KOCAELİÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ÇİFT GÖRÜNTÜ TABANLI YÜKSEK KAPASİTE VE GÜVENLİĞE SAHİP YENİ BİR TERSİNİR VERİ GİZLEME YÖNTEMİ

GÖKHAN TEZCAN

KOCAELİ 2023

KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ÇİFT GÖRÜNTÜ TABANLI YÜKSEK KAPASİTE VE GÜVENLİĞE SAHİP YENİ BİR TERSİNİR VERİ GİZLEME YÖNTEMİ

GÖKHAN TEZCAN

Doç.Dr. Serdar SOLAK	
Danışman, Kocaeli Üniversitesi	.....
Prof.Dr. Yıldıray YALMAN	
Jüri Üyesi, Piri Reis Üniversitesi	.....
Dr.Öğr.Üyesi Mehmet Zeki KONYAR	
Jüri Üyesi, Kocaeli Üniversitesi	.....

Tezin Savunulduğu Tarih:11.01.2023

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.

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

[x] 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.

Gökhan TEZCAN

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.

Gökhan TEZCAN

ÖNSÖZ VE TEŞEKKÜR

Kocaeli Üniversitesinde yüksek lisans dönemim boyunca değerli bilgilerini benimle paylaşan ve anlattıkları ile bana değer katan, çalışmam sırasında yardımını hiçbir zaman eksik etmeyen, güler yüzünü ve samimiyetini benden esirgemeyen, bana her konuda destek olan ve anlayış gösteren saygıdeğer danışman hocam, Doç.Dr. Serdar SOLAK'a ve yüksek lisans sürecim boyunda bana bolca emeği geçen çalışma arkadaşım Murat UZUN'a teşekkür ederim. Ayrıca Prof. Dr. Yıldıray Yalman ve Dr. Öğr. Üyesi M.Zeki Konyar'a tez jürimde bulunarak vermiş oldukları katkılardan dolayı teşekkür ederim. FBA-2021-2488 numaralı proje kapsamında destek sağlayan Bilimsel Araştırma Projeleri Destek Programına (BAP) teşekkürlerimi sunarım.

Ocak - 2023 Gökhan TEZCAN

İÇİNDEKİLER

ETİK BEYAN VE ARAŞTIRMA FONU DESTEĞİ i
YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI ii
ÖNSÖZ VE TEŞEKKÜR iii
İÇİNDEKİLER iv
ŞEKİLLER DİZİNİ v
TABLOLAR DİZİNİ vi
SİMGELER VE KISALTMALAR DİZİNİ vii
ÖZET viii
ABSTRACT ix
1. GİRİŞ 1
2. GENEL BİLGİLER 3
2.1. Veri 3
2.2. Veri Güvenliği 3
2.3. Steganografi Nedir? 4
2.3.1. Steganografi Tarihi 5
2.3.2. Steganografinin Başarı Ölçütleri 6
2.3.3. Steganografinin Sınıflandırılması 9
2.3.4. Steganografinin Uygulama Alanları 11
2.3.4.1. Görüntü Nedir? 11
2.3.5. Görüntü Steganografisi 12
2.3.6. Tersinir Steganografi Uygulamaları 13
2.3.7. Çift Görüntü Tabanlı Steganografi Yöntemleri 16
2.3.8. Çift Görüntü Tabanlı Steganografi Yöntemlerine Örnekler 17
2.3.8.1. Konum Temelli Çift Görüntü Tekniği 17
2.3.8.2. Merkez Katlama Tekniği 20
2.3.8.3. Üçlü Atama ve Merkez Katlama Stratejisi 21
3. ÖNERİLEN YÖNTEM 25
4. DENEYSEL ÇALIŞMALAR 30
5. SONUÇ 41
KAYNAKLAR 44
KİŞİSEL YAYIN VE ESERLER 49
ÖZGEÇMİŞ 50

ŞEKİLLER DİZİNİ

Şekil 2.1. Alice ve Bob, mahkum problemi 7
Şekil 2.2. Dijital görüntü ve piksel değerleri..... 12
Şekil 2.3. Görüntü Steganografisi Hiyerarşi Şeması 13
Şekil 3.1. Veri Gizleme Akış Şeması 25
Şekil 3.2. n=4 için gizli veri ve piksel değişimlerinin aralıkları 27
Şekil 3.3. Orijinal görüntüyü elde etme ve veri çıkarma akış şeması 27
Şekil 4.1. Deneysel çalışmada kullanılan görüntüler 30
Şekil 4.2. Kapasite ve PSNR ilişkisi 34
Şekil 4.3. N=1 için Lena görüntüsüne ait görüntülerin piksel dağılımları 37
Şekil 4.4. N=2 için Lena görüntüsüne ait görüntülerin piksel dağılımları 37
Şekil 4.5. N=3 için Lena görüntüsüne ait görüntülerin piksel dağılımları 38
Şekil 4.6. Ardışık piksel değerleri farklarının dağılımı 39
Şekil 4.7. N=1-4 için RS analizi sonuçları 40

TABLOLAR DİZİNİ

Tablo 2.1. Piksel çifti kümelerini gösteren çapraz model 18
Tablo 2.2. Veri çıkarma kombinasyonları ve gizli veri değerleri..... 19
Tablo 2.3. Veri çıkarma kombinasyonları ve örtü görüntü piksel değerleri..... 19
Tablo 2.4. k = 3 için katlama örneği..... 20
Tablo 2.5. Üçlü atama için eşleşen değişimler tablosu..... 23
Tablo 4.1. N=1 seviyesi için yüke göre kapasite ve PSNR sonuçları 31
Tablo 4.2. N=2 seviyesi için yüke göre kapasite ve PSNR sonuçları 32
Tablo 4.3. N=3 seviyesi için yüke göre kapasite ve PSNR sonuçları 32
Tablo 4.4. N=4 seviyesi için yüke göre kapasite ve PSNR sonuçları 33
Tablo 4.5. N=5 seviyesi için yüke göre kapasite ve PSNR sonuçları 33
Tablo 4.6. N=1-5 için ortalama kapasite ve PSNR sonuçları..... 35
Tablo 4.7. Ortalama veri gizleme ve çıkarma süreleri 35
Tablo 4.8. Önerilen yöntemin literatürdeki diğer çalışmalarla karşılaştırılması 36
Tablo 4.9. SSIM ölçüm sonuçları..... 38

SİMGELER VE KISALTMALAR DİZİNİ

Kısaltmalar

bpb	: Byte Per Bit (Bayt Başına Düşen Bit Sayısı)
dB	: Desibel
DCT	: Discrete Cosinus Transformation (Ayrık Kosinüs Dönüşümü)
DWT	: Discrete Wavelet Transformation (Ayrık Dalga Dönüşümü)
EMD	: Exploiting Modification Direction (Değişiklik Yönünün Kullanılması)
LSB	: Least Significant Bit (En Az Önemli Bit)
MSE	: Mean Square Error (Ortalama Karesel Hata)
PDH	: Pixel Difference Histogram (Piksel Farkları Dağılımı)
PSNR	: Peak Signal Noise Ratio (Tepe Sinyal Gürültü Oranı)
PVD	: Pixel Value Difference (Piksel Değerleri Farkları)
RS	: Regular and Singular (Düzenli ve Tekil)
SSMI	: Structural Similarity İndex Measure (Yapısal Benzerlik İndeksi Ölçüsü)

ÇİFT GÖRÜNTÜ TABANLI YÜKSEK KAPASİTE VE GÜVENLİĞE SAHİP YENİ BİR TERSİNİR VERİ GİZLEME YÖNTEMİ

ÖZET

Tez çalışması kapsamında, çift görüntü tabanlı tersinir veri gizleme yöntemi önerilmiştir. Önerilen yöntem çift görüntülerin en önemli bitleri ve bu bitlerin sebep olduğu değişikliğin etkisini azaltan merkez kaydırma tekniğini kullanmaktadır. Bu yöntem, yüksek kapasiteli gizli verileri, güvenli bir şekilde gizlemeyi amaçlamaktadır. Yöntem, gizli verileri doğrudan gizlememektedir. Bunun yerine gizli veriden alınan (n+1) bitlik veri kümelerinden her birini ve örtü görüntüsü piksel değerlerinin en önemli n bitiyle birleştirip yeni değerler hesaplar. Bu nedenle, orijinal örtü görüntüsü elde edilmeden gizli verilerin çıkarılması imkansızdır. Ayrıca, ortalama karesel hatayı en aza indirmek için merkez kaydırma işlemi gerçekleştir. Bu işlemden sonra çift görüntülerde gizlenecek semboller $\left[-3 * -2^{(n-1)} + 1, 3 * 2^{(n-1)} - 1\right]$ aralığında olmaktadır. Bu aralık değerindeki gizli semboller ve örtü görüntüsünün piksel değerleri kullanılarak stego görüntülerin piksel değerleri elde edilir. Deneysel çalışmalar sonucunda, yük 2,5 bit/byte (bpb) olduğunda, görsel kaliteyi ifade eden tepe sinyal gürültü oranı değeri (PSNR) 34 (dB) civarındadır. Ek olarak, önerilen yöntemin RS analiz saldırılarına karşı güvenli olduğu kanıtlanmıştır.

Anahtar Kelimeler: Çift Görüntü Steganografisi, En Önemli Bitler, Merkez Kaydırma Stratejisi, Tersinir Veri Gizleme, Veri Güvenliği.

A NEW REVERSIBLE DATA HIDING METHOD BASED ON DUAL IMAGE WITH HIGH CAPACITY AND SECURITY

ABSTRACT

In this study, dual image-based reversible data hiding method is proposed. The proposed method uses the most significant bits and center shift technique, which reduces the change caused by these most significant bits. The proposed reversible data hiding method aims to securely hide high-capacity confidential data. The method does not directly hide confidential data. Instead, it calculates new values by combining each of the (n+1) bit datasets taken from the hidden data and the most significant n bits of the cover image pixel values. Therefore, it is impossible to extract confidential data without obtaining the original cover image. In addition, center shifting is performed to minimize the mean square error(MSE). After this process, the hidden data to be embeded in dual images remains in the range [-3*-2^((n-1))+1,3*2^((n-1))-1]. The pixel values of the stego images are obtained using the secret data and the cover image pixel values in this range. Experimental studies show that when the payload is 2.5 bits/byte, the peak signal-to-noise ratio (PSNR), which indicates the visual quality, is around 34 (dB). It has also been proven that the proposed method is secure against RS (regular and singular) analysis attacks.

Keywords: Dual-İmage Steganography, Most Significant Bits, Center Shifting Strategy, Reversible Data Hiding, Data Security.

1. GİRİŞ

Günümüz dünyasını değiştirip şekillendiren yegâne şey bilgidir. İnsanoğlu bilgi edindikçe, iletişim becerilerini arttırıp topluluklar kurmuş, teknolojisini ilerletip yeni aletler geliştirmiş, yaşam standartların iyileştirmiştir ve yaşadığı gezegene şekil verir hale gelmiştir.

Bu değişimin arkasındaki ana unsur bilginin kendisidir. Yaşadığımız çevredeki olaylar ve gerçekliklerin gözlemlenmesiyle elde edilen bilgi yaratıcı bir şekilde kullanılarak birçok değişik icadın doğuşunu sağlar.

İnsanlığın sahip olduğu bilgi kazanımının artmasıyla birlikte gelişen teknoloji, yuvarlanan bir kar topu misali, verinin elde edilmesini ve işlenmesini de hızlandırmaktadır. Geçen zamanla birlikte elde edilen bu bilginin kullanılabileceği alanlar ve bu alanlara ait dallanmalar da artmaktadır. Bu şekilde veri her geçen gün daha çok önem kazanmakta ve değerlenmektedir.

Bilginin hammaddesi veridir. Veri elde edilmeden ve işlenmeden asla anlamlı bir bütün haline gelemez, bilgi haline getirilemez. Bilgisayarların gelişimi ile ortaya çıkan bilişim dünyasında veri de dijitalleşmiştir. Bu veri günümüzde her yerde ve kolayca ulaşılabilir haldedir. Ancak bilgi ve verinin kaybedilebilmesi, unutulabilmesi ya da kasıtlı olarak imha edilebilmesi ya da kötüye kullanılması da mümkündür. Bazı bilgiler insanlara zarar verecek, kitleleri manipüle edecek, ekonomik dengeleri bozacak vb. niteliğe sahip olabilir. Veri güvenliği de burada devreye girmektedir (Loukides, 2011).

Verinin bozulmadan saklanması, aktarımı sırasında takip edilememesi, erişebilecek kişilerin yetkilendirilmesi ve sınırlandırılması, şifrelenerek anlaşılmaz hale getirilmesi veri güvenliği kapsamına girer (Diffie ve Hellman, 1976).

Gizli ya da az sayıda kişi tarafından bilinmesi gereken bir veri için, güvenilir bir şekilde saklanmasından sonraki kuşkusuz en önemli şey bu verinin üçüncü taraflarca bilinmemesidir. Ancak bu verinin taşınması sırasında devreye iyi veya kötü niyetli olması fark etmeksizin muhakkak üçüncü bir taraf girecektir. Bu üçüncü tarafın art niyeti olmasa bile isteği dışında veri sızdırmayacağının bir garantisi yoktur. Bu nedenle verinin masum görünüşlü başka bir ögenin içine gizlenmesiyle, verinin aktarım yolu ve bu yol üzerindeki

kontrol noktalarının aslından farklı bir görünüme sahip olan ögeyi taşıdıkları yönünde kandırmak gerekebilir. Verinin bu şekilde gizlenmesine steganografi (Gizli Yazı) denir (Johnson, 1998).

Bu tez çalışmasında çift görüntü tabanlı steganografi yöntemleri için yeni bir yaklaşım önerilmiştir. Önerilen veri gizleme yönteminde şunlar sağlanmıştır;

- Önerilen teknikte veri gizleme ve çıkarma işlemleri tamamen kayıpsız olarak yapılabilmektedir.
- Önerilen teknik, sınır düşmesi probleminin çözülmesini sağlar.
- İki adet stego görüntüyü üçüncü şahıslar tarafından ele geçirilse dahi orijinal örtü görüntüyü oluşturulmadan gizli veriye ulaşılamaz.
- Tersine çevrilebilir veri gizleme algoritması, mevcut benzer algoritmalara göre daha yüksek gizli veri taşır.
- Önerilen teknik deneysel sonuçlara göre RS analiz tekniğine dirençlidir.

Tez çalışmasının ilerleyen bölümleri şu şekilde düzenlenmiştir. Bölüm 2'de veri, bilgi ve steganografi hakkında genel bilgiler verilmiştir. Devamında çift görüntü tabanlı steganografi yöntemlerine örnekler verilmiştir. Bölüm 3’te Önerilen çift görüntü tabanlı tersinir veri gizleme tekniğinin nasıl çalıştığı açıklanmıştır. Önerilen algoritmayı değerlendirmek için deneysel sonuçlar ve karşılaştırmalar Bölüm 4’te verilmiştir. Son olarak, sonuç Bölüm 5'te sunulmuştur.

2. GENEL BİLGİLER

2.1. Veri

Veri, bilginin ham halidir. Veri, bilgi edinmek amacıyla gerçeklikten elde edilen, gerçekliğin bir alt kümesidir. Bilgi ise insanların düşüncelerini, deneyimlerini ve dünyayı anlamalarını sağlayan, anlamlı ve kullanışlı veriler topluluğudur. Bilgi, insanların kararlar alabilmeleri ve daha verimli çalışabilmeleri için gereklidir (Garcia ve diğ. 2016). Veriden bilgi elde etmek, verilerin işlenip anlamlı bir biçimde sunulmasına dayalı bir süreçtir. Veri işlendiğinde karar verici açısında yol gösterici nitelik kazanır. Bu işlemler toplamak, gruplandırmak, özetlemek vb. şeklindedir. Ancak veri tek başına hiçbir anlama sahip değildir. Verinin faydalı olabilmesi için ona bir anlam kazandırılması ve yorumlanması gerekir.

Veri, bir olayın veya nesnenin özelliklerini tanımlayan sayısal veya alfa sayısal bir ifadedir. Örneğin, bir kişinin adı, yaşı, cinsiyeti gibi bilgileri veri olarak ifade edilebilir. Veri, birçok alanda kullanılabilir ve önemi farklı nedenlerle vardır. Örneğin, bir sağlık kuruluşu tarafından toplanan hasta verileri, doktorların hastalarını daha iyi anlamalarını ve tedavi etmelerini sağlar. Ayrıca, bir şirket tarafından toplanan müşteri verileri, şirketin pazarlamasını ve satışlarını daha etkili bir şekilde yapmasını sağlar. Genel olarak, veri önemlidir çünkü insanların ve kuruluşların daha bilinçli kararlar alabilmeleri ve daha verimli çalışabilmeleri için gereklidir (Runker, 2020).

Veri, bilgi işleme için ihtiyaç olan kaynaktır. Bilginin elde edilebilmesi için veririn elde edilmesi ve işlenmesi gerekmektedir. Bu veri çeşitli semboller, harfler, işaretler, sayılar vb. ile temsil edilen henüz işlenmemiş halde bulunan izlenimler ya da gerçeklikler olarak ifade edilebilir. Nicel ya da mantıksal her türlü değer bir çeşit veridir.

2.2. Veri Güvenliği

Veri güvenliği, verilerin güvenli bir şekilde saklanması, korunması ve kullanılmasını sağlayan bir kavramdır. Veri güvenliği, verilerin yanlış kişilere veya kuruluşlara ulaşmamasını, değiştirilmemesini veya silinmemesini sağlar. Bu sayede, verilerin güvenliği ve bütünlüğü korunarak insanların ve kuruluşların güvenli bir şekilde erişebileceği ve kullanabileceği bilgi elde edilir. Bu, verinin yanlış kişilere veya kötü amaçlı yazılımlara karşı korunması gerekir. Genellikle bir veri güvenliği yönetim sistemi

kullanılarak gerçekleştirilir. Bu sistem, verilerin nasıl saklanacağı, kimlerin erişebileceği ve nasıl korunacağı gibi konuları düzenler ve izler. Veri güvenliği, özellikle kişisel verileri içeren bilgilerin korunması açısından önemlidir, ancak genel olarak tüm verilerin korunması için önemlidir. Veri güvenliği, verilerin fiziksel, dijital ve hukuki açıdan korunmasını içerir. Örneğin, verilerin fiziksel olarak güvenli bir ortamda saklanması, dijital olarak parola koruması ve şifreleme ile korunması ve hukuki olarak yasal haklarının korunması veri güvenliği için gereklidir (Zhang, 2018).

Veri güvenliği, bilgi veya veriye yetkisiz kişilerce erişilmesinin ve kullanılmasının önüne geçmek için gizlilik, bütünlük ve erişebilirlik ana işlevlerini yerine getirmesi gerekir (Sun ve diğ., 2014). Bu kapsamda;

- Erişebilirlik: Yetkili kişilerin bilgiye ihtiyaç duyulduğunda, ona ulaşabilip kullanmasıdır.
- Bütünlük: Bilginin bir arıza, kaza, eskime veya yetkisiz müdahale tarafından değiştirilmemesi için alınan önlemdir.
- Gizlilik: Bilginin yetkisiz kişilerce bilinmemesi ve elde edilememesi için alınan önlemlerdir.

2.3. Steganografi Nedir?

Steganografi kelimesi antik Yunancadaki gizlenmiş, örtülü, ya da korunmuş anlamına gelen “Steganos” ve yazı anlamına gelen “Graphein” kelimelerinin birleşmesi ile oluşur ve gizlenmiş yazı anlamına gelmektedir. Uygulamada veri gizleme olarak kullanılır (Şahin ve diğ., 2006).

Steganografi, bir mesajın gizli bir şekilde içerdiği bilgiyi saklamak için kullanılan bir tekniktir. Steganografi, gönderilen mesajın içeriğini değiştirmez veya mesajın gönderilme biçimini değiştirmez, ancak mesajın görünüşünü değiştirerek bilginin gizliliğini sağlar. Örneğin, bir görüntü dosyasında gizli bir mesaj saklanabilir ve görüntü dosyası görüntülenirken bu mesaj göz ardı edilebilir. Ancak bu mesajın varlığını bilen birisi tarafından okunabilir. Bu teknik, mesajların güvenli bir şekilde iletilebilmesi ve gizliliğinin sağlanması için kullanılır (Solak ve Altınışık, 2019).

Steganografi iki ana aşamada gerçekleştirilir. Bu aşamalar gizleme (gömme) ve çıkarma işlemleridir. Steganografide ilgili veriyi taşımsı için taşıyıcı bir araca ihtiyaç duyulur.

Gizli mesajı içeren bu nesneye örtü(cover) nesnesi denir. Bu örtünün içinde gizlenen ögeye ise stego(gizli) nesne denir. Steganografinin amacı örtü nesnenin içine maksimum miktarda veriyi saklayıp, verinin fark edilmeden alıcıya iletilmesidir. Ardından mesajın alıcıya iletilmesiyle verinin örtü nesne üzerinden çıkarılması süreci başlar.

Steganografi ve şifreleme genellikle birbiriyle birlikte kullanılır çünkü bu teknikler birbirlerini tamamlayıcıdır. Örneğin, bir görüntü dosyasında gizli bir mesaj saklanarak steganografi kullanılabilir, ancak bu mesaj hala görülebilir ve okunabilir. Bu nedenle, bu mesajın güvenliğini sağlamak için şifreleme kullanılabilir. Böylece, mesajın anlamını sadece şifre çözme yöntemini bilen birisi anlayabilir. Bu iki teknik birbiriyle birlikte kullanıldığında, mesajın gizliliği ve güvenliği hem steganografi hem de şifreleme sayesinde sağlanır.

Şifrelemeden farklı olarak steganografi, verinin üçüncü taraflarca fark edilmesinin önüne geçmeye çalışır. Şifreleme ise veriyi ele geçiren üçüncü taraf kişilerin verinin içeriğini anlayamamasını amaçlar. Saklanan hiçbir nesnenin fark edilemez olmaması gibi hiçbir şifreleme yöntemi de kırılamaz değildir. Bu yüzden steganografi ve şifreleme genellikle bir arada kullanılarak güvenlik seviyesi arttırılmaya çalışılır.

2.3.1. Steganografi Tarihi

Steganografi insanların yazılı olarak gönderebilecekleri mesajların okunamamasını sağlama ihtiyacına yönelik ortaya çıkmıştır. Steganografinin tarihteki yazılı en eski kaynağı Yunan yazar Heredot'un eserinde yer almaktadır. Heredot eserinde iki olaydan bahseder. Eski Yunanistan'da insanlar tabletlerin üstüne yazdıkları mesajların üzerini bal mumuyla kaplarlardı. Bu şekilde yüzeyi işlenen tabletler kullanılmamış tabletlere benzerdi. Mum eritildiğinde ise tabletin üzerine işlenen metin ya da desen ortaya çıkardı (Şahin ve diğ., 2006).

Heredot'un eserinde bahsettiği bir diğer olay ise Antik Yunanistan'ın Pers imparatorluğu ile savaştığı dönemde Histiaeus'un Milet'e gönderdiği mesajdır. Pers imparatorluğu bazı Yunan devletlerini ele geçirmiştir. O sırada Milet'in Yöneticilerinden Histieaus, bugün İran sınırlarında yer alan Susa'ya gönderilmiştir. Yerinde ise Aristagoras geçirilmiştir. Histiaeus Milet'e geri dönmek istemektedir ve bu nedenle sadık kölesinin saçlarını kazıtıp

Aristagoras'tan isyan başlatmasını isteyen bir metni kölesinin kafasına yazmıştır. Kölenin saçları tekrar uzadıktan sonra mesaj gizlenmiştir ve dikkat çekmeden ulaştırılmıştır.

Steganografinin tarihteki bir başka kullanımı ise görünmez mürekkepler şeklindedir. Düz bir kâğıt üzerine gün ışığında gözükmeyen bir mürekkeple iletilmek istenen mesaj yazılmakta ve bu mesaj morötesi ışığa tutulduğunda, üstene asidik çözelti döküldüğünde veya ısıya maruz bırakıldığında kendini göstermektedir (Stefan ve Fabien, 2000).

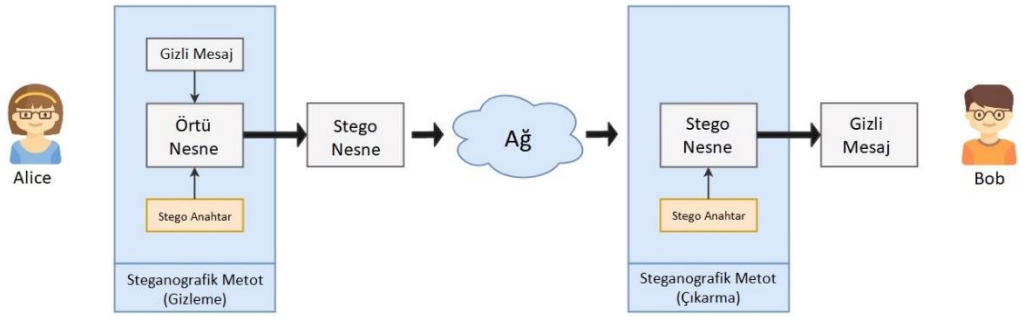
İkinci dünya savaşı zamanlarında fotoğrafçılığın gelişmesiyle birlikte mikro noktalama tekniği ortaya çıkmıştır. Metindeki karakter boyutları yüzlerce kat küçültülerek nokta boyutuna indirgenir. Gazete ve dergi gibi baskılı taşıyıcılar üzerine yerleştirilerek gönderilir. Mesaj insan gözüyle algılanamayacak kadar küçük olduğu için dikkat çekmez. Okunması için mercek kullanmak gerekir (Zhao ve Koch 1995).

Yine dünya savaşında kullanılan bir başka yöntem boş şifrelemedir. Bu yöntemde alakalı olmayan bir metnin içine mesaj gizlenir. Bu metin öyle bir şekilde hazırlanır ki metindeki her kelimenin baştan belirli bir sıradaki harfi alındığında aslında iletilmek istenen mesaj ortaya çıkmaktadır (Khan ve Gutub, 2007).

2.3.2. Steganografinin Başarı Ölçütleri

Bir uygulamanın başarılı olmasının en önemli şartı asıl amacını yerine getirmesidir. Dolaysıyla steganografinin başarı ölçütleri de bu amaç doğrultusunda şekillenir. Ayrıca kullanılacağı şartlara bağlı olarak ek başarım ölçütleri de var olabilir.

Steganografinin asıl amacı veriyi gizlemek olduğu için en önemli başarı ölçütü fark edilmezliktir. Steganografide fark edilmezliğin tasviri için genellikle Alice ve Bob'un mahkum problemi gösterilir. Bu problemde Alice ve Bob adında iki mahkumun birbiriyle iletişim kurması gerekmektedir. İki mahkum arasındaki iletişim, gardiyan Wendy aracılığıyla sağlanabilmektedir ve mahkumların birbirine gönderdiği mesajların Wendy tarafından fark edilmemesi gerekmektedir. Bu nedenle Alice ve Bob birbiriyle olan iletişimi steganografi kullanarak hazırlanmış mesajlar sayesinde gardiyandan gizlemektedirler (Yalman ve Ark, 2014).



Şekil 2.1. Alice ve Bob, mahkum problemi

Bunun için iyi bir steganografi yönteminin, verinin gizlendiği ortamda üzerinde mümkün olan en küçük bozulmaya sebep olması gerekir. Sadece küçük bozulmalara sahip olmak her zaman yeterli olmayabilir. Bu bozulmaların çok düzenli aralıklarla gerçekleşmesi bile fark edilme sebebi olabilir. Fark edilmezlik sadece örtü nesne üzerinde değil aktarma ağı üzerinde de uygulanabilmelidir. Benzer nitelikteki mesajların sürekli olarak aynı aktarım ağı üzerinde taşınması kuşku uyandırabilir. Bu yüzden mümkün olduğunca küçük alana mümkün olan en yüksek miktardaki verinin gizlenmesi gerekir. Bu şekilde en az sayıda örtü nesne kullanılarak aktarım sırasındaki fark edilme riski azaltılır. Bu da birim alan başına gizlenen verinin önemini ortaya çıkartır. Tabiki de başarım kıstasları bunlarla kısıtlı değildir. Gizlenen verinin bir yerde muhafaza edilmesi gerekmekteyse bozulmadan uzun süre boyunca muhafaza edilebilmesi gerekir. Ayrıca aktarma sırasında aktarım organlarının yapısına bağlı olarak örtü nesnenin uğrayabileceği deformasyonlardan gizlenen verinin etkilenmemesi gerekir.

Ayrıca steganografinin bir de veri çıkarma işlemi vardır. Bu işlem sırasında en önemli ölçüt ise verinin bozulmadan birebir çıkartılabiliyor olmasıdır. Tabi ki bu da şartlara bağlıdır. Örneğin gizlenen veri bir yazılım koduna ait parça ise noktası noktasına doğru olması gerekirken, bu veri bir şekil içeren görüntü dosyasıysa çıktı görüntüde şeklin ana hatlarının anlaşılması engellemeyecek kadar bir bozulma kabul edilebilir. Yine şartlara bağlı olarak örtü nesnenin gerek maliyet gerek çevresel kısıtlamalar sebebiyle olsun tekrar tekrar kullanılması gerekiyorsa bu örtü nesnenin veri gizlemesinden önceki haline çevrilebilmesi de bir başarı ölçütü olur (Hamid ve diğ., 2021).

Yani bir steganografi yönteminin başarılı olabilmesi için, verinin gizlendiği ortamın içinde en az miktarda bozulmaya sebep olması, bu bozulmaların rastgele gözükmesi,

birim alana maksimum miktarda veriyi saklayabiliyor olması, saklanan verinin saklandığı sürece bozulmaması, örtü üzerinde yapılan değişikliklerden veya örtüde meydana gelen bozulmalardan etkilenmemesi, gizlenen verinin eksiksiz şekilde çıkarılabilmesi ve örtü nesneye zarar vermemesi gerekir. Bunlara ek olarak uç seviyedeki kullanıma bağlı olarak daha birçok şartı getirmesi gerekebilir. Örneğin gigabaytlar hatta terabaytlar boyundaki bir dosyanın taşıması sırasında saklanabilen veri kapasitesinin dışında bu verinin gizlenmesi ve çıkarılması sırasında geçen süre de başarı ölçütü olabilir. Ya da verini içerdiği bilginin belirli bir zaman aralığı için geçerli olduğu bir senaryoda, gizlenen verinin varlığı fark edildiğinde, gizlenmiş veriyi ele geçiren kişi için verinin nasıl çıkarılacağının algılaması için gereken zaman ne kadar çoksa, bilginin işlevini yitirmiş olma olasılığı o kadar yüksek olur (Habibi ve diğ. 2011).

Günümüzde steganografi uygulamalarının daha çok bilgisayarlar ile teknik yöntemler kullanılarak yapılması nedeniyle, steganografinin başarımını ölçmek için analitik ölçütler geliştirilmiştir. Kapasite başarımını ölçmek için piksel ya da bayt başına gizlenen bit miktarı(bpb) gibi birimlerle alana gizlenen verinin ölçümü başarımı ifade edilir.

Örtü görüntüdeki değişimden kaynaklanan gürültüyü ölçmek için, örtü ile stego öge arasındaki ortalama karesel hatadan (MSE- Mean Square Error) faydalanılır. Ortalama karesel hatanın kullanılan değer aralıklara göre yanıltıcı olabilmesi sebebiyle, değer aralığının karesinin ortalama karesel hataya olan oranının logaritması alınması ile bu ifade daha okunaklı hale getirilir. Ortalama karesel hatanın daha anlaşılır olan bu ifadesine tepe sinyal gürültü oranı (PSNR – Peak signal to noise ratio) denir (Huynh-Thu ve Ghanbari, 2008). Ortalama karesel hatanın PSNR'a dönüştürülmesi Denklem 2.2'de verilmiştir.

$$MSE = \frac{1}{H\ x\ W} \sum_{i=1}^{H} \sum_{j=1}^{W} (C(i,j) - S(i,j))^2 \quad (2.1)$$

$$PSNR = 10\ x\ log_{10} \frac{255^2}{MSE} \quad (2.2)$$

Kullanılan bir başka analitik yöntem ise yapısal benzerlik indeksi ölçüsüdür (SSIM-Structural similarity index measure). Tepe sinyal gürültü oranının aksine örtü ve stego ögelerin farkını değil, birbirine ne kadar benzediklerini ölçmeye dayanır (Setiadi, 2021). SSIM'nin hesaplanması için denklem 2.3 kullanılır.

$$SSIM = \frac{(2\mu_x\mu_y+C_1)*(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)*(\sigma_x^2+\sigma_y^2+C_1)} \quad (2.3)$$

Geliştirilen bir başka ölçüm yöntemi ise örtü ögenin histogramlarını veya dağılımlarını çıkartmaktır. Bu işlem sayısal olduğu kadar görsel bir yöntemdir. Burada gizli veriyi taşıyan nesnenin sayısal değerler, bu sayısal değerlerin farkları ya da mutlak farkları veya değerlerin modlarına karşılık gelen değerleri gibi pek çok farklı şekilde bu değerlerin kaçar kere gözlemlendiği görselleştirilerek histogram dağılımları çıkartılır. Çıkartılan bu dağılımlarda çift ortalamalı bir dağılım, taraklanma, belirli aralıklarla basamaklanma, normal, poisson, pearson, logaritmik, beta… gibi herhangi bir dağılıma benzeyen (Evans ve diğ. 2011) ama dağılımın sürekliliğini aşırı derecede bozan anormallik durumları analitik ya da sezgisel olarak incelenerek sıra dışı bir davranış sergileyip sergilemediğine bakılır.

Bu yöntemler aynı zamanda birer steganaliz yöntemleridir. Steganaliz, gizlenmiş bir mesajı bulma ve okuma işlemine verilen genel bir isimdir. Bu işlem genellikle bir görüntü veya ses dosyasının içinde bulunan gizli bir mesajı tespit etme ve okuma işlemi olarak da tanımlanabilir (Sallie, 2005).

En sık kullanılan steganaliz yöntemlerinden birisi de düzenli ve tekil (RS) analizidir (Wang ve diğ. 2010). RS analizi, steganaliz için uyarlanan istatistiksel bir yaklaşımdır. Bir veri dosyasının bir kısmının korelasyonunu kullanarak gizli bir mesajın varlığını tespit etmeyi amaçlar. Bu, veri dosyasının belirli bir bölümünün benzer bir bölümüyle kıyaslanmasıyla gerçekleştirilir. Eğer veri dosyasında bir gizli mesaj varsa, bu bölümler arasındaki korelasyon düşük olacaktır ve bu, bir gizli mesajın varlığına işaret eder. Eğer veri dosyasında bir gizli mesaj yoksa, bu bölümler arasındaki korelasyon yüksek olacaktır ve bu, veri dosyasında bir gizli mesajın bulunmadığını gösterir.

2.3.3. Steganografinin Sınıflandırılması

Bir verinin gizlenmesinde, kullanım yeri ve amaçları çok çeşitli olduğundan pek çok açıdan sınıflandırılabilir. En yaygın kabul edilen sınıflandırmaya göre steganografi dilbilimsel ve teknik steganografi olmak üzere ikiye ayrılır (Kaur ve diğ. 2014).

Dilbilimsel steganografisi verinin gizlenmesi için dilbilimini kullanan steganografi türüdür. Genellikle metin üzerinde kullanılır. Dilbilimsel steganografi kendi içinde üç alt dala ayrılır.

- Açık Alan Yöntemleri: Genellikle metinlerdeki açık alanları kullanan yöntemlerdir. Kelime veya noktalama işaretlerin arasındaki boşlukların büyüklükleri, satır sonralında bırakılan boşlukların miktarı, satırların arasındaki boşlukların mesafesi ve benzeri yöntemler açık alan yöntemleri olarak gruplandırılır.
- Yazımsal Yöntemler: Bir ifadenin farklı yazım şekilleri kullanılarak kodlama yapılır.
- Anlamsal Yöntemler: Bir takım seçilmiş eş veya benzer anlamlı sözcükler her biri farklı bir değere karşılık gelecek şekilde kodlanarak, gizli mesaj metin içerisine gizlenir.

Teknik steganografi, mesajı gizlemek için bir araç, cihaz veya yöntemin kullanıldığı steganografi yöntemidir. Bazı teknik steganografi türleri şu şekildedir.

- Görünmez mürekkep: Saklanmak istenen mesajın sadece mor ötesi veya aşırı yoğun ışıkta gözüken mürekkep kullanılarak boş bir kâğıda veya satır aralarına yazılmasıyla uygulanır.
- Gizli yerler: Gizli verinin kimsenin göremeyeceği yerlerde saklanması.
- Mikrodot: Mikrodot bir sayfanın birkaç yüz mikron boyutunda basılmasına imkân sağlayan fotoğrafçılık biçimidir. Mikrodot, modern dünyada otomobilleri ve diğer motorlu araçları benzersiz bir şekilde tanımlamak için kullanılıyor. Günümüzde mikro noktanın bir DNA zincirine bağlanma potansiyeli bile bulunmaktadır.
- Bilgisayar Tabanlı Yöntemler: 1990'lar boyunca bilgisayar teknolojilerindeki gelişmelerle birlikte ortaya çıkmıştır. Steganografi yöntemlerinin en yenisidir ve bilgisayar ortamında çok etkilidir.

Steganografinin bir başka sınıflandırma yöntemi ise kullanılan ortama göre yapılmaktadır. Buna göre steganografi başlıca dört bölümde sınıflandırılır.

- Metin steganografisi: Taşıyıcı olarak metnin kullanıldığı steganografi türüdür. Veri gizlemek için metin üstünde göze batmayacak düzenlemeler yapılır veya metin yazılırken gizlenecek mesaja göre oluşturulabilir. Bir mesajı uzun bir metinde belirli

harfleri sıralayarak, kelimeler arası boşluk uzunluklarını değiştirerek, noktalama işaretlerini değiştirerek veya cümlelerin kelime sayıları ile şifreleyerek saklamak mümkündür. Dilbilimsel steganografisi kendi içinde birçok dala ayrılabilir

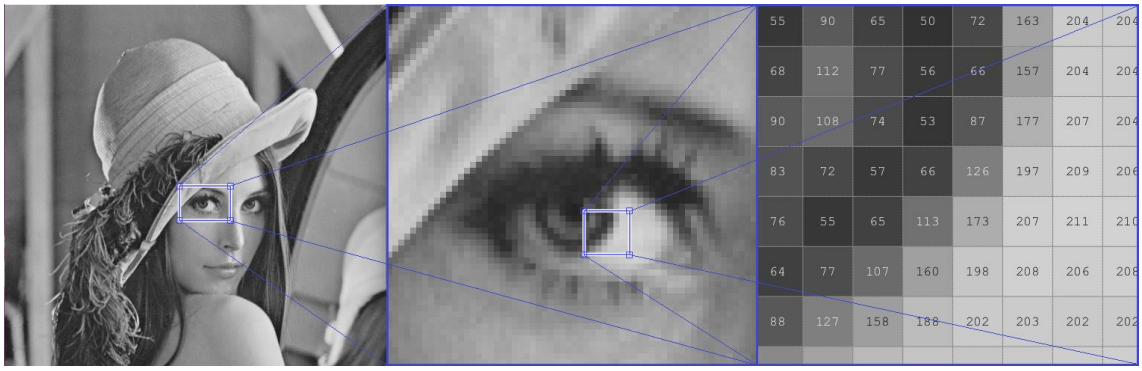
- Ses Steganografisi: Gizli mesaj ses dosyalarının ikili dizilerinin içine gömülüdür. Bilginin; ses üzerine parazit şeklinde işlendiği basit algoritmalar veya karmaşık frekans fonksiyonları kullanan bir çok yöntemi bulunmaktadır.
- Görüntü Steganografisi: Verinin gizlenmesi için görüntü dosyalarının kullanıldığı steganografi türüdür.

2.3.4. Steganografinin Uygulama Alanları

Steganografi hemen hemen her alanda ve ortamda kullanılabilir. Steganografinin kullanım çeşitliliği insanoğlunun yaratıcılığı ve hayal gücüyle kısıtlıdır. Sanal veya gerçek her ortamda bir steganografinin kullanılması mümkündür. Steganografi, genellikle güvenlik amaçlı olarak kullanılan bir teknik olduğu için verinin kullanıldığı her sektörde steganografiye ihtiyaç duyulmaktadır. Günümüzde İnternetin gelişmesi ile bilgi akışı dijital olarak gerçekleştirilmeye başlamıştır. Veri ve bilgiler daha çok dijital olarak üretilmeye, dijital olarak aktarılmaya ve dijital olarak tüketilmeye başlamıştır. Verinin dijitalleşmesiyle birlikte steganografi teknikleri de dijital dünyaya uyarlanmaya başlamıştır ve normal hayatta olduğu gibi bilgisayarlar üzerinde de yaygın kullanılır hale gelmiştir. Görüntü, yazı, ses, video, metin dosyası ve akla gelebilecek her türlü bilgisayar dosyası veri gizlemek için farklı şekillerde kullanılmaya başlanmıştır. Hatta çalışan programların kaynak kodlarında bile gizlenmiş verilere denk gelmek mümkündür.

2.3.4.1. Görüntü Nedir?

Görüntü, bir ortamda gözle algılanabilen ışık veya radyo dalgalarının bir yansımasıdır. Görüntü, gözümüz tarafından algılanan bir dizi noktadan oluşur ve bu noktaların yerlerine göre bir görüntü oluşturur. Dijital görüntü, bir ortamda gözle algılanabilen ışık veya radyo dalgalarının bir yansımasını dijital olarak saklayan bir veridir (Castleman, 1996). Dijital görüntü, bir dizi pikselden oluşur ve bu piksellerin değerlerine göre görüntü oluşturulur. Piksel, bir görüntünün en küçük birimi olarak kullanılır ve her bir piksel, bir renk ve parlaklık değerine sahiptir. Dijital görüntüler, fotoğraf veya video gibi farklı ortamlarda saklanabilir ve bu ortamlarda görüntünün içeriği de farklılık gösterebilir.



Şekil 2.2. Dijital görüntü ve piksel değerleri

2.3.5. Görüntü Steganografisi

Günümüzde Bilgisayar ortamında steganografi daha büyük alana sahip olması ve dosya üzerinde yapılan ufak oynamaların görünürde büyük değişikliklere sebep olmaması nedeniyle daha çok görüntü dosyaları üzerinde gerçekleştirilmektedir.

Görüntü steganografisi, görüntüler üzerinde gizli bir biçimde veri saklama tekniğidir. Bu teknik, bir görüntünün kalitesini ve görünümünü değiştirmeden gizli bilgileri içerebilir. Görüntü steganografisi, birçok farklı yöntemle gerçekleştirilebilir ve genellikle güvenlik amacıyla kullanılır. Bu sayede, gizli bilgilerin üçüncü kişiler tarafından görülmesi veya okunması engellenir.

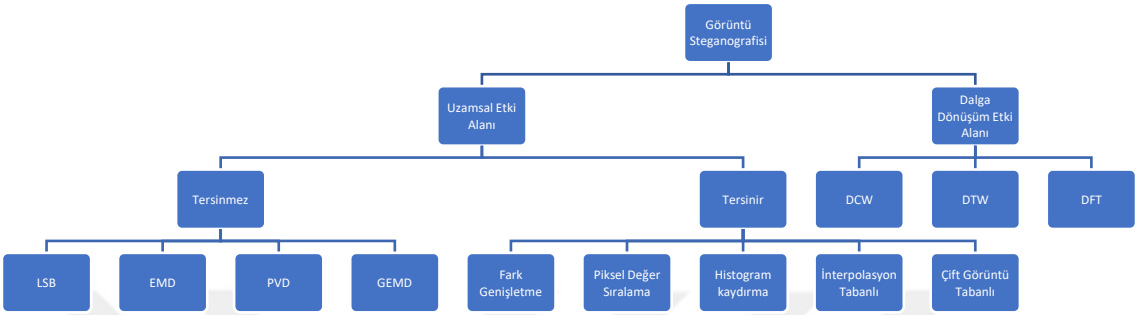
Görüntü steganografisi kendi içinde alanına ve geri dönüşebilirliğine göre ikiye ayrılır.

Veri gizleme ve çıkarma işlemleri yapıldıktan sonra, örtü nesne kusursuz şekilde geri elde edilebiliyorsa bu tarz steganografi yöntemlerine tersinir yani geri dönüştürülebilir steganografi yöntemleri denir. Ancak bu işlemler sonrasında verinin taşındığı örtü nesne üzerindeki değişiklikler kalıyorsa ve örtü nesne ilk haline geri döndürülemiyorsa tersinmez yani geri dönüşümsüz steganografi yöntemi olarak adlandırılır (Lu ve Vo, 2020).

Kullanılan alana göre ise, Uzamsal Etki Alanı (Spital/Image domain) ve Dalga Dönüşüm Alanıdır. Dalga Dönüşüm Alanı yöntemleri kosinüs dalgalarıyla (Zhang ve diğ. 2018) sıkıştırma işlemi yapan .jpeg gibi dosya formatlarının dalga frekanslarının ağırlıkları üzerinde değişiklik yapılarak gerçekleştirilir. Daha çok DCT (Ayrık Kosinüs Dönüşümü- Discrete Cosine Transform) ve DWT (Ayrık dalgacık dönüşümü- Discrete Wave Transform) olarak karşımıza çıkar (Gutub ve Al-Shaarani, 2020). Uzamsal Etki Alanı

yöntemlerinde Piksel değerleri, piksel değerleri farkları veya piksel değerlerinin sıklıkları üzerinde değişiklik yapılarak veri gizleme işlemi gerçekleştirilir.

Uzasal etki alanını yöntemleri de kendi içinde kullanılan görüntü sayısına veya kullanılan metodolojiye göre sınıflandırılmaktadır.



Şekil 2.3. Görüntü Steganografisi Hiyerarşi Şeması

Uzamsal etki alanı yöntemleri içinde en yaygın kullanılan yöntem en küçük bitler (LSB-Least-significant bit) yöntemidir (Neeta ve diğ. 2006). LSB'de bir görüntü dosyasındaki her bir pikselin RGB (renkli) veya gri tonlu katmanındaki değerin sondan "n" adet biti silinerek, bu bitlerin yerine gizlenecek veriden alınan n adetlik bit parçası yerleştirilir. Daha sonra her pikseldeki son "n" Adet bitler alınır tekrar sıralanarak örtü görüntü içine gizlenen veri elde edilir. Bu yöntemde son bitlerin silinmesi nedeniyle görüntü orijinal haline geri çevrilemez. Dolayısıyla LSB yöntemi tersinmez yöntemlere bir örnektir.

Bir başka uzamsal etki alanı yöntemi ise değişiklik yönünün kullanılmasıdır (EMD-Exploiting Modification Direction). EMD algoritması 2n+1 sayı sistemindeki n bitişik piksele veri gizlemektedir. Bu n pikselden sadece bir pikselin değeri bir birim değiştirilerek veri gizleme işlemi gerçekleştirilir. EMD algoritmasının küçük değişikliklerle veri gizlemesi onların fark edilirliğini minimalize etse de gizlenen veri miktarı da az olmaktadır (Hajizadeh ve diğ., 2013).

2.3.6. Tersinir Steganografi Uygulamaları

Bir steganografi uygulamasının tersinir olması, verinin gizlendiği örtü nesne ne olursa olsun, veri çıkartıldıktan sonra bu örtü nesnenin ilk haline geri dönüştürülebiliyor olması gerekmektedir (Lu ve Vo, 2020).

Uzamsal etki alanındaki tersinir yaklaşımlardan birisi fark genişletme uygulamalarıdır. Fark genişletme algoritması ardışık iki pikselin arasındaki farklara odaklanır. Genellikle piksel farkı iki katına çıkarılarak bu farkın üzerine bir bitlik veri gizlenir. Gizlenen bu bir bitlik veri teklik ve çiftlik üzerine dayandığı için kolayca geri okunabilir. Ayrıca ikiye çarpılarak uygulanmış fark genişletme işlemi tekrar ikiye bölündüğünde eklenen bir bitlik veri tam sayıya yuvarlama sırasında yok olacağı için gizlenen veri dışında verinin gizlendiği örtü görüntü de ilk haline geri dönüştürülebilir. Bu nedenle fark genişletme algoritması tersinir bir veri gizleme algoritması olarak sınıflandırılabilir.

İlk örneği 2003 yılında Tian tarafından önerilen fark genişletme yöntemi, bir biti gizlemek için iki örtüşmeyen piksel arasındaki farkın genişletilmesi olarak bilinir. Bu yöntemde kapasite ve stego görüntünün görsel kalitesi düşüktür ve sınır sorunu vardır (Tian, 2003). Düşük hesaplama karmaşıklığı nedeniyle, küçük bir veri miktarını gizlemek için geri dönüşümlü yöntemler arasında tercih edilebilir. Bu yöntemde görsel kalite ve kapasiteyi artırmak için literatürde birçok çalışma bulunmaktadır. Li ve arkadaşları piksel karmaşıklıklarını kaba ve düz parçalara ayıran bir adaptif veri gizleme yöntemi sunmuştur (Li ve diğ., 2011). Ayrıca, bu çalışma, farklı sınıflandırma sonuçlarına göre gömülü piksel tahmini hata ve gömülü gizli veri miktarını kararlaştırmıştır. Gui ve arkadaşları karmaşıklık türlerini artırarak tahmin hata gömme kapasitesini arttırarak Li'nin yöntemini gelişirmiştir (Gui ve diğ., 2014).

İkinci bir yaklaşım, interpolasyon yöntemidir. İnterpolasyon temelli steganografi yöntemleri örtü görüntüdeki piksellerin arasında orijinal pikselleri koruyacak şekilde istatistiksel genişletme (yukarı ölçekleme) uygulanarak, bozulma konusunda tereddüt etmeden harcanabilecek yeni piksellerin oluşturulmasına dayanır (Jung ve diğ., 2009), (Hu ve Li, 2015), (Malik ve diğ. 2020), (Hassan ve Gutub, 2020), (Yang ve diğ. 2017), (Lu ve Huang, 2021). Bu şekilde aslında tersinir olmayan yöntemler bu pikseller üzerinde uygulandığında orijinal görüntüye ait pikseller korunmuş olur. Çıkarma işleminde orijinal pikseller haricindeki pikseller silindiğinde görüntünün ilk hali birebir geri elde edilir.

Tersinir veri gizlemedeki üçüncü yaklaşım türü histogram kaydırma yaklaşımıdır (Tsai ve diğ. 2009). Histogram kaydırma yönteminde piksel değerlerinin veya piksel değerleri farklarının dağılımlarından faydalanan yöntemleridir (Zhao ve diğ.,2011). Burada piksel değerlerinin veya piksel değerleri farkları histogramlarında belirlenen bir veya birkaç

değer sınır alınıp bu sınırların dışında kalan değerler bir miktar kaydırılarak histogram üzerinde boş değerler oluşturulur. Veri oluşturulan bu boş değerlere gizlenir. Veri geri çıkarılırken belirlenen aralıktaki veya oluşturulan boşluktaki değerler okunur. Stego görüntüden elde edilen histogramda seçilen sınırlar dışındaki aralık aynı miktarda ters yöne kaydırılarak orijinal görüntü geri elde edilir.

Ni ve arkadaşları histogram kaydırma tekniğini kullanarak gizli verileri en sık tekrarlanan piksellere gizlemiştir (Ni ve diğ, 2009). Tsai ve arkadaşları, veri gömme kapasitesini geliştirmek için histogram tabanlı bir yaklaşım önererek, gizli veriler doğrusal tahminden sonra kalan görüntülerde gizlendi ve ekstra kapasite için tepe noktası ve sıfır noktası çiftlerini kullanmıştır. Zhao ve diğerleri tarafından önerilen yöntemde, ilk olarak doğrusal tahmin yöntemi ile piksel farklarını kullanarak pozitif ve negatif fark histogramları oluşturmuşlardır (Zhao ve diğ.,2011). Daha sonra bu histogramlar üzerinde kaydırma işlemi yapılarak boş sütunlar elde edilir. Ve son olarak, bu boş sütunlara sıfır merkezli bir aralık dağıtarak veri gizlemeyi uygulamışlardır. Wang ve arkadaşları, piksel başına iki fark üreten, önce farklılıklara dayalı olarak iki boyutlu bir histogram oluşturan ve ardından bu histogramı veri gizlemek için birkaç tek boyuta indirgeyen ve yüksek gömme kapasitesi elde etmeyi amaçlayan yeni bir yaklaşım geliştirdi (Wang ve diğ., 2013).

Dördüncü bir yaklaşım piksel değerlerini sıralamaktır (Li ve diğ., 2013). Piksel değerleri sıralama yaklaşımda görüntünün içinden ufak piksel blokları alınır. Alınan bu blokların her birisi kendi içinde küçükten büyüğe doğru sıralanır. Bu piksel grupları için sadece en büyük iki değeri arasındaki farın bire eşit olması durumunda veri gizleme yapılır ve sadece bir bitlik veri gizlenir. Gizlenecek verinin sıfır olması durumunda hiçbir şey değiştirilmez, kalan büyün durumlarda en büyük iki pikselin farkı bir birim arttırılır. Veri tekrardan çıkarılırken aynı blokların en büyük iki sayısının farkları alınır. Bu fark kümesinin bütün değerleri bir birim eksilttiğinde elde edilen yeni kümedeki 0 ve 1'e eşit olan değerler bize gizlenen veriyi geri verir. Her blok için en büyük iki sayıdaki farkın 2'den büyük olduğu yani veri gizlenmediği durumda ve farkın ikiye eşit olduğu yani gizlenen bitin 1 olduğu durumda en büyük sayıdan bir çıkartılarak blok ilk haline geri getirilir. Böylece orijinal görüntü korunmuş olur.

Tersinir veri gizlemedeki beşinci yaklaşım ise çift görüntü tabanlı yöntemlerdir. Çift görüntü tabanlı Steganografi yöntemleri veri gizlemek için aslında yine bir taşıyıcı

görüntü kullanır. Stego sistemin veri gizleme kısmında bu taşıyıcı görüntüden iki kopya oluşturulur. Gizlenecek veri iki parçaya bölünerek, taşıyıcı görüntünün kopyaları üzerine uyarlanır. Bu şekilde bir taşıyıcı görüntüden iki stego görüntü elde edilir. Çoğu metodolojide stego görüntüler tek başına kullanılamaz. Orijinal görüntünün ve verinin elde edilmesi için stego görüntülerin her ikisi de gereklidir.

2.3.7. Çift Görüntü Tabanlı Steganografi Yöntemleri

Çift görüntü tabanlı çoğu steganografi yaklaşımında ikili sayı tabanındaki gizli verileri önce diğer sayı tabanlarına çevirerek gizli semboller yaratılır. Çevrilen bu sayı tabanı genlikle onluk sayı tabanı olur. Bu sembollerin, içine gizleneceği görüntünün pikselleriyle toplanmasıyla birinci, çıkartılmasıyla ise ikinci stego görüntü elde edilir. Bu gizli sembollerin sayısal değerleri ne kadar büyükse stego görüntü ile orijinal görüntü arasındaki değişimler de o kadar büyük olacaktır. Bu da stego görüntüdeki bozulmalara sebebiyet vererek, gizlenen verinin varlığının anlaşılabilir hala gelmesine sebep olur (Jung, 2016).

Çift görüntü tabanlı steganografi üzerine yapılan ilk çalışmalardan birisi Chang ve arkadaşlarının 2007 yılında, EMD yöntemini ikili görüntü tekniği ile birleştirmesidir. Yöntem $256x256$ ebatlarındaki bir fonksiyon matrisini harita olarak kullanır (Chang ve diğ., 2007). Gizlenecek verideki iki birlik serileri alıp, sıfırdan dörde kadar değişebilen değişen beşli sembollere çevirir. Son olarak haritalama tablosundaki sol ve sağ köşegenlere karşılık gelen stego görüntüdeki piksel değerlerindeki değişimleri elde eder.

2009 yılında ise Lee ve arkadaşları yatay ve dikey ardışık değerlerin karşılıklı birleşimiyle bir araya gelen çapraz desen kullanan bir çift görüntü tabanlı yöntemi geliştirmiştir (Lee ve diğ., 2009). Yönteminde dörder bitlik gizli veri parçaları alıp bu veri parçalarının ilk iki bitini oluşturulacak desenin nerede başlayacağını belirtmek için, geriye kalan bitleri ise desenin üzerindeki hareketin hangi yönde ilerletileceğini belirlemek için kullanır. Daha sonra stego görüntü üzerindeki piksellerde yapılması gereken değişiklik için desen üstündeki hücrelerde meydana gelen değişikliklerden faydalanılır.

2015 Yılında Lu ve arkadaşları, merkez katlama stratejini kullanarak çift görüntü tabanı yeni bir yaklaşımda bulunmuşlardır (Lu ve diğ., 2015). Bu yaklaşımda ilk olarak gizli veri desimal tabandaki sembollere dönüştürülür. Ardından bu semboller sıfırı merkez

alacak şekilde ikiye katlanarak hem pozitif hem de negatif değerler alabilen ikincil semboller hesaplanır. Son olarak bu ikincil semboller ikiye bölünerek her iki stego görüntüde üstende yapılacak değişimleri ifade eden değişimler elde edilir. Değişim değerlerinin, görüntünün piksellerindeki değerlerle toplanması yoluyla gizleme işlemini gerçekleştir.

Chi ve arkadaşları, merkeze katlama stratejisini içeren yeni bir çift görüntü tabanlı tersinir veri gizleme yöntemi önerdi (chi ve diğ. 2018). Yöntem, merkezi katlama stratejisini geliştirmek için ortak komşu kodlamayı kullanan dinamik bir kodlama stratejisi kullanır.

Shastri ve arkadaşları merkez katlama stratejisini ve kaydırılabilir piksel koordinat seçme tekniğini (Shasktri ve diğ., 2019) kullanarak ikili görüntü tabanlı tersine çevrilebilir bir veri gizleme şeması geliştirdi. Bunun için üçlü sayı sisteminden faydalandı. Kullandığı üçlü sayı sistemi yönteminde basamak farkı yüzünden piksel başına bazen üç bazen dört bit gizlemektedir. Yöntemin görüntüyü geri dönüştürebilmektedir fakat, geri dönüştürme işleminde gizlenen veri için artı ya da eksi yönlü bir birim bozulma mevcuttur. Bu bozulmanın düzeltilmesi için iki stego görüntüye ek olarak düzeltme amaçlı üçüncü bir harita bilgisine ihtiyaç duyar. Bu harita şifre olarak tanımlanır.

Devamında Meikap ve arkadaşları, farklı blok boyutu ile düzenin yönlü piksel değeri aracılığıyla merkezden katlamaya dayalı bir veri gizleme şeması geliştirdi (Meikap ve diğ., 2021).

2.3.8. Çift Görüntü Tabanlı Steganografi Yöntemlerine Örnekler

2.3.8.1. Konum Temelli Çift Görüntü Tekniği

Lee ve ekip arkadaşları tarafından 2009 yılında konum temelli çift görüntü tabanlı steganografi tekniği önerildi. Yöntemde piksel çiftleri sırasıyla X ve Y eksenleri üzerinde koordinat kümesi olarak alınır. Bu piksel çifti kümesi, Tablo 2.1'deli çapraz desenin merkez noktasını ardışık pikseller olarak yani $X_{i,j}$, $X_{i,j+1}$ olarak kabul eder. Üst, alt, sol ve sağ piksel çiftleri, her biri 2 bit olan farklı gizli veri S_1ve S_2 kombinasyonlarına karşılık gelir.

Tablo 2.1. Piksel çifti kümelerini gösteren çapraz model

	$X_{i,j}+1, X_{i,j+1}$ $S_1 = 10$	
$X_{i,j}-1, X_{i,j+1}$ $S_1 = 11$	$X_{i,j}, X_{i,j+1}$	$X_{i,j}+1, X_{i,j+1}$ $S_1 = 00$
	$X_{i,j}, X_{i,j+1}-1$ $S_1 = 01$	

Bu tablodaki desen Denklem 2.4'teki şekilde ifade edilebilir. Birinci stego görüntü için yapılacak değişimler bu Denklem 2.4'e göre gerçekleştirilir.

$$\left(X'_{i,j}, X'_{i,j+1}\right) = \begin{cases} \left(X_{i,j}+1, X_{i,j+1}\right) Eğer\ S_1 = 00 \\ \left(X_{i,j}, X_{i,j+1}-1\right) Eğer\ S_1 = 01 \\ \left(X_{i,j}, X_{i,j+1}+1\right) Eğer\ S_1 = 10 \\ \left(X_{i,j}-1, X_{i,j+1}\right) Eğer\ S_1 = 11 \end{cases} \tag{2.4}$$

Daha sonra gelen S_2 gizli mesajına göre Denklem 2.4'teki ifade ikinci stego görüntü için Denklem 2.5' deki gibi uygulanır.

$$\left(X''_{i,j}, X''_{i,j+1}\right) = \begin{cases} \left(X_{i,j}+1, X_{i,j+1}\right) Eğer\ S_2 = 00 \\ \left(X_{i,j}, X_{i,j+1}-1\right) Eğer\ S_2 = 01 \\ \left(X_{i,j}, X_{i,j+1}+1\right) Eğer\ S_2 = 10 \\ \left(X_{i,j}-1, X_{i,j+1}\right) Eğer\ S_2 = 11 \end{cases} \tag{2.5}$$

Örneğin, $X_{1,1}$= 45 ve $X_{1,2}$= 46 olsun ve gizli 0011 olarak kabul edelim. Burada $S_1 = 00$ ve $S_1 = 11$ olacaktır. Denklem 2.4'ten $S_1 = 00$ karşılığı olarak $\left(X'_{i,j}, X'_{i,j+1}\right) = \left(X_{i,j}+1, X_{i,j+1}\right)$ eşitliği gelir. Bu eşitlikte i ve j değerleri düzenlendiğinde, $\left(X'_{1,1}, X'_{1,2}\right) = \left(X_{1,1}+1, X_{1,2}\right)$ ifadesi elde edilecektir. Birinci stego görüntü için ilk iki stego piksellerin değerleri $X'_{1,1} = 45 + 1 = 46$ ve $X'_{1,2} = 46$ olacaktır. $S_2 = 11$ için Denklem 2.5'e baktığımızda $\left(X''_{i,j}, X''_{i,j+1}\right) = \left(X_{i,j}-1, X_{i,j+1}\right)$ ifadesine denk olduğunu görürüz. Bu durumda da $\left(X''_{1,1}, X''_{1,2}\right) = \left(X_{1,1}-1, X_{1,2}\right)$ eşitliğiyle karşı karşıya kalırız. Bu eşitlikte $X_{1,1}$ ve $X_{1,2}$ değerleri yerine koyulduğunda ikinci stego görüntünün piksel değerleri $X''_{1,1} = 45 - 1 = 44$ ve $X''_{1,2} = 46$ olur.

Tablo 2.2. Veri çıkarma kombinasyonları ve gizli veri değerleri

Koşul	Eylem
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 2, X''_{i,j+1})$	$S_1 = 00, S_2 = 11$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 2, X''_{i,j+1})$	$S_1 = 11, S_2 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 2)$	$S_1 = 10, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 2)$	$S_1 = 01, S_2 = 10$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} + 1)$	$S_1 = 00, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} - 1)$	$S_1 = 01, S_2 = 11$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} - 1)$	$S_1 = 11, S_2 = 01$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} + 1)$	$S_1 = 10, S_2 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1})$	$S_1 = 00$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1})$	$S_1 = 11$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 1)$	$S_1 = 10$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 1)$	$S_1 = 01$

Gizli mesajın geri elde edilmesi için öncelikle piksellerin eşitliğine bakılır. Eğer ardışık iki piksel her iki stego görüntü için de eşitse yani $X'_{i,j}, X''_{i,j}$ ve $X'_{i,j} + 1, X''_{i,j+1}$ eşitliklerinin ikisi de sağlanıyorsa burada veri gizlenmediği anlamına gelir. Gizli veriyi geri elde etmek için iki stego görüntünün ikili piksel grupların değerleri arasındaki farklara bakılır. Burada $[-2,2]$ aralığında farklar söz konusudur. Farkların birinci veya ikinci piksellerde farklı miktarlarda oluşabilmesi sebebiyle on iki çeşit kombinasyon söz konusudur. Bu on iki kombinasyon için gerçekleşen koşula karşılık gelen gizli verinin çıkarılması ilgili eylemler Tablo 2.2'de de gösterilmiştir.

Tablo 2.3. Veri çıkarma kombinasyonları ve örtü görüntü piksel değerleri

Koşul	Eylem
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 2, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j}, X''_{i,j}}{2}, \frac{X'_{i,j+1}, X''_{i,j+1}}{2}\right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 2, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j}, X''_{i,j}}{2}, \frac{X'_{i,j+1}, X''_{i,j+1}}{2}\right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 2)$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j}, X''_{i,j}}{2}, \frac{X'_{i,j+1}, X''_{i,j+1}}{2}\right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 2)$	$(X_{i,j}, X_{i,j+1}) = \left(\frac{X'_{i,j}, X''_{i,j}}{2}, \frac{X'_{i,j+1}, X''_{i,j+1}}{2}\right)$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X'_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X'_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X'_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X'_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} + 1, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j} - 1, X''_{i,j+1})$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} + 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$
$(X'_{i,j}, X'_{i,j+1}) = (X''_{i,j}, X''_{i,j+1} - 1)$	$(X_{i,j}, X_{i,j+1}) = (X''_{i,j}, X''_{i,j+1})$

Daha sonra stego görüntünün orijinal örtü görüntüye geri dönüştürülmesi için aynı şekilde on iki kombinasyon vardır. Stego görüntüde karşımıza gelecek aynı on iki koşul için orijinal görüntünün geri elde edilmesi sırasında gerçekleştirilecek eylemler Tablo 2.3'te verilmiştir.

2.3.8.2. Merkez Katlama Tekniği

Merkez katlama tekniği Lu ve ekip arkadaşları tarafından 2015 yılında geliştirilmiştir. Yöntemde veri gizleme sırasında k bit sayısı belirlenir. Gizli mesaj k bitlik d paketlerine bölündükten sonra bu paketlerin her biri için Denklem 2.6'teki Dönüşüm kullanılır.

$$d' = d - 2^{k-1} \tag{2.6}$$

Tablo 2.4'te, merkez katlama stratejisinde bu dönüştürme işlemi için bir k = 3 örneğini göstermektedir.

Tablo 2.4. k = 3 için katlama örneği

0	1	2	3	4	5	6	7
↓	↓	↓	↓	↓	↓	↓	↓
-4	-3	-2	-1	0	1	2	3

Denklem 2.7, veri gizleme işlemi sırasında stego görüntüsündeki piksel değerlerindeki değişimi hesaplamak için kullanılır. Bu değerler, Denklem 2.8 kullanılarak stego görüntü piksel değerlerinin elde edilmesinde kullanılır.

$$d_1' = \left\lfloor \frac{d'}{2} \right\rfloor \; and \; d_2' = \left\lceil \frac{d'}{2} \right\rceil \tag{2.7}$$

$$X_{i,j}' = X_{i,j} + d_1' \; ve \; X_{i,j}'' = X_{i,j} - d_2' \tag{2.8}$$

Mesaj gizleme aşamasında stego piksellerin sıfırın altına düşme veya 255 in üzerine çıkma durumu söz konusu olacağında gömme işlemi her değerdeki pikselde gerçekleştirilemez. d''nün değişim aralığı $[-2^{k-1}, 2^{k-1} - 1]$ aralığına eşit olduğundan 0 ve 255 ten bu mesafedeki piksellere gömme işlemi yapılmaz. Bu da Gömme aralığının $[0 + 2^{k-1}, 255 - 2^{k-1} + 1]$ yani $[2^{k-1}, 256 - 2^{k-1}]$olacağı anlamına gelir.

Yöntemin veri çıkarma işleminde esas olarak iki stego görüntü piksel değerinin farkı hesaplanmakta, bu işlemi gösteren formül Denklem 2.9'da sunulmaktadır.

$$d = \left[X'_{i,j} - X''_{i,j}\right] + 2^{k-1} \tag{2.9}$$

Orijinal örtü görüntüsünü kurtarmak için, iki stego görüntü piksel değerinin ortalaması hesaplanmalı ve Denklem 2.10'de gösterildiği gibi yuvarlanmalıdır.

$$X_{i,j} = \left\lfloor \frac{X'_{i,j} + X''_{i,j}}{2} \right\rfloor \tag{2.10}$$

Gömme işlemi için örtü görüntünün piksel değerlerinin $X = \{45, 46\}$ olduğunu farz edelim. $k = 3$ için her piksele 3 bit veri gizlenebilir. Bu da 6 bit uzunluğunda bir mesaj demektir. $S = 001111$ için $S_1 = 001$ ve $S_2 = 111$ şeklinde gruplanır. Bunlar onluk tabana çevrildiğinde $S_1 = 1$ ve $S_2 = 7$ olur. Yani $d = \{1, 7\}$'e eşittir. Denklem 2.6'teki dönüşüm yapıldığında $d' = \{1, 7\} - 4 = \{-3, 3\}$ olacaktır. Denklem 2.7'te gösterilen katlama işlemi gerçekleştirildiğinde $d'_1 = \lfloor\{-3, 3\}/2\rfloor = \{-2, 1\}$ ve $d'_1 = \lceil\{-3, 3\}/2\rceil = \{-1, 2\}$ olacaktır. Son olarak Denklem 2.8'teki gibi $d_1{}'$ ve $d_2{}'$ ile stego görüntüler oluşturulduğunda $X'_{i,j} = X' = X + d'_1 = \{45, 46\} + \{-2,1\} = \{43, 47\}$, $X'' = X - d'_2 = \{45, 46\} - \{-1, +2\} = \{46, 44\}$ olacaktır.

Aynı örnek için devam edersek $X' - X'' + 2^{k-1} = \{43, 47\} - \{46, 44\} + 4 = \{-3,3\} + 4 = \{1,7\}$ şeklinde gizli veri geri elde edilmiş olur. Orijinal görüntüyü geri elde etmek için ise Denklem 2.10'da gözüktüğü gibi iki stego görüntünün ortalaması alınıp, yukarıya yuvarlanması gerekir. $X = \lceil(X' + X'')/2\rceil = \lceil(\{43, 47\} + \{46, 44\})/2\rceil = \lceil\{89, 91\}/2\rceil$ → X=⌈ {89,91} /2 ⌉ = {45,46}.

2.3.8.3. Üçlü Atama ve Merkez Katlama Stratejisi

Birleştirme aşamasında, ikili gizli veri üçlü gruplar halinde alınır ve ondalığa çevrilir. Eğer ondalık gizli veri 7 ise, sonraki ikili gizli bit eklenir. Örneğin, ondalık gizli veri 7 ve sonraki ikili bit 0 ise, yeni gizli veri 4 bit yerine üç bite sığacak şekilde olur.

Değişimler, ikili gizli verilerin üçlü eşdeğerinden ve örtü görüntüsünde neden oldukları ilgili kaymalardan oluşur. Kaymaları oluşturmak için, merkez kaydırma stratejisi ve onun üçlük tabandaki temsilini kullanarak elde edilen katlanmış ondalık veriler kullanılır.

Üçlük tabana çevrilen bitler m_1 ve m_2 (-1, 0, 1) kümesine aittir. Artan sıra ile ondalık tabanda sıfırı iden küçük sembol $(-1-1)_3$ ve ondalık tabanda sekizi ifade eden en büyük en büyük sembol $(11)_3$ sayısıyla temsil edilir. Gizli verinin üçlüye çevrilmesi kaydırma yönünü belirlemeye yardımcı olur. Kaydırma şu şekilde hesaplanır:

Sıfır ve sekiz arasında bir ondalık sayı d için, merkez kaydırma kullanılarak d_b üretilir. Bu durumda k değeri 3 olur çünkü ikili gizli veriden 3 bitlik gruplar kullanılacaktır. Bu nedenle, d aralığı [-4, 4] olarak kaydırılır ve Denklem 2.11'da gösterildiği gibi elde edilir.

$$d_b = d - 2^{k-1} = d - 2^{3-1} = d - 4 \tag{2.11}$$

Ardından başlangıç değişimleri s1 ve s2 hesaplanır. Bunun için Denklem 2.12 ve 2.13'ten faydalanılır.

$$\delta_1 = \begin{cases} -m_1 \frac{\lceil d_b/3 \rceil}{2} & Eğer\ m_1 = 1\ (mod\ 2) \\ -m_1 \frac{\lfloor d_b/3 \rfloor}{2} & Eğer\ m_1 = 0\ (mod\ 2) \end{cases} \tag{2.12}$$

$$\delta_2 = \begin{cases} -m_2 \frac{\lfloor d_b/3 \rfloor}{2} & Eğer\ m_1 = 1\ (mod\ 2) \\ -m_2 \frac{\lceil d_b/3 \rceil}{2} & Eğer\ m_1 = 0\ (mod\ 2) \end{cases} \tag{2.13}$$

Kaydırmaların son halleri s1 ve s2 denklem 2.14 ve 2.15 kullanılarak hesaplanır:

$$s_1 = \begin{cases} \lfloor \delta_1 \rfloor & Eğer\ d < 7 \\ -\lfloor \delta_1 \rfloor & Eğer\ d \geq 7 \end{cases} \tag{2.14}$$

$$s_2 = \begin{cases} \lceil -\delta_1 + \delta_2 \rceil, & Eğer\ d < 7\ ve\ d = 1\ (mod\ 2) \\ -\lceil \delta_1 + \delta_2 \rceil, & Eğer\ d < 7\ ve\ d = 0\ (mod\ 2) \\ [\delta_1 + \delta_2], & Eğer\ d \geq 7\ ve\ d = 1\ (mod\ 2) \\ \lceil \delta_1 + \delta_2 \rceil, & Eğer\ d \geq 7\ ve\ d = 0\ (mod\ 2) \end{cases} \tag{2.15}$$

Hesaplanan s_1 ve s_2 değerleri stego görüntülerdeki değişikliklerdir. Bu sayılar örtü görüntüye denklem 2.16 ve 2.17'teki gibi eklendiğinde stego görüntüler oluşur.

$$X' = X + s_1 \tag{2.16}$$

$$X'' = X + s_2 \tag{2.17}$$

Orijinal görüntünün çıkartılması iki görüntünün ortalaması yukarıya yuvarlanmasıyla sağlanır (denklem 2.18).

$$X_{i,j} = \left\lceil \frac{X'_{i,j} + X''_{i,j}}{2} \right\rceil \tag{2.18}$$

Orijinal görüntü elde edildikten sonra gizli semboller denklem 2.19 ve 2.20'daki gibi stego görüntüden orijinal görüntünün çıkartılmasıyla elde edilir.

$$s_1 = X' - X \tag{2.19}$$

$$s_2 = X' - X \tag{2.20}$$

Fakat veri gizleme sırasında $d \in \{0,1\},\{2,5\},\{3,4\},\{7,8\}$ durumunda gizlenen s_1 ve $s_2$değerleri birbiriyle aynı olmaktadır. Yani gizlenen verinin 1 ya da 0 olması durumda veriyi çıkaran kişi verinin hangisi olduğunu bilemez veriyi ± 1 bozulmayla elde edebilir.

Tablo 2.5. Üçlü atama için eşleşen değişimler tablosu

Gizli veri	d	d_b	Üçlü Harita		Başlangıç kaydırma		Değişim	
			m_1	m_2	δ_1	δ_2	s_1	s_2
000	0	-4	-1	-1	-0,5	-1	-1	1
001	1	-3	-1	0	-0,5	0	-1	1
010	2	-2	-1	1	0	0,5	0	-1
011	3	-1	0	-1	0	0	0	0
100	4	0	0	0	0	0	0	0
101	5	1	0	1	0	-0,5	0	-1
110	6	2	1	-1	-0,5	0	-1	0
111+0	7	3	1	0	-0,5	0	1	-1
111+1	8	4	1	1	1	-0,5	1	-1

Bu bozulmanın giderilmesi için göndericinin alıcıya ayriyeten bir harita göndermesi gerekir. Tabloda gözüktüğü gibi $d = 6$ hariç bütün değerler birbiriyle eşleşmektedir. Eşleşmeyen tek değerin çift olması sebebiyle, buradaki bütün tek sayıların alıcıya ayrıca verilmesi gerekir. Bunum için hazırlanan haritada d'nin çift olduğu bütün değerlerin bulunması gerekir. Bu konum haritası Denklem 2.21 de verildiği şekildedir.

$$LM_i \begin{cases} 1, & Eğer\ d_i = 1\ (mod\ 2) \\ 0, & Eğer\ d_i = 0\ (mod\ 2) \end{cases} \tag{2.21}$$

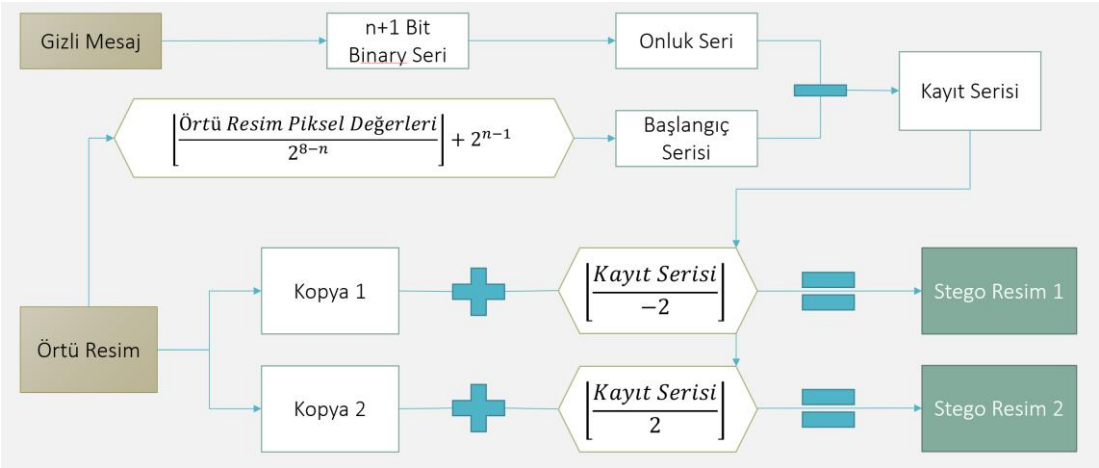
Denklem 2.17'de 1 alan yerler bozulmanın olduğu mesaj parçalarını gösterir. Verinin bozulmasız şekilde elde edilebilmesi için gönderici ve alıcı arasında LM_i (Konum haritası – Location Map) değerlerin aslının ne olduğu paylaşılması gerekir. İnisiyatif olarak LM serisi iki parçaya bölünerek denklem 2.22 ve 2.23'teki gibi de hazırlanabilir.

$$LM_{1_i}\begin{cases}1, & Eğer\ d_i = 1\ (mod\ 2)\ ve\ d_i \leq 0\\ 0, & Eğer\ d_i = 0\ (mod\ 2)\end{cases} \tag{2.22}$$

$$LM_{2_i}\begin{cases}1, & Eğer\ d_i = 1\ (mod\ 2)\ ve\ d_i > 0\\ 0, & Eğer\ d_i = 0\ (mod\ 2)\end{cases} \tag{2.23}$$

3. ÖNERİLEN YÖNTEM

Bu bölümde, en önemli bitleri ve merkez kaydırma tekniğini kullanan yeni bir çift görüntü tabanlı tersinir veri gizleme yöntemi önerilmiştir. Veri gizleme işlemi sırasında önerilen yöntem, tek bir örtü görüntüden iki farklı stego görüntü oluşturarak verileri güvenli bir şekilde gizlemektedir. Veri çıkarma işlemi sırasında bu iki stego görüntüden gizli veri ve orijinal örtü görüntüsü kayıpsız olarak elde edilir.



Şekil 3.1. Veri Gizleme Akış Şeması

Veri gizleme işleminin akış şeması Şekil 3.1'de gösterilmektedir. Veri gizleme işleminin ilk adımında piksel değerinin en önemli bitlerinden kaç tanesinin kullanılacağını temsil eden n sayısı belirlenir. Gizli verinin boyutu veya kabul edilebilir maksimum bozulma oranları, n sayısının seçilmesinde belirleyici faktörlerdir. İkinci adımda gizli veri $(n+1)$ bit ikili diziye dönüştürülür ve dizideki her bir eleman ondalık sisteme dönüştürülerek gizlenecek sembolleri temsil eden s serisi elde edilir. Kısaca seçilen n değeri için $(n+1)$ bit gizleme işlemi gerçekleştirilir. Bu nedenle, orijinal örtü görüntüsündeki bayt başına $(n+1)/2$ bit gizli veri gizlenir. Bu şekilde, piksel başına gizlenen bit sayısı her zaman 1'den büyük olur. Belirlenen n sayısı için piksel değerlerinin en anlamlı n biti kullanılarak başlangıç serisi oluşturulur ve bu serinin aralığı $[0, 2^n - 1]$ arasındadır. Denklem 3.1, bu başlangıç serisini hesaplamak için kullanılır.

$$d = \left\lfloor \frac{X_{i,j}}{2^{8-n}} \right\rfloor \tag{3.1}$$

Başlangıç seri değerleri ile gizli veriler arasındaki fark, stego görüntüsüne gömülecek gizli verilerin ortalamasını düşürmeyi amaçlamak için hesaplanır. Bu işlem gizli veriden

gelen $[0, 2^{n+1} - 1]$ aralığının genişlemesine ve $[-2^n + 1, 2^{n+1} - 1]$aralığında değer almasına neden olur. Denklem 3.2, bu gizli verilerin hesaplanmasını gösterir.

$$d' = s_i - d_i \tag{3.2}$$

$$d'' = d' - 2^{n-1} \tag{3.3}$$

Ortalama kare hatasını en aza indirmek için bu aralığın orta noktası sıfıra gelene kadar ters yönde kaydırılması gerekir. Bunun için denklem 3.3'teki eşitlik kullanılarak örtü görüntüde gizlenecek olan kayıt serisi elde edilir. Elde edilen gizli semboller serisinden 2^{n-1} değeri çıkarılarak değişim aralığı $[-2^n - 2^{n-1} + 1,\ 2^{n+1} - 2^{n-1} - 1]$ haline gelir. Bu aralık ifadesi sadeleştirildiğinde $[-3 * -2^{n-1} + 1,\ 3 * 2^{n-1} - 1]$ olur ve sıfır değerini ortalayan bir dağılım gösterir. Bu kayıt serisi sırasıyla 2 ve -2'ye bölünerek birinci ve ikinci stego görüntülerin değişimi elde edilir. Bu değişiklikler, denklem 3.4 kullanılarak elde edilir.

$$d_1 = \left\lfloor \frac{d''}{2} \right\rfloor, d_2 = \left\lfloor \frac{d''}{-2} \right\rfloor \tag{3.4}$$

Bu değişimler denklem 3.5'teki gibi örtü görüntünün üzerine eklenerek iki adet stego görüntüsü elde edilir ve veri gizleme işlemi tamamlanır.

$$X' = X + d_1 \quad ve \quad X'' = X + d_2 \tag{3.5}$$

Veri gizleme işlemi sırasında, kayıt serisi ikiye bölündüğü için değişiklik aralığı da ikiye bölünür. Bu nedenle, değişim aralığı $[-3 * -2^{n-1} + 1,\ 3 * 2^{n-1} - 1]$'den $[-3 * -2^{n-2} + ½,\ 3 * 2^{n-2} - ½]$'e dönüşür. Elde edilen stego piksel değerleri aşağı yuvarlandığı için değişim aralıkları $[-3 * -2^{n-2},\ 3 * -2^{n-2} - 1]$ haline gelir.

Sınır değerlerin aşımından kaçınmak için veri gizleme işlemi yalnızca $[3 * -2^{n-2},\ 256 - 3 * 2^{n-2}]$ aralığındaki pikseller için gerçekleştirilir. Şekil 3.2, n = 4 için gizli verilerde yapılan değişikliklerle değişiklik farkının nasıl değiştiğini göstermektedir.

Başlangıç Değişimleri		Gizli veri	
		0	31
Başlangıç Bitleri	0	0	31
	15	-15	16

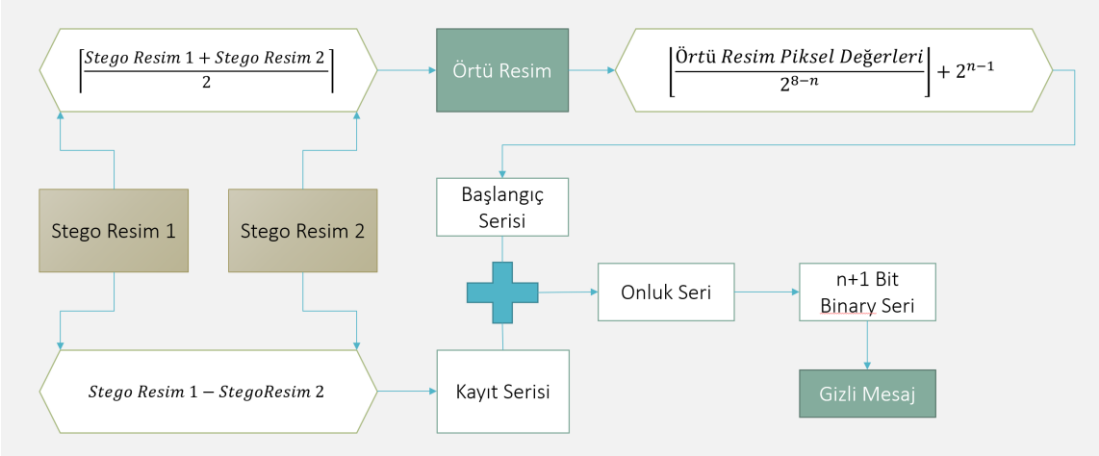
Düzeltme -8		Gizli veri	
		0	31
Başlangıç Bitleri	0	-8	23
	15	-23	8

Stego 1 Değişimler		Gizli veri	
		0	31
Başlangıç Bitleri	0	-4	11
	15	-12	4

Stego 2 Değişimler		Gizli veri	
		0	31
Başlangıç Bitleri	0	4	-12
	15	11	-4

Şekil 3.2. n=4 için gizli veri ve piksel değişimlerinin aralıkları

Veri çıkarma işlemi sırasında iki stego görüntünün aynı konumdaki piksel değerlerinden herhangi biri bu aralık içindeyse, burada gizli veri saklı demektir (Sınır aşımını engellemek için tüm piksel değerlerine veri gömülü değildir). Bu iki değer eşitse ve $[3 * -2^{n-2}\ ,\ 256 - 3 * 2^{n-2}]$ aralığının içindeyse, kayıt serisindeki bu piksellerdeki gizli verinin sıfır olduğu anlamına gelir. İki stego görüntüdeki piksel değerleri bu aralığın dışında ve eşit ise burada hiçbir gizli verinin saklanmadığı anlaşılır. Veri çıkarma işleminin akış şeması Şekil 3.3'te verilmiştir.



Şekil 3.3. Orijinal görüntüyü elde etme ve veri çıkarma akış şeması

Veri çıkarma işleminde, iki stego görüntünün piksel değerleri değiştiği için başlangıç serisi doğrudan elde edilemez. Bu nedenle veri çıkarma sürecinde öncelikle orijinal örtü görüntü elde edilmelidir. Başka bir deyişle, orijinal örtü görüntüsü kurtarılmadan gizli verileri olduğu gibi çıkarmak imkansızdır.

Orijinal örtü görüntüsünü kurtarmak için, Denklem 3.6'teki gibi iki stego görüntünün ortalaması alınır ve yukarı yuvarlanır. Yukarı yuvarlamanın ana nedeni, veri gizleme sırasında gerçekleştirilen aşağı yuvarlama işlemini etkisiz hale getirmektir.

$$X_{i,j} = \left\lceil \frac{X'_{i,j} + X''_{i,j}}{2} \right\rceil \tag{3.6}$$

Orijinal örtü görüntü kurtarıldıktan sonra, ilk dizi, denklem 3.7 kullanılarak elde edilebilir. Kayıt dizisinin çıkarılması, ilk stego görüntü ile ikinci stego görüntü arasındaki farkın hesaplanmasıyla denklem 3.7' gösterildiği gibi gerçekleştirilir.

$$d'' = X'_{i,j} - X''_{i,j} \tag{3.7}$$

Son olarak başlangıç serisi ve kaydırma miktarı ana kayıt serisine eklenir ve Denklem 3.8 kullanılarak s ile ifade edilen gizli veri sembolleri elde edilir.

$$s = d + d'' + 2^{n-1} \tag{3.8}$$

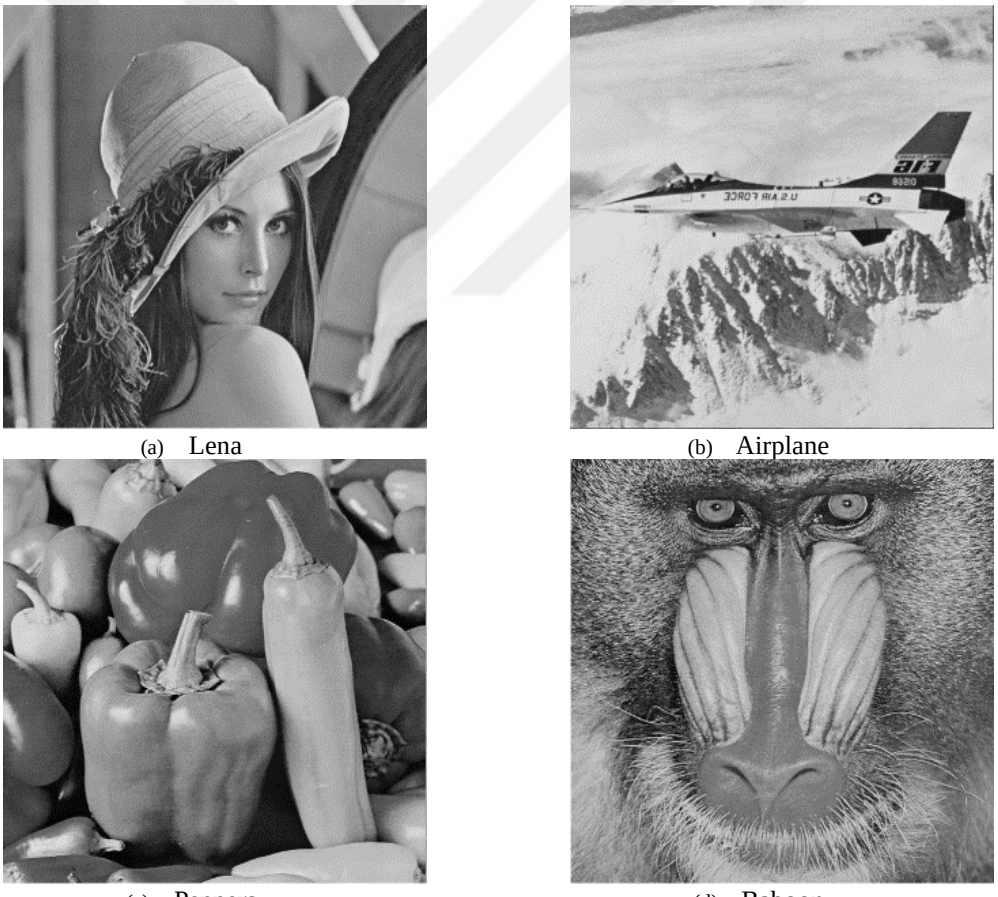
Örneğin, örtü görüntünün piksel değerlerini $X_{10} = \{146, 52, 85, 168\}$ farz edelim. Sekiz bitlik seriden oluşan bir baytın ikiye bölündüğünde 4 bitlik parçalar etmesi sebebiyle, kolay olması için n sayısını bunun bir eksiği olan $n = 3$ seçelim. Böylece her piksel için $k = n + 1 = 4$ bit veri gömebiliriz. Piksel sayısını 4 seçtiğimiz görüntü için kapasite16 bit gizli veri yapar. Her biri sekiz bitlik sayı olarak ifade edilebilecek iki adet gizli veriyi $S_{10} = \{212, 134\}$ olarak kabul edip bunun ikili sistemini elde ettiğimizde $S_2 = \{11010100,\ 1000110\}$ olduğu görülür. Bu ifade $k = 4$ bitlik veri kümesine çevrilirse $s_2 = \{1101, 0100, 1000, 0110\}$ elde edilir. Bu veriler ondalık sistemde $s = \{13, 4, 8, 6\}$'ye eşittir. Bir sonraki adımda, başlangıç serisini denklem 3.1 ile hesaplamamız gerekiyor. Burada başlangıç serisi $d = \{4, 1, 2, 5\}$ olarak hesaplanır. Denklem 3.2 ile başlangıç serisine gizli veriler eklediğimizde, $d' = \{9, 3, 6, 1\}$ elde ederiz. Bir sonraki adımda ortalamayı sıfıra eşitlemek için denklem 3.3 ile 2^{n-1}

miktarında kaydırma işlemi yapılır ve $d'' = \{5, -1, 2, -3\}$ serisi elde edilir. Her iki stego görüntüde yapılacak değişikliklerin hesaplanması için denklem 3.4 kullanılarak bu değişimler $d_1 = \{2, -1, 1, -2\}$ ve $d_2 = \{-3, 0, -1, 1\}$ olarak hesaplanır. Bu iki seri, denklem 3.5'e göre örtü görüntüsünün piksel değerlerine eklenir, $X' = \{148, 51, 86, 166\}$ ve $X'' = \{143, 52, 84, 169\}$ stego görüntüleri piksel değerleri elde edilir.

Gizli verilerin çıkarılması için, önce denklem 3.6'ya göre orijinal örtü görüntüsünün piksel değerlerini hesaplamamız gerekir. Denklem 3.6'yı kullandıktan sonra orijinal görüntünün piksel değerlerini, $X = \{146, 52{,}85{,}168\}$ olarak elde ederiz. İkinci adımda denklem 3.7 ile bu iki stego görüntü piksel değerinin farkını almalıyız. Böylece $d'' = \{5, 3, -5, -6\}$ elde ediyoruz. Daha sonra başlangıç serisinin elde edilmesi gerekir. Veri gizleme işlemi ile aynı yöntemle denklem 3.1 kullanılarak $d = \{4, 1, 2, 5\}$hesaplanır. Son olarak, gizli sembolleri elde etmek başlangıç serisini ve gizli sembolleri toplayıp, sonucu terse kaydırmamız gerekir. Denklem 3.8 ile bu işlemler yapılınca $s = \{14, 8, 2, 2\}$ olarak bulunur. Ve bu gizli veri, ikili gizli sistemde $n + 1 = 4$ bitlik serilere çevrildiğinde $s_2 = \{1110, 1000, 0010, 0010\ \}$ olarak dönüştürülür. Daha sonra sekiz bitlik gruplar ikiliden ondalık sisteme dönüştürüldüğünde gizli veriler $S_{10} = \{212{,}134\}$ elde edilir.

4. DENEYSEL ÇALIŞMALAR

Bu bölümde önerilen yöntemin deneysel sonuçları ve karşılaştırmaları yer almaktadır. Önerilen algoritma, gömme kapasitesi, yük, tepe sinyal gürültü oranı (PSNR) ve yapısal benzerlik indeksi ölçüsü (SSIM) gibi veri gizleme ölçütleriyle değerlendirmek için bir dizi gri renkli örtü görüntüsü üzerinde test edilmiştir. Çalışmada ayrıca önerilen yöntemin güvenlik testleri için histogram analizi, RS analizi ve piksel dağılımları analizi yapılmıştır. Şekil 4.1'de, deneysel çalışmalarda çeşitli veri gizleme kapasitesine sahip gizli verileri gömmek için kullanılan dört adet 512x512 gri tonlamalı orijinal örtü görüntüsünü verilmektedir. Testler yapılırken aynı görüntüler tekrar tekrar kullanılmıştır ve deneylerde bilgisayar tarafından rastgele oluşturulan gizli veriler, bu orijinal örtü görüntülerine gömülmüştür.



(a) Lena (b) Airplane

(c) Peppers (d) Baboon

Şekil 4.1. Deneysel çalışmada kullanılan görüntüler

PSNR değeri, orijinal örtü görüntü ile stego görüntüsü arasındaki benzerliği ölçmek için kullanılır, bu değer ne kadar yüksek olursa stego görüntü kalitesi o kadar iyi olur. Orijinal

örtü görüntüsü ile stego görüntü arasındaki ortalama karesel hatanın (MSE) hesaplanmasını gösteren formüller sırasıyla Denklem 2.2 ve 2.3'te verilmiştir. Bu formüller kullanılarak PSNR değerleri hesaplanmıştır. PSNR değerlerinin hesaplanmasında bu denklemler kullanılmıştır.

Gömme kapasitesi, iki stego görüntüsüne gömülen toplam gizli veri biti olarak ifade edilirken, Denklem 4.1'teki yük değeri, bayt başına gizlenen gizli veri biti (bpb) olarak temsil edilir.

$$P = \frac{EC}{2\ x\ H\ x\ W} \tag{4.1}$$

Tablo 4.1, $n = 1$ için farklı stego görüntülerinin gömme kapasitesinin ve PSNR değerinin karşılaştırmasını sunar. Deneysel çalışmalardan da görüleceği üzere farklı örtü görüntülerinde kapasitenin tamamı kadar gizli veri yüklendiğinde stego görüntü 1 ve stego görüntü 2'nin PSNR değerleri 51.15 (dB) civarındadır. Tablo 4.1 ve Tablo 4.5 arasında, sırasıyla n = 2-5 aralığı için yük, taşıma kapasitesi ve PSNR değerleri arasındaki ilişkiyi göstermektedir. Bu tablolar incelendiğinde önerilen yöntemde 1,5 (bpb) ile 3 (bpb) arası faydalı yük değerleri için sırasıyla 46 (dB) ile 28,5 (dB) arasında PSNR değerleri elde edilmektedir.

Tablo 4.1. N=1 seviyesi için yüke göre kapasite ve PSNR sonuçları

N=1 Yük Oranı	Lena				Baboon			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	52480	61,13	61,17	61,15	52256	61,15	61,20	61,18
20%	104912	58,11	58,11	58,11	104680	58,16	58,14	58,15
30%	157344	56,36	56,38	56,37	157104	56,37	56,38	56,38
40%	209768	55,16	55,08	55,12	209520	55,13	55,13	55,13
50%	262200	54,14	54,17	54,16	261944	54,13	54,14	54,14
60%	314632	53,38	53,37	53,38	314360	53,38	53,37	53,38
70%	367056	52,68	52,69	52,69	366776	52,70	52,70	52,70
80%	419488	52,10	52,12	52,11	419200	52,11	52,09	52,10
90%	471912	51,58	51,60	51,59	471616	51,60	51,59	51,60
100%	524288	51,14	51,14	51,14	524190	51,14	51,13	51,14

N=1 Yük Oranı	Airplane				Peppers			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	52264	61,21	61,19	61,20	52264	61,14	61,13	61,14
20%	104704	58,12	58,12	58,12	104696	58,13	58,11	58,12
30%	157136	56,37	56,38	56,38	157120	56,39	56,40	56,40
40%	209560	55,12	55,14	55,13	209552	55,12	55,13	55,13
50%	261992	54,17	54,16	54,17	261976	54,15	54,16	54,16
60%	314416	53,35	53,38	53,37	314400	53,36	53,38	53,37
70%	366848	52,69	52,70	52,70	366824	52,69	52,68	52,69
80%	419280	52,11	52,11	52,11	419256	52,12	52,12	52,12
90%	471704	51,60	51,60	51,60	471680	51,61	51,60	51,61
100%	524288	51,13	51,13	51,13	524104	51,15	51,14	51,15

Tablo 4.2. N=2 seviyesi için yüke göre kapasite ve PSNR sonuçları

N=2 Yük Oranı	Lena				Baboon			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	78354	56,36	56,12	56,24	78330	56,29	56,21	56,25
20%	157002	53,31	53,00	53,16	156960	53,29	53,09	53,19
30%	235650	51,57	51,20	51,39	235584	51,53	51,28	51,41
40%	314289	50,31	49,82	50,07	314202	50,25	50,06	50,16
50%	392928	49,35	48,90	49,13	392826	49,27	49,09	49,18
60%	471576	48,49	48,16	48,33	471450	48,46	48,33	48,40
70%	550218	47,72	47,50	47,61	550074	47,77	47,66	47,72
80%	628866	47,12	46,90	47,01	628698	47,20	47,08	47,14
90%	707505	46,61	46,39	46,50	707313	46,68	46,58	46,63
100%	786432	46,12	45,92	46,02	786222	46,23	46,14	46,19

N=2 Yük Oranı	Airplane				Peppers			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	78354	54,79	56,29	55,54	78345	56,13	55,60	55,87
20%	157002	51,87	53,23	52,55	156984	53,16	52,58	52,87
30%	235650	50,08	51,47	50,78	235626	51,38	51,05	51,22
40%	314289	48,84	50,23	49,54	314256	50,12	49,77	49,95
50%	392928	47,92	49,28	48,60	392889	49,19	48,88	49,04
60%	471576	47,16	48,52	47,84	471528	48,39	48,15	48,27
70%	550218	46,47	47,83	47,15	550161	47,71	47,49	47,60
80%	628866	45,90	47,25	46,58	628794	47,15	46,92	47,04
90%	707505	45,34	46,76	46,05	707794	46,63	46,37	46,50
100%	786432	44,84	46,31	45,58	786351	46,16	45,94	46,05

Tablo 4.3. N=3 seviyesi için yüke göre kapasite ve PSNR sonuçları

N=3 Yük Oranı	Lena				Baboon			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	104440	50,37	50,44	50,41	104368	50,44	50,57	50,51
20%	209296	47,43	47,36	47,40	209152	47,46	47,47	47,47
30%	314160	45,70	45,58	45,64	313936	45,62	45,62	45,62
40%	419016	44,44	44,30	44,37	418720	44,31	44,36	44,34
50%	523872	43,46	43,31	43,39	523504	43,37	43,42	43,40
60%	628728	42,66	42,59	42,63	628280	42,62	42,67	42,65
70%	733584	41,94	41,91	41,93	733064	41,90	41,98	41,94
80%	838456	41,34	41,29	41,32	837856	41,36	41,41	41,39
90%	943312	40,82	40,78	40,80	942640	40,87	40,92	40,90
100%	1048576	40,37	40,33	40,35	1047832	40,40	40,44	40,42

N=3 Yük Oranı	Airplane				Peppers			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	104440	49,67	50,07	49,87	104376	50,20	50,02	50,11
20%	209296	46,73	47,07	46,90	209160	47,20	47,05	47,13
30%	314160	44,97	45,35	45,16	313952	45,43	45,41	45,42
40%	419016	43,71	44,12	43,92	418744	44,15	44,10	44,13
50%	523872	42,75	43,16	42,96	523536	43,24	43,14	43,19
60%	628728	41,97	42,38	42,18	628320	42,49	42,40	42,45
70%	733584	41,31	41,72	41,52	733112	41,86	41,76	41,81
80%	838456	40,73	41,16	40,95	837912	41,25	41,17	41,21
90%	943312	40,22	40,64	40,43	942696	40,73	40,63	40,68
100%	1048576	39,73	40,18	39,96	1047896	40,30	40,21	40,26

Tablo 4.4. N=4 seviyesi için yüke göre kapasite ve PSNR sonuçları

N=4 Yük Oranı	Lena				Baboon			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	131050	44,47	44,46	44,47	130915	44,47	44,53	44,50
20%	262120	41,48	41,40	41,44	261840	41,46	41,47	41,47
30%	393195	39,75	39,65	39,70	392770	39,70	39,68	39,69
40%	524265	38,49	38,37	38,43	523705	38,38	38,40	38,39
50%	655330	37,48	37,38	37,43	654635	37,44	37,45	37,45
60%	786400	36,68	36,62	36,65	785570	36,65	36,68	36,67
70%	917480	36,00	35,96	35,98	916505	35,99	36,02	36,01
80%	1048555	35,39	35,35	35,37	1047440	35,42	35,44	35,43
90%	1179625	34,87	34,84	34,86	1178370	34,90	34,91	34,91
100%	1310710	34,40	34,38	34,39	1309315	34,48	34,50	34,49

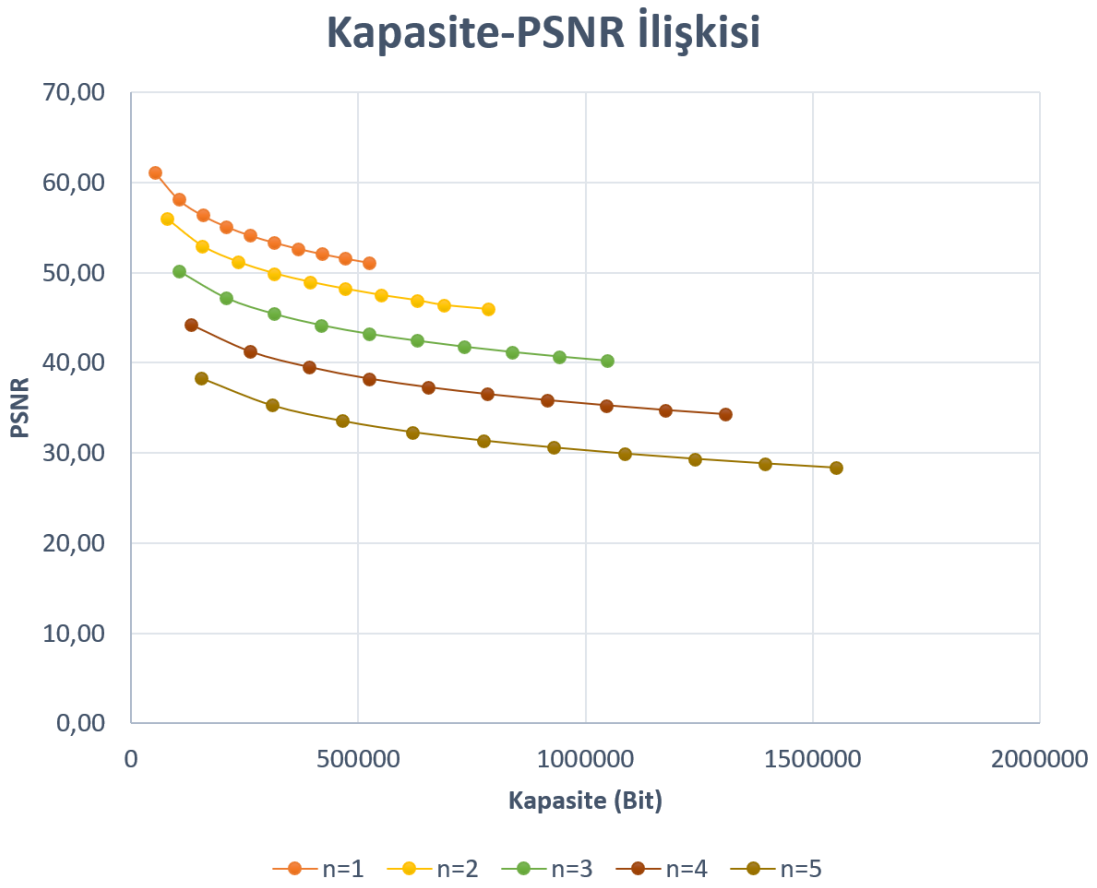
N=4 Yük Oranı	Airplane				Peppers			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	131050	43,71	43,99	43,85	129730	44,22	44,13	44,18
20%	262120	40,81	41,05	40,93	259480	41,24	41,17	41,21
30%	393195	39,04	39,28	39,16	389235	39,53	39,52	39,53
40%	524265	37,81	38,05	37,93	518985	38,23	38,21	38,22
50%	655340	36,85	37,11	36,98	648740	37,32	37,29	37,31
60%	786410	36,08	36,33	36,21	778490	36,59	36,55	36,57
70%	917490	35,42	35,67	35,55	908250	35,91	35,87	35,89
80%	1048560	34,84	35,09	34,97	1038000	35,36	35,33	35,35
90%	1179635	34,32	34,57	34,45	1167755	34,80	34,78	34,79
100%	1310720	33,81	34,09	33,95	1297515	34,32	34,35	34,34

Tablo 4.5. N=5 seviyesi için yüke göre kapasite ve PSNR sonuçları

N=5 Yük Oranı	Lena				Baboon			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	157218	38,46	38,46	38,46	156570	38,49	38,52	38,51
20%	314484	35,45	35,41	35,43	313194	35,50	35,50	35,50
30%	471744	33,70	33,65	33,68	469812	33,70	33,69	33,70
40%	629010	32,42	32,37	32,40	626436	32,43	32,44	32,44
50%	786276	31,46	31,41	31,44	783048	31,50	31,51	31,51
60%	943548	30,66	30,64	30,65	939672	30,70	30,71	30,71
70%	1100820	29,97	29,95	29,96	1096296	30,01	30,02	30,02
80%	1258080	29,37	29,36	29,37	1252914	29,45	29,46	29,46
90%	1415346	28,85	28,84	28,85	1409538	28,94	28,94	28,94
100%	1572648	28,39	28,38	28,39	1566192	28,48	28,49	28,49

N=5 Yük Oranı	Airplane				Peppers			
	Bit	PSNR			Bit	PSNR		
		Psnr1	Psnr2	Ort.		Psnr1	Psnr2	Ort.
10%	157098	37,86	37,99	37,93	149052	38,49	38,45	38,47
20%	314244	34,82	34,94	34,88	298140	35,48	35,45	35,47
30%	471384	33,10	33,22	33,16	447228	33,76	33,76	33,76
40%	628536	31,89	32,01	31,95	596316	32,48	32,49	32,49
50%	785682	30,94	31,07	31,01	745404	31,58	31,58	31,58
60%	942834	30,17	30,29	30,23	894498	30,83	30,83	30,83
70%	1099980	29,51	29,63	29,57	1043586	30,16	30,15	30,16
80%	1257120	28,92	29,04	28,98	1192674	29,58	29,57	29,58
90%	1414266	28,37	28,50	28,44	1341762	29,08	29,08	29,08
100%	1571454	27,89	28,02	27,96	1490850	28,59	28,59	28,59

Şekil 4.2, deneysel çalışmalarda kullanılan tüm gri tonlamalı görüntülerde n=1 ile 5 arası için elde edilen ortalama taşıma kapasitesini ve PSNR değerlerini gösterir. Önerilen algoritmada en yüksek PSNR değerlerinin n=1 için, maksimum yük değerinin ise n=5 için elde edildiği grafikten görülmektedir.



Şekil 4.2. Kapasite ve PSNR ilişkisi

Tablo 4.6, renkli örtü görüntüleri için yük, gömme kapasitesi ve PSNR değerlerinin karşılaştırmasını sunan tabloyu vermektedir. $n = 1$ için, PSNR değeri 51(dB)'den fazladır ve 1561416 bite kadar gizli veri gömülebilir. n= 4 olduğunda, PSNR değeri 34'ten (dB) fazladır ve 3847636 bite kadar gizli veri gömülebilir ki bu, bu çalışmada gömme kapasitesi ile PSNR arasındaki en uygun ilişkidir. $n = 5$ olduğunda, gömme kapasitesi önemli ölçüde artar, ancak PSNR değerinin kabul edilebilir değerin (30dB) altında olduğu gözlenir.

Tablo 4.6. N=1-5 için ortalama kapasite ve PSNR sonuçları

		Gizleme Kapasitesi Oranı									
		10%	**20%**	**30%**	**40%**	**50%**	**60%**	**70%**	**80%**	**90%**	**100%**
n=1	**Kapasite (bit)**	156148	312306	468466	624624	780780	936950	1093106	1249262	1405424	1561416,5
	PSNR	61,17	58,17	56,40	55,16	54,18	53,39	52,72	52,15	51,63	51,18
n=2	**Kapasite (bit)**	233880	467809,5	701741	935678	1169605	1403535	1637465	1871393	2105321	2339292
	PSNR	55,93	52,84	51,09	49,83	48,85	48,06	47,39	46,81	46,30	45,84
n=3	**Kapasite (bit)**	310680	621446	932218	1242986	1553752	1864518	2175286	2486050	2796818	3107663
	PSNR	50,21	47,11	45,37	44,10	43,14	42,34	41,67	41,09	40,58	40,13
n=4	**Kapasite (bit)**	384641	769402	1154175	1538936	1923702	2308465	2693227	3077991	3462753	3847631
	PSNR	44,29	41,22	39,47	38,21	37,23	36,45	35,77	35,19	34,68	34,23
n=5	**Kapasite (bit)**	446355	892873,5	1339386	1785895	2232403	2678914	3125422	3571933	4018444	4465063
	PSNR	38,49	35,42	33,67	32,41	31,44	30,65	29,97	29,39	28,87	28,42

Veri gizleme ve çıkarma için önerilen yöntemin hız testleri Tablo 4.7'de sunulmuştur. $n = 1\ ve\ 5$ Arası için, hız testi çalışmalarında bilgisayar tarafından her seferinde görüntünün kapasitesine göre rastgele oluşturulan gizli veriler farklı gri tonlamalı örtü görüntülere gizlenmiş ve çıkarılmıştır. Yapılan hız testleri incelendiğinde veri gizleme ve çıkarma sürelerinin arasında 20-25% kadar fark vardır. Veri çıkarma işlemi orijinal görüntünün geri getirilmesini gerektirdiği için gizlemeden uzun sürmektedir. Yine de çalışma süreleri birbirine yakın olduğu ve milisaniye cinsinden ölçüldüğü görülmektedir. Yükün artmasıyla veri saklama ve çıkarma sürelerinin arttığı ama birim zamanda gizlenen ve çıkartılan verinin korunduğu ölçülmüştür. Bu hız saniyede yaklaşık 65 milyon bit verinin gizlenmesine ve 50 milyon bit verinin çıkartılabilmesine karşılık gelmektedir.

Tablo 4.7. Ortalama veri gizleme ve çıkarma süreleri

		Test 1 (sn)	**Test 2 (sn)**	**Test 3 (sn)**	**Test 4 (sn)**	**Test 5 (sn)**	**Ortalama(sn)**
n=1	**Veri Gizleme**	0,0118	0,0131	0,0142	0,0149	0,0135	**0,0135**
	Veri Çıkarma	0,0156	0,0138	0,0154	0,0207	0,0146	**0,0160**
n=2	**Veri Gizleme**	0,0162	0,0160	0,0147	0,0160	0,0186	**0,0163**
	Veri Çıkarma	0,0190	0,0199	0,0174	0,0251	0,0195	**0,0202**
n=3	**Veri Gizleme**	0,0175	0,0196	0,0179	0,0190	0,0209	**0,0190**
	Veri Çıkarma	0,0221	0,0255	0,0219	0,0245	0,0235	**0,0235**
n=4	**Veri Gizleme**	0,0187	0,0213	0,0189	0,0204	0,0198	**0,0198**
	Veri Çıkarma	0,0248	0,0280	0,0246	0,0282	0,0247	**0,0260**
n=5	**Veri Gizleme**	0,0209	0,0220	0,0206	0,0239	0,0206	**0,0216**
	Veri Çıkarma	0,0273	0,0304	0,0273	0,0299	0,0268	**0,0283**

Tablo 4.8, literatürdeki ikili görüntü tabanlı veri gizleme yöntemlerinin önerilen tersinir veri gizleme yöntemiyle karşılaştırmasını sunmaktadır. Önerdiğimiz tersinir veri gizleme

yöntemi literatürdeki yöntemlere benzer sonuçlar vermektedir. Bazı çalışmalar, önerdiğimizden daha iyi PSNR değerleri sağlar.

Tablo 4.8. Önerilen yöntemin diğer çalışmalarla karşılaştırılması

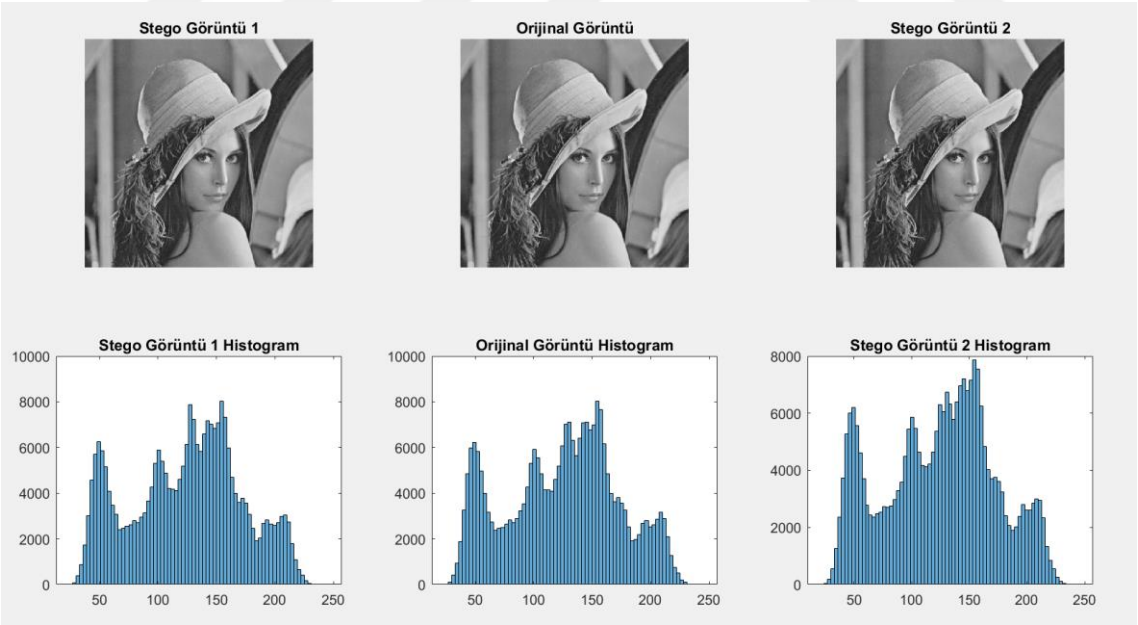
References	Measurement Metrics	Lena	Baboon	Peppers	Barbara	Goldhill	Average
Lu. T.C. (2015) - CFS	PSNR (dB) (Stego-1)	46,37	47,34	46,72	46,15	46,16	46,66
	PSNR (dB) (Stego-2)	46,36	46,56	46,12	46,71	46,64	46,55
	PSNR(Ortalama)	46,37	46,95	46,42	46,43	46,40	46,61
	KAPASİTE (Bit)	786432	786258	786670	786432	786432	786442
	Yük (bpb)	1,50	1,50	1,50	1,50	1,50	1,50
Shastri, S (2019) (Bozulma var, bozulma yı gidermek için harici şifre kullanır)	PSNR (dB) (Stego-1)	51,15	51,16	51,16	51,14	50,13	51,15
	PSNR (dB) (Stego-2)	50,18	50,17	50,18	50,16	50,18	50,17
	PSNR(Ortalama)	50,66	50,66	50,66	50,65	50,65	50,66
	KAPASİTE (Bit)	818914	818814	818948	819315	819386	819085
	Yük (bpb)	1,56	1,56	1,56	1,56	1,56	1,56
Jafar, I. F(2016).	PSNR (dB) (Stego-1)	48,70	48,71	48,71	48,70	48,72	48,71
	PSNR (dB) (Stego-2)	48,71	48,71	48,71	48,71	48,71	48,71
	PSNR(Ortalama)	48,71	48,71	48,71	48,71	48,72	48,71
	KAPASİTE (Bit)	650369	650799	650637	650781	650726	650568
	Yük (bpb)	1,24	1,24	1,24	1,24	1,24	1,24
Yao (2017) (Bozulma var)	PSNR (dB) (Stego-1)	45,93	46,38	47,20	46,38	46,83	46,65
	PSNR (dB) (Stego-2)	45,35	47,43	46,79	46,57	46,62	46,66
	PSNR(Ortalama)	45,64	46,91	47,00	46,48	46,73	46,66
	KAPASİTE (Bit)	819356	819080	818342	819156	819269	819034
	Yük (bpb)	1,56	1,56	1,56	1,56	1,56	1,56
Lee, C. F. (2013)	PSNR (dB) (Stego-1)	49,63	49,63	49,64	49,62	49,63	49,63
	PSNR (dB) (Stego-2)	49,63	49,61	49,63	49,63	49,62	49,63
	PSNR(Ortalama)	49,63	49,62	49,64	49,63	49,63	49,63
	KAPASİTE (Bit)	560801	560686	560572	561223	560740	560880
	Yük (bpb)	1,07	1,07	1,07	1,07	1,07	1,07
Lu, T. C. (2015) - LSB	PSNR (dB) (Stego-1)	49,20	49,21	49,19	49,22	49,23	49,21
	PSNR (dB) (Stego-2)	49,21	49,20	49,21	49,20	49,18	49,20
	PSNR(Ortalama)	49,21	49,21	49,20	49,21	49,21	49,21
	KAPASİTE (Bit)	524288	524204	524192	524288	524288	524257
	Yük (bpb)	1,00	1,00	1,00	1,00	1,00	1,00
[Lu, T. C. (2020)	PSNR (dB) (Stego-1)	47,34	47,34	47,34	47,34	47,34	47,34
	PSNR (dB) (Stego-2)	47,41	47,41	47,41	47,41	47,41	47,41
	PSNR(Ortalama)	47,37	47,38	47,37	47,37	47,37	47,37
	KAPASİTE (Bit)	917504	917504	917504	917504	917504	917504
	Yük (bpb)	1,75	1,75	1,75	1,75	1,75	1,75
Önerilen Yöntem (n = 1)	PSNR (dB) (Stego-1)	51,14	51,14	51,15	51,15	51,15	51,15
	PSNR (dB) (Stego-2)	51,14	51,13	51,14	51,15	51,14	51,14
	PSNR(Ortalama)	51,14	51,14	51,15	51,15	51,15	51,14
	KAPASİTE (Bit)	524288	524190	524104	524136	524136	524171
	Yük (bpb)	1,00	1,00	1,00	1,00	1,00	1,00
Önerilen Yöntem (n = 2)	PSNR (dB) (Stego-1)	46,12	46,23	46,16	46,07	46,11	46,14
	PSNR (dB) (Stego-2)	45,92	46,14	45,94	45,77	45,93	45,94
	PSNR(Ortalama)	46,02	46,19	46,05	45,92	46,02	46,04
	KAPASİTE (Bit)	786432	786222	786351	786144	786144	786259
	Yük (bpb)	1,50	1,50	1,50	1,50	1,50	1,50
Önerilen Yöntem (n = 3)	PSNR (dB) (Stego-1)	40,37	40,40	40,30	40,23	40,33	40,33
	PSNR (dB) (Stego-2)	40,33	40,44	40,21	40,14	40,18	40,26
	PSNR(Ortalama)	40,35	40,42	40,26	40,19	40,26	40,29
	KAPASİTE (Bit)	1048576	1047832	1047896	1048168	1048168	1048128
	Yük (bpb)	2,00	2,00	2,00	2,00	2,00	2,00

n = 1 ve 3'e göre örtü, stego1 ve stego2 görüntülerinin piksel değeri dağılımlarını gösteren bir analiz gerçekleştirilmiştir. Şekil 4.3, 4.4 ve 4.5'te, gri tonlamalı bir Lena görüntüsünde

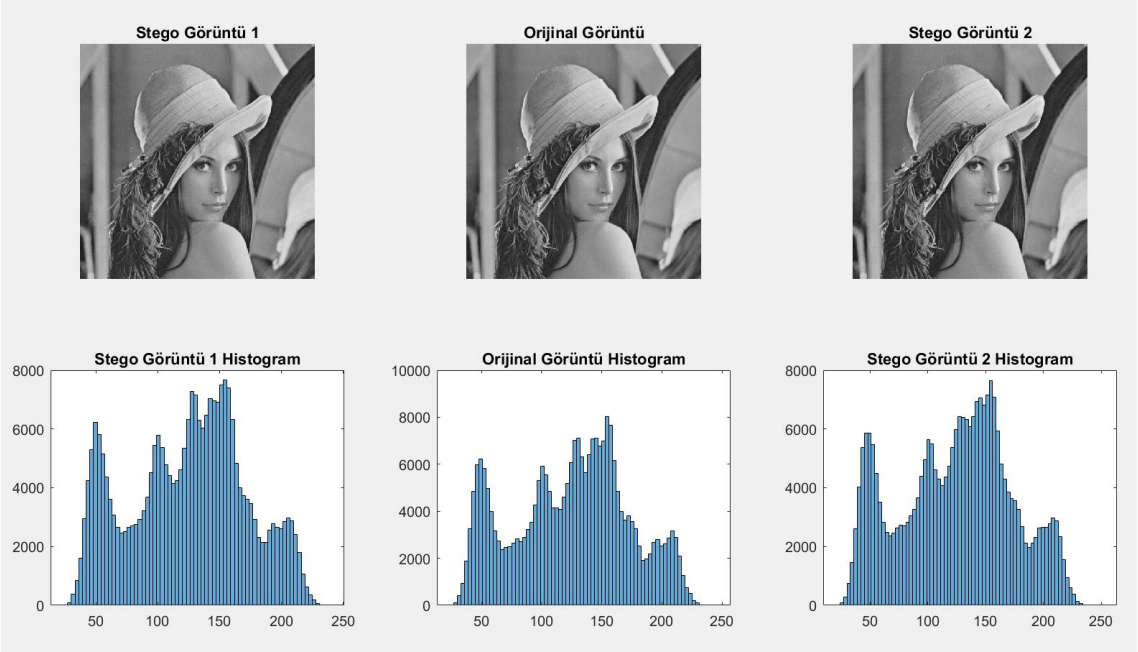
n = 1 ila 3 için histogram analizlerini göstermektedir. Burada stego görüntülerde gizli veri olduğuna dair kuşku uyandıracak bir karakteristik özellik gözlenmemiştir.



Şekil 4.3. N=1 için Lena görüntüsüne ait görüntülerin piksel dağılımları



Şekil 4.4. N=2 için Lena görüntüsüne ait görüntülerin piksel dağılımları



Şekil 4.5. N=3 için Lena görüntüsüne ait görüntülerin piksel dağılımları

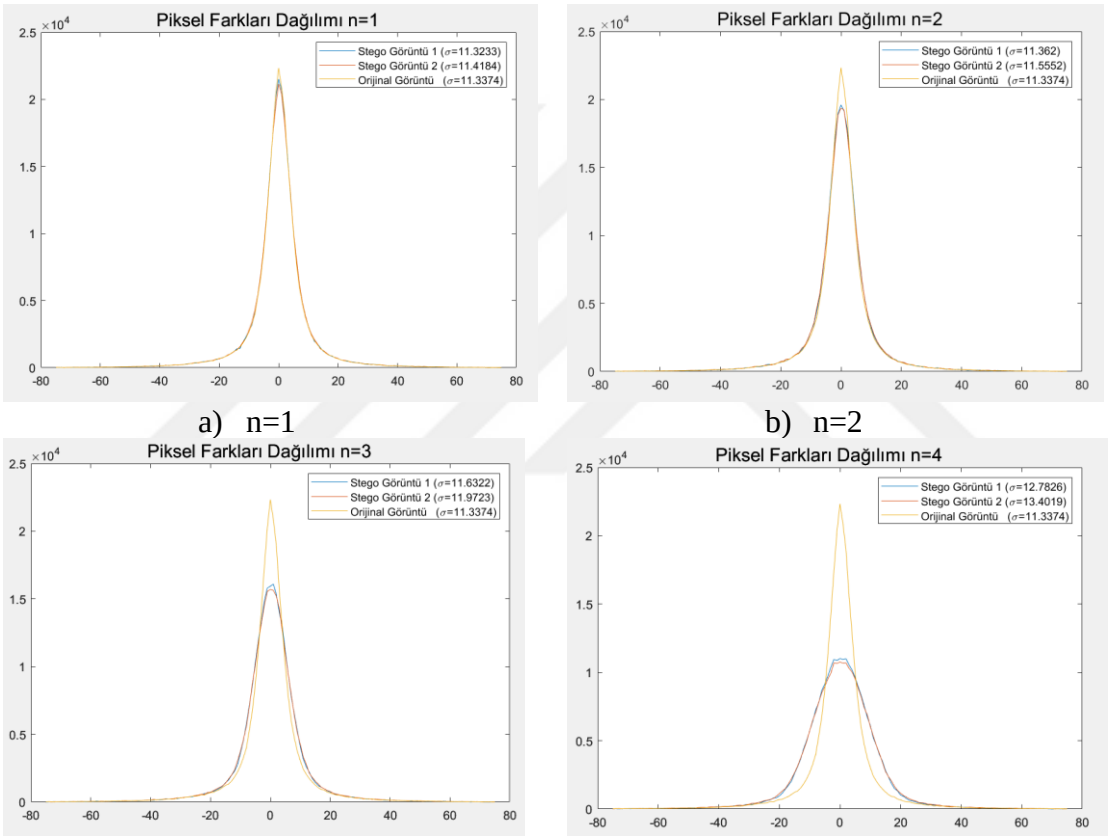
Deneyde ayrıca görüntüler üzerinde yapısal benzerlik indeksi ölçümü de yapılmıştır. Orijinal görüntü ile stego görüntülerin benzerliklerinin yanı sıra, gizleme sonrası elde edilen iki stego görüntünün birbirine olan yapısal benzerlikleri de ölçülmüştür. Yapılan ölçümde elde edilen sonuçlar n=1,2,3 ve 4 için Tablo 4.9'da verilmiştir. Ölçümler sonucunda hem stego görüntüler ile orijinal görüntü arasında hem de iki stego görüntü arasında yüksek yapısal benzerlik gözlemlenmiştir.

Tablo 4.9. SSIM ölçüm sonuçları

Metot	Lena 512x512		Baboon 512x512		Pepper 512x512		Airplane 512x512		Stego1-Stego2			
	Orijinal- Stego1	Orijinal- Stego2	Orijinal- Stego1	Orijinal- Stego2	Orijinal- Stego1	Orijinal- Stego2	Orijinal- Stego1	Orijinal- Stego2	Lena	Baboon	Peppers	Airplane
n=1	99,98%	99,98%	99,97%	99,97%	99,98%	99,98%	99,76%	99,65%	99,94%	99,91%	99,94%	99,12%
n=2	99,93%	99,93%	99,90%	99,90%	99,94%	99,93%	98,71%	98,88%	99,76%	99,64%	99,77%	98,90%
n=3	99,75%	99,76%	99,63%	99,64%	99,77%	99,77%	98,19%	98,19%	99,04%	98,60%	99,10%	97,21%
n=4	99,03%	99,08%	98,88%	98,95%	99,12%	99,14%	97,47%	97,59%	97,30%	97,66%	97,61%	96,79%

Güvenlik testlerinde kullanılan ikinci yöntem ise PDH olarak adlandırılan piksel farklılıklarının dağılımını elde etmektir. PDH diyagramında örtü görüntüsünün sıfır ortalama normal dağılıma göre olması beklenir. Bazı veri gizleme yöntemleri kullanılarak

alınan stego görüntü PDH'de, dağılım eğrisinin zikzak çiziyor olması, periyodik olarak düzlükler oluşturması, birden fazla tepe oluşturması gibi göze çarpan davranışlar gözlemlenebilir. Ayrıca iki stego görüntünün dağılımlarının birbirine benzerliği ikili görüntü tabanlı tersinir veri gizleme yöntemlerinde bir kriter olabilir. Önerilen veri gizleme yöntemi için, n = 1-4 değerleri için PDH'ler Şekil 4.6'da sunulmuştur. Tablo 4.11'den tüm n değerleri için iki stego görüntünün PDH grafiklerinin birbiriyle örtüştüğü görülmektedir. Ayrıca n=1 ile 3 için örtü ve stego görüntüleri PDH analizlerinin birbirine yakın olduğu görülmektedir.



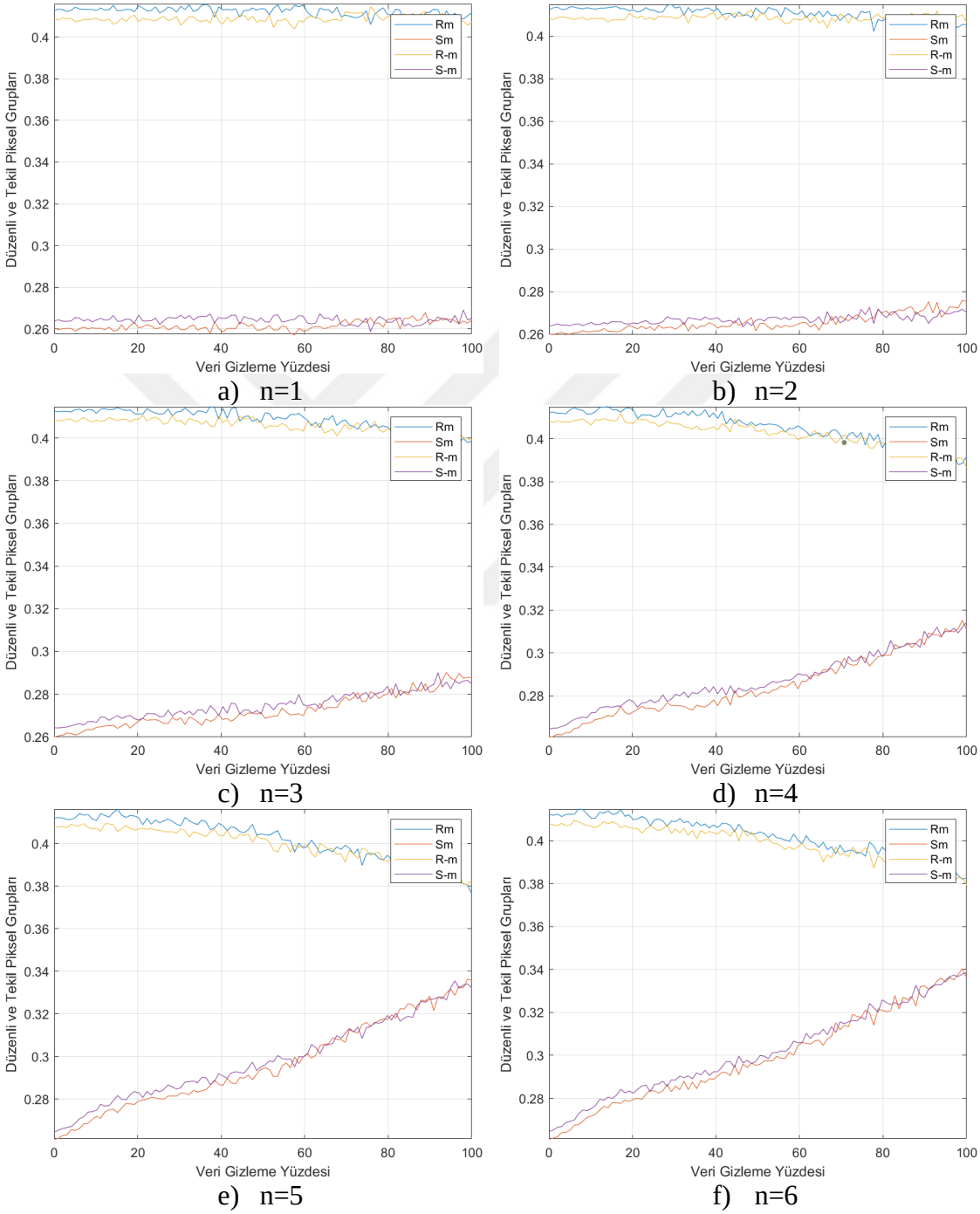
a) n=1 b) n=2

c) n=3 d) n=4

Şekil 4.6. Ardışık piksel değerleri farklarının dağılımı

Son olarak, algoritmanın güvenliğini ölçmek için Düzenli (R) ve Tekil (S) piksel gruplarının oranını ölçen RS analizi adı verilen istatistiksel bir steganaliz yöntemi kullanıldı. Bu analizde normal piksel gruplarının (Rm, R-m) tekil piksel grubunun (Sm, S-m) oranından küçük olması görüntüde bozulma olduğunu, yani gizli veri gömülü olabileceğini gösterir. Bunun tersi olduğunda yani "Sm ≈ S-m < Rm ≈ R-m" ifadesi verildiğinde o görüntünün normal olduğu düşünülür. (Rm, R-m) değerleri ile (Sm, S-m)

değerleri arasındaki fark arttığında görüntüde gizli veri olduğu anlaşılır. Şekil 4.7, önerilen yöntem için RS analizi sonuçlarını sunar. Şekil 4.7 incelendiğinde, önerilen yöntemin stego görüntüsünde yüksek gizli veri kapasitesi olsa bile steganaliz saldırılarına karşı dirençli olduğu kanıtlanmıştır.



Şekil 4.7. N=1-4 için RS analizi sonuçları

5. SONUÇ

Bu tez çalışmasında yeni bir çift görüntü tabanlı veri gizleme algoritması önerilmiştir. Algoritma, veri gizleme işleminde gizli verileri kayıpsız şekilde gizlemeyi ve orijinal görüntüyle gizli verinin her ikisini de kayıpsız olarak çıkarmayı başarmıştır. Veri gizleme algoritması, yüksek gömme kapasitesi ve güvenliği sağlamak için merkez kaydırma tekniğini ve en önemli bitleri kullanır. En orijinal görüntüye ait en önemli bitler bir nevi şifre görevi gördüğü için veri çıkartma işlemi sırasında gizli verinin çıkarılması orijinal görüntüye sahip olmayı gerektirir. Dolayısıyla orijinal görüntü elde edilmeden veri çıkarmak olanaksızdır.

Algoritma en yüksek PSNR başarımını en düşük n ($n = 1$) değerinde vermektedir. Kapasite başarımını ise n değeri arttıkça artmaktadır. PSNR ile kapasite başarımları birbirine ters düşmektedir. İkisinin başarımı birlikte göz önüne alındığında $n = 4$ değeri en kullanışlı seviyedir. Aslında bu başarım n sayısı arttırıldıkça artmaktadır fakat $n = 5$ ve üzerindeki seviyelerde kabul edilir PSNR değeri olan 30 dB seviyesinin altına düşüldüğü için $n = 5$ üzerindeki seviyeler kullanılamaz. Burada $n = 4$ seviyesinde 512x512 boyutundaki 8 bitlik gri renkli bir görüntüye yaklaşık 1,31 milyon bit veri gizlenebilmektedir. Bu gri renkli bir görüntüde her piksel bir bay olduğu için bu oran iki görüntü kullanıldığını düşünürsek bayt başına 2,5 bit olarak hesaplanır. Bu seviyede tam doluluk oranında PSNR değeri 34 dB olarak ölçülmüştür. Daha düşük kapasitenin yeterli olduğu durumlarda PSNR başarımını arttırmak için daha küçük n değerleri tercih edilerek PSNR seviyesi 62'ye kadar yükseltilebilir. Görüntünün gizleme kapasitesinin tamamen kullanıldığı durumunda en yüksek PSNR başarımı $n = 1$ yaklaşık 51 dB olarak sağlanmıştır.

Oluşturulan stego görüntüler sadece orijinal görüntüyle değil birbiriyle de benzer görünürler. Her iki stego görüntü de orijinal görüntüye benzer PSNR oranlara sahiptir. Stego görüntülerin orijinal görüntüye olan yapısal benzerlikleri (SSIM) en kötü senaryoda bile 97%'nin üzerindedir. Stego görüntülerin birbirine olan PSNR oranı ve yapısal benzerlikleri orijinal görüntüyle yapılan kıyaslamadan daha farklı sonuçlar vermemektedir.

Önerilen yöntem ölçümü yapılan bütün steganaliz yöntemlerinden başarıyla geçmiştir. Yönteme PSNR ve SSIM haricinde Histogram, RS ve PDH analizleri de uygulanmıştır.

Stego ve örtü görüntünün piksel değerleri histogramları çıkartılmıştır. Hiçbir seviyede Taraklanma, tavan ya da taban yapma, ardışık sütün değerlerinin birbirine yaklaşıp özellikle tepelerin ve çukurların yassılaşması ve ayrışma (her iki tarafında da sıfır göstermeyen değerler olmasına rağmen tekrarlanmayan değer aralığı) gibi hiçbir olumsuzluğa rastlanmamıştır.

Piksel farkları dağımı analizi hem orijinal hem de gizleme sonrası oluşan iki stego görüntüye uygulanmıştır. Bir görüntünün piksel farklarının normal dağılıma uygunluk göstermesi beklenir. Yapılan analiz sonucunda orijinal görüntünün piksel farkları dağılımı beklendiği gibi normal dağılıma uygunluk göstermiştir. Stego görüntülerin piksel farkları dağılımı, orijinal görüntünün taşıdığı dağılıma sahiptir. Stego görüntülerde her ne kadar sigma seviyesi artmış olsa da burada orijinal görüntü asla taşıma sırasında kullanılmadığı için bu sigma değerinin artması durumumu bir anlam ifade etmez. En önemli olan şey stego görüntülerin sahip olduğu piksel farkları dağılımlarının sahip oldu dağılımlara uygunluklarının eşdeğer olması ve bu dağılımların üst üste koyulduğunda birbiriyle örtüşmesidir. Çünkü taşıyıcı sadece stego görüntüleri taşıyacak ve bunları kıyaslayabilecektir. Yapılan çalışmada ise stego görüntülerin piksel farkları dağılımlarının özdeş sigma değerlerine sahip oldukları ve dağılımların birbiriyle örtüştüğü görülmüştür. Ayrıca bu dağılımda çoğunlukla histogram kaydırma tabanlı yöntemlerde görülen çift merkezli dağılım, piksel değerleri farkları (PVD- Pixel Value Difference) gibi yöntemlerde kullanılan basamaklaşma veya zikzak çizme gibi olumsuz etkilerin hiçbirisiyle karşılaşılmamıştır.

Ayrıca, deneysel sonuçlar, algoritmanın RS saldırılarına karşı dayanıklı olduğunu göstermektedir. Yapılan RS analizi sonucunda kabul edilebilir PSNR seviyesinin dışında kalan n değerlerinde bile tekil piksel grubunun oranından küçük olması durumunda rastlanılmamıştır. Bu da RS analizinde gizli veri olduğunun anlaşılamadığı anlamına gelir.

Veri gizleme ve çıkarma işlemi çok kısa bir zaman aralığında yapılabilmektedir. Algoritmanın çalışma hızı yani birim zamanda gizlenen ya da çıkartılan veri miktarı,

verinin büyüklüğünden veya kullanılan n seviyesinden etkilenmemektedir. Matlab programının 2022b sürümünde yapılan ölçümlerde bir saniyede yaklaşık 65 milyon bit gizlenebilmekte ya da 50 milyon bit çıkartılabilmektedir. Bu hız 7-8 MB/s ye denk gelmektedir. Bir gigabayt verinin gizlenmesi tahmini iki dakika on saniye gibi kısa bir süre içinde yapılabilmektedir, aynı boyutta verinin çıkartılması ise yaklaşık iki dakika kırk saniye sürecektir.

Önerilen algoritmanın diğer yöntemlerle kıyaslandığında, bozulmayı kabul etmeyen ve harici bir veri parçası göndermeyi gerektirmeyen bütün yöntemlerden kapasite ve PSNR açısından geride kalmadı bazen de öne geçebildiği görülmüştür. Ayrıca, önerilen veri gizleme yöntemi kullanılan n seviyesi sayesinde kullanım esnekliği sağlamaktadır. Kullanıcı ihtiyacına göre yüksek PSNR ya da yüksek kapasite başarımı arasında seçim yapılabilir.

KAYNAKLAR

Castleman, K. R. (1996). *Digital image processing* (5th ed). New Jersey: Prentice Hall.

Chang, C. C., Kieu, T. D.,Chou, Y. C. (2007). Reversible data hiding scheme using two steganographic images. *TENCON 2007-2007 IEEE Region 10 Conference*, Taipei, Taiwan 30 October 2007 - 02 November 2007.

Chang, C. C., Lu, T. C., Horng, G., Huang, Y. H.,Hsu, Y. M. (2013). A high payload data embedding scheme using dual stego-images with reversibility. *2013 9th International Conference on Information, CommunicationsSignal Processing*, Tainan, Taiwan, 10-13 December 2013.

Chen, Y. Q., Sun, W. J., Li, L. Y., Chang, C. C.,Wang, X. (2020). An efficient general data hiding scheme based on image interpolation. *Journal of Information Security and Applications, 54*, 102584.

Chi, L. P., Wu, C. H.,Chang, H. P. (2018). Reversible data hiding in dual stegano-image using an improved center folding strategy. *Multimedia Tools and Applications, 77*(7), 8785-8803.

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

Evans, M., Hastings, N., Peacock, B.,Forbes, C. (2011). *Statistical distributions*. New York: John Wiley & Sons.

García, S., Ramírez-Gallego, S., Luengo, J., Benítez, J. M., Herrera, F. (2016). Big data preprocessing: methods and prospects. *Big Data Analytics, 1*(1), 1-22.

Gui, X., Li, X.,Yang, B. (2014). A high capacity reversible data hiding scheme based on generalized prediction-error expansion and adaptive embeding. *Signal Processing, 98*, 370-380.

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

Habibi Lashkari, A., Abdul Manaf, A., Masrom, M.,Mohd Daud, S. (2011). A survey on image steganography algorithms and evaluation. *International Conference on Digital Information Processing and Communications* Berlin, Germany, 7-9 July 2011.

Hajizadeh, H., Ayatollahi, A.,Mirzakuchaki, S. (2013). A new high capacity and EMD-based image steganography scheme in spatial domain, *2013 21st Iranian Conference on Electrical Engineering (ICEE)*, Mashhad, Iran, 14-16 May 2013.

Hamid, N., Sumait, B. S., Bakri, B. I.,Al-Qershi, O. (2021). Enhancing visual quality of spatial image steganography using SqueezeNet deep learning network. *Multimedia Tools and Applications, 80*(28), 36093-36109.

Hassaballah, M. (2020). *Digital media steganography: principles, algorithms, and advances* (1st ed). Cambridge: Academic Press.

Hassan F. S., Gutub A., (2020). Efficient reversible data hiding multimedia technique based on smart image interpolation. *Multimedia Tools and Applications, 79*(39), 30087-30109.

Hu J., Li T., (2015). Reversible steganography using extended image interpolation technique. *ComputersElectrical Engineering, 46*, 447-455.

Huynh-Thu, Q.,Ghanbari, M. (2008). Scope of validity of PSNR in image/video quality assessment. *Electronics letters, 44*(13), 800-801.

Jafar, I. F., Darabkh, K. A., Al-Zubi, R. T.,Saifan, R. R. (2016). An efficient reversible data hiding algorithm using two steganographic images. *Signal Processing, 128*, 98-109.

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

Jung K. H., Yoo K. Y., (2009). Data hiding method using image interpolation. *Computer StandardsInterfaces, 31*(2), 465-470.

Jung, K. H. (2016). A survey of reversible data hiding methods in dual images. *IETE Technical Review, 33*(4), 441-452.

Jung, K. H. (2018). A survey of interpolation-based reversible data hiding methods. *Multimedia Tools and Applications, 77*(7), 7795-7810.

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.

Khan, F., Gutub, A. (2007). Message concealment techniques using image based steganography, *The 4th IEEE GCC Conference*, Riffa, Bahrain, 11-14 Nov. 2007.

Kaur, S., Bansal, S.,Bansal, R. K. (2014). Steganography and classification of image steganography techniques, *2014 International Conference on Computing for Sustainable Global Development*, New Delhi, India, 05-07 March 2014.

Kim, P. H., Ryu, K. W.,Jung, K. H. (2020), Reversible data hiding scheme based on pixel-value differencing in dual images, *International Journal of Distributed Sensor Networks, 16*(7), 1550147720911006.

Lee, C. F., Wang, K. H., Chang, C. C.,Huang, Y. L. (2009, February). A reversible data hiding scheme based on dual steganographic images. *Proceedings of the 3rd international conference on ubiquitous information management and communication*, Suwon, Korea,15 February 2009.

Lee, C. F.,Huang, Y. L. (2013). Reversible data hiding scheme based on dual stegano-images using orientation combinations. *Telecommunication Systems, 52*(4), 2237-2247.

Li, X., Li, J., Li, B.,Yang, B. (2013). High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. *Signal processing, 93*(1), 198-205.

Li, X., Yang, B., Zeng, T. (2011). Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection. *IEEE transactions on image processing, 20*(12), 3524-3533.

Loukides, M. (2011). *What is data science?* California: O'Reilly Media, Inc..

Lu, T. C., Chang, T. C., Shen, J. J. (2020). An Effective Maximum Distortion Controlling Technology in the Dual-Image-Based Reversible Data Hiding Scheme. *IEEE Access, 8*, 90824-90837.

Lu, T. C., Huang, S. R.,Huang, S. W. (2021). Reversible hiding method for interpolation images featuring a multilayer center folding strategy. *Soft Computing, 25*(1), 161-180.

Lu, T. C., Tseng, C. Y.,Wu, J. H. (2015). Dual imaging-based reversible hiding technique using LSB matching. *Signal Processing*, 108, 77-89.

Lu, T. C., Wu, J. H.,Huang, C. C. (2015). Dual-image-based reversible data hiding method using center folding strategy. *Signal Processing, 115*, 195-213.

Lu, T. C., & Vo, T. N. (2019). Introduction of Reversible Data Hiding Schemes. *Proceedings of the 3rd International Conference on Security with Intelligent Computing and Big-data Services (SICBS)*, New Taipei City, Taiwan, 4–6 December 2019.

Lu, T. C., & Vo, T. N. (2020). Reversible steganography techniques: A survey. Hassaballah, M., *Digital Media Steganography* (1st Ed) (189-213). Cambridge: Academic Press.

Malik, A., Sikka, G., Verma, H. K. (2020). A reversible data hiding scheme for interpolated images based on pixel intensity range. *Multimedia Tools and Applications, 79*, 18005-18031.

Meikap, S.,Jana, B. (2021). Improved center-folding based directional pixel value ordering for reversible data hiding scheme. *Multimedia Tools and Applications, 80(*4), 5617-5652.

Neeta, D., Snehal, K.,Jacobs, D. (2006). Implementation of LSB steganography and its evaluation for various bits. *2006 1st international conference on digital information management,* Bangalore, India, 06 December 2006.

Ni, Z., Shi, Y. Q., Ansari, N.,Su, W. (2006). Reversible data hiding. *IEEE Transactions on circuits and systems for video technology, 16*(3), 354-362.

Qin, C., Chang, C. C.,Hsu, T. J. (2015). Reversible data hiding scheme based on exploiting modification direction with two steganographic images. *Multimedia Tools and Applications, 74*(15), 5861-5872.

Runkler, T. A. (2020). *Data analytics*. Springer Fachmedien Wiesbaden (3rd ed). Muchen: Springer Vieweg Wiesbaden.

Sallee, P. (2005). Model-based methods for steganography and steganalysis. *International Journal of Image and graphics, 5*(01), 167-189.

Setiadi, D. R. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications, 80*(6), 8423-8444.

Shastri, S.,Thanikaiselvan, V. (2019). Dual image reversible data hiding using trinary assignment and centre folding strategy with low distortion. *Journal of Visual Communication and Image Representation, 61*, 130-140.

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

Solak, S. (2020). High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms. *IEEE Access, 8*, 166513-166524.

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.

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

Stefan, K., Fabien, A. P. (2000). *Information hiding techniques for steganography and digital watermarking* (1st ed). London: Artech House.

Sun, Y., Zhang, J., Xiong, Y., Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks, 10*(7), 190903.

Şahin, A., Buluş, E., Sakallı, M. (2006). 24-bit renkli resimler üzerinde en önemsiz bite ekleme yöntemini kullanarak bilgi gizleme. *Trakya Üniversitesi Fen Bilimleri Dergisi, 7*(1), 17-22.

Tian, J. (2003). Reversible data embedding using a difference expansion. *IEEE transactions on circuits and systems for video technology, 13*(8), 890-896.

Tsai, P., Hu, Y. C.,Yeh, H. L. (2009). Reversible image hiding scheme using predictive coding and histogram shifting. *Signal processing, 89*(6), 1129-1143.

Wang, S. Y., Li, C. Y.,Kuo, W. C. (2013). Reversible data hiding based on two-dimensional prediction errors. *IET image processing, 7*(9), 805-816.

Wang, S., Yang, B.,Niu, X. (2010). A secure steganography method based on genetic algorithm. *J. Inf. Hiding Multim, Signal Process., 1*(1), 28-35.

Wang, X. T., Chang, C. C., Nguyen, T. S.,Li, M. C. (2013). Reversible data hiding for high quality images exploiting interpolation and direction order mechanism. *Digital Signal Processing, 23*(2), 569-577.

Yalman, Y., Özdemir, Ç., Ertürk, İ., & Akar, F. (2014). *Veri gizleme (Birinci Baskı)*. İstanbul: Beta.

Yang C. N., Hsu S. C., Kim C., (2017). Improving stego image quality in image interpolation based data hiding. *Computer Standards Interfaces*, 50, 209-215.

Yao, H., Qin, C., Tang, Z.,Tian, Y. (2017). Improved dual-image reversible data hiding method using the selection strategy of shiftable pixels' coordinates with minimum distortion. *Signal Processing, 135*, 26-35.

Zhang, D. (2018). Big data security and privacy protection. *8th international conference on management and computer science (ICMCS 2018)*, Zhengzhou, China, 1 October 2018.

Zhang, X., Peng, F.,Long, M. (2018). Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*, 20(12), 3223-3238.

Zhao, J., Koch, E. (1995). Embedding Robust Labels into Images for Copyright Protection, *KnowRight '95: Proceedings of the conference on Intellectual property rights and new Technologies*, Munich, Germany, 1 January 1995.

Zhao, Z., Luo, H., Lu, Z. M.,Pan, J. S. (2011). Reversible data hiding based on multilevel histogram modification and sequential recovery. *AEU-International Journal of Electronics and Communications*, 65(10), 814-826.

KİŞİSEL YAYIN VE ESERLER

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

Tezcan, G., Solak, S. (2020). An Investigation of the Relationship between Agricultural Production and Greenhouse Gas Emissions. *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications,* Ankara, Türkiye, 26-28 June 2020.

ÖZGEÇMİŞ

İlk ve orta okul eğitimimi Çanakkale'de Mustafa kemal ilk öğretim okulunda tamamladım. Lise eğitimime 2011 yılında eski Adıyla Milli Piyango Anadolu Lisesinin İngilizce bölümünde başladım ve 2015 yılında yeni adıyla Vahit Tuna Anadolu Lisesinden Mezun Oldum. 2015 Yılında Lisans Eğitimim için Kocaeli'ne geldim ve Kocaeli Üniversitesi'nin Endüstri Mühendisliği Bölümünden mezun oldum. Ardından 2019 yılının başında Kocaeli Üniversitesi'nin Bilişim sistemleri bölümünde yüksek lisansıma başladım ve devam etmekteyim. Aktif olarak Palazoğlu Tarım Aletlerinde R&D Mühendisliği yapmaktayım.