Derin Sinir Ağları ile Tekrar Saldırılarının Tespiti

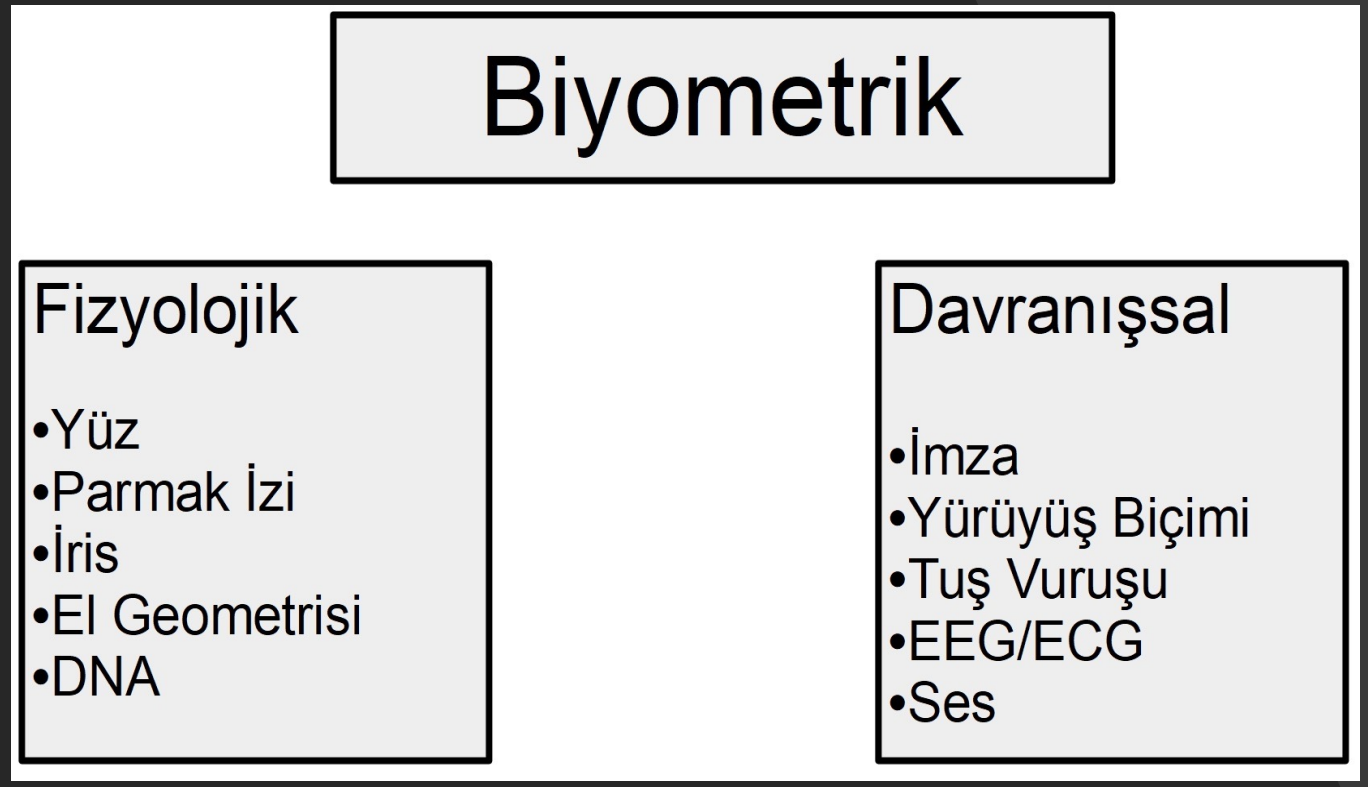
Bekir Bakar & Cemal Hanilçi
Elektrik-Elektronik Mühendisliği
Bursa Teknik Üniversitesi
b.bakar@outlook.com

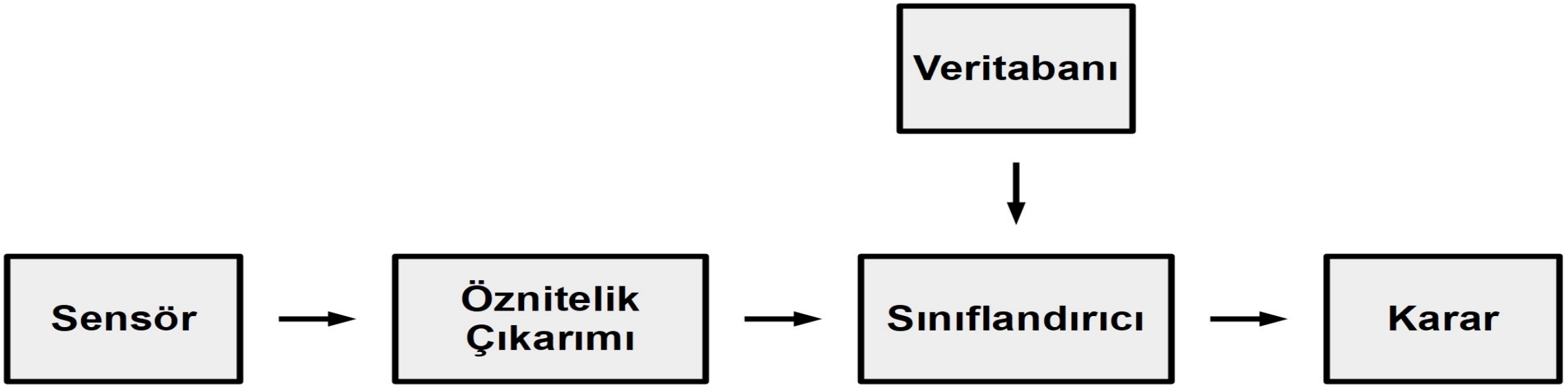
Sunum İçeriği

- Biyometrik Sistemler
- Konuşmacı Doğrulama
- Yanıltma Saldırıları
- Saldırı Tespiti
- Sonuçlar

Biyometrik Sistemler – Çeşitleri ve Avantajları

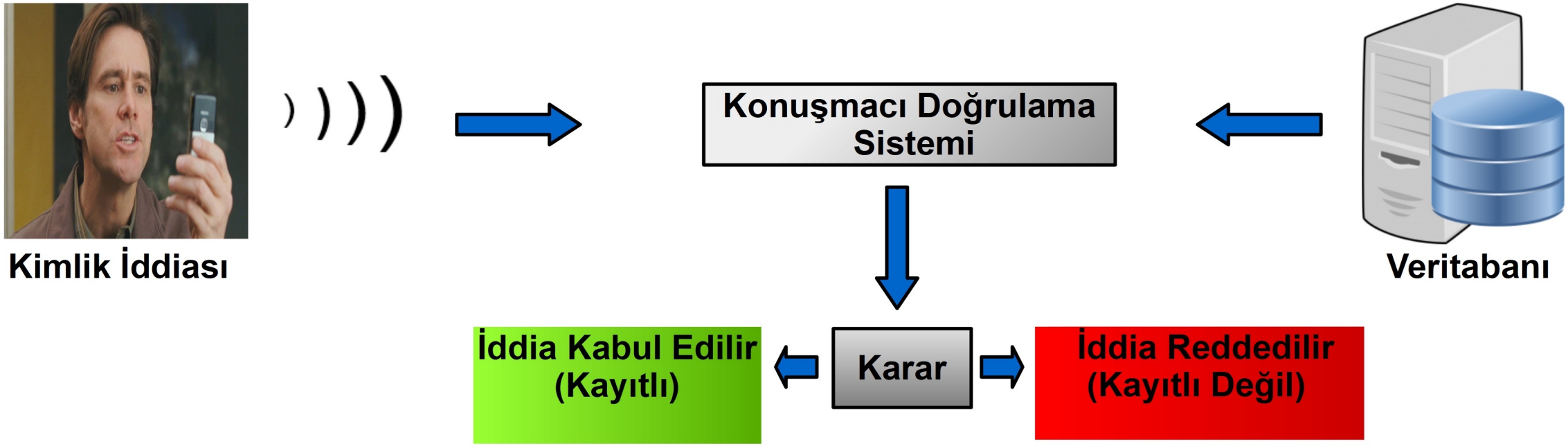
- Kişiye Özel
- Çalınması/Kopyalanması Zor
- Depolama/Yedekleme Problemi Yok
- Şifre Unutma veya Kaybetme Yok
- Kullanıcı Dostu
- Mobil Sistemlere Uyumlu





Biyometrik Sistemler-Çalışma Prensibi

[*]A. Hadid, N. Evans, S. Marcel and J. Fierrez, "Biometrics Systems Under Spoofing Attack: An evaluation methodology and lessons learned," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 20-30, Sept. 2015.



Konuşmacı Doğrulama

Yanıltma Saldırıları

- Ses Dönüştürme (Voice Conversion)
- Ses Sentezleme (Speech Synthesis)
- Taklit (Mimicry)
- Tekrar Oynatma (Replay)

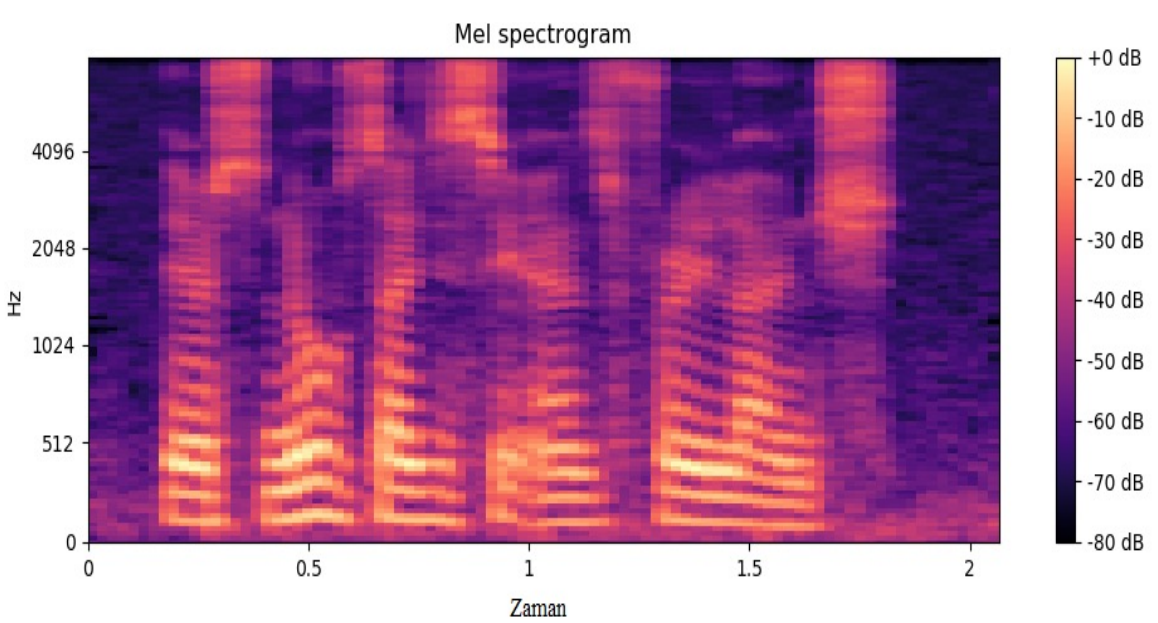
[*]Y. Qian, N. Chen, H. Dinkel and Z. Wu, "Deep Feature Engineering for Noise Robust Spoofing Detection," in IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 25, no. 10, pp. 1942-1955, Oct. 2017.

Saldırı Tespiti – Veri Tabanı (ASVspoof 2017)

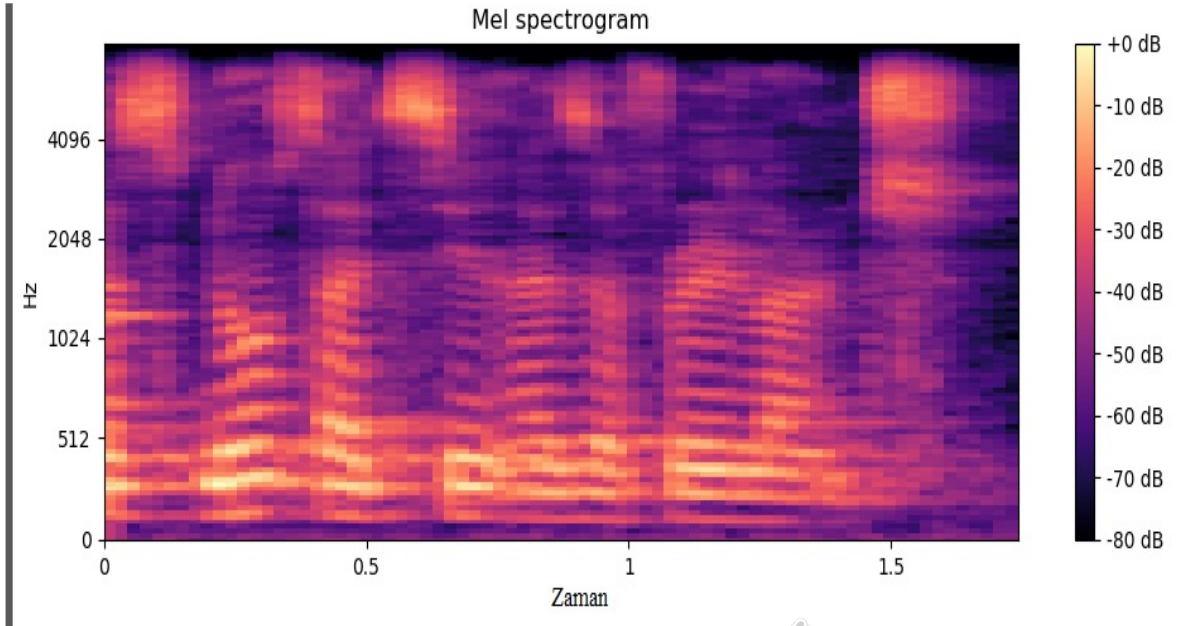
Alt Küme	Konuşmacı Sayısı	Kayıt Sayısı	
		Gerçek	Sentetik
Eğitim	10	1508	1508
Geliştirme	8	760	950
Değerlendirme	4	1294	11987

- 16 Khz
- 16 Bit
- Birbiri ile Örtüşmeyen

[*]http://www.asvspoof.org/



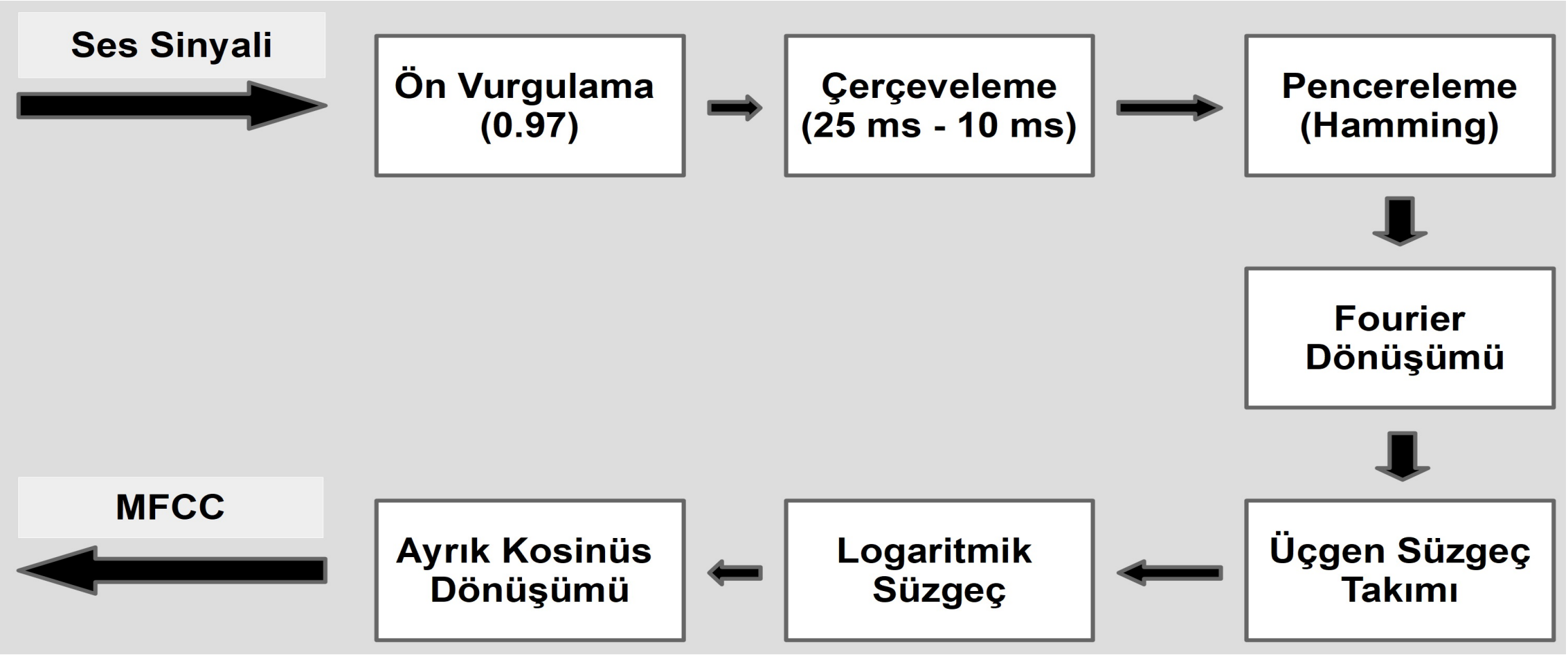
Gerçek Ses



Sahte Ses

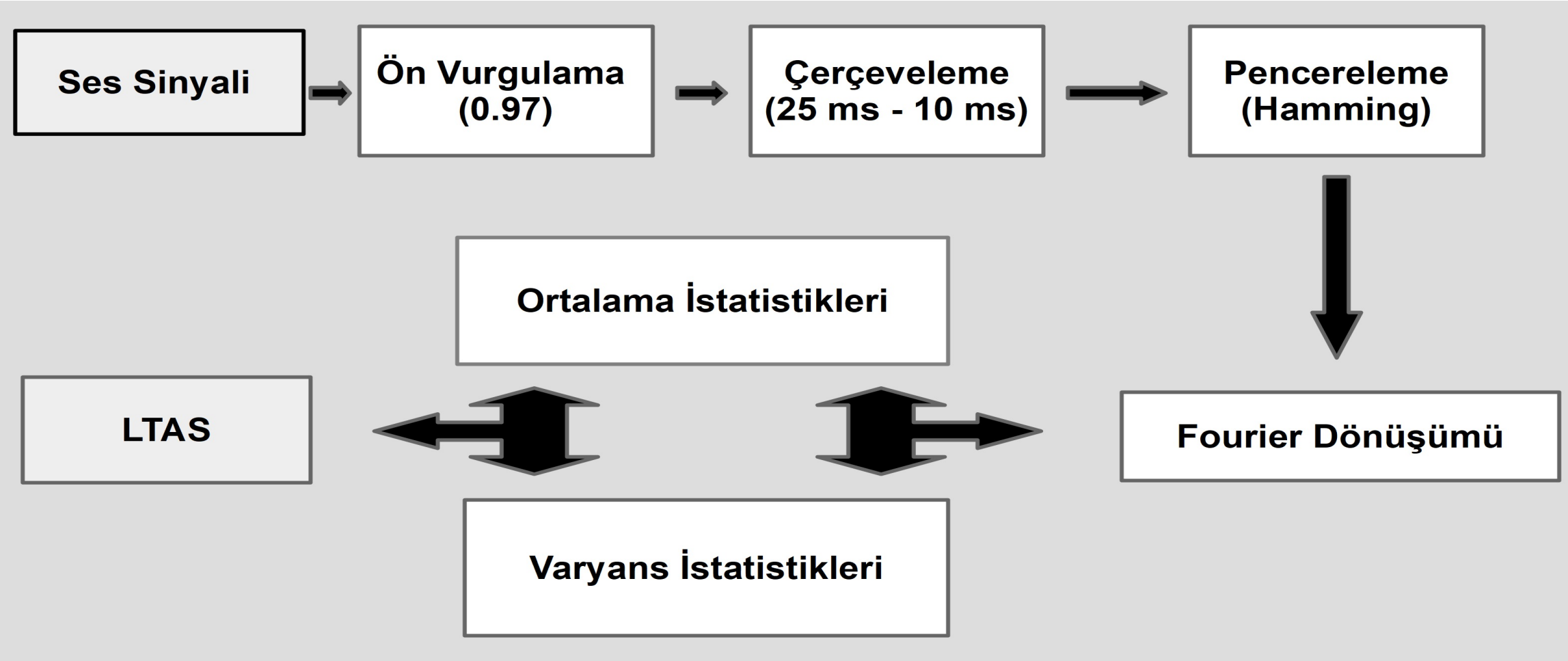
Saldırı Tespiti – Gerçek ve Sentetik Ses

Saldırı Tespiti - Öznitelikler (MFCC)



[*]S. Davis and P. Mermelstein, "Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences," in IEEE Transactions on Acoustics, Speech, and Signal Processing, vol. 28, no. 4, pp. 357-366, Aug 1980.

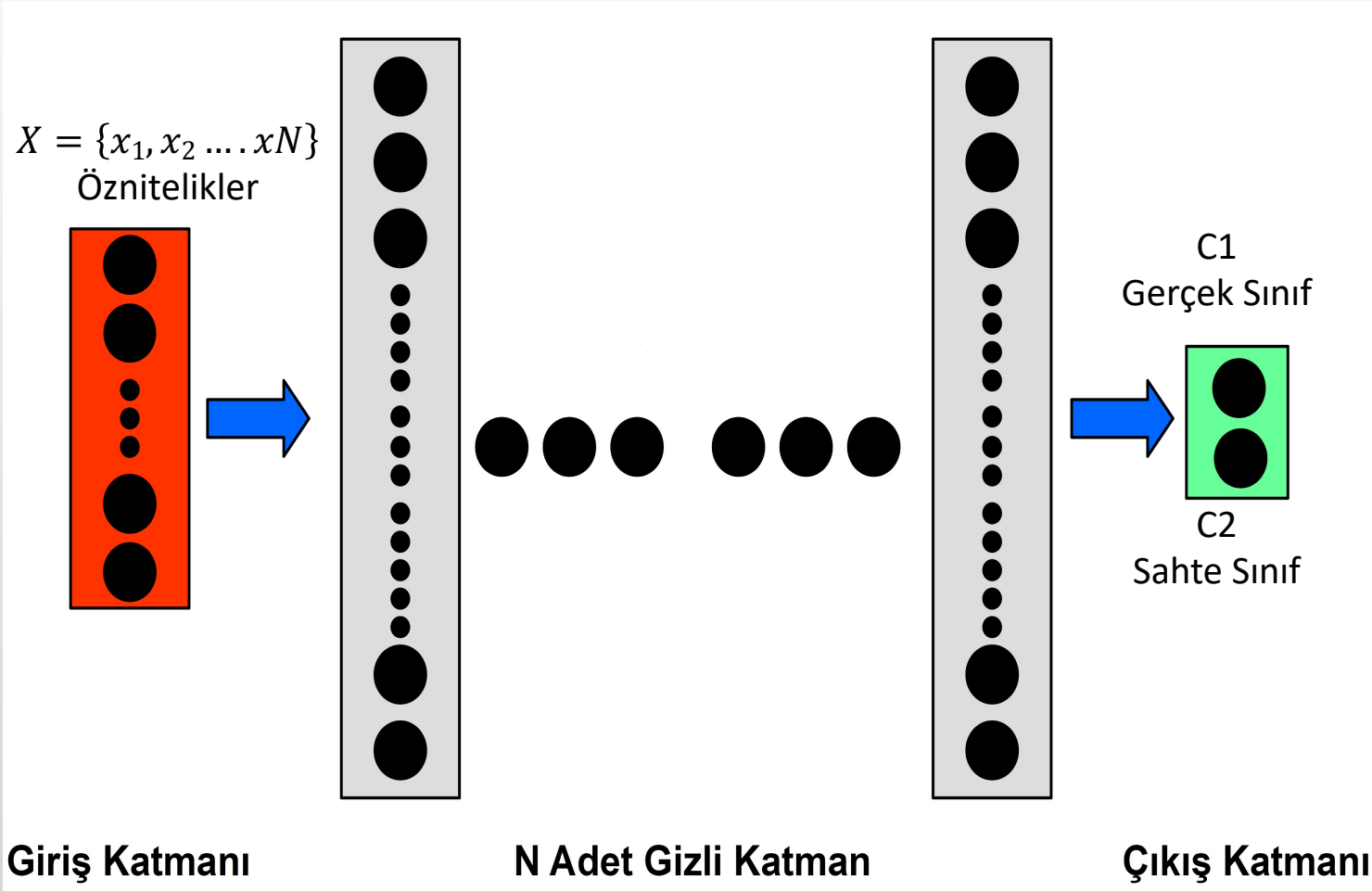
Saldırı Tespiti - Öznitelikler (LTAS)



[*]H. Muckenhirn, M. Magimai-Doss and S. Marcel, "Presentation Attack Detection Using Long-Term Spectral Statistics for Trustworthy Speaker Verification," *2016 BIOSIG*, Darmstadt, 2016, pp. 1-6.

Saldırı Tespiti – DNN

- İleri Beslemeli
- Relu Activasyon Fonksiyonu
- Dropout (0.75)
- LTAS - 1024 x 5 Gizli Katman
- MFCC - 512 x 3 Gizli Katman
- Softmax
- Her bir çıkış nöronu ilgili sınıfın sonsal (posterior) olasılığını temsil eder.
- Sonsal olasılıklar, logaritmik olabilirlik oranı skoruna dönüştürülür.



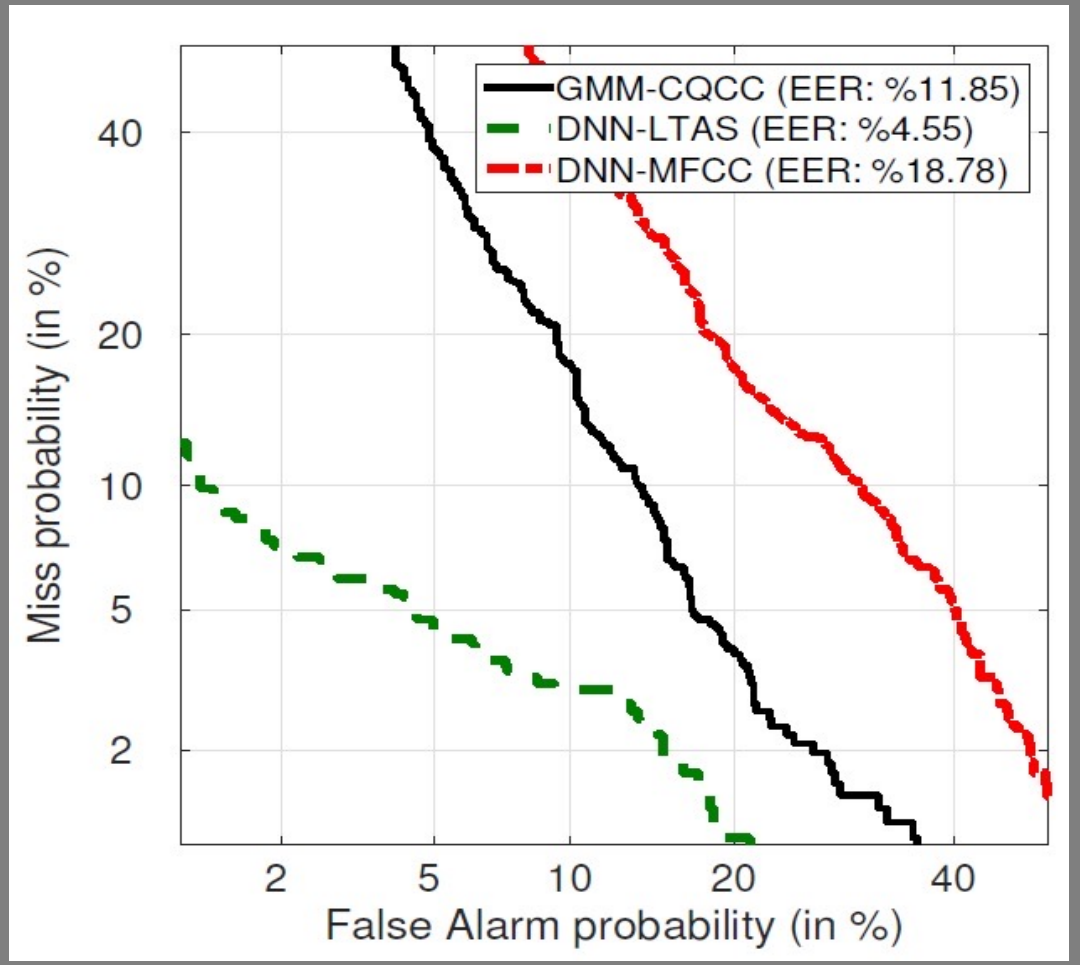
$$LLR = logp(X|C_1) - logp(X|C_2)$$

Sonuçlar – EER[%] Değerleri

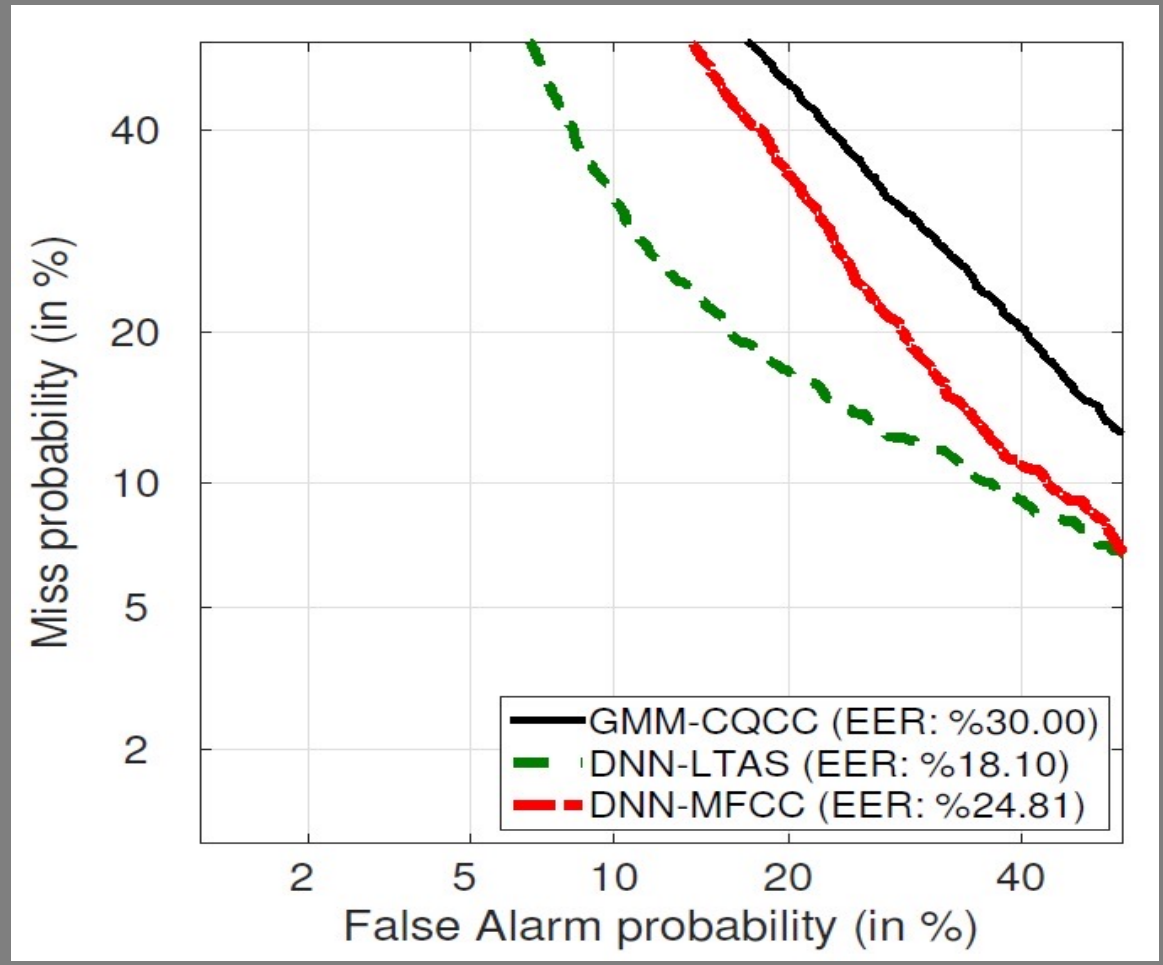
Öznitelik	Sistem	Alt Küme	
		Geliştirme	Değerlendirme
MFCC	DNN	18.78	24.81
LTAS	DNN	4.55	18.10
CQCC	GMM	11.85	30.00

EER, yanlış kabul ve yanlış red oranlarının birbirine eşit olduğu eşik değerdeki hata oranına karşılık gelmektedir.

Sonuçlar – DET Eğrileri



Geliştirme Kümesi



Değerlendirme Kümesi

TEŞEKKÜRLER

Bu çalışma TÜBİTAK (proje numarası 115E916) tarafından desteklenmiştir.