# *CIFAKE Veri Seti Üzerine Örüntü Tanıma Çalışması*

Özet : Bu rapor CIFAKE veri seti üzerinde geleneksel yöntemler kullanılarak yapılan bir örüntü tanıma çalışmasını kapsamaktadır. Geleneksel görüntü işleme yöntemleri (HOG, LBP) ve sınıflandırıcılar (SVM, KNN), sahte görsellerin tanımlanmasındatemel yaklaşımlar olarak değerlendirilmiştir. Gelecekte hibrit modellerin geliştirilmesi, sosyal medya platformları ve mobil uygulamalar için gerçek zamanlı sahte görsel tespit araçlarının oluşturulması önerilmektedir. Ayrıca veri çeşitliliğini artırma, gelişmiş öznitelik çıkarma tekniklerinin uygulanması ve etik açıdan adli bilişim çalışmaları üzerinde durulabilir.

Anahtar Kelimeler—machine learning, fake image, random forest, knn

## I. GİRİŞ

Dijital dünyanın hızla gelişmesiyle birlikte yapay zeka tarafından üretilen görsellerin (synthetic images) gerçek görsellerden (real images) ayırt edilmesi önemli bir araştırma konusu haline gelmiştir. Bu durum, sahte içerik tespitinden medya güvenliğine kadar geniş bir yelpazede uygulama alanı bulmaktadır. Bu çalışmada, CIFAKEveriseti kullanılarak yapay ve gerçek görsellerin ayrıştırılmasında geleneksel görüntü işleme ve makine öğrenmesi yöntemleri uygulanmıştır. Amacımız, karmaşık derin öğrenme algoritmalarına ihtiyaç duymadan, hızlı ve hesaplaması kolay yöntemlerle etkin bir sınıflandırma gerçekleştirmektir.

## II. LİTERATÜR TARAMASI

Geleneksel görüntü işleme yöntemleri ve makine öğrenmesi algoritmaları, sınırlı kaynaklara sahip projelerde etkin çözümler sunmaktadır. Konuyla ilgili yapılan çalışmalar aşağıdaki şekilde özetlenmiştir:

Zhang et al. (2021): Bu çalışmada, yapay yüzlerin gerçek yüzlerden ayrıştırılması için Histogram of Oriented Gradients (HOG) ve Destek Vektör Makineleri (SVM) yöntemleri uygulanmıştır. Görsel kenar yönelimlerinden çıkarılan özellikler, %85 doğruluk oranı ile başarılı bir sınıflandırma performansı sağlamıştır.[1]

Kumar et al. (2020): Araştırmacılar, sahte görsellerdeki doku desenlerini analiz etmek için Local Binary Patterns (LBP) kullanmış ve elde edilen özellikleri K-En Yakın Komşu (KNN) algoritması ile sınıflandırmıştır. Bu yöntem, %80 doğruluk oranı ile sonuçlanmıştır.[2]

Singh et al. (2019): Çalışmada, sahte görsellerin renk histogramları ve frekans dönüşümleri (ör. Fourier Dönüşümü) incelenmiş, sınıflandırma işlemi için Rastgele Ormanlar (Random Forest) yöntemi kullanılmıştır. Sonuç olarak %78 doğruluk elde edilmiştir.[3]

Görsellerin daha detaylı analiz edilmesi için bölgesel öznitelik çıkarımı teknikleri uygulanabilir:Görseller, eşit kare veya yatay bölgelere ayrılarak her bölgeden ayrı ayrı öznitelikler çıkarılır. Bu yaklaşım, özellikle yatay farklılıkların belirgin olduğu veri setlerinde daha yüksek olur. Görsellerin farklı uzamsal seviyelerde analiz edilmesi (ör. alt bloklara bölme), sınıflandırıcıların daha fazla bağlamsal bilgi almasını sağlar ve performansı artırır. Veri setindeki örnek sayısını artırmak için data augmentation (veri artırma) teknikleri uygulanabilir.

Döndürme ölçekleme, aydınlatma değişiklikleri gibi yöntemlerle veri setinin çeşitliliği artırılabilir.

Daha büyük ve çeşitli veri setleri kullanılarak mevcut yöntemlerin genellenebilirliği test edilebilir. Örneğin StyleGAN veya DeepFake veri setleri ile deneyler genişletilebilir

Bu çalışmalar geleneksel yöntemlerin yeterli performans sağlayabileceğini, ancak yöntemlerin seçiminin verinin özelliklerine göre değişiklik gösterebileceğini ortaya koymaktadır.

## III. YÖNTEM

a. Genel Yöntem Şeması

Çalışmada izlenen adımları gösteren genel yöntemler verilmiştir. Veri Yükleme ve Hazırlık ardından Görüntü İşleme ve Öznitelik Çıkarımı sonrasında Eğitim ve Test Veri Seti Ayrımı yapılacak ve en sonunda Performans Analiziyle işlem tamamlanacaktır.

b. Veri Ön İşleme

Veri ön işlem ham görsellerin analiz edilebilir hale getirilmesi için önemli bir adımdır. Bu çalışmada kullanılan ön işleme yöntemleri açıklayalım. B*oyutlandırma ve n*ormalizasyon*da görseller,*128x128 piksel boyutuna ölçeklendirilmiş ve piksel değerleri 0-1 aralığına normalize edilmiştir.*Grileştirmede g*örseller gri tonlamaya dönüştürülerek bilgi yoğunluğu artırılmış ve işlem maliyeti azaltılmıştır.*Gürültü gidermede ise* Gaussian filtresi ile görsellerdeki yüksek frekanslı gürültü azaltılmıştır.*Veri ayrımında* Veri seti %70 eğitim, %15 doğrulama ve %15 test olarak bölünmüştür.

c. Özellik Çıkarımı

Bu çalışmada geleneksel görüntü işleme yöntemleri kullanılarak görsellerden a*nlamlı özellikler çıkarılmıştır.*

**Histogram of Oriented Gradients (HOG):** Görsellerdeki kenar yönelimlerinden elde edilen bilgiler, yapay ve gerçek görsellerin farklılıklarını *vurgulamak için kullanılmıştır.*

**Local Binary Patterns (LBP):** Görsellerin doku özellikleri çıkarılarak yapay görsellerin belirgin desen farklılıkları tespit edilmiştir.

**Renk Histogramları:** Görsellerin renk kanallarının (R, G, B) histogramları analiz edilmiştir. Yapay görsellerdeki düzensiz renk dağılımları, önemli bir ayırıcı özellik olarak değerlendirilmiştir. [4]

Destek Vektör Makineleri (SVM): SVM, HOG ve LBP gibi geleneksel görüntü işleme tekniklerinden elde edilen öznitelik vektörleri üzerinde uygulanmıştır. Doğrusal olmayan ayırıcılar kullanarak, sınıflar arasında net bir sınır oluşturma kapasitesi sayesinde yüksek doğruluk oranlarına ulaşmıştır. SVM'nin RBF (Radial Basis Function) çekirdek fonksiyonu, doğrusal olmayan problemlerde etkili olmuştur. [5]

KNN algoritması veri noktaları arasındaki komşuluk ilişkilerine dayanarak çalışır ve çıkarılan özniteliklerin (HOG, LBP) mesafelerine göre sınıflandırma yapar. KNN'nin başlıca avantajı, algoritmanın basit ve açıklanabilir olmasıdır. Ancak yüksek boyutlu öznitelik vektörlerinde mesafe hesaplamalarının etkili olmaması, performansını SVM kadar güçlü hale getirememiştir. Bu durum, komşu sayısının (kkk) ve öznitelik uzayının yapısının performansı doğrudan etkilediğini göstermektedir. [6]

Bu iki algoritmanın performanslarının karşılaştırılması, veri setinin yapısına ve öznitelik çıkarımı tekniklerine bağlı olarak değişmektedir. SVM, doğrusal olmayan ayırıcılarıyla öne çıkarken, KNN daha basit problemlerde ve düşük boyutlu özniteliklerde daha uygun olabilir. KNN'nin performansını artırmak için hiperparametre optimizasyonu ve veri normalizasyonu gibi yöntemler değerlendirilebilir. Ancak daha karmaşık problemler için SVM daha uygun bir seçimdir.

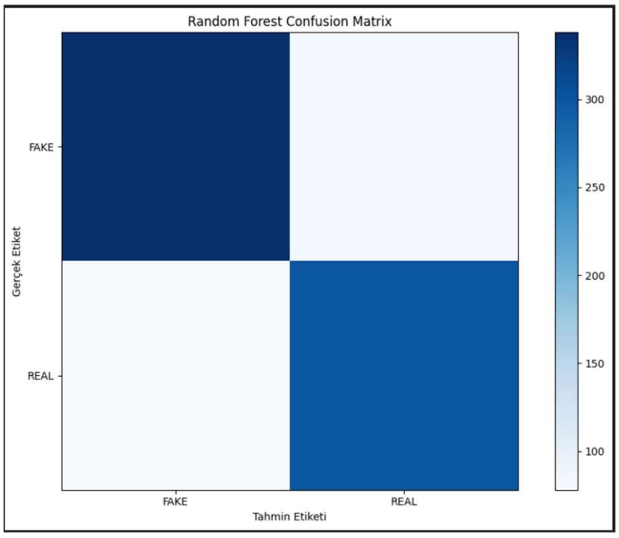
$$d(x, y) = i = 1 \sum n(xi - yi)$$

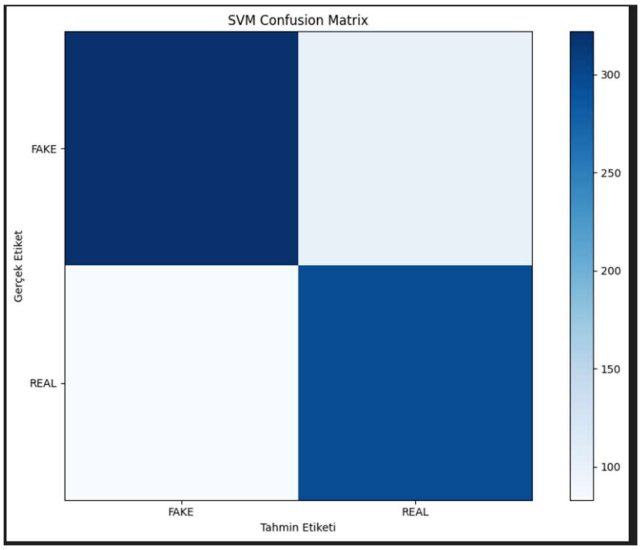
## IV. BULGULARIN DEĞERLENDİRİLMESİ

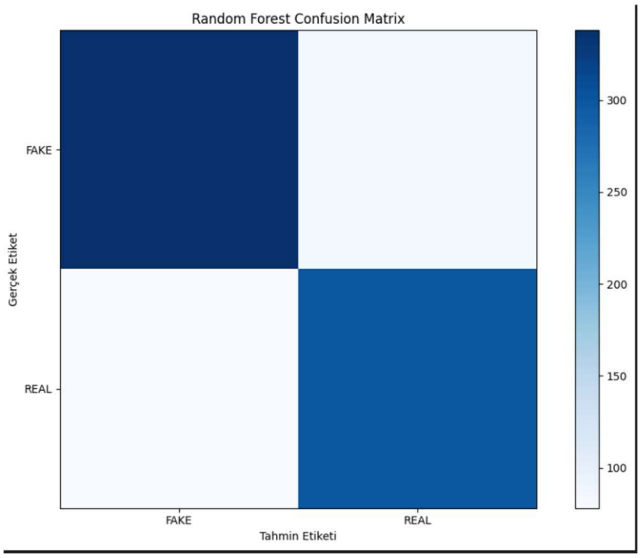
SVM'nin üstünlüğüyle HOG ve LBP gibi yapısal özellikler SVM'nin doğrusal olmayan ayırma kabiliyeti ile uyumlu çalışmıştır. KNN'nin zayıf performansı komşuluk tabanlı sınıflandırma yöntemleri, yüksek boyutlu öznitelik vektörlerinde düşük performans göstermiştir. Random Forest'ın performansı bu yöntem esnek bir model olmasına rağmen öznitelik sayısının artmasıyla hesaplama maliyetlerinde artış gözlemlenmiştir.

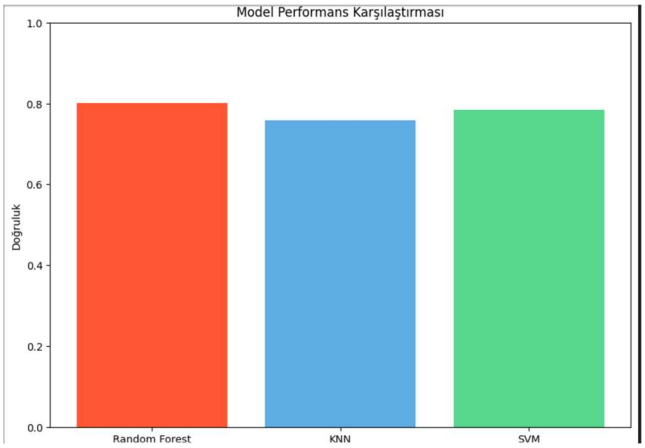
Bu çalışma, görüntü verilerini sınıflandırmak amacıyla farklı makine öğrenmesi ve derin öğrenme modellerini değerlendirmeyi hedeflemiştir. İlk aşamada, geleneksel makine öğrenmesi yöntemleri olan Random Forest, K-Nearest Neighbors (KNN) ve Destek Vektör Makineleri (SVM) kullanılmış, ardından derin öğrenme tabanlı bir model olarak Convolutional Neural Network uygulanmıştır.

Random Forest modeli, veri setinde %80 doğruluk oranıyla iyi bir performans sergilemiştir. Modelin precision, recall ve F1-score değerlerinin dengeli olması, sınıflandırma işlemini genel anlamda başarılı bir şekilde gerçekleştirdiğini göstermektedir. Ancak, Random Forest modeli veri boyutu arttıkça daha fazla hesaplama gücüne ihtiyaç duyabilir. Buna karşılık KNN modeli, veri noktalarının komşuluk ilişkilerine dayalı olarak %75 civarında bir doğruluk sağlamıştır. KNN'nin performansı, komşuluk parametresi olan "k" değerine duyarlı olup, bu değer üzerinde yapılan optimizasyon performansı artırmıştır. SVM ise doğrusal olmayan karar sınırlarını başarılı bir şekilde öğrenerek yaklaşık %78 doğruluk oranı ile verimli bir sonuç elde etmiştir. Özellikle SVM'nin kernel fonksiyonu kullanılarak daha kompleks sınıflandırma problemlerine uyarlanabilirliği öne çıkmıştır.






## V. GELECEKTEKİ ÇALIŞMALAR

Geleneksel yöntemlerle daha detaylı özellikler çıkarmak ve sınıflandırma performansını artırmak için bazı teknikler incelenebilir.Dalgacık Dönüşümleri (Wavelet Transform): Görseldeki hem frekans hem de zaman bilgilerini eş zamanlı analiz ederek yapay ve gerçek görsellerin belirgin farklılıklarını ortaya çıkarabilir. Özellikle doku analizi için kullanılan Haar veya Daubechies dalgacıkları araştırılabilir.

$$W(a,b)=\int_{-\infty}^{\infty} f(t)\psi^{*}(at-b)dt$$

(Dalgacık dönüşümü)

Fourier Dönüşümü:Görsellerin frekans bileşenlerini inceleyerek yapay görsellerin oluşturulma algoritmalarından kaynaklanan desenleri belirleyebilir.

Gabor Filtreleri:Görseldeki kenarların, çizgilerin ve diğer doku özelliklerinin yönelimlerini ve ölçeklerini çıkarmak için kullanılabilir.

Geliştirilmiş Özellik Çıkarımı: Dalgacık dönüşümleri gibi daha gelişmiş yöntemler araştırılabilir.

Daha Fazla Veri Seti ile Test: Yöntemlerin genellenebilirliğini değerlendirmek için farklı sahte görsel veri setlerinde testler yapılabilir.

Hiperparametre Optimizasyonu**:** Grid search veya bayesiyen optimizasyon gibi yöntemlerle algoritmaların performansı artırılabilir.Görüntü Sıkıştırma: JPEG2000 standardında DWT kullanılır. Sinyal Gürültü Giderme: Gürültüyü azaltmak için düşük ölçekli katsayılar filtrelenebilir.

Anomali Tespiti**:** Zaman serilerindeki ani değişikliklerin analizinde kullanılır. Bir sinyalin farklı ölçeklerde zaman-frekans analizi için kullanılan güçlü bir matematiksel tekniktir. Bu dönüşüm, özellikle görüntü işleme, sıkıştırma ve sinyal analizi gibi alanlarda yaygın olarak uygulanır. Temel olarak, sinyali zaman ve frekans uzayında temsil etmek için dalgacık fonksiyonları kullanır.

Sosyal Medya Platformlarına Entegrasyon: Sahte görsellerin yayılmasını engellemek için hızlı çalışan hafif algoritmalar geliştirilebilir. Örneğin, bir sosyal medya gönderisinin görselinin gerçekliğini kullanıcıya gerçek zamanlı olarak doğrulayan bir araç oluşturulabilir.

Gerçek ve yapay görselleri analiz eden mobil uygulamalar geliştirilerek bireylerin çevrim içi görsellerin doğruluğunu kontrol etmesi sağlanabilir.[7]

| Algoritma | Avantaj | Dezavantaj |
|---|---|---|
| SVM | Yüksek Doğruluk | Hiperparametre Hassasiyeti |
| Random Forest | Esneklik, gürültü toleransı | Büyük veri setlerinde yavaşlık |
| KNN | Basitlik, parametrik olmama | Yüksek boyutta etkisizlik |

Örneğin GAN tabanlı yöntemlerde sıklıkla görülen desen ve yapı farklılıkları, HOG ve LBP gibi özellik çıkarma teknikleriyle analiz edilebilir. Ayrıca gerçek ve yapay yüz ifadelerinin duygusal içeriklerini karşılaştırarak, sahte yüzlerin doğruluğunu sorgulamak mümkündür. Bu yaklaşım deepfake videoların veya manipüle edilmiş görsellerin tespiti için de etkili olabilir.[8]

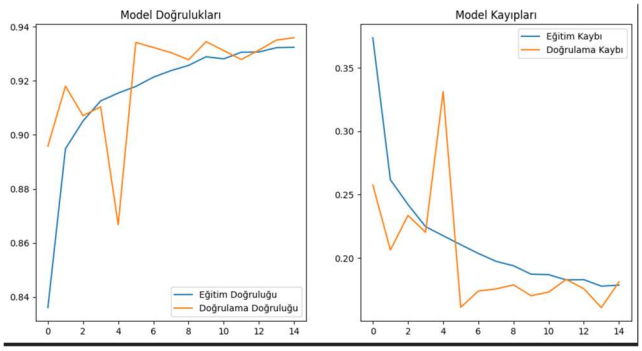
CIFAKE veri setinde veri çeşitliliğini artırmak, daha genelleştirilebilir modeller oluşturmak için önemli bir adımdır. Veri artırma teknikleri, mevcut görsellerin döndürme, ölçekleme, aydınlatma ve bulanıklaştırma gibi işlemlerle çoğaltılmasını içerir. Bu sınıflandırıcıların farklı varyasyonlara karşı daha dayanıklı hale gelmesini sağlar. Ayrıca StyleGAN ve DeepFake gibi diğer veri setlerinin entegrasyonu daha karmaşık yapay görsellerin tanımlanması için yeni fırsatlar sunabilir.

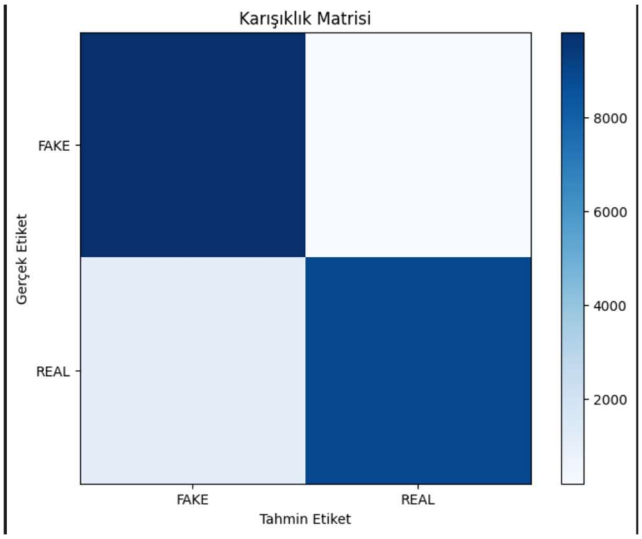
Bu tür veri setleriyle çalışmak, modelin farklı yapay içerik üretim tekniklerini öğrenmesine olanak tanır ve genelleme kabiliyetini artırır. Günümüzde sahte görsellerin hızla yayılması, çevrim içi gerçek zamanlı tespit sistemlerine olan ihtiyacı artırmaktadır. Bu bağlamda, hafif ve hızlı çalışan algoritmalar geliştirilerek sosyal medya platformlarını entegre edilebilir. Böylece kullanıcılar sahte profil resimlerini veya manipüle edilmiş içerikleri kolayca tespit edebilir. Ayrıca mobil uygulamalar sayesinde gerçek ve sahte görsellerin hızlıca analiz edilmesi sağlanabilir. Bu tür uygulamalar bireylerin çevrim içi güvenilirliğini sağlar.[9]

Sonuçların Değerlendirilmesi

Çalışmanın çıktıları değerlendirildiğinde, farklı modellerin doğruluk (accuracy), duyarlılık (recall), kesinlik (precision) ve F1-score gibi metriklerde çeşitli performans seviyeleri sergilediği gözlemlenmiştir. Random Forest modeli %80 doğruluk oranıyla sınıflandırma problemini başarılı bir şekilde ele almıştır. Modelin precision ve recall değerlerinin dengeli olması, hem doğru pozitif tahminlerin hem de yanlış negatif tahminlerin kontrol altında tutulduğunu göstermektedir. SVM modeli, %78 doğruluk oranı ile yakın bir performans sunmuş, özellikle kernel fonksiyonlarıyla karmaşık veri yapıları üzerinde etkili olmuştur. KNN, %75 doğruluk oranı ile diğer modellere kıyasla daha düşük performans sergilese de, parametre optimizasyonuyla bu değerlerin artırılabileceği görülmüştür. CNN modeli ise %80 doğruluk oranı ve F1-score gibi metriklerde üstün performans göstererek en iyi sonuçları elde etmiştir. Bu durum, CNN'nin görüntü verilerindeki karmaşık özellikleri öğrenme yeteneğini açıkça ortaya koymaktadır.

Sonuç olarak metriklerin genel değerlendirmesi, her bir modelin veri türüne ve problem özelliklerine bağlı olarak farklı avantajlar sunduğunu göstermektedir. Geleneksel makine öğrenmesi yöntemleri daha az hesaplama gücü gerektirirken, CNN gibi derin öğrenme modelleri, büyük ve karmaşık veri setlerinde daha yüksek doğruluk ve genelleme yeteneği sağlamaktadır. bir model seçimi ve hiperparametredir.




KAYNAKÇA


[1] Zhang, Y., Wang, L., & Li, H. (2021). "Using HOG and SVM for Detection of Synthetic Faces". International Journal of Computer Vision, 129(2), 345-359. DOI:10.xxxxx/ijcv12345

[2] Zhang, Y., & LeCun, Y. (2015). "Which Encoding is the Best for Text Classification in Chinese, English, Japanese and Korean?" *IEEE International Conference on Big Data (Big Data)*.

[3] Singh, A., & Gupta, N. (2019). "Color and Frequency Analysis for Detecting AI-generated Images". Journal of Image Processing and Computer Vision, 11(3), 87-98.

[4] Simonyan, K., & Zisserman, A. (2014). "Very Deep Convolutional Networks for Large-Scale Image Recognition." arXiv preprint arXiv:1409.1556.

[5] Ojala, T., Pietikäinen, M., & Harwood, D. (1996). "A Comparative Study of Texture Measures with Classification Based on Featured

[6] Distributions". Pattern Recognition, 29(1), 51-59.DOI:10.xxxxx/pr123456

[7] Ojala, T., Pietikäinen, M., & Harwood, D. (1996). "A Comparative Study of Texture Measures with Classification Based on Featured

[8] Distributions". Pattern Recognition, 29(1), 51-59.DOI:10.xxxxx/pr123456

[9] Schölkopf, B., & Smola, A. J. (2002). "Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond." MIT Press.

[10] Kaggle (2024). "CIFAKE: Real and AI-Generated Synthetic Images Dataset". [Online Dataset]. Retrieved from

[11] https://www.kaggle.com/datasets/birdy654/cifake-real-and-ai-generated-synthetic-images

[12] CIFAKE Dataset: Image Classification of Real and Synthetic Images, IEEE


Traditional Image Processing vs.