# Biyometrik Güvenlik Sistemleri

**Rüya Şamlı, M. Erkan Yüksel**
İstanbul Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul
rsamli @istanbul.edu.tr,eyuksel@istanbul.edu.tr

**Özet:** Bilgi güvenliği günümüz teknoloji dünyasının en önemli problemlerinden biridir. Kişiler ya da kurumlar, her türlü bilgiyi güvenli bir ortamda tutabilmek ve bu bilgileri saklamak, korumak için büyük çabalar ve paralar harcamaktadır. Bir bilginin gizliliğinden ve güvenliğinden bahsedebilmek için söylenebilecek tek şey o bilginin kimsenin eline geçmemesi değildir. Bunun yanında bilginin bütünlüğü, bilgiyi gönderen kişinin gönderdiğini; alan kişinin de aldığını inkar edememesi gibi kavramlar da önem taşımaktadır. Bunlara bakıldığında gizliliğin en kritik noktalarından birinin yalnızca yetki verilmiş kişiler tarafından bilgiye erişmesi olduğu açıktır. Gerçek dünya ortamında kişilerin kimliklerini doğruladıkları imza, mühür gibi elemanlar, bu uygulamalar dijital ortamda gerçekleştiginde geçerliliklerini yitirmektedirler. Dijital dünyada bunların yerine verilerin bazı matematiksel algoritmalardan geçirilmesi ile elde edilen dijital imzalar ya da sözkonusu kişilerin kendine has özelliklerinin kullanıldığı biyometrik güvenlik sistemleri kullanılarak sözkonusu kişinin kimlik doğrulaması sağlanabilir. Bu çalısmada dijital kimlik doğrulama yöntemlerinden biri olan biyometrik güvenlik sistemleri anlatılmıştır.

**Anahtar Kelimeler**: Biyometrik Güvenlik Sistemleri, Parmakizi Tanıma, Yüz Tanıma, Dijital İmza

**Abstract:** Information security is one of the most important problems in technology world today. People or companies send serious force and money for holding every type of information in secure environments, storing these information and keeping them secret. The only thing that can be said while mentioning about an information's being secret and secure is not its not being obtained by anyone. In addition to this, completeness of the information, sender's and receiver's having no ability for denying that he/she sent or received the information are also important effects for information security. So it can be understood that one of the most and critical points of security is only aurhorized people's accessing to information. In real life, the elements like signature, seal etc that validate people's identification lose their validities when these applications are done in digital world. In digital world, instead of them, aforementioned person's identity validation can be provided bye digital signatures that are obtained with datas' operating in some mathematical algorithms or biometric secure systems in that personal properties of aforementioned people are used. In this paper, biometric secure systems that are one of the digital identitiy validation methods are explained.

**Keywords :** Biometric Security Systems, Fingerprint Recognition, Face Recognition, Digital Signature.

## 1. Giriş

Kriptoloji biliminden ya da herhangi bir güvenlik sisteminden bahsedilirken, bilginin gizliliği kavramından söz edilir. Bilgi, insanlarla paylaşıldıkça anlam kazandığına göre bilginin gizliliği mutlaka ki kişilerle paylaşılması dışında bir anlama sahip olmalıdır. Bu anlam nedir diye bakacak olursak, bilginin gizliliğinin iletilmesi amaçlanan kişiye bozulmadan, değiştirilmeden, başka birisinin eline geçmeden ulaşması olduğunu görürüz. Bu tanımdan bilginin gizliliğinin kişiye göre değiştiği anlamı da elde edilebilir. Şöyle ki bir bilgi, ona ulaşma yetkisi olan kişiler tarafından gizli bir bilgi değilken, 3. şahıslar olarak tabir

edilen ve yetkisi olmayan kişiler için gizli bir bilgidir.

Herhangi bir bilginin gizliliğinden dolayısıyla da güvenliğinden bahsedebilmek için kimlik doğrulama kavramı oldukça önemlidir. Bilgi, gönderilmek istenen kişiye veya kuruma değil de başka kişi veya kuruma gönderilirse istenmeyen sonuçlar ortaya çıkar. Özellikle bu bilgi tıp ya da askerîye gibi kritik sektörlerde ise kayıp daha fazla olabilir.

Bilgi güvenliği için kullanılan kimlik doğrulama işlemi genel olarak bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç farklı şekilde incelenebilir. Bu çalışmanın konusu biyometrik temelli güvenlik sistemleridir.

Bilgi temelli kimliklendirme kullanıcıların ve sözkonusu sistemi yöneten kişi(ler)in belirli bilgilere sahip olması gerekir. Bu bilgiler, kullanıcı adı ve şifre olabileceği gibi, pin olarak ifade edilen numara dizileri de olabilir. Bu çeşit sistemlerde kullanıcılar ve karşılık gelen bilgiler (şifre, pin vs) bir veritabanında tutulur. Kullanıcılar bilgilerini sisteme girdiklerinde veritabanında karşılaştırma yapılır. Eğer karşılaştırma sonucu birbirini tutuyorsa doğru kullanıcı olduğu anlaşılır ve sözkonusu kullanıcının sisteme giriş yapmasına ve sistemde yetkisi dahilindeki işlemleri gerçekleştirmesine izin verilir. Bu tip sistemlerin en önemli dezavantajı kullanıcının şifre-pin bilgilerini unutmasının ya da bu bilgilerin bir başkası tarafından elde edilmesinin kolay oluşudur [1].

Kimlik doğrulamanın diğer bir çeşidi olan aidiyet temelli kimliklendirmede; kullanıcılar kendileri ile eşleşen bir objeye sahiptirler. Bu obje genelde manyetik kart, rozet veya anahtardır [1]. Sözkonusu sisteme giriş, kullanıcılar tarafından bu objeler kullanılarak yapılır. Objenin içerisinde sisteme giriş yapanın kim olduğunu belli edecek ve kimlik doğrulaması yapacak bilgiler mevcuttur. Bu çeşit sistemlerde de kişinin sözkonusu objeyi unutması, kaybetmesi, çaldırması ihtimali bir dezavantaj yaratmaktadır.

Biyometrik temelli kimliklendirme sistemlerinde kullanıcı sisteme kendisine ait olan ve üzerinde her daim taşıdığı parmakizi, iris, ses, el geometrisi, yüz gibi bir fizyolojik özelliğini veya imza atış, yürüyüş gibi bir davranışsal özelliğini kullanarak giriş yapar [2]. Kullanıcı bu şekildeki bir sisteme giriş yapmak istediğinde, sistem tarafından kullanıcının uygun biyometrik bilgisi (parmak izi, retina, ses retina) alınır. Alınan bu bilgi aynı kişiden alınıp veritabanına kaydedilmiş biyometrik bilgi ile karşılaştırılır. Karşılaştırma sonucu doğru ise aynı ise kişinin kimlik doğrulandırılması gerçekleştirilmiş olur.

## 2. Biyometrik Sistemler

Biyometrik sistemlerin basit halleri ile binlerce yıl önceden beri kullanıldığı bilinmektedir [3]. Yakın zamanda ise araşatırmacıların insanların fiziksel özellikleri ve karakteristiklerin suça eğilimleri ile bir ilgisinin olup olmadığını araştırmaları biyometri alanına ilgiyi arttırmıştır.

Günümüzde biyometrik incelemelerin boyutu, çeşitliliği ve kullanım alanları artmıştır. Bu sayede de pek çok yeni biyometrik kimlik doğrulama sistemi yerini almıştır.

Biyometrik sistemlerin uygulama alanları günümüzde oldukça çeşitlidir [4]. Özellikle havaalanları giriş ve çıkış işlemleri, kredi kartı uygulamaları, kriminal amaçlı teşhis ve tespit uygulamaları, sigorta şirketleri, ağ ve veri güvenliği, sosyal güvenlik, vergi süreçleri gibi kamu hizmetleri, e-ticaret, elektronik imza uygulamaları, internet bankacılığı, ATM'ler, çağrı merkezleri, personel takibi, hasta takibi bu gibi sosyal sistmlerde kullanılmalarının yanında artık, bilgisayarlar, pda olarak adlandırılan el bilgisayarları, cep telefonları ve ev kilit sistemlerinde de kullanılmaktadırlar [5]. Örneğin parmak izi, iris veya yüz tanıma sistemini barındıran bir bilgisayar, kimliğini doğrulayamayan kullanıcıların bilgileri açmasına ve işlem yapmasına izin vermemektedir.

Biyometri uygulayıcılarının genel amacı kişilerin kimliklerini doğrulayabilmeleri için, akıllarında tutmaları gereken herhangi bir bilgi ya da yanlarında taşımak, kaybetmemek ya da unutmamak zorunda oldukları kart, anahtar gibi araçların yerine; kopyalanması ya da taklit edilmesi imkansız olan özelliklerini kullanmalarını sağlamaktır. Biyometrik sistemlerde, kimlik belirleme işlemi, kişilerin fiziksel ya da davranışsal özelliğine dayanarak gerçekleştirildiği için başkasına devredilmesi, unutulması ya da kaybedilmesi durumu söz konusu değildir. Diğer yöntemlere göre çok daha az riske sahiptir. Ancak biyometrik sistemlerin oluşturulabilmesi için bazı standart ölçüler kullanılmalıdır. Biyometrik ölçüler olarak adlandırılan bu ölçülerin şifrelerde kullanımı için INCITS [6] (International Committee for Information Technology Standarts-Uluslararası Bilgi Teknolojileri Standartları Komitesi) tarafından oluşturulmuş uluslararası bir standart mevcuttur.

## 3. Biyometrik Sistem Çeşitleri

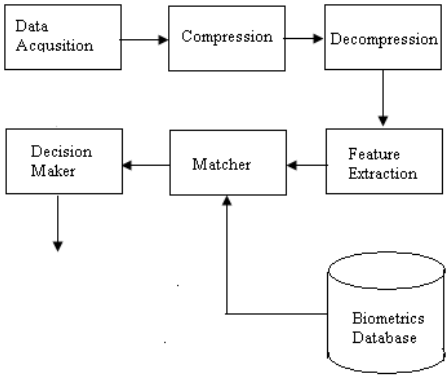
Günümüzdeki mevcut biyometrik tanıma sistemleri şunlardır :

**Fizyolojik özellikler [7]:**

- Parmak izi
- Retina
- DNA
- Damar
- Yüz
- El Geometrisi
- Ses
- Yüz Termogramı
- İris

**Davranışsal özellikler :**

- İmza Atımı
- Yürüyüş
- Tuş Vuruşu
- Konuşma




**Şekil 1 :** Biyometrik Sistemlerin Genel Çalışma Mekanizması

### 3.1 Parmakizi

Kullanılan biyometrik sistemlerin belki de en önemlisi polis merkezlerinde, pasaport ve vize başvurularında (İngiltere 2007 yılından beri vize başvurularında, başvuran kişiden biyometrik veriler almaktadır [8]) kullanılan parmak izi sistemleridir.

Parmak izi en fazla kullanılan, taklit edilemez bir biyometrik bilgidir. İlk kullanılmaya başlandığı yıllardan bu yana gerek yazılım gerekse donanım alanında parmak izi sistemlerinde önemli ilerlemeler kaydedilmiştir [9]. Bir otomatik parmakizi tanıma sisteminde (OPTS) parmakizi tanıma genellikle parmakizinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır [10].

**Şekil 2:** Bir Parmakizi Örneği

Bu sistemlerin en önemli dezavantajı, parmakizinin taklit edilmesi durumunda sistemin yanılabilmesidir. Diğer bir dezavantaj bazı

kişilerin pek çok sebepten ötürü (organ eksikliği, yanma, deri hastalıkları) parmak izlerinin bulunmamasıdır. Parmakizi taklit problemi, parmakizinin alındığı parmağın canlılığını test edecek gelişmiş sensörlerin kullanılması ile giderilebilecekken parmakizinin bulunmaması probleminin çözümü bulunmadığından bu sistem bu tip kişilerde uygulanamaz.

### 3.2 DNA

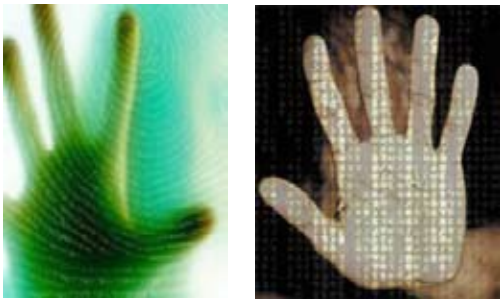
Kişinin saç, tırnak, deri parçası, kan, sperm veya herhangi diğer bir biyolojik materyali ele alınarak hücre içerisinde bulunan DNA moleküllerindeki dizilim incelenir. Özellikle emniyet güçleri tarafından cinayet mahallinde kalan biyolojik materyaller incelenerek katillere ulaşılması veya babalık davalarının sonuçlanması işlemlerinde kullanılmaktadır.

Doğruluğu çok yüksek bir yöntem olmasına rağmen maalesef pek çok dezavantaja da sahiptir. DNA'nın elde edileceği biyolojik dokunun kirlenmesi gibi durumlarda örnek kalitesi düşeceğinden analiz yapmak zorlaşır. Diğer dezavantajları işlemin 24 saat gibi bir sürede gerçekleştirilme zorunluluğu ve yüksek maliyet olarak sayılabilir.

### 3.3 El Geometrisi

Kişinin elinin veya kullanılan sisteme göre iki parmağının geometrik yapısı analiz edilir [11]. Sözkonusu yöntemde belirleyici özellikler parmakların uzunluğu, genişliği ve büküm noktalarıdır. Özellikle Amerika'da havaalanları ve nükleer güç istasyonlarında kullanılır.

El geometrisi de diğer biyometrik yöntemler gibi doğruluk oranı yüksek bir yöntemdir. Ancak büyük ve ağır okuma cihazları nedeniyle maliyet ve kullanım açısından, resmin alınma süresinin uzun oluşu nedeniyle hız açısından dezavantajlara sahiptir. Bunun dışında elde bulunan yüzük gibi aksesuarlar, yara bandı gibi maddeler sebebiyle ya da yaralanma ve parmakların kaybedilmesi, gut veya kireçlenme gibi bir takım hastalıklar nedeniyle elin tanınması zorlaşır. Çocuklarda ve el ve ayakların çok hızlı büyüdüğü hastalıklara sahip olan kişilerde ise bu sistem kullanılamamaktadır.



**Şekil 3 :** El Geometrisi

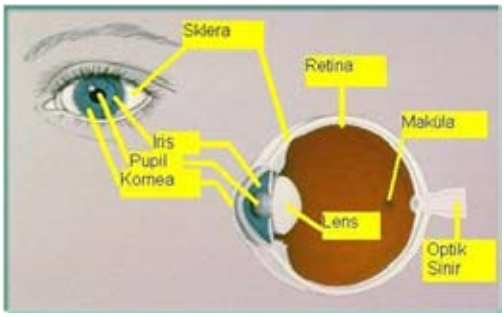
### 3.4 Yüz

Biyometrik teknolojide devrim sayılabilecek buluşlardan bir tanesi olan yüz tanıma sistemleri gelişen bir çok teknolojide olduğu gibi ilk kez askerîyede kullanılmıştır. Yüksek teknoloji silahlarının yönetimi için, özellikle ABD'de sıkça kullanılan bu sistemler bunun dışında, caddelere yerleştirilen güvenlik kameraları ile caddelerin izlenmesi ve aranmakta olan bir suçlunun bu şekilde yakalanması gibi uygulamalarda da kendilerine yer edinmişlerdir [12]. Özellikle son 10 yıldır uygulama alanlarının artması nedeniyle yüzlerin otomatik olarak tanınması popüler bir konu haline gelmiştir [13].

### 3.5 İris

Yaklaşık 30 senedir kullanılan iri tanıma sistemlerinin çıkış noktası, kişinin sahip olduğu iris şeklinin ömrü boyunca değişmemesi ve diğer biyometrik sistemlere göre gözün daha az deforme olacak ve dış etkenlerden daha az zarar görecek bir yapıya sahip olmasıdır. Uykusuzluk, gözyaşı, hastalıklar iris yapısını etkilemekle beraber diğer yöntemlerdeki kadar bariz bir etkilenme sözkonusu değildir. Elbette ki bu yöntem gözü olmayan, gözleri görmeyen, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan kişilerde uygulanamaz. Ancak bu kişiler dışında havaalanı gibi kimlik doğrulamanın mutlak surette önemli olduğu yerlerde oldukça yüksek bir doğruluk oranı ile uygulanabilmektedir.

Genel olarak parmakizi tanımaya benzetilen bu sistemin, parmakizine göre en önemli avantajı, parmak izi kullanılan biyometrik sistemlerde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karşılaştırma için yaklaşık 200 referans noktası kullanılmasıdır [14].




**Şekil 4:** Göz Yapısı

### 3.6 İmza

Bir kişinin, herhangi bir yazının altına sözkonusu bu yazıyı yazdığını, okuduğunu veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işaretler olarak tanımlanabilen imza kişiler tarafından yaşamları boyunca pek çok kez kullanılmaktadır. Özellikle hukuksal açıdan büyük yaptırımlarının bulunması ve taklit edilmesi sonucunda kişiyi borç altına sokabilmesi, tüm malvarlığını başka bir kimseye bağışlamasına sebep olması, işlemediği suçların üzerine kalmasına neden olması gibi sebeplerle hayatî önem taşımaktadır. Dolayısıyla kimlik doğrulamasında belki de en sık kullanılan yöntem olan imzanın gerçekten o kişi tarafından atılıp atılmadığının belirlenmesi önemli bir sorun olarak karşımıza çıkmaktadır. Bu sebeple kullanılan imza tanıma sistemlerinde imzayı tanımak için iki tip bilgi kullanılmaktadır. Bunlardan ilki imzalama süresi, hızı, ivmesi, kalemin basım şiddeti, kalemin gibi kişinin imzalama işlemi ile ilgili özellikler, diğeri ise bir desen olarak imzaya ait özelliklerdir. Bir imzayı taklit eden herhangi bir kişi desen olarak imzayı taklit edebilse bile imza atış şeklini (süre, ivme, kalemi yerden kaldırma miktarı vs) tekrarlaması güçtür. İmza tanıma sistemlerinin dezavantajları, sistemin kullanıcının hızını, imza atma davranışını vs öğrenebilmesi için uygun sayıda örneğe ihtiyaç duyması ve imza atımının kullanıcının o anki ruh haline, özellikle de acelesi olup olmadığına bağlı olarak değişmesidir.

## 4. Biyometri Tabanlı Yöntemler ile Diğer Yöntemlerin Karşılaştırılması

Kullanıcı kimliğini belirleyen diğer sistemler (bilgi temelli ya da aidiyet temelli) ile biyometrik sistemler benzer yönlere sahip olmakla beraber birbirlerinden ayrıldıkları noktalar da oldukça çoktur. Biyometrik yöntemler dışındaki yöntemlerin biyometrik yöntemlere göre en önemli dezavantajı kullanıcıya bazı bilgileri bilme ve hatırında tutma ya da bazı araçları sürekli olarak yanında taşıma, çaldırmama, unutmama gibi sorumluluklar vermesidir. Biyometrik sistemlerde böyle bir durum sözkonusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, nesnye vs ihtiyacı yoktur. Biyometrik sistemlerin diğer sistemlere göre avantajları, dezavantajları, benzer ve farklı yönleri kısaca aşağıdaki gibi ifade edilir [15].

- Diğer kimlik doğrulama yöntemlerinde kullanılan veri her kullanıcı için kesinlikle farklı ve eşsiz iken biyometrik veriler farklı olmakla beraber benzerliklere sahip olabilir.
- Diğer yöntemlerde kullanılan veri, kullanıcı tarafından değiştirilebilir (sistem yöneticisinin isteği üzerine, güncelleme amacıyla veya başka herhangi bir sebepten ötürü). Buna karşın biyometrik veri kişinin istemesi ile değiştirebileceği bir veri değildir, ancak kaza, hastalık vs geçirilmesi durumunda değişir.
- Biyometrik sistemler genelde ek bir donanım, yazılım gerektirdiğinden ek bir maliyet getirir iken diğer yöntemler genelde kullanılan mevcut sistemlerle uyumludur.

- Diğer yöntemler çalındığı veya benzeri bir duruma uğradığı zaman yenisi ile değiştirilebilir, oysa ki biyometrik veriler herhangi bir şekilde elde edildiğinde, geçerliliği kalmaz.
- Biyometrik veriler zaman içerisinde deformasyona uğrayabilir, buna karşın diğer yöntemler için böyle bir durum sözkonusu değildir.

Biyometrik sistemler dışındaki tanıma sistemlerinde verinin unutulması, çalınması, kaybedilmesi riski oldukça fazladır. Ancak biyometrik sistemlerde kullanılan veri kişinin fiziksel ya da davranışsal bir özelliği olduğundan bu tarz bir tehlike ile karşı karşıya kalma ihtimali yok denecek kadar azdır.

## 5. Sonuç

Bu çalışmada kağıt üzerinde yapılan pek çok işlemin dijital ortama geçirilmesi sonucunda bir gereksinim olarak ortaya çıkan dijital kimlik doğrulama yöntemlerinden biri olan biyometrik güvenlik yöntemleri incelenmiştir. Kişinin şifresini kendi üzerinde taşıması olarak ifade edebileceğimiz biyometrik güvenlik sistemleri, gerçek anlamda sosyal hayatta kısa bir zaman öncesinde kullanılmaya başlanmasına rağmen, her geçen gün daha fazla yerde kendini göstermektedir. Kişilerin parmak izi, iris, yüz gibi fiziksel sabit özellikler veya imza atış şekli, yürüme şekli gibi davranışsal özelliklerin herhangi birisini kullanan sistemler günümüzde oldukça rağbet görmektedir.

Kullanılan her güvenlik sisteminde olduğu gibi, biyometrik tabanlı güvenlik sistemlerinde de sistemin kullandığı herhangi bir yazılıma ya da donanıma yapılabilecek saldırılar mevcuttur.

Biyometrik verileri algılayan cihazlara yapılan saldırılar olduğu gibi, biyometrik verileri taklit etmeye yönelik saldırılar da bulunmaktadır. Ayrıca iletişim kanalı saldırıları ya da ma-in-the-middle saldırılar olarak adlandırılan ve kullanılan sisteme gizlice girip bilgi elde eden ve hatta bu bilgileri değiştiren saldırılar da biyometrik sistemler için birer tehdit unsurudur.

Bu saldırılardan korunabilmek kimlik doğrulama sağlayan sözkonusu biyometri sistemlerinde hayatî bir öneme sahiptir. Bu yüzden tüm bu saldırılar ve bunların kombinasyonları biyometrik güvenlik sistemlerinde iyi tanımlanmalı ve saldırılardan korunmak için gerekli önlemler alınmalıdır.

Günümüzde özellikle havaalanları, karakollar gibi güvenliğin yüksek olarak tutulması gereken noktalarda, şirket çalışanlarının şirkete giriş çıkışlarında ve bilgisayar gibi aletlerin kullanıcıyı tanıması sırasında kullanılan sistemlerin gelecekte kullanılması beklenen potansiyel kullanım alanlarından bazıları şu şekilde ifade edilebilir :

- Turizm: Yolcuların araçlar için bilet satın alma, otel odası rezervasyonu yaptırma ya da araç kiralama gibi çeşitli turizm hizmetlerinde kullanabilecekleri biyometrik sistemlerin tasarlanması yapılacak işleri oldukça kolaylaştıracaktır.
- İnternet: Bilgisayarlara biyometrik bir okuyucunun entegre edilmesi sayesinde internetten bankacılık işlemleri, resmî işlemler, pasaport vs başvuruları gibi dijital işlemlerin biyometrik kimlik doğrulama sayesinde yapılabilmesi işlemi fikri oldukça ön plana çıkmaktadır.
- Telefon: Telefon cihazlarına entegre edilecek bir aygıt ile kişinin telefon üzerinden işlemlerini gerçekleştirilmesi amaçlanmaktadır. Ancak, telefon cihazının, hatlarının ve kullanıcı ortamlarının sabit olmayışı bu yöntemi zor kılmaktadır.
- ATM: Pek çok kullanıcısı olan ve bu kullanıcıların sıklıkla işlem yaptığı bankalarda sahteciliğin boyutları göz önüne alındığında bankaların bu sorunu biyometri teknolojisi kullanarak çözmek uygun bir çözüm olarak görünmektedir.

Biyometrik güvenlik sistemleri, genelde ek maliyet getirmeleri, kullanımlarının bazen uzmanlık gerektirmesi, ele geçirildiği anda yenilenme şansı olmamasından dolayı geçerliliğinini kalmaması gibi dezavantajlarının yanında kişinin kendisi dışında ek bir bilgi, 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.

**Kaynaklar**

[1] Açık Anahtar Altyapısı ve Biyometrik Teknikler, Necla Özkaya, Şeref Sağıroğlu

[2] Bilgisayar Destekli Kimlik Tespit Sistemlerinde Biometrik Yöntemlerin Değerlendirilmesi Taha Saday, Nurdan Akhan

[3] http://www.turkeyforum.com/satforum/archive/index.php/t-202.html

[4] http://www.vizyotek.com/Teknoloji/Iris_Tanıma.htm

[5] Mücahit YOZGAT, "Bilgisayarda Parmak İzi Tanıma", Gazi Üniversitesi Elektronik ve Bilgisayar Bölümü, Yüksek Lisans Tezi

[6] www.incits.org

[7] Halici U.; Jain L. C.; Hayashi, I.; Lee, S.B.; Tsutsui T., Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC press, USA, 1999.

[8] http://www.haberler.com/birlesik-krallik-icin-vize-basvurusunda-biyometrik-haber

[9] Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi , Elena Battini Sönmez, Nilay Özge Özbek, Önder Özbek

[10] Otomatik Parmakizi Tanıma Sistemlerinde Kullanılan Önişlemler İçin Yeni Yaklaşımlar, Şeref Sağıroğlu ve Necla Özkaya, Gazi Üniv. Müh. Mim. Fak. Der. Cilt 21, No 1, 11-19, 2006.

[11] http://www.infomet.com.tr/handgeometry.aspx

[12] http://www.bildirgec.org/yazi/biyometrik-tanimlama-sistemleri

[13] http://www.yuztanima.net/

[14] shttp://www.turksan.com/biyometrik-sistemler-nedir.html

[15] E-Dönüşüm Türkiye Projesi 2005 Eylem Planı 6. Eylem Maddesi, "Akıllı Kartların Kamuda Kullanımı" Konusunda Ön Çalışma Raporu, TÜBİTAK-UEKAE, Ocak / 2006.