T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

HASTANE OTOMASYON SİSTEMLERİNDE YÜZ TANIMA SİSTEMLERİNİN KULLANIMI

(Yüksek Lisans Tezi)

Tezi Hazırlayan:

Mehmet ŞAM

İstanbul, 2018

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

HASTANE OTOMASYON SİSTEMLERİNDE YÜZ TANIMA SİSTEMLERİNİN KULLANIMI

(Yüksek Lisans Tezi)

Tezi Hazırlayan:

Mehmet ŞAM

Öğrenci No:

120820011

Danışman:

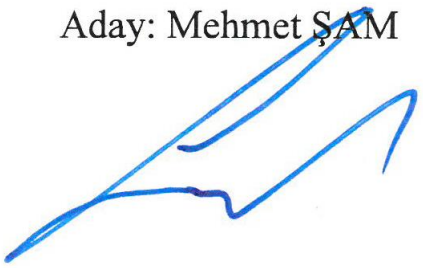
Yrd. Doç. Dr. Ediz ŞAYKOL

İstanbul, 2018

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Hastane Otomasyon Sistemlerinde Yüz Tanıma Sistemlerinin Kullanımı” başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmanın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım.

Aday: Mehmet ŞAM



T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi 120820011... no'lu .....MEHMET.....ŞAM...'in ..../..../2018 tarihinde yapılan tez savunma sınavı[1] sonucunda 45 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle KABUL... kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ

Programı : BİLGİSAYAR MÜHENDİSLİĞİ

Tez Başlığı[3] : Hastane Otomasyon Sistemlerinde Yüztanıma Sistemlerinin Kullanımı

Tez Sınav Jürisi	**Öğretim Üyesi**	**İmza**
Danışman	: Yrd.Doç.Dr.Ediz ŞAYKOL	
Üye	: Doç. Dr. Gökhan SİLAHTAROĞLU	
Üye	: Yrd.Doç.Dr. Turhan KARAGÜLER	

---

[1] Jüri üyeleri söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez savunma sınavına alır. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda jüri en geç onbeş gün içinde toplanarak adayı tez savunma sınavına alır. Tez savunma sınav süresi en az 45 dakikadır. Yüksek lisans tez savunma sınavı, tez çalışmasının sunulması ve bunu izleyen soru-yanıt bölümlerinden oluşur ve dinleyiciye açıktır. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-3)

[2] Tez sınavının tamamlanmasından sonra jüri, tez hakkında "kabul", "düzeltme" veya "red" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış sınav tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi başarısız bulunan öğrencinin Enstitü ile ilişiği kesilir. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve yönetmelikte belirtilen usullere uygun olarak tezini aynı jüri önünde yeniden savunur. Bu savunma sınavında da tezi kabul edilmeyen öğrencinin enstitü ile ilişiği kesilir.(Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

[3] İleride doğabilecek aksaklıkların engellenmesi için tezin başlığının yazılması gerekmektedir.

Adı ve Soyadı : Mehmet ŞAM

Danışmanı : Yrd. Doç. Dr. Ediz ŞAYKOL

Türü ve Tarihi : Yüksek Lisans, 2018

Alanı : Bilgisayar Mühendisliği

Anahtar Kelimeler : Biyometrik Sistemler, Hastane Otomasyon Sistemleri, Yüz Tanıma Sistemleri

ÖZ

HASTANE OTOMASYON SİSTEMLERİNDE YÜZ TANIMA SİSTEMLERİNİN KULLANIMI

Biyometrik tanıma sistemleri günümüz dünyasında pek çok alanda kullanılmaktadır. Parmak izi tarama, avuç içi damar tanıma gibi yaygın kullanılan yöntemlerin de aralarında bulunduğu biyometrik sistemlerin yanında, yüz tanıma gibi, insanları ayırt edecek kimlik doğrulama sistemleri insanın biyolojik yapısından yararlanarak bireyin kimliğini belirlemeyi ve doğrulamayı amaçlar.

Bu çalışmada biyometrik sistemlerin ayrıntılarına değinilmiş ve çeşitleri detaylandırılmıştır. Bu çeşitler arasından yüz tanıma sistemlerine ayrıntıyla yer verilmiş, ardından, hastane kavramı incelenerek, yüz tanıma sistemlerinin olası kullanım alanları incelenmiş, sonuç bölümünde ise, uygulama önerileri anlatılmıştır.

Bu bağlamda, yüz tanıma sistemlerinin faydaları üzerinde durulmuş ve hastane otomasyon sistemlerinde kullanımı önerilmiştir. Ayrıca, hastane otomasyon sistemlerinde var olan avuç içi damar tanıma sistemlerine alternatif olarak yüz tanıma sistemlerinin kullanımının avantajlarına değinilmiştir.

Name and Surname : Mehmet ŞAM

Supervisor : Asst. Prof. Ediz ŞAYKOL

Degree and Date : Master, 2018

Major : Computer Engineering

Key Words : Biometric Systems, Hospital Automation Systems, Facial Recognition Systems

ABSTRACT

USE OF FACE RECOGNITION SYSTEMS IN HOSPITAL AUTOMATION SYSTEMS

Biometric recognition systems are used in many fields in today's world. In addition to biometric systems such as fingerprint scanning and palm vein recognition, authentication systems that distinguish people, such as face recognition, aim to identify and verify the individual's identity by making use of the biological structure of the human being.

In this study, the details of the biometric systems are mentioned and their types are detailed. Facial recognition systems were explained in detail, then the hospital concept was examined and the possible uses of facial recognition systems were examined. In the conclusion, the application proposal was explained.

In this context, the benefits of face recognition systems are emphasized and their use in hospital automation systems is proposed. In addition, the advantages of using face recognition systems as an alternative to palm vein recognition systems in hospital automation systems have been addressed.

İÇİNDEKİLER

Sayfa No.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

1. GİRİŞ

Hızlı ve güvenli bir şekilde kaliteli bakım sağlamak için dönüşüm sürecinde olan sağlık sistemi çok yönlü sorunlar yaşamaktadır. Bu süreçte, bilgisayar ağı çok hayati bir rol oynamaktadır ve uygulanmada çok büyük katkıları olmuştur. Ancak örneğin, bilgisayar ağı sistemlerini yetkisiz kullanıma karşı koruyan ancak yanlış bir güvenlik duygusu sağlayabilecek şifreler gibi problemler de mevcuttur. Bazıları kolayca tahmin edilen şifreleri kullanır ve böylece yetkisiz erişimi kolaylaştırır. Hasta kayıtları hasta bakımı için hayati öneme sahiptir, ancak eksik sağlık kayıtları veya yanlış bilgi veya başka bir hastanın kaydıyla karıştırılması yanlış ilaç ile sonuçlanabilir. Buna ek olarak, kayıtlar yanlış kişinin elindeyse, hastanın sağlığı için büyük bir tehlike oluşturabilir.

Biyometrik tanımlama sistemleri, ses, yüz ve imza taramaları biçimindeki biyolojik verilerin kullanılmasını sağlar. En yaygın fizyolojik biyometrik olarak parmak tarama, retina tarama, el tarama ve iris tarama bulunmaktadır. Biyometrik tanımlama unutulmayacak veya çalınamaz ve genetik verileri elde etmek, analiz etmek, depolamak, yönetmek ve iletmek için kullanılan bilişim teknolojilerini içerir.

Bir hastane, uzman personel ve teçhizat ile hasta muayenesi sağlayan sağlık hizmetleri kurumudur. Hastanelerin ana görevleri, doktorlar tarafından hastalıkların konsültasyonu ve teşhisi, tedavi hizmetlerinin sağlanması, hastalara yataklar, bakım ve ilaçlar gibi hizmetleri sağlanması, aşı uygulamaları yapmakta olup, tedavi için hastaneye gelen hastalar hakkında bilgi kaydını ve faturalama: işlemlerini de gerçekleştirmektedirler. Hastalar bahsedilen hizmetleri vermekle olduğu kadar, aşı kaydını tutmak, hastaları tedavi etmek için mevcut olan çeşitli hastalık ve ilaçlarla ilgili bilgi toplama gibi görevlere de sahiptir.

Bu bağlamda hastaların ve hastanenin kendi finansal kayıtlarının otomasyon sistemlerinde tutulması önem taşımaktadır. Otomasyon bilgi sistemleriyle bütünleşik halde uygulanan bütün araçların, karşılıklı bağıntılı ve güvenilir bir şekilde kullanılmasıdır. Hastane otomasyon sistemleri ise, hastane bilgi yönetim sistemi

şeklinde yürütülerek, hastaların, medikal, özlük ve mali bilgilerinin kayıt ve tanıma yönetimidir.

Otomasyon sistemlerinin güvenilirliğinin sağlanması, çeşitli biyometrik sistemlerle sağlanmaktadır. Biyometrik sistemler, kişinin parmak izi, iris veya yüz gibi ayırt edici fizyolojik özelliklerine, imza, ses veya tuş vuruş dinamikleri gibi kendine özgü davranışsal özelliklerine dayalı kimlik doğrulamasının otomatik yöntemleri olarak tanımlanmaktadır.

Yüz tanıma teknolojisi, sıkça uygulanan bir biyometrik sistemdir. Genellikle bu sistemler, spesifik özellikleri yüz görüntülerinden elde eder ve sonrasında bu özellikleri kullanarak yüz eşleştirmeyi gerçekleştirir. Bir yüzün belirli özellikleri olan gözler arasındaki mesafeyi, burun genişliğini, elmacık kemiklerinin pozisyonunu, çene çizgisini, çene ve benzeri faktörleri kullanmakta olan bu sistemin güvenilirliği bu diğer biyometrik tanıma yöntemlerinden biraz daha düşüktür. Bununla birlikte, özellikle kullanıcı için kolaylığı göz önüne alındığında birçok uygulama için uygundur.

Bu bağlamda, bu ilişkinin açıklanması açısından çalışmanın birinci bölümünde, biyometri kavramına yer verilerek, biyometrik sistemlerden bahsedilmiş ve aşamalarına yer verilmiştir. Biyometrik sistemlerin çeşitleri anlatıldıktan sonra, yüz tanıma sistemleri detaylı ve ayrı olarak ele alınmış ve bir sonraki bölümde hastane otomasyon sistemlerinden bahsedilmiştir. Son bölümde ise bu iki kavramın birlikte kullanımına değinilmiştir.

2. BİYOMETRİ

2.1. Biyometrinin Tanımı

"Biyometri" kelimesi Yunanca kökenli olup; biyo (hayat) ve metrik (ölçmek) kelimelerinin türemesiyle oluşmaktadır. Otomatik biyometrik sistemler, bilgisayar işlem alanındaki önemli gelişmelere bağlı olarak, ancak yıllarda kullanımı artan sistemlerdir. Ancak bu yeni otomatik tekniklerden çoğu, yüzlerce, hatta binlerce yıl önce tasarlanmış fikirlere dayanmaktadır. İnsanlar tarafından tanınması için kullanılan en eski ve en temel örneklerden biri de yüzdür. Medeniyetin başlangıcından bu yana, insanlar bilinen (tanıdık) ve bilinmeyen (yabancı) kişileri tanımlamak için yüzü kullanmıştır. Nüfus arttıkça bu basit görev gittikçe zorlaşmakta ve bireylerin, bilinçsizce sergilediği davranışsal özellikler de kullanılmaya başlamıştır [1].

1800'lü yılların ortalarında, sanayi devrimi ve tarımın verimli hale gelmesiyle kentler hızla büyümüş, insanların belirlenmesi için resmen bir ihtiyaç haline gelmiştir. 1800'lerin sonlarına doğru, parmak izlerinin kaydını tutmak için bir yöntem geliştirilmiştir. Gerçek biyometrik sistemler 20. yüzyılın ikinci yarısında bilgisayar sistemlerinin ortaya çıkması ile başlamıştır. Yeni oluşum alanı 1990'lı yıllarda bir patlama yaşamış ve 2000'li yılların başında günlük uygulamalarda yüzeye çıkmaya başladı [2].

Biyometri, kimlik belirlemek veya doğrulamak için fizyolojik veya davranışsal özelliklerin otomatik olarak kullanılmasıdır. Burada, otomatik kullanım, fizyolojik veya davranışsal özellikleri doğrulamak veya belirlemek için insan yerine bilgisayarlar veya makineler kullanmak anlamına gelmektedir. Fizyolojik veya davranışsal özellikler, biyometrinin temel ölçümünü sağlayan ayırt edici özellikleridir [3].

Fizyolojik biyometri, parmak tarama, yüz tarama, iris tarama, el tarama ve retina tarama gibi insan vücudunun bir bölümünün doğrudan ölçümlerine dayanır. Davranışsal biyometri, bir eylemden elde edilen ölçümlere ve verilere dayanır ve dolayısıyla sesli tarama ve imza tarama gibi dolaylı olarak insan vücudunun özelliklerini ölçer. Zaman unsuru, davranışsal biyometri için esastır çünkü zamanla değişebilir [4].

Biyometri, bir kişinin iddia ettiği kimliği tanımlamak veya doğrulamak için kullanılabilen ölçülebilir, sağlam, ayırıcı fiziksel özellik veya kişisel nitelik olarak da tanımlanabilir. Biyometrik kimlik doğrulama, yaşayan bir kişinin kimliğini tanımlama veya doğrulama yöntemlerini belirtir. Ölçülebilir olma, bir karakteristiğin veya özelliğin, bir sensöre kolayca sunulabilecek ve ya dijital bir formata dönüştürülebilecek şekilde sayısal veri haline getirilebilecek olma anlamına gelmektedir. Bu, otomatik eşleme işleminin birkaç saniye içinde gerçekleşmesini sağlar. Biyometrik sağlamlık, bahsedilen karakteristik veya özelliğin zaman içindeki önemli değişimlere maruz kalma derecesinin bir ölçüsüdür. Bu değişiklikler yaş, yaralanma, hastalık, mesleki kullanım veya kimyasal maddelere maruz kalınması sonucu ortaya çıkabilir. Oldukça sağlam biyometrik ölçümler zamanla önemli ölçüde değişmez. Daha az sağlam bir biyometrik özellikler de bulunmaktadır. Örneğin, bir kişinin yaşamı boyunca çok az değişen iris, bir sese göre daha sağlamdır [5].

Farklılık, genel popülasyonda biyometrik modeldeki varyasyonların bir ölçüsüdür. Farklılık derecesi ne kadar yüksekse, tanımlayıcı da o kadar özeldir. Ayrım derecesinin en yüksek derecesi, benzersiz bir tanımlayıcı anlamına gelir. Düşük derecede farklılık, genel popülasyonda sıkça bulunan biyometrik bir düzeni gösterir. İris ve retinanın el veya parmak geometrisinden daha yüksek ayrım derecesi vardır. Uygulama, sağlamlık derecesini ve belirginliği belirlemeye yardımcı olur [6].

2.2. Biyometrik Sistemlerin Öğeleri

Biyometri, kişinin tanımlanması ya da doğrulamasına olanak tanıyan fiziksel özelliklerin sayısal temsilidir. Biyometri fiziksel veya davranışsal olabilir. Fiziksel biyometri, kişinin parmak izi, el geometrisi ve iris veya retinal desenler gibi fiziksel özelliklerine odaklanır. Davranışsal biyometri, bir kişinin yürüme biçimine veya klavyede yazdığı şekilde hareketlerini ölçer [7].

Tüm biyometrik sistemler katılım, eşleştirme ve şablon olmak üzere üç temel öğeden oluşur [8].

2.2.1. Katılım

Katılım, bir kişiden biyometrik örnekler toplama ve sonraki bir şablon oluşturma işlemidir. Genellikle, cihaz aynı biyometrik özellikten üç örnek alır ve daha sonra bir kayıt şablonu üretmek için bunların ortalaması alır [8].

Biyometrik bir sistem için önemli bir aşama olan katılım sırasında birey, ölçülecek olan öğeyi veya işlemi ölçüm aygıtına veya tarayıcıya sunar. Cihaz taramayı yapar ve yazılım, ayarlanmış algoritmalara dayalı olarak görüntünün sayısal bir temsilini üretir. Örnek olarak; parmak izinde, kişi parmağını tarayıcıya yerleştirir. Tarayıcı parmak izi desenini bir veya daha fazla okumakta ve sistemin kendine özgü algoritmik ayarlarını uygulamaktadır. Belirli parmak izi desenine dayanarak sayısal bir dize oluşturulur ve bu sayı biyometrik şablon olarak saklanır [9].

Kayıt modülü, sistemin belirli bir kişiyi tanımlamasından sorumludur. Kayıt aşamasında, biyometrik bir sensör, kişinin fizyolojisini dijital bir temsil oluşturmak için tarar. Bir özellik çıkarıcı, bu gösterimi, şablon adı verilen daha kompakt ve etkileyici bir gösterim üretmek için işler. Yüzdeki bir görüntü için bu özellikler göz, burun ve ağızın boyutunun konumlarını içerebilir. Her kullanıcı için şablon bir biyometrik sistem veri tabanında saklanır; Veri tabanı, her bir kullanıcının şablonunun bir akıllı kartta saklandığı ve kullanıcıya verildiği gibi merkezi veya dağıtılmış bir veri tabanı olabilir [10].

2.2.2. Şablon

Sunumda, önceden kaydolan kişi, öğeyi (örneğin parmak) tekrar sunar. Bu sefer amaç, bireyi sisteme kaydetmek değil, kişinin iddia ettiği kişi olduğunu doğrulamak ya da kişileri bir havuzdan tanımlamaktır. Parmak izi taramasının önceki örneğini elinde bulunduran kişi, parmağını tarayıcıya yerleştirir ve aynı algoritma uygulanır. Ortaya çıkan sayısal şablon kayıtlı şablonla karşılaştırılır ve eşleşmeleri halinde erişim izni verilir.

Bu aşama, kayıtlı kişinin biyometrik bilgilerini temsil eden verilerdir. Kayıtlı kişinin örneklerinden o teknolojiye uygun özellikleri çıkarmak için uygun algoritmayı kullanan biyometrik cihazlarla yaratılırlar. Bu özelliklere parmak izi sistemleri gibi bazı teknolojiler için “minutiae” noktaları da denir. Şablonlar yalnızca

bir kişinin biyometrik karakteristiğinin veya özelliklerinin ayırt edici özelliklerinin bir kaydı olduğu için genellikle küçüktür ve kimlik doğrulama için biyometrik ölçümün hemen anlık işleme zamanı özelliğini sağlar. Bazı şablonların küçük boyutu, plastik kartlara veya akıllı kartlara yerleştirilen manyetik şeritler veya barkodlarda depolamaya izin verir [8].

Biyometrik sistemlerin temeli, kayıtlı şablonun depolanmasını içerir. İşlemek için kayıtlı biyometrik şablon, yeni sunulan parmak izi ve sonuç şablonu ile karşılaştırmak için kullanılabilir olmalıdır. Ancak sistemin, kayıtlı şablonu saklayacağı yer önemlidir. Kayıtlı şablon sisteme yerleştirildiğinde ve şablonun şahsın elinde bulunduğunda (ör. bir akıllı kart üzerinde) genelde "okuyucu, panel veya sistemdeki depolama" terimleri kullanılır. Bu, önemsiz bir farklılık gibi görünse de, anti-biyometrik özel muhalefet argümanlarının çoğunun kökenini oluşturur. Şablon sisteme sahipse, varsayılan olarak kişinin mutlak kontrolü dışındadır. Bu, gizlilik savunucuları arasında kayda değer endişe kaynağı olmuştur. Şablon yalnızca kişinin mülkiyetinde kalan bir karta yerleştirilirse, bu endişe hafiflemiş olur [11].

Biyometrik bir sistemin çalışabilmesi ve sunulan bir şablonun eşleşebilmesi için kayıtlı bir şablonun veya şablonların kayıtlı olduğu bir veri tabanın varlığı gerekir. Tıpkı şablonun bulunduğu yerin biyometrik sistemlerin önemli bir ayırt edicisi olduğu gibi bu karşılaştırma veya eşleme işlemi için de yer olması gerekir.

2.2.3. Eşleştirme

Eşleştirme, gönderilen biyometrik örneği sistemin veri tabanındaki bir (doğrulama) ve ya çok sayıda (tanımlama) şablonla karşılaştırma işlemidir. Bir eşleştirmenin başarısız olmasının üç yolu vardır. Bunlar kaydolmanın başarısız olması, yanlış eşleme ve yanlış eşleşmemedir. Kaydolma (veya edinme) başarısızlığı, teknolojinin bu teknolojiye uygun ayırt edici özellikleri ayıklamadaki başarısızlığıdır. Bu başarısızlığın iki nedeni vardır: bireyin (örneğin) parmak izleri, sistem tarafından alınacak kadar belirgin değildir ve ya kişinin yaşı veya mesleği, kişinin parmak izinin ayırt edici özellikleri değiştirilmiştir [8].

Ayrıca, yanlış eşleşme veya eşleşememe olasılığı da vardır. Bu iki terim sırasıyla "yanlış kabul" ve "yanlış ret" olmakla birlikte, bu terimlerin anlamı

uygulamaya bağlıdır. Yanlış eşleşme, veri tabanında, kişinin kendine ait olmayan bir şablonla eşleşmesi anlamına gelmekteyken, yanlış eşleşme de veri tabanında şablon bulunmasına rağmen eşleşmenin gerçekleşmemesidir.

Tanıma modülü kişiyi tanımakla sorumludur. Tanımlama aşamasında biyometrik sensör, tanımlanacak kişinin karakteristik özelliklerini yakalar ve şablonla aynı dijital biçimde dönüştürür. Ortaya çıkan şablon, özellik eşleştiricisine gönderilir; bu özellik, iki şablonun eşleşip eşleşmediğini belirlemek için depolanan şablonla karşılaştırır. Kimlik doğrulama, iddia edilen bir kimliğin doğrulanması veya kimlik tespiti, bilinen kişilerin bir veri tabanından bir kişinin kimliğinin belirlenmesi şeklinde olabilir. Bir doğrulama sisteminde, yakalanan karakteristik ve talep edilen kimliğin depolanmış şablonu aynı olduğunda, sistem talep edilen kimliğin doğru olduğuna karar verir. Bir tanıma sisteminde, yakalanan karakteristik ve saklanan şablonlardan biri aynı olduğunda, sistem eşleşen şablonu olan kişiyi tanımlar [2].

Biyometrik bir eşleştirme, şablonun saklanmasıyla aynı iki temel alanda gerçekleştirilebilir: sistemde veya kartta. Buradaki püf nokta yine kişinin biyometrik şablonunun bulunduğu yerdir. Eşleştirme işlemi sistem üzerinde gerçekleştirilirse, bu tanım gereği bireyin mutlak kontrolü dışındadır. Bu nedenle birçok sistem, akıllı kartın işlem kapasitesini kullanarak kart üzerinde eşleme işlemini gerçekleştirmek üzere tasarlanmıştır. Bu senaryoda, kayıtlı biyometrik hiçbir zaman kartı terk etmemektedir ve böylece daha az bir tehlike altına girmiş olmaktadır [9].

Neredeyse her biyometrik temsilcisinin kanıtlayacağı gibi, gerçek fiziksel veya davranışsal özelliği bir biyometrik şablondan elde etmek imkânsızdır. Parmak izi örneği kullanılarak, taranan parmak izi görüntüsündeki belli başlı noktalara dayanan bir dizi basamakta matematiksel olarak özetlenmiştir. Rakam dizisine sahip olan birisi parmak izini yeniden oluşturamamaktadır. Bir kişinin fiziksel görünümünü tanımlamak da benzer özellik göstermektedir. Kişinin boyu 1.80 olabilir ve kahverengi gözleri ve siyah saçları olabilir. Hatta sağ kulağında bir doğum lekesi olup ve sol gözünün üstünde küçük bir yara izi de olabilir. Bu açıklama, bir kişiyi tanımlamak için kullanılabilir ancak kişinin veya benzerinin doğru şekilde yeniden oluşturulması imkânsızdır [7].

2.3. Biyometrik Sistemler

Çeşitli biyometrik teknolojiler, farklı fiziksel özelliklere odaklanır. Biyometrik yazınında, bu farklı uygulamalar "yöntemler" olarak anılır. Ortaya çıkan bazı biyometrik yöntemler bulunmaktadır. Bunlar; el, yüz, parmak izi, yürüyüş, imza, ses, iris, retina, damar, DNA, kulak ve dudaktır. Genellikle biyometrik yöntemler dört tipe ayrılabilir. Bunlar, eller, kafa ve yüz, diğer fiziksel özellikler ve davranışsal özelliklerdir [4].

Aşağıda alt başlıklar halinde tanıma sistemlerinden bahsedilecek ve daha sonra yüz tanıma sistemleri ayrıntılı bir şekilde incelenecektir. Yaygın kullanılan fiziksel ve davranışsal biyometrik sistemler aşağıda verilmiştir.

Tablo 1. Fiziksel Ve Davranışsal Biyometrik Sistemler

Fiziksel	**Davranışsal**
Yüz Tanıma	İmza
El Tanıma	Ses
İris Tanıma	Tuş Vuruşu
Retina Tanıma	Yürüyüş
DNA	Dudak Hareketleri
Damar Tanıma	Vücut Kokusu
Kulak Tanıma	
Parmak İzi	

Kaynak: Jain, Shruti, Surabhi Gupta, and Raj Kumar Thenua. "A review on Advancements in Biometrics." Int J Electron Comput Sci Eng 1 (2012): 853-9.

İnsanların kimliklerini belirleme veya doğrulama farklı şekillerde yapılabilir. İnsan beyni, yüzlerine bakarak veya seslerini duyarak insanları tanıyabilir. Bununla birlikte, otomatik bir dünyada, insanların biyometri kullanarak otomatik olarak tanınması giderek daha fazla önem ve ilgi kazanmaktadır. Biyometrik sistemler, kişinin parmak izi, iris veya yüz gibi ayırt edici fizyolojik özelliklerine, imza, ses veya tuş vuruş dinamikleri gibi kendine özgü davranışsal özelliklerine dayalı kimlik doğrulamasının otomatik yöntemleri olarak tanımlanmaktadır.

Doğrulama ve tanımlama olarak bilinen iki tür biyometrik sistem vardır. Doğrulama sistemi, belirli bir kimliğin sahibi olduğunuzu iddia eder. Diğer bir deyişle, kullanıcının kimliğini doğrulamak için tek bir eşleşme yapılır. Doğrulama sistemlerine çoğunlukla kredi kartı ve bankacılık işlemleri, ağ oturum açma işlemleri ve cep telefonlarında ihtiyaç duyulmaktadır. Öte yandan, bir tanımlama sisteminde, kişisel biyometrik bir karakteristik sunulmakta ve sistem, belirli bir kişinin kimliğini bir dizi özellikte bulmaya çalışmaktadır. Kimliklendirme sistemleri çoğunlukla ceza soruşturmalarında ve ya sınır denetimlerinde kullanılır. Biyometrik doğrulama, tek bir eşleşme yerine bir veri tabanı araması gerektirdiğinden, biyometrik tanımlamadan daha zor bir iştir. Her şeyden önce, tanımlama veya doğrulama işlemini gerçekleştirmek için öncelikle kişi sisteme kaydolmalıdır. Kayıt aşamasında, biyometrik özelliğin belirgin özellikleri ayrıştırılır ve sistemin veri tabanında saklanır. Bundan sonra kişi doğrulama veya tanımlama aşamasında kimliğini ispatlayarak uygulamayı kullanabilir. Bu işlemlerin her ikisinde de mevcut ve sorgu şablonlarına ait bir algoritma veya bir işlev uygulanır ve bunların benzerliği ölçülür. Eğer yeterince yakınlarsa, diğer bir deyişle, farkları bir eşiğin altında ise, kullanıcının tanımlanması beklenir. Yukarıda da belirtildiği gibi, biyometri bir kişinin fizyolojik veya davranışsal özellikleri olabilir [11].

Fizyolojik özelliklere bir örnek olarak, parmak izleri, “minutiae” adı verilen sırtlarda detay noktaları ile temsil edilir. Parmak izleri, en çok kullanılan biyometrik verilerdir, çünkü geçmişte suçluları tanımak için polis tarafından kullanılmıştır. Dolayısıyla insanlar buna daha fazla aşinadırlar. Iris, iris üzerindeki desenleri gösteren ikili bir dize olan iris kodu ile temsil edilir. Her ne kadar iris kalıpları parmak izlerinden daha detaylı olsa da, mükemmel bir edinim ortamı oluşturmak, parmak izi taramasından daha zordur. Ayrıca, yüzler insan beyninin en çok kullanılan tanıma nitelikleridir. Dijital sistem, yüzeylerin özelliklerin göreceli konumlarına, boyutlarına ve şekillerine göre tanır. Bu nedenle, yüz tanıma, baş pozisyonu, ifadeler ve yüz tüyleri gibi değişikliklere karşı çok hassastır. El geometrisi elin üç boyutlu bir şablonunu oluşturur. Ancak bir el geometrisi biyometrik sistemi, yapay bir elle kandırılabilir ve insanlar arasında çok belirgin değildir. Fizyolojik özelliklere bir alternatif olarak davranışsal özelliklerin yakalanması daha kolaydır. İmza dinamiği, imza doğrulama işlemini

otomatikleştirmek için çoğunlukla finansal uygulamalarda gerekli olan davranışsal özelliklere bir örnektir. Ayrıca, ses normal bir cihaz kullanılarak kaydedilebilir ve bundan sonra sesin dalga biçimleri tanıma sürecinde kullanılır. Ses taklit edilebilmesine rağmen, konuşmanın özellikleri de bazı fizyolojik yönleri içerir ve kimliğine bürünmek neredeyse imkânsızdır. Tuş vuruş dinamiklerinin ise klavyeden yakalanması çok kolaydır. Doğrulama süreci, bir uygulamanın düzenli akışında gizlendiğinden tanımlanacak kişiyi rahatsız etmez.

Fizyolojik ve davranışsal özelliklerin temel farkı kalıcılıklarıdır. Fizyolojik özellikler davranışsal olanlardan daha kararlıdır. Bir kişinin hayatı boyunca hemen hemen aynı kalırlar. Öte yandan, duygusallık, nörolojik hastalıklar, ses kısıklığı vb. gibi kontrol edilebilir ve kontrol edilemeyen nedenlerden ötürü davranışsal özellikler zaman içinde değişir. Dolayısıyla, davranışsal özellikleri kullanan biyometrik sistemler, her kullanımdan sonra şablonlarını güncellemektedir. Dolayısıyla, davranış biyometrik sistemleri sıkça kullanıldıklarında daha iyi çalışırlar. Fizyolojik özellikleri kullanan sistemler, kalıcılık, evrensellik, ayırt edici olma ve performans bakımından davranışsal olanlardakinden daha iyi performans gösterirler. Öte yandan, davranışsal özelliklerin toplanması daha kolaydır ve insanlar onları kullanmaya daha çok razıdır. Sonuç olarak, bir biyometrik tanıma sistemi tasarlarken, kullanılacak biyometrik verilerin türü ve sistem gereksinimleri ciddiye alınmalıdır.

Bir biyometrik sistem tasarlanırken, özelliklerin türünün yanı sıra, biyometrik verilerin gizliliği de düşünülmelidir. Biyometrik özellik gizli tutulmalı ve sadece amaçlanan kapsam için kullanılmalıdır. Buna ek olarak, kullanımı kolay olmalı ve biyometrik verileri yakalarken insanlar rahatsız edilmemelidir. Ayrıca, zamanlama ve bellek maliyetleri küçük olmalıdır. Sorgular, gerçek zamanlı uygulamalarda gecikmeye neden olmaksızın hızlı bir şekilde işlenmelidir. Milyonlarca insanın şablonları, çok büyük veri tabanlarında bile kabul edilebilir boyutlarda olmalıdır.

2.3.1. El Tanıma Sistemleri

El geometrisi sistemleri şu anda en çok kullanılan biyometrik teknolojiler arasında yer almaktadır. Biyometrik el tanıma sistemleri, elin genel yapısını, şeklini ve oranlarını ölçer ve analiz eder. Bu sistemin elde ölçtüğü bazı özellikler

bulunmaktadır. Bunlar; elin uzunluğu, genişliği ve kalınlığı, parmaklar ve eklemler, cilt yüzey alanının kırışıklığı gibi özellikleridir [12].

El biyometrisi el ve parmak geometrisine dayandığından, sistem kirli ellerle de çalışacaktır. Tek sınırlama, şiddetli arteriti olan ve ellerini okuyucuya açamayan insanlar içindir. Kullanıcı elinin avucunu okuyucunun yüzeyine yerleştirir ve parmağının doğru yerini gösteren kılavuz saplarla elini hizalar. Cihaz, kullanıcının tanımlanması ve doğrulanması için veri tabanını kontrol eder. Süreç standart olarak birkaç saniye sürer [13].

Kullanıcı kaydolmak için avucunu okuyucunun yüzeyine yerleştirir. Görüntü toplama sistemi, bir ışık kaynağı, bir kamera, basit bir ayna ve düz bir yüzeyi (beş mandalı olan) kapsar. Kullanıcı elini avucunu aşağı bakacak şekilde cihazın düz yüzeyine yerleştirir. Beş mandalı, kullanıcının sağ elinin uygun bir şekilde yerleştirilmesi için kontrol noktaları olarak hizmet eder. Cihaz aynı zamanda ışık kaynağının yoğunluğunu ve kameranın odak uzaklığını değiştirmek için düğmelere sahiptir. Yalnız ayna, kullanıcının elinin yan görüşünü kameraya yansıtmaktadır. Cihaz, elin üstten görünüşünün canlı bir görsel geribildirimini sağlayan bir GUI uygulamasıyla bilgisayara bağlanmıştır. GUI el görüntüsünü yakalamaya yardımcı olur [14].

Özellik ekstraksiyonu, çekilen görüntüyü kullanarak çeşitli konumların parmaklarının genişliklerini ve uzunluklarını hesaplamayı içerir. Bu metrikler, kullanıcının elinin özellik vektörünü tanımlar. Bir kalıp veya el dökümünü önlemek için, bazı el biyometrik sistemleri kullanıcıların parmaklarını hareket ettirmesini gerektirecektir. Ayrıca, el termografı elin ısısını kaydetmek için kullanılabilir veya cilt iletkenliği ölçülebilir. Bir kişinin eli belli bir yaştan sonra önemli ölçüde değişmez. Bireysel el özellikleri tanımlama için yeterince açıklayıcı değildir. Bununla birlikte, el biyometrik tanıma sistemleri, çeşitli bireysel özellikleri ve parmakların ve ellerin ölçümlerini birleştirirken doğrulama amacıyla doğrudur. El biyometrik tanıma sistemleri oldukça avantajlı olup kullanımı kolaydır. Diğer tanıma sistemlerine göre daha az veri gerekir. Bununla çok sayıda bağımsız şablon kolayca bağımsız bir cihazda saklanabilir. Bu biyometrik belleğin zayıf yönleri, parmak izi sistemleri ile karşılaştırıldığında oldukça doğru olmayan tarayıcının boyutu, ellerin

yaralanmaları el biyometrik sisteminin düzgün çalışmasını engelleyebilmektedir [15].

2.3.2. Yürüyüş Tanıma Sistemleri

Yürümenin biyometrik olarak eşsiz bir avantajı, diğer biyometri algılanamayacağı zaman uzaktan veya düşük çözünürlükte tanıma potansiyeli sunmasıdır. Tanıma, (statik) insan şekline ve harekete dayanarak daha zengin bir tanıma ipucu anlamına gelebilir. Ayrıca, yürüme, diğer biyometriğin gizlendiği durumlarda kullanılabilir; çünkü hareketi gizlemek zordur [16].

Erken tıbbi çalışmalar, yürüyüş analizinin temel ilkelerini ortaya koymuştur. Biyomekanik literatürü de benzer gözlemleri ortaya koymaktadır. Bu bağlamda "Belli bir kişi, yürüyüş şeklini oldukça tekrarlanabilir ve karakteristik bir şekilde yerine getirmekte olup, bir kişiyi kendi yürüyüşüyle tanınması mümkündür [17].

Öte yandan yürüyüş tanıma sistemlerinin belirli sınırlamaları bulunmaktadır. r. Araştırmalar, yürüme hızı, adım uzunluğu ve duruş ve salınım fazı zamanları gibi zamansal ve mesafe ölçümlerinde yaşla birlikte önemli değişiklikler ortaya çıkabileceğini göstermiştir. Buna ek olarak, frenleme ve itici fazlardaki ayak tepki kuvveti verileri ve ayak bileği, diz ve kalça eklem açısı gibi eklem açılı hareketi verileri yaşlanmanın etkilerini göstermiştir [18].

2.3.3. Retina Tanıma Sistemleri

İris tanıma, gözün yüksek çözünürlüklü görüntülerini kullanan bir biyometrik tanımlama teknolojisidir. Göz irisi kimlik doğrulama amacıyla oldukça örtüşmektedir. Çoğu durumda, hasarın ve yıpranmanın çoğundan korunan bu iç organ, pratik olarak düz ve tekdüzedir ve genetik olarak aynı ikizlerde bile benzersiz olan bir özelliktir [19].

İris tanımada ilk adım, iris işareti özelliklerini kullanarak irisin bulunmasıdır. Bu belirteç özellikleri ve irisin kendine özgü şekli görüntüleme, özellik izolasyonu ve görüntü çıkarımı için olanak tanır. İrisin iyi bir görüntüsünü elde etmek için, tanıma sistemleri çoğunlukla çoğu kamera tarafından gözlemlenebilen ancak insanlar tarafından tespit edilemeyen ya da insanlara yaralanmaya neden olabilen, yakın

kızılötesi ışının ışığıyla irisi aydınlatmaktadır. İris görüntüleri bir şablon oluşturmak için kullanılır [20].

Iris tanıma algoritmaları olağanüstü sonuçlar vermektedir. Daugman'ın algoritmaları, doğrulamada diğer yöntemlerden daha iyi doğruluk oranları üretmektedir. Daugman'ın çalışmalarından türetilen ticari bir sistem olan iris kodu, Birleşik Arap Emirlikleri'nde göç sürecinin bir parçası olarak kullanılmıştır. 200 milyondan fazla karşılaştırmanın ardından, bir tane dahi yanlış eşleşme olmamıştır [14].

2.3.4. Ses Tanıma Sistemleri

"Konuşmacı tanıma" olarak da bilinen ses tanıma sistemleri, doğrulama ve / veya tanımlama için kişinin sesini kullanan bir biyometrik modeldir. Ses tanıma, konuşma sırasında bireyler arasında farklılık gösteren akustik özelliklerini kullanır. Bu akustik modeller hem anatomiyi (boğazın ve ağızın boyut ve şeklini) hem de öğrenilen davranış kalıplarını (ses aralığı, konuşma stili, ton, frekans) yansıtır. Öğrenilen kalıpları ses şablonlarına dâhil etmek, bu sistemin fizyolojik yerine "davranışsal biyometrik" olarak sınıflandırılmasını sağlamıştır [21].

Ses biyometrik sistemleri, üç farklı stilde konuşma girdisi kullanmaktadır. Bunlar; metin bağımlılığı, metin gerektiren ve metin tabanlı metin girişi ve bağımsızdır. Çoğu ses doğrulama uygulaması, bir veya daha fazla ses şifresinin seçilmesi ve kaydedilmesini içeren, metin bağımlı girişi kullanır. Metin talep eden girdi, sahtekarlardan endişe duyulduğunda kullanılır. Sesli harfleri işlemek ve saklamak için kullanılan çeşitli teknolojiler, gizli marker modelleri, desen eşleştirme algoritmaları, sinir ağı ve matris gösteriminden oluşmaktadır. Ses tanıma sisteminin bazı güvenlik açıkları aşağıda verilmiştir [22].

• Sabit metin: Konuşmacı, kayıt sırasında önceden belirlenmiş kaydedilen bir sözcüğü veya deyimi söyler. Sözcük gizli olabilir, bu nedenle şifre gibi davranır, ancak bir kez kaydedildiğinde tekrarlaması oldukça kolaydır ve şifreyi değiştirmek için yeniden kayıt yapılması gerekir.

• Metin-bağımlı: Konuşmacı, kimlik doğrulama sistemi tarafından belirli bir şeyi söylemeye yönlendirilir. Makine, kullanıcıyı belirlemek için sözcüğü bilinen metne göre hizalar. Bunun için kayıt genellikle daha uzun olur, ancak metin isteğe göre değiştirilebilir. Sınırlı sistemler "splicing" tabanlı yeniden oynatma saldırılarına karşı savunmasızdır.

• Metin-bağımsız: Konuşmacı kimlik doğrulama sistemi hoparlörün herhangi bir konuşmasını işler. Burada konuşma görev odaklı olabilir, bu nedenle sahtecinin hedefini gerçekleştiren konuşmayı kaydetmek ve tekrarlamak zor olabilmektedir. İzleme sürekli olabilir ve söylendiği gibi, sistemin kullanıcının kimliğine olan güveni o kadar artar.

• Konuşma: Kimlik doğrulama sırasında, konuşma, gizli olan veya en azından bir taklitçi tarafından bilinmesi veya tahmin edilmesinin mümkün olmadığı bir bilgiyi sorgulayarak kimliği doğrulamak için bilinir.

2.3.5. İmza Tanıma Sistemleri

Biyometrik tanımlama ve kimlik doğrulama teknikleri, bir kişiyi tanımlamak için genellikle o kişiye benzersiz şekilde bağlı olan bazı fiziksel ölçümler veya göstergeler vasıtasıyla daha doğrudan bir araç sağlar. Mevcut ve önerilen biyometrik teknikler arasında parmak izleri, retina taramaları, iris kalıpları, yüz özellikleri olduğu kadar imza dinamikleri de bulunmaktadır.

Toplumumuzda, bir kişinin kendisini, başka bir insana veya bir bilgisayar sistemine tanımlaması ve kimliğini doğrulaması için geleneksel ve kabul gören bazı araçlar bulunmaktadır. Bu araçlar üç genel ilkeden birine veya birden fazlasına dayanabilmektedir. Bunlar: kişinin ne bildiğini (bazı paylaşılan gizli bilgiler); Sahip olduğu bir şey (bir çeşit benzersiz belirteç) ve ya onun fiziksel varlığı. Yazılı imza, bu özelliklerden biridir çünkü bir kişinin normal imzasının yavaşça değişmesi ve ya kasıtlı olarak değiştirilmesi çok zayıf ir ihtimaldir. Buna göre imza, yazılı bir belgeyi imzalayan kişiyi tanımlamanın birincil aracı olarak görülür [23].

Bu bağlamda; bu teknoloji bir kişinin kimliğini doğrulamak için imza dinamik analizini kullanır. Dinamik imza, kişinin adını imzalarken kullanılacak hızı

ve basıncı ölçer ve imzanın nasıl göründüğü ile ilgilenmez. Bir imza üretildiğinde kişinin kullandığı hız, basınç ve açı ölçümüne dayanır. Yaygın dinamik özellikler arasında imza vuruşlarının hızı, ivmesi, zamanlaması, basıncı ve yönü bulunur-hepsi X, Y ve Z eksenleri boyunca analiz edilmiştir. Bu özellikler, Kişisel Dijital Asistanlar (PDA'lar) veya dijital tabletler gibi sözleşmeye duyarlı teknolojileri kullanarak toplanır. Bu teknoloji için bir odak noktası, imza, kişisel kimlik doğrulamasında kabul edilen bir yöntem olan e-iş uygulamaları ve diğer uygulamalar olmuştur [24].

2.3.6. Parmak izi Tanıma Sistemleri

Parmak izleri, aynı yumurta ikizleri de dahil olmak üzere bir kişinin her parmağı için benzersizdir. Günümüzde piyasada bulunan en geniş biyometrik teknolojilerden biri olan masaüstü ve dizüstü erişim için de kullanılan parmak izi tanıma cihazları, birçok farklı satıcıdan düşük maliyetle geniş şekilde temin edilebilir. Bu cihazlarla kullanıcıların artık şifre yazması gerekmemekte; yalnızca bir dokunuş anlık erişim sağlanabilmektedir. Parmak izi sistemleri, tanımlama modunda da kullanılabilir [25].

Biyometrik parmak izi algılayıcısı, parmak izinin dijital bir resmini çeker. Parmak izi taraması, bir parmak izinin yükselti ve çukurlarını tespit eder ve onları bir ve sıfıra dönüştürür. Kompleks algoritmalar, "minutiae" olarak bilinen parmak izinin özelliklerini tanımlamak için bu ham biyometrik taramayı analiz eder. Minutiae bir şablonda saklanır, ancak tanımlama veya doğrulama için bunların bir alt kümesi ile uyuşması gerekir. Çoğu sistemde, 10 ila 20 arasında eşleşme yapılırsa, parmak izi bir eşleşme olarak kabul edilir [14].

2.3.7. Retina Tanıma Sistemleri

Retina, gözün arka tarafında bulunan kan damarlarının tabakası, benzersiz bir şekil oluşturur. Retina biyometrisi, genellikle en güvenli biyometrik yöntem olarak kabul edilmektedir [26].

Retinaya dayalı biyometri, gözün arka tarafında bulunan kan damarlarının tabakasını analiz etmektedir. Yerleşik bir teknoloji olan bu teknik, retinanın benzersiz modellerini taramak için optik bir birleştirici aracılığıyla düşük yoğunluklu

bir ışık kaynağı kullanmaktadır. Retinal tarama oldukça doğru olabilir, ancak kullanıcının bir kaba bakıp belirli bir noktaya odaklanmasını gerektirir. Gözlüklü ve ya bu cihaza yakın temas kurmak istemeyen bireyler, bu taramaya uygun değildir. Bu sebeplerden dolayı, retina taraması, iyi çalışsa da, tüm kullanıcılar tarafından sıcak bakılan bir uygulama değildir [27].

Retina tarayıcıları gözdeki kan damarlarını karşılaştırır. Düşük ışık kullanan bir tarama cihazı, retina üzerindeki benzersiz desenleri kıyaslar. Gözlüklerin varlığı, retina taramasını olumsuz şekilde etkiler. Bir retina taraması, parmak izi görüntüsüyle aynı veri hacmini üretir. Uygulamada, retina taraması çoğunlukla doğrulama için kullanılır. Göz imza şablonunun boyutu 96 bayttır. Retina taraması nadiren yapılır çünkü oldukça pahalıdır. Retina tarama, yüksek güvenlik gerektiren ve kullanıcının kabulünün önemli olmadığı uygulamalar için uygundur [28].

2.3.8. Damar Tanıma Sistemleri

Gözün retina üzerindeki damar desenleri, insanlar tarafından sahip olunan en eşsiz özelliklerden biri olarak bilinir. Bu model genetik olarak belirlenmemiştir, ancak her birey tarafından rasgele geliştirilmiştir. Bir kişinin hayatında en istikrarlı özelliklerden biridir. Damar yapısı veya "damar ağacı", kızılötesi ışık kullanılarak yakalanır [29].

Göz damar yapısı dışında el damar tanıma sistemleri de bulunmaktadır. Parmak izi tanıma ile karşılaştırıldığında, el damar tanıma sistemleri pek çok avantaja sahiptir. Bunlar [30];

1) Damar vücudun iç özellikleri olup, imal edilemez.
2) Damar tanıma temassızdır.
3) Damar özellikleri süreklidir.

Parmak damarı tanıma sistemleri ise, biyometrik bir tanımlayıcı olarak aşağıdaki özelliklere sahiptir [31]:

1) Damar vücut içinde gizlendiğinden ve çoğunlukla insan gözü için görünmez olduğundan çalınması oldukça zordur.

2) İnvaziv olmayan ve temassız yakalama, kullanıcı için kolaylık ve hijyen sağlarken kullanıcı tarafından kabul edilmesi daha kolaydır.

3) Kişinin on parmağıyla da doğrulanabilen bir sistemdir.

Parmak damarı tanıma sistemlerinin ise iki zorluğu bulunmaktadır. Bunlar;

1) Parmak damarlarının kızıl ötesi görüntülerinin kalitesi tanıma performansını önemli ölçüde etkiler.

2) Parmak damarının doku bilgisini sınırlıdır ve parmağın poz varyasyonu, parmak damarının kızılötesi görüntüsünü etkiler [32].

2.3.9. DNA Tanıma Sistemleri

DNA (deoksiribonükleik asit), her insan hücresinde bulunan iyi bilinen çift sarmal yapıdadır. Bir DNA örneği ya DNA parmak izi ya da bir DNA profili üretmek için kullanılır. DNA numunelerini elde etmek için mevcut işlemler oldukça müdahaleci olup doku, kan veya diğer vücut örneklerinden bir miktar gerektirir. DNA testi, çok yüksek bir doğruluk derecesine sahip bir tekniktir. İstatistiksel örneklemede, aynı profile sahip iki kişinin buluma şansının 6 milyarda bir olacağını göstermektedir. Mono zigot ikizler dışında insanlar için mevcut en belirgin biyometrik belirteçtir. DNA, kişinin yaşamı boyunca değişmez; Bu nedenle kalıcılığı inkâr edilemez. Günümüzde adli tıp ve babalık testlerinde kullanılmaktadır [14].

2.3.10. Kulak Tanıma Sistemleri

Dış kulak şekli, loblar, kemik yapısı ve boyutu her insan için özgündür. Kulak kalıbı tanıma, fiziksel temassız olarak kullanılır ve kulak şeklini doğrulamak için bir optofon kullanır. Bir Fransız şirketi olan ART Teknikleri, optofon sürecini geliştirmiş ve iki bileşenden (ışık kaynağı ve kameralar) oluşan bir telefon tipi ahize haline getirmiştir. Bir palmiye baskısı veya parmak izinin “minutiae” noktaları gibi, dış kulağın ölçülebilen ve biyometrik bir şablonla karşılaştırılabilen birçok ayrıntılı özelliği vardır.

2.3.11. Dudak Tanıma Sistemleri

Dudak baskısı, insan dudak geçişinde, iç labiyal mukoza ve dış cilt arasında bulunan kırışıklıklar ve yivler şeklindeki normal çizgiler ve çatlaklardır. Bu yapı herhangi bir anatomik isime sahip değildir. Dudak izlerinin görünümü parmak izi

gibi görünür ve kişiden kişiye değişir. Bir insan için ölüm öncesi kayıtları olarak yapılan ayrıntılı bir çalışma ile üst dudak ve alt dudağın farklı parçalarının kesin ve ayrıntılı bir tarifi oluşturulursa, bu kayıt, bilinmeyen bir merhumda kaydedilen dudak izlerinin ayrıntılarının eşleştirilmesi için kullanılabilir. Ölüm öncesi ve sonrası kayıtları dudak şekillerini karşılaştırırken, her iki dudak kayıtları eşleştirilirse, birey belirlenebilir. Dudak baskıda temel özellikler; insan dudaklarının kırmızı kısmındaki oluklar, dudak oyukları, labiyal kırışıklıklardır [17].

2.3.12.Tuş Vuruşu Dinamiği

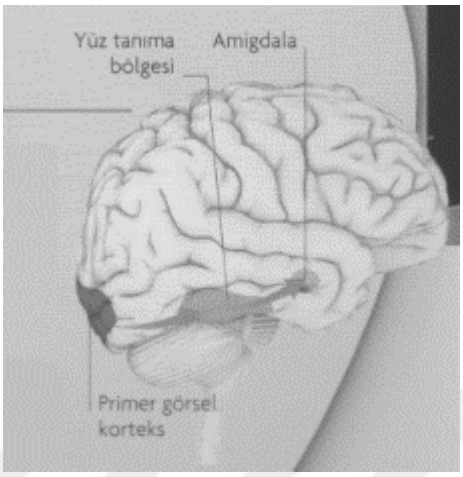
Tuş vuruş dinamiği, bir kişinin bir tuş takımındaki tuş vuruşlarını inceleyen otomatik bir yöntemdir. Teknoloji, bilgisayarlarla uyumlu bir klavye ile kullanılmaktadır. Bu teknoloji, hız belirli bir şifre ve bir kullanıcının belirli tuşlara basması arasında geçen süre ve basınç gibi dinamikleri analiz ederek, kimliği sürekli olarak doğrulama potansiyeline sahiptir [33].

2.3.13. Vücut Kokusu Tanıma

Vücut kokusu tanıma, insan vücudu kokusunun koku özelliklerini analiz ederek bir kişinin kimliğini teyit etmeye çalışan temassız bir fiziksel tanıma yöntemidir. Cambridge Üniversitesi'ne göre, geliştirilen sensörler vücuttaki kokuyu el gibi vücut parçalardan alabilirler. İnsan kokusunun her bir kimyasal maddesi biyometrik sistem tarafından çıkarılır ve benzersiz bir veri dizesine dönüştürülür [34].

3. YÜZ TANIMA SİSTEMLERİ

Beyinde, yüzlerin tanınması sırasında çeşitli görsel uyaranlar, çeşitli alanlarda işlenmektedir. İnsan yüzü özellikleriyle anlaşılan yüzler bu alanları aktif hale getirmektedir. Bu alanlar, ifadelerden bilgiyi çıkartır ve bu alanlara aktarır. Yüzün bir ifadeyle eşleştiği durumlarda ise, bu bilgi frontal loblara aktarılır [35].



Şekil 1. Tanıdık Bir Yüz Gördüğünde Beynin Etkilendiği Alanlar

Kaynak: Carter, R. (2014). The brain book. Dorling Kindersley Ltd. S.82

Yüz tanıma teknolojisi, yaygın olarak kullanılan bir biyometrik sistemdir. Genellikle bu sistemler, belirli özellikleri yüz görüntülerinden çıkarır ve daha sonra bu özellikleri kullanarak yüz eşleştirmeyi gerçekleştirir. Bir yüzün spesifik özellikleri gözler arasındaki mesafeyi, burun genişliğini, elmacık kemiklerinin pozisyonunu, çene çizgisini, çene ve benzeri faktörleri içerir. Bir yüzün, parmak izi ve göz iriliği kadar benzersiz olarak ölçülebilir özelliği yoktur. Yüz tanımanın güvenilirliği bu diğer biyometrik tanıma yöntemlerinden biraz daha düşüktür. Bununla birlikte, özellikle kullanıcı için kolaylığı göz önüne aldığımızda birçok uygulama için hala uygundur. Yüz tanıma, parmak izi tanıma gibi başka bir biyometrik yöntemlerle birlikte kullanılabilmektedir [36].

Yüz tanıma, insanların günlük yaşamlarında rutin ve zahmetsizce parçası olabilecekleri bir tanıma sistemidir. Güçlü ve düşük maliyetli bilgisayar ve bilgi işlem sistemlerinin yaygınlığı, biyometrik kimlik doğrulama, izleme, insan-bilgisayar etkileşimi ve multimedya yönetimi de dâhil olmak üzere bir dizi uygulamada dijital görüntü ve videoların otomatik olarak işlenmesine büyük bir ilgi yaratmıştır.

Otomatik yüz tanımada araştırma ve geliştirme doğal akış içerisinde gerçekleştirilir [37].

Yüz tanıma araştırması, yalnızca bu tanıma sorununun oluşturduğu temel zorluklarla değil, aynı zamanda insan tanımasına ihtiyaç duyulan sayısız pratik uygulamada da kullanılır. Birincil biyometrik teknolojilerden biri olan yüz tanıma, dijital kameralar, internet ve mobil cihazların maliyetinin azalması ve artan güvenlik talepleri gibi teknolojilerdeki hızlı ilerlemeler nedeniyle gittikçe önem kazanmıştır. Yüz tanıma, diğer biyometrik teknolojilere göre daha doğal bir şekilde edinilir ve kullanımı kolaydır [38].

Bir yüz tanıma sisteminin görüntü ve videolarda bulunan yüzleri otomatik olarak tespit etmesi beklenir. Yüz doğrulama (veya kimlik doğrulama) ve yüz tanımlama (veya tanıma) olmak üzere iki türden birinde veya her ikisinde de çalışabilir. Yüz doğrulama, sorgu yüz görüntüsünü, kimliği iddia edilen bir şablon yüz görüntüsüyle karşılaştıran bire bir eşleşmeyi yapan sistemdir. Bu bağlamda, yüz tanımlama, bir sorgu yüz imgesini, sorgu yüzünün kimliğini belirlemek için veri tabanındaki tüm şablon görüntüleriyle karşılaştıran çoklu eşleşmelerden oluşur [39].

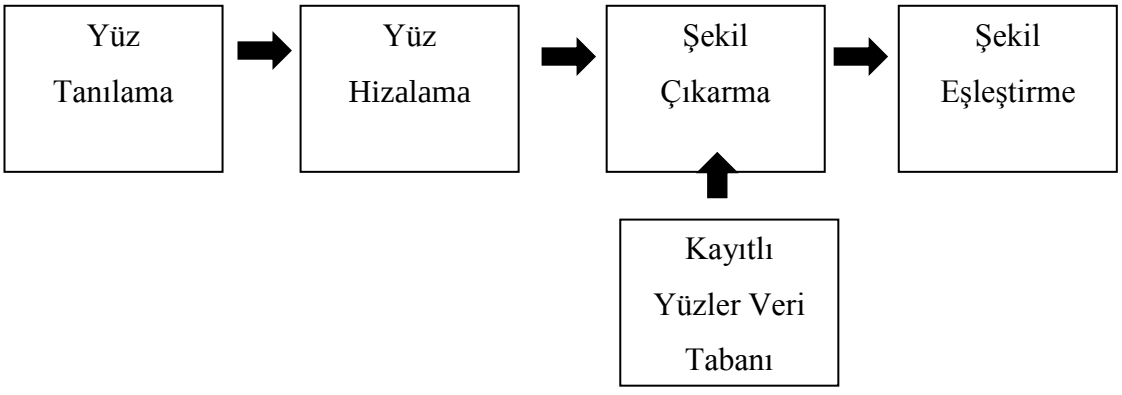
Çoklu biyometrik yaklaşım, tanımlama sistemleri için özellikle önemlidir. Genel olarak, bu tanımlama sistemleri, ek bir güvenlik bilgisi gerektirmeyen, kullanımı çok kolay sistemlerdir. Bununla birlikte, yalnızca bir biyometrik yöntemle kullanılması, yanlışlıklara neden olabilir. Yüz tanımlamasını ek biyometrik bir yöntem olarak kullanmak bu etkiyi önemli ölçüde azaltabilir. Bu çok biyometrik yaklaşım, belirli bir biyometrik özelliğin bazı kullanıcı grupları için optimal olmadığı durumlarda da yardımcı olur. Örneğin, elleri ile yoğun bir emek harcayan insanların kaba parmak izleri olabilir; bu, parmak izi tanımlaması tek başına kullanıldığında, yanlışlık oranını artırabilir [36].

Yüz tanıma, en uygun biyometrik sistemi seçmek ve geliştirmek için bir alternatif olabilmektedir. Avantajı, bir görüntü yakalama aygıtı (kamera) ile uygulanıp fiziksel temas gerektirmemesidir. Bir yüz tanımlama sistemi, mevcut görüntü yakalama cihazlarıyla (web kameraları, güvenlik kameraları, vb.) kullanılabilir olduğu için gelişmiş bir donanım gerektirmez. Yüz tanıma, biyometrik

veya multi-modal sistemlerin geliştirilmesinde ciddi bir alternatif olarak düşünülmektedir [14].

Yüz tanıma sistemlerinin nasıl gerçekleştiği ile ilgili bir akış sunmak gerekirse şunlardan bahsedilebilir: Yüz tanıma görsel desen tanıma problemidir. Değişen aydınlatma, poz, ifade ve benzeri tabi tutulan üç boyutlu bir nesne olarak bir yüz, onun iki boyutlu imgesine (üç boyutlu görüntüler, örneğin lazerden elde edilebilir) dayalı olarak tanımlanacaktır. Bir yüz tanıma sistemi genellikle dört modülden oluşur. Bunlar; tanıma, hizalama, özellik çıkarma ve eşlemedir.

Yüz tanıma fotoğrafla gerçekleşebileceği gibi video ile de gerçekleşebilir. Bu durumda, tespit edilen yüzlerin bir yüz izleme bileşenini kullanarak izlenmesi gerekebilir. Yüz hizalaması daha doğru lokalizasyona ulaşmayı ve yüzleri normalleştirmeyi amaçlamaktadır, oysa yüz algılama, saptanan yüzlerin her birinin konumunu ve ölçeğini kaba şekilde tahmin etmektedir. Gözler, burun ve ağız ve yüz hatları gibi yüz bileşenleri bulunur; konum noktalarına dayalı olarak girdi yüz görüntüsü, geometrik dönüşümler veya şekil değiştirme kullanılarak boyut ve poz gibi geometrik özelliklere göre normalize edilir. Yüz genellikle aydınlatma ve gri tonlama gibi fotometrik özelliklere göre de normalize edilmiştir. Bir yüz geometrik ve fotometrik olarak normalize edildikten sonra, farklı insanların yüzleri arasında ayrım yapmak için yararlı olan ve geometrik ve fotometrik varyasyonlara göre sabit olan etkili bilgi sağlamak için özellik çıkarma gerçekleştirilir. Yüz eşleştirmesi için girilen yüzün çıkarılan özellik vektörü, veri tabanındaki kayıtlı yüzlerinkilerle eşleştirilir; eşleşen uygun bir yüz bulunursa yüzün kimliğini çıkarır veya aksi halde yüz bilinmeyen olarak kalır [39]. Aşağıdaki şekilde, yüz tanıma sistemlerinin akışına yer verilmiştir.



Şekil 2. Yüz Tanıma Sistemlerinin Akışı

Kaynak: Jain, A. K., & Li, S. Z. (2011). Handbook of face recognition. New York: Springer. S.4.

Yüz tanıma sistemlerinin performansı, ilk otomatik yüz tanıma sistemi geliştirildiğinden beri önemli derecede gelişmiştir. Ayrıca, yüz tanıma yüz özelliği çıkarma ve tanınma, şimdi kısıtlı imkânlar altında çekilen görüntüler için "gerçek zamanlı" olarak da yapılabilmektedir.

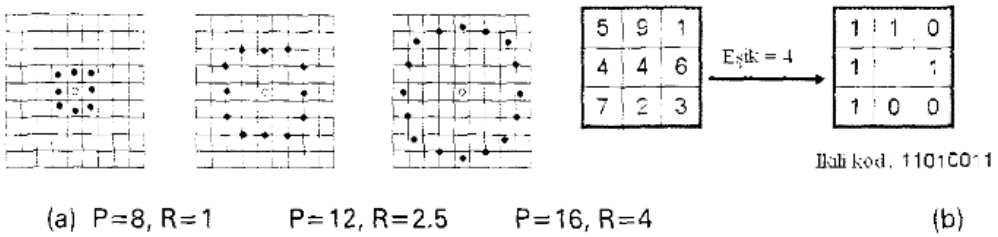
Yüz tanıma sistemlerinin çeşitleri bulunmaktadır. Nabiyev (2012) yüz tanıma sistemlerini bazı alt başlıklarda incelemiştir. Bunlardan ilki ten bulmadır. Bu bağlamda, ten bulma işlemi, RGB bileşenleri gibi aydınlatma koşullarının yetersiz olduğu durumlarda, HSV, YIQ ve YCbCr renk uzayında parlaklık bilgisi üzerinden işlem gerçekleştirebilmektedir. Bu bağlamda, RGB bileşenleri, YCbCr'ye çevrilebilir. Bu işlem ise şu şekilde gerçekleştirilebilmektedir [40]:

$$Y = 0{,}299R + 0{,}587G + 0{,}114B$$
$$Cb = -0{,}169R - 0{,}332G + 0{,}500B$$
$$Cr = 0{,}500R - 0{,}419G - 0{,}081B$$

Şekil 3. RGB Bileşenlerinin YCbCr'ye Çevrilmesi

Kaynak: Nabiyev, V. V. (2012). Yapay zeka: insan-bilgisayar etkileşimi. Seçkin Yayıncılık. S.746

Yüz tanıma ile ilgili bir başka alt başlık ise, yüz ifadelerinin değerlendirilmesidir. Bu ise, yüzün özellik vektörünün çıkartılmasıyla mümkün olmaktadır. Özellik çıkarma işlemi ise, Yerel İkili Örnekler ile gerçekleştirilebilmektedir. Bu örnekler operatörü görüntüdeki her piksele karşılık yerel komşuları merkez piksele göre eşiklendirerek bir ikili kod oluşturur. Yerel ikili örneklerin üç farklı dairesel komşuluklar kümesi bulunmaktadır. P komşu sayısını, R örnekleme yarıçapını ifade etmektedir [40].



Şekil 4. Yerel İkili Örnekler Kodunun Üretilmesi

Kaynak: Nabiyev, V. V. (2012). Yapay zeka: insan-bilgisayar etkileşimi. Seçkin Yayıncılık. S.747.

Örnek tanıma ise, resmin Yerel ikili örnek histogramına uzaklığının ölçülmesi olarak tanımlanırken bunun için Chi karesi istatistiği kullanılabilmektedir. Bir diğer teknik ise morfleme tekniği olup, iki farklı resimden bir resim elde etme sistemidir etmektedir [40].

4. HASTANE SİSTEMLERİNDE TEKNOLOJİNİN KULLANIMI

4.1. Hastane Kavramı

Bir hastane, uzman personel ve teçhizat ile hasta muayenesi sağlayan sağlık hizmetleri kurumudur. Genellikle, hastaneler kamu sektörü, sağlık kuruluşları (kâr amacı veya kar amacı gütmeyen kuruluşlar), sağlık sigortası şirketleri veya doğrudan bağış yoluyla sağlanan fonlar da dâhil olmak üzere hayır kurumları tarafından finanse edilebileceği gibi özel de olabilmektedir [41].

4.1.1 Hastanelerin Sınıflandırılması

Hastaneler mülkiyet, hizmetin kapsamı ve akademik bağlılıklarıyla hastanelerde eğitim veriyor olmaları bakımından ayırt edilirler. Hastaneler ya şirketler ya da doktorlar gibi bireylerin sahip olduğu ya da kar amacı gütmeyen kuruluşların mülkiyetinde olan ya da kamu yönetimi tarafından işletilen işletmeler haline getirilebilir Bu bölümde, uluslararası normlarda hastane sınıflandırılmasından bahsedilecektir [42].

4.1.1.1 Yerel Hastaneler

Yerel hastanelerinin çoğu acil servislerin yanı sıra bir dizi yatarak tedavi ve ayakta tedavi tıbbi ve cerrahi hizmetleri de sunmaktadır. Çoğu kişinin bakım gördüğü yerel hastaneler genellikle küçüktür ve elli ila beş yüz yataklıdır. Bu hastaneler normalde rutin tıbbi ve cerrahi sorunlar için kaliteli bakım sağlarlar. Bu hastaneler, giderek daha rekabetçi bir sektörde varlıklarını sürdürmek için ek mali kaynaklara ihtiyaç duyarlar [43].

4.1.1.2 Eğitim Hastaneleri

Eğitim hastaneleri, tıp fakülteleri, hemşirelik okulları veya müttefik sağlık meslekleri eğitim programlarına bağlı olan hastanelerdir. Eğitim hastaneleri, hekimlerin gözetiminde stajyerlerin çalıştığı ve ya yeni hekimleri eğitmek için oluşturulmuştur. Eğitim hastanesi olmayan hastaneler de tıp fakülteleri ile olan bağlarını sürdürebilir ve bazıları aynı zamanda hemşirelik ve müttefik sağlık meslek öğrencilerine hizmet edebilir. Tıp öğrencileri ve diğer sağlık profesyonelleri için klinik eğitim veren çoğu eğitim hastanesi, bir tıp fakültesine bağlı olup, birkaç yüz yatak ihtiva edebilmektedir [42].

Üniversiteye bağlı bir eğitim hastanesinde bakım almanın bir avantajı, son derece gelişmiş hekimlere, en gelişmiş teknoloji ve ekipmana erişim olanağı sağlaması olup, dezavantajı, öğrencilerin yaptığı çok sayıda muayene sonucunda ortaya çıkabilecek mahremiyet eksikliğidir. Bununla birlikte, bu hastanelerde, karmaşık, olağandışı veya zor tanı konulan hastalar, kabul edilen tıp uzmanlarının varlığından ve bu tesislerde daha kapsamlı kaynaklardan yararlanmaktadır. Bir eğitim hastanesi, tıp öğrencilerine ve hemşirelere öğrenim imkânı sağlarken çoğunlukla bir tıp fakültesine, hemşirelik okuluna veya üniversiteye bağlıdır [44].

4.1.1.3 Kamu Hastaneleri

Devlet hastaneleri, devlet tarafından işletilmektedir. Genellikle hastalarının çoğu hizmet için ödeme yapamazlar ve ya hizmet bedelinin belirli bir kısmını öderler [45].

4.1.1.4 Genel Hastaneler

Bu hastane türü en kapsamlı hastane türüdür ve birçok hastalık ve yaralanma ile başa çıkmak adına entegre bir hizmet sunması bakımından önemlidir. Hem yatarak ve ayakta tedavilerde hem de acil tehditlerle başa çıkmak için bütünleşik bir tesis görevi görmektedir [42].

4.1.1.5 Bölge Hastaneleri

Bu hastaneler, bölgedeki ana sağlık kuruluşudur ve yoğun bakım ve uzun süreli bakım için çok sayıda yatak bulunmaktadır. Cerrahi, plastik cerrahi, doğum ve laboratuvarlar bulunmaktadır [46].

4.1.1.6 Özelleşmiş Hastaneler

Travma merkezleri, rehabilitasyon hastaneleri, çocuk hastaneleri, yaşlı hastaneleri ve psikiyatrik sorunlar gibi belirli tıbbi gereksinimleri karşılamak adına özel durumlar için kurulan hastane türüdür. Bakım ünitesi, nöroloji, kanser merkezi ve doğum ve jinekoloji, onkoloji veya ortopedik hastaneler bu kategoriye girmektedir [47].

4.1.1.7 Klinikler

Hastaneden küçük tıbbi tesisler genellikle klinik olarak adlandırılır ve sağlık hizmetleri veya özel hekimlerin özel bir ortaklığı ile oluşturulur. Klinikler genelde ayakta tedavi hizmetleri sunmaktadır [42].

4.1.2 Hastanelerin Genel İş Akışı

Bazı hastalar sadece teşhis, tedavi veya terapi için hastaneye gider ve ayakta tedavi edilir. Diğer hastalar, yatılı olarak birkaç gün, haftalar veya aylarca kalabilirler. Hastaneler, yatılı hastaları kabul etme ve bakma kabiliyeti ile genellikle diğer tıbbi tesis türlerinden ayırt edilirken, diğerleri genellikle klinik olarak tanımlanmaktadır. Bir hasta hastaneye girdiğinde aşağıdaki işlem sırası uygulanır. Her şeyden önce hasta kaydı gerçekleştirir ve hasta muayene için hemşireye yönlendirir. Burada hemşire yaşamsal göstergeleri kontrol eder ve daha sonra hemşireler tanı için hastanın klasörünü oluşturur. Tanı doktor tarafından konduktan sonra hasta test için laboratuvara gönderilir ve ya ilaç tedavisi uygulanır [48].

Tanı konduktan sonra hasta başka bir kliniğe sevk edilebilir veya aynı hastanede tedavi görebilir. Örneğin, radyoloji hizmetleri, cerrahi hizmetler ya da diş bakımı gibi özel hizmetler için sevk edilebilir. Yatan hasta tamamen iyileşebilir ve taburcu edilir veya ölüm gerçekleşirse ölüm raporu verilir. Hastane yönetim sisteminin amacı, sistemde saklama ve kolay veri alımı, bilgi akışı ve hastane yönetimi için otomatik hale getirmektir [42].

4.1.3 Hastane Etkinliklerinin Genel Çerçevesi

Hastane, hastaların tıbbi kontrol, teşhis ve tedavi için ziyaret ettiği bir yerdir. Hastanelerin sağladığı olanaklar şu şekilde sıralanabilir [49]. Doktorlar tarafından hastalıkların konsültasyonu ve teşhisi,

- Tedavi hizmetlerinin sağlanması,
- Hastalara yataklar, bakım ve ilaçlar gibi hizmetleri sağlama olanağı
- Aşı uygulamaları

Ayrıca, bir hastanede çeşitli operasyonel çalışmalar yapılmaktadır. Bunlar operasyon personeli ve doktorlar tarafından bir hastanede yapılan çeşitli işlerdir. Bu çalışmalar aşağıdaki şekilde özetlenebilmektedir:

- Tedavi için hastaneye gelen hastalar hakkında bilgi kaydı,
- Faturalama: hastaya verilen her bir hizmet için kayıt fiyatı ile oluşturulur ve en sonunda hepsi toplanır.
- Hastalara verilen tanı ile ilgili kayıtlama: hasta tanı bilgileri, genel olarak, hasta bilgilerinin bulunduğu belgede kaydedilir. Bir süre sonra ofisteki kağıt yükünü azaltmak için yok edilir.
- Aşı kaydını tutmak: bu kayıtlar önceden formatlanmış, bir dosyada saklanır.
- Hastaları tedavi etmek için mevcut olan çeşitli hastalık ve ilaçlarla ilgili bilgi toplama.

Tüm bu çalışmalar, manuel olarak yapıldığında, doktorlar ve elbette resepsiyonist ve diğer operasyonel personel tarafından ele alınması için çok sayıda kağıt gerekmektedir.

4.1.4 Manuel Sistemlerin Otomasyon Sistemleriyle Karşılaştırılması

Hastane yönetimi, güçlü bir yönetim sistemi mevcut değilse, oldukça zor olan çok sayıda karar aşamaları içermektedir. Her aşamada hassas ve doğru bir şekilde uygulanan sistemlere ihtiyaç duyulduğundan, hastanedeki otomasyon sistemleri yeterli olmalıdır. Güvenilir, düşük maliyetli ve verimli bir sistem bir hastanenin başarısının belkemiğini oluşturur. Bunun sebebi ise manuel sistemlerin bazı problemler teşkil etmesi ve otomasyon sistemlerinin bu problemlerin üstesinden gelmesidir Bu bağlamda birkaç karşılaştırmadan bahsedilebilir [50].

Hastane bilgi sistemlerinin yönetimi, hizmet kalitesi anlamında oldukça önemlidir. Manuel sistemlerde veriler, otomatik bir sistem olduğu kadar güvenilir olmamaktadır. Bunun sebebi ise bu sistemlerdeki hata eğilimidir. Elle girilen veriler, kişilerin hatalarına oldukça açık olmakta ve tekrar başvurulması gerektiğinde hazır bulunmamaktadır. Bu kritik kalite göstergelerinden biridir. Hasta bilgileri ve tıbbi

raporları elektronik olarak gönderebilen ve alan bir hastane her zaman diğerlerine göre daha güvenilir olacaktır.

Otomatik bir yönetim sistemi kurmak, hata şansını tamamen ortadan kaldırır ve tıbbi merkezler ve hastaneler için en büyük iki zorluk olan uyumluluk sorunları ve davalardan kaçınılmış olur. Buna ek olarak, oda doluluk, personelin hazır bulunması ve operasyonel bilgileri hakkında dakikalık detaylı bir izlemeler hızlı bir şekilde gerçekleştirilir.

İş gereksinimlerine göre uyarlanmış otomatik hastane yönetim sistemi, gelir yönetimi için gereken iş gücünü oldukça azaltan bir unsur olarak karşımıza çıkmaktadır. Manuel sistemler, hızlı ve doğru işlem ve yönetim raporları sunmakta zorlanmaktadır.

Manuel sistemlerin tercih edilmesinin en önemli yanı, veri hırsızlığına konu olma ihtimalinin olmasıdır. Tam teşekküllü bir hastane yönetim sistemi, bilginin her bir parçasını yetkisiz erişime karşı korur. Bununla birlikte, en son teknoloji ürünü bir sistem uygulamaması da aynı derecede önemlidir. Bilginin erişilebilirliğinin kullanıcı haklarına bağlı olduğu erişimli bir sistem tarafından ele alındığında hata olasılığı yoktur.

4.1.5. Hastane Otomasyon Sistemlerine Duyulan İhtiyaç

Hastane Otomasyon sistemlerine duyulan gereksinim şu şekilde özetlenebilir [42]:

- *İşe Planlı Yaklaşım:* Organizasyon sistemleri sayesinde hastanelerdeki faaliyetler iyi planlanacak ve organize edilecektir. Veriler, veri alışveriş merkezlerine düzgün bir şekilde depolanacak ve bu, bilgilerin alınmasına ve güvenliğin arttırılmasına yardımcı olacaktır.
- *Doğruluk:* Otomasyon sistemleri, kuruluşta gerçekleşen etkinliklerin doğruluk seviyesini arttıran bir unsur olarak karşımıza çıkmaktadır. Tüm işlemler doğru yapılsa da, uygulamada hatalar tamamen ortadan kaldırılmaz, ancak azaltılır.
- *Güvenilirlik:* Bilgiler düzgün ve güvenli bir şekilde saklandığından sistemin güvenilirliği yüksek olacaktır.

- *Fazlalığın Olmaması:* Önerilen sistemde herhangi bir bilginin depolamada herhangi bir yerde tekrarlanmamasını sağlamak için azami özen gösterilen bu sistemlerde, bu şekilde, depolama alanının ekonomik olarak kullanılmasını ve saklanan verilerin tutarlı olmasını sağlar.
- Hızlı bilgi edinme: Otomasyon sistemlerinin asıl amacı, bilgilerin hızlı ve verimli bir şekilde alınmasını sağlamaktır. Kullanıcıların her istediğinde her tür bilgi kullanılabilir olacaktır.
- *Bilginin Derhal Depolanması:* Manuel sistemde, çok miktarda bilgiyi depolamaya çalışırken bir sürü problemle karşılaşılır.
- *Kolay Çalışır Olma:* Sistemin kullanımı kolay olmalı ve kısa sürede geliştirilebilecek ve kullanıcının sınırlı bütçesine uyacak şekilde olmalıdır.

4.1. Hastane Bilgi Sistemleri

Sağlık, birçok kilit unsuru olan ve bu unsurların etkileşim halinde olduğu karmaşık ve dinamik bir çerçevedir. Sağlığın diğer sektörlerden en önemli farkı, ağırlıklı olarak kamusal olması ve yaşamsal bir işlevi olmasıdır. Bu karmaşık ortamda, sağlık sektöründe bilgilerin yönetimi etkili bir yönetim için esastır.

Sağlıkta bilgi sistemlerinin kullanılması, elektronik sağlık bilgi sistemleri vasıtasıyla bu artan bilgi talebinin bir cevabı olabilir. Literatürde, hastane bakım servislerinde bilgi akışını ve depolanmasını yöneten benzer yaklaşımları tanımlayan çeşitli terminolojiler bulunmaktadır. Bunlar; Hastane Bilgi Sistemi, Sağlık Bilgi Sistemi, Klinik Bilgi Sistemi, Hasta Veri Yönetim Sistemi veya Elektronik Sağlık Kaydı olabilmektedir. Hastane Bilgi Sistemi, veri toplama, depolama ve taşıma gibi görevleri olan sistemlerdir. Bu sistemler, manuel olabileceği gibi elektronik de olabilir ve ya her ikisinin birleşimi şeklinde de gerçekleşebilir. Hastane Bilgi Sistemleri, hem idari hem de klinik işlevleri üstlenir [51].

Hastane Bilgi Sistemleri hastane operasyonlarını yönetmek için kullanılan bilgi teknolojileridir. Bunlara örnek olarak örneğin hasta finansal kayıtları, kayıt, zaman çizelgesi, genel finansal sistemler, operasyon sistemleri ve sipariş iletişimleri olarak tanımlanmaktadır. Hastane Bilgi Sistemleri temelde bir hastanedeki sağlık çalışanlarının işlerini etkili bir şekilde yerine getirebilmeleri için tüm bilgileri

yönetebilen, bir hastanedeki çeşitli sağlık faaliyetlerini stratejik, taktiksel ve operasyonel düzeyde destekleyen bir bilgisayar sistemidir [52].

Hastane Bilgi Sistemleri, ilk defa 1960'lı yıllarda kullanılmış olup, personel tarafından öncelikle fatura ve hastane envanteri yönetimi için kullanıldı. Günümüzde, gelişmiş altyapı ve daha hızlı bilgisayar sistemleri sayesinde, sağlık ve hastanelerde gerçek zamanlı elektronik tıbbi kayıtlara erişim, eğitim veya araştırma için bilgi sistemleri kullanılmaktadır [51].

Birçok hastane organizasyonu içinde Hastane Bilgi Sistemleri, tek bir kesintisiz entegre sistem değil, zaman içinde gelişen birçok farklı bölüm ve uzmanlık için birçok uygulamadan oluşan bir karışım olarak görülmektedir. Hastaneler, esnekliği ve etkinliği birleştiren çok disiplinli klinik süreçleri olup tüm hastaneye yayılması verimini arttırıcı bir unsur olarak karşımıza çıkmaktadır. Bununla birlikte, giderek artan karmaşık hastane sistemleri, hasta merkezli yaklaşım ve hastalardan gelen talebin artması nedeniyle entegre bir sistem daha fazla fayda sağlamaktadır [53].

Bir hastanede karmaşık idari ve klinik süreçleri yönetmek, personelin hastanede hastalara bakma konusunda daha fazla zaman ayırmasını sağlamak ve hastanede yatan hastadan uzun süreli bakıma ve evde bakım hizmetlerine kadar uzanan hizmetlerin gerçekleştirilmesi hastane bilgi sistemleri sayesinde olmaktadır. Kritik görevlerin ve iş akışının bilgi ve otomasyona erişimi, yalnızca bu görevi yerine getirmekle kalmayıp verimli bir şekilde çalışmanın anahtarıdır. Hastane bilgi sistemlerinin işlevleri aşağıda verilmiştir. Bu işlevler, aşağıda sıralanmış olup şu şekildedir [54].

- Hastane tesislerinin etkin kullanımı ve envanter kontrolünün iyileştirilmesi,
- Toplanan verileri araştırma amaçlı olarak hazır hale getirilmesi,
- Yönetimin politika kararları vermesine yardımcı olan raporların üretilmesi,

- Hasta bakımını desteklemek için gerekli bilgilerin hastane yönetimine ve ya ilgili personele aktarılması,
- Kanuni gereklilikler için gerekli kayıtların arşivlenmesi, korunması ve gerektiğinde personel tarafından ilgililerle paylaşılması,
- Veri güvenliği, bütünlüğü ve erişilebilirliği,
- Kritik kamu sağlığına ilişkin verilerin etkin bir şekilde takip edilmesi ve analiz edilmesidir.

4.2. Hastane Bilgi ve Otomasyon Sistemleri İlişkisi

Bir sonraki bölümde bahsedileceği üzere otomasyon, bilgi sistemleriyle bütünleşik halde uygulanan bütün araçların, karşılıklı bağıntılı ve güvenilir bir şekilde kullanılmasıdır. Hastane otomasyon sistemleri ise, hastane bilgi yönetim sistemi şeklinde yürütülerek, hastaların, medikal, özlük ve mali bilgilerinin kayıt ve tanıma yönetimidir. Bilgi sistemleri, bahsedilen tüm araçların, bilgilerinin kaydedilmesi ve depolanması, korunması ve de ihtiyaç halinde ortaya çıkarılmasından sorumludur. Bilgi sistemler, verimliliği artıran bir unsur olarak karşımıza çıkarken, özellikle hastanelerde, kayıtlama sisteminin önemi düşünüldüğünde, geçmiş verilere ulaşımı kolaylaştırarak ve kontrolünü sağlayarak hem hizmet hızına da olumlu yönde etki etmiş olur [55].

4.3. Hastane Otomasyon Sistemleri

Otomasyon, malların ve hizmetlerin üretiminde insan çalışmalarına olan ihtiyacı azaltmak için kontrol sistemleri ve bilgi teknolojilerinin kullanılması olarak tanımlanır. Artık otomasyon, ATM'ler, cep telefonuyla kontrol edilen akıllı sistemler, araçlarda otomatik park yardımı gibi teknolojilerle günlük hayatta var olan bir sistem haline gelmiştir. Bankacılık, perakende ve diğer endüstrilerde yıllardır kullanılmasına rağmen, sağlık hizmetleri otomasyon kullanımında geride kalmıştır. Sağlık reformundan ve artan rekabetten kaynaklanan ve piyasa tarafından oluşturulan baskı, maliyetleri düşürmek ve sağlık hizmeti sunumunda israfı ortadan kaldırmak adına otomasyonu bu sektörde de önemli hale getirmiştir. Yaşlanma sürecindeki bir nüfus ile birlikte sağlık sisteminde daha fazla kişi daha fazla bakıma ihtiyaç duyması sağlık alanında kadrolaşma düzeylerini yetersiz bırakan bir durum olarak karşımıza

çıkmaktadır. Bu durum bu sektörde otomasyon sistemlerini önemli hale getirmektedir [56].

Otomasyon sağlık sektörüne ilk entegre edildiğinde bu eczane kolundan yapılmıştır. Robotik makinelerden ilaç alımını sağlayan bu sistem elbette gerçek eczanenin önüne geçememiş hasta bu alışverişi bilirkişiyle yapmak istemiştir. Aynı mantık doktorlar için söz konusu olduğunda da geçerli olacaktır. Bununla birlikte, otomasyon, bakım dağıtım süreçlerinin geniş bir bölümünü çok daha verimli hale getirmek ve verimliliği artırmak için iş akışlarına harmanlanabilir. Örneğin hasta hatırlatıcılardan tedavi sırasında büyük bir destek alabilir [57].

Hastanelerde otomasyon sistemleri, sağlık profesyonelleri için verimli bir çalışma ortamı sağlama amacıyla oluşturulmuştur. Doğru sağlık verilerine hızlı bir şekilde erişmek bu sistemin temel işlevlerinden biridir. Hastalarla ilgili bilgiler, hastadan, test sonuçlarından, doktor teşhislerinden, sağlık ölçüm cihazlarından ve daha önce depolanmış hasta bilgilerinden olmak üzere birçok kaynaktan elde edilebilir. İlgili verilerin elde edilmesinin en olağan yolu, kağıt üstünde kaydı alınmış verilerin toplanmasıdır. Kâğıt temelli kayıtların maliyeti düşüktür ve erişilmesi zor, güncellenmesi çok zaman alıcı olduğundan bazı sınırlamalara sahiptir. Akıllı depolama mekanizması kullanarak hastane otomasyon sistemlerinin kapsamı genişletilip sorunlar çözülebilir [58].

Hastanelerde bu sistemlerin kullanılmasının pek çok faydası bulunmaktadır. Hastanelerde otomasyon sistemlerinin kullanılmasının faydaları şu şekilde özetlenebilmektedir [56].

Tablo 2. Hastanelerde Otomasyon Sistemlerinin Kullanılmasının Faydaları

1. İşgücü Tasarrufları	Makine tarafından daha iyi yapılması gereken yoğun görevleri yerine getirmek için otomasyonu kullanmak büyük bir zaman kazandırabilir. Bu durum, çalışanları elimine etmekten ziyade eğitim gördükleri klinik tecrübelerden faydalanan daha işlevli rollerde bulunmalarını sağlaması açısından önemlidir.
2. Geliştirilmiş Kalite ve Tutarlılık	Otomasyon araçları insan hatasına veya yorgunluğa maruz kalmaz, bu nedenle bakım faaliyetlerinin tutarlı bir temelini sağlamaya yardımcı olabilirler.
3. Azaltılmış Atık	Fazla bir iş yükü için gerekli kâğıt ve elektronik tabloların ve diğer geçici çözümlerin kullanılması çok miktarda israfa neden olabilir.
4. Çıktıların Artan Tahmin Edilebilirliği	Hastalar, otomasyon tarafından desteklenen standart bir bakım yolunu izlediklerinde, tahmin edilen sonuçlara doğru yolda kalacakları daha muhtemeldir. Buna ek olarak, otomasyon, bir hastanın önerilen bakım planından ne zaman ayrıldığını tespit etmenize yardımcı olabilir; böylece bakım ekibi müdahale edebilir.
5. Daha Yüksek Üretim	Otomasyon araçları tarafından desteklenen bir hemşire, aynı anda daha geniş bir hasta popülasyonunu idare edebilir. Hasta potansiyelinin hacmi büyüdükçe ve küçüldükçe personel sayısını arttırmak yerine, otomatikleştirilmiş bir platform her ölçekteki adres grubuna esnek bir şekilde ölçeklendirebilir.
6. Verilere Dayalı Analizler	Süreçleri otomatik hale getirmek için kullanılan teknoloji, performans iyileştirmesi ve optimizasyonu için kullanılabilen sürekli bir geri besleme döngüsünde zengin bir veri sunabilir. Her çevrimde, otomasyon sistemleri, işlemin nasıl yürüdüğü konusunda veri toplayabilir ve programı iyileştirmek için bu bilgiyi kullanabilir. Böylece zamanla kendini geliştirir ve takımın iş yükü için daha verimli, daha doğru ve daha yararlı olur.

Kaynak: Çevrimiçi, http://hitconsultant.net/2014/07/21/6-big-benefits-of-applying-automation-to-healthcare/

Yeni ve pahalı teknolojiler ve her zamankinden daha uzun yaşayan bir nüfusla birlikte artmasıyla hastaneler ve diğer sağlık tesisleri, rekabet edebilmek ve maliyetleri artırmak için artan baskılarla karşı karşıyadır. Bu baskılar onları, hasta sistemlerinde teknolojiyi kullanmaya itmekte ve bu şekilde verimliliği arttırarak maliyeti düşürmeyi amaçlamaktadırlar. Bu açıdan bakıldığında, hastane otomasyon sistemlerinde, özellikle, kayıtlama ve tanımlama alanlarında, daha ileri düzeyde ise, çeşitli hayati fonksiyonları kontrol etme şeklinde ortaya çıkabilecek biyometrik uygulamalara sıkça rastlanabilecektir.

Bilgisayarın kullanıldığı, hastane bilgi sistemleri, idari ve finansal sistemler; klinik bilgi sistemleri ve stratejik karar sistemleri olmak üzere üçe ayrılmaktadır. Bu bağlamda idari ve finansal sistemler; elektronik talepler, hasta hesap sistemleri, malzeme ve ofis yönetimi, insan kaynakları gibi özellikleri barındırırken; kinik bilgi sistemleri, bilgisayarlı hasta kaydı, laboratuvar ve ilaç kayıtları, hemşire ve diğer yarımcı bilgi sistemleri ve klinik karar sitemlerinden oluşmaktadır. Stratejik karar sistemleri ise, pazarlama, market planlaması, kaynakların kullanımı ve performans ve çıktıların değerlendirilmesinden oluşmaktadır [59].

Bu bağlamda; Esatoğlu ve Köksal (2002)'ın yaptığı çalışmaya göre, hastaneler bilgisayarlı bu sistemleri birincil olarak muhasebe işlemlerinde fatura kaydı için kullanmaktadır. Bu oran %93.5'tur. İkincil olarak kullanım amacı hasta kayıt olup, %87.1 oranında kullanılırken, ilaç sistemlerinde %92.6, laboratuvarda ise %72 oranında kullanılmaktadır [60].

Bahsedildiği üzere hastane otomasyon sistemleri, hastanenin güvenlik önlemleri, sağlık hizmetleri ve ya muhasebe işlemleri için kullanılabilmekte olduğu gibi, hasta kayıt sistemlerinde de kullanılmaktadır. Bu şekilde bahsedilen amaçlara da hizmet eden bu sistemler, kayıt sistemlerinde fark yaratabilecek bir teknoloji olarak karşımıza çıkmaktadır.

4.4. Hasta Kayıt Sistemleri

Nüfusun giderek arttığı güncel dünyada, özellikle sağlık hizmetleri düşünüldüğünde, kayıt konusu oldukça önemli bir husustur. Bu bağlamda, hastaların, o hastanede ya da herhangi bir başka sağlık kurumunda kaydının olup olmadığının ilk etapta anlaşılması, var ise yapılan tedaviler ve ya teşhislere ulaşılması, geçirilen cerrahi operasyonların bilinmesi oldukça hayatidir.

Sağlık hizmetlerinin hemen hemen her bölümünde, gereksinim duyulan bilgiler, çeşitli şekillerde geçmişten bugüne kayıt altında tutulmaya çalışmıştır. Bu bağlamda her sağlık kuruluşunun kendi ihtiyacına göre bir kayıt sisteminin bulunduğundan bahsedilebilmektedir [61]. Hasta kayıtlarının en önemli özelliği, doktorlarla ve diğer sağlık görevlileriyle hasta arasında bir iletişimin sağlanmasıdır. Bu bağlamda hayati önem taşıyan bu sistemin, bilgisayarlı sistemlerle birleştirilip veriminin arttırılması oldukça önemlidir.

Bütün hasta bilgilerinin eş zamanlı kaydedilmesine ve bu bilgilerle tedavi planı gerçekleştirilmesine imkân sağlayabilecek bilgisayarlı sistemlerle donatılmış hasta kayıt sistemlerinin verimli kullanımı, gerçekleştirilen hasta tedavisinin devamının gelmesinde ve iyileştirilmesinde önemli bir unsur olarak karşımıza çıkmaktadır.

Bilgisayar sistemlerinin kurulu olduğu, hastanelerde, bu sistemler, klinik kararlar alınırken gerekli olan veriyi sağlarken, mali düzenlemeler ve birincil kurum gereksinimlerinin ortaya çıkarılması, kaynakların verimli kullanılması, kurum stratejisi ve organizasyonun değişim gereksinimleri gibi amaçlarla da kullanılabilmektedir. Bu sistemler, manuel sistemlerden, bahsedildiği üzere, hasta kaydı konusunda da oldukça üstün gelmektedir. Bu bağlamda, bu avantajların sıralanması gerekirse, bilgisayar sistemlerinin kullanıldığı otomasyon sistemlerindeki hasta verileri, ulaşımı kolay ve zamanında kullanılabilir bilgileri ihtiva etmekte olup, manuel hasta kayıtlarında ise bilgi kaybı ve hata imkânı oldukça fazladır [62].

Hasta kayıt sistemleriyle amaçlanan hastane personelleri arasındaki iletişimi verimli hale getirmek, araştırmalar için istatistiksel bilgi akışını oluşturmak, hastada gerçekleştirilen bakım ve tedavinin belgelenmesini sağlamaktadır. Bu şekilde

oluşturulan hasta kayıtları aranılan bilginin kolayca bulunması açısından kritikken, dosyaların arşivlenmesi, yeni kayıtların açılabilmesi açısından da işgücü ve kaynak verimi sağlar. Sağlık alanında kullanılan bilgi sistemleri hasta verilerinin kolayca anlaşılır, zamandan tasarruf eden ve farklılıkların anlaşılmasına elverişli bir kayıt sistemi olması bakımından kritiktir.

Ay (2009) global dünyada kullanılan bilgisayarlı hasta kayıt sistemlerini özetlemiştir. Bu bağlamda; ilk olarak, yaygın olarak kullanılan Problem Merkezli Tıbbi Kayıt (POMR) sisteminden bahsedilebilir. Bu sistem; hasta problemlerinin bir listesini ve bu problemlere dair çözümleri içermektedir. Problem Merkezli Tıbbi Kayıt Sistemi hastane personellerinin tüm kayıtlarını birleştirerek ve problemleri tanımlayarak entegre bir sistem oluşturulmasını sağlar [62].

Problem Merkezli Tıbbi Bilgi Sistemi (PROMIS) ise; tıbbi sürece fayda sağlamak adına hastane personeli tarafından kullanılan geniş bir sistem olarak tedavi ve bakım süreçlerini içerir. Bilgisayar Destekli Hasta Bakım Kayıtları (CPCR) ise, hastaların klinik problemlerinin kapsamını içermektedir. Bu sistem, hastaların sağlık durumlarının sistematik olarak kayıt edilmesini ve ölçülmesi konusunda fayda sağlar. Telefon ile Verilen Sağlık Hizmeti (Telehealth) ise; hastane personeli ile hasta arasında, interaktif bir şekilde gerçekleştirilen sağlık hizmetidir.

5. HASTANE SİSTEMLERİNDE YÜZ TANIMA

5.1. Hastane Sistemlerinde Biyometri

2000'li yılların başında, sağlık hizmetlerinin biyometri sistemi bir hasta tanımlama sistemi olarak kullanabileceğini düşünmek imkânsız görünüyordu. O zamana kadar, biyometri, sadece ticari pazarla ilişkilendirilen bir sistem olmakla birlikte, devlet güvenlik sistemlerinde de kullanılmaktaydı. Ancak; hastaneler tüm dünyada hasta tanımlama için biyometri yöntemlerini kullanmaya başladıktan sonra bu sistemlerin amacı [63];

- Hasta güvenliği standart düzeylerini yükseltmek;
- Hastane sorumluluğunu azaltmak;
- Bilinçsiz hastaların kimliğini doğrulamak;
- Yabancı dilin bir engel oluşturmasını ortadan kaldırmak;
- Tıbbi kimlik hırsızlığını önlemek olarak sıralanmıştır.

Bununla birlikte, bu avantaj listesinden belirgin bir şekilde eksik olan biyometrinin, hasta kayıtlarında yinelenen tıbbi kayıtların engellenmesi için en önemli yöntemlerinden biri olduğuna dikkat etmek önemlidir. Sağlık sektöründe, yinelenen tıbbi kayıtların hem parayla hem de kaynaklarda bir drenaj olduğu çokça bilinmektedir. Biyometrik bir hasta tanımlama çözümü, yalnızca yeni çoğaltılmış tıbbi kayıtların oluşturulmasını engelleyebilir, ancak bu, ancak bire çok kimliklendirmeye (1: N) dayalı bir sistemde mümkündür.

Biyometride, bir kişiyi tanımak için üç farklı yol vardır. Bunlar: doğrulama (bire bir veya 1: 1), bölümlü tanımlama (bire az veya 1:F) ve kimlik belirleme (bire-çok veya 1: N)'dır. Bire Bir (1: 1) Doğrulama: Bu kimlik doğrulama yöntemi, biyometrik tarama kullanılarak kişinin hak talep ettiği kimliğini onaylar veya reddeder ve normalde bir kimlik belgesinin fiziksel sunumunu gerektirir. Sağlanan kimlik belgesi, bir önceki kayıttan kendisine bağlı olan ve saklanan biyometrik şablonun yerini belirtir. Kimlik bilgileri sağlandıktan sonra kişi biyometrik taraması yapar ve yakalanan şablon yalnızca kimlik bilgisiyle birlikte bulunan saklanan şablon ile karşılaştırılır [64].

Bire Az (1: Az) Bölümlü Tanımlama: Bu yöntem, biyometrik bir tarama ile bir kimsenin iddia ettiği kimliği onaylamayı veya reddetmeyi ve ardından genel bir tanımlama sorusuna ya da bazı bilinen genel bilgilerin (cinsiyet, ırk, göz rengi, vb.). birbirleriyle karşılaştırılmasıyla oluşturulur [65].

Bire Çok (1: N) Kimlik Belirleme: Bu sistem, hastanın yakalanan biyometrik şablonunu sistemdeki tüm kayıtlı biyometrik şablonlarla anında karşılaştırır. Hastanın biyometrik kimlik bilgileri haricinde, bu eşleme için başka bir bilgi gerekmemektedir ve bu eşleme tipi, yinelenen tıbbi kayıtların hasta veri bütünlüğünü elde etmesini ve sürdürmesini önlemenin tek yoludur. [63].

1: 1 veya 1:F'e dayanan biyometrik hasta tanımlama sistemleri, birkaç eşleşmeye, hasta biyometrik tarama yapmadan önce bir takım tanımlama veya kimlik belgelerini istemek için tıbbi olanaklara ihtiyaç duyar. Sağlanan kimlik bilgisi, belirli bir hasta kaydını veya kayıt grubunu tespit eder. Biyometrik bir tarama gerçekleştirildiğinde, yakalanan şablon yalnızca bir kayıt (doğrulama) ya da çok küçük, bölünmüş bir kayıt grubu (1: Az) ile karşılaştırılır. Bu, hastanın taranmış biyometrik şablonunu, çoğaltılmayı kontrol etmek veya birinin birden fazla kimlik numarası altında kaydedilmesini önlemek için veri tabanındaki tüm kayıtlarla karşılaştırma mekanizması sağlamamaktadır. 1: 1 ve 1:F doğrulamasında, yinelenen kaydın oluşturulmasını engellemez ve hastaların birden fazla kişi adına kaydolması ve dolandırıcılık ihtimalini yükseltir [65].

Aksine, 1: N ve o sağlık ağı içinde herhangi bir yere check-in yaptığı her seferde her bir ana hasta endeksini tarar. İlk kimlik formunu sunduktan sonra listede gruplandırılmış olanlar yerine tüm sistemdeki her bir hastanın şablonunu arayarak tıbbi kayıtların çoğaltılmasını önlemek için tek araç olan 1: N, sağlık sisteminin verimliliğinin artırılması için tek gerçek yoludur. Hasta güvenliği seviyesi, daha düşük sorumluluk riski ve tıbbi kimlik hırsızlığı önleme programlarını güçlendirir [66].

Sağlık sektöründe biyometri, pahalı, verimsiz ve tehlikeli kimlik kartı PIN'ini veya şifre sistemlerinin yerine geçmekte ve avantajlı yeni özellikler sunmaktadır. Bu değişikliğin sebepleri ise şu şekilde sıralanabilir:

- Çalışan ve hasta kimliği, inkâr edilemez kanıt ve doğrulukla olmalıdır.
- Biyometrik sistemlerde, sağlık çalışanları, eylemlerinden daha doğru bir biçimde sorumlu tutulmaktadır.
- Kimlik kartlarının veya PIN'lerin yönetimi ve yeniden üretilmesinde önemli maliyet tasarrufları sağlanmaktadır.
- Biyometrik sistemler, kolay kullanımı sayesinde, hasta bakımını ile ilgili konularda zamandan kazandırır.
- İnsanlar asla parmak izlerini unutmaz veya paylaşmazlar [67].

Yenilikçi sağlık kuruluşları daha güvenli hasta erişimi ve bilgi paylaşımı için biyometri kullanmaktadır. Endüstrinin hızla sayısallaştırılması ve bireysel ve toplumsal sağlığın iyileştirilmesi için ulusal sağlık bilgi alışverişi için uyumlu bir itki nedeniyle doğru hasta tanımlaması ivme kazanıyor ve ivedi." "Artan birlikte çalışabilirlik için yapılan itki, hataları ve uyuşmazlıkları eşleştiren hasta verilerini katlanarak daha sorunlu ve tehlikeli hale getirebilir ve yetersiz hasta tanımlamasının hastanın güvenliğini tehlikeye atmaya ve yapay olarak bakım maliyetini arttırdığına inanılır" diye belirtiyor. Sağlık sektöründe biyometriye duyulan ihtiyaç astronomik oranlarda artmaktadır. Dünya çapındaki pazar potansiyeli 1,9 milyar dolar olarak tahmin edilmektedir. Bu miktarın 2018 yılına kadar %31.68 artacağı tahmin edilmektedir [68].

Biyometrik pazarın büyüme hızlarında önemli olan bir faktör ise HIPAA Yasası'dır. HIPAA, hasta gizliliğini ve hasta bilgilerinin gizliliğini korumak için federal gereklilikleri uygulayan katı yasalardır. Bu, tüm sağlık kuruluşlarının bu yeni standartları karşılamak için uygunluk prosedürlerini geliştirmeye başlamasına neden olmaktadır. Sonuç olarak, sağlık kuruluşları biyometrinin kullanımını kabullenmeye başlamaktadır. Biyometriyi kurumsallaştırmak, HIPAA uyumluluğunu sağlama stratejisini ile paralel olarak bazı maddeler ışığında paralel olarak ilerlemektedir. Bu maddeler [70];

• Kullanıcı Doğrulama,
• Hasta Bilgilerin Gizliliği,

• Ağ Güvenliği,
• E-Ticaret Uygulamaları İçin Web Güvenliği,
• İnternet Kimlik Doğrulama Hizmetleri,
• Veri Depolama ve Geri Alma Yönetimidir.

Biyometri, aynı zamanda tüm kimlik prosedürleri için operasyonel verimlilik yaratır, doğru hasta tanımlamasının bakım veya tedavi planlarına bağlanmasını veya her bir hasta için tıbbi kayıt yönetim sistemlerine uydurulmasını sağlayarak risk yönetiminde iyileştirmeler sağlar. Öte yandan, multi-spektral biyometri, özellikle de yetkili kullanıcıların olumlu tanımlanması yoluyla erişimi kontrol altına alma ihtiyacı olduğunda sağlık uygulamalarında önemli bir rol oynamaktadır. HIPAA düzenlemeleri doğrultusunda hasta gizliliğini önemsemekte ve biyometri, yalnızca yetkili personelin bu kayıtlara erişmesini sağlamaya yardımcı olabilmektedir. Biyometri, sigorta dolandırıcılığını en aza indirmeye ve ilaç gibi kontrollü stokların çalınmasını önlerken pahalı tıbbi cihazların yetkisiz kullanımına karşı güvence altına alınmasını sağlar [68].

Erişimi denetlemenin yanı sıra, multispektral biyometri, sağlık bakımında operasyonel verimliliği kolaylaştırmada rol oynamaktadır. Güvenlik çözümlerinin çoğu, işlemleri kolaylaştırmak yerine, sahtekârlık içeren eylemleri engellemek için tasarlanmıştır. Bununla birlikte, özenle tasarlanmış biyometrik sistemler yetkili kullanıcılara hızlı ve kolay erişim sağlayarak işlemleri düzene sokabilir. Biyometrik sistemler hastane politikaları ve prosedürlerine uyumu zorunlu hale getirebilir ve belgeleyebilir, hasta ve personel güvenliğini arttırır. Biyometri, teknoloji ve çözüm her kullanıcı için her seferinde güvenilir çalışabilirse uygulanabilir. Biyometrik teknoloji, kişisel sağlık bilgilerinin güvenli kullanımını, depolanmasını ve transferini iyileştirecektir. Hasta kimliği koruma önlemlerinin olmaması, hastalar için birçok önemli hususu ortaya koymakta, hastalar tıbbi kimlik hırsızlığının kurbanları olduklarında kayıtlarının çalınması, gelecekteki tedavileri ve mali sınırlarını tehlikeye düşürebilmektedir. Sağlık hizmetlerinde biyometrik sistemlerinin kullanımı sahtekârlığı bazı yollarla azaltabilir. Bunlar [70]:

• Sağlayıcı konumunda hastanın kimliğini doğrulayarak kart paylaşımı ve hasta kimlik hırsızlığı önleme;

• Hizmet için ücretli programlarda, hastanın hizmet tarihinde tedarikçinin yerinde olmadığı durumlarda sağlayıcıların "hayali iddialar" veya hizmetler için faturalandırmasını önleme;

• "upcoding" olarak adlandırılan potansiyel dolandırıcılığın bir göstergesi olarak verilen hizmet türüne kıyasla karşılaştırma yapmak için check-in ve check-out sürelerinin "denetim izi"ni oluşturma.

Bir hastanenin, tıbbı dolaplar ve depo odaları, ameliyathaneler ve hasta kayıtlarının yönetildiği ve saklandığı veri merkezleri de dahil olmak üzere bir çok alanı sıkı güvenlik gerektirir. Tehlikeli virüs üzerine araştırma çalışmaları ile ilgili olanlar gibi bazı hassas veriler, bu bilgileri suiistimal edebilecek kişilerin elinde korkunç sonuçlar doğurabilir. Sonuç olarak, bu hassas verileri korumak için biyometrik güvenlik yöntemleri kullanılmalıdır [71].

Biyometrik teknolojiyi sağlık hizmetine getirirken olası sosyokültürel, etik ve yasal sonuçların kabul edilmesi önemlidir. Örneğin, sosyokültürel uygulamalara bağlı olarak, bazı kişiler, sıklıkla dokunulan cihazın hastalığı yayabileceği düşüncesinden dolayı bir parmak izi tarayıcı kullanmayı reddedebilir. Dini inançları olan ve vücut bölümünün taramasını müdahaleci bulan diğer kişiler de bu sistemleri reddedebilir.

Öte yandan, biyometriyle mahremiyetin ahlaki çatışması bazı kişiler için bir endişe kaynağıdır çünkü taranan bilgi kimliğin bir parçasıdır. Biyometri, şu anda gizliliğin korunması için bir takım kurallara sahip olmadığından bireylerin özerkliği ve özgürlüklerinin tehdit altında kaldığı düşünülmektedir. Biyometri ile ortaya çıkabilecek bazı yasal konular da bulunmaktadır. Bunlar, yetkili bir kişinin kimliğine bürünme girişimi ve kimlik hırsızlığını içermektedir. Biyometri ile ilgili dikkate alınması gereken bir diğer yasal husus, yanlış reddedilme söz konusu olduğunda, bir kişinin gerekli tıbbi bakımın zamanında yerine getirilmesi için haklarının reddedilebileceğidir.

Biyometrik teknoloji tanıma mekanizması hasta tanımlamasında gelecek olabilir. John Trader'a (2012) göre, Joint Commission'un 2012'deki hasta güvenliği hedefi hasta kimliğinin doğruluğunu iyileştirmekti. Sonuç olarak, hasta güvenliğini

arttırmanın yanı sıra, sağlık hizmetlerinde sorumluluk ve tıbbi kimlik hırsızlığı da azaltılacaktı. Günümüzde ise, sağlık sisteminin çoğu, dolandırıcılıktan kolayca etkilenen, hasta kimliği için sigorta kartlarını, doğum tarihini veya bar kodlu bilezikleri kullanmaktadır. Tanıma biyometri uygulanması sadece hasta dolandırıcılıklarının oluşumunu azaltmakla kalmaz, aynı zamanda doğru hastaya bakım verilip verim artmış olur [66].

5.2. Hastane Sistemlerinde Yüz Tanıma

Dünya çapındaki hastaneler ve teşhis laboratuvarları, sigorta ödemelerinin azaltılması, ödememe yapılmaması ve sağlık dolandırıcılığından dolayı önemli zarara uğramıştır. Bu durum, hasta bekleme sürelerinin uzun olması ve bakım kalitesinin düşük olması gibi sonuçlara yol açmıştır. Yüz tanıma sistemleri ise, yalnızca yapay zekâ yüz algılama yöntemini kullanarak hastaları tanımlamakla kalmaz aynı zamanda tüm işlemleri gerçek zamanlı olarak izler ve yöneticilerin ölçülebilir ve düzeltici yönergelerle işlem yapmalarını kolaylaştırır [37].

Yüz tanıma sistemi, bir kişiyi bir video kaynağındaki bir dijital resim veya bir video karesinden otomatik olarak tanımlamak veya doğrulamak için kullanılan bir bilgisayar uygulamasıdır. İnsanlar genellikle yüzleri kişileri tanımak için kullanmaktadır ve son on yılda bilgi işlem yeteneğindeki gelişmeler otomatik olarak benzer tanımaları mümkün kılmaktadır. Erken yüz tanıma algoritmaları basit geometrik modeller kullanmıştır, ancak tanıma süreci şimdi karmaşık matematiksel gösterimler ve eşleme süreçleri bilimine dönüşmüştür. Son on ila on beş yıldaki önemli ilerlemeler ve girişimler, yüz tanıma teknolojisini dikkat çekici hale getirmiştir [71].

Otomatik yüz tanıma görece yeni bir konsepttir. 1960'lı yıllarda geliştirilen yüz tanıma sistemi için ilk yarı otomatik sistem, yönetici tarafından ortak bir referans noktasına olan uzaklık ve oranlar hesaplanmadan önce özellikler üzerinde (gözler, kulaklar, burun ve ağız gibi) bulunmasını gerektirmiş ve daha sonra referans verilerle karşılaştırılmıştır. 1970'lerde saç rengi ve dudak kalınlığı gibi 21 spesifik öz saptayıcı özellik otomatikleştirilerek tanıma yapılmıştır. Bu erken çözümlerin her ikisinde de sorun, ölçümün ve konumların elle hesaplanmasıdır. 1988'de, bir dönüm noktası olarak kabul edilen standart bir lineer cebirsel teknik kullanılmıştır [38].

1991'de gerçek zamanlı otomatik yüz tanıma sistemi geliştirilmiştir. 1993'ten beri, otomatik yüz tanıma sistemi hata oranı 272 oranında azalmıştır. 2006'da, en yeni yüz tanıma algoritmalarının performansları Yüz Tanıma Büyük Mücadelesi (FRGC) içinde değerlendirilmiştir. Sonuçlar, yeni algoritmaların, yüz tanıma algoritmasının 2002'nin 10 kat daha doğru ve 1995'ün 100 kat daha doğru olduğuna işaret etmiştir [37].

Çoğu durumda, yüz tanıma, diğer biyometri çözümlerine göre, sağlık sektöründe büyük avantajlara sahiptir. Yüz tanıma teknolojisi, hedefle temas gerektirmez ve geniş kapsamlı uygulamalar için uygundur. Kuşkusuz % 100 hijyenin gerekli olduğu sağlık sektörü bu avantajın en yoğun yaşandığı yerlerden biridir. Bir hastanede yüz tanımanın bazı çeşitli amaçlarla kullanılabilir. Bunlar [72]:

Tablo 3. Hastanede Yüz Tanıma Sistemlerinin Kullanım Amaçları

1. Hasta Yönetimi: Yüz tanıma kimlik kartını gerektirmez. Hastalar, yüzlerine göre sisteme kaydedilir.	Hastaneye gelen tüm hastalara bir hasta yönetim kartı verilmektedir ve hastaneye her gittiklerinde sunulması beklenmektedir. Bununla birlikte, kartların iki büyük dezavantajı vardır: 1. Hastalar kartlarını unutur veya kaybederler. 2. Kart manyetik alanların arızalanması kolaydır.
2. Temassız Doktor Bilgisayar Giriş Sistemleri	Doktorlar ellerini temiz tutmalı fakat aynı zamanda hasta bilgi formlarını kontrol etmek için yoğun bir şekilde bilgisayar kullanmalıdırlar. Yüz tanıma, doktorların ve diğer personelin yüzlerine bilgisayarlara temassız girmesini sağlar. Bilgisayar klavyelerine dokunmaları bu sayede gerekmez.
3. Kapı Erişim Kontrolü	Ameliyathane, doktor odası, laboratuvar, sınırlı bölge, Yoğun Bakım Ünitesine (ICU) girmek için ayrılmış tüm alanlara bu şekilde girilmelidir. Çünkü yüz tanıma bu girişleri güvence altına alır, girme girişimi varsa veya orada bulunmaması gereken bir hasta varsa bir alarm gönderir.
4. Spastik, Down Sendromlu Hastaların Tanınması	Düzgün konuşamayacak bazı hasatlık türlerine sahip kişilerin kimliklerinin doğrulanması şarttır. Bu hastalar için yüz tanıma en önemli adaydır. Sadece kameraya bakmak hastayı kolayca ve basitçe doğrulayacaktır.

Kaynak: Çevrimiçi, http://ayonix.com/tag/hospital-face-recognition/ Erişim Tarihi: 14.04.2017

Uygun klinik bakımı sağlamak için, hastaların doğru bir şekilde tanımlanması ve tıbbi kayıtlarının güncellenmesi gerekir. Bunu yapmak için, hastane personeli, hastaların adlarını ve ya diğer kimlik bilgilerini kullanarak tanımlamayı

gerçekleştirir. Ancak bu durum hastaların yanında kimliklerini bulunmadığında problem teşkil etmektedir. Buna ek olarak, kimlik bilgileri, hastalar arasında benzeşebilmektedir. Bir hastanın kaydı bulunmadığında, personel mevcut profili ve onunla ilişkili tıbbi geçmişi teşkil eden yeni bir profil oluşturur. Bu durum verimliliği azaltan bir durum olarak karşımıza çıkmaktadır. Hem iş gücünün arttığı bu durumda, hem de, medikal anlamda, hasta kayıtlarına ulaşılamaması, çeşitli testlerin tekrarına sebep olabilmektedir.

Bu durum, yüz tanıma ile hasta tanımlamasını hızlandırılarak giderilebilmektedir. Bir web kamerasıyla dahi gerçekleştirilebilecek olan bu sistemlerde, yüz tanıma anında bir hastayı tespit edebilir ve tıbbi kayıtlarını çıkarabilir. Mevcut arama işlevlerine ek olarak, web kamerasını başlatmak, hastanın yüzünü çerçevede tespit etmek ve daha önce öğrendiği yüzlerin veri tabanını bulmak için "yüze göre ara" işlemleri sıralanır. Yüz tanımlanırsa, o hasta için kayıt ekranda görünebilir. Aksi halde yeni bir hasta eklemek için kullanıcı arabirimi başlatılabilir, böylece hastane personeli hastanın ayrıntılarını girebilir.

Bahsedildiği üzere hastane otomasyon sitemlerinde, yüz tanıma sistemleri çeşitli şekillerde kullanılabilmektedir. Bunlardan ulaşılabilir olanları, hasta kayıt uygulaması ve hasta tanımlama uygulamasıdır.

Hasta kayıt uygulaması, bir hastayı sisteme kaydetmek için kullanılır. Kayıt süreci, hastanın pasaport büyüklüğünde dijital fotoğrafı da dahil olmak üzere gerekli, kritik acil tıbbi bilgilerini içeren “bir kimlik kartı” oluşturulmasını içerir. Bu acil tıbbi bilgiler, herhangi bir müdahale konusunda önemli olabilecek alerjiler gibi hastalıklar, isim, yaş ve cinsiyet gibi bazı kişisel bilgilerden oluşur. Ayrıca, hastanın geçmiş tıbbi öyküsü, geçmiş cerrahi geçmişi, sosyal geçmişi, aile geçmişi ve ilaçları gibi diğer opsiyonel bilgi parçaları da yakalanabilir. Hasta kayıtları hastanın izniyle yapılabilir veya doğrudan hasta tarafından yapılır. Kayıt için bir cep telefonu kullanılabilirken, kayıtçının kişisel bilgilerinden bazıları ilişkili cep telefonundan otomatik olarak alınabilir ve güvenlik amacıyla ve kayıt sonrası doğrulama için saklanır. Hasta bilgisinin kalitesi ve güvenilirliği amacıyla, bilgiye erişildiğinde hem depolama hem de geri çağırma konusunda bilgi kaynakları hakkında bir ayrım yapılır. Bu bilgi kaynaklarına dayalı olarak hasta bilgisi hakkında bir dereceye kadar

güvenin anlaşılmasına yardımcı olur. Güvenlik ve gizlilik amaçları için, gizlilik etkileri olmaksızın ve hiçbir zaman tanımlama ölçütünün parçası olmayacak orijinal metinsel veriler şifreli biçimde saklanır. Hasta Tanımlama uygulaması ise, hastanın yüzünden hastanın öncede kaydedilmiş tüm bilgilerine ulaşabilmesi durumudur. Tıbbi bir acil durum sırasındaki en iyi durum senaryosunda, hastanın adı, yaşı ve cinsiyeti bilinmektedir. Bu durumda, mevcutsa, ilişkili bilgileri almak için yaş, ad ve cinsiyet ile bir doğrulama işlemi gerçekleştirilir. En kötü senaryoda, ne ad ne de yaş bilinmektedir. Bu durumda, hastanın cinsiyetini ve tahmini yaşı kullanarak aşağıda tanımlandığı gibi bir tanımlama işlemi gereklidir [73].

Bu sistemler, yüz eşleme, şifreleme, şifre çözme, depolama ve kurtarma işlemlerini yapan bir diğer sistem tarafından desteklenmelidir. Bahsedilen sistem yapılan kayıt verilerini kabul eder, verileri gerektiği gibi biçimlendirir, şifreleme ve yüz şablonu ayıklama gerçekleştirir ve bilgileri veri tabanında saklar. Yüz şablonu çıkarımı başarısız olursa kayıt başarısız olur. Hastanın tanımlanması sırasında, arka uç yüz eşleme etkinliğini gerçekleştirir ve eşleşen hastaların yüz görüntülerini ve daha sonraki tıbbi bilgileri verir.

Hastanede yüz tanıma sistemlerinin kullanılmaya başlaması oldukça güncel bir konudur. Bir İskoç hastanesi olan Fife Victoria Hastanesi acil bakıma ihtiyacı olan hastaları tespit etmek için yüz tanıma teknolojisini kullanmaya Eylül, 2016'da karar vermişlerdir. St. Andrews Üniversitesi'ndeki bilim adamları tarafından geliştirilen yenilikçi kamera tabanlı teknolojiyi ilk defa denemeye başlayacak olan bu hastane nabız sayısı ve kan oksijen seviyeleri gibi yaşamsal bulguları ölçmek için kullanılan parmak klipsi yerine hastanenin solunum koğuşunda test edilecek bu yeni teknoloji ile, uzmanlaşmış kamera görüntüleri kullanarak aynı anda altı kişiye kadar olan kan oksijen seviyelerini ve kalp atış hızını tespit edebilmektedir [74].

5.3. Hastane Sistemi Önerisi ve Değerlendirme

Türkiye'de hasta kayıt sistemlerinde biyometrik uygulamalar kullanılmaya başlanmıştır. Ancak, yaygın olarak kullanılmadığı mevcut sistemde ve geçiş yapılacak avuç içi damar okuma ile gerçek kişileri takip etmek zor ve güvensizdir. Bu sistem; başkası adına giriş ve işlem yapılmasını engelleyecek bir sistem değildir. Doktor kaşesini asistan, uzman kaşesini doktor veya asistanın kullanması birden fazla yerde işlem yapıyor gözükmesi daha vahimi yetkili olmayan kişilere işlem hakkı verilmiş olması sorununu çözmeyecektir. Kaşeyi teslim eden personel asistanının avuç içini okutup işine devam edecektir.

Mevcut sistemlerde görev yeri tanımı çok zordur. Yüz tanıma sistemlerinde diğer yöntemlere nazaran kendi yüzünü bir başkası tanıtılamayacağından maksimum verimlilik hedeflenmektedir. Bu durum maliyetinin de görece düşük olmasından kaynaklanmakta ve sistem oldukça kolay bir biçimde uygulanabilmektedir. Çünkü yüz tanıma sistemleri yüze bakan, doksan derece de sabitlenmiş bir kamera ile bu durum kolayca yapılabilir. Özetle; hastane otomasyon sistemlerinin sorunu, ulusal bir veri tabanı bulunmaması üst başlığında toplanabilir.

Bu bağlamda, yüz tanıma sistemleri ulusal veri tabanının bilgisayar insan etkileşimleri bakımından takip, güvenlik, maliyet ve en önemlisi insan ilişkilerinde de olduğu gibi doğru şekilde tanıştırılan bir altyapıda olması gerekmektedir. Biyometrik tanıma sistemleri kurumların kullanımından ziyade devlet elinde bir ulusal veri tabanında tutulması ve bunun için mernis, e- devlet, uvap, pol-mer gibi sistemlerde olduğu gibi web servisleri kullanılarak haberleşilmesi böylelikle kişilerin anayasal hakları çiğnenmeden ve gelecekteki başka sistemlerle de entegre kullanılabilecektir.

Hastanelerde, yüz tanıma sistemlerinin kullanılacağı yazılımın iki ayağı olmalıdır. Bu ayaklardan ilki hastane personeli takip bölümü, ikincisi ise hasta takip bölümüdür. Adından da anlaşılacağı gibi personel, personel takibi amaçlı olan bölümdür. Personel giriş-çıkışı, bakılan hasta sayısı, reçete ve sevkler gibi alanları içermektedir. Amaç gerçekçi, verimli ve iş ahlakına uygun çalışma imkânı sağlamaktır.

Öte yandan mevcut donanımla yukarıdaki sistem kullanıldığında bilgisayarın başına oturan kişi takip edilemez. Nitekim doktor kaşesi ve parafı takibi yapılamadığı gibi verilecek olan kullanıcı adı parolanın da takibini yapmak oldukça zordur. Bundan dolayı getirilen avuç içi damar okuma sistemi de çözüm olmamış kötüye kullanıma açıktır. Bu bağlamda; aynı uzman kaşesi kullanımında olduğu gibi; uzman doktor asistanın elini okutabilir ve adına işlem yaptırabilir. Yüz tanıma sisteminde takip çok kolaydır. Fotoğrafla eşleştirme uzaktan takip veya geriye dönük denetim dahi gerçekleştirilebilmektedir.

Hasta takibinde genel olarak kimlikli işlem kaydı ve ya avuç içi damar okuma sistemi kullanılmaktadır. Bu sistemlerde işlemler şu şekilde gerçekleşmektedir:

- Hasta Girişi;
- Aciliyet Durumunun Tespiti;
- Hasta Acil Değilse Hastanın Önceki Kayıt Durumunun Tespiti;
- Randevu Kontrolü;
- Randevulu ise Bilgi İşlem Kaydı ve Sıra Numarası İşlemlerinin Gerçekleştirilmesidir.

Mevcut sistemde dosyalı hasta olduğunda ise dosya doktor tarafından arşivden istenmektedir. Hastaya buna göre tedavi edilmektedir. Öte yandan hastanın, diğer sağlık kurumlarında bir geçmişi olup olmadığı ve ya uygulanan tedaviler görünmemektedir. Bu durum tekrarlanan tedavilerden ve istenen tahlillerden hastayı ve doktoru korumaktadır. Bu şekilde kaynak israfı da önlenecektir. Bu bağamda, e-devlet sistemiyle entegre ulusal bir yüz tanıma sisteminin oluşturulması, bu gibi sorunlardan sağlık sistemini arındıracaktır.

Bu sistem şu şekilde özetlenebilir. Pasaport, ehliyet gibi kimlik belirleyici belgelerdeki verilerim bir veri tabanında toplanır. Bu veri tabanında parmak izi raporu biyometrik fotoğraf, kimlik bilgileri gibi alanlar bulunmaktadır. Bu bağlamda benzer bir sistemde tüm hastanelerde de uygulayabilir. Tüm hasta bilgileri, kimlik numarası ve fotoğraf ile eşleştirilip genetik hastalık verileri de dahil olmak üzere

doktorların hizmetine sunulabilir. Böylelikle güvenlik ve takip için kurulan sistem ilerleyen zamanlarda doktorların istatistiksel veriler ışığında bilimsel araştırma yapmaları için olanak sağlayabilir.

Bu durum ülke çapında gerçekleştirilecek olan kimlik kartı yeniliği ile de eşleştirilebilir. Bu bağlamda; çipli kartlara biyometrik bilgiler yüklenmesi halinde basit bir eşleme gerçekleştirilerek bu gibi bilgiler hasta kayıt sistemlerinde de kullanılabilir hale gelebilmektedir.

Önerilen sistemin aşamaları ise şu şekilde sıralanabilir:

- Personel girişi;
- Kimlik ve ya çipli kimlik ile kimlik tespiti;
- Bilgi işlemde yüz okuma;
- Randevu kontrolü;
- Kayıtlı ise sıra numarası
- Hiçbir sistemde kayıtlı değil ise kimlik tarama ve yüz kayıt işleminin gerçekleştirilmesi.

Mevcut sistemde hastanelerin hasta takibinde de kötüye kullanımlar söz konusu olabilmektedir. Örneğin hastaneye hiç gitmemiş veya geçmiş zamanda gitmiş bir hasta başka bir hastalık tedavisi görmüş gibi gösterilebilir. Türkiye'de hasta kayıt sistemleri için yayın olarak kullanılan avuç içi damar okuma sistemi de bu kötüye kullanımların önüne geçememektedir. Çünkü gözle tespiti imkânsızdır. Öte yandan biyometrik yüz kaydı ile bilgi işlem girişindeki yüz kaydı karşılaştırılarak otomatik veya elle sonuca kolaylıkla ulaşılabilir.

Sistem sanılanın aksine yüksek donanım seviyesi gerektirmemektedir. Yüze bakan standart bir 8MP CCD sensörlü kameraya ek olarak yüz tanıma kütüphanesi veya özel yazılmış bir algoritma ile doğru bir şekilde çalışmaktadır. Ek olarak Bir aydınlatma kullanılabilir. Güvenirliği artırmak adına kızılötesi kamera kullanılarak karanlık ortamlarda sonuç elde edilebilir.

6. SONUÇ

Biyometri, güvenlik protokolü gerektiren her şeyin içine uygulanabilen gelişen ve değişen bir teknoloji alanıdır. Uygulama maliyeti arttıkça artan güvenlik ve elbette değişken yeteneklere sahip kişilerin erişilebilirliğinin artması, maliyetin artmasının sebepleri arasında gösterilebilir.

Biyometri iki şekilde çok yararlıdır. Öncelikle, teröristlerin biyometrik tanımlaması, önleyici amaçlar için ulus içerisinde ve dışındaki tüm potansiyel risk alanlarına elektronik olarak dağıtılabilir. İkincisi, hastalığın tespit edilmesinde yardımcı olabilir ve eğer etkili ise, gizlilik gerektiren biyolojik saldırıların erken uyarı sistemi algılanması ile ölüm oranlarını önemli ölçüde azaltacaktır.

Biyometri, sadece sağlık yönetim sisteminin mahremiyetini ve güvenliğini sağlamakla kalmaz, ayrıca, tıbbi tesislerle bağlantı kurarak bulaşıcı hastalıkları bildirmek ve ölüm oranlarını kontrol etmek için biyo-terörizm ve halk sağlığı faaliyetlerinde de hayati bir rol oynamaktadır. Yeni ve pahalı teknolojiler ve her zamankinden daha uzun yaşayan bir nüfustan gelen talebin artmasıyla hastaneler ve diğer sağlık tesisleri, rekabet edebilmek ve maliyetleri artırmak için artan baskılarla karşı karşıyadır. Bu bağlamda, hasta kaydı kadar doktor görev tanımlarında da ciddi iyileşmeye ve verimliliğe sebep olacak yüz tanıma sistemleri oldukça önemli bir yeri olacak bir uygulamadır. Bunun dışında, hastane sistemlerinde yüz tanıma sistemleri, hasta yönetimi, temassız doktor bilgisayar giriş sistemleri, kapı erişim kontrolü, spastik, Down sendromlu hastaların tanınması gibi konularda kullanılabilmektedir.

Öte yandan, biyometri, tüm teknolojik gelişmelerde olduğu gibi, en son teknolojiye olan bağımlılık yaratabilir ve bu durum güvenlik yanılsaması sebebiyle bir kurumu daha da savunmasız hale getirebilir. Bu nedenle devlet kurumlarının ve ticari şirketlerin tetikte olmaları ve bir işletmenin teknolojik varlıklarını güvence altına almanın en güncel yöntemlerini sürekli araştırmaları gerekir.

Bu bağlamda, biyometrik uygulamalar ve önerilen hastane sistemi, uygun koşullar ve temkinli yönetimler sayesinde, bahsedilen kurumlara oldukça faydalı olabilecek bir yöntem olarak karşımıza çıkmaktadır.

7. KAYNAKLAR

[1] Xiao, Q. (2004, June). A biometric authentication approach for high security ad-hoc networks. In Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC (pp. 250-256). IEEE.

[2] Jain, Shruti, Surabhi Gupta, and Raj Kumar Thenua. "A review on Advancements in Biometrics." Int J Electron Comput Sci Eng 1 (2012): 853-9.

[3] Zhang, D. D. (2013). Automated biometrics: Technologies and systems (Vol. 7). Springer Science & Business Media.

[4] Vallabhu, H., & Satyanarayana, R. V. (2012). Biometric authentication as a service on cloud: Novel solution. International Journal of Soft Computing and Engineering

[5] Riera, A., Soria-Frisch, A., Caparrini, M., Cester, I., & Ruffini, G. (2009). Multimodal physiological biometrics authentication. Biometrics: Theory, Methods, and Applications, 461-482.

[6] Rawat, Ajay, and Shivani Gambhir. "Biometric: Authentication and Service to Cloud." Handbook of Research on Securing Cloud-Based Databases with Biometric Applications (2014): 251.

[7] Çevrimiçi, https://www.secureidnews.com/news-item/biometrics-101-part-ii-storing-and-matching-biometric-templates/ Erişim Tarihi: 06.04.2017

[8] Camp, L. J., & Johnson, M. E. (2012). The economics of financial and medical identity theft. Springer Science & Business Media.

[9] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634.

[10] Alliance, S. C. (2011). Smart Cards and Biometrics. Erişim: www. smartcardalliance. org.

[11] Boulgouris, N. V., Plataniotis, K. N., & Micheli-Tzanakou, E. (Eds.). (2009). Biometrics: theory, methods, and applications (Vol. 9). John Wiley & Sons.

[12] Yoruk, E., Konukoglu, E., Sankur, B., & Darbon, J. (2006). Shape-based hand recognition. IEEE transactions on image processing, 15(7), 1803-1815.

[13] Bulatov, Y., Jambawalikar, S., Kumar, P., & Sethia, S. (2004). Hand recognition using geometric classifiers. Biometric Authentication, 1-29.

[14] Adeoye, O. S. (2010). A survey of emerging biometric technologies. International Journal of Computer Applications, 10.

[15] Doublet, J., Lepetit, O., & Revenu, M. (2006, November). Contact less hand recognition using shape and texture features. In Signal Processing, 2006 8th International Conference on (Vol. 3). IEEE.

[16] Nixon, M. S., Carter, J. N., Shutler, J. D., & Grant, M. G. (2002). New advances in automatic gait recognition. Information Security Technical Report, 7(4), 23-35.

[17] Winter, D., (1991). The Biomechanics and Motor Control of Human Gait: Normal, Elderly and Pathological. University of Waterloo Press, Waterloo.

[18] Begg, R., & Kamruzzaman, J. (2005). A machine learning approach for automated recognition of movement patterns using basic, kinetic and kinematic gait data. Journal of biomechanics, 38(3), 401-408.

[19] Proenca, H. (2010). Iris recognition: On the segmentation of degraded images acquired in the visible wavelength. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(8), 1502-1516.

[20] Daugman, J. (2004). How iris recognition works. IEEE Transactions on circuits and systems for video technology, 14(1), 21-30.

[21] Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern recognition, 47(8), 2673-2688.

[22] Bolle, R. M., Connell, J., Pankanti, S., Ratha, N. K., & Senior, A. W. (2013). Guide to biometrics. Springer Science & Business Media.

[23] Jueneman, R. R., & Robertson, R. J. (1998). Biometrics and digital signatures in electronic commerce. Jurimetrics, 38(3), 427-457.

[24] Marc Gaudreau (1999), "On the distinction between Biometrics, and Digital Signatures" CIC Enterprise Solutions http://www.cic./enterprise/whitepapers.asp.

[25] Çevrimiçi, http://www.eschoolnews,com/showstory.cfm?ArticleID=2146.eSchoolNewsonline.April26,2001 Erişim Tarihi: 15.04.2017

[26] Çevrimiçi, https://www.pcpd.org.hk/english/infocentre/files/cakouk ian-paper.doc Erişim Tarihi: 16.01.2017

[27] Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27-32.

[28] Matyáš, V., & Rıha, Z. (2000, November). Biometric authentication systems. In verfügbar über: http://grover. informatik. uni-augsburg. de/lit/MM-Seminar/Privacy/riha00biometric. pdf.

[29] Bleumer, G. (1999). Biometric authentication and multilateral security. Multilaterial security in communications, Addison-Wesley, 157-172.

[30] Ding, Y., Zhuang, D., & Wang, K. (2005, July). A study of hand vein recognition method. In Mechatronics and Automation, 2005 IEEE International Conference (Vol. 4, pp. 2106-2110). IEEE.

[31] Mulyono, D., & Jinn, H. S. (2008, April). A study of finger vein biometric for personal identification. In Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on (pp. 1-8). IEEE.

[32] Liu, Z., Yin, Y., Wang, H., Song, S., & Li, Q. (2010). Finger vein recognition with manifold learning. Journal of Network and Computer Applications, 33(3), 275-282.

[33] Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation computer systems, 16(4), 351-359.

[34] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

[35] Carter, R. (2014). The brain book. Dorling Kindersley Ltd.

[36] Jain, A., Bolle, R., & Pankanti, S. (Eds.). (2006). Biometrics: personal identification in networked society (Vol. 479). Springer Science & Business Media.

[37] Bruno, J. (2008). Face Recognition. Villanova University. 8-14.

[38] Tanaka, J. W., & Farah, M. J. (1993). Parts and wholes in face recognition. The Quarterly journal of experimental psychology, 46(2), 225-245.

[39] Jain, A. K., & Li, S. Z. (2011). Handbook of face recognition. New York: Springer.

[40] Nabiyev, V. V. (2012). Yapay zeka: insan-bilgisayar etkileşimi. Seçkin Yayıncılık.

[41] Çevrimiçi, http://nursing.uomosul.edu.iq/files/pages/page_3184920.pdf Erişim Tarihi: 15.05.2017

[42] Agnes, O. N. (2011). Automated Hospital Management System (Master's Thesis). University of Nigeria.

[43] Primrose, W. R. (1998). Community hospitals. Age and Ageing 1998; 27: 261-263

[44] Ayanian, J. Z., & Weissman, J. S. (2002). Teaching hospitals and quality of care: a review of the literature. The Milbank Quarterly, 80(3), 569-593.

[45] Sultz, H. A., & Young, K. M. (2006). Health care USA: Understanding its organization and delivery. Jones & Bartlett Learning.

[46] English, M., Lanata, C., Ngugi, I., & Smith, P. C. (2006). The district hospital. Disease Control Priorities in Developing Countries, 2, 1211-1228.

[47] Çevrimiçi, https://www.sst.dk/da/planlaegning/specialeplanlaegning/~/media/3499BD6FE4894BF1B75A27CAD2A3AB29.ashx Erişim Tarihi: 14.02.2017

[48] Çevrimiçi, http://www.hipaajournal.com/improve-hospital-workflows/ Erişim Tarihi: 14.03.2017

[49] Çevrimiçi, http://www.who.int/hospitals/en/ Erişim Tarihi: 04.04.2017

[50] Seth T. (2015). Erişim: https://www.linkedin.com/pulse/benefits-implementing-hospital-management-system-tanmay-seth

[51] Kuipers, B. (2016). Evaluation of a Hospital Information System (HIS) implementation success from a users' perspective: A Mixed Method Research (Master's thesis).

[52] Yusof, M. M., Papazafeiropoulou, A., Paul, R. J., & Stergioulas, L. K. (2008). Investigating evaluation frameworks for health information systems. International journal of medical informatics, 77(6), 377-385.

[53] Chaudhry, B., Wang, J., Wu, S., Maglione, M., Mojica, W., Roth, E., ... & Shekelle, P. G. (2006). Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Annals of internal medicine, 144(10), 742-752.

[54] Çevrimiçi, https://acgilsoftwares.wordpress.com/2013/11/07/functions-of-hospital-management-information-system/ Erişim Tarihi: 14.04.2017

[55] Çevrimiçi, http://www.meddata.com.tr/tr/index.php?sayfa=hizmetler-hastane-bilgi-yonetim-sistemleri. Erişim Tarihi:12.03.2017

[56] Çevrimiçi, http://hitconsultant.net/2014/07/21/6-big-benefits-of-applying-automation-to-healthcare/ Erişim Tarihi: 09.04.2017

[57] Bepko Jr, R. J., Moore, J. R., & Coleman, J. R. (2009). Implementation of a pharmacy automation system (robotics) to ensure medication safety at Norwalk hospital. Quality Management in Healthcare, 18(2), 103-114.

[58] Agarwal, P., Kothari, P., Kadam, M., Bangera, A., Rughwani, V. A (2016). Survey on Hospital Management System Using Smart Card and Cloud Infrastructure.

[59] Ceylan, F. (2015). Erişim: http://www.uludag.edu.tr/dosyalar/shmyo/ders_notlari/kaynak/HBYS-2015.pdf Erişim Tarihi: 12.03.2017

[60] Esatoğlu A.E., Köksal A. (2002). Hastanelerde bilgisayar teknolojisi kullanımı. Ankara Üniversitesi Tıp Fakültesi Mecmuası. 55: 29-40.

[61] Cox CL. (1995). The health care system. In: Heath HBM (ed). Potter and Perry's Foundations in Nursing Theory and Practice. London: Mosby: 30-31.

[62] Ay, F. (2009). Uluslararası elektronik hasta kayıt sistemleri, hemşirelik uygulamaları ve bilgisayar ilişkisi. Gülhane Tıp Dergisi, 51(2), 131-136.

[63] Çevrimiçi, http://www.rightpatient.com/blog/the-difference-between-1n-11-and-1few-and-why-it-matters-in-patient-id/ Erişim Tarihi: 16.03.2017

[64] Bolle, R. M., Ratha, N. K., & Pankanti, S. (2004). Performance evaluation in 1: 1 biometric engines. In Advances in Biometric Person Authentication (pp. 27-46). Springer Berlin Heidelberg.

[65] Çevrimiçi, http://web.science.mq.edu.au/~isvr/Documents/pdf%20files/biometrics/Biometrics%20Explained.pdf Erişim Tarihi: 14.04.2017

[66] Çevrimiçi, http://www.m2sys.com/blog/important-biometric-terms-to-know/defining-patient-verification-identification-in-healthcare/ Erişim Tarihi: 14.03.2017

[67] Çevrimiçi, http://www.versos.com.sa/solutions/iss/iam/healthcare_biometric_iam.htm Erişim Tarihi: 12.04.2017

[68] Caldwell, T. (2015). Market report: border biometrics. Biometric Technology Today, 2015(5), 5-11.

[70] Shawl, D. (2013). Biometrics–implementing into the healthcare industry increasesthe security for the doctors, nurses, and patients (Doctoral dissertation, thesis for masters degree, davenport university).

[71] Jain, A., Flynn, P., & Ross, A. A. (Eds.). (2007). Handbook of biometrics. Springer Science & Business Media.

[72] Çevrimiçi, http://ayonix.com/tag/hospital-face-recognition/ Erişim Tarihi: 14.04.2017

[73] Nwosu, K. C. (2016). Mobile Facial Recognition System For Patient Identification In Medical Emergencies For Developing Economies. Journal for the Advancement of Developing Economies. 55-66.

[74] Çevrimiçi, http://www.scotsman.com/future-scotland/tech/fife-hospital-to-use-facial-recognition-to-detect-vital-signs-1-4221845 Erişim Tarihi: 15.03.2017

ÖZGEÇMİŞ

1983 yılında Kırklareli Vize'de doğdum. İlkokul, Ortaokul ve Lise eğitimimi İstanbul'da tamamladım. Eskişehir Anadolu Üniversitesi İktisat Fakültesi Kamu Yönetimi bölümünden mezun oldum. 2013 yılında Beykent Üniversitesinde Yüksek Lisans eğitimime başladım. 2001 yılında Çeşitli firmalarda web yazılım alanında görev aldım. 2006 yılından beri kendi firmamda özel yazılım ve danışmanlık hizmeti vermekteyim.

Mehmet ŞAM