KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

TEKRARLI SIKIŞTIRMADA FREKANS KATSAYILARININ VARYANSI TEMELLİ DAYANIKLI VERİ GİZLEME YÖNTEMİ

ABDIWAHAB MOHAMED ABDIRASHID

KOCAELİ 2023

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

TEKRARLI SIKIŞTIRMADA FREKANS KATSAYILARININ VARYANSI TEMELLİ DAYANIKLI VERİ GİZLEME YÖNTEMİ

ABDIWAHAB MOHAMED ABDIRASHID

Doç.Dr. Serdar SOLAK		
Danışman,	**Kocaeli Üniversitesi**	**.....**
Prof.Dr. Yıldıray YALMAN		
Jüri Üyesi,	**Piri Reis Üniversitesi**	**.....**
Doç.Dr.Öğr. Mustafa Hikmet Bilgehan UÇAR		
Jüri Üyesi,	**Kocaeli Üniversitesi**	**.....**

Tezin Savunulduğu Tarih: 13.06.2023

ETİK BEYAN VE ARAŞTIRMA FONU DESTEĞİ

Kocaeli Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez/proje çalışmasında,

- Bu tezin/projenin bana ait, özgün bir çalışma olduğunu,
- Çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı,
- Bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi,
- Bu çalışmanın Kocaeli Üniversitesi'nin abone olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun olduğunu,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Tezin/Projenin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez/proje çalışması olarak sunmadığımı, beyan ederim.

[X] Bu tez/proje çalışmasının herhangi bir aşaması hiçbir kurum/kuruluş tarafından maddi/alt yapı desteği ile desteklenmemiştir.

[ ] Bu tez/proje çalışması kapsamında üretilen veri ve bilgiler ..... tarafından no'lu proje kapsamında maddi/alt yapı desteği alınarak gerçekleştirilmiştir.

Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

.....

Abdiwahab MOHAMED ABDIRASHID

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI

Fen Bilimleri Enstitüsü tarafından onaylanan lisansüstü tezimin/projemin tamamını veya herhangi bir kısmını, basılı ve elektronik formatta arşivleme ve aşağıda belirtilen koşullarla kullanıma açma izninin Kocaeli Üniversitesi'ne verdiğimi beyan ederim. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet hakları bende kalacak, tezimin/projemin tamamının ya da bir bölümünün gelecekteki makale, kitap, tebliğ, lisans, patent gibi çalışmalarda kullanımı, danışmanımın isim hakkı saklı kalmak koşuluyla ve her iki tarafın bilgisi dâhilinde bana ait olacaktır.

Tezin/projenin kendi özgün çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin/projenin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim kurulu tarafından yayınlanan **"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"** kapsamında tezim aşağıda belirtilen koşullar haricinde YÖK Ulusal Tez Merkezi/ Kocaeli Üniversitesi Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

☐ Enstitü yönetim kurulu kararı ile tezimin/projemin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir.

☐ Enstitü yönetim kurulu gerekçeli kararı ile tezimin/projemin erişime açılması mezuniyet tarihinden itibaren 6 ay ertelenmiştir.

☒ Tezim/projem ile ilgili gizlilik kararı verilmemiştir.

.....

Abdiwahab MOHAMED ABDIRASHID

ÖNSÖZ VE TEŞEKKÜR

Her şeyden önce yüksek lisans öğrenimim boyunca birlikte çalışma ayrıcalığına sahip olduğum danışman hocam saygıdeğer Doç. Dr. Serdar SOLAK'ın öğrencisi olmaktan büyük mutluluk ve gurur duymaktayım. Son derece destekleyici, açık fikirli ve maksimum uzmanlık niteliği ile aktarmış oldukları araştırmalarımdaki derin ve geniş açıdan kavrama anlayışı kazandırıp, bilimsel araştırma tutkusu ekolunu benimseterek bana sürekli ilham kaynağı olmuştur. Akademik alt yapımı inşa etme hususunda desteğini hiç esirgemeden büyük emeği olan ve bir o kadar da sonsuz katkısı olduğundan danışman hocama özellikle sonsuz şükranlarımı iletirim. Araştırmalarım sürecinde benimle çalışan ve bana paha biçilmez desteğinden esirgemeyen değerli meslektaşım ve iş arkadaşım Arsene ADJEVİ'ye kattıkları değerli bilgi ve birikim için şükranlarımı sunmak istiyorum. Ayrıca, tez komitemin jüri üyelerine saygı değer hocalarıma benimle paylaştıkları paha biçilmez görüş, rehberlik ve destek vermek için ayırdıkları değerli zamanlarından dolayı şükranlarımı sunarım. Tüm bu yıllar boyunca bana katlandıkları için başta annem ve ablam olmak üzere değerli büyük aileme moral ve desteklerinden dolayı teşekkür etmek istiyorum. Onların muazzam desteği ve fedakarlığı olmadan, bu tez de dahil olmak üzere başarılarımın hiçbiri mümkün olmazdı. Ve son olarak, hayatım boyunca desteğini hiç esirgemeyen tüm emeğiyle ilim ve irfan talebi yolunda yetiştiren, doğru tercihleri yapmama ışık tutan, bizi erdemlik ve azimle eğitimde yol almayı gösteren, bugün burada gerçekleşen başarıma şahit olmasını dilediğim sevgili rahmetli babama bu başarıyı armağan ediyorum. Allah'tan rahmet ve mekânı da cennet eylemesini dilerim.

Haziran- 2023 Abdiwahab MOHAMED ABDIRASHID

İÇİNDEKİLER

ETİK BEYAN VE ARAŞTIRMA FONU DESTEĞİ i
YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI ii
ÖNSÖZ VE TEŞEKKÜR iii
İÇİNDEKİLER iv
ŞEKİLLER DİZİNİ v
TABLOLAR DİZİNİ vi
SİMGELER VE KISALTMALAR DİZİNİ vii
ÖZET viii
ABSTRACT ix
1. GİRİŞ 1
2. GENEL BİLGİLER 4
2.1. Steganografi 5
2.2. Kriptoloji 7
2.2.1. Simetrik (Özel Anahtarlı Algoritmalar) 8
2.2.2. Asimetrik (Açık Anahtar Bazlı Algoritmalar) 9
2.3. Literatür Taraması 10
3. ÖNERİLEN METOD 14
3.1. Blok Zinciri Şifreleme (AES-CBC) 16
3.2. Veri Gizleme 17
3.2.1. Örtü Görüntünün Ön-işlenmesi ve JPEG Tekrarlı Sıkıştırma 18
3.2.2. JPEG Dönüşüm Formatı 20
3.2.3. JPEG Renk Dönüşüm Kanalları 20
3.2.4. Ayrık Kosinüs Dönüşümü 21
3.2.5. Nicemleme (Quantization) 23
3.3. Sıkıştırılmış Görüntülerin DCT Katsayılarına Varyans Uygulanması 23
3.4. Varyans Katsayılarının Min-max Normalizasyon ile Eşleştirilmesi 27
4. DENEYSEL ÇALIŞMALAR 29
4.1. Deneysel Ön Hazırlığı 29
4.2. Anti Sıkıştırmaya Dayalı Ataklarına Karşı Deneysel Sonuçları 30
4.3. Gizlenmiş Verinin Geri Elde Edilmesi 35
4.4. Performans Karşılaştırmaları 37
5. SONUÇLAR VE ÖNERİLER 43
KAYNAKLAR 45
KİŞİSEL YAYIN VE ESERLER 48
ÖZGEÇMİŞ 49

ŞEKİLLER DİZİNİ

Şekil 2.1. Alıcı ve Gönderici arasında gizli mesaj gönderimi 4
Şekil 2.2. Steganografi alt kategorileri 5
Şekil 2.3. Kriptografinin çalışma mantığı 8
Şekil 2.4. Özel anahtarlı şifreleme süreci 9
Şekil 2.5. Şifreleme algoritmaları 9
Şekil 3.1. Önerilen Metot Genel Şema 15
Şekil 3.2. AES blok zinciri şifreleme şeması 16
Şekil 3.3. AES blok zinciri deşifreleme şeması 17
Şekil 3.4. Şifreleme ve veri gizleme blok şeması 17
Şekil 3.5. Örtü görüntü ön işleme süreci 18
Şekil 3.6. JPEG renk dönüşüm kanalları 21
Şekil 3.7. Frekans domain 22
Şekil 3.8. Varyans Hesaplama İşlemi 25
Şekil 3.9. Katsayıların Varyans ile Eşleştirilmesi ve Veri Gömme İşlemi 26
Şekil 4.1. BOSSbase 1.01 Veri tabanı deneysel çalışmada kullanılan görüntüler 30
Şekil 4.2. BER vs Varyans [0 – 0,1] Grafiği 32
Şekil 4.3. BER vs Varyans [0-0,2] Grafiği 32
Şekil 4.4. BER vs Varyans [0-0,3] Grafiği 33
Şekil 4.5. BER vs Varyans [0-0,7] Grafiği 35
Şekil 4.6. AC DCT katsayıların AC Varyanslar ile Eşleştirilmesi 36
Şekil 4.7. Veri Çıkarma Süreci 37

TABLOLAR DİZİNİ

Tablo 3.1. Katsayıların Varyans Yüzdelik Değişim Oranları 27
Tablo 3.2. Katsayıların Yüzdelik Değişim Oranların Değişkenleri..... 28
Tablo 4.1. Deneysel Ayarları 29
Tablo 4.2. Boss1 varyans [0-0,1] bazlı bpnzAC BER değerleri..... 31
Tablo 4.3. Boss1 varyans [0-0,2] bazlı bpnzAC BER değerleri..... 34
Tablo 4.4. Benzer çalışmalar 37
Tablo 4.5. WU et al PSNR değerleri 39
Tablo 4.6. Kalite faktörlerine göre orijinal ile stego görüntülerin PSNR değerleri..... 39
Tablo 4.7. Orijinal görüntü ve sıkıştırma aşamaların PSNR karşılaştırmaları 40
Tablo 4.7. (Devamı) PSNR karşılaştırmaları Kalite Faktörü 85..... 41
Tablo 4.7. (Devamı) PSNR karşılaştırmaları Kalite Faktörü 95..... 42

SİMGELER VE KISALTMALAR DİZİNİ

Kısaltmalar

AC	: Alternating Current (Alternatif Akım)
AES	: Advanced Encryption Standard (İleri Şifreleme Standardı)
BER	: Bit Error Rate (Bit Hata Oranı)
BMP	: Bitmap Image Format (Bitmap Görüntü Formatı)
BPNZAC	: Bit Per Non Zero AC Coefficients (Sıfır Olmayan AC Katsayıların .Başına Düşen Bit Sayısı)
CBC	: Cipher Block Chaining (Blok Zinciri Şifreleme)
dB	: Decibel (Desibel)
DC	: Direct Current (Doğru Akım)
DCT	: Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)
DFT	: Discrete Fourier Transform (Ayrık Forier Dönüşümü)
DWT	: Discrete Wavelet Transform (Ayrık Dalgacık Dönüşümü)
ECB	: Electronic Codebook (Elektronik Şifreleme Kitabı)
HVS	: Human Visual Systems (İnsan Görsel Algılama Sistemi)
IDCT	: Inverse Discrete Cosine Transform (Ayrık Kosinüs Ters Dönüşümü)
JPEG/JPG	: Joint Photographic Experts Group (JPEG Görüntü Format)
LED	: Light Emmitting Diodes (Işık Yayan Diyotlar)
MSE	: Mean Squared Error (Ortalama Karesel Hata)
PNG	: Portable Network Graphics (Taşınabilir Ağ Grafikleri)
PSNR	: Peak Signal to Noise Ratio (Tepe Sinyal Gürültü Oranı)
RGB	: Red, Green, Blue colour model (Kırmızı, Yeşil, Mavi)
YCrCb	: Y = Luminance, CrCb=Chrominance (Lumen ve Kroma Renk Uzayı)

TEKRARLI SIKIŞTIRMADA FREKANS KATSAYILARININ VARYANSI TEMELLİ DAYANIKLI VERİ GİZLEME YÖNTEMİ

ÖZET

Bilgi ve iletişim teknolojilerinin hızlı ilerlemesiyle, bilgi güvenliği kavramı günümüzde büyük önem arz etmektedir. Özellikle internet ortamında uçtan uca iletişim sağlarken bilgilerin güvenliğini sağlamak için, gizlilik, bütünlük ve erişilebilirlik kavramlarının etkili bir şekilde gerçekleştirilmesi gerekir. Bilgi gizliliğini sağlamak için Kriptoloji ve Steganografi teknikleri kullanılmaktadır. Kriptoloji bilgiyi matematiksel teknikler kullanarak anlaşılmayacak şekilde ifade etme işlemidir. Steganografi ise, metin, ses, görüntü veya video dosyaları içerisine gizli bilgiyi şüphe uyandırmadan saklama işlemidir. Yüksek veri gizleme kapasitesi ve yaygın kullanımı sebebiyle veri gizleme çalışmalarında görüntüler daha fazla tercih edilmektedir. Özellikle sosyal medya platformlarında paylaşılan görüntüler, gizli verileri göndermek için iyi bir taşıyıcı olabilir. Ancak, sosyal medya platformları görüntüleri uçtan uca aktarırken sıkıştırma uygulayarak göndermektedir. Tez çalışması kapsamında, Kriptoloji ve Steganografi tekniklerini beraber kullanan sıkıştırma ataklarına karşı dayanıklı yeni bir veri gizleme yöntemi önerilmektedir. Yöntem ilk olarak gizlenecek veriyi Gelişmiş Şifreleme Standardı Şifreli Blok Zincir (Advanced Encryption Standard Cipher Block Chaning- AES CBC) tekniği ile şifrelemektedir. Sonrasında, tekrarlı sıkıştırma uygulanmış JPEG görüntülere Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform - DCT) yapılarak elde edilen katsayılar üzerinde veri gizleme yapılmaktadır. Tekrarlı sıkıştırma işlemleri sonucunda az değişen veya hiç sıkıştırmadan etkilenmeyip değişmeyen katsayılara veriler gizlenmektedir. Bu sayede gizlenmiş olan veri yüksek doğrulukta geri elde edilmektedir. Yapılan deneysel çalışmalarda, önerilen yöntem BOSSBase veri setinde bulunan görüntüler üzerinde denenmiş olup, literatürde yer alan yöntemlerden daha iyi sonuçlar verdiği gözlemlenmiştir.

Anahtar Kelimeler: Bilgi Güvenliği, DCT Frekans Domain ile Veri Gizleme, Görüntü Steganografisi, JPEG Anti-sıkıştırma, JPEG Nonzero AC Katsayıların Varyansları.

ROBUST DATA HIDING METHOD BASED ON THE VARIANCE OF FREQUENCY COEFFICIENTS IN REPETITIVE COMPRESSION

ABSTRACT

The rapid progress of information and communication technologies has made information security more important than ever. Safeguarding data integrity and ensuring secure communication have become critical challenges in the digital era. To address these challenges, the fields of cryptography and steganography have emerged as essential disciplines. Cryptography involves the use of mathematical techniques to transform information into an unreadable format while ensuring its confidentiality. Steganography, on the other hand, focuses on hiding sensitive data within various types of files, making it imperceptible to unauthorized individuals. By combining these two disciplines, implementing a powerful approach to secure information transmission is possible to obtain. In the context of data hiding, images are preferred due to their high data capacity and widespread usage. Sharing accurate and lossless images with higher quality through digital mediums is challenging, particularly, images shared on social media platforms can serve as good carriers for sending hidden data. However, social media platforms apply compression when transferring images end-to-end. Within the scope of this thesis, the proposed method introduces a novel approach by combining cryptographic and steganographic techniques, providing a robust solution to protect hidden data even when subjected to compression. The method first encrypts the secret data to be hidden using the Advanced Encryption Standard Cipher Block Chaining (AES CBC) technique. Then, data hiding is performed on the coefficients obtained by applying Discrete Cosine Transform (DCT) to repeatedly compressed JPEG images, coefficients that are minimally affected by compression or remain unaffected are specifically selected for data hiding. Thus, the hidden data is retrieved with high accuracy. Experimental evaluations demonstrate that the proposed method outperforms existing techniques in terms of achieving robust and effective data-hiding techniques.

Keywords: Information Security, Data Hiding in DCT Frequency Domain, Image Steganography, Anti-repetitice compression of JPEG Images, Variances of JPEG Nonzero AC Coefficients.

1. GİRİŞ

Günlük Bilgilerin bir noktadan başka bir noktaya gizli bir şekilde aktarılması asırlardır kullanılmaktadır. Genel olarak gizli haberleşme eski zamanlarda hükümetler, casuslar veya kurumlar tarafından kullanılırdı. Gizli haberleşme, o zamanlarda teorik temeli yaklaşımlar yerine günlük hayatta kullanılan yöntemlerin hileli bir şekli olduğundan bir araştırma disiplini değildi. İlerleyen yıllarda bilişim teknolojilerinin artması ve bu teknolojilerin kullanımının yaygınlaşması gizli haberleşme sistemlerinin önemini arttırarak bir araştırma disiplini haline gelmesini sağladı. Bilişim teknolojilerinin yaygın kullanılmasıyla, analog sistemlerden sayısal sistemlere geçiş hızlı bir şekilde gerçekleşmiştir. Sayısal sistemlerde bilgilerin depolanması, saklanması ve uçtan uca güvenli bir şekilde iletilmesi önemli bir araştırma konusu haline gelmiştir. Araştırmacılar, günlük hayatta kullanılan gizli haberleşme yöntemlerini sayısal ortamlara entegre etmeye ve yeni yöntemler geliştirmeye başladılar.

Sayısal sistemlerde, bilgi güvenliğini sağlamak için gizlik, bütünlük ve erişilebilirlik sağlanması gerekmektedir. Göndericinin yolladığı verinin alıcı tarafından tamamının bozulmadan veya değiştirilmeden alınması bütünlük kavramını ifade ederken, gönderenin ve alıcının sürekli uygun durumda olması erişilebilirlik olarak ifade edilmektedir. Gizlilik kavramı ise, bilginin üçüncü kişiler tarafından elde edilememesi, varlığının anlaşılamaması veya bilginin ne olduğunun anlaşılamaz hale getirilmesidir. Sayısal sistemlerde bu gizliliği sağlamak için şifreleme olarak bilinen Kriptografi ve veri gizleme olarak bilinen Steganografi kullanılmaktadır.

Kriptografi bilginin gizliliğini korumak için etkili bir yöntemdir. Örneğin, iletişim kuran taraflar, yalnızca kendilerinin belirlediği paylaşılan bir anahtarı kullanarak bilgiyi şifreleyebilir ve bu bilgi ilgili tarafa ulaşınca deşifre edebilir (Bender, Gruhl, Morimoto, & Lu, 1996). Kullanılan şifreleme algoritması yeterince güçlü olduğunda, şifrelenen bilgi üçüncü şahıslar tarafından okunsa bile bilginin gizliliğine yönelik bir tehdit olarak değerlendirilmemektedir. Öte yandan, kriptografinin çok kolay tespit edilebilir olma gibi bir dezavantajı vardır. Yani bilginin anlamı anlaşılmasa bile gizli bir iletişimin olduğu ve kimin kime yazdığı belli olmaktadır. Veri gizleme olarak bilinen Steganografi ise, karşı tarafa iletilecek bilginin çaktırmadan, metin, ses, görüntü veya video dosyalarının içerisine yerleştirilmesi işlemidir. Bu sayede karşı tarafa gönderilecek olan dosyada ilk

bakışta herhangi bir olağan dışılık görülmemektedir. Kısacası Steganografi tekniklerindeki temel beklenti, karşı tarafa aktarılacak gizli bilgiyi taşıyan nesnenin üçüncü şahıslar tarafından anlaşılmasını imkânsız kılınmasını sağlamaktır.

Steganografi kullanarak veri gizleme yapılırken, gizli bilgi, gizli bilgiyi saklayacak örtü nesne, etkili ve verimli bir veri gizleme tekniğine ihtiyaç duyulmaktadır. Veri gizleme işlemi tamamlandığında elde edilen bilgi gizlenmiş nesneye stego nesne denilmektedir. Örtü nesne olarak görüntünün kullanıldığı veri gizleme çalışmaları Görüntü Steganografisi olarak adlandırılmaktadır. Görüntü pikselleri üzerinde direk veri gizleme yapılması Uzamsal domain teknikleri, sıkıştırma işlemi yapılmış görüntülerde veri gizleme yapılması dönüşüm veya frekans domain teknikleri ile yapılmaktadır. Uzamsal alan yöntemlerinde veri gizleme algoritmasının kolay, hızlı ve hesaplama maliyetlerinin düşük olması gibi avantajlar olmasına rağmen bazı eksiklikler de mevcuttur. Örtü görüntüye gizlenebilecek veri kapasitesinin sınırlı olması, görüntünün barındırdığı tüm piksel alanlarının değerlendirilememesi gibi bazı kısıtları bulunmaktadır. Tüm bu kısıtları kaldırabilecek olan frekans dönüşüm alanında örtü görüntü pikselleri frekans alanına dönüştürülerek işlem yapılmaktadır. Bu dönüşümden sonra görüntü yüksek ve düşük frekanslara ayrılmaktadır. Sonrasında, ayrık kosinüs dönüşümü (Discrete Cosine Transform - DCT) gibi sıkıştırma algoritması ile yüksek frekansların katsayılarına veriler gizlenmektedir. Frekans dönüşüm alanı, veri gizleme kapasitesini arttırmak, piksellerin tamamını değerlendirmek, görüntü kalitesindeki bozulmaları engellemek gibi avantajlara sahiptir.

Özellikle, son yıllarda sosyal medya platformlarında kullanıcılar fotoğraf görüntülerini paylaşmaktadır. Bu paylaşım sırasında ilgili platformlar görüntüler üzerinde sıkıştırma teknikleri uygulayarak boyut azaltmaktadır. Dolayısıyla, görüntü içerisinde gizli bilgi olması durumunda kaybolma, bozulma veya tekrar elde edilememe riski bulunmaktadır. Özellikle verilerin uçtan uca aktarılması sırasında görüntülere uygulamış olan tekrarlı sıkıştırma aşamaları kalite bozukluklarına sebep vermektedir. Buda verilerin tamamının alıcı tarafından kusursuz ve başarılı bir şekilde tekrar elde edilmesine mâni olmaktadır.

Tez çalışması kapsamında, sayısal ortamda bilgi güvenliğini sağlamak amacıyla Kriptografi ve Steganografi tekniklerini kullanan çift katmanlı yeni bir veri gizleme yöntemi önerilmektedir. Yöntem, sıkıştırmalara karşı etkili olması amacıyla frekans

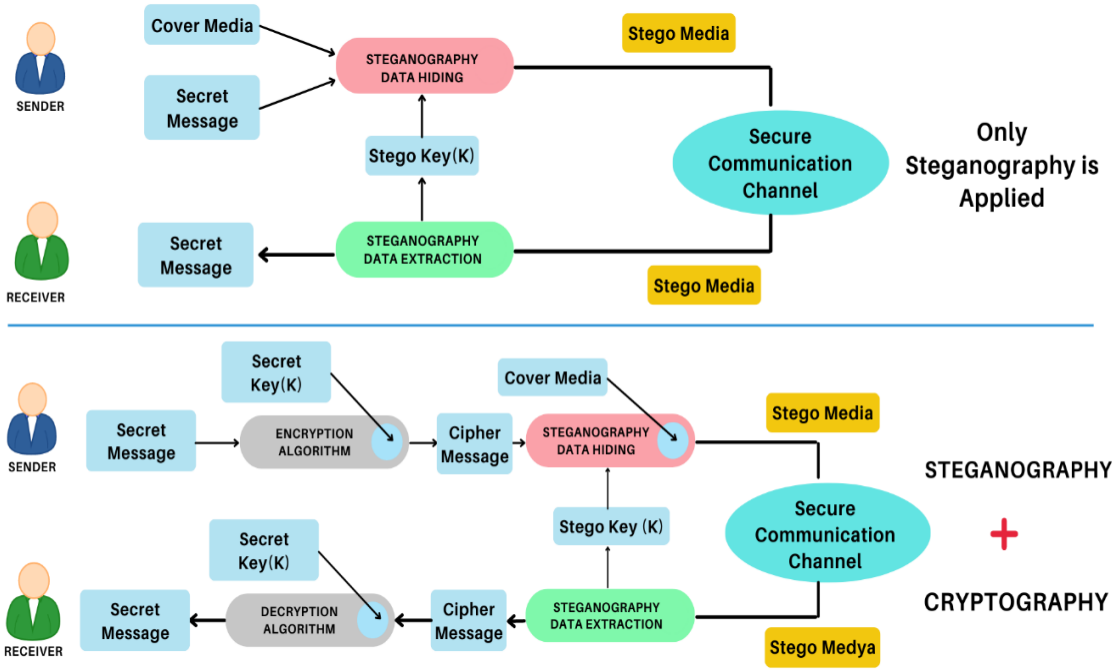
domain teknikleri kullanılarak gerçeklenmiştir. Yöntemde ilk olarak gizli bilgi kriptoloji teknikleriyle şifrelenmekte, aynı zamanda örtü görüntü frekans domaine çevrilmekte ve sıkıştırmadan etkilenmeyen katsayılar bulunmaktadır. Sonrasında veri gizleme işlemi gerçeklenmektedir. Önerilen yöntem, tekrarlı sıkıştırmaya dayanıklı olup farklı kanallardan aktarılan stego görüntüden verinin yüksek başarımla çıkarılmasını sağlamaktadır. Çalışma kapsamında önerilen yöntemin, literatürde önerilen benzer yöntemlere göre daha dayanıklı olduğu deneysel çalışmalarda test edilmiştir.

Tez çalışmasının ikinci bölümünde Genel Bilgiler başlığı altında, literatürde yapılan benzer çalışmalar, görüntü steganografisi ve kriptoloji kavramları anlatılmaktadır. Üçüncü bölümde, tez kapsamında önerilen yöntem sunulmaktadır. Dördüncü bölümde önerilen yönteme ait deneysel sonuçlar ve son bölümde elde edilen sonuçlar yer almaktadır.

2. GENEL BİLGİLER

Bu bölümde, Günümüzde taşınabilir cihazlar, iletişim teknolojileri ve sosyal medya platformlarının yaygınlaşmasıyla birlikte ses, görüntü ve video verileri insanlar arasında yaygın olarak paylaşılmaktadır. Ayrıca, insanlar verilerini hızlı bir şekilde erişecekleri bulut ortamında daha yaygın olarak saklamaktadırlar. Dolayısıyla bu ortamlarda, insanların verilerini koruması ve saklanması için çeşitli güvenlik önlemleri alması gerekmektedir. Bu güvenliği sağlamak için, verinin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak gerekmektedir. Tez çalışması kapsamında önerilen yöntem veri gizliliğini sağlamak için, Kriptografi (Diffie ve Hellman, 1976) ve Steganografi (Johnson ve Jajodia, 1998; Yalman, 2010) yaklaşımlarını kullanan bir tekniktir.

Şekil 2.1'de gönderici ile alıcı arasında gizli mesajın steganografi kullanılarak gönderilmesini sağlayan akış sunulmaktadır.



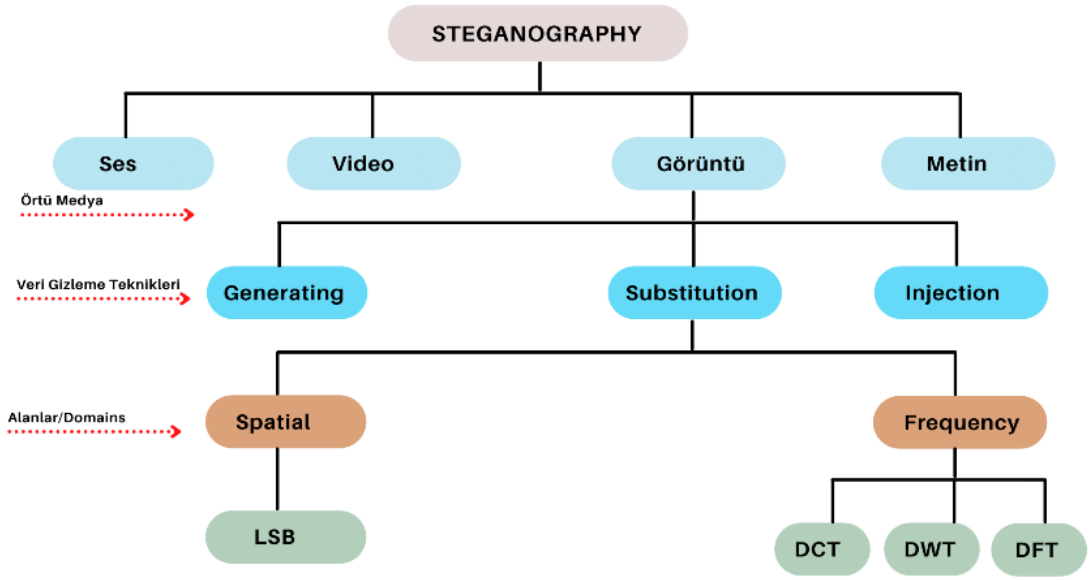
Şekil 2.1. Alıcı ve Gönderici arasında gizli mesaj gönderimi

Şeklin üst kısmında sadece steganografi kullanılırken, alt kısımda ise steganografi ve kriptoloji beraber kullanılmaktadır. Kriptoloji ve steganografinin beraber kullanışdığı çalışmalar, sadece steganografi kullanılan çalışmalara göre daha yüksek güvenlik ve gizlilik sağlamaktadır. Bu kapsamda, bu alt bölümde tez çalışmasının temelini oluşturan

Kriptografi, Steganografi kavramları ve literatürde yapılan benzer çalışmalar sunulmaktadır.

2.1. Steganografi

Steganografi, eski çağlardan beri kullanılan bilgi gizleme tekniğidir. Bazen, gizli bir mesaj ormandaki ağaca balçıkla sıvanarak saklanmış, bazen bir habercinin saçları kestirilerek kafasına yazılmış ve tekrar saçları uzadığında ilgili yere gönderilmiştir. Bazen de ilaç içmek istemeyen çocuklara, çorbanın içerisinde çaktırmadan ilaç verilerek kullanılması durumudur (Kadhim ve diğ., 2019). Örneklerden görüldüğü üzere, günlük hayatta kullanılmakta olup her şey doğal akışındadır ve gizli bilgi, mesaj ve/veya nesnenin orada olduğunun kimse farkında değildir. Bilgisayar ortamında kullanılan, Sayısal Steganografi, metin, ses, görüntü ve video gibi çeşitli dosyalara gizli mesajların çaktırmadan gizlenmesidir (Hussain ve diğ., 2018; Uzun ve Solak, 2022). Şekil 2.2'de steganografinin sınıflandırılması ile ilgili şema sunulmaktadır.



Şekil 2.2. Steganografi alt kategorileri

Steganografi çalışmalarında, örtü nesne (cover object), gizli mesaj (secret message), veri gizleme algoritması ve stego nesne kavramları bulunmaktadır. Örtü nesne ve gizli mesaj girdi olarak veri gizleme algoritmasına verilmektedir. Veri gizleme işlemi sonunda oluşan çıktı ise stego nesne olarak adlandırılır. Örtü nesne olarak görüntülerin kullanılması, Görüntü Steganografisi olarak adlandırılmaktadır (Solak 2020; Solak ve Tezcan, 2022).

Birinci bölümde de sunulduğu üzere görüntü steganografi teknikleri uzamsal alan ve frekans dönüşüm alanı olmak üzere iki grupta incelenmektedir. Uzamsal alan teknikleri, pikseller üzerinde yoğunluk değerlerine göre direk işlem yapmaktadır. Uzamsal alanda, en az anlamlı bitlerin değiştirilmesi (Least Significant Bit - LSB) (Swain ve Lenka, 2012; Solak ve Altınışık, 2019), piksel değeri farkları (Pixel Value Differencing - PVD) (Wu ve Tsai, 2003), değişim yönünü kullanma (Exploiting Modification Directions - EMD) (Zhang ve Wang, 2006) yöntemleri en yaygın kullanılan tekniklerdir. Bu istatistiksel veri gizleme teknikleri döndürme, kırpma, ölçekleme saldırılarına karşı genellikle savunmasızdır. Ayrıca bu veri gizleme teknikleri genellikle kayıpsız görüntü sıkıştırma formatlarında uygulanmaktadır. Ancak JPEG gibi kayıplı sıkıştırma uygulanmış görüntü formatlarında bu veri gizleme tekniklerinin direk uygulanması uygun değildir. Bu görüntü formatlarında kayıplı sıkıştırma teknikleri uygulandığından, gizlenecek mesaj bitleri kaybolmaktadır. Dolayısıyla JPEG görüntüler için frekans dönüşüm alanında çevrilerek veri gizleme yapılması gerekir. Frekans dönüşüm alanında, DCT (Khayam, 2003; Lam ve Goodman, 2000), DWT (Po-Yueh ve Lin, 2006; Kumar ve Kumar, 2018) veya ayrık fourier dönüşümü (Discrete Fourier Transformation – DFT) (Wang ve Moulin, 2006) gibi yöntemler kullanılarak dönüşüm işlemi yapılmakta ve sonrasında veri gizleme gerçekleştirilmektedir. Bu sayede, gizlenen veriler, frekans dönüşüm alanına gömülerek daha sağlam bir alanda bulunmakta ve tüm görüntüye yayılmaktadır. Dolayısıyla, sinyal işlemeye ve sıkıştırma ataklarına karşı etkili olmaktadır.

Genel olarak, DCT ile veri gizleme çalışmalarında, ilk olarak görüntü bloklara ayrılmaktadır. Bu bloklar genellikle 8x8'lik bir matris şeklindedir. Sonrasında, her blok için DCT uygulanmaktadır. DCT, -128 ile 127 arasındaki değerler üzerinde çalıştığından, piksel değerleri, her piksel değerinden 128 çıkarılarak bu aralığa getirilmektedir. Daha sonra, 8x8lik blokta yer alana DCT katsayıları, kuantalama ile sıkıştırılmaktadır. Kuantalama sırasında önemi az olan frekanslar atılmaktadır. Ardından kualtalanmış DCT katsayılarını içeren matris elde edilir. Bunun için, DCT katsayılarının olduğu bloklar, kuantalama matrisinde karşılık gelen değerlere bölünerek işlem görmektedir. Sonrasında, kuantalanmış DCT katsayıları üzerinde seçilen veri gizleme algoritması ile veri gizleme işlemi yapılmaktadır. Ardından, elde edilen yeni değerler, kuantalama matrisindeki değerler ile çarpılarak dekuanlatama işlemi yapılmaktadır. Sonrasında, ters DCT işlemi yapılır ve elde edilen değerlere 128 değeri eklenerek veri gizlenmiş stego görüntü elde

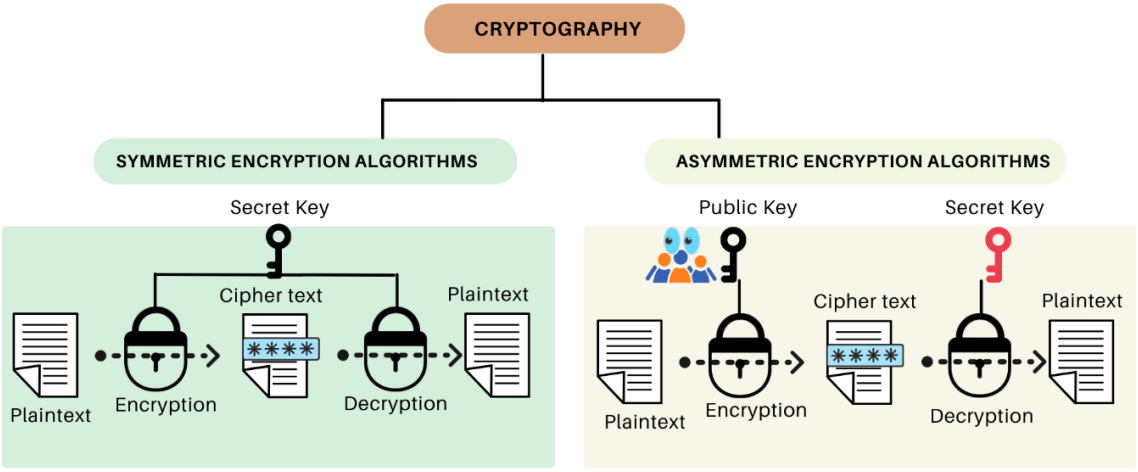
edilir (Piva ve diğ., 1997; Maurya ve dig.,2023).

DWT, fourier analizindeki sinüs ve kosinüslere benzer bir biçimde olan dalgacık sinyallerini temsil etmek için kullanılan özel fonksiyonlardır. Ayrık dalgacık dönüşümü çalışmalarında yayın olarak kullanılan genellikle DWT'nin en basit hali Haar-DWTdir. Burada uygulama mantığı, düşük frekanslı dalgacık katsayısını üretmek için, iki piksel değerinin ortalaması alınırken, yüksek frekansı üretmek için aynı iki pikselin farklarının yarısı alınarak hesaplanmaktadır. DWT uygulamak, görüntüyü daha düşük çözünürlükle temsil eden benzer bir görüntü oluşturmayı veya bant (LL) ile yatay (HL), dikey (LH) ve çapraz (HH) detay bileşenlerine ayrıştırmaya yaramaktadır. Dalgacık dönüşüm sonrasında, görüntüde yer alan pürüzsüz kısımlar düşük frekans dalgacık katsayılarında (LL) ile temsil edilirken, görüntüdeki kenar ve doku gibi detaylar yüksek frekans dalgacık katsayıları (HL, LH ve HH) ile temsil edilmektedir. DWT ile veri gizleme uygulamasında, renkli örtü görüntü ilk olarak renk kanallarına ayrılmaktadır. İlk olarak kırmızı renk kanalındaki değerler alınmakta, soldan sağa yatay yönde tarama yapılmakta ve ardından DWT işlemi uygulanmaktadır. Bu işlemde, toplamlar sol tarafta, farklar sağ tarafta olacak şekilde gruplanır ve toplamlar düşük frekansları farklar yüksek frekansları temsil etmektedir. Yatay tarama işleminden sonra, pikseller yukarıdan aşağıya dikey yönde taranmaktadır. Komşu piksellerde toplama ve çıkarma işlemleri gerçekleştirilmektedir. Sonrasında toplam üstte ve fark altta saklanmaktadır. Bu işlemlerden sonra, LL, HL, LH ve HH olarak ifade edilen dört alt bant elde edilmektedir. Bu bantlar kullanılarak, gizli mesaj seçilen yöntem ile saklanmaktadır. Sonrasında ters DWT yapılarak stego görüntü elde edilmektedir (Po-Yueh ve Lin, 2006; Gutub ve Al-Shaarani, 2020; Dalal ve Juneja, 2023).

2.2. Kriptoloji

Kriptoloji, bütünlük, kimlik denetimi, gizlilik ve güvenlik üzerinde bilgileri korumak için birincil bir araçtır. Kriptolojinin bu kavramları, bilgi alışverişinde bulunan tarafların arasında istenmeyen herhangi bir üçüncü şahıs olarak da nitelendirilen kulak misafirlerinin bilgileri ele geçirmelerine karşı önlem alınması ve bilgiyi karmaşık hale getirilmesi amacı taşır (Hu, J., & Han, F. 2009). Kriptoloji zengin bir geçmişe sahiptir; ancak günümüzde Blok zinciri teknolojisi ve Nesnelerin interneti (IoT)'nin güvenliğini sağlamaya yardımcı olan bir araç haline gelmiştir. Verilerin güvenli aktarılmasını

sağlamak için birçok uygulama geliştirilmiştir. Kriptografi, sofistike ve sağlam bir algoritma kullanarak verileri şifreli metin adı verilen anlamsız görünen bitlere dönüştürür. Bu, amaçlanan alıcının orijinal mesajı bir kriptografik anahtar aracılığıyla veriyi elde etmesine yardımcı olacaktır. Anahtarı olmayanlar için, şifrelenmiş mesaj anlamsız kodlardan oluşan bir akış olarak görünecektir (Bender, Gruhl, Morimoto, & Lu, 1996). Şifreleme algoritmalarında gereken temel adımlar Şekil 2.3'deki şemada gösterilmiştir.



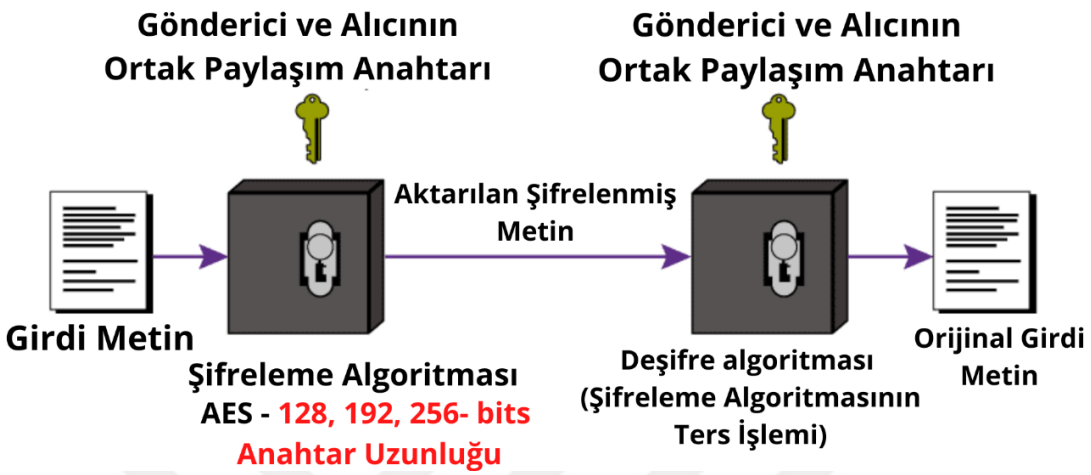
Şekil 2.3. Kriptografinin çalışma mantığı

2.2.1. Simetrik (Özel Anahtarlı Algoritmalar)

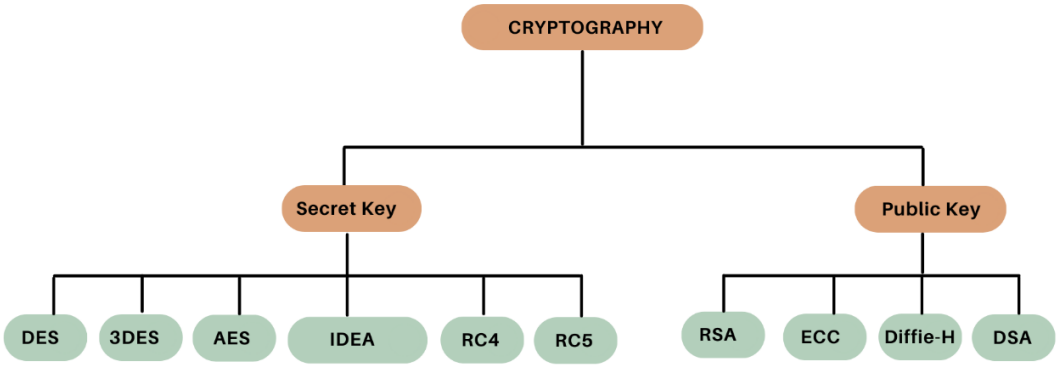
Gizli anahtar algoritmaları olarak da adlandırılan simetrik anahtarlı kriptoloji algoritmaları aynı şifreleme anahtarı kullanarak bilgiyi gizli ve anlaşılamaz hale getirmektedir. Simetrik anahtarlı algoritmalarda taraflar tarafından paylaşılan şifreleme anahtarın gizliliği çok önem arz etmektedir, yani bu tek anahtarın açığa çıktığı halde verinin gizliliği de deşifre olabileceği anlamına gelmektedir.

Şekil 2.4 'de Özel anahtarlı şifrelemenin genel şeması gösterilmiştir. Akış şemasında da gösterildiği gibi gönderici kişinin şifrelemiş olduğu bilgiyi alıcıya göndermek üzere ilk önce bir simetrik şifreleme algoritması kullanarak daha sonra anahtar ile veriyi şifreler, sonra şifreli bilgiyi alıcıya aktarır. Alıcı ise aynı gizli anahtarı kullanarak simetrik şifreleme algoritmasının ters işlemini uyguladıktan sonra bilgiyi elde etmektedir. Simetrik şifreleme algoritmalarından biri olan blok şifreleme düz metni blok bazlı işlenir ve daha sonra şifreleme algoritmalarının işlemi uygulanmaktadır. Blok şifreleme algoritmaların

en yaygını olanlardan sırasıyla Veri Şifreleme Standardı (DES), İleri Şifreleme Standardı (AES), 3DES bunlardan sadece birkaçıdır. Şekil 2.5' de şifreleme algoritmalarına ait sınıflandırılma sunulmaktadır.



Şekil 2.4. Özel anahtarlı şifreleme süreci



Şekil 2.5. Şifreleme algoritmaları

2.2.2. Asimetrik (Açık Anahtar Bazlı Algoritmalar)

Asimetrik şifrelemede iki adet anahtar vardır. Bu şifreleme yönteminde, ilk anahtar genel veya açık anahtar olarak adlandırılırken diğeri özel veya gizli anahtar olarak bilinmektedir. Genel anahtar şifreleme veya doğrulama işlemleri için kullanılmaktadır. Özel anahtar ise, şifreli metnin çözülmesi veya imzalama için kullanılmaktadır. Özel anahtar sadece sahibi tarafından bilinirken, genel anahtar dağıtılan diğer kişiler tarafından bilinmektedir. Gizli bilgi, özel anahtar ile şifrelenmektedir. Genel anahtara sahip olan kişiler şifrelenmiş gizli

bilgiyi açarak okuyabilirler. Özel anahtar ile genel anahtar elde edilmektedir, ancak tersi bir durum söz konusu değildir. Asimetrik şifreleme, gizlilik, anahtar paylaşımı ve inkâr edilemezlik için kullanılmaktadır. Simetrik şifrelemeye göre daha yavaş olduğundan, asimetrik şifreleme anahtar değişinde yaygın olarak kullanılmaktadır. Literatürde, RSA, Diffie-Hellman ve Eliptik Eğri Kriptolojisi gibi asimetrik şifreleme yöntemleri yaygın kullanılmaktadır (Kocher, 1996; Ahmed ve diğ.,2022).

2.3. Literatür Taraması

Kriptoloji, bütünlük, kimlik denetimi, gizlilik ve güvenlik üzerinde bilgileri korumak için birincil bir araçtır. Kriptolojinin bu kavramları, bilgi alışverişinde bulunan tarafların arasında istenmeyen herhangi bir üçüncü şahıs olarak da nitelendirilen kulak misafirlerinin bilgileri ele geçirmelerine karşı önlem alınması ve bilgiyi karmaşık hale getirilmesi amacı taşır (Hu, J., & Han, F. 2009).

Günümüzde sayısal verinin artmasıyla beraber bilgi güvenliğinin önemi her geçen gün artmaktadır. Dolayısıyla veri gizleme konusunda yapılan akademik çalışmaların da son yıllarda arttığı görülmektedir. Bu bölümde, frekans domaininde veri gizleme konusunda gerçekleştirilen son yıllardaki çalışmalar sunulmaktadır.

Örtü nesneleri amaca göre yer değiştirirken en yaygın kullanılan görüntü steganografisi gizli bilgiyi görüntünün piksellerinde yerleştirilmektedir (Li, He, Huang, & Shi, 2011; Shejul & Kulkarni, 2011). Steganografinin uygulama alanları çok geniştir, en yaygın alanlardan biri de istihbarattaki gizli haberleşme ve askeri haberleşme sistemlerinde güvenliği sağlamak için kullanılan yöntemler den biridir. Steganografinin filigranlama ile birleştirilmiş biçimi de fikir ve mükiyeti korumak için aynı zamanda parmak izleri alma yöntemlerinde yaygın olarak kullanılmaktadır (Morkel, Eloff, & Olivier, 2005). Filigranlama ve steganografi bilgi gizleme için kullanılmaları bakımından bazı temel benzerlikleri paylaşsa da, çok farklı uygulamalara hitap ederler. Steganografide, kapak görseli yalnızca bir tuzaktır ve gizli mesajla hiçbir ilişkisi yoktur. Filigran ise aksi söylenebilir, genellikle kapak resmi hakkında ek bilgiler içerir örneğin: gönderici veya alıcıyı tanımlayan etiketler gibi kapakla görsel ile ilgli bazı verileri taşır (M. Barni ve F. Bartolini, 2004), (I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, 2007), (K. Petrowski, M. Kharrazi, H. T. Sencar, and N. D. Memon. Psteg, 2005).

Steganografide bilginin iletilmesinde önemli rol oynayan üç kriter vardır. Bu kriterler ortam uygunluğu, inkâr etmeme ve algılanamazlıktır. Gizlenen verinin insan görsel duyu sistemi tarafından algılanamaz olması hedeflenir.

Zhu ve ark., tarafından 2021 yılında yapılan çalışmada, JPEG sıkıştırmasına ve istatistiksel algılamaya direnen bir veri gizleme yöntemi önerilmiştir. Görüntü sıkıştırma ve sıkıştırmayı açma sürecini analiz ederek bir özellik bulmuş ve bu özellik "JPEG nicemlemeli DCT katsayılarının sıfır olmayan değişmezliği" olarak adlandırılmıştır. Önerilen yöntem ile, "sıfır olmayan son JPEG nicemlemeli DCT katsayılarının konum değişmezliğini" iyi bir şekilde kullanarak JPEG sıkıştırma saldırılarına karşı dayanıklı hale getirilmiştir. Ayrıca veri gizlemek için belirli kurallar kullanılarak en uygun gömme pozisyonu bulan bir fonksiyon önerilmektedir. Çalışmada sunulan deneysel sonuçlar, önerilen yöntemin yüksek güvenilirliğini ve JPEG sıkıştırma ve istatistiksel algılamada sağlamlığını göstermektedir (Zhu ve ark., 2021).

Wang ve ark., 2021 yılında yapmış oldukları çalışmada, sıfırdan farklı DCT katsayılarının konumunu ve diferansiyel Manchester kodunu birleştirerek, konum özelliklerini üreten görüntünün sağlam alanını tespit ederek mesajı gizleyen sağlam bir steganografi yöntemi tasarlamışlardır. Bu yöntem, JPEG sıkıştırma saldırılarından sonra gizli mesajın tamamen çıkarılmasına katkıda bulunarak sağlamlık performansını arttırmıştır. Önerilen algoritma, çeşitli sosyal medya platformlarına uygulanabilmekte ve yalnızca JPEG sıkıştırma saldırılarını içeren kanal işleme işlemlerine karşı koyabilmektedir. Aynı zamanda, tekrarlanan sıkıştırma veya zorla sıkıştırmadan sonra gizli mesaj tamamen çıkarılabilmektedir (Wang ve ark., 2021).

Abdirashid ve ark., tarafından 2022 yılında yapılan çalışmada, frekans dönüşüm alanına dayalı veri gizleme tekniklerinden DCT ve DWT teknikleri gerçekleştirilmiş ve sonuçlar elde edilmiştir. Yapmış oldukları bu çalışma sonuçlarına göre stego görüntüdeki bozulmayı en aza indirilmekte ve örtü görüntüsünde maksimum veri gizleme kapasitesi elde edilmektedir. Çalışmada sunulan deneysel sonuçlar, gizli mesajların başarılı bir şekilde stego görüntüden elde edildiğini göstermektedir. Ayrıca deneysel çalışmalara göre PSNR değeri ortalama 50 dB'in üzerinde olduğu sunulmuştur (Abdirashid ve ark.,2022).

Baziyad ve ark., 2022 yılında yapmış oldukları çalışmada, veri gizleme kapasitesi ile

stego görüntü kalitesi ödünleşmesini etkili bir şekilde kontrol edecek yeni bir veri gizleme yöntemi sunulmaktadır. Bu yöntem, DCT katsayılarını ve polinom eğrisi yöntemini birleştirmektedir. İletişim maliyetini azaltmak için önerilen bu algoritma, önemli ve az önemli DCT katsayıları arasında bir polinom oluşturulmasını sağlamaktadır (Baziyad ve ark., 2022).

Song ve ark., 2022 yılında yapmış oldukları çalışmada, görüntü sıkıştırmaya direnebilen ve gömülü gizli mesajı sıkıştırılmış stego görüntüden doğru bir şekilde çıkarabilen sağlam bir JPEG steganografi algoritması önerilmiştir. Shearlet dönüşümü, DCT ve SVD'nin avantajlarını birleştirerek etkili ve sağlam veri gömme alanı yöntemi önerilmiştir. Yazarların yaptığı deneysel sonuçlar, önerilen JPEG steganografi algoritmasının, son teknoloji sağlam steganografi algoritmalarının aksine, rekabetçi sağlamlık ve algılama önleme yeteneği elde edebildiğini göstermektedir. Ayrıca stego görüntüsü WeChat gibi sosyal medya platformu tarafından sıkıştırılmış olsa bile gizli mesajı doğru bir şekilde çıkarabilmektedir (Song ve ark., 2022).

Sabeti ve Aghabagheri tarafından 2022 yılında yapılan çalışmada, GA-Shield adı verilen yeni bir yöntem önermiş olup, katsayı büyüklüğüne göre nicelenmiş DCT katsayılarına farklı sayıda bit gömülerek gizli mesaj bitlerini en uygun katsayılarda yaymak için kullanmaktadır. Yöntemde bozulmaları aza indirmek için genetik algoritma kullanılmaktadır. Önerilen yöntem, kapak görüntüsüne ortalama 300 ila 20.000 bit veri gömebilir, PSNR değeri 65 ila 40 aralığında ve SSIM değeri 0.985'in üzerinde olan stego görüntüsünü üretilebilmektedir (Sabeti ve Aghabagheri, 2022).

2023 yılında Melman ve Evsutin tarafından yapılan çalışmada, Ayrık Fourier Dönüşümü'nün (Discrete Fourier Transform - DFT) faz spektrumunda en iyi gömme seçeneklerini bulmak için metasezgisel optimizasyon algoritmalarının verimliliği üzerine kapsamlı bir çalışma sunmuşlardır. Yazarlar çalışmasında, geliştirilmiş DFT tabanlı veri gizleme algoritması önermişler ve meta sezgisel optimizasyon kullanmışlardır. Çalışmada kullanılan, meta sezgisel optimizasyon kullanımı, PSNR değerinde ortalama %2–%6 ve kapasite değerinde ortalama %16–%25 oranında bir artış sağlamıştır (Melvan ve Evsutin, 2023).

Chowdhuri ve ark., 2023 yılında yapmış oldukları çalışmada, Destek Vektör Makinesi

(Support Vector Machine - SVM) ve Tam Sayı Dalgacık Dönüşümü (Integer Wavelet Transform - IWT) tekniklerini kullanarak tıbbi görüntüler üzerinde, görüntü steganografisi için etkili bir kimlik doğrulama şeması sunmaktadırlar. Tıbbi görüntüdeki ilgi alanı ve ilgili alanı olmayan bölgeleri ayrıştırmak için SVM kullanılırken, tıbbı görüntüdeki ilgi alanı olmayan bölgeye gizli veriyi saklamak için IWT kullanılmaktadır (Chowdhuri ve ark., 2023).Bilinen Stego Saldırısı: Örtü ve stego nesneleri bilinmektedir.

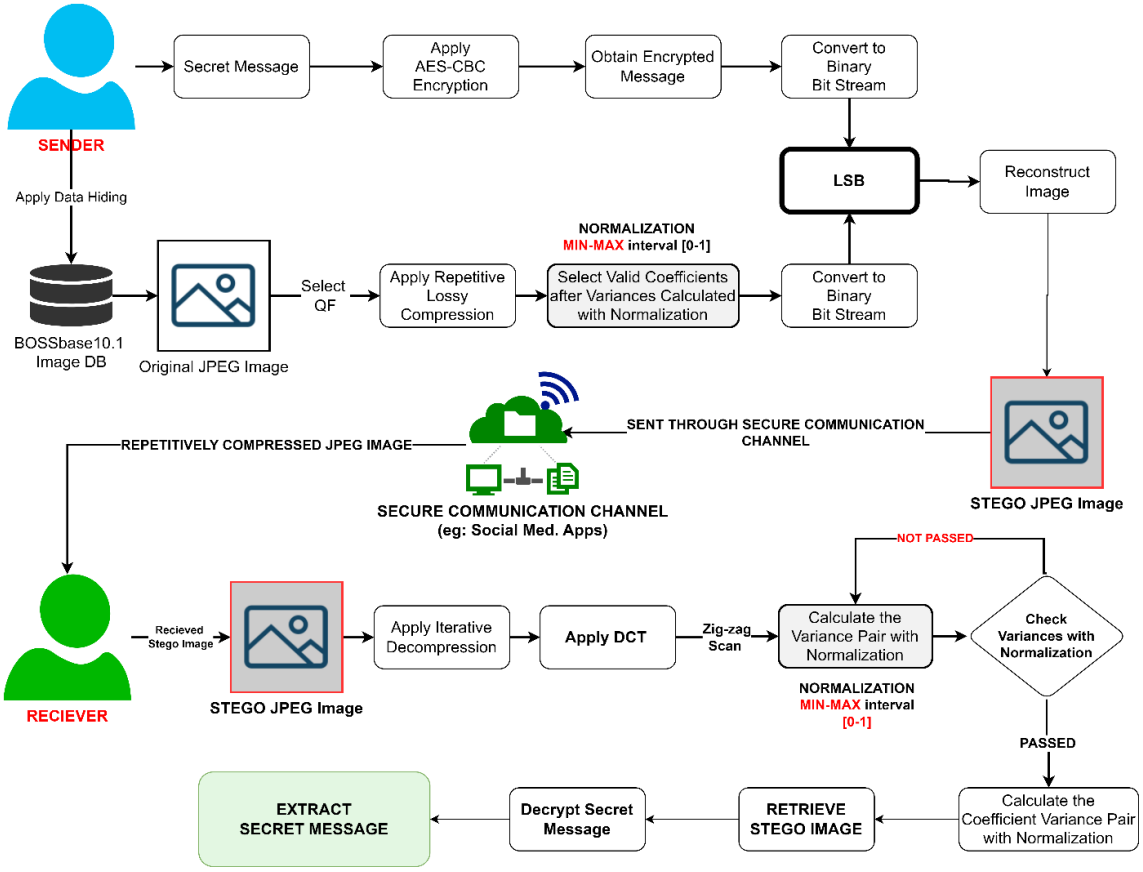
3. ÖNERİLEN METOD

Tez çalışması kapsamında, veri güvenliğini sağlamak amacıyla, veri şifreleme ve veri gizlenme içeren tekrarlı sıkıştırma ataklarına dayanıklı bir yöntem sunulmaktadır. Yöntem bilgileri şifrelemek için öncelikle gizli mesajı simetrik kriptografi algoritmalardan biri olan AES-CBC ile şifrelendikten sonra şifreli mesajı bir örtü görüntüde gömülmek üzere ikili sayı dizisi (binary-bit) haline getirilerek görüntü steganografi algoritmaları ile entegre edilmektedir. Bu şekilde şifreleme aşmasında AES-CBC algoritması yüksek hızda kimliği doğrulama ve veri bütünlüğünü korunmasını sağlar.

Veri gizleme süreci ise şifreli bilgilerin görüntüye gömülmesi için steganografi algoritmaları kullanılarak gerçekleştirilmektedir. Görüntü steganografi tekniklerinin en büyük hedeflerinden bazıları da veri gömme kapasitesini arttırarak, kapak resminin boyutunu olabildiğince en aza indirgeyerek, stego görüntünün kalitesini korumak, olası steg-analiz atakları ve sıkıştırma yöntemlerinin hedefi uygulanmasına karşı önlem alınmasıdır. Bu karakteristikleri gerçekleştirmek için bazı ön-hazırlıkları yapmakta fayda vardır: JPEG sıkıştırma algoritması birçok görüntü işleme alanlarında çok yaygın kullanılmaktadır. Önerilen yöntemde, görüntüdeki uygulanan sıkıştırma öncesi ve sonrası piksellerin DCT katsayılarının nasıl değiştiğini aşama-aşama varyanslarını incelemek ve çıkan sonuca göre sıkıştırma işlemlerinden etkilenmeyen katsayıları seçilerek, veri gömme kapasitesini arttırmak için en uygun katsayılarına karar verilip etkin bir sonuç elde edilerek literatürdeki ilgili benzer yöntemler ile karşılaştırılmaktadır.

Literatürdeki yöntemlerde, yukarıda belirtilen karakteristikler, dosya boyutu artışını azaltırken görsel görüntü kalitesini ve veri gizleme kapasite artışı geliştirmeye çalışsa da sonuçlar tatmin edici değildir. Bu tez kapsamında sunulan yöntemin daha önce literatürde var olan özelliklerden ziyade, kapasiteyi artırırken bir yandan da gizli veriyi taşıyan stego görüntüsünün algılanamaz özelliğini koruması için yüksek frekanslara sahip olan sıfırdan farklı (No-zero AC coefficients) AC DCT katsayılarının varyanslarını hesaplanarak tekrarlı sıkıştırmadan etkilenen ve veri gömme için uygunluk sağlamayan katsayıları fark etmeyi sağlamaktadır. Bu sayede katsayılara uygulanan [0-1] (Min-max) normalizasyon aralıkları ile saklanmak istenen veriye varyans değerleri eşleştirilerek belirlenen aralıklara göre koşulları sağlayıp veri gömme işlemi uygulanmaktadır. Veri gizleme aşamasında kullanılacak olan örtü görüntüleri BOSSbase-1.01 veri tabanından referans

alınarak uygulanmaktadır. Önerilen yöntemin genel yapısı itibariyle Şekil 3.1'de gösterilmektedir.



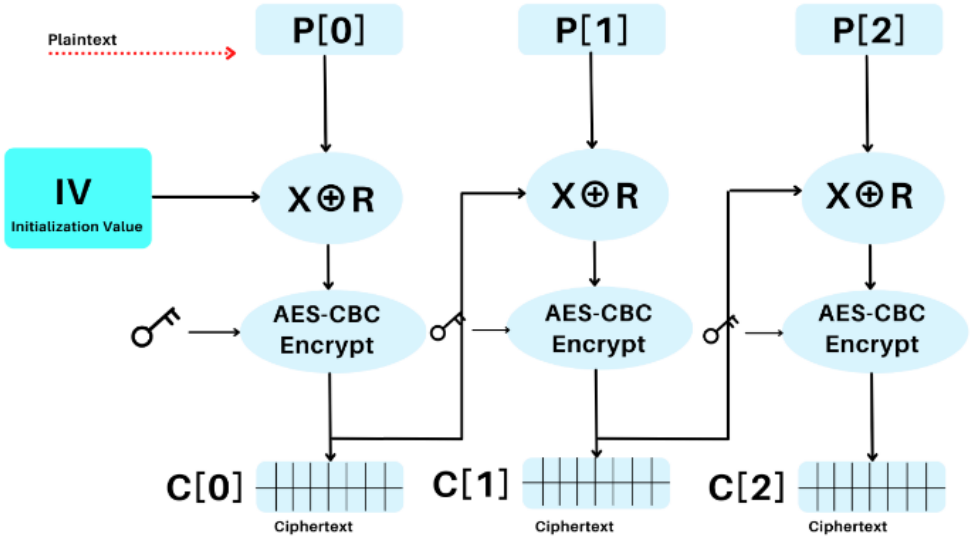
Şekil 3.1. Önerilen Metot Genel Şema

Şekil 3.1'de görüldüğü üzere, bir göndericinin ileteceği gizli mesaj, şifreleme aşamasından başlayarak veri gizleme ve çıkarma aşamasına kadar genel olarak sunulmaktadır. Önerilen yöntemde çift katmanlı adlandırılmasından kasıt şifreleme ve veri gizleme aşamalarının olmasından ibarettir. Günümüzde haberleşme sırasında veri akışı yaygın olarak sosyal medya platformları üzerinden gerçekleştirilmektedir. Bu sebeple pek çok yaygın platform veya uygulama, verilere uçtan uca şifreleme uygularken, aynı veriyi her gönderim aşamasında verinin türü (Örn. Görüntü, Ses, Video) ve kalite faktörlerine göre iteratif sıkıştırma uygulamaktadır. Bunları gerçekleştirirken, verinin boyutu, kalitesi ve veri bütünlüğünü sağlamayı hedeflenmektedir. Bu vesile ile şemada da gösterildiği gibi gönderilmesi hedeflenen gizli mesaj öncelikle şifrelenmekte, ardından şifreli metni gizlemek üzere frekans domain steganografisi ile belirtilen yöntem kullanılarak stego bir görüntü üretilmektedir. Keza iletilen gizli veriyi geri elde edilmek

üzere alıcı tarafından işleme alınmaktadır. Bu aşamalar detaylı olarak bir sonraki bölümlerde anlatılmaktadır.

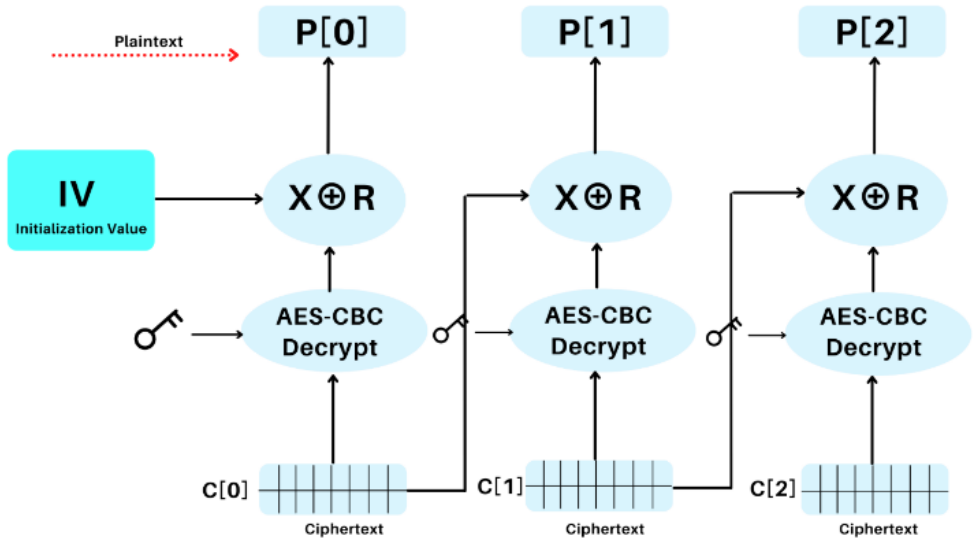
3.1. Blok Zinciri Şifreleme (AES-CBC)

AES-CBC, gelişmiş AES blok şifreleme olduğundan verilerin girişi 128-bit uzunluktan oluşan bir blok olması gerekmektedir. Bir blok şifreleme oluşturmak için Şekil 3.2'te de gösterildiği gibi bir şifreleme anahtar üretimi standardına tabidir. Öncelikle belirlenen P[0,1,2] metin blokları bir önceki bloklar ile XOR işlemi uygulanarak şifreleme işlemi uygulanır. Elde edilen şifreli metin olan C[0,1] zincir değeri olarak kullanılmak üzere P[1,2] ile XOR işlemi yapılır. Buradan çıkaracağımız yaklaşım ise ilk baştaki metin bloğun bir öncesinde XOR işlemi uygulanacak bir blok olmadığından (initial value, IV) olarak rasgele bir değer üretilir. Belirlenen başlangıç değeri rastgele bir gizli anahtar olması gerekmektedir.

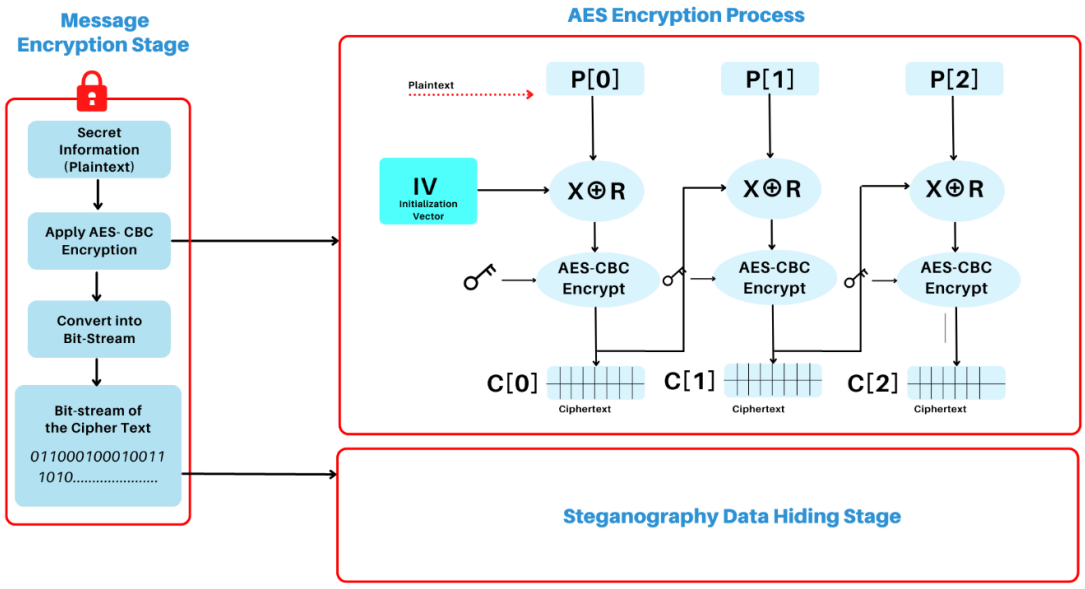


Şekil 3.2. AES blok zinciri şifreleme şeması

Verinin geri elde edilmesi işlemi olan deşifreleme süreci ise şifrelemenin ters işlemidir. Deşifreleme aşaması olarak Şekil 3.3'de gösterilmiştir. Şekil 3.4'te şifreleme ve veri gizleme aşamasının çalışma mantığı sunulmaktadır. Şekilden görüldüğü üzere, mesaj ilk olarak AES-CBC yöntemi ile şifrelenmektedir. Şifrelenmiş bu veri, ikili bit dizisine çevrilmekte ve veri gizleme işlemi yapılmaktadır. Veri gizleme işlemi frekans uzayında DCT katsayılarının varyansı hesaplanarak gerçekleştirilmektedir.



Şekil 3.3. AES blok zinciri deşifreleme şeması



Şekil 3.4. Şifreleme ve veri gizleme blok şeması

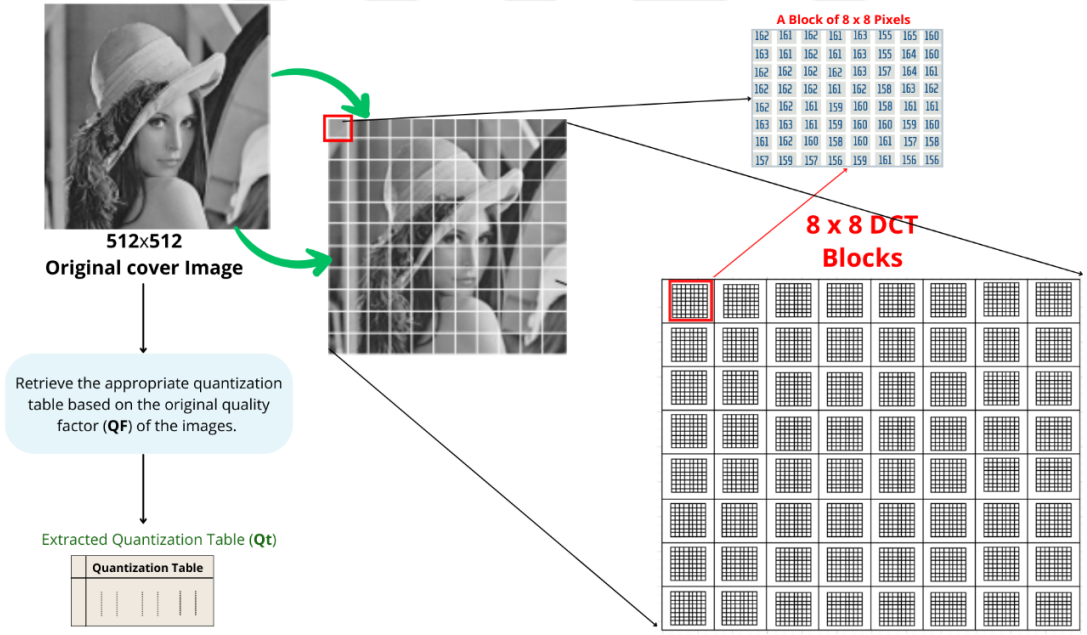
3.2. Veri Gizleme

Veri gizleme aşamasında, örtü görüntünün ön işlenmesinden başlayarak gizli veriyi görüntünün içerisine gömülme sürecine kadar tüm aşamalar detaylı bir şekilde sunulmaktadır. Bu alt bölümde, özellikle yöntemde kullanılan tekrarlı sıkıştırma tekniği detaylı olarak sunulmaktadır.

3.2.1. Örtü Görüntünün Ön-işlenmesi ve JPEG Tekrarlı Sıkıştırma

Veri gizleme aşamasından önce, bu tez kapsamında veriyi saklamak için kullanılan veri tabanı BOSSbase 1.01'in görüntüleri pgm uzantısından JPEG formatına dönüştürülmektedir. Format dönüştürme aşamasında JPEG araçlarından (IJG) yararlanılmaktadır. Görüntülere ön işleme olarak uygulanabilecek teknikler başlıca teknikleri gürültünün resimden temizlenmesi, kontrast ayarının yapılması, kalite faktörlerine dayalı olarak kuantizasyon matrislerinin çıkarılması veya görüntünün belirli bir ölçüye göre yeniden boyutlandırılması gibi işlemlerdir. Görüntü ön işleme sürecine ait akış şeması Şekil 3.5' te sunulmaktadır.

Ön işlemenin temel amacı, kalite faktörünün belirlenerek JPEG sıkıştırma işlemi sürecinde önemli bir rol oynamasını sağlamaktır. Kalite faktörleri, görüntü üzerinde ne kadar sıklıkla sıkıştırma uygulanabileceğini kararlaştırmakta olup, aynı zamanda görüntünün görüntü kalitesi ile dosya boyutu arasındaki dengeyi etkilemektedir.



Şekil 3.5. Örtü görüntü ön işleme süreci

Farklı kalite faktörleri, sıkıştırma sırasında frekans katsayılarına uygulanan kuantizasyon (nicemleme) düzeyini belirleyen farklı kuantizasyon matrislerine karşılık gelmektedir. Kuantizasyon matrislerine baz alınarak çeşitli kalite faktörlerinin görüntülerden elde edilmesi işlemi aşağıdaki adımlar ile anlatılmaktadır. Bu tez çalışması kapsamında

önerilen yöntemde kullanılan kalite faktörleri (50, 65, 75, 85, 90, 95) olarak belirlenmiştir.

Adım 1 : JPEG formatında görüntünün alınması :

- Görüntünün boyutu 512×512 piksellerden oluşup BOSSbase 1.01 ten seçilmiştir.
- Görüntüye JPEG sıkıştırma algoritmasını uygulamak için 8×8 bloklara bölünüp her bloğa ayrı-ayrı DCT uygulanmaktadır.
- Elde edilen frekans katsayılarına kuantizasyon matrisi bölerek nicemleme (quantization) işlemi yapılır.
- Nicelme matrisindeki yüksek değerler, daha yoğun bir kuantizasyona yol açarak daha yüksek sıkıştırma ve potansiyel olarak daha düşük görüntü kalitesi ile sonuçlanır.
- Katsayılar, kuantizasyon uygulanmış halde öncelikle kodlanır ve nihai JPEG görüntüsünü üretmek için sıkıştırılır.

Adım 2 : Kuantizasyon matrisleri :

- Farklı kalite faktörleri, JPEG sıkıştırmasında farklı nicemleme matrislerine karşılık geldiği anlamına gelir.
- Nicemleme matrisindeki her giriş, nicemleme için kullanılan adım boyutunu temsil eder.
- Daha yüksek kalite faktörleri, yoğunluğu daha az nicemleme ve daha iyi görüntü kalitesi sağlar.
- Düşük kalite faktörleri, daha yüksek sıkıştırma için görüntü kalitesinden ödün vererek daha yoğun ve agresif nicemleme sağlar.

Adım 3 : Kalite faktörlerin belirlenmesi ve görüntüden elde edilmesi :

- Belirlemiş olduğumuz kalite faktörleri 50, 65, 75, 85 ve 90, ilgili nicemleme matrislerini kullanarak sıkıştırma gerektirir.
- Her kalite faktörü, belirli adım boyutlarına (yüksek veya düşük kalite faktörü) sahip farklı bir nicemleme matrisine karşılık gelir.
- Orijinal görüntü, istenen kalite faktörü için karşılık gelen nicemleme matrisi kullanılarak sıkıştırılır.
- Her kalite faktöründe ortaya çıkan sıkıştırılmış görüntüler, sonraki veri gizleme veya işleme için kullanılabilir.

Görüntüdeki kalite faktörü azaldıkça (düşük kalite), sıkıştırma oranı artarken görüntü kalitesinin düştüğünü yukarıdaki adımlar ile vurgulanmıştır. Düşük kalite faktörleri, daha agresif nicemleme (quantization) ile sonuçlanarak daha yüksek sıkıştırmaya yol açar, ancak potansiyel olarak fark edilebilir görüntü ayrıntıları kaybı ve artan sıkıştırma artefaktlarının oluşmasına yol açabilmektedir. Daha yüksek kalite faktörleri daha fazla görüntü detayını korur ancak daha büyük dosya boyutlarına neden olur. Görüntü ön işlenmesinin tekniklerinden biri olan sıkıştırma işlemi görüntünün veri gizleme uygulanmadan önce kalitesini en uygun halini ayırt etmek veya stego görüntüsünün algılanamaz özelliğini en yüksek seviyeye çıkarmak gibi işlemleri içermektedir.

3.2.2. JPEG Dönüşüm Formatı

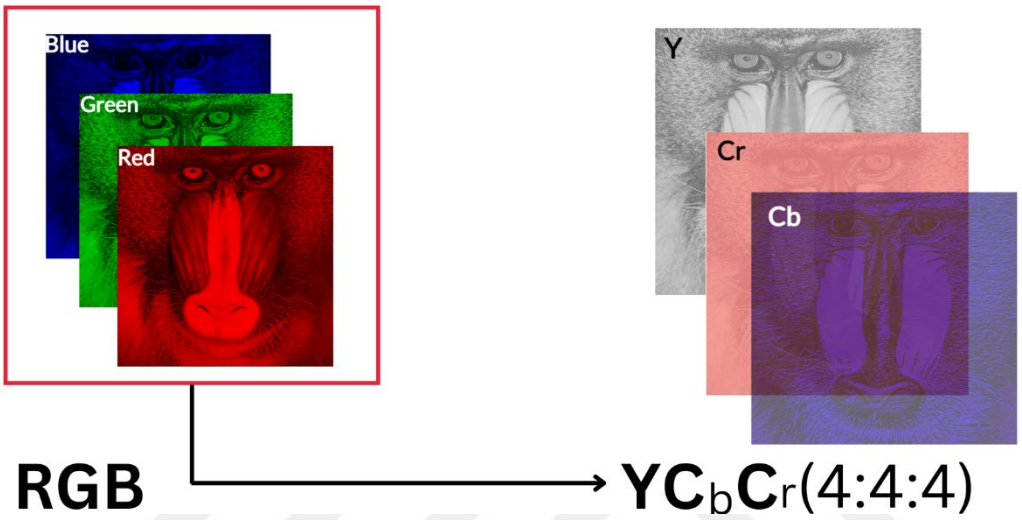
İnsan görsel algılama sistemi (HVS) doğal görüntüleri piksel matrisleri yerine dokuyla dolu bir segment koleksiyonu olarak algılamaktadır. Özellikle insan, nesneler üzerinde yapılan testler, görsel sistemimizin renkteki küçük değişikliklere veya yüksek uzamsal-frekanslı gürültüye karşı oldukça duyarsız olduğunu göstermektedir. Bu nedenle, veri sıkıştırma alanında daha verimli birkaç görüntü formatı önerilmiştir. Görüntüyü kolayca sıkıştırılabilir "seyrek" bir biçimde temsil edilebileceği farklı bir alana dönüştürerek çalışabilir. Bu tür formatlar tipik olarak (Lossy) yani kayıplıdır, yani format dönüştürme, normal görüntüleme koşullarında algılanamayan bir miktar algısal kayıp beraberinde getirir. Günümüzde en yaygın kullanılan iki dönüşüm, Ayrık Kosinüs Dönüşümü (DCT) ve Ayrık Dalgacık dönüşümü ‘dür (DWT). DCT, JPEG formatının kalbidir, DWT ise JPEG2000'de kullanılır. JPEG sıkıştırma yönteminde uygulanan aşamalar bu bölümün bir sonraki başlıklarında yer verilmiştir.

3.2.3. JPEG Renk Dönüşüm Kanalları

JPEG formatındaki görüntünün oluşumunda katkıda bulunan renk kanalı, RGB modelinden YCbCr modeline dönüştürülür. Bu adım gerekli olmasa da (JPEG doğrudan RGB temsiliyle çalışabilir), fakat YCbCr aynı doğrulukta daha yüksek sıkıştırma oranları sağladığı için tipik olarak kullanılır. İnsan gözü, renkteki değişikliklere parlaklıktan daha az duyarlı olduğu için, krominans sinyalleri, Cr, Cb, daha yüksek bir sıkıştırma oranı elde etmek için DCT uygulanmadan önce tipik olarak alt örnekleme yapılır. Bu, başlangıçta görüntüyü 16 × 16 piksellik makro bloklara bölerek uygulanır. Her makro blok, dört adet 8 × 8 parlaklık (lumen) bloğu ve makro bloktaki krominansın nasıl alt-örneklendiğine

bağlı olarak her bir renklilik için 1, 2 veya 4 blok üretir.

Her yönde 2 faktör ile alt örnekleme yapılırsa, her makro blok yalnızca bir 8 × 8 krominans Cr bloğuna ve bir krominans Cb bloğuna (ve tabii ki dört parlaklık bloğuna) sahip olacaktır. Şekil 3.6'da RGB formatında bulunan bir görüntünün, YCrCb formatında ifade edilmesi sunulmaktadır.



Şekil 3.6. JPEG renk dönüşüm kanalları

Bu genellikle kısaltılmış bir biçimde 4:1:1 yazılır. Hiçbir krominans sinyali alt örneklemeli değilse, 4:4:4 dizini ile temsil edilir. Hem Cr hem de Cb yalnızca bir yönde alt örneklenebilir, bu da her makro blokta 4:2:2 iki renklilik 8 × 8 bloğa yol açar. Cr'nin yalnızca bir yönde alt örneklemesi ve Cb'nin her iki yönde (4:2:1) alt örneklemesi gibi başka olasılıklara da format tarafından izin verilir.

3.2.4. Ayrık Kosinüs Dönüşümü

Ayrık kosinüs dönüşüm alanı (DCT)'da YCrCb sinyallerindeki her bloğu uzamsal alanından frekans alanına dönüştürmektedir. DCT 8 × 8 piksel matrislere baz alınarak dönüşümü sağlanmaktadır. DCT, ayrık fourier dönüşüm (DFT) alanına benzer, fakat sadece reel sayılar kullanmaktadır. Uygulamaya misal olarak, B [i, j] matrisi, i, j = 0,1,2, ..., 7, (8 × 8) piksel bloklardan oluşan bir DCT değerleri olsun, öyleyse buradaki 8 × 8 piksel blokların DCT katsayıları olan C[k,l], k,l = 0,1,2, ... , 7, aşağıdaki lineer kombinasyon Denklem (3.1) fonksiyonu ile hesaplayabiliriz, C[0,0]'deki katsayılara DC , kalan tüm diğer katsayılarına ise k+1 > 0 olacak şekilde AC olarak ifade edilir. Bir DCT

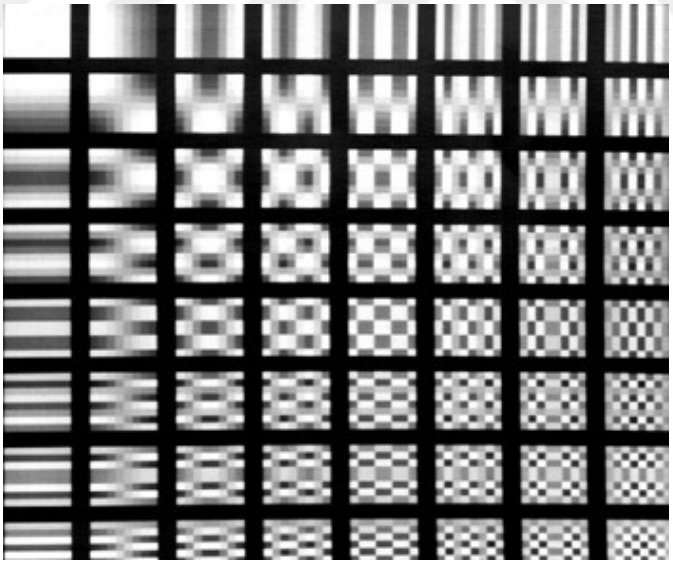
dönüşümünün sonuçları, matristeki indekse karşılık gelen ayrık frekanslarda orijinal bloğun uzamsal frekans bilgisini temsil eder.

$$\mathrm{DCT}(i,j) = \frac{1}{\sqrt{2N}}\mathrm{C(i)C(j)}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\mathrm{pixel}(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)\mathrm{j}\pi}{2N}\right]$$

$$C(x) = \frac{1}{\sqrt{2}} \text{ if } x \text{ is } 0, \text{ else } 1 \text{ if } x > 0 \qquad (3.1)$$

$$N = 8$$

DCT'nin frekans gösterimi Şekil 3.7'de görülebilir. Sol üstteki elemanların daha düşük frekanslara sahip olduğu, sağ alttaki elemanların ise daha yüksek frekanslara sahip olduğu aşikârdır. Orijinal mesajı içeren gizli bilgilerin çoğu, düşük frekansa sahip katsayılarından kolayca ayırt edilebilir, sebebi ise bu katsayılardaki yüksek enerjili sıkıştırmadan ibarettir. Ayrıca, insan gözü yüksek frekanslı elementlerde oluşan değişiklikleri daha az algılar. Bu faktörler göz önüne alındığında, daha düşük frekans bileşenlerinde değişiklikler veya hatalar oluştuğunda, bunların insan gözü tarafından daha fazla fark edileceği açıkça söylenebilir.



Şekil 3.7. Frekans domain

DCT ters işlem mekanizmaya sahip olduğundan, daha önce sıkıştırma işleminden geçirilen JPEG formatı görüntüden orijinal gizli veriyi içeren bilgiyi dışa aktarmak mümkündür. Bu ters işlemi inverse DCT yani (IDCT) olarak Denklem (3.2) ile ifade edilmektedir.

Bu işlemin uygulanmasından sonra uzamsal domainde yer alan görüntü elde edilir.

$$IDCT(x,y) = \frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} C(x)C(y) * pixel(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (3.2)$$

3.2.5. Nicemleme (Quantization)

Nicemleme (Quatization) işlemi kayıplı sıkıştırmada özellikle JPEG görüntülerde yüksek frekansa sahip olan AC ve düşük frekanslı olan DC katsayılarının birbirinden ayırarak insanların görsel sistemine göre algılanması zor olan görüntüde AC bölgesindeki kritik bilgi kaybın veya değişikliğin fark edilmesini önler. Nicemleme uygulamanın amacı, DCT dönüşümünün elde edilen matrisi bir nicemleme matrisine bölünür ve sonuçlar en yakın tamsayı değerine yuvarlanır. Nicemleme matrisi tamsayı değerlerden oluşur ve buna nicemleme adımı da denir. Nicemleme matrisi DCT dönüşüm bloklarından elde edilen katsayılar matrisine bölünür ve çıkan sonucu en yakın tam sayı değerlerine yuvarlayarak nicemlenmiş (Quantized DCT coefficients) tam sayı katsayıları elde edilir. Nicemleme adımı uygulamanın başka bir amacı da daha az bit kullanarak DCT katsayılarını temsil edebilmektir. Bu nedenle bilgi kaybına yol açar, yani bu, JPEG sıkıştırmanın kayıplı kısmı olarak da adlandırılır. Denklem (3.3) 2-D DCT için nicemleme fonksiyonu hesaplaması gösterilmektedir.

$$D[k,l] = round\left(\frac{d[k,l]}{Q[k,l]}\right), k,l \in \{0,\dots\dots,7\} \quad (3.3)$$

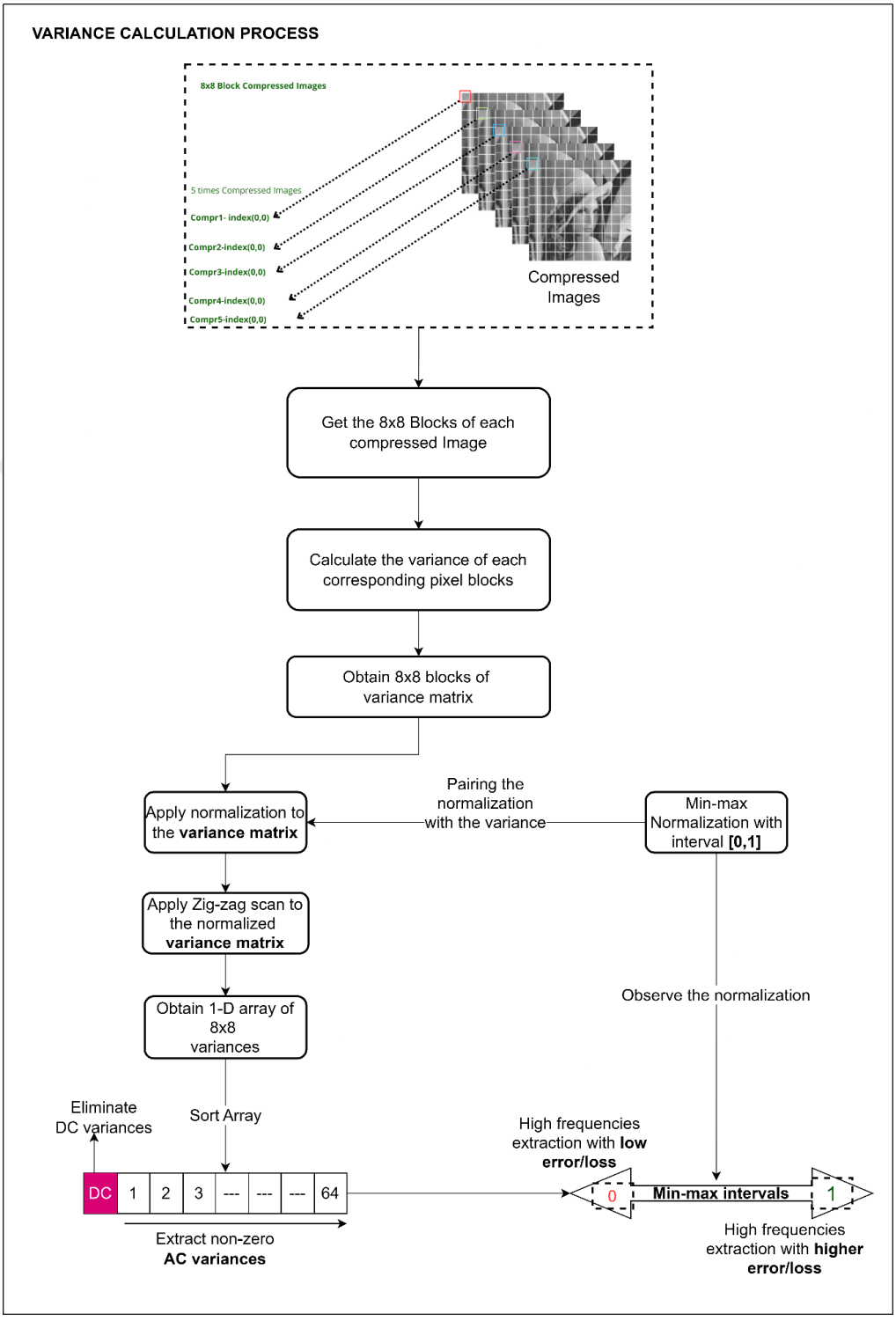
3.3. Sıkıştırılmış Görüntülerin DCT Katsayılarına Varyans Uygulanması

JPEG sıkıştırmasındaki katsayıların varyansların hesaplanmasındaki amaç, öncelikle iteratif biçimde sıkıştırılmış görüntünün kalitesini değerlendirmektir. Bu işlem, sıkıştırma sırasında etkilenmeyen veya kaybolan bilgi miktarına belirlenmesi kullanılır. Varyans, veri noktalarının ortalama değerinin etrafında yayılmasını veya dağılımını ölçer. Bu durumda varyansların sıkıştırılan JPEG görüntülerin üzerinde uygulanmasının ana hedefi, kuantizasyondan sonrası sıfır olmayan AC katsayılarının nasıl değişkenlik gösterdiklerinin gözlenmesidir. JPEG sıkıştırma algoritmasında DCT katsayılarına kuantizasyon uygulanmasının nedeni, görsel açısından daha az önemli olan bilgileri atarak yüksek sıkıştırmayı amaçlar, bu sebepten kaynaklı meydana gelen katsayıların içerdiği bilgilerin kesinlik veya tam olma doğruluk payının kaybolmasına yol açmaktadır.

Varyans uygulama aşamaları aşağıda maddeler halinde sunulmaktadır.

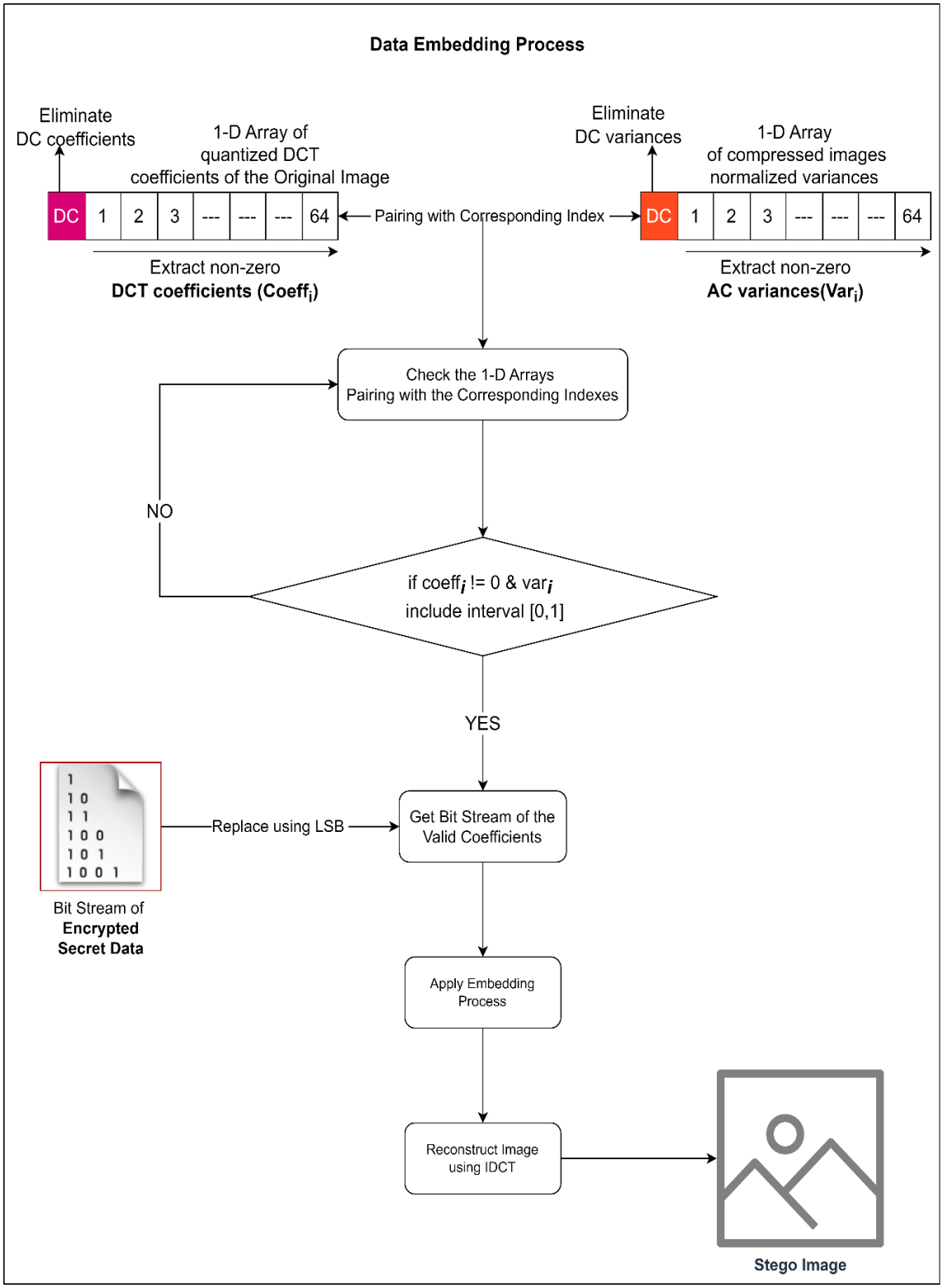
1. Görüntünün alınması:
- Kullanılan görüntü 512×512 piksel boyutundan oluşmaktadır.
2. Görüntünun bloklara ayrılması:
- Görüntüyü 8×8 blocklara böl.
- Her blok (8×8) yani 64 pikselden oluşmaktadır.
3. Ayrık Kosinüs Transform (DCT) uygulanır:
- Her 8×8 bloka ayrı-ayrı DCT'yi uygula.
- DCT görüntünün verilerini uzamsal alanından frekans alanına dönüştürmektedir.
4. Nicemleme (Quantization):
- İstenen kalite faktörüne (50, 65, 75, 85, 90). karşılık gelen nicemleme tablosunu elde edilir.
- Her bir DCT katsayısını nicemleme tablosundan karşılık gelen nicemleme matrisine bölünür.
- Çıkan sonucu en yakın tamsyıya yuvarlanır.
- Görüntünün sıkıştırılmış versiyonunu temsil eden nicelenmiş katsayıları elde edilir.
5. Tekrarlı sıkıştırmayı uygulanmak üzere daha önceden belirlenmiş kalite faktörlerine (50, 65, 75, 85, 90) teker-teker sıkıştırmadan geçirilir.
6. Önerilen yöntemdeki uygulanan sıkıştırma sayısı 5 defa olarak belirlenmiştir.
7. Sıfırdan Farklı AC Katsayıları:
- Kuantize edilen DCT katsayıları arasından sıfırdan farklı AC (Alternate Current) katsayıları belirlenir.
- AC katsayıları, ortalama renk değerini temsil eden DC (Direct Current) katsayısı hariç, görüntünün frekans bileşenlerini veya ayrıntılarını temsil eder.
8. Varyans Hesaplama:
- Sıfırdan farklı AC katsayılarını yinele.
- Sıfır olmayan AC katsayılarının varyansını hesaplanır.
- Varyans, nicemlemeden (quantization) sonra sıfır olmayan AC katsayıları arasındaki değişkenliği veya farklılıkları nicelleştirir.
9. Çıktı Değerlerin 8×8 Varyans Matrisi olarak Elde Edilmesi:
- JPEG-nicelenmiş sıfır olmayan AC katsayılarının varyanslarını elde edin.
- Varyanslar, orijinal sıkıştırılmamış görüntüye kıyasla sıkıştırılmış görüntüdeki

değişkenlik veya bilgi kaybı derecesini temsil eder.



Şekil 3.8. Varyans Hesaplama İşlemi

Şekil 3.8. Varyans Hesaplama İşlemi blok şemasında varyansın nasıl hesaplandığı görselleştirilmektedir.



Şekil 3.9. Katsayıların Varyans ile Eşleştirilmesi ve Veri Gömme İşlemi

Şekil 3.9'da orijinal görüntüsünün katsayılarını kuantize edildikten sonra varyansı hesaplanan sıkıştırma sonrası katsayılarının eşleştirilmesi işlemi gösterilmektedir.

3.4. Varyans Katsayılarının Min-max Normalizasyon ile Eşleştirilmesi

Bir önceki bölümde sıkıştırılan görüntülere ait kuantize sonrası katsayıların varyanslarını ayrı 8×8 matris haline getirilmiştir. Sonraki aşama olan katsayıların varyans değerleri [0-1] min-max intervali ile eşleştirilmesi aşamasıdır. Frekans [0-1] eşleştirmedeki amaç, veri gizleme aşamasında yüksek frekanslı katsayılardan faydalanmak ve sıfıra yakın olan yüksek frekanslı değerlerin veri çıkarılırken daha az hatalı veya veri kaybı çok az olduğunu göstermektir. Bir başka ifade ile maksimum 1 değere yakın olan yüksek frekanslı değerlerin veri çıkarma aşamasında daha yüksek hatalı ve kayıplı veri elde edilebilir olduğunu vurgulamaktır. Varyanslar ve sıfır olmayan AC katsayıların karşılaştırılması yapılırken aşağıdaki denklemden hesaplaması yapılabilir.

$$Min_{Max\,[0-1]} = \frac{Max\ Value_{\,8\times8\ variance} - Current\ Valuex_{8\times8\ variance}}{Max\ Value_{\,8\times8\ variance} - Min\ Value_{8\times8\ variance}} \qquad (3.4)$$

Tablo 3.1. Katsayıların Varyans Yüzdelik Değişim Oranları

512×512 Görüntüdeki Toplam DCT Katsayılar = 262144						
Varyans Matrisine göre Katsayıların Yüzdelik Değişim Oranları [Per_{Coeff}(%)]						
QF	**50**	**65**	**75**	**85**	**90**	**95**
Boss 1	0,073	0,075	0,112	0,122	0,135	0,143
Boss 2	0,084	0,085	0,085	0,099	0,101	0,109
Boss 3	0,115	0,148	0,152	0,160	0,173	0,185
Boss 4	0,067	0,071	0,096	0,096	0,097	0,099
Boss 5	0,195	0,224	0,226	0,229	0,237	0,250
Boss 6	0,157	0,196	0,199	0,212	0,228	0,231
Boss 7	0,267	0,269	0,288	0,289	0,292	0,308
Boss 8	0,096	0,109	0,112	0,115	0,121	0,133
			Az Değiştiren		**Çok Değiştiren**	
Interval Offset Min-max Normalizasyon			**0**		**1**	

Tablo 3.1'de gösterildiği gibi görüntülerin kalite faktörleri baz alınarak sıkıştırma sonrasında hesaplanan AC ve DC katsayılarının varyansları ne kadar oranla yüzdelik olarak değişiklik gösterdiklerini incelenmektedir. Interval offset değerlerimizi belirleyen Min-max [0-1] aralığı normalizasyonumuz Denklem (3.4) ile hesaplandıktan sonra

varyanslarımızdan elde ettiğimiz yüzdelik değişim oranı ile eşleştirme yapmak mümkündür. Burada, 0'a daha yakın tüm yüzdelik oranları katsayıların sıkıştırma sonrasında az değişikliğe uğradığı anlamına gelmektedir. Keza varyans değişimi yüzdelik oranı farkın 1'e daha yakın olması katsayıların görüntü sıkıştırma sonrasında çok değiştiği anlamına gelmektedir. Denklem (3.5)'te katsayıların değişimi oranını yüzdelik olarak gösteren matematiksel denklem yer almaktadır. Tablo 3.2'de Katsayıların Yüzdelik Değişim oranların Değişkenlerini gösteren ifadeler sunulmaktadır.

Tablo 3.2. Katsayıların Yüzdelik Değişim Oranların Değişkenleri

Denklem Notasyonu	
Değişken	**Açıklama**
$Coeff'_{var}$	Sıkıştırma sonrası varyansı hesaplanan ve değişen DCT katsayıların sayısı
Per_{Coeff}	Varyans matrisine göre katsayıların yüzdelik Değişim Oranları
$DCTCoeff_{sum}$	Toplam mevcut DCT katsayıları

$$Per_{Coeff}(\%) = \frac{Coeff'_{var}}{DCTCoeff_{sum}} \times 100 \quad (3.5)$$

Katsayıların varyansları yüzdelik değişim oranları hesaplarken 8x8 orijinal AC-DCT katsayılarının matrisinde ile 8x8 varyans katsayılarına karşılık gelen her indisi eşlettirilmektedir. Daha sonra varyansı hesaplanan ve değişen DCT katsayıların sayısı, orijinal sıfır olmayan AC-DCT katsayılarının toplamına bölünüp yüzdeliği hesaplanmaktadır.

4. DENEYSEL ÇALIŞMALAR

Tez çalışması kapsamında geliştirilen algoritmanın deneysel çalışmaları bu bölümde sunulmaktadır. Yöntem frekans alanında yer alan sıkıştırma algoritması içerdiğinden stego görüntüsü üzerinde gizlenmiş verileri barından sıfırdan farklı AC katsayıların katsayı başına düşen bit sayısının (bit per non-zero AC coefficients- bpnzAC) varyans bazlı iteratif sıkıştırmayı defalarca uygulanarak gizli veriyi elde edilirken ki oluşabilecek kayıp oran bit hata oranı (BER) ile hesaplanmaktadır. Ayrıca çalışmada, cihaz ve sistem olarak Linux tabanlı Parrot OS 5.3 (Electro Ara) işletim sisteminden debian paketleri içerikli Security Edition versiyonundan yararlanılarak, programlama dili olarak da Python 3.8, cihazın işlemcisi olarak AMD64 ve 8 GB RAM hafızaya sahip bir dizüstü bilgisayar kullanılarak gerçekleştirilmektedir. Frekans domainde yer alan DCT görüntü steganografisi ile geliştirilen yöntemde, kullanılan görüntüler 10.000 adet çeşitli görüntüleri sunan BOSSbase1.01 veri setinden 8 adet görüntü ile gerçekleştirilmiştir.

4.1. Deneysel Ön Hazırlığı

Deneysel çalışmasında kullanılan görüntülere öncelikle 512×512 boyutunda JPEG formatı olacak biçimde belirli iterasyona göre (yöntemimizde ×5 iterasyonda) sıkıştırma atakları uygulanmıştır.

Tablo 4.1. Deneysel Ayarları

Deney Ayarları	
Görüntü veriseti kaynağı	Bossbase-1.01
Görüntü boyutu	512×512
Görüntü tipi ve formatı	JPEG gri ton
Sıkıştırma öncesi kalite faktörleri	*QF1=50, QF2=65, QF3=75, QF5=85, QF6=90, QF7=95*
BER	Veri çıkarıldıktan sonraki Hatalı olan Bitlerin Oranı
Gömme yük kapasitesi (Payload capacity bit per non-zero AC coeff bpnzAC)	0,01 ile 0,12 arasında gömme kapasitesidir.
Varyans aralıkları	[0-1]

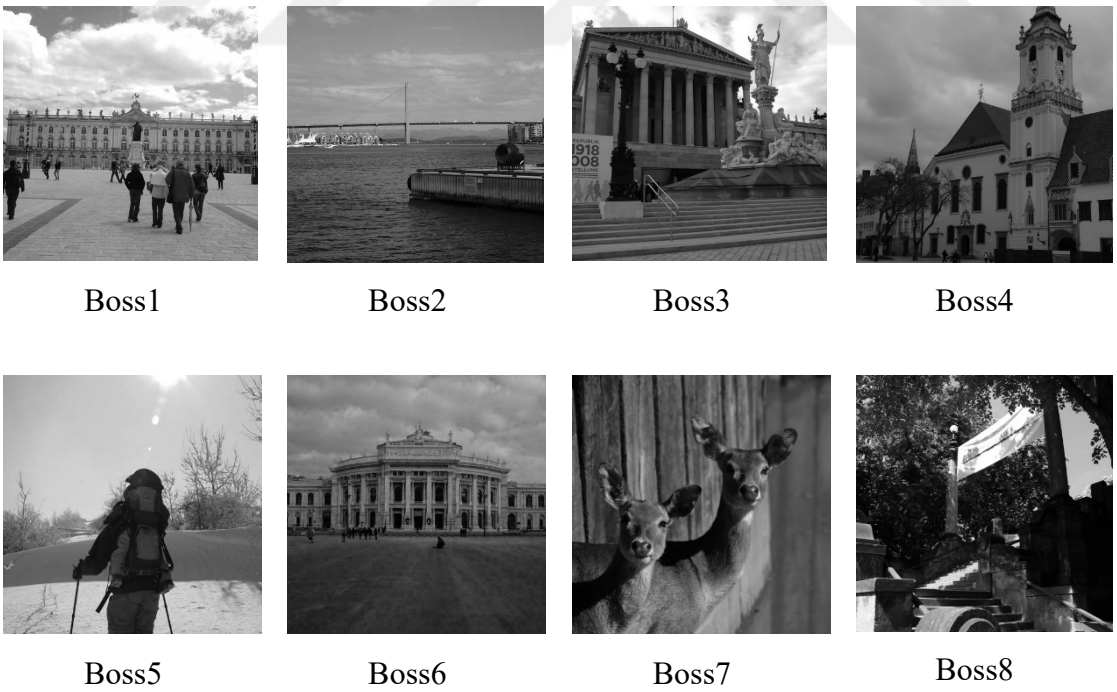
Görüntülerin kalite faktörleri olarak (QF1, QF2, QF3, QF4, QF5, QF6) ayarlanmaktadır. Deneysel çalışmalarda kullanılan diğer ek açıklama ve parametreleri Tablo 4.1'de sunulmaktadır.

4.2. Anti Sıkıştırmaya Dayalı Ataklarına Karşı Deneysel Sonuçları

Deneysel çalışmada kullanılan görünütülerin listesi Şekil 4.1'de yer almaktadır. Görüntüler BOSSbase 1.01 veri setinden örneklem olarak seçilen sekiz farklı aynı boyuttan oluşan görüntülerdir.

Görüntülerdeki katsayıların içerisine gömülen mesajların 0,01-0,12 arasındaki gömme kapasitelerine ve kalite faktörlerine göre varyans aralık değerlerinin değişkenlik gösterdiği sonuçları baz alınarak Denklem (4.1)'deki ile hesaplanan BER sonuçları gösterilmiştir.

$$BER(\%) = \frac{Number\ of\ Error\ Bits}{Total\ Number\ of\ Bits} \tag{4.1}$$



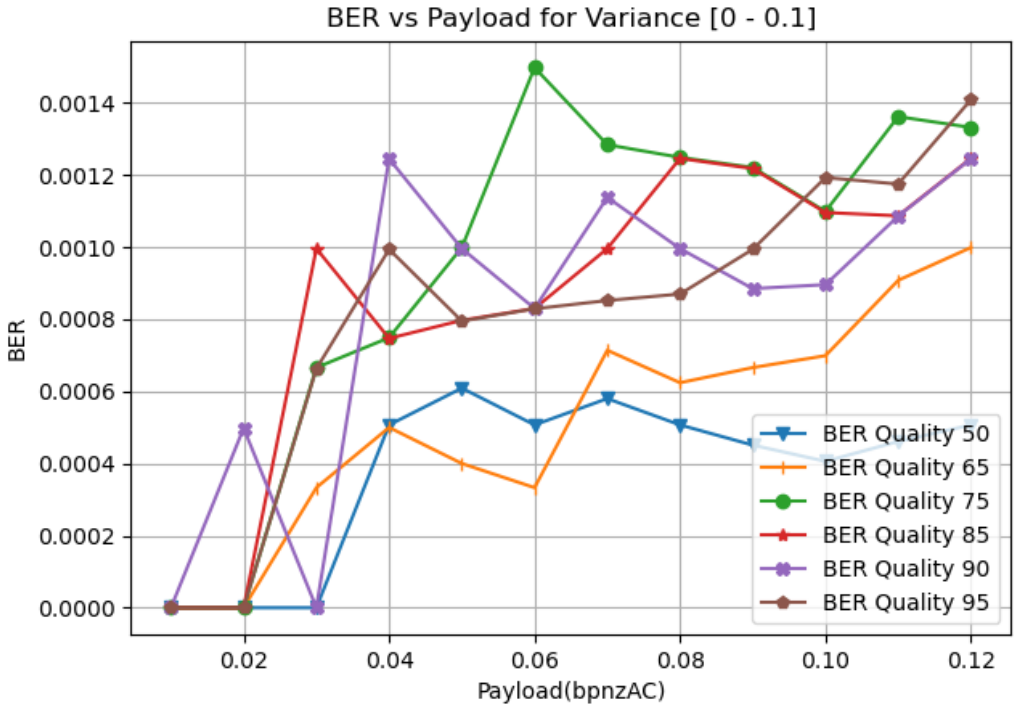
Şekil 4.1. BOSSbase 1.01 Veri tabanı deneysel çalışmada kullanılan görüntüler

Veri tabanın görüntüleri performans ölçütleri tablolar ve grafiklerle ile sonuçları gösterilmiştir.

Tablo 4.2. Boss1 varyans [0-0,1] bazlı bpnzAC BER değerleri

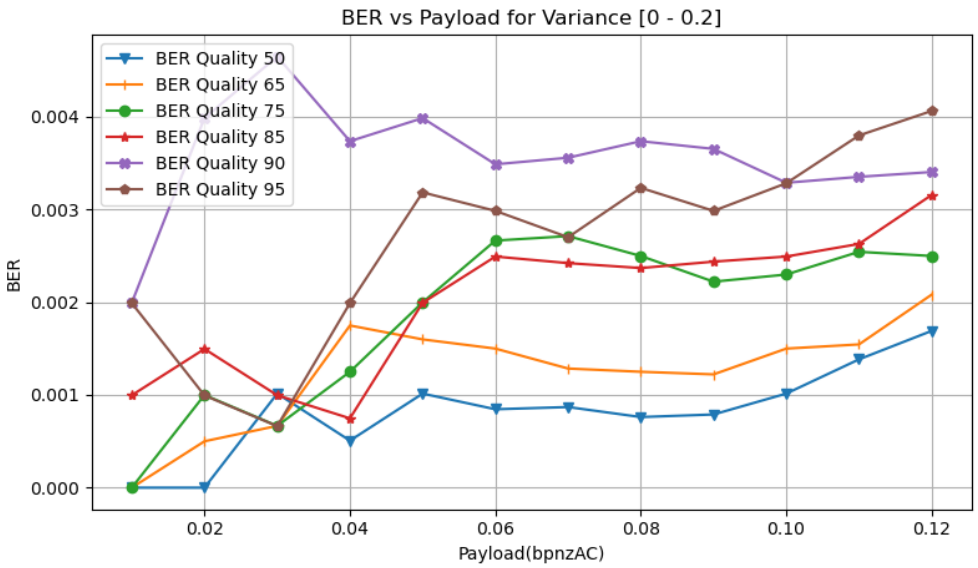
Gizlenen mesajların yük kapasitesine göre(Payload Bit per non-zero AC coefficients) geri elde edilmesi												
Bits / BER per QF	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**	**0,06**	**0,07**	**0,08**	**0,09**	**0,1**	**0,11**	**0,12**
BER QF 50	0	0	0	0,000507	0,000609	0,000507	0,00058	0,000507	0,000451	0,000406	0,000461	0,000507
BER QF 65	0	0	0,000333	0,0005	0,0004	0,000333	0,000714	0,000624	0,000666	0,000699	0,000908	0,000999
BER QF 75	0	0	0,000666	0,000749	0,000999	0,001498	0,001284	0,001249	0,001221	0,001099	0,001362	0,001332
BER QF 85	0	0	0,000996	0,000747	0,000797	0,00083	0,000996	0,001246	0,001218	0,001096	0,001087	0,001246
BER QF 90	0	0,000498	0	0,001245	0,000996	0,00083	0,001138	0,000996	0,000885	0,000896	0,001086	0,001245
BER QF 95	0	0	0,000663	0,000994	0,000795	0,000829	0,000852	0,00087	0,000994	0,001193	0,001175	0,001409

Tablo 4.2'de Boss1 görüntüsünün kalite faktörlerine göre varyans [0 – 0,1] arasındaki BER değerleri sunulmaktadır



Şekil 4.2. BER vs Varyans [0 – 0,1] Grafiği

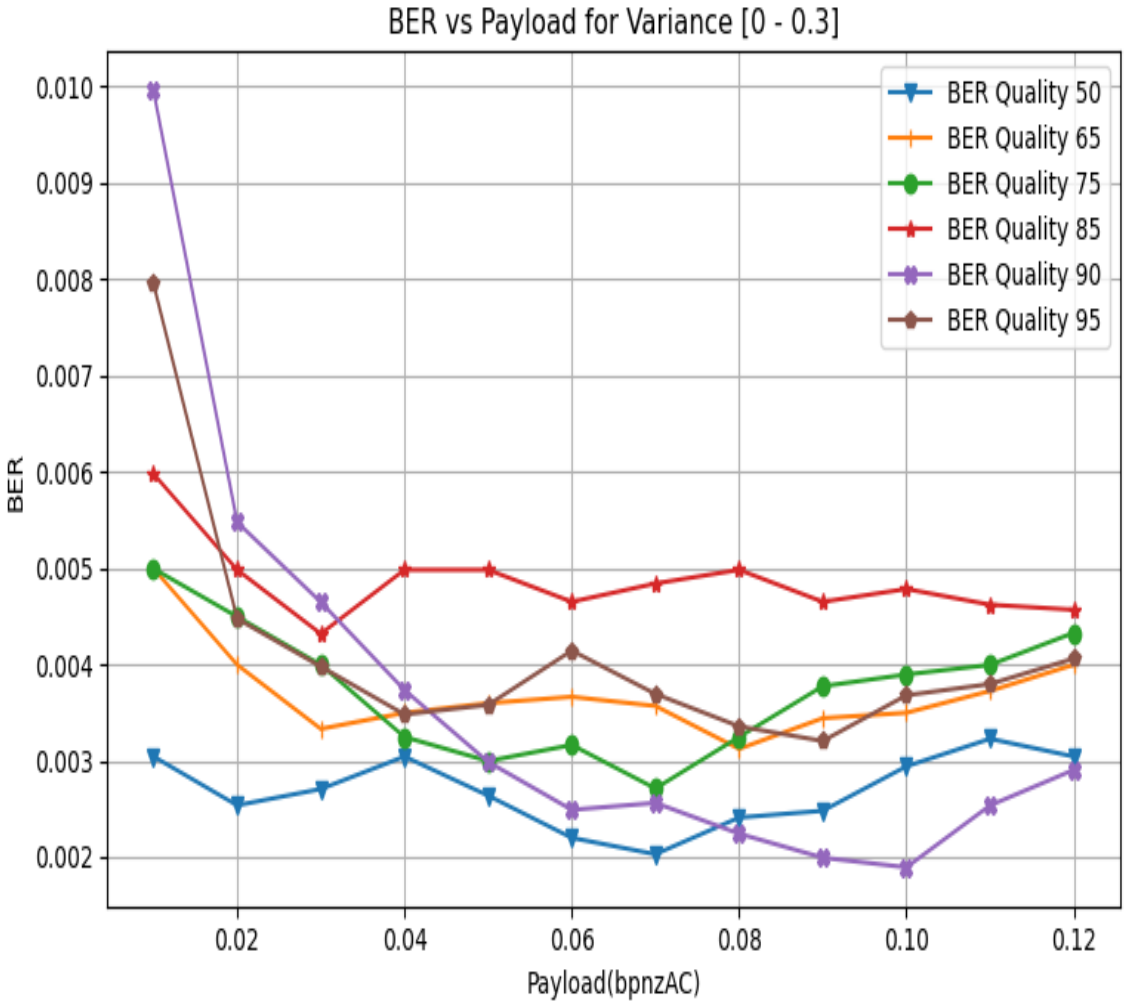
Tablo 4.2'deki gizli mesajların geri elde edilmesi sonucunda, gizli mesajların gömülü olduğu sıfır olmayan katsayılara düşen bit sayısına dikkat edildiğinde Şekil 4.2'deki grafikte Varyans [0 – 0,1] arasında gömme en yüksek mesaj geri elde etme sürecindeki maksimum BER hata oranının 0,0014 civarında olduğu gözlenmektedir.



Şekil 4.3. BER vs Varyans [0-0,2] Grafiği

Gömme kapasitesi arttıkça BER oranının arttığı da gözlemlenmiştir.

Bu sebeple sıfır olmayan katsayıların varyans oranları ne kadar oranla sıkıştırmalardan etkilendiği göstermektedir. Yüksek varyanslar daha yüksek BER demektir.



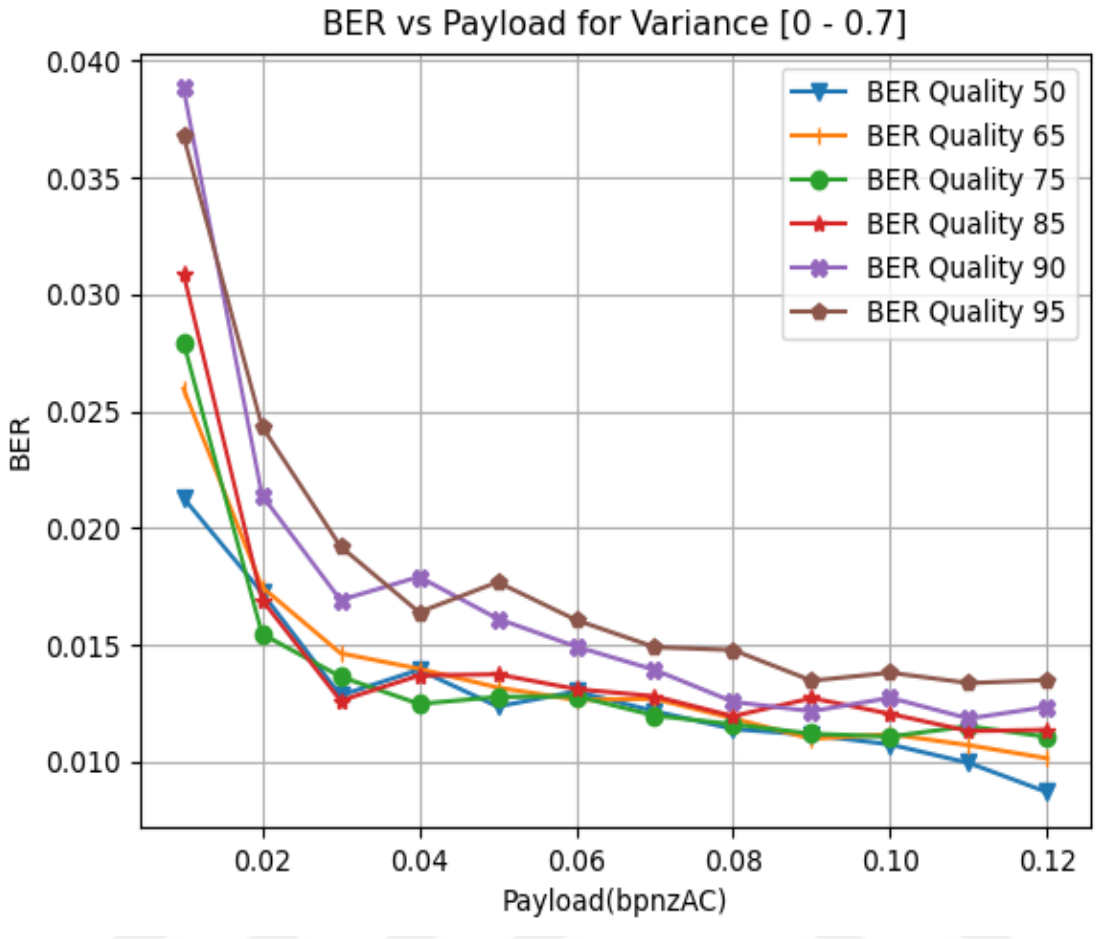
Şekil 4.4. BER vs Varyans [0-0,3] Grafiği

Şekil 4.3'deki grafikte BER değere dikkat edildiğinde bir önceki varyans aralıklarına baz alındığında varyans 0-0,2 arasında görüntüdeki QF 90 Kalite faktöründe 0,02 ile 0,04 arasındaki gömme kapasitesinde en yüksek BER değerinin 0,0046 olduğu görülebilmektedir. Varyans aralıkları 0,1 aralıklı fark ile ilerlediğinden hesaplanan varyans değerleri 0,7'ye kadardır.

Şekil 4.4' te bir önceki katsayıların veryansın ve BER değerlerin arasındaki ilişkiye kıyaslandığında maksimum 0,01-0,02 arasındaki gömme kapasitesinde görüntünün 90 kalite faktörünün BER değerleri 0,010 olduğu gözlemlenmektedir. Yani bir önceki 0-0,2 varyansa sahip grafikle kıyaslandığında eski değer 0,004 iken güncel BER değer 0,010 olarak yükseldiği görülebilmektedir.

Tablo 4.3. Boss1 varyans [0-0,2] bazlı bpnzAC BER değerleri

Gizlenen mesajların yük kapasitesine göre(Payload Bit per non-zero AC coefficients) geri elde edilmesi												
Bits / BER per QF	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**	**0,06**	**0,07**	**0,08**	**0,09**	**0,1**	**0,11**	**0,12**
BER QF 50	0	0	0,001014	0,000507	0,001014	0,000845	0,000869	0,000761	0,000789	0,001014	0,001383	0,00169
BER QF 65	0	0,0005	0,000666	0,001748	0,001598	0,001499	0,001284	0,001249	0,001221	0,001499	0,001544	0,002081
BER QF 75	0	0,000999	0,000666	0,001249	0,001998	0,002663	0,002711	0,002497	0,00222	0,002297	0,002542	0,002497
BER QF 85	0,000996	0,001495	0,000996	0,000747	0,001993	0,002491	0,00242	0,002367	0,002436	0,002491	0,002627	0,003155
BER QF 90	0,001992	0,003983	0,004647	0,003734	0,003983	0,003485	0,003556	0,003734	0,003651	0,003286	0,00335	0,003402
BER QF 95	0,001989	0,000994	0,000663	0,001989	0,003182	0,002983	0,002699	0,003231	0,002983	0,003281	0,003796	0,00406

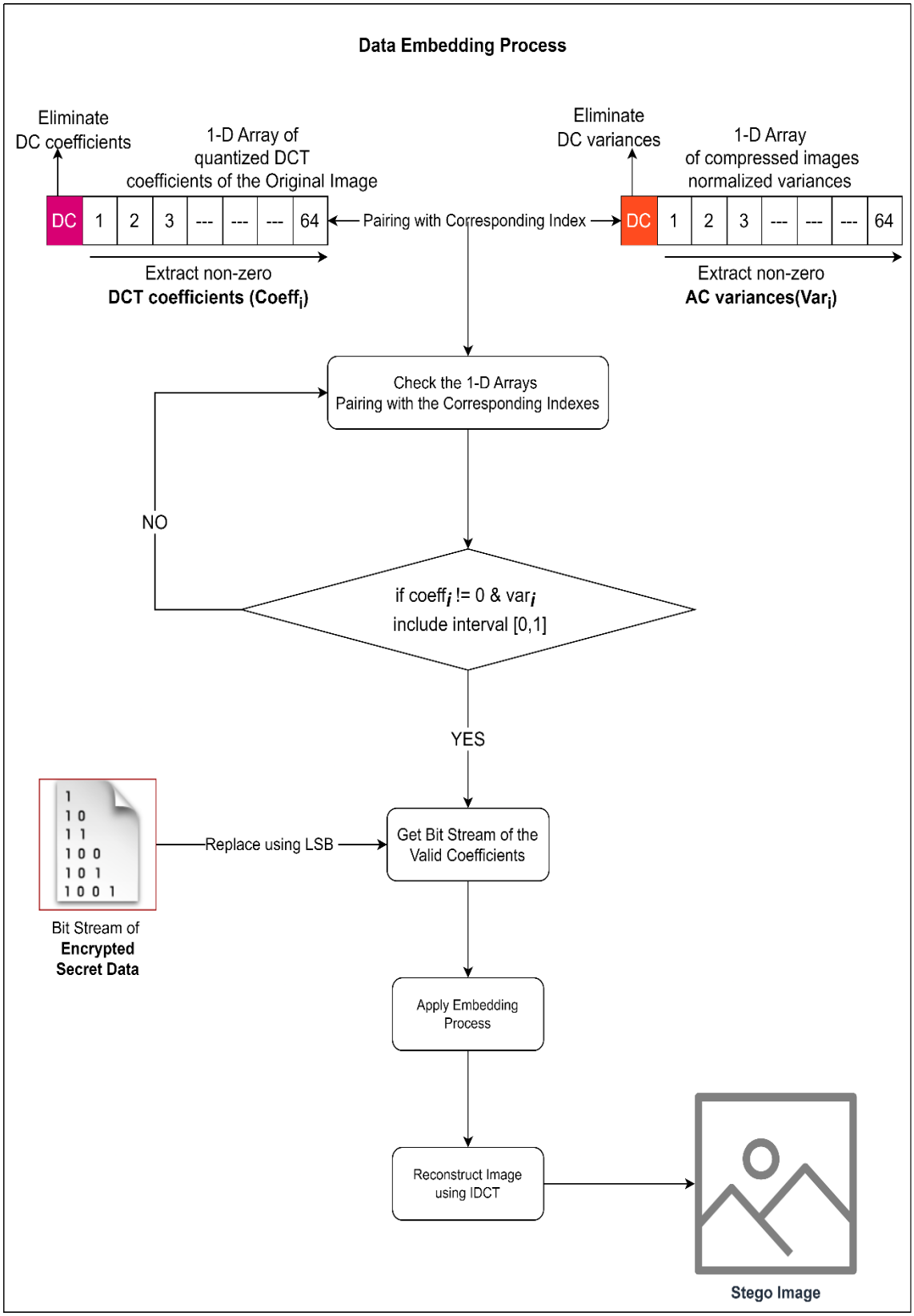


Şekil 4.5. BER vs Varyans [0-0,7] Grafiği

Şekil 4.5' te katsayıların 0-0,7 arasındaki varyansı kalite faktörlerin veri gömülerek 8x8 sıfır olmayan AC-DCT katsayılarının 0,01-0,12 arasındaki gömme kapasitesinde BER değerlerin son durumu görselleştirilmiştir.

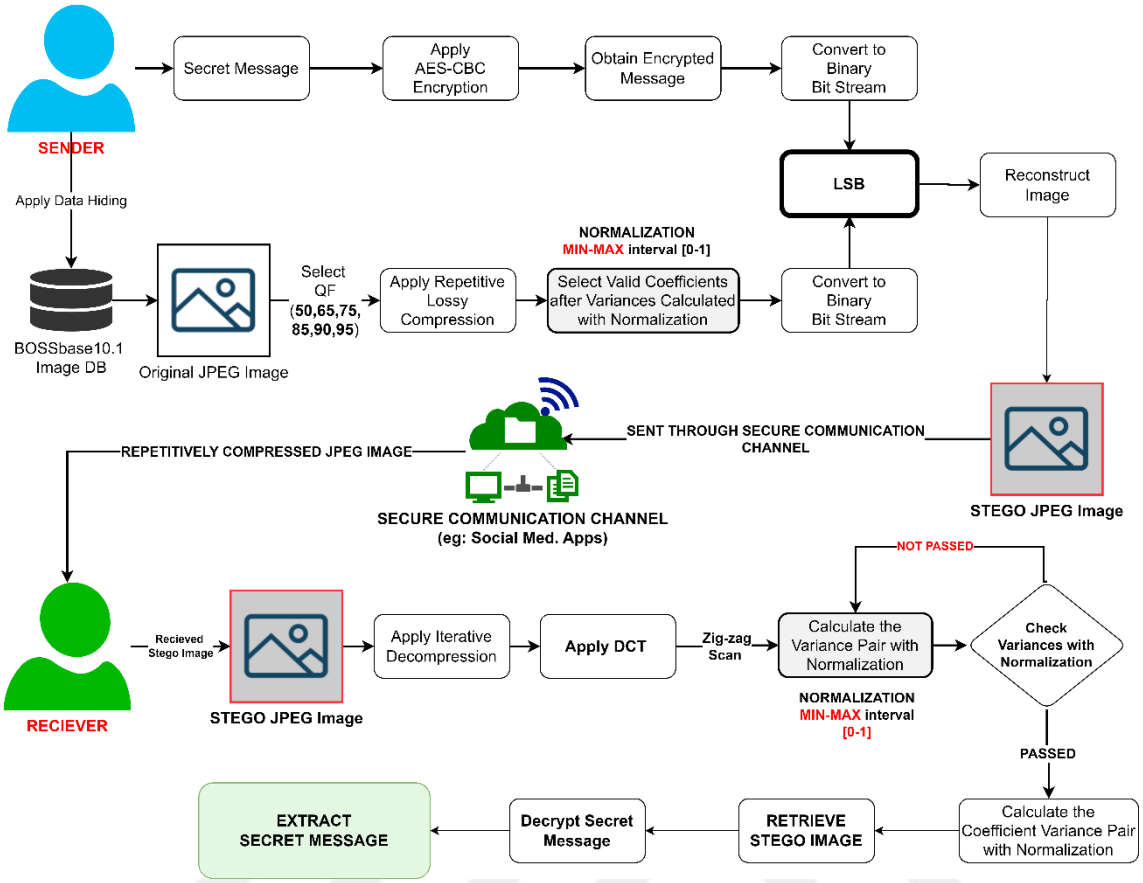
4.3. Gizlenmiş Verinin Geri Elde Edilmesi

Bu bölümde, elde edilen stego görüntüden gizlenmiş verinin çıkarılma işlemi anlatılmaktadır. Öncelikle kullanıcı stego görüntüsünü tekrarlı sıkıştırılmış halde geldiğinden gizli veri elde etmek için sıkıştırmanın çözülmesi gerekmektedir; onun için (Decompression) uygulanması gerekir. Daha sonra DCT frekans domain işlemi uygulayarak gizli verileri taşıyan sıfır olmayan AC katsayılarının varyansını teker-teker hesaplandıktan sonra zigzag taraması uygulanır, sonraki aşamada daha önce hesaplanan ve bölüm 4.1'de verilen varyans tabloların aralıklarına göre bir eşleştirme yapmak için 8x8 DCT matrisi mantığı ile uygulanmaktadır. Bu eşleştirme işlemi Şekil 4.6'de detaylı olarak anlatılmaktadır.



Şekil 4.6. AC DCT katsayıların AC Varyanslar ile Eşleştirilmesi

Verinin geri elde edilmesi işlemi detaylı olarak Şekil 4.7'te anlatılmaktadır.



Şekil 4.7. Veri Çıkarma Süreci

4.4. Performans Karşılaştırmaları

Önerilen yöntem ile yapılan deneysel çalışmaların sonuçları Tablo 4.4'de yer alan benzer çalışmalar ile karşılaştırılmıştır.

Tablo 4.4. Benzer çalışmalar

Çalışmalar	Açıklamalar
1. E.Li.WU C.Kin et al	- Tersinir algoritmasıyla JPEG veri gizleme
2. Hou et al	- Tersinir algoritması ile JPEG DCT frekans alanında blok seçme ve veri gizleme
3. Wu et al	- Tersinir Algoritma kullanılarak Katsayıları eşleştirme yöntemi ile JPEG görüntülere veri gizleme

Bu tez kapsamında geliştirilen yöntemin diğer yöntemler ile karşılaştırılması için seçilen kriterler, stego görüntüsünün göz ile görülür bir bozulmaya uğrayıp uğramadığı test edilmiştir. Tepe sinyal gürültü oranı (Peak Signal to Noise Ratio – PSNR), Örtü ve Stego görüntüsü arasındaki ortalama kare hata değerini analiz ederek stego-görüntüsünün kalitesini ölçmek için çok kullanılan metriklerden biridir. Kısaca PSNR, görüntünün kalitesini ifade eder. 0 ile 100 arasında değer alan PSNR, görüntü kalitesinin korunduğu bir stego görüntüde en az 30 olması beklenir. 8 bitlik görüntülerde PSNR hesaplamak için önce ortalama karesel hata (Mean Squared Error - MSE) Denklem (4.2) ile bulunur. Bulunan değer, Denklem (4.3)'te kullanılarak PSNR değeri hesaplanır.

$$MSE = \frac{\sum_{i=1}^{n}(C_i - C\prime_i)^2}{N} \tag{4.2}$$

MSE: stego ve örtü görüntüsünü karşılaştırmasındaki ortalama kare hatası

N: örtü görüntüsü piksellerinin sayısı

C'i: stego görüntüsündeki i. pikselin yoğunluğu

Ci: örtü resmindeki i. pikselin yoğunluğu

$$PSNR(dB) = 10log_{10}\frac{255^2}{MSE} \tag{4.3}$$

Tablo 4.6'de önerilen yöntem ile Tablo 4.4 ve Tablo 4.5'da yer alan yöntemlerin kalite faktörleri ve gömme kapasitelerine göre karşılaştırmaların PSNR sonuçları sunulmaktadır. Kalite faktörler diğer yöntemler ile aynı seviyede gösterebilmek amacı ile sadece önerilen yöntemimizde (QF= 75, 85, 95), diğer çalışmalarda ise yer (QF= 70, 80, 90). Performans Karşılaştırma yapılırken Denklem (4.3)' teki PSNR ile görüntülerin kalite faktörlerine göre beş kere sıkıştırılarak daha sonra her sıkıştırma aşamasından sonra 0,01 ile 0,12 gömme kapasitesi baz alınıp veri gömülerek öncelikle hiç veri gömülmeyen orijinal görüntü ile stego görüntüsü arasındaki PSNR farkları hesaplanmaktadır. Daha sonra ne kadar benzerlik veya değişkenlik meydana geldiği gözlemlenmektedir.

Tablo 4.5. WU et al PSNR değerleri

QF	PSNR (in dB) with different payload (in bpnzAC)									
Kalite Faktör	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,10
65	57,80	55,18	53,08	51,43	50,07	48,92	47,97	47,13	46,46	45,90
75	58,62	55,55	53,29	51,52	50,14	48,95	48,01	47,26	46,67	46,19
80	59,52	55,42	53,02	51,19	49,73	48,55	47,61	46,89	46,32	45,90
85	59,89	56,13	53,63	51,76	50,36	49,31	48,55	47,97	47,54	47,24

Tablo 4.6. Kalite faktörlerine göre orijinal ile stego görüntülerin PSNR değerleri

Görüntüler **JPEG** 512×512		**Toplam Gömülebilir Mevcut Nonzero-AC Katsayıları (bit)**			**Orijinal Görüntü ile Stego Görüntünün PSNR Karşılaştırmaları (dB)**					
		Kalite Faktörleri (QF)			**Kalite Faktörleri (QF)**					
BOSSbase1.01 Dataset		**75**	**85**	**95**	**75**		**85**		**95**	
					0,01	0,12	0,01	0,12	0,01	0,12
	Boss 1	100119	100355	100578	49,88	42,08	51,06	45,38	51,08	47,63
	Boss 2	95511	97233	100185	50,35	41,25	51,39	44,18	51,14	40,40
	Boss 3	96809	98452	100065	49,19	41,01	50,51	43,60	49,40	36,00
	Boss 4	100119	100355	100578	46,82	39,24	48,06	41,81	45,66	40,12
	Boss 5	104810	105366	106059	49,13	40,03	50,22	42,17	50,92	40,96
	Boss 6	90390	91190	102117	48,08	39,11	49,52	42,07	49,02	44,88
	Boss 7	106916	107899	109098	49,99	43,95	51,31	46,71	50,93	44,21
	Boss 8	170849	171568	190541	46,47	38,03	48,00	40,64	50,50	40,00

Tablo 4.7. Orijinal görüntü ve sıkıştırma aşamaların PSNR karşılaştırmaları

Boss1, BOSS 2, Boss 3 , Boss 4, Boss 5, Boss 6 , Boss 7, Boss 8 Görüntülerinin Kalite Faktörlerine göre Orijinal ve Sıkıştırma Aşamaların Stego Görüntüsü ile PSNR değerleri													
Compresse vs Stego Images		**PSNR (dB) Orijinal Görüntü ile Sıkıştırılan Görüntülerin PSNR Karşılaştırmaları**											
QF	**Boss 1 Image**	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**	**0,06**	**0,07**	**0,08**	**0,09**	**0,10**	**0,11**	**0,12**
75	**Original**	42,98	42,47	42,08	49,88	49,16	48,69	48,26	47,60	46,39	45,06	44,24	43,61
	Compress 1	43,52	42,92	42,48	56,22	53,50	52,10	51,06	49,79	47,88	46,08	45,03	44,25
	Compress 2	42,83	42,32	41,93	50,03	49,20	48,62	48,12	47,43	46,22	44,91	44,09	43,45
	Compress 3	41,59	41,19	40,89	45,66	45,34	45,09	44,85	44,51	43,85	43,05	42,49	42,04
	Compress 4	40,10	39,82	39,59	42,57	42,41	42,28	42,15	41,96	41,58	41,09	40,73	40,42
	Compress 5	38,64	38,43	38,27	40,25	40,16	40,08	40,00	39,88	39,64	39,32	39,08	38,87

Tablo 4.7. (Devamı) PSNR karşılaştırmaları Kalite Faktörü 85

QF	**Boss 1 Image**	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**	**0,06**	**0,07**	**0,08**	**0,09**	**0,10**	**0,11**	**0,12**
85	**Original**	46,38	45,84	45,39	51,06	50,54	50,18	49,94	49,70	49,32	48,90	48,01	47,13
	Compress 1	47,32	46,63	46,04	58,85	55,95	54,50	53,61	52,83	51,94	51,08	49,61	48,33
	Compress 2	45,57	45,11	44,72	49,16	48,79	48,54	48,36	48,18	47,90	47,58	46,90	46,19
	Compress 3	43,47	43,19	42,93	45,36	45,20	45,08	45,00	44,91	44,78	44,61	44,25	43,85
	Compress 4	41,33	41,15	40,99	42,41	42,32	42,26	42,21	42,16	42,08	41,99	41,79	41,56
	Compress 5	39,39	39,28	39,17	40,02	39,97	39,94	39,92	39,89	39,85	39,80	39,67	39,53

Tablo 4.7 Kalite faktörleri baz alınarak orijinal görüntünün sıkıştırma aşamalarında veri gömüldükten sonra PSNR değerleri ile Tablo 4.6’ da yer alan orijinal görüntü ve hiç veri gömülmeyen sıkıştırma aşamaları karşılaştırıldığında sıkıştırmadan kaynaklı ufak farklarla PSNR değerlerinde değişkenlikler olduğu iki tablodaki sonuçlar incelendiğinde görülmektedir. PSNR’deki bu değişimin veri gizlemeden değilde, tekrarlı şıkıştırmadan kaynaklandığı aşikardır.

Tablo 4.7. (Devamı) PSNR karşılaştırmaları Kalite Faktörü 95

QF	Boss1 Image	0,01	0,02	0,03	0,04	0,05	0,06	0,07	0,08	0,09	0,10	0,11	0,12
95	**Original**	47,76	47,70	47,63	51,08	50,94	49,14	47,92	47,88	47,84	47,83	47,81	51,16
	Compress 1	49,86	49,73	49,58	64,73	61,63	53,08	50,48	50,35	50,22	50,14	50,05	66,73
	Compress 2	47,73	47,67	47,60	51,05	50,92	49,13	47,91	47,87	47,82	47,81	47,79	51,14
	Compress 3	45,77	45,72	45,66	47,75	47,66	46,71	45,96	45,92	45,88	45,86	45,83	47,78
	Compress 4	43,24	43,21	43,19	44,15	44,12	43,68	43,30	43,29	43,27	43,27	43,26	44,17
	Compress 5	41,41	41,39	41,37	42,03	42,01	41,73	41,48	41,46	41,45	41,44	41,43	42,04

Tablo 4.7. Orijinal görüntü ve sıkıştırma aşamaların PSNR karşılaştırmaları sunulmuştur. Sonuçların yorumlaması bir sonraki bölümde sonuçlar ve öneriler yer verilmiştir.

5. SONUÇLAR VE ÖNERİLER

Tez çalışması kapsamında, Kriptoloji ve Steganografi tekniklerini beraber kullanan sıkıştırma ataklarına karşı dayanıklı yeni bir veri gizleme yöntemi önerilmektedir. Yöntem ilk olarak gizlenecek veriyi AES CBC tekniği ile şifrelemektedir. Sonrasında, tekrarlı sıkıştırma uygulanmış JPEG görüntülere DCT uygulanarak elde edilen katsayılar üzerinde veri gizleme yapılmaktadır. Önerilen yöntemde, tekrarlı sıkıştırma işlemleri sonucunda az değişen veya hiç sıkıştırmadan etkilenmeyip değişmeyen katsayılara veriler gizlenmektedir. Bu sayede gizlenmiş olan veri, yüksek doğrulukta geri elde edilmektedir.

Literatürde var olan yöntemler incelendiğinde, daha çok JPEG sıkıştırmayla ilgili görüntü alanlarındaki istatistiksel dağılım özelliklerine odaklanmıştır. Tez çalışması kapsamında, istatistiksel dağılım özelliklerinden farklı olarak, tekrarlı sıkıştırmadan geçirilerek JPEG nicemlemeli sıfır olmayan AC-DCT katsayılarının varyanslarının her sıkıştırma iterasyonunda değişkenlik gösterdiği fark edilmektedir. Görüntü sıkıştırma uygulanarak (Pre-compression) ve sıkıştırmadan önceki eski haline dönüştürme sürecinde (Decompression), sıfır olmayan katsayıların nasıl değiştiği takip ve teşhis edildikten sonra, iki özelliğe göre (1- JPEG nicemlemeli DCT katsayılarının sıfır olmayan değişkenliği ve 2- sıfır olmayan JPEG nicemlemeli DCT katsayılarının, [0 - 1] arasında uygulanan minimum - maksimum normalizasyonu baz alınarak varyans aralıklarına göre) keşfedilir.

Önerilen yöntemin etkinliğini kanıtlamak için açık kaynaklı BOSSbase1.01 veri setinden yararlanmaktadır. Çalışmada, anti sıkıştırma, damgalama ve günümüzde güncel anti sıkıştırmayı sunan sağlam görüntü steganografi yöntemleri ile karşılaştırılarak deneysel sonuçlar verilmiştir. Deneysel sonuçlara göre, görüntü üzerinde uygulanan tekrarlı sıkıştırma ataklarının kalite faktörleri ile ön sıkıştırmanın kalite faktörü arasındaki ve [0 - 1] arasındaki varyans aralıkları arttıkça, kalite faktörüne göre maksimum bit hata oranının (BER) çok düşük düzeyde olduğu gözlemlenmiştir. Kısacası sıfır olmayan AC-DCT katsayıları kullanılarak gizlenen mesajın hatasız veya çok düşük hata ile geri elde edildiği gözlemlenmiştir. Önerilen yöntemin deneysel sonuçları, literatürde sunulan benzer yöntemler ile karşılaştırıldığında, daha iyi performans sunduğu görülmüştür.

Çalışma tekrarlı sıkıştırma ataklarına karşı dayanıklı bir yöntemdir. Ayrıca, orijinal

görüntü ve tekrarlı sıkıştırılmış görüntüler her aşamada karşılaştırılmış olup PSNR değerlerinin birbirine çok yakın olduğu gözlemlenmiştir. Buda, PSNR değerindeki değişimin, veri gizlemeden değil veri sıkıştırmadan kaynaklandığı anlamına gelmektedir.

Sonuç olarak, önerilen veri gizleme yönteminin tekrarlı sıkıştırma kullanan sosyal medya platformlarında gerek damgalama gerekse gizli verilerin çaktırmadan karşı tarafa hatasız veya düşük hata ile aktarılması için kullanılabilir.

İlerleyen çalışmalarda gizlenecek verinin istatistiksel analizi de yapılarak, frekans domainde tüm AC-DCT katsayılarının hangi bölgelerde etkin bir şekilde kullanılacağına karar veren yüksek kapasiteli yeni yöntemler önerilebilir.

KAYNAKLAR

Abdirashid, A. M., Solak, S., Sahu, A. K. (2022). Data Hiding Based on Frequency Domain Image Steganography. *Avrupa Bilim ve Teknoloji Dergisi, (42),* 71-76.

Ahmed, A., Nanne, M. F., Gueye, B. (2022, January). The effectiveness of a hybrid Diffie-Hellman-RSA-AES model. In 2022 *International Conference on Computer Communication and Informatics (ICCCI),* 1-5 *IEEE*.

Baziyad, M., Rabie, T., Kamel, I., Benkhelifa, M. (2022). Polynomial fitting: enhancing the stego quality of DCT-based Steganography schemes. *Multimedia Tools and Applications, 81,* 43999–44019.

Chowdhuri, P., Pal, P., Si, T. (2023). A novel steganographic technique for medical image using SVM and IWT. *Multimedia Tools and Applications,* 1-20.

Dalal, M., Juneja, M. (2023). Steganalysis of DWT Based Steganography Technique for SD and HD Videos. *Wireless Personal Communications, 128*(4), 2441-2452.

Diffie, W.,Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory, 22*(6), 644-654.

Gutub, A., Al-Shaarani, F. (2020). Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. *Arabian Journal for Science and Engineering, 45*(4), 2631-2644.

Hou D. D., Wang H. Q., Zhang W. M. and Yu N. H. (2018). "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing, 148*, 41-47.

Huang F., Qu X., Kim H. J. and Huang. J. "Reversible data hiding in JPEG images," *IEEE Transactions on Circuits & Systems for Video Technology, 26*(9)*,* 1610-1621.

Hussain, M.; Wahab, A. W. A.; Idris, Y. I. Bin; Ho, A. T. S.; Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication., 65*, 46–66.

Johnson, N. F.,Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26-34.

Kadhim, I. J.; Premaratne, P.; Vial, P. J.; Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*., *335*, 299–326.

Khayam, S. A. (2003). The discrete cosine transform (DCT): theory and application. Michigan State University, *114*(1), 31.

Kocher, P. C. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Advances in Cryptology—CRYPTO'96: *16th Annual International Cryptology Conference* Santa Barbara, California, USA August 18–22, 1996 Proceedings *16* (104-113). *Springer Berlin Heidelberg.*

Kumar, V., Kumar, D. (2018). A modified DWT-based image steganography technique. *Multimedia Tools and Applications, 77*, 13279-13308.

Lam, E. Y., Goodman, J. W. (2000). A mathematical analysis of the DCT coefficient distributions for images. *IEEE transactions on image processing, 9*(10), 1661-1666.

Maurya, S., Nandu, N., Patel, T., Reddy, V. D., Tiwari, S., Morampudi, M. K. (2023). A discrete cosine transform-based intelligent image steganography scheme using quantum substitution box. *Quantum Information Processing, 22*(5), 206.

Melman, A., Evsutin, O. (2023). Comparative study of metaheuristic optimization algorithms for image steganography based on discrete Fourier transform domain. *Applied Soft Computing, 132*, 109847.

Piva, A., Barni, M., Bartolini, F., Cappellini, V. (1997, October). DCT-based watermark recovering without resorting to the uncorrupted original image. *In Proceedings of international conference on image processing, 1*, 520-523. IEEE.

Po-Yueh, P. Y., Lin, H. J. (2006). A DWT based approach for image steganography. *International Journal of Applied Science and Engineering, 4*(3), 275-290.

Sabeti, V., Aghabagheri, A. (2022). Developing an adaptive DCT-based steganography method using a genetic algorithm. *Multimedia Tools and Applications,* 1-24.

Solak, S., Altınışık, U. (2019). Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3. *Journal of Electronic Imaging, 28*(4), 043025-043025.

Solak, S. (2020). High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms. *IEEE Access, 8*, 166513-166524.

Solak, S., Tezcan, G. (2022). A New Dual Image Based Reversible Data Hiding Method Using Most Significant Bits and Center Shifting Technique. *Applied Sciences, 12*(21), 10933.

Song, X., Yang, C., Han, K., Ding, S. (2022). Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain. *Multimedia Tools and Applications, 81*(25), 36453-36472.

Swain, G., Lenka, S. K. (2012). A technique for secret communication using a new block cipher with dynamic steganography. *International Journal of Security and Its Applications, 6*(2), 1-12.

Uzun, M. Solak, S. (2022). GÖRÜNTÜ STEGANOGRAFİSİNDE YAYGIN KULLANILAN VERİ GİZLEME TEKNİKLERİNİN İNCELENMESİ. *Mühendislik Bilimleri ve Tasarım Dergisi, 10*(3), 816-830 .

Wang, S., Zheng, N., Xu, M. (2021). A Compression Resistant Steganography Based on Differential Manchester Code. *Symmetry, 13*(2), 165.

Wang, Y., Moulin, P. (2006, February). Statistical modeling and steganalysis of DFT-based image steganography. In Security, Steganography, and Watermarking of *Multimedia Contents VIII, 6072*, 14-24 SPIE.

Wu, D. C., Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern recognition letters, 24*(9-10), 1613-1626.

Wu T. Y. Huang. F. J. (2022) "Adaptive reversible data hiding in JPEG images based on coefficient pairing," *Journal of Software, 33*(2), 725+728-739.

Yalman, Y. (2010). Sayısal Görüntüler İçin Histogram Temelli Veri Gizleme Yöntemi Ve Uygulama Yazılımı. Kocaeli Üniversitesi. Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı, i, Doktora Tezi, Tez No 275801.

Zhang, X., Wang, S. (2006). Efficient steganographic embedding by exploiting modification direction. *IEEE Communications letters, 10*(11), 781-783.

Zhu, L., Luo, X., Yang, C., Zhang, Y., & Liu, F. (2021). Invariances of JPEG-quantized DCT coefficients and their application in robust image steganography. *Signal Processing, 183*, 108015.

KİŞİSEL YAYIN VE ESERLER

Abdirashid, A. M., Solak, S., & Sahu, A. K. (2022). Data Hiding Based on Frequency Domain Image Steganography. *European Journal of Science and Technology,* (42), 71-76. DOI: 10.31590/ejosat.1188597

ÖZGEÇMİŞ

2015 yılında lisans eğitimimi Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, Sakarya Üniversitesinde başladım. 2020-Güz yarı yılında halihazırda okumakta olduğum yüksek lisans eğitimi için KOCAELİ Üniversitesi, Fen Bilimleri Enstitüsü, Teknoloji Fakültesi'nden Bilişim Sistemleri Mühendisliği Anabilim Dalı'nda başladım. Lisans mezuniyetimin hemen ardından 2019 yılında mezun olduktan sonra Sakarya Üniversitesi UPEP (Üniversiteden Pazar Elçisi) projesinde bir elçi olarak seçildikten sonra SATSO (Sakarya Sanayi ve Ticaret Odası) 'dan çeşitli üretim, imalat ve İhracat firmaları ile dış ticaret ve pazarlama alanında; ürünlerde dış ticaret pazarlama stratejisi geliştirme, dijital pazarlama veri toplama ve analizleri üzerinde çalışmalar üstlendim. 2020 yılında Sakarya Üniversitesi Teknoloji ve Transfer Ofisinden (TEKNOKENT)'te CREA Cubed Technologies Inc. Sağlık cihazları üzerinde yazılım uygulamaları geliştirme departmanında Ön-uç geliştirici (Frontend Developer) olarak çalıştım. Halihazırda 2022 yılından beri, Finlandiya merkezli dijital transformasyon, inovasyon girişimcilik eğitimi ve öğretimi, ekosistem geliştirme danışmanlığı üzerinde hizmet sunan, ve işletmeler için yazılım hizmeti geliştiren STARTUP COMMONS Service by Digiole Oy firmasında, yazılım ekosistem ürünleri ön-uç geliştiricisi (Ecosystems Frontend Developer) ve API ile integrasyonu olarak çalışma pozisyonunda görev almaktayım.