T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PARMAK İZİ VE SES TANIMA SAYISAL KANIT İŞLEMLERİNİN ANALİZİ

Gülşah AKKAN

Yüksek Lisans Tezi
Elektronik ve Bilgisayar Eğitimi Anabilim Dalı
Danışman: Prof. Dr Asaf VAROL

HAZİRAN -2013

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

PARMAK İZİ VE SES TANIMA SAYISAL KANIT İŞLEMLERİNİN ANALİZİ

Yüksek Lisans Tezi

Gülşah AKKAN

Tezin Enstitüye Verildiği Tarih:
Tezin Savunulduğu Tarih:

Tez Danışmanı: **Prof. Dr. Asaf VAROL**
Diğer Jüri Üyeleri: **Doç. Dr. Engin AVCI**
Doç. Dr. Sami EKİCİ

TEŞEKKÜR

Bu tezi hazırlarken her türlü bilgi ve tecrübesi ile hep yanımda olan, desteğini ve emeğini gördüğüm danışman hocam Sayın Prof. Dr. Asaf VAROL'a teşekkür ederim.

Çalışmalarım esnasında yardımlarını esirgemeyen, bana yol gösteren hocalarım Yrd. Doç. Dr. Murat KARABATAK'a ve Doç. Dr. Engin AVCI'ya içtenlikle teşekkür ederim.

Bu günlere gelmemde üzerimde büyük emeği olan aileme, öğretmenlerime, yoğun çalışma dönemlerimde yanımda olan arkadaşlarıma ve çalışmalarımda bana hep destek olan sevgili eşime teşekkürü bir borç bilirim.

Gülşah AKKAN

Elazığ- 2013

İÇİNDEKİLER

ÖZET

Bilişim teknolojilerinin baş döndürücü bir hızla geliştiği günümüzde bilgi güvenliği en önemli sorunlardan biri haline gelmiştir. Bilginin elde edilmesi kolaylaştıkça, muhafaza edilmesi zorlaşmıştır. Gelişen teknoloji insanlara yarar sağlamanın yanı sıra yeni suç türlerinin ortaya çıkmasına zemin hazırlamıştır. Bu suçların faillerinin ortaya çıkarılmasında mevcut sistemler yetersiz kalmış hem güvenlik güçleri hem de adli merciler, bilişim yoluyla işlenen bu suçların, tespitinde ve değerlendirilmesinde yine bilişim teknolojilerine ihtiyaç duymuşlardır.

Dijital delillerin elde edilmesi ve analizi son derece önemli hale gelmiş ve klasik yöntemlerin yerine daha modern tekniklerin kullanılması zorunluluğu doğmuştur. Gerek güvenliğin sağlanması için önleyici tedbirlerin alınmasında gerekse suçluların kimliklerinin tespit edilmesinde biyometrik sistemler kullanılmaya başlanmıştır. Bu tezde adli bilişimin değerlendirme aşamasında kullanılmak üzere parmak izi ve ses biyometriklerinden kimliklendirme yaparak suçluların tespit edilmesine yardımcı olacak bir sistem tasarlanması amaçlanmıştır.

Bu amaçla MATLAB' da geliştirilen yazılımın parmak izi ve ses olmak üzere iki ayrı fonksiyonu bulunmaktadır. Parmak izi tanıma sisteminde; parmak izi resimleri, görüntü işleme teknikleri kullanılarak iyileştirilmekte ve iki parmak izi resmi karşılaştırılarak aralarındaki benzerlik yüzdesi bulunmaktadır. Konuşmacı tanıma sisteminde ise dosyadan ya da mikrofondan girilen ses ile daha önceden veri tabanına kaydedilmiş sesler arasında eşleştirme yapılmakta ve sesin kime ait olduğu tespit edilmektedir.

Anahtar Kelimeler: Adli Bilişim, Sayısal Delil, Parmak İzi Tanıma, Konuşmacı Tanıma

SUMMARY

ANALYSIS OF FINGERPRINT AND VOICE RECOGNITION DIGITIAL EVIDENCE PROCESSES

Because information technology is developing at a dazzling pace today, information security has become one of the most important problems. As it get easier to obtain information, it becomes difficult to protect it. In addition to provide benefits to mankind, developing technology has led to the new types of crime. In discovering the perpetrators of these crimes, present systems were inadequate both security forces and judicial authorites needed information technologies to determine and evaluate these crimes which are committed through informatics.

Acquisition and analysis of digital evidences have become extremely important and it became necessary to use modern techniques rather than classical methods. Biometric systems were started to use both taking preventive measures to ensure security and determination of the identity of the criminals. In this thesis, it is aimed to design a system that will help identify criminals from their fingerprints and voice biometrics in computer forensic evaluation stage.

The software which is developed in MATLAB has two seperate functions. In identification, it aims to use fingerprints and voice biometrics are most widely used in computer forensic analyzing. In fingerprint recognition system, fingerprint image are improved by using imace processing techniques and the percentage of similarity between two fingerprints images. In speaker recognition system, the voice which is entered from the file or through microphone is matched with the voices which are prerecorded in database and it is determined that whose voice it is.

Key Words: Computer Forensic, Digital Evidence, Fingerprint Recognition, Speaker Recognition

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR LİSTESİ

EGM	**:**	Emniyet Genel Müdürlüğü
TADOC	**:**	Turkish Academy Against Drug and Organised Crime (Türkiye Uluslararası Uyuşturucu ve Organize Suçlarla Mücadele Akademisi)
TCK	**:**	Türk Ceza Kanunu
TÜİK		Türkiye İstatistik Kurumu
ISO	**:**	International Organization for Standardization (Uluslararası Standartlar Örgütü)
ATM	**:**	Automatic Teller Machine (Otomatik Vezne Makinesi/Bankamatik)
PIN	**:**	Personal Identification Number (Kişisel Tanımlama Numarası)
CDR	**:**	Call Detail Record (Arama Detay Kayıt Bilgileri)
GPS	**:**	Global Positioning System (Küresel Konumlandırma Sistemi)
DNA	**:**	Deoksiribonükleik Asit
ÖSYM	**:**	Ölçme, Seçme ve Yerleştirme Merkezi
MTOK	**:**	Mesleki Teknik Ortaöğretim Kurumları
AFIS	**:**	Automated Fingerprint Identification System (Otomatik Parmak İzi Teşhis Sistemi)
MOBESE	**:**	Mobil Elektronik Sistem Entegrasyonu
CAT	**:**	Computerized Axial Tomography (Bilgisayarlı Aksiyal Tomografi)
OPTS	**:**	Otomatik Parmak İzi Tanıma Sisteminde
MFCC	**:**	Mel-Frequency Cepstral Coefficients (Mel Frekansı Kepstral Katsayıları)
LBG	**:**	Linde- Buzo- Gray Algoritması
VQ	**:**	Vector Quantization (Vektör Nicemleme)

1. GİRİŞ

1990'lardan günümüze uzanan süreç için bilgi çağı ya da bilişim çağı ifadesi kullanılmaktadır. Sanayi devriminden sonraki süreçte oluşan endüstri toplumunun, ilerleyen yıllarda internet kullanımının yaygınlaşmaya başlamasıyla bilgi toplumuna dönüştüğü görülmektedir. Bu dönemde teknolojik gelişmelerle birlikte bilişim sistemleri ortaya çıkmış ve bilgi, geniş coğrafyalara yayılmıştır. Daha sonraki dönemde mobil iletişim teknolojilerindeki gelişim, bilgiye erişimin mekândan ve zamandan bağımsız hale gelmesini sağlamıştır [1].

İnternet, teknolojik gelişmelerin en büyüğü olarak görülmekte ve bilginin hazırlanması, işleyişi, paylaşımı ve pazarlanmasında çok büyük rol oynamaktadır. İnternetin ülkemizde yaygınlaşmaya başladığı yıllarda, sadece üniversiteler ve bazı devlet kurumlarında internet erişimi bulunurken, ticari kuruluşlar ve ev kullanıcıları gibi geniş kitlelere ulaşması 1996 yılı itibariyle mümkün olmuştur. 1997 yılı sonunda internet erişimi olan ticari kuruluş sayısı 10.000'e, internete bağlı bilgisayar sayısı ise 30.000'e yükselmiştir. Günümüzde ise her evin hatta mobil teknolojiler ile birlikte her bireyin internete erişimi mümkün olabilmekte ve 26,5 milyon insanın internet kullanıcısı olduğu tahmin edilmektedir. Artan internet kullanımı, internete yatırım yapan yerli ve yabancı yatırımcı sayısını da artırmıştır. Özellikle e-ticaret alanında gelişmeler sağlanmış, facebook gibi sosyal paylaşım alanlarında birçok dijital ajans hayata geçirilmiştir. Bankalar, müşterilerine internet üzerinden hizmet sunmaya başlamışlardır. Ticari kuruluşlar, sanal âlemde de varlıklarını duyurma çabasına girmiş ve rekabet ortamı doğmuştur. İnternet üzerinden geniş kitlelere ulaşılması, geleneksel medyanın da ilgisini çekmiş, kalabalıklara ulaşmak için internetin tüm nimetlerinden faydalanmaya başlamışlardır [2,3].

İnternetin bu kadar yoğun kullanılması toplum hayatında da değişikliklere yol açmıştır. Hayatımıza yeni kavramlar dâhil olmuştur. İnsanlar, alışveriş ve bankacılık işlemlerini internetten yapmak gibi, arkadaşlarını, dostlarını internet ortamından seçmek gibi yeni alışkanlıklar kazanmıştır. Hatta toplumda internet bağımlılığı yaygınlaşmış, insanlar bulundukları her ortamdan internete bağlanma ihtiyacı duyar hale gelmişlerdir.

İnternetin hayatımıza bu ölçüde yerleşmiş olması suçluların da ilgisini çekmiş ve internete yönelmelerini sağlamıştır. Bu yeni dünyaya çok hızlı adapte olan suçlular, kendilerini teknoloji alanında da hızlı bir şekilde geliştirmiş, klasik yöntemler ile oldukça zor gerçekleşecek suçları, internet ortamından kolay bir şekilde yapabilmeye

başlamışlardır. Bu suçlar günümüzde bilişim suçları, bilgisayar suçları, ileri teknoloji suçları gibi birçok kavramla ifade edilmektedir [2].

Bilişim suçları şu anda, bütün dünyayı tehdit eden en büyük meselelerden biri olarak görülmektedir. Bu nedenle birçok ülkenin polis birimleri altında, konu ile ilgili özel birimler oluşturulmuştur.

Bilişim suçları, çok kapsamlı bir konu olduğu için birçok tanım ve sınıflandırma ile karşılaşmak mümkündür. Örneğin Amerikan Adalet Departmanı'na göre ceza kanununu ihlal eden, işlenmesinde veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç, bilişim suçu olarak tanımlanmaktadır [4].

Bilişim suçlarının aydınlatılması için delillendirme şarttır. Bilişim suçları kapsamında fiziksel delillerden ziyade, dijital deliller daha büyük bir önem arz etmektedir. Fiziksel delillerin aksine dijital deliller çok çabuk zarar görebilir ve hatta yok olabilirler. Bu nedenle dijital delillerin doğru bir şekilde toplanması, analiz edilmesi ve mahkemeye sevk edilebilmesi için bazı standart prosedürler izlemek gerekmektedir [4].

1.1. Tez Çalışmasının Amacı

Bu tez çalışmasının amacı kriminal olaylarda, olay yerinde bulunan parmak izi ve ses biyometrik verilerinin analiz edilerek suçluya ait olup olmadığını belirleme konusunda kolluk kuvvetlerine destek sağlamaktır. Ayrıca ülkemizde çok yeni bir kavram olan adli bilişim konusu teknik ve hukuksal açıdan detaylı bir şekilde ele alınmıştır. Bu sayede gelişen bilişim teknolojilerinin adli süreçlere daha fazla katkı sağlaması amaçlanmaktadır.

1.2. Tez Çalışmasının Kapsamı

Bu tezin ilk bölümünde Türkiye'de henüz yeni bir bilim dalı olan adli bilişim hakkında genel bilgiler verilerek, tez çalışmasının amaç ve kapsamı açıklanmıştır.

İkinci bölümde bilişim suçları kavramı teknik ve hukuki boyutları ile ele alınmış, Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporu temel alınarak sınıflandırılmıştır.

Üçüncü bölümde adli bilişim kavramı detaylı bir şekilde irdelenmiş, tarihçesi, süreçleri ele alınmıştır. Sayısal kanıt yöntemleri, dijital delillerin elde edilmesi, değerlendirilmesi süreçlerinden bahsedilmiştir. Ülkemizde adli bilişimin dünü ve bugünü

karşılaştırılmış, istatistiksel veriler ile değerlendirilmeler yapılmıştır. Son olarak ülkemizde adli bilişim eğitimi konusunda hangi noktada olduğumuz gözler önüne serilmiş ve adli bilişim eğitimi veren kurum ve kuruluşlar incelenmiştir.

Dördüncü bölümde günümüzde güvenlik ve kimlik doğrulama konularında sıkça başvurulan biyometrik sistemler ele alınmış bu sistemlerin adli bilişim süreçlerinde nasıl kullanıldığı açıklanmıştır.

Beşinci bölümde ise suçluların kimliğini tespit edebilmek için parmak izi ve ses verilerini analiz etmek için kullanılan görüntü ve ses işleme konularından ve tasarlanan uzman sistemin uygulama aşamalarından bahsedilmiştir.

2. BİLİŞİM SUÇLARI

2.1.Bilişim Kavramı

Bilişim kavramının sözlük anlamı, Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü başlığıyla internet sayfasında şöyle belirtilmiştir:

"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinler arası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim, bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevim alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır" [5].

Bilişim; insanların teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi, enformatik olarak ifade edilmektedir [6].

Bilişim, bilginin elektronik ortamda üretilmesi, kaydedilmesi, saklanması, taşınması ve/veya kullanılması ile ilgili cihaz, materyal, işlem ve yöntemleri kapsamaktadır. Çoğu zaman bilgisayar ve bilişim kelimeleri eş anlamda kullanılsa da durum aslında öyle değildir. Bilgisayar; verileri işleyen, onlar üzerinde aritmetiksel ve mantıksal işlemler yapan bu işlemlerin sonucunu depolayabilen elektronik bir cihazdır. Bilişim ise bilgisayar kullanılarak bilgi üretilmesi, işlenmesi, saklanması, bilginin değerlendirilmesi ve iletilmesi gibi faaliyetleri kapsamaktadır.

2.2. Bilişim Suçu Nedir?

Baş döndürücü bir hızla gelişmekte olan bilişim teknolojileri, insanoğlunun hayatını kolaylaştırmakla kalmayıp yeni kavramları da telaffuz edilir hale getirmiştir.

Eğitim, sağlık, ticaret, sanayi, ekonomi, sanat, eğlence ve daha birçok alanda ezberi bozarak yepyeni bakış açıları kazandırmıştır.

Günümüzde bilgi, eskisinden daha çok değerli hale gelmiştir. Bilginin sosyal, siyasal, kültürel ve ekonomik alandaki gücünü keşfeden ve ön plana çıkaran devletler dünya siyasetine yön verir hale gelmişlerdir. İnternet ile birlikte bilginin elde edilmesi, işlenmesi, paylaşılması ve pazarlanması süreçleri hızlanmış fakat olumlu birçok gelişmeye sahne olan bu süreç beraberinde kontrol edilmesi güç sorunları da getirmiştir. Bilginin bu kadar değerli ve önemli olması suçluların da dikkatini çekmiş, bilginin güvenliğini sağlamak başlı başına bir sorun haline gelmiştir.

Klasik yöntemlerle işlenmesi güç olan ya da belirli bir coğrafya ile sınırlı kalan suçlar, bilişim teknolojilerinin imkânları kullanılarak hayal gücünün gittiği yere kadar uzanmış ve sınırları aşarak küresel bir boyut kazanmıştır.

Bilişim suçları çok yönlü yapısı nedeniyle çok farklı şekillerde tanımlanmaktadır. Bunlardan birkaçı:

"Ceza kanununu ihlal eden, işlenmesinde veya araştırılmasında bilgisayar teknolojisi bilgilerini içeren her suç bilişim suçu" olarak tanımlanmaktadır [4].

"Her türlü teknoloji kullanılarak, kanuni olmayan yollarla kişisel ya da kurumsal bilgisayarlarda, sistemler üzerinde zarar verici etki bırakmaktır" [7].

Bilişim suçlarının Avrupa da ki ilk tanımı ise Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısında yaptığı tanımlamaya göre; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanun, gayri ahlakî ve yetki dışı gerçekleştirilen her türlü davranıştır." denmektedir [8].

Bilişim Suçlarının Hukuki tanımı ve TCK' daki yeri ise; "Bilgileri otomatik bir sisteme tabi olan bilgisayar, bilgisayar programları ile iletişim teknolojilerinin verilerini hukuka aykırı bir biçimde ele geçiren, ele geçirerek değiştiren, yok eden, erişilmez kılan böylece bir başkasının zarara uğratılmasının sağlanması veya kendisine ve başkasına maddi bir çıkar sağlanması bilişim suçunu oluşturmaktadır" şeklinde tanımlanmaktadır [8].

Yukarıda ifade edildiği üzere bilişim suçunun ne olduğu konusunda çok çeşitli düşünceler bulunmaktadır. Bilişim suçlarının yapılışı, işlenişi ve kullanılan unsurlar dikkate alındığında genel olarak ve kısaca ''bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlardır'' diye tanımlamak mümkündür [9]. Bu noktada iki farklı suç tipi ortaya çıkmaktadır. İlki; geleneksel suçların bilişim teknolojileri kullanılarak işlenmesidir. Bu suçlara hakaret, dolandırıcılık gibi faaliyetlerin dijital ortamlarda işlenmesini örnek

verebiliriz. Diğeri ise bilişim teknolojilerinin gelişmesi ile ortaya çıkan dijital ortamlarda işlenen suçlardır. Bilgisayar sistemlerine izinsiz girişler bu suçlara örnek olarak verilebilir.

2.3. Bilişim Suçlarının Sınıflandırılması

Bilişim suçlarını keskin çizgilerle kategorilere ayırmak çok zordur. Çünkü bilişimle ilgili suç türleri çok değişik şekillerde karşımıza çıkabilmektedir. Suç çeşitleri ayrımında, 11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporu temel alınmaktadır. Bu rapora göre bilişim suçları 6 ana başlıkta incelenmektedir.

2.3.1. Bilgisayar Servislerine Yetkisiz Erişim ve Dinleme

2.3.1.1. Yetkisiz Erişim

Bu suç türünde bir bilgisayar sistemine ya da bilgisayar ağına yetki olmaksızın erişim söz konusudur. Suçun hedefinde bir bilgisayar sistemi ya da bilgisayar ağı vardır. Yetkisiz erişim, sistemin bir kısmına ya da bütününe olabileceği gibi programlara veya içerdiği verilere ulaşma şeklinde de olabilir. Ayrıca müdahale kişi tarafından yakın mesafeden direkt yapılabileceği gibi uzak mesafeden bilgisayar ağ sistemleri aracılığıyla da gerçekleştirilebilir [10].

2.3.1.2. Yetkisiz Dinleme

Bir bilgisayar veya ağ sisteminin yetki dâhilinde olmaksızın teknik anlamda dinlenmesidir [11]. Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferi dinlemenin hedefindedir. Dinlemenin hedefinde olan iletişim aşağıdaki şekillerde olabilir [12];

- Tek bir bilgisayar sistemi içerisinde
- Aynı kişiye ait iki bilgisayar sistemi arasında
- Bir biriyle iletişim kuran iki bilgisayar arasında
- Bir bilgisayar ve bir kişi arasında

Teknik anlamda dinleme, iletişimin içeriğinin "izlenmesi", verilerin kapsamının elde edilmesidir. Verileri ya direkt olarak bilgisayar sistemini kullanma veya erişme yoluyla ya da dolaylı olarak elektronik dinleme cihazlarının kullanımı yoluyla elde edilmektedir. Suçun oluşması için dinlemenin yetkisiz olarak yapılması gerekir. Uygun yasal şartlar çerçevesinde, soruşturma yetkililerinin yaptıkları bu kategoriye girmez [12].

2.3.1.3. Hesap İhlali

Hesap ihlali, bir başkasının dijital hesabına yetkisiz bir şekilde erişerek ödeme yapmak ya da sistemden istifade etmek şeklinde ortaya çıkabilir. Geleneksel hırsızlık ve dolandırıcılık suçlarıyla benzerdir. Hesap ihlali konusunda mağduriyet yaşamak istemeyen pek çok bilgisayar servis şirketleri ve ağları, hesaplarını kontrol etmek amacıyla otomatik faturalandırma araçları temin etmek zorunda kalmışlardır [12].

2.3.2. Bilgisayar Sabotajı

Bu suç mantıksal ve fiziksel olmak üzere iki farklı şekilde karşımıza çıkmaktadır.

a) Mantıksal (Bilgisayar verilerine zarar verme ya da değiştirme)

Bir bilgisayar ya da iletişim sisteminin çalışmasını engellemek amacıyla, verilerin girilmesi, silinmesi veya değiştirilmesi ya da programlarının yüklenmesi, silinmesi gibi dışardan yapılan eylemlerdir. Veri ya da programlara; Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horse), Virüs, Solucan (Worm) gibi yazılımlar kullanılarak zarar verilemektedir [12].

b) Fiziksel

Bir bilgisayar ya da iletişim sistemine fonksiyonlarını engelleme amacıyla, fiziksel yollarla zarar vermedir.

2.3.3. Bilgisayar Yoluyla Dolandırıcılık

Bilgisayar yoluyla dolandırıcılık, kendisine veya başkasına haksız kazanç sağlamak ya da mağdura zarar vermek adına yapılan, bilgisayar ve iletişim sistemleri kullanılarak

verilerin bozulması, değiştirilmesi, yok edilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi şeklinde gerçekleştirilen eylemlerdir. Bilgisayar bağlantılı dolandırıcılık suçları genellikle dolandırıcılığın geleneksel ceza kanunları içerisindeki tanımlarındaki gibi değerlendirilir ve kovuşturması bu kapsamda yapılır [13, 14]. Bilgisayar dolandırıcılığı suçluları, klasik dolandırıcılık yöntemleriyle gerçekleştirilmesi zor hatta imkânsız olan faaliyetleri, modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını kullanarak çok rahat bir şekilde gerçekleştirebilmektedirler.

2.3.3.1. Banka Kartı Dolandırıcılığı

Bankamatik sistemlerinden yapılan dolandırıcılık ve hırsızlık suçlarıdır. Bankamatik sistemleri (ATM- Automated Teller Machine), bankalar ya da benzer finans kuruluşları tarafından kullanılmakta olan bir dağıtım kanalıdır. Önceleri sadece para ödeme ve ekstre basma gibi işler için kullanılırken, günümüzde, para yatırma, para transferi, fatura ödeme ve yatırım gibi birçok konuda müşterilere hizmet vermektedir. Çoğunlukla üzerinde manyetik bir banda sahip plastik kartlar ile işlem yapılabilen bankamatiklerde, işlemlere başlanmadan önce kullanıcıdan bir kişisel tanımlama numarası (PIN- Personel Identification Number) talep edilerek güvenli giriş temin edilmektedir. Zaman içinde, bankamatik cihazlarına kartsız işlem menüleri de dâhil edilmiştir. Dolandırıcılık bu kartların çoğaltılması, kopyalanması ya da iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur [15, 16].

Türk Ceza Kanunu'nun 245. maddesinde banka kartı dolandırıcılığı suçu;

- Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlaması,
- Bir kimsenin başkalarına ait banka hesaplarıyla ilişkilendirerek sahte banka veya kredi kartı üretmesi, satması, devretmesi, satın alması, satması veya kabul etmesi,

- Bir kimsenin, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlaması şeklinde ifade edilmektedir [17].

Alışveriş sırasındaki ödemelerde kredi kartlarının kullanımı yaygınlaşmıştır. Bu sayede kredi kartlarının değişik yöntemlerle dolandırıcılık amacıyla kullanımı da artmıştır. Emniyet Müdürlüğü yetkililerinin açıklamalarına göre, bugüne kadar çok değişik türlerde kredi kartı dolandırıcılığı polis kayıtlarına girmiştir. Bu suç türünün işleniş biçimi incelendiğinde; alışveriş ya da ATM makinelerinin kullanımı sırasında manyetik kopyalama cihazları vasıtasıyla bilgilerin alınması, internet üzerinde bulunan online alışveriş sitelerinin kayıtlarının elde edilmesi, internet üzerindeki sohbet kanalları (facebook, messenger gibi) vasıtasıyla kart bilgilerinin alınması, sahte olarak oluşturulan web sayfalarına yönlendirme yapılarak kredi kartı bilgilerinin elde edilmesi, pornografik içerikli sitelerden cüzi ücretler karşılığı hukuka aykırı içerik sunularak kredi kartlarının ödeme vasıtası olarak kullanılması sırasında kart bilgilerinin ele geçirilmesi, bağış amaçlı sitelere cüzi ücretler bağışlanabilmesi için banka veya kredi kartı bilgisinin istenmesi sırasında kart bilgilerinin ele geçirilmesi gibi çok farklı yöntemler olduğu görülmektedir [14].

Bugüne kadar polis kayıtlarına geçen, kredi kartı dolandırıcılığı yöntemleri şunlardır [18]:

- **Kayıp ve çalıntı kartlar:** Dolandırıcılar, kimlik ve imza kontrolü yapılmayan iş yerlerindeki alışverişlerde kayıp ya da çalıntı kartları kullanabilmektedirler. Bunu engellemek için kredi kartı kaybolan kişinin en kısa sürede bankasına bildirim yapması gerekmektedir.
- **Ele geçmeyen kartlar:** Kredi kartının müşteriye, posta ya da kargo yoluyla ulaştırılırken çalınarak kullanılması yöntemidir. Bu dolandırıcılık, sahte kimlik belgeleriyle banka şubesinden kart alınarak da yapılabilmektedir.
- **Boş plastik:** Kredi kartı boyutundaki boş plastik plakalara gerçek kredi kartlarına ait numaralar basılarak müşteri sanki alışveriş yapmış gibi, bu kart pos cihazından geçirilerek satış belgesi düzenlenmesi yöntemidir. Sonra bu para bankadan tahsil edilmek suretiyle dolandırıcılık gerçekleştirilmektedir.

- **Değiştirilmiş kart:** Dolandırıcının kendisine ait ya da bir şekilde ele geçirdiği kredi kartındaki numara, ütüleme yöntemiyle yok edilerek yerine yeni ve başkasına ait bir numara basılmak suretiyle dolandırıcılık yapılması yöntemidir.
- **Sahte kartlar:** Öncelikle sahte bir kredi kartı basılıp kartın arkasında bulunan manyetik şeride, encoder (kodlayıcı) adı verilen bir cihazla gerçek kredi kartı bilgilerinin kodlanması suretiyle gerçekleştirilen dolandırıcılık yöntemidir.
- **Manyetik şerit sahteciliği:** Dolandırıcının, kendisine ait kredi kartının arkasındaki manyetik şerit bilgilerini silerek encoder cihazıyla başkasına ait bilgileri yüklemesiyle gerçekleştirdiği dolandırıcılık yöntemidir.
- **Kart kopyalama:** Alışveriş yapan müşterilerin kartlarının, müşteri görmeden encoder cihazından geçirilip kopyalanarak elde edilen bilgilerin, üretilen sahte bir kartın şeridine aktarılmasıyla gerçekleştirilen dolandırıcılık yöntemidir.
- **ATM dolandırıcılığı:** Dolandırıcıların, ATM'nin kart giriş haznesine bir cisim yerleştirerek gelen müşterinin kartının ATM cihazında kalmasını sağladıkları, daha sonra yardım etmek bahanesiyle şifreyi öğrenerek müşterinin bankadan ayrılmasından sonra da kartı ATM cihazından çıkarıp kullandıkları dolandırıcılık yöntemidir.
- **Hesap yönlendirme:** Kart sahibinin kimlik bilgileri, kredi kart bilgileri öğrenilerek bankaya telefonla veya başvuru formuyla müracaat edilerek kartın adresi değiştirilmekte ve bir süre sonra kaybolma bahanesiyle yeni adrese yeni kart istenmektedir. Gelen kartın arkasına imza atan dolandırıcı kartı kullanmaya başlayabilmektedir [18].

2.3.3.2. Girdi/Çıktı/ Program Hileleri

Bir bilgisayar sistemine zarar verme veya menfaat sağlama amacıyla; yanlış veri girişi yapmak, sistemden çıktı almak ya da sistemdeki programları değiştirmek suretiyle gerçekleştirilen dolandırıcılık ve hırsızlıktır.

Bir bilgisayar veri tabanına yanlış veri girmek yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistemde kullanılan yazılım programlarını da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır. Yanlış çıktı daha az yaygındır ve genellikle sahte dokümanların veya çıktıların üretiminde kullanılır. Bu tür suçları araştırırken

kullanılan sistem incelenmelidir ve saklı veya silinmiş dosyaları kurtarmak için her türlü çaba gösterilmelidir. Program hilelerinin tanımlanması teknik açıdan daha zordur [19].

2.3.3.3. İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma

Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerine veya diğer bilgisayar sistemlerine yetkisiz olarak girilmesidir.

İletişim servislerinin değişik şekillerde kötü kullanımı olarak tanımlanabilir. Fiil bazen yüksek telefon faturalarının önüne geçmek için işlenebilir [20].

2.3.4. Bilgisayar Yoluyla Sahtecilik

Kendisine veya başkasına yasa dışı ekonomik yarar sağlamak veya kişilere zarar vermek amacıyla; bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturulması veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapılmasıdır.

Günümüzde grafik yazılım fonksiyonlarının artmasıyla, ticari alanda kullanılan form ve belgelerin sahtesini yapmak oldukça kolaylaşmıştır. Modern teknoloji, özellikle renkli lazer yazıcıların ve fotokopi cihazlarının gelişimi ile daha önceden üretilmesi çok zor olan belgelerin kopyalanmasını mümkün kılmıştır [12].

2.3.5. Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Ulusal ve uluslararası telif sözleşmeleri ve kanunlarla lisans hakkı korunan yazılım ürünlerinin, yetkisiz olarak kopyalanması, çoğaltılması, dağıtılması ve ticari olarak kullanılmasıdır [14].

2.3.5.1. Lisans Sözleşmesine Aykırı Kullanma

Tek bir bilgisayar için kullanımı yasal olan bir yazılımın, birden fazla bilgisayarca paylaşılarak kullanılmasıdır. Yazılım lisansları genellikle tek bir bilgisayarda kullanılmak üzere tanzim edildiğinden, ayrıca ek lisans alınmaması halinde diğer bilgisayarlarca da

kullanılması durumunda lisans sözleşmesi ihlâl edilmiş olur. Tüm bilgisayarlar için ayrı ayrı lisans alınması şarttır [12].

2.3.5.2. Lisans Haklarına Aykırı Çoğaltma

Lisans Sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kopyalanmasıdır. Genel itibariyle; ödemeden kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılım, başka bir medya ortamına taşınır. Burada söz konusu yazılımı kopyalayan da kopyalatan da sözleşmeyi ihlal etmiş olmaktadır [12].

2.3.5.3. Lisans Haklarına Aykırı Kiralama

Değişik medyalar üzerine kayıtlı oyun, film ve yazılım programlarının lisans haklarına aykırı olarak kiralanmasıdır [12].

2.3.6. Yasadışı Yayınlar

Yasadışı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılmasıdır. Kanun tarafından yasaklanmış her türlü materyalin web sayfaları, elektronik postalar, haber grupları, sosyal paylaşım siteleri ve her türlü veri saklanabilecek optik medyalar gibi dijital kayıt yapan sistemler vasıtasıyla saklanması, dağıtılması ve yayınlanmasıdır [12].

2.3.6.1. Terör İçerikli Yayınlar

Terör örgütleri yardım toplamak, gelir elde etmek, terör örgütünün aldığı kararları ve izleyeceği politikaları yayımlamak, taraftar toplamak ve eleman temin etmek, topluma nifak sokarak bölücülük yapmak ve bunun propagandasını gerçekleştirmek, devletin faaliyetlerini kötüleme, karalama ve hakaret, terör örgütünün eylemlerini yönlendirme, terör örgütünün toplumsal hareketlerini organize etme, toplum nazarında sempati oluşturmaya çalışma, geniş kitlelere hitap etme, baskı yapma ve yaratma gibi eylemlerini kitap, doküman, broşür, gazete, dergi ve el ilanları vasıtasıyla gerçekleştirmekteydiler.

Günümüzde ise bilişim teknolojilerinin gelişmesi ve internetin yaygınlaşmasıyla bu tür faaliyetleri bilişim ortamlarına taşımışlardır. Terör örgütleri bununla da yetinmeyip, kamu kurumlarının veya özel şirketlerin bilişim sistemlerine sızmaya çalışarak bu sistemleri işlemez hale getirmeye çalışmaktadırlar [21].

Sempatizanlarını eğitmek maksadıyla oluşturdukları web sayfalarında amaçlarına hizmet edecek zararlı içerikler paylaşmaktadırlar. Bu sitelerde teröristin el kitabı, teröristin yemek kitabı gibi dokümanlara yer verilmekte ve bomba yapımından suikast hazırlığına kadar bir teröristin bilmesi gereken birçok konuda ayrıntılı bilgiler yer almaktadır [22].

2.3.6.2. Pornografik Yayınlar (Çocuk Pornosu Yayınları)

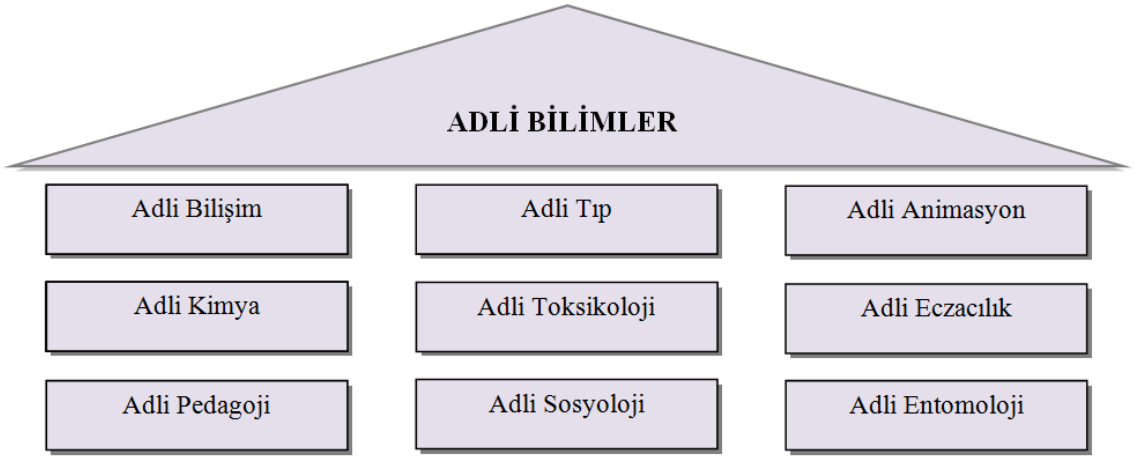
Çocuk pornografisi, genel anlamda 18 yaş altındaki kız ve erkek çocuklarının cinsel istismarını içeren filmler ve resimlerden oluşan, uluslar arası olarak da yasaklanmış zararlı pornografi türüdür [14].

Çocuk pornografisi internet aracılığıyla çocuklara gelebilecek en büyük zararlardan birini oluşturmaktadır. Çocuklara yönelik pornografik içerikler ve bu içeriklerin hazırlanmasında çocukların kullanılması birçok yabancı ülke ceza hukukunda suç tipi olarak düzenlenmiştir. Bu önemli konu, hem çocukların bu içeriklerden etkilenmesi ve hem de çocukların bu içeriklerin elde edilmesinde nesne olarak kullanılması açısından Avrupa Birliği'nin ve Avrupa Konseyi'nin üretmiş olduğu belgelere konu olmuşlardır. Özellikle Avrupa Siber Suç Sözleşmesi'ne göre sözleşmeci devletlere bu alanda önemli ve ciddi düzenlemeler yapma yükümlülüğü getirilmiştir [23].

3.ADLİ BİLİŞİM

3.1.Adli Bilişim Nedir

Topluma zarar verdiği ya da tehlikeli olduğu kanun koyucu tarafından kabul edilen ve belirtilen eylem, davranış ve hareketlere suç denir [24]. Suçun var olduğu yerde suçlunun bulunması ve hukuk sistemi tarafından belirli kurallar çerçevesinde yargılanması gerekliliği doğmaktadır. Aksi halde ünlü düşünür Platon'a göre "en yüce erdemlerden biri" olan adalet kavramından söz edilmesi mümkün olmayacaktır. Suçun ve suçlunun tespiti; detaylı araştırmaların yapılması, delillerin toplanması, bu delillerin derin bir analizinin yapılması ve elde edilen bulguların ilgili otorite makamına sunulması gibi süreçler sonucu mümkün olabilmektedir. Delillerin bulunması, analiz edilmesi, incelenmesi ve gerekli biçimlerde adli makamlara sunulması, hukuk bilimi üst başlığı altında çeşitli alt bilim dallarının meydana gelmesine neden olmuştur. Bunlardan bazıları adli bilişim, adli tıp, adli psikoloji ve birçok adli ile başlayan bilim dalı olarak sıralanabilir [25].



Şekil 1. Adli bilimler

Teknolojik gelişmelerin paralelinde delil kaynakları da değişmiştir. 19. yüzyılda adli anlamda kullanılan en önemli delil kaynağı günümüzde de çok yaygın olarak kullanılan parmak izi olarak kabul edilirken, 20. yüzyılda silahlı olayların aydınlatılması için yapılan tespit işlemlerinde kurşuna ait balistik raporları en fazla gündeme oturan adli delil yöntemlerinden biri olmuştur. Günümüzde ise suçların büyük bir kısmı, bilişim sistemleri kullanılarak ya da doğrudan bilişim sistemleri üzerinde işlendiği için birçok delilin bilgisayar ya da diğer elektronik araçlar üzerinde bulunduğunu görülmektedir [25].

Klasik kâğıt dokümanlar yıllardan beri keşif prosedüründe talep edilmektedir ve hâkimler ve avukatlar kâğıt formdaki delillere aşinadır. Ancak şimdi davanın tarafları ve vekilleri, yine keşif prosedüründe bu defa, bilgisayar tabanlı delillerin delil değerini anlamaya başlamışlardır. Mahkemeler, avukatlar ve davanın tarafları dikkatlerinin bilgisayar sabit disk sürücülerine, zip disklere, cep telefonlarına, avuç içi bilgisayarlara ve bunun gibi birçok bilgi teknolojisi aracının keşfine yöneltmişlerdir. Delillerin bu yeni şekilleri keşfe yeni bir boyut kazandırmış ve "adli bilişim (computer forensic)" adlı yeni bir bilim dalının doğmasına sebep olmuştur [20].

Terimin kökeni, İngilizce orijinal ismi ile Computer Forensics'tir. Bu kavram, bilgisayar anlamındaki computer ile; mahkemeye ait olan, adli anlamlarına gelen forensic kelimelerinden oluşmaktadır. Dilimize tam çevrildiğinde Adli Bilgisayar gibi bir anlam ortaya çıkmakla birlikte, ağırlıklı olarak Adli Bilişim terimi tercih edilmektedir. İfade etmek gerekir ki, Adli Bilişim yerine Bilgisayar Kriminalistiği de kullanılabilmektedir [27].

3.1.1. Sayısal Veri Kavramı

Bilgisayarlar ve verileri otomatik olarak işleyen elektronik cihazlar ikili sayı sistemini kullanırlar. İkili sayı sistemi 1 ve 0'dan oluşur. Harfler, rakamlar, görüntüler ve sesler kısacası her türlü bilgi sadece bu iki sayının bir kombinasyonu olarak saklanabilir.

Bilgisayarın içinde 0 ve 1 sayıları çok küçük elektronik devreler üzerinde elektrik akımı olarak kaydedilir. Bir devre elektrik akımı taşıyorsa 1, taşımıyorsa 0'dır. Bilgisayara girilen tüm girdiler akımların varlık ve yokluklarının farklı kombinasyonları biçiminde kodlanmıştır. Her bir elektronik devre 1 bit'lik veri oluşturur. 8 bitlik grup ise byte olarak adlandırılır. Ayrıca bilgisayarda depolanan ve ağ üzerinden aktarılan veriler de hep bu iki sayının kombinasyonlarıdır [28].

3.1.2.Dijital Delil Kavramı

Dijital/ elektronik delil; elektronik ya da manyetik ortamlarda saklanan veya bu araçlar aracılığıyla iletilen, soruşturma açısından değeri olan ve mahkemeye delil olarak sunulabilen her türlü veridir. Dijital deliller, klasik delillerden farklılık arz eder. Klasik deliller, gözle görülebilen, üzerinde el koyma, muhafaza altına alma kararı verilerek

kolayca götürülebilen deliller iken; dijital deliller, bu kadar somut bir yapıya sahip değildir. Elde edilmesi ve muhafazası çeşitli işlemler gerektirmektedir [29].

Dijital delil olarak elektronik aygıtlardan elde edilebilecek ve delil oluşturabilecek bulgular şunlar olabilir:

- Video görüntüleri
- Fotoğraflar
- Yazı dosyaları (word, excell, open office vb. dosyaları)
- Çeşitli bilgisayar programları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları)
- Gizli ve şifreli dosyalar / klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan internet siteleri
- İnternet ortamından indirilen (download) dosyalar
- İnternet ortamından indirilmiş ve sonradan silinmiş dosya/klasörler
- Hard diskler, CD, DVD ve Disketler
- USB Hardisk ve USB Flash Diskler
- ZIP, DAT, DLT gibi teyp veri yedekleme birimleri
- Hafıza Kartları (SD, MMS, CF, MemoryStick vs)
- Dijital Kameralar, Fotoğraf Makinelerinde ve MP3 Çalarlar
- El bilgisayarları (PDA, PALM, PocketPC vs)
- Cep Telefonları
- Oyun Konsolları
- Bazı Yazıcı ve Faks Cihazları
- Network Cihazları (Hafızaları varsa)
- İnternet ve Network Ortamları (Canlı Akışkan Delil)

3.2. Adli Bilişimin Tarihçesi

18 Ekim 1966 Minneapolis Tribune Gazetesinde ” Bilgisayar Uzmanı Banka Hesabında Tahrifat Yapmakla Suçlanıyor” başlıklı bir haber yer almıştır.

Habere göre Amerika Birleşik Devletleri'nde Federal Polisin ilk olarak tespit ettiği bu olayda; 1996 yılında Minneapolis City Bank'ın bilgisayarlarının programlanmasından ve bakımından sorumlu olan kişi maddi olarak zor durumda olduğu için bankadan hesabının üzerinde para çekmiştir. Banka programında gerçekleştirdiği değişiklik sayesinde sistemin bu durumu tespit etmesini önlemiştir. Aslında programda yaptığı bu değişikliği üç günlüğüne uygulamayı düşünmüştür fakat unutunca aradan 4 ay geçmiş ve fazladan çektiği para miktarı 1352 doları bulmuştur. Bu manipülasyon olayı, bir gün bankanın bilgisayar sisteminin çökmesi üzerine, bütün işlemler yine eskiden olduğu gibi elle yapılmaya başlanmış ve fazla miktarda çekilen para bu şekilde ortaya çıkmıştır. Bu olay banka için o kadar anlaşılmazdır ki işin çözümü için FBI çağrılmıştır. Bu ve benzeri birçok olayın ABD'de yaşanması bilişim alanında ilk hukuk düzenlemelerinin burada yapılmasına neden olmuştur [30].

Bilişim suçlarıyla ilgili ilk yasa tasarısı, ABD kongresinde 1977 yılında verilmiş olup bu adım sonraki yasal düzenlemeler ve uygulamalar açısından büyük önem arz etmektedir. ABD' de ilk defa 1984 yılında Erişim Aygıtlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu İle Kredi Kartı Sahtekârlığı Kanunu ihdas edilmiştir.

Amerika' da teknolojik suçlarla mücadele amacıyla; FBI Infrastructure Protection Center (FBI Altyapı Koruma Merkezi), Information Technology Association of America (Amerika Bilgi Teknolojileri Derneği), Trap and Trace Center (Yakalama ve İzleme Merkezi) ve Carnegie Mellon's Emergency Response Team (Carnegie Mellon Acil Durum Müdahale Ekibi) ile bazı üniversiteler bünyesinde kurulan birimler bunların en önemlilerindendir. FBI bilgisayar sistemlerine girme ve benzeri suçları takip amacıyla birimler kurmuş; diğer kuruluşlar da bilişim suçları ile mücadele için özel ekipler oluşturmuştur [31].

Türkiye'de ise ilk bilişim suçu 1999 yılında Türkiye'nin en büyük internet servis sağlayıcısı bilgisayar sistemlerine girilmesi şeklinde ortaya çıkmıştır. Suçu işleyen kişi Türkiye Cumhuriyeti'nin resmi olarak yargıya intikal eden ve ceza alan ilk kırıcısı (hacker) olarak literatürde yer almıştır. Hukuk fakültesi kitaplarında, derslerinde işlenen olay sonrası verilen 1 yıl 8 ay hapis cezası, infaz edilmeden ertelenmiştir.

Bahsedilen iki örnek resmi olarak yargılanan ve medyada yer alan dünyada ve Türkiye'de ilk bilişim suçunu anlatmaktadır. Yargıya intikal etmeyen bunun gibi daha birçok bilişim suçunun olduğu düşünülmektedir [30].

3.3. Adli Bilişimin Alt Dalları

3.3.1. Bilgisayar Adli Bilişimi

Adli bilişimin en çok kullanılan ve yaygın olarak bilinen alt disiplinidir. Bilgisayar adli bilişimi (computer forensic), adli bilişim alt dalları arasında ilk olarak ortaya çıkmış bir disiplindir ve temeli veri kurtarma projesine dayanmaktadır. Adli vakaların birçoğunda suçla ilgili deliller bilgisayarlarda yer alır. Bilgisayarlar başlı başına büyük miktarda veriyi taşıyabilen, kendine has logları oluşturan, e-posta işlemlerinin yapıldığı, dâhili sabit diskinin bulunduğu, kullanıcı hesaplarının yönetilebildiği ve en yaygın kullanılan elektronik cihazlar olması nedeni ile adli makamlar için çok önemli bir veri kaynağı konumundadır. Bu nedenle olayı aydınlatılacak deliller genelde maktulün ya da olay yerinde bulunan herhangi bir bilgisayarın incelenmesi ile elde edilebilir [27].

3.3.2. Bilgisayar Ağlarına Yönelik Adli Bilişim

Bilgisayar ağlarına yönelik adli bilişim (network forensic), temel olarak ağ trafiğinin analiz edilmesine dayanmaktadır. Ağ trafiğinin izlenmesi, analiz edilmesi ve analiz neticeleri doğrultusunda adli makamlara gerekli bilgilerin verilmesi şeklinde ifade edilebilir. Ağda yapılan incelemeler sonucu elde edilen veriler gerektiğinde erken uyarı sistemleri için kullanılabilir ya da depolanıp belirli zaman aralıklarında analiz edilebilirler [32,33].

3.3.3. Olaya Müdahale

Adli bilişim uzmanlarının bazıları tarafından farklı bir disiplin olarak görülmesine rağmen olaya müdahale (incident response) adli süreçlerin başlatılmasına neden olmasından dolayı bir adli bilişim alt disiplini olduğu şeklindedir. “incident response” tanımındaki “incident” den kasıt ağ güvenliğine karşı bir atak ya da güvenlik ihlali olduğu durumlardır. Organizasyonlara karşı yapılan saldırı ya da güvenlik ihlalleri korsanlardan, kurum içindeki personelden, bilinçsiz kullanıcılardan, zararlı kodlardan, truva atlarından ya da herhangi bir zararlı yazılımdan kaynaklanabilir. Olaya müdahelede asıl amaç ağa yapılan saldırıların ya da güvenlik ihlallerinin saldırı yapan kişilerden habersiz olarak

tespit edilip takip edilmesi ve bu süreçte adli makamlar için delil teşkil edecek verilerin elde edilmesidir [32].

3.3.4. Cep Telefonlarına Yönelik Adli Bilişim

GSM telefonları içerisinde tutulan servis sağlayıcılara ait fatura bilgileri ya da CDR (call detailed record) adı verilen arama detay kayıt bilgilerinin elde edilmesini sağlayan adli bilişim alt disiplinidir [32]. CDR bilgileri; kişinin ne zaman, kim ile, ne kadar süre görüştüğü bilgilerini tutmaktadır. Bu bilgiler birçok adli olayda ihtiyaç duyulan ve olayın çözülmesini sağlayan bilgilerdir. Bunun yanında günümüzde telefonların artan sabit disk kapasiteleri, e-posta alıp gönderebilmeleri, ses kaydı yapabilmeleri, fotoğraf çekebilmeleri gibi birçok fonksiyonu telefonları adli bilişim açısından oldukça değerli kılmaktadır.

Yukarda bahsedilen verilerin çoğu cep telefonuna ait sabit diske kaydedilmekte ve silinebilmektedir. Böylece gerektiği zaman bu verilerin kurtarılması söz konusu olabilmekte ve delil olarak adli makamlara sunulabilmektedir. Piyasada binlerce GSM telefonu modeli bulunması ve yapılacak incelemelerin bazı durumlarda model bağımlı olması, bu disiplinin en zayıf olduğu noktadır.

3.3.5. GPS'e Yönelik Adli Bilişim

GPS (Global Positioning System- Küresel Konumlandırma Sistemi), düzenli olarak kodlanmış bilgi yollayan bir uydu ağıdır ve uydularla arasındaki mesafeyi ölçerek dünya üzerindeki kesin yeri tespit etmeyi mümkün kılar [34]. Günümüzde aktif bir biçimde kullanılmaya başlanması ile beraber GPS birimlerine ait teknolojik ilerlemelerde de büyük aşamalar kaydedilmiştir. Kiralanan araçlarda, taşımacılıkta, askeri alanda, haritacılıkta, havacılıkta ve çeşitli araştırmalarda GPS sistemlerinden faydalanılmaktadır.

GPS forensic gelişmiş GPS birimlerinin analizini içeren bir disiplindir. Gelişmiş GPS birimleri, araçların ziyaret ettikleri yerleri, favori yerleri ve araması yapılan yerleri zaman bilgisi ile beraber tutması nedeni ile ölümcül kazalar gibi önemli adli durumlarda ilgili aracın o anda orada olup olmadığı ile ilgili kararlarda önemli bir veri kaynağı olarak kullanılabilir [32, 34].

3.3.6. Medya Aygıtlarına Yönelik Adli Bilişim

PDA, Tablet PC, USB bellekler, taşınabilir sabit diskler, sayısal müzik oynatıcılar, ses kayıt cihazları, kameralar ve bunun gibi elektronik cihazlar günümüzde çok yaygın olarak kullanılmaktadır. Bu cihazlarla uygunsuz ses kaydı yapmaktan, çocuk pornosu ihtiva eden videolar izlemeye kadar çok çeşitli suçlar işlenebilmektedir. Bu cihazlar üzerinde taşınan tüm veriler ve zaman damgaları sabit disklerde bulunmaktadır. Medya aygıtlarına yönelik adli bilişim bu verilerin kurtarılması ve adli makamlara sunulması ile ilgilenen bir alt disiplin olarak karşımıza çıkmaktadır [32].

3.3.7. Sosyal Ağlara Yönelik Adli Bilişim

2000'li yıllardan itibaren sosyal ağların popülaritesinin arttığı görülmektedir. Sadece Harvard Üniversitesi'ndeki öğrencilerle başlayan facebook serüveni bugün dünyada 800 milyonu aşkın kullanıcısıyla devam etmektedir. Bunun dışında en çok kullanılan sosyal ağlara örnek olarak twitter, myspace ve linkedin verilebilir. Kişiler üyesi oldukları sosyal ağlarda çok fazla zaman geçirmekte, aile, iş ve arkadaş çevresi ile iletişim kurabilmektedir. Üye oldukları gruplar, beğenileri, fotoğrafları, katıldıkları etkinlikler, o an nerede ve kiminle oldukları ile ilgili detaylar diğer insanlar tarafından görülmekte böylece mahremiyet kavramı tamamen ortadan kalkmaktadır. ABD'li psikoloji profesörü Rowland Miller, 30 yıllık araştırmalarına dayanarak facebook gibi sosyal paylaşım sitelerinin utanma duygusunu yok ettiğini ortaya koymuştur. Miller'a göre, insanların hayatlarının bütün detaylarını tüm dünyayla paylaşmalarını sağlayan facebook gibi sosyal paylaşım siteleri utanma duygusunu yok etmektedir. Bu cümle, 30 yıl boyunca utanma duygusu üzerine araştırma yapan ABD'li psikoloji profesörü Rowland Miller'ın ulaştığı sonucu özetlemektedir [35].

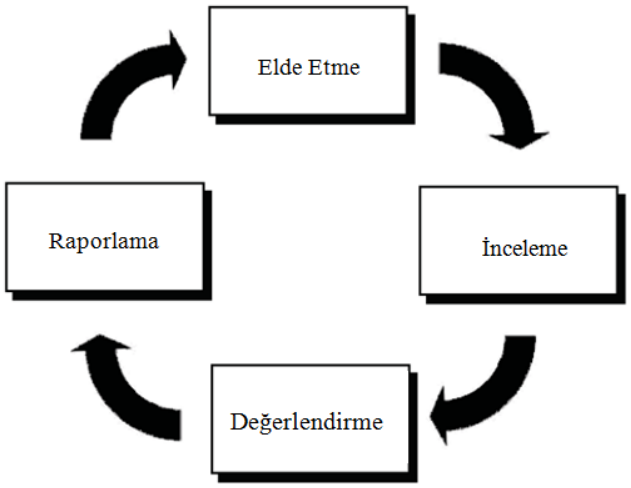
Sosyal ağlarda insanlar kendi kişiliklerini, hayatlarını farklı yansıtarak adeta başka bir kişiliğe bürünerek var olmakta ve bunun sonucunda suç diye nitelendirilebilecek birçok davranışın altına imza atmaktadırlar. Gerek direkt sosyal ağlar üzerinden gerçekleşen tehdit, hakaret, hesap çalma gibi suçlarda gerekse gerçek hayatta gerçekleşen ve sosyal ağlar üzerinden ipuçlarına ulaşılabilen suçlarda verilerin incelenmesi, analiz edilmesi ve adli makamlara sunulması ile sosyal ağlara yönelik adli bilişim disiplini ilgilenmektedir [32, 35].

3.4. Adli Bilişim Süreçleri

Elektronik delillerin klasik delillerden farklı özellikler taşıması, delillere ulaşma konusunda da bazı farklılıklar ortaya çıkarmaktadır. Örneğin bir cinayet vakasında olay yerinde bulunan bir silah çok büyük ihtimalle suçun delilidir ve muhafaza altına alınarak incelenmek üzere götürülebilir. Fakat söz konusu dijital deliller olunca durum çok daha karmaşık bir hale gelir. Ortamda bulunan elektronik aygıtlarda suçla ilgili delil bulunup bulunmadığı belli değildir. Suç mahallinde bulunan bir bilgisayar bu duruma örnek gösterilebilir. Bu bilgisayarın suçta kullanılıp kullanılmadığı, suça ilişkin bir delil içerip içermediği meçhuldür. Şüphesiz silah örneğinde de bu belirsizlik mevcuttur fakat ortamda bulunan elektronik aygıtta bu belirsizlik daha çok daha fazladır.

Muhafaza altına alınan dijital bir delilin incelenmesi de şüphesiz klasik delillere göre daha zordur. Dijital delillerin elde edilmesi, muhafazası, incelenmesi ve analizi teknik açıdan bilgi gerektiren, sabır ve dikkatle yürütülmesi gereken bir süreçtir. Ayrıca çoğu zaman çeşitli donanım aygıtları ve yazılımlar kullanmayı gerektirir ki bu açıdan da oldukça pahalı bir süreç olduğunu söyleyebiliriz.

Çeşitli yöntemlerle elde edilen dijital verilerin adli bilişimde hukuki bir delil niteliği taşıması için belli prosedürlerden geçmesi gerekir. Bu sürece adli bilişim süreci denir ve bu süreç 4 başlıkta incelenebilir [28].



Şekil 2. Adli bilişim süreçleri

3.4.1. Elde Etme Süreci

Olay yeri müdahalesi kriminalistik biliminde çok önemli bir yere sahiptir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz saptanması ve zarar görmeden toplanması ilk olay yeri müdahalesinin düzgün yapılmasıyla mümkündür [37]. Bilişim sistemlerinin veya elektronik cihazların veri depolama medyaları üzerinde bulunan, suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasında kullanılabilecek verilere "dijital veri" denir. Parmak izi ve DNA gibi gizli verilerde elektronik delil olarak nitelendirilir. Delil ihtiva etmesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin birebir alınmış kopyaları üzerinde gerçekleştirilmelidir. İnceleme için alınan birebir kopyaya bilgisayar kriminalistiğinde imaj (Forensic Image) adı verilmektedir. Elde etme süreci potansiyel veri depolama özelliği olan kaynakların yani dijital delillerin belirlenmesi, toplanması ve imajlarının alınarak incelemeye hazır hale getirmesi işlemlerini kapsar.

3.4.1.1. Dijital Deliller Nerelerde Bulunur?

Dijital deliller elektronik bir araç tarafından iletilen ya da bu araçlar tarafından kaydedilmiş ve soruşturma açısından değeri olan her türlü bilgi ile görüntü, ses, parmak izi, DNA gibi verilerdir. Dijital deliller, olay yeri sahnesinde ilk bakışta görünmeyen delillerdir. Bu delilleri görünür hale getirmek için bazı araçlara ve yazılımlara ihtiyaç vardır. Dijital deliller özel yapıları gereği oldukça hassastır. Yanlış bir işlem ya da yanlış bir inceleme sonucunda kolayca değiştirilebilir, tahrip edilebilir, yok edilebilir. Bu nedenle bu delil çeşidini toplamak, muhafaza etmek ve incelemek için özel önlemlerin alınması gerekmektedir. Bu yapılmazsa bu deliller ya kullanılamaz hale gelecektir ya da soruşturmanın yanlış sonuçlanmasına sebep olacaktır [38].

Dijital delilleri inceleme işlemini yürütecek kişinin bu alanda eğitimli ve tecrübeli olması gerekmektedir. Dijital delillerin gizli ve hassas yapısı göz önünde bulundurulunca yapılacak yanlış bir müdahale ya da bir delilin gözden kaçırılması ciddi sorunlara yol açabilmektedir.

Dijital deliller olay sahnesinde çok çeşitli cihazlar üzerinde bulunabilir. Teknolojinin hızlı gelişimiyle birlikte hayatımıza giren elektronik araçların çokluğu düşünülünce, dijital kanıtların bulunabileceği olası yerleri tespit etmenin de zorluğu gözler

önüne serilmiş olur. Buna, olayla ilgili çok ciddi bulguları ortaya çıkaran parmak izi, DNA, ses ve görüntü verileri de eklenince olay yerinin çok ciddi bir şekilde irdelenmesi gerçeği ortaya çıkmaktadır.

Dijital deliller aşağıdaki şekillerde olay yerinde bulunabilirler;

- ***Bilgisayar Sistemleri:*** Bir bilgisayar sistemi tipik olarak merkezi işlem birimi, veri kaydetme aygıtları, monitör, klavye ve fareden oluşmaktadır. Bilgisayar sistemi bağımsız olabileceği gibi, bir ağa da bağlı olabilir, dizüstü, masaüstü, minibilgisayar ve büyük boy bilgisayarlar gibi birçok farklı bilgisayar sistemi mevcuttur. Bilgisayar sistemlerinde ilave bileşenler olarak; modemler, yazıcılar, tarayıcılar, harici kayıt aygıtları gibi birçok aygıt bulunabilmektedir. Dijital deliller daha çok sabit disk ve diğer depolama cihazları üzerinde bulunmaktadır. Bunlar adres defterleri, e-posta dosyaları, ses/video dosyaları, görüntü/grafik dosyaları, takvimler, internette en çok ziyaret edilen siteler, veri tabanı dosyaları, elektronik çizelge dosyaları, doküman ve metin dosyalarıdır. Ayrıca bu veriler kullanıcı tarafından koruma altına alınmış ve ya gizlenmiş olabilir. Kullanıcıların delilleri birçok değişik şekilde gizleme imkânları mevcuttur. Örneğin kendileri için önemli bir veriyi şifreleyebilir veya parola korumalı hale getirebilirler. Yine kullanıcılar sabit disk üzerinde veya diğer dosyalar içinde veya kasten yanlış bir isim vererek yarattığı bir dosya içinde bir suçun delilini gizleyebilirler. Deliller bilgisayar işletim sisteminin rutin bir işlevi olarak oluşturulan dosyalar veya diğer veri alanları içerisinde bulunabilirler [38].
- ***Masaüstü ve Laptop Bilgisayarlar:*** Elektronik keşif sırasında karşılaşılan bilgisayarların çoğunluğunu masaüstü ve laptop bilgisayarlar oluşturmaktadır [38]. Dijital delillerin zarar görmemesi ve yok olmaması için bilgisayarların açık ya da kapalı olması durumunda yapılacak işlemler farklıdır. Eğer olay yerindeki bilgisayarlar kapalı ise kesinlikle açılmamalıdır, eğer açık ise güç kabloları çıkarılarak kapatılmalıdır. Aksi halde veri kayıpları yaşanması muhtemeldir.
- ***Erişim Kontrol Araçları (Acces Control Devices):*** Akıllı kartlar, konnektörler, biyometrik tarayıcılar; üzerlerinde dijital delillerin olması muhtemel cihazlardır. *Akıllı kart*; şifreleme anahtarlarını, onay bilgilerini (örneğin parola), dijital sertifika ve ya diğer bilgileri saklayabilen bir mikroişlemci ihtiva eden, küçük

avuç içi kadar aygıtlardır. *Konektörler* de akıllı kart üzerindeki bilgilere benzer bilgileri ihtiva eden, bilgisayarın portlarına takılabilen küçük aygıtlardır. *Biyometrik Tarayıcı* ise bireylerin fiziksel özelliklerini (retina, ses, parmakizi gibi) teşhis edebilen, bir bilgisayar sistemine bağlı parçalardır. Tüm bu aygıtlar bir şifreleme anahtarı olarak bilgisayara, programlara veya fonksiyonlara erişimin kontrol altında tutulmasını sağlarlar. Kart üzerindeki teşhis/onay bilgileri, erişim seviyesi, yapılanışlar, izinler ve bizzat aracın kendisi delil olarak kullanılabilecektir [38].

- ***Avuçiçi Aygıtlar (PDA) ve Akıllı Telefonlar:*** *PDA;* bilgi işlem, telefon/faks, çağrı sistemi, ağ oluşturma (networking) ve diğer özelliklere sahip küçük aygıtlardır. Bu araçlarda yer alan adres defterleri, takvimler, dokümanlar, el yazıları, parolalar, yazılı mesajlar, sesli mesajlar, e-postalar potansiyel delillerdir [38]. *Akıllı telefonlar* ise işletim sistemine (örnek: symbian, android, ios, bada, os) sahiptir. Bu işletim sistemleri kendi üzerlerinde uyumlu programların kurulmasına olanak sağlamaktadırlar [39]. Uygulama programları kurabilir, internete bağlanabilir, dijital fotoğraf makinesi ve kamera gibi kullanılabilir, ses kaydı yapılabilir. Böylece akıllı telefonlar günümüzün vazgeçilmez teknolojisi haline gelmiş ve çok yaygın bir kullanım alanı bulmuştur. Akıllı telefonlara o yüzden küçük bilgisayar da diyebiliriz. Çünkü bu cihazlarda da tıpkı PC'ler gibi işlemci, hafıza, RAM, grafik ve ses gibi donanımlar mevcuttur. Hal böyle olunca akıllı telefonlar adli bilişim olaylarında dijital delilleri ihtiva etme olasılığı çok yüksek cihazlar haline gelmişlerdir. Ses kayıtları, videolar, fotoğraflar, yazılı mesajlar, telefon konuşmalarının kayıtları, seyahat günlükleri, ajandalar, takvimler, ziyaret edilen web sayfası adresleri olayların çözülmesinde kullanılabilecek dijital delillerdir.
- ***Sabit disk, CD, DVD, Hafıza Kartları, Taşınabilir Bellekler, Taşınabilir diskler:*** Verilerin saklanabileceği manyetik ve optik kayıt ortamlarıdır. Bilgisayarların içinde ya da dış ortamda bulunan bu birimler birçok dijital delil ihtiva ederler. Verilerin silinmiş olması onları delil olmaktan çıkarmaz. Çünkü çeşitli donanım ve yazılım araçlarıyla silinmiş bu veriler geri getirilebilmektedir.
- ***Ağ Bileşenleri:*** *Modemler*; bilgisayarın diğer bilgisayar sistemleri ve/veya ağlar ile telefon hatları, kablosuz veya diğer iletişim vasıtaları aracılığıyla bağlantısını sağlayarak, elektronik haberleşmeyi sağlar. Modemin bizzat kendisi potansiyel

olarak delil olabilmektedir [38]. Yerel alan ağı kartı, Ağ arayüz kartı (NIC), yönlendirici (router), hub, anahtar (switch), tekrarlayıcı (repeater) gibi ağ cihazları, sunucu bilgisayarlar, ağ kabloları ve konektörler dijital delillerin bulunması muhtemel ortamlardır.

- ***Küresel Konum Sistemleri (GPS- Global Positioning System):*** Küresel konum sistemleri hedef bilgileri, yol işaretleri ve yönlendiriciler aracılığıyla, yapılan seyahat hakkında bilgi verilmektedir. Bazıları önceki hedefleri depolamakta ve seyahat günlüklerini kapsamaktadır. Önceki hedefler, seyahat günlükleri, yol işaret koordinatları, yol işaret adları potansiyel delillerdir [38].
- ***Kredi Kartı Okuyucuları (POS Cihazları***): Kredi kartı okuyucuları, plastik kart üzerindeki manyetik şeridin ihtiva ettiği bilgileri okumak amacıyla kullanılmaktadır. Bu manyetik şerit üzerinde yer alan; kredi kartı numarası, kart sahibinin adresi ve adına ilişkin bilgiler, kredi kartının geçerlilik süresinin sona ereceği tarih gibi bilgiler potansiyel delillerdir [38].
- ***Yazıcı, Faks Makinaları ve Fotokopi Makinaları:*** *Yazıcı*; bilgisayardan gelen verileri kâğıt ortamına döken aygıttır. Bazı yazıcılar, yazdırma işlemi yapılırken birden çok sayfadan oluşan dokümanları alma ve saklama özelliği sunan bir arabelleğe sahiptir. Yazıcılar kullanım loglarını, tarih ve zaman bilgilerini ve eğer ağa bağlı iseler, ağ kimlik bilgilerini ihtiva edebilirler. *Faks Makinaları*; programlanmış telefon numaralarını ve gönderilen veya alınan belgelerin tarihlerini depolayabilir. Ayrıca bazıları birden çok sayfanın fakslanması söz konusu olduğunda bunları önce tarayıp, daha sonra göndermek ya da gelen faksları hafızada saklayıp daha sonra yazdırma olanağını sağlayan bir belleğe sahiptir. Belgeler, film kartuşları, telefon numaraları ve gönderildi/alındı logları potansiyel delillerdir. Fotokopi makinelerinde kullanıcı erişim kayıtları ve çekilen fotokopilerin tarihi muhafaza edilebilmektedir. Dokümanlar, tarih ve zaman bilgileri, kullanıcı logları potansiyel delillerdir.
- ***Kamera ve Fotoğraf Makineleri, Ses Kayıt Cihazları:*** Bugün artık dijital sisteme bürünmüş olan kamera ve fotoğraf makinelerinde en sık karşılaşılabilecek delil, fotoğraf ve video dosyalarıdır. Bu tür cihazların verileri hafıza kartına depolamasının yanında ayrıca kendi hafızalarının bulunduğu da delil araştırmalarında gözden kaçırılmaması gereken bir husustur. Elde edilen fotoğraflar ve görüntüler çeşitli görüntü işleme teknikleriyle analiz edilerek

dijital deliller ortaya çıkarılabilir. Ayrıca ses dosyaları ses analizi işlemlerinden sonra olayla ilgili çok çarpıcı sonuçlar verebilmektedir.

- ***İnternet Ortamındaki Veriler:*** İnternet ortamındaki bilgilerde esasen bilgisayarlarda saklanmaktadır. Sunucu adı verilen ve web hizmeti sunan bu bilgisayarlar, web sitelerine ilişkin kayıtları ve çeşitli dosyaları barındırmaktadır. İnternet ortamında bulunabilecek deliller, e-postalar, internet sitelerinde yazılmış bir yorum, sosyal paylaşım sitelerinde paylaşılmış bir öğe ya da mesaj gibi değişik biçimlerde olabilir. Bunlar da dijital delil olarak suçun aydınlatılmasında kullanılabilir [29].

3.4.1.2. Dijital Deliller Toplanırken Nelere Dikkat Edilmelidir?

Dijital deliller çok hassas yapıda oldukları için kolayca zarar görebilirler. Bu nedenle dijital deliller toplanırken dikkat edilmesi gereken bir takım kurallar vardır. Olay yerinde bulunan bilgisayarın kapalı ya da açık olması durumunda uygulanacak işlemler farklıdır. Bu işlem basamakları aşağıda verilmiştir.

A) Olay yerinde rastlanılan bilgisayarın kapalı olması durumunda;

1. Delilin bulunduğu alan güvenlik ve kontrol altına alınmalıdır.
2. Diğer insanlar bilgisayardan ve güç ünitesinden uzaklaştırılmalıdır.
3. Hiçbir koşul altında bilgisayar açılmamalıdır.
4. Bilgisayarın tam olarak kapalı olduğundan emin olunmalıdır. Bazı ekran koruyucular bilgisayarın kapalıymış gibi gözükmesine neden olabilir. Bunu anlamak için kasa üzerideki sabit disk aktivite ışığını kontrol edilir. Aktivite varsa bilgisayar çalışıyordur.
5. Dizüstü bilgisayarların kapağı açıldığı zaman çalışmaya başlayabileceği için kapağı açılmamalıdır.
6. Güç kablosu öncelikle bilgisayar kasasından, daha sonra duvardaki prizden sökülmelidir.
7. Kasaya bağlı olan iletişim hatları ve diğer kablolar uygun şekilde çıkarılmalıdır.
8. İmkânlar el veriyorsa olay yeri kameraya alınmalı, fotoğrafları çekilir veya krokisi çizilmelidir.
9. Bilgisayara bağlı olup da sökülen kablolar etiketlenmelidir.
10. Parçaları taşımak için uygun kutular ve delil torbaları (anti statik) kullanılmalı

ve hareket sırasında zarar görmemesine dikkat edilmelidir.

11. Bilgisayarın toplandığı alanın etrafında bulunan kâğıtlar, not defterleri ve günlükler şifrelerin bulunabileceği düşünülerek incelenmelidir. Ayrıca olay yerinde bulunan, sıradan gibi görünen nesnelerin aslında elektronik bir aygıt olabileceği göz önünde bulundurulmalıdır. Kalem şeklinde kameralar bu duruma örnek verilebilir.

12. Bilgisayar sahibine bilgisayarın herhangi bir yerinde şifre olup olmadığını varsa ne olduğunu sorulur cevap verirse not alınmalıdır.

13. Delillerin toplanması aşamaları basamak basamak yazılmalıdır.

B) Olay yerinde rastlanılan bilgisayarın açık olması durumunda;

1. Delilin bulunduğu alan güvenlik ve kontrol altına alınmalıdır.

2. Diğer insanlar bilgisayardan ve güç ünitesinden uzaklaştırılmalıdır.

3. Modem'in kablosu bağlı ise sökülmelidir.

4. Bilgisayarın kablosuz bir ağa bağlı olduğunu düşünülüyorsa bir uzmandan yardım alınmalıdır.

5. Bilgisayar sahibinden yardım alınmamalıdır ve yardım teklifi kabul edilmemelidir.

6. Klavyeye dokunulmamalı ve fare ile tıklama yapılmamalıdır.

7. Ekran kapalıysa farenin tuşlarına tıklamadan hareket ettirilmelidir. Eğer ekran görüntüsü gelir ve şifre sorarsa sonraki adıma geçilmelidir. Şifre sorulmaz ise ekranın görüntüsü fotoğraflanmalı, hiçbir program kapatılmamalı veya açılmamalıdır.

8. Kasanın arkasında bulunan güç kablosu yavaşça çıkarılmalı, daha sonra duvardan sökülmelidir. Bu adım eğer bilgisayara bağlı bir UPS (kesintisiz güç kaynağı) var ise sabit diske veri yazılmasını engellemek içindir.

9. Kasaya bağlı olan iletişim hatları ve diğer kabloları uygun şekilde çıkarılmalıdır.

10. İmkânlar el veriyorsa olay yeri kameraya alınmalı, fotoğrafları çekilmeli veya krokisi çizilmelidir.

11. Bilgisayara bağlı olup da sökülen kablolar etiketlenmelidir.

12. Parçaları taşımak için uygun kutular ve delil torbaları (anti statik) kullanılmalı ve hareket sırasında zarar görmemesine dikkat edilmelidir.

13. Bilgisayarın toplandığı alanın etrafında bulunan kâğıtlar, not defterleri ve günlükler şifrelerin bulunabileceği düşünülerek incelenmelidir.

14. Bilgisayar sahibine bilgisayarın herhangi bir yerinde şifre olup olmadığını varsa ne olduğunu sorulup cevap verirse not alınmalıdır.
15. Delillerin toplanması aşamaları basamak basamak yazılmalıdır. Bilişim suçu vakalarında, olay yeri incelemesi yapıldıktan sonraki aşama el koyulan delillerin veri (data) inceleme laboratuarına sevk edilmesidir. Elde edilen delillerin laboratuara taşınırken her hangi bir zarara uğramamaları için azami gayret gösterilmeli ve her delil için ayrı ayrı tedbirler alınmalıdır [40].

3.4.2. İnceleme Süreci

İnceleme sürecinde, toplanan veri kaynaklarının kopyaları alınmakta ve yapılacak her türlü çalışma alınan kopyalar üzerinde yapılmaktadır. Bu kopyalara "forensic image" adı verilmektedir. Burada incelenen delilin veri bütünlüğünün korunması esastır. Yani delile el konulduğu ilk andan itibaren araştırma boyunca orijinalliğinin korunması sağlanmalıdır [37].

Adli bilişim alanında yapılan tüm inceleme ve analizler delilin orijinalinde herhangi bir değişiklik meydana gelmemesi için, özel yazılım ve donanım araçları ile alınmış bire bir kopyaları üzerinde yapılmaktadır. Birebir kopya delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelmektedir. Alınan birebir kopya; mevcut verileri, silinmiş verileri, gizli bölümlerini, veri depolama biriminde bulunan diğer verileri de kapsar. Kullanılan "birebir aynısı" terimi, orijinal medyanın her sektör ve bayt'ının kopyalanması anlamındadır. Verinin kopyasında orijinal medyada bulunmayan en ufak bir bilgi olmamalıdır. İdeal bir kopyalama işlemi orijinal medya üzerinde herhangi bir değişiklik meydana getirmemelidir [41].

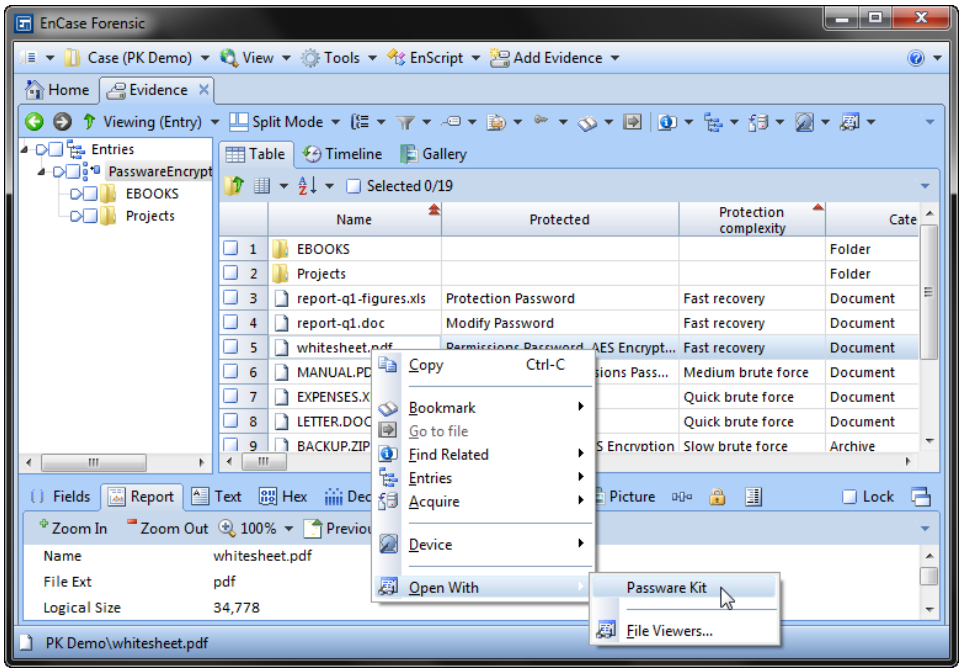
Adli bilişimde elektronik delillerin veri bütünlüğünün korunması genelde "hash fonksiyonu" denilen, matematik algoritması ile sağlanır. Hash fonksiyonu sonlu ve değişken uzunluktaki bir veriyi alıp sabit uzunlukta rastgele görünümlü bir çıktı üretmektedir. Her girdi için yalnız bir çıktı vardır. Girdideki bir bitlik değişim bile, çıktıda öngörülemez değişikliklere yol açarak bir öncekiyle ilişkilendirilemeyecek yeni bir çıktı vermektedir. Burada bahsedilen girdi; delil niteliği taşıyan bir dosya, bir mesaj ya da komple bir sabit disk olabilmektedir. Hash fonksiyonu sayesinde adli bilişim orijinal depolama ortamındaki veri ile kopyalanan verinin birebir aynı olup olmadığına karar verebilir. En çok kullanılan Hash algoritmaları MD-5 ve SHA-1'dir [42,43].

3.4.2.1. Adli Bilişimde Kullanılan Araçlar

Adli bilişim araçları, şüpheliye ait elektronik cihazlardan yazılım ya da donanım yolu ile delillerin elde edilmesini sağlayan araçlar olarak tanımlanabilir. Adli makamlarda elektronik delillerin adli delil olarak kullanılabilmesi için standartlaşmış ve yetkilendirilmiş makamlardan alınan adli bilişim yazılım ya da donanımı sertifikasına sahip araçlar tarafından elde edilmiş olması gerekmektedir. Amerika'da herhangi bir yazılım ya da donanımın adli bilişim makamlarında yasal olarak kullanılabilmesi için National Institute of Standarts and Technology (NIST) tarafından kabul edilmesi gerekmektedir. NIST bünyesinde bulunan Computer Forensic Tool Testing (CFTT) programı tarafından yapılan temel testleri geçmesi neticesinde yazılım ya da donanım adli bilişim amaçlı kullanılabilir sertifikası alabilmektedir. Adli süreçleri doğrudan etkilemesi neticesinde standartlaşma ve test süreçlerinin olması adli bilişim yazılım ve donanımları için çok önemlidir fakat ülkemizde bu konuda standartlaşma ve test makamı henüz bulunmamaktadır [44].

Adli bilişimde kullanılan yazılımlardan bazıları aşağıda verilmiştir [41, 45];

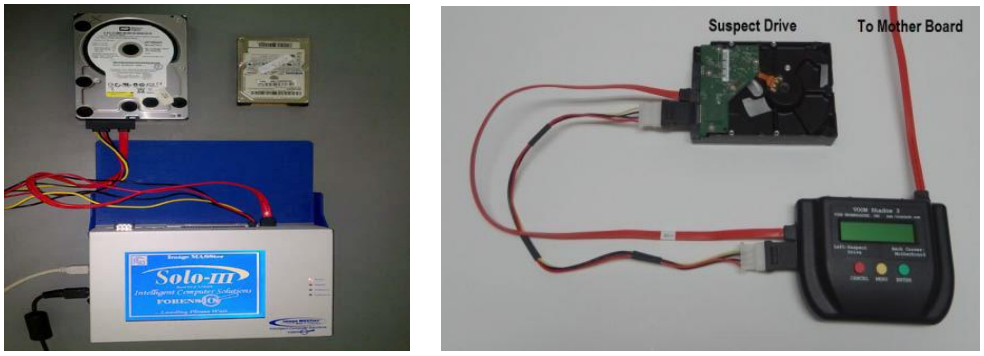
- Encase
- Forensic Tool Kit,
- ProDiscover,
- SMART,
- The Sleuth Kit/Autopsy
- Safe BACK
- Symantec Emergency Data Recovery
- Data Elimination Suite
- Encryption Linux Boot Disk
- Coroner's Toolkit,
- Knoppix STD



Şekil 3. EnCase- adli bilişim yazılımı

Adli bilişimde kullanılan donanımlardan bazıları aşağıda verilmiştir [41];

- PC3000
- Tableau yazma-koruma cihazları,
- Voom Technology cihazları,
- Solo-III kopyalama cihazları



Şekil 4. Adli bilişim araçları

Adli Bilişim Uzmanlığı için dünyaca geçerliliği olan sertifikasyonlar aşağıdaki gibidir [46];

- EnCase Certified Examiner (ENCE)
- Certified Computer Examiner (CCE)
- Certified Computer Crime Investigator (CCCI)
- Computer Forensic Computer Examiner (CFCE),
- Certified Information Forensics Investigator (CIFI)
- Professional Certified Investigator (PCI)
- Certified Cyber-Crime Expert(C3E)
- Advanced Information Security (AIS)
- Certified Computer Forensic Technician (CCFT)
- Certified Information Systems Auditor (CISA)
- GIAC Certified Forensic Analyst (GCFA)

3.4.3. Analiz Süreci

Sistemden imajı alınmış verilerin tümünün gözle görünür hale getirilmesinden sonra analiz aşamasına geçilir. Bu aşamada, yapılan analizler sonucu elde edilen verilerin hangilerinin ne ölçüde adli makamlara sunulmak üzere raporlanacağının tespiti yapılmaktadır [29]. En çok teknik bilgi gerektiren safhadır. Analiz safhası dört aşamada ele alınabilir; öncelikle herhangi bir işleme tabi tutulmadan okunabilir dijital veri nesnelerinin içeriği incelenerek bazı anlamsal verilere ulaşılabilir. Bu aşamaya *Değerlendirme* aşaması denir. Daha sonra *Deney* aşaması gelmektedir. Araştırma esnasında bazı yöntemlerin uygulanmasını kapsar. Tabi bu yöntemlerin bazı standart ve prosedürlere uyması ve ayrıntılı bir şekilde rapor edilmesi şarttır. Araştırma esnasında dijital ve dijital olmayan birçok kaynaktan veri toplanmaktadır. Sadece dijital deliller ya da sadece klasik deliller hikâyeyi aydınlatmaya yetmeyebilir. Anlamlı sonuçlara ulaşabilmek için verilerin bir araya getirilmesi gerekmektedir. Buna *Birleştirme* denir. Örneğin olayların oluş sırasına göre kronolojik bir sıraya konulması konu ile ilgili aydınlatıcı ipuçları verebilmektedir. Birleştirme esnasında verilerin içerik olarak da birbirleriyle ilişkili olup olmadığının incelenmesi ise *Korelasyon* olarak adlandırılır. Son aşama olarak *Onaylama* gelir. Kısaca analiz safhasının çıktısı ve sonucudur denilebilir. Bulgular pozitif delil olarak ilgili birimlere gönderilir [2].

3.4.4. Raporlama Süreci

Adli bilimcilerin en önemli görevlerinden biri de uygulanan sürecin adli makamlara aktarılmasıdır. Elektronik verilere uygulanan teknik işlemler ve elde edilen sonuçlar anlaşılır bir dille rapora aktarılmalıdır. Ayrıntılı olarak dijital delillerin nasıl elde edildiğine ilişkin teknik boyutu ve adli bilişimin hangi yöntemlerinin kullanıldığı da anlaşılır bir dille belirtilmeli, açıklayıcı bir rapor hazırlanmalıdır. Unutulmamalıdır ki iyi düzenlenmemiş ve doğru yazılmamış bir rapor olayın aydınlanmasını engelleyebilir [40].

Hazırlanan bu raporda ayrıca, olayla ilgili bilgiler, araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller, inceleme esnasında kullanılan yazılım ve donanımlar hakkında bilgiler, inceleme sırasında kullanılan yöntemler, araştırma sonunda ele geçen bulgulara ilişkin bilgiler yer almalıdır [29].

3.5. Türkiye'de Adli Bilişim

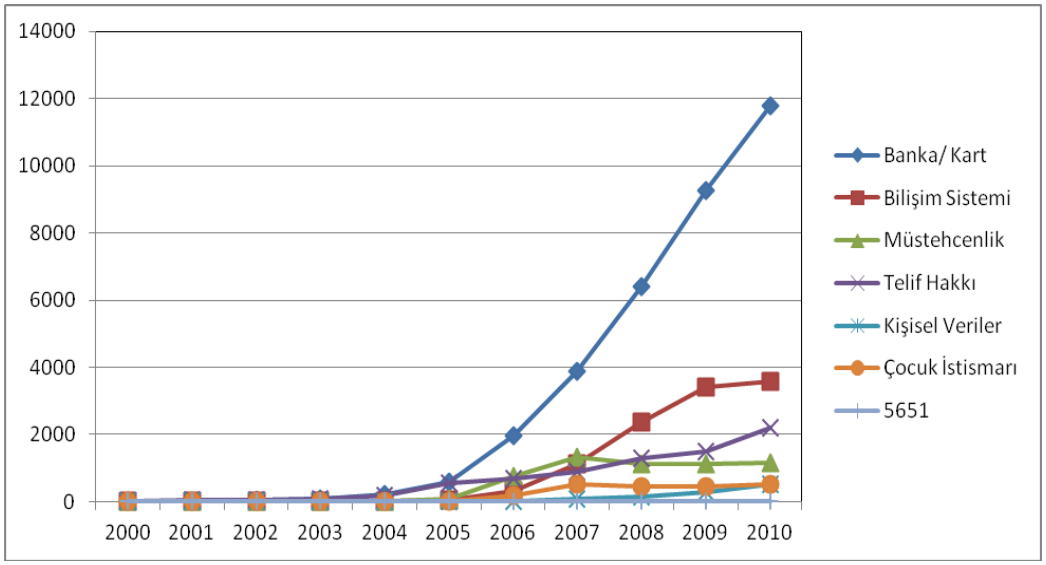
Türkiye İstatistik Kurumu (TÜİK) 'nun yaptığı "2012 Yılı Hanehalkı Bilişim Teknolojileri Kullanım Araştırması" sonuçlarına göre Türkiye'de hanelerin yüzde 47,2'si internet erişim imkânına sahip bulunmaktadır. Bu oranın geçen yılın aynı döneminde yüzde 42,9 düzeyinde olduğu belirtilmektedir. İnternet erişim imkânı olan hane oranının kentlerde yüzde 55,5, kırsal yerlerde ise yüzde 27,3 olduğu görülmektedir. Ayrıca Türkiye'de her 5 kullanıcıdan 1'inin internette alışveriş yaptığı ifade edilmektedir [47].

Türk Telekom, Ipsos KMG tarafından 2012 yılının ilk çeyreğinde gerçekleştirilen, "Türkiye'de Bilgisayar ve İnternet Kullanım Detayları ile Alışkanlıklarımız" konulu bir başka araştırmanın sonuçlarına göre ise Türkiye'de 19,1 milyon hanenin yüzde 52'sinde bilgisayar, yüzde 41'inde ise internet bağlantısının mevcut olduğu görülmektedir. Araştırmaya göre, bilgisayarı olan hane sayısı çoğalırken, internet kullanımı da buna bağlı olarak artış kaydetmektedir. En çarpıcı sonuç ise internet kafelerden internete bağlanmanın gözle görülür şekilde düştüğü. Türkiye'deki internet kullanıcıları internete daha çok evden bağlanırken hanelerde en çok tercih edilen internet bağlantısı ADSL olarak gözlenmiştir. Türkiye'deki hanelerin yüzde 31,2'si ADSL bağlantısını kullanırken 3G modem, kablo ve fiber gibi diğer bağlantı türlerinin sahipliği oranı yüzde 9,9'dur [48].

Adli Bilişim Uzmanı Çığır İlbaş ve Avukat Mehmet Ali Köksal'ın 1990 yılından 2011 yılının Temmuz ayına kadar yıl ve il bazında mahkemelere intikal eden 40 farklı suç

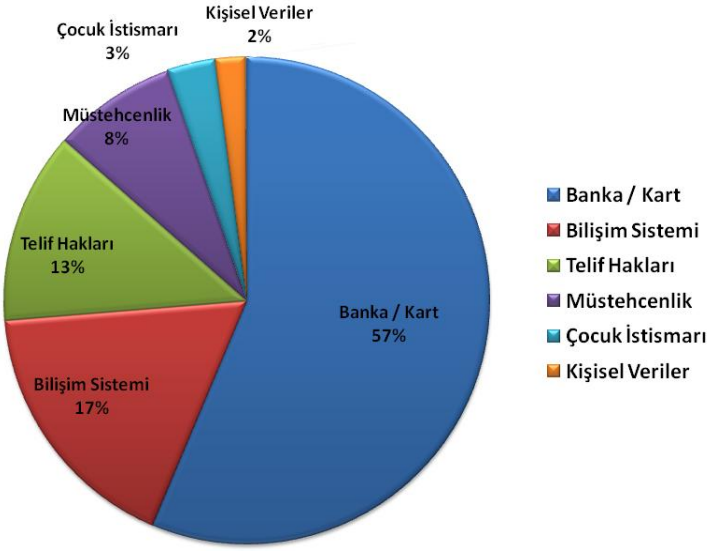
maddesine ait 73.185 adet ceza ve hukuk davasının dosya ve sanık sayısı açısından analizlerinin gerçekleştirdikleri çalışmaya göre aşağıdaki sonuçlar elde edilmiştir [49].

- Banka/kart dolandırıcılıkları, bilişim sistemlerine yetkisiz ve izinsiz girme, müstehcenlik, telif haklarının ihlali, kişisel veriler ile ilgili suçlar, çocuk istismarı, açık veya kapalı alanlarda ücretli veya ücretsiz herhangi bir kişiye kablolu veya kablosuz internet sağlayan oteller, restoranlar, alışveriş merkezleri, kafeler, internet kafeler, üniversiteler, kobiler, fabrikalar için kullanıcı hareketlerini saklama zorunluluğu getiren 5651 sayılı kanunun ihlal edilmesi gibi suçların 2000 yılından 2010 yılına kadar olan süreçte artış gösterdiği görülmektedir. 1990- 2003 yılları arasındaki dosya sayılarının az olmasının sebebi ise bilişim suçları konusunda özel ilk yasal düzenlemeleri getiren Yeni Türk Ceza Kanunu'nun 12.10.2004 tarihinde kabul edilmesi ve önceki yıllarda bilişim suçları ile mücadele eden özel kolluk kuvvetlerinin bulunmayışıdır [49, 50].



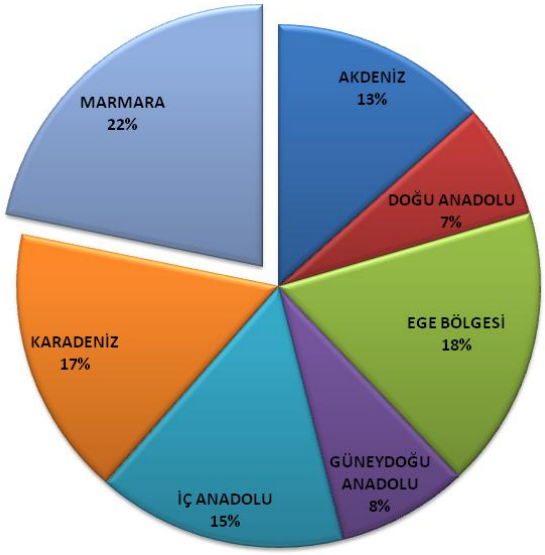
Şekil 5. 2000- 2010 yılları bilişim suçları dosya sayıları

- 1990- 2011 yılları arası işlenen bilişim suçlarının oranları aşağıdaki grafikte verilmiştir. Bu yıllar arasında incelenen dosyaların %57'sinin banka/kredi kartı dolandırıcılığı olduğu görülmektedir. Bunu sırasıyla bilişim sistemine yönelik suçlar, telif haklarının ihlali sonucu ortaya çıkan suçlar, müstehcenlik içeren suçlar, çocuk istismarı ve kişisel verilere müdahale suçları izlemektedir.



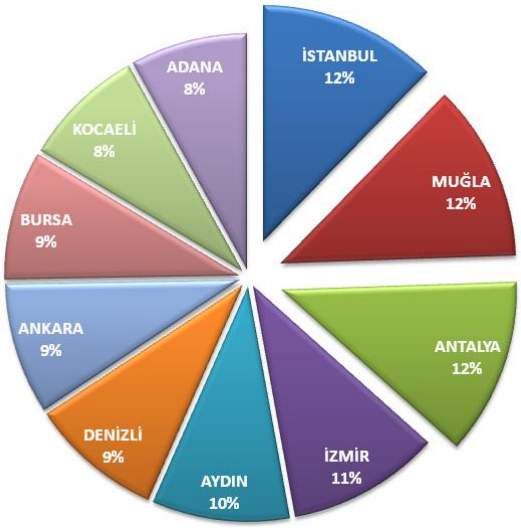
Şekil 6. 1990- 2011 yılları suçlara göre toplam dosya sayıları

- Türkiye'de bölgelere göre nüfusa oranlı bilişim suçu dosya sayıları aşağıdaki grafikte verilmiştir. Ülkemizde bilişim suçlarının en fazla işlendiği bölge Marmara Bölgesi olarak görülmektedir.



Şekil 7. 1990- 2011 yılları bölgelere göre nüfusa oranlı dosya sayıları

- Türkiye'de nüfusa oranlandığı zaman en çok bilişim suçu işlenen 10 il aşağıdaki grafikte verilmiştir. %12 oranla İstanbul, Muğla ve Antalya ülkemizde bilişim suçlarının en fazla işlendiği iller olarak görülmektedir.



Şekil 8. 1990- 2011 yılları illere göre dosya sayıları

Norton firması 24 ülkeden 13.000 kişinin katıldığı, siber suçların kullanıcıları nasıl etkilediğini ve yeni teknolojilerin gelişim ve kullanımının güvenlik açısından kullanıcılara ne gibi faydalar sunduğunu ortaya koyan bir araştırma yapmıştır. Dünyanın en kapsamlı siber suç araştırmalarından biri olan ve her yıl yayınlanan Norton Siber Suç Raporu'nun 2012 yılı sonuçlarına göre son on iki ayda kullanıcılar tarafından maruz kalınan global siber suçlara ilişkin doğrudan zarar maliyeti 110 milyar ABD doları olarak açıklanmıştır. Türkiye'de ise, son on iki ayda 10 milyondan fazla kişinin siber suç mağduru olduğu ve bunun toplam net maliyetinin ise 556 milyon ABD dolarına tekabül ettiği belirtilmektedir.

Yine aynı rapora göre, sosyal ağlar veya mobil cihazlar üzerinde karşılaşılan yeni siber suç yöntemlerinde artış görülmekte ve bu gelişme, siber suçluların daha popüler platformlara odaklandıklarını ortaya koymaktadır. Derlenen veriler ışığında görülmektedir ki çevrimiçi işlem yapan kullanıcıların beşte biri (yüzde 21) sosyal ya da mobil platformlarda dolandırıcılığa uğrarken, sosyal ağ kullanıcılarının ise yüzde 39'u sosyal ağ siber suçlarının mağduru konumundadır [51].

Yukarıda bahsedilen araştırmaların sonuçları göstermektedir ki:

- Türkiye'de her geçen gün bilgisayar kullanımı yaygınlaşmakta ve buna bağlı olarak internet kullanımı artmaktadır.
- Evlerde internet bağlantısı oranı artmakta ve buna bağlı olarak da internet kafelerden internete bağlanma oranı düşmektedir.

- Mobil teknolojilerin ve sosyal ağların kullanımı hızla yaygınlaşmaktadır.
- İnternet kullanıcılarının beşte biri internette alışveriş yapmaktadır.

Bilişim teknolojileri kullanımındaki artış beraberinde bilişim suçlarındaki artışı da getirmiştir. Son bir yılda ülkemizde 10 milyon insan siber suç mağduru olmuştur. Hırsızlık, dolandırıcılık, soygun, terörizm, sabotaj, telif haklarının ihlali ve kaçakçılık gibi pek çok suç dijital ortama taşınmıştır. Emniyet Genel Müdürlüğü (EGM) Bilgi İşlem Daire Başkanlığı Bilişim Suçları Araştırma Büro Amirliği bilişim suçlarının araştırılıp incelenmesinde ve bilişim suçlarına verilen önemde etkin olmuştur. Fakat her geçen gün yeni suç tipleri ortaya çıkmakta ve bu suçlarla mücadele edebilmek için ülkemizde daha etkili çalışmaların yapılmasına ihtiyaç duyulmaktadır.

3.5.1. Türkiye 'de Adli Bilişimin Gelişimi

Türkiye'de Emniyet Teşkilatı'nda bilişim ile ilgili temel, 1982 yılında Bilgi İşlem Daire Başkanlığının kurulmasıyla atılmıştır. 1997 yılında ise Bilişim Suçları Bürosu kurulmuştur. 2001 yılında bu büronun adı İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirilmiştir. Bu birimin dışında da diğer daire başkanlıkları altında Bilgi İşlem Şube müdürlükleri kurulmuştur. Bu daireler kendi görev alanlarına giren konularda bilişim suçları ile mücadele etmektedir. Ayrıca merkez teşkilatı içinde bir Bilgisayar Suçları ve Bilgi Güvenliği Kurulu ve Üst Kurul oluşturulmuştur. 2001 yılında Kaçakçılık ve Organize Suçlar Daire Başkanlığı ile Birleşmiş Milletler tarafından ortaklaşa kurulan TADOC (Turkish Academy Against Drug and Organised Crime) bünyesinde de Bilişim Suçları Araştırma Merkezi oluşturulmuştur. Bu merkez faaliyetlerini daha çok bu suçlar ile mücadelede, ilgili birimlere yön göstermek amacıyla akademik destek niteliğinde çalışmalar yapmaktadır. Bu merkezi yapılanmanın yanında büyük illerde de bilgi işlem büroları kurulmuş ve bu alanda karşılaşılan sorunlar ile ciddi anlamda mücadele etmeye başlanmıştır.

Bilişim suçları kavramı, son yıllarda ülkemizde de mevzuatın güncellenmesine rağmen, hukuki süreci destekleyecek teknik altyapı konusunda gündeme gelmeye başlamıştır. Türkiye dışında birçok ülke, artan bilişim suçları ve suçlunun tespiti için çoğu açık kaynak kodlu ulusal Adli Bilişim Analizi araçları ve yazılımları geliştirmektedir. ABD (Carnivore, EnCase, Autopsy, The Sleuth Kit), İtalya, Belçika (FCCU), Hollanda içerik geliştiren ülkelere örnek verilebilir. Türkiye'de Adli Bilişim 2000'li yıllardan

günümüze adli tıp, emniyet, askeriye tarafından uygulanırken 2006 yılından itibaren özel sektör tarafından da adli bilişim hizmeti verilmektedir.

Türkiye özel sektörde ISO 17025 standartlarında Adli Bilişim danışmanlık hizmeti sunan şirket bulunmamaktadır. (TS EN ISO 17025 belgesi standardı genel olarak; Laboratuvar Kalite Yönetim Sistemi+Laboratuar Teknik Şartları kapsayan bir standarttır.) Türkiye'de ISO 9001 ve ISO 17025 standartlarına uyan tek Adli Bilişim laboratuarı Adli Tıp Kurumudur. Adli Tıp Kurumu 2009 Haziran ayından itibaren ISO 17025 standartların da hizmet vermeye başlamıştır [46].

3.5.2. Türkiye'de Adli Bilişim Laboratuarlarının Kurulması

Adli bilişim sürecinde, olay yeri incelemede, delillerin elde edilmesinde, delillerin değerlendirilmesi ve suçla ilişkilendirilmesi aşamalarında yaşanan çeşitli sorunlar ve zorluklar vardır. Bunlar aşağıdaki şekilde sıralanabilir [52];

- Olay yerinin incelenmesi uzmanlık gerektirir. Uzman kişiler tarafından yapılmayan bir inceleme delillerin yok olmasına, soruşturmanın çıkmaza girmesine neden olabilmektedir. Kolluk kuvvetlerinin yaptığı ilk incelemelerin sağlıklı olarak yapılabilmesi için teknik anlamda donanımlı personele ihtiyaç vardır.
- Olay yerinde delil niteliği taşıyan elektronik verilerin imajları alınarak orijinal verilere zarar verilmemesi gerekmektedir. Verilerin imajlarının alınması çeşitli donanım ve yazılımsal araçlar gerekmektedir. Ayrıca verilerin mahkemeye delil olarak sunulabilmesi için doğruluğunun ve bütünlüğünün sağlanması ve inkâr edilememesinin sağlanması gerekmektedir.
- Bilirkişiler siber suç ile ilgili delilleri tespit ederken herhangi bir standart izlememekte ve birçoğu lisanssız program kullanmaktadır. Ortaya konulan raporda da yine belirli bir format yoktur. Mevcut uygulama uluslararası mahkemelerde tazminat ödenmesine yol açabilir. Her ne kadar rapor hazırlanırken lisanssız program kullanmanın, ülkemizdeki hukukçular tarafından başka bir suç oluşturduğuna kanaat edilmiş olsa da; teknik olarak lisanssız programın incelenen sistem üzerinde delil niteliğini bozacak işlemler yapması mümkündür.

- Uygulamada kamu bilişim laboratuarları olayların çok az bir kısmında inceleme yapmaktadır. Bu oranın düşük olmasının nedeni, yeterli laboratuar olmamasıdır.

Bilişim suçları konusundaki problemler süreçteki; hukuki, uygulama ve teknik boyut arasındaki koordinasyon eksikliğinden kaynaklanmaktadır. Hukuk ve kolluk tarafındakiler yeterli teknik bilgiye sahip değildir. Suçla, günümüzde ve gelecekte daha etkin mücadele edebilmek için daha iyi teşkilatlanma ve teknik altyapı gereklidir. Delillendirmeyi, faile ulaşmayı, diğer bir ifadeyle fiil ile fail arasındaki bağlantıyı sağlayacak standartlara sahip, Adli Bilişim Laboratuarlarının kurulmasının kaçınılmaz olduğu görülmektedir.

3.6.Türkiye'de Adli Bilişim Eğitimi

Ülkemizde internetin kullanılmaya başlandığı ilk yıllarda altyapı yetersizliklerinin olduğu, insanların bilgisayar ve internet kullanımı konusunda bilinçsiz olduğu görülmektedir. Süregelen zaman içerisinde Türkiye'de internet altyapısı güçlendirilmiş ve insanlar internetin nimetlerinden gerektiği gibi faydalanmaya başlamışlardır. Günümüzde özellikle cep telefonlarından ve mobil cihazlardan internet erişiminin yaygınlaşmasıyla havaalanından üniversite yerleşkelerine, kamu kuruluşlarından eğlence mekânlarına kadar her yerde internet erişimi söz konusu olmaktadır. İnsanlar evlerinde, işyerlerinde, okullarında, eğlenmek için gittikleri mekânlarda, bir şeyler yiyip içerken, yürürken bile internete girmeden duramaz hale gelmişlerdir. Hatta halkımızın bir bölümünün internet bağımlısı olduğunu söylemek dahi söz konusudur.

Yaygınlaşan internet kullanımı, bilişim suçlarındaki artışı ve çeşitliliği kaçınılmaz hale getirmiştir. Bilgi güvenliği ve kişisel mahremiyetin sağlanması, internet bankacılığı ve e-ticaret alanında dolandırıcılıkların önüne geçilmesi, biyometrik sistemler kullanılarak güvenlik sistemlerinin oluşturulması gibi birçok alanda hem yasal hem de teknik anlamda çalışmalar yapma gerekliliği ortaya çıkmıştır. Bu suçlarla ilgili yürürlükte olan mevzuat yetersiz kalmış ve mahkemeye intikal eden olayların birçoğunda dijital delillerin elde edilmesindeki yetersizlikler nedeniyle takipsizlik kararı verilmiş ya da yargılama süreci çok fazla uzamıştır. Bütün bu olumsuz gelişmelerin yaşanması, bilim insanlarını bu yönde araştırma yapmaya itmiştir. Birçok eğitim kurumu bilişim suçları ile mücadele etmek için uzman yetiştirme çabasına girmişlerdir.

Bilgisayar bilimleri, bilgisayar mühendisliği, bilgisayar öğretmenliği, bilgisayar ve öğretim teknolojileri vb. bölümlerin ders listeleri arasında, siber suçlar, ağ güvenliği, kötü amaçlı yazılımlar, biyometrik sistemler vb dersler yer almaktadır. İnternet üzerinden suç işleme oranları arttıkça, bu alana ait derslerin bilişim program müfredatlarında günden güne artış gösterdiği görülmektedir. Ülkemizde adli bilişim alanında eğitim veren bazı kurumlar aşağıda verilmiştir [53].

3.6.1. Polis Akademisi Güvenlik Bilimleri Fakültesi/Enstitüsü

3201 Sayılı Emniyet Teşkilatı Kanunun 18. Maddesi gereğince orta ve üst kademe yöneticilerini yetiştirmek üzere, Polis Enstitüsü adı altında bir yıllık meslek içi Yüksek Okul olarak 06 Kasım 1937 yılında kurulmuştur. Polis Enstitüsü'ndeki Eğitim Milli Eğitim Bakanlığı Talim Terbiye Kurulu Kararlarıyla 1940 yılında iki yıllık, 1962 yılında üç yıllık yüksek okullar içerisine alınmış olup 1980 yılından itibaren öğretim süresi 4 yıla çıkarılmıştır.

Emniyet Teşkilatı'nın ihtiyaç duyduğu diğer branşlardaki personel ihtiyacını karşılamak amacıyla, 3201 sayılı Emniyet Teşkilatı Kanunu kapsamında 1989 yılında değişiklik yapılarak 1991 yılından itibaren Fakülte Yüksek Okullar (FYO) adı altında öğrenci alınmaya başlanmış ve bu hizmetlerin yürütülmesi için Polis Akademisi görevlendirilmiştir.

25 Nisan 2001 tarih ve 4652 sayılı kanunla, Polis Üniversitesi anlayışıyla yeniden yapılandırılmıştır. Bünyesinde eğitim hizmeti veren Güvenlik Bilimleri Fakültesi, Güvenlik Bilimleri Enstitüsü, 27 Polis Meslek Yüksek Okulu ve Fakülte ve Yüksek Okullar bölümü ile üniversite statüsüne kavuşturulmuştur.

2002 Yılında kuruluşu tamamlanan Güvenlik Bilimleri Enstitüsünde 9 ana bilim dalında (Adli Bilimler, Ceza Adaleti, Güvenlik Stratejileri ve Yönetimi, İstihbarat Araştırmaları Programı, Suç Araştırmaları, Ulaşım Güvenliği ve Yönetimi, Uluslararası Güvenlik, Uluslararası Güvenlik (İngilizce) Programı, Uluslararası Terörizm ve Sınıraşan Suçlar Programı) eğitim verilmektedir [54].

3.6.2. Yaşar Üniversitesi'nde Siber Güvenlik Bilim Dalı

24 Mayıs 2012 Tarih ve 8/1 nolu kararı uyarınca Bilgisayar Mühendisliği Anabilim Dalında 2012-2013 Güz döneminden itibaren Siber Güvenlik Bilim Dalı açılmıştır. Eğitim süresi 2 yıl olan Siber Güvenlik Bilim Dalında öğrenciler 120 AKTS (ECTS)'lik (Avrupa Kredi Transfer Sistemi/Europe Credit Transfer System) ders almaktadırlar [53].

Tablo 1. Yaşar Üniversitesi siber güvenlik bilim dalı dersleri

Course Names	Ders İsimleri	ECTS/AKTS
Probability and Stochastic Processes for Engineers	Olasılık ve Mühendisler için Stokastik Süreçler	8
Advanced Information Security	İleri Bilgi Güvenliği	8
Information Theory	Bilgi Teorisi	8
Computational Number Theory	Hesaplamalı Sayısal Teorisi	8
Algorithm Analysis and Complexity Theory	Algoritma Analizi ve Karmaşıklık Teorisi	8
Information Warfare	Bilgi Savaşları	8
Cryptography	Kriptografi	8
Seminar	Seminer	4
Master's Thesis	Yüksek Lisans Tezi	60

3.6.3. Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Anabilim Dalı

Gazi Üniversitesinde 2013- 2014 akademik döneminde yüksek lisans ve doktora eğitimi vermesi planlanan Adli Bilişim Anabilim Dalı kurma çalışmaları hızla sürdürülmektedir.

Bu programda eğitim öğretim faaliyetlerinin uzaktan ve örgün eğitim şeklinde yapılması planlanmaktadır. Programa hukuk fakültesi, polis akademisi, bilgisayar, elektrik ve elektronik mühendisliği lisans diplomasına sahip olan mezunlar, şartsız olarak kabul edileceklerdir. Diğer alanlardan gelecek öğrenciler ise adli bilişim alanında eğitim aldıklarını sertifikalarla belgelemeleri durumunda, bu programa kabul edilebileceklerdir. Programı başarı ile tamamlayanlar, Adalet Bakanlığı, Emniyet Genel Müdürlüğü ve adliyelerde adli bilişim uzmanı ve bilirkişi unvanlarıyla çalışabileceklerdir [53, 55].

3.6.4. Hacettepe Üniversitesi Adli Bilişim Araştırma ve Uygulama Merkezi

Hacettepe Üniversitesi'nde, bilişim alanında ortaya çıkan hukuki sorunlar ve konular ile ilgili olarak bilimsel araştırma, uygulama, eğitim çalışmaları yapmak, veri bankası oluşturmak, dokümantasyon ve arşivleme faaliyetinde bulunmak, adli bilişim uygulamaları konusunda teorik ve uygulamalı faaliyet göstermek, bilişim ve hukuk ile ilgili konularda özel ve kamu kuruluşları ile birlikte faaliyet göstermek ve ilgili kuruluşlara yardımcı olma amaçlı "Adli Bilişim Araştırma ve Uygulama Merkezi" kurulmuştur [56].

3.6.5. Fırat Üniversitesi Adli Bilişim Mühendisliği Bölümü

Fırat Üniversitesi Türkiye'de bir ilki gerçekleştirerek Teknoloji Fakültesi bünyesinde Adli Bilişim Mühendisliği bölümünü açmıştır. Bu bölüm ile ilgili çalışmalar 07 Temmuz 2010 tarihinde başlatılmış 18 Mayıs 2011 tarihinde tamamlanmıştır.

Yükseköğretim Genel Kurulu Adli Bilişim Mühendisliği Bölümünün Fırat Üniversitesi Teknoloji Fakültesi bünyesinde kurulmasına onay vermiştir. 2013-2014 akademik yılında bu bölüme öğrenci alımının gerçekleştirilmesi için çalışmalar yoğun bir biçimde sürdürülmektedir.

Fırat Üniversitesi Teknoloji Fakültesi bünyesinde kurulmuş bulunan Adli Bilişim Mühendisliği Bölümünün iki programı mevcuttur. Bu programlardan biri, Türkçe eğitim yapacaktır. Diğer bir program ise Uluslararası ortak lisans programı kapsamında Amerika Birleşik Devletleri Texas Eyaletinde bulunan Sam Houston State Üniversitesi ile ortak yürütülecek olan çift diplomaya yönelik İngilizce eğitim yapacaktır [53].

Adli bilişim mühendisliği bölümünde öğrenim görecek öğrenciler, ÖSYM tarafından her yıl gerçekleştirilen merkezi sınav sistemi usulüyle, normal lise ya da Mesleki Teknik Orta Öğretim Kurumları (MTOK) öğrencileri ayırt edilmeksizin MF-4 puan türü esas alınarak yapılacak sıralamaya göre seçilecektir. Ancak, MTOK ve normal lise öğrencileri kendi aralarında sıralamaya tabi tutulacaktır. Bu uygulamayla hem MTOK öğrencilerinin lehine bir tutum sergilenmekte hem de MTOK öğrencilerine kayıt olduktan sonra 1 yıl süre ile Bilimsel Hazırlık Eğitimi verilerek fizik, matematik ve kimya gibi temel ders eksiklikleri giderilmektedir [53]

Tablo 2. Adli bilişim mühendisliğinde ilk 2 yılda okutulacak alan dersleri

Güz Yarıyılı	**AKTS**	**Bahar Yarıyılı**	**AKTS**
Algoritma ve Programlama I	7	Algoritma ve Programlama II	7
Bilgisayar Bilimlerine Giriş	7	Yazılım Mühendisliğinin Temelleri	7
Ayrık Yapılar	5	Sayısal Analiz	5
Mantık Devreleri	6	Mikroişlemciler ve Programlama	6
Programlama Dilleri	6	Nesne Tabanlı Programlama	6
Veri Yapıları	4		

Tablo 3. Adli bilişim mühendisliğinin 3. ve 4. yıllarında okutulacak alan dersleri

Güz Yarıyılı	**AKTS**	**Bahar Yarıyılı**	**AKTS**
Sayısal Adli Bilişime Giriş	7	Adli Bilişimde Donanım	6
C programlama Dilinde Özel Konular	8	Ağ Güvenliği	5
Veritabanı Yönetim Sistemleri	8	İleri Dil Konseptleri	7
Ağlar	7	Sayısal Metotlar	6
Yazılım Mühendisliği	5	Kötü Amaçlı Yazılımlar	6
Sayısal Adli Bilişim Araçları	7	Bilgi Güvenliği	7
Kriptografi	6	Siber Kanunlar	6
Siber Savaşlar	6	Profesyonellik ve Etik	7
		Bitirme Projesi	10

İngilizce eğitimde ise öğrenciler 1 inci ve 2 inci sınıf derslerini Fırat Üniversitesi Adli Bilişim Mühendisliği Bölümünden İngilizce olarak alacaklardır. Dersleri başarı ile tamamlayanlar 3 üncü ve 4 üncü sınıf derslerini almak için Sam Houston State Üniversitesine gideceklerdir. Orada 2 yıl süresince alacakları dersleri başarı ile tamamlayan öğrenciler hem Fırat hem de Sam Houston State Üniversitesi Adli Bilişim Mühendisliğinden diploma almaya hak kazanacaklardır. Tablo 4'te İngilizce eğitim görecek Adli Bilişim Mühendisliği öğrencilerin eğitimleri süresince alacakları alan dersleri görülmektedir [53].

Tablo 4. Adli bilişim mühendisliği ingilizce eğitim programı alan dersleri

Fall Semester	ECTS	Spring Semester	ECTS
Firat University			
Algorithm and Programming I	7	Algorithm and Programming II	7
Introduction to Computer Science	7	Principles of Software Engineering	7
Discrete Structures	5	Numerical Analysis	5
Logic Circuits	6	Microprocessor and programming	6
Programming Languages	6	Object Oriented Programming	6
Data Structures	4		
Sam Houston State University			
Introduction to Digital Forensics	7	Hardware Forensics	6
Special Topics Programming "C"	8	Network Security	5
Database Management Systems	8	Advanced Language Concepts	7
Networks	7	Numerical Methods	6
Software Engineering	5	Malware	6
Digital Forensics Tools	7	Information Security	7
Cryptography	6	Cyber Law	6
Cyber Warfare	6	Professionalism and Ethics	7

3.6.5. Adli Bilişimin Sivil Toplum Kuruluşları Olarak Yapılanması

Türkiye'de 2006 yılından itibaren adli bilişim konusuna ilgi duyulmaktadır. Bu ilgi ile birlikte adli bilişim etkinlikleri, konferanslar düzenlenmekte ve dernekler kurulmaktadır. Ülkemizde bilgi güvenliği ve adli bilişim konusunda aktif olarak faaliyet gösteren dernek ve kulüpler aşağıda verilmiştir [53].

Tablo 5. Ülkemizde faaliyette bulunan adli bilişim dernek ve kulüpleri

Adli Bilimciler Derneği
Adli Bilişim Derneği
Adli Bilişim Kulübü, Fırat Üniversitesi, 2013
Alternatif Bilişim Derneği
Bilgi Güvenliği Derneği
Bilişim 2023 Derneği
Bilişim Suçları Mücadele Derneği
İstanbul Bilirkişiler Derneği
Siber Güvenlik Derneği
TEID – Etik ve İtibar Derneği
Telekomcular Derneği
Türk Bilişim Derneği
Türkiye Bilişim Derneği

3.6.6. Adli Bilişim ve Bilgi Güvenliği Alanlarında Ülkemizde Düzenlenen Bazı Etkinlikler

Ülkemizde adli bilişim ve bilgi güvenliği alanında çeşitli sempozyum, konferans, çalıştay, panel ve seminerlerin yapıldığı görülmektedir. Yapılan çeşitli etkinlikler Tablo 6'da verilmiştir.

Tablo 6. Türkiye'de adli bilişim alanında yapılan bazı etkinlikler

1st International Symposium on Digital Forensics and Security (Elazığ)
1st Sec 2011 (İstanbul)
ADEO Security Labs Güvenlik Günleri (İstanbul)
Adli Bilimler Konferansı, 07 Temmuz 2010, Fırat Üniversitesi (Elazığ)
Adli Bilişim Konferansı (İstanbul Üniversitesi)
Adli Bilişim ve Biyometrik Sistemler Paneli, Kahramanmaraş Sütçü İmam Üniversitesi & Kahramanmaraş Barosu, 22 Mayıs 2012, (Kahramanmaraş)
Adli Bilişim ve Biyometrik Sistemler Paneli, Mustafa Kemal Üniversitesi, 25 Mayıs 2012, (Hatay)
Akademik Bilişim Konferansı (İstanbul)
AnkaSec (Ankara)
Bilişim Güvenliği Konferansı (İstanbul)
Bilişim Hukuku Konferansı (İzmir)
Bilişim Hukuku Semineri (İstanbul)
Bilişim Zirvesi (İstanbul)
Bulut Bilişim Konferansı (Yalova)
CeBIT Sinerji Zirvesi (İstanbul)
Dünya Bilişim Teknolojileri Konferansı (İstanbul)
ECN-Adli Bilişim Çalışma Grubu(İstanbul)
EMEA Intelligence (İstanbul)
Euroforencis Adli Tıp ve Adli Bilişim Konferansı (İstanbul)
International Conference on Information Security &Cryptology
IT Forensic Konferansı (İstanbul)
inet-tr Konferansı (İstanbul)
İstanbul Üniversitesi Çalıştayları
Microsoft Güvenlik Seminerleri (İstanbul)
Polis Akademisi Başkanlığı Bilişim Topluluğu (Ankara)
Siber Suçlar Sözleşmesi Semineri (İstanbul-İzmir)
Sosyal Güvenlik Reformu Semineri (Konya)
Türkiye Barolar Birliği Hukuk Semineri (İstanbul)
Ulusal Bilişim Kongresi (İstanbul)
VeriSign Bilişim Suçları ve Siber Terörizm Konferansı (İstanbul)

4. ADLİ BİLİŞİMDE BİYOMETRİNİN KULLANILMASI

4.1. Biyometrik Sistemler

Günümüzde bilginin önem kazanmasıyla bilginin güvenliğinin sağlanması da sorun haline gelmiştir. Eskiden iş süreçleri ve faaliyetlerin çok küçük bir kısmı bilişim sistemleri kullanılarak yürütülmekte iken günümüzde bilişim sistemleri hemen hemen her iş sürecinin bir parçası olarak yerini almıştır. İşte bu sebeple bilişim sistemlerinin güvenliği kişisel güvenlik ve iş süreçlerinin, faaliyetlerin yürütülebilirliği açısından çok önemlidir. Dijital ortamda bulunan bilgilerin yetkisiz kişilerin eline geçmesi ya da yetkisiz kişiler tarafından değiştirilmesi sonucunda meydana gelen olumsuzluklardan bireyler, kurumlar hatta devletler etkilenmektedir. Ayrıca bilginin gönderilmek istenilen kişi ya da kuruma değil de başka kişilere gönderilmesi gibi durumlarda da istenmeyen sonuçlar ortaya çıkmaktadır. Özellikle savunma sanayisi, tıp gibi sektörlerde bilgi kayıpları büyük mağduriyetler doğurabilmektedir.

Bilgi güvenliği için kullanılan kimlik doğrulama işlemi genel olarak bilgi temelli, aidiyet temelli ve biyometrik temelli olmak üzere üç farklı şekilde incelenebilir. Bilgi temelli kimliklendirmede kullanıcılar ve sistem yöneticisi kullanıcı adı, şifre ya da pin denilen gizli bilgilere sahiptir. Aidiyet temelli kimliklendirmede kullanıcılar eşi olmayan anahtar, kart, rozet gibi bir objeye sahiptirler. Biyometrik sistemlerde ise kişilerin herhangi bir bilgi ya da objeye sahip olmadan sadece kendi biyolojik özelliklerini kullanarak kimliklendirilmesi söz konusudur [57- 59].

Biyometri, biyolojik verileri, yani bireyin kişisel bir nitelik ya da davranışını analiz ederek kimliğini doğrulama bilimidir. “bio” (yaşam) ve “metron” (ölçüm), kelimelerinden türeyen biyometri, biyolojik veriyi ölçmekte ve istatiksel olarak analiz etmektedir. Bilişim teknolojisi ile birlikte biyometri genel olarak insan vücudunun parmak izi, el geometrisi, retina, iris, ses, yüz şekilleri gibi özellikleriyle ilgilenmekte ve bunları doğrulama ve/veya kimlik tespiti için kullanmaktadır. Ayrıca insanların imza, yazı dinamiği, konuşma, konuşma esnasında dudak hareketleri, yürüyüş, tuş vuruşu gibi davranışsal birtakım özellikleri de biyometri biliminde kimlik tespiti ve doğrulamada kullanılmaktadır [57- 59].

4.2. Biyometrik Sistem Çeşitleri

Günümüzde biyometrik alanda çok hızlı bir gelişme söz konusudur. Şüphesiz bunda güvenlik ihtiyacının artmış olması birinci derecede etkilidir. Aşağıdaki tabloda biyometrik sistemlerin sektörlere göre kullanılma yüzdeleri verilmiştir. Tablodaki veriler göstermektedir ki biyometrik sistemler birçok sektörde güvenlik zafiyetlerini önlemek ve fiziksel erişim kontrolü sağlamak amacıyla kullanılmaktadır.

Tablo 7. Biyometrik sistemlerin kullanıldığı sektörler ve kullanılma yüzdeleri

Sektör	Oran
Fiziksel Erişim Kontrolü	%52.8
Polis Teşkilatları	%12.9
Sağlık	%10.2
Bankacılık	%8.3
Gümrük Kontrolü	%4.9
Bilgisayar Güvenliği	%4.1
Sosyal Güvenlik	%4.1
Telekomünikasyon	%2.7

Biyometrik tanımada kullanılabilecek bazı yöntemler aşağıda verilmiştir.

- Parmak izi tanıma
- DNA tanıma
- Retina tanıma
- İris tanıma
- Yüz tanıma
- Ses tanıma
- El geometrisi tanıma
- Damar tanıma
- Diş izi tanıma
- Yüz termogramı
- İmza atımı
- Konuşma

- Tuş vuruşu
- Yürüyüş

4.2.1. Parmak İzi Tanıma

Yapılan araştırmalar, parmak izinin tek yumurta ikizleri de dâhil olmak üzere her insanda farklı olduğunu göstermiştir. Parmaklarda bulunan çizgilerin her insanda farklılık göstermesi, yıllarca değişmemesi, kolay kullanımı parmak izinin yüzyılı aşkın süredir kimlik tespitinde kullanılmasını sağlamıştır. Günümüzde personel devam ve takip sistemlerinde, resmi kurumlarda imza yerine, polis teşkilatı tarafından kriminal olaylarda delil olarak, gümrüklerde, hava alanlarında ve ATM'lerde fiziksel erişim kontrolü sağlamak amacıyla yaygın olarak kullanılmaktadır.

İlk kullanılmaya başlandığı yıllardan bu yana gerek yazılım gerekse donanım alanında parmak izi sistemlerinde önemli ilerlemeler kaydedilmiştir. Parmak izi sistemlerinin maliyetleri gelişen teknoloji sayesinde geçmiş yıllara göre oldukça düşmüştür. Buna paralel olarak kullanım alanı da genişlemiştir. Bir parmak izi tanıma sistemi sırasıyla aşağıdaki işlemleri gerçekleştirmektedir [61]:

1. Parmak izlerinin alınıp sayısala çevrilmesi
2. Parmak izinde bilgi taşıyan, üzerinde işlem yapılacak kısmın arka plandan ayrılması
3. Parmak izinin temizlenip iyileştirilmesi
4. Resmin ikili resme çevrilmesi
5. İkili resmin inceltilmesi
6. Özellik noktalarının ve bu noktaların parametrelerinin bulunması
7. Yalancı özellik noktalarının elimine edilmesi
8. Sistemin başarısının değerlendirilmesi

Şekil 9. Parmak izi örneği

Parmak izleri, adli olaylarda olay sahnesinde bulunan ve maddi delil niteliği taşıyan izlerden şüphesiz en önemlisidir. Nedeni ise bir olaya karışmış veya yakından-uzaktan ilişkisi olan kişi veya kişilerin kimliğini tespit etmekte en emin yol, en kesin delil parmak izidir. Kesin sonuç vermenin yanında değişmez-değiştirilemez, benzemez-benzetilemez ve tasnif edilebilir oluşu, parmak izinin değerini daha da arttırmaktadır. Bir olayın aydınlatılmasında şahitler yanılabilir ve bir kısım deliller yetersiz kalabilirler. Fakat parmak izlerinin ne yanılmalarından ne de yetersiz kalmalarından söz edilebilir. Birçok gelişmiş ülke yeni ve gelişmiş teknikleri kullanmakla birlikte, parmak izi sadece kişinin kendine özgü olduğundan bireysel kimlik tespitinde ilk akla gelen yöntemdir. Parmak izlerinin değişmez olması ve devamlılık göstermesi, sınıflandırılabilmesi, birbirine benzemez ve benzetilemez oluşları gerçek kimliklerin belirlenmesi açısından da önemlidir. Parmak izleri, özellikleri nedeniyle suçluların adli sicillerinin tutulmasına da imkân vermekte ve yakalandıklarında daha önce işlediği suçları da tespit edilebilmektedir. Özet olarak parmak izleri "şahsın ikinci kimliğidir" denilebilmektedir [62].

Suçluların tespit edilmesi için günümüzde hızlı ve hatasız çalışma yöntemleri gerekmektedir. Parmak izinin bilgisayarlı ortamda saklanması ve mukayesesinin yapılması bu yöntemlerden biridir. 1997 yılında Emniyet Genel Müdürlüğü bünyesinde AFIS (Otomatik Parmak İzi Tanıma Sistemi) kurulmuştur. Sistemle beraber ülke genelinde güvenli bir parmak izi arşivi oluşturulmuş olacaktır. Bu sistemle, faillerin tespit ve teşhis oranının yükseltilmesi, hizmette verimlilik sağlanması amaçlanmaktadır. AFIS sistemi, olay yeri inceleme ve kimlik tespit hizmetlerinde "delilden sanığa" ilkesi ile çözüm sağlayan bir teknoloji olarak son zamanlarda polis teşkilatında kullanılmaya başlanmıştır. AFIS terimi , "Automated Fingerprint Identification System" kelimelerinin baş harflerinin birleştirilmesinden oluşmakta ve "Otomatik Parmak İzi Teşhis Sistemi" anlamına gelmektedir. Bu sistemde tek parmak ve on parmak izleri scanner (tarayıcı) veya CCD kamera aracılığıyla bilgisayar ortamına atılmakta, işlenip tüm düzeltme işlemleri yapıldıktan sonra yine otomatik olarak karşılaştırma yapacak seviyeye gelmektedir.

Kriminal Polis Laboratuarları Dairesi Başkanlığı koordinesinde 1. Aşama olarak 9 bölge merkezli ilde AFIS (Otomatik Parmak İzi Tespit Sistemi) ile olay yerinden alınan bir parmak izinin AFIS sistemi sayesinde ülkemiz genelinde kısa sürede araştırma yapılmaktadır. Emniyet Genel Müdürlüğü'nün yeni geçtiği bu sistem sayesinde şüpheli, sabıkalı veya suçlu bulunan kişilerin parmak izleri Türkiye'deki kayıtlarda

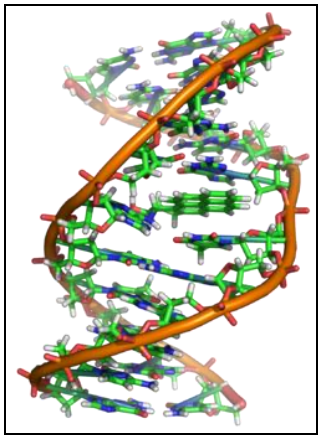
sorgulanabilmekte ve en fazla 20 dakika içinde parmak izinin ilgili kişiye ait olup olmadığı belirlenebilmektedir.

AFIS Sisteminin ana kumanda merkezi Ankara'da, Emniyet Genel Müdürlüğü (EGM) Kriminal Polis Laboratuarları Dairesi Başkanlığı'na bağlı Olay Yeri İnceleme ve Kimlik Tespit Şube Müdürlüğü bünyesinde bulunmaktadır. Otomatik parmak izi işlemlerinin yapılabileceği dokuz ana makine bulunmaktadır. Bunlar İstanbul'un dışında Ankara, İzmir, Erzurum, Diyarbakır, Antalya, Samsun, Adana ve Bursa'da konuşlandırılmıştır. Sistem, merkezle bağlantılı olarak, ilk önce İstanbul'da kullanılmaya başlanmıştır [62].

4.2.2. DNA

1953 yılında mikroskobun altında hücre yapısını deşifre ederken DNA'yı belirleyen J.D.Watson ve F.H.C. Crick adlı biyologlar 20'inci yüzyılın en büyük keşiflerinden birine imza atmışlardır. 1984 yılında Leicester Üniversitesi genetik bilimcilerinden Prof Alec Jeffrey, DNA'nın tıpkı süpermarketlerde ürünlerin üzerine yapıştırılan barkotlar gibi filmler üzerinde görüntülenebileceğini ispatlamıştır. İlk başlarda babalık testi için kullanılmaya başlanan DNA analizine daha sonra cinayet ve tecavüz davalarında suçlunun bulunması için başvurulmuştur. DNA yapısı, mezarda bile uzun yıllar değişmeden saklanmaktadır. Kan, sperm, tükürük, saç, kıl, hatta tere bile DNA testi uygulanabilmektedir. DNA testi sayesinde yıllarca önce ölmüş kişileri teşhis etmek ya da yıllanmış bir cinayeti aydınlatmak bile mümkün olmaktadır [63].

DNA testi kimlik tespitinde kullanılan doğruluğu çok yüksek bir yöntemdir. Fakat DNA analizinin maliyetinin fazla olması ve uzun sürmesi soruşturmanın seyrini yavaşlatmaktadır. Özellikle gerçek zamanlı kimlik tespitinin gerektiği durumlarda kullanışlı değildir. Ayrıca DNA analizinde yöntemin doğruluğu örnek kalitesine bağlıdır. Örneklerin karışması, kirletilmesi, kemik iliği nakli gibi durumlarda yöntemin başarısı düşmektedir [57].

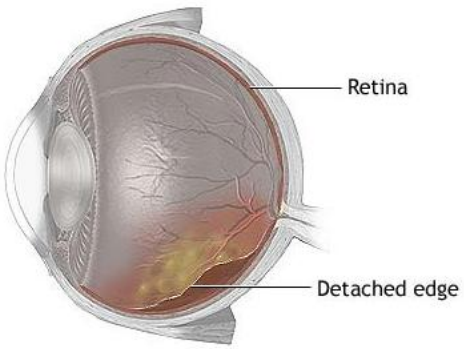


Şekil 10. DNA

4.2.3. Retina Tanıma

Retina tanıma sistemleri, retina tabakasında bulunan kılcal damarların oluşturduğu karakteristik şekilleri tanıma amaçlı kullanılmaktadırlar. Retina, göz yuvarlağının içinde arka duvarda bulunan ve kılcal damarlarca zengin tabakadır. Kızılötesi ışık, göz merceği üzerinden retinadaki kılcal kan damarlarına gönderilmekte ve damarların oluşturduğu karakteristik şekil standart bir video kameraya yansıtılmaktadır.

Retina tanıma sistemleri, son zamanlarda büyük rağbet görmeye başlamıştır. CIA, FBI, NASA, General Dynamics firmaları bu sistemlerin müşterileri arasındadır. Türkiye'de de Akbank Etiler şubesinin ATM'sinde test amaçlı bir retina tanıma sistemi bulunmaktadır [60].



Şekil 11. Retina

4.2.4. İris Tanıma

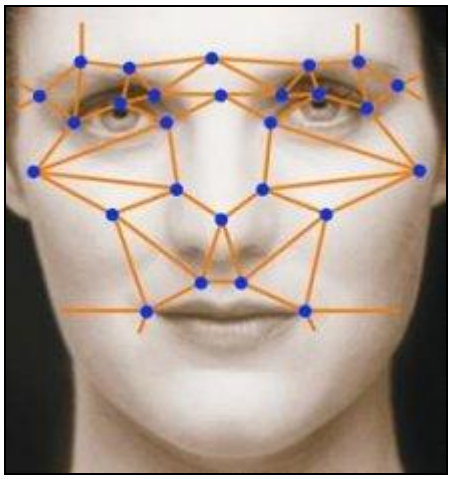
İris, gözün ön kısmında bulunan renkli kısımdır. Üzerinde 400'den fazla ayırt edici karakteristik taşımaktadır. Bunlar çukurlar, kara noktalar, damarlar gibi fiziksel özelliklerdir ve herkeste farklıdır. Bu özellikler, parmak izinden altı kat daha ayırt edici sayılmaktadır [60]. 1936 yılında Frank Burch isimli göz doktoru, bir bireyi tanımak için iris desenlerinin kullanılabileceği fikrini öne sürmüştür. 1985 yılında Dr. Leonard Flom ve Dr. Aran Safir tüm irislerin eşsiz olduğunu ispatlayarak 1987'de iris tanıma ile ilgili patenti almışlardır. Dr. Flom, Dr. John Daugman'dan iris tanımayı otomatik hale getirecek bir algoritma geliştirmesini istemiştir. 1993 yılında ABD'de Defense Nuclear Agecny bu işlemi yapacak bir prototip üstünde çalışmalara başlamıştır. 1995 yılında tamamlanan sistem Dr. Daugman'a bu dalda bir patent kazandırmıştır. 1995 yılında otomatik iris tanıma yapabilen cihazlar piyasaya çıkmaya başlamıştır [64].

İris tanıma sistemleri yüz ve parmak tanımada olduğu gibi özel noktaların çıkarılmasıyla yapılamamaktadır. Daha çok 'pattern recognition' olarak bilinen örüntü tanıma yöntemiyle yapılmaktadır. İris tanımada ilk adım göz resminden iris bölgesinin bulunmasıdır. İris bölgesi seçildikten sonra bu bölge üzerinden dokuya dayalı olarak özellik çıkarma işlemleri yapılır. Bu özellik çıkarma ve karşılaştırma işleminin de birden fazla yolu bulunmaktadır. Bu yöntemlerden biri, göz bebeğinin etrafından alınan parçalar üzerinde işlem yapmaktır. Tüm iris üzerinde işlem yapılmamasının bir diğer sebebi ise göz kapağının yarı kapalı olması ve kirpiklerin irisi örtmesidir. İris üzerinden göz bebeğine bitişik yerlerden belirli sayıda parça alınarak bu karşılaştırma yapılabilmektedir [60, 64].

Şekil 12. İris

4.2.5. Yüz Tanıma

Günlük hayatta insanlar yüzlerine bakarak kolayca ayırt edilebilir. Bu sebeple bu yöntem neredeyse insanlık tarihiyle yaşıt bir biyometrik ayırt etme yöntemidir. Yüz tanıma sistemleri de bu mantıktan hareketle tasarlanmışlardır. İnsan yüzü her ne kadar birbirine benzer olsa da her yüzün kendine özgü bazı özellikleri bulunmaktadır. İki yüzü birbirinden ayırmaya yarayan noktalara düğüm noktaları (nodal points) adı verilir. Mesela; gözlerin birbirinden uzaklığı, burnun uzunluğu, göz çukurlarının derinliği ve elmacık kemiklerinin çıkıklığı yüz tarayıcıların odaklandığı yerlerdendir [65].



Şekil 13. Yüz tanıma sistemi

Yüz tanıma sistemleri, yüzün karakteristik özelliklerini analiz ederek ya da çeşitli noktalarda yüzün ölçülebilir ve davranışsal karakteristiklerini ifade eden biyometrik ölçümler yaparak daha önceden oluşturulmuş bir veri tabanı ile karşılaştırma yapmak suretiyle kişiyi tanımlamaktadırlar. Genel bir otomatik yüz tanıma sisteminin blok diyagramı aşağıda şekilde verilmiştir [66].

Şekil 14. Yüz tanıma sistemi blok diyagramı

Yüz tanıma sistemleri güvenlik birimlerinde çok geniş bir yelpazede kullanım alanı bulmaktadır. Terör ve toplumsal olaylar ile mücadelede, genel asayiş ve kolluk hizmetlerinde, hudut kapılarında yolcu giriş çıkış kayıt hizmetlerinde, Kriminal Polis Laboratuarı görüntü inceleme hizmetlerinde ve her geçen gün yaygınlaşan "Mobil Elektronik Sistem Entegrasyonu" MOBESE projesinde yer alan "Bölge Görüntüleme Sistemi" ile elde edilen kamera görüntülerinin bu gibi akıllı yazılımlar ile değerlendirilerek güvenlik hizmetlerini yerine getirmede kullanılabilmektedir. Yüz tanıma ve eşleştirme; polis laboratuarlarında suçluların tespitinde, gerçek zamanlı yüz takibi; metro, havaalanları, stadyum girişleri gibi kalabalık alanlarda aranılan şahısların bulunmasında, robot yüz oluşturma, çoklu fotoğraf ve videolardan yüz modelleme ise eldeki veriler ışığında aranılan şahısların yüz modellerinin oluşturulması ve sabıkalı şahısların bulunduğu veri tabanından karşılaştırılma yapılmasında kullanılabilecek yöntemlerdendir [67,68].

4.2.6. Ses Tanıma

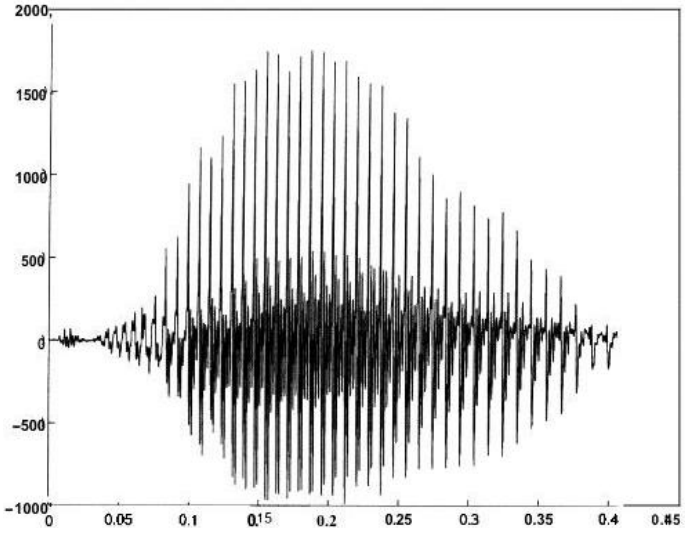
Ses tanıma sistemleri, sesin dijital bir veriye dönüştürülüp saklanması ve daha sonra diğer örneklerle karşılaştırılması mantığı üzerine kurulmaktadır. Bu tür sistemleri kullanacak kişiler önce kullanacakları kelimeyi ya da kelime grubunu birkaç defa sisteme tanıtmaktadırlar. Bu sırada sesin dalga boyu, şiddeti, frekansı gibi bilgiler veritabanına kaydedilmektedir. Ancak sesin karakteristiği ortamla ya da ruh haliyle kolayca değişebildiği için bu yöntemin güvenilirliği nispeten daha azdır. Hata oranı %1-15 arasında hesaplanmaktadır. Bu oranı düşürmek için yapılan çalışmalar devam etmektedir.

Ses tanıma sistemleri, sabit bir donanım ve yazılım grubu olarak dizayn edilebildikleri gibi telefon üzerinden dial-up bağlantıyla ulaşılan sistemler olarak da dizayn edilebilmektedirler. Güvenlik amacı dışında komut algılayan ses tanıma sistemleri de vardır. Bu sistemler, geniş kelime ve cümle veritabanlarına sahiptirler ve yapay zekâ kullanarak söylenişi aynı olan kelimeleri ayırt edebilmektedirler.

Hemen hemen bütün kriminal olaylarda ses, suçun işlenmesinde vasıta olarak kullanılmaktadır. Ses ve görüntü kasetleri içerisinde yer alan ses kayıtları, olayın ortaya çıkarılmasında eldeki tek delil olabilmekte ve şüpheliler ortaya çıkarılarak işlenen suçun faillerinin bulunmasını sağlayabilmektedir.

Ses tanıma ve tanımlama işlemi, bütün işitsel ve görsel duyuların kullanıldığı çok yönlü bir işlemdir [69]. Bu işlemi, bilinmeyen bir sesin bir veya daha fazla bilinen sesle tanınması veya elenmesi amacıyla işitsel veya görsel olarak karşılaştırılması şeklinde tanımlanabilir. Bu olayın temel olarak dayandığı varsayım, seslerin sahip olduğu karakteristik özellikleri yardımıyla, çeşitli analiz teknikleri uygulanarak diğerlerinden ayırt edilmesidir [70].

Ses tanıma ve tanımlama işlemi cinayet, soygun, hırsızlık, zorla kaçırma, tecavüz, uyuşturucu, kumar, kaçakçılık, başkası adına yapılan taklit konuşmalar, şantaj, rüşvet, tehdit telefonları, terörist eylemler, bombalı eylemler, suikast girişimleri gibi kriminal olaylarda kullanılmaktadır.

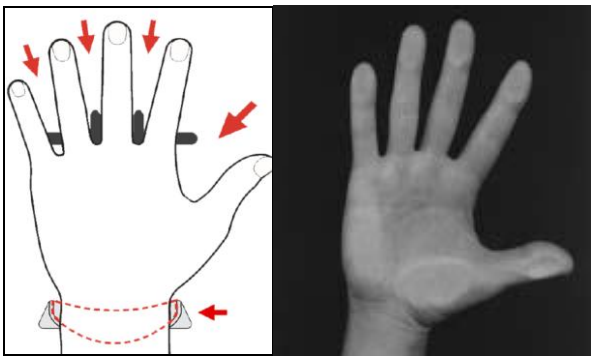


Şekil 15. Ses dalgası

4.2.7. El Geometrisi Tanıma

El geometrisi, kişi tanımada kişilerin el şekillerini kullanan bir biyometrik özelliktir. El görüntüsünün geometrik özellikleri analiz edilmekte ve parmakların uzunlukları, genişlikleri, kalınlıkları, avuç içi, büküm yerleri gibi özellikler incelenmektedir. Sistem, el ve parmak geometrisini dijital bir kamera ve ışık kullanarak ölçmektedir. El, ölçüm yuvasına konulmakta ve parmaklar ölçüm yuvasına uygun şekilde hizalanmaktadır. Bundan sonra kamera bir veya birden fazla resim alarak

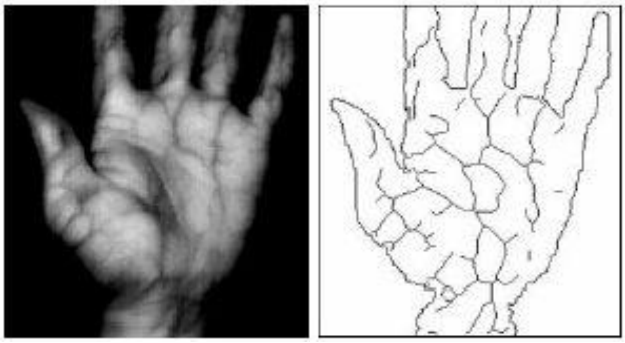
akabinde bu bilgilerden ele ait uzunluk, kalınlık, eğrilik bilgileri tespit edilip sayısal bilgiye çevrilmektedir [71].



Şekil 16. El geometrisi

4.2.8. Damar Tanıma

İris ve parmak izinde olduğu gibi damar yapıları da herkeste farklıdır. Bu farklılıktan yola çıkılarak damar tanıma sistemleri geliştirilmiştir. Tanımlama yapılacak uzuvdaki damar yapısını ortaya çıkarmak için infrared ışık gönderilmektedir. Kandaki hemoglobin ışığı emmekte ve damarlar siyah resimde görünür hale gelmektedir. Damarların görüntülenmesi hemoglobinin gönderilen infrared ışını soğurmasıyla mümkün olmakta, dolayısıyla tanımlama yapılan uzvun canlı olması yani içerisinde kan bulunması önem kazanmaktadır. Böylece uzvun canlı olup olmadığı bilgisine de ulaşılmaktadır. Ayrıca birçok damar, deri üzerinden görünür olmadığı için damar yapısının kopyalanması gibi bir şey söz konusu değildir. Bu da damar tanıma sistemlerinin güvenirliğini arttıran bir etmendir.



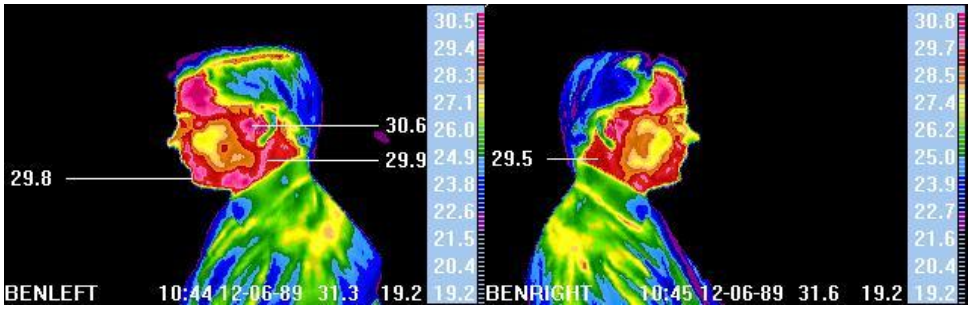
Şekil 17. El damar görüntüsü

4.2.9. Diş İzi Tanıma

Yapılan araştırmalar ısırık izinin herkeste farklı olduğunu göstermiştir. İster ciltte, ister cansız bir obje üzerinde olsun ısırık izinin, tek yumurta ikizleri de dâhil olmak üzere kişiye özel olduğu kanıtlanmıştır. Bu özelliğinden dolayı kriminal olaylarda delil olarak kullanılmaktadır. Isırık izleri saldırı sonucunda mağdurda, savunma sonucunda da saldırganda bulunabilmektedir. Dişler ve izin mukayesesi ile şüpheliyi tanımlamak ya da dışlamak mümkün olabilmektedir. Olay yerinde inceleme yapılırken rastlanan ısırık izleri "bilgisayarlı aksiyal tomografi (CAT: Computerized Axial Tomography)" ya da "toneline bite mark photography" yöntemleri ile model ile eşleştirilmektedir [72].

4.2.10. Yüz Termogramı

Yüzün ısı haritası çıkarma yöntemi 1996 yılında geliştirilen çok yeni bir teknolojidir. Bu yöntemde bir kızılötesi kamerayla yüzün görüntüsü çekilerek ısı haritası çıkarılmaktadır. Vücutta dolaşan kan, vücudun diğer bölgelerinden daha sıcak olduğu için çekilen görüntüde yüz derisinin altındaki damarların geçtiği yerler ve kalınlıkları açıkça belli olmaktadır. Bu özellikler her bireyde farklı olduğu için bu sistemlerin oldukça güvenilir olduğu kabul edilmektedir. Ayrıca tamamıyla karanlık bir ortamda da çalışabilmekte ve yüzdeki fiziksel değişimlerden etkilenmemektedir. Bu yöntemin en olumsuz tarafı, termal kameranın oldukça pahalı olmasıdır [60].

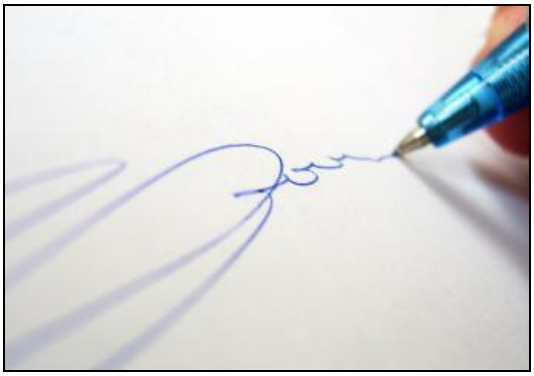


Şekil 18. Yüz termogramı

4.2.11. İmza Atımı

Dinamik imza tanıma olarak da bilinen bu yöntem, imza gerektiren her türlü resmi yazışmalarda kullanılmak amacıyla tasarlanmıştır. Dinamik olmalarının sebebi, imza şeklinin yanında imzayı atarken zemine yapılan basınç ya da kaç defa zemine dokunulduğu gibi durumları da inceleyen sistemler olmalarıdır. Hâlihazırda dünyada 100'den fazla patenti alınmış imza tanıma sistemi mevcuttur. Patent sahipleri arasında IBM, NCR, VISA gibi büyük şirketler de bulunmaktadır.

Bir kişinin imzasını taklit etmek, çok karışık bir imza da olsa, teorik olarak mümkündür. Ancak o imzanın atılışı sırasındaki şartları oluşturmak imkânsızdır. Bu şartlar; imzanın hızı, kalemin yaptığı basınç, kalemin kâğıttan yukarı kalktığı noktalar gibi özelliklerdir. Bu karakteristikler, imzanın şekli ile birleştiğinde hata yapma olasılığı çok azalmaktadır. Öte yandan bu sistemler, kişinin imza atma alışkanlıklarının zamanla değişebileceğini de göz önüne alarak art arda birçok kullanım sonucunda basınç, hız gibi karakteristikler üzerinde istatistiksel analizler yaparak bir sonraki kullanım hakkında fikir sahibi olabilmektedirler [60].



Şekil 19. Bir imza örneği

4.2.12. Konuşma Tanıma

Konuşma Tanıma (Speech Recognition) sistemleri, belirli bir kişi tarafından söylenmiş olan bir ifadenin metin karşılığını elde etmeye çalışır. Konuşma tanıma klavyeyi kullanmak yerine konuşarak komut vermeye ve konuşmaların yazıya dönüştürülmesine olanak sağlayan bir teknolojidir. Bu sistem çağrı merkezlerinde, engellilere yönelik uygulamalarda, gömülü sistemlerde kullanılmaktadır.

4.2.13. Tuş Vuruşu Tanıma

Tuş vuruş dinamiği, kişinin klavye kullanarak yazımı esnasında ritmindeki karakteristik bilgilerden kim olduğunu belirlemeye yarayan bir yöntemdir. En basit örneği, ikinci dünya savaşı sırasında, "Göndericinin Vuruşu" (The Fist of the Sender) olarak bilinen ritme bağlı olarak mors alfabesi ile gönderilen mesajın müttefikler veya düşmanlar tarafından gönderilip gönderilmediğini anlamada askeri istihbarat tarafından kullanılmaktaydı. Günümüzde, klavyenin yaygınlaşmasıyla birlikte biyometri alanında kullanımı da yaygınlaşmaya başlamıştır. Tuş vuruşu dinamiğinde, harflerin, karakterlerin veya rakamların yazımı esnasındaki ritim ve klavye kullanım hızlarını analiz ederek, karşılaştırma yapılacak biyometrik şablon kişiye özgü bir şekilde oluşturulmaktadır. Ham veri, tuş basım süresi ve tuş geçiş süresi gibi ölçümlerle oluşmaktadır. Tuş basış süresi bir tuşun ne kadar süre basılı kaldığını gösterir. Tuş geçiş süresi ise bir tuştan diğerine geçişin ne kadar zaman aldığını gösterir. Çünkü klavye kullanarak herhangi bir metni yazarken tuş basış süresi ve tuş geçiş süresi genel yazım hızından bağımsızdır. Metin ne kadar hızlı yazılırsa yazılsın tuş basış karakteristikleri kişiye özgüdür. Kişinin kullandığı dile bağlı olarak aşina olduğu kelimeleri daha hızlı yazabilmektedir. Ayrıca, örneğin kişi solak ise soldaki tuşları daha kolay bulabildiği ve sağdakileri bulmada ise gecikme yaşadığı belirlenmiştir. Bazı durumlarda, herhangi bir işyerinde yönetici belli işlemlerde yardımcı olması için asistanına bilgisayara giriş şifresini vermiş olabilir. Fakat her ikisi de aynı şifre ile giriş yaptığından dolayı bilgisayarın kullanımı esnasında kullanan kişinin yönetici mi yoksa asistan mı olduğu anlaşılamazken, klavye kullanım karakteristiği kimin bilgisayar başında olduğunu ayırt etmeye yarar. Ayrıca son zamanlarda geliştirilen yazılımlarla, fare benzeri bilgisayar bileşenlerinin kullanımında ivmelenme ya da tıklanma frekansı gibi bilgileri tuş vuruşu dinamiği ile birleştirerek değişik karşılaştırma şablonları oluşturabilmektedir. Ancak kişinin yazım stilinin farklı zamanlarda değişiklik gösterebilmesinden dolayı, şablon oluşturulması esnasında çok sayıda örnek alınması gerekmektedir. Uzaktan sohbet programlarındaki yazım esnasında değerlendirmeyi yapacak sistem, başka bir bilgisayarda ise iletimdeki gecikmeler tanıma işlemini güçleştirir. Kişiye bağlı olarak, klavyenin çeşidi ve nerede kullanıldığı da önemlidir. Örneğin hareketli bir araç içerisinde yazım şekli etkilenecektir. Ayrıca, bu biyometrik veri ancak klavye bilgisi olan kişilerde kullanılabilir. Klavye kullanım stili kişinin yorgun, uykusuz olduğunda ya da bilgisayar, klavye şekli değiştiğinde değişkenlik gösterebilir.

Böyle durumlarda fiziksel biyometrik özellikler kadar yüksek ayırt edici özelliğe sahip olmayabilir. Doğrudan birebir aynı olmasa da birbirine benzer tuş vuruş dinamiğine sahip kişiler olabilir. Bu yüzden şifreli kimlik doğrulama yöntemi ile birlikte kullanımı daha yüksek performans sağlayacaktır. Bu açıdan tuş vuruş dinamiği biyometrik veri olarak kullanımda dezavantajlara sahiptir. Ancak diğer biyometrik cihazlarla karşılaştırıldığında özel bir donanıma ihtiyaç duyulmaz. Her bilgisayarda bulunabilen bir klavye yeterlidir [73].

4.2.14. Yürüyüş Tanıma

Yapılan son araştırmalar, yürüyüş şeklinin kişiden kişiye farklılık gösteren ayırt edici bir özellik olduğunu ortaya koymaktadır. Bu sebeple, yürüyüş şeklini biyometrik güvenlik sistemlerinde kimlik doğrulama için kullanmak mümkündür. Bu güvenlik sistemlerinde, genellikle tünel veya koridor gibi uzun bir alana görüntü almak için kameralar yerleştirilmektedir. Kişinin bu mekândan yürüyerek geçişi esnasındaki hareketleri kameralar vasıtasıyla kaydedilmekte ve kaydedilen video üzerinde bilgisayarlı görü yöntemleri kullanarak, kişinin hareketleri tespit edilerek yürüyüş karakteristiğine ait özellikler elde edilmektedir. Son olarak bu özellikler, veri tabanına önceden eklenmiş yürüyüş şekli bilgileri ile karşılaştırılarak kimlik doğrulaması sağlanmaktadır. Yürüyüş şekli verisini kullanan biyometrik güvenlik sistemleri, kişilerin belirli bir mesafe boyunca yürürken görüntüsünün alınmasına ihtiyaç duyduğu için, küçük mekânlarda kullanılamamaktadır. Ancak, havaalanı gibi büyük tesislerde faydalı olabilmektedir [73].

5. ADLİ PARMAKİZİ VE SES ANALİZİ

Bu çalışmada parmak izi ve ses olmak üzere iki biyometrik özelliğin suçluların tespitinde kullanılmasını sağlayacak bir sistem tasarlanmıştır.

5.1. Problemin Tanımlanması

Her suçlu suçu işlerken olay yerinde izler bırakır. Suçun aydınlatılması ve olayın çözülmesi, olay sahnesinde bırakılan bu izlerin tespit edilmesi ve doğru bir şekilde analiz edilmesiyle mümkündür. Suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanılarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesi işlemlerini kapsayan sürece olay yeri incelemesi denir [40].

Olay yerinde sadece nitel gözlem yoluyla tespit edilebilecek deliller olabileceği gibi insanın duyu organlarıyla algılayamayacağı ancak nicel gözlem yapılarak elde edilebilen deliller de olabilir. Örneğin olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani nicel gözlem yapılmalıdır. Delillerin gizli yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirmektedir. [40].

Olay yerinden elde edilen delillerin değerlendirilmesi analiz sürecinde gerçekleştirilmektedir. Delillerin değerlendirme süreci, kullanılan yöntem ve teknikler ise tamamen delilin türüne bağlı olarak değişebilmektedir. Bu çalışmada dijital deliller ele alındığından olay yerinde bulunabilecek dijital delillerle örnek vermek yerinde olacaktır. Olay yerinde yer alan elektronik cihazlarda bulunan olayı aydınlatabilecek her türlü bilgi ile görüntü, ses, parmak izi ve DNA gibi verileri dijital delillere örnek verebiliriz. Günümüzde bilişim teknolojilerinde yaşanan süratli gelişmeler göz önüne alındığında işlenen suçların çoğunda dijital delillerin bulunabileceği ve bu olayların çözülebilmesi için dijital delillerin yapısının doğru şekilde analiz edilmesinin gerekliliği ortaya çıkmaktadır. Bu tez çalışmasında olay yerinde bulunan parmak izi ve ses biyometrik verilerinin analiz edilerek suçluya ait olup olmadığını belirlemek amaçlanmıştır.

5.2. Problemin Çözümlenmesi

Yaşayan ve ölü kişilerin kimliğinin tespit edilmesinde, sosyal, ekonomik ve ceza-i açıdan birçok yarar vardır. Bu nedenle kimlikle ilgili düzenleme ve uygulamalar günümüzde önemli bir yere sahiptir. Herhangi bir suçla ilgili soruşturmalarda ya da birçok insanın yaşamını kaybettiği olaylarda ölenlerin kimlik tespitinin yapılmasının insani, kanuni, dini, etik ve sosyal boyutu vardır [74]. Günümüzde kolluk kuvvetleri kimlik belirleme işlemlerini klasik yöntemlerin yanında gelişmiş teknolojinin nimetlerinden faydalanarak daha güvenilir ve daha hızlı bir şekilde gerçekleştirebilmektedirler. Biyometrik verilerin bilişim teknolojileri kullanılarak değerlendirilmesi ve kimlik tespitinde kullanılması şüphesiz birçok olayın çözülmesinde önemli rol oynamıştır. Bu noktada elde edilen biyometrik verilerin değerlendirilmesi için kullanılacak sistemlerin gerekliliği ön plana çıkmaktadır.

Bu tez çalışmasında biyometrik yöntemlerden parmak izi ve sesin kimlik tespitinde kullanılması amaçlanmıştır. Sistem, parmak izi eşleştirmesi yaparak iki ayrı parmak izinin benzerlik yüzdelerini vermekte ve aynı kişiye ait olup olmadığı konusunda fikir vermektedir. Aynı şekilde iki ses kaydını karşılaştırarak aynı kişiye ait olup olmadığını tespit etmekte böylece adli olaylarda parmak izinden ve sesten kimlik tespit etme konusunda bir çözüm sunmayı amaçlamaktadır.

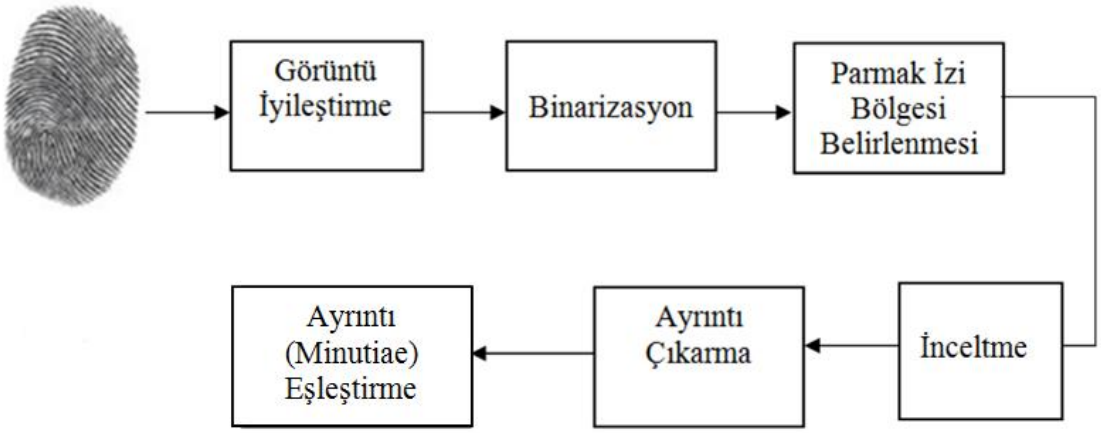
5.3. Sistemin Tasarımı

Tasarlanan sistemin otomatik parmak izi tanıma (OPTS) ve konuşmacı tanıma olmak üzere iki fonksiyonu bulunmaktadır.

5.3.1. OPTS Tasarımı

Parmak izi tanıma algoritmalarından en temel üç tanesi korelâsyon bazlı, ayrıntı (minutiae) bazlı ve çizgi (ridge) bazlı eşleme teknikleridir. Korelâsyon bazlı eşleme tekniğinde iki farklı parmak izindeki çizgi ve oluk-kırık modellemeleri karşılaştırılır. Ayrıntı (minutiae) bazlı eşleme tekniğinde ise ilk olarak parmak izindeki ayrıntı noktalarının yerleri belirlenir (çizgiler, çizgi sonlanmaları ve çatallanmalar gibi) ve bu ayrıntı noktaları oluş sıralarına göre karşılaştırılır. Son olarak çizgi (ridge) bazlı eşleme

tekniğinde çizgiye ait yön ve şekil bilgileri kullanılır [75]. Bu tezde ayrıntı (minutiae) bazlı eşleme tekniği kullanılmıştır.



Şekil 20. Ayrıntı eşleştirme algoritması

5.3.1.1.Parmak İzi Görüntüsünün İyileştirilmesi

Bir otomatik parmak izi tanıma sisteminde (OPTS), resim temizleme ve iyileştirme işlemleri oldukça önemlidir. Çünkü sonraki işlem basamaklarında elde edilen iyileştirilmiş resim, giriş olarak kullanılacaktır. Resmin bilgi taşımayan gereksiz kısımlarından ve gürültüden arındırılması, OPTS için işlem hızının artması, işlem zamanının kısalması, özellik noktalarının bulunmasında sistem başarımının ve güvenilirliğinin artması gibi bir takım üstünlükler sağlar. Resim ne kadar yüksek kalitede iyileştirilirse, OPTS'nin başarımı da o kadar artar [76] .

Görüntü iyileştirmek için birçok yöntem ve çeşitli filtreler kullanılmaktadır. Bu çalışmada Histogram Eşitleme ve Fourier Analizi yöntemleri kullanılmıştır.

- **Histogram Eşitleme**

Histogram, görüntü üzerindeki piksellerin değerlerinin grafiksel ifadesidir. Buna görüntü histogramı veya gri-düzey histogramı denir. Görüntü histogramı, görüntünün her bir noktasındaki piksellerin tespiti ile bu piksellerin sayısının ne kadar olduğunu gösterir. Bu sayede histogram üzerinden görüntü ile ilgili çeşitli bilgilerin çıkartılması sağlanır.

Matematiksel olarak, bir dijital görüntü histogramı Eşitlik 5.1'de verildiği gibi tanımlanabilir:

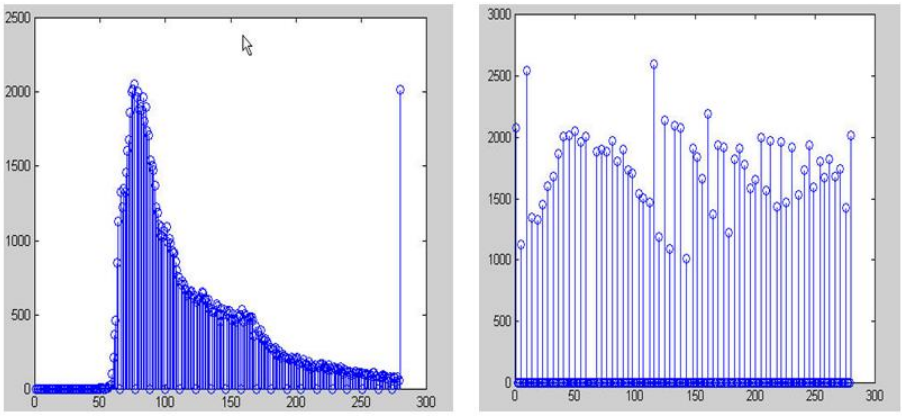
$$p(r_k) = \frac{n_k}{n} \tag{5.1}$$

Burada;

r_k: k'ıncı gri seviye,

n_k: bu gri seviyeye sahip toplam piksel adedi,

n: görüntü üzerindeki toplam piksel adedi, olarak tanımlanmıştır.



Şekil 21. Histogram eşitleme

- **Fourier Dönüşümü**

Fourier dönüşümü, zaman tanım kümesindeki bir işaretin frekans içeriğini analiz etme imkanı tanımaktadır. Dönüşüm, ilk olarak tanım kümesi zaman olan bir fonksiyonu, tanım kümesi frekans olan bir fonksiyona çevirmek suretiyle çalışır. O zaman sinyalin frekans içeriği incelenebilir. Çünkü dönüştürülen fonksiyonun Fourier katsayıları, her frekans değerinde sinüs ve kosinüs fonksiyonlarının her birinin katkısını temsil eder. Ters Fourier dönüşümü de, verinin frekans tanım kümesinden zaman tanım kümesine dönüştürülmesini gerçekleştirir. Bu çalışmada parmak izi resimleri 32x32 pixellik bloklara bölünüp fourier dönüşümü gerçekleştirilmiştir;

$$f(u,v) = \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x,y).e^{-j2\pi(\frac{ux}{m}+\frac{vy}{n})} \tag{5.2}$$

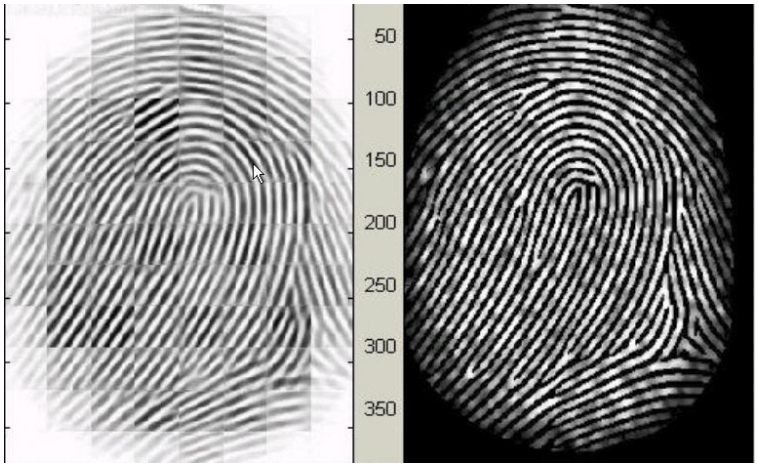
u = 0, 1, 2, ..., 31 ve v = 0, 1, 2, ..., 31.

$$g(x,y) = F^{-1}\left\{F(u,v).\left|F(u,v)\right|^{k}\right\} \tag{5.3}$$

$$f(x,y) = \frac{1}{MN} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(u,v).e^{j2\pi(\frac{ux}{m}+\frac{vy}{n})} \tag{5.4}$$

x = 0, 1, 2, ..., 31 ve y = 0, 1, 2, ..., 31.

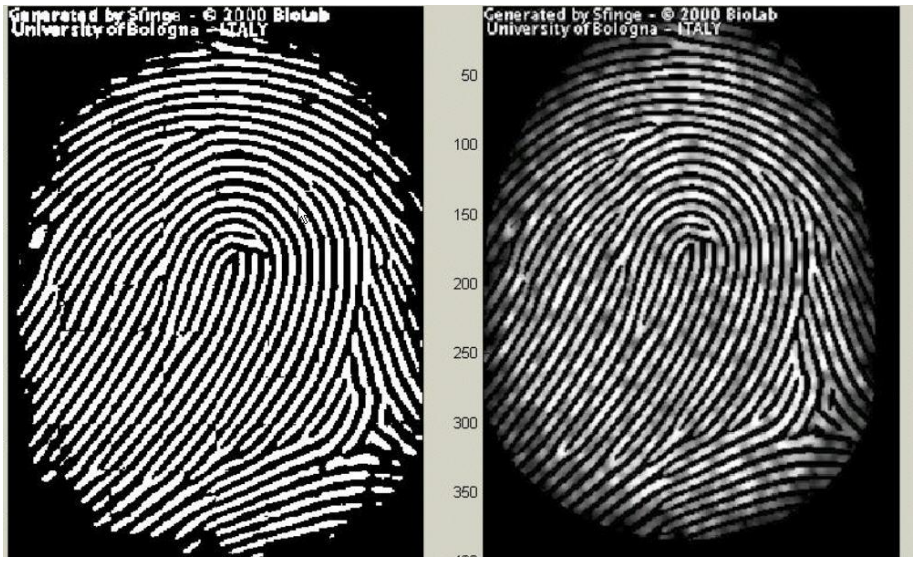
Eşitlik 5.2'deki "k" deneysel olarak belirlenmiş bir katsayıdır. Bu çalışmada k=0.45 alınmıştır. k değerinin çok fazla büyütülmesi parmak izi görüntüsündeki bazı bitiş noktalarını çatal noktasına dönüştürebilmekte bu da ayrıntı noktalarının yanlış belirlenmesine yol açabilmektedir.



Şekil 22. Fourier dönüşümü

5.3.1.2. Binarizasyon (İkilendirme)

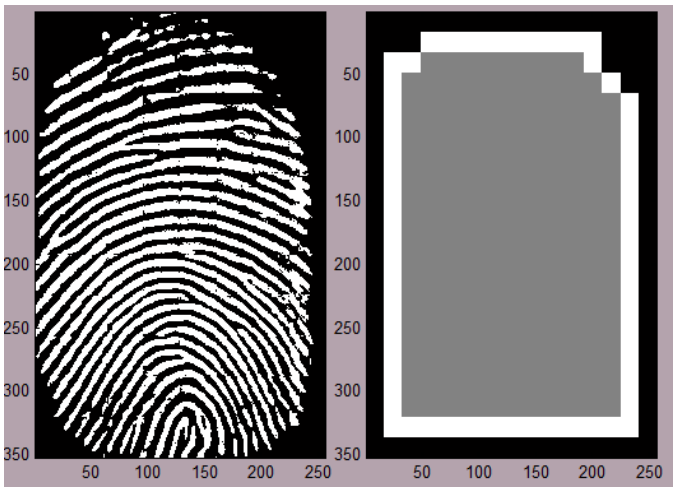
Temizlenip iyileştirilmiş bile olsa, gri seviye bir parmak izi resmi üzerinde işlem yapılması, özellik noktalarının bulunması oldukça zor bir iştir. Resim analizinin daha kolay ve hızlı bir şekilde gerçekleştirilebilmesi için, resmin siyah beyaz renk değerlerinden oluşan ikili hale dönüştürülmesi gereklidir. Bir parmak izi resmine ikili dönüşüm uygulanırken, resmin renk değerlerinin ortalaması göz önünde bulundurularak bir eşik değeri belirlenir. Bu eşik değerinden küçük değerlerin yerine siyah, büyük değerlerin yerine ise beyaz konularak resim ikili hale çevrilir [76].



Şekil 23. Binarizasyon işlemi

5.3.1.3. Parmak İzi Bölgesinin Belirlenmesi

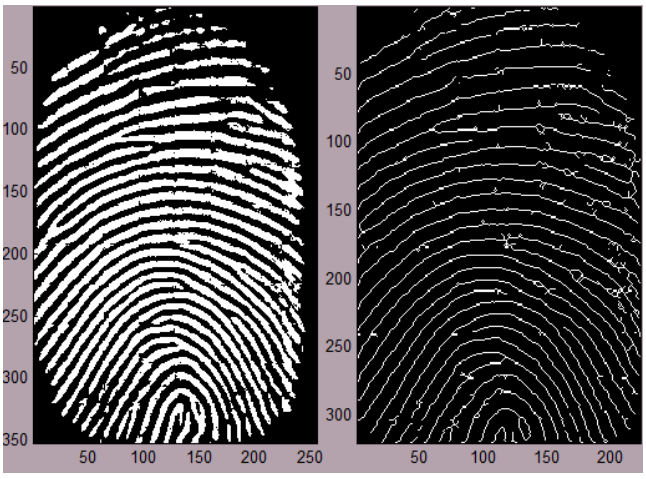
Parmak izi tanıma işleminin başarıyla gerçekleştirilebilmesi için sisteme giriş olarak verilen parmak izi ile veritabanında kayıtlı bulunan parmak izi resimlerinin aynı bölgeleri üzerinde çalışılması gerekmektedir. Bu nedenle geliştirilen OPTS özellik noktalarını ve bunlarla ilgili parametreleri bulurken parmak izine ait belli bir bölge üzerinde işlem yapmaktadır. Bu, sistemin güvenilirliği, performansı ve hızı açısından önemlidir [76].



Şekil 24. Parmak izi alanının belirlenmesi

5.3.1.4. İnceltme

İnceltme, parmak izi resmi üzerinde bulunan her bir hat çizgisi genişliğinin daraltılarak 1 piksel ile ifade edilmesi şeklinde tanımlanabilir. Resim inceltme ve inceltilen resmi iyileştirme işlemi tamamlandığında resim özellik noktalarının bulunması için hazır hale gelir.



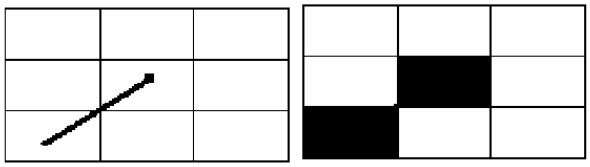
Şekil 25. Parmak izi resminin inceltilmesi

5.3.1.5. Ayrıntı (Minutiae) Çıkarımı

Parmak izi binarize edildikten ve inceltildikten sonra ayrıntılar belirlenmektedir. Parmak izinin tespitinde referans olarak kullanılan noktalar bitiş, çatal ve tek noktalardır. Bitiş noktaları tepenin sonlandığı piksele karşılık gelmektedir. Çatal noktaları ise tepe

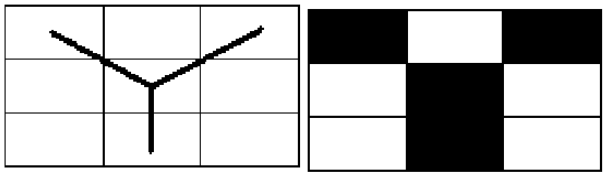
hattının iki farklı kola ayrıldığı piksele karşılık gelmektedir. Tek nokta ise etrafında komşusu olmayan tek piksele tekabül eden noktadır [77, 78].

Bitiş noktası, parmak izindeki bir tepe çizgisinin sonlandığı yerdir. İlgilenilen piksel 3x3 lük bir matrisin orta noktası olarak düşünülür ve komşulukları incelenir. Eğer etrafında sadece bir komşuluğu varsa bu nokta bir bitiş noktasıdır denilebilir [78].



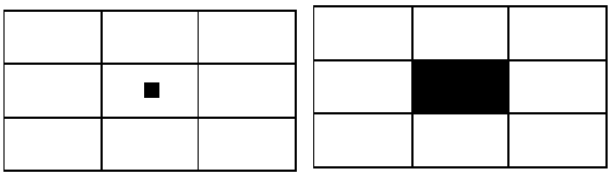
Şekil 26. Bitiş noktasının tespit edilmesi

Çatal noktası, parmak izindeki bir tepe çizgisinin iki farklı kola ayrıldığı yerdir. İlgilenilen piksel 3x3 lük bir matrisin orta noktası olarak düşünülür ve komşulukları incelenir. Eğer etrafında üç komşuluğu varsa bu nokta bir çatal noktasıdır denilebilir [78].



Şekil 27. Çatal noktasının tespit edilmesi

Tek nokta, parmak izindeki bir tepe çizgisine mensup olmayan etrafında hiçbir tepe çizgisi olmayan pikseldir. İlgilenilen piksel 3x3 lük bir matrisin orta noktası olarak düşünülür ve komşulukları incelenir. Eğer etrafında komşuluğu yok ise bu nokta bir tek noktadır denilebilir [78].



Şekil 28. Tek noktanın tespit edilmesi

5.3.1.6. Ayrıntı (Minutiae) Eşleştirme

Parmak izi algılama ve doğrulama sistemlerinde piksel ya da iz tabanlı eşleme yerine nokta tabanlı eşleme algoritmaları kullanılır. Nokta tabanlı eşlemede geometrik/nokta tabanlı eşleme ve grafik tabanlı eşleme olmak üzere iki temel teknik vardır. Bu çalışmada geometrik/nokta tabanlı eşleme tekniği uygulanmıştır.

Nokta tabanlı eşleme basit geometrik, trigonometrik hesaplamaları içerir. Nokta tabanlı eşlemede, hizalama aşamasında giriş ve eşleme yapılacak taslak arasında çevirme, döndürme ve boyutlandırma gibi dönüşümler hesaplanır ve hesaplanan parametrelere göre giriş ayrıntı noktaları, taslak ayrıntı noktaları ile hizalanır [78].

İki nokta kümesini hizalamak için genelde aşağıdaki eşitlik kullanılır.

Girilen ve taslak görüntüdeki hatların kümesi R^d, R^D ise, her bir hat uzunluğu $d \varepsilon R^d$ ile $D\varepsilon R^D$ eşlenir.

$$S = \frac{\sum_{i=0}^{L} d_i D_i}{\sqrt{\sum_{i=0}^{L} d_i^{\,2} D_i^{\,2}}} \tag{5.5}$$

L: iki hat arasındaki minimum uzunluk

D_i,d_i : i. noktanın x ekseninden olan uzaklık

Eğer ilişki değeri (S) 0.8' den büyük ise kabul edilir ve bir sonraki eşlemeye geçilir. Eşlemeden sonra hizalama aşamasına geçilir. Dönüklük açısı ve dönüşüm vektörü hesaplanır.

$$\begin{pmatrix} \Delta x \\ \Delta y \end{pmatrix} = \begin{pmatrix} x^d \\ y^d \end{pmatrix} - \begin{pmatrix} X^d \\ Y^d \end{pmatrix}$$

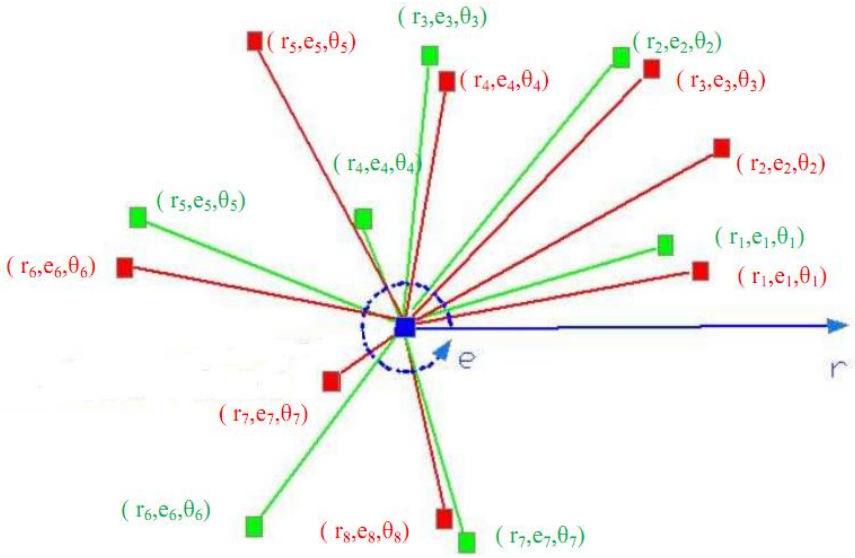
$$\Delta\theta = \frac{1}{L}\sum_{i=0}^{L}(\gamma_i - \Gamma_i) \tag{5.6}$$

Γ, γ : Referans noktaya göre i. noktanın radyal açılarıdır.

Girilen N sayıdaki özellik noktasının dönüşümü aşağıdaki şekilde yapılır.

$$\begin{pmatrix} x_i^{\,A} \\ y_i^{\,A} \\ \theta_i^{\,A} \end{pmatrix} = \begin{pmatrix} \Delta x \\ \Delta y \\ \Delta\theta \end{pmatrix} + \begin{pmatrix} \cos\Delta\theta & \sin\Delta\theta & 0 \\ \sin\Delta\theta & -\cos\Delta\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_i - x^d \\ y_i - y^d \\ \theta_i - \theta^d \end{pmatrix} \tag{5.7}$$

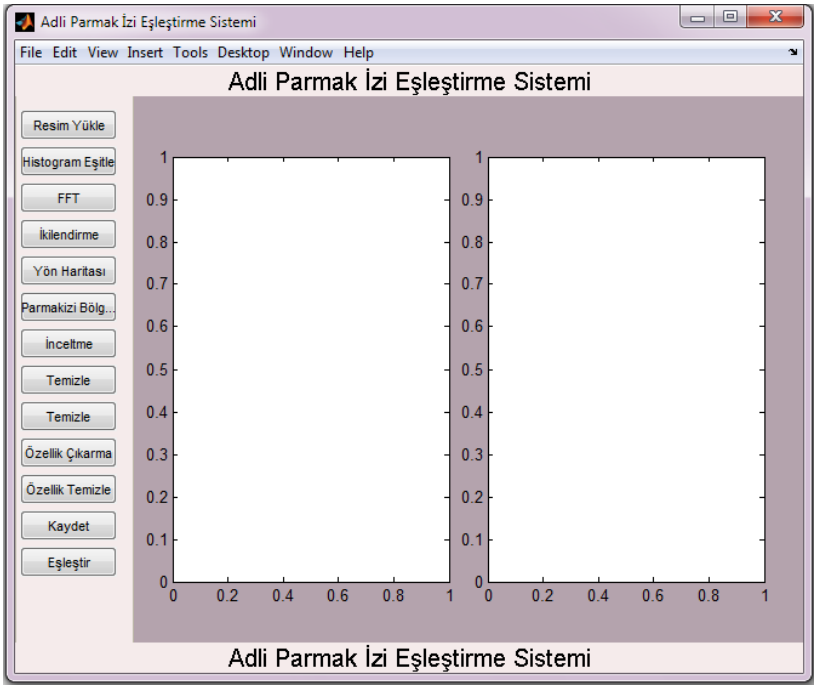
Dönüşümden sonra noktalar referans noktaya göre kutupsal koordinat sistemine çevrilir.



Şekil 29. Noktaların referans noktaya göre koordinat sistemine dönüştürülmesi

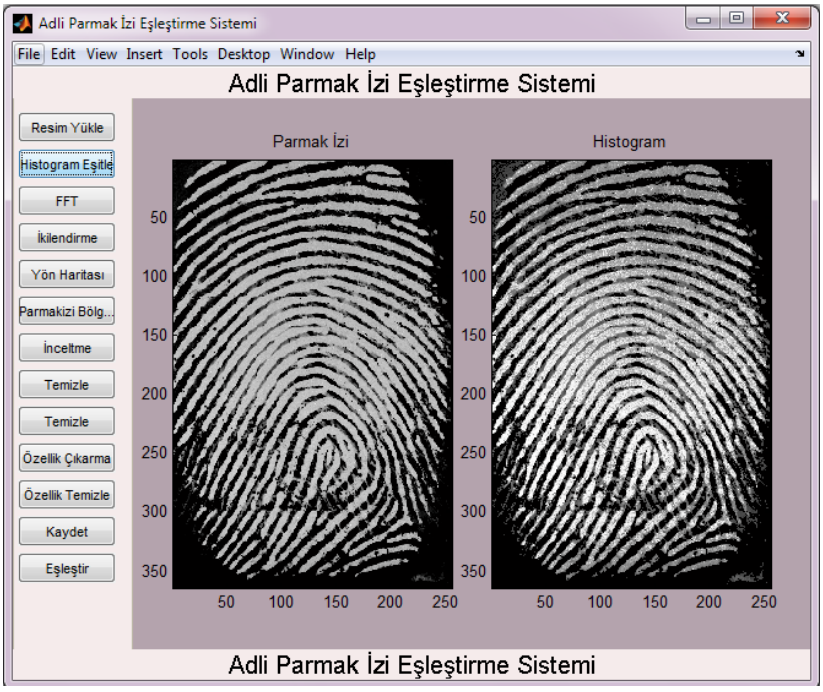
5.3.1.7. Parmak İzi Eşleştirme Uygulaması

Parmak izi eşleştirme uygulamasının çalışma görüntüsü Şekil 30'da gösterilmektedir. Pencerenin sol tarafında bulunan butonlar ile parmak izi resmi alınarak görüntü iyileştirilmekte, özellik noktaları belirlenmekte ve özellik noktaları eşlenerek aradaki benzerlik oranı yüzde olarak verilmektedir. Resim üzerinde yapılan her işlem basamağı aşama aşama görüntülenmektedir.



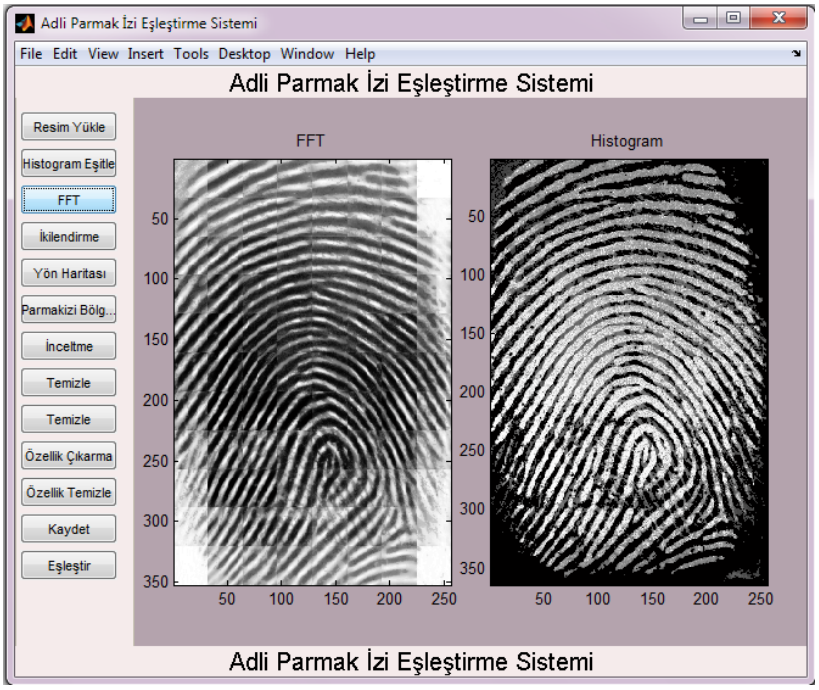
Şekil 30. Parmak izi eşleştirme sistemi

"Resim Yükle" butonu kullanılarak dosyadan .tif formatındaki parmak izi resmi alınmaktadır. Daha sonra sırayla butonlara tıklanarak parmak izi görüntüsü işlenmektedir. Her bir işlem basamağının resim üzerinde meydana getirdiği değişiklik görülebilmektedir. İlk olarak "Histogram Eşitle" butonun tıklanarak resmin histogram eşitlemesi gerçekleştirilmektedir.



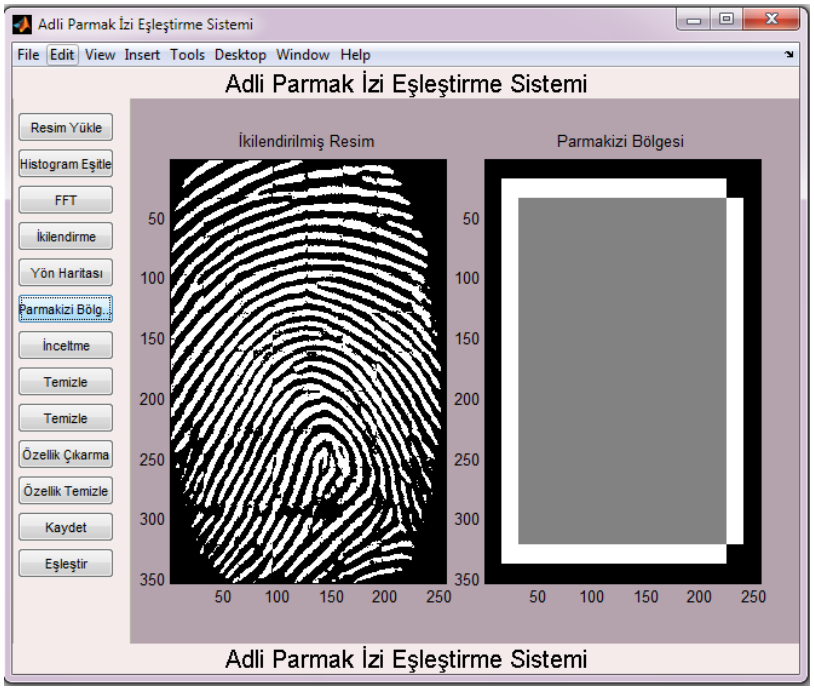
Şekil 31. Histogram eşitlemesi

Histogram eşitlemesi yapılan resim “FFT” butonuna tıklanarak Fourier Dönüşümü gerçekleştirilerek iyileştirilmiştir.



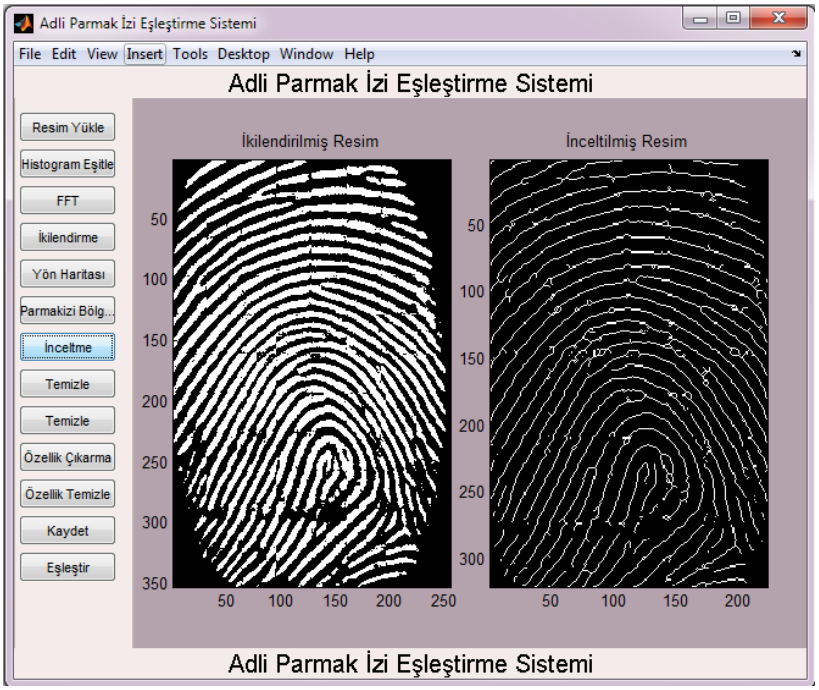
Şekil 32. Fourier dönüşümü

Histogram eşitlemesi ve Fourier Dönüşümü ile iyileştirilen parmak izine binarizasyon işlemi uygulanır ve siyah beyazdan oluşan ikili hale getirilir. Daha sonra OPTS’nin özellik noktalarını ve bunlarla ilgili parametreleri bulurken işlem yapacağı parmak izi bölgesi belirlenir.



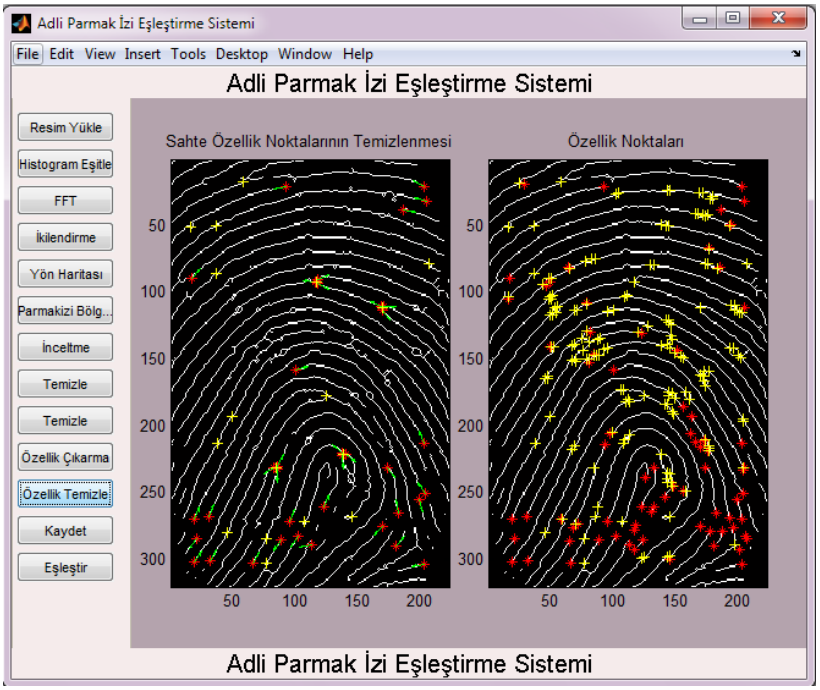
Şekil 33. Binarizasyon ve parmak izi bölgesinin belirlenmesi

İkilendirilmiş resim üzerinde inceltme işlemi yapılarak her bir hat çizgisi genişliği daraltılarak 1 piksel ile ifade edilmiştir. İnceltilen resim üzerinde temizleme işlemi yapılarak fazlalıklar temizlenmiş ve resim özellik noktalarının bulunması için hazır hale gelmiştir.



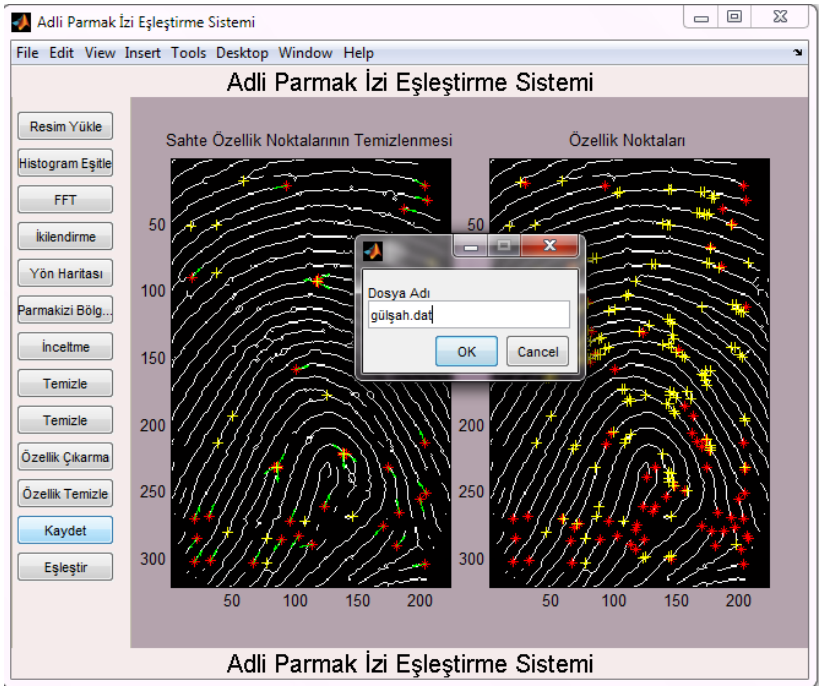
Şekil 34. İnceltme işlemi

İyileştirilen ve inceltilen parmak izi resmi özellik noktalarının bulunmasına hazır hale gelmiştir. Şekil 35'te sağ tarafta özellik noktaları tespit edilmiştir. Sarı renkle işaretlenen noktalar çatal noktası ve kırmızı renkle işaretlenen noktalar bitiş noktalarıdır. Özellik noktaları belirlendikten sonra sahte özellik noktaları temizlenmiş ve sol taraftaki görüntü elde edilmiştir. Bu resimdeki yeşil renkle işaretlenen noktalar gerçek özellik noktalarıdır.



Şekil 35. Özellik noktalarının belirlenmesi

Özellik noktalarının tespit edilen parmak izi şablonu kaydedilir.

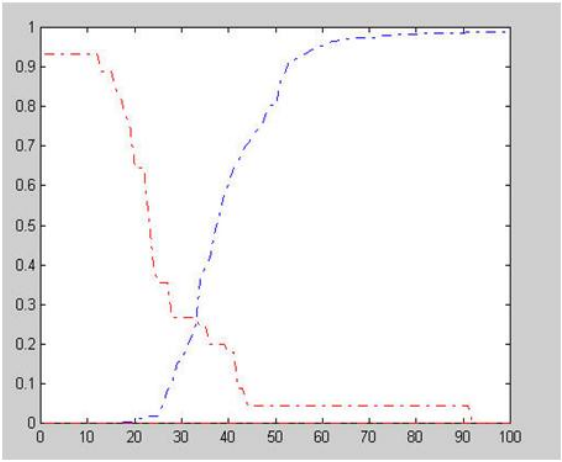


Şekil 36. Oluşturulan parmak izi şablonunun kaydedilmesi

Kaydedilen parmak izi şablonu daha önceden kaydedilen şablonlarla eşleştirilir ve benzerlik yüzdesi bulunur.

Şekil 37. Eşleştirilen parmak izi şablonları arasındaki benzerlik oranının gösterilmesi

Uygulamada, parmak izi için FVC2000 veri tabanındaki parmak izi görüntüleri kullanılmıştır. Hatalı eşleme kabul oranı (False Acceptance Rate- FAR) ve Hatalı eşleme ret oranı (False Reject Rate -FRR) olarak bilinen bu istatistiksel ölçümler, bir biyometrik sistemin güvenilirliği hakkındaki en doğru bilgiyi verirler. Yanlış kabul oranı, yetkili olmayan kişilerin giriş izni alma olasılığıdır. Yanlış ret oranı ise yetkili bir kişiye giriş izni verilmemesi olasılığıdır. FAR ve FRR oranları Şekil 38'de gösterilmiştir.



Şekil 38. Parmak izi eşleştirme sistemi FAR ve FRR oranları
Mavi Çizgi**:** FRR oranı
Kırmızı Çizgi: FAR oranı

Şekil 36 incelendiğinde sistemin eşit hata oranının (EER) %25 civarında olduğu ve %75 doğrulama oranına sahip olduğu görülmektedir.

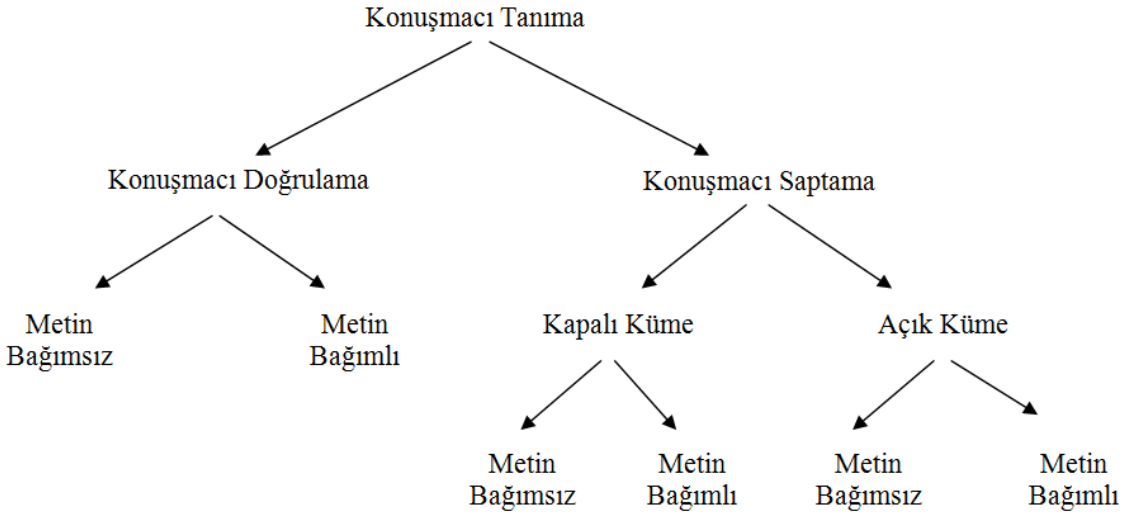
5.3.2. Konuşmacı Tanıma

Konuşmacı tanıma, ses dalgalarında bulunan konuşmacıya özgü bilgileri kullanarak, konuşmacılar arasından kimin konuştuğunun saptanmasıdır. Konuşmacı tanıma iki ana bölüme ayrılabilir;

- Konuşmacı doğrulama (speaker verification)
- Konuşmacı saptama (speaker identification)

Konuşmacı doğrulama, bilinmeyen bir ses örneğinin, iddia edilen kişiye ait olup olmadığının belirlenmesidir. Konuşmacı doğrulama, iletişim hizmetlerinde, bankacılık hizmetlerinde, özel kayıtlara vb. güvenli erişimler sağlamak amacıyla birçok uygulamada

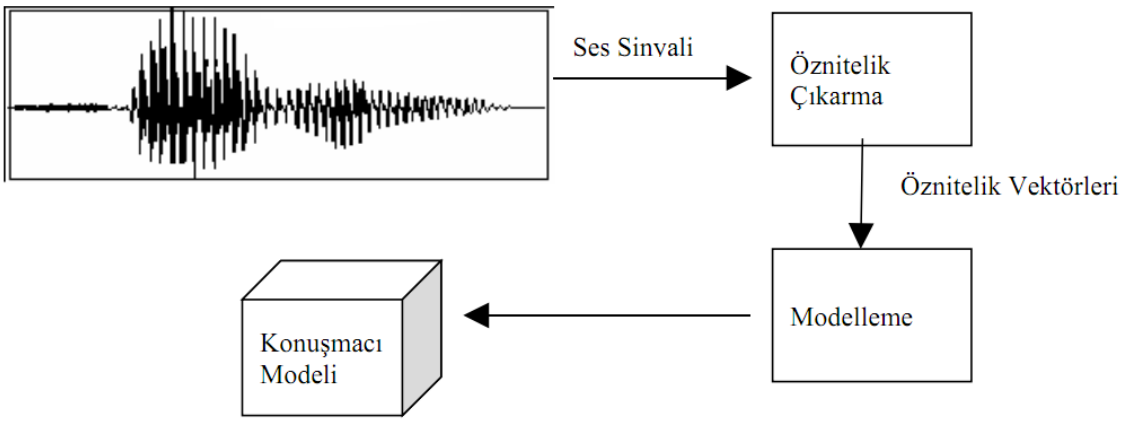
kullanılabilmektedir. Konuşmacı saptama ise bilinmeyen bir ses örneğinin, belli konuşmacıların ses kayıtlarından oluşan bir veritabanı içerisinde hangi kişiye ait olduğunun bulunmasıdır. Konuşmacı tanıma, metin bağımlı (text- dependent) ya da metin bağımsız (text- independent) olabilmektedir. Metin bağımlı sistemlerde konuşulan metin sistem tarafından önceden bilinmektedir. Metin bağımsız sistemlerde ise, metin, herhangi bir sözdizimi olabilmektedir. Diğer taraftan, konuşmacı tanıma, açık küme ya da kapalı küme olabilir. Kapalı kümede bilinmeyen ses örneği, veritabanındaki konuşmacılardan birisine aittir. Açık kümede ise ses örneği veritabanındaki konuşmacılardan hiç birisine ait olmayabilir [79].



Şekil 39. Konuşmacı tanıma sınıflandırma aşamaları

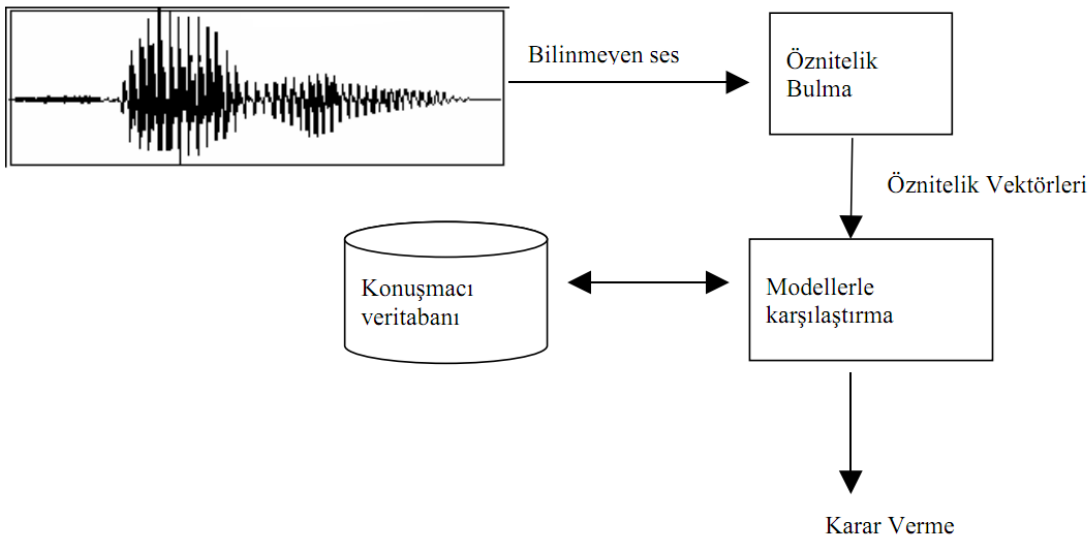
5.3.2.1. Konuşmacı Saptama

Konuşmacı saptama, kaydolma aşaması (enrollment) ve saptama (identification) aşaması olmak üzere iki aşamadan oluşmaktadır. Kaydolma aşamasında konuşmacıların tüm ses örnekleri alınarak çeşitli sinyal işleme teknikleriyle işlenmekte ve öznitelik vektörleri çıkarılarak bir veritabanında saklanmaktadır. Kaydolma aşmasının amacı her konuşmacı için bir referans modeli oluşturmaktır. Daha sonra bu modeller saptama aşamasında kullanılırlar.



Şekil 40. Kaydolma aşamasının genel diyagramı [79].

Saptama aşamasında, girdi olarak verilen bilinmeyen bir ses örneği işlenip öznitelik vektörleri çıkarılmakta ve veritabanında bulunan seslerin öznitelik vektörleri ile bir karşılaştırma algoritması yardımıyla (matching algorithm) karşılaştırılmaktadır. Bu işlem sonunda her model için bir benzerlik değeri bulunur. Bulunan en benzer model, ses örneğinin sahibi olarak nitelendirilir.



Şekil 41. Saptama aşamasının genel diyagramı [79].

5.3.2.2. Öznitelik Çıkarma

Öznitelik, bir sinyalin sahip olduğu başlıca karakteristik özelliklerdir. Ses işleme alanında en çok kullanılan ve daha önce yapılan çalışmalarda en iyi sonuç vermiş olan öznitelikler Mel Frekans Kepstrum Katsayıları (Mel-Frequency Cepstrum Coefficients, MFCC) ve Doğrusal Öngörü Katsayılarıdır (Lineer Prediction Coefficients, LPC)[80]. Bu

çalışmada öznitelik olarak MFCC kullanılmıştır. Öznitelik çıkarma işlem adımları aşağıdaki gibidir:

1. **Çerçeveleme (Frame Blocking):** Araştırmalar göstermiştir ki ses sinyali karakteristikleri yeteri kadar küçük bir zaman aralığında kararlı kalmaktadır. Bu nedenle ses sinyali 20-30 ms'lik çerçeveler halinde incelenmekte ve akustik özellikleri çıkarılmaktadır. Başarılı çerçeveler arası kaydırma zamanı ise tipik olarak 5-10 ms'dir. Bu şekilde bir sinyalin incelenmesine kısa süreli analiz de denir [81].
2. **Pencereleme:** Ses sinyali içerisinde çok fazla bilgi içermeyen kısımların kesilmesi için kullanılır. Pencerelemenin amacı çerçeve başında ve sonundaki süreksizlikleri ortadan kaldırmaktır. Bu işlemde x(n) sinyali ile çerçevelenmiş sinyal w(n) çarpılır ise pencerelenmiş sinyal elde edilir. Bu aşamada en çok kullanılan pencereleme fonksiyonlarından birisi Hamming fonksiyonudur. Hamming fonksiyonu, aşağıdaki gibi tanımlanır [79, 81].

$$y_1(n) = x_1(n).w(n) \qquad 0 \le n \le N-1$$

$$w(n) = 0{,}54 - 0{,}46.\cos\left(\frac{2\pi\, n}{N-1}\right) \qquad 0 \le n \le N-1 \tag{5.8}$$

$w(n)$: Çerçevelenmiş sinyal

$y_1(n)$: Pencerelenmiş sinyal

1. FFT (Hızlı Fourier Transform): Bir çerçevenin zaman alanından frekans alanına alınabilmesi için Hızlı Fourier dönüşümü kullanılır. Sürekli sinyal için Fourier dönüşüm formülü şu şekildedir [81].

$$X(f) = \int_{-\infty}^{\infty} x(t).e^{i2\pi f t}.dt \tag{5.9}$$

Sürekli bir sinyal ile ayrık zamanda çalışabilmek için onu sonlandırmak Discrete Fourier Transform (DFT) uygulanması gerekmektedir.

$$X_k = \sum_{n=0}^{N-1} x_n . e^{-2\pi i / N} \qquad k = 0,..., N-1 \tag{5.10}$$

2. Mel Frekansı Saptırması: Normal bir insan kulağı frekansları doğrusal olmayan bir şekilde algılar. İnsan kulağının frekans yanıtını karakterize eden ölçüye Mel-Ölçüsü (Melodi Ölçüsü) denir. Konuşmacı tanımanın bu aşaması bant geçiren süzgeç (band pass filter) olarak kullanılır. Bir frekansı mel-frekansına çevirmek için aşağıdaki formül kullanılır:

$$m = 2595 \log_{10} .(1 + f / 700) \tag{5.11}$$

f : hertz biriminden frekans

m : mel frekansı

3. Kepstrum: Öznitelik çıkarmanın son aşaması olarak, her çerçeveye ters fourier dönüşümü uygulanır ve frekans uzayından tekrar zaman uzayına döndürülür. Bu işlemin sonucu olarak Mel-Frekansı Kepstral Katsayıları (MFCC: Mel-Frequency Cepstral Coefficients) elde edilir. MFCC aşağıdaki gibi hesaplanır:

$$MFCC_i = \sum_{k=1}^{20} X_k . \cos\left[i . \left(\frac{k-1}{2} \right) . \frac{\pi}{20} \right] \qquad i = 1,2,..., M \tag{5.12}$$

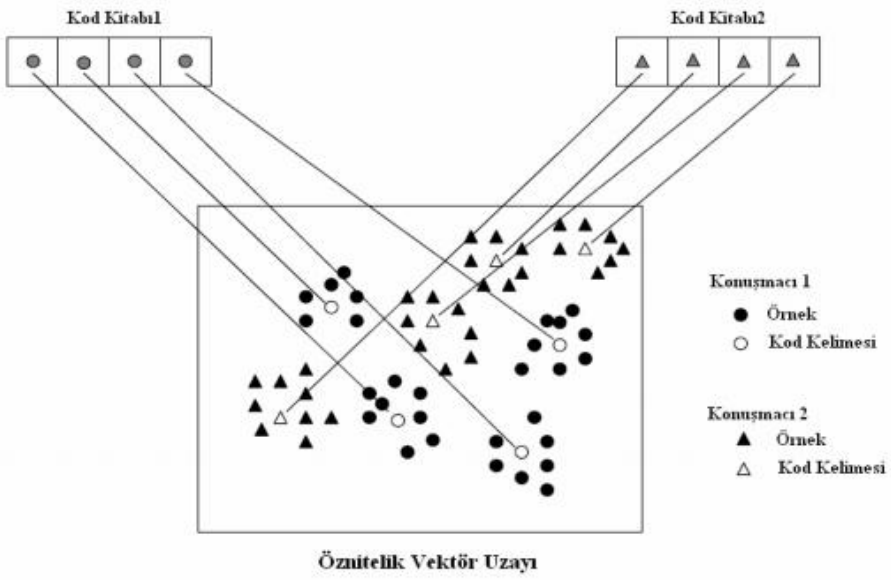
5.3.2.3. Vektör Niceleme (Vector Quantization)

Kepstrum aşamasından sonra elde edilen öznitelik vektörlerinin sayısı çok büyük boyutlardadır. Yüksek boyutlarda veriyi işlemek çok zaman alacağından bu vektörlerin bir yöntemle daha küçük boyutlara indirgenmesi sağlanmalıdır. Vektör niceleme geniş bir vektör uzayından sınırlı sayıda bölgeye dönüşüm gerçekleştiren bir tür veri sıkıştırma yöntemidir. Bu yöntemle her bir konuşmacıdan elde edilen öznitelik vektörü M adet bölgeye gruplandırılarak konuşmacı modeli oluşturulur. Her bir bölge kod kelimesi olarak isimlendirilen merkez noktasıyla temsil edilir. Kod kelimeleri ise kod kitabını oluşturur. N

adet eğitim vektörü kümesini M adet (M<N) kod kitabı vektörüne sıkıştırmada kullanılan yöntemlerden birisi LBG algoritmasıdır. Bu çalışmada LBG algoritması kullanılmıştır [79, 82]. Bu algoritma aşağıdaki özyinelemeli prosedür takip edilerek gerçekleştirilir.

1. Bütün eğitme vektörlerinin ağırlık merkezi bulunur.
2. Bütün eğitme vektörleri en yakın sınıfa konur
3. Her sınıfın ağırlık merkezi hesaplanır. Bu ağırlık merkezi o sınıfı temsil edecek kod vektördür.
4. Toplam bozulma hesaplanır. Toplam bozulma miktarı ile bir önceki yinelemedeki bozulma miktarı arasındaki fark büyükse 2. adıma dönülür.
5. Kod vektör sayısı yeterli ise özyineleme durdurulur.
6. Her kod vektör ikiye bölünür

Şekil 42'de iki konuşmacıya ait iki boyutlu öznitelik uzayının VQ yöntemiyle sınıflandırılması gösterilmiştir.



Şekil 42. İki konuşmacı için vektör nicemleme

5.3.2.4. Öznitelik Karşılaştırma

Son aşama olan karar verme aşamasında bilinmeyen ses örneğinin öznitelik vektörleri, veritabanına önceden kaydedilmiş diğer konuşmacılara ait öznitelik vektörleriyle karşılaştırılır. En iyi bilinen karşılaştırma algoritmalarından birisi, vektörler arasındaki öklid uzaklıklarının bulunmasıdır. Benzerlik ölçüsü iki vektör arasındaki uzaklık ile ters orantılıdır. Şöyle ki iki vektör birbirine ne kadar yakınsa, aralarındaki uzaklık değeri azalır ancak benzerlik değeri de artar. Öklid uzaklığını, konuşma saptama sistemine uyarlarsak, ses örneği için bulunan kod kitabı ile modellere ait olan kod kitapları arasındaki benzerlik bulunurken kullanılacak formül aşağıdaki gibidir:

$$S(C_k, C_x) = \sum_{i=1}^{T} \frac{1}{d_{\min}(v_i, C_x)} \tag{5.13}$$

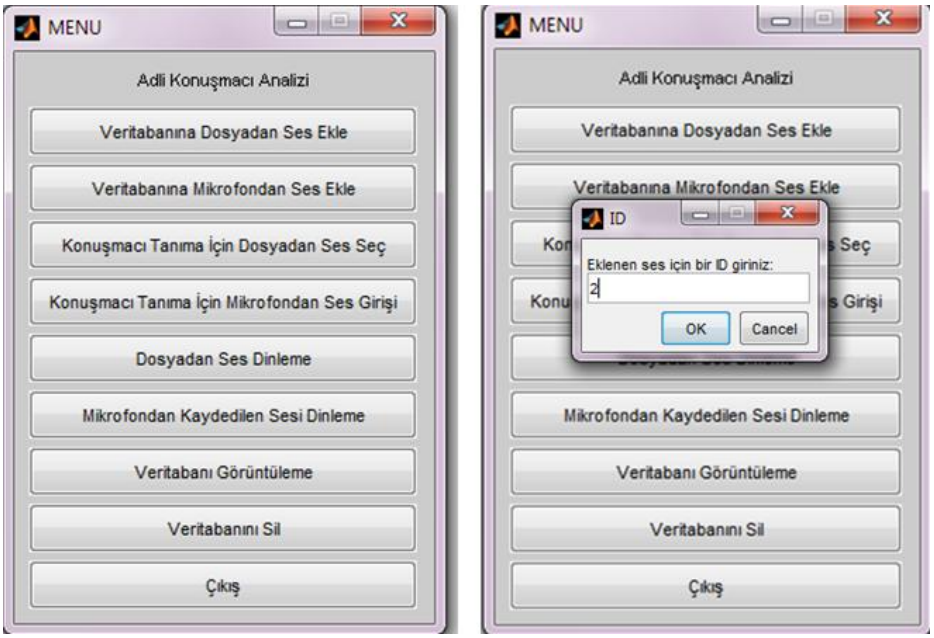
$S(C_k, C_x)$	:	İki kod kitabı (C_k, C_x) arasındaki benzerlik değeri
C_x	:	Bilinmeyen ses örneğine ait kod kitabı
C_k	:	Konuşmacı veritabanındaki k. kod kitabı
v_i	:	C_k kod kitabındaki i. kod vektörü
d_{min} (v_i, C_x)	:	v_i kod vektörüne C_x kod kitabındaki en yakın uzaklıkta bulunan kod vektörünün uzaklığı
T	:	Kod kitaplarındaki vektör sayısı (bütün kod kitaplarında aynıdır)

5.3.2.5. Konuşmacı Tanıma Uygulaması

MATLAB'da tasarlanmış konuşmacı tanıma sisteminin ara yüzü Şekil.40'da görülmektedir. Bu sistemde .wav formatında ses dosyaları öznitelikleri çıkarılarak ve tanımlayıcı bir ID numarası verilerek veritabanına kaydedilmektedir. Daha sonra dosyadan seçilen ya da mikrofondan kaydedilen bir sesin veritabanında kayıtlı olan hangi sesle eşleştiği bulunmaktadır.

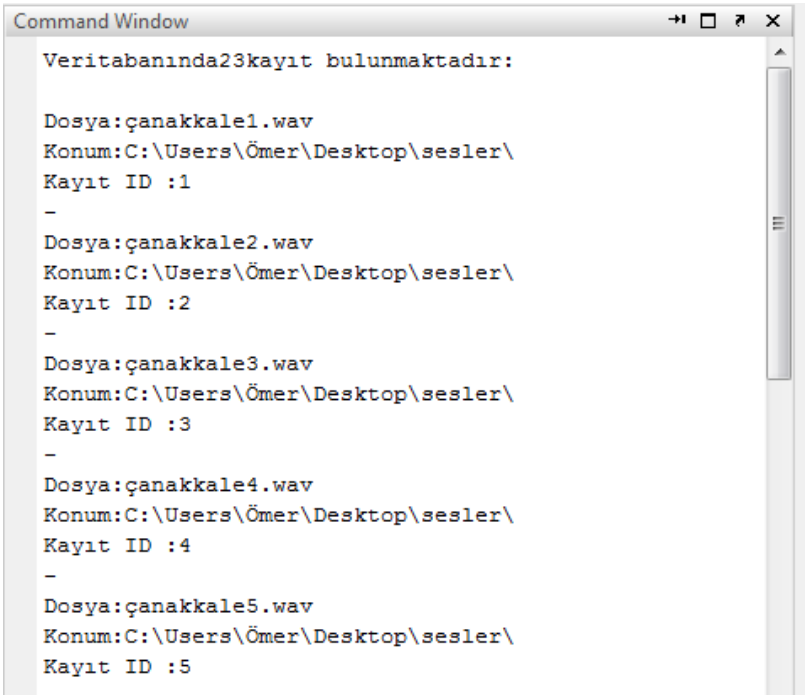
"Veritabanına Dosyadan Ses Ekle" ve "Veritabanına Mikrofondan Ses Ekle" butonları ile veritabanına ses dosyalarının kaydedilmesi işlemi gerçekleştirilmektedir. Bu işlem sırasında eklenen sesler için tanımlayıcı bir ID numarası verilmektedir.

“Dosyadan Ses Dinleme” ve “Mikrofondan Kaydedilen Sesi Dinleme” butonları ile veri tabanında bulunan sesler dinlenebilmektedir.



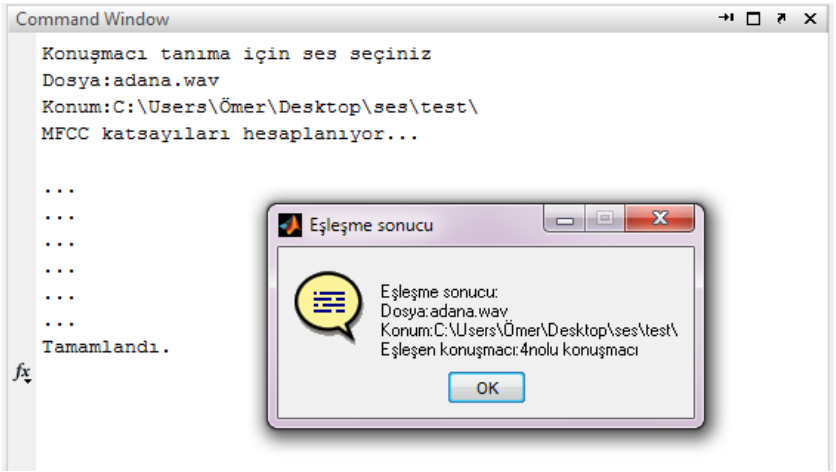
Şekil 43. Konuşmacı tanıma sistemi

“Veritabanı Görüntüleme” seçeneği ile veri tabanında bulunan ses kayıtları, ID numaraları ve bulundukları konumlar görüntülenmektedir. “Veritabanını Sil” butonu ile veritabanında bulunan bütün kayıtlar silinebilmektedir.



Şekil 44. Veritabanında bulunan kayıtların görüntülenmesi

Saptama aşamasında, girdi olarak verilen bilinmeyen bir ses örneği işlenip öznitelik vektörleri çıkarılmakta ve veritabanında bulunan seslerin öznitelik vektörleri ile karşılaştırılmaktadır. "Konuşmacı Tanıma İçin Dosyadan Ses Seç" ve "Konuşmacı Tanıma İçin Mikrofondan Ses Seç" butonları ile bilinmeyen ses örneğinin veritabanında kayıtlı seslerle karşılaştırılması ve kime ait olduğunun belirlenmesi işlemi gerçekleştirilmektedir.



Şekil 45. Eşleşme sonucunun gösterilmesi

Test süreci, tasarlanan konuşmacı tanıma sisteminin öznitelik eşleme safhası olarak da adlandırabilir. Test aşamasında konuşmacıların test verilerinin de öznitelik vektörleri çıkarıldıktan sonra referans model olarak hazırlanan kod kitabı vektörleriyle en yakın uzaklığı veren kod vektörleri bulunmuştur. Uzaklık kriteri olarak öklid uzaklığı kullanılmıştır. Bilinmeyen konuşmacı bu kod vektör sayısı en fazla olan konuşmacı olarak atanmıştır.

Uygulamanın test edilmesi 10 erkek ve 10 kadın konuşmacıdan alınan ses kayıtları ile gerçekleştirilmiştir. Konuşmacılar gürültüsüz ortamda 3 farklı kelime seslendirmişlerdir ve ses örnekleri kayıt altına alınmıştır. Alınan kayıtların gürültüsüz ortamda olması ve kaydın başında ya da sonunda sessiz alanların bulunmaması sistemin başarısını etkileyeceğinden kayıtların başında ve sonunda bulunan sessiz alanlar bir program kullanılarak kırpılmıştır. Kaydedilen 3 kelimenin 2'si sistemin eğitilmesinde 1'i ise test edilmesinde kullanılmıştır. Yapılan denemeler sonucunda sistemin %90 doğru tanıma oranına sahip olduğu görülmüştür.

6. SONUÇ

Teknolojinin hızla gelişmesi, bilişim teknolojilerinin ve internetin yaygınlaşması ile birlikte insanlık bilişim çağını yaşamaya başlamıştır. Sanayi devrimiyle oluşan endüstri toplumu, ilerleyen yıllarda internet kullanımının yaygınlaşmaya başlamasıyla bilgi toplumuna dönüşmüştür. Teknolojik gelişmelerin en büyüğü olarak görülen internetle insanların hayat tarzları değişmiş, bilginin hazırlanması, işleyişi, paylaşımı ve pazarlanması çok kolay hale gelmiştir. Toplumda her kesimden insanın yaygın olarak kullandığı internet, aynı zamanda yeni suç türlerinin ortaya çıkması için de bir platform oluşturmuştur. Bilişim suçları şu anda, bütün dünyayı tehdit eden en büyük meselelerden biri haline gelmiştir. Bu nedenle birçok ülkenin polis birimleri altında, konu ile ilgili özel birimler oluşturulmuştur.

Teknolojik gelişmelerin paralelinde suç türleri değişmiştir ve bu suçları aydınlatmak için klasik yöntemler yetersiz kalmıştır. Teknolojinin sebep olduğu bu duruma yine teknoloji ile çözüm bulunması kaçınılmaz olmuştur. Sayısal delillerin elde edilmesi ve analizi son derece önemli hale gelmiş ve bu sayısal delillerin analiz edilmesi için klasik yöntemlerin yerine daha modern tekniklerin kullanılması zorunluluğu doğmuştur. Gerek güvenliğin sağlanması için önleyici tedbirlerin alınmasında gerekse suçluların kimliklerinin tespit edilmesinde biyometrik sistemler kullanılmaya başlanmıştır. Biyometrik sistemler, değişen suç yelpazesinde hem önleyici olarak hem de tespit ve değerlendirme aşamalarında kullanılan en önemli çözümlerden biri olmuştur.

Ses tanıma ve tanımlama işlemi cinayet, soygun, hırsızlık, zorla kaçırma, tecavüz, uyuşturucu, kumar, kaçakçılık, başkası adına yapılan taklit konuşmalar, şantaj, rüşvet, tehdit telefonları, terörist eylemler, bombalı eylemler, suikast girişimleri gibi kriminal olaylarda kullanılmaktadır. Yine parmak izi ve parmak izi tanıma işlemleri hemen hemen bütün kriminal olaylarda kullanılmaktadır. Bu nedenle bu tezde suç sahnesinde en sık karşılaşılan biyometrik verilerden olan parmak izi ve ses ele alınmıştır.

Parmak izi ve ses tanıma uygulamaları MATLAB'da gerçekleştirilmiştir. Parmak izi tanıma uygulamasında ayrıntı (minutiae) bazlı eşleme tekniği kullanılmıştır. Parmak izi resimleri bir dizi görüntü iyileştirme işlemine tabi tutulmuş ve ayrıntı noktaları belirlenmiştir. Belirlenen ayrıntı noktaları karşılaştırılmış ve benzerlik yüzdesi elde edilmiştir. Uygulamada gerçekleştirilen parmak izi tanıma sisteminin %75 doğrulama oranına sahip olduğu görülmüştür.

Konuşmacı tanıma uygulaması metin bağımsız, kapalı küme konuşmacı tanıma sistemi olarak geliştirilmiştir. Seslere ait öznitelik vektörleri MFCC algoritması kullanılarak elde edilmiştir. LBG algoritmasıyla her bir konuşmacı için kod kitapları oluşturulmuştur. Tanınması istenen konuşmacının verilerinin de öznitelik vektörleri çıkarıldıktan sonra referans model olarak hazırlanan kod kitabı vektörleriyle en yakın uzaklığı veren kod vektörleri bulunmuştur. Yapılan denemeler sonucunda sitemin %90 doğru tanıma oranına sahip olduğu görülmüştür.

KAYNAKLAR

[1] Bilişim Çağı, http://tr.wikipedia.org/wiki/Bili%C5%9Fim_%C3%87a%C4%9F%C4%B1, Erişim Tarihi: 13.10.2012.

[2] **Uzunay, Y.,** 2005. Dijital Delil Araştırma Süreci, 2.Polis Bilişim Sempozyumu, Ankara, 14- 15 Nisan.

[3] Türkiye'de İnternetin Kısa Tarihi, http://www.socialmediatr.com/blog/turkiyede-internetin-kisa-tarihi/, Erişim Tarihi: 13.10.2012.

[4] Bilişim Suçları Kapsamında Dijital Deliller, http://ab.org.tr/ab05/tammetin/134.pdf, Erişim Tarihi: 20.12.2012

[5] Türk Dil Kurumu, http://www.tdkterim.gov.tr/?kelime=bili%FEim&kategori=terim&hng=md, Erişim Tarihi: 03.11.2012.

[6] **Özgür, A.Z. ve Sözen, S.,** 2003. Polisin Görev ve Yetkileri, Anadolu Üniversitesi Açıköğretim Fakültesi Yayını, Eskişehir.

[7] Dijital Deliller, http://www.caginpolisi.com.tr/50/14-15-16-17-18.htm, Erişim Tarihi: 03.11.2012.

[8] Çarşamba İlçe Emniyet Müdürlüğü, http://www.carsamba.samsun.pol.tr/bilisim-suclari.htm, Erişim Tarihi: 18.10.2012.

[9] **Kshetri, N.,** 2005. Pattern of Global Cyber War and Crime: A Conceptual Framework, Journal of International Managament 11, University of North Carolina (UNC), Greensboro.

[10] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.2

[11] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.3

[12] Bilişim Suçları Hangi Yollarla İşlenir, http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-hangi-yollarla islenir.html, Erişim Tarihi: 01.02.2013.

[13] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.6

[14] Adli Kolluk Eğitim Semineri, www.antalya.adalet.gov.tr/duyurular%5Cbasin 2013.ppt, Erişim Tarihi: 24.01.2013.

[15] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.7

[16] Bankamatik, http://tr.wikipedia.org/wiki/Bankamatik, Erişim Tarihi: 05.02.2013.

[17] TCK Madde 245, http://www.turkhukuksitesi.com/mevzuat.php?mid=5193, Erişim Tarihi: 05.02.2013.

[18] Kredi Kartı Dolandırıcılığında 10 Yöntem, http://arsiv.ntvmsnbc.com/news/195214.asp, Erişim Tarihi:18.02.2013.

[19] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.9

[20] Interpol Computer Crime Manuel 2. Officer, İnterpol, s.10

[21] **Boğa, U.,** 2011. Bilişim Suçları ile Mücadele Yöntemleri, Radyo Televizyon Üst Kurulu Uzmanlık Tezi, Ankara.

[22] **Atalıç Taş, K.,** 2010. Bilişim Suçları ve Adana İlinde 2006- 2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi, Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü , Adana.

[23] Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler, http://www.dulger.av.tr/assets/pdf/akveabcocukpornografisi.pdf, Erişim Tarihi: 28.03.2013.

[24] **Dönmezer, S.,** 1994. Kriminoloji, 8.Baskı, Beta Yayınları, İstanbul.

[25] Adli Bilişim, http://www.telepati.com.tr/izbirakanlar/adlibilisim203.htm, Erişim Tarihi: 30.03.2013.

[26] **Keser Berber, L.,** 2004. Adli Bilişim, Yetkin Yayınları, Ankara.

[27] T.C. Edirne Barosu, http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer forensic.html, Erişim Tarihi:10.10.2012.

[28] Bilgi Teknolojilerinde Temel Kavramlar, http://moodle.midas.baskent.edu.tr/file.php/3/dersnotlari/bilgi_teknolojilerinde_temel_kavramlar.pdf, Erişim Tarihi: 27.03.2013.

[29] Adli Bilişim, http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic /, Erişim Tarihi: 27.03.2013.

[30] Bilinen İlk Bilişim Suçu, http://internethukuku.net/bilinen-ilk-bilisim-sucu-ve-turkiyede-yargilanan-ilk-hacker/, Erişim Tarihi:02.04.2013.

[31] Dünya Uygulamasında Bilişim Suçları, http://bilisimhukukukulisi.blogspot.com/2012/02/dunya-uygulamasinda-bilisim-suclari.html, Erişim Tarihi: 02.04.2013.

[32] Adli Bilşimin Alt Dalları, http://www.telepati.com.tr/izbirakanlar/adlibilisim203.htm, Erişim Tarihi: 19.04.2013.

[33] Ağ Trafiğinde Adli Bilişim Analizi, http://www.mertsarica.com/ag-trafiginde-adli-bilisim-analizi/, Erişim Tarihi: 19.04.2013.

[34] GPS Nedir ve Nasıl Çalışır, http://www.bilgiustam.com/gps-nedir-ve-nasil-calisir/, Erişim Tarihi: 08.03.2013.

[35] **Uçar, C.,** 2012. Sosyal Paylaşım Ağlarının Önemi ve İnsan Üzerindeki Etkileri, Yüksek Lisans Projesi, Fatih Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

[36] Adli Bilişim, http://www.hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/, Erişim Tarihi:18.03.2013.

[37] Bilişim Yazıları, http://sayisaldelil.net/?cat=3, Erişim Tarihi:18.03.2013.

[38] Bilişim ve İnternet, http://www.leylakeser.org/search/label/Bili%C5%9Fim%20ve%20%C4%B0nternet, Erişim Tarihi:17.04.2013.

[39] Akıllı Telefonlar, http://www.bunedemek.com/akilli-telefon-ne-demek.html, Erişim Tarihi: 08.02.2013.

[40] **Say, K.,** 2006. Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuarda İncelenmesi, Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara.

[41] **Şirikçi, A.S. ve Cantürk, N.,** 2012. Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi, Bilişim Teknolojileri Dergisi Cilt: 5, Sayı: 3

[42] Bilişim Suçlarına Karşı Mücadelede Kullanılan Bir Teknoloji Olarak Adli Bilişim, http://bilgimikoruyorum.org/index.php?option=comcontent&view=article&id=57:dl-blm-ve-blm-suclari&catid=36:adli-biliim&Itemid=73, Erişim Tarihi: 13.02.2013.

[43] Hash Fonksiyonları, http://blog.kadiraltan.com/hash-ozet-fonksiyonlar-nedir-ne-degildir-bolum-1/, Erişim Tarihi:10.02.2013.

[44] Adli Bilişim Süreçleri, http://www.telepati.com.tr/agustos12/konu8.htm, Erişim Tarihi:23.04.2013.

[45] **Ercan, T.,** 2001. Adli Bilişim Uygulamalarında Kullanıcı Bazlı Değerlendirme, Yaşar Üniversitesi, İstanbul.

[46] Türkiye'de Adli Bilişim, http://blog.serkankurt.com.tr/adli-bilisim/adli-bilisim-ve-turkiyede-adli-bilisim-2011 12-63.html, Erişim Tarihi: 25.04.2013.

[47] Türkiye Bilişim Derneği 2012 Değerlendirme Raporu, http://www.tbd.org.tr/usr_img/raporlar/TBD2012Degerlendirme%20Raporu.pdf, Erişim Tarihi:27.04.2013.

[48] Türkler'in İnternet Kullanım Alışkanlıkları, http://www.sabah.com.tr/Teknoloji/Haber/2012/10/26/turklerin-internet-kullanimaliskanliklari, Erişim Tarihi: 26.10.2012.

[49] Köksal, M.A. ve İlbaş, Ç., Türkiye'nin Siber Suç Haritası, Türkiye Bilişim Derneği Aylık Bilişim Kültür Dergisi, Sayı: 137, Sayfa: 14- 19.

[50] TCK 5651 Sayılı Kanun, http://www.simyacibilisim.com/5651-sayili-kanun-nedir, Erişim Tarihi:25.03.2013.

[51] Norton 2012 Siber Suç Raporu, http://www.symantec.com/tr/tr/about /news/release/article.jsp?prid=20121113_03, Erişim Tarihi:14.04.2013.

[52] Çiçek, İ. ve Okatan A., Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları, Ankara Barosu Bilişim ve Hukuk Dergisi, Sayı:6.

[53] Varol, A., 2013. Digital Forensics Education in Turkey, 4th International Forensics Sciences, Cyber Security and Surveillance Technologies Conference & Exhibition, Harbiye Military Museum & Culture Site, İstanbul, 27th – 29th March 2013.

[54] Polis Akademisi Tarihçe, http://www.pa.edu.tr/?appcode=web_akademi_ tarihcesi, Erişim Tarihi:28.04.2013.

[55] Bilişim Suçlarına Karşı Uzman Yetiştirilecek, http://www.haber7.com/egitim/ haber/1000314-bilisim-suclarina-karsi-uzmanyetistirilecek, Erişim Tarihi: 11.03.2013.

[56] Hacettepe Üniversitesi Adli Bilişim Araştırma ve Uygulama Merkezi Yönetmeliği, http://www.resmigazete.gov.tr/eskiler/2009/05/20090526-1.htm, Erişim Tarihi: 25.04.2013.

[57] Şan, S., 2013. Parmak Damar Tanıma Teknolojisi, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.

[58] Biyometrik Sistemler, http://www.pitsteknoloji.com/biyometrik-sistemler.php, Erişim Tarihi:12.05.2013.

[59] Şamlı,R. ve Yüksel, M. E., 2009. Biyometrik Güvenlik Sistemleri , Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa, 11-13 Şubat, s. 691-697.

[60] Biyolojik Sistemlerin Özelliklerinden Yararlanarak Kimlik Tespit Etme, http://elektroteknoloji.com/Elektrik_Elektronik/Teknik_Yazilar/Biyometrik_SistemleFiziksel_Ozelliklerden_Yararlanarak_Kimlik_Tespit_Etme_bilgisayar_destekli.html, Erişim Tarihi: 12.05.2013.

[61] Parmak İzi, http://m.friendfeed-media.com/3b2cb3b530b29c02f7586c4829b1c34cd9d6d857, Erişim Tarihi:13.05.2013.

[62] Kimlik Tespitinde Parmak İzi Arşivlerinin Gerekliliği, http://www.caginpolisi.com.tr/35/42-43-44-45-46-47.htm, Erişim Tarihi: 01.05.2013.

[63] DNA Testi Nedir, http://www.frmartuklu.net/seviyeli-ciddi-konular/212902 dna-testi-nedir-dna-testininkullanim-alanlari-nelerdir.html,Erişim Tarihi: 08.04.2013.

[64] Biyometrik Tanıma Sistemleri, http://www.ahmetkakici.com/genel/biyometrik-tanima-sistemleri/, Erişim Tarihi:08.04.2013.

[65] Biyometrik Sistemler, http://e-bergi.com/2008/Agustos/Biyometrik-Sistemler, Erişim Tarihi: 09.04.2013.

[66] **Turhal, Ü.Ç.,** 2008. İki Boyutlu Yüz Tanıma Metodlarına Yeni Yaklaşımlar: Satır ve Sütun Vektörleri Arasındaki Değişimlerin Kullanılması, Doktora Tezi, Osmangazi Üniversitesi Fen Bilimleri Enstitüsü, Eskişehir.

[67] Emniyet Genel Müdürlüğü Ulusal Emniyet ve İç Güvenlik Kamu Araştırma Programı,http://www.tubitak.gov.tr/tubitak_content_files/ARDEB/kamag/Ulusal_Emniyet_ve_c_Guvenlik_Kamu_Arastirma_Programi.pdf, Erişim Tarihi: 27.04.2013.

[68] "Bu Kameradan Hiç kimse Kaçamaz" Başlıklı Haber, http://teknoloji.bugun.com.tr/bu-kameradan-hickimse-kacamaz-haberi/197793, Erişim Tarihi: 05.05.2013.

[69] **Tosi, O.,** 1979. Voice Identification Theory and Legal Applications, University Park Press, Baltimore, Maryland.

[70] **Cain, S.,** 1990. Voiceprint Identification, The Legal Investigator, November 1990, pp.16-19.

[71] **Ergen, B. ve Çalışkan, A.,** 2011. Biyometrik Sistemler ve El Tabanlı Biyometrik Tanıma Karakteristikleri, 6th International Advanced Technologies Symposium (IATS'11), Fırat Üniversitesi, Elazığ, Turkey, 16-18 May.

[72] **Zeybek, İ.S.,** 2011. Diş Isırık İzlerinin Adli Tıp Açısından Değerlendirilmesi, Bitirme Tezi, Ege Üniversitesi Tıp Fakültesi, Adli Tıp Anabilim Dalı, İzmir.

[73] **Oysal, Y.,** 2012. Güvenlik Sistemleri, Anadolu Üniversitesi Yayını No:2489, 1. Baskı, Eskişehir.

[74] **Kaygusuz, Z.,** 2008. Kimlik Sorma ve Kimlik Tespiti, Polis Bilimleri Dergisi Cilt:10 (1).

[75] Sönmez, E.B., Özbek, N.Ö., Özbek, Ö., 2007. Avuç İzi ve Parmak İzine Dayalı Bir Biyometrik Tanıma Sistemi, IX. Akademik Bilişim Konferansı, Dumlupınar Üniversitesi, Kütahya, 31 Ocak- 2 Şubat.

[76] Sağıroğlu, Ş., ve Özkaya, N., 2006. Otomatik Parmakizi Tanıma Sistemlerinde Kullanılan Önişlemler İçin Yeni Yaklaşımlar, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi Cilt 21, No 1, 11-19.

[77] Görgünoğlu, S., Çavuşoğlu, A., 2009. Parmakizi Tanıma Sistemlerinde Kullanılan Özellik Çıkartma Algoritmalarının Performans Analizi, 5. Uluslararası İleri Teknolojiler Sempozyumu (IATS'09), Karabük Üniversitesi, Karabük, Türkiye, 13-15 Mayıs.

[78] Biyometrik Sistemler, http://m.friendfeed-media.com/3b2cb3b530b29c02f7586c4829b1c34cd9d6d857, Erişim Tarihi:08.05.2013.

[79] Mut, O., 2005. Konuşmacı Tanıma, Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli

[80] Kumaşoğlu, G., Bolat, B., 2011. Yapay Sinir Ağlarıyla Müzikal Tür Tanıma, Elektrik- Elektronik ve Bilgisayar Sempozyumu, Fırat Üniversitesi, Elazığ

[81] Selçuklu, A.M., 2008. Mobil İmzada Güvenliğin Artırılması İçin Farklı Yöntemlerin Geliştirilmesi, Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi Fen Bilimleri Enstitüsü, Kahramanmaraş.

[82] Nabiyev, V.V., Yücesoy, E., 2009. VQ Yöntemiyle Konuşmacı Cinsiyetinin Belirlenmesi, Turkish Journal of Computer and Mathematics Education, Vol.1 No.1, pp. 37-49.

ÖZGEÇMİŞ

Gülşah AKKAN, 1984 yılında Elazığ'da doğdu. İlk, orta ve lise öğrenimini Elazığ'da tamamladıktan sonra 2003 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik Bilgisayar Eğitimi Bölümü, Bilgisayar Öğretmenliği'ni kazandı. 2007 yılında bu bölümden mezun oldu. Yine 2007 yılında Balıkesir'in Gönen ilçesinin Sarıköy Beldesi, Sarıköy Çok Programlı Lisesi'nde sözleşmeli bilişim teknolojileri öğretmeni olarak göreve başladı. 2008 yılında Bitlis Merkez Bitlis Lisesi'ne kadrolu bilişim teknolojileri öğretmeni olarak atandı. 2010 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Bilgisayar Eğitimi Ana Bilim Dalı, Bilgisayar Sistemleri Bölümü'nde yüksek lisans eğitimine hak kazandı. 2010 yılının Temmuz ayında Elazığ Merkez 75. Yıl Anadolu Lisesi'ne tayin oldu ve halen 75. Yıl Anadolu Lisesi'ndeki görevini sürdürmektedir. Yabancı dili İngilizcedir.