

KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

HİBRİT YAKLAŞIMLI YENİ BİR STEGANOĞRAFI YÖNTEMİNİN
GELİŞTİRİLMESİ

HARUN KURNAZ

KOCAELİ 2019

KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

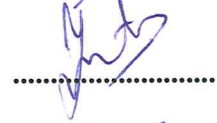
HİBRİT YAKLAŞIMLI YENİ BİR STEGANOĞRAFI
YÖNTEMİNİN GELİŞTİRİLMESİ

HARUN KURNAZ

Dr. Öğr. Üyesi Adnan SONDAŞ
Danışman, Kocaeli Üniversitesi

Prof. Dr. Mehmet YILDIRIM
Jüri Üyesi, Kocaeli Üniversitesi

Doç. Dr. Cüneyt BAYILMIŞ
Jüri Üyesi, Sakarya Üniversitesi


.....

.....

.....

Tezin Savunulduğu Tarih: 18.02.2019

ÖNSÖZ VE TEŞEKKÜR

Bu tez çalışması, histogram temelli yeni bir veri gizleme algoritması geliştirilerek diğer üç farklı yöntemle göre başarımlar değerlendirilmesi amacıyla gerçekleştirilmiştir.

Tez çalışmamda desteğini esirgemeyen, çalışmalarına yön veren, bana güvenen ve yüreklendiren danışmanım Dr. Öğr. Üyesi Adnan SONDAŞ'a sonsuz teşekkürlerimi sunarım.

Hayatım boyunca bana güç veren en büyük destekçim, her aşamada sıkıntılarımı ve mutluluklarımı paylaşan sevgili eşim Nesrin KURNAZ'a ve oğlum Ayaz KURNAZ'a minnettarım.

Ocak -2019

Harun KURNAZ

İÇİNDEKİLER

ÖNSÖZ VE TEŞEKKÜR	i
İÇİNDEKİLER	ii
ŞEKİLLER DİZİNİ.....	iv
TABLOLAR DİZİNİ	v
SİMGELER VE KISALTMALAR DİZİNİ	vi
ÖZET.....	vii
ABSTRACT.....	viii
GİRİŞ	1
1. KAYNAK ARAŞTIRMASI.....	3
1.1. Veri Gizleme	4
1.2. Kriptoloji.....	5
1.3. Damgalama	6
1.4. Steganografi	7
1.4.1. Steganografinin tarihçesi.....	9
1.4.2. Steganografinin alt alanları	10
1.4.2.1. Ses steganografisi.....	11
1.4.2.2. Video steganografisi.....	11
1.4.2.3. Metin steganografisi.....	12
1.4.2.4. Network steganografisi	12
1.4.2.5. Görüntü (Image) steganografisi	12
1.4.3. Uzamsal alan steganografi yöntemleri	12
1.4.4. Frekans uzayında steganografi yöntemleri.....	13
1.5. Sayısal Görüntü ve Temel Kavramlar.....	14
1.5.1. Piksel.....	14
1.5.2. Histogram.....	16
1.5.3. Görüntü formatları	17
1.5.3.1. Bmp.....	17
1.5.3.2. Jpeg/Jpg.....	17
1.5.3.3. Png	18
1.5.3.4. Tiff	18
1.5.3.5. Gif	18
2. VERİ GİZLEME YÖNTEMLERİ	19
2.1. LSB Veri Gizleme Yöntemi.....	19
2.2. Histogram Temelleri Veri Gizleme Yöntemi(HSV)	21
2.3. Maksimum Histogramlar Yöntemi (MHY)	22
2.4. Yakın Histogramlar Yöntemi (YHY)	25
3. UYGULAMA YAZILIMI VE YÖNTEMLERİN ÇIKTISININ DEĞERLENDİRİLMESİ.....	30
3.1. Test Yöntemi.....	30
3.2. Uygulama Yazılımının Tanıtılması.....	32
3.3. Örnek Uygulamalar ve Başarım Değerlendirilmesi.....	34
4. SONUÇLAR VE ÖNERİLER	41
KAYNAKLAR	43

KİŞİSEL YAYIN VE ESERLER	48
ÖZGEÇMİŞ	49



ŞEKİLLER DİZİNİ

Şekil 1.1.	Veri gizleme yöntemleri.....	5
Şekil 1.2.	Kriptografi yöntemi.....	6
Şekil 1.3.	Resim üzerinde gerçekleştirilen damgalama örneği.....	7
Şekil 1.4.	Temel steganografi sistemi	8
Şekil 1.5.	Fridrich üçgeni	9
Şekil 1.6.	Steganografi biliminin uygulama şekillerine göre sınıflandırılması	10
Şekil 1.7.	Piksel yapısı ve renk bileşenleri	15
Şekil 1.8.	24-bit bir resmin piksel haritasındaki bileşen değerleri	15
Şekil 1.9.	Bir imge histogramına ait parlaklık ve frekans değerleri.....	17
Şekil 2.1.	LSB veri gizleme yöntemi	19
Şekil 2.2.	HSV yöntemi veri gizleme ve ortaya çıkarma akış şemaları	22
Şekil 2.3.	MHY’de parlaklık değeri seçimi.....	23
Şekil 2.4.	MHY’de veri gizleme ve veriyi ortaya çıkarma akış şemaları.....	25
Şekil 2.5.	YHY’de gömülecek bitler için parlaklık değeri tespiti	26
Şekil 2.6.	YHY’de veri gizleme akış şeması.....	27
Şekil 2.7.	YHY’de gizli veriyi çıkarma akış şeması	29
Şekil 3.1.	Uygulama yazılımının görseli	33
Şekil 3.2.	Uygulama yazılımının analiz formu görseli.....	34
Şekil 3.3.	Örnek bir resim için elde edilen histogram değerleri.....	34
Şekil 3.4.	Uygulama yazılımında kullanılan referans resimlerin orijinal halleri (a-Lena, b-Peppers, c-Airplane, d-Babbon).....	35
Şekil 3.5.	Lena referans resminin yöntem-I için veri gömmeden önce (a) ve gömüldükten sonraki (b) histogram grafikleri	38
Şekil 3.6.	Airplane referans resminin yöntem-II için veri gömmeden önce (a) ve gömüldükten sonraki (b) histogram grafikleri	38
Şekil 3.7.	Babbon referans resminin yöntem-III için veri gömmeden önce (a) ve gömüldükten sonraki (b) histogram grafikleri	39
Şekil 3.8.	Peppers referans resminin yöntem-IV için veri gömmeden önce (a) ve gömüldükten sonraki (b) histogram grafikleri	39

TABLÖLAR DİZİNİ

Tablo 2.1. LSB yöntemi veri gizleme örneği	20
Tablo 2.2. MHY’de örnek bir resim bileşen değeri.....	23
Tablo 2.3. Resim histogramına ait bazı sayısal değerler	27
Tablo 3.1. PSNR başarımlar değeri	36
Tablo 3.2. MSE başarımlar değeri.....	36
Tablo 3.3. Bozulmuş piksel sayıları	36
Tablo 3.4. Piksel bozulma oranları.....	36
Tablo 3.5. Yöntem I’in referans resimlerde uygulanması	38
Tablo 3.6. Yöntem II’in referans resimlerde uygulanması.....	38
Tablo 3.7. Yöntem III’in referans resimlerde uygulanması	38
Tablo 3.8. Yöntem IV’in referans resimlerde uygulanması	38
Tablo 3.9. StegSPy yazılımı sonuçları.....	40
Tablo 3.10. Stegdetect yazılımı sonuçları	40

SİMGELER VE KISALTMALAR DİZİNİ

I	: Giriş görüntüsü
I_0	: Çıkış görüntüsü
M	: Sütun sayısı
N	: Satır sayısı

Kısaltmalar

ASCII	: American Standard Code for Information Interchange (Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi)
AVI	: Audio Video Interleave (Ses Video Interlive)
BMP	: Bitmap (Dosya Biçimi)
CMYK	: Cyan Magenta Yellow Key (Cam Göbeği, Eflatun, Sarı, Siyah)
dB	: Desibel
FPS	: Frame Per Second (Saniyedeki Çerçeve)
HSV	: Histogram Temelli Veri Gizleme Yöntemi
IP	: İnternet Protokolü
İGS	: İnsan Görme Sistemi
JPEG	: Joint Photographic Experts Group (Sayısal Görüntü Kodlama Biçimi)
LSB	: Least Significant Bit Methods (En Önemsiz Bit)
MHY	: Maksimum Histogramlar Yöntemi
MÖ	: Milattan Önce
MPEG	: Motion Pictures Experts Group (Hareketli Görüntü Uzmanlar Birliği)
MSE	: Mean Squared Error (Ortalama Karesel Hata)
OSI	: Open System Interconnection (Açık Sistem Ara Bağlantısı)
PD	: Parlaklık Değeri
PNG	: Portable Network Graphics (Taşınabilir Ağ Grafiği)
PSNR	: Peak Signal to Noise Ratio (Tepe Sinyal Gürültü Oranı)
RGB	: Red Green Blue (Kırmızı Yeşil Mavi)
TCP	: Transmission Control Protocol (Transfer Kontrol Kuralı)
TIFF	: Tagged Image File Format (Resim Dosya Biçimi)
VF	: Varlık Frekansı
YHY	: Yakın Histogramlar Yöntemi

HİBRİT YAKLAŞIMLI YENİ BİR STEGANOĞRAFI YÖNTEMİNİN GELİŞTİRİLMESİ

ÖZET

Verinin gizlenmesi farklı ortamlar üzerinde sıklıkla yapılmakta ve bu alanda ki uygulamalar oldukça ilgi görmektedir. Sayısallaşan dünyada veri aktarım hızları, iletişim yöntemlerinin çeşitlenmesi ile bilgi gizleme çalışmalarının önemini artırmaktadır. Gizli bilginin üçüncü şahıslar tarafından algılanmaması, istenen kişilerin veriyi ortaya çıkarması bu çalışmalarda temel amaçtır. Gizlenen veri kapasitesinin artırılması, örtü verideki değişimi azaltmak ve tespitini zorlaştırmak steganografi uygulamalarındaki hedeflerdir.

Steganografik alanında geliştirilen uygulamalar ve güncel araştırmalar taranmıştır. Literatür bulguları temel alınarak yeni bir veri gizleme yöntemi önerilmiştir. Sayısal görüntülerdeki piksellerin parlaklık değerine göre dağılımını histogram grafiği göstermektedir. Önerilen yöntem, histogram grafiğini saklama yapılacak piksel değerlerinin tespitinde kullanılmaktadır. Veri üzerindeki değişimi minimize ederek histogram değerlerinin korunması sağlanmıştır.

Bu çalışmanın amacı, geliştirilen hibrit yaklaşımlı yeni bir veri gizleme yönteminin uygulama ortamında hazırlanarak diğer farklı üç veri gizleme yöntemi ile karşılaştırmalı başarımlar değerlendirilmesinin yapılmasıdır.

Önerilen yöntemin PSNR, MSE ve bozulan piksel değerlerinin diğer yöntemlerden daha başarılı sonuçlar verdiği görülmüştür.

Anahtar Kelimeler: Hibrit Veri Gizleme, Histogram, LSB, Steganografi.

THE DEVELOPMENT OF A NEW HYBRID APPROACHED STEGANOGRAPHY METHOD

ABSTRACT

The concealment of the data is frequently performed on different environments and the applications in this area are very popular. Data transfer rates in the digitized world is increasing the importance of information hiding work with the diversification of communication methods. The main purpose of these studies is that the confidential information is not perceived by third parties and the requested persons reveal the data. Increasing the hidden data capacity, reducing the change in cover data and making the detection difficult are the targets in steganography applications.

The applications which were developed in the field of stegonografik and current researches were scanned. The distribution of the pixels in digital images according to the brightness value shows the histogram graph. The proposed method uses the histogram graph to determine the pixel values to be stored. The histogram values are preserved by minimizing the change on the data.

The aim of this study is to prepare a new data hiding method with a hybrid approach in the application environment and to make a comparative performance evaluation of it with the other three different data hiding methods.

PSNR, MSE and deteriorated pixel values of the proposed method were found to be more successful than other methods.

Keywords: Hybrit Data Hidding, Histogram, LSB, Steganography.

GİRİŞ

Teknolojinin gelişmesiyle birlikte verinin güvenliğinin sağlanması, günümüzün en büyük problemi haline gelmiştir. Bu doğrultuda şirketlerin dijital platformlardaki güvenlikleri için ayırdıkları miktar her geçen gün artmakta sonucunda da güvenlik yöntemleri gelişmektedir. Milattan önce dahi kullanılan gizli haberleşme yöntemleri günümüzde farklı yöntem ve platformlarda da ortaya çıkmaktadır. İnternetin hayatımıza girmesi, haberleşmenin sayısallaşması ve sayısal verileri işleyen ürünlerin çeşitlenmesi sonucunda, steganografi uygulamalarının sayısal ortamlarda kullanılmasına başlanmıştır.

Steganografinin gelişmesine paralel olarak gelişen bir diğer bilim ise steganalizdir. Amacı ise steganografinin tam tersine, veri saklanan her ortamdaki gizli verinin ortaya çıkarılmasını amaçlamaktadır [1]. Steganaliz, taşıyıcı objeler ile stego objeleri arasında ayrımı yapmak üzere geliştirilmiş teknikler bütünüdür. Temelinde obje üzerinde saklanan verinin bir takım izler bıraktığı düşüncesidir. Saklama sonrasında oluşan stego nesne, görsel, işitsel veya işlevsel olarak orijinalinden ayırt edilemez olsa da istatistiksel olarak belirgin farklılıkları saptamaya çalışır [2].

Yapılan bu tez çalışmasında, geliştirilen arayüz aracılığı ile sayısal görüntü içerisine dört farklı yöntem kullanılarak veri gizlemesi yapılmış ve sonuçları uygulamalı olarak karşılaştırılmıştır. Kullanılan bu yöntemler, Klasik LSB Yöntemi [3], HSV Yöntemi [4], Maksimum Histogramlar Yöntemi (MHY)[3] ve önerilen Yakın Histogramlar Yöntemi (YHY)'dir.

Tezin genel düzeni şu şekilde belirlenmiştir;

Bölüm 1’de, görüntü steganografisinde temel olan resim, histogram, piksel ve resim türleri anlatılarak, literatürde veri gizleme içerisinde yer alan şifreleme, damgalama ve steganografi terimleri açıklanarak farklılıkları sunulmuştur.

Bölüm 2’de, uygulama üzerinde gerçekleştirilen dört farklı veri gizleme yöntemi anlatılmaktadır. Yöntemlerin algoritmaları akış şemaları gösterilerek örnekler ile detaylandırılmaktadır.

Bölüm 3’te, geliştirilen uygulama yazılımı tanıtılarak, program çıktıları elde edilmiştir. Deneysel sonuçlara ilişkin başarımlar analizleri detaylandırılarak sunulmaktadır. Referans steganaliz yazılımları kullanılarak yöntemler değerlendirilmiştir.

Bölüm 4’te, sonuç ve değerlendirmeler ifade edilmektedir.



1. KAYNAK ARAŞTIRMASI

Bu bölümde literatürde yer alan ve günümüze kadar yapılmış birçok veri gizleme çalışmaları kısaca özetlenerek, şifreleme(kriptoloji), damgalama(watermarking) ve steganografi terimleri açıklanmıştır.

RGB ağırlık tabanlı geliştirilen kodlama ile gömü veri kapasitesinin artırıldığı yöntem önerilmiştir [5]. Yöntemin PSNR değerleri ve görsel analiz başarıları yüksek ancak histogram çıktıları gömülen veri ile tarak etkisi oluşturmaktadır. Kapasite başarımı açısından başarılı bir yöntemdir.

Resim histogramlarının kullanıldığı ver gizleme yöntemi [6] önerilmiştir. Yöntemin gömü kapasite değerleri ve PSNR değerleri düşüktür. Histogramda oluşturduğu değişimler algılanamayacak seviyelerdedir. Yöntemin görsel ataklara karşı dayanıklılığı hakkında bilgi verilmemiştir.

Histogram bilgisinin kullanılarak geliştirilen veri gizleme yöntemi [7] önerilmiştir. Yöntem histogram bilgisinin dairesel bir çevrimde dizilimin esas olarak veri gizleme yapmaktadır. Yöntem, PSNR değerleri kabul edilebilir seviyelerde sonuç üretirken gömü verisi kapasite değerleri düşüktür.

İmgeyi oluşturan renk bileşenlerinin histogram değerleri ayrı ayrı oluşturularak bileşenler üzerine veri gömme işlemi yöntemi uygulanmıştır [8]. Yöntem de piksel kanalındaki pikseller için ortalama hesaplanarak en az önemli bit(LSB) kullanılarak gömme işlemi gerçekleştirilmiştir. PSNR değerleri kabul edilebilecek seviyelerde ve histogram tarak etkisi oluşmamaktadır.

Orijinal kapak görüntüsünün ve stego görüntüsü histogramları arasındaki farkları en aza indirmek görüntüdeki her bir renk değerinin frekansına zıt değişiklikler yaparak renklerin değişmeden korunmasını sağlayan yöntem önerilmiştir [9]. Yöntem en az önemli bit(LSB) yöntemine göre kıyaslamalar içermektedir. PSNR, MSE ve mesaj boyutları açısından değerlendirilmiştir.

Histogram deęiřiklięi yapılarak kayıpsız veri gömme yöntemi önerilmiştir [10]. Oluřturulan algoritma ile belli aralıktaki histogram parlaklık deęerleri algoritmanın yürütölmesinde kullanılmıştır. Lena, Peppers, Babbon, Airplane referans resimleri üzerindeki yüksek kapasitelerde veri gömme sonucu oluřan PSNR başarımları yüksektir.

RGB görüntüler için veri gömme kapasitesi yüksek yöntem önerilmiştir [11]. Yöntem resmin bileřen kanalları olana RGB üzerinde kanalın ikisinde verileri birinde ise rastgele piksel manipölasyonlarını saklamaktadır. Kapasite deęerleri olarak yüksek kapasite sonuçları vermektedir. Yöntemin başarıml deęerlerine yer verilmemiřtir.

Parlaklık deęerlerinin tekrarlanma sayıları kullanılarak veri gizleme yöntemi önerilmiştir [4]. Yöntem de imge histogramı oluřturularak parlaklık deęer aralıęı ve tekrarlanma sayıları belirlenir. Gömöllecek bit deęerine göre tekrarlanma sayıları kullanılarak veri gömme iřlemi geręeklenir. Önerilen yöntem PSNR ve MSE deęerleri kullanılarak farklı yöntemler ile karřılařtırılmıştır. Başarıml seviyesi dięer yöntemlere göre üstün olduęu tespit edilmiştir. Görsel ataklara karřı dayanıklılıęı yüksek olmasına karřı veri gömme kapasitesi düşüktür. Tez kapsamında geliřtirilen yöntemin bu yöntem ile karřılařtırmalı başarımlı deęerlendirilmiştir.

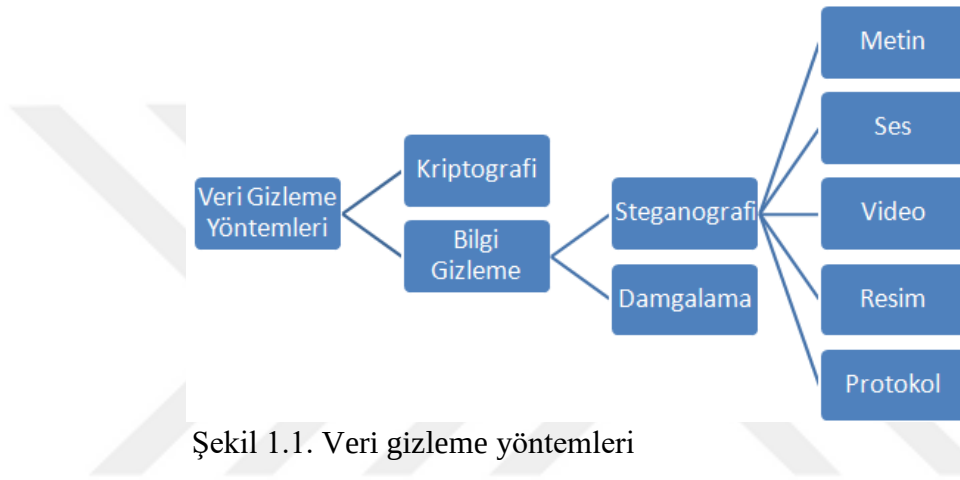
İmge histogram bilgisi oluřturup, en fazla tekrar eden parlaklık deęerine göre algoritma oluřturularak veri gömme yöntemi önerilmiştir [12]. Yöntem de referans resimler üzerinde PSNR ve MSE oranları deęerlendirilmiştir. Histogram modifikasyonu yapılarak kayıpsız veri gizleme yaptıęı savunulmuřtur.

1.1. Veri Gizleme

Dijital sistemler ięerisinde verinin güvenlięi, bilginin řifrelenmesi (kriptografi) ve/veya bilginin saklanması yöntemleri kullanılarak saęlanmaya ęalıřılmaktadır. Kriptografi yönteminde bilgi řifrelendięi için dięer kiřiler mesajlara rahat bir řekilde ulařabilirler fakat řifreyi bilmedikleri için bilgiye ulařamamaktadırlar. Bu durum, ilgisiz kiřilerin merakını uyandırmakta ve řifreyi ęözerek bilgiye ulařmaya teřvik etmektedir. Bilgi gizleme yöntemlerinde ise bilgi farklı bir ortamın ięerisine gizlenerek ilgili kiřilere ulařtırılmaktadır. Bu yöntemde mesaj ilgisiz kiřilerin eline

geçse dahi içerisinde bilgi gizli olduğunu bilmediklerinden dolayı bilgiye ulaşmak için çaba harcamayacaklardır.

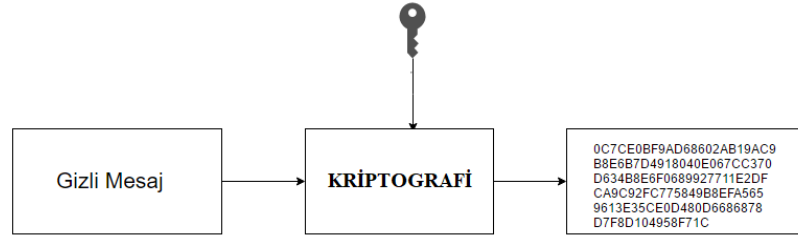
Bilgi gizleme uygulamaları, steganografi ve damgalama olmak üzere iki ayrı temele ayrılmaktadır. Literatürde yer alan çalışmalarda, dijital ortamlarda gerçekleştirilen steganografi uygulamalarında, 5 farklı dosya formatı (metin, ses, video, resim, protokol) kullanılmaktadır [13]. Şekil 1.1’ de, yukarıda anlatılan veri gizleme yöntemleri grafiksel olarak gösterilmiştir.



Şekil 1.1. Veri gizleme yöntemleri

1.2. Kriptoloji

Şifreleme (Cryptography) kelimesi, “secret (crypto-)” ve “writing (-graphy)” kelimelerinden türetilmiş ve gizli yazı anlamına gelmektedir. Kriptografi, haberleşen iki veya daha fazla tarafın bilgi alış verişini emniyetli olarak yapmasını sağlayan ve gizli ya da özel bilgiyi istenmeyen kişilerin anlayamayacağı hale getirerek korumayı esas alan, temeli matematiksel yöntemlere dayalı tekniklerin ve uygulamaların bütünüdür [14]. Gizli anahtara sahip olmayan bir kişinin mesajı elde etmesini önlemek amaçlanır. Verinin varlığını gizlemek değil, gizli verinin içeriğini korumak hedeflenir. Şekil 1.2’ de, kriptografi yöntemi grafiksel olarak gösterilmiştir.



Şekil 1.2. Kriptografi yöntemi

Gizlenmesi gereken mesaj, bir algoritma kullanılarak şifrelenir ve şifreli mesajın kendisi herhangi bir taşıyıcı kullanılmadan gönderilir. Alıcı, aldığı mesajı elindeki anahtarı kullanarak çözer ve bilgiyi elde eder [15]. Şifrelenmiş verinin güvenliği, büyük oranda şifreleme algoritmasının dayanıklılığı ve anahtarın gizliliğine bağlıdır.

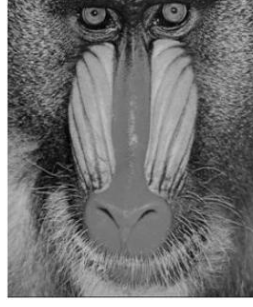
Güvenli şifreleme yöntemleri temel olarak iki grupta incelenebilir. Şifreleme ve şifre açma aynı anahtarla yapılan “simetrik kriptografi” ve şifreleme ve şifre çözmenin farklı anahtarlar ile yapıldığı “asimetrik kriptografi”dir [16].

1.3. Damgalama

Günümüzdeki teknolojik gelişmeler sonucunda sayısal resim, film, ses ve çoklu ortam uygulamaları günlük hayatımızın bir parçası haline gelmiştir. Özellikle internet aracılığıyla sayısal ürünlere çok kolay bir şekilde erişilebilmekte veya kopyalama yapılabilmektedir. Bu durum sonucunda ise telif hakkı problemleri ile karşılaşmaya başlanmıştır. Sayısal teknolojiden kaynaklanan telif hakkı problemlerinin giderilmesi konusunda çeşitli yöntemler uygulanmıştır. Damgalama, telif haklarını korumak (Copyright protection), doğrulama yapmak (Authentication), gizli haberleşme yapmak ve imge hakkında açıklayıcı bilgi saklamak için en sık kullanılan yöntemlerden birisidir. Bu yöntemde, imgenin içine bir logonun (damga, watermark) çeşitli yöntemlerle görünmeyecek şekilde eklenmektedir. Gerçekleştirilen bu işlem, damgalama (watermarking) olarak adlandırılmaktadır[17]. Bir resim üzerine yapılan damgalama örneği Şekil 1.3’te verilmiştir.



Orijinal Resim



Damga



Damgalanmış Resim

Şekil 1.3. Resim üzerinde gerçekleştirilen damgalama örneği

Literatürdeki birçok çalışmada, damgalama ve steganografi kavramları birbiri ile karıştırılmaktadır. Söz konusu iki kavram tanımları ve gereksinimleri itibariyle birbirinden çok farklıdır. Gizlenen verinin kullanım amacı kavramların en büyük farklılığını oluşturmaktadır. Damgalama da gizlenen veri, telif haklarına ait olan veya bütünlük kontrolü sağlayan bir bilgidir. Her iki tipteki damgalama bilgisi, içine saklandıkları taşıyıcı veri ile bir şekilde alakalıdır. Steganografi de ise gömülen veri taşıyıcı veriden tamamen bağımsız mesajlarından oluşur [13]. Her iki yöntemde de en önemli kıstas, gizlenen verinin farkına varılamamasıdır.

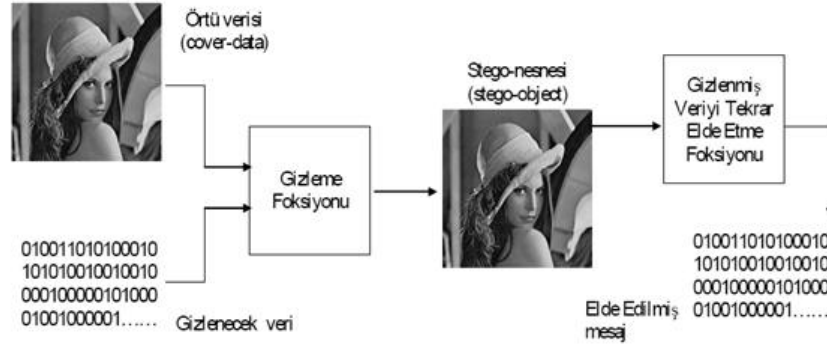
Dayanıklılık, algılanamazlık, güvenlik, hızlı gizleme, geri elde etme ve orijinal resme ihtiyaç duymama sayısal damgalamanın sağlaması gereken gereksinimlerdir. Gereksinimler sayısal damgalamanın kullanılacağı yere göre değişiklik gösterebilir [18]. Bazı uygulamalar için görüntüde yapılacak küçük değişiklikler bile kabul edilmez durumdadır. Örneğin askeri görüntüler yüksek stratejik önem arz edeceği gibi, tıbbi sonuç görüntülerinin de hayati derecede önemli değerleri vardır. Bu ve benzeri durumlar kayıpsız damgalama gerektiren görüntüler arasında yer alır [19].

1.4.Steganografi

Steganografi eski bir veri gizleme sanatıdır. Steganografi kelimesi, yunanca steganos (örtülü, gizli veya korumalı) ve graphtein (yazma) kelimelerinin bir araya getirilmesi sonucunda oluşturulmuştur ve “gizlenmiş yazı” anlamına gelmektedir [20].

Steganografide kullanılmak üzere bir taşıyıcı nesneye ihtiyaç duyulmaktadır. Taşıyıcı nesne verinin gömüleceği dosyadır ve örtü dosyası (Cover-File) olarak isimlendirilir. Örtü nesnelerde gizlenecek olan veri (gizli veri veya gömü verisi) metin veya başka

bir resim ya da ses dosyaları olabilir. Örtü resim içine veri gömüldükten sonra elde edilen resime “stego resim” denir. Örtü nesne içinde gizli verileri gömme işleminde ve daha sonra stego nesneden gizli verileri tekrar elde etmek için kullanılan gizleme fonksiyonları ise anahtar olarak tanımlanmaktadır [21]. Yukarıda anlatılan temel steganografi işlemi Şekil 1.4’te grafiksel olarak anlatılmıştır.

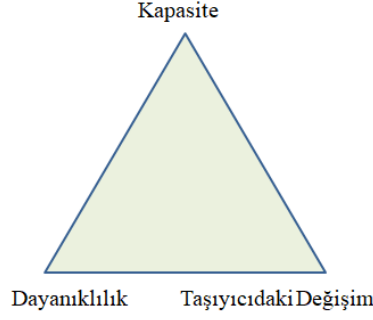


Şekil 1.4. Temel steganografi sistemi[22]

Günümüzde dijital verinin çeşitlenmesiyle birlikte gizleme işlemi sadece resim ya da grafik dosyaları üzerine yapılmamakta, bunun yanı sıra ip paketleri, exe uygulamaları, html ve xml dosyaları, videolar gibi birçok yapı tercih edilmektedir. Video ve ses gibi medya dosyaları büyük boyutları ve yüksek oranda bilgi içermeleri sayesinde en sık tercih edilen saklama alanlarıdır.

Geliştirilen steganografik bir yöntemin başarılı olabilmesi için veri gizleme işlemi sonucunda oluşan değişim, veri kapasitesi ve ortaya çıkarılma güçlüğü (dayanıklılık) gereksinimlerini sağlamalıdır. Bu ölçütler, steganografi ve steganaliz alanında birçok çalışmalar yapmış olan Jessica Fridrich tarafından ortaya çıkarılmıştır [23].

Kapasite, bilginin saklanacağı ortamın büyüklüğüdür. Dayanıklılık, stego nesne üzerine uygulanan işlemlerde gizlenen veriyi kaybetmeden saklamasıdır. Algılanabilirlik, stego nesnesinin gizli veri taşıdığının üçüncü şahıslar tarafından sezinlenmesidir [24]. Sezinlenmenin olmaması en önemli güvenlik gereksinimidir. Kapasitenin artırılması güvenliği olumsuz etkilemektedir. Araştırmacıların geliştirdiği yöntemler bu iki ölçüt üzerinde yoğunlaşmaktadır. Fridrich tarafından ortaya atılan yapı Şekil 1.5’te gösterilmiştir.



Şekil 1.5. Fridrich üçgeni

1.4.1. Steganografinin tarihçesi

M.Ö. 5.Yüzyılda, Eski Yunan’da saç derisine kazınan dövme ile mesajın iletilmesi steganografinin ilk ortaya çıkması olarak kabul edilmiştir. Yine aynı çağda avcı kılığındaki bir ulağın, avladığı hayvanın karnına parşömen saklayarak Yunanistan’a girmesi anlatılmaktadır.

Çinliler de kendi kaynaklarında meyve sepetini nasıl gizli iletişim için kullandıklarını anlatmaktadırlar. Bu yöntemde, meyve sepetindeki her meyvenin birbirine göre pozisyonu farklı bir anlam ifade etmektedir [25].

Eski Romalılar satırların arasına gözle görünmeyen mürekkepler kullanarak farklı gizleme teknikleri geliştirmişlerdir. Bu mürekkepler genellikle meyve özü (limon gibi) ve süt gibi doğal maddelerden oluşmaktadır. Isıtılınca ortaya çıkan bu gizli mesajlaşma tekniği günümüzde de hala kullanılmaktadır.

İkinci dünya savaşı sırasında almanlar tarafından, mikro–nokta (microdot) olarak adlandırılan farklı bir gizleme tekniği geliştirilmiştir. Bu teknikte, alfabede kullanılan noktalama işaretleri içerisine, ebatları küçültülmüş fotoğrafik bir takım gizli mesajlar gömülerek bilgi gönderilebilmiştir [26].

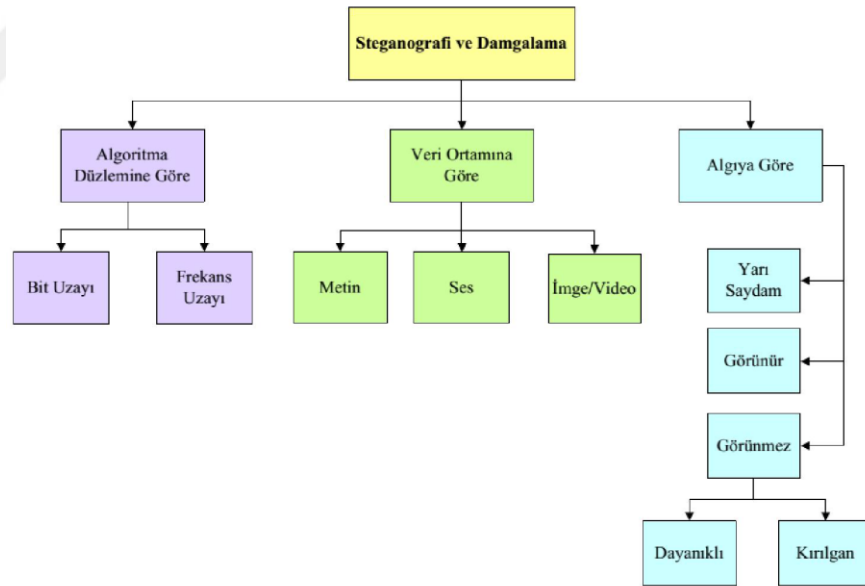
Dünya savaşları sırasında ülkeler arasında posta yolu ile gönderilecek her türlü satranç oyunları, gazete parçaları gibi gizli bir mesaj taşınması muhtemel dokümanlar yasaklanmıştır. İngiltere ve ABD tarafından koyulan bu yasaklamalar Sovyetler Birliği(SSCB) tarafından da tüm uluslar arası casusluk aktivitelerine karşı ülkeye giren tüm evraklar sürekli olarak taranmıştır. Bilginin daha da dijitalleşmesiyle bu

sınırlamalar geçerliliğini yitirmiştir. Çünkü günümüzde herkes steganografinin üstünlüklerini kullanabilir hale gelmiştir [27].

Steganografide gizli bir iletişimin sağlanması en temel ilkedir bu nedenle üçüncü kişilerin bu haberleşmeyi fark etmemeleri amaçlanır. Bilimsel ortamda Steganografi çalışmaları, 1983 yılında Simmons tarafından “Prisoner Problemi”nin tanımlanması ile başlamaktadır [28]. Bu problemde, Alice ve Bob hapishanededir ve hapishaneden kaçmak için planlar yapmaktadırlar. Fakat bu planların gardiyan Willie’ye fark ettirilmeden yapılması gerekmektedir. Eğer Willie bu durumu fark ederse kaçma planları suya düşecektir. Bu nedenle, çeşitli gizli haberleşme yöntemlerinin geliştirilmesi gerekmektedir.

1.4.2.Steganografinin alt alanları

Steganografi de yaygın olarak kullanılan yöntemlerin uygulama şekillerine göre sınıflara ayrılması Şekil 1.6’ de gösterilmiştir.



Şekil 1.6. Steganografi biliminin uygulama şekillerine göre sınıflandırılması[26]

Steganografi teknikleri insan gözünün görsel algılama kabiliyeti doğrultusunda geliştirilmektedir. Bu nedenle İnsan Görme Sistemi (İGS) yapısının ve sınırlarının bilinmesi birçok noktanın anlaşılmasında faydalı olacaktır. Çünkü sayısal görüntülere

veri gizleyen yöntemler, İGS'nin algılamadaki hassasiyetinin nispeten az olmasından faydalanmaktadır [29].

Trikromasite teorisi ile renkli görme açıklanmaktadır. Bu teori, kırmızı (R), yeşil (G) ve mavi (B) üç ayrı renkteki ışığın uygun karışımıyla bütün renklerin algılanabileceği gözlemine dayanmaktadır. Koniler mavi, yeşil ve kırmızı renge duyarlı fopsinlerdir. Fovea, koni algılayıcılarının en yoğun olduğu ve en yüksek renk duyarlılığının olduğu noktadır. Görüntünün algılanmasında önemli bir yeri vardır ve 1,5mm çapında yuvarlak noktadır. Görüntü işleme tekniklerinde bir görüntünün algılanmasında 1,5mm x 1,5mm boyutlarında kare veya dikdörtgen diziler kullanılır. Koni algılayıcılarının %65'i kırmızı, %33'ü yeşil ve %2 si ise mavi rengin algılanmasını sağlar. İnsan gözünde mavi rengin algılanma hassasiyeti diğer renklerden düşüktür. Genellikle mavi renk üzerine veri gizleme uygulamaları tercih edilmektedir bunun nedeni ise algılamanın diğer renklere göre daha düşük olmasıdır [30].

Önerilen hibrit yöntem, algoritma düzlemine göre hem bit uzayını hem de frekans uzayını kullanmaktadır.

1.4.2.1.Ses steganografi

Ses dosyaları, veri gizleme işlemlerinde örtü verisi olarak kullanılmaktadır. Bozulmalara karşı hassas olduklarından ses üzerindeki değişimler minimum seviyede tutulmalıdır. Ses dosyaları için birçok veri gizleme yöntemi geliştirilmiştir. Düşük bit kodlama, insan kulağının dosya içerisindeki bazı sesleri algılayamaması yöntemini kullanan yankı gizleme ve ses sinyaline frekans uzayında rastgele gürültü eklenerek gizleme işleminin yapıldığı yayılı gizleme ses üzerine veri gizleme yöntemlerinden bazılarıdır [26]. WAVE, MIDI, AVI, MPEG vb. formatlar ses steganografisinde kullanılmaktadır [31, 32].

1.4.2.2.Video steganografi

Video dosyalarının veri gizleme kapasitelerinin daha fazla olması, tercih nedenini artırmaktadır. Videoyu oluşturan fps'ler(frame-per-second) resim çerçevesi olarak

düşünülebilir. 24 fps değerine sahip bir video dosyasının her saniyesinde, 24 adet resim mevcuttur.

Video üzerine veri saklama yöntemleri, resim üzerine gizleme yöntemlerine benzer yapıdadır. Farklı olarak videoyu oluşturan her kare ayrı ayrı değerlendirilmektedir. Yapılan çalışmalar, internet ortamında da kullanılması nedeniyle, sıkıştırılmış videolar üzerine gizleme işlemlerinin yoğunlukta olduğu görülmektedir. Li ve diğ. [33, 34] yerleştirme yeri seçme algoritması ile eşik değerini kullanarak video dizilerine gömme yöntemi geliştirmiştir. Yöntem 4x4 matrisi şeklinde video framelerinden kalıntı blokları seçilip, belirlenen eşik değerinden büyük küçük olma durumuna göre veriler saklanmaktadır.

1.4.2.3. Metin steganografi

Veri saklama ortamı olarak metinler kullanılır. Açık alan yöntemleri (satır kaydırma, kelime kaydırma, gelecek kodlaması), yazılımsal yöntemler ve anlamsal yöntemler metin steganografide kullanılan yöntemlerdir. Metin üzerinde gereksiz alanlar ve boşlukların az olması taşıyıcı üzerinde gizlenen veri kapasitesini kısıtlar. Metin tabanlı veri gizleme yöntemlerinin hepsi, gizli mesajı tekrar elde edebilmek için ya orijinal metne ya da orijinal metnin biçimlendirme bilgisine ihtiyaç duyarlar [35].

1.4.2.4. Network steganografi

Gizli verinin TCP, UDP, ICMP, IP gibi ağ protokolleri içerisinde saklandığı yöntemlerdir. OSI ağ katmanları modelinde steganografinin uygulanabileceği kanallar mevcuttur. TCP/IP alanlarının kullanılmayan başlık bitlerinde steganografi kullanılmaktadır [36, 37].

1.4.2.5. Görüntü (Image) steganografi

Resimler, steganografi uygulamalarında kullanılan en popüler örtü nesneleridir. Genel olarak, bu yöntemde piksel yoğunlukları verileri gizlemek için kullanılır. Resim steganografi için çok fazla sayıda farklı yöntem ve algoritma kullanılmaktadır [31]. Bu tez çalışması resim içerisine histogram bilgilerinin kullanılmasıyla geliştirilen yöntem sunulmuş ve resim steganografi ayrıntılı olarak incelenmiştir.

1.4.3.Uzamsal alan steganografi yöntemleri

Uzamsal alan yöntemleri, verileri doğrudan piksel değerleri içerisine gizlenmesi ilkesine dayanır. En önemsiz bit, kenar tabanlı gömme, rastgele piksel yerleştirme, piksel haritası yöntemi, etiketleme, piksel yoğunluğuna göre gömme, histogram tabanlı, palet tabanlı gömme piksel değerleri içerisine veri gizlemeyi kullanan yöntemlerdir. Bu yöntemlerde piksel değerlerinin amaca uygun olarak değiştirilmesi amaçlanır [31].

En önemsiz bit yöntemlerinin (Least Significant Bit methods- LSB) uygulanmasında, piksel değerlerinin en önemsiz bitleri kullanılır. Verinin gizlenmesi sonucu oluşan örtü resim ve orijinal resim arasında oluşan farklılıklar göz tarafından algılanamaz. Kapasite, kullanılan kanal(RGB) sayısına göre değişiklik gösterebilir. LSB kodlama tekniği literatürde en çok kullanılan ve karşılaşılan tekniktir[38]. Bu yöntemde, öncelikle gizlenecek olan veri ASCII karakter kodlarına çevrilir ve bu kod pikselin kanallarının en düşük değerlikli bitlerine sırası ile yazılır. Örneğin 8 bitlik bir ASCII kod karşılığı olan karakter için 3 pikseldeki 9 değerlikten 8 tanesine gömülme işleminin yapılması gerekir. Bitlerin değiştirilmesi mantığına dayanan LSB yöntemi sonucunda oluşacak olan değişimler, insan gözünün algılamayacağı seviyededir [39].

Uzamsal alan yöntemlerinin genel avantajları; saklanan veri kapasitesi yüksektir, hesaplama karmaşıklığı azdır, verinin gizlenmesi sonucu oluşan örtü resimdeki değişim insan gözü tarafından algılanmaz şeklindedir. Resim üzerinde yapılan değişiklikler gizli verinin güvenliğini etkileyebilir. Bu ise en büyük dezavantajını oluşturmaktadır [31].

1.4.4.Frekans uzayında steganografi yöntemleri

Dönüşüm alanında, hem örtü resmi hem de gizlenecek veri frekans alanına dönüştürülür ve daha sonra gizlenecek veri örtü resim içerisine gömülür. Dönüşüm alan steganografi, algoritma değişiklikleri ve resim dönüşümlerini içermektedir. Bu yöntemlerde, gizli veriler örtü resmin belirgin alanlarında gizlenmektedir [40].

Dönüşüm alan yöntemleri, örtü resmin içerisine verileri gizlemek için çeşitli algoritmalar ve dönüşümler kullanan yöntemlerdir. Algoritmanın karışıklığı daha

yüksektir. İşaretler üzerinde çalışırken frekans düzleminde işlem yapmak uzamsal düzleminde işlem yapmaya göre çok daha hızlı sonuçlar üretmektedir. Bu amaçla resim üzerinde işlem yaparken frekans düzleminde çalışmak zaman düzleminde çalışmaktan çok daha avantajlıdır [31].

Ayrık kosinüs dönüşümü yöntemi (Discrete Cosine Transformation technique- DCT), hızlı Fourier dönüşüm yöntemi (Fast Fourier Transformation technique - FFT) , ayrık Fourier dönüşüm yöntemi (Discrete Fourier Transform- DFT) [41, 42] , ayrık dalgacık dönüşüm yöntemi (Discrete Wavelet Transformation technique- DWT) [43-45], tamsayı dalgacık dönüşümü yöntemi (Integer Wavelet Transform technique- IWT) frekans uzayında steganografi yöntemleridir.

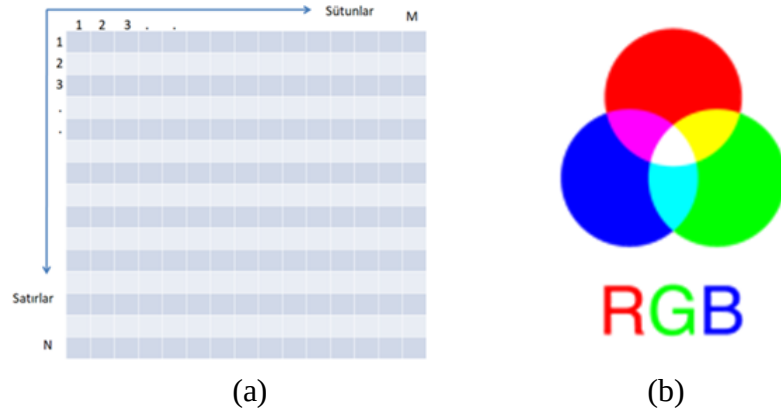
Saldırılara karşı gizli verinin kaybolma olasılığının düşük olması, kullanılacak formatların esnek olması, saklanan verinin resim üzerine yayılarak saklanması bu yöntemlerin avantajlarını oluşturmaktadır. Gömme kapasitesinin sıklığı, hesaplama karmaşıklıkları ve gömme de kullanılan katsayıların dikkatli seçilip işlem yapılması ise dezavantajlarıdır [31].

1.5.Sayısal Görüntü ve Temel Kavramlar

Dijitalleşen dünya ile iletişim cihazları çeşitlenmiş ve gelişmiştir. İnternet vasıtasıyla iletişimler yoğunlukla sayısal olarak gerçekleşmektedir. İnternet ortamında bulunan her cihaz verileri sayısal olarak işlemektedir. Ses, video, resim vb. türdeki her verinin sayısal bir karşılığı oluşmuştur.

1.5.1.Piksel

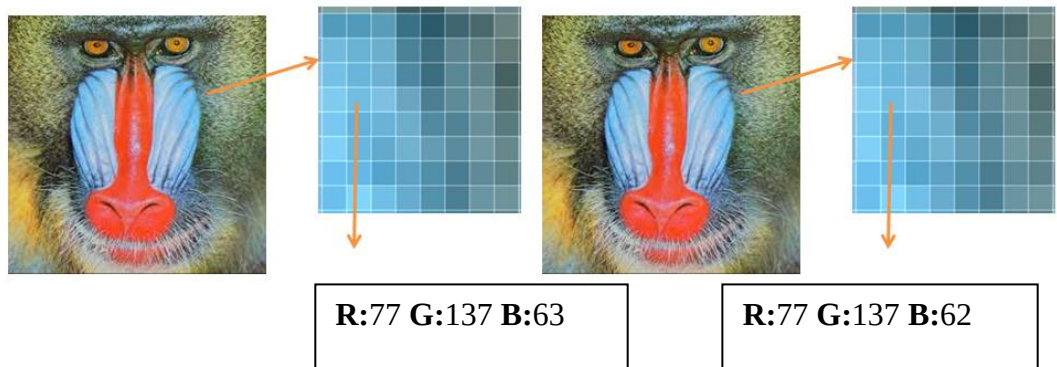
Görüntülerin en küçük üçlü nokta grubuna piksel denir veTürkçede'ki karşılığı ise gözek'tir [46]. Resimler N satır M sütünlük bir dizi ile gösterilir. Dizin her bir elemanı piksel olarak ayrılır. Pikselin yapısı ve pikseli oluşturan renk bileşenleri Şekil 1.7'de gösterilmiştir.



Şekil 1.7. (a) Piksel yapısı ve (b) renk bileşenleri

Her piksel değeri 24 bit (3-Bayt) sayısal ifadeden meydana gelmektedir. Her pikselin rengi “Kırmızı (Red; R), Yeşil (Green; G), Mavi (Blue; B)” olmak üzere üç ana renkten elde edilir. Her renk değeri 8 bit veriden oluşmaktadır. Şekil 1.8’de gösterildiği gibi, her renk farklı oranlarda RGB bileşiminden meydana gelmektedir. Bir pikselde (255, 255, 255) değerlerinin birleşimi sonucunda beyaz rengi, (0,0,0) birleşimi ise siyah rengi ortaya çıkarmaktadır [46]. Gri seviyeli resimlerde ise her bir piksel 0 ile 255 arasında (8 bitlik) parlaklık seviyesi değerleri alır.

Görüntüler üzerinde gerçekleşen steganografi uygulamaları resmin sayısal değerlerinde küçük değişimler yapılarak gerçekleştirilmektedir. Sayısal değerlerdeki farklılıklar ya da bozulmalar insan gözü tarafından algılanamayacak seviyelerdedir. Şekil 1.8’de gösterilen piksel haritasında resmin B kanalı üzerindeki değişim resim piksel değerlerinin çok büyütülmesine rağmen algılanamayacak seviyededir.



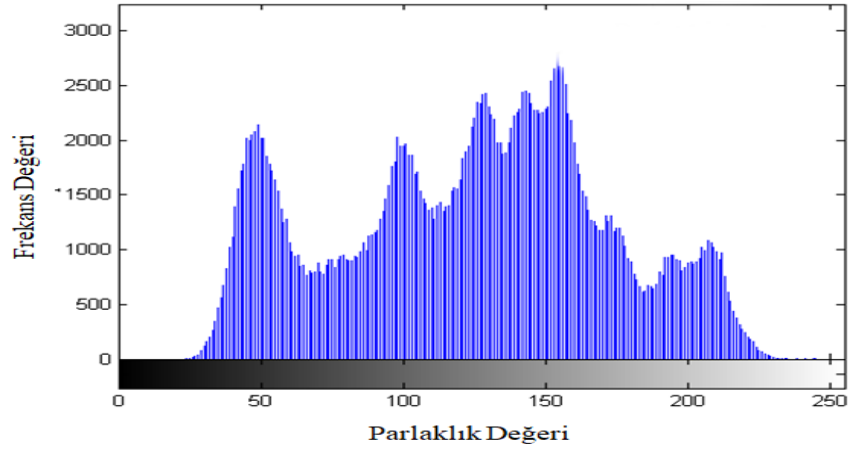
Şekil 1.8. 24-bit bir resmin piksel haritasındaki bileşen değerleri

Görüntüler üzerinde gerçekleşen steganografi uygulamaları resmin sayısal değerlerinde küçük değişimler yapılarak gerçekleştirilmektedir. Sayısal değerlerdeki farklılıklar ya da bozulmalar insan gözü tarafından algılanamayacak seviyelerdedir. Şekil 1.8’de gösterilen piksel haritasında resmin B kanalı üzerindeki değişim resim piksel değerlerinin çok büyütülmesine rağmen algınamayacak seviyededir.

1.5.2.Histogram

Histogram, bir işlem neticesinde elde edilen ölçüm sonuçlarının dağılımını gösteren grafiklerdir. Analog bir işaret için histogram ilgili işaretin hangi frekans değerinde kaçar adet bileşene sahip olduğu bilgilerini verir. Bu sayede işaret bileşenlerinin hangi frekanslarda yoğunlaştığı bilgisine ulaşılır. Sayısal imge histogramı ise sayısal bir resmin renk tonlarının dağılımını gösterir [26, 27]. Histogram, resimdeki piksellerin renk bileşenlerinin dağılımını gösteren değerler dizisi olarak düşünülebilir. Resmi oluşturan RGB kanallarının ortalama değeri olabileceği gibi her bir kanalın kendisine ait histogram değeri de olabilmektedir. Histogram değerleri 0-256 değerleri arasındadır ve bu değerlerin dağılımı resim hakkında bilgi vermektedir. Örneğin değerler ne kadar farklı noktada ise resmin o kadar fazla renk veya ton içermekte olduğu, renk aralığının daralması ise yakın tonların ağırlıkta olduğu bilgisini verir.

İmgelerin histogram değerleri veri gizlemede sıklıkla kullanılan yöntemlerdir. Histogram kaydırma yöntemi resim üzerinde bölümler oluşturularak, tepe değerleri tespit edilip belli algoritmalar oluşturularak gömme işlemi yapılmaktadır. Veri gömme kapasitesi olarak düşük yöntemlerdir [47]. Örnek bir resme ait 8 bitlik (0-255) aralığındaki parlaklık değeri bir imge histogramı üzerinde Şekil 1.9’da gösterilmiştir.



Şekil 1.9. Bir imge histogramına ait parlaklık ve frekans değerleri

Histogram grafikleri her renk değeri için elde edilebileceği gibi ortak renk karışımı değerlerine göre de oluşturulabilir. Renkli resimlerde R, G, B, bileşenleri yer aldığından üç adet ayrı histogram grafiği elde edilir. Tez kapsamında kullanılan yöntemlerde, histogram değerleri R, G, B bileşenleri için ayrı ayrı oluşturulup uygun olan bileşen belirlenmektedir.

1.5.3.Görüntü formatları

Bilişim sitemlerinde yazılımlar birbirleriyle farklı formatlarda dosya alış verişi yaparlar. Görüntünün uygulama programından bağımsız olarak her hangi farklı uygulama üzerinde işlenebilmesi için ortak formatlar geliştirilmiştir. Tez içerisinde geliştirilen uygulama jpg, bmp ve png uzantıları için çıktı oluşturmaktadır. Varsayılan olarak kullanılan format jpg görüntü formatıdır. Günümüzde yaygın olarak kullanılan görüntü formatlarından bazıları şunlardır.

1.5.3.1.Bmp

Microsoft tarafından PCX formatını değiştirerek geliştirdiği, 1-24 bit arasında değişen bir piksek derinliği içeren hızlı bir formattır. Varsayılan olarak görüntü de sıkıştırma olmaz, kayıpsız sıkıştırma yöntemi kullanılır.

1.5.3.2.Jpeg / Jpg

Standart JPG formatında, resmin kalitesinden bir miktar ödün verilerek sıkıştırma gerçekleştirilen, gerçek renk değerlerini içeren bir formattır. Sıkıştırma ile detay

arasında ters bir orantı vardır, sıkıştırma artınca resimdeki detaylar azalmaktadır. 24 bitlik bir resim dosyasında, resim kalitesinin düştüğünü göz ile anlamak mümkün değildir [48]. Ayrıca bu formattaki resimler saydamlık kanalına sahip değildirler [49].

1.5.3.3.Png

Kayıpsız sıkıştırarak görüntü saklamak için kullanılan dosya formatıdır. Daha çok internet ortamında kullanılır.

1.5.3.4.Tiff

Yüksek renk derinliği olan görüntülerde kullanılan ve matbaacılıkta kullanılmak üzere planlandığından hem RGB hem de CMYK şeklinde renkleri ayrıştırmaktadır. CMYK genellikle baskıda kullanılan 4 ana renk olan (turkuaz (cyan), eflatun (magenta), sarı (yellow) ve siyahtır. (black)). Belli açılara ve değerlere sahip bu renkler, üst üste basılarak tüm ara renkler ortaya çıkarılır. Dosya boyutları jpg dosyalarına göre daha büyüktür.

1.5.3.5.Gif

CompuServe firmasının Graphics Interchange Formatı (GIF), internet üzerinde yaygın kullanılan bir formattır. Hareketli resimler ve animasyonlar için tercih edilir. Gerçek renk desteği yoktur. Oldukça iyi sıkıştırma sağlaması, animasyonlarda zamanlama ve farklı boyutlardaki imgeleri bir arada tutma desteği, saydam renk tanımlaması bu formatı popüler yapan nedenlerden bir kaçıdır [50].

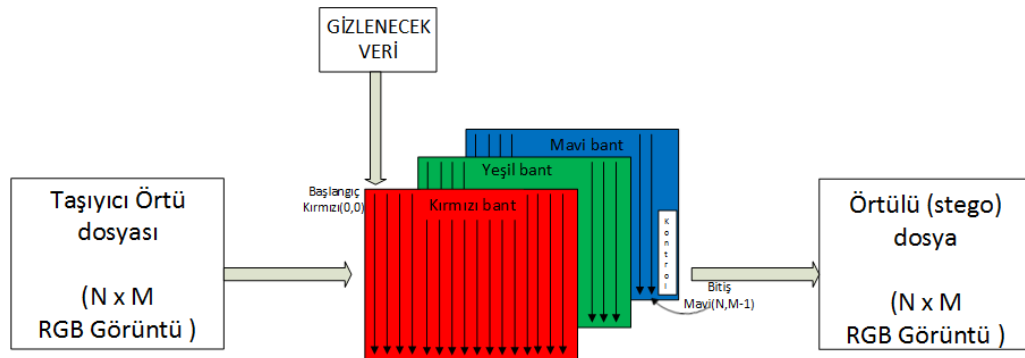
2. VERİ GİZLEME YÖNTEMLERİ

2.1. En Önemsiz Bite Veri Gizleme (LSB) Yöntemi

En önemsiz bite veri gizleme yöntemi (Least Significant Bit Insertion Method, LSB) steganografi alanında temel bir yöntemdir. Bu yöntemde, öncelikle gizlenmek istenen veri ikili biçime dönüştürülür. Ardından bu verinin her bir biti, örtü resimdeki piksellerin en önemsiz bitine gömülmektedir. Böylece örtü resminin en az öneme sahip olan bitleri, gizli veriyi taşıyacak şekilde değiştirilmiş olur.

LSB, stenografik uygulamalar için yeni bir başlangıç olmuştur ve günümüzde en çok kullanılan teknikler arasında yer almaktadır [51-52]. Çok fazla kullanılmasının sebebi ise veri gizlendikten sonra resim üzerindeki değişimlerin insan gözü tarafından algılanamayacak seviyede olması ve veri gizleme kapasitesinin oldukça yüksek olmasıdır. Örneğin 1024×768 boyutundaki 24 bitlik bir resim dosyasında, her üç kanaldaki piksellerin en önemsiz bitlerine verinin saklandığı düşünülürse, toplam saklanabilecek veri boyutu, $1024 \times 768 \times 3 = 2.359.296$ bit olacaktır.

LSB ile veri gizleme işleminde genelde ilgili pikselin ikilik sistemdeki son bitine gizli bit yazılır. Şekil 2.1’de, LSB veri gizleme yönteminin üç boyutlu (RGB) taşıyıcı örtü dosyasına eklenmesi gösterilmiştir.



Şekil 2.1. LSB veri gizleme yöntemi [53]

Gizlenecek bilgi RGB görüntünün kırmızı bandının sütunlarına/satırlarına yazılmaya başlanır. Her sütun/satır bittiğinde sonraki sütuna/satıra geçilerek devam edilir. Gizli metnin uzunluğuna göre yeşil ve mavi bantlarda aynı şekilde kullanılır. Genellikle gizlenecek verinin sonuna belirli bir karakter eklenerek sonlandırılır. Gizli verinin elde edilme aşamasında da ilgili karakter elde edildiğinde verinin bittiği anlaşılır [53].

LSB işlemi için ilk olarak gizlenecek metin ele alınır. İlgili metnin her bir harfine karşılık gelen onluk sistem ASCII kodları belirlenir. Daha sonra bu ASCII kodların ikilik sistemde karşılıkları tespit edilir. Tablo 2.1’de “kocaeli” gizli kelimesi için bu anlatım örneklenmiştir. Son olarak bu ikilik sayı dizisinin uzunluğu belirlenip, kırmızı bandın ilk pikselinden başlayarak Şekil 2.1’de gösterildiği gibi sütunlar boyunca bu uzunluğa denk gelen piksellerin son bitlerine veriler yazılır [53].

Tablo 2.1. LSB yöntemi veri gizleme örneği

Örnek:	kocaeli	Gizli metin
	107 , 111 , 99 , 97 , 101 , 108 , 105	Harflerin ASCII Kod karşılıkları (Onluk)
	01101011 , 01101111 , 01100011 , 01100001 , 01100101 , 01101100 , 01101001	Harflerin ASCII Kodları (İkilik)

Gizlenecek verinin ikilik kod karşılığının ilk biti kırmızı renk kanalının ilk (0,0) pikseline Denklem (2.1) ve (2.2)’de gösterilen şekilde gizlenir. Burada Δ , son bit olarak piksele eklenecek bit değerini, “m” ise gizlenecek bit değerini göstermektedir. Bir sonraki bit için alt satırdaki piksele (1,0) geçilerek aynı işlem tekrarlanır. Sütun sonuna gelindiğinde bir sonraki sütuna geçilerek devam edilir. Bu işlem son bit gizlenene kadar tekrar eder.

$$\text{pikseldeğeri}_{\text{yeni}} = \text{pikseldeğeri}_{\text{sonbit_sıfır}} + \Delta \quad (2.1)$$

$$\Delta = \begin{cases} 1 & ; \text{eğer “m=1”} \\ 0 & ; \text{eğer “m=0”} \end{cases} \quad (2.2)$$

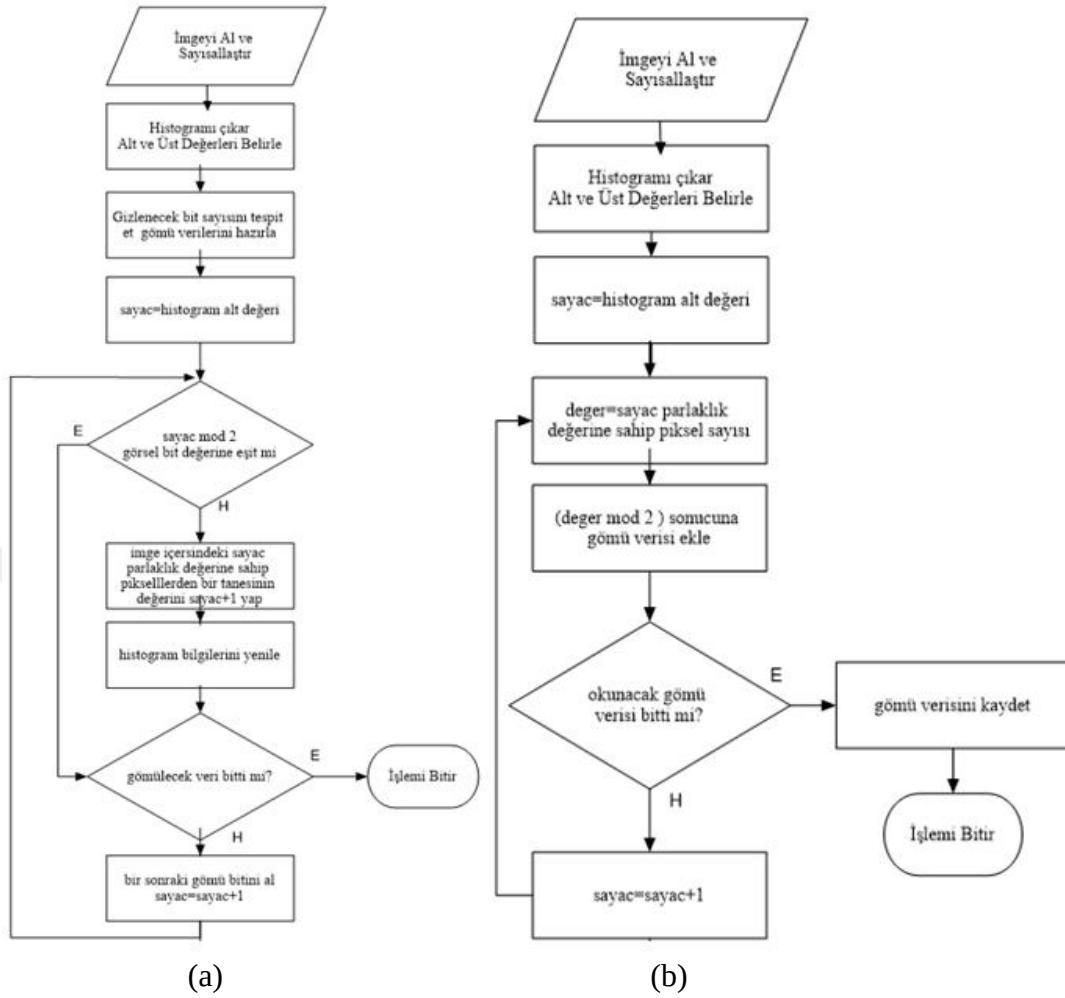
Veri gizleme işlemi tamamlandıktan sonra alıcı tarafta gizlenen verinin doğru olarak elde edilebilmesi için, gizlenen verinin sonuna NULL (00000000) işareti aynı mantıkla gizlenir. Böylece gizli yazı içeren örtülü dosya hazırlanmış olur [53].

Veri gömüldükten sonra verinin tekrar elde edilebilmesi için Şekil 2.1’de yapılan işlemin tersi uygulanır. 3 pikselin 9 adet renk değerinden, ilk 8 adet renk değeri okunur ve bu değerlerin en önemsiz bitleri alınarak 8 bit bir araya getirilir. Bir araya getirilen bu değerlerin decimal değerliği alınarak ASCII karakter kod karşılığı bulunur. Bu işleme, NULL karakteri elde edilene kadar devam edilir.

2.2. Histogram Temelli Veri Gizleme (HSV) Yöntemi

HSV yöntemi, tez çalışması[4] kapsamında Yalman tarafından geliştirilen bir veri gizleme yöntemidir. Uygulamada ki temel amaç histogram değerlerini kullanarak veri gizleme işlemini gerçekleştirmektir. Histogram temelli veri gizleme yöntemi(HSV), LSB kullanılarak yapılan veri gizleme tekniğini histogram işleme ile birleştirmektedir.

Yöntemin uygulanışında öncelikle imgeye ait histogram değerleri oluşturulup alt ve üst değerleri belirlenir. Veri gizleme işlemi bu parlaklık değerleri arasında gerçekleşmektedir. Belirlenen aralık içerisinde parlaklık değeri ve tekrarlanma sayıları kullanılarak veri gizlenir. Gizlenecek veri biti 0 ise sırayla aralıkta parlaklık değerlerinin tekrarlanma sayıları mod-2 işlemine tabi tutulur. 0 gizlenecek bit için mod sonucu 0 ise o parlaklık değerine gizlenir. Eğer mod işlem sonucu 1 ise, bir sonraki parlaklık değerin frekans değeri bir artırılır, o parlaklık değerin frekans değeri 1 azaltılarak imge güncellenir. Şekil 2.2’de gösterilen akış şemaları ilgili kaynak üzerinden faydalanılarak oluşturulmuştur [26].



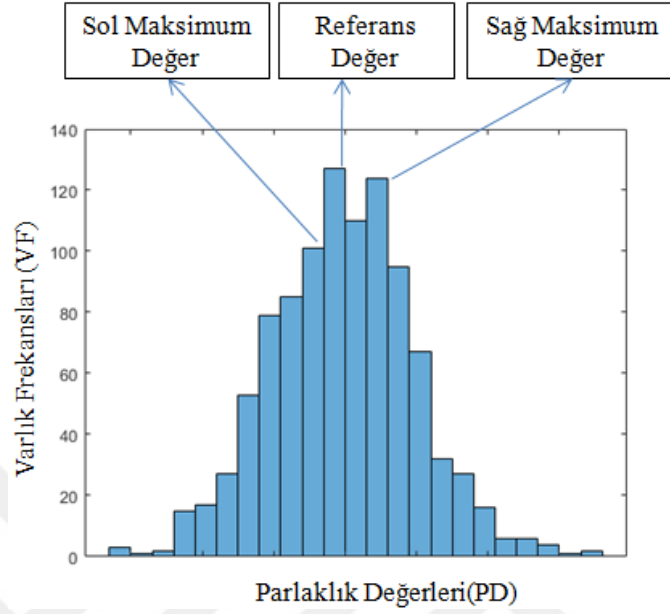
Şekil 2.2. HSV yöntemi ile (a) veri gizleme, (b) gizli veriyi ortaya çıkarma akış şemaları

Bu yöntemin tez içerisinde kullanılma amacı geliştirdiğimiz farklı histogram yöntemleri ile test sonuçlarının değerlendirilmesidir. Yöntemin algoritması geliştirilen uygulama üzerinde işletilip veri gizleme işlemi yapılmaktadır.

2.3.Maksimum Histogramlar Yöntemi (MHY)

Bu yöntemde, öncelikle imgeye ait histogram değerleri ortaya çıkarılarak varlık frekansı en yüksek olan parlaklık değeri belirlenir. Maksimum frekans değeri referans olarak alınır ve buna en yakın sol ve sağ maksimum değeri belirlenerek, gizleme işlemi bu parlaklık değerlerine yapılmaktadır. Diğer parlaklık değerleri göz ardı edilmektedir. Maksimum frekans değerine en yakın sağ ve soldaki maksimum değerlerinin frekans değerleri seçilen renk bileşenine göre değişmektedir. Resmin

bileşen seçimi(R, G, B) değiştirilerek uygun bileşenin seçilmesi kapasite açısından önemlidir [3].



Şekil 2.3.MHY’de parlaklık değeri seçimi

Şekil 2.3’te gösterildiği gibi maksimum değer referans değer olarak kabul edilip, referans değerın konumuna göre sağ ve solundaki maksimum değeler tespit edilmektedir. Sağ ve sol maksimum parlaklık değeri referans değeri hemen yanında olabileceği gibi farklı noktalarda da olabilir. Bileşen seçimi kullanırken sağ ve sol maksimum değeri varlık frekanslarının büyüklüğü ve referans değere yakınlığı tercih sebebi olmalıdır. Böylece kapasite artırılmış ve resimdeki değişim minimuma indirilmiş olur.

Tablo 2.2. MHY’de örnek bir resim bileşen değeri

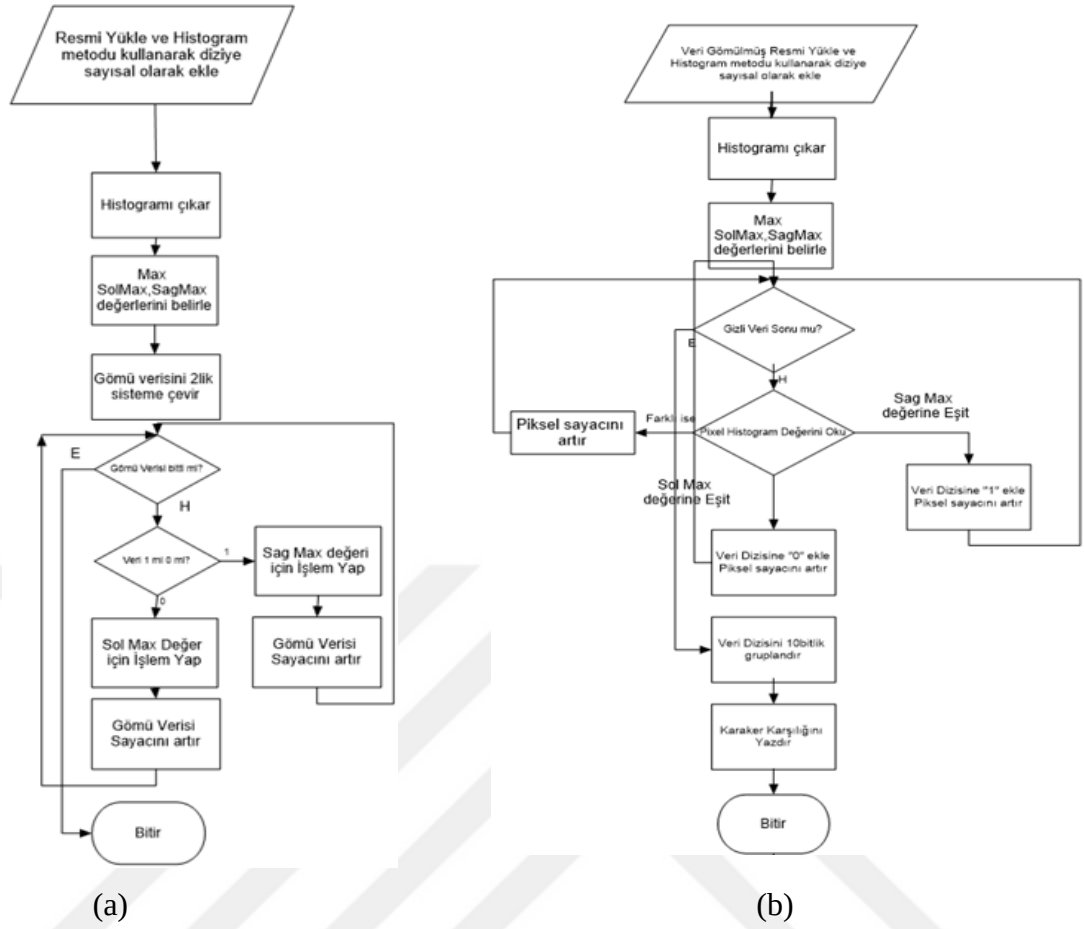
Stego.jpg	Maksimum (Referans)		Sol Maksimum		Sağ Maksimum	
	<i>Hist. Sırası</i>	<i>Değeri</i>	<i>Hist. Sırası</i>	<i>Değeri</i>	<i>Hist. Sırası</i>	<i>Değeri</i>
R	250	1296	180	1253	251	1266
G	184	1367	182	1366	185	1333
B	106	1108	101	1078	102	1101

Örnek resim (Stego.jpg) için histogram değeri Tablo 2.2’de verilmektedir. Bu değerler incelediğinde, resmin G kanalı histogram değeri diğerlerinden fazla olduğu yani resim üzerinde yeşil tondaki bir değeri daha fazla tekrarlandığı

görülmektedir. Bu nedenden dolayı, G kanalına verinin gömülmesi gizlenebilecek veri kapasite değerini artıracaktır. Sol ve sağ maksimum değerlerin referans değere yakın parlaklık değerlerde olması ise resim üzerindeki değişimi azaltacaktır. Bu steganografi yöntemlerinde istenen bir durumdur. Gömülecek veri üzerindeki 0 değeri 1 değerinden fazla ise varlık frekansı fazla olan parlaklık değeri 0 bitleri için gömülecek alan olarak belirlenir. Bu şekilde değişim azaltılmış olur.

Gizlenmek istenen ilk dört bit değerinin $(0010)_2$ olduğu ve verinin gizleneceği resmin G kanalının ise Tablo 2.2'deki gibi histograma sahip olduğu kabul edilsin. 0 değerleri için sol maksimum değerine karşılık gelen piksel değerleri, 1 değerleri için sağ maksimum piksel değerleri kullanılmaktadır. Oluşturulan fonksiyon değerine göre piksel değerleri sırayla alınmakta ve gizlenecek binary ifadenin ilk bitinden başlanarak ilk iki bit histogram sırası 182 olan piksel değerlerine, sonraki bit ise histogram sırası 185 olan piksel değerleri şeklinde sıralanmaktadır. Piksel değeri eğer bu tonda değilse ilgili pikselin değeri değiştirilecektir. Gömülecek veri bitiminde; sol maksimum histogram değeri sağ maksimum olarak değiştiyse, değişme sayısı kadar sağ maksimum histogram değerine sahip piksellerde değişim olacaktır. Şekil 2.4'te verinin gizlenmesinin akış şeması gösterilmiştir.

Resim üzerine gizlenen metnin ortaya çıkarılırken resim histogramı tekrar oluşturulmaktadır. Öncelikle histogram tablosundaki maksimum (referans) değerlerin sağ ve sol tarafındaki maksimum değerler tespit edilmektedir. Gizleme fonksiyonunun tersi işlenerek, sağ ve sol maksimum değerlere eşit piksel değerleri tespit edilir ve çözümlenen metin dizinine sol maksimum değeri için "0", sağ maksimum değeri için "1" eklenir. Gömü verisi sonu kodu NULL $(0000000000)_2$ elde edilince, elde edilen metin dizisi 10 bitlik gruplara ayrılır. Bu kodun belirlenmesinde metin içerisinde yer almayan karakter seçilmiştir. 10 bit değeri decimal sayıya çevrilerek ASCII kodu alınıp karakter bulunur. Metin dizisinin tamamı çevrilerek gizlenen metin elde edilir. Şekil 2.4'te gizlenen verinin tekrar elde edilmesi için akış şeması gösterilmiştir.



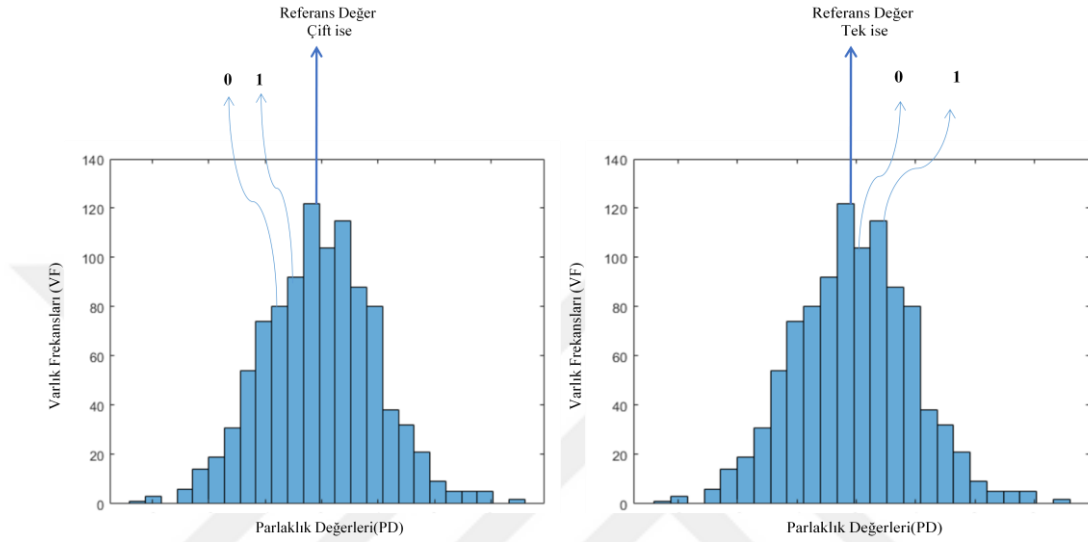
Şekil 2.4. MHY’de (a) veri gizleme (b) veriyi ortaya çıkarma akış şemaları

2.4.Yakın Histogramlar Yöntemi (YHY)

Önerilen bu yöntem, hibrit bir yapıda çalışmaktadır. Bu yöntemin algoritmasında öncelikle histogram grafiği taranarak verinin gizleneceği piksellerin parlaklık değerleri tespit edilmekte ve LSB yönteminin mantığı ile de ilgili piksellere gömme yapılmaktadır. Kapasite ve dayanıklılığın artırılarak resim üzerindeki değişikliğin minimize edilmesi amaçlanmaktadır. Veri gizleme işlemi sonucunda histogram grafiğinde ilgili referans değerinin yine maksimum olarak kalması yöntem için olmazsa olmaz bir durumdur.

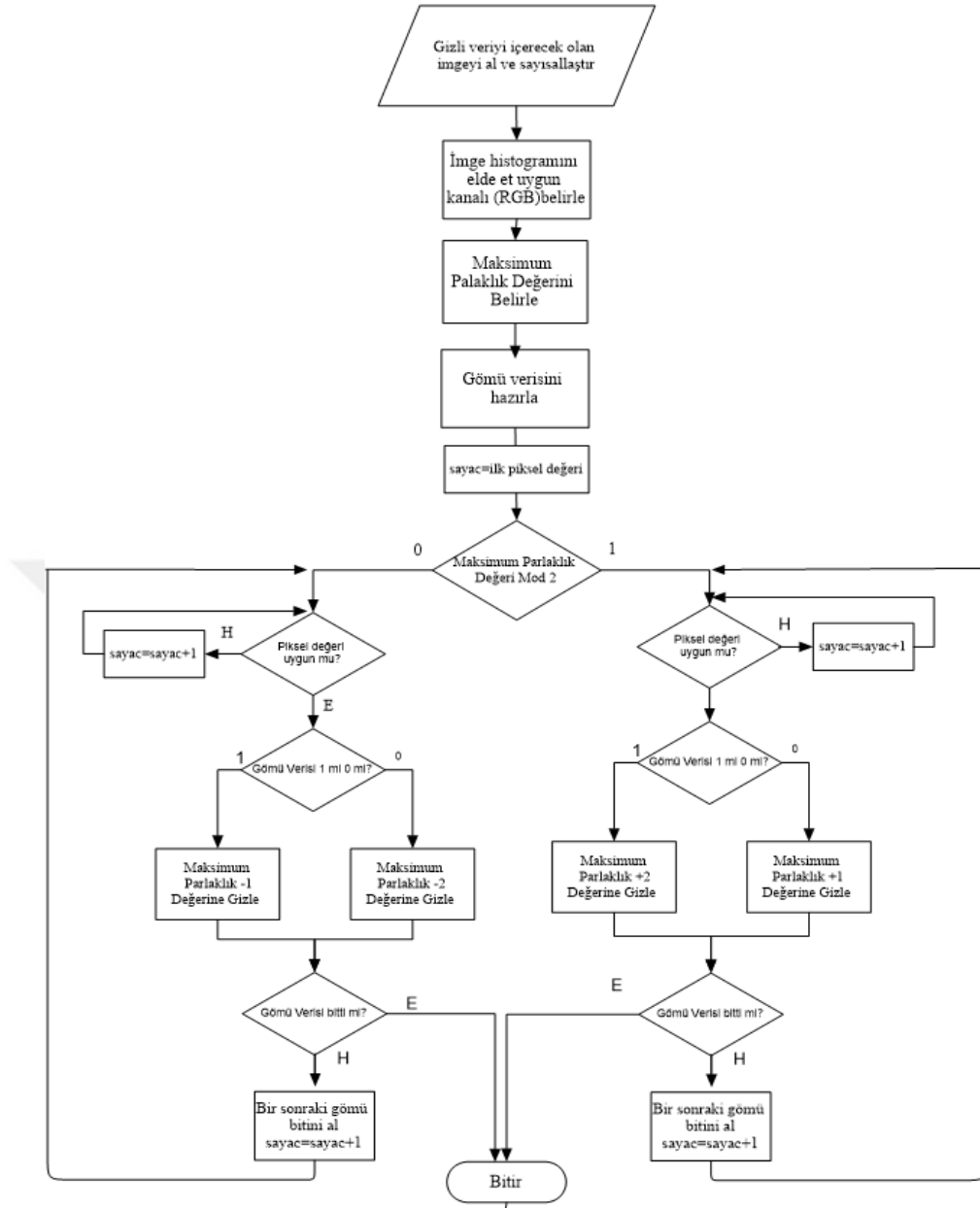
Yöntemin uygulanmasında öncelikle imgenin histogramı oluşturulmaktadır. Maksimum histogram yönteminde olduğu gibi varlık frekans değeri en yüksek parlaklık değeri tespit edilir. Referans alınan maksimum değerinin sağ ve solundaki en yakın parlaklık değerleri bulunur. Gizlenecek veriler binary sayı sisteminde kodlandığından 0 ve 1’lerden oluşmaktadır. Referans değerin parlaklık değeri çift ise

histogramın sol tarafındaki parlaklık değerleri, tek ise sağ tarafındaki parlaklık değerleri verinin gizlenmesi için kullanılır. Bu şekilde seçilmesinin nedeni ise dönüşüm gerektiğinde minimum sayıda (1 bit) değişimin olabilmesi içindir. Referans değerin çift veya tek olma durumuna göre gizlenecek verinin saklanacağı piksellerin parlaklık değerleri Şekil 2.5'te gösterildiği gibi belirlenir.



Şekil 2.5. YHY'de gömülecek bitler için parlaklık değerlerinin tespiti

Önerilen yaklaşımda öncelikle resmin histogramı oluşturularak parlaklık değeri tekrarlanma sayıları tespit edilmektedir. Maksimum tekrar eden parlaklık değeri referans alınarak veri gizleme işlemi gerçekleştirilmektedir. Şekil 2.6'da, önerilen YHY'nin veri gizleme akış şeması verilmiştir. Algoritma, referans seçilen maksimum parlaklık değerine göre gizleme yapılacak olan parlaklık değerlerini tespit etmekte ve gizlenecek verinin değerine göre akış ilerlemektedir.



Şekil 2.6. YHY’de veri gizleme akış şeması

Gizlenmek istenen ilk 4 bit değeri $(1011)_2$ olarak kabul edilsin. Verilerin gizleneceği imgenin Tablo2.3’te maksimum tekrar eden parlaklık ve çevre değerlerinin sayıları gösterilmektedir.

Tablo 2.3. Resim histogramına ait bazı sayısal değerler

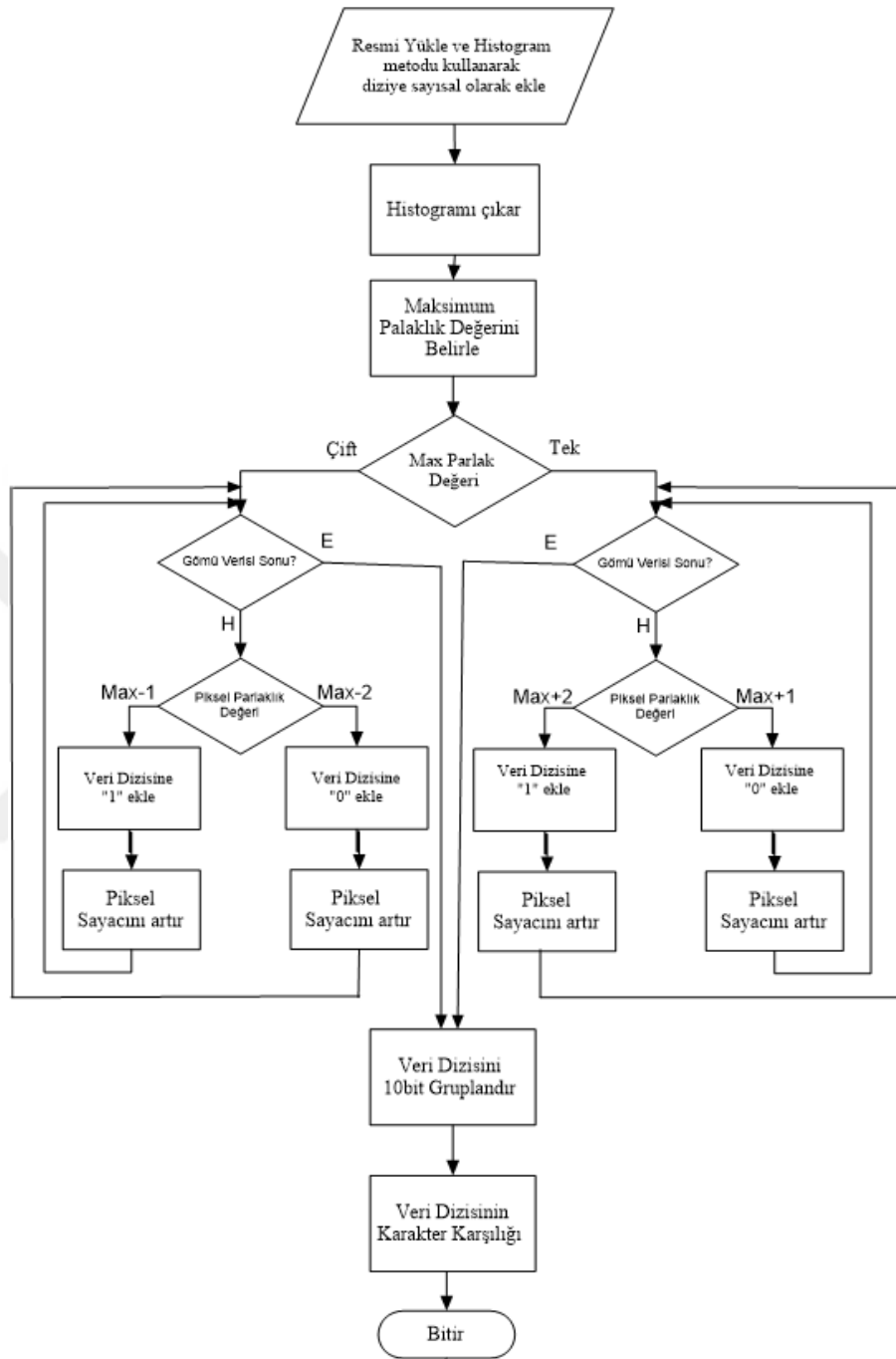
Parlaklık Değeri	112	113	114	115	116
Tekrarlanma Sayısı	87	96	158	125	136

Uygulama yazılımı ilk olarak öncelikle gömü verisinin (yani $(1011)_2$) ilk biti olan 1 değerini ele almaktadır. Histogram bilgileri kullanılarak en fazla tekrar eden

parlaklık değeri çift veya tek olma durumuna göre gömülecek verilerin hangi parlaklık değerlerine gömüleceği tespit edilir. Maksimum tekrarlanma sayısına sahip parlaklık değeri (114) çift olduğundan “0” değeri için “112” ve “1” değerleri için “113” parlaklık değerine sahip piksel değerleri veri gömülmesi için kullanılacaktır. İlk bit “1” değeri alınarak resim piksel değerleri okunduğunda parlaklık değeri “112” veya “113” olan piksellerden herhangi birine ulaşıncaya kadar resim okunur. Karşılaşılan ilk değer “113”ise değişiklik yapılmaz, “112”ise parlaklık değeri “113”olarak değiştirilir. Sonraki bir “0” değeri için resim okunmaya devam edilir. Karşılaşılan ilk “112” veya “113” parlaklık değeri için “112” ise değişiklik yapılmaz “113” ise “112” olarak piksel parlaklık değeri değiştirilir. Gömü verisi sonlanıncaya kadar bu döngü devam eder. Gömü verisi bittiğinde eğer değiştirilen parlaklık değerlerinden biri referans değeri geçer ise ilgili referans değerinin altına düşünceye kadar sıradaki değerler diğer değere dönüştürülür. Böylece maksimum (referans) değer değişmemesi sağlanmış olur.

Üç kanallı (RGB) resimlerde, bu algoritma her kanal için ayrı ayrı histogramlarının hesaplanması ve her kanalın aynı işleme tabii tutulması ile gerçekleştirilmektedir. Stego resmi, uygulama içerisine aktarılarak histogram değerleri oluşturulur. Frekans değeri en yüksek olan parlaklık değeri tespit edilerek tek mi çift mi olduğu kontrol edilir. Tek ise frekans değeri maksimum olan parlaklık değerinin sağ tarafındaki ilk iki parlaklık değeri, çift ise sol tarafındaki ilk iki parlaklık değeri verinin ortaya çıkarılması için kullanılacaktır. Resim ilk piksel değerinden okunmaya başlanır. Maksimum parlaklık değerinin çift olduğunu varsayarsak piksel değeri parlaklık değeri maksimum parlaklık değerinin bir altında ise veri dizisine “1” iki altında ise “0” kullanılan imgelerin renk tonlarına göre gömülecek veri kapasitesi değişmektedir.

Saklanan verinin ortaya çıkarılması için kullanılan akış şeması Şekil 2.7’de gösterildiği gibidir. Gizli veri sonu kodu elde edilene kadar bu döngü devam eder ve ilgili veri dizisi oluşturulur. Tez kapsamında gerçekleştirilen ara yüzde gömülen veri içerisinde Türkçe karakterlerin de olabileceği durumu göz önünde bulundurularak, 10 bitlik bloklara ayrılmıştır. Her 10 bit değer desimal değerine karşılık gelen ASCII kodu okunarak karakter karşılığı bulunur. Karakterin birleşmesiyle resim içerisinde yer alan gizli veri ortaya çıkarılmış olur.



Şekil 2.7. YHY’de gizli veriyi çıkarma akış şeması

3.UYGULAMA YAZILIMI VE YÖNTEMLERİN ÇIKTISININ DEĞERLENDİRİLMESİ

Bu bölümde, tez çalışması kapsamında geliştirilen yöntem ve daha önce farklı kişiler tarafından uygulanmış yöntemler uygulama üzerinde gerçekleştirilmiş, ilgili yöntemlerin çıktıları oluşturulmuştur. Veri gizleme yöntemleri için kullanılan kapasite, değişim ve dayanıklılık referansları kullanılarak yöntemler değerlendirilmiş ve başarımları sunulmuştur.

3.1.Test Yöntemi

Steganografi alanında gizlenecek veriyi örtü resim içerisine gömmek kadar stego resmin bilgi sakladığının üçüncü kişiler tarafından anlaşılmaması da önemlidir. Bu kapsamda kullanılan algoritmanın sağlamlığını test etmek için pek çok yöntem geliştirilmiştir. Bu tez çalışmasında kullanılan yöntem sonuçlarını test etmek için tepe sinyal-gürültü oranı (peak signal to noise ratio-PSNR), ortalama kare hatası (Mean Square Error-MSE), histogram analizi ve steganaliz yazılımları kullanılmıştır.

Bir steganografik yöntemin başarısı, steganaliz yöntemlerine karşı güçlülüğüdür. Steganalizin en önemli amacı bir örtü nesnesinde bir verinin gizli olup olmadığını tespit etmektir. Eğer stego nesnede gizli veri olduğu tespit edilirse, gizli veriyi elde etmek için çalışılır. Gizlenecek verinin tespit edilmemesi veya zor tespit edilmesi için stego nesne üzerinde yapılacak değişikliklerin olabildiğince az olması gereklidir [54].

PSNR, iki resim arasındaki benzerlik hakkında bilgi verir ve benzerlik ne kadar fazla ise PSNR değeri o kadar yüksektir. İki aynı resim arasında bu değer sonsuz olarak ifade edilir. Geliştirilen uygulama da orijinal resimler ile gömü verisi gizlendikten sonra kaydedilen resim arasındaki PSNR değerleri incelenerek, LSB yönteminin uygulanması durumundaki değerler ile karşılaştırma yapılmaktadır. Gömü verisi gizlenmesi sonucunda resim üzerinde değişim olması kaçınılmazdır. Ancak değişimi

minimal seviyelerde tutmak veri gizleme yöntemlerinin başarısını ortaya koymaktadır. Tabi gizlenen veri boyutu da bunun için oldukça önemlidir.

Görüntü kalitesini bozan önemli bir faktör, gürültüdür. PSNR'ın yüksek değeri, oldukça kaliteli bir görüntü ve daha düşük bir gürültü seviyesini ifade eder. PSNR'ın hesaplanması için referans olarak bir giriş görüntüsü alınır ve giriş görüntüsündeki gürültü seviyesini ölçmek için bir çıkış görüntüsüyle giriş görüntüsü karşılaştırılır [55]. Eğer iki görüntü aynı ise PSNR değeri sonsuzdur [56]. Bir görüntünün PSNR değerini hesaplayan formül, Denklem(3.1)'de gösterilmektedir [57].

$$PSNR=10\log_{10}\left(\frac{R^2}{MSE}\right) \quad (3.1)$$

MSE, Denklem (3.2)'deki formül aracılığı ile piksel değerlerinin farkının karelerinin tüm piksel değerine oranlanması sonucunda hesaplanır. Eğer iki imge aynı ise MSE değeri 0'dır [56, 58].

$$MSE=\frac{1}{MN}\sum [I_1(m,n)-I_2(m,n)]^2 \quad (3.2)$$

Denklem (3.1) ve Denklem (3.2)'de I_1 ve I_2 sırasıyla giriş ve çıkış görüntülerini, M ve N ise resim boyutlarını, R ise bir pikselin alabileceği en yüksek değeri ifade etmektedir. PSNR ve MSE arasında ters orantılı bir ilişki bulunmaktadır. Daha düşük MSE daha büyük PSNR anlamına bu ise daha az hata anlamına gelmektedir [55].

Histogram analizleri resme veri gömme sonucu değişen piksel değeri çiftlerinin istatistiksel analizlerini esas almaktadır. Parlaklık değeri ve parlaklık değerine ait frekans değeri resmin histogram bilgisini oluşturur. Uygulama yazılımında orijinal resim ve veri gizlenmiş resimlerin histogram analizi yapılmaktadır. Yöntemlerin başarısının değerlendirilmesinde histogram analizi ölçüt olarak kullanılmıştır.

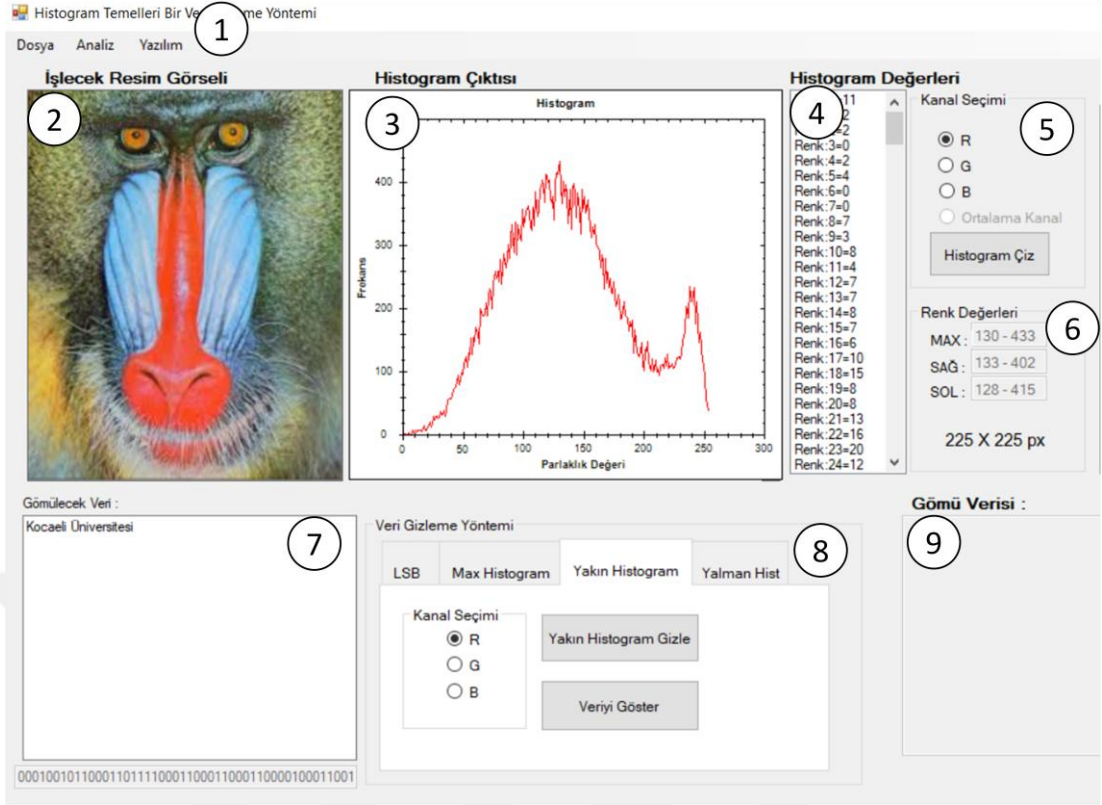
Stegspy ve stegdetec yazılımları kullanılarak yöntemler için gizli veri şüphe durumu belirlenmeye çalışılmıştır. Yazılımlar dosyada veri saklı olup olmadığını ve saklıysa hangi yazılımla saklandığını tespit edebilmektedirler.

Yöntemlerin performans sonuçları, resim üzerindeki değişime tabi tutulan bit sayısı, sinyal gürültü oranı, yapısal benzerlik indeksi ve steganaliz saldırıları ölçülür [59].

3.2.Uygulama Yazılımının Tanıtılması

Bu tezde tasarlanan uygulama yazılımı, Visual Studio 2017 platformunda C# programlama dili kullanılarak, çalıştırılabilir program dosyası (*exe*) biçiminde tasarlanmıştır. Resim formatı olarak, çok kullanılması nedeniyle,“*jpg*” uzantılı resimler tercih edilmiştir. Uygulamanın ekran görüntüsü bölüm numaraları eklenerek Şekil 3.1’ de gösterilmiştir.

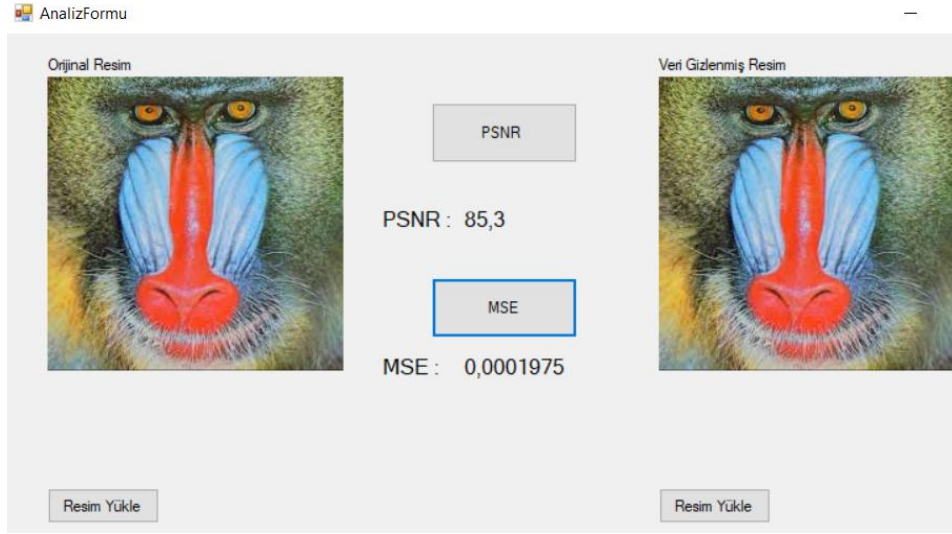
- 1 numaralı alan: Uygulama menüsüdür ve uygulama üzerinde işlenecek resmin yüklenmesi ve test yöntemleri iletişim araçları bulunur.
- 2 numaralı alan: İşlenecek resmin gösterildiği bölümdür. Gizleme işlemi yapılacak resim veya gizli verinin ortaya çıkarılması için kullanılacak resim aynı alan üzerine gösterilir.
- 3 numaralı alan: İşlenecek resimlerin histogram değerlerinin grafik halinde gösterildiği bölümdür.
- 4 numaralı alan: İşlenecek resimlerin histogram değerlerinin sayısal olarak gösterildiği bölümdür.
- 5 numaralı alan: Farklı kanallardaki histogram değerlerinin gösterilmesi için kullanılır. Uygun kanalın belirlenmesi için önemlidir.
- 6 numaralı alan: Yöntemlerin kullanacağı parlaklık değerlerinin frekans değerlerini sayısal olarak gösterir,
- 7 numaralı alan: Gömülecek verinin metinsel olarak yazıldığı bölümdür.
- 8 numaralı alan: Veri gizleme yönteminin seçildiği kısımdır.
- 9 numaralı alan: Gizli verinin gösterilmesi için kullanılır.



Şekil 3.1. Uygulama yazılımının görseli

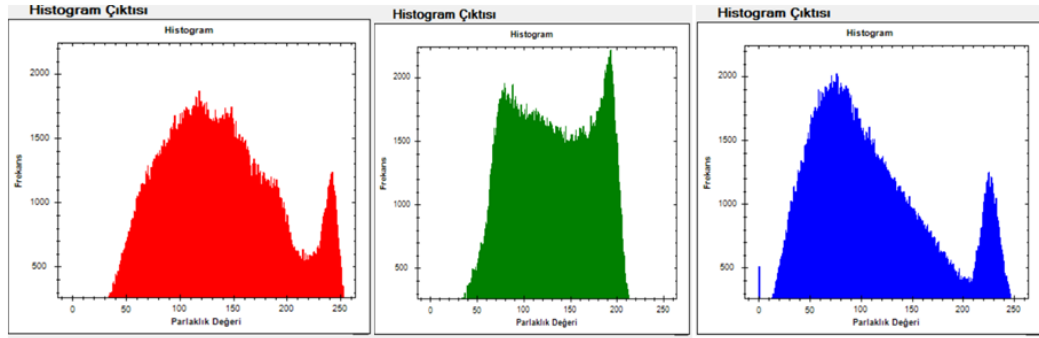
Uygulama, gömülmek istenen veri yazıldıkça, karakterlerin ASCII kodunu alarak ilgili metni binary sayı sistemine çevirmektedir. Türkçe karakterlerin desteklenebilmesi için her ASCII kod, 10-bitlik veri olarak ifade edilmektedir. Gömü verisi sonu NULL (0000000000) ifadesinin eklenmesiyle sonlandırılır. Gizli verinin ortaya çıkarılması esnasında ise yine NULL kodundan faydalanılmaktadır.

Şekil 3.2’de, yöntemlerin değerlendirilmesi için kullanılan PSNR ve MSE değerlerinin hesaplanması aşamasında kullanılan analiz formu ara yüzü yer almaktadır.



Şekil 3.2. Uygulama yazılımının analiz formu görseli

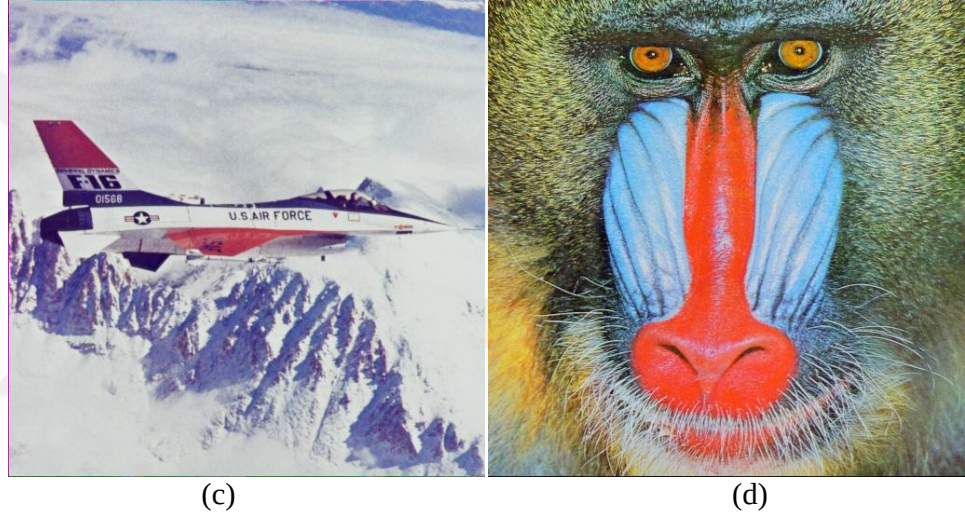
Şekil 3.3'te ise resimlere ait histogram değerleri yer almaktadır. Görüldüğü üzere RGB bileşenlerinin her biri için histogram değerleri oluşturulmaktadır.



Şekil 3.3. Örnek bir resim için elde edilen histogram değerleri

3.3.Örnek Uygulamalar ve Başarım Değerlendirmesi

Literatürde veri gizleme çalışmalarında referans olarak kullanılan Lena, Peppers, Airplane ve Baboon imgeleri Şekil 3.4'te verilmektedir. Referans olarak kullanılan tüm resimler literatürde olduğu gibi 512×512 piksel boyutlarındadır [60].



Şekil 3.4. Uygulama yazılımında kullanılan referans resimlerin orijinal halleri (a-Lena, b-Peppers, c-Airplane, d-Babbon)

Başarım değerleri, uygulama üzerindeki farklı yöntemlerden elde edilen sonuçlarla yapılan karşılaştırmalı tablolar üzerinde verilmektedir. Veri gizleme çalışmaları deneysel sonuçların değerlendirilmesinde istatistiksel kalite ölçümü için PSNR ve MSE ölçütleri kullanılmıştır.

Oluşturulan tablolar üzerinde;

- LSB Yöntemi: Yöntem-I
- HSV Yöntemi: Yöntem-II
- Maksimum Histogramlar Yöntemi: Yöntem-III
- Yakın Histogramlar Yöntemi: Yöntem-IV olarak ifade edilmiştir.

Referans resimler üzerine farklı boyutlardaki verilerin gizlenmesi sonucu oluşan PSNR ve MSE değerleri Tablo 3.1, Tablo 3.2’de gösterilmiştir. Yöntem-I’in PSNR değeri her ne kadar yüksek sonuçlar üretse de taşıyıcı resmin histogramını değiştirmesi, gizli veri algısını oluşturmaktadır. Önerilen Yöntem-IV’ün PSNR değerleri ve kapasite olarak fazla veri gömme imkanı sağlaması diğerlerinden üstünlüğüdür. Yöntem-II’nin ise PSNR başarımı yüksektir ancak kapasite sınırlıdır.

Tablo 3.1. PSNR başarım değerleri

Resim	Gömü Verisi	PSNR Değeri (dB)			
		Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Lena	70Bit	97,5	98,38	70,47	99,12
Babbon	190Bit	83,21	89,50	58,13	90,60
Peppers	100Bit	85,20	91,20	75,30	92,30
Airplane	150Bit	92,30	93,10	74,18	94,30

Tablo 3.2. MSE başarım değerleri

Resim	Gömü Verisi	MSE (%)			
		Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Lena	70Bit	0,0001	0,00008	0,0056	0,00008
Babbon	190Bit	0,0001	0,0001	0,0078	0,0001
Peppers	100Bit	0,0001	0,00009	0,0006	0,00008
Airplane	150 Bit	0,00008	0,00009	0,0006	0,00008

Tüm veri gizleme yöntemleri, uygulandıkları taşıyıcıda insan gözünün algılayamayacağı seviyelerde bir miktar değişim oluştururlar. Değişimin fazla olması imge üzerindeki gizli verinin sezilebilirliğini artırır. Tablo 3.3’de yöntemlerin Babbon referans resmi üzerinde uygulanması ile bozulan piksel sayılarını, Tablo 3.4’de ise piksel bozulma oranlarını göstermektedir. Kullanılan resme, gizleme bileşenine, gizlenecek veriye göre çarpıcı değerler oluşturabilmektedir. Yakın histogramlar yöntemi ile elde edilen bozulma oranı diğer yöntemlere göre her seferinde daha düşük seviyelerde elde edilmiştir.

Tablo 3.3. Bozulan piksel sayıları

Resim	Gömü Verisi	Piksel Sayısı	Bozulan Piksel Sayıları			
			Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Babbon	190Bit	$512 \times 512 \times 3 = 786432$	86	94	93	17

Tablo 3.4. Piksel bozulma oranları

Resim	Gömü Verisi	Piksel Sayısı	Piksel Bozulma Oranları (%)			
			Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Babbon	190Bit	$512 \times 512 \times 3 = 786432$	0.0109	0.0119	0.0118	0.0021

Yöntemlerin, referans resimler üzerindeki test sonuçları Tablo 3.5, Tablo 3.6, Tablo 3.7 ve Tablo 3.8’de verilmiştir.

Tablo 3.5. Yöntem-I’in referans resimlerde uygulanması

Örtü Resmi	Kanal-I		Kanal-II		Kanal-III		Gömü Verisi
	Kırmızı (R)		Yeşil (G)		Mavi (B)		
	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	
Lena	0,001	78,02	0,001	78,6	0,001	78,02	210 Bit
Babbon	0,0001	85,5	0,0001	85,5	0,0001	84,5	210 Bit
Peppers	0,0002	83,4	0,0001	84,4	0,0001	85,4	210 Bit
Airplane	0,0003	82,5	0,001	82,5	0,0001	82,5	210 Bit

Tablo 3.6. Yöntem-II’nin referans resimlerde uygulanması

Örtü Resmi	Kanal-I		Kanal-II		Kanal-III		Örtü Resmi
	Kırmızı (R)		Yeşil (G)		Mavi (B)		
	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	
Lena	0,0001	90,64	0,0001	89,7	0,00007	94,9	170 Bit
Babbon	0,0001	88,8	0,0001	89,1	0,0001	88,9	210 Bit
Peppers	0,0001	87,15	0,0001	90,2	0,0001	89,4	210 Bit
Airplane	0,0001	89,5	0,0001	89,6	0,0001	89,6	210 Bit

Tablo 3.7. Yöntem-III’nin referans resimlerde uygulanması

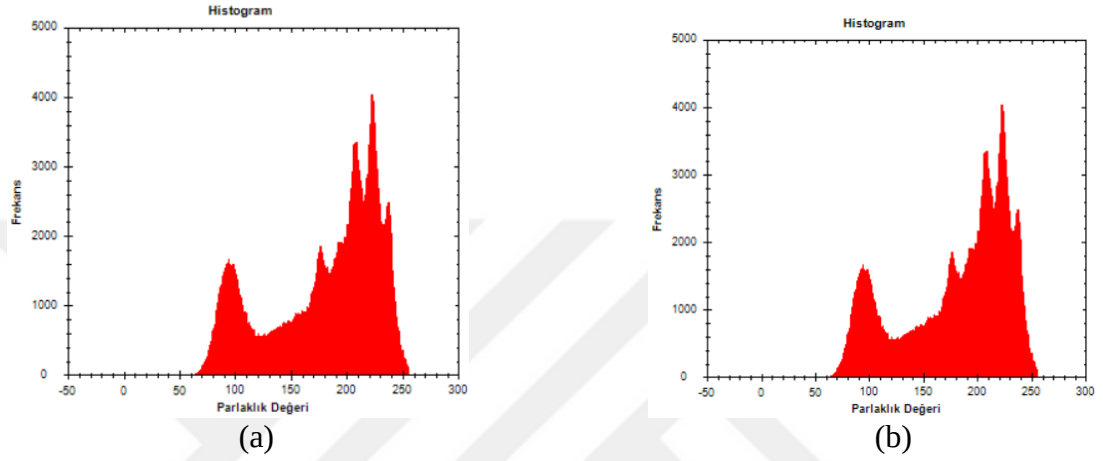
Örtü Resmi	Kanal-I		Kanal-II		Kanal-III		Örtü Resmi
	Kırmızı (R)		Yeşil (G)		Mavi (B)		
	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	
Lena	0,001	62,31	0,362	15,25	0,425	12,20	210 Bit
Babbon	0,003	55,36	0,025	36,81	0,006	50,79	210 Bit
Peppers	0,0005	75,45	0,001	65,26	0,002	61,98	210 Bit
Airplane	0,0007	71,65	0,001	66,52	0,001	62,49	210 Bit

Tablo 3.8. Yöntem-IV’ün referans resimlerde uygulanması

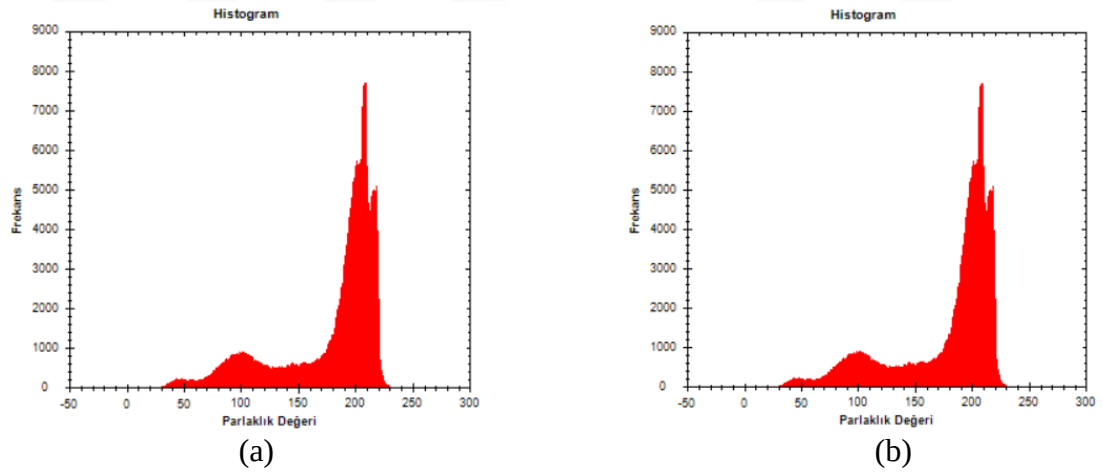
Örtü Resmi	Kanal-I		Kanal-II		Kanal-III		Örtü Resmi
	Kırmızı (R)		Yeşil (G)		Mavi (B)		
	MSE	PSNR(dB)	MSE	PSNR(dB)	MSE	PSNR(dB)	
Lena	0,0001	89,02	0,0001	90,32	0,0001	89,21	210 Bit
Babbon	0,0001	89,5	0,0001	89,80	0,0001	88,93	210 Bit
Peppers	0,0001	89,31	0,0001	88,75	0,0001	90,64	210 Bit
Airplane	0,0001	89,5	0,0001	89,9	0,001	90,32	210 Bit

Yöntemlerin referans resimlere uygulanması sonucu oluşan tablolar incelendiğinde, önerilen Yöntem-IV’ün PSNR ve kapasite değerleri açısından üstün olduğu saptanmıştır. Yöntem-II’nin ise dayanıklılık açısında çok üst seviyelerde olmasına rağmen kapasite açısından Yöntem IV’e göre daha sınırlı olduğu gözlemlenmiştir.

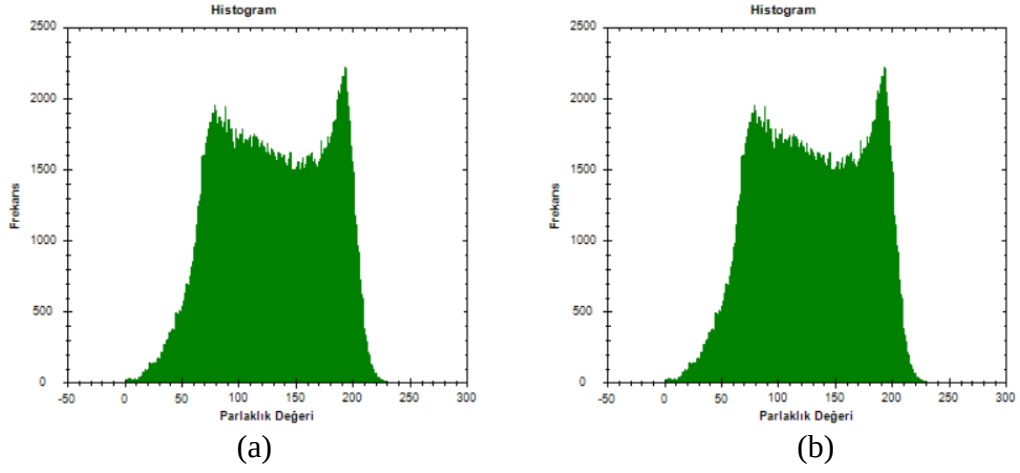
Yöntemlerin histogram grafikleri incelendiğinde ise Yöntem I’de, verinin gömülmesi sonucunda grafik üzerinde değişiklikler olduğu gözlemlenmiştir. Gizli veri kapasitesinin artırılması sonucunda bu değişim daha da artmaktadır. Yöntem-III ve Yöntem-IV için histogram grafiklerinin hiç değişmediği, orijinal resim histogramının korunduğu, Yöntem-II’de ise değişimin çok düşük seviyelerde olduğu tespit edilmiştir.



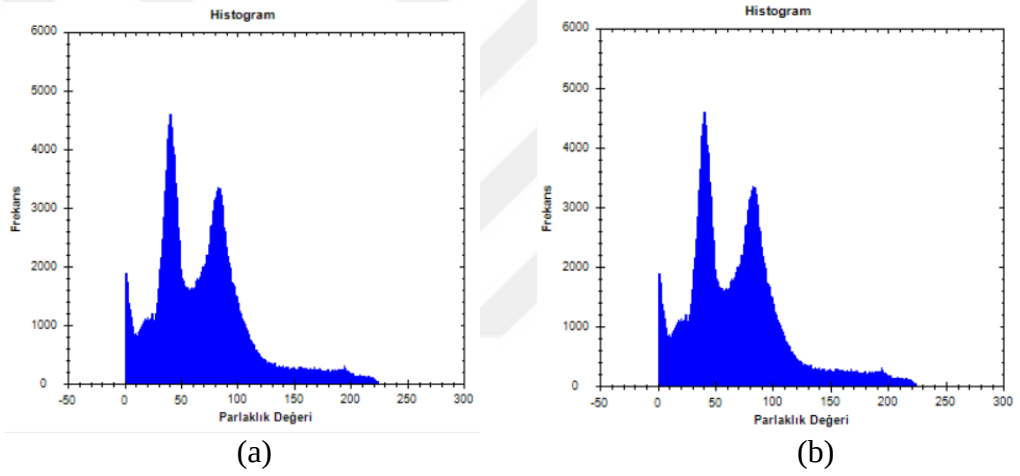
Şekil 3.5. Lena referans resminin Yöntem-I için (a) veri gömmeden önce (b)gömüldükten sonraki histogram grafikleri



Şekil 3.6. Airplane referans resminin Yöntem-II için (a) veri gömmeden önce(b) gömüldükten sonraki histogram grafikleri



Şekil 3.7. Babbon referans resminin Yöntem-III için (a) veri gömmeden önce (b) gömüldükten sonraki histogram grafikleri



Şekil 3.8. Peppers referans resminin Yöntem-IV için (a) veri gömmeden önce (b) gömüldükten sonraki histogram grafikleri

Tablo 3.9. Yöntemlerin histogram analiz sonuçları

Yöntemler	Histogram
Yöntem-I	Değişir
Yöntem-II	Değişir
Yöntem-III	Değişmez
Yöntem-IV	Değişmez

Orijinal resim ile gizleme sonucu oluşan stego nesnesinin histogramları karşılaştırılmıştır. Tablo 3.9’da yöntemlere göre sonuçlar gösterilmiştir.

Tablo 3.9. StegSPy yazılımı sonuçları

Resim	Gömü Verisi	Yöntemler			
		Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Lena	70Bit	Tespit Edildi	Tespit edilemedi	Tespit edilemedi	Tespit edilemedi
Babbon	190Bit	Tespit Edildi	Tespit edildi	Tespit edildi	Tespit edilemedi
Peppers	100Bit	Tespit Edildi	Tespit edilemedi	Tespit edilemedi	Tespit edilemedi
Airplane	150 Bit	Tespit Edildi	Tespit edildi	Tespit edildi	Tespit edilemedi

Steganaliz programı StegSPy referans resimler üzerinde uygulanması Tablo 3.10’da verilmiştir. Önerilen yöntem kullanılarak saklanan resimlerde steganaliz yazılımı tarafından gizli verinin olduğu tespiti yapılamamıştır.

Tablo 3.10. Stegdetect yazılımı sonuçları

Resim	Gömü Verisi	Yöntemler			
		Yöntem-I	Yöntem-II	Yöntem-III	Yöntem-IV
Lena	70Bit	Tespit Edildi	Tespit edilmedi	Tespit edilmedi	Tespit edilmedi
Babbon	190Bit	Tespit Edildi	Tespit Edildi	Tespit Edildi	Tespit edilmedi
Peppers	100Bit	Tespit Edildi	Tespit edilmedi	Tespit Edildi	Tespit edilmedi
Airplane	150 Bit	Tespit Edildi	Tespit Edildi	Tespit Edildi	Tespit Edildi

Stegdect steganaliz yazılımı elde edilen sonuçlar Tablo3.10 üzerinde gösterilmiştir.

4. SONUÇLAR VE ÖNERİLER

Steganografi çalışmaları, bilgi güvenliğinin giderek daha fazla önem kazandığı günümüzde yaygın olarak uygulanmaktadır. Bu yöntem, askeri haberleşme, kişisel verilerin korunması ve kimlik doğrulama gibi birçok alanda veri güvenliği için kullanılmaktadır. İnternetin hızla gelişerek geldiği bu aşamada ortaya çıkan güvenlik açığı sorunu nedeniyle verilerin gizlenmesi resim yada metin olarak iletilmesi artan bir ilgi konusu olmuştur [61]. Bu tez çalışmasının amacı, klasik yöntem olan LSB, geliştirilen iki hibrit yöntem ve Yalman [26] tarafından geliştirilen HSV yönteminin karşılaştırmalı başarımlarını değerlendirmesinin yapılmasıdır. Gömme işlemi sonucunda örtü nesnesinde insan gözü tarafından algılanamayacak düzeyde piksel değişimleri oluşmaktadır. Örtü nesnesi üzerinde maksimum düzeyde bilgi saklanması sunulan yöntemlerde hedeflenmiş ve kapasite kriterleri kullanılarak yöntemlerin başarımları belirtilmiştir. Yöntemlerin hesaplama karmaşıklıkları, görsel ve istatistiksel olarak fark edilmezlikler ve görsel ataklara karşı dayanıklılıkları değerlendirilmiştir.

- Uygulama üzerinde gerçekleştirilen dört farklı yöntemde de gömü verisinin elde edilmesinde orijinal imgeye ihtiyaç duymamaktadır. Sadece stego-nesneler kullanılarak gizli veriler elde edilebilmektedir.
- Uygulama üzerindeki tüm yöntemler, farklı formatlardaki 24bitlik RGB imgelere uygulanabilmektedir.
- Tez kapsamında geliştirilen uygulama dört farklı veri gizleme yönteminin gizleme işlemini gerçekleştirmesini sağlamıştır. İlgili yöntemler için başarımlarını değerlendirmesi sağlamaktadır.
- Daha önce geliştirilen LSB, Yalman yöntemi [4] ve tez içerisinde sunulan histogram temelli iki farklı yöntemin tüm algoritmaları ve detayları sunulmuştur. Tez akademik bir çalışmadır, algoritma ve tüm kodları açık olarak mevcuttur.
- Tercihen jpg dosya uzantısı kullanılmıştır. Farklı uzantıdaki resimlerde uygulama üzerinde işlenebilmektedir.

- Klasik steganografi yöntemlerinin birçoğunda verinin gizlenmesinden sonra resim üzerinde değişiklikler oluşmaktadır. Resmin histogram analizinde bu durum ortaya çıkmakta, orijinal resim histogramından farklı bozucu etkiler oluşmaktadır. Önerilen yöntemde orijinal resimle veri gizlenen resim histogram grafiğinde hiçbir farklılık yoktur. Resim üzerinde gömü verisi varlığı şüphesini ortadan kaldırmaktadır.
- Önerilen hibrit yöntemin histogram bilgisini kullanarak veri gömülecek alanları tespit etmesi, değişen bit değerleri sayısınca zıt değişiklik yapması resim histogramının aynı kalmasını sağlamaktadır.
- İnsan gözü tarafından algılanamaz seviyelerde olan resim üzerindeki değişikliklerin bir ve üçüncü yöntem için uygulanacak görsel bir atakta gömülen veri kaybolabilmektedir.
- Steganaliz yazılımları üzerinde stego nesneleri test edilmiş ve önerilen yakın histogramlar yönteminin başarılı sonuçlar ürettiği görülmüştür.

4.1. Öneriler

Geliştirilen hibrit yöntem üzerinde aşağıdaki şekilde sıralanan durumların eklenmesi yöntemin başarımlar seviyesini artıracaktır.

- Gömü veri kapasitesinin artırılması için imge histogramının imgeyi bölümlere ayırarak ve bölgesel histogram değerleri kullanılarak veri gizleme işlemi yapılabilir. Bu şekilde kapasite ve dayanıklılık seviyeleri artırılabilir.
- Geliştirilen uygulamada, verilerin saklanması şifreleme fonksiyonu kullanılmaktadır. Gömülecek veri bir şifreleme algoritmasından geçirilerek gömülmesi güvenliğini artıracaktır.

KAYNAKLAR

- [1] Hassan D.M., Steganaliz Yaklaşımlarının Karşılaştırılması, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2008, 233706.
- [2] Phan R.C.W., Ling H.C., Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cita03, *MMU International Symposium on Information and Communication Technologies/M2USIC 2003*, Petaling Jaya, Malaysia, 2-3 Oct 2003.
- [3] Kurnaz H., Sondaş A., Histogram Temelli Bir Veri Gizleme Yönteminin Uygulanması, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi*, Kocaeli, Türkiye, 23-25 Kasım 2018.
- [4] Yalman Y., Ertürk İ., İmge Histogramı Kullanılarak Geometrik Ataklara Dayanlı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulanması, *XI. Akademik Bilişim Konferansları*, Harran Üniversitesi, Şanlıurfa, 11-13 Şubat 2009.
- [5] Akar F., Varol H. S., A New RGB Weighted Encoding Technique For Efficient Information Hiding in Images, *Journal of Naval Science and Engineering*, 2004, **12**(2), 21-36.
- [6] Chrysochos E., Fotopoulos V., Skodras A., Xenos M., Reversible Image Watermarking Based on Histogram Modification, *11th Panhellenic Conference on Informatics with international participation*, Patras, Greece, 18-20 May 2007.
- [7] Ni Z., Shi Y.Q., Ansari N., Su W., Reversible Data Hiding, *IEEE Transactions on Circuits and Systems for Video Technology*, 2006, **16**(3), 354-362.
- [8] Meiamai V., Minu A., Anushia Devi R., Histogram Technique With Pixel Indicator For High Fidelity Steganography, *International Journal of Engineering and Technology*, 2013, **3**(5), 0975-4024.
- [9] Mohammed A., Al-Husainy F., Image Steganography Method Preserves the Histogram Shape of Image, *European Journal of Scientific Research*, 2015, **1**(130), 101-106.
- [10] Xuan G., Shi Y. Q., Chai P., Cui X., Ni Z., Tong X., Optimum Histogram Pair Based Image Lossless Data Embedding, in *Proc. Int. Workshop Digit. Watermarking Ser. Springer Lect. Notes Comput. Sci.*, Guangzhou, China, 3-5 December 2007.

- [11] Gutub A., Ankeer M., Abu-Ghalioun M., Shaheen A., Alvi A., Pixel Indicator High Capacity Technique for RGB Image Based Steganography, *WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E., 18 - 20 March 2008.
- [12] Chang C. C.; Tai W. L., Chen K. N., Lossless Data Hiding Based on Histogram Modification for Image Authentication, *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, DOI 10.1109/EUC.2008.20.
- [13] Yargıçoğlu A.U., Düşük Veri Hızlarında Çalışan Konuşma Kodlayıcılarına Gürbüz Bilgi Saklama ve Damgalama, Doktora Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2010, 285037.
- [14] Yalman Y., Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi, Yüksek Lisans Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, 2007, 232677.
- [15] Farid H., Detectic Steganographic Messages in Digital Images, *Dartmouth Collage Computer Science*, Hanover, Bileşik Devletler, 8 April 2005.
- [16] Bandırmalı N., Yeni Bir Kablosuz Algılayıcı Ağ Veri Bağı Katmanı Güvenlik Protokolü Tasarımı, Doktora Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, 2010, 259437.
- [17] Chouse C., ve Albayrak S., Dayanıkl Sayısal Resim Damgalama, Yıldız Teknik Üniversitesi, https://www.academia.edu/2519034/DAYANIKLI_SAYISAL_RES%20C4%B0M_DAMGALAMA (Ziyaret tarihi : 20 Ocak 2019).
- [18] Barni M., Bartolini F., Enabling *Digital Assetssecurity and Other Applications*, 10rd ed., Marcel Dekker Inc., New York, 2004.
- [19] Che Wei L., Wen Hsiang T., A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme, *Pattern Recognition and Machine Vision*, River Publishers, Aalborg, Denmark, 1-14, 2010.
- [20] Doğan F., Daş R., Türkoğlu İ., İmgeler İçin Farklı Veri Gizleme Yaklaşımı, *Dicle Üniversitesi Mühendislik Dergisi*, 2016, 7(3), 511-514.
- [21] Patel Z. V., Gadhiya S. A. A Survey Paper on Steganography and Cryptography, *International Multidisciplinary Research Journal (RHIMRJ)*, 2015, 2(5), 2349-7637.
- [22] <http://bilgisayarkavramlari.sadievrenseker.com/2009/06/05/steganografi-ve-lsb/> (Ziyaret tarihi: 20.01.2018).
- [23] Avcı E., Tuncer T., Ertam F., Çok Katmanlı Görüntü Steganografi, *7thInternatinal Conference on Information Security and Cryptology*, İstanbul, Türkiye, 17-18 Oct 2014.

- [24] Anderson R. J., Petitcolas F. A. P., On the Limits of Steganography, *IEEE Journal On Selected Areas In Communications*, 1998, **16**(4) 474-481.
- [25] Şahin A., Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 2007, 199963.
- [26] Yalman Y., Sayısal Görüntüler İçin Histogram Temelli Veri Gizleme Yöntemi ve Uygulama Yazılımı, Doktora Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli, 2010, 272801.
- [27] Cetin O., Ozcerit A.T., A New Steganography Algorithm Based On Color Histograms For Data Embedding Into Raw Video Streams, *Computers & Security*, 2009, **28**(7), 670–682.
- [28] Simmons G., The Prisoners Problem and the Subliminal Channel, *CRYPTO83 Advances in Cryptology*, California, USA, 22 -24 Aug 1984.
- [29] Gürcan O.G., Güvenli Veri İletişimi İçin Ön Anahtarlama Farklı Bir Veri Gizleme Tekniğinin Geliştirilmesi, Yüksek Lisans Tezi, Deniz Harp Okulu, Deniz Bilimleri ve Mühendisliği Enstitüsü, 2014, 365492.
- [30] <https://www.dicle.edu.tr / Contents / 0c966fc8-a6a4-47a5-9ef8-156e81ed49c.pdf>, (Ziyaret tarihi: 10 Ocak 2019).
- [31] Hussain M., Survey of Image Steganography Techniques, *International Journal of Advanced Science and Technology*, 2013, **54**(1), 113-123.
- [32] Kondo K., A Data Hiding Method for Stereo Audio Signals Using the Polarity of the Inter-Channel Decorrelator, *IEEE Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP'09*, Washington, USA, 12-14 September 2009.
- [33] Yu L., He-xin C., Yan Z., A New Method of Data Hiding Based on H.264 encoded video sequences, *IEEE 10th International Conference on Signal Processing(ICSP)*, Lucknow, India, 24-28 Oct. 2010.
- [34] Xiaoyin Qi, Xiaoni Li, Mianshu Chen, Hexin Chen, Research on CAVLC Audio Video Synchronization Coding Approach Based on H.264, *IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE)*, Bali, Indonesia, 4- 7 Aug. 2011.
- [35] Yiğit Y., Sayısal İmgelerde Güvenli Veri Gizlemeye Yönelik Uygun Maske Belirleme, Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ, 2018, 501144.
- [36] Patel Z. V., Gadhiya S. A., A Survey Paper on Steganography and Crptography, *International Multidisciplinary Research Journal*, 2015, **2**(5) 68-71.

- [37] Kamran A., Deepa K., Practical Data Hiding in TCP/IP, *Proceedings of ACM Workshop on Multimedia Security*, Mumbai, India, 7-19 July 2002.
- [38] Neeta D., Snehal K., Jacobs D., Implementation of LSB Steganography and Its Evaluation for Various Bits, *Digital Information Management*, Bangalore, India, 04 June 2006.
- [39] Doğan F., Daş R., Türkoğlu İ., İmgeler İçin Farklı Veri Gizleme Yaklaşımı, *Dicle Üniversitesi Mühendislik Fakültesi Dergisi*, 2016, **3**(7), 501-514.
- [40] Tiwari A., Yadav S. R., Mittal N.K., A Review on Different Image Steganography Techniques. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2014, **3**(7), 121-124.
- [41] Pereira S., Pun T., Robust Template Matching For Affine Resistant Image Watermarks. *IEEE Trans. Image Process.*, 2000 **9**(6), 1123-1129.
- [42] Pun C.M., A novel DFT-Based Digital Watermarking System for Images. *Proc., Signal Processing*, 2006, **2**(3), 137-138.
- [43] Lumini A., Maio A., Wavelet-Based Image Watermarking Scheme. In *Proceedings, International Conference on Information Technology*, DOI:10.1109.
- [44] Wang H. S., Lin Y. P., Wavelet Tree Quantization for Copyright Protection Watermarking, *IEEE Trans. Image Process.*, 2004, **13**(2):154-165.
- [45] Wang Y. P., Chen M.J., Cheng P. Y., Robust Image Watermark With Wavelet Transform and Spread Spectrum Techniques, *Proceedings Thirty-Fourth Asilomar Conference on Signals Systems and Computers*, 2000, **2**(1), 1846-1850.
- [46] <https://www.tech-worm.com/piksel-nedir/> (Ziyaret tarihi: 09 Ocak 2019)
- [47] Kumar R., Chand S., Singh S., A Reversible Data Hiding Scheme Using Pixel Location, *The International Arab Journal of Information Technology*, 2018, **4**(15), 10056-10060.
- [48] http://yunus.hacettepe.edu.tr/~eacar/dersler/SBE238/resim_format.pdf (Ziyaret tarihi: 09 Ocak 2019).
- [49] <https://99designs.com/blog/tips/image-file-types/> (Ziyaret tarihi: 09 Ocak 2019).
- [50] Tuncer T., Resimler İçin Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları, Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ, 2011, 287054.
- [51] Coşun I., Akar F., Çetin Ö., A New Digital Image Steganography Algorithm Based on Visible Wavelength, *Turkish Journal of Electrical Eng. & Computer Sci.*, DOI:10.3906/elk-1108-74.

- [52] Charudhary A., Vasavada J., A Hash Based Approach for Secure Keyless Image Steganography in Lossless Rgb Images, *First Int. Workshop on Cyber Crime*, St. Petersburg, Russia, 3-5 Oct. 2012.
- [53] Konyar Z., İlkin S., Çelik N., Sondaş A. Steganografi İçin En Uygun Resmi Belirleyen Uygulama Arayüz Tasarımı, *İleri Teknoloji Bilimleri Dergisi*, 2018, **1**(7), 83-89.
- [54] Razavı N., LSB Steganografi Yönteminde Yüksek Kapasiteli Veri Gizleme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2017, 472694.
- [55] Kaş Ü., Tanyıldızı E., Euler Renk ve Hareket Büyütme Yöntemlerinin Performans Analizi, *Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi*, DOI: 10.5578/fmbd.58648.
- [56] Olcay C., Saran N., İmge İçine Bilgi Gizlemede Kullanılan LSB Yöntemlerinin Karşılaştırılması, *Çankaya University Journal of Science and Engineering*, 2013, **1**(10), 17-32.
- [57] Sencar H.T., Ramkumar M., Akansu A.N., Data Hiding Fundamentals and Applications, *Elsevier*, Academic Press, New York, 2004.
- [58] Honsinger C. W., Jones, P., Rabbani M., Stoffel J. C., Lossless Recovery of an Original Image Containing Embedded Data, 2001, *United States Patent No: 6,278,791*, USE Patent.
- [59] Aydoğan T., Bayılmış C. A New Efficient Block Matching Data Hiding Method Based on Scanning Order Selection in Medical Images, *Turkish Journal of Electrical Engineering & Computer Sciences*, DOI:10.3906/elk-1506-189.
- [60] <https://homepages.cae.wisc.edu/~ece533/images/> (Ziyaret tarihi :09 Ocak 2019)
- [61] Gümüşsu A., Veri Gömme Tabanlı Bir Kimliklendirme Sisteminin Tasarımı, Yüksek Lisans Tezi, Deniz Harp Okulu Elektronik Mühendisliği Bölümü, İstanbul, Haziran 2013, 333142.

KİŞİSEL YAYIN VE ESERLER

Kurnaz H., Sondaş A., Histogram Temelli Bir Veri Gizleme Yönteminin Uygulanması, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi*, Kocaeli Türkiye, 23-25 Kasım 2018.

Kurnaz H., Mobil Öğrenme Özelliğinin Öğrenciler Tarafından Kullanılabilirliği, Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, Sakarya Üniversitesi, Sakarya, Türkiye 2010, 273129.

ÖZGEÇMİŞ

Harun KURNAZ 1986'da Erzurum'da doğdu. Lise öğrenimini Artvin Teknik ve Endüstri Meslek Lisesi'nde tamamladı. 2007 yılında Karaelmas Üniversitesi Karabük Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümünden mezun oldu. 2008 yılından itibaren Milli Eğitim Bakanlığı'nda, bilişim teknolojileri alan öğretmeni olarak çalışmaktadır. Evli ve bir evlat sahibidir.

