

BILGISAYAR DESTEKLI KIMLIK TESPIT SİSTEMLERİNDE BIOMETRİK YÖNTEMLERİN DEĞERLENDİRİLMESİ

Ars.Gör.Taha SADAY, Ars.Gör.Nurdan AKHAN

T.C. Selçuk Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü

ÖZET :

Biometrik cihazlar insanların benzeri olmayan parmak izi, göz retinası, iris, yüz şekli, ses, imza, avuç içi vs gibi karakteristiklerini ölçerek; bilgisayar sistemleri, veri bankaları ve benzer ortamlara giriş için kimlik doğrulamasını yapmaktadırlar. Bunun dışında, bu sistemler emniyet ve istihbarat birimlerinde de çok değişik amaçlarla kullanılmaktadır. Biometrik sistemler, temelde, kişinin sadece kendisinin sahip olduğu, kendisi olduğunu kanıtlamaya yarayan, değiştiremediği ve diğerlerinden ayırıcı olan, fiziksel veya davranışsal bir özelliğinin tanınması prensipleri ile çalışmaktadırlar. Ancak bu sistemlerin güvenilir olmalarının yanı sıra pratik olmaları da gerektiğinden dolayı, kişileri hangi yöntemler ile tanındıkları da önemli bir etkidir. Bu çalışmada ağırlıklı olarak parmak izi tanımlama ve araştırma yöntemleri ele alınmıştır. Parmak izleri en yaygın olan karakteristiklerine göre sınıflandırılmış, elde edilen sınıflar ise ayrıntılara göre alt sınıflara bölünmüştür. Çalışmada verilerin elde edilmesi, bilgisayar ortamına aktarılması ve veri tabanında yerleştirilmesi hususlarına ayrıca dikkat edilmiş, örnek seçme ve değerlendirme yöntemleri ele alınmış ve burada karşıya çıkan problemler gösterilmiştir. Sonuç olarak biometrik sistemlerin özellikle parmak izinin, ayırt edici özelliğinin bulunmasıyla birlikte, güvenlik sistemlerinin geliştirilmesinde, suçluların bulunmasında, insanların tanımlanmasında kullanımı gittikçe yaygınlaşmıştır.

Anahtar Kelimeler :

Biometrik, parmak izi, kimlik tespiti, güvenlik.

GIRIS

Insanlari; parmak izlerinden, gözlerinden ve fizyolojik özelliklerinden tanıyabilen Biometri teknolojisi, her geçen gün biraz daha geliyor. Ancak bu teknolojinin yaygınlaşabilmesi için maliyetlerin daha uygun hale getirilmesi gerekiyor.

İnternet üzerindeyken, hiç kimse kim olduğunuzu bilemez. Kim olduğunuzu kanıtlamanızın geleneksel yolu, e-posta atarken, on-line alışveriş yaparken veya güvenli bir Web sitesine girerken şifre yazmaktır. Fakat bu yol şifreleme algoritmalarının çözümlenmesi sayesinde gün geçtikçe güvenliğini daha çok kaybetmektedir.

Şifreler ağ korsanları tarafından birçok kez kırıldığı için yada kullanıcılar tarafından sık sık unutulduklarından artık yerlerini Akıllı Kartlar ve Biometrik cihazlar gibi yeni teknolojilere bırakmaktadır. Biometrik Cihazlar insanların benzeri olmayan parmak izi, göz retinası gibi karakteristiklerini ölçerek kullanıcıların şifre kullanmaksızın bilgisayar sistemleri, veri bankaları ve benzer ortamlara giriş için kimlik doğrulamasını yaparlar. Bu fizyolojik ölçü yöntemlerinin tümü "Biometri" olarak tanımlanmaktadır. Biometrik bilgiler; kaybolmamak, unutulmamak ve bir baskısı tarafından kullanılmamak gibi özelliklerinin yanı sıra taklit edilememesi gibi çok önemli olan bir özelliğe de sahiptir.

Biometri teknolojisiyle, bilgisayara parmak izi tarayıcısını kullanarak girmek, göz tarayıcısı yardımıyla ATM'den parayı çekmek, ses tanıma ile bankalara sesli talimat vermek, korunmakta olan mekanlara yüz tanıma cihazı yardımıyla girebilmek vs mümkün olabilmektedir.

Biometri teknolojisi, halen, yukarıda gösterilen gelişmelerin yanı sıra aşağıdaki önemli problemlerle karşı karşıyadır.

- Biometri için gereken donanımın pahalı olması
- Farklı sistemlerin birbirleriyle sorunsuz bağlantısının henüz sağlanamamış olması
- Biometri teknolojisinin bir bütün halinde yeni yeni gelişmekte olmasıdır.

Bilgisayarlar günlük hayatın giderek daha önemli bir parçası haline gelmesiyle, belgelerin imzalanmasından alışverişe kadar pek çok işlem dijitalleşerek, biometri ürünleri vazgeçilmez bir hal alacak gibi görünüyor.

BIOMETRİNİN BİLGİ İŞLEM TEKNOLOJİSİNDE KULLANILMASI

Biometri, kullanıcının fiziksel ve davranışsal özelliklerini tanıyarak kimlik saptamak üzere geliştirilmiş bilgisayar kontrollü otomatik sistemler için kullanılan genel bir terimdir. Bu

sistemler mümkün olduğunca, insan beyninin kişiyi tanıma ve diğerlerinden ayırt etme yöntemleri ile aynı şekilde çalışmaktadır. Kart, şifre veya pin numarası kullanan diğer tanıma yöntemlerine oranla daha çok tercih edilmektedirler. Bu durumun başlıca sebepleri aşağıdakilerdir:

- Kullanıcının, kimlik saptama yapılacak yerde bizzat bulunma gerekliliği
- Kullanıcının yanında kendini tanıtmak için kimlik kartı benzeri tanıtıcılar taşımak zorunda olmayışı
- Kullanıcının şifre/pin numarası gibi gizli olması gereken bilgileri ezberlemek zorunda olmayışı

İnternetin bilgi teknolojisi aracı olarak etkin kullanılmaya başlanması ile birlikte, bazı kişisel bilgilere veya firmalara ait gizli verilere, yetkili olmayan kişi veya kuruluşlarca ulaşmanın engellenmesi zorunluluğu doğmuştur. Bilinen ve yaygın olarak kullanılan sistemler, kullanıcıları tanımlamak yerine kullanıcının sunduğu tanıtıcılara onay vermektedir. Halbuki biyometrik teknolojiler kişileri doğrudan tanıdıkları için, yetkisi olmayan kişilerin değerli bilgilere erişimini, ATM, cep telefonu, smart kart, masaüstü bilgisayar, iş istasyonu ve bilgisayar ağları gibi sistemlerin uygunsuz kullanımının engellenmesi için en çok başvurulan yöntem olmaktadır. Günümüzde çeşitli biyometrik sistemler, eşzamanlı tanıma uygulamalarında yaygın olarak kullanılmaktadır. Bunların en bilinenleri aşağıdakilerdir :

- Parmak izi eşleştirme
- Iris tanıma
- Retina taraması
- Ses ve konuşma tanıma
- Yüz tanıma
- El tanıma

Biyometrik sistemlerin güvenilir olmalarının yanı sıra pratik olmaları da gerekir ve bu yüzden kişileri hangi yöntemlerle tanıdıkları da önemli bir etkidir. Bu yöntemlere örnek olarak aşağıdakiler verilebilir :

1. Teshis (Identification) prensibi: Bu prensibe göre sisteme imza(bilginizi) sunulur ve sistem bu bilgiye göre imza sahibine ait olan tüm diğer bilgileri veritabanından bulup çıkarıyor.
2. Doğrulama (Verification) prensibi :Bu prensibe göre bir kimse sisteme kimliğini giriyor. Sistem bu kimsenin gerçekten girilen kimliğin sahibi olup olmadığını o kimliğe ait olan kayıtları inceleyerek karar vermeye çalışır.

Söz konusu sistemler oldukça güvenli sonuçlar vermektedirler. Fakat ikinci prensibe göre kişilerin bir şifre veya kullanıcı kodunu ezberlemeleri gerekiyor. Kullanıcıların ezberleme problemi ortaya çıktığı durumlarda ise kişiye kaybetmemesi gereken bir kart verilebilir. Ama tüm bunlar risk faktörünü artırdığı için genelde Doğrulama prensibi yoğun olarak tercih edilmez.

Biometrik sistemin en temel avantajı, kişilerin hiçbir zaman hiçbir yerde unutma veya kaybetme olanakları bulunmayan bir uzuvları ile kendilerini tanıtabilmeleridir. Bu yüzden gelecek için planlanmakta olan güvenlik sistemlerinin en esas amacı insanların hiçbir kart veya anahtar tasımadan veya şifre ezberlemeden evlerinden çıkabilmeleri ve belli bir kişinin sadece o olduğu için tanınabilmesidir.

BIOMETRİK SİSTEMLERİN ÇALIŞMA PRENSİPLERİ

Biometrik tanıma sistemlerinin çalışma prensibi aşağıdaki şekilde özetlenebilir.

Önce kayıtlı bir imaj alınır. Bu imaj dijital koda çevrilir. Bu kod da gerekirse yapılan işleme göre şifrelenir ve bilgisayara kaydedilir. Daha sonra kullanıcı herhangi bir cihaz aracı ile kendini sisteme tanıtır. Genellikle aynı kişiye ait olsa bile, girilen kod ile kayıtlı olan kodun birebir tutuma olasılığı yoktur. Bunda birçok faktör etkili olabilir. Bunlarda en yoğun olarak rastlananları aşağıdakilerdir :

- Ortamın ısılandırması
- Kişinin bakış açisi
- Teshisi yapılacak uzvun cihaza göre durma açisi
- Cihazın ve kontrol edilen uzvun temizlik derecesi ve nemi

Bu olumsuz etkilerden dolayı girilen kod, belli bir yüzde tutuncaya kadar sistemde kayıtlı bulunan kodlarla karşılaştırılır. Gereken yüzde yakalandığında şahıs tanınır ve işlem için onay verilir.

BIOMETRİNİN KULLANIM ALANLARI

Halen biometrik sistemler aşağıdaki alanlarda kullanılmaktadır :

- Personel devam ve takibi
- Otomatik para çekme makinelerinde kullanıcı tanımlama
- Çağrı merkezlerinde kimlik saptama

- Havalimanlarında check-in ve boarding işlemleri
- On-line bankacılık kullanıcı tanımlama
- Sınır kontrolü ve sınır kapılarından girişlerin kontrolü
- İnternet bankacılığında kullanıcı tanımlama
- Elektronik para transferlerinde kullanıcı tanımlama
- Kredi kartı uygulamaları
- Kurumsal ağ
- Bilgisayar güvenliği
- Kiralık kasalara erişim güvenliği
- Satış noktası terminallerinde (POS) kullanıcı tanımlama
- Askeri kaynakların etkin takibi
- Çek onaylama işlemlerinde kullanıcı güvenliği
- Hastane ve sigorta kuruluşlarında hasta takibi ve kimlik saptama
- Kamu hizmetlerine yönelik kayıt takibi (SSK, vergi, trafik)
- Hesap açma işlemlerinde kimlik tespiti
- Binalara, tesislere ve ofislere erişim güvenliği
- Elektronik ticarete kullanıcı tanımlama
- Şube bankacılığı işlemlerinde kullanıcı tanımlama

BIOMETRİK ÇEŞİTLERİ

Parmak izi Doğrulama

Parmak izi doğrulamaya birçok farklı yaklaşım vardır. Bir kısmı bilinen polis metodu olan iz karşılaştırmasını taklit etmeye çalışır, diğerleri ise "moire fringe" şablonu yada ultrasonik gibi kendilerine özgü yaklaşımlar ile düz şablon karşılaştırması yaparlar. Bazıları canlı bir parmağı hissedebilirler bazıları edemezler. Diğer biometriklere kıyasla parmak izi cihazlarında çok fazla çeşitlilik vardır. Yüksek verimli ve düşük hata paylı olmalarına rağmen tecrübesiz kullanıcıların hatalı işlemleri nedeniyle sorunlar doğurabilmektedir. Kullanıcı arabiriminin de geniş çaplı kullanımlarda nasıl olması gerektiği düşünülmesi gerekir. Parmak izi doğrulama, kullanıcılara yeterli eğitimin verilebileceği ev içi sistemlerde ve kontrollü ortamlarda kullanıma uygundur. Entegrasyon ve kullanım kolaylığı, düşük fiyatları ve küçük ebatları

nedeniyle is istasyonu erisim sistemlerinde Parmak izinin yaygin bir kullanıcı kitlesi bulması sasirtici degildir.

El Geometrisi

İsminden anlaşılabacağı üzere üç boyutlu bir perspektiften kullanıcının elinin ve parmaklarının fiziksel karakteristikleri esas alınır. En yaygın metotlardan biri olarak iyi performans sağlar ve kullanımı göreceli olarak daha kolaydır. Kullanıcı sayısının fazla olduğu yada sisteme çok fazla erişimin olmadığı ortamlarda ve fazla kullanım disiplini gerektirmemesi nedeniyle tercih edilebilir. Kararlılığın istenirse çok yüksek olabileceği gibi, esnek performans ayarları ve konfigürasyon geniş uygulamalarda kullanıma izin verir. El geometrisi okuyucuları Personel Devam Kontrol Sistemleri gibi senaryolarda popülerliğini kanıtlamıştır. Diğer sistemlere entegrasyon ve kullanım kolaylığı el geometrisini birçok projede ilk adım olarak ön plana çıkarmaktadır.

Ses Doğrulama

Günlük işlerde ne kadar çok sesli iletişimin kullanıldığı düşünülduğünde oldukça ilginç bir teknik olarak karşımıza çıkar. Bazı tasarımlar duvara monteli olarak karşımıza çıkarken bir kısmı da bilinen telefon cihazlarıyla entegre olarak kullanılırlar. Pazara birçok ses doğrulama ürünü girmiş olmasına rağmen çoğu lokal akustik ve alıcı sorunları nedeniyle yetersiz kalmıştır. Ek olarak kullanıcı tanıma işlemleri diğer biometriklere göre daha karışık olduğu için pek dostça karşılanmamıştır. Bununla birlikte birçok çalışma yapılması gerekmekte olup gelişmeleri izlemek ilginç olacaktır.

Retina Tarama

Bir optik alıcı vasıtası ile retinanın benzersiz sablonlarının düşük yoğunluklu bir ışık kaynağı ile taranmasına dayalı yerleşmiş bir teknolojidir. Kararlılığı kanıtlanmış bir teknik olmasına rağmen kullanıcının bir noktaya sabit bakmasını gerektirmektedir. Eğer gözlük kullanıyorsanız yada okuyucu ile göz temasına girmekten endişe duyuyorsanız pek güvenilir bir yöntem değildir. Bu nedenlerden ötürü retina taramasının kullanıcılar tarafından kabullenilmesi zor olmakla birlikte teknoloji oldukça verimli çalışmaktadır. Doksanlı yılların

ortalarında yeniden tasarımı son haline gelmiş olup gelişmiş bağlanılabilirlik ve kullanıcı arabirimi sağlamaktadır ama yine de marjinal bir biyometrik teknoloji olarak görülmektedir.

Iris Tarama

Iris tarama, gözle ilgili biyometrikler arasında süphesiz en basitlerinden biridir. Basit sira dan bir ccd kamera ile çalışır ve kullanıcı ile okuyucu arasında direk kontak olmasına gerek yoktur. Ek olarak, ortalamanın üzerinde sablon karşılaştırma potansiyeline sahiptir. Teknoloji olarak, üçüncü parti üreticilerin ilgisini çekmiş ve ilave ürünlerin ortaya çıkmasına öncülük etmiştir. Gözlükle birlikte kullanılabilmesi nedeniyle birtakim dini gruplarında ilgisini çekmiş tanımlama modunda iyi çalışan birkaç cihazdan biri olarak kendini ispatlamıştır. Kullanım kolaylığı ve sistem entegrasyonu iris tarayıcılar için söylenmesi pek kolay olmamakla birlikte yeni ürünler tanıtıldıkça gelişmeleri takip edeceğimizi umuyoruz.

İmza Doğrulama

İmza doğrulamanın diğer biyometriklerde görülmeyen farklı yönleri vardır. İnsanlar imzaya günlük işlemlerinde bir kimlik doğrulama aracı olarak kullandıklarından dolayı zaten alıştırlar ve bunun biyometriğe aktarılmasında bir anormallik görmemişlerdir. İmza doğrulama sistemleri çalışmalarındaki kararlılığı ispatlamışlardır ve imzanın doğrulama aracı olarak kullanıldığı uygulamalarda yerlerini almışlardır. Ne yazık ki diğer biyometrik ürünlere kıyasla çok az sayıda uygulaması görülmektedir. Eğer uygulamanıza uygunsa, düşünülme ye değer bir teknolojidir.

Yüz Tanımlama

Oldukça fazla ilgi çeken ancak yetenekleri yanlış anlaşılmış bir tekniktir. Pratikte ispatlanması zor asiri iddialar yüz tanımlamaya yapılmıştır. Tüm yapılan, sabit iki görüntünün karşılaştırılmasıdır (çoğu sistemin gerçekte yaptığı budur, biyometrik ile pek ilgisi yoktur). Bir grup içindeki kişinin kimliğini doğrulamak için kullanılır (bazı sistemler iddia etmektedir). Kullanıcı açısından yüz tanımlamanın çekiciliğini anlamak kolaydır, ama teknolojinin beklentileri konusunda gerçekçi olmak gerekmektedir. Şu ana kadar yüz tanımlama sistemleri uygulamalarda sınırlı başarı sağlamışlardır. Ancak çalışmalar devam etmektedir ve gelecekteki uygulamaların neler olacağını görmek ilginç olacaktır. Teknik zorluklar aşılabılırsa, yüz

tanımlamanın birincil biyometrik metod haline geldiğini görebiliriz. Sima, kulak memesi ya da birçok farklı parametreyi kullanan metodlar mevcuttur. Teknik olarak ilginç olmalarıyla birlikte günlük hayatta kullanılabilir olarak değerlendirilmemektedirler.

BIOMETRİK VERİLERİN GİRİLMESİ VE İŞLENMESİ

Bu işleme örnek olarak parmak izi alimini verelim. Parmak izi ilk defa alındığında üzerinde karşılaştırma, arama, eşleme ve veri tabanına kaydetme gibi işlemleri yapmadan önce belirli işlemlere tabii tutulması gerekmektedir. Bu işlemlere ön işleme adı verilir.

İşlenmemiş bir parmak izi üzerinde bulanık bölgeler bulunabilir. Bu bulanıklıkların ortadan kaldırılması gerekir. Parmak izi üzerinde işlem yapabilmek için fiziksel ortamdaki parmak izinin manyetik ortama aktararak sayısallaştırılması gerekir.

Resim olarak bilgisayar ortamına aktarılan bir resim aslında sayısal bilgiler içermektedir. Kullanılan bilgisayarın teknik özelliklerine göre sayısal bilgiler resim aynı olmasına rağmen bilgisayarlar arasında farklılık gösterir. Bu farklılığın temel nedeni kullanılan çözünürlük seçenekleridir. Eğer bilgisayarınız en fazla 256 rengi destekliyorsa elinizde bulunan resmi ekranda görüntülemek için kullanılacak olan renk aralığı 0-256 renk arasında olur. Yani resim üzerinde bulunan siyah noktalar 0, beyaz noktalar ise 256 ile gösterilir. Bilgisayarınızın ekran kartı 16 bit çözünürlüğü destekliyorsa kullanılan renkler için renk ayırımı daha da hassas bir duruma gelir. Renklerin kalitesi çok daha artar. Siyah noktalar yine 0 ile gösterilir. Fakat beyaz renk 16777216 ile gösterilir. Bunun anlamı; 16777216 adet farklı renk kullanılabilir demektir.

Her renk; Kırmızı (Red), Yeşil (Green) ve Mavi (Blue) ana renklerinin belirli oranlarda birleştirilmesiyle elde edilmektedir. Her ana rengin alabileceği maksimum değer 256'dir.

$$256 \times 256 \times 256 = 16777216 \text{ adet renk}$$

$$\text{RGB} (256 , 256 , 256) = \text{Beyaz}$$

$$\text{RGB}(1 , 1 , 1) = \text{Siyah}$$

Bir resmi sayısallaştırmak demek her renge karşılık gelen sayıyı bulmak demektir. Eğer bir resim içerisinde kırmızı 15702248 renk kodu ile gösterilmişse, tüm resim içerisinde kırmızı aynı renk kodu ile gösterilir. Kırmızı renkteki en ufak bir değişiklik bu sayıyı etkiler.

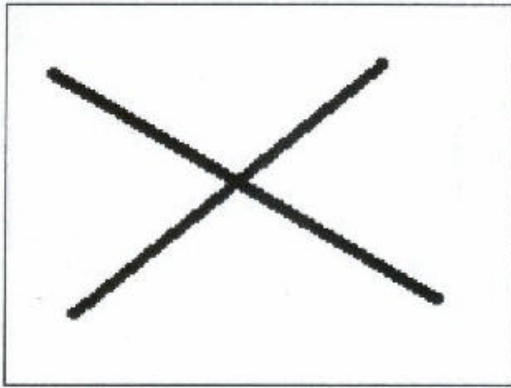
Sayısallaştırma işlemi; ekran pikellerine karşılık gelen renk kodunun herhangi bir program aracılığıyla alınarak bir dosyaya V(ij) formatında yazdırılması demektir.



00000000016777215167772151677721516777215167772
77215001677721516777215167772151677721516777215
7215000000000000000000000000000000000016777215167772151
000000000000000000001677721516777215167772151677
7721516777215167772151677721516777215167772151
1516777215016777215167772150000000000000000000
77215167772151677721516777215000000000000000000
00
0000000000000000000167772151677721516777215167772
000000000000000000167772151677721516777215167772
215167772151677721516777215000000000000000000000
1677721516777215167772151677721516777215167772
7721516777215167772151677721501677721516777215
1677721516777215001677721516777215167772151677
7721516777215167772151677721516777215167772151
7721516777215167772151677721516777215167772151
21516777215167772150000167772151677721516777215
7721516777215167772151677721516777215167772151
2151677721516777215167772151677721516777215167
15167772151677721500000167772150000000000000000

Şekil 6.2 Bir parmak izi resminin sayısal görünümü

Yukarıda ki şekilde ön işleme yapılmamış bir parmak izinin sayısallaşmış durumu görülmektedir. Dikkat edilirse iç içe girmiş bir sürü sayı görülmektedir. Parmak izi üzerinde bulunan ve aynı bölgeye karşılık gelen alanlardaki sayılar aynıdır. Bu haliyle parmak izi üzerinde işlem yapmak pek mümkün görülmemektedir. Parmak izini işlem yapılabilir duruma getirebiliriz. Öncelikle bu parmak izi üzerinde bulunan değişik renk kodlarını ortadan kaldırarak resmi anlaşılabilir kodlara dönüştürmek gerekmektedir. Bu işleme kısaca resmi sadece siyah ve beyaz renklerden oluşan bir görüntü haline getirmek de diyebiliriz. Eğer kullanılan monitör siyah-beyaz bir monitör ise görüntü sadece iki renkle gösterilecektir. Bu durumda siyah-beyaza dönüştürme işlemine gerek yoktur. Tercih edilen yöntem de budur. İkinci aşamada resmin üzerinde bulunan kalınlıklar standart bir hale getirerek inceltme işlemi yapılmalıdır. Daha sonra yapılacak olan işlem ise resim üzerinde yalnız basına kalmış hiç bir anlam ifade etmeyen renk kodlarının temizlenmesi işlemidir. Aşağıdaki şekilde basit olarak çizilmiş bir resim için hafıza görüntüsü ele alınarak incelenmiştir.



Parmak izi üzerinde bulunan renkleri siyah - beyaza dönüştürmek için değişik yöntemler kullanılabilir. Bu yöntemlerden birisi 1993 yılında Mehtre'nin yapmış olduğu; $V(i,j)$ dizisi içerisinde bulunan her bir elemanın sabit bir sayıya göre karşılaştırılması ve karşılaştırma işlemi sonucunda sabit sayıdan büyük olanlara 0, sabit sayıdan küçük olanlara 1 değerinin verilmesi yöntemi ile mümkündür. Bu işlem yapıldığında $V(i,j)$ dizisiyle ifade edilen parmak izi aşağıdaki şekilde görünecektir.



Parmak izi üzerinde ayrıntılı arama çalıřmaları yapabilmek için siyah-beyaza dönüřtürülmüř parmak izi üzerinde inceltme işlemi yapılmalıdır. Inceltme işlemi birden fazla pixele denk gelen görüntünün islenerek resim genelinde bir yada iki pixel ile gösterilmesi işlemidir.



SONUÇ

Teknolojik gelişmelerin bu kadar hızlı olması olumlu olmasının karşısında olumsuz olarak da insanlığı etkilemekte sahteciliğin de teknolojinin nimetlerinden yararlanmasına sebebiyet vermektedir. Bu nedenle son zamanlarda şifreleme yerine uygulanan biyometrik sistemlerin

birleştirelmesi çalıřmaları yoğunluk kazanmaktadır. Buna örnek olarak bir kapıdan geçiři saęlamak için parmak izinin yanında yüz seklı tanıma, ses tanıma, iris yada retina tanıma gibi güvenliik sistemleri ortak kullanılmaktadır.

Son zamanlarda ise bilim adamları kisilerin DNA bilgilerinden yararlanarak kimlik tespitini saęlamak için yoğun çalıřmalar sürdürmektedirler. Bu sistemin gerçektelesmesi durumunda dięer biometrik tanıma sistemlerine gerek kalmayacağı beklenmektedir. Fakat ilgili kaynaklarda verilen ön görülere göre bu sistemin geliřtirilmesi ve yaygın duruma gelmesi yıllar alacaktır.

Günümüzde bilgisayar destekli bilgi islem teknolojisinin son derece gelişmiş olmasına rağmen Biometrik verilerin islenmesinde hale halledilmesi gereken problemler çoktur. Bunun esas nedeni biometrik verilerin islenmesi yöntemlerinin çok zor bir şekilde algoritmleştirelmesi bilmesidir. Zennimizce bu problem asılırsa geriye kalanların çözümlenmesi de sadeleşmiş olacaktır.

KAYNAKLAR

- http://www.ergosis.com.tr/biometrics_tr.html
- <http://212.154.21.40/2001/11/18/bilisim/bilisimdevam.htm>
- Parmak izinin ayırt edici özelliklerinin kullanılması suretiyle analiz edilmesi ve otomatik ön işleme yönteminin programlanması (Ertugul Geççil)
- Emniyet Genel Müdürlüğü, Asayis Daire Başkanlığı, Parmak Izi Sube Müdürlüğü Dokümanları
- Parmakizi sınıflandırması, Bora Susmaz