KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

SAYISAL RENKLİ GÖRÜNTÜLER İÇİN UZAMSAL DÜZLEM YÖNTEMLERİ KULLANAN YENİ BİR HİBRİT STEGANOGRAFİ ALGORİTMASI

MURAT UZUN

KOCAELİ 2023

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

SAYISAL RENKLİ GÖRÜNTÜLER İÇİN UZAMSAL DÜZLEM YÖNTEMLERİ KULLANAN YENİ BİR HİBRİT STEGANOGRAFİ ALGORİTMASI

MURAT UZUN

Doç.Dr. Serdar SOLAK		
Danışman,	**Kocaeli Üniversitesi**	**.....**
Prof.Dr. Yıldıray YALMAN		
Jüri Üyesi,	**Piri Reis Üniversitesi**	**.....**
Doç.Dr. 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 BAP tarafından FBA-2021-2488. 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.

.....

Murat UZUN

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.

.....

Murat UZUN

ÖNSÖZ VE TEŞEKKÜR

Kocaeli Üniversitesindeki yüksek lisans eğitimim boyunca güler yüzünü ve samimiyetini benden esirgemeyen, değerli bilgilerini benimle paylaşan ve anlattıkları ile ufkumu açıp bana değer katan, tez ve yayın çalışmam sırasında yardımını hiçbir zaman eksik etmeyen, bana her konuda destek olan ve anlayış gösteren, hakkını asla ödeyemeyeceğim saygıdeğer danışman hocam Doç. Dr. Serdar SOLAK'a;

yüksek lisans eğitimim boyunca bana yardımcı olan çalışma arkadaşım Gökhan TEZCAN'a;

yüksek lisans eğitimimde beni destekleyen işyeri Müdürüm Sayın Doç. Dr. Suhap ŞAHİN ve Müdür Yardımcım Dr. Samet DİRİ ile iş dostlarım Berna ÜLKÜSAYAR, Dilek GARAN, Zehra ALTUNTAŞ, Ahmet AKCAKAYA ve Ayhan GÜLTEKİN'e;

hayatım boyunca ve özellikle yüksek lisans ders süreci ve tez yazım aşamasında bana karşı son derece sabırlı, destekleyici ve anlayışlı olan sevgili eşim Dilek UZUN, sevgili fidanım Selmin Nazra UZUN ve sevgili çiçeğim Elvin Buğlem UZUN ile canım annem Zehra UZUN'a;

tez jürimde bulunarak vermiş oldukları katkılardan dolayı saygıdeğer hocalarım Prof. Dr. Yıldıray Yalman ve Doç. Dr. Mustafa Hikmet Bilgehan UÇAR'a

çok teşekkür ederim.

Mayıs - 2023 Murat UZUN

İÇİNDEKİLER

ETİK BEYAN VE ARAŞTIRMA FONU DESTEĞİ i
YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI ii
ÖNSÖZ VE TEŞEKKÜR iii
İÇİNDEKİLER iv
ŞEKİLLER DİZİNİ vi
TABLOLAR DİZİNİ vii
KISALTMALAR viii
ÖZET ix
ABSTRACT x
1. GİRİŞ 1
2. GENEL BİLGİLER 5
2.1. Çalışmanın Amacı 11
2.2. Steganografi Nedir? 12
2.2.1. Görüntü Steganografisi Teknikleri 13
2.2.2. Sayısal Steganografi Çeşitleri 14
2.3. Görüntü Steganografisi 15
2.3.1. Görüntü Yapısı 16
2.3.2. Görüntü Steganografisinin Hedefleri 17
2.3.3. Görüntü Steganografisinin Özellikleri 17
2.3.3.1. Algılanamazlık (Imperceptibility) 17
2.3.3.2. Güvenlik (Security) 18
2.3.3.3. Yük Kapasitesi (Payload Capacity) 18
2.3.3.4. Sağlamlık (Robustness) 18
2.3.4. Performans Değerlendirme Ölçütleri 18
2.3.4.1. Yük Kapasitesi (BPP) 19
2.3.4.2. Tepe Sinyal Gürültü Oranı (PSNR) 19
2.3.4.3. Yapısal Benzerlik İndeksi (SSIM) 20
2.3.4.4. Kapasite (Payload) 20
2.4. Steganaliz 21
2.4.1. Piksel Farkları Dağılımı (PDH) 22
2.4.2. RS Analizi 22
3. UZAMSAL DOMAİNDE YAYGIN KULLANILAN TEKNİKLER 23
3.1. En Az Anlamlı Bit (LSB) 23
3.2. Piksel Değeri Farkı (PVD) 26
3.3. Değişim Yönünü Kullanma (EMD) 28
3.4. Genelleştirilmiş Değişim Yönünü Kullanma (GEMD) 30
3.5. PVD + LSB2 Hibrit Bir Yöntem 32
4. ÖNERİLEN YÖNTEM 34
4.1. Veri Gizleme Yöntemlerinin Belirlenmesi 34
4.2. Veri Gizleme Süreci 38
4.3. Gizlenmiş Verinin Geri Elde Edilmesi 40
4.4. Taşma Sorunu (Fall Off Baundary Problem) 45
4.4.1. PVD için FOBP Sorununun Giderilmesi 46
4.4.2. GEMD için FOBP Sorununun Giderilmesi 47
4.5. Önerilen Yöntem ile örnek veri gizlenmesi ve verinin elde edilmesi 48
4.5.1. Veri Gizlenmesi 49

4.5.2. Verilerin Elde Edilmesi 50
5. DENEYSEL ÇALIŞMALAR 52
5.1. Uzamsal Domainde Kullanılan Yöntemlerin Deneysel Sonuçları 53
5.2. Önerilen Yöntemin Deneysel Sonuçları 63
5.2.1. Güvenlik Testleri 71
5.2.1.1. Piksel Farkları Dağılımı (PDH) 71
5.2.1.2. RS Analizi 72
6. SONUÇ 74
KAYNAKLAR 77
KİŞİSEL YAYIN VE ESERLER 82
ÖZGEÇMİŞ 83

ŞEKİLLER DİZİNİ

Şekil 2.1. II.Dünya savaşında gönderilen bir gizli mesaj 12
Şekil 2.2. Kölenin kafasına yazılan gizli mesaj 13
Şekil 2.3. Steganografi tekniklerinin sınıflandırılması 14
Şekil 2.4. Sayısal görüntü steganografisi süreci 14
Şekil 2.5. Gri ölçekli resmin yapısı 16
Şekil 2.6. RGB görüntünün piksel yapısı 16
Şekil 2.7. Veri gizleme özellikleri arasındaki değiş-tokuş 17
Şekil 3.1. Sekiz bitlik veride LSB ve MSB 23
Şekil 3.2. Bir piksel RGB'de LSB ve MSB 23
Şekil 3.3. 256x256 Gri House görüntüsü 24
Şekil 3.4. Bit katarının oluşturulması 24
Şekil 3.5. Çözülen verinin 8'lik bitlere dönüştürülmesi 26
Şekil 3.6. Örtü görüntünün R kanalının piksel katarına dönüştürülmesi 33
Şekil 3.7. PVD yöntemi uygulanacak kısım 33
Şekil 4.1. Veri gizleme yöntemlerinin belirlenmesi süreci 35
Şekil 4.2. Veri gizleme süreci 39
Şekil 4.3. Gizli veriyi elde etme süreci 41
Şekil 4.4. PVD için FOBP çözümü akış diyagramı 46
Şekil 4.5. PVD için Görüntü-FOBP yoğunluk grafiği 46
Şekil 4.6. GEMD için FOBP çözümü akış diyagramı 47
Şekil 4.7. GEMD için Görüntü-FOBP yoğunluk grafiği 48
Şekil 5.1. Örtü-görüntü olarak kullanılan görüntüler 52
Şekil 5.2. LSB-k için artan "k" değerinin görüntüye etkisi 53
Şekil 5.3. Altı örtü görüntünün için LSB-k bit SSIM değerleri (%) 56
Şekil 5.4. PVD Yöntemi için Kapasite, PSNR ve SSIM karşılaştırması 57
Şekil 5.5. EMD-GEMD için Kapasite, PSNR ve SSIM karşılaştırması 58
Şekil 5.6. Tüm yöntemlerin karşılaştırması - Lena 59
Şekil 5.7. PVD için Baboon ve Peppers görüntülerinin kapasiteleri 59
Şekil 5.8. Baboon görüntüsü için LSB 1-2-3 bit histogramları 60
Şekil 5.9. Baboon görüntüsü için EMD, GEMD ve PVD histogramları 61
Şekil 5.10. Görüntü bazında uygulanan yöntem sayıları 65
Şekil 5.11. Piksel-Yöntem kıyaslamaları 65
Şekil 5.12. Önerilen yöntemin PSNR, SSIM, Yük ve Kapasite grafikleri 66
Şekil 5.13. Airplane örtü görüntüsü için tüm yöntemlerin kıyaslanması 67
Şekil 5.14. Önerilen Yöntem için histogram Karşılaştırmaları 68
Şekil 5.15. Görüntülere ait PDH'ler 71
Şekil 5.16. RS Analizi Sonuçları 72

TABLOLAR DİZİNİ

Tablo 1.1. Bilgi güvenliği tekniklerinin özelliklerinin karşılaştırılması 2
Tablo 3.1. "GEL" kelimesi için ASCII ve ikili taban değerleri 24
Tablo 3.2. LSB-1 uygulaması 25
Tablo 3.3. LSB-3 bit için gizli veriyi elde etme işlemi 25
Tablo 3.4. Elde edilen bitlerin karakterlere dönüşümü 26
Tablo 3.5. PVD referans tablosu 26
Tablo 3.6. İşlem gören piksel sayısına göre bpp 29
Tablo 3.7. n=4 için EMD piksellerindeki değişim 30
Tablo 3.8. İşlem gören piksel sayısına göre bpp 31
Tablo 3.9. n=3 için GEMD piksellerindeki değişim 32
Tablo 3.10. R kanalına ait bir pikselin iki parçaya ayrılması 33
Tablo 4.1. PVD için görüntü bazında FOBP miktarları 47
Tablo 4.2. GEMD için görüntü bazında FOBP miktarları 48
Tablo 5.1. Çalışma sonucu elde edilen veriler 53
Tablo 5.2. Dört farklı görüntüde LSB 1-2-3 bit uygulama sonuçları 54
Tablo 5.3. 512x512 Gri ölçekli görüntü sonuçları 62
Tablo 5.4. 512x512 RGB görüntü sonuçları 62
Tablo 5.5. 512 ve 1024 Gri görüntü için EMD-GEMD verileri 63
Tablo 5.6. Yüzdesel olarak görüntü-yöntem yoğunluğu 64
Tablo 5.7. Uygulanan görüntü-yöntem adedi 64
Tablo 5.8. Örtü görüntüler için önerilen yönteme ait performans değerleri 66

SİMGELER VE KISALTMALAR DİZİNİ

Kısaltmalar

BPP	: Bit Per Pixel (Piksel Başına Düşen Bit Sayısı)
EMD	: Exploiting Modification Direction (Değişim Yönünü Kullanma)
FOBP	: Fall Off Baundary Problem (Sınır Taşması)
GEMD	: Generalized Exploiting Direction Modification (Genelleştirilmiş Değişim Yönünü Kullanma)
LSB	: Least Significant Bit (En Az Anlamlı Bit)
MSB	: Most Significant Bit (En Çok Anlamlı Bit)
MSE	: Mean Square Error (Ortalama Karesel Hata)
PSNR	: Peak Signal Noise Ratio (Tepe Sinyal Gürültü Oranı)
PDH	: Pixel Difference Histogram (Piksel Farkları Dağılımı)
PVD	: Pixel Value Difference (Piksel Değeri Farkı)
RGB	: Red Green Blue (Kırmızı Yeşil Mavi – Renkli Görüntü)
RS	: Regular and Singular (Düzenli ve Tekil)
SSIM	: Structural Similarity Index Measure (Yapısal Benzerlik Endeksi)

SAYISAL RENKLİ GÖRÜNTÜLER İÇİN UZAMSAL DÜZLEM YÖNTEMLERİ KULLANAN YENİ BİR HİBRİT STEGANOGRAFİ ALGORİTMASI

ÖZET

İnternet ve iletişim teknolojilerinin yaygınlaşmasıyla beraber, insanların birbirleriyle haberleşmesi ve sosyal medya ortamlarında çoklu ortam nesnelerini paylaşması kolay bir şekilde gerçekleştirilebilmektedir. Ancak kişisel ve telif hakları ile korunan verilerin uçtan uca güvenli bir şekilde aktarılması önem arz etmektedir. Şifreleme olarak bilinen Kriptografi ile veri gizleme olarak bilinen Stegonagrafi kavramları ve teknikleri, veri gizliliğini sağlamak için yaygın olarak kullanılmaktadır. Steganografik teknikler, gizli verileri metin, ses, görüntü ve video dosyaları içerisine çaktırmadan gizlemek için kullanılmaktadır. Bu tekniklerdeki başarım, yüksek sağlamlık ve kapasite, yüksek algılanamazlık elde edilmesiyle ölçülmektedir. İlgili başarım ölçütlerini arttırmak için uzamsal ve frekans alanında çok sayıda teknik önerilmektedir. Tez çalışması kapsamında, uzamsal alanda yaygın kullanılan LSB, PVD, EMD ve GEMD teknikleri detaylı incelenmiş olup, bu teknikler ve bunların beraber kullanımına yönelik görüntü steganografisi için yeni bir veri gizleme yöntemi sunulmaktadır. Genel olarak, literatürde görüntü steganografisi için yapılan veri gizleme çalışmalarında, örtü görüntü içerisine veriler tek bir teknik ile gizlenmektedir. Tez çalışması kapsamında önerilen yöntemde, örtü görüntünün her bir pikseline farklı farklı tekniklerle veriler gizlenmektedir. Veri gizleme tekniklerinin belirlenmesi örtü görüntünün ilk piksel değeri ve kullanılacak tekniklerinin sayısına bağlıdır. Bu sayede örtü görüntü içerisine saklanacak verinin gizliliği, güvenliği ve algılanmazlığı sağlanmaktadır. Önerilen yöntemde, veri gizlemede 1 ila 4 adet arasında yöntem kullanımına ilişkin çalışma yapılmıştır. Ancak, yöntem sayısının 1 ila 8 adete yükseltilmesi, kapasiteden önemsenmeyecek bir kayıpla, çok basit bir şekilde gerçekleştirilebilmektedir. Bu nedenle önerilen yöntem, esnek ve geliştirilmeye son derece müsaittir.

Anahtar Kelimeler: Bilgi Güvenliği, Görüntü Steganografisi, Uzamsal Domain Metotları, Veri Gizleme.

A NEW HYBRID STEGANOGRAPHY ALGORITHM USING SPATIAL DOMAIN METHODS FOR DIGITAL COLOR IMAGES

ABSTRACT

With the widespread use of the Internet and communication technologies, it is easy for people to communicate with each other and share multimedia objects in social media environments. However, it is important to transfer personal and copyrighted data securely from end to end. Steganography, known as data hiding, is widely used to ensure data privacy. Steganographic techniques are used to hide confidential data in text, audio, image and video files. Performance in these techniques is measured by achieving high robustness and capacity, high imperceptibility. In this thesis, LSB, PVD, EMD and GEMD techniques, which are widely used in the spatial domain, are examined in detail, and a new data hiding method for image steganography is also proposed for these techniques. In general, in data hiding studies for image steganography in the literature, data is hidden in the cover image with a single technique. In the proposed method, the secret data is hidden in each pixel of the cover image with different techniques. The determination of data hiding techniques depends on the first pixel value of the cover image and the number of techniques. In this way, the privacy, security, and invisibility of the secret data in the cover image is ensured. The experimental results were carried out with 4 different methods. However, up to 8 methods can be adapted very simply, with a negligible loss of capacity. The proposed method is therefore flexible and highly adaptable.

Keywords: Information Security, Image Steganography, Spatial Domain Methods, Data Hiding.

1. GİRİŞ

Günlük hayatta, internet üzerinden gönderilen e-postalar, sosyal medya paylaşımları, yorumlar, mesajlar, fotoğraf ve video görüntülemeleri gibi birçok veri çeşidi bulunmaktadır. Bu verilerin anlık miktarı tahmin edilemeyecek kadar fazladır. Her gün yeni uygulamaların ortaya çıkmasıyla birlikte, veri trafiği de hızla artmaktadır. Bu aşırı veri trafiğinde, veri güvenliği oldukça önemlidir. Veri güvenliği, yetkisiz erişime karşı verilerin korunması olarak tanımlanabilmektedir. Veri güvenliğinde en önemli konu, kişisel veya kurumsal verilerin korunmasının yanı sıra, verilerin gizliliğinin sağlanması ve bütünlüğünün doğrulanmasıdır.

Veriler cep telefonu, tablet/dizüstü/masaüstü bilgisayarlar, ağlar, veri tabanları, sunucular vb. ortamlarda saklanmaktadır. Gerek bu ortamların gerekse ortamda saklanan verinin güvenliğinin sağlanması çok önemlidir. Özellikle de sayısallaşan verilerin son yıllarda önemli bir değer ifade etmesi ve karşılığında kazanç elde edilebilir hale gelmesi veri güvenliğinin gerekliliğini son derece arttırmaktadır.

Kurumların sahip olduğu varlıkların en başında veri gelmektedir. Kurumlar, ellerindeki verileri toplayabilir, düzenleyebilir, bunlardan değer elde edebilir, satışa sunabilir, bir ürün veya hizmete dönüştürebilir, paylaşabilir ve bu faaliyetlerden gelir sağlayabilirler.

Bu veriler, çalışanlar, ürünler, müşteriler, pazar, rakipler ve benzeri unsurlar hakkında bilgi edinmeyi ve geleceğe yönelik planlamalar yapmayı mümkün kılmaktadır. Bu bilgiler, maddi açıdan ve stratejik açıdan önemli olduğundan, siber saldırganlar için oldukça değerlidir. Siber saldırganlar, bu bilgilere erişmek ve bu veriler üzerinden yasadışı yollardan gelir elde etmek için çaba sarf edebilmektedirler. Bu nedenle, büyük koruma ekiplerine sahip kurumlar yerine, güvenlik duvarı ürünleri dahi kullanmayan küçük işletmeleri daha kolay hedef olarak görerek, çaba harcamadan kolayca gelir elde etmeye odaklanabilmektedirler. Bu verilere izinsiz olarak erişilmesi, birçok soruna neden olabilmektedir. Banka hesap bilgilerinin veya müşteri bilgilerinin veri tabanından çalınması ve verilerin şifrelenerek fidye talep edilmesi, en sık görülen siber saldırı türleridir.

Veri iletiminde veri güvenliğinin sağlanması, şifreleme veya gizleme yoluyla gerçekleştirilmektedir. Şifreleme işlemine tabi tutulmuş veri, Kriptografi (Thambiraja ve Umarani, 2012) olarak bilinir. Kriptografi güvenli bir yöntemdir. Ancak, şifrelenen veri dikkat çekebilmektedir. Bu yüzden verinin gizli bir şekilde iletilmesi gerekebilmektedir. Bu noktada, bilgi gizleme teknikleri devreye girmektedir. Steganografi (Kadhim ve diğ., 2019) ve Filigran (Petitcolas ve diğ., 1999), mesajı gizlemek için kullanılan bilgi gizleme teknikleridir. Her ikisi de veriyi gizler ancak kullanım nedenleri farklıdır. Steganografide amaç verinin gizli ve hatta mümkün olduğunca tespit edilemez bir şekilde iletilmesi iken, filigranlamada ise içeriklerin telif haklarının korunması ön plandadır.

Kriptografi, Steganografi ve Filigranlama ile ilgili karşılaştırmalar Tablo 1.1'de verilmiştir.

Tablo 1.1. Bilgi güvenliği tekniklerinin özelliklerinin karşılaştırılması

Özellikler	Steganografi	Filigran	Kriptografi
Hedef	Gizli verileri tespitten koruma	Örtü medyasının orijinalliğinin korunması	Verilerin biçimini veya içeriğini gizleme
Örtü Seçimi	Özgür	Kısıtlı	Yok
Zorluklar	Algılanamazlık, Güvenlik ve Kapasite	Sağlamlık	Sağlamlık
Anahtar	İsteğe Bağlı	İsteğe Bağlı	Zorunlu
Çıktı	Stego-dosya	Filigranlı-dosya	Şifrelenmiş Metin
Görünürlük	Görünmez	Bazen	Her Zaman
Sistem Çökme Koşulu	Algılanma	Değiştirilme veya Silinme	Çözülme
Saldırılar	Steganaliz	Herhangi bir görüntü işleme	Kriptanaliz

İnternet ortamında kullanılan tüm dijital içerikler, steganografinin uygulanmasını daha elverişli hale getirmiş ve araştırmacıların bu alana ilgisini arttırmıştır. Steganografi teknikleri, tersinebilirlik özelliğine göre Tersine Çevrilebilir (Reversible) ve Tersine Çevrilemez (Irreversible) olmak üzere iki gruba ayrılır. Tersine Çevrilebilir tekniklerde, stego görüntüden veri çıkarma işlemini gerçekleştirdikten sonra orijinal görüntüde bozulma olmaz. Bu yüzden orijinal görüntü yeniden elde edilebilir. Tersine Çevrilemez tekniklerde ise, gizli verinin orijinal görüntüye gizlenmesi sonucu oluşan stego görüntüden gizli veri çıkarıldığında, orijinal görüntüde bozulmalar meydana geldiğinden dolayı orijinal görüntü geri kazanılamaz. Bazı alanlarda orijinal görüntünün aslını

koruması, gizli mesaj kadar önem taşır. Verinin gizlenmesi işlemi, görüntüye veya gizli verinin iletildiği medyaya zarar vermemelidir. Tıp, Askeriye vb. birçok alanda Tersine Çevrilemez yerine Tersine Çevrilebilir teknikler tercih kullanılmaktadır.

Uygulandığı domain'e göre steganografik teknikler ikiye ayrılır : Uzamsal (Spatial) Domain, Frekans (Frequency) Domain. Bir görüntü, matrisin her bir öğesinin piksel yoğunluğunu temsil ettiği bir 2D matris biçiminde temsil edilebilir. Bir görüntünün yoğunluk dağılımını gösteren bu matris durumuna Uzamsal Alan adı verilir. Frekans Domain'de ise yöntemler, bir görüntünün Fourier Dönüşümüne dayanır. Frekans alanında, önce görüntüler dönüştürülür ve ardından mesaj, görüntünün içine yerleştirilir.

İki domain arasındaki bazı farklılıklar:

- Uzamsal domain görüntü düzleminin kendisiyle ilgilenirken, Frekans alanı piksel değişim oranıyla ilgilenir.
- Uzamsal domain, piksellerin doğrudan manipülasyonuna dayalı olarak çalışır, Frekans alanı ise fourier dönüşümünün değiştirilmesine dayalı olarak çalışır.
- Uzamsal domainin anlaşılması daha kolay olabilirken, Frekans domainin anlaşılması daha az kolay olabilir.
- Uzamsal domain daha az maliyetiyken, Frekans domaini nispeten daha fazla maliyetlidir.
- Uzamsal domain daha az zaman alırken, Frekans domain hesaplamalarının yapılması bilgisayarda daha fazla zaman alır.
- Veriler Frekans domainine gömüldüğünde, gizli veriler daha sağlam alanlarda bulunur, görüntünün tamamına yayılır ve istatistiksel saldırılara karşı daha iyi direnç sağlar.

Tez çalışması kapsamında, uzamsal domainde yaygın kullanılan teknikler detaylı olarak incelenmiş olup, bu yöntemlerin beraber ve etkili bir şekilde kullanımına yönelik yeni bir veri gizleme yöntemi sunulmaktadır. Önerilen yöntemde, örtü görüntü birinci piksel değeri kullanılarak gizleme yapılacak yöntem sayısı ve yöntemleri gösteren tablo belirli bir kurala göre oluşturulmaktadır. Aynı örtü görüntülerde farklı yöntem sayısı, farklı örtü görüntülerde farklı yöntem sayısına göre, veri gizleme yöntemlerini gösteren tablo farklı konumlara saklanmaktadır. Bu tabloda yer alan yöntemlere göre veri gizleme işlemi yapılmakta ve tablo her işlemden sonra kaydırılmaktadır. Bu sayede her bir piksele farklı

yöntemlerle veri gizleme yapılmış olmaktadır. Önerilen yöntemin kapasitesini, kullanılan yöntemlerin ortalaması belirlemektedir. Deneysel sonuçlar incelendiğinde, algılanamazlığı yüksek, güvenli ve ortalama kapasite sağlayan literatürde bulunan yöntemlerin beraber kullanılmasını sağlayan yeni bir yöntem sunulmuştur.

Tez çalışmasının bir sonraki bölümde literatür taraması, çalışmanın amacı, sayısal steganografi; steganografinin çeşitleri, hedefleri, özellikleri ve değerlendirme kriterleri hakkında bilgiler verilmektedir. Üçüncü bölümde, Uzamsal Domain'de yaygın kullanılan bazı steganografi teknikleri ile hibrit bir yöntem, örneklerle açıklanmaktadır. Önerilen Yöntem bölümünde, önerilen yöntem, metin ve grafiklerle detaylı olarak anlatılmakta, yöntemin uygulanmasında karşılaşılan sorunun nasıl giderildiği ile ilgili bilgi verilmektedir. Deneysel Çalışmalar bölümünde, Uzamsal Domain'de yaygın kullanılan teknikler ve önerilen yöntemden elde edilen veriler, karşılaştırmalı tablolar ve grafikler ile paylaşılmaktadır. Sonuç bölümünde ise, uzamsal yöntemlerden bazılarını içeren çalışma ve önerilen yöntem ile ilgili sonuçlar yorumlanmıştır.

2. GENEL BİLGİLER

Bu bölümde, steganografi hakkında genel bir bilgi verildikten sonra görüntü steganografisinin detaylı anlatımı sunulacaktır. Ayrıca, başarılı bir görüntü steganografi algoritmasının taşıması gereken özellikler, matematiksel örnekleriyle birlikte yaygın olarak kullanılan bazı teknikler, steganaliz konuları ve literatür taraması yer almaktadır.

En düşük anlamlı bit (Least Significant Bit - LSB) (Chan ve Cheng, 2004; Solak ve Altınışık, 2019; Solak ve Altınışık, 2021), en yaygın kullanılan ilk uzamsal alan steganografi tekniğidir. LSB steganografisi, bir örtü görüntüsünde, göze çarpan görsel bozulmalar olmaksızın büyük gizli bilgileri gizleyebilen temel ve geleneksel yöntemlerden biridir (Li ve diğ., 2011). Gizli mesaj bitlerin, verinin gizleneceği örtü görüntüdeki sıralı veya rastgele seçilen piksellerin en düşük anlamlı bitleriyle değiştirme yolunu izlemektedir. İsteğe bağlı olarak, piksellerin seçimi veya gömme sırası, bir stego anahtarı ile belirlenebilir. Steganografik yöntemlerde, zaman içinde, LSB'nin piksel veya bit düzlemlerinin farklı varyasyonları kullanılmıştır. Bu yöntemlerin çoğu, yükü optimize etmek amacıyla geliştirilmiştir. Kedi sürüsü stratejisi kullanılarak optimize edilmiş LSB ikamesi (Wang ve diğ., 2012), enterpolasyon görüntüsü ile LSB ikamesi (Jung ve diğ., 2015) ve LSB ikamesi kullanan tersine çevrilebilir şifreli tıbbi görüntü (Liu ve diğ., 2016) gibi farklı birçok uyarlamaları mevcuttur. Histogram algılama saldırılarına direnen, örtü görüntüsüne göre benzer bir stego görüntü histogramı oluşturmak için kasıtlı olarak bazı ekstra bitleri gömdüğü başka bir iyi bilinen yaklaşım ise LSB+ 'dır. Bununla birlikte, LSB+ yöntemi yine de örtü görüntüsünün istatistiksel ve algısal özelliklerini etkilemektedir. (Qazanfari ve Safabakhsh, 2014) 'te, yazarlar, hassas pikselleri tanımlamak ve anahtar kilidi yöntemini kullanarak fazladan bit gömülmesini önlemek için mevcut LSB+ tabanlı yöntemi geliştirmektedir. LSB++ yöntemi, örtü resminin algısal ve istatistiksel özniteliklerinde yapılan değişikliklerin miktarını azaltır. Bu yöntem, LSB +'da ekstra gömme işleminin neden olduğu histogramdan ve istatistiksel saldırılardan kaçınmayı da sağlar. Bu teknik aynı zamanda tepe sinyal-gürültü oranının (PSNR) görsel kalitesini de geliştirebilmektedir. Son zamanlarda (Carneiro Tavares ve Madeiro Bernardino Junior, 2016), Dünya-Avı bulmacasından esinlenen LSB Kelime Avı (LSB WH) olarak adlandırılan LSB tabanlı yöntemi tanıttı. Yaklaşımın motivasyonu, stego-görüntünün görsel kalitesini dolaylı olarak artıran piksel değeri başına değişikliği

azaltmaktır. LSB WH yaklaşımı yalnızca istatistiksel ki-kare tespit saldırılarına direnebilmektedir. Gömme işleminden önce gizli mesajın güvenliğini artırmak için farklı steganografik yöntemler şifreleme algoritmaları ile ortaya çıkar. Amirtharajan ve Balaguru Rayappan (Amirtharajan ve Balaguru Rayappan, 2012) LSB ikamesi ile rastgele k-bit gömme yaklaşımını kullandı. Örtü görüntüsü, eşit boyutta üst üste binmeyen bloklara bölünür ve şifrelenmiş gizli veriler, dört farklı rastgele yürüyüş yoluyla her bloğa gömülür. Herhangi bir rastgele yürüyüş belirli bir blok için minimum bozulma üretirse, bu aynı blokta kaydedilir ve gizli bir anahtar olarak tutulur. Sonuç olarak, stego-imajının sağlamlığını sağlar ve kalitesini arttırır. Benzer şekilde, Muhammad ve diğ. (Muhammad ve diğ., 2016 a), LSB ikamesine dayanan güvenli bir gömme yöntemi önerdi. Bu yöntemde, farklı şifreleme seviyelerine sahip stego anahtar kullanılmaktaydı. Gizli bilgiler, gömme işleminden önce çok seviyeli şifreleme algoritması (MLEA) ile şifrelenirken, stego anahtarı iki seviyeli şifreleme algoritması kullanılarak şifrelenir. Ayrıca, şifrelenmiş veriler, kırmızı kanala, MLEA'ya ve gizli verilere bağlı olarak uyarlanabilir LSB gömme yaklaşımı ile gömülür. Deneysel sonuçlar, önerilen yöntemin güvenlik ve görsel kalite arasında daha iyi bir denge sağladığını göstermiştir. Ayrıca, geleneksel şifreleme tekniklerine kıyasla hesaplama daha az karmaşıktır. Uyarlanabilir LSB tabanlı bir yöntem, Nguyen (Nguyen ve diğ., 2015) vd. tarafından geliştirilmiş olup tüm görüntü bölgelerini (pürüzsüz veya gürültülü) kullanarak blok veri gizlemeyi (MPBDH) kullanan çok bitli düzlem görüntü steganografisi sağlamıştır. Yöntemde, birden fazla bitlik düzlem kullandı ve gizli verileri gömmek için bir örtü görüntüsünün karmaşık bölgelerini seçecek uyarlanabilir bir karmaşıklık eşiği uyguladı. Gömme kapasitesi ve güvenlik performansı, önceki piksel / blok tabanlı uyarlanabilir LSB yöntemlerine göre önemli ölçüde iyileştirildi. (Tuncer ve Sönmez, 2019), çok-örtülü uyarlanabilir steganografiye dayanan yeni bir yöntem önerdi. Bu yöntemde gizli görüntü gömme, farklı örtü görüntülerinin dokulu bölgelerine uyarlanabilmektedir. LSB'lerde gizli veri gömme işlemi, XOR tabanlı işlem kullanılarak çıkarılabilir, SPAM özelliklerine dayalı steganaliz ve AUS steganalizi gibi modern steganaliz tespit saldırılarına direnebilir (Pevny ve diğ., 2010). LSB tabanlı steganografik yöntemlerde, stego görüntülerin görsel kalitesi korunurken, gömülü yükü artırmak için birçok girişimde bulunulmuştur. LSB, steganalize karşı hassas olduğundan bunun üstesinden gelebilmek için bazen LSB yöntemi, diğer tekniklerle birleştirilmiştir. Örneğin,

Hussain ve ark. (Hussain ve diğ., 2016), uyarlanabilir LSB'yi, en doğru rakam değiştirme (RMDR) birleştirmiştir. Örtü görüntünün pikselindeki bitler yerine rakamlar kullanılarak, gerek görsellik gerekse kapasite olarak gelişim sağlanırken RS steganalizine (Fridrich ve diğ., 2001) yakalanma riskinin azaltılabilmesi sağlanabilir ama bu yöntem daha yüksek (> 1 bpp) gömme hızında SPAM (Pevny ve diğ., 2010) 'e direnememektedir. Yükü artırmak için modulo üç stratejisini kullanan LSB ile (Xu ve diğ., 2016)'da bir çalışma sunulmuştur. Her pikseldeki iki üçlü sayı gömülebilir, bu da genellikle pikselin iki LSB'sini değiştirerek taşma / yetersizlik sorunlarının nedeni olabilir. Böylece gömme işleminden önce piksele ± 1'lik bir ön işlem uygulanır. Önerilen yöntem, 3 bitlik LSB gömme yöntemlerine göre benzer görsel kaliteyi (PSNR değeri olarak) korurken gömme kapasitesini de geliştirir, ancak aynı zamanda uyarlanabilir gömme özelliklerinin olmaması nedeniyle yüksek gömme oranlarında modern steganaliz tarafından daha kolay ortaya çıkarılmaktadır.

LSB tabanlı teknikler basit veri gizleme yöntemidirler ve diğer yöntemlerle entegre edilmesi bakımından oldukça uyumludurlar. Ancak, gizli verinin gömülme kapasitesi ile stego-görüntünün görsel kalitesi arasında doğrudan bir ilişki vardır. Bu nedenle LSB ile maksimum seviyeye ulaşmaya çalışarak gömme kapasitesini artırmak, genel görsel kaliteyi düşürebilmektedir. Bunun üstesinden gelebilmek için, (Wu ve Tsai, 2003), piksel farkı değerini (Pixel Value Difference-PVD) baz alan bir steganografik yaklaşım önermiştir. Bu yöntem, komşu pikseller arasındaki fark değerine dayanarak gizli veri gömülebilme miktarını belirlemektedir. Gizlenebilecek veri miktarı, ard arda gelen iki piksel arasındaki farkın ne kadar fazla olduğu ile doğrudan orantılıdır. Pikseller komşu ikili bloklar şeklinde gruplandırılır. Her blokta, bitlerin gömülme boyutuna karar vermek için iki piksel arasındaki fark değeri hesaplanır ve bu fark değerleri bir dizi aralıkta gruplandırılır. Bir değer aralıkları tablosundaki aralık seviyelerinin veya aralıkların seçimi, insan görüşünün hassasiyetine dayanır. Son olarak, fark değeri, gizli veriler boyunca yeni fark değeri ile değiştirilir. Gizli verilerin gömülme miktarı, tablonun aralık seviyeleri tarafından belirlenir ve görüntünün doku farkındaki yüksekliğe doğrudan bağlıdır. Genellikle, PVD yaklaşımı, LSB ikame yöntemine göre daha az görsel algılanabilirliğe sahiptir ve daha çok verinin gizlenmesine olanak tanır. PSNR değeri genellikle 40 dB'nin üzerinde kalır ve RS algılama saldırılarını atlayabilir. PVD yönteminin ana sorunu, histogramda, gizli bir mesajın varlığını ortaya çıkabilmektedir.

İkinci olarak, sınırdan düşme (FOBP) önemli sorunlardan biridir. Üçüncü olarak görüntüler genellikle yüksek doku yerine daha pürüzsüz alan içerir, bu nedenle gizli veri bitleri, küçük bir değerle aralıklarda gizlenecektir. Literatürde, PVD'nin geliştirilmesi ile ilgili çalışma yapılmıştır. Örneğin Çoklu Piksel Farkı (MPD) (Yang ve diğ., 2010), Modül İşlevi (MF) (Pan ve diğ., 2011; Liao ve diğ., 2012 a, 2013), blok tabanlı PVD (Yang ve diğ., 2011) ve çeşitli (Hussain ve diğ., 2015, 2017; Liao ve diğ., 2018) 'de tartışılan yöntemler. Gömme kapasitesini iyileştirmek için (Hussain ve diğ., 2016), PVD yöntemini uyarlanabilir LSB ikamesi ve optimum piksel ayarlama süreciyle birleştirilmiştir.

İyi görsel kalite ve yüksek taşıma kapasitesi elde etmek için (Huang, 2015), üç yollu PVD ve mod seçim sürecini birleştirerek çok yollu bir PVD yöntemi önermişti ki bu kombinasyon görsel kaliteyi iyileştirmesine rağmen (Khodaei ve Faez, 2012) ile karşılaştırıldığında düşük yüke sahiptir. Mandal vd. (Mandal ve Das, 2012) , orijinal PVD ile benzer yük ve algılanamazlığı korurken sınırdan düşme koşullarını çözmek için modül işlevli uyarlanabilir bir PVD yöntemi önerdi. Üç yollu PVD'yi kullanmak için Lee ve ark. (Lee ve diğ., 2012), gizli görüntü iletişiminin sıkıştırma kombinasyonu ile pratik bir şekilde yerleştirilmesini önerdi. Gizli görüntü (veriler) JPEG2000 tarafından yüksek sıkıştırma oranında sıkıştırılır ve üç yollu PVD ile gömülür. Gömme ve çıkarma işleminden sonra, yüksek sıkıştırılma oranı nedeniyle gizli görüntünün kalitesi bozulduğu gözlemlenmiştir. Ayrıca, geri kazanılan gizli görüntüdeki görsel bozulmayı azaltmak için bir artık değer kodlaması önerilmektedir. Önerilen yöntem, ikili istatistiksel tespit saldırılarından kaçınırken gizliliği sağlayabilmiştir.

Balasubramanian vd. (Balasubramanian ve diğ., 2014), görsel bozulmayı ve düşük yükü işlemek için sekizlik bir piksel eşleştirme şeması önerdi. Yöntem, daha büyük modifikasyon için kenar alanlarının düz alanlara göre daha tolere edilebilir olduğu ve dolayısıyla daha fazla gizli veri tutabileceği ilkesine dayanmaktadır. Böylelikle bölge seçimi aşamasında ilk olarak kenar alanlar belirlenir. Daha sonra, her piksel çiftinin içine gömülebilen bit sayısı, aralık tablosuna başvurarak belirlenir. Bölgeler, verilen gizli mesajı gizlemek için yeterince büyükse, gizli veriler seçilen bölgelere gömülür. Aksi takdirde, tüm kenar bölgeleri kullanıldıktan sonra düz bölgeler gömme için kullanılır. Veri gizleme, sekizlik PVD şemasına göre gerçekleştirilir. Son olarak, algısal kaliteyi ve istatistiksel tespit edilemezliği iyileştirmek için yeniden piksel ayarlaması uygulanır. Liu

ve ark. (Liu ve diğ., 2014), yükü iyileştirmek için piksel bloklarının karmaşıklığına dayanan uyarlanabilir bir PVD önerdi.

Shen ve diğerleri tarafından sunulan PVD hibrit yönteminde (Shen ve diğ., 2015 a), gizli kapasiteyi iyileştirmek için PVD'yi modülüs işleviyle birleştirdi. Yöntem, renkli görüntüde R, G ve B düzlemlerinin korelasyonunun avantajlarından tam olarak yararlanmaktadır. Gizli bitlerin sayısı, karşılık gelen G düzlemi piksellerinin farkı ile belirlenir. Ayrıca, taşma ve alt akış problemlerini sürdürmek için çeşitli ayarlama işlemleri uygulanır. Önerilen yöntem, kabul edilebilir bir görsel kalite sağlarken RS diyagramına ve histogram analizine karşı güvence altına alınmıştır. Ancak, diğer PVD tabanlı yöntemlere göre düşük yük sıkıntısı vardır. Modifikasyon yönünden yararlanma (EMD) steganografik yöntemini ile PVD'nin hibrit kullanıldığı bir başka yöntem, Shen ve diğerleri tarafından yük ve algılanamazlığı iyileştirmek için önerilmiştir (Shen ve Huang, 2015 b). İlk olarak, bir örtü görüntüsü, geleneksel zig-zag sıralaması yerine Hilbert doldurma eğrisi ile 1D piksel dizisine eşlenir. Hilbert doldurma sırası, raster taramaya veya zig-zag tarama sıralamalarına karşı özellikleri korumada daha iyiydi. Taşma / yetersizlik sorunlarını çözebilir ve gömme bozulmasını en aza indirebilirdi. Son zamanlarda, G. Swain (Swain, 2015) , dikey ve yatay kenarları kullanan iki uyarlanabilir PVD tabanlı steganografik çözüm önerdi. İlk yaklaşım 2 × 2 piksel blokları kullandı ve ikincisi 3 × 3 piksel bloklara uygulandı. Her iki yöntem de daha büyük kapasiteyi ve stego görüntülerin daha iyi görsel kalitesini hedeflemiştir. Yakın zamanda, I. R. Grajeda-Marín ve ark. (Grajeda-Marín ve diğ., 2016), PVD'deki taşma ve yetersizlik sorununu çözmek için başka bir çözüm sundu. Yöntem, üç yollu PVD'ye odaklanır ve her bir gömme bloğu için en uygun piksel değerlerini hesaplar. Sonuç olarak, yükü iyileştirirken yetersizlik (underflow) ve taşma (overflow) sorunlarını çözebilir. Khodaei vd. (Khodaei ve diğ., 2016), LSB yöntemleriyle PVD'ye dayalı uyarlanabilir bir hibrit gömme yaklaşımı önerdi. Örtü görüntüsünü iki piksel bloğuna böldü ve dahası, bu iki piksel arasındaki farkı daha iyi tahmin edebildi. Gizli bitlerin sayısı, fark değerine ve uyarlamalı kullanılan uyarlamalı LSB gömme şemasına göre tahmin edilir. Önerilen yöntem, farkı, örtü görüntüsü piksellerinde olduğu gibi korumak için bir yeniden ayarlama süreci getirmiştir. Benzer şekilde G. Swain (Swain, 2016), uyarlamalı steganografik yöntem için yönlü PVD'yi LSB ile birleştirdi. İlk olarak, k-bit gizli verilerini 2 × 2 piksel bloğundan sol üst piksele yerleştirdi. Daha sonra, PVD gömme işlemi, sol üst taban pikseline ve kalan diğer

piksellere yatay ve dikey kenar yönlerinde uygulandı. Sırasıyla yalnızca PSNR ve PSNR'yi yüksek yük ile iyileştirmek için Tip 1 ve Tip 2 olmak üzere iki gömme tekniği önerildi.

Değişim Yönünü Kullanma (EMD), iyi bilinen ve stego görüntülerinin görüntü kalitesini üst düzeyde koruyan bir gömme tekniğidir (Zhang ve Wang, 2006). EMD, örtü görüntüden alınan "n" adet piksele, gizli verinin (2n+1)'lik sayı sistemine dönüştürülmüş halinin gizlenmesi işlemidir. Bozulma aralığının maksimum piksel değeri sadece (± 1) 'dir. Başka bir deyişle, EMD, görüntüdeki piksel yoğunluğunun yerel varyasyonunu belirlemek için belirli bir sayı tabanını kullanır, bu nedenle yüksek doku alanlarındaki pikseller daha fazla gizli mesajı saklamaktadır. Sonuç olarak EMD, LSB ve PVD yöntemleriyle karşılaştırıldığında iyi bir görsel kalite elde etmektedir. EMD yönteminde en yüksek kapasite, (n = 2) iki piksel için uygulandığında elde edilen piksel başına 1,16 bittir. "n" değeri arttıkça piksel başına gizlenebilen bit miktarı azalmaktadır. Bu durumu çözmek için EMD tabanlı farklı yöntemler geliştirilmiştir. (Kieu ve Chang, 2011)-(Kuo ve diğ., 2013 a)-(Kuo ve diğ., 2013 b)-(Liao ve diğ., 2012 b)-(Liao ve diğ., 2017) 'de yazarlar, yükü ve algılanamazlığı iyileştirmek için HoEMD ve AdEMD adlı iki EMD tabanlı yerleştirme tekniği önerdiler. HoEMD konsepti, daha büyük varyasyonlara sahip piksellerin daha büyük yönlere sahip olduğu ve daha büyük gömme yüküne sahip olabileceği piksel yönünden yararlanmaktı. Öte yandan, AdEMD mantığında, piksellerin kenar bölgelere ait olması daha fazla gizli veri karşılayabilmekte, ancak bunlar taşma sorunu yaşatabilmekteydi. T. D. Kieu ve Chang (Kieu ve Chang, 2011), Değişim Yönünü Tamamen Kullanan (FEMD) (2n+1) sayı sistemi tabanlı bir sistem önerdi. FEMD tekniği, (Zhang ve Wang, 2006) 'ya karşı iyi görsel algılanamazlık ile birlikte gömme kapasitesini 1 bpp'den 4,5 bpp'ye yükseltti. Bir ek yük olarak yerleştirmek için bir arama matrisi gerektiriyordu ve taşma koşullarının üstesinden de gelemedi. Kuo ve Kao (Kuo ve Kao, 2013 b) bahsi geçen taşma sorununu çözdü ve gömme kapasitesini korudu. Gizli veriler, formül işlemleriyle (veya bir arama matrisi kullanmadan) doğrudan gömülür ve Değişim Yönünü Tamamen Kullanan (FFEMD) yöntem olarak bilinir. Benzer şekilde, (Kuo ve diğ., 2013 a) 'de sunulan yöntem, Genelleştirilmiş Değişim Yönünü Kullanma (GEMD) olarak genelleştirilmiştir. Basitçe, GEMD tekniği her piksel için ikiden fazla gizli biti saklayamaz; bu arada gizli veri gömme sırasında gruptaki piksellerde hiçbir değişim olmayacağı gibi birden fazla pikselde de değişim olabilir. Piksel değiştirme probleminin

zayıflığını çözmek için (Kuo ve diğ., 2016 a) W.-C. Kuo vd. Modified Signed-Digit (MSD) olarak bir yöntem önerdi. Yalnızca ±1 aralığındaki n/2 pikseli değiştirir ve n pikseli de artırsa bile 1 bpp kapasiteye sahiptir. MSD şeması, RS steganalizine (Fridrich ve diğ., 2001) karşı iyi bir algılanamazlık sunar. W.- C. Kuo vd. tarafından ortaya konan başka bir yöntem (Kuo ve diğ., 2016 b) ise gömme yükünü daha da iyileştirmek için çok bitli bir kodlama işlevi kullanır. Önerilen yöntem, her piksel için ortalama olarak (n+1/n) piksel başına gömülü bit sayısıyla belirlenir. Gizli veri dönüştürme ek yükünü azaltabilir ve ayrıca bitişik piksel ilişkisinin esnekliğini sağlayabilir. Bu arada, MSD yöntemi, RS ve bit düz algılama analizine karşı güvenliği korur, ancak mevcut EMD tabanlı yöntemlerle karşılaştırıldığında düşük görsel kalite sunar çünkü daha yüksek gömme kapasitesi, daha düşük görsel kaliteye neden olmuştur. İyi bir algılanamazlıkla gömme yükünü iyileştirmek için K. Wu ve ark. (Wu ve diğ., 2015) LSB ile EMD'ye hibrit bir yaklaşım ve tahmin hatalarının (MPE) modifikasyonunu önerdi. Yöntem hedefleri yerine getirdi, ancak histogram ve RS algılama analizi gibi güven açısından sorunluydu. Bununla birlikte, çoğu EMD tabanlı yöntem, yukarıda adı geçen yöntemlerde gömme sürecinden önce n-tabanlı notasyon işlemi uygulamıştır ki bu, tekniklerinin ana dezavantajı haline gelmektedir.

2.1. Çalışmanın Amacı

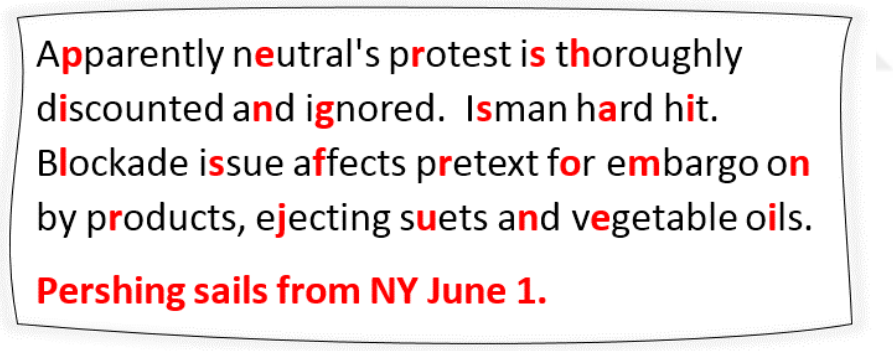
Uzamsal Domainde, görüntü steganografisinde yaygın kullanılan yöntemler ile tersine çevrilemez birçok yöntem geliştirilmiştir ve geliştirilmeye devam edilmektedir. Çalışmamızda, Uzamsal Domainde yaygın kullanılan yöntemler detaylı olarak incelenmiş olup başarım sonuçları sunulmuştur. Çalışmamız ile, güvenliğin ve gizliliğin ön planda olduğu yeni bir yöntem geliştirilmesi hedeflenmiş ve elde edilen bulgular paylaşılmıştır. Uygulamada, önemli birçok karar mekanizması, çeşitli değişkenlere bağlı tutularak güvenlik konusunda bir gelişim hedeflenmiştir. Yöntemimizde, kullanılacak örtü görüntünün kendisi ve ebatları birer değişken ifade etmekte olup uygulamada kullanılacak olan yöntem sayısının ile sırasının gizleneceği piksel koordinatlarını ve R kanalına uygulanacak yöntemi belirlemektedir. Uygulamamızda, G ve B kanallarında uygulanmak üzere 4 yöntem seçilmiş olup yöntem-sıra bilgisinin aktarılması için 2x4=8 piksele ihtiyaç duyulmuştur. Sadece 8 piksel daha fazla kullanılarak yöntem sayısı 8'e çıkarılabilir ve böylece güvenlik seviyesi ve karmaşıklık arttırılabilir. 16 pikselden

kaynaklı meydana gelecek kapasite kaybı ve görüntü kalitesindeki düşüş önemsenmeyecek kadar düşük olacaktır. Ayrıca, alıcı taraf ile paylaşılmış olan Yöntemler Tablosu ve R Kanalı Yöntemleri Tablosunun başlangıç dizilimleri farklı seçilebilir. Tüm bu değişkenlere bağlılık durumu, geliştirilen yöntemin kolay bir şekilde farklılaştırılması konusunda son derece esneklik sağlamaktadır. Bu yönüyle önerilen yöntem, konusunda farklı ve öncü olmakla birlikte geliştirilmeye son derece açıktır.

2.2. Steganografi Nedir?

Steganografi, dijital medyalara (video, metin, ses, görsel) veri gizleme tekniklerini içeren bilimdir (Hussain ve diğ., 2018). Karşı tarafa iletilecek olan veri, dikkat çekmeyecek bir dijital bir medyada saklanır. Böylece, üçüncü şahısların, mesajın varlığından haberdar olması engellenir.

Steganografi kelimesi eski Yunanca'da kaplanmış, gizli, saklı anlamına gelen Steganos (στεγανός) ile çizim, yazım anlamına gelen Graphy (γραφή) kelimelerinden oluşur.



Şekil 2.1. II.Dünya savaşında gönderilen bir gizli mesaj

Tarihte, birçok farklı biçimde uygulamaları görülmüştür. Örnek olarak, mesajlar kullanılmamış bir tahta üzerine yazılıp altındaki yazının görülmeyeceği şekilde tahtanın üzeri mumla kaplanır ve kullanılmamış boş tablet görünümü verilirdi. Mesajı alıcı taraf mumu eritir ve mesajı görürdü. Demeratus tarafından Yunanistan'ın işgal edileceği haberi bu yöntemle Sparta'ya ulaştırılmıştır (Kadhim ve diğ., 2019). II.Dünya Savaşı'nda gizli mesajlaşmalar için, Enigma makinesi, görünmez mürekkep, Şekil 2.1'de görüldüğü gibi kelimelerin belirli harflerinin bir araya getirilmesi ile oluşan metinler vb. birçok teknik

kullanıldı (Kadhim ve diğ., 2019). Herodot'un bir hikâyesine göre, Şekil 2.2'de de görüldüğü üzere, bir kölenin saçları kazıtılıp kafa derisine gizli mesaj yazılmış ve kölenin saçları uzadıktan sonra alıcı tarafa gönderilmiştir. Böylece, Pers saldırısının olacağını haber veren mesaj, dikkat çekmeden gerekli yere ulaşabilmiş ve kölenin saçları tekrar kesilerek uyarı okunabilmiştir.

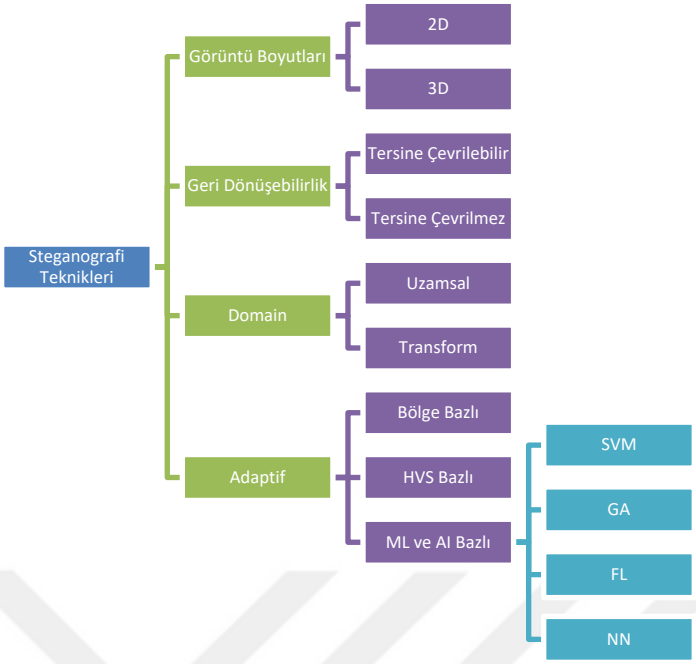


Şekil 2.2. Kölenin kafasına yazılan gizli mesaj

Steganografi, bir gizli mesajın (secret-message) örtü medya (cover-media) adı verilen bir dijital nesne içerisinde gizlenmesini içeren bir tekniktir. Veri gizleme işlemi, var olan ya da yeni üretilen bir yöntem kullanılarak gerçekleştirilir. Oluşturulan stego-medya (stego-media), örtü medyada saklanan gizli veriyi içerir. Eğer gizlenmiş verinin çözülmesi için ek bilgilere ihtiyaç duyulursa, stego-anahtar (stego-key) adı verilen ve bu bilgileri içeren bir veri oluşturulabilir.

2.2.1. Görüntü Steganografisi Teknikleri

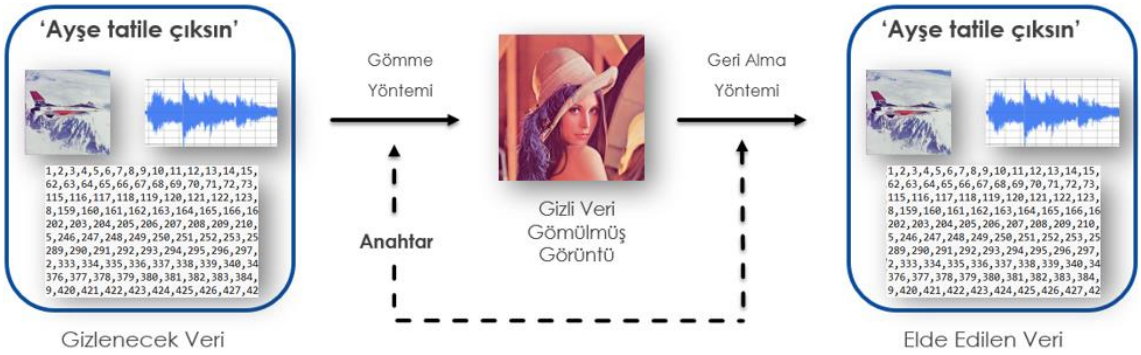
Steganografinin uygulama ve veriyi yerleştirme işlemlerine dahil edilen aşamalara bağlı olarak görüntü steganografisi için birçok farklı, hatta hibrit yöntemler önerilmiştir. Bu nedenle, bu sistemler birden fazla yönteme göre sınıflandırılabilmektedir. Steganografi tekniklerinin sınıflandırılması ile ilgili detaylı bir şema Şekil 2.3'te görülmektedir (Kadhim ve diğ., 2019). İncelemelerimiz, Uzamsal Domain'de ve Tersinir Olmayan teknikler üzerine olacaktır.



Şekil 2.3. Steganografi tekniklerinin sınıflandırılması

2.2.2. Sayısal Steganografi Çeşitleri

Şekil 2.4 'te genel hatlarıyla Sayısal Steganografi Süreci görülmektedir. İlk olarak gizlenecek bir veri seçilir. Bu veri bir metin, ses, görüntü, video vb. olabilir. Verinin gizleneceği yöntem ve bu yönteme bağlı olarak bir anahtar seçilip seçilmeyeceğine karar verilir. Sonraki adımda bir örtü medyaya ihtiyaç vardır. Şekil 2.4 'te örtü medya olarak Lena görüntüsü seçilmiştir. Veriler bu örtü görüntüye saklanmaktadır. Alıcı tarafta ise süreç tersine işletilerek gizli veri tekrar elde edilmektedir.



Şekil 2.4. Sayısal görüntü steganografisi süreci

Genel olarak sayısal steganografi çeşitleri aşağıda kısaca açıklanmıştır.

Metin Steganografisi: Metin steganografisi, metin biçimlendirmesini değiştirerek veya metin öğelerinin (örneğin, karakterler) belirli özelliklerini değiştirerek elde edilebilmektedir. Amaç, güvenilir bir şekilde kodu çözülebilen (gürültü varlığında bile) ancak okuyucu tarafından büyük ölçüde fark edilemeyen değişiklikler geliştirilmesidir.

Ses Steganografisi: Ses steganografisinde gizli mesaj, sayısallaştırılmış ses sinyaline gömülmektedir.

Görüntü Steganografisi: Görüntü steganografisinde gizli mesaj çeşitli tekniklerle görüntünün piksellerine gizlenmektedir.

Video Steganografisi: Video dosyaları genellikle görüntülerden ve seslerden oluştuğu için verileri görüntülere ve sese gizlemeye yönelik ilgili tekniklerin çoğu, video medyasına da uygulanabilmektedir.

Diğer Popüler Steganografi Çeşitleri: Bahsedilenlerin dışında, günümüzde gelişmekte olan bazı steganografi çeşitleri de vardır. Bunlar: Sabit disklerin boş alanlarına ya da ana önyükleme kaydı (MBR) vb. alanlara verilerin gizlendiği Disk Alanı Steganografisi; TCP, IP, UDP vb. protokollerin kullanıldığı Ağ Steganografisi; elektronik devre düzeyinde gizlemelerin yapıldığı Devre Steganografisi; primerler arasına gizleme yapılan DNA Steganografisi; HTML vb. dillerde, etiketler (tag) kullanılarak verinin gizlendiği Yazılım Steganografisi vb.dir.

2.3. Görüntü Steganografisi

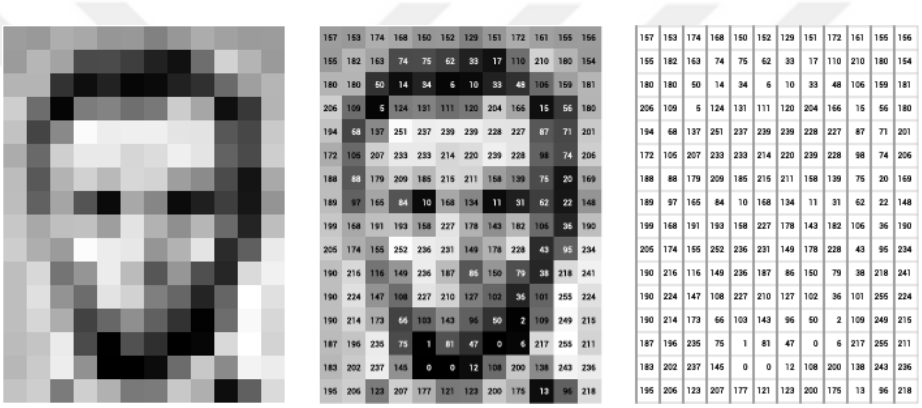
Örtü medya olarak görüntünün kullanıldığı steganografi çeşididir. Gizlenecek veri, belirli bir yöntem veya algoritma kapsamında, örtü-görüntüye gömülerek stego-görüntü elde edilir. Süreç genel hatlarıyla Şekil 2.4 ‘te belirtilmiştir.

Görüntü steganografisinde amaç, resmin kalitesinde gözle görünür bir bozulmaya sebep olmadan yüksek miktarda veriyi güvenli ve sağlam bir şekilde gizlemektir. Kullanım amacına göre öncelik bunlar arasında değişiklik gösterebilir.

2.3.1. Görüntü Yapısı

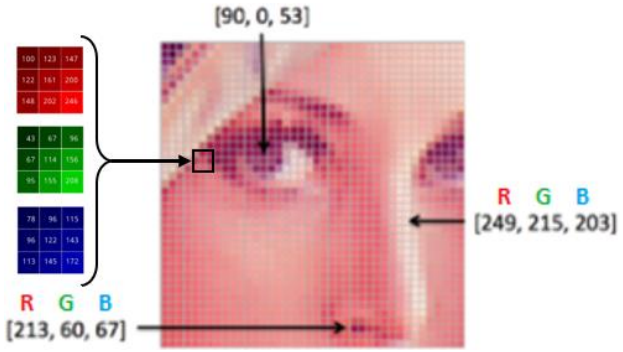
Görüntü steganografisinde yapmış olduğumuz çalışmalarda genellikle gri ölçekli veya renkli görüntüler kullanılmaktadır. Görüntü steganografisinin iyi anlaşılabilmesi için öncelikle bu görüntüler hakkında yeterli düzeyde bilgi sahibi olmak gerekmektedir.

Gri Ölçekli Görüntü: Her resim piksellerden oluşmaktadır. Gri ölçekli resimlerde her piksel bir değer ile ifade edilmektedir. Bu değer 0-255 arasındadır. Güneş ışığının ne kadar alındığı esas olduğundan, hiç güneş ışığı almadığını temsilen 0 ile siyah; tersi durumla da 255 ile beyaz kastedilir. Burada 1 piksel 8 bitten oluşmaktadır. Düşük çözünürlüklü bir resmin piksel yapısı Şekil 2.5'te ayrıntılı olarak görülmektedir.



Şekil 2.5. Gri ölçekli resmin yapısı

Renkli Görüntüler: Gri ölçekli görüntüden farklı olarak renkli görüntüler üç kanaldan oluşmaktadır çünkü her bir pikselin renk ifade edebilmesi için üç değere ihtiyaç vardır: kırmızı, yeşil ve mavi (Red-Green-Blue→RGB). Bu 3 renk karışıp istenen tek rengi oluşturmaktadır. Bu yüzden, Şekil 2.6'da da görüldüğü üzere bir piksel 3 kanaldan oluşur ki bu da 1 pikselin 3x8bit=24bit olduğu anlamına gelmektedir.



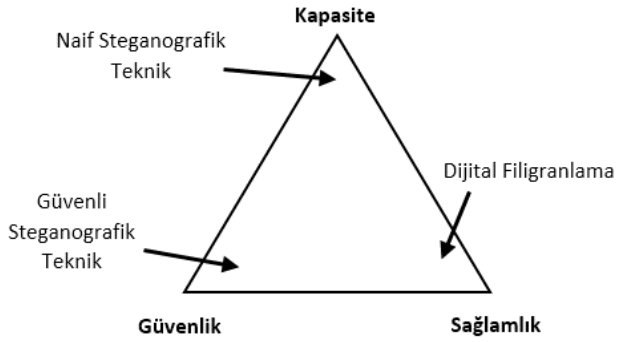
Şekil 2.6. RGB görüntünün piksel yapısı

2.3.2. Görüntü Steganografisinin Hedefleri

Genellikle, yüksek veri gizleme kapasitesine sahip steganografik yaklaşımlar, stego görüntülerde görüntü kalitesinin bozulmasına neden olur ve steganalize karşı da savunmasızdır. Diğer yandan, iyi görsel görüntü kalitesine sahip steganografik yöntemlerde de düşük yük problemdir. Bu nedenle, ideal steganografik yöntemde, yüksek kapasite, iyi görsel görüntü kalitesi ve tespit edilemezlik kriterlerinin aynı anda yerine getirilmesi hedeflenir.

2.3.3. Görüntü Steganografisinin Özellikleri

Bir görüntü steganografi tekniği geliştirilirken aşağıdaki özellikler göz önünde bulundurulmalıdır. Bunlar, steganografik bir sistemin etkinliğini test eden en etkili parametrelerdir (Kadhim ve diğ., 2019). Steganografi tekniğinin uygulanacağı sisteme göre bu özelliklerden kimisine daha fazla ağırlık verilebilir. Yine de tüm özellikler optimum bir seviyede tutulmalıdır. Örneğin dijital filigran basma durumunda, belirsizlik ve yüksek kapasite değil, yüksek güvenlik ve gizli bilgilerin anlaşılmazlığı gereklidir. Şekil 2.7, bu takas durumunu göstermektedir.



Şekil 2.7. Veri gizleme özellikleri arasındaki değiş-tokuş (Kadhim ve diğ., 2019)

2.3.3.1. Algılanamazlık (Imperceptibility)

Gizli verileri bir örtü nesnesi içinde saklamak, herhangi bir steganografi tekniğinin temel özelliğidir. Çıplak insan gözüyle veya istatistik kullanımıyla anlaşılamayacak şekilde dijital görüntüye verilerin gizlenmesine denir (Kadhim ve diğ., 2019). Orijinal veri

dosyası ve veri gizlenmiş dosya için istatistiksel veriler benzer ise, algılanamazlık yüksek demektir ki bu da veri iletişimi için güvenliğin daha iyi olması anlamına gelir.

2.3.3.2. Güvenlik (Security)

Steganografik bir sistemde, gizli veriler saldırgan tarafından tespit edilemiyorsa ya da edildikten sonra istatistiksel yöntemlerle kaldırılamıyorsa, steganografi tekniği güvenli olarak kabul edilir. Steganografik sürecin temel gerekliliği, gizli verilerin güvenli aktarımıdır. Bu nedenle, açık bir kanaldan iletim yaparken yetkisiz kişilerin veya bilgisayarların veri erişimini önlemek için güvenlik çok önemlidir.

2.3.3.3. Yük Kapasitesi (Payload Capacity)

Kapasite veya yük, görsel bozulma olmaksızın bir örtü ortamında gizlenen maksimum veri miktarını ifade etmektedir. Minimum kapsam ortamını kullanarak maksimum bilgiyi gönderme hedeflendiği için önemli bir kriterdir.

Algılanamazlıktan ve güvenlikten ödün vermeden daha yüksek yük kapasitesi sağlamak, steganografide büyük bir zorluktur ve bu yönde hibrit yöntemlerin de kullanıldığı birçok çalışma yapılmıştır.

2.3.3.4. Sağlamlık (Robustness)

Stego görüntüsü; döndürme, ölçekleme, yeniden boyutlandırma vb. görüntü işleme tekniklerini kullanan üçüncü bir el tarafından bozulsa bile, stego görüntünün gömme ve kod çözme şemasının geçerliliğini koruyabilme yeteneğidir. Steganografik sistemler, dosya formatı dönüştürme, sıkıştırma gibi stego dosyalarında herhangi bir değişiklik yapıldığında daha az dayanıklıdır.

2.3.4. Performans Değerlendirme Ölçütleri

Görüntü steganografisi tekniklerinin farklı özelliklerini değerlendirmek için farklı ölçütler kullanılmaktadır (Chan ve Cheng, 2004; Li ve diğ., 2011). Popüler metriklerden bazıları aşağıda tanımlanmıştır.

2.3.4.1. Yük Kapasitesi (BPP)

Veri gizlenmiş bir (stego) görüntüdeki her bir piksele gizlenmiş bit sayısı, Yük Kapasitesi olarak adlandırılır. BPP ile temsil edilir. Stego görüntüye gizlenen bit sayısı, örtü görüntüdeki toplam piksel sayısına bölünerek bulunur. Tekniklerin kıyaslanmasından önemli bir kriterdir. Görsel kalite ve diğer değerlendirme parametresi faktörleri korunurken BPP'nin de mümkün olduğunca yüksek olması iyi bir veri gizleme yönteminde istenen özelliklerdir ve Denklem (2.1) ile hesaplanır;

$$BPP = \frac{Gizlenen\ bit\ sayısı}{Kapak\ görüntüdeki\ toplam\ piksel\ sayısı} \tag{2.1}$$

2.3.4.2. Tepe Sinyal Gürültü Oranı (PSNR)

Gizli verileri yerleştirmek için örtü görüntü değiştirilirken, örtü görüntünün piksel değerlerinde değişiklikler meydana gelmektedir ve bu da stego görüntüsünün algılanamazlığını etkilediği için değişikliklerin incelenmesi gerekir.

Stego ve örtü görüntü arasındaki ortalama karesel hatanın (Mean Squared Error - MSE) hesaplanıp yorumlanmasıyla PSNR, görüntünün kalitesini ölçmede sıklıkla kullanılmaktadır. PSNR, 0 ile 100 dB arasında değer almaktadır. Görüntü kalitesinde, 40 dB PSNR değeri iyi sayılırken, 30dB PSNR değeri kabul edilebilirdir. Kısaca veri gizleme çalışmalarında PSNR, görüntünün kalitesini ifade eder ve 30dB altına düşmemesi beklenmektedir.

8 bitlik görüntülerde, Denklem (2.2) ile MSE hesaplandıktan sonra PSNR değeri kolaylıkla elde edilebilmektedir. MSE değeri, Denklem (2.3)'te yerine konarak PSNR değeri bulunur;

$$MSE = \frac{\sum_{i=1}^{n}(C_i - C\prime_i)^2}{n} \tag{2.2}$$

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

$$PSNR(dB) = 10log_{10}\frac{255^2}{MSE} \quad (2.3)$$

2.3.4.3. Yapısal Benzerlik İndeksi (SSIM)

İki görüntü arasındaki benzerliği incelemek için gerekli ölçüttür. SSIM değeri, 0-1 arasında bir değere karşılık gelmekte olup, 1'e yakın bir değer olması istenir. Denklem (2.4) ve Denklem (2.5) hesaplanarak Denklem (2.6)'da yerine konur ve SSIM değeri hesaplanır;

$$c_1 = k_1L^2 \quad (2.4)$$

$$c_2 = k_2L^2 \quad (2.5)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_x\sigma_y+c_2)}{(\mu_{x^2}+\mu_{y^2}+c_1)(\sigma_{x^2}+\sigma_{y^2}+c_2)} \quad (2.6)$$

μ_x ve μ_y: x ve y görüntülerinin ortalama yoğunluk değerleri

σ_x^2: x'in varyansı

σ_y^2: y'nin varyansı

σ_{xy}, x ve y'nin kovaryansı

c_1 ve c_2 iki stabilize etme parametresi

L, piksel değerlerinin dinamik aralığı ($2^{\#\text{piksel başına düşen bit}}$ - 1)

$k_1 = 0{,}01$ ve $k_2 = 0{,}03$'tür.

2.3.4.4. Kapasite (Payload)

Stego-görüntüye gizlenebilen bitlerin toplam sayısını ifade eder. Veri gizlemede, bir örtü görüntüye, görüntünün kalitesini bozmadan maksimum kapasite ile veri gizlenmesi hedeflenir. Ancak, farklı kriterler, kapasiteden ödün verilmesine neden olabilmektedir.

2.4. Steganaliz

Steganaliz, steganografinin içerdiği gizli verileri açığa çıkarma sanatı ve bilimidir (Johnson ve Jajodia, 1998) denebilir. Stego-görüntüye gizlenen veriler, göz ile fark edilmese de steganalizde tespit saldırıları mümkündür. Steganografi ve steganaliz her zaman birbirlerine karşı önlem alır. İdeal bir steganografik yaklaşım tasarlandığında, bunun karşı önlem steganalizi de gömme süreçlerini analiz etmek veya alt etmek için geliştirilir (Wang ve Wang, 2004).

Genellikle, steganaliz yöntemleri iki ana kategoriye ayrılır: pasif steganaliz ve aktif steganaliz (Johnson ve Jajodia, 1998). Pasif steganaliz, gizli verilerin varlığını veya yokluğunu tanımlar veya hatta sadece belirli gömme sürecini açığa çıkarır. Aktif steganaliz ise, gizli verileri kurtarabilir, değiştirebilir veya sadece gizli verilerin uzunluğunu tahmin edebilir.

Literatürde hem istatistiksel hem de istatistiksel olmayan steganaliz yöntemleri mevcuttur. Bunlardan bazıları, belirli bir tür gömülü steganaliz teknikleri için tasarlanmıştır; diğerleri ise evrensel steganalizdir.

Stego-görüntüye saldırı yani steganaliz yapan kişiye Steganalist denir. Steganaliz yapılabilmesi için işlem öncesinde bilinmesi gereken veriler vardır. Sahip olduğu verilere göre bir Steganalist, saldırı modellerinden birini veya duruma göre birkaçını seçebilir.

- Sadece Stego Saldırısı: Steganalist tarafından, analiz için yalnızca stego-nesnesi bilinmektedir.
- Bilinen Örtü Saldırısı: Steganalist, örtü ve stego görüntüye sahiptir.
- Bilinen Mesaj Saldırısı: Örtü görüntüye saklanan mesaj Steganalist tarafından bilinmektedir.
- Seçilmiş Stego Saldırısı: Steganalist, veri gizlemede kullanılan algoritmaya ve stego nesnelerine sahiptir.
- Seçilmiş Mesaj Saldırısı: Steganografik araçlar, seçilen çeşitli mesajlara uygulanarak algoritma elde edilmeye çalışılır.
- Bilinen Stego Saldırısı: Örtü ve stego nesneleri bilinmektedir.

2.4.1. Piksel Farkları Dağılımı (PDH)

Pixel Difference Histogram (PDH), bir dijital görüntü üzerindeki pikseller arasındaki farkları ölçen ve görüntünün gizli bilgi taşıyıp taşımadığını belirlemek için kullanılan bir yöntemdir. PDH analizi, görüntüye eklenen gizli bilginin saptanmasında etkilidir ve yaygın olarak steganografi ve güvenlik uygulamalarında kullanılmaktadır.

PDH analizinde, öncelikle bir örtü görüntüye (cover image) ve gizli bilgi eklenmiş stego görüntüsü (stego image) oluşturmasına gerek vardır. Daha sonra, stego görüntüsünün PDH'si hesaplanır ve orijinal görüntünün PDH'si ile karşılaştırılır. Eğer stego görüntüsünün PDH'si, orijinal görüntüye göre farklı bir dağılım sergiliyorsa, görüntüde gizli bilgi taşıdığı düşünülür.

2.4.2. RS Analizi

RS analizi, dijital görüntüler üzerinde gizli bilgi taşıyan stego görüntülerinin tespitinde kullanılan bir analiz yöntemidir. Stego görüntüdeki Düzenli (R) ve Tekil (S) piksel gruplarının oranlarını ölçen bu yöntemde, orijinal görüntü ve stego görüntü pikselleri değerlerindeki küçük değişimler tespit edilerek arasındaki farklılıklar incelenmektedir.

RS Analizinde, tekil piksel gruplarının (Sm, S-m) normal piksel gruplarının (Rm, R-m) oranından büyük olması, görüntüde gizli veri gömülü olabileceğini göstermektedir. Tersi durumunda ise görüntünün normal olduğu düşünülür. Analiz grafiklerinde, Rm ile R-m ve/veya Sm ile S-m değerleri arasındaki fark arttığında görüntüde gizli veri olduğu anlaşılabilmektedir.

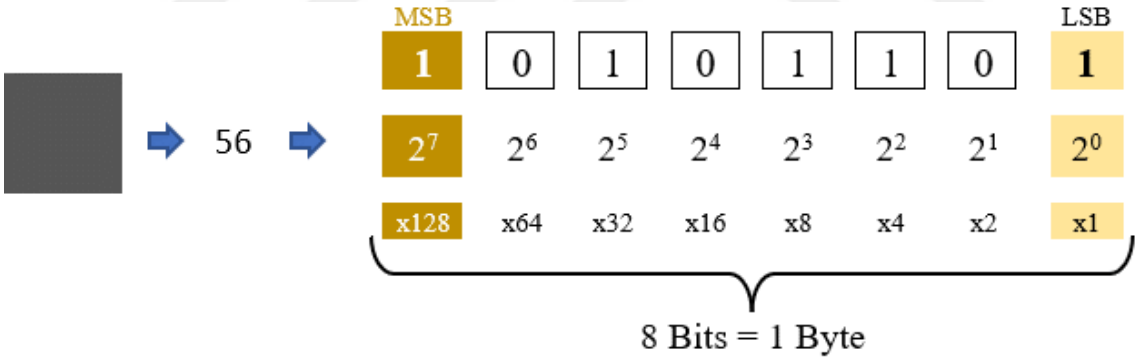
RS analizinde, orijinal görüntü ve stego görüntü arasındaki farkın küçük olduğu varsayılır. Bu nedenle, RS analizi, orijinal görüntüyü taklit etmeye çalışan stego yöntemlerine karşı daha etkili olabilmektedir. Ancak, bu yöntem stego yöntemlerinin tespitini tam olarak garanti etmez ve diğer steganaliz yöntemleriyle birlikte kullanılması önerilmektedir.

3. UZAMSAL DOMAİNDE YAYGIN KULLANILAN TEKNİKLER

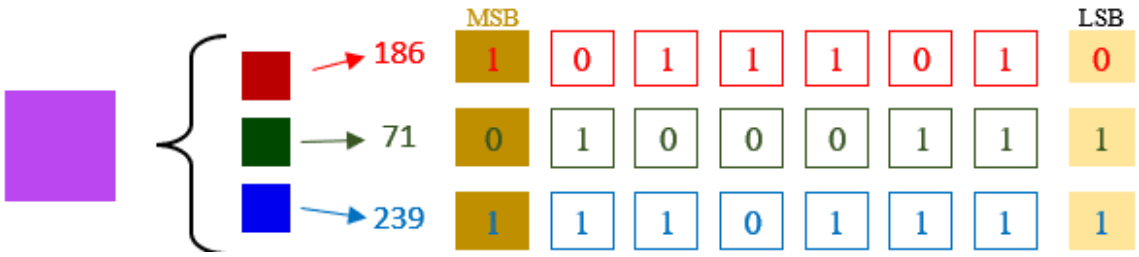
Uzamsal domain tekniklerinde gizli verilerin gömülmesi işlemi, doğrudan piksel değerlerinin işlenmesiyle yapılmaktadır. Bu, kolay ve hızlı uygulanmasını sağlar. Bu yüzden steganografi için en çok kullanılan alandır.

3.1. En Az Anlamlı Bit (LSB)

En az anlamlı bit yönteminde, örtü görüntüye ait onluk sistemdeki piksel değerleri ikili sisteme dönüştürülür. Şekil 3.1'de görüldüğü üzere, gri ölçekli bir görüntüde tek renk kanalı olduğundan görüntüdeki herhangi bir piksel 8 bitten oluşur. Bu 8 bitin bit bazında en yüksek değere sahip biti (2^7) En Anlamlı Bit (Most Significant Bit) olarak adlandırılırken, en düşük değere sahip biti (2^0) ise En Az Anlamlı Bit (Least Significant Bit) olarak adlandırılmaktadır. En az anlamlı bit yönteminde, işlemler genellikle 2^0,2^1,2^2 bitleri ile gerçekleştirilir. Böylece, Şekil 3.2'de de görülebileceği gibi, her bir renk için LSB üzerinde yapılacak bir birimlik bir değişim, o rengin değerini 255'te bir oranında değiştirecektir. Bu değişimin çıplak göz tarafından algılanması mümkün değildir.



Şekil 3.1. Sekiz bitlik veride LSB ve MSB



Şekil 3.2. Bir piksel RGB'de LSB ve MSB

Aşağıdaki bölümde LSB-k yöntemi k={1,2,3} için bir örnek ile açıklanmaktadır. “GEL” kelimesi, Şekil 3.3‘te görülen 256x256 ebatlarındaki, gri ölçekli House görüntüsüne gizlenmektedir.



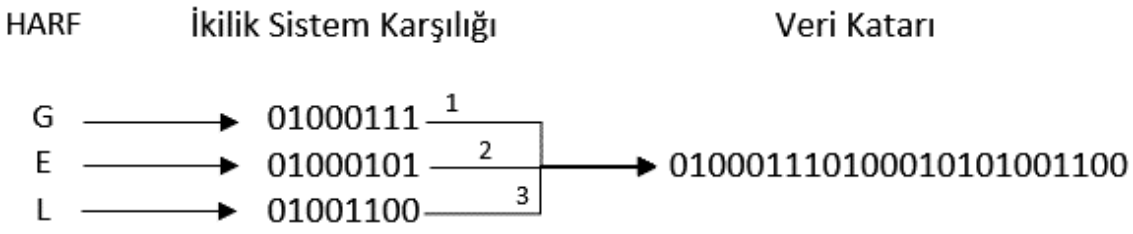
Şekil 3.3. 256x256 Gri House görüntüsü

Tablo 3.1’de detayları verilen işlemde öncelikle, gizli veri niteliği taşıyan kelimenin harflerinin ASCII değerleri bulunmaktadır. Bu değerlerin ikilik sayı sistemindeki karşılığı alınmaktadır. İkilik sayı sistemindeki bu üç adet sekiz veriden bir veri dizisi oluşturulmaktadır.

Tablo 3.1. "GEL" kelimesi için ASCII ve ikili taban değerleri

Karakterler	ASCII Karşılığı	İkili Taban
"G"	71	01000111
"E"	69	01000101
"L"	76	01001100

Şekil 3.4’te görüldüğü üzere bit veri katarı oluşturulurken bitler sırayla yan yana dizilmiştir ki bu, yönteme göre değişiklik gösterebilmektedir.



Şekil 3.4. Bit katarının oluşturulması

Veri gizlenecek olan gri House görüntüsüne ait piksellerin ASCII değerleri ikili sisteme dönüştürülüp uygulanacak LSB-k bit için gizlenecek k adet bit alınır ve pikselin LSB-k biti ile değiştirilir. LSB-1 yöntemi (k=1) için uygulanacak adımlar açık bir şekilde Tablo 3.2'de görülmektedir. LSB-2 uyglanırken ise pikselin en düşük anlamlı 2; LSB-3 uygulanırken de en düşük anlamlı 3 biti değiştirilmektedir.

Tablo 3.2. LSB-1 uygulaması

Örtü Görüntü	ASCII	Piksel Değeri	Gizlenecek (k=1) bit	Yeni Piksel Değeri
House 1. Piksel	102	0110011**0**	**0**	0110011**0**
House 2. Piksel	65	0100000**1**	**1**	0100000**1**
House 3. Piksel	93	0101110**1**	**0**	0101110**0**
House 4. Piksel	53	0011010**1**	**0**	0011010**0**
House 5. Piksel	72	0100100**0**	**0**	0100100**0**
House 6. Piksel	100	0110010**0**	**1**	0110010**1**
House 7. Piksel	101	0110010**1**	**1**	0110010**1**
House 8. Piksel	97	0110000**1**	**1**	0110000**1**

Tablo 3.3'te, Şekil 3.3'te yer alan gri House görüntüsünün piksellerine LSB-3 bite göre gizlenmiş olan veriyi çözme işlemini gerçekleştirilmiştir.

Tablo 3.3. LSB-3 bit için gizli veriyi elde etme işlemi

Stego Görüntü	ASCII	İkilik Sistem	Alınacak ilk 3 LSB	Elde Edilen bit Katarı
House 1. Piksel	98	01100**010**	**010**	**010**
House 2. Piksel	65	01000**001**	**001**	010 **001**
House 3. Piksel	94	01011**110**	**110**	010 001 **110**
House 4. Piksel	52	00110**100**	**100**	010 001 110 **100**
House 5. Piksel	74	01001**010**	**010**	010 001 110 100 **010**
House 6. Piksel	101	01100**101**	**101**	010 001 110 100 010 **101**
House 7. Piksel	97	01100**001**	**001**	010 001 110 100 010 101 **001**
House 8. Piksel	100	01100**100**	**100**	010 001 110 100 010 101 001 **100**

Çözme işlemi için, gizleme işleminde kullanılan piksel sırasının korunması gerekmektedir. Tablo 3.3'te, veri gizlenmiş olan stego görüntünün ilk 8 pikseli ve gizli veriyi elde etmek için bu piksellerin hangi bitlerinin alınacağı görülmektedir. Her bir pikselden alınan 3'er bit yan yana getirilerek Şekil 3.5'te görüldüğü gibi bir bit katarı oluşturulmaktadır. Elde edilen bit katarı 8'er bitlik parçalara bölünmektedir.

010 001 **110** 100 **010** 101 **001** 100 → **01000111 01000101 01001100**

Şekil 3.5. Çözülen verinin 8'lik bitlere dönüştürülmesi

Tablo 3.4'de elde edilen 8'er bitlik verilerin karşılıkları görülmektedir. Elde edilen karakterler, Tablo 3.1'den de görülebileceği üzere, gri Baboon görüntüsüne gizlenen karakterlerdir.

Tablo 3.4. Elde edilen bitlerin karakterlere dönüşümü

İkilik Sistem	ASCII Karşılığı	Karakterler
01000111	71	"G"
01000101	69	"E"
01001100	76	"L"

3.2. Piksel Değeri Farkı (PVD)

LSB-k bit yöntemi, uygulanmasının basit olması ve diğer yöntemlere entegre olma konusunda çok esnek olması nedeniyle sıkça başvurulan bir yöntemdir. Ancak, "k" değerindeki artışla doğru orantılı olarak gömme kapasitesi de artıyor olsa da bu artış, stego-görüntünün görsel kalitesindeki olumsuz bir etkiyi de beraberinde getirmektedir. Stego-görüntüde meydana gelen bu olumsuz etkiyi çözmek için Wu ve Tsai (Wu ve Tsai, 2003) piksel değeri farkı yöntemini önermişlerdir. Önerilen bu yöntem, belirli bir desene bağlı kalarak, örtü görüntüsünün ikişerli piksel gruplarına bölünmesine dayanmaktadır. Piksel gruplarındaki iki pikselin desimal değerleri arasındaki fark baz alınır. Bu fark ne kadar büyükse ki bu iki piksel arasındaki dokunun yüksek olması anlamına gelir, piksel çiftine o kadar fazla bit gömülebilmektedir. Tablo 3.5'te, pikseller arası fark/aralık ile aralığın izin verdiği gizlenebilecek bit sayısı verilmiştir.

Tablo 3.5. PVD referans tablosu

Referans	**Aralık (R_{alt})**	0	8	16	32	64	128
	Aralık ($R_{üst}$)	7	15	31	63	127	255
Genişlik (w)		8	8	16	32	64	123
Gizlenebilecek Bit Sayısı (t)		3	3	4	5	6	7

Yöntemi açıklamak için, Tablo 3.2'de bulunan House pikselleri alınarak ardışık olmak koşulu ile 2'li gruplara bölünmüş ve PVD ile örnek bir veri gizleme işlemi yapılmıştır.

1. Piksel Grubu : $P_1 = 102$, $P_2 = 65$

2. Piksel Grubu : $P_1 = 93$, $P_2 = 53$

…

İlk grup için :

$d=|P_1 - P_2|$

$d=|102-65|=37$

Bulunan d=37 değerinin Tablo 3.5'teki karşılığı 32 ile 63 arasında olduğundan bu iki piksel, 5 bitlik veri gizlenmesi için elverişlidir. Gizlenecek verinin 5 biti $(01000)_2$ onluk sisteme dönüştürülür ;

$(01000)_2 \Rightarrow Dec = (8)_{10}$

$d' = R_{Alt} + Dec = 32 + 8 = 40$

$m = |d'-d| = |40 - 37| = 3$

$$(P'_i, P'_{i+1}) = \begin{cases} \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i \geq P_{i+1}\ ve\ d_i > d'_i \\ \left(P_i - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), eğer\ P_i < P_{i+1}\ ve\ d_i > d'_i \\ \left(P_i - \left\lceil \frac{m}{2} \right\rceil, P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i \geq P_{i+1}\ ve\ d_i \leq d'_i \\ \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), eğer\ P_i < P_{i+1}\ ve\ d_i \leq d'_i \end{cases} \quad (3.1)$$

Elde edilen P_1, P_2 , m, d ve d' değerleri, Denklem (3.1) 'de verilen şartlara uygun olarak işleme tabi tutulur ve yeni piksel değerleri $P'_1 = 104$ ve $P'_2 = 64$ olarak elde edilir. Sıradaki piksel gruplarına da aynı işlemler uygulanarak stego-görüntü nesnesi elde edilir.

Gizlenmiş verinin elde etmesi için izlenecek yol, gizleme işlemine benzemektedir.

İlk iki piksele veri gizlendiğinde yeni piksel değerleri $P_1 = 104$ ve $P_2 = 64$ olmuştu.

$d=|P1 - P2|$

d=|104-64|=40

d=40 değeri, Tablo 3.5'te $32 \leq d \leq 63$ 'tür. İki piksel farkı, 5 bitlik verinin gizlendiğini göstermektedir.

$R_{Alt} = 32$ olur.

$d' = R_{Alt} + Dec$ idi. Benzer şekilde:

$Dec = |d - R_{Alt}|$ olur.

$Dec = |40-32| = 8$

$(8)_{10} = (01000)_2$ elde edilir. Gizlenen verinin ilk 5 biti elde edilmiş olur. Süreç sonraki piksel çiftleri için uygulanır ve bulunan bitler bir önceki ile birleştirilerek bit katarı elde edilir. İşlemler sonuçlanınca elde edilen bit katarı gizlenen veriyi içerir. LSB yönteminde olduğu gibi veri katarından gizlenen veri elde edilir.

3.3. Değişim Yönünü Kullanma (EMD)

EMD, iyi bilinen ve stego görüntülerinin görüntü kalitesini üst düzeyde koruyan bir gömme tekniğidir (Zhang ve Wang, 2006). Yöntem, kısaca, verinin gizleneceği örtü görüntüden seçilen "n" adet piksele, gizli verinin (2n+1)'lik sayı sistemine çevrilmiş değerlerin gizlenmesidir. Verinin ilgili piksellere gizlenmesi sonucunda, örtü-görüntüden alınan n adet pikselden sadece bir tanesinde ±1 miktarınca değişim olmakta (Solak, 2020) ya da hiçbir piksel değerinde değişim olmayabilmektedir. Kısacası, bu yöntemde, piksellerde değişim azdır. EMD'ye ait payload Denklem (3.2) ile hesaplanır;

$$P_{EMD} = \frac{\log(2n+1)}{n} \tag{3.2}$$

Tablo 3.6'da, n=2 için 1,16 ile en yüksek bpp değeri elde edildiği görülmektedir. Aynı zamanda, gizleme başına örtü-görüntüden alınan piksel miktarı artış gösterdikçe bpp değeri düşmektedir. Bu da, kapasitenin önemli olduğu durumlarda bu yöntem için n=2 seçilmesi gerektiğini göstermektedir.

Tablo 3.6. İşlem gören piksel sayısına göre bpp

n	bpp
2	1,16
3	0,94
4	0,79
5	0,69
6	0,62
7	0,56
8	0,51
9	0,47
10	0,44

EMD yöntemi bir örnek ile açıklanacak olursa ;

n=4 piksel için (2n+1) = 9 olur. Denklem (3.3) ile g_{EMD} hesaplanırsa;

$$g_{EMD}(P_1, P_2, \ldots, P_n) = [\sum_{k=1}^{n}(p_k \; x \; k)\;] mod\; (2\; x\; n + 1) \tag{3.3}$$

$g_{EMD}(P_1,P_2,P_3,P_4)=(102,65,93,53)$ mod 9

g_{EMD} (102,65,93,53) = (102x1+65x2+93x3+53x4) mod 9

g_{EMD} = 3

Gizlenecek veri “G” nin ASCII karşılığı 71’tir.

$(71)_{10}$ => $(SD)_9$= **7**8 => SD_1= **7** ve Denklem (3.4)’e göre diff değeri;

$$diff = (SD_i - g_{EMD}) mod\; (2\; x\; n + 1) \tag{3.4}$$

diff = (**7**-3) mod 9 = 4

Elde edilen diff değer, Denklem (3.5)’e göre değerlendirilir;

$$\begin{cases} p_1, p_2, \ldots p_n, \rightarrow\; diff\; =\; 0\; veya\; diff\; =\; g_{EMD} \\ p'_{diff} = p_{diff}\; +\; 1, \rightarrow\; diff\; \leq\; n \\ p'_{(2n+1-diff)} = p_{(2n+1-diff)}\; -\; 1, \rightarrow\; diff\; >n \end{cases} \tag{3.5}$$

diff ≤ n olduğu için $\mathbf{P'_4}$ = 53+1 = **54** olur. Bu süreç tüm n'li piksel grupları için tekrarlanarak stego-görüntü elde edilir. . n=4 piksel için işlem yapıldığında Tablo 3.7'de görüldüğü üzere gruptaki sadece bir pikselin ($\mathbf{P_4}$) değeri 1 artmış oldu. Görüntüdeki değişim az oldu ancak, kapasite düştü.

Tablo 3.7. n=4 için EMD piksellerindeki değişim

	$\mathbf{P_1}$	$\mathbf{P_2}$	$\mathbf{P_3}$	$\mathbf{P_4}$
Örtü Görüntü	102	65	93	**53**
Stego Görüntü	102	65	93	**54**

Gizlenen veriyi elde etmek için, gizlemede kullanılan n değerine göre işlem yapılır.

Gizleme işlemi, n=4 için yapılmıştı. Denklem (3.3)'te yeni piksel değerleri yerine konulduğunda:

$g_{EMD}(P_1,P_2,P_3,\mathbf{P_4})=(102,65,93,\mathbf{54}) \bmod 9$

$g_{EMD}\ (102,65,93,\mathbf{54}) = (102x1+65x2+93x3+\mathbf{54}x4) \bmod 9$

$g_{EMD} = \mathbf{7}$

Bulunan "**7**" değeri gizlenmiş olan ilk değerdir. Diğer değerleri bulmak için de aynı süreç işletilir ve gizli verinin tamamı elde edilir.

Örtü-görüntüden gömme işlemi için seçilen piksel sayısı artış gösterdikçe EMD yönteminin gömme yükü, büyük ölçüde düşmektedir. Kapasitede meydana gelen bu sorunun giderilmesi amacıyla EMD tabanlı farklı yöntemler geliştirilmiştir. Geliştirilen yöntemlerden birisi de GEMD'dir.

3.4. Genelleştirilmiş Değişim Yönünü Kullanma (GEMD)

Genelleştirilmiş değişim yönünü kullanma (GEMD) veri gizleme algoritması, 2013 yılında Kuo ve Wang tarafından önerilmiştir (Kuo ve Wang, 2013 c). EMD'ye kıyasla daha iyi bir stego görüntü kalitesi sağlayan GEMD geliştirilmiştir. GEMD'nin yükü Denklem (3.6) kullanarak hesaplanır;

$$P_{GEMD} = \frac{n+1}{n} \tag{3.6}$$

Tablo 3.8'de görüldüğü üzere EMD yöntemindeki "n" ile "bpp" arasındaki ilişkiye çok benzer bir durum burada da mevcuttur. Bu yöntemde de n=2 olduğunda en yüksek bpp değerine ulaşılmaktadır.

Tablo 3.8. İşlem gören piksel sayısına göre bpp

n	2	3	4	5	6	7	8	9	10
bpp	1,5	1,33	1,25	1,2	1,17	1,14	1,13	1,11	1,1

GEMD yöntemi bir örnek ile açıklanacak olursa;

n=3 piksel için (2^{n+1}) = 16 olur. Denklem (3.6)'ya göre g_{EMD} hesaplanırsa;

$$g_{EMD}(P_1, P_2, \dots, P_n) = [\sum_{k=1}^{n}(p_k\ x\ (2^k - 1))\ ] mod\ (2^{n+1}) \tag{3.7}$$

$g_{EMD}(P_1,P_2,P_3)=(53,72,100)$ mod 16

$g_{EMD}(102,65,93) = (53x1+72x3+100x7)$ mod 16

$g_{EMD} = 9$

Gizlenecek veriden n+1=4 bitlik parça alınır.

$(0100)_2$ => $SD_1 = (4)_{10}$ ve Denklem (3.8)'e göre diff hesaplanırsa;

$$diff = (SD_i - g_{EMD}) mod\ (2^{n+1}) \tag{3.8}$$

diff = (4-9) mod 16 = 11

Elde edilen diff değeri, Denklem (3.9)'a göre değerlendirilir;

```
if diff = 2^n → P'1 = P1 + 1, P'n = Pn + 1
if 0 < diff < 2^n → diff değeri (n+1) bite dönüştürülür.
Veriler, (sn, sn-1, … s0)2 formatında elde edilir.
for(x=n; x≥1; x=x+1)
    if (sx=0 ve sx-1,=1) => P'x = Px + 1
    elseif (sx=1 ve sx-1,=0) => P'x = Px – 1
    else P'x = Px
end
```
(3.9)

if diff > 2^n → temp = 2^{n+1} – diff, değeri (n+1) bite dönüştürülür.
Veriler, $(s_n, s_{n-1}, \ldots s_0)_2$ formatında elde edilir.
for(x=n; x≥1; x=x+1)
    if (s_x=0 ve s_{x-1},=1) => $P'_x = P_x - 1$
    elseif (s_x=1 ve s_{x-1},=0) => $P'_x = P_x + 1$
    else $P'_x = P_x$
end

diff > 2^n olduğundan temp = 2^{n+1} - diff = 1 olur. (3.9) yardımıyla (**P'_1 , P'_2 , P'_3**) = (52,73,99) bulunur. Bu süreç tüm n'li piksel grupları için tekrarlanarak stego-görüntü elde edilir. Tablo 3.9'da, yukarıdaki işleme ait piksel değişimleri gösterilmiştir.

Tablo 3.9. n=3 için GEMD piksellerindeki değişim

	P_1	**P_2**	**P_3**
Örtü Görüntü	53	72	100
Stego Görüntü	**52**	**73**	**99**

Gizlenen veriyi elde etmek için, gizlemede kullanılan n değerine göre işlem yapılır.

Gizleme işlemi, n=3 için yapılmıştı. Denklem (3.7)'de yeni piksel değerleri yerine konulursa :

$g_{EMD}(\mathbf{P_1},\mathbf{P_2},\mathbf{P_3})=(\mathbf{52,73,99})$ mod 16

$g_{EMD}(52,73,99) = (52x1+73x3+99x7)$ mod 16

$g_{EMD} = 4$

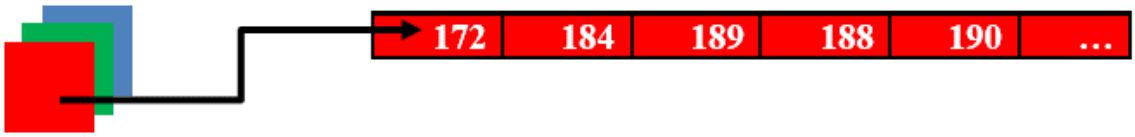
$SD_1 = (4)_{10}$ => $SD_1 = \mathbf{(0100)_2}$ olarak gizlenmiş veri bulunur.

3.5. PVD + LSB2 Hibrit Bir Yöntem

PVD ve LSB-k bit yöntemlerini içeren bir hibrit yöntemdir. Örtü görüntünün renk kanallarından belli bir kurala göre alınan piksel çiftlerine uygulanır. Piksel çiftindeki her bir piksel, kullanılacak LSB-k bite göre iki parçaya ayrılır. Burada belirleyici olan "k" parametresidir. Pikselin ikilik sistemdeki değeri, k=2 için pikselin LSB-2 biti ve geriye kalan 6 biti olmak üzere iki parçaya ayrılır. İki pikselden gelen altışar bitlik iki değere PVD yöntemi uygulanırken ayrılan k=2 bitlik kısımlara LSB-2 uygulanır. PVD'den elde

edilen yeni yeni piksel değerleri ile LSB-2 uygulanan değerler birleştirilerek yeni piksel değerleri oluşturulur. Bu bölümde, bu yöntem detaylı olarak anlatılmaktadır.

Şekil 3.6'da, örtü görüntünün R kanalı, piksel dizisine çevrilmektedir.



Şekil 3.6. Örtü görüntünün R kanalının piksel katarına dönüştürülmesi

R kanalının piksel değerlerini içeren diziye Hibrit (PVD+LSB2) uygulanacağı için Tablo 3.10'da R serisindeki tüm pikseller ikilik sisteme dönüştürülüp ikiye ayrılmaktadır.

Tablo 3.10. R kanalına ait bir pikselin iki parçaya ayrılması

Piksel Onluk	Piksel İkilik	1. Kısım	2. Kısım
172	$(10101100)_2$	$(\mathbf{10101100})_2$	$(10101\mathbf{00})_2$

Bit serisine dönüştürülmüş olan gizlenecek veri öncelikle, piksellerin Şekil 3.7'de ayrılmış olan 1. kısımlara PVD yöntemi ile gizlenir. Buradaki tüm piksellere gizleme işlemi yapıldıktan sonra geriye kalan gizlenecek veriler, pikselin 2. kısmına LSB-2 yöntemiyle gizlenmeye devam edilir. Böylece, Hibrit veri gizleme tamamlanmış olmaktadır.



Şekil 3.7. PVD yöntemi uygulanacak kısım

4. ÖNERİLEN YÖNTEM

Bu bölümde, renkli görüntüler içine, PVD, GEMD, Hibrit (PVD + LSB-2) ve LSB-1 yöntemlerinin kullanıldığı, örtü görüntünün kırmızı renk kanalının referans oluşturduğu ve diğer iki renk kanalına uygulanacak yöntemin her döngüde değişen bir tablodan alındığı, güvenliği ön planda tutan yeni bir yöntem önerilmiştir.

4.1. Veri Gizleme Yöntemlerinin Belirlenmesi

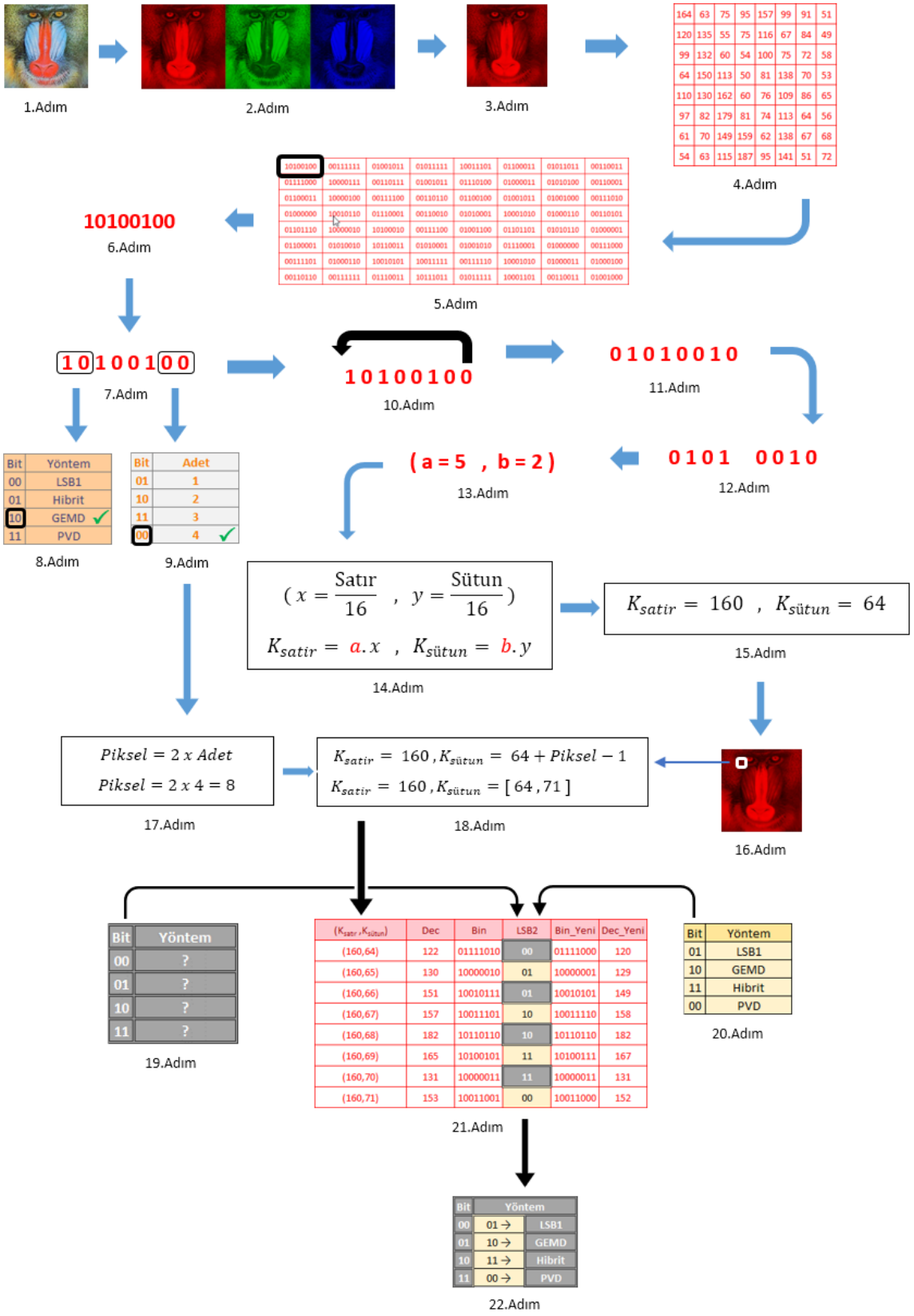
Bu bölümde örtü görüntünün R kanalı referans alınarak veri gizleme işleminde kullanılacak olan veri gizleme yöntemleri belirlenmektedir. R kanalının ilk piksel değeri ikilik sisteme dönüştürülmektedir. Elde edilen 8 bitlik değerin MSB 2 biti, R kanalına hangi yöntem ile veri gizleme işlemi yapılacağını göstermekte iken LSB 2 biti ise G ve B kanallarında veri gizleme işlemi yapılırken kaç adet yöntemin kullanılacağını göstermektedir. G ve B kanallarında kullanılacak yöntemlerin hangileri olduğu ve başlangıçta tabloda hangi sırada yer alacağını belirlemek için gerekli bilgi, yine R kanalındaki başlangıç konumu değişkenlik gösteren sıralı piksellere gizlenmektedir. Bu piksellerin başlangıç konumu, R kanalının ilk pikselinin 8 bitlik değerini ve görüntü boyutlarını içeren bir takım işlem ile belirlenmektedir. Bu nedenle bu piksellerin başlangıç konumu, farklı görüntünün kullanılması ve/veya görüntü ebatlarının değişmesine bağlı olarak değişmektedir.

RGB görüntünün R kanalında yapılan işlemler, G ve B kanallarına uygulanacak yöntemleri belirleyici olduğundan bu başlık altında ayrıca incelenmiştir. Süreç, detaylı olarak Şekil 4.1'te görülmekte ve adım adım anlatılmaktadır:

Adım 1 – Görüntünün Alınması : Sürecin açıklanmasında örnek görüntü olarak 512x512 Baboon resmi kullanılmaktadır.

Adım 2 – Görüntünün Renk Kanallarına Ayrılması : Baboon görüntüsü R-G-B renk kanallarına ayrılmaktadır.

Adım 3 – Yöntem Belirleyici Renk Kanalının Seçilmesi : Yöntemlerin belirlenmesinde görüntünün sadece R kanalı kullanılmaktadır.



Şekil 4.1. Veri gizleme yöntemlerinin belirlenmesi süreci

Adım 4 – R Kanalının Piksel Değerlerinin Belirlenmesi : R kanalına ait piksel değerleri desimal olarak alınmaktadır. (Örnek olarak 512x512 görüntünün 8x8'lik kısmı seçilmiştir.)

Adım 5 – İkilik Sisteme Geçiş : R Kanalının piksel değerleri ikilik sisteme dönüştürülmektedir.

Adım 6 – Referans Pikselin Seçilmesi : Uygulamamızda referans olarak R Kanalının ilk pikseli (R(1,1)) seçilmektedir.

Adım 7 – İlk Pikselin Ayrışması : İkilik sistemdeki bu piksel değerinin en düşük anlamlı 2 biti ile en yüksek anlamlı 2 biti dikkate alınmaktadır.

Adım 8 – MSB 2 Bitin Anlamı : Alınan en yüksek anlamlı 2 bit, "R Kanalı Yöntemleri" tablosundaki bit değerleri ile karşılaştırılır. (Bu tablo statik bir tablodur ve gizli veriyi çözecek tarafça bilinmektedir.) Örnekte MSB-2 değerimiz "10"dur. "10"un tablodaki karşılığı GEMD yöntemine denk gelmektedir. Bu, R kanalına veri gizlemek için GEMD yönteminin kullanılacağını göstermektedir.

Adım 9 – LSB 2 Bitin Anlamı : Alınan en düşük anlamlı 2 bit, G ve B Kanal çiftlerinde veri gizleme yapılırken kaç farklı yöntemin kullanılacağını ifade etmektedir. Bu 2 bit, kaç adet yöntem kullanılacaksa bunun "Yöntem-Adet" tablosundaki bit karşılığı ile değiştirilerek bu pikselin LSB 2 bitine işlenmektedir. (Bu tablo statik bir tablodur ve gizli veriyi çözecek tarafça bilinmektedir.) Örneğimizde 4 adet yöntem kullanmaktadır. 4 adet yöntemin tablodaki karşılığı "00" ve LSB 2 bit değerimiz de "00" olduğundan bu pikselin LSB 2 bitinde bir değişiklik yapılmamıştır.

Adım 10 – İlk Pikselde Bit Kaydırma : R Kanalının ilk pikselinin ikilik sistemdeki karşılığı "10100100", bit bazında sağ yöne doğru bir bit ötelenmektedir. Sondaki bit en sola yani başa geçmektedir.

Adım 11 – Yeni Piksel Değeri : Bit bazında öteleme yapılamasıyla yeni bir piksel değeri oluşmaktadır : "01010010".

Adım 12 – Yeni Pikselin İşlenmesi : Elde edilen yeni değer dörder bitlik iki parçaya ayrılmaktadır.

Adım 13 – Onluk Sisteme Geçiş : Dörder bitlik iki parçanın değerleri onluk sisteme dönüştürülmekte ve bu değerler “a” ve “b” katsayılarını oluşturmaktadır.

Adım 14 – Formüller : G ve B kanallarında kullanılacak olan 4 farklı yöntemin ve sıralarının belirlenmesi için karşı tarafa gönderilecek verilerin R kanalının hangi pikselinden itibaren gizleneceğini belirlemektedir. Görüntünün satır sayısı 16’ya bölünerek “x”, sütun sayısı 16’ya bölünerek “y” bulunmaktadır. “a” katsayısı “x” ile çarpılarak $K_{satır}$, “b” katsayısı “y” ile çarpılarak $K_{sütun}$ değerlerini oluşturmakta ve ($K_{satır}$, $K_{sütun}$) ikilisi, sıra-yöntem ikililerinin gizleneceği piksellerin başlangıç koordinatlarını belirtmektedir.

Adım 15 – Başlangıç Koordinatların Hesaplanması : ($K_{satır}$, $K_{sütun}$) ikilisi (a*x = 5*512/16 , b*y = 2*512/16) = (160 , 64) olarak hesaplanmaktadır.

Adım 16 – Örnek Gösterim : Baboon R Kanalı görüntüsü üzerinden temsili olarak (160 , 64) Pikseli gösterilmektedir.

Adım 17 – Gerekli Piksel Sayısının Hesaplanması : Sıra-Yöntem ikililerinin her bir eşlenmiş çifti için 4 bitlik veriye ihtiyaç vardır. Gizlemede standart olarak LSB-2 yöntemi kullanılacağından her bir çifti gizlemek için 2 adet piksel gerekmektedir. 4 adet sıra-yöntem çifti gizleneceğinden gizleme işlemi için 8 adet piksele ihtiyaç vardır.

Adım 18 – Piksellerin Belirlenmesi : R Kanalının (160 , 64) konumundan başlayarak 8 adet piksel belirlenmektedir. Uygulamamızda aynı satırda yer alan sıradaki pikseller kullanılmaktadır. (Bu durum gizli veriyi çözecek tarafça bilinmektedir.) Bu nedenle (160,64)…(160,71) pikselleri kullanılmaktadır.

Adım 19 – GB Yöntem Tablosu : G ve B kanallarındaki piksel çiftlerine uygulanacak yöntemleri içeren “GB Yöntem Tablosu” gösterilmektedir. (Yöntemler ve sıralamalar belli olmadığından bitlerin karşılıkları boştur.)

Adım 20 – Yöntemler Tablosu : Bit indeksleriyle birlikte kullanılabilecek yöntemlerin bulunduğu tablodur. (Bu tablo statik bir tablodur ve gizli veriyi çözecek tarafça bilinmektedir.)

Adım 21 – Yöntemlerin Gizlenmesi : R Kanalının (160 , 64) konumundan başlayarak (160 , 71) e kadar alınan 8 adet pikselin her birine LSB-2 yöntemi ile sıra-yöntem değerleri gizlenmektedir. “GB Yöntem Tablosu” ndaki “00” değerine karşılık gelecek yöntem belirlenmektedir ki örnekte bu yöntem “01” değeri ile LSB1’dir. Sonrasında, “01”e karşılık gelecek yöntem belirlenmektedir ki bu da “10” değeri ile GEMD’dir. 4 adet yöntem sıra ikilisi bu şekilde belirlenmekte ve R kanalındaki ilgili 8 piksele gizlenerek yeni piksel değerleri elde edilmektedir. Böylece çözüm işleminde kullanılmak üzere tablo karşı tarafa gönderilmektedir.

Adım 22 - GB Yöntem Tablosu : Sıra-yöntem değerleri gizlendikten sonra, G ve B kanallarında veri gizlemede kullanılacak olan tablonun son hali görülmektedir.

4.2. Veri Gizleme Süreci

Bu bölümde, son şeklini almış olan örtü görüntüye veri gizleme süreci anlatılmaktadır.

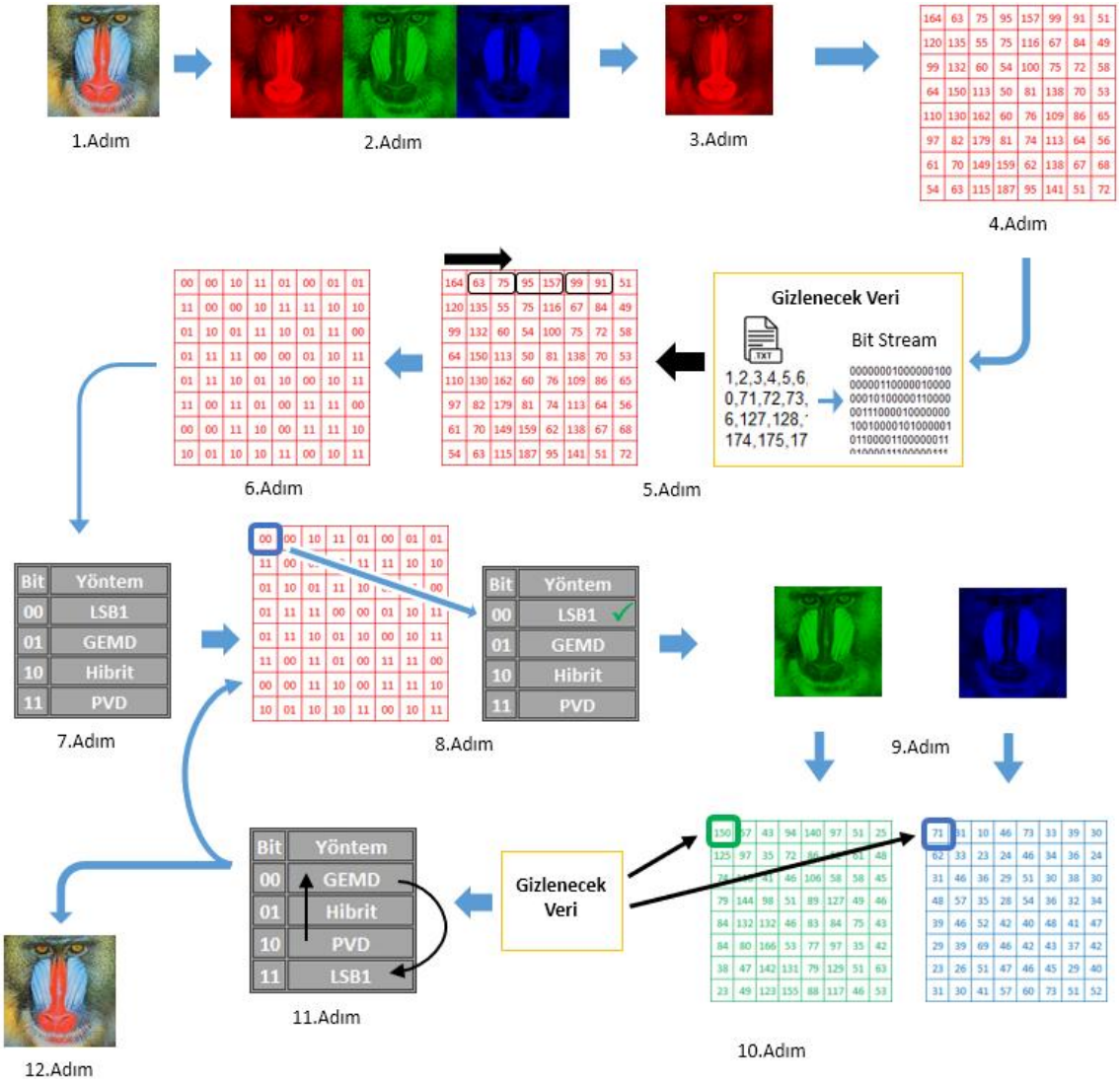
Örtü görüntünün R kanalının 1. pikseli önemli bilgiler içerdiğinden veri gizlemede kullanılmamaktadır. Ayrıca, yine R kanalının (Ksatır , Ksütun) koordinatlarından itibaren sıralı duruma göre 2,4,6 veya 8 piksel de tablo bilgileri içerdiğinden veri gizlemenin dışında bırakılmaktadır.

Örtü görüntünün R kanalının 1. pikselinde belirtilen yöntem ile R kanalına veri gizlenmektedir. G ve B kanallarından alınan aynı indeksli piksel çiftlerine ise R kanalı ve GB Yöntem Tablosunun eşleştirilmesi ile elde edilen yönteme göre veri gizlenmektedir. Ancak bu gizleme sırasında tablodaki eşleşmeler her döngüde değişmektedir. Süreç, Şekil 4.2’te detaylı olarak gösterilmekte ve adım adım anlatılmaktadır:

Adım 1 – Görüntünün Alınması : Sürecin açıklanmasında örnek görüntü olarak 512x512 Baboon resmi kullanılmaktadır.

Adım 2 – Görüntünün Renk Kanallarına Ayrılması : Baboon görüntüsü R-G-B renk kanallarına ayrılmaktadır.

Adım 3 – Yöntem Belirleyici Renk Kanalının Seçilmesi : Yöntemlerin belirlenmesinde görüntünün sadece R kanalı kullanılmaktadır.



Şekil 4.2. Veri gizleme süreci

Adım 4 – R Kanalının Piksel Değerlerinin Belirlenmesi : R kanalına ait piksel değerleri desimal olarak alınmaktadır. (Örnek olarak 512x512 görüntünün 8x8'lik kısmı seçilmiştir.)

Adım 5 – R Kanalına Verinin Gizlenmesi : Veri gizlemeye, R Kanalının ikinci pikselinden başlanmaktadır. Bu pikselden itibaren R kanalı için belirlenen yöntem olan GEMD ile gizlenecek veriler R kanalındaki piksel çiftlerine gizlenmektedir. (Sıra-yöntem ikililerini içeren 8 piksel de bu gizlemenin dışında tutulmaktadır.)

Adım 6 – Karşılaştırma Verilerinin Oluşturulması : R Kanalına veri gizlendikten sonra piksel değerleri ikilik sisteme dönüştürülür ve her pikselin LSB-2 biti alınır.

Adım 7 - GB Yöntem Tablosu : G ve B kanallarında veri gizlemede kullanılacak olan tablo görülmektedir.

Adım 8 – Yöntemin Belirlenmesi : Birinci pikselden başlayarak R kanalındaki ilgili pikselin LSB-2 değeri GB Yöntem Tablosundaki bitler ile eşleştirilir. Örnekte LSB-2 değeri olarak "00", tablodaki LSB1 ile eşleşmektedir.

Adım 9 – G ve B Kanallarına Geçiş : Baboon görüntüsünün G ve B kanalları gösterilmektedir.

Adım 10 – G-B Kanalı Piksel Çiftlerine Veri Gizleme : G ve B kanallarından sıradaki birer piksel alınarak (ilk durum için birinci pikseller) LSB1 yöntemi ile bu iki piksele veri gizlenir. (LSB1 yönteminde piksel çifti gerekmediği için gizleme işlemi önce G, sonra B kanalına uygulanmaktadır.)

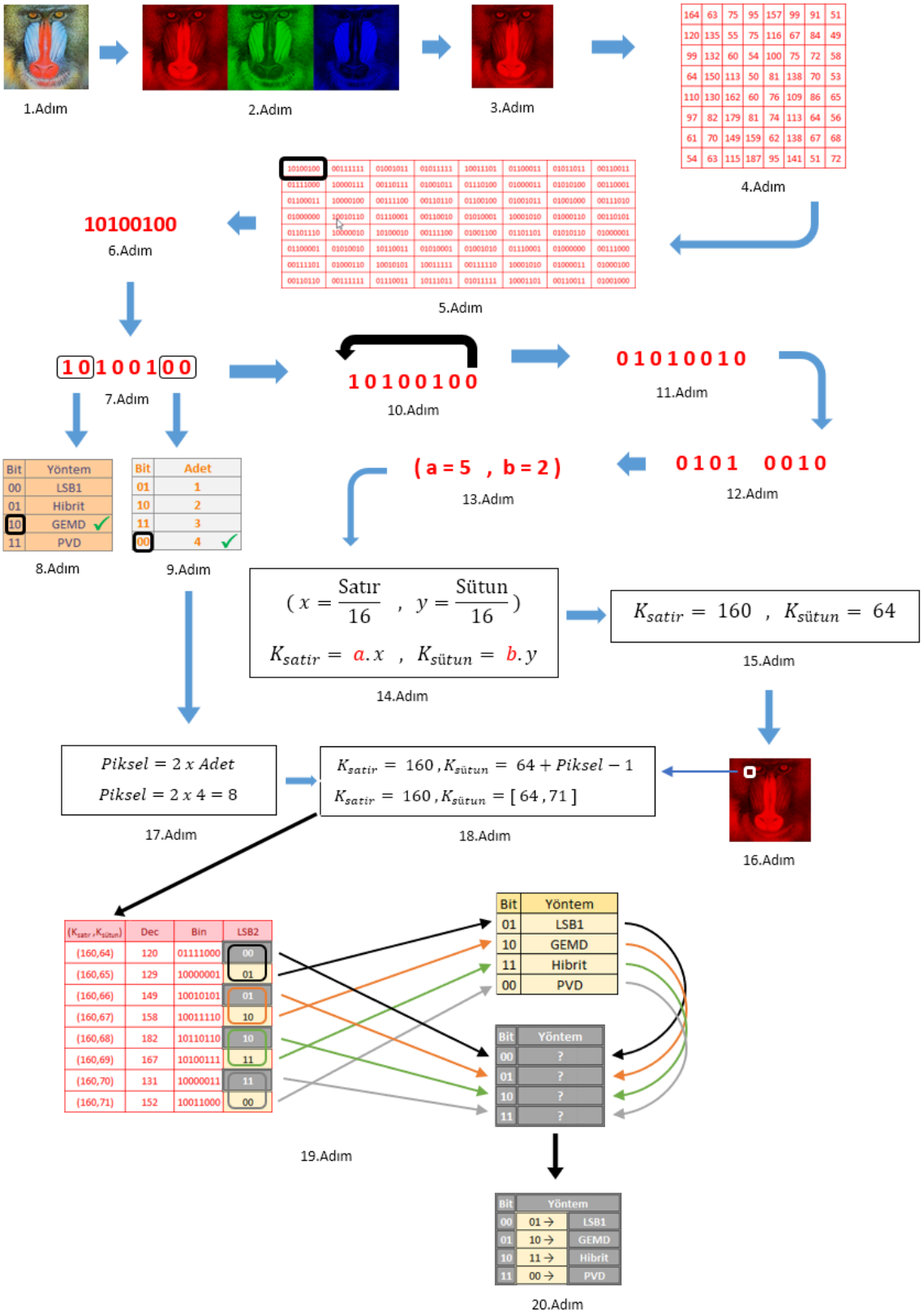
Adım 11 - GB Yöntem Tablosundaki Sıralamanın Değişmesi : GB Yöntem Tablosundaki bit sırası sabit kalmak koşuluyla, yöntemler birer sıra yukarı yönde yer değiştirmektedir. En üstteki yöntem ise en alt sıraya geçmektedir. Böylece tablodaki sıra-yöntem eşleşmesi değişmiş olmaktadır. Veri gizlenecek piksel çifti mevcutsa sekizinci adıma dönülmektedir. Sıradaki LSB-2 değeri ("00"), yeni GB Yöntem Tablosu ile kıyaslanarak bir sonraki G-B piksel çiftine hangi yöntem ("00" → "GEMD") ile veri gizleneceğine karar verilmektedir.

Adım 12 - Stego Görüntü Elde Edilmesi : 11.Adımdan sonra veri gizlenecek piksel çifti kalmadığında Stego görüntü oluşmuş olmakta ve işlem sonlanmaktadır.

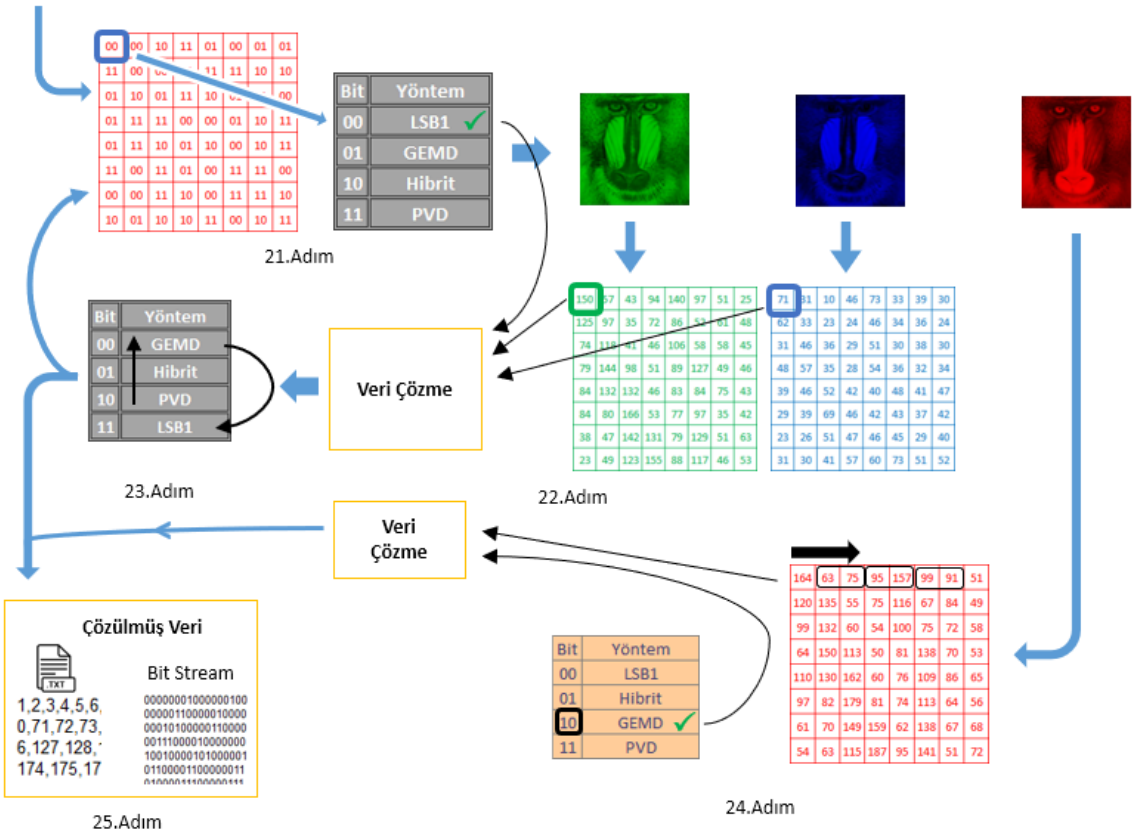
4.3. Gizlenmiş Verinin Geri Elde Edilmesi

Bu bölümde, elde edilen stego görüntüden gizlenmiş verinin çıkarılma işlemi anlatılmaktadır. R kanalının ilk pikselinden, R kanalında veri gizlemek için hangi yöntem kullanıldığı, G-B kanallarında gizleme için kaç yöntem kullanıldığı ve bu yöntemlerin listesini içeren bilginin hangi pikselden itibaren gizlendiği bilgileri elde edilmektedir. Elde edilen bilgilere göre G-B ve R kanallarından veri çıkarma işlemi yapılmaktadır.

Stego görüntüyü alacak olan tarafta "R Kanalı Yöntemleri", "Yöntemler Tablosu" ve sıra-yöntem piksellerini hangi sırada seçildiği bilgisi mevcuttur. Çıkarma işlemi detaylı olarak Şekil 4.3'te görülmektedir.



Şekil 4.3. Gizli veriyi elde etme süreci



Şekil 4.3. (Devam) Gizli veriyi elde etme süreci

Adım 1 – Görüntünün Alınması : Sürecin açıklanmasında örnek görüntü olarak 512x512 Baboon resmi kullanılmaktadır.

Adım 2 – Görüntünün Renk Kanallarına Ayrılması : Baboon görüntüsü R-G-B renk kanallarına ayrılmaktadır.

Adım 3 – Yöntem Belirleyici Renk Kanalının Seçilmesi : Yöntemlerin belirlenmesinde görüntünün sadece R kanalı kullanılmaktadır.

Adım 4 – R Kanalının Piksel Değerlerinin Belirlenmesi : R kanalına ait piksel değerleri desimal olarak alınmaktadır. (Örnek olarak 512x512 görüntünün 8x8'lik kısmı seçilmiştir.)

Adım 5 – İkilik Sisteme Geçiş : R Kanalının piksel değerleri ikilik sisteme dönüştürülmektedir.

Adım 6 – Referans Pikselin Seçilmesi : Uygulamamızda R Kanalının ilk pikselinin referans olduğu bilinmektedir.

Adım 7 – İlk pikselin ayrışması : İkilik sistemdeki bu piksel değerinin en düşük anlamlı 2 biti ile en yüksek anlamlı 2 biti dikkate alınmaktadır.

Adım 8 – R Kanalına Uygulanan Yöntemin Belirlenmesi : Alınan en yüksek anlamlı 2 bit, "R Kanalı Yöntemleri" tablosundaki bit değerleri ile karşılaştırılır. Örnekte MSB-2 değerimiz "10"dur. "10"un tablodaki karşılığı GEMD yöntemine denk gelmektedir. Bu, R kanalına veri gizlemek için GEMD yönteminin kullanıldığını göstermektedir.

Adım 9 – G ve B Kanalları için Kullanılan Yöntem Sayısının Belirlenmesi : Alınan en düşük anlamlı 2 bit, G ve B Kanal çiftlerinde veri gizleme yapılırken kaç farklı yöntemin kullanıldığını göstermektedir. Bu 2 bit ile "Yöntem-Adet" tablosundaki bitler karşılaştırılarak kullanılan yöntem adedi bulunmaktadır. Örneğimizde LSB 2 bit "00" olduğundan ve bunun tablodaki karşılığı 4 olduğundan 4 adet yöntem kullanıldığı anlaşılmaktadır.

Adım 10 – İlk Pikselde Bit Kaydırma : R Kanalının ilk pikselinin ikilik sistemdeki karşılığı "10100100", bit bazında sağ yöne doğru bir bit ötelenmektedir. Sondaki bit en sola yani başa geçmektedir.

Adım 11 – Yeni Piksel Değeri : Biz bazında öteleme yapılamasıyla yeni bir piksel değeri oluşmaktadır : "01010010".

Adım 12 – Yeni Pikselin İşlenmesi : Elde edilen yeni değer dörder bitlik iki parçaya ayrılmaktadır.

Adım 13 – Onluk Sisteme Geçiş : Dörder bitlik iki parçanın değerleri onluk sisteme dönüştürülmekte ve bu değerler "a" ve "b" katsayılarını oluşturmaktadır.

Adım 14 – Formüller : G ve B kanallarında kullanılan 4 farklı yöntemin ve sıralarının belirlenmesi ve GB Yöntem Tablosunun ilk halinin oluşturulmasında kullanılmaktadır. Bu verilerin R kanalının hangi pikselinden itibaren gizlendiğini belirtmektedir. Görüntünün satır sayısı 16'ya bölünerek "x", sütun sayısı 16'ya bölünerek "y" bulunmaktadır. "a" katsayısı "x" ile çarpılarak Ksatır , "b" katsayısı "y" ile çarpılarak

Ksütun değerlerini oluşturmakta ve (Ksatır , Ksütun) ikilisi, sıra-yöntem ikililerinin gizlendiği piksellerin başlangıç koordinatlarını belirtmektedir.

Adım 15 – Başlangıç Koordinatların Hesaplanması : (Ksatır , Ksütun) ikilisi (a*x = 5*512/16 , b*y = 2*512/16) = (160 , 64) olarak hesaplanmaktadır.

Adım 16 – Örnek Gösterim : Baboon R Kanalı görüntüsü üzerinden temsili olarak (160 , 64) Pikseli gösterilmektedir.

Adım 17 – Gerekli Piksel Sayısının Hesaplanması : Sıra-Yöntem ikililerinin her bir eşlenmiş çifti için 4 bitlik veriye ihtiyaç vardır. Gizlemede standart olarak LSB-2 yöntemi kullanılacağından her bir çifti gizlemek için 2 adet piksel gerekmektedir. 4 adet sıra-yöntem çifti gizlendiğinden gizleme işlemi için 8 adet piksele ihtiyaç duyulmuştur.

Adım 18 – Piksellerin Belirlenmesi : R Kanalının (160 , 64) konumundan başlayarak 8 adet piksel belirlenmektedir. Uygulamamızda aynı satırda yer alan sıradaki pikseller kullanılmaktadır. Bu nedenle (160,64)…(160,71) pikselleri kullanıldığı sonucuna varılmaktadır.

Adım 19 – Yöntemlerin Çözülmesi : R Kanalının (160 , 64) konumundan başlayarak (160 , 71) e kadar seçilen 8 adet pikselin her birinin LSB 2 bit değerleri çiftler halinde alınmaktadır. Bu 4 bitlik çiftten ilk 2 bit, “GB Yöntem Tablosu” (Gri Tablo) ndaki “bit” değerini; ikinci 2 bit ise “Yöntemler Tablosu” (Sarı Tablo) nda karşılık geldiği yöntemi belirtmektedir. Örnekte, (160,64) ve (160,65) koordinatlarındaki pikseller bir çift oluşturmaktadır. Bunların LSB 2 bitleri sırasıyla “00” ve “01”dir. İlk 2 bit (“00”) “GB Yöntem Tablosu” ndaki sırasına, ikinci bit (“01”) ise “Yöntemler Tablosu” nda “LSB1” e denk gelmektedir. Bu durumda, “GB Yöntem Tablosu” nda “00” bitin karşılığı “LSB1”dir. Bu şekilde tüm piksel çiftleri incelenerek “GB Yöntem Tablosu” oluşturulmaktadır.

Adım 20 - GB Yöntem Tablosu : Tablonun ilk durum değerleri oluştuğundan, G ve B kanallarında veri gizlemede kullanmış olan tablonun son hali görülmektedir.

Adım 21 – G ve B Kanallarında Çözüme Başlama : R kanalının Piksel değerlerinin LSB 2 biti GB Yöntem Tablosu ile karşılaştırılarak G ve B kanallarındaki sıradaki piksel çiftine

hangi yöntem uygulandığı belirlenmektedir. Örnekte, ilk piksel çifti için LSB1 uygulandığı görülmektedir.

Adım 22 – G ve B Kanallarında Verinin Elde Edilmesi : Stego görüntüden G ve B kanalları alınarak GB Yöntem Tablosundan elde edilen yöntem (LSB1) ile veri çözme işlemi yapılmaktadır.

Adım 23 – GB Yöntem Tablosundaki Sıralamanın Değişmesi : GB Yöntem Tablosundaki bit sırası sabit kalmak koşuluyla, yöntemler birer sıra yukarı yönde yer değiştirmektedir. En üstteki yöntem ise en alt sıraya geçmektedir. Böylece tablodaki sıra-yöntem eşleşmesi değişmiş olmaktadır. Çözülecek veri piksel çifti mevcutsa yirmi birinci adıma dönülmektedir. Sıradaki LSB-2 değeri (“00”), yeni GB Yöntem Tablosu ile kıyaslanarak bir sonraki G-B piksel çiftinden hangi yöntem (“00” → “GEMD”) ile veri çıkarılacağına karar verilmektedir.

Adım 24 – R Kanalından Verinin Elde Edilmesi : R Kanalının 2. Pikselinden başlayarak 8. Adımda elde edilen yöntem (“GEMD”) ile veriler çıkartılmaktadır. İşlem sırasında (Ksatır , Ksütun) ve sonrasında gelen sıra-yöntem belirleyici pikseller de işlem dışında tutulmaktadır.

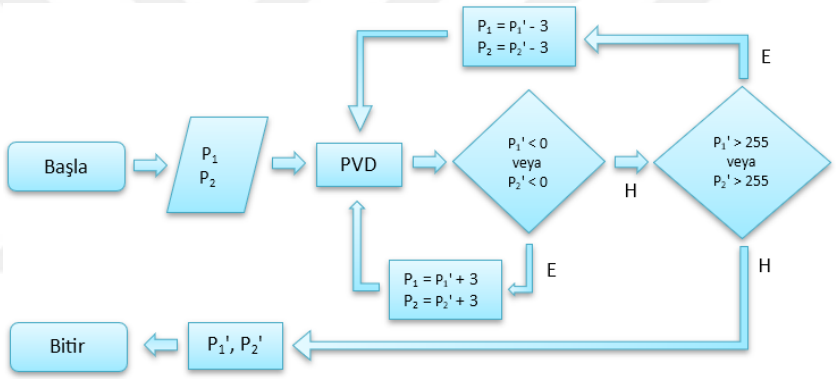
Adım 25 – Gizli Verinin Elde Edilmesi : İstisna pikseller hariç tüm pikseller işlem gördükten sonra R ve G-B kanallarından elde edilen veriler birleştirilerek oluşturulan bit katarından gizli veri elde edilmektedir.

4.4. Taşma Sorunu (Fall Off Baundary Problem)

Uygulamada kullanılan GEMD ve PVD yöntemleri, piksellere veri gizlenmesi için piksel değerlerinin arttırılması veya azaltılması ile sonuçlanan süreçlerdir. Her iki yöntem de işlem gören pikselin değerinin arttırılması ile yeni piksel değeri 255’i aşmakta; değerinin azaltılması ile de 0’dan düşük bir değer elde edilebilmektedir. Bu durum, verinin gizlenmesinde ve tekrar elde edilmesinde sorun teşkil etmektedir. Uygulamada bu sorunu aşmak için farklı yöntemler geliştirilmiştir.

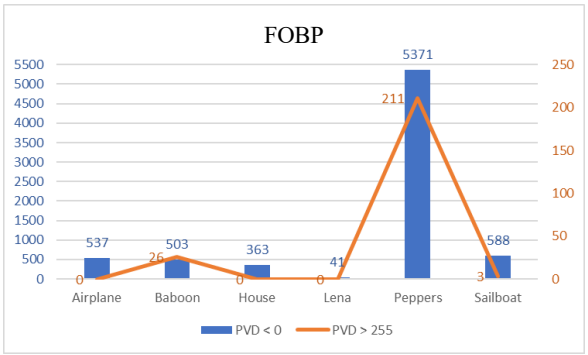
4.4.1. PVD için FOBP Sorununun Giderilmesi

Uygulama kullanılan PVD yöntemine ait FOBP sorununun giderilmesinde kullanılan yönteme ait akış diyagramı Şekil 4.4'te verilmiştir. Veri gizlenecek piksel çiftine PVD yöntemi uygulanmaktadır. Elde edilen yeni piksel değerlerinden herhangi biri 0'dan küçükse yeni piksel değerlerine 3 eklenmekte ve tekrar PVD işlemine gönderilmektedir. Yeni elde edilen piksel çiftinden herhangi biri 0'dan küçükse döngü devam etmektedir. Aksi taktirde, piksellerin 255'ten büyük olup olmadığı kontrol edilmektedir. Yeni piksel değerlerinden herhangi biri 255'ten büyükse, yeni piksel değerlerinden 3 eksiltilmekte ve tekrar PVD yöntemi uygulanmaktadır. Yeni elde edilen piksel değerleri tekrar 255 ile karşılaştırılmakta ve duruma göre döngü devam etmekte ya da sonuç olarak PVD yöntemi uygulanmış yeni piksel değerleri elde edilmektedir.



Şekil 4.4. PVD için FOBP çözümü akış diyagramı

Uygulamamızda kullanılan görüntülerde bu sorunla ne sıklıkla karşılaşıldığı Şekil 4.5'te verilmiştir. Şekil incelendiğinde, PVD yönteminde FOBP sorunu ile en az Lena ve House görüntülerinde; en çok ise Peppers görüntüsünde karşılaşıldığı görülmektedir.



Şekil 4.5. PVD için Görüntü-FOBP yoğunluk grafiği

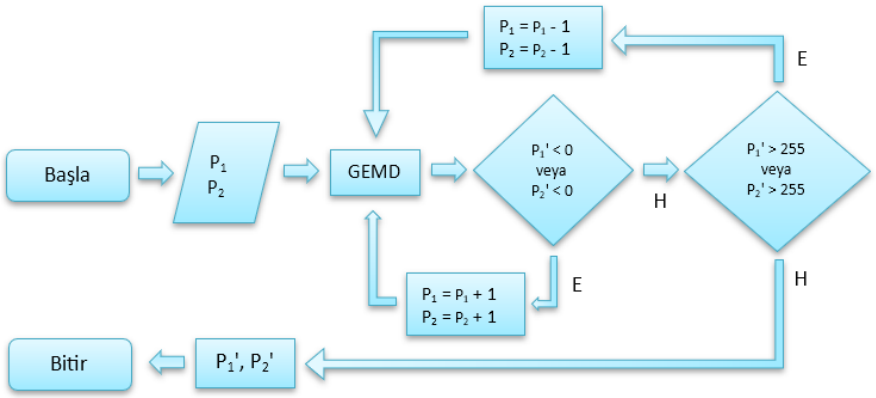
FOBP Sorunu ile ilgili sayısal detaylar Tablo 4.1'de verilmiştir.

Tablo 4.1. PVD için görüntü bazında FOBP miktarları

Görüntü	PVD < 0	PVD > 255
Airplane	537	0
Baboon	503	26
House	363	0
Lena	41	0
Peppers	5371	211
Sailboat	588	3

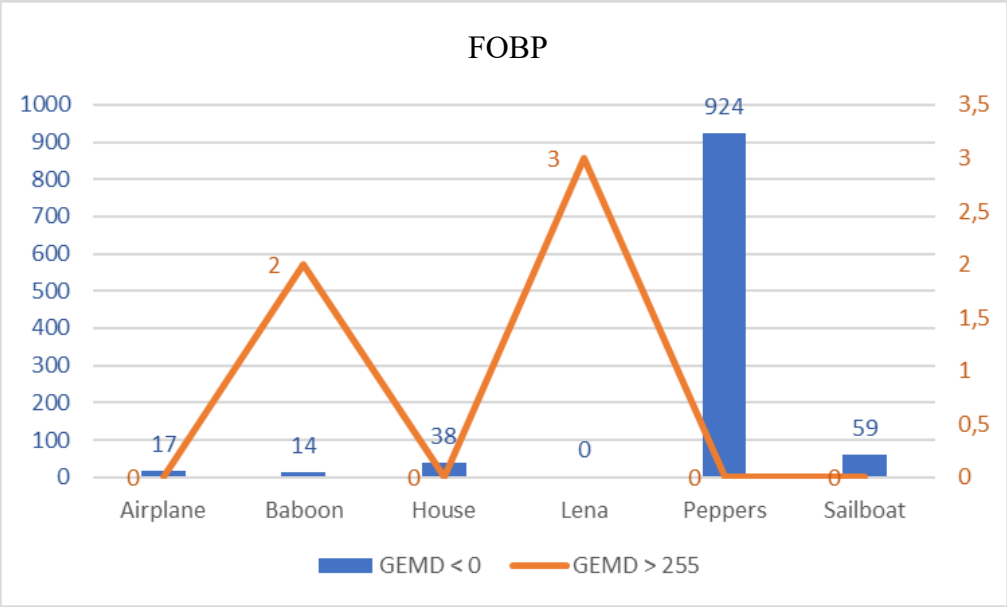
4.4.2. GEMD için FOBP Sorununun Giderilmesi

Uygulama kullanılan GEMD yöntemine ait FOBP sorununun giderilmesinde kullanılan yönteme ait akış diyagramı Şekil 4.6'da verilmiştir. Veri gizlenecek piksel çiftine GEMD yöntemi uygulanmaktadır. Elde edilen yeni piksel değerlerinden herhangi biri 0'dan küçükse GEMD uygulanmadan önceki piksel değerlerine 1 eklenmekte ve tekrar GEMD işlemine gönderilmektedir. Yeni elde edilen piksel çiftinden herhangi biri 0'dan küçükse döngü devam etmektedir. Aksi taktirde, piksellerin 255'ten büyük olup olmadığı kontrol edilmektedir. Yeni piksel değerlerinden herhangi biri 255'ten büyükse, GEMD uygulanmadan önceki piksel değerlerinden 1 eksiltilmekte ve tekrar GEMD yöntemi uygulanmaktadır. Yeni elde edilen piksel değerleri tekrar 255 ile karşılaştırılmakta ve duruma göre döngü devam etmekte ya da sonuç olarak GEMD yöntemi uygulanmış yeni piksel değerleri elde edilmektedir.



Şekil 4.6. GEMD için FOBP çözümü akış diyagramı

Uygulamamızda kullanılan görüntülerde bu sorunla ne sıklıkla karşılaşıldığı Şekil 4.7'de verilmiştir. Şekil incelendiğinde, PVD yönteminde FOBP sorunu ile en az Airplane, Baboon ve Lena görüntülerinde; en çok ise Peppers görüntüsünde karşılaşıldığı görülmektedir.



Şekil 4.7. GEMD için Görüntü-FOBP yoğunluk grafiği

FOBP Sorunu ile ilgili sayısal detaylar Tablo 4.2'de sunulmuştur.

Tablo 4.2. GEMD için görüntü bazında FOBP miktarları

Görüntü	PVD < 0	PVD > 255	GEMD < 0	GEMD > 255
Airplane	537	0	17	0
Baboon	503	26	14	2
House	363	0	38	0
Lena	41	0	0	3
Peppers	5371	211	924	0
Sailboat	588	3	59	0

4.5. Önerilen Yöntem ile örnek veri gizlenmesi ve verinin elde edilmesi

Önerilen yöntem ile veri gizleme ve elde etme işlemi için Şekil 5.1'deki Baboon görüntüsü kullanılacaktır.

4.5.1. Veri Gizlenmesi

Önerilen yöntem için R kanalının 1. pikseli referans oluşturmaktadır. Baboon örtü görüntüsünün R kanalına ait ilk pikselinin değeri 164'tür. 164'ün ikilik sistemdeki karşılığı (**10**1001**00**)$_2$'dır. İkilik sistemdeki bu sayının MSB 2 biti, R kanalına uygulanacak yöntemi; LSB 2 biti ise yöntem adedini belirlemektedir. Bu durumda, "R Kanalı Yöntemleri" tablosunda "10"un karşılığı GEMD yöntemidir ki bu bağlayıcıdır. Ancak, "00" a karşılık gelen 4 yöntem bağlayıcı değildir. Yöntem sayısı ayarlanabilir olduğundan "00" istenen değer ile değiştirilebilir. Örneğin "11" yapılarak 3 yöntem kullanılabilir. Bu örnekte yöntem sayısı değiştirilmeyip 4 olarak belirlenmiştir.

Yöntem sayısına karar verildikten sonra yapılması gereken işlem, bu yöntemlerin neler olduğu, nasıl sıralandığı ve bu bilgilerin R kanalındaki hangi piksellere gizleneceğinin belirlenmesidir. $(10100100)_2$ sayısı sağ yönde bir basamak kaydırılarak $(01010010)_2$ sayısı elde edilir. Bu sayı 4'er bitlik 2 parçaya bölünür ve onluk sisteme çevrilir. MSB 4 bitten $(0101)_2 = 5$; LSB 4 bitten $(0010)_2 = 2$ elde edilir. Verinin gizleneceği piksellerin başlangıç koordinatlarını bulmak için örtü görüntünün ebatları 16'ya bölünür ve bir önceki adımda elde edilen sayılar ile çarpılır. X = 5x512/16 ve Y = 2x512/16'dan (X,Y)=(160,64) elde edilir. Yöntemlerin ve sıralarının gizlenmesi işleminde LSB-2 yöntemi uygulanacağı için 4 adet yöntemin her birinin tablodaki sırası için 2 bite, yöntem indeksini belirtmek için yine 2 bite ihtiyaç vardır. Bu durumda, her bir yöntemin gizlenmesi için 4 bit gerekmektedir ki LSB-2 ile bu bilgi 2 piksele gizlenebilir. 4 yöntem için 8 piksele ihtiyaç vardır. (X,Y)=(160,64) koordinatlarından başlayarak Y artacak şekilde 8 sıralı piksel seçilir. "GB Yöntem Tablosu" için ilk sıra indeksi "00" a "01" indeksli LSB1; "01" e "10" indeksli GEMD; "10" a "11" indeksli Hibrit ve "11" e "00" indeksli PVD yöntemini temsil eden "0001011010111100" bit katarı oluşur. Bu bit katarı, 8 piksele LSB-2 yöntemi ile gizlenir.

P(122,130,151,157,182,165,131,153)=>[LSB-2]=>P'(120,129,149,158,182,167,131,152) elde edilir.

R kanalına 2. Pikselden başlamak ve yukarıdaki 8 pikseli işleminde dışında tutmak kaydıyla GEMD yöntemi ile veriler gizlenir.

G-B kanalındaki piksel çiftlerine uygulanacak olan yöntemi R kanalındaki aynı koordinata sahip pikselin LSB 2 biti belirlemektedir.

G-B kanalına gizlenecek veri = “00111001100011000…”

GB Yöntem Tablosundaki ilk sıralama “00” : LSB-1, “01” : GEMD, “10” : Hibrit ve “11” : PVD şeklindedir.

$R_1=164=(101001\mathbf{\underline{00}})_2$ olduğundan “00” a denk gelen yöntem LSB-1’dir.

$G_1=150$ ve $B_1=71$ piksellerine ayrı ayrı LSB-1 ile “0” ve “0” gizlenirse $G'_1=150$ ve $B'_1=70$ olmaktadır.

GB Yöntem Tablosundaki yöntemlerin sıralaması birer kaydırılır ve yeni sıralama “00” : GEMD, “01” : Hibrit, “10” : PVD ve “11” : LSB-1 olur.

$R_2=63=(001111\mathbf{\underline{11}})_2$ olduğundan “11” a denk gelen yöntem LSB-1’dir.

$G_2=57$ ve $B_2=31$ piksellerine ayrı ayrı LSB-1 ile “1” ve “1” gizlenirse $G'_2=57$ ve $B'_2=31$ olmaktadır.

GB Yöntem Tablosundaki yöntemlerin sıralaması birer kaydırılır ve yeni sıralama “00” : Hibrit, “01” : PVD, “10” : LSB-1 ve “11” : GEMD olur.

$R_3=76=(010011\mathbf{\underline{00}})_2$ olduğundan “00” a denk gelen yöntem Hibrit’tir.

$G_3=43$ ve $B_3=10$ piksellerine ayrı ayrı Hibrit yöntem ile “100110” gizlendiğinde $G'_3=53$ ve $B'_3=3$ olmaktadır.

…

Pikseller sona erene kadar bu döngü devam etmekte ve veriler gizlenmektedir.

4.5.2. Verilerin Elde Edilmesi

Verilerin elde edilebilmesi için öncelikle stego görüntünün R kanalının ilk pikseline bakılmaktadır. Veri gizlemede izlenen yöntem burada da geçerli olduğundan R kanalına GEMD ile veri gizlendiği ve 4 yöntem kullanıldığı belirlenebilmektedir çünkü R

kanalının ilk pikseline herhangi bir veri gizleme işlemi yapılmadığından değeri sabit kalmaktadır. Pikselin ikilik tabandaki değerine basamak kaydırma işlemi yapıldığında ise yöntem sırasının gizlendiği başlangıç pikseli (160,64) olarak bulunmaktadır. Buradaki 8 piksel değerinin LSB 2 bitine bakılarak yöntem sıralaması oluşturulmaktadır.

P(120,129,149,158,182,167,131,152)=>[LSB 2]=>(00,01,01,10,10,11,11,00)

Elde edilen LSB 2 bitler ikişerli gruplara ayrılırsa tablo sıralaması elde edilmektedir :

(**00**,01) (**01**,10) (**10**,11) (**11**,00)

Gruplardaki ikinci bitlerin karşılığı "Yöntemler Tablosu"ndan bakılıp hangi yöntemlere karşılık geldiği belirlenmektedir.

(**00**, LSB-1) (**01**, GEMD) (**10**, Hibrit) (**11**, PVD)

G-B kanalı için kullanılacak "GB Yöntem Tablosu" belirlenmiş olur.

G(150,57,53,…) ve B(70,31,3,…) pikselleri G_1B_1(150,70), G_2B_2(57,31), G_3B_3(53,3) vb. gruplanarak R kanalındaki aynı indisli R_x in LSB 2 bitine karşılık gelen yöntem ile çözme işlemi uygulanır. Her piksel grubuna ilgili yöntem uygulandıktan sonra "GB Yöntem Tablosu", veri gizlemede uygulanan kaydırma işlemine tabi tutulur. İstisnai pikseller hariç tüm pikseller için döngü gerçekleştirilerek gizli veri elde edilir.

5. DENEYSEL ÇALIŞMALAR

Çalışmamız PVD, GEMD ve Hibrit (PVD+LSB-2) gibi birçok yöntemi içerdiğinden şifreleme-çözme kontrollerinin hatasız yapılabilmesi için 1'den 300.000'e kadar sayıların küçükten büyüğe doğru sıralı olarak yazıldığı ve her sayının birbirinden virgüllerle ayrıldığı bir metin dosyası oluşturulup gizli mesaj olarak kullanılmıştır. Veriler, kütüphanedeki 512x512 boyutundaki renkli örtü görüntülere gizlenmiştir. Tüm işlemler, Matlab R2020a yazılımı ile Windows 11 Professional 64-bit işletim sistemi kurulu, Intel Core i7-10750H işlemci ve 16 GB 2933Mhz RAM'e sahip bir dizüstü bilgisayar kullanılarak gerçekleştirilmiştir.

Uzamsal Domainde Kullanılan Yöntemleri incelemek için örtü görüntü olarak Şekil 5.1'de görülen 512x512 boyutlarındaki, SIPI görüntü veri tabanlarında (USC, 2022) yer alan renkli Airplane, Baboon, House, Lena, Peppers ve Sailboat görüntüleri kullanılmıştır. Uygulamamızda, gizlenecek veri olarak içerisinde 1'den 300.000'e kadar virgüllerle ayrılmış sayıların bulunduğu bir metin dosyası kullanılmıştır.



(a) Airplane (b) Baboon (c) House

(d) Lena (e) Peppers (f) Sailboat

Şekil 5.1. Örtü-görüntü olarak kullanılan görüntüler

5.1. Uzamsal Domainde Kullanılan Yöntemlerin Deneysel Sonuçları

İlk olarak LSB-k bit uygulamasında k değerinin artışıyla doğru orantılı olarak görüntüdeki görsel bozulma incelenmiştir. Şekil 5.2, farklı k değerleri için LSB uygulanmış örtü görüntüleri içermektedir. k değerinin artışı her ne kadar gizlenebilecek veri miktarının artmasını sağlasa da belli bir aşamadan sonra görüntüde gözle görülür bozulmaya sebep olmaktadır. Bu durum Şekil 5.2'de açık bir şekilde gözlemlenebilmektedir.



(a) k=1 (b) k=2 (c) k=3 (d) k=5

Şekil 5.2. LSB-k için artan "k" değerinin görüntüye etkisi

Örtü görüntü olarak kullanılan renkli altı farklı görüntüye LSB-k (k={1,2,3}), EMD, GEMD ve PVD yöntemleri ayrı ayrı uygulanmıştır. Uygulama sonucunda elde edilen Kapasite, Yük, PSNR ve SSIM verileri Tablo 5.1'de ayrıntılı olarak görülmektedir.

Tablo 5.1. Çalışma sonucu elde edilen veriler

Görüntü	Yöntem	SSIM (%)	PSNR (dB)	Kapasite	Yük (bpp)
Airplane	LSB1	99,6755	51,1346	786.432	1,0000
	LSB2	98,4582	43,0164	1.572.864	2,0000
	LSB3	94,9662	36,4366	2.359.296	3,0000
	GEMD	99,5847	50,1404	1.179.536	1,4999
	EMD	99,7285	52,1205	783.752	0,9966
	PVD	98,0702	40,9318	1.228.977	1,5627
Baboon	LSB1	99,9688	51,1371	786.432	1,0000
	LSB2	99,8441	43,0351	1.572.864	2,0000
	LSB3	99,4260	36,4209	2.359.296	3,0000
	GEMD	99,9609	50,1734	1.179.536	1,4999
	EMD	99,9746	52,1162	783.752	0,9966
	PVD	99,3990	37,0630	1.405.795	1,7876

Tablo 5.1. (Devam) Çalışma sonucu elde edilen veriler

Görüntü	Yöntem	SSIM (%)	PSNR (dB)	Kapasite	Yük (bpp)
House	LSB1	99,9011	51,1572	786.432	1,0000
	LSB2	99,5411	43,0582	1.572.864	2,0000
	LSB3	98,3976	36,4373	2.359.296	3,0000
	GEMD	99,8756	50,1753	1.179.536	1,4999
	EMD	99,9183	52,1017	783.752	0,9966
	PVD	99,3689	40,1234	1.263.038	1,6060
Lena	LSB1	99,9793	51,1310	786.432	1,0000
	LSB2	99,8979	43,0268	1.572.864	2,0000
	LSB3	99,6311	36,4020	2.359.296	3,0000
	GEMD	99,9740	50,1654	1.179.536	1,4999
	EMD	99,9832	52,1268	783.752	0,9966
	PVD	99,8330	41,6905	1.234.394	1,5696
Peppers	LSB1	99,9783	51,1660	786.432	1,0000
	LSB2	99,8895	43,1642	1.572.864	2,0000
	LSB3	99,5798	36,5659	2.359.296	3,0000
	GEMD	99,9723	50,1534	1.179.536	1,4999
	EMD	99,9779	51,8858	783.752	0,9966
	PVD	99,8699	42,5910	1.202.867	1,5295
Sailboat	LSB1	99,9386	51,1505	786.432	1,0000
	LSB2	99,6891	43,0470	1.572.864	2,0000
	LSB3	98,8677	36,4200	2.359.296	3,0000
	GEMD	99,9228	50,1852	1.179.536	1,4999
	EMD	99,9495	52,1003	783.752	0,9966
	PVD	99,5147	39,6694	1.289.359	1,6395

LSB-k bit yönteminin farklı “k” değerleri için daha kolay kıyaslama yapılabilmesi için LSB yöntemine ait olan veriler Tablo 5.2’de bir araya getirilmiştir.

Tablo 5.2. Dört farklı görüntüde LSB 1-2-3 bit uygulama sonuçları

Görüntü	Yöntem	SSIM (%)	PSNR (dB)	Kapasite	Yük (bpp)
Airplane	LSB1	99,6755	51,1346	786.432	1,0000
	LSB2	98,4582	43,0164	1.572.864	2,0000
	LSB3	94,9662	36,4366	2.359.296	3,0000
Baboon	LSB1	99,9688	51,1371	786.432	1,0000
	LSB2	99,8441	43,0351	1.572.864	2,0000
	LSB3	99,4260	36,4209	2.359.296	3,0000

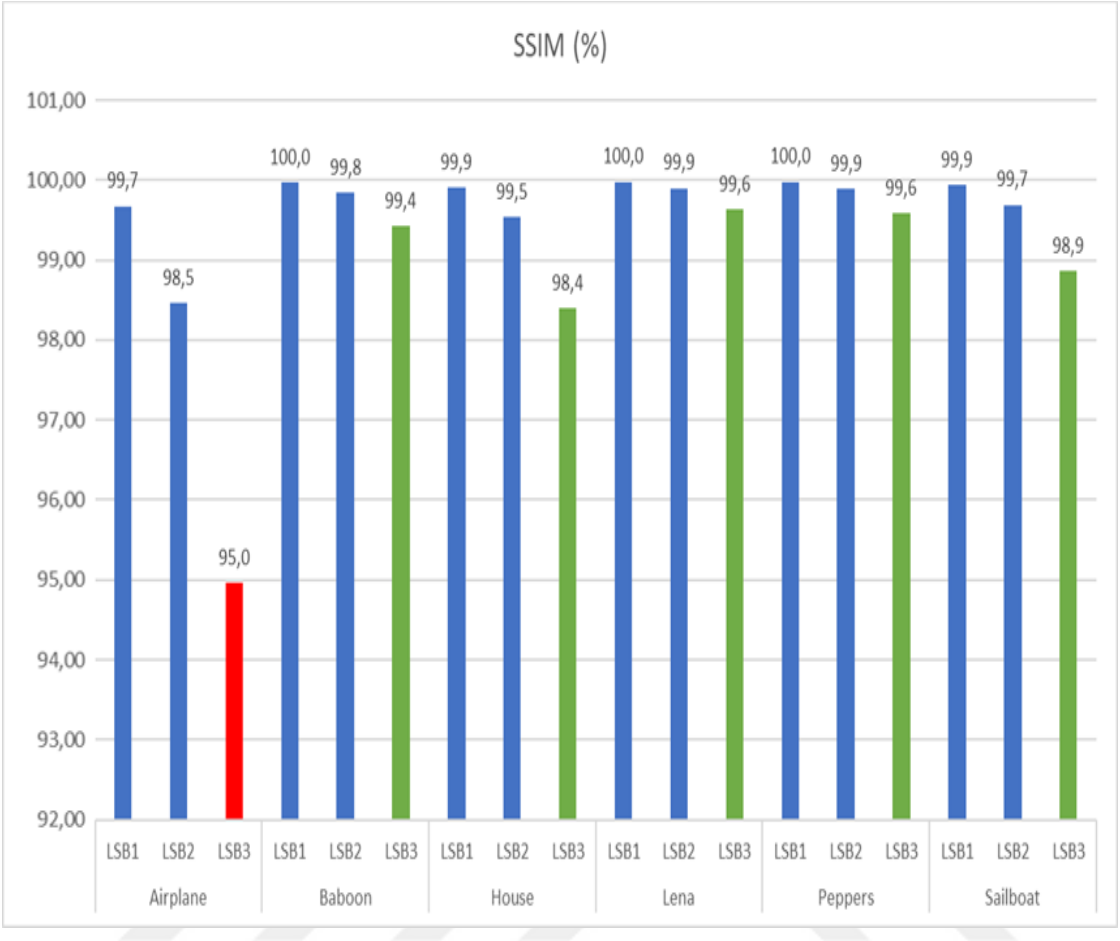
Tablo 5.2. (Devam) Dört farklı görüntüde LSB 1-2-3 bit uygulama sonuçları

Görüntü	Yöntem	SSIM (%)	PSNR (dB)	Kapasite	Yük (bpp)
House	LSB1	99,9011	51,1572	786.432	1,0000
	LSB2	99,5411	43,0582	1.572.864	2,0000
	LSB3	98,3976	36,4373	2.359.296	3,0000
Lena	LSB1	99,9793	51,1310	786.432	1,0000
	LSB2	99,8979	43,0268	1.572.864	2,0000
	LSB3	99,6311	36,4020	2.359.296	3,0000
Peppers	LSB1	99,9783	51,1660	786.432	1,0000
	LSB2	99,8895	43,1642	1.572.864	2,0000
	LSB3	99,5798	36,5659	2.359.296	3,0000
Sailboat	LSB1	99,9386	51,1505	786.432	1,0000
	LSB2	99,6891	43,0470	1.572.864	2,0000
	LSB3	98,8677	36,4200	2.359.296	3,0000

Farklı örtü görüntülerine uygulanan LSB-k bit için kapasite değerleri aynıdır. Fakat k değeri arttıkça kapasite yükselmektedir. LSB-1 bit ile renkli görüntüde renk kanalı başına 1 bit veri gizlenirken (1bpp), LSB-3 bit ile 3 bit (3bpp) veri gizlenebilmekte ve bu da doğrudan kapasiteyi etkilemektedir.

LSB-k yönteminde "k"nın artmasıyla birlikte bpp artışı, görüntü kalitesindeki (PSNR) azalmayı da beraberinde getirmektedir. Diğer görüntülerin de LSB-k bit için PSNR değerlerine Tablo 5.2'den bakıldığında, bu durumun kullanılan örtü görüntüsünden bağımsız olduğu ve sonucun değişmediği görülmektedir. Kısacası, LSB-1 bit ile minimum kapasite, maksimum görüntü kalitesi elde edilirken; LSB-3 bit ile maksimum kapasite, minimum görüntü kalitesi elde edilmektedir.

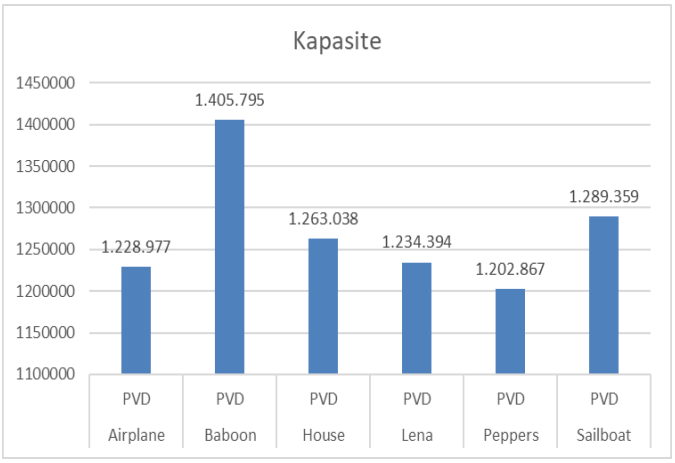
Şekil 5.3'te de görüldüğü üzere örtü görüntülerine LSB-k bit yöntemiyle veri gizlenmesiyle elde edilen stego görüntüler ile aralarındaki yapısal benzerlik oranı (SSIM), k arttıkça azalmaktadır. Bunun sebebi, piksel başına değiştirilen bit sayısının artmasıdır. Farklı örtü görüntüleri için kullanılan aynı LSB yöntemine ait SSIM değerleri Tablo 5.2'de de görüldüğü gibi birbirine çok yakın olsa da Şekil 5.3'te LSB-3 uygulanan Airplane görüntüsündeki yapısal benzerlik oranı diğerlerine göre düşük kalmaktadır. Uygulanan yöntemin görüntüde oluşturacağı etkinin resmin yapısına bağlı olduğu görülmektedir.



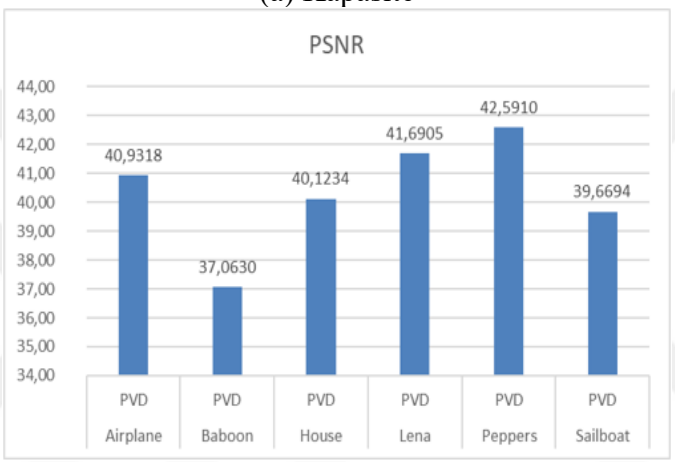
Şekil 5.3. Altı örtü görüntünün için LSB-k bit SSIM değerleri (%)

Diğer bir yöntem olan PVD'de ise gizleme kapasitesi, sıralı iki piksel arasındaki farkın büyüklüğüne bağlı olduğundan, diğer görüntülere kıyasla doku yüksekliğinin en sık rastlandığı Baboon görüntüsü, Şekil 5.4'te görüldüğü üzere en yüksek kapasiteyi sunmuştur. Her bir örtü görüntüye ait piksel başına veri gizleme kapasitesinin yer aldığı Tablo 5.1'den de 1,7876 ile en yüksek bpp değerine Baboon görüntüsünün sahip olduğu görülmektedir. Şekil 5.4 (a) ve (b) birlikte incelenecek olursa, PVD yöntemindeki kapasite artışının görüntü kalitesine etkisi açık bir şekilde görülebilmektedir. Her ne kadar Baboon görüntüsünün kalitesi en düşük olsa da alt sınır kabul edebileceğimiz 30dB'nin üzerindedir.

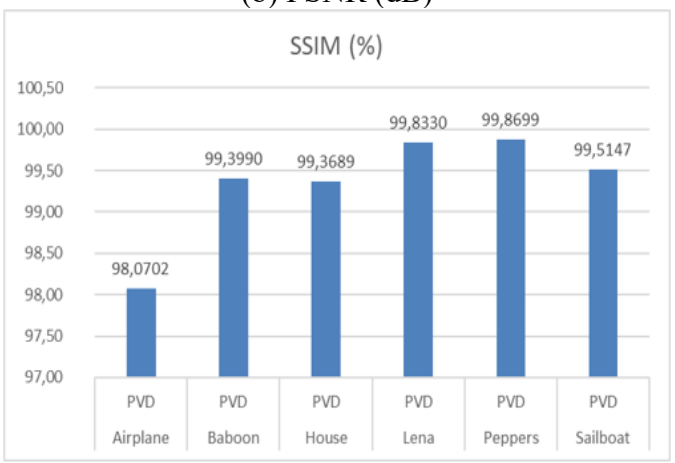
Görüntü kalitesindeki azalmaya rağmen Baboon görüntüsü, Şekil 5.4 (c)'de görüldüğü üzere yapısal benzerlik indeksi (SSIM) olarak yüksek bir değere sahiptir.



(a) Kapasite



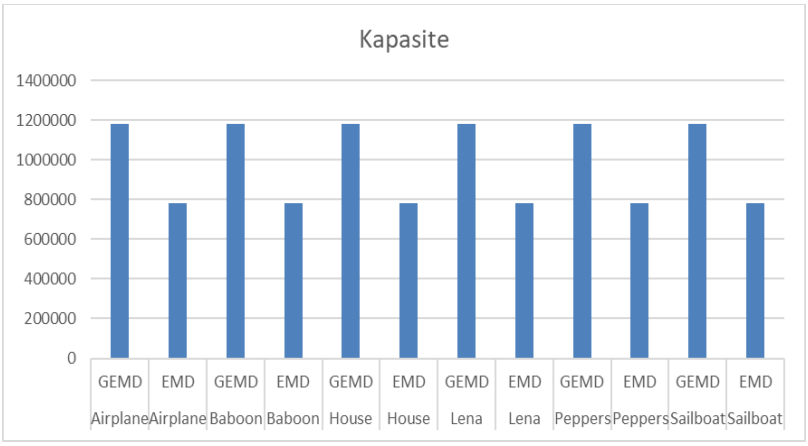
(b) PSNR (dB)



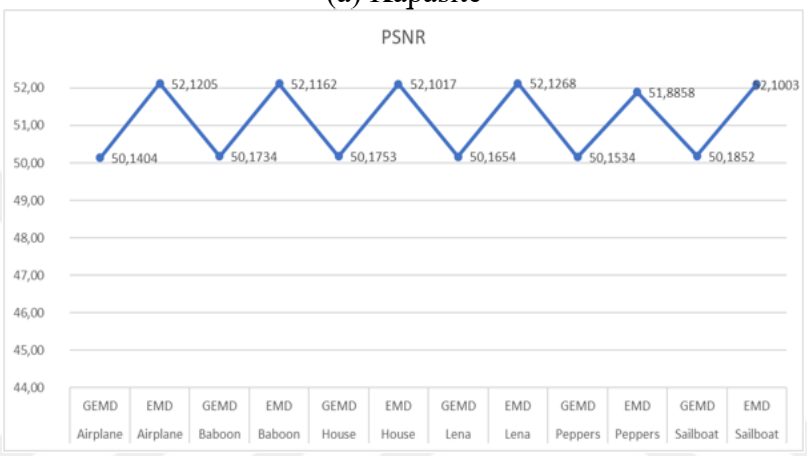
(c) SSIM (%)

Şekil 5.4. PVD Yöntemi için Kapasite, PSNR ve SSIM karşılaştırması

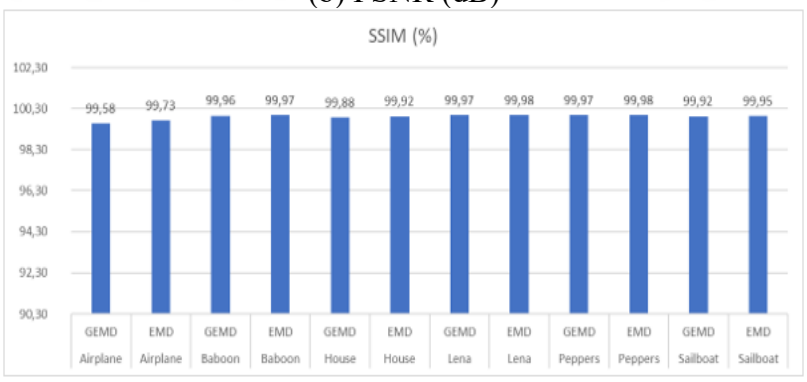
Şekil 5.5 (a) ve (b) incelendiğinde, GEMD yöntemi ile elde edilen stego görüntünün EMD yöntemiyle edilen stego görüntüye göre görüntü kalitesinin nispeten daha düşük ancak veri gizleme kapasitesinin çok daha yüksek olduğu görülmektedir. SSIM değerleri olarak EMD daha yüksek olsa da (c)'de görüldüğü üzere arada büyük bir fark bulunmamaktadır.



(a) Kapasite



(b) PSNR (dB)

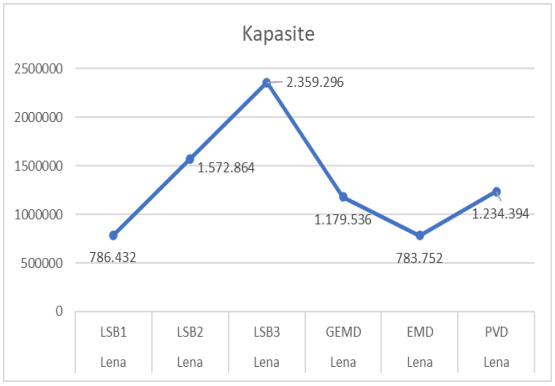


(c) SSIM (%)

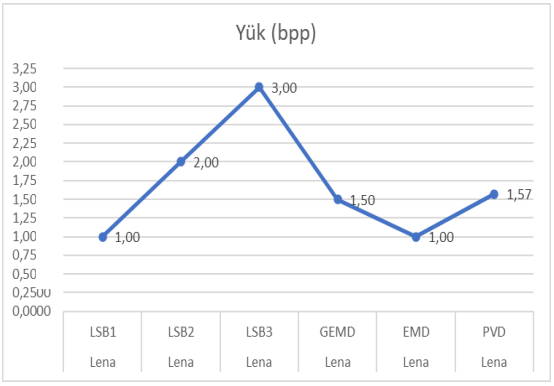
Şekil 5.5. EMD-GEMD için Kapasite, PSNR ve SSIM karşılaştırması

LSB 1-2-3 bit, PVD, EMD ve GEMD yöntemlerinin Lena örtü görüntüsüne uygulanmasıyla elde edilen PSNR, SSIM, bpp ve Kapasite değerlerinin kıyaslanması Şekil 5.6'da görülmektedir. En yüksek görsel kalite ve yapısal benzerlik endeksini LSB-1 bit ve EMD sunmaktayken bu yöntemler kapasite açısından listenin en altında kalmaktadırlar. Buna rağmen EMD yöntemi, steganaliz ataklarına karşı dayanıklı bir yöntemdir ve diğer yöntemlere göre daha iyi bir görsel kalite sunabilmektedir.

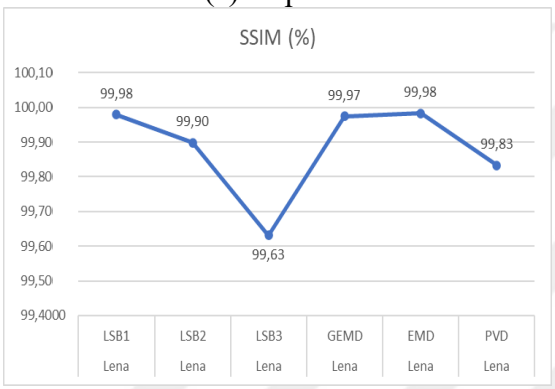
LSB-3 bit yönteminde ise görsel kalite, yapısal benzerlik endeksi ve kapasite açısından tam tersi bir durum söz konusudur.



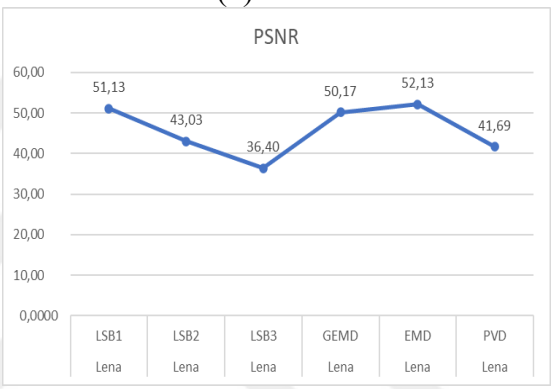
(a) Kapasite



(b) Yük



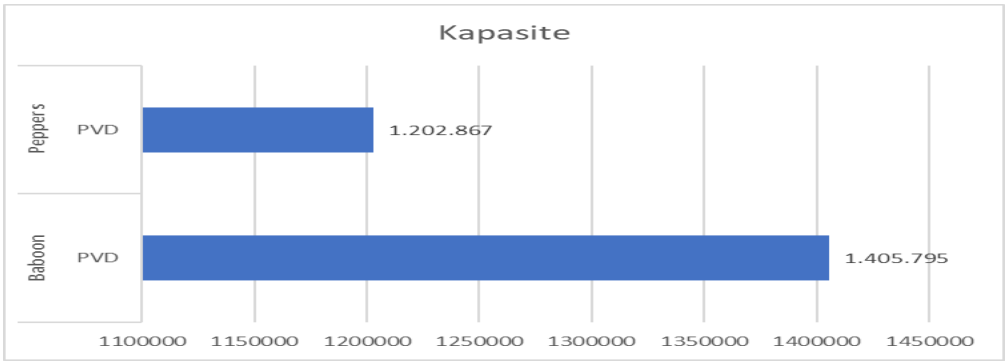
(c) SSIM (%)



(d) PSNR (dB)

Şekil 5.6. Tüm yöntemlerin karşılaştırması - Lena

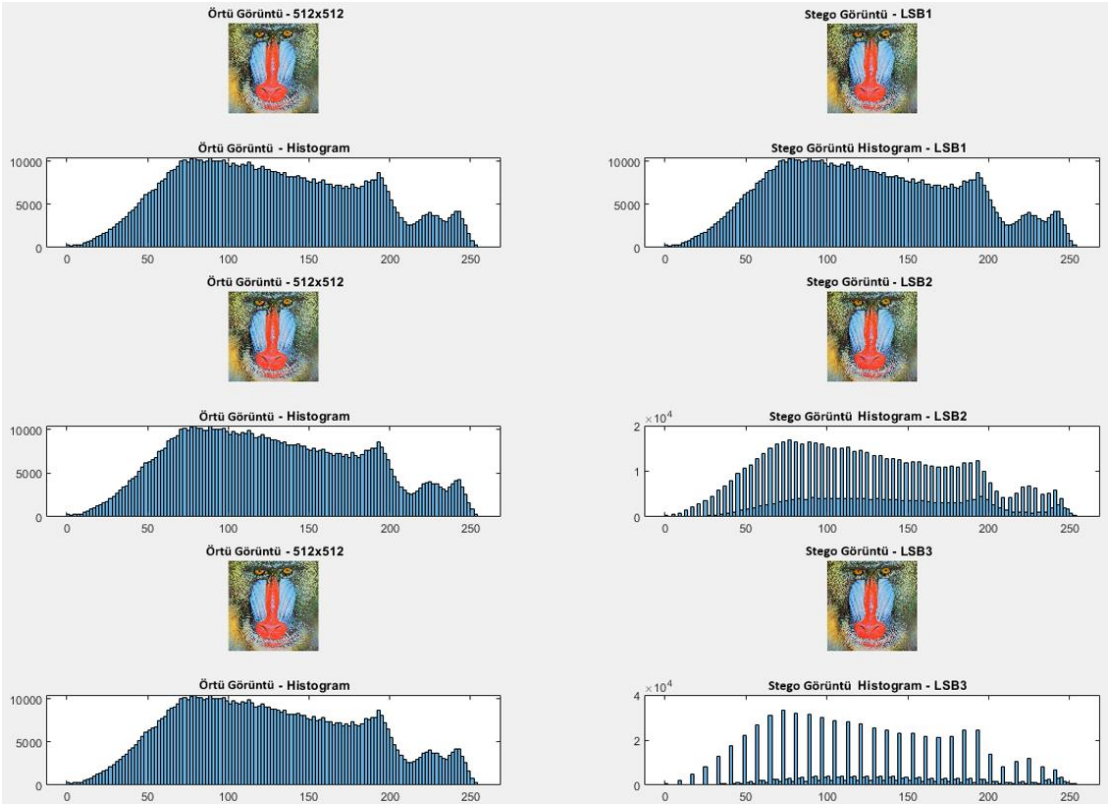
Daha önce de değinildiği üzere PVD yöntemi için kullanılan örtü resmi önem taşımaktadır. PVD yönteminde, Baboon ve Peppers görüntülerinin örtü görüntüsü olarak kullanılması arasındaki kapasite farkı Şekil 5.7'de gösterilmektedir.



Şekil 5.7. PVD için Baboon ve Peppers görüntülerinin kapasiteleri

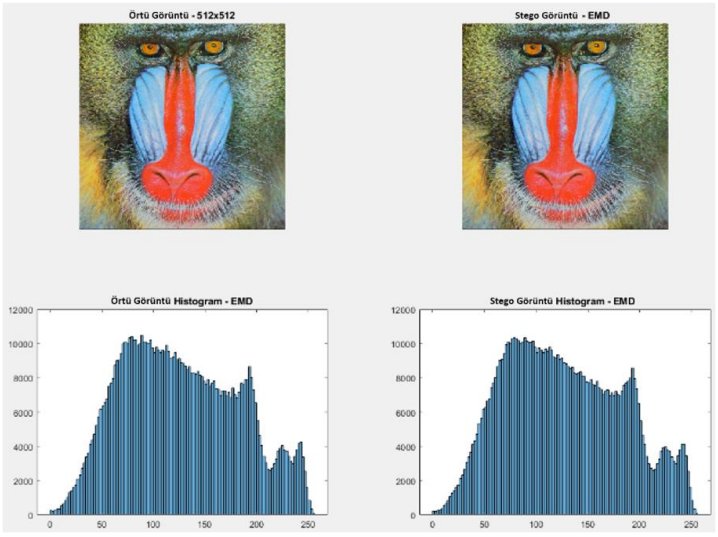
LSB-k bit yöntemiyle veri gizlenmiş stego görüntülerin histogramını örtü görüntüler ve birbirleriyle kıyasladığımızda, Şekil 5.8'de görüldüğü üzere stego görüntülerin histogramlarındaki tarak etkisi göze çarpmaktadır. Bu durum, görüntüde bir veri gizleme işleminin yapıldığını göstermektedir. LSB-k yöntemindeki "k" değeri arttıkça stego görüntüdeki tarak etkisinin belirginliği de artmaktadır. Bu da stego görüntünün algılanamazlığını etkilemektedir.

Bu etkinin LSB-1 bit yönteminde daha az belirgin oluşunun sebebi, her pikselde sadece bir bit değişim olması ve bazı bitlerde değiştirilecek bitin eski değeri yeni bitle aynı değeri taşıdığı için bit değerinde bir değişim olmamasından kaynaklanmaktadır.

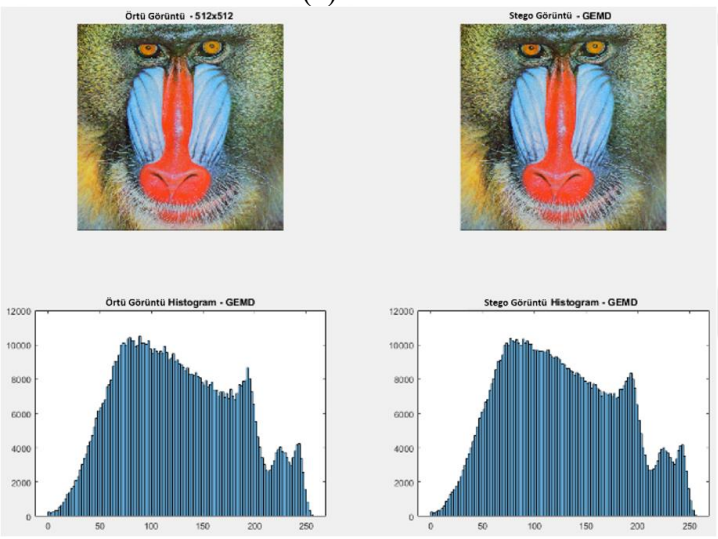


Şekil 5.8. Baboon görüntüsü için LSB 1-2-3 bit histogramları

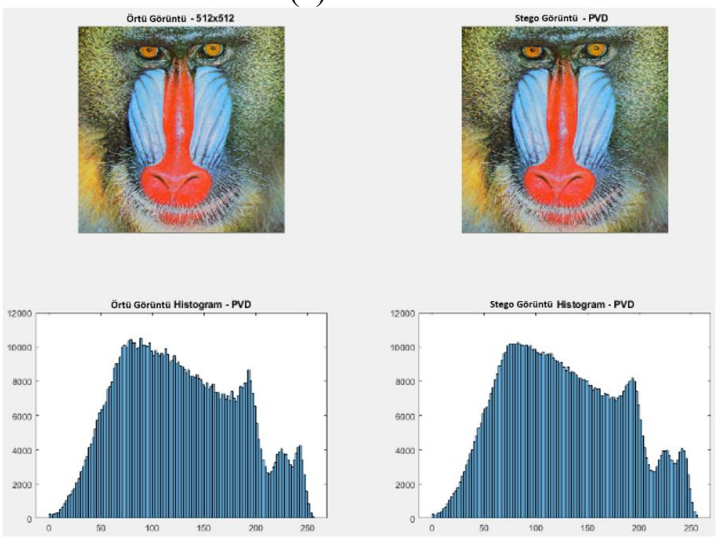
LSB-k bit yönteminde belirgin bir şekilde görülen tarak etkisi, Şekil 5.9'da da görüldüğü üzere PVD, EMD ve GEMD yöntemlerinde görülmemektedir. Bu, bu yöntemlerin histogramdaki tarak etkisine karşı daha dayanıklı ve çok daha iyi algılanamazlığa sahip olduğunu göstermektedir.



(a) EMD



(b) GEMD



(c) PVD

Şekil 5.9. Baboon görüntüsü için EMD, GEMD ve PVD histogramları

LSB ile PVD yöntemlerinin performans analizi ile ilgili yapılan bir çalışma Tablo 5.3 ve Tablo 5.4'te sunulmuştur. Tablolar incelendiğinde, Baboon görüntüsü ile ilgili çalışmamızda elde ettiğimiz sonuçların tutarlı olduğunu göstermektedir.

Tablo 5.3. 512x512 Gri ölçekli görüntü sonuçları

Örtü Görüntü		Lena	Baboon	Peppers	Airplane
LSB	Kapasite (bpp)	1	1	1	1
	PSNR (dB)	51,141	51,148	51,14	51,15
	SSIM (%)	0,996	0,9987	0,9963	0,9956
PVD	Kapasite (bpp)	1,563	1,744	1,554	1,563
	PSNR (dB)	41,417	38,529	41,392	40,311
	SSIM (%)	0,9728	0,9876	0,9748	0,9674

Tablo 5.4. 512x512 RGB görüntü sonuçları

Örtü Görüntü		Lena	Baboon	Peppers	Airplane
LSB	Kapasite (bpp)	2,67	2,67	2,67	2,67
	PSNR (dB)	51,656	51,654	51,619	51,653
	SSIM (%)	0,9998	0,9997	0,9998	0,997
PVD	Kapasite (bpp)	4,708	5,362	4,717	4,669
	PSNR (dB)	41,283	37,829	40,934	40,611
	SSIM (%)	0,9981	0,9945	0,998	0,9751

Veriler, PVD yönteminin LSB yöntemine göre yüksek gömme kapasitesi sağladığını göstermektedir. Ancak, LSB yöntemi, PVD yönteminden daha yüksek PSNR ve SSIM değerleri vermiştir. Örtü görüntüsüne az miktarda veri gömüleceği zaman, LSB ikame yönteminin kullanılması tercih edilir çünkü gerçekleştirmesi daha kolaydır. PVD yönteminin kullanılması, yüksek miktarda veri gizlenmişse daha uygun olacaktır (Solak ve Altınışık, 2018).

Tablo 3.6 ve Tablo 3.8 birlikte incelendiğinde hem EMD hem de GEMD için en yüksek kapasiteye n=2 piksel için ulaşılmaktadır. Gömme işlemi için seçilen pikseller arttıkça (n) EMD'nin gömme yükü büyük ölçüde azalmaktadır. GEMD'nin EMD'den farklı olarak yük (bpp) hep 1'den yüksektir; bu yüzden daha iyi gömme kapasitesi sağlar. Ayrıca GEMD, bellek ve zaman tüketiminde daha iyidir (Essad ve Lamiles, 2016). Şekil 5.6'dan GEMD'nin PSNR değerlerine bakıldığında yöntem, LSB ve PVD'ye göre daha yüksek görsel kalite sunarken EMD'ye göre düşük kalmıştır. Bu konuda yapılan ve farklı iki

ebattaki görüntüyü içeren bir çalışmadan (Essad ve diğ., 2016) elde edilen veriler, Tablo 5.5'te sunulmuştur. Bu verilerde de aynı sonuçlar gözlemlenmektedir.

Tablo 5.5. 512 ve 1024 Gri görüntü için EMD-GEMD verileri (Essad ve Lamiles, 2016)

Yöntem	Boyut	PSNR (dB)	MSE	Süre (sn.)	Hafıza (MB)	Kapasite (BPP)
EMD	512x512	**53,97**	0,27	5,71	488	0,89
GEMD	512x512	50,77	**0,54**	**5,36**	**485**	**1,32**
EMD	1024x1024	**53,97**	0,27	3,81	496	0,89
GEMD	1024x1024	50,77	**0,54**	**3,33**	**494**	**1,32**

5.2. Önerilen Yöntemin Deneysel Sonuçları

Önerilen yöntemin deneysel sonuçları, bu bölümde yer almaktadır. Yöntem, gizleme kapasitesi, tepe sinyal gürültü oranı (PSNR) ve yapısal benzerlik indeksi ölçüsü (SSIM), yük (bpp) gibi veri gizleme ölçütleriyle değerlendirilebilmek üzere altı farklı örtü görüntü üzerinde denenmiştir. Önerilen yöntem, "Algılanamazlık" konusunda bir yenilik olduğu için RS analizi, histogram analizi ve piksel dağılımları analizi gibi güvenlik testleri uygulanmıştır. Uygulamada Şekil 5.1'deki altı adet 512x512 ebatlarında renkli orijinal örtü görüntü kullanılmış olup örtü görüntülere, 1'den 300.000'e kadar sıralı sayıların virgüllerle ayrılmış halde bulunduğu bir metin dosyasından alınan veriler gizlenmektedir. Böylece, önerilen yöntemi oluşturan geliştirilme sürecinde yer alan farklı yöntemlerin test işlemleri ile çözme işleminden sonra elde edilen verinin, gizlenen veri ile aynı olup olmadığının kontrolü çok daha hızlı ve kolay bir şekilde gerçekleştirilmiştir.

Önerilen yöntemde 4 farklı veri gizleme yöntemi kullanılmıştır. Örtü görüntünün G ve B renk kanallarından alınan birer piksele uygulanacak yöntem, birden fazla parametreye bağlı olduğundan sürekli değişkenlik göstermektedir. Bu değişkenlik, örtü görüntünün R kanalının sıradaki pikseli değeri ve her döngüde Bit-Yöntem sıralaması değişen GB Yöntem Tablosundaki veriler ile elde edilmektedir. Bu nedenle, yöntemlerin örtü görüntülerde ne sıklıkla kullanıldığı, görüntüden görüntüye farklılık göstermektedir. Tablo 5.6'da tekrarlı kullanılan yöntemlerin kullanım miktarları yüzdesel olarak, Tablo 5.7'de ise adet olarak detaylı olarak verilmiştir. Bu tablolardaki veriler incelendiğinde örtü görüntüler için en çok kullanılan yöntem, her görüntü için farklılık göstermektedir. Airplane görüntüsünde LSB1 ve Hibrit; Baboon görüntüsünde PVD ve Hibrit; House

görüntüsünde LSB1 ve Hibrit; Lena görüntüsünde GEMD; Peppers görüntüsünde PVD ve Hibrit; Sailboat görüntüsünde ise LSB1 ve GEMD yöntemleri en çok kullanılmış olan yöntemler olarak görülmektedir. Yöntemlerin her bir görüntüdeki kullanım sıklıkları ve kullanım adetleri arasındaki farklarda da belirli bir örüntü bulunmamaktadır. Bu da, önerilen yöntemin her bir resimde farklı bir davranış sergilediğini ve tespit edilebilirliğinin zorluğunu göstermektedir.

Tablo 5.6. Yüzdesel olarak görüntü-yöntem yoğunluğu

	LSB1	**GEMD**	**HİBRİT**	**PVD**
Airplane	25,17	24,90	25,15	24,78
Baboon	24,91	24,91	25,06	25,12
House	25,16	24,76	25,11	24,97
Lena	24,92	25,16	24,93	24,99
Peppers	24,99	24,99	25,02	25,00
Sailboat	25,07	25,07	24,92	24,94

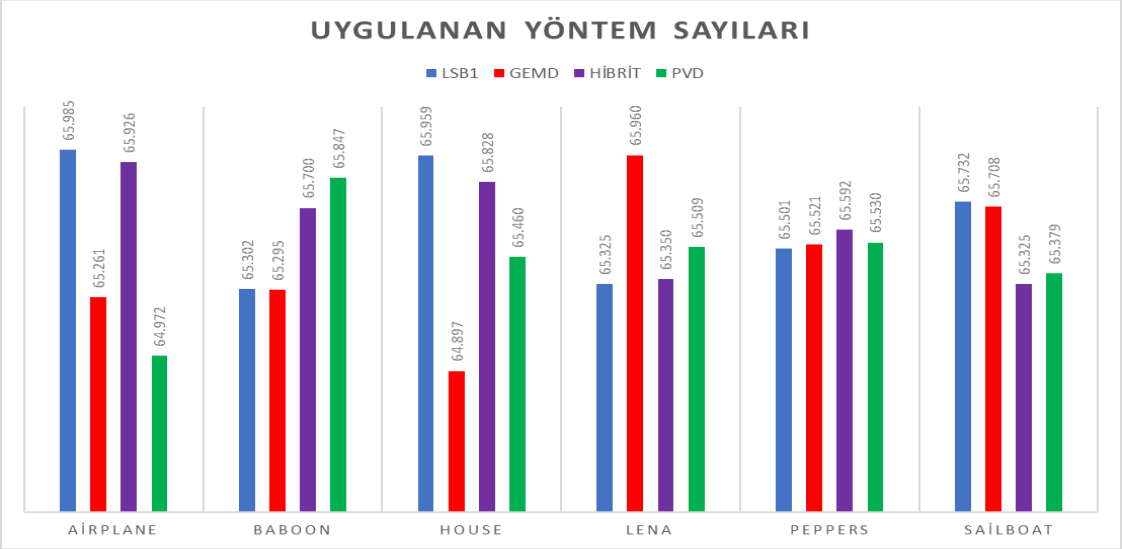
Tablo 5.7. Uygulanan görüntü-yöntem adedi

	LSB1	**GEMD**	**HİBRİT**	**PVD**
Airplane	65.985	65.261	65.926	64.972
Baboon	65.302	65.295	65.700	65.847
House	65.959	64.897	65.828	65.460
Lena	65.325	65.960	65.350	65.509
Peppers	65.501	65.521	65.592	65.530
Sailboat	65.732	65.708	65.325	65.379

Şekil 5.10'da görüldüğü üzere farklı örtü görüntülerde 4 yöntemin kullanım sıklığı farklılık göstermektedir. House görüntüsünde en az kullanılan GEMD yöntemi, Lena görüntüsünde en çok kullanılan yöntem olmuş; Sailboat görüntüsünde en az kullanılan PVD yöntemi ise Baboon görüntüsünden en çok kullanılan yöntem olmuştur. Bu durum, uygulamada 4 yöntemin kullanılması ve LSB1-GEMD-Hibrit-PVD başlangıç sırasına sahip GB Yöntem Tablosunun sonucudur.

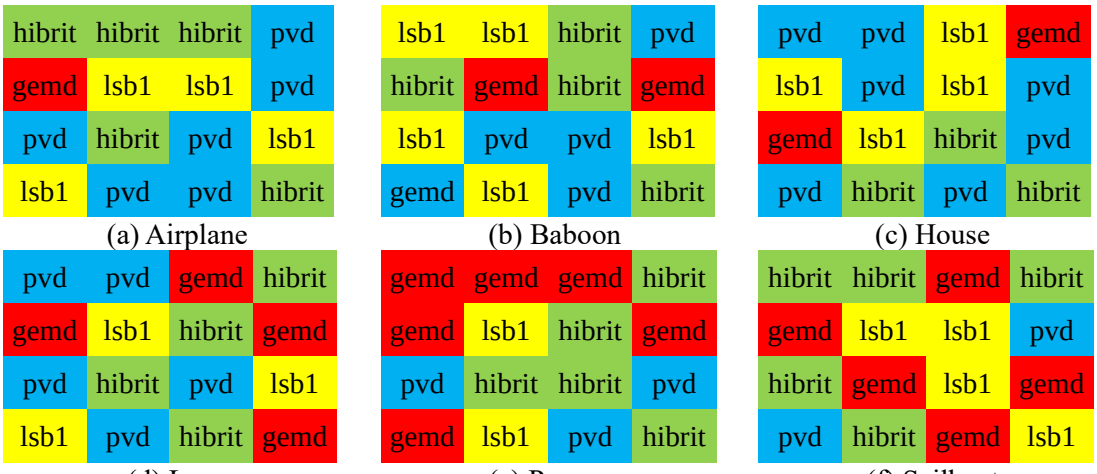
Uygulamada 4 yerine 3 yöntem kullanılması durumunda bu dağılım tamamen değişebilecektir.

Yine, GB Yöntem Tablosundaki yöntemlerin başlangıç sıralarının farklı olması da bu dağılımın farklı olmasıyla sonuçlanacaktır. Görüldüğü üzere yöntem, örtü görüntü, yöntem sayısı ve yöntem sıralamasına göre değişken sonuçlar üretmektedir. Bu durum, önerilen yöntemin algılanamazlık kabiliyetini arttırmaktadır.



Şekil 5.10. Görüntü bazında uygulanan yöntem sayıları

Her bir örtü görüntüde kullanılan piksel çiftlerinden artarda gelen 16 adet piksel alınarak 4x4'lük piksel grupları elde edilmiştir. Bu gruplardaki pikseller, o piksellerde uygulanan yönteme göre adlandırılmış ve renklendirilmiş olup Şekil 5.11'de görülmektedir. Farklı örtü görüntülerdeki aynı konuma sahip piksel çiftleri için kullanılan yöntemlerin gösterdiği farklılık çok net bir şekilde gözlemlenebilmektedir.

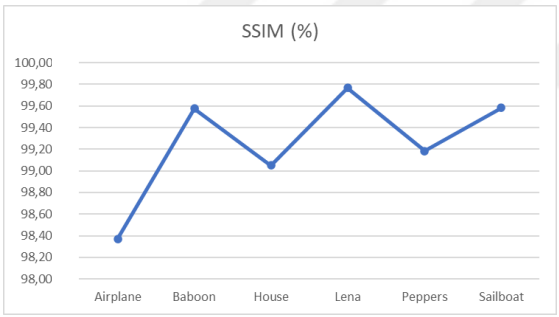


Şekil 5.11. Piksel-Yöntem kıyaslamaları

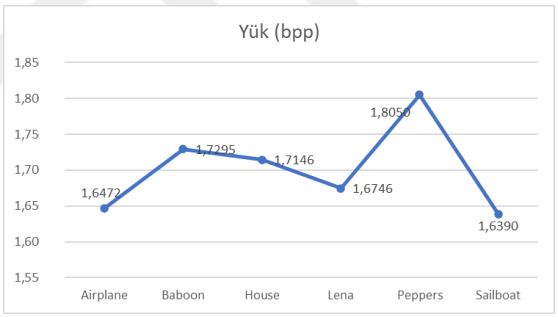
Önerilen yöntem ile farklı örtü görüntülerde elde edilen sonuçlar Tablo 5.8'de verilmiştir. Yöntem, SSIM, yük ve kapasite konusunda başarılı sonuçlar elde etmiş olup PSNR değeri olarak da kabul edilebilir alt sınır olan 30dB'nin üzerinde kalmayı başarmıştır. Şekil 5.12'de görülen Peppers görüntüsüne ait PSNR değerinin diğer görüntülere göre düşük seviyede kalması, görüntüde yoğun olarak karşılaşılan FOBP sorunundan kaynaklı olabilir. Tablo 5.8'de yer alan verilerin kıyaslamasının yapıldığı grafikler Şekil 5.12'de görülmektedir.

Tablo 5.8. Örtü görüntüler için önerilen yönteme ait performans değerleri

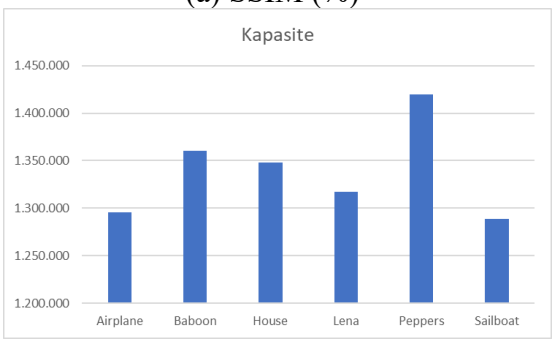
Görüntü	PSNR (dB)	SSIM (%)	Yük (bpp)	Kapasite
Airplane	39,3756	98,3729	1,6472	1.295.405
Baboon	37,5724	99,5769	1,7295	1.360.151
House	37,2735	99,0514	1,7146	1.348.409
Lena	40,6940	99,7657	1,6746	1.316.969
Peppers	33,9616	99,1817	1,8050	1.419.531
Sailboat	40,8000	99,5836	1,6390	1.288.930



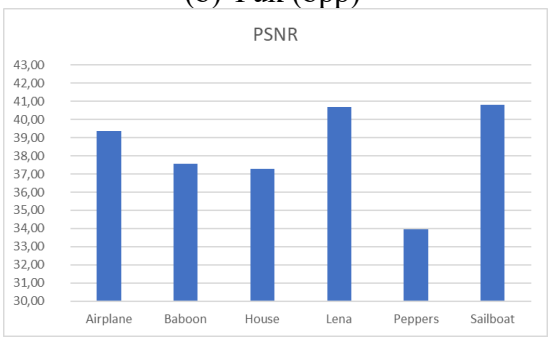
(a) SSIM (%)



(b) Yük (bpp)



(c) Kapasite

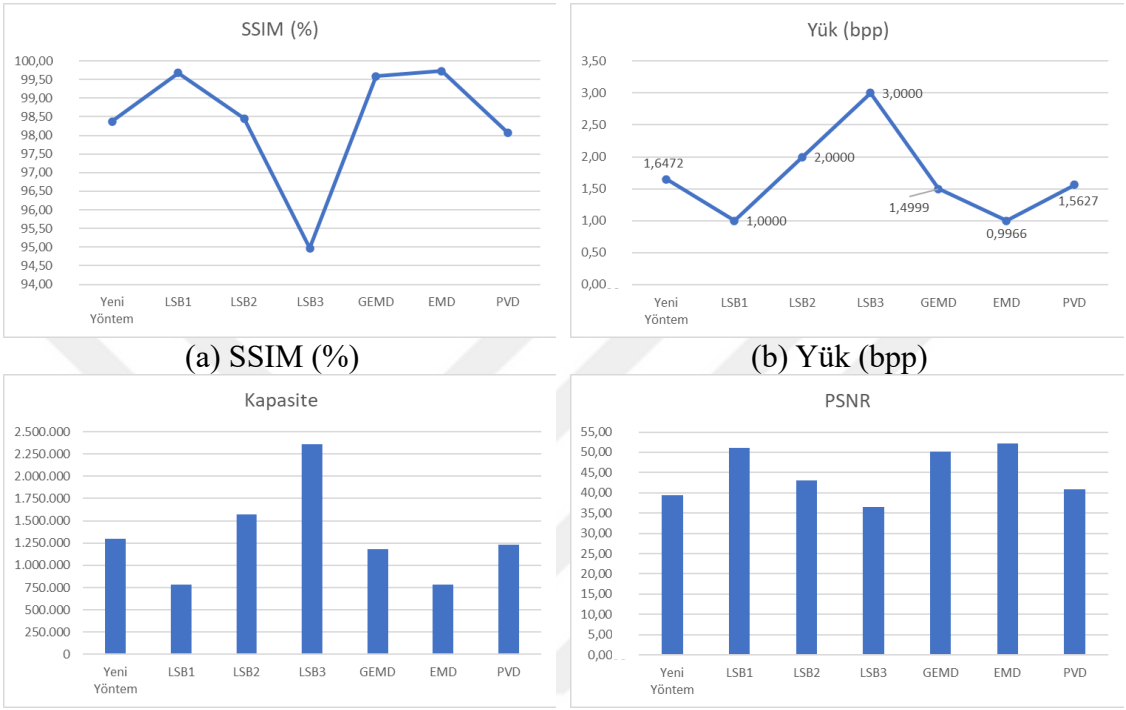


(d) PSNR (dB)

Şekil 5.12. Önerilen yöntemin PSNR, SSIM, Yük ve Kapasite grafikleri

Önerilen yöntem ile mevcut Uzamsal Domainde Kullanılan yöntemlerin Airplane örtü görüntüne ait kıyaslanmasını içeren grafikler Şekil 5.13'te verilmiştir. Güvenliğin ön

planda tutulduğu önerilen yöntem, SSIM-Yük-Kapasite olarak diğer yöntemlerin ortalamasının üstünde değerler elde ederek bu kriterlerdeki başarısını koruyabilmiştir. Sadece PSNR değerinde ortalamanın altında olsa da 40dB'ye yakın bir değerle örtü-stego görüntü benzerliği adına başarılı bir stego görüntü kalitesi elde edilmiştir.

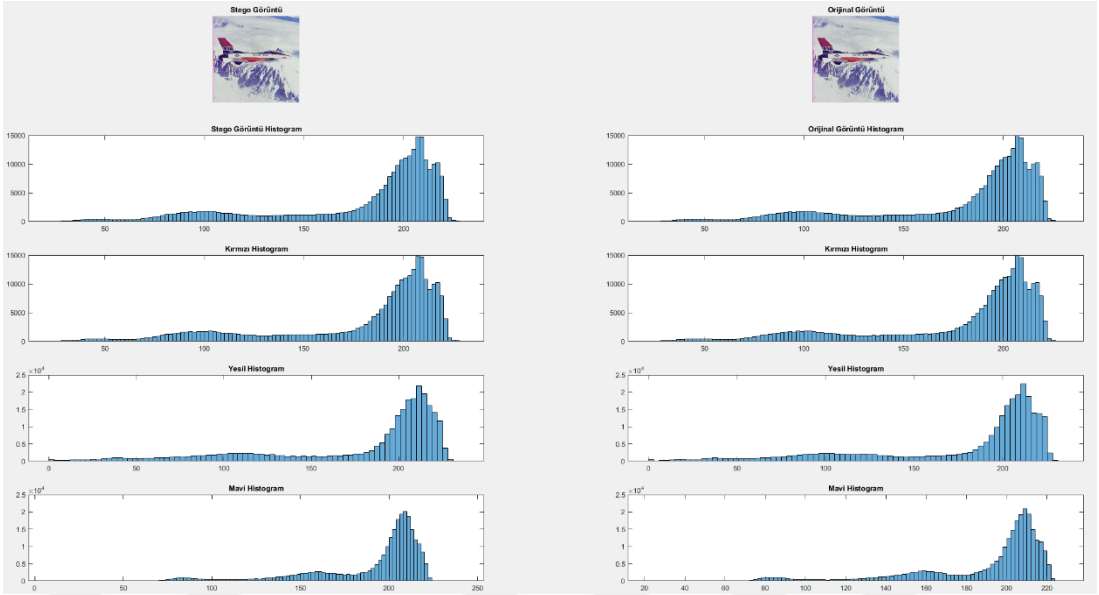


(a) SSIM (%) (b) Yük (bpp)

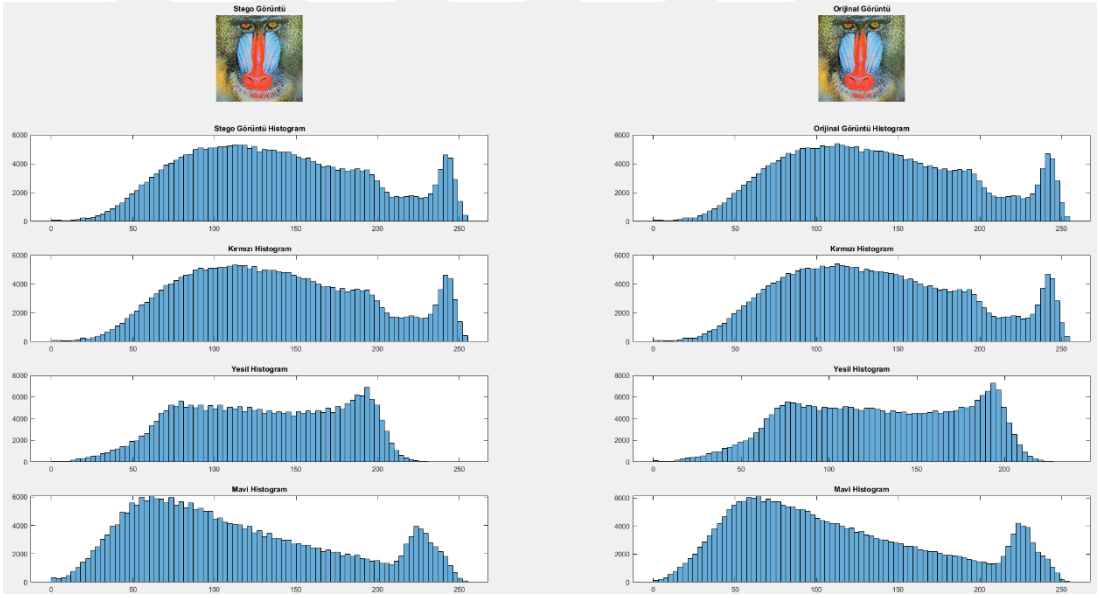
(c) Kapasite (d) PSNR (dB)

Şekil 5.13. Airplane örtü görüntüsü için tüm yöntemlerin kıyaslanması

Uygulamada kullanılan örtü görüntüler ile önerilen yöntem ile elde edilmiş stego görüntülere ait histogramlar birbirine çok benzer olup Şekil 5.14'te verilmiştir.

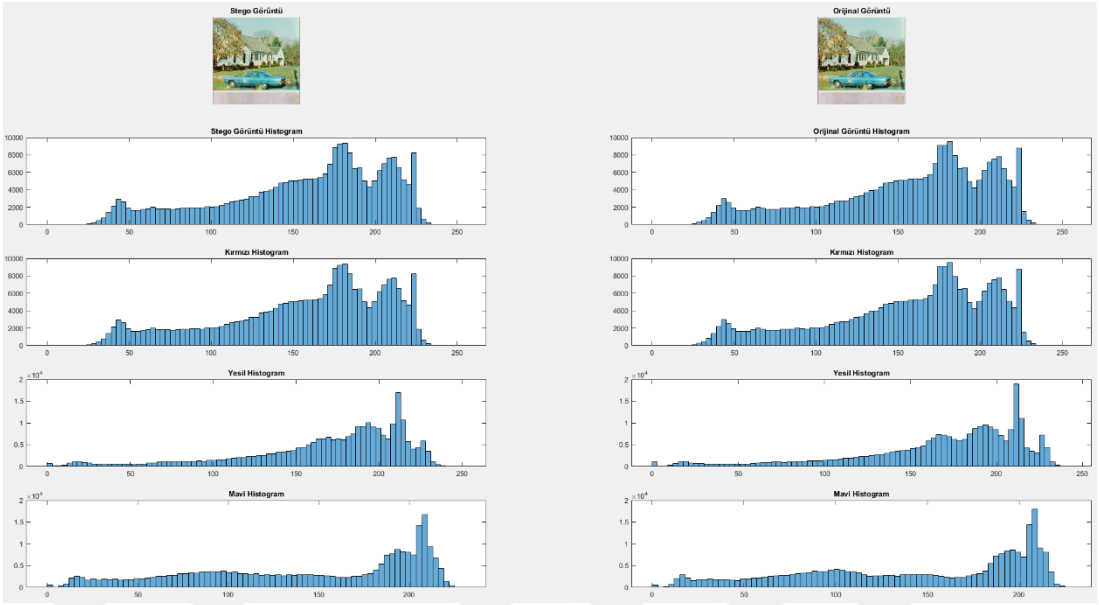


(a) Airplane

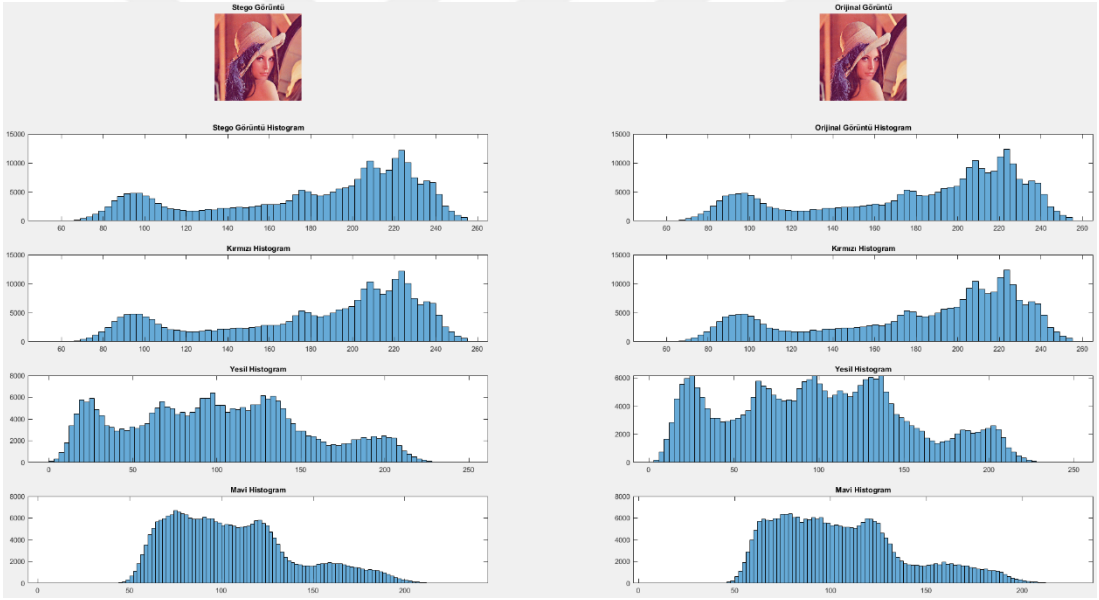


(b) Baboon

Şekil 5.14. Önerilen Yöntem için histogram Karşılaştırmaları

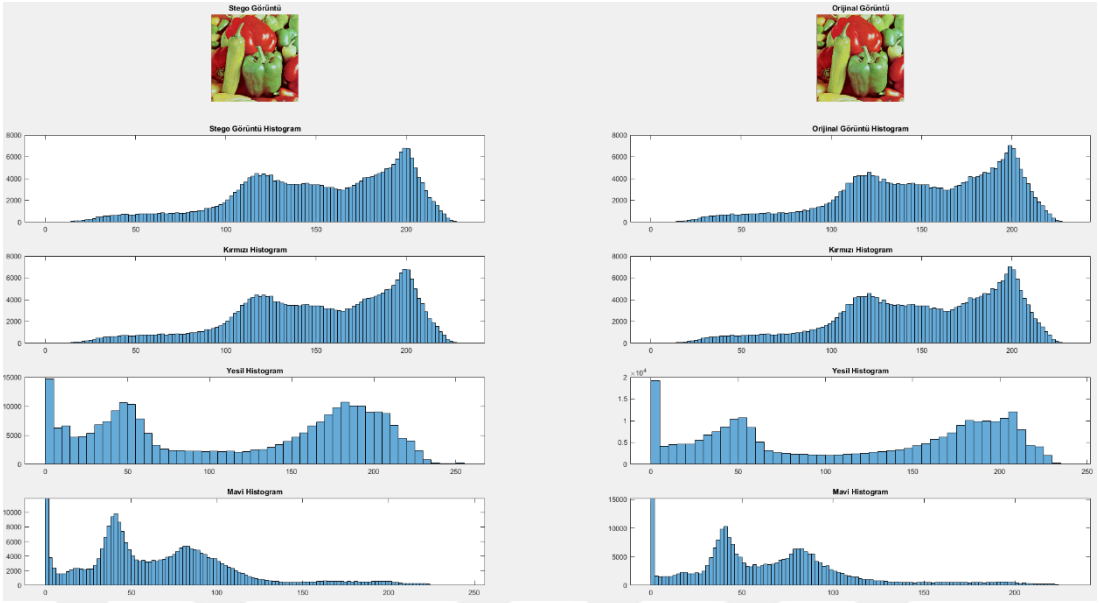


(c) House

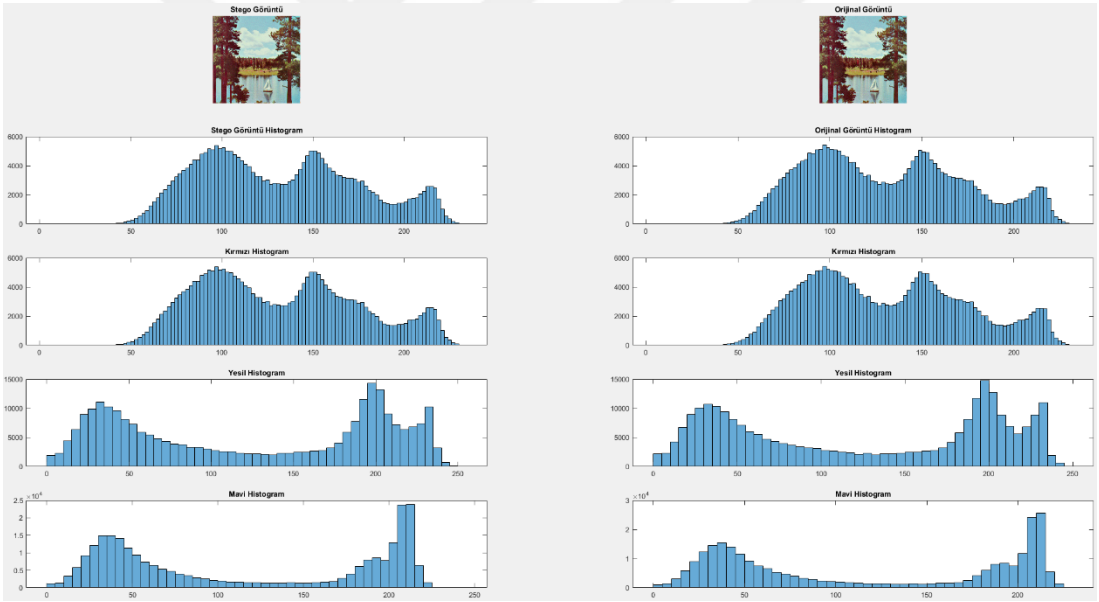


(d) Lena

Şekil 5.14. (Devam) Önerilen Yöntem için histogram Karşılaştırmaları



(e) Peppers



(f) Sailboat

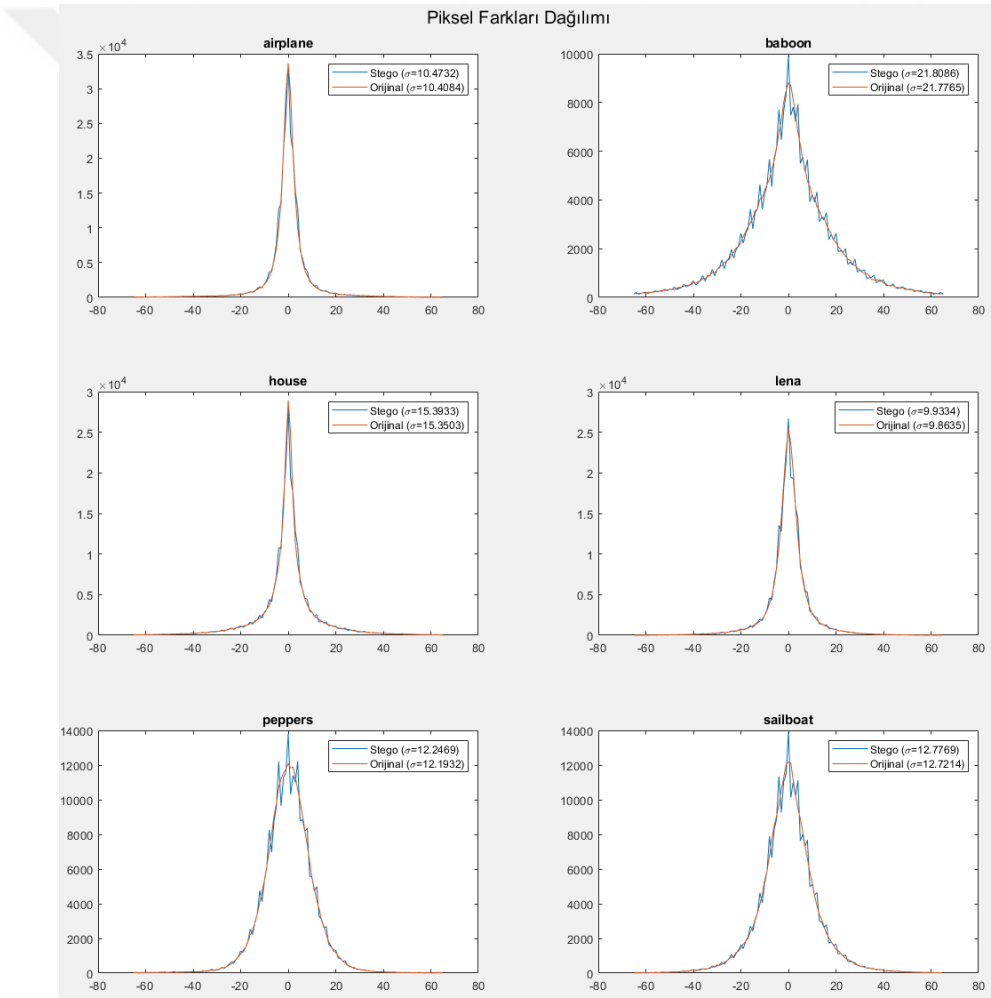
Şekil 5.14. (Devam) Önerilen Yöntem için histogram Karşılaştırmaları

5.2.1. Güvenlik Testleri

Önerilen yöntem ile elde edilen stego görüntüye ait Piksel Farkları Dağılımı ve RS Analizi ile sonuçları paylaşılmaktadır.

5.2.1.1. Piksel Farkları Dağılımı (PDH)

Piksel farkları histogramında, stego görüntüye ait dağılım eğrisinde testere dişi formunda dağılım, düzenli eğriler veya çoklu tepe oluşması görülebilir. Önerilen yöntem ile elde edilen stego görüntülerin örtü görüntüler ile piksel farkları dağılımları Şekil 5.15'te verilmektedir.



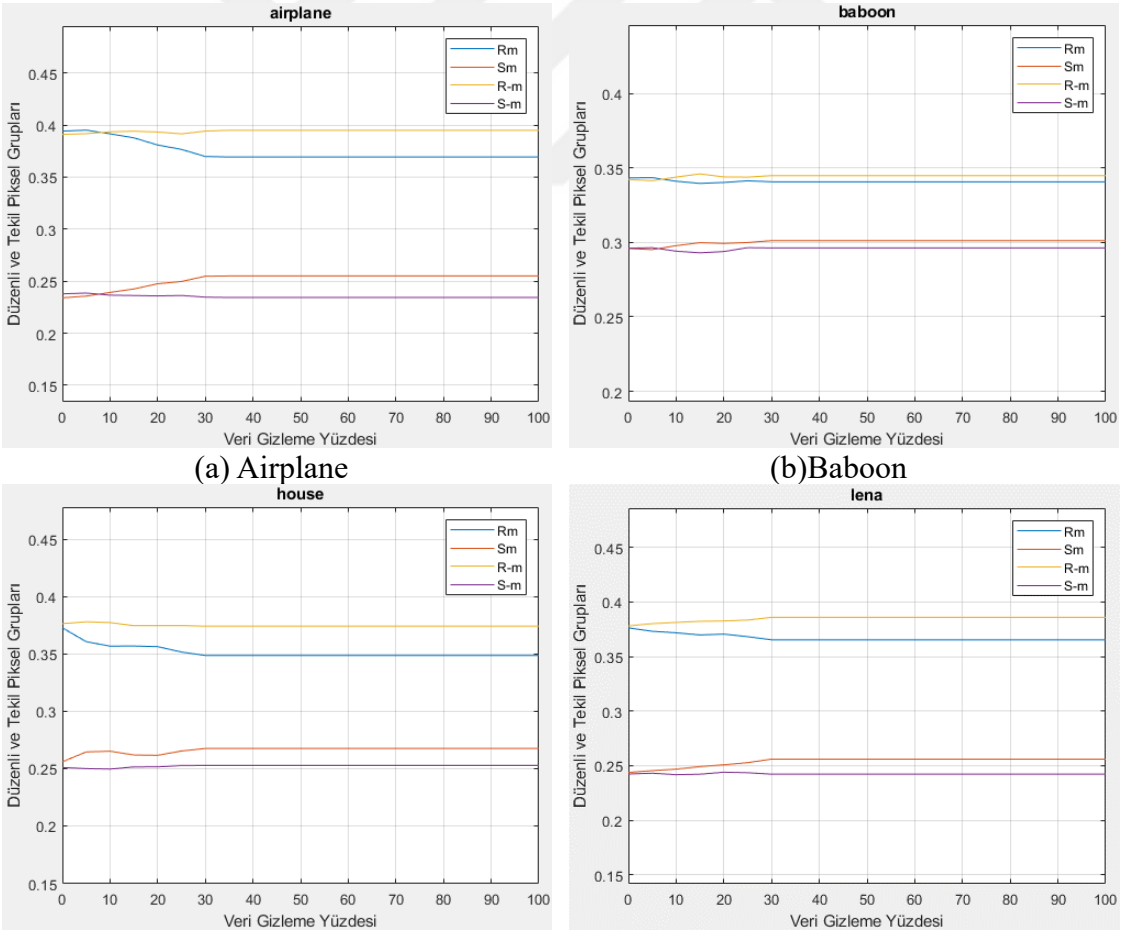
Şekil 5.15. Görüntülere ait PDH'ler

Şekil 5.15 incelenecek olursa, Airplane-House-Lena görüntülerindeki dağılımın neredeyse birebir örtüştüğü görülmektedir. Baboon-Peppers-Sailboat görüntülerinde ise

zigzaglar mevcuttur. Kullanılan yöntemin FOBP duyarlılığı, örtü görüntünün dokusu, kullanılan yöntemlerin yoğunluğu, R kanalı için denk gelen yöntem, FOBP için alınan yöntem vb. birçok parametre, yoğunluk grafiğinde bu tarz değişmelere neden olabilmektedir. Uygulamada kullanılan yöntemlerden farklı yöntemlerin dahil edilmesi, yöntem sayısının farklılaştırılması gibi değişimler bu dağılımı da doğrudan etkileyecektir.

5.2.1.2. RS Analizi

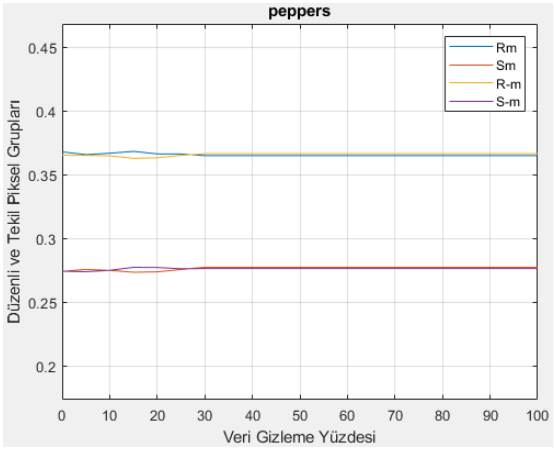
Önerilen uygulamanın steganalize karşı dayanıklılığını incelemek için istatistiksel bir yöntem olan RS analizi yapılmıştır. Uygulamada kullanılan 6 adet örtü görüntünün her birine %0'dan başlayarak %100'e kadar %5'lik adımlarla veri gizlenerek her bir örtü görüntünün 20 farklı stego görüntüsü hazırlanmıştır. Toplam 120 adet görüntü, RS Analizinde kullanılarak Şekil 5.16'daki analiz sonuçları elde edilmiştir. Sonuçlar göstermektedir ki önerilen yöntem, RS Analizine karşı gizlenme konusunda etkilidir.



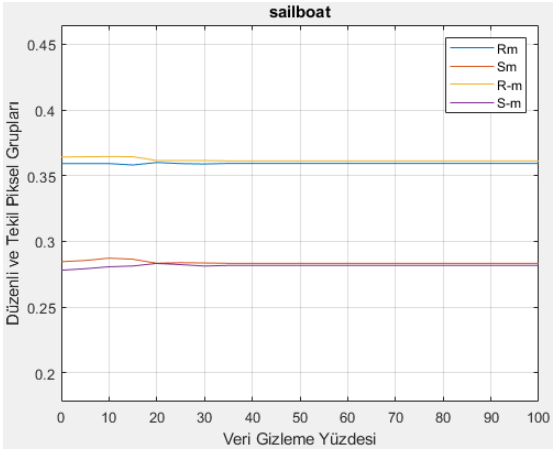
(a) Airplane (b)Baboon

(c) House (d) Lena

Şekil 5.16. RS Analizi Sonuçları



(e) Peppers



(f) Sailboat

Şekil 5.16. (Devam) RS Analizi Sonuçları

6. SONUÇ

Tez çalışmasında, uzamsal alanda yaygın kullanılan LSB, EMD, GEMD ve PVD teknikleri detaylı incelenmiş ve bunların beraber (tekil veya hibrit olarak) kullanımına yönelik görüntü steganografisi için yeni bir veri gizleme yöntemi önerilmiştir.

Deneysel çalışmalarda, 512x512 ebatlarındaki 6 örtü görüntü üzerinde LSB-k (K={1,2,3}), EMD, GEMD ve PVD olmak üzere 6 veri gizleme yöntemi denenmiştir. PSNR değerlerine bakıldığında, tüm görüntüler için en yüksek görüntü kalitesi EMD ile elde edilmiştir. EMD ile tüm görüntülerde 51,88 dB ve üzeri PSNR değeri elde edilirken LSB-3 yöntemi ~36,4 dB ile en düşük görüntü kalitesini sunmuştur. PVD yöntemi, LSB-3'e kıyasla biraz fazla olmakla birlikte düşük bir görüntü kalitesi sergilemektedir. Diğer yandan LSB-3 yöntemi, 3 bit'lik yük kapasitesi olarak en yüksek değeri ve dolayısıyla en yüksek veri gizleme kapasitesini sunmuştur. EMD yöntemi, tüm yöntemlerin ortalama kapasitesinden ~%40 daha düşük bir değer ile en düşük kapasiteyi sunmuştur. Bu da, EMD ve LSB-3 yöntemlerinde, kapasite ve görüntü kalitesi arasında ciddi bir takas olduğunu göstermektedir. LSB-1 yönteminin görüntü kalitesi, görüntü kalitesi en yüksek yöntem olan EMD'ye çok yakındır. Ancak, LSB-1'in RS analizine karşı zayıf olduğu ve histogramlardaki tarak etkisinin algılanamazlığını etkilediği bilindik bir gerçektir. Bu zayıflıkları taşımaması ve nispeten daha yüksek kapasite sunması nedeniyle PVD yöntemi, LSB-1'e iyi bir alternatif oluşturmaktadır. Tüm bu veriler ışığında, LSB-3 ile yüksek kapasite; GEMD – EMD ile yüksek algılanamazlık ve görüntü kalitesi; PVD ile yoğun doku farklılığı olan görüntülerde yüksek kapasite elde edilmesi mümkündür. Steganografik yöntemin, yüksek kapasite, yüksek algılanamazlık ve/veya yüksek stego görüntü kalitesi gibi hangi amaçla kullanılacağına bağlı olarak uygun yöntem seçilmelidir.

Tez kapsamında, önerilen yeni veri gizleme yönteminin uygulanmasında 4 farklı yöntem belirlenmiş olup bu yöntemler GEMD, LSB-1, PVD ve Hibrit (PVD + LSB-1) olarak seçilmiştir. Tüm analizler, bu kapsamda gerçekleştirilerek sonuçlar elde edilmiştir.

6 adet örüntü görüntü üzerinde test edilen önerilen yöntem, tüm görüntülerde, LSB-3 ve LSB-2'den sonra ortalama 1,70 bpp ile yük kapasitesi, 1.338.233 bit ile toplam kapasitede diğer yöntemleri geride bırakmıştır. PSNR ölçümlerinde 30 dB'yi geçerek ~34 – 41 dB aralığında değerler almış olup ortalama 38 dB'lik bir değer elde etmiştir. Yöntem ile

görüntü kalitesi korunmuş olsa da diğer yöntemlere göre en yüksek değerleri elde edilmemiş olmasının nedeni, seçilen 4 adet yöntem ve bu yöntemlerde karşılaşılan FOBP çözümü için kullanılan algoritmalardır. Uygulamada kullanılan yöntemlerden PVD yöntemi, EMD veya PSNR sonuçları yüksek bir başka yöntem ile değiştirilirse görüntü kalitesinde gözle görülür bir artış elde edilecektir. Görüntü benzerliği ölçümlerinde ise SSIM değeri, uzamsal alanda yaygın olarak kullanılan 6 yöntemle Airplane görüntüsünde kıyaslandığında %94,96 – %99,72 maksimum ve minimum değerleri arasında, %98,37 ile orta sıralarda yer almıştır.

Stego ve örtü görüntülere ait histogramlar karşılaştırılmış olup çok benzer grafikler elde edilmiştir. Histogramlarda belirgin bir tarak etkisi gözlemlenmemiştir. Bunun yanında, grafiklerde, tavan ya da taban yapma durumu gibi olumsuzluklara da rastlanmamıştır.

PDH analizi örtü ve stego görüntü için uygulanmıştır. Yapılan analizde, orijinal görüntü için piksel farkları dağılımının normal dağılıma uygun olduğu gözlemlenmiştir. Stego görüntülerin piksel farkları dağılımı da orijinal görüntüye çok yakın dağılımlara sahiptir. Bu analizde, orijinal ve stego görüntüden elde edilen grafikler aynı düzlemde incelendiğinde, grafiklerin birbiriyle örtüşmesi gerekmektedir. Yapılan çalışmada ise örtü-stego görüntülerin PDH'lerinin birbiriyle örtüştüğü ancak, PVD yönteminin kullanılmış olmasından kaynaklı olarak bazı stego görüntülerde basamaklanma veya zikzak çizme gibi etkiler görülmüştür.

Önerilen yöntemin güvenlik testi için yönteme RS Analizi de uygulanmıştır. RS Analizi sonuçları göstermiştir ki önerilen yöntem bu ataklara karşı dayanıklıdır.

Önerilen yöntemi farklı kılan nokta, görüntü steganografisinde veri gizleme işleminde farklı bir yaklaşım sergilenmiş olmasıdır. Genel olarak, literatürde görüntü steganografisi için yapılan veri gizleme çalışmalarında, örtü görüntü içerisine veriler tek bir teknik ile gizlenmektedir.

Önerilen yöntemin algoritması, örtü görüntünün kırmızı kanalını referans almakta ve verinin iletileceği tarafça bilinmeyen bilgilerin bazıları bu kanalda gizlenmektedir. R kanalına uygulanacak yöntem de yine bu kanaldaki ilk piksel tarafından belirlenmektedir. R kanalına veri gizlendikten sonra oluşan yeni piksel değerleri ise G ve B kanallarındaki

piksellere uygulanacak yöntemi, her piksel çiftinde sıralaması değişmekte olan bir tablo (GB Yöntem Tablosu) aracılığıyla belirlemektedir. Tüm bu bilgiler ışığında, yöntem son derece parametrik ve doğal olarak değişken bir yapıda olduğundan tahmin edilmesi ve algılanması son derece zordur. Ayrıca, R kanalına uygulanacak yöntemin belirlendiği statik tablodaki yöntemler (R Kanalı Yöntemleri), yöntem adetlerinin bit bazında ifade edildiği diğer bir statik tablodaki (Yöntem-Adet Tablosu) eşleşmeler, yöntemler ile onları ifade eden bitlerin eşleştirildiği tablodaki (Yöntemler Tablosu) veriler, G-B kanallarına veri gizlemede kullanılacak olan sıra-yöntem bilgilerinin tutulacağı başlangıç pikselinin belirlenmesinde rol oynayan örtü görüntü boyutu değişken niteliği taşımaktadırlar. Bu nedenle, yöntem farklı ebatlardaki görüntü kullanımına, farklı yöntem ve farklı dizilişler uygulanmasına, mevcut yöntemlerin değiştirilmesine ve/veya sayısının arttırılmasına son derece müsaittir. Bu, yöntemin esnekliğini ve dolayısıyla gelişime açık olduğunu göstermektedir.

KAYNAKLAR

Amirtharajan, R., Balaguru Rayappan, J. B. (2012). An intelligent chaotic embedding approach to enhance stego-image quality. *Information Sciences, 193*, 115–124. DOI: 10.1016/j.ins.2012.01.010

Balasubramanian, C., Selvakumar, S., Geetha, S. (2014). High payload image steganography with reduced distortion using octonary pixel pairing scheme. *Multimedia Tools and Applications, 73*, 2223–2245. DOI: 10.1007/s11042-013-1640-4

Carneiro Tavares, J. R., Madeiro Bernardino Junior, F. (2016). Word-Hunt: A LSB Steganography Method with Low Expected Number of Modifications per Pixel. *IEEE Latin America Transactions, 14*(2), 1058–1064. DOI: 10.1109/TLA.2016.7437258

Chan, C. K., Cheng, L. M. (2004). *Hiding data in images by simple LSB substitution. Pattern Recognition, 37*(3), 469–474. DOI: 10.1016/j.patcog.2003.08.007

Lamiles, O. (2016). Analysis and Experimental Study of EMD and GEMD Steganographic Methods. Master of Science in Computer Engineering, Gazimağusa/North Cyprus

Fridrich, J., Goljan, M., Du, R. (2001). *Reliable Detection of LSB Steganography in Color and Grayscale Images. IEEE Multimedia 8*(4), 22-28

Grajeda-Marín, I. R., Montes-Venegas, H. A., Marcial-Romero, J. R., Hernández-Servín, J. A., De Ita, G. (2016). An Optimization Approach to the TWPVD Method for Digital Image Steganography. In: Martínez-Trinidad, J. F., J. A. Carrasco-Ochoa, V. Ayala Ramirez, J. A. Olvera-López & X. Jiang (eds.), *Pattern Recognition* (125–134). Cham: Springer International Publishing.

Huang, H. S. (2015). A combined image steganographic method using multi-way pixel-value differencing. *Sixth International Conference on Graphic and Image Processing (ICGIP 2014)*, Taoyuan 326, Taiwan, 2015.

Hussain, M., Wahab, A. W. A., Anuar, N. B., Salleh, R., Noor, R. M. (2015). Pixel value differencing steganography techniques: Analysis and open challenge, *2015 IEEE International Conference on Consumer Electronics*, Taiwan, 2015.

Hussain, M., Wahab, A. W. A., Javed, N., Jung, K. H. (2016). *Hybrid data hiding scheme using right-most digit replacement and adaptive least significant bit for digital images 8*, 41.

Hussain, M., Abdul Wahab, A. W., Ho, A. T. S., Javed, N., Jung, K. H. (2017). A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. *Signal Processing: Image Communication, 50*, 44–57.

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). Steganalysis: The investigation of hidden information. *1998 IEEE Information Technology Conference: Information Environment for the Future, IT 1998*, Fairfax, Virginia, September 1998.

Jung, K. H., Yoo, K. Y. (2015). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications, 74*, 2143–2155.

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.

Khodaei, M., Faez, K. (2012). New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. *IET Image Processing, 6*, 677–686.

Khodaei, M., Bigham, B., Faez, K. (2016). Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution. Cybernetics and Systems, 1–12.

Kieu, T. D., Chang, C. C. (2011). A steganographic scheme by fully exploiting modification directions. *Expert Systems with Applications, 38*, 10648–10657.

Kuo, W. C., Kuo, S., Huang, Y. (2013a). Data hiding schemes based on the formal improved exploiting modification direction method. *The Imaging Science Journal, 61*(6), 484-490, DOI: 10.1179/1743131X12Y.0000000011

Kuo, W. C., Kao, M. C. (2013b). A steganographic scheme based on formula fully exploiting modification directions. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 96*, 2235–2243.

Kuo, W. C., Wang, C. C. (2013c). Data hiding based on generalised exploiting modification direction method. *The Imaging Science Journal, 61*(6), 484-490, DOI: 10.1179/1743131X12Y.0000000011

Kuo, W. C., Wang, C. C., Hou, H. C. (2016a). Signed digit data hiding scheme. Information Processing Letters, 116, 183–191.

Kuo, W. C., Kuo, S. H., Wang, C. C., Wuu, L. C. (2016b). High capacity data hiding scheme based on multi-bit encoding function. *Optik, 127*, 1762–1769.

Lee, Y. P., Lee, J. C., Chen, W. K., Chang, K. C., Su, I. J., Chang, C. P. (2012). High-payload image hiding with quality recovery using tri-way pixel-value differencing. *Information Sciences, 191*, 214–225.

Li, B., He, J., Huang, J., Shi, Y. Q. (2011). A survey on image steganography and

steganalysis. *Journal of Information Hiding and Multimedia Signal Processing, 2*, 142–172.

Liao, X., Wen, Q. Y., Zhao, Z. L., Zhang, J. (2012a). A novel steganographic method with four-pixel differencing and modulus function. *Fundamenta Informaticae*, *118*(2012), 281–289. DOI: 10.3233/FI-2012-714

Liao, X., Wen, Q., Zhang, J. (2012b). A Novel Steganographic Method with Four-Pixel Differencing and Exploiting Modification Direction. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, E95-A*, 1189–1192.

Liao, X., Wen, Q., Zhang, J. (2013). Improving the adaptive steganographic methods based on modulus function. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E96-A*, 2731–2734.

Liao, X., Qin, Z., Ding, L. (2017). Data embedding in digital images using critical functions. *Signal Processing: Image Communication, 58*, 146–156.

Liao, X., Guo, S., Yin, J., Wang, H., Li, X., Sangaiah, A. K. (2018). New Cubic Reference Table Based Image Steganography. *Multimed Tools Appl (2018) 77*, 10033–10050. DOI: 10.1007/s11042-017-4946-9

Liu, G., Liu, W., Dai, Y., Lian, S. (2014). Adaptive steganography based on block compl exity and matrix embedding. *Multimedia Systems*, *20*(2), 227–238. DOI: 10.1007 /s00530-013-0313-5

Liu, Y., Qu, X., Xin, G. (2016). A ROI-based reversible data hiding scheme in encrypted medical images. *Journal of Visual Communication and Image Representation, 39*, 51–57. DOI: 10.5121/csit.2012.2211

Mandal, J. K., Das, D. (2012). Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/ Underflow*, Computer Science & Information Technology (CS & IT),* 93–102. DOI:10.5121/csit.2012.2211

Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., Sajjad, M. (2016a). CISSKA-LSB: Color Image Steganography Using Stego Key-Directed Adaptive LSB Substitution Method. *Multimedia Tools Appl (2017), 76*(6), 8597-8626. DOI: 10.1007/s11042-016-3383-5

Nguyen, T. D., Arch-int, S., Arch-int, N. (2015). An adaptive multi bit-plane image steganography using block data-hiding. *Multimed Tools Appl (2017) 76*(6), 8597-8626. DOI: 10.1007/s11042-016-3383-5 1

Pan, F., Li, J., Yang, X. (2011). Image steganography method based on PVD and modulus function. *2011 International Conference on Electronics, Communications and*

Control (ICECC). 282–284. DOI: 10.1109/ICECC.2011.6067590

Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G. (1999). Information hiding - a survey. *Proceedings of the IEEE, 87*(7), 1062–1078. DOI: 10.1109/5.771065

Pevny, T., Bas, P., Fridrich, J. (2010). Steganalysis by Subtractive Pixel Adjacency Matrix. *IEEE Transactions on Information Forensics and Security, 5*, 215–224. DOI : 10.1109/TIFS.2010.2045842

Qazanfari, K., Safabakhsh, R. (2014). A new steganography method which preserves histogram: Generalization of LSB++. *Information Sciences (2014), 277*, 90–101. DOI: 10.1109/TIFS.2010.2045842

Shen, S., Huang, L., Tian, Q., Shen, S. Y., Huang, L. H., Tian, Q. L. (2015a). A novel data hiding for color images based on pixel value difference and modulus function. *Multimed Tools Appl (2015), 74*, 707–728. DOI: 10.1007/s11042-014-2016-0

Shen, S. Y., Huang, L. H. (2015b). A data hiding scheme using pixel value differencing and improving exploiting modification directions. *Computers and Security, 48*, 131–141. DOI: 10.1016/j.cose.2014.07.008

Solak, S., Altınışık, U. (2018). LSB Substitution and PVD performance analysis for image steganography. *International Journal of Computer Sciences and Engineering, 6*, 1–4. DOI: 10.26438/ijcse/v6i10.14

Solak, S., Altınışık, U. (2019). A new approach for Steganography: Bit shifting operation of encrypted data in LSB (SED-LSB). *Bilişim Teknolojileri Dergisi, 12*(1), 75-81. DOI: 10.17671/gazibtd.435437

Solak, S., Altınışık, U. (2019). Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3. *Journal of Electronic Imaging, 28*(4), 043025. DOI: 10.1117/1.JEI.28.4.043025

Solak, S. (2020). High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms. *IEEE Access, 8*, 166513–166524. DOI: 10.1109/ACCESS.2020.3023197

Solak, S., Altınışık, U. (2021). Image Steganography-Based GUI Design to Hide Agricultural Data. *Gazi University Journal of Science, 1*(1). DOI: 10.35378/gujs.703803

Swain, G. (2015). Adaptive pixel value differencing steganography using both vertical and horizontal edges. *Multimed Tools Appl (2016), 75*, 13541–13556 DOI: 10.1007/s11042-015-2937-2

Swain, G. (2016). A Steganographic Method Combining LSB Substitution and PVD in a Block. *Procedia Computer Science, 85*(2016), 39–44. DOI:

10.1016/j.procs.2016.05.174

Thambiraja, E., G., R., Umarani, R. (2012). A Survey on Various Most Common Encryption Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 2*, 226–233.

Tuncer, T., Sönmez, Y. (2019). A Novel Data Hiding Method based on Edge Detection and 2k Correction with High Payload and High Visual Quality. *Balkan Journal of Electrical and Computer Engineering, 7*(3), 311–318. DOI: 10.17694/bajece.573514

URL-1 : https://sipi.usc.edu/database/database.php?volume=misc (Ziyaret tarihi: 16 Ağustos 2022)

Wang, H., Wang, S. (2004). October: Cyber warfare: Steganography vs. steganalysis. *Communications of the ACM, 47*(10), 76-82. DOI: 10.1145/1022594.1022597

Wang, Z. H., Chang, C. C., Li, M. C. (2012). Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences, 192*, 98–108. DOI: 10.1016/j.ins.2010.07.011

Wu, D. C., Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters, 24*, 1613–1626. DOI: 10.1016/S0167-8655(02)00402-6

Wu, K. S., Liao, W. D., Lin, C. N., Chen, T. S. (2015). A high payload hybrid data hiding scheme with LSB, EMD and MPE. The Imaging Science Journal, 63, 174–181.

Xu, W. L., Chang, C. C., Chen, T. S., Wang, L. M. (2016). An improved least-significant-bit substitution method using the modulo three strategy. *Displays, 42*, 36–42. DOI: 10.1016/j.displa.2016.03.002

Yang, C. H., Wang, S. J., Weng, C. Y. (2010). Capacity-raising steganography using multi-pixel differencing and pixel-value shifting operations. *Fundamenta Informaticae, 98*, 321–336. DOI: 10.3233/FI-2010-229

Yang, C. H., Weng, C. Y., Tso, H. K., Wang, S. J. (2011). A data hiding scheme using the varieties of pixel-value differencing in multimedia images. Journal of Systems and Software. *Elsevier, 84*, 669–678. DOI: 10.1016/j.jss.2010.11.889

Zhang, X., Wang, S. (2006). Efficient Steganographic Embedding by Exploiting Modification Direction. *IEEE Communications Letters, 10*, 781–783. DOI: 10.1109/LCOMM.2006.060863

KİŞİSEL YAYIN VE ESERLER

Uzun, M., Solak, S. (2022), Görüntü Steganografisinde Yaygın Kullanılan Veri Gizleme Tekniklerinin İncelenmesi. *Mühendislik Bilimleri ve Tasarım Dergisi, 10*(3), 816-830. DOI: 10.21923/jesd.960733

ÖZGEÇMİŞ

İlkokulu, Samsun'da Karadeniz İlkokulunda bitirdikten sonra hazırlık sınıfını ve eğitim dili İngilizce olan ortaokulu Özel Samsun Kolejinde tamamladı. Liseyi Samsun'da Özel Meralcan Fen Lisesinde burslu olarak okudu ve okul birincisi olarak mezun oldu.

1998 yılında lisans eğitimi için Kocaeli'ye geldi. Kocaeli Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünde Mühendislik eğitimine başladı. Bu süreçte, kendisi de bir depremzede olarak kısıtlı imkanlara sahip öğrencilere 2 yıl boyunca Türkiye Eğitim Gönüllüleri Vakfına bağlı Körfez depremzede prefabriklerinde, gönüllü öğretmen statüsünde Matematik ve Bilgisayar dersleri verdi.

Kocaeli Üniversitesi Bilgi İşlem Daire Başkanlığına, Öğrenci Bilgi Sistemi Yazılımında görev almak üzere Çözümleyici unvanıyla kamu personeli olarak atandı. Unvan Değişikliği Sınavında gösterdiği başarı ile Mühendis kadrosuna geçmeye hak kazandı. 2019 yılında Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Bilişim Sistemleri Mühendisliği bölümünde yüksek lisansa başladı.

Kocaeli Üniversitesince halen kullanılmakta olan Öğrenci Bilgi Sistemi yazılımının birçok kritik modülünde bizzat veya danışman olarak görev aldı. Murat UZUN şimdilerde, Kocaeli Üniversitesi bünyesindeki Bilgisayar Araştırma ve Uygulama Merkezinde Veri Tabanı Yöneticisi olarak iş hayatına devam etmektedir.

Evli ve iki muhteşem kızın babasıdır.