T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

BİYOMETRİK GÜVENLİK SİSTEMLERİNDE MAHREMİYET, GÜVENLİK VE GÜVEN İLİŞKİSİNİN MODELLENMESİ

Alper KANAK
DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

GEBZE
2013

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

BİYOMETRİK GÜVENLİK SİSTEMLERİNDE MAHREMİYET, GÜVENLİK VE GÜVEN İLİŞKİSİNİN MODELLENMESİ

Alper KANAK
DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ
ANABİLİM DALI

TEZ DANIŞMANI
Prof. Dr. İbrahim SOĞUKPINAR

GEBZE
2013

DOKTORA TEZİ JÜRİ ONAY SAYFASI

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...21/01/2013..tarih ve 2013/03 sayılı kararıyla oluşturulan jüri tarafından ...11/02/2013.. tarihinde tez savunma sınavı yapılan .....Alper KANAK.....'ın tez çalışması ...Bilgisayar Mühendisliği... Anabilim Dalında DOKTORA tezi olarak kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : Prof. Dr. İbrahim Soğukpınar

ÜYE : Prof. Dr. Coşkun Sönmez

ÜYE : Doç. Dr. Yusuf Sinan Akgül

ÜYE : Doç. Dr. Erdoğan Sevilgen

ÜYE : Yrd. Doç. Dr. Serdar Süer Erdem

ONAY

G.Y.T.E. Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ...../...../20... tarih ve ...../..... sayılı kararı.

İMZA/MÜHÜR

Not: Formdaki boşluklar mutlaka Ms Word ortamında doldurulacak.

ÖZET

TEZİN BAŞLIĞI: BİYOMETRİK GÜVENLİK SİSTEMLERİNDE MAHREMİYET, GÜVENLİK VE GÜVEN İLİŞKİSİNİN MODELLENMESİ

YAZAR ADI: Alper KANAK

Biyometrik kimlik yönetimi sistemlerinde (Biometric Identity Management Systems) güvenlik ve mahremiyet arasındaki ödünleşim yıllardır tartışılan ve çeşitli formel modellerle ifade edilebilen bir konudur. Mahremiyet ve güvenlik birlikte sağlanması gereken gereklerdir. Bu iki gerek arasında en optimum noktanın bulunması önemlidir. Ancak optimum nokta bulunsa bile, bu operasyon noktasında çalışan sisteme kullanıcıların ne kadar güveneceği belirsiz olabilir. Burada sosyal, kültürel, politik veya ekonomik etkenler toplumun bir biyometrik kimlik yönetimi sistemine duyacağı güveni etkileyebilir. Bu bakımdan mahremiyet ve güvenliğin "güven"le ilişkisinin incelenmesi gerekir. Bu doktora çalışmasında, mahremiyet, güvenlik ve güven arasındaki ilişki için matematiksel bir model oluşturulmuş ve örnek uygulamalar üzerinde biyometrik teknolojileri kullanan bazı ülkelerdeki Mahremiyet-Güvenlik-Güven ilişkisi sayısal verilerle ortaya konmuştur. Böylece, öznel bir nicelik olan güven etmeninin ölçülebilmesi ve uygulama alanına göre mahremiyet ya da güvenliğin daha önemli olduğu koşulların benzetilmesi mümkün olabilir.

SUMMARY

THESIS TITLE: MODELING PRIVACY, SECURITY AND TRUST RELATION IN BIOMETRIC SECURITY SYSTEMS

AUTHOR NAME: Alper KANAK

The tradeoff between privacy and security has been discussed and modeled through formal methods for many years. Privacy and security should be guaranteed cooperatively. Finding optimum point between privacy and security is crucial. However, even such an optimum point is found, it is uncertain that how much people trust the system at this point. Here, social, cultural, political and economic factors may influence the trustworthiness of biometric identity management systems. Therefore, the relationship between privacy, security and trust has to be investigated. In this doctoral thesis, the relationship between these three aspects, privacy, security and trust is presented in a formal way. The privacy-security-trust relationship is demonstrated through case studies where country profiles related to biometric usage are benefited to present quantitative analyzes. Thus, trust a subjective criterion, can be measured through an objective way and simulating the scenarios where privacy or security is more important might become possible.

TEŞEKKÜR

Uzun yıllar süren bu tez çalışmamda bana yol gösteren ve uluslararası düzeyde ses getiren çalışmaların altına imza atmama yardımcı olan değerli danışmanım Prof.Dr. İbrahim Soğukpınar'a;

Çalışmalarımı dikkatle takip eden ve çok değerli katkılarda bulunan tez komite üyelerim Prof.Dr. Coşkun Sönmez ve Doç. Dr. Yusuf Sinan Akgül'e;

Bu tez çalışması sırasında çıkardığım yayınlarla ilgili değerli geribildirimlerde bulunan arkadaşlarım Yücel Bicil, Dr. Şeniz Demir'e, Dr. Salih Ergün'e, Dr. Umut Uludağ'a, Mehmet Kayaoğlu'na ve Berkay Topçu'ya;

Üzerinde uzun zaman harcayarak oluşturduğum matematiksel modelin geliştirilmesinde, haberleşme alanındaki çalışmaları ile yeni ufuklar açan ve makalelerimin yazımında katkıda bulunan değerli arkadaşım Dr. Ömer İleri'ye;

Yeri geldiğinde psikolojik, yeri geldiğinde idari anlamda çalışmalarıma destek veren ve TÜBİTAK'taki mevcut projelerle paralellik arz eden konularda seyahat desteği sunan TÜBİTAK Yönetimine ve değerli yöneticilerim Dr. Hasan Palaz, Dr. Murat Erat, Dr. Oktay Adalıer ve Mehmet Uğur Doğan'a;

Ve tabi ki tüm bu süreçte her zaman yanımda yer alan biricik eşim Meryem Kanak ve aileme;

Teşekkürü bir borç bilirim.

İÇİNDEKİLER DİZİNİ

Sayfa

SİMGELER VE KISALTMALAR DİZİNİ

b	: Şablon biyometrik işareti
x	: Şablon biyometrik özniteliği
h	: Şablon biyo-kıyım katarı
s	: Sendrom
PIN	: Personal Identity Number
b'	: Sorgu biyometrik işareti
x'	: Sorgu biyometrik özniteliği
h'	: Sorgu biyo-kıyım katarı
$\hat{h}$	: Tekrar üretilen biyo-kıyım
$\hat{s}$	: Tekrar üretilen sendrom
k	: Gizli anahtar
X	: Biyometrik işaret olasılık yoğunluk fonksiyonu
S	: Sendrom olasılık yoğunluk fonksiyonu
Θ	: Biyo-kıyım olasılık yoğunluk fonksiyonu
κ	: Özel anahtar olasılık yoğunluk fonksiyonu
C	: Kod sözcüğü uzayı
d	: Kod sözcükleri arasındaki uzaklık
δ	: Komşuluk değeri
Ψ_{XY}	: X ve Y arasındaki normalize sızıntı oranı
m	: Biyometrik bit dizisinin uzunluğu
n	: Özel anahtarın uzunluğu
P	: Mahremiyet faktörü
S	: Güvenlik faktörü
T	: Güven faktörü
ω	: Kamusal isteklilik
c	: Biyometriklerden emin olma düzeyi
u	: Haberleşme verimliliği
p	: Ödenen para miktarı
η	: Mahremiyet ağırlığı
ζ	: Güvenlik ağırlığı
BI	: Davranışsal niyet

A	: Kullanıcının sisteme karşı tutumu
U	: Algılanan kullanışlılık
E	: Algılanan kullanım kolaylığı
e_i	: Dışsal değişkenler
EV	: Dışsal değişkenlerin toplam etkisi
H_i	: Teknoloji kabul modeli hipotezleri

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1 Giriş

1.1 Problem Tanımı

Biyometrik teknolojiler, kimlik yönetiminde kolay unutulabilir ya da kaybedilebilir şifrelere alternatif ya da yardımcı bir yöntem olarak öne çıkmaktadır. Ancak biyometrik teknolojiler, nihayetinde kişiye özel (mahrem) bilgilerdir ve bu bilgilerin çok iyi korunması kişisel gizlilik açısından büyük önem taşır. O nedenle erişim güvenliğini sağlamak için öne sürülen biyometrik teknolojilerin bir yandan da mahremiyeti koruması beklenir.

Mahremiyet ve güvenlik, birbiriyle ödünleşen iki kavram olarak kabul edilir. Mahremiyeti arttıran uygulamalar yüzünden güvenlik riskleri oluşabilmekte, ya da güvenliği sağlarken mahremiyet hiçe sayılabilmektedir. Biyometri dünyasında da durum farklı değildir. Biyometrik işareti gizleyip mahremiyete saygılı öznitelikler ya da bit dizileri üretilirken, bu betimleyici özellikler doğru tanıma başarımını azaltabilmektedir. Benzer biçimde, daha güçlü öznitelikler ya da sınıflandırıcılar kullanarak tanıma başarımları arttırılırken saf biyometrik bilgiye ulaşmak da kolaylaşabilir. O nedenle, insanların biyometrik teknolojilere güvenmesi için hem mahremiyetin hem de güvenliğin mümkün olan en üst düzeyde sağlanması ve insanların da bu sistemleri kullanırken istekli ve kendilerinden emin olması gerekir.

Biyometrik teknolojilerin kabul görmesinde güven faktörü dikkatle ele alınmalıdır. Zira, bu tip sistemlerde insanların sisteme güveni ile ilgili yargıları,sistemde bir mahremiyet veya güvenlik açığı olduğunda ortaya çıkar. Söz konusu istenmeyen durumlar olmadan bir biyometrik kimlik yönetimi sistemine (BKYS) duyulan güveni ölçmek oldukça zordur. O nedenle, bu öngörüye yardımcı olabilecek, mahremiyet, güvenlik ve güven arasındaki ilişkiyi ifade eden matematiksel bir modele ihtiyaç vardır. Bu matematiksel model sayesinde, güven hakkında ölçülebilir nesnel değerlendirmeler yapmak mümkün olacaktır.

Güven, biyometrik teknolojilerin kabulünde oldukça kritik bir öneme haizdir. Ancak tek faktör de değildir. Bir teknolojinin kabul edilmesinde algılanan kullanışlılık,

algılanan kullanım kolaylığı, kullanıcıların tutumları ve davranışsal niyet gibi faktörler de öne çıkar. Bu faktörler, kimi zaman ergonomik yaklaşımlarla, psikolojik etkilerin analiziyle, bilgilendirme yöntem ve faaliyetleri ile şekillenebilir. Güven faktörü, teknik veya teknik olmayan diğer tüm faktörlerle bir arada değerlendirilerek teknolojinin kabulüne ilişkin bir modelin içine yerleştirilmelidir.

Bu tez çalışmasında mahremiyet-güvenlik-güven arasındaki matematiksel ilişki ve bunun bir teknoloji kabul modeli içine yerleştirilmesi ele alınmıştır. Tezin odağını oluşturan problemler şunlardır:

1. Bir BKYS'de, mahremiyet-güvenlik-güven arasındaki ilişkiyi nesnel biçimde modelleyen matematiksel bir yaklaşım yoktur. Böyle bir matematiksel yaklaşım olsaydı, karar vericiler bir BKYS'ye duyulan güveni, güvensizliği yaratacak unsurlar gerçekleşmeden, nesnel biçimde ölçmek için yeni bir alternatif yöntem kazanmış olacaklardı.

2. Bir BKYS için nesnel bir değerlendirmeye dayanarak ölçülen güven faktörünü içeren bir teknoloji kabul modeli yoktur. Güven faktörü nesnel biçimde ölçülse bile teknolojinin kabulüne etkisi belirsizdir. Biyometrik teknolojinin kabulünü etkileyen tüm faktörler (güven dahil) bir arada gözlenecek şekilde bir model önerilmelidir.

Bu problemlere çözüm bulunduğu takdirde özellikle karar vericiler, stratejistler, analistler ve bu konuya ilgi duyan tüm araştırmacılar BKYS'lerin kullanıldığı tüm durumları sayısal verilere dayanarak değerlendirebilme imkanına kavuşacaklardır. Aynı zamanda, BKYS'yi isteyen son kullanıcılar ihtiyaçlarını bu modele göre betimleyebilecek, tasarımcılar da tüm BKYS'yi belirlenen kriterlere göre şekillendirebileceklerdir. Böylece BKYS'lerin değerlendirilmesi, karşılaştırılması, kabul ve muayenesi için nesnel yöntemler ortaya çıkmış olacaktır.

1.2 Tez motivasyonu

Son yıllarda biyometrik güvenlik sistemlerinin odağına iyiden iyiye yerleşen biyometrik şablon koruma yöntemleri, hem kişi tanımada hem de kişinin bilgilerini

gizlemede önemli bir araştırma alanı haline gelmiştir. Bu alandaki çalışmalar, biyometriklerin genel problemi olan, biyometrik işaretteki belirsizlikleri gidermeye ve tanıma başarımını arttırmaya çalışır. Bununla beraber, kişiye özel (mahrem) biyometrik bilgiler de biyometrik işaretteki belirsizlikleri tolere edebilecek biçimde gizlenerek, mahremiyet korunmaya çalışılır.

Biyometrik şablon koruma yöntemleri, bir yandan güvenliği arttıracak güvenilir öznitelikler ve eşleştirme/karşılaştırma algoritmaları peşinde koşarken bir yandan da kişisel bir biyolojik veri olan biyometrikleri de gizleyerek mahremiyeti sağlamaya çalışır. Yemek yemeyi çok seven birinin şişmanlamayı göze alması gibi, sağlam bir yuva yapmak isteyen bir kuşun çok fazla enerji tüketmek zorunda kalması gibi veya sınırlarını genişletip daha fazla kazanmayı hedefleyen bir şirketin yönetimde zaaflar yaşaması gibi doğanın ve hayatın bir parçası olan ödünleşim, mahremiyet ve güvenlik arasında da görülmektedir. Örneğin, biyometrik şablon korumada güvenliği arttıran özniteliklerin temel amacı kişiyi en iyi şekilde betimleyecek vektörler üretmektir. Ancak bu vektörlerin bir şekilde başka birinin eline geçmesi aslında teorik anlamda hiçbir zaman değişmeyecek biyolojik bir bilginin de kaybolması anlamına gelir. Bu mahrem bilginin gizliliğini sağlamak için çeşitli kriptografik kıyım fonksiyonları ve biyometrik anahtarlar önerilebilir. Ancak bu yöntemler genelde salt biyometriklerin sunduğu ayırt ediciliği azaltmakta ve tanıma başarımını düşürerek güvenlik risklerine yol açabilmektedir.

Sadece biyometrik güvenlik sistemlerinde değil, hemen hemen güvenliğin önemli olduğu tüm uygulamalarda, mahremiyet ve güvenlik arasında bir ödünleşim olduğu söylenebilir. Örneğin, çok kritik askeri uygulamalara erişimde güvenlik o kadar önemlidir ki mahremiyet neredeyse hiç dikkate alınmaz. Zira, herhangi bir güvenlik açığı olduğunda sorumlu kişinin hemen belirlenmesi ve cezalandırılması gerekir. Aynı durum bankacılık uygulamalarında, eDevlet süreçlerinde de öne çıkabilir. Karayolu ulaşımında ücretli yollara giriş çıkışın takip edilerek kullanım sıklığının ölçülmesi ve belediyecilik hizmetlerinin kalitesinin arttırılmasında geri beslemelerin değerlendirilmesi gibi güvenliğin o kadar da kritik sayılmadığı durumlarda ise mahremiyet çok daha önemli olabilir. Örneğin, belediye başkanının hizmetlerinden memnun olmayan biri bu yönde bir açıklama yapmaktan çekinebilir.

Günlük hayatta sıklıkla karşılaşılan güvenlik-mahremiyet ödünleşimi biyometrik güvenlik sistemlerinde çok daha büyük tartışmalara eşiklik eder. Örneğin, George Orwell'in ünlü "1984" romanında bahsi geçen "Büyük Birader" korkusu, günümüzde devlet-vatandaş ilişkilerinde de ortaya çıkar. Devletin, vatandaşları eDevlet uygulamaları ile, telefon konuşmalarını kaydederek ve hatta insanları takip eden ajanlar aracılığıyla mahremiyeti hiçe sayacak uygulamaları başlattığına dair bir inanç da gitgide yayılmaktadır. Hollywood filmleri ile daha da alevlenen bu inanış halkın biyometrik teknolojilere bakışını da etkileyebilir. Biyometrik teknolojiler, kimi zaman elektronik oylama gibi kritik uygulamalarda dahi gizliliği ve güvenliği sağlayacak kesin bir çözüm olarak görülürken kimi zaman da mahremiyeti tehlikeye atacak ve "sürekli izleniyorum" korkusu salacak bir mekanizma gibi de algılanabilir. Bu algılar aslında tek bir insani ihtiyaçla ilgilidir: Güvenme dürtüsü. İnsanların biyometrik güvenlik sistemlerine, veya genel anlamda tüm güvenlik sistemlerine, güvenmesi o sistemlerin hem güvenliği hem de mahremiyeti ne derecede garanti ettiğine bağlıdır. İnsanların güvenini kazanacak bir biyometrik güvenlik sistemi, bir yandan güvenliği en yüksek derecede sağlayacak öznitelikler ve tanıma algoritmaları sunmalı bir yandan da kişiye özel biyometrikleri geri dönüştürülemeyecek fonksiyonlarla başka bir biçeme dönüştüren ve yeri geldiğinde de bu gizli biyometrik şablonu iptal edebilen yöntemleri içermelidir. O halde, başarılı bir biyometrik güvenlik sistemi mahremiyet-güvenlik arasındaki tezatı dikkate almalı buna ek olarak da mahremiyet-güven ve güvenlik-güven arasındaki paralelliği göz önünde bulundurmalıdır.

Mahremiyet-güvenlik-güven arasındaki ilişkiyi açıklamak ve bunu matematiksel bir model üzerinde yapmak biyometrik güvenlik sistemlerinin tasarlanmasında ve yeri geldiğinde mukayesesinde önemli bir yer tutar. Mahremiyetin ölçülmesinde genelde entropik hesaplamalara dayalı sızıntı oranları dikkate alınırken güvenliğin ölçülmesinde tanıma oranları, kullanılıyorsa sentetik anahtarların tekilliği gibi hususlara dikkat edilir. Literatürde mahremiyet-güvenlik arasındaki ilişkiyi formel yollarla betimleyen ve mahremiyeti ya da güvenliği nitel olarak ölçen yaklaşımlar mevcuttur. Oysaki mahremiyet ve güvenliğin, veya bu iki kavram arasındaki ödünleşimin güvenle ilişkisini gene formel olarak açıklayan bir yöntem bulunmamaktadır. Hele hele, bu üç kavram arasındaki karmaşık ilişkiye kamunun istekliliği (public willingness) ve kullanıcıların biyometriklerden emin olması (user confidence) gibi faktörleri de ekleyip

biyometrik teknolojilerin kabul edilebilirliğini inceleyen bir çalışma tarafımızca bilinmemektedir.

Bu tez çalışmasının en temel motivasyonu ve genel amacı geleceğin güvenlik uygulamaları olarak görülen kriptografi ile güçlendirilmiş biyometrik şablon koruma odaklı biyometrik kimlik yönetimi sistemlerinde mahremiyet-güvenlik-güven ilişkisini matematiksel bir yolla açıklayabilmektedir. Bu genel amaç doğrultusundaki özel amaçlar ise şöyle sıralanabilir:

1. Mahremiyet-güvenlik ödünleşiminin güvenle ilişkisini, kamunun istekliliği ve kullanıcıların biyometriklerden emin olma düzeyini de dikkate alarak matematiksel biçimde açıklamak.
2. Öznel bir kavram olan biyometrik güvenlik sistemlerine duyulan güveni mümkün olduğunca nesnel biçimde ölçebilmek.
3. Mahremiyet-Güvenlik-Güven ilişkisinden yararlanarak biyometrik teknolojilerin kabul modelini çıkarmak.
4. Örnek uygulamalarla bu ilişkileri ortaya koyarak genelleştirilmiş modeller için dayanak oluşturmak.

1.3 Önerilen Çözüm ve Yenilikler

Bu tez çalışmasında, güvenlik-mahremiyet ödünleşiminin güven üzerindeki etkisini incelemek için bir kabul olasılık fonksiyonu (acceptance probability function) önerilmiştir. Önerilen Güven fonksiyonu $T(\mathbf{P}, \mathbf{S})$, mahremiyet ($\mathbf{P}$) ve güvenlik ($\mathbf{S}$) değişkenlerinin bir isteğe bağlı fiyatlandırma (demand responsive pricing) yaklaşımı ile ölçülmesi esasına dayanır. Ekonomide ve telekomünikasyon alanında kullanılan bu yaklaşımda, servis edilen hizmetin hangi kaynağı ne kadar sömürdüğü ve buna karşın ne kadarlık bir fiyat ödendiği üstel bir fonksiyonla ifade edilir. Örneğin, telekomünikasyon sektöründe GSM operatörlerinin müşterilerine sunduğu farklı spektral verimlilikler, saniyede iletilen veri miktarı (bps) ve ödenen ücrete bağlı bir fonksiyon olarak betimlenebilir. Müşterilerin her bir teklife yaklaşımı aslında üstel bir kabul olasılık

yoğunluk fonksiyonu olarak gösterilebilir. Müşterinin önerilen spektral verimi kabul etmesi, hem saniyede iletilen veri miktarının çok olması hem de ücretin uygun olması ile sağlanabilir.

Biyometrik kimlik yönetimi sistemlerine duyulan güven de benzer biçimde bir kabul olasılık fonksiyonuna bağlanabilir. Güvenin sağlanması için hem mahremiyetin hem de güvenliğin kabul edilebilir düzeyde olması gerekir. Bu tez çalışmasında öne çıkan en büyük yenilik, güveni inşa eden kullanıcının biyometriklerden emin olması ve kamusal isteklilik faktörlerini de dikkate alan üstel bir kabul olasılık fonksiyonu ile mahremiyet-güvenlik ödünleşimi ve güven arasındaki ilişkiyi açıklamaktır. Önerilen bu matematiksel modele "BioPSTM - Biometric Privacy-Security-Trust Model" adı verilmiştir [3].

Mahremiyet-güvenlik ödünleşiminin ölçülmesi ve aralarındaki matematiksel ilişkinin formüle edilmesi de bu çalışmanın ilgi çekici yönlerindendir. Literatürdeki mevcut çalışmalardan esinlenerek önerilen bu formel yaklaşımda gelişmiş bir biyometrik kimlik yönetimi sistemindeki tüm bileşenler arasındaki sızma oranları (equivocation rate) hesaplanır. Bu çalışmada örnek olması açısından biyometrik kıyım, sentetik anahtar üretimi, sendrom kodlama gibi biyometrik kriptografide öne çıkan tüm bileşenleri içeren bir sistem üzerinde çalışılmıştır. Bu sistemde, biyometrik güvenlik ve mahremiyetle ilgili tüm tehditler analiz edilmiş ve ilgili bileşenler arasındaki sızıntı oranlarının entropik olarak nasıl ölçüleceği gösterilmiştir. Bu örnekten hareketle herhangi bir biyometrik güvenlik sisteminin mahremiyet-güvenlik ödünleşiminin nasıl ölçülebileceği gösterilmiş daha sonra güven ile ilişkisi BioPSTM ile ortaya konmuştur.

BioPSTM, biyometrik güvenlik sistemlerine duyulan güveni göstermede nesnel bir ölçüt sunar. Öyle ki, tasarımcılar bu ölçüte dayanarak biyometrik güvenlik sisteminin parametrelerini (tanımada kullanılan eşik değeri, sentetik anahtar uzunluğu, sendrom kodu uzunluğu, vs.) ayarlayabilirler. Güven, herhangi bir teknolojinin kabul edilebilirliğini etkileyen önemli bir unsur olarak ortaya çıkar. Ancak sadece bir sisteme güvenilip güvenilmediğini ölçmek o teknolojinin kabul edilip edilmediğini anlamakta yeterli olmayabilir. Güven herşeyden önce insanların algıladığı kullanım kolaylığını (perceived ease of use) etkileyen önemli bir unsurdur. Kullanım kolaylığı, biyometrik sistemdeki tüm yazılım ve donanım bileşenlerinin kullanıcıya bakan tarafının işler-

liği, pratikliği, anlaşılabilirliği ve kavranabilirliği gibi faktörlere bağlıdır. Buna ek olarak, kişinin arayüzlerle sunulan tüm bu yeteneklere güvenmesi, herhangi bir güvenlik veya mahremiyet riskinin oluşmayacağına inanması gerekir. Biyometrik teknolojilerin kabul edilebilirliğinde öne çıkan bir başka nokta ise algılanan kullanışlılıktır (perceived usefullness). Burada esas olan, kullanıcının biyometrik teknolojileri kullanarak zaman kazanacağına ve iş performansının iyileşeceğine ya da bu teknolojiyi kullanan kurumun kazançlarının artacağına inanmasıdır. Tüm bu algılar kullanıcının tutumunu ve dolayısıyla da biyometrik güvenlik sistemini kullanmadaki davranışsal niyetini belirler.

Bu tez çalışmasında öne çıkan bir diğer yenilik de insanların bir biyometrik güvenlik sistemini etkin biçimde kabul edip etmeyeceğini ölçebilecek bir model önerilmesidir. "BioTAM - Biometric Technology Acceptance Model" adı verilen teknoloji kabul modeli [4], BioPSTM ile açıklanan güven faktörünü, algılanan kullanışlılık ve kullanım kolaylığı, kullanıcı tutumu ve davranışsal niyet gibi etmenler arasındaki ilişkiyi ortaya koymaktadır. Tez çalışmasında İngiltere'de uygulanan bir biyometrik güvenlik sisteminin BioTAM ile incelenmesi de örnek uygulama olarak sunulmuştur.

BioPSTM ve BioTAM için kapsamlı deneyler ve anket çalışmaları yapılması gerekir. Bu tez kapsamında amaç matematiksel modelleri literatüre bir an önce kazandırmak olduğu için çok fazla emek gerektiren deneysel çalışmalara girilmemiştir. Bunun yerine, literatürde mevcut bazı analizlerin sonuçlarından yararlanılarak örnek uygulamalar yapılmıştır. Bu örnek uygulamalar Bölüm 4'te görülebilir. Tezin genel yapısı ise şöyledir: Bölüm 1'de genel bir giriş yapılarak çalışmanın motivasyonu ve yenilikçi yönleri vurgulanmıştır. Bölüm 2'de mahremiyet-güvenlik-güven arasındaki ilişkiye detaylı bir bakış ile birlikte mevcut literatür taraması verilmiştir. BioPSTM Bölüm 2'de sunulmuştur. Bölüm 3'te BioTAM tanıtılmış ve biyometrik kimlik yönetiminde nasıl kullanılabileceği gösterilmiştir. Bölüm 4'teki örnek uygulamaların ardından Bölüm 5'te elde edilen çıktılar ve çıkarımlar masaya yatırılmıştır.

2 Mahremiyet-güvenlik-güven arasındaki ilişki ve ilgili çalışmalar

2.1 Kriptografi ile Güçlendirilmiş Biyometrik Şablon Koruma

Son yıllarda biyometriklerin güvenlik sistemlerinde kullanılması çok sıcak araştırma konuları arasında yer almaktadır. Biyometrik, kişiye özel, tekil, ölçülebilen biyolojik veya davranışsal karakteristiklerdir. Bu karakteristiklerin istatistiksel yöntemlerle analiz edilmesi, işaret işleme teknikleri ile daha kolay temsil edilebilir hale dönüştürülmeleri, ayırt edici özellikleri belirlendikten sonra bu özelliklere göre tanıma yapılması ve buna benzer tüm yöntemler "biyometrik işaret işleme" araştırma alanı altında toplanabilir. En çok bilinen ve uygulama alanı bulan biyometrikler, parmak izi, yüz, konuşma, imza, iris, retina, el ayası, el geometrisi, tuşabasım ritmi, DNA ve vücut şeklidir.

Bunların yanında çok fazla uygulama alanı bulmasa da araştırmaları devam eden kulak şekli, RNA, EEG, EKG, vücut kokusu, oturma izi, davranış biçimi gibi çeşitli biyometrikler de bulunmaktadır. Bu örneklerden anlaşılacağı gibi biyometrikler sadece erişim kontrol amaçlı değil aynı zamanda kişi takibi, iş akış takibi, adli uygulamalarda bir olayın aydınlatılması gibi geniş uygulama alanlarına sahiptir [1; 2].

Geleneksel güvenlik sistemlerinde doğrulama, kişiye özel PIN veya parola ile ya da akıllı kart, token gibi bir araç aracılığıyla yapılmaktadır. Burada çok uzun tekil kriptografik anahtarlar kullanmak pratik olmayacağından bu anahtarları kişinin rızası doğrultusunda açığa çıkaran daha kolay hatırlanabilir karakter dizileri kullanılmaktadır. Genel anlamda parola diye tanımlanan bu diziler ortalama 6 karakter uzunluğunda olmakta ve birçok uygulamada sadece rakamlardan oluşmaktadır. Bu şüphesiz, kişiye özel parolanın daha kolay tahmin edilebileceği anlamına gelir. Bunun ötesinde birçok kullanıcı bu parolaları kullanırken dikkatsiz davranmakta, parolalar unutulmakta, kaybedilmekte hatta çalınabilmektedir. İşte bu noktada kişiye özel biyometriklerin güvenlik amaçlı kullanımı çok sıcak bir araştırma alanı haline gelmiştir. Biyometrik doğrulama ilk etapta anahtarı serbest bırakacak, alt katmandaki parola korumasından bağımsız bir yetkilendirme protokolü olarak kullanılsa da yapılan araştır-

malarla biyometriklerin sadece yetkilendirme için değil kişiye özel kriptografik anahtar üretmek, özel kıyım ve biyometrik güçlendirme fonksiyonları tasarlamak ve biyometrik kriptosistemler oluşturmak için de kullanılabileceği öne sürülmüştür [1]. Geleneksel biyometrik yetkilendirme çözümlerinde çok iyi tasarlanmış sınıflandırıcılar kullanılarak kişiye ait şablon veya modeller oluşturulmakta ve sahte-gerçek sınıf ayrımı arttırılmaya çalışılmaktadır. Yeni nesil biyometrik güvenlik uygulamalarında ise, kişiye ait öznitelikleri kötü niyetli kişiler tarafından tekrar üretilemeyecek tekil anahtarlara dönüştürmek, geri dönüşümsüz kıyım fonksiyonları ile gizliliği arttırmak ya da ayırt ediciliği arttıracak yardımcı fonksiyonlar kullanmak mümkün olabilmektedir. Burada amaç ayırt ediciliği sağlayarak tanıma başarımını düşüren problemlerle başa çıkmak ve her biyometrik veri tanıtımında kişisel bilgileri gizli tutacak, gerektiğinde iptal edilebilirliği sağlayacak bit dizilerini elde edebilen gürbüz algoritmalar bulmaktır. Bu alandaki çalışmalar genel anlamda "Kriptografi ile güçlendirilmiş biyometrik şablon koruma (Biometric template protecting enhanced with cryptography)" yöntemleri olarak anılabilir.

Kriptografi ile güçlendirilmiş biyometrik şablon korumada amaç biyometrik ayırt ediciliği mümkün olduğunca azaltmayan, aynı zamanda kişiye özel bu karakteristik bilgileri de sızdırmayan tanımlayıcı öznitelikler ve güçlü karşılaştırma algoritmaları tasarlamaktır. Biyometrik şablonun korunmasındaki temel amaç öncelikle mahremiyeti sağlamak, ardından gizliliği bir şekilde garanti altına alınmış kişisel bilgileri kullanarak en güvenli biçimde tanıma (sorgu verisini, kime ait olduğunu bilmeden bir küme içinde tarayan 1:N karşılaştırma yaklaşımı) veya doğrulama (sorgu verisini, o veriye sahip olduğu iddia edilen kişinin başka bir verisiyle 1:1 karşılaştırma yaklaşımı) yapabilmektir. Kriptografi ile güçlendirilmiş şablon koruma yöntemleri, geleneksel biyometrik tanıma yaklaşımlarının çok ötesinde, insanın biyolojik karakteristiklerinde oluşabilecek yapısal veya geçici değişimlerden bağımsız öznitelik çıkarma ve eşleştirme/karşılaştırma algoritmaları gerektiren çok sıcak bir araştırma alanıdır. Bu konuda araştırma yapılacaksa öncelikle yukarıda anılan özelliklerdeki algoritmaların tasarlanmasını böylesine zorlaştıran etmenleri gözden geçirmek gerekir. Biyometrik işaret işlemenin de temelini oluşturan bu temel problemler şunlardır:

1. Biyometriklerin doğasından gelen ayırt ediciliğin işaret işleme ve sınıflandırma

teknikleri ile sınırlı olarak ifade edilebilmesi: Biyometrik işaretler biyometriğin tipine göre farklı düzeylerde ayırt edicilik sağlamaktadır. Örneğin, parmak izi, iris, retina, DNA gibi biyometrikler konuşma, tuşabasım ritmi, vücut hareketleri gibi biyometriklere göre çok daha fazla ayırt ediciliğe sahiptir. Bu biyometriklerden bazıları veri toplamadaki sorunlar (kullanıcı direnişi, vücuttan bir parçayı gerektirmesi vb.), bazıları da veriyi işlemedeki zorluklar nedeniyle tercih edilmeyebilir. Bunun yanında, işaret işleme teknikleri ile çıkarılan öznitelikler, biyometrikleri mükemmel biçimde yansıtamadığından, gerçekte %100 ayrım sağladığına inanılan parmak izleri nispeten küçük veritabanlarında (örneğin 1000 kişi) yaklaşık %1 eşit hata oranı ile ancak ayrıştırılabilmektedir. Burada sınıflandırma ve öğrenme temelli algoritmalarla güçlendirme düşünülebilir. Biyometrik şablon koruma yöntemlerinde seçilen biyometrik hem çok iyi ayırt ediciliğe sahip olmalı, hem kolay işlenebilmeli hem de kullanıcılar tarafından geniş ölçekte kabullenilmelidir.

2. Biyometrik işaretlerdeki belirsizlikler: Biyometrik işaretler, tiplerine göre değişmekle beraber, özellikle çevresel etmenlerden, ışık koşullarından, poz değişimlerinden, dönme-öteleme-kayma problemlerinden, ölçek farklılıklarından, sensör farklılıklarından, verinin okutulması sırasında olabilecek ufak değişimlerden, biyometrikte oluşabilecek değişimlerden (yaralanma, bıyık, sakal, hastalık, vb.), kullanılan aksesuarlardan (gözlük, peruk, makyaj, atkı, bere, vb.), ve buna benzer birçok faktörden etkilenmektedir. Bunun yanında kimi zaman kötü niyetli kişiler kendi biyometriğini değiştirmekte veya başka birini taklit edebilmektedir. Tüm bunlar biyometrikteki entropiyi kriptografik anahtarlara kıyasla ciddi biçimde düşürebilmekte ve işaretteki belirsizliği arttırmaktadır. Bu nedenle bu problemleri asgari düzeye indirecek öznitelikler kullanmak; güçlü sınıflandırma, topaklama ve öğrenme temelli istatistiksel yöntemlere odaklanmak; ve kişiye ait birden fazla enformasyonu bir arada kullanmak hem anahtar üretimini hem de doğrulama başarımını arttıracak unsurlardır.

3. Tekrar üretilebilme ve iptal edilemezlik: Biyometrik işaretler her ne kadar kişiyi ifade eden tekil işaretler olsa da başka güvenlik açıkları verebilir. Örneğin, biyometrik, kötü niyetli kişiler tarafından çalınabilir ve tekrar üretilebilir. Bu durum, biyometriğin bir kere çalınmasıyla aslında sonsuza dek çalınmış olduğu

anlamına gelir. O nedenle biyometriğin kendisini kullanmaktansa herhangi bir yolla başka bir biçeme dönüştürülmüş halini kullanmak, ve gerektiğinde (biyometrik çalındığında) dönüşüm fonksiyonunu ya da parametrelerini değiştirerek kişiye ait şablonu yenilemek yeni bir araştırma alanı doğurmuştur. Burada dönüşüm sırasında biyometrik işaretteki entropiyi arttıracak, başka bir deyişle biyometriği güçlendirecek fonksiyonların bulunması, anahtar üretimi için gerekli olan daha güçlü sahte-gerçek sınıf ayrımını da sağlayabilir.

Literatürde bu problemlerle başa çıkmak için birçok yöntem önerilmiştir. Kimi araştırmacılar daha gürbüz öznitelikler elde etmeye uğraşmış, kimileri bu belirsizlikleri azaltacak gürültü giderme, düzgeleme gibi önişleme algoritmaları üzerinde çalışmış, kimileri biyometrikteki entropiyi arttıracak yardımcı enformasyonları bir arada kullanacak katıştırma (füzyon) teknikleri geliştirmiş, kimileri de modelleme ve karar verme mekanizmalarında iyileştirmeler önermiştir.

2.2 Mahremiyet-güvenlik-güven arasındaki ilişki

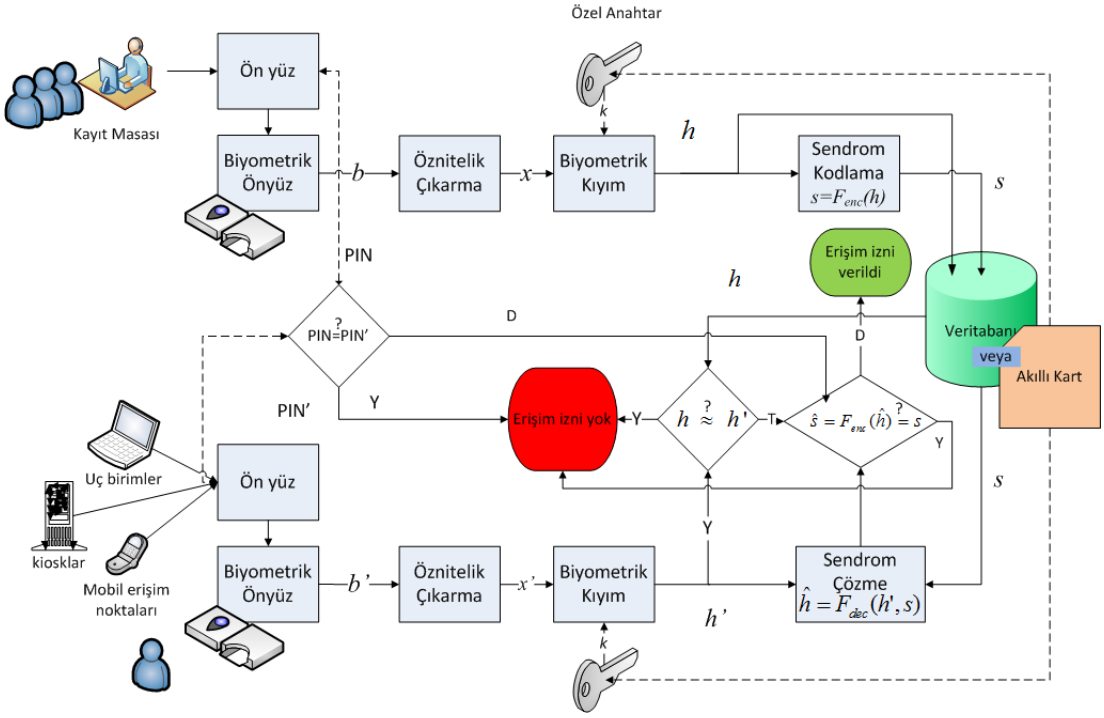
2.2.1 Gelişmiş bir Biyometrik Kimlik Yönetimi Sistemi

Tipik bir Biyometrik Kimlik Yönetimi Sistemi'nde (BKYS) kullanıcıların sisteme kayıt yaptırdığı kayıt noktaları ve daha sonra hizmet aldıkları kiosklar, terminaller ve mobil cihazlardan oluşan uç noktaları bulunur. Biyometrik kayıt (enrolment) genelde bu kayıt noktalarında tamamlanır ve kullanıcılara akıllı kart gibi erişim materyalleri ile birlikte sisteme girişte kullanılacak PIN numaraları ya da şifreler verilir. Biyometrik kayıt da bu esnada tamamlanır ve verilen şifreler aktive edilir. BKYS çözümlerinin çoğunda biyometrik imza, merkezi bir veritabanında saklanır ve doğrulama da merkezi sunucularda gerçeklenir. Doğrulama esnasında biyometrik imza ya akıllı karttan ya da merkezi veritabanında daha önceden saklı şablon veriden alınır ve biyometrik sensöre o an tanıtılan sorgu verisi ile karşılaştırılır. Bu tip merkezi uygulamaların hem avantajları hem de dezavantajları olabilir. Örneğin, doğrulama ve kayıt için güçlü sunuculardan yararlanmak, yedekleme mekanizmalarından faydalanmak mümkün olurken bir taraftan da özellikle istihbari açıdan fayda sağlanabilir. Ancak bu tip merkezi sistemlerin en zayıf yanı mahremiyet çekinceleri ve kişisel bilgilerin

gizliliği ile ilgili tartışmalardır. O nedenle son yıllarda "Match-on-Device - Cihaz üzerinde Eşleme" ve "Match-on-Card - Kart üzerinde Eşleme" teknolojileri geliştirilerek biyometrik verinin geniş bir ağda açığa çıkmasını engelleyecek ve eşleştirmeyi hemen o anda ya kişiye ait bir medyada (akıllı kart gibi) ya da güvenliği garanti altına alınmış bir terminalde yapacak çözümler geliştirilmiştir.

Mahremiyeti ve güvenliği sağlamada cihaz veya kart üzerinde eşleme tekniklerini kullanmak nispeten rahatlatıcı önlemler olarak görülse de problemi tam olarak çözemez. Zira, gelişen yan kanal analizi, tersine mühendislik, ağ güvenliğini riske edecek siber saldırılar biyometrik imzaların güvenliğini ve gizliliğini tehlikeye atabilir. O nedenle daha gürbüz doğrulama ve şifreleme yöntemleri, özel sentetik anahtarlarla güçlendirilmiş daha gelişmiş biyometrik imzaların kullanılması gündeme gelmiştir. Bu tez çalışmasının da önemli ayaklarından birini oluşturan kriptografi ile güçlendirilmiş biyometrik şablon koruma teknikleri sayesinde hem güvenliği hem de mahremiyeti sağlayacak bir yapı ele alınabilir. Bu çalışmada ele alınan BKYS, biyometrik kriptosistemler [5] ve biyo-kıyım (biohash [6]) yöntemlerini etkin biçimde kullanan yeni nesil uygulamalara bir örnek olarak seçilmiştir. İstendiği takdirde bu örnek uygulamanın bazı bileşenleri dikkate alınmadan daha basit çözümler de düşünülebilir ve tasarıma yansıtılabilir.

Şekil 2.1'de gösterilen BKYS, tüm biyometrik güvenlik sistemlerinde olduğu gibi, iki ana fazdan oluşur: Kayıt ve doğrulama. Kayıt fazında, biyometrik sensör aracılığıyla alınan biyometrik işaret (b) çeşitli işaret işleme teknikleri ile bir öznitelik vektörüne (örneğin, x) dönüştürülür. Daha sonra x, geridönüşümsüz (non-invertible) özel kriptografik kıyım fonksiyonları ile belirli uzunluktaki ikili (binary) katarlara çevrilir. Bu ikili katarlara biyo-kıyım (biohash, h) adı verilir. Biyo-kıyım fonksiyonları biyometrik işaretteki belirsizlikleri mümkün olduğunca tolere edecek şekilde tasarlanmalıdır. Biyometrik veri alımında ortam koşulları, pozisyon değişimleri ve benzeri dış faktörlerden kaynaklanan belirsiz durumlar her defasında farklı bir biyo-kıyım çıkmasına neden olabilir. O nedenle biyo-kıyımda kullanılacak fonksiyon ve daha sonra biyo-kıyımları karşılaştırmada seçilen yöntemler, geleneksel kriptografik yöntemlerden farklı olarak, bu belirsizlikleri dikkate almalıdır. Bu tez çalışmasında seçilen örnek biyo-kıyım yöntemi Teoh ve arkadaşları tarafından 2004 yılında önerilen rasgele üretilmiş işaret dizileri ile biyometrik işareti iç çarpım yoluyla çırpan (scrambling)



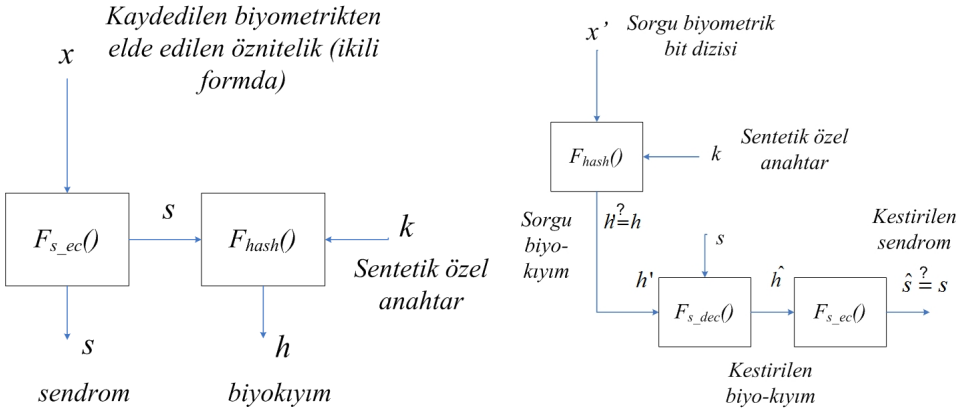
Şekil 2.1 Gelişmiş bir BKYS.

genel-geçer bir tekniğe dayanır [6]. Bu teknik, sonraki yıllarda daha da geliştirilmiş ve birçok farklı biyometriğe uyarlanmıştır. Seçilen bu biyo-kıyım yönteminde rasgele işaret dizilerinin oluşturulmasında kişiye ait özel anahtarlardan yararlanılır (k). k nın üretilmesinde rasgele sayı üreteçlerinden faydalanılır. Biyo-kıyım yöntemiyle hem kişisel bir bilgi olan biyometrik işaretlerin gizlenmesi, hem de sentetik anahtarlarla biyometriklerdeki belirsizliklerin mümkün olduğunca giderilmesi sağlanır.

Sentetik özel anahtarların kullanılması her zaman kesin çözüm anlamına gelmez. Zira, üretilen sentetik bilgi biyometrik bilgiye göre daha baskın bir hale gelirse biyometrik ayırt ediciliğin bir anlamı kalmaz ve sanki sadece PIN'le doğrulama yapılıyormuş gibi bir durum ortaya çıkar. O nedenle tasarımcının tüm sentetik anahtarların bilindiğini varsayması ve en azından sadece biyometriklerin kullanıldığı durumdaki ayırt ediciliğin garanti edilmesini sağlaması gerekir. Özel anahtar kullanmanın getirdiği bu riski bertaraf etmek ve biyometrik işaretteki berlirsizliklere gürbüz bir doğrulama mekanizması geliştirmek için sendrom kodlama yaklaşımı tercih edilir. Bu yöntemle, biyometrik işareti uzayda tanımlı kodsözcüklerine çeşitli geri dönüşümsüz fonksiyonlarla eşleştirmek ve doğrulamayı bu uzayda yapmak amaçlanır. Şekil 2.1'deki BKYS'de de görüleceği gibi güvenliği ve gizliliği arttırmak için öncelikle b biyomet-

rik işaretinden elde edilen x biyometrik özniteliğine biyo-kıyım foksiyonu uygulanarak $h = F_{hash}(x)$ elde edilir. Ardından, biyo-kıyım katarına (h), sendrom kodlama [7; 8] uygulanarak $s = F_{enc}(h)$ sendromu üretilir. Sonuç olarak, sendrom s ve biyo-kıyım h akıllı kartta veya güvenli bir merkezi sunucuda PIN numarası ile birlikte saklanır. Böylece, orijinal biyometrik bilgi yerine istenildiği zaman iptal edilebilecek ve tekrar üretilebilecek, kötü niyetli kişilerin hiçbir işine yaramayacak iki bit dizisi elde edilmiş olur.

Doğrulama fazında ise üç ayaklı bir sorgulama yapılır. Öncelikle o an girilen PIN numarası ile kartta veya sistemde kayıtlı olan numara (PIN') karşılaştırılır. Eğer doğrulama yapılırsa, iki aşamalı bir sorgulama daha yapılır. Öncelikle sorgu biyometriğinden (b') elde edilen (x') özniteliğine gene aynı kıyım fonksiyonu uygulanarak ($h' = F_{hash}(x')$) elde edilir. Eğer h ve h' belirli oranda birbirine benziyorsa (Hamming uzaklıkları yeterince yakınsa) sendrom kod çözücü devreye girer. h' ve sistemde/kartta kayıtlı sendrom s girdi olarak alınır ve kod çözme fonksiyonu işletilir: $\hat{h} = F_{dec}(h', s)$. Ardından $\hat{h}$ tekrar sendrom kodlamaya tabi tutularak $\hat{s} = F_{enc}(\hat{h})$ elde edilir. s ve $\hat{s}$ birebir aynıysa doğrulama başarılı olur. Bu üç ayaklı mekanizmanın herhangi bir aşamasında başarısızlık olursa doğrulama da başarısız sayılır ve BKYS uyarı verir. x; s; h, ve k değişkenleri X; S; Θ ve κ olasılık yoğunluk fonksiyonları ile temsil edilebilir. Biyometrik kayıt ve doğrulama fazlarının kavramsal gösterimi Şekil 2.2'de görülebilir.



Şekil 2.2 Gelişmiş bir BKYS'de kayıt (a) ve doğrulama (b) bileşenleri.

Bir BKYS'nin güvenli ve mahremiyete saygılı olması için şu temel şartları sağlaması gerekir:

- Sahte (impostor) ve gerçek (genuine) sınıf dağılımlarının birbirinden yeterince ayrık olması gerekir ki biyometrik doğrulamada hatalı kabul ve hatalı red olasılığı minimum düzeyde kalsın.

- Sentetik olarak bir rasgele sayı üreteci ile oluşturulan özel anahtarlar tahmin edilemez olmalı ve mümkün olan en üst düzeyde rasgele oluşturulmalıdır.

- Biyo-kıyım algoritması öyle tasarlanmalıdır ki oluşturulan biyo-kıyım orijinal biyometrikle ilgili bilgi içermemeli ve çok yüksek ayırt ediciliğe sahip olmalıdır.

- Sendrom kodlama ile oluşturulan biyometrik sendromlar hem kişisel bilgi sızdırmayacak şekilde tasarlanmalı hem de güçlü hata düzeltme mekanizmaları ile kendisine girdi olarak verilen biyo-kıyımları hatasız biçimde geriçatmalıdır.

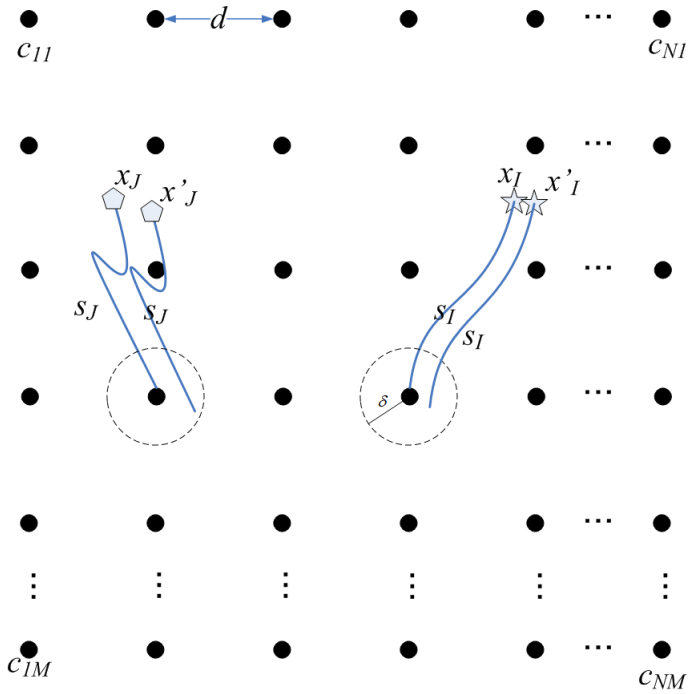
- BKYS'deki tüm bileşenler arasında herhangi bir kişisel bilginin sızmaması ve bir güvenlik açığının olmaması gerekir.

2.2.2 Mahremiyet ve Güvenlik Riskleri

Bu çalışmada ele alınan sendrom oluşturma yöntemi literatürde bulanık özütleyici (fuzzy extractor) [7] yönteminden türetilen gizli taslak (secure sketch [8]) yöntemi olarak da bilinmektedir. Bu yöntemde bir kod sözcüğü uzayı C, d parametresi ile tanımlıdır. d bir vektör de olabilir. Şekil 2.3'te iki boyutlu örnek bir uzay, d uzaklığı ile betimlenmiştir. Bu yaklaşımda her bir biyometrik işaret bu uzayda herhangi bir noktaya düşebilir. Biyometrik işaret, sendrom kodlama (encoding) fonksiyonu ile dönüştürülür ve belirli bir δ toleransı ile kendisine en yakın kod sözcüğüne eşlenir [9; 10]. Sorgu biyometriği gene aynı fonksiyondan geçirildiğinde kayıt biyometriğinin eşlendiği kod sözcüğüne yeterince yakınsa (kod sözcüğünün δ komşuluğunda ise) sendrom kod çözücü başarılı sayılır.

Sendrom kodlama yaklaşımında çeşitli riskler ortaya çıkabilir:

1. Durum I: Birbirinden çok iyi ayrılabilen farklı iki biyometrik dizi aynı kod sözcüğüne eşlenebilir. Bu durumda geri dönüştürmede hangi biyometrik kaynağın seçileceği problemi ortaya çıkar (bkz. Şekil 2.4-a).



Şekil 2.3 Gizli Sendrom Kodlama.

2. Durum II: Farklı kişilere ait olsa da uzayda birbirine benzeyen iki biyometrik dizi aynı kod sözcüğüne eşlenebilir. Bu durumda hatanın biyometrik ön işlemeden mi yoksa sendrom üreten şifreleme algoritmasından mı kaynaklandığı bilinemez (bkz. Şekil 2.4-b).

3. Durum III: d parametresi öyle bir seçilir ki uzaydaki kod sözcükleri birbirinden çok uzakta kalır. Böyle bir durumda biyometrik çeşitlilikten yeterince sağlıklı biçimde sendrom çeşitliliğine geçilemez (bkz. Şekil 2.4-c).

4. Durum IV: d parametresi öyle bir seçilir ki kod sözcükleri birbirine çok yakın durur. Bu durumda çözümleme sırasında yanlış kod sözcüğüne eşleme olasılığı artar (bkz. Şekil 2.4-d).

Bu dört durum Şekil 2.4'te temsili olarak gösterilmiştir. Tasarımcının, sendrom fonksiyonunu seçerken en optimum çözümü bulması gerekir.

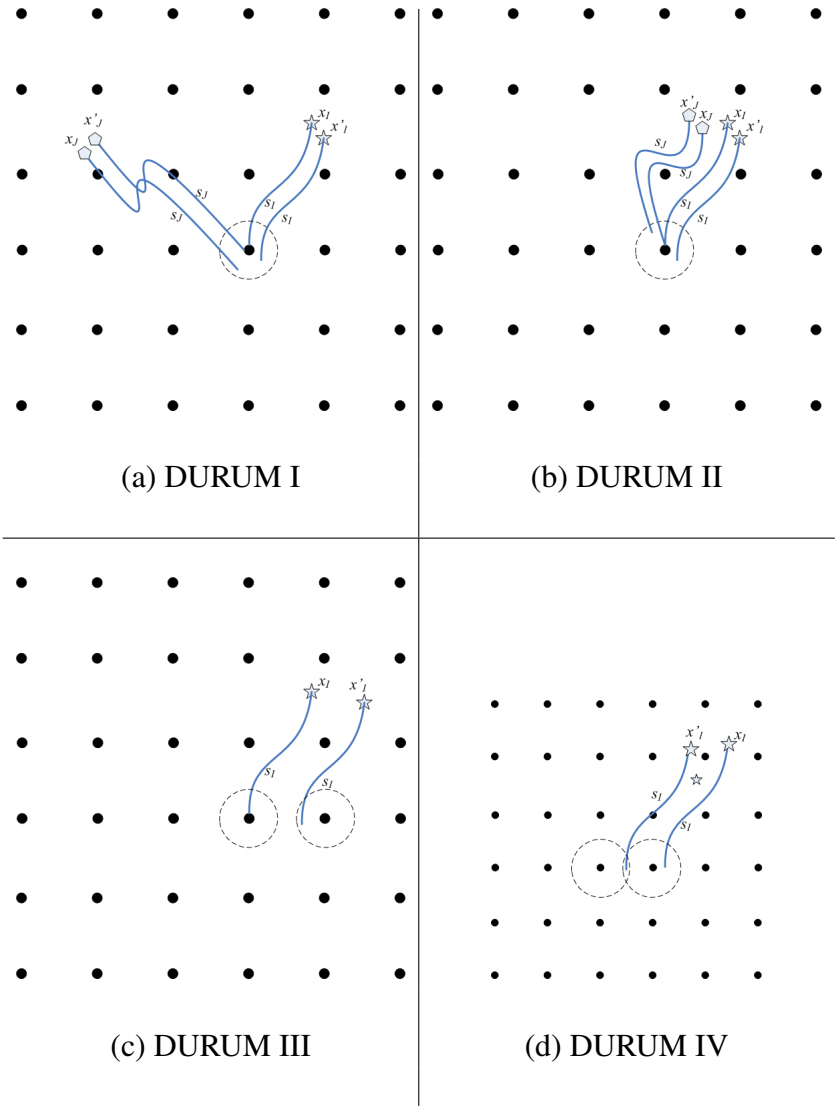
Sendrom kodlama dışında biyometrik kıyımla ilgili de riskler bulunabilir:

1. Durum V: Biyometrik ayırt edicilik yüksek iken farklı anahtarlar kullanılsa bile aynı kıyım sonucunun elde edilmesi ($h_I = h_J$, Şekil 2.5-a). Bu durumda problem kıyım fonksiyonundadır. Bazı uç durumlarda, aynı anahtar kullanılması halinde biyometrik ayırt edicilik yüksek bile olsa aynı kıyım sonucu çıkabilir. Bu durumda anahtar, kıyım oluşturmada biyometrik işarete göre ciddi biçimde baskındır. Böyle bir sistemde biyometrik bileşeni kullanmanın bir anlamı kalmaz.

2. Durum VI: Biyomerik ayırt edicilik yüksek değilken aynı veya farklı anahtarlar kullanıldığında aynı kıyım sonucunun elde edilmesi (Şekil 2.5-b). Bu durumda ya biyometrik önişlemede, ya anahtar üretiminde ya da kıyım fonksiyonunda problem olabilir. Bu durumların detaylı biçimde incelenmesi gerekir.

2.2.3 Mahremiyet - Güvenlik Ödünleşiminin Formel Gösterimi

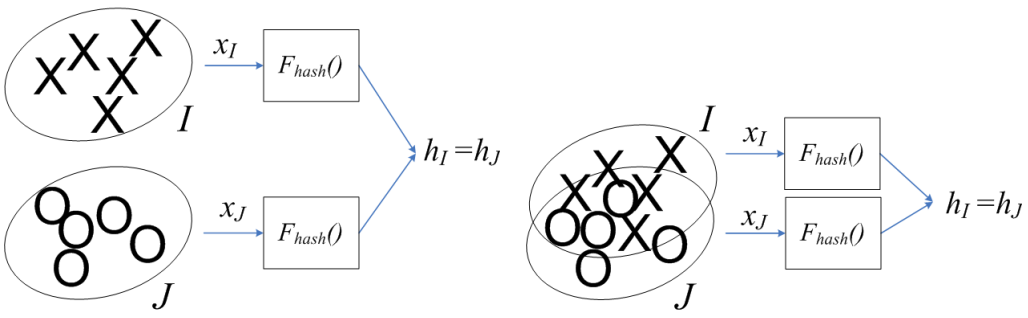
Mahremiyet ve güvenlik arasındaki ödünleşim yıllardır üzerinde durulan bir tartışma konusudur. Şekil 2.6'da kavramsal olarak gösterildiği gibi güvenliğin çok kri-



(a) DURUM I (b) DURUM II

(c) DURUM III (d) DURUM IV

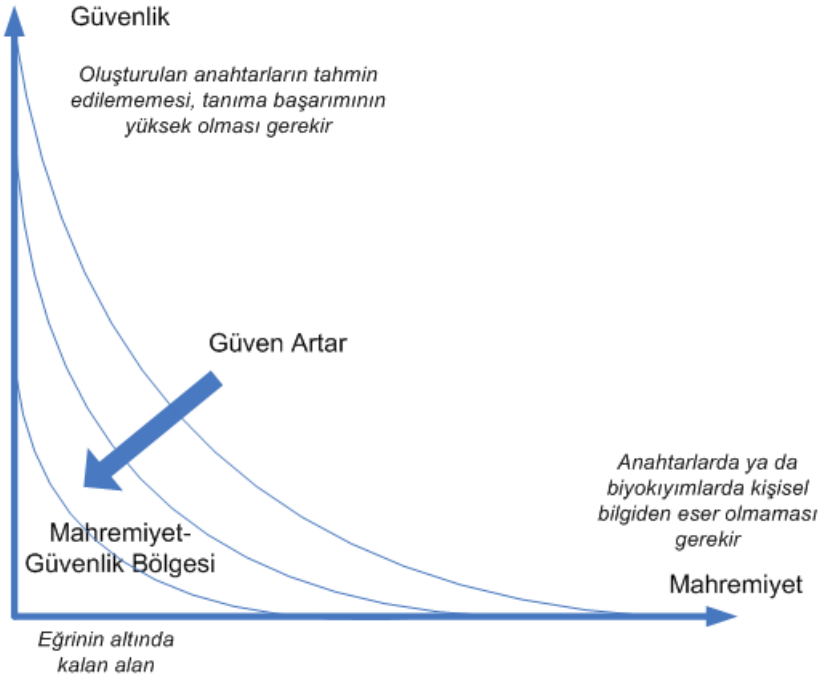
Şekil 2.4 Sendrom Kodlama ile İlgili Riskler.



(a) DURUM V (b) DURUM VI

Şekil 2.5 Biyometrik Kıyımla İlgili Riskler.

tik olduğu uygulamalarda mahremiyet ikinci planda tutulur. Örneğin, askeri ve istihbari uygulamalarda kişisel gizlilik kritik bir kural ihlalinin yapılmasından veya suç işlenmesinden daha önemli değildir. Bunun yanında bazı özel uygulamalarda, örneğin bankacılık, sosyal güvenlik, vs., kişisel gizlilik öne çıkar. Mahremiyette genelde biyometrik bilginin sızdırılmaması; güvenlikte ise biyometrik imzanın (biyometrik anahtar) tanımada ne kadar ödün verdiği dikkate alınır. Şekil 2.6'daki kavramsal ödünleşim eğrisi orijine yaklaştıkça insanların biyometrik kimlik yönetimi sistemine güvenleri artar.



Şekil 2.6 Mahremiyet-Güvenlik Ödünleşimi.

Mahremiyet-güvenlik ödünleşiminin gösteriminde yukarıda anılan güvenlik-mahremiyet şartlarının sağlanması ve yukarıda altı durumla ifade edilen risklerin dikkate alınması gerekir. Literatürde birçok farklı yaklaşım olsa da güvenlik-mahremiyet ödünleşiminin formel bir dille ifade edilmesi için normalize sızıntı oranının kullanılması öngörülmüştür [11]. Bunun yanında başka kriterler de kullanılabilir. Ancak aritmetik işlemlerde sağladığı kolaylık nedeniyle bu oran seçilmiştir. Normalize sızıntı oranının tanımı şöyledir:

Tanım:

$X = \{X_1, X_2, \ldots\}$ ve $Y = \{Y_1, Y2, \ldots\}$ iki rassal proses olmak üzere X ile Y arasın-

daki normalize sızıntı oranı:

$$\Psi_{XY} = \frac{H(X|Y)}{H(X)} \tag{2.1}$$

Burada, $H(\bullet)$ entropi fonksiyonudur. Ψ_{XY} oranının 1'e yakın olması Y nin X hakkında bir bilgi kaçırmadığı anlamına gelir.

Güvenlik Gerekleri

Yukarıda verilen tanıma istinaden bir biyometrik kimlik yönetimi sisteminin güvenli olması için aşağıdaki şartların sağlanması gerekir. x; s; θ ve k bileşenleri arasındaki ilişki için Şekil 2.2'ye bakılabilir. Bahsi geçen bileşenleri betimleyen olasılık yoğunluk fonksyionları X; S; Θ ve κ) olarak ifade edilmiştir.

- κ ve S arasındaki sızıntı en düşük düzeyde olsun ($\Psi_{\kappa S}$ 1'e yakın olsun)
- κ ve Θ arasındaki sızıntı en düşük düzeyde olsun ($\Psi_{\kappa\Theta}$ 1'e yakın olsun)
- S ile Θ arasındaki sızıntı en düşük düzeyde olsun ($\Psi_{S\Theta}$ 1'e yakın olsun)
- m uzunluğundaki biyometrik bit dizisinin ortalama entropisi mümkün olduğunca yüksek olsun: $1/mH(X) \leq R_X$ (sınıflar arası değişinti yüksek olsun). Burada $R_X \leq 1$ sabit pozitif bir gerçel sayıdır.

Bu şartları bir arada ifade etmek için **S** güvenlik faktörünün hesaplanması gerekir (Bkz. Denklem:2.2):

$$\begin{aligned} \mathbf{S} &= \frac{1}{m} H(X) \Psi_{\kappa S} \Psi_{\kappa\Theta} \Psi_{S\Theta} \\ &= \frac{1}{m} H(X) \frac{H(\kappa|S)}{H(\kappa)} \frac{H(\kappa|h)}{H(\kappa)} \frac{H(S|\Theta)}{H(S)} \end{aligned} \tag{2.2}$$

Mahremiyet gerekleri

Yukarıda verilen tanıma istinaden bir biyometrik kimlik yönetimi sisteminin mahremiyeti güvence altına alması için şu şartları sağlaması gerekir:

- X ve S arasındaki sızıntı en düşük düzeyde olsun (Ψ_{XS} 1'e yakın olsun)

- X ve Θ arasındaki sızıntı en düşük düzeyde olsun ($\Psi_{X\Theta}$ 1'e yakın olsun)
- S ile Θ arasındaki sızıntı en düşük düzeyde olsun ($\Psi_{S\Theta}$ 1'e yakın olsun)
- n uzunluğundaki özel anahtarın ortalama entropisi mümkün olduğunca yüksek olsun: $1/nH(\kappa) \leq R_k$ (sınıflar arası değişinti yüksek olsun). Burada $R_k \leq 1$ sabit pozitif bir gerçel sayıdır.

Bu şartları bir arada ifade etmek için **P** mahremiyet faktörünün hesaplanması gerekir (Bkz. Denklem:2.3):

$$\begin{aligned} \mathbf{P} &= \frac{1}{n} H(\kappa) \Psi_{XS} \Psi_{X\Theta} \Psi_{S\Theta} \\ &= \frac{1}{n} H(\kappa) \frac{H(X|S)}{H(X)} \frac{H(X|\Theta)}{H(X)} \frac{H(S|\Theta)}{H(S)} \end{aligned} \tag{2.3}$$

P ve **S** birbiriyle ters orantılı olarak basit bir aritmetikle şu şekilde formule edilebilir:

$$\begin{aligned} \mathbf{P}.\mathbf{S} &= \frac{1}{mn} H(\kappa|S) H(X|S) \frac{H(\kappa|\Theta)}{H(\kappa)} \frac{H(X|\Theta)}{H(X)} [\frac{H(S|\Theta)}{H(S)}]^2 \\ &= \frac{1}{mn} H(\kappa|S) H(X|S) \Psi_{\kappa\Theta} \Psi_{X\Theta} [\Psi_{S\Theta}]^2 \end{aligned} \tag{2.4}$$

2.4 denkleminde hesaplanan mahremiyet-güvenlik ödünleşim değeri 1'e yaklaştıkça hem mahremiyet açısından hem de güvenlik açısından mükemmel bir BKYS'ye yakınsanmış olur.

Mahremiyet ve güvenlik arasındaki bu ilişkiden yararlanarak farklı uygulama alanlarına uyarlanabilecek farklı güven modelleri tanımlanabilir. Örneğin, bir modelde mahremiyet ve güvenliğe ek olarak kamusal isteklilik tek ve geçerli faktör olarak tanımlanabilirken, bir başka model kamusal isteklilik yanında insanların kullanılan teknolojiden emin olma düzeyini (user confidence) de dikkate alabilir. Uygulamaya göre mahremiyet ve güvenlik için ağırlıklandırma yapılabilir. Bölüm 2.2.4 ve 2.2.5'te önerilen kullanıcı kabul olasılık fonksiyonları temel alınarak güveni etkileyen farklı faktörler yeni bir parametre olarak devreye alınabilir.

2.2.4 BioPSTM (Alternatif #1)

BioPSTM [3], gelişmiş BKYS'lere kullanıcıların duyacağı güveni mahremiyet-güvenlik ödünleşimi üzerine inşa eden matematiksel bir modeldir. BioPSTM'de güven (T), mahremiyet (**P**) ve güvenlik (**S**) faktörlerinin bir kabul olasılık fonksiyonu olarak ifade edilir. Burada T aslında insanların bir BKYS'yi hangi düzeyde mahremiyet ve güvenlik bedeli ile kabul edeceklerini ifade eden üstel bir fonksiyondur. BioPSTM, bu üstel foksiyonu temel alarak insanların bir BKYS'ye ne derecede güveneceğini ölçmeye yarayan matematiksel bir yaklaşımdır. BKYS'de **P** ve **S** haricinde kamusal isteklilik (ω , public willingness) ve kullanıcının biyometriklerden emin olma düzeyi (c , user confidence) de parametrik olarak yer alır. ω insanların bir BKYS'i kullanma istekliliğini ifade eder ki kimi zaman ya "büyük birader" korkusuyla ya da mevcut iş akışına yük getirdiği algısı nedeniyle bu oran düşük çıkabilir. c ise daha ziyade hangi biyometrik kipin (parmak izi, yüz, iris, DNA, vs.) kullanılacağı ve biyometrik yetkilendirmenin ne amaçla bir süreç haline getirildiği ile ilgilidir. Kullanıcılar, örneğin parmak izinin eDevlet uygulamalarında kullanılması konusunda ne kadar az endişeli ise (kendilerini rahat hissediyorlarsa) c değerinin de o kadar yüksek çıkması beklenir.

T nin yüksek çıkması için insanların genel anlamda istekli olmaları ve sistemle ilgili fazla endişe duymamaları gerekir. Buna ek olarak da hem **P** faktörünün hem de **S** faktörünün 1'e yakın olması istenir ki böylece mahremiyet ve güvenlik çekinceleri minimum düzeyde kalsın. O nedenle seçilen $T(\mathbf{P}, \mathbf{S})$ fonksiyonu, mahremiyet ve güvenlik arasındaki pariteyi çok iyi yansıtmalıdır.

Bir BKYS'ye duyulan güveni, o sistemi kurmadan ölçmek aslında pek mümkün değildir. Zira, insanların sisteme güven duyup duymadıklarını gerçek anlamda anlamak için bir mahremiyet veya güvenlik açığının ortaya çıkması gerekir. Ancak güven, mahremiyet-güvenlik ödünleşimini ölçmek yoluyla belirli bir düzeyde öngörülebilir. BKYS'deki temel bileşenler arasındaki normalize sızıntı oranlarını ölçerek, entropik hesaplamalarla anahtarların ve biyometrik işaretlerin rasgeleliliğini gözlemleyerek en azından güven ile ilgili nesnel çıkarımlarda bulunmak mümkün olabilir. BioPSTM, nesnel bir yaklaşımla öznel bir kavram olan güveni ölçmede kullanılabilir.

BioPSTM, Badia ve arkadaşları tarafından 2003 yılında önerilen ve isteğe bağlı

fiyatlandırmaya dayalı bir kullanıcı kabul modelinden esinlenerek geliştirilmiştir [12]. Bu kullanıcı kabul modeli ekonomide ve telekomünikasyon alanında özellikle müşteri memnuniyeti ve servis kalitesinin ölçümünde de kullanılmıştır. BioPSTM, tipik bir BKYS'de servis edilen hizmetin hangi kaynağı ne kadar sömürdüğü ve buna karşın ne kadarlık bir fiyat ödendiğini üstel bir fonksiyonla ifade eder. Biyometrik teknolojilerle ilgi kurulduğunda BKYS'yi kullanıma açan yüklenici varlığın (şirket, devlet, kamu iştiraki, vs.) kullanıcılara sunduğu biyometrik doğrulama hizmeti, kullanıcıların mahremiyet ve güvenlik faktörlerinin bir fonksiyonu olarak betimlenebilir. Burada gereksinimlere göre farklı düzeyde mahremiyet ve güvenlik teklifleri sunulabilir. Kullanıcıların her bir teklife yaklaşımı aslında üstel bir kabul olasılık fonksiyonu olarak gösterilebilir. Müşterinin önerilen T değerini kabul etmesi için **P**, **S**, ω ve c değerlerinin 1'e yakın olması gerekir.

Bu alanda öne çıkan araştırmalardan biri İleri ve arkadaşları tarafından 2005 yılında önerilmiştir [13]. Telekomünikasyon sektöründeki frekans spektrum politikası ile ilgili olarak önerilen yöntemde bir $A(u;p)$ kullanıcı kabul olasılık fonksiyonu tanımlanmıştır. Burada u haberleşme verimliliği (utility), p ise ödenen para miktarıdır. BioPSTM de benzer biçimde bu ilişkiyi uyarlayarak bir kullanıcı kabul fonksiyonu önermektedir. Bu fonksiyonun nicel özellikleri şöyle olmalıdır (Bkz. Denklemler 2.5-2.7):

$$\frac{\partial T}{\partial \mathbf{P}} \leq 0, \frac{\partial T}{\partial \mathbf{S}} \leq 0, \omega > 0, c > 0 \tag{2.5}$$

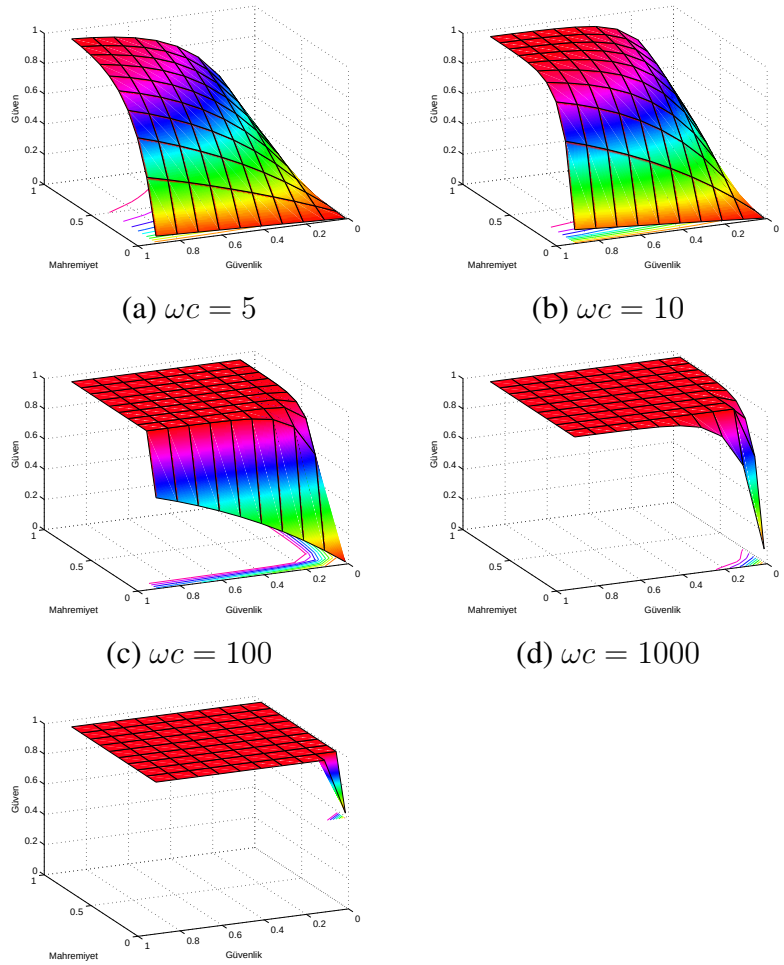
$$\forall \mathbf{P} > 0, \lim_{\mathbf{S} \longrightarrow 0} T(\mathbf{P}, \mathbf{S}) = 0, \lim_{\mathbf{S} \longrightarrow \infty} T(\mathbf{P}, \mathbf{S}) = 1, \tag{2.6}$$

$$\forall \mathbf{S} > 0, \lim_{\mathbf{P} \longrightarrow 0} T(\mathbf{P}, \mathbf{S}) = 0, \lim_{\mathbf{P} \longrightarrow \infty} T(\mathbf{P}, \mathbf{S}) = 1 \tag{2.7}$$

Bu özellikler ışığında, seçilecek fonksiyonla ifade edilen T nin **P** veya **S** sıfıra yaklaşırken sıfıra yaklaşması; **P** veya **S** sonsuza yaklaşırken de T nin 1 e yakınsaması gerekir. Buna ek olarak, T nin **P** ve **S** ile paralel olarak, **P** veya **S** arttığında artarak 1 e; **P** veya **S** azaldığında ise 0 a yakınsaması gerekir. Bu kısıtlar ışığında önerilen güven fonksiyonu şöyledir (Bkz. Denklem 2.8):

$$T(\mathbf{P}, \mathbf{S}) = 1 - e^{-\omega c \mathbf{PS}} \tag{2.8}$$

ω ve c parametreleri T değerini ayarlamada öne sürülen kamusal isteklilik ve kullanıcıların biyometriklerden emin olma düzeyini ifade eder. Empirik çalışmalar göstermiştir ki, ω ve c için 5'ten büyük değerler uygun değildir. Zira 3 boyutlu uzayda gözlenen güven yüzeyi büyük değerler için yeterince ayırt edici olmaz. Şekil 2.7'de de görülebileceği gibi, bu değerler arttıkça sanki BKYS'ye güven tammış gibi algılanır ve **P** ile **S** nin etkinliği kaybolur. O nedenle ω ve c için, MOS puanlamada (Mean Opinion Score) olduğu gibi, 1-5 arası derecelendirme önerilmektedir.



(a) $\omega c = 5$ (b) $\omega c = 10$

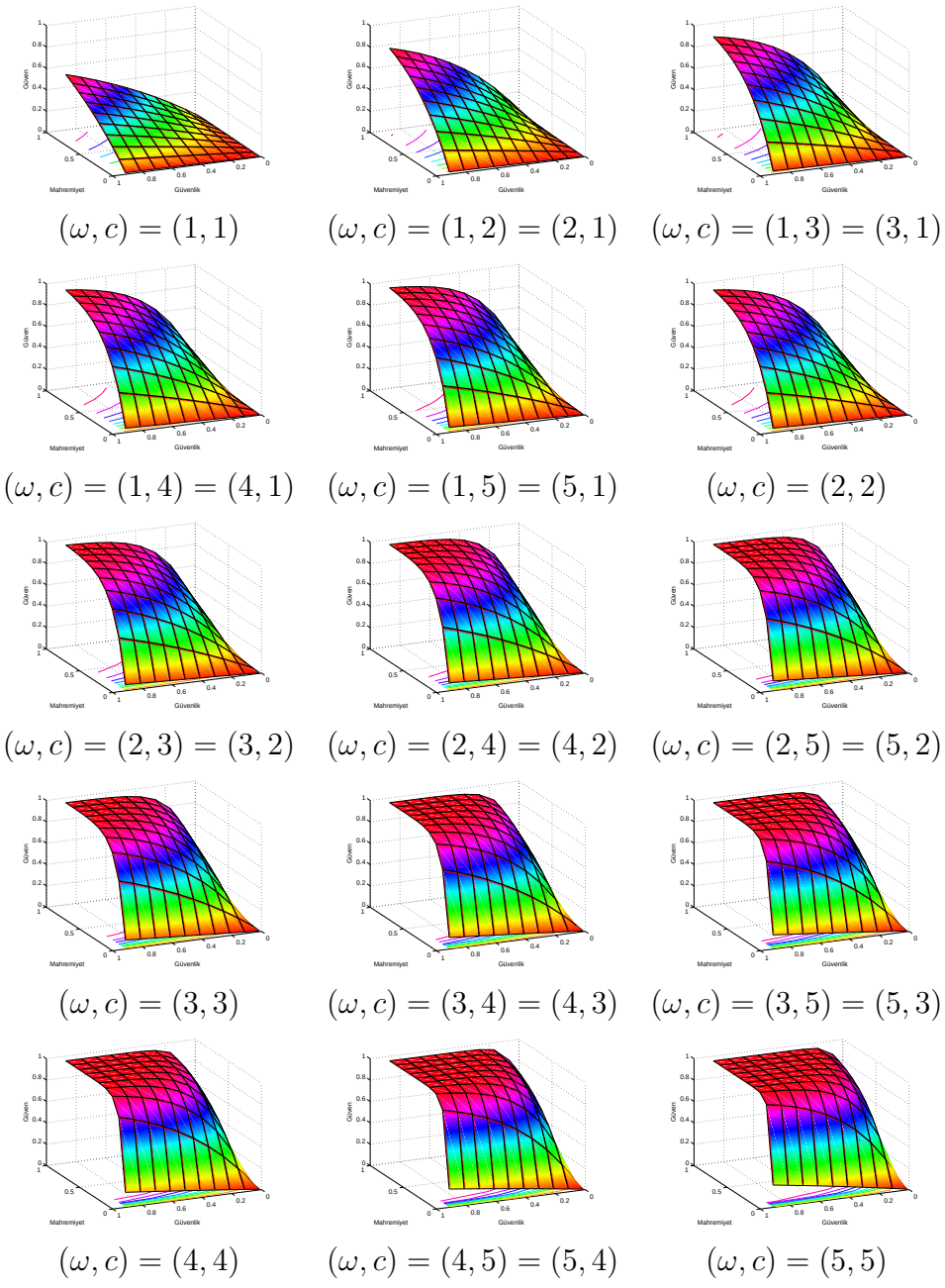
(c) $\omega c = 100$ (d) $\omega c = 1000$

(e) $\omega c = 10000$

Şekil 2.7 Artan ωc değerlerine göre değişen güven yüzeyleri.

Şekil 2.8'de, 1 ila 5 arasında değişen farklı ω ve c değerleri için güven yüzeyleri görülebilir. $\omega = c = 5$ olduğunda BKYS'nin güven yüzeyinin genişlediği ve idealde $T = 1$ sağlanabileceği görülebilir. $\omega = c = 1$ olduğunda ise sağlanabilecek en yüksek güven değeri $T = 0.63$ olabilir. Bu durumda **P** ve **S** en mükemmel şekilde sağlanabilse bile toplumun %27'si $(1 - T = 0.27)$ BKYS'ye güvenmeyebilir. Bu da göstermektedir ki kullanıcıları ikna etmeden (istekliliği arttırmadan ve kullanıcıların sistemden emin

olmasını sağlamadan) bir BKYS'yi tam anlamda işler hale getirmek mümkün değildir.



$(\omega, c) = (1, 1)$ $(\omega, c) = (1, 2) = (2, 1)$ $(\omega, c) = (1, 3) = (3, 1)$

$(\omega, c) = (1, 4) = (4, 1)$ $(\omega, c) = (1, 5) = (5, 1)$ $(\omega, c) = (2, 2)$

$(\omega, c) = (2, 3) = (3, 2)$ $(\omega, c) = (2, 4) = (4, 2)$ $(\omega, c) = (2, 5) = (5, 2)$

$(\omega, c) = (3, 3)$ $(\omega, c) = (3, 4) = (4, 3)$ $(\omega, c) = (3, 5) = (5, 3)$

$(\omega, c) = (4, 4)$ $(\omega, c) = (4, 5) = (5, 4)$ $(\omega, c) = (5, 5)$

Şekil 2.8 Farklı ω ve c değerleri için güven yüzeyleri.

3 boyutlu dağılımların mahremiyet-güvenlik düzlemindeki izdüşümleri incelendiğinde ödünleşim eğrileri görülebilir. Benzer eğrilere biyometrik teknolojilerin başarımını gözlemede kullanılan, bir ekseni hatalı kabul oranı, bir ekseni hatalı red oranı olan hata tespit ödünleşim eğrilerinde (Detection Error Tradeoff) veya başka bir deyişle alıcı operasyon eğrilerinde (Receiving Operating Curve) rastlanır.

2.2.5 BioPSTM (Alternatif #2)

BioPSTM için önerilen ikinci alternatifte c faktörü devre dışı bırakılarak kamusal isteklilik (ω) tek bir parametre olarak kabul edilir. Buradaki temel mantık, kamusal istekliliğin zaten c parametresinin taşıdığı bilgileri içermesi olabilir. Bu varsayım için kuşkusuz derinlemesine sosyolojik araştırmalar yapılmalıdır. Örnek olması açısından bu alternatif modelde ω nın, c ile ilgili tüm bilgileri içerdiği varsayılır. Alternatif #2 için uygun kullanıcı kabul olasılık fonksiyonunu oluşturmak için öncelikle sınır değerleri hesaplanmalıdır. İlgili sınır değerleri şöyledir (Bkz. Denklem 2.9-2.11):

$$\frac{\partial T}{\partial \mathbf{P}} \leq 0, \frac{\partial T}{\partial \mathbf{S}} \leq 0, \omega > 0 \tag{2.9}$$

$$\forall \mathbf{P} > 0, \lim_{\mathbf{S} \longrightarrow 0} T(\mathbf{P}, \mathbf{S}) = 0, \lim_{\mathbf{S} \longrightarrow \infty} T(\mathbf{P}, \mathbf{S}) = 1, \tag{2.10}$$

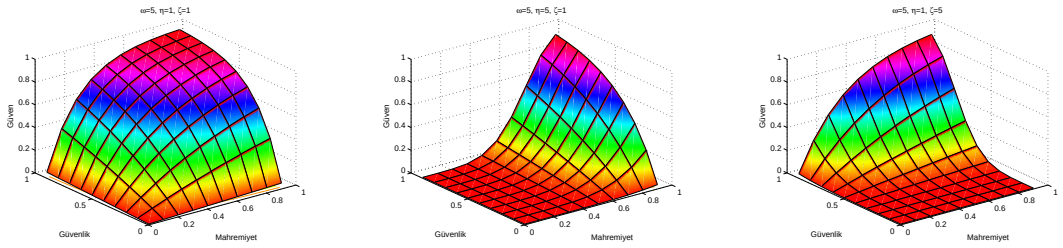
$$\forall \mathbf{S} > 0, \lim_{\mathbf{P} \longrightarrow 0} T(\mathbf{P}, \mathbf{S}) = 0, \lim_{\mathbf{P} \longrightarrow \infty} T(\mathbf{P}, \mathbf{S}) = 1 \tag{2.11}$$

Sınır değerlerinden de görüleceği gibi, Alternatif #1'e benzer biçimde **P** ve **S** birbiriyle çatışan iki parametre iken T güven faktörü hem **P** hem de **S** ile işbirliği yapmayı tercih eder. Bu şartlar altında önerilen matematiksel model şöyledir (Bkz. Denklem 2.12):

$$T(\mathbf{S}, \mathbf{P}) = 1 - e^{-\omega \mathbf{S}^{\zeta} \mathbf{P}^{\eta}} \tag{2.12}$$

Burada η mahremiyet ağırlığını, ζ ise güvenlik ağırlığını ifade eden pozitif değerlerdir. Eğer bir toplumda veya sistemde mahremiyet güvenliğe göre daha kritik bir kriter ise $\eta > \zeta$ seçilir. Güvenlik çok daha kritikse $\zeta > \eta$ seçilmelidir. Her iki parametrenin eşit seçildiği durumda mahremiyet de güvenlik de eşit derecede önemli sayılır. Bu parametrelerin büyük seçilmesi mahremiyet ve güvenliğin ne kadar kritik olduğunu betimler. Şekil 2.9'da aynı kamusal isteklilik düzeyinde ($\omega = 5$) mahremiyet ve güvenlik ağırlıklarının güveni nasıl etkilediği görülmektedir. ζ veya η dan birinin büyük olduğu durumlarda hangi kriter büyükse onun olduğu tarafta daha geniş bir spektrum gözlenir. Örneğin, Şekil 2.9-c'de $\zeta > \eta$ seçilmiştir. Bu durumda, güvenlik daha kritik olduğu için tasarımcıya güvenlikle ilgili parametrelerle oynadığı

zaman daha geniş spektrumda hareket imkanı sağlanır. Kamusal isteklilik parametresi ise güven dağılımının tepesindeki düzlüğü etkiler. Bu düzlük ne kadar genişse, toplum biyometrik teknolojileri kullanmada o kadar rahat ve isteklidir. Şekil 2.10'da , $\zeta = \eta = 1$ iken ω nın farklı değerleri için güven dağılımları görülebilir (soldan sağa $\omega = [1, 5, 10, 100, 1000]$). ω nın büyük değerleri için güven yüzeyleri neredeyse yatay bir düzleme dönüştüğünden pratik olarak daha küçük değerler seçilmelidir. MOS puanlamasıyla paralel olması açısından ω nın, [1,5] aralığından seçilmesi önerilmektedir.



$\omega = 5, \zeta = 1, \eta = 1$ $\omega = 5, \zeta = 1, \eta = 5$ $\omega = 5, \zeta = 5, \eta = 1$

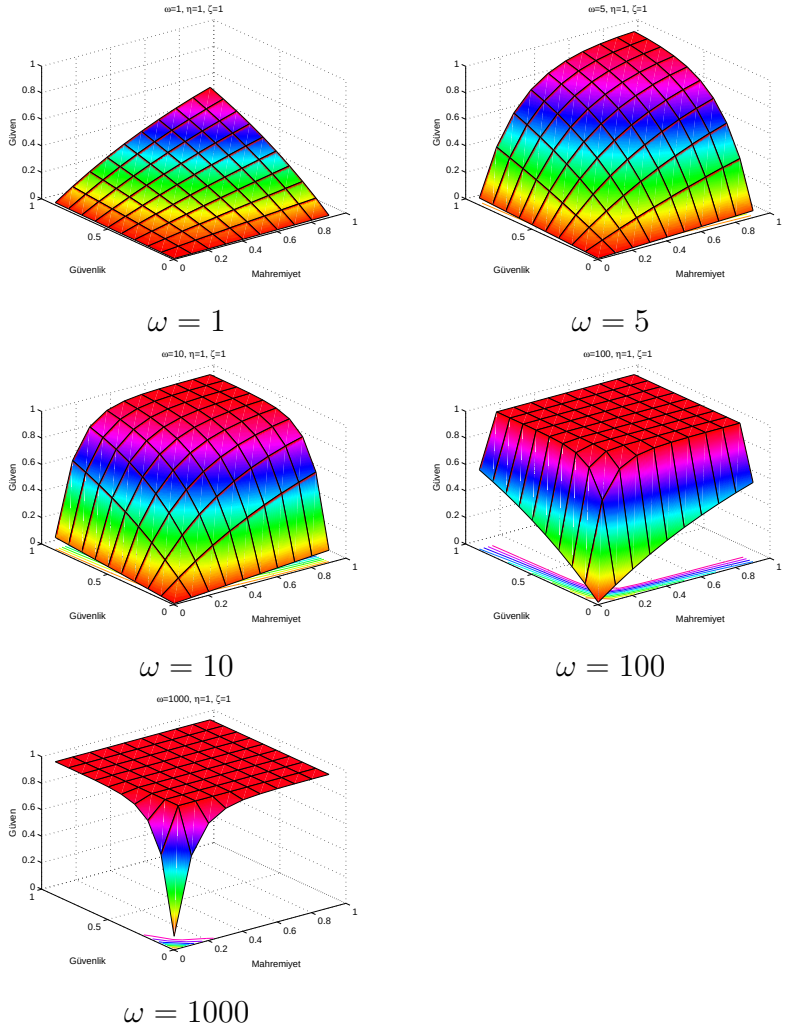
Şekil 2.9 Değişen mahremiyet ve güven ağırlıklarına göre güven dağılımları.

2.3 İlgili Çalışmalar

2.3.1 Biyometrik Şablon Koruma ile İlgili Çalışmalar

Biyometrikler kişiye özel bir bilgi sağlayarak güvenlik yaklaşımlarında yeni bir çığır açmıştır. Ancak kişiye özel bu bilgilerin gerektiğinde iptal edilebilmesi, kişiye özel başka bilgilerle korunmaya alınması, doğalarında bulunan belirsizliklerden bağımsız biçimde temsil edilerek direk gizli anahtar olarak kullanılmaları son yıllarda önem kazanan araştırma alanlarıdır [5]. Biyometrik şablon koruma ana başlığında toplanabilecek bu çalışmalar incelendiğinde önerilen çözümlerin genel olarak beş sınıf altında toplandıkları söylenebilir:

1. Biyometrik tuzlama (biometric salting): Bu yöntem UNIX şifreleme sisteminde kullanılan tuzlama yaklaşımına benzer. Bu yöntemde kişiye ait p şifresi, rasgele bir R dizisi ile birleştirilir ve gerekirse kıyılarak (hashing) saklanır. Burada eklenen R rasgele dizisi şifrenin entropisini ve güvenliğini arttırmaktadır. Biyometrik tuzlamada bir nicemleme (quantization) ile ikili kriptografik anahtar



$\omega = 1$ $\omega = 5$ $\omega = 10$ $\omega = 100$ $\omega = 1000$

Şekil 2.10 Kamusal istek parametresinin etkisi.

üretilebilir. R rasgele dizisi kişiye özel bir ortamda (akıllı kart, jeton vb.) saklanmaktadır.

2. Biyometrik anahtar üretimi (biometric key generation): Bu yaklaşımda kriptografik anahtar, biyometrik işaretin kendisinden direk olarak hesaplanabilir. Bu yöntemde kişiye özel herhangi bir rasgele sayı dizisi kullanılmaz. Burada en büyük problem biyometrik verideki belirsizliklerden kaynaklanan hatanın tolere edilmesidir. O nedenle gürbüz özniteliklerin ve hata düzeltme mekanizmalarının kullanılması gerekmektedir.

3. Bulanık yöntemler (fuzzy schemes) veya biyometrik kriptosistemler: Biyometriğin güçlendirilmesinde önerilen bulanık yöntemlerde, açık yardımcı (helper data, auxiliary data) bir verinin yardımıyla kişiye özel biyometrik verinin koruma altına alınarak kullanıcılar arası değişintiyi azaltmak amaçlanmaktadır. Bu

tür sistemlerde şablon ve sorgu verileri arasındaki uzaklığı ölçen bir metrik (Hamming, Öklit, küme farkı uzaklığı gibi) tanımlanır. Bir üreteç fonksiyon ile kişiye özel biyometrikten bir açık bir de gizli katar oluşturulur. Tanımada ise sorgu biyometriği ve açık katar bilgisi birlikte kullanılarak gizli katar tahmin edilmeye çalışılır. Bunun için uzaklık metriği kullanılır.

4. Evrilemeyen (geridönüşümsüz) dönüşümler (non-invertible Transforms): Bu tür sistemlerde biyometrik veri tek yönlü bir fonksiyonla gene aynı uzayda temsil edilir. Karşılaştırmada sorgu biyometriği gene aynı fonksiyonla dönüştürülür ve şablonun dönüştürülmüş hali ile karşılaştırma yapılır.

5. İstatistiksel yöntemler: Bu yöntemlerin ortak noktası kişiye ait biyometrikleri uzayda bir sınıf veya topak (cluster) olarak ifade ederek bu sınıfın veya topağın betimleyici özelliklerinden gürbüz anahtarlar üretmektir.

Biyometrik güçlendirme

Biyometrik güçlendirme ile ilgili en başarılı yöntemlerden biri Teoh ve arkadaşları [6] tarafından önerilen "Biohashing" yöntemidir. Bu yöntemde kişiye özel biyometrik işaretten çıkarılan öznitelikler gene kişiye özel ortonormal rasgele sayı dizisi ile iççarpılarak güçlendirme yapılmakta; iç çarpımdan çıkan sayılar bir eşik değeri ile karşılaştırılarak bir bit dizisi elde edilmektedir. Bir başka çalışmada ise gizli bilgi bir bit-yer değiştirme (bit-replacement) algoritması ile parmak izi işaretine gömülür [14].

Burada anahtar, biyometrik veriden tamamen bağımsızdır ve istenildiği gibi yenilenebilir. Biyometrik güçlendirme ile ilgili önemli bir diğer çalışma Savvides ve arkadaşları [15] tarafından önerilen Minimum Ortalama İlinti Enerjisi (Minimum Average Correlation Energy - MACE) yaklaşımıdır. Bu çalışmada kişinin N adet yüz imgesinden çıkarılan kişiye özel bir modelin her kişi için bir kereliğine üretilen rasgele çekirdek matrisi ile iliştirilerek (correlation) güçlendirilmesi söz konusudur. Biyometrik güçlendirme ile ilgili çalışmalar taranırken Ratha ve arkadaşlarının [16] çalışmasını da gözden geçirmek gerekir. Bu çalışmada parmak izinden çıkarılan olay noktaları, bir kereliğine üretilmiş kişiye özel rasgele bilgilere dayanan bir geometrik dönüşümle korunmaya ve güçlendirilmeye çalışılmaktadır. Dönüşüm, olay noktalarının yerlerinin kartezyen ve radyal düzlemde rasgele değiştirilmesi veya kişiye özel yük dağılım veya

Gauss karışım fonksiyonu ile çırpılması (scrambling) ile sağlanır. Bu ve buna benzer güçlendirme yöntemlerindeki ortak özellik, biyometrik verinin entropisindeki eksikliklerin kişiye özel, bir kereliğine oluşturulmuş rasgele enformasyonla güçlendirilmesidir. Bu çalışmalarda kimi zaman %0 eşit hata oranı bile elde edilmekle beraber bu mükemmel sonuçların biyometrik verideki enformasyondan mı yoksa rasgele oluşturulmuş sentetik enformasyondan mı geldiği, başka bir deyişle hangisinin baskın olduğu belli değildir.

Biyometriklerden anahtar üretimi

Biyometriklerden anahtar üretmek biyometrik kriptosistem araştırmalarında en problemli alanlardan biridir. Çünkü burada sentetik olarak rasgele üretilmiş, kişiye özel bir bilgi kullanılmamaktadır. Biyometrik anahtar üretiminde biyometrik verideki belirsizliklerden bağımsız bir öznitelik çıkarılarak her defasında aynı bit dizisinin elde edilmesi hedeflenir. Bu, kuşkusuz zor bir problemdir. Bu konuda yapılan araştırmalar henüz emekleme aşamasındadır. Örneğin Davida ve arkadaşlarının [17] iris kodları üzerinde yaptıkları çalışmada iris öznitelikleri ikili gösterime dönüştürüldükten sonra Hamming uzaklığına bağlı olarak karşılaştırma yapılmaktadır. Monrose ve arkadaşlarının çalışmasında [18; 19] ise davranışsal biyometrikler olan tuşabasım ritmi ve konuşma işareti kullanılmıştır. Bu çalışmalar kayıt aşamasında kişiye özel rasgele üretilmiş k bitlik r sayısı ve bir tablo, merkezi veritabanında saklanır. Bu tablo, biyometrik verilerin bir eşik değeri ile ikilenmesi sonucu elde edilen bit dizisi ve r nin Shamir Giz Paylaşımı yöntemi için parametre olarak kullanılması ile oluşturulur. Bu tablo, biyometrik anahtar olarak kullanılabilir. Bu iki çalışmada, tuşabasım ritmi için 15, konuşma için 60 efektif bit üretilebilmiştir.

Bulanık yöntemler ve biyometrik kriptosistemler

Yeni nesil biyometrik kriptosistem yaklaşımlarından biri de bulanık yöntemler üzerine inşa edilmiştir. Biyometriklerden direk anahtar üretmekte yaşanan problemler, araştırmacıları gizli enformasyonla değil açık yardımcı verilerle biyometriği korumaya yönlendirmiştir. Dodis ve arkadaşlarının gürültülü veriden anahtar üretme üzerine yazdıkları teorik makaleden [7] esinlenen bu yöntemlerde rasgele oluşturulmuş sentetik bir bilgi yerine başka yardımcı bilgilerden yararlanılır ve anahtar, biyometrik veri ile öyle bir bağlanır ki başarılı bir eşleştirme olmadan anahtar bırakılmaz. Örneğin,

Boyen'in çalışmasında kıyım fonksiyonu uygulamadan önce sabit bir permütasyonun iris kodlarına uygulandığı bir bulanık özütleyici tanıtılmaktadır [20]. Bulanık Kasa (Fuzzy Vault) [21] adı verilen çalışmada ise Juels ve Wattenberg'in Bulanık Üstlenme (Fuzzy Commitment) yöntemi [22] temel alınmış, şifrelenmiş uzayda bulanık eşleme yapabilen bir benzerlik yaklaşımı önerilmiştir. Bu yaklaşım birçok biyometriğe uygulansa da elde edilen başarım pek tatmin edici olmamış ve sistemin güvenliğinin kullanılan polinoma fazlaca bağımlı olduğu anlaşılmıştır.

Literatürde Bulanık Kasa (Fuzzy Vault) [21] olarak bilinen yöntemler Juels ve Wattenberg'in [22] çalışmaları temel alınarak geliştirilmektedir. Juels ve Wattenberg'in çalışmaları literatürde anahtar bağlama adıyla da anılmaktadır ve bu yöntemde kişiye ait gizli bilgi mantıksal bir kasaya konmakta ve kasa sıralı olmayan bir küme ile kilitlenmektedir. Kayıtlı küme ile sorgu kümesi belli bir oranda örtüşüyorsa doğrulama yapılır. Anahtar bağlama yaklaşımında hata düzeltme kodları sıklıkla kullanılmakta ve başarımı etkileyen en önemli faktörlerden biri olarak kabul edilmektedir. Bu yöntemin biyometriklere ilk uygulaması Clancy ve arkadaşları [23] tarafından gerçeklenmiştir. Bu çalışmada parmak izi olay noktalarının kanonik pozisyonları sıralı olmayan kayıt kümesinin oluşturulmasında kullanılır. Burada olay noktalarının apsisleri daha önce seçilmiş bir polinomun katsayıları olacak şekilde tanımlandıktan sonra polinoma belli bir minimum uzaklıkta birçok yanıltıcı nokta, polinom üzerindeki noktalarla tümleştirilerek bir güvenli kasa oluşturulur. Tanımada sorgu kümesinden bu sefer katsayıları yeni kümeye göre belirlenmiş bir polinom oluşturulur ve kasada sorgu polinomuna oturan bir polinom araştırılır. İki polinom belli bir oranda örtüşüyorsa doğrulama başarılı olur. Bu yöntemde parmak izlerinin düzgelenmiş olduğu varsayılır. Oysa ki gerçek hayatta dönme, öteleme ve kayma ciddi bir problemdir ve bu çalışmada göz ardı edilmiştir. Buna çözüm olarak Uludağ ve arkadaşları [24] global dönme ve kaymadan bağımsız bir öznitelik önermişlerse de sahte sınıf testlerinde (A kişisinin verisi B kişisi ile test ediliyor) önerdikleri yöntem çok başarılı olmamıştır. Bulanık yöntemlerin en büyük problemlerinden biri doğrulama fazında kod çözümü sırasında çok fazla nokta kombinasyonunun ortaya çıkmasıdır. Bu durum özellikle yarı-gerçek zamanlı sistemlerde problem olmaktadır.

Biyometrik kriptosistemlerde bir başka yaklaşım Dodis ve arkadaşlarının çalışmalarını temel alan anahtar üretimi yaklaşımıdır [7]. Bu yaklaşımda anahtar bağlama

yöntemindeki hata düzeltme kodları yerine ya nicemleme (quantization) yöntemleri ile ya da güvenli taslak (secure sketch) kullanılarak bit dizisi üretilmesi hedeflenir. Burada amaç, biyometriği bir kod kitabının elemanları ile eşleştirerek bir güvenli taslak oluşturmak ve test verisi geldiğinde bu taslak ve kod kitabını kullanarak biyometriği açığa çıkarmaktır. Kod kitabı oluşturulurken nicemleme kullanılır ve kimi zaman bu nicemleme kişiye özel bir biçemde gerçeklenebilir.

Biyometrik kriptosistemlerde öne çıkan diğer önemli çalışmalara örnek olarak hata düzeltme ve kuantalama temelli yöntemler [32; 33; 34; 35], bulanık taslaklar için Buhan ve arkadaşları, Chang ve arkadaşları ile Ong ve arkadaşlarının çalışmaları [34; 36; 37] ve son olarak da bulanık özütleyicilerin ilginç uygulamaları olarak Tong ve arkadaşları ile Alvarez ve arkadaşlarının çalışmaları [38; 39] sayılabilir.

Evrilemeyen (geridönüşümsüz) dönüşümler Evrilemeyen dönüşümlerle ilgili çalışmalarda da kayda değer çabalar görülmektedir. Ancak bu yöntemin problemleri henüz tam anlamıyla çözüme ulaşmamıştır. Bu konudaki çalışmalar biyometrik güçlendirme ve iptal edilebilirlik kapsamında da değerlendirilebilir zira aynı biyometriğin evrilmiş iki örneğinin geleneksel kriptografideki gibi birebir örtüşmesini sağlamak çok ciddi bir problem olarak hala maceracı araştırmacıların ilgisini çekmektedir. Bu konuda en adamakıllı çalışma Tulyakov ve arkadaşlarının [25] çalışmasıdır. Bu çalışmada parmak izi olay noktaları için m adet simetrik evrilemeyen fonksiyon (symmetric hash functions) tanımlanmıştır. Burada m adet fonksiyondan her biri, olay noktalarının $1.$ den $m.$ dereceye kadar kuvvetlerinin toplamını hesaplar. Bir başka geometrik dönüşüm, Sütçü ve arkadaşları [26] tarafından önerilen yine olay noktaları üzerine kurulu bir yöntemdir. Bu çalışmada merkezi olay noktalarının ağırlık merkezi ve yarı çapı R olacak biçimde bir çember tanımlanır. Daha sonra tüm olay noktası ikililerinden geçen doğruların çemberi kestiği noktalar belirlenir. Çember φ açısı kadar yaylara bölünür ve her yay üzerindeki kesişim noktasının sayısı tutulur. Böylece $360/\varphi$ uzunluğunda evrilemeyen kodlar elde edilmiş olur. Sütçü ve arkadaşlarının bir başka çalışmasında ise geometrik evirme yaklaşımındansa, akla daha mantıklı görünen ve birçok veriden elde edilen bilgilerin bir şekilde istatistiksel olarak modellendiği bir yöntem önerilmektedir [27]. Bu çalışmada tek yönlü evirme fonksiyonu N adet gauss dağılımının toplamı olarak ifade edilmektedir. Bu N dağılımdan biri kişinin özniteliklerinden uyarlanan gerçek gauss dağılımı diğerleri ise yanıltıcı dağılımlardır. Burada

birbirinden bağımsız her öznitelik için farklı, bir kişiye özel gerçek dağılım ve N-1 adet yanıltıcı dağılım tanımlıdır. Bu ve buna benzer yöntemlerde umut verici başarımlar elde edilmekle beraber, bu yöntemlerin düzgelenmiş biyometrikler üzerinde çalışma zorunluluğu, imgenin tümündense belli bir bölgesine odaklanılması ve testlerin küçük veritabanlarında yapılması dezavantaj olarak nitelenebilir.

İstatistiksel yöntemler

İstatistiksel yöntemlerle biyometrik anahtar veya imza üretimi yukarıda bahsedilen yöntemlere alternatif olarak geliştirilmiştir. Bu tip yöntemlerde kişiye ait biyometrik verilerin bir kısmı eğitim amaçlı kullanılarak kişiye özgü bir model oluşturulmakta ve bu modelden kişiye özgü bir bit dizisi çıkarılmaktadır. Örneğin, topaklama yöntemi kullanılarak çok boyutlu uzayda kişiyi temsil eden en iyi noktayı bulup bu noktanın içinde bulunduğu ve bir şekilde kodlanmış bölgeden bir kimlik bilgisi çıkarmak en yeni çalışmalardan biri olarak bilinmektedir [28; 29]. Bir başka çalışmada ise ardışıl iki-sınıflı doğrusal ayırtaç analizi kullanılarak biyometrik kod oluşturulmuştur [30]. Tüm bu yöntemlerde amaç kişiye ait birçok veriyi bir arada kullanarak biyometriklerin doğasında bulunan belirsizlikleri en aza indirmek, istisnai örneklerden kurtulmak ve mümkün olduğunca gürbüz bir yaklaşım önermektir. Örneğin istatistiksel yöntemlerle anahtar üretimi için en ilginç çalışmalardan biri olan Chang ve arkadaşlarının [31] çalışmasında tüm özniteliklerden hesaplanan bir global dağılım ile sadece bir kişiye özel öznitelik dağılımları hesaplanır. Bu iki dağılım üst üste bindirilir ve ikisinin kesişim bölgesi güvenli bölge olarak tanımlanır. Global dağılım, güvenli bölge ile aynı büyüklükteki bölümlere ayrılır. Bu bölümlerin sayısı K ise her bir bölüm $logK$ bit ile temsil edilir. Burada kişiye özel dağılımı temsil eden bit dizisi anahtar olarak kullanılabilir. Bu çalışmada en fazla 88 efektif bit elde edilebilmiştir. İstatistiksel yöntemlerle biyometrik anahtar veya imza üretimi ile ilgili çalışmalar çoğunlukla küçük veritabanlarında denenmiş, gerçek hayatı temsil edecek deneyler yapılmamıştır.

İstatistiksel yöntemlere örnek olabilecek diğer önemli çabalar ise Kanak ve Soğukpınar, Hao ve arkadaşları, Vielhauer ve arkadaşları, Yamazaki ve arkadaşları ile Lee ve arkadaşlarının [40; 41; 42; 43; 44] literatüre kazandırdıkları çalışmalardır.

2.3.2 Mahremiyet-Güvenlik Ödünleşimi ile İlgili Çalışmalar

Mahremiyeti ve güvenliği dikkate alan biyometrik güvenlik sistemleri ile ilgili çalışmalar özellikle son on yılda hız kazanmış ([5; 45; 46]) ve buna paralel olarak mahremiyet-güvenlik arasındaki matematiksel ilişkiyi inceleyen önemli çalışmalar [11; 47; 48; 49]; yeni biyometrik anahtar üretme teknikleri [50]; mahremiyet ve güvenlik tehditlerinin derinlemesine analizleri [51; 52; 53] gibi farklı yaklaşımlarla yeni bir boyut kazanmıştır.

Öne çıkan çalışmalar arasında güvenlik ve mahremiyet için geçerli ölçütlerin tanımlandığı görülebilmektedir. Bu çalışmalar ya Shannon entropisi [32; 33], ya ortalama minimum entropisi [7] ve sızıntı oranları [8; 27; 54] üzerine kurulu ölçütler önermişlerdir [55]. Bunun yanında mahremiyet ve güvenlik arasındaki ilişkiyi gene benzer entropik ölçütler kullanarak matematiksel bir yolla açıklayan çalışmalar da mevcuttur.

Mahremiyet-Güvenlik ödünleşimini en kapsamlı biçimde açıklayan matematiksel modeller Ignatenko ve arkadaşları ile Lai ve arkadaşları tarafından bilim dünyasına kazandırılmıştır [11; 48; 49]. Bu çalışmalarda daha ziyade gizli anahtar üretilirken ortaya çıkabilecek potansiyel tehditler ve ataklar öne çıkar. Örneğin, Lai ve arkadaşlarının çalışmasında mahremiyet ve güvenlik arasındaki ödünleşim mükemmel güvenlik ve gizlilik koşulları ile birlikte sızıntı oranları ve ortalama entropi cinsinden ifade edilmiştir [49]. Ignatenko ve arkadaşları ise sır üreten (secret generation) sistemlerde orantı-sızıntı ikilisini (rate-leakage pair) matematiksel olarak ifade ettikten sonra sıfır-sızdırmalı bir biyometrik sistemi betimleyen formülü sunmuşlardır [11; 48]. Ignatenko ve arkadaşları mahremiyet sızıntı oranını ise sendrom gibi bir yardımcı veri ile biyometrik veri arasındaki karşılıklı (mutual) bilgi cinsinden ifade etmişlerdir. Vetro ve arkadaşları [56] ve daha öncesinde Sütçü ve arkadaşları [8; 57] ise güvenlik ve gürbüzlük arasındaki ilişkiyi Slepian-Wolf kodlama oranının bir fonksiyonu olarak temsil etmişlerdir.

2.3.3 Formel Güven Modelleri ile İlgili Çalışmalar

Güven faktörü özellikle işletme ve yönetim bilimleri ile telekomünikasyon sektörlerinde incelenmiş ve bazı formel yaklaşımlar öne sürülmüştür. Literatürde güven,

talep ve verimlilik arasındaki ilişkiyi modelleyen çalışmalar mevcuttur. Bu çalışmaların arkasındaki anafikir güven faktörünün ana oyuncular arasındaki etkileşimi ve bu oyuncuların taleplerini nasıl etkilediğini gözlemektir [58]. Bu konuda öne çıkan modeller FIRE [59], Regret [60], Yu ve Shing Modeli [61] ve olasılıksal güven modelleridir [62]. Tüm bu modellerin kapsamlı analizi Sabater ve arkadaşları tarafından yapılmıştır [63]. Literatürdeki güven modelleri genelde anketlerle ölçülen kullanıcı eğilimleri üzerine kuruludur ve kullanıcıların bir sisteme güvenmesine etki eden faktörlerin mantıksal ilişkilerini inceler.

Mevcut güven modelleri her ne kadar güven, talep ve verimliliği modellese de mahremiyet ve güvenliğin kamusal istek, kullanıcı eğilimleri ve kullanıcı tutumları ile ilişkilerini ortaya koyan ciddi bir matematiksel model yoktur.

2.3.4 Teknoloji Kabul Modelleri ile İlgili Çalışmalar

Kullanıcı kabul edilirliği ve davranışsal kullanım niyeti (Behavioral Intention to use - BI) üzerine temel olarak iki teorik model vardır. Öne çıkan ilk yaklaşım Nedensel Eylem Teorisi (Theory of Reasoned Action - TRA) olarak bilinir ve birçok farklı alanda davranışın açıklanması ve öngörülmesinde temel alınır [64]. TRA'ya göre kişinin davranışı onun herhangi bir eylem üzerindeki davranışsal niyetine göre belirlenir. Bu niyet kişinin hem o aksiyonla ilgili tutumuna (attitude) hem de öznel normuna göre şekillenir. TRA her ne kadar toplumsal psikolojiden etkilenmiş jenerik bir yaklaşım sunsa da tipik bilgi sistemleri için pek de uygun bir model değildir. TRA'da kullanım davranışının bir kişinin kendi tutumundan mı yoksa bir referantın o kişi üzerindeki etkisinden mi kaynaklandığı belirgin değildir. Bu durum, özellikle bilgi sistemleri gibi hem kişisel hem de evrensel bir dünyayı içeren fonksiyonlarda davranışın doğasını açıklamaya yetmez. Örneğin, biyometrik sensörlerin kullanıldığı bir BKYS'de, kullanıcı arayüzünün hem kişisel düzeyde hem de toplumsal düzeyde kolaylıkla kullanılıp kullanılamayacağına dair algının ölçülmesi gerekir. TRA burada sadece bireylerin algısını yansıtabilir. Oysaki toplumsal algı, örneğin o teknolojinin geniş ölçekte kabul edilebilirliği ve kamusal istek gibi daha geniş perspektifli bakış TRA ile yeterince açıklanamaz. Eksiği gidermek amacıyla, Davis ve arkadaşları [65; 66], TRA'dan etkilenerek iki önemli faktör tanımlamışlardır: (i) algılanan kul-

lanışlılık (perceived usefulness) ve (ii) algılanan kullanım kolaylığı (perceived ease to use). Teknoloji Kabul Modeli (Technology Acceptance Model) temel olarak bu iki faktör üzerine kurulur. Algılanan kullanışlılık, kullanıcının spesifik bir uygulamanın kullanımıyla, organizasyonel düzeyde etki yaratacak kişisel iş performansının artma olasılığı olarak tanımlanabilir. Burada, kişisel kullanımın daha geniş ölçekte çok kullanıcılı durumdaki etkisi betimlenmiş olur. Algılanan kullanım kolaylığı ise bir insanın o sistemi hangi dereceye kadar efor sarf etmeden (ya da belirli düzeyde sarf ederek) kullanabileceğine olan inancıdır. Bu iki faktör genelde anketlerle ya da kimi zaman kullanım alışkanlıklarını otomatik ölçen akıllı sistemlerle gözlenebilir.

TAM, tasarımcıların gerçek dünya problemlerini daha iyi anlamalarına yardımcı olan bir yöntem olarak uzun süredir kullanılmaktadır. Örneğin Kaasinen mobil Internet [67] ve heterojen ağların [68] kullanımı konusunda TAM'ı uygulamıştır. Kaasinen, klasik TAM üzerine bir de güven faktörünü eklemiştir. Güven faktörü özellikle kamusal istek ve kullanım niyetinin modellenmesinde yenilikçi bir yaklaşım olarak ortaya çıkmıştır. Levy ve arkadaşları [69] ile Nwatu ve arkadaşları [70] daha sonra TAM'ı kimlik sahteciliği ve eÖğrenme alanlarına başarılı biçimde uyarlamışlardır.

TRA ve TAM'dan farklı olarak, özellikle telekomünikasyon ve ekonomi alanlarında uygulanan kullanıcı kabul modelleri de vardır. Badia ve arkadaşları [12] tarafından önerilen ve İleri ve arkadaşlarının [13] geliştirdiği isteğe bağlı fiyatlandırma (demand responsive pricing) ile Varian'ın [71] Cobb-Douglass eğrileri sırasıyla telekomünikasyon ve mikroekonomi alanlarında önerilen yöntemlerdir. Bu modellerin temelindeki anafikir, GSM operatörlerinin ya da hizmet sağlayıcılarının, müşterileri çekmek için uygulayacakları pazarlama stratejisinin betimlenmesidir.

Bu alandaki çalışmalar belirli bir olgunluğa eriştiyse de BKYS, insan-bilgisayar etkileşimi veya ileri diğer teknolojiler (robot etkileşimi, kişiselleşmiş tıp) için hala açık araştırma konuları mevcuttur.

2.3.5 Mevcut Çalışmalardaki Eksiklikler ve Fırsatlar

Biyometrik şablon koruma ile ilgili çalışmalar her geçen gün daha da derinleşerek devam etmektedir. Ancak biyometrik şablon koruma ile ilgili çalışmaların gelip

tıkandığı en önemli nokta gerçekten gürbüz biyometrik özniteliklerin çıkarılamamasıdır. Sınıf içi ve sınıflar arası değişintiyi en iyi şekilde ifade eden özniteliklerin oluşturulmasıyla biyometrik anahtar üretiminden daha etkin biyo-kıyım fonksiyonlarının üretimine BKYS'nin hemen hemen tüm bileşenlerini olumlu etkileyecek gelişmeler yaşanabilir. O nedenle son yıllarda araştırmacılar çok kipli biyometrik uygulamalara, alt düzey işaret işleme teknikleri ile tanıma başarımını düşüren faktörlerle baş etmeye çalışmaktadır.

Mahremiyet-güvenlik ödünleşimi ile ilgili teorik çalışmalar hemen hemen olgunluğa erişmiştir. Burada asıl sorun hem mahremiyeti hem de güvenliği sağlayacak tekniklerin geliştirilmesi ve hayata geçirilmesidir. Mahremiyet-güvenlik ödünleşiminin güven üzerine etkisi ve BKYS'lerin toplum tarafından kabulunun incelenmesinde nesnel yöntemlerin geliştirilmesi ise oldukça sığ bir araştırma alanı olarak dikkat çekmektedir. Güven faktörü için genel kabul görecek bir formel modelin olmaması, bu çalışmada önerilen BioPSTM'in değerini arttırmaktadır. Aynı şekilde, biyometrik teknolojilerin kabulunun modellenmesi ve nesnel yöntemlerle kamunun niyetini ve algısını öngörecek tekniklerin geliştirilmesi de sıcak araştırma konuları arasındadır. Bu bakımdan, tıpkı BioPSTM gibi BioTAM da dikkat çeken bir yaklaşım olarak öne çıkabilir.

3 Biyometrik Teknoloji Kabul Modeli - BioTAM

3.1 Biyometrik Teknolojiler ve TAM

Bilimsel gelişmelerle beraber günlük hayatın bir parçası haline gelen bilgi ve iletişim teknolojilerinin yaygınlaşmasında en önemli etkenlerden biri bu teknolojilerin halk arasında nasıl daha fazla kabul görmesini inceleyen algısal modellerdir. Bu modeller, geliştirilen tekniklerin son ürüne dönüşmesinde ve gerçekten kullanılabilir sistemler içinde etkin biçimde yer almasında kılavuzluk etmektedir. Teknolojiyi geliştirmek kadar o teknolojinin geniş bir kitle tarafından kabul görmesi, teknolojinin yaygınlaşmasında politik, ekonomik, sosyal ve kültürel engellerin bertaraf edilmesi ve önyargıları giderecek önlemler alınması da bir o kadar önemlidir. Özellikle üzerinde tartışılan mahremiyet, etik, kültürel, milli veya dini unsurlar, teknoloji ne kadar ileri düzeyde olursa olsun yaygınlaşmayı engelleyebilir. Bu teknik olmayan faktörler İnternetin yaygınlaşmasıyla insanların zararlı sitelere yönlenmesinin engellenememesi veya sosyal ağlarda kurulan arkadaşlıkların çoğunlukla sağlam bir zemine oturamaması gibi sosyal gerçekliklerin görülmesine neden olabilmektedir.

Biyometrik teknolojiler için de benzer tartışmalar kimi zaman bu teknolojilerin yaygınlaşmasının önüne zorluklar çıkarmaktadır. Kötü tecrübeler, başarısız uygulamalar, basın-yayın organlarında çıkan haberler biyometrik teknolojilere bakışı olumsuz yönde etkileyebilmektedir. Örneğin, "Azınlık Raporu (Minority Report)", "Devlet Düşmanı (Enemy of the State)" gibi aksiyon filmlerinde ya da "1984" gibi ütopik romanlarda insanların ileri bilgi ve iletişim teknolojileri ile izlendiği ve biyometrik izleme yöntemlerinin özel hayatı bitirme noktasına getirdiği algısı yaygınlaşabilmektir. Bu tip algılar, insanların teknolojiye alışma süresi, genelde ek bir zaman ve maliyet yükü getirmesi gibi daha gerçekçi faktörlerle birleşince teknolojinin kabulü zorlaşabilmektedir.

Olumsuz yönler dışında, teknolojilerin yaygınlaşmasında olumlu algılar da pozitif etki edebilmektedir. Örneğin, İnternet bankacılığının yaygınlaşması insanlara çok ciddi bir zaman tasarrufu sağlamaktadır. eDevlet uygulamaları ile vergi kaçaklarının azalması, nüfus bilgilerine ve adli kayıtlara çabuk ulaşım mümkün olabilmektedir. Otomatik geçiş sistemleri veya hastanelerdeki otomasyon uygulamaları ile insanlar

daha az sıra beklemenin keyfini sürebilmektedir. Biyometrik teknolojiler için de benzer bir olumlu algı yaygınlaşmaktadır. Örneğin, banka hesaplarının güvenliği, elektronik oylamanın gizliliğinin sağlanması, sürekli unutulan ya da güvenlik açığı oluşturan şifrelerin hatırlanmak zorunda olunmayışı, adli vakalarda biyometrik delillere duyulan güven gibi faktörler biyometrik teknolojilerin daha geniş bir kitle tarafından kabul edilmesini sağlamaktadır.

Teknolojilerin kabul edilmesinde, ya da özel olarak biyometrik teknolojilerin kabul görmesinde öne çıkan önemli kavramlardan biri güven duygusudur. Eğer birey ve toplum teknolojiye ve teknolojiyi kabul ettirmeye çalışan kurum ve kişilere güven duyarsa, o teknoloji daha kolay yaygınlaşır. Bunun yanında, teknolojinin pratik oluşu, kolay anlaşılabilmesi, kullanımının kolay olması, insanlara zaman ve para tasarrufu sağlayacak olması gibi faktörler de teknolojinin daha kolay kabul görmesini sağlayabilir. Teknolojinin hem dışa dönük yüzünün hem de iç yapısının mümkün olan en yüksek kalitede tasarlanması, işlerliğinin ve sürekliliğinin sağlanması, hata düzeltme ve geriye dönme esnekliğinin olması teknolojinin kabul görmesinde önemli etkenlerdir.

Tüm bu etkenler, insanların tutumunu ve teknoloji kullanma alışkanlıklarını etkiler. Başarılı örnekler insanların önce birey düzeyinde sonra toplum düzeyinde teknolojiyi kullanmasını tetikler. Böylece aslında davranışsal bir niyet oluşur ki bu niyet aslında teknolojiyi kullanma niyetidir. Sadece biyometrik teknolojiler için değil tüm teknolojiler için geçerli olabilecek bu yaklaşım "Teknoloji Kabul Modeli (Technology Acceptance Model - TAM)" adı altında formüle edilir [65]. Bu tez çalışmasında biyometrik teknolojiler için özelleştirilen, ve BioPSTM ile güven faktörünün modellendiği bir TAM önerilmiş ve "BioTAM [4]" olarak adlandırılmıştır.

3.2 Biyometrik Teknoloji Kabul Modeli- BioTAM

Önerilen BioTAM, TAM'ın BKYS için yenilikçi bir yaklaşımla uyarlanması esasına dayanır. BioTAM'da amaç nihai olarak davranışsal niyetin (Behavioral Intention - BI) nesnel biçimde betimlenebilmesidir. Bunun için TAM ve daha önce BioPSTM olarak adlandırılan güven modeli bir arada kullanılmıştır. Güven (T) modelinde kamusal istekle ve kullanıcıların kendilerini emin hissetmesi ile beraber, mahremiyet

ve güvenlik değerlendirmesi birlikte yapılır. Burada önerilen matematiksel model, İleri ve arkadaşlarının haberleşme teknolojileri için önerdiği üstel bir fonksiyonla açıklanır [13]. TAM ise kullanıcının sisteme karşı tutumu (A: Attitude Toward Using) ile betimlenir. BI, T ve A ya bağlı bir fonksiyon olarak gösterilebilir. BioTAM, güven ve TAM'ı herhangi bir gelişmiş BKYS için uygulayan ilk yöntem olarak literatüre ciddi bir katkı sağlama potansiyeline sahiptir.

BioTAM, algılanan kullanışlılık (perceived usefulness - U), algılanan kullanım kolaylığı (perceived ease of use " E), güven (trust - T), sistemi kullanmadaki davranışsal niyet (behavioral intentions - BI) ve sistemin nihai kullanımı (actual use - A) faktörlerini kapsayan hipotezler üzerine kurulu bir modeldir.

Davis'in tanımına [65] göre algılanan kullanışlılık, U, sistemi kullanan kişilerin öznel anlamda o sistemin sunduğu uygulamalar sayesinde çalıştığı kurum bağlamında kendi iş performansını arttırma olasılığı olarak tanımlanır. BKYS'ler için de geçerli olan bu tanım ekseninde, biyometrik kimlik yönetimi öyle tasarlanmalıdır ki insanların, örneğin eKimlik uygulamalarının, daha hızlı ve kolay yürüdüğüne inançları artsın. U, genel olarak kapsayıcı veya özeldeki başarılı hizmetlerden olumlu etkilenir. Örneğin, BKYS'-lerdeki veri yapısı ve veriye erişim yordamları öyle tanımlanmalıdır ki kullanıcı istediği verimlilikte ve derinlikte aradığı bilgiyi bulabilsin. Burada, çok iyi sınıflandırılmış veriler süreç yönetimini de olumlu etkileyebilir. Bunlara ek olarak, günümüzün eKimlik sistemleri kişisel tercihlere veya profillere göre şekillendirilebilen hizmetler de sunabilmektedir. Kullanıcıyı sürekli uyaran ve kullanıcıyla etkileşebilen efektif çözümler de öne çıkabilmektedir. Bu tip hizmetler U faktörünü olumlu yönde etkileyen ve buna ilişkin skoru arttıran unsurlardır.

Davis'in önerdiği TAM'da [65; 66] algılanan kullanım kolaylığı ise kullanıcının sistemi veya sistemin bir parçasını kullanmasıyla ne derece az efor sarf edeceğine duyduğu inanç olarak tanımlanır. E aslında BKYS'nin dışa bakan yüzünün (örneğin arayüzlerin, dokunmatik ekranların, kioskların, menülerin, kullanım rehberlerinin vs.) kullanıcının işini ne düzeyde kolaylaştırdığının ölçümüdür. Biyometrik sensörlerle ilgili algılanan kullanım kolaylığı BKYS'lerde en çok dikkat edilmesi gereken konulardan biridir. Sensörler üzerindeki ledlerle yönlendirme, ekranlar üzerinde kişilere gösterilen animasyonlar, sesli uyarılar biyometrik kayıtların kalitesini arttıran ve kayıt

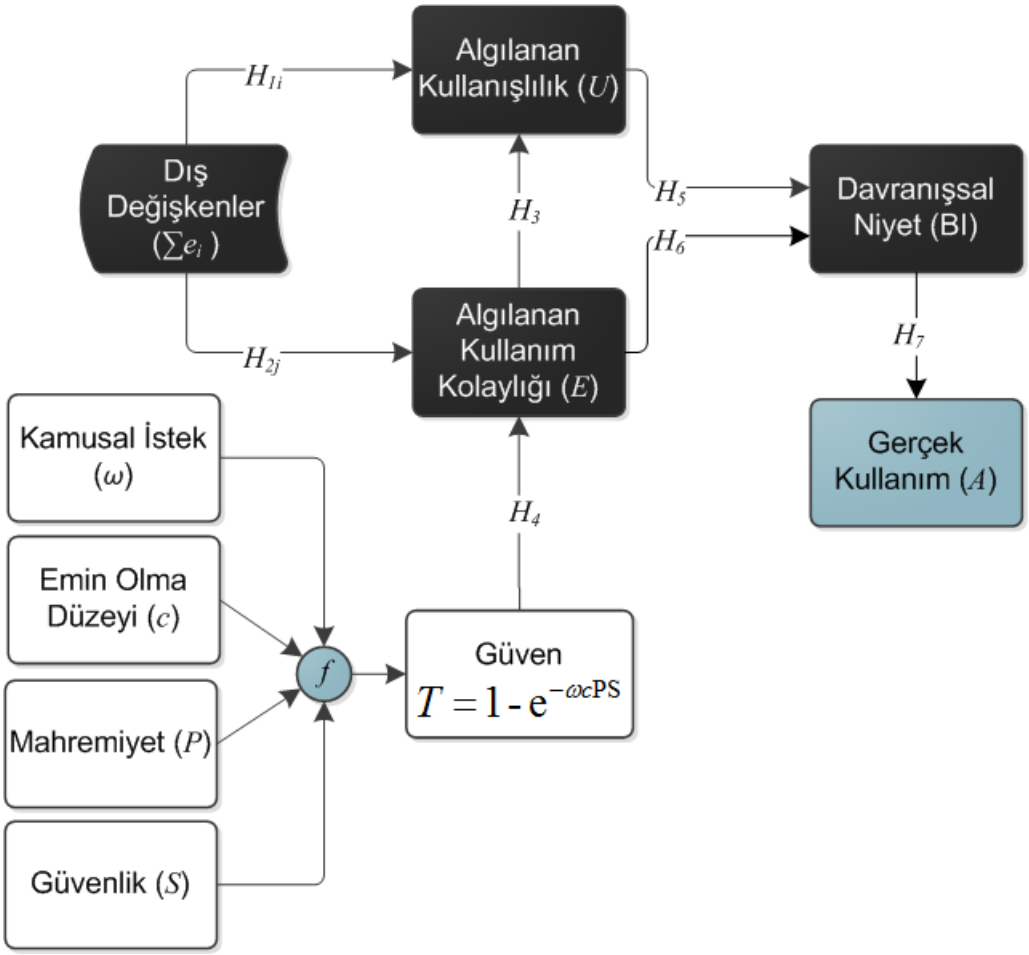
süresini azaltan önlemlerdir. O nedenle uç noktalarda erişim kolaylığının sağlanması, etkin yönlendirme yordamlarının ve uyarı mekanizmalarının tasarlanması BKYS'nin daha kolay kabul edilmesine yardımcı olabilecek unsurlardır.

Hem E hem de U, dışsal faktörlerden etkilenir. Örneğin, kullanıcıların genç olması, artan eHazırOlma (eReadiness), daha iyi hizmet kalitesi, operasyon sürelerinin azalması, 7/24 destek hatları U faktörünü olumlu etkileyen dışsal değişkenlerdir. Benzer biçimde, arayüzlerin kullanıcı dostu olması, dokunmatik ekranların büyüklüğü, kioskların tasarımı, biyometrik sensörlerin üzerindeki ışıklı uyarıların biçimi, sunulan eHizmet adımlarının navigasyonu, kullanıcıları yönlendiren uyarılar ve hatta sistem kullanımı ile ilgili bilgilendirme dokümanlarının tasarımı dahil tüm dışsal değişkenler E yi belirler. Tüm bu dışsal değişkenler $EV = \sum_{i=1}^{N} e_i$ biçiminde teorize edilir. Burada her e_i, kullanıcıların ilgili dışsal değişken için verdikleri 1 ile 5 arasındaki skorlardan (Mean Opinion Score) oluşur ve EV ortalama bir skor verir.

Önerilen BioTAM'daki bir diğer önemli faktör ise güvendir (T). Bölüm 2'de detayları verilen BioPSTM ile modellenen T, mahremiyet, güvenlik, kamusal isteklilik ve kullanıcıların BKYS'yi kullanma konusunda kendilerini emin hissetmesi gibi faktörleri tek bir potada eriterek üstel bir fonksiyon olarak gösterilebilmektedir. BioPSTM, insanların bir BKYS'ye duyacakları güveni öngörmeye çalışan bir kullanıcı kabul olasılık fonksiyonu ile gösterildiği için, mahremiyet veya güvenlik tehditleri hayata geçmeden bir uzgörü sağlar. Normalde TAM bir şekilde sahaya çıkmış bir teknolojinin kabul edilip edilmediğini anlamaya çalışırken, T ile güçlendirilmiş BioTAM, BKYS işler hale gelmeden de insanların bu teknolojiye güven duyup duymayacaklarını anlamaya çalışır. T algılanan kullanım kolaylığını direk olarak etkiler öyle ki insanlar kendilerini BKYS'yi kullanma konusunda daha emin hissederler ve istekli olurlar.

Şekil 3.1'de gösterildiği gibi BioTAM aslında U, E, T, BI, A ve dışsal değişkenler arasındaki ilişkileri hipotezler yoluyla açıklar. Dışsal değişkenlerin U ve E yi, T nin de E yi etkilediği belirtilmiştir. Buna ek olarak E nin U yu, U ve E nin birlikte BI yi, BI nin de direk olarak A yı etkilediği Davis [65; 66] tarafından daha önceki çalışmalarda öne sürülmüştür.

Dışsal değişkenlerle ilgili hipotezler $H_{1i}(i = 1, \ldots N)$ ve $H_{2j}(j = 1, \ldots, M)$



Şekil 3.1 BioTAM.

olarak gösterilir. H_{1i}, U yu etkileyen hipotezler ve N bu hipotezlerin toplam sayısı olarak gösterilmiştir. Benzer biçimde H_{2j}, E yi etkileyen hipotezler ve M de bu hipotezlerin toplam sayısı olarak ifade edilir. Eğer istenirse bu hipotezlere ilişkin dışsal değişkenlerden U veya E için tek bir skor şeklinde hesaplanabilir.

H_{1i} ve H_{2j} haricindeki diğer hipotezler ise şöyledir:

- H_3 : Algılanan kullanım kolaylığı E, algılanan kullanışlılığı U yu olumlu etkiler.
- H_4 : BKYS'ye duyulan güven T, algılanan kullanışlılığı U yu arttırır.
- H_5 : BKYS'yi kullanım sırasındaki algılanan kullanışlılık U, sistemi kullanma konusundaki davranışsal niyeti BI yi olumlu etkiler.
- H_6 : BKYS'yi kullanım sırasındaki algılanan kullanım kolaylığı E, sistemi kullanma konusundaki davranışsal niyeti BI yi olumlu etkiler.

- H_7 : BKYS'yi kullanma konusunda kullanıcıların davranışsal niyeti BI, sistemin gerçek kullanımı A yı olumlu etkiler.

Şekil 3.1'de gösterilen hipotezler ve aralarındaki ilişkileri ifade eden matematiksel model Denklem 3.1-3.7'de gösterilmiştir.

$$U = \alpha_0 + \alpha_1 H_{1i} + \alpha_2 E = EV_1 \leftrightsquigarrow E \tag{3.1}$$

$$E = \beta_0 + \beta_1 H_{2j} + TH_4 = EV_2 \leftrightsquigarrow T \tag{3.2}$$

$$BI = \gamma_0 + \gamma_1 H_5 + \gamma_2 H_6 = U \leftrightsquigarrow E \tag{3.3}$$

$$A = \lambda_0 + \lambda_1 H_7 = BI \tag{3.4}$$

$$H_{1i} = \sum_{i=1}^{N} e_{1i} \tag{3.5}$$

$$H_{2j} = \sum_{j=1}^{M} e_{2j} \tag{3.6}$$

$$T = 1 - e^{-\omega c \mathbf{PS}} \tag{3.7}$$

Burada, α, β, γ ve λ katsayıları (0,1] aralığında gerçel sayılardan oluşmaktadır ve Bio-TAM'daki faktörler arasındaki ilişkilerin ağırlıklarını ifade etmektedir. α_0, β_0, γ_0 ve λ_0 tolerans katsayıları olarak modele eklenmiştir. Böylece, tasarım aşamasında öngörülemeyen ancak bir şekilde etkisi olabilecek tüm diğer faktörlerin modele eklenmesi için bir açık kapı bırakılmış olur. Matematiksel modelde "$\leftrightsquigarrow$" işareti faktörler arasındaki hipotetik ilişkiyi betimler. EV_1 ve EV_2, sırasıyla U ve E yi etkileyen dış faktörlerin toplam etkisini ifade eder. e_{1i} ve e_{2j} ise ($i = 1, \ldots, N$, $j = 1, \ldots, M$), sırasıyla EV_1 ve EV_2 yi etkileyen dış faktörlerin her birini gösterir. T faktörü ise Denklem 2.8 olarak Bölüm 2'de gösterilmiştir.

Yukarıda anılan hipotezler genelde anketlerle ya da kamuoyu yoklamalarıyla incelenir. Her bir hipoteze karşın bir soru kümesinin oluşturulması ayrı bir araştırma alanıdır. Bunun yanında, seçilen denek kümesinin tüm popülasyonu mümkün olduğunca iyi temsil etmesi de önemli unsurlardandır. Popülasyonun uygunluğunu ölçmede chi-kare uygunluk geçerlemesi (chi-square fitness validation) uygulanabilir. Bunun yanında BKYS'de kullanılan teknolojik çözümlerin benzerlerinin kullanım sıklığı ve yaygınlaşma oranları da nesnel değerlendirme kriterleri olarak kullanılabilir. Örneğin,

BKYS'-de kullanılan bir parmak izi sensörünün bir başka ülkede hangi sıklıkla kullanıldığı, kabul oranları, veya satış miktarları da hipotezlere ilişkin değerlendirmelerde ölçüt olarak seçilebilir.

T ile ilgili ölçümlerde mümkün olduğunca çok denekten toplanan biyometrik verilerle sızıntı oranlarının ölçülmesi, hatalı red ve kabul oranlarının tespiti (False Acceptance Rate, False Rejection Rate), kayıt hata oranları (Failure-to-Enroll), biyometrik tanıma hata oranları (Failure-to-Acquire) gibi göstergelerin kullanılması daha nesnel sonuçlar verebilir. Önerilen BioTAM, kuşkusuz başka uygulamalar için geliştirilebilir ya da uyarlanabilir.

Denek kümesinin popülasyonu yeterince temsil ettiğine karar verildikten sonra, geçerlilik ve güvenilirlik testlerinin de yapılması gerekir. Güvenilirlik testlerinde hipotezlere ilişkin değişkenlerin tutarlılıkları değişkenin çoklu ölçümleri ile sağlanır. Güvenilirlik analizinde öne çıkan bir başka tanısal ölçüm ise Cronbachs alfa değerleridir. Değişkenler arasındaki korelasyonları ölçmek de faktörlerin hangisinin hangisi üzerinde daha çok etkisi olduğunu anlamak için yarar sağlar. Son olarak da çoklu regresyon analizi ile BioTAM bileşenlerinin birbirini ne kadar etkilediği ölçülebilir. Örnek bir uygulama için Bölüm 4'e bakılabilir.

4 BioPSTM ve BioTAM için Örnek Uygulamalar

4.1 Örnek Uygulama #1: İngiltere için BioTAM

BioTAM'ın nasıl kullanılabileceğine bir örnek olması açısından Furnell ve Evangeltos'un (2007) İngiltere'de biyometrik sistemlerin kullanımı ile yaptıkları araştırma [72] ile Unisys'in 2008 ve 2009 yıllarında yaptığı çalışmalar [73; 74] temel alınarak, ilgili bulgular BioTAM'a uyarlanmıştır.

Furnell ve Evangeltos'un çalışmasında, biyometrik farkındalık (biometric awareness), biyometrikler için beklenen güvenilirlik (reliability), tercih rankı, kimlik dokümanlarına biyometriklerin eklenmesi konusunda kullanıcıların desteği, algılanan kullanışlılık ve gizlilik düzeyi gibi faktörler, kimlik çalınması, sağlık riskleri ve kopyalama gibi durumlar göz önünde bulundurularak ölçülmüştür. Anket yönteminin kullanıldığı bu 4 aylık çalışmada anketler basılı veya elektronik ortamda deneklerle buluşturulmuştur. 350 e-ileti davetiyesine 154 kişi olumlu yanıt vermiş ve buna ek olarak 80 kişiye de basılı anket dağıtılmıştır. Bu 80 kişiden 55'i geri dönüş yapmış ve böylece toplamda 154+55=209 kişilik bir denek kümesine ulaşılmıştır. Deneklerin %57'si bayan iken %81'i 30 yaş altındadır. Furnell ve Evangeltos'un bu çalışmasında parmak izi için biyometrik farkındalık ve biyometrik teknolojileri kullanma oranları, sırasıyla %84 ve %16 olarak ölçülmüştür. Benzer biçimde yüz biyometriği için popülasyonun %67'si yüzün bir biyometrik olduğunun farkında iken sadece %4'ü bu biyometriği etkin biçimde kullanmaktadır.

Furnell ve Evangeltos'un çalışmasının BioTAM için önemli yanı parmak izi ve yüz biyometriği için E ve U faktörlerini küçük bir küme için de olsa ölçmüş olmalarıdır. Çizelge 4.1'de Furnell ve arkadaşlarının ölçümleri ile Unisys araştırmalarından elde edilen değerler ve bunların BioTAM için ne anlam ifade ettikleri gösterilmiştir.

Ölçülen Etmen	Kaynak	Analiz Sonuçları	İlgili BioTAM Terimi	Normalize Değer
Parmak izi teknolojilerinin kullanım rahatlığı	Furnell ve Evangeltos [72]	%59 (tamamen rahat), %24 (rahat)	E_{fp}	0,59+0,24=0,83
Yüz biyometriği teknolojilerinin kullanım rahatlığı	Furnell ve Evangeltos [72]	%36 (tamamen rahat), %25 (rahat)	E_{face}	0,36+0,25=0,61
Biyometriklerin ulusal kimlik kartlarında kullanımı ile ilgili algılanan kullanışlılık	Furnell ve Evangeltos [72]	%53	U	0,53
Biyometriklerin ulusal kimlik kartlarında kullanımı ile ilgili davranışsal tutum	Unisys araştırmaları[73; 74]	%32 (kesinlikle destekliyorum), %27 (destekliyorum)	BI	0,32+0,27=0,59
Parmak izlerinin gerçek kullanımı	Furnell ve Evangeltos [72]	%16	A_{fp}	0,16
Yüz biyometriğinin gerçek kullanımı	Furnell ve Evangeltos [72]	%4	A_{face}	0,04
Biyometriklerin sadece ulusal kimlik kartıiçin kullanılacağına olan inanç	Furnell ve Evangeltos [72]	%5 (kesinlikle inanıyorum) %15 (inanıyorum)	c	0,05 + 0,15=0,20 (MOS=1,0)
Parmak izlerinin kullanılması yönünde kamusal istek	Unisys araştırmaları [73; 74]	%75	ω_{fp}	0,75 (MOS=3,75)
Yüz biyometriğinin kullanılması yönünde kamusal istek	Unisys araştırmaları [73; 74]	%67	ω_{face}	0,67 (MOS=3,35)

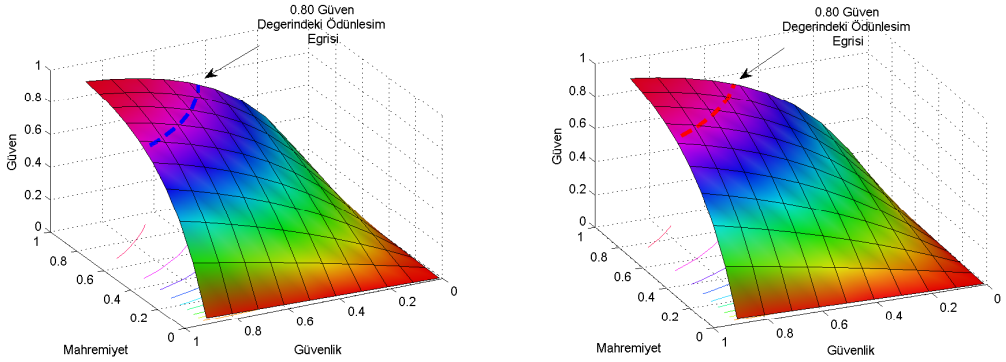
Çizelge 4.1 İngiltere'nin ulusal kimlik kartı uygulamaları için BioTAM verileri.

Çizelge 4.1.'deki değerler ışığında parmak izi ve yüz biyometriği için elde edilen güven dağılımları, T_{fp} ve T_{face}, BioPSTM modeline göre sırasıyla şöyledir (Bkz. Denklem 4.1 ve 4.2):

$$T_{fp}(\mathbf{P},\mathbf{S}) = 1 - e^{-3{,}75\mathbf{PS}} \tag{4.1}$$

$$T_{face}(\mathbf{P},\mathbf{S}) = 1 - e^{-3{,}35\mathbf{PS}} \tag{4.2}$$

Örnek olması açısından, T_{fp} ve T_{face} dağılımları ve $T_{fp} = T_{face} = 0,80$ kesitindeki ödünleşim eğrileri Şekil 4.1'de görülebilir. $T_{fp} = T_{face} = 0,80$ kesitindeki ödünleşim eğrilerinin iki boyutlu uzaydaki gösterimi ise Şekil 4.2'de gösterilmiştir.

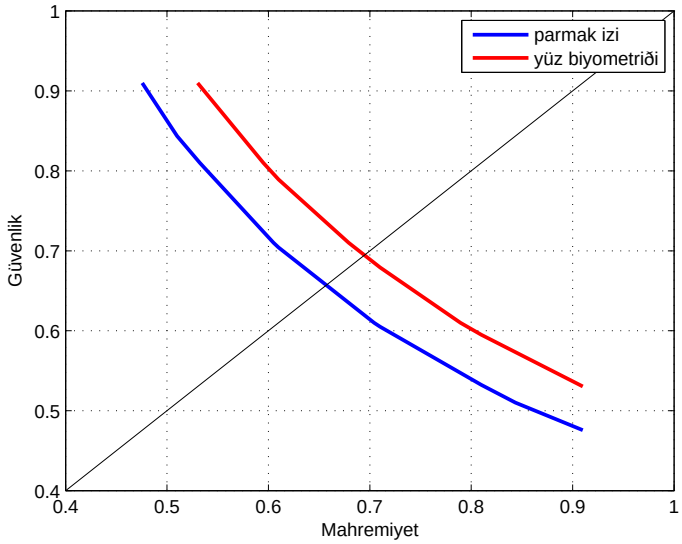


(a) (b)

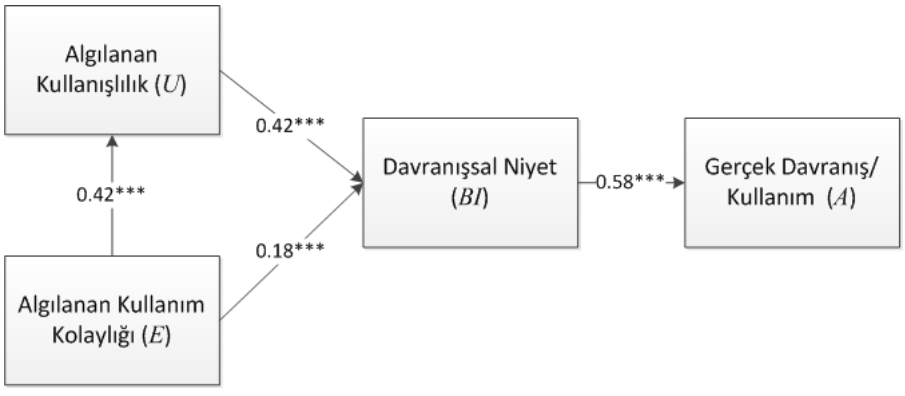
Şekil 4.1 İngiltere'deki ulusal kimlik kartı uygulamalarında güven dağılımları.

BioTAM modelinin İngiltere'deki ulusal kimlik kartı uygulamasına uyarlanmasında Çizelge 4.1'deki değerler yanında, E, U, BI ve gerçek kullanım A arasındaki ilişkileri de ölçmek gerekir. Literatürde İngiltere özelinde bu konuda malesef ciddi bir çalışma bulunamamıştır. Ancak Davis ve arkadaşlarının 1989 yılında yayınladıkları ve temel referanslardan biri kabul edilen çalışmasında [66] teknoloji kabul modelinin genel anlamda tüm bilgi sistemleri için nasıl uygulandığı gösterilmiştir. Şekil 4.3'te gösterilen modelde bir bilgi sisteminin teknoloji kabul modeli, U, E, BI ve A arasındaki Cronbach değerleri ve istatistiksel anlamlılığı ifade eden p ölçütleri görülebilir.

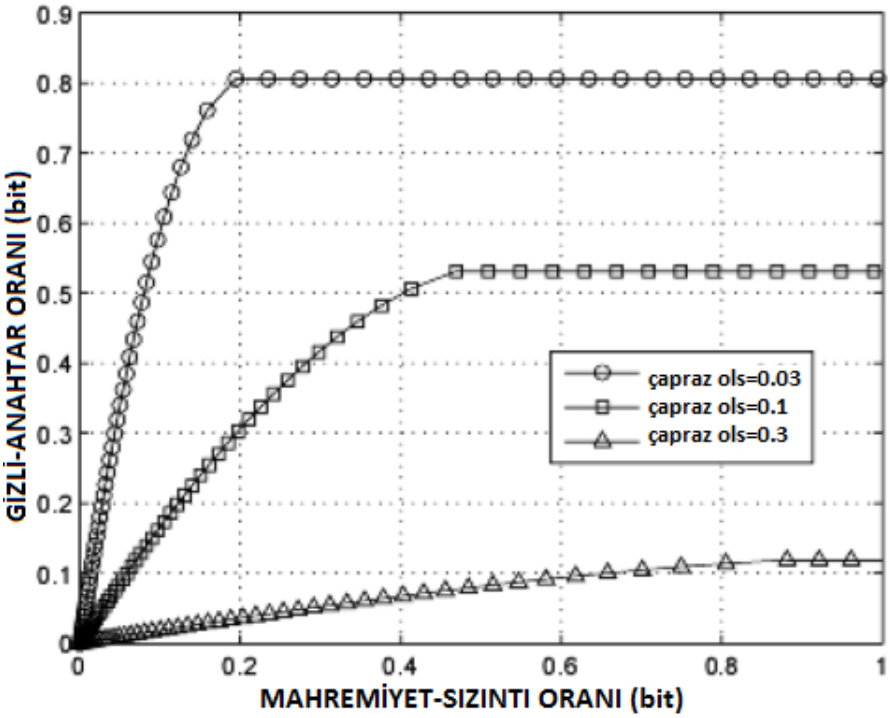
BioTAM'daki tüm parametreleri tamamlamak amacıyla **P** ve **S** için uygun değerlerin seçilmesi gerekir. Bunun için, Ignatenko ve Willems tarafından 2009 yılında yayınlanan ve Şekil 4.4'deki mahremiyet-sızıntısının (privacy leakage) gizli-anahtar oranıyla (secret-key rate) ilişkisini gösteren grafikten yararlanılmıştır [48]. Bu grafikte



Şekil 4.2 $T_{fp} = T_{face} = 0,80$ kesitindeki ödünleşim eğrileri.



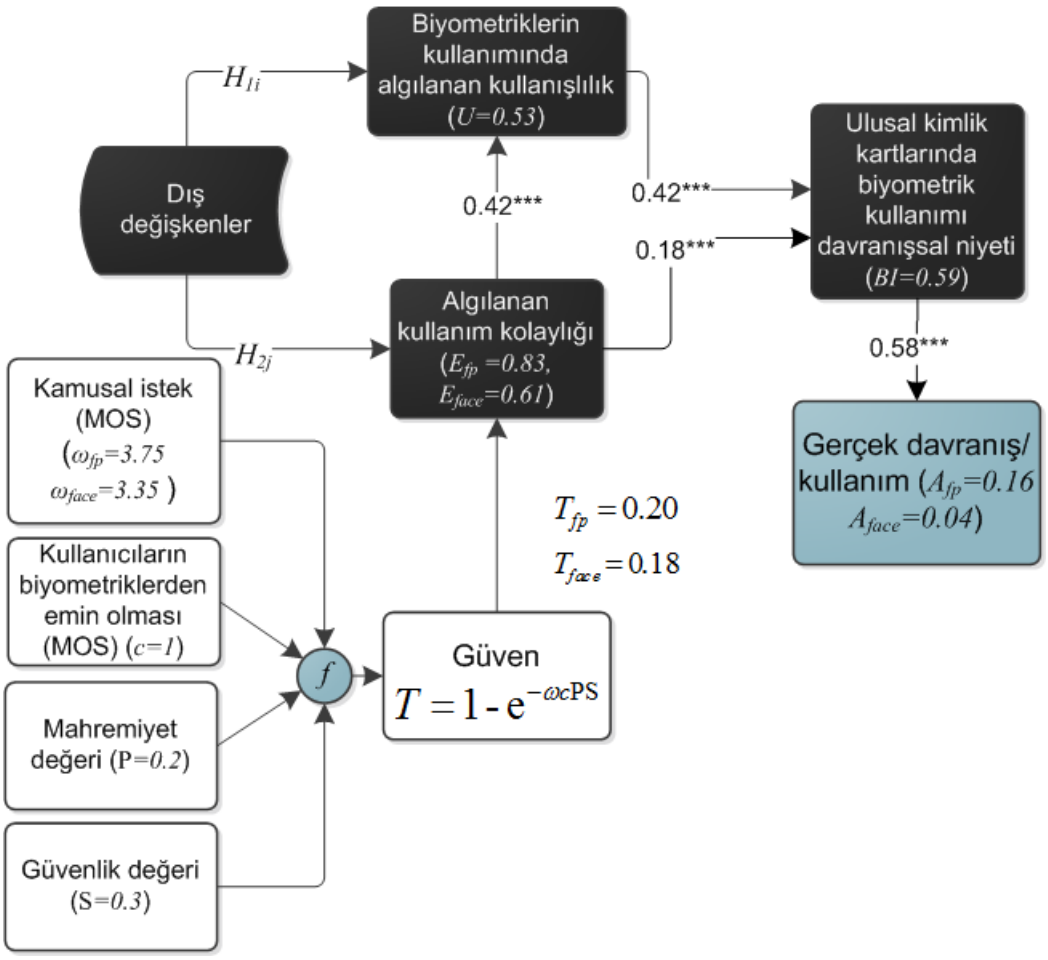
Şekil 4.3 Davis tarafından bilgi sistemleri için önerilen teknoloji kabul modeli.



Şekil 4.4 Mahremiyet-sızıntı oranının gizli-anahtar oranı ile ilişkisi [48].

0,003 çapraz geçiş olasılığında (cross-over probability) mahremiyet-sızıntı oranının 0,3 olduğu yerde gizli-anahtar oranının 0,2 olarak ölçüldüğü görülmüştür. Bu değerler sırasıyla $\mathbf{P} = 0,3$ ve $\mathbf{S} = 0,2$ olarak kabul edilmiştir. Burada, örnek olması için rasgele seçilen bu değerlerin gerçek uygulamalarda daha derinlemesine analizlerle belirlenmesi gerekir.

Tüm bu değerler, Çizelge 4.1'deki oranlar ve Şekil 4.3'teki bulgularla birleştirildiğinde İngiltere'deki ulusal kimlik kartlarında parmak izi veya yüz biyometriği kullanımı durumundaki BioTAM Şekil 4.5'de gösterilmiştir. Şüphesiz, Şekil 4.5'deki BioTAM gerçek verilerin bir kolajı olarak sunulmuştur ve bir bütün olarak bakıldığında gerçeği tam olarak yansıtmamaktadır. Ancak bu model, BioTAM'ın nasıl kullanılabileceğine ve ilgili bileşenlerin nasıl hesaplanabileceğine dair güzel bir örnek teşkil etmektedir. Karar verici bu modeldeki düğüm ve bağlantı değerlerini kullanarak nihai bir skor elde edebilir. Bu skor aslında ilgili teknolojinin göreceği genel kabulü ifade etmiş olur. Daha gerçekçi sonuçlar için aynı denek kümesinde, çok daha geniş bir popülasyonda, uzun soluklu değerlendirmelerin yapılması gerekir.



Şekil 4.5 İngiltere'nin ulusal kimlik kartı projesi için BioTAM.

4.2 Örnek Uygulama #2: Ülkeler için BioPSTM

Önerilen matematiksel modelin nasıl kullanılabileceğini göstermek üzere, biyometrik teknolojileri çeşitli alanlarda kullanan ülkelerdeki eğilimler esas alınarak, bu ülkelerin güven dağılımları çıkarılmıştır. Bunun için ζ, η ve ω parametreleri için kestirimlerde bulunulmuştur. Kestirimlerde UNISYS Security Indexing ve "Privacy International Organization" (*www.privacyinternational.org*) kaynaklarındaki anket çalışmaları baz alınmıştır. Bu çalışmalardaki kriterler ve hesaplama yöntemi Çizelge 4.2'de görülebilir.

Mahremiyet duyarlılığı, *www.privacyinternational.org* sitesindeki değerlendirme kriterlerine göre 1 ile 5 arasında notlandırılmıştır. 5, o ülkede ilgili kriterde mahremiyet çekincesinin hiç olmadığını ifade eder. Değerlendirmeye katılan ülkeler Avustralya -AU, Belçika-BE, Brezilya-BR, Fransa-FR, Almanya-DE, Hong Kong-HK, İtalya -IT, Malezya-MY, Hollanda-NL, Yeni Zelanda-NZ, İspanya-ES, İngiltere-UK ve ABD-US'dir. Çizelge 4.3'te bu ülkelerin mahremiyet notları ve (Çizelge 4.2'deki hesaplama yöntemiyle hesaplanan) mahremiyet değerlendirmeleri görülebilir. Bazı ülkelerdeki mahremiyet kriterleri ile ilgili değerlendirmeler mevcut değildir. Bu durumda ilgili kriterler yok sayılarak, bir şekilde veri sağlanan kriterlerle ilgili skorların aritmetik ortalaması alınmıştır.

Mahremiyet Kriterleri	Sembol	Ulusal Güvenlik	Finansal Güvenlik	Internet Güvenliği	Kişisel Güvenlik
Sınır geçişi	a				√
Haberleşme verisi saklama	b			√	
Veri paylaşımı	c		√	√	
Finansal hareket	d		√		
Devletin verilere ulaşımı	e	√			
Kimlik kartları ve biyometrikler	f				√
Kanuni koruma	g	√			
Görsel istihbarat	h	√			
		(e+g+h)/3	(c+d)/3	(b+c)/2	(a+f)/2

Çizelge 4.2 Mahremiyet ve güvenlik kriterleri.

Güvenlik ve kamusal isteklilik parametrelerinin belirlenmesi için UNISYS Security Index parametreleri [73; 74] kullanılmıştır. Güvenlik ağırlığı ζ için, her kriterin 0-300 aralığındaki Unisys değerleri [1-5] aralığına normalize edilmiştir. Böylece mahremiyet ağırlıklandırılmasıyla paralellik sağlanmıştır. Kamusal isteklilik parametresi

Mahremiyet kriterleri	AU	BE	BR	FR	DE	IT	MY	NL	NZ	ES	UK	US
a	1	2	2	1	2	3	1	2	-	-	1	1
b	4	2	2	1	1	1	3	1	3	2	1	3
c	2	1	2	1	4	-	1	1	2	-	1	2
d	1	3	1	2	4	2	1	2	2	1	1	1
e	2	3	2	1	3	2	1	2	2	2	2	2
f	3	1	2	2	2	2	1	1	3	1	1	1
g	2	4	2	2	4	4	2	4	2	4	2	1
h	-	-	2	2	2	3	1	2	-	2	1	1

Çizelge 4.3 Mahremiyet değerlendirmeleri (*www.privacyinternational.org*).

ω ise UNISYS'in anketleri sonucunda ulaşılan 0-100 arasındaki değerlerdir ve gene [1-5] aralığına normalize edilmiştir. Çizelge 4.4'te ülkelere göre η, ζ ve ω değerleri görülebilir. Çizelge 4.5.'te ise, Çizelge 4.4'teki değerler ışığında ülkelere göre farklı uygulama alanları (ulusal, finansal, kişisel güvenlik ve Internet güvenliği) ve biyometrik kipler (parmak izi, yüz) için $T(\mathbf{S}, \mathbf{P})$ fonksiyonları verilmiştir.

Çizelge 4.4 Ülkelere göre η, ζ ve ω değerlendirmeleri.

Alan	AU	BE	BR	FR	DE	IT	MY	NL	NZ	ES	UK	US
Mahremiyet Ağırlığı η												
Ulusal Güvenlik	2	3,5	2	1,7	3	3	1,3	2,7	2	2,7	1,7	1,3
Finansal Güvenlik	1,5	2	1,5	1,5	4	2	1	1,5	2	1	1	1,5
Internet Güven-ligi	3	1,5	2	1	2,5	1	2	1	2,5	2	1	2,5
Kişisel Güvenlik	2	1,5	2	1,5	2	2,5	1	1,5	3	0,5	1	1
Güvenlik Ağırlığı ζ												
Ulusal Güvenlik	117 (2)	80(2)	205(4)	90(2)	146(3)	113(2)	187(4)	74(2)	124(3)	169(3)	124(3)	161(3)
Finansal Güvenlik	127(3)	110(2)	186(4)	95(2)	162(3)	115(2)	155(3)	96(2)	123(3)	156(3)	141(3)	152(3)
Internet Güven-liği	100(2)	93(2)	148(3)	91(2)	164(3)	78(2)	121(3)	96(2)	111(2)	91(2)	111(2)	127(3)
Kişisel Güvenlik	111(2)	102(2)	187(4)	79(2)	167(3)	99(2)	179(3)	84(2)	108(2)	136(3)	133(3)	140(3)
Kamusal isteklilik ω												
ω_{fp}	72(4)	61(4)	71(4)	58(3)	62(4)	63(4)	63(4)	80(4)	71(4)	69(4)	75(4)	72(4)
ω_{face}	61(4)	40(2)	47(3)	37(2)	43(3)	35(2)	22(2)	59(3)	45(3)	42(3)	67(4)	52(3)

Çizelge 4.5 Ülkelere göre T fonksiyonları.

Ülke	Biyometrik	Ulusal Güvenlik	Finansal Güvenlik	Internet Güvenliği	Kişisel Güvenlik
AU	Parmak izi	$1-e^{-4S^2P^2}$	$1-e^{-4S^3P^{1,5}}$	$1-e^{-4S^2P^3}$	$1-e^{-4S^2P^2}$
	Yüz	$1-e^{-4S^2P^2}$	$1-e^{-4S^3P^{1,5}}$	$1-e^{-4S^2P^3}$	$1-e^{-4S^2P^2}$
BE	Parmak izi	$1-e^{-4S^2P^{3,5}}$	$1-e^{-4S^2P^2}$	$1-e^{-4S^2P^{1,5}}$	$1-e^{-4S^2P^{1,5}}$
	Yüz	$1-e^{-2S^2P^{3,5}}$	$1-e^{-2S^2P^2}$	$1-e^{-2S^2P^{1,5}}$	$1-e^{-2S^2P^{1,5}}$
BR	Parmak izi	$1-e^{-4S^4P^2}$	$1-e^{-4S^4P^{1,5}}$	$1-e^{-4S^3P^2}$	$1-e^{-4S^4P^2}$
	Yüz	$1-e^{-3S^4P^2}$	$1-e^{-3S^4P^{1,5}}$	$1-e^{-3S^3P^2}$	$1-e^{-3S^4P^2}$
FR	Parmak izi	$1-e^{-3S^2P^{1,7}}$	$1-e^{-3S^2P^{1,7}}$	$1-e^{-3S^2P}$	$1-e^{-3S^2P^{1,5}}$
	Yüz	$1-e^{-2S^2P^{1,7}}$	$1-e^{-2S^2P^{1,7}}$	$1-e^{-2S^2P}$	$1-e^{-2S^2P^{1,5}}$
DE	Parmak izi	$1-e^{-4S^3P^3}$	$1-e^{-4S^3P^4}$	$1-e^{-4S^3P^{2,5}}$	$1-e^{-4S^3P^2}$
	Yüz	$1-e^{-3S^3P^3}$	$1-e^{-3S^3P^4}$	$1-e^{-3S^3P^{2,5}}$	$1-e^{-3S^3P^2}$
IT	Parmak izi	$1-e^{-4S^2P^3}$	$1-e^{-4S^2P^2}$	$1-e^{-4S^2P}$	$1-e^{-4S^2P^{2,5}}$
	Yüz	$1-e^{-2S^2P^3}$	$1-e^{-2S^2P^2}$	$1-e^{-2S^2P}$	$1-e^{-2S^2P^{2,5}}$
MY	Parmak izi	$1-e^{-4S^4P^{1,3}}$	$1-e^{-4S^3P}$	$1-e^{-4S^3P^2}$	$1-e^{-4S^3P}$
	Yüz	$1-e^{-2S^4P^{1,3}}$	$1-e^{-2S^3P}$	$1-e^{-2S^3P^2}$	$1-e^{-2S^3P}$
NL	Parmak izi	$1-e^{-4S^2P^{2,7}}$	$1-e^{-4S^2P^{1,5}}$	$1-e^{-4S^2P}$	$1-e^{-4S^2P^{1,5}}$
	Yüz	$1-e^{-3S^2P^{2,7}}$	$1-e^{-3S^2P^{1,5}}$	$1-e^{-3S^2P}$	$1-e^{-3S^2P^{1,5}}$
NZ	Parmak izi	$1-e^{-4S^3P^2}$	$1-e^{-4S^3P^2}$	$1-e^{-4S^2P^{2,5}}$	$1-e^{-4S^2P^3}$
	Yüz	$1-e^{-3S^3P^2}$	$1-e^{-3S^3P^2}$	$1-e^{-3S^2P^{2,5}}$	$1-e^{-3S^2P^3}$
ES	Parmak izi	$1-e^{-4S^3P^{2,7}}$	$1-e^{-4S^3P}$	$1-e^{-4S^2P^2}$	$1-e^{-4S^3P^{0,5}}$
	Yüz	$1-e^{-3S^3P^{2,7}}$	$1-e^{-3S^3P}$	$1-e^{-3S^2P^2}$	$1-e^{-3S^3P^{0,5}}$
UK	Parmak izi	$1-e^{-4S^3P^{1,7}}$	$1-e^{-4S^3P}$	$1-e^{-4S^2P}$	$1-e^{-4S^3P}$
	Yüz	$1-e^{-4S^3P^{1,7}}$	$1-e^{-4S^3P}$	$1-e^{-4S^2P}$	$1-e^{-4S^3P}$
US	Parmak izi	$1-e^{-4S^3P^{1,3}}$	$1-e^{-4S^3P^{1,5}}$	$1-e^{-4S^3P^{2,5}}$	$1-e^{-4S^3P}$
	Yüz	$1-e^{-3S^3P^{1,3}}$	$1-e^{-3S^3P^{1,5}}$	$1-e^{-3S^3P^{2,5}}$	$1-e^{-3S^3P}$

Çizelge 4.3 ve 4.4'teki değerler ışığında, örnek olması açısından ulusal, finansal ve kişisel güvenlik ile Internet güvenliği bağlamında 12 ülkenin parmak izi ve yüz biyometriği için güven dağılımları Şekil 4.6-4.13'de görülebilir. Grafiklerden de görüleceği gibi parmak izinin yüz biyometriğine göre daha çok kabul gördüğü söylenebilir. Bununla beraber, BKYS'nin ulusal güvenlik ve finansal güvenlik alanında kullanımının daha çok kabul gördüğü ve buna ilişkin mahremiyet ve güvenlik ağırlıklarının daha yüksek olduğu ortaya çıkmaktadır. Ülkeler bazında bir değerlendirme yapıldığında, örneğin Brezilya halkının güvenlik ile ilgili tehditlerle BKYS'nin başa çıkmasında, hizmet sağlayıcılara daha az güven duyduğu gözlenmektedir. Buna karşın, Hollanda, Fransa ve İngiltere'nin BKYS'lere nispeten daha çok güven duyduğu çıkarımı yapılabilir. En çarpıcı sonuçlardan biri İspanya, Malezya ve İngiltere'nin güvenliğe mahremiyete nazaran daha çok önem vermesidir. Dağılımlarda T'nin yüksek değerleri için geniş düzlüklere fazla rastlanmamıştır. Bu durum gösteriyor ki 12 ülkede

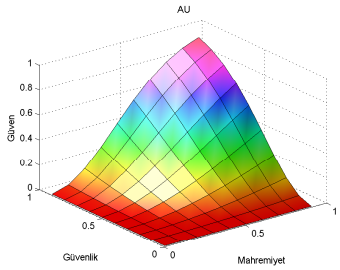
de BKYS'lere geniş çapta güven duyulmamaktadır. 12 ülkenin de BKYS'lere bakışı birbirinden çok farklı değildir. Ancak küçük farklılıklar göze çarpmaktadır. Bunun birkaç sebebi olabilir. Herşeyden önce BKYS'ler yeni yeni gelişen teknolojilerdir ve gelişmiş ülkelerde bile biyometrik güvenlik konusunda bir bilinç oluşmamış olabilir. Bununla beraber, basın-yayın organlarının, özellikle Internet'in gelişmesiyle kültürler arası difüzyonun arttığı, bu nedenle global ölçekte insanların davranışlarının ve algılarının birbirine yakınsadığı düşünülebilir. Bu yakınsama nedeniyle güven dağılımları birbirine yakın çıkabilmektedir. Bu çıkarımların daha geniş ölçekte değerlendirilmesi ve sosyologlar tarafından derinlemesine incelenmesi gerekir. Güzel olan nokta şudur ki, bu tez çalışmasında önerilen BioPSTM'nin sosyologların kullanabilecekleri nesnel bir karşılaştırma zemini sunmasıdır. Örnek olması açısından, $T = 0,7$ için parmak izine veya yüz biyometriğine dayalı BKYS'lerin ulusal, finansal, kişisel güvenlik ile Internet güvenliği alanlarındaki kullanımlarında mahremiyet-ödünleşim eğrileri de Şekil 4.14'de sunulmuştur.

Çizelge 4.6'te görüleceği gibi ulusal güvenlik alanında parmak izi uygulamalarında BKYS'lere duyulan güven yeterli seviyede kabul edilebilir. Hemen hemen tüm ülkelerde ulaşılabilecek azami güven değeri 0.9 üzerindedir. Genelde mahremiyet ve güvenlik ağırlıkları birbirine yakındır. Ancak Belçika'da güvenlik mahremiyete göre daha öncelikli bir konu olarak değerlendirilebilir. Öte yandan, güvenliğe nazaran mahremiyete daha çok önem veren ğlkeler Brezilya, Malezya, İngiltere ve ABD'dir.

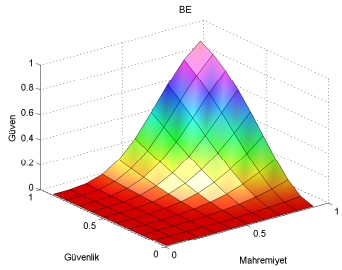
Çizelge 4.7'de ulusal güvenlik uygulamalarında yüz biyometriğinin kullanımı ele alınmıştır. Güven yüzeylerinden de görüleceği gibi parmak iziyle karşılaştırıldığında yüz biyometriğinin kullanılıdyğı BKYS'lere güven nispeten daha azdır. Avusturya, Yeni Zelanda, ABD ve İngiltere'de güven değerlerinin diğer ülkelere göre daha yüksek olduğu söylenebilir. Ancak özellikle Belçika, İtalya ve Malezya'da çıkılabilen azami güven değeri 0.6 düzeylerindedir. Genelde mahremiyet ve güvenlik ağırlıkları birbirine yakın olsa da mahremiyete, güvenliğe nazaran, daha çok önem veren ülkeler Brezilya, Malezya, İngiltere ve ABD'dir.

Finans uygulamalarındaki güven dağılımları ise Çizelge 4.8 ve 4.9'da gösterilmiştir. Ulusal güvenlik uygulamalarında olduğu gibi finans alanında da parmak izinin kullanıldığı BKYS'lere güven yüksek düzeydedir. Tüm ülkelerde erişilebilecek

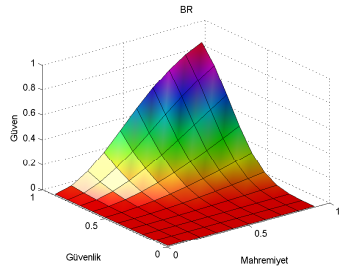
Çizelge 4.6 Ulusal güvenlikte parmak izine dayalı güven dağılımları.



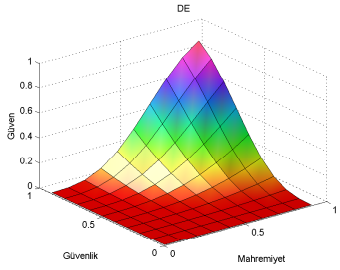
AU



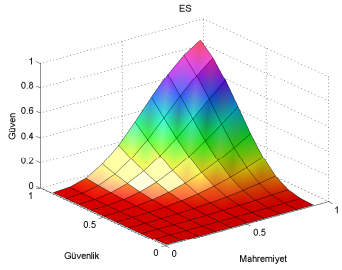
BE



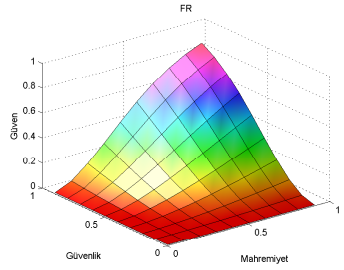
BR



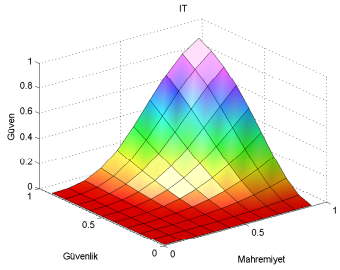
DE



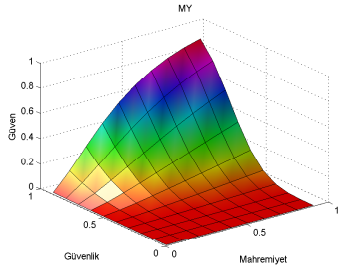
ES



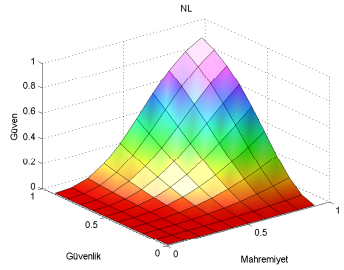
FR



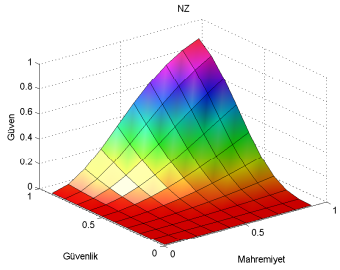
IT



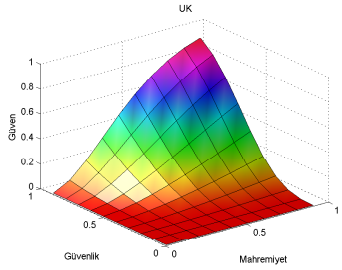
MY



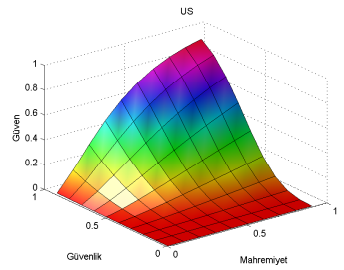
NL



NZ

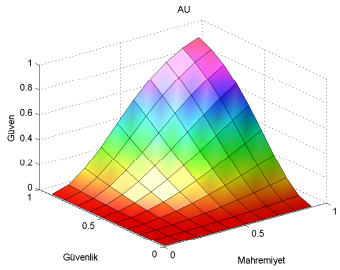


UK

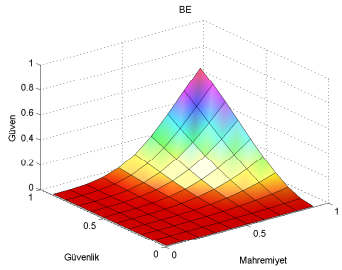


US

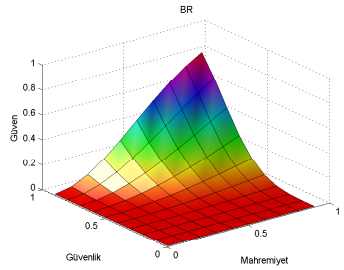
Çizelge 4.7 Ulusal güvenlikte yüz biyometriğine dayalı güven dağılımları.



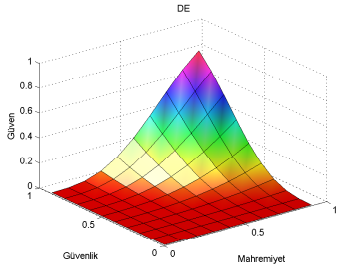
AU



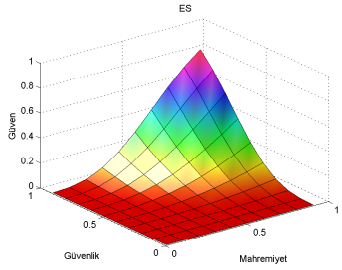
BE



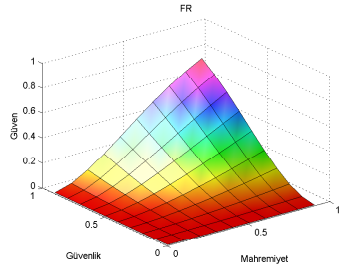
BR



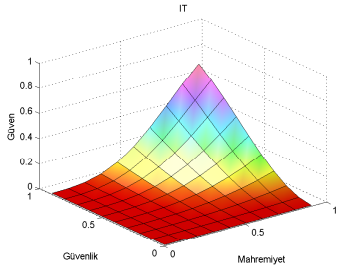
DE



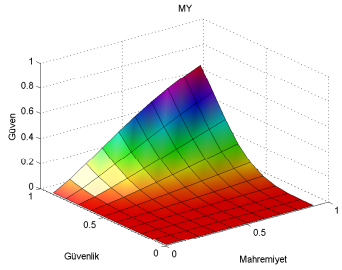
ES



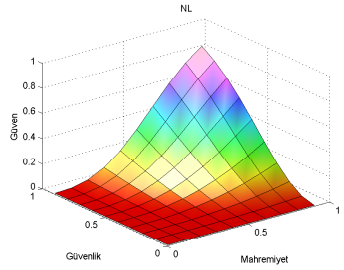
FR



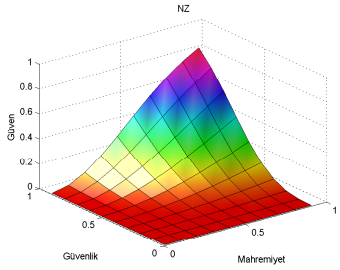
IT



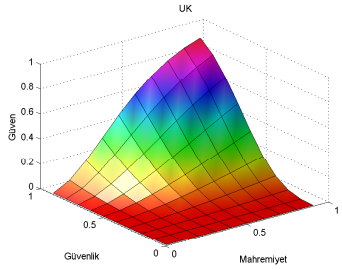
MY



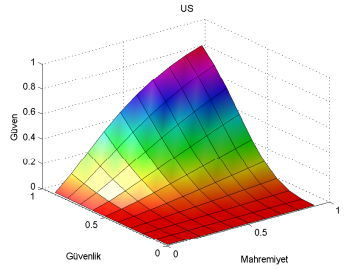
NL



NZ



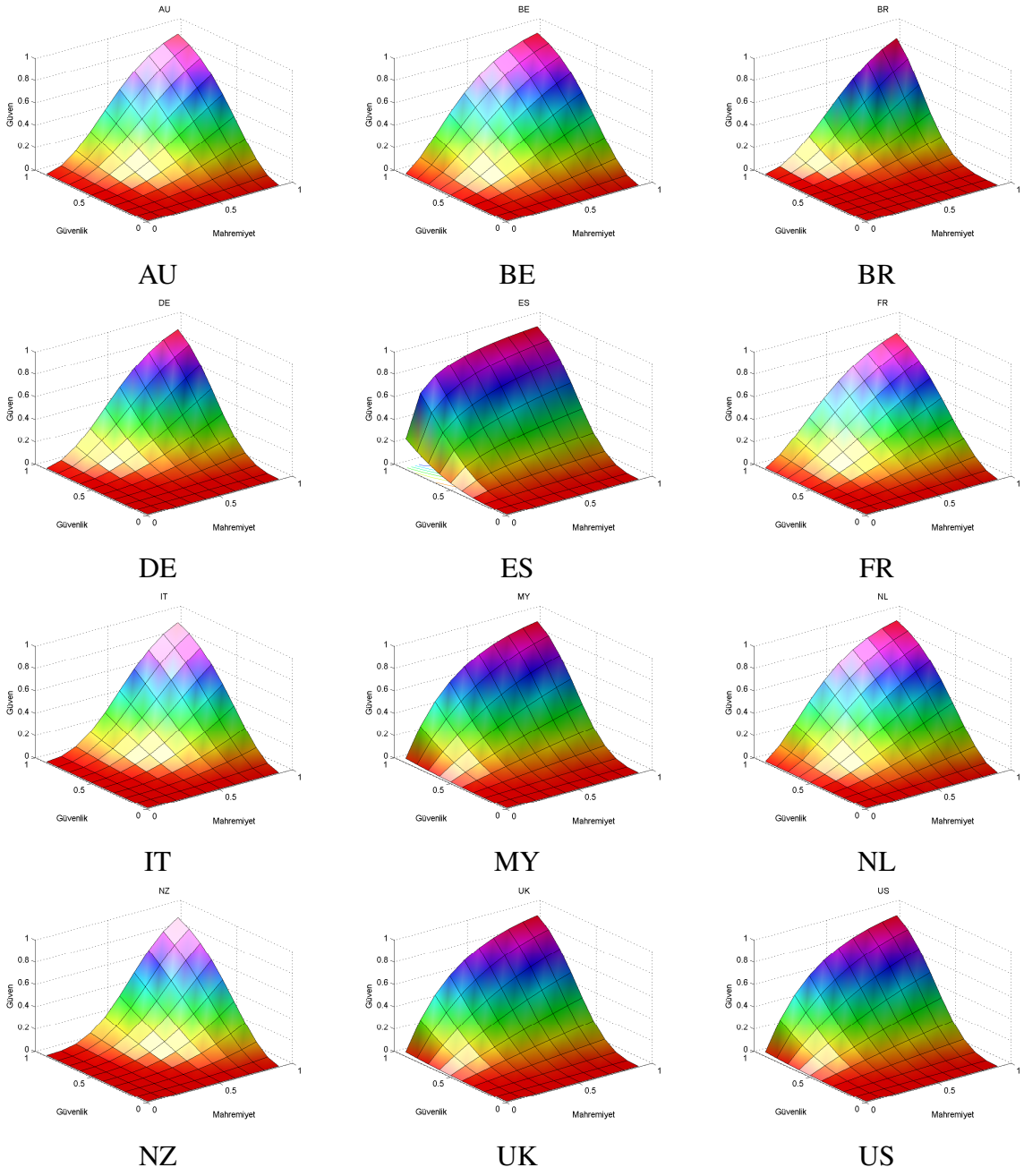
UK



US

azami güven değeri 0.9 üzerindedir. Burada en çarpıcı sonuçlardan biri İspanya'da görülmüştür. İspanya'da halk, mahremiyete güvenliğe göre çok daha fazla öncelik tanımaktadır. Benzer biçimde Brezilya, İngiltere ve ABD'de mahremiyet güveni daha fazla etkileyen bir faktör olarak ortaya çıkmaktadır.

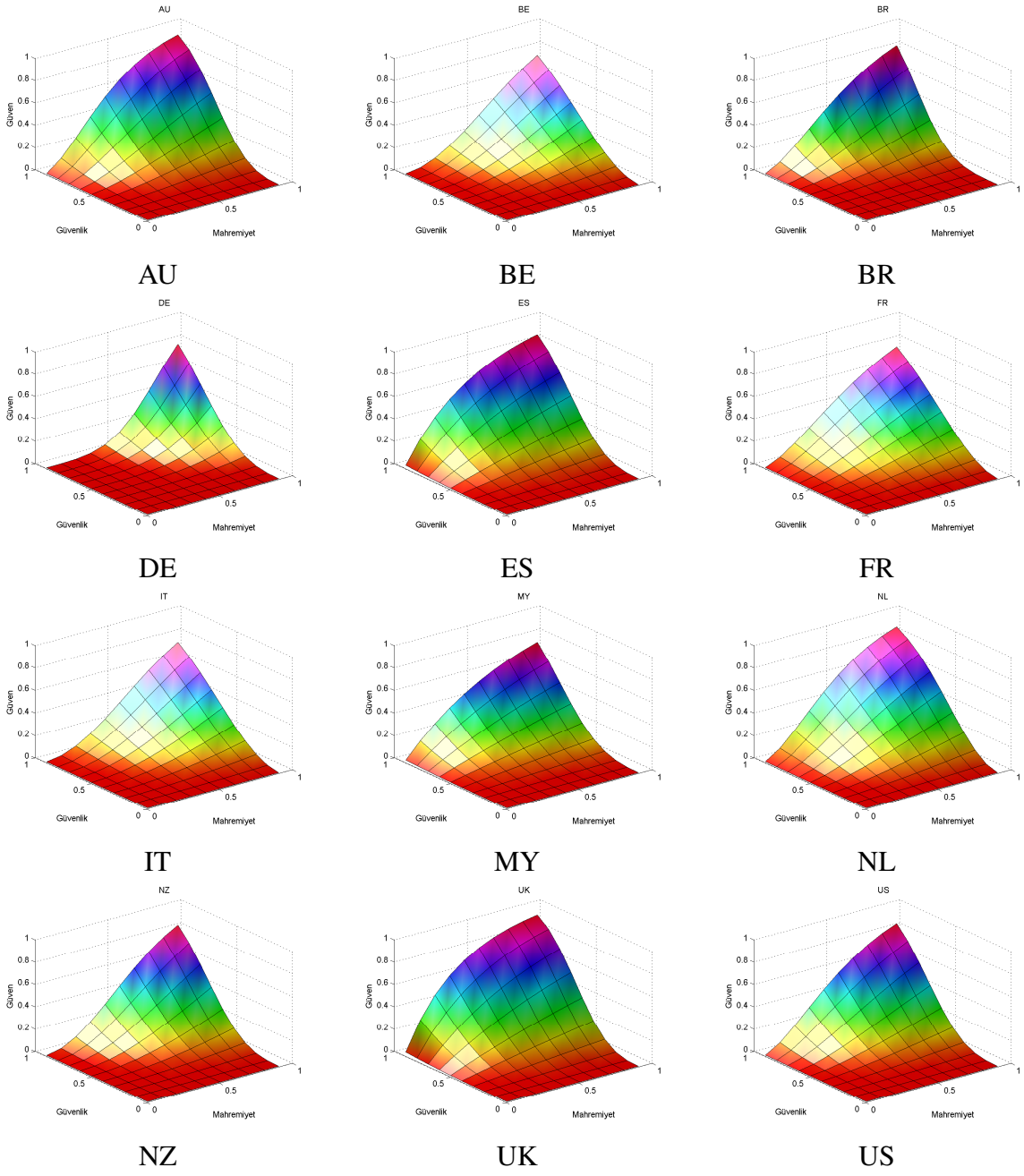
Çizelge 4.8 Finans uygulamalarında parmak izine dayalı güven dağılımları.



Çizelge 4.9'da yansıtılan, yüz biyometriğine dayalı BKYS'lerin finans alanında uygulanması durumunda ise gene ulusal güvenlikte olduğu gibi güven seviyeleri düş-

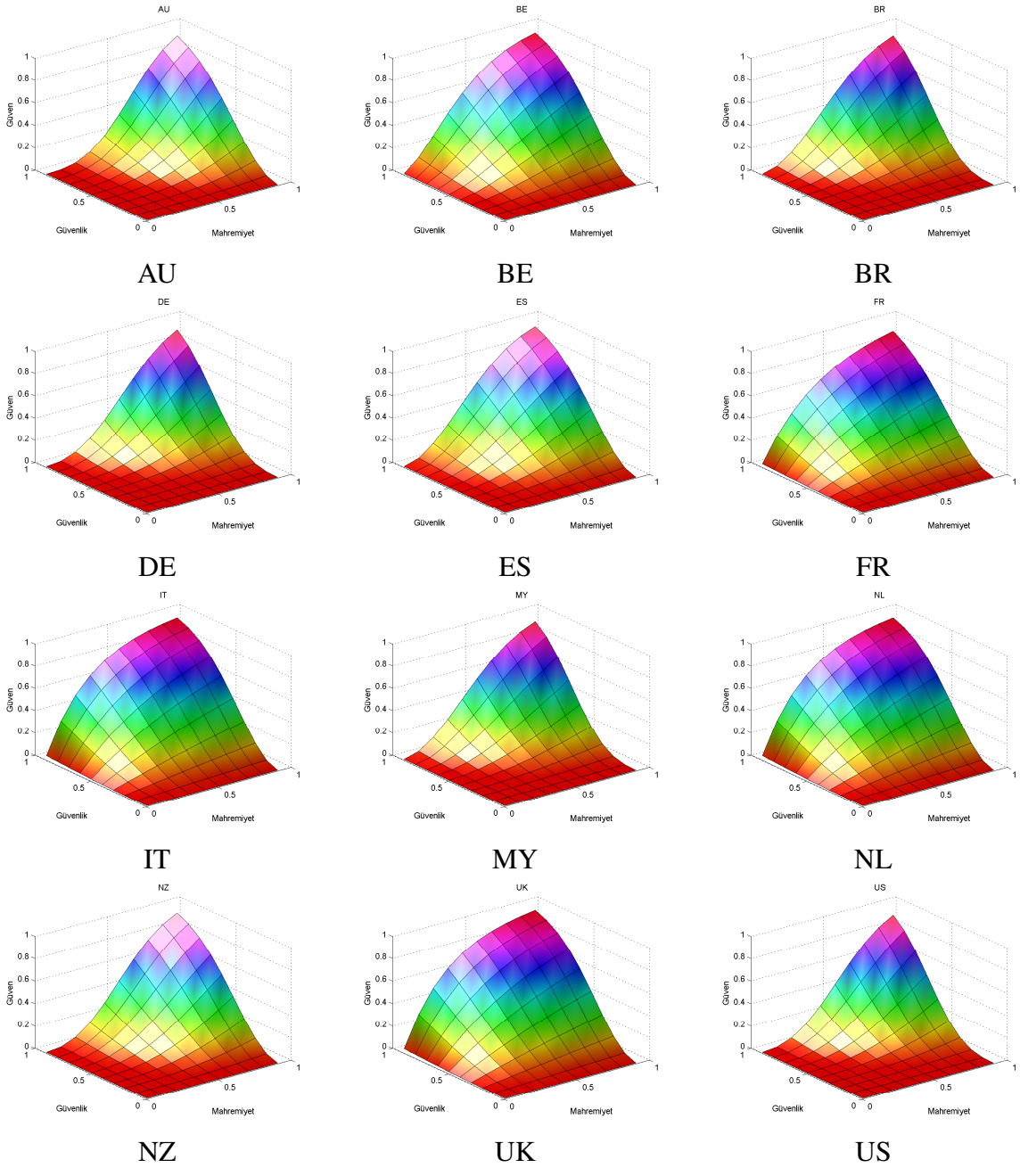
meye başlamaktadır. Belçika, Almanya, Fransa, İtalya ve Malezya'da elde edilebilecek azami güven değeri 0.7 civarındadır. İlginç biçimde Almanya ve Belçika'da ise en ufak bir güven düzlüğüne bile rastlanmamıştır. Bu durum, Alman ve Belçika halkalarının hem güvenlik hem de mahremiyet konusunda ciddi şüphelerinin olduğu anlamına gelir. Bununla birlikte, Avustralya, Brezilya, İspanya, Malezya ve İngiltere'de mahremiyet güveni daha çok etkileyen bir faktör olarak görülmüştür.

Çizelge 4.9 Finans uygulamalarında yüz biyometriğine dayalı güven dağılımları.



Parmak izine dayalı BKYS'lerin Internet güvenliğine etkisi araştırıldığında gene ilginç sonuçlar ortaya çıkar. Güven için elde edilebilecek azami değerler 0.9 civarındadır. Özellikle İtalya, Hollanda ve İngiltere'de güven yüzeyleri geniş sayılabilir. Çizelge 4.10'da görülebileceği gibi, beş ülkede (Belçika, Fransa, İtalya, Hollanda ve İngiltere) mahremiyetin güvenliğe nazaran daha çok dikkate alındığı söylenebilir.

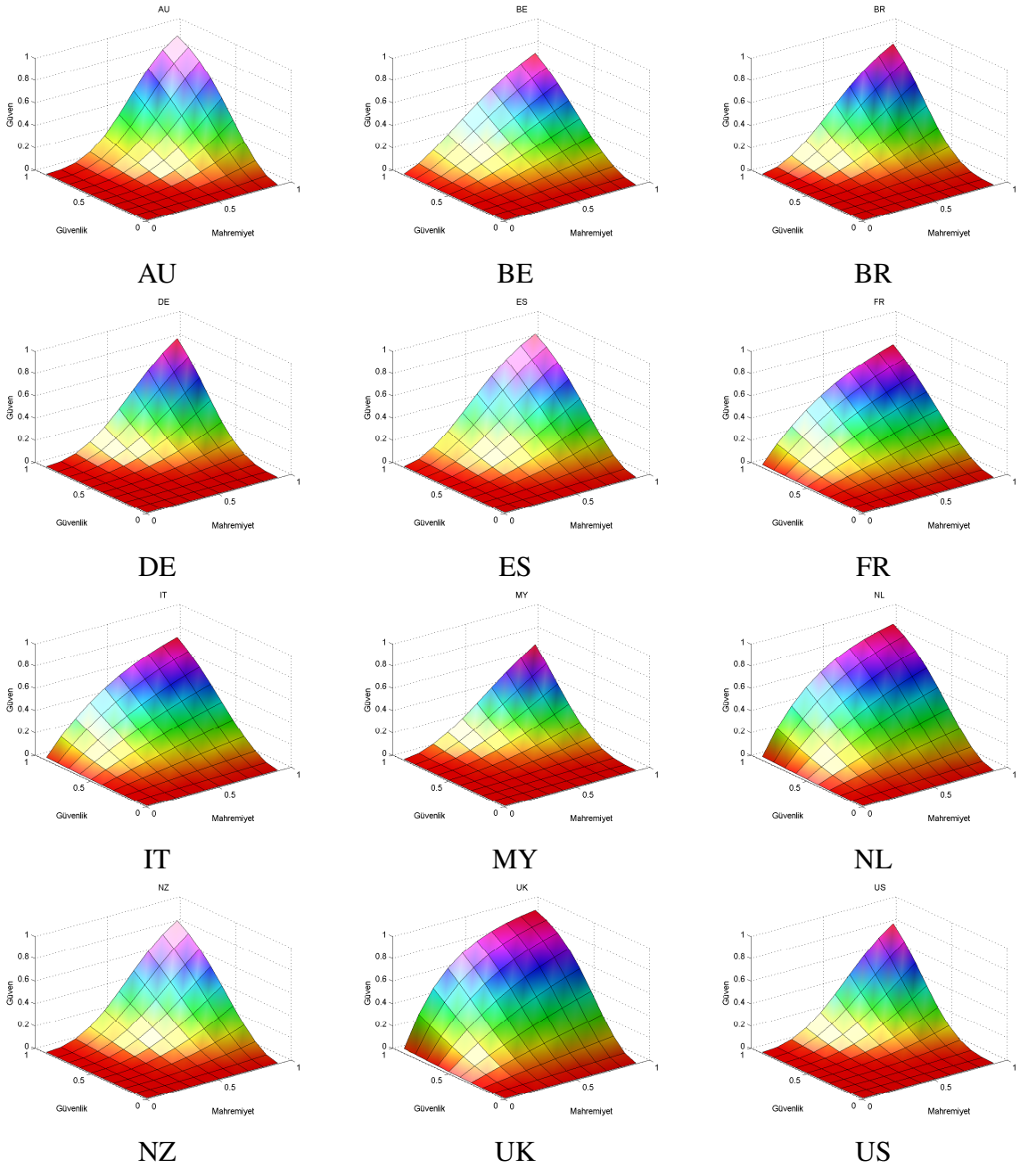
Çizelge 4.10 Internet uygulamalarında parmak izi güven dağılımları.



Yüz biyometriğinin Internet uygulamalarında kullanımına ilişkin analizlerde

ise güven değerleri parmak izine göre bir miktar düşmektedir (Bkz. Çizelge 4.11). Ancak bu düşüş, finans ve ulusal güvenlik uygulamalarındaki gibi dramatik değildir. Burada en dikkat çekici sonuç Malezya'da görülmektedir. Malezya'da hem mahremiyet hem de güvenlik çekinceleri çok yüksektir ve güven için elde edilen azami değer yaklaşık 0.6 civarındadır. Benzer bir durum Belçika'da da görülmektedir.

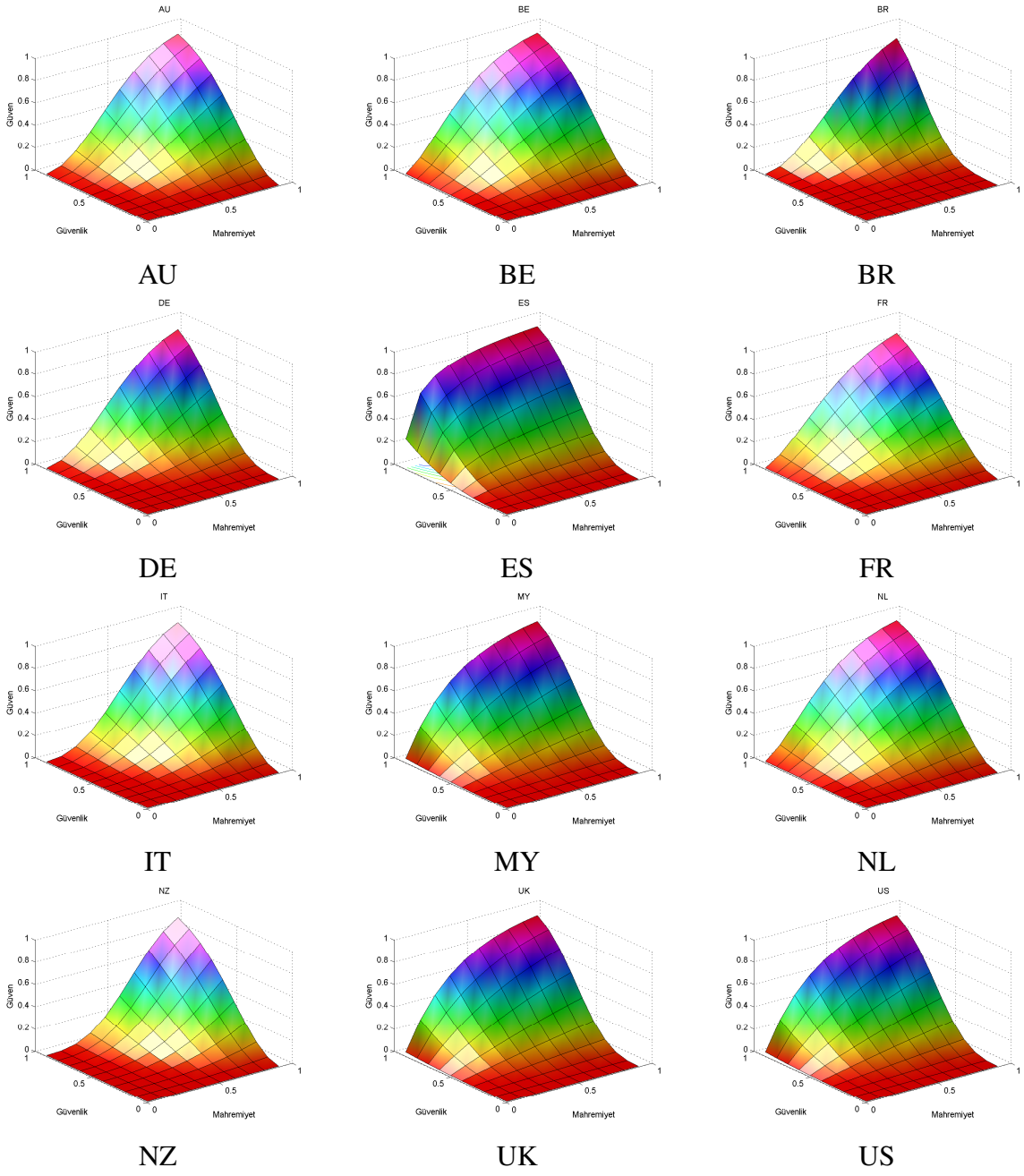
Çizelge 4.11 Internet uygulamalarında yüz biyometriği güven dağılımları.



Kişisel güvenlik alanındaki analizlere bakıldığında, parmak izinin BKYS'lerde

kullanıldığı durum ele alınacak olursa, güven değerlerinin gene yüksek seyrettiği anlaşılmaktadır. Çizelge 4.12'te görülebilecek çarpıcı sonuçlardan biri, özellikle İspanya, Malezya, İngiltere ve ABD'de güvenliğe nazaran mahremiyet çok daha baskın biçimde öne çıkmaktadır.

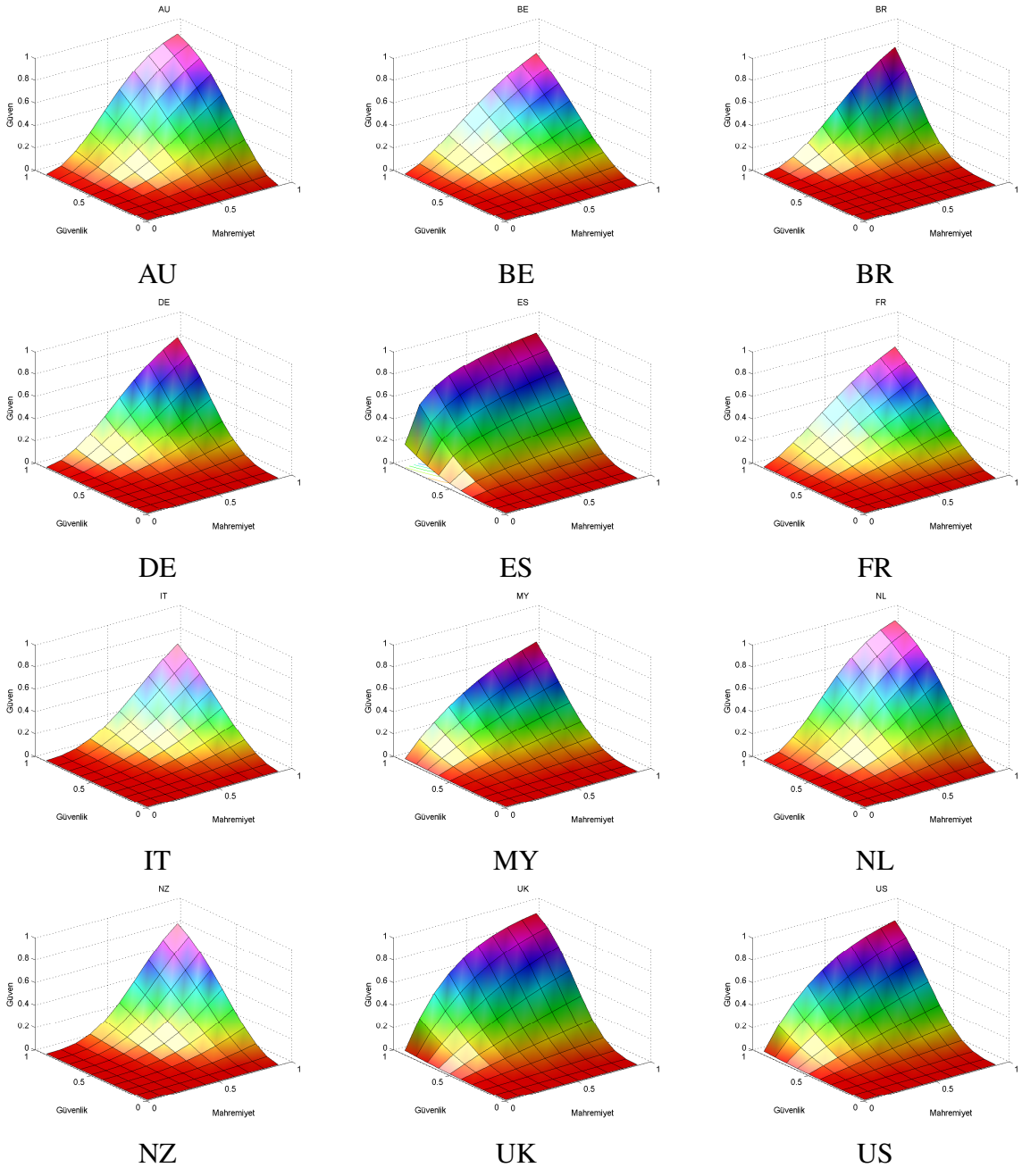
Çizelge 4.12 Kişisel Güvenlikte parmak izine dayalı güven dağılımları.



Çizelge 4.13'te gösterilen güven dağılımlarında ise gene beklenildiği gibi parmak izine göre yüz daha az güvenilir bir biyometrik kip olarak karşımıza çıkar. An-

cak burada çok ciddi bir düşüş gözlenmemiştir. Burada özellikle İtalya ve Malezya'da ciddi bir güvensizlik göze çarpmaktadır. Buna ek olarak, hermen hemen tüm alanlarda göze çarpan mahremiyete daha çok önem verilmesi konusu burada da görülmektedir. Özellikle İspanya, İngiltere ve ABD, önceki alanlardaki uygulamalara benzer biçimde mahremiyete çok daha fazla önem veren ülkeler olarak gözükmektedir.

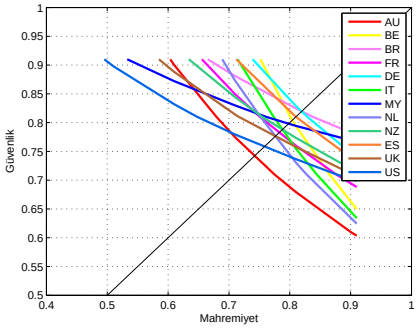
Çizelge 4.13 Kişisel Güvenlikte yüz biyometriğine dayalı güven dağılımları.



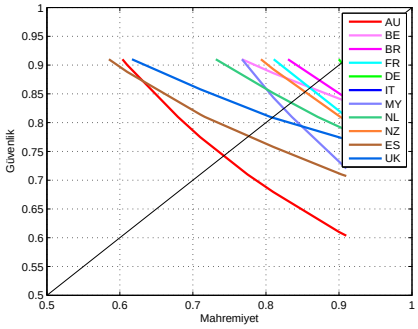
BioPSTM'in, iki farklı biyometrik kip ve dört farklı alana uygulandığı durum-

larda elde edilen ödünleşim eğrileri ise Şekil 4.14'te görülebilir. Bu ödünleşim eğrileri, halkın biyometrik teknolojileri BKYS'ler özelinde kullanması durumunda, mahremiyet ve güvenlik'ten ne kadar ödün verileceğini ifade etmektedir. Şüphesiz bu çalışmadaki sonuçlar ülkelerdeki algıyı yansıtır. Devletlerin aldığı güvenlik ve mahremiyeti ilgilendiren kararlar, kanunlar ve yürütmelikler o ülkenin mahremiyet ve güvenlik karnesini belirleyen diğer unsurlar olarak ele alınmalıdır.

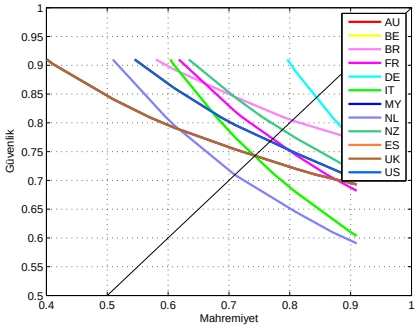
Çizelge 4.14 $T = 0.7$ kesitinde ödünleşim eğrileri.



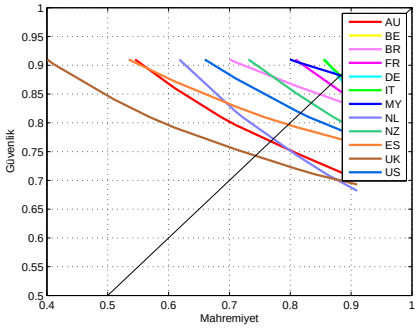
Ulusal güvenlik uygulamalarında parmak izi kullanımı



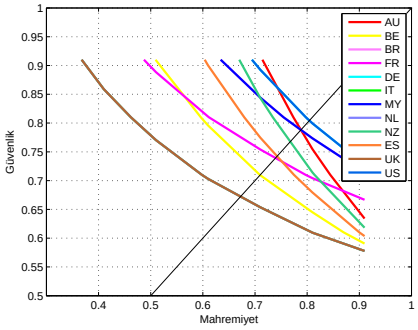
Ulusal güvenlik uygulamalarında yüz biyometriği kullanımı



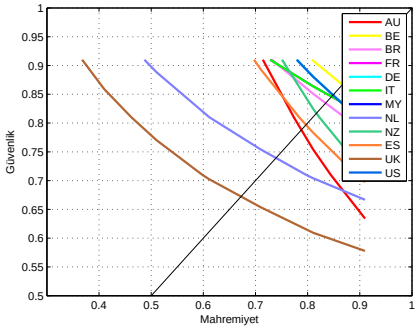
Finansal güvenlik uygulamalarında parmak izi kullanımı



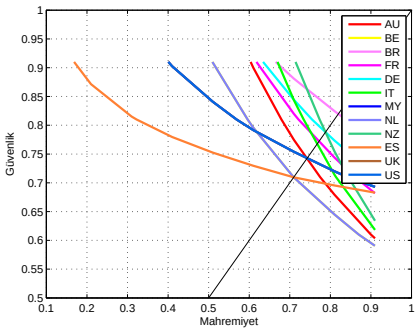
Finansal güvenlik uygulamalarında yüz biyometriği kullanımı



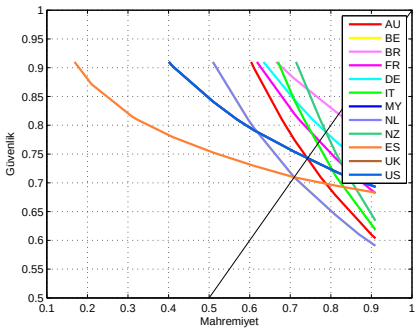
Internet güvenliği uygulamalarında parmak izi kullanımı



Internet güvenliği uygulamalarında yüz biyometriği kullanımı



Kişisel güvenlik uygulamalarında parmak izi kullanımı



Kişisel güvenlik uygulamalarında yüz biyometriği kullanımı

4.3 Yorum ve Karşılaştırma

TAM'ın biyometrikler üzerine uygulanması anlamında derinleşen çalışmalar yeni yeni literatüre girmektedir. Bunlar arasında en dikkat çekenler biyometriklerin empirik analizine yoğunlaşan ve TAM ile bağdaştıran, biyometriklerin ne derecede benimsendiği konusuna odaklı çalışmalardır. Ho ve arkadaşları [75] ile Chau ve arkadaşlarının [76] çalışmaları biyometrik teknolojilerin benimsenmesine etki eden faktörleri ve bunlara ilişkin hipotezleri küçük veya orta ölçekli denek kümelerinde denemişlerdir. Giesing'in yüksek lisans tezinde [77] yaptığı çalışma ise elektronik iş/ticaret uygulamalarına odaklı bir yaklaşım sunar. James ve arkadaşlarının [78] kapsamlı çalışması ise biyometrik sensörlerin teknoloji kabul modelinin çıkarılmasına odaklanır ve elde edilen sonuçlar biyometrik sensörlerin tasarımlarının ciddi biçimde ele alınması gerekliliğini ortaya koyar. Jones ve arkadaşları [79] ise yetkilendirmeye dayalı tüm teknolojilere genel bir bakışla konuyu ele alır ve bilgi güvenliği sistemlerindeki yetkilendirme bileşenlerinin teknoloji kabul modelindeki yerini inceler. Kim ve arkadaşları [80] ile Murphy ve Rottet'in çalışmaları [81] ise turizm sektöründe önemli bir problem olan turistlerin güvenliğini sağlama konusunda otellerdeki biyometrik erişim çözümlerinin ne derecede kabul edilebileceğini ortaya koyan deneysel incelemeleri yansıtır. Öte yandan, Tassabehji ve arkadaşları [82] da oldukça popüler olan ve riski yüksek bir alanda, e-Bankacılıkta, kullanıcı tutumlarını ve güvenilirliği sorgulayan bir model önerir. F.Al-Harby ve arkadaşları da biyometrik sistemlerdeki çevrimiçi (online) işlemlerde cinsiyet farklılıklarının teknoloji kabul modeline etkisini inceleyen ilginç bir çalışma yapmışlardır [83]. Daha sonra aynı ekip bu çalışmayı genişleterek biyometrik unsurları da içeren eTicaret uygulamalarının modellenmesi üzerine eğilmişlerdir [84]. Gene paralel bir konuda da Michael ve arkadaşları [85] finansal işlemlerde biyometrik teknolojilerin kabul edilirliğine dair hipotezler önermişler ve saptamalarda bulunmuşlardır.

Yukarıda anılan çalışmalarda, Michael ve arkadaşlarının kavramsal analizi [85] haricinde, TAM'ın çeşitli uygulamaları ele alınmış ve genelde onlarla veya yüzlerle ifade edilen denek kümelerinde yapılan anket sonuçlarında anlamlılık analizi yapılmış ya da gözlemsel sonuçlar analitik olmasa bile paylaşılmıştır. TAM haricinde de bazı teknoloji kabul modellerinin biyometrik teknolojilere uyarlandığı bilinmektedir. Örne-

ğin, biyometrik güvenlik teknolojileri konusunda hatırı sayılır bir topluluk olan BioSec Konsorsiyumunun 2005 yılında yayınladığı anket [86] biyometrik teknolojilerle ilgili kullanışlılık, kullanım kolaylığı, istek, güven, mahremiyet ve güvenlik gerekleri gibi konularda anahtar sorular önermişlerdir. BioSecure Konsorsiyumu'nun çalışması, kısa adı DART (Dynamic Acceptance Model for Re-evaluation of Technology-based Application) olan bir model kullanmıştır. Amberg ve arkadaşları tarafından önerilen bu modelde [87], TAM'daki algılanan kullanışlılık ve kullanım kolaylığına ek olarak algılanan maliyet (parasal veya parasal olmayan) ile algılanan işbirliği ağı etkisi (perceived network effect: populerlik, yenilikçi ürünlere erişim, mevcut teknolojik altyapılarla sinerji) faktörleri de hesaba katılmıştır. TAM'ın yanında biyometrik teknolojilerin kabul edilebilirliğini modellemede Venkatesh ve arkadaşlarının önerdiği UTAUT (Unified Theory of Acceptance and Use of Technology- Birleştirilmiş Kabul ve Teknoloji Kullanımı Teorisi) yöntemi de tercih edilmiştir [88]. Al-Harby ve arkadaşlarının uygulamalarında parmak izinin eTicarette kullanımı ve genel biyometrik güvenlik sistemlerindeki kabul modelleri incelenmiştir [89; 90]. UTAUT'ta TAM'daki davranışsal niyet ve gerçek kullanım faktörlerini başarım beklentisi, efor beklentisi, sosyal etkiler ve kolaylaştırıcı şartlar ile cinsiyet, yaş, deneyim ve gönüllülük gibi kişisel özellikler etkilemektedir.

Teknoloji kabul modelleri, biyometrik teknolojilerin bir şekilde kullanıma geçtiği ülkelerde halkın nabzını tutmak adına tercih edilen yöntemlerdir. Örneğin, Alhussein bir çalışmasında maliyet, mahremiyet, güvenlik, verimlilik ve uyumluluk gibi faktörleri işin içine katan özgün bir kabul modeli önermiştir [91]. Uzoka ve Ndzinge de, Botswana'daki biyometrik teknolojilerin kabul modelini TAM'dan esinlenerek ortaya koymuştur [92]. Breward ve Hassanein'in Kanada'da yaptığı bir çalışmada ise kullanışlılık ve tutum ile beraber güven, güvenme öneğilimi, mahremiyet ve güvenlik sakıncaları ile PIIT (Personal Innovativeness in the domain of Information Technology) denilen bilgi teknolojilerindeki kişisel yenilikçilik faktörleri bir arada açıklanmıştır [93]. Elgarah ve Falaleeva'nın Amerika Birleşik Devletleri'ndeki hastanelerde biyometrik teknolojilerinin kullanımı ile ilgili yaptıkları geniş çaplı bir başka çalışmada ise TAM üzerine, mahremiyet çekinceleri ile ilgili bir faktör eklenmiştir [94]. Bunlara ek olarak, Yeow ve arkadaşlarının 2005 ve 2007 yılındaki çalışmaları [95; 96] ile Loo ve arkadaşlarının 2009 yılında yayınladıkları sonuçlar [97] Malezya'daki

eKimlik uygulamalarındaki kabul modelinin UTAUT ile gösterimine odaklanmıştır.

Şüphesiz, ülkelerde genel anlamda bilgi iletişim teknolojileri üzerine kabul modelleri çıkarılsa da biyometik teknolojiler özelindeki çalışmalar hala emekleme seviyesindedir. İster TAM ile ister UTAUT ile ya da başka bir kabul modeliyle olsun, biyometrik teknoloji kabul modellerinde çoğunlukla öznel değerlendirmelerin nesnel analizine dayalı yaklaşımlar ele alınmıştır. TAM en çok tercih edilen yöntemlerden biri olarak göze çarparken, UTAUT yöntemindeki başarım, efor, sosyal etki gibi kavramları tam anlamıyla kapsamaz. O nedenle genişletilmiş-TAM uygulamaları (örneğin Venkatesh ve arkadaşlarının önerdiği TAM3 gibi) düşünülmüştür. Tez kapsamında gösterilen uygulamalarda da görüleceği gibi TAM'ın mevcut haliyle sunulması mahremiyet ve güvenlik tehditlerini modellemede yetersiz kalabilir. Zira TAM, tehdit unsurları gerçekleştiği anda ancak fark edilebilecek mahremiyet ve güvenlik risklerini öngörmekte yetersizdir. TAM algılanan kullanım kolaylığı ve kullanışlılık gibi önceden tahmin edilebilecek faktörleri başarıyla hesaba katabilir. Ancak çok nadiren bile olsa bir mahremiyet sızıntısı veya güvenlik açığının doğuracağı zararın halk üzerinde ne etki bırakacağını açıklamak oldukça zordur. Oysa ki bu tez çalışmasında önerilen BioTAM, TAM'a çok farklı biçimde yaklaşarak çeşitli çalışmalarda bir şekilde anket sorularıyla araştırılmaya çalışan güven faktörünü mahremiyet-güvenlik ödünleşimi üzerine inşa ederek bir güven öngörüsü yapmayı sağlar. Bunu sağlarken de TAM'da çoğunlukla kullanılan anket yöntemi yerine, hesaplanabilir ve ölçülebilir normalize sızıntı oranlarını kullanır. Bu yönüyle BioTAM, özgün BioPSTM modelini etkin biçimde kullanarak, güven faktörünün analizine farklı bir bakış açısı getirir.

BioPSTM ve bunun üzerine inşa edilen BioTAM'ın literatürdeki biyometrik kabul modellerinden en temel farklarından biri her şeyden önce hem biyo-kıyım hem de sendrom kodlamaya dayalı biyometrik saklama tekniklerini bir arada kullanan bir BKYS üzerine kurulu olmasıdır. Ne Ho ve arkadaşları ile Chau ve arkadaşlarının ne de Giesing'in ya da Jones ve arkadaşlarının çalışmalarında yeni nesil biyometrik kriptosistem türevi yaklaşımlar ele alınmaz. Bunun yerine standart doğrulamaya dayalı ve kişisel bilgilerin rutin kriptografik yöntemlerle şifrelendiği BKYS'ler ele alınır. Bu tez çalışmasında yapılan çalışmalarda BioPSTM'in normalize sızıntı oranları cinsinden açıkladığı mahremiyet ve güvenlik riskleri yeni nesil BKYS'lerdeki anahtar üreteci, sendrom kodlama ve biyo-kıyım gibi gelişmiş yaklaşımları ele alarak daha kapsamlı

bir analiz imkanı sunar. **P** ve **S** değerlerinin ölçüldüğü Ignatenko ve arkadaşlarının çalışmasında (Şekil 4.4) gizli anahtar oranı ve mahremiyet sızıntı oranları aslında bu çalışmadaki mahremiyet ve güvenlik ölçümleri için güzel bir örnek teşkil eder. Burada, orijinal biyometrik işaret ile biyo-kıyım ve sendrom kodlama benzeri bir yaklaşımla üretilen biyometrik anahtar arasındaki çapraz geçiş olasılığı bir parametre olarak kullanılmıştır. Bu çapraz geçiş aslında biyometrik bilgi ile biyometrik bilginin korunmuş hali arasındaki bilgi sızıntısını da ifade eder. Bu sızıntı oranı, ya da çapraz geçiş olasılığı arttıkça gizli anahtar oranı düşer ki bu da güvenlik sorunlarına davetiye çıkarır. BioPSTM işte tüm bu ilişkileri matematiksel olarak ifade edebilen bir ölçüt sunar. Mevcut teknoloji kabul modelleri, bu matematiksel ölçütler yerine daha çok anketlere ya da kullanım istatistiklerine dayalı gözlemsel bilgiler kullanmayı tercih eder. BioPSTM gelişmiş bir BKYS üzerine kurulu belki de ilk mahremiyet-güvenlik-güven modelini sunması bakımından literatüre bir yenilik katmaktadır.

BioPSTM'in kattığı bir diğer yenilik ise BioPSTM'in BKYS'yi modüler bir sistem olarak ele alıp, gerektiğinde risk oluşturmayan veya bir şekilde tercih edilmeyen (örneğin, maliyet ve zaman kısıtları yönünden) modülleri çıkarılabilir veya eklenebilir kılmasıdır. Örneğin, biyo-kıyım yönteminin yeterli olduğu ancak sendrom kodlamaya ihtiyaç duyulmayan bir uygulamada, sendrom kodlama ile ilgili normalize sızıntı oranı terimleri ($\Psi_{\kappa S}$, $\Psi_{S\Theta}$, Ψ_{XS}) çıkarılabilir. Ya da çok daha ileri seviyede güvenlik isteyen bir uygulamada biyo-kıyım ve sendrom kodlamaya ek olarak başka bir bulanık özütleyici daha BKYS'ye eklenecek olursa, buna ilişkin yeni terimler BioPSTM'e çarpanlar halinde eklenebilir. BioPSTM'in bu esnekliğinden faydalanan BioTAM, bu yönüyle yukarıda sıralanan kabul modellerine göre daha gelişmiş bir yapı sunar.

BioTAM özelinde yapılan çalışmalarda, örneğin İngiltere'deki BioTAM örnek uygulamasında, güven için yeni bir etmen tanımlanmıştır. Literatürdeki çalışmalarda, örneğin Giesing'in çalışmasında [77] genelde güven sosyal etmenlerden biri olarak ele alınmaktadır. Giesing, Breward ve arkadaşları [93] ile James ve arkadaşlarının [78] çalışmalarında görüldüğü gibi güven, güvenlik ve mahremiyet ile aynı düzeyde psikolojik ve sosyolojik kökenli bir etmen olarak görülmüştür. Malezya'daki kimlik kartı uygulamasının kabul modelinde [95; 96; 97] de aynı yaklaşım geçerlidir. Güven adı altında tek bir etmen belirlenmese de güvenlik ve mahremiyet yukarıda adı geçen tüm çalışmalarda çok da öznel olmayacak biçimde ele alınmış ve çoğun-

lukla herhangi bir matematiksel öngörü olmaksızın incelenmiştir. Biyometrik sistemlerde değil ama genel anlamda bilgi sistemlerinde insanların sisteme sunduğu güveni ölçmek için yeni etmenler tanımlanmış ve hatta bazen kültürel etmenler bile dikkate alınabilmiştir. Bu tezde yer alan, İngiltere için yapılan BioTAM uygulamasında ve BioPSTM'in ülkelere uygulandığı örnek çalışmalarda ise mevcut teknoloji kabul modellerinde alışık olunmayan bir yaklaşım ortaya konmuştur. Öyle ki bu yaklaşımda ancak riskler veya tehditler gerçekleştiği anda görülebilecek güvenlik sorunları ve mahremiyet sıkıntıları BioPSTM ile öngörülmeye çalışılmış ve hem mahremiyet hem de güvenlik için nicel olarak bir kestirimde bulunulabilmiştir. Örneğin, İngiltere için BioTAM uygulamasında daha önce yapılan bazı kamuoyu yoklamalarında elde edilen veriler algılanan kullanım kolaylığı ve kullanışlılık, davranışsal niyet ve gerçek kullanım gibi TAM'ın temel bileşenlerinin ifade edilmesinde kullanılmıştır. Hem parmak izi hem de yüz biyometriği için kamusal isteklilik ya da biyometrikleri kullanmada kişilerin kendini emin hissetmesi gibi parametreler yardımıyla, İgnatenko ve arkadaşlarının teorik çalışmalarındaki bulgular birleştirilmiş ve tek bir güven değeri bulunabilmiştir. BioPSTM'in ülkelere uygulandığı çalışmada ise güven dağılımları hesaplanmış mahremiyet ve güvenlik etmenlerinin ağırlıklandırılabildiği yaklaşımlar öne sürülmüştür. Tüm bu analizler göstermiştir ki, BioPSTM üzerine kurulu BioTAM sayesinde biyometrik teknolojilerin ülkelere ve kullanım alanlarına göre kullanım karakteristikleri ölçülebilmekte, güvenlik ve mahremiyet sıkıntıları olma durumunda halkın bu teknolojiyi hangi düzeyde kabul edebileceği öngörülebilmektedir.

BioTAM'ın ve BioPSTM'in değerlendirildiği örnek çalışmalarda da görülebileceği gibi biyometrik teknolojiler artan güvenlik tehditleri ve gelişen teknolojiler nedeniyle daha kolay kabul edilebilmektedir. Bunun yanında mahremiyet çekinceleri de artan bilinçle öne çıkabilmektedir. Ülkeler bazında da mahremiyet-güvenlik ödünleşiminin etkilediği güven faktörü önem kazanmaktadır. Örneğin, İspanya, İngiltere ve Malezya'da güvenlik odaklı BKYS'ler öne çıkarken, Almanya özellikle ulusal güvenlik ve finansal güvenlik uygulamalarında mahremiyet odaklı çözümleri daha kolay kabul etme eğilimindedir. Internet'in güvenli olduğuna en çok inanan ülkeler ise Brezilya, Almanya ve Amerika Birleşik Devletleri olarak görülürken, mahremiyet-güvenlik ödünleşiminin güven üzerinde olumsuz yönde en çok etki ettiği ülke ise Brezilya olmuştur. Demek ki, sadece güvenliğe ya da sadece mahremiyete odaklanan

teknoloji kabul modelleri güven etmenini incelemede yanılgıya düşebilirler. Brezilya'da Internet güvenliği konusunda pozitif bir eğilim varken mahremiyet sakıncaları nedeniyle biyometrik web teknolojilerine güven düşük çıkabilmektedir. BioTAM'ı her şeyden önce BioPSTM ile sunduğu bu bütüncül yaklaşım farklı kılar. Öyle ki hem mahremiyet hem de güvenlik gereklerinin analiz edilmesinde ve buradan tek ve ölçülebilir bir güven değerinin çıkarılmasında, daha sonra bu etmenin TAM'ın klasikleşen etmenleri ile bütünleştirilmesinde, BioTAM ilginç ve yenilikçi bir model olarak değerlendirilebilir.

5 Sonuçlar ve Çıkarımlar, Gelecek Çalışmalar

5.1 Sonuçlar ve Çıkarımlar

Kimlik yönetiminden gözetim sistemlerine, Internet bankacılığından sosyal medyaya kadar birçok farklı alanda kullanımı git gide artan biyometrik güvenlik sistemleri farklı koşullar için farklı çözümler üreten alternatif güvenlik sistemleri olarak dikkat çekmektedir. Biyometrik güvenlik sistemlerinin ilk çıkış amacı olan veri güvenliğini ve erişim kontrolüne dayalı üst güvenlik düzeyi sağlamanın yanında, mahrem bilgi olarak kabul edilen biyometrik bilgilerin gizliliğini sağlamak da önem kazanmıştır. Literatürde bu konuda teorik çalışmalar mevcut olsa da bu ödünleşimin güven ile ilişkisinin kurulmadığı görülmüştür. Oysaki bu teknolojilerin geniş ölçekte kabul edilebilmesi için kullanıcıların biyometrik çözümlere güven duyması beklenir. Başka bir deyişle, nasıl güvenlik ile mahremiyet arasında bir ödünleşim varsa, güvenle de hem mahremiyet hem de güvenlik arasında paralel bir bağlantı vardır. İnsanların biyometrik sistemlere güvenmesi için hem mahremiyet hem de güvenlik çekincelerinin (ikisinin birden) asgari düzeyde olması gerekir. Bu çalışmanın ilk odak noktası biyometrik kimlik yönetimi sistemlerindeki güvenlik ve mahremiyet arasındaki ödünleşimin güven ile ilişkisini betimleyen matematiksel bir model (BioPSTM) sunmaktır. Bu matematiksel model sayesinde karar vericiler, bir BKYS'nin güven dağılımını gözleyebilecek ve uygulamanın isterlerine göre hangi mahremiyet ve güven seviyesinde kullanıcıların sisteme ne kadar güvendiğini nesnel olarak ölçme imkanı bulabileceklerdir. Bu nesnel ölçüm sayesinde karar vericiler, bir BKYS'nin başarımını sadece tanıma oranları ve bilgi sızıntı oranları cinsinden değil, bir güven parametresi biçiminde de inceleyerek en doğru kararı vermiş olacaklardır.

Bu tez çalışmasında, güvenlik ve mahremiyet arasındaki bu ödünleşim gelişmiş sayılabilecek bir BKYS'de normalize sızıntı oranları ve ortalama entropiler cinsinden ifade edilmiştir. Burada ele alınan BKYS'de, bir biyometrik sistemdeki temel (öznitelik çıkarma gibi) modüllerin yanında sentetik anahtarlarla güçlendirilmiş bir kıyım mekanizması ile gizliliği ve geri çatma başarımını arttıracak bir sendrom kodlama modülü de dikkate alınmıştır. Kuşkusuz bu yaklaşım genel geçer değildir zira uygulamaya göre bu modüllerden bazıları devre dışı bırakılabilir. Bu durumda, çıkarılan modüllerle

ilgili terimler de devre dışı kalarak ödünleşim hesaplanabilir.

Bu doktora tezinin ikinci önemli odağı ise BioPSTM'i daha geniş bir perspektifle bir teknoloji kabul modelinin içine yerleştirmektir. Güven, bir teknolojinin kabul edilmesinde her ne kadar önemli bir rol oynasa da tek önemli etmen değildir. Kimi zaman çok basit uygulamalar bile insanların bu teknolojiyi daha kolay kabullenmelerini sağlayabilir ve bu yöndeki algıyı olumlu yönde etkileyebilir. O nedenle teknolojinin kabulunde algılanan kullanışlılık ve kullanım kolaylığı insanların tutumlarını, tutumlar da teknolojiyi kullanma yönündeki davranışsal niyeti etkiler. Tüm bu öznel faktörler sistemin gerçek kullanımını arttırabilir veya azaltabilir. İşte bu tez çalışmasındaki ikinci önemli odak noktası BioPSTM'in güveni betimlediği modelden faydalanarak önerilen BioTAM teknoloji kabul modelidir. BioTAM sayesinde bulmacanın eksik yönleri tamamlanmış ve biyometrik teknolojilerin gördüğü kabulü nesnel olarak gösteren bir model önerilmiş olur. BioTAM'da öne çıkan her durum ve durumlar arasındaki ilişkileri betimleyen hipotezler nesnel yöntemlerle (güvenlik testleri, anketler, kullanım istatistikleri, vs.) ölçüldüğü takdirde bir biyometrik kimlik yönetimi sisteminin ne oranda kabul göreceği anlaşılmış olur.

Tez çalışmasında bu iki önemli odak noktasının kullanımına ilişkin iki uygulama yapılmıştır. Bu senaryolardan ilkinde 12 farklı ülkedeki ulusal, finansal, kişisel güvenlik ve Internet güvenliği gibi konularda biyometrik güvenlik sistemlerinin kullanımının BioPSTM ile modellenmesi ele alınmıştır. Dünyaca kabul gören güvenlik ve mahremiyet araştırmaları yapan Unisys ve privacyinternational.org kuruluşlarının raporlarından faydalanılan analizlerde, parmak izi veya yüz biyometriğinin kullanıldığı durumlardaki güven dağılımları çıkarılmıştır. Güven dağılımlarında istenilen güven değerinde bir kesit alındığında mahremiyet ve güvenlik ödünleşim eğrileri de görülmüş olur. Deney sonuçları göstermiştir ki, ülkeler genelde BKYS'lere güven duymaktadır. Ülkeler arasında coğrafi, kültürel veya ekonomik farklılıklara dayalı ciddi bir kümelenme veya sınıflandırma görülmemiştir. Örneğin, mahremiyetin çok sıkı tartışıldığı ve bu konuda yasal düzenlemelerin nispeten ağır olduğu Avrupa ülkelerinde bile güvenlik önlemlerinin ağırlığı mahremiyete oranla daha yüksek çıkmıştır. İspanya ve İngiltere buna iyi birer örnektir. Brezilya ve Amerika Birleşik Devletleri gibi kanun dışı sınır geçişlerinden mustarip olan suç oranının yüksek olduğu ülkelerde de güvenlik mahremiyete oranla daha çok önemsenen bir etmen olarak göze çarpmaktadır. Burada,

11 Eylül saldırılarının da yarattığı bir algı olabilir ve bunun araştırılması gerekebilir. Hollanda, Fransa ve Almanya gibi merkez Avrupa ülkelerinde ise genelde BKYS'lere güven yüksek değerlerde seyretmektedir. Malezya gibi biyometrik teknolojileri çok uzun yıllardır geniş ölçekte kullanan ülkelerde ise güven değerleri genelde yüksek seyretse de güvenlik mahremiyete göre daha öncelikli bir ihtiyaç olarak kabul edilmiştir. Demografik ve kültürel yapısı ile ekonomik koşulları göz önüne alındığında belki de Türkiye'ye en yakın ülkelerden biri kabul edilebilecek Malezya'nın daha derinlemesine incelenmesinde fayda olabilir. Biyometrik kiplerin seçimi açısından sonuçlar değerlendirildiğinde parmak izinin yüz biyometriğine oranla daha çok kabul gördüğü söylenebilir. Tez çalışmasında, BioPSTM'in 12 ülkede işletilmesine dayanan örnek uygulamada kullanılan kriterler ve ölçüm değerleri iki farklı kaynaktan alınan (Unisys ve privacyinternational.org) verilerin kolajına dayandığı için yanıltıcı olabilir. Bunun için daha geniş çapta ve kapsayıcı bir çalışma yapılarak tek bir denek kümesinde modelleme yapılmalıdır. Buradaki amaç, sadece BioPSTM'in nasıl kullanılabileceğine dair araştırmacılara bir fikir vermektir.

Tez çalışmasındaki ikinci önemli senaryo ise İngiltere'deki kimlik kartı uygulamalarının teknoloji kabul modelinin BioTAM'a uyarlanarak sunulmasıdır. Bu örnek senaryoda yüz ve parmak izi biyometrik kiplerinin ulusal kimlik kartları için uygulanması durumu BioTAM çerçevesinde modellenmiştir. Bu örnek senaryoda, biyometrik teknolojilerin İngiltere'de kullanımı ile ilgili bazı araştırma sonuçlarından ve Unisys Güvenlik Endeksi analizlerinden yararlanılmıştır. Bu araştırmalar ile Ignatenko ve arkadaşlarının 2009 yılında yayınladıkları teorik bulgular sayesinde BioPSTM parametreleri için de uygun değerler seçilmiştir. Bunlara ek olarak, dışsal faktörlerin etkilediği, algılanan kullanışlılık ve kullanım kolaylığı, davranışsal niyet ve gerçek kullanım faktörleri ve bunlar arasındaki ilişki, Davis ve arkadaşlarının önerdiği ve tüm bilişim sistemleri için yaptıkları analizleri yansıtan teknoloji kabul modeli üzerinden açıklanmıştır. Sonuçta ortaya çıkan örnek uygulama farklı araştırmaların bulgularını BioTAM potasında eriterek biyometrik teknolojilerin kabul edilebilirliğini ölçebilecek nesnel bir değerlendirme modeli ortaya koymuştur. Buna göre BioTAM'ı oluşturan her bileşen ve bunlar arasındaki ilişkilerde kullanılan Cronbach değerleri ya da benzer istatistikler teknoloji ile ilgili genel bir fikir verebilir. Örneğin, tüm bu değerler 1'e yaklaştıkça çok daha kolay kabul gören bir BKYS'den bahsedilebilir. BioTAM sayesinde karar veri-

ciler bir BKYS'yi sahaya kurmadan ya da yatırımcılar BKYS için kaynak ayırmadan önce bu sistemin ne düzeyde işe yarayacağını ve kabul edilebileceği kestirmiş olurlar. Veya bileşenler arasındaki ilişkilere bakarak nesnel biçimde hangi bileşenin ne tür eksiklikleri olduğunu öngörüp çözüm yolları oluşturabilirler.

İngiltere'deki uygulamada da parmak izinin yüz biyometriğine göre daha kolay kabul edilebileceği görülmüştür. Paralel olarak, parmak izinin hem güven değeri hem de kullanım kolaylığı ve dolayısıyla da gerçek kullanım değerleri yüz biyometriğine göre daha yüksek çıkmıştır. Algılanan kullanım kolaylığı algılanan kullanışlılığı, algılanan kullanışlılık ise davranışsal niyeti aşağı yukarı aynı düzeyde etkilemiştir. Algılanan kullanım kolaylığının davranışsal tutum üzerindeki etkisi ise diğer faktörlerin etkisine nazaran çok daha düşük düzeyde seyretmiştir. Beklendiği gibi davranışsal niyet, gerçek kullanımı çok yüksek düzeyde etkilemektedir. Seçilen örnekte çok düşük mahremiyet ve güvenlik değerleri seçildiği için güvenin algılanan kullanım kolaylığı üzerindeki etkisi de sınırlı kalmıştır.

5.2 Gelecek Çalışmalar

Bu tez çalışmasında üzerinde durulan BioPSTM ve BioTAM yöntemlerinin nasıl kullanılabileceği, nihayetinde daha önce birbirinden bağımsız olarak yürütülmüş araştırmaların sonuçları üzerinden verilmiştir. Bu örnek çalışmaların gerçek saha verileri üzerinde binlerle ifade edilen denek kümelerinde tekrarlanması çok daha anlamlı bilgiler sunabilir. Bu geniş denek kümesinde gerçek biyometrik veriler toplanmalı, çapraz testler yapılarak sınıf içi ve sınıflar arası değişintiler ile normalize sızıntı oranları hesaplanmalıdır.

BioTAM'daki hipotezlere de eğilmek gerekir. Özellikle dışsal etmenlerin ne olduğunun daha derinlemesine analiz edilmesi, psikolojik ve sosyolojik faktörlerin toplum bilimciler ve diğer uzmanlarla irdelenmesi ve yeni hipotezlerin üretilmesi daha etkin BioTAM'lar için zemin hazırlayabilir.

Bu çalışmada ele alınan BKYS'nin özellikle biyo-kıyım ve sendrom kodlama gibi bileşenleri de daha yeni ve gelişmiş yöntemlerle değiştirilebilir. Özellikle çoklu

biyometriklere uyarlanmış kıyım algoritmaları, daha az örnek ile eğitilebilen biyometrik modeller ve daha gürbüz hata düzeltme kodlarının araştırılması normalize sızıntı oranlarını olumlu yönde etkileyebilir.

BKYS'lerde sentetik özel anahtarlardan tamamen kurtulmak çok mümkün görünmemektedir. O nedenle anahtar üretim mekanizmalarının da gözden geçirilmesi gerekir. Yazılımsal anahtar üreteçleri yerine donanım tabanlı rasgele sayı üreteçleri ile tahmini neredeyse imkansız özel anahtarlar üretilebilir.

Son olarak, her ne kadar bu çalışmada normalize sızıntı oranları ve kullanıcı kabul olasılık fonksiyonları tercih edilmiş olsa da, farklı entropik ölçütler ve olasılıksal modeller incelenebilir, temel bileşen analizi gibi yöntemlerle BioPSTM ve BioTAM'ı etkileyen faktörler arasında önceliklendirme yoluna gidilebilir.

KAYNAKLAR

[1] D. Maio, D. Maltoni, A.K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition. Springer, Verlag, 2003.

[2] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle, "Generating Cancelable Fingerprint Templates," *IEEE Trans. on Pat. An.and Mac. Intelligence*, Vol. 29(4) pp. 561-572, 2007.

[3] A. Kanak and I. Ispinar, "BioPSTM: A Formal Model for Privacy, Security, and Trust in Template-protecting Biometric Authentication," *Security Comm. Netwoks*, 2012.

[4] A. Kanak and I. Ispinar, "BioTAM: A Technology Acceptance Model for a Privacy-Preserving, Secure and Trustworthy Biometric Identity Management System," *Computers and Security*, (under review).

[5] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," *Proc. of IEEE*, Vol. 92, No. 6, pp. 948-960, 2004.

[6] A.T.B. Jin, D.N.C. Ling, and A. Goh, "Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number," *Pattern Recognition*, Issue 11(37) pp. 2245-2255, 2004.

[7] Y. Dodis, L. Reyzin, and A.Smith, "Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data," *EUROCRYPT'04, LNCS3027*, Berlin, Germany; Springer Verlag, Vol. 3027, pp. 523-540, 2004.

[8] Y. Sutcu, Q. Li, and N. Memon, "Protecting Biometric Templates with Sketch: Theory and practice," *IEEE Trans. on Inf. Forensics and Security*, Vol. 2, No.3, pp. 502-512, 2007.

[9] R.G. Gallager, Low-Density Parity-Check Codes. M.I.T. Press, 1963.

[10] D.J.C. Mackay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. on Informatioan Theory*, vol.45, No. 2, pp.399-411, March 1999.

[11] T. Ignatenko and F. Willems, "Privacy leakage in biometric secrecy systems," *46th Allerton Conf. Comm., Control and Comp.*, Monticello, Sep. 2008.

[12] L. Badia, M. Lindstrom, J. Zander, M. Zorzi, “Demand and pricing effects on the radio rsource allocation of multimedia communication systems,” *Globecom2003*, 2003.

[13] O. Ileri, D. Samardzija, and N.B. Mandayam, “Demand responsive pricing and competitive spectrum allocation via a spectrum server,” *IEEE DySpan*, Baltimore, MD, pp.194-202, 8-11Nov., 2005.

[14] C. Soutar, D. Roberge, S.A. Stojanov, R. Gilroy, and B.V.K. Vijaya Kumar, “Biometric Encryption Using Image Processing,” *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II.*, Vol.3314, pp. 178-188, 1998.

[15] M. Savvides, B.V.K. Vijaya Kumar, and P.K. Khosla, “Cancelable Biometric Filters for Face Recognition,” *Proc. of Int. Conf. on Pattern Recognition*, pp. 922-925, 2004.

[16] N.K. Ratha, J.H. Connel, R. Bolle, and S. Chikkerur, “Cancelable Biometrics: A Case Study in Fingerprints,” *Proc. of Int. Conf. on Pattern Recognition*, 2006.

[17] G.I. Davida, Y. Frankel, and B. Matt, “On Enabling Secure Applications Through OFF-line Biometric Identification,” *Proc. IEEE Symp. Privacy and Security*, pp. 148-157, 1998.

[18] F. Monrose, M.K. Reiter, and S. Wetsel, “Password Hardening Based on Keystroke Dynamics,” *Proc. ACM Conf. Computer and Communication Security*, pp. 73-82, 1999

[19] F. Monrose, M.K. Reiter, Q. Li, and S. Wetsel, “Using Voice to Generate Cryptographic Keys,” *Proc. 2001: A Speaker Odyssey, Speaker Recognition Workshop*, pp. 237-242, 2001.

[20] X. Boyen, “Reusable Cryptographic Fuzzy Extractors,” *Proceedings of the 11th ACM conference on Computer and Communications Security*, pp. 82-91, 2004.

[21] A. Juels, and M. Sudan, “A Fuzzy Vault Scheme,” *Des. Codes Cryptography* Vol. 38, No: 2, pp. 237-257, 2006.

[22] A. Juels, and M. Wattenberg, “A Fuzzy Commitment Scheme,” *Proc. ACM Conf. Computer and Communications Security*, G. Tsudik, Ed., pp. 28-36, 1999

[23] T.C. Clancy, N. Kiyavash, and D.J. Lin, “Secure Smartcard-based Fingerprint Authentication,” *Proc. ACM SIGMM Multimedia, Biometrics Methods and Applications Workshop*, pp.45-52, 2003.

[24] U. Uludag, and A.K Jain, “Securing Fingerprint Template: Fuzzy Vault with Helper Data,” *Proc. IEEE Workshop on Privacy Research in Vision*, New York City, NY., 2006.

[25] S. Tulyakov, F. Farooq, V. Govindaraju, “Symmetric Hash Functions for Fingerprint Minutiae,” *ICAPR (2)*, pp. 30-38, 2005.

[26] Y. Sutcu, H.T. Sencar, and N. Memon, “A Geometric Transformation to Protect Minutiae-Based Fingerprint Templates,” *SPIE International Defense and Security Symposium*, Orlando, USA, 2007.

[27] Y. Sutcu, H.T. Sencar, and N. Memon, “A Secure Biometric Authentication Scheme Based on Robust Hashing,” *Conf. MM-SEC*, New York, USA, 2005.

[28] M. Fairhust, S. Hoque, W.G.J. Howells, and F. Deravi, “Evaluating Biometric Encryption Key Generation,” *Proc. 3rd Cost 275 Workshop Biometrics Internet*, 93-96, 2005.

[29] W. Sheng, G. Howells, M. Fairhust, and F. Deravi, “Template-Free Biometric Key Generation by means of Fuzzy Genetic Clustering,” *IEEE Trans. Information Forensics and Security*, Vol.3, No.2, 183-191, 2008.

[30] W. Zhang, and T. Chen: “Generalized Optimal Thresholding for Biometric Key Generation Using Face Images,” *Proc. Int. Conf. Image Processing*, Vol. 3, 784-787, 2005.

[31] Y.J. Chang, W. Zhang, and T. Chen, “Biometric-based Cryptographic Key Generation,” *Int. Conf. on Multimedia and Expo*, 2004.

[32] J.P. Linnartz and P.Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates,” *4th Int. Conf. Audio- and Video-Based Biometric Person Authentication*, pp. 393-402, 2003.

[33] P. Tuyls and J. Goseling, “Capacity and examples of template-protecting biometric authentication systems,” *in ECCW Workshop bioAW, LNCS3087*, Berlin, Germany; Springer Verlag, Vol. 3087, pp. 158-170, 2004.

[34] I.R. Buhan, J.M. Doumen, P.H. Hartel, and R.N.J. Veldhuis, “Fuzzy Extractors for Continuous Distributions,” *ACM Symp. on Inf., Comp. and Comm. Security*, Singapore , pp. 353-355, 2007.

[35] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, “Embedding renewable cryptographic keys into continuous noisy data,” *10th Int. Conf. on Inf.and Comm. Sec. (ICICS), LNCS5308*, vol.5308, Springer Verlag, pp.294-310, Oct. 2008.

[36] E. Chang and Q. Li, “Hiding secret points amidst chaff,” in *EUROCRYPT, LNCS4004, Workshop* Vol. 4004, pp. 59-72, May 2006.

[37] T.S. Ong and A.B.J. Teoh, “Fuzzy Key Extration from Fingerprint Biometrics based on Dynamic Quantization Mechanism”, *3rd Int. Symp. on Inf. Assurance and Sec.*, pp. 71-76, 2007.

[38] V.V.T. Tong, H. Sibert, J. Lecoeur, M. Girault, “Biometric fuzzy extractors made practical: A proposal based on fingercodes,” *Advances in Biometrics, LNCS4642*, vol. 4642, pp.604-613, 2007.

[39] F.H. Alvarez and L.H. Encinas, “Security efficiency analysis of a biometric fuzzy extractor for iris templates,” *Adv. in Soft Computing*, Vol. 63, pp.163-170, 2009.

[40] Y. Yamazaki, and N. Komatsu, “A Secure Communication System Using Biometric Identity Verification,” *IEICE Trans. Inf. Syst*. vol. E84-D, No. 7, pp. 879-884, 2001.

[41] F. Hao and C.W. Chan, “Private Key Generation from On-line Handwritten Signatures,” *Inf. Mngmt. Comput. Sec.*, Vol. 10, No. 4, pp. 159-164, 2002.

[42] C. Vielhauer and C. Steinmetz, “Feature Correlation Analysis for Biometric Hashes,” *EURASIP J. Appl. Signal Process.* vol. 4, pp.542-558, 2004.

[43] Y.J. Lee, K.R. Park, S.J. Lee, K. Bae, J. Kim, “A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System”, *IEEE Trans. on Sys., Man. and Cyber.*, Part B, Vol.38, Issue: 5, pp. 1302-1313, 2008.

[44] A. Kanak and I. Sogukpinar, “Classification Based Revocable Biometric Identity Code Generation,” *BioID- MultiComm2009, LNCS 5707*, pp. 276-284, 2009.

[45] A.K. Jain, K. Nandakumar, A. Nagar, “Biometric template security,” *EURASIP J. on Adv. in Sig. Proc., Special Issue on Adv. Sig. Proc. and Pat. Recogn. Methods for Biometrics*, vol.2008, pp.1-17, Jan. 2008.

[46] L. Ballard, S. Kamara, F. Monrose, “Towards practical biometric key generation with randomized biometric templates,” *CCS’08, 15th ACM Conf. on Comp. and Comm. Sec.*, pp. 235-244, 2008.

[47] Q. Tang, J. Bringer, H. Chabanne, D. Pointcheval, “A formal study of the privacy concerns in biometric-based remote authentication schemes,” *ISPEC2008, LNCS 4991*, pp.56-70, Sydney, Australia, April 2008.

[48] T. Ignatenko and F. Willems, “Secret rate-privacy leakage in biometric systems,” *IEEE Int. symp. on Inf. Theory*, pp. 2251-2255, 2009.

[49] L. Lai, S.W. Ho, H.V. Poor, “Privacy-security tradeoffs in biometric security sytems,” *46th Allerton Conf. Comm., Control and Comp.*, Monticello, Sep. 2008.

[50] J.D. Golic and M. Baltatu, “Entropy analysis and new constructions of biometric key generation system,” *IEEE Trans. On Information Theory*, Vol. 54, No. 5, May 2008.

[51] N.K. Ratha, J.H. Connel, R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, Vol. 40(3), pp. 614-634, 2001.

[52] P. Tuyls, B. Skoric, T. Kevenaar, “Security with noisy data: Private biometrics, secure key storage and anti-counterfeiting,” Springer Verlag, London, 2007.

[53] K. Simoens, P. Tuyls, B. Preenel, “Privacy weaknesses in biometric sketches,” *30th IEEE Symp. on Security and Privacy*, pp. 188-203, May 2009.

[54] Y. Sutcu, S. Rane, J. Yedidia, S. Draper, A. Vetro, “Feature transformation of biometric templates for secure biometric systems based on error correcting codes,” *IEEE Computer Vision and Pattern Recognition Workshop, CVPRW2008*, pp.1-6, 2008.

[55] I. Buhan, E. Kelkboom, K. Simoens, "A survey of the security and privacy measures for anonymous biometric authentication systems," *6th Int. Conf. on Intelligent Inf. Hiding and Multimedia Sig. Proc.*, 2010.

[56] A. Vetro, S.C. Draper, S. Rane, J.S. Yedidia, "Securing biometric data," *Preprint of a chapter in Distributed Source coding, P.L. Dragotti and M. Gastpar Eds.*, Academic Press, Feb. 2009.

[57] Y. Sutcu, S. Rane, J. Yedidia, S. Draper, A. Vetro, "Feature extraction for a Slepian-Wolf biometric system using LDPC codes," *IEEE Int. Symp. on Information Theory*, 2008.

[58] A. Salehi-Abari and T. White, "The relationship of trust, demand, and utility: Be more trustworthy, then I will buy more," *8th Annual Int. Conf. on Privacy, Security and Trust*, pp. 72-79, 2010.

[59] T.D. Huynh, N.R. Jennings, N.R. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Autonomous Agents and Multi-Agent Systems*, Vol. 13, No. 2, pp.119-154, 2006.

[60] J. Sabater and C. Sierra, "Regret: A reputation model for gregarious societies," *4th Workshop on Deception Fraud and Trust in Agent Societies*, pp. 61-70, 2001.

[61] B. Yu and M.P. Shingh, "A social mechanism of reputation management in electronic communities," *Proceedings of CIA'00*, pp. 154-165, 2000.

[62] A. Josang and R. Ismail, "The beta reputation system," *15th Bled Electronic Commerce Conf.*, 2002.

[63] J. Sabater and C. Sierra, "Review on computational trust and reputation models," *Artif. Intell. Rev.*, Vol.24, No. 1, pp. 33-60, 2005.

[64] I. Ajzen and M. Fishbein, Understanding attitudes and predicting social behaviour. Prentice-Hall, Englewood Cliffs, NJ, 1980.

[65] F.D. Davis, "A technology acceptance model for empirically testing new end-user information systems: Theory and results," Doctoral dissertation, Sloan School of Management,Massachusettes Institute of Technology, 1986.

[66] F.D. Davis, “Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology,” *MIS Quarterly*: 13, pp. 319-339, 1989.

[67] E. Kaasinen, “User acceptance of mobile services - value, ease of use, trust and ease of adoption,” Doctoral dissertation, VTT publications 566, Espoo: VTT Information Technology, 2005.

[68] E. Kaasinen, V. Ermolov, M. Niemela, T. Tuomisto and P. Valkkynen, “ Identifying user requirements for a mobile terminal centric ubiquotious computing architecture,” *Workshop at Ubicomp FUMCA 2006: System Support for Future Mobile Computing Applications*, 2006.

[69] Y. Levy and M.M. Ramim, “Initial Development of a Learners Ratified Acceptance of Multibiometrics Intentions Model (RAMIM),” *Interdisciplinary Journal of E-Learning and Learning Objects*, Vol. 5, 2009.

[70] G.U. Nwatu, “Biometrics Technology: Understanding Dynamics Influencing Adoption for Control of Identification Deception Within Nigeria”, PHD thesis, 2011.

[71] H.R. Varian, Intermediate Microeconomics: A Modern Approach. New York, W.W. Norton, 1987.

[72] S. Furnell and K. Evangeltos,“Public awareness and perception of biometrics,” *Computer Fraud and Security*, pp.8-13 January 2007.

[73] Unisys Security Index: Global Summary, conducted by Lieberman Research Group, 1 December 2008 (Wave 3)

[74] Unisys Security Index: Supplemental Question, conducted by Lieberman Research Group, 1 December 2008 (Wave 3)- Revised 4/9/2009.

[75] G. Ho, G. Stephens and R. Jamieson,“Biometric Authentication Adoption Issues,” *Australasian Conference on Information Systems*, pp. 1-12, 2003.

[76] A. Chau, G. Stephens and R. Jamieson, “Biometrics Acceptance - Perceptions of Use of Biometrics,” *Australasian Conferences on Information Systems (ACIS)*, 2004.

[77] I. Giesing, "User Perceptions Related To Identification Through Biometrics Within Electronic Business," Master's Thesis. South Africa: University of Pretoria, 2003.

[78] T. James, T. Pirim, K. Boswell, B. Reithel and R. Barkhi, "Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model," *Journal of Organizational and End User Computing*, Vol. 18, No. 3, pp. 1-24, 2006.

[79] L.A. Jones, A.I. Ant and J.B. Earp, "Towards Understanding User Perceptions of Authentication Technologies," *Workshop On Privacy In The Electronic Society*, pp. 91-98, 2007.

[80] J. Kim, P. Brewer and B. Bernhard, "Hotel Customer Perceptions of Biometric Door Locks: Convenience and Security Factors," *Journal of Hospitality and Leisure Marketing*, Vol. 17, No. 1-2, pp. 162-182, 2008.

[81] H.C. Murphy and D. Rottet, "An Exploration of the Key Hotel Processes Implicated in Biometric Adoption," *International Journal of Contemporary Hospitality Management*, Vol. 21, No. 2, pp. 201-212, 2008.

[82] R. Tassabehji and M.A. Kamala, "Improving e-Banking Security with Biometrics: Modeling User Attitudes and Acceptance," *IEEE International Conference on New Technologies, Mobility and Security*, pp. 1-6, 2009.

[83] F. Al-Harby, R. Qahwaji and M. Kamala, "The Effects of Gender Differences in the Acceptance of Biometrics Authentication Systems within Online Transaction," *IEEE International Conference on CyberWorlds*, pp. 203-210, 2009.

[84] F. Al-Harby, R. Qahwaji and M.K amala, "Towards an Understanding of User Acceptance to Use Biometrics Authentication Systems in E-Commerce: Using an Extension of the Technology Acceptance Model," *International Journal of E-Business Research*, Vol. 6, No. 3, pp. 34-55, 2010.

[85] B. Michael, H. Milena and H. Khaled, "Consumer Acceptance of Biometrics for Identity Verification in Financial Transactions," *Proceedings of European Conference on Information Systems*, 2009.

[86] BioSec Consortium, “Introduction of A Multi-Modular Attitude and Usability Questionnaire for Biometric Security,” 2005.

[87] M. Amberg, M. Hirschmeier, J. Wehrmann, “The Compass Acceptance Model for the analysis and evaluation of mobile services,” *International Journal of Mobile Communications (IJMC)*, vol. 2, is. 3, pp. 248-259, 2004.

[88] V. Venkatesh, M.G. Morris, F.D. Davis, and G.B. Davis “User Acceptance of Information Technology: Toward a Unified View,” *MIS Quarterly*, 27, 425-478, 2003.

[89] F. Al-Harby, R. Qahwaji and M. Kamala, “The Role of User Self-Efficacy for the Acceptance of Biometrics Fingerprint Authentication System in E-commerce: The Use of UTAUT Model,” *Proceedings of the Saudi International Conference*, 2009.

[90] F. Al-Harby, R. Qahwaji and M. Kamala, “Users’ Acceptance of Secure Biometrics Authentication System: Reliability and Validate of an Extended UTAUT Model,” *In F. Zavoral et al. (Eds.), Networked Digital Technologies, Communications in Computer and Information Science*, Vol. 87, Part 2, pp. 254-258. New York: Springer-Verlag Berlin Heidelberg, 2010.

[91] T. Alhussain, S. Drew, “Towards user acceptance of biometric technology in E-Government: A survey study in the Kingdom of Saudi Arabia.” *Proceedings of IFIP International Federation for Information Processing*, pp.26-38, Springer Boston, 2009.

[92] F.E. Uzoka and T. Ndzinge, “Empirical Analysis of Biometric Technology Adoption and Acceptance in Botswana,” T*he Journal of Systems and Software*, Vol. 82, pp. 1550-1564, 2009.

[93] M. Breward, M. Head, K. Hassanein “Consumer Acceptance of Biometrics for Identity Verification in Financial Transactions,” *Proceedings of the 17th European Conference on Information Systems (ECIS 2009)*, Verona, Italy, June, 2009.

[94] W. Elgarah, N. Falaleeva “Adoption of Biometric Technology: Information Privacy and TAM , ” *Proceedings of the Eleventh Americas Conference on Information Systems*, pp.1209-1212, Omaha, NE, USA August 11th -14th, 2005.

[95] P.H.P. Yeow, and F. Miller, “The Attitude of Malaysians towards MyKad,” *Proceedings of the 4th International Conference on Information Technology in Asia 2005 (CITA’05)*, Hilton, Kuching, Malaysia: Universiti Malaysia Sarawak, pp.39-44, 2005.

[96] P.H.P. Yeow, W.H. Loo, and S.C. Chong, “User Acceptance of Multipurpose Smart Identity Card in a Developing Country,” Journal of Urban Technology 14(1): 23-50, 2007.

[97] W.H. Loo, P.H.P. Yeow, and S.C. Chong, “User acceptance of Malaysian government multipurpose smartcard applications,” *Government Information Quarterly* 26: 358-367, 2009.

ÖZGEÇMİŞ

Alper Kanak, lisans eğitimini 2001 yılında İstanbul Teknik Üniversitesi - Kontrol ve Bilgisayar Mühendisliği'nde, yüksek lisans eğitimini ise 2004 yılında Koç Üniversitesi - Elektrik ve Bilgisayar Mühendisliği'nde tamamladı. Ardından Koç Üniversitesi'nde "İşitsel-Görsel bir Konuşmacı Tanıma ve Doğrulama Sistemi"ni tasarladı ve bu konuda birçok ulusal ve uluslararası makaleye katkıda bulundu. 2003 yılında TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - Tasarım ve Geliştirme Bölümüne "Araştırmacı" olarak kabul edildi. Kanak, bazı bilimsel dergi ve konferanslar ile ulusal ve uluslar arası AR-GE destek programlarında hakemlik yaptı ve organizasyon faaliyetlerine katkıda bulundu. 2005 yılından itibaren bağlı bulunduğu Ses İşleme Grubu'nun çalışmalarını genişletme ve grubun vizyonunu gelişen yeni teknolojilere göre güncelleme çalışmaları kapsamında "Çoklu-Ortam Teknolojileri Araştırma ve Geliştirme Laboratuvarı"nın kurulmasında aktif görev aldı. Konuşma ve ses teknolojilerine ek olarak, özellikle biyometrik işaret işleme, kişisel şablon koruma, dağıtık mimarilerde ses işleme yöntemlerinin gerçeklenmesi gibi alanlarda uzmanlık kazandı. Alper Kanak, AB Çerçeve Programları REGPOT-2008-1 çağrısına gönderilen MULTISAUND (Multilingualism Integrated to Speech and Audio Understanding) proje teklifinin hazırlanmasında ve daha sonra teklifin 15 üzerinden 15 tam puan alarak kabul edilmesinde öncü rol oynadı. 2005 yılında "Uzman Araştırmacı", 2009 yılında da "Başuzman Araştırmacı" ünvanı alan Alper Kanak, kurum içinde çeşitli projelerde görev aldıktan sonra 2012 yılından itibaren halen yöneticiliğini yaptığı "Avrupa Birliği Projeleri Programı" kapsamında TÜBİTAK Gebze Yerleşkesi'ndeki tüm Merkez ve Merkez'lere bağlı Enstitülerin uluslar arası fonlardan daha fazla yararlanmasını sağlayacak koordinasyon faaliyetleri sürdürmeye başladı. Kanak, 2004 yılında Gebze Yüksek Teknoloji Enstitüsü - Bilgisayar Mühendisliği Bölümünde başladığı doktora tez çalışmaları kapsamında literatüre biyometrikler üzerine biri değerlendirme aşamasında olan 4 dergi makalesi ve 2 konferans bildirisi kazandırmıştır.