Konuşmacı Doğrulama Sistemlerinde Tekrar Saldırısı Tespiti İçin Yapay Sinir Ağlarının Kullanılması

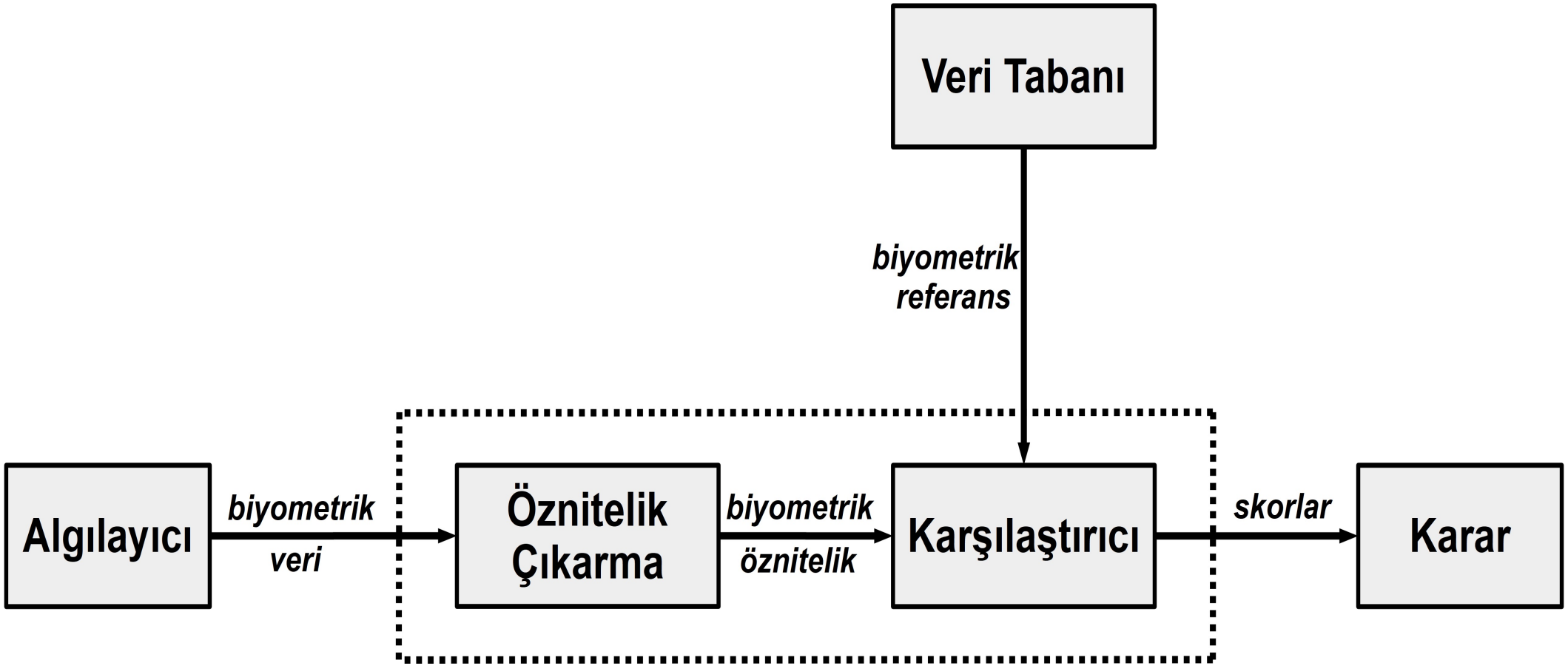
Öğrenci: Bekir BAKAR, 161082310
Danışman: Doç. Dr. Cemal HANİLÇİ

Yüksek Lisans Tez Savunması, 26 Aralık 2018

Biyometrik Sistem

- Güvenliğin sağlanması gereken durumlar vardır.
- Geleneksel/eski şifreleme yöntemlerinin bazı dezavantajları vardır.
- Fizyolojik ve davranışsal özelliklere biyometri denir.
- Biyometrik doğrulama, biyometrik verileri kullanır.

Biyometrik Sistem



Konuşmacı Doğrulama

- Ses sinyali birçok bilgi barındırmaktadır.

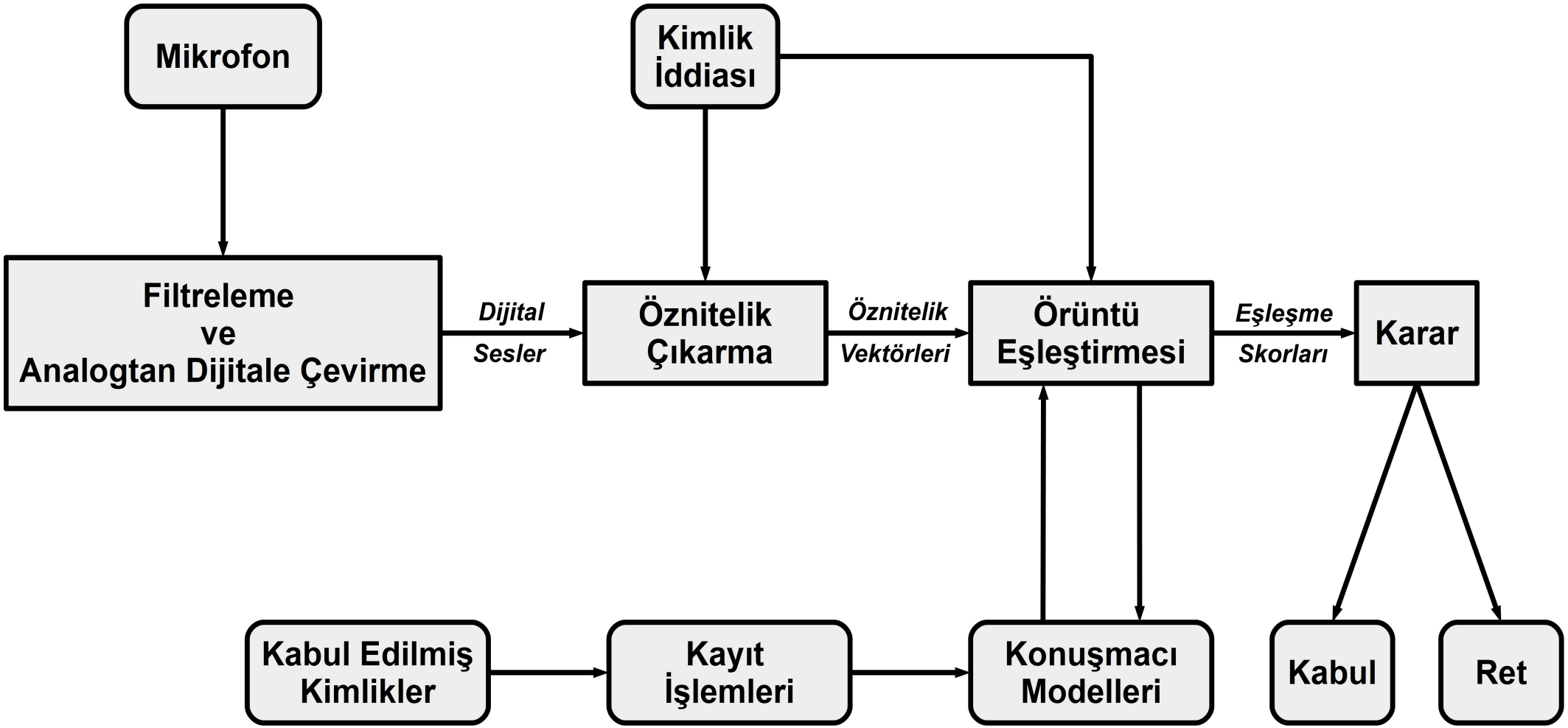
- Konuşmacı doğrulama kimlik kabul veya reddetme işlemidir.

- Konuşmacını doğrulamanın bazı avantajları konuya olan ilgiyi artırmıştır.

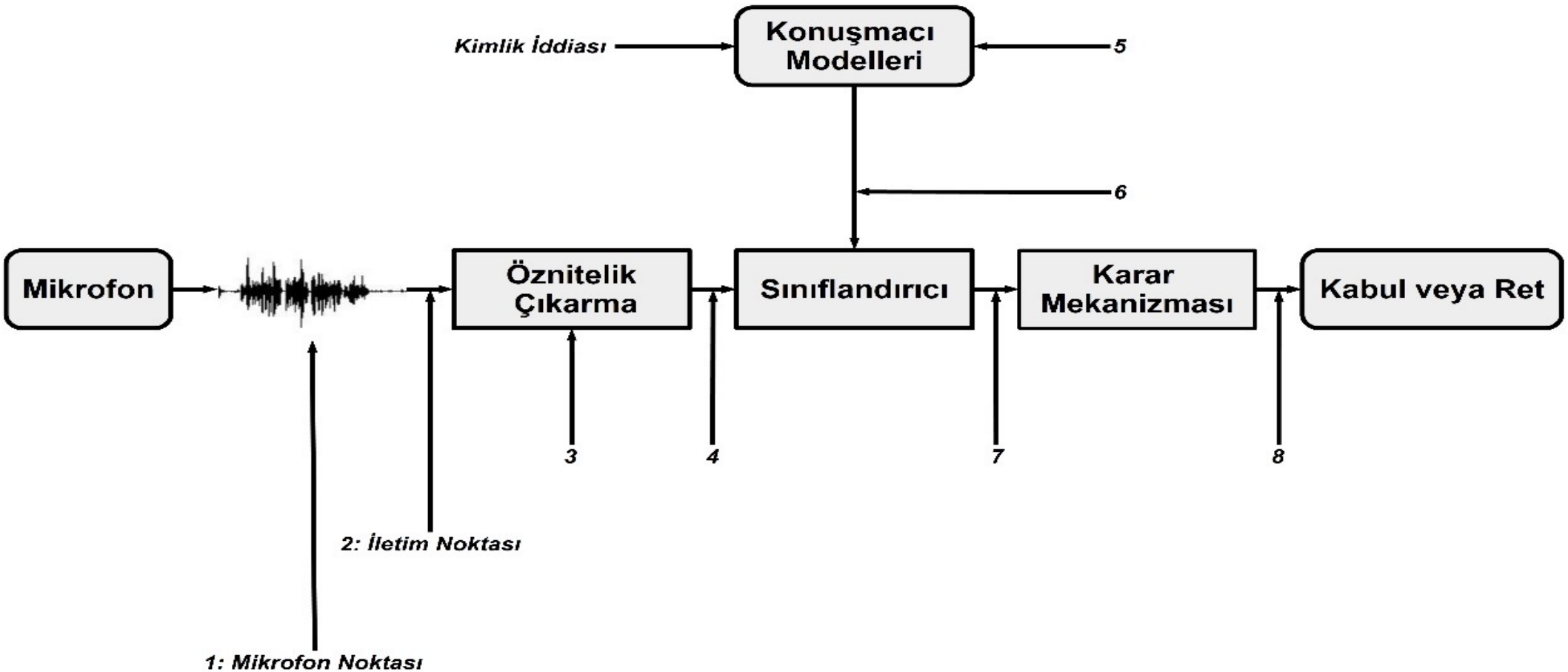
Konuşmacı Doğrulama

- Telekomünikasyon operatörleri
- Banka işlemleri, çağrı merkezleri
- Kişisel verilerin güvenliği
- Çeşitli sistemlere erişim kontrolü

Konuşmacı Doğrulama



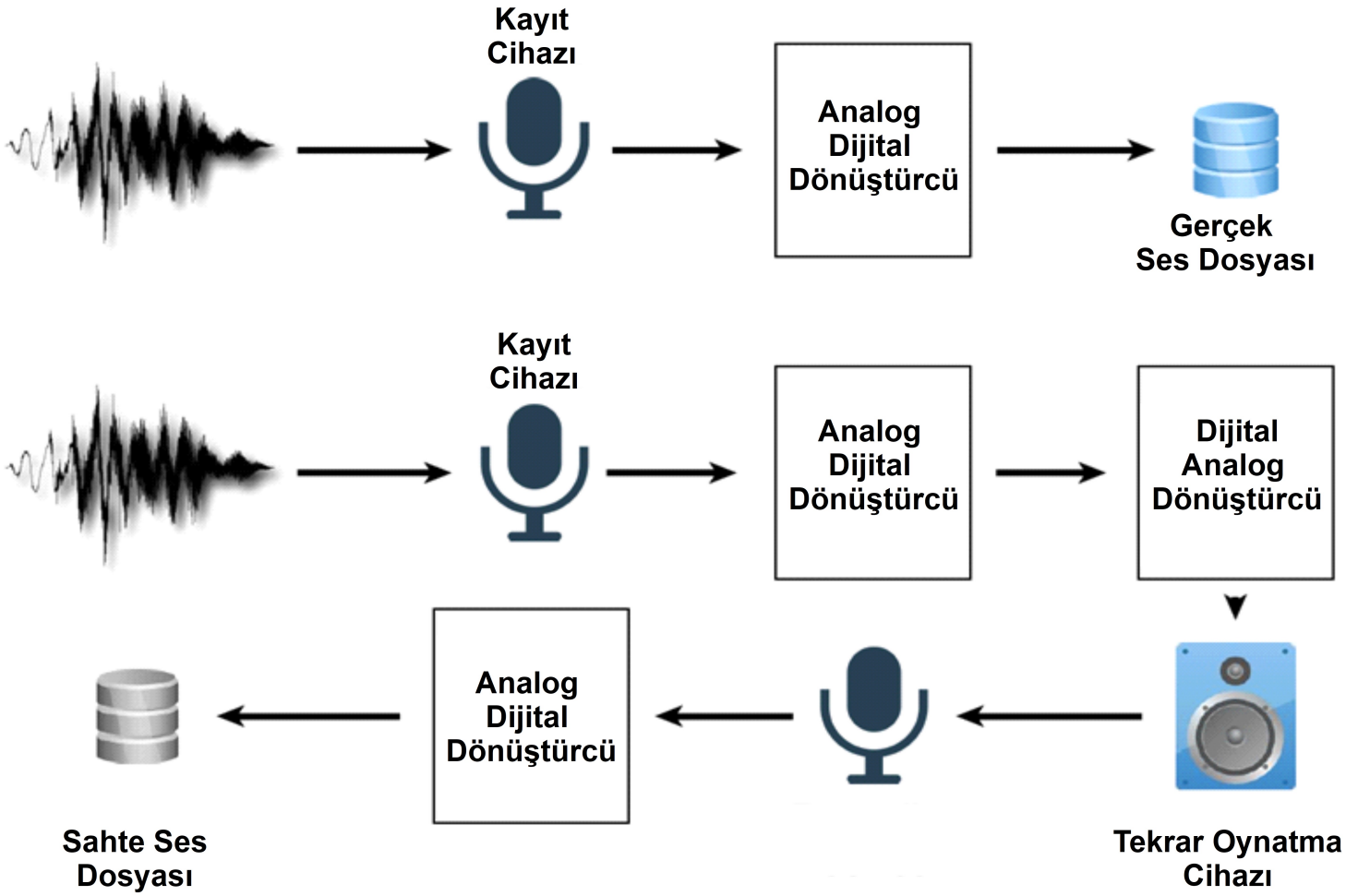
Yanıltma Saldırıları



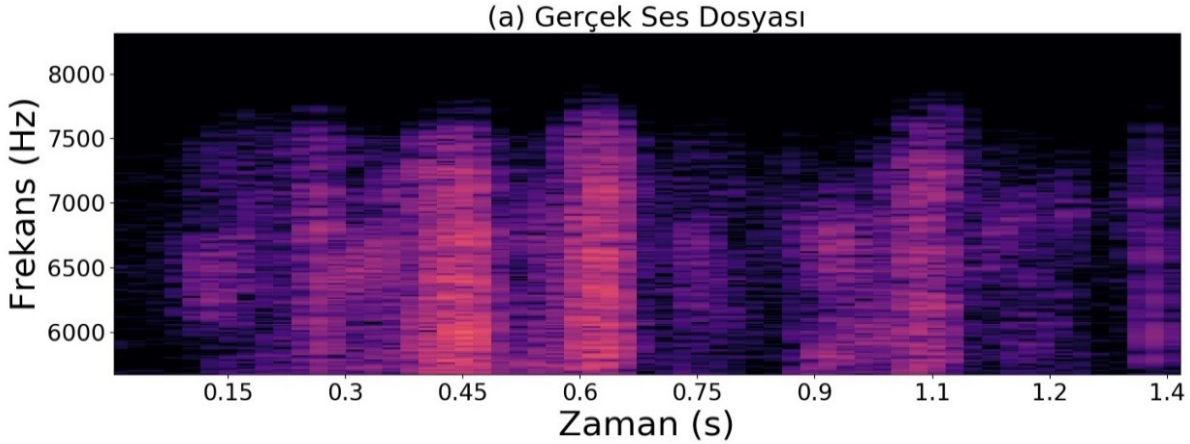
Yanıltma Saldırıları

- Ses Sentezleme
- Ses Dönüştürme
- Taklit
- Tekrar Oynatma

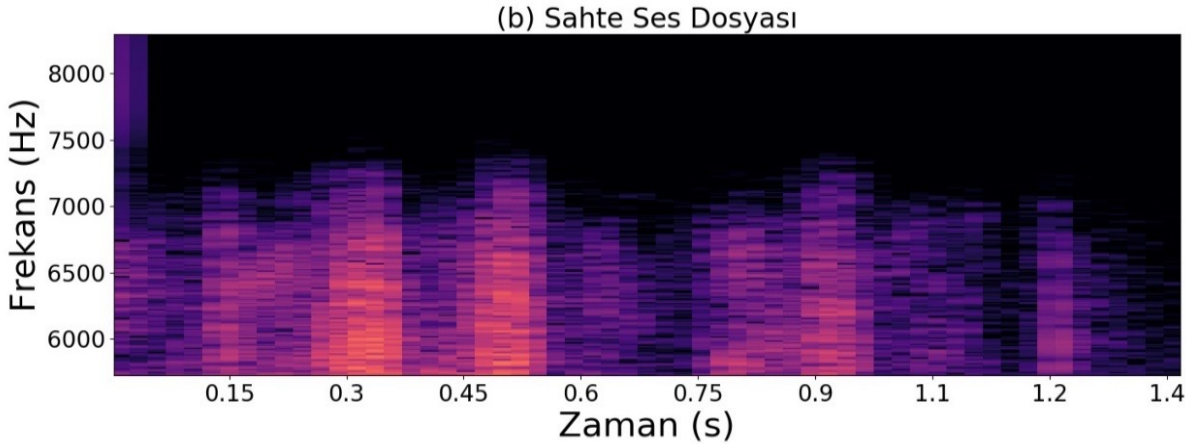
Yanıltma Saldırıları



Yanıltma Saldırıları



Gerçek Ses



Sahte Ses

Veri Tabanı

- Saldırı tespiti için yapılan çalışmaların karşılaştırılabilmesi ve karşı önlemlerin iyileştirilebilmesi için ortak bir veri tabanı gereklidir.

- ASVspoof 2015 yarışması düzenlenmiş ve yarışma ile aynı ismi taşıyan ASVspoof 2015 veri tabanı oluşturulmuştur.

- ASVspoof 2015'in devamında ASVspoof 2017 düzenlenmiştir.

Veri Tabanı

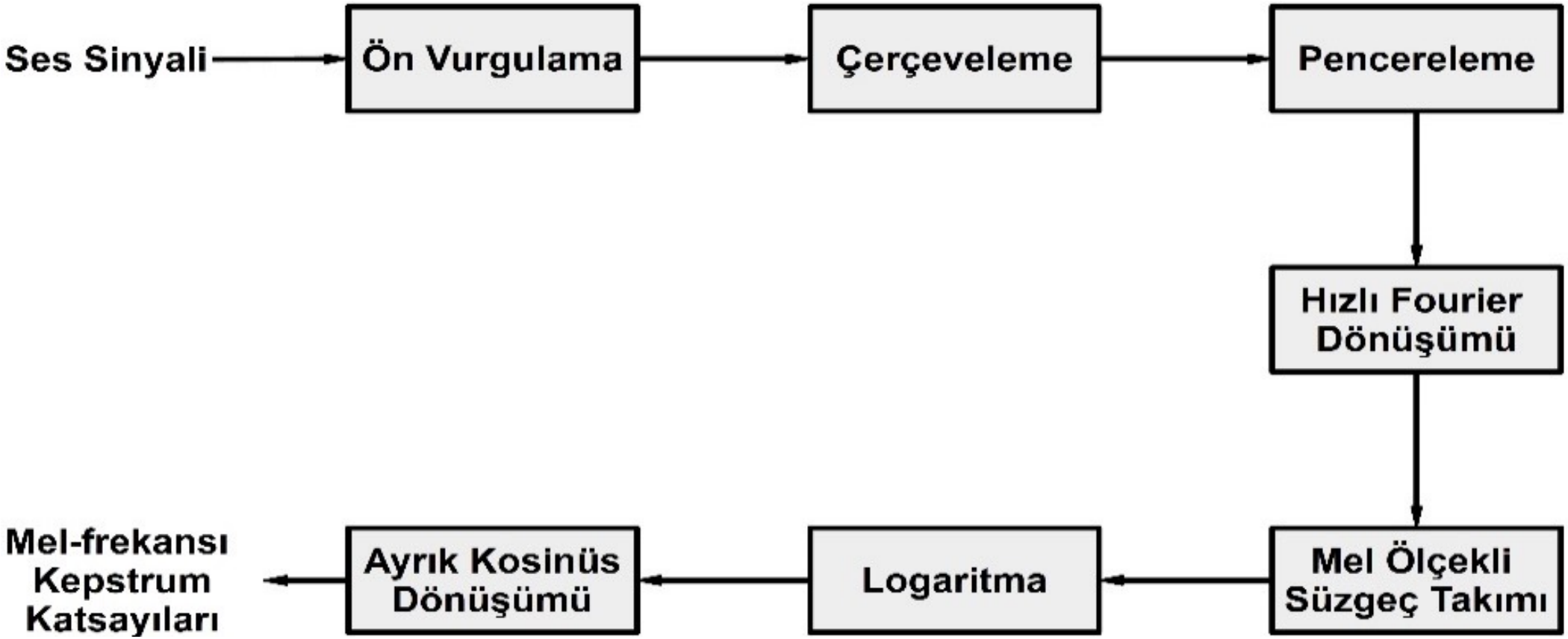
Alt Küme	Konuşmacı Sayısı	Gerçek Kayıt Sayısı	Sahte Kayıt Sayısı
Eğitim	10	1507	1507
Geliştirme	8	760	950
Değerlendirme	24	1298	12008

- 16 kHz örnekleme, 16 bit çözünürlük
- Alt kümelere ait protokol dosyaları

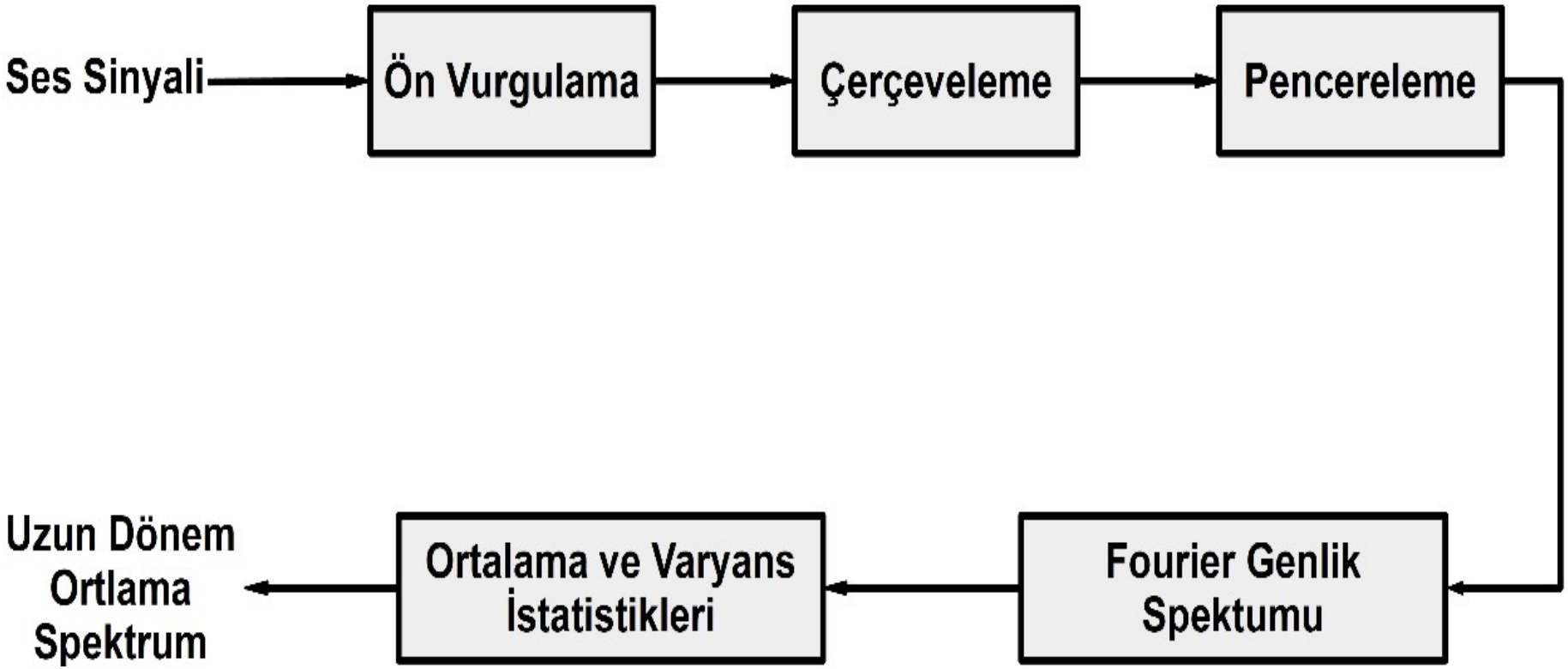
Öznitelikler

- Sabit Q Kepstrum Katsayıları (SQKK)
- Mel Frekansı Kepstrum Katsayıları (MFKK)
- Uzun Dönem Ortalama Spektrum (UDOS)

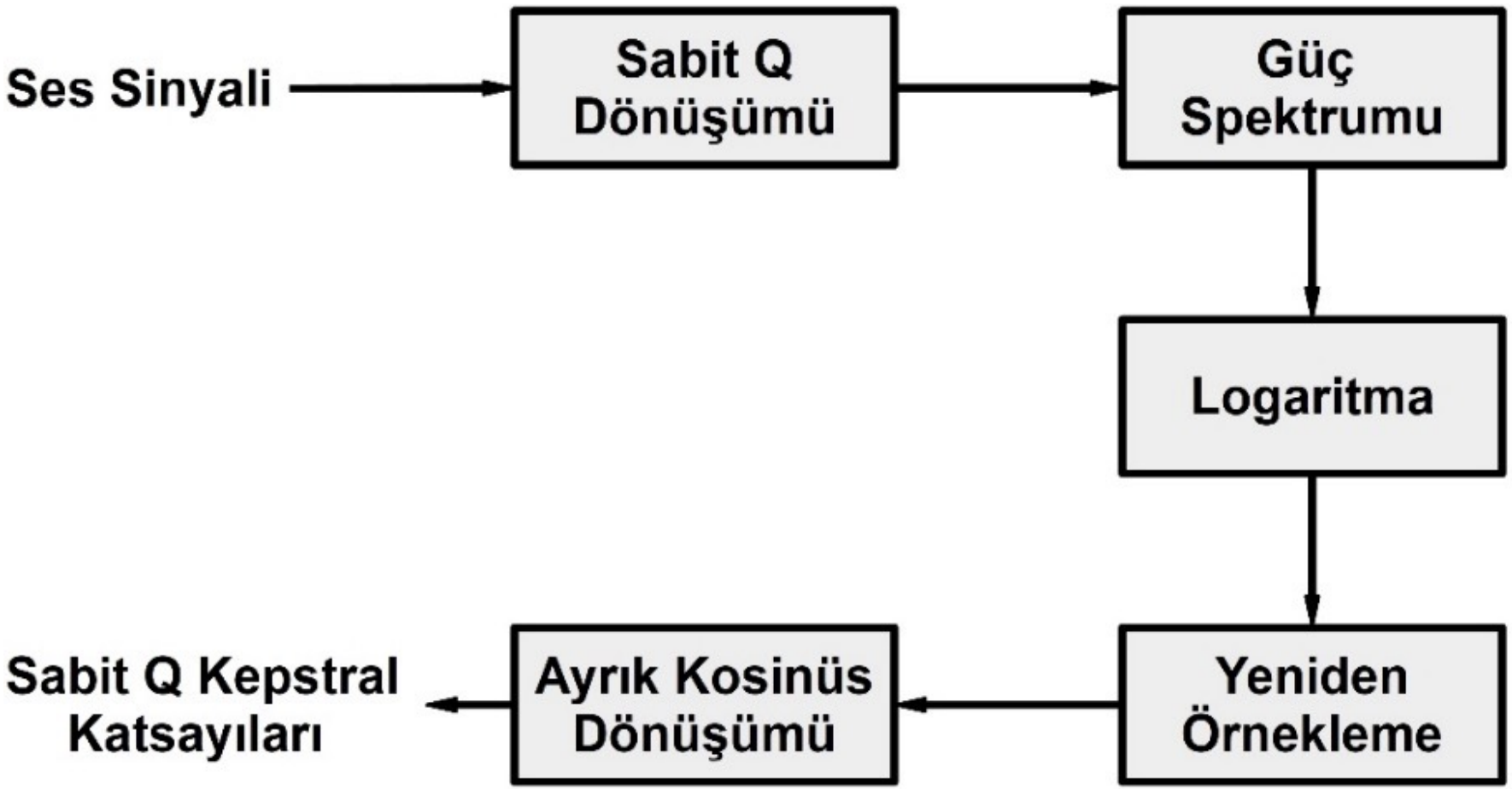
Öznitelikler-MFKK



Öznitelikler-UDOS



Öznitelikler-SQKK



Sınıflandırıcılar

- Gauss karışım modeli (GKM), konuşmacı doğrulama sistemlerinde kullanılan en eski ve en güvenilir sınıflandırıcılardan biri olarak bilinmektedir.

- Derin sinir ağları (DSA), son yıllarda kullanımı yaygınlaşan bir sınıflandırıcıdır.

Sınıflandırıcılar-GKM

- GKM, KD sistemlerinde kullanılan en eski ve en güvenilir sınıflandırıcılardan biri olarak bilinmektedir.

- GKM yönteminde, gerçek ve tekrar örüntü sınıfları M adet çok boyutlu Gauss yoğunluk fonksiyonunun ağırlıklandırıl- mış toplamı şeklinde ifade edilir:

$$p(x|\gamma) = \sum_{i=1}^{M} w_i p_i(x)$$

Sınıflandırıcılar-GKM

- GKM yönteminin eğitim aşamasında her bir sınıfın öznitelik vektörleri $X = \{x_1, x_2 \ldots, x_N\}$, eğitim öznitelikleri kullanılarak beklentinin maksimumlaştırılması algoritması ile GKM parametreleri tahmin edilir.

- Logaritmik olabilirlik oranı skoru şu şekilde hesaplanır:

$$LLR = log\left(Y|\lambda_{gerçek}\right) - log(Y|\lambda_{sahte})$$

Sınıflandırıcılar-DSA

- Derin öğrenme resim, ses, yazı gibi verilerin daha anlamlı hale getirilmesi ve yorumlanmasını hedefleyen çok katmanlı gösterim ve soyutlama algoritmasıdır.

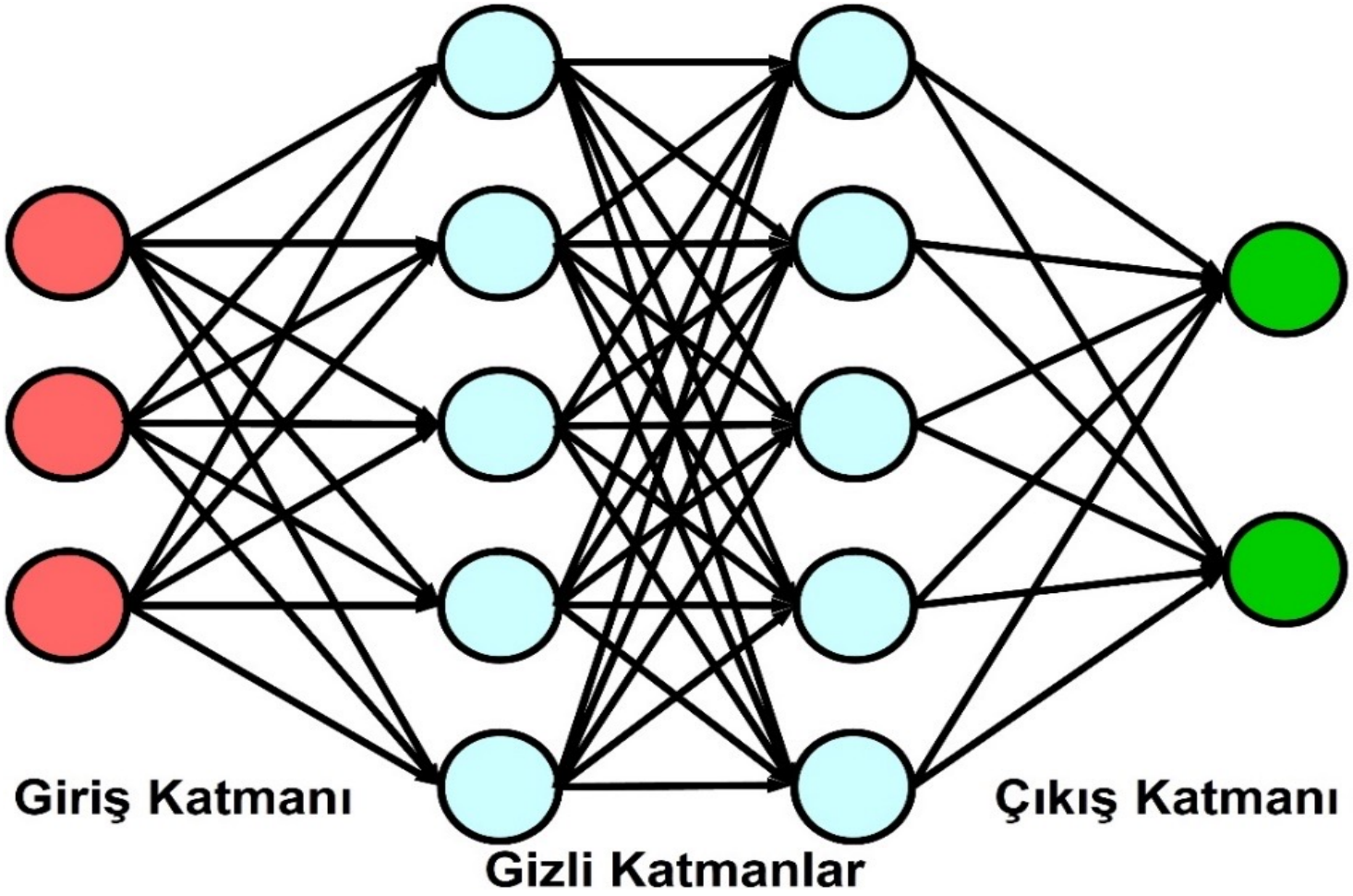
- Derin sinir ağları (DSA) öznitelik çıkarma veya daha önceden çıkarılmış özniteliklerin sınıflandırılmasında kullanılır.

- Derin öğrenme çalışmaları için geliştirilmiş yazılımlar, kütüphaneler ve donanımlar vardır.

Sınıflandırıcılar-DSA

- DSA çalışmalarında en çok kullanılan programlama dili Python'dur.
- DSA için geliştirilmiş bir çok kütüphane vardır (tensorflow, theano, caffe, keras).
- DSA çalışmalarında GPU kullanımı zorunludur.
- DSA çalışmalarında işlemci hızı ve RAM boyutu önemlidir.

Sınıflandırıcılar-DSA



Sınıflandırıcılar-DSA

- DSA çalışmalarında GPU kullanımı zorunludur, işlemci hızı ve RAM boyutu önemlidir.
- Batch training, over training, learning rate.
- Epoch, early stopping.
- Aktivasyon fonksionu (relu), optimizer (sgd).

Sınıflandırıcılar-DSA

- Çıkış nöronları, ilgili sınıfın sonsal olasılığını temsil eder.

- Sonsal olasılıklar, logaritmik olabilirlik oranı skoruna şu şekilde dönüştürülmüştür:

$$LLR = log(Y|\lambda_{gerçek}) - log(Y|\lambda_{sahte})$$

Performans Kriteri

- KD sistemlere yanlış kişinin reddedilmesi (yanlış ret) ve yanlış kişinin kabul edilmesi (yanlış kabul) şeklinde iki hata oluşabilir.

- $\text{Yanlış Kabul Oranı} = \frac{\text{Kabul Edilen Yanlış Sınama Sayısı}}{\text{Toplam Yanlış Sınama Sayısı}} \; X \; 100$

- $\text{Yanlış Red Oranı} = \frac{\text{Kabul Edilen Yanlış Red Sayısı}}{\text{Toplam Doğru Sınama Sayısı}} \; X \; 100$

Performans Kriteri-EHO

- Yanlış kabul ve yanlış ret oranlarına, uygulama türüne göre belirlenen eşik değere göre karar verilir.

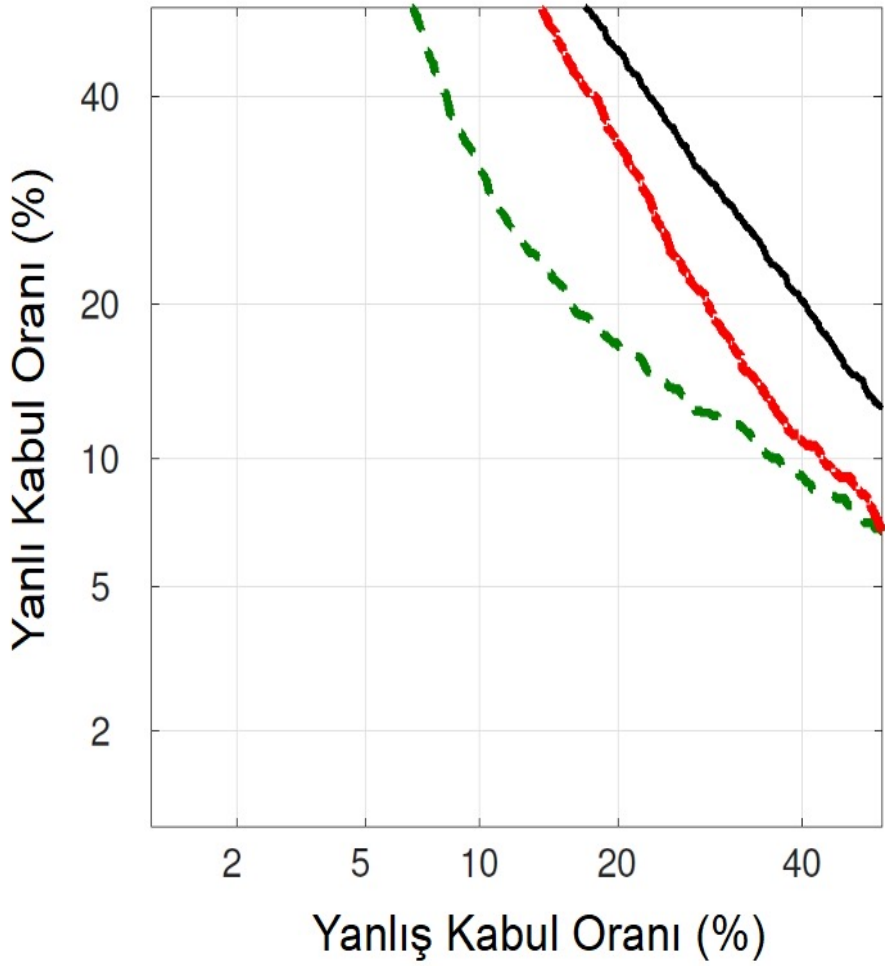
- Akademik çalışmalarda yanlış kabul oranının, yanlış ret oranına eşit olduğu değere denk gelen eşit hata oranı (EHO) yöntemi kullanılmaktadır.

- EHO'nun düşük olması, saldırı tespit sistemin başarısını gösterir.

Performans Kriteri-SHÖ

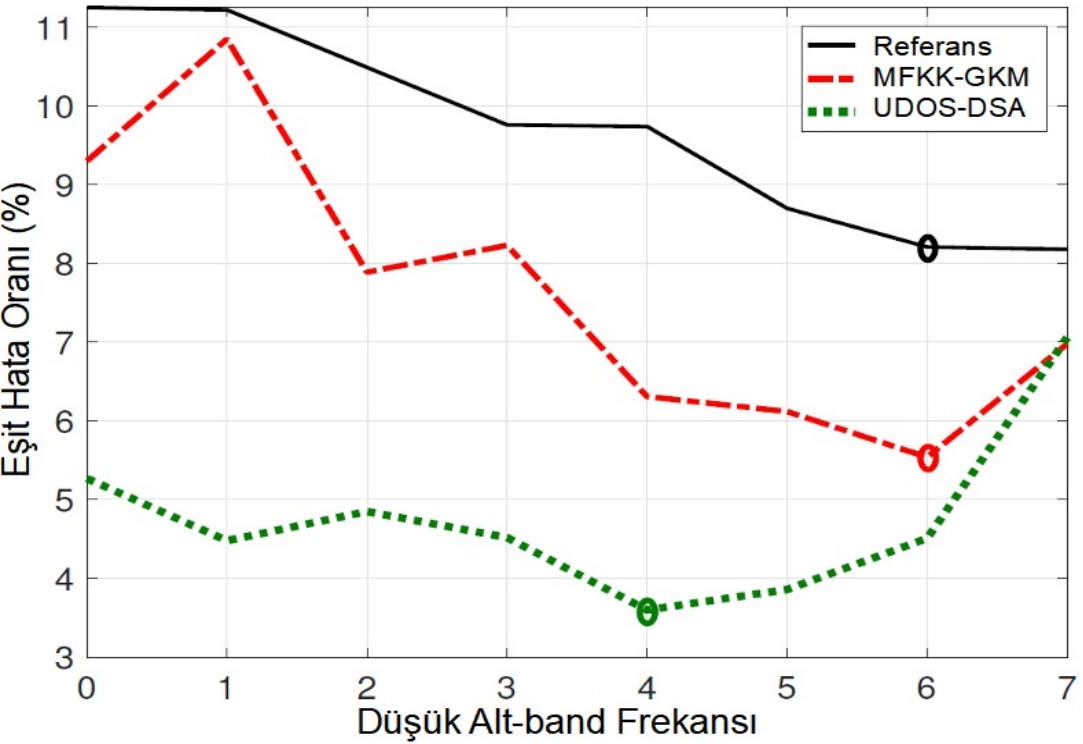
- Sezim hata ödünleşimi (SHÖ) eğrileri, her iki hata durumun birbirine göre değişimlerinin grafiksel olarak gösterilme yöntemidir .

- Bu eğrilerde yanlış kabul ve yanlış ret oranlarının birbirine eşit olduğu, siyah nokta ile vurgulanmış nokta EHO noktasıdır.



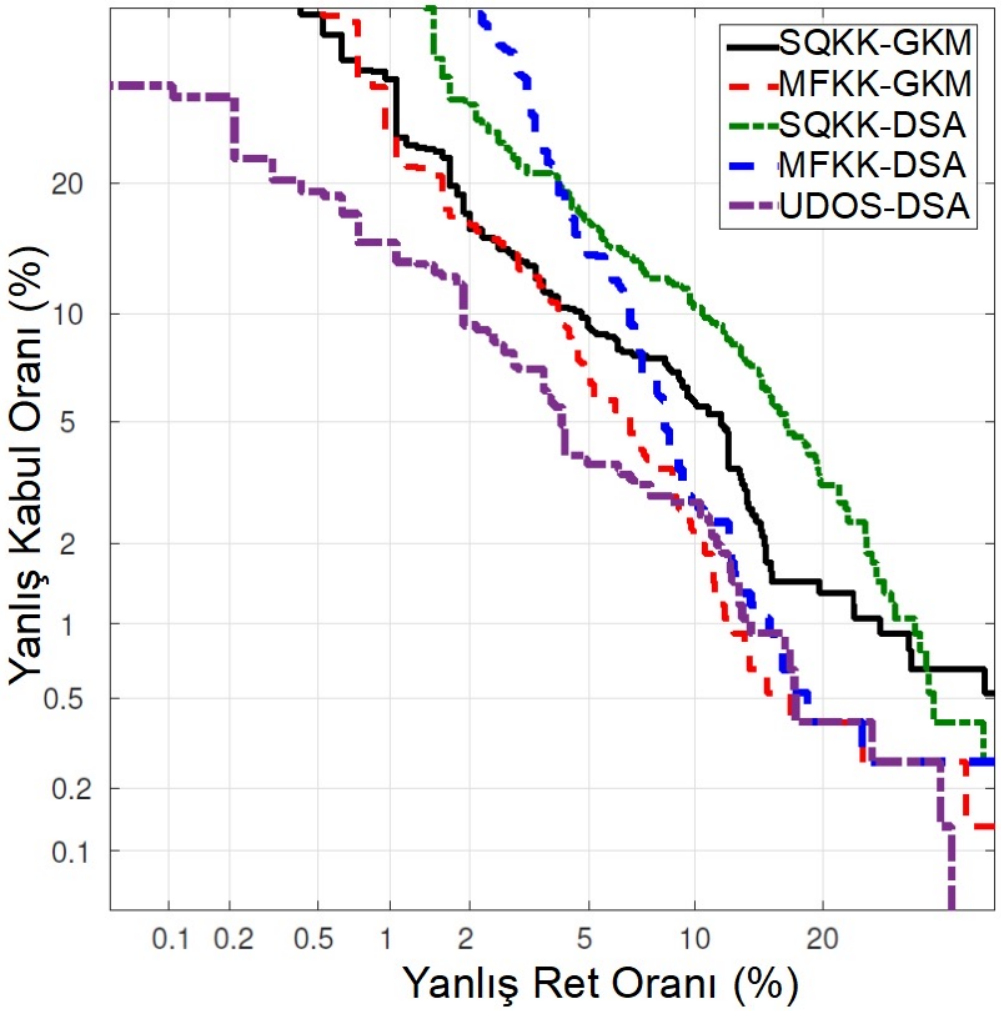
Geliştirme Kümesi Sonuçları

- İlk olarak frekans bölgesi analizi ve ortalama-varyans normalizasyonu işlemlerinin etkisi incelenmiştir.



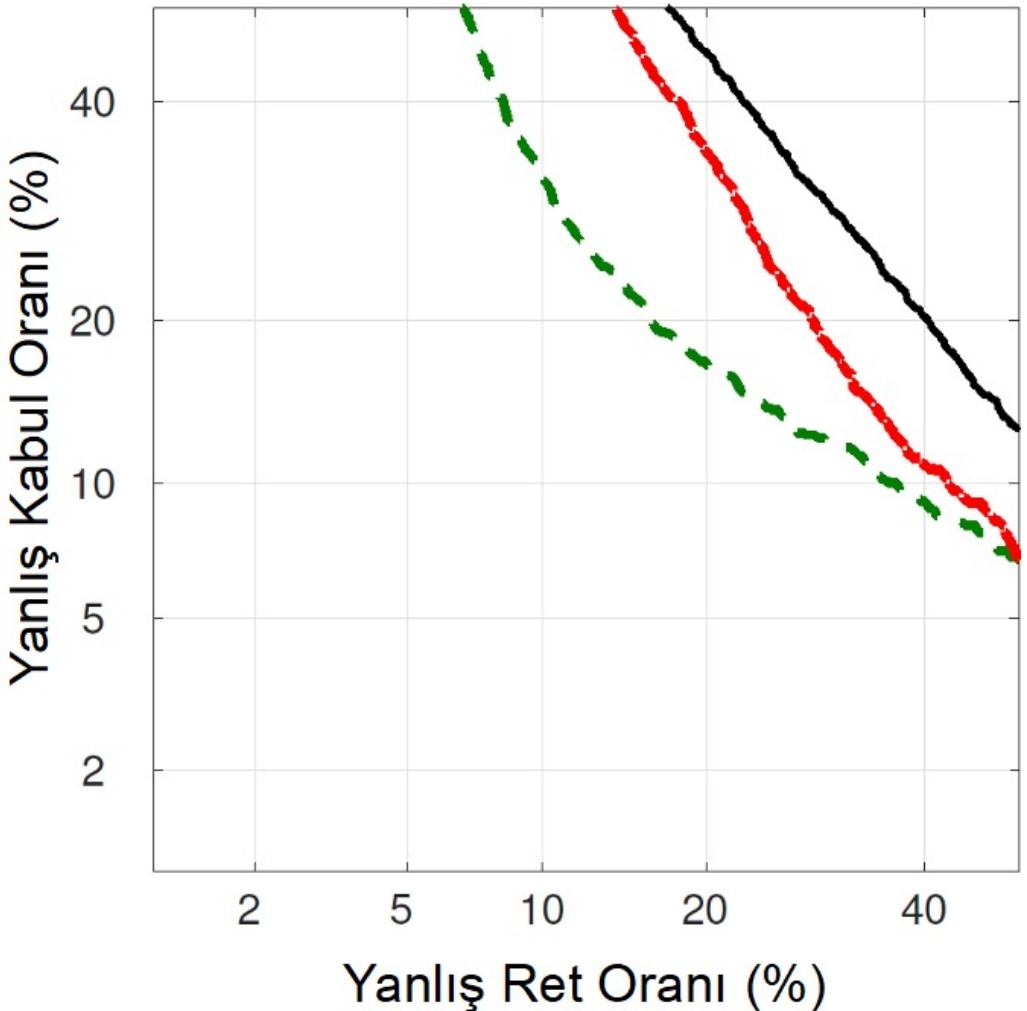
Sistem	EHO	EHO
SQKK-GKM	8.18	15.15
MFKK-GKM	5.54	13.40
SQKK-DSA	10.05	17.18
MFKK-DSA	6.64	12.51
LTAS-DSA	**4.10**	**6.05**

Geliştirme Kümesi Sonuçları



Sistem	EHO (%)
SQKK-GKM	8.18
MFKK-GKM	5.54
SQKK-DSA	10.05
MFKK-DSA	6.64
LTAS-DSA	**4.10**

Değerlendirme Kümesi Sonuçları



Sistem	EHO (%)
SQKK-GKM	29.94
MFKK-GKM	27.74
SQKK-DSA	32.64
MFKK-DSA	25.34
LTAS-DSA	**20.77**