Biyometrik Sistemler

Yapay Zekâ ve Veri Dersleri Rehberi · Kısım III: Sinyal, Görüntü ve Ses

Biyometrik özellikler | Doğrulama, tanımlama | Hata oranları | Sahtecilik | Gizlilik | Komşu dersler

Sercan KÜLCÜ · Giresun Üniversitesi · Bilgisayar Mühendisliği

© Sercan Külcü. Tüm hakları saklıdır. · Sunumun etkileşimli HTML sürümü: https://sercankulcu.github.io/files/ai_courses/sunumlar/Bolum_24_Biyometrik_Sistemler.html

GİRİŞ

Ders Hangi Soruyu Sorar?

> **Bir kişi yüzünden, parmak izinden ya da sesinden nasıl tanınır?**

Biyometrik sistemler, kişiyi yüz, parmak izi, iris ya da ses gibi **bedensel ve davranışsal özelliklerinden** tanır. Ders bir örnekten şablon çıkarmayı, iki şablonu eşlemeyi ve eşik seçerek kabul ya da ret kararı vermeyi inceler; güvenlik ve gizlilik bu kararın ayrılmaz parçasıdır.

Bir bakışta

YAKLAŞIM eşleme ve doğrulama	**GİRDİ** yüz, parmak izi, iris, ses	**ÇIKTI** kimlik kararı
BAŞARI ÖLÇÜTÜ FAR, FRR, EER	**MATEMATİK YÜKÜ** orta	**VERİ İHTİYACI** kişi başına az örnek

GİRİŞ

Kısa Tarihçe

1892
Galton "Finger Prints" kitabını yayımlar: parmak izinin kişiye özgü ve kalıcı olduğu gösterilir.

1901
Scotland Yard parmak izlerini Henry sınıflandırma sistemiyle kullanmaya başlar.

1991
Turk ve Pentland yüz tanımada özyüzleri (eigenfaces) yayımlar.

1993
Daugman iris tanıma yöntemini yayımlar; bugünkü iris sistemlerinin temeli olur.

2013
Parmak izi algılayıcısı (Touch ID) akıllı telefonlarda yaygınlaşmaya başlar.

2014
DeepFace ve ardından gelen derin ağlar yüz doğrulamada insan düzeyine yaklaşır.

DERS

Temel Kavramlar

Kayıt
Kişinin örneğinden şablon çıkarıp veri tabanına yazmak.

Şablon
Ham görüntü yerine saklanan öznitelik vektörü.

Doğrulama (1:1)
"Bu kişi iddia ettiği kişi mi?" sorusu.

Tanımlama (1:N)
"Bu kişi kayıtlılardan hangisi?" sorusu.

FAR ve FRR
Yanlış kabul ve yanlış ret oranı; eşik ikisini dengeler.

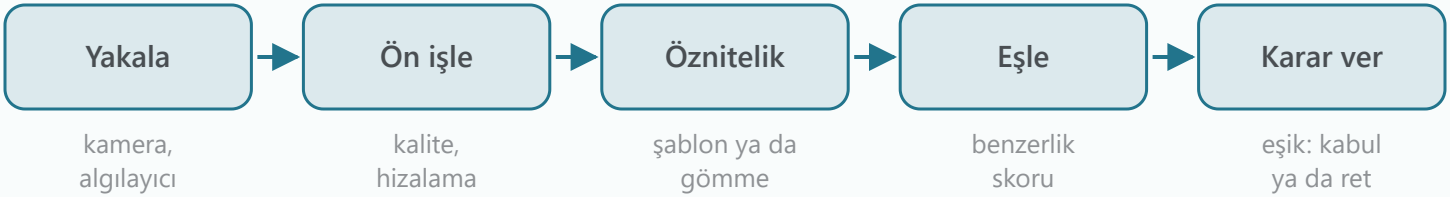
EER ve DET eğrisi
İki hatanın eşitlendiği nokta; sistemleri kıyaslamak.

Canlılık tespiti
Fotoğraf, maske ya da kalıp parmakla saldırıyı yakalamak.

Çok kipli biyometri
Yüz ile sesi ya da parmak izi ile irisi birleştirmek.

DERS

Tipik İş Akışı



Örnek: Telefonun yüz kilidi kızılötesi kamerayla yüzü yakalar, yüzü bulup hizalar, derin bir ağla gömme vektörü çıkarır, kayıtlı şablonla benzerliği ölçer ve skor eşiği geçerse kilidi açar. Canlılık denetimi fotoğrafla açılmasını engeller.

DERS

Derste Neler İşlenir?

1. Biyometrik sistem: kayıt, doğrulama, tanımlama
2. Başarım ölçümü: FAR, FRR, ROC, DET, EER
3. Parmak izi: ön işleme, minütyeler, eşleme
4. Yüz algılama ve hizalama
5. Yüz tanıma: özyüzler, LBP, derin gömmeler
6. İris: bölütleme, Daugman kodu, Hamming uzaklığı
7. Sesle konuşmacı doğrulama
8. Davranışsal biyometri: imza, yürüyüş, tuş vuruşu
9. Çok kipli biyometri ve skor birleştirme
10. Sunum saldırıları ve canlılık tespiti
11. Şablon koruma ve iptal edilebilir biyometri
12. Büyük ölçekli tanımlama, dizinleme ve standartlar

Kazandırdığı beceriler

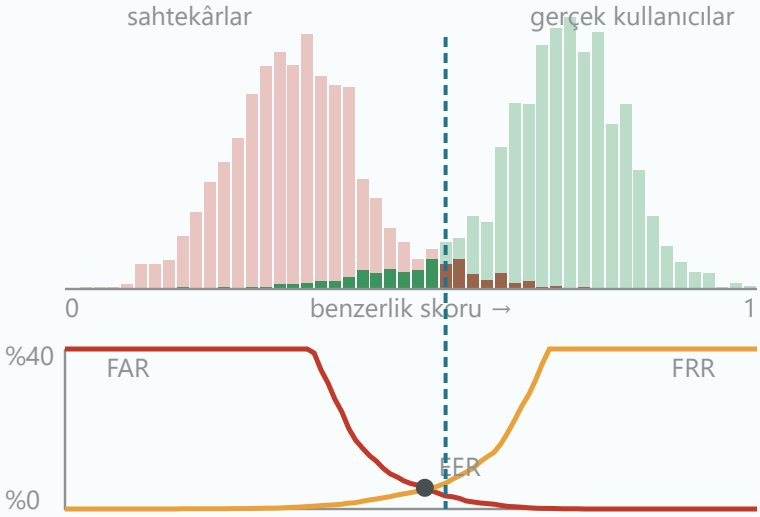
OpenCV ve dlib ile yüz işleme | InsightFace ile yüz gömmesi çıkarmak | DET eğrisi çizip EER hesaplamak | eşiği uygulamanın riskine göre seçmek | başarımı gruplara ayırarak ölçmek

Tipik bir dönemin akışıdır; sıra ve kapsam üniversiteden üniversiteye değişir.

DENE

Kapı Kimi İçeri Alsın?

Yüz tanıma kapısı her kişi için 0 ile 1 arası bir benzerlik skoru üretir; skor eşiği geçerse kapı açılır. Eşiği kaydırın ya da bir senaryo seçin: sahtekâr kabulü ile gerçek kullanıcının reddi arasındaki dengeyi görün.



Eşik = **0,55**

Havalimanı | Telefon kilidi | EER noktası

FAR (sahtekâr kabulü) = **%3,25**
FRR (gerçek kişi reddi) = **%6,45**
10 000 girişte ≈ 325 sahtekâr içeri girer, 645 yolcu kapıda kalır.

EER ≈ %5,3 (eşik 0,52): iki hatanın eşit olduğu nokta.

Biyometrik sistem hiçbir zaman “kesin” demez: iki dağılım örtüşür ve eşik, hangi hatanın daha pahalı olduğuna göre seçilir. Ders, bu skorları üreten öznitelik çıkarmayı ve FAR/FRR ile değerlendirmeyi öğretir.

KONUM

Ön Koşullar

Bu dersten önce bilinmesi yararlı olan dersler ve neden gerektikleri.

Ders	Neden gerekir
Örüntü Tanıma	eşleme, doğrulama ve tanımlama
Bilgisayarlı Görü	yüz tanıma
Programlama	Python ile görüntü okuma, vektörlerle çalışma
Veri Yapıları	1:N aramada milyonlarca şablonu hızla taramak için dizinleme

KONUM

Bu Ders Sana Göre mi?

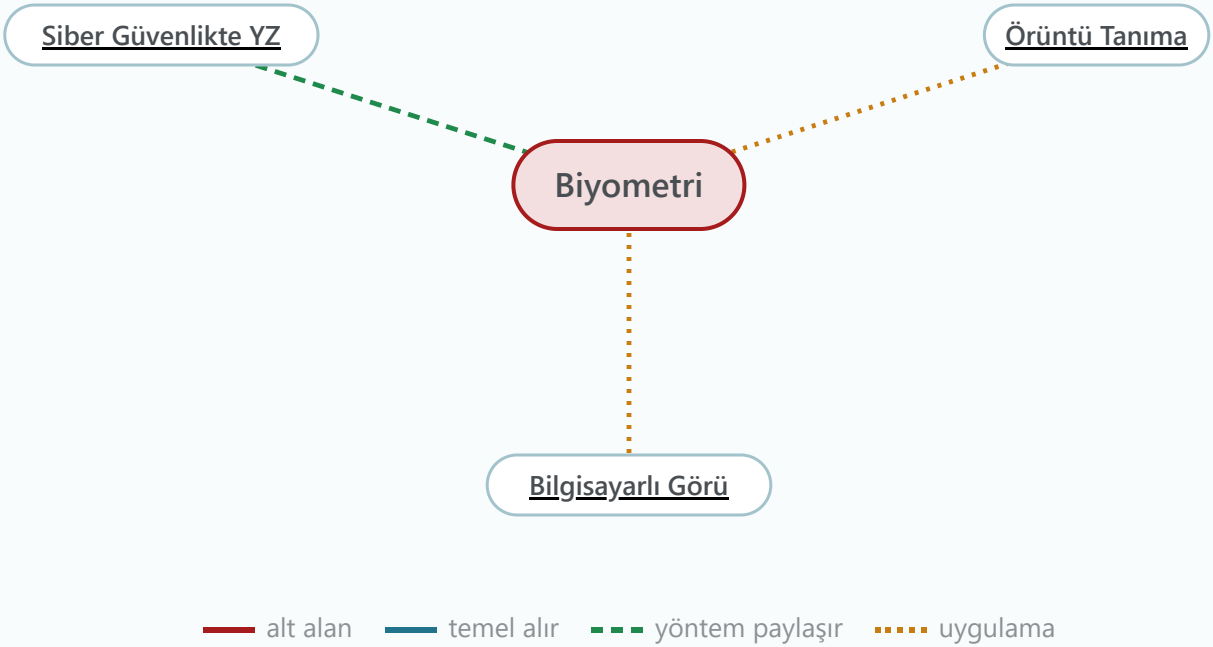
Kendine sor; "hayır" dediklerin için sağdaki sütun nereden başlayacağını gösterir.

Kendine sor	Hayırsa önce
Bir görüntüyü okuyup kırpabiliyor ve gri tona çevirebiliyor musun?	Görüntü İşleme
Bir sınıflandırıcının ROC eğrisini ve yanlış pozitif oranını açıklayabiliyor musun?	Örüntü Tanıma
İki vektör arasındaki kosinüs benzerliğini hesaplayabiliyor musun?	Doğrusal Cebir
Python'da NumPy dizileriyle bir klasördeki görüntüleri işleyebiliyor musun?	Programlamaya giriş, ardından NumPy'a kısa bir giriş

Çoğuna "evet" diyebiliyorsan derse hazırsın; bir ya da iki "hayır" dönem içinde kapanabilir.

KONUM

Dersin Komşuları



ÖRTÜŞME

Örtüştüğü Dersler

İlişki	Ders	Ortak konu
uygulama	Bu ders Örüntü Tanıma yöntemlerini uygular	eşleme, doğrulama ve tanımlama
uygulama	Bu ders Bilgisayarlı Görü yöntemlerini uygular	yüz tanıma
yöntem paylaşır	Siber Güvenlikte Yapay Zekâ ile yöntem paylaşır	kimlik doğrulama, sahtecilik tespiti

Ayrıştığı Noktalar (1/2)

Ölçüt	Biyometri	Örüntü Tanıma	Bilgisayarlı Görü
Temel soru	Bir kişi yüzünden, parmak izinden ya da sesinden nasıl tanınır?	Ölçümlerden bir nesnenin hangi sınıfa ait olduğuna nasıl karar verilir?	Bilgisayar bir görüntüde ya da videoda ne olduğunu nasıl anlar?
Yaklaşım	eşleme ve doğrulama	istatistiksel karar kuramı	görüntüden anlam çıkarma
Girdi	yüz, parmak izi, iris, ses	ölçüm ya da öznitelik vektörü	görüntü ya da video
Çıktı	kimlik kararı	sınıf etiketi	etiket, kutu, derinlik, 3B yapı
Başarı ölçütü	FAR, FRR, EER	sınıflandırma hatası	doğruluk, mAP, IoU
Matematik yükü	orta	orta-yüksek: olasılık, doğrusal cebir	yüksek: geometri, doğrusal cebir
Veri ihtiyacı	kişi başına az örnek	etiketli örnekler	çok etiketli görüntü

- **Örüntü Tanıma:** Örüntü tanıma bir örneği sınıflara ayırır; biyometri kişiyi tanır, sınıf sayısı kişi sayısı kadardır ve sürekli artar.
- **Bilgisayarlı Görü:** Bilgisayarlı görü görüntüdeki her şeyi anlamaya çalışır; biyometri yalnız kimliği soran dar ve güvenlik odaklı bir görevdir.

AYRIŞMA

Ayrıştığı Noktalar (2/2)

Ölçüt	Biyometri	Siber Güvenlikte YZ	Konuşma ve Ses İşleme
Temel soru	Bir kişi yüzünden, parmak izinden ya da sesinden nasıl tanınır?	Yapay zekâ saldırıları nasıl yakalar ve kendisi nasıl saldırıya uğrar?	Ses dalgasından sözcükler, konuşmacı ve olaylar nasıl çıkarılır?
Yaklaşım	eşleme ve doğrulama	güvenlik bilgisi ve MÖ	akustik sinyal ve dil modeli
Girdi	yüz, parmak izi, iris, ses	ağ trafiği, kayıtlar, dosyalar	ses dalgası
Çıktı	kimlik kararı	uyarı, sınıf, risk puanı	metin, konuşmacı, ses olayı
Başarı ölçütü	FAR, FRR, EER	tespit oranı, yanlış alarm oranı	sözcük hata oranı (WER)
Matematik yükü	orta	orta	orta-yüksek
Veri ihtiyacı	kişi başına az örnek	dengesiz ve sürekli değişen	çok saatlik kayıt

- **Siber Güvenlikte YZ:** Siber güvenlikte YZ saldırıları yakalar; biyometri kimlik doğrulamanın kendisidir ve sahte örnek saldırılarına karşı korunur.
- **Konuşma ve Ses İşleme:** Konuşma tanıma ne söylendiğini çıkarır; konuşmacı tanıma, yani biyometri, kimin konuştuğunu çıkarır.

UYGULAMA

Uygulama Alanları

Telefon kilidi
Yüz ve parmak iziyle cihaz açma.

Sınır kapısı
E-pasaport fotoğrafıyla otomatik geçiş.

Adli bilimler
Olay yeri izlerini veri tabanında aramak.

Bankacılık
Uzaktan müşteri doğrulama, ödeme onayı.

Giriş denetimi
Bina ve personel giriş-çıkış kaydı.

Nüfus kaydı
Ulusal kimlik sistemlerinde mükerrer kayıt önleme.

UYGULAMA

Riskler ve Etik

Kitlesel gözetim
Kamusal alanda gerçek zamanlı yüz tanıma, kimseye sorulmadan herkesi izlemeyi mümkün kılar; birçok ülke bunu yasayla sınırlar.

Yanlış eşleşmeyle gözaltı
ABD'de yüz tanımanın yanlış eşleşmesine dayanılarak suçsuz kişilerin gözaltına alındığı belgelenmiş olaylar vardır.

Amaç dışı kullanım
Kapı girişi için alınan yüz ya da parmak izi başka amaçla kullanılabilir; KVKK biyometrik veriyi özel nitelikli sayar.

Merkezî şablon deposu
Milyonlarca şablonu tek yerde toplamak sızıntıda herkesi birden etkiler; 2015'te ABD OPM sızıntısında 5,6 milyon parmak izi çalındı.

Ayrıntılı tartışma: Açıklanabilir Yapay Zekâ ve Yapay Zekâ Etiği.

UYGULAMA

Araçlar ve Örnek Veriler

Araçlar ve kütüphaneler

OpenCV · dlib · InsightFace · NIST NBIS · SpeechBrain

Tanınmış veri setleri

LFW (Labeled Faces in the Wild) · VGGFace2 · FVC2004 (parmak izi) · CASIA-Iris · VoxCeleb (konuşmacı)

Biyometrik veri **kişisel veridir**: KVKK ve GDPR kapsamındadır; bazı yüz veri setleri bu yüzden yayından kaldırılmıştır.

UYGULAMA

Sık Karıştırılanlar

Yaygın düşünce	Doğrusu
Biyometrik sistemler hata yapmaz.	Her sistem yanlış kabul ve yanlış ret yapar; eşik bu iki hatadan birini seçer.
Biyometrik veri parola gibi değiştirilir.	Yüz ya da parmak izi değiştirilemez; sızan şablon kalıcı risktir, şablon koruma gerekir.
Doğruluk herkes için aynıdır.	Başarım yaşa, ten rengine ve algılayıcıya göre değişebilir; değerlendirme gruplara ayrılarak yapılır.
Eşleşme varsa kişi oradadır.	Fotoğraf, maske ya da kayıt sesle sunum saldırısı yapılabilir; canlılık tespiti gerekir.

SONRASI

Bu Dersten Sonra

Bu dersi temel alan ya da genişleten dersler

Bu ders çoğunlukla uç noktadır; öteki dersleri temel alır.

İlgili meslekler

Biyometri mühendisi | Bilgisayarlı görü mühendisi | Kimlik ve erişim yönetimi uzmanı | Adli bilişim uzmanı

Biyometri, örüntü tanıma ve görünün güvenlikle buluştuğu yerdir. Buradan derin yüz tanıma ve konuşmacı tanımaya, sahtecilik tespitiyle siber güvenliğe ya da adalet ve gizlilik sorularıyla açıklanabilir YZ ve etiğe geçilebilir.

SONRASI

Kaynaklar

- Jain, Ross ve Nandakumar, *Introduction to Biometrics*, Springer, 2011.
- Li ve Jain (ed.), *Handbook of Face Recognition*, 2. baskı, Springer, 2011.
- Maltoni, Maio, Jain ve Feng, *Handbook of Fingerprint Recognition*, 3. baskı, Springer, 2022.
- Daugman, "How Iris Recognition Works", *IEEE Transactions on Circuits and Systems for Video Technology* 14(1), 2004.

Son

Bölüm 24: Biyometrik Sistemler

← Önceki bölüm · Alanın haritası · Sonraki bölüm →