmişteki bazı yaygın biyometrik tekniklerinden türetilmiştir. Doğal olarak en yaygın olan ve suçluların tespitinde, çalışanların lisanslarında kullanılan parmak izidir. Bu süreç, yazılı kopya üzerinden manuel olarak haftalarca süren bir inceleme sonucunda bazen de yanlış sonuçlar vererek gerçeklenirdi. Bilgisayar teknolojisinin gelişmesiyle, bazı kuruluşlar, arşivlerini elektronik olarak tutmaya ve parmak izi eşleştirme sürecini daha hızlı ve doğru olarak yapmaya başladılar. Parmak izi tanıma sürecinin sonraki adımı sadece kişileri tanımak değil aynı zamanda belirli yerlere erişimlerini denetlemektir. Bu teknik ile birlikte biyometrik tanıma koddaki bilginin çözümlenmesiyle, kişilerin belirli yerlere girişlerini sağlayacak biyometrik parola olarak kullanılmaya başlamıştır.

Biyometrik Tanıma Nasıl Çalışır?

- Tanıma, iletilen veya bir veritabanında saklanan bilginin anlaşılmasına yardım eden bir matematiksel süreçtir, ve bir kripto sistemini belirleyen üç ana faktör vardır, matematiksel süreç veya algoritmanın karmaşıklığı, mesajı anlamakta kullanılan tanıma özelliğinin uzunluğu, anahtar yönetimi olarak bilinen anahtarın emniyetli saklanması. 68 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. Algoritmanın karmaşıklığı, ters işlem ile doğrudan bağıntısı olması nedeniyle önemlidir. Bazıları tanımanın bu alanının kolayca kırılabileceğini düşünür, bununla birlikte kripto sistemleri saldırılara karşı zafiyet olan en az bu üç faktörü içerecek şekilde iyi tasarlanır.

Biyometrik Tanıma Nasıl Çalışır?

- Mesajı anlamakta kullanılan tanıma anahtarının uzunluğu, tanıma sürecinin ikinci en önemli parçasıdır. Daha kısa olan anahtarlar brute force saldırılarına karşı daha zayıftır. Bunun anlamı bir kişinin hesaba girebilmek için bütün mümkün parola kombinasyonlarını denemesi demektir.
- Parola veya PIN numarası gibi biyometrik olmayan tanıma süreçlerinde, anahtarın uzunluğuna bağlı olarak enformasyon yetkisiz kişilerce erişilmeye karşı güvensizdir.Örneğin üç karakterlik bir şifre, mümkün olan permutasyonlar bakımından on karakter uzunluğundaki bir şifreye göre daha zayıftır. Mevcut bilgisayar gücü ile, 64 karakter uzunluğundaki bir anahtarın bulunabilmesi için gerekli permutasyonlarının hesabı dört yüz yıl alabilecektir Biyometrik tanıma, personel tanımlayıcısı ile normal anahtar karakterlerinin yerlerini değiştiren bir standart karakter uyuşturma yapar. Bu biyometrik anahtar olmadan veriye erişilemez.

Biyometrik Tanıma Nasıl Çalışır?

- Anahtarların emniyetli olarak saklanması tanıma sürecinin en zayıf yönüdür. En kolay olarak gözüken saklama süreci en zor işlemdir çünkü parola veya PIN numarası kaybolabilir veya çalınabilir. İyi tanıma özelliği çok uzun olan ve hatırlanamayan parolaların, kağıtta akıllı kartlarda, veya disketlerde saklanarak yetkisiz kişilerin erişiminin önlenmesidir. Biyometrik tanıma sistemleri anahtarın kaybetme veya çalınma olmadan taşınmasını mümkün kılar.

Örüntü Tanıma Teknikleri

- Örüntü Tanıma, gereksiz detaylardan arındırılmış olan giriş datasından çıkartılan anlamlı özellikler yardımıyla teşhis sınıflarına ayrılan verinin sınıflandırılmasıdır.
- Görüntü, geçici mantıksal gibi değişik örüntü sınıfları mevcuttur. Geniş bir yorumlama ile örüntü tanımayı birçok akıllı faaliyette kullanabiliriz. Tek bir teorisi olmayan örüntü tanıma geniş çaptaki problemin çözümünde kullanılabilir. Bununla birlikte birkaç standart model aşağıda özetlenmiştir.

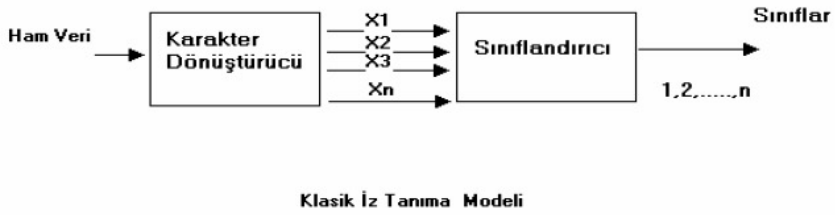
Örüntü Tanıma Teknikleri

- İstatistiksel veya bulanık örüntü tanıma
- Sentetik veya yapısal örüntü tanıma
- Bilgi tabanlı örüntü tanıma(Yapay sinir ağları, Uzman sistemler)
- Burada istatistiksel yaklaşım ile kendimizi sınırlandıracağız. Örüntü tanımayı, bir girişi bir sınıfa atayan sınıflandırma olarak göreceğiz.. Problemi böyle sınırlamakla ihtiyaçlarımızı gören bazı yararlı teknikleri geliştirecek ve aşağıdaki temel kavramlar üzerinde yoğunlaşacağız:
- Sınıflandırma
- Özellikler
- Özellik vektörleri
- Standart sınıflandırma modelleri

Sınıflandırma Modeli

- Görsel örüntü ile çalıştığımızı ve Roman alfabesinin 26 harfini temsil eden örüntüyü bildiğimizi kabul edelim. Buradan örüntü tanıma problemini, giriş verisini 26 sınıftan birisine atama olarak ifade edebiliriz.(Şekil 8-1) Genelde girişin sınıf 1 veya Sınıf 2 veya .. veya …Sınıf c 'ye ait olduğu şeklinde kendimizi sınırlayacağız..

Şekil 8-1. Harflerden oluşan Görsel örüntü



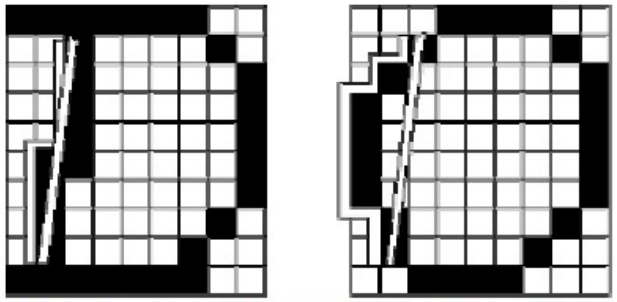
Şekil 8-2. Örüntü(iz) tanıma modeli

Sınıflandırma Modeli

- Daha ileriye giderek, görsel girişi sayısal hale getirmek için bir kamera kullandığımızı ve bir karakteri parlaklık değerlerinin dizisi olarak ayrıştırdığımızı kabul edelim. Bilgisayar bu veriyi 70 Dr.İ.SOĞUKPINAR G.Y.T.E. Bil.Müh.Böl. nasıl sınıflandıracaktır. Belli bir yaklaşım, girişi, her bir sınıf için standart bir örüntü ile karşılaştırmak ve en iyi uyuşan sınıfı seçmektir. Bu yaklaşımdaki açık problem neyin karşılaştırılacağı ve uyuşmanın mertebesini ölçmenin söylenmeyeceğidir.(Şekil 8-2.) Aynı sınıfa ait olan girişlerin, farklı sınıflardaki örüntüler arasındaki farklılığa göre değişkenliği örüntü tanıma problemlerini böyle karmaşıklaştırır. Bu problemin üstesinden gelmenin bir yolu karakteristik özelliklerin araştırılmasıdır.

Özellikler

- Bir nesne veya bir olayı sınıflandırmanın tek yolu onun karakteristik özelliklerinin veya belirleyici niteliklerinin ölçülmesidir. Örneğin yazılı bir harfi sınıflandırmak için onun alan ve çevresini bilmek faydalı olacaktır. Onun alanının çevresinin karesine oranı ile onun sıkılığını ölçebilirdik.Onun yatay eksene göre üst ve altta kalan kısımlarının alanlarını karşılaştırarak simetrikliğini ölçebiliriz.(En iyi ölçmenin simetriklik olduğu düşünülebilir.)
- Bazı özellikler önemli küçük farklara duyarlı olabilir. Örneğin Şekil 8-3'te gösterilen "D" harfini "O"'dan ayırt etmek için sol tarafın düzlüğü ölçülebilir, belki de düz çizgi farkının yay uzunluğuna oranı ölçülebilir Açıkçası, çözülmesi gereken önemli bir özellik olan belirleyici niteliklerin tasarımı bir bilimden çok sanattır.



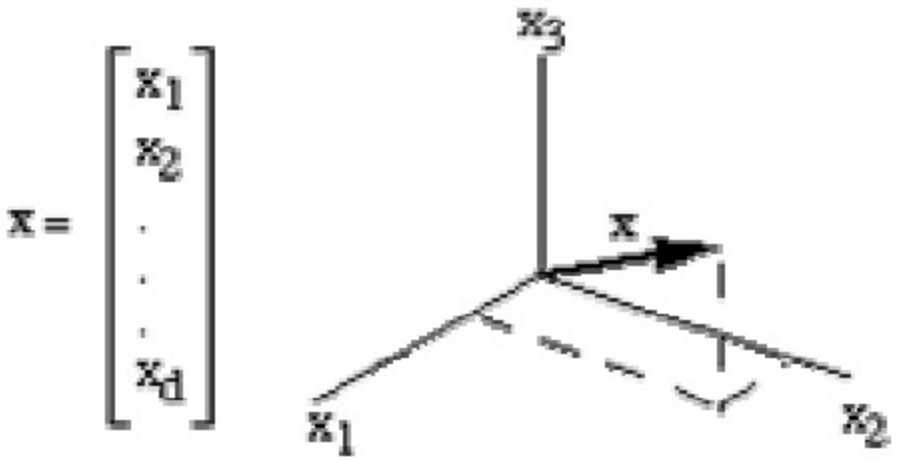
Şekil 8-3: D ve O harflerine ait görsel veri

Belirleyici Özellik Vektörleri

- Herhangi bir nesne veya olayı sınıflandırmak için sıkça belirleyici özelliklerin sabit bir kümesi elde edilir. Örneğin her zaman,.
- x1 = alan
- x2 = çevre
- ...
- xd = yay uzunluğu / Düz çizdi uzaklığı her zaman ölçülebilir.
- Bu durumda, belirleyici özellik kümesini, x belirleyici özellik vektörü olarak düşünebiliriz, burada
- x, d boyutlu bir sütun vektörüdür. Şekil 8-4 de gösterilmiştir.

Belirleyici Özellik Vektörleri

- Benzer olarak, x'i d boyutlu belirleyici özellik uzayında bir nokta olarak düşünebiliriz.



Şekil 8-4: Özellik vektörü

Standart Sınıflandırma Modelleri (*Klasik Model)*

- Aşağıdaki klasik model örüntü tanıma için önde gelir.

- Belirleyici özellik çıkartıcı olarak adlandırılan bir sistem veya program, bir özellik vektörü olan x'in elemanlarına karşılık gelen belirleyici özellikleri x1, x2, ..., xd olan d sayısal kümesini belirlemek için ham veriyi işler. Sınıflandırıcı denilen bir sistem veya program, x'i alır ve Sınıf 1 sınıf 2 , , sınıf c 'den birine atar.

Standart Sınıflandırma Modelleri (*Klasik Model)*

- Belirleyici özellik çıkartıcının tasarımı çoğunlukla probleme bağlıdır. İdeal belirleyici özellik çıkartıcı aynı sınıftaki bütün örüntüler için aynı x özellik vektörünü, farklı sınıftaki örüntüler için ise farklı özellik vektörünü üretmelidir. Pratikte, farklı girişler, belirleyici özellik çıkartıcı tarafından farklı özellik vektörü üretilmesin sağlar, fakat sınıf içindeki değişkenliğin sınıf arasındakine göre küçük olmasını bekleriz.

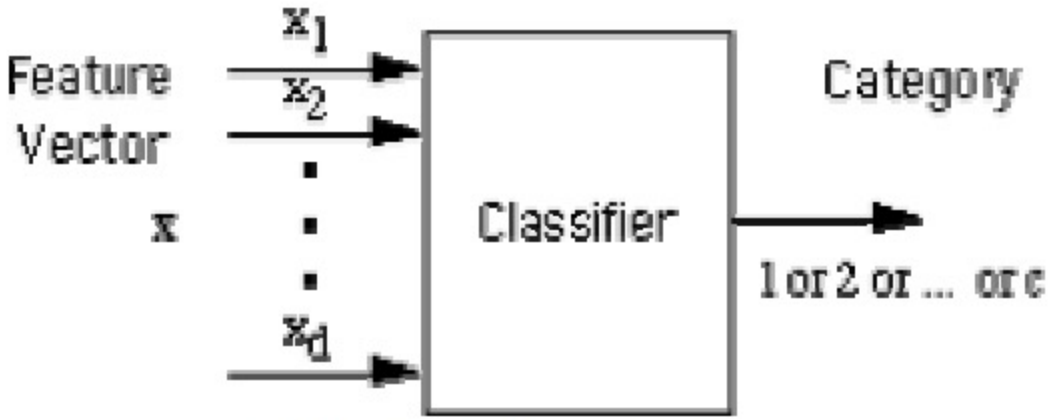
Standart Sınıflandırma Modelleri (*Klasik Model)*

- Bu noktada, belirleyici özellik çıkartıcının tasarımcısının yapabileceğinin en iyisi ile işini tamamladığını kabul ederiz, ve özellik vektörü örüntüleri ayırt etmek için gerekli olan bilgiyi içerir. Verilen belirleyici özellik kümesinden sınıflandırıcıyı tasarlamak bizim işimizdir.

Basit Sınıflandırıcılar

Bir sınıflandırıcı tasarlama yaklaşımı için en az iki yol vardır:

- Makul bir çözümün varsayımı ve onu probleme uydurulması
- Problemin matematik modelinin çıkartılması ve en iyi sınıflandırıcının üretimi



Şekil 8-5: Basit sınıflandırıcı

Basit Sınıflandırıcılar

Daha çok sezgisel olan ilk yöntem pratikte daha çok kullanılır, ve bizim ele alacağımız yaklaşımdır. Basit bir çözüm ile başlayacağız, karakteristiklerinin analizi, zayıf yönlerin belirlenmesi, ve sadece gerektiği şekilde karmaşıklaştırma.. Bu bölümde aşağıdaki kavramlar üzerinde duracağız:

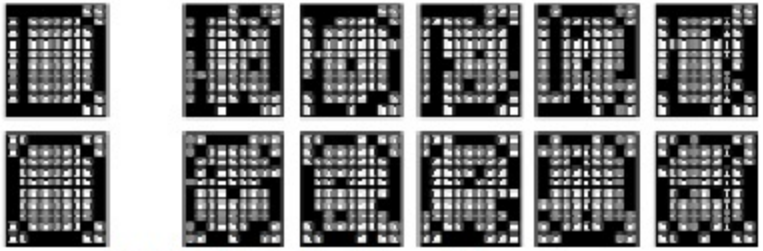
- Şablon Uyuşturma(Template matching)
- En az mesafe sınıflandırıcılar(Minimum-distance classifiers)
- Metrikler(Metrics)
- İç Çarpımlar(Inner products)
- Doğrusal farklılıkların anlaşılması(Linear discriminants)
- Karar sınırları(Decision boundaries)

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma örüntü sınıflandırma için doğal bir yaklaşımdır. Örneğin Şekil 8-6'da gösterilen gürültülü "D" ve "O" yu düşünelim. Gürültüsüz versiyon şablon olarak sol tarafta gösterilmiştir. Gürültülü örneklerin birisini sınıflandırmak için, onu iki şablon ile karşılaştırmak gerekir. Bu işlem aşağıdaki yöntemlerden birisi ile yapılabilir:
- Uyuşmaların miktarını say(uyuşan siyahlar siyah, uyuşan beyazlar ise beyaz).
- En fazla sayıda uyuşan sınıfları ayıkla. Bu en fazla karşılıklı ilişki yaklaşımıdır.
- Uyuşmayanların miktarını say (Siyah yerde beyaz, beyaz yerde siyah olmalı). En az sayıda uyuşmayanların olduğu sınıfları ayıkla. Bu en az hata yaklaşımıdır.

Şablon Uyuşturma (Template Matching)

- Şablon uyuşturma , eğer farklılıklar sınıf içinde kalırsa iyi çalışır. Açıkça, bu örnekte karakterlerde öteleme, dönme, kırpma, çarpıklık, genişleme veya, büzülme gibi başka bozukluk olmadığı için yöntem çalışır. Yöntem bütün problemlerde çalışmayacaktır fakat uygun olduğu zaman çok verimlidir. Aynı zamanda kullanışlı şekilde genelleştirilebilir.



Şekil 8-6: Şablon Uyuşturma

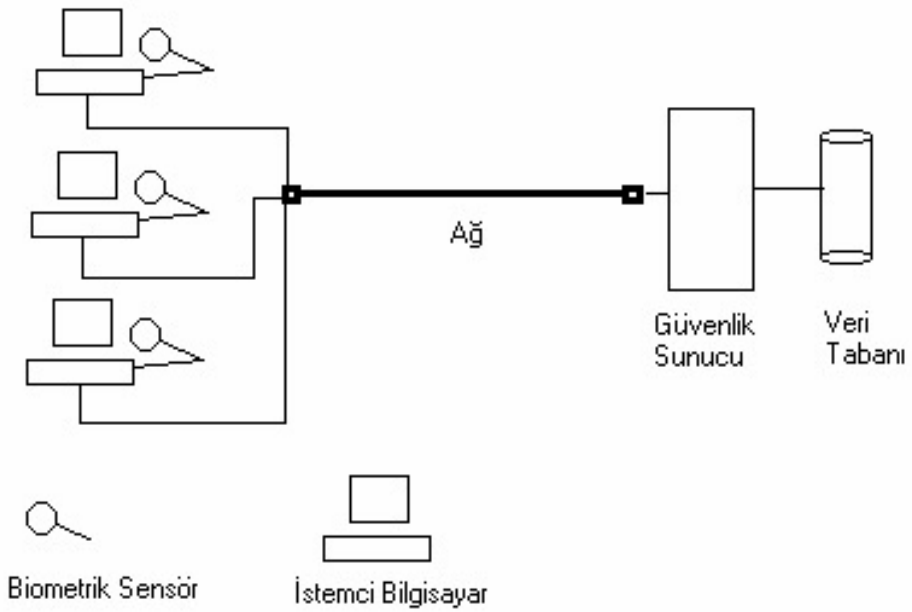
Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

- Şimdiye kadar ki bölümlerde biyometrik yöntemlerin genel çalışma prensiplerinden öte bu tür sistemlerin çalışabilmeleri için nasıl bir fazladan donanıma ihtiyaç duyduklarını anlatıldı.Örneğin bir parmakizi tanıma sisteminde her istemci için bir CCD kamera içeren sensöre ihtiyaç vardı. Bahsedilen sensörlerin içeriklerinin farklı olmasına rağmen yaptıkları iş aynıdır. Bütün biyometrik sistemlerin kurulumu için istemci başına bir sensör gerekmektedir.Daha sonra buradan okutulan bilgiler tasarlanan sistemin mimarisine bağlı olarak işletilirler. Şekil 8-22'de bir biyometrik sisteme ait kuramsal çizim yer almaktadır.

Biyometrik Sistemlerin Kuramsal Tasarım Yöntemleri

Biyometrik sistemlerin tasarımı için uygulanan iki model vardır.

- On-line Model
- Off-line Model



On-line Model

- On-line model yapısında, kullanıcı okunması gereken biyometrik parametresini sisteme okutturur. Sistem almış olduğu biyometrik parametreleri eğer gerekliyse şifreleyerek ağ üzerinden güvenlik parametrelerinin tutulduğu sunucuya gönderir. Sunucu bu parametreleri veritabanı içerisindeki bilgilerle karşılaştırır. Eğer kullanıcı sisteme kayıtlı biriyse sisteme giriş izni gönderir. Kullanıcı tanımlanamadıysa sistem giriş izni vermez. Günümüzde on-line sistemler kullanılmaktadır.

On-line Model

- On-line bir sistemde önemli olan nokta biyometrik bilgileri okuyan sensörlerin sunucuya çok güvenli bir şekilde bağlanmaları gerekmektedir. Bunun için ya sensörler ve sunucu arasında güvenli bir yol tayin edilmelidir yada bilgiler yukarıda bahsedildiği üzere çok iyi şifrelenmiş olarak gönderilmelidir.Bilgilerin herhangi bir nedenden dolayı yetkisiz insanların eline geçmesi sistemin büyük bir zaafa uğramasına sebep olabilir. Öyleyse parametreler öyle bir şekilde şifrelenmeli ki bu parametreler bir şekilde elde edilse bile kullanılamamalılar

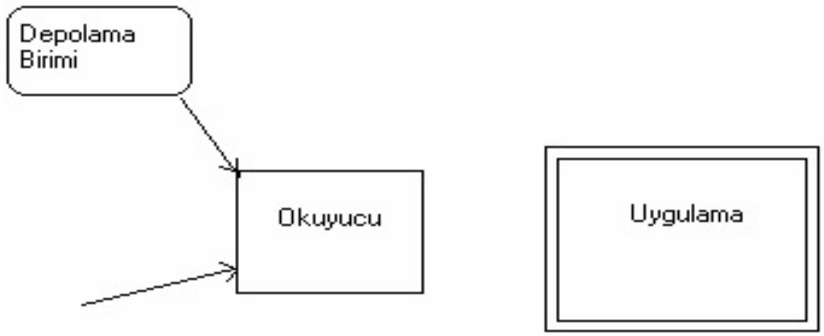
On-line Model

Off-line Model

- Off-line sistemlerde ,On-line sistemlerde olduğu gibi gerçek zaman bir doğrulama işlemi yapılmaz. Bunun için gerekli olan bir manyetik kart gibi aparatlar kullanmaktır. Kullanıcıya ait olan bilgiler bu kart üzerinde tutulurlar. Kullanıcı sisteme girmek istediği zaman bu kartı kullanır. Bu tür sistemlerde güvenlik tamamen kullanıcının inisiyatifindedir. Kendisine verilmiş olan depolama aygıtını çok iyi korumak zorundadır. Tersi bir durumda sistemin güvenilirliğinden söz etmek gerçekçi olmayacaktır.

Off-line Model

- Bu sebeplerden dolayı off-line bir sistem tasarlanırken güvenlik açısından üzerinde çok daha fazla düşünülmesi gereklidir.



Biyometrik Tanıma Teknikleri

Bu gün birçok biyometrik tanıma uygulaması vardır. Aşağıda bunların türleri verilmiştir.

- Parmak izi tanıma
- Optik Tanıma
- Yüz Yapısı Tanıma
- Ses Tanıma
- İmza Tanıma
- Yazma Ritmi Tanıma
- Toplardamar İzi Tanıma
- Avuç içi izi
- Kulak Şeklinden tanıma

Sonuç

Sorular

Kaynaklar