

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ



**UYDU İMGELERİNE STEGANOĞRAFİK YÖNTEMLER
KULLANARAK KONUM VE YER BİLGİSİ GİZLEME**

Fatma Nur SÖNMEZ

Yüksek Lisans Tezi

EKOİLİŞİM ANABİLİM DALI

Ekobilışım Bilim Dalı

OCAK 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ekobilışım Anabilim Dalı

Yüksek Lisans Tezi

UYDU İMGELERİNE STEGANOĞRAFİK YÖNTEMLER KULLANARAK KONUM VE YER BİLGİSİ GİZLEME

Tez Yazarı
Fatma Nur SÖNMEZ

Danışman
Doç. Dr. Derya AVCI

OCAK 2022
ELAZIĞ

T.C.
FIRATÜNİVERSİTESİ
FENBİLİMLERİENSTİTÜSÜ

Ekobilişim Anabilim Dalı

Yüksek Lisans Tezi

Başlığı: Uydu İmgelerine Steganografik Yöntemler Kullanarak Konum Ve Yer Bilgisi Gizleme

Yazarı: Fatma Nur SÖNMEZ

İlk Teslim Tarihi: 13.12.2021

Savunma Tarihi: 14.01.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık Yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

Danışman:	Doç. Dr. Derya AVCI Fırat Üniversitesi, Teknik Bilimler Meslek Yüksek Okulu	<i>İmza</i> Onayladım
Başkan:	Dr. Öğr. Üyesi Murat AYDOĞAN Fırat Üniversitesi Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Hüseyin KUTLU Adıyaman Üniversitesi Besni Meslek Yüksek Okulu	Onayladım

Bu tez, Enstitü Yönetim Kurulunun/...../20..... tarihli toplantısında tescillenmiştir.

İmza
Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım “ Uydu İmgelerine Steganografik Yöntemler Kullanarak Konum Ve Yer Bilgisi Gizleme ” Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

14.01.2022

Fatma Nur SÖNMEZ



ÖNSÖZ

Yaygın olarak kullanılan veri gizleme yöntemlerinden steganografi de dikkat edilmesi gereken en önemli unsurlardan biri güvenilirliktir. Güvenilir bir steganografi de görünmezlik, güvenlik, kapasite ve sağlamlık gibi unsurlar göz önünde bulundurulmalıdır. Bu unsurlardan biri gözetilmediğinde veri gizliliği ve güvenilirliği ihlal edilmiş olmaktadır. Steganografik yöntemlerden en az anlamlı bit(LSB) tekniği kullanılarak uydu üzerinden alınan 14 farklı görüntü 128x128 ve 256x256 boyutlarına getirilerek veri gizleme işlemi yapılmıştır. Gizlenen verilerin boyutu arttırılarak, farklı bitlere veri gizleme işlemi yapılarak görüntülerdeki bozulmalar gözlemlenmiştir. Gizlenecek verinin tersi alınıp veri gizleme işlemi yapılarak tepe sinyal gürültü oranına (PSNR) etkisine bakılmıştır.

Çalışmalarım sırasında yakın ilgi, anlayış gördüğüm ve beni destekleyip motive eden danışman hocam Doç. Dr. Derya AVCI'ya ve tez konusu için önerilerde bulunan Prof. Dr. Engin AVCI' ya, uygulamalarım sırasında oluşan hatayı çözmeme yardım eden çalışma arkadaşım Emrullah EZBERCİ' ye, çalışmam süresince manevi desteklerini esirgemeyen aileme ve arkadaşlarıma teşekkür eder, saygılarımı sunarım.

Fatma Nur SÖNMEZ
ELAĞ, 2022

İÇİNDEKİLER

SAYFA

ÖNSÖZ.....	iv
İÇİNDEKİLER.....	v
ÖZET.....	vi
ABSTRACT.....	vii
ŞEKİLLER LİSTESİ.....	viii
TABLolar LİSTESİ.....	ix
SİMGELER VE KISALTMALAR.....	x
1. GİRİŞ.....	1
2. STEGANOĞRAFI.....	4
2.1. Steganografi Çeşitleri.....	5
2.1.1. Metin Steganografisi.....	5
2.1.2. Video Steganografisi.....	6
2.1.3. Ses Steganografisi.....	6
2.1.4. Protokol Steganografisi.....	6
2.1.5. Görüntü Steganografisi.....	6
2.2. Steganaliz.....	8
2.2.1. Görsel Steganaliz.....	9
2.2.2. İstatistiksel Steganaliz.....	9
2.2.2.1 Histogram Tabanlı Analiz.....	9
2.2.2.2 RS Steganaliz.....	9
2.2.2.3 Ki-Kare Analizi.....	10
2.2.2.4 Bit Düzlem Analizi.....	10
2.2.3. Yapısal Olmayan Steganaliz.....	10
3. EN AZ ANLAMLI BİT (LSB) TEKNİĞİ.....	11
4. MATERYAL METOT.....	13
5. BULGULAR VE TARTIŞMA.....	20
6. SONUÇLAR.....	33
KAYNAKLAR.....	34
ÖZGEÇMİŞ.....	

ÖZET

Uydu İmgelerine Steganografik Yöntemler Kullanarak Konum Ve Yer Bilgisi Gizleme

Fatma Nur SÖNMEZ

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü

Ekobilişim Anabilim Dalı

Ocak 2022, Sayfa: x +35

Dijital ortamda veri aktarılırken veri güvenliği ve gizliliği giderek daha önemli hale gelmiştir. Bunu sağlamak için birçok yöntem geliştirilmiştir. Steganografi de bu yöntemlerden biridir. Steganografi, mesajları veya verileri bir medyaya gizleme bilimidir. Steganografi de veriler karşı tarafa aktarılırken video, ses, metin, protokol ve görüntü gibi ortamlar kullanılır. Görüntü steganografisinin de yaygın olarak kullanılan yöntemlerden biri an az anlamlı bit (LSB) tekniğidir. Bu çalışma da uydu üzerinden almış olduğumuz 128x128 ve 256x256 boyutlarında ki 14 farklı imgeye konum ve yer bilgisi LSB tekniği kullanılarak 6, 7 ve 8. bite gizlenmiştir. Görüntülerde ki bozulmaları önlemek ve PSNR değerini arttırmak için gizlenen verilerin tersi alınıp veri gizleme işlemi yapılmıştır. PSNR değeri hesaplanıp görüntüde ki bozulmalar gözlemlenmiştir.

Anahtar Kelimeler: Steganografi, Görüntü Steganografisi, LSB Tekniği, PSNR Değeri, Veri Gizleme

ABSTRACT

Hiding Location and Location Information to Satellite Images Using Steganographic Methods

Fatma Nur SÖNMEZ

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences
Department of Eco-informatics

January 2022, Pages: x + 35

Data security and privacy have become more and more important when transferring data in the digital environment. Many methods have been developed to achieve this. Steganography is one of these methods. Steganography is the science of hiding messages or data in a media. Steganography also uses media such as video, audio, text, protocol, and image, while data is transferred to the opposite party. One of the commonly used methods in image steganography is the least significant bit (LSB) technique. In this study, the location and location information of 14 different images in 128x128 and 256x256 dimensions that we received over the satellite have been hidden in 6, 7 and 8 bits by using LSB technique. In order to prevent distortions in the images and to increase the PSNR value, the data hiding has been performed by inverting the hidden data. PSNR value has been calculated and the distortions in the image have been observed.

Keywords:Steganography, Image Steganography, LSB Technique, PSNR Value, Data Hiding

ŞEKİLLER LİSTESİ

	Sayfa
Şekil 2.1. Steganografi ile veri oluşturulması ve gizli verinin elde edilmesi.....	4
Şekil 2.2. Steganografik Ortamlar	5
Şekil 2.3. Görüntüler de steganografik diyagram	7
Şekil 2.4. (a) hedeflenen hedefleri ile görüntü steganografik alanlar, (b) görüntü kodlu format tabanlı gömme teknikleri, (c) gizli mesaj formatına dayalı steganografik teknikler.....	8
Şekil 3.1. İkili kodda üç piksel değeri	11
Şekil 3.2. LSB' de veri gizlendikten sonra üç piksel değeri	11
Şekil 4.1. Ascii kod karşılığının ikilik forma çevrilmesini sağlayan sözde kod	18
Şekil 4.2. 6, 7 ve 8. bite gizleme işlemini gösteren sözde kod	18
Şekil 4.3. Gizleme işleminde verilerin tersini alan fonksiyonun sözde kodu	19
Şekil 5.1. 128x128 boyutunda ki orijinal görüntü	25
Şekil 5.2.128x128 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü.....	25
Şekil 5.3. 128x128 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü.....	25
Şekil 5.4. 256x256 boyutunda ki orijinal görüntü	27
Şekil 5.5. 256x256 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü.....	27
Şekil 5.6. 256x256 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü.....	27
Şekil 5.7. 128x128 boyutunda ki orijinal görüntü	29
Şekil 5.8. 128x128 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü	29
Şekil 5.9. 128x128 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü.....	29
Şekil 5.10. 256x256 boyutunda ki orijinal görüntü	31
Şekil 5.11. 256x256 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü.....	31
Şekil 5.12. 256x256 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü.....	32
Şekil 5.13. 128x128 ve 256x256 büyüklüğünde ki 14 görüntüye verilerin üç katı büyüklüğü alınıp tersi işlemi uygulandıktan sonra ki PSNR değerleri	32

TABLÖLAR LİSTESİ

	Sayfa
Tablo 4.1. Uydu üzerinden alınmış 128X128 ve 256X256 boyutunda ki imgeler.....	13
Tablo 5.1. 128X128 boyutunda ki görüntülerde son bir bite gömme işlemi yapıldığında oluşan metrik değerler	20
Tablo 5.2. 256X256 boyutunda ki görüntülerde son bir bite gömme işlemi yapıldığında oluşan metrik değerleri	21
Tablo 5.3. 128X128 boyutunda ki görüntülerde son iki bite gömme işlemi yapıldığında oluşan metrik değerleri	22
Tablo 5.4. 256X256 boyutunda ki görüntülerde son iki bite gömme işlemi yapıldığında oluşan metrik değerleri	23
Tablo 5.5. 128X128 boyutunda ki görüntülerde son üç bite gömme işlemi yapıldığında oluşan metrik değerleri	24
Tablo 5.6. 256X256 boyutunda ki görüntülerde son üç bite gömme işlemi yapıldığında oluşan metrik değerleri	26
Tablo 5.7. 128X128 boyutunda ki görüntülerde verilerin tersi alındıktan sonra son üç bite gömme işlemi yapıldığında oluşan metrik değerleri.....	28
Tablo 5.8. 256X256 boyutunda ki görüntülerde verilerin tersi alındıktan sonra son üç bite gömme işlemi yapıldığında oluşan metrik değerleri.....	30

SİMGELER VE KISALTMALAR

Kısaltmalar

PSNR	: Tepe Sinyal Gürültü Oranı
LSB	: En Önemsiz Bit
MSE	: Ortalama Kare Hatası
SNR	: Sinyal Gürültü Oranı
RMSE	: Kök Ortalama Kare Hatası
MSB	: En Önemli Bit
AKD	: Ayrık Kosinüs Dönüşümü
SSIM	: Yapısal Benzerlik İndeksi Ölçüsü
PVD	: Piksel Değeri Farkı
HCF-COM	:Histogram Karakteristik Fonksiyon-Kütle Merkezi
SPAM	: Eksiltici Piksel Komşuluk Matrisi
SRM	: Mekansal Zengin Model
DVM	: Destek Vektör Makinesi

1. GİRİŞ

İnternet teknolojilerinin gün geçtikçe gelişmesi ve hızlı bir şekilde hayatımıza girmesiyle birlikte iletişim olanakları son derece artmıştır. İletişim olanaklarının artması verilerin saklanması, korunması ve iletilmesi gibi problemleri de beraberinde getirmiştir. Böylece anlık olarak sürekli hızlı iletişim ortamlarının en büyük sorunu güvenlik olmuştur. İletişimde güvenlik unsuru üzerinde çalışan birçok çalışma vardır. Kriptografi ve steganografi yöntemleri bunlar arasında sayılabilir[1].

Kriptografi, Yunanca *kryptos* (gizli) ve *graphein* (yazmak) sözcüklerinden türetilmiştir. Kriptografi verilerin bir sisteme göre şifrelenmesi ve güvenli bir ortamda karşı tarafa iletilmesinden oluşur. Şifreleme işlemi yapılırken iki anahtara ihtiyaç vardır. Bunlardan birincisi göndericinin elinde bulunan verinin şifrelemesini yapan anahtar diğeri ise alıcının elinde bulunan ve şifrenin çözülmesine yardımcı olan anahtardır. Böylece gizli veriler üçüncü kişiler tarafından okunmamış veya değiştirilmemiş olur.

Bu şifreleme yönteminde en büyük açık gönderilen verinin anlamsızlığı nedeniyle şifreli olduğunun bilinmesi ve içerdiği bilginin önem taşıdığının anlaşılmasıdır. Bu nedenle şifreli veri çözülemese de iletişimin engellenebilmesi için iletim hattına saldırılarda bulunulabilir. Veri iletişiminin engellenmesi, şifreleme işlemi geçersiz ve yararsız kılacaktır[1].

Steganografi, bir bilgiyi, bir başka bilgi içerisinde saklama sanatı olarak tanımlanabilir. Klasik steganografi, bir seri numarası, telif hakkına ait bir işaret gibi gizli bir mesajı, bilgisayar kodu, video filmi veya bir müzik kaydı gibi bir kılıf mesajı içerisine gömme yollarıyla ilgilenir. Gömme işlemi, genellikle bir parola kullanılarak yapılır ve bu parola bilinmeksizin üçüncü bir kişinin gizlenen bilgiyi bulması ya da yok etmesi çok zordur[2]. Steganografiye çok benzeyen ama farklı olan bir başka teknoloji de filigrandır. Bir müşterinin fikri mülkiyetini korumak için yapılır ve herhangi bir ürünün lisansını kıran ve onları üçüncü taraflara tedarik eden yanlış müşterileri bulmak için kullanılır[3]. E-imzada, kâğıt parada vs. filigran kullanılmaktadır.

Gelişen teknolojilerin modern dünyada gün geçtikçe, teknoloji ilerledikçe internet üzerinden güvenli iletişim ihtiyacı da büyük bir ihtiyaç olarak ortaya çıkmaktadır. Steganografi, güvenli iletişimin sağlanmasında kullanılan tekniktir. Olası bir güvenli iletişim kurmak için bilgileri başka bir ortamda gizleme sanatıdır. Gizlenecek bilgiler görüntü, metin ve video gibi herhangi bir biçimde olabilir. Kriptografiden farklı olarak, veriler başarıyla gizlendikten sonra steganografi, üçüncü şahıslar tarafından bile görülemez, bu da bu tekniği daha güvenli kılar[3].

Steganografi, eski zamanlarda güvenli veri aktarımı için kullanılan görüntü işleme alanıdır. Veri gizlemek için çeşitli steganografi ve yaklaşımlar kullanılmıştır. Steganografi sürecinde gizli bilgiler bir sinyale gömülür, böylece bir iletim kanalı yoluyla güvenli bir şekilde iletebilir. Kaynak [4]' te görüntü, video ve ses sinyallerinde saklanan veriler için farklı yaklaşımlar

bulunmaktadır. Farklı sinyal türlerinde veri gizlemek için farklı yaklaşımları inceleyerek video steganografinin büyük veri iletimi ve güvenliği için en iyi ortam olduğu gözlemlenmiştir. Video dosyası, verilerin bu karelerin arkasına kolayca gizlenebilmesi için birkaç kare içermektedir[4].

Optik steganografi, görüntü şifreleme yoluyla güvenlik iyileştirmesi ile analog aktarım hızını arttırmak ve verilerin kaynaktan hedefe aktarımı için koaksiyel kablo, bükümlü çift teller kullanılmıştır. Bu veri aktarım ortamı doğası gereği daha yavaştır ve aktarılan veriler iletim sırasında sızabilir veya kaybolabilir. Ayrıca veri güvenliği yoktur. İletim sırasında bu sorunların üstesinden gelmek için fiber optik kablolar kullanılır. Fiber optikte veriler ışık huzmesi şeklinde aktarılır, böylece veri sızıntısına daha az eğilimlidir. Ayrıca verilerin güvenli aktarımı için bazı güvenlik mekanizmaları kullanır[2]. Aktarılan veriler önce şifrelenir ve daha sonra hedefe ışık demetleri şeklinde aktarılır. Kaynak[5]'deki sistemde fiber optikte görüntü kullanarak şifreleme yapılmaktadır. Ayrıca, optik ortam verilerini güvenli hale getirmek ve AES, DES, RSA algoritmaları arasında en iyi güvenlik algoritmasını bulmak, karşılaştırmalar yapmak için çeşitli şifreleme algoritmaları önerilmiştir[5].

Bit farkını kullanarak görüntü piksellerinin en önemli biti (MSB)tabanlı geliştirilmiş bir görüntü steganografi tekniği, gizli verileri görüntü, metin, ses ve video gibi farklı dosya biçimlerinde gizler. Görünmezlik, yük kapasitesi, tepe sinyal gürültü oranı(PSNR) ve sağlamlık açısından güvenlik, steganografinin temel zorluklarıdır. Kaynak[6]'da, görüntü piksellerinin en önemli bitlerine dayanan yeni bir görüntü steganografi tekniği önerilmektedir. 5. bit, kapak görüntüsünün 5. ve 6. bitlerin farkına göre gizli bitleri saklamak için kullanılır. 5. ve 6. bitlerin farkı gizli veri bitinden farklıysa, 5. bitin değeri değiştirilir. Sonuçlar, önerilen tekniğin sinyal / gürültü oranında önemli gelişmeler sağladığını belirtmektedir. Genellikle, bilgisayar korsanları gizli veri çıkarımı için LSB bitlerine odaklanır, ancak önerilen teknik, yetkisiz erişimden daha güvenli olmasını sağlayan MSB bitlerini kullanır. Ayrıca, sunulan teknik sadece güvenli değil aynı zamanda hesaplama açısından da verimlidir[6].

Veri gizliliği, steganografi ve kriptografik teknikler kullanılarak, gönderen gizli mesajı hem gönderen hem de alıcı tarafından bilinmesi gereken gizli bir anahtar kullanan şifre algoritmasını kullanarak şifreler. İkili güvenlik sağlamak için, farklı şifreleme yöntemlerinden elde edilen şifreli mesaj en önemsiz bit (LSB) steganografisine dayanan bir görüntüde gizlenir. Alıcı tarafta, şifreli mesaj görüntüden çıkarılır ve daha sonra orijinal gizli mesajı almak için şifre çözme yöntemleri kullanılarak şifresi çözülür[7].

MATLAB kullanarak bilgi paylaşımı için QR kod tabanlı güvenli sistemin uygulanması teknoloji çağında veri güvenliği ve bilgi paylaşımı her zaman tartışılması gereken bir konudur. Güvenlikte kriptografi, steganografi, filigran vb. gizli bilgi paylaşımı için kullanılan birçok yöntem bulunmaktadır. İnsanlar tarafından kullanılan başka bir teknoloji QR kod tabanlı bilgi paylaşımıdır, ancak bu teknoloji gizlilik sağlamak için yeterli değildir. Bu nedenle, güvenli

iletiřim iin kullanılabilen ve diğerklerinden daha iyi verimlilik ve dođruluđa sahip olan daha iyi bir gvenlik algoritmasına ihtiya vardır. Kaynak[8]'de, bilgi paylařımında 3 gvenlik katmanı kullanan QR kod tabanlı bir řifreleme tekniđi nerilmiřtir[8].

LSB tekniđi ile renkli grnt steganografisinin de yeni bir yntem ile nerilen řemada,  gvenlik seviyesine, eřitli olası stego anahtarlarına, gizleme iřleminin bařladıđı ilk pikselin rastgele piksel seimine ve gmlecek mesajın her 24 bitlik blođuna uygulanan aktarıma sahiptir. İlk piksel konumundan bařlayarak gmme iřlemi stego anahtarı kullanılarak hesaplanmaktadır[9]. Gri tonlamalı grntler iin grnt paylařım řemasında gizli grnt, kayıplı sıkıřtırma tekniđine dayalı olarak blokla kodlanır. Arnold dnřm, gvenlik seviyesini artırmak iin karıřtırılmıř alt grntleri elde etmek iin her alt grntye uygulanır ve ardından Shamir'in gizli paylařımı yardımıyla paylařımlar oluřturulur[10]. LSB ve Arnold dnřmne dayalı tek bir 24 bitlik kapak grntsnde birden fazla gizli grnty gizlemek iin yeni bir grnt steganografisinin de  adet 8 bitlik gizli grnt alınarak Arnold dnřm kullanılmıř 24 bitlik tek bir renkli grnt iinde oklu grnt gizleme yapılmıřtır. Bu yntem, diğerk yntemlere kıyasla dřk hesaplama karmařıklıđı ve yksek kapasite elde edilmiřtir[11].

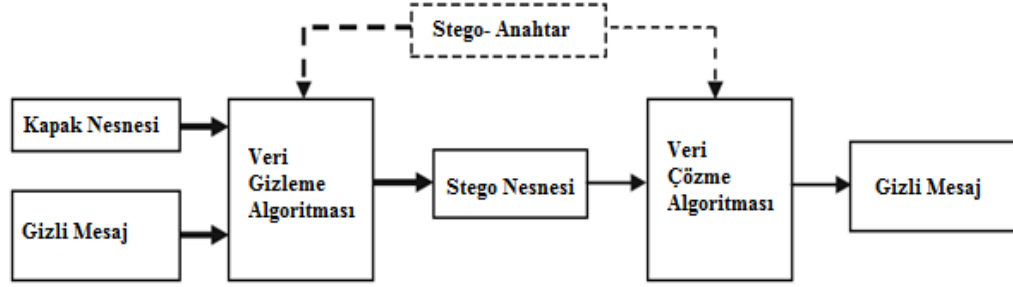
Keskin kenar detektr ve 2k dzeltmeye dayalı olarak grnt iindeki gizli verileri gizlemek iin bir uzaysal alan steganografi ynteminde gizli mesajı sıkıřtırmak iin Huffman kodlamasını ve tutarlı bit uzunluđunu kullanılmıřtır. Gvenliđi artırmak iin kenar piksellerini rastgele sıralamak iin sıralama tekniđi kullanılmıřtır. Bu yaklařım, geliřmiř PSNR ile yksek gvenlik sađlamaktadır[12].

Bu tezin amacı uydu zerinden alımıř olduđumuz grntlere steganografik yntemlerden LSB tekniđini kullanarak 6, 7 ve 8. bite veri gizleyerek Tepe Sinyal-Grlt Oranı (PSNR), Ortalama Kare Hatası (MSE), Kk Ortalama Kare Hatası (RMSE), Sinyal Grlt Oranı (SNR) deđerlerini hesaplayarak grntlerdeki bozulmalar gzlemlemektir. Uydu zerinden alımıř olduđumuz 128x128 ve 256x256 boyutlarında 14 imgeye konum zelliklerini anlatan farklı boyutlarda veriler gizlenmiřtir. Veri boyutları arttırılıp azaltılarak grntde ki bozulma deđerleri hesaplanmıř ve gizlenen verinin tersi alınarak hesaplanan PSNR, MSE, RMSE ve SNR deđerlerinde ki artma ve azalma gzlemlenerek grntlerdeki bozulmalara bakılmıřtır.

Giriř blm ile daha nce yapılmıř alıřmalar incelenip, tez alıřmasında yapılacak iřlemler, tez amacı, kapsamı ve nemi vurgulanmıřtır. İkinci blmde steganografinin tarihesi, gvenilir bir steganografi de dikkat edilmesi gereken unsurlar ve steganografi eřitleri hakkında bilgi verilmiřtir. nc blmde LSB tekniđi zerinde durulmuřtur. MSE, RMSE, PSNR ve SNR parametrelerinin forml ile hesaplanması ve deđerlerinden bahsedilmiřtir. Drdnc blmde kullanılan uydu imgeleri detaylı anlatılmıř ve yapılan uygulama anlatılmıřtır. Beřinci blmde uygulama sonucu elde edilen tablolar ve grntler hakkında bilgi verilip analizi yapılmıřtır. Altıncı blmde ise sonular verilmiřtir.

2. STEGANOGRAFI

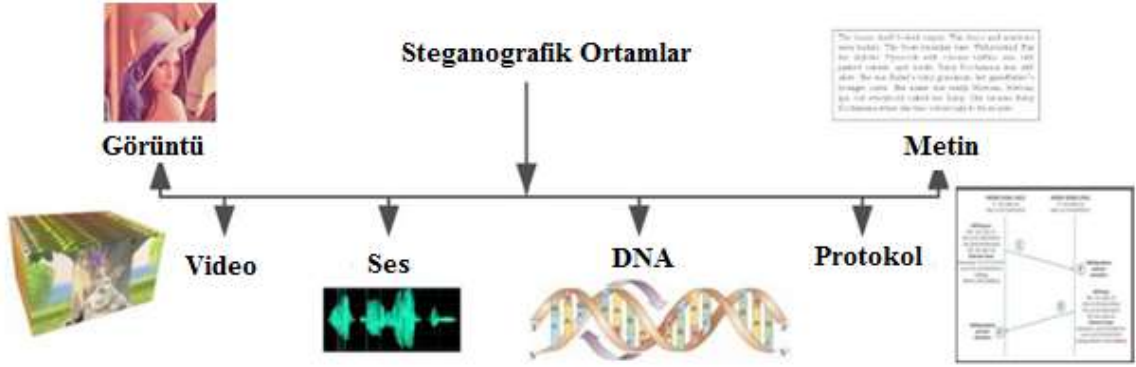
Yunancadan türetilen steganografi, kelimesi tam anlamıyla “örtülü yazı” anlamına gelir. Steganografi bir verinin farklı bir ortama aktarılırken içerisine veri gizlenmiş olan dosyanın fark edilmeden aktarılabilmesi yani bilginin gizlenmesi sanatıdır. Steganografide ki temel amaç güvenli ve gizli haberleşmedir. Steganografide kriptografiden farklı olarak gizli mesaj; dijital resim, video, ses ve farklı bilgisayar dosyaları içerisinde saklanarak, üçüncül kişilerin bilginin aktarımını fark etmemeleri sağlanır. Ses, sayısal görüntü, video görüntüleri üzerine veri saklanarak taşınmak istenen mesaj karşı tarafa, içinde gizli veri olduğu hissettirilmeden aktarılabilir. Şekil 2.1.’ de steganografi ile verinin oluşturulması ve gizli verinin elde edilmesi verilmiştir. Eğer uygulanan steganografi yöntemi üçüncü kişilerde örtü verisi içerisinde gizli bir veri olabileceği şüphesini uyandırıyorrsa, bu yöntem başarısız olacaktır[13].



Şekil 2.1. Steganografi ile veri oluşturulması ve gizli verinin elde edilmesi

Genel olarak, iletişim ortamları / taşıyıcılar dijital dosyalar veya verilerdir. Şekil 2.2.’de görüntü, video, metin, ses, ağ protokolü ve DNA verilmiştir. Farklı dijital ortamlar, gizli bilgileri gömmek için çeşitli özelliklerini kullanılmaktadır. Örneğin, metin steganografisi, satır / kelime kaydırmalı kodlamayı [14] ve gizli iletişimi sağlamak için son zamanlarda metin sohbetinde kullanılan ifadeleri kullanılmaktadır [15]. Ses steganografisinde, genellikle gizli bilgilerin gömülmesi için faz kodlaması, yaygın spektrum ve düşük bit kodlaması kullanılmaktadır [16]. Gizli bilgiler ayrıca paket yüküne, ağ protokolü [17] olarak başka bir ortamda paket başlıklarına gömülebilir ve hatta yeniden iletim steganografisi [18] olarak bilinen paketlerin onaylanması ve yeniden iletilmesinde kullanılmaktadır. DNA tabanlı steganografide, DNA'daki rastgelelik özellikleri gizli verileri gömmek için kullanılabilir, yani gizli verileri kodlamak DNA dizisini haritalamak için sayısal haritalama tablosu kullanılmaktadır [19]. Video steganografisinde, görüntü ve ses steganografisinin birleşimi sıklıkla kullanılır. Ayrıca, video akışı göz önüne alındığında farklı bir görüntü kombinasyonu nedeniyle daha gizli veri gömmek için daha fazla derinliğe sahiptir [20]. Kaynak [21] 'ye göre, gizli mesajı yerleştirmek için en iyi ortam iki özelliğe sahip

olmalıdır; medya popüler olmalı ve kapak ortamındaki değişiklik üçüncü şahıslar tarafından görülmemelidir. Dijital steganografi literatüründe, görüntü, yüksek frekanslı fazlalık veriye sahip olması ve içindeki gizli verileri görünmez efektlerle birlikte gizleyebilmesi nedeniyle en popüler ortamdır[22].



Şekil 2.2. Steganografik Ortamlar

Güvenilir bir steganografi sistemi inşa ederken dikkat edilmesi gereken unsurlar şunlardır:

- Görünmezlik:** Steganografik sistemin insanlar tarafından (insan gözüyle) farkına varılamaz olmasıdır. Steganografik mesajın taşıyıcı unsur üzerine gömülümü işleminden sonra imgede meydana gelecek değişimler insan çıplak gözüyle farkına varılamaz olmalıdır.

- Güvenlik:** Saldırgan taşıyıcı obje üzerinde gizli mesajın varlığını fark etse bile mesajı ortaya çıkarmasının imkânsıza yakın olması durumudur. Tepe sinyalinin gürültüye oranı ölçü birimi ne kadar yüksek değerli olursa sistemimiz o kadar güvenli demektir.

- Kapasite:** Mesajın kapasitesinin taşıyıcı mesajın kapasitesinden fazla olmaması durumudur. Bu yaklaşık olarak maksimum %51'lik kısmı geçmemesi tavsiye edilir aksi durumda, steganografinin unsurlarından olan görünmezlik unsuru delinmiş olur.

- Sağlamlık:** Steganografinin taşıyıcı unsuru resim, video vb. üzerinde yapılan filtreleme, kesme, kırpma, yön değiştirme ve sıkıştırma gibi manipülasyonlara karşı dayanıklı olması durumudur[23].

2.1. Steganografi Çeşitleri

2.1.1. Metin Steganografisi

Metinde bilgileri gizlemek steganografinin en önemli yöntemidir. Yöntem, bir metin mesajının her kelimesinin her n. harfinde gizli bir mesajı gizlemektir. İnternet ve farklı dijital

dosya formatları yayıldıktan sonra önemi azaldı. Dijital dosyaları kullanan metin steganografisi, metin dosyalarında çok az miktarda yedek veri bulunduğundan çok sık kullanılmamaktadır[4].

2.1.2. Video Steganografisi

Video steganografi, herhangi bir kayıt türünü bir video belgesine gizlemek için kullanılan bir yöntemdir. Özellik tabanlı steganografinin kullanımı, boyutu ve bellek önkoşulları nedeniyle diğer etkileşimli ortam belgelerinden daha nitelikli olabilir. Video steganografi, herhangi bir uzantıdaki her türlü kaydı taşıyan bir video dosyasına gizleyen bir sistemdir. Bu girişim, taşıyıcı kayıt olarak adlandırılan alternatif bir belgeye herhangi bir veri eklemek için oluşturulan uygulamadır. Taşıyıcı belge özellikli bir kayıt olmalıdır. Bu korumalı ve güçlü bir şekilde zararsız yayılmış medya veri ekleme ile ilgilidir. Bu çerçevede fikirleri Steganografi ve kriptografi kullanarak dosyaları daha güvenli hale getirir[4].

2.1.3. Ses Steganografisi

Ses steganografisi, bilgileri fark edilmeden gizlemek için insan kulağının özelliklerinden yararlanan maskeleyedir. Yüksek seviyede ki bir ses, başka bir yüksek seviyede ki işitilebilir sesin varlığında duyulmayabilir. Bu özellik, bilgilerin gizleneceği kanalı seçmeye izin verir[4].

2.1.4. Protokol Steganografisi

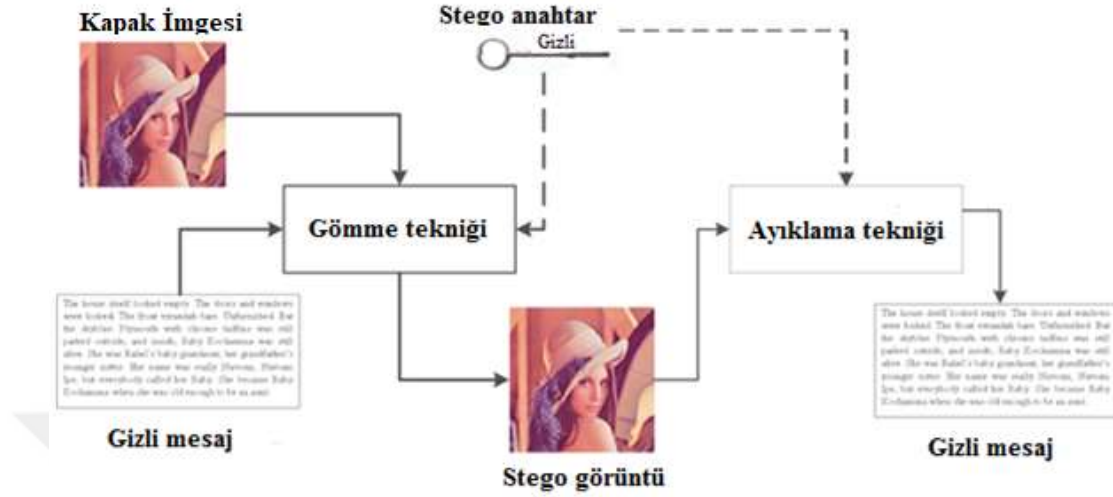
Protokol steganografisi terimi, TCP / IP gibi ağ protokollerine bilgi katmaktır. TCP / IP paketinin başlığında, isteğe bağlı olabilecek veya hiç kullanılmayacak bazı alanlarda bilgiler gizlenir[4].

2.1.5. Görüntü Steganografisi

Görüntüler steganografi için popüler kapak nesneleri olarak kullanılır. Bir mesaj, gizli anahtarı kullanarak bir gömme algoritması aracılığıyla dijital bir görüntüye gömülür. Ortaya çıkan stego görüntüsü alıcıya gönderilir. Diğer tarafta, aynı anahtar kullanılarak çözme algoritması tarafından işlenir. Stego görüntüsünün iletimi sırasında kimliği doğrulanmamış kişiler yalnızca bir görüntünün iletimini fark edebilir, ancak gizli mesajın varlığı tahmin edilemez[4].

Görüntü steganografisinde, gizli bilgiyi içeren / gizleyen taşıyıcı bir görüntüdür. Temel görüntü steganografi diyagramı Şekil 2.3' te gösterilmektedir. Şekil 2.3' te, "kapak imgesi" terimi, gizli verileri bir yük veya "gizli mesaj" olarak gizlemek için kullanılan görüntüyü ifade eder. "Gömme tekniği" aslında isteğe bağlı "stego-anahtar" ile "kapak imgesi" yani "stego-görüntü" içeride "gizli mesaj" gizlemek için kullanılan algoritma işlemidir. İsteğe bağlı "stego-anahtar" her iki uçla paylaşılmalıdır. "Stego görüntüsü", gizli bilgiyi gizleyen son çıktı görüntüsünü belirtir.

Benzer şekilde, gömme işleminin karşılığında gizli bilgiyi çıkarabilir, burada "çıkarma tekniği", isteğe bağlı "stego-anahtar" ile "stego-image" dan "gizli mesajı" kurtarma işlemidir[22].



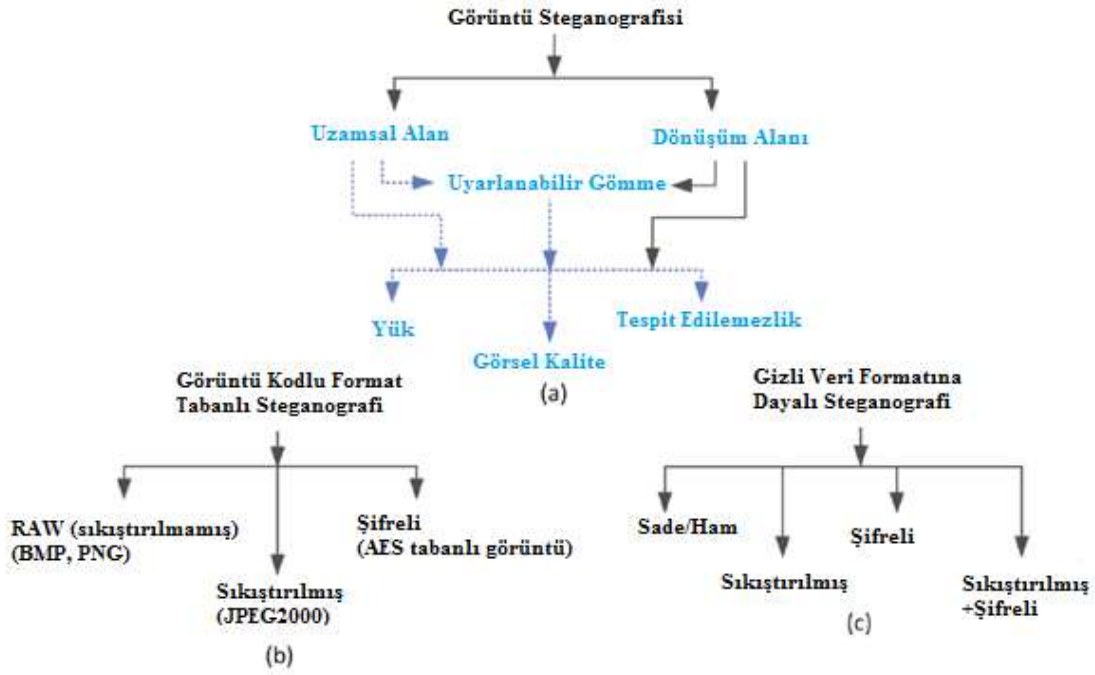
Şekil 2.3. Görüntüler de steganografik diyagram

Literatürde, çeşitli steganografik yöntemler önerilmiştir ve en önemlisi gizli veri elde etmek için ayrı bir yaklaşım kullanmaktadır. Bu yaklaşımları sınıflandırırsak, uygulamalarına bağlı olarak farklı türlere ayrılabilir. Şekil 2.4'te gösterildiği gibi farklı kategorilere ayrılmaktadır. Ayrıca, uyarlanabilir (istatistiksel farkındalık) gömme yöntemi, hem uzamsal hem de dönüşüm alanlarında kullanılabildiği için yukarıdaki bölümün altına girebilir. Şekil 2.4. (a) genel amaçları veya hedefleri ile sınıflandırmayı göstermektedir. Başka bir sınıflandırma, Şekil 2.4. (b) 'de gösterildiği gibi kodlanmış görüntü formatlarını, yani ham (BMP), sıkıştırılmış (JPEG2000) ve şifreli görüntü verilerini (AES gelişmiş şifreleme standardı) hedeflemek için özel olarak tasarlanmış ayırt edici steganografik tekniklere dayanabilir. Literatürde, steganografik tekniklerin bazıları, farklı steganografik hedefleri iyileştirmek için gizli verilerin (yani metin, sıkıştırılmış, gizli görüntü) formatına / türüne göre özel olarak tasarlanmıştır. Şekil 2.4. (c) için, steganografik tekniklerin gizli veri formatlarına / türlerine göre sınıflandırılması tasvir edilmiştir.

Şekil 2.4. (a) 'dan, uzamsal alan, örneğin, gizli bilgileri gizlemek için kapak görüntüsü verilerini / pikselleri doğrudan kullanır, örneğin piksel değeri içindeki gizli bitlerin değiştirilmesinde kullanılmaktadır. Tersine dönüşüm alanı, kapak görüntüsünün verileri ilk olarak gömme işlemi uygulanmadan önce başka sinyale / forma dönüştürülür. Örneğin, pikselleri kaplamak için ayırık kosinüs dönüşümü (AKD) uygulanır ve daha sonra gizli veriler AKD bloklarının farklı katsayısına gömülebilir. Ayrıca, Şekil 2.4. (a) 'da ki adaptif gömme şeması, model temeli veya istatistiksel farkındalıkla bilgi gizleme teknikleri olarak bilinir. Temel olarak mekânsal ve dönüşüm alanı ile bağlantılıdır. Bu tür gömme yöntemleri, gizli bilgileri uzamsal

veya dönüşüm alanına gömmeden önce görüntünün istatistiksel özelliklerini alır. Bu istatistiksel özellikler aslında steganografik amaç için görüntüde modifikasyonun nerede gerçekleştiğini belirlemektedir [24].

Uzamsal etki alanı gömme yöntemleri, gömme ve çıkarma işlemindeki kolaylıkta, daha az güvenilirliği nedeniyle dönüştürme etki alanından daha popüler kullanılır.



Şekil 2.4. (a) hedeflenen hedefleri ile görüntü steganografik alanlar, (b) görüntü kodlu format tabanlı gömme teknikleri, (c) gizli mesaj formatına dayalı steganografik teknikler.

Steganaliz, gizli mesajın varlığını tespit etme veya gizli mesajı stego görüntülerinden kurtarmaya yönelik bir sanat ve bilimdir[22].

2.2. Steganaliz

Steganaliz, steganografi tarafından gömülü olan gizli verileri açığa çıkarma sanatı ve bilimidir [25]. Steganografi ve steganaliz her zaman birbirinin karşıtıdır. İdeal bir steganografik yaklaşım tasarlandığında, gömme süreçlerini analiz etmek veya yenmek için karşı önlem steganalizi de geliştirilmiştir [26]. Steganografinin asıl amacı, herhangi bir steganaliz, gömülü nesnenin içinde gizli verilerin varlığını tespit etse bile başarısız olur. Görüntü steganografisinin de gömme yöntemleri görsel olarak insan gözüne şeffaf olsa da steganalizde yine de tespit saldırıları mümkündür. Genel olarak, steganografik yöntem gömme işlemi sırasında görsel kaliteye göre stego görüntüsünün olağandışı karakteristik varyasyonlarına neden olan çeşitli görsel eserler bıraktığında veya ortaya çıkardığında, diğer steganaliz teknikleri stego görüntüsünün içindeki

gizli verilerin varlığını tespit etmek için olağandışı görüntü özelliklerinin avantajlarını kullanır. Genellikle, steganaliz yöntemleri pasif steganaliz ve aktif steganaliz olmak üzere iki ana kategoriye ayrılır [25]. Pasif steganaliz, gizli verilerin varlığını yokluğunu veya sadece belirli bir gömme sürecini ortaya çıkarmayı tanımlar. Aktif steganaliz, pasif steganalizden daha fazla derinliğe sahiptir; gizli verileri kurtarabilir, değiştirebilir veya sadece gizli verilerin uzunluğunu tahmin edebilir. Literatürde hem istatistiksel hem de istatistiksel olmayan steganaliz yöntemleri mevcuttur, bunlardan bazıları belirli bir tür gömülü steganaliz teknikleri için tasarlanmıştır ve diğerleri evrensel steganalizdir[22].

Literatürde sık kullanılan bazı test analizi ve tespit saldırıları bulunmaktadır. Aşağıdaki bölümde temel testler ve analiz teknikleri gösterilmektedir.

2.2.1. Görsel Steganaliz

Algısal görünmezlik, herhangi bir steganografik yöntemin en önemli gereksinimlerinden biridir. Gömüldükten sonra, insanın sınırlı görme sistemi nedeniyle bazı göze çarpan görsel eserler görünmezdir. Bu nedenle, görsel kalite ölçümlerini tahmin etmek için farklı görsel kalite ölçümleri uygulanır. Genel olarak, görsel şeffaflığı değerlendirmek için literatürde en yaygın MSE, PSNR, SSIM, Q indeks ölçümleri kullanılmaktadır[22].

2.2.2. İstatistiksel Steganaliz

İstatistiksel steganaliz, herhangi bir steganografik yöntemin neden olduğu olağandışı özellikleri tespit etmek için görüntülerin yapısal özelliklerini kullanır. Histogram analizi, bit düzlemi analizi, ki-kare olarak örnek çifti analizi, gizli verilerin varlığını kolayca ortaya çıkarabilen ve hatta gizli veri boyutunu tahmin edebilen RS analiz yöntemleri gibi çeşitli istatistiksel analiz türleri vardır[22].

2.2.2.1 Histogram Tabanlı Analiz

Histogram analizi, bir stego görüntüsünün etkili bir şekilde test edilmesi olarak da kabul edilir. Kapak ve stego görüntülerinin histogramları, gömme algoritması nedeniyle izlenen piksel dağılımını veya olağandışı şekilleri tanımlamak için karşılaştırılır. Çoğunlukla, Piksel Değeri Farkı(PVD) tabanlı steganografik yöntemler histogram analizinin farklı varyasyonları, yani piksel farkı histogram analizi, histogram karakteristik fonksiyon-kütle merkezi (HCF-COM) analizi ile değerlendirilir[27].

2.2.2.2 RS Steganaliz

RS analiz yöntemi olarak bilinen düzenli ve tekil analiz, rastgele LSB gömme yöntemlerini tespit etmek için tasarlanmıştır[28]. Yöntem, piksellerin LSB' sinde ki küçük değişikliklerden

yararlanır ve bu değişiklikleri ve bu pikselleri normal tekil gruplar halinde sınıflandırmak için bir ayırım işlevi kullanılmaktadır. Bu grupların sıklığı, stego görüntülerindeki gizli mesajın uzunluğunu tanımlar. Literatürde, çok sayıda steganografik teknik, güvenlik veya tespit edilemezliklerini kanıtlamak için RS steganaliz tarafından değerlendirilir[22].

2.2.2.3 Ki-Kare Analizi

Ki-kare saldırı yöntemi, gizli veri gömme sırasında değiş tokuş edilen değer çiftlerinin (PoVs) istatistiksel analizine dayanır. Yöntem, LSB tabanlı gömmeyi tespit etmek için tasarlanmıştır [29]. Ki-Kare steganaliz saldırıları ile gömme yöntemi sayısı tespit edilir.

2.2.2.4 Bit Düzlem Analizi

Genel olarak, bir görüntünün her bit düzlemi, diğer komşu bit düzlemleri ile bir korelasyona sahiptir. Steganografik yöntem uygulandıktan sonra korelasyonu değiştirebilir ve bu da bit düzlem analizi ile görülebilir. Bit düzlemi analizi, yer değiştirme tabanlı gömme teknikleri ile güçlü bir şekilde değerlendirilir[22].

2.2.3. Yapısal Olmayan Steganaliz

Yapısal olmayan steganalizde, özellik çıkarıcı kapak görüntüsünü modellemek ve gömülü gizli verileri tespit etmek için kapak ve stego görüntüsü arasındaki bozulmayı daha fazla tahmin etmek için kullanılır. Özellik kümesinin seçimi, steganografik yönelimli veya evrensel özellik kümesi olarak belli olabilir. Genel olarak, bir makine öğrenimi tabanlı sınıflandırıcı, özellik kümesini, daha büyük kapak veri kümesi ve stego görüntüleri arasındaki özelliklerin farklılıklarını öğrenecek şekilde eğitir. En belirgin yapısal olmayan steganaliz, stego görüntüsü için daha iyi steganaliz olasılığı olarak kabul edilen Eksiltici Piksel Komşuluk Matrisi (SPAM) ve Mekansal Zengin Model(SRM)' dir[30, 31]. Steganaliz, sınıflandırma aşaması için denetimli eğitim ile destek vektör makinesi (DVM) veya topluluk sınıflandırıcısı kullanılır. Literatürde çok sayıda özellik tabanlı steganaliz türü vardır [32, 33].

3. EN AZ ANLAMLI BİT (LSB) TEKNIĞİ

Görüntü içerisine en az anlamlı bit (LSB) yöntemiyle veri gizleme en yaygın kullanılan yöntemlerden biridir. LSB, birim değerini veren, yani sayının çift mi yoksa tek mi olduğunu belirleyen, ikili bir tamsayıdaki bit konumudur. LSB, sağa doğru daha az anlamlı bir rakam yazmanın konumsal gösterimindeki kural nedeniyle, en sağdaki bit olarak adlandırılır [34]. Görüntüyü oluşturan her bir pikselin her baytının en anlamsız bitine ikilik sistemdeki verinin eklenmesi ile yapılmaktadır. Bir bitlik değişim göz ile görülür bir fark yaratmayacaktır[35]. Görüntüdeki bozulmalar gözle görülemediği için veri gizliliği sağlanmış olacaktır.

LSB tekniğinde öncelikle gizlenecek karakterlerin ASCII değerleri bulunur. Daha sonra ASCII değerine göre ikili forma dönüştürülür. İkili forma dönüştürülen veri görüntünün en az anlamlı bitine yani 8. bitine gömülür. Yerleştirme kapasitesine göre ve gizleme işlemi yapıldıktan sonra ki görüntü kalitesine bağlı olarak gizleme için son iki veya üç bit de kullanılabilir.

Örneğin “Y” karakterini imgeye gömme işlemi yapılırken öncelikle ASCII karşılığı bulunur daha sonra ikili forma çevrilir. “Y” harfi için ASCII kod 89 ’dur ve ikilik sistemde ki karşılığı 01011001’dir. Daha sonra en az anlamlı bite yani 8. bite sırayla gömme işlemi yapılır.

(0010110 <u>0</u>	0101111 <u>1</u>	0111111 <u>0</u>)
(0011101 <u>0</u>	0000111 <u>0</u>	1110011 <u>0</u>)
(0100111 <u>1</u>	1101000 <u>0</u>	0111001 <u>0</u>)

Şekil 3.1. İkili kodda üç piksel değeri

(0010110 <u>0</u>	0101111 <u>1</u>	0111111 <u>0</u>)
(0011101 <u>1</u>	0000111 <u>1</u>	1110011 <u>0</u>)
(0100111 <u>0</u>	1101000 <u>1</u>	0111001 <u>0</u>)

Şekil 3.2. LSB' de veri gizlendikten sonra üç piksel değeri

Şekil 3.1.' de ikili kodda üç piksel değerleri verilmiştir. Şekil 3.2' de piksel değerleri verilere göre LSB' de değişikliğe sebebiyet vermektedir. Yeşil renkli LSB biti, veri biti ve pikselin LSB biti aynı olduğundan, verileri gizledikten sonra bile piksel değerinin değişmediğini

gösterir. Kırmızı renk, veri bitinin piksel değerinin LSB bitine eşit olmadığı için piksel değerinin değiştiğini gösterir[3].

Görsel kalite analizi, açıkça herhangi bir steganografik yöntemle gömülü gizli veriler, kapak görüntüsünün görsel kalitesini, herhangi bir insan gözü tarafından kolayca fark edilemeyecek şekilde değiştirilmektedir. Steganografik yöntemin algısal olarak şeffaf olup olmadığına karar vermek için görsel modifikasyon seviyelerini tahmin edebilen veya değerlendirebilen standart ölçüm tekniklerine ihtiyaç vardır. Bununla birlikte, literatürde hem steganografi (örneğin MSE, RMSE, PSNR, SNR, WPSNR, Q, SIMM) hem de filigran (örneğin IF, NCC) için çeşitli görsel kalite ölçüm ölçütleri mevcuttur[22].

Kapak görüntüsünde, veriler gizlenmeden önceki ve sonraki değişiklik, yani bozulma, PSNR, MSE, RMSE, SNR gibi bazı parametrelerle hesaplanabilir[3]. Aşağıda ki eşitliklerde bu parametrelerin nasıl hesaplandığı gösterilmektedir.

MSE ortalama karesel hatadır. Görüntü kalitesi ölçümünün temeli olmuştur. Genellikle, orijinal görüntünün herhangi bir bozulma içermediği varsayılırken, diğer görüntünün gürültü veya başka bir tür hata ile kirlenmiş olduğu varsayılır. Aralarındaki fark ise hata sinyali olarak adlandırılır [36].

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (X_{ij} - Y_{ij})^2 \quad (3.1)$$

PSNR tepe sinyal gürültü oranıdır. Genel olarak görüntü işlemede PSNR kullanılır. PSNR, yalnızca farklı dinamik aralıklardaki görüntüler karşılaştırılırken MSE' den daha kullanışlıdır, aksi takdirde MSE' ye eşdeğerdir [36].

$$PSNR = 10 \times \log_{10} \frac{C_{max}^2}{MSE} \quad (3.2)$$

Max=maksimum piksel yoğunluğu değeri 255.

$$RMSE = \sqrt{MSE} \quad (3.3)$$

$$SNR = 10 \times \log_{10} \left(\frac{\sum_{i=1}^{H \times W} C_i^2}{\sum_{i=1}^{H \times W} (C_i - S_i)^2} \right) \quad (3.4)$$

Hesaplanan MSE ve RMSE değeri 0-1 arasında değer alır. 1'e yaklaştıkça ortalama kare hatası ve kök ortalama kare hatası değerleri artar. Yani görüntüdeki bozulmalar artar. PSNR ve SNR değerleri ise 0-100 arasında değer alır. 100'e yaklaştıkça görüntüdeki bozulmalar azalır. Hesaplanan PSNR değeri %40'ın altında ise görüntüde ki bozulma gözle görülebilecek seviyededir. PSNR değeri resme gizlenecek verinin boyutu ile ters orantılıdır. Yani gömülecek verinin boyutu arttıkça PSNR değeri düşer ve imgedeki bozulma artar.

4. MATERYAL METOT

Uygulamamızın veritabanı google earth pro ile Elazığ üzerinden alınmış 14 farklı bölgede ki uydu görüntülerinden oluşmaktadır. Aşağıda tablo 4.1.' de yer alan 128X128 ve 256X256 boyutlarına getirilen toplamda 28 görüntü üzerinde uygulama yapılmıştır.

Tablo 4.1. Uydu üzerinden alınmış 128X128 ve 256X256 boyutunda ki imgeler

128X128 Boyutunda ki görüntü	256X256 Boyutunda ki görüntü
1 Hazarbaba kayak merkezi 	
2 Hava limanı 	

3 Harput kalesi



4 Fırat Üniversitesi



5 Keban barajı



**6 Saklıkapı
kanyonu**



7 Palu kalesi



**8 Feti Sekin şehir
hastanesi**



9 Kltrpark



10 Hazar gl



**11 Alacakaya
mermer iletmesi**



**12 Çimento
fabrikası**



**13 Çırçır şelalesi
keban alabalık**



**14 Kapalı
çarşı- izzetpaşa
cami**



Uydudan alınan görüntülere görüntünün alındığı bölgenin özelliklerini anlatan bilgiler steganografik yöntemlerden LSB ile gizlenmiştir. Bu bilgilerin oluşturduğu karakter uzunlukları 423 ile 542 arasında değişiklik göstermektedir. Daha sonra bu karakter uzunluklarının üç katı alınarak yani 1269 ile 1626 boyutlarında karakterlerle gizleme işlemi yapılmıştır. Böylece veri

uzunluğunun LSB tekniğinde kullanılan parametrelere etkisine bakılmış ve görüntüde ki bozulmalar gözlenmiştir.

LSB tekniğiyle ilk olarak gömülecek verilerin ASCII karşılığı bulunmuştur. Daha sonra bulunan ASCII karşılıkları ikilik forma dönüştürülmüştür. Şekil 4.1.' de ASCII kod karşılığının ikilik forma çevrilmesini sağlayan sözde kod verilmiştir.

```
1 Başla
2 say diye bir değişken tanımla ve mesajı aktar
3 mesajın ascii kod karşılığını g değişkenine ata
4 8 bitlik bir döngü oluştur 1 azalt
5 g değişkenini mod 2 ye göre al diziye ata
6 g yi tam sayıya yuvarlama yap
7 bitir
```

Şekil 4.1. Ascı kod karşılığının ikilik forma çevrilmesini sağlayan sözde kod

Dönüştürülen veriler en son bite gömülmüştür. Veri boyutları üç kat artırılarak gömme işlemi yapıp aradaki değerlerde ki artma ve azalma oranları karşılaştırılmıştır. Daha sonra ki aşamalarda son iki ve son üç bite gömme işlemi yapılarak veri boyutları değiştirilerek görüntülerde ki PSNR, SNR, MSE ve RMSE değerlerindeki değişim oranlarına bakılmış ve görüntülerde ki bozulmalar gözlenmiştir. Aşağıda şekil 4.2.'de 6, 7 ve 8. bite gömme işlemini gösteren sözde kod verilmiştir.

```
1 Başla
2 gizlenecek veriyi metin değişkenine ata
3 görüntüyü copyresim değişkenine ata
4 metni 2 boyutlu bir vektöre dönüştürüp boyut değişkenine ata
5 satır sayısı k =1
6 sütun sayısı j=1
7 for i=1 den boyut'a
8 metin karakterlerinin ascii kod karşılığını bul
9 for m=1 den 8 e çift say
10 copyresimi x'e ata
11 x'i ikilik sisteme çevir y'ye ata
12 y'nin 8. bitine gizleme işlemi yap
13 m'yi 1 arttır
14 y'nin 7. bitine gizleme işlemi yap
15 y'nin 6. bitine gizleme işlemi yap
16 j'yi 1 arttır
17 eğer j copyresimin boyutuna eşit ise
18 k'yi 1 arttır
19 j'yi 1 yap
20 bitir
```

Şekil 4.2. 6, 7 ve 8. bite gömme işlemini gösteren sözde kod

Son üç bite gizleme işlemi ile bitlikte gizlenen mesajın ikilik sistemde ki tersi alınarak imgeye gizleme işlemi yapılmıştır ve değerlerdeki artma ve azalma işlemleri karşılaştırılmıştır. Aşağıda şekil 4.3.' te gizleme işleminde verilerin tersini alan fonksiyonun sözde kodu verilmiştir.

```
1 Başla
2 say diye bir değişken oluştur
3 for i=1 den say değişken uzunluğuna
4 eğer say(i) değeri 0 ise 1 yap
5 değilse 0 yap
6 bitir
```

Şekil 4.3. Gizleme işleminde verilerin tersini alan fonksiyonun sözde kodu

Böylece mesaj bitlerinin tersi işleminin görüntü işlemede ki PSNR, MSE, RMSE ve SNR değerleri üzerinde ki etkisine bakılmıştır.

5. BULGULAR VE TARTIŞMA

Uygulama da kullanılan görüntüler 128x128 ve 256x256 boyutlarına getirilerek son bir bitine gömme işlemi uygulanmıştır. Daha sonra gömülen verilerin üç katı alınarak gömme işlemi uygulanmıştır.

Tablo 5.1’ de 128x128 boyutundaki 14 görüntüye, görüntülerin konumu ile ilgili bilgilerin son bir bitine gömme işlemi uygulanmıştır. Görüntülerde ki değerlere bakıldığında PSNR değeri 10. görüntü de en düşük 54.8986 olarak hesaplanmıştır. MSE değeri 14. görüntüde en yüksek 0.1293 olarak hesaplanmıştır. RMSE değeri 14. görüntüde en yüksek 0.3596 olarak hesaplanmıştır. SNR değeri en düşük 10. görüntüde 49.7685 olarak hesaplanmıştır. Daha sonra gömülen mesajın üç katı büyüklüğünde bir veri ile işlem yapıldığında PSNR değeri en düşük 10. görüntüde 50.1252, MSE değeri en yüksek 14. görüntü de 0.3906, RMSE değeri en yüksek 14. görüntüde 0.6250 ve SNR değeri en düşük 10. görüntüde 44.9956 olarak hesaplanmıştır.

Tablo 5.1. 128X128 boyutunda ki görüntülerde son bir bite gömme işlemi yapıldığında oluşan metrik değerler

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbaba kayak merkezi	423	57.7202	0.1023	0.3198	52.7407
	1269	52.9723	0.3052	0.5525	47.9923
	430	56.9933	0.1057	0.3251	52.5216
2 Hava limanı	1290	52.2329	0.3163	0.5624	47.7613
	458	57.7830	0.1083	0.3291	52.2248
3 Harput kalesi	1374	52.9278	0.3314	0.5756	47.3694
	484	57.3724	0.1191	0.3451	50.3886
4 Fırat Üniversitesi	1452	52.6445	0.3537	0.5947	45.6612
	446	57.3938	0.1076	0.3280	50.5451
5 Keban barajı	1338	52.5768	0.3262	0.5712	45.7284
	478	55.6544	0.1177	0.3430	51.5995
6 Saklıkapı kanyonu	1434	50.8652	0.3545	0.5954	46.8104
	479	56.6452	0.1196	0.3458	51.5599
7 Palu kalesi	1437	51.9238	0.3546	0.5955	46.8386
	487	57.0514	0.1193	0.3454	53.4838
8 Feti Sekin şehir hastanesi	1461	52.3211	0.3546	0.5955	48.7532
	452	57.8026	0.1078	0.3284	51.2189
9 Kültürpark	1356	52.9817	0.3273	0.5721	46.3982
	497	54.8986	0.1218	0.3490	49.7685
10 Hazar gölü	1491	50.1252	0.3657	0.6047	44.9956
	469	57.4715	0.1164	0.3412	53.5583
11 Alacakaya mermer işletmesi	1407	52.7908	0.3420	0.5848	48.8777
	495	57.1831	0.1234	0.3513	52.7097
12 çimento fabrikası	1485	52.4406	0.3678	0.6065	47.9669
	466	57.6174	0.1125	0.3355	50.9180
13 Çırçır şelalesi keban alabalık	1398	52.8079	0.3406	0.5836	46.1091
	542	57.0137	0.1293	0.3596	50.9685
14 Kapalı çarşı- izzetpaşa cami	1626	52.2139	0.3906	0.6250	46.1688

Tablo 5.2’ de 256x256 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgilerin son bir bitine gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 61.3648, MSE değeri en yüksek 14. görüntüde 0.0327, RMSE değeri en yüksek 14. görüntüde 0.1808 ve SNR değeri en düşük 10. görüntüde 51.1349 olarak hesaplanmıştır. Gizlenecek bilgilerin üç katı alınıp son bir bite gömme işlemi yapıldığında ise PSNR değeri en düşük 10. görüntüde 56.5530, MSE değeri en yüksek 14. görüntüde 0.0982, RMSE değeri en yüksek 14. görüntüde 0.3134 ve SNR değeri en düşük 10. görüntüde 51.1349 olarak hesaplanmıştır.

Tablo 5.2. 256X256 boyutunda ki görüntülerde son bir bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbaba kayak merkezi	423	64.0045	0.0251	0.1583	58.8638
	1269	59.1886	0.0759	0.2756	54.0477
2 Hava limanı	429	63.8460	0.0256	0.1599	58.7275
	1287	59.0080	0.0779	0.2791	53.8895
3 Harput kalesi	459	63.7550	0.0274	0.1655	58.2831
	1377	58.8888	0.0840	0.2898	53.4170
4 Fırat Üniversitesi	485	63.3797	0.0299	0.1728	56.6296
	1455	58.6263	0.0892	0.2987	51.8764
5 Keban barajı	447	63.7938	0.0271	0.1648	56.6108
	1339	59.0520	0.0809	0.2844	51.8692
6 Saklıkapı kanyonu	479	62.5169	0.0296	0.1721	57.6212
	1435	57.7167	0.0895	0.2992	52.8211
7 Palu kalesi	480	63.2996	0.0292	0.1710	57.7279
	1438	58.4991	0.0883	0.2972	52.9273
8 Feti Sekin şehir hastanesi	488	63.4243	0.0296	0.1719	59.6070
	1462	58.6568	0.0886	0.2976	54.8395
9 Kültürpark	453	63.7865	0.0272	0.1649	57.4124
	1357	58.9951	0.0820	0.2863	52.6209
10 Hazar gölü	498	61.3648	0.0298	0.1726	55.9465
	1492	56.5530	0.0902	0.3004	51.1349
11 Alacakaya mermer işletmesi	471	63.4830	0.0292	0.1708	59.6435
	1411	58.7125	0.0875	0.2957	54.8731
12 Çimento fabrikası	496	63.3268	0.0302	0.1739	58.9155
	1486	58.6137	0.0895	0.2991	54.2023
13 Çırçır şelalesi keban alabalık	468	63.5818	0.0285	0.1688	56.9485
	1402	58.8324	0.0851	0.2917	52.1991
14 Kapalı çarşı- izzetpaşa cami	543	62.9854	0.0327	0.1808	57.1281
	1627	58.2088	0.0982	0.3134	52.3514

Tablo 5.3’ te 128x128 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgileri son iki bite gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 51.0869, MSE değeri en yüksek 14. görüntüde 0.3206, RMSE

değeri en yüksek 14. görüntüde 0.5662, SNR değeri en düşük 10. görüntüde 45.9579 olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri 10. görüntüde en düşük 46.3731, MSE değeri en yüksek 14. görüntüde 0.9490, RMSE değeri en yüksek 14. görüntüde 0.9742, SNR değeri en düşük 10. görüntüde 41.2455 olarak hesaplanmıştır.

Tablo 5.3. 128X128 boyutunda ki görüntülerde son iki bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbaba kayak merkezi	423	54.0212	0.2397	0.4896	49.0415
	1269	49.2529	0.7188	0.8478	44.2722
2 Hava limanı	430	53.1236	0.2577	0.5076	48.6520
	1290	48.3220	0.7785	0.8823	43.8510
3 Harput kalesi	459	54.0757	0.2544	0.5044	48.5176
	1377	49.1961	0.7825	0.8846	43.6387
4 Fırat Üniversitesi	484	53.7904	0.2717	0.5212	46.8071
	1452	48.9122	0.8353	0.9140	41.9310
5 Keban barajı	446	53.6560	0.2545	0.5044	46.8072
	1338	48.7538	0.7867	0.8870	41.9058
6 Saklıkapı kanyonu	478	51.9292	0.2775	0.5268	47.8748
	1434	47.3070	0.8043	0.8968	43.2535
7 Palu kalesi	479	53.2198	0.2631	0.5130	48.1350
	1437	48.4154	0.7954	0.8919	43.3318
8 Feti Sekin şehir hastanesi	487	53.2355	0.2873	0.5360	49.6679
	1461	48.4710	0.8605	0.9277	44.9031
9 Kültürpark	452	53.8002	0.2711	0.5206	47.2166
	1356	49.0811	0.8035	0.8964	42.4984
10 Hazar gölü	501	51.0869	0.2930	0.5413	45.9579
	1503	46.3731	0.8676	0.9314	41.2455
11 Alacakaya mermer işletmesi	473	53.5865	0.2847	0.5336	49.6737
	1419	48.9132	0.8351	0.9139	45.0008
12 Çimento fabrikası	495	53.7049	0.2749	0.5243	49.2318
	1485	48.8765	0.8356	0.9141	44.4036
13 Çırçır şelalesi keban alabalık	467	53.8891	0.2656	0.5153	47.1903
	1401	49.1036	0.7993	0.8940	42.4060
14 Kapalı çarşı- izzetpaşa camii	542	53.0709	0.3206	0.5662	47.0261
	1626	48.3580	0.9490	0.9742	42.3134

Tablo 5.4'te 256x256 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgilerin son iki bite gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 57.4126, MSE değeri en yüksek 14. görüntüde 0.0816, RMSE değeri en yüksek 0.0816, SNR değeri en düşük 10. görüntüde 51.9945 olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri 10. görüntüde en düşük 52.7624, MSE değeri en yüksek 14. görüntüde 0.2465, RMSE değeri en yüksek 14. görüntüde 0.4965, SNR değeri en düşük 10. görüntüde 47.3448 olarak hesaplanmıştır.

Tablo 5.4. 256X256 boyutunda ki görüntülerde son iki bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbabakayak merkezi	423	60.1747	0.0605	0.2460	55.0340
	1269	55.5419	0.1759	0.4194	50.4009
2 Hava limanı	430	59.8182	0.0647	0.2543	54.6997
	1290	55.0514	0.1938	0.4402	49.9330
3 Harput kalesi	459	59.7906	0.0682	0.2612	54.3187
	1377	55.1552	0.1984	0.4454	49.6837
4 Fırat Üniversitesi	485	59.6164	0.0710	0.2665	52.8665
	1455	54.8864	0.2111	0.4594	48.1369
5 Keban barajı	450	59.9217	0.0662	0.2573	52.7389
	1350	55.2283	0.1951	0.4417	48.0456
6 Saklıkapıkanyonu	480	58.9226	0.0678	0.2604	54.0270
	1440	54.1063	0.2055	0.4533	49.2110
7 Palu kalesi	480	59.5017	0.0701	0.2648	53.9301
	1440	54.7469	0.2095	0.4577	49.1755
8 Feti Sekinşehir hastanesi	487	59.7031	0.0696	0.2639	55.8858
	1461	54.8564	0.2125	0.4610	51.0390
9 Kültürpark	453	59.8581	0.0672	0.2592	53.4839
	1359	55.0968	0.2011	0.4484	48.7228
10 Hazar gölü	503	57.4126	0.0740	0.2721	51.9945
	1509	52.7624	0.2160	0.4648	47.3448
11 Alacakaya mermer işletmesi	473	59.6680	0.0702	0.2649	55.8286
	1419	54.9993	0.2057	0.4535	51.1601
12 Çimento fabrikası	496	59.7212	0.0693	0.2633	55.3099
	1488	54.8962	0.2106	0.4589	50.4848
13 Çırçır şelalesi keban alabalık	468	59.8414	0.0674	0.2597	53.2081
	1404	55.1077	0.2006	0.4479	48.4745
14 Kapalı çarşı- izzetpaşa camii	549	59.0137	0.0816	0.0816	53.1564
	1647	54.2125	0.2465	0.4965	48.3554

Tablo 5.5'te 128x128 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgileri son üç bite gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 47.1193, MSE değeri en yüksek 14. görüntüde 0.8199, RMSE değeri en yüksek 14. görüntüde 0.9055, SNR değeri en düşük 10. görüntüde 41.9954 olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri en düşük 10. görüntüde 42.4393, MSE değeri en yüksek 14. görüntüde 2.4348, RMSE değeri en yüksek 14. görüntüde 1.5604, SNR değeri en düşük 10. görüntüde 37.3251 olarak hesaplanmıştır.

Tablo 5.5. 128X128 boyutunda ki görüntülerde son üç bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbaba kayak merkezi	423	50.4832	0.5414	0.7358	45.5056
	1269	45.5791	1.6748	1.2941	40.6061
2 Hava limanı	430	49.3416	0.6156	0.7846	44.8733
	1290	44.5275	1.8651	1.3657	40.0653
3 Harput kalesi	459	50.1076	0.6343	0.7965	44.5524
	1377	45.2462	1.9429	1.3939	39.6970
4 Fırat Üniversitesi	485	50.0068	0.6492	0.8057	43.0266
	1455	45.2163	1.9564	1.3987	38.2451
5 Keban barajı	451	49.8394	0.6127	0.7828	42.9941
	1353	45.0128	1.8618	1.3645	38.1762
6 Saklıkapı kanyonu	480	48.0923	0.6713	0.8193	44.0413
	1442	43.3303	2.0095	1.4176	39.2868
7 Palu kalesi	481	49.0866	0.6815	0.8255	44.0049
	1443	44.3486	2.0290	1.4244	39.2728
8 Feti Sekin şehir hastanesi	488	49.5281	0.6746	0.8214	45.9624
	1464	44.7170	2.0425	1.4294	41.1549
9 Kültürpark	454	49.9227	0.6619	0.8136	43.3410
	1362	45.2298	1.9503	1.3965	38.6527
10 Hazar gölü	505	47.1193	0.7306	0.8547	41.9954
	1515	42.4393	2.1462	1.4650	37.3251
11 Alacakaya mermer işletmesi	474	49.9702	0.6547	0.8092	46.0595
	1422	45.0921	2.0131	1.4188	41.1871
12 Çimento fabrikası	497	49.7382	0.6852	0.8278	45.2682
	1491	44.8558	2.1091	1.4523	40.3925
13 Çırçır şelalesi keban alabalık	469	49.8832	0.6680	0.8173	43.1872
	1407	45.0517	2.0319	1.4255	38.3628
14 Kapalı çarşı- izzetpaşa cami	550	48.9929	0.8199	0.9055	42.9503
	1650	44.2661	2.4348	1.5604	38.2298

Aşağıda şekil 5.1’de 128x128 boyutunda ki orijinal görüntü, şekil 5.2’de 128x128 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü, şekil 5.3’te 128x128 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü verilmiştir.



Şekil 5.1. 128x128 boyutunda ki orijinal görüntü



Şekil 5.2. 128x128 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü



Şekil 5.3. 128x128 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü

Tablo 5.6’da 256x256 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgileri son üç bite gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 53,4713, MSE değeri en yüksek 14. görüntüde 0,1982, RMSE değeri en yüksek 14. görüntüde 0.4452, SNR değeri en düşük 48.0544 olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri en düşük 10. görüntüde 48,8411, MSE değeri en yüksek 14. görüntüde 0.6133, RMSE değeri en yüksek 14. görüntüde 0.7832, SNR değeri en düşük 10. görüntüde 43.4272 olarak hesaplanmıştır.

Tablo 5.6. 256X256 boyutunda ki görüntülerde son üç bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbabakayakerkezi	423	56.3166	0.1471	0.3836	51.1764
	1269	51.5980	0.4361	0.6604	46.4587
2 Hava limanı	430	56.1553	0.1503	0.3876	51.0374
	1290	51.3688	0.4524	0.6726	46.2524
3 Harputkalesi	459	56.1007	0.1596	0.3995	50.6296
	1377	51.4150	0.4694	0.6852	45.9454
4 Fırat Üniversitesi	485	56.0610	0.1611	0.4013	49.3117
	1455	51.2823	0.4840	0.6957	44.5349
5 Keban barajı	451	56.0030	0.1632	0.4040	48.8210
	1353	51.3527	0.4762	0.6901	44.1728
6 Saklıkapıkanyonu	481	54.8778	0.1721	0.4148	49.9832
	1443	50.1076	0.5161	0.7184	45.2151
7 Palu kalesi	481	55.7410	0.1666	0.4082	50.1702
	1443	50.9528	0.5019	0.7084	45.3837
8 Feti Sekinşehir hastanesi	488	56.0030	0.1632	0.4040	52.1862
	1464	51.1742	0.4962	0.7044	47.3584
9 Kültürpark	454	55.9848	0.1639	0.4049	49.6110
	1362	51.1593	0.4979	0.7056	44.7865
10 Hazar gölü	505	53.4713	0.1835	0.4283	48.0544
	1515	48.8411	0.5328	0.7300	43.4272
11 Alacakaya mermer işletmesi	474	56.1345	0.1584	0.3979	52.2956
	1422	51.1794	0.4956	0.7040	47.3419
12 Çimento fabrikası	497	55.7941	0.1713	0.4138	51.3836
	1491	51.0528	0.5103	0.7143	46.6437
13 Çırçır şelalesi keban alabalık	469	55.6698	0.1762	0.4198	49.0373
	1407	51.0922	0.5057	0.7111	44.4613
14 Kapalı çarşı- izzetpaşa cami	550	55.1592	0.1982	0.4452	49.3026
	1650	50.2539	0.6133	0.7832	44.3986

Aşağıda şekil 5.4'te 256x256 boyutunda ki orijinal görüntü, şekil 5.5'te 256x256 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü, şekil 5.6'da 256x256 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü verilmiştir.



Şekil 5.4. 256x256 boyutunda ki orijinal görüntü



Şekil 5.5. 256x256 boyutunda son 3 bite 505 karakter veri gizlenmiş görüntü



Şekil 5.6. 256x256 boyutunda son 3 bite 1515 karakter veri gizlenmiş görüntü

Tablo 5.7’de 128x128 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgileri son üç bite tersi alınarak gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 43.3267, MSE değeri en yüksek 14. görüntüde 1.9099, RMSE değeri 1.3820, SNR değeri en düşük 10. görüntüde 38.1939 olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri en düşük 10. görüntüde 39.5817, MSE değeri en yüksek 14. görüntüde 5.6729, RMSE değeri en yüksek 14. görüntüde 2.3818, SNR değeri en düşük 10. görüntüde 33.3841 olarak hesaplanmıştır.

Tablo 5.7. 128X128 boyutunda ki görüntülerde verilerin tersi alındıktan sonra son üç bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbaba kayak merkezi	423	46.4141	1.3818	1.1755	41.4354
	1296	41.5521	4.2332	2.0575	36.5741
2 Hava limanı	430	45.4283	1.5157	1.2312	40.9560
	1290	40.7448	4.4564	2.1110	36.2713
3 Harput kalesi	459	46.1427	1.5806	1.2572	40.5837
	1377	41.2939	4.8271	2.1971	35.7331
4 Fırat Üniversitesi	485	45.7943	1.7126	1.3087	38.8075
	1455	41.0527	5.1028	2.2589	34.0617
5 Keban barajı	451	45.9211	1.5104	1.2290	39.0709
	1353	41.0971	4.5867	2.1417	34.2438
6 Saklıkapı kanyonu	481	44.2640	1.6208	1.2731	40.2077
	1443	40.4846	4.8716	2.2072	35.4272
7 Palu kalesi	481	45.1844	1.6738	1.2937	40.0979
	1443	40.5315	4.8864	2.2105	35.4431
8 Feti Sekin şehir hastanesi	488	45.4743	1.7157	1.3098	41.9068
	1464	40.7935	5.0411	2.2452	37.2262
9 Kültürpark	454	45.9261	1.6614	1.2889	39.3424
	1362	41.3131	4.8058	2.1922	34.7301
10 Hazar gölü	507	43.3267	1.7496	1.3227	38.1939
	1521	39.5817	5.2897	2.2999	33.3841
11 Alacakaya mermer işletmesi	474	46.0601	1.6109	1.2692	42.1459
	1422	41.2493	4.8770	2.2084	37.3327
12 Çimento fabrikası	497	45.7529	1.7155	1.3098	41.2797
	1491	41.1288	4.9749	2.2305	36.6551
13 Çırçır şelalesi keban alabalık	469	46.0530	1.6135	1.2702	39.3532
	1407	41.3142	4.8047	2.1920	34.6121
14 Kapalı çarşı- izzetpaşa cami	550	45.3207	1.9099	1.3820	39.2749
	1650	40.5928	5.6729	2.3818	34.5461

Aşağı da şekil 5.7’de 128x128 boyutunda ki orijinal görüntü, şekil 5.8’de 128x128 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü, şekil

5.9’da 128x128 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü verilmiştir.



Şekil 5.7. 128x128 boyutunda ki orijinal görüntü



Şekil 5.8. 128x128 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü



Şekil 5.9. 128x128 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü

Tablo 5.8'de 256x256 boyutunda ki 14 görüntüye görüntülerin konumu ile ilgili bilgileri son üç bite tersi alınarak gömme işlemi uygulanmıştır. Uygulama sonucunda değerlere bakıldığında PSNR değeri en düşük 10. görüntüde 49.7212, MSE değeri en yüksek 14. görüntüde 0.4923, RMSE değeri en yüksek 0.7016, SNR değeri en düşük 10. görüntüde 44.3021olarak hesaplanmıştır. Karakter boyutunun üç katı büyüklüğü alınıp imgeye gömme işlemi yapıldığında PSNR değeri en düşük 10. görüntüde 44.8983, MSE değeri en yüksek 14. görüntüde 1.4649, RMSE değeri en yüksek 14. görüntüde 1.2103, SNR değeri en düşük 10. görüntüde 39.4776 olarak hesaplanmıştır.

Tablo 5.8. 256X256 boyutunda ki görüntülerde verilerin tersi alındıktan sonra son üç bite gömme işlemi yapıldığında oluşan metrik değerleri

RESİM	KARAKTER BOYUTU	PSNR	MSE	RMSE	SNR
1 Hazarbabakayak merkezi	423	52.4754	0.3563	0.5969	47.3349
	1269	47.6836	1.0740	1.0363	42.5434
2 Hava limanı	430	52.2753	0.3672	0.6059	47.1564
	1290	47.4562	1.1137	1.0553	42.3368
3 Harput kalesi	459	52.1192	0.3992	0.6318	46.6469
	1377	47.3595	1.1944	1.0929	41.8868
4 Fırat Üniversitesi	485	51.9306	0.4169	0.6457	45.1799
	1455	47.1183	1.2626	1.1236	40.3666
5 Keban barajı	451	52.0620	0.4045	0.6360	44.8788
	1353	47.3519	1.1964	1.09388	40.1682
6 Saklıkapıkanyonu	481	51.1894	0.4023	0.6342	46.2935
	1443	46.3312	1.2312	1.1096	41.4350
7 Palu kalesi	481	51.8330	0.4098	0.6402	46.2609
	1443	47.0945	1.2202	1.1046	41.5219
8 Feti Sekinşehir hastanesi	488	51.7376	0.4358	0.6602	47.9204
	1464	46.9684	1.3069	1.1432	43.1514
9 Kültürpark	454	52.0970	0.4012	0.6334	45.7229
	1362	47.2669	1.2201	1.1046	40.8927
10 Hazar gölü	507	49.7212	0.4351	0.6596	44.3021
	1521	44.8983	1.3209	1.1493	39.4776
11 Alacakaya mermer işletmesi	474	51.9094	0.4189	0.6472	48.0697
	1422	47.2448	1.2263	1.1074	43.4046
12 Çimento fabrikası	497	51.8528	0.4244	0.6515	47.4414
	1491	47.0391	1.2858	1.1339	42.6274
13 Çırçır şelalesi keban alabalık	469	52.1641	0.3951	0.6285	45.5305
	1407	47.4056	1.1817	1.0871	40.7717
14 Kapalı çarşı- izzetpaşa cami	550	51.2086	0.4923	0.7016	45.3511
	1650	46.4727	1.4649	1.2103	40.6152

Aşağıda şekil 5.10’da 256x256 boyutunda ki orijinal görüntü, şekil 5.11’de 256x256 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü, şekil 5.12’de 256x256 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü verilmiştir.



Şekil 5.10. 256x256 boyutunda ki orijinal görüntü

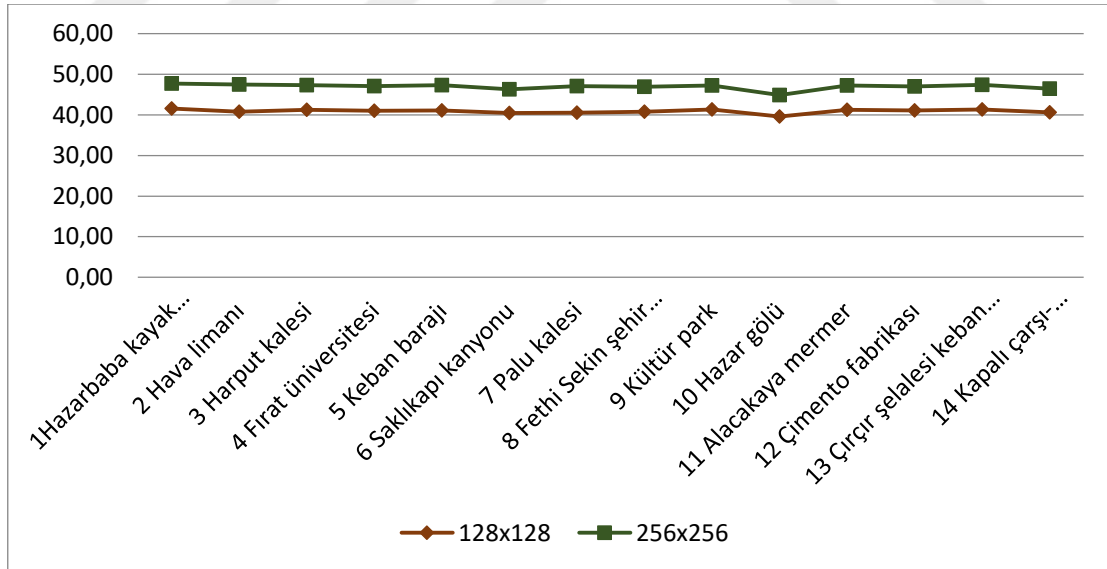


Şekil 5.11. 256x256 boyutunda 507 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü



Şekil 5.12. 256x256 boyutunda 1521 karakter verinin tersi alınarak son 3 bite gömme işlemi yapılmış görüntü

Aşağıda şekil 5.13.' te 128x128 ve 256x256 boyutunda ki uydu üzerinden alınmış 14 görüntüye verilerin üç katı büyüklüğü alınıp ve tersi işlemi uygulandıktan sonra son üç bite veri gizleme işlemi yapıldığında ortaya çıkan PSNR değerlerinin karşılaştırması grafik olarak verilmiştir.



Şekil 5.13. 128x128 ve 256x256 büyüklüğünde ki 14 görüntüye verilerin üç katı büyüklüğü alınıp tersi işlemi uygulandıktan sonra ki PSNR değerleri

6. SONUÇLAR

Uydu imgelerine veri gizleme işlemi yapılırken gizlenen bit sayısı, imgenin boyutu, verinin uzunluğu ve verinin tersi gibi parametrelerin PSNR değerine etkisine bakılarak görüntüde ki bozulmalar karşılaştırılmıştır.

Tez amacına ulaşmak için yapılan uygulamaların karşılaştırılması ile uydu imgelerine veri gizleme işlemi yapılırken görüntünün boyutu arttıkça veri gizleme kapasitesi arttığı için 256x256 boyutunda ki imgelerde PSNR değeri artmış ve başarı oranının daha yüksek olduğu görülmüştür. Uydu imgelerine gizlenen verilerin üç katı büyüklüğü alınıp gömme işlemi yapıldığında PSNR değeri azalmış ve görüntüde ki bozulmalar artmıştır. LSB tekniği ile yapılan en anlamsız bite gizleme işleminde gizlenen bit sayısı arttıkça PSNR değeri azalmış ve görüntüde ki bozulmalara artmıştır. Gizlenecek verinin tersi alınıp PSNR değerine bakıldığında PSNR değerinde büyük bir artış görülmemiştir.

Yapılan uygulamalar sonucunda 256x256 ve 128x128 boyutlarında ki 28 görüntüye bakıldığında 128X128 boyutunda ki görüntülerin PSNR değerlerinin daha düşük çıktığı gözlemlenmiştir. PSNR değeri genel olarak 10. görüntü de ve veri boyutunun 3 katı alınıp gizlendiğinde en düşük olarak hesaplanmıştır. 128X128 boyutunda ki veriler 8. bite gömüldüğünde en düşük 1491 karakterde 50.1252, 7 ve 8. bite gömüldüğünde en düşük 1503 karakterde 46.3731, 6, 7 ve 8. bite gömüldüğünde en düşük 1515 karakterde 42.4393 olarak hesaplanmıştır. Sonuç olarak PSNR değeri en düşük 128x128 boyutunda ki görüntüde son üç bite verinin tersi işlemi alınıp gizleme işlemi yapıldığında 10. görüntü de ve 1521 karakter veri gizlendiğinde 39.5817 olarak hesaplanmıştır. PSNR değeri %40'a yakın olduğu için görüntüde ki bozulmalar gözle görünmemektedir.

KAYNAKLAR

- [1] Durdu, A., & Özcerit, A. (2015). Güvenli iletişim için yeni bir veri gizleme algoritması. uluslararası bilgi güvenliği mühendisliği dergisi, 1(1), 32-36.
- [2] Çivicioğlu, P.& Alçı, M. Güvenli İletişim İçin Veri Gizleme Tekniklerinin Kullanımı.
- [3] Roy, C. Y., & Goel, M. K. (2016). Review on image steganography. Indian J. Sci. Technol, 9(47), 1-5.
- [4] Sharma, U. (2019). A review on various approaches of data hiding for secure data transmission.
- [5] Chapman, M., Davida, G. I., & Rennhard, M. (2001, October). A practical and effective approach to large-scale automated linguistic steganography. In International Conference on Information Security (pp. 156-165). Springer, Berlin, Heidelberg.
- [6] Islam, A. U., Khalid, F., Shah, M., Khan, Z., Mahmood, T., Khan, A., ... & Naeem, M. (2016, August). An improved image steganography technique based on MSB using bit differencing. In 2016 Sixth International Conference on Innovative Computing Technology (INTECH) (pp. 265-269). IEEE.
- [7] Prashanti, G., Jyothirmai, B. V., & Chandana, K. S. (2017, April). Data confidentiality using steganography and cryptographic techniques. In 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-4). IEEE.
- [8] Sharma, S., & Sejwar, V. (2016, December). Impementation of QR code based secure system for information sharing using Matlab. In 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 294-297). IEEE.
- [9] Al-Tamimi, A. G. T., & Alqobaty, A. A. (2015). Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm. International Journal of Computer Science and Information Security, 13(1), 1.
- [10] Das, S. K., & Dhara, B. C. (2015, April). An image secret sharing technique with block based image coding. In 2015 Fifth International Conference on Communication Systems and Network Technologies (pp. 648-652). IEEE.
- [11] Das, P., Kushwaha, S. C., & Chakraborty, M. (2015, February). Multiple embedding secret key image steganography using LSB substitution and Arnold Transform. In 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (pp. 845-849). IEEE.
- [12] Sun, S. (2016). A novel edge based image steganography with 2k correction and Huffman encoding. Information Processing Letters, 116(2), 93-99.
- [13] Şentürk, Z., Vatankulu, Y. E., & Durna, Y. LSB Yöntemiyle Renk Değişimi Esaslı Yeni Bir Steganografik Yaklaşım A New Steganographic Approach Based On Color Change With LSB Method.
- [14] Alattar, Adnan M.; Alattar, Usame Muhammed. Yaslanmış paragraflar ve düzensiz satır aralığı içeren elektronik metin belgelerine filigran ekleme. İçinde: Çoklu Ortam İçeriklerinin Güvenliği, Steganografisi ve Filigranı VI . Uluslararası Optik ve Fotonik Topluluğu, 2004. s. 685-695.
- [15] Liu, Yuling; Yang, Ting; Xin, Guojing. İfadelere ve ünlemlere dayalı sohbet metin steganografisi. Hesaplamalı ve Teorik Nanobilim Dergisi , 2015, 12.9: 2091-2094.
- [16] Djebbar, Fatiha, vd. Dijital ses steganografi tekniklerinin karşılaştırmalı incelenmesi. EURASIP Ses, Konuşma ve Müzik İşleme Dergisi , 2012, 2012.:25.
- [17] Murdoch, Steven J .; Lewis, Stephen. Gizli kanalları TCP / IP'ye gömme. In: Uluslararası Bilgi Gizleme Çalıştayı . Springer, Berlin, Heidelberg, 2005. s. 247-261.

- [18] Mazurczyk, Wojciech; Smolarczyk, Milosz; Szczypiorski, Krzysztof. Yeniden iletim steganografisi ve saptanması. Yumuşak Hesaplama , 2011, 15.3: 505-515.
- [19] Santoso, Kevin Nathanael, vd. DNA steganografisi için kodlamayan DNA'da saklanan bilgiler. Elektronik, İletişim ve Bilgisayar Bilimlerinin Temelleri üzerine IEICE İşlemleri , 2015, 98.7: 1529-1536.
- [20] Sadek, Mennatallah M.; Khalıfa, Amal S.; Mostafa, Mostafa GM. Video steganography: a comprehensive review. Multimedia tools and applications, 2015, 74.17: 7063-7094.
- [21] Zielińska, Elżbieta; Mazurczyk, Wojciech; Szczypiorski, Krzysztof. Steganografide eğilimler. ACM'nin İletişimleri , 2014, 57.3: 86-95.
- [22] Hussain, Mehdi, et al. Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 2018, 65: 46-66.
- [23] Sönmez, Ferdi; Takaoğlu, Faruk; Kaynar, Oğuz. İdeal Steganografi Senaryosu: Taşıyıcı Resimlerin Kapasitelerinin Hesaplanması, Frekans Tabanlı Steganografide OPA Yöntemi. Acta INFOLOGICA, 2.1: 12-21.
- [24] Kharrazi, Mehdi; Sencar, Husrev Taha; Memon, Nasir D. Performance study of common image steganography and steganalysis techniques. Journal of Electronic Imaging, 2006, 15.4: 041104.
- [25] Johnson, Neil F.; Jajodia, Sushil. Steganalysis: The investigation of hidden information. In: 1998 IEEE Information Technology Conference, Information Environment for the Future (Cat. No. 98EX228). IEEE, 1998. p. 113-116.
- [26] Wang, Huaiqing; Wang, Shuozhong. Siber savaş: steganografi ve steganaliz. ACM'nin İletişimleri , 2004, 47.10: 76-82.
- [27] Ker, Andrew D. Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, 2005, 12.6: 441-444.
- [28] Fridrich, Jessica; Goljan, Miroslav; Du, Rui. Renkli ve gri tonlamalı görüntülerde LSB steganografisinin güvenilir tespiti. İçinde: Multimedya ve güvenlik üzerine 2001 çalıştayının bildirileri: yeni zorluklar . 2001. s. 27-30.
- [29] Westfeld, Andreas; Pfitzmann, Andreas. Attacks on steganographic systems. In: International workshop on information hiding. Springer, Berlin, Heidelberg, 1999. p. 61-76.
- [30] Zhang, Hao, vd. Eksiltici piksel bitişik matrisi ve boyut indirgeme ile steganaliz. Science China Information Sciences , 2014, 57.4: 1-7.
- [31] Fridrich, Jessica; Kodovsky, Ovac. Dijital görüntülerin steganalizi için zengin modeller. Bilgi Adli Tıp ve Güvenlik IEEE İşlemleri , 2012, 7.3: 868-882.
- [32] Denemark, Tomas, et al. Selection-channel-aware rich model for steganalysis of digital images. In: 2014 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2014. p. 48-53.
- [33] Sedighi, Vahid; Cograne, Rémi; Fridrich, Jessica. Content-adaptive steganography by minimizing statistical detectability. IEEE Transactions on Information Forensics and Security, 2015, 11.2: 221-234.
- [34] Sharma, Urvashi. A review on various approaches of data hiding for secure data transmission. 2019.
- [35] Özbılın, Ferdi; Durmuş, Fatih; Karagöl, Serap. Yazılı Metni Şifreleyip LSB Yöntemi ile Gizleme. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 6.3: 676-685.
- [36] Ndajah, Peter, et al. SSIM image quality metric for denoised images. In: Proc. 3rd WSEAS Int. Conf. on Visualization, Imaging and Simulation. 2010. p. 53-58.