Biyometrik Sistemlerde Güvenlik Üzerine Bir İnceleme

Ceren GÜZEL TURHAN, Eyüp Burak CEYHAN, Şeref SAĞIROĞLU

***Özet*—Biyometrik teknolojilerdeki gelişmeler bu alanda yeni bir endüstrinin ortaya çıkmasına neden olmuştur. Günümüzde biyometrik teknolojiler geleneksel doğrulama mekanizmaları yerine kabul görmüştür. Bu teknolojilerin geleneksel yaklaşımlara göre çok daha güvenli oldukları kabul edilmiştir; fakat yapılan araştırmalarda biyometrik sistemlere de kolaylıkla sızılabildiği görülmüştür. Bu çalışmada bu ihtiyaçtan yola çıkılarak biyometrik teknolojilerde güvenlik kavramına odaklanılmıştır. Bu amaçla, biyometrik sistemlerde güvenlik üzerine literatürde yer alan çalışmalar kapsamlı şekilde incelenmiştir. Güvenlik üzerine sunulan modeller de tanımlanan saldırıya maruz kalınabilecek noktalar ele alınarak biyometrik güvenlik konusunda bir farkındalık oluşturmak amaçlanmıştır.**

***Anahtar Kelimeler*—Biyometri, biyometrik sistemler, güvenlik, biyometrik saldırılar**

***Abstract*—Advances on biometric technologies occur a new industry on this field. Nowadays, biometric technologies are considered as a verification mechanism against traditional mechanisms. Although these technologies are supposed to be much more secure, it is seen that it is also possible to penetrate these systems. Therefore, this study focuses on security requirement on biometric systems. In this study, a comprehensive review is presented to answer this need. It is aimed to raise awareness about biometric security with analyzed attack points models.**

***Index Terms*—Biometrics, biometric systems, security, biometric attacks**

I. GİRİŞ

Teknolojik gelişmeler biyometrik tabanlı doğrulama sistemlerinin ortaya çıkmasına ve birçok alanda yaygın kullanımına olanak tanımıştır. Parmak izi gibi biyometri adı verilen karakterleri tanımaya odaklı çalışan doğrulama mekanizmaları ile yetkili kişileri sisteme sızmaya çalışan kişilerden ayırt edebilmek söz konusu olmaktadır. Bu durum, farklı biyometrik özelliklere dayalı sistemlerin geliştirilmesine neden olmuştur.

Ceren Güzel Turhan, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570, Maltepe, Ankara, Türkiye (İlgili yazar, e-posta: cerenguzel@gazi.edu.tr)

Eyüp Burak Ceyhan, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570, Maltepe, Ankara, Türkiye (e-posta: ebceyhan@gazi.edu.tr)

Şeref Sağıroğlu, Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570, Maltepe, Ankara, Türkiye (e-posta: ss@gazi.edu.tr)

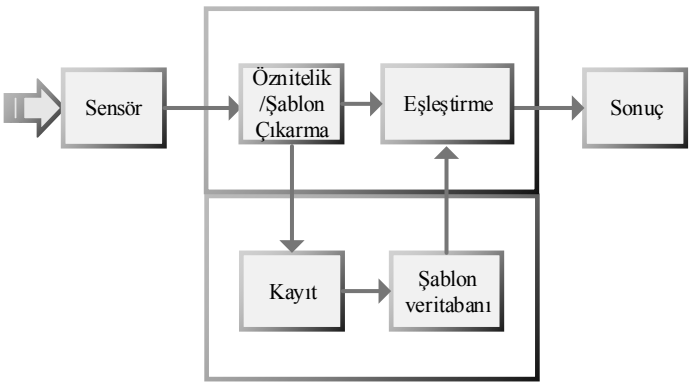
Geleneksel olarak şifre, anne kızlık soyadımız gibi bildiğimiz bilgiler doğrulanarak güvenlik sağlanmaya çalışılmaktadır. Şifre, kullanıcı adı gibi bilgiler bir veritabanında tutularak sisteme erişmeye çalışan bir kişiden alınan bilgiler ile eşleştirme yapılmaktadır. Eşleştirme yani doğrulama işlemi gerçekleştirilirse ise sisteme erişim yetkisi elde edilmektedir. Bu geleneksel yaklaşım performans açısından etkin olmakla birlikte bilgilerin saldırganlar tarafından elde edilmesi ile saldırganların sisteme yetkisiz erişimi gibi tehlikelere maruz kalabilmektedir. Doğrulama işlemi bildiklerimizin sorgulanması yerine sahip olunan bir akıllı kart ya da anahtar gibi nesneler ile de gerçekleştirebilmektedir. Bu doğrulama yaklaşımında ise kaybetme, çalınma gibi durumlarda sistem yetkisiz kişilerin hedefi haline gelebilecektir. Bahsedilen geleneksel yöntemlerin yerini günümüzde biyometrik denilerek nitelendirilen kendimize ait olan özellikler ile yapılan doğrulama işlemleri almaktadır. Biyometrik doğrulama mekanizmaları çalınamaz ve kaybedilemez olmaları nedeniyle diğer doğrulama mekanizmaları arasından en güvenilir olanı olarak nitelendirilmektedir [1]. Biyometrinin daha güvenli bir doğrulama mekanizması olarak değerlendirilmesi bu konu üzerine çalışmalara neden olmuştur. Bu çalışmalar farklı biyometrik karakterlerin doğrulama amacıyla kullanılabildiğini ortaya koydukları gibi farklı alanlarda uygulamalar geliştirilmesine imkan vermiştir. Güvenli olarak algılanan biyometri tabanlı doğrulama mekanizmalarının düşünüldüğü kadar güvenli olmamaları çeşitli çalışmalarda ortaya koyulmuştur. Bu nedenle, makale çalışması kapsamında günümüzde hemen her alanda hayatımızda yer edinen biyometri tabanlı sistemlerdeki güvenlik kavramı üzerine odaklanılarak bu alanda yapılan çalışmalar üzerine bir inceleme sunulmuştur. Daha önce yapılan çalışmalarda tanımlanan farklı güvenlik problemleri ele alınmıştır.

Bu makale 4 bölümden oluşmaktadır. Makalenin devam eden kısmı şu şekilde organize edilmiştir. 2. bölümde biyometrik sistemler ele alınarak basit bir biyometrik sistemde olması gereken bileşenler tanımlanmıştır. Biyometrik sistemlerde biyometrik karakter olarak kullanılabilecek karakterler kategorik olarak ele alınmıştır. Biyometrik teknolojilerin kullandıkları karakterlere göre uygulama alanları açıklanmıştır. 3. bölümde biyometrik sistemlerde güvenlik sağlamak üzere tanımlanan modellere ilişkin çalışmalar incelenmiştir. Son olarak sonuç bölümünde ise biyometrik sistemlerde güvenlik gereksinimi vurgulanarak bu

amaçla yapılan çalışmalardan elde edilen kazanımlar değerlendirilmiştir.

II. BİYOMETRİK SİSTEMLER

Basit bir biyometrik sistem temel olarak 4 adımdan oluşacak şekilde incelenebilmektedir. Bu adımlar biyometrik verilerin bir algılayıcı aracılığıyla sisteme alınması, alınan veriden öznitelik vektörlerinin elde edilmesi, elde edilen öznitelik vektörlerinin daha önce yapılan bir kayıt işlemi ile veritabanlarına kaydedilen şablonlar ile eşleştirmesi ve yapılan eşleştirme sonucunda alınan skora göre sisteme erişim kararının oluşturulmasıdır [2]. Şekil 1'de temel bir biyometrik sistem modeli gösterilmektedir.



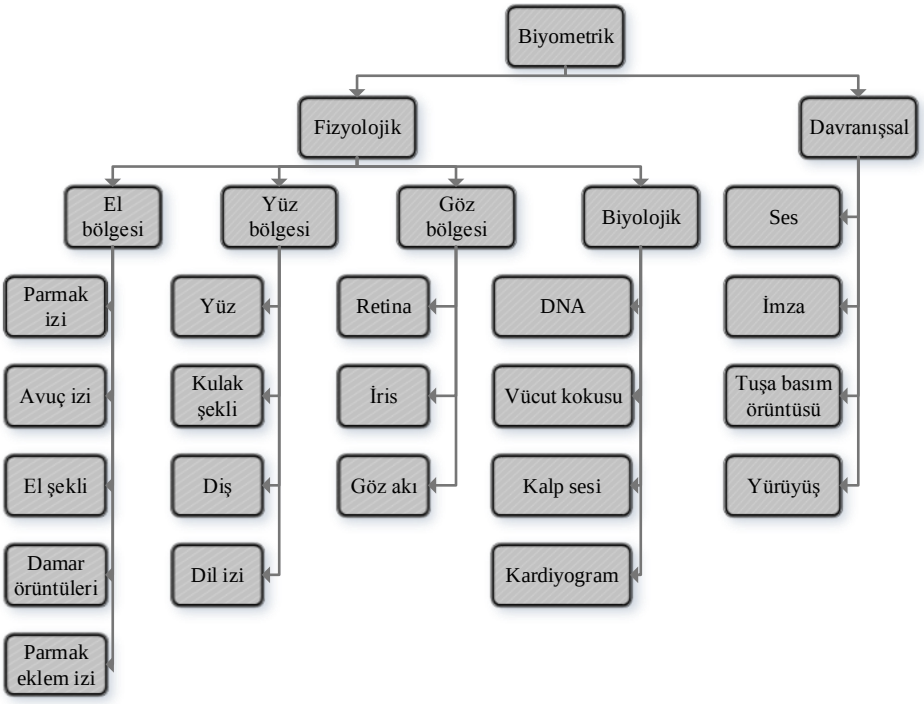
Şekil 1. Biyometrik sistem modeli

Biyometrik sistemler doğrulama amacıyla kullanılmalarının yanı sıra tanıma işlemlerini gerçekleştirebilmek üzere kullanılabilmektedir. Doğrulama sistemleri, veritabanında daha önceden kaydedilen bir şablon ile karşılaştırma yapılarak kişinin doğru kişi olup olmadığının doğrulanmasını hedeflenmektedir. Bu sistemler erişim kontrolü, güvenlik, takip gibi amaçlara hizmet etmek üzere farklı uygulama alanlarına sahiptir. Bu uygulamalarda şüphesiz güvenlik önemli bir konuya sahiptir. Tanıma sistemlerinde ise veritabanında yer alan tüm şablonlar ile örnek veri karşılaştırılarak biyometrik özellikten kimlik tespiti yapılmaya çalışılmaktadır [3].

Biyometrik sistemlerde rol alan 3 farklı kullanıcı tanımlanabilmektedir. Kullanıcılar taklitçi, saldırgan veya yetkili kullanıcı olarak gruplandırılabilmektedir. Yetkili bir kişi gibi görünerek biyometrik sistemlere erişebilen ya da erişmeye çalışan kişiye taklitçi adı verilmektedir. Biyometrik sistemlere düzenlediği saldırılarla erişmeye çalışan ya da hizmet aksattırma işlemini hedefleyen kişi saldırgan olarak ifade edilmektedir. Yetkili kullanıcı ise biyometrik sistemlere erişim yetkisi olan kişidir [4].

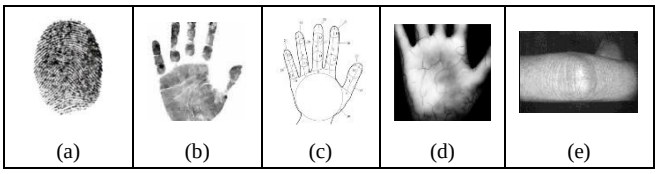
A. Biyometrik Sistem Karakterleri

Biyometrik sistemler bir algılayıcı ile dış ortamdan alınan biyometrik verinin tipine göre adlandırılmaktadır. Biyometrik sistemlere konu olan biyometrik karakterler fizyolojik ve davranışsal karakterler olmak üzere iki grupta ele alınmıştır. Fizyolojik biyometrik karakterler kategorisi altında Şekil 2'de görüldüğü gibi biyometrik karakterlerin yer aldığı bölgelere göre bir alt kategorizasyon yapılabilmektedir. Fizyolojik karakterler el, yüz ve göz bölgesinde bulunan fiziksel özelliklerimiz olabildikleri gibi DNA, vücut kokusu, kalp sesi ve kardiyogram gibi biyolojik özellikler de olabilmektedir.



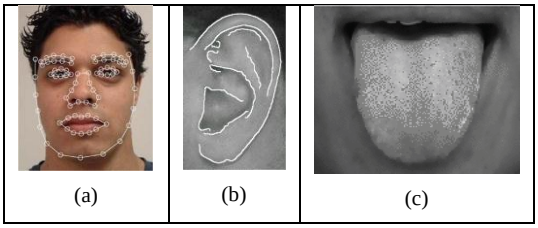
Şekil 2. Biyometrik sistemlerde kullanılan biyometrik karakterler [5]

Özellikle parmak izi olmak üzere el bölgesinin önemli doku bilgileri içermesi bu karakterler tabanında çalışan tanıma sistemlerinin yaygın şekilde kullanılmasına neden olmuştur. El bölgesinde ele alınabilecek karakterler Şekil 3'de gösterildiği gibi, bilinen en eski biyometrik karakter olarak ele alınan parmak izinin yanı sıra avuç izi, el geometrisi, damar örüntüleri ve parmak eklem izi gibi karakterlerdir. Parmak izi sistemlerinde sırt iskeleti, sırt örüntüleri, vadi ve geçit gibi öznitelikler dikkate alınarak eşleştirici bir skor elde ederek tanıma işlemi gerçekleştirilmeye çalışılmaktadır. Avuç içi karakterine dayalı çalışan sistemlerde temel çizgiler, kırışıklıklar, yoğunluk, avuç dokusu, ortalama ve varyans gibi öznitelikler kullanılmaktadır. Eller üzerinde yer alan damar izini tanımak üzere geliştirilen sistemlerde ise damar çatallanmaları gibi öznitelikler ayırt edici olmaktadır [5].



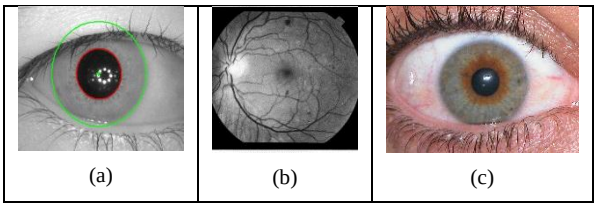
Şekil 3. El bölgesi biyometrik karakterleri (a) parmak izi (b) avuç izi (c) el geometrisi (d) damar izi (e) parmak eklem izi

Yüz bölgesi parmak izi gibi ayırt ediciliği yüksek bir biyometrik karakterlerden oluştuğu için en çok çalışılan bölgelerden biri olmuştur. Şekil 4'de biyometrik sistemlerde kullanılan yüz bölgesi karakterleri gösterilmiştir. Yüz bölgesinde en fazla ön plana çıkan biyometrik karakter yüz olmuştur. Yüz üzerinde gözler, ağız ve burun arası uzaklıklar gibi öznitelikler tabanında tanıma problemi çözümlenmeye çalışıldığı gibi tüm görüntü, yüz sınırları gibi farklı öznitelikler belirlenerek yüzden kimlik tespiti yapılmaya da çalışılmıştır. Kulak, şekli ve kepçe olarak ifade edilen doku yapısı itibariyle ayırt edici bir özellik olarak önerilmiştir [6]. Kulak için tanımlanan öznitelikler kulak boyu, genişliği, yüksekliği, rengi ve sınırları gibi öznitelikler olmuştur [5]. Dil izinin eşi olmayan bir biyometrik karakter olması bu karaktere dayalı olarak yapılan çalışmalar da vardır [7]. Bu çalışmalarda dil genişliği, kalınlığı, dokusu ve şekli gibi öznitelikler tanımlanmıştır [5].



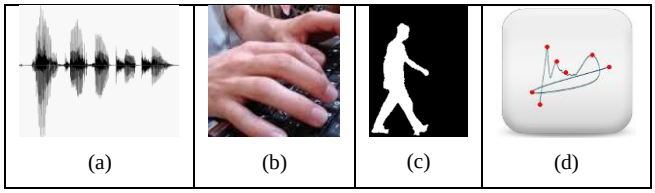
Şekil 4. Yüz bölgesi biyometrik karakterleri (a) yüz (b) kulak (c) dil

Göz bölgesinde yer alan biyometrik karakterlerin daha doğru, güvenilir ve sabit yapıda olmaları göz bölgesini tanımak üzere geliştirilen çok sayıda yaklaşıma neden olmuştur [5]. Göz bölgesinde ele alınan karakterler Şekil 5'de gösterilmektedir. İris tabanlı biyometrik sistemlerde renk, şekil ve iris dokusu özniteliklerinden yararlanılarak tanıma problemi çözümlenmeye çalışılmaktadır. İrisin ayırt edici özelliğinin aksine bu karaktere dayalı geliştirilen sistemlerin pahalı ve saldırıya açık olması sistemlerin kullanılabilmesine engel teşkil etmektedir [8]. Retina için damarlar ve optik alanı gibi öznitelikler ayırt edici olmaktadır. Gözün geri kalan kısmını oluşturan göz akı bölgesi ise göz damarlarından oluştuğu için bu damarlar yardımıyla eşleştirme yapılmaya çalışılmaktadır [5].



Şekil 5. Göz bölgesi biyometrik karakterleri (a) iris, (b) retina (c) göz akı

Biyolojik karakterler, medikal sensörler ile alınan DNA, vücut kokusu ve kalp sesi gibi kişiye özgü olarak nitelendirilen biyolojik bulgulardır. DNA, kişiye özgü olarak kullanılabilecek en iyi ayırt edici biyometrik karakterlerden biridir. Kişiden alınan saç, kan ve tırnak gibi örneklerden DNA kodu kolaylıkla elde edilebilmektedir [5]. Bu sebeple başkasına ait DNA kodu, bir kişi tarafından kolaylıkla elde edilebilecek bir bilgidir. DNA kodunu değerlendirebilecek bir uzmana olan gereksinim DNA tabanında çalışabilecek gerçek zamanlı uygulamaları mümkün kılmamaktadır [6]. Vücut kokusu, bir sensör aracılığıyla alınarak sınıflandırılabilecek olan bir biyometrik karakterdir. Alınan kokuyu sınıflandırabilen e-nose olarak adlandırılan sistemler mevcuttur [5].



Şekil 6. Davranışsal biyometrik karakterler (a) ses (b) tuşa basma örüntüsü (c) yürüyüş tarzı örüntüsü (d) imza

Davranışsal karakterler insanların kendilerini ifade edebildikleri, ayırt edici olan ses, imza, tuşa basım gibi davranışlarına ait özellikleridir. Davranışsal karakterler olarak nitelendirilen biyometriklere Şekil 6'da yer verilmiştir. Davranışsal karakterler tabanında en yaygın şekilde kullanılan sistemler ses, tuşa basım ve imza tanıma sistemleridir. Bu sistemler fiziksel ve biyolojik karakterlere dayalı sistemlere göre herhangi bir harici donanıma gerek duymadıkları için daha avantajlıdır. Davranışsal karakterlerden biri olan sesi tanımak üzere spektrum, ritim, durak ve enerji gibi öznitelikler tanımlanmıştır. Tuşa basım örüntüsü, davranışın analiz edilerek kimlik tespitini sağlayan karakterlerden biridir. Bu sistemler, tuşa basım işleminin kişiye özgü bir ritme sahip olduğu varsayımı üzerine ortaya çıkmıştır. Tuşa basım

örüntüsüne dayalı sistemlerde tuşa basım ve tuş bırakma anına bağlı olarak tanıma işlemi gerçekleştirilmeye çalışılmaktadır [9]. Bu nedenle tuşa basım, bekleme, gecikme süreleri ile hız gibi öznitelikler bu sistemlerde ayırt edici özellikler olarak kişileri birbirinden ayırt etmek üzere kullanılmaktadır. Yürüyüş tarzı tabanlı çalışan sistemler ise hız, bir adım mesafesi ve siluet şekli gibi öznitelikler ile değerlendirme yapabilmektedir. İmza, üzerinde çalışılan farklı bir davranışsal karakterdir. Bu karakteri kullanan sistemlerde imza şekli, kalem yönü, ivme ve imza uzunluğu gibi hususlara dikkat edilmektedir [5].

TABLO I
BİYOMETRİK KARAKTER KARŞILAŞTIRMALARI [1]

Biyometrik Özellik	Kullanım kolaylığı	Sorunlar	Doğruluk	Güvenlik gereksinimi
Parmak izi	Yüksek	Kuruluk, kir ve yaş	Yüksek	Yüksek
El geometrisi	Yüksek	Elde hasar, yaş	Yüksek	Orta
Retina	Düşük	Gözlük	Çok Yüksek	Yüksek
İris	Orta	Işık	Çok Yüksek	Çok yüksek
Yüz	Orta	Işık, yaş, gözlük, saç	Yüksek	Orta
İmza	Yüksek	İmza değişikliği	Yüksek	Orta
Ses	Yüksek	Gürültü, ses kısıklığı	Yüksek	Orta

Biyometrik sistemlerde yaygın olarak kullanılan özellikler parmak izi, avuç izi, retina, iris, yüz, imza ve ses olmuştur. Biyometrik sistemlerde kullanılan biyometrik karakterlerin her birinin kendine özgü güçlü ve zayıf yönleri bulunmaktadır. Parmak izi, düşük maliyetli ve diğer karakterlere göre daha ayırt edici bir özellik olması nedeniyle çok sayıda sistemde kullanılmıştır. Parmak izi, kontrollü bir çevrede yeterli sayıda eğitim adımın sonunda tanıma yapabilecek akıllı ev sistemleri için iyi bir özellik olarak nitelendirilmiştir. Retina tanıma sistemleri performansı yüksek olan sistemler olmalarına rağmen belirli bir noktaya odaklanma gereksinimleri nedeniyle yaygın olarak kullanılan biyometrik sistemler olamamıştır. Yüz tanıma sistemleri yüz karakterlerine dayalı olarak analiz yapan sistemlerdir. Bir algılayıcı ile çalışan bu sistemlerde çok sayıda uygulamada kullanılmıştır. Ses tanıma sistemleri ise herhangi bir ek donanıma gerek duymaksızın sesi metin dosyalarına dönüştürerek işlem yapan sistemler oldukları için ilgi görmüşlerdir. Bu sistemlerin de gürültü gibi dış etkenlerden etkilenmesi sistemlerin pratikte kullanılabilirliğini olumsuz yönde etkilemektedir [10]. Biyometrik karakterlerin özelliklerine göre yapılan bir karşılaştırmaya Tablo I'de yer verilmiştir. Tabloda karakterler tabanında çalışan sistemlerin kullanım kolaylığı, karşılaşılabilecekleri sorunlar, performansları ve güvenlik gereksinimleri kıyaslanmıştır. Karakterlerin bu özellikleri dikkate alınarak uygulamaya yönelik biyometrik sistemler ortaya çıkmıştır. Parmak izine dayalı biyometrik sistemler, kullanım kolaylığı ve performanslarına rağmen parmak izi yüzeyinde olabilecek kuruluk, yaş ve kir gibi durumlar karşısında başarısız olmaktadır. Yüz karakteri için tablo incelendiğinde ise yüz tanıma sistemlerinin kullanım kolaylığı orta, performansı yüksek, güvenlik gereksinimi ise orta olarak nitelendirildiği görülmektedir. Yüz tanıma sistemlerinin ışık varyasyonları, saç, gözlük gibi aksesuarlar ile yaşa karşı hassas olmaları dikkat çekmektedir.

Biyometrik olarak kullanılabilecek karakterleri belirleyebilmek üzere ayırt edicilik, evrensellik, kalıcılık ve ölçülebilirlik gereksinimleri sağlanmalıdır. Dikkat edilmesi gereken diğer unsurlar ise performans, kabul edilebilirlik ve aldatılabilirliktir. Ayırt edicilik, farklı iki kişide aynı karakterin aynı olma olasılığının neredeyse sıfır olmasıdır. Evrensellik, tüm insanların biyometrik veri olarak kullanılacak karaktere sahip olmasıdır. Kalıcılık, biyometrik karakterin zaman içinde değişiminin söz konusu olmamasıdır. Performans, biyometrik sistemlerde kullanılan biyometrik karakterin yüksek tanımlama başarısına sahip olmasıdır. Ölçülebilirlik, biyometrik karakterin niceliksel olarak ölçülebilir olması anlamına gelmektedir. Kabul edilebilirlik, söz konusu biyometrik karakterin insanlar tarafından biyometrik veri olarak görülebilmesidir. Aldatılabilirlik ise biyometrik sistemin kolaylıkla kandırılarak yetkisiz kişiler tarafından erişilebilmesidir [11].

TABLO II
BİYOMETRİK KARAKTER KARŞILAŞTIRMALARI [11]

	Ayırt edicilik	Evrensellik	Kalıcılık	Ölçülebilirlik	Performans	Kabul edilebilirlik	Aldatılabilirlik
Yüz	D	Y	O	Y	D	Y	Y
İris	Y	Y	Y	O	Y	D	D
Tuşa basım	D	D	D	O	D	O	O
Avuç izi	O	O	Y	O	Y	O	O
Parmak izi	Y	O	Y	O	Y	O	O
Kulak	O	O	Y	O	O	Y	O
DNA	Y	Y	Y	D	Y	D	D
Retina	Y	Y	O	D	Y	D	D
İmza	D	D	D	Y	D	Y	Y
Ses	D	O	D	O	D	Y	Y
Yürüyüş	D	O	D	G	D	Y	O
Vücut kokusu	D	Y	Y	D	D	O	O

Biyometrik sistemler için ayırt edici olan bir karakterin performansı hız ve doğruluk bakımından yeterli değil ise uygulanabilir olamayacaktır. Pratikte uygulanacak biyometrik bir karakterin gereksinimleri sağlamasına ek olarak tüm bu unsurları taşıması gerekmektedir [6]. Bu sebeple biyometrik

sistemlerde doğrulanacak karakterler sistem biyometrik karakter ölçütlerine ek olarak uygulama alanları da dikkate alınarak belirlenmelidir. Tablo II'de farklı biyometrik karakterlerin biyometrik karakter ölçütlerine göre karşılaştırmalarına yer verilmiştir. Tablo üzerinde Y ile ifade edilen ölçütler Yüksek, O ile ifade edilenler Orta ve D ile ifade edilenler ise Düşük anlamına gelmektedir. Tabloda görülebildiği gibi yüz ayırt ediciliği düşük, tüm insanlarda aynı olan bir karakter olması sebebiyle evrenselliği yüksek, yaşa bağlı değişken bir karakter olması sebebiyle kalıcılığı orta, niceliksel olarak değerlendirilebileceği için ölçülebilirliği yüksek olarak değerlendirilmiştir. Ayrıca bir biyometrik veri olarak kabul edilebilirliği yüksek ve başka bir kişiye ait yüz ile taklit edilebilir olabileceğinden aldatılabilirliği yüksek olarak ifade edilmiştir.

B. Biyometrik Teknoloji Uygulama Alanları

Biyometrik sistemlerin uygulama alanları sınır kontrol, suçlu tanımlama, erişim kontrolü, e-ticaret, bilgisayar oturum açma işlemleri, kimlik kartları, pasaportlar, görüntüleme sistemleri, akıllı telefonlarda kullanıcı doğrulama, kalabalık görüntüleme, elektronik bankacılık, video izleme ve adli bilişim gibi alanlardır. Biyometrik sistemlerin uygulama alanları Tablo III'de özetlenmiştir.

TABLO III
BİYOMETRİK SİSTEMLERİN UYGULAMA ALANLARI [5]

	Parmak izi	Avuç izi	El geometrisi	El damar örüntüleri	Parmak eklem izi	Yüz	Kulak	Dil izi	İris	Retina	Göz akı	Ses	Tuşa basma örüntüsü	Yürüyüş tarzı	İmza
Sınır kontrol	×					×			×	×					
Adli bilişim	×					×								×	
Suçlu tanıma	×					×			×	×				×	
Kimlik kartı	×					×			×						
Pasaport	×					×			×						
Bilgisayar oturum açma işlemleri	×	×	×	×	×	×	×	×	×		×	×	×		×
Erişim kontrolü	×	×	×	×	×	×	×	×	×	×	×	×			×
E-ticaret	×	×	×	×	×	×	×	×	×		×	×			×
Akıllı telefon	×	×	×	×								×	×		
Görüntüleme sistemleri	×	×	×		×		×		×					×	
Video izleme						×								×	
Kayıp çocuk tanıma	×					×			×						
Kalabalık görüntüleme						×								×	
E-banka															×

Tablo III'de görüldüğü üzere erişim kontrolü uygulamalarında hemen her karakter tabanında geliştirilen sistemler kullanılabilmektedir. Sınır kontrol uygulamalarında ise en yaygın kullanılan biyometrik karakterler olan parmak izi, yüz, iris ve retina kullanılmaktadır. Yürüyüş tarzı karakterine dayalı sistemlerin ise belirli bir mesafeden tanımaya imkan verdiği için video görüntüleri üzerinde adli bilişim, suçlu tanımlama, görüntüleme sistemleri, kalabalık görüntüleme ve video izleme uygulamalarında kullanıldığı görülmüştür. Kimlik kartı ve pasaport kartlarında ise yüz, parmak izi ve iris gibi karakterler kullanılmıştır.

Biyometrik teknolojilere duyulan gereksinim bu alanda bir endüstrinin ortaya çıkmasına neden olmuştur. Bu endüstride farklı teknolojiler ile 2013 ve 2019 yılları arasında elde edilen ve beklenen gelirler BBC raporlarında [12] ifade edilmiştir. 2013 yılı verileri ile oluşturulan raporda piyasada en çok kullanılan biyometrik teknoloji parmak izi teknolojileri olmuştur. Tüm teknolojilerin özellikle de parmak izi teknolojilerine ait pazar payının önemli derecede arttığı görülmektedir. Bu raporda 2013 yılında 8,7 milyar dolara varacağı öngörülen pazar payının 2014 yılında yıllık % 19,8 artışla 11,2 milyar dolar, 2019 yılında ise 27,5 milyar dolar olacağı tahmin edilmiştir.

III. BİYOMETRİK SİSTEMLERDE GÜVENLİK

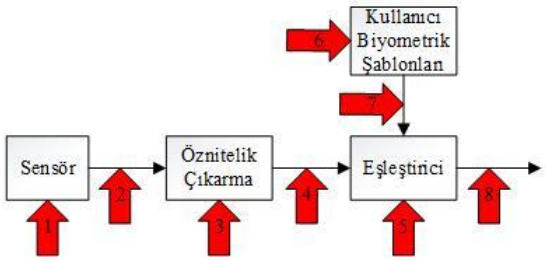
Geleneksel doğrulama mekanizmalarındaki verilerin çalınabilme ve kaybedilebilme gibi sorunlarının aksine biyometrik sistemlerin taklit edilemez ve kopyalanamaz olarak görülmesi bu sistemlerin en güvenli doğrulama mekanizmaları olarak vurgulanmasına neden olmuştur. Biyometrik sistemlerin geleneksel doğrulama mekanizmalarına göre üstünlüklerine karşın bazı problemleri mevcuttur. İncelenen pek çok çalışmada biyometrik sistemlerin düşünüldüğü kadar güvenli sistemler olmadıkları görülmüştür. 2009 yılında gerçekleştirilen Black Hat konferansında bir araştırma grubu tarafından Asus, Toshiba ve Lenova dizüstü bilgisayarların bazı modellerinde bulunan gömülü biyometrik sistemlerde (Asus SmartLogon V1.0005, Toshiba Face Recognition 2.0.2.32 ve Lenova Veriface III) taklit edilen biyometrik veriler ile sistemlere kolaylıkla erişilebildiği gösterilmiştir [13]. Apple'ın parmak izi sensörüne sahip ilk akıllı telefonu olan iPhone 5s'e yapıştırıcı bir ürünle kopyalanan bir parmakla bir başkası tarafından erişilebileceği gösterilmiştir [14].

Birçok çalışmada saldırı vektörleri olarak tanımlanan saldırı noktalarından biyometrik sistemlere erişilerek, bu sistemlerde güvenlik açısından tehditler oluşturulabilmektedir. Olası güvenlik açıklarının önceden bilinmesi bu saldırı noktalarına karşı önlem alınarak sistemlerin güvenli kılınması açısından önem teşkil etmektedir. Bu gereksinim üzerine literatür incelendiğinde biyometrik sistemlerde saldırı vektörlerini tanımlamak üzere yapılan çeşitli çalışmalara rastlanmıştır. Bu alandaki çalışmalardan ilkini Ratha ve arkadaşları [15] tarafından yapılan çalışma oluşturmaktadır. Ratha ve arkadaşları yaptıkları çalışmada biyometrik sistemlerde güvenlik unsuru üzerine odaklanmışlardır. Bu çalışmalarında biyometrik sistemlerin saldırılara maruz kalabileceği güvenlik

açıklarına değinmişlerdir. Bu amaçla bir saldırı noktaları modeli önermişlerdir. Önerilen model 8 farklı saldırı vektöründen oluşmaktadır. Modelde tanımlanan saldırı vektörleri;

1. Sahte biyometrik,
2. Tekrarlı gönderim,
3. Öznitelik çıkarımının geçersiz kılınması,
4. Öznitelik vektörünün değiştirilmesi,
5. Eşleştiricinin etkisiz kılınması,
6. Veritabanına yetkisiz erişim,
7. Şablon verisinin değiştirilmesi,
8. Eşleştirici sonucunun değiştirilmesidir.

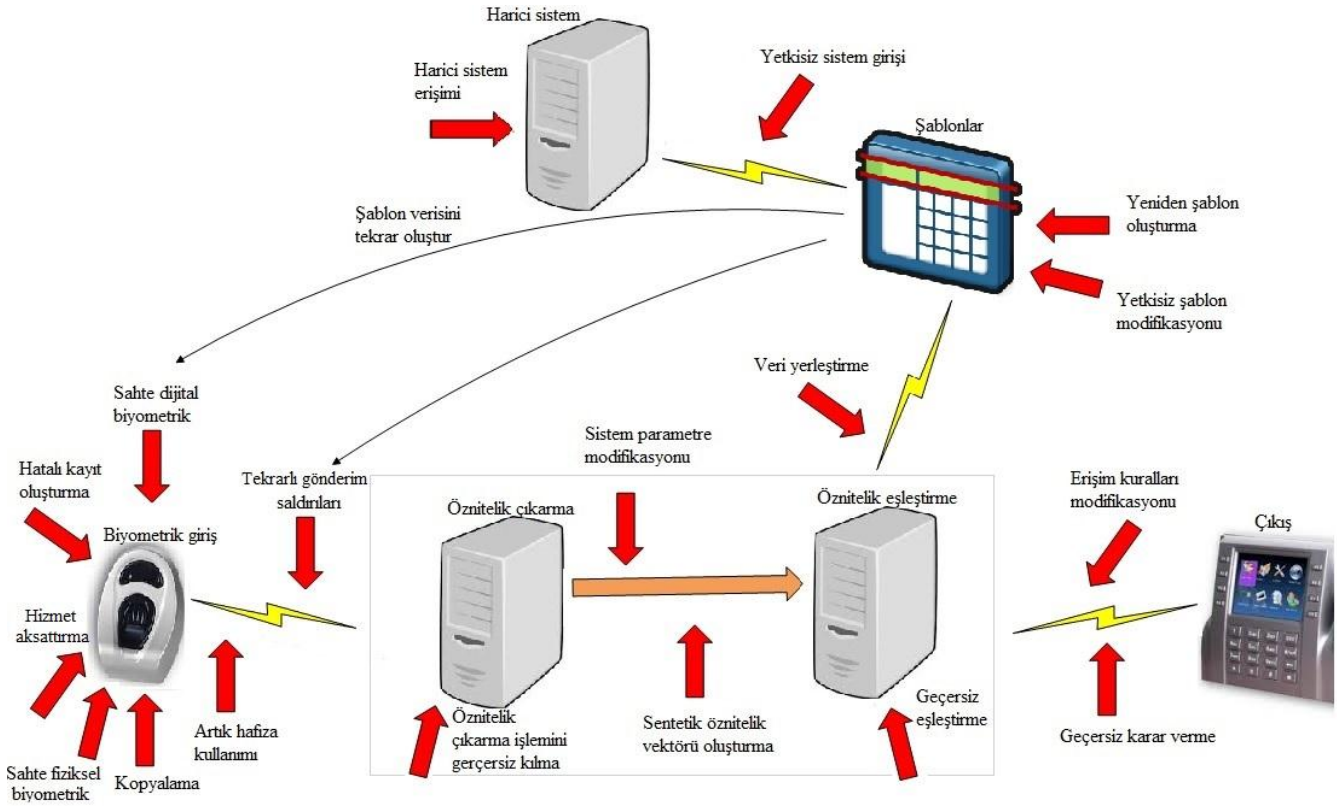
Bu modele ilişkin görsele Şekil 7'de yer verilmiştir. Şekilde kırmızı oklarla ifade edilen adımlardan sisteme yetkisiz kişiler tarafından erişilebileceği vurgulanmıştır.



Şekil 7. Ratha ve arkadaşlarının saldırı vektörleri modeli [15]

Cukic ve Bartlow [16] yaptıkları çalışma ile Ratha ve arkadaşlarının [15] yaptıkları çalışmaya kıyasla daha kapsamlı bir model sunmuşlardır. Çalışmalarında biyometrik sistemler için bir saldırı ağacı modellemişlerdir. Bu model ile 20 olası saldırı vektörü ile 22 güvenlik açığı tanımlanmıştır. Jain ve arkadaşları [17] kılçık modeli diye tanımladıkları modelleriyle biyometrik sistemlerin maruz kalabileceği problemleri kategorize ederek ele almışlardır. Modellerinde saldırıları, düşman ve sıfır çaba saldırıları olarak iki sınıfa ayırmışlardır. Roberts [4] yaptığı çalışmada tanımladığı 18 olası saldırı vektöründen oluşan model ile bu saldırı vektörlerine karşı savunma yollarını ele almıştır. Roberts'ın modeline Şekil 8'de yer verilmiştir. Modelde görülebildiği gibi;

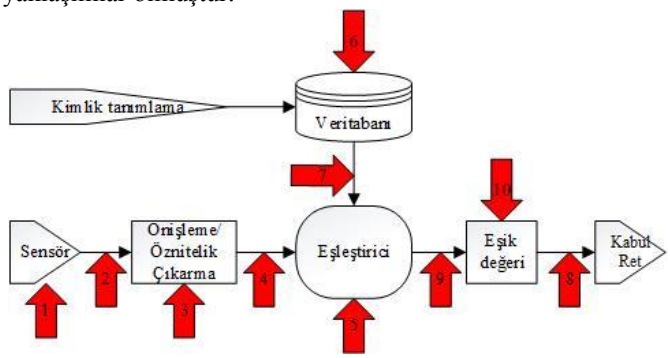
- Sahte dijital biyometrik
- Hatalı kayıt oluşturma
- Hizmet aksattırma
- Sahte fiziksel biyometrik
- Kopyalama
- Artık hafıza kullanımı
- Tekrarlı gönderim
- Öznitelik çıkarma işleminin geçersiz kılınması
- Sistem parametre modifikasyonu
- Sentetik öznitelik vektörü oluşturma
- Harici sistem erişimi



Şekil 8. Roberts'ın saldırı vektörleri modeli [4]

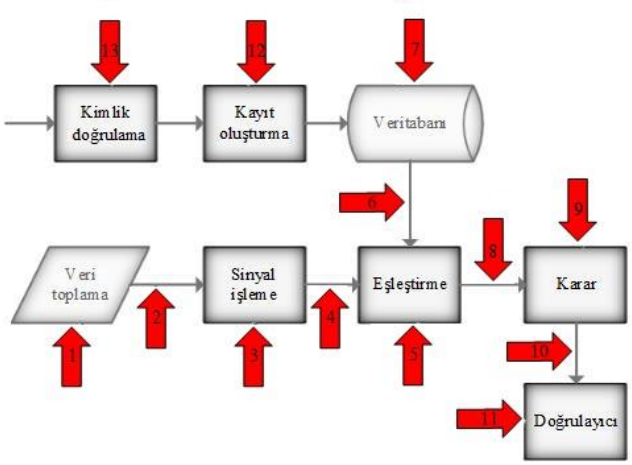
- Yetkisiz şablon modifikasyonu
- Veri yerleştirme
- Geçersiz eşleştirme
- Erişim kuralları modifikasyonu
- Geçersiz karar verme

saldırı vektörleri tanımlanmıştır. Bu çalışmada yukarıda da sıralanan güvenlik sorunlarına karşı biyometrik sistemleri güvende tutabilmek üzere bazı savunma yolları önerilmiştir. Bunlar güvenlik yanıtı, rastsal biyometrik veri, hafızada tutma, gerçeklik tespiti, çoklu biyometrik, çok karakteristikli biyometrik, faktörlü doğrulama, ayırt edici biyometrik, veri bütünlüğü, şifreleme, dijital imza, şablon bütünlüğü, iptal edilebilir biyometrik, donanım bütünlüğü, ağ güvenliği, fiziksel güvenlik, aktivite günlüğü ve politikalar gibi yaklaşımlar olmuştur.



Şekil 9. Galbally saldırı vektörleri modeli [18]

Galbally [18], daha önce tanımlanan kılçık modelinde [17] yapılan kategorizasyonu dikkate alarak düşman saldırılarını doğrudan ve dolaylı saldırılar olarak kategorize ederek ele almıştır. Bu kategorizasyon 10 saldırı noktasından oluşan model üzerinde ifade edilmiştir. İlgili modele Şekil 9'da yer verilmiştir. Model incelendiğinde Ratha ve arkadaşlarının [15] geliştirdiği modele benzerlik dikkat çekmektedir. Bu çalışmada 4 ve 5 ile gösterilen saldırı noktaları 9 ve 10 ile tekrar ifade edilerek model detaylandırılmıştır.



Şekil 10. Alaswad saldırı vektörleri modeli [19]

Alaswad ve arkadaşları [19], 13 farklı saldırı noktası ile modellerini ifade etmişlerdir. Bu saldırı modeline Şekil 10'da gösterilmektedir. Şekilde görüldüğü gibi model bir biyometrik sistemde yer alan her adım için geliştirilmiştir. Bu çalışmada saldırı noktaları her bir saldırı seviyesi için ele alınmıştır. Her bir adımda ayrı olarak ele alınan saldırılara karşı alınabilecek savunma yollarına da yer verilmiştir.

IV. SONUÇ VE DEĞERLENDİRMELER

Bilgi teknolojilerindeki gelişmeler geleneksel doğrulama mekanizmalarının yerini biyometrik veri tabanlı doğrulama mekanizmalarının almasına neden olmuştur. Biyometrik verilerin kaybedilemez, kopyalanamaz ve unutulamaz gibi özellikleri nedeniyle biyometrik teknolojiler üzerine bir endüstri ortaya çıkmıştır. Makalede ele alındığı gibi farklı biyometrik karakterlere dayalı biyometrik teknolojiler ortaya çıkmıştır. Biyometrik teknolojilerin özellikleri dikkate alınarak uygulama alanları da farklılık gösterebilmektedir. Bu teknolojilerin hayatımızın bir parçası haline gelmesi, bu sistemlerin varsayıldığı kadar güvenli sistemler olup olmadıkları sorusunu gündeme getirmiştir. Literatürde biyometrik sistemlerin düşünüldüğü gibi güvenli sistemler olmadıkları örnekleri ile gösterilmiştir. Bu nedenle sunulan çalışmada biyometrik teknolojilerde güvenlik kavramına odaklanılmıştır. Biyometrik sistemlerde güvenlik konusunu ele alan çalışmalar incelendiğinde sistemlerin maruz kalabileceği saldırılar üzerine çeşitli çalışmalar yapıldığı görülmüştür. Bu çalışmalarda sunulan saldırı noktaları modellerindeki olası saldırılar değerlendirilmiştir.

Sunulan çalışma ile biyometrik teknolojilerin saldırılara ne kadar açık olduğu gözler önüne serilerek, ülkemizde de giderek kullanımı artan biyometrik sistemlerin güvenliği konusunda bir farkındalık oluşturulmaya çalışılmıştır. Biyometrik teknolojilerin, geleneksel doğrulama mekanizmalarına göre çok daha güvenli teknolojiler olarak nitelendirilmelerine rağmen beklenildiği kadar güvenli olmadıkları literatürdeki çalışmalar incelenerek ortaya konmuştur. Ayrıca, biyometrik karakterlerin kopyalanmasının, biyometriklerin değiştirilemez yapıları nedeniyle, şifre ve kullanıcı adı gibi bilgilerin bir başkası tarafından elde edilmesinden çok daha büyük tehdit oluşturduğu tespit edilmiştir. Bu nedenle, biyometrik sistemlerde güvenlik önlemleri alınarak gerekli politikalar sağlanması gerektiği sonucuna ulaşılmaktadır. Gelecek çalışmalarda, günümüzde kullanımı hızla artan biyometrik sistemlerin daha güvenli ve performanslı olmasını sağlayacak yaklaşımların üzerinde daha fazla durulması gerektiği değerlendirilmektedir.

KAYNAKÇA

[1] S. Liu, M. Silverman, "A practical guide to biometric security technology", IT Professional, vol. 3, no. 1, pp. 27–32, 2001.
[2] K. Delac, M. Grgic, "A survey of biometric recognition methods", in 46th International Symposium Electronics in Marine, Crotia, pp.184-193, 2004.
[3] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: Security and privacy concerns", IEEE Security & Privacy, no. 2, pp. 33–42, 2003.
[4] C. Roberts, "Biometric attack vectors and defences," Computers & Security, vol. 26, no. 1, pp. 14–25, 2007.

[5] J. Unar, W. Senga, A. Abbasia, " A review of biometric technology along with trends and prospects", Pattern recognition, vol. 47, pp. 2673–2688, 2014.
[6] A. K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
[7] D. Zhang, Z. Liu, J. Q. Yan, P. F. Shi, "Tongue-print: A novel biometrics pattern", In Advances in Biometrics, vol. 4642, pp. 1174–1183, 2007.
[8] F. Monrose, A. Rubin, "Authentication via keystroke Dynamics", In Proceedings of the 4th ACM conference on Computer and communications security, Switzerland, pp. 48–56, 1997.
[9] P. R. Dholi, K. P. Chaudhari, "Typing pattern recognition using keystroke Dynamics", Mobile Communication and Power Engineering, vol. 296, pp. 275-280, 2013.
[10] S. Liu, M. Silverman, "A practical guide to biometric security technology", IT Professional, vol. 3, no. 1, pp. 27-32, 2001.
[11] A. K. Jain, R. Bolle, S. Pankanti, "Biometrics: personal identification in networked society", Springer Science & Business Media, 1999.
[12] BBC, "Biometrics: Technologies and Global Markets", [Çevrimiçi]: http://www.bccresearch.com/market-research/information-technology/ biometrics-technologies-ift042d.html. [Erişim Tarihi: 14 Ağustos 2015]
[13] Z. Zhang, D. Yi, Z. Lei, S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions", IEEE International Conference on. Automatic Face & Gesture Recognition and Workshops (FG 2011), USA, pp. 436–441, 2011.
[14] A. Hadid, "Face biometrics under spoofing attacks: vulnerabilities, countermeasures, open issues, and research directions," IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), USA, pp. 113–118, 2014.
[15] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, no. 3, pp. 614–634, 2001.
[16] B. Cukic, N. Bartlow, "Biometric system threats and countermeasures: a risk based approach," in Proceedings of the Biometric Consortium Conference (BCC05), USA, 2005.
[17] A. K. Jain, A. Ross, S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.
[18] J. Galbally, "Vulnerabilities and attack protection in security systems based on biometric recognition," IEscuela Politecnica Superior, Universidad Autónoma de Madrid, PhD Tezi, 2009.
[19] A. O. Alaswad, A. H. Montaser, F. E. Mohamad, "Vulnerabilities of biometric authentication 'threats and countermeasures'," International Journal of Information & Computation Technology, vol. 4, no. 10, pp. 947–958, 2014.