BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ DOKTORA PROGRAMI

ARTIK BLOK DESTEKLİ U-NET MİMARİSİ KULLANARAK GÖRÜNTÜ STEGANOGRAFİSİ VE GİZLİ VERİ BOYUTUNUN ANALİZİ

HAZIRLAYAN

DİLARA ŞENER

DOKTORA TEZİ

ANKARA – 2024

BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ DOKTORA PROGRAMI

ARTIK BLOK DESTEKLİ U-NET MİMARİSİ KULLANARAK GÖRÜNTÜ STEGANOGRAFİSİ VE GİZLİ VERİ BOYUTUNUN ANALİZİ

HAZIRLAYAN

DİLARA ŞENER

DOKTORA TEZİ

TEZ DANIŞMANI

DOÇ. DR. SELDA GÜNEY

ANKARA – 2024

BAŞKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Elektrik-Elektronik Mühendisliği Anabilim Dalı Doktora Programı çerçevesinde Dilara ŞENER tarafından hazırlanan bu çalışma, aşağıdaki jüri tarafından Doktora Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 26 / 01 / 2024

Tez Adı: Artık Blok Destekli U-Net Mimarisi Kullanarak Görüntü Steganografisi ve Gizli Veri Boyutunun Analizi

Tez Jüri Üyeleri (Unvanı, Adı - Soyadı, Kurumu)	**İmza**
Prof. Dr. Hasan Şakir BİLGE, Gazi Üniversitesi	……..
Prof. Dr. Hamit ERDEM, Başkent Üniversitesi	……..
Doç. Dr. Emre SÜMER, Başkent Üniversitesi	……..
Doç. Dr. Selda GÜNEY, Başkent Üniversitesi	……..
Dr. Öğr. Üyesi Koray AÇICI, Ankara Üniversitesi	……..

ONAY

Prof. Dr. Faruk ELALDI
Fen Bilimleri Enstitüsü Müdürü
Tarih : … / … / 2024

BAŞKENT ÜNİVERSİTESİ

FEN BİLİMLER ENSTİTÜSÜ

DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 20/02/2024

Öğrencinin Adı, Soyadı: Dilara ŞENER

Öğrencinin Numarası: 21520177

Anabilim Dalı: Elektrik-Elektronik Mühendisliği Anabilim Dalı

Programı: Elektrik-Elektronik Mühendisliği Doktora Programı

Danışmanın Unvanı/Adı, Soyadı: Doç. Dr. Selda GÜNEY

Tez Başlığı: Artık Blok Destekli U-Net Mimarisi Kullanarak Görüntü Steganografisi ve Gizli Veri Boyutunun Analizi

Yukarıda başlığı belirtilen Doktora tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 96 sayfalık kısmına ilişkin, 20/02/2024 tarihinde tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 5'dir. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası: …….

ONAY

Tarih: 20/02/2024

Öğrenci Danışmanı

Doç. Dr. Selda GÜNEY

Canım oğluma…

Dilara ŞENER

Ankara-2024

TEŞEKKÜR

Hayatım boyunca yanımda olan ve her daim sevgi, sabır ve anlayışlarını esirgemeyen canım annem, babam ve abime en içten teşekkürlerimi sunarım. Sizin gibi bir ailem olduğu kendimi çok şanslı hissediyorum. Değerinizi kelimelerle ifade edemem.

Yanımda olmanın ötesinde, varlığıyla hayatıma ışık tutan sevgili eşime her anımızda bana sunduğu anlayış, sarsılmaz destek ve sınırsız sevgisi için derin minnettarlığımı sunmak istiyorum. İyi ki hayatımdasın. Hayat seninle çok güzel bir yolculuk.

Ve mucizem canım oğluma, hayatımıza getirdiği mutluluk için teşekkür ederim. Seninle geçirdiğim her dakika, her gülüşün, her bakışın benim için dünyadaki en büyük hazine. Her gün yeni şeyler öğrenmeni, yeni cümleler kurmanı, bizi kendine hayran bırakmanı gözlerim dolarak izliyorum. Senin varlığın her şey demek.

Her zaman ve her anlamda yanımda olan sevgisini ve desteğini hiç esirgemeyen tez danışmanım Doç. Dr. Selda GÜNEY hocama ve değerli katkılarıyla bu süreçte yol gösteren Prof. Dr. Hamit ERDEM ve Doç. Dr. Emre SÜMER hocalarıma en içten teşekkürlerimi sunarım.

ÖZET

Dilara ŞENER

ARTIK BLOK DESTEKLİ U-NET MİMARİSİ KULLANARAK GÖRÜNTÜ STEGANOGRAFİSİ VE GİZLİ VERİ BOYUTUNUN ANALİZİ

Başkent Üniversitesi Fen Bilimleri Enstitüsü

Elektrik-Elektronik Mühendisliği Anabilim Dalı

2024

Günümüz iletişim sistemlerinde veri güvenliği, hayati bir öneme sahiptir. Temel amaç, hassas bilgilerin yetkisiz kişilerin eline geçmeden veya anlaşılamayacak şekilde güvenli bir biçimde hedefe iletilmesidir. Dijital teknolojideki gelişmeler ve cihazların yaygınlaşması veri güvenliği konusunda yeni zorlukları da beraberinde getirmektedir. Özellikle bankacılık, sağlık sektörü ve özel yaşam gibi alanlarda veri güvenliği daha da önem kazanmıştır. Bu bağlamda, steganografi gibi veri gizleme yöntemleri, kötü niyetli erişimlerden korunma amacıyla öne çıkmaktadır. Steganografi, önemli bilgileri fark edilmeden dijital medyaların içine gizleyerek, bu bilgilerin sadece gönderici ve alıcı tarafından bilinmesini sağlayan bir yöntem olması nedeniyle bilgi güvenliği alanında sıkça kullanılan yöntemlerden biridir.

Bu tez çalışmasında, temel amaç, artık blok destekli U-Net mimarisi kullanılarak 256x256 boyutlarındaki renkli mesaj görüntülerinin aynı boyutlardaki kapak görüntülerine etkili bir şekilde gizlenmesini sağlamaktır. Literatürdeki çalışmalarda genellikle görüntü segmentasyonu amacıyla kullanılan klasik U-Net mimarisi, bu çalışmada veri gizleme ve çıkarma amacıyla düzenlenerek kullanılmıştır. Modelin test edilmesi aşamasında, iki farklı analiz yapılmıştır. İlk analiz kapsamında, literatürdeki mevcut çalışmalardan farklı olarak, Linnaeus 5 veri seti kullanılarak 32x32, 64x64, 128x128, ve 256x256 olmak üzere farklı boyutlardaki renkli mesaj görüntülerinin kapak görüntüsü üzerindeki etkisini incelemiştir. İkinci analiz kapsamında, farklı karakteristik özelliklere sahip görüntüler üzerinde genelleştirme yeteneğini ölçmek amacıyla model, Linnaeus 5 veri setine ek olarak ImageNet ve Labeled Faces in the Wild (LFW) veri setleri ile de test edilmiş ve ölçüm metrikleri elde edilmiştir. Elde edilen sonuçlar literatürde yer alan diğer çalışmalarla kıyaslanmıştır. Gerçekleştirilen kapsamlı literatür taramasından elde edilen mevcut bilgiler çerçevesinde, çalışmanın literatürdeki mevcut derin öğrenme algoritmalarına kıyasla Tepe Sinyal-Gürültü Oranı (Peak Signal to Noise Ratio, PSNR) ve Yapısal Benzerlik İndeksi Ölçümü (Structural

Similarity Index, SSIM) açısından umut verici sonuçlar verdiği değerlendirilmektedir. Elde edilen analiz sonuçları hem yüksek veri gizleme kapasitesi hem de yüksek algılanamazlık düzeyinin elde edildiğini göstermektedir.

Tez çalışması kapsamında ayrıca kapak görüntüleri karmaşıklık düzeylerine göre kategorize edilerek iki ayrı kategorideki bu resimlere aynı gizli görüntülerin gizlenmesiyle elde edilen ölçüm sonuçları değerlendirilmiştir. Böylece, karmaşıklık düzeyine göre optimum kapak resmi seçilmesi konusunda istatistiksel bir değerlendirme yapılmıştır.

ANAHTAR KELİMELER: Görüntü steganografisi, Veri gizleme, U-net mimarisi, Derin öğrenme, Bilgi güvenliği, Görüntü İşleme.

ABSTRACT

Dilara ŞENER

IMAGE STEGANOGRAPHY USING U-NET ARCHITECTURE SUPPORTED BY RESIDUAL BLOCKS AND ANALYSIS OF HIDDEN DATA SIZE

Başkent University Institute of Science and Engineering

Department of Electrical and Electronics Engineering

2024

In modern communication systems, data security is of paramount importance. The primary goal is to ensure that sensitive information is transmitted to the intended recipient securely and unintelligibly to unauthorized individuals. Advancements in digital technology and the proliferation of devices have introduced new challenges in data security. In fields such as banking, healthcare, and personal privacy, the importance of data security has become increasingly critical. In this context, methods of data concealment like steganography have gained prominence for their ability to protect against malicious access. Steganography, by discreetly embedding crucial information within digital media, ensures that the data is only known to the sender and the receiver, making it a frequently employed method in the field of information security.

This thesis is primarily focused on employing the U-Net architecture, which is supported by residual blocks, for the efficient concealment of colored message images of 256x256 dimensions within cover images of identical size. The classical U-Net architecture, traditionally used for image segmentation in the literature, has been adapted in this study for data hiding and extraction. During the testing phase of the model, two distinct analyses were conducted. Differing from existing studies, the first analysis investigated the impact of colored message images of various sizes (32x32, 64x64, 128x128, and 256x256) on the cover image using the Linnaeus 5 dataset. The second analysis aimed to measure the generalization capability of the model on images with different characteristics, employing additional datasets such as ImageNet and Labeled Faces in the Wild (LFW), and the results were compared with other studies in the literature. Comprehensive analyses have shown promising results in terms of Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) compared to current deep learning algorithms in the literature, to the

best of our knowledge. The results demonstrate both a high capacity for data concealment and a high level of imperceptibility.

Additionally, as part of the thesis work, cover images categorized based on their complexity levels and evaluates the measurement results obtained by embedding the same secret images into these two different categories. This provides a statistical assessment for selecting the optimum cover image based on complexity level.

KEYWORDS: Image steganography, Data hiding, U-net architecture, Deep learning, Information security, Image Processing.

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR LİSTESİ

Adam	Adaptive Moment Estimation
ANN	Artificial Neural Networks
BPP	Bit Per Pixel
CNN	Convolutional Neural Network
CPU	Central Process Unit
CT	Computed Tomography
dB	Decibel
DCT	Discrete Cosine Transform
DE	Difference Expansion
DFT	Discrete Fourier Transform
DL	Deep Learning
DWT	Discrete Wavelet Transform
FL	Fuzzy Logic
GA	Genetic Algorithm
GAR	Global Adaptive Region
GIF	Graphics Interchange Format
GPU	Graphics Processing Unit
HVS	Human Vision System
ISBI	International Symposium on Biomedical Imaging
IWT	Integer Wavelet Transform
JND	Just Noticeable Difference
LSB	Least Significant Bit
LFW	Labeled Faces in the Wild
MSE	Mean Square Error
MRI	Magnetic Resonance Imaging
PIM	Pixel Intensities Modulation Based Steganography
PNG	Portable Network Graphic
PPL	Perceptual Path Length
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
ReLU	Rectifier Linear Unit
RGB	Red, Green, Blue
RMSProp	Root Mean Square Propagation
SGD	Stochastic Gradient Descent
SSIM	Structural Similarity Index
SVD	Singular Value Decomposition
SVM	Support Vector Machine

1. GİRİŞ

1.1. Tezin Amacı, Kapsamı ve Özgünlüğü

Bilgisayar ve ağ teknolojilerinin gelişimi, iletişimde bilgi akışı ve değişimini büyük ölçüde kolaylaştırmıştır. Ancak, bu kolaylık, büyük miktarda verinin işlenmesi ve korunmasıyla ilgili güvenlik endişelerini de beraberinde getirmiştir.

Bu çalışmada, dijital iletişim alanındaki güvenli veri aktarımı ihtiyacına bir çözüm olarak, literatürde genel olarak tıbbi görüntü segmentasyonu alanında kullanılan U-Net mimarisinin veri gizleme amacıyla kullanılmasıyla, görüntü stenografisine yenilikçi bir uygulama sunulmuştur. Çalışmanın amacı, gizli resimlerin kapak resimleri içine daha yüksek kapasite ve algılanamazlık seviyesi ile gizlenmesini sağlamaktır.

Çalışmanın kapsamı ve önemli katkıları aşağıda belirtilmiştir:

a) Önerilen yöntem, steganografi alanında yaygın olarak kullanılan en az ağırlıklı bite (Least Significant Bit, LSB) gizleme ve piksel değer farkı (Pixel Value Differencing, PVD) gibi uzaysal alan yöntemlerinden, ayrık Fourier dönüşümü (Discrete Fourier Transform- DFT) ve ayrık kosinüs dönüşümü (Discrete Cosine Transform, DCT) gibi dönüşüm alanı yöntemlerinden farklılık göstermektedir. Bahsedilen yöntemlerde, kapak görüntüsü üzerine gizlenebilen veri miktarı sınırlıdır. Ancak bu çalışmada, gizli görüntünün tamamı, kapak görüntüsünde bulunan bitler üzerine dağıtılmıştır. Bu durum, algılanamazlık ilkesini bozmadan veri gizleme kapasitesini artırmıştır.
b) Tez çalışması kapsamında 256x256 çözünürlüğündeki RGB (Red, Green, Blue) kapak resimleri kullanılarak, bu kapak resimlerine farklı boyutlardaki RGB mesaj resimleri gizlenmiştir. Gizli resimlerin boyutları, 32x32 pikselden başlayarak 64x64, 128x128 ve en son 256x256 piksele kadar kademeli olarak artırılmıştır. Bu yöntem kullanılarak, farklı boyutlardaki mesaj resimlerinin steganografik süreç üzerindeki etkileri detaylı bir şekilde analiz edilmiştir.
c) Literatürdeki diğer çalışmalardan farklı olarak modelin test aşamasında Linnaeus 5 veri seti kullanılmıştır. Bu veri setinin seçilmesinin nedeni 32x32, 64x64, 128x128 ve 256x256 olmak üzere farklı boyutlardaki görüntüleri ayrı klasörler olarak içermesidir. Bu durum farklı mesaj resmi boyutlarının kapak resmi üzerindeki etkisini incelme noktasında avantaj sağlamıştır. Ancak buna ek olarak hem modelin çeşitli veri tabanları üzerindeki çalışma performansını görmek hem de literatürde yer alan diğer

çalışmalarla daha etkin kıyaslama yapabilmek adına ImageNet ve Labeled Faces in the Wild (LFW) veri tabanları ile de model test edilmiştir.

d) Literatürde yer alan diğer U-Net tabanlı steganografi çalışmalarından farklı olarak, mimariye artık (residual) bloklar dahil edilmiştir. Artık blokların dahil edilmesi, modelin öğrenme sürecini ve özellik aktarımını iyileştirmiş, bu da steganografik sürecin etkinliğini artırmıştır.

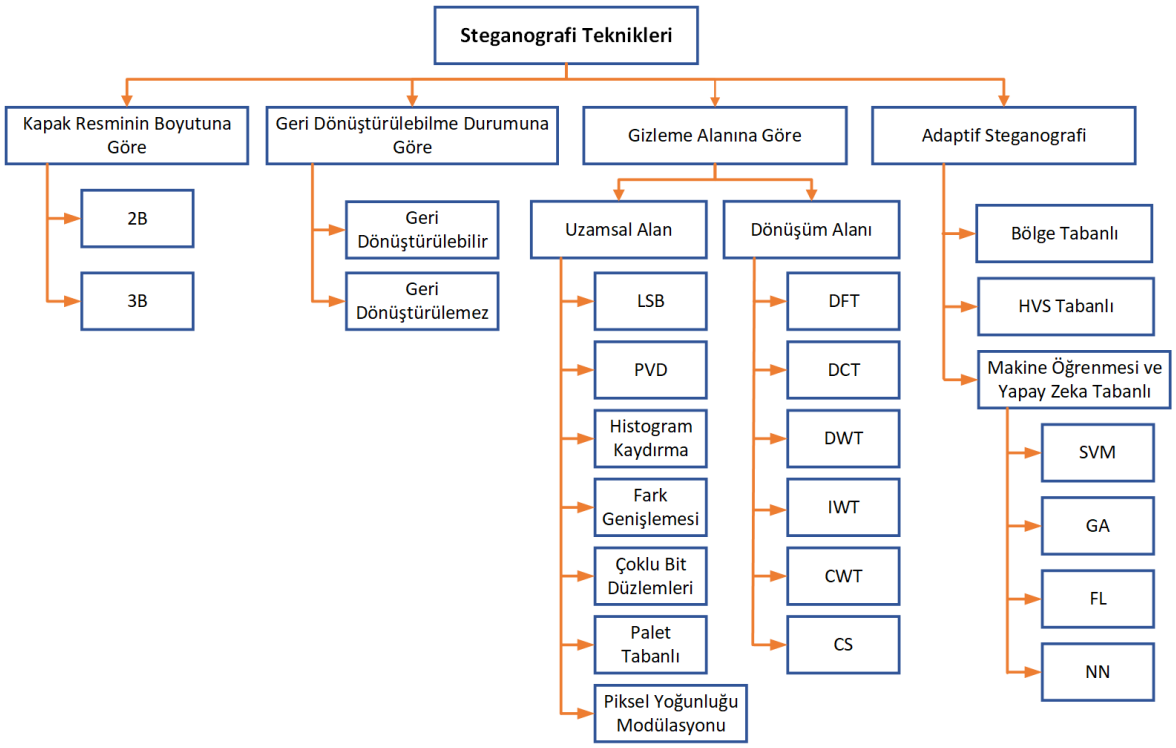
e) Literatürdeki diğer çalışmalardan farklı olarak, Tek Döngü Öğrenme Oranı Planlayıcısı (One Cycle Learning Rate Scheduler) AdamW optimizasyon algoritması ile birlikte kullanılmıştır. Tek Döngü Öğrenme Oranı Planlayıcısı, modelin eğitimi sırasında öğrenme oranını etkili bir şekilde yöneterek, öğrenme oranının eğitimin başlangıcında hızlı ilerleme ve sonrasında hassas bir ayarlama yapılmasını sağlar. Bu yaklaşım, modelin karmaşık veri yapıları içinde hızlı ve istikrarlı bir şekilde yakınsamasına olanak tanır. Diğer yandan, AdamW'nun ağırlık azaltma özelliği, aşırı uyum (overfitting) riskini azaltarak modelin genelleme kabiliyetini güçlendirir. Her iki yöntemin birleştirilmesi, U-Net modelinin hem öğrenme hızını optimize ederken hem de performansının artmasını sağlamıştır.

f) Gerçekleştirilen kapsamlı literatür taramasından elde ettiğimiz mevcut bilgilerimiz çerçevesinde, tez çalışması kapsamında geliştirilen mimariden elde edilen tepe değeri gürültü oranı (Peak Signal to Noise Ratio, PSNR) ve yapısal benzerlik indeksi (Structural Similarity Index, SSIM) sonuçları bakımından aynı boyutlara sahip kapak ve gizli resimleri ve metodu kullanan önceki derin öğrenme çalışmalarına kıyasla umut verici bulgular elde edilmiştir. Bu bulgular, analiz sonuçlarının görsel kaliteyi koruma konusunda önceki çalışmalara göre belirgin bir iyileşme sağladığını ortaya koymaktadır.

g) Son olarak uygun kapak resmi seçimine ilişkin istatistiksel analizler ortaya konulmuştur.

1.2. Literatür Taraması

Görüntü steganografisinin temel amacı, kapak resmi içine gizlenmiş gizli görüntünün herhangi bir iletişim kanalı aracılığıyla aktarılırken güvenli bir şekilde iletilmesini sağlamaktır. Gizleme işlemine dahil olan aşamalar ve uygulama tiplerine göre çeşitli görüntü steganografisi metotları geliştirilmiştir. Şekil 1.1'de bu alanda gerçekleştirilen farklı yaklaşımlar gösterilmektedir.



Şekil 1.1. Görüntü steganografi tekniklerinin sınıflandırılması.

Şekil 1.1'de görüldüğü gibi steganografi teknikleri kapak resminin boyutuna göre, geri dönüştürülebilir ve geri dönüştürülemez oluşuna, veri gizleme alanlarına göre sınıflandırılabilmektedir. Veri gizleme alanına göre yöntemler uzaysal alan ve dönüşüm alan metotları olarak ikiye ayrılmaktadır [1-2]. Uzaysal alan yöntemlerinde, veri doğrudan görüntünün pikselleri üzerine yerleştirilir. Dönüşüm alanı yöntemleri, görüntü üzerinde bir dönüşüm (örneğin, Fourier, Kosinüs, Dalgacık dönüşümü) uygulayarak, elde edilen dönüşüm katsayılarında değişiklik yaparak veri saklar. Uzaysal alan teknikleri LSB ve histogram kaydırma gibi çeşitli metotları kapsamaktadır. Bu teknikler, genellikle az işlem yükü gerektirir ve uygulamaları görece basittir. Bununla birlikte, uzaysal alan teknikleri, sıkıştırma, geometrik transformasyonlar ve görüntü filtreleme gibi etkenlere karşı daha az direnç gösterir. Diğer taraftan, dönüşüm alan yöntemleri; DCT, DFT ve ayrık dalgacık dönüşümü (Discrete Wavelet Transform - DWT) gibi yöntemleri temel almaktadır. Bu yöntemler, önceki bahsedilen geometrik bozulmalara karşı daha sağlam bir yapı sergilerler. Fakat, bu yöntemler genellikle daha fazla hesaplama yükü ve karmaşıklık gerektirir [3].

Steganografi uygulamaları incelendiğine en yaygın olarak kullanılan ve uygulaması en kolay yöntem olarak öne çıkan metot en önemsiz bite veri gizleme yöntemi olarak karşımıza çıkmaktadır. LSB yönteminde, görüntüyü oluşturan her pikselin her baytının en az ağırlıklı

biti (son biti) gizlenmek istenilen verinin bitleri ile yer değiştirilmektedir. Pikseldeki sekiz bitten en az ağırlıklı bir bit değiştirildiğinde, insan gözü bu değişimi algılayamamaktadır. Ancak istatistiksel olarak değerlendirildiğinde, özellikle yüksek gizleme oranlarında, steganaliz yöntemlerinin kullanılmasıyla tespit edilebildiği görülmektedir.

Joshi ve arkadaşları 2 KB, 4 KB ve 8KB'lık mesaj verilerini 256x256 boyutundaki gri tonlu resimler içine LSB yöntemi ile gizlemiş ve sırasıyla 57,15 dB, 54,15 dB, 51,13 dB PSNR seviyelerini elde etmişlerdir [4]. Her baytın en az anlamlı 1 biti, daha sonra en az anlamlı 4 biti gömülü verileri saklayacak şekilde bir model kurgulamışlardır. Her LSB işlemi için hem subjektif hem de objektif analizler yapılmıştır. Subjektif analiz olarak tüm resim varyasyonlarının histogram sunulmuştur.

LSB kapsamında yapılan bir diğer çalışmada farklı boyutlardaki kapak resimlerinde gizli bilgilerin saklanma performansını değerlendirilmiştir. Araştırma, 576 KB'den 7.31 MB'ye kadar değişen boyutlardaki kapak resimleri kullanılarak yapılmıştır. Örneğin, 576 KB boyutundaki bir kapak resmi, 175 KB boyutunda bir metin dosyasını, yani kapak resminin yaklaşık %30'u kadarını saklayabilmektedir. En büyük kapak resmi olan 7.31 MB, 4.29 MB'lık bir metin dosyasını, yani kapak resminin %58.69'unu saklayabilmektedir. Bu sonuçlar, kapak resminin boyutu arttıkça, saklanabilecek veri miktarının da arttığını göstermektedir. Makalede ayrıca, kapak resmi ve stego resmi arasındaki PSNR değerleri de sunulmuştur. Elde edilen değerler, 52.45 ile 52.29 arasında değişmektedir [5].

LSB yönteminin kullanıldığı bir diğer çalışmada öncelikle 8 bit derinliğinde kapak ve gizli resimler kullanılmıştır. Daha sonra ise kapak resmi 24 bit ve gizli resim 8 bit derinliğe sahip olacak şekilde analizler de gerçekleştirilmiştir. Gizlenecek resimler ikili formata dönüştürüldükten sonra gizlenecek resim boyutuna göre sırasıyla en önemsiz 1 bitten başlayarak en önemsiz 4 bite kadar artan gizleme işlemi gerçekleştirilmiş ve sonuçlar birbiriyle kıyaslanmıştır. Her bir işlem adımı için ayrı ayrı sonuçlar sunulmuş olmakla birlikte PSNR değerleri genel olarak 40dB'nin üzerindedir [6].

Literatürde uzamsal alan yöntemleri içinde yaygın olarak kullanılan bir diğer metot PVD yöntemidir. PVD yöntemi, bir görüntüdeki bitişik piksellerin değerleri arasındaki farkı kullanarak gizli verileri saklar [7]. PVD, özellikle detaylı ve karmaşık doku desenlerine sahip bölgelerde etkilidir. Çünkü bu alanlardaki küçük değişiklikler, görsel olarak daha az dikkat çeker. Yöntemin etkinliği, piksel çiftleri arasındaki korelasyona bağlıdır ve bu verilerin görsel kalitesini ve algoritmanın performansını etkiler.

Swain, gerçekleştirdiği çalışmada LSB ve PVD yöntemlerini bir arada kullanmıştır. Çalışmada kapak görüntüsü 2x2 piksellik birbirini örtmeyen bloklara bölünmüştür. Her bir 2x2 piksel blok için, pikseller belirlenmiştir. İlk adımda, blok içindeki bir piksele veri gizlenmesi LSB yer değiştirme yöntemiyle yapılmıştır ve bu aşamada veri gizlemek için en önemsiz 3 bite odaklanılmıştır. Sonraki adımlarda, bu gömülen veri kullanılarak, aynı blok içindeki diğer üç piksel ile olan piksel değer farkları hesaplanmıştır. Bu piksel değer farklarından yararlanılarak ek veri gizleme işlemi gerçekleştirilmiştir. Her bir piksel değer farkı için ayrı ayrı veri gizleme kapasitesi hesaplanmıştır. Çalışmada 40,44 dB PSNR değerine ulaşılmıştır [8].

Steganografide kullanılan diğer bir metot Ni ve arkadaşları tarafından tanıtılan histogram kaydırma yöntemidir (Histogram Shifting Method) [9]. Bu yöntem genellikle görüntüdeki piksel değerlerinin dağılımını değiştirerek veri gizlemeyi amaçlamaktadır. Yöntemde öncelikle, hedef görüntünün histogramını analiz edilmektedir. Histogram üzerinde, kaydırmanın yapılacağı bir nokta veya aralık seçilir. Bu nokta, genellikle düşük sıklıkta olan piksel değerleri içerir, böylece yapılan değişiklik görsel olarak az fark edilir. Daha sonra seçilen kaydırma noktasına yakın piksel değerleri, gömülecek veriyi temsil edecek şekilde değiştirilir. Bu metot, genellikle en düşük ve en yüksek histogram bölümlerini belirleyerek ve bu noktalarda kaydırmalar yaparak çalışır. Böylece, veri gizleme işlemi bu bölümlere odaklanır ve görüntüdeki görsel bozulmalar minimize edilir [10].

Nyeem çalışmasında bit düzlemi dilimleme ve histogram kaydırma yöntemlerini birleştirilerek kullanılmıştır. Bit düzlemi dilimleme işlemi, bir görüntüdeki piksellerin ikili kodlamasındaki her biti ayrı bir katman olarak ele alır. Örneğin, 8 bitlik bir görüntüde her piksel 8 bit bilgi içerir. Bit düzlemi dilimleme, bu 8 biti ayrı ayrı katmanlara böler. En önemli bit en yüksek bit düzeyini, en az önemli bit ise en düşük bit düzeyini temsil eder. Düşük düzey bitlerde yapılan değişiklikler, görüntünün görsel kalitesini azaltmadan veri saklamak için kullanılır, çünkü bu bitler genel görüntü kalitesine daha az etki eder. Bu yöntemle, gizli veriler, görüntünün az etkilenen bölümlerine yerleştirilir. Histogram kaydırma ise bu ayrılan piksel değerlerine göre uygulanır ve histogramın farklı bölümlerine veri yerleştirmek için kullanılır. Çalışmada PSNR seviyesi 40 dB üzerine çıkmıştır [11].

Bir diğer uzamsal alan yöntemi olan fark genişletme (Difference Expansion, DE) tabanlı steganografi, gizli verileri piksel çiftlerinin fark değerlerine gömme yöntemidir. Bu teknikte, iki bitişik pikselin yoğunluk farkı alınır ve bu fark, gizli verilerin saklanacağı daha

geniş bir aralığa dönüştürülür. Bu yaklaşım, görsel kaliteyi korurken daha fazla veriyi saklamayı mümkün kılar [12]. Chang ve arkadaşları bu kapsamda gerçekleştirmiş oldukları bir çalışmada 33.78 dB PSNR değerine ve 0,97 SSIM değerine ulaşmışlardır [13].

Çoklu bit düzlemleri yöntemi tabanlı steganografi (Multiple Bit Planes Based Steganography) LSB tekniğinin bir uzantısı olarak 2006 yılında tanıtılmıştır [14]. Bu teknikte, bir görüntünün bit düzlemleri, gizli veri bitlerini saklamak için kullanılır. Her bir pikselin birden fazla bit düzlemi (örneğin, en az anlamlı bitlerin yanı sıra daha yüksek düzeydeki bitler) gizli verileri yerleştirmek için kullanılır. Bu yöntem, daha fazla veri saklama kapasitesi sunarken, görüntünün görsel kalitesindeki değişiklikleri minimize etmeye çalışır. Bu yöntem sıklıkla, toplam sistem verimliliğini yükseltmek amacıyla farklı tekniklerle birlikte kullanılmaktadır [11].

Palet tabanlı steganografi (Palette Based Steganography), özellikle PNG (Portable Network Graphic) veya GIF (Graphics Interchange Format) gibi belirli görüntü formatlarında uygulanır [15]. Bu yöntemde, gizli veriler, görüntünün renk paletinde değişiklik yaparak saklanır. Palet renkleri, parlaklık değerlerine göre sıralanır. En koyudan en açığa veya tersi bir sıralama yapılır. Her pikselin rengi, palet içindeki bir indeksle temsil edilir. Bu indekslerin en az anlamlı bitleri, gizli veriyi saklamak için kullanılacak alanlardır. Örneğin, bir GIF resminde, her bir renk palet girişi belirli bir renge karşılık gelir. Gizli veriyi saklamak için, bu palet girişlerinden biri veya birkaçı, gizli verinin bitlerine göre değiştirilmektedir. İmaizumi ve ekibi tarafından geliştirilen palet tabanlı steganografi sisteminde bir piksele birden fazla bit gizlemenin yansıra yaklaşık 40 dB PSNR değeri sağlanmıştır [16].

Piksel yoğunluk modülasyonu tabanlı steganografi (Pixel Intensities Modulation Based Steganography, PIM), gizli veriyi bir görüntüdeki piksellerin yoğunluk değerlerini küçük değişiklikler yaparak saklayan bir tekniktir. Bu yöntemde, öncelikle gizli veri ikili formata dönüştürülür ve ardından belirli piksellerin yoğunlukları, bu ikili veriye göre artırılır ya da azaltılır. Değişiklikler, gözle fark edilemeyecek kadar küçük tutulur, böylece görüntünün doğal kalitesi korunur. Gizli verinin çıkarılması sürecinde, modüle edilen piksellerin yoğunluk değerleri analiz edilerek orijinal ikili veri elde edilir. Bu çerçevede yapılan bir çalışmada, gizli mesaj önce ikili diziye dönüştürülmüş ve sonra kapak görüntüsünden alınan 3x3'lük alt matrisler içine gizlenmiştir. Veri gizleme işlemi, bitişik piksellerin değerleri üzerinde modülasyon yaparak gerçekleştirilmiştir. Bu modülasyon, ikili

dizideki bit çiftlerini temel almış ve her çift için piksel yoğunlukları arasındaki farka göre kodlama yapılmıştır. Önerilen algoritmanın gizleme kapasitesi 1 yakındır ve çalışma sonuçları PSNR ve MSE olarak sunulmuştur. Çalışmada elde edilen en yüksek sonuçlar bazında, 1000 karakterlik bir gizli metin için 64,365 dB PSNR ve 0,023 MSE, 5000 karakterlik bir gizli metin için 50,961 dB PSNR ve 0,521 MSE, 10000 karakterlik bir gizli metin için 39,953 dB PSNR ve 6,574 MSE değerleri elde edilmiştir [17].

Dönüşüm alanında, daha önce de bahsedildiği gibi hem kapak resim ve hem gizlenecek veri frekans alanına dönüştürülür ve daha sonra gizleme işlemi gerçekleştirilir. Bu sınıflandırmada altında olan yöntemlerden biri DCT'dir. Bu yaklaşımda, kapak olarak seçilen görüntü, öncelikle DCT kullanılarak frekans alanına dönüştürülür ve yüksek, orta ve düşük frekans bantlarına ayrılarak gizli verinin eklenmesi için ideal bir zemin hazırlanır [18]. Dönüşüm işlemi, görüntüyü genelde 8x8 piksellik bloklara ayırarak ve bu blokların her birinin DCT katsayılarını hesaplayarak yapılır. Daha sonra, bu katsayılar gizli bilgileri saklamak için kullanılır. Sonrasında görüntünün ters kosinüs dönüşümü alınarak tekrar zaman uzay eksenine geçilmektedir ve görüntü tekrar elde edilmektedir. Dönüşüm alan yöntemlerinin çoğu DCT'ye dayanmaktadır. DCT, Fourier dönüşümüne benzer bir frekans dönüşümü yöntemidir. Ancak, Fourier dönüşümünün aksine, DCT yalnızca kosinüs bileşenlerini içerir ve hem kosinüs hem de sinüs bileşenlerini barındırmaz. Bu özellik, DCT'nin karmaşık değil, gerçek bileşenlere dayalı olmasını sağlar ve bu yönüyle Fourier dönüşümünden ayrılır. Dolayısıyla, DCT, görüntü işleme ve sinyal işleme uygulamalarında gerçek değerli verilerle çalışırken tercih edilen bir yöntem haline gelmiştir.

Metha ve Bhatti tarafından yapılan çalışmada kapak resmi olarak, DCT kullanılarak işlenen gri tonlamalı bir görüntü tercih edilmiştir. Gizli veri, karakterlerin oktal sayı formatındaki anahtarlarla şifrelenerek gizlenmiştir. 8192 bitlik bir yük (payload) gri tonlamalı resmin içine gizlenmiş 64 dB seviyesinde PSNR değeri ve 0,99 seviyesinde SSIM değeri elde edilmiştir [19].

Ayrık Fourier Dönüşümü (Discrete Fourier Transform, DFT) yöntemi, yapısı itibarıyla Ayrık Kosinüs Dönüşümü'ne (DCT) oldukça benzer özellikler taşır. Ancak, DCT'nin aksine, bu yöntemde Fourier dönüşümü esas alındığı için, işlem süreci daha karmaşık bir yapıdadır. DFT, hem kosinüs hem de sinüs bileşenlerini içerdiğinden, hesaplama süreci daha detaylı ve kapsamlıdır. Bu durum, özellikle veri işleme ve analiz süreçlerinde, DCT'ye kıyasla daha yüksek bir işlem yüküne yol açmaktadır [18].

Melman ve Evsutin çalışmalarında DFT tabanlı bir steganografi algoritması kullanılmıştır. Kapak medyası olarak gri tonlamalı bir resim tercih edilmiş ve gizli veri, bu resme gömülerek saklanmıştır. Çalışmada elde edilen stego görüntülerin PSNR değerleri 58.05 dB ile 63.06 dB arasında değişmektedir [20].

DWT tabanlı steganografi, dijital görüntü steganografisinde yaygın olarak kullanılan bir diğer yöntemdir. Bu teknik, görüntüyü farklı frekans bantlarına ayırarak çalışır ve böylece gizli veriyi bu bantlara gömme olanağı sunar [21]. DWT uygulandığında, görüntü düşük ve yüksek frekanslı bileşenlere ayrıştırılır. Ardından, saklanacak gizli bilgi ikili formata dönüştürülür ve ana resmin frekans bileşenlerine eklenir. Modifiye edilen katsayılar daha sonra birleştirilerek stego görüntü oluşturulur.

Vanitha ve ekibinin gerçekleştirdiği bir araştırmada, gizli verilerin bir resim içine gizlenmesi için hem LSB hem de DWT tekniklerinin kullanıldığı bir yöntem sunulmuştur. Araştırmada, her iki yöntemin sonuçları karşılaştırılmıştır. LSB tekniğiyle yapılan uygulamada, PSNR değeri 53,27 dB ve MSE 0,55 olarak kaydedilmiştir. Buna karşılık, DWT yöntemi kullanıldığında ise PSNR değeri 44,86 dB ve MSE 1,45 olarak elde edilmiştir [22].

Bir diğer çalışmada yine DWT ve LSB ile gerçekleştirilen analiz sonuçları karşılaştırılmıştır. DWT aşamasında, gizli resimlere tekil vektör ayrıştırması (Singular Value Decomposition, SVD) uygulanmıştır. Analiz sonuçlarına göre LSB ile 45 dB'nin üzerinde PSNR değeri elde edilirken DWT için elde edilen değerler genel olarak 30 dB'nin altındadır. [21].

Tamsayı dalgacık dönüşümü (Integer Wavelet Transform, IWT) görüntü verilerini tamsayı katsayıları kullanarak işleyen bir dalga dönüşümü yöntemidir. Ahmad ve ekibi tarafından gerçekleştirilen çalışmada 512x512 piksel boyutunda ve 16-bit derinlikte gri tonlamalı manyetik rezonans görüntüleme (Magnetic Resonance Imaging, MRI) ve bilgisayarlı tomografi (Computed Tomography, CT) tarama görüntüleri kullanılmıştır. Kapak görüntüsü, IWT kullanılarak uzamsal alandan frekans alanına dönüştürülmüş ve en önemsiz 1-3 bit belirlenerek gizli veri bu bitler üzerinde gizlenmiştir. 1000 karakter gizlenmesi durumunda 79,9528 dB PSNR ve 0,00526 MSE, 5000 karakter gizlenmesi durumunda 63,9818 dB PSNR ve 0,0262 MSE ve 10000 karakter gizlenmesi durumunda 59,4653 dB PSNR ve 0,07413 MSE değerleri elde edilmiştir [23].

Adaptif steganografi yöntemleri bu zamana kadar bahsedilen yöntemlerden farklı olarak veri gizleme süreçlerini kapak ve gizli resimlerinin kendine has özelliklerine göre dinamik olarak ayarlayarak fark edilmezliği artırma üzerine yoğunlaşmaktadır. Bu ana başlık altında bölgesel tabanlı steganografi (Region Based Steganography), insan görsel sistemi tabanlı (Human Vision System, HVS) ile makine öğrenimi ve yapay zeka tabanlı steganografi alt başlıklarının yer aldığı ifade edilebilir. Bölgesel tabanlı steganografide gizleme işlemi genellikle görüntülerin doku ve kenar detayları gibi belirgin özellikler içeren bölgelerine odaklanmaktadır. Bu durum, düz ve daha az detay içeren bölgelere kıyasla gizlenecek verilerin daha az fark edilmesini sağlamaktadır [24-25].

Rabie ve Kame, yaptıkları çalışmada bölgesel tabanlı steganografi ve DCT yaklaşımlarını birlikte kullanmışlardır. Çalışmada global uyarlanabilir bölge (Global Adaptive Region, GAR) kullanılmıştır. GAR kapak resminin dokusu, renk yoğunluğu ve parlaklık gibi özelliklerini değerlendirerek görsel bozulmayı en aza indirecek uygun bölgeleri tespit etmektedir. DCT aşamasında 512x512 boyutlarındaki kapak görüntüsü 8, 16, 32, 64, 128 ve 256 lık bloklara bölünmüş ve her bir blok boyutu için analiz sonuçları sunulmuştur. Analiz sonuçlarında 64x64'lük blok boyutu için, bit başına piksel oranı (Bit Per Pixel, BPP) 17,25 ve PSNR değeri 32,2 dB olarak en optimum sonuçlar elde edilmiştir [26].

HVS'yi temel alan steganografi, insan gözünün görüntüleri algılama şeklini kullanarak gizli verileri saklamaktadır. HVS'nin bazı sınırlamaları ve eksiklikleri nedeniyle, insan görsel algısı küçük değişikliklere tepki veremez. Ayrıca, yapılan pek çok deneye göre, insan gözü kapak görüntüsünün karanlık bölgelerindeki piksel değerindeki değişikliklere hassas değildir. Bu sebeple, bilgi, karmaşık dokulu ve karanlık alanları olan görüntülere daha fazla gizlenebilir[27]. HVS'nin bölgesel tabanlı steganografi ile temel farkları mevcuttur. HVS, insan gözünün görsel algılamasına odaklanırken, bölge bazlı steganografi, görüntünün kendine özgü bölgesel özelliklerine dayanır ve ayrıca HVS, görüntünün genel algılanabilirlik özelliklerini temel alırken, bölge bazlı yaklaşım, görüntünün belli bölümlerinde veri gizlemeyi hedefler. HVS tabanlı steganografi kapsamında gerçekleştirilen bir çalışmada resmin belirli bir pikselinde ya da bölgesinde yapılacak en küçük değişikliğin, insan gözü tarafından algılanabilir seviyede olup olmadığını belirten fark edilebilir fark indeksi (Just Noticeable Difference, JND) kullanılarak ortalama 40dB PSNR elde edilmiştir. Ancak BPP oranı 0,6 seviyesindedir [28].

Adaptif steganografi başlığı altındaki sınıflandırmalardan bir diğeri de, artık bu alanda en yaygın olarak kullanılan yöntemleri içeren makine öğrenimi ve yapay zeka tabanlı steganografidir. Geleneksel steganografi tekniklerinde, gizli bilgilerin gömülmesi sırasında BPP oranının artması sonucunda oluşan görsel bozulmalar, bu tekniklerin gizleme etkinliğini sınırlandırır. Buna karşın, tipik görüntü steganografi tekniklerinde verimlilik, stego görüntüdeki bozulmayı minimuma indirgeyip gömme kapasitesini en üst düzeye çıkararak artmaktadır. Makine öğrenimi tabanlı steganografik tekniklerde, bu verimlilik iyileştirmelerini elde etmek için ileri düzey yöntemler kullanılır [56]. Bu alanda kullanılan yaygın yöntemler arasında destek vektör makinaları (Support Vector Machine, SVM), genetik algoritma (Genetic Algorithm, GA), ve bulanık mantık (Fuzzy Logic, FL) bulunmaktadır. Bu yaklaşımlar, steganografik sistemlerin verimliliğini çeşitli yollarla geliştirmektedir. Ama özellikle son zamanlarda, evrişimsel sinir ağı (Convolutional Neural Network, CNN) ve derin öğrenmeye dayalı görüntü steganografisine yönelik araştırmalarda önemli bir artış olmuştur. Görüntü steganografisinde bu mimarilerin kullanımı, kodlayıcı-kod çözücü mimarisinden önemli ölçüde ilham almıştır. Kodlayıcı, kapak resmi ve gizli resim olmak üzere iki girdi alır ve bunları stego görüntüsünü oluşturmak için kullanır. Daha sonra kod çözücü stego görüntüsünü girdi olarak alır ve gizli görüntüyü tekrar üretir. Temel fikir değişmeden kalırken, araştırmacılar farklı mimari çerçeveleri araştırmak için farklı metodolojiler kullanmışlardır.

Rehman ve arkadaşları, renkli kapak resminin içine gri tonlamalı gizli görüntüyü gizleyerek stego görüntüsünün görsel kalitesini artıran bir CNN tabanlı görüntü steganografi tekniği önermişlerdir. Evrişimsel katmanlar aracılığıyla, hem kapak hem de gizli resimlerden özellikler çıkarılır ve daha sonra bu özellikler birleştirilir. Bu birleştirilmiş özellikler, stego görüntüsünü oluşturmak için kullanılır. Analiz, MNIST, CIFAR10, PASCAL-VOC12, ImageNet ve LFW veri setleri kullanılarak gerçekleştirilmiştir [29].

Baluja, aynı boyutlu ve aynı derinliğe sahip kapak ve gizli resimleri kullanabilmeyi amaçlayarak CNN tabanlı olarak geliştirdiği mimaride kodlayıcı ve kod çözücü olarak bir şema sunmaktadır. Bu şema 3 ayrı ağ yapısından oluşmaktadır. İlk ağ, gizli görüntünün RGB piksellerini özelliklere dönüştürmek için kullanılır. İkinci ağ, bir saklama ağıdır ve bu ağ, ilk ağ tarafından hazırlanan özellikleri kapak resmi içinde gizler, böylece stego görüntüsü oluşturulur. Üçüncü ve son bileşen olan çıkarma ağı ise, kapak görüntüsünden gizli görüntüyü çıkartır. Çalışmada eğitim ve test için ImageNet ve Corel veri tabanları kullanılmıştır. Stego resim ile kapak resmi arasındaki PSNR değeri 41,2 dB ve SSIM değeri

0,98 olarak elde edilirken, gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değeri 37,6 dB ve SSIM 0,97 olarak sunulmuştur [30].

Bir diğer çalışmada, görüntü steganografisi için "Image Steganography Generative Adversial Network" (ISGAN) adında bir evrişimsel sinir ağı mimarisi uygulanmaktadır. Bu yöntemde, kapak görüntüsü YCrCb görüntü formatına dönüştürülür. Bu format, Luma (Y), Chroma Red (Cr) ve Chroma Blue (Cb) bileşenlerinden oluşan ve dijital görüntü ve video işlemede kullanılan bir renk uzayıdır. Gizli görüntü, sadece Y kanalına gizlenir. Bu yöntem özellikle gri tonlamalı görüntülerin gizlenmesi için tasarlanmıştır. Kodlayıcı-kod çözücü ağı, kapak görüntüsünün Y kanalını ve gri tonlamalı gizli görüntüyü girdi olarak kullanarak stego görüntüsünü oluşturur. Y kanalını kullanarak, sadece gizlenen gri tonlamalı görüntü gizlenirken, Cr ve Cb kanalları etkilenmez çünkü bu kanallar tüm renk ile ilgili verileri içerir. Gizli görüntüyü çıkarmak için, stego görüntüsünün Y kanalı çıkarma ağına gönderilir ve bu ağ, gri tonlamalı gizli görüntüyü üretir. Bu yöntem, LFW, PASCAL-VOC ve ImageNet veri setleri üzerinde test edilmiştir. Stego resim ile kapak resmi arasındaki PSNR ve SSIM değerleri ile gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR ve SSIM değerleri sırasıyla ImageNet veri tabanı için 34,89 dB, 0,9681, 33,42 dB, 0,9474, PASCAL-VOC12 veri tabanı için 34,49 dB, 0,9661, 33,31 dB, 0,9467 ve LFW veri tabanı için 34,63 dB, 0,9573, 33,63 dB ve 0,9429 olarak sunulmuştur [31].

Subramanian ve ekibi çalışmalarında, derin evrişimsel otomatik kodlayıcı/kod çözücü mimarisi kullanmışlardır. Bu mimari üç ana aşamadan oluşmaktadır: hazırlık, gömme ve çıkarma. Hazırlık aşamasında, hem kapak hem de gizli görüntüler, özelliklerinin çıkarılması için bir ön işleme modülünden geçirilir. Gömme ağının kodlayıcı kısmı, sırasıyla 64 ve 128 filtre sayısına sahip iki evrişimsel katmandan oluşur. Kod çözücü kısmı ise beş evrişimsel katmandan oluşur ve burada filtre sayısı aşamalı olarak azalır (128, 64, 32, 16, 8). Çıkarma ağının kodlayıcı kısmı da beş evrişimsel katmandan oluşur, ancak burada filtre sayısı artar (8, 16, 32, 64, 128). Benzer şekilde, kod çözücü kısmı da beş evrişimsel katmandan oluşur, ancak filtre sayısı azalır (128, 64, 32, 16, 8). Bu çalışmada, COCO, CelebA ve ImageNet veri setleri deneyler için kullanılmıştır. Analizler sonucunda stego resim ile kapak resmi arasındaki ve gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değerleri sırasıyla ImageNet veri tabanı için 34,55 dB, 27,93 dB, COCO veri tabanı için 31,96 dB, 27,90 dB ve CelebA veri tabanı için 32,26 dB ve 27,92 dB olarak sunulmuştur [32].

Liu ve arkadaşları U-Net ve dalgacık dönüşümü tabanlı yöntemleri birleştiren bir çalışma yapmışlardır. Sistem iki ana bölümden oluşur. Birinci bölüm, gizli verilerin dalgacık katsayılarını kapak resmine yerleştiren gizleme ağıdır. İkinci bölüm ise, stego resmi dört dalgacık katsayısına ayırarak orijinal gizli veriyi ters dalgacık dönüşümüyle geri kazanan bir çıkarma ağıdır. Bu çalışmada stego resim ile kapak resmi arasındaki PSNR 39,7708 dB ve SSIM 0,9828 olarak sunulurken, gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değeri 43,3571 dB ve SSIM değeri 0,9862 olarak elde edilmiştir [33]. Liu ve ekibinin daha sonraki çalışmalarında, daha küçük bir ağ ölçeğine sahip geliştirilmiş bir U-Net mimarisi sunulmuş ve bu yeni sistemle, önceki çalışmalarına göre daha yüksek kalitede sonuçlar (gizleme kısmı için 1,12 dB ve çıkarma kısmı için 6,24 dB daha yüksek PSNR) elde edilmiştir [34]. Her iki çalışmada da PASCAL-VOC ve ImageNet veri setlerindeki görüntüler eğitim ve test amaçları için kullanılmıştır.

Duan ve ekibi yaptıkları çalışmada gizleme ve çıkarma işlemleri için sırasıyla bir U-Net mimarisi ve altı katmanlı bir CNN mimarisi önermişlerdir. ImageNet veri seti hem eğitim hem de test amacıyla kullanmıştır. Gönderici, gizli görüntüyü, alıcıya iletmek üzere başka bir aynı boyutlu görüntüye gizleme ağını kullanarak yerleştirir. Alıcı daha sonra, kapak görüntüsünü ve gizli görüntüyü doğru bir şekilde yeniden oluşturmak için çıkarma ağını kullanır. Çalışma sonuçlarında, stego resim ile kapak resmi arasındaki PSNR değeri 40,4716 dB ve SSIM değeri 0.9794 olarak elde edilirken, gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değeri 40,6665 dB ve SSIM 0.9842 olarak elde edilmiştir [35].

Himthani ve arkadaşları, görüntü steganografisi için U-Net, V-Net ve U-Net++ mimarilerini uygulamışlardır. U-Net++, U-Net'in yapısal bağlantılarını genişletmek için geliştirilmiş bir modeldir, ancak eklenen karmaşıklık ve hesaplama yükü, daha yüksek donanım gereksinimleri ve daha uzun işlem süreleri ile sonuçlanmaktadır. Yapısal olarak U-Net'e benzer olan V-Net, genel olarak üç boyutlu görüntüler için tasarlanmış bir varyasyondur ve üç boyutlu veriler üzerinde daha iyi sonuçlar sunmaktadır. Çalışmada U-Net, V-Net ve U-Net++ mimarilerinin etkinliğini analiz etmek için, LFW ve Know Your Data veri setleri kullanılarak karşılaştırmalı bir değerlendirme yapılmıştır. Bu mimariler, gizli görüntüyü kapak görüntüsü içine gizlemek için kullanılmıştır. Ayrıca, tüm senaryolar için kapak görüntüsünden gizli görüntüyü çıkarmak üzere CNN tabanlı mimari kullanılmıştır. Stego resim ile kapak resmi arasındaki PSNR ve SSIM değeri ile gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR ve SSIM değerleri sırasıyla

U-Net için 38,00 dB, 0,9875, 38,00 dB, 0,9869, V-Net için 30,00 dB, 0,9680, 33,00 dB, 0,9810 ve son olarak U-Net++ için 24,00 dB, 0,910, 27,00 dB ve 0,930 olarak elde edilmiştir. Deneysel sonuçlara göre, kullanılan üç mimari arasında en optimum sonuçlar U-Net mimarisi ile alınmıştır [36].

Diğer bir çalışmada, U-Net kullanılarak, hem gizli resmin hem de kapak resminin Y kanalı kullanılarak gizleme işlemi gerçekleştirilmiştir. Bu yaklaşım, diğer çalışmalardan farklı olarak algısal yol uzunluğu (Perceptual Path Length - PPL) ile MSE değerlerini kayıp fonksiyonu kullanmaktadır. PPL, modelin ürettiği farklı çıktılar arasındaki geçişlerin, insan algısına göre ne seviyede doğal ve akıcı göründüğünü ölçmek amacıyla kullanılmıştır. Ağ, LFW ve PASCAL-VOC veri setleri üzerinde test edilmiştir. Stego resim ile kapak resmi arasındaki PSNR ve SSIM değeri ile gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR ve SSIM değerleri sırasıyla 39,3912 dB, 0,9894, 35,8427dB, 0,9833 olarak elde edilmiştir [37].

Wang çalışmasında, gri tonlamalı bir gizli görüntüyü renkli bir kapak görüntüsüne gizlemek için U-Net++ mimarisini kullanmıştır. Gizleme işlemini gerçekleştiren gizli ağ, kapak görüntüsünün Y kanalını gizli resim ile birleştirerek, iki kanallı bir tensör (çok boyutlu dizi) olarak girdi oluşturur ve bu şekilde bir kodlayıcı görevi görür. Ağın çıkarma kısmı, herhangi bir havuzlama katmanı olmaksızın altı evrişimsel katmandan oluşur. Bu çalışmada, analizler için ImageNet ve LFW veri setleri kullanılmıştır. Analizler sonucunda ImageNet veri tabanı için stego resim ile kapak resmi arasındaki PSNR değeri 37,1381 dB, SSIM değeri 0,9768 ve gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değeri 35,4812 dB, SSIM değeri 0,9681 olarak elde edilmiştir. Ayrıca LFW veri tabanı için stego resim ile kapak resmi arasındaki PSNR değeri 37,5614 dB, SSIM değeri 0,9821 ve gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değeri 35,4321 dB, SSIM değeri 0,9743 olarak sunulmuştur [38].

Bir diğer çalışmada gizleme ve çıkarma aşamaları için Baluja [30] tarafından önerilen evrişimsel sinir ağı ve Duan [35] tarafından önerilen U-Net ağı mimarileri oluşturularak sonuçlar incelenmiş ve swin dönüştürücü (Swin Transformer) ağ mimarisi sonuçları ile kıyaslanmıştır. Bu yapılar, ImageNet veri seti kullanılarak doğrulanmıştır. Stego resim ile kapak resmi arasındaki PSNR ve SSIM değeri ile gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR ve SSIM değerleri sırasıyla CNN için 36,50 dB,

0.978, 36,68 dB, 0.942, U-Net için 36.96 dB, 0.970, 35.98 dB, 0.963, son olarak swin dönüştürücü için 38.55 dB, 0.981, 38.15 dB ve 0.985 olarak elde edilmiştir [39].

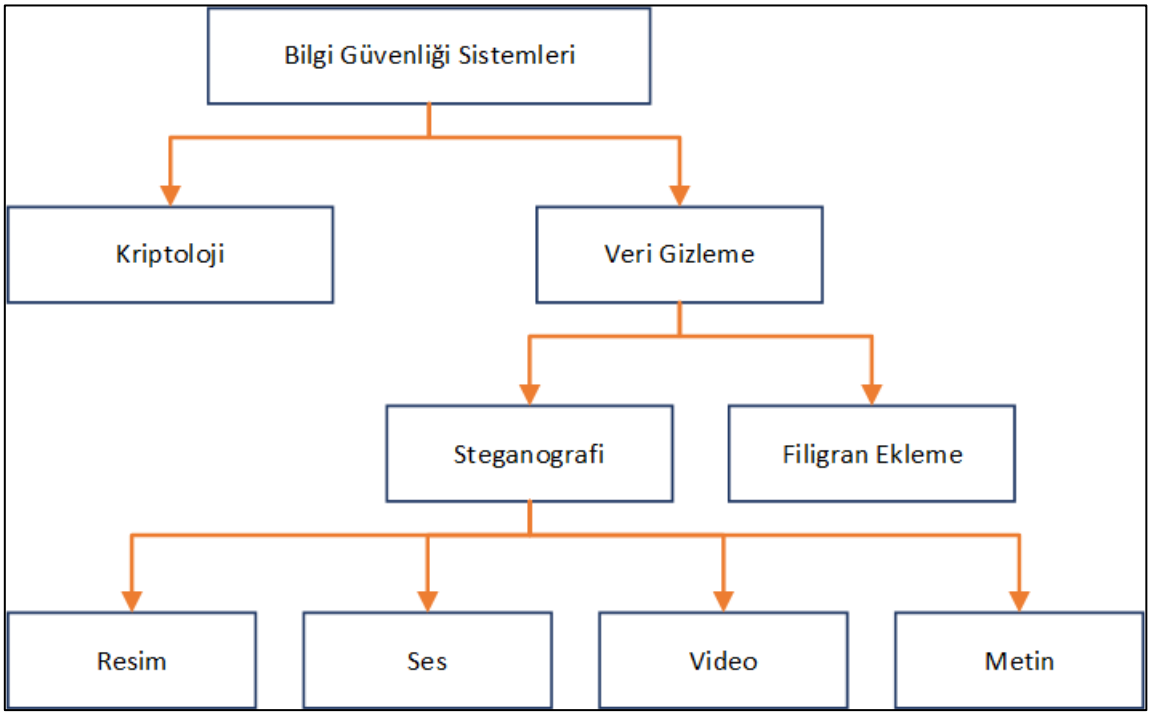
Başka bir araştırmada, bir görüntüyü diğerine gizlemek için MobileNet evrişimsel sinir ağı ve U-Net mimarisini kullanan bir yöntem tanıtılmıştır. MobileNet CNN mobil ve gömülü cihazlarda kullanım için tasarlanmış hafif, daha az hesaplama gücü gerektiren verimli bir derin öğrenme modelidir. Bu çalışmada, MobileNet hem gizleme hem de çıkarma ağlarında U-Net yapısının temelini oluşturur. Yöntem, CIFAR10, StanfordCars ve STL10 veri setleri kullanılarak eğitim ve test aşamalarından geçirilmiştir. Stego resim ile kapak resmi arasındaki ve gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR değerleri sırasıyla CIFAR 10 için 27,663 dB ve 27,552 dB, StanfordCars veri seti için 23,171 dB ve 23,531 dB ve son olarak STL10 veri seti için 28,226 dB ve 28,767 dB olarak sunulmuştur [40]. Görsel sonuçlar incelendiğinde, kapak ve gizli görüntülerde gözle görülür düzeyde değişiklikler tespit edilmiştir.

Kich ve ekibi, U-Net mimarisini, bir renkli görüntünün içine aynı boyutta başka bir renkli görüntüyü gizlemek için kullanmışlardır. Bu ağda, kapak ve gizli görüntüleri birleştiren genişletilmiş başlangıç bloğu (Dilated Inception Block) adı verilen özel bir yapı kullanılmıştır. Genişletilmiş evrişim ile filtreler arası boşluklar bırakılarak görüntünün daha geniş alanlarının incelenebilmesi, başlangıç bloğu ile de birden fazla farklı boyutta evrişim filtresi çalıştırılarak görüntünün farklı boyutlardaki detaylarının yakalanması amaçlanmıştır. Çalışmada eğitim ve test amacıyla ImageNet, LFW ve PASCAL-VOC12 veri setleri kullanılmıştır. Çalışmada analizler sonucunda stego resim ile kapak resmi arasındaki PSNR ve SSIM değeri ile gizli resim ile stego resimden tekrar çıkartılmış gizli resim arasındaki PSNR ve SSIM değerleri sırasıyla ImageNet veri tabanı için 37,83 dB, 0,9786, 31,77 dB, 0,9077, LFW veri seti için 40,03 dB, 0,9797, 33,13 dB, 0,9280 ve PASCAL-VOC12 veri tabanı için 37,40 dB, 0,9790, 30,80 dB, 0,9094 değerleri elde edilmiştir [41].

2. MATERYAL VE METOT

2.1. Veri Gizleme Teknikleri

Modern dünyada, dijital iletişimdeki gelişmeler, günlük yaşantımızda kritik bir öneme sahiptir. İnternet teknolojilerindeki yenilikler ve bilginin dijitalleşmesi, veri aktarımını büyük bir hızla artırmıştır. Bilgi güvenliği, bilgileri korumada zorunlu bir unsur haline gelmiştir. Mevcut birçok güçlü ve yüksek güvenlikli yöntem bulunmasına rağmen, bu alan sürekli olarak bu teknikleri daha güvenli ve performans açısından daha sağlam hale getirilmesi yönünde ilerlemektedir. Kuşkusuz, veri güvenliği, veri iletişiminin temel taşıdır. Genellikle, bilgi güvenlik sistemleri iki ana kategoriye ayrılmaktadır. Bunlardan ilki şifreleme diğeri ise bilgi gizlemedir [42]. Her iki kategorinin de odak noktası bilgi güvenliği olmakla birlikte, kullandıkları teknikler birbirinden farklıdır. Şekil 2.1, genel bir veri güvenlik sistemlerinin nasıl sınıflandırıldığını göstermektedir.



Şekil 2.1. Veri güvenliği sistemleri [42].

Kriptografi, veri analizi ve güvenliği alanında son derece önemli bir yere sahiptir. Kriptografinin temel amacı, hassas bilgileri, yetkisiz kişilerin erişimine karşı korumak ve bu bilgileri güvenli bir şekilde iletmektir. Şifreleme işlemi, veriyi, orijinal formunu kaybedecek şekilde değiştirir, bu da üçüncü tarafların bu verileri anlamasını zorlaştırır. Kriptografi,

özellikle uçtan uca iletişimde güvenliği sağlamak için büyük öneme sahiptir. Bu alandaki teknikler, genellikle karmaşık matematiksel algoritmalar ve permütasyon işlemleri temelinde geliştirilir. Şifreleme işlemleri, genellikle bir anahtar kullanılarak gerçekleştirilir ve bu anahtarlar, simetrik ve asimetrik olmak üzere iki ana kategoriye ayrılır. Simetrik anahtar kriptografisinde, aynı anahtar hem şifreleme hem de şifre çözme işlemlerinde kullanılır. Buna karşılık, asimetrik anahtar kriptografisinde, şifreleme için açık anahtarlar ve şifre çözme için özel anahtarlar kullanılır. Bu yöntemler, verilerin güvenliğini sağlamanın yanı sıra, dijital imzalar ve kimlik doğrulama gibi işlemlerde de kullanılır [43].

Steganografi, veri iletişimi ve güvenliği alanında kullanılan başka önemli bir tekniktir. Steganografi, mesajları, bir görüntü, ses dosyası veya başka bir medya dosyası içinde gizleme mantığında çalışmaktadır. Orijinal veriyi değiştirmeden, mesajı fark edilmeden bir medya dosyasının içine yerleştirir ve özellikle hassas bilgilerin gizli kalmasını sağlamak için kullanılır. Steganografinin en büyük avantajlarından biri, verinin varlığının fark edilmemesidir. Bu, potansiyel saldırganların, gizli bir mesajın varlığından habersiz olmasını sağlar.

Steganografi ve kriptografinin nihai hedefleri benzer olmakla birlikte, yaklaşımları farklıdır. Steganografi, verinin veya mesajın formatını değiştirmeden, asıl verinin varlığını korurken; kriptografi, veriyi okunamaz bir forma dönüştürerek gizliliğini sağlar. Bu iki tekniğin saldırılara karşı sağlamlık tanımları da farklıdır. Kriptografik sistem, üçüncü bir taraf orijinal verilere eriştiğinde kırılmış olarak kabul edilirken; bir steganografi sistemi, üçüncü bir taraf gizli verinin varlığını tespit ettiğinde kırılmış sayılır [44].

Bir başka veri güvenliği yöntemi olan filigran ekleme dijital içeriklerin korunmasında kritik bir rol oynar. Bu teknik, dijital medya dosyalarına görünür veya görünmez işaretler ekleyerek, telif hakkı koruması ve içeriğin yetkisiz kullanımını önleme amacı taşır. Filigran ekleme, özellikle dijital görüntüler, videolar ve ses dosyalarında yaygın olarak kullanılır. İki temel türü vardır: görünür ve görünmez filigran ekleme. Görünür filigran ekleme, genellikle telif hakkı sahibinin logosu veya ismi gibi açıkça görülebilen işaretler içerir. Görünmez filigran ekleme ise, içeriğin içine gizlenmiş ve çıplak gözle görülemeyen, ancak özel yazılımlarla tespit edilebilen işaretler içerir. Filigran ekleme yönteminin uygulamaları çok çeşitlidir. Örneğin, dijital fotoğrafçılıkta, görüntülerin telif hakkını korumak için sıklıkla görünür filigranlar kullanılır. Görünmez filigranlar ise genellikle yayın endüstrisinde, özellikle televizyon yayınlarında ve çevrimiçi video platformlarında içeriklerin yayın

haklarını korumak için tercih edilir. Özellikle dijital çağda, içeriklerin hızlı bir şekilde kopyalanıp dağıtılabilmesi nedeniyle, filigran ekleme, içerik üreticileri ve hak sahipleri için vazgeçilmez bir araç haline gelmiştir [45-47].

Filigran ekleme, steganografi ile bazı ortak özelliklere sahiptir. Her iki teknik de veriyi medya içinde gizleme prensibine dayanır, ancak amaçları farklıdır. Steganografi, verinin varlığını gizlerken, filigran daha çok içeriğin kökenini ve sahipliğini belirlemeye yöneliktir. Bu, özellikle dijital medyanın kolayca kopyalanabilir ve değiştirilebilir olmasının yarattığı zorluklara bir çözüm sunar [48]. Ayrıca, filigran ekleme teknikleri, içeriğin bütünlüğünü korurken, bu içeriğin izinsiz kullanımını tespit etmek ve önlemek için de etkili bir yöntemdir.

Sonuç olarak; kriptografi, steganografi ve filigran ekleme, veri güvenliği ve iletişimi alanında birbirini tamamlayan, önemli teknolojilerdir. Her biri, dijital çağın getirdiği zorluklara karşı farklı çözümler sunarken, verilerin korunması ve güvenliğinin sağlanmasında hayati bir rol oynarlar. Bu teknolojilerin etkin kullanımı, dijital içeriğin korunması ve güvenli bir şekilde paylaşılması için temel bir gerekliliktir. Bahse konu bu üç yöntemin özelliklerine ilişkin karşılaştırma Tablo 2.1'de yer almaktadır.

Tablo 2.1. Bilgi güvenliği yöntemlerinin karşılaştırılması

	Kriptoloji	Steganografi	Filigran Ekleme
Amaç	Verilerin formunu anlaşılmaz hale getirmek	Gizli veriyi algılanamayacak şekilde saklamak	Kapak medyanın özgünlüğünü korumak
Kapak Seçimi	Uygulanamaz (doğrudan veri üzerinde)	Serbest kapak seçimi	Kısıtlamalar olabilir
İşlem çıktısı	Şifreli dosya	Stego dosya	Filigranlı dosya
Geçersiz Olma Durumu	De-şifre edilirse	Fark edilirse	Silinirse veya değiştirilirse
Saldırı Türü	Kriptoanaliz	Steganaliz	Her türlü görsel işlemeye karşı

2.2. Steganografi

Steganografi, iletişim güvenliğinin sağlanması amacıyla tarihsel süreçte önemli bir rol oynamış olan eski bir sanattır. Steganografi terimi, Yunancada 'Steganos' (saklanmış, gizli veya korunmuş) ve 'Graphtein' (yazı) kelimelerinden türetilmiştir, dolayısıyla bu terim tam olarak "gizli yazı" anlamına gelir [49].

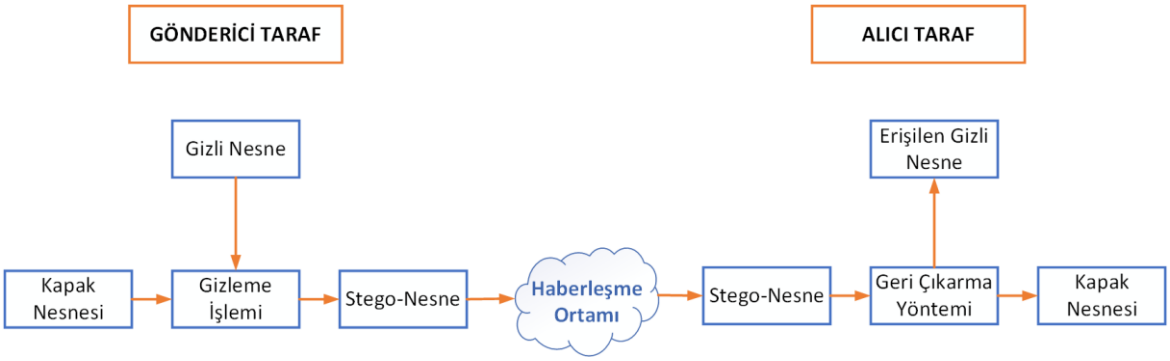
Temelde steganografi, hassas veya gizli bilgileri gizlemek ve bu bilgileri yetkisiz erişimden korumak amacıyla tasarlanmış bir dizi teknik ve metodolojiyi ifade eder.

Steganografinin kökenleri, antik çağlara kadar uzanmaktadır. Tarihsel belgeler, veri gizleme pratiğinin ilk örneklerinin antik çağlara kadar uzandığını göstermektedir. M.Ö. 485-525 yıllarında yaşamış olan tarihçi Heredot, bir eserinde, Pers İmparatorluğu ile Yunan şehir devleti arasındaki çatışma sırasında, Pers İmparatoru'na bir bilgi iletilirken veri gizleme metodunun kullanıldığını detaylandırmıştır. Gizli planın Perslere iletilmesi için ilk olarak, planı taşıyacak kişinin kafası tıraş edilmiştir. Ardından, taşıyıcının kafasına dövme ile gizli plan işlenmiş ve saçlarının uzaması beklenmiştir. Saçları uzadıktan sonra, taşıyıcı gizli mesajı iletmesi amacıyla yola çıkarılmıştır. Pers İmparatorluğuna ulaşan bu taşıyıcı, saçlarını tıraş ettirerek gizli bilgiyi iletmeyi başarmıştır. Antik Yunanda, insanlar gizli verileri bir tahtaya yazıp yüzeyini mum ile kapatarak gizlemişlerdir. Bu durum, objeyi kullanılmamış bir tablet gibi göstermiştir. Daha sonra mum eritildiğinde, içerisindeki gizli mesaj açığa çıkartılıp okunabilmiştir [50,51]. 17. yüzyılda, Gaspar Schott isimli bir sanatçı, müzik notaları arasında bilgi gizleme tekniği geliştirmiştir. Schott'un “Schola Steganographica” isimli eserinde detaylandırdığı bu teknikte, her bir nota spesifik bir harfi temsil etmektedir [52]. Almanlar, İkinci Dünya Savaşı'nda birbirlerine gönderdikleri sıradan bir metinde her sözcüğün sadece baştan ikinci harflerini kullanarak veriyi gizlemişler. Bu ikinci harfleri yan yana getirdiklerinde oluşan cümle ile gizli verileri iletmeyi başarmışlardır [53].

Zaman içinde dijital çağın getirdiği teknolojik yeniliklerle birlikte steganografi teknikleri de evrim geçirmiştir. Modern çerçevede, steganografinin temelini Simmons tarafından ortaya konulmuş olan mahkum problemi oluşturmuştur [54]. Bu senaryoda, iki mahkum, birbirleriyle gizli bir şekilde haberleşme ihtiyacı duymaktadırlar. Bu süreçte, gardiyan gözetimi altındadırlar. Gardiyan, herhangi bir iletişimi denetleme yetkisine sahip olup, şifreli mesajlar tespit ettiğinde ilgili tutuklulara yaptırım uygulama hakkına sahiptir.

Bu bağlamda, mahkumların, gardiyanın şüphesini uyandırmadan haberleşebilmek için steganografi gibi gizleme tekniklerine başvurmaları gerekmektedir. [55].

Modern steganografi uygulamaları, gizli bilgileri fark edilemez bir şekilde taşıyıcı medya dosyaları içerisine gizlemeyi amaçlamaktadır. Steganografik sistemin genel çalışma mantığını özetleyen diyagram Şekil 2.2'de yer almaktadır. Görselden anlaşılacağı üzere, gizlenmesi gereken hassas veriler, bir veri gizleme algoritması kullanılarak, kapak nesnesi olarak adlandırılan taşıyıcı bir nesnede küçük değişiklikler yapmak suretiyle saklanır. Bu taşıyıcı metin dosyaları, dijital görüntüler, ses dosyaları veya video dosyaları gibi farklı formatlarda olabilir. Gizlenmesi istenen mesaj de metin, ses, görüntü, video vb. formatlarda olabilir. Gizleme işlemi sonucu oluşan, gizli veriyi içeren dijital nesne "stego" olarak adlandırılır. Stego nesne üzerine veri çıkarma algoritması uygulanarak da gizlenmiş nesneye yeniden ulaşılabilir.



Şekil 2.2. Steganografik sistemin blok diyagramı [56].

Steganografik işlemler, gizli bilgileri taşıyıcı medya dosyasının içine yerleştirirken, bu medya dosyasının görsel veya akustik özelliklerini korumayı ve bu şekilde gizli bilgilerin yetkisiz kişiler tarafından tespit edilememesini amaçlamaktadır. Steganografi, kriptografi ile birlikte, dijital iletişim güvenliği ve veri saklama alanlarında kritik bir öneme sahiptir ve geniş bir uygulama yelpazesi sunmaktadır.

Steganografik sistemlerin dört temel özelliği vardır: algılanamazlık, güvenlik, bilgi gizleme kapasitesi ve dayanıklılık.

Algılanamazlık, gizli verinin kapak nesnesine entegre edilmesi sırasında gözle görülür veya istatistiksel olarak tespit edilebilir her hangi bir iz bırakmamasını ifade etmektedir. Bu kritik özellik, gizli verinin varlığının, hem insan görsel algısı hem de istatistiksel analiz yöntemleri tarafından saptanamayacak derecede gizli kalmasını gerektirmektedir [57].

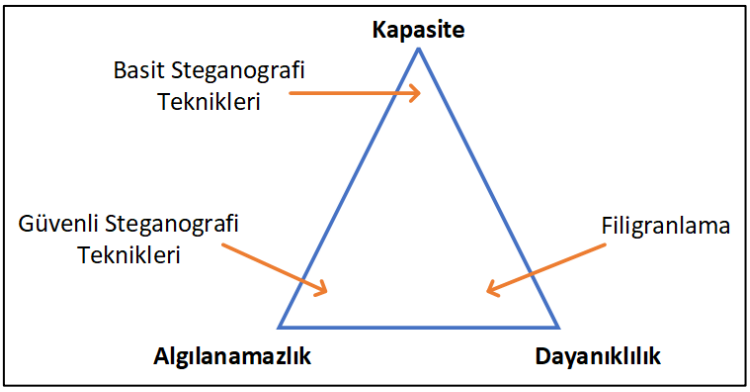
Algılanamazlık, steganografik tekniklerin başarısının en önemli göstergelerinden biri olarak kabul edilir. Bu kavram, steganografinin temel amacı olan gizliliği korumakla doğrudan ilişkilidir. Algılanamazlık, verinin taşıyıcı ortama gizlenmesi sonucu kapak resminde bir miktar gürültü oluşsa bile, oluşabilecek herhangi bir kalite düşüşünü veya gözle görülür değişikliği en aza indirgeyerek, kapak nesnesinin doğal görünümünü ve işlevselliğini korur [58]. Etkin bir algılanamazlık, gizli verinin varlığını sadece yetkili alıcılar için erişilebilir kılar, bu da steganografiyi güvenli veri iletimi için uygun bir yöntem haline getirir.

Steganografik bir sistem içinde, "güvenlik" kavramı, genellikle "algılanamazlık" veya "tespit edilemezlik" prensiplerini içerir. Güvenlik, gizli verinin istatistiksel analiz veya bir saldırgan tarafından tespit edilememesi, tespit edilse bile kaldırılamaması ve çıkarılamaması yeteneği ile tanımlanır [56]. Steganografi işleminin temel amacı, gizli verinin güvenli bir şekilde iletilmesidir ve bu nedenle güvenlik, verinin açık bir kanal üzerinden yetkisiz erişimden korunması için kritik öneme sahiptir.

Veri kapasitesi, steganografik işlem sırasında taşıyıcı medya içine g gizli verinin miktarını tanımlar. Daha fazla gizli veri gizleme kapasitesi, daha fazla bilgiyi taşıyıcı nesne içine gömmeyi mümkün kılar. Ancak, bu kapasitenin artırılması, taşıyıcı medya üzerinde yapılacak değişikliklerin algılanma riskini de artırabilir. Bu nedenle, steganografi uygulamalarında yük kapasitesi önemli bir denge kavramıdır. Etkili bir steganografik sistemin temel amacı, en fazla miktarda bilgiyi kapak nesnesinde en az değişikliğe neden olacak şekilde iletmektir [59]. Veri kapasitesi, bit cinsinden ölçülen gizli bilginin miktarının kapak medyasına boyutuna oranı olarak tanımlanabilir.

Dayanıklılık kavramı, steganografik işlemin, stego nesne üzerinde yapılan dışsal değişikliklere karşı etkinliğini sürdürebilme yeteneğini ifade eder. Örneğin, bir stego-nesnenin döndürülmesi, ölçeklendirilmesi veya yeniden boyutlandırılması gibi dışsal müdahalelere rağmen gizli bilginin başarıyla çıkarılabilmesi, bir steganografik sistemin dayanıklı olup olmadığını belirler [60-61]. İyi bir dayanıklılık seviyesi, steganografinin güvenilirliğini artırır, çünkü stego-nesnenin dışsal değişikliklere karşı dayanıklı olması, gizli verinin kaybını veya bozulmasını engeller. Şekil 2.3.'de veri gizleme özellikleri arasındaki denge gösterilmektedir. Her steganografi yöntemi, bu özellikler arasında bir denge kurmaya çalışır ve kullanım senaryosuna bağlı olarak tercih edilen özellikler değişebilir. Örneğin, bir uygulamada daha fazla veri saklama önemliyken, diğer bir uygulamada gizlilik önceliklidir.

Bu nedenle, steganografi yöntemi seçerken bu dengelemeyi göz önünde bulundurmak önemlidir.



Şekil 2.3. Veri gizleme özellikleri arasındaki denge üçgeni [62].

2.2.1. Görüntü Steganografisi

Görüntü steganografisi genel anlamda kapak nesnesinin resim olarak seçildiği uygulamaları ifade etmektedir. Steganografide, metin, ses, video ve dijital görüntüler gibi farklı dosya türleri içinde veri gizlemek mümkündür. Gizlenen veriler de kapak resminde olduğu gibi değişik formatlarda kullanılabilir [63]. Ancak bu format zenginliğinin yanında görüntü steganografisi, steganografinin itici gücüdür. Bunun en temel nedenleri şu şekilde özetlenebilir;

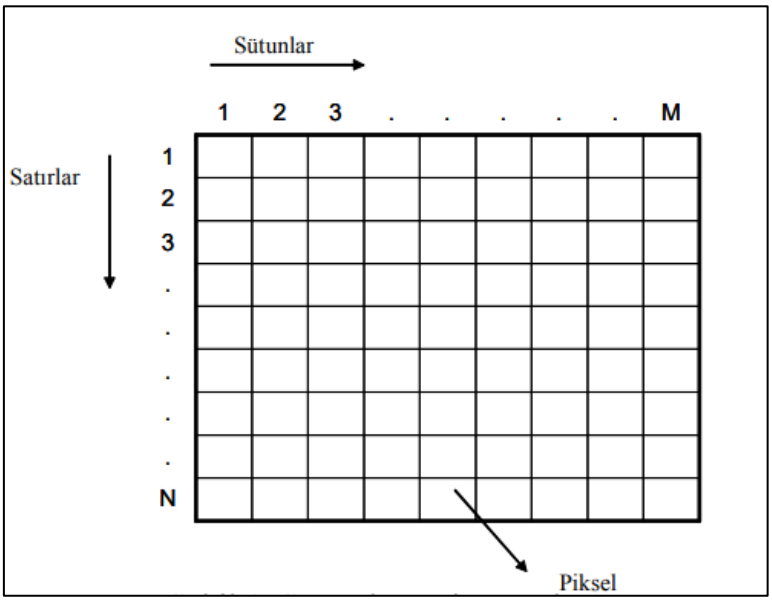
- Erişilebilirlik ve paylaşım kolaylığı:
  Görüntülerin kolayca taşınabilir ve internet üzerinden rahatlıkla paylaşılabilir olmasıdır. Ses ve video gibi formatlar büyük dosya boyutlarına sahip olup paylaşımı ve erişimi daha zor olabilmektedir.
- Yüksek kapasite:
  Resimler büyük miktarda veriyi saklayabilecek geniş bir alana sahiptir. Her bir piksel veya renk kanalı gizli veriler için kullanılabilir. Metinin kapak nesnesi olarak kullanıldığı bir senaryoda gizlenebilecek veri miktarı daha düşüktür.
- Görsel algıya dayanıklılık:
  İnsan gözü, küçük değişiklikleri ayırt etmede sınırlıdır. Görüntü steganografisinde yapılan küçük değişiklikler, örneğin bir pikselin rengindeki hafif bir ton değişikliği, genellikle gözle fark edilmez. Bu, gizli veriyi etkili bir şekilde gizlemenin yanı sıra, görüntünün görsel kalitesini korumak için de önemlidir [64]. Öte yandan video veya

ses dosyalarında yapılan değişiklikler, özellikle kalite ve bütünlük açısından daha kolay fark edilebilmektedir.

- Çoklu uygulama alanları:
  Görüntü steganografisi, telif hakkı koruma, kimlik doğrulama, gizli iletişim ve veri güvenliği gibi çeşitli alanlarda kullanılabilir.
- Teknolojik Gelişmelere Uyumluluk:
  Görüntü işleme teknolojilerindeki yenilikler, gelişmiş algoritmalar ve artan işlem gücü, daha karmaşık ve etkili görüntü steganografi yöntemlerinin geliştirilmesine olanak tanır. Özellikle yapay zeka ve makine öğrenimi, görüntü steganografisini daha da geliştirmekte ve daha sofistike hale getirmektedir.

2.2.2. Sayısal Görüntüler

Şekil 2. 4'de de görüldüğü gibi resim piksellerden oluşan bir matristir. Piksel resmi oluşturan en küçük yapıtaşı olarak ifade edilebilir. Matrisin yatay ekseni, resmin sütunlarını temsil ederken, dikey eksen satırları temsil eder. Resimdeki her piksel, bu matriste bir koordinatla belirlenir; örneğin, (1,2) ikinci sütunun ilk satırındaki pikseldir. "N" ve "M" harfleri matrisin boyutlarını gösterir; "N" satır sayısını, "M" ise sütun sayısını ifade eder. Matrisin boyutu, resmin çözünürlüğünü belirler; yani "N x M" boyutunda bir matris, toplamda N x M sayıda piksele sahiptir.



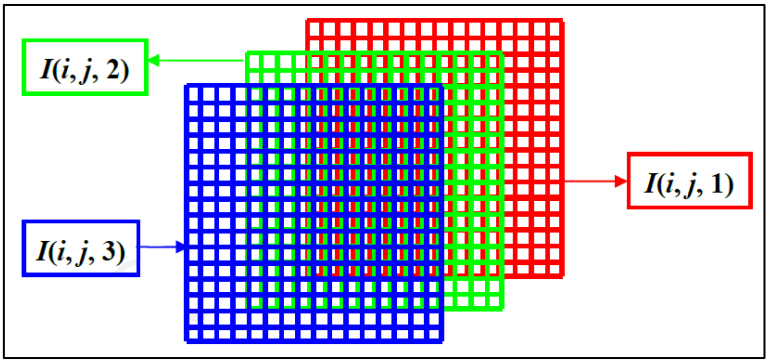
Şekil 2.4. Sayısal resimlerin genel yapısı [65].

Bit derinliği, bir pikselin renk bilgisini ifade etmek için kullanılan bit sayısını ifade eden bir kavramdır. Daha yüksek bit derinliği, daha fazla renk ve tonlama seçeneğini mümkün kılmaktadır.

İkili resimler en basit resim türüdür ve her piksel için sadece 1 bit kullanılır. Bu da demektir ki her piksel ya siyah ya da beyaz olabilir. Burada bit derinliği 1'dir çünkü her piksel için sadece iki olası durum vardır (0 veya 1).

Gri tonlamalı resimlerde, her bir pikselin farklı bir gri tonunun ifade edebilmesi için daha fazla bit kullanılır. Genellikle 8 bit derinlik kullanılır, bu da her bir piksel için 2^8, yani 256 farklı gri tonu oluşturulabileceği anlamına gelir. Burada 0 tam siyahı, 255 ise tam beyazı ifade eder ve aradaki sayılar çeşitli gri tonlarına karşılık gelmektedir.

Renkli resimler genellikle RGB renk modelini kullanır ve her bir renk kanalı (Kırmızı, Yeşil, Mavi) için ayrı bit derinliği barındırır. Şekil 2.5. RGB görüntüsüne ilişkin renk kanallarını temsil eden bir görsel sunmaktadır. Eğer her bir renk kanalı için 8 bit kullanılıyorsa, bu 24 bit renk (8 bit x 3 kanal) anlamına gelir ve teorik olarak 2^{24} yani 16,777,216 farklı renk oluşturulabilir. Bu da oldukça detaylı ve renkli görüntüler oluşturulmasını sağlamaktadır [6]. Renkli resimlerin bu üç kanallı yapısı, gizli veriyi entegre etmek için daha fazla alan sağlar ve böylece steganografik tekniklerle daha fazla verinin kodlanmasına izin verir.

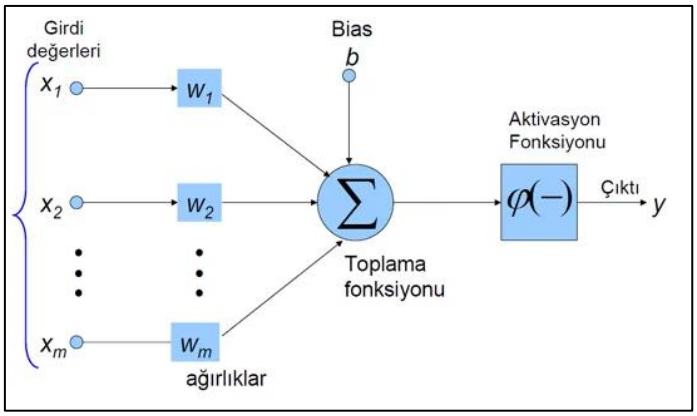


Şekil 2.5. RGB görüntüsünü oluşturan renk kanalları gösterimi [66].

2.3. Yapay Sinir Ağları (Artificial Neural Networks-ANN)

Yapay sinir ağları, insan beyninin işlevini taklit eden bilgisayar algoritmalarıdır ve bu görseldeki gibi nöronlar, bu algoritmaların temel yapı taşlarıdır. Şekil. 2.6 ‘da görüldüğü

gibi nöron yapısı giriş değerleri, ağırlıklar, bias, toplama fonksiyonu ve aktivasyon fonksiyonu ve çıktı değerlerinden oluşmaktadır.



Şekil 2.6. Yapay nöron yapısı [67].

Girdi Vektörü: Nöronun işleyeceği veri serisini içermektedir. Her bir elemanı, ağırlıklandırma sürecine dahil edilmek üzere nörona verilir.

Ağırlıklandırma: Her bir girdi değeri, nöronun çıktısında ne kadar etkili olacağını belirleyen ağırlıklar ile çarpılmaktadır. Bu ağırlıklar, eğitim aşamasında belirlenen ve sürekli güncellenen parametrelerdir ve ağın öğrenme kabiliyetini doğrudan etkiler.

Toplama Fonksiyonu: Ağırlıklandırılmış girdilerin toplanması işleminin gerçekleştirildiği yerdir. Bu toplam, aktivasyon fonksiyonuna giriş olarak hizmet eder.

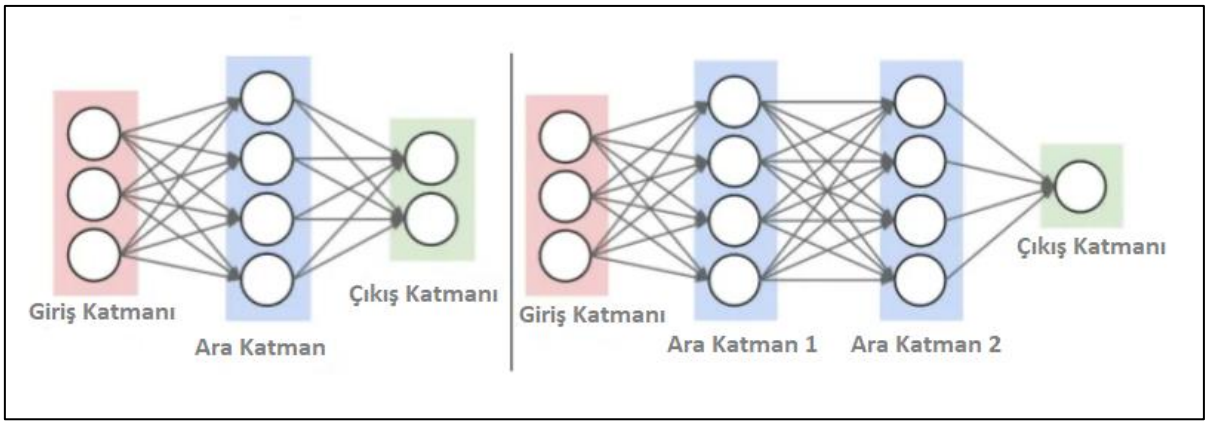
Bias: Toplama fonksiyonuna eklenen ve nöronun aktivasyon eşiğini ayarlamaya yarayan bir sabittir. Ağırlıklar gibi, bias da eğitim sürecinde optimize edilen bir parametredir ve modelin daha geniş bir veri yelpazesine genelleme yapabilmesinin önemli bir unsuru olarak görev yapmaktadır.

Aktivasyon Fonksiyonu: Önceki katmandan gelen, ağırlıklandırılmış girdilerin toplamını işleyen ve ardından genellikle doğrusal olmayan bir çıktı değeri üreten fonksiyondur [68].

Şekil 2.6'da yer alan görsel matematiksel olarak (2.1) ile ifade edilebilir. Girdi değerleri (x), ilgili ağırlıklar (w) ile çarpılır ve toplama fonksiyonu ile toplanır, bu toplama bias (b) değeri eklenir ve böylece Z değerine erişilir. Sonra elde edilen toplam, aktivasyon fonksiyonu ile işlenir ve nöronun çıktısı *y* olarak elde edilir [69].

$$Z = \sum_{i=1}^{n} x_i \, w_i + b \tag{2.1}$$

Şekil 2.7’de gösterildiği gibi yapay sinir ağları, genellikle üç ana katmandan oluşan bir yapıya sahiptir.



Şekil 2.7. Tek katmanlı ve çok katmanlı sinir ağı yapısı [70].

Giriş katmanı, verilerin sinir ağına girdiği ilk noktadır. Giriş katmanı, her biri bir veri öğesine karşılık gelen düğümler içermektedir.

Ara katman (gizli katman), en az bir katmandan oluşan ve giriş ile çıkış katmanı arasındaki işlemi gerçekleştiren katmandır. Bu katmanda, veriler üzerinde ağırlıklarla ve biaslarla çeşitli matematiksel işlemler yapılarak, öğrenme süreci gerçekleştirilir. Ara katmanların sayısı, modelin hesaplama yükünü ve algoritmik karmaşıklığını belirleyen önemli parametrelerdendir. Kullanılan modelin türüne göre, bu katmanların sayısı değişebilmektedir [71].

Çıkış katmanı, elde edilen sonuçların temsil edildiği bölümdür. Ara katmanlardan iletilen verilerin işlenmesi sonucu elde edilen çıktılar bu katmanda formüle edilir. Hata fonksiyonları tahmin edilen değerler ile gerçek değerler arasında uyumsuzluğu hesaplar. Optimizasyon algoritmaları bu hata metriğini temel alarak ağırlık parametrelerinin ayarlanmasını gerçekleştirir. Bu süreç, modelin doğru tahminler yapmayı öğrenmesini sağlar [72].

2.4. Derin Öğrenme (Deep Learning, DL)

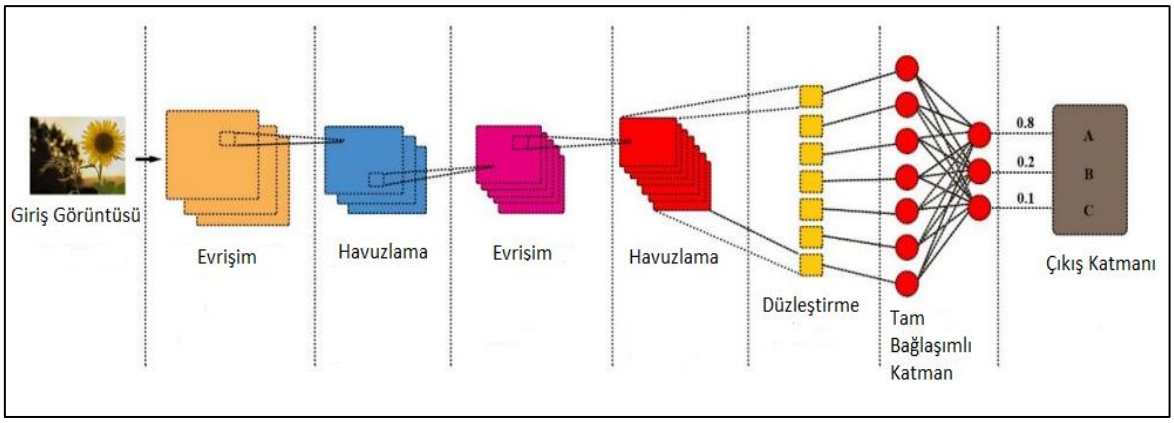
Derin öğrenme, yapay zeka araştırmalarının öncü ve dinamik bir dalı olarak öne çıkmakta olup, çok katmanlı sinir ağlarına dayalı algoritmaları içermektedir. Bu alan, insan beyninin işlevsel yapısını modelleyen ve çok sayıda katmandan oluşan yapay sinir ağları teknolojilerini temel alır. 1980'li yıllardan itibaren geliştirilen derin öğrenme, görüntü ve ses işlemeden doğal dil işlemeye, stratejik oyun analizlerinden karmaşık veri analizlerine kadar

geniş bir uygulama alanına sahiptir. Daha somutlaştırmak gerekirse, insanların biyometrik özelliklerini tanıma [73-75] ve duygusal durumlarını analiz etme [76], nesne algılama [77] ve sınıflandırma [78], tıbbi tanı süreçlerinin doğruluğunu ve hızını artırma [79] gibi çok fonksiyonel kullanım alanlarına mevcuttur.

Derin öğrenme, geniş veri kümelerinden elde edilen karmaşık desenleri ve yapıları analiz ederek, bu bilgileri benzer yeni veri setleri üzerinde tahminlerde bulunmak için kullanılır. Bu süreç, özellikle büyük verinin ve hesaplama gücünün artan erişilebilirliği ile birlikte, sağlık bilimlerinden finansa, eğitimden endüstriyel otomasyona kadar çeşitli sektörlerde etki yaratma potansiyeline sahiptir. Büyük veri, çok çeşitli kaynaklardan toplanan, işlenen ve analiz edilen devasa veri kümelerini ifade eder. Büyük veri, yapay zeka ve özellikle derin öğrenme sistemlerinin eğitiminde kullanılan temel kaynaktır. Öte yandan, hesaplama gücünün artan erişilebilirliği, daha güçlü işlemcilerin, bulut bilişim hizmetlerinin ve diğer ileri teknolojilerin daha geniş kullanıcı kitlesine ulaşmasını ve daha uygun maliyetle erişilebilir olmasını ifade etmektedir. Bu gelişmeler, derin öğrenme algoritmalarını eğitmek ve çalıştırmak için gerekli olan yoğun hesaplama işlemlerin daha hızlı ve etkili bir şekilde gerçekleştirilmesini sağlamakta ve derin öğrenme teknolojisinin çeşitli alanlarda uygulama başarısını ve verimliliğini önemli ölçüde artıran temel faktörler arasında yer almaktadır.

Derin öğrenme, hem faydalı yönleriyle hem de bazı zorluklarıyla dikkat çekmektedir. Bu teknolojinin en önemli avantajları arasında, geniş ve karmaşık veri setlerini işleyebilme ve veri özelliklerini otomatik olarak çıkarma yeteneği, lineer olmayan sorunları çözme becerisi, gelecek tahminleri yapabilme, genellemeler oluşturabilme ve Grafik İşlem Birimi (Graphics Processing Unit, GPU) destekli yüksek hesaplama gücü sayılabilir. Öte yandan, yüksek sayıda parametre içermesinden dolayı modelin eğitim veri setindeki küçük detayları ve hatta gürültüyü bile öğrenmesinden kaynaklanabilecek aşırı uyum (overfitting) sorunu, büyük miktarda veri gereksinimi ve bu verilerin her zaman elde edilememesi, konu üzerine uzman sayısının sınırlı olması, parametre seçimlerindeki standart eksikliği ve yüksek maliyetli GPU'lar ve donanımlar gerektirmesi derin öğrenmenin sayılabilecek bazı dezavantajlarıdır [69].

Standart bir derin öğrenme modeli, bir giriş katmanı, çok katmanlı evrişim ve havuzlama işlemleri ile zenginleştirilmiş ara katmanlar ve bir çıkış katmanından oluşmaktadır. Modelin ara katmanları, klasik sinir ağlarının yapısından daha derin ve detaylıdır. Şekil 2.8'de, bu modelin yapısal bir özeti grafiksel olarak göstermektedir.



Şekil 2.8. Derin öğrenme mimarisi örneği [81].

Görüntü işleme ve analizinde, Evrişimsel Sinir Ağları sıklıkla başvurulan ve etkili sonuçlar sunan derin öğrenme modellerindendir. CNN'lerin temel taşı olan evrişim katmanları, girdi olarak alınan verilerden öznitelikleri çıkarmada kritik rol oynar. Bu yapay zeka modeli, girdi olarak verilen görüntülerdeki önemli desenleri ve yapıları algılayarak, nesne tanıma, izleme, sınıflandırma ve biyomedikal görüntü işleme gibi çeşitli alanlarda başarıyla kullanılmaktadır. CNN'lerin bu uygulamalardaki etkinliği, onları görüntü tabanlı analiz gerektiren pek çok alanda kullanılan bir araç haline getirmektedir.

2.4.1. Katmanlar

Temel bir CNN modeli, aşağıda açıklanan temel katmanları içermektedir.

a) Giriş Katmanı:

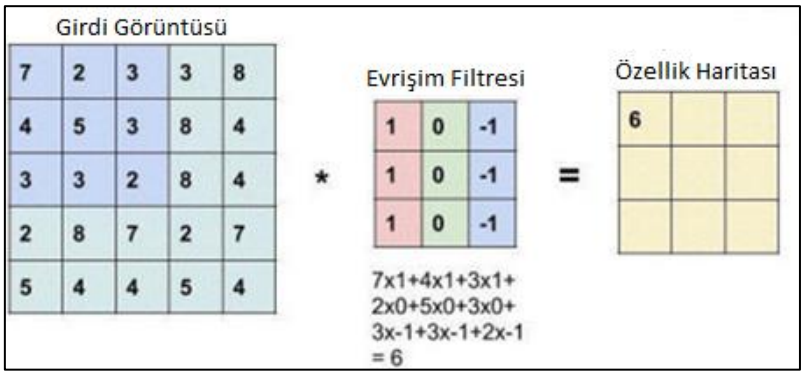
CNN'nin ilk katmanı olarak işlev gören giriş katmanı, genellikle ham veriyi (örneğin, bir resim) alır ve bu veriyi diğer katmanlara işlenmek üzere aktarır. Görüntü işlemede bu giriş, genellikle yükseklik, genişlik ve renk kanallarının (RGB) ölçülerini içeren üç boyutlu bir dizi, yani bir tensör olarak ifade edilir. Örnek olarak, bir resmin 200x200 piksel çözünürlüğünde ve 3 renk kanalına sahip olması durumunda, bu resim 200x200x3 boyutlarında bir tensör olarak tanımlanır. CNN mimarilerinde, giriş katmanında işlenecek görüntü boyutlarının belirlenmesi, modelin eğitim sürecinin hızı ve gerektireceği hesaplama kaynakları üzerinde önemli bir etkiye sahiptir. Büyük boyutlu görüntüler, hesaplama yükünü ve bellek ihtiyacını artırarak eğitim sürecini uzatabilirken, daha küçük görüntüler bu kaynakları daha az tüketir, fakat bu durum modelin öğrenme kapasitesini ve sonuç olarak tahmin başarısını sınırlayabilir [81].

b) Evrişim Katmanı (Konvolüsyon Katmanı):

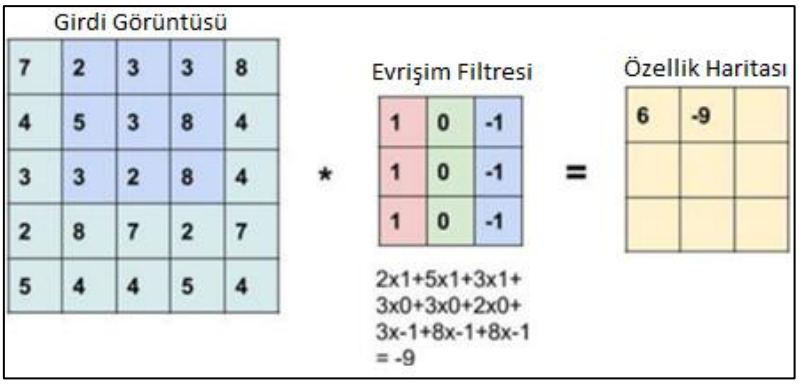
Evrişim katmanlarının temel öğeleri küçük, öğrenilebilir matrisler olan filtreler veya çekirdeklerdir. Evrişim süreci, görüntüyü oluşturan matrisler üzerinde, boyutu daha küçük bir filtre kullanarak gerçekleştirilen özellik tespiti işlemi olarak ifade edilebilir [82]. Evrişim işlemi sırasında filtre, giriş görüntüsünün üzerinde kaydırılarak, her bir konumda filtre ile giriş verisi arasında bir matris çarpımı gerçekleşir. Filtrenin içindeki her bir eleman, filtrenin üzerinde bulunduğu veri noktalarının karşılık gelen piksel değerleri ile çarpılır. Bu çarpma işlemlerinin her biri için elde edilen değerler toplanır ve bu toplam, sonuç olarak bir çıktı değerini oluşturur [83]. Bu işlem, filtrenin kapsadığı alandaki özelliklerin bir özetini çıkarmaktadır. Filtre kaydırılarak görüntünün tüm alanı tarandığında, elde edilen sonuçlar bir özellik haritası (feature map) oluşturur. Bu özellik haritası, filtrenin algıladığı özelliklerin giriş görüntüsü üzerindeki dağılımını temsil etmektedir [84].

Her bir evrişim katmanı genellikle çok sayıda filtre içerir ve her bir filtre kendi özellik haritasını üretir. Bu özellik haritaları, giriş görüntüsünün farklı özelliklerini temsil eder. Bir sonraki evrişim katmanı, bu özellik haritalarını giriş olarak alır ve daha yüksek seviyeli özellikler öğrenir.

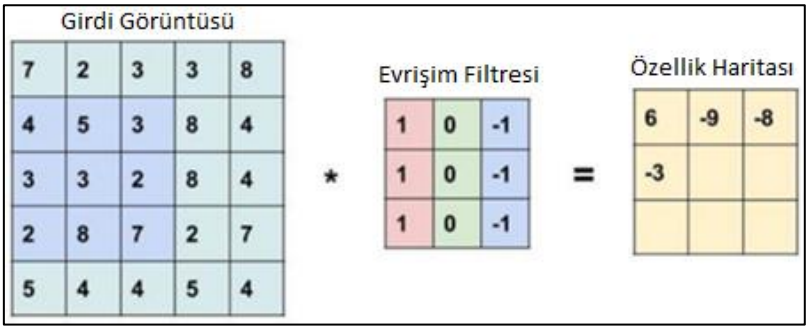
Şekil 2.9-2.12'de adım adım evrişim işlemi gösterimi yapılmıştır.



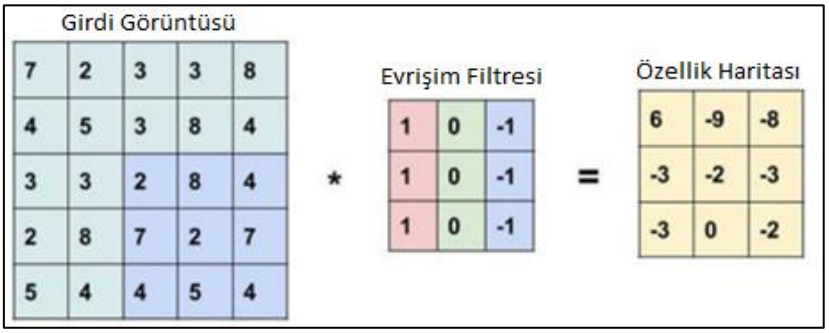
Şekil 2.9. Evrişim işlemi 1. adım [85].



Şekil 2.10. Evrişim işlemi 2. adım [85].

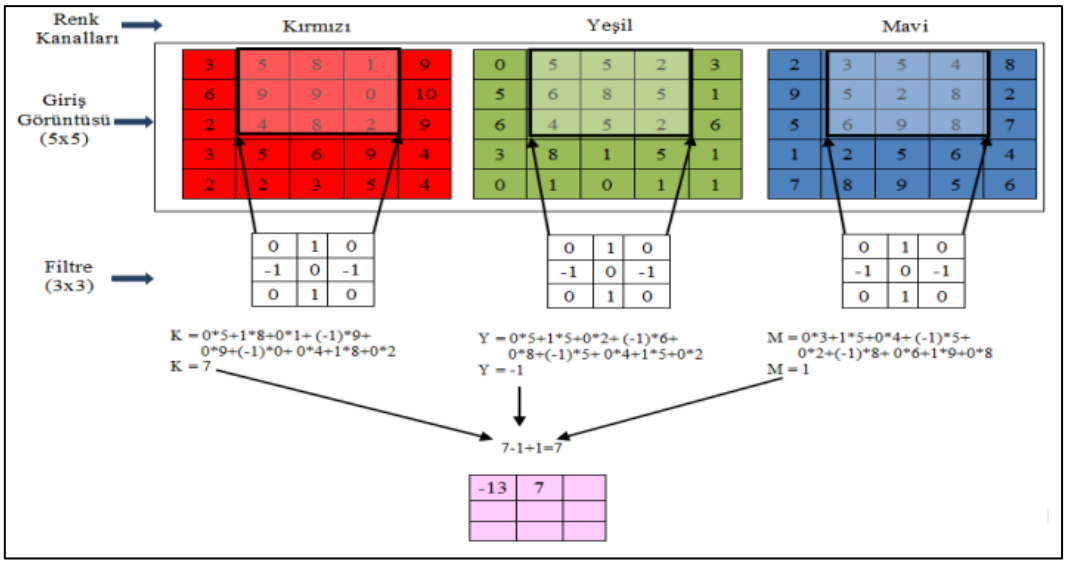


Şekil 2.11. Evrişim işlemi 4. adım [85].



Şekil 2.12. Evrişim işlemi son adım [85].

Bahsedilen bu evrişim adımlarında tek kanallı bir görüntü örneği üzerinden ilerlenmiştir. Ancak giriş görüntüsü RGB gibi üç ayrı renk kanalını içeriyorsa, bu süreç her bir kanal için ayrı ayrı gerçekleştirilir. Her renk kanalında yer alan değerler, ilgili evrişim filtresi katsayıları ile çarpılır ve en son bu değerlerin toplamı hesaplanır. Uygulanan filtrenin katsayıları, her bir renk kanalı matrisi için aynı kullanılabileceği gibi farklılık da gösterebilir [84]. RGB bir giriş görüntüsü için evrişim işlemi Şekil 2.13'de yer almaktadır.



Şekil 2.13. Evrişim İşlemi Son Adım [84].

Bu gösterilen evrişim işlemi aşamalarında filtrenin adım boyutu (stride size) 1 değerindedir. Adım boyutu ifadesi, filtrenin giriş matrisi üzerindeki her bir hareketinde kaç satır ve sütun kayacağını belirten parametredir. Örneğin, adım boyutu 1 ise, filtre her seferinde bir sütun veya satır ilerlemektedir. Adım boyutu arttıkça, çıktı matrisinin boyutu küçülmektedir.

Evrişim işlemi sonucunda elde edilecek özellik haritasının boyutu, girdi görüntüsü ve evrişim filtresi boyutlarına göre (2.2)'de gösterildiği gibi hesaplanabilmektedir [86].

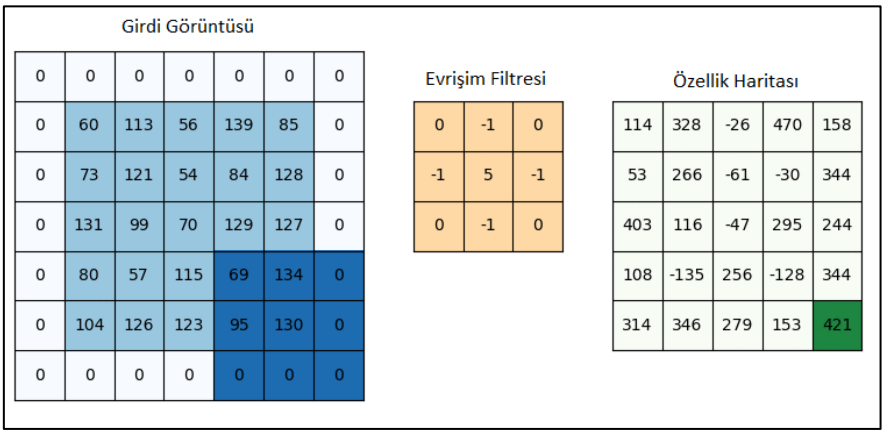
$$\text{Özelllik haritası boyutu} = \frac{\text{Girdi görüntüsü boyutu} - \text{Evrişim filtresi boyutu}}{\text{Adım boyutu}} + 1 \qquad (2.2)$$

Şekil 2.9-2.12'de verilen örnek üzerinde ilerlediğimizde (2.3) ile hesaplandığı gibi özellik haritası boyutu 3 olarak elde edilmektedir.

$$\text{Özelllik haritası boyutu} = \frac{5-3}{1} + 1 = 3 \qquad (2.3)$$

Görüldüğü gibi girdi görüntüsü üzerinde evrişim filtresini kaydırarak elde ettiğimiz özellik haritası matrisinin boyutu giriş matrisine göre küçülmektedir. Bu durumun istenmediği durumlarda, sıfır dolgusu (zero padding) işlemi, görüntünün boyutunun küçülmesini önlemek için uygulanabilir. Bu yöntemle, bir görüntü veya veri matrisinin etrafına ekstra sıfır değerleri eklenir. Bu eklemeler, evrişim işlemleri sırasında ve özellikle

de ağın derinleştiği durumlarda verinin boyutunun azalmasını engellemeyi ve kenar bölgelerdeki bilgilerin daha etkin şekilde işlenmesini sağlamaktadır [87]. Şekil 2.14'de giriş görüntüsü etrafına 0 değerlerinin eklemesiyle oluşan dolgulama işlemi örneği yer almaktadır.



Şekil 2.14. Dolgulama yöntemi ile evrişim işlemi örneği [88].

Doldurma işlemi yapıldığında, özellik haritasının boyutları, (2.4) formülü kullanılarak belirlenir [86].

$$\text{Özelllik haritası boyutu} = \frac{\text{Girdi görüntüsü boyutu} + 2 \text{ x Dolgulama boyutu} - \text{Evrişim filtresi boyutu}}{\text{Adım boyutu}} + 1 \quad (2.4)$$

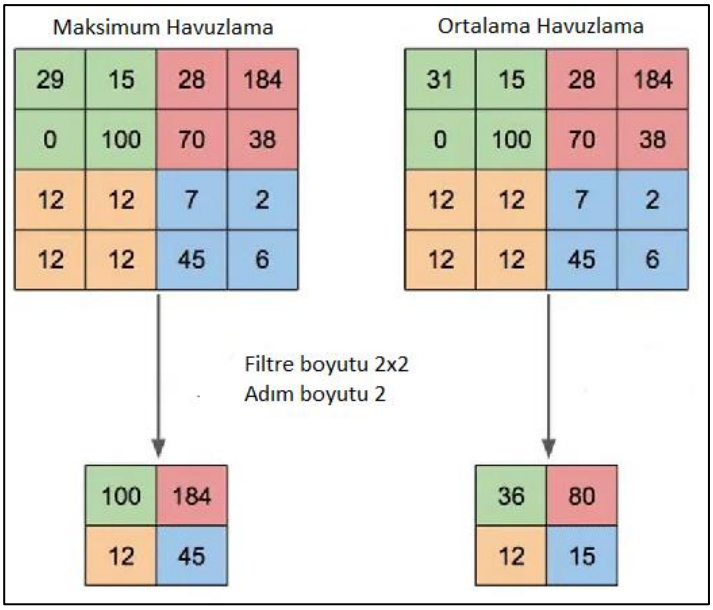
Şekil 2.14'de yer alan örnek üzerinde ilerleyerek (2.4)'ü uyguladığımızda girdi görüntüsünün boyutunun, evrişim işlemi sonrasında dolgulama işlemi sayesinde aynı kaldığını (2.5) ile görebiliriz.

$$\text{Özelllik haritası boyutu} = \frac{5+2 \text{ x } 1-3}{1} + 1 = 5 \quad (2.5)$$

c) Havuzlama Katmanı:

Evrişimli sinir ağlarının havuzlama katmanı, derin öğrenme yapılarında işlem yükünü azaltmak için kritik bir rol oynar. Havuzlama işlemi sırasında, görüntünün derinlik özelliği korunurken, genişlik ve yükseklik boyutları küçültülür. Evrişim katmanının ardından oluşan genişlemiş özellik haritaları, eğitim sürecinde önemli miktarda hesaplama yüküne sebep olur. Havuzlama katmanı, bu haritaların uzamsal boyutlarını ve parametrelerini efektif bir şekilde azaltarak, ağın toplam işlem yükünü önemli ölçüde hafifletir. Bu strateji, ağın verimli bir şekilde eğitilmesini sağlar ve kaynak kullanımını optimize eder [89].

Havuzlama, veri işleme sürecinde çeşitli teknikler kullanılarak gerçekleştirilir. Bu tekniklerde, bir önceki katmandan alınan veri üzerinden belirli bir pencere gezdirilir ve bu pencereye denk gelen değerler incelenir. Eğer bu pencere içerisindeki en yüksek değer esas alınıyorsa, bu yönteme maksimum havuzlama denir. Diğer yandan, pencere içindeki değerlerin aritmetik ortalaması hesaplanarak kullanılıyorsa, bu işleme ortalama havuzlama adı verilir [90]. Maksimum havuzlama yöntemi, önemli özellikleri temsil eden en yüksek değerleri seçmesi nedeniyle, gürültülü verinin bir sonraki katmana iletilmemesi konusunda avantaj sağladığından literatürde daha yaygın olarak yer almaktadır [91]. Şekil 2.15'de iki havuzlama yöntemi için de örnek bir gösterim verilmiştir.



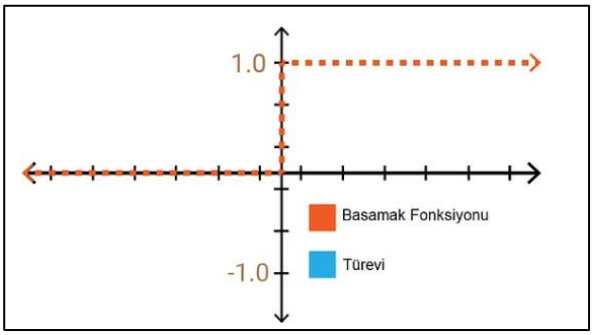
Şekil 2.15. Havuzlama işlemi [92].

Evrişimli sinir ağlarındaki evrişim ve havuzlama katmanlarının kaç adet olacağı esnek bir şekilde ayarlanabilir. Her katmanın eklenmesiyle, mimari daha detaylı ve karmaşık özniteliklerin elde edilmesine olanak sağlar, bundan dolayı daha derin bir özellik alanına ulaşılır [86].

Bu katmanlara ek olarak, evrişim katmanından hemen sonra aktivasyon fonksiyonları kullanılmaktadır. Aktivasyon fonksiyonlarının CNN'lerde kullanılmasının en temel amacı, ağın doğrusal olmayan özellikleri öğrenebilmesini sağlamaktır. Bu fonksiyonlar, modelin karmaşık ve doğrusal olmayan ilişkileri anlamasına yardımcı olur. Özellikle görüntü işleme gibi karmaşık senaryolarda, bu doğrusal olmayan ilişkilerin anlaşılması esastır. Eğer aktivasyon fonksiyonları kullanılmasaydı, CNN'lerin her katmanı basitçe doğrusal bir

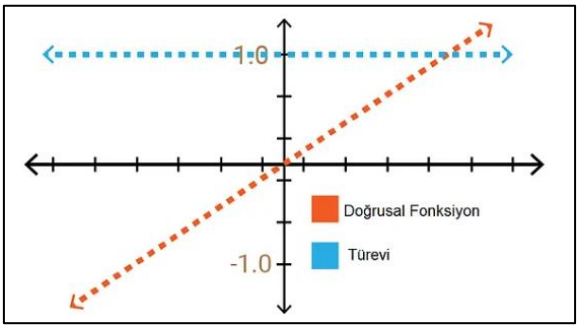
dönüşüm işlemi gerçekleştirecekti. Bu durumda, ne kadar çok katman eklenirse eklensin, ağın tümü yine de temelde bir doğrusal fonksiyonu temsil edecekti. Bu, ağın yalnızca doğrusal problemleri çözebileceği anlamına gelirdi ki bu da görüntü işleme, nesne tanıma ve benzeri karmaşık görevler için yetersiz kalırdı. Özetle, aktivasyon fonksiyonları olmadan, ağın karmaşık örüntüleri ve özellikleri öğrenmesi, dolayısıyla etkili tahminler yapabilmesi mümkün olmazdı [93]. Farklı problemlere göre geliştirilmiş ve literatürde kullanılan çeşitli aktivasyon fonksiyonları mevcuttur.

Basamak (step) fonksiyonu, ikili değerler üretir ve daha yaygın olarak ikili sınıflandırma görevlerinde kullanılır. Bu nedenle, genellikle sinir ağlarının çıkış katmanlarında tercih edilir. Gizli katmanlarda bu fonksiyonun kullanımı önerilmez, çünkü Şekil 2.16'da gösterildiği gibi türevi alındığında öğrenme sürecine katkı sağlayacak bir değer sunmaz [93].



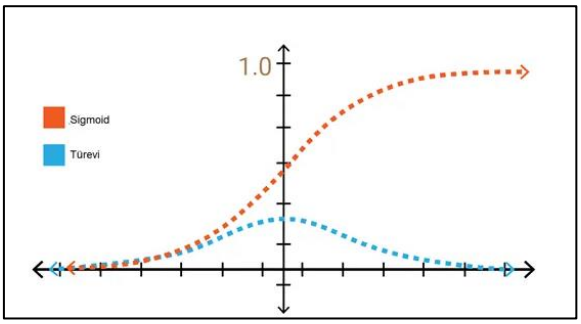
Şekil 2.16. Basamak aktivasyon fonksiyonu ve türevi [94].

Doğrusal (Linear) fonksiyonu, Şekil 2.17'de görüldüğü gibi girdi değerini doğrudan çıktı olarak vermektedir. Lineer yapısından dolayı türevi sabittir ve bu durum modelin öğrenme kapasitesini sınırlar ve karmaşık örüntüleri öğrenmesini engeller. Bu nedenle genel olarak basit regresyon modellerinde tercih edilir [95].



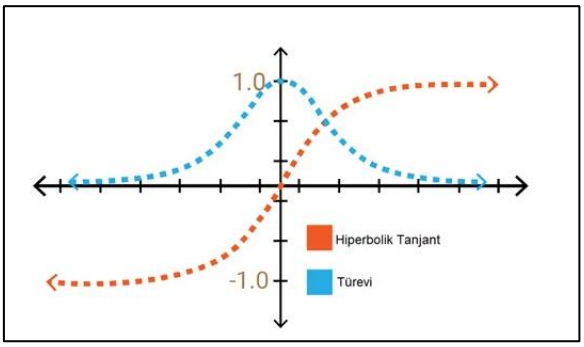
Şekil 2.17. Doğrusal aktivasyon fonksiyonu ve türevi [94].

Sigmoid fonksiyonu, sinir ağlarındaki uygulamalarda girdileri 0 ile 1 aralığına dönüştüren bir yöntemdir. Sigmoid, girdileri bu sınırlı aralığa çekerek özellikle ikili sınıflandırma görevlerinde çıktıların olasılık olarak değerlendirilmesine imkan sağlamaktadır. Doğrusal olmayan yapısı nedeniyle, ağın karmaşık ilişkileri öğrenmesine imkan tanır. Türevlenebilir olmasından dolayı geriye yayılım sürecinde kullanılabilir, fakat Şekil 2.18'de görülebileceği gibi yüksek veya düşük girdi değerlerinde türevinin azalması ölü gradyan (vanishing gradient) problemine yol açabilmektedir. Çünkü bu bölgelerde öğrenme işlemi minimum seviyede gerçekleşmektedir [94].



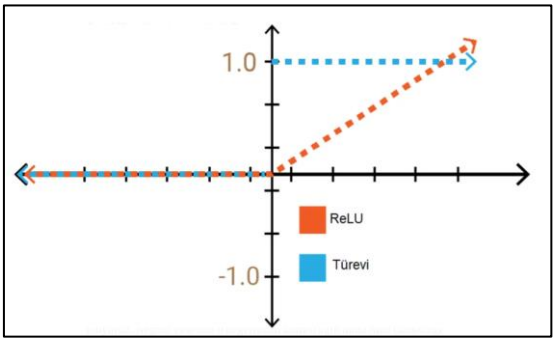
Şekil 2.18. Sigmoid aktivasyon fonksiyonu ve türevi [94].

Hiperbolik tanjant fonksiyonu, sigmoid fonksiyonunun yapısal bir benzeridir, ama bu sefer çıktı değerleri (-1 ile +1 arasında) olarak ayarlanmıştır. Sigmoid fonksiyonuna göre bir artısı, türevinin daha geniş bir değer aralığına sahip olmasıdır, bu da öğrenme ve sınıflandırma işlemlerini daha hızlı ve verimli hale getirebilir. Bununla birlikte, bu fonksiyonunun da uç değerlerinde gradyan kaybı sorunu bulunmaktadır [93,94]. Hiperbolik tanjant fonksiyonun ilişkin gösterim Şekil 2.19'da yer almaktadır.



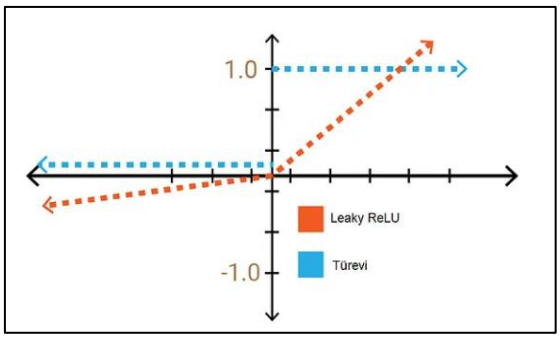
Şekil 2.19. Hiperbolik tanjant aktivasyon fonksiyonu ve türevi [94].

Düzeltilmiş Doğrusal Birim (Rectified Linear Unit, ReLU) aktivasyon fonksiyonu, Şekil 2.20'de gösterildiği gibi, bir nöronun çıktısı sıfırın üzerinde olduğunda bu çıktıyı olduğu gibi bırakırken, eğer çıktı sıfırın altındaysa sonucu otomatik olarak sıfırlamaktadır [96]. Bu özellik, ReLU'nun sigmoid ve hiperbolik tanjant fonksiyonlarına göre hem daha hızlı çalışmasını hem de hesaplama açısından daha verimli olmasını sağlar. Bu nedenle, ReLU en yayın kullanılan aktivasyon fonksiyonlarından biridir. Pozitif değerler için doğrusal bir fonksiyon olması, ağın karmaşık öğrenme problemlerinde etkili olmasını sağlarken sıfırdan küçük değerler için öğrenmenin olamaması ReLU'nun dezavantajı olarak karşımıza çıkmaktadır.



Şekil 2.20. ReLU aktivasyon fonksiyonu ve türevi [94].

Sızıntı (Leaky) ReLU fonksiyonu, ReLU'nun temel prensibini korurken, sıfırdan küçük olan nöron çıktılarını tamamen sıfıra eşitlemek yerine, Şekil 2.21'de görüldüğü gibi çok küçük bir eğim (sızıntı) ile çarparak negatif değerleri korumaktadır [97]. Bu küçük değişiklik, ReLU'nun negatif alanda yaşadığı "ölü nöron" sorununun önüne geçmek için geliştirilmiştir. Böylece, negatif girdiler artık belirli bir değere sahip olur ve böylece nöronların tamamen inaktif hale gelmesinin önüne geçilmiş olur. Bu durum ReLU'ya göre hesaplama karmaşıklığını biraz arttırmaktadır.



Şekil 2.21. Sızıntı ReLU aktivasyon fonksiyonu ve türevi [94].

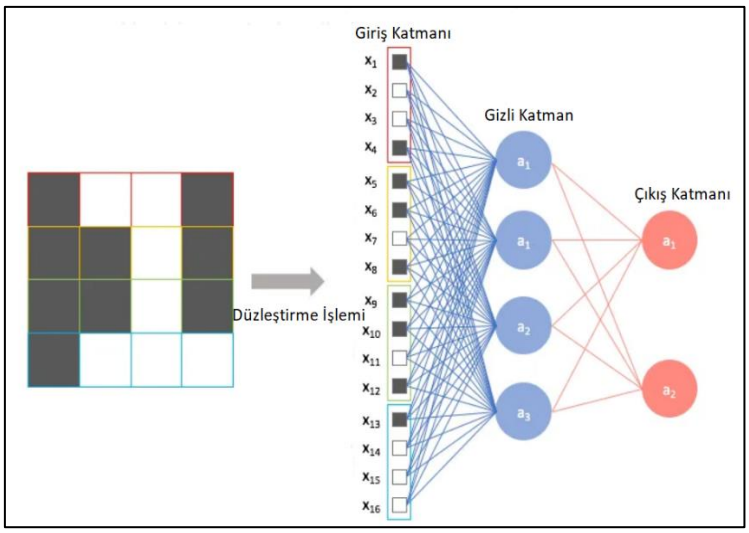
Sonuç olarak, tüm anlatılanlar göz önünde bulundurulduğunda, işlem hızının da önemli bir parametre olduğu çok katmanlı ve derin ağ yapılarında ReLU aktivasyon fonksiyonunun daha elverişli olduğu sonucuna varılabilmektedir [86].

d) Düzleştirme Katmanı:

Bu katmanda, CNN'nin evrişim ve havuzlama katmanları tarafından işlenen çok boyutlu özellik haritaları tam bağlaşımlı katmana girdi oluşturmak üzere, tek boyutlu bir vektöre dönüştürülmektedir [98]. Düzleştirme işlemi sayesinde, bu çok boyutlu veriler, modelin nihai çıktıları üretmesi için ihtiyaç duyduğu tam bağlaşımlı katmanlarda verimli bir şekilde kullanılabilir hale gelir.

e) Tam Bağlaşımlı Katman:

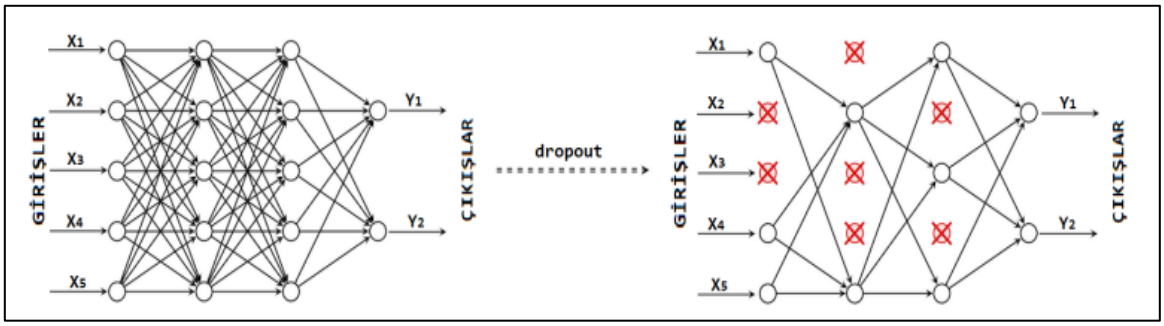
Görüntüler üzerindeki özellik çıkarma süreçleri tamamlandığında, oluşturulan özellik haritaları düzleştirilir ve ardından bu katmana aktarılır. Bu süreç Şekil 2.22'de gösterilmektedir. Bu katman, evrişimli sinir ağının içerisinde yer alan, bir yapay sinir ağı bileşenidir [99]. Tam bağlaşımlı katmanda her nöron, önceki katmandaki tüm nöronlara bağlıdır. Bu katman, son katmanı olarak işlev görür ve problem senaryosuna bağlı olarak giriş verisini, sınıf sayısına eşit boyutta bir vektöre veya belirlenen hedef boyutlarına uygun bir vektör formatına dönüştürebilir.



Şekil 2.22. Düzleştirme katmanı ve tam bağlaşımlı katman [100].

Derin sinir ağlarında genellikle tam bağlaşımlı katmanlar arasına modelin eğitim sırasında belirli nöronlara veya nöron gruplarına bağımlılığını azaltmak amacıyla seyreltme

katmanı (bırakma katmanı, dropout layer) yerleştirilir [86]. Seyreltme işlemi, her eğitim adımında rastgele seçilen nöronları devre dışı bırakarak çalışır. Böylece bu nöronların çıktısı sıfıra eşitlenirler ve bu nöronlar o adımda ağın geri kalanına hiçbir katkıda bulunmaz. Bu sayede model, veri setindeki farklı özellikleri öğrenmek için farklı nöron kombinasyonlarını kullanmak zorunda kalır ve genelleştirme yeteneği artar. Şekil 2.23'de seyreltme işlemine ilişkin görsel yer almaktadır.



Şekil 2.23. Seyreltme işlemi [101].

2.4.2. Hiper parametreler

Modelin eğitimi esnasında ayarlanması gereken ve öğrenme sürecini doğrudan etkileyen dışsal değişkenlerdir. Bu parametreler model tarafından öğrenilmez, ancak modelin verimliliği ve başarısı üzerinde belirleyici bir rol oynamaktadır.

a) Veri seti boyutu

Derin öğrenme modellerinin etkinliği, temel olarak veri setinin büyüklüğü ve içeriğinin çeşitliliği ile artmaktadır. Geniş ve çeşitli bir veri seti, modelin gerçek dünya senaryolarını anlamasına ve genelleştirmesine olanak tanımaktadır. Ancak, büyük veri setlerinin işlenmesi ve saklanması da göz önünde bulundurulması gereken faktörlerdir. Bu nedenle veri setinin boyutunun dengeli bir şekilde seçilmesini önemlidir. Veri setinin büyüklüğünün yetersiz olması, modelin yeterli öğrenme sürecini tamamlamamasına neden olmaktadır. Bu durumda yapay veri oluşturulması gibi yöntemlere başvurulması gerekebilir [93].

b) Öğrenme oranı (Learning rate)

Bu parametre, modelin ağırlıklarının her bir eğitim iterasyonunda ne kadar büyük adımlarla güncelleneceğini belirler. Öğrenme oranının olması gerekenden yüksek olması,

modelin optimizasyon sürecinde ideal çözüm noktalarını gözden kaçırmasına ve böylece eğitim aşamasında istikrarsız bir performans sergilemesine neden olabilir. Bu durum, modelin hedef fonksiyonun minimum değerlerini aşmasına ve optimum sonuçlara ulaşamamasına yol açar. Öte yandan, öğrenme oranı düşük seviyede tutulursa, bu durum modelin öğrenme sürecinin gereğinden fazla uzamasına ve potansiyel olarak yerel minimumlarda sıkışıp kalmasına sebep olabilir. Yerel minimumda sıkışma, modelin global minimuma ulaşmasını engelleyerek, genel performansının ve tahmin başarısının düşmesine yol açar. Bu noktada, momentum kavramı, önceki adımlardan elde edilen gradyanların birikimi ile modelin yerel minimumlardan çıkışını kolaylaştırır ve geniş bir bakış açısıyla global minimuma yönelmesini sağlayabilmektedir. Bu nedenle, sadece öğrenme oranı değil, aynı zamanda momentumun da dikkatli bir şekilde ayarlanması, modelin etkin bir şekilde öğrenmesini sağlamak açısından büyük önem taşımaktadır [102].

c) Küme boyutu (Batch size)

Küme boyutu, modelin her bir eğitim iterasyonunda işleyeceği veri örneklerinin sayısını ifade etmektedir. Geniş veri setlerinin olduğu durumlarda, veri setinin tamamını aynı anda işlenmek yerine, veri seti daha yönetilebilir küçük segmentlere bölünür [69]. Bu parametre, modelin her iterasyonda kaç adet veri üzerinden öğrenme işlemini sürdüreceğini belirler ve bu da modelin öğrenme süreci hızını ve hafıza kullanımını etkiler. Küçük bir küme boyutu, modelin daha sık ağırlık güncellemesi yapmasına neden olarak daha hızlı ama daha az kararlı bir öğrenme sürecine yol açabilir. Diğer yandan, büyük bir küme boyutu, her bir iterasyonda daha geniş veri seti üzerinden öğrenmeyi sağlamaktadır. Bu durum, genellikle daha kararlı bir gradyan tahmini demektir, ancak aynı zamanda her iterasyonun hesaplama süresinin ve ihtiyaç duyulan hafıza miktarının da artması anlamına gelmektedir. Bu nedenle, küme boyutunun ayarlaması aşamasında, modelin öğrenme hızı, kararlılığı ve kullanılabilir hafıza kaynakları arasında dengeli bir uyum yakalamak hedeflenmelidir. Küme boyutunun belirlenmesinde yaygın bir yaklaşım, bu değeri 2'nin üsleri olarak ayarlamaktır. Bu tercih, GPU'nun çok sayıda çekirdeğinin daha verimli şekilde kullanılarak işlem yeteneklerinden en etkin şekilde yararlanılmasını amaçlar [103].

d) Döngü (Epoch) Sayısı

Algoritmanın veri seti üzerinde kaç kez tam tur atacağını gösteren önemli bir hiper parametredir. Döngü sayısının belirlenmesi uygulamanın özelliklerine göre değişiklik

gösterir. Eğer bu sayı çok düşük tutulursa, modelin veri setinden yeterince öğrenememesi ve dolayısıyla yetersiz performans sergilemesi problemi oluşur. Diğer yandan, gereğinden yüksek bir döngü sayısı belirlendiğinde, modelin doğruluk oranının belirli bir noktadan sonra sabit kalması ya da çok küçük değişiklikler göstermesi sonucu ile karşılaşılır [69]. Bu nedenle modelin doğru miktarda döngü ile eğitilmesi, veri setinin içerdiği örüntüleri ve karakteristikleri başarılı bir şekilde kavraması açısından önemlidir.

e) Optimizasyon algoritması

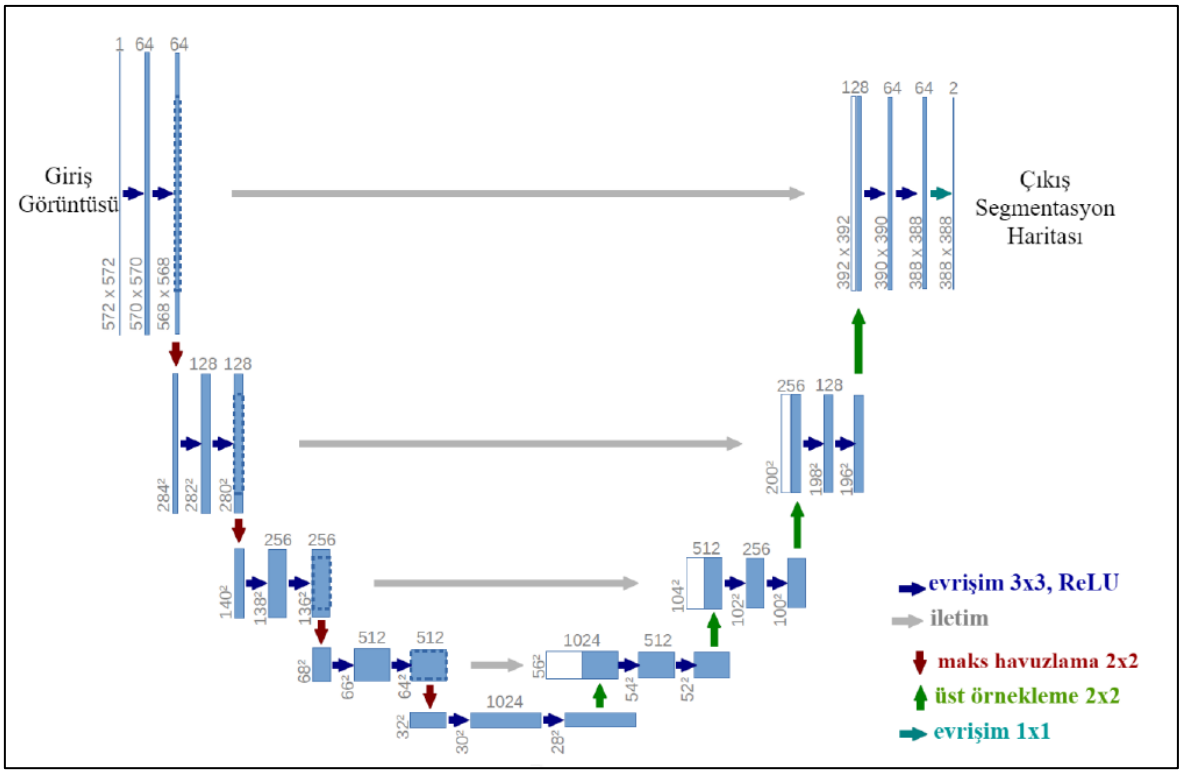
Derin öğrenme modellerinde başarılı bir öğrenme sürecinin gerçekleştirilebilmesi için, kayıp fonksiyonunun en düşük değerine ulaşılması esastır. Bu en düşük nokta, yani mutlak minimum, modelin tahminleri ile gerçek veriler arasındaki hatayı en aza indirgeyerek optimum sonuçların elde edilmesini sağlamaktadır. Bu hedefe ulaşmak için kullanılan yöntemler, optimizasyon algoritmaları olarak bilinir. Bu algoritmalar, modelin ürettiği çıktıların gerçek değerlere olan uyumunu arttırarak, hata oranını minimuma indirmeyi amaçlar [104]. Literatürde yer alan farklı optimizasyon algoritmaları, çeşitli problemlere ve veri setlerine göre farklı avantajlar sunar. Örneğin, Stokastik Gradyan İnişi (Stochastic Gradient Descent, SGD) yöntemi daha basit problemlerde etkili olabilirken, Uyarlanabilir Momentum Tahmini (Adaptive Moment Estimation, Adam) veya Kök Ortalama Kare Yayılımı (Root Mean Square Propagation, RMSProp) gibi daha gelişmiş optimizasyon algoritmaları, adaptif öğrenme hızları sunarak karmaşık veri yapılarında daha hızlı ve etkili sonuçlar elde etmeye yardımcı olmaktadır. Bu algoritmaların seçimi, veri setinin niteliklerine, modelin karmaşıklığına ve elde edilmesi istenen sonuçlara göre yapılmalıdır. Doğru optimizasyon algoritmasının seçimi, eğitim sürecinin verimliliğini artırır ve modelin daha hızlı ve etkin bir şekilde genelleyebilmesini sağlar.

Bu bahsedilen yöntemlerin haricinde, katman sayılarının ve gizli katmanlardaki nöron sayılarının belirlenmesi, uygun filtre boyutlarının seçilmesi, ağırlık başlangıç değerlerinin atanması, aktivasyon fonksiyonlarının seçilmesi, seyreltme işlemi uygulanacak katmanların ve seyreltme miktarının belirlenmesi gibi ağ performansını etkileyen çok sayıda parametre mevcuttur [102].

2.5. U-Net Mimarisi

U-Net mimarisi, ilk kez 2015 yılında Olaf Ronneberger, Philipp Fischer ve Thomas Brox tarafından Uluslararası Biyomedikal Görüntüleme Sempozyumu'nda (International

Symposium on Biomedical Imaging, ISBI) tanıtılmıştır. Bu mimari, sempozyumda düzenlenen Hücre İzleme Yarışması'nda (Cell Tracking Challenge) birinci olmuştur [69]. Bu başarı, U-Net yapısının tıbbi görüntü segmentasyonunda ne kadar etkili olduğunu göstermiş ve bu alandaki araştırmalara önemli bir katkı sağlamıştır. Ronneberger ve ekibi tarafından bu alandaki ilk çalışma, "U-Net: Convolutional Networks for Biomedical Image Segmentation" başlığı altında yayınlanmıştır [105]. Görüldüğü gibi ortaya çıkış amacı itibari ile U-Net, esas olarak görüntü segmentasyonu amacıyla geliştirilen bir derin sinir ağı mimarisidir.



Şekil 2.24. U-Net mimarisi [105].

Şekil 2.24'de görüldüğü gibi U-Net yapısı, iki ana bölümden meydana gelmektedir: biri kodlayıcı (encoder) veya daralan kısım (contracting path), diğeri ise kod çözücü (decoder) veya genişleyen kısım (expanding path).

Daralan kısımda evrişimli bir ağın geleneksel yapısı mevcuttur [106]. Süreç, ağın girişine verilen giriş görüntüsüne iki defa üst üste 3x3 evrişim işleminin ve ardından ReLU aktivasyon fonksiyonunun uygulanmasını ile başlamaktadır. Bu işlemlerle elde edilen özellik haritalarına daha sonra 2 adımlı bir 2x2 maksimum havuzlama işlemi uygulanarak maksimum özellikler tutulacak şekilde boyutu yarıya düşürülmektedir. Bu evrişim ve

havuzlama adımları giriş görüntüsüne peş peşe 4 defa uygulanmaktadır [105]. Böylelikle alt örnekleme (downsampling) işlemi gerçekleştirilmiş olur. Bu esnada Şekil 2.24'de görüldüğü gibi her katmanda giriş görüntüsünün uzamsal boyutları yarıya düşürülürken, özellik kanallarının sayısı (derinlik) iki katına çıkarılmaktadır. Özellik kanallarının sayısını arttırmak, ağın girdi verilerinden daha kapsamlı ve detaylı özellikler öğrenmesine imkan sağlamaktadır.

U-Net mimarisinin genişleyen yolu ise, daralan yolda kaybedilen uzamsal detayları geri kazanmak için tasarlanmıştır. İlk olarak, üst örnekleme işlemiyle özellik haritalarının boyutu artırılır. Daha sonra, bu genişletilmiş özellik haritaları, daralan yol tarafındaki simetrik katmandan gelen özellik haritaları ile birleştirilir. Ardından, iki adet peş peşe 3x3 evrişim işlemi uygulanarak, birleştirilmiş haritalar daha ayrıntılı olarak işlenir. Her konvolüsyon katmanından sonra ReLU aktivasyon fonksiyonu kullanılmaktadır. Genişleyen yol kısmında daralan yol kısmın tam aksine her katmanda giriş görüntüsünün uzamsal boyutları iki katına çıkarılırken ve özellik kanallarının sayısı (derinlik) yarıya düşürülmektedir.

Ağın son katmanında ise 1x1 evrişim işlemi ile 64 bileşenden oluşan özellik vektörleri modelin hedeflediği çıktı sınıflarına uygun formata dönüştürülmektedir [107]. Adından da anlaşılacağı gibi 1x1 evrişim, her özellik haritasında tek piksel genişliğinde bir alana uygulanan bir işlemdir. Karmaşık özellik bilgisini korurken ağın derinlik boyutunu azaltır, böylece modelin hesaplama verimliliğini ve son katmanda daha az parametreyle etkili bir şekilde çıktı üretme yeteneğini artırmaktadır.

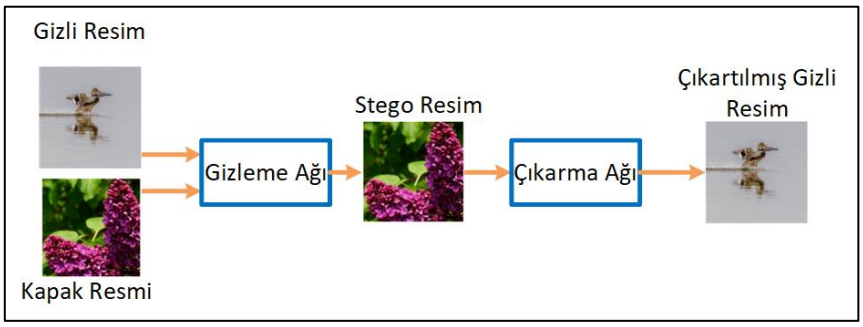
U-Net modelinin en önemli özelliği, her seviye arasındaki atlamalı bağlantılardır (skip connections, bypass connections). Bu bağlantılar, Şekil 2.24'de görüldüğü gibi daralma yolunun her seviyesinde üretilen özellik haritalarını, genişleyen yolun karşılık gelen seviyesine doğrudan aktararak, daralma yolundan gelen genel bağlam bilgisini genişleyen yoldan gelen ayrıntılı yerel bilgilere entegre etmektedir. Böylelikle U-Net, daha doğru ve kapsamlı görsel analiz gerçekleştirmek için girdi görüntüsünden elde edilen üst düzey özellikleri (örneğin, genel şekiller veya yapılar) ayrıntılı yerel özelliklerle (belirli kenarlar veya doku bilgileri gibi) birleştirebilmektedir. Özetle, bypass bağlantıları U-net mimarisinin kritik bir bileşenidir ve giriş görüntüsünün hem genel bağlamını hem de ince ayrıntılarını koruyarak yüksek kaliteli sonuçlar üretmesini sağlamaktadır.

3. TEZ KAPSAMINDA YAPILAN ÇALIŞMALAR

Bu bölümde doktora tezi kapsamında gerçekleştirilen tüm çalışmalara ayrıntılı olarak yer verilmiştir.

3.1. U-Net Mimarisinin Steganografi Amacıyla Kullanılması

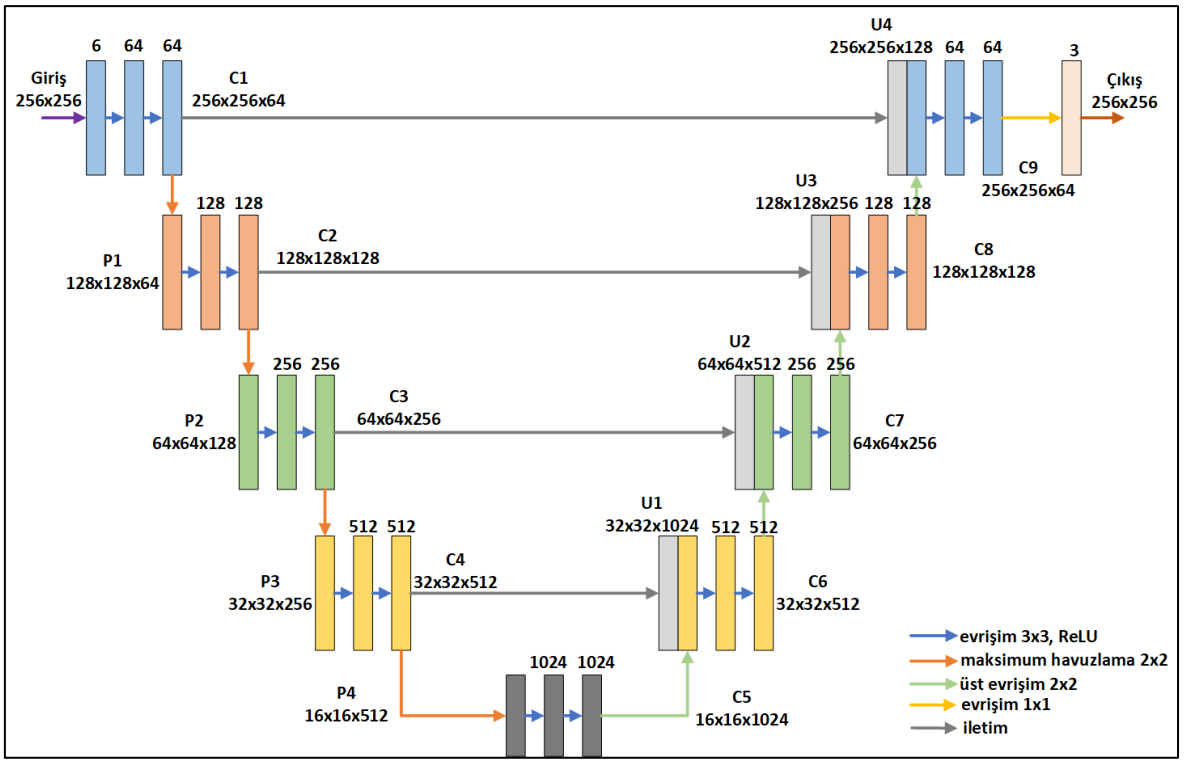
Daha önce de belirtildiği gibi, U-Net mimarisi literatürde esas olarak görüntü segmentasyonu amacıyla kullanılıyor olmasına rağmen, tez çalışması kapsamında U-Net mimarisi steganografi uygulaması için kullanılmıştır.



Şekil 3.1. Veri gizleme ve çıkarma işlemi blok diyagramı.

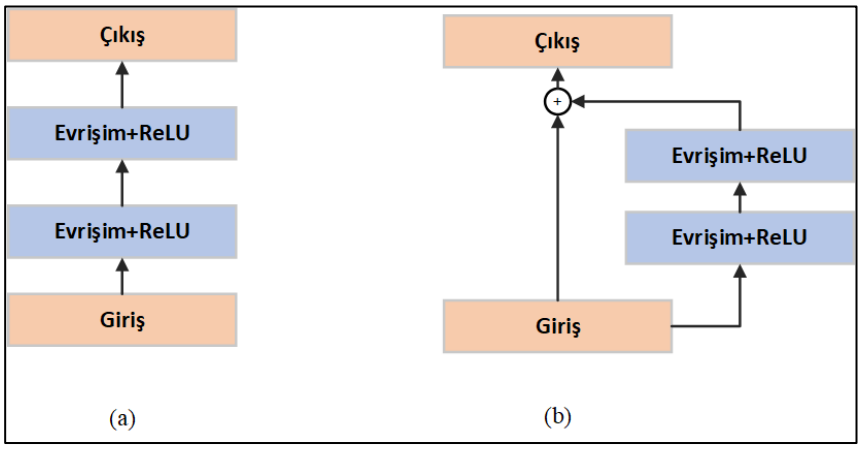
Şekil 3.1'de yer aldığı gibi kapak resmi ve kapak resmi içine gizlenmesi istenen mesaj (gizli) resmi gizleme ağına verilir. Gizleme ağının çıktısı stego resim olarak adlandırılmaktadır. Daha sonra stego resim çıkarma ağına girdi olarak verilir ve çıktı olarak stego resimden tekrar çıkartılmış gizli resim elde edilir.

U-Net mimarisi, geleneksel yöntemlere kıyasla steganografide önemli avantajlar sunmaktadır. Özellikle atlamalı bağlantıları sayesinde, ağdaki alt seviyelerden üst seviyelere özelliklerin doğrudan aktarılmasını sağlar, bu da gizli verilerin daha hassas ve etkili bir şekilde gizlenmesini ve çıkarılmasını kolaylaştırır. U-Net'in derin öğrenme tabanlı yapısı, karmaşık görsel detayları öğrenmede başarılı olduğundan, steganografik süreçlerde daha yüksek doğruluk ve verimlilik sağlar. Bu özellikler nedeniyle, bu çalışmada U-Net mimarisi tercih edilmiş ve gizli görüntünün hem gizlenmesi hem de çıkarılması aşamalarında kullanılmıştır. Şekil 3.2'de çalışmada önerilen U-Net mimarisi yer almaktadır.



Şekil 3.2. Önerilen U-Net mimarisi.

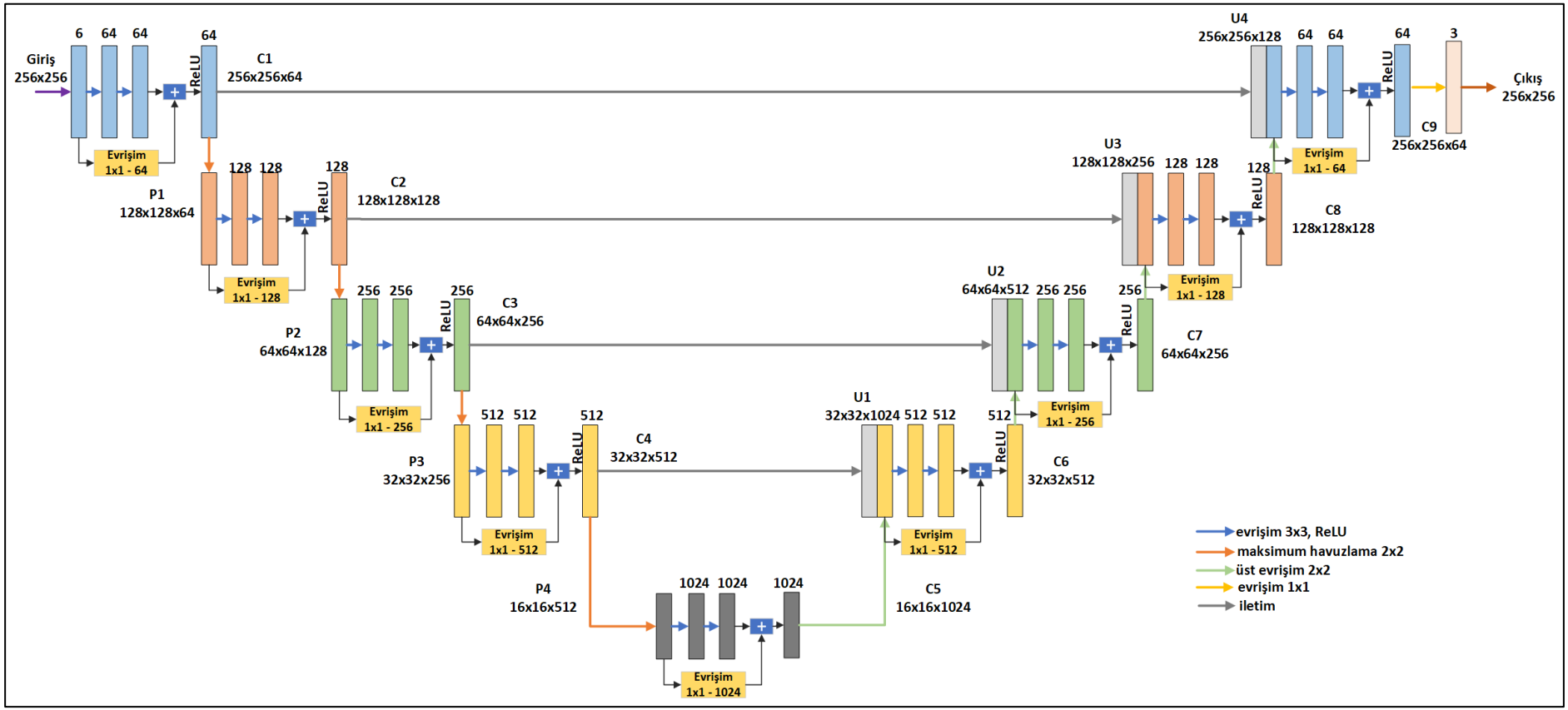
U-Net mimarisini steganografiye uyarlarken artık bloklar (residual blocks) mimariye entegre edilmiştir. Şekil 3.3'de klasik U-Net mimarisinde yer alan evrişim katmanları ve önerilen mimaride kullanılan artık bloklara ilişkin gösterim yer almaktadır.



Şekil 3.3. İleri evrişimli blok (a) ve artık blok (b) gösterimi.

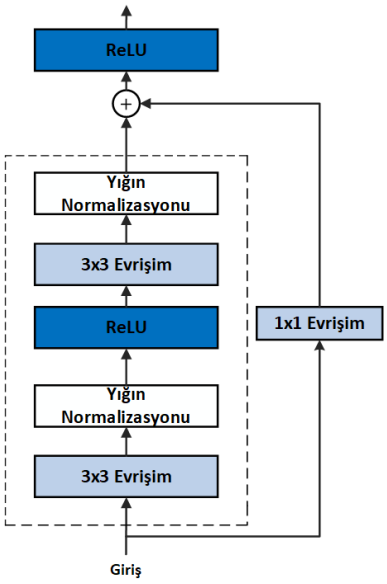
Şekil 3.3 (a) bölümünde, bir ileri evrişimli blok (forward convolutional block) yapısı yer almaktadır. Bu yapı, giriş verisini ardışık bir şekilde evrişim ve ReLU aktivasyon katmanlarından geçirerek çıkışa ulaştırır. Her katman, bir önceki katmanın çıktısını alarak ilerler. Bu aşamalar sonucunda, veri giderek daha soyut bir temsile dönüşür ve sonunda bir

çıktı üretilir. Bu yapıda katmanların her biri sadece önceki katmanın çıktılarına bağlıdır. (b) bölümünde ise, bir artık blok yapısı yer almaktadır. Burada, giriş verisi hem ardışık evrişim ve ReLU katmanlarına girer hem de bir kısa yol bağlantısı aracılığıyla bu katmanların çıktısına doğrudan eklenir. Bu kısa yol bağlantısı, giriş verisinin bir kısmını veya tamamını, katmanların işlemesinden sonra oluşan sonuca toplama işlemiyle ekler. Bu toplama, birleştirme noktasında gerçekleştirilir ve ağın derin katmanlarına ulaşan gradyanların güçlendirilmesine yardımcı olur. Bu yapı, geri yayılım sırasında gradyanların katmanlar arasında azalmasını önleyerek, kaybolan gradyan problemine karşı etkili bir çözüm sunar ve böylece ağın her katmanının eğitim sürecine eşit derecede katkıda bulunmasını sağlar. Sonuçta, giriş verisinin önemli öznitelikleri korunur ve ağın daha derin katmanlarının eğitimine katkıda bulunur. Artık blokların bu entegrasyonu, derin öğrenme modellerinin daha hızlı ve daha kararlı bir şekilde eğitilmesine olanak tanırken, aynı zamanda modelin daha karmaşık özellikleri öğrenmesine imkan sağlamaktadır. Şekil 3.4’ de U-Net mimarisine artık blokların entegre edilmesi işlemi görselleştirilmiştir.



Şekil 3.4. Önerilen U-Net mimarisi (Artık blokların detaylı gösterimi).

Model, ilk artık blok ile başlamaktadır. Şekil 3.5'de görüldüğü gibi artık blok yapısı 2 adet 3x3 evrişim katmanı, aktivasyon fonksiyonu ve yığın normalizasyonu içermektedir. İlk artık blokta yer alan evrişim katmanlarında 64'er adet filtre yer almaktadır. Bu blok kapak resim ve gizli resimden oluşan 6 kanallı giriş tensörü üzerinde çalışır. Şekil 3.5'de de görselleştirildiği gibi giriş tensörü alınır, ilk evrişim katmanı ve ilk yığın normalleştirme katmanı üzerinden geçirilir ve sonrasında ReLU aktivasyon fonksiyonu uygulanır. Elde edilen sonuç, ikinci evrişim katmanı ve ikinci yığın normalleştirme katmanı üzerinden geçirilir ve 256x256x64 boyutunda bir özellik haritası elde edilir. Bu işlemden sonra, 256x256x6 boyutundaki giriş tensörü, 256x256x64 boyutunda bir özellik haritası ile toplanabilmesi için 64 kanallı 1x1 evrişim katmanından geçirilir ve bu sonuç, ikinci evrişim ve yığın normalizasyonu işleminden çıkan sonuçla toplanır. Toplama işleminden sonra, sonuç ReLU aktivasyon fonksiyonundan geçirilir. Daha sonra, toplama kısmından elde edilen özellik haritalarının boyutunu azaltmak ve en önemli özellikleri korumak amacıyla, 2x2 boyutunda ve adım büyüklüğü 2 olan bir pencere kullanarak maksimum havuzlama işlemi gerçekleştirilir. Böylece ilk artık bloktan çıkan 256x256x64 boyutlu özellik haritasının yükseklik ve genişlik boyutları 128x128x64 boyutuna indirgenir ve bu çıktı bir sonraki artık blok katmanına girdi olarak verilir.



Şekil 3.5. U-Net mimarisinde kullanılan artık blok yapısı.

Sonraki seviye, 128 filtre içeren evrişim katmanlarından oluşan yeni bir artık blok katmanından oluşmaktadır. Önceki bloğa benzer şekilde, bu blok, her biri 128 filtreli iki evrişimli katmandan ve ardından ReLU aktivasyon fonksiyonu ve BN'den oluşmaktadır. Bu

blok işlendikten sonra özellik haritası 128 kanala genişler. Artık blok kısmında, bu defa giriş tensörü boyutu 128x128x64 olduğundan, evrişim işlemi sonucunda elde edilen 128x128x128 tensörü ile toplanabilmesi için 128 kanallı 1x1 evrişim katmanından geçirilerek kanal sayısı artırılmıştır. Toplama işleminden sonra sonuç ReLU aktivasyon fonksiyonundan geçirilmiştir. Ardından tekrar, özellik haritaları boyutlarını yarıya indirmek için 2x2 pencereli ve 2 adımlı bir maksimum havuzlama katmanı kullanılmıştır. Böylece artık bloktan çıkan 128x128x128 boyutlu özellik haritasının yükseklik ve genişlik boyutları 64x64x128 boyutuna indirgenir ve bu çıktı bir sonraki artık blok katmanına girdi olarak verilir.

Bu işlemler, ağın daralan yol kısmı boyunca devam eder. Her seviye, ilgili artık bloğundaki filtre sayısını sırasıyla 256, 512 ve en son 1024 olmak üzere iki katına çıkarır. En son aşamada 1024 filtrelik artık blok çıkışında 16x16x1024 boyutlu bir tensör elde edilir.

U-Net mimarisinin genişleyen yolu tarafında havuzlama katmanı yerine üst evrişim (upconvolution) kullanılarak 16x16x1024 özellik haritasının genişlik ve yükseklik boyutu iki katına çıkarılır. Daha sonra, 32x32x1024 boyutlu genişletilmiş özellik haritası, daralan yol tarafındaki simetrik katmandan gelen 32x32x512 boyutlu özellik haritası ile birleştirilir. Ardından bu birleştirilmiş özellik haritaları artık blok katmanına girdi olarak verilir. İlk evrişim katmanı ve ilk yığın normalleştirme katmanı üzerinden geçirilir ve sonrasında ReLU aktivasyon fonksiyonu uygulanır. Elde edilen sonuç, ikinci evrişim katmanı ve ikinci yığın normalleştirme katmanı üzerinden geçirilir ve 32x32x512 boyutunda bir özellik haritası elde edilir. 32x32x1024 boyutlu tensör, 32x32x512 boyutunda bir özellik haritası ile toplanabilmesi için 512 kanallı 1x1 evrişim katmanından geçirilir ve bu sonuç, ikinci evrişim ve yığın normalizasyonu işleminden çıkan sonuçla toplanır. Toplama işleminden sonra, sonuç ReLU aktivasyon fonksiyonundan geçirilir. Daha sonra, toplama kısmından elde edilen özellik haritalarının genişlik ve yükseklik boyutu yukarı evrişim ile 2 katına çıkarılır ve böylece ilk artık bloktan çıkan 32x32x512 boyutlu özellik haritasının yükseklik ve genişlik boyutları 64x64x512 boyutuna gelir. Bu çıktı bir sonraki simetrik daralan yol katmanın gelen özellik haritası ile birleştirilerek bir sonraki artık blok katmanına girdi olarak verilir.

Sonraki aşama, 256 filtre içeren evrişim katmanlarından oluşan yeni bir artık blok katmanından oluşmaktadır. Önceki bloğa benzer şekilde, bu blok, her biri 256 filtreli iki evrişimli katmandan ve ardından ReLU aktivasyon fonksiyonu ve BN'den oluşmaktadır.

Yukarı evrişim ile boyutu 64x64x512 olarak genişletilmiş özellik haritası, daralan yol tarafındaki simetrik katmandan gelen 64x64x256 boyutlu özellik haritası ile birleştirilerek bu artık blok katmanına girdi oluşturur. Sırasıyla evrişim, BN, ReLU, ikinci evrişim, ikinci BN katmanlarından geçirildikten sonra 64x64x256 boyutlu özellik haritası elde edilir. 64x64x512 boyutlu tensör, 64x64x256 boyutunda bir özellik haritası ile toplanabilmesi için 256 kanallı 1x1 evrişim katmanından geçirilir ve bu sonuç, ikinci evrişim ve yığın normalizasyonu işleminden çıkan sonuçla toplanır. Toplama işleminden sonra, sonuç ReLU aktivasyon fonksiyonundan geçirilir. Daha sonra, toplama kısmından elde edilen özellik haritalarının genişlik ve yükseklik boyutu yukarı evrişim ile 2 katına çıkarılır ve böylece ilk artık bloktan çıkan 64x64x256 boyutlu özellik haritasının yükseklik ve genişlik boyutları 128x128x256 boyutuna gelir. Bu çıktı bir sonraki simetrik daralan yol katmanın gelen özellik haritası ile birleştirilerek bir sonraki artık blok katmanına girdi olarak verilir.

Bu işlemler, ağın genişleyen yol kısmı boyunca devam eder. Her seviye, ilgili artık bloğundaki filtre sayısını sırasıyla 128 ve 64 olarak yarıya düşürür. Yani genişleyen yol kısmında daralan yol kısmın tam aksine her katmanda giriş görüntüsünün genişlik ve yükseklik boyutları iki katına çıkarılırken ve özellik kanallarının sayısı (derinlik) yarıya düşürülmektedir. En son aşamada 64 filtrelik artık blok çıkışında 256x256x64 boyutlu bir tensör elde edilir.

Mimarinin son katmanı, 3 kanala sahip 1x1 evrişim katmanıdır. 3 kanal olarak belirlenmesinin nedeni 64 bileşenden oluşan özellik vektörlerini RGB resim formatında elde etmektir. 1x1 evrişim katmanı, entegrasyon sürecinin final aşamasını oluşturur. Bu katman, modelin derin katmanlarından elde edilen özellikleri son çıktıya aktararak, gizli resmin kapak resmine hassas bir şekilde entegre edilmesini sağlar ve kanal sayısını ayarlar.

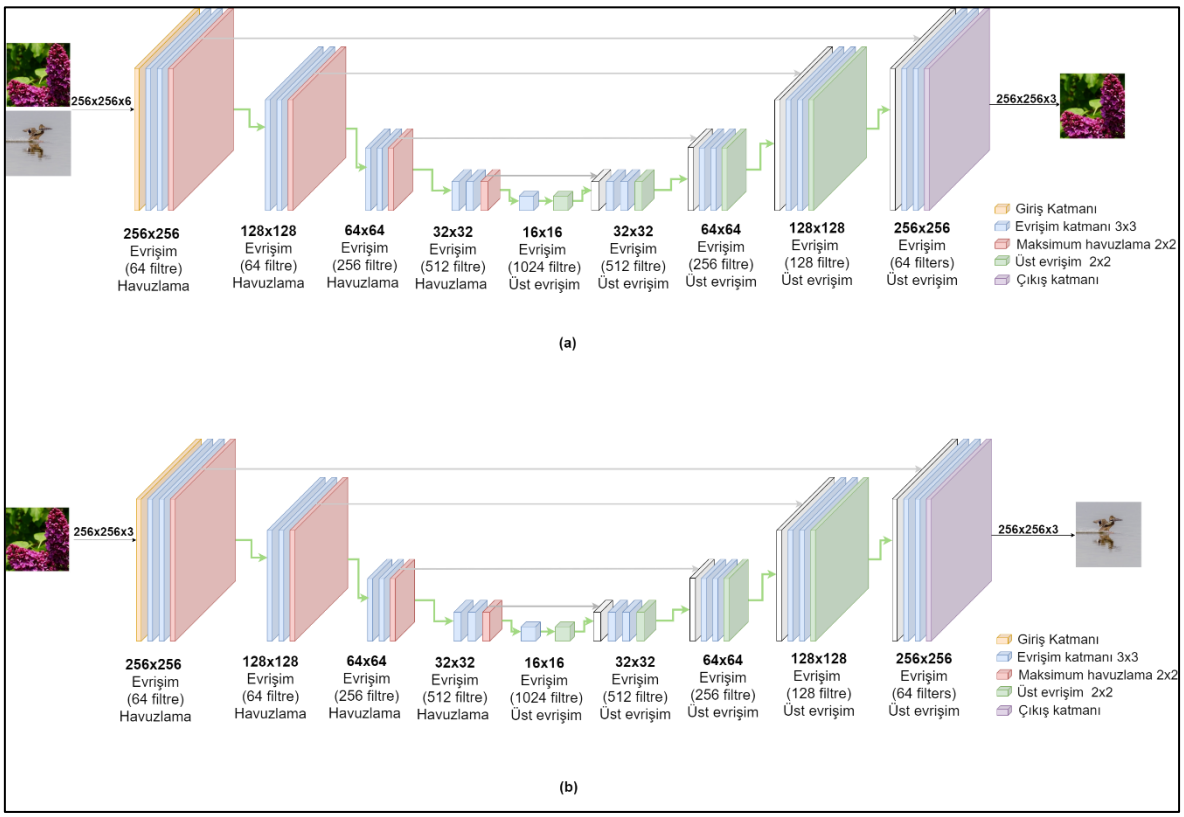
Kapak resminde gizli resmi çıkarmak için kullanılan ikinci U-Net ağı olan çıkarma ağı, gizleme ağı ile aynı katman konfigürasyonuna ve filtre boyutlarına sahiptir. Ancak iki ağ arasında operasyonel işlemler ve modellerin odaklandığı hedefler anlamında bazı farklar mevcuttur:

Gizleme işlemi için, model kapak resmi ve gizli resmi alır ve bunları birleştirerek yeni bir stego resim üretir. Bu süreçte, modelin eğitim veri seti, kapak resimleri ve mesaj resimlerinden oluşur. Çıkarma işlemi için, model stego resmi alır ve bu resimden mesaj resmini ayırarak geri kazanmayı amaçlar. Eğitim veri seti bu kez stego resimler ve karşılık gelen orijinal mesaj resimlerinden oluşur.

Gizleme işlemi için, modelin hedefi, gizli resmi kapak resmi ile efektif bir şekilde birleştirmektir. Kayıp fonksiyonu, stego resmin kapak resmine ne kadar benzer olduğunu değerlendirir. Çıkarma işlemi için, modelin hedefi, birleştirilmiş resimden gizli resmi tekrar çıkarmaktır. Kayıp fonksiyonu bu kez, modelin çıktısının orijinal gizli resimle ne kadar benzer olduğunu değerlendirir.

Gizleme işlemi sırasında model, gizli verinin görsel algılanabilirliğini minimuma indirirken, kapak resminin doğal yapısını korumaya odaklanır. Çıkarma işlemi sırasında modelin odak noktası, stego resimden gizli veriyi mümkün olan en yüksek doğrulukla ayırmak ve geri kazanmaktır.

Şekil 3.6'da gizleme ve çıkarma ağları görsel olarak yer almaktadır.



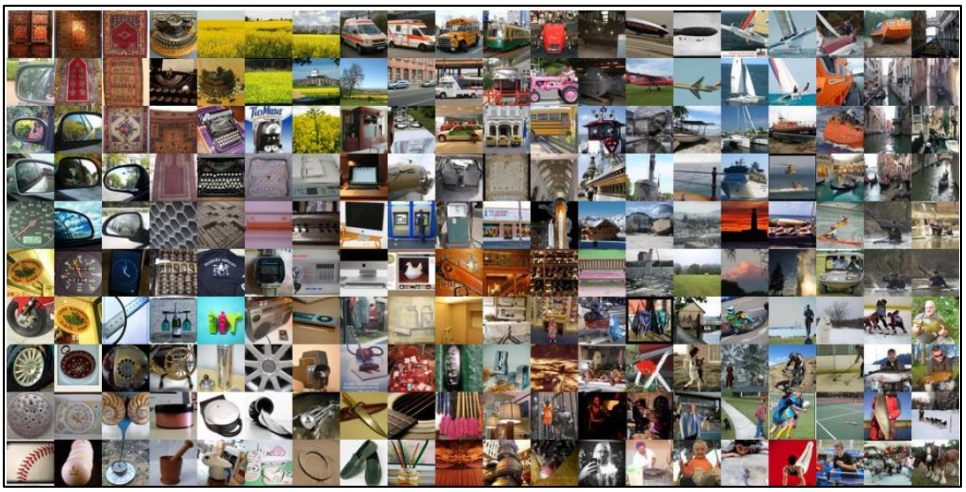
Şekil 3.6. Gizleme (a) ve çıkarma (b) ağları.

3.2. Kullanılan Veri Tabanları, Ön İşleme Adımları ve Hiper parametreler

Tez çalışmasında modelin eğitimi için Imagenet veri tabanına ait görseller kullanılmıştır. Test aşamasında ise Linnaeus 5, Imagenet ve Labeled Faces in the Wild (LFW) veri tabanları kullanılmıştır. Bu bölümde öncelikle her veri tabanın genel özellikleri açıklanmış ardından veri setlerinin kullanımlarına ilişkin detaylar verilmiştir.

a) ImageNet

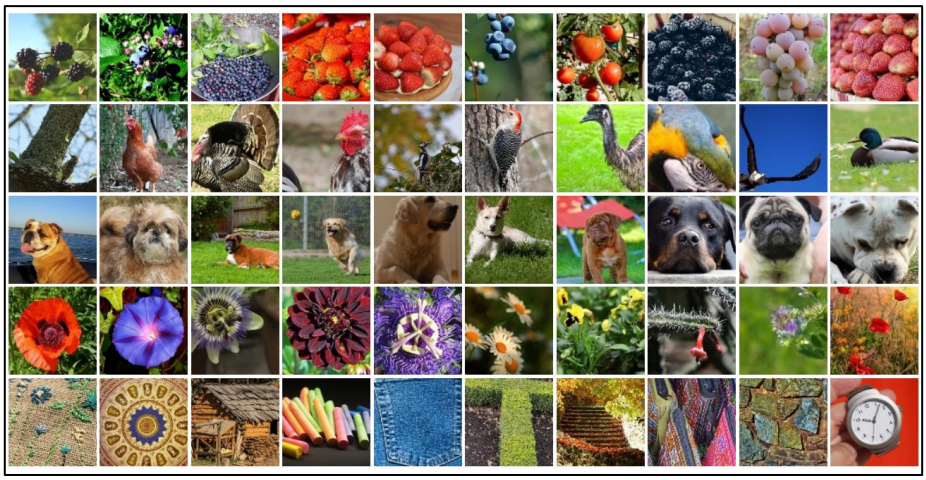
ImageNet, 22,000'den fazla kategoriye (nesneler, taşıtlar, hayvanlar, bitkiler, manzara unsurları vb.) ait yaklaşık 15 milyon etiketlenmiş resim içeren bir veri setidir [108]. Görseller internetten çeşitli kaynaklardan toplanmıştır ve farklı çözünürlük seviyelerine sahiptir. Bu durum da bilgisayarlı görü sistemlerinin farklı kalite ve boyuttaki görsel veriler üzerindeki performansını kapsamlı bir şekilde test etme imkanı sunmaktadır. Kategoriler, genellikle oldukça fazla sayıda resim içerir, bu da modelin her bir sınıf için yeterli öğrenme unsuruna sahip olmasına olanak sağlamaktadır. Şekil 3.7'de ImageNet veri setine ilişkin resim örnekleri yer almaktadır.



Şekil 3.7. ImageNet Veri Tabanı Resim Örnekleri [109].

b) Linnaeus 5 Veri Tabanı

Linnaeus 5 veri seti, makine öğrenimi ve görüntü işleme uygulamalarında kullanılan bir veri tabanı olup her biri meyve, kuş, köpek, çiçek ve 'diğer' kategorilerinden olmak üzere toplamda 8.000 adet renkli görsel içermektedir. Her bir sınıf için 1200 adet eğitim, 400 adet test resmi mevcuttur. Görseller 256x256, 128x128, 64x64 ve 32x32 piksel olmak üzere çeşitli çözünürlüklerde ve renkli olarak sunulmaktadır. Linnaeus 5 veri setine resim örnekleri Şekil 3.8'de yer almaktadır.



Şekil 3.8. Linnaeus 5 Veri Tabanı Resim Örnekleri [110].

c) LFW Veri Tabanı

LFW, yüz tanıma problemi üzerine çalışmalar yapmak için oluşturulmuş bir veri tabanıdır. Veri seti, web üzerinden toplanan 13.000'den fazla yüz görüntüsü içermektedir. 5.749 farklı kişiye ait görüntüleri barındırır ve bu kişilerden 1.680'i iki veya daha fazla resme sahiptir [111]. Bu veri tabanı farkı çözünürlüklerde resimler içermektedir ve her bir yüz, resimdeki kişinin adıyla etiketlenmiştir. Şekil 3.9'da LFW veri setine ilişkin resim örnekleri yer almaktadır.

Şekil 3.9. LFW Veri Tabanı Resim Örnekleri [112].

Tez çalışması kapsamında modelin eğitimi ImageNet veri tabanı ile gerçekleştirilmiştir. Bu veri tabanından 37.500 adet resim modeli eğitecek kapak resimleri olarak seçilmiş ve 7500 adet resim de doğrulamanın gerçekleştirileceği kapak resimleri olarak için kullanılmıştır. Yine aynı şekilde 37.500 adet resim modeli eğitecek gizli resimler

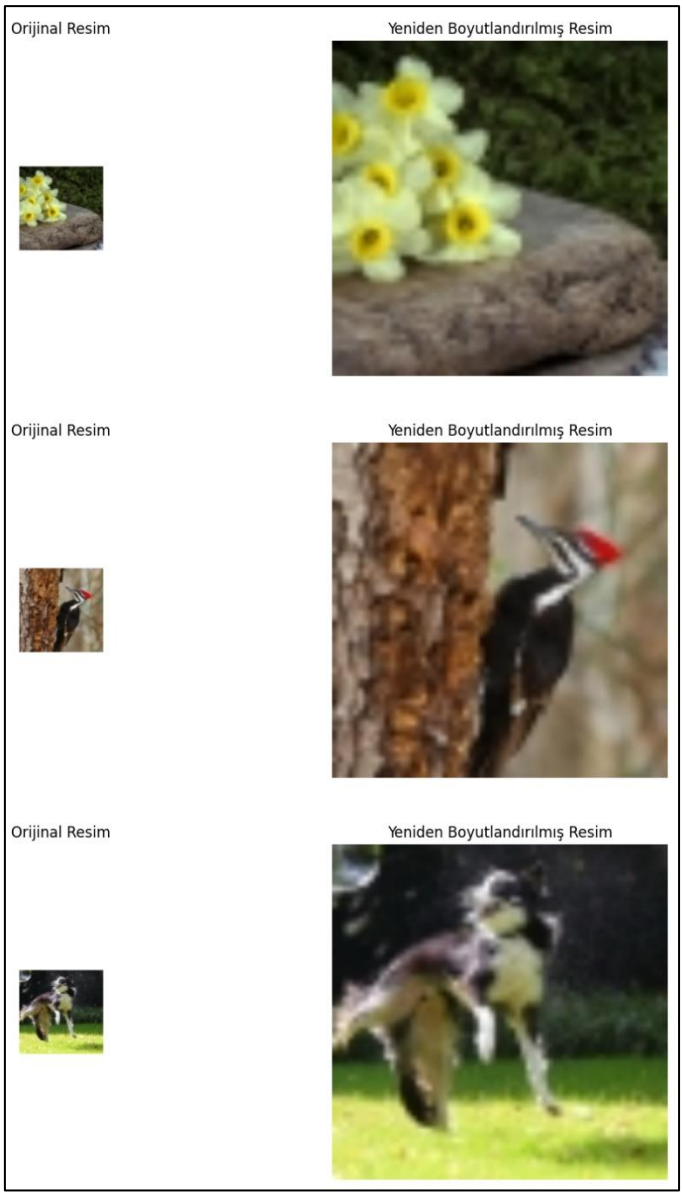
olarak seçilmiş ve 7500 adet resim de doğrulamanın gerçekleştirileceği gizli resimler olarak belirlenmiştir.

Modelin test edilmesi aşamasında ilk olarak Linnaeus 5 veri tabanı kullanılmıştır. Linnaeus 5 veri tabanının seçilmesinin en önemli sebebi 32x32, 64x64,128x128 ve 256x256 olmak üzere fark çözünürlüklere sahip ve ayrı ayrı kategorize edilmiş renkli resimler içermesi nedeniyle farklı orijinal boyutlardaki gizli resimlerin kapak resmi üzerindeki etkisini değerlendirme imkanını sunmasıdır. Linnaeus 5 veri tabanı ile modeli test ederken kapak resmi olarak 256x256 orijinal çözünürlüğe sahip 1600 adet resim kullanılmıştır. Bu kapak resimleri 32x32,64x64, 128x128 ve 256x256 orijinal çözünürlük değerlerine sahip 1600'er adet mesaj resmi ile test edilmiştir.

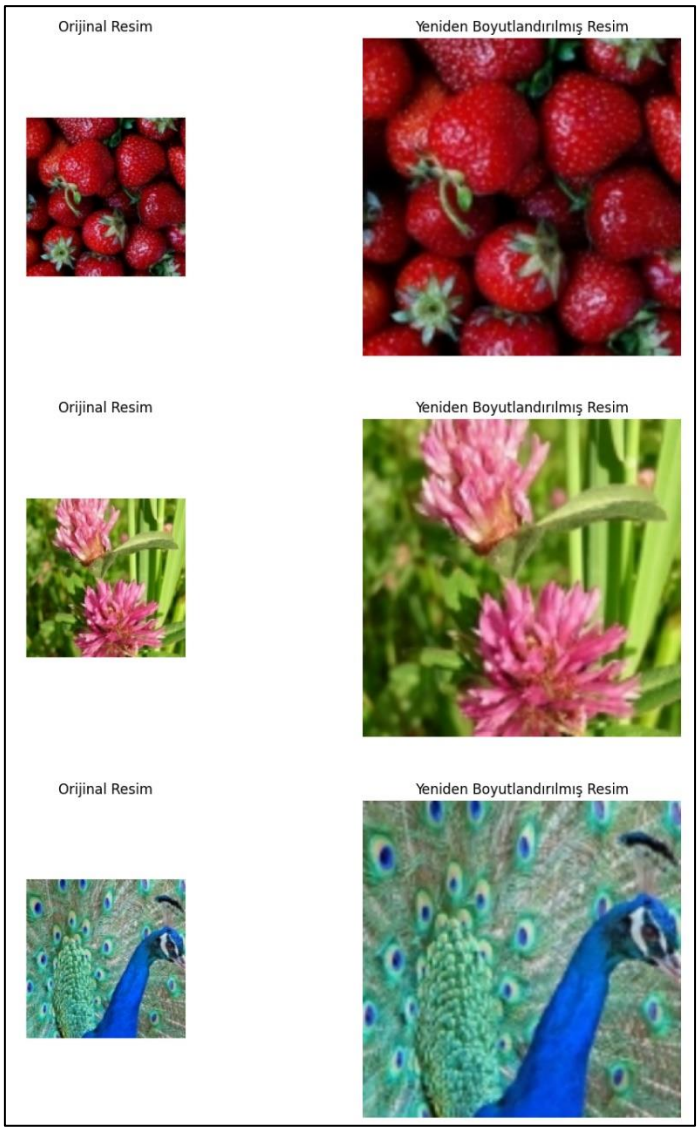
Test aşamasında Linnaeus 5 veri tabanının yanı sıra steganografi alanındaki çalışmalarda yaygın olarak kullanılan ImageNet ve LFW veri tabanları da kullanılmıştır. Böylece hem farklı veri tabanlarında modelin performansı değerlendirilebilinmiş hem de literatürdeki çalışmaların sonuçları ile kıyas yapma olanağı elde edilmiştir. Test aşaması için her iki veri tabanından da 2000'er adet resim kullanılmıştır.

Modele uygulanmadan önce tüm veri setlerindeki görüntüler, modelin giriş boyutlarına uyacak şekilde 256x256 piksellik tek tip bir boyuta standartlaştırılmıştır. Şekil 3.10, 3.11 ve 3.12 de sırasıyla 32x32, 64x64 ve 128x128 orijinal boyutlarına sahip resimlerin 256x256 olarak yeniden boyutlandırılmasına ilişkin görseller yer almaktadır.

Şekil 3.10. 32x32 boyutundaki görüntülerin 256x256 boyutuma getirilmesi işlemi.



Şekil 3.11. 64x64 boyutundaki görüntülerin 256x256 boyutuma getirilmesi işlemi.



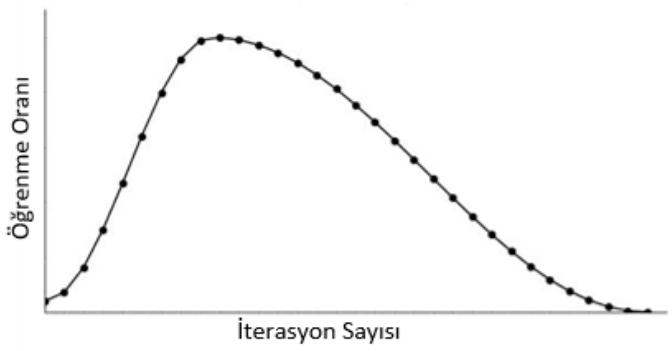
Şekil 3.12. 128x128 boyutundaki görüntülerin 256x256 boyutuma getirilmesi işlemi.

Ayrıca modelin öğrenme verimliliğini artırmak için normalleştirme uygulanmıştır. Bu süreç, veri kümesindeki her piksel değerinin [-1,1] aralığına ölçeklendirilmesini ve standartlaştırılmasını, böylece eğitim sürecinin verimlilik ve hız açısından optimize edilmesini sağlamaktadır.

Modelin eğitim aşamasında öğrenme oranının başlangıç değeri optimum değer olarak 0.001 olarak belirlenmiştir. Yığın boyutu olarak 32 kullanılmıştır. Model 200 devir boyunca eğitilmiştir. Ağın daha hızlı ve daha istikrarlı bir şekilde eğitilmesi amacıyla BN kullanılmıştır.

Optimizasyon algoritması olarak ağırlık bozulmasını etkili bir şekilde iyileştirme yeteneği ve adaptif öğrenme oranı ayarlamaları gibi özellikleri nedeniyle AdamW

kullanılmıştır. Ek olarak, dinamik öğrenme oranı ayarlamalarını daha da iyileştirmek amacıyla Tek Döngü Öğrenme Oranı Planlayıcısı (One Cycle Learning Rate Scheduler) yöntemi uygulanmıştır. Şekil 3.13'da bu planlayıcının çalışma prensibi görselleştirilmiştir.



Şekil 3.13. Tek Döngü Öğrenme Oranı Planlayıcısı.

Grafikte yer alan eğri minimum öğrenme oranı ile başlamaktadır. Daha sonra yükselme aşaması başlar. Öğrenme oranının kademeli artışını içeren yükseleme aşaması, modelin parametrelerinin geniş bir değer aralığında araştırılmasını hedefler. Bu süreçte, öğrenme oranı başlangıçta minimum bir değerden başlar ve iterasyonlar ilerledikçe maksimum bir değere doğru artar. Buradaki temel amaç, modelin eğitim veri setindeki potansiyel çözüm uzayını hızlı ve etkili bir biçimde taramasını sağlamaktır. Bu sayede, model, sınırlı bir bölgede sıkışıp kalmaktan ziyade, çok daha geniş bir perspektiften optimum parametre değerlerini keşfetme imkanı bulur. Yükseleme aşaması boyunca model, farklı parametre kombinasyonlarını test ederek, veri setinin genel yapısını daha iyi yansıtan ve dolayısıyla yeni ve görülmemiş verilere karşı daha iyi genelleme yapma yeteneğine sahip olabilecek parametrelerin belirlenmesine katkıda bulunur. Maksimum öğrenme oranına ulaştıktan sonra kademeli olarak azalma aşaması başlar ve minimum değere ulaşılır. Bu aşamanın amacı, modelin daha önce geniş arama sırasında keşfettiği parametre uzayını, daha dar ve spesifik bir alana odaklanarak incelemesini sağlamaktır. Model, bu aşamada, eğitim verilerindeki örüntüleri daha hassas bir şekilde öğrenir, aşırı uyum riski azalır ve böylece daha kararlı bir duruma ulaşır. Eğitim sürecinin sonuna doğru, öğrenme oranı daha da küçük bir değere düşürülerek modelin optimum noktaya stabil bir şekilde yakınsaması sağlanır. Tez çalışmasında tek döngü öğrenme oranı planlayıcısı parametreleri, öğrenme oranının 1e-4'ten başlayıp 1e-2'ye kadar artması ve ardından 1e-6 seviyesine düşmesi şeklinde ayarlanmıştır.

3.3. Kullanılan Platform Bilgileri

Tez çalışması kapsamında hesaplama işlemleri ve model geliştirme süreçleri, Python programlama dili ve PyTorch kütüphanesi kullanılarak gerçekleştirilmiştir. Eğitim ve test süreçleri, yerel bir bilgisayar ortamında yüksek hesaplama gücü gereksinimleri nedeniyle yürütülemediğinden Google Colab (Colaboratory) Pro platformu tercih edilmiştir. Google Colab, yapay zeka, makine öğrenimi ve derin öğrenme projelerinin bulut tabanlı bir ortamda çalışmasını sağlayan, çeşitli kütüphane ve araçları içeren ayrıca ücretsiz Merkezi İşlem Birimi (Central Process Unit, CPU) ve GPU erişimi sunan interaktif bir platformdur [113]. Bu platform, kullanıcıların Python programlama dili modellemelerini etkili bir şekilde gerçekleştirmelerine olanak tanımaktadır.

Colab Pro, standart sürümüne kıyasla artırılmış bellek kapasitesi, uzatılmış oturum süreleri, daha güçlü hesaplama kaynakları ve öncelikli erişim gibi ek özellikler sunmaktadır. Bu durum, özellikle büyük veri setleriyle çalışan ve modellerini daha hızlı eğitmek isteyen kullanıcılar için avantaj sağlamaktadır. Bu tez çalışmasında eğitim ve test aşamaları Colab Pro tarafından sağlanan Nvidia Tesla A100 40Gb GPU ile gerçekleştirilmiştir.

3.4. Ölçüm Metrikleri ve Kayıp Fonksiyonu

Tez çalışması kapsamında mimarinin performansını değerlendirmek ve literatürdeki diğer çalışmalarla kıyas yapabilmek için MSE, PSNR ve SSIM metrikleri kullanılmıştır. Literatür taraması kısmındaki çalışma özetlerinde de belirtildiği gibi bu metrikler steganografi mimarilerinin performansını değerlendirme noktasında en çok kullanılan ölçütlerdir. Bunların haricinde histogram çizimleri ve görüntülerin fark görselleriyle birlikte görsel sonuçları da değerlendirilmiştir.

MSE, kapak görüntüsü ile stego görüntü arasındaki kümülatif karesel hatayı hesaplayarak, stego görüntüsündeki bozulma oranını ölçmek için kullanılmaktadır [114]. MSE değeri ne kadar küçük ise, stego görüntüsü o oranda kapak görüntüsüne benzemektedir. Aynı metrik gizli görüntü ile çıkartılmış gizli görüntü arasındaki bozulma oranını hesaplamak için de kullanılmaktadır. Bu durumda metrik sonucu, stego resimden çıkartılmış gizli görüntünün orijinal gizli görüntüye ne kadar benzediğini ifade etmektedir. MSE, (3.1) denklemi kullanılarak hesaplanmaktadır.

$$\mathrm{MSE} = \frac{\Sigma_{M,N}\,[I_1(m,n) - I_2(m,n)]^2}{M * N} \tag{3.1}$$

(3.1)'de $I_1(m, n)$ kapak resminin (m,n) konumundaki piksel değerini, $I_2(m, n)$ stego resminin (m,n) konumundaki piksel değerini göstermektedir. M ve N ise görüntünün satır ve sütun sayısını ifade etmektedir. Aynı formül kullanılarak, gizli resim ile stego resimden çıkarılan gizli resim arasındaki fark hesaplanabilir.

PSNR, kapak ve stego görüntüleri arasındaki ortalama hata oranını piksel başına ölçen bir metriktir ve görüntüleri arasındaki benzerlik derecesini ölçer. Bu metrik, kapak ve stego görüntüleri arasındaki bozulmaların miktarını ve bu bozulmaların görsel kalite üzerindeki potansiyel etkilerini değerlendirmek için kullanılır. Aynı prensip, gizli bir resmin çıkarılma işlemi için de geçerlidir. Bu durumda, orijinal gizli resim ile çıkarılan gizli resim arasındaki farklar PSNR metriği kullanılarak ölçülür. Bu ölçüm, çıkarma işleminin doğruluğunu ve etkinliğini, yani gizli verinin ne derece hasarsız bir şekilde geri kazanıldığını belirlemek için kullanılır. PSNR değeri, desibel (dB) cinsinden ölçülür ve MSE parametresi ile ters orantılıdır. Başka bir deyişle, PSNR değeri, MSE ne kadar düşükse (yani hatalar ne kadar azsa) o kadar yüksek olur [115]. PSNR (3.2) kullanarak hesaplanabilmektedir.

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{R}^2}{\mathrm{MSE}}\right) \tag{3.2}$$

(3.2) de R bir pikselin görüntüde alabileceği en yüksek değeri temsil eder. Bu değer, $R=2^n-1$ formülü ile hesaplanır, burada n piksel derinliğini temsil eder. Sekiz bitlik bir görüntü için, bu değer 255'tir.

Derin öğrenme uygulamalarında PSNR değerinin 40 dB üzerinde olması, gizli resmin kapak resmi içine gömülmesi veya çıkarılması sırasında çok iyi bir algılanamazlık düzeyini ve kaliteyi ifade eder. PSNR değerinin 30 dB ile 40 dB aralığından olması kabul edilebilir olarak değerlendirilir. Ancak, 30 dB'in altındaki PSNR değerleri, bozulmanın fazla olduğunu gösterir ve genellikle kabul edilmez [114].

SSIM, görüntü kalitesinin değerlendirilmesi sürecinde, insan görsel algısını yansıtmayı hedefleyen bir metriktir. Sadece piksel bazlı farkları değerlendirmek yerine görüntülerin parlaklık, kontrast ve yapısal özelliklerini ele alarak, kapak ve stego görüntüler arasındaki yapısal bütünlüğün korunup korunmadığını değerlendirmektedir [116]. SSIM, görüntünün ortalama parlaklık değerlerini, kontrast düzeylerini ve özellikle piksellerin birbirine göre konumlarını ve bu konumların oluşturduğu dokuları ve desenleri dikkate alarak, bu yapısal öğeler üzerinden bir analiz gerçekleştirir. Aynı şekilde, bu metrik orijinal gizli resim ile stego resimden çıkarılmış gizli resim arasındaki yapısal benzerliği

değerlendirirken de kullanılmaktadır. SSIM, 0 ile 1 arasında bir değer aralığında sonuçlar üretir. Bu ölçek üzerinde, 1'e yaklaşan değerler, stego görüntünün orijinal kapak görüntüsüne yüksek derecede benzerlik gösterdiğini ifade etmektedir [117].

Görüntüler arasındaki parlaklık benzerliği (3.3), kontrast benzerliği (3.4), yapı benzerliği (3.5) ve tüm bu bileşenlerin bir araya gelmesiyle ifade edilen SSIM ise (3.6) ile hesaplanmaktadır.

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \tag{3.3}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \tag{3.4}$$

$$\mathrm{s(x,y)} = \frac{2\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \tag{3.5}$$

$$\mathrm{SSIM} = \mathrm{l(x,y)} * \mathrm{c(x,y)} * \mathrm{s(x,y)} \tag{3.6}$$

μ_x ve μ_y sırasıyla x ve y görüntülerinin ortalama parlaklık değerlerlerini temsil eder. σ_x and σ_y, x ve y görüntülerinin standart sapmalarıdır ve görüntülerin kontrast düzeyini ifade eder. σ_{xy} , x ve y görüntülerinin kovaryansını ifade eder, yani piksellerin birbirleriyle olan ilişkisini ve bu ilişkinin tutarlılığını göstermektedir.

SSIM, PSNR ve MSE gibi metrikler, bir modelin görüntü kalitesi üzerindeki etkilerini değerlendirmede kullanılırken bu parametrelerin yanı sıra, modelin veri gizleme kapasitesini belirlemek için BPP ölçütü de sıklıkla kullanılır. BPP, her bir piksel başına düşen gizli veri miktarını ifade eder ve böylece modelin veri saklama verimliliğini ortaya koyar. Yüksek bir BPP değeri, daha fazla verinin görüntüye gizlenebildiğini göstermektedir. Bu metrik (3.7) ile hesaplanmaktadır.

$$\mathrm{BPP} = \frac{\text{Gizlenen Bit Sayısı}}{\mathrm{MxN}} \tag{3.7}$$

MxN stego görüntüsünün satır ve sütun sayıları çarpımını ifade etmektedir. Örneğin 256x256x3 boyutundaki bir kapak resmine aynı boyutlu bir resmi gizlediğimizde (3.8)'de görüldüğü gibi BPP 24 değerini vermektedir.

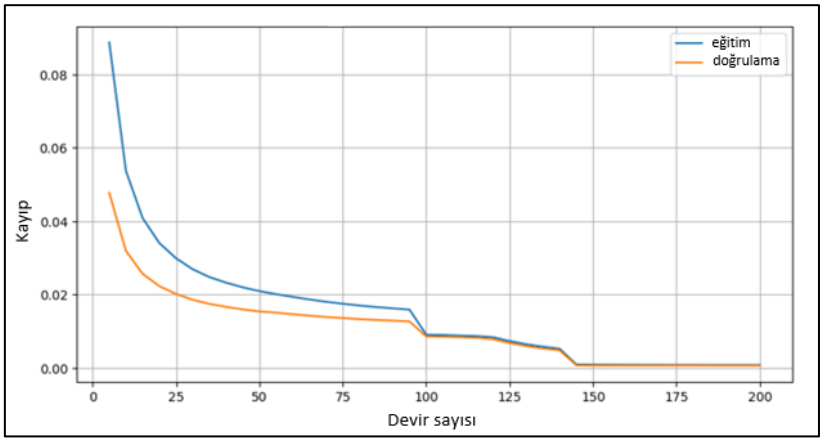
$$\mathrm{BPP} = \frac{256\mathrm{x}256\mathrm{x}3\mathrm{x}8}{256\mathrm{x}256} = 24 \tag{3.8}$$

SSIM, PSNR ve MSE ile birlikte kullanıldığında, BPP, gizlenen veri miktarı ile elde edilen görüntü kalitesi arasındaki dengeyi değerlendirmek için bir çerçeve sunmaktadır.

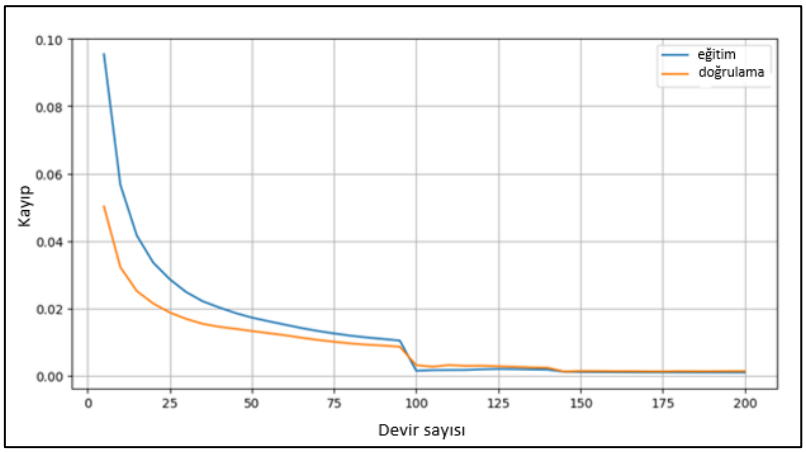
Modelin eğitim aşamasında , MSE ve SSIM olmak üzere iki temel bileşeni birleştiren özel bir kayıp fonksiyonu kullanılmıştır. Bu kayıp fonksiyonu, bu iki bileşen arasında bir denge kurmayı amaçlar. MSE, modelin çıktısı ile hedef arasındaki piksel düzeyindeki farkları ölçerken, SSIM, modelin çıktısı ile hedef arasındaki yapısal ve dokusal benzerliği değerlendirir. (3.9)'da gösterildiği gibi α olarak gösterilen bir parametre, her bileşene verilen ağırlığı belirlemektedir. Tez çalışmasında α değeri 0.6 olarak belirlenmiştir.

$$L = \alpha . MSE + (1 - \alpha) . (1 - SSIM) \tag{3.9}$$

Şekil 3.14'de modelin gizleme ve çıkarma için kullanılan U-Net mimarilerine ilişkin kayıp fonksiyonları grafikleri verilmiştir.



(a)

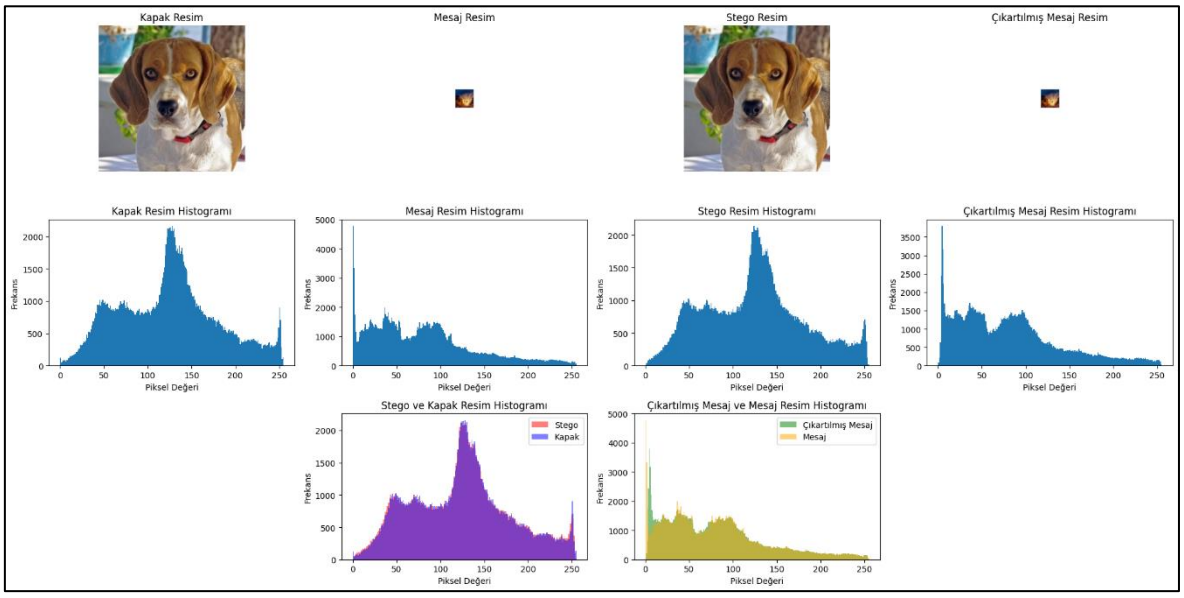


(b)

Şekil 3.14. Gizleme ve çıkarma ağı kayıp fonksiyonları, (a) gizleme ağı, (b) çıkarma. ağı.

3.5. Linnaues 5 Veri Tabanı Kullanılarak Farklı Orijinal Boyutlara Sahip Gizli Görüntülerin Kapak Görüntüsü Üzerindeki Etkisinin İncelenmesi

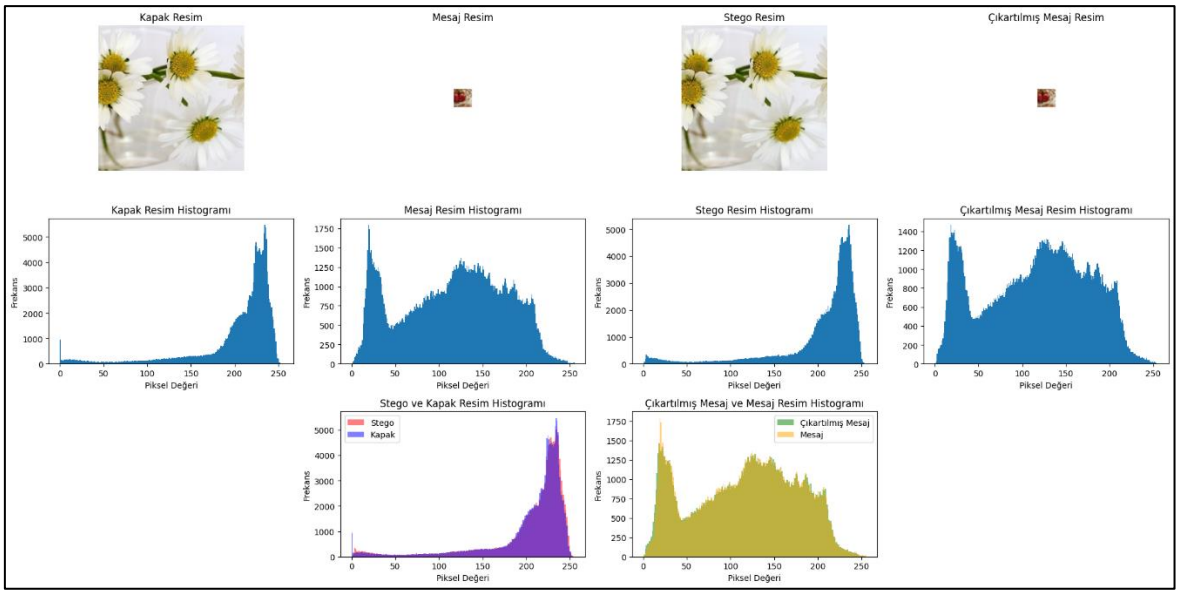
Tez çalışmasının bu aşamasında Linnaues 5 veri tabanın kendi içinde farklı klasörlerde tuttuğu 32x32x3, 64x64x3, 128x128x3 ve 256x256x3 orijinal boyutuna sahip resimlerden faydalanılmıştır. Kapak resmi olarak orjinal boyutu 256x256x3 olan görüntüler kullanılmış ve bahsedilen bu farklı gizli resim boyutları kapak resmi ile aynı boyuta getirilerek mimariye uygulanmıştır. Böylece gizli görüntülerin orjinal boyutlarının kapak resmi üzerindeki etkisinin incelenmesi mümkün olmuştur. Şekil 3.15 ve 3.16'da orjinal mesaj resmi boyutunun 32x32x3 olduğu duruma ilişkin steganografi işlemi öncesi ve sonrası histogram sonuçları ve Tablo 3.1 ve 3.2'de de bu sonuçlara ilişkin PSNR ve SSIM metriklerinin değerleri yer almaktadır. Orjinal mesaj resmi boyutunun görsel olarak sunulabilmesi adına ilgili şekillerde 256x256 boyutuna getirilmemiş orjinal boyuttaki görseller kullanılmıştır.



Şekil 3.15. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-1 (kapak resmi 256x256x3, orjinal mesaj resmi 32x32x3).

Tablo 3.1. Şekil 3.15 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
49,8863	49,5489	0,9963	0,9890

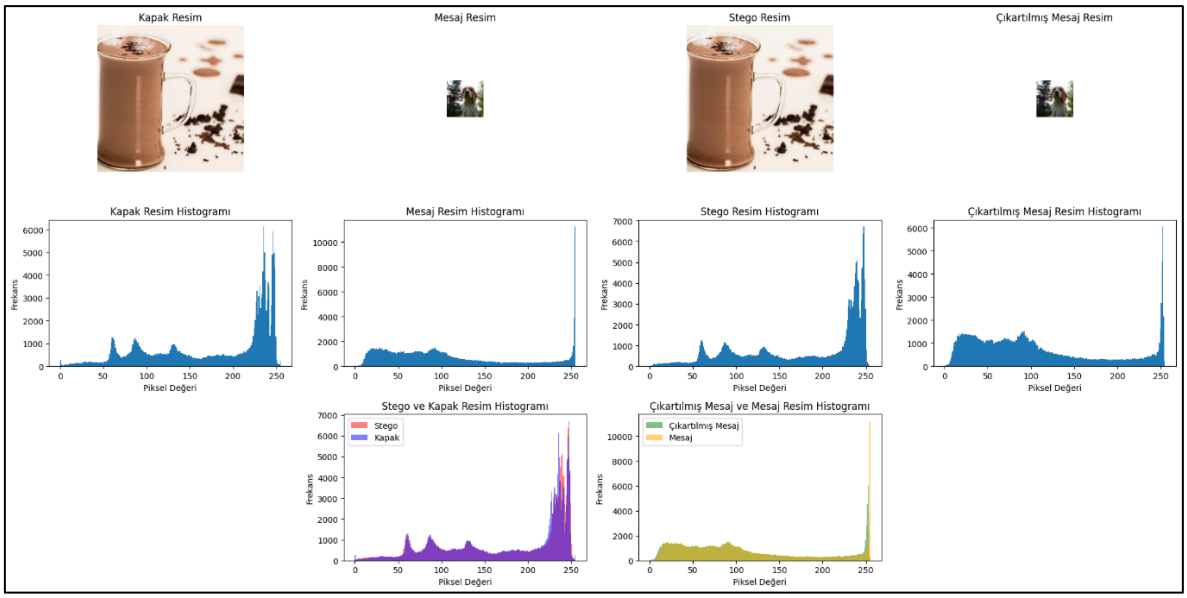


Şekil 3.16. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-2 (kapak resmi 256x256x3, orjinal mesaj resmi 32x32x3).

Tablo 3.2. Şekil 3.16 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
49,0578	51,8331	0,9951	0,9970

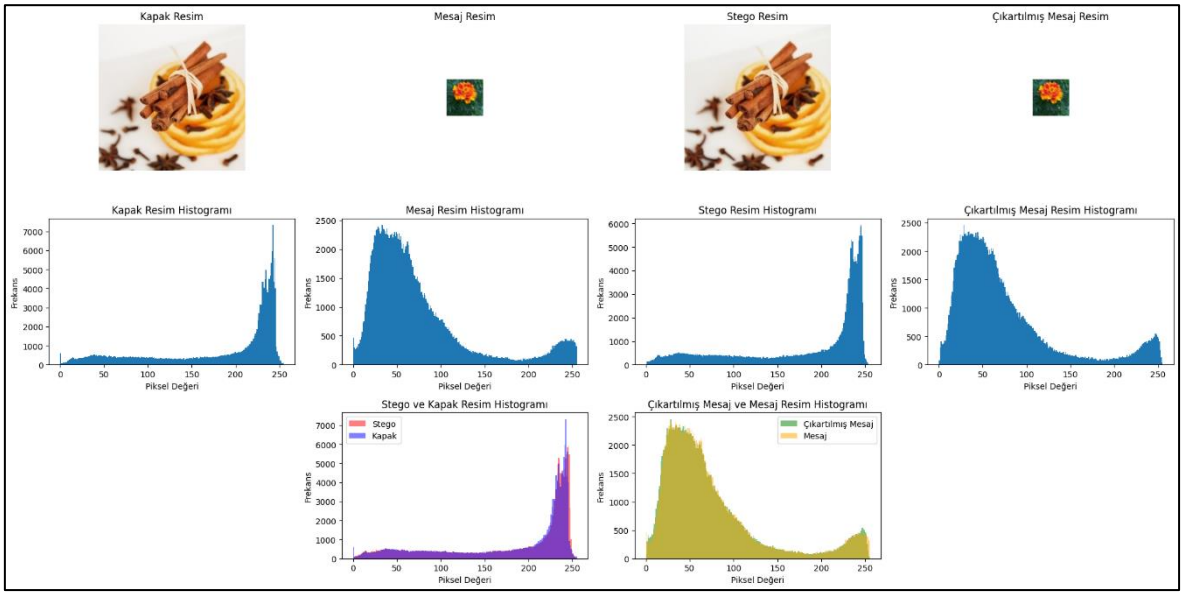
Şekil 3.17 ve 3.18'de, orijinal mesajın 64x64x3 boyutlarında olduğu durumda, steganografi uygulamasının öncesine ve sonrasına dair histogram analizleri sunulmuştur. Tablo 3.3 ve 3.4 ise bu analizlerin PSNR ve SSIM metrikleriyle ölçümlenmiş sonuçlarını içermektedir.



Şekil 3.17. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasındaki histogram farklarına ilişkin örnek-1 (kapak resmi 256x256x3, orjinal mesaj resmi 64x64x3).

Tablo 3.3. Şekil 3.17 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
48,6180	47,5668	0,9965	0,9929

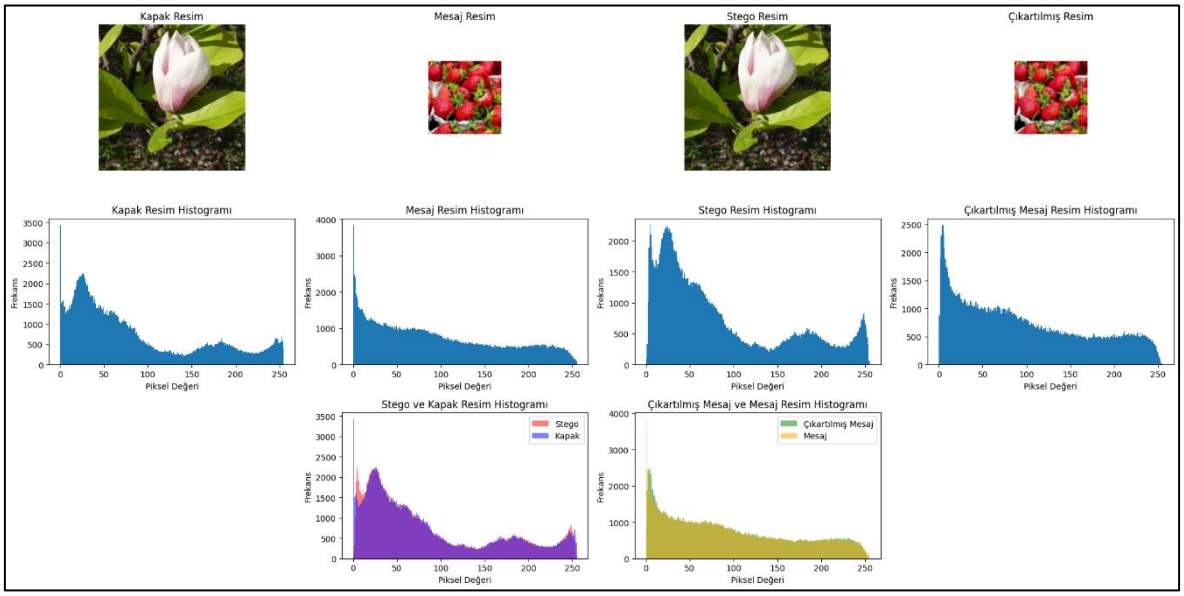


Şekil 3.18. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasındaki histogram farklarına ilişkin örnek-2 (kapak resmi 256x256x3, orjinal mesaj resmi 64x64x3).

Tablo 3.4. Şekil 3.18 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
47,9566	47,205	0,9929	0,9938

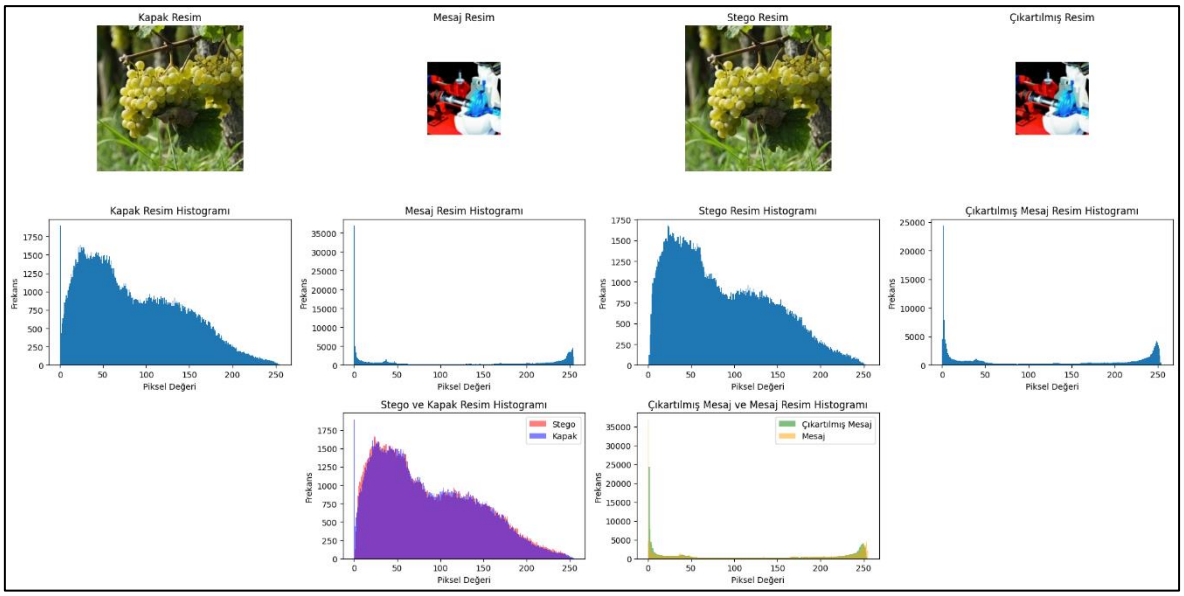
128x128x3 boyutlarındaki orijinal mesaj görüntüleri için steganografi öncesi ve sonrası durumların histogram karşılaştırmaları Şekil 3.19 ve 3.20'de yer almakta, bu işlemlerin PSNR ve SSIM gibi kalite metrikleriyle ölçüm sonuçları da Tablo 3.5 ve 3.6'da sunulmaktadır.



Şekil 3.19. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-1 (kapak resmi 256x256x3, orjinal mesaj resmi 128x128x3).

Tablo 3.5. Şekil 3.19 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
46,0646	46,9345	0,9885	0,9931

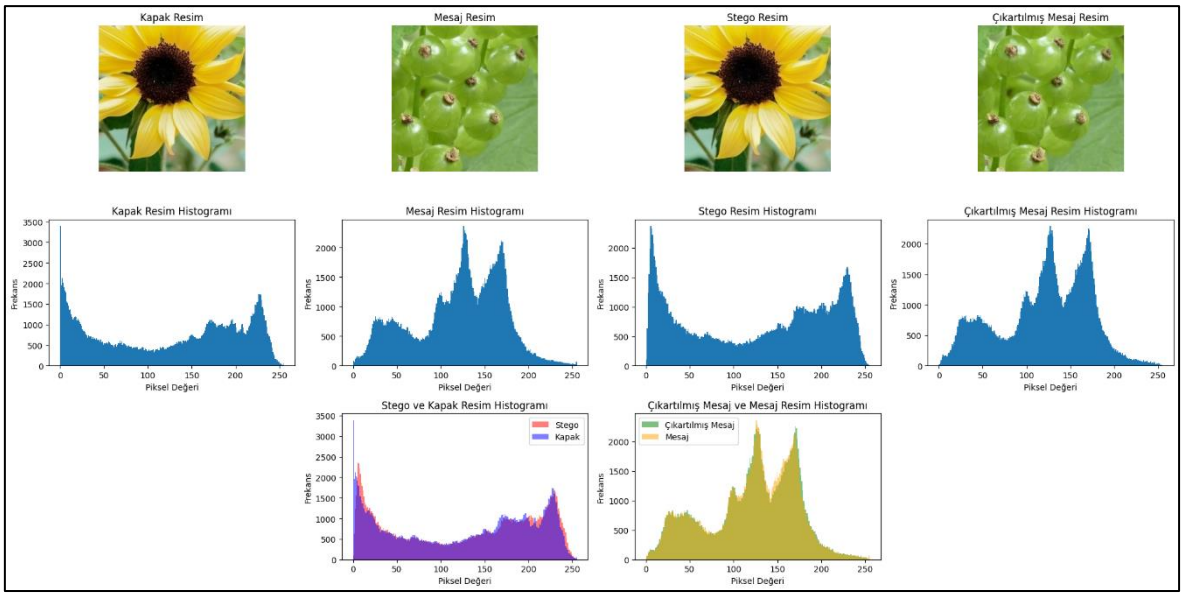


Şekil 3.20. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasındaki histogram farklarına ilişkin örnek-2 (kapak resmi 256x256x3, orjinal mesaj resmi 128x128x3).

Tablo 3.6. Şekil 3.20 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
45,0943	45,1938	0,9924	0,9777

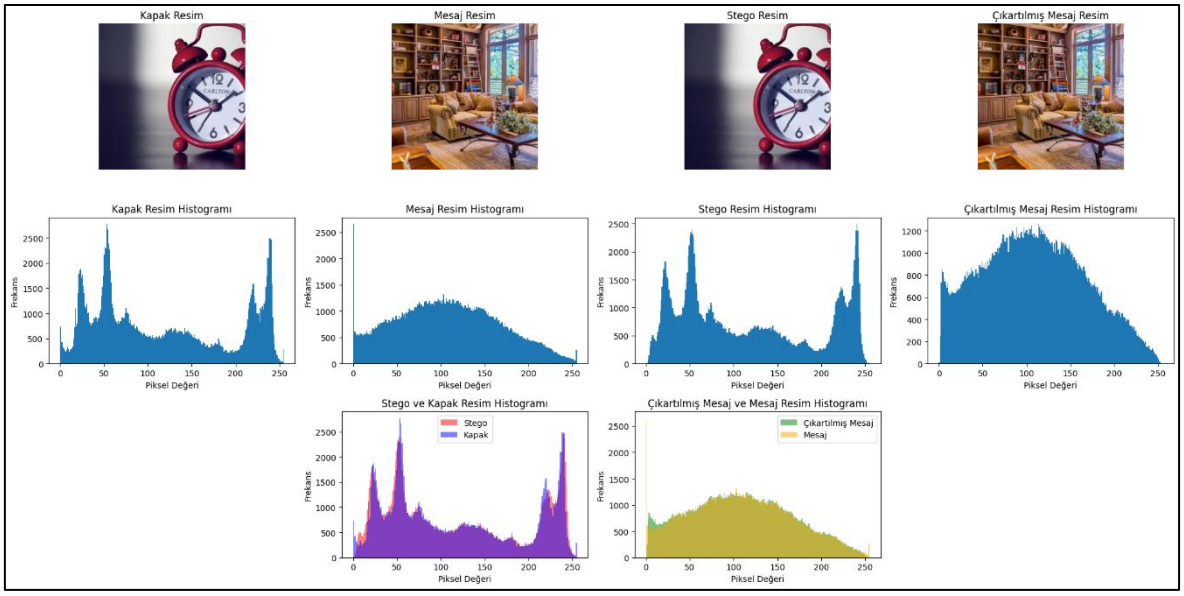
Son aşama olarak, Şekil 3.21 ve 3.22'de orijinal mesajın 256x256x3 boyutlarında olduğu durumda, steganografi uygulamasının öncesine ve sonrasına dair histogram analizleri sunulmuştur. Tablo 3.7 ve 3.8 ise bu analizlerin PSNR ve SSIM metrikleriyle ölçümlenmiş sonuçlarını içermektedir.



Şekil 3.21. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-1 (kapak resmi 256x256x3, orjinal mesaj resmi 256x256x3).

Tablo 3.7. Şekil 3.21 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
43,5219	46,2242	0,9838	0,9928



Şekil 3.22. Steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-2 (kapak resmi 256x256x3, orjinal mesaj resmi 256x256x3).

Tablo 3.8. Şekil 3.22 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
45,4304	42,0345	0,9883	0,9913

Tablo 3.9'da 32x32,64x64,128x128 ve 256x256 olmak üzere farklı boyutlara sahip mesaj görüntülerinin, 256x256 boyutuna sahip kapak resmine gizlenmesi ve tekrar çıkarılması sonucunda elde edilen ortalama PSNR ve SSIM değerleri yer almaktadır.

Tablo 3.9. Farklı mesaj resmi boyutları için ortalama PSNR ve SSIM değerleri

Kapak Resmi Boyutu	Orijinal Mesaj Resmi Boyutu	Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
256x256x3	32x32x3	49,5532	49,0738	0,9946	0,9940
256x256x3	64x64x3	49,0185	48,6563	0,9933	0,9924
256x256x3	128x128x3	47,9247	46,7569	0,9911	0,9902
256x256x3	256x256x3	44,4656	43,5393	0,9897	0,9875

Tablo 3.9'da sunulan ortalama değerler incelendiğinde, 32x32x3 boyutlarındaki orijinal görüntülerin 256x256x3 boyutlarına çıkarıldığında ve mesaj görüntüsü olarak mimariye verildiğinde, PSNR ve SSIM değerlerinin en yüksek sonuçları verdiği gözlemlenmiştir. Araştırma bulguları, orijinal mesaj görüntülerinin boyutları ile steganografik kalitenin PSNR ve SSIM metrikleriyle ölçülmesi arasında bir korelasyon olduğunu göstermektedir. Küçük boyutlu görüntülerin daha büyük bir formata dönüştürülmesi sürecinde, interpolasyon yöntemi devreye girer; bu, orijinal görüntünün mevcut pikselleri arasında yeni pikseller oluşturarak boyutunun artırılmasını sağlar. Interpolasyon işlemleri sırasında genellikle piksel değerlerinin arasındaki geçişler düzgünleştirerek bir tür yumuşatma etkisi yaratılır. Bu yumuşatma, görüntünün yüksek frekanslı bileşenlerini ve gürültüyü azaltarak steganografik süreç üzerinde olumsuz etkileri minimuma indirir. Sonuç olarak, mesaj görüntüsü kapak görüntüsüne daha uyumlu şekilde gizlenir ve bu da yüksek PSNR ve SSIM değerleri ile sonuçlanır. Öte yandan, daha yüksek çözünürlüklü orijinal görüntüler, daha fazla ayrıntı ve piksel başına daha yoğun bilgi içerdiğinden, bunlar kapak görüntüsü içerisine gizlendiğinde, hem gizleme hem de çıkarma mimarilerinde daha düşük PSNR ve SSIM değerleri elde edilmiştir.

Tek döngü öğrenme oranı planlayıcısının AdamW ile birlikte kullanılmasının metriksel sonuçlara kattığı iyileşme oranını değerlendirebilmek amacıyla bu kombinasyon ile elde edilen PSNR ve SSIM değerleri ile modelin sadece AdamW kullanılarak eğitildiği durumda elde edilen metriksel sonuçlar ve iyileşme oranları Tablo 3.10'da verilmiştir.

Sonuçlar hem kapak hem de mesaj görüntülerinin 256x256 boyutunda olduğu senaryo üzerinden kıyaslanmıştır.

Tablo 3.10. Tek döngü öğrenme oranı planlayıcısı kullanımının PSNR ve SSIM sonuçları üzerindeki etkisi

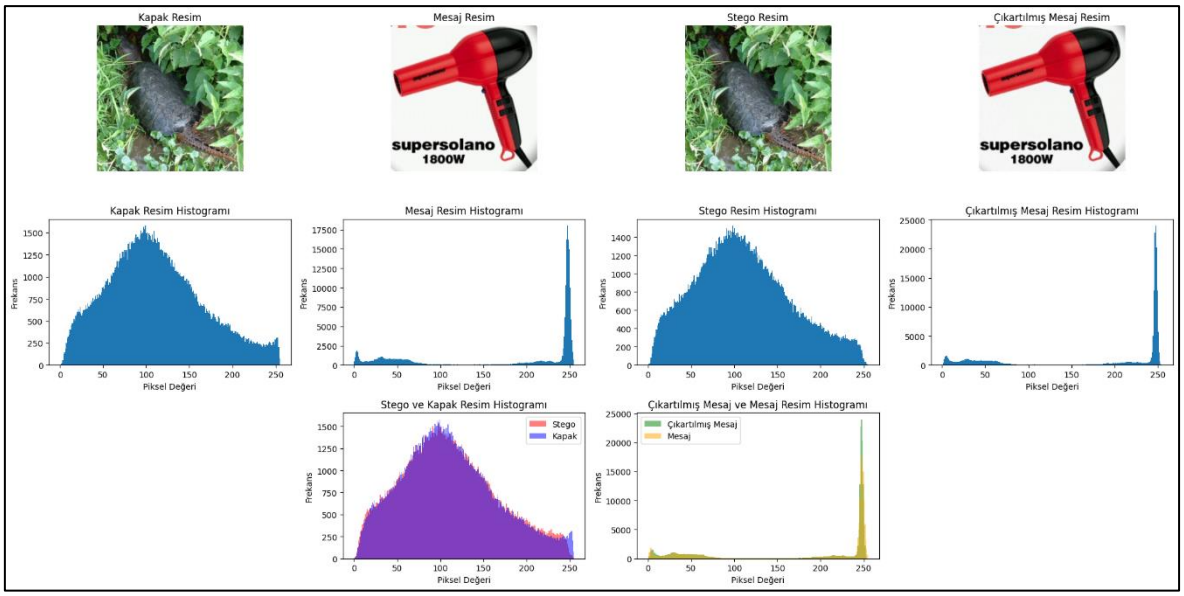
	Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
AdamW	36,6115	33,2610	0,9640	0,9561
AdamW+ Tek Döngü Öğrenme Oranı Planlayıcısı	44,4656	43,5393	0,9897	0,9875
İyileşme Oranı	%21,45	%30,90	%2,67	%3,28

Görüldüğü gibi AdamW tek başına kullanıldığında elde edilen PSNR ve SSIM metriklerine göre, tek döngü öğrenme oranı planlayıcısının eklenmesiyle her iki metrikte de önemli iyileşmeler görülmüştür. PSNR değerinde stego-kapak resimleri için %21,45 ve çıkartılmış mesaj-mesaj resimleri için %30,90, SSIM'de ise sırasıyla %2,67 ve %3,28 oranında iyileşme kaydedilmiştir. Bu sonuçlar, tek döngü öğrenme oranı planlayıcısının, modelin öğrenme sürecine ve sonuçlarına olumlu katkıda bulunduğunu göstermektedir.

3.6. Gizleme ve Çıkarma Mimarilerinin ImageNet ve LFW Veri Tabanları ile Test Edilmesi

Tez çalışmasının bu kısmıda gizleme ve çıkarma ağları farklı karakteristikte görüntüler içeren ImageNet ve LFW veri tabanları ile de test edilmiş ve model performansı değerlendirilmiştir. Böylece modelin farklı veri tabanları üzerinde genelleştirme yeteneği de test edilmiş olmuştur.

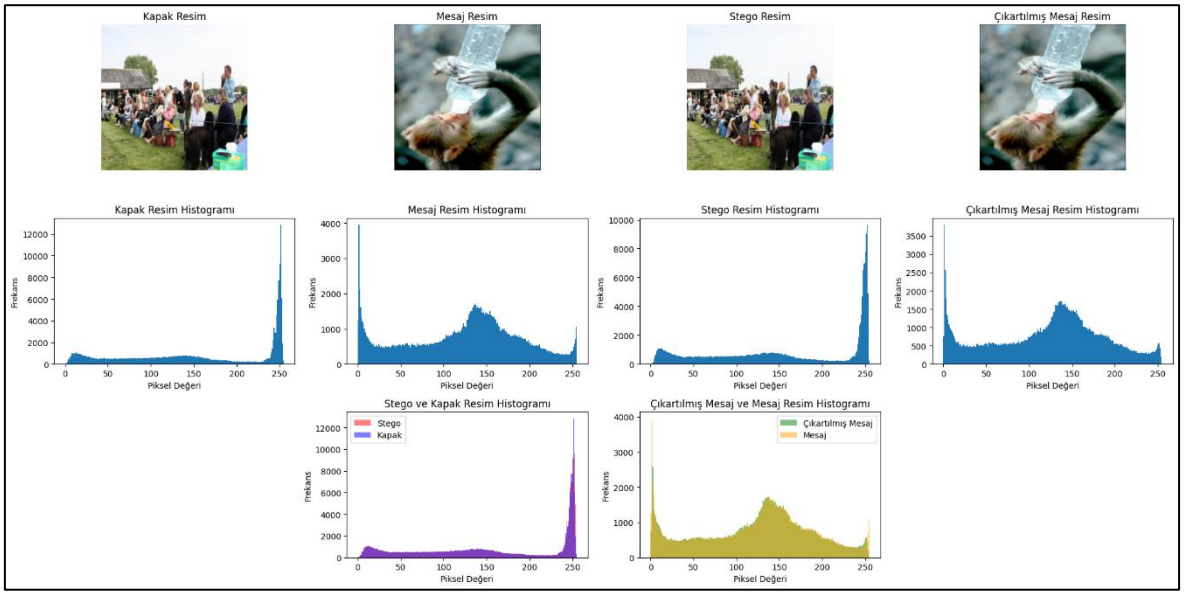
Şekil 3.23 ve 3.24'de, Imagenet veri tabanı görüntüleri üzerinde steganografi uygulamasının öncesine ve sonrasına dair histogram analizleri sunulmuştur. Tablo 3.11 ve 3.12 ise bu analizlerin PSNR ve SSIM metrikleriyle ölçümlenmiş sonuçlarını içermektedir.



Şekil 3.23. ImageNet veri tabanı görüntülerinde steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasındaki histogram farklarına ilişkin örnek-1.

Tablo 3.11. Şekil 3.23 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
43,6510	45,0808	0,9931	0,9880

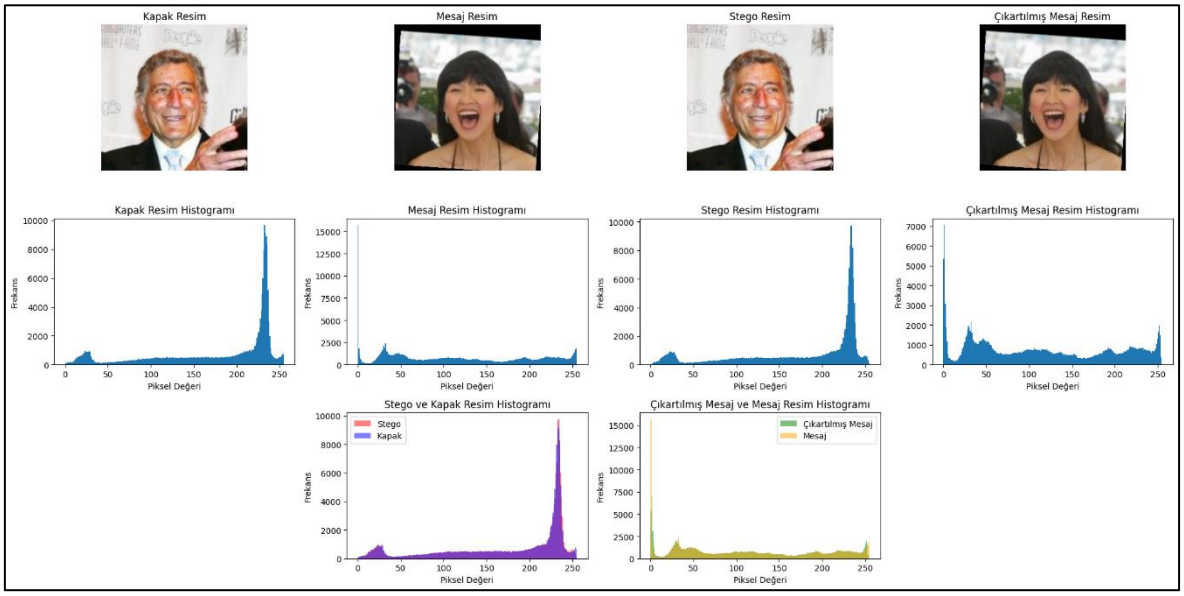


Şekil 3.24. ImageNet veri tabanı görüntülerinde steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasındaki histogram farklarına ilişkin örnek-2.

Tablo 3.12. Şekil 3.24 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
45,3357	45,4995	0,9946	0,9932

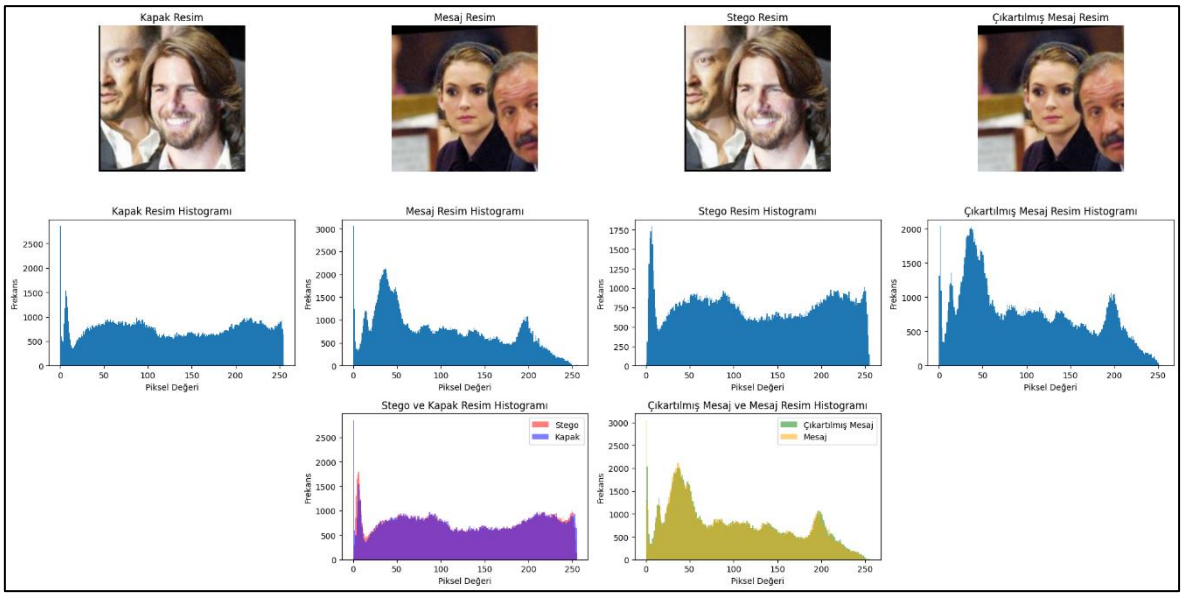
LFW veri tabanına ait görüntülerin steganografi öncesi ve sonrası durumların histogram karşılaştırmaları Şekil 3.25 ve 3.26'da yer almakta, bu işlemlerin PSNR ve SSIM gibi kalite metrikleriyle ölçüm sonuçları da Tablo 3.13 ve 3.14'de sunulmaktadır.



Şekil 3.25. LFW veri tabanı görüntülerinde steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-1.

Tablo 3.13. Şekil 3.25 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
49,7835	48,3560	0,9956	0,9952



Şekil 3.26. LFW veri tabanı görüntülerinde steganografi öncesi ve sonrası kapak ve mesaj görüntüleri arasıdaki histogram farklarına ilişkin örnek-2.

Tablo 3.14. Şekil 3.26 için PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
48,9175	49,3105	0,9965	0,9968

Tablo 3.15'de Linnaeus 5 veri seti ile gerçekleştirilen 256x256x3 kapak ve mesaj görüntülerinin kullanıldığı test sonuçlarına ek olarak ImageNet ve LFW veritabanları ile gerçekleştirilen test sonuçlarının ortalama PSNR ve SSIM değerleri yer almaktadır.

Tablo 3.15. Farklı veritabanları için ortalama PNSR ve SSIM değerleri

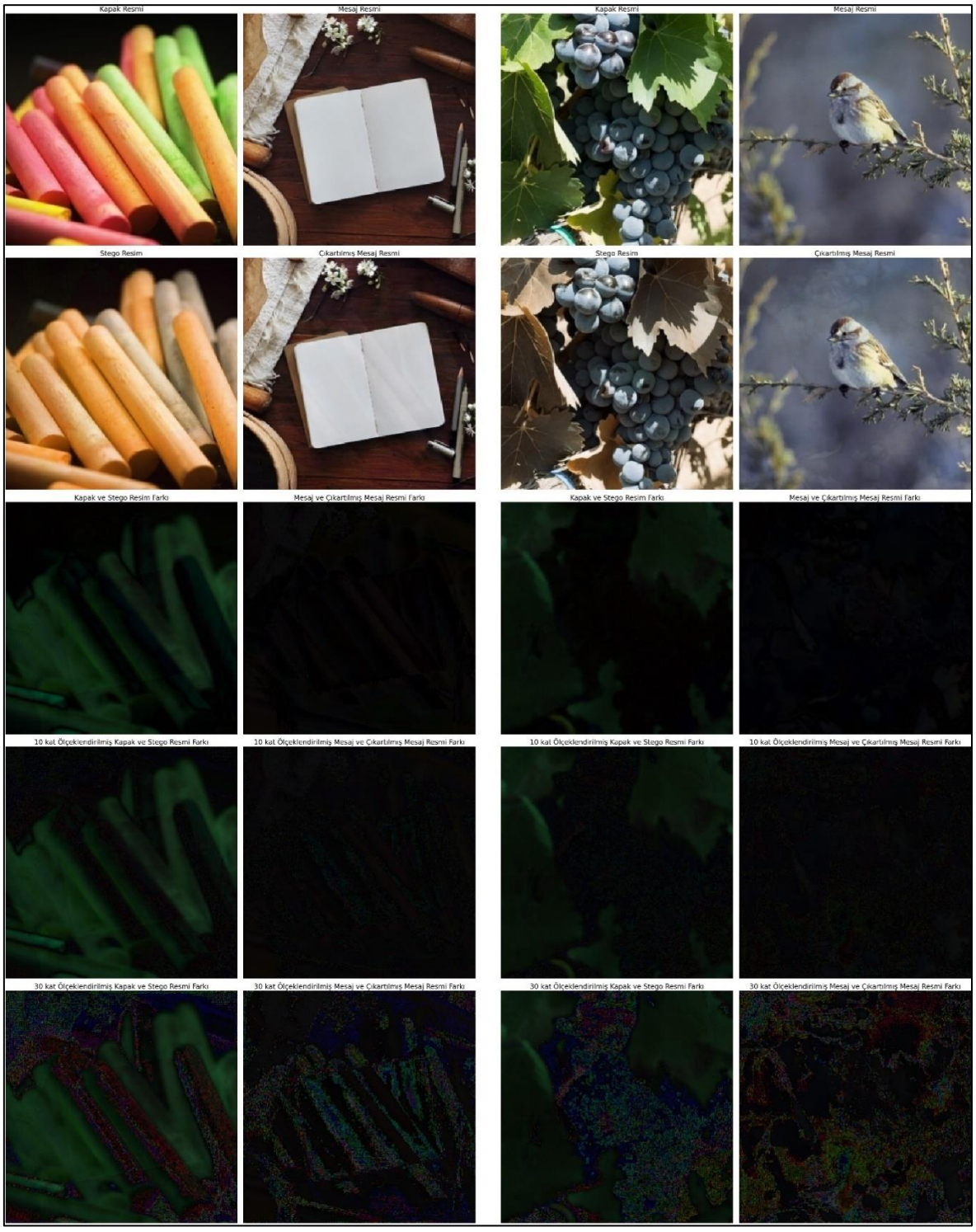
Veritabanı	Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Cover SSIM	Çıkartılmış Mesaj-Mesaj SSIM
Linnaeus 5	44,4656	43,5393	0,9897	0,9875
ImageNet	45,3966	44,8206	0,9906	0,9903
LFW	48,1407	47,5296	0,9930	0,9907

Tablo 3.15'de de görüldüğü gibi üç farklı veri kümesinden elde edilen oldukça iyi seviyede sonuçlar, modelin çeşitli veri türleri ve koşullarına karşı genelleme yeteneğini ve çeşitli görsellikte ve karmaşıklıktaki içerikleri başarılı bir şekilde işleyebildiğini göstermektedir.

3.7. Model Performansının Farklı Devir Sayılarına Göre Değerlendirilmesi

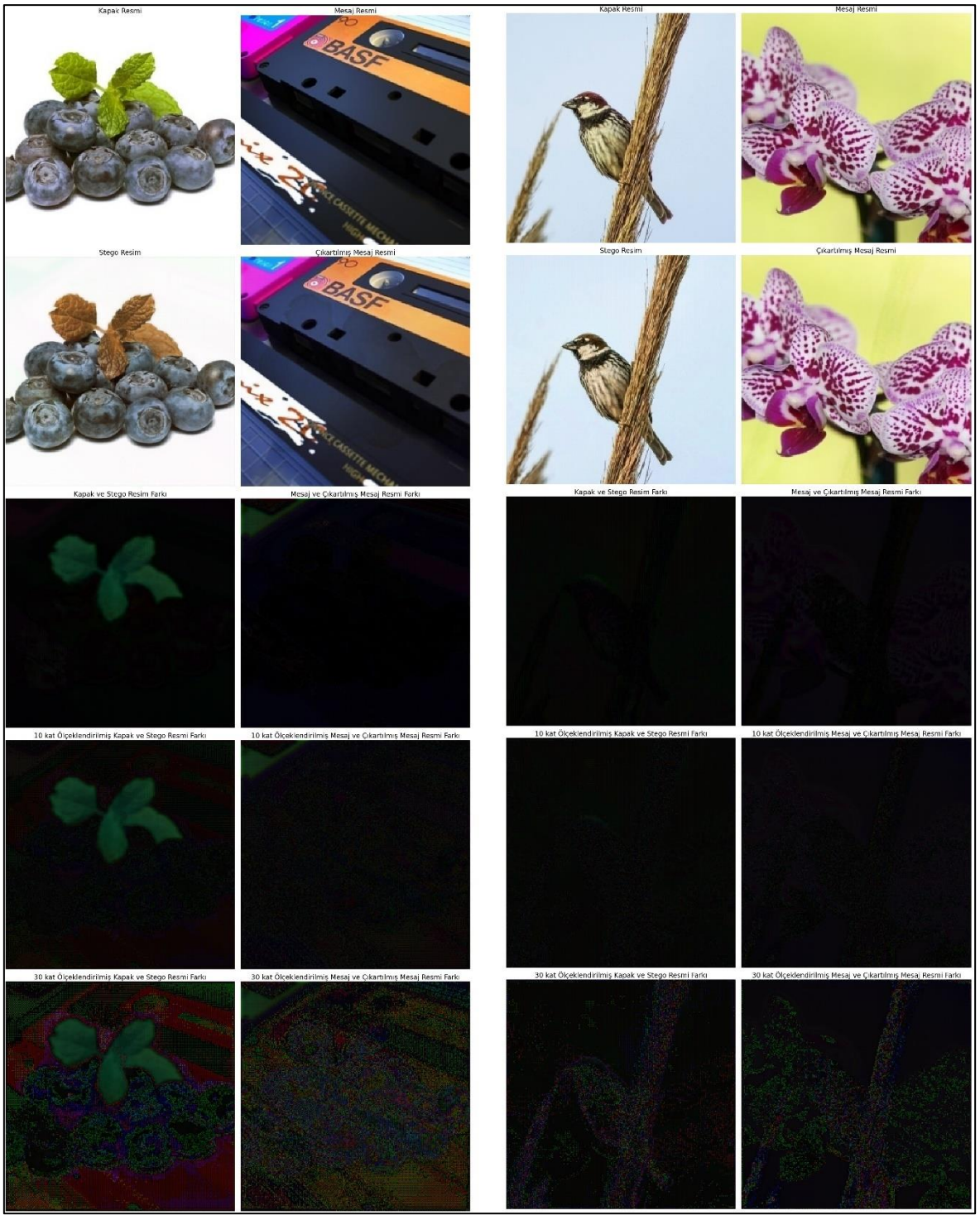
Tez çalışmasının bu bölümünde kullanılan 3 veri tabanı içinde modelin 50, 100 ve 200. devir sayılarındaki kapak-stego görüntüleri ve mesaj-çıkartılmış mesaj görüntülerine ilişkin görseller sunularak modelin devri sayıları boyunca gösterdiği performans iyileşmesi sunulmuştur. Ayrıca kapak-stego görüntüleri ve mesaj-çıkartılmış mesaj görüntülerine ilişkin fark resimleri ve farkların daha net görülmesi için ölçeklendirilmiş versiyonları sunulmuştur.

Şekil 3.27-3.29'da Linnaeus 5 veri tabanına ilişkin farklı devir sayılarındaki kapak-stego, mesaj-çıkartılmış mesaj görüntüleri ve ayrıca bunlara ilişkin fark görselleri verilmektedir.

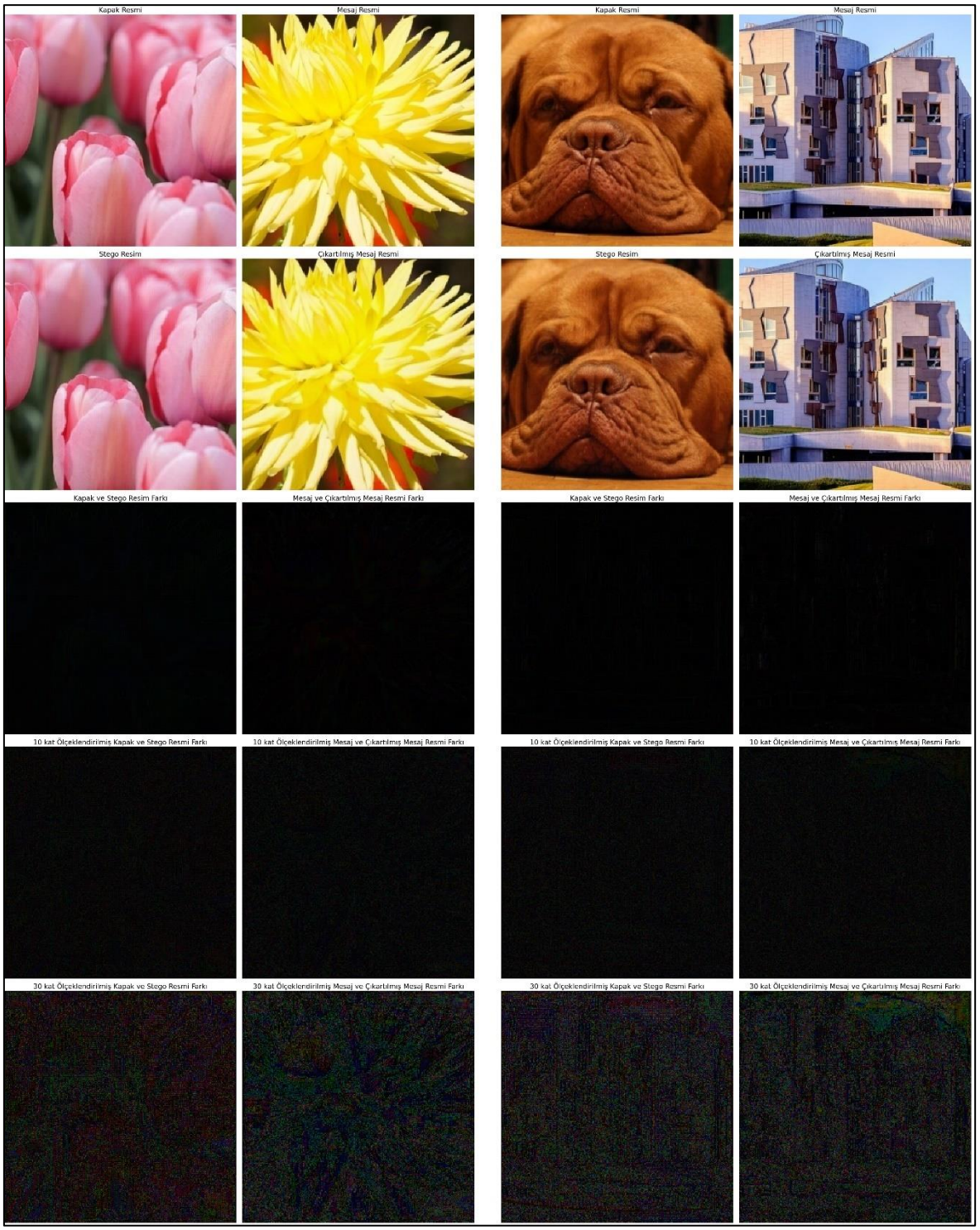


Şekil 3.27. Linnaeus 5 veritabanı için görsel sonuçlar (50 devir).

Şekil 3.27'de ilk satır sırasıyla kapak ve mesaj resimlerini, ikinci satır sırasıyla stego ve çıkartılmış mesaj resimlerini, 3. satır kapak-stego ve mesaj-çıkartılmış mesaj resimlerinin fark görsellerini, 4.ve 5. satırlar fark görsellerinin sırayla 10 kat ve 30 kat ölçeklendirilmiş versiyonlarını göstermektedir.

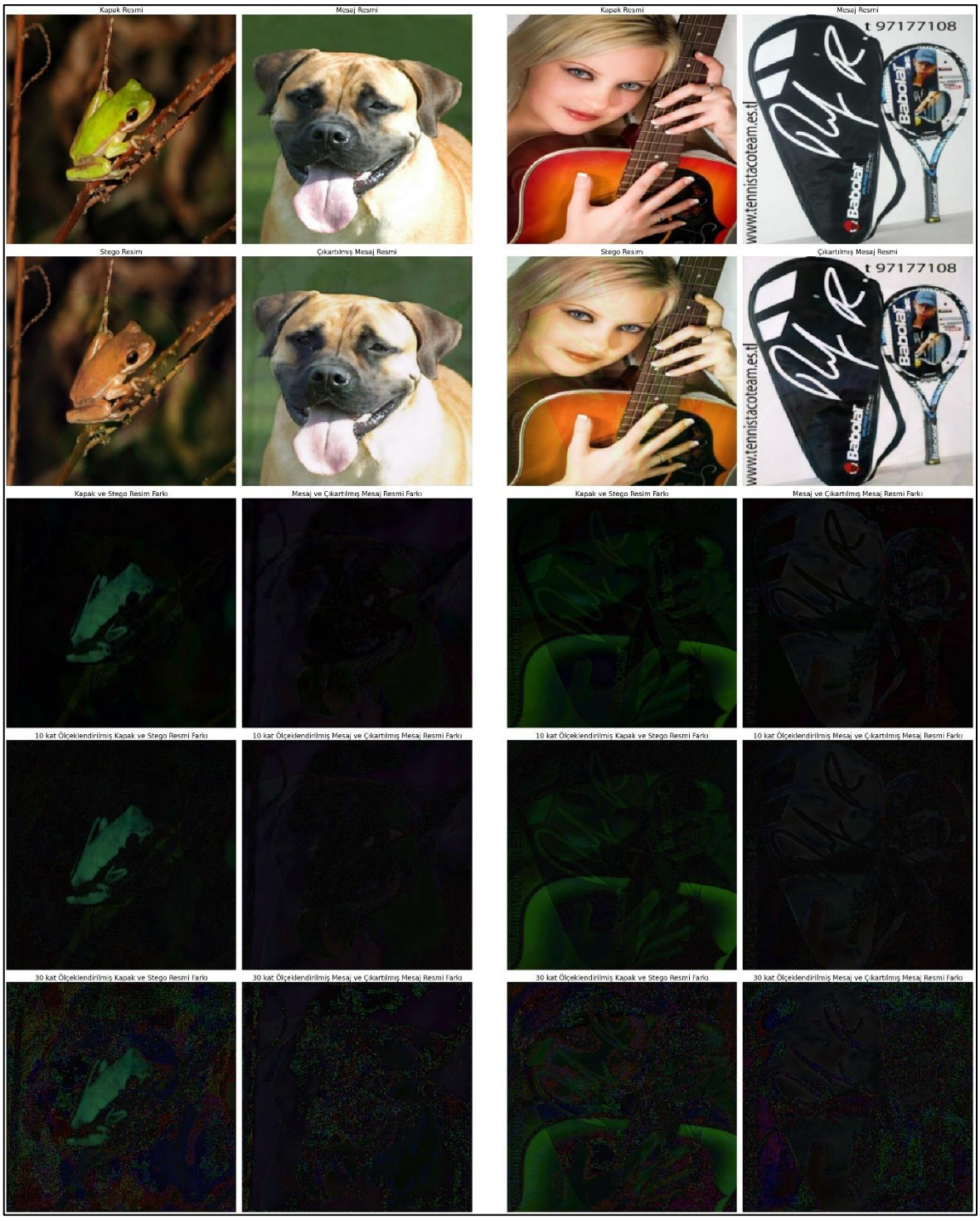


Şekil 3.28. Linnaeus 5 veritabanı için görsel sonuçlar (100 devir).

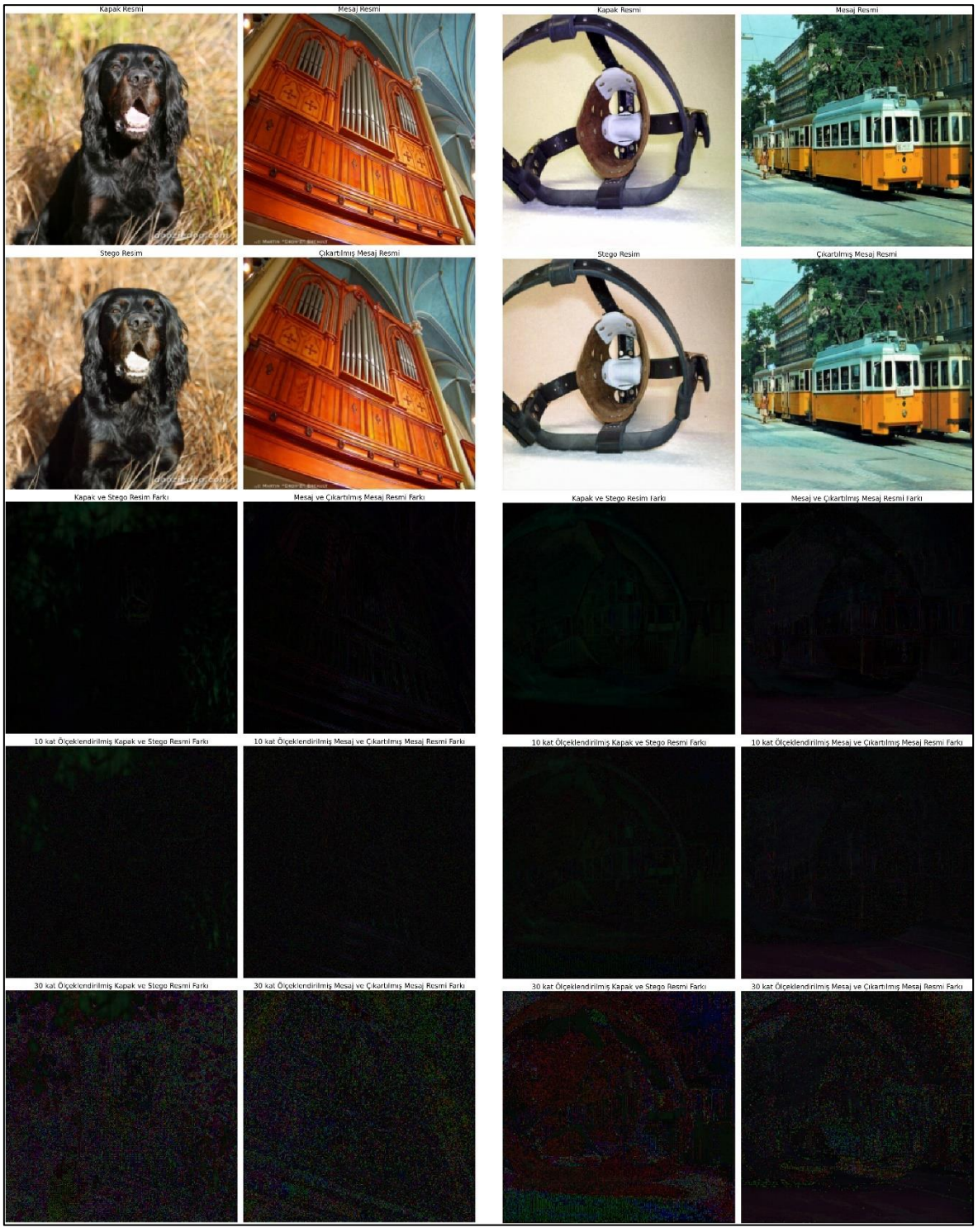


Şekil 3.29. Linnaeus 5 veritabanı için görsel sonuçlar (200 devir).

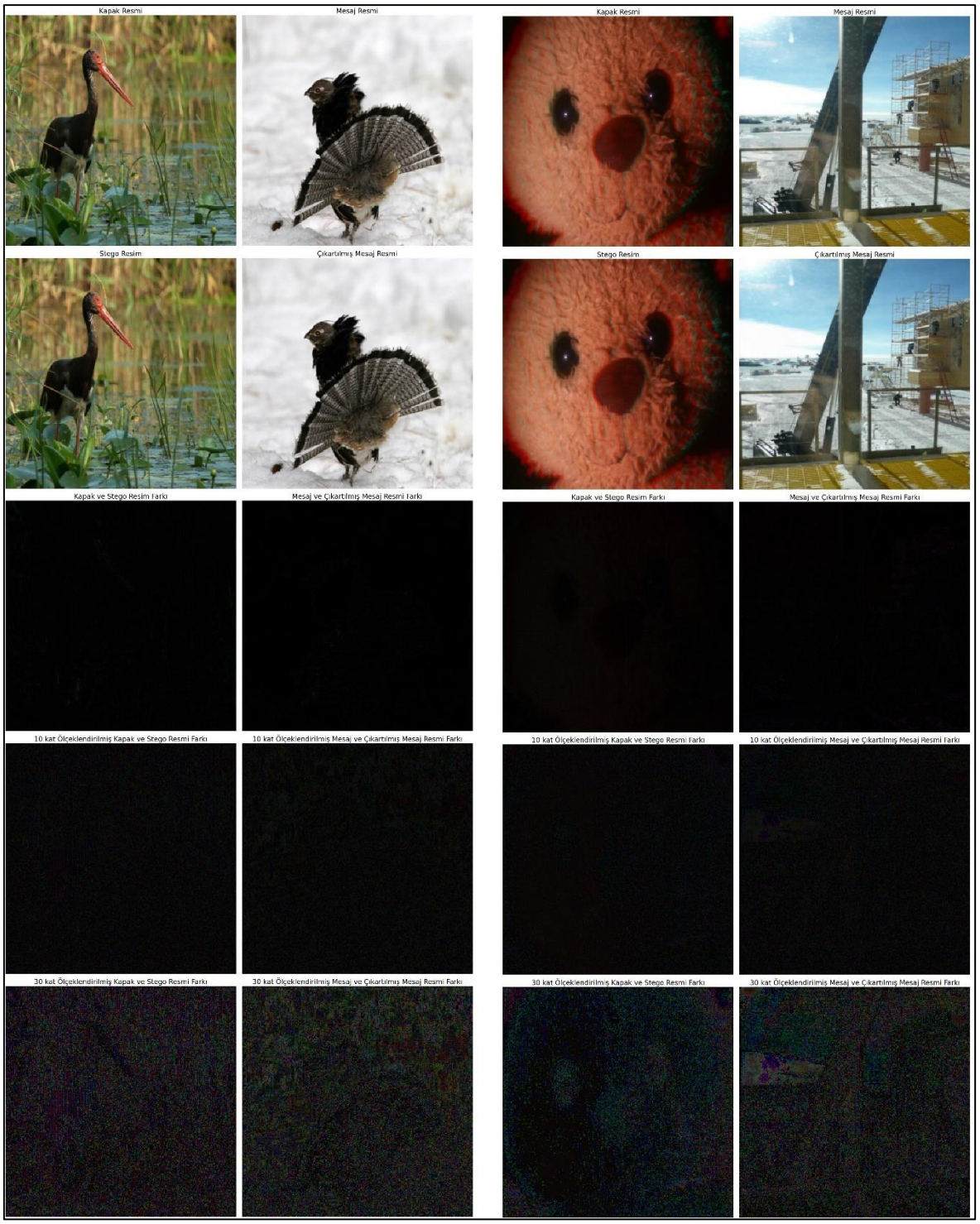
Şekil 3.30-3.32'de ImageNet veri tabanına ilişkin farklı devir sayılarındaki kapak-stego, mesaj-çıkartılmış mesaj görüntüleri ve ayrıca bunlara ilişkin fark görselleri sunulmuştur.



Şekil 3.30. ImageNet veritabanı için görsel sonuçlar (50 devir).

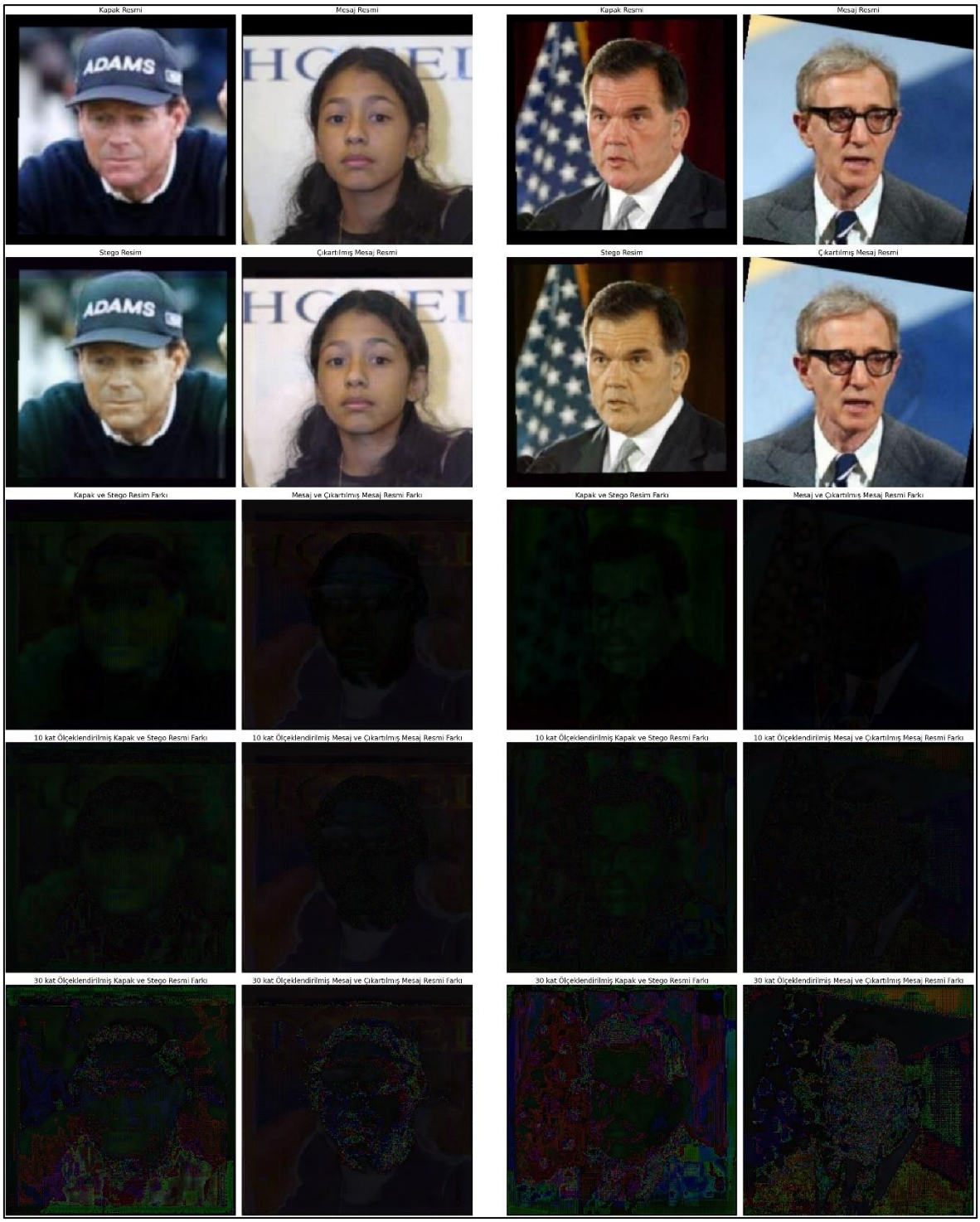


Şekil 3.31. ImageNet veritabanı için görsel sonuçlar (100 devir).

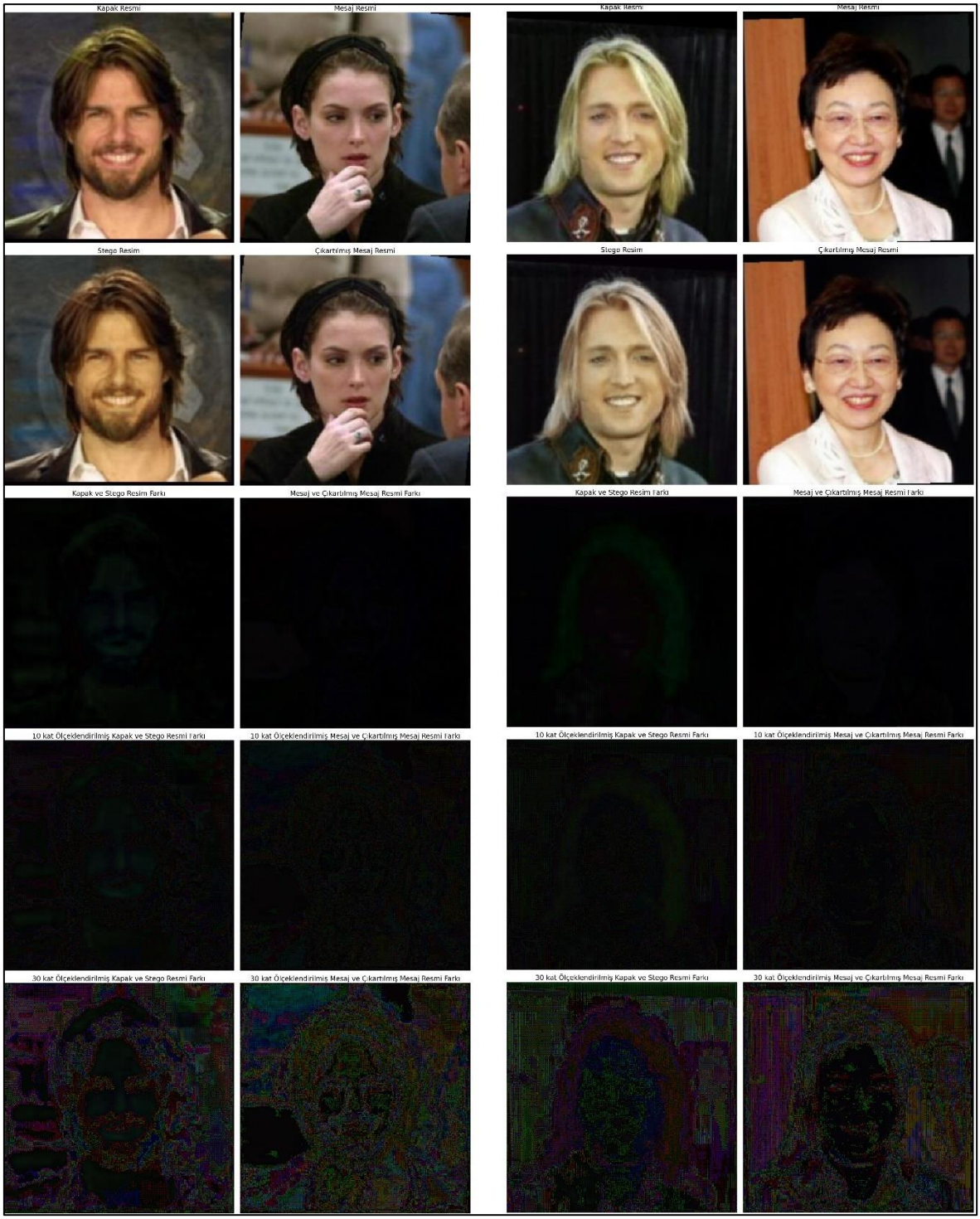


Şekil 3.32. ImageNet veritabanı için görsel sonuçlar (200 devir).

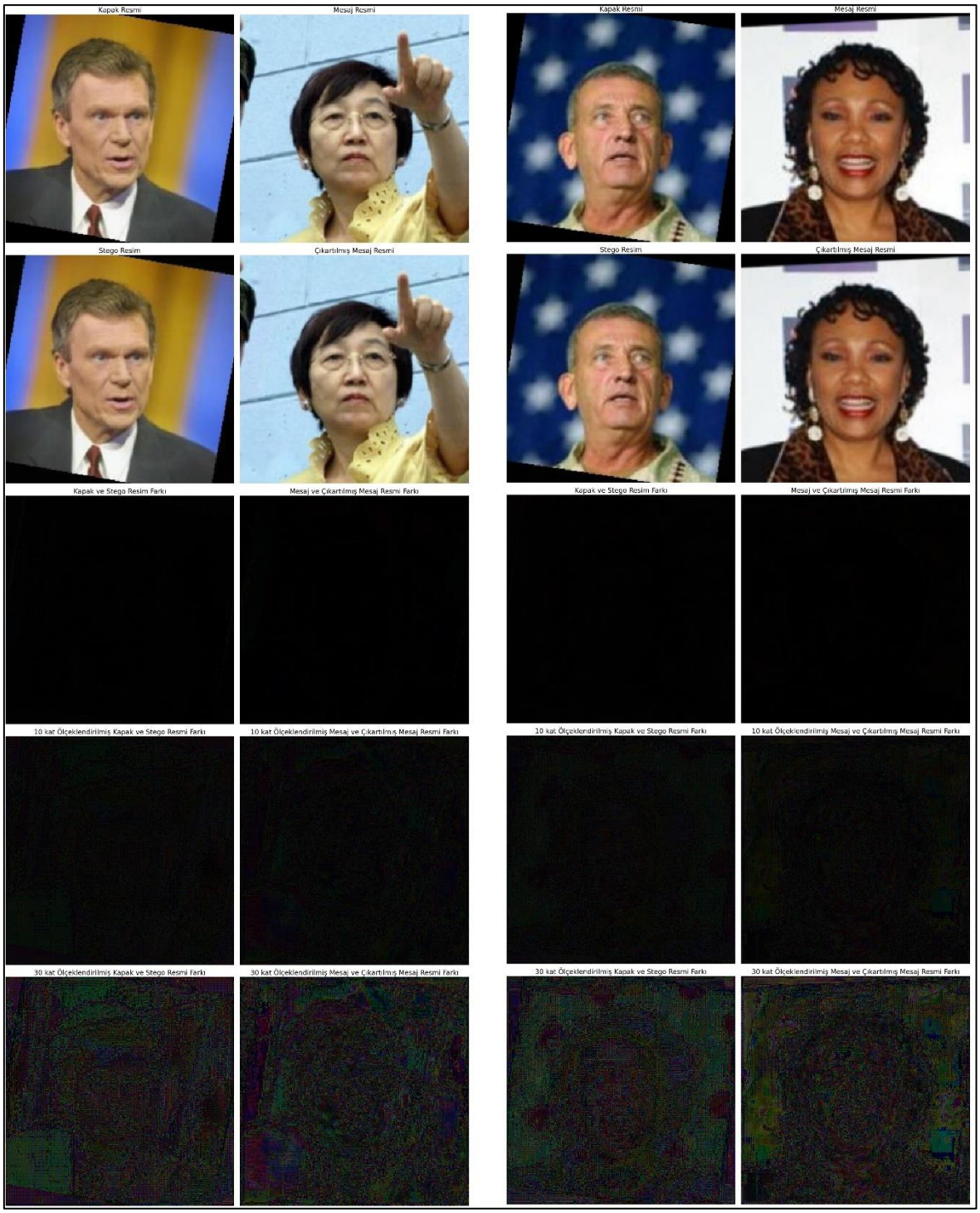
LFW veri tabanına ilişkin farklı devir sayılarındaki kapak-stego, mesaj-çıkartılmış mesaj görüntüleri ve ayrıca bunlara ilişkin fark görselleri Şekil 3.33-3.35'de verilmektedir.



Şekil 3.33. LFW veritabanı için görsel sonuçlar (50 devir).



Şekil 3.34. LFW veritabanı için görsel sonuçlar (100 devir).



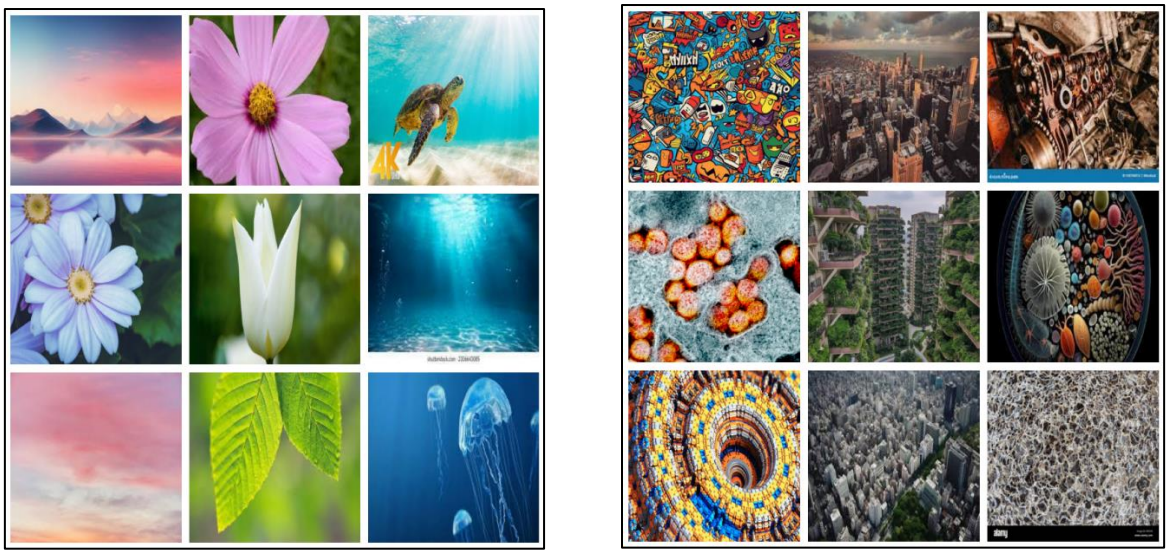
Şekil 3.35. LFW veritabanı için görsel sonuçlar (200 devir).

Sonuçlar incelendiğinde, modelin eğitim sürecince devir sayısının artışı ile performansının önemli ölçüde geliştiği gözlemlenmektedir. Her bir devir, modelin eğitim veri setini bir kez daha işlemesi ve öğrenme sürecini tekrarlaması anlamına gelir. Bu tekrarlamalar, modelin ağırlıklarının daha doğru bir şekilde ayarlanmasını sağlar, böylece

model, girdi verilerinin karmaşık özelliklerini daha iyi anlar ve tahminlerini buna göre optimize eder.

3.8. Kapak Görüntülerinin Karmaşıklık Düzeyine Optimum Kapak Resmi Olarak Belirlenmesi

Tez çalışmasının bu aşamasında, görsel algıya dayanarak karmaşık yapılı ve daha düz yapılı 100'er adet resim seçilmiştir. Seçilen bu karmaşık yapılı ve düz yapılı resimlere ilişkin örnek görseller Şekil 3.36'da yer almaktadır.



(a) (b)

Şekil 3.36. Düz ve karmaşık yapılı resim örnekleri. a) düz yapılı görüntüler, b) karmaşık yapılı görüntüler.

Şekil 3.36'da örnekleri verilen resimler öznel olarak seçildiğinden gerçek nesnel karmaşıklık düzeylerini de belirleyebilmek için ilgili resim klasörlerlerinin ortalama olarak entropi, kenar yoğunluğu (edge density), renk çeşitliliği (color diversity), doku özellikleri (texture features) ve kontrast parametreleri ölçülmüştür.

Entropi, bir görüntünün içerdiği bilgi miktarını ve görsel karmaşıklığını ölçen bir metriktir. Bu değer, görüntüdeki piksellerin dağılımının ne kadar rastgele ve öngörülemez olduğunu gösterir. Entropi değeri yüksek olan bir görüntü, daha fazla bilgi içerir ve genellikle daha karmaşık yapıya sahiptir.

Kenar yoğunluğu, görüntüdeki kenar piksellerinin oranını ifade eden bir metriktir. Bir görüntüdeki keskin geçişler ve çizgiler, kenar olarak tanımlanır ve bu kenarların toplam

piksel sayısına oranı, kenar yoğunluğunu verir. Yüksek kenar yoğunluğuna sahip bir görüntü, daha fazla detay ve doku içermektedir.

Renk yoğunluğu, görüntü içerisindeki farklı renk tonlarının sayısını ve dağılımını olarak ölçen bir parametredir.

Doku özellikleri, bir görüntünün yüzey özelliklerini ve yapısal bilgisini ifade eder. Doku analizi, görüntüdeki desenlerin, düzenliliğin veya düzensizliklerin ölçülmesini içerir. Görüntüdeki doku, farklı yoğunluklar, renkler veya parlaklık seviyeleri arasındaki lokal değişimlerle tanımlanabilir.

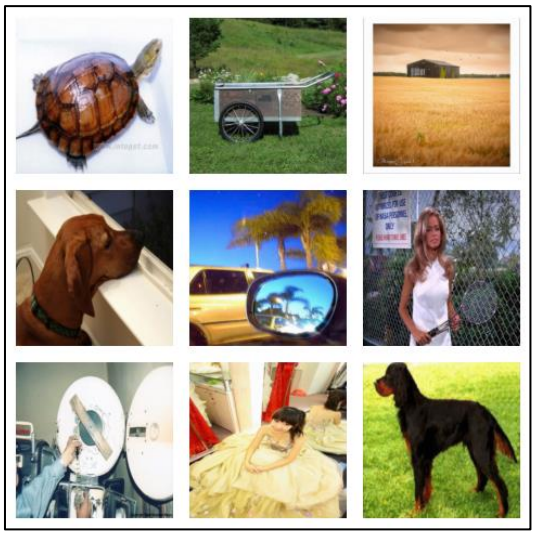
Kontrast, bir görüntüdeki en karanlık ve en parlak bölgeler arasındaki farkı ifade etmektedir. Yüksek kontrast, daha belirgin renk veya yoğunluk geçişlerini barındıran görüntüler anlamına gelirken düşük kontrast, renklerin veya tonların birbirine daha yakın olduğu, daha az belirgin geçişlerle karakterize edilen görüntüler anlamına gelmektedir.

Tablo 3.16'da düz yapılı ve karmaşık yapılı görüntü sınıflarının bahsedilen parametreler ile nesnel ölçüm sonuçları verilmiştir.

Tablo 3.16. Düz yapılı resimler ile karmaşık yapılı resimlerin nesnel ölçüm sonuçları

Metrik	**Düz Yapılı Resimler İçin Ortalama Değer**	**Karmaşık Yapılı Resimler için Ortalama Değer**
Entropi	7,25	7,72
Kenar Yoğunluğu	0,13	0,29
Renk Yoğunluğu	28.437	48.975
Doku Özellikleri	5,64	6,15
Kontrast	0,19	0,26

Tablo 3.16'da yer alan sonuçlar incelendiğinde nesnel metrik ölçüm sonuçlarıyla öznel olarak oluşturulmuş karmaşık yapılı ve düz yapılı görsellerin tutarlı sonuçlar verdiği görülmektedir. Karmaşıklık seviyelerine göre oluşturulmuş bu iki görüntü klasörü kapak resimleri olarak kullanılmış ve her iki klasördeki görüntülere de ImageNet veri tabanından rastgele seçilmiş aynı mesaj resimleri gizlenmiştir. Şekil 3.37'de toplamda 50 adet olarak uygulanan mesaj görüntülerinden örnekler yer almaktadır.



Şekil 3.37. Mesaj resmi örnekleri.

Tablo 3.17. Düz yapılı resimler için ortalama PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
43,9412	43,8071	0,9854	0,9841

Tablo 3.18. Karmaşık yapılı resimler için ortalama PSNR ve SSIM değerleri

Stego-Kapak PSNR (dB)	Çıkartılmış Mesaj-Mesaj PSNR(dB)	Stego-Kapak SSIM	Çıkartılmış Mesaj-Mesaj SSIM
45,7264	42,9113	0,9935	0,9807

Tablo 3.17 ve 3.18'deki metrik sonuçlarının detaylı incelenmesi, tez çalışmasında ele alınan modelin, kapak resminin karmaşık veya düz yapısından bağımsız olarak, steganografi uygulamalarında tutarlı ve yüksek kalitede sonuçlar elde ettiğini göstermektedir.

Ancak gizleme aşaması özelinde karmaşık resimlerde çıkarma aşamasında ise daha düz yapılı resimlerde daha yüksek PSNR ve SSIM sonuçlarının elde edilmesi şu şekilde yorumlanabilir:

Gizleme sürecinde karmaşık yapılı kapak resimlerinde daha düz yapıya sahip kapak resimlerine göre daha yüksek PSNR ve SSIM değerlerinin elde edilmesi, karmaşık yapılı kapak resimlerinin zengin doku ve desen özellikleri sayesinde gizli verinin varlığını daha etkili bir şekilde maskeleyebilmesiyle açıklanabilir. Karmaşık bir resimde gizli bilgi eklemek, resmin algılanan kalitesini ve yapısal bütünlüğünü korurken gizliliği sağlamak için daha fazla alan sunmaktadır. Dolayısıyla, mesaj resminin kapak resmine gizlenmesi sırasında oluşan hata miktarı azalmaktadır.

Öte yandan, çıkarma aşamasının daha az karmaşık hale gelmesi ve bu durumun da çıkarılan mesaj resminin orijinal mesaj resmine olan sadakatini artırması nedeniyle düz yapılı resimlerde karmaşık yapılı görüntülere göre daha yüksek PSNR ve SSIM değerleri elde edildiği değerlendirilmektedir. Çıkarma sürecinde steganografi algoritmasının gizli resmi, kapak resminin diğer ögelerinden ayırt etmesi gereken karmaşık desenler veya doku farklılıkları daha azdır. Bu, çıkarma algoritmasının daha az hata ile çalışmasını sağlar, çünkü potansiyel olarak yanıltıcı arka plan özelliklerini filtrelemek zorunda kalmaz. Böylece daha homojen bir arka plan, steganografi algoritmalarının çıkarma sürecinde gizli veriyi daha doğru bir şekilde tanımlamasına ve böylece orijinal mesajın bütünlüğünü korumasına imkan tanımaktadır.

Bu çerçevede, iletişim ortamında stego resmin algılanamazlık düzeyi kritik öneme sahip olduğunda, karmaşık kapak resimlerinin tercih edilebileceği değerlendirilebilir. Bu senaryolarda, çıkarma aşamasında mesaj resminde gözlemlenen hafif bozulmalar kabul edilebilir düzeyde kalırken, gizliliğin korunması öncelikli hedef haline gelmektedir. Ancak, çıkarma aşamasında mümkün olan en düşük bozulmayı hedefleyen ve orijinal mesajın sadakatini en üst seviyede tutmayı amaçlayan senaryolarda, düz yapılı kapak resimlerinin kullanımının avantaj sağlayacağı değerlendirilmektedir.

Ancak tez aşamasında geliştirilen model özelinde hem karmaşık hem de düz yapılı kapak resimleri ile oldukça yüksek metrik sonuçları alındığından, optimum kapak resmi seçimi konusunda katı bir ayrım yapılmasına gerek olmadığı söylenebilmektedir. Model hem karmaşık yapılı hem de düz yapılı kapak resimleri ile rahatlıkla çalışılabilmektedir. Bunun bir nedeni de modelin ImageNet gibi geniş ve çeşitli görüntüler içeren bir veri tabanı ile eğitilmesidir. Modelin, LFW gibi daha homojen bir yapı çeşitliliğine sahip bir veri tabanı ile eğitilmiş olması durumunda, belirli türdeki kapak resimlerine özelleşmiş performans sergilemesinin olası olabileceği değerlendirilmektedir.

4. TARTIŞMA VE YORUM

Tez çalışması kapsamında, 256x256x3 boyutlarında bir mesaj resmini aynı boyutta bir kapak resminin içine gizlemek ve tekrar çıkarmak üzere U-net tabanlı steganografi modeli geliştirilmiştir. Model, ImageNet veri tabanı kullanılarak eğitilmiştir. Doğrulama aşamasında iki farklı analiz gerçekleştirilmiştir.

İlk analiz, steganografi süreci sırasında farklı orijinal boyutlardaki gizli resimlerin kapak resmi üzerindeki etkisini incelemek üzerinedir. Bu aşamada, farklı boyutlarda (32x32, 64x64, 128x128, 256x256) kategorize edilmiş renkli görüntüler içerdiğinden Linnaeus 5 veri tabanı kullanılmıştır. 256x256 boyutundan daha küçük ölçekli resimler, mimarinin girişine uyumlu şekilde yeniden boyutlandırılmış, 256x256 boyutunda renkli kapak resimlerinin içine gizlenmiştir ve ardından tekrar çıkarılarak PSNR ve SSIM sonuçları incelenmiştir. Elde edilen sonuçlar, en yüksek PSNR ve SSIM değerlerinin orijinal boyutu 32x32x3 olan mesaj resimlerinden elde edildiğini mesaj görüntülerinin boyutu arttıkça PSNR ve SSIM değerlerinin azaldığını göstermektedir. Küçük boyutlu görüntülerin interpolasyon yoluyla büyütülmesi, yumuşatma etkisi yaratarak steganografi için daha uygun bir temel sağlamaktadır. Böylece yüksek frekanslı bileşenler azalır ve süreç yüksek PSNR ve SSIM değerleri ile sonuçlanır. Diğer yandan, yüksek çözünürlüklü orijinal görüntüler, daha fazla detay ve piksel başına yoğun bilgi içerdiklerinden, steganografik süreçte daha düşük PSNR ve SSIM değerleriyle sonuçlanmıştır. Ancak sonuç itibariyle tüm farklı orijinal görüntü boyutları için elde edilen ölçüm sonuçları literatür standartlarının üzerindedir.

İkinci analiz kapsamında, hem modelin çeşitli veri tabanları üzerindeki çalışma performansını görmek hem de literatürde yer alan diğer çalışmalarla daha etkin kıyaslama yapabilmek adına Linnaeus 5 veri tabanına ek olarak literatürde yaygın olarak kullanılan ImageNet ve LFW veri tabanları ile de model test edilmiştir. Tablo 4.1'de literatürde yer alan diğer U-Net steganografi çalışmaları ile elde edilen kapasite, PSNR ve SSIM sonuçları ile tez çalışması kapsamında elde edilen sonuçlar yer almaktadır. Ayrıca tabloda diğer derin öğrenme yöntemlerini kullanan ve bu alanda çoğu yayında kaynak olarak gösterilen bazı yayınların metrik sonuçlarına da yer verilmiştir

Tablo 4.1. Literatürde yer alan diğer çalışmalarla yük, PSNR ve SSIM değerleri karşılaştırması

Referans Çalışma	**Gizleme Ağı**	**Çıkarma Ağı**	**Yük**	**Devir Sayısı**	**Eğitim/Test Veri Tabanı ve Eğitim/Test Görüntüsü Sayısı**	**Sonuçların Alındığı Test Veri Tabanı**	**Stego-Kapak PSNR (dB)**	**Çıkartılmış Mesaj-Mesaj PSNR(dB)**	**Stego-Kapak SSIM**	**Çıkartılmış Mesaj-Mesaj SSIM**
Rehman [29]	CNN	CNN	%33	150	Eğitim Veri Tabanı ImageNet-6.000 Test Veri Tabanı ImageNet-2.000 PASCAL VOC12-1.000 LFW-1.000	ImageNet	32,9	36,6	0,96	0,96
						PASCAL-VOC12	33,7	35,9	0,96	0,95
						LFW	33,7	39,9	0,95	0,96
Baluja [30]	CNN	CNN	%100	-	Eğitim/Test Veri Tabanı ImageNet Corel Veri Tabanı İnternetten rastgele seçilmiş görseller (Toplam 2.650.000 görüntü)	ImageNet Corel Veri Tabanı İnternetten rastgele seçilmiş görseller	41,2	37,6	0,98	0,97
Zhang [31]	ISGAN	ISGAN	%33	-	Eğitim Veri Tabanı ImageNet-50.000 PASCAL-VOC12-16.000 LWF-10.000 Test Veri Tabanı ImageNet-30.000 PASCAL VOC12-5.000 LWF-3.000	ImageNet	34,89	33,42	0,9681	0,9474
						PASCAL-VOC12	34,49	33,31	0,9661	0,9467
						LFW	34,63	33,63	0,9573	0,9429
Subramanian [32]	Encoder	Decoder	%100	5	Eğitim Veri Tabanı ImageNet, COCO ve CelebA veri tabanlarından toplam 45.000 adet Test Veri Tabanı ImageNet, COCO ve CelebA veri tabanlarından toplam 5.000 adet	ImageNet	34,55	27,93	-	-
						COCO	31,96	27,90	-	-
						CelebA	32,26	27,92	-	-

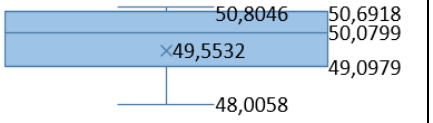
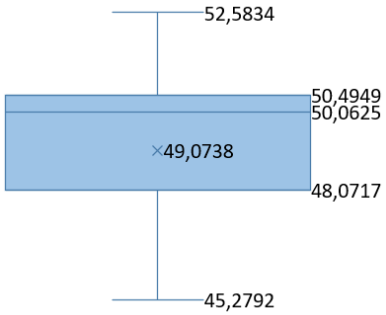
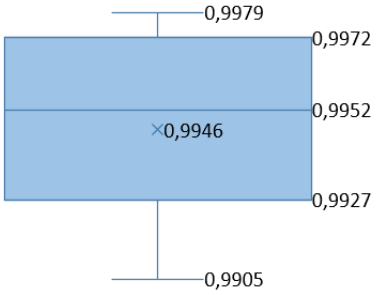
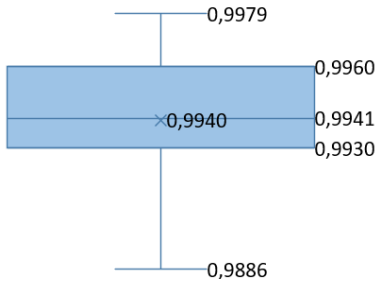
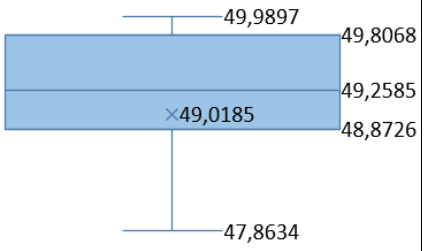
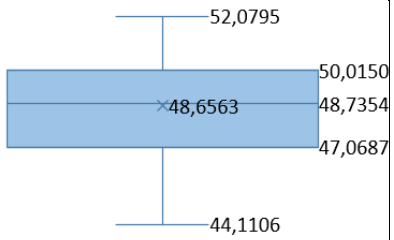
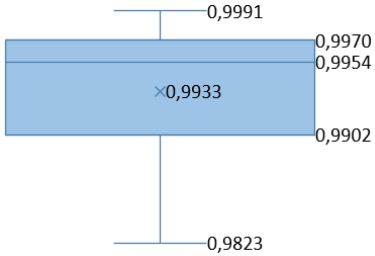
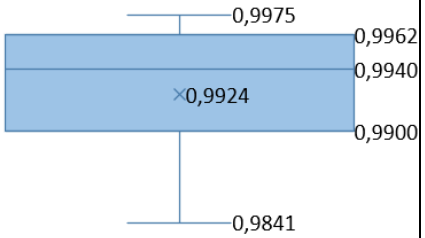
Liu [33]	U-Net	CNN	%33	2000	Eğitim Veri Tabanı ImageNet ve PASCAL-VOC12 veri tabanlarından toplam 60.000 adet Test Veri Tabanı ImageNet ve PASCAL-VOC12 veri tabanlarından toplam 7.000 adet	ImageNet PASCAL-VOC12	39,7708	43,3571	0,9828	0,9862
Liu [34]	U-Net	U-Net	%33	1000	Eğitim Veri Tabanı ImageNet ve PASCAL-VOC12 veri tabanlarından toplam 40.000 adet Test Veri Tabanı ImageNet ve PASCAL-VOC12 veri tabanlarından toplam 6.000 adet	ImageNet PASCAL-VOC12	40,8965	49,6028	0,9813	0,9963
Duan [35]	U-Net	CNN	%100	200	Eğitim Veri Tabanı ImageNet- 45.000 Test Veri Tabanı ImageNet-5.000	ImageNet	40,4716	40,6665	0,9794	0,9842
Himthani [36]	U-Net	CNN	%100	-	Eğitim Veri Tabanı LFW ve Know Your Data veri tabanlarından toplam 6.616 adet Test Veri Tabanı LFW ve Know Your Data veri tabanlarından toplam 250 adet	LFW Know Your Data	38,00	38,00	0,9875	0,9869
	V-Net						30,00	33,00	0,9680	0,9810
	U-Net++						24,00	27,00	0,910	0,930
Zeng [37]	U-Net	U-Net	%33	50	Eğitim Veri Tabanı LFW-13.232 PASCAL-VOC12- 11.540 Test Veri Tabanı LFW-5.000 PASCAL-VOC12- 5.000	LFW	39,3912	35,8427	0,9894	0,9833

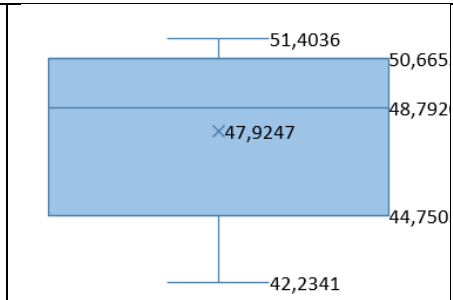
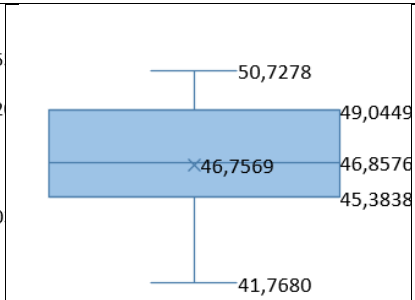
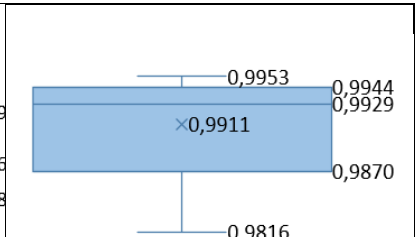
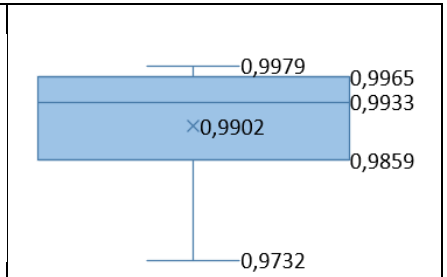
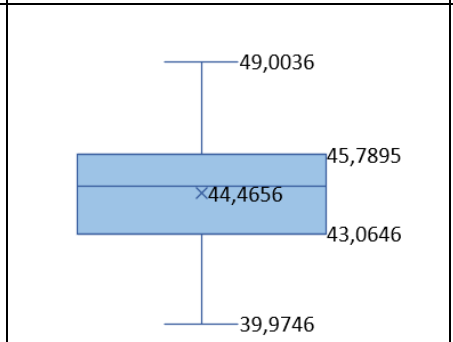
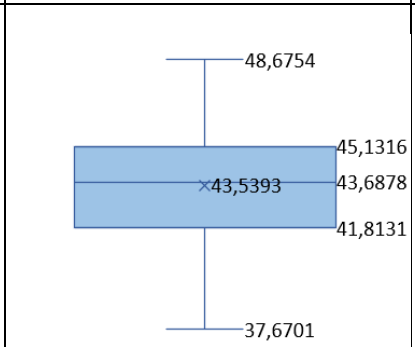
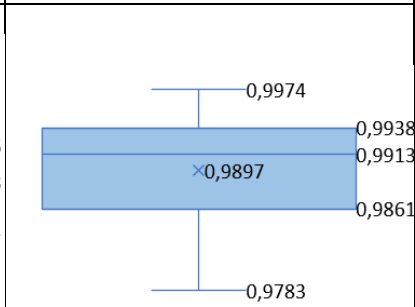
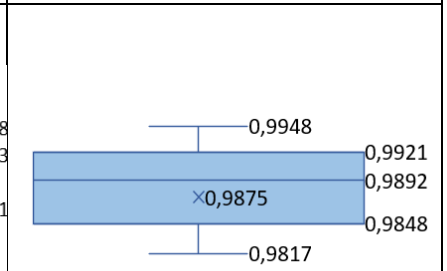
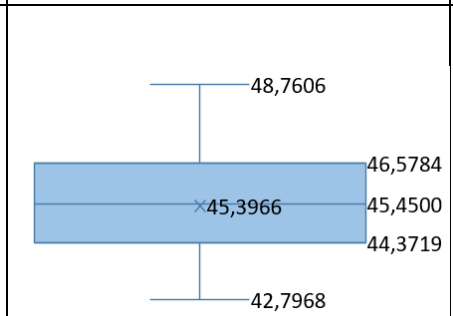
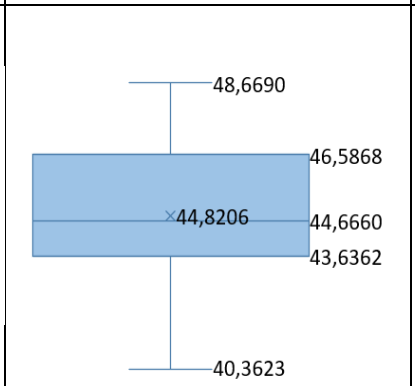
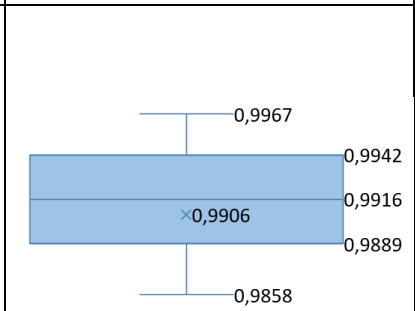
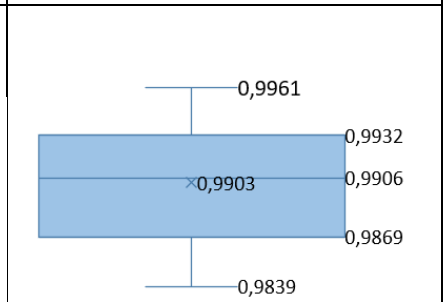
Wang [38]	U-Net++	CNN	%33	200	Eğitim Veri Tabanı ImageNet- 45.000 LFW-10.000 Test Veri Tabanı ImageNet- 5.000 LFW-3.232	ImageNet	37,1381	35,4812	0,9768	0,9681
						LFW	37,5614	35,4321	0,9821	0,9743
Wei [39]	U-Net	CNN	%100	200	Eğitim Veri Tabanı ImageNet- 40.000 Test Veri Tabanı ImageNet- 2.000	ImageNet	36,96	35,98	0,970	0,963
Jenynof [40]	U-Net	U-Net	%100	100	Eğitim Veri Tabanı CIFAR10- 50.000 StanfordCars-8144 STL10-500 Test Veri Tabanı CIFAR10- 10.000 StanfordCars-8041 STL10-800	CIFAR10	27,663	27,552	-	-
						StanfordCars	23,171	23,531	-	-
						STL10	28,226	28,767	-	-
Kich [41]	U-Net	CNN	%100	>150	Eğitim Veri Tabanı ImageNet LFW PASCAL-VOC12 Test Veri Tabanı ImageNet-5.000 LFW-5.000 PASCAL-VOC12-5.000	ImageNet	37,83	31,77	0,9786	0,9077
						LFW	40,03	33,13	0,9797	0,9280
						PASCAL-VOC12	37,40	30,80	0,9790	0,9094
Önerilen Model	**U-Net**	**U-Net**	**%100**	**200**	**Eğitim Veri Tabanı** **ImageNet-70.000** **Test Veri Tabanı** **Linnaeus 5- 1.600** **ImageNet-2.000** **LFW-2.000**	**Linnaeus 5**	**44,4656**	**43,5393**	**0,9897**	**0,9875**
						ImageNet	**45,3966**	**44,8206**	**0,9906**	**0,9903**
						LFW	**48,1407**	**47,5296**	**0,9930**	**0,9907**

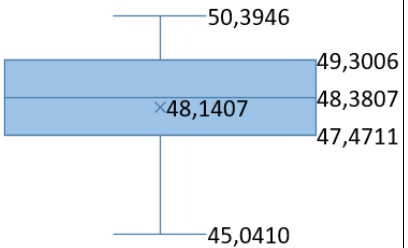
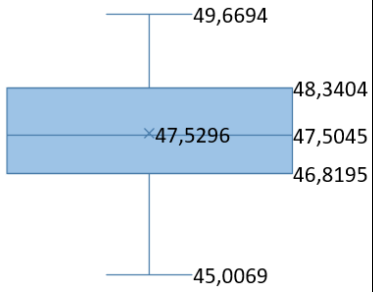
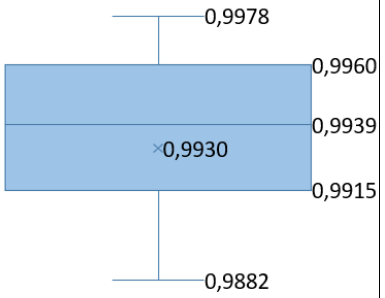
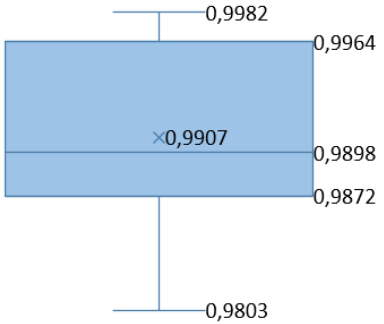
Tablo 4.1’de, yük miktarı %33 olarak belirtilen çalışmalar, gizli resim olarak 256x256 boyutlarında gri ölçekli resimleri, yük miktarı %100 olarak belirtilen çalışmalar, mesaj resimleri olarak 256x256 boyutlarında renkli resimleri kullanmıştır. Sonuçlar incelendiğinde, tez çalışması sonucunda 3 veri tabanı için de elde edilen PSNR ve SSIM değerlerinin aynı yük miktarına sahip diğer çalışmalarda elde edilen PSNR ve SSIM değerlerinden yüksek olduğu görülmektedir. Bu sonuç mimaride kullanılan artık bloklar, AdamW algoritmasıyla birlikte kullanılan tek döngü öğrenme oranı planlayıcısı ve diğer kullanılan hiper parametrelerin etkisini yansıtmaktadır.

Tablo 4.2’de yer alan kutu grafikleri tez çalışması kapsamında incelenen her adım için PSNR ve SSIM metriklerinin veri dağılımının özetini görsel olarak sunmak amacıyla verilmiştir.

Tablo 4.2. PSNR ve SSIM değerlerine ilişkin kutu grafikleri

Database	Stego-Cover PSNR	Extracted-Message PSNR	Stego-Cover SSIM	Extracted-Message SSIM
Linnaeus 5 (mesaj resim 32x32)				
Linnaeus 5 (mesaj resim 64x64)				

Linnaeus 5 (mesaj resim 128x128)				
Linnaeus 5 (mesaj resim 256x256)				
ImageNet				

LFW	 50,3946 49,3006 48,3807 48,1407 47,4711 45,0410	 49,6694 48,3404 47,5296 47,5045 46,8195 45,0069	 0,9978 0,9960 0,9939 0,9930 0,9915 0,9882	 0,9982 0,9964 0,9907 0,9898 0,9872 0,9803

Kutu grafiklerde üst çizgi aykırı değerler haricinde alınan en büyük değeri göstermektedir. Kutunun üst kenarı ile maksimum değer arasındaki kısım, verilerin %25'lik kısmını temsil etmektedir. Aynı şekilde alt çizgi aykırı değerler haricinde alınan en küçük değeri, kutunun alt kenarı ile minimum değer arasındaki kısım ise verilerin diğer %25'lik kısmını temsil etmektedir. Kutunun ortasındaki çizgi veriler küçükten büyüğe sıralandığında ortada kalan değeri, "x" ile işaretlenerek belirtilen değer ise ortalama değeri göstermektedir. Tablo 4.2'de yer alan sonuçlar Tablo 4.1'de gösterilen ortalama PSNR ve SSIM değerlerine ek olarak maksimum ve minimum değerlerin yanı sıra genel varyansı da dahil ederek daha detaylı bir içerik vermektedir. Böylece, çeşitli veri kümeleri ve koşullar genelinde steganografik sürecin gizleme ve çıkarma kalitesinin tutarlılığının anlaşılmasına fayda sağlamaktadır.

Ek olarak, kapak görüntülerinin karmaşıklık seviyelerine göre sınıflandırılması yapılarak, bu iki farklı kategori altında aynı gizli görüntülerin gizlenme ve çıkarılması sonucunda elde edilen metrik sonuçlar incelenmiş ve modelin, hem karmaşık hem de düz yapılı kapak resimleri için yüksek metrik sonuçları verdiği görülmüştür.

5. SONUÇ

Tez çalışması kapsamında, artık blok destekli U-Net mimarisi kullanılarak 256x256 boyutlarındaki renkli mesaj görüntülerinin aynı boyutlardaki kapak görüntülerine etkili bir şekilde gizlenmesi ve kapak görüntülerinden tekrar çıkarılması işlemleri gerçekleştirilmiştir. Ayrıca çeşitli veri setleri ve görüntü boyutlarının mimari sonuçları üzerindeki etkileri ayrıntılı olarak değerlendirilmiştir. Bu çerçevede gerçekleştirilen çalışmalar aşağıdaki şekilde özetlenebilir:

1) Linnaeus 5 veri seti kullanılarak farklı boyutlardaki renkli mesaj görüntülerinin kapak görüntülerine gizlenmesi işlemi gerçekleştirilmiştir. Böylece farklı boyutlara sahip gizli resimlerin steganografik süreç üzerindeki etkisi analiz edilmiştir. Araştırma bulguları, orijinal mesaj görüntülerinin boyutları ile elde edilen PSNR ve SSIM metrikleri arasında bir korelasyon olduğunu göstermektedir. Elde edilen sonuçlar, en yüksek PSNR ve SSIM değerlerinin orijinal boyutu 32x32x3 olan mesaj resimlerinden elde edildiğini mesaj görüntülerinin boyutu arttıkça PSNR ve SSIM değerlerinin azaldığını göstermektedir.
2) Tek döngü öğrenme oranı planlayıcısının AdamW optimizasyon algoritması ile birlikte kullanılmasının ölçüm sonuçları üzerinde sağladığı iyileşme metriksel sonuçlarla sunulmuştur. Tek döngü öğrenme oranı planlayıcısının AdamW optimizasyon algoritması ile birlikte kullanılmasıyla, sadece AdamW kullanılarak elde edilen sonuçlara göre PSNR değerinde stego-kapak resimleri için %21,45 ve çıkartılmış mesaj-mesaj resimleri için %30,90, SSIM değerlerinde ise sırasıyla %2,67 ve %3,28 oranında iyileşme kaydedilmiştir.
3) Modelin ImageNet ve LFW veri setleri gibi farklı karakteristik özelliklere sahip görüntülerle genelleştirme yeteneği başarılı bir şekilde test edilmiştir. Kapsamlı literatür taramasından elde edilen mevcut bilgiler çerçevesinde, modelin Linnaeus 5, ImageNet ve LFW veri tabanlarının üçünde de test edilmesi sonucu elde edilen görsel ve metriksel sonuçlara göre, literatürdeki mevcut derin öğrenme algoritmalarına kıyasla PSNR ve SSIM metrikleri açısından umut verici sonuçlar elde edildiği değerlendirilmektedir.
4) Model performansının farklı devir sayılarına göre değerlendirilmesi yapılmış ve devir sayısı arttıkça elde edilen iyileşme görsel sonuçlarla sunulmuştur.

5) Kapak görüntülerinin karmaşıklık düzeyine göre optimum kapak resmi olarak belirlenmesi konusunda istatistiksel bir çıkarım yapılmıştır. Ayrıca modelin hem karmaşık hem de düz yapılı kapak resimlerinde etkin sonuçlar verdiği görülmüştür.

Sonuç olarak, tez çalışması kapsamında geliştirilen mimarinin, steganografik uygulamalarda resim kalitesini optimize etmedeki etkinliğinin açıkça görüldüğü, metriksel sonuçlar ve görsel doğruluk açısından umut verici sonuçlar elde edildiği ve bu alandaki gelecek araştırmalar için bir referans noktası oluşturduğu değerlendirilmektedir. Ayrıca modelin farklı karakteristiklere sahip görüntüler üzerindeki olumlu sonuçları, modelin çeşitli veri türleri ve koşullarına karşı genelleme yeteneğini ve çeşitli görsel içerikleri başarılı bir şekilde işleyebildiğini göstermektedir. Uygulama alanları açısından değerlendirildiğinde, modelin yüz görüntüleri de dahil olmak üzere gerçek dünya senaryolarında karşılaşılan çeşitli görüntü türlerine uyum sağlama ve bu durumlarda yüksek performans sergileme kapasitesinin olduğu ifade edilebilmektedir.

Bundan sonraki çalışmaların modelin hesaplama verimliliğini artıracak optimizasyon tekniklerinin araştırılması ve uygulanması üzerine olabileceği değerlendirilmektedir. Örneğin algoritmanın eğitim sürecini hızlandırmak için dağıtık hesaplama tekniklerinin kullanımı göz önünde bulundurulabilir. Bu yaklaşımın, hesaplama yükünü birden fazla işlemci veya sunucu arasında dağıtarak, toplam eğitim süresini azaltma konusunda faydalı olabileceği düşünülmektedir.

KAYNAKLAR

[1] B.A. Usha, N.K, Srinath, A. Nanjangud, A.M. Deshpande and A. Rebello, "A survey on patient information protection using cryptographic and data hiding techniques," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no.4, pp. 6334-6336, 2014.

[2] M.S. Nambakhsh, A., Ahmadian and H., Zaidi, "A contextual based double watermarking of PET images by patient ID and ECG signal,*"Computer Methods and Programs in Biomedicine,* vol.104, no.3, pp. 418-425, 2011.

[3] R. Karakış, "Epileptik MRG ve EEG verileri için bulanık mantık tabanlı steganografi uygulaması," Doktora Tezi, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı, Gazi Üniversitesi, Ankara, Türkiye, 2015.

[4] K. Joshi, R. Yadav and S. Allwadhi, "PSNR and MSE based investigation of LSB," *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT),* pp. 280-285, 2016. doi: 10.1109/ICCTICT.2016.7514593.

[5] E. Gedkhaw, N. Soodtoetong and M. Ketcham, "The performance of cover image steganography for hidden information within image file using least significant bit algorithm," *18th International Symposium on Communications and Information Technologies (ISCIT)*, pp. 504-508, 2018. doi: 10.1109/ISCIT.2018.8588011

[6] N. Razavı, "LSB steganografi yönteminde yüksek kapasiteli veri gizleme," Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi, Ankara, Türkiye, 2017.

[7] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9–10, pp. 1613–1626, 2003, doi: 10.1016/S0167-8655(02)00402-6

[8] G. Swain, "A steganographic method combining LSB substitution and PVD in a block," *Procedia Computer Science*, vol.85, pp. 39–44, doi:10.1016/j.procs.2016.05.174.

[9] Z. Ni, Y. Shi, N. Ansari and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006, doi: 10.1109/TCSVT.2006.869964.

[10] C. Qin, C.C. Chang, Y. H. Huang and L.T. Liao, "An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 7, pp. 1109-1118, 2013, doi: 10.1109/TCSVT.2012.2224052.

[11] H. Nyeem, "Reversible data hiding with image bit-plane slicing," *20th International Conference of Computer and Information Technology (ICCIT)*, pp. 1-6, 2017, doi: 10.1109/ICCITECHN.2017.8281763

[12] C.F. Lee, H.L. Chen and H.K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion,"*Journal of Systems and Software*, vol. 83, pp.1864–1872, 2010, doi: 10.1016/j.jss.2010.05.078

[13] C.C. Chang, Y.H. Huang and T.C. Lu, "A difference expansion based reversible information hiding scheme with high stego image visual quality," *Multimedia Tools and Applications*, vol. 76, pp. 12659–12681, 2017, doi: 10.1007/s11042- 016- 3689-3

[14] B.C. Nguyen, S.M. Yoon and H.K. Lee, "Multi bit plane image steganography," *Lecture Notes in Computer Science*, vol. 4283, pp. 61–70, 2006.

[15] M. Niimi, H. Noda, E. Kawaguchi and R.O. Eason , "High capacity and secure digital steganography to palette based images," *Proceedings of the IEEE International Conference on Image Processing*, pp. 917-920, 2002.

[16] S. Imaizumi and K. Ozawa, "Multibit embedding algorithm for steganography of palette-based images," *Lecture Notes in Computer Science*, vol. 8333, pp. 99–110, 2014, doi: 10. 1007/978- 3- 642- 53842- 1 _ 9

[17] S. Das, S. Sharma, S. Bakshi and I. Mukherjee, "A framework for pixel intensity modulation based image steganography," *Advances in Intelligent Systems and Computing*, vol. 563, pp. 3–14, 2018, doi: 10.1007/978- 981- 10- 6872- 0 _ 1

[18] A. Tiwari, S.R. Yadav and N.K. Mittal, “A review on different image steganography techniques,” *International Journal of Engineering and Innovative Technology (IJEIT),* vol.3 no.7, pp.121-124, 2014.

[19] D. Mehta and D. Bhatti, “Blind image steganography algorithm development which resistant against JPEG compression attack,” *Multimedia Tools and Applications*, vol.81 no.1, pp. 459–479, 2021.

[20] A. Melman and O. Evsutin, “Comparative study of metaheuristic optimization algorithms for image steganography based on discrete fourier transform domain,”*Applied Soft Computing*, vol.132, pp. 109847, 2023, doi: 10.1016/j.asoc.2022.109847

[21] A. Gutub and F. Al-Shaarani, “Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons,” *Arabian Journal for Science and Engineering*, vol. 45, no.4, pp. 2631–2644, 2020, doi:10.1007/s13369-020-04413-w

[22] T. Vanitha, A. Dsouza, B. Rashmi and S. Dsouza, “A review on steganography – least significant bit algorithm and discrete wavelet transform algorithm,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol.2, no.5, pp. 89-95, 2014.

[23] M.A. Ahmad, M. Elloumi, A.H. Samak, A. M. Al-Sharafi, A. Alqazzaz, M. A. Kaid and C. Iliopoulos, “Hiding patients medical reports using an enhanced wavelet steganography algorithm in DICOM images,” *Alexandria Engineering Journal*, vol. 61, no.12, pp. 10577–10592, 2022, doi:10.1016/j.aej.2022.03.056

[24] W. Luo, F. Huang and J. Huang, “ Edge adaptive image steganography based on LSB matching revisited,” *IEEE Transactions on Information Forensics and Security*, vol.5, no.2, pp. 201–214,2010, doi:10.1109/tifs.2010.2041812

[25] S. Chakraborty, A.S. Jalal and C. Bhatnagar, “LSB based non blind predictive edge adaptive image steganography,” *Multimedia Tools and Applications*, vol.76, no.6, pp. 7973–7987, 2017.

[26] T. Rabie and I. Kamel, "High capacity steganography: a global adaptive region discrete cosine transform approach," *Multimedia Tools and Applications*, vol. 76, pp. 6473–6493, 2017.

[27] R. Chen, S. Z. Zhu, J. F. Cui, G. S. Li, W. Li and K. S. Wu, "HVS and MBNS based steganography algorithm design and implementation," *10th International Conference on Computer Science & Education (ICCSE)*, pp. 703-706, 2015, doi: 10.1109/ICCSE.2015.7250336

[28] I.J. Kadhim, P. Premaratne, P.J. Vial, and B. Halloran, "Comprehensive survey of image steganography: techniques, evaluations, and trends in future research," *Neurocomputing*, pp. 299-326, 2019.

[29] A. U. Rehman, R.Rahim, M. S. Nadeem and S. U. Hussain, "End-to-end trained CNN encoder-decoder networks for image steganography," *Lecture Notes in Computer Science*, pp. 723-729, 2019.

[30] S. Baluja, "Hiding images within images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.42, no.7, pp. 1685–1697, 2020.

[31] R. Zhang, S. Dong and J. Liu, "Invisible steganography via generative adversarial networks", *Multimedia Tools and Applications,* 2018, doi: 10.1007/s11042-018-6951-z

[32] N. Subramanian, I. Cheheb, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "End-to-end image steganography using deep deconvolutional autoencoders," *IEEE Access*, vol.9, pp.135585-135593, 2021, doi: 10.1109/ACCESS.2021.3113953

[33] L. Liu, M. Lingzhuan, P. Yanjun, and W. Xiaoli, "A data hiding scheme based on U-Net and wavelet transform," *Knowledge Based Systems*, vol. 223, no. 107022, 2022 doi:10.1016/j.knosys.2021.107022

[34] L. Liu, M. Lingzhuan, Z. Weimin, P. Yanjun and W. Xiaoli, "A novel high-capacity ınformation hiding scheme based on improved U-Net,"*Security and Communication Networks*, pp.1–12, 2022, doi:10.1155/2022/4345494

[35] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang and C. Qin, "Reversible image steganography scheme based on a U-Net structure," *IEEE Access*, vol.7, pp.9314–9323, 2019, doi:10.1109/access.2019.2891247

[36] V. Himthani, V.S. Dhaka, M. Kaur, M.G. Oza and H.N. Lee, "Comparative performance assessment of deep learning based image steganography techniques," *Scientific Reports*, *Nature Portfolio*, 2022, doi:10.1038/s41598-022-17362-1

[37] L. Zeng, N. Yang, X. Li, A. Chen, H. Jing and J. Zhang, "Advanced image steganography using a U-Net based architecture with multi-scale fusion and perceptual loss," *Electronics*, vol.12, no.18, 2023, doi:10.3390/electronics12183808

[38] Z. Wang, "End-to-end image steganography scheme based on U-Net++ structure", *4th International Conference on Frontiers Technology of Information and Computer (ICFTIC)*, pp.1-6, 2022, doi: 10.1109/ICFTIC57696.2022.10075116

[39] B. Wei, X. Duan and H. Nam, "Image steganography with deep learning networks," *13th International Conference on Information and Communication Technology Convergence (ICTC)*, *IEEE,* pp. 1371-1374, 2022, doi:10.1109/ICTC55196.2022.9952432

[40] A. Jenynof and T. Ahmad, "Image to image steganography using U-Net architecture with mobilenet convolutional neural network," *14th International Conference on Computing Communication and Networking Technologies (ICCCNT) ,IEEE*, pp. 1-6. 2023, doi:10.1109/ICCCNT56998.2023.10306352

[41] I. Kich, A. El Bachir and T. Youssef, "CNN auto-encoder network using dilated inception for image steganography," *International Journal of Fuzzy Logic And Intelligent Systems*, vol.21, no. 4, pp. 358-368, 2021, doi: 10.5391/ijfis.2021.21.4.358

[42] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," *Signal Processing*, vol.90, pp. 727–752, 2010.

[43] S. B. Sasi and N. Sivanandam, “A survey on cryptography using optimization algorithms in WSNs,” *Indian Journal of Science and Technology*, vol. 8, pp. 216-221, 2015, doi: 10.17485/ijst/2015/v8i3/59585

[44] N. F. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen,” *Computer (Long. Beach. Calif)*, vol. 31, no. 2, pp. 26–34, 1998, doi: 10.1109/mc.1998.4655281

[45] P. Premaratnei and F. Safaei, “2D barcodes as watermarks in image authentication,” *6th IEEE/ACIS International Conference on Computer and Information Science*, pp. 432-437, 2007, doi: 10.1109/ICIS.2007.2

[46] P. Premaratne and M. Premaratne, “Key-based scrambling for secure image communication,” *International Conference on Intelligent Computing*, vol 304. pp. 259–263, 2012, doi: 10.1007/978-3-642-31837-5_38

[47] T. H. N. Le, K. H. Nguyen and H. B. Le, “Literature survey on image watermarking tools, watermark attacks and benchmarking tools,” *Second International Conferences on Advances in Multimedia*, pp. 67-73, 2010, doi: 10.1109/MMEDIA.2010.37

[48] F.Y. Shih, *Digital watermarking and steganography: fundamentals and techniques.* Boca Raton, Florida, USA: CRC Press, 2017.

[49] M. Uzun, “Sayısal renkli görüntüler için uzamsal düzlem yöntemleri kullanan yeni bir steganografi algoritması,” Yüksek Lisans Tezi, Bilişim Sistemleri Mühendisliği Anabilim Dalı, Kocaeli Üniversitesi, Kocaeli, Türkiye, 2023.

[50] J.C. Judge, “Steganography: past, present, future steganography: past, present, future,” *Lawrence Livermore National Lab*oratory, pp. 2-4, 2001.

[51] D. Kahn, “The history of steganography, information hiding,” *International Workshop on Information Hiding*, pp. 1–5, 1996.

[52] F. Petitcolas, R. Anderson and M. Kuhn, “Information hiding - a survey”, *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[53] T. Jamil, “Steganography: the art of hiding information in plain sight”, *IEEE Potentials*, vol. 18, no.1, pp. 10-12, 1999.

[54] G.J. Simmons, “The prisoners problem and subliminal channel,” *Advances in Cryptology*, pp. 51-57, 1994.

[55] X. Zhao, C. Yang and Liu, F. “On the sharing-based model of steganography,” *Digital Forensics and Watermarking, Lecture Notes in Computer Science*, vol. 12617, pp. 94-105, 2021.

[56] I. J. Kadhim, P. Premaratne, P.H. Vial and B. Halloran, “Comprehensive survey of image steganography: techniques, evaluations, and trends in future research,” *Neurocomputing*, vol.335, pp. 299–326, 2019.

[57] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital watermarking and steganography*. 2nd ed. San Francisco, California, USA: Morgan Kaufmann, 2007.

[58] S. Venkatraman, A. Abraham and M. Paprzycki , “Significance of steganography on data security,” *ITCC 2004 International Conference on Information Technology: Coding and Computing, IEEE,* vol.2, pp. 347–351, 2004.

[59] P. C. Mandal, I. G. Mukherjee, G. Paul and B.N. Chatterji, “Digital image steganography: a literature survey,*”Information Sciences*, vol. 609, pp. 1451–1488, 2022. doi: 10.1016/j.ins.2022.07.120

[60] H. Mathkour, B. Al-Sadoon and A. Touir, “A new image steganography technique,” *4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2008, doi: 10.1109/WiCom.2008.2918

[61] A. A. J. Altaay, S. B. Sahib and M. Zamani, “An introduction to image steganography techniques,” *International Conference on Advanced Computer Science Applications and Technologies (ACSAT),* pp. 122-126, 2012, doi: 10.1109/ACSAT.2012.25

[62] Z. Wang, O. Byrnes, H. Wang, R. Sun, C. Ma, H. Chen, Q. Wu and M. Xue. "Data hiding with deep learning: a survey unifying digital watermarking and steganography," *IEEE Transactions on Computational Social Systems*, pp.1–15, 2023, doi:10.1109/tcss.2023.3268950

[63] N. Deshpande, S. Kamalapur, D. Jacobs, “Implementation of LSB steganography and its evaluation for various bits,” *1st International Conference on Digital Information Management*, pp.173–178, 2006, doi:10. 1109/ ICDIM. 2007. 369349

[64] A. Nolkha, S. Kumar and V.S. Dhaka, “Image steganography using LSB substitution: a comparative analysis on different color models,” *Smart Systems and IoT: Innovations in Computing*, pp. 711–718, 2020.

[65] A. Şahin, E. Buluş and M.T. Sakallı, “24-bit renkli resimler üzerinde en önemsiz bite ekleme yöntemini kullanarak bilgi gizleme,” *Trakya University Journal of Natural Sciences*, vol.7, no. 1, pp.17-22, 2006.

[66] İ.Çayıroğlu, “Görüntü işleme- 1. hafta.” http://www.ibrahimcayiroglu.com/Dokumanlar/GoruntuIsleme/Goruntu_Isleme_Ders_Notlari-1.Hafta.pdf (Erişim tarihi: 25 Aralık 2023).

[67] U. K. Çınar, “Yapay sinir ağları ve R programıyla uygulama.” https://l24.im/dXSE7N (Erişim tarihi: 26 Aralık 2023).

[68] E. Yıldırım, “Yapay sinir ağı (artificial neural network).” https://l24.im/bJ3Pmo9 (Erişim tarihi: 26 Aralık 2023).

[69] D. Alkan, “U-Net derin öğrenme mimarisi kullanılarak yanmış alanların uydu görüntülerinden tespiti,” Yüksek Lisans Tezi, Harita Mühendisliği Anabilim Dalı, Konya Teknik Üniversitesi, Konya, Türkiye, 2023.

[70] A.Kızrak, “Şu kara kutuyu açalım: yapay sinir ağları.” https://bit. ly/3JzH2ui (Erişim tarihi: 27 Aralık 2023).

[71] M. Kotan, “EKO 469-veri madenciliği: hafta 12 – sınıflandırma.” https://mkotan.sakarya.edu.tr/sites/mkotan.sakarya.edu.tr/file/EKO469_VM_H12_Siniflandirma3.pdf (Erişim tarihi: 28 Aralık 2023).

[72] B. Erhandı, "Derin öğrenme ile metin özetleme," Yüksek Lisans Tezi, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı, Sakarya Üniversitesi, Sakarya, Türkiye, 2020.

[73] K. Zhang, Z. Zhang, Z. Li and Y. Qiao, "Joint face detection and alignment using multitask cascaded convolutional networks," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499-1503, Oct. 2016.

[74] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, *Handbook of fingerprint recognition*. 2nd ed. London, UK: Springer-Verlag, 2009.

[75] Sivaanandh M, Sai Surya and G. Priyanka, "Hand written indian numeral character recognition using deep learning approaches," *2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE)*, pp. 1301-1304, 2018.

[76] R. R. Subramanian, C. S. Niharika, D. U. Rani, P. Pavani and K. P. L. Syamala, "Design and evaluation of a deep learning algorithm for emotion recognition," *5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 984-988, 2021.

[77] B. Wang, Y. Zhou, H. Zhang and N. Wang, "An aircraft target detection method based on regional convolutional neural network for remote sensing images," *9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, pp. 474-478, 2019.

[78] Y. A. Kara, Ö. K. Uçarer and B. Gündoğdu, "Automatic warship recognition system: dataset, feature representation and classification analysis," *27th Signal Processing and Communications Applications Conference (SIU)*, pp. 1-4, 2019.

[79] R. M. James and A. Sunyoto, "Detection of CT - scan lungs COVID-19 image using convolutional neural network and CLAHE," *3rd International Conference on Information and Communications Technology (ICOIACT)*, pp. 302-307, 2020.

[80] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning.* Cambridge, MA, USA: MIT Press, 2016.

[81] Ö. Özcan and M. Karaaltun, "Görüntü artırma tekniklerinin cilt kanseri türleri üzerinde evrişimsel sinir ağları ile sınıflandırma başarılarının karşılaştırılması," *Niğde Ömer Halisdemir University Journal of Engineering Sciences*, vol.12, no.4, pp.1141-1156, 2023, doi: 10.28948/ngumuh.1270466

[82] S. Albawi, T. A. Mohammed, S and Al-Zawi, "Understanding of a convolutional neural network," *International Conference on Engineering and Technology (ICET)*, pp. 1-6, 2017, doi: 10.1109/ICEngTechnol.2017.8308186

[83] H.İ. Sarıyıldız, "Uydu görüntüleri ve İHA ile derin öğrenme algoritmaları kullanılarak hasarlı yapıların tespit edilmesi," Yüksek Lisans Tezi, Harita Mühendisliği Anabilim Dalı, On Dokuz Mayıs Üniversitesi, Samsun, Türkiye, 2021.

[84] Ö. İnik and E.Ülker, "Derin öğrenme ve görüntü analizinde kullanılan derin öğrenme modelleri," *Gaziosmanpaşa Bilimsel Araştırma Dergisi*, vol.6, no. 3, pp. 85-104, 2017.

[85] Ichi.Pro, "Evrişimli sinir ağları."
https://l24.im/bs1VR7 (Erişim tarihi: 28 Aralık 2023).

[86] G.B. Cangöz, "Köpeklerin uzun kemiklerinin ve uzun kemiklerindeki kırıkların sınıflandırılması," Doktora Tezi, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Başkent Üniversitesi, Ankara, Türkiye, 2022.

[87] A. D. Nguyen, S. Choi, W. Kim, S. Ahn, J. Kim, and S. Lee, "Distribution padding in convolutional neural networks," *International Conference on Image Processing (ICIP)*, pp. 4275–4279, 2019, doi: 10.1109/ıcıp.2019.8803537

[88] Medium, "Zero-padding in convolutional neural networks."
https://l24.im/6O9Y (Erişim tarihi: 29 Aralık 2023).

[89] E. Kurnaz, “Abdomen BT görüntülerinde pankreas segmentasyonu için yeni bir derin öğrenme yaklaşımı: PASCAL U-Net,” Yüksek Lisans Tezi, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Konya Teknik Üniversitesi, Konya, Türkiye, 2021.

[90] Z. Song, Y. Liu, R. Song, Z. Chen, J. Yang, C. Zhang and Q. Jiang, “A sparsity-based stochastic pooling mechanism for deep convolutional neural networks,” *Neural Networks*, vol. 105, pp. 340–345, 2018. doi: 10.1016/j.neunet.2018.05.015

[91] K.Patel, “Convolutional neural networks - a beginner’s guide.” https://bit.ly/3GXpYMX (Erişim tarihi: 29 Aralık 2023).

[92] V. Rajput, “Pooling layers in neural nets and their variants.” https://l24.im/M0g7aKr (Erişim tarihi: 29 Aralık 2023).

[93] E. Balık, “Derin öğrenme yöntemleri ile CXR görüntülerinden covid-19/zatürre/normal sınıflandırması ve U-Net Tabanlı covid-19 bölütlemesi,” Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı, Fırat Üniversitesi, Elazığ, Türkiye, 2022.

[94] A. Kızrak, “Derin öğrenme için aktivasyon fonksiyonlarının karşılaştırılması.” https://bit.ly/3JzH2ui (Erişim tarihi: 29 Aralık 2023).

[95] Derin Öğrenme, “Yapay sinir ağlarında aktivasyon fonksiyonları.” https://dltr.asmaamir.com/0-nn-kavramlari/4-aktivasyon_fonksiyonlari (Erişim tarihi: 29 Aralık 2023)

[96] E. Çakı and F. Bayram, “CNN-FL modeli ile pnömoni tespitinin aktivasyon fonksiyonlarına göre karşılaştırılması,”, *3rd International Conference on Applied Engineering and Natural Sciences,* Konya, Türkiye, 2022.

[97] A. Akbaş, “Yapay sinir ağlarında aktivasyon fonksiyonları çeşitleri.” https://l24.im/6ysmR (Erişim tarihi: 29 Aralık 2023).

[98] J. Ji, A. Dundar and E. Culurciello, “Flattened convolutional neural networks for feedforward acceleration,” *International Conference on Learning Representations (ICLR)*, 2014, doi:10.48550/arXiv.1412.5474

[99] J. X. Mi, J. Feng and K. Y. Huang, “Designing efficient convolutional neural network structure: a survey,” *Neurocomputing*, vol. 489, pp. 139–156, 2022. doi: 10.1016/j.neucom.2021.08.158

[100] M. S. Konca, “Evrişimli sinir ağları (convolutional neural networks-CNN).” https://l24.im/81ed7h (Erişim tarihi: 29 Aralık 2023).

[101] S. Metlek and K. Kayaalp, “Derin öğrenme ve destek vektör makineleri ile görüntüden cinsiyet tahmini,” *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, vol.8, pp. 2208-2228, 2020, doi: 10.29130/dubited.707316

[102] N. Çarkacı, “Derin öğrenme uygulamalarında en sık kullanılan hiper parametreler.” https://l24.im/yNYcmi (Erişim tarihi: 29 Aralık 2023).

[103] S.Sivri, “Farklı derin öğrenme yaklaşımları ile yolların segmentasyonu”, Yüksek Lisans Tezi, Harita Mühendisliği Anabilim Dalı, Yıldız Teknik Üniversitesi, İstanbul, Türkiye, 2019.

[104] S. Gazel and C.T. Bati, “Derin sinir ağları ile en iyi modelin belirlenmesi: mantar verileri üzerine keras uygulaması,” *Yuzuncu Yıl University Journal of Agricultural Sciences*, vol.29 no.3, pp.406-417, 2019.

[105] O. Ronneberger, P. Fischer and T. Brox, , “U-Net: convolutional networks for biomedical image segmentation,” *International Conference on Medical Image Computing and Computer-Assisted Intervention*, pp. 234-241, 2015, doi:10.48550/arXiv.1505.04597

[106] A. Farasin, L. Colomba, G. Palomba, G. Nini and C.Rossi, “Supervised burned areas delineation by means of Sentinel-2 imagery and convolutional neural networks”, *International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, pp.1060-1071, 2020.

[107] N. Siddique, P. Sidike, C. Elkin and V Devabhaktuni, “U-Net and its variants for medical image segmentation: a review of theory and applications,” *IEEE Journals & Magazine*, vol.9, pp. 82031-82057, 2021, doi:10.1109/access.2021.3086020.

[108] F. Z. Ünal, “Derin öğrenme ile yüz tanıma,” Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı, Ankara Üniversitesi, Ankara, Türkiye, 2017.

[109] Stanford University, “T-SNE visualization of CNN codes.” https://l24.im/EJYZq (Erişim tarihi: 29 Aralık 2023).

[110] “Linnaeus 5 dataset.”, Chaladze.com. http://chaladze.com/l5/ (Erişim tarihi: 30 Aralık 2023).

[111] UMass Amherts, “Labeled faces in the wild home.” https://vis-www.cs.umass.edu/lfw/ (Erişim tarihi: 30 Aralık 2023).

[112] Deeplake, “Machine learning datasets.” https://l24.im/OezM5n (Erişim tarihi: 30 Aralık 2023).

[113] Google, “Google colaboraty.” https://colab.research.google.com/ (Erişim tarihi: 01 Ocak 2024).

[114] S. Karakuş, “Veri gizlemede steganografik yöntemlerin performansını artırabilmek için yeni bir yaklaşımın geliştirilmesi,” Doktora Tezi, Yazılım Mühendisliği Anabilim Dalı, Fırat Üniversitesi, Elazığ, Türkiye, 2020.

[115] D. Setiadi, “PSNR vs SSIM: imperceptibility quality assessment for image steganography,” *Multimedia Tools and Applications, Springer Science Business Media*, 2020.

[116] F. Q. A Alyousuf, R. Din, A.J. Quasim, “Analysis review on spatial and transform domain technique in digital steganography,” *Bulletin of Electrical Engineering and Informatics*, vol.9, no.2, pp. 373-38, 2020.

[117] A.A. Abd El-Latif, B. Abd-El-Atty, S.E. Vegenas-Andraca, “A novel image steganography tecnique based on quantum substitution boxes,” *Optics and Laser Technology,* vol. 116, pp. 92-102, 2019.