Journal of the Faculty of Engineering and Architecture of Gazi University 40:1 (2025) 443-453

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Investigation of steganalysis performance of selected steganography methods with deep learning models

Ercan Buluş*
Department of Computer Engineering, Corlu Faculty of Engineering, Tekirdağ Namık Kemal University, 59860, Tekirdağ, Türkiye

Highlights:

- Steganography
- Artificial Intelligence
- Convolutional Network

Keywords:

- Image Steganography
- Image Steganalysis
- Data Hiding
- Deep Learning Networks
- Cryptography

Article Info:

Research Article
Received: 09.07.2023
Accepted: 08.04.2024

DOI:

10.17341/gazimmfd.1324765

Correspondence:

Author: Ercan Buluş
e-mail:
ercanbulus@nku.edu.tr
phone: +90 282 250 2328

Graphical/Tabular Abstract

In this study, 0.2 bpp and 0.4 bpp data were loaded into BOSSBase 1.01 and BOWS 2 image set mixtures using HILL, MiPOD, S-UNIWARD and WOW steganography methods. The data sets were trained with VGG16, Xu-Net, Ye-Net and Yeroudj-Net Deep learning models. The test accuracy rates of the results obtained with the test data sets are as in Table 1 below.

Table 1. Test Accuracy in stego-images

	VGG16	XUNET		YENET		YEDROUDJ	
Model	*0,4bpp*	0,2bpp	*0,4bpp*	0,2bpp	*0,4bpp*	0,2bpp	*0,4bpp*
WOW	*0,864*	0,694	*0,809*	0,695	*0,814*	0,668	*0,828*
S-UNI	*0,847*	0,693	*0,797*	0,647	*0,79*	0,627	*0,815*
HILL	*0,77*	0,693	*0,725*	0,636	*0,764*	0,578	*0,79*
MIPOD	*0,765*	0,623	*0,723*	0,626	*0,729*	0,5	*0,757*

Purpose:
It is to research whether steganalysis can be done with deep learning methods.

Theory and Methods:
10,000 BOWS 2 and 4,000 BOSSBase 1.01 pairs were used for training, 1,000 BOSSBase 1.01 pairs for validation, and 5,000 BOSSBase 1.01 pairs for testing. HILL, MiPOD, S-UNIWARD and WOW steganography methods were used to information hiding. Steganalysis was performed with VGG16, Xu-Net, Ye-Net and Yeroudj-Net Deep learning models.

Results:
At 0.2 bpp load there is not much difference between the results and not quite as expected. The best result in wow at 0.4 payload was obtained with the VGG16 (86.4%) method. However, VGG16 test times are twice as long compared to others. In this case, the Yedroudj method seems more suitable in terms of accuracy rate and processing time.

Conclusion:
When the test accuracy results for 0.2bpp load are examined in the study; It is seen that the lowest result is 50% (0.500) in the YEDROUDJ model with the MIPOD method, and the most efficient result is 69% (0.69) in the XU-net model for all methods. Since acceptable results could not be achieved with the VGG16 model under 0.2bpp load, it was not evaluated. In this case, the Xu-net model can be preferred to investigate whether information is hidden in images with a low amount of information such as 0.2bpp. Again, when the test accuracy results for 0.4bpp load are examined in the study; It is seen that the lowest result is obtained with the Xu-net model in the MIPOD method with 72% (0.72) and again with the Ye-Net model in the MIPOD method with 72% (0.72). On the other hand, the highest result was obtained with the VGG16 model in the WOW method with 86% (0.864) and with the VGG16 model with 84% (0.847). However, when the processing times in Table 11 are examined, it is clear that the processing time of the examinations made with the VGG16 model is almost twice as long as the others, and this is a very undesirable situation. In this case, the Yedroudj method is seen as a more useful method since it has the second best accuracy rate between 75%-82% with 0.4bpp load and a lower processing time (half) than VGG16.

Journal of the Faculty of Engineering and Architecture of Gazi University 40:1 (2025) 443-453

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Seçilen steganografi yöntemlerinin derin öğrenme modelleri ile steganaliz performansının incelenmesi

Ercan Buluş *
Tekirdağ Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 59860, Tekirdağ, Türkiye

Ö N E Ç I K A N L A R

- İçine bilgi saklı resimlerin tespiti
- Derin öğrenme metotları ile steganaliz
- Yapay zeka yöntemlerinin kriptolojide kullanımı

Makale Bilgileri
Araştırma Makalesi
Geliş: 09.07.2023
Kabul: 08.04.2024

DOI:
10.17341/gazimmfd.1324765

Anahtar Kelimeler:
Görüntü steganografisi, görüntü steganalizi, veri gizleme, derin öğrenme, ağları, kriptografi,

ÖZ

Görünüşte zararsız dijital ortamlarda bilgi gizleme sanatı olan steganografi, bilgi güvenliği için önemli bir sorun teşkil etmektedir. Son yıllarda, derin öğrenme teknikleri, çeşitli bilgisayarla görme görevleri için güçlü araçlar olarak ortaya çıkmıştır. Bu makale, derin öğrenme tabanlı steganalizdeki en son teknolojinin kapsamlı bir incelemesini sunmakta olup, dijital ortamdan gizli bilgilerin tespit edilmesine odaklanmaktadır. Çalışmada steganografik kavramlar ve sonuçları araştırılmış, ardından steganalizde kullanılan farklı derin öğrenme mimarileri ve metodolojileri incelenilmiştir. 0,2 bpp veri yükündeki test verileri için en başarılı sonuç, tüm yöntemler için %69 ile Xu-net modeliyle elde edilmiştir. 0,4 bpp yükte ise en başarılı sonuç, WOW yönteminde VGG16 modeli %86 ile elde edilmiştir. Ancak VGG16 test süresi iki kat daha uzun olduğundan daha kullanışlı yöntem olarak Yedroudj yöntemi görülmektedir. Ayrıca çalışmada derin öğrenmeye dayalı steganaliz ile ilgili zorlukları ve sınırlamaları vurgulanmış ve gelecekteki araştırmalar için potansiyel yollar önerilmiştir.

Investigation of steganalysis performance of selected steganography methods with deep learning models

H I G H L I G H T S

- Detection of images with information hidden in them
- Steganalysis with deep learning methods
- Use of artificial intelligence methods in cryptology

Article Info
Research Article
Received: 09.07.2023
Accepted: 08.04.2024

DOI:
10.17341/gazimmfd.1324765

Keywords:
Steganography, ımage steganalysis, data hiding, deep learning networks, cryptography

ABSTRACT

Steganography, the art of hiding information in seemingly harmless digital environments, poses a significant problem for information security. In recent years, deep learning techniques have emerged as powerful tools for a variety of computer vision tasks. This article provides a comprehensive review of the state-of-the-art in deep learning-based steganalysis, focusing on detecting confidential information from the digital environment. In the study, steganographic concepts and their results were investigated, and then different deep learning architectures and methodologies used in steganalysis were examined. The most successful result for test data at 0.2 bpp payload, for all methods, 69% was obtained with the Xu-net model. The most successful result is at 0.4 bpp load, in the WOW method, the VGG16 model was obtained with 86% accuracy. However, since the VGG16 test time is twice as long, the Yedroudj method is seen as the more useful method. Additionally, the study highlights the challenges and limitations of deep learning-based steganalysis and suggests potential avenues for future research.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *ercanbulus@nku.edu.tr / Tel: +90 282 250 2328

1. Giriş (Introduction)

Dijital çağda, bilginin çoğalması ve dijital medyanın yaygın kullanımı, gizli verileri zararsız örtü nesneleri içinde gizlemek için çeşitli tekniklerin yükselişine yol açmıştır. Bilgileri diğer veriler içinde saklama sanatı olan steganografi, veri güvenliği alanında önemli bir endişe kaynağı haline gelmiştir. Sonuç olarak, gizli bilgileri tespit etme ve analiz etme çalışması olan steganaliz [1, 2], dijital adli tıp alanında büyük önem kazanmıştır.

Geleneksel steganaliz yöntemleri, gizli bilgilerin varlığını ortaya çıkarmak için geleneksel olarak istatistiksel ve makine öğrenimi yaklaşımlarına dayanmaktadır. Bununla birlikte, derin öğrenme tekniklerinin ortaya çıkması ve verilerden karmaşık özelliklerin çıkarılması yeteneği ile steganaliz görevleri için derin öğrenme yöntemlerinin uygulanmasını keşfetmeye yönelik artan bir ilgi olmuştur.

Seçilen derin öğrenme yöntemlerinin performansını değerlendirmek için hem stega hem de kapak görüntülerinden oluşan kapsamlı bir veri seti kullanılmıştır. Veri seti, en az önemli bit (LSB) gömme, ayrık kosinüs dönüşümü (DCT) alan yöntemleri ve uzamsal alan teknikleri gibi çeşitli steganografik teknikleri içermiştir. Çeşitli steganografi algoritmaları kullanarak, derin öğrenme modellerinin genelleştirme yeteneklerini ve farklı gömme şemalarında gizli bilgileri tespit etmedeki etkinliklerini değerlendirmeyi amaçlanmaktadır.

Titiz deneyler ve analizler yoluyla, steganaliz bağlamında her bir derin öğrenme yönteminin güçlü yanlarını ve sınırlamalarını belirlemek amaçlanmıştır. Bu durumun bunların uygulanabilirliği ve gerçek dünyaya yayılma potansiyeli hakkında değerli bilgiler edinmemizi sağlayacağı düşünülmektedir.

Bu çalışmanın bulguları, steganaliz tekniklerinin ilerlemesine katkıda bulunacak ve dijital ortamlardaki gizli bilgileri tespit etmek için daha sağlam ve etkili yöntemlerin geliştirilmesi için değerli rehberlik sağlayacaktır. Nihayetinde amaç, dijital adli soruşturmaları geliştirmek ve giderek birbirine bağlı hale gelen bir dünyada dijital verilerin bütünlüğünü ve güvenliğini sağlamaktır.

Genel olarak, bu araştırma, gizli iletişim ve veri manipülasyonuna karşı mücadelede derin öğrenmenin gücünden yararlanmaya yönelik çok önemli bir adımı temsil etmekte ve steganaliz alanındaki teknolojik gelişmelerin ön saflarında kalmanın önemini vurgulamaktadır [3]. Bu araştırmada, evrişimli sinir ağları (CNN, Convulational Neural Networks) gibi son teknoloji derin öğrenme mimarilerine odaklanılmıştır. Bu mimariler, çeşitli bilgisayar görüşü ve doğal dil işleme görevlerinde olağanüstü yetenekler sergileyerek onları steganaliz için umut verici adaylar haline getirmiştir [4-6].

Ayrıca bu araştırmada, seçilen derin öğrenme yöntemlerinin steganaliz alanındaki performansı araştırılmıştır. Derin sinir ağlarının gücünden yararlanarak, steganografik içeriği etkili bir şekilde tespit edip analiz edebilen sağlam ve verimli modeller kullanılmıştır (Şekil 1).

2. İlgili Çalışmalar (Related Works)

Karen Simonyan ve Andrew Zisserman, çok küçük (3x3) evrişim filtrelerine sahip bir mimari kullanarak artan derinliğe (16-19 ağırlık katmanı) sahip CNN'nin kapsamlı bir değerlendirmesini yaptılar [7].

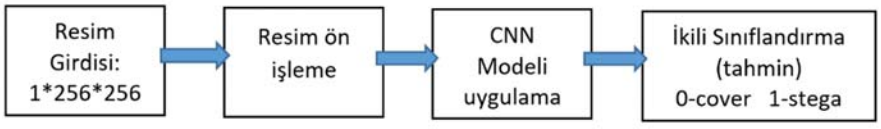
Yinlong Qian vd., 2015 yılında steganaliz için özelleştirilmiş bir evrişimsel Sinir Ağı önerdiler. Mevcut şemalarla karşılaştırıldığında, bu modelle, özellik çıkarma ve sınıflandırma adımlarını çeşitli evrişimli katmanlarla tek bir mimari altında birleştirdikleri görülür. Önerilen modelin etkinliğini üç uzamsal alan steganografik algoritma - HUGO [8], WOW ve S-UNIWARD üzerinde gösterdiler. Mekânsal Zengin Model (SRM, Spatial Rich Model) ile karşılaştırıldığında, onların modeli BOSSbase ve ImageNet veritabanında oldukça iyi performanslar elde etti [9].

Guanshuo Xu vd., önerdikleri ayrıntılı mimaride, sonraki katmanlarda istatistiksel modellemeyi kolaylaştırmak ve geliştirmek için ilk evrişimsel katmandan oluşturulan özellik haritalarındaki öğelerin mutlak değerlerini almışlardır. Aşırı uydurmayı önlemenin yanı sıra, ağların erken aşamalarında hiperbolik tanjantın (TanH) doygunluk bölgeleriyle veri değerleri aralığını sınırladılar ve daha derin katmanlarda 1×1 evrişim kullanarak modellemenin gücünü azalttılar. Önerilen CNN'nin, BOSSbase veri tabanı [10, 11] ile S-UNIWARD ve HILL'i tespit etmek için SRM'ye kıyasla daha rekabetçi olduğunu gösterdiler.

2017'de önerilen CNN, Jian Ye vd. geleneksel bilgisayarla görme görevlerinde kullanılanlardan oldukça farklı bir yapıya sahipti. Rastgele bir stratejiden ziyade, önerilen CNN'nin ilk katmanındaki ağırlıklar, mekânsal zengin bir modelde (SRM) artık haritaların hesaplanmasında kullanılan temel yüksek geçiren filtre seti ile başlatılmıştır. Önerilen modelde, genellikle son derece düşük SNR'ye (stega signal to image content) sahip olan gömülü sinyallerin yapısını daha iyi yakalamak için CNN modellerinde kesik doğrusal birim adı verilen yeni bir aktivasyon işlevi benimsenmiştir. Son olarak, seçim kanalı bilgilerini birleştirerek önerilen CNN tabanlı steganalyzer'ın performansı iyileştirildi. Uzamsal alanda son teknoloji ürünü üç steganografik algoritma, örneğin WOW, S-UNIWARD ve HILL yöntemleri, modellerin etkinliğini değerlendirmek için kullanıldı [5].

Mehdi YEDROUDJ vd., bir ön işleme filtre bankası ve bir Kesme aktivasyon işlevi, bir Ölçek Katmanı ile ilişkili bir Toplu Normalleştirmeye sahip beş evrişimli katman ve ayrıca yeterince boyutta tam bağlantılı bir bölümün kullanımını kullanan bir CNN modeli önerdi. Bu modele yeroudj-net adını verdiler [12].

Reinel Tabares-Soto vd., eğitim sırasında doğruluğu, yakınsamayı ve kararlılığı geliştirmeye yönelik bir strateji sunuyordu. Strateji, Spatial Rich Models filtreleri, Spatial Dropout, Absolute Value katmanı ve Batch Normalization ile bir ön işleme aşamasını içeriyordu. Stratejiyi kullanmanın, doğruluğu %2'den %10'a yükselterek üç steganaliz CNN'sinin ve iki görüntü sınıflandırma



Şekil 1. Çalışmanın genel akışı (General flow of the study)

CNN'sinin performansını iyileştirdiğini, eğitim süresini 6 saatin altına indirdiğini ve ağların kararlılığını iyileştirdiğini gösterdiler [13].

T. Fu vd. üç modülden oluşan bir model önermiştir: gürültü çıkarma modülü, gürültü analiz modülü ve sınıflandırma modülü. SE(Squeeze-and-Excitation) modülünün artık bloğa gömülmesiyle gerçekleştirilen gürültü çıkarma modülü ve analiz modülünde bir kanal dikkat mekanizması kullanılmıştır. Ardından, özellikleri bir araya getirmek için ortalama havuzlama yerine evrişimli havuzlamayı kullandılar [14]. BossBase 1.01 veritabanı, P.Bas vd. yazılan "Break our steganographic system: the ins and outs oforganizasyon BOSS" makalesi için geliştirilmiştir.

3. Materyal ve Metotlar (Materials and Methods)

3.1. Çalışmanın Genel Algoritması (General Algorithm of Work)

Öncelikle diğer çalışmalarla eşit şartlarda CNN metotlarının kontrol edilebilmesi için standart olarak kullanılan BossBase 1.01 [15] ve Bows 2 [16] veri tabanları indirildi. Yine aynı şartları sağlayabilmek için resimler 256*256 çözünürlükte siyah-beyaz resimlere çevrildi. Buradaki her bir resme “cover” ile başlayan bir isim verilip oluşturulan “cover” dizinine taşındı. Cover dizininde bulunan resimlere seçilen steganografi yöntemi (WOW, S-UNIWARD, HILL, Mipod) ile bilgi saklanılıp oluşan resme “stega” ile başlayan bir isim verildi ve oluşturulan “stega” dizinine taşındı. Örnek vermek gerekirse cover001.jpg ile stega001.jpg biri içine bilgi saklanılmamış resim diğeri içine bilgi saklanılmış resimdir, bunlara bir resim çifti (pair) denildi. Eğitim (Training) için bir training dizini içine 10.000 BOWS 2 + 4.000 BOSSBasel 1.01, toplam 14.000 çift resim, Doğrulama (validation) için 1.000 BOSSBase 1.01 resim çifti validation dizini içine, Test (Testing) için 5.000 BOSSBase 1.01 resim çifti Testing dizini içine aktarıldı. Dizinlerdeki resim çiftleri daha hızlı işlem yapabilmek adına numpy dosyasına dönüştürülüp kaydedildi. Eğitim için ayrılan veriler seçilen CNN modeline göre resim ön işlemeden geçirilip özellikler çıkarıldı. Eğitim sonucu elde edilen özellikler test için daha sonra kullanılmak üzere bir dosya olarak kayıt edildi. Test için ayrılan test resim çiftleri ile testler yapıldı (Tablo 1).

3.1. Kullanılan Veritabanları (Databases Used)

Seçilen modellerin eğitimi, test edilmesi ve doğrulanması için BossBase 1.01 ve Bows 2 veritabanlarını kullandık. BossBase 1.01 veritabanı, P. Bas vd. tarafından yazılan "Break our steganographic system: the ins and outs oforganizasyon BOSS" makalesi için geliştirilmiştir [16]. Bows 2 veritabanı [17] W. Mazurczyk vd. tarafından "Information Hiding: Challenges for Forensic Experts" 2017 makalesinde geliştirilmiştir. Bu veritabanları en çok mekânsal alanda steganaliz için popülerdir. Denetimlerde kullanılan veritabanları için aşağıdaki işlemleri gerçekleştirdik:

- Tüm resimler 256 × 256 piksel siyah-beyaz olarak yeniden boyutlandırıldı.
- Seçilen algoritmaya sahip her bir kapak (cover) resmi, piksel başına 0,2 bit (bpp) ve 0,4 bpp'lik iki yük (payload) için incelenindi.
- Deneyler için veritabanını BOSSBase 1.01 + BOWS 2 kombinasyonu ile kullanıldı.
- Bir çift (pair), bir kapak (cover) ve bir stega görüntüsü içerir.
- Eğitim (Training) için kullanılan çiftler (pairs): 10.000 BOWS 2 + 4.000 BOSSBasel 1.01, toplam 14.000
- Doğrulama (validation) için kullanılan çiftler: 1.000 BOSSBase 1.01
- Test (Testing) için kullanılan çiftler: 5.000 BOSSBase 1.01
- Her set, okuma süresini hızlandıran [13] NumPy dizisi (npy) formatında kaydedildi.

Bu veritabanı için dağıtım ve bölümleme, Jian Ye vd. [5], Mehdi Yedroudj vd. [12], Ru Zhang vd. [18] tarafından önerildiği gibi yapıldı.

3.2. Kullanılan Steganografi Algoritmaları (Steganography Algorithms Used) [20, 21]

3.2.1. WOW steganografi yöntemi (WOW steganography method)

WOW (Wavelet Obtained Weights) yöntemi, uzamsal alanda güvenli bir gömme yöntemidir. Bu yöntem, güvenliği artırmak için düz kenarlardan kaçınırken doku bölgelerine gömme değişikliklerini kısıtlayarak çalışır. İlk olarak, kapak görüntüsünün her bir pikseli için yönlü artıkları elde etmek için üç yönlü filtre kullanılmış ve bu artıklar kullanılarak her bir pikselin gömme uygunluğu hesaplanmıştır. Ardından, bu yerleştirme uygunlukları, yerleştirme maliyetlerini elde etmek için toplanır. Distorsiyon fonksiyonu kurulduktan sonra, distorsiyon fonksiyonunu minimize etmek ve stega görüntüsünü elde etmek için STC'ler (Syndrome-Trellis Codes) uygulanır. Genel olarak, dokusal bölgelerdeki piksellerin gömme maliyetleri daha düşüktür ve bu piksellerin, STC'ler kullanılarak gizli mesaj gömüldüğünde değişme olasılığı daha yüksektir. Bu sayede, tipik steganalitik yöntemlere karşı yüksek güvenlik sağlayabilir [19].

Tablo 1. Çalışmanın genel algoritması (General algorithm of work)

BossBase 1.01 ve Bows 2 veri tabanları indirildi
İndirilen veri tabanları 256x256 çözünürlükte siyah-beyaz resimlere dönüştürüldü.
Buradaki her bir resime “cover” ile başlayan bir isim verildi ve cover dizinine taşındı
Seçilen steganografi yöntemi (WOW, S-UNIWARD, HILL, Mipod) ile resim içine bilgi saklanılıp oluşan resme “stega” ile başlayan bir isim verildi ayrı dizine taşındı
Eğitim (Training) için çift olarak (cover ve stega bir çift) 10.000 BOWS 2 + 4.000 BOSSBasel 1.01, toplam 14.000 resim ayrıldı.
Doğrulama (validation) için 1.000 BOSSBase 1.01 çifti ayrıldı.
Test (Testing) için 5.000 BOSSBase 1.01 çifti ayrıldı.
Eğitim için ayrılan cover dizininde bulunan veriler “X_train.npy” isimli numpy dosyasına dönüştürülüp kaydedildi, stega dizininde bulunan veriler “y_train.npy” isimli numpy dosyasına dönüştürülüp kaydedildi.
Eğitim için ayrılan veriler seçilen CNN modeline göre resim ön işlemeden geçirilip özellikler çıkarıldı.
Eğitim sonucu elde edilen özellikler test için daha sonra kullanılmak üzere bir dosya olarak kayıt edildi.
Test için ayrılan test resim çiftleri ile testler yapıldı.

3.2.2. S-UNIWARD steganografi yöntemi
(S-UNIWARD steganography method)

S-UNIWARD (spatial-universal wavelet relative distortion) algoritması, WOW algoritmasına benzerdir. Bu teknik, gizli bir mesajı uzamsal alana gömmek için UNIWARD distorsiyon işlevini kullanır. Piksel maliyetleri yatay, dikey ve çapraz dalgacık katsayılarına bağlı olarak üç yönden hesaplanır [22].

3.2.3. HILL steganografi yöntemi (HILL steganography method)

HILL (High-pass, Low-pass, and Low-pass) steganografisi, görüntüler veya ses dosyaları gibi dijital ortamlardaki bilgileri gizlemek için kullanılan bir yöntemdir. Verileri gömmek ve çıkarmak için geçen süreyi daha kısadır. HILL steganografi yöntemi, gizli bilgileri gömmek için kapak (cover) resminin en önemsiz bitlerinin (LSB) manipüle edilmesini içerir. LSB'ler, ortamın her bir pikseli veya örneğindeki en önemsiz ikili basamaklardır ve ortamın genel görünümü veya kalitesi üzerinde en az etkiye sahiptirler [23].

3.3. Kullanılan CNN Modelleri (CNN Models Used)

3.3.1. VGG16 modeli (VGG16 Model)

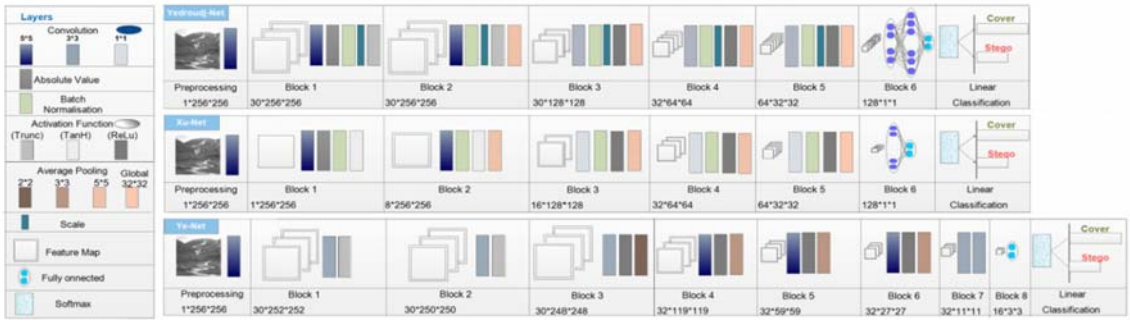
VGG16 (Visual Geometry Group 16) (Şekil 2), Oxford Üniversitesi'ndeki Görsel Geometri Grubu tarafından tanıtılan bir evrişimli sinir ağı (CNN) mimarisidir [24]. Simonyan ve Zisserman tarafından 2014 yılında "Very Deep Convolutional Networks for Large-Scale Image Recognition" başlıklı araştırma makalelerinde önerilmiştir [7].

VGG16, görüntü sınıflandırma görevlerinde basitliği ve etkinliği ile bilinir. 13 evrişimli katman ve 3 tam bağlı katman olmak üzere 16 katmandan oluşur. Şekil 3. Konvolüsyonel katmanlar, girdi görüntülerinden özniteliklerin çıkarılmasından sorumluyken, tamamen bağlantılı katmanlar sınıflandırıcı görevi görür.

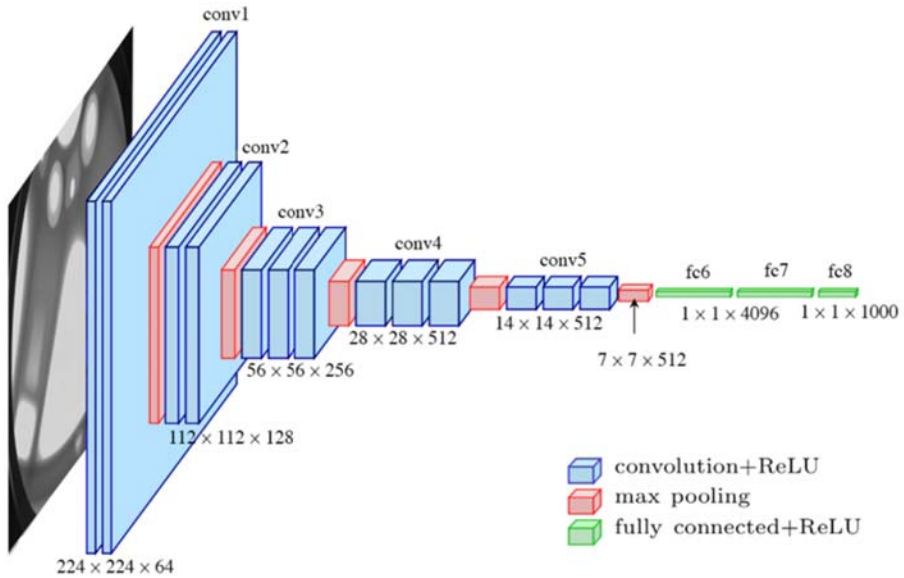
VGG16'nın temel özelliği, ağ boyunca önceki modellere kıyasla daha derin bir mimariye yol açan 3x3 evrişimli filtrelerin kullanılmasıdır. VGG16, çoklu evrişimli katmanları istifleyerek, girdi görüntülerinde giderek daha karmaşık hale gelen desenleri ve özellik hiyerarşilerini yakalama yeteneğine sahiptir.

VGG16'nın mimarisi, aralarında maksimum havuzlama katmanları bulunan birden çok evrişimli katmanı tutarlı bir şekilde istifleme modelini takip ettiği için tekdüzeliğiyle bilinir. Ağın son katmanı, girdi görüntüsü için sınıf olasılıkları üreten bir softmax katmanıdır.

VGG16, ImageNet Büyük Ölçekli Görsel Tanıma Mücadelesi (ILSVRC, ImageNet Large Scale Visual Recognition Challenge) veri setinde mükemmel performans elde ederek, derin CNN'lerin



Şekil 2. Yedroudj-Net, Xu-Net ve Ye-Net yapısı (Yedroudj-Net, Xu-Net and Ye-Net structure) [12]



Şekil 3. VGG16 yapısı (VGG16 Structure) [15]

görüntü sınıflandırma yeteneğini gösterdi. VGG16, ResNet veya EfficientNet gibi daha yeni mimarilere kıyasla daha eski bir model olsa da, bilgisayarla görme alanında hala değerli bir kıyaslama ve temel bir model olarak hizmet ediyor [25, 26].

3.3.2. Xu-Net modeli (Xu-Net Model)

Xu-Net (Şekil 2), Guanshuo Xu vd. [10] tarafından önerilen CNN'nin adıdır. Bu mimari, bir Yüksek Geçiren Filtre (HPF) katmanından oluşan bir özellik çıkarma aşamasına, özellik çıkarımı için beş evrişimli katmana, ilk evrişimli katmandan sonra bir ABS katmanına, her bir evrişimli katmandan sonra BN'ye, tamamen bağlantılı iki katmandan ve bir softmax katmandan oluşan bir sınıflandırma aşamasına sahiptir. İlk iki katman TanH aktivasyon fonksiyonunu ve son üç katman için ReLU'yu kullanır.

3.3.3. Ye-Net modeli (Ye-Net Model)

Ye-Net (Şekil 2), Jian Ye vd. tarafından önerilmiştir [5]. Steganografik gürültü çıkarma için bir SRM filtre bankası kullanır. Özellik çıkarma aşaması, sekiz konvolüsyonel katmandan, ilk katmandan sonra bir TLU aktivasyon fonksiyonundan vd. için TanH'den oluşur. Sınıflandırma aşaması, tamamen bağlı bir katmana ve Softmax aktivasyon fonksiyonuna sahiptir.

3.3.4. Yedroudj-Net modeli (Yedroudj Model)

Yeroudj-Net (Şekil 2), Mehdi YED-ROUDJ vd. tarafından önerilmiştir [12]. Xu-Net ve Ye-Net'in en iyi özelliklerini alır ve bunları aynı mimari altında birleştirir. Bu mimari, SRM'den ilham alan bir filtre bankası, özellik çıkarma için beş evrişimli katman, birinci katmandan sonra bir ABS katmanı, ikinci katmandan başlayarak her katmandan sonra Ortalama Havuzlama kullanır. İlk iki katmanda TLU aktivasyon işlevini ve son üç katmanda ReLU'yu kullanır. Sınıflandırma aşaması tamamen bağlantılı iki katmana ve Softmax aktivasyon fonksiyonuna sahiptir.

Bütün modellerdeki hesaplama öğeleri için Reinel Tabares-Soto vd. [13] kullanılan stratejiler kullanıldı.
Modeller 100 epoch için eğitilmiş ve her biri 1600 epoch kullanıldı.

3.3.5. Çalışmada kullanılan yazılım ve donanımlar
(Software and hardware used in the study)

Programlama dili : conda-forge Python 3.10.9
Yapay zeka kütüphanesi : TensorFlow 2.10.1
İşletim sistemi : Windows 10 Pro 64bit
İşlemci (CPU) : INTEL I5-4690 4-Core Processor
Hafıza (RAM) : 16 GB SSD: 256 GB HD: 1 TB
Grafik kart (GPU) : GeForce RTX 3060 (12 GB)
Cuda Version : 11.0

3.4. Başarım Ölçütleri (Performance Criteria)

Çalışmanın ilerleyen bölümlerinde modellere yönelik testlerden elde edilen doğruluk değerleri karşılaştırılmıştır. Doğruluk (Accuracy), bir sınıflandırma modelinin performansını ölçmek için kullanılan bir yöntemdir. Doğruluk, tahmin edilen değerin gerçek değere eşit olduğu tahminlerin sayısıdır. Çalışmada modellerin sadece doğruluk değerleri değil; bir sonraki bölümde Kesinlik (Precision), Duyarlılık (Recall) ve F-Measure değerlerini de inceleyeceğiz.

Karışıklık Matrisi (Tablo 2), tahmini ve gerçek değerlerinin dört farklı kombinasyonunu içeren bir tablodur. Tabloda Pozitif Doğru (True Positive -TP) doğrunun doğru olarak adlandırıldığı durumu, Negatif Doğru (True Negative - TN) yanlışın yanlış olarak adlandırıldığı durumu, Pozitif Yanlış (False Positive -FP) doğrunun yanlış olarak adlandırıldığı durumu, Negatif Yanlış (False Negative - FN), yanlışın doğru olarak adlandırıldığı durumu temsil eder.

Kesinlik (precision, Eş. 1), gerçek pozitifler (TP) ile tüm pozitifler arasındaki orandır. Kesinlik, olumlu tanımlamalardan kaçının gerçekten doğru olduğu sorusunu yanıtlamayı amaçlamaktadır.

$$\text{Kesinlik} = \frac{\text{TP}}{\text{TP+FP}} \quad (1)$$

Duyarlılık (recall, Eş. 2), Gerçek Pozitifleri (TP) doğru bir şekilde tanımlayan modelin ölçüsüdür. Duyarlılık, gerçek Pozitiflerden kaçının doğru şekilde tanımlandığını yanıtlamaya çalışır.

$$\text{Duyarlılık (Recall)} = \frac{\text{TP}}{\text{TP+FN}} \quad (2)$$

Bir modelin etkililiğini tam olarak değerlendirebilmek için hem kesinlik hem de hatırlamanın birlikte incelenmesi gerekir. F-measure (Eş. 3) bize kesinlik ve geri çağırma değerlerinin harmonik ortalamasını verir. Mükemmel bir modelin F-measure 1,0 olmalıdır.

$$\text{F} - \text{Measure} = 2 \cdot \frac{\text{Kesinlik} * \text{Duyarlılık}}{\text{Kesinlik+Duyarlılık}} \quad (3)$$

4. Sonuçlar ve Tartışmalar (Results and Discussions)

4.1. Eğitim (Training)

4.1.1. VGG16

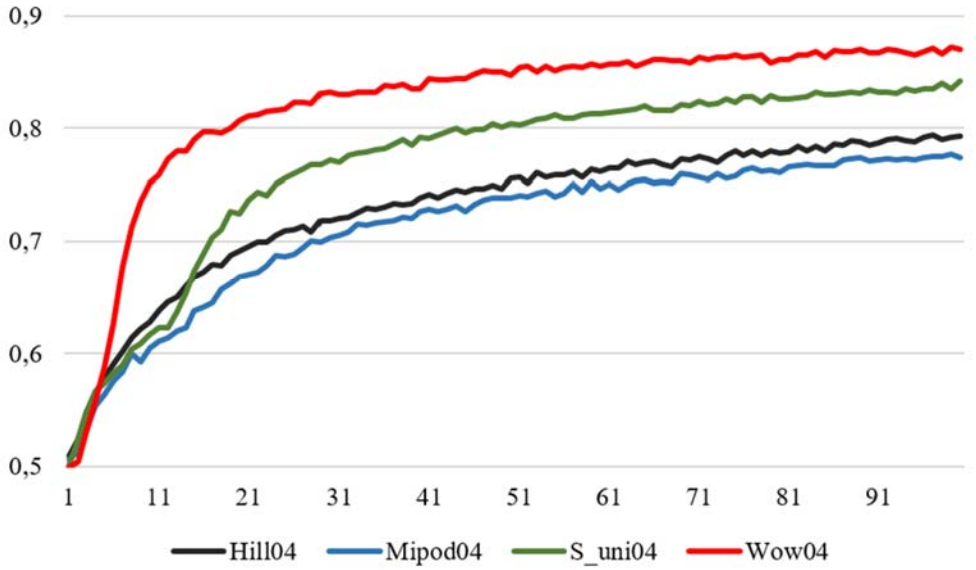
VGG16 Modelinde (Şekil 3), sınıflandırma için maksimum havuzlama (max.pooling) kullanılmıştır. Ancak, VGG16 için seçilen dört Steganografi Metodu 0,2 bpp'lik yük (payload) için istenen sonucu vermediğinden, yalnızca 0,4 bpp'lik yük kullanıldı. 0,4 bpp yük ile VGG16 Max Pooling eğitim eğrileri, Şekil 4'teki gibidir. En iyi eğitim eğrisi Wow steganografi yöntemi için elde edilmiş, ikinci eğri S-Uniward için elde edilmiş, eğitim için harcanan süre Tablo 3'deki gibidir. Eğitim süreleri arasında anlamlı bir fark görülmemiştir.

Tablo 3. 0,4 bpp'de vgg16'nın toplam eğitim süresi (saat:dakika:saniye)
(Total training time of vgg16 at 0.4 bpp (hours:minutes:seconds))

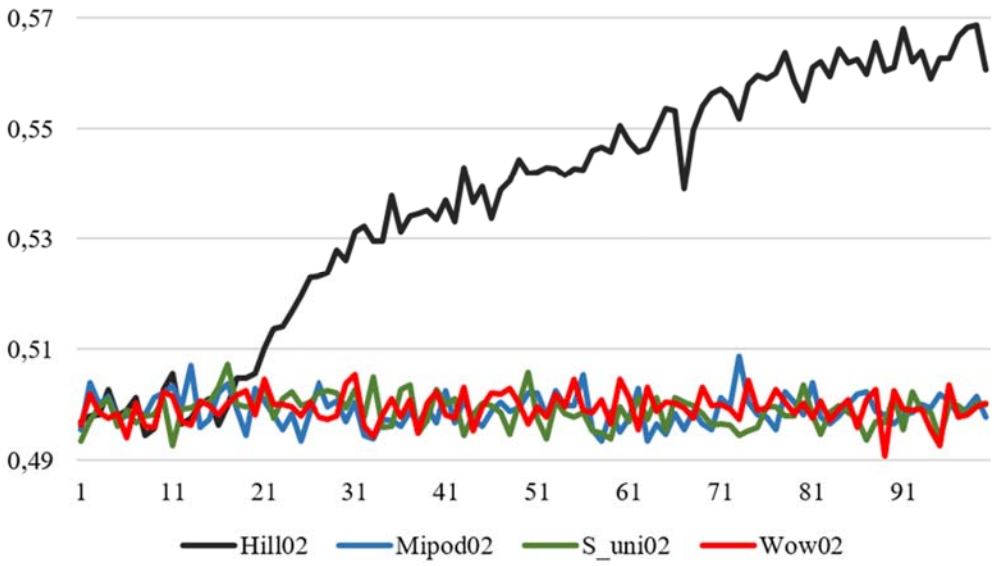
HILL	MiPOD	S-UNIWARD	WOW
20:24:59	20:24:33	20:24:46	20:23:07

Tablo 2. Karışıklık Matrisi (Confusion Matrix)

		Gerçek Değerler (Actual Values)	
		Pozitif (P)	Negatif (N)
Tahmin Edilen Değerler (Predicted values)	Pozitif (P)	Pozitif Doğru (TP)	Negatif Yanlış (FN)
	Negatif (N)	Pozitif Yanlış (FP)	Negatif Doğru(TN)



Şekil 4. Hill, Mipod, S-uniward ve Wow yöntemi için 0,4 bpp ile VGG16 eğitim eğrileri
(VGG16 training curves with 0.4 bpp for Hill, Mipod, S-uniward and Wow method)



Şekil 5. 0,2 bpp ile Xu-Net eğitim eğrileri (Xu-Net training curves with 0.2 bpp)

4.1.2. Xu-Net

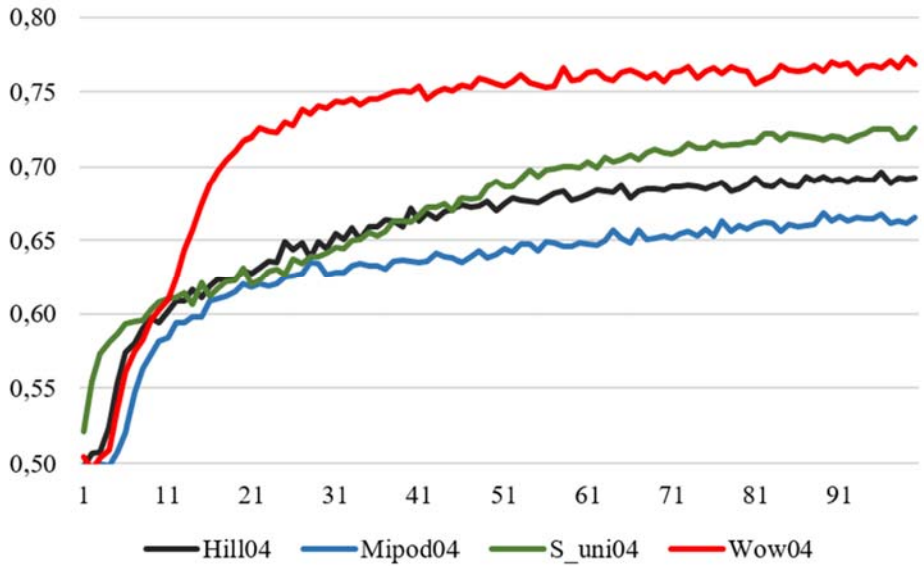
Xu-Net'te 0,2 bpp için en iyi eğitim eğrisi HILL steganografi yönteminde (Şekil 5), 0,4 bpp için en iyi eğitim eğrisi WOW steganografi yöntemindedir (Şekil 6). 0,2 bpp için eğitim eğrisi, diğerleri için hemen hemen aynıdır. İkinci eğitim eğrisi S-Uniward 0,4 bpp'de, Üçüncü eğitim eğrisi HILL 0,4 bpp'de, en kötü eğitim eğrisi MiPOD 0,4 bpp'de. Tablo 4'den de görülebileceği gibi, eğitim süreleri arasında anlamlı bir fark yoktur.

4.1.3. Ye-Net

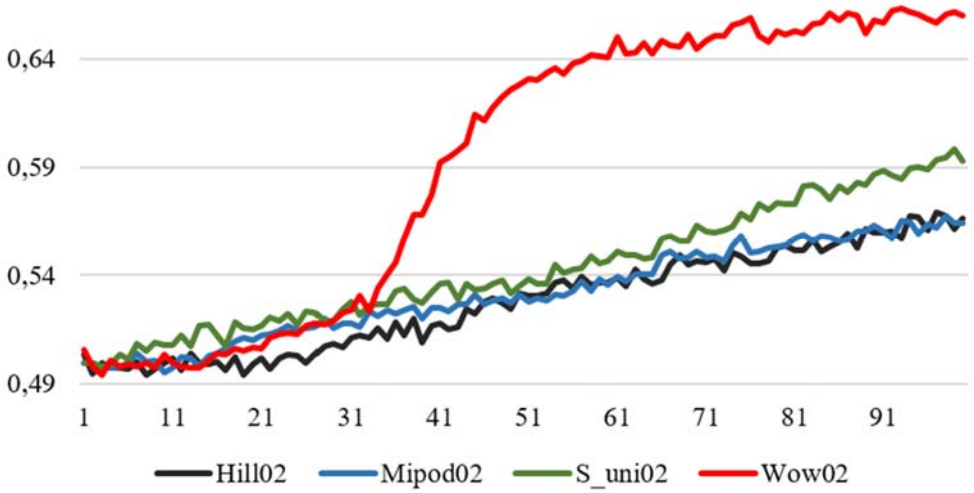
Ye-Net'te 0,2 bpp için en iyi eğitim eğrisi HILL steganografi yönteminde (Şekil 7), 0,4 bpp için en iyi eğitim eğrisi WOW steganografi yöntemindedir (Şekil 8). 0,2 bpp ve 0,4 bpp için steganografi yöntemlerinin eğitim eğrilerine bakıldığında sıralamanın S-Uniward, MiPod, HILL olduğu görülmektedir. TABLO 5'den de görülebileceği gibi, eğitim süreleri arasında anlamlı bir fark yoktur.

Tablo 4. 0, Xu-net'in 0,2 bpp ve 0,4 bpp'de toplam eğitim süresi (saat:dakika:saniye)
(Total training time of Xu-net at 0.2 bpp and 0.4 bpp (hours:minutes:seconds))

HILL		MiPOD		S-UNIWARD		WOW	
0,2	0,4	0,2	0,4	0,2	0,4	0,2	0,4
04:09:05	04:08:45	04:08:45	04:08:36	04:08:18	04:09:03	04:08:59	04:08:36



Şekil 6. 0,4 bpp ile Xu-Net eğitim eğrileri (Xu-Net training curves with 0.4 bpp)



Şekil 7. 0,2 bpp ile Ye-Net eğitim eğrileri (Ye-Net training curves with 0.2 bpp)

4.1.4. Yedroudj-Net

Yeroudj-Net'te 0,2 bpp için en iyi eğitim eğrisi MiPod steganografi yönteminde (Şekil 9), 0,4 bpp için en iyi eğitim eğrisi ise WOW steganografi yöntemindedir (Şekil 9). 0,2 bpp için ikinci eğitim eğrisi HILL steganografi yöntemindedir (Şekil 9). 0,4 bpp için ikinci eğitim eğrisi HILL, S-UNIWARD ve Mipod steganografi yöntemleridir (Şekil 10). 0,2 bpp için üçüncü eğitim eğrileri S-UNIWARD ve WOW yöntemleridir. Tablo 6'dan da görülebileceği gibi, eğitim süreleri arasında anlamlı bir fark yoktur.

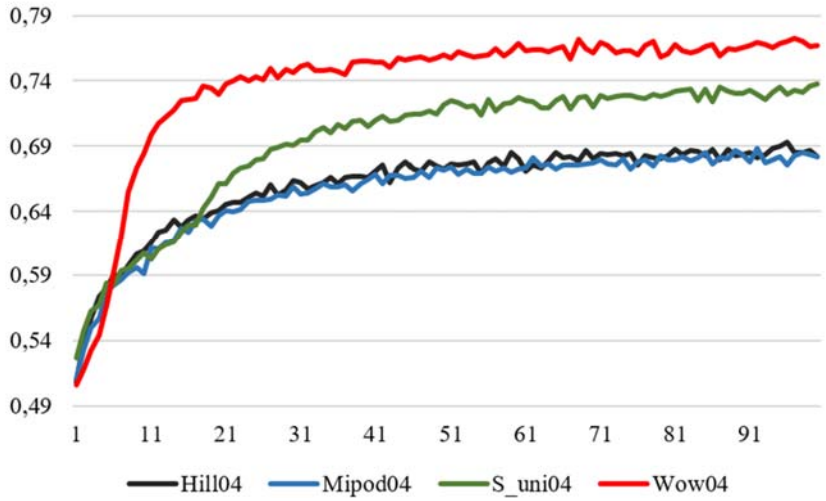
4.2. Eğitim Verimliliği (Training Efficiency)

Tablo 7 incelendiğinde 0,2 bpp payload için en iyi eğitim sonucunun %66 ile WOW steganografi yöntemine uygulanan Ye-Net Modeli ile elde edildiğini görmekteyiz. Bu durumda 0,2 bpp payload için hiçbir model ile iyi performans elde edilemeyeceğini söyleyebiliriz.

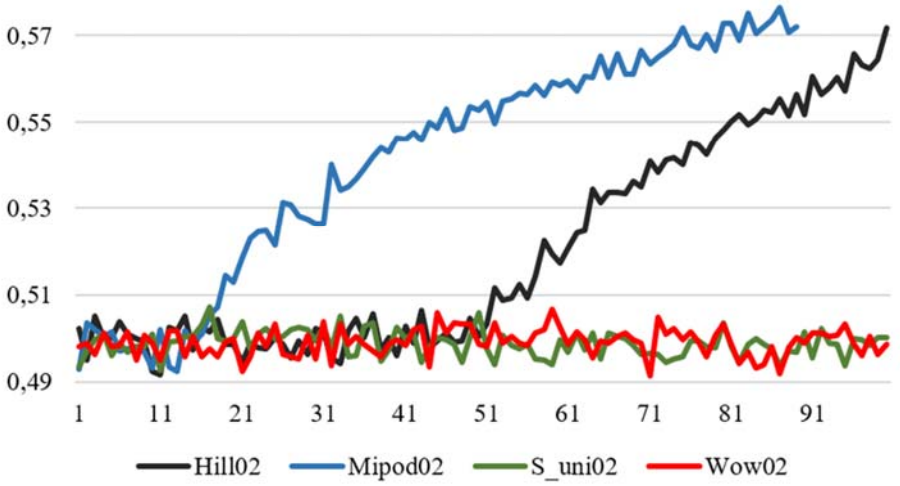
Tablo 8 incelendiğinde ise VGG16 modelinin 0,4 bpp yük ile WOW steganografi yöntemi için yüzde 86,7'ye ulaştığı görülmektedir. 0,4 yük ile en kötü performansın yüzde 66,55 ile Mipod steganografi yöntemine uygulanan Xu-net olduğu görülüyor. Ancak bu durum bile 0,2 yük ile en iyi performans durumundan daha iyidir.

4.3. Test (Testing)

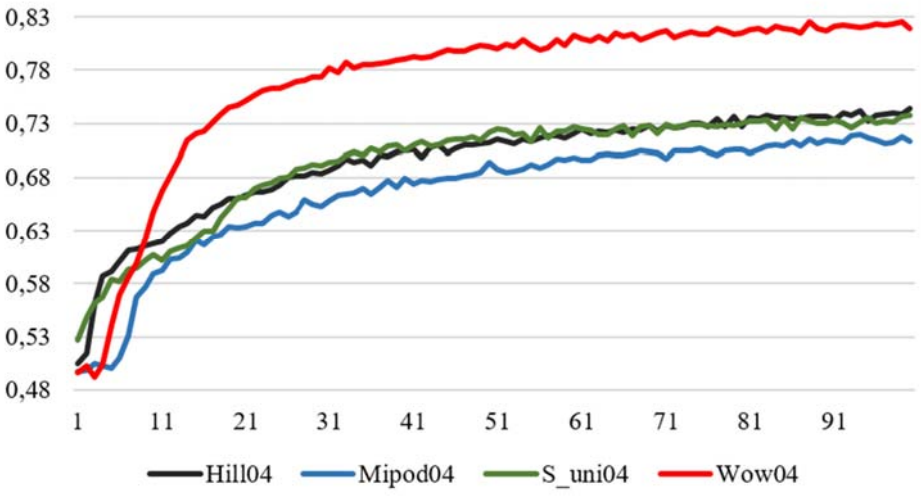
0,2 bpp yükte eğitim dizisi (Tablo 7) ile test dizisi (Tablo 9) karşılaştırıldığında, aralarında farklılıklar gözlenir. HILL yöntemi, Eğitim sıralamasında birinci, WOW yöntemi ise Test sıralamasında birincidir. HILL yöntemi, test sıralamasında son sırada yer aldı. Ancak 0,4 bpp yükte sıralamanın değişmediği dikkat çekmektedir (Tablo 8, Tablo 10). Test süresi incelendiğinde (Tablo 11) en hızlı modelin Xu-Net, en yavaş modelin VGG16 olduğu göülmektedir.



Şekil 8. 0,4 bpp ile Ye-Net eğitim eğrileri (Ye-Net training curves with 0.4 bpp)



Şekil 9. 0,2 bpp ile Yedroudj-Net eğitim eğrileri (Yedroudj-Net training curves with 0.2 bpp)



Şekil 10. 0,4 bpp ile Yedroudj-Net eğitim eğrileri (Yedroudj-Net training curves with 0.4 bpp)

Tablo 5. 0, Ye-net'in 0,2 bpp ve 0,4 bpp'de toplam eğitim süresi (saat:dakika:saniye)
(Total training time of Yeu-net at 0.2 bpp and 0.4 bpp (hours:minutes:seconds))

HILL		MiPOD		S-UNIWARD		WOW	
0,2	0,4	0,2	0,4	0,2	0,4	0,2	0,4
06:41:17	06:26:15	06:41:06	06:40:23	06:26:19	06:40:22	06:41:54	06:41:45

Tablo 6. Yedroudj-net'in 0,2 bpp ve 0,4 bpp'de toplam eğitim süresi (saat:dakika:saniye)
(Total training time of Yedroudj-net at 0.2 bpp and 0.4 bpp (hours:minutes:seconds))

HILL		MiPOD		S-UNIWARD		WOW	
0,2	0,4	0,2	0,4	0,2	0,4	0,2	0,4
08:52:14	08:57:22	08:52:00	08:58:11	08:52:58	08:51:49	08:51:58	08:51:12

Tablo 7. 0,2 bpp için eğitim doğruluğu
(Training accurancy for 0.2 bpp)

Xu-net 0,2		Ye-net 0,2		Yedroudj 0,2	
Metod	Max ACC	Metod	Max ACC	Metod	Max ACC
HILL	0,560	WOW	0,660	MiPod	0,572
MiPod	0,498	S-UNI	0,593	HILL	0,571
S-UNI	0,500	HILL	0,566	S-UNI	0,500
WOW	0,500	MiPod	0,563	WOW	0,498

Tablo 8. 0,4 bpp için eğitim doğruluğu
(Training accurancy for 0.4 bpp)

VGG16		Xu-net		Yenet		Yedroudj-net	
Metod	Max ACC	Metod	Max ACC	Metod	Max ACC	Metod	Max ACC
WOW	0,86	WOW	0,76	WOW	0,76	WOW	0,81
S-UNI	0,83	S-UNI	0,72	S-UNI	0,73	HILL	0,74
HILL	0,78	HILL	0,69	HILL	0,68	S-UNI	0,73
MiPod	0,77	MiPod	0,66	MiPod	0,68	MiPod	0,71

Tablo 9. 0,2 bpp için kullanılan steganografi yöntemlerinin test doğruluklarının karşılaştırılması (Comparison of test accuracies of steganography methods used for 0.2 bpp)

XUNET		YENET		YEDROUDJ	
Model	Test ACC	Model	Test ACC	Model	Test ACC
WOW	0,694	WOW	0,695	S-UNI	0,668
MiPOD	0,693	HILL	0,647	MiPOD	0,627
S-UNI	0,693	S-UNI	0,636	HILL	0,578
HILL	0,623	MiPOD	0,626	WOW	0,500

Tablo 10. 0,4 bpp için kullanılan steganografi yöntemlerinin test doğruluklarının karşılaştırılması (Comparison of test accuracies of steganography methods used for 0.4 bpp)

	VGG16	XUNET	YENET	YEDROUDJ
Model	Test ACC	Test ACC	Test ACC	Test ACC
WOW	0,864	0,809	0,814	0,828
S-UNI	0,847	0,797	0,790	0,815
HILL	0,770	0,725	0,764	0,790
MIPOD	0,765	0,723	0,729	0,757

Tablo 11. Steganografi yöntemlerinin test sürelerinin (sn.), CNN modelleri ile karşılaştırılması
(Testing times (sec.) of the steganography methods and comparison with the CNN models)

	0,2 bpp				0,4 bpp			
	HILL	MIPOD	S-UNI	WOW	HILL	MIPOD	S-UNI	WOW
YENET	39,28	39,08	39,02	34,86	35,86	38,88	38,96	34,57
XUNET	18,94	18,89	18,9	18,85	18,88	19,04	18,89	34,92
YEDRUJ	58,13	45	45,06	44,82	45,01	45,2	45	58,43
VGG16	------	------	------	------	81,93	82,22	82,94	82,14

Tablo 12. S-UNI sonuçlarının REF.13 ile karşılaştırılması (Comparison of S-UNI results with REF.13)

S-UNI	REF [13]		Bu çalışma	
bpp	*0,2*	*0,4*	*0,2*	*0,4*
Xu-net	0,712	0,818	0,693	0,797
Ye-Net	0,726	0,833	0,647	0,79
Yedroudj	0,733	0,841	0,627	0,815
VGG16	0,747	0,851	--	0,847

Tablo 13. WOW sonuçlarının Ref 13 ile karşılaştırılması (Comparison of WOW results with REF.13)

WOW	REF [13]		Bu çalışma	
bpp	*0,2*	*0,4*	*0,2*	*0,4*
Xu-net	0,748	0,847	0,694	0,809
Ye-Net	0,771	0,862	0,695	0,814
Yedroudj	0,782	0,869	0,668	0,828
VGG16	0,805	0,885	--	0,864

5. Sonuçlar (Conclusions)

Çalışmada 0,2bpp yük için test doğruluğu (test accuracy) sonuçları incelendiğinde (Tablo 9); en düşük sonucun MIPOD yöntemiyle YEDROUDJ modelinde %50 (0,500) olduğu, en verimli sonucun %69 (0,69) ile tüm yöntemler için XU-net modelinde olduğu görülmektedir. VGG16 modeli ile 0,2bpp yük altında kabul edilebilir sonuçlar elde edilemediğinden değerlendirilmeye alınmamıştır. Bu durumda 0,2bpp gibi az oranda bilgi yüklenilmiş resimlerde bilgi gizlenip gizlenilmediğini araştırmak için Xu-net modeli tercih edilebilir.

Yine çalışmada 0,4bpp yük için test doğruluğu (test accuracy) sonuçları incelendiğinde (Tablo 10); en düşük sonucun %72 (0,72) ile MIPOD yönteminde Xu-net modeliyle ve yine %72 (0,72) ile MIPOD yönteminde Ye-Net modelinde elde edilmiştir. Diğer taraftan en yüksek sonuç %86 (0,864) ile WOW yönteminde VGG16 modeliyle ve %84 (0,847) ile VGG16 ile elde edilmiştir. Ancak Tablo 11'deki işlem süreleri incelenildiğinde VGG16 modeliyle yapılan incelemelerin işlem süresinin diğerlerine göre neredeyse 2 katı fazla olduğu, bununda pek istenmeyen bir durum olduğu açıktır. Bu durumda 0,4bpp yük ile %75-%82 arasındaki ikinci en iyi doğruluk oranına ve VGG16'ya göre daha düşük işlem süresine (yarı yarıya) sahip olduğundan Yedroudj yöntemi daha kullanışlı bir yöntem olarak görülmektedir.

Yukarıda ifade edilen %86 test başarısını, test için daha önce kullanılmayan 5000 veriden 4300 adedinin doğru olarak tespit edilmesi olarak yorumlayabiliriz.

Kaynaklarda belirtilen en başarılı sonuçlar ref.13 olduğundan, çalışma sonuçlarımızla S_UNI (Tablo 12) ve WOW (Tablo 13) yöntemlerini karşılaştırdık. İlgili çalışmada [6] elde edilen sonuçlar bizim elde ettiğimiz sonuçlara göre %10 civarında daha başarılıdır, hatta 0,4 bpp yükte sonuçtaki fark daha da düşüktür ve %3 civarındadır.

Çalışmada basit bir donanım ve yazılım ortamı ile durumun tespit edilip edilemeyeceği incelenmiş ve başarılı kabul edilebilecek sonuçlar alınmıştır. Gelecekteki çalışmalarda, aynı ortamlarda daha hızlı ve daha iyi sonuçlar elde edebilecek yöntemlerin önerilmesi düşünülmektedir.

Kaynaklar (References)

1. Kodovsky J.S., Sedighi V., Fridrich J., Study of Cover Source Mismatch in Steganalysis and Ways to Mitigate its Impact, Proc. SPIE 9028, Media Watermarking, Security, and Forensics 2014, San Francisco, California, USA, 2014.
2. Sedighi V., Cogranne R., Fridrich J., Content-adaptive steganography by minimizing statistical detectability, IEEE Transactions on Information Forensics and Security, 11 (2), 221–234, 2016.
3. Forouzan B.A., Introduction to Cryptography and Network Security, McGraw-Hill Higher Education, isbn: 978-0-07-287022-0, New York, USA, 2008.
4. Fridrich J., Kodovsky J., Rich models for steganalysis of digital images, IEEE Transactions on Information Forensics and Security 7 (3), 868–882, 2012.
5. Ye J., Ni J., Yi Y., Deep learning hierarchical representations for image steganalysis, IEEE Transactions on Information Forensics and Security, 12 (11), 2545–2557, 2017.
6. Tompson J., Goroshin R., Jain A., LeCun Y., Bregler C., Efficient object localization using convolutional networks, 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 648-656., 2015.
7. Simonyan K., Andrew Z., Very Deep Convolutional Networks for Large-Scale Image Recognition, ICLR 2015, San Diego, USA, 2015.
8. Pevny T., FillerT., Bas P., Using High-Dimensional Image Models to Perform Highly Undetectable Steganography., Information Hiding, Calgary, Canada, 161-177, 2010.
9. Qian Y., Dong J., Wang W., Tan T., Deep learning for steganalysis via convolutional neural networks, Proc. SPIE 9409, Media Watermarking, Security, and Forensics 2015, San Francisco, California, USA, 2015.
10. Xu G., Wu H., Shi Y.Q., Structural Design of Convolutional Neural Networks for Steganalysis, IEEE Signal Processing Letters, 23, 708-712, 2016.
11. Xu G., Wu H., Shi Y.Q., Ensemble of CNNs for Steganalysis: An Empirical Study, IH&MMSec '16: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, New York, USA, 103-107, 2016.
12. Yedroudj M., Comby F., Chaumont M., Yedroudj-Net: An Efficient CNN for Spatial Steganalysis, 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, Canada, 2092-2096, 2018.
13. Tabares-Soto R., Arteaga H.B., Mora-Rubio A., Bravo-Ortíz M.A., Garzón D.A., Grisales J.A.A., Jacome A.B., Orozco-Arias S., Isaza G., Pollan R.R., Strategy to improve the accuracy of convolutional neural network architectures applied to digital image steganalysis in the spatial domain., PeerJ Computer Science, 2021.
14. Fu T., Chen L., Fu Z., Yu K., Wang Y., CCNet: CNN model with channel attention and convolutional pooling mechanism for spatial image steganalysis, Journal of Visual Communication and Image Representation, 88, 2022.
15. Buluş E., Gender Determination from Pictures with CNN Models, 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 310-313, 2021.
16. Bas P., Filler T., Pevny T., Break our steganographic system: the ins and outs of organizing BOSS, Information Hiding IH 2011, Lecture Notes in Computer Science, 6958, 59–70, 2011.
17. Mazurczyk W., Wendzel S., Information Hiding: Challenges for Forensic Experts, Communications of the ACM. 61, 86-94, 2017.
18. Zhang R., Zhu F., Liu J., Liu G., Depth-Wise Separable Convolutions and Multi-Level Pooling for an Efficient Spatial CNN-Based Steganalysis, in IEEE Transactions on Information Forensics and Security, 15, 1138-1150, 2020.
19. Holub V., Fridrich J., Designing steganographic distortion using directional filters, In: IEEE International Workshop on Information Forensics and Security 2012, 234–239, 2012.
20. Binghamton University, Steganographic algorithms, http://dde.binghamton edu/download/stego_algorith ms/, yayın tarihi 2015, Erişim tarihi Temmuz 2023.
21. Boroumand M., Fridrich J., Synchronizing Embedding Changes in Side-Informed Steganography, Proc. IS&T Int'l. Symp. on Electronic Imaging: Media Watermarking, Security, and Forensics, 290, 1-12, 2020.
22. Holub V., Fridrich J., Denemark T., Universal distortion function for steganography in an arbitrary domain. EURASIP Journal on Information Security, 2014.
23. Li B., Wang M., Huang J, Li X., A new cost function for spatial image steganography, In: 2014 IEEE International Conference on Image Processing (ICIP). Piscataway: IEEE, 4206–4210, 2014.
24. StanfordVisionLab, ImageNet Large Scale Visual Recognition Challenge 2014 (ILSVRC2014), https://www.image-net.org/challenges/LSVRC/2014/, yayın tarihi 2014, Erişim tarihi Temmuz 2023.
25. Karahanlı G., Taşkın C., Determining the growth stages of sunflower plants using deep learning methods, Journal of the Faculty of Engineering and Architecture of Gazi University, 39(3), 1455-1472, 2024.
26. Kadiroğlu Z., Deniz E., Şenyiğit A., A comparison of deep learning models for pneumonia detection from chest x-ray images, Journal of the Faculty of Engineering and Architecture of Gazi University, 39 (2), 729-740, 2023.