BİYOMETRİK GÜVENLİK SİSTEMLERİ

Rüya ŞAMLI, M. Erkan YÜKSEL
İstanbul Üniversitesi Bilgisayar Mühendisliği
Avcılar , İstanbul

Bu sunumda...

- Giriş
- Biyometrik Ölçüler
- Biyometrik Sistemler ve Özellikleri
- Biyometrik Sistem Çeşitleri
- Parmakizi Tanıma
- DNA Tanıma
- Yüz Tanıma
- İris Tanıma
- El Geometrisi Tanıma
- İmza Tanıma
- Biyometrik Sistemlerin Diğer Yöntemlerle Karşılaştırılması
- Sonuç

GİRİŞ

- Bir bilginin gizli olmasından kastedilen, bilginin tamamen gizli tutulması değil, iletilmesi amaçlanan kişiye bozulmadan, değiştirilmeden, başka birisinin eline geçmeden ulaşması demektir.

- Bir bilgi, iletilmesi gereken kişi için gizli bir bilgi değilken, 3. şahıslar için gizli bir bilgidir.

- Bilgi gizliliği için kimlik doğrulaması oldukça önemlidir.

- Gönderilecek bilgi istenen kişiye değil de başka birisine gönderilirse istenmeyen, beklenmeyen sonuçlar doğurabilir.

- Bu yüzden geliştirilen kimlik doğrulama yöntemleri temelde bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç kısımda incelenebilir.

Bilgi Temelli Kimliklendirme

- Bilgi temelli kimliklendirmede kullanıcılar ve sistem yöneticisi kullanıcı adı, şifre veya PIN denilen gizli bilgilere sahiptir.

- Kullanıcının girdiği bilgiler ile sistemin veritabanındaki bilgiler eşleşirse sistem yöneticisi tarafından sisteme giriş yapan kişinin doğru kişi olduğu anlaşılır.

- Bu sayede kullanıcının yapmak istediği işlemler kolayca gerçekleştirilebilir.

- Bu tip sistemlerin en büyük dezavantajı kişinin kullanıcı adı - şifresinin ya da PIN numarasının başka biri tarafından kolaylıkla elde edilebilecek olmasıdır.

- Bunun dışında kullanıcının şifresini unutma ihtimali de büyük bir dezavantajdır.

Aidiyet Temelli Kimliklendirme

- Bu yöntemde kullanıcılar genelde anahtar, rozet veya manyetik kart gibi eşi olmayan ve kendileri ile bütünleşen bir objeye sahiptirler.

- Sisteme bu obje ile giriş yaparlar.

- Objenin içerisinde sisteme giriş yapanın sözkonusu kişi olduğunu doğrulayacak bilgiler mevcuttur.

- Ancak bu yöntem de bilgi temelli yöntemler gibi pek çok dezavantaja sahiptir. Kişinin sahip olduğu eşyası, sürekli olarak çalınma, unutulma, kaybolma gibi tehlikelerle karşı karşıyadır.

BİYOMETRİK SİSTEMLER

- Biyometrik sistemler kişilerin herhangi bir bilgi ya da objeye sahip olmadan sadece kendilerini kullanarak sisteme giriş yapmasını sağlayan güvenlik sistemleridir.

- Biyometrik sistemlerin en basit şekilleri ile binlerce yıl öncesinden beri kullanılmaktadır.

- 19. yüzyılda kriminoloji araştırmacılarının insanların fiziksel özellikleri ve karakteristiklerin suça eğilimleri ile bir ilgisinin olup olmadığını araştırmaları bu alana olan ilgiyi arttırmıştır.

- Ortaya çıktığı andan itibaren biyometrik incelemelerin boyutu ve çeşitliliği artmış, pek çok biyometrik sistemi yerini almıştır.

BİYOMETRİK ÖLÇÜLER

- Biyometri uygulayıcılarının amacı kişilerin kimlik ispatı için, yanlarında herhangi bir şey taşımak ya da bir bilgiyi hatırlamak yerine; bireyin kopyalanması ya da taklit edilmesi imkansız olan kendine ait özelliklerini kullanmalarını sağlamaktır.

- Kimlik belirleme işlemi, fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir.

- Biyometrik sistemlerin oluşturulabilmesi ve kullanılabilmesi için bazı ölçüler kullanılmalıdır.

- Bu ölçülere biyometrik ölçüler denir.

- Bu ölçülerin şifrelerde kullanımı için INCITS (International Committee for Information Technology Standarts- Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur.

BİYOMETRİK SİSTEM ÇEŞİTLERİ

- Biyometrik sistemler, temel olarak fiziksel (pasif) ve davranışsal (aktif) sistemler olmak üzere 2 gruba ayrılır.

- Fiziksel biyometrik sistemler :

  - parmakizi
  - el geometrisi
  - yüz
  - ses
  - iris
  - retina

  gibi kişide bulunan, diğer kişilerden ayrılmasını sağlayan sabit fiziksel özellikler üzerine kurulmuştur.

BİYOMETRİK SİSTEM ÇEŞİTLERİ

- Davranışsal biyometrik sistemler ise :

  – imza
  – yazı dinamiği
  – konuşma esnasındaki dudak hareketleri
  – yürüyüş şekli

  gibi belli bir zamanda belli amaçlar için gerçekleştirilmiş ve herkesin birbirinden farklı olarak gerçekleştirdiği davranışlar üzerine kurulmuştur.

Fiziksel Biyometrik Sistemler - Parmakizi Tanıma

- Parmak izi en fazla kullanılan biyometrik bilgilerden biridir.
- Ortaya çıktığı 1960'lı yıllardan beri parmak izi tanıma sistemlerinde yazılım ve donanım alanında büyük ilerlemeler kaydedilmiştir.
- Bir otomatik parmakizi tanıma sisteminde (OPTS) parmakizi tanıma genellikle parmakizinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır.
- Günümüzde en çok polis tarafından kimlik tespitinde ve pasaport başvurularında da kullanıcıdan alınan parmak izidir.

Fiziksel Biyometrik Sistemler - Parmakizi Tanıma

- Parmakizi tanıma sistemlerinin en önemli sorunu, taklit parmakizlerinde sistemin yanılmasıdır. Parmakizi taklidi zor olsa da imkansız değildir.

- Diğer bir sorun da bazı kişilerin deri hastalıkları, organ eksikliği, yanma gibi sebeplerden ötürü parmak izlerinin bulunmamasıdır.

- Parmakizi taklitleri, parmakizinin alındığı kişinin o anda yaşıyor olduğunu kanıtlayacak araçlar kullanılması ile çözülebilirken, diğer sorunun çözümü olmadığından bu tip kişilerde bu yöntem kullanılamaz.

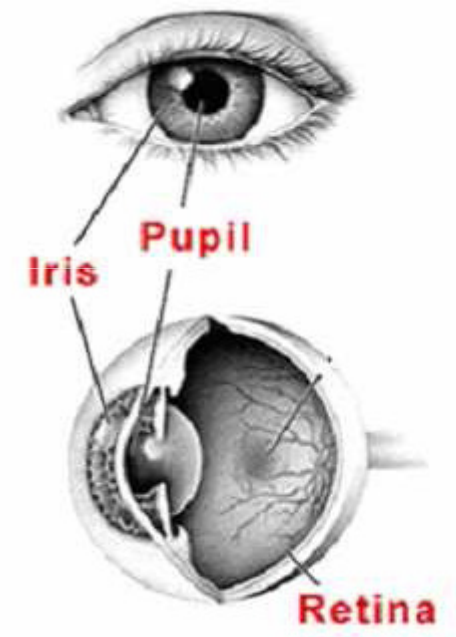
Fiziksel Biyometrik Sistemler - DNA Tanıma

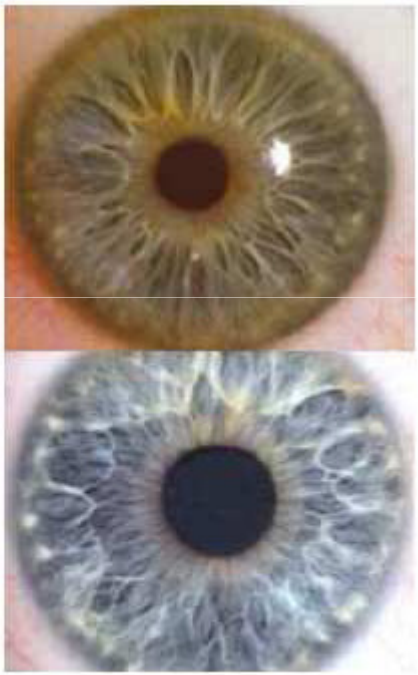
- DNA tanıma günümüzde en güvenilir kimlik doğrulama yaklaşımlarından biridir.
- Kişinin saç, kan veya diğer herhangi bir biyolojik materyali ele alınıp incelenir.
- Yöntemde hücre nukleuslarındaki kromozomlarda saklanan DNA molekülleri kullanılmaktadır. DNA moleküllerinin dizilim eşleşmesine göre doğruluk kontrol edilir.
- Doğruluğu çok yüksek bir yöntem olmasına rağmen diğer yöntemlerdeki gibi dezavantajları mevcuttur.
  - Diğer biyokimyasal ve kimyasal analizlerde olduğu gibi DNA analizinde de yöntemin doğruluğu örnek kalitesine bağlıdır.
  - Örneklerin karışması, kirletilmesi gibi örnek kalitesini düşüren durumlarda yöntemin başarısı da düşmektedir.
  - DNA analizi diğer biyometrik teknikler ile karşılaştırıldığında maliyeti yüksek bir tekniktir.
  - İşlem süresinin 24 saat gibi bir zaman gerektirmesi bu yöntemi bazı durumlarda elverişsiz hale getirmektedir.

Fiziksel Biyometrik Sistemler - Yüz Tanıma

- Özellikle son 10 yıldır cazibesini artırmıştır.
- Askerî, ticarî ve yasal uygulama alanları artmaktadır.
- Yüz işleme ile ilgili işlemler yüz tanıma, yüz takibi, poz kestirimi, yüz ifadesi analizi şeklinde gruplandırılabilir.

Fiziksel Biyometrik Sistemler - İris Tanıma





Fiziksel Biyometrik Sistemler - İris Tanıma

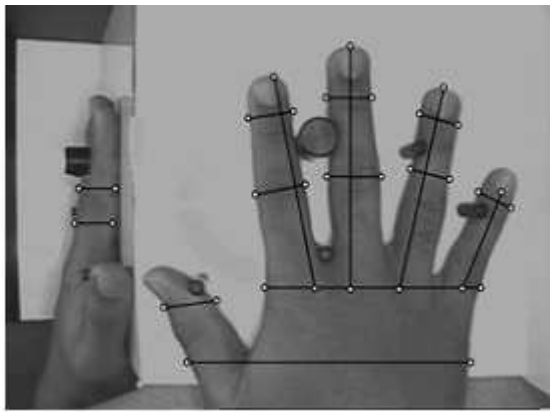
- 1990'ların başında geliştirilmiştir.
- Genellikle havaalanları gibi giriş çıkış kontrol noktalarında kullanılmaktadır.
- Parmak izi sistemlerinde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karsılastırma için yaklasık 200 referans noktası kullanılmaktadır.
- Bu yöntemle gözleri görmeyen, Nistagmus (göz titremesi)hastalığına sahip veya irisleri olmayan kişilerin kimliklendirilmesi mümkün değildir.
- Ayrıca iris resmi alınırken gözlerin durumu, gözkapaklarının ve/veya kirpiklerin iris desenini bozması gibi faktörler sistemi olumsuz yönde etkilemektedir.

Fiziksel Biyometrik Sistemler - El Geometrisi Tanıma

- El geometrisi tanıma özellikle Amerika'da 20 yıldan beri kullanılan, özellikle havaalanları ve nükleer güç istasyonlarında tercih edilen bir yöntemdir.

- Bu metotta, kullanılan sisteme göre kişilerin elinin veya iki parmağının geometrik yapısı analiz edilir.

- Parmakların uzunluğu, genişliği ve büküm noktaları ayırt edici özelliklerdir.



Fiziksel Biyometrik Sistemler - El Geometrisi Tanıma

- El geometrisi tanıma doğruluk oranı yüksek olan bir yöntem olmakla birlikte dezavantajları da vardır :

  - Okuma cihazları büyük ve ağırdır.
  - Resmin alınma süresinin uzundur.
  - Yüzük, yara bandı gibi araçlar resmin alınmasında sorun yaratabilir.
  - Yaralanma ve parmakların kaybedilmesi, gut veya kireçlenme gibi hastalıklar nedeniyle sistem performansı düşebilir.
  - Çocuklarda ellerin çok hızlı büyüyüp gelişmesinden dolayı sistem hemen hiç kullanılamamaktadır.
  - Ayrıca çocuklara benzer şekilde ellerin ve ayakların çok hızlı büyümesi hastalığına sahip olan kişilerde de çocuklarda olduğu gibi kullanılamamaktadır.

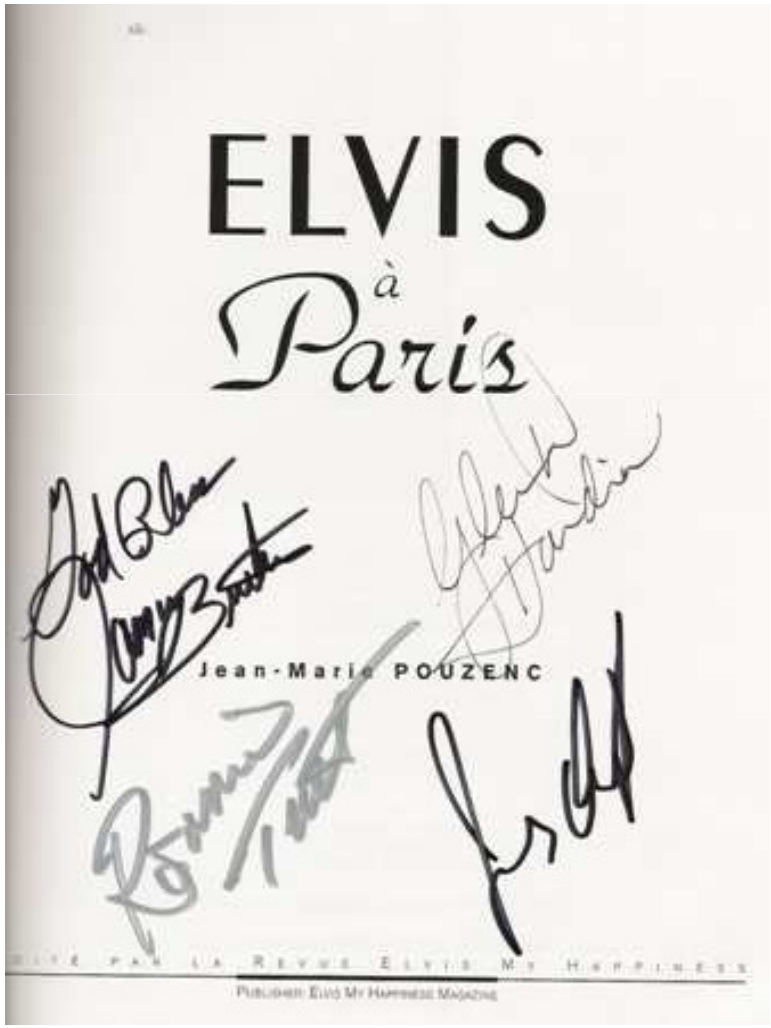
Davranışsal Biyometrik Sistemler - İmza Tanıma

- Kişinin kendi ismini yazma şekli olarak tanımlanabilen imzayı kişiler sosyal hayatın birçok alanında kullanmaktadır.
- Bir dokümanın altına atılan imza, imzayı atan kişinin o dokümanı okuduğunu, yazdığını ya da onayladığını gösterir.
- İmza tanımada sistemlerinde iki tip bilgi kullanılmaktadır.
- Bunlardan ilki imzalama süresi, hızı, ivmesi, kalemin basım şiddeti gibi imzalama işlemi ile ilgili davranışsal özellikler, diğeri ise bir desen olarak imzaya ait özelliklerdir.
- Gerçek kullanıcı olmayan herhangi birinin, başka birinin imzasını taklit etmesi güçtür.
- İmza desen olarak taklit etse bile imza atış şekli kolay kolay benzetilemez.

Davranışsal Biyometrik Sistemler - İmza Tanıma

Bu sistemin dezavantajları olarak sistemin kullanıcısının hızı, imza atma davranışı ve diğer özellikleri öğrenebilmesi için uygun sayıda örneğe ihtiyaç duyması sayılabilir.

Ayrıca imza atımının kullanıcının o anki ruh haline, sağlığına, acelesi olup olmadığına bağlı olarak değişmesi de diğer bir dezavantajtır.



BİYOMETRİK TABANLI YÖNTEMLER İLE DİĞER YÖNTEMLERİN KARŞILAŞTIRILMASI

- Biyometrik tabanlı yöntemler diğer kimlik doğrulama yöntemlerine (bilgi temelli ve aidiyet temelli sistemler) göre avantaj ve dezavantajlara sahiptir.

- Biyometrik tabanlı yöntemlerin diğer yöntemlerle olan benzerlikleri ve farklı yönleri bir tablo ile şu şekilde ifade edilebilir :

BİYOMETRİK TABANLI YÖNTEMLER İLE DİĞER YÖNTEMLERİN KARŞILAŞTIRILMASI

Diğer Kimlik Doğrulama Yöntemleri	Biyometrik Sistemler
Kullanılan veri her kullanıcı için kesinlikle farklı ve eşsizdir	Kullanılan veri her kullanıcı için farklı olmakla beraber bazı kullanıcıların verilerinde benzerlikler görülebilir
Kullanılan veri açıktır	Kullanılan veri açıktır
Veri kullanıcı tanımlamak için kullanılır	Kullanıcı tanımlamak için kullanılmakla beraber daha zengin bir veridir
Kullanıcı kimliği verisi kişinin istemesi halinde rahatça değiştirilebilir	Biyometrik veri kaza vs dışında değiştirilemez
Kullanıcı kimlikleri sabit olarak oluşturulur	Biyometrik veri sabit değildir
Genelde mevcut sistemlere uyumludur	Ek bir donanım maliyeti getirir
Çalınma vb durumlarda değiştirilmesi talep edilebilir	Biyometrik ölçüler değiştirilemediğinden herhangi bir şekilde elde edildiğinde geçerliliği kalmaz
Herkes için kullanılabilir	Herhangi bir biyometrik tarama sisteminde biyometrik özelliklere sahip olmayan (parmağı, gözü olmayan vb) kişiler bu sisteme dahil edemeyecektir
Zaman içerisinde değişim göstermesine sebep olacak bir durum sözkonusu değildir	Zaman içerisinde biyometrik veriler deformasyona, değişime uğrayabilir
Veri kaybı, çalınma, kaybetme tehlikesi büyüktür	Veri kaybı, çalınma, kaybetme tehlikesi needeyse hiç yoktur

BİYOMETRİK TABANLI YÖNTEM SALDIRILARI

- Her güvenlik sisteminde olduğu gibi, biyometrik tabanlı güvenlik sistemlerine de saldırılar yapılabilir.
- Biyometrik sistemlerde organizasyon dahilindeki herhangi bir yazılıma ya da sistemin donanımsal bir bileşenine saldırılar yapılabilir.
- Saldırılar biyometrik sensöre/algılama cihazına yapılabilir.
- Saldırılar iletişim kanalına yapılabilir.
- Saldırılar sistemi gizlice dinleyip bilgi elde etmek hatta transfer eden bilgileri değiştirip sisteme geri vermek şeklinde olabilir.
- Bu saldırılar biyometrik güvenlik sistemlerinde iyi tanımlanmalı ve saldırılardan korunmak için gerekli önlemler alınmalıdır.

SONUÇ

- Bu çalışmada biyometrik güvenlik yöntemleri incelenmiştir.
- Basit anlamda uzun süredir kullanılmalarına rağmen gerçek anlamda kullanılmaya başlanmaları kısa bir zaman öncesine dayanır.
- Kişinin şifresini kendi üzerinde taşıması olarak ifade edebileceğimiz biyometrik güvenlik sistemleri, her geçen gün daha fazla alanda kullanılmaya başlanmaktadır.
- İris, parmak izi, el geometrisi gibi fiziksel sabit özellikler ve imza atış sekli, yürüme şekli gibi davranışsal özelliklerin herhangi birisini kullanan sistemler günümüzde oldukça rağbet görmektedir.

SONUÇ

- Günümüzde özellikle havaalanları, karakollar gibi güvenliğin yüksek olarak tutulması gereken noktalarda kullanılan sistemlerin gelecekte kullanılması beklenen potansiyel kullanım alanlarından bazıları su şekilde ifade edilebilir :

SONUÇ

- Atm kullanımı: Binlerce kullanıcısı olan, bankalarda sahteciliğin boyutları düşünüldüğünde bu sorun biyometri kullanarak çözülebilir.
- Turizm: Yolcuların uçak, tren vs bileti alma, otel odası ayırtma ya da araç kiralama gibi çeşitli turizm hizmetlerinde ve havaalanı gibi kontrol noktalarından geçişlerinde kullanabilecekleri biyometrik sistemlerin tasarlanması işleri oldukça kolaylaştıracaktır.
- İnternet işlemleri: Kişiye özel biyometrik bir okuyucunun pc'lere entegre edilmesi ile internetten yapılabilecek bankacılık işlemleri, resmî işlemler, pasaport vs başvuruları gibi dijital işlemler kişinin biyometrik kimlik doğrulaması sayesinde yapılabilir.
- Telefon işlemleri: İnternete benzer şekilde telefon üzerinden alışveriş vs işlemleri gerçekleştirilebilir. Ancak, telefon cihazının, telefon hatlarının ve kullanıcı ortamlarının sabit olmayıp çeşitlilik göstermesi bu işlemi zor kılmaktadır.

SONUÇ

- Biyometrik güvenlik sistemleri genelde ek maliyet gerektirir.
- Kullanımları bazen uzmanlık gerektirir.
- Biyometrik bilgiler ele geçirildiği anda yenilenmesi sözkonusu olmadığından geçerliliği kalmaz.
- Bunlar biyometrik güvenlik sistemlerinin dezavantajları olarak sayılabilir.
- Ancak
  - kişinin kendisi dışında ek bir donanım, yazılım, şifre, araç kullanmak zorunluluğunun olmaması,
  - çalınma, unutulma, kaybolma gibi tehlikelerin yok denebilecek kadar az olması

  gibi avantajları ile biyometrik sistemler gelecekte daha çok yer edinecek gibi görünmektedir.

TEŞEKKÜRLER...