Medikal Görüntülerde Derin Öğrenme ile Steganaliz

Araştırma Makalesi/Research Article

Rukiye KARAKIŞ[1]*, Kali GÜRKAHRAMAN[2]

[1] Yazılım Mühendisliği Bölümü, Teknoloji Fakültesi, Sivas Cumhuriyet Üniversitesi, Sivas, Türkiye
[2] Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Sivas Cumhuriyet Üniversitesi, Sivas, Türkiye
rkarakis@cumhuriyet.edu.tr, kgurkahraman@cumhuriyet.edu.tr
(Geliş/Received:24.09.2020; Kabul/Accepted:10.03.2021)
DOI: 10.17671/gazibtd.799370

Özet— Steganaliz ile bir medya dosyasındaki gizli mesajı elde etmek ya da sadece mesajın varlığını tespit etmek amaçlanır. Literatürde medikal verilerin güvenliğini sağlamayı amaçlayan pek çok steganografi yöntemi mevcut olsa da medikal steganaliz çalışması çok azdır. Bu çalışmada, medikal görüntü steganografi yöntemlerinin dayanıklılığının arttırılmasında kullanılabilecek ve medikal bir görüntüde gizli mesajların varlığını tespit edebilecek bir sınıflandırıcı geliştirilmesi amaçlanmıştır. Bunun için karmaşık ve maliyetli öznitelik analizine gerek duymayan bir derin öğrenme mimarisi olan evrişimsel sinir ağı(ESA) taşıyıcı ve stego medikal görüntüler ile eğitilmiş ve test edilmiştir. Doğruluk, kesinlik, hassasiyet ve F1 değerleri sırasıyla 0,964, 0,966, 0965 ve 0964 olarak elde edilmiştir. Bu çalışma, derin öğrenme yönteminin medikal görüntü steganalizinde de kullanılabileceğini ilk kez göstermiştir.

Anahtar Kelimeler— derin öğrenme, evrişimsel sinir ağı, medikal görüntü steganalizi, medikal görüntü steganografi, uzamsal düzlem.

Steganalysis with Deep Learning on Medical Images

Abstract— With steganalysis, it is aimed to obtain a hidden message from a media file or only to detect the presence of the message. Although there are many steganography methods in the literature aiming to ensure the medical data security, medical steganalysis studies are very few. In this study, it is aimed to develop a classifier that can be used to increase the durability of medical image steganography methods and detect the presence of hidden messages in a medical image. For this, the convolutional neural network (CNN), a deep learning architecture that does not require complex and costly feature analysis, has been trained and tested with cover and stego medical images. Accuracy, precision, recall and F1 values were obtained as 0.964, 0.966, 0965 and 0964, respectively. This study has shown for the first time that the deep learning method can also be used in medical image steganalysis.

Keywords—deep learning, convolutional neural network, medical image steganalysis, medical image steganography, spatial transform.

1. GİRİŞ (INTRODUCTION)

Steganografi; sadece alıcının ve gönderenin bildiği gizli mesajın, üçüncü şahısların fark etmemesini sağlayacak yöntemlerle, görüntü, ses, video ya da metin gibi bir taşıyıcı (cover) nesne içerisine gömülmesidir. Steganografi bilimi; veri gizleme ve veri elde etme olmak üzere iki aşama içerir. Veri gizlemede, taşıyıcı nesneye bir stego anahtar ve veri gizleme algoritması ile mesaj gizlenerek stego nesnesi oluşturulur ve bu nesne karşı tarafa aktarılır. Veri elde aşamasında ise veriyi alan kişi aynı stego anahtarı ve algoritmayı kullanarak stego nesnesinden gizlenen mesajı elde eder. Steganaliz ise steganografinin tam karşısındadır ve bir medya dosyasından gizli mesajı elde etmeye ya da sadece mesajın varlığını tespit etmeye çalışır [1-6]. Aynı zamanda, steganalizin varlığı yeni steganografi yöntemlerinin daha dayanıklı geliştirilmesine katkıda bulunur.

Veri gizleme teknikleri medikal veriler üzerinde de kullanılmaktadır. Taşıyıcı medikal veriler, radyoloji görüntüleri ya da biyolojik sinyaller olabilir. Bunlara,

kişisel bilgiler ya da hastaların diğer medikal kayıtları gizlenir ve oluşturulan stego nesneleri ağ üzerinden aktarılır. Steganografi ile bu veri aktarım işleminde kişisel bilgilerin mahremiyetinin yetkisiz girişlere karşı korunması amaçlanır [7-8].

Steganografi ve kriptografi bilgi güvenliğinde tek başlarına ya da çoğu zaman birlikte kullanılmaktadır. Kriptografik veri anlamsız olduğundan kolayca fark edilirken, steganografi de gizli mesaj ilk bakışta algılanamaz. Bu gizli mesajı elde etmeyi hedefleyen steganaliz, saldırı teknikleri açısından literatürde 6 grupta analiz edilmektedir. Bunlar; (1) *yalnız stego saldırısı:* sadece stego nesnesi üzerinde analiz yapılır, (2) *bilinen taşıyıcı saldırısı:* taşıyıcı ve stego nesneleri birlikte analiz edilir, (3) *bilinen mesaj saldırısı:* mesaj biliniyordur ve stego nesnesi ile karşılaştırılır, (4) *seçilen stego saldırısı:* stego nesnesi ve bilinen veri gizleme algoritması kullanılarak analiz yapılır, (5) *seçilen mesaj saldırısı:* bilinen bir mesaj, bazı steganografi araçları ve algoritmaları yardımıyla stego nesnesi oluşturulur ve böylece nesnede yöntemin yarattığı örüntü anlaşılmaya çalışılır, (6) *bilinen stego saldırısı:* bilinen veri gizleme yöntemi, taşıyıcı ve stego nesneleri kullanılarak analiz yapılır [2-3].

Steganalistler, eğer stego ve taşıyıcı görüntülerin ikisini de elde etmişlerse öncelikle bunları birbirleriyle karşılaştırırlar. Bu durumda, yaygın olarak kullanılan steganaliz yöntemleri şunlardır: (1) görüntülerin dosya boyutlarını kontrol etmek, (2) benzersiz olan renklerdeki artma ya da azalmayı incelemek ve (3) görüntülerde yeniden ölçeklendirme ya da kırpma gibi işlemler yapılıp yapılmadığını tespit etmektir. Literatürde en sık kullanılan steganografi yönteminde verinin en az ağırlıklı bitlerine (EAB) mesaj bitleri gizlenir. Bu sebeple, steganalistler, stego ve taşıyıcı görüntülerin piksellerinin EAB'lerindeki 0 ve 1 bitlerinin sayılarını karşılaştırırlar. Eğer sadece stego görüntüye sahiplerse, bu görüntüdeki piksellerin EAB'lerindeki 0 ve 1 bitlerinin sayılarını kıyaslarlar. Ancak, EAB bit analizi gürültülü görüntülerde başarılı sonuçlar vermez [2].

Bazı stego araçları (Marker, Jpegx vb.) veri gizlerken imzalarını da nesneye gömerler. Steganalistler bu imzalardan yola çıkarak kullanılan araçları ve veri gizleme yöntemlerini tahmin edebilirler. Ayrıca, stego araçlarının imzalarına bakılmaksızın da analizler yapılabilir. Örneğin, JPEG görüntülerde gerçekleştirilen gizleme işlemini belirlemek için görüntüler 8x8 bloklara ayrıştırılır ve Ayrık Kosinüs Dönüşümü (AKD) kullanılarak bloklardan nicemleme matrisi oluşturulur. Bu matris tablosu ile standart JPEG nicemleme tablosu karşılaştırılır. Uyumsuz herhangi bir blok varlığı, nesnenin stego olduğunu gösterir [2].

Steganalistler eğer gizleme yöntemini biliyorlarsa istatistiksel teknikler de kullanırlar. Sıralı EAB veri gizleme yöntemi kullanılmışsa, Ki-kare analizi ile gri seviye görüntülerden değişen piksel çiftleri tespit edilebilir. Renkli görüntülerde ise veri gizleme yakın renk çiftlerinin sayısını artırır. Bu sebeple, renk çiftleri analiz edilerek mesajın varlığı tespit edilebilir [2]. RS analizi [4] hem renkli hem de gri görüntülerin steganalizinde kullanılabilir. Bu yöntemde görüntü gruplara ayrılır ve her grubun gürültüsü piksellerin EAB'leri çevrilerek ölçülür. Literatürde steganaliz için çok fazla yöntem önerilmiştir. Genel olarak önerilen yaklaşımlar iki gruba ayrılabilir. İlk gruptaki yaklaşımlarda, yukarıda bahsedildiği gibi istatistiksel öznitelikler taşıyıcı ve/veya stego görüntülerden elde edilir ve bunlar birbirleri ile karşılaştırılır. İkinci grupta ise makine öğrenmesi yaklaşımları ile görüntülerden elde edilen öznitelikler kullanılarak sınıflandırıcı önce eğitilir ve ardından test edilir. Öznitelik çıkarımında ortalama, kovaryans, basıklık, çarpıklık, histogram analizi gibi istatistiksel değerler ya da kovaryans matrisi, gri seviye eş oluşum matrisi (korelasyon, enerji, homojenlik, entropi vb.) ve farklı benzerlik ölçme değerleri (piksel farkı, korelasyon, kenar, spektral-uzaklık, içerik, insan-görme sistemi gibi yöntemlere dayalı ölçümler) kullanılabilir [2, 5-6]. Makine öğrenmesiyle yapılan steganalizde, en sık kullanılan sınıflandırıcılar destek vektör makineleri (DVM) ve yapay sinir ağlarıdır (YSA). Ayrıca, öznitelik analizi gerektirmeyen, ham görüntüleri giriş olarak kullanan evrişimsel sinir ağı (ESA) ve oto kodlayıcı gibi derin öğrenme (DL: Deep Learning) mimarileri steganalizde son yıllarda kullanılmaktadır [1-2, 8]. Literatürde BOSSbase, BOWS2 ve ImageNet vb. veri setlerindeki görüntüler kullanılarak veri gizleme ve steganaliz deneyleri uzamsal ya da frekans düzleminde gerçekleştirilmektedir. Araştırmacılar, uzamsal düzlemde sıklıkla WOW (Wavelet Obtained Weights), HUGO (Highly Undetectable steGO) S-UNIWARD, HILL ve MiPOD gibi yöntemler kullanırken, frekans düzleminde UED, UERD, J-UNIWARD yöntemleri kullanılarak veri gizlemektedir. Ayrıca, sınıflandırıcının gizli mesaj varlığını tespit etmede zorlandığı gizleme kapasite sınırını ortaya koymak için görüntülere 0.1-1.0 aralığında farklı bpp (bit per pixel) oranlarında veri gizlenerek deneyler yapılır. Makine öğrenmesi ya da istatistiksel tabanlı steganaliz yaklaşımlarda en temel güçlük öznitelik analizidir. Karmaşık özniteliklerle beslenen makine öğrenmesi yaklaşımları taşıyıcı görüntülerin birbirlerinden farklı olan özelliklerinin belirlenmesinden ziyade mesajın gizlenmesi sonrasında bu görüntü özelliklerinin nasıl değişeceğini öğrenmeye çalışmaktadır.

Medikal görüntü steganografisi, temelde medikal görüntülerin dosya başlık kısmında yer alan hasta kişisel bilgilerinin buradan silinip görüntü pikselleri içerisine yalnız yada hastanın farklı medikal kayıtları (biyolojik sinyaller, hasta raporları, doktor yorumu gibi) ile birlikte gizlenmesini amaçlar. Böylece, üçüncü parti kişilere karşı medikal görüntüler içerisinde yer alan tüm bilgilerin korunması sağlanmış olur. Son yıllarda medikal görüntü steganografisi için pek çok çalışma önerilmiştir [7-8], ancak steganalizle ilgili çalışma yoktur. Steganaliz, saldırılara karşı daha dayanıklı steganografi tekniklerinin geliştirilmesini sağlar. Ayrıca, kötücül saldırılarda medikal görüntüler araç olarak kullanılıyorsa bu durum medikal steganalizi ile tespit edilebilir. Bu sebeple, bu çalışmada medikal görüntü steganalizi için DL tabanlı bir model

geliştirilmesi amaçlanmıştır. Önerilen ESA modeli DICOM uzantılı beyin Manyetik Rezonans (MR) görüntüleri ile eğitildikten sonra eğitim setinde bulunmayan verilerle test edilmiştir. Stego görüntülerin oluşturulmasında uzamsal düzlemde 6 farklı EAB tekniği kullanılmıştır ve farklı bpp oranlarında veri gizlenmiştir.

Bu kısımda verilen genel bilgileri, literatür taraması takip etmektedir. Bölüm 2'de çalışmanın veri gizleme stratejisi ve ESA mimarisinin detayları ortaya konmuştur. Bölüm 3'te elde edilen deneysel sonuçlar verilmiştir. Son bölümde, çalışma değerlendirilmiş ve gelecek çalışmalar için öneriler aktarılmıştır.

1.1. Literatür Taraması (Literature Review)

Literatürde medikal görüntülerin steganalizi ile ilgili çalışma bulunmadığından bu kısımda DL tabanlı görüntü steganalizi için önerilen yaklaşımlar incelenmiştir. Qian ve ark. [10] BOSSbase ve ImageNet'deki görüntüleri kullanarak uzamsal düzlemde veri gizlemişler ve bu görüntülerin analizi için Gaussian Nöron ESA (GNESA) mimarisini önermişlerdir. Kullanılan ESA'da ReLU ya da sigmoid gibi aktivasyon fonksiyonları yerine Gaussian fonksiyonu tercih edilmiştir. Çalışmanın sonuçları literatürde görüntü steg analizinde yaygın olarak kullanılan uzamsal zengin model (SRM:Spatial Rich Model) yöntemi ile kıyaslandığında, önerilen sınıflandırıcının performansının başarılı olduğu görülmektedir. Araştırmacılar diğer bir çalışmada [11] BOSSbase görüntülerine WOW ve S-UNIWARD yöntemleri ile 0,1-0,5 bpp oranlarında veri gizleyerek 5 farklı veri seti oluşturmuşlardır. Bu veri setleri ile eğitilen her bir ESA'nın ağırlıkları bir sonraki ağa transfer edilmiştir. ESA'larda ön işlemede sabit yüksek geçiren filtreler kullanılmıştır. Buna göre, WOW yöntemi ile 0,4 bppli görüntüler için ESA'nın elde ettiği minimum sezme hatası (DE: Detection Error) %24,87'dir. S-UNIWARD yönteminin 0,5 bpp'li veriler için elde ettiği minimum sezme hatası ise %22,05'tir.

Xu ve ark. [12] iki uzamsal gizleme yöntemi (S-UNIWARD ve HILL) kullanarak 0,1 ve 0,4 bpp oranlarında BOSSbase veri tabanı görüntülerinden stego görüntüler oluşturmuşlardır. Çalışmada önerilen ESA modelinde 5 evrişim katmanı, 1 tam bağlantılı katman kullanılmıştır. İlk evrişim katmanında, istatistiksel modelleme için mutlak aktivasyon katmanı (ABS: Absolute Activation Layer) kullanılmıştır. Sonraki iki katmanda ağın ezberlemesini engellemek amacıyla hiperbolik tanjant (tanh) aktivasyon fonksiyonunu tercih etmişlerdir. Tüm evrişim katmanlarında aktivasyon katmanı öncesi yığın normalizasyon katmanı (BN: Batch Normalization) eklenmiştir. 0,4 bpp gizleme oranı için S-UNIWARD ve HILL yöntemlerinde ESA'nın bulduğu ortalama doğruluk değerleri sırasıyla %80,24 ve %79,24'tür. Araştırmacılar diğer bir çalışmalarında [13] bu yöntemi topluluk sınıflandırıcısı (EC: Ensemble Classifier) [14] için temel olarak kullanmışlardır ve SRM ile kıyaslandığında başarılı sonuçlar elde etmişlerdir. Liu ve ark. [15] BOSSbase görüntülerinde S-UNIWARD ve WOW yöntemleri ile veri gizlemişlerdir ve bu görüntüleri SRM ve ESA'yı birleştirdikleri bir sınıflandırıcı ile analiz etmişlerdir. Böylece, literatüre göre doğruluk değeri yaklaşık olarak %2 oranında iyileştirilmiştir. Ye ve arkadaşları [16] tasarladıkları ESA'da evrişim katmanlarından önce artık (residual) hesaplama kullanılmıştır. Ayrıca, katmanlarda ReLU'dan türetilen yeni bir transfer fonksiyonu tercih edilmiştir. Çalışmanın WOW, S-UNIWARD, ve HILL yöntemleri ve farklı bpp oranları için performans sonuçları yüksektir.

Sharifzadeh ve ark. [17] BOSSbase veri setinde 0,1 ve 0,4 bpp için oluşturdukları stego görüntülerini kullanarak ESA modelini eğitmişlerdir. Ağın sezme hatası, düşük bpp oranında diğerine göre daha düşüktür. Salomon ve ark. [1] BOSSbase veri tabanında WOW, HUGO ve J-UNIWARD yöntemleriyle 0,1 ve 0,4 bpp oranlarında veri gizlemişlerdir. Çalışmada önerilen ESA'da yüksek sayıda filtre içeren evrişim katmanları kullanılsa da 0,1 bpp için ESA başarılı olamamıştır. 0,4 bpp için ESA sınıflandırıcısının WOW, HUGO ve J-UNIWARD yöntemleri için elde ettiği doğruluk değerlerini sırasıyla %95,44, %97,09 ve %95,44'tür.

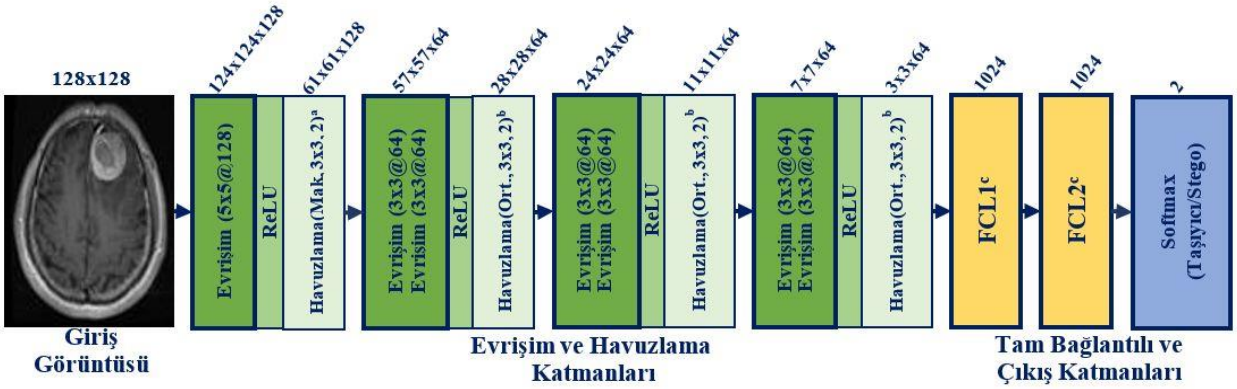
Ozcan ve ark. [18] BOSS ve BOWS2 veri tabanlarında HUGO ve WOW yöntemleri kullanarak 0,1-1,0 bpp oranlarında veri gizlemişlerdir. Çalışmada öncelikle, Resnet50 ağından transfer edilerek oluşturulan ESA mimarisi, EAB ile veri gizlenen görüntüler kullanılarak eğitilmiştir. Ardından eğitilmiş bu temel ağ en büyük bpp oranından başlıyarak ve ağın ağırlıkları bir sonraki bpp için eğitilecek ESA'ya aktarılarak 10 ardışık eğitim gerçekleştirilmiştir. Çalışmada düşük bpp oranları ile eğitilen ESA'ların performansının düşük olduğu görülmüştür. Ayrıca ardışık ağırlık transferi yapılmadan da eğitimler gerçekleştirilmiş ve transfer öğrenme ile daha yüksek sonuçlar elde edilmiştir. Wu ve ark. [19] görüntü steganalizi için artık öğrenme tabanlı yeni bir ESA modeli önermişlerdir. Modelde görüntülerdeki istatistiksel özellikleri ortaya çıkarmak için fazla sayıda katman kullanılmıştır. Artık öğrenme böylece görüntülerdeki gizli mesajın sebep olduğu stego sinyalin varlığını korumuştur ve stego ve taşıyıcı görüntülerin ayırt edilmesini sağlamıştır. Taşıyıcı ve stego görüntüler arasındaki farklılıklar ESA modellerinde yalnızca ön işleme katmanlarında belirginleşir. Artık bloklar kullanılarak bu farklılığın sonraki katmanlara aktarılması amaçlanır. Bu sebeple [20]'de da artık DL mimarisi (RestegNet) önerilmiştir. Bu modelde, artık bağlantı tabanlı keskinleştirme ve yumuşatma blokları ile sırasıyla steg sinyalin algılanması ve özellik haritalarının steg sinyali ayrıştıracak şekilde alt örneklenmesi sağlanılmıştır. Çalışmada yüksek performans değerleri elde edilmiştir.

Literatürdeki ilgili bu çalışmalara göre, steganografi ile veri gizleme sonrası stego görüntüsü üzerinde düşük seviyede bozulma oluşur. Bu sebeple, görüntü steganalizinde görüntüdeki bu bozulmadan yola çıkarak steg sinyalin varlığını tespit etmek zordur. DL katmanlarında fazla sayıda filtre kullanarak bu sinyali belirlemek mümkündür. Yapılan çalışmalarda farklı bpp

oranları ile eğitilen ağların ağırlıklarının ardışık olarak diğer ağlara transfer edilmesi ESA modellerinin genelleme performansını artırmıştır. ESA mimarisinde artık ağ bloklarının kullanılması da steg sinyalinin tespitinde faydalıdır.

2. MATERYAL VE METOT (MATERIAL AND METHOD)

Bu çalışmada, steganaliz için "seçilen stego saldırısı" na göre bilinen stego nesnesi ve veri gizleme algoritması



Şekil 1. Önerilen ESA modelinin akış diyagramı, [a] Mak: maksimum havuzlama, [b] Ort: ortalama havuzlama, [c] FCL: tam bağlantılı katman (Flowchart of the proposed CNN model, [a] Mak: max pooling, [b] Ort: average pooling, [c] FCL: fully connected layer)

senaryosu kullanılarak oluşturulan görüntülerle sınıflandırıcı eğitimi gerçekleştirilmiştir (Şekil 1). Medikal steganaliz için mevcut bir veri seti olmadığından DICOM uzantılı radyolojik görüntülerden bir veri seti hazırlanmıştır [21].

DICOM görüntülerin dosya başlık kısmında yer alan hasta kişisel bilgileri (hastanın adı ve soyad, kimlik no, doğum tarihi, cinsiyeti, kilosu ve adresi), görüntülere ait seri bilgileri (seri tarihi, saati ve açıklaması) ve çalışma bilgileri (çalışma tarihi, ID, modalitesi ve açıklaması) kullanılarak farklı bpp oranları için gizli mesajlar oluşturulmuştur [6-7]. Steganografide mesajı olası saldırıları karşı korumak amacıyla şifreleme yöntemlerinden yararlanılır. Bu sebeple, gizli mesaj 128-bitlik bir anahtar ile Rijndael simetrik şifreleme aracılığıyla mesajın güvenliğini sağlamak amacıyla şifrelenmiştir. Daha sonra, EAB ile 6 farklı şekilde 0,05, 0,1, 0,2, 0,5 ve 1,0 bpp oranlarında görüntülere veri gizlenerek stego görüntüler oluşturulmuştur. Veri seti ve EAB ile veri gizlemenin detayları aşağıda verilmiştir.

2.1. Veri Seti (Dataset)

Bu çalışmada, figshare beyin veri setinde bulunan 233 hastanın seçilen 3015 adet beyin MR görüntüsü taşıyıcı nesne olarak kullanılmıştır [21]. Veri setindeki görüntülerin dosya başlık kısmında hasta kişisel bilgileri mevcut olmadığından her görüntü için rassal bilgiler oluşturulmuştur. Çalışmada 512x512 boyutlarında olan orjinal görüntüler 128x128 çözünürlüğe yeniden boyutlandırılmıştır. Bu görüntüler üzerinde gerçekleştirilen veri çoğaltma ve veri gizleme işlemleri sonrasında veri setinde 93465 adet taşıyıcı görüntü ve 90450 adet stego görüntü sayısına ulaşılmıştır. Veri seti %60, %30 ve %10 oranlarında eğitim, test ve doğrulama olarak ayrıştırılmıştır. Veri gizleme işlemleri MATLAB'da, ESA analizleri ise 3.6 python dili üzerinde Keras DL kütüphanesi kullanılarak Google COLAB'da gerçekleştirilmiştir.

Genel görüntü steganaliz çalışmalarında farklı bpp oranları için ayrı ayrı veri setleri hazırlanmıştır. Ancak bu çalışmada, medikal görüntü steganalizi için eğitilen ESA'ların farklı veri gizleme oranlarını tahmin etme başarısı üzerine odaklanılmamıştır. Bu sebeple, ESA'nın eğitiminde kullanılacak tüm stego veriler tek bir veri setinde bir araya getirilmiştir. Çalışmada, her bir görüntüden 30 (6 EAB yöntemi ve 5 bpp oranı) farklı stego görüntü oluştuğundan taşıyıcı ve stego görüntüler arasındaki sınıf dengesizlik problemini engellemek amacıyla piksel seviye ve afin dönüşüm veri çoğaltma teknikleri kullanılmıştır. Bu teknikler aşağıdaki gibidir.

a) İki Çevirme (flip): Yatay ve dikey çevirme
b) 12 Döndürme (rotasyon): açılar (-90, -45, -40, -30, -20, -10, 10, 20, 30, 40, 45, 90)
c) 8 Öteleme (translation): X,Y koordinatları (5,5), (-5,-5), (10,10), (-10,-10), (20,20), (-20,-20), (30,30), (-30,-30)
d) 4 Keskinleştirme (sharpening): miktarlar 0,5, 1, 1,5, 2.
e) 4 Blurlaştırma (blurring): miktarlar 0,25, 0,5, 1, 1,5.

2.2. En az Ağırlıklı Bit ile Veri Gizleme (Data Hiding with Least Significant Bit)

Görüntü steganografisinde uzamsal düzlemde en sık kullanılan yöntem; hızlı, kolay ve yüksek kapasiteli olması sebebiyle en az ağırlıklı bite (Least Significant Bit-LSB) gizleme yöntemidir. Gizleme işlemi, görüntünün seçilen pikselinin EAB olarak belirlenen bitine, mesajın bitinin yerleştirilmesiyle gerçekleştirilir. Örneğin, gri seviye değeri 150 olan bir pikselin ikilik karşılığı 10010110, gizlenmek istenen mesaj biti **1** ve EAB 0. bit olsun. Mesaj biti, pikselin 0. bitine yerleştirildiğinde 10010111 ikilik sayısı için 151 değeri elde edilir. EAB ile veri gizleme Eş.1' de formülize edilmiştir [8].

$$Y_i = 2\left|\frac{X_i}{2}\right| + m_i \quad (1)$$

m_i mesajın i. bitini, x_i seçilen pikselin gri seviye değeri ve Y_i ise mesaj gizleme sonrası oluşan stego görüntündeki ilgili pikselin gri seviye değerini ifade etmektedir. EAB yönteminde mesaj, görüntü piksellerine sıralı ya da rassal olarak gizlenebilir. Medikal bir görüntüde uzamsal düzlemde gizleme kapasitesi, *Yükseklik x Genişlik x Piksel Bayt Miktarı* ile hesaplanır. Örneğin, 128x128 boyutlu, her bir pikselini 2 bayt olan bir DICOM dosyasına 128x128x2=32 768 bit (1.0 bpp oranında) veri gizlenebilir. Piksellerin 0-4 aralığındaki bitlerinden en az biri, ya da gizleme kapasitesini artırmak amacıyla birden fazlası mesaj biti gizlemek için kullanılabilir. Ancak steganografi yönteminin farkedilmeme özelliğini sağlamak amacıyla genelde görüntü pikselinin her baytına ait 0. biti EAB olarak kullanılmaktadır [8].

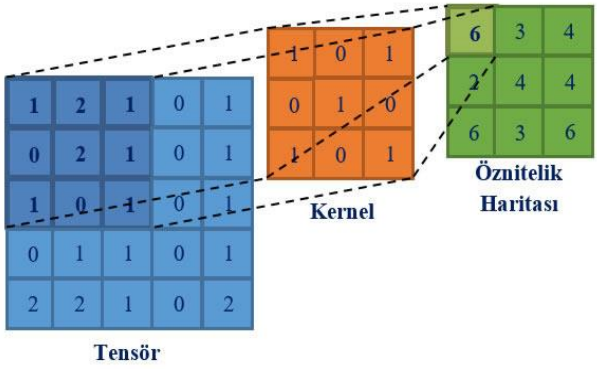
Bu çalışmada, [22]'de önerildiği gibi medikal görüntülere 6 farklı EAB yöntemi ile veri gizleme yapılmıştır. Bu yöntemler aşağıda sıralanmıştır. $X_{(1,1)}$ görüntünün ilk satır ve sütunundaki piksel değerini, $X_{(m,n)}$ görüntünün son satır ve sütunundaki piksel değerini, μ görüntünün ortalama değerini ifade etmektedir.
(1) EAB1: $X_{(1,1)}$ pikselden başlayarak soldan-sağa doğru sıralı veri gizleme,
(2) EAB2: $X_{(m,n)}$ pikselden başlayarak sağdan sola doğru sıralı veri gizleme,
(3) EAB3: $X_{(1,1)}$ pikselden başlayarak yukarıdan aşağıya doğru sıralı veri gizleme,
(4) EAB4: $X_{(m,n)}$ pikselden başlayarak aşağıdan yukarıya doğru sıralı veri gizleme,
(5) EAB5: μ değerinin üstünde olan piksellere (ilgi bölgesi) sıralı veri gizleme,
(6) EAB6: μ değerinin altında olan piksellere (ilgi bölgesi olmayan-arkaplan) sıralı veri gizleme [22].

2.3. Evrişimsel Sinir Ağı (Convolutional Neural Network)

DL, YSA tabanlı büyük veri ve hesaplama gücü gerektiren, basit kavramlardan yola çıkarak karmaşık kavramları birleştiren bir makine öğrenmesi yöntemidir [22]. DL'nin temelini oluşturan çok katmanlı YSA, girdileri (X_1,...X_n) çıktılara (Y_m) eşleyen matematiksel bir modeldir. YSA, temelde karmaşık analizler sonucu elde edilen özniteliklerin girildiği giriş katmanı, toplam giriş bilgisini nöron olarak adlandırılan proses elemanlarında işleyerek çıkışa ileten gizli katman/katmanlar ve çıkış katmanından oluşur. Çok katmanlı YSA bir kavramın genellemesini, ağın ürettiği çıktı ile gerçek çıktı arasındaki hatayı $(e_j(n) = d_j(n) - o_j(n))$ minimize eden bir amaç fonksiyonu aracılığıyla ağın katmanları arasındaki ağırlıkları (w) ve nöronların sapma değerlerini (b) güncelleyerek gerçekleştirir.

ESA ise son yıllarda özellikle bilgisayarla görmede ve tıpta radyolojide sınıflandırma, bölütleme ve algılama problemlerinin çözümünde yaygın olarak kullanılan bir DL mimarisidir. ESA evrişim katmanları, havuzlama katmanları ve tam bağlantılı katmanlar gibi çoklu yapı bloklarının birleşiminden oluşmaktadır ve ağa sunulan giriş verisinin geri yayılım yoluyla özelliklerini otomatik ve uyarlamalı olarak öğrenmektedir. ESA, harici öznitelik analizi gerektirmez ancak genelleme için mimarisinde milyonlarca parametre ile öğrenebilmesinde büyük veriye ihtiyaç duyar. Modeldeki öğrenme sürecinin hesaplama maliyeti yüksek olduğundan grafik işlem birimi/birimleri (GPUs) gerektirir. ESA'nın ilk iki katmanını evrişim ve havuzlama katmanları oluşturmaktadır. Öznitelik haritalarını veren evrişim katmanında, kernel adı verilen 3x3 veya 5x5 boyutlarındaki bir filtrenin, tensör adı verilen giriş görüntüsü üzerinde dolaştırılarak doğrusal bir işlem olan evrişim işlemi gerçekleştirilir. Şekil 2'de görülen evrişim işlemi görüntünün özelliklerini öğrenerek pikseller arasındaki komşuluk ilişkisini korur [23-28]. Matematiksel olarak ESA'da (i,j). konumda yer alan öznitelik değeri $z^l_{i,j,k}$; k. öznitelik haritası ve l. katman için Eş. 2 ile hesaplanır [23, 28].

$$z^l_{i,j,k=} {w^l_k}^T x^l_{i,j} + b^l_k \quad (2)$$



Şekil 2. 5x5'lik tensör ile 3x3'lük kernel üzerinde adım 1 ile gerçekleştirilen evrişim işlemi [27]
(The convolution process performed with step 1 on a 3x3 kernel with a 5x5 tensor [27])

Eş. 2'deki w^l_k ve b^l_k sırasıyla k. filtre ve l. katmandaki ağırlık vektörünü ve sapma vektörünü ifade etmektedir. $x^l_{i,j}$ ise l. katmanındaki (i,j) konumundaki girişi ifade etmektedir. ESA içinde evrişim ile elde edilen öznitelik değerleri sigmoid, tanh ya da ReLU gibi bir aktivasyon fonksiyonundan geçirilerek $(a(z^l_{i,j,k}))$ doğrusal olmayan hale getirilir [23, 27-31].

Havuzlama katmanında, öznitelik haritalarının boyutlarını ve ağın öğrenebilir parametre sayısını azaltan alt örnekleme işlemi gerçekleştirilir (Eş. 3). Bu katmanda öğrenebilir parametre bulunmaz. Hiperparametreler, ESA eğitim süreci başlamadan önce geliştirici tarafından ayarlanması gereken değişkenleri ifade eder. Bu sebeple, havuzlama ve evrişim katmanlarında kullanılan filtre boyutu, adım ve dolgu değerleri ESA geliştiricileri tarafından optimize edilmesi gereken hiperparametrelerdir [27, 32].

$$y^l_{i,j,k=} pool\left(a^l_{m,n,k}\right), \forall (m,n) \in R_{ij} \quad (3)$$

R_{ij} giriş parçasının (i, j). konumundaki yerel komşularıdır. Havuzlama katmanlarında yaygın olarak ortalama ve maksimum havuzlama işlemleri tercih edilmektedir [28]. ESA'da son evrişim ya da havuzlama katmanından sonra öznitelik haritalarını düzleştirerek tek boyutlu vektöre dönüştüren tam bağlantılı katmanlar kullanılır [23-32]. Katmanın her bir çıktısı farklı bir ağırlık ile çarpılarak bir sonraki tam bağlantılı katmanın tüm girişlerine aktarılır. Katmanlarda her nöronda net giriş bilgisi ReLU gibi bir aktivasyon fonksiyonundan geçirilir [27].

Son katman ise problemin sınıf sayısıyla aynı sayıda nörona sahiptir ve burada genellikle softmax fonksiyonu ile çıktıların olasılıkları hesaplanır. θ ağırlık ve sapma gibi ağın tüm öğrenebilir parametrelerini sembolize etsin. Spesifik bir problem için oluşturulan ESA'da optimum parametreler amaç/ceza fonksiyonu (Eş. 4) minimize edilerek hesaplanır. $x^{(n)}$ *n.* girişi, $y^{(n)}$ bu girişe ait *n.* gerçek çıkışı ve $o^{(n)}$ ise ESA'nın ürettiği çıkışı göstermektedir [28].

$$\mathcal{L} = \frac{1}{N}\sum_{n=1}^{N} l(\theta; y^{(n)}, o^{(n)}) \quad (4)$$

Ceza fonksiyonunu minimize etmek için SGD, ADAM, RMSprop gibi optimizasyon yöntemleri kullanılarak iteratif olarak öğrenebilir parametreler güncellenir ve böylece ağın eğitimi gerçekleştirilir [27-28]. Ancak, ağ eğitiminde ezberleme problemi ile karşılaşılabilir. Eğitim süresince ezberleme olup olmadığı eğitim ve doğrulama veri setlerinin hata ve doğruluklarının izlenmesi ile tespit edilir. Ezberleme varsa öncelikle eğitim veri setindeki örnek sayısını artırmak gerekir. Bu mümkün değilse, veri çoğaltma teknikleri ile veri seti örnek sayıları sınıf dengesi sağlanacak şekilde artırılabilir [33]. Ayrıca, ezberlemeyi azaltmak için dropout, ağırlık azaltma, yığın normalizasyon gibi düzenleme ya da mimarinin karmaşıklığının azaltılması yolları alternatif olarak kullanılabilir [27].

2.4. Karşılaştırma Yöntemleri (Comparison Methods)

Çalışmada medikal görüntülerde gizli mesaj olup olmadığının tespiti için geliştirilen ESA mimarisinin test verileri üzerindeki başarısı, eğri altında kalan alan (AUC: area under curve), duyarlılık (sensitivity), özgüllük (specificity), doğruluk (accuracy), kesinlik (precision), hassasiyet (recall) ve F1 ölçüm değerleri ile belirlenmiştir [7-8, 34-35]. Medikal test analizlerini değerlendirmede kullanılan karışıklık matrisinde, TP (True Positive): doğru pozitif, FP (False Positive): yanlış pozitif, TN (True Negative): doğru negatif, FN (False Negative): yanlış negatifi göstermektedir. Buna göre Eş 5'te verilen kesinlik değeri, bu problem için gerçek stego görüntülerinin kaçının doğru tespit edildiğini gösterir [35].

$$Precision = TP/(TP + FP) \quad (5)$$

Hassasiyet değeri, stego görüntülerinin doğru tespit edilme oranını verir (Eş. 6) [35].

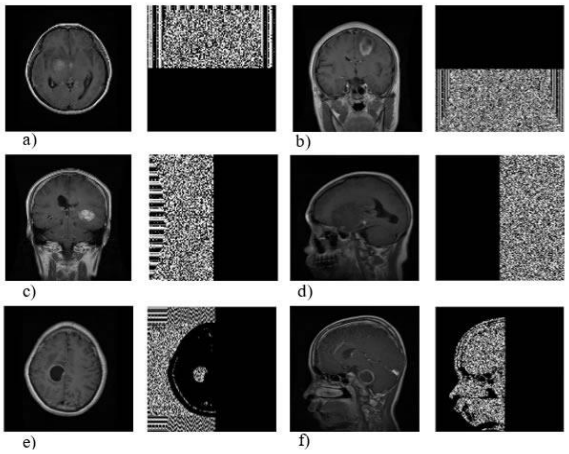
$$Recall = TP/(TP + FN) \quad (6)$$

F1 ölçümü, kesinlik ve hassasiyet değerlerinin harmonik ortalamasını göstermektedir (Eş. 7) [35].

$$F1 = 2\frac{Precision.Recall}{Precision+Recall} = 2\frac{TP}{2TP+FP+FN} \quad (7)$$

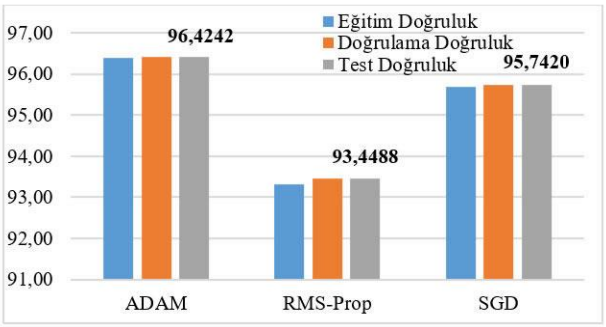
3. ELDE EDİLEN SONUÇLAR VE TARTIŞMA (OBTAINED RESULTS AND DISCUSSION)

Bu çalışmada, medikal görüntü steganografide yaygın olarak kullanılan ve veri gizleme için piksel seçimlerinin farklılaştırıldığı 6 EAB tekniği kullanılmıştır. Şekil 3'den, bu teknikler ile 0,5 bpp oranında veri gizleme sonrasında elde edilen stego görüntüler ve mesajı gösteren fark görüntüler görülmektedir. Çalışmada, medikal görüntülerde gizli mesajın varlığını tespit etmek için Şekil 1'de verilen ESA mimarisi stego ve taşıyıcı görüntüler ile eğitilmiş ve test edilmiştir. Eğitim süresince ağın ezberlemesi, eğitim ve doğrulama veri setlerinin hata ve doğruluğu izlenerek tespit edilmiştir. Ezberlemeyi engellemek ve aynı zamanda ağın öğrenebilir parametre sayısını azaltmak için tam bağlantılı katmanlardan sonra 0,2'lik seyreltme gerçekleştiren dropout kullanılmıştır. Tüm ESA mimarileri 10 kez çalıştırılarak optimum sınıflandırıcı tespit edilmiştir. Yığın miktarı 16, öğrenme oranı 0,001 iken ADAM, RMSprop ve SGD optimizasyon algoritmaları ile ESA'nın sınıflandırma başarısı ortaya konmuştur. Buna göre Şekil 4'te ADAM, RMSprop ve SGD yöntemlerinin test doğruluk yüzdeleri sırasıyla %96,4242, %93,4488, %95,7420 olarak bulunmuştur.



Şekil 3. Stego ve fark görüntüler
(Stego and difference images)

Tablo 1'de optimizasyon yöntemlerinin performans sonuçları verilmiştir. Buna göre ADAM yöntemini kullanan ESA'nın AUC, duyarlılık, özgüllük, kesinlik, hassasiyet ve F1 değerleri sırasıyla 0,965, 0,965, 0,965, 0,966, 0,965 ve 0,964'tür. Tablo 1 ve Şekil 4'te verilen sonuçlara göre ADAM yöntemi ile eğitilen ESA daha yüksek performans sonuçları elde etmiştir.



Şekil 4. Optimizasyon yöntemlerinin doğruluk değerleri
(Accuracy values of optimization methods)

Tablo 2'de, ADAM ile optimize edilen ESA'nın stego ve taşıyıcı sınıflar için elde ettiği değerler verilmiştir. Buna göre ESA'nın taşıyıcı medikal görüntüler için kesinlik, hassasiyet ve F1 değerleri sırasıyla 1,00, 0,93 ve 0,96'dır. Çalışmada, stego görüntülerin sınıflandırılmasında bu değerler sırasıyla 0,93, 1,00 ve 0,97 olarak bulunmuştur.

Tablo 1. Optimizasyon yöntemlerinin performans sonuçları
(Performance results of optimization methods)

Yöntem	*AUC*	*Duyarlılık*	*Özgüllük*	*Kesinlik*	*Hassasiyet*	*F1*
ADAM	0,9649	0,9649	0,9649	0,9661	0,9649	0,9642
RMSprop	0,9356	0,9356	0,9356	0,9408	0,9356	0,9343
SGD	0,9582	0,9582	0,9582	0,9601	0,9582	0,9574

Tablo 2. ESA'nın sınıflara göre performans sonuçları
(Performance results of ESA according to classes)

Sınıflar	*Kesinlik*	*Hassasiyet*	*F1*	*TN*	*FP*	*FN*	*TP*
Taşıyıcı	1,0000	0,9297	0,9636	27079	0	1971	26070
Stego	0,9322	1,0000	0,9649	26070	1971	0	27079

Tablo 3'den literatürdeki ilgili çalışmaların sonuçları görülmektedir. Bu çalışmalarda [10-12, 15-18, 20] BOSSbase veritabanında yer alan.pgm uzantılı görüntülere HUGO, WOW ya da S-UNIWARD teknikleri ile farklı bpp oranlarında veri gizlenmiştir. Qian ve ark [10] ESA ile farklı bpp oranlarında HUGO, WOW ve S-UNIWARD için sezme hatalarını sırasıyla %25,7-%33,8, %24,8-%34,3 ve %26,3-%35,9 olarak elde etmişlerdir. Diğer bir çalışmada [11] ESA'nın WOW ve S-UNIWARD yöntemleri için elde ettiği sezme hataları sırasıyla %24,9-%38,4 ve %22,1-%42,9'dur. Ye ve ark. [16] WOW, S-UNIWARD ve HILL yöntemleri için sezme hatalarını sırasıyla %15,5-%39,2, %19,9-%44,5, %25,9-%45,5 olarak elde etmiştir. Salomon ve ark. [1] geliştirdikleri ESA ile farklı bpp oranlarında WOW, HUGO ve J-UNIWARD yöntemleri için doğruluk değerlerini sırasıyla %74,6-%95.4, %74,6-%97,1, %70,9-%95,4 olarak hesaplamışlardır. Diğer bir çalışmada [12] S-UNIWARD ve HILL teknikleri için ESA'nın bulduğu doğruluk değerleri %57,3-%80,2, %58,4-%79,2'dir. Liu ve ark. [15] ESA ve SRM-EC yöntemlerini birleştirdikleri steganaliz modeli ile S-UNIWARD yöntemi için farklı bpp oranlarındaki doğruluk değerlerini %64,0 ve %83,4; WOW yöntemi için doğruluk değerlerini %70,8 ve %86,3 olarak tespit etmişlerdir. Diğer bir çalışmada [17] 0,1 ve 0,4 bpp oranlarında HUGO, S-UNIWARD ve HILL teknikleri kullanılarak veri gizlenmiştir. ESA ile ortalama doğruluk değeri %69,8 olarak elde edilmiştir. Ozcan ve ark. [18] farklı bpp oranlarında HUGO ve WOW yöntemleri kullanarak veri gizlemişlerdir. Transfer öğrenme kullanılan ESA'nın HUGO için elde ettiği F1 değerleri 0,57-0,89 aralığında ve WOW için hesaplanan F1 değerleri ise 0,59-0,85 aralığındadır. You ve ark. [20] geliştirdikleri ESA ile farklı bpp oranlarında S-UNIWARD yöntemi için doğruluk değerlerini %55,7-%79,3 olarak hesaplamışlardır. Buna göre, literatürde BOSSbase görüntüleri ile eğitilen ESA modellerinin farklı bpp oranlarında elde ettiği doğruluk ve F1 değer aralıkları sırasıyla %57,3-%97,1 ve %57,0-%89,0'dur [12, 15, 17-18, 20].

Tablo 3. Literatür Karşılaştırması
(Comparison literature)

Çalışma	*Gizleme Yöntemi*	*bpp*	S*	*Doğruluk (%)*	*Sezme Hatası (%)*
Salomon ve ark. [1]	WOW HUGO J-UNIWARD	0,1 ve 0, 4	ESA	74,6-95.4 74,6-97,1 70,9-95,4	-
Qian ve ark. [10]	HUGO WOW S-UNIWARD	0,3, 0.4, ve 0,5	ESA	-	25,7-33,8 24,8-34,3 26,3-35,9
Qian ve ark. [11]	WOW S-UNIWARD	0,1, 0,2, 0,3, 0,4 ve 0,5	ESA	-	24,9-38,4 22,1-42,9
Xu ve ark. [12]	S-UNIWARD HILL	0,1 ve 0,4	ESA	57,3-80,2 58,4-79,2	-
Liu ve ark. [15]	S-UNIWARD WOW	0,1 ve 0,4	ESA + SRM-EC	64,0-83,4 70,8-86,3	-
Ye ve ark. [16]	WOW S-UNIWARD HILL	0,05, 0.1-0.5	ESA	-	15,5-39,2 **19,9-44,5** **25,9-45,5**
Sha.ve ark. [17]	HUGO S-UNIWARD HILL	0,1 ve 0,4	ESA	69,8	-
Ozcan ve ark.[18]	HUGO WOW	0,1-1,0	ESA	57,0-89,0 59,0-85,0 (F1)	-
You ve ark. [20]	S-UNIWARD	0,1-0,4	ESA	55,7-79,3	
M.Ozcan ve ark. [22]	LSB	0,05, 0,1, 0,2, 0,5, ve 1,0	AKD+ DVM	99,28	-
Bu çalışma	**LSB**	**0,05, 0,1, 0,2, 0,5, ve 1,0**	ESA	**96,42**	-

S*: Sınıflandırıcı

Literatürde medikal görüntü steganografi için çok fazla çalışma mevcutken steganalizi için çok az sayıda çalışma mevcuttur. M. Ozcan ve arkadaşları [22] medikal görüntü steganalizi için DVM yöntemi ile gizli mesajın varlığını sınıflandırmışlardır. Önerilen yöntemin özgüllük, duyarlılık, AUC ve doğruluk değerleri sırasıyla 0,994, 0,992, 0,993 ve 0,993'tür. DVM'in giriş vektörü, Liu ve arkadaşları tarafından önerilen [36] AKD dönüşümü ile elde edilmiştir ve 216 öznitelik içerir. Ancak, burada kullanılan öznitelik analizi karmaşıktır ve her bir hastanın görüntü serisi için işlem maliyeti saatler süren yüksek analizler içermektedir. Bu çalışmada ise karmaşık ve maliyetli öznitelik analizleri olmaksızın DL tabanlı steganaliz gerçekleştirilmiştir. Önerilen ESA modelinin doğruluk, AUC, duyarlılık, özgüllük, kesinlik, hassasiyet

ve F1 değerleri sırasıyla %96,4, %96,5, %96,5, %96,5, %96,6, %96,5 ve %96,4'tür. Bu değerler literatürdeki BOSSBase ile gerçekleştirilen çalışmalara [12, 15, 17-18] göre yüksek, medikal görüntü steganaliz için önerilen DVM modeline [22] göre maliyetli öznitelik analizleri olmaksızın elde edildiğinden anlamlıdır.

4. SONUÇLAR (CONCLUSION)

Literatürde son yıllarda medikal verilerin güvenliğinin sağlanmasında steganografi yöntemleri önerilmektedir. Ancak, medikal veriler için hem gizli mesaj varlığını belirleyecek ve dolayısıyla hem de steganografi yöntemlerinin gelişmesini teşvik edecek steganaliz çalışması azdır. Görüntü steganalizi için önerilen mevcut sınıflandırıcılar, BOSSbase gibi veri setleri için uzamsal ya da frekans düzlemde veri gizleme yapan yöntemleri analiz etmektedir. Makine öğrenmesi tabanlı bu sınıflandırıcılar karmaşık ve maliyetli öznitelik analizleri gerektirmektedir. Bu sebeple, bu çalışmada harici öznitelik analizine gerek duymayan DL mimarisi olan ESA ile medikal görüntü steganalizi gerçekleştirilmiştir. Çalışmada EAB tekniği kullanılarak, figshare veri setinde farklı oranlarda veri gizlenmiştir. Önerilen ESA modeli mesajın varlığını tespit etmek için taşıyıcı ve stego görüntülerle eğitilmiş ve test edilmiştir. ESA mimarisi, test veri seti üzerinde 0,964 doğruluk değeri elde etmiştir. Buna göre bu çalışmada, DL mimarisi olan ESA'nın medikal görüntü steganalizinde kullanılabileceği ilk kez gösterilmiştir.

Gelecek çalışmalarda, farklı DL mimarileri medikal görüntü steganalizi için geliştirilebilir.

KAYNAKLAR (REFERENCES)

[1] M. Salomon, R. Couturier, C. Guyeux, J.-F. Couchot, J.M. Bahi, "Steganalysis via a Convolutional Neural Network Using Large Convolution Filters for Embedding Process with Same Stego Key: A Deep Learning Approach For Telemedicine", **European Research in Telemedicine/La Recherche Européenne en Télémédecine,** 6, 79-92, 2017.

[2] K. Karampidis, E. Kavallieratou, G. Papadourakis, "A Review of Image Steganalysis Techniques for Digital Forensics", *Journal of Information Security and Applications*, 40, 217-235, 2018.

[3] M. Bilgin, "Steganaliz", **Akademik Bilişim'14 - XVI. Akademik Bilişim Konferansı Bildirileri**, Mersin Üniversitesi, Mersin, 693-698, 2014.

[4] J. Fridrich, M. Goljan, R. Du, "Reliable detection of LSB steganography in color and grayscale images", **Proceedings of the 2001 workshop on multimedia and security new challenges - (MM&Sec '01)**, 27, 2001.

[5] I. Avcibas, N. Memon, B. Sankur, Steganalysis Based on Image Quality Metrics, **2001 IEEE Fourth Workshop on Multimedia Signal Processing**, 517-522, 2001.

[6] I. Avcıbas, B. Sankur, K. Sayood, "Statistical evaluation of image quality measures", *Journal of Electronic Imaging*, 11(2), 206-223, 2002.

[7] R. Karakis, I. Güler, I. Capraz, E. Bilir, "A novel fuzzy logic based image steganography method to ensure medical data security", *Computers in Biology and Medicine*, 67, 172-183, 2015.

[8] R. Karakis, I. Guler, "Steganography and Medical Data Security", **Cryptographic and Information Security Approaches for Images and Videos**, Cilt 22, Editor: S. Ramakrishnan, CRC Press, USA, ISBN: 9781138563841, 627-660, 2019.

[9] M. Chaumont, "Deep Learning in steganography and steganalysis from 2015 to 2018", **Digital Media Steganography: Principles, Algorithms, Advances**, Editor: M. Hassaballah, Elsevier Inc, 1-45, 2020.

[10] Y. Qian, J. Dong, W. Wang, T. Tan, "Deep learning for steganalysis via convolutional neural networks," **Proc. SPIE 9409, Media Watermarking, Security, and Forensics 2015**, 94090J, 2015.

[11] Y. Qian, J. Dong, W. Wang, T. Tan, "Learning and Transferring Representations for Image Steganalysis Using Convolutional Neural Network", **2016 IEEE International Conference on Image Processing (ICIP)**, 2752-2756, 2016.

[12] G. Xu, H.-Z. Wu, Y.-Q. Shi, "Structural Design of Convolutional Neural Networks for Steganalysis", *IEEE Signal Process. Lett.*, 23(5), 708-712, 2016.

[13] G. Xu, H.-Z. Wu, Y.-Q. Shi, "Ensemble of CNNs for steganalysis: An empirical study", **Proc. 4th ACM Workshop Inf. Hiding Multimedia Secur.**, 103-107, 2016.

[14] J. Kodovsky, J. Fridrich, V. Holub, "Ensemble classifiers for steganalysis of digital media", *IEEE Transactions on Information Forensics and Security***,** 7(2), 432-444, 2012.

[15] K. Liu, J. Yang, X. Kang, "Ensemble of CNN and rich model for steganalysis", **2017 International Conference on Systems, Signals and Image Processing (IWSSIP)**, Poznan, 1-5, 2017.

[16] J. Ye, J. Ni, Y. Yi, "Deep Learning Hierarchical Representations for Image Steganalysis", *IEEE Transactions on Information Forensics And Security*, 12(11), 2545-2557, 2017.

[17] M. Sharifzadeh, C. Agarwal, M. Aloraini, D. Schonfeld, "Convolutional neural network steganalysis's application to steganography", 2**017 IEEE Visual Communications and Image Processing(VCIP)**, 1-4, 2017.

[18] S. Ozcan, A.F. Mustacoglu, "Transfer Learning Effects on Image Steganalysis with Pre-Trained Deep Residual Neural Network Model", **2018 IEEE International Conference on Big Data (Big Data)**, 2280-2287, 2018.

[19] S. Wu, S. Zhong, Y. Liu, "Deep residual learning for image steganalysis". *Multimed Tools Appl.*, 77, 10437-10453, 2018.

[20] W. You, X. Zhao, S. Ma, Y. Liu, "RestegNet: a residual steganalytic network", *Multimed Tools Appl.*, 78, 22711-22725, 2019.

[21] Internet: Figshare brain tumor dataset, https://doi.org/10.6084/m9.figshare.1512427.v5., 21.09.2020.

[22] F.B. Maroof Ozcan, R. Karakis, I. Guler, "Medikal Görüntüler Üzerinde Destek Vektör Makinesi ile Steganaliz, **The 28th IEEE Conference on Signal Processing And Communications Applications**, Gaziantep, 2020.

[23] I. Goodfellow, Y. Bengio, A. Courville, Deep learning (Adaptive computation and machine learning), **The MIT Press**, Cambridge, Massachusetts, 2016.

[24] K. Gurkahraman, R., Karakis, Brain Tumors Classification with Deep Learning using Data Augmentation, *Journal of the Faculty of Engineering and Architecture of Gazi University*, 36 (2), 997-1011, 2021.

[25] M. Yapıcı, A. Tekerek, N. Topaloğlu, "Literature Review of Deep Learning Research Areas", *Gazi Mühendislik Bilimleri Dergisi (GMBD)*, 5(3), 188-215, 2019.

[26] A. Krizhevsky, I. Sutskever, I., G. Hinton, "ImageNet classification with deep convolutional neural networks", **NIPS'12 Proceedings of the 25th International Conference on Neural Information Processing Systems**, 1, 1097-1105, 2012.

[27] R. Yamashita, M. Nishio, R.K.G. Do, K. Togashi, "Convolutional neural networks: an overview and application in radiology", *Insights Imaging*, 9, 611-629, 2018.

[28] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, T. Chen, "Recent advances in convolutional neural networks", *Pattern Recognition*, 77, 354-377, 2018.

[29] Y.A. LeCun, L. Bottou, G.B. Orr, K.-R. Muller, "Efficient backprop", **Neural Networks: Tricks of the Trade-Second Edition**, 9-48, 2012.

[30] V. Nair, G.E. Hinton, "Rectified linear units improve restricted boltzmann machines", **Proceedings of the International Conference on Machine Learning (ICML),** 807-814, 2010.

[31] M. Ayyüce Kızrak ve B. Bolat, "Derin Öğrenme ile Kalabalık Analizi Üzerine Detaylı Bir Araştırma", *Bilişim Teknolojileri Dergisi*, 11(3), 263-286, 2018.

[32] A. Khan, A. Sohail, U. Zahoora, U., A.S. Qureshi, "A survey of the recent architectures of deep convolutional neural networks", *Artificial Intelligence Review*, 53, 5455-5516, 2020.

[33] J. Nalepa, M. Marcinkiewicz, M. Kawulok, Data Augmentation for Brain-Tumor Segmentation: A Review, *Frontiers in Computational Neuroscience*, 13(83), 1-18. 2019.

[34] R. Karakis, M. Tez, Y.A. Kilic, B. Kuru, I. Guler, "A genetic algorithm model based on artificial neural network for prediction of the axillary lymph node status in breast cancer", *Engineering Applications of Artificial Intelligence*, 26(3), 945-950, 2013.

[35] Internet: Precision and recall, https://en.wikipedia.org/wiki/Precision_and_recall, 21.09.2020.

[36] Q. Liu, "Steganalysis of DCT-Embedding Based Adaptive Steganography and YASS", **Proceedings of the 13th ACM Multimedia & Security Workshop**, Niagara Falls, NY, 77-86, 2011.