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

ONLİNE İMZA DOĞRULAMA

Yüksek Lisans Tezi

Tezi Hazırlayan:

Dima MARACHI

İSTANBUL, 2017

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

ONLİNE İMZA DOĞRULAMA

Yüksek Lisans Tezi

Tezi Hazırlayan:

Dima MARACHI

Öğrenci No:

080820010

Danışman:

Yrd. Doç. Dr.Turhan KARAGÜLER

İSTANBUL, 2017

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum "*Online İmza Doğrulama*" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım 19/12/2017.

Dima Marachi

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi 0808.2001.0 no'lu Dima....Maraashi.....'in 19./12./2017 tarihinde yapılan tez savunma sınavı[1] sonucunda 45 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle .KABÜL... kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : BİLGİSAYAR MÜHENDİSLİĞİ
Programı : BİLGİSAYAR MÜHENDİSLİĞİ
Tez Başlığı[3] : Online....İmza....Doğrulama.....

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

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

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

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

Teşekkür

Her şeyden önce, tez çalışmam boyunca sağladıkları rehberlik ve destek için danışmanlarıma Yrd.Doç.Dr.Turhan KARAGÜLER ve Yrd.Doç.Dr.Ediz ŞAYKOL saygılarımı ve teşekkürlerimi iletmek isterim.

Ayrıca, gösterdikleri sevgi ve desteği için aileme de teşekkür ediyorum.

Adı Soyadı : Dima MARACHİ
Danışmanı : Yrd. Doç. Dr.Turhan KARAGÜLER
Türü ve Tarihi : Yüksek Lisans Tezi, 2017
Alanı : Bilgisayar Mühendisliği
Anahtar Kelimeler : Online İmza Doğrulaması, Dinamik Zaman Çözgüsünü (DTW), Statik Özellikler, Offline İmza, Dinamik Özellikler, Online İmza.

ÖZ

ONLİNE İMZA DOĞRULAMA

El yazısı imza doğrulama sistemi herhangi bir insan faaliyetinin kimliğinin yetkilendirilmesi için herhangi bir finansal ve diğer belge faaliyetlerinde yaygın kullanılmaktadır, ancak yine de bu tür doğrulama sistemleri esas olarak manuel doğrulamaya dayanmaktadır, yani, verilen imzayı test imza ile karşılaştırılması yalnızca bir kişinin bakışıyla gerçekleşir. Bu yüzden daha sağlam bir sistem gerekir bu da bazı bilgisayar temelli sınıflandırmaya dayalı olabilir. Böylece bu tezde bir imzanın normalleştirilmiş dinamik özelliklerine dayanan ve Dinamik Zaman Çözgüsünü (DTW) (Dynamic Time Warping) sınıflandırma metodu olarak kullanan online imza doğrulama sistemi önerildi. *Online İmza Doğrulaması*, imza doğrulama sistemini kullanarak, yazarın kimliğini doğrulamak için kullanılan bir süreçtir. Bu sistem, bir güvenlik sistemi olarak kullanılabilir örneğin; giriş başvurusunu ve şifre ikamelerini değerlendiren doğrulama işlemi. İmza doğrulama teknolojisi başlıca, bir bilgisayarın Evrensel Seri Veri Yolu Bağlantı Noktasına (USB bağlantı noktası) bağlı olan sayısallaştırıcı tablet ve özel kalem gerektirir. Bir kişi, imzasının boyutu ve konumunu dikkate almadan, sayısallaştırıcı tabletin üzerine özel kalemi kullanarak imzalayabilir. İmza, x-y koordinatlarını içeren kalem vuruşları ve kalemin tabletin üzerindeki basıncı olarak karakterize edilir ve veri, bir .txt dosyası biçiminde imza veri tabanında depolanır. Bu özellikler bir kişiyi benzersiz bir şekilde tanımlar ve taklit edilemez ve çalınamaz bir veri seti oluşumunu mümkün kılar.

Name and Surname : Dima MARACHİ
Supervisor : Assist. Prof. Dr. Turhan KARAGÜLER
Degree and Date : Master, 2017
Major : Computer Engineering
Key Words : Online Signature Verification, Dynamic Time Warping (DTW), Static Features, Offline Signature, Dynamic Features, Online Signature.

ABSTRACT

ONLINE SIGNATURE VERIFICATION

Handwritten signature verification systems are most widely used in any financial and other documentation activities for authorization of identity of any human activity. However still these types of systems are mainly based on manual verification, such that a person only by looking with eyes and comparing the given signature with the test signature. Thus a more robust system is required which can be based on some computer based classification. For this aim, in this thesis, an online signature verification is proposed. This purposed system is simply based on normalized dynamic features of the signature using Dynamic Time Warping (DTW) as the classification method. Online Signature Verification is a process of verifying the writer's identity by using signature verification system. This system can be used as a security system such as verification for assessing entry application and password substitutions. Signature verification technology requires primarily a digitizing tablet and a special pen connected to the Universal Serial Bus Port (USB port) of a computer. An individual can sign on the digitizing tablet using the special pen regardless of his signature size and position. The signature is characterized as pen-strokes consisting x-y coordinates and the data will be stored in the signature database in the form of a .txt file. These characteristics uniquely identify a person and cannot be imitated or stolen.

İÇİNDEKİLER

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

TABLOLAR LİSTESİ

Sayfa No.

KISALTMALAR

DTW	Dynamic Time Warping
IBG	International Biometric Group
FAR	False Accept Rate
FRR	False Reject Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
EER	Equal Error Rate
CAR	Correct Acceptance Rate
CRR	Correct Rejection Rate
ROC	Receiver Operating Characteristic
DET	Detection Trade-off Curve
TPIR	True Positive Identification Rate
FNIR	False Negative Identification Rate
FTE	Failure to Enroll Rate
FTA	Failure to Acquire Rate
HTER	Half Total Error Rate
GMR	Genuine Match Rate
CCR	Correct Classification Rate
CIR	Correct Identification Rate
BiSP	Biometric Smart Pen
HMM	Hidden Markov Models
GMM	Gaussian Mixture Model
SVM	Support Vector Machines
ANN	Artificial Neural Networks
FIR	Finite Impulse Response
GUI	Graphical User Interface
CPU	Central Processing Unit
USB	Universal Serial Bus

Bölüm 1

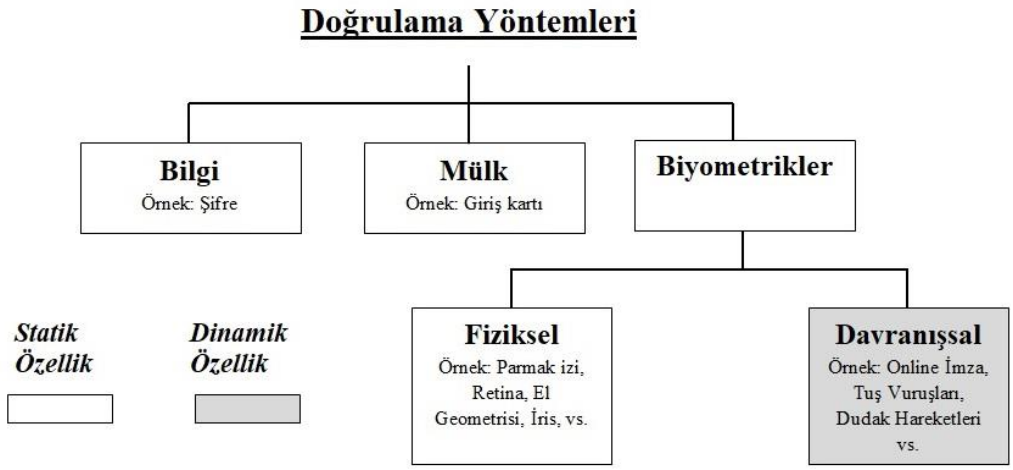
Giriş

1.1 Motivasyon

Bilişimde güvenlik bugünki dünyada en büyük sorunlarından biridir çünkü günlük hayatta birçok yerde giriş sağlayabilmek için kişinin kimliğini sunmayı ihtiyacına kaliyoruz. Çoğumuz, sık kullanılan değişik türlü şifrelerle uğraşmak zorundayız örneğin; internet hesapları, kredi kartları, ATM kartları, PİN şifreleri...vs. Bu şifrelere ait bazı sorunlar vardır; şifrelerin sürekli yetkisiz kullanıcıların tarafından kırılma riski altında kalması, kimlik kartların çalınması, bunlara ek olarak unutulan şifreler ve kaybedilmiş kimlik kartların olması. Bütün bu sorunlara çözüm arayışı sayesinde biyometrik alanın doğuşu gerçekleştirildi [1] [2] [3].

Biyometrikler bireylerin davranışsal ve biyolojik özelliklerine göre otomatik tanıma sistemidir [4]. Bugüne kadar biyometriğin temel kullanımı, doğrulamada şifreleri ve giriş kartlarının yerine geçmekti. Biyometrik doğrulama daha güvenilir ve popüler güvenlik sistemlerinden biri olup şifreye dayalı güvenlik sistemlerin yerine geçebilmiştir. Yüksek derecede güvenlik ve tanıma kabiliyeti biyometrik teknolojilerin en büyük avantajlarıdır, ardından doğruluk (accuracy) derecesi, diğer avantajları ise paylaşılamaması/kopyalanamaması/kaybedilememesi gibi benzersiz özelliklerinin olmasıdır [5].

Yakın geçmişte, biyometrik teknikleri makinaya dayalı olan doğrulama bireyin kimliğinin doğrulanması için geliştirlmişti. Genel olarak, bir kişinin doğrulanması için üç yöntem vardır. Bunlar Şekil (1-1)'de görüldüğü gibi; neyin var, neyi bildiği ve kim olduğu sorularının yanıtlarıdır.



Şekil (1-1): Doğrulama Yöntemleri – Bilgi, Mülk ve Biyometrikler [6].

Fiziksel biyometriklerin ve davranışsal biyometriklerin farkı çıkarılan özelliklerin statik veya dinamik olmasıdır [6]. İmzalar, kişinin kimliğinin doğrulamasında en popüler ve güvenilir biyometrik özelliklerinden biridir.

İmzalar belirli bir süre sonra değişen, bir davranışsal biyometriktir ve kişinin fiziksel ve duygusal durumundan etkilenir. İmza zaman içerisinde değişebilir ve iris paterni veya parmak izleri kadar benzersiz veya taklit etme zorluluğu yoktur, ancak imzanın halk tarafından yaygın kabul edildiği için düşük-seviyeli-güvenlik doğrulama ihtiyaçlarında daha uygundur [9].

El ile yazılan imzaların edinme işlemi online veya offline olur:

- *Offline:* Taramalar, fotoğraflar veya yazı sürecini tamamladıktan sonra el yazısının başka herhangi bir statik çekim yöntemiyle elde edilmesi.
- *Online:* kalem hareketini zamansal dizilim olarak elde eden ve depolayan cihazları kullanarak, el yazısının verileri yazıldığı an'da elde edilmesi [60].

Online imzaları gerçekleştirebilmek için bireyin mevcut olup doğrulama sürecinde aktif olarak katılması gerekiyor. Böylelikle, çıkarılan özellikler dinamik olup kolaylıkla kaydedilmez. El-yazısı ile imza doğrulama sistemi, bireyin doğrulanmasında en ucuz yöntem olduğu için, doğrulama sürecinde önemli derecede ilgi kazanmıştır [10]. Ayrıca, imzaların kimlik doğrulamada onlarca yıldır kullanılması nedeniyle hem sosyal hem de

hukuksal olarak kabul görmüştür. Yaygın olarak banka çeklerinde, kredi kart ödemelerinde, sözleşmelerde ve her tür idari belgelerde tanımlamak için veya bireyin iyi niyetinin ve iradesinin teminatı olarak kullanılmaktadır.

Online İmza Doğrulaması belgelerinin dijital olarak doğrulanma probleminin en doğal çözümü olup depolanmış imza paterni ile kullanıcının girilmiş imzası ile benzerlikleri karşılaştırarak doğrulama işlemini tamamlar. Bu benzerlik, dinamik imzaların özelliklerini (örneğin: hız, hızlanma ve basınç) kullanarak hesaplanır. Bu özellikler, dinamik zaman çözgüsü metodunu kullanarak karşılaştırılır [11].

Online İmza Doğrulaması, belgelere eklediğimiz taranmış imzalar gibi, imzayı grafik resim olarak davranmaz. Çünkü taranmış imzalarda bireyin imzasının dinamikleri belirlenmemektedir. Bundan dolayı taranmış imzalar kolaylıkla kopyalanmaktadır.

Online İmza Doğrulaması imzanın tam olarak nasıl atıldığını ve yazının zamanlamasındaki değişiklikleri, duraklamaları, uygulanan basıncı, vuruşların yönünü ve hızını hesaplar. İmzanın grafik görüntüsünü kopyalamak kolay olabilir ancak bireyin imzasını atarken gösterdiği aynı davranışı kopyalamak pek kolay değildir.

Burda kullanılan teknoloji bir kalem ve özelleştirilmiş bir yazma tabletten oluşmaktadır. Şablon karşılaştırması ve doğrulama işlemini gerçekleştirebilmek için, her ikisi bir bilgisyara bağlanır. Yüksek kaliteli tablet kullanımı, imza atarken davranışsal özellikleri (hız, basınç ve zamanlama) yakalayabilir. Dijitalize tabletler online imza yakalama işlemine izin verir, bu demektir ki imzanın zaman içerisinde bir sekans olarak temsil edildiğini demektir. İmzaların karakteristik özelliği, bir imzanın durumları (instances) birbirinden çok farklı olabilmesidir. Bunun iki nedeni olabilir; birincisi doğal dalgalanmalar ve ikincisi ise fiziksel veya duygusal durumlardır. Verilen iki durum (instances) belli noktalarda amplitüd veya değer açısından farklılık gösterebilir. Diğer bir deyişle, iki imzanın zaman ölçekleri farklı olabilir, buda doğrudan (noktadan noktaya) karşılaştırmaları imkansız hale getirir. Bu sorunu çözebilmek için, nonlinear sekans hizalama metoduna gerek duyulur.

Dinamik zaman çözgüsü (Dynamic time warping) (DTW) kullanılabilen bir yaklaşımdır, ve bu çalışmada bu yaklaşıma odaklanıldı. DTW ’nun arkasındaki temel

fikir: iki çözgülen zaman sekansların nonlinear şekilde zaman boyutunu "eğimektir". Buda aralarındaki farklılıkların ölçülmesine izin verir.

1.2 Sorun Bildirimi

El yazısı imza kişisel doğrulamanın en yaygın metodudur. İmzalar, genellikle kişilerin kimliklerini idari, devlet ve finansal kurumlarca doğrulamanın yasal yolu olarak kabul edilir. Kişi doğrulaması, invaziv (girişimsel) ölçümler gerektirmez bu nedenle pratik olarak insanlar günlük hayatlarında imza kullanımını tercih eder.

İmza doğrulama teknikleri, kişinin kimliğini doğrulamak için imzasının birçok farklı özelliğini kullanır [13]. Böyle bir kimlik doğrulama tekniğini kullanmanın avantajları şunlardır:

(i) İmzalar, kimliklendirme ve doğrulama biçimi olarak toplum tarafından yaygın şekilde kabul edilmektedir.
(ii) Gerekli bilgiler hassas değildir.
(iii) Bir kişinin imzasının taklit edilmesi, o kişinin kimliğinin hayat boyu kaybedileceğine anlamına gelmez.

1.3 Araştırma Amacı ve Hedefleri

İmza doğrulaması (veya onaylaması), bir kişinin bir girdisini veri tabanındaki bir girdiye karşı doğrulama işlemidir. Yani sistem, kişinin iddia ettiği kişi olup olmadığını kontrol eder [16].

Bu araştırmanın genel fikri; maliyetli olmayan bir imza doğrulama tekniğini araştırmak ve gerçekleştirmektir. Bu arada imza sisteminin yapılandırma açısından kullanışlı, sahteciliklere karşı sağlam ve bireyin farklı duyguların etkisi altında olsa bile güvenilir olması nedeniyle tercih edilmesi söz konusudur. Sistem bir kalem ile bir tabletin üzerine imzanın atıldığı sistemlerde el-yazısı-ile-imza doğrulama algoritmalarının performansını geliştirmek, ve birçok farklı geçici imza özelliği yakalayabilmektir.

1.4 Bu Projede Kullanılan Donanım ve Yazılım

1.4.1 Donanım

Dijitalize tablet, imzayı canlı olarak elde etmek için kullanılır. Kişi, tablet yüzeyine stylus adlı özel bir elektronik kalemle yazar. Tablet yüzeyindeki küçük mesafede kalemin tüm hareketi yakalanır [11]. Tablet, kalemin ucundaki bilgiyi alır ki pozisyon ve diğer bilgileri belirlemek için kalem basıncı, yazı gücü ve kalem eğimi (tablet yüzeyi ile kalem arasındaki açı) gibi. Kalemin ucunda dokunmaya duyarlı bir anahtarı vardır ki yalnızca kalem ile yazılan numuneler (kalem kağıda dokunduğunda) kaydedilir.

Bu projede şekil (1-2)'de gösterildiği gibi WACOM CTH 490 Intuos dijital kalem tableti, el yazısı imzanın dinamik özelliklerini yakalamak için kullanılmış olup, aşağıdaki özelliklere sahiptir:

- Aktif Alan: 152 x 95 mm,
- Hareket Çözünürlüğü: 2540 dpi (inç başına nokta sayısı) (100 satır/mm),
- Basınç Seviyeleri: 2048
- Arabirim: USB
- Güç kaynağı: USB üzerinden
- Pili olmayan sensör kalemi.

Şekil (1-2) WACOM Intuos dijital kalem tableti.

Bu Wacom bamboo sayısallaştırıcı, esas olarak grafik tasarımcıları tarafından kullanılır, ancak el yazısı imzalar için bir sensör olarak kullanımını tartışıcağız. Bu

cihazın bir özelliği, konvansiyonel parametrelerle birlikte, bu cihaz ayrıca imzalarken kalemin ucundaki Z koordinatını verir. Bu, 3 Boyutlu bir alanda imzanın X, Y ve Z koordinatlarını yakalamamızı sağlar.

1.4.2 Yazılım seçimi

İmza doğrulama tekniklerini sayısallaştırıcı tablete bağlama imkanı yaratan yazılım seçilmelidir. MATLAB, imza doğrulama teknikleri uygulamak için ideal bir çözümdür, çünkü çok güçlü bir sayısal program ortamıdır. Ek olarak, MATLAB kendi programlama dilini içerir ve kullanıcıların algoritmaları geliştirmeye, verileri görselleştirmeye, verileri analiz etmeye ve yoğun sayısal hesaplamaları yürütülmesine izin verir. MATLAB'ı kullanmanın bir başka nedeni, makine öğrenme teknikleri için çok çeşitli yerleşik yöntemler sunmasıdır. Bu, güçlü hesaplamaların nispeten az talimatlar ile yürütülebileceği anlamına gelir.

İmza verilerini hazırlamak ve MATLAB için girdi olarak kullanması için C# seçildi. C # bir nesne-odaklı programlama dilidir, ve önemli bilgi sistemleri kurmak için uygun olan güçlü bir bilgisayar programlama dilidir. C# dili yaygın kulanılan bir programlama dilidir, geliştirmesi ve sürdürülmesi kolay, ve diğer gelişmiş özellikleri olan, özellikle bellek idaresi. C# ve MATLAB M-dosyalarından oluşturulan C paylaşımlı kütüphaneyi kullanan programlama dillerinden biridir [17] .

1.5 Tezin Başlıkları

Bu tez, 6 bölüm olarak düzenlenmiştir.

Bölüm 1'de araştırmanın tanıtımı yapılmaktadır.

Bölüm 2; biyometriklerin kavramını ve farklı yöntemlerini tanıtır. Biyometrik sistemi ve özelliklerini ayrıntılı olarak açıklar ve hata oranlarını açıklayarak performansı değerlendirir.

Bölüm 3; imza doğrulama sisteminde tasarlanan; veri toplama, ön işleme, özellik çıkarma, karşılaştırma ve performans değerlendirme aşamalarını tanımlar. Ayrıca imza doğrulama türleri ve sahte imzaların türleri açıklanmıştır.

Bölüm 4'te otomatik imza doğrulamasına uygulanan çeşitli modelleme yaklaşımlarını özetler ve test imzası ile referans imzasının arasındaki mesafeyi hesaplamak için çok güçlü olduğu ispatlanmış daha güncel tekniklerin hakkında bilgi verir. Ayrıca bu projede kullandığımız DTW algoritmasının ayrıntılı bir açıklaması da kapsamıştır.

Bölüm 5'te Dijital kalem ile atılan imzanın gerçek olup olmadığını doğrulamak için kullanılan yöntemi sunar. Ayrıca programın test ve uygulaması ve akış diyagramı açıklanmaktadır.

Bölüm 6; bu çalışmanın sonuçlarını gösterir.

Bölüm 2

Biyometrikler

2.1 Biyometrik Teknoloji

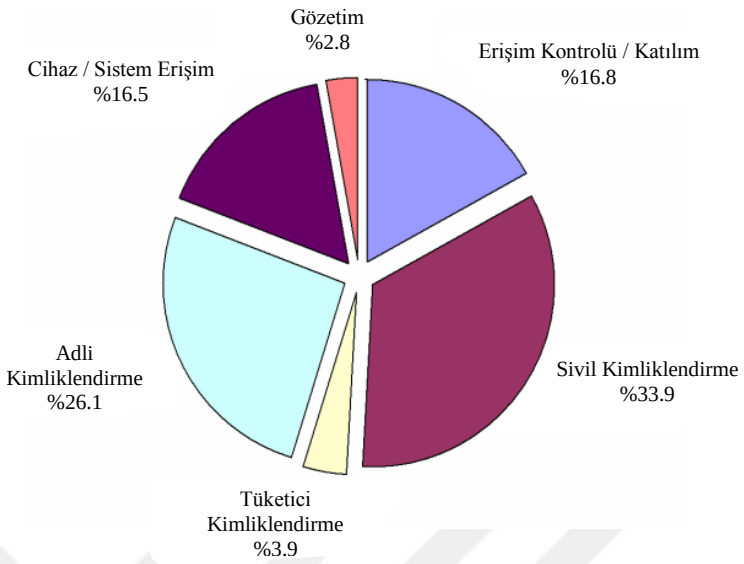
Son yıllarda, teknoloji çağında bulunan bulut bilgisayarlığı ve kişisel mobil cihazların gelişmeleriyle otomatik kişi tanıma sistemi günlük hayatımızda anahtar rol oynamaya başladı. Tanınmamız, sadece ülke sınır kapılarını geçmek için değil, aynı zamanda banka işlemlerini gerçekleştirmek ve hatta akıllı telefonlarımızın kilitini açmak için de gerekli. Bunun sonucunda, biyometrik tanıma veya biyometrikler diye yeni bir teknolojik alan oluşturulmuştur [18].

Biyometrikler: şahısın fiziksel ve davranışsal özelliklerini belirleme, analiz etmek ve ölçmek için kullanılan bir teknoloji yöntemidir [19]. Biyometrikler şahısın davranışsal ve biyolojik özelliklerine göre otomatik tanıma sistemidir [4]. Böylelikle 'biyometrik teknolojiler'otomatik olarak insanın kimliğini fizyolojik veya davranışsal özelliklerine göre doğrulama veya tanıma işlemi olarak tanımlanabilir [20]. Son yıllarda, biyometrik yöntemler kaydadeğer gelişme gösterdi.

Modern tanıma sisteminde, biyometrik teknolojisini sıklıkla kimlik doğrulamada ve değişik günlük aktivitelerde kullanırız.

Biyometrikler bir çok uygulamada kullanılabiliyor, örneğin:

- Fiziksel erişim kontrol sistemleri (fiziksel alanlara erişim: kuruluş binaları, evler vs. gibi)
- Mantıksal erişim kontrol sistemleri (elektronik sistemlere erişim ağı, kişisel bilgisayarlar vs. gibi)
- Tüketici tanıma sistemleri (sağlık hizmetleri, banka işlemleri, online alışveriş vs.)
- Sınır- kontrolleri (e-kapıları, vs.)



Şekil (2-1) 2006-2010 yıllarındaki Biyometrik market ve endüstri raporu (Uygulama ile)

Şekil (2-1) de biyometriklerin 2006-2010 yıllarında değişik uygulamalarının dağılımı gösteriliyor. Sivil ve adli tanımlamaları marketin yarısından fazlası oluşturuyor.

Biyometriklerin temel amacı hedef uygulamaya göre otomatik olarak insanları fiziksel yada davranışsal özelliklerden türetilmiş sinyalleri kullanarak (örneğin yüz, parmak izi, iris, ses, el, imza, vs.) güvenilir bir şekilde ayırdetmektir. Bu kişisel özellikler sıklıkla *biyometrik karakteristikleri* olarak ifade edilir [18].

2.2 Biyometriklerin tarihi

Biyometrik terimi yunancadaki biyo (Hayat) ve metrik (ölçmek) ten türetilmiş ve hayatı ölçmek anlamına gelir (biyolojik verileri ölçmek). Bu kelime günlük hayatımıza kimlik tanıma eşanlamlı sözcüğü olarak girmiştir [25].

Otomatik biyometrik teknolojinin oluşturulmasından yıllar önce insan halihazırda değişik şartlar altında biyometrik özellikleri kullanmaya öğrenmişti. Bazı biyometrik özellikler, örneğin, yüz, ses, ve figür, sıklıkla tanıdık insanları veya tanıdık olmayan insanları tanımak için kullanılırdı. Diğer biyometrik özellikler, parmak izi ve el imzası, sıklıkla bağlayıcı yasaları uygulamak için kişi ile anlaşmalar arasında kullanılırdı.

Biyometriklerin üzerindeki araştırmalar, değişik formlardaki (konuşma, yüz, ve parmak) otomatikleştirilmiş tanıma sistemlerinin gelişmeleri ile beraber 1960 yılında başladı. 1970 yılında ilk kullanıma hazır parmak izi ve el geometri sistemleri ortaya

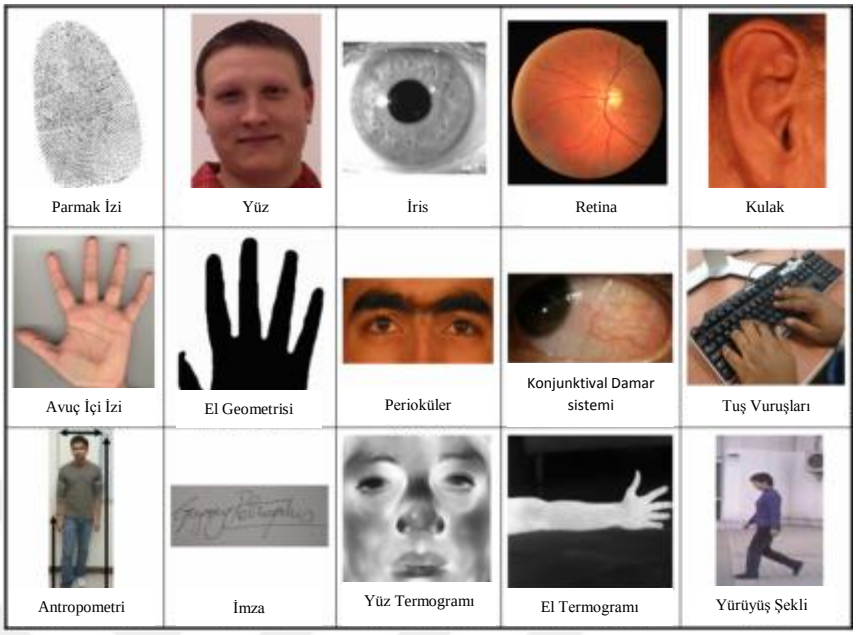
çıkarıldı. 1980 yllarında biyometrik standardizasyonda ilk adımlar başladı (parmak izi exchange standartlarının ilk versiyonu), ve 1990 yıllarda iris ve yüz tanıma sistemleri ortaya çıktı.

Günümüzde parmak izi, iris, vasküler, ses, el imzası, tuş vuruşları ve daha fazlası gibi biçimlere dayalı ticari olarak bulunan sistemler ve biyometrik kişisel kimliklerin kesin teknoloji ile kurulmaları bağımsız bir çalışma alanına dönüştü [19] [30].

2.3 Biyometrik Biçimler

Biyometrikler çoğunlukla istastiktir. Numunenin verileri ne kadar fazlaysa, sistem o kadar güvenilir ve eşsiz olur. Biyometrik biçimler kişinin biyolojik özelliklerine göre sınıflandırılmış olup; vücut ölçümleri, özellikleri ve davranışsal kalıpları gibi bir çok özelliğinin üzerinden işleyebilir [19]. Biyometrik özellikler normalde iki ana gruba ayrılır: Fiziksel veya Davranışsal.

- **Fiziksel Biyometrik Biçimler**: kullanıcının biyolojik özelliğine denilir ve zamanla sabit kalan kişinin konjenital fiziksel özelliklerini ölçer. En sık kullanılan fiziksel biyometrik biçimler: parmak izi, yüz, iris, parmak veni, vasküler (avuç içi veni, parmak veni vs.), avuç içi izi ve el geometrisi.
- **Davranışsal Biyometrik Biçimler**: kullanıcının bir işi yaptığı şekile dayanır ve edinilen davranışsal özellikleri ölçer ve bu özellikler değişikliklerden (sağlık durumu, kullanıcının duygudurumu veya zaman geçmesi) etkilenmemeli. ses tanıma, imza, el yazısı, tuş vuruşları, ve yürüyüş şekli, davranışsal biçimlere birer örnektir [31] [32].

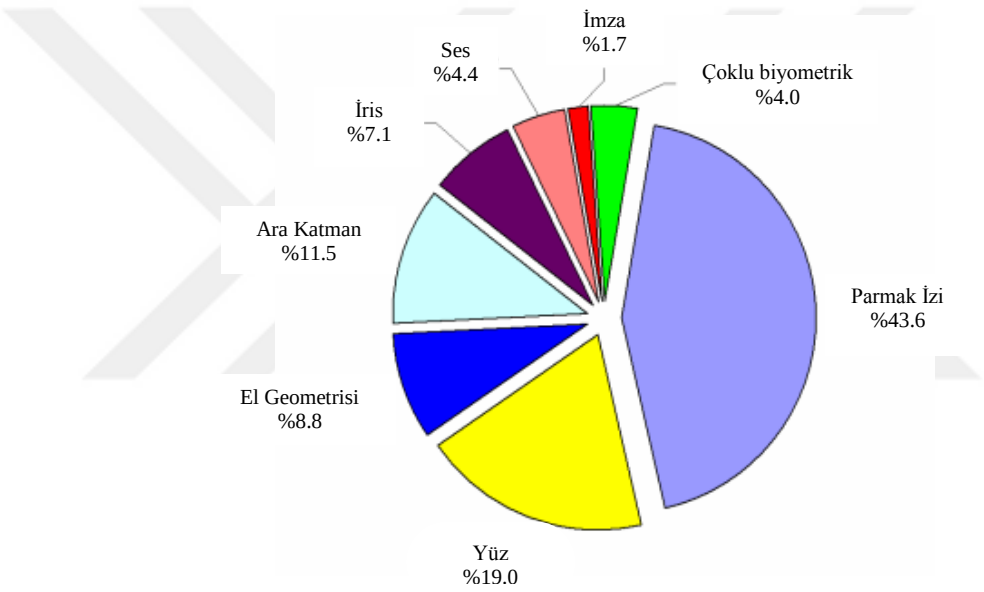


Şekil (2-2) Bazı sık kullanılan biyometrikler (fiziksel ve davranışsal) [71].

Fizyolojik	Davranışsal
Yüz	İmza
Parmak izi	Ses
El Geometrisi	Yürüyüş Şekli
İris	Tuş Vuruşları
DNA	Dudak Hareketi
Kulak Şekli	
Koku	
Retina	
Peri-oküler	

Tablo (2-1) Varolan bazı biyometrik biçimlerin örnekleri [60]

Fiziksel biyometrikler ile davranışsal biyometriklerin arasındaki fark: çıkarılan özellikler statik veya dinamik olmalarıdır. Davranışsal biyometrikler, örneğin, online imzalar, kişinin mevcut olması ve aktif olarak kimlik doğrulama sürecine katılması gerektirir. Böylelikle, çıkarılan özellikler dinamiktir ve kolaylıkla kaydedilemez [24]. Şekil (2-2)'de 2006-2010 yıllarındaki teknoloji raporun biyometrik market ve endüstrinin yüzdesi, Uluslararası Biyometrik Grup (International Biometric Group - IBG)



Şekil (2-3) biyometrik market ve endüstri raporu 2006-2010 (Teknoloji ile) [21]

2.4 Biyometrik biçimler için gereken kriterler

Herhangi bir insanın özelliği eğer bu gereksinimleri karşılıyorsa biyometrik tanımlayıcı olarak kullanılabilir. Biyometrik özelliğin uygunluğunu değerlendirmek için bu gereksinimler genel olarak yeterli rehberlik sağlar.

- **Evrensellik**: dünya nüfusunda biyometriğin varlık derecesini belirtir ve bir biyometrik özelliğinin kullanıcılar arasında ne kadar yaygın olduğunu gösterir.
- **Benzersizlik:** Biyometrik özelliklerin kullanıcıları ne kadar iyi ayırtettiği ile ilgilidir, nitekim her iki kişinin arasında yeteri farklı biometri olmalıki iki insan aynı özelliği paylaşmasın.

- **Süreklilik**: Bir biyomerik özelliğinin yaşlanmaya, hastalığa, hasara veya başka herhangi bir duruma karşı direncini ölçer. Biyometrik özellik, ideal olarak, zamandan bağımsız olmalı ve hayatboyu değişmemesi gerekir. Ancak gerçekçi olmak gerekirse sistem performansını anlamlı dercede etkilemedikçe, küçük değişiklikler kabul edilebilir.
- **Toplama kabiliyeti**: Verilerin toplama sürecinin kolaylığına ve biyometrik özelliğinin niceliksel olarak ölçülme kabiliyetine dayanır. Sensör teknolojisine ve çevresel koşullara bağlıdır.
- **Performans**: Biyometriğin belli uygulamaların etkinliğine, kesinliğine, sağlamlığına, hızına ve kaynak ihtiyaçlarına dayalı olmasıdır.
- **Kabul Edilebilirlik**: İnsanların biyometrik teknolojiyi kullanma isteklerine dayanır. Bu özellik sosyal, kültürel, ve yasal etmenlerden etkilenebilir.
- **Atlatmak**: Belirli bir özelliğe dayalı olan sistemin dolandırıcılık yöntemlerle kandırılmasının zorluğunu yansıtır [18].

Günümüzde, çoğu biyometrik sistemlerin kullanılmasına rağmen, hiçbir biyometrik özellik bütün gereksinimleri karşılayamaz. Bu yüzden biyometrik özelliği seçmek, kullanmak istediğimiz uygulamaya bağımlıdır çünkü sadece teknik problemler değil aynı zamanda sosyal ve kültürel sorunlar da içeriyor.

Tablo (2-1)'de bu gereksinimler, birçok biyometrik biçimleri için niteliksel olarak sunulmuştur (Jain et al., 2007)**.**

Biyometrik Biçim	Evrensellik	Benzersizlik	Süreklilik	Toplama Kabiliyeti	Kabul Edilebilirlik	Atlatmak
Yüz	Yüksek	Düşük	Orta	Yüksek	Yüksek	Düşük
Parmak İzi	Orta	Yüksek	Yüksek	Orta	Orta	Yüksek
El Geometrisi	Orta	Orta	Orta	Yüksek	Orta	Orta
Tuş vuruşu	Düşük	Düşük	Düşük	Orta	Orta	Orta
El venleri	Orta	Orta	Orta	Orta	Orta	Yüksek
İris	Yüksek	Yüksek	Yüksek	Orta	Düşük	Yüksek
Retina	Yüksek	Yüksek	Orta	Düşük	Düşük	Yüksek
Yüz Termogram	Yüksek	Yüksek	Düşük	Yüksek	Yüksek	Yüksek
Ses	Orta	Düşük	Düşük	Orta	Yüksek	Düşük
DNA	Yüksek	Yüksek	Yüksek	Düşük	Düşük	Düşük
İmza	Düşük	Düşük	Düşük	Yüksek	Yüksek	Düşük

Tablo (2-2): Biyometrik biçimlerin özellikleri [33].

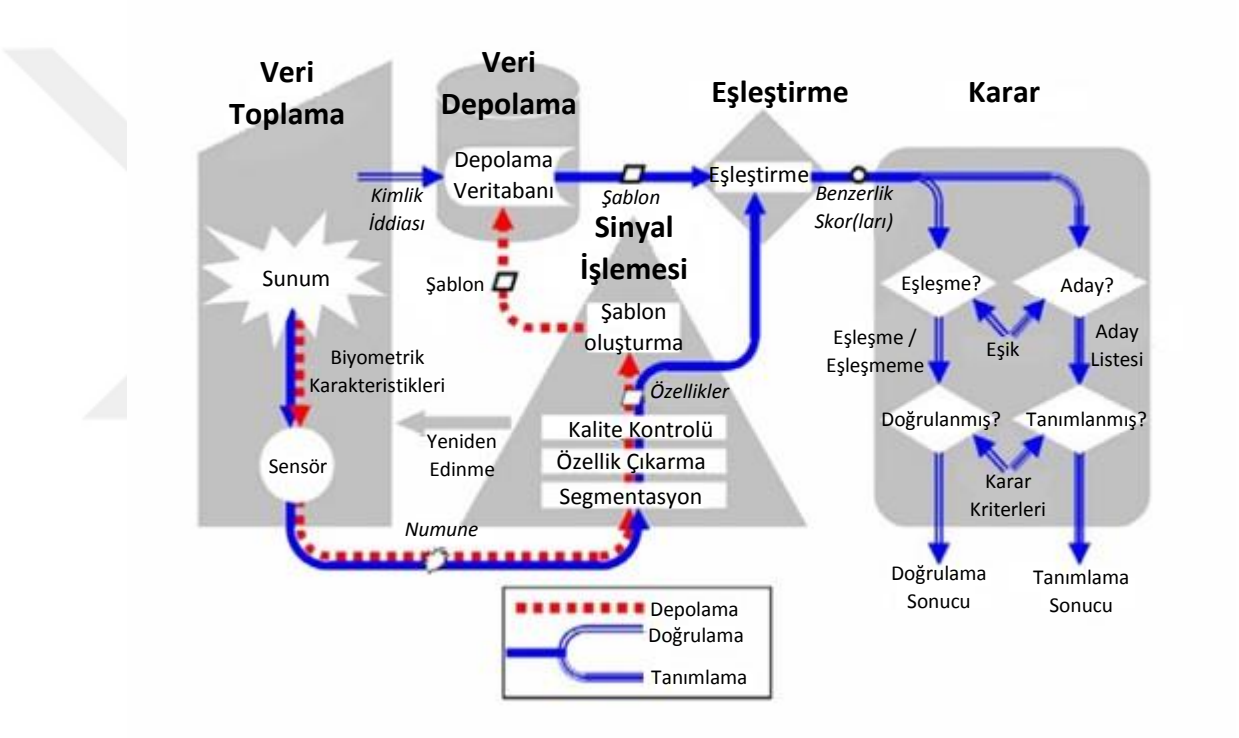
2.5 Genel Biyometrik Sistemi

Biyometrik sistem bir tür teknolojidir, kişinin fizyolojik, davranışsal veya her ikisini veri olarak alır, analiz eder ve kişiyi gerçek veya sahte kullanıcı olarak tanımlar [19].

Amaç: kimlik oluşturmaktır -neye sahip olduğunu- veya –neyi bildiğini- den ziyade kim olduğuna- (fizyolojik özellikleri gösterir) veya -ne ürettiğine- (davranışsal özellikleri gösterir) göre.

Bu paradigma tanımlama uygulamalarında sadece gelişmiş güvenlik sağlamamakta aynı zamanda birçok şifreleri hatırlama ve birçok doğrulama simgesini taşıma zorunluluğunuda önler. Birçok değişik özellik ve uygulama yöntemleri olmasına rağmen, çoğu biyometrik sistem aynı genel şemayı paylaşır, şekil (2-3)'te belirtildiği gibi. Bu şema biyometrik uzmanları tarafından kabul edilmiş olup standardizasyon prosedürleri için referans olarak kullanılır.

"ISO/IEC TR 24741 Bilgi Teknolojisi- Biyometrik Rehberi" Cenevre, 2006



Şekil (2-4) Genel Biyometrik sistem bileşenleri [22]

Bu şema hem verilerin kaydı hem de tanımlama veya doğrulama sistemlerin işletme sürecini gösterir.

Aşağıdaki maddeler bu alt sistemleri daha detaylı olarak tarif etmektedir:

- Veri toplama alt sistemi: bu sistem kişiden biyometrik sensöre sunulan biyometrik özelliği bir görüntü veya sinyal (işlenmemiş halinde) olarak toplar ve bu görüntü/sinyali biyometrik numune olarak sunar.

- Sinyal işleme alt sistemi: sinyal işleme alt sistemi ayırt edici özellikleri biyometrik numuneden çıkarır. Bu, kişinin biyometrik özelliğinin sinyalini alınan numunenin içinde tayin etmek (segmentasyon süreci), ayırt edici özelliği çıkartmak, ve kalite kontrolünü içerir. Böylece çıkarılan özelliğinin ayırt edilebilirliği ve tekrarlanabilirliği sağlanmış olur. Eğer kalite kontrolü toplanan numuneyi reddederse, kontrol sistemi yeni numune toplamak için veri toplama alt sistemine dönebilir. Kaydetme işleminde sinyal işleme alt sistemi çıkarılan biyometrik özellikten yeni bir şablon oluşturur. Çoğu zaman kaydetme sureci kişinin biyometrik özelliklerini birkaç kez sunulmasına gerektirir. Bazen, şablon sadece özellikleri kapsar.
- Veri Depolama alt sistemi: Şablonlar veri depolama alt sistemindeki kayıt veri tabanında depolanırlar. Her şablon kaydedilen kişinin detayları ile birlikte depolanır. Belirtmek gerekirki; kayıt veri tabanında depolanmadan önce, şablonlar biyometrik veri değişimi formatına yeniden format edilebilir. Şablonlar biyometrik toplama cihazında, taşınabilir cihazda lokal akıllı kart gibi, kişisel bilgisayarda, lokal sunucuda veya santral veri tabanında kaydedilebilirler.
- Eşleştirme alt sistemi: Burda, özellikler bir veya daha fazla şablonlar ile karşılaştırılır ve karar alt sistemi için benzerlik skoru oluşturulur. Benzerlik skorları özellikler ile karşılaştırılan şablonların uyum derecesini gösterir. Bazı durumlarda, özellikler kaydedilen şablonun aynı formunu alabilir. Doğrulamak için, tek spesifik bir kişi kaydı tek bir benzerlik skoruna neden olur. Tanımlamak için, birçok veya bütün şablonlar özellikler ile karşılaştırılabilir, ve her karşılaştırma için ayrı bir benzerlik skoru çıkartılır.
- Karar verme alt sistemi: Karar verme alt sistemi, doğrulama veya tanımlama işlemini gerçekleştirmek için bir veya daha fazla denemeden oluşturulan benzerlik skorlarını kullanıp sonuç kararını verir. Doğrulama durumunda, eğer karşılaştırılan özellikler ile şablonun benzerlik skoru belli bir eşiği geçerse aralarında uyum var demektir. Kişinin kaydı o zaman karar politikası kapsamında doğrulanabilir, bu da birçok denemeyi gerektirebilir.

Tanımlama durumunda, benzerlik skoru belli bir eşiği geçtiğinde, kaydedilen tanımlayıcı veya şablon özne için olası aday olabilir, ve/veya benzerlik skoru en yüksek *k* değerlerin arasında olup önceden belirlenmiş bir *k* değeri için oluşturulmuş var sayılır. Karar politikası, tanımlama kararını almadan önce birden fazla denemeyi isteyebilir [34].

2.6 Biyometrik Özellikler

Her biyometrik özellik kendi (lehte ve aleyhte) leri var, bu yüzden belirli bir özelliği seçmek sınıflandırma performansına bağlıdır aynı zamanda ana faktörler herhangi bir uygulama için biyometrik özelliğinin seçmesini etkiler. Doğrulama için kullanılan bazı çok bilinen biyometrik özellikler, Tablo (2-2)'de gösterilmiştir.

Biyometrik Özellik	**Açıklama**
Parmak izi	Parmak hatları, gözenek yapısı
İmza	Değişik özellikler kişinin yazısına dayalı
Yüz geometrisi	Spesifik fasiyel yapıların arasındaki mesafe (gözler, burun, ağız)
İris	İris paterni
Retina	Gözün arka fonu (ven yapıların paterni)
El geometrisi	Parmakların ve avuç içinin ölçümleri
Parmak geometrisi	Parmak ölçümleri
El üstü ven yapıları	El üstü ven yapıları
Kulak şekli	Gözüken kulağın boyutları
Ses	Ses tonu veya tını
DNA	Kalıtsal özelliklerin taşıyıcısı olan DNA kodu
Koku	Kişinin kokusunun kimyasal kompozisyonu

Tablo (2-3)'de doğrulama işlemi için en çok bilinen biyometrik özellikler [23].

2.7 Genel Biyometrik sistemlerin fonksiyonları

Sistem işleminde iki farklı aşama tanımlayabiliriz: Kaydetme aşaması, referans verileri depolandığında ve test aşaması veya sorgu aşaması, yeni girilmiş veri kaydı ile referanslarla karşılaştırıldığında gerçekleşir [33].

2.7.1 Kaydetme

'Kaydetme' terimi veri tabanına ilk kez bir şablon veya model yerleştirme işlemine denir. 'Şablon' terimi depolanmış özellikler için kullanılır. Biyometrik sistemin ilk aşaması kaydetme aşamasıdır. Bu aşamada her kullanıcı için ayrı bir biyometrik referans model oluşturulur. Bu, biyometrik referans karşılaştırma işlemi için kullanılır. Kaydetme aşamasının gerçekleşmesi için en az bir biyometrik numunenin sisteme girilmesi gerekir (veri toplama alt sistemi). Sonrasında biyometrik numune işlenme aşamasına geçer (sinyal işleme alt sistemi), özellikleri çıkarabilmek için (özellik çıkarılması), çıkarılan özellikler ile her kullanıcı için yeni bir biyometrik referans oluşturulur (şablon oluşturması). Oluşturulan referans depolanır (veri depolama alt sistemi) ve gerektiği zaman doğrulama veya tanımlama işlemini gerçekleştirmek için karşılaştırma da kullanılır. Kaydetme aşaması sırasında bazı bilgiler; kullanıcının ismi gibi, referans veriler ile beraber depolanabilir [20].

Referans şablon modeli tek bir numuneden veya birçok numunelerden oluşturulabilir.

2.7.2 Sorgu:

Bu basamakta kullanıcının biyometrik verileri tekrardan sisteme giriliyor ancak bu sefer önceden kaydedilmiş şablon ile karşılaştırılır. Sonra, sınıflandırma bileşeni tarafından yeni girilen numune için etiket tahsis edilir. Sorgu aşaması **Doğrulama** ve **Tanımlama** diye iki ana başlığa ayrılabilir:

2.7.2.1 Doğrulama:

Bu durumda bilmek istediğimiz, bir kişi gerçekten iddia ettiği kişi ile aynı olması. Doğrulama sırasında kullanıcı biyometrik verileri sisteme sunar (veri toplama alt sistemi) ve aynı zamanda iddia ettiği kişinin kimliği. Bu toplanılmış ve işlenmemiş

biyometrik verileri işleme safhasına geçer (sinyal işleme alt sistemleri) aynı zamanda iddia edilen kimliğinin biyometrik referans verileri veri depolama alt sistemlerinden çıkarılır. Her iki veri, kullanıcı tarafından sunulan biyometrik veriyi temsil eden özellikler ve veri deposundan çıkarılan biyometrik referans verileri birbiriyle karşılaştırılıyor (karşılaştırma alt sistemleri). Böylelikle, 'Karşılaştırma skoru' denilen benzerlik derecesini oluşturmuş olur. Bu skor karar alt sistemi tarafından alınır buda önceden belirlenmiş eşik seviyesini kullanarak kişinin iddia ettiği kimlik pozitif mı teyit eder.

Doğrulama iddia'yı kabul veya reddeder. Doğrulama kararının sonucu başarılı olacak eğer gerçek iddia kabul edilip yanlış iddia reddedilirse. Doğrulama kararının sonucu hatalı olarak kabul edilir eğer yanlış iddia kabul edilmişse Yanlış Kabul Etme Oranı (False Accept Rate - FAR) veya gerçek iddia reddedilmişse Yanlış Reddetme Oranı (False Reject Rate - FRR) [34].

Bu iki hatanın reytingi doğrulama görevlerinde değişik algoritmaların performanslarını karşılaştırmak için kullanılıyor. Bu kontrollü giriş uygulamalarında en sık kullanılan işleme modudur iki ana sebepten dolayı:

a) [1:1] karşılaştırması bütün veri tabanına karşılaştırılmasından daha güvenli. Çünkü hata olasılığı ikincisinde veri tabanın hacmi bereber katlanarak büyür.
b) Daha hızlı bir süreç olduğundan (tek bir karşılaştırma), daha özenli özellik çıkartma ve karşılaştırma algoritmaları daha düşük hata oranı ve muhtemelen daha yüksek bilgisayarsal maliyet her doğrulama için.

2.7.2.2 Tanımlama:

Kullanıcı kim olduğu söylemesine gerek yok, sisteme sunulan soru şöyle: bu kişi veri tabanında kayıtlı mı? Sistem veri tabanında bütün kayıtlı kişilerin arasından kimin numunesi alınmış diye belirtmesi gerekiyor. Cevap hayır olabilir (yani kişi sisteme yabancıdır) veya veri tabanındaki kayıtlı herhangi bir kimlik olabilir. Nitekim, sistem bir'e-çok karşılaştırma süreci uygulaması gerekir çünkü girilen numuneyi bütün depolanmış şablonlarla karşılaştırması gerekir.

Bu bir [1: N] ilişkisi, ve bu yüksek hızlı algoritmaların kullanılmalarını gerektirir ve etkili arama yöntemleri ki sistem kabul edilen zaman içerisinde çalışsın diye.

Tanımlama işlemi doğru olarak kabul ediliyor eğer kişi biyometrik sistemde kayıtlı ise, ve kimliği kayıtlı kişilerin aday listesinde dahil ise Gerçek Pozitif Tanımlama (True positive identification-TPIR). Tanımlama süreci hatalı olarak kabul edilir eğer kullanıcının kimliği aday listesinde kayıtlı değil ise (yanlış-negatif tanımlama hatası), veya eğer kullanıcı kayıtlı değil ve aday listesi boş değil ise (Yanlış-pozitif tanımlama hatası)

2.8 Performans Değerlendirilmesi: Hata Oranları

Biyometrik sistem giriş aygıtından toplanan kullanıcı verilere dayanır.

Kullanıcılar ile giriş aygıtların arasındaki her etkileşimden alınan biyometrik numune farklıdır. Bu numuneler, kayıt sırasında şablon oluşturmak için veya doğrulama/tanımlama süreçlerinde karşılaştırma skorunu hesaplamak için kullanılabilirler. Hesaplanan skorlara göre, sistem eşikleme işlemini kullanarak kullanıcı gerçek mı yoksa sahteci mı karar verir. Belli bir eşiğin (t) altındaki skorlar gerçek olarak etiketlenir ve bu eşiğin üstündeki skorlar sahteci olarak etiketlenir.

Biyometrik kararlar, olasılıklara dayanır ve bu uyumsuzluk hatalarına sebep olabilir. Hata oranlarını ölçmek biyometrikte çok önemli çünkü bu sistemler sadece patern tanıma hatalarına değil aynı zamanda toplama sürecinin hatalarına da bağlıdır. En sık hata oranları ISO/IEC 19795-1 ve "Biyometrik cihazlarının performansının test ve raporlamada en iyi pratik uygulamaları" 'ına göre:

Yanlış eşleştirme oranı (False Match Rate - FMR): yanlış eşleştirme oranı (sıfır - efor) sahteci girişimlerinden gelen numune orantılarıdır. Bunlar da kişiye ait olmayan şablon ile yanlış olarak eşleştirilenlerdir.

Yanlış eşleştirme oranı bir numunenin yanlış olarak tek, rasgele-ile-seçilmiş, "kişiye ait olmayan" şablonu ile eşleştirmenin beklenen olasılığıdır, ve bu biyometrik sistemin yanlış olarak yetkisiz kullanıcıyı geçerli kullanıcı olarak tanımlama olasılığını yansıtır (yanlış pozitif).

FMR, Yanlış Kabul Etme Oranı (FAR) veya Tip-II hata olarak da adlandırılır.

FAR = Yanlış Kabul Etme sayısı / Tanımlama denemelerin sayısı

Yanlış Eşleştirmeme Oranı (False Non-Match Rate - FNMR): Yanlış eşleştirmeme oranı gerçek denemelerden elde edilen numunelerin orantısı, ve yanlış olarak, numuneyi sunan aynı kişinin aynı özelliklere taşıyan şablonu ile eşleştirmeme.

Yanlış eşleştirmeme oranı aynı ölçülere sahip olan ve aynı kullanıcı tarafından sunulan numunenin yanlış olarak kendi şablonu ile eşleştirmemenin beklenen olasılığıdır. Bu, biyometrik sistemin yanlış olarak yetkili kullanıcıyı geçersiz kullanıcı olarak tanımlamasının olasılığını gösterir (Yanlış negatif).

FNMR aynı zamanda Yanlış reddetme oranı (FRR) veya Tip-I hata olarak ta adlandırılır.

FRR = Yanlış reddetmelerin sayısı / Tanımlama denemelerin sayısı

Biyometrik sistemde performans ölçümleri Yanlış Reddetme Oranı (FRR) ve Yanlış Kabul Etme Oranı (FAR)'a yakından bağlıdır. İdeal biyometrik sistem FRR ve FAR için sıfır değer vermesine beklenir. Yani bütün geçerli kullanıcıları kabul etmesi gerekir aynı zamanda bütün sahteci kimlikleri reddetmesi de gerekir ve bu pratik te pek mümkün değil.

FRR ve FAR birbirine ters orantılı. Eğer FAR daha fazla ise, FRR azalır. Yüksek FRR veya düşük FAR'ı sunan bir biyometrik sistem yüksek güvenlik sağlar. Eğer FRR çok yüksek olursa, sistem canlı numuneyi birçok kere sisteme girilmesine gerektirir ve bu etkinliğini azaltır.

Bugünkü biyometrik teknolojileri ideal olmaktan çok uzak. Bu yüzden, sistem kurucuları bu iki faktörün arasında iyi bir denge kurmaları gerekiyor güvenlik gereksinimlerine göre.

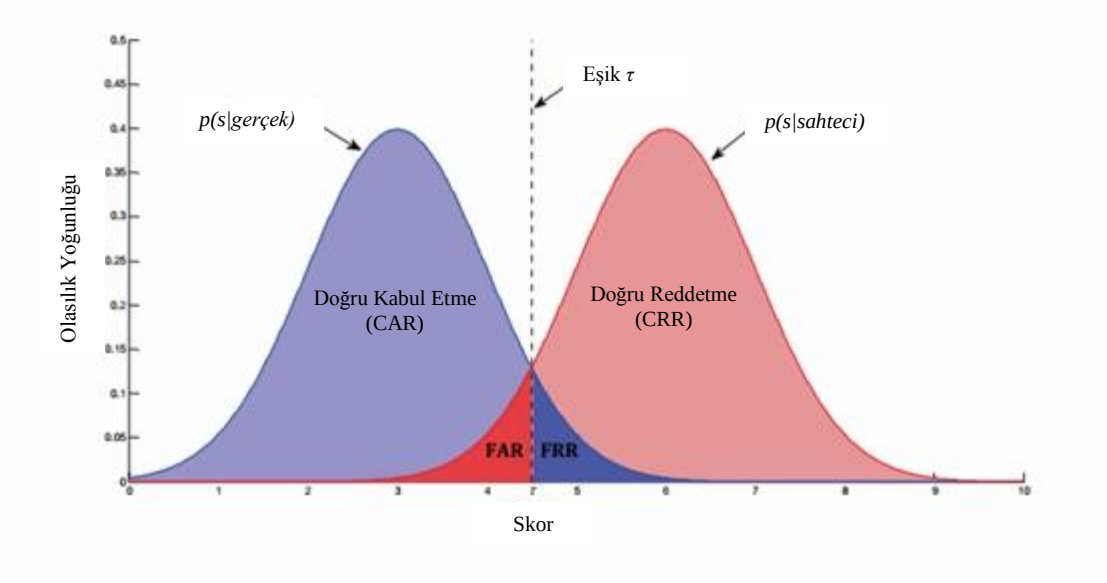
Bu iki olasılıkların tamamlayıcıları, Doğru Kabul Etme Oranı (Correct Acceptance Rate - CAR) ve Doğru Reddetme Oranı (Correct Rejection Rate - CRR)'dir.

Bu yüzden CAR = 1 – FAR ve CRR = 1 - FRR

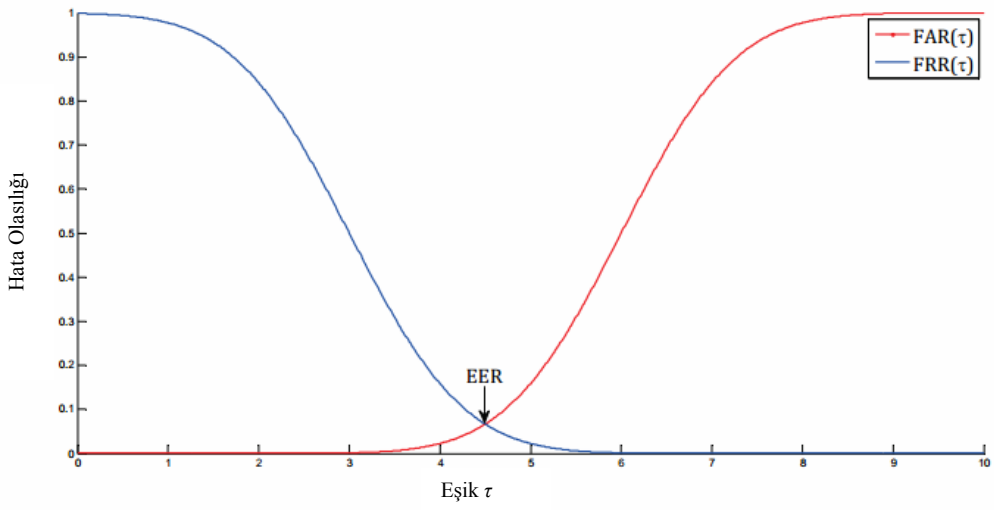
FAR ve FRR beraber, belli bir karar verme eşiği için tanımlama sisteminin doğruluğunu karakterize ederler.

<u>Eşit Hata Oranı (Equal Error Rate - EER):</u> her iki hata kabul etme ve hata reddetme oranlarının eşitlenince pratikteki biyometrik sistemlerin en sık kullanılan ölçüm yöntemlerinden biridir FAR = FRR.

EER değeri ne kadar düşük olursa sistemin doğruluğu o kadar artar.



Şekil (2-5) Eşiğin süreci ve FAR ve FRR'lerinin şekli

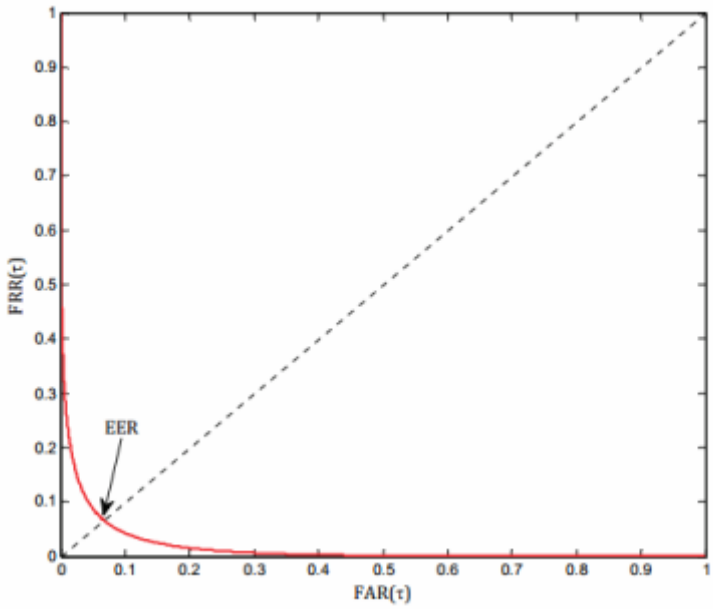


Şekil (2-6) τ eşiğinin FAR ve FRR'leri. İki eğrilerin kesiştiği nokta EER'dır.

Değişik biyometrik sistemlerin performanslarını karşılaştırmak ve analiz etmek için, Alıcı İşletme Karakteristik eğrisi (ROC) tanımlama sistemleri için kullanılır.

Alıcı İşletme Karakteristik eğrisi (Receiver operating characteristic curve - ROC): Doğrulama sisteminin kapasitesinin görüntüsel temsili için sık kullanılan bir eğridir.

(ROC) eğrisi, x-eksenindeki yanlış pozitiflerin oranları (kabul edilen sahteci denemeleri)'ine karşı y-eksenindeki gerçek pozitiflerin oranları (kabul edilen gerçek denemelerinin) eğri çizimidir. Karar verme eşiğinin bir fonksiyonu olarak parametrik ölçümlerle çizilmiş.



Şekil (2-7) ROC eğrisi FAR ve FRR'leri temsil ederken.

EER, eğrinin çapraz çizgi ile kesiştiği noktasıdır (FAR = FRR)

Pazarlıksız hata bulma eğrisi (Detection error trade-off curve - DET): modifiye ROC eğrisidir. Her iki hata oranlarını her iki eksende çizer (FAR x-ekseninde ve FRR y-ekseninde). Bu eğride, FAR ve FRR'nin eşit olduğu nokta EER olarak adlandırılmıştır. Linear olmayan skalayı kullanmak, rakip olan sistemlerin karşılaştırmasını kolaylaştırır.

Tanımlama Oranı (Gerçek-Pozitif) (True-Positive Identification Rate - TPIR): Gerçek-pozitif tanımlama oranı, sistemde kaydedilen kullanıcılar tarafından gerçekleştitlen tanımlama işlemlerinin orantısı. Burada kullanıcının doğru tanımlayıcısı elde edilenlerin arasındadır.

Hata-Tanımlama Oranı (Yanlış-Negatif) (False-Negative Identification Error Rate - FNIR): Yanlış-negatif hata-tanımlama oranı, sistemde kaydedilen kullanıcılar tarafından gerçekleştirilen tanımlama işlemlerinin orantısı. Burada kullanıcının doğru tanımlayıcısı elde edilenlerin arasında değildir.

Kaydetme Başarısızlığının Oranı (Failure-to-enroll Rate - FTE): Kaydetme başarısızlığının oranı, sistem tarafından kaydetme sürecini tamamlamayı başarılmayan popülasyon orantısı. Kaydetme başarısızlığının oranı aşağıdakilere içermeli:

- Kullanıcının gereken biyometrik özellikleri sağlayamadığı denemeler.
- Kaydetme işleminde yeterli kaliteli numune sağlayamayan kullanıcılar.
- Kaydedilen bilgilerin kullanışlı olduklarını onaylamak için yapılan denemeler sırasında yeni oluşturulmuş şablon ile güvenilir bir eşleştirme kararını sağlayamama.

Sistemde kaydedilemeyen kullanıcıların denmeleri edinememe orana veya eşleştirme hata oranlarına etkilemez.

Edinememe Oranı (Failure-to-acquire Rate - FTA): Edinememe oranı, tanımlama veya doğrulama işlemini gerçekleştirmek için yapılan denemelerin orantısı. Burada sistem yeterli kaliteye sahip olan numuneyi yerleştirme veya elde etmeyi başaramaz.

Edinememe oranı aşağıdakilere sahip olmalı:

- Biyometrik özelliklerin sunulmama veya elde edilememe durumu ile sonuçlanan denemeler (hastalık veya hasar durumunda).
- Özellik çıkarma veya segmentasyon işleminde başarısızlık ile sonuçlanan denemeler.
- Çıkarılmış özelliklerin kalite kontrol eşiğini geçmemesi ile sonuçlanan denemeler.

Bütün bahsedilen hatalar biyometrik sistemlerin tasarımında çok önemli parametrelerdir ve sık sık alınacak kararları yönlendirirler. İlaveten, araştırmacılar bazen biyometrik sistemleri değerlendirmek için başka parametreler de kullanır.

Yarım-Tam Hata Oranı (Half Total Error Rate - HTER): FAR ve FRR'lerin arasındaki ortalama

Gerçek Eşleştirme Oranı (Genuine Match Rate - GMR): Gerçek numunenin kabul etme orantısı (1-FRR).

Doğru Sınıflandırma Oranı (Correct Classification Rate - CCR): sınıftan bağımsız, numunelerin doğru sınıflandırma orantısı.

Doğru Tanımlama Oranı (Correct Identification Rate - CIR): Kimlikten bağımsız, doğru tanımlanmış numunelerin orantısı.

Hata oranlarına ve daha önce biyometrik özelliklerin hakkında bahsedilen güçlüklere ilaveten, daha pratik faktörler de; maliyet, kolay kullanışlı olması, sensör kalitesi ve hız gibi bir sistemin bir uygulamaya uygun olmasına etkiler.

2.9 Biyometrikler ve Gizlilik

1. Daha sık kullanılan tanımlama yöntemlerine karşın, biyometrik ölçümler kişisel bilgileri içermez ve çalması veya sahtesini oluşturmak daha zor.
2. Biyometrik ölçümler, isim veya sosyal güvenlik numarası yerine güvenli isimsiz işlemleri gerçekleştirmek için kullanılabilir.
3. Bazı biyometrik ölçümler (yüz görüntüsü, ses sinyalleri ve yüzeylerde bulunan 'latent' parmak izleri gibi) kişinin bilgisi olmadan alınabilir ancak, daha önce kaydedilmiş veri tabanı olmadan belli bir kimliğe bağlanamaz.
4. Sosyal güvenlik numarası veya kredi kartının numarası ve bazen hatta kişinin yasal ismi, büyük bir popülasyon da bir insanı tanımlayabilir. Bu kabiliyet herhangi bir biyometrik ölçümü kullanarak gösterilmemiş.
5. Telefon ve kredi kartın bilgileri gibi, mahkeme kararı ile biyometrik veritabanları tasarlanmış amaçları dışında da incelenebilir.
6. Kredi kardı, telefon ve sosyal güvenlik numarası karşın, biyometrik özellikler bir ölçümden diğer ölçüme değişir.

7. Biyometrik ölçümleri kullanarak kişisel verileri aramak, diğer daha iyi olan tanımlayıcıları kullanmak gibi güvenilir ve etkin değildir (kişinin yasal ismi ve sosyal güvenlik numarası gibi).
8. Biyometrik ölçümler hep gizli değildir, bazen herkesçe gözlemlenebilir ve risk altında olursa iptal edilemez.

Bölüm 3

İmza Doğrulama Sistemi

3.1 Genel Bakış

Yüzyıllar boyunca günlük aktivitelerde kişisel doğrulama için en yaygın olarak kullanılan teknikler el yazısı imzasıdır [70]. El yazısı imza, zaman içinde en çok kullanılan tanımlama modeli olduğu için diğer biyometrik biçimlerin arasında çok özel bir yere sahiptir [35]. El yazısı imza, resmi bir belgenin doğrulaması için hep en basit ve kabul gören yöntemlerden olmuştur. Elde edilmesi kolaydır, anlık davranışlardan kaynaklanır ve her bir bireye özgüdür [40]. "İmza kişiyi yansıtır" diye eski bir çinli deyiş vardır. Bir kişinin ismini imzaladığı şekil, özgül bir bireysel özelliktir; çünkü el yazısı imza her kişiye özgündür. Binlerce yıldır imzalanmış belgeler için yasal bir delil olarak kabul edilmiştir [6].

Bir kişinin imzası, ardışık edinimde bile önemli ölçüde değişiklik gösterebilir [33]. Bir kişinin iki gerçek imzasının kesinlikle aynı olmadığı bilindiği üzere bazı imza uzmanları, aynı kişinin kağıda atılmış iki imzasının aynı olması halinde, ikinci imzanın sahte olarak nitelendirebilirler. Aynı kişi tarafından atılan ardışık imzalar hem küresel hem de yerel olarak farklılık gösterir ayrıca ölçek ve oryantasyon açısından da farklılık gösterebilirler. Olağandışı koşulların altında atılan imzalar, imzayı etkiliyebilir. Örneğin, aceleyle, dikkatsizlik ile, ayrıca, garip bir kalemle ve alışılmadık bir yerde atılan imzalar aynı kişinin normal imzalarından farklı olması muhtemeldir [38].

İmza doğrulaması, bir kişinin el yazısı imzasını tanımak için kullanılan süreçtir [13]. İmza doğrulaması, davranış temelli biyometrik sistemlerden biri olarak kabul edilmektedir, ve son birkaç yıl içerisinde bu konuyla ilgili geniş bir araştırma yelpazesi bildirilmiştir [54]. İmza doğrulama sisteminin amacı, gerçek bir imzayı sahte bir imzadan ayıran bir süreçle, imzayı analiz ederek bir kişinin kimliğini doğrulamaktır. Süreç, klasik patern tanıma modeli adımlarını izler, bunlar veri toplama, önişleme, özellik çıkarma ve sınıflandırmadır (genellikle imza doğrulama alanında "doğrulama" olarak anılır) [40].

İmzalı kimlik doğrulama ile ilgili ele alınması gereken üç ana konu vardır. Birinci konu uygun imza özelliklerinin seçilmesidir. İkincisi, seçilen özellikleri için uygun bir sınıflandırıcıya sahip olma seçeneğidir ve son olarak, seçilen özelliklerini etkileyen duyguların sorunu [24].

3.2 İmza Doğrulama Sorunları

İmza doğrulama, benzersiz imza özelliklerine göre kişileri doğrulamak için tasarlanmıştır. Sonuç olarak, tutarlı bir şekilde imzasını atmayan bireylerin imzalarını doğrularken kaydolmalarında ve doğrulamalarında zorluk çekebilirler. Kayıt sırasında bireylerin, sistemin kaydedilen imzaların arasında ortak özelliklerin büyük bir yüzdesini bulması için, yeterince benzer bir dizi imzayı sağlamalıdırlar.

Doğrulama sırasında yetkili kişinin imzaladığı güvenle onaylamak için yeteri özelliklerin sabit kalması gerekir. Sonuç olarak, kas hastalıkları olan kişiler ve bazen yalnızca baş harfleriyle imzalayan kişiler daha yüksek "Yanlış Reddetme Oranı" (FRR) ile sonuçlanabilir ki, bu sistemin yetkili bir kullanıcıyı hatalı bir şekilde reddetme ihtimalini ölçer. Birçok kullanıcı tablet üzerine imzalamayı alışkın olmadığından, bazı dijital imzalar, mürekkep ile kağıda atılan imzalardan farklılık gösterebilir, böylece yanlış reddedilme olasılığı artma eğilimi gösterir [54].

3.3 İmza Doğrulama Türleri

İmza doğrulaması, dünya çapında kişiyi tanımlamak için kullanılan benzersiz bir yöntemdir [41]. İmzanın doğrulama sürecinde, kendi imzası olduğunu iddia eden kişinin o imzanın kişiye ait olup olmadığını belirlenir. Veri toplama mekanizmasına dayanarak, imza doğrulama süreci offline (genellikle statik olarak anılır) veya online (dinamik olarak anılır) olarak sınıflandırılabilir.

- **Offline veya statik**–Offline doğrulaması, imzanın resiminden gelen bilgilerin tek mevcut olan bilgi olduğunda olur. Bu, vuruşların çizilme şeklini, hangi sırayla ve hangi hızda atıldığına dair bilgi olmadığı anlamına gelir [43].

  Offline doğrulaması, daha önce toplanan görüntü veya sinyallere dayanır. İmza, kağıda atılır ve daha sonra taranır veya dijital pad gibi cihazları kullanarak

doğrudan bilgisayara atılır. İmza numunesi daha sonra bir veri görüntüsü (dijital görüntü) biçiminde yeniden oluşturulur. Sonuç, M × N pikselden oluşan bir bitmap görüntüsü (dijital görüntü) oluşmasıdır ve doğrulamanın tüm süreçleri buna dayanmalı.

Görüntü çözünürlüğü ne kadar büyük olursa, kimliği doğrulamak için uzmanlar ve sistemler o kadar fazla bilgiyi değerlendirmek zorunda kalacaktır. Birçok banka, kayıtlı imza kartlarıyla imzalı çekleri hızlı bir şekilde karşılaştırmalarına olanak tanıyan bir tür yakalama yöntemiyle imza doğrulaması kullanmaktadır. Bu sistem imza karşılaştırmalarına dayanır ve bankaların sahteciliği azaltmalarına yardımcı olmuştur, ancak tanımlama sürecinde sınırlı kullanımları vardır. Böyle bir tekniğin zorluğu, iyi bir sahteci imzanın şeklini kopyalayabilmesidir (kopyalanması kolaydır).

Offline imzada doğrulama işlemi için, imza resminin yalnızca X ve Y koordinatları (statik özellikleri) mevcuttur [13] [24] [42] [70], ve imza bir gri seviyeli görüntü olarak gösterilir {S(x, y)} $0 \leq x \leq X$, $0 \leq y \leq Y$, S(x, y)'da resimdeki (x, y) pozisyonda gri seviyeyi belirtir [37].

Şekil (3-1) Taranan imza, işlenmeden önce ve işlendikten sonra[11].

- **Online veya dinamik**–Doğrulamanın, resim veya sinyal gönderildiği sırada yapıldığı anlamına gelir. Bu durumda, imza bir sekans olarak gösterilir{S(n)} n=0, 1,..., N , burada S(n) imzalama işleminin ($0 \leq n \leq N$) $n\Delta t$ zamanında örneklenen sinyal değeridir, Δt'de örnekleme süresidir [37].

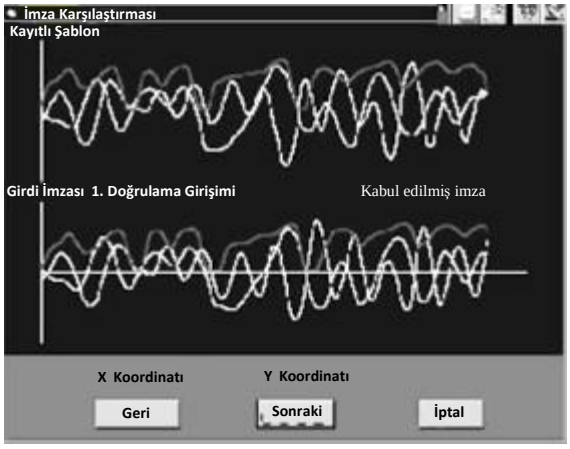
Online imzalar, hem dinamik özelliklerini hem de şekil bilgilerini yakalayan, tablet sayısallaştırıcı ve akıllı kalemler gibi özel cihazlar kullanılarak yakalanırlar [69]. Online imza doğrulamasında, imzanın nasıl çizildiğine dair bilgiler mevcuttur [43].

Dinamik imza doğrulamasında, imzanın şekil veya görünümü anlamlı değildir; anlamlı olan ise imzalama işlemi sırasında oluşan hız, basınç ve zamanlamadaki değişikliklerdir. Zamanlamadaki ve X, Y ve Z (basınç)'taki değişiklikleri yalnızca orijinal imzalayan kişi yeniden oluşturabilir. İmzayı bu benzersiz yöntemle analiz etmek, başka bir kişinin X, Y ve Z'deki zamanlama değişikliklerini kopyalaması neredeyse imkansız hale getirir.

Sahtecinin hem görüntünün şeklini hem de asıl imzacı tarafından yazıldığı şekilde taklit etmesi zordur ve dolayısıyla offline imza ile karşılaştırıldığında daha güvenilirdir [69]. Online doğrulamada, imza doğrudan sayısallaştırıcı cihazda yapılır. Bu amaca uzmanlaşmış cihazlar vardır, ancak akıllı telefonlar ve tabletler gibi genel amaçlı cihazlar da imzayı yakalayabilirler. Uzmanlaşmış cihazlar daha iyidirler çünkü çözünürlükleri daha iyi ve sonuç daha hassas [13] [42].

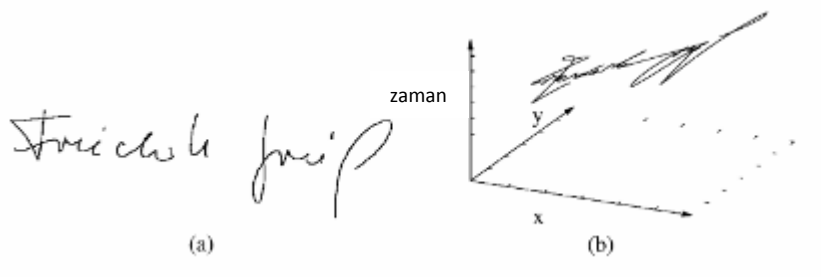
Bu girdi cihazları imza atma işlemi sırasında stylus kalemin x-y düzlemindeki hareketini yakalarlar, aynı zamanda kalemin ucu ile yazma yüzeyine uyguladığı basınç ile kalemin karakteristik tutulumu sırasında oluşan genel eğim ve azimut açıları da yakalanır [70]. Dinamik imza doğrulama teknolojisi, bir bilgisayar kullanıcısının kimliğini doğrulamak için el yazısı ile atılmış bir imzanın davranış biyometriklerini kullanır. Eski teknolojilerin aksine (sıkça paylaşılan, kolayca unutulan, kaybolan veya çalınan parola ve anahtar kartları gibi), dinamik imza doğrulaması, artmış bilgisayar güvenliği ve güvenilir belge yetkilendirmesi için basit bir yöntem sunar [13].

Genel olarak, online imza doğrulaması, offline doğrulama yöntemlerinden daha yüksek doğrulama oranı verir, çünkü sadece statik özellikleri kullanan offline doğrulamanın aksine, problem alanının hem statik hem de dinamik (veya geçici) özelliklerini kullanır [2]. Offline ve online doğrulama yöntemlerin arasındaki farklılıklar sadece özellik çıkarma aşamalarıyla ve doğruluk oranlarıyla değil, aynı zamanda veri toplama modlarında, önişleme ve doğrulama / tanıma evrelerinde de olur, ancak online doğrulama (veya tanıma) prosedüründeki görevlerin temel sırası, offline işleminin aynısıdır [2].



Şekil (3-2) İmzayı atan orijinal kişi, zamanlamadaki değişiklikleri ve X, Y ve Z'yi yeniden oluşturabilir [13].

Online ve offline teknikleri, nesneye ait bilgiler açısından çok farklıdırlar. Dinamik sistemler, statik sistemlerden daha çok fazla bilgiye sahiptirler. Bu gerçek doğrulama performansına yansır ve daha düşük hata oranlarına ulaşılmasını sağlar [70].



Şekil (3-3) Offline imzaya karşı Online imza

(a) Offline iken yakalanan imza. Sadece mekansal bilgi mevcut.

(b) Z-ekseni boyunca görüntülenen zamansal bilgiyle beraber, aynı imzayı gösterir.

Azimut ve yükseklik göreceli yüksek standart sapmalara sahipken, *X, Y* pozisyon koordinatları, *V* hızı ve *P* basıncı, en güvenilir dinamik özelliklerdir [59]. Bu projede, online imza doğrulaması kullanıldı ve imzanın nasıl atıldığı ile ilgili kullanılan bilgiler, kalem ucunun koordinatları (x ve y koordinatları) ve basınç olarak alındı.

Konuyla ilgili birçok araştırma çalışmaları online imza doğrulaması üzerine yapılmıştır [54].

3.4 Dinamik imza doğrulamasının avantajları

Bu tip biyometrik sistemin avantajlarından biri, imzaların yüzyıllarca kabul edilmiş bir kimlik doğrulama aracı olması gerçeğidir. Binlerce yıldır ticari işlemlerde kağıt belgelerin yasal bir kanıtı olarak kabul edilmiştir. Yeni e-ticaret ortamında doğal bir dönüşüm, e-belgeleri imzalamak için online imzaları kullanmaktır. Dinamik imza doğrulama sisteminin bir diğer avantajı, şifrelerin, PIN'lerin veya anahtar kartlarının yerine geçmesidir. Çalınması, kaybolması veya unutulması muhtemel olan kimliklerin yerine basit bir imza geçti. Uzak bir yerden güvenli bir bilgisayar sistemine giriş yapmak, bir grafik tableti ve imza ile yapılabilir. Diğer avantajları da toplam hata oranının düşük olması ve sahteci kişinin gerçek imzanın bir kopyasını almayı başarsa bile sahteciliğinin tespit edilmesidir [13][6].

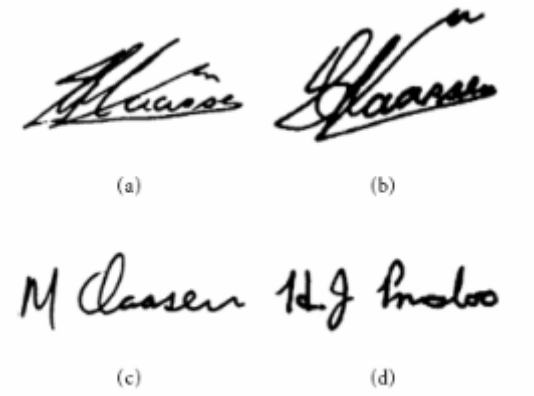
3.5 İmza Sahteciliği

İmza doğrulama sistemlerinin en büyük zorluklarından biri, hem şekil hem de atılma sırasındaki davranışları taklit eden sahte imzalar ile uğraşmaktır [70]. İmza doğrulama sistemleri, bir kişinin imzasını oldukça tutarlı bir şekilde üretebileceği varsayımına dayanmaktadır; Bir sahtecinin genel imza görünümünü, yazma hızını, kalem ucuna uygulanan kuvveti, ve kalemin tutulduğu açıyı aynı anda kopyalaması zordur. Araştırma amaçları için, sahtecilik modelleme yaklaşımının performansını ölçmek için çok önemlidir. Bir sistemin gerçek imzaları kabul etmesi, sahtecilikleri önlenebileceği garantisini veremez. Bu nedenle, bir veri tabanındaki sahteciliklerin kalitesi, veri tabanından türetilen sonuçların güvenilirliklerini büyük ölçüde belirleyecektir [44]. Sahteciler, çok pratik yapmadan balistik bir hareketle başka birinin imzasını atamaz ve bu nedenle hiçbir zaman iyi bir sahte imzayı üretmek mümkün olamaz [38]. Bir imza, iddia eden kişiye ait olduğu onaylandıysa, imzanın orijinal / özgün olduğu söylenir ve kişiye *müşteri* veya *orijinal* / *hedef* / *örnek yazar* / *yazar* / *imzalayan* adı verilir. Aksi takdirde, imzaya sahte ya da simülasyon denir ve onu atan kişiye *taklitçi* / *sahteci* ya da *örnek-olmayan yazar* denir. Genellikle, sahte imza / simülasyon aşağıdaki türlerden herhangi birinde sınıflandırılır:

- **Rastgele Sahtecilik / Basit veya Sıfır-Efor Sahtecilik**: Sahtecinin otantik yazarın gerçek imzalarının hakkında hiç bir fikri olmayan ve daha önce hiç

görmeden, yazarın imzasının şeklini bilmeyip ancak kafasından ürettiği imzayı atan sahtecilik türü'ne denir. Bunu yazarın isminden türetebilir [74]. Bu sahtecilik için EER (Eşit Hata Oranı) % 0.01'den azdır temel güvenlik modunda.

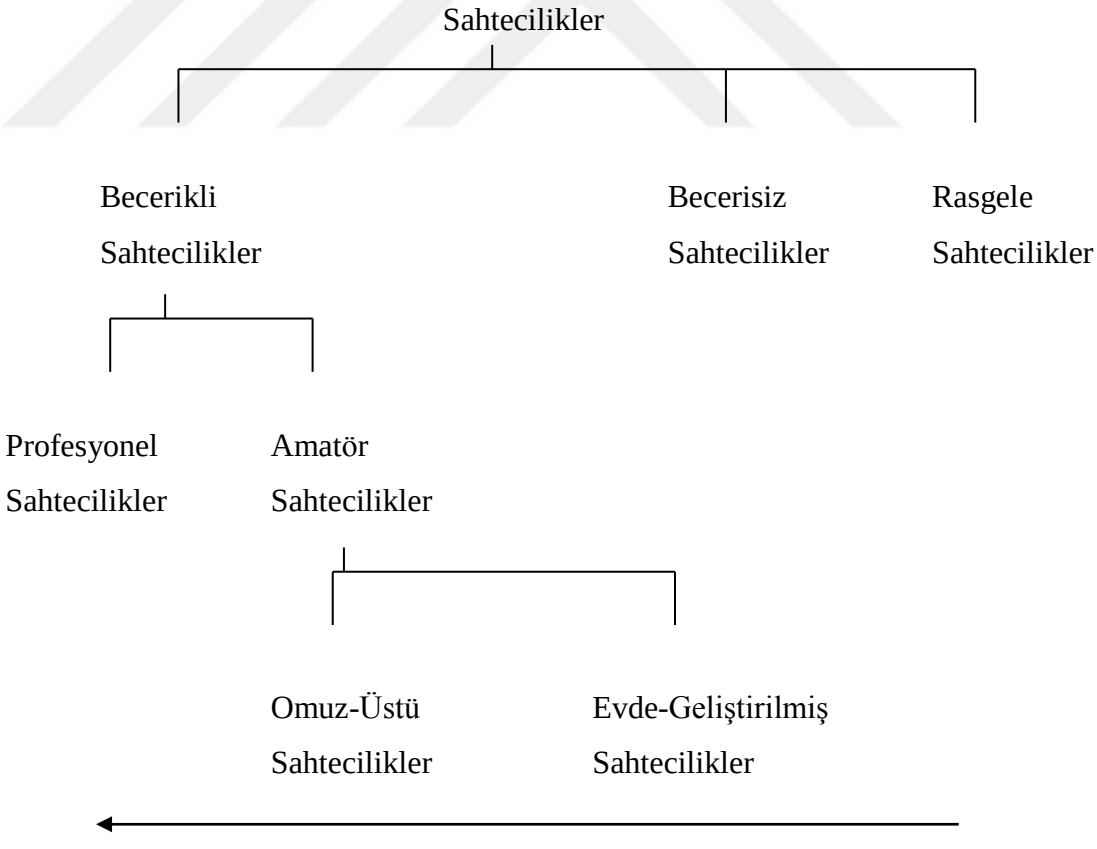
- **Becerisiz Sahtecilik / Basit veya sıradan sahtecilik:** Sahtecinin bir kişinin orijinal imzalarını gördüğü ve çok fazla pratik yapmadan taklit etmeye çalıştığı türdür. EER, imzanın türüne göre değişebilir, çünkü basit imzaların taklidi daha kolayken karmaşık imzaların dinamik olarak taklit edilmesi çok zordur. Bu sahtecilik için EER, temel güvenlik modunda tipik olarak % 0.5'in altındadır.
- **Becerikli Sahtecilik:** Sahtecinin, bir kişinin gerçek imzasını görmüş ve pratik yapmış olmasıdır. Sahteci, imzayı gözlemlemek ve taklidin pratiğini yapması için çeşitli cihazlardan faydalanabilir. Bu sahtecilik için EER, Biyometrik Motor'un temel güvenlik modunda % 2,5'ten az ve gelişmiş güvenlik modunda % 0,5'ten azdır. Yüksek güvenlik modunda, % 0.01'den azdır [45] [46] [50]. Becerikli sahtecilik kategorisi de, amatör ve profesyonel sahteciliğe ayrılmıştır. Profesyonel sahtecilik, el yazısı analizinde profesyonel uzmanlığa sahip bir kişi tarafından yapılır ve yüksek kaliteli sahtecilik ile sonuçlanır. Amatör sahtecilikleride tekrar, evde geliştirilmiş ve omuz-üstü sahteciliklerine ayrılır. Evde geliştirilmiş tipte, sahteci da imzanın kopyası var ve evde pratik yapması için yeterli vakti vardır. İmzanın reprodüksiyonu, görüntünün statik özelliklerine dayanır. Omuz-üstü imza sahtecilikleri de, sahtecinin yazarın gerçek imzasını atarken hemen tanık olduğu zaman üretilir; Bu durumda sahteci de imzanın dinamik özellikleri ve mekansal görüntüsü vardır [74].



Şekil (3-4) (a) Gerçek bir imzanın örneği (b) Becerikli sahtecilik

(c) Becerisiz sahtecilik (d) Rasgele sahtecilik [48].

Ancak, çeşitli becerikli sahtecilik seviyelere dayanılarak, farklı alt gruplara da ayrılabilir. Aşağıdaki tablo (3-1), Sahtecilik Türlerini gösteriyor:



Tablo (3-1) Sahteciliklerin Sınıflandırılması.

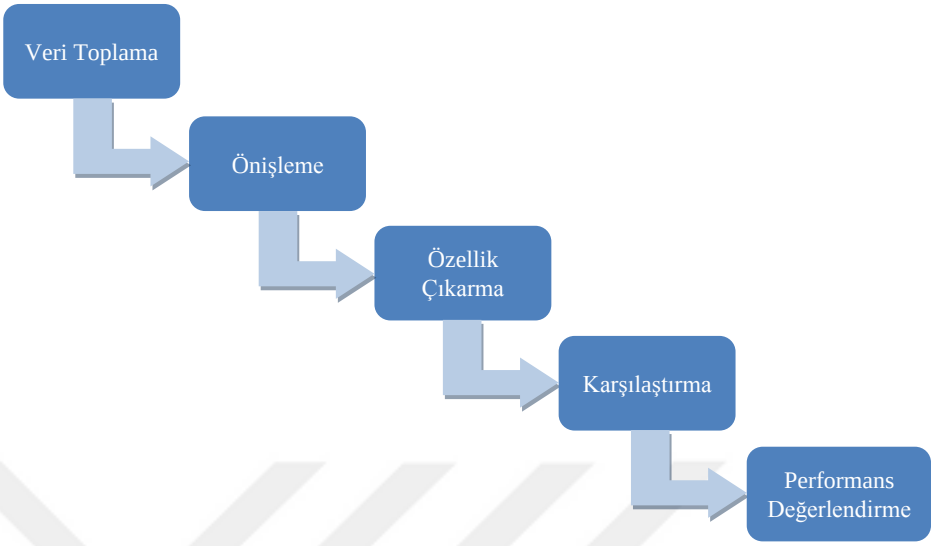
Hangi sahtecilik türü kullanıldığına bağlı olarak, imza doğrulama süreci farklı biçimlerde olabilir. Tablo (3-2), imzanın önceden bilinmesi ile sahteciliğin başarısı arasındaki ilişkiyi göstermektedir. "Aktif sahteci girişimleri" nin yedi farklı seviyeleri tanımlanmaktadır; bunların hepsi, sahtecinin taklit edilecek imzanın önceki bilgisine dayanır.

Seviye	Mevcut olan Bilgiler
0	Sahteci, iddia ettiği kullanıcının kimliği ile ilgili bilgi sahibi olmaması
1	Sahteci, iddia ettiği kullanıcı kimliğinin adını bilmesi
2	Sahteci, iddia ettiği kullanıcı kimliğinin imzasının statik görüntüsünü görmesi
3	Sahteci, iddia ettiği kullanıcı kimliğinin imzasını, imza atma işlemi sırasında, statik görüntüsünü görmesi
4	Sahteci, iddia ettiği kullanıcı kimliğinin imzasının bir örneğini çizebilmesi
5	Sahteci, iddia ettiği kullanıcı kimliğinin imzasına yeni tanık olması
6	Sahteci, iddia ettiği kullanıcı kimliğinin imzasına defalarca tanık olması

Tablo (3-2) Sahtecinin imza verileri ile ilgili önceki bilgisi [47].

3.6 Genel İmza Doğrulama Sistemi

İmza doğrulama sistemi genelde, imzayı kabul veya reddetmek için, girilen verileri iteratif olarak işleyen ardışık birimler halinde bölünür [45]. Doğrulama işlemi birkaç aşamaya bölünmüştür. Bunlar veri toplama, önişleme, özellik çıkarma, karşılaştırma ve performans değerlendirme kısımlarıdır [42].



Şekil (3-5) Genel imza doğrulama adımları.

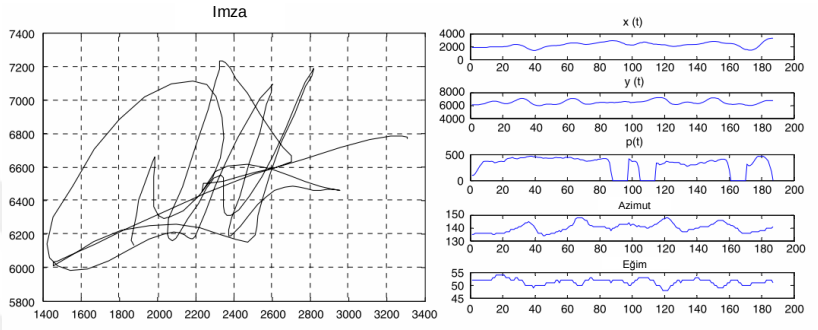
3.6.1 Veri Toplama

Veri toplama süreci çok önemlidir, çünkü sinyallerin kalitesi karşılaştırma sürecini optimize etmek için kritik önem taşır. Ayrıca, sinyallerin kalitesi iyi ise, önişleme ile ilişkili uygulama zamanı en aza indirilir, çünkü önişlemenin rolü bazen veri toplama sistemindeki arızaları düzeltmektir. Dinamik imza doğrulamasında, işlenebilen sinyallerin seçiminin önemi oldukça büyüktür (bir kalem ucunun x ve y koordinatlarının zamanı, hızı, hızlanması, basıncı vb.) [63].

3.6.1.1 İmza veri tabanı ve toplama işlemi

İmza doğrulaması, veri toplama işlemi ile başlar. Kalem tableti ve stylustan CPU'ya (Merkezi İşlem Birimine) aktarılan gerçek zamanlı imza girdilerinin okunması, işlenmesi ve imza veri tabanında depolanma işlemine Veri Toplama işlemi denir [7] [58]. El yazısı imza doğrulama sisteminin ilk adımı imzayı elde etmektir. Veri toplama süreci, bireylerin imzalarını toplayıp sistemin eğitimi ve kimlik doğrulama amacı sağlamaktadır. Veri Toplama işlemi, kullanıcının imzasını elde etmek için gereklidir ve sınıflandırma işlemi için farklı tiplerden oluşan girdi araçlarını kullanarak sinyalleri toplar, ayrıca imzanın gerçek zamanlı girdisi ile uğraşır. İmza doğrulama sisteminde, test amaçlı imza görüntülerini elde etmek için sayısallaştırıcı, dokunmatik ekran gibi özel girdi cihazları kullanark imza edinilir [61]. Online yaklaşımda imzanın dinamik

özelliklerini içeren daha fazla bilgi edinebiliriz. Vuruşların sayısı ve sırası, imzanın genel hızı, basınç noktaları, hızlanma ve imzanın statik özelliklerinin bilgilerini çıkarabiliriz. Bu, daha iyi doğruluk sağlar, çünkü dinamik özellikleri taklit etmek çok zor ancak sistem, kullanıcının işbirliği ve kompleks donanımı gerektiriyor. Sayısallaştırıcı tabletler veya basınca duyarlı tabletler, imzayı dinamik olarak taramak için kullanılır [56].



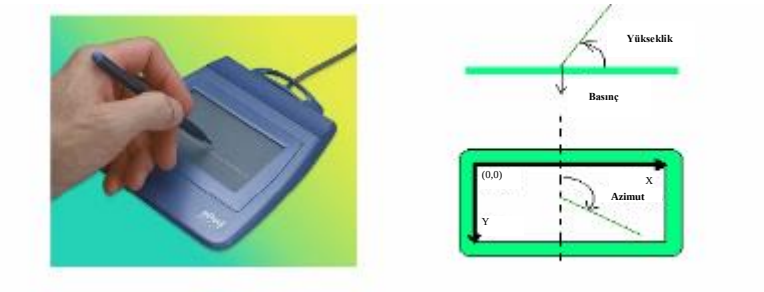
Şekil (3-6) İmza örneği ve dinamik bilgileri [28]

3.6.1.2 Online Sistemleri için Veri Toplama Cihazları

Dinamik doğrulama sistemindeki verileri elde etmek için, aşığada belirtilen imzanın dinamik bilgilerini yakalayan (imzalama sırasında) dijital tableti kullandık:

- Kalemin pozisyonu (x, y koordinatları): X-koordinatı, x ekseni boyunca ölçekli kürsör pozisyonu ve Y-koordinatı, y ekseni boyunca ölçekli kürsör pozisyonu.
- Basınç, (normal basıncın düzeltilmiş hali).
- Zaman damgası, (olayın gönderildiği sistem saati).
- Azimut açıları (0-360°), (uç açısına karşılık gelen kalem ucu azimutu).
- Yükseklik açısı (0-90°) her örnekleme periyoduna göre (uç yüksekliğine karşılık gelen kalemin farklı uçları).

Bu dinamik veri setini kullanarak hızlanma, hız, eğrilik yarıçapı, vb. gibi başka bilgiler de çıkarılabilir.



Şekil (3-7) Tipik Tablet Donanımı ve Verilerin Çıkarılması [6]

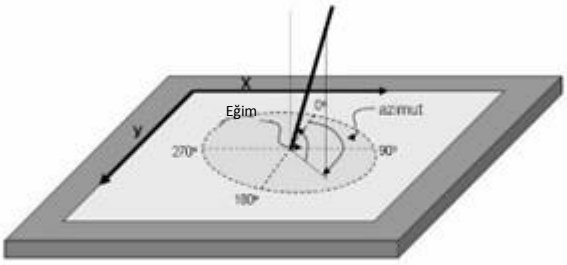
Online veri toplama cihazı pazarının geniş bir alanı tabletlerden (veya dokunmatik ekranlardan) oluşur. Kalem ile tablet arasında arabirimi sağlayan fiziksel cihaza sayısallaştırıcı denir. Kalemle yapılan hareketleri tanıyan ve tablet yüzeyine aktaran yüksek çözünürlüklü donanımıdır. Kalem tabletindeki sayısallaştırıcının temel amacı, kalemin pozisyonunu x ve y koordinat değerlerine çevirmektir. Piyasada birçok araştırma grubu tarafından online veri toplama işlemi için kullanılan başarılı ticari tabletler bulunmaktadır. Bilimsel makalelerde en sık Wacom tabletlerinden bahsedilir. Şekil (3-8)'de dijital tablet örnekleri gösterilmektedir.

Şekil (3-8) Wacom tabletleri [51].

Genel olarak dijital tabletler bilgisayara USB arabirimi üzerinden bağlanır. Tabletin hassas yüzeyi vardır ve bu yüzey stylus kaleminin hareketlerini yakalar ve bilgisayara aktarır (Şekil 3-9).

Şekil (3-9) Online İmza Taraması için bilgisayara bağlı Wacom tabletleri [51].

Tablet, x ve y pozisyonu, basınç gibi zamansal seri vektörleri iletir ve daha gelişmiş tabletler eğim ve azimut de içerir. İnç başına nokta (dpi) olarak adlandırılan alan çözünürlüğü 1000 ila 5000 dpi arasında değişir. Varsa, basınç tipik olarak 256 ila 2048 seviyeleri arasında değişir. Eğim ve azimut açılarının çözünürlüğü yaklaşık +/- 0.5º'tir. Bu sinyaller, uygulamaya bağlı olarak 50Hz ila 200Hz arasında değişen frekanslarda örneklenir. Daha yüksek örnekleme oranı ile daha yüksek çözünürlük elde edilir ve bu, hızlı vuruşları doğru bir şekilde ölçmesine neden olur, ters durumuda kaba çözünürlüktür [49]. Şekil (3-10)'da, imza girdi cihazı olarak kullanılan dijital tablet tarafından yakalanan, farklı sinyallerden oluşan bir grafik tanımlama sunulmuştur [70].



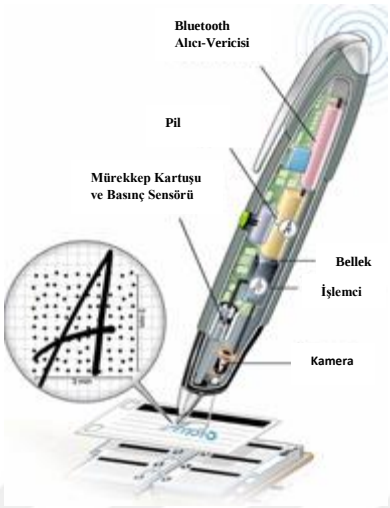
Şekil (3-10) Dijital tabletlerle elde edilen sinyaller

Bu cihazların imza girdi cihazları olarak endüstride kullanılması sürekli olarak artıyor, ve yeni üretim süreçleri, online imza doğrulama özelliklerine uyan tasarımlardan oluşuyor. Bu cihazlar kullanıcılar tarafından yaygın bir şekilde kabul gördü ve dahili ekranda kullanıcılara interaktif bilgi sunulur.

Dijital tabletler hâlâ en çok kullanılan imza girdi cihazları olmalarına rağmen, herhangi bir ek donanıma ihtiyaç duymadan, imza dinamiklerini yakalayabilen stylus kalem geliştirmeye yönelik bazı girişimler olmuştur. Örneğin, Biyometrik Akıllı Kalem (Biometric Smart Pen (BiSP)) [3], el yazısı kayıt ve analizi için kalem sistemidir, x ve y hareketlerini kaydeden optik sensörler, basıncı 3 yönde kaydeden basınç sensörleri ve açıları ölçmek için eğme sensörlerden oluşur, çizim ve işaret hareketleri ile bir kağıt defter üzerine veya boşlukta serbest hareketleri kaydeder. Bu stylus kalemi, düşük maliyetli, kullanıcı-dostu bir cihaz olup, hızlı online satın alma, keyfi defterler üzerine ve boşlukta el yazısını yakalayan ve düşük gücü olan cihazıdır [2] [52] [70].

Şekil (3-11) Biyometrik Akıllı Kalem - Pentrikler [52]

Dijital kalemler genellikle dijitalize tabletler gibi yazma ile ilgili ek bilgileri de yakalayabilirler. Kalemin takibi gerinim ölçerleri, manyeto elastik sensörler, rezonans frekansının kayması, lazer diyotları, kalemde yerleşik kamera ile küçük desenleri masa üzerinde takip etmek ve yazıyı filme kaydederek kalem hareketini izlemek aşamaları şeklinde gerçekleşir. Bazı dijital kalemler geleneksel mürekkep kalemi kullanır ve kağıda yazı yazmasına izin verir. Buda, kağıttan önemli dokunsal geribildirim sağlar. Şekil (3-12) bu cihazların kompozisyonlarını açıklamaktadır.



Şekil (3-12) Dijital kalem kompozisyonları [53]

Son birkaç yılda, yeni dokunmatik ekranlı cihazlar bir gerçeklik haline geldi. Bu cihazlar çok popüler olup teknoloji pazarının büyük bir bölümüne ulaştı. Bu ürünler (Şekil 3-13)'te görüldüğü gibi akıllı telefonlar, tablet-pc ve tabletlerdir. Bu cihazlar imzayı elde etmek için kullanılabilir.

a) Akıllı Telefon b) Tablet Bilgisayar c) Tablet

(Şekil 3-13) Bazı dokunmaya-duyarlı ekran cihazları

Bu yeni cihazlar, kayda değer geniş kapsamları nedeniyle, imza doğrulama sistemlerinin yakın geleceğinde önemli bir rol oynamaları bekleniyor.

3.6.2 Önişleme

Kullanıcılardan doğrudan toplanan veriler çoğunlukla eksik, gürültülü ve tutarsızdır, bu yüzden doğru sınıflandırmayı alabilmek için sisteme başvurmadan önce önişlemeden geçmeleri gerekir [49]. Genel olarak önişleme, veri toplama sürecinde ortaya çıkan gürültüyü ortadan kaldırmak, gereksiz örnekleri azaltmayı ve boyut,

pozisyonun vb. normalleştirmesini sağlar [5]. Önişleme aşaması hem eğitim hem de test aşamalarında uygulanır. Bu aşamanın amacı, imzayı standartlaştırılıp özellik çıkarımı için hazır hale getirmektir [76]. Veri donanımdan geldiğinde işlenmemiş haldedir ve örnekleme, niceleme, donanım hızı, imzalama pozisyonun vb. nedeniyle oluşan hataları normalleştirme için önişlemeden geçirilmesi gerekir [65].

Bir imza doğrulama sisteminin karşılaştığı güçlüklerden biri, aynı imza sahibinin farklı imzalarının açı, konum, genişlik ve hatta boyut bakımından farklı olabilmesidir. İmzaların şekillerini karşılaştırmak istendiğinde, bu bir soruna neden olabilir. Geniş kabul gören normal durum basitçe, imzayı standart boyut ve oryantasyona çevirmektir [57]. Genellikle, imza önişleme işleminin amacı, hem girdi imzadan (yakalama cihazından) hem de imzanın kendisinden gelen gürültüyü mümkün olduğunca azaltmaktır, çünkü bu gürültü doğrulama sürecini zorlaştıracak. Önişlemenin diğer amacı da sonradan doğrulama işlemini gerçekleştirmek için gerçek imzaya ulaşmaktır [45]. Sık kullanılan önişleme yaklaşımları; normalleştirme, düzleştirme ve yeniden örnekleme yöntemleridir.

3.6.2.1 Normalleştirme

Öncelikle tabletlerden elde edilen işlenmemiş veriler, imza boyutu ve yönü ile ilgili olmak üzere, normalleştirilmelidir [6].

1. Boyutu normalleştirme: Hepimizin bildiği gibi, bir kişinin imzası, bir kağıda ya da başka materyallerin üzerine imza attığı her sefer farklı olacaktır. Böylece, özellikleri çıkarmaya başlamadan önce her kişinin imzasını boyut olarak aynı kılmak için boyut normalizasyonuna ihtiyaç duyulmaktadır [7]. İki imza arasındaki boyut farkı önişleme ile ilgili problemlerden biridir [66]. Aynı şekle sahip iki imzanın farklı boyutlarla karşılaştırılması, benzerlik skorlarının düşük olmasına neden olur. Boyut normalizasyonu şekil (3-14)'te görüldüğü üzere bu etkinin ortadan kaldırılması için verilmiştir [68]. İmza boyutu, boyutlardan (genişlik veya yükseklik) birine göre normalize edilebilir, yükseklik bir resimdeki sütunun maksimum uzunluğudur ve benzer şekilde genişlik maksimum uzunluk sırasıdır [66]. İmzanın x ve y vuruşları, 2

boyut vektörünün [x, y] normalini kullanarak normalize edilir ve normalleştirme işlemi, aşağıdaki denklemi kullanarak, gerçekleştirilebilir;

$$x_i = \frac{x_i^o - x_{min}}{x_{max} - x_{min}} W$$

$$y_i = \frac{y_i^o - y_{min}}{y_{max} - y_{min}} W$$

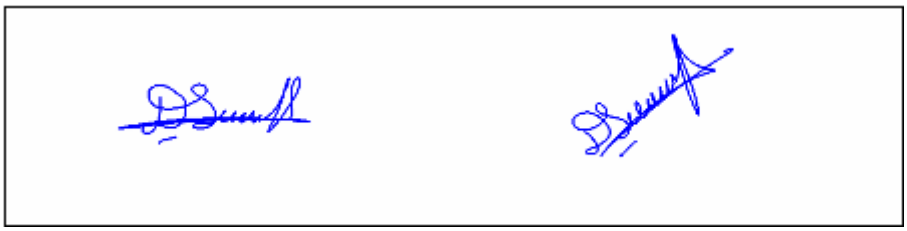
Burada $(x_i^o,\ y_i^o)$ orijinal noktayı, $(x_i,\ y_i)$ dönüştürmeden sonra karşılık gelen noktayı belirtir.

$$x_{min} = \min i\{x_i^o\}, x_{max} = \max i(x_i^o)$$

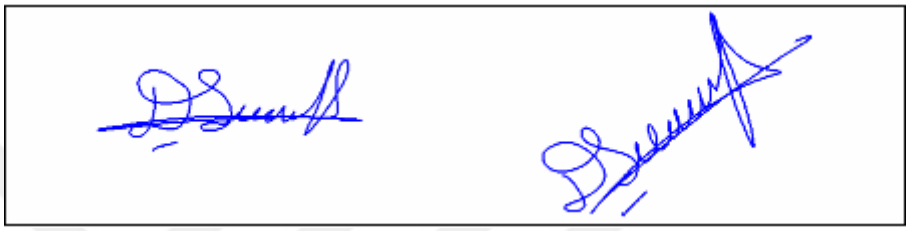
$$y_{min} = \min i\{y_i^o\}, y_{max} = \max i(y_i^o)$$

Burada W ve H normalleştirilmiş imza genişliği ve yüksekliğidir [7] [61] [64].

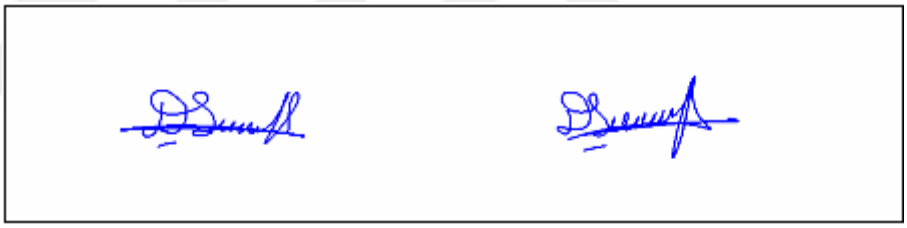
Yer normalleştirmesi: x-ekseninin ve y-ekseninin zamansal fonksiyonları, koordinatların orijinini merkezileştirerek imza kütlenin merkezinde belirli bir rotasyonla normalize edilir [64].



a. Orijinal imzalar



b. Boyutu normalleştirilmiş imzaları

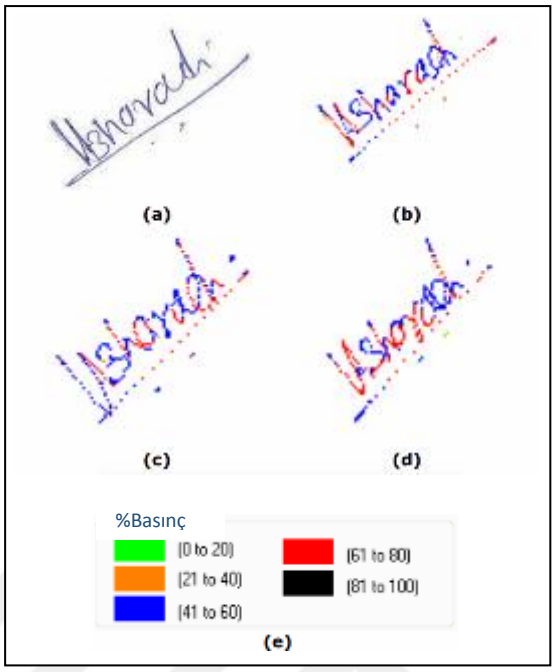


c. Döndürülmüş imzalar

Şekil (3-14) Normalleştirme örneği [12] [66].

3.6.2.2 Düzleştirme

Girdiyi almak için sayısallaştırıcı tabletin ve sayısallaştırıcı kalemin kullanılması nedeniyle, verilerin, kaldırılması gereken gürültülü noktaları vardır. Sayısallaştırıcının sayılı örnekleme oranı ve veri aktarım hızına sahip olduğu için, bir eğri üzerindeki tüm noktaları yakalayamaz, ancak örnekleme oranına göre sayılı noktaları yakalar. Bu da, şekil (3-15)'te gösterildiği gibi sonuç verir.



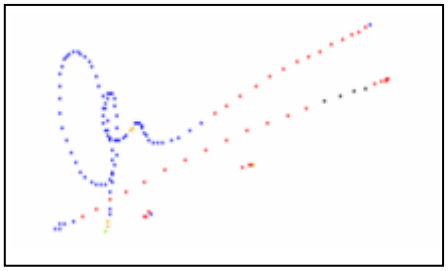
Şekil (3-15) Bir kişinin imza örnekleri

(a) Taranan Statik İmza,

(b),(c),(d) Taranan Dinamik İmza

(e) Gösterilen Dinamik İmzaların Basınç Seviyeleri [67].

Yakalanan noktalarda süreklilik kaybı söz konusudur; Şekil (3-15) (a)'da gösterildiği gibi statik taranmış bir imza var, şekil (3-15) (b), (c), (d)'de aynı kişinin dinamik imzaları gösterilyor, şekil (3-15) (e)'de gösterildiği gibi farklı renkler farklı basınç seviyelerini göstermektedir. Örneklenen noktalar açıkça görülebilir. Böyle bir durum Şekil (3-16)'da gösterilmektedir. Bu, girdi verisinde kesinlik kaybına neden olur ve eşleme algoritmasının doğruluk oranının azalmasına neden olabilir [67].



Şekil (3-16) Yüksek imzalama hızından dolayı, düşük örneklenmiş imza [67].

Bu sorunu çözmek için, eksik nokta bilgisini hesaplayan ve örnekleme hatasını azaltan bir yöntem önerilmiştir. Bu yöntem, yakalanan noktaları enterpole eder ve

komşu noktalardan büyük Öklid uzaklığını veya büyük hızını tanımlayarak, tutarlığını kaybetmeden, eksik bilgileri hesaplar. Düzleştirme işlemi, hareketli bir ortalama (moving average) ile veya ağırlıklı hareketli ortalamalara eşdeğeri olan çeşitli filtreleri kullanarak yapılabilir [62] [66] [67]. Bazı araştırmacılar imzayı düzleştirmek için Gauss filtresini tercih etti. Gauss filtresi sinyalin genel yapısını korurken, küçük dalgalanmaları yumuşatır.

3.6.2.3 Yeniden örneklemek

Yeniden örneklemek, girdi imzasını yeniden örneklemek için bazı araştırmacıların tarafından kullanılan bir süreçtir. Yeniden örneklemenin temel görevi, gereksiz imza noktalarını ortadan kaldırmaktır [61]. Bu, karşılaştırma işlemini hızlandırır ve zaman bağımlılığını kaldırarak şekle dayalı bir temsil elde etmeye yardımcı olur.

Yeniden örnekleme, işlenmemiş veri noktalarını aşağıda gösterildiği gibi basit bir doğrusal enterpolasyon algoritmasını kullanarak zamanda eşit mesafede düzenlenmeleri için yapılır. yeniden örnekleme adımı ΔS, toplam yay uzunluğunun (L) bir kısmıdır:

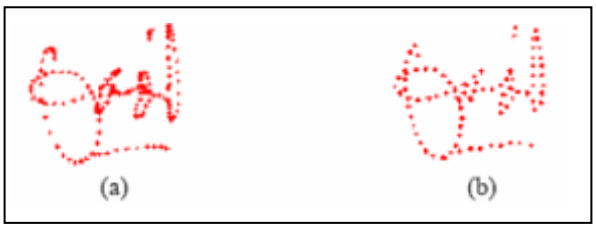
$$d_i = \sqrt{(x_i - x_{i+1})}\,2 + (y_i - y_{i+1})2$$

$$L = \sum_{i-1}^{n-1} d_i$$

$$\Delta S = \frac{L}{n_1}$$

Burada d_i, noktadan noktaya olan mesafeyi, n ise noktaların sayısını belirtir. Tekrar örneklemeden sonra karakterler, sabit bir boyut girdisi sağlayan, sabit karakter-başına-nokta sayısına (n_1) sahiptirler [7]. Bununla birlikte, yeniden örnekleme, önemli bilgi kaybına neden olur, çünkü görünüşte gereksiz veriler orijinal imzalayıcının hız karakteristiklerini içerir. Yeniden örneklemenin diğer sorunu, imzanın kritik noktalarının kaybolabilmesidir; bu sorunun çözümü bazen, yeniden örneklemeden sonra elde edilen eşit uzaklıktaki noktaların setine kritik noktaların ayrı olarak eklenmesidir. Yeniden

örneklememenin faydaları, hız için normalleştirmeme dezavantajından önemli ölçüde daha fazladır [74].



Şekil (3-17) a) Orijinal b) Örneklemeyi tekrarladıktan sonra

3.6.3 Özellik Çıkarma

İmza, pek çok günlük uygulamada kişisel ve belge kimlik doğrulaması için en yaygın kabul gören davranışsal biyometrik özelliğidir. İmza doğrulaması, banka çeklerinin, kredi kartı işlemlerinin, sözleşmelerin ve senetlerin geçerliliği gibi pek çok mali ve yasal işlemlerde kimlik doğrulama amaçlı geniş kabul görmesi nedeniyle aktif bir araştırma alanı olmuştur [69]. Bir imza doğrulama sisteminin etkinliği esas olarak Özellik çıkarma aşamasına bağlıdır. Özellik çıkarma teknikleri hızlı ve hesaplanması kolay olmalı, böylece sistemin hesaplama gücü düşük olur. Seçilen özellikler orijinal ve sahte imzaların arasında ayırım yapmalıdır. Edinme yöntemine bağlı olarak, imzayı doğrulayan iki özellik türü vardır. Statik özellikler, görüntü olarak kaydedilen imzalardan çıkarılır.

Dinamik özellikler ise gerçek zamanda atılan imzalardan çıkarılır. Örneğin, vuruşların sayısı, sırası ve uzunluğu, imzanın genel hızı, her noktadaki kalem basıncı, genişlik-yükseklik oranı, kesişme noktalarının sayısı, döngülerin sayısı, kanca sayısının vb. hakkında bilgi sağlar, bu da imzayı daha eşsiz kılar [77]. İmza doğrulama uygulamasında imzalar, daha sonra sınıflandırıcıya gönderilen, özellikleri çıkarmak için işlenir. Tipik olarak veriden, imzanın belirli karakteristiklerini tanımlayan, özellik vektörü çıkarılır, ve şablon olarak depolanır. Doğrulama işlemi sırasında, aynı özellikler test imzasından çıkarılır ve şablonla karşılaştırılır.

Bu adımda, gerçek kişinin imzasının benzersizliğini temsil etmek için en iyi şekilde kullanılabilecek özellikler çıkarılır. Bireyler arasında maksimum ayrım yapmayı sağlayan uygun özellikler seçilirken, alakasız özelliklerin atılması önemlidir [24].

3.6.3.1 Online İmzadan Çıkarılan Özellikler

Araştırmacılar tarafından, online imza doğrulaması için, çok sayıda özellik öne sürülmüştür. Dinamik özellikler, gerçek zamanlı atılan imzalardan çıkarılır. Bu özellik türleri, fonksiyon'a dayalı özellikler ve parametre'ye dayalı özellikler olmak üzere iki tür olarak ayrılabilir [24].

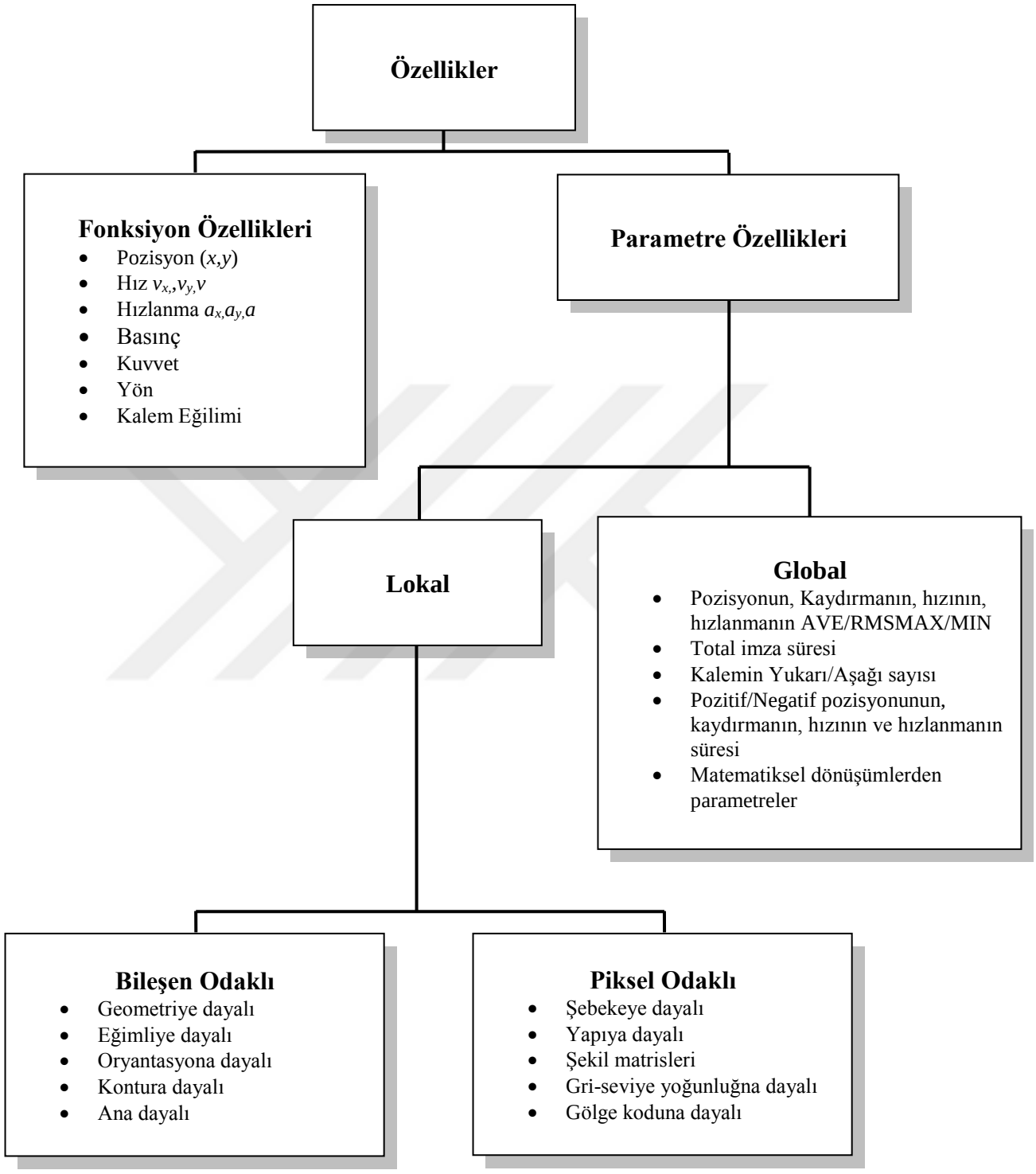
Fonksiyon'a dayalı özellikler, özellik kümesini oluşturan değerinin imzayı bir zaman fonksiyonu olarak tanımlar. Fonksiyon'a dayalı özelliklere örnek olarak pozisyon, basınç, hızlanma, eğim, hız ve kalem hareketinin yönü bulunur.

Parametre'ye dayalı özellikler, bir imzadan çıkarılan özellikler, öğelerden oluşan bir vektör oluşturur ve her biri bir özelliğin değerini temsil eder [24] [77]. Parametre'ye dayalı özelliklere örnekler; kalemin yukarı/aşağı sayıları, imzaların oryantasyonu ve Fourier, Kosinüs ve Wavelet matematiksel dönüşümleri uygulayarak hesaplanan çeşitli metodlardır [45]. Parametreler genellikle iki ana kategoriye ayrılır: lokal ve global.

Lokal özellikler, imza içindeki bir konuma denk gelen özelliklerdir, ve imzanın her noktası ile ilişkileri nedeniyle böyle adlandırılmıştır bunlar. Lokal özelliklerin örneği; vuruşun yükseklik-genişlik oranı, vuruş oryantasyonu, piksel yoğunluğu, imza yörüngesi üzerindeki ardışık noktaların arasındaki mesafe ve eğrilik değişimidir [72] [73]. Lokal parametreler, imzanın belirli bölümlerinden çıkarılan özelliklerle ilgilenirler. Çıkarılan özelliklere bağlı olarak, lokal parametreler **bileşen-odaklı** parametreler ve **piksel odaklı** parametrelere bölünebilir. **Bileşen-odaklı** parametreler her komponentin seviyesinde çıkarılır (yani, vuruşun yükseklik-genişlik oranı, vuruşların rölatif pozisyonları, vuruş oryantasyonu, vs.). **Piksel odaklı** parametreler de piksel seviyesinde çıkarılır (yani, şebeke-tabanlı bilgi, piksel yoğunluğu, gri-seviye yoğunluğu, yapı, vb.). Genellikle, lokal özellikler hesaplama açısından pahalıdır, ancak global özelliklerden daha kesindir. Genellikle global özellikler olarak kabul edilen bazı parametre özellikleri lokal olarak da uygulanabilir ve tersi de geçerlidir [77].

Global özellikler, total imzalama süresi, ortalama basınç, ortalama hız, sınırlayıcı kutu veya vuruş sayısı vb. gibi imza sürecinin ve imzanın tümüyle ilişkileri

nedeniyle böyle adlandırılmışlardır. Bir vuruş, kalemin kağıda dokunurken hareket ettiği noktaların sekansıdır. İmza genellikle birkaç vuruştan oluşur, ve önişleme sırasında tüm vuruşlar, bir uzun vuruş olarak birleştirilir [72] [73]. Global özellikler kolaylıkla çıkarılabilir, ancak imza hakkında sınırlı bilgi sunar [77].



Şekil (3-18) Özellik kategorileri.

Genel olarak: Fonksiyona dayalı özellikler, parametrelere göre daha iyi performans sağlarlar, ancak genellikle zaman alıcı eşleştirme prosedürleri gerektirirler. Parametreye dayalı özellikler, basit oldukları nedeniyle kolayca hesaplanırlar ve eşleştirilirler.

3.6.3.2 Online İmzalama da Sık Kullanılan Özellikler

Kısaca, en yaygın fonksiyon ve parametre özelliklerinden bazıları aşağıdaki gibi verilebilir:

- *Koordinat Sekansları x, y*: [*x; y*] Maksimum yatay ve dikey histogramı. Yatay histogramı imza görüntüsünün her satırından geçerek siyah piksellerin sayısını sayarak hesaplanır. Maksimum sayıda siyah piksel içeren bir satır maksimum yatay histogramı olarak kaydedilir. Benzer şekilde, dikey histogramı imza görüntüsünün her sütunundan geçerek, maksimum sayıda siyah piksel bulunan bir sütun bularak hesaplanır. Bu özelliklerin uzunlukları değişkendir. Genellikle, DTW elastik eşleştirmeye izin verdiği için, mesafe ölçümü olarak kullanılır.
- *İmza Süresi*: Kullanıcının toplam imzayı tamamlaması için gereken süre. Bu, kişi imzalarken kaydedilen koordinatların sayısını sayarak elde edilir. Her koordinat sabit bir oranda örneklenir.
- *İmza Genişliği*: Yatay ekseni boyunca her iki ucun arasındaki en kısa mesafedir.
- *İmza Yüksekliği*: Dikey ekseni boyunca her iki ucun arasındaki en kısa mesafedir.
- *Kalem-Yukarı Sayısı*: İmzalama süresi boyunca kalemin temas yüzeyinden kaldırma sayısıdır. Binary özelliğinin "0" olması, kalemin ekranı dokunmadığını gösterir (kalem-yukarı).
- *Kalem-Aşağı Sayısı*: İmzalama süresi boyunca kalemin temas yüzeyine indirme sayısıdır. Binary özelliğinin "1" olması, kalemin ekranı dokunduğunu gösterir (kalem-aşağı).
- *Total İmza Uzunluğu*: Eğriyi tek bir hat'ta dönüştürdüğümüzde ölçülen imzanın toplam mesafesi.

- *Basınç, Yükseklik, Azimut*: online imzalarda tipik bir dinamik özelliktir. Bazı sayısallaştırıcı cihazlar ek bilgi de yakalayabilir örneğin, azimut (kürsörun z ekseni etrafında saat yönünde döndürülmesi) ve yükseklik (pozitif z-eksene doğru, yukarıya doğru olan açı) gibi.
- *Kütlenin Merkezi x (l) ve y (l), Tork T (l), Eğrilik-elips s_1 (l) ve s_2 (l)*: Kütlenin Merkezi aslında düzleştirilmiş bir Gauss koordinat sekansıdır. Tork, kalem hareketi vektörü tarafından taranan alanı ölçer. s_1 *(l)* ve s_2 *(l)*: eğrilik elipslerini, anlara dayanarak, ölçer. İlişkili mesafe ölçüsü, noktaların tutarlılığı ile ağırlıklandırılan çapraz-korelasyon (Pearson's r)'dir. Kütlenin merkezi, imza görüntüsünü iki eşit parçaya böler ve tek tek parçaların kütle merkezini bulur.
- *Kalemin (Stylusun) hızı*: Bir yazarın tablet üzerindeki imzasını tuttuğu hızdır, *V x+* (*x*-ekseni üzerinde ortalama pozitif hız), *V y+* (*y*- ekseni üzerinde ortalama pozitif hız), Ts (total imzalama süresi). Hız sekansından, *Va* hızlanması daha da türetilebilir.
- *Cos (α), sin (α), Eğrilik α. β* : hız vektörü ve *x*-ekseni arasındaki açıdır.

Bu özellikler, online imza doğrulamasında kullanılan özelliklerin yalnızca küçük bir alt kümesidir [58] [75] [76].

#	Özellik	Mesafe Ölçümü
1	*X*-koordinatı: *X*	DTW
2	*Y* koordinatı: *Y*	DTW
3	Koordinatlar: [*X; Y*]	DTW
4	Hız: *V*	DTW
5	Hız *X: Vx*	DTW
6	Hız *Y: Vy*	DTW
7	Basınç: *P*	DTW
8	Hızlanma: *Va*	DTW
9	Yükseklik: *Al*	DTW
10	Azimut: *Zu*	DTW
11	Kütle Merkezi *X*: $x(\overline{l})$	Ağırlıklı *r*
12	Kütle Merkezi *Y* : $y(\overline{l})$	Ağırlıklı *r*
13	Tork: $T(l)$	Ağırlıklı *r*
14	Eğrilik-elips:$s_1(l)$	Ağırlıklı *r*
15	Eğrilik-elips: $s_2(l)$	Ağırlıklı *r*
16	Ortalama hız:$\overline{V}$	Öklid
17	Ortalama pozitif *Vx*: $\overline{V}x+$	Öklid
18	Ortalama pozitif *Vy*: $\overline{V}y+$	Öklid
19	Total imzalama süresi: *T s*	Öklid
20	Eğrilik: β	DTW
21	Açı: $\sin(\alpha)$	DTW
22	Açı: $\cos(\alpha)$	DTW

Tablo (3-3), Online imza doğrulamasında yaygın olarak kullanılan özellikleri ve karşılık gelen uzaklık ölçümlerini içermektedir [75].

3.6.3.3 Segmentasyon

İmza, bağlantısı kesilmiş segment kümesinden oluşuyor. Segment, birleşik noktalardan oluşan kümedir, kullanıcı yazmaya başladığında segment başlar ve kalemi cihazdan kaldırdığında sona erer [42]. Segmentasyon, imza doğrulama sisteminin ardışık aşamalarını da etkileyen önemli bir önişleme aşamasıdır. Bunun nedeni, segmentasyonun daha fazla özellik çıkarmaya yardımcı olması ve iki imzanın, tüm imzayı karşılaştırmak yerine sabit segmentlere dayalı olarak, karşılaştırılmasını kolaylaştırmasıdır. İmza segmentasyonu karmaşık bir görevdir, çünkü aynı imzalayıcı tarafından üretilen farklı imzalar, lokal germe, bastırma, ihmal veya ek parçalar nedeniyle birbirinden farklı olabilirler. Bu nedenle, imza segmentasyonuna özel önem verilmiştir ve çeşitli teknikler önerilmiştir. Tablo (3-4) imza segmentasyonu için en uygun tekniklerden bazılarını göstermektedir [34].

Segmentasyon Teknikleri	Kategori
Kalem-aşağı/Kalem-yukarı sinyalleri	Online
Hız sinyal analizi	Online
Algısal olarak bağıntılı noktalar	Online
Dinamik Zaman Çözgüsü	Online
Bağlı bileşenler	Offline
Ağaç Yapısı Analizi	Offline
Yönlü Veri İstatistikleri	Offline

Tablo (3-4) Segmentasyon Teknikleri

İmza bloklarına ulaşmak için en basit yaklaşım; imzaları yazı sekansları (kalem-aşağı) ve kesintiler (kalemle-yukarı) halinde düşünmektir. İleri teknikler aynı zamanda yazı hızını ve açılardaki değişiklikleri de hesaba katar [45]. İki veya daha fazla imzanın aynı sayıda mükemmel şekilde karşılık gelen segmentlere bölünmesini sağlamak için, imza segmentasyonunda yaygın olarak kullanılan dinamik zaman çözgüsü (DTW) kullanılır. Birinci imzanın bölünmesinden sonra, üniform mekansal ölçütlere veya geometrik uçların konumuna göre, DTW, diğer numunelerdeki ilgili noktaları belirlemek için uygulanır. Daha sağlam olan model-yönlendirmeli segmentasyon tekniği de öne sürülmüştür. Bu yöntem, aynı sayıda segmenti temin edip segment-segment eşleşmeyi

kolaylıkla sağlayan yöntemdir. Bu da, DTW'yu kullanarak referans modeldeki karşılık gelen segmentlere göre girdi imzayı segmentlere böler.

3.6.3.4 Özellik Seçimi

Son birkaç yılda imza sağlamlığını analiz etmek için özel ilgi gösterildi. Eğer bir kişi, imzasını "N" kere atarsa, yazı pozisyonları, kağıt, kalem, duruş şekli vb. aynı olsa bile, imzalar az yada çok ölçüde değiştiğini gözlemlendi. İmzaların analizi, imzaların neredeyse daima çok benzer/sabit oldukları alanları tanımlamaya amaçlar. Bu alanlardan seçilen özelliklerin hem offline hem de online doğrulama da çok iyi sonuçlar verdikleri gösterilmiştir [45].

Özellikleri seçerken göz önüne alınması gereken hususlar; orijinal imzalardaki özelliklerin değişkenlere duyarsız olmaları, ve gerçek ile sahte imzaların arasında iyi ayırtaç olmaları. Çünkü, hangi olası geniş spektrumlu özelliklerden, en iyi ayrımcı gücüye sahip olacağına dair önsel bilgi yoktur. Bir özellik kümesi, özellikleri budamak için gereken rehberlik yolu yoksa, çok sayıda gereksiz bilgi içerebilir.

Özellik seçimin amacı, esas olarak orijinal kümenin tüm ayrımcı gücünü içeren, azaltılmış bir özellik kümesi elde etmektir. Özellik seçimi, özelliğe dayalı doğrulama sisteminin gereksiz bilgileri kaldırarak etkinlik sağlanması, özellik vektörünün boyutunu azaltarak hız sağlanması, yalnızca optimum bir özellik kümesiyle çalışarak performans sağlanması yönlerini ele almaktadır. Genel olarak, özellik seçim tekniklerinin çoğu aynı temel prosedürü izler. Başlangıç noktası, analistin örnekler arasında ayrım yapmak için faydalı olduğuna inandığı, geniş bir özellik kümesidir. Özellik kombinasyonlarının veya özelliklerin her birinin ayırt edici gücü, popülasyonu yeterince temsil ettiğine inanılan bir veri eğitim setinde, istatistiksel testleri uygulayarak belirlenir. En iyi performansa (bazı kriterlere göre) sahip olan ve minimum sayıda özellik içeren özellik kombinasyonları, en iyi özellik kümesi olarak kabul edilmektedir. Ayrıca, en iyi özellik kümesinin farklı imzalayıcılar arasında aynı olmasına gerek yoktur [44]. Bu sistem için, imza yörüngesindeki noktaların aşağıdaki lokal özellikleriyle testler yapıldı: En düşük hata oranlarını veren iki ardışık noktaların (Δx, Δy) arasındaki x ve y koordinat farklılıkları. (Δx, Δy) özelliklerinin çeviriye göre değişmez olduğunu dikkati çeker [74].

İki ardışık nokta (Δp) arasındaki kalem basıncı (p) farkları. İki ardışık nokta (Δv) arasındaki hız farkları. Δy/Δx . Δp/Δx.

3.6.4 Karşılaştırma

Özellik çıkarma aşamasından sonraki aşama imza karşılaştırma aşamasıdır. Çıkarılan özellikleri, şablonda depolanan referans değerlerle karşılaştırır. İmza doğrulamasında sık kullanılan iki karşılaştırma metodolojisi: fonksiyonel yaklaşım ve parametrik yaklaşımdır. Fonksiyonel yaklaşımda, tamamlanmış sinyaller (x(t), y(t), v(t) vb.), özellik setini doğrudan veya dolaylı olarak oluşturur. Bir dizi örneklenmiş noktalardaki sinyal değerleri, test imza ve referans imzayı noktaya-nokta olarak karşılaştırılırlar. Parametrik yaklaşımda, yalnızca hesaplanan parametrik özellikler karşılaştırılır. Bu iki yaklaşımın yanı sıra, Rhee, segmentten-segmente karşılaştırmaya dayalı bir yaklaşım önerdi. Her segment için on bir parametre çıkarılıp karşılaştırıldı. Segmentasyonun daha fazla parametre çıkarmaya yardımcı olduğu ve karşılaştırma işleminin hala parametrelere dayandığı belirtilmelidir [6].

3.6.4.1 Fonksiyonel Yaklaşım

Fonksiyonel yaklaşım, tamamlanmış noktaları nokta-nokta olarak karşılaştırır. Tamamlanmış sinyal, mekansal bir fonksiyon örneğin: x, y eğrisi boyunca veya geçici bir fonksiyon olabilir örneğin: x, y zaman ekseni boyunca. İki sinyali karşılaştırmak için, basit bir yöntem olan, doğrusal korelasyon kullanılır, ancak aşağıdaki iki problem nedeniyle korelasyon katsayısının doğrudan hesaplanması geçerli değildir:

1. Toplam sinyal sürelerinin farkı
2. Sinyallerin içinde doğrusal-olmayan bozuklukların varlığı

Mekansal fonksiyonel sinyal veya geçici fonksiyonel sinyalde; sinyal süresinin, farklı numunelerin aynı imzalayıcıdan gelmiş olması bile, aynı olması muhtemel değildir. Buna ek olarak, her iki sinyal için de bozukluklar, doğrusal-olmayan bir şekilde sinyalin içinde ortaya çıkar. Bozukluğu düzeltmek için karşılaştırmadan önce doğrusal-olmayan bir hizalama uygulanması gerekir. Geçici bir sinyal için, en yaygın kullanılan yöntem Dinamik Zaman Çözgüsüdür (DTW). DTW'den sonra çözgülen sinyal, tanımlanmış bir çözgü yolunu izleyerek elde edilir. Çözgülenmiş sinyali ile referans

sinyalin arasındaki noktadan-noktaya Öklid uzaklığı hesaplanabilir. Çözgülenmiş sinyalinin yanı sıra, çözgü yolu da, sahte imzaları orijinal imzalardan ayırdetmek için önemli bir yöntem olarak kullanılabilir. İki lineer-korelasyon sinyallleri, doğrusal-eğri den oluşan bir çözgü yoluna sahip olacaktır. İki sinyal için daha az doğrusal-korelasyona sahipken, çözgü eğrisi daha az doğrusal olacaktır [6].

3.6.4.2 Parametrik Yaklaşım

İki parametre kümesini ayırt ederken, birisi gerçek bir imzadan diğeri sahte bir imzadan yola çıkarsak, Öklid uzaklığı en basit ve sıklıkla kullanılan ölçüdür. Öncelikle, birkaç prototip imzadan parametrelerin referans seti tanımlanır. Aynı parametre kümesi bir örnek imzadan çıkarıldıktan sonra, test örneğinin güvenilirliği referans setine olan Öklid uzaklığına dayanarak kararlaştırılabilir. Öklid uzaklığından başka, parametrik karşılaştırma için başka birkaç metodoloji vardır. Kiran, ortak bir 10 özellik kümesinden bir skoru hesaplamak için bir olasılıksal özellik modeli önerdi. Dolfing ise, parametrik yaklaşımda Soldan-Sağa Gizli Markov Modeli uyguladı. Ayrıca parametrik karşılaştırmaya Sinir Ağı Uygulaması önerilmektedir. Wijesoma, parametrik karşılaştırma için belirsiz bir mantığı benimsedi. Tüm bu çalışmalar [6] nolu referansta ayrıntılı verilmiştir.

3.6.5 Performans değerlendirmesi

Çoğu elle atılan imza doğrulama teknikleri, performans değerlendirmesi için aşağıdaki prosedürü kullanır:

1. Kayıt – Depolama veya kayıt sırasında her bir kişi için birkaç imza alınır (bu imzalara örnek imzaları denir, ancak eğitim imzaları gibi başka terimler de kullanılmıştır).
2. Önişleme ve Referans İmza(ları) Oluşturmak - örnek imzaları önişlemeden geçirilir, gerekli özellikleri hesaplanır ve bir veya daha fazla referans imzası üretilir. İmza doğrulama aşamasından önce hangi eşiğin kullanılacağına karar verilir.

3. Test İmzası - Kullanıcı kimliğini doğrulamak istediğinde, iddia ettiği kişinin kimlik bilgilerini sunar ve bir imza atar (bu imzaya, test imzası denilir). İkinci aşamada olduğu gibi imza önişlemeden geçirilir ve imza özellikleri hesaplanır.
4. Karşılaştırma İşlemi - Test imza, özelliklerin değerlerine göre, referans imza(lar) ile karşılaştırılır ve ikisinin arasındaki fark, var olan (veya özel olarak geliştirilmiş) birçok mesafe ölçüsünden birini kullanarak hesaplanır.
5. Performans Değerlendirmesi - Gerçek bir imza olduğunu iddia eden her imza için, 2. adımda belirlenen eşik, hesaplanan mesafe ile karşılaştırılır. Mesafe daha az ise imza kabul edilir, aksi halde reddedilir.
6. Bu kişi için verilen, gerçek imza seti ve sahte denemeleri için 3-5 adımları tekrarlanır ve 1-6 adımları yeni bir kişi için tekrarlanır; FRR, becerikli FAR ve rasgele FAR hesaplanır [38].

Özellikleri karşılaştırdıktan sonra, hata oranları sistem performansının göstergeleridir. Genellikle iki tür hata oranı kullanılır. Bunlar Yanlış Reddetme Oranı (FRR) ve Yanlış Kabul Etme Oranıdır (FAR) [26].

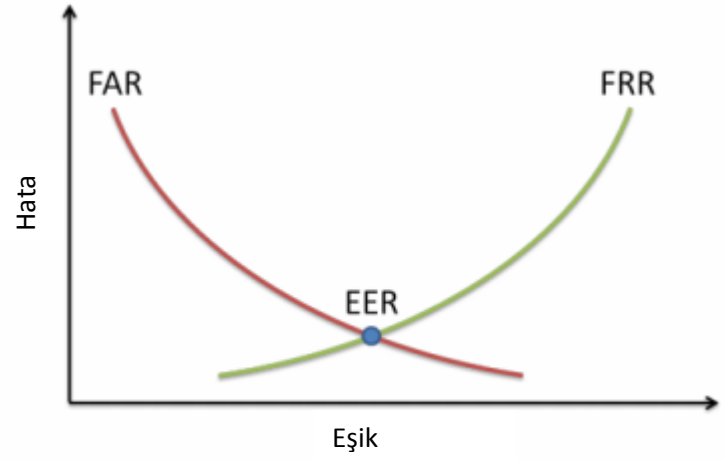
$$\text{FAR} = \frac{\text{Kabul edilen sahte imzaların sayısı}}{\text{Test edilen sahte imzaların sayısı}} * 100$$

$$\text{FRR} = \frac{\text{Reddedilen gerçek imzaların sayısı}}{\text{Test edilen gerçek imzaların sayısı}} * 100$$

Hem FAR hem de FRR birbiriyle ilişkilidir, böylece oranlardan birinde bir değişme olursa diğerine ters etki yapacaktır. İki eğri, eşik ayarlarına göre değişiklik gösterir. Sistemin performansını değerlendirmek için yaygın olarak kullanılan bir diğer alternatif, FAR = FRR'de oluşan Eşit Hata Oranını (EER) hesaplamaktır. Bu da diğer sistemlerle karşılaştırıldığında hata oranı performansının göstergesi olarak yaygın kullanılmaktadır. EER, FRR eğrisinin FAR eğrisiyle kesiştiği noktadır. Genel olarak, düşük EER'li sistemler daha iyidir.

En iyi EER'ı bulmak için bir iteratif yaklaşım yöntemini kullanabiliriz. Yöntem, doğrusal-olmayan programlama için simpleks algoritmasının bir uzantısına dayanır, bu

da kısıtlamasız ve kısıtlı optimizasyonu için yöntemi uygun hale getirir. Yöntemin birkaç uzantısı ile, lokal optima'dan kurtulabiliriz, ve birçok lokal optima ile doğrusal-olmayan fonksiyonların optimizasyonu için iyi bir araç haline getirmesine neden olur. Oldukça sağlam olduğu kanıtlanan bir strateji, doğru kurulumla lokal aramaya rasgele başlamak. Temel fikir; başlangıçta çok büyük bir simpleks kullanmaktır; Bu simpleksin başlangıç hareketleri çok büyük, ve bu nedenle bir tür filtre gibi davranırlar, ve aramayı iyi alanlara doğal olarak yönlendirir. Bu nedenle, objektif fonksiyon olarak, EER'ı en aza indirgemeyi seçebiliriz [42].



Şekil (3-19) FRR ve FAR'ın genel davranışı [42].

Daha yüksek eşik değeri ile sistem her şeyi kabul etme eğilimi gösterir, bu nedenle FRR düşük ve FAR yüksek olur. Eşiği azaltırsak, FRR artacak ve FAR düşecektir. Ancak eşik değeri çok düşük olursa, sistem kullanılamaz hale gelir, çünkü kabul edilmek çok zorlaşır. EER genellikle en iyi dengedir, fakat farklı türlü cevap vermemiz gereken bazı vakalara da rastlanabiliriz. Yüksek derecede güven içeren sonuçlara varmak istiyorsak, FAR ile çok kısıtlayıcı olmaliyiz ve sonuç olarak FRR yüksek olduğundan bir kullanıcının kabul edilmesi zorlaşır [42].

Bölüm 4

Karşılaştırma Algoritmaları

4.1 Giriş

Otomatik imza doğrulaması, hem bilimsel hem de ticari açıdan oldukça ilgi çeken bir araştırma alanıdır. Son yıllarda, internetin sürekli büyümesi ve gelişme içinde olması ve dolaysıyla artan güvenlik gereksinimleri ile birlikte, otomatik imza doğrulama alanına ilgi yoğunlaştırıldı.

Online el-yazısı edinimi için kullanımı kolay girdi aygıtları ortaya çıkmaları ve geliştirilmelerinden dolayı, online imza doğrulaması için olası uygulama sayısı sürekli artmaktadır. Örneğin, otomatik imza doğrulaması; bilgisayar ağları, belgeler ve veritabanlarında erişim güvenliğini kontrol etmekte etkin katkı sağlayabilir. Mesela, doğrulama işlemi gerçekleştirilmesi için, bir kullanıcının canlı online imzası, kişisel akıllı kartta depolanabilen el-yazısı imzasını içeren biyometrik bilgileri ile karşılaştıralarak, kartı kullanan kişinin hak sahibi olup olmadığı doğrulanabilir.

Bu bölümde, otomatik imza doğrulamasına uygulanan çeşitli modelleme yaklaşımları özetlenmektedir.

Modelleme tekniğinin uygulanabilirliği ve gerçek imzalayacıları ve sahtecileri (forgers) tanıyabilme becerisi, bir doğrulama sisteminin kalitesinde en önemli faktördür [44]. Global özelliklere dayalı sistemler de kullanılan en yaygın algoritmalar, istatistiksel sınıflandırıcılara dayanmaktadır, Gauss Karışım Modelleri (Gaussian Mixture Models - GMM) veya Mahalanobis mesafesi (Mahalanobis distance) gibi, buna karşın fonksiyona dayalı sistemler de Dinamik Zaman Çözgüsü (DTW), Gizli Markov Modelleri (Hidden Markov Models - HMM), Nöral ağları (Neural Networks - NN) ve Destek Vektör Makineleridir (Support Vector Machines - SVM). DTW, kullanıcı modellerinin önceki eğitimine ihtiyaç duymaması avantajına sahiptir [14].

İmza örneği iddia edilen kimliğe ait olup olmadığı karar vermek için kullanılan imza karşılaştırma algoritmaları, genellikle iki ana gruba ayrılır. Bunlar; mesafeye dayalı yaklaşım ve modele dayalı yaklaşımdır [70].

4.2 Dinamik Zaman Çözgüsü (DTW)

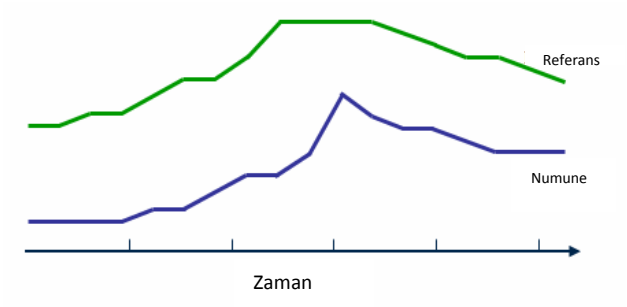
Özellik çıkarma işleminden sonra, bir sonraki adım doğrulama yapmaktır, yani, sorgulanmış bir imza iddia eden kişiye ait olup olmadığını saptamak. Online doğrulama durumunda, en yaygın yaklaşımlar Dinamik Zaman Çözgüsüne (DTW) dayanır. DTW, belirli bir mesafe ölçüsünün minimumunu elde etmek için, imza sinyal sekanslarının zaman ekseninin genişletilmesi ve kompresyonuna izin verir, bu da online doğrulaması için uygun hale getirir. Parametreler özellik olarak kullanıldığında, doğrulama için sıklıkla Mahalanobis ve Öklid gibi uzaklik ölçüleri kullanılır. Gerçek durumlarda, bir doğrulama sistemi yalnızca orijinal numunelere ve bir veya daha fazla sorgulanmış imzaya sahip olabilir [45].

Dinamik Zaman Çözgüsü (DTW), iki zamansal sekansları, kullanıcının referans imzası ve sorgulanmış imzanın arasındaki hizalamayı belirlemek için kullanılan iyi bilinen bir tekniktir. DTW geniş uygulama alanlarında kullanılır ve herhangi doğrusal sekansı olarak gösterilebilen bir veriye uygulanabilir.

Dinamik Zaman Çözgüsü (DTW) iki zamansal sekansların (sorgu ve şablon) arasındaki hizalamayı hesaplamak için kullanılan bir algoritmadır. İki zaman serisi arasındaki karşılık gelen bölgelerin bulunması, ya da iki zaman serisi arasındaki benzerliği saptamak için kullanılır. Mümkün olduğunca birbirine benzetmek için, bu iki zaman serisi, gerdirerek doğrusal olmayan şekilde veya zaman ekseni boyunca lokal olarak kompresyon uygulayarak çözgülenebilir.

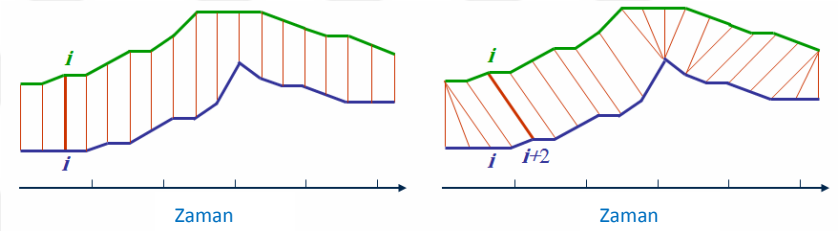
DTW aşağıdaki özelliklere sahiptir:

1. Sekans noktaları üzerinde bir-birdençok haritalama.
2. Sekansların eşit uzunlukta olması gerekli değildir.
3. Gürültüye karşı tolerans göstermesi; iki sekansların küçük bir kısmı önemli ölçüde farklı olsa bile benzer olabilmesi [8].



Şekil (4-1) İki zaman serileri [27]

Germe sonrası, bireysel hizalanmış öğelerin mesafelerini toplamasıyla, iki serinin arasındaki mesafe hesaplanır.



A **B**

Şekil (4-2) A. İki zaman serisi arasındaki Öklid uzaklığı

B. İki zaman serisi arasındaki DTW mesafesi

B'de zaman ekseni çözgülenmiş olup böylece örnek sekanlardaki her veri noktası referans sekanslardaki bir noktaya optimal şekilde hizalanır.

DTW 1960'lı yıllarda tanıtıldı ve 1970'lerde konuşma tanıma çatısı altında da keşfedildiğinde popülaritesi daha da arttı. Daha sonra, DTW'de düzelmeler yapıldı ve farklı alanların birçok bilgisayar uygulamalarında yaygın şekilde kullanıldı. Bunların örneği; imza eşleştirmesi, hareket tanıma, veri madenciliği, bilgisayar görüntüsü, gözetim, kimya mühendisliği, protein sekans hizalaması, insan hareketi tanıma ve kelime tanıma gibi alanlardır [36] [55]. Bu tez çalışmasında bir DTW algoritması uygulandı ve sonraki bölümde ayrıntılı olarak da açıklandı. Vurgulamaya değerki, DTW ye dayalı algoritmaları, iki kamu değerlendirme yarışmasında İDY'2004 ve BSEC'2009'da kazanan imza sistemleri idi [70].

4.2.1 Klasik DTW Algoritması

Sırasıyla n ve m uzunluğundaki X ve Y zaman serilerinin karşılaştırılmasında, burda

$$X = x_1, x_2, x_3, x_4, x_5, \ldots, x_n \quad (1)$$

$$Y = y_1, y_2, y_3, y_4, y_5, \ldots, y_m \quad (2)$$

Klasik DTW, iki zaman serisi arasındaki hizayı bulmak için dinamik programlama yaklaşımını kullanır ve minimize mesafeye dayanan zaman serilerini hizalandırır. İki zaman serisi arasındaki DTW hizalamasını hesaplamanın ilk adımı; n-ile-m kost matrisini (cost matrix) oluşturmaktır, burada her bir (i^{th}, j^{th}) öğesi, x_i ve y_i arasındaki ölçülen mesafeye karşılık gelir. Mesafe, farklı mesafe metriklerini kullanarak ölçülebilir örneğin, basit Manhattan farkı $d(x_i, y_i) = |x_i - y_i|$, Kare mesafe $d(x_i, y_i) = (x_i - y_i)^2$ veya Öklid uzaklığı veya zaman serileri arasındaki hizayı tanımlayan başka herhangi bir mesafe ölçüsü. Kost matrisindeki her bir yol için kümülatif mesafeye dayanarak, zaman serileri arasında en iyi eşleşme, Öklid uzaklığı ile bulunabilir. Ayrıca DTW'de mesafe hesaplaması için en yaygın kullanılan yöntemlerden birisidir. Aşağıdaki (3) numaralı denklemde gösterildiği gibi:

$$DTW(X,Y) = \min \{ \sum^{k}_{k=1} d(w_k) \} \quad (3)$$

Burada, d iki zaman serisi arasındaki seçilen mesafe ölçüsü, ve w_k, çözgü yolunun W, k^{th} öğesinin Kost matrisi öğesidir, denklem 4'te gösterildiği gibi:

$$W = w_1, w_2, w_3, w_4, w_5, \ldots .w_k \quad (4)$$

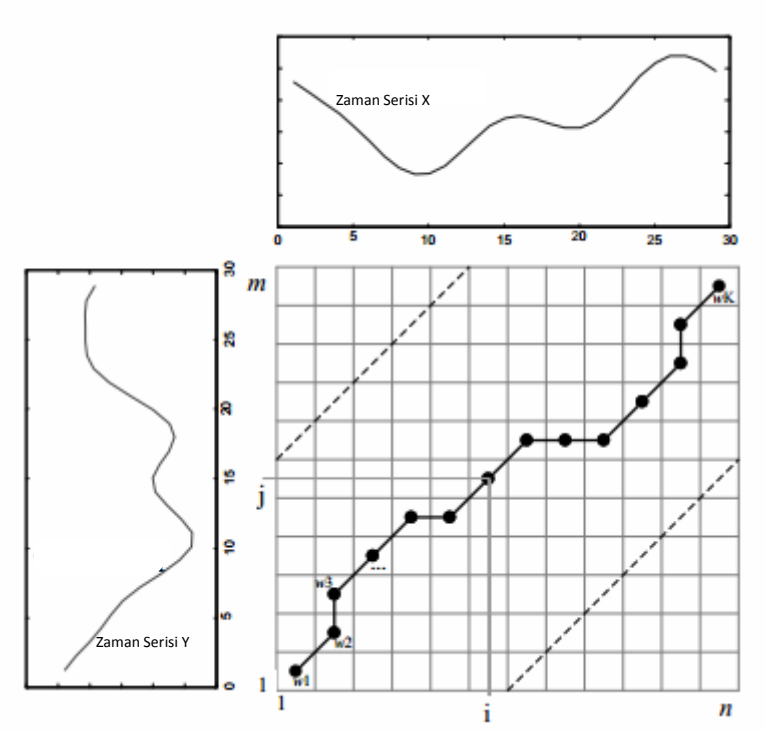
Çözgü yolu, dinamik programlama formülasyonunu (basamak desenleri, lokal kısıtlamalar olarak da bilinir) kullanarak bulunabilir, bu da D (i, j) hücresini doldurmak için, kost matrisindeki komşu hücrelerin katkısını belirler. Dinamik Programlama formülasyonu, komşu çapraz noktaların kümülatif uzaklıklarının minimumu ile mesafenin toplamını alarak, her nokta için toplam mesafeyi verir. Ilk olarak, matrisin ilk sütununu ve birinci satırını doldurarak global kost matrisini D doldurur, böylece D (0, 0) = 0 başlatılıyor, denklem 5, 6 ve 7'de gösterildiği gibi.

$$D(i, 1) = D(i-1, 1) + d(i, 1) \quad (5)$$

$$D(1, j) = D(1, j-1) + d(1, j) \quad (6)$$

$$D(i, j) = d(i, j) + \min [D(i-1, j), (i-1, j-1), (i, j-1)] \quad (7)$$

Global kost matrisi biriken mesafelerle doldurulduğunda, sonraki adım, kost matrisini kullanarak zaman serilerinin arasındaki çözgü yolunu bulmaktır. Kost matrisini geri çekerek, çözgü yolu greedy yaklaşımın yardımıyla kolayca bulunabilir. Algoritma teorisinde, greedy yaklaşım olduğu pozisyonda lokal optimal kararları verir, ve sonunda global optimal vereceğini varsayar. Çözgü yolu araştırması D (n, m)'den başlar ve komşu hücrelerin hepsini soldan, aşağıdan, çaprazdan, sol alta kadar değerlendirerek geri çeker. Bu komşu hücrelerden herhangi biri minimum değerleri içeriyorsa, D (1,1)'e ulaşana kadar çözgü yolunun başına ekler [15] [36] [39].

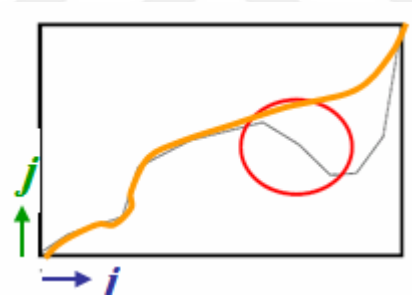


Şekil (4-3): Çözgü yolu [29].

4.2.2 Kısıtlamalar

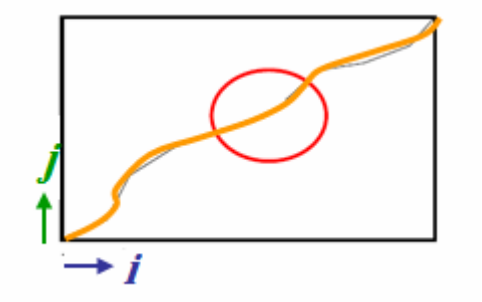
Olası tüm çözgü yollardan en uygun çözgü yolunu bulmak için, DTW algoritmasını çalıştırırken, birkaç kısıtlama sağlanmalıdır. Kısıtlamalar sadece çözgü yolu için arama alanını azaltmakla kalmaz aynı zamanda algoritmanın performansını da arttırır. Kısıtlamalar lokal ve global olmak üzere iki kategoriye ayrılabilir. Lokal yolda bir adım atıldığında, lokal kısıtlamalar eğim ile ilgilenir; dolayısıyla doğru yolu hesaplamaya katkıda bulunur. Kısıtlamalar aşağıdaki gibi tanımlanmıştır [27]:

- Monotonluk Kısıtlaması: Hizalama yolu "zaman" indeksinde geri dönmez. Çözgü yolunun noktaları, artan eğilimi olmalıdır. Belirtmek gerekir ki, bir çözgü yolu zaman da azalamaz; düz olabilir veya artabilir. $I_{k-1} \leq i_k$ ve $j_{k-1} \leq j_k$. Hizalamada özelliklerin tekrar edilmediğini garanti eder.



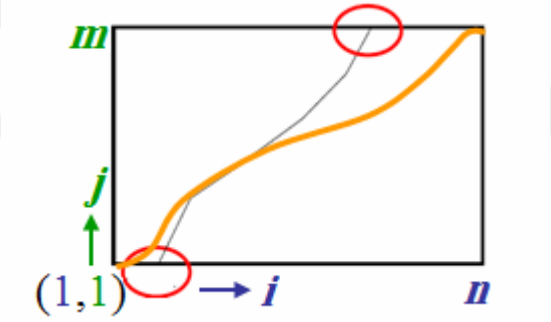
Şekil (4-4) Monotonluk Kısıtlaması [27]

- Süreklilik Kısıtlaması: Süreklilik kısıtlaması, geçerli bir çözgü yolu aralıksız olmasından emin olur. Hizalama yolu "zaman" indeksinde atlamaz. $I_k - i_{k-1} \leq 1$ ve $j_k - j_{k-1} \leq 1$ Kost matrisindeki herhangi bir noktanın önceki noktası(i_k-1, j_k),(i_k, j_k-1),(i_k-1, , j_k-1) olmalıdır. Hizalamanın önemli özellikleri atlamadığını garanti eder.



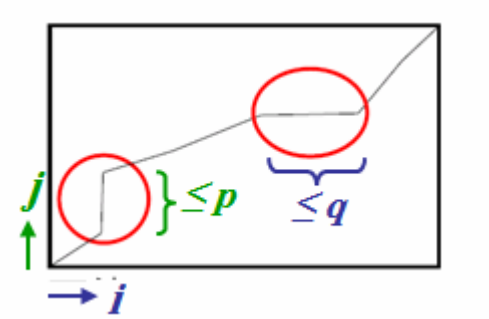
Şekil (4-5) Süreklilik Kısıtlaması [27]

- Sınır Kısıtlaması: Hizalama yolu sol alt köşede başlar ve sağ üst köşede biter. $i_1 = 1$, $i_k = n$ ve $j_1 = 1$, $jk = m$. Çözgü noktasının ilk noktası $w_1 = (1, 1)$ ve son noktası $w_k = (n, m)$ olması gerektiğini belirtir, burada n, m sırasıyla sorgunun uzunluğunu ve şablon zaman serisini temsil eder. Hizalamanın sekansın bir kısmını dikkate almadığını garanti eder



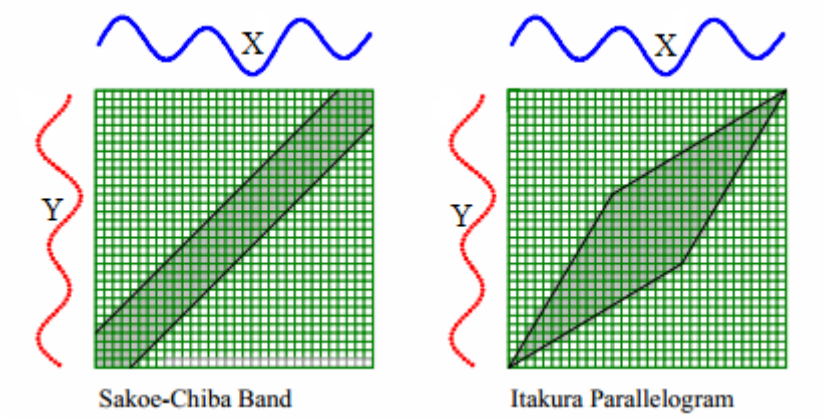
Şekil (4-6) Sınır Kısıtlaması [27]

- Eğim Kısıtlaması: Hizalama yolu çok dik veya çok sığ olmamalıdır. $(j_{kp} - j_{k0}) / (i_{kp} - i_{k0}) \leq p$ ve $(i_{kq} - i_{k0}) / (j_{kq} - j_{k0}) \leq q$, burada $\boldsymbol{q} \geq 0$, $\boldsymbol{x}$-yönündeki adım sayısıdır ve $\boldsymbol{p} \geq 0$, $\boldsymbol{y}$-yönündeki adım sayısıdır. $\boldsymbol{q}$, $\boldsymbol{x}$'e girdiktien sonra, biri $\boldsymbol{y}$'ye girmesi gerekiyor ve tersi: $S = p / q \in [0,\infty]$. Hizalama yolu çok dik veya çok sığ olmamalıdır. sekansların çok kısa parçalarının çok uzun parçalarla eşleştirilmelerine önler.



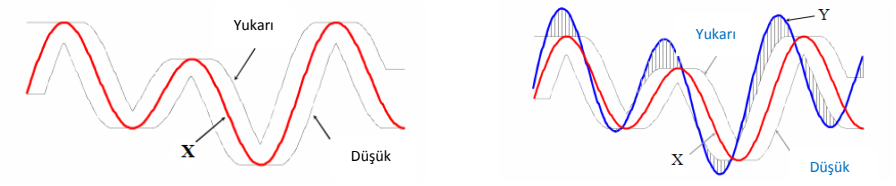
Şekil (4-7) Eğim Kısıtlaması [27]

- Çözgü Pencerisi: Global kısıtlamalar, çözgü yolu için arama alanını azaltır ve DTW algoritmasının çalışma süresini 0 (nm)'den 0 (nk)'ye yükseltir, burada *k* pencere boyutudur. Global kısıtlamalar yalnızca çözgü penceresine giren, kost matrisinden gelen noktalara izin verir $|i_k - j_k| \leq \omega$, burada ω, pencerenin genişliğini temsil eden pozitif tamsayıdır. Bu yaklaşım, bir singularitinin maksimum boyutunu sınırlar, ancak meydana gelmelerine engellemez [29]. Lokal kısıtlamalar doğru çözgü yolunu bulmaya katkıda bulunurken, global kısıtlamalar (pencerelemek/bant) hesaplama sürecini hızlandırır, kost matrisindeki hücre sayısının geçişini sınırlandırarak. Kost matrisindeki hücrelerin hesaplanmasını sınırlamak için kullanılan, n=m durumunda uygun global kısıtlamalardan biri olan Sakoe-Chiba grubudur, bunlar en basit ve en sık kullanılan bantlardır. Ayrıca Itakura paralelogram, en yaygın global kısıtlamalardan biridir, konuşma topluluğunda yaygın olarak kullanılmaktadır, ancak SCband'ı kadar basit değildir [36].



Şekil (4-8): Sakoe-Chiba Band ve Itakura Parallelogram, en yaygın iki kısıtlama'dır [39].

DTW hesaplamasını hızlandıran, DTW'ye yeni eklenen bir uzantı, çözgü penceresini kullanarak, sorgu sekansının üstünde ve altında sınırlayıcı bir zarf oluşturma için bir alt sınırlama tekniğidir. Ardından mesafelerin kare toplamı, sınırlayıcı zarfta olmayan aday sekansının her bölümünden, sınırlayıcı zarfın en yakın ortogonal kenarına kadar, alt sınırı olarak iade edilir.



A B

Şekil (4-9): A. Bir sorgu sekansının X etrafında
B. DTW mesafeleri için alt sınır [15].

4.3 Gizli Markov Modelleri (Hidden Markov Models - HMM)

Patern analizi için en yaygın kullanılan istatistiksel model HMM'dir. HMM tekniği, girdi sinyallerinin, Markov süreçleri olarak bilinen yaklaşım, parametrik rasgele süreç olarak tanımlanabileceğini varsayar. Birçok araştırmacı (Camino et al., 1999,

Wessels and Omlin, 2000, Ferrer et al., 2005; Igarza et al., 2003; Muramatsu and Matsumoto, 2003; Zou et al., 2003), önerdikleri imza doğrulama sistemi için HMM'yi bir sınıflandırıcı olarak dahil ettiler [24].

Bir dizi rasgele fonksiyonların her birinin bir durumla ilişkili olduğu ve sınırlı sayıda durumla altta yatan bir Markov zinciri tarafından yönetilen bu yöntem çift stokastik bir süreçtir. Ayrı anlarda, süreç durumların birindedir ve mevcut duruma karşılık gelen rasgele fonksiyona göre bir gözlem sembolü üretir.

Model, görülebilen her şeyin gözlem sekansı olması bakımından gizlidir. Her sembolü oluşturan altta yatan durum gizlidir [42]. Algoritmanın üzerindeki imzalama zamanın değişiklikleri etkisini azaltmak için, hesaplanan olasılıklar, örnek noktalarının sayısına bölünür. Bir test imzası için olasılık ile eğitim seti için ortalama olasılığın arasındaki fark, imza orijinalliğini belirlemek için bir hata ölçütü olarak kullanılır.

Bir sonuca ulaşmak için global ve lokal hatalar, bir Öklid mesafesi ölçüsü kullanarak birleştirilir. Sonuçlar, global ve lokal özelliklerin kombine kullanımının performansı, iki parçanın kendi başlarından daha iyi performans sergilediğini gösterir [44].

Temel HMM teorisi Baum tarafından tanıtıldı. İlk ve ana yayınlanmış eserlerden biri olan, HMM'yi imza doğrulamasına uygulamak, Dolfing tarafından sunuldu. 1995'de L. Yang ve ortak çalışanları farklı HMM topolojilerini test ettiler, böylece imza karakteristikleri için en iyi yaklaşımın soldan sağa topoloji olduğunu göstermiş oldular [70].

4.4 Gauss'un Karışım Modeli (Gaussian Mixture Model - GMM)

Bu yöntem istatistiksel bir yöntemdir. Birkaç yazar, bu tekniği yalnızca bir durumu içeren HMM'nin dejenere hali olarak görür. Jonas Richiardi ve Andrzej Drygajlo, GMM'yi 2003'te online imza doğrulaması için kullanan ilk yazarlar'dı. O zamandan beri, farklı yazarlar imza doğrulama sistemlerdeki kullanışını araştırdı [70].

GMM, online imza doğrulama'da uygulanmış olsa da, yapılan araştırmalar diğer teknikler kadar geniş değildir, HMM ve DTW'de olduğu gibi. Gauss'un Karışım Modelleri (GMM), patern tanıma işlemi için çok iyi bilinen ve çok tercih edilen bir

tekniktir. Eğitiminden sonra ortaya çıkan Beklenti-Maksimizasyon algoritmasının görünümü, bu tekniğin patern tanıma görevleri için uygun bir alternatif olduğunu göstermiştir [70].

4.5 Destek Vektör Makineleri (Support Vector Machines - SVM)

SVM yeni bir sınıflandırma tekniğidir ve istatistiksel öğrenme teorisi alanının bir parçasını oluşturur, ayrıca patern tanıma uygulamaları için başarıyla uygulanmıştır. İmza doğrulamasına da uygulanmıştır [70]. Bu yöntem, patern tanıma ve regresyon problemleri için bir tür öğrenme makinesidir ve çözümünü eğitim verisinin bir alt kümesi olan, Destek Vektörü, açısından kurar. Yöntem çok iyi sonuçlar verdiğinden, çeşitli patern tanıma problemlerinde popülerdir [42].

Seyrek veri probleminin bir kısmını ve görünmeyen verilerin genellemesini çözmeye çalışan Destek vektörleri, Vapnik tarafından geliştirildi. Birinci problem genellikle gerçek hayattaki uygulamalarda ortaya çıkar, veri yüksek boyutlu ve birçok özelliğe sahip olduğunda. Buna göre, sınıflandırma görevini çok iyi temsil etmek için genellikle yeterli veri yoktur. Bunun nedeni, tüm makine öğrenme uygulamalarının kesinlikle kötü örneklenmiş (yani problem alanının eşit dağılımından değil) deneysel veriler üzerinde çalışmalarıdır. Bu, eğitim setini yamuk hale getirir ve sistemin performansı buna göre indirgenir.

Bir diğer sorun ise, verinin seyrek olmasıdır. Bu durumda sistemin genelleştirmesini beklemek pek olası değildir. Destek vektör makinelerinde (SVM) bu problemler, bir dereceye kadar, aynı zamanda çözülüyor. Yapay sinir ağlarında olduğu gibi, hangi sınıfa yeni bir veri örneği sınıflandırılacağını seçmek ve sert bir sınırın inşaatı için tüm verileri kullanmaya çalışmak yerine, SVM eldeki görevi en iyi temsil eden verileri seçer. Bu veri örneklerine destek vektörleri denir, ve bunları karar sınırını oluşturmak için kullanır. Bu yaklaşımın avantajı ise, sistemin sınırını, konumunu ve yönünü bozacak şekilde uç değerlere karşı hassas olmamasıdır.

Eldeki verilere göre, oluşturulan sistem elde edilebilecek en iyi sistemdir ve optimal bir karar sınırını oluşturur. Burada optimal, yanlış sınıflandırmalar olmadığı durum olarak tanımlanır; ya da hiç yanlış sınıflandırmanın olmaması imkansız ise, en az

miktarda olması, ve hiper düzleme en yakın destek vektörlerinin maksimumda olmaları halidir (veya ona en yakın mesafe) [44].

4.6 Yapay Sinir Ağları (Artificial Neural Networks - ANN)

Yapay sinir ağları (ANN) günümüzde çok çeşitli uygulamalarda kullanılmaktadır. Bunların bazıları; borsa tahmini, tıbbi teşhis, sismik olay tahmini, konuşma tanıması ve yapay görme gibi alanları içerir. Bu yöntem, makine öğrenmesinde kullanılan istatistiksel bir yöntemdir, ve biyolojik (beyin) sinir ağlarından esinlenerek oluşturulmuş olup büyük girdileri olan fonksiyonları tahmin etmek için kullanılır ve bu fonksiyonlar genellikle bilinmemektedir.

Yapay sinir ağları genellikle, değerleri girdiden hesaplayabilen, birbirine bağlı nöron sistemlerinden oluşmaktadır. ANN'ler, eğitim örneklerinden öğrenebilir ve bilgileri sıkıştırma yeteneğine sahiptirler. Kompresyon önemlidir, çünkü modelin bir kredi kartı manyetik şeritte depolanması gerektiğinden, çalışma 80 byte sınırıyla kısıtlanmalıdır. İmza, enterpolasyonla sabit nokta sayısına göre yeniden örneklenir. Bu şekilde yeniden örneklenmiş iki imza, zaman gecikmeli nöral ağı paradigmasına dayalı olarak iki alt ağa sunulur. İki alt ağı çıktı katmanında birleştirilir ve amaç, alt ağları tarafından çıkarılan iki özellik vektörlerinin kosinüs mesafesini en aza indirgemektir [44].

El yazısı tanımada kullanmasının bir başka örneği, giriş görüntüsünün pikselleri tarafından aktive edilen nöronlardır. Daha sonra ağ ağırlaştırılır ve bir fonksiyonla dönüştürülür ve aktivasyonlar diğer nöronlara geçirilir. Bu işlem çıktı nöronu aktive edilene kadar tekrarlanır. Nöral ağlarının örnekleri: Bayesian, zaman geciktirme ve geri yayılım ağlarıdır [42]. ANN'yi kullanmanın en büyük avantajı, ağın parametrik olmayan niteliğidir ve bir kullanıcı için profesyonel olmayan bir kullanıcı tarafından yeniden konfigüre edilme uygunluğudur. Bu, sınıflandırma için daha basit araçlardan biri olmasına sağlar, ancak ANN'yi eğitmek için yeterli miktarda veri sağlanması gereklidir [24].

4.7 İmza modellemesi için Fourier dönüşümleri

Fourier dönüşümü muhtemelen günümüzde sinyal işleme uygulamalarında en çok kullanılan matematik araçtır. İmzanın doğrulama işlemine de bu yöntem denenmektedir. Doğrulama, iki adım olarak gerçekleşir;

İlk adım, şüpheli bir imzanın otantik olarak sınıflandırılması için, bileşenlerinin sekansları, iddia edilen imzalayıcının yapısal tanım grafiğinde olası bir sekansla eşleşmelidir.

Bu adım başarılı bir şekilde tamamlanırsa, ikinci adım doğrulama, her bir kümenin tek tek doğrulanmasıyla gerçekleştirilir. Fourier tanımlayıcıları, bir eşik değerine karşı mesafe ölçüsünde kullanılırlar. Herhangi bir bileşen testi geçmezse, imza, sahte imza olarak sınıflandırılır. Her küme için eşik değeri, orijinal bileşenlerden elde edilen en kötü doğrulama sonucunu kullanarak otomatik olarak türetilir.

Hız sinyalleri pozisyonel sinyallerden türetilebilir. v_x ve v_y hız sinyalleri için, otokorelasyon fonksiyonları Rv_x ve Rv_y hesaplanır. Bu sinyaller daha sonra, bir sayılı dürtü yanıtı (finite impulse response - FIR) filtresinin, sırasıyla, girdi ve çıktısı olarak kabul edilir.

Dürtü yanıtı, otokorelasyon sinyalleri arasındaki en küçük karesel hatayı en aza indirgeyerek elde edilir. Dürtü yanıtlarının bir referans vektörü, eğitim setinden rasgele örneklerden hesaplanır. Şüpheli bir imzanın dürtü yanıtı ile referans dürtü yanıtı arasındaki mesafe, otantikliğini karar vermek için, bir eşik değeri ile karşılaştırılır [44].

4.8 Özet

Hiçbir yöntem bir özellik veya bir dizi özellik ile sınırlı değildir. Sistemi uygulayan kişi, kendi sistemi için daha uygun özellik koleksiyonunu seçmelidir. Ancak ne kadar fazla özellik kullanılırsa, sistemin o kadar iyi olma ihtimali artar. Her yaklaşım (yöntem ve özellik seti), sistemi farklı şekillerde eğitilmesine neden olacaktır [42]. Bu bölümde, dinamik zaman çözgüsünün imza modellemesi için nasıl kullanıldığını ve bunun uygulamada kullanılmasını detaylı olarak açıklanmıştır.

Bölüm 5

DTW ile Uygulama

Analiz ve tasarım aşaması tamamlandıktan sonra, imza doğrulama sisteminin gerçeklenme aşamasına geçilebilir. Öncelikle, önerilen imza doğrulama sistemi ve matematiksel kavramlar tanıtıldı. Daha önce belirtildiği gibi, iki imza serisini "çözgülemek" için Dinamik Zaman Çözgüsü (DTW) tekniği kullanılacaktır. Kullanıcı, basınç kalemini kullanarak tablette gerçek zamanlı imzayı atar ve farklı noktalardaki *x*, *y* koordinatları ve basınç gibi dinamik verileri alınır ve gerçek zamanlı olarak text dosyasına kaydedilir. Burda 7 imza referanse olarak alınır ve verileri *x, y* koordinatı ve basınç formunda depolanır. Toplanan veriler ilk önce normalize edilir, böylece yüksek değerli özellikler düşük değerli özelliklerin üzerine baskın olmaz.

Veriler temel olarak üç parametre biçimindedir:

1. Her noktada imzanın X, Y-koordinatları.
2. İmzanın farklı noktalarındaki basınç değerleri.

Bu sistem için, imza yörüngesi üzerindeki noktaların aşağıdaki üç lokal özelliği ile ve bunlardan türetilmiş üç özelliği ile deney yapıldı: *x (t), y (t),* zaman *(t)* daki kalem konumu olduğuna göre, *p(t) ε{ 0,1,2,...,1024 }* kalem basıncını temsil eder, imza yörüngesinin ilk noktasına göre x-y koordinatları, iki ardışık noktanın arasındaki x ve y koordinat farkları, ve iki ardışık noktanın arasındaki eğrilik farkları [İki ardışık noktanın *(Δx, Δy)* arasındaki *x* ve *y* koordinat farkları en düşük hata oranlarını verdi]. İki ardışık noktanın *(Δp)* arasındaki *(p)* kalem basıncı farkları. İki ardışık noktanın *(Δv)* arasındaki hız farkları. *Δy / Δx. Δp / Δx.*

5.1 Yöntem

İmza doğrulama sisteminin ana aşaması şöyledir:

5.1.1 Kayıt (Enrollment)

Sisteme kayıt sırasında, kullanıcı, kullanıcının imzalarındaki varyasyonlarının ölçülmesinde kullanılması için, birkaç tane imza sağlar, bunlar da daha sonra eğitim ve

doğrulama süreçlerinde kullanılırlar. İlk olarak, sağlanan imzalar çift olarak hizalı hale getirilir. Bu hizalanma skorlarını kullanarak her çiftin arasındaki mesafeleri bulmak için, öncelikle, diğer tüm sağlanan imzalarla minimum ortalama mesafesi olan referans imza seçilir ve şablon imza olarak da belirlenir. Ardından, referans seti imzalarının yayılımını/varyasyonunu karakterize eden istatistikler hesaplanır. Özellikle, bir referans seti R_{ID} için, referans seti üzerinden ortalama değerleri hesaplanır, bunun için aşağıdaki hesaplamalar yapılır;

• Referans imzalarının en yakın komşularına olan mesafeleri $\{d_{min}(R_{ID})\}$,

• Referans imzalarının en uzak komşularına olan mesafeleri $\{d_{max}(R_{ID})\}$,

• Referans imzalarının şablon imzasına olan mesafeleri $\{d_{template}(R_{ID})\}$

Mesafeler bir test imzası için hesaplananlara benzemektedir

5.1.2 Eğitim sınıflandırıcıları (Training classifiers)

İlk olarak, her bir eğitim imzası (Y), ait olduğu iddia ettiği referans setindeki imzalarla (R_{ID}) karşıaştırılır, böylece üç mesafe değerleri verir $\{d_{min}(Y,R_{ID})\}$, $\{d_{max}(Y,R_{ID})\}$, $\{d_{template}(Y,R_{ID})\}$. Aynı normalizasyon süreci hem eğitim süreci sırasında eğitim imzaları için, hem de test süreci sırasında test imzaları için yapılır. Bu mesafe değerleri daha sonra referans setinin karşılık gelen ortalamaları ile normalize edilir, üç boyutlu özellik vektörünü (F_Y) vermek için:

$$F_Y = \begin{bmatrix} d_{min}(Y, R_{ID}) / \, d_{min}(R_{ID}) \\ d_{max}(Y, R_{ID}) / \, d_{max}(R_{ID}) \\ d_{template}(Y, R_{ID}) / \, d_{template}(R_{ID}) \end{bmatrix}$$

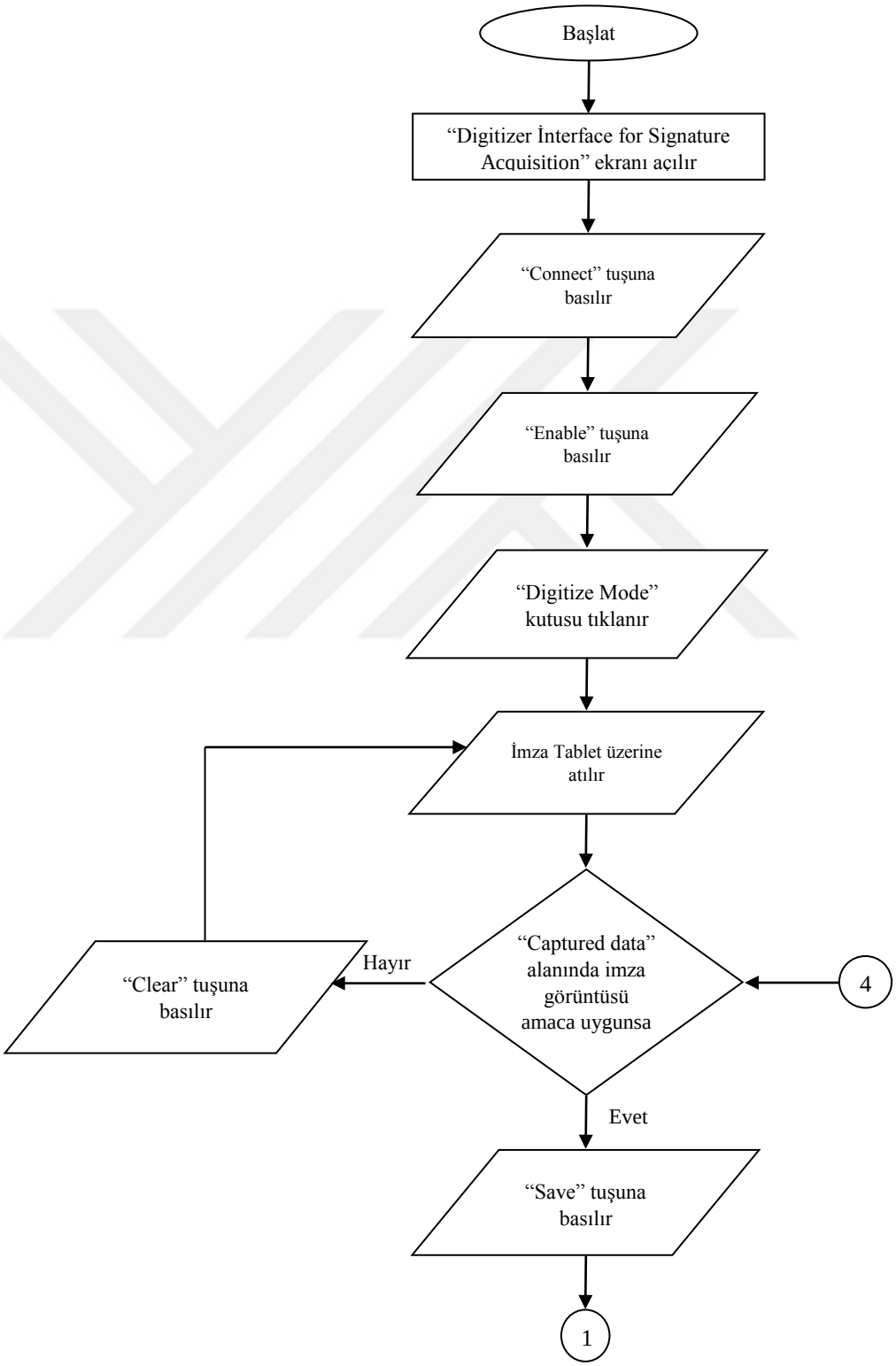
5.1.3 Doğrulama (Verification)

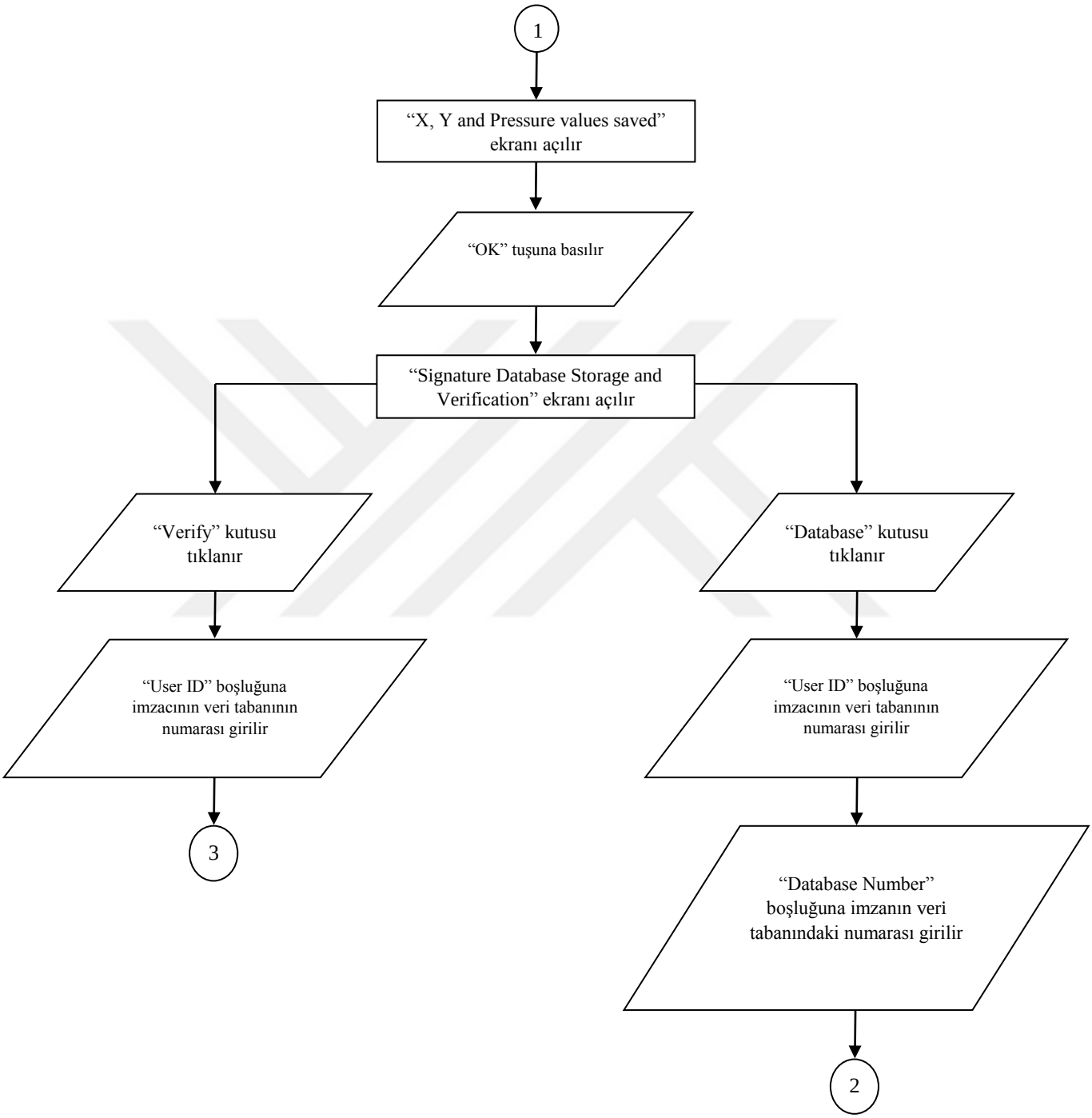
Bir test imzasını doğrulamak için, ilk olarak, imza, iddia edilen kimliğe ait olan tüm referans imzalarıyla karşılaştırılır. Farklı uzunluklardaki imzaları karşılaştırmak için, dinamik zaman çözgüsü (DTW) algoritması kullanıldı. Bu da, farklı uzunluklardaki vektörlerin hizalanması için yaygın olarak kullanılan bir yöntemdir. Dinamik zaman çözgü algoritması, iki vektörün en iyi doğrusal olmayan hizalamasını bulur böylece

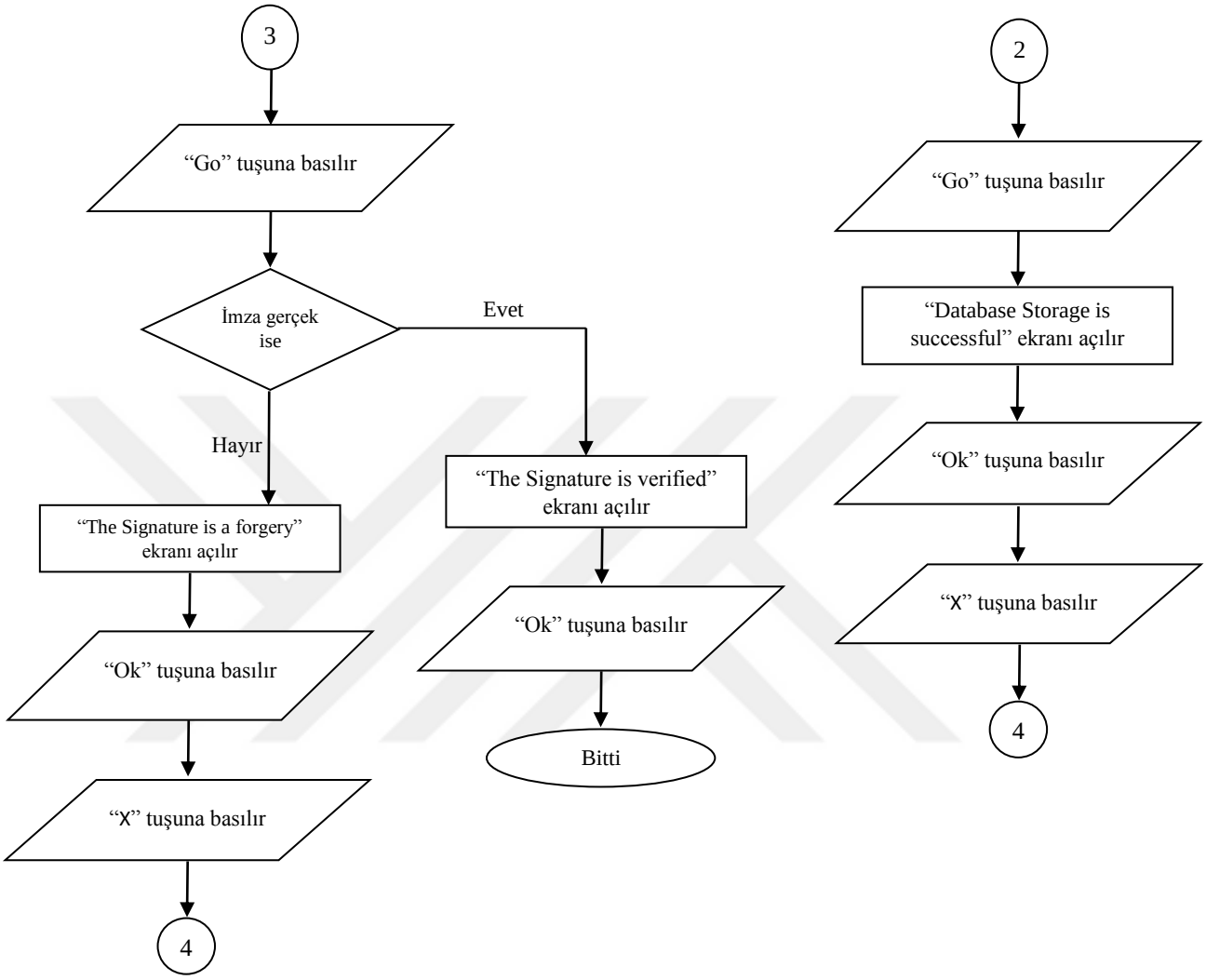
aralarındaki toplam mesafe asgari düzeye indirilir, ve elde edilen mesafe değerleri iddia edilen referans setinin ortalamaları ile normalleştirilir. Sonuçlanan üç boyutlu özellik vektörleri, imzayı orijinal veya sahte olarak sınıflandırmasında kullanılır.

5.2 Program Akış Diyagramı

Bu tezde kullanılan program temel olarak, *Online İmza Doğrulamasının* MATLAB kodunu, MATLAB programını kullanarak kodu ".dll" library dosyaları şekilde birleştirir. Ardından oluşturulan ".dll" library dosyaları, DigitizerInterface ekranına eklenir ve program çalıştırılır. *Online İmza Doğrulaması* programı C# kodunu kullanarak, grafik kullanıcı arabirimi ekranını açar. Açılan ekranda, WACOM tabletini kullanarak, referans veya test imza atılır. "Save" tuşu basıldıktan sonra C#, MATLAB'a erişir ve kodu uygulayarak referans imzayı imza veri tabanında depolar ve test imzayı kabul veya reddeder.


Başlat
"Digitizer İnterface for Signature Acquisition" ekranı açılır
"Connect" tuşuna basılır
"Enable" tuşuna basılır
"Digitize Mode" kutusu tıklanır
İmza Tablet üzerine atılır
"Captured data" alanında imza görüntüsü amaca uygunsa
Hayır
"Clear" tuşuna basılır
4
Evet
"Save" tuşuna basılır
1


1
"X, Y and Pressure values saved" ekranı açılır
"OK" tuşuna basılır
"Signature Database Storage and Verification" ekranı açılır
"Verify" kutusu tıklanır
"Database" kutusu tıklanır
"User ID" boşluğuna imzacının veri tabanının numarası girilir
"User ID" boşluğuna imzacının veri tabanının numarası girilir
3
"Database Number" boşluğuna imzanın veri tabanındaki numarası girilir
2



Şekil (5-1) Program Akış Diyagramı

5.3 Test ve Uygulama

5.3.1 Test

Tez, Dinamik Zaman Çözgüleme Yöntemi ile online imza doğrulaması hakkındadır. Hazırlanan program, 7 adet imzayı, referans olarak kullanıcının veritabanında depolar. Ardından, kullanıcı bir test imzası sunar ve program bu imzayı veritabanındaki imzalar ile karşılaştırır ve test imzayı kabul veya reddeder. Bu program, kod'ta bazı düzeltmeleri yapmak suretiyle, değişik referans imzalarının sayıları ile çalışabilir haldedir, örneğin 15 referans imza kullanarak bazı denemeler yapıldı. Ancak 15 imza işlem yerine, 7 referans imzanın seçmenin nedeni, kullanıcı açısından daha kullanışlı ve fazla zaman tüketmeden, daha az imza sayısı ile daha hızlı veritabanı oluşturmaktır. Bir diğer nedeni, yapılan gözlemlerden sonra, 15 referans imzalarının hata oranlarına yanı sıra en yakın ve en düşük hata oranlarına sahip olan ancak performans açısından 15 sayılı referans imzaya en yakın olan, 7 referans imzanın olması bulundu. Tablo (5-3) ve (5-4)'te görüldüğü gibi 5 sayılı veri tabanlarda FAR ve FRR %13.04 ve %22.61 olduğu tespit edildi buna karşın, tablo (5-1) ve (5-2)'de görülen 7 sayılı veri tabanlarda FAR ve FRR %5.21 ve %11.3 olduğu yani daha az referans sayısı ile oluşturulan veritabanlarda, yanlış kabul etme oranının yanı sıra yanlış reddetme oranının büyük ölçüde arttığı tespit edildi. Örneğin 5 referans imza ile oluşturulan veritabanlar, test imzaların daha az numune ile karşılaştırılması sonucu oluşan yüksek yanlış kabul etme ve reddetme oranlarının dolayısıyla, kullanıcının test aşamasında daha fazla denemelere yani daha fazla test imza atmasına gerektirir buda kullanıcı açısından sakıncalı olmasının yanı sıra, yüksek güvenlik gerektiren iş yerlerinde programın güvenilirliğini kaybetmesine yol açar. En son yapılan gözlemlerin ve denemelerin sonucu, 7 den daha az bir sayıda (örneğin 5 referans imza) elde edilen sonuçların ve hata oranlarının arttığını ve performansın düştüğünü, 7 den daha fazlaki bir sayıda (örneğin 15 referans imza) kullanıcı açısından daha az konforlu ve kullanışlı olduğu sonuca varıldı. Sonuç olarak, 7 referans imzanın en ideal sayı olduğu gözlemlendi ve programa uygulandı.

Gerçek İmzalayıcılarının Sayısı	Her İmzalıyıcı için Alınan Referans İmza Sayısı	Her İmzalıyıcı için Test Edilen Gerçek İmza Sayısı	Test Edilen İmzaların Total Sayısı	Reddedilen İmzaların Total Sayısı	Yanlış Reddetme Oranı (FRR)
23	7	5	115	13	%11.3

Tablo (5-1) 7 Sayılı Veritabanlardaki Gerçek İmzalarının Yanlış Reddetme Oranı (FRR)

Sahtecilerinin Sayısı	Her Sahteci için Test Edilen Sahte İmza Sayısı	Test Edilen Sahte İmzaların Total Sayısı	Kabul Edilen Sahte İmzaların Total Sayısı	Yanlış Kabul Etme Oranı (FAR)
23	5	115	6	%5.21

Tablo (5-2) 7 Sayılı Veritabanlardaki Sahte İmzalarının Yanlış Kabul Etme Oranı (FAR)

Gerçek İmzalayıcılarının Sayısı	Her İmzalıyıcı için Alınan Referans İmza Sayısı	Her İmzalıyıcı için Test Edilen Gerçek İmza Sayısı	Test Edilen İmzaların Total Sayısı	Reddedilen İmzaların Total Sayısı	Yanlış Reddetme Oranı (FRR)
23	5	5	115	26	%22.61

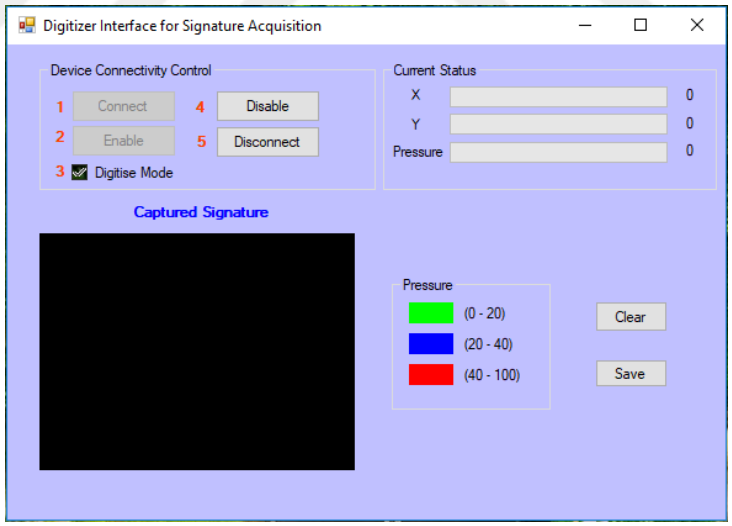
Tablo (5-3) 5 Sayılı Veritabanlardaki Gerçek İmzalarının Yanlış Reddetme Oranı (FRR)

Sahtecilerinin Sayısı	Her Sahteci için Test Edilen Sahte İmza Sayısı	Test Edilen Sahte İmzaların Total Sayısı	Kabul Edilen Sahte İmzaların Total Sayısı	Yanlış Kabul Etme Oranı (FAR)
23	5	115	15	%13.04

Tablo (5-4) 5 Sayılı Veritabanlardaki Sahte İmzalarının Yanlış Kabul Etme Oranı (FAR)

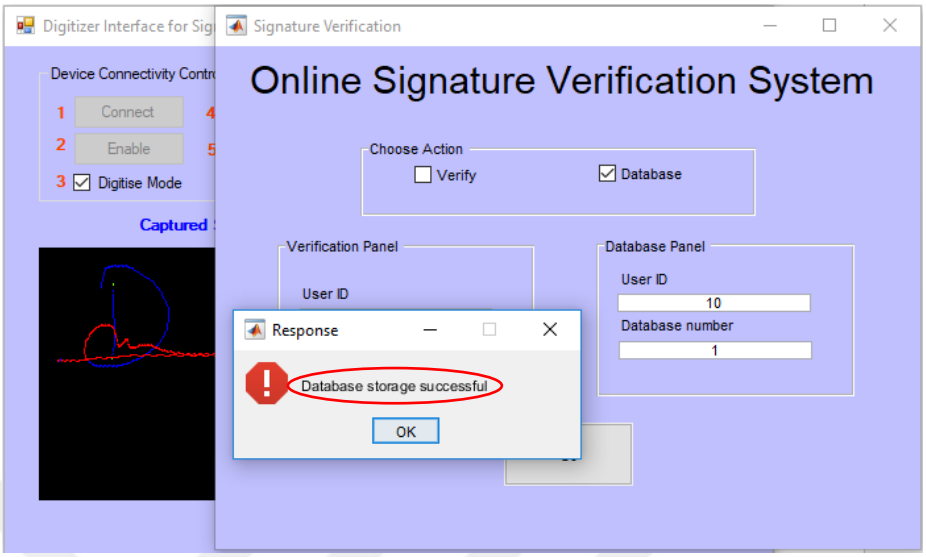
5.3.2 Uygulama

Programı çalıştırmak için WACOM tableti bilgisayara bağlanır. DigitizerİnterfaceTest uygulamasını tıklayarak program açılır (şekil 5-2).



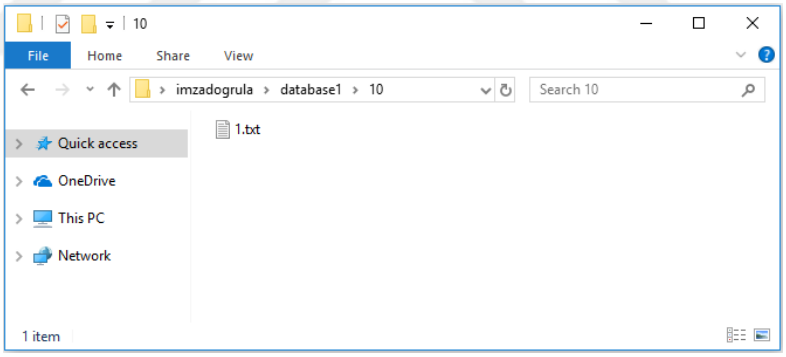
Şekil (5-2) Tabletten imza verilerini almak için kullanılan GUİ

Şekil (5-3)'de gösterildiği gibi referans imza atıldıktan sonra "Database Storage Successful" ekranı açılır.



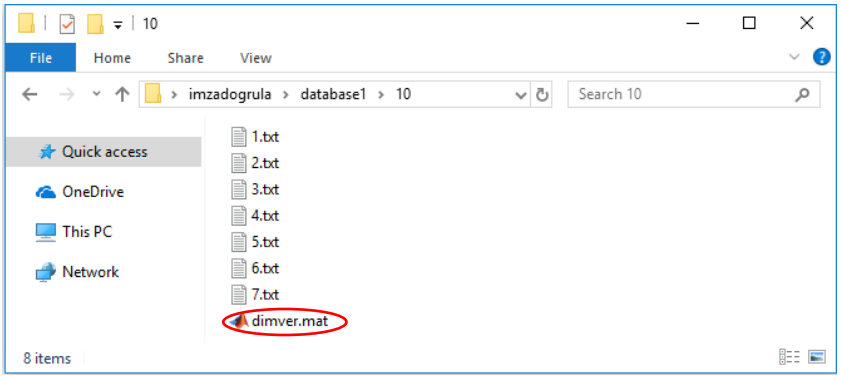
Şekil (5-3) Veri tabanı oluşturma işlemi

Atılan imzanın belli noktaların x, y ve basınç verilerini bir .txt dosyası formatında, referans imza veri tabanında kaydedilir (şekil 5-4).



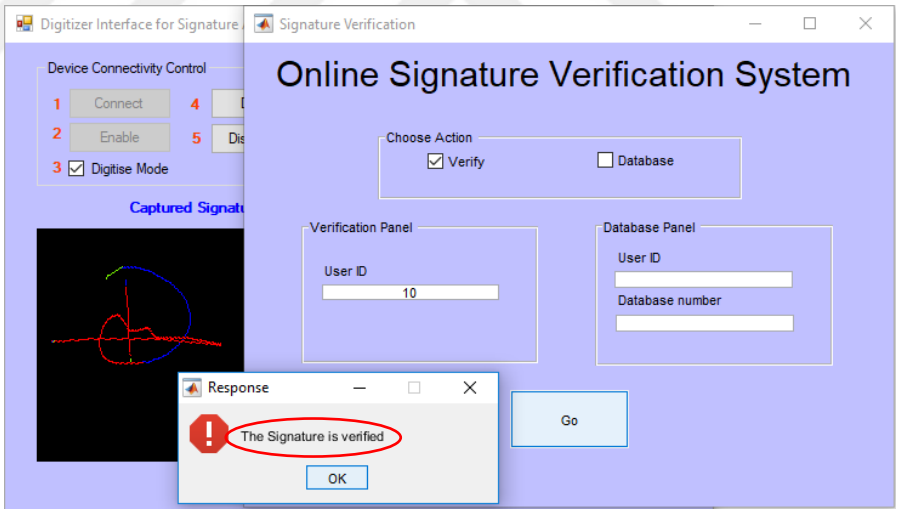
Şekil (5-4) Veri tabanı klasöründe, .txt formatında depolanan birinci referans imza

7 referans imzayı attıktan sonra veri tabanı klasöründe “dimver.mat” dosyası oluşturulur ve o imzanın veri tabanını kapatır (şekil 5-5).

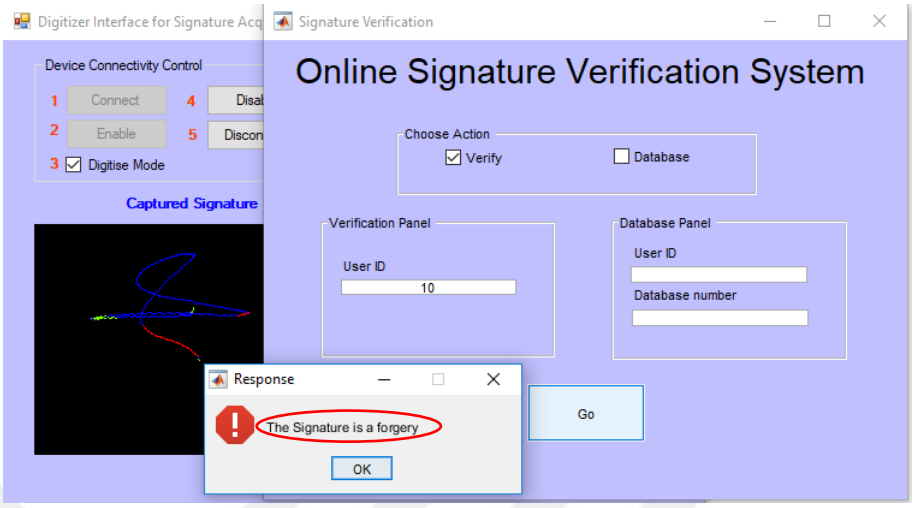


Şekil (5-5) Tamamlanmış veri tabanı

Doğrulama işlemini gerçekleştirmek için test imzası atılır ve o imzanın veri tabanı'nın numarası girilir. Atılan test imzası, referans imzalarla karşılaştırılır ve program o imzayı şekil (5-6) ve (5-7)'de gösterildiği gibi kabul veya reddeder.



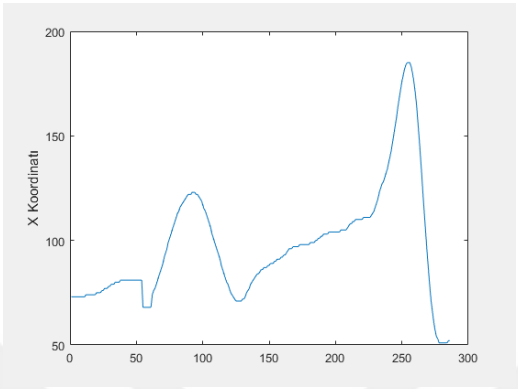
Şekil (5-6) Doğrulanan imza



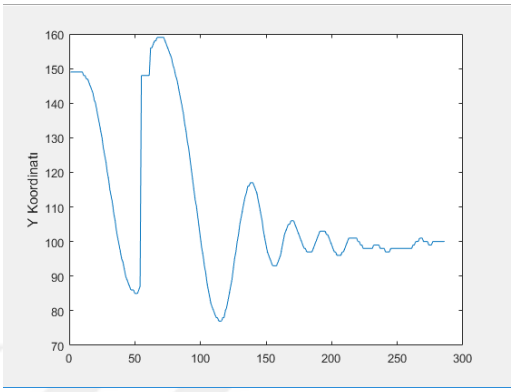
Şekil (5-7) Reddedilen imza

5.3.3 Test Analizi

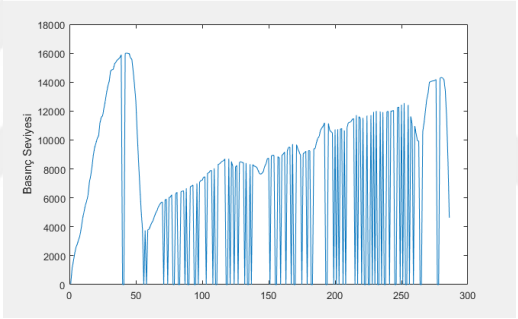
Bu şekilde x, y ve p koordinatları için bir imza örneği gösterilmektedir.



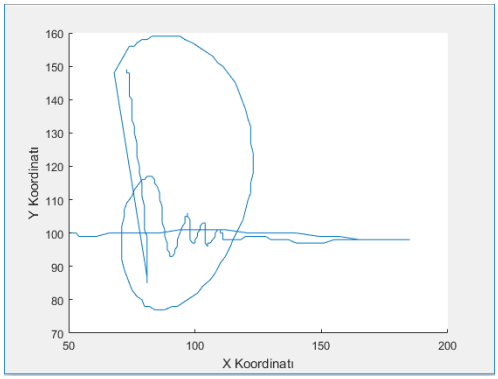
a) x koordinatı



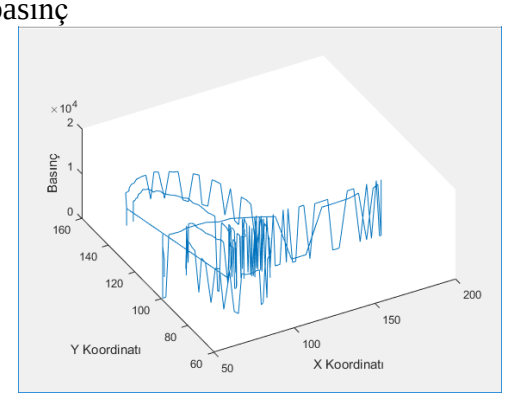
b) y koordinatı



c) p basınç



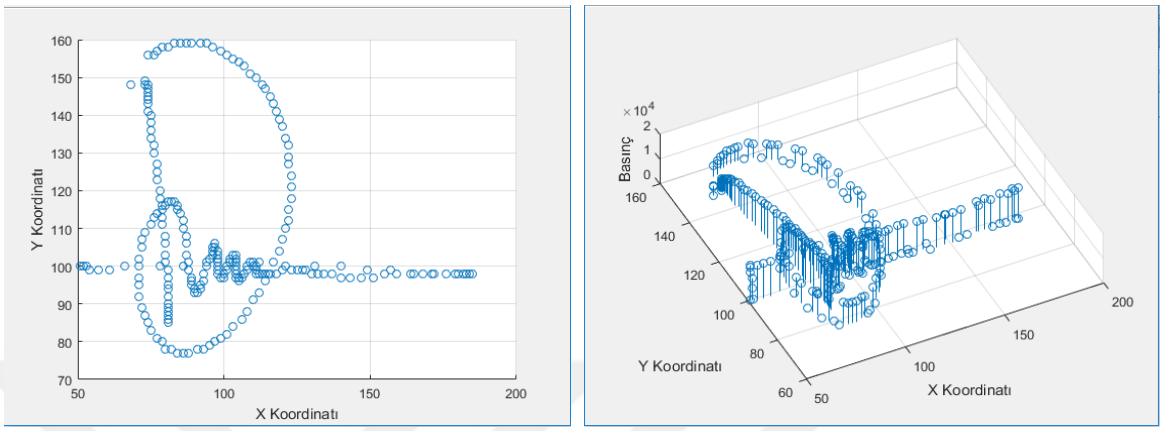
d) x, y koordinatları



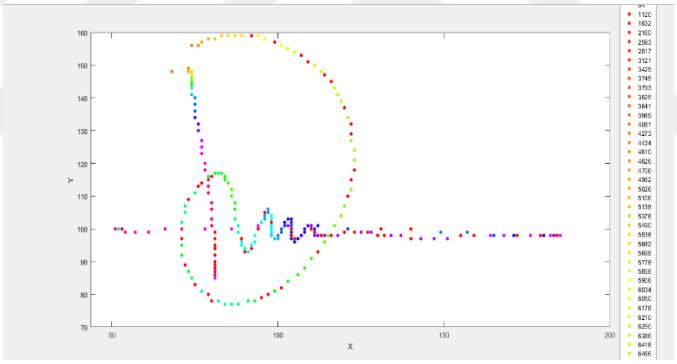
e) x, y ve p koordinatları 3 boyut olarak

Şekil (5-8) x, y ve p koordinatlarının örnekleri

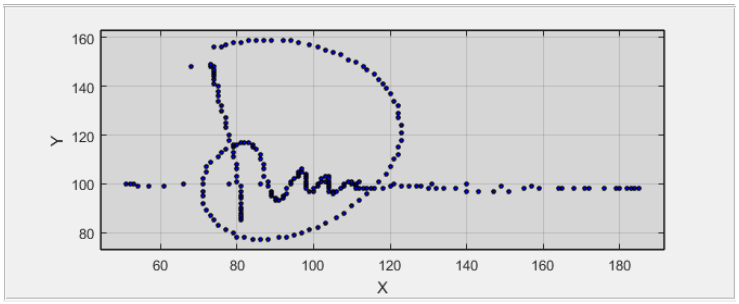
x, y ve p'nin bir biriyle integrasyonu;



Şekil (5-9) İmza enterpolasyonu



Şekil (5-10) İmza yörüngesi boyunca yakalanan değişik basınç noktaları



Şekil (5-11) İmza yörüngesi boyunca örneklenen noktalar

Bölüm 6

Sonuç

Bu tezde online imza doğrulama çerçevesi önerilmiştir. Sistem, referans imzaları üretip sisteme kaydetmek ve test imza ile karşılaştırılmaları için bir algoritma sunmaktadır. Bu proje temelde, gerçek ya da sahte imzaların doğrulamalarında *Dinamik Zaman Çözgüsünü* kullanarak online imza doğrulamasının geliştirilmesiyle ilgilidir.

İmzanın doğru segmentasyonu, imza doğrulama sisteminin önemli bir faktörüdür. Pek çok umut verici teknik ve algoritma geliştirildi ancak, imza segmentasyon metodolojilerinin gelişmeleri için hala eksikler söz konusudur. Tezde, imza doğrulama sistemlerinde yapılan çalışmaların sayısı incelendi ve mevcut çok sayıda sistemin sınırlı sayıda özellik çıkarımı kullandığını görüldü, algoritma boyutunu azaltmak amacıyla, tasarlanan ve gerçeklenen sistemin en ideal olduğu kanısına varıldı.

KAYNAKLAR

[1] Fincy Francis1, Aparna M.S, Anitta Vincent **"**Biometric Online Signature Verification" IOSR Journal of Electronics and Communication Engineering PP 82-89

[2] M.Govindarajan and RM.Chandrasekaran" Bagged ensemble of genetic algorithm for signature verification" Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar-608002, Tamil Nadu, India. 2011

[3] C. Hook, J. Kempf, and G. Scharfenberg, "New Pen Device for Biometrical 3D Pressure Analysis of Handwritten Charakters, Words and Signatures," January 2003, https://www.researchgate.net/publication/228599824_New_pen_device_for_biometrical_3D_pressure_analysis_of_handwritten_characters_words_and_signatures (Erişim Tarihi Haziran, 2017)

[4] Khalid Saeed, Marcin Adamski, Tapalina Bhattasali, Mohammad K. Nammous, Piotr Panasiuk, Mariusz Rybnik, and Soharab H. Shaikh "New Directions in Behavioral Biometrics" 2016

[5] Mariko Nakano Miyatake, Katina Toscano M. "Dynamics features Extraction for on-Line Signature verification" https://www.scribd.com/document/7231907/Dynamic-Features-Extraction-for-Online-Signature-Verification (Erişim Tarihi Haziran, 2017)

[6] Hao Feng **"**A Cryptosystem with Private Key Generation from Dynamic Properties of Human Hand Signature" Stage of Thesis 2002

[7] Fauziyah Salehuddin, Hazura Haroon, Zahariah Manap "Online Signature Verification system" https://www.researchgate.net/publication/224503084_Online_Signature_Verification_system (Erişim Tarihi Haziran, 2017)

[8] https://www.ibm.com/support/knowledgecenter/ar/SSGU8G_12.1.0/com.ibm.tms.doc/ids_tms_471.htm (Erişim Tarihi Haziran, 2017)

[9] Vinayak Balkrishana Kulkarni "A colour Code Algorithm for Signature Recognition" Electronic Letters on Computer Vision and Image Analysis 6(1):1-12, 2007

[10] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3967422/ (Erişim Tarihi Haziran, 2017)

[11] Juraj H´amorn´ık "Signature-based User Authentication" Stage of Thesis 2015

[12] Amaç Herdağdelen, Ethem Alpaydın , Boğaziçi University **"**Dynamic Alignment Distance Based Online Signature Verification" ISBN : 975-441-213-8 The 13th Turkish Symposium on Artificial Intelligence & Artificial Neural Networks, 10-11 June 2004, Izmir, Turkey

[13] John Vacca "Biometric Technologies and Verification Systems" 2007 https://books.google.com.tr/books?id=Pwv_4mnIRFEC&pg=PA170&lpg=PA170&dq=The+original+signer+can+re-create+the+changes+in+timing+and+X,+Y,+and+Z&source=bl&ots=L4EONT2z0w&sig=CDo1Py_yhDDhMG58PviPVbgT35U&hl=en&sa=X&ved=0ahUKEwiI9-ThydrWAhUF0xoKHc4zBNMQ6AEIJzAA#v=onepage&q=The%20original%20signer%20can%20re-create%20the%20changes%20in%20timing%20and%20X%2C%20Y%2C%20and%20Z&f=false (Erişim Tarihi Haziran, 2017)

[14] Ruben Tolosana, Ruben Vera-Rodriguez, Javier Ortega-Garcia, (Senior Member, IEEE), and Julian Fierrez, (Member, IEEE) **"**Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification" Digital Object Identifier 10.1109/ACCESS.2015.2431493 May 2015

[15] Paolo Ciaccia Time Series (2) Information Systems http://www-db.deis.unibo.it/courses/SI-M/ (Erişim Tarihi Haziran, 2017)

[16] Riccardo Simon Corradin "Signature verification in consignment notes" Stage of Thesis August 2008

[17] Jack Phan "MATLAB - C# for Engineers" LePhan Publishing, 2010 ISBN: 978-1-452-80256-5

[18**]** Marta Gomez Barrero "Improving Secrurity and Privacy in Biometric Systems"

Stage of Thesis Madrid, April 2016

[19] http://www.tutorialspoint.com/biometrics/biometrics_quick_guide.htm (Erişim Tarihi Haziran, 2017)

[20] James Wayman, Anil Jain, Davide Maltoni and Dario Maio (Eds) **"**Biometric Systems Technology, Design and Performance Evaluation" 2004

[21] Marcia Y. Jung International Biometric Group (IBG), "biometric Market and Industry Report, 2006-2010," International Biometric Group, 2005.

[22] ISO/IEC TR 24741, "Information Technology - Biometrics Tutorial", ISO/IEC, Geneva, 2007.

[23] Rajdeep Das, Sangeeta Dhar, Sabarni Das, Saurav Dutta, Subra Mukherjee **"**A Comparative Study of Biometric Authentication Based on Handwritten Signatures" International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 02 Issue: 12 December 2013

[24] Shern Cheng Yau **"**Validation of Dynamic Signature for Identity Verification" Stage of Thesis August 2008

[25] H. David, "An overview of biometrics support in NetWare through NMAS", July 2001 http://support.novell.com/techcenter/articles/ana20010701.html (Erişim Tarihi Haziran, 2017)

[26] Patel Bhumika A, Shashwat Kumar "A Survey on Handwritten Signature Verification Techniques" ISSN: 232 7782 Volume 3, Issue 1, January 2015

[27] Elena Tsiporkova "Dynamic Time Warping Algorithm for Gene Expression Time Series"

[28] Marcos Faundez-Zanuy "On-line signature recognition based on VQ-DTW" https://www.researchgate.net/publication/222631032_On-line_signature_recognition_based_on_VQ-DTW (Erişim Tarihi Haziran, 2017)

[29] Eamonn J. Keogh, Michael J. Pazzani **"**Derivative Dynamic Time Warping" Department of Information and Computer Science University of California, Irvine, California 92697 USA

[30] W. Zhao, R. Chellappa, A. Rosenfeld, P.J. Phillips, "Face Recognition: A Literature Survey", ACM Computing Surveys, 2003, pp. 399-458

[31] Ross J. Anderson, "Biometrics", Security Engineering, Wiley Computer

Publishing, pp. 272 - 286, 2001. books.google.com.tr https://books.google.com.tr/books?id=eo4Otm_TcW8C&printsec=frontcover&dq=Biometrics%E2%80%9D,+Security+Engineering,+Wiley+Computer+Publishing,+pp.+272+-+286,+2001.&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false (Erişim Tarihi Haziran, 2017)

[32] Ondrej Rohlik "Handwritten Text Analysis" Stage of Thesis March 2003

[33] Janio Coutinho Canuto **"**Biomechanical online signature modeling applied to verification" Stage of Thesis May 2015

[34] Carmen S´anchez Avila, Javier Guerra Casanova, Francisco Ballesteros, Lorenzo Javier Mart´ın Garc´ıa, Miguel Francisco Arriaga G´omez, Daniel de Santos Sierra, Gonzalo Bailador del Pozo **"**State of the art of mobile biometrics, liveness and non-coercion detection" January 2014

[35] M. C. Fairhurst "Signature verification revisited: Promoting practical exploitation of biometric technology" Electronics & Communication Engineering Journal December 1997 p.273-280

[36] Hafiz Muhammad Gulzar **"**Comprehensive Python Module for Computing and Visualizing Dynamic Time Warping Alignment: DTWPy" UNIVERSITY OF STAVANGER, NORWAY June 2015

[37] Donato Impedovo and Giuseppe Pirlo "Automatic Signature Verification: The State of the Art" IEEE Transactions on Systems, Man and Cybernetics — Part C: Applications and Reviews, Vol. 38, No. 5, September 2008 p. 609 - 635

[38] G. K. Gupta "The State of the Art in On-line Handwritten Signature Verification" Faculty of Information Technology Monash University, May 2006

[39] Chotirat Ann Ratanamahatana, Eamonn Keogh "Everything you know about Dynamic Time Warping is Wrong" Department of Computer Science and Engineering, University of California, Riverside

[40] Dominique Rivard **"**Multi-Featre Aproach for Writer-Independent Offline Signature Verification" Montreal, Stage of Thesis October 2010

[41] Akhil Garg and Sachin Tyagi "Signature Verification" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 6, June 2015

[42] Ricardo Manuel Pereira Gonçalves “Handwritten signature authentication using motion detection and QRCodes” Stage of Thesis 2015

[43] Beatrice Drott, Thomas Hassan-Reza **“**On-line Handwritten Signature Verification using Machine Learning Techniques with a Deep Learning Approach” September 2015

[44] Raghuram Malladi “Automatic signature verification system” Stage of Thesis November 2013

[45] Muhammad Imran Malik “Automatic Signature Verification: Bridging the Gap between Existing Pattern Recognition Methods and Forensic Science” Stage of Thesis October 2015

[46] ISO/IEC19795-1 "Information technology - Biometric performance testing and reporting" First edition 2006-04-01 Reference number ISO/IEC 19795-1:2006(E)

[47] S. J. Elliott **“**Development of a Biometric Testing Protocol for Dynamic SignatureVerification” Seventh International Conference on Control, Automation, Robotics and Vision (ICARCV'02), Singapore, December 2002

[48] Ashish Dhawan, Aditi R. Ganesan **“**Handwritten Signature Verification” The university of Wisconsin Madison

[49] Santosh K.C., Cholwich Nattee **“**A comprehensive survey on on-line handwriting recognition technology and its real application to the Nepalese natural handwriting” Kathmandu University Journal of Science, Engineering, and Technology, Kathmandu University, 2009, 5 (I), pp.31-55.

[50] Namirial GmbH “Biometric Signature Verification in Real-Time Secure transactions through authentication signers with their handwritten signature”

[51] http://www.wacom.com (Erişim Tarihi Haziran, 2017)

[52] https://www.oth-regensburg.de/index.php?id=5312/%20BIOMETRIC%20SMART%20PEN%20PROJECT?id=5312/%20BIOMETRIC%20SMART%20PEN%20PROJECT (Erişim Tarihi Haziran, 2017)

[53] http://www.infosysinternational.com/digitalpen.aspx (Erişim Tarihi Haziran, 2017)

[54] Hamam M.Ibrahim Mokayed **“**Signature Verification System Based on Multiple Classifiers and Multi Fusion Decision Approach” Faculty of Electrical

Engineering, Universiti Teknologi Malaysia, Stage of Thesis January 2010

[55] Toni Giorgino **"**Computing and Visualizing Dynamic Time Warping Alignments in R: The dtw Package" Journal of Statistical Software Volume 31, Issue 7, August 2009

[56] H B Kekre, V A Bharadi **"**Gabor Filter Based Feature Vector for Dynamic Signature Recognition" International Journal of Computer Applications (0975 – 8887) Volume 2 – No.3, May 2010

[57] Saeid Rashidi, Ali Fallah, Farzad Towhidkhah "Authentication Based on Pole-zero Models of Signature Velocity" J. Med Signals Sens 2013 October – December; 3(4): 195-208 PMCID: PMC 3967422

[58] Akondi Vyasa Bharadwaja "The Analysis of Online and Offline Signature Verifcation Techniques to Counter Forgery" Indian Journal of Science and Technology, Vol 8(20), DOI: 10.17485/ijst/2015/v8i20/77735, August 2015

[59] Qiushi Fu, Baro Hyun **"**System Identification Approach in Signature verification" State University of New York at Buffalo, Department of Mechanical and Aerospace Engineering, 2007

[60] Prabhu Teja S **"**Representation of Ballistic Strokes of Handwriting for Recognition and Verification" Center for Visual Information Technology, International Institute of Information Technology, Hyderabad - 500 032, INDIA January 2015

[61] Ghazaleh Taherzadeh, Roozbeh Karimi, Alireza Ghobadi, Hossein Modaberan Beh "Optimized Features Set for On-line Signature Verification" https://www.researchgate.net/publication/263776415_Optimized_Features_Set_for_On-line_Signature_Verification (Erişim Tarihi Haziran, 2017)

[62] Ronaldo F. Ramos, Oscar Miguel-Hurtado, Enrique Canto "Embedded System for Biometric Online Signature Verification" https://www.researchgate.net/publication/260710701_Embedded_System_for_Biometric_Online_Signature_Verification (Erişim Tarihi Haziran, 2017)

[63] Franck Leclerc and Rejean Plamondon **"**Automatic Signature Verification: The State of the Art —1989-1993" P. 643 – 660 November 1993

[64] Fincy Francis, Aparna M.S, Anitta Vincent **"**Biometric Online Signature

Verification" IOSR Journal of Electronics and Communication Engineering e-ISSN: 2278-2834,p- ISSN: 2278-8735.PP 82-89

[65] "Signature Recognition & Keystroke Dynamics" P 203-240

[66] Ghazaleh Taherzadeh, Roozbeh Karimi, Alireza Ghobadi, Hossein Modaberan Beh **"**Evaluation of Online Signature Verification Features" Faculty of Information Technology Multimedia University, Selangor, Malaysia ISBN 978-89-5519-154-7 February 2011

[67] Hemant B Kekre, Vinayak Ashok Bharadi "Dynamic signature pre-processing by modified digital difference analyzer algorithm" https://www.researchgate.net/publication/226940002_Dynamic_signature_pre-processing_by_modified_digital_difference_analyzer_algorithm (Erişim Tarihi Haziran, 2017)

[68] Anjali Deshpande, Kishor Wane **"**A Review: Embedded System for Biometric Online Signature Verification" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 3 Issue: 5 ISSN: 2321-8169 PP 204 – 207 May 2015

[69] D. S. Guru, K. S. Manjunatha and S. Manjunath **"**User Dependent Features in Online Signature Verification" PP 229 - 240

[70] Óscar Miguel Hurtado **"**Online Signature Verification Algorithms and Development of Signature International Standards" Charles III University of Madrid, Stage of Thesis, September 2011

[71] Jonathan Wu **"**Gesture Passwords: Concepts, Methods, and Challenges" Carnegie Mellon University, Stage of Thesis 2011

[72] Mohsen Fayyaz, Mohammad Hajizadeh Saffar, Mohammad Sabokrou, Mahmood Fathy **"**Feature Representation for Online Signature Verification" Malek-Ashtar University of Technology, Tehran, Iran https://arxiv.org/abs/1505.08153 (Erişim Tarihi Haziran, 2017)

[73] Anil K. Jain, Friederike D. Griess, Scott D. Connell **"**On-line signature verification" Pattern Recognition 35 (2002) 2963–2972

[74] Alisher Kholmatov, Berrin Yanikoglu **"**Identity authentication using improved online signature verification method" Pattern Recognition Letters 26 (2005)

2400–2408

[75] Hansheng Lei, Venu Govindaraju **"**A Comparative Study on the Consistency of Features in On-line Signature" Preprint submitted to Elsevier Science November 2004

[76] Ashwini Pansare, Shalini Bhatia **"**Handwritten Signature Verification using Neural Network" International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 1– No.2, January 2012

[77] Prathiba M.K, Dr. L. Basavaraj **"**Online handwritten signature verification system: A Review" International Journal of Emerging Trends & Technology in Computer Science Volume 3, Issue 2, March – April 2014 ISSN 2278-6856

[78] Fauziyah Salehuddin, Hazura Haroon, Zahariah Manap "Online Signature Verification system" https://www.researchgate.net/publication/224503084_Online_Signature_Verification_system (Erişim Tarihi Haziran, 2017)

[79] https://www.codeproject.com/ (Erişim Tarihi Haziran, 2017)

[80] https://www.mathworks.com/matlabcentral/fileexchange/16350-continuous-dynamic-time-warping (Erişim Tarihi Haziran, 2017)

ÖZGEÇMİŞ

1 Ekim 1983 tarihi doğumluyum. Liseyi, İstanbuldaki Ali İzzat Bey okulunda 1999 yılında tamamladıktan sonra, T.C. İstanbul Kültür Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümüne kaydoldum. Bu bölümden 2005 yılında mezun oldum. Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Dalında Yüksek Lisans eğitimine sürdürmekteyim.

Konuştuğum diller: Türkçe, İngilizce ve Arapça'dır.

Dima Marachi