Düzce Üniversitesi
Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Biyometrik Güvenlik Sistemlerinin İncelenmesi

Nursel YALÇIN[a], Filiz GÜRBÜZ[b,*]

[a] *Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Eğitim Fakültesi, Gazi Üniversitesi, Ankara, TÜRKİYE*
[b] *Bilişim Enstitüsü, Gazi Üniversitesi, Ankara, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: gurbuz.flz@gmail.com*

ÖZET

Biyometrik sistemler, bireylerin fiziksel ve davranışsal özelliklerini tanımlayarak kimliklendirme yapan sistemlerdir. En yaygın kullanılanları ise parmak izi, el geometrisi, ses, retina, yüz, imza vb. biyometriklerdir. Bu sistemler günümüzde hava alanlarında, fabrikalarda ve yüksek güvenlik gerektiren binalar gibi alanlarda, giriş çıkışları kontrol etmede ya da girilen verileri onaylama gibi süreçlerde kullanılmaktadır. Bunun yanında yaşam içerisinde bireylerin hayatını kolaylaştıracak akıllı sistemlerde, dijital fotoğraf makinelerinde, e-ticarette, kriminal incelemelerde vb. birçok alanda kullanılmaktadır. Her bir sistemin kendi içerisinde avantajları ve dezavantajları bulunmaktadır. Bu nedenle bu tür teknolojilerin başarısını belirlemek özellikle güvenliğin ön planda olduğu durumlarda kritik faktörler öngörmek çalışmalara yardımcı olacaktır. Bu çalışmada da genel olarak kullanılan biyometrik sistemler araştırılmış ve incelenen güncel çalışmalar içerisinde bu sistemlerle ilgili karşılaşılan sorunlara, biyometrik sistemlerinin birbirlerine göre avantajlarına yer verilmiş ve değerlendirmelerde bulunulmuştur.

Anahtar Kelimeler: *Biyometrik sistemler, Biyometrik analiz, Parmak izi tanıma, İmza tanıma, Ses tanıma, İris tanıma*

Analysis of Biometric Security Systems

ABSTRACT

Biometric Systems is systems which make identification by describing physical and behavioral features of individuals. The most widespread ones, which are used, are the biometrics of finger print, hand geometry, voice, retina, face and etc. These systems are now used in the areas such as airports, buildings and etc. which require high security and in the processes such as controlling of entrances and exits or confirming data entered in the digital environment. Besides, they are used in many fields such as smart systems, digital cameras, e-commerce, criminal investigation and etc. There are many different biometric systems and every system has advantages and disadvantages itself. So, the success of this kind technology should be evaluated and critical factors should be predicted especially in the situations which the security is at the forefront. This study includes general information about biometric systems which are widely used and advantages and disadvantages of them.

Keywords: *Biometric systems, Fingerprint recognition, Signature recognition, Voice recognition, Signature recognition, İris recognition*

Geliş: 11/02/2015, Düzeltme: 06/03/2015, Kabul: 16/07/2015

I. GİRİŞ

MODERN yaşam ve artan teknoloji kullanımı beraberinde güvenlik tedbirlerine olan ihtiyacı da artırmaktadır. Artan güvenlik ihtiyacı ile birlikte biyometrik güvenlik sistemlerine olan ilgi de artmaktadır. Biyometrik güvenlik sistemlerinde kişilerin kimlik ispatı için yanlarında taşımak, kaybetmemek ya da unutmamak zorunda oldukları kart, anahtar ya da şifre gibi araçların yerine, bireyin unutması, kaybetmesi, kopyalanması ya da taklit edilmesi daha zor olan fiziksel ya da davranışsal özelliklerine dayalı bir analiz sistemi kullanılmaktadır.

Parmak izi, el geometrisi, avuç içi, yüz, iris, retina, ses, ıslak imza gibi biyometrik veriler, bir bireyi tanımlamak için teknolojiden de faydalanarak kullanılan temel biyometriklerdir.

Bu çalışmada incelenen ilgili çalışmalardan elde edilen bilgiler ışığında biyometrik tabanlı güvenlik sistemleri, kullanılabilirlikleri açısından avantajları ve dikkat edilmesi gereken noktaları ele alınarak incelenmiştir.

II.BİYOMETRİK SİSTEMLER

Biyometri, insanları birbirinden ayırt edebilecek fiziksel ve davranışsal özellikleri inceleyen bilim dalıdır [6]. Biometri kelimesi, Yunancada yaşam anlamına gelen "Bios" ve ölçü anlamına gelen "Metron" kelimelerinin birleşmesinden oluşmaktadır [7].

Biometrik sistemlerin basit halleri ile uygulanması aslında çok eski zamanlara dayanmaktadır. Binlerce yıl öncesinde Nil Vadisi'nde tahıl ve erzakların merkezi bir depodan sağlandığı tarım sektöründe ve bununla ilgili hukuki işlemlerde biyometrik veriler kullanılmıştır. Bireyler yara gibi ölçülebilen parametreleri ya da ten rengi, göz rengi ve boy uzunluğu gibi kendilerine has fizyolojik özellikleri ile tanımlandığı belirtilmektedir [18].

19. Yüzyılda kriminoloji araştırmacıları tarafından fiziksel özellikler ve karakteristiklerin kriminal eğilimlerle ilgisi olup olmadığının araştırılması bu alana olan eğilimi artırmıştır. Bu araştırmalar sonucunda birçok ölçüm aleti üretilmiş ve birçok veri toplanmıştır. Kesin sonuçlara ulaşılamasa da bireylerin fiziksel özelliklerinin ölçülmesi kabul görmüş ve polis tarafından kimlik tespitinde parmak izinin kullanılması uluslararası bir metodoloji olmuştur [18].

Kimlik tanımlama işleminin otomatik olarak gerçekleştirilebilmesi durumu uzun süre askeri ve ticari sektörleri meşgul etmiştir. Biyometri endüstrisi üreticilerinin satışlarını etkinleştirmesi biyometrik güvenlik sektöründe çalışan firma sayının artması ile bu alandaki çalışmalar gelişmiştir.

Biyometrik sistemler fiziksel ve davranışsal olmak üzere iki temel gruba ayrılmaktadır [8,14]. Fiziksel biyometrikler; iris, yüz, parmak izi, retina, el tanıma vb. sistemleri ele alırken, bireyin davranışsal özelliklerini temel alan davranışsal biyometri ise; ses ve el yazısı, ıslak imza vb. sistemleri ele almaktadır. Bazı kaynaklarda biyometrik özellikler fizyolojik, biyokimyasal ve davranışsal özellikler olarak üçe ayrılmaktadır. Genellikle göz ile görülen insan bedenine ait bir parçasının fiziksel özelliklerinin ölçülerek elde edilen veriler fizyolojik özelikler olarak tanımlanmaktadır. Fizyolojik özelliklere yüz, iris, retina, el geometrisi, kulak şekli, parmak izi, avuç içi, cilt gözenekleri, kılcal damar yapısı ve toplardamar yapısını kapsamaktadır. İnsan bedeninin belirli bölümlerinin kimyasal yapı özelliklerinin ölçülüp değerlendirilmesi ile elde edilen veriler biyokimyasal özellikler olarak

tanımlanmaktadır. Vücut ısısı, vücut kokusu, kalp ritmi, DNA yapısı ve yüz ısısı biyokimyasal özelikler olarak ifade edilmektedir. İnsanın belirli bir fiziki davranışının ölçülüp değerlendirilmesi ile elde edilen özelliklere de davranışsal özellikler denilmektedir. Yürüme biçimi, konuşma sesi, imza, el yazısı ve tuş vuruşları/yazma ritmi gibi özelliklerde davranışsal özellikler olarak ifade edilmektedir [11].

Literatürde, bir biyometrik özelliğin sorgulandığı sistemler "tekli model biyometrik sistemler" olarak adlandırılırken birden çok biyometrik özelliğin sorgulandığı sistemler "çoklu model biyometrik sistemler" olarak adlandırılmaktadır. Örneğin; ses ve yüz tanıma analizinin bir arada yapıldığı bir sistem, çoklu model biyometrik sistem olarak tanımlanmaktadır.

Biometrik sistemler;

İnternet bankacılığında kullanıcı tanımlama
Çağrı merkezlerinde kimlik tespiti
Hastanelerde hasta takibi
İş yerlerinde personel devam takibi
ATM'lerde kullanıcı tanımlama
Sigorta şirketlerinde kimlik tespiti
Havaalanları giriş çıkış işlemleri
Sınır kapılarında girişlerin kontrolü
Kiralık kasalara erişim güvenliği
Askeri kaynakların etkin takibi
Kombine bilet uygulamaları
Hastanelerde hasta takibi ve kimlik saptama
Sigorta firmalarında kimlik saptama
Masaüstü ve dizüstü bilgisayarlarda bilgi güvenliği
E-ticaret işlemleri
Yüksek güvelik gerekli binaların giriş çıkış işlemleri
Uzaktan eğitim sınav işlemleri
Ulusal kimlik uygulamaları, sürücü ehliyet ve pasaportlarda kimlik tespiti
Fotoğraf makineleri
Cep telefonları
Akıllı ev sistemleri

gibi birçok farklı alanda kullanılmaktadır.

İnsan karakteristik özellikleri, aşağıda verilen özellikler açısından kullanılabilir ise biyometrik güvenlik sistemi için de kullanılabilirdir.

Evrensellik: Her insanın sahip olduğu bir biyometrik karakteristik olmalıdır [8,22].
Teklik/Eşsiz Olma: Biyometrik karakteristiğin her insanda diğer insanlardan ayıracak farklı bir şekilde yer almasıdır [8,22].
Süreklilik: Karakteristiğin zamanla değişmemesidir [8,22].
Elde edilebilirlik(Collectability): Karakteristik ölçümün kolay elde edilebilirliğidir [8,22].
Performans (Performance): doğruluk, hız ve kullanılan teknolojinin sağlamlığıdır [8].
Kabul Edilebilirlik(Acceptability): Teknolojinin onay derecesidir [8]. Bir başka deyişle, bireyin biyometriğin ölçüm ve toplanmasında itirazların olmaması [22] olarak da tanımlanmaktadır.
Atlatma/Tuzak (Circumvention): Yedeğinin, yerine kullanım kolaylığıdır [8].

Biyometrik yöntemlerinin kullanım amaçlarına göre üç ayrı kullanımı mevcuttur. Birinci yöntem de bire-çok (1αN) karşılaştırma yapılır. Bu işlem veri tanıma(identification) ya da algılama(recognition) olarak tanımlanmaktadır. Sisteme giriş yapmaya çalışan kullanıcı bilgisi, sistemde daha önce tanımlanmış kullanıcı bilgilerinin hepsi ile karşılaştırılır ve bu bilgilerden herhangi birine karşılık gelmesi durumunda sistem giriş onayı verir. İkinci yöntemde ise bire-bir (1α1) karşılaştırma yapılır. Bu işlem veri doğrulama(verification) olarak tanımlanmaktadır. Sisteme girilen biyometrik veri ile birlikte kullanıcıdan ikinci bir veri(kimlik numarası gibi) daha alınır. Sistemde kayıtlı olan veriler içerisinden ikinci verinin karşılığındaki biyometrik veri ile sisteme giriş yapmaya çalışan kişiden sistemin aldığı veri karşılaştırılır ve uygun olması durumunda sistem giriş onayını verir. Bire-çok karşılaştırma yönteminde veri tabanındaki kıyaslama yapılacak kayıt sayısı fazla ise sistem hantallaşacaktır. Bu bire-çok yönteminin dezavantajıdır. Bire-bir karşılaştırmada ise sistemin çok sayıda karşılaştırma işlemi yapmaması için kullanılan ikinci verinin(kimlik numarası, şifre, akıllı kart vb.) unutulma ya da kaybedilme riski vardır. Üçüncü yöntem ise sınıflandırma(classification) yöntemidir. Bu yöntemde büyük veri tabanlarında biyometrik girdiler benzer özelliklerine göre gruplandırılmaktadır.

Veri tabanlarında kişilere ait biyometrik verilerin saklanması çeşitli problemleri de beraberinde getirmektedir. Veri tabanlarında kayıtlı, kişilere ait biyometrik verilerin çalınması durumu sistem yöneticileri ve üreticiler için problem oluşturmaktadır. Bu tür problemler için sunulan çözüm biyometrik verinin kullanıcısının taşıyacağı bir taşınabilir bellek üzerinde bulunması ve kullanılacak sistemde taşınabilir bellek içerisindeki verinin kişi biyometriği ile karşılaştırılmasıdır.

Biyometrik sistemler hassas olmalıdır. Ama sistem karşılaştırması sırasında %100 uygunluk söz konusu olmayabilir. Kullanılan cihazın kirlenmesi, ortam nemliliği, verinin elde edilmesi ya da iletilmesi sırasında oluşan istenmeyen gürültüler gibi dış faktörlere bağlı olarak tamamen aynı kod üretilemeyebilir.

Biyometrik sistemlerin genel çalışma mekanizması adımları;

- Veri toplama
- Veri iletimi
- Öznitelik çıkarımı
- Modelleme-ID kod oluşturma
- Karşılaştırma

olarak sıralanır.

Biyometrik sistemlerin oluşturulabilmesi 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 [17]. Oluşturulan bu standart sayesinde, bir ülkede bir banka hesabı bulunan ve bu hesaba parmak izi ile erişebilen bir kişi, dünyanın başka bir ülkesindeki bir bankanın bankamatiğinden de kendi ülkesindeki hesabına ulaşarak işlem yapabilecektir.

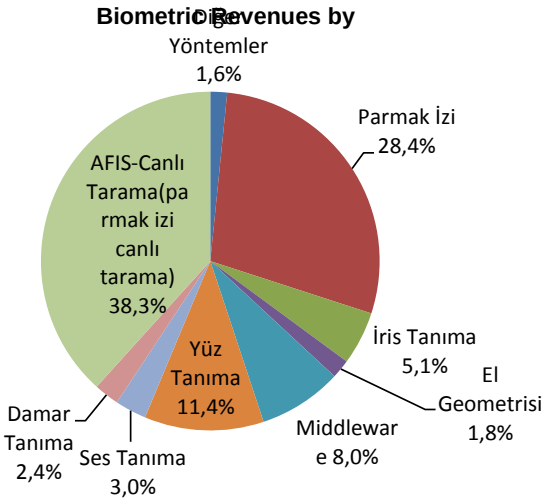
Yaygın olarak kullanılan biyometrik sistemler; parmak izi, el geometrisi, yüz, iris, retina, ses, imza olarak sıralanabilir. Bunların dışında damar tanıma, el yazısı tanıma, yürüyüş tanıma, el ve damar tanıma, kulak biyometriğine göre kimlik tespiti, tuş vuruşu gibi daha pek çok çeşitli yöntem de biyometrik sistemler arasında yer almaktadır.

A. PARMAK İZİ

Genel olarak bir parmak izinin her kişi için benzersiz olduğu bilinmektedir ve bu nedenlide kimlik doğrulaması için güvenli bir yöntem olarak düşünülmektedir [3]. Parmak izi sırtlar serisi ve oluklardan oluşmaktadır. Bunlar birbirinden farklı ve değişmezdir. Özdeş ikizler de dahi parmak izleri birbirinden farklıdır.

Parmak izi tanıma sistemlerinin en önemli sorunu, taklit parmak izinde sistemin yanılmasıdır [17]. Bu sorunu ortadan kaldırmak için parmak izinin alındığı parmağın canlılığını test edecek gelişmiş sensörlerin kullanımı önerilmektedir [17]. Bu nedenle sadece parmak ucu desensel ayrıntılarının ilgilenilmesinin yanında çok daha detaycı ve gelişmiş sistemler geliştirilmektedir. Örneğin termal görüntüleme sistemlerinde parmağın ısısından faydalanılır ve parmağın canlılığı test edilir. Parmak izi tanıma ile ilgili bir diğer sorun ise bazı kişilerin deri hastalıkları, organ eksikliği, yanma gibi sebeplerden ötürü parmak izlerinin bulunmamasıdır [17].

Uluslararası Biyometrik grubun (International Biometric Group) yapmış olduğu 2009-2014 biyometri pazar ve sanayi raporunda 2009 yılında kullanılan biyometrik teknolojilerin içerisinde, otomatik parmak izi teşhis sistemi ve parmak izi tanıma sistemleri Şekil 1'de gösterildiği gibi biyometrik pazarda önemli bir paya sahip olduğu görülmektedir [1].



Şekil 1. *Uluslararası Biyometrik Grubun 2009-2014 Biyometri Pazar ve Sanayi Raporu [1]*

Şekil 1'de görülen Uluslararası biyometrik grubun yapmış olduğu 2009-2014 biyometri pazar ve sanayi raporu verisi pasta grafiğinde 2009 yılında kullanılan en büyük biyometrik %38.3 ile canlı parmak izi tarama olarak görülmektedir. İkinci en büyük payı ise %28.4 ile parmak izi tanıma almıştır.

Parmak izi tanıma sistemleri daha çok kampüs yemekhaneleri, yurtları ve binaları gibi giriş çıkış kontrol sistemlerinde kullanılmaktadır.

Rutgers Üniversitesi (ABD), araştırma cihazlarını gözlemlemek ve kontrol etmek için parmak izi tarama sistemini kullanmaktadır [1].

Bentley Üniversitesi (ABD), öğrencilerinin kullandığı ve fakültelerinde sahip oldukları bilgisayarlarında parmak izi tanıma sistemini kullanmaktadır. Kullandıkları bu sistem sayesinde, unutulan ya da paylaşılan kullanıcı adları ve şifrelerin sonucunda oluşabilecek güvelik riski azaltılır [1]. Ayrıca kullanıcılar içinde hesaplarına ulaşım çok daha kolay olur.

Resim 1'de farklı marka ve özelliklerdeki parmak izi okuyucu sistemleri görülmektedir.

Resim 1. *Farklı Marka ve Özellikdeki Parmak İzi Okuyu Sistemleri*

B. EL GEOMETRİSİ

Bu biyometrik yaklaşımda bireyin kimliğini doğrulamak için elin geometrik formu kullanılır [3]. Parmakların uzunluğu, eni, büküm yerleri ayırt edici özellikler olarak kullanılmaktadır. El tarama için bir CCD (Charge-Coupled Device) kamera gereklidir. Bu kamera, elin üstünden ve yanından fotoğraflarını alarak bir şablon oluşturur. Oluşturulan bu şablon veri tabanındaki kayıtlar ile kıyaslanır.

El geometrisinin diğer biyometrik sistemlere göre kullanımı daha kolaydır [18]. Bu nedenle daha çok kullanıcı yoğunluğunun fazla olduğu yerlerde tercih edilmektedir.

El taraması için kullanılacak cihazlar diğer biyometrik yöntemler için kullanılan cihazlara göre kaplayacağı alan daha büyüktür. Bu cihazlar en azından bir el büyüklüğündedir. Bu nedenle alan kullanımının önemli olduğu durumlarda tercih edilmemektedir. Örneğin; dizüstü bilgisayarlarda bilgi güvenliği için parmak izi okuma sistemi gibi biyometrik sistemler kullanılmaktadır. Bu tür sistemlerde el izi tanıma sisteminin kullanılması teorikte mümkün olsa da pratikte kullanılması uygun değildir.

El geometrisi yaklaşımı ile kullanılan güvenlik sistemlerine örnek:

1996 yılı olimpiyat oyunlarında personel taraması
San Francisco havaalanı personel taramaları
New Hampshire Üniversitesi (ABD) yemek salonlarında bulunan el okuma sistemi [1].
Keene State College (ABD) yemek salonları [1].

El geometrisi tanıma, yüksek doğruluk oranına sahip bir yöntem olmakla birlikte büyük ve ağır okuma cihazı nedeniyle maliyet ve kullanım açısından dezavantajlara sahiptir [17]. Ayrıca yaralanma, parmakların kaybedilmesi, gut veya kireçlenme gibi bir takım hastalıklarda sistemin çalışma performansını etkileyen olumsuzluklardandır. Resim 2'de farklı marka ve özelliklerdeki el izi okuyucu sistemleri görülmektedir.

Resim 2. *Farklı Model ve Özellik deki El Geometrisi Okuyucu Sistemleri*

C. AVUÇ İÇİ TANIMA

Avuç içi, kişilere özgüdür [21]. Avuç içi tanıma sistemlerinde, avuç çizgilerinin özelliklerinin belirlenmesi üzerinde durulur. Çizgilerin eğimleri, karşılıklı ilişkileri, konumları ve sayıları gibi nitelikler çalışmalarda kullanılır. Resim 3'te farklı model ve markalardaki avuç içi tanıma sistemleri gösterilmektedir.

Resim 3. *Farklı model ve özelliklerdeki avuç içi tanıma sistemleri*

Avuç içi tanıma sistemleri daha az sayıda veriyi daha kısa sürede işlemektedir [21]. Bu nedenle işlem süresi kısadır. Kullanıcı ve sistem etkileşimi basit olması nedeniyle hata kayıt oranları da küçüktür. Ayrıca avuç içi tarama teknolojileri yüksek kullanıcı kabulüne sahiptir [22]. Avuç içi tanıma sistemlerinin kolay, maliyeti düşük teknolojiler ile gerçekleştirilmesi ve kullanımının da kolay olması bu biyometriğin diğer avantajlı yönleridir.

D. YÜZ TANIMA

Kişi tanıma için yüz biyometrik karakterleri yaygın olarak kullanılan bir yöntemdir [3]. Çoğunlukla kullanılan yaklaşım temel olarak yüzün gözler, kaşlar, burun, dudaklar, çene şekilleri ve bunlar arasındaki ilişkilerine dayanmaktadır.

Yüz tanıma sistemlerinde, görüntü yakalama cihazı(kamera) ile herhangi bir fiziksel temas gerektirmemesi bu yöntemin bir avantajıdır.

Yüz tanıma;

- Alzheimer hastalarının gördüğü kişiyi tanımasına yardımcı olmak için kullanılmaktadır. Bunun için Alzheimer hastasının gözlüğüne yerleştirilen küçük bir kamera ve yüz tanıma yazılımı kullanılmaktadır [1]. Benzer cihazlarla güvenlik güçleri tarafından suçlu tanıma ve tespiti için de kullanılmaktadır.
- Web ortamında sosyal paylaşım sitelerinde, Microsoft Photo Gallery, Google Picasa gibi ticari uygulamalarda fotoğrafla etiketlemede yüz tanıma uygulamaları kullanılmaktadır [1].
- Halka açık alanlarda suçlu ve terörist araması [1]

gibi birçok farklı alanda kullanılmaktadır.

Bu sistemde yüzün çok sayıda özellik içermesi ve çok fazla karşılaştırma yapılması nedeniyle eşleştirme zordur [3]. Resim 4'de farklı marka ve özelliklerdeki yüz tanıma sistemleri görülmektedir.

Resim 4. *Farklı Marka ve Özellik deki Yüz Tanıma Sistemleri*

E. İRİS TANIMA

İris gözün içindeki dairesel renkli bölgedir. Kişinin yaşamı süresince değişmediği gerçeğinden yola çıkılarak geliştirilen bir sistemdir.

İris tabakası her insanda farklılık gösterir. Tek yumurta ikizleri aynı DNA yapısına sahip olsa da farklı iris tabakalarına sahiptir [15]. Bu tabaka bir insanın her iki gözünde de farklılık göstermektedir [18].

İris insanın doğumunun 16. haftasından ölümüne kadar değişmez. İnsanın yaşamını yitirmesinden sonra en çabuk (3 sn) canlılığını yitiren organ gözdür [15]. Ayrıca iris, dış ortamdan izole edilmiş olup cerrahi müdahaleler ile de değiştirilememektedir [4].

Bu sistemde çok sayıda referans noktası kullanılabilmektedir. Örneğin kesin bir doğruluk için parmak izi kullanılan biyometrik sistemlerde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karşılaştırma için yaklaşık 200 referans noktası bulunmaktadır [17].

İris tanıma kullanacak sistemlerde karşılaşılan sorunlar arasında; gözleri görmeyen, Nistagmus hastalığına sahip (gözleri titreyen) veya irisleri olmayan kişilerin kimliklendirilmelerinin mümkün olmaması gelmektedir. Bir diğer sorun ise iris resmi alınırken göz kapaklarının veya kirpiklerin iris desenini bozması gibi faktörlerin sistemi olumsuz etkilemesidir. Ayrıca, iris görüntüsü alınması sırasında belirli bir miktarda ışık yayılmakta olup bu ışığın günlük yaşantıda insanları rahatsız edici etkisi vardır [4].

F. RETİNA TANIMA

Retina tanıma işlemi insanın göz bebeği arkasındaki damar tabakanın tanınmasıdır [1]. Bazı hastalıklardan dolayı damar yapısının çok kolay etkilenmesi ve bozulabilmesi bu yöntemin en büyük dezavantajıdır. Resim 5'te farklı marka ve özelliklerdeki göz ve retina tanıma sistemleri görülmektedir.

Resim 5. *Farklı Marka ve Özellik deki İris ve Retina Tanıma Sistemleri*

G. SES TANIMA

Davranışsal biyometrik sistemlerdendir. Genel olarak bir ses sinyali, konuşanın ağzından dinleyenin kulağına doğru giden bir hava basınç dalgasıdır [23]. Bu dalganın kişinin anatomik, fizyolojik ve psikolojik yapısına göre ayırt ediciliği mevcuttur.

Ses ile ilgili tanıma çalışmaları ses tanıma ve konuşmacı tanıma olarak sınıflandırılabilir. Bunlardan güvenlikle ilgili olan kısmı konuşmacı tanımadır.
Sadece belirli kişilerin seslerine cevap veren cihazlar, güvenliği gerekli olduğu binalardaki kapılar veya güvenlik kuruluşlarında ses kaydından konuşan kişinin kimliğinin belirlenmesi gibi alanlarda kullanılmaktadır [11].

Konuşmacı tanıma, metne dayalı tanıma ve metin bağımsız tanıma olarak ikiye ayrılmaktadır. Metne dayalı konuşmacı tanıma işleminde belirli bir metnin söylenmesi ve bu metne bağlı olarak tanıma işleminin gerçekleştirilmesi sağlanır. Metin bağımsız konuşmacı tanımada ise belirli bir metnin seslendirilmesi gerekmez [19].

Bu yöntemin dezavantajı genel olarak çalışma koşullarının uygun olmamasından kaynaklanmaktadır. Konuşmacıların sisteme kaydedilmesi için konuşma sinyalinin herhangi bir sebeple bozulmaya uğramayacak şekilde sağlıklı bir ortam sağlansa ve kayıtlar bu ortamda alınsa da sistemde sonradan kullanılacak veri kayıt ortamı birçok durumda denetlenememekte ve ortamda istenmeyen gürültülerin yer alması gibi durumlardan sistem olumsuz etkilenmektedir. Ayrıca insanın değişik durumlarda farklı tonda ve vurguda konuşmaları, duygusal koşulların değişmesinin sese yansıması sonucu çıkarılan seslerin farklı olması ve rahatsızlık gibi bazı olumsuz durumlarda, sesin değişmesi sistemi olumsuz etkileyen diğer dezavantajlardır [19].

H. İMZA TANIMA

Kimlik doğrulanmasında güvenilir bir metot olarak tanımlanan ve uzun zamandır kullanılan imza kişinin kendi ismini yazma şekli olarak tanımlanmaktadır [17]. İnsanlar davranışsal biyometrik sistemlerden biri olan imzalarını sosyal hayatın birçok aşamasında kullanmaktadırlar.

Çevrimdışı sistemler ve çevrimiçi sistemler olmak üzere imza tanıma ikiye ayrılır. Çevrimiçi sistemlerde yazma sırasında, hareket dedektörleri ile kalem hareketleri değerlendirilerek tanıma yapılır. İmza doğrulama için birçok elektronik ekipmana ihtiyaç duyulur. Basınca duyarlı tabletler imzanın dinamik özellikleri ve şeklini yakalar. İmzalama süresi, hızı, ivmesi, kalemin yüzeye uyguladığı basınç şiddeti tanımlamada kullanılan önemli özelliklerdir.

Çevrim dışı imza doğrulama sisteminde ıslak imzanın analizi sonucu tanıma gerçekleştirilir. Çevrimdışı imza tanıma sisteminde, çevrimiçi imza tanıma sistemlerine göre daha az sayıda ekipmana ihtiyaç duyulur. Bu alan bir desen olarak imzaya ait özellikleri inceler.

Bu sistemlerin dezavantajları olarak; sistemin kullanıcının hızını, davranışsal özelliklerini ve diğer özelliklerini öğrenebilmesi için çok sayıda uygun örneğe ihtiyaç duyması ve imza atımının hayat boyu sabit kalmayıp zaman içerisinde yaşlanmaya, sağlık durumuna ve ruh haline göre değişen bir biyometrik olmasıdır.

Çevrimdışı imza tanıma sistemlerinde ıslak imzanın desensel özelliklerinin öğrenilebilmesi ve taklit edilmesi de sistemin bir diğer dezavantajıdır. Bir başka dezavantajı ise bazı kişilerin imzalarını desensel olarak sık sık değişmesi ya da faklı alanlarda iş hayatı, sosyal hayat gibi farklı imza modelleri kullanmayı alışkanlık edinmeleri de gösterilebilir.

El yazısı ve imza tanıma sistemleri diğerleri kadar geniş kullanım alanı olmayan, genellikle belge kullanılan güvenlik sistemlerinde tercih edilen bir sistemdir. Fakat finansal alanlarda otomatik imza tanımanın önemi artmakta el yazısı ve imza tanıma çalışmaları ilerlemektedir.

I. DNA TANIMA

Deoksiribonükleik asit (DNA) biyometri herhangi bir bireyi tanımlamanın en kesin formu olabilmektedir. Her insan her hücresi için bir kişisel haritaya sahiptir ve bu harita diğer adıyla blueprint her vücut hücresinde bulunabilmektedir.

Kişinin saç, tırnak, deri, sperm, kan, tükürük vb. biyolojik materyallerin incelenmesi sonucu içinde bulunan DNA moleküllerindeki dizilim incelenir. Özellikle emniyet güçleri tarafından olay yeri inceleme sonucu bu alandan bulunan biyolojik materyallerin incelenmesiyle suçlulara ulaşılır. Ya da hukuki olaylarda babalık davalarının sonuçlanması işlemlerinde kullanılmaktadır. Doğruluğu çok yüksek bir yöntemdir.

DNA'nın elde edileceği biyolojik materyalin kirlenmesi örnek kalitesini düşüreceğinden analiz yapmak zorlaşır. Bu biyometriğe ait bir diğer dezavantaj ise DNA inceleme işlemlerinin 24 saat gibi uzun bir sürede gerçekleştirilmesi ve yüksek maliyetli olmasıdır [11].

J. YAZMA/ TUŞ BASMA RİTMİ TANIMA

Bir insan klavye üzerinde yazmaya başladığında, klavye üzerinde gezinmesi de tıpkı bir yazma hareketi ritmi gibi kişiye ait farklılıklar içerir. Bu yöntemde kullanıcı yazı yazarken klavyeden girilen karakterler arasında geçen zamanı ölçerek kullanıcıların yazma ritimleri tespit etmeye çalışılmaktadır.

Bir kullanıcıdan klavye ile "stephenson" yazılması istenmiş ve yazılma aşamasında geçen süreler tespit edilmiştir. Kullanıcı, "t" ve "e" karakterleri arasında oldukça zaman kaybederken "n" ve "s" ya da "s" ve "o" karakterleri arasında geçişi oldukça hızlı yapabilmektedir [11].

Bir yazma ritmi sistemi tasarlamak için ihtiyaç duyulan tek girdi aygıtı sadece klavyedir. Diğer biyometrik sistemlere kıyasla bu sistemin avantajı kendisine has bir donanıma ihtiyaç duymamasıdır.

Yazma ritmi sistemlerinin en büyük dezavantajı ise karar verme için sadece tek bir parametre kullanmasıdır. Sadece tuş aralıklarını değil tuşlara basılırken geçen sürenin tespiti yazma ritmi çalışmalarında güvenilirlik oranını artıracaktır [11].

III. ÇOKLU BİYOMETRİK SİSTEMLER

Birden fazla biyometriğe ait teknoloji birleştirilerek çoklu model biyometrik sistemler oluşturulur. Bu tür sistemlerin oluşturulmasının amacı güvenliği daha üst seviyelere çıkarabilmektir. Birden fazla sensöre, veri tabanına, analize, ekipmana sahip olunması gerektiği için maliyeti tekli biyometrik sistemlere göre daha fazladır. Resim 6'da parmak izi ve yüz tanıma sistemlerinin birlikte yer aldığı çoklu biyometrik sistem görülmektedir.

Resim 6. *Parmak İzi ve Kartlı Yüz Tanıma Sistemi*

Çoklu biyometrik sistemlere verebileceğimiz bir diğer örnek; gözlüklere yerleştirilen kameralar aracılığıyla ortamdaki ses ve görüntülerin bluetooth ile başka bir sisteme aktarılıp buradaki yazılımlar aracılığıyla görüntü ve ses tanıma işleminin gerçekleştirilmesi olarak verilebilir. Buna ait bir örnek Resim 7'de görülmektedir.

Resim 7. *Ses ve Görüntü Aktarımı Yapabilen Bir Gözlük*

IV. BİYOMETRİK SİSTEMLERİN KARŞILAŞTIRILMASI

Yapılan araştırmalarda karşılaştırılan biyometrik sistemler için bazı istatistiksel ölçümlere rastlanılmıştır [3,8,12,14]. Bu ölçümler;

FRR (False Rejection Rate): Yetkili kullanıcıyı reddeder. Yanlış reddetme oranıdır. İyi bir biyometrik kimliklendirme sistemi için bu değer düşük olmalıdır.

FRR= Yanlış red sayısı / istemci erişim sayısı

FAR (False Acceptence Rate): Yetkili olmayan kişi kabul eder. Yanlış kabul etme oranıdır. İyi bir biyometrik kimliklendirme sistemi için bu değer düşük olmalıdır.

FAR= Yanlış kabul sayısı / istemci erişim sayısı

FTE (Failure to Enroll): Yeni kullanıcı kimlik oluşturmak istenildiğinde başarısız olunur. Kayıt için arıza oranıdır. İyi bir biyometrik kimliklendirme işlemi için azaltılmış olmalıdır.

ERR (Equal Error Rate): Eşit hata oranıdır. FRR/FAR hesaplanarak bulunur. İyi bir biyometrik kimliklendirme sistemi için bu oran düşük olmalıdır.

ERR=FRR/FAR

Tablo 1'de farklı biyometrik sistemlerin güvenlik sistemleri için kullanılabilirlik özellikleri yüksek, orta ve düşük olarak sınıflandırılmıştır. Bu tabloda; Y=Yüksek, O=Orta, D=Düşük olarak ifade edilmektedir.

Tablo 1. *Biyometrik sistemlerin kullanılabilirlik özelliklerinin sınıflandırılması [8,12].*

	Evrensellik	Eşsizlik	Süreklilik	Elde Edilebilirlik	Performans	Kabul Edilebilirlik	Yaygınlık
DNA	Y	Y	Y	D	Y	D	D
Kulak	O	O	Y	O	O	Y	O
Yüz	Y	D	O	Y	D	Y	Y
Yüz Termogramı	Y	Y	D	Y	O	Y	D
Parmak izi	O	Y	Y	O	Y	O	O
El Geometrisi	O	O	O	Y	O	O	O
Iris	Y	Y	Y	O	Y	D	D
Retina	Y	Y	O	D	Y	D	D
İmza	D	D	D	Y	D	Y	Y
Ses	O	D	D	O	D	Y	Y

Y: Yüksek, O: Orta, D: Düşük

Tablo 1'e bakıldığında imza biyometriğinde evrensellik özelliği düşük olarak ifade edilmektedir. Organ kayıpları gibi nedenlerden dolayı imza atma yeteneğine sahip olunamamasından ya da okuma yazma bilmeyen kişilerin kendilerine ait bir imza formu oluşturmayıp yerine parmak izi ve mühür gibi yöntemleri kullanmaları gibi nedenlerden dolayı bu özellik düşüktür. İrisi, DNA, Yüz, Retina biyometriklerinin sahip oldukları özellikler bakımından evrenselliği yüksel olarak sınıflandırılmaktadır.

Eşsizlik yani her insanda diğer insandan farklı bir şekilde yer alması özelliği açısından baktığımızda DNA, yüz termogramı, parmak izi, iris, retina biyometrikleri aynı yumurta ikizi kardeşlerde dahi farklı olduğundan dolayı yüksek olarak sınıflandırılmıştır.

Süreklilik özelliği bakımından değerlendirildiğinde DNA, parmak izi, iris biyometrikleri yüksek olarak sınıflandırılmaktadır. Bu özellikler insan yaşamı boyunca sabit kalır fizyolojik ya da psikolojik bir etkene bağlı olarak değişmezler. İmza ve ses biyometrikleri ise Emosyenel durum (neşe, üzüntü, heyecan, stres, korku, kızgınlık gibi…) Çevresel koşullar (soğuk hava, yazı yazan kişiye anlık müdahale ile duraksama gibi…) ve anlık değişimlere bağlı olarak değişim göstermeleri ya da zamana bağlı olarak değişim içinde olması ya da kasıtlı olarak değiştirilme durumlardan ya da bazı hastalıklar ve bazı evrelere bağlı olarak meydana gelen değişiklikler nedeniyle bu özellikler hayat boyu aynı kalmamaktadır. Bu nedenle süreklilik özellikleri düşüktür.

Elde edilebilirlik özelliği bakımından en düşük olarak sınıflandırılan biyometrik iristir. Gözün hassas yapısı kullanılan cihazın temasının ya da kullanılan ışınların verdiği rahatsızlık gibi nedenlerden dolayı iris görüntüsünün elde edilebilirliği diğer biyometrik karakteristiklere göre zordur. En kolay elde edilebilir biyometrik özellikler yüz, el geometrisi ve imzadır.

Doğruluk, hız ve kullanılan teknolojinin sağlamlığı açısından DNA, parmak izi, İris, retina biyometrikleri performansı yüksek olarak sınıflandırılmaktadır.

Kabul edilebilirlik açısından yani biyometrik verilerin ölçüm ve toplanması açısından, yüz, imza ve ses biyometrikleri yüksek olarak sınıflandırılmaktadır. Yaygınlık açısından da yüz, imza ve ses biyometrikleri yüksek olarak sınıflandırılmaktadır.

Tablo 2'de ise biyometrik sistemlerin doğruluk, kullanım kolaylığı ve kullanıcı kabul oranlarına göre yüksek, orta ve düşük olarak sınıflandırılan bir başka tablo görülmektedir. Tabloda; Y=Yüksek, O=Orta, D=Düşük olarak ifade edilmektedir.

Tablo 2. *Biyometrik sistemlerin karşılaştırılması [12].*

Faktörler	Doğruluk	Kullanım Kolaylığı	Kullanıcı Kabul Oranı
Parmak izi	Y	O	D
El Geometrisi	O	Y	O
Yüz	D	Y	Y
İris	O	O	O
Retina	Y	D	D
Ses	O	Y	Y
İmza	O	O	Y

Tablo 2'ye baktığımızda doğruluk faktörünün en yüksek parmak izi ve retinada olduğu görülmektedir. Kullanım açısından en iyi biyometrikler el geometrisi, yüz ve ses olarak belirlenmiştir. Kullanıcı kabul oranının en yüksek olduğu biyometrikler ise yüz, ses ve imzadır.

Uluslararası Biyometrik Grubun (International Biometric Group) yapmış olduğu 2009-2014 biyometri pazar ve sanayi raporu Tablo 3'de görülmektedir. Uluslararası Biyometrik Grubun (International Biometric Group) yapmış olduğu 2009-2014 biyometri pazar ve sanayi raporunda, parmak izi tanıma sistemleri, otomatik parmak izi teşhis sistemi (AFIS) ve yüz tanıma sistemleri 2014 yılında biyometrik pazarın en çok kullanılan teknolojileri olması öngörülmektedir [1].

Tablo 3. *Uluslararası Biyometrik Grubun (International Biometric Group) Yapmış Olduğu 2009-2014 Biyometri Pazar ve Sanayi Raporu [1].*

Teknoloji Piyasa Hacmi						
(Unit: MS USD)						
	2009	2010	2011	2012	2013	**2014**
Parmak izi	971.0	1.380.9	1,740.1	2.064.1	2.422.9	**2.827.2**
AFIS/	1.309.1	1.489.9	1.816.5	2.154.4	2.525.9	**2.965.8**
İris	174.4	287.8	360.8	480.5	578.3	**730.3**
El Geometrisi	62.0	62.8	63.7	68.2	76.0	**85.0**
Özel yazılım (middleware)	275.0	327.7	413.8	525.2	625.2	**732.6**
Yüz	390.0	510.8	675.4	848.5	1.097.3	**1.417.8**
Ses	103.8	109.3	113.5	136.3	167.5	**189.7**
Damar	83.0	102.1	132.2	172.2	199.5	**235.7**
Diğerleri	54.0	85.6	107.5	131.8	154.2	**184.9**
Toplam	**3.422.3**	**4.356.9**	**5.423.6**	**6.581.2**	**7.846.7**	**9.368.9**

V. SONUÇ VE ÖNERİLER

Bir biyometrik sistem oluşturulacağı zaman göz önünde bulundurulması gereken iki önemli unsur vardır, gereksinimler ve maliyet. Bu yüzden güvenlik sistemi maliyet ve gereksinimler göz önüne alınarak en uygun şekilde oluşturulmalıdır. Bu da kullanım farklılıkları ve kullanım alanlarına bağlı olarak her güvenlik sistemini kendi içerisinde önemli kılmaktadır. Bununla birlikte bir biyometrik sistem oluşturulurken; kullanılacak biyometriğin avantajları ve dezavantajları göz önünde bulundurulmalı sistem için en uygun biyometrik veri seçilmelidir.

Bir biyometrik sistemin başarısı büyük oranla giriş verisinin kalitesine bağlıdır. Bu yüzden kalabalık ve ortam izolasyonunun iyi olmadığı açık alanlarda istenmeyen gürültü oluşumu engellenemeyeceği için bu alanlarda ses biyometriğinin kullanılması sistem başarısını olumsuz etkileyecektir. Bu tür alanlarda yüz tanıma, el tanıma ya da avuç içi tanıma sistemleri kullanılabilir.

Kimyasal biyometriklerin analizlerinin uzun sürmesi nedeniyle güvenlik sistemlerinde bu biyometriklerin kullanılması tercih edilmemektedir.

Araştırmalar sonunda, biyometrik özellikler arasından retina ve parmak izi biyometriklerinin doğruluk oranı diğer biyometrik özelliklere göre yüksek olduğu sonucuna ulaşılmıştır. Kullanım kolaylığı açısından ise parmak izi biyometriğinin retina biyometriğinden daha başarılı olması nedeniyle biyometrik sistemler içerisinde en yaygın kullanılan biyometrik veri parmak izidir.

Finansal alanda, biyometrik güvenlik sistemlerinin gelişmesi ile birlikte otomatik imza tanıma sistemleri yaygınlaşacaktır.

Değişen yaşam koşulları ilerleyen teknoloji ile birlikte zamanla günlük yaşantı içersine daha çok teknoloji dâhil olmaktadır. Örneğin ABD'de yer alan West Alabama Üniversitesi, biyometrik sistemleri uzaktan eğitim alan öğrencilerinin sınavlarında kimlik tespitinin bir parçası olarak kullanmaktadır[1]. Öğrenci sınava giriş yapmadan önce parmak izi kontrolü yapmaktadır ve sınav sırasında bir kamera ve mikrofon sayesinde hareket veya ses değişikliği olduğu zaman sınav yöneticilerine bu değişikliğin video görüntüsü gönderilmektedir. Bu kullanım örneğinde de olduğu gibi ihtiyaçlara göre farklı biyometriklerin bir arada kullanılması ile çoklu model biyometrik sistemlerin üzerinde çok daha fazla çalışılacak ve kullanılan uygulama alanları çeşitlenecektir.

Elektronik ortamda gerçekleştirilen alışveriş, bankacılık işlemleri, resmi işlemler, pasaport vb. işlemler biyometrik bir okuyucunun standart bilgisayarlara bütünleştirilmesi ile elektronik ortamda biyometrik tanımlama ile de gerçekleştirilecektir.

Kişiye özel olması, kart veya şifre kullanılmaması gibi nedenlerden dolayı daha avantajlı görülen biyometrik sistemlerin genel dezavantajları da unutulmamalıdır. Biyometrik verilerin kayıtlı olduğu veri tabanlarına yetkisiz kişilerin erişimi maddi manevi kişisel ya da ulusal birçok zarara yol açabilecektir. Bu yüzden oluşturulacak sistemin bilgi güvenliği çok önemlidir. Özel bir uzmanlık alanı gerektiren ve belli bir maliyet karşılığı sahip olunan bu sistemlere ait biyometrik verilerin dijital ortamdaki kayıtlarının kötü niyetli kişiler tarafından elde edilmesi durumunda sistemin kullanılamama durumu söz konusu olabilir. Şifre ile ulaşılan bir güvenlik sisteminde bilgilerin çalınması durumunda yetkili kullanıcıların şifre bilgileri değiştirilerek sistemin devamı sağlanabilirken biyometrik sistemlerde biyometriğin değiştirilmesi söz konusu değildir. Aynı kullanıcılar için sistemin değiştirilmesi gerekecektir. Ayrıca elde edilen biyometrik bilgiler ile bu biyometriği kullanan birçok farklı sisteme de sistem yöneticilerinden habersiz, yetkisiz kişiler tarafından ulaşım söz konusu olacaktır. Biyometrik verilerin canlılığını tespit eden sistemlerin kullanılması yetkisiz erişimler için önleyici bir tedbirdir. Özellikle elektronik ortamla bağlantısı olan sistemlerde biyometrik verilerin kullanılmasında bilgi güvenliği açısından çok dikkatli olunmalıdır.

VI. KAYNAKLAR

[1] M. Akçay, H. H. Çetinkaya, *Kampüslerde Uygulanan Yeni Biyometrik Sistemler*, **Akademik Bilişim**, Malatya-Türkiye, (2011).

[2] H. Arıç, *Bulanık Kümelemeli Yapay Sinir Ağları ile Biyometrik Tanıma*, Yüksek Lisans Tezi, Haliç Üniversitesi, İstanbul-Türkiye, (2011).

[3] A.N. Barbole, M. Godase *Indian Streams Research Journal* **2(8)** (2012).

[4] M. Bilgin, *Biyometrik Seçim Sistemi Tasarımı ve Gerçekleştirilmesi*, Yüksek Lisans Tezi, Selçuk Üniversitesi, Konya-Türkiye, (2008).

[5] H. H. Çetinkaya, M. Akçay, *Yüz Tanıma Sistemleri ve Uygulama Alanları*, **Akademik Bilişim Konferansı**, Uşak-Türkiye, (2012).

[6] G. Dede, M. H. Sazlı, *Biyometrik Sistemlerin Örüntü Tanıma Perspektifinden İncelenmesi ve Ses Tanıma Modülü Similasyonu*, **EEBM Ulusal Kongresi**, (2010).

[7] E. Derya, *Parmak İle Yüz Arasındaki İlişki Analizi*, Yüksek Lisans Tezi, Gazi üniversitesi, Ankara-Türkiye, (2011).

[8] K. Elumalai, M. Kannan *International Journal on Computer Science and Engineering (IJCSE)* **3(2)** (2011) 687-692.

[9] B. Eren, *Biyometrik Teknolojilerin Etkili Tasarlanması ve Uygulanmasında Yeni Bir Öneri: Multimodel Teknoloji*, Yüksek Lisans Tezi, Mimar Sinan Güzel Sanatlar Üniversitesi, İstanbul-Türkiye, (2009).

[10] B. Ergen, A. Çalışkan, *Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri*. **International Advanced Technologies Symposium(IATS)**, Elazığ-Türkiye, (2011).

[11] S. Kaymaz, *Çevrim Dışı İmza Tanıma*, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul-Türkiye, (2010)

[12] P. Manivannan *International Journal on Computer Science and Engineering (IJCSE)* **3(5)** (2011).

[13] V. Nabiyev, *Kulak Biyometrisine Göre Kimlik Tespiti*, **2. Mühendislik ve Teknoloji Sempozyumu**, Ankara-Türkiye, (2009).

[14] B. Nugugi, A. Kamis, M. Tremaine Intention to Biometric Systems, *e-Service Journal* **7(3)** (2011), 20-46.

[15] Önen Yıldız H. G., *Avuçiçi Esaslı Biyometrik Kimlik Tanıma ve Doğrulama*, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul-Türkiye, (2010).

[16] D. S. Özer, *İristen Kimlik Tanıma*, Yüksek Lisans Tezi, Kocaeli Üniversitesi, Kocaeli-Türkiye, (2010).

[17] R. Şamlı, M. E. Yüksel, *Biyometrik Güvenlik sistemleri*, **Akademik Bilişim**, Şanlıurfa-Türkiye, (2009).

[18] M. B. Tosun, *Akıllı Kart ve Parmak İzi Kullanan Geliştirilmiş Güvenlik Sistemi Tasarımı*, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara-Türkiye, (2009).

[19] N. Yalçın, *Konuşmacı Tanıma Teknolojisi Yardımıyla İlköğretim Birinci Sınıf Öğrencilerine İlkokuma Yazma Öğretimi için Bir Yazılım Geliştirme*, Doktora Tezi, Gazi Üniversitesi, Ankara-Türkiye, (2006).

[20] M. Yıldız, *Biyometrik e-Kimlik ile Güvenli Alışveriş Sistemi*, Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Gebze-Türkiye, (2010).

[21] V. Nabiyev, M. Ekinci, Y. Öztürk, *Avuç İçi Çizgilerine Göre Biyometrik Tanıma*, **Elektrik-Elektronik – Bilgisayar Mühendisliği 10. Ulusal Kongresi**, İstanbul-Türkiye, (2003).

[22] B. Ergen, A. Çalışkan, *Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri*, **6th International Advanced Technologies Symposium**, Elazığ-Türkiye, (2011).

[23] O. Meral, *Doğrusal Öngörülü Kodlama ve Adaptif Algoritma Tabanlı Konuşmacı Tanıma*, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul-Türkiye, 2008