SİBER GÜVENLİKTE BİYOMETRİK SİSTEMLER VE YÜZ TANIMA

Süleyman FİLİZ

YÜKSEK LİSANS TEZİ
BİLGİSAYAR BİLİMLERİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

NİSAN 2012
ANKARA

Süleyman FİLİZ tarafından hazırlanan SİBER GÜVENLİKTE BİYOMETRİK SİSTEMLER VE YÜZ TANIMA adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Hasan Şakir BİLGE
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Bilimleri Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan: : Doç. Dr. Suat ÖZDEMİR

Üye : Doç. Dr. Hasan Şakir BİLGE

Üye : Yrd. Doç. Dr. Nursel AKÇAM

Tarih : ...../12/2012

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Süleyman FİLİZ

SİBER GÜVENLİKTE BİYOMETRİK SİSTEMLER VE YÜZ TANIMA

(Yüksek Lisans Tezi)

Süleyman FİLİZ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ
Nisan 2013

ÖZET

Globalleşen ve dijital ağların yaygınlaştığı dünyamızda insanların hayatında teknoloji giderek artan bir oranda yer almaya devam etmektedir. Bu sistemlerin güvenliğinin sağlanması büyük önem taşımaktadır. Elektrik, elektronik sistemler, internet, intranet, bilgi ve bilişim sistemleri güvenliği ile ilgili her şey ve bu kapsamda alınan her türlü güvenlik önlemi siber güvenlik olarak ifade edilmektedir.

Siber güvenliğin kapsadığı alanlardan biri olan ve insanları farklı kılan ölçülebilir psikolojik veya davranışsal özelliklerin kimlik tespit amacıyla kullanıldığı biyometrik sistemler hızla yaygınlaşmaktadır. Özellikle otomatik kimliklendirme yaparak giriş çıkış kontrolünde kullanımı ön plandadır. Biyometrik sistemlerden olan yüz tanıma ise günümüzde halen üzerinde çalışılan bir konudur. Bu tezde yüz tanıma ile ilgili daha iyi sonuçlar elde etmek için yeni yaklaşımlar incelenmiş ve yüz tanıma işlemini gerçekleştiren bir yaklaşım geliştirilmiştir.

Özellikler, nesne tanımanın temel unsurlarıdır. Bu nedenle, bir yüzü tanımlamak için yüz tanıma sürecinde, hangi özelliklerin verimli kullanıldığını bilmek gerekir. Bu kapsamda birçok yaklaşımın yanında, SIFT algoritması yüz

tanıma amaçlı özellikle yüz bölgesindeki etkin değişmez özellikleri bulmak için kullanılmıştır.

Bu tezde, siber güvenlik, biyometrik yöntemler ve yüz tanıma problemi üzerinde araştırma yapılarak, kullanılan temel yöntemler incelenmiştir. Nesne eşleştirmede kullanılan yöntemlerden biri olan SIFT yöntemi yüz tanıma amacıyla farklı yüz veritabanlarında ve farklı şekillerde denenmiştir.

Bilim Kodu : **902.1.067**
Anahtar Kelime : **yüz tanıma, SIFT, görüntü işleme, destek vector makinesi, siber güvenlik, biyometrik sistemler**
Sayfa Adedi : **51**
Tez Yöneticisi : **Doç. Dr. Hasan Şakir BİLGE**

BIOMETRIC SYSTEMS IN CYBER SECURITY AND FACE RECOGNITION

(M.Sc. Thesis)

Süleyman FİLİZ

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

April 2013

ABSTRACT

The era of digital technology in our globalizing world is increasingly continuing to taking place in the lives of people. Ensuring the security of these systems is of great importance. Electrical, electronic systems, internet, intranet, knowledge, and information systems security and everything to do with all kinds of security measures are taken in this context, is referred to as cyber security.

Cyber security is one of the areas covered by measurable psychological or behavioral traits that distinguish people and is used for identification. Biometric systems are becoming increasingly common. In particular, the use of automatic identification is important in the control of entry and exit. Today, Biometric face recognition systems are still hot topic. In this thesis, new approaches about face recognition are investigated and a face recognition approach is developed to achieve better results.

Features are essential elements of object recognition. Therefore, to define a face in recognition process, it must be known what features are being used effectively. In this context, beside many approaches, SIFT algorithm is used to find unchanged features for face recognition.

In this thesis, cyber security, biometric systems, and face recognition methods

are investigated. SIFT, one of the methods used in the object matching, is tested in different ways and with different face data for the purpose of face recognition.

Science Code : **902.1.067**
Key Words : **face recognition, SIFT, image processing, support vector machines, cyber security, biometric systems**
Page Number : **51**
Adviser : **Assoc. Prof. Dr. Hasan Şakir BİLGE**

TEŞEKKÜR

Tezin hazırlanması aşamasında bana her türlü desteği veren danışman hocam sayın Doç. Dr. Hasan Şakir BİLGE'ye teşekkürü bir borç bilirim.

İÇİNDEKİLER

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

TABLOLARIN LİSTESİ

Tablo **Sayfa**

KISALTMALAR

Bu çalışmada kullanılan bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklama**
DNS	Domain Name System (Alanadı Adlandırma Sistemi)
SIFT	Scale Invariant Feature Transform (Ölçekten Bağımsız Özellik Dönüşümü)
SVM	Support Vector Machine (Destek Vektör Makinası)
CALTECH	California Institute of Technology (Kaliforniya Teknoloji Enstitüsü)

1. GİRİŞ

Günümüz dünyasında hayatımızın her alanında yer eden ve hayatımızı kolaylaştıran teknolojinin gelişmesi paralelinde bu teknolojilerin güvenliği konusu da önemli bir konu haline gelmiştir. Bu bağlamda hayatımızdaki tüm elektrik elektronik sistem ve yazılımların olası güvenlik açıklarına karşı topyekûn koruma olarak siber güvenlik kavramı son yıllarda güncel bir konu haline gelmiştir. Siber güvenlik kavramı ile ilgili birçok tanım olmakla birlikte, genel olarak elektrik elektronik sistemlerin, her türlü büyüklük ve özellikteki ağların, haberleşme sistemlerinin, yazılımların her türlü açık ve/veya gizli tehlikelere karşı güvenliğinin sağlanması olarak tanımlarız.

Siber güvenlik konularından bir tanesi olan biyometrik sistemler günümüzde yaygın kullanımı olan ve özellikle kontrollü giriş çıkış sağlanan alanlarda artan bir oranda kullanılmaktadır. Biyometri teriminin birçok tanımı olmakla birlikte kısaca insanları farklı kılan ölçülebilir psikolojik veya davranışsal özelliklerin kimlik tespit amacıyla kullanılan bilişim sistemi ile kontrol edilen kontrollü sistemler olarak ifade edilebilir. Biyometrik sistemler aslında insana özgü olan ve sadece onu niteleyen özelliklerini kullanarak yapılan tanıma yol ve yöntemlerdir. Bu yöntemler parmak izi, el ve yüz geometrilerinin incelenmesi, konuşma incelemesi, göz tanıma gibi birçok değişik yaklaşım ve yöntem içermektedir.

Güvenlik olgusunun öneminin arttığı yerlerde yüz tanıma sistemleri artan bir derecede kullanılmaya başlanmıştır. Yüz resimlerinin çoğunu yada bir kısmını inceleyip yüz tanıma maksadıyla geliştirilmiş değişik yöntemler söz konusudur. Peki, yüz tanıma nedir diyecek olursak yüz tanıma kısaca her insana özgü yüz yapısının ayırt edici karakteristik özelliklerini kullanılarak yapılan işlemdir. Gerçekte birçok biyometrik tanıma sistemlerinde olduğu gibi yüz tanımadaki yol ve yöntemler de benzerdir ve diğerleri ile aynı yaklaşımları göstermektedir.

Yüz tanımada aslında işin temelinde yüce yaratıcının insanı eşsiz ve benzersiz yaratması yatmaktadır. Göz bebeğine benzer bir şekilde insan yüzlerinde de insanlara özgü ve her insanının birbirinden farklı olacak şekilde eşsiz özellikleri mevcuttur. Ama birçok konuda olduğu gibi aslında bu durum birçok insan tarafından bilinmez. İnsan oğlunun yüz bölgesinde yer alan tüm organların kendi aralarında altın oran

dediğimiz müthiş bir oran yer almaktadır ve oran eğer ki dışarıdan yapay bir müdahale olmadığı sürece insan hayatı boyunca değişmez. İşte insan yüzündeki bu özellikler değişik yöntemlerle belirlenip farklı eşleştirme yöntemleri ile yüz tanıma gerçekleştirilmiş olur. Bir bilişim sistemi ile yapılan bu işlemde yüz resmi veritabanındaki birçok yüz görüntüsü ile karşılaştırılır ve eşleşen bir durum varsa o yüze sahip kişiye erişim veya geçiş izni verilir.

Bu tezde yüz tanıma ile ilgili literatürde yer alan birçok yöntem incelenmiştir. Yapılan incelemeler sonucunda daha çok nesne algıma ve tespit etme için geliştirilmiş olan Scale Invariant Feature Transform (SIFT) algoritmasının kullanılması uygun görülmüştür. Peki neden bu algoritma sorusuna kısaca cevap verecek olursak algoritmanın değişik ölçek, açı ve yön şartlarından fazla etkilenmemesi bizim için tercih sebebi olmuştur. Fakat yapılan çalışmalarda SIFT algoritması üzerinde değişik yöntem ve parametrelerde başarılı sonuçlar elde etse de bu algoritmanın tek başına yeterli olmayacağı gözlemlenmiştir. Bu gözlemler sonucunda bu algoritmanın değişik yöntemler ile birlikte kullanılması incelenmiştir. Netice olarak; değişik ortam ve şartlarda SIFT algoritması ile birlikte Support Vector Machine (SVM) algoritmasının kullanılmasının daha doğru sonuçlar verdiği görülmüştür. Bu yaklaşım birçok yüz veritabanında çalıştırılarak elde edilen sonuçlar tablo olarak verilmiştir. Geliştirilen yaklaşım yüz tanıma sistemlerinde aşağıda belirtilen amaçlar için kullanılabilir.

İnsan tanıma: Bir veritabanı içindeki insanın kimliğinin otomatize bir şekilde tespitinde kullanılabilir.

İnsan kontrolü: Bu insan gerçekten bu kişi mi sorusuna yanıt bulmak için kullanılabilir.

İnsan teyit etme: Bu insan veritabanına kayıtlı mı, değilse kayıt altına alma amacıyla kullanılabilir.

Belirtilen bu amaçlar için kullanılmakla birlikte üzerinde bazı değişiklikler yapılarak hareket algılama ve konum değişimlerinin tespiti için de kullanılabilir. Bu tez çalışması 6 bölümden oluşmakta olup aşağıda detayları verilmiştir.

İkinci bölümde siber güvenlik hakkında detaylı bilgi verilmiştir. Bu bölümde genel olarak siber güvenliğin ne olduğu, günümüzdeki ve gelecekteki güncel siber güvenlik konuları ve yaşanmış örnekler hakkında bilgiler verilmiştir.

Üçüncü bölümde siber güvenlik alt başlıklarından olan biyometrik sistemler hakkında detaylı bilgi verilmiştir. Bu bölümde genel olarak biyometrik sistemler, günümüzdeki ve gelecekteki biyometrik uygulamalar hakkında bilgiler verilmiştir.

Dördüncü bölümde yüz tanıma ile ilgili bilgiler verilmiştir. Ayrıca SIFT ve özyüz yönteminden kısaca bahsedilmiştir. Yine bu bölümde yüz tanıma problemi için yapılmış olan çalışmalardan ve uygulanan metotlardan bahsedilmiştir.

Beşinci bölümde önerilen yüz tanıma sistemi ve sistemin çalışmasından bahsedilmiştir. Altıncı bölümde ise elde edilen sonuçlar ve çalışma ile ilgili öneriler yer almaktadır.

2. SİBER GÜVENLİK

Siber güvenlik kısaca elektrik, elektronik sistemler, internet ve bilgisayarlar güvenliği ile ilgili her şey olarak tanımlanabilir. Örneğin iletişim sistemleri, taşıma sistemleri, alışveriş, ilaç sanayi siber güvenliğin önemli olduğu sektörlerden belli başlıca olanlarıdır. Siber güvenlik bilginin her türlü atağa ve tehdide karşı genel olarak korunmasını içerir. Başka bir tanım olarak siber güvenlik: kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır[1].

Yaşadığımız yüzyılda siber âlemde devletler ciddi çalışmalar ve yatırımlar yapmaktadırlar. Bu yatırımlar birçok alanda olmakla birlikte kritik altyapının olduğu alanlarda daha da ön plana çıkmaktadır. Ama devletler siber terörizm konusunda yeteri derecede önem göstermemektedir. Bu durum da tartışmalarda yer alan 2 karşıt görüşle ifade edilebilir. İlk görüşe göre siber terörizm kimseye zarar vermeyen bir mittir [2]. Diğer görüş ise sanal ortamda yapılan eylem ve atakların gerçek bir tehdit olduğu görüşündedirler [3]. Desouza ve Hensgen (2003) göre ise de siber terörizm : *"Bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması aracılığıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinliklerdir"*[3].

2.1. Riskler

Hayatımızda gittikçe yaygın bir şekilde kullanmış olduğumuz teknoloji hayatımıza birçok avantaj getirmiştir. Ancak bu gelişmelerin kötü niyetli bazı kişiler tarafından suistimal edilmesi, siber ortamın tehdit, saldırı ve zarar verme gibi amaçlarla kullanılması ile siber saldırılar dolayısıyla kişilerin ve ülkelerin gördüğü zararların büyük boyutlara ulaşması güvenlik anlayışında değişikliklere yol açmış ve bilgi güvenliği konusu bireylerin, kurumların, ülkelerin ve uluslararası kuruluşların en önemli gündem maddelerinden biri haline gelmiştir [4]. 31 Aralık 2009 itibariyle

dünyada 1,8 milyar internet kullanıcısı bulunmaktadır[5]. Türkiye'deki internet kullanıcı sayısı da her geçen gün artmış ve 2009 yılı itibariyle yaklaşık 26,5 milyona ulaşmıştır[6]. Tüm dünyada günlük iletilen e-posta sayısı yaklaşık 250 milyardır [7]. 2009 yılı itibariyle yaklaşık 25 milyarı aşkın internet sayfası bulunmaktadır [8]. Siber uzayda bazıları hususlar diğerlerinden daha tehlikeli olmakla birlikte birçok risk bulunmaktadır. Bunlar içinde belli başlı olanlar sisteme zarar veren ve bilgileri silen veya değiştiren veya sistemi çalışamaz hale getiren virüsler, bilgisayarına atak yaparak gizli bilgilerini ele geçiren saldırılar ön plana çıkmaktadır. Bu örnekler gibi milyonlarca sisteme ve bilgiye her türlü zarar verecek çok farklı çeşitte ve milyonlarca zararlı yazılım vardır. Maalesef tüm bunlara rağmen %100 güvenlik sağlanamamakla birlikte bazı alınacak önlemler ile bu riskler kaynaklanacak zararlar minimize edilebilir. Bu önlemler ve genel alınması gereken kurallar siber güvenlik standartları içinde belirtilmiştir. Belli başlı ve son yıllarda ortaya çıkan terminolojiye yerleşmiş ifadelerden siber terör konusuna bakacak olursak; Siber Terörizm konusunun ulusal ve uluslar arası ölçekte birçok alanda yer aldığı görülmektedir. Birçok yöntem ve araç olmakla birlikte virüsler, DoS saldırıları siber terörizmin belli başlı sıradan araçlardır.

Siber terörizmde yöntem ve araçlar aynı bıçak örneğinde olduğu gibi kullanım amacına göre yemek yapmak için birşeyler de kesilebilir, insan da öldürülebilir. Velasıl Desouza ve Hensgen'e göre gerçekte önemli olan; alet değil, onu kullanan insanların amaç ya da hedefleridir. Günümüz dünyasında bilişim sistemlerinin kullanılmadığı alan hemen hemen yok gibidir. Bu durum insanların hayatını kolaylaştırsa da bu alanlara yönelik sofistike atak ve yöntemler gitgide artmaktadır. Pollitt'in deyimiyle ,"Amerika, tamamen bilgisayarlara bağımlıdır. Bu yüzden artan bir şekilde risk altındadır" ifadesi aslında dünyada ki tüm ülkeler için aynı durumu ifade etmektedir.

2.2. Siber Terörizm

Siber terörizmin net bir tanımını yapmak zor olsa da, birçok araştırmacı gelişen şartlar ve konunun uzmanları siber saldırı türleri sınıflandırma amaçlı değişik yaklaşımlar göstermişlerdir. Bu siber ataklara bakacak olursak ilki basit ve

kurgulanmamış ataklardır. Çoğunlukla şahsi zevk ve çıkar için veya sadece yapabildiğini göstermek için yapılan atak türleri olan virüs, trojen vb. kullanılarak yapılan ataklar bu sınıftadırlar. Diğer bir sınıf da birçok bilişim alt yapısını yada sistemini hedef alan planlanmış ataklardır. Son olarak da sofistike ama iyi koordine edilmiş ataklardır. Bu saldırılar çok iyi planlanmış, koordine edilmiş ve üstün bir akıl ürünü özelliklerini içerir. Naval Postgraduate'de yer alan araştırmacılar çalışması sonucunda üst seviyede bir saldırı konunun uzmanı bir grup insanın yıllarca çalışması sonucu meydana gelebileceği yönündedir. Çünkü bu tip saldırılar her şeyi ile her yönden müthiş bir analiz ve plan ürünü olabilmesi için üzerinde ciddi emek sarf edilmelidir. Hatta en üst seviyede bir saldırı için ise daha çok yıl üzerinde çalışmak ve planlama yapmak gerektiği düşünülmektedir. Siber uzayda artan tehditlere karşı Avrupa Komisyonu da siber güvenliğe katkı yapacak değişik projeler üzerinde çalışmaktadır. Kurumsal olarak kullanılabilecek düzeyde toplumun önüne getirilen projeler bu günde tanıtılmakta ve uygulamaya konmaktadır [9].

Desouza ve Hensgen, siber terörizm kavramını "geleneksel" ve "nadir" saldırılar olarak nitelendirmektedirler. Bu kişiler saldırılardan geleneksel olanlar açık, nadir olanlar kapalı yada örtülü saldırı olarak nitelendirmektedirler. Keza ikisine göre geleneksel ataklar zararlı yazılım olarak nitelendirdiğimiz trojen, virüs, truva atı vb. yazılımlar ile yapılan saldırılar olarak görmektedirler. Mesela günümüzde özel yada kamu birçok sektörü ve siteyi etkileyen DDoS saldırıları da bu tür geleneksel ataklardandır. Ayriyeten yine ILOVEYOU, Melissa tarzı birçok virüs de binlerce insanı ve sistemi etkileyerek milyonlarca dolar maddi kayba yol açmışlardır. Siber terörizmin başka bir türü olan nadir saldırılar da terörist grupların kendi aralarındaki iletişime yardımcı olmak için elektronik çıkışlar değerlendirilmektedir. Mesela sanal alemde yer alan birçok insan için sıradan olan mesajlar bir takım terörist gruplar için haberleşme yol ve yöntemi olabilir ki keza günümüz de birçok terör örgütü bu yöntemi kullanmaktadır. Bu durum bilginin bilgi içinde gizlendiği, steganografi gibi teknikler kullanarak gerçekleştirilmektedir [10]. Şu da bir gerçektir ki bilgi ve bilişim teknolojileri hayatımızın her alanında kendine yer edinmiştir. Keza öyle iş, ev veya hayatımızın başka bir alanında günlük hayatımızda en sık kullandığımız ve yaptığımız işler arasına girmiştir. Tabi her ne kadar bu kadar hayatımızın içinde

olması hayatımızı kolaylaştırmasından kaynaklansa da yine bu sistemlerin hiçbir zaman tam güvenli olmadığı ve her zaman insanlar için çeşitli güvenlik riskleri taşıdığı aklımızdan çıkarmamakta fayda vardır. Özellikle çocuk ve gençlerimizi daha bilinçli hale getirmek için değişik faaliyetler yapılmaktadır. Bu kapsamda Birleşmiş Milletlere bağlı ilgili kurum tarafından çocukların çevrimiçi ortamlarda korunması ana tema olarak benimsenmiş ve bu çerçevede Child Online Protection adlı Çocukların Çevrimiçi Korunması etkinliği başlatılmıştır [11]. Ayrıca Türkiye'de Bilgi Teknolojileri ve İletişim Kurumuna bağlı Telekomünikasyon İletişim Başkanlığı tarafından çocukların interneti güvenli ve bilinçli kullanmalarına yönelik bir kitapçık hazırlanmıştır. Bu kitapçık toplam 12 milyon adet basılmış ve tüm ilköğretim öğrenci ve öğretmenlerine dağıtılmıştır [12].

Günümüz dünyası bilgi ve bilişim teknolojilerinin getirmiş olduğu üst seviyede imkanlar ile hayatımızın olmazsa olmazı haline gelmişlerdir. Teknolojideki gelişmeler, kamu sektöründen özel sektöre kadar hayatın her alanında ve her safhasında yer almış ve yeni bir anlayış, tarz, yöntemler getirmiştir. Artık teknoloji hayatımızın olmazsa olmazı haline gelmiştir. Bu kadar teknolojinin geliştiği ve hızla değiştiği çağımızda bu değişime ve gelişime de ayak uydurmamız kaçınılmaz bir hal almıştır. Ayrıca günümüz dünyasında siber alemde birçok farklı yöntem ve araçla değişik suçlar işlenir hale gelmiştir. Bu durum öyle bir hal almıştır ki sürekli yeni yöntemlerle suç işlenir hale gelmiştir. Çünkü gelişen teknoloji paralelinde işlenen suç türleri ve yöntemleri de gelişmiştir ve gelişen teknoloji paralelinde de artacaktır. Tüm bunlarda gösteriyor ki; siber güvenliğin sağlanması kişisel verilerin ve mahremiyetin korunmasında, şebekelerin güvenliğinin ve güvenilirliğinin sağlanmasında ve siber suçlarla mücadelede önemli bir unsurdur [13].

Siber güvenlik kapsamında bilişim suçlarıyla ilintili olarak birçok suç ve tanım söz konusu olmaktadır; bilişim suçları, sanal suçlar, siber suçlar, bilgisayar suçları. Farklı ülkelerde ise; IT Crimes ,Computer Crimes, Cyber Crimes, Crimes of Network gibi birçok ifade söz konusudur. Aslında bu kadar farklı isimlendirmenin olması biraz bu suç türlerinin işleme biçimi ve yöntemi ile ilgilidir. Keza bu suçlar bir ağ, elektrik şebekesi, sanal alem vb. kullanılarak da işlenebilmektedir. Tüm yöntem ve araçlar paralelinde birçok terim adlandırma söz konusu olmaktadır. Fakat bilişim kelimesi

ülkemizde bilgisayar, bilgi ve iletişim teknolojilerinin hepsini kapsayacak şekilde kullanıldığından dolayı bilişim suçları olarak tanımlanmıştır. Kısacası bu tür teknolojiler kullanılarak işlenen suçlar da bilişim suçu olarak nitelendirilmektedir.

Değişik adlandırması olan bilişim yoluyla işlenen suçların iyi bir tanımlaması ve gruplandırması olursa eğer o zaman daha iyi bir sistematik çalışma olması söz konusu olacak ve her türlü suç türü daha iyi anlaşılmış olacaktır. Tabi bilişim suçlarını sınıflandırırken yada tanımlama yaparken en önemli husus suçun işleniş amacı ve hedefidir. İşlenen suçların en büyük karakteristiği nasıl bir amaca hizmet ettiği çok önemlidir. Keza bu suçların işlenmesinin her zaman yegane bir amacı olur ve bu amaç yada amaçlara göre suç işlenir. Mesela bir bilişim sisteme girmenin birçok değişik yöntemi vardır; malware olarak nitelediğimiz : truva atı, back door, shell script, virüs bunların belli başlıcalarıdır. Fakat önemli olan daha önce belirttiğimiz gibi suçun işleniş hedefidir.

Peki, günümüz siber dünyasında bilişim suç türleri nelerdir, hangi sınıflarda bunları değerlendirebiliriz. Bu bağlamda yaygın olarak işlenen bilgisayar sistemlerine ve servislerine yetkisiz erişim en başlıca işlenen suçlardandır. Anayasamız başta olmak üzere birçok kanunda güvence altına alınan özel hayatın gizliliği konusunda teknolojinin gelişmesi paralelinde birçok yasadışı dinlemenin yapıldığıyla ilgili haberlerle günümüz dünyasında sıklıkla karşımıza çıkmaktadır. Hızlı ve etkin bir iletişim ve erişim imkanı veren bilişim sistemleri nedeniyle hayatımızın her alanında ve her konuda kullanılmaktadır. Ve kişisel verimiz bu ortamlarda tutmaktayız. Bunların yanında başta kamu olmak üzere özel sektördeki tüm firmalar kendileri ile ilgili birçok konudaki bilgiyi yine bu mecralarda tutmaktadırlar. Tutulan bu bilgilere yine bilişim teknolojileri kullanılarak ulaşılmaktadır.

Ön planda gelen diğer suç türlerinden biri de bilişim sistemlerinin sabotaj yapılmasıdır. Sabotaj genelde 2 şekilde meydana gelmektedir. Genelde sabotaj yapılan bilişim sistemine girilip verilerin silinmesi veya değiştirilmesi şeklinde olmaktadır. Diğer bir yöntem de hedef bilişim sistemine fiziksel zarar verme yada fizikse erişim sağlayarak zarar verme şeklinde meydana gelmektedir. Tabi bu

yöntemde amaç mala zarar vermek değil içindeki bilgileri yok etmektir. Çünkü maddi zarardan ziyade bilgi kaybı daha önemlidir. Bilgi güçtür.

Yine yaygın olarak karşılaştığımız diğer bir suç türü de klasik anlamda işlenen dolandırıcılık suçunun bilişim teknolojileri kullanılması vasıtasıyla yapılıyor olmasıdır. Bu tür dolandırıcılık genelde insanların bankacılık bilgilerinin ele geçirilmesi yada değişik senaryolar ile kandırılıp paralarının havale yada eft yapmasını sağlamak suretiyle meydana geldiğini görmekteyiz. Tabi bir de finansal bilgilerin yer aldığı sistemler üzerinde değişiklikler yapmak suretiyle para transferi yaparak gerçekleştirilen dolandırıcılık türü ile de karşılaşmaktayız.

Sahtecilik suçu da yine bilişim teknolojileri kullanılarak yapılan suç türlerinden biridir. Bu suç türü genelde bilişim sistemleri kullanarak değerli bir malın sahtesinin yapılması şekilde olmaktadır. Ama burada bilişim suçu olması için bilişim teknolojileri kullanılarak yapılıyor olmasıdır. Ayrıca bu suç türünde bu suç unsuru ürünlerin nasıl oluşturulduğu konusu teknik olarak iyi incelenmelidir. Özetle bilinen klasik anlamdaki sahtecilik suçu ile bilişim teknolojileri suçu arasındaki ince çizgiyi iyi yakalamak gerekir.

Tüm dünyada olduğu gibi Türkiye de yaygın bir şekilde kullanılan korsan program konusu da diğer bilişim suç türlerinden birisidir. Keza her program bir emeğin çalışmanın ürünü olması hasabiyle fikir ve sanat eseri kanunu kapsamına girmektedir. Bu nedenle bu yazılımların bir lisans yada telif ücreti karşılığında kullanılması gerekmektedir. Bilişim sistemleri yazılımları genelde tek kullanıcı lisanslı olmaktadır ve sadece bir kişi tarafından kullanılması gerektiği belirtilmektedir. Fakat bu duruma genelde riayet edilmeyerek izinsiz bir şekilde kopyaların dağıtımı söz konusu olmaktadır. Lisansız yazılım kullanım konusunda birçok firmanın yapmış olduğu araştırma sonucunda Türkiye'de lisanssız yazılım kullanımının % 80'ler seviyesinde olduğu gözlemlenmiştir. Bu durumda ülkemizde korsan yazılım kullanımın ne kadar yaygın olduğunu göstermektedir.

Özellikle yasadışı örgütler ve radikal grupların sıklıkla başvurduğu yöntemlerden olan yasadışı yayınlar önemli ve yaygın bir suç türlerinden biridir. Bu tip durumlar genelde 3 surette yapılmaktadır. Bunlardan ilki vatanın bütünlüğüne karşı yapılan

bölücü yayınlardır. Genelde terör örgütlerin kendi hedef ve ideolojileri çerçevesinde gerçekleştirdikleri içerikleri içeren web siteleri vasıtasıyla olmaktadır. Bu durum onların milyonlarca insan ulaşmasını sağlamaktadır. Diğer bir konuda toplum ve aile ahlakını hedef alan ve insanları yozlaştıran müstehcen ve cinsel içerikli internet sitelerinin yer aldığı yayınlardır. Bu konu diğer ülkelerde genelde çocuk pornosuna yoğunlaşma şeklinde meydana gelmektedir. Türkiye de ise pornografik yayınların her türlüsüne karşı mücadele söz konusudur. Toplumun temeline bir dinamit gibi tesir eden bu yayınların sosyal hayata olumsuz etkisi yadsınamaz bir gerçektir. En son yayın türü de genelde özel, kamu tüzel yada gerçek kişilere karşı yapılan hakaret içeren yayınlardır. Genel şahsi meselelerden kaynaklanan bu tür durumlar insanlar tarafından ciddi problemlere neden olmakta ve olumsuz sonuçları olmaktadır. Netice birçok suç türü olmakla birlikte buraya kadar bahsedilenler belli başlıca olanlardır. Bahsetmiş olduğumuz suç türleri yanında birçok farklı suç türü daha sayılabilir. Bu türler zaman geçtikçe artmaktadır. Öyle ki gelecekte herhangi bir sınıfa tabi tutamayacağımız suç türleri de çıkacaktır. Eğer bir sistemde güvenlik sorunu varsa, önemli dosyaların yedeği alındıktan sonra, işletim sisteminin yeniden kurulup güvenlik önlemlerinin alınması ya da güvenlik konusunda hizmet veren bir firmadan teknik destek alınması ve internetten bir programla çözmeye çalışarak yeni bir ajan program yüklemekten kaçınılması yerinde olacaktır [14].

Toplumların bilgi ve iletişim teknolojileriyle (BİT) değişime uğraması sonrası, BİT güvenliği birçok hükümetin politika önceliği haline gelmiştir. Bu kritik altyapıların korunması üzerine odaklanılması ile siber güvenlik stratejilerinin benimsenmesini yansıtmaktadır. Hükümetler, suçluları adalete teslim etmek için ve siber suçlara karşı insanları ve onların haklarını korumak için pozitif yükümlülüğe sahiptir. Bu nedenle hükümetler, siber güvenlik stratejileri ya da politikaları çerçevesinde siber suç stratejilerinin veya siber suç bileşenlerini geliştirme hazırlığını düşünmelidir.

İlgili makamlar ilerleyen bölümlerdeki eylemleri dikkate almalıdır. Siber suç politika veya stratejilerin benimsenmelidir. Bilgisayara karşı ve bilgisayar aracılığıyla işlenen suçların yanı sıra elektronik delil içeren herhangi bir suça karşı etkin bir ceza adaleti müdahalesinin sağlanması ile siber suç politika ve stratejilerin benimsenmelidir. Siber suç politika veya stratejilerinin temel unsurları; önleyici tedbirler, mevzuat,

özel kolluk birimleri ve özel savcılık hizmetleri, kurumlar arası işbirliği, kolluk ve adli personel eğitimi, kamu/özel sektör işbirliği, etkili uluslararası işbirliği, kara para aklamanın ve dolandırıcılığın önlenmesi için mali soruşturma ve cinsel şiddete karşı çocukların korunması olarak düşünülmelidir. Siber suçlara karşı önlemler alırken, insan hakları ve hukukun üstünlüğü gereksinimleri karşılandığından emin olunmalıdır. Siber suçların raporlanması üzerine kamu için online platformlar oluşturulmalıdır. Bu durum siber suç tehditlerinin ve eğilimlerinin daha iyi anlaşılmasını sağlamalı ve ceza adalet eylemlerini kolaylaştırmalıdır.

Herşeyin başı eğitim olduğu gibi bu konularda farkındalık oluşturmalı ve her düzeyde önleyici tedbirler teşvik edilmelidir. Özellikle kolluk birimleri ve internet servis sağlayıcıları arasında olmak üzere kamu/özel sektör işbirliği konusunda girişimde bulunulmalıdır. Mümkün olan en geniş ölçüde uluslararası işbirliği üzerine girişimde bulunulmalıdır. Bu, özellikle Budapeşte Siber Suç Sözleşmesi dahil mevcut ikili, çok taraflı ve bölgesel anlaşmalardan tam olarak yararlanılmasını içermektedir. Adli yardımlaşmayı hızlandırmak için önlemler ve eğitimler uygulanmalıdır. Hükümetler Siber Suç Sözleşmesi Komitesi (T-CY) çalışmalarına aktif bir şekilde katılmalı ve Avrupa Siber Suç Merkezi (EC3) ve Avrupa Birliği'nin diğer girişimleriyle işbirliği için girişimlerde bulunmalıdır. Düzenli olarak siber suçlara karşı ceza adaleti müdahalesinin etkinliğini değerlendirmek ve istatistikleri sağlamalıdır. Bu tür analizler ceza adalet eylem performansını artırmak için kaynakların verimli bir şekilde belirlenmesine ve tahsis edilmesine yardımcı olacaktır.

Globalleşen dünyamızda teknolojinin gelişmesi beraberinde bu mecralara yönelik tehdit ve risklerin artmasını da sağlamıştır ve artmaya devam edecektir. Tabi bu tür mecraların birçok açıdan güvenliğini sağlayacak değişik yöntem ve araçlar olmakla birlikte özellikle fiziksel güvenliğin ön plana çıktığı yerlerde biyometrik uygulamalar son yıllarda geniş bir şekilde kullanılmaktadır. Peki nedir biyometrik sistemler? Tam ve kesin bir tanım olmamakla birlikte; biyometrik, insanlara özgü eşsiz özelliklerin kullanılarak kimlik tespiti başta olmak üzere birçok alanda kullanılan teknolojik bir yaklaşımdır denebilir. Tabi bu teknoloji ile birçok alanda özellikle insan kimlik tespiti, yetkilendirme, kontrollü giriş çıkış ortamlarında sahtekarlık ve dolandırıcılık

ihtimalleri kullanılarak fiziksel güvenlik başta olmak üzere birçok açıdan kullanımı söz konusudur. Yaşadığımız yüzyılda birçok farklı türü olan bu yöntem kendi başına başlıca bir uzmanlık alanı oluşturmuş, bir iş ve endüstri olmuştur.

3. BİYOMETRİK SİSTEMLER

Biyometrinin birçok tanımı olmakla birlikte bilişim sistemleri kullanarak insana özgü ve her insandan insana değişen eşsiz özellikleri kullanarak tanımayı sağlayan sistemler olarak ifade edilebilir. Bu sistemler sadece bireye özgü tıpkı bir kimlik numarası gibi başka bir bireyde olmayan eşsiz özellikleri tanıma mantalitesi ile çalışan bir yapıdır. Bu yöntemde parmak izi, el ve yüz şekilleri, ses ve retina gibi faktörlerin tanınması içerilir. Kimlik doğrulamanın bir türü olan sahiplik temelli kimliklendirmede; kullanıcılar kendileri ile eşleşen bir objeye sahiptirler. Bu obje genelde manyetik kart, rozet veya anahtardır [15]. Aslında birçok biyometrik yöntem bir birine benzemektedir. İlk olarak eşsiz karakteristik özellikler elde edilir ve bunlar digital hale getirilip bir veritabanında tutulur. Tanıma sürecinde ise tanınmak istenen kişinin özellikleri yine bu veritabanında yer alan verilerle değişik yöntemlerle kıyaslanarak sonuca gidilmektedir. Bu sistemlerin en güzel yanlarından biri hızlı sonuç alabilmektir. Keza bu hız kısa sürede sonuca varmamızı sağlayarak, tanıma işlemini yapmamızı sağlar. Güvenlik noktasında en az risk ve hata payı ile bu sistemler kart, şifre veya pin gibi yöntemlere göre tercih edilmesinin en önemli faktörü kişinin herhangi bir kart taşıma gereği olmaması ve şifre ezberleme ihtiyacı olmasıdır. Zaten kişi kendisi ile birlikte tekil ve kendine münhasır özelliklerini taşımaktadır. Zaten biyometrik temelli kimliklendirme sistemlerinde kullanıcı sisteme kendisine ait olan ve üzerinde her daim taşıdığı parmakizi, iris, ses, el geometrisi, yüz gibi bir fizyolojik özelliğini veya imza atış, yürüyüş gibi bir davranışsal özelliğini kullanarak giriş yapar [16]. Bu kadar kolay hızlı ve güvenli sonuç elde etmemizi sağlayan bu sistem sayesinde birçok işlem rahatlıkla gerçekleştirilebilir. Bu sebepledir ki bu teknoloji günümüz dünyasında başlı başına bir sektör haline gelmiştir.

3.1. Biyometrik Sistemlerin Tarihi

Günümüz dünyasında yaygın kullanımı olan biyometri teknolojisinin mantalite olarak geçmişe dayanan bir mazisi vardır. Biyometrik sistemlerin basit halleri ile binlerce yıl önceden beri kullanıldığı bilinmektedir. Şöyle ki eski Mısır'da bu

teknoloji günlük hayatta yaygın olarak kullanılmıştır. Keza birçok antik mısır kaynağın da insanların kendilerine has özellikleri olan göz, saç, kaş vb. özellikler insanları nitelendirmede kullanıldığı belirlenmiştir. Birçok yöntem tarımsal süreçler başta olmak üzere hukuki süreçlerde kullanıldığı yine incelenen kaynaklarda yer aldığı görülmüştür. Yine geçen yüzyılda kriminalistlerin insan fiziksel özelliklerinin insanların kriminal eğilimler noktasında etkisi olup olmadığı konusundaki araştırmaları dikkat çekmiş, bu alana olan ilgili artırmıştır. Bu çalışmalar neticesinde birçok alet, edavat ve ölçüm ortaya çıkmıştır. Elde edilen ölçümlerin doğruluğu tartışılmakla birlikte özellikle parmak izi kolluk kuvvetleri tarafından kullanılmaya başlanmıştır ve giderek kabul görmüştür. Fakat bu durum her ne kadar tartışmalı bir konu olsa da kolluk kuvvetlerince yaygın kullanımı olmuş ve halen günümüz dünyasında da kullanılmaktadır. Diğer yandan biyometrik özelliklerin bilişim sistemler tarafından otomatize edilmiş olarak tanıma meselesi ticari ve askeri alanda yıllarca ciddi araştırma konusu haline gelmiştir. Bu alanda birçok proje yapılmıştır. Örneğin el geometrisi okuyucusu bunlardan bir tanesidir. Fazla başarılı olmamakla birlikte bu cihaz daha başka çalışmaların yapılması konusunda araştırmacıları cesaretlendirmiş ve yeni çalışmalara yitmiştir. Bu çalışmalar meyvesini vermiş değişik firmalar bu alanda değişik ürünler pazara sürmüş ve bu sektörün mihenk taşı haline gelmiştir. Diğer yandan parmak izi alanında da çalışmalar yapılmış ve ciddi anlamda ilerleme kaydedilmiştir. Biyometrik sistemlerin uygulama alanları günümüzde oldukça çeşitlidir. Özellikle havaalanları giriş ve çıkış işlemleri, kredi kartı uygulamaları, kriminal amaçlı teşhis ve tespit uygulamaları, sigorta şirketleri, ağ ve veri güvenliği, sosyal güvenlik, vergi süreçleri gibi kamu hizmetleri, e-ticaret, elektronik imza uygulamaları, internet bankacılığı, ATM'ler, çağrı merkezleri, personel takibi, hasta takibi bu gibi sosyal sistmlerde kullanılmalarının yanında artık, bilgisayarlar, pda olarak adlandırılan el bilgisayarları, cep telefonları ve ev kilit sistemlerinde de kullanılmaktadırlar [17].

İçinde bulunduğumuz yüzyıl başta olmak üzere özellikle doksanlardan itibaren yüz tanıma ve retina tanıma başta olmak üzere temassız tanıma teknolojileri ağırlık kazanmıştır. Son çeyrek yüzyıllık dönemde birçok üretici bu alanda uzmanlığını

artırmış ve daha iyi bir pazar payına sahip olmak için yeni teknolojiler ve metodolojiler üzerinde çalışmalar yürütmektedir.

3.2. Biyometrik Teknolojiler

Biyometrik sistemlerde özellikle kimlik doğrulamada birçok teknoloji kullanılmakla birlikte birkaç teknoloji aşağıda yer almaktadır. Günümüzdeki birçok biyometrik tanıma sistemi olmakla birlikte bunlardan başlıcaları aşağıda yer almaktadır. Fizyolojik özellikler: Parmak izi, Retina, DNA, Damar, Yüz, El Geometrisi, Ses, Yüz Termogramı, İris [18].

3.2.1. İris tanıma

İris tanıma temassız bir tanıma teknolojidir. Şöyle ki belli bir mesafe ortam koşullarında başarılı bir tanıma sağlayan bir teknolojidir. İris karakteristikleri kısa bir mesafeden tanınabilmektedir. İris bölümü gözün renkli kısmında yer almakta olup her insandan insana değişkenlik göstermektedir. Öyle ki aynı insan da bile iki gözün iris desenleri farklılık arz etmektedir. Yine diğer biyometrik teknolojilerde olduğu gibi bu teknolojide de iris deseni sayısal hale getirilip veri tabanında saklanmakta olup karşılaştırma yapılmaktadır. İris tanıma bu alandaki teknolojiler arasındaki en güvenli olanlardandır. Genel olarak parmakizi tanımaya benzetilen bu sistemin, parmakizine göre en önemli avantajı, parmak izi kullanılan biyometrik sistemlerde 60 veya 70 karşılaştırma noktası bulunurken, iris taramada karşılaştırma için yaklaşık 200 referans noktası kullanılmasıdır.

3.2.2. Parmak izi tanıma

Bu teknolojide birçok yöntem bulunmaktadır. Çünkü geçmişten gelen yaygın kullanımı söz konusudur. Bilinen yaklaşımlardan en bilineni kolluk kuvvetlerinin kullandığı yöntemlerdir. İlk kullanılmaya başlandığı yıllardan bu yana gerek yazılım gerekse donanım alanında parmak izi sistemlerinde önemli ilerlemeler kaydedilmiştir [19]. Bir otomatik parmakizi tanıma sisteminde (OPTS) parmakizi tanıma genellikle parmakizinde bulunan özellik noktalarının ve bunlara ait parametrelerin karşılaştırılması esasına dayanır [20]. Bu nedenledir ki diğer yöntemlere göre daha çok cihaz ve çeşidi söz konusudur. Fakat parmak izine dayanan tanımada daha etkili

yöntemler söz konusudur. Mesela daha hassas ölçüm sağlayan termal görüntüleme bunlardan biridir. Keza bu yöntemde parmak ısısından faydalanılmaktadır. Parmak bir sensörden geçirilir ve parmak ısısının izleri okunarak kayıt altına alıp kıyaslama yapılır. Başka yöntem de parmak izi elektrik akımından yararlanarak yapılan yöntemdir. Bu yöntem birçok alanda kullanılmaktadır. Öyle ki İngiltere 2007 yılından beri vize başvurularında, başvuran kişiden biyometrik veriler almaktadır [21].

3.2.3. Yüz tanıma

Yüz tanıma yıllardan beri üzerinde çalışılan ve daha iyi sonuçlar elde etmek için çaba sarf edilen bir tanıma sistemidir. İnsan tanıma o insana ait eşsiz özelliklerin kullanılarak otomatik olarak tanıma işlemidir. Yüz tanıma hakkında birçok yaklaşım olmakla birlikte yüz bölgesinin bir kısmı yada tamamı üzerinde değişik teknikler uygulayarak yapılabilmektedir. Bu teknikler değişmekle birlikte esas olan insan özgü yüz hat ve değerlerini tespit edip tanıma işlemini gerçekleştirme şeklinde yapılmaktadır. İleri teknoloji silahlarının yönetimi için, özellikle ABD'de sıkça kullanılan bu sistemler bunun dışında, caddelere yerleştirilen güvenlik kameraları ile caddelerin izlenmesi ve aranmakta olan bir suçlunun bu şekilde yakalanması gibi uygulamalarda da kendilerine yer edinmişlerdir. Özellikle son 10 yıldır uygulama alanlarının artması nedeniyle yüzlerin otomatik olarak tanınması popüler bir konu haline gelmiştir. Günümüzde yaygın kullanımı olmamakla birlikte ilerde gelişen teknoloji paralelinde daha yaygın kullanım alanı olacağını düşünmekteyim.

3.2.4. El geometrisi tanıma

Bu yöntem de her insana özgü olan el uzuv oranlarından yararlanarak yapılan tanımadır. Kişinin elinin veya kullanılan sisteme göre iki parmağının geometrik yapısı analiz edilir [22]. Tabi bu tanıma işlemi elin üç boyutlu bir görüntüsü elde edilerek gerçekleştirilir. Tanıma işleminde ise el bir tarayıcıdan geçirilerek üç boyutlu bir profili elde edilerek veritabanındaki diğer kayıtlar ile karşılaştırmak suretiyle gerçekleştirilmektedir. Bu teknolojinin kullanımı ve uygulanması diğer teknolojilere göre daha rahattır. Ayrıca diğerleri entegrasyonu daha kolay olması sebebiyledir ki daha yaygın bir kullanım alanı bazı alanlarda oluşmuştur.

3.2.5. Ses tanıma

Hayatımızda sesin ne kadar kullanıldığı konusu düşünüldüğünde etkili bir tanıma yöntemi olarak düşünülse de seslerin kolay taklit edilebilme özelliği nedeniyle güvenliği zayıftır. Fakat insan sesi birçok yönden spesifik özellikler içermesi nedeniyle ayırt edici bir yönü bulunmaktadır. Bu alanda birçok yöntem olmakla birlikte ses frekansları küçük birimler olarak sınıflandırılıp karakterize edilerek veritabanına kaydedilir.

3.2.6. Retina tanıma

Retina tanıma gözün kendine has optik yapısı itibariyle bu yapının taranması mantığı ile çalışsa da kullanıcının belirli bir noktaya bakma mecburiyeti nedeniyle kullanımı zordur. Güvenlik seviyesi iyi olmasına rağmen kullanım zorluğu nedeniyle fazla yaygınlaşmamıştır.

3.3. Gelecekteki Biyometri Uygulamaları

Yaşadığımız yüzyılda birçok değişik biyometrik güvenlik sistemleri kullanılmakla birlikte bunlardan birkaçı aşağıda belirtilmiştir. Fakat gelişen teknoloji ve yapılan araştırmalar sonucunda gelecekte daha yaygın bir kullanım alanı olacağını öngörmekteyiz.

- Sanal bankacılıkta kullanıcı tanıma,
- Otomatik ödeme cihazlarında kullanıcı tanıma,
- İş yerinde çalışan insan tanımada,
- Hastanelerde hasta tanıma,
- Sigorta şirketlerinde kimlik tanıma,
- Havaalanlarındaki giriş ve çıkış işlemleri,
- Kredi kartı uygulamaları,
- Masaüstü ve dizüstü bilgisayarların güvenliği,
- Kurumsal ağların güvenliği,
- Kiosklarda kullanıcı tanıma,
- SSK,vergi süreçleri gibi kamu hizmetleri,

- Evlere,ofislere ve binalara erişim,
- E-ticaret işlemleri,

Günümüz dünyasında ATM kullanımında özellikle kart sahtekarlığının önüne geçmek için biyometrik yöntemler test edilmektedir. Ancak bu problemin sadece biyometrik yöntemler ile çözülmesi zor gözükmektedir. Keza konunun birçok yönü vardır. Hırsıza kapıyı kapatsan pencereden girer, pencereyi kapatsan bacadan girer misali bir durum vardır.

Turizm sektöründe yaygın olarak kullanımı olacağı görüşü git gide yaygınlaşmakla özellikle uçak bileti, otel odası ve araç kiralama başta olmak üzere birçok işlemi insanların akıllı kartlar ile yapabileceği öngörülmektedir. Çözüm teknik anlamda uygulanabilir gözükse de olayın ticari ve politik boyutu nedeniyle uygulanmamaktadır. Bu konu ile ilgili birçok soru işaretleri olmakla birlikte özellikle bu kartların kimler tarafından ve nasıl yönetileceği konusu ciddi bir problem olarak karşımızda durmaktadır. Konunun uzmanları pilot bir uygulama ile bu sisteme geçilebileceğini düşünmektedirler.

İnternet işlemlerinde biyometrik sistemlerin iyi bir şekilde kullanımın sağlanabileceği diğer konuşulan konulardandır. Bir biyometrik okuyucunun bilgisayara takılarak rahatlıkla kullanabilecek ve cihaz maliyetini düşürecek yaklaşımlar söz konusu olmakla birlikte değişik sorunlar söz konusudur. Fakat biyometrik sisteminin karta monte edilerek özellikle kredi kartlarına monte edilmesi ve kullanıcıya verilmesi bazı kolaylıklar sağlayacaktır.

Telefon sistemleri de yine biyometrik sistemlerin kullanım alanı oluşacak alanlardan biridir. Keza bu sistemlerin herhangi bir sürecinde yer alan birçok kişiye değişik biyometrik çözümlerin sunulması iş süreçlerin güvenliğinin sağlanması ve performans artışının sağlanması noktasında ciddi katkı sağlayacaktır. Diğer yandan biyometrik sistemlerin özellikle otomatik geçişlerde kullanılması iyi bir alternetif oluşturacak olup, özellikle bu konu ile ilgili ciddi çalışmalar söz konusudur. Bir diğer yöntem de ses tanıma değişik zorlukları ve sakıncaları olmakla birlikte kullanabilecek yöntemlerden birisidir. Telefon cihazlarının ve müşterilerin değişiklik

arz etmesi daha da önemlisi insan seslerinin taklit edilebilmesi ses tanımanı güvenlik seviyesini düşürmektedir. Fakat dünyada birçok kurum ve kuruluş başta fiziksel güvenlik olmak üzere birçok alanda biyometrik sistemleri kullanmaktadır. Gelecek yıllarda giderek artan teknoloji ve yeni yöntemler ile biyometrik sistemlerin güvenlik seviyesi artacaktır. Bunun paralelinde bu sistemlerin kullanımı artacaktır.

Biyometrik sistemlerde böyle bir durum söz konusu değildir ve kişinin kimliğini doğrulayabilmek için kendisinden başka herhangi bir bilgiye, nesneye vs ihtiyacı yoktur. Biyometrik sistemlerin diğer sistemlere göre avantajları, dezavantajları, benzer ve farklı yönleri kısaca aşağıdaki gibi ifade edilir [23].

• Diğer kimlik doğrulama yöntemlerinde kullanılan veri her kullanıcı için kesinlikle farklı ve eşsiz iken biyometrik veriler farklı olmakla beraber benzerliklere sahip olabilir.

• Diğer yöntemlerde kullanılan veri, kullanıcı tarafından değiştirilebilir (sistem yöneticisinin isteği üzerine, güncelleme amacıyla veya başka herhangi bir sebepten ötürü). Buna karşın biyometrik veri kişinin istemesi ile değiştirebileceği bir veri değildir, ancak kaza, hastalık vs geçirilmesi durumunda değişir.

• Biyometrik sistemler genelde ek bir donanım, yazılım gerektirdiğinden ek bir maliyet getirir iken diğer yöntemler genelde kullanılan mevcut sistemlerle uyumludur.

4. YÜZ TANIMA

İnsan tanıma ve kimliklendirme günümüzün gelişen toplum ve teknolojisiyle önem kazanmış ve önemli bir bilgi sistemi haline gelmiştir. Beynin aşamalı öğrenme sistemi yapay sinir ağlarında da denenmiş, yüz tanıma ve dilin modellenmesinde başarıyla kullanılmıştır [24]. çalışmaları özetledikleri makalede araştırmacıları uyarıyorlar: "Yüz tanıma algoritmaları ve sistemleri tasarlayanlar psikofiziksel ve nörofizyolojik bulgulardan haberdar olmalı, ama sadece pratik anlamda işe yarayacak olanları modellerinde kullanmalıdırlar" [25]. Kişi tanıma; bir kişinin fiziksel karakteristikleri veya kişisel özellikleri kullanılarak otomatik olarak kimliğinin belirlenmesi veya doğrulanması işlemidir. Bu işlemin otomatik olması kullanıcının sisteme ya çok az müdahale etmesi ya da hiç müdahale etmemesi anlamına gelir, temel olarak o kişiye ait yüz, parmak izi, el geometrisi, iris, retina, dna ve ses ana başlıkları altında sayılan biyometrik özellikler kullanılarak yapılabilir. Biyolojik yüz tanıma sistemleriyle tutarlı olma iddiası taşıyan ilk yüz tanıma modeli Turk ve Pentland'ın özyüz (eigenface) modelidir [26]. Bir diğer biyolojik yaklaşım da elastik çizge (elastic graph) modelidir [27]. Bu modelde Gabor dalgacıkları ile yüzlerden öznitelikler çıkartılmak suretiyle tanıma yapılır. Ramasubramanian ve Venkatesh yüz imgelerine ayrık kosinüs değişimi (discrete cosine transform, DCT) uygulamışlardır [28]. Özelliklede biyometrik tabanlı kimliklendirme sivil toplumda veya yasal düzenleme bulunan alanlarda kullanılır. Ama yüz tanımada bu özniteliklerin ne şekilde dağıldığı, hangisinin altta, hangisinin üstte olduğu, yani özniteliklerin konfigürasyonu, özniteliklerin kendisinden daha önemli bir bilgidir [29]. İnsanın görsel olarak karşısındakini tanımada kullandığı en yaygın yöntem, yüz tanıma, günümüzde en çok kabul gören biyometrik tabanlı tanımlamadır. Bu nedenle yüz tanıma her dönemde güncelliğini korumuş ve üzerinde fazla sayıda çalışma yapılan bir konu olmuştur. Fakat Bir tarafta "Bu kadarcık yüz görerek yüzleri böylesine iyi tanımak mümkün değildir, yüz tanıma doğuştan var olan, kendine has bir sistem tarafından gerçekleştirilir" diyen bir grup var. Bu gruba göre yüz tanıma Jerry Fodor'un zihnin modülleri olarak adlandırdığı izole fonksiyonlardan biri [30]. Geçmişten günümüze insan yüz tanıma alanında ciddi gelişmeler olmuştur. Bu sebepledir ki özellikle fiziksel güvenliğin kontrolün olduğu havaalanlarında,

bankacılıkta, güvenlik kuvvetlerinin yapmış olduğu çalışmalarda kullanım alanı geniştir. Gelişen yöntem ve teknikler paralelinde diğer alanlarda da kullanım alanı yaygınlaşacaktır. Dahası ülkedeki birçok kamera vasıtasıyla otomatik yüz tanıma işlemi film karelerinden çıkıp gerçek dünyada da yaygın kullanımı olacaktır.

Gelişim perspektifinden bakılınca yüz tanıma aşama aşama öğrenilen, her aşamada bir önceki aşamada kullanılan gösterimlere yeni fonksiyonların ve gösterimlerin eklendiği karmaşık bir sistem gerektiren bir problemdir [31]. Yüz tanıma, tanımlanacak kişiye ait bir dijital fotoğrafa ihtiyaç duyduğu için diğer biyometrik tanıma sistemlerinde olduğu gibi çok karmaşık bir sistem gerektirir. Yüz tanıma sistemleri kullanıcının yalnızca güvenlik kamerasının önünden geçmesi ile teşhis edilmesini mümkün kılar. Örneğin yaygın olan parmak izi tanımada deneğin hassas bir şekilde alınmış parmak izi ya da iris tanıma için deneğin yüksek çözünürlüklü bir kamerada yakın mesafeden göz resimleri gerekir. Ayrıca diğer biyometrik tanımla sistemlerinin kişilik haklarını ihlal etmesi (parmak izi vs.) ve bazı biyometrik izlerin alınması kanunla saklı tutulmuş gerekli mahkeme kararı ve yasal zorunluluklar durumunda kayıtları alınabilmektedir. Bu sayılan sebepler dolayısıyla yüz biyometrisi çalışmaları daha bir önem kazanır.

4.1. Tanıma İçin Ölçekten Bağımsız Özellik Dönüşümü (SIFT)

Bir resimde yer alan özelliklerin çıkarılması örüntü tanımada kullanılan yöntemlerden birisidir. Özellikli noktalarda aranan nitelikler [32], aşağıdaki şekilde tanımlanabilir. Buna göre, özellikli bir nokta;

- Açık, belli, tercihen matematiksel olarak iyi tanımlanmış olmalıdır.

- Resim düzleminde iyi tanımlanmış konuma sahip olmalıdır.

- Bu noktanın etrafındaki resim yapısı bilgi içeriği yönünden zengin olmalıdır.

- Resimde oluşabilecek değişimlere (boyutsal, döngüsel, parlaklık, görünüş) karşı kararlı, başka bir deyişle yüksek tekrar edilebilirliğe sahip olmalıdır.

Literatürde var olan en önemli özellikli nokta bulan, nokta tanımlayıcıları; Moravec

operatörü [33], Harris Algılayıcısı [34], KLT dedektörü [35], ve SIFT dedektörüdür [36]. Bu çalışmada Ölçekten Bağımsız Özellik Dönüşümü (Scale Invariant Feature Transform - SIFT) algoritması kullanılarak yüz tanıma işlemi çeşitli yüz veritabanları üzerinde uygulanmıştır. SIFT yaklaşımı genel olarak basitliği ve hızı nedeniyle yaygın kullanılan bir metottur.

SIFT algoritmasını kullanan bir çalışma Luo, Yong Ma, Erine Takikawa, Shihong Lao, Masato Kawade ve Bao-Liang Lu tarafından yapılmıştır. Burada yüzlerde tanıma için k-means kümeleme algoritması kullanılmış ve özellik seçiminde de SIFT kullanılmıştır. Bu tezde Luo, Yong Ma, Erine Takikawa, Shihong Lao, Masato Kawade ve Bao-Liang Lu tarafından sunulana çalışmaya benzer bir şekilde SIFT algoritmasına dayalı bir yüz tanıma sistemi önerilmiştir.

Geliştirilen sistem birçok olumsuz etkiye rağmen yüzdeki değişmez sabit özellikleri tespit ederek çalışır. Tanıma sürecinde yeni bir görüntü geldiğinde, o görüntüye ait değişmez sabit özellikler tespit edilir. Sonra bu yüz görüntüsünün özellikleri Öklid uzaklığı kullanılarak en yakın komşuluk algoritması mantığı ile veritabanındaki yüzlerin özellikleri ile eşleştirilir. En uygun eşleşmenin aranan kişiye ait olması beklenir. Bu arada en düşük eğim hesapları yapılarak yanlış eşleşmeler elenmeye çalışılır.

Bu sistemde kullanılan SIFT yaklaşımı hız, basitlik ve yüz görüntüsündeki küçük değişikliklere dayanıklılık açısından diğer özellik çıkarma metotlarına göre avantajlara sahiptir.

4.1.1. Ölçekten bağımsız özellik dönüşümü (SIFT)

SIFT resimlerde yerel özellikleri tanımlamak ve tespit etmek amacıyla bilgisayarda görmede kullanılan bir yöntemdir. Bu yöntem ile ilgili ilk çalışma 1999 yılında David Lowe [23] tarafından yayınlanmıştır. Uygulama alanları genel olarak 3 boyutlu modelleme, nesne tanıma, hareket algılama, robotik gibi alanlar sayılabilir. Yöntem Birleşik Devletler lisanslı olup, sahibi British Columbia Üniversitesidir.

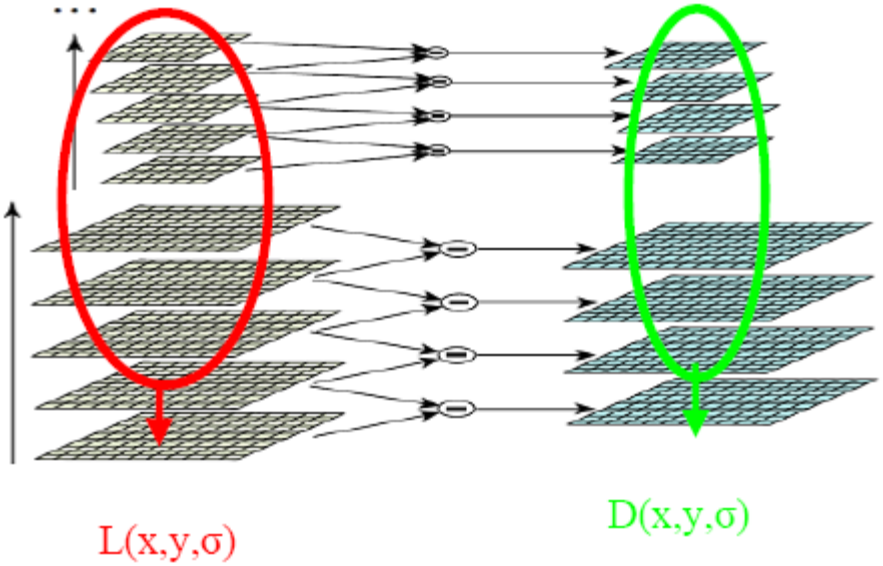
Herhangi bir nesnenin görüntüsünde o nesne ile ilgili tanımlayıcı olacak birçok özellik vardır. Bu özellikler o nesneden elde edilerek o nesne ile ilgili tanımlayıcı

özelliklere ulaşılabilir. Bu tanımlar bir eğitici resimden alınarak bir test resminde diğer nesnelerin yerinin belirlenmesinde ve nesnenin tanınmasında kullanılabilir. Eğitim resminden çıkarılan özelliklerin resim boyutunda, gürültüde ve yerel geometrik bozulmalardaki değişimlere dayanıklı olması iyi bir nesne tanıma için önemlidir.

Lowe'un metodu bu tür değişimlere genel olarak dayanıklıdır. SIFT yönteminde ilk olarak referans resimlerden özellikler elde edilir ve bir veritabanında saklanır. Yeni bir resimden elde edilen özellikler bu veritabanındaki özellikler ile eşleştirilir. En iyi eşleşme öklid uzaklığı en az olarak seçilir. Tüm bu testlerden geçen nesne eşleşmeleri ile yüksek bir oranda tanıma gerçekleştirilmesi hedeflenmiştir. Fakat uygulamada bazı özelliklerin yanlış eşleştiği yada çoklu eşleştiği görülmüştür. Burada yanlış ve çoklu eşleşmeleri elemek gerekmiştir. Böylece birçok ortamda ve koşulda çalışabilecek bir algoritma elde edilmeye çalışılmıştır. Bu bağlamda SIFT algoritmasının adımları takip eden kısımlarda genel olarak anlatılmıştır.

Ölçeksel uzaydaki minimum ve maksimum değerlerin elde edilmesi

Ölçeksel uzayda birçok faktörden etkilenmeyen sabit noktaların elde etmek için birçok farklı yöntem oluşturulup kullanılabileceği ön görülmektedir. Bu yöntemlerden biri de Gauss Farkları (Difference of Gaussians - DoG) yöntemidir. Koenderink (1984) ve Lindeberg (1994) çalışmalarından elde ettiği sonuçlara göre ölçeksel uzayın (Şekil 4.1) Gauss fonksiyonu ile elde edileceğini tespit etmişlerdir. SIFT algoritmasında DoG yöntemini kullanılması uygun görülmüştür.



Gauss filtresinden geçirilmiş resimler DoG resimleri

Şekil 4.1. Ölçeksel uzayın oluşumu [36]

İlk yapılan işlem ölçeksel uzay oluşturulmasıdır. Sonraki aşamada ise anahtar nokta olabilecek aday noktaların elde edilmesidir. Akabinde resmin ilk hali farklı standart sapmaya sahip Gauss filtreleriyle işleme tabi tutulur.

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2}$$

(5.1)

I: resimin ilk hali, G: değişen oranlara sahip Gauss fonksiyonu olmak üzere, ölçeksel uzay fonksiyonu aşağıda belirtildiği gibidir:

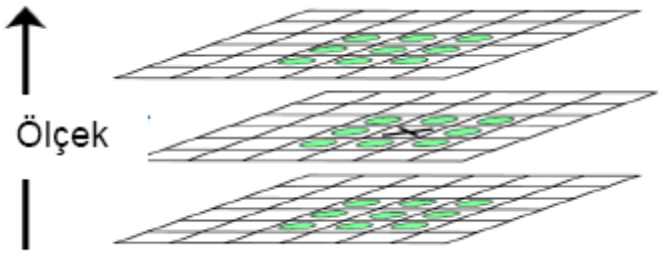
$$L(x, y, k\sigma) = G(x, y, k\sigma) * I(x, y) \quad (5.2)$$

Gauss fonksiyonu ifadesi olan D(x, y, σ), aralarında k kadar orantılı değer sahip Gauss filtreli 2 görüntü arasındaki farkın sonucunda elde edilmektedir.

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \quad (5.3)$$

Bu durum görüntüyü Gauss filtresiden geçirmekle Laplace dönüşüm fonksiyonu arasında önemli bir benzerliğin olduğunu göstermektedir. Bu çalışmada, 26 nokta

arasında bir noktanın komşularına nazaran (Şekil 4.2) minimum veya maksimum olup olmadığı denetlenmektedir.



Şekil 4.2. Uç noktaların bulunması [36]

Anahtar noktalarının yerlerinin tespit edilmesi

Önceki kısımda net olmamasına rağmen elde edilen birçok aday nokta söz konusudur. Bu bölümde net olmayan yani düşük değere sahip ve gürültüden etkilenen veya zayıf kalan noktaların elenmesi gerçekleştirilir. Bu eliminizasyon işlemi Gauss fonksiyonunun (D(x,y,σ)) anahtar aday noktaları esas olmak üzere ikinci dereceden Taylor serisi açılımı işlemine tabi tutularak aşağıdaki fonksiyon elde edilir: Kenar noktaların yeni yerleri,

$D(x) = D + \frac{1}{2}\frac{\partial D^T}{\partial x}x$ fonksiyonu ortaya çıkar.

Bu fonksiyonda Gauss fonksiyonlarından olan D(x) ve türevi, her kenar nokta için hesaplama yapılır ve |D(x)| < 0.02 durumunda eleminize edilir. Uçlarda elde edilen anahtar noktalar ise aşağıdaki ifadeye göre eliminizasyona tabi tutulur.

D : DoG fonksiyonu,

Hessian matrisi H= [Dxx, Dxy; Dyx, Dyy],

a: büyük değer, b: küçük değer,

r=a/b alırsak,

R= (r+1)2/r => SIFT için olması gereken ifadedir.

Döngüsel değişimlere nazaran sağlamlık elde edilmesi

Bu aşama objenin 2 boyutlu eksen tarafında hareket etmesine nazaran sağlamlık elde edilmesi açısından kritiktir. Bu kısımda tüm anahtar noktalar için ayrı ayrı bir veya daha çok döngüsel atama işlemi gerçekleştirilir. Önceki bölümlerde hesaplanan σ ölçeğindeki Gauss filtresine tabi tutulmuş görüntü olan L(x, y, σ) = G(x, y, σ) * I(x, y) fonksiyonu kullanarak gradyent büyüklük m(x,y) ve açı θ(x,y) hesaplanır :

$$m(x,y) = \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2} \tag{5.4}$$

$$\theta(x,y) = \tan^{-1} \frac{(L(x+1,y) - L(x-1,y))}{(L(x,y+1) - L(x,y-1))} \tag{5.5}$$

Yön ve büyüklük hesaplamaları Gauss filtrelerine tabi tutulmuş görüntüde elde edilen anahtar noktaların, çevresindeki her piksel için uygulanır. Anahtar noktaların çevresinde 10 derecelik yönü içeren 36lık döngüsel histogram meydana getirilir. Histograma ilave edilen tüm noktalar ayrı ayrı sahip olmuş olduğu gradyent büyüklükleri ile ağırlıklandırma işlemine tabi tutulur. Histogram içinde en değerli nokta yüzde seksen histogram içinde kalan noktadır. Halbuki söz konusu noktaların yalnızca yüzde onbeşi birden fazla döngüsel atama gerçekleştirilmesine rağmen bi önceki yapılan işlemde eşleşme durumlarındaki netliği ve stabiliteyi ciddi derecede artırmaktadır.

Anahtar noktalara sahip olduğu niteleyicilerinin elde edilmesi

Bu kısımda ışık, 3 boyutlu görüntü vb. değişikliklere karşı netlik ve stabilite kazandırma gerçekleştirilir. İlk olarak anahtar noktalar çevresinde gradyent büyüklük ve açı değerleri anahtar noktanın ölçeksel değeri kullanmak suretiyle nxn'lik bir bölümde örnekleme işlemi yapılır. Döngüsel stabiliteyi gerçekleştirmek amacıyla kilit nokta niteleyicinin yeri ve gradyent açı değerleri, kilit nokta açı değeri esas alınarak döndürme işlemine tabi tutulur. Bu kısımda gerçekleştirilenler, döngüsel stabilite elde etme işlemine benzerlik göstermektedir. 8x8 değerindeki vektörler, anahtar noktanın çevresinde yer alan nxn boyutundaki bir bölgenin içerisinde kalan

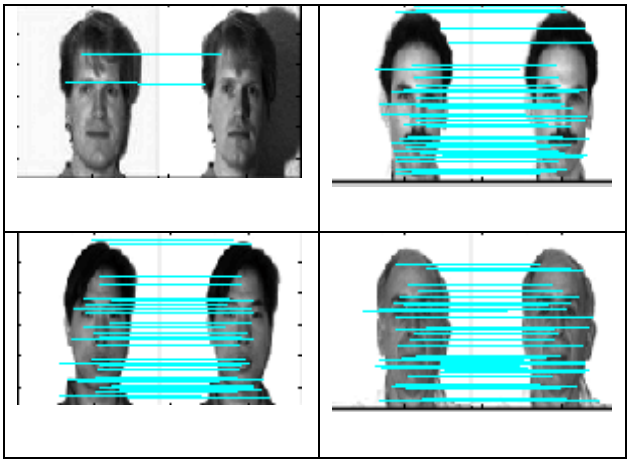
tüm noktalar için ayrı ayrı tanımlama işlemi yapılır. Bu durumda her bir anahtar noktayı nitelemek için oluşturulan vektör $n \times n \times r$ boyutunda olur.

4.1.2. Yapılan çalışmalar

SIFT algoritması ile yüz tanıma için birçok farklı yöntem denenmiştir. Bu yöntemler farklı veritabanları üzerinde test edilmiş ve sonuçları elde edilmiştir. Daha iyi bir tanıma için en uygun yöntem ve metodoloji arayışı ile yola çıkıp aşağıda belirtilen yöntemler denenmiştir.

Farklı yüz veritabanları için sift ile eşleştirme

Bu çalışmada farklı yüz veritabanlarında geliştirilen algoritma ile tanıma işlemi gerçekleştirilmiştir. Yale yüz veritabanı (Şekil 4.3) Hint (indian) yüz veritabanı, Japon kadın yüz veritabanı, AT&T yüz veritabanı kullanılan veritabanlarından başlıcalarıdır. Tanıma işleminde yöntemimiz SIFT algoritmasını tüm kişilerin ilk yüzlerini kendisi dahil diğer kişilerin ilk yüzleri ile karşılaştırarak en yüksek sayıda eşleşme oranı elde etmektir. Elde edilen en yüksek eşleşme doğru kişi mi değil mi kontrolünü yaparak başarı oranı elde edilmiştir. Kullanılacak yüz veritabanların dünyada kabul görmüş yüz veritabanlarından olmasına dikkat edilmiştir. Bu konuda iyi bir araştırma yapılarak kullanılacak veritabanları ve özellikleri incelenmiştir. Yale yüz veritabanı, Indian yüz veritabanı, Japon kadın yüz veritabanı, AT&T yüz veritabanı kullanılan veritabanlarından sadece birkaçıdır. Ayrıca çalışmamızda kendimizin oluşturduğu veritabanları da test amaçlı kullanılmıştır.



Şekil 4.3. Yale yüz veritabanında elde edilen en yüksek eşleşme sayılarına göre yüzler

Tablo 4.1. Yale yüz veritabanında elde edilen başarı oranları

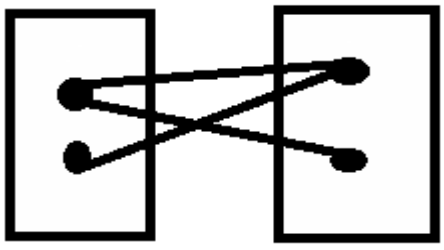
Veritabanı	**Kişi**	**Başarı Oranı**
Yale Yüz Veritabanı	1.	%98.13
	2.	%97.6
	3.	%97.6
	4.	%97.6
	5.	%97.6
	6.	%98.13
	7.	%97.6
	8.	%97.6
	9.	%97.6
	10.	%97.2
	11.	%97.6
	Ortalama	**%97.66**

Aynı yöntem Hint yüz veritabanı üzerinde de denenmiş elde edilen sonuçlar Şekil 4.4'de gösterilmektedir.

Şekil 4.4. Hint yüz veritabanında en yüksek eşleşme sayılarına göre yüzler

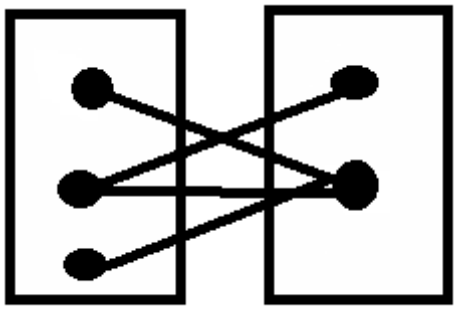
Tanıma başarı oranı artırma için yapılan çalışmalar

Farklı yüz veritabanları üzerinde yapılan çalışmalarda bazı eşleşmeleri çoklu ve yanlış eşleşme olduğu gözlemlenmiştir. Bu durumun önüne geçip daha doğru sonuçlar elde etmek ve tanıma başarı oranını artırmak için çoklu eşleşme durumlarında iki nokta arasındaki mesafeye ve aradaki açının kosinüsüne bakılmıştır. Eğer ki aradaki mesafe daha küçük ve eşleşen iki nokta arasındaki açının kosinüsü de daha büyükse o doğru eşleşme olarak ele alınmıştır. Geliştirilen algoritma öncelikle eşleşen noktalar için çoklu eşlem durumu olup olmadığı tespit eder ve indis vektöründe Şekil 4.5'de belirtilen çoklu eşleşen noktaları tutar.



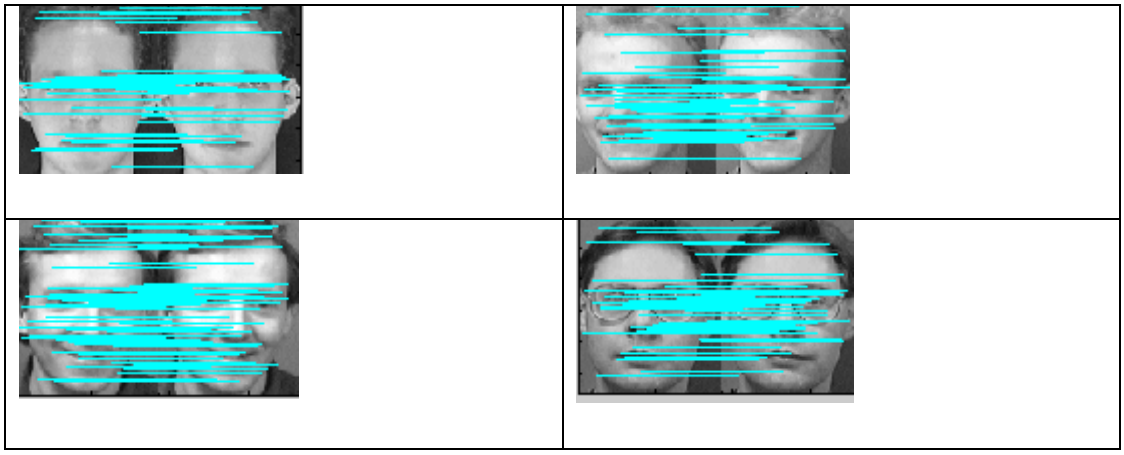
Şekil 4.5. İlk yüz resminden 2. yüz resmine çoklu eşleşme durumu

Algoritmanın diğer bir özelliği de Şekil 4.6'da ifade edildiği gibi 2. yüz resminden 1. yüz resmine çoklu eşleşme durumuna bakılarak eşleşen noktalar tespit ediliyor.



Şekil 4.6. İkinci yüz resminden 1. yüz resmine çoklu eşleşme durumu

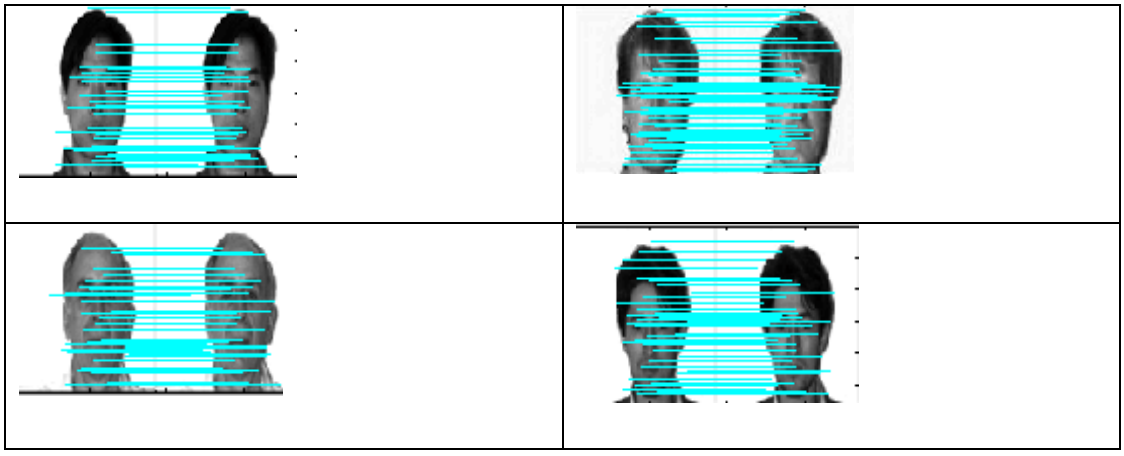
Ayrıca algoritmada tespit edilen çoklu eşleşme noktalarından doğru eşleşmeyi belirlemek için çoklu eşleşen noktaların birbirine olan mesafesine ve aralarındaki açının ters kosinüsüne bakılarak doğru eşleşme tespit edilmektedir. Hesaplanan değerlerden aradaki mesafenin ve açının küçük olanı olan eşleşme doğru eşleşme olarak kabul edilmektedir.



Şekil 4.7. AT&T yüz veritabanında çoklu eşleşmelerin eleminize edilmesi

Tablo 4.2. AT&T yüz veritabanında çoklu eşleşmelerin başarı oranları

	Yüzler	**SIFT 1. Yöntem**	**SIFT 2. Yöntem**
AT&T **Yüz Veritabanı**	1.	%100	%100
	2.	%99.6	%99.6
	3.	%99.65	%99.65
	4.	%99.25	%99.5
	5.	%99.25	%99.45
	6.	%99.5	%99.7
	7.	%98.95	%99.3
	8.	%99.45	%99.5
	9.	%99.4	%99.45
	10.	%99	%99.5
	Ortalama	**%99.405**	**%99.565**



Şekil 4.8. Yale yüz veritabanında çoklu eşleşmelerin eleminize edilmesi

Tablo 4.3. Yale yüz veritabanında çoklu eşleşmelerin başarı oranları

	Yüzler	**SIFT 1. Yöntem**	**SİFT 2. Yöntem**
Yale Yüz Veritabanı	1.	%98,13	%98.133
	2.	%97.6	%97.66
	3.	%97.6	%97.66
	4.	%97.6	%98.13
	5.	%97.6	%97.66
	6.	%98.13	%98.13
	7.	%97.6	%97.66
	8.	%97.6	%98.13
	9.	%97.6	%97.66
	10.	%97.2	%97.6
	11.	%97.6	%98.13
	Ortalama	**%97.66**	**%97.868**

Tablo 4.2 ve Tablo 4.3'de görüldüğü gibi çoklu eşleşme durumları tespit dilip bunlardan doğru olan eşleşmeler seçildiği takdirde başarı oranında bir artış olduğu gözlemlenmektedir.

Topluluk içinde yüz bulma ve tanıma

Farklı yüz veritabanları için elde edilen başarılı sonuçlardan sonra kalabalık resimleri üzerinde yüz bulma ve tanıma hedeflenmiştir. Bu kapsamda birçok farklı yöntem denenmiştir. Fakat anlamlı sonuçlar elde edilememiştir. Aşağıdaki kısımlarda test edilen bazı yöntemler anlatılmıştır.

Logaritmik bölgede ayrık kosinüs dönüşümü (Discrete Cosine Transform – DCT)

Kalabalık resimlerinde yüz bulmak için SIFT metodu ile elde edilen özelliklerin logaritmik bölgede DCT'si alınarak bulma ve tanıma işlemi gerçekleştirilmeye çalışılmış ve başarılı sonuçlar elde edilememiştir.

K-ortalama kümeleme

Kalabalık resimlerinden elde edilen özellikler k-ortalama algoritmasına tabi tutularak orta noktaları tespit edilmiş ve elde edilen orta noktalara göre resim küçük parçalara bölünerek tek tek bulunmak istenen yüz ile karşılaştırılmış ve en yüksek eşleşmenin olduğu resim alınmıştır. Elde edilen özelliklerin orta noktalarının büyük ihtimalle yüz bölgeleri olacağı varsayımından yola çıkılmıştır. Ayrıca aramayı yerelleştirmek için resim bu orta noktalara göre belli bir ebatlarda kesilmiş sıra ile bulunmak istenen yüz resmi ile karşılaştırılmıştır. Fakat elde edilen sonuçların başarılı olmadığı gözlemlenmiştir.

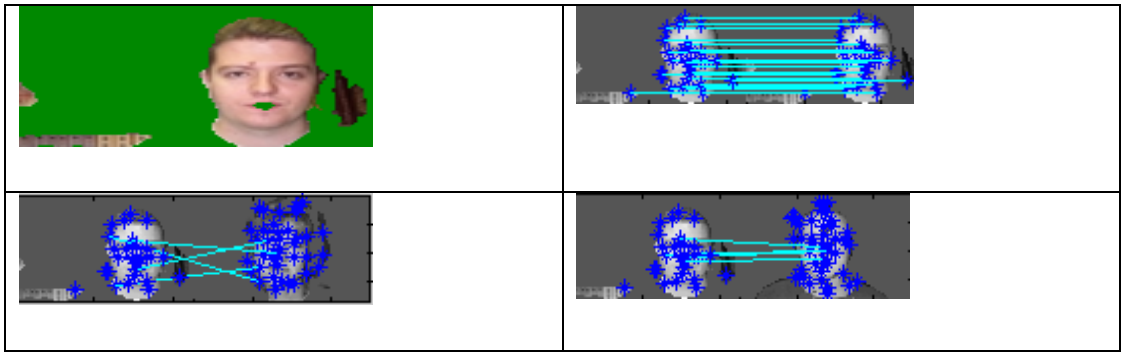
Şekil 4.9. Topluluk resimlerinde elde edilen sonuçlar

Blok eşleme

Kalabalık resimleri üzerinde özelliklerin bloklar halinde eşleştirilmesi yapılması için çalışma yapılmış. Fakat anlamlı sonuçlar elde edilememiştir.

YCbCr renk uzayında eşikleme ve morfolojik işlemler

Kalabalık resimler üzerinde anlamlı sonuçlar elde edilemeyince ışık, ifade, arka plan ve yön bilgileri değişen Kalifornia Teknoloji Üniversitesi (CALTECH) ön yüzler veritabanı kullanılmıştır. Bu veritabanında yer alan resimlerdeki yüz bölgelerini bulmak için çeşitli morfolojik işlemler uygulanmıştır. Bu işlemler sonucunda elde edilen yüz bölgeleri karşılaştırılmış ve anlamlı sonuçlar Şekil 4.10'de elde edilmiştir.



Şekil 4.10. Kalifornia Teknoloji Üniversitesi ön yüzler veritabanı üzerinde elde edilen görüntüler

Şekil 5.14'deki gibi tüm yüzlerde en yüksek eşleşme 36 adet ile aynı kişinin olmuştur. Fakat söz konusu kişilerin kendi resimlerinin farklı ışık, ölçek, oran, eğitim ve yüz mimik değişimlerindeki eşleşmelerinde Tablo 4.4'de belirtilen başarı oranları elde edilmiştir. Söz konusu veritabanında yer alan 27 farklı kişiden 10 farklı kişi seçilmiş ve seçilen 10 farklı kişinin farklı yüzleri kendisinin de farklılıklar arz eden yüzünün bulunduğu diğer 10 kişi ile karşılaştırılmış ve başarı oranları hesaplanmıştır. Söz konusu Tablo 4.4'de belirtilen yüzler 1'den 10'a kadar olan kısım 10 farklı kişiyi ifade etmektedir.

Tablo 4.4. CALTECH yüz veritabanında başarı oranları

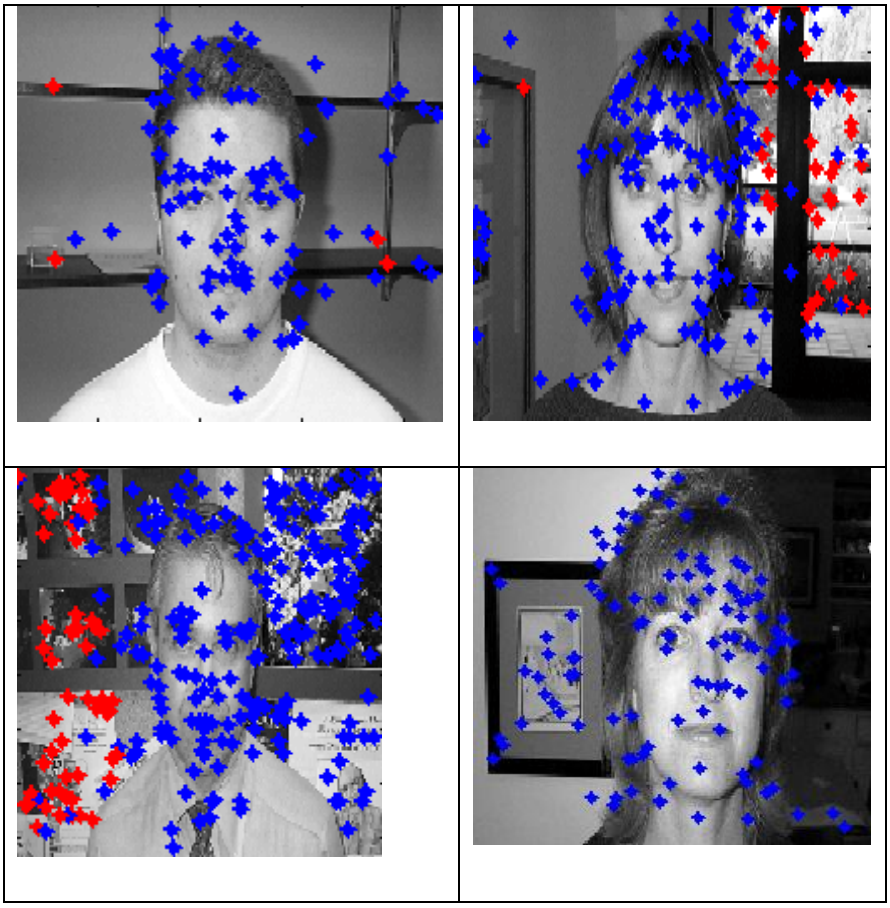
Yüzler	**Başarı Oranı**
1.	%20
2.	%20
3.	%30
4.	%20
5.	%30
6.	%20
7.	%40
8.	%20
9.	%30
10.	%20
Ortalama	**%25**

Destek Vektör Makinaları ile özelliklerin sınıflandırılması

Sınıflandırma konusunda kullanılan oldukça etkili ve basit yöntemlerden birisi de Destek Vektör Makinaları (SVM) olarak bilinen sınıflandırma yöntemidir. Gruplandırma yöntemi bir düzlem üzerinde bir veri kümesi arasında belli bir noktadan bir çizgi ile 2 sınıf oluşturulabilir. Bu hat çizgisi de 2 gruba en uzak nokta olabilir. Böyle bir durumda SVM bu sınırın nasıl çizileceği sorusuna yanıt bulur.

Örnek vermek gerekirse 2 farklı gruba yakın 2 çizgi çizilir ve bu 2 çizgi birbirine yaklaştırılarak ortak bir hat oluşturulur. Böylelikle bu veri setinde 2 farklı grup bir düzlem üzerinde gösterilebilir. Söz konusu düzlemsel alan ve ebatları birer özellik olarak farz edilebilir. Sonuçta sisteme sunulan her verinin özellikleri çıkarılmış ve düzlemsel alanda her girilen değeri belirten farklı bir nokta elde edilmiş olur. Ve tabi bu noktaların gruplandırılması demek, elde edilen özelliklere göre giriş özelliklerinin gruplandırılması demektir. SVM metodu ile herhangi bir veri kümesinde bir sınıflandırma yapmak mümkündür.

Kalifornia Teknoloji Üniversitesi yüz veritabanında SIFT metodu ile elde edilen özellikleri SVM metodu ile sınıflandırıp eşleşme başarı oranını tespit etmek amacıyla SIFT ve SVM metodu birlikte kullanılmıştır. Bu amaç doğrultusunda Kalifornia Teknoloji Üniversitesi'nde ve diğer yüz veritabanlarında yer alan resimler üzerinde de değişen arka plan bölgeleri yüz değil, yüz olan kısımlarda yüz resmi diye alınmış ve eğitim seti oluşturulmuştur. Öncelikle SIFT metodu ile yüz ve yüz olmayan resimlerin değişmez, sabit özellikleri elde edilmiştir. Elde edilen özellikler üzerinde eğitim işlemi yapılmış ve eğitim seti oluşturulmuştur. Eğitim işlemi sonucu eldeki veritabanındaki resimler tek tek bu eğitim seti sonuçları kullanılarak sınıflandırma yapılmıştır. Elde edilen başarı oranları kaydedilmiştir. Örnek bir eşleşme görüntüsü Şekil 4.11'de gösterilmiştir. Bu yöntem farklı algoritma ve parametreler için denenmiş elde edilen sonuçların başarı oranları hesaplanıp kayıt altına alınmıştır.



Şekil 4.11. CALTECH yüz veritabanı üzerinde elde edilen görüntüler

Şekil 4.11'de belirtilen yüz resimlerinde mavi noktalar SVM tarafından sınıflandırılmış ve yüz bölgesi olarak işaretlenmiş görüntülerdir. Kırmızı noktalar ise yüz olmayan kısımları ifade etmektedir. Söz konusu yöntemimizi Caltech yüz veritabanında 10 farklı insanın yüzünde tanıma amaçlı kullanarak elde edilen başarı oranları Tablo 4.5'de belirtilmiştir. Tablo 4.5'de rbf ve showplot ifadeleri SVM algoritması sınıflandırma parametrelerini ifade etmektedir.

Tablo 4.5. CALTECH yüz veritabanında SIFT ve SVM yöntemi başarı oranları

Yüzler	**Başarı Oranları**	
	Rbf	**Showplot**
1.	%58	%67
2.	%58	%74
3.	%57	%75
4.	%57	%71
5.	%57	%72
6.	%58	%74
7.	%57	%72
8.	%57	%73
9.	%57	%75
10.	%57	%75
Ortalama	**%57.3**	**%72.8**

Geliştirmiş olduğumuz yöntemimizi AT&T yüz veritabanında 10 farklı insanın yüzünde tanıma amaçlı kullanarak elde edilen başarı oranları Tablo 5.9'de belirtilmiştir. Tablo 4.6'de autoscale ve showplot ifadeleri SVM algoritması sınıflandırma parametrelerini ifade etmektedir.

Tablo 4.6. AT&T yüz veritabanında SIFT ve SVM yöntemi başarı oranları

Yüzler	**Başarı Oranları**	
	Autoscale	**Showplot**
1.	%71	%72
2.	%71	%71
3.	%72	%72
4.	%72	%72
5.	%72	%72
6.	%72	%72
7.	%73	%74
8.	%73	%72
9.	%72	%73
10.	%72	%72
Ortalama	**%72**	**%72.2**

Tablo 4.7. Yale yüz veritabanında SIFT ve SVM yöntemi başarı oranları

Kişiler	**Başarı Oranları**		
	Kernel Polinamial	**Kernel Quadratic**	**Kernel Rbf**
1.	%73	%74	%68
2.	%72	%73	%67
3.	%73	%73	%67
4.	%73	%73	%67
5.	%72	%74	%67
6.	%72	%74	%67
7.	%72	%74	%67
8.	%73	%74	%67
9.	%73	%74	%67
10.	%73	%75	%67
Ortalama	**%72.6**	**%73.8**	**%67.1**

Geliştirmiş olduğumuz yöntemimizi AT&T yüz veritabanında 10 farklı insanın yüzünde tanıma amaçlı kullanarak elde edilen başarı oranları Tablo 4.6'de belirtilmiştir. Tablo 4.6'da autoscale ve showplot ifadeleri SVM algoritması sınıflandırma parametrelerini ifade etmektedir.

5. ÖNERİLEN YÜZ TANIMA SİSTEMİ

İnsanların kendine has yüz geometrisi ve uzuvları söz konusudur. Kişinin yaşı, makyajı, saç stili değişse de kişinin yüz hatları değişmez. Aynı şekilde objelerin de kendine has özellikleri söz konusudur. Bu mihvalde bu özellikler nesne algılama yada tanımada kullanarak tanıma yapan çeşitli yöntemler söz konusudur. Bizim çalışmalarımızda da bu iki durum göz önüne alınarak, yüz hatlarında ve uzuvlarındaki spesifik özellikler kullanılarak bir eşleşme sağlamak suretiyle tanıma ve kimliklendirme sistemi geliştirilmesi hedeflenmiştir. Daha önce özellikle nesne algılama ve tespitinde Lowe tarafından nesne tanıma için geliştirilen ve uygulanan SIFT tanımlayıcılarından başarılı sonuçlar elde edilmiştir [36]. Bu bağlamda, yüz resimlerinde yer alan yüz bölgeleri bir nesne gibi düşünülüp araştıra işlemleri gerçekleştirilmiştir. Öncelikli olarak yüz tanımada kullanmak için AT&T yüz veritabanı kullanılmasına karar verilmiştir. Bu bağlamda veritabanındaki yüzlerin eşlenmesi için kullanılan yöntemin gösterildiği akış şeması Şekil 5.1'de yer almaktadır.

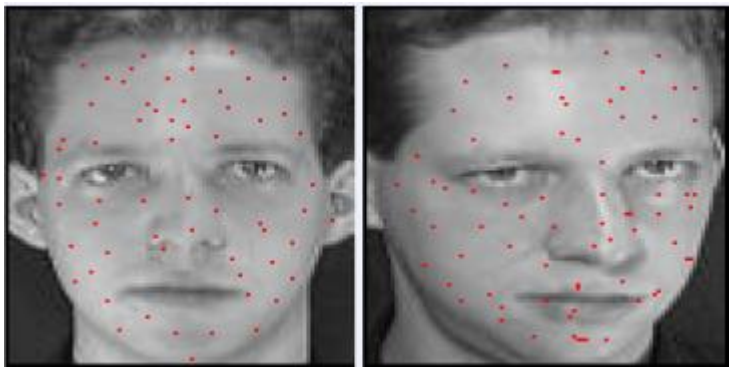
Şekil 5.1. Yöntem akış şeması

5.1. Resmi Sisteme Yüklemek

İlk aşamada geliştirilen sisteme, veritabanından diğer resimlerle eşleştirilip bir sonuç döndürülmesi için istenen resim yüklenir.

5.2. Yüzün İlgi Noktalarının Belirlenmesi

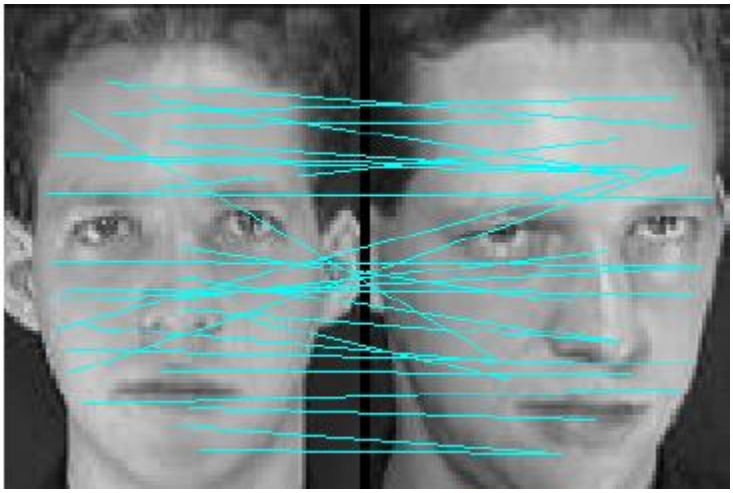
Sisteme yüklenen yüz resminin kendisi de dahil olmak üzere veritabanındaki diğer bütün kişilerin tüm resimleri ile karşılaştırma yapmak amacıyla ilgi noktalarının belirlenmesi için Lowe tarafından nesne tanımada kullanılan SIFT [36] yöntemi kullanılmıştır. İlgi noktaları belirlenmiş iki resim şekil 5.2'de görülebilir.



Şekil 5.2. İlgi noktaları belirlenmiş yüzler

5.3. İki Yüz Arasındaki İlgi Noktalarını Eşleştirme

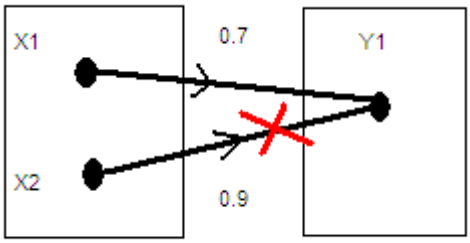
Elde edilen mihenk noktalarının 2 resim arasında eşleşmesi gerekmektedir. Fakat Lowe'n yöntemiyle tüm noktalar tam anlamıyla eşleşmez. Lowe'un yöntemi nesnelerdeki elde ettiği başarıyı her zaman yüz resimlerinde göstermez ve keza yanlış eşleşmeler olur (Bkz. Şekil 4.5). İyi sonuçlar elde etmek için yüzlere özgü ve yüz özelliklerini iyi belirleyen çeşitli sınırlama ve yöntemler ile eliminasyon işlemleri gerçekleştirilmelidir. Yüzlerdeki eşleştirmelerin ideali çizgilerin yatay ve birbirlerine paralel olmasıdır.



Şekil 5.3. Yüz resimleri arasında ilgi noktalarının eşleştirilmesi

5.4. Benzersiz Eşleşmeleri Eleyerek Sınırlama

Şekil 6.3'de de görülebileceği gibi yanlış eşleşmelerin çoğu çok yönlü eşleşmeler yada tek yönlü birçok nokta ile eşleşme durumlarından kaynaklanmaktadır. Örneğin A yüzündeki bir mihenk noktası B yüzündeki birçok ilgi noktası eşleşmişse, bu durum başarısız ve anlamsız eşleşmedir. Tek taraflı eşleşmelerde tek bir yüz resmindeki nokta diğer yüz resminde birden çok nokta ile eşleşme durumlarındaki durumdur. Bu iki tip yanlış eşleşme tekil ve doğru eşleme sınırlaması ile engellenebilir. Şekil 5.4'de çoklu eşlemenin nasıl engelleneceği gösterilmiştir. A yüzündeki bir ve iki numaralı mihenk anahtar noktaları B resminde bir numaralı mihenk anahtar noktasıyla eşleşme durumu görülmektedir. Böyle eşleşme durumlarında eşleşen noktalar arasındaki Oklid mesafeleri elde edilmiştir. Hesaplamadan elde edilen değerler hangi eşleşmenin eleneceğini belirler. Öklid uzunluğu kısa olan eşleşme tanıma işlemi için tercih edilir. Bu yöntem AT&T yüz veritabanından ilgi noktalar arasındaki farklı vektörel açı değerleri için (0.5,0.6,…,0.9) 40 farklı kişinin 10 farklı açıdan çekilen yüzlerin kendisi dahil diğer 40 kişi ile SIFT algoritması ile eşleşen aynı noktaların Oklid uzaklığı hesabı ile doğru eşleşmeyi seçerek yapılan eşleştirme başarı sonuç tablosu Tablo 5.1'de yer almaktadır.



Şekil 5.4. Çoklu eşleşmelerin elenmesi

Tablo 5.1. AT&T veritabanında çoklu eşleşmelerin Öklid başarı oranları

Yüzler\Oran	0.5	0.6	0.7	0.8	0.9
1.	%100	%100	%100	%100	%100
2.	%78	%83	%90	%88	%88
3.	%80	%83	%88	%85	%85
4.	%73	%83	%80	%83	%70
5.	%53	%63	%63	%60	%60
6.	%73	%70	%78	%83	%70
7.	%63	%63	%65	%75	%68
8.	%68	%78	%75	%73	%65
9.	%73	%78	%80	%85	%78
10.	%63	%65	%75	%70	%80

Şekil 5.4'de çok yönlü eşleştirmelerin gösterimi bulunmakta ve eşleşen noktaların eğimine göre elemine edilmesi işlemini göstermektedir. Burada eğer eşleşen noktalardan arasındaki açının tanjantı küçük olan değerin seçildiği ve geriye kalan eşlemenin elendiği gösterilmektedir.

Bu yöntem AT&T yüz veritabanından ilgi noktalar arasındaki farklı vektörel açı değerleri için (0.5,0.6,…,0.9) 40 farklı kişinin 10 farklı açıdan çekilen yüzlerin kendisi dahil diğer 40 kişi ile SIFT algoritması ile eşleşen aynı noktaların arasındaki

açının eğim hesabı ile doğru eşleşmeyi seçerek yapılan eşleştirme başarı sonuç tablosu Tablo 5.2'de yer almaktadır.

Tablo 5.2. AT&T veritabanında çoklu eşleşmelerin eğim başarı oranları

Yüzler\Oran	0.5	0.6	0.7	0.8	0.9
1.	%100	%100	%100	%100	%100
2.	%78	%83	%90	%88	%88
3.	%80	%83	%88	%85	%85
4.	%73	%73	%83	%80	%68
5.	%53	%63	%63	%60	%60
6.	%73	%70	%78	%83	%73
7.	%63	%63	%65	%75	%68
8.	%68	%78	%75	%73	%65
9.	%73	%78	%80	%85	%78
10.	%63	%65	%75	%70	%78

Şekil 5.5. Çoklu eşleşmeler elendikten sonra geriye kalan eşleşmeler

Yanlış eşleştirmelerin elenmesinden sonraki sonuç Şekil 5.5'de gösterilmiştir. Tablo 5.3 iki resimdeki ilgi noktalarının çoklu eşleşmesi ve bu eşleşmelerin Oklid hesabına

göre seçilmesi yönteminin Yale [37] yüz veritabanı üzerinde uygulanması sonucu elde edilen tanıma başarı oranları gösterilmektedir.

Tablo 5.3. Yale veritabanında çoklu eşleşmelerin Oklid başarı oranları

Oran\Yüzler	1.	2.	3.	4.	5.	6.	7.	8.	9.
0.5	%100	%100	%100	%93	%93	%93	%100	%93	%93
0.6	%100	%93	%93	%100	%93	%93	%100	%93	%93
0.7	%100	%93	%93	%93	%93	%93	%100	%93	%93
0.8	%100	%100	%93	%93	%93	%93	%100	%93	%93
0.9	%100	%93	%93	%100	%100	%100	%93	%100	%100

5.5. Sonuçları Sıralandırma

Geliştirilen yüz tanıma yazılımındaki son kısım elde edilen sonuçların sıralama işlemidir. Veritabanında yer alan tüm yüz görüntülerinin sisteme girilen yüz resmi ile eşleştirilmesi ve diğer 39 kişinin kendisi dahil diğer kişilerin sisteme girilen ilk yüzleri eşleştirilmesi sonucu hesaplanan değerlerinin sıralanmasıyla oluşur. Bu değerler sıralanır ve en büyük değer en iyi eşleşme sonucunu verir. Bu sonuç ta sisteme girilen yüz resminin veritabanındaki en çok benzeyen yüz resmi ile eşleşmesi demektir. Ayrıca kayıt o kişi ait bir yüz mü değil mi kontrol edilir. Eğer doğru ise başarılı bir eşleşme; değilse başarısız bir eşleşme olarak ele alınır. Bu uygulamada da AT&T yüz veritabanındaki her kişinin tüm yüzleri diğer kendisi dahil diğer 39 kişi ile 40 karşılaştırma sonucu tüm yüzlerdeki tanıma başarı oranları elde edilmiştir.

5.6. SVM ile Sınıflandırma

Sınıflandırma konusunda kullanılan oldukça etkili ve yöntemlerden birisi olan SVM yöntemi ile sınıflandırma yapılmıştır. Öncelikle yüz ve yüz olmaya bölgelerden oluşan yüz veritabanları oluşturulmuştur. Oluşturulan bu veritabanları kullanılarak SVM eğitim işlemi yapılmıştır. Eğitim işlemi sonucunda tanınmak istenen resim SVM metodu ile sınıflandırılmış ve doğru tanıma başarı oranı elde edilmiştir.

Kaliforniya Teknoloji Üniversitesi yüz veritabanındaki yüz resimleri kullanılarak SIFT ve SVM yöntemleri birlikte kullanılarak tanıma işlemi gerçekleştirilmiştir. Tanıma başarı oranını elde etmeden önce yüz ve yüz olmayan resimlerden SVM eğitim veritabanı oluşturulmuştur. Oluşturulan veri tabanlarından SIFT yöntemi ile ışık, yön, eğiğim faktörlerinden etkilenmeyen değişmez tanımlayıcılar elde edilmiştir. Elde edilen tanımlayıcılar yüz ve yüz değil olarak etiketlenip SVM eğitilmiştir. Yüz veritabanındaki resimler tek tek SVM yöntemi ile sınıflandırılmış sınıflandırma ve dolayısıyla tanıma başarı oranı her bir resim için ayrı ayrı elde edilmiştir. Elde edilen verilere göre tanıma başarı oranı %72 civarı olduğu görülmüştür.

6. SONUÇLAR VE ÖNERİLER

Bu araştırmada, yüz tanıma problemi için iki ana yaklaşım üzerinde araştırma yapılmıştır. SIFT ve SVM algoritmasına dayalı bir yüz tanıma sistemi önerilmiştir. Bu algoritmalar yaptığım çalışmalar neticesinde daha doğru sonuçlar elde etmemden dolayı tercih edilmiştir. Ayrıca güçlü bir yüz tanıma sistemi aşağıda belirtilen özelliklerden etkilenmemesi gerektiğinden bu yöntemler seçme nedenimi oluşturmuştur.

- Işık kaynağındaki değişimler
- Başın açısından ve oranından
- Yüzde bulunan gözlük ve sakal gibi detaylardan
- Yüz arka zemininden

Bu çalışmada önerilen yüz tanıma sistemi, yüz arka zemininden ve kafa açısından oldukça fazla miktarda etkilendiği deneyimler sonucu görülmüştür. Doğru tanıma oranı seçilen mesafe oranına göre değişmektedir. Örneğin 0.7 civarı mesafe oranlarında daha başarılı sonuçlar elde edildiği gözlemlenmiştir. Tabi mesafe oranının yanında diğer yaklaşımlarda tanıma başarı oranı artırmaktadır. Ayrıca SVM yöntemini eğitiminde kullanılan yüz ve yüz olmayan resim veritabanları ne kadar çok örnek üzerinden seçilirse daha iyi sonuçlar elde edildiği gözlemlenmiştir.
Bu tezde yapılan çalışmanın geliştirilmesi için aşağıdaki işlemler yapılabilir:

-Hibrit yaklaşımlar : Çalışmamızda önerilen yüz tanıma algoritması için SIFT ve SVM yöntemi kullanılmıştır. Fakat yüz bölgesini daha iyi tespit edecek yaklaşımlar ile birlikte kullanılırsa daha iyi sonuçlar elde edilebilir.

- YCbCr eşikleme ve morfolojik işlemler : Özellikle yüz resminin arka planını yok edip aydınlanma etkisinden azaltmak için yüz resmini YCbCr formatına çevirip bir takım eşik değerleri bulunarak yüz resmi tespit edilebilir. Ayrıca bu yöntem ile aydınlatma etkisi azaltılmış olur. Bulunan yüz bölgesini daha belirginleştirmek ve ışık, bozulma etkilerini azaltmak için morfolojik işlemlerden geçirilen yüz resimlerinde SIFT ve SVM yöntemimiz daha iyi sonuçlar elde edilebilir.

- Farklı görünümlerden tanıma: Bu tezde yapılan çalışma, yüzün ön yüz görünümü için çalışmaktadır. Yapay sinir ağları ile yüzün yönü tespit edilerek en uygun tanıma sistemi seçilebilir.
- Kamera ve tarayıcı desteği : Şu anda yüz resimleri bilgisayardaki dosyalardan alınmaktadır. Tarayıcı yardımıyla herhangi bir resim taranarak tanıma işlemi yapılabilmesi büyük kolaylık sağlayacaktır. Ayrıca güvenlik kameralarının görüntülediği ortamlarda sistemde tanımlı bir kişi görüntüye girdiğinde uyarı verilmesi sağlanabilir.

KAYNAKÇA

[1] İnternet: Emniyet Genel Müdürlüğü 2009 Yılı Faaliyet Raporu, http://www.egm.gov.tr/Duyurular (2000).

[2] İnternet: Forno R., Shredding the Paper Tiger of Cyberterrorism, SecurFocus Online, http://www.onlinesecurity.com/columnists/111 (2000).

[3] Denning, D. E., Cyberterrorism, ***Testimony Before The Special Oversight Panel on Terrorism, Committee on Armed Services***, U.S. House of Representatives (2000 (May 23)).

[4] Güvenli İnternet İçin Kullanıcı Bilinci Çalıştayı, ***Bilgi Güvenliği ve Kriptoloji Konferansı***, 6-8 Mayıs 2010.

[5] İnternet: APWG, 2008, Phishing Activity Trends Report, http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf.

[6] Network and Information Security: Proposal for a European Policy Approach, **Avrupa Komisyonu, Brussels, Belgium**, 2001.

[7] Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler, **BTK, Ankara**, Mayıs 2009.

[8] Değirmenci, O., "Bilişim Suçları", Yüksek Lisans Tezi, **Marmara Üniversitesi Sosyal Bilimler Enstitüsü**, İstanbul, 2002.

[9] Krause, M., Tipton, H., ***Information Security Management Handbook***, CRC Press, 6th Ed., 2007.

[10] Press, W. H., Flannery, B. P., Teukolsky, S. A., Vetterling, W. T., "Numerical recipes in C", ***Cambridge University Press***, pp. 353-380, (1988).

[11] Nickolov, E., Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure, ***Regional Cybersecurity Forum***, Sofia, Bulgaria, 7-8 Ekim 2008.

[12] OECD, ***OECD Guidelines For The Security of Information Systems and Networks: Towards a Culture of Security***, İnternet: http://www.oecd.org/dataoecd/16/22/15582260.pdf, 2002.

[13] Özsoy, O., "İnternetin Kararttığı Hayatlar", ***Pozitif Yayınlar Kelepir***, 2010.

[14] Sağıroğlu, Ş., "Bilgi Güvenliği ve Yapılması Gerekenler Sunumu", ***II. Ulusal IPv6 Konferansı***, Ankara, 2012.

[15] Sağıroğlu, Ş., Özkaya, N., "Açık Anahtar Altyapısı ve Biyometrik Teknikler", ***I. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı***, 2006.

[16] Saday, T., Akhan, N., "Bilgisayar Destekli Kimlik Tespit Sistemlerinde Biometrik Yöntemlerin Değerlendirilmesi", ***Akademik Bilişim Konferansları***, 2003.

[17] Yozgat, M., "Bilgisayarda Parmak İzi Tanıma", Yüksek Lisans Tezi, ***Gazi Üniversitesi Bilişim Enstitüsü***, Ankara, 2004.

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

[19] Sönmez, E. B., Özbek N. Ö., Özbek Ö., "Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi", ***Akademik Bilişim Konferansları***, 2007.

[20] İnternet: İngiltere Büyükelçiliği, http://www.ingilterekonsoloslugu.net, (2007) .

[21] Sağıroğlu Ş., Özkaya N., Otomatik Parmak izi Tanıma Sistemlerinde Kullanılan Önişlemler İçin Yeni Yaklaşımlar, ***Gazi Üniv. Müh. Mim. Fak. Dergisi***, Cilt 21, No 1, 11-19, 2006.

[22] Harmon, L. D., Khan, M. K., Lasch, R., and Ramig, P. F., "Machine identification of human faces", ***Pattern Recognition***, Vol. 13(2), pp. 97-110, (1981).

[23] E-Dönüşüm Türkiye Projesi 2005 Eylem Planı 6. Eylem Maddesi, "Akıllı Kartların Kamuda Kullanımı Konusunda Ön Çalışma Raporu", ***Tübitak-Uekae***, Ocak -2006.

[24] Elman, J.L., E.A. Bates, M.H. Johnson, A. Karmiloff-Smith, D. Parisi, K. Plunkett, Rethinking innateness: A connectionist perspective on development, ***Cambridge, MA: MIT Press***, 1996.

[25] Chellappa, R., C.L. Wilson, S. Sirohey, "Human and machine recognition of faces: a survey", ***Proceedings of the IEEE***, vol.83, no.5, 1995.

[26] Turk, M., A. Pentland, "Eigenfaces for recognition", ***Journal of Cognitive Neuroscience***, vol.3, no.1, pp.71-86, 1991.

[27] Wiskott, L., J.-M Fellous, N. Krüger, C. von der Malsburg, "Face recognition by elastic bunch graph matching", ***IEEE Transactions on Pattern Analysis and Machine Intelligence***, vol.19, no.7, pp.775-779, 1997.

[28] Ramasubramanian, D., Y.V. Venkatesh, "Encoding and recognition of faces based on the human visual model and DCT", ***Pattern Recognition***, vol.34, pp.2447-2458, 2001.

[29] Tanaka, J. W., Farah M.J., "Parts and wholes in face recognition," ***Quarterly Journal of Experimental Psychology: Human Experimental Psychology*** ,vol.46A, 225-245, 1993.

[30] Fodor, J.A., The Modularity of Mind, ***MIT Press, Cambridge, MA***, 1983.

[31] Karmiloff-Smith, A., Beyond modularity: A developmental perspective on cognitive science, ***Cambridge MA: MIT Press***, 1992.

[32] Özgen, N., "Bilgisayar Kontrollü Hedef Takibi", ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, Ankara, 2008.

[33] Moravec, H., "Visual mapping by a robot rover", ***Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI).*** 598–600 (1979).

[34] Harris, C., Stephens, M., "A combined corner and edge detector",***4th Alvey Vision Conference***,147–151(1988).

[35] Kanade, T., Collins, R., Lipton, A., Burt, P., And Wixson, L., "Advances in cooperative multi-sensor video surveillance", ***Darpa IU Workshop***, 3–24 (1998).

[36] Lowe, D., "Distinctive image features from scale-invariant keypoints", ***Int. J. Comput. Vision***, 2, 91–110(2004).

[37] İnternet : Amerika Yale Üniversitesi "Yüz Veritabanı" http://cvc.yale.edu, (1997).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : FİLİZ, Süleyman

Uyruğu : T.C.

Doğum tarihi ve yeri : 20.10.1984 Çorum

Medeni hali : Bekar

Telefon : 0 (312) 462 55 63

e-posta : sfiliz@egm.gov.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Gazi Üniversitesi/ Bilgisayar Mühendisliği	2008
Lise	Tokat Anadolu Öğretmen Lisesi	2002

İş Deneyimi

Yıl	Yer	Görev
2008-….	Emniyet Genel Md.	Bilgisayar Mühendisi/Komiser

Yabancı Dil

İngilizce

Hobiler

Futbol,Yakın savunma, Bilgisayar teknolojileri, Basketbol