T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLERDE BLOK VE TARAMA SIRASI TEMELLİ YENİ BİR VERİ GİZLEME ALGORİTMASI TASARIMI

DOKTORA TEZİ

Turgay AYDOĞAN

Enstitü Anabilim Dalı : ELEKTRONİK ve BİLGİSAYAR EĞİTİMİ

Tez Danışmanı : Doç. Dr. Cüneyt BAYILMIŞ

Aralık 2016

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLERDE BLOK VE TARAMA SIRASI TEMELLİ YENİ BİR VERİ GİZLEME ALGORİTMASI TASARIMI

DOKTORA TEZİ

Turgay AYDOĞAN

Enstitü Anabilim Dalı : ELEKTRONİK ve BİLGİSAYAR EĞİTİMİ

Bu tez 16/12/2016 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Doç. Dr. Cüneyt BAYILMIŞ Jüri Başkanı	Doç. Dr. Ecir Uğur KÜÇÜKSİLLE Üye	Yrd. Doç. Dr. İsmail Serkan ÜNCÜ Üye
Yrd. Doç. Dr. Devrim AKGÜN Üye	Yrd. Doç. Dr. Sezgin KAÇAR Üye	

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Turgay AYDOĞAN

16.12.2016

TEŞEKKÜR

İnsanın özünde yer alan, doğumundan ölümüne kadar devam etmekte olan öğrenme içgüdüsü sayesinde insanoğlu yeni konuları öğrenmekte ve yenilikçi olan fikirlerini ortaya çıkarmak için çalışmaktadır. Öğrenme içgüdüsü içerisinde yer alan, lisansüstü akademik süreçlerin en önemlisi, en büyük sabrın ve oldukça fazla azmin ihtiyaç duyulduğu doktora tez çalışması sürecinde, insan özgün ve modern bir uygulamayı ortaya çıkarmaya çalışmaktadır.

Bu süreç içerisinde elbette belli bir akademik birikimin desteğini hissetmek de oldukça önem arz etmektedir. Bu akademik birikimi bana sunan, karşılaştığım her sorunda ve yaşadığım problemlerde beni büyük sabırla dinleyip bana destek olan, tezimin geliştirilmesinde bana yön veren tez danışmanın Sayın Doç. Dr. Cüneyt BAYILMIŞ'a en içten teşekkürlerimi sunarım.

Benim bu günlere gelmemde tepeden tırnağa büyük destekleri ve emekleri olan, benden maddi manevi desteklerini hiçbir zaman esirgemeyen çok değerli annem Nevin AYDOĞAN'a ve babam Mehmet AYDOĞAN'a, beni her zaman için destekleyen ve teşvik eden biricik abim Tuncay AYDOĞAN'a, lisansüstü çalışmalarıma şahit olup yıllardır bana manevi desteğini esirgemeyen, beni her zaman için destekleyen, bütün zor zamanlarımda benim yanımda olan ve tez çalışmasının her sürecinde hakkı olduğunu düşündüğüm değerli eşim Dilek AYDOĞAN'a ve bu süreçte zamanlarından çaldığım beni hayata bağlayan afacanlarım prensesim, canım kızım Elif ve aslan parçası oğlum Melih'e canı gönülden en içten duygularımla çok ama çok teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

AD	: Average Difference
AES	: Advanced Encryption Standard
ASCII	: American Standard Code for Information Interchange
B	: Blue-Mavi Renk Kanalı
bpp	: Bit Per Pixel
CMYK	: Cyan Magenta Yellow Key Black
CT	: Computed Tomography
CQM	: Color Image Quality Measure
dB	: Desibel
DCT	: Discrete Cosine Transform
DES	: Data Encryption Standard
DFT	: Discrete Fourier Transform
DICOM	: Digital Imaging and Communications in Medicine
DPI	: Dot Per Inch
DWT	: Discrete Wavelet Transform
EC	: Embedding Capacity
EEG	: Elektroensafolagram
f(x,y)	: Görüntü Fonksiyonu
G	: Green-Yeşil Renk Kanalı
HSI	: Hue Saturation Intensitiy
HLS	: Hue Lightness Saturation
HSV	: Hue Saturation Value
K	: Anahtar
KB	: Kilo Bayt
L	: Gizlenecek Veri Gruplarındaki Eleman Sayısı
LSB	: Least Significant Bit

LZW	: Lempel Ziv Welch
M	: Görüntünün Satır Sayısı
MD4	: Message-Digest Algorithm 4
MD5	: Message-Digest Algorithm 5
MR	: Manyetik Rezonans
MSE	: Mean Squared Error
M–SSIM	: Mean Structural Similarity Index Measure
N	: Görüntünün Sütun Sayısı
NAE	: Normalized Absolute Error
NCC	: Normalized Cross Correlation
nm	: Nanometre
NTSC	: National Television Standards Committee
O	: Orijinal Görüntü
OPENI	: Open Access Biomedical Image Search Engine
PAL	: Phase Alternate Line
PPI	: Piksel Per Inch
PVD	: Pixel Value Difference
R	: Red-Kırmızı Renk Kanalı
RC4	: Rivest Cipher 4
PSNR	: Peak Signal-to-Noise Ratio
RGB	: Red Green Blue Renk Uzayı
S	: Stego görüntü
SC	: Structural Content
SECAM	: Système Electronique Couleur Avec Mémoire
SHA	: Secure Hash Algorithm
SSIM	: Structural Similarity Index Measure
USC-SIPI	: University of Southern California Signal and Image Processing Institute
UQI	: Universal Image Quality Index
YUV	: Luminance Chrominance1 Chrominance2

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Veri gizleme, steganografi, blok eşleştirme, tarama sırası seçimi, en önemsiz bit, sayısal görüntü

Teknolojinin hızlı ilerleyişiyle sayısal veri elde etme oldukça kolay hale gelmiştir. Uçtan uca veri iletiminde ise ister istemez özel veya gizli veriler üçüncü şahısların eline geçebilmektedir. Rahatlıkla veri iletimi gerçekleştirebilmek için, veri gizleme gibi bazı ek önlemlerin alınması gerekmektedir. Gizli veri iletiminin kullanılabileceği yerlerden biri de sayısal görüntülerdir. Amacı veri gizleme olan steganografi bilimi ile istenilen bu gizliliği sağlamak mümkündür. Yapılan bu çalışmada, sayısal görüntülerde kullanılmak üzere blok eşleştirmeli ve tarama sırası seçimli tabanlı LSB tekniğini kullanan yeni bir veri gizleme algoritması geliştirilmiştir.

Ana amacı görüntü üzerinde en az değişimi yapmak olan bu yeni algoritmada, görüntü ilk olarak 8×8 boyutunda bloklara ayrılmaktadır. Yaygın olarak kullanılan iki tarama sırasına ilave olarak, yeni tasarlanan altı çeşit tarama sırasıyla bu bloklardaki pikseller taranarak verinin gizleneceği en uygun yer belirlenmektedir. Değişimin en az yapılacağı bloklar ve bunu sağlayan tarama sırası seçilip veriler bu bloklara gizlenmektedir. Oluşan yeni görüntünün piksellerinde böylece en az değişimin yapılması sağlanmıştır. Geliştirilen algoritmanın başarımında ise MSE, PSNR, UQI, M−SSIM, CQM, AD, SC, NCC ve NAE kalite ölçütleri kullanılıp yapılan hesaplamaların tamamında en iyi sonuçlar elde edilmiştir. Ayrıca görüntülerde gizli verinin olup/olmadığını ve eğer varsa ortaya çıkarılmasında kullanılan steganaliz ataklarına karşı testler yapılmış, geliştirilen algoritma bu ataklara karşı da başarılı olmuştur. Nihai olarak, algoritmanın kullanılabilmesi için bir yazılım gerçekleştirilmiş, yazılımla tıbbi görüntülerin incelenmesi, rapor hazırlanması ve veri gizlenmesi sağlanmıştır.

DESIGN OF A NEW STEGANOGRAPHY ALGORITHM BASED ON BLOCK AND SCANNING ORDER IN DIGITAL IMAGES

SUMMARY

Keywords: Data hiding, steganography, block matching, scanning order selection, least significant bit, digital image

With the rapid progress of the technology, obtaining of digital data has been become very simple. During data transmissions, special and secret data might fall into the hands of third parties. Data can be protected using some data hiding methods during their transmission through communication. Digital images are the one of the places where confidential data transmission can be used. It is possible to provide the desired privacy with steganography, which aims to hide data. In this study, a new algorithm is proposed that is based on block matching and scanning order selection using LSB to hide information in digital images.

The fundamental aim of this study is ensuring as few bit changes as possible on the image, and so, firstly the cover image separated into different sub-blocks and each sub-block has a dimension of 8×8 pixels. To find the best block for secret data, the cover image scanned with eight different scanning orders where two of these scanning orders are commonly used and where six of these scanning orders are newly designed. After scanning progress, blocks are selected which need minimum changes and uses the most suitable one of eight scanning orders. Then the secret data can be hidden in these blocks. So that, the stego image which has secret data, includes minimum changes. The image quality of the stego images obtained via the proposed method has been measured with the MSE, PSNR, UQI, M−SSIM, CQM, AD, SC, NCC and NAE image quality metrics, and best results have been achieved. The results of steganalysis, which is the process used for identifying hidden data within stego images, have been verified the robustness of the stego images. Finally, a software is developed to hide data in medical image, to create report about medical image and to analyze medical image.

BÖLÜM 1. GİRİŞ

Sayısal teknolojinin hızlı gelişmesi, ucuzlaması ve internet kullanımının yaygınlaşmasıyla artık her ev hatta mobil cihazlar sayesinde her birey her an dünyaya açılan bu ağa kolaylıkla erişebilmektedir. Günlük hayattaki sayısal veri elde etme ve bunların paylaşım oranı bu gelişmelere bağlı olarak hızla artmaktadır. Bununla birlikte veri iletimi sırasında kullanıcılar için iletişim güvenliğinin sağlanması, dikkat edilmesi gereken sorunların başında gelmektedir. İletişim anında özel verilerin gizliliği ve bu özel verinin üçüncü şahısların eline geçme endişesi de önem arz etmektedir.

Hasta ile ilgili muayene, teşhis, bakım ve hastaya yapılan tedavi hizmetleri ile ilgili uygulanan işlemler sonucunda elde edilen bilgilerin kaydedildiği bilgi kaynakları ve kayıt ortamları "tıbbi kayıt" olarak nitelendirilmektedir. Bu kayıtlar, hastanın yaşamı, sağlık geçmişi ve en son tedavisiyle ilgili bilgileri düzenli olarak kapsayan, hasta için önemli olabilecek bilgiler içermektedir. Gelişen teknolojiye bağlı olarak, sağlık sektöründe kullanılan sağlık ve hastane bilgi sistemleri kullanımı artmıştır. Sağlık bilgi sistemi içerisinde yer alan ve görüntü elde etmede kullanılan cihazların çeşitliliğinin fazlalaşmasıyla günlük elde edilen sayısal görüntü miktarı eskiye oranla oldukça artmıştır. Sağlık bilgi sistemlerinin yaygın olarak kullanılması ile hastalara ait olan muayene, teşhis, bakım ve tedavi işlemlerine ait tıbbi veriler elektronik ortamda "elektronik hasta dosyası" olarak adlandırılan belgelerde saklanmaktadır (Ataklı ve ark., 2016).

Yüksek derecede kritik bilgi içeren elektronik hasta dosyalarının oluşturulması ve kullanılması esnasında dikkat edilmesi gereken iki önemli durum vardır. Birincisi hastanın mahremiyeti mutlaka sağlanmalıdır. İkincisi ise, elektronik hasta dosyalarında yer alan veriler tahrifat veya tahribatlara karşı korumalı olmalıdır.

Örneğin bu veriler, yasa/kural dışı elde edilmesi ve kullanımına karşı güvence altına alınmalıdır. Dikkat edilmesi gereken bu durumlar ile elektronik dosya kayıtlarına ilgisiz kişilerin bilerek veya bilmeyerek ulaşıp, ele geçirmesi ve zarar vermesi veri güvenliğini önemli hale getirmiştir (Sümbüloğlu ve Akdağ, 2010). Hasta haklarının korunması, hasta mahremiyetine saygı gösterilmesi ve bilgilerinin gizli tutulması, sağlık hizmeti verilen resmi ve özel bütün kurum ve kuruluşları, bu kurum ve kuruluşlarda veya bunların dışında hizmete katılan her kademedeki ve ünvandaki ilgilileri ve hizmetten faydalanma hakkına haiz olan bütün fertleri kapsayan Hasta Hakları Yönetmeliği'nin 21. ve 23. maddelerinde açık ve net bir şekilde ifade edilmiştir (Mevzuat, 1998). Hasta mahremiyetinin sağlanması ve hastanın bilgilerinin gizli tutulması için veri gizleme teknikleri kullanılabilir. Böylece kişiye özel olan bu tıbbi kayıtlar veri gizleme teknikleri kullanılarak koruma altına alınmış olur.

Veri gizleme teknikleri çok eski zamanlardan beri kullanılmaktadır. Steganografi veri gizleme tekniklerinden biridir. Günümüze kadar steganografi kullanılarak görüntü, video, ses, metin yani sayısal olarak ifade edilebilecek her veri üzerinde çalışmalar ve araştırmalar yapılıp yeni yöntemler/algoritmalar geliştirilmiştir.

1.1. Literatürde Yapılan Çalışmaların Özetleri

Bu bölümde görüntüler için geliştirilmiş veri gizleme yöntemlerine/algoritmalarına yönelik, bu araştırmaya katkı sağlayan literatür tarama özeti verilmiştir.

Wang ve ark. (2001) çalışmalarında, örtü görüntüsünün en önemsiz bitini (LSB − Least Significant Bit) kullanan yeni bir yöntem sunmuşlardır. Örtü görüntüsünün en fazla kullanabileceği sağ taraftaki en önemsiz bit adetini bulmak için genetik algoritmaya dayalı bir ön işlem yapmışlar ve piksellerin belirledikleri, kullanabilecekleri LSB değerlerine veri gizleme işlemlerini gerçekleştirmişlerdir. Çalışmalarını 8 bit gri seviyeli görüntülerde test etmişlerdir.

Zhou ve ark. (2001), meme mamografisi görüntüsüne hastaya ait hasta bilgilerinin gizlenmesi üzerine bir çalışma yapmışlardır. Çalışmalarında birinci adımda görüntüde ön işleme yaparak görüntü parçalara ayrılır ve DICOM (Digital Imaging and Communications in Medicine) görüntü başlığı içerisinden hasta bilgileri alınır. İkinci adım da MD5 özet algoritması kullanılıp görüntünün özet bir değeri hesaplanmaktadır. Bir sonraki adımda verinin şifrelenmesi yapılmaktadır. Son olarak da elde edilen şifrelenmiş veri görüntü içerisine en önemsiz biti (LSB) yer değiştirilerek veri gizleme işlemi gerçekleştirilmektedir. Geliştirdikleri yöntem sayesinde hastaya ait bilgilere sadece veri gizlemede kullanılan özel anahtarı bilen kullanıcıların erişebilmeleri sağlanmıştır ve veri gizleme işlemi sonucunda elde edilen görüntü ile orijinali arasında görüntü kalitesinde her hangi bir fark tespit edilememiştir.

Luo ve ark. (2003), e-tanı uygulamalarında kullanılmak üzere yaptıkları çalışmada tıbbi görüntüler ile bu görüntülere ait olan belgelerin bütünlüğünü sağlamak, ayrıca hastanın kişisel verilerinin korunması için bir yöntem önermişlerdir. Veri gizleme işleminde tıbbi görüntünün en önemsiz bitleri olan LSB_0, LSB_1, LSB_2, LSB_3 ve LSB_4 kullanmışlardır. Deneysel çalışmaları sonucunda LSB_{0-2} seçilerek yapılan veri gizleme işlemlerinde görüntülerin hepsinde meydana gelen bozulma insan gözü tarafından fark edilememiştir. Fakat, LSB_{0-3} ve LSB_{0-4} seçilerek yapılan veri gizleme işlemlerinde görüntülerde meydan gelen bozulmalar insan gözü tarafından algılanabilmiştir.

Srinivasan ve ark. (2004) tıbbi görüntülerde hasta bilgilerinin gizlenmesi için renkli görüntülere uygulanacak yeni bir veri gizleme yaklaşımı sunmuşlardır. Görüntüleri ilk önce bit düzlemi parçalarına ayırıp her bir bit düzlemi için 8×8 boyutunda bloklara ayırıp bu bloklardaki 1 ve 0 değerlerinin dağılımına göre karmaşıklık değeri hesaplamaktadırlar. Rastgele yaptıkları aramalar ile gizlemek istedikleri verilere uygun 8×8 boyutunda blokları bulup verilerini bu bloklara gizlemişlerdir. Gizleme işleminde görüntünün kırmızı, yeşil ve mavi renk kanallarının her birinin en önemsiz 3'er bitini kullanmışlardır.

Ji ve ark. (2006), örtü görüntüsünde gizleme yapılması için en uygun blok boyutunu bulan genetik algoritma tabanlı bir veri gizleme yöntemi geliştirmişlerdir. En uygun boyuttaki blokları arayıp belirlendikten sonra örtü görüntüsünün piksellerinin LSB değerleri değiştirilerek veri gizleme işlemi yapmışlardır. 512×512 boyutundaki gri seviyeli örtü görüntüsünü toplamda 6 bloktan 16384 bloğa kadar bölerek yaptıkları test işlemlerinde en iyi sonucu 4096 blokta elde etmişlerdir.

Wang ve Tsai (2007), görüntü içerisine başka bir görüntüyü gizledikleri çalışmalarında örtü görüntüsünü ve gizlenecek görüntüyü bloklara ayırıp bir biri ile en benzer bloğu bulmaya çalışmışlardır. Benzer blokları bulmak için k−means sınıflandırma algoritmasını kullanmışlardır. Veri gizleme işlemi yapılırken ise örtü görüntüsünün LSB değerini kullanmışlardır.

Li ve ark. (2007) çalışmalarında, mamografi görüntülerinde hasta bilgilerinin gizlenmesi ile ilgili yeni bir yöntem sunmuşlardır. Veri gizleme işlemi sırasında mamografi görüntüsünün detaylarında her hangi bir değişiklik yapılmamaktadır. Buna ek olarak tıbbi görüntüye kötü niyetli değişimler yapmak isteyenleri ve kanunsuz erişimleri engellemek adına damgalamada uygulamışlardır. Önerdikleri bu yöntemlerin mamografi görüntülerinin internet aracılığı ile iletimi ve görüntü arşivleme sistemlerinde saklanması için uyumlu olduğunu belirtmektedirler.

Fazli ve Kiamini (2008), gri seviyeli görüntüler üzerinde geliştirdikleri yöntemlerinde, örtü görüntüsünü 8×8 boyutunda bloklara ayırıp, gizli mesaj grupları için en uygun yerleri bulmaya çalışmışlardır. Bloklardaki en uygun yerlerin bulunmasında ise Parçacık Sürü Optimizasyonu (Particle Swarm Optimization − PSO) kullanmışlardır. Veri gizleme işlemlerini ise piksellerin LSB değerleri değiştirerek yapmışlardır.

Lou ve ark. (2009), çok katmanlı veri gizleme yöntemi üzerine çalışmışlardır. Yaptıkları çalışmalarında gri seviyeli görüntülere veri gizleme uygulamışlardır. Veri gizleme işlemi esnasında görüntünün en önemsiz bitini değiştirmişlerdir. En önemsiz bit değişimini ilk önce soldan sağa yatay tarama ile yapmışlar ve buna birinci katman

adını vermişlerdir. Sonra üstten alt tarafa doğru bir tarama ile veri gizleme işlemini sürdürerek bunu da ikinci katman olarak adlandırmışlardır. M×N boyutundaki görüntü için her bir katmana M×N/2 bit veri gizleme işlemi yapmışlardır.

Bourbakis ve ark. (2009) en önemsiz bit kullanılarak yaptıkları çalışmalarında, tıbbi görüntüler kullanmışlardır. Önerdikleri yöntemde kriptoloji ve steganografi tekniklerini birleştirerek veri gizlemeyle bilgi güvenliğini sağlamışlardır. Hem görüntüyü görüntü içerisine hem de metin bilgilerini görüntü içerisine gizlemişlerdir. Tıbbi görüntüye ait olan metin biçimindeki tanı ve tedavi bilgilerini görüntü içerisine gizlemeden önce iki boyutlu mesaja (görüntüye) dönüştürmüşlerdir. Bundan sonra veri gizleme işlemi gerçekleştirilmiştir. Veri gizleme işlemi sonrası örtü görüntüsü sıkıştırılmıştır.

Chhajed ve Shinde (2010) siyah beyaz görüntüleri sol üstten başlayıp 2×2, 3×3 vb. boyutunda bloklara ayırıp bilgileri bu bloklara gizlemişlerdir. Gizleme işlemi yapılırken gizlenecek verilerin, ayırdıkları bloklarla eşleşmesine dikkat etmişlerdir. Bu bloklardaki gizlenen mesajlara ait gizli mesaj uzunluğu, blok boyutu ve blok konumu bilgilerini ise görüntülerin sağ alt tarafından başlayıp 3×3 boyutundaki bloklara gizlemişlerdir.

Nergui ve ark. (2010), metin olan hasta bilgilerinin tıbbi görüntülere gizlenmesi ile ilgili çalışma yapmışlardır. Hastaya ait bilgi ilk önce 128 bit uzunluğundaki anahtar ile AES algoritmasına göre şifrelenmiştir. Tıbbi görüntü içerisine şifrelenen veri gizleme işlemi, geliştirdikleri hata kontrol kodlaması ile gerçekleştirilmiştir.

Martiri ve ark. (2011), sağlık alanında kullanılan görüntü bilgi sistemlerinde kullanılmak üzere yeni bir veri gizleme yöntemi önermişlerdir. Önerdikleri yaklaşımda hasta adı, hastaya ait tıbbi görüntü adı, görüntü kaynağı tipi, sağlık merkezi adı ve tarih bilgileri birleştirilip, bunlardan bir anahtar oluşturulmuştur. Bu bilgilerin şifrelenmesinden sonra bilgiler görüntü içerisine en önemsiz biti kullanılarak gizlenmiştir. Gizleme işlemi bittikten sonra görüntüyü veri tabanına kaydetmektedirler.

Kao ve ark. (2011), mamografi görüntüleri içerisine veri gizleme çalışması yapmışlardır. Mamografi görüntüsü içerisine görüntünün oluşturulma tarihi ve saati, görüntünün elde edildiği cihaz adı, görüntü tipi, hasta bilgisi, doktor bilgisi, hastalık tipi ve tedavi şekli bilgilerine gizleme işleminden önce ADAPT adı verdikleri 26 karakterlik özel bir mesajı ekleyip bu yeni bilginin özetini çıkartmışlardır. Tıbbi veri ve üretmiş oldukları ADAPT bilgisini görüntü içerisine en önemsiz bit kullanılarak gizlemişlerdir.

Pandey ve ark. (2012) tıbbi görüntülerin güvenli iletimi için sundukları yöntemlerinde tıbbi görüntünün korunması için şifreleme ve steganografi yöntemlerini birleştirmişlerdir. İlk olarak orijinal tıbbi görüntü, şifreleme algoritması ile şifrelenmektedir. Şifrelenen görüntüye hasta bilgileri özel bir anahtar üretilerek gizlenmektedir. Şifrelenen ve veri gizlenen görüntü bir alıcıya yollandığında eğer alıcıda anahtar yok ise alıcı görüntü içerisindeki bilgilere ulaşamamaktadır. Pandey ve Shrivastava (2012), bir sonraki çalışmalarında yine tıbbi görüntülerin korunması için şifreleme ve steganografi yöntemlerini birleştirmişlerdir. Bu çalışmalarında ise veri gizlemede en önemsiz bit kullanılarak veri gizleme yapmışlardır.

Liu ve ark. (2013), çalışmalarında piksellerin sayısal değerlerinin farklarına dayalı (Pixel Value Difference-PVD) veri gizleme yöntemi geliştirmişlerdir. PVD tabanlı veri gizleme metotlarında veri gizleme işlemi esnasında piksellere uygulanacak gezintide ızgara (raster) tarama sırası veya zikzak (zig-zag) tarama sırası kullanılmaktadır. Bu çalışmada ise raster ve zig-zag tarama sıraları yerine piksellerdeki gezinti için hilbert eğrisi tarama sırası olarak kullanılmıştır.

Prabakaran ve ark. (2013), geliştirdikleri steganografi metodu ile Manyetik Rezonans (MR) görüntüleme ile elde edilen görüntüleri başka bir görüntü içerisine gizlemişlerdir. Bu yöntemi uygulamak için iki adet görüntüye ihtiyaç vardır. Birincisi örtü görüntüsü diğeri ise hastaya ait olan tanının olduğu görüntüdür. Örtü görüntüsü tıbbi görüntü veya normal bir görüntü olabilir. Veri gizleme işlemi yapılmadan önce hastaya ait tanıyı içeren MR görüntüsüne Arnold dönüşümü uygulanmış ve gizleme işlemi gerçekleştirilmiştir.

Lavania ve ark. (2014), renkli görüntülerde kullanılmak üzere bir steganografi yöntemi kullanmışlardır. Veri gizleme işlemini frekans düzleminde en önemsiz bit kullanarak yapmışlardır. Görüntüye uygulayacakları gizleme işleminde sadece kırmızı renk kanalını kullanmışlardır.

Taghipour ve ark. (2014), tıbbi görüntü olan patoloji görüntülerine hasta bilgisini, mikroskobik tanımlamayı ve tanısını içeren patoloji raporlarını gizlemek için bir yöntem sunmuşlardır. Önerdikleri veri gizleme yöntemini tıbbi görüntülere uyguladıklarında 0,8 bpp (Bit Per Pixel) veri gömme kapasitesi için PSNR değeri 30 dB'den büyük hesaplanmıştır. 1 bpp veri gömme kapasitesi için ise bu değer 30 dB'den küçük hesaplanmıştır.

Umeda ve ark. (2014), tıbbi görüntülerin iletimi sırasındaki güvenlik riskini azaltmak için yaptıkları çalışmada bilgisayarlı tomografi (Computed Tomography-CT) görüntülerini kullanmışlardır. En önemsiz son iki bit (LSB_0 ve LSB_1) düzlemine yaptıkları veri gizleme sonucunda SSIM görüntü kalite ölçütünü 0,99 dB olarak hesaplamışlardır.

Al-Dmour ve ark. (2014), çalışmalarında tıbbi görüntülere hasta bilgilerini saklamak için yeni bir steganografi yöntemi sunmuşlardır. Örtü görüntüsünün kalitesini yüksek tutmak için görüntüdeki detayların önemli olduğu alana veri gizleme yapılmamıştır. Bu alana ait olan koordinatlar örtü görüntüsünün son satırında saklanmıştır. Bu alanlar dışında kalan piksellerde veri gizleme yapılacak yerleri belirlemek için görüntünün keskin karşıtlık (kontrast) içeren alanlarının bulunduğu pikseller seçilmektedir. Bu seçme işlemi yapılırken piksel değerleri farkını (Pixel Value Difference-PVD) kullanmışlardır. Gizleme esnasında piksellerin son 2 biti kullanılmıştır. Hamming kodlaması kullanarak gizli veriye ait olan 3 bit, örtü görüntüsünün 4 bitine gizlenmiştir. Literatürdeki diğer çalışmalardan bu çalışmayı ayıran en önemli özelliği veri gizlemenin yapılmayacağı alanın belirlenmesidir.

Karakış ve ark. (2015), tıbbi veri güvenliği için bulanık mantık tabanlı görüntü steganografi yöntemi sunmuşlardır. Yöntemlerinde veri gizlemeyi en önemsiz bite

yapmışlardır. Gizlenecek piksellerin seçiminde ise bulanık mantık tabanlı ve benzerliğe dayalı geliştirdikleri algoritmalarını kullanmışlardır. Veri gizlemede kullanılan piksellerin sıralı olmadığını belirtmişlerdir. Manyetik Rezonans (MR) görüntüleri içerisine hastaya ait bilgiler, hastaya ait Elektroensafolagram (EEG) sinyali ve doktor yorumundan oluşan bilgileri gizlemişlerdir. Örtü görüntüsüne gerçekleştirilecek saldırılara karşı, verilere Huffman ve LZW (Lempel Ziv Welch) kayıpsız sıkıştırma metotları ve 128 bit anahtarlı Rijndael simetrik şifreleme algoritması uygulanmıştır.

Mantos ve Maglogiannis (2016), internet aracılığı ile paylaşılan tıbbi görüntüler ve bulut bilişim sistemlerinde depolanan tıbbi görüntülerin güvenliği için bir steganografi yöntemi önermişlerdir. Yöntemlerinde DICOM görüntüler kullanılmış, DICOM görüntü başlık bilgisindeki hastaya ait olan bilgiler şifrelenerek görüntünün en önemsiz bitlerine veriler gizlenmiştir.

Literatür özetleri incelendiğinde görüntüler üzerinde verilerin gizlenmesi ile ilgili birçok çalışma olduğu görülmektedir. Bu çalışmalarda geliştirilen yöntemlerin birçoğunun gri seviyeli görüntüler için olduğu fark edilmektedir. Tıbbi görüntüler ile yapılan çalışmalarda ise veri gizleme işlemlerinde hastaya ait olan metin içerikli bilgilerin gizlenmesi yapılmıştır. Bu tez çalışmasında geliştirilen algoritma ile hem renkli görüntüler hem de gri seviyeli görüntüler kullanılabilmektedir. Ayrıca gerek metin bilgileri gerekse görüntü üzerine yapılan geometrik şekilsel işaretlemeler görüntüye gizlenebilmektedir.

1.2. Tez Çalışmasının Amacı ve Hedefleri

Teknolojinin ilerlemesi internet kullanımının yaygınlaşmasıyla hayatımızın birçok alanına yenilikler girmiş ve bu yeniliklerin sunduğu birçok avantajlar vardır. Sunmuş olduğu en önemli avantaj ise hayatımızın her alanında yapılan işlerin kolaylaştırmasıdır. Örneğin dijital fotoğraf makineleri veya cep telefonları ile yüksek kalitede görüntü elde edebilir, bunları bilgisayara yükleyip saklayabilir, üzerinde değişiklikler yapabilir ve bilgisayarımız bir ağa bağlıysa verilerimizi istediğimiz kişi

veya kişilere yollayıp bizim için özel olan bu verileri paylaşabiliriz. Bu noktada öne çıkan, kolay bir yolla elde ettiğimiz ve paylaşabildiğimiz kişisel bilgilerimizin güvenliği ve bu bilgilerin içeriğinin gizli kalabilmesidir. Bize ait olan kendi bilgisayarımızdaki bilgilere veya çeşitli kurumlarda bizden elde edilen özel bilgilerimize ulaşmak isteyen, izni ve yetkisi olmayan kişilere karşı bir önlem yöntemi olarak, verilerin fark edilmeyecek biçimde gizlenmesi önemli bir araştırma konusu haline gelmiştir.

Bu tez çalışmasında, bir örtü görüntüsü üzerinde en az değişimi yaparak görüntü kalitesini en üst seviyede tutacak ve böylece gizli verinin fark edilmesi güçleştirecek, blok eşleştirme ve LSB tabanlı yeni bir veri gizleme algoritması tasarlanması amaçlanmıştır.

Tasarlanan algoritma ile sağlık kurumlarında hastalardan elde edilen tıbbi görüntülere; hasta adı, hastalık teşhisi, tıbbi görüntüye ait geometrik şekilsel işaretlemeleri içeren doktor raporunun bir bütün halinde gizlenebileceği bir uygulama geliştirilmiştir.

Bu tez çalışması amaçları doğrultusunda aşağıdaki hedefler belirlenmiştir:

1. Veri gizleme işlemi için yeni bir LSB tabanlı algoritma geliştirmek,
2. Geliştirilecek veri gizleme algoritmasında, gizlenecek veri ile örtü görüntüsünün piksellerinden en benzer olan piksellerinin bulunmasını sağlamak,
3. Literatürde yapılan veri gizleme yöntemlerine kıyasla örtü görüntüsünde oluşan bozulma seviyesini en aza indirmek ve bu sayede örtü görüntüsü üzerinde en az değişim/bozulma yapılarak stego görüntüde yüksek kalite sağlamak,
4. Görüntüye metin bilgilerine ek, görüntü üzerinde yapılan geometrik şekilsel işaretlemeler ve bu şekillere ait bilgilerin gizlenebilmesi için bir uygulama yazılımı geliştirmektir.

1.3. Tez Çalışmasının Katkıları

Bu tez çalışmasında tasarlanan algoritmanın klasik LSB ve literatürdeki LSB tabanlı diğer veri gizleme çalışmalarına göre istatistiksel açıdan ve içerisindeki verinin fark edilememesi ile ilgili değerlendirme sonuçlarının başarılı olduğu görülmektedir. Bu tez çalışmasının katkıları aşağıdaki gibidir;

1. Blok eşleştirme ve tarama sırası seçimli, görüntü üzerinde en az değişimi yapan ve steganaliz ataklarına karşı dayanıklı yeni bir LSB tabanlı veri gizleme algoritması tasarlanması,
2. Tasarlanan algoritmanın hem renkli veya gri seviyeli hem de tıbbi görüntülere uygulanması,
3. Tasarlanan algoritmanın başarımının Ortalama Karesel Hata (Mean Square Error − MSE), Tepe Sinyal Gürültü Oranı (Peak Signal Noise Rate − PSNR) Evrensel Görüntü Kalite İndeksi (Universal Image Quality Index − UQI), Ortalama Yapısal Benzerlik (Mean Structural Similarity − M-SSIM), Renkli Görüntü Kalite Ölçütü (Color Image Quality Measure − CQM), Ortalama Fark (Average Difference − AD), Yapısal İçerik (Structural Content – SC), Normalize Karşıt Korelasyon (Normalized Cross Correlation – NCC) ve Normalize Mutlak Hata (Normalized Absolute Error – NAE) metrikleri ile değerlendirilmesi,
4. Diğer yöntemler sadece metin içerikli sağlık kurumu adı, tarih, görüntünün elde edildiği cihaz adı, görüntü tipi, hasta bilgisi, doktor bilgisi, hastalık tipi ve tedavi bilgilerini veri gizlemede kullanırken, bu çalışma ile başta hasta adı, hastalık teşhisi gibi metin içerikli bilgiler yanında tıbbi görüntüye ait geometrik şekilsel işaretlemeler ve bu şekillere ait bilgileri içeren doktor raporunu bir bütün halinde gizlenebileceği bir uygulama geliştirilmesi.

1.4. Tez Organizasyonu

Bu tez çalışmasında geliştirilen veri gizleme ve verinin tekrar elde edilmesi yöntemleri, aşağıdaki organizasyon yapısında anlatılmaktadır.

Bölüm 2’de, sayısal görüntü işleme ile ilgili temel kavram ve veri gizleme hakkında genel bilgiler verilmektedir. Bu tez çalışmasında kullanılan LSB tabanlı veri gizleme ile ilgili bilgiler bu bölümde sunulmaktadır.

Bölüm 3’de, RGB görüntüler ve gri seviyeli görüntüler için geliştirilmiş olan veri gizleme algoritmasının aşamaları olan örtü görüntüsünde gizlenecek en uygun piksel bloklarının bulunması, verinin bu bloklara gizlenmesi ve gizlenen verinin tekrar elde edilmesi hakkında bilgiler verilmektedir.

Bölüm 4’de, geliştirilen veri gizleme algoritmasının başarım değerlendirmesi sunulmaktadır. Burada örtü görüntüsünün piksellerinde ve bitlerinde meydana gelen bozulma/değişim sayısı, stego görüntüsünün görüntü kalitesinin değerlendirilmesi ve stego görüntüsünün steganaliz ataklara karşı performansı test edilmiştir.

Bölüm 5’de, geliştirilen yeni veri gizleme algoritmasının, yapılan deneysel hesaplamalardan elde edilen sonuçları değerlendirilerek, sunmuş olduğu katkılar ifade edilmektedir. Buna ek olarak, bu çalışmanın devamı niteliğinde yapılabilecek yeni çalışmalar hakkında öneriler verilmektedir.

BÖLÜM 2. SAYISAL GÖRÜNTÜ İŞLEME VE VERİ GİZLEMENİN TEMELLERİ

2.1. Giriş

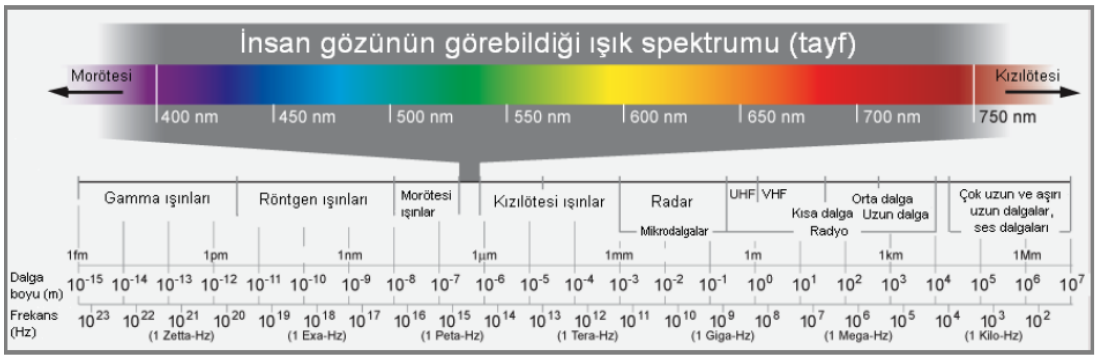
Bilişim teknolojileri alanında yaşanan gelişimin hızlı olmasına bağlı olarak sayısal verilerin elde edilmesi, depolanması ve bu veriler üzerinde yapılan işlem sayısı da gün geçtikçe artmıştır. Bilişim teknolojilerinde elektronik/sayısal olarak elde edilen verilerin büyük bir çoğunluğunu görüntüler oluşturmaktadır. Görüntü elde etmede kullanılan mobil cihazların ve fotoğraf makinalarının teknolojik gelişimi ve kullanımının yaygınlaşmasıyla analog görüntülerin yerini sayısal görüntüler almıştır. Buna ek olarak internetin yaygın olarak kullanımı, kolay elde edilen ve saklanabilen sayısal görüntünün, paylaşımını da kolay hale getirmiştir.

Bu bölümde görüntülerin elektronik ortamlara aktarılmasına ilişkin detaylar verilmektedir. Ayrıca veri gizleme başlığı altında yer alan şifreleme (kriptoloji), damgalama (watermarking) ve steganografi üzerinde durularak bilgi güvenliğindeki rolleri, birbirlerine olan üstünlükleri ve farklılıkları vurgulanmaktadır. Tez çalışmasının temelini oluşturan renkli ve gri seviyeli görüntülere steganografi yönteminin uygulanma amacı ele alınmaktadır.

2.2. Renk ve Renk Modelleri

Elektromanyetik dalgaların insan gözü tarafından algılanabilen bölümüne görülebilir tayf, görülebilir ışık veya sadece ışık denir. Cisimler tarafından yansıtılan bu ışığın gözde oluşturduğu algılama renk olarak tanımlanır. Görülebilir ışığın en küçük dalga boyunu mor renk (350 nm) ve en büyük dalga boyunu kırmızı renk (780 nm) oluşturmaktadır. Şekil 2.1.'de verilen elektromanyetik tayfta görüldüğü üzere

görülebilir ışık, mor ötesi (ultraviyole) ve kızıl ötesi (infrared) ışınlar arasındadır (Yılmaz ve ark., 2002).



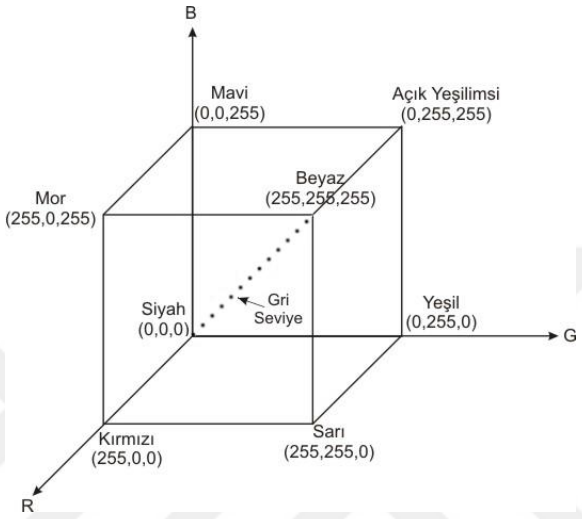
Şekil 2.1. Elektromanyetik tayf (Kuzay, 2014).

Görülebilir ışıkta yer alan ışınların gözde oluşturdukları renkleri tanımlamak için matematiksel modeller kullanılmaktadır. Bunlar renk modeli veya renk uzayı olarak adlandırılmaktadır. Renk modelleri bütün renkleri temsil edecek biçimde oluşturulmaktadır ve renk modellerinin her birinin kendine özgü olarak renk oluşturmak için bazı standartları vardır. Renkmetri biliminin temelini oluşturan Grassman'ın kuralına göre renkleri belirlemek için birbirinden bağımsız 3 adet değişkene ihtiyaç vardır ve bundan dolayı renk modelleri 3 boyutlu olarak tasarlanmaktadırlar. En çok kullanılan renk modellerine örnek olarak; bilgisayar grafiklerinde kullanılan RGB, renkli baskı sistemlerinde kullanılan CMYK ve video sistemlerinde kullanılan YCbCr verilebilir. Bunlara ek olarak HSI, HLS, HSV, YUV ve YIQ olarak adlandırılan renk modelleri de kullanılmaktadır (Yılmaz, 2002). Bu tez çalışmasında yapılan veri gizleme işlemleri RGB renk modeli kullanılarak gerçekleştirilmiştir.

2.2.1. RGB renk modeli

RGB renk modelinde ana renkler yani birincil renkler olarak ifade edilen kırmızı (Red), yeşil (Green) ve mavinin (Blue) farklı oranlarda karıştırılmasıyla diğer renkler oluşmaktadır. Bu karışımda birincil renklerin her birinin alacağı en küçük değer 0 en büyük değer ise 255'dir. Birincil renklerin karışımından olan diğer renklerin bazıları Şekil 2.2.'de görülen kartezyen koordinat sisteminde renkli görüntü modelinde

görülmektedir. Başlangıç noktası (0,0,0) siyah, renklerin değerlerinin (255,255,255) olduğu yer beyaz olacaktır. En az iki rengin bir araya gelmesi ile de morun tonu olan eflatun (Magenta), açık yeşilimsi-camgöbeği- (Cyan) ve sarı (Yellow) renkler yani ikincil renkler oluşmaktadır. Bu renk modeli genellikle televizyon ve bilgisayar ekranı gibi göstergelerde kullanılır (Tüzün ve Akan, 2005; Karakuş, 2006).



Şekil 2.2. Renklerin 3 boyutlu uzayda gösterimi (Tüzün ve Akan, 2005; Karakuş, 2006).

RGB renk modeli monitörlerde istenilen rengi oluşturmak için kırmızı, yeşil ve mavi rengi kullanmalarından dolayı bilgisayar grafikleri için en uygun renk modelidir. RGB renk modelinin seçilmesi sistemin tasarımı ve mimarisini basitleştirmektedir (Taşkın, 2007).

2.2.2. CMYK, HSI, HLS, HSV, YUV renk modelleri

CMYK, RGB renk modelinde birincil renklerin birleşmesinde oluşan ikincil renkleri ana renk olarak kullanan renk modelidir. Camgöbeği (Cyan), eflatun (Magenta), sarı (Yellow) ve siyah (Black) renkleri bu renk modelinde ana renk olarak kullanılır. Bu renk modeli baskı alanında kullanılmaktadır (Nishad ve Chezian, 2013).

İnsanın sezgisel olarak ve daha kolay renk seçimi yapabilmesi amacıyla HSI (Hue − Saturation – Intensitiy = Renk tonu – Doygunluk – Yoğunluk) ve HSV (Hue − Saturation – Value = Renk tonu – Doygunluk – Parlaklık) renk modelleri

geliştirilmiştir. Gündelik işler esnasında kişilerin renkleri görerek seçmeleri gerektiği durumlarda ve renklerin kişilere el ile gösterilmesi gerektiğinde bu modellerin kullanımı idealdir. HSI ve HLS (Hue − Lightness − Saturation = Renk tonu – Parlaklık – Yoğunluk) birbirine çok benzemektedir. Yoğunluk bileşeni I yerine parlaklık bileşeni L kullanılmıştır. Büyük bir dinamik aralığa sahip olan HSV renk modeli renkleri değiştirme ya da renk yoğunluğu ayarlamada kullanılmaktadır. Parlaklık değerleri ile doğrudan alakalı katsayı, eşitleme, histogram gibi geleneksel resim işleme metotları için de HSI renk modeli tercih edilmektedir (Taşkın, 2007).

YUV renk modelinde Y bileşeni parlaklık/ışıklık (luminance, luma) değerini, U bileşeni renklilik (chrominance1) değerini ve V bileşeni de yine renklilik (chrominance2) değerini ifade etmektedir. Bu renk modeli PAL (Phase Alternate Line), NTSC (National Television Standards Committee), SECAM (Système Electronique Couleur Avec Mémoire) bileşik ve renkli analog video standartlarında kullanılmaktadır (Taşkın, 2007).

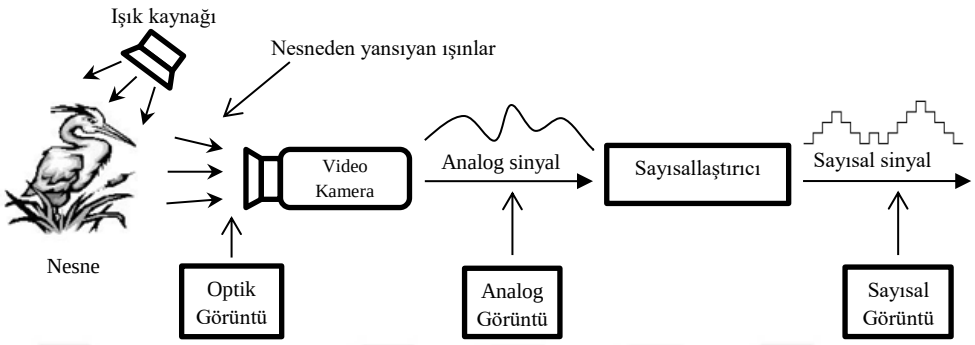
Renk modellerin uygulamalardaki kullanım alanlarının farklı olması nedeni ile sayısal ortamda renk modelleri arasında dönüşüm matematiksel formüller ile gerçekleştirilir.

2.3. Sayısal Görüntü

Bir nesnenin merceğe ya da göze yansıyan şekline görüntü denir. Bir görüntü iki boyutlu f(x,y) fonksiyonu olarak tanımlanabilir. Burada x ve y uzamsal düzlem koordinatlarını temsil etmektedir. f fonksiyonun herhangi bir (x,y) koordinatındaki genliği görüntünün o noktadaki gri seviyesi veya yoğunluğu olarak adlandırılır. x, y ve f'nin genlik değerleri hep birlikte sonlu ve ayrık büyüklükte olduğunda görüntü sayısal görüntü olarak adlandırılır (Gonzalez ve Woods, 2002).

Bir görüntüyü bilgisayar ortamına aktarabilmek için geçen aşamalar Şekil 2.3.'de gösterilmektedir. Işık kaynağı ile aydınlatılan nesneden yansıyan ışınlar optik formda kameraya aktarılır. Nesneyi temsil eden bu ışınlar, kamerada elektrik sinyallerine

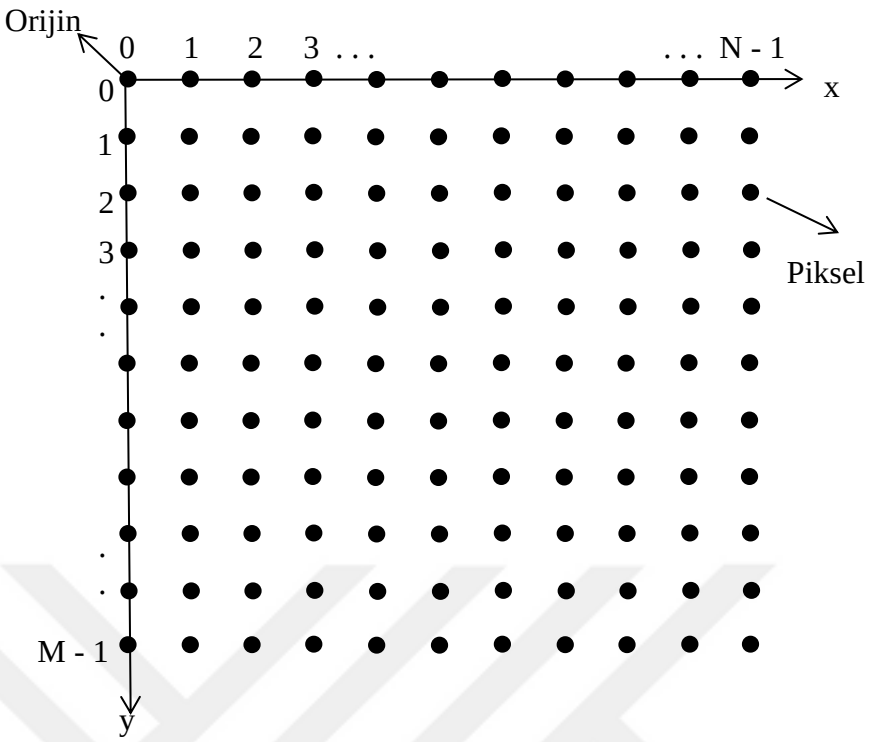
dönüştürülür ve görüntü analog forma dönüşmüş olur. Analog sinyaller sayısal dönüştürücü kullanılarak sayısal sinyallere çevrilir. Böylece görüntü artık bilgisayar ortamına aktarılacak hale getirilmiştir (Yaman ve ark., 2001).



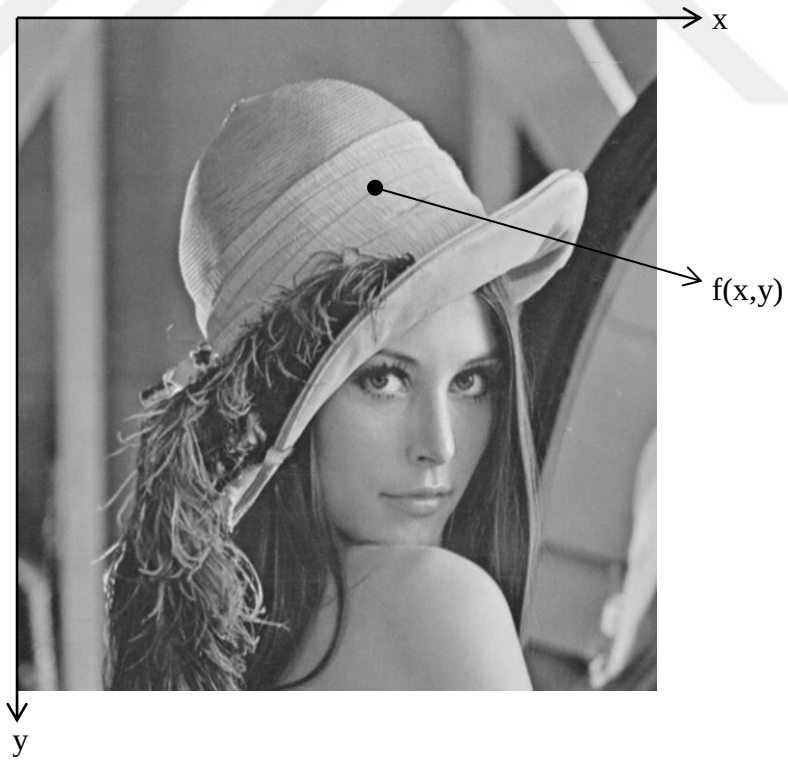
Şekil 2.3. Görüntünün sayısallaştırılması (Yaman ve ark., 2001).

Sayısal görüntünün sonlu olan belirli bir nokta ve değere sahip her bir bileşenine resim elemanı, görüntü elemanı, pels veya piksel denir (Gonzalez ve Woods, 2002). Şekil 2.4.'de görüldüğü gibi sayısal görüntü noktalarla ifade edilen piksellerden oluşur. Görüntünün sol üst köşesi olan orijin, piksellerin x ve y doğrultusunun başladığı referans noktadır. Piksellerin görüntü içerisindeki konumu x ve y sıra numarasına göre (x,y) tanımlanır. Orijin (0,0) konumundadır. Bu konuma iki boyutlu düzlemde koordinat da denir. Bir pikselin koordinatı matematiksel olarak f(x,y) biçiminde ifade edilir. Denklem 2.1.'de sayısal görüntü modelinin matematiksel gösterimi görülmektedir. Şekil 2.5.'de bir sayısal görüntü üzerinde örnek bir pikselin yeri f(x,y) gösterilmiştir. (Kurtulmuş, 2012).

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix} \qquad (2.1)$$



Şekil 2.4. Sayısal görüntü gösterim modeli



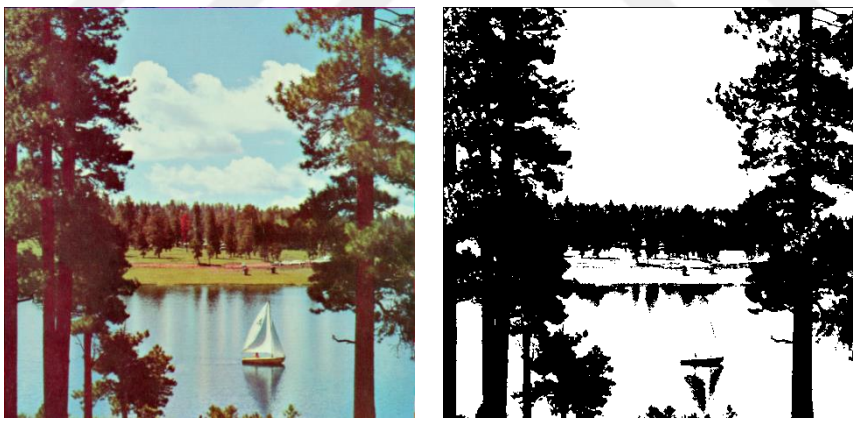
Şekil 2.5. Örnek bir sayısal görüntü

2.3.1. Görüntü türleri

Sayısal görüntü ikili görüntü, gri seviyeli görüntü ve renkli görüntü biçiminde oluşturulup kullanılabilmektedir.

2.3.1.1. İkili görüntü (Binary image)

Sayısal görüntüyü oluşturan ve piksel olarak ifade edilen her bir bileşeninin alacağı değerler sadece 1 ve 0 olması durumunda bu görüntülere ikili (binary) görüntü denir. Piksellerin alacağı 1 ve 0 değerleri sırasıyla aydınlık ve karanlığı, nesne ve zemini veya başka bir ifadeyle beyaz ve siyah bölgeleri temsil etmektedirler. Görüntü işleme uygulamalarında maskeleme işlemlerinde hedef bölge pikselleri 1 diğer pikseller 0 yapılarak ikilileştirme (binarization) yoluyla, gri seviyeli görüntülerin yoğunluk değerlerinde ya da renkli görüntülerin farklı renk kanallarının değerlerinde eşikleme (thresholding) yapılarak ikili görüntüler elde edilebilmektedir (Şahin, 2007; Yalman ve Ertürk 2009; Kurtulmuş, 2012). Şekil 2.6.'da ikili görüntü örneği görülmektedir.



a) b)

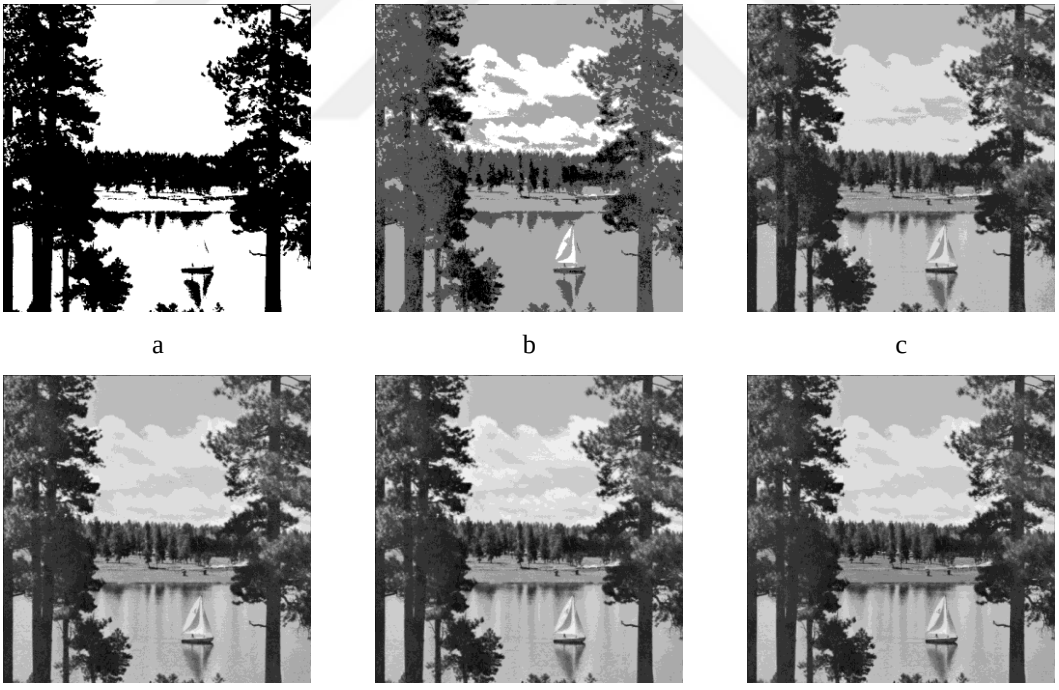
Şekil 2.6. İkili görüntü örneği a) renkli görüntü, b) renkli görüntünün ikili görüntüsü

2.3.1.2. Gri seviyeli görüntü (Gray scale/level image)

Gri seviyeli görüntü olarak adlandırılan görüntülerde her bir pikselinin alacağı 256 farklı değer -gri seviyesi veya parlaklık değeri- vardır ve bu değerler 0 ile 255 arasında olmaktadır. En parlak piksel 255 değerindedir ve beyaz olarak ifade edilir.

En karanlık piksel ise 0 değeriyle siyah olarak temsil edilir. Böylece her pikselin değerinin farklı olması ile gri tonda bir görüntü elde edilir. Pikselin alabileceği 0-255 arasındaki değerler bit olarak ifade edilirse bir pikselin değerini belirleyebilmek için her piksel başına (bit per piksel – bpp) 1, 2, 3, 4, 6 ya da 8 bit kullanılabilir. Böylece bir pikselde olabilecek gri seviye değerleri 2^1, 2^2, 2^3, 2^4, 2^6 ya da 2^8 olarak belirlenir ve sırasıyla 2, 4, 8, 16, 64 ya da 256 farklı değere eşittir (Akar, 2009). Şekil 2.7.'de bit değeri (derinliği) 1 bpp, 2 bpp, 3 bpp, 4 bpp, 6 bpp ve 8 bpp olan görüntüler verilmektedir. Bit derinliği 1 bpp olduğunda pikseller 2 farklı gri seviye ile ifade edilecektir ve bu değerler 1 ile 0'dır. Bu tip görüntülere yukarıda bahsedildiği üzere ikili görüntü denir.

Görüntüyü ifade eden bit derinliği ne kadar az olursa ilgili sayısal görüntünün depolama biriminde kapladığı alan o oranda azalacaktır ve bellekte de o kadar az yer kaplayacaktır (Yalman, 2010).



Şekil 2.7. Gri seviyeli görüntü örnekleri. a) 1bpp 2 gri seviyeli, b) 2 bpp 4 gri seviyeli, c) 3 bpp 8 gri seviyeli, d) 4 bpp 16 gri seviyeli, e) 6 bpp 64 gri seviyeli, f) 8 bpp 256 gri seviyeli

2.3.1.3. Renkli görüntü (Color image)

Renkli görüntülerde her bir pikselin renk değeri 3 rengin karışımı sonucu elde edilir. Bu renkler birincil renkler olarak ifade edilen kırmızı (Red), yeşil (Green) ve mavinin (Blue) farklı oranlarda karıştırılmasıyla oluşmaktadır. Renkli görüntüler 16 bit (16 bpp), 24 bit (24 bpp) ve 32 bit (32 bpp) veriler olarak oluşturulabilirler. 16 bit'lik görüntüler yüksek renkli görüntü olarak isimlendirilirler ve pikseldeki renk dağılımı; kırmızı renk için 5 bit, yeşil renk için 6 bit ve mavi renk için 5 bit olarak belirlenmiştir. İnsan gözünün yeşil renklerdeki hataları diğer iki renkteki hatalardan daha çok fark edebilmesinden dolayı yeşil renkteki bit değeri diğer renklere göre fazla belirlenmiştir. Gerçek renk (true color) olarak ifade edilen görüntüler sayısal olarak 24 bit'lik (24 bpp) veriler olarak oluşturulurlar. Yani her bir piksel 8'er bitlik (1 bayt) kırmızı, yeşil ve mavi renk değerleri karışımıdır. Bu sayede 16777216 adet farklı renk elde edilebilmektedir. Bir piksel hafızada 3 bayt alana ihtiyaç duymaktadır ve bu standart haline gelmiştir. Bu karışımda birincil renklerin her birinin alacağı en küçük değer 0 en büyük değer ise 255'dir. 32 bit kullanılan renkli görüntüler de fazlalık olan 8 bit ise ışık geçirmezlik değerini ifade eden saydamlığı (opaklık) belirlemek için kullanılır (Karakuş, 2006; Çetin ve ark., 2012). Tablo 2.1.'de renkli görüntü elde edilirken piksellerin alacağı renk değerlerinden bazıları verilmiştir.

Tablo 2.1. Renkli resimdeki piksellerin alacağı renk değerlerinin karışım oranları

Renk adı	Kırmızı renk değeri	Yeşil renk değeri	Mavi renk değeri	Rengin algılanması
Siyah	0	0	0	
Koyu yeşil	0	128	0	
Gri	128	128	128	
Kahverengi	150	75	0	
Turuncu	255	127	0	
Camgöbeği	0	255	255	
Fuşya	255	0	255	
Sarı	255	255	0	
Beyaz	255	255	255	

2.4. Çözünürlük Kavramı

Çözünürlük, sayısal görüntünün sakladığı detaylar ölçüsüdür. Yani sayısal görüntüyü oluşturan piksel sayısı çözünürlüğü oluşturmaktadır (Kurtulmuş, 2012). Örneğin bir görüntü 448×336 çözünürlüğüne sahip ise; bu görüntü alanının yatay olarak 448 piksel, dikey olarak 336 piksel kullanılıp, toplamda 448×336=150528 pikselden oluşturulduğu söylenebilir. Eğer bir sayısal görüntünün çözünürlüğü ne kadar fazla ise ifade ettiği gerçekte ki görüntüsüne o kadar benzer bir görüntüdedir denebilir. Başka bir deyişle çözünürlüğün artmasıyla görüntünün netliği de artmaktadır.

Sayısal görüntünün çözünürlüğü arttıkça hafıza da kapladığı yer yani dosya boyutu da artmaktadır. Denklem 2.2.' de sayısal görüntünün dosya boyutunun hesaplanması verilmiştir.

Dosya boyutu = (yatay piksel sayısı × dikey piksel sayısı × renk derinliği) / 8 (2.2)

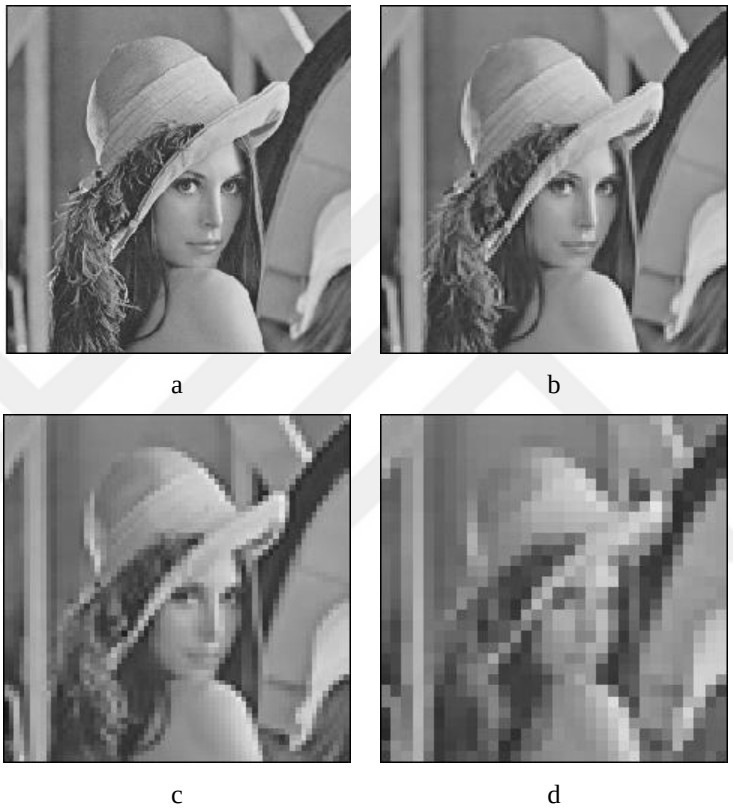
Denklem 2.2. kullanılarak elde edilen bazı görüntülere ait dosya boyutu Tablo 2.2.'de hesaplanmıştır.

Tablo 2.2. Sayısal görüntü dosya boyutları

Görüntünün piksel sayısı	Renk derinliği (8 bpp)	Görüntü dosyasının boyutu (bayt)
128×128	8	16384
128×128	16	32768
128×128	24	49152
256×256	8	65536
256×256	16	131072
256×256	24	196608
512×512	8	262144
512×512	16	524288
512×512	24	786432

Bir sayısal görüntüde örnekleme, her bir inç başına düşen nokta (DPI − Dot Per Inch) sayısı veya her bir inç başına düşen piksel (PPI − Piksel Per Inch) sayısı ile ifade

edilir. Sayısal görüntünün örnekleme frekansının arttırılması ile çözünürlüğü de arttırılır. 1 inç (2,54 cm) uzunluğundaki bölgenin kaç noktadan meydana geldiğini gösteren DPI, sayısal görüntülerde çözünürlüğü ifade etmek için kullanılana bir ölçektir. Örneğin, bir görüntünün çözünürlüğü 256×256 dpi ise bu görüntünün eni ve boyu her inç başına 256 noktadan oluşmaktadır (Yalman, 2010). Şekil 2.8.'de farklı boyuttaki görüntülerin farklı DPI değerindeki etkisi görülmektedir.



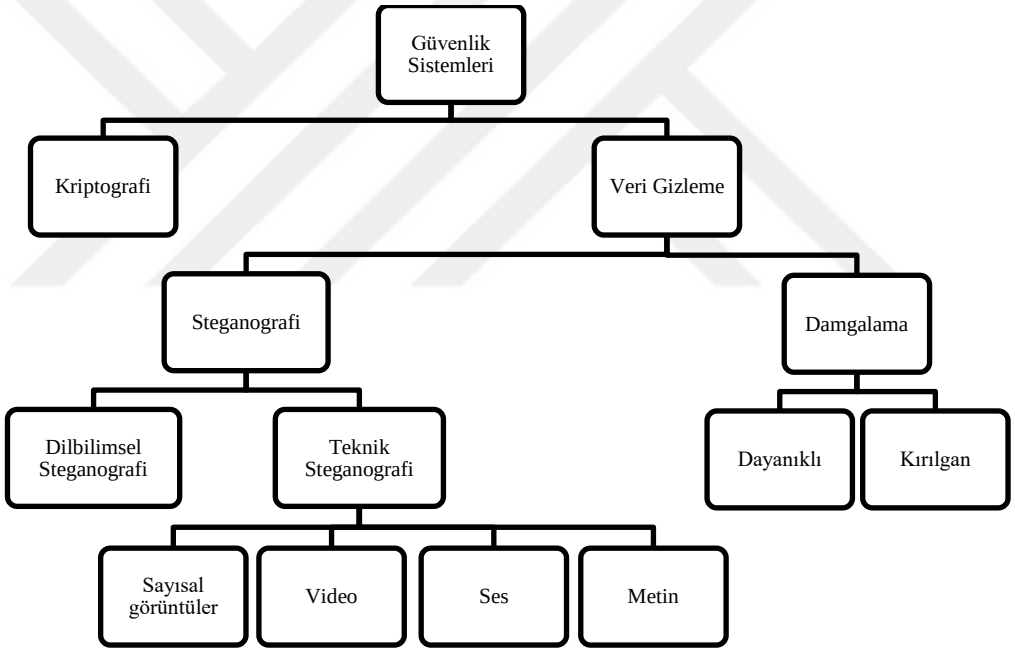
Şekil 2.8. DPI değerinin çözünürlük üzerindeki etkisi a) 256×256 72 dpi b) 128×128 36 dpi c) 64×64 18 dpi d) 32×32 9 dpi

2.5. Veri Gizleme Bilimi

Eski Yunan ve Roma uygarlıklarının gelişip yayıldığı antik çağlardan günümüze kadar insanoğlu gizli haberleşmeye ihtiyaç duymuştur. İnsanoğlu bu süre içerisinde kullandığı gizli haberleşmenin şekli ve yöntemi teknolojinin değişimi ve gelişimiyle farklılıklar göstermiştir. İletişim cihazlarının oldukça çeşitli olduğu ve birbiriyle çok kolay haberleştiği bu günlerde ise gizli haberleşme önemini iletişim alanında arttırarak korumuştur. Gizli iletişimin yapılması gereken uygulamalarda; gizlenmek

istenilen bilginin üçüncü şahısların eline geçmeden veya onların anlayamayacağı şekle getirilerek ilgili hedefe gönderilmesi temel amaç olarak benimsenmektedir. Ancak gönderilecek olan bilginin herhangi bir nedenden dolayı üçüncü şahısların eline geçmesi durumunda gizlenen bilginin açığa çıkması veya açığa çıktığı durumda anlaşılması istenmeyen bir durumdur. Bundan dolayı pratik uygulamalarda *şifreleme* (cryptography) bilimi kullanılır. Ancak şifrelemeye ek olarak bilginin gizlenmesi ihtiyacının karşılanması, *veri gizleme* (data hiding) başlığı altında *gizliyazı/ steganografi* (steganography) ve *damgalama* (watermarking) bilimi ile birlikte ele alınır (Yalman ve ark., 2014).

Şekil 2.9.'da bilgi güvenliği gerektiren uygulamalarda kullanılan veri gizleme yöntemleri görülmektedir.



Şekil 2.9. Veri gizleme bilimi ve çeşitleri (Coşkun ve ark., 2013)

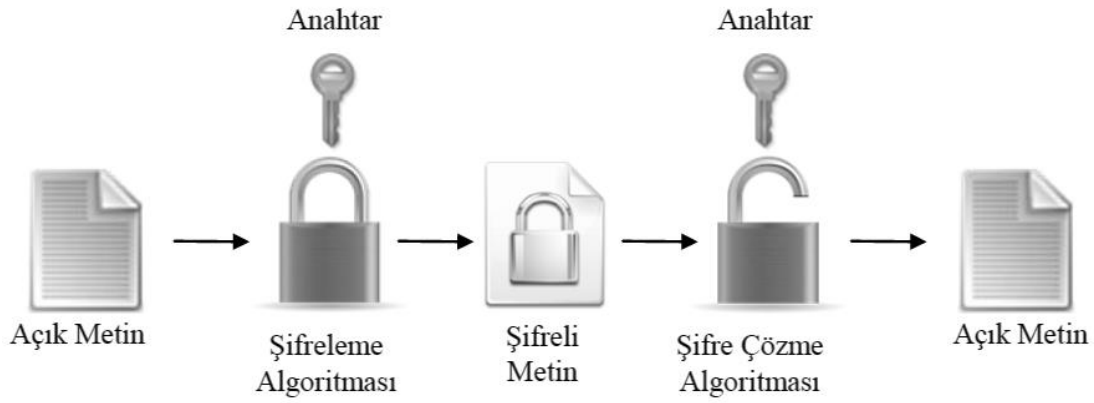
2.5.1. Şifreleme

Şifreleme bilimi olan kriptoloji Yunanca krypto's (saklı) ve lo'gos (kelime) kelimelerinin birleştirilmesinden oluşturulmuştur ve iletişimde gizli olan bilgilerin istenilmeyen kişiler tarafından anlamasını zorlaştırmaya çalışan ve şifrelenmiş verilerin çözülmesini gerçekleştirmeyi amaçlayan bilim dalıdır. Yani bilginin şifrelenerek gizlenmesi ve ortaya çıkarılması ile ilgilenir. Kriptoloji, kriptografi ve

kriptoanaliz olarak iki başlık altında incelenmektedir (Yerlikaya ve ark., 2006; İncetaş ve Sağıroğlu, 2015).

Verinin şifrelenerek gizli hale getirilmesi işlemine kriptografi (cryptography) denir. Böylelikle şifrelenen verinin bütünlüğü, gizliliği ve güvenliği sağlanmış olunur. Kriptografinin temel amacı veri içindeki bilginin gizliliğini sağlamaktır. Şifrelenen verileri analiz edip şifrelerin çözülmesi ile ilgilenen kriptoloji alt bilim dalına ise kriptoanaliz (cryptanalysis) denir (Coşkun ve Ülker, 2013).

Kriptosistem olarak adlandırılan şifreleme ve şifre çözme işlemleri bütünü, şifreleme algoritması, açık metin, şifreli metin ve anahtardan oluşmaktadır (Yavuzer Aslan ve ark., 2012). Şekil 2.10.'da genel bir kriptosistem gösterilmektedir.



Şekil 2.10. Kriptosistem yapısı (Aslan, 2013).

Modern şifreleme algoritmaları 3 ana başlık altında incelenmektedir. Bunlar;

1. Simetrik şifreleme algoritmaları,
2. Asimetrik şifreleme algoritmaları,
3. Hash algoritmaları.

Simetrik şifreleme algoritmaları içerisinde blok şifreleme ve akış (stream) şifreleri yer alır. Bu tür algoritmalarda şifreleme ve şifreyi çözme işlemi gizli anahtar denilen aynı anahtar ile yapılmaktadır. Asimetrik şifreleme algoritmalarında şifreleme işlemi yapılırken gizli bir anahtar kullanılırken şifre çözme işlemi yapılırken açık bir anahtar kullanılmaktadır. Açık anahtar herkesin erişebileceği bir anahtardır. Bu

algoritmalar kimlik denetiminin sağlanmasında büyük rol oynamaktadırlar (Sakallı, 2006; Akgün, 2011). Tablo 2.3.'de şifreleme algoritmalarına örnekler verilmiştir.

Tablo 2.3. Şifreleme algoritmaları (Aslan, 2013).

Simetrik Şifreleme Algoritmaları		Asimetrik Şifreleme Algoritmaları	Hash Algoritmaları
Blok Şifreler	Akan Şifreler		
DES	RC4	RSA	MD4
AES	HC-256	ECC	MD5
ARIA	Trivium	ElGamal	SHA
Present			RIPEMD-160
Serpenst			
Camellia			
Khazad			

Birçok şifreleme algoritması geliştirilmiş ve yeni şifreleme algoritmaları oluşturulmaktadır. Bu algoritmalarının birbirleriyle olan performansı incelenirken aşağıdaki ölçütler dikkate alınmaktadır:

1. Kırılma süresi uzunluğu: Şifrelenmiş verinin 3. şahıslar tarafından şifresinin çözülmesi için harcadıkları süre,
2. Zaman karmaşıklığı: Verinin şifrelenmesi ve şifrelenen verinin çözülmesi işlemleri için harcanan zaman,
3. Bellek karmaşıklığı: Verinin şifrelenmesi ve şifrelenen verinin çözülmesi işlemlerinde ihtiyaç duyulan bellek miktarı,
4. Esneklik: Kullanılan algoritmaya dayalı şifreleme uygulamalarının esnekliği,
5. Kolaylık ve standartlaşma: Uygulamaların dağıtımında kolaylık ya da algoritmaların standart hale getirilebilmesi,
6. Uygunluk: Algoritmanın kurulacak sisteme olan uygunluğu (Yerlikaya, 2006).

2.5.2. Sayısal damgalama

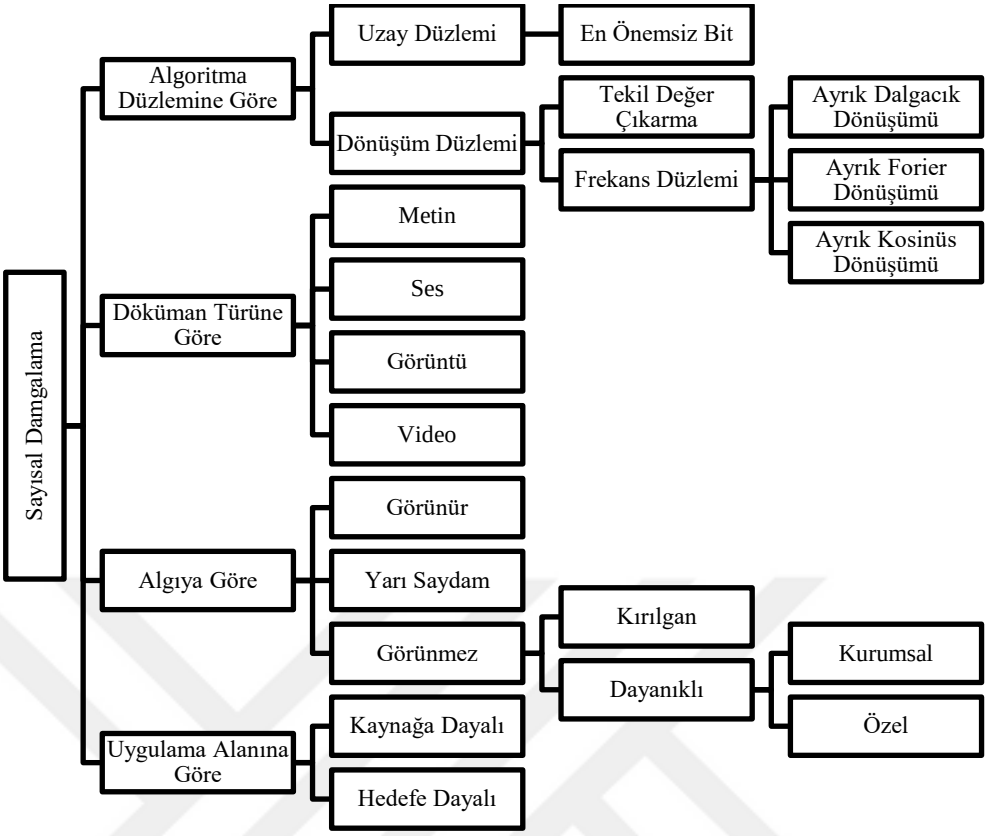
Çoklu ortam/multimedya (multimedia) verileri; metin, grafik, ses, animasyon, durağan ve hareketli görüntüden oluşan ve sayısal olarak işlenen, saklanan ve

gönderilen bilgisayar destekli tüm bilgiler olarak ifade edilmektedir (Akkoyonlu ve Yılmaz, 2005). İnternetin hızlı gelişimi ile bu çoklu ortam verilerinde herhangi bir kalite kaybı olmadan 3.şahıslar tarafından, izinsiz olarak üzerinde değişiklik yapılıp yeniden oluşturulup tekrardan dağıtılması kolay hale gelmiştir. İzinsiz olarak yapılan yasal olmayan bu işlemleri engellemek için sayısal verilerin güvenliğini sağlamak adına sayısal damgalama yöntemleri geliştirilmiştir (Üstübioğlu ve ark., 2015).

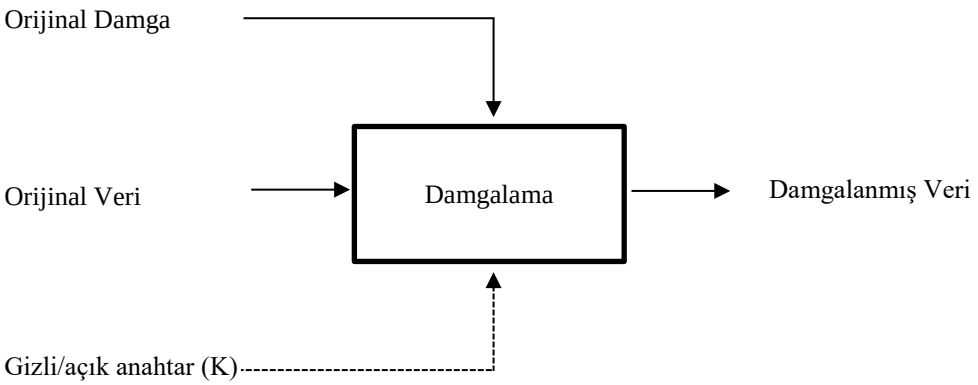
Sayısal damgalama işlemi gerçekleştirilirken herhangi bir sayısal bilgiye bilinen bir işareti (örneğin yazarın imzası, doğrulama kodu veya logo) orijinal bilginin anlamını bozmayacak şekilde ekleme yapılır. Damga adı verilen bu ekleme, orijinal bilgi anlamsız olacak derecede bozulmadığı sürece var olacak ve yasadışı kopyalama veya dağıtma girişimlerine karşı orijinal bilgiyi koruyacaktır. En yaygın olarak telif hakkı koruma, kopyalama koruma ve kimlik tespiti uygulamalarında damgalama kullanılmaktadır (Baraklı ve Vural, 2012).

Kullanım alanına göre sayısal damgalama Şekil 2.11.'de gösterildiği gibi algoritma düzlemi, doküman türü, uygulama alanı ve algıya göre dört sınıfa ayrılabilir (Doğan, 2011).

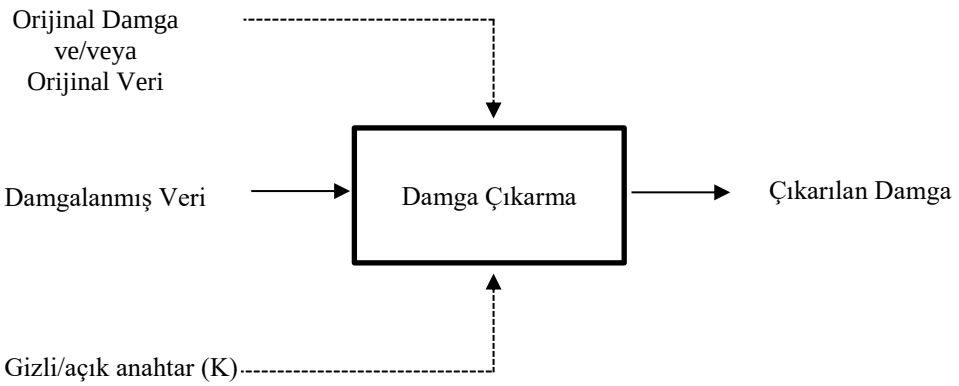
Sayısal damgalama işlemi gerçekleştirilirken orijinal damga, orijinal verinin içerisine bir K anahtarı kullanılarak eklenir. Böylece damgalanmış veri elde edilir. Damgalamanın kullanım amacına göre K anahtarı açık veya gizli olabilir. Şekil 2.12.'de temel sayısal damgalama işlemi gösterilmektedir. Şekil 2.13.'de ise sayısal damga çıkarma işlemi verilmektedir. Damga çıkarma işlemleri üç şekilde yapılabilmektedir. Bunlar denetimli, yarı-denetimli ve denetimsiz damga çıkarma işlemleridir. Denetimli damga çıkarma işlemi gerçekleştirilirken orijinal veri, orijinal damga ve anahtar birlikte kullanılmaktadır. Yarı-denetimli damga çıkarma işlemi yapılırken ise orijinal damga ve anahtar gerekmektedir. Denetimsiz damgalama işleminde ise sadece anahtarın kullanılması yeterlidir (Öztürk, 2009).



Şekil 2.11. Sayısal damgalama türlerinin sınıflandırılması (Doğan, 2011).



Şekil 2.12. Temel sayısal damgalama işlemi



Şekil 2.13. Temel sayısal damga çıkarma işlemi

Sayısal damgalama uygulamalarının sahip olduğu özellikleri aşağıdaki gibi sıralayabiliriz;

1. Görünmezlik ve Kalite: Damgalama uygulanmış olan bir veri orijinal haline göre değişikliğe uğramamalıdır. Görünmezlik sadece telif hakkının korunması amacıyla yapılan damgalama işlemlerinde değil damgalama uygulamalarının hepsinde olması gereken genel bir özelliktir. Damga ekleme işleminden sonra sayısal veride herhangi bir bozulmanın olmaması yani damgalanmış verinin orijinal veri ile aynı kalitede olması demektir (Fındık, 2010).
2. Sağlamlık: Damgalanmış veride damganın elde edilmesini engellemek için gerçekleştirilen saldırılara karşı direnci olarak tanımlanabilir. Damgalanmış veriye yapılan bilinçli veya bilinçsiz saldırılardan sonra damga büyük bir zarara uğramadan elde edilmesi gerekmektedir. Uygulamalara göre sayısal damganın sağlam olması değişiklik göstermektedir. Örneğin telif hakkının korunması için yapılan damgalamaların çok sağlam olması hedeflenirken, sayısal veriler üzerinde yapılan değişikliklerin tespiti için ise damganın kırılgan olması beklenir (Fındık, 2010).
3. Kapasite: Orijinal veri içerisine yapılacak orijinal damga miktarıdır. Damgalama uygulamaları gerçekleştirilirken orijinal verinin içerisine eklenecek olan damganın miktarının arttırılması yanında damgalanmış veriye karşı yapılacak saldırılara dayanıklılığının da aynı oranda korunması amaçlanmaktadır (Doğan, 2011).

4. Güvenlik: Damgalanmış verinin içerisinde bulunan damganın içeriğine erişmeye çalışan saldırılara karşı damgalama işlemi yapılırken bir güvenlik anahtarı kullanılarak şifreleme yapılır. Böylelikle saldırılarda damga saldırgan tarafından deşifre edilse bile damganın silinerek veya değiştirilerek zarar görmesini engellemeye yönelik bir önlem alınmış olunur (Yalman ve ark., 2014).

Damgalanmış veriye karşı bilinçli veya bilinçsiz olarak çeşitli saldırılar olabilir. Bu saldırılara karşı damgalama ne kadar fazla direnç gösterebilirse damgalama yöntemi o kadar dayanıklıdır. Bir damgalama sistemine karşı yapılacak saldırılar aşağıda listelenmiştir (Kazan, 2009):

1. Gürültü ekleme,
2. Filtreleme,
3. Gürültü yok etme,
4. Damga kaldırma ve engelleme,
5. Sıkıştırma,
6. İstatiksel ortalama,
7. Çoklu damgalama,
8. Geometrik ataklar,
9. Kırpma,
10. Rastgele geometrik bozulmalar,
11. Şifreleme,
12. Yazdırma-tarama saldırıları.

2.5.3. Steganografi

Bu çalışmanın temelini oluşturan steganografi, bilgi gizleme yöntemlerinin önemli bir alt dalı olup, görünmez iletişim sanatı ve bilimi olarak tanımlanabilir. Çoklu ortam bilgileri içerisine farklı bir bilgi gizlenerek yapılan bu görünmez iletişim oldukça başarılıdır. Buna en basit örnek olarak gizli bir mesajın sayısal bir resim içerisine gizlenmesi verilebilir. Görüntülerin ve diğer sayısal belgelerin yazdırılması sırasında kullanılan bir bilgisayar terimi olan *"Ne görüyorsan onu alırsın." (What*

You See Is What You Get-WYSIWYG), veri gizleme işlemi yapan kişiler için pek de geçerli olmayan bir terimdir. Çünkü sayısal olarak insan görme sistemi tarafından görünen bir görüntü veri gizleme işlemi yapan kişiler için görünenden fazla bilgiyi ifade edebilir (Bajpai ve Saxena, 2012).

Tarihi kaynağı ve gelişimi incelendiğinde steganografi kelimesi Yunanca olan ve örtülü/gizli/saklı anlamına gelen "steganos" ve çizim/yazım anlamına gelen "graphia" kelimelerinin birleşiminden oluşmaktadır (Fridrich, 2010). Yunan tarihçi Herodot'un aktardığı bilgilere göre; Milet (Muğla-Milas çevresi) tiranı Histiaeus, Aristagoras'a gizli bir mesaj göndermek ister. Histiaeus yanındaki kölelerinin birinin saçını kazıtır ve kölesinin kafa derisine mesajı dövme şeklinde işler. Kölenin saçı uzadıktan sonra onu Milet'e gönderir. Köle Milet'e vardığında saçını kazıtır ve mesajı ortaya çıkartır. Bu mesaj ile Aristagoras'ın Pers kralına karşı bir isyan başlatması teşvik edilmiştir. İşte bu örnek tarihteki ilk gizli haberleşme olarak karşımıza çıkmaktadır (Cox ve ark., 2007). Ayrıca yine Heredot'un bilgilerine göre aynı dönemlere ait olan başka bir gizli haberleşme örneği ise; Yunanlılara yapılan bir uyarı mesajına aittir. Bu mesajda Pers Kralı Serhas'ın düşmanca niyetlerini ve Yunanlara karşı bir saldırı yapacağı ile ilgili uyarısını içeren bilgiler yer almaktadır. Bu mesaj tahta bir plakaya kazındıktan sonra belli olmaması için üzeri balmumu ile kaplanmıştır (Anderson ve Petitcolas, 1998).

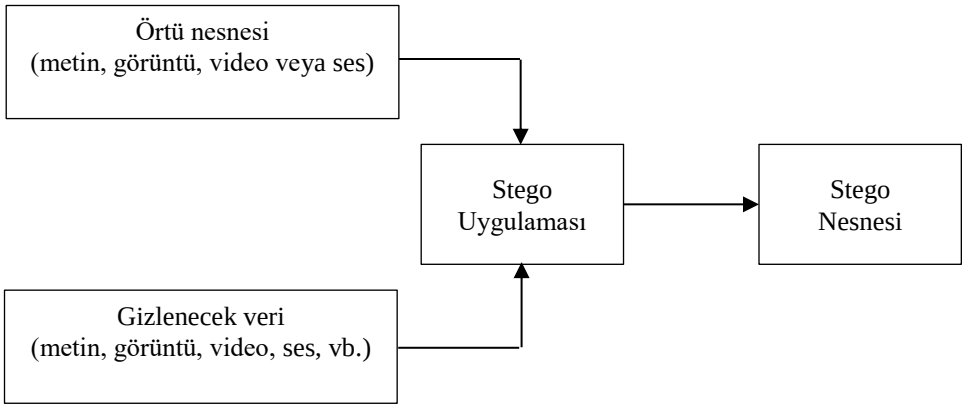
Romalılar meyve suyu ve süt gibi doğal maddelerden meydana getirdikleri içeceklerden oluşturdukları görünmez mürekkepler kullanarak gizli yazışmalar yapmışlardır. Bu mürekkeplerin günümüze kadar ulaştığı bilinmektedir (Dunbar, 2002). 1462-1516 yılları arasında yaşamış ve Alman bir başrahip olan Johannes Trithemius tarafından Latince yazılan "Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa" isimli eserde, verilerin şifrelenmesi ile ilgili bilgiler verilmektedir (Borse ve ark., 2013).

1941 yılında Almanların geliştirdikleri ve "microdot" olarak isimlendirilen alet ile gizli mesajı resimleme tekniğinden faydalanarak kâğıtlara yazdırmışlardır. Burada gizli mesajın boyutu küçültülerek işlem yapılmaktadır. Böylece büyük miktarda

veriler gizli iletişimde kullanılmıştır (Kumar ve Pooja, 2010). Ayrıca II. Dünya Savaşı sırasında Romalılarında kullanmış olduğu gizli mürekkeplerin kullanıldığı yazışmalar yapılmıştır (Jamil, 1999).

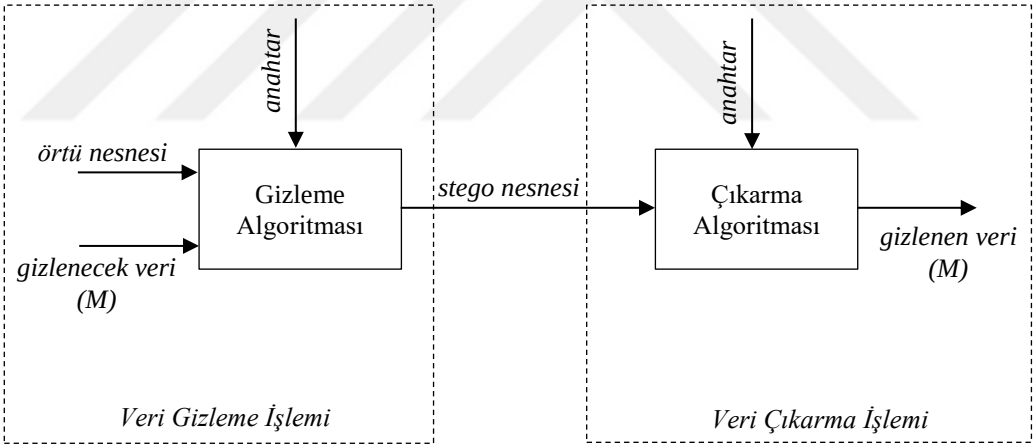
Günümüzde steganografi uygulamalarına bakıldığında ise bu uygulamaların sayısal veriler üzerinde yapıldığı görülmektedir. Gelişen teknolojiyle bağlantılı olarak verilerimizi korumak amacıyla günümüzde sıklıkla kullanılmaya başlanmıştır (Şahin ve ark., 2006). Çoklu ortam verilerinin telif hakkı kontrolünün gerçekleştirilmesi, bireylere ait bilgilerin kendi fotoğrafları içerisine gömülü olan akıllı kimlik kartlarının dayanıklılığı-sağlamlığının arttırılması, video-ses senkronizasyonunun gerçekleştirmesi, şirketlerin gizli verilerinin dolaşımının sağlanması, televizyon yayını, TCP/IP paketlerinin iletimi ve tıbbi görüntüleme sistemlerinde hastaya ait bilgilerin hasta görüntüsü verisi içerisine gizlenmesi sırasında, steganografi yöntemleri kullanılabilmektedir (Cheddad ve ark., 2010).

Sayısal veriler kullanılarak yapılan steganografi işlemi gerçekleştirilirken temel fikir; gizli olarak ifade edilen veriyi örtü nesnesi olarak adlandırılan çoklu ortam verisi içerisine gömülmesi/gizlenmesidir. Burada ifade edilen çoklu ortam verisi bir metin, görüntü, video veya ses parçası olabilir (Wang ve Chen, 2006). Gizli verinin ve bu gizli veriyi içerisinde barındıran taşıyıcı olan örtü nesnesinin birleşmesi ile yeni bir sayısal veri ortaya çıkmaktadır. Bu sayısal veri stego nesnesi olarak adlandırılır ve elde edilen stego nesnesi örtü nesnesi gibi sıradan bir metin, görüntü, video veya ses verisi olarak görünür (Chen ve Wang, 2010). Şekil 2.14.'de basit yapıda sade bir steganografi sistemi uygulaması görülmektedir.



Şekil 2.14. Steganografi sistemi uygulaması (Jayaram ve ark., 2011).

Şekil 2.15.'de steganografi sisteminin genel yapısı gösterilmektedir (Naji ve ark., 2009; Al-Ani ve ark., 2010). Şekil 2.15.'de gösterilen steganografi sistemine (stego sistem - steganografik sistem) ek olarak gizlenecek verinin gizlenmesi sırasında stego anahtar adı verilen ek bir gizli veri kullanılarak gizlilik derecesi arttırılabilir. Steganografi sistemlerinde bu anahtarın kullanılması isteğe bağlıdır. Bir steganografi sistemi iki bölümden oluşmaktadır. Bunlardan birincisi veri gizleme işlemi, ikincisi ise veri çıkarma işlemidir. Veri gizleme işlemi gerçekleştirilirken örtü nesnesi, gizlenecek veri ve varsa anahtar ile gizleme algoritması uygulanarak stego nesnesi oluşturulur. Elde edilen stego nesnesi iletişim kanalı kullanılarak hedefe yollandığında varsa anahtar kullanılarak gizleme algoritmasının tersi işlem yapılarak gizlenen veri açığa çıkartılır. Anahtar bilgisi ile gizleme algoritmasının nasıl yapıldığı veya çıkarma algoritmasının nasıl yapılacağı bilgisi dışarıdan temin edilir. Anahtar kullanılarak yapılan gizleme işlemlerinde anahtar olmadan veri gizleme veya çıkarma işlemi başarılı olarak gerçekleştirilemez.



Şekil 2.15. Steganografi sistemin genel yapısı (Naji ve ark., 2009; Al-Ani ve ark., 2010).

Veri gizleme metotları tasarlanırken dikkat edilmesi gereken bazı parametreler vardır. Bu parametreler dayanıklılık/sağlamlık, fark edilemezlik/güvenlik ve kapasite olarak sıralanabilir (Zhang ve ark., 2009; Tang ve ark., 2013).

1. Kapasite: Örtü nesnesi içerisine gömülen gizli veri miktarını ifade etmektedir. Gizli veri miktarı arttırılırken dikkat edilmesi gereken durumlardan bir tanesi ise stego nesnesinin orijinalliğe (örtü nesnesine) ve güvenliğine etki etmeden

bu arttırmanın yapılmasıdır. Eğer güvenliği değişirse steganaliz tarafından fark edilebilir (Ahani ve Ghaemmaghami, 2014).

2. Güvenlik: Örtü nesnesinin iletimi sırasında bu iletişimi gizlice dinleyen kişilere karşı uygulanan veri gizleme metodunun hem istatiksel olarak hem de algısal olarak görünmez olması gerekmektedir. Bir steganografi sisteminin güvenli kabul edilmesi demek bu tasarlanan sistem içerisindeki gizli verinin varlığının, 3. şahıslar tarafından her hangi bir yöntem kullanarak, tespit/fark edilememesidir (Wang ve Wang, 2004).
3. Sağlamlık: Örtü nesnesine iletişim sırasında bazı saldırılar yapılabilir. Bu saldırılar sonucunda içerisindeki gizli verinin bozulmaması sağlamlık olarak ifade edilir (Ramaiya ve ark., 2013). Rastgele gürültü ekleme, ölçeklendirme, döndürme ve sıkıştırma örtü nesnesine yapılabilecek saldırılara örnek olarak verilebilir (Naji ve ark., 2009). Sağlamlık daha çok damgalama uygulamalarında dikkat edilen bir özelliktir. Steganografi uygulamaları için aranan önemli bir özellik değildir. Ancak steganografi uygulamasında örtü nesnesi JPEG kodlama yöntemi ile oluşturulmuşsa dayanıklı olması arzu edilir (Wang ve Wang, 2004).

Şekil 2.9.'da görüldüğü üzere steganografi, dilbilimsel ve teknik steganografi olmak üzere ikiye ayrılmaktadır. Dilbilimsel steganografi de gizli verinin taşınması için örtü nesnesi olarak doğal dil yani metin (text) kullanılmaktadır (Sharif ve ark., 2016). Teknik steganografi de ise taşıyıcı olarak farklı nesneler kullanılmaktadır. Bunlar görünmez mürekkepler, gizli yerler, microdotlar ve bilgisayar tabanlı yöntemler olarak alt başlıklara ayrılabilir (Kipper, 2003). Bilgisayar tabanlı sayısal veriler kullanılarak yapılan veri gizleme işleminde taşıyıcı olarak görüntü, ses, hareketli görüntü kayıtları (video) ve metin belgeleri kullanılmaktadır (Pavani ve ark., 2013).

2.5.3.1. Sayısal görüntülerde steganografi

Sayısal görüntü içerisindeki detayların insan görme sistemi tarafından algılanması düşük olduğundan dolayı sayısal görüntüler veri gizleme işlemlerinde çoğu zaman taşıyıcı olarak kullanılmaktadırlar. İçerisine gizlenen mesaj herhangi bir metin,

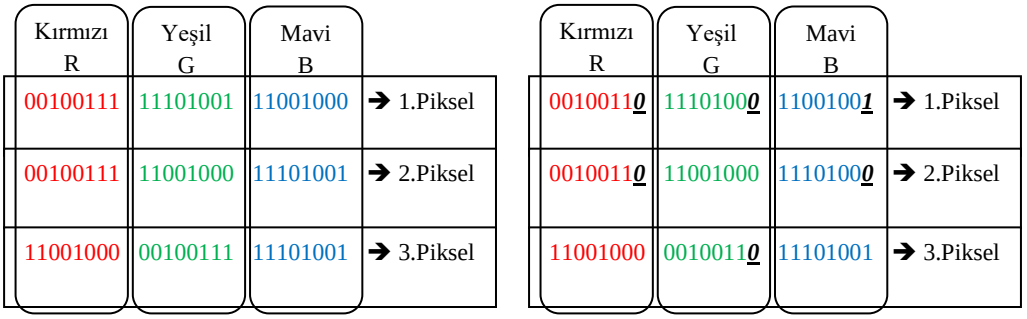
görüntü, ses veya video olabilir (Ghebleh ve Kanso, 2014). Yani sayısal olarak ifade edebileceğimiz her türlü veriyi sayısal görüntüler içerisine gizleyebiliriz.

Literatür incelendiğinde sayısal görüntülerde steganografi metodunu kullanan birçok çalışma ile karşılaşmak mümkündür. Bu çalışmalarda yapılan sayısal görüntü steganografisi iki ana başlık altında sınıflandırılabilir. Bunlar bit uzayı-düzlemi ve frekans uzayıdır (Safy ve ark., 2009; Wang ve ark., 2010).

2.5.3.1.1. Bit uzayında steganografi

Örtü görüntüsünün piksellerinin "en düşük değerlikli bit (LSB)" değeri ile gizli mesajın bit değerinin yer değiştirildiği bu yöntem en eski ve en basit olarak uygulanılan veri gizleme metodudur (Rosaline ve Raj, 2013; Lerch-Hostalot ve Megias, 2013). Bitlerin yer değiştirme işlemi yapılmadan önce, örtü görüntüsünün pikselleri ile gizlenmek istenilen veri ikili sayı (binary) biçimine dönüştürülür (Vashishtha ve ark., 2013). Elde edilen bu bitlerin örtü görüntüsünün LSB bitleri ile yer değiştirmesi sırasında görüntünün piksellerinin sayısal olarak değişeceğinden bir renk değişimi olacaktır. Fakat bu değişimler insan görme sistemi tarafından fark edilemeyecek kadar küçük değişimlerdir (Raj ve Soumya, 2013). 24 bit renkli bir görüntünün her bir pikseline kırmızı, yeşil ve mavi renk kanalları kullanılarak 3 bit veri gizleme yapılabilir (Shrikalaa ve ark., 2013).

Şekil 2.16.'da 24 bit renkli bir görüntünün üç pikseline A harfinin gizlenmesi gösterilmektedir. İlk önce A harfinin ASCII karşılığını yani 65'i ikili sayı sistemine dönüştürmeliyiz. 65 sayısının ikili sayı sistemindeki karşılığı $(001000001)_2$'dir. Elde edilen bu 9 bitlik değeri sırasıyla her pikseldeki en önemsiz bit değeri ile karşılaştırıp bu değere göre değiştirirsek Şekil 2.16.b.'deki yeni piksel değerleri elde edilmiş olunur. 1.pikselin bütün renk değerleri, 2.pikselin kırmızı ve mavi renk değeri, 3.pikselin ise yeşil renk değerlerinin son biti ilk halinden farklı olduğu Şekil 2.16.b.'de gösterilmiştir (Aydoğan ve ark., 2011).



Şekil 2.16. A harfinin bir görüntünün piksellerine gizlenmesi a) veri gizleme öncesi piksellerin bit değerleri, b) veri gizleme sonrası piksellerin bit değerleri (Aydoğan ve ark., 2011).

24 bit renkli görüntünün yüksek kaliteye sahip olması nedeniyle bu tür görüntülere gizlenebilecek veri miktarı en üst seviyede olabilmektedir. Bunun için veri gizlemede kullanılabilecek en iyi görüntü biçimi 24 bit renkli görüntülerdir (Yalman, 2010).

2.5.3.1.2. Frekans uzayında steganografi

Frekans uzayında veri gizleme işlemi yapmak için ilk olarak örtü görüntüsü ayrık kosinüs dönüşümü (discrete cosine transform − DCT), ayrık dalgacık dönüşümü (discrete wavelet transform − DWT) ve ayrık fourier dönüşümü (discrete fourier transform − DFT) gibi dönüşüm işlemleri gerçekleştirilip görüntü bileşenleri elde edilir ve bu bileşenlerin dönüşüm katsayılarında veri gizleme işlemi gerçekleştirilir (Chang ve ark., 2007). Bu katsayılar sıfır ve sıfırdan farklı değerlerden oluşmaktadırlar. Sıfır değerine sahip olan bileşenler insan görme sistemi tarafından algılanamayan bölgeleri ifade eder. Kayıplı sıkıştırma işlemi yapılırken bu bölgedeki veriler atılır. Sıfırdan farklı değere sahip olan bölgeler ise insan görme sistemi tarafından algılanabilir bölgeleri temsil eder. İnsan görme sistemi tarafından algılanabilir olan bölgelere veri gizleme işlemi uygulanır. Böylece kayıplı ve kayıpsız görüntü olarak yapılacak dönüşümler sırasında gizlenen veri kaybolmayacaktır (Yalman, 2010).

Frekans uzayı kullanılarak yapılan veri gizleme işlemi ile veriler daha dayanıklı bölgelere gizlenmiş olurlar. Bu bölgeler görüntüye yapılacak olan saldırılara karşı daha dirençli olmaktadırlar (Kafri ve Suleiman, 2009).

2.5.3.2. Sayısal seste steganografi

Sayısal olarak çok kolay elde edilebilen ses dosyalarında da veri gizleme işlemleri yapılabilmektedir. Ses dosyaları ile ilgili birçok veri gizleme yöntemi geliştirilmiştir. Ses dosyalarına veri gizleme işlemi gerçekleştirilirken kullanılan yöntemleri aşağıdaki gibi maddeleyebiliriz (Qiao ve ark., 2012):

1. Düşük bit kodlama (Low bit encoding): LSB olarak da bilinen bu metot kullanılan en eski veri gizleme yöntemlerindendir. Gizlenecek mesajın bitleri örtü nesnesi olan ses dosyasının bitleri ile değiştirilir. Yüksek kapasitede veri gizleme sağlamasına karşın gürültü ekleme gibi basit ataklara dayanıklı değildir. Stego nesnesi olan ses dosyasının filtreden geçirilmesi, gürültü eklenmesi veya kayıplı sıkıştırılma yapılması durumunda çok büyük olasılıkla gizlenen veriler yok olur (Djebbar ve ark., 2011).
2. Faz/Aşama kodlama (Phase encoding): Görüntüye veri gizlerken kullanılan yöntemlerden biri olan frekans uzayı yöntemine benzemektedir. Ses dosyası küçük bölütlere ayrılarak her bölüt için ayrık fourier dönüşümü (DFT) uygulanarak aşama-faz ve büyüklük matrisleri oluşturulur. Komşu olan bölütlerin aralarındaki aşama farklılıkları hesaplanır. Bundan sonra her bölüt için yeni bir aşama değeri bilgisi gizlenerek oluşturulur ve yeni aşama matrisleri ile büyüklük matrisleri birleştirilerek yeni bölütler elde edilir. Bu bölütlerin birleştirilmesi ile veri gizlenmiş ses dosyası elde edilir (Şahin, 2007).
3. Yayılı spektrum (tayf yayılması) kodlama (Spread spectrum encoding): Gizlenmek istenilen dar bantlı bir sinyalin yani mesajın daha geniş bantlı sinyaller içerisine gizlenmesi ile gerçekleştirilir. Gizlenmek istenilen mesaj, ses sinyalinin neredeyse bütün frekans spektrumu içerisine yayılmış bir gürültü gibi taşınacaktır. Burada gürültünün örtü nesnesi olan ses sinyalinin frekans spektrumunun olabildiğince tamamına yayılması istenmektedir (Yürüklü, 2013).
4. Yankı veri kodlama (Echo data encoding): İnsan kulağının ses dosyalarındaki milisaniyeler mertebesindeki kısa süreli yankıları algılayamaması özelliğinin kullanılarak veri gizleme yapılan bir dönüşüm kodlama tekniğidir.

Gizlenecek veri yankı sinyali içerisine ‘0’ ve ‘1’ olarak kodlanır ve bu yankı sinyali, gecikme ve bağıl genlik değerlerine göre ses dosyasının içerisine eklenir (Çetin, 2008).

2.5.3.3. Hareketli görüntü kayıtlarında steganografi

Görüntü dosyalarında veri gizleme işlemi sırasında gömülebilecek veri kapasitesi sınırlıdır. Bu sınırı aşmak için hareketli görüntü kayıtları (video) kullanılarak veri gizleme işlemi yapılabilmektedir. Video dosyaları çok sayıda görüntünün peşi sıra sürekli olarak akmasıyla ve bununla birlikte ses dosyalarının akışıyla oluşur. Bunun için video içerisine veri gizleme yapılırken, görüntü ve ses içerisine veri gizleme yöntemlerinin birleştirilmiş hali kullanılmış olur. Video kayıtlarına veri gizleme işleminde ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT) ve ayrık fourier dönüşümü (DFT) kullanılır (Yalman, 2010; Yıldız ve Özcerit, 2015).

Video kayıtları üzerinde yapılan veri gizleme yöntemleri, ham video (raw video) kayıtlarında veri gizleme ve sıkıştırılmış video (bit stream) kayıtlarında veri gizleme olarak iki başlıkta incelenmektedir. İlk olarak ham videolar kullanılmıştır. Ham videolar üzerinde yapılan çalışmalar hareketli görüntü kayıtlarındaki veri gizleme çalışmalarının temelini oluşturmaktadır. Sonraki zamanlarda ise büyük dosya kapasitesindeki videoların sıkıştırılması ihtiyacının doğmasından dolayı sıkıştırılmış video kayıtları üzerinde veri gizleme uygulamaları geliştirilmiştir (Çetin, 2008).

2.5.3.4. Metinde steganografi

Örtü nesnesi olarak metinlerin kullanıldığı metin steganografi yöntemi metin dosyalarında gizli veriyi gömmek için gereksiz bit bulunmasının zor olmasından dolayı çok tercih edilmemektedir (Gutub ve Fattani, 2007). Görüntü ve ses gibi sayısal verilere göre metin steganografisi en zor olan steganografi türüdür (Shahreza ve Shahreza, 2007). Fakat diğer steganografi uygulamalarına göre de bellekte daha az yer işgal etmesi ve iletiminin basit olması metin steganografisinin avantajları olarak karşımıza çıkmaktadır. Diller ve yapıları gereği tasarlanacak olan steganografi

sistemlerde farklılıklar olmaktadır. Yani tek bir steganografi sistem bütün dillerde kullanılamamaktadır (Gutub ve Fattani, 2007).

Metin steganografisinde kullanılan teknikler aşağıda maddeler halinde belirtilmiştir (Gutub ve Fattani, 2007; Şatır, 2013). Bunlar:

1. Kelimelerdeki belirli karakterler
2. HTML dokümanları
3. Satır ve kelime kaydırma
4. Kısaltmalar ve boşluklar
5. Anlamsal ve karakter öznitelik metotlarıdır.

2.5.4. Steganografi, damgalama ve şifreleme arasındaki farklar

Gizli iletişimde kullanılan kavramlar olan şifreleme biliminin alt dalı kriptografi, veri içerisine başka bir veri gömmede kullanılan steganografi ve damgalama ile karıştırılan kavramlardır.

Kriptografide var olan bir mesaj bir alıcıya gönderilirken farklı bir biçimde, kamufle edilmiş olarak gönderilir. Yollanan bu mesajı sadece alıcılar çözebilir/anlayabilir ve kamufle edilen mesajı okuyabilirler. Kriptografi, göndericiden alıcıya mesaj iletimi sırasında, sadece alıcı tarafından çözülebilecek/anlaşılabilecek mesajın içeriğinin korunmasıyla ilgilenir (Mohanty, 1999). Kriptografide, yollanan mesajın içeriğinde gizli bir bilgi olduğunu herkes bilir (Sabokdast ve Mohammadi, 2013).

Steganografide yazı, görüntü, ses veya video gibi taşıyıcı olan sayısal bir veri içerisine başka bir mesaj gömülerek iletim gerçekleşir. Bu iletim sırasında gönderici ve alıcı dışındaki 3. şahıslar tarafından sayısal veri içerisindeki mesajın tespit edilmemesi amaçlanır (Al-Husainy, 2009). Yani iletilen veri içerisindeki herhangi bir gizli mesajın olup olmadığı kimse tarafından anlaşılamaz (Sabokdast ve Mohammadi, 2013).

Damgalamada steganografide olduğu gibi taşıyıcı olan sayısal bir veri içerisine başka bir mesaj gömülerek iletim gerçekleşir. Fakat damgalamanın kullanım amacı taşıyıcı olan verinin telif hakkı koruması, yayın izleme, işlem takibi ve benzeri faaliyetlerdir (Şatır ve Işık, 2012).

Steganografide sayısal veri içerisine gizlenen mesajın duyu organları tarafından algılanamaz olması ve çeşitli matematiksel analizlerle fark edilememesi en önemli ölçütlerdendir. Damgalamada ise sayısal veri içerisine gizlenen mesajın duyu organları tarafından algılanamaz olması istenirken matematiksel analizlere karşı fark edilemez olması mutlaka olması gereken bir ölçüt değildir. Buna karşın bir damgalama sisteminde sayısal veri içerisindeki damganın çıkartılamaması yani dayanıklılığı (robustness) en önemli kriterlerdendir. Fakat bir steganografi sisteminde dayanıklılık daha az önemlidir (Yargıçoğlu, 2010). Tablo 2.4.'de steganografi ve damgalama yöntemlerinin kıyaslanması verilmiştir.

Tablo 2.4. Steganografi ve damgalama yöntemlerinin karşılaştırılması (Wang ve Wang, 2004).

	Gereksinimler	Damgalama		Steganografi
		Özel	Açık	
Amaç	Fikri mülkiyet haklarının korunumu	++++		–
	Şüpheye mahal vermeden gizli veri iletimi	–		++++
Özellikler	İnsan duyuları açısından görünmezlik	++++		+++++
	İstatistikî ve algoritmasal görünmezlik	+		+++++
	Çıkarılma, yok edilme ve değiştirilmeye karşı dayanıklılık	+++++		–
	Normal sinyal işlemeye karşı dayanıklılık	++++		+
	Sıkıştırmaya karşı dayanıklılık	++++		++
	Büyük gömme kapasitesi	++		++++
Algılama / Geri elde etme	Örtü nesnesi olmadan algılama/geri elde etme	–	++++	++++
	Örtü dosyası ile geri elde etme	++++	–	–
	Geri elde etme/algılama sırasında karmaşıklık ihtiyacı	++		+++

Çok önemli: +++++ Gerekli: ++++ Önemli: +++ İstenir: ++ İşe yarar: + İlgisiz veya gereksiz: –

2.5.5. Steganaliz

Steganografi sistemi içerisinde gizlenen bilgiyi açığa çıkarma işlemine steganaliz denir (Şatır, 2013). Steganaliz ile uğraşan kişilere ise steganalist (steganalyst) denir (Yürüklü, 2013).

Bir steganografi sisteme, içerisinde gizli bir bilgi varlığının olup olmadığını bulmaya çalışan veya eğer bilgi var ise bu bilgiyi açığa çıkarmak için, yapılan saldırılarda saldırıyı yapan kişinin bu steganografi sistemini bildiği varsayılır. Bu varsayım Kerchoffs'un prensibi olarak bilinir. Steganalistin saldırı yapabilmesi için elinde steganografi sistemin bazı verilerine sahip olması gerekir. Sahip olduğu bu verilere göre ise saldırı modellerinden birini seçebilir (Şahin, 2007). Saldırı modelleri aşağıda maddelendirilmiştir (Yürüklü, 2013). Bunlar;

1. Stego saldırısı: steganalist tarafından sadece stego nesnesi biliniyorsa yapılacak olan saldırı.
2. Bilinen örtü saldırısı: steganalist tarafından örtü nesnesinin ilk hali yani orijinal bir kopyası biliniyorsa yapılacak olan saldırı.
3. Bilinen mesaj saldırısı: steganalist tarafından örtü nesnesi içerisine gizlenen mesaj biliniyorsa yapılacak olan saldırı.
4. Seçilmiş stego saldırısı: steganalist tarafından steganografi sisteminin algoritması ve stego nesnesi biliniyorsa yapılacak olan saldırı.
5. Seçilmiş mesaj saldırısı: steganalist bu saldırıda çeşitli mesajlar seçerek önceden geliştirilen steganografi sistem metotları (steganografik araçlar) kullanır ve gizleme algoritmasını bulmaya çalışır.
6. Bilinen stego saldırısı: steganalist tarafından örtü nesnesi, stego nesnesi ve steganografi sistem metotları (steganografik araçlar) biliniyorsa yapılacak olan saldırı.

Bu saldırı modellerinden her hangi biri seçilerek yapılan saldırılar iki farklı amaç için yapılabilir. Bunlardan ilki aktif saldırı olarak adlandırılır. Aktif saldırıda stego nesnesi içerisindeki gizli mesaj yok edilmeye veya bozulmaya çalışılır. İkincisi ise

pasif saldırıdır. Buradaki amaç ise stego nesnesi içerisinde gizli bir mesajın olup olmadığının tespitidir (Yürüklü, 2013).

2.6. Sonuç

Bu bölümde sayısal görüntüler hakkında temel bilgiler verilmiştir. Tez çalışmasının konusu olan steganografi ile ilgili bilgiler sunulmuştur. Steganografiye ek olarak veri gizleme başlığı altında yer alan şifreleme (kriptoloji) ve damgalama (watermarking) tekniklerinin gizli haberleşmedeki rolleri, birbirlerine olan üstünlükleri ve farklılıkları vurgulanmıştır. Tez çalışmasının temelini oluşturan sayısal görüntülere steganografi yönteminin nasıl uygulanacağı sunulmuştur.

BÖLÜM 3. SAYISAL GÖRÜNTÜLER İÇİN BLOK EŞLEŞTİRMELİ VE TARAMA SIRASI SEÇİMLİ VERİ GİZLEME ALGORİTMASI

3.1. Giriş

Steganografi; örtü nesnesi içerisine, gizli verinin fark edilemez bir biçimde gizlenmesini amaçlamaktadır. Bilgiyi gizleyen kişi ve bu gizli verinin yollandığı kişi dışında başka hiçbir kimse, bu iletişimde gizli verinin var olup olmadığını anlayamaz. Buna karşın, yollanan stego nesnelerinde bulunabilecek istatistiksel farklılıklardan faydalanmayı deneyerek steganaliz saldırıları yapılabilmekte ve bu saldırılarla stego nesnesi içerisindeki gizli verilerin varlığı ortaya çıkarılmaya çalışılmaktadır (Tang ve ark., 2013).

Steganografi sistemleri tasarlanırken dayanıklılık/sağlamlık, fark edilemezlik/güvenlik ve kapasite gibi dikkat edilmesi gereken bir kaç önemli gereksinimler vardır (Zhang ve ark., 2009; Tang ve ark., 2013; Şatır ve Işık, 2014). Bir steganografi sistemine güvenli denilebilmesi için, tasarlanan sistemde gizlenen verinin varlığının, 3. şahıslar tarafından her hangi bir yöntem kullanarak, tespit/fark edilememesi gerekmektedir (Wang ve Wang, 2004). Stego nesnesi içerisindeki gizli verinin fark edilememesi steganografi uygulamalarındaki en önemli gereksinimlerdendir (Luo ve ark., 2010; Khalind ve Aziz, 2013).

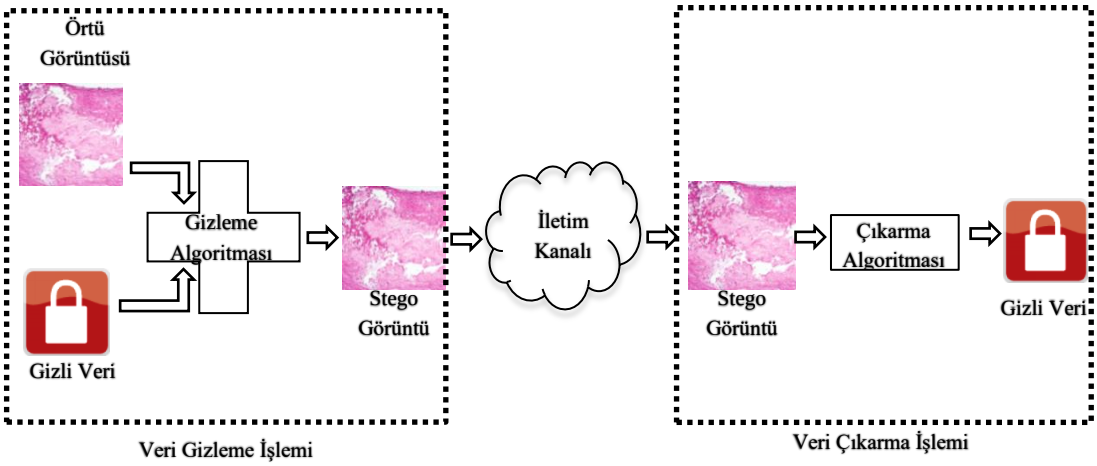
Stego nesnesi olarak bir görüntü ele alındığında, bu görüntü içerisinde yapılan veri gizleme yönteminin/algoritmasının güvenli sayılabilmesi için ise örtü görüntüsü üzerinde az bozulmaya/değişime neden olunması gerekmektedir (Nayak ve Bhagvati, 2013). Görüntü bozulması, görüntü üzerinde yapılacak değişikliği ifade etmektedir (Şahin, 2007). İçerisine veri gizlenen her görüntü değişikliğe uğrar ve bozulur. Bir görüntü üzerinde ne kadar az değişim yapılırsa görüntü o kadar az bozulmuştur.

Buna karşın bozulma miktarı artıkça da görüntü kalitesi düşer. Veri gizleme yöntemlerinden örtü görüntüsü üzerinde az bozulma yapanlar, çok bozulma yapanlara kıyasla daha güvenlidirler. Az bozulma yapılan veri gizleme yöntemleri steganaliz saldırılarına karşı güçlü olabilirler. Bu nedenle veri gizleme yöntemleri tasarlanırken görsel kalite faktörüne daha fazla önem verilir (Nayak ve Bhagvati, 2013).

Örtü görüntüsü ile içerisine gizlenecek veri görsel ve sayısal olarak ne kadar birbirine benzer ise stego görüntü içerisinde gizli verinin fark edilmesi o kadar güçleşecektir (Luo ve ark., 2010). Bir başka deyişle, örtü görüntüsü üzerinde yapılacak değişimler/bozulmalar ne kadar az olursa gizli verinin fark edilmesi de o kadar azalmış olur.

Bu tez çalışmasında örtü görüntüsü içerisindeki gizli verinin fark edilmesini engellemek amacıyla yeni bir steganografi yöntemi/algoritması geliştirilmiştir. Önerilen algoritma ile görüntü kalitesinin daha da arttırılması ve gizlenen verinin 3. şahıslar tarafından ele geçirilmesini güçleştirmek için daha güvenli olmasına odaklanılmıştır.

Şekil 3.1.'de önerilen algortimanın veri gizleme, iletim ve veri çıkarma süreçleri görülmektedir. Yöntem iki ana bölümden oluşmaktadır. Bunlardan ilki "*Veri Gizleme İşlemi"* diğeri ise "*Veri Çıkarma İşlemi"* dir.



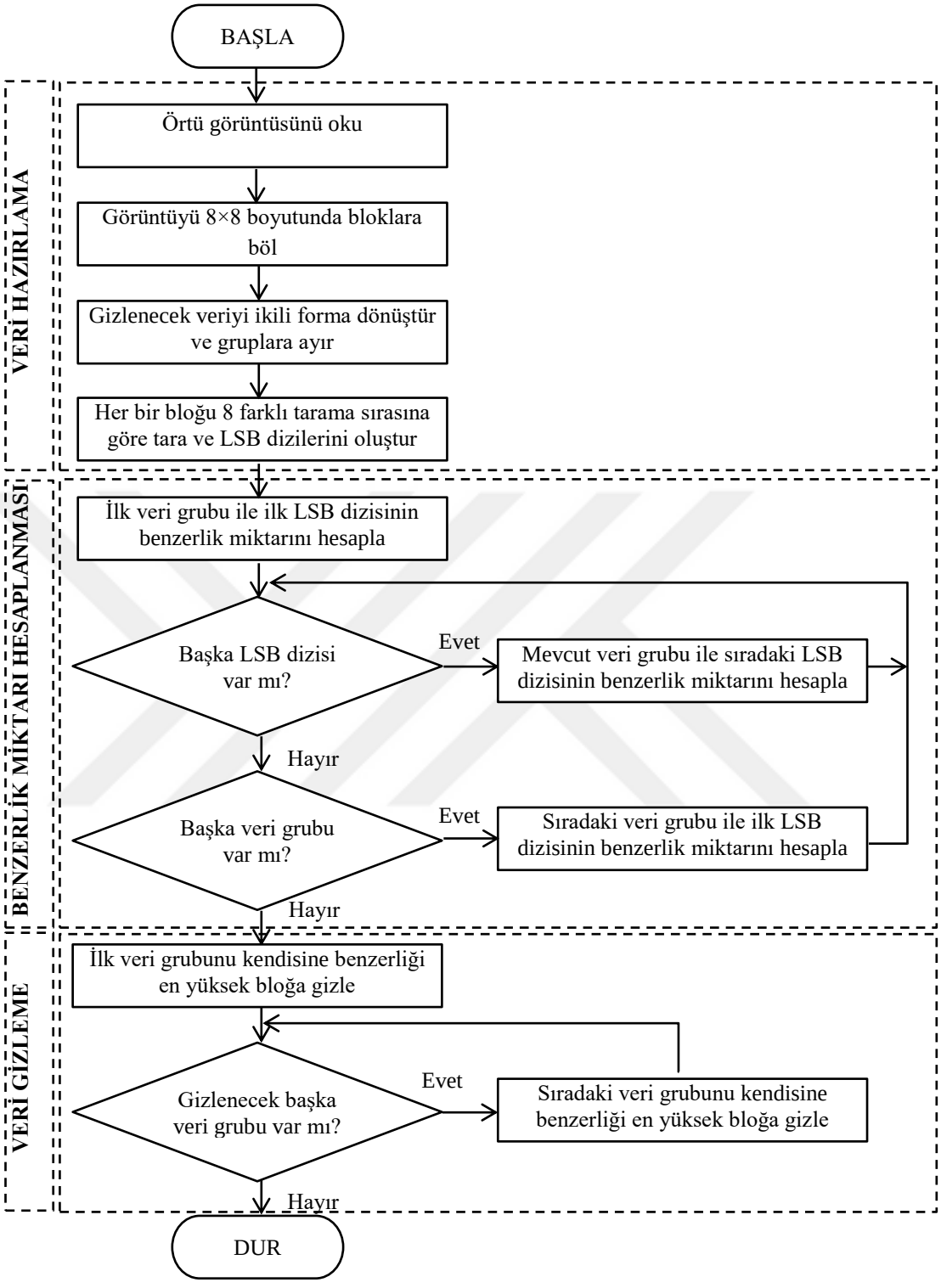
Şekil 3.1. Önerilen yöntemin veri gizleme ve çıkarma işlemi süreçleri

3.2. Veri Gizleme İşlemi

Veri gizleme işleminde LSB yöntemi olarak da adlandırılan örtü görüntüsünün piksellerinin en son biti yani en önemsiz biti kullanılmıştır. LSB yöntemi en basit ve en çok kullanılan veri gizleme yöntemidir (Zhu ve ark., 2013; Aydoğan ve Bayılmış, 2016).

Klasik veri gizleme işleminde örtü görüntüsüne gizlenecek veri bitleri, örtü görüntüsünün ilk pikselinden itibaren sırasıyla komşu piksellere gizlenir. Geliştirilen algoritmada ise bu sıradan veri gizleme işlemi yerine önceden yapılan bir ön işlem ile gizleme işlemi yapılacak piksellerin sırası değiştirilmektedir. Böylelikle örtü görüntüsü üzerinde en az bit değişimi yapılabilmesi için gizli verimiz ile örtü görüntüsünün sayısal olarak benzer parçaları bulunması amaçlanmaktadır. En az bit değişimi güvenli bir steganografi yöntemi sunacaktır.

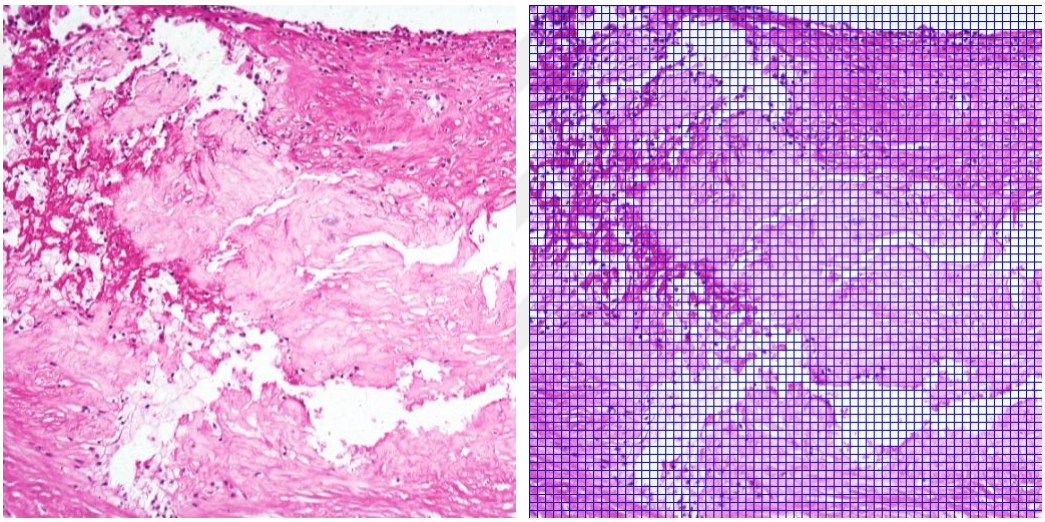
Şekil 3.2.'de geliştirilen algoritmanın akış diyagramı görülmektedir. Gösterildiği üzere geliştirilen algoritmada veri gizleme işlemi üç aşamada yapılır. Bunlar *Veri Hazırlama, Benzerlik Miktarı Hesaplanması* ve *Veri Gizleme* aşamalarıdır.



Şekil 3.2. Geliştirilen veri gizleme işlemi akış diyagramı

3.2.1. Veri hazırlama

Veri hazırlamanın ilk aşaması olan örtü görüntüsünü bloklara ayırma; örtü görüntüsü, veri gizleme işlemi aşamasında 8×8 boyutlarında bloklara ayrılacağından, boyutunun 8'in katları biçiminde olması gerekir. Örnek olarak örtü görüntüsünün boyutu 512×512 boyutunda ise bu görüntü 8×8 boyutunda 4096 alt görüntü bloğuna bölünür. Her bir alt görüntü bloğunda örtü görüntüsüne ait 64 piksellik parçalar bulunmaktadır. Şekil 3.3.'de 512×512 boyutunda bir örtü görüntüsü ve 4096 adet alt bloklara ayrılmış biçimi görülmektedir.



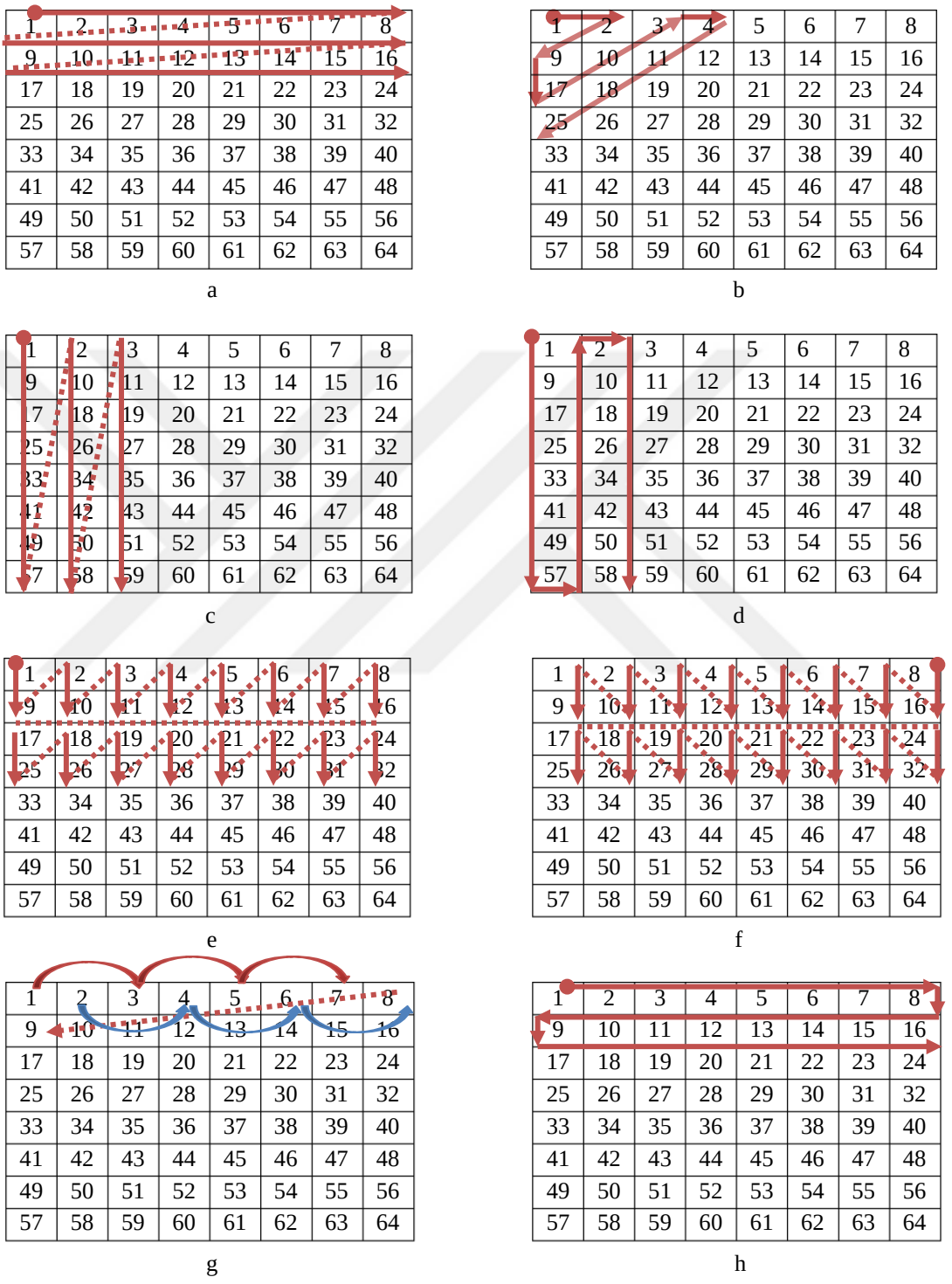
a b

Şekil 3.3. Örtü görüntüsü a) orijinal hali b) 8×8 boyutunda bloklara bölünmüş şekli

Gizlenecek verinin dizi biçimine dönüştürülmesi ve gruplara ayrılması; örtü görüntüsüne gizlenecek veri her türlü dosya biçiminde olabilir. Bu verinin gizleme işleminden önce ikili sayı (binary) biçimine dönüştürülmesi gerekmektedir. Bu dönüşüm sonunda gizlenecek veriler, "1" ve "0" dan oluşan eleman sayısı oldukça fazla bir boyutlu dizi olarak temsil edilir. Sonra dizi eleman sayısı L olacak şekilde gruplara ayrılır. L değeri örtü görüntüsünün bölüneceği alt blok sayısına göre değişmektedir. L ifadesinin alacağı değerler Tablo 3.9.'da verilmiştir.

Verinin gizlenebileceği alt örtü bloklarının tespit edilmesi; gizlenecek veri grupları ile örtü görüntüsünün alt blokları arasındaki en benzer olanlarının bulunması için

örtü görüntüsünün her bir bloğundaki piksellerin LSB değeri Şekil 3.4.'deki 8 adet piksel tarama sırasına göre taranır.



Şekil 3.4. Örtü görüntüsündeki bloklara veri gizlemede takip edilen tarama sıraları. a) Raster tarama b) Zig-Zag tarama c-h) Yeni tarama sıraları

Kullanılan tarama sıralarının ilk ikisi (Şekil 3.4.a ve 3.4.b) yaygın olarak kullanılan raster tarama sırası ve zig-zag tarama sırasıdır. Diğer altısı (Şekil 3.4.c−h) bu çalışmada tasarlanmış yeni tarama sıralarıdır.

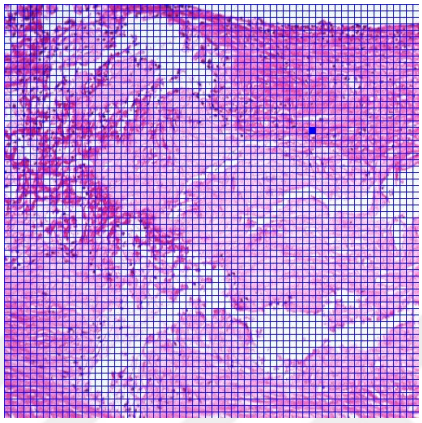
Tablo 3.1. Bloklardaki piksellerde izlenecek tarama sırası

Tarama Sırası	Piksel Sırası
a	1−2−3−4−5−6−7−8−9−10−11−12−13−14−15−16−17−18−19−20−21−22−23−24−25−26−27−28−29−30−31−32−33−34−35−36−37−38−39−40−41−42−43−44−45−46−47−48−49−50−51−52−53−54−55−56−57−58−59−60−61−62−63−64
b	1−2−9−17−10−3−4−11−18−25−33−26−19−12−5−6−13−20−27−34−41−49−42−35−28−21−14−7−8−15−22−29−36−43−50−57−58−51−44−37−30−23−16−24−31−38−45−52−59−60−53−46−39−32−40−47−54−61−62−55−48−56−63−64
c	1−9−17−25−33−41−49−57−2−10−18−26−34−42−50−58−3−11−19−27−35−43−51−59−4−12−20−28−36−44−52−60−5−13−21−29−37−45−53−61−6−14−22−30−38−46−54−62−7−15−23−31−39−47−55−63−8−16−24−32−40−48−56−64
d	1−9−17−25−33−41−49−57−58−50−42−34−26−18−10−2−3−11−19−27−35−43−51−59−60−52−44−36−28−20−12−4−5−13−21−29−37−45−53−61−62−54−46−38−30−22−14−6−7−15−23−31−39−47−55−63−64−56−48−40−32−24−16−8
e	1−9−2−10−3−11−4−12−5−13−6−14−7−15−8−16−17−25−18−26−19−27−20−28−21−29−22−30−23−31−24−32−33−41−34−42−35−43−36−44−37−45−38−46−39−47−40−48−49−57−50−58−51−59−52−60−53−61−54−62−55−63−56−64
f	8−16−7−15−6−14−5−13−4−12−3−11−2−10−1−9−24−32−23−31−22−30−21−29−20−28−19−27−18−26−17−25−40−48−39−47−38−46−37−45−36−44−35−43−34−42−33−41−56−64−55−63−54−62−53−61−52−60−51−59−50−58−49−57
g	1−3−5−7−9−11−13−15−17−19−21−23−25−27−29−31−33−35−37−39−41−43−45−47−49−51−53−55−57−59−61−63−2−4−6−8−10−12−14−16−18−20−22−24−26−28−30−32−34−36−38−40−42−44−46−48−50−52−54−56−58−60−62−64
h	1−2−3−4−5−6−7−8−16−15−14−13−12−11−10−9−17−18−19−20−21−22−23−24−32−31−30−29−28−27−26−25−33−34−35−36−37−38−39−40−48−47−46−45−44−43−42−41−49−50−51−52−53−54−55−56−64−63−62−61−60−59−58−57

Her blok için uygulanan 8 tarama sırası sonunda içerisinde 64 bit değer barındıran diziler biçiminde farklı LSB dizileri elde edilir. 4096 blok için 32768 LSB dizisi oluşturulur. Tarama sırasının sayısını arttırılmasıyla, gizlenecek veri grupları ile benzer blokların bulunma olasılığının yükseltilmesi ve bu sayede örtü görüntüsü içerisindeki bloklarda en az değişimin yapılması hedeflenmiştir. Şekil 3.4.'de

görülen, bloklardaki izlenecek tarama sırasına göre piksellerin tarama sıra numaraları Tablo 3.1.'de verilmektedir.

Şekil 3.5.'de örtü görüntüsü içerisindeki belirtilmiş bir bloğun piksellerinin R renk kanalı değerleri ve LSB değerleri görülmektedir.



a

248	251	252	250	254	254	248	246
252	250	249	250	254	254	237	242
248	247	246	244	249	249	241	243
240	242	244	240	241	240	246	246
243	247	248	244	238	240	246	249
248	252	253	244	243	241	249	251
247	250	253	242	244	241	247	242
242	244	244	235	235	241	240	238

b

0	1	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	1	1	1	1
0	0	0	0	1	0	0	0
1	1	0	0	0	0	0	1
0	0	1	0	1	1	1	1
1	0	1	0	0	1	1	0
0	0	0	1	1	1	0	0

c

Şekil 3.5. Örtü görüntüsünden örnek bir bloğa ait piksel bilgileri a) Örnek bir bloğun seçilmesi b) Seçilen bloğun R renk kanalı piksel değerleri c) Seçilen bloğun R renk kanalı piksellerinin LSB değerleri

Örtü görüntüsünün Şekil 3.4.'de ve Tablo 3.1.'de gösterilen tarama sıralarına göre Şekil 3.5.'de verilen örnek bloğun LSB dizileri Tablo 3.2.'deki gibi oluşturulur. Tablo 3.2.'ye bakıldığında klasik LSB yöntemi ile veri gizleme işlemlerinde ilk satırdaki dizilişe göre veriler gizlenir. Fakat 8 farklı tarama yolu ile veri gizlemede kullanılacak piksel sayısı arttırılmıştır. Bir sonraki başlıkta anlatılacak olan kurala göre bu 8 farklı tarama sırasından biri seçilecektir.

Tablo 3.2. Örtü görüntüsünün seçilen bloğuna ait piksellerin 8 tarama sırasına göre LSB değerleri

Tarama Sırası	LSB Değerleri
a	0100000000100010010011110000100011000001001011111010011000011100
b	0100000110100000000101000100011101000100010100100101001111111000
c	0000101010101000010001100000000100110101001001110110011000101100
d	0000101000010101010001101000000000110101111001000110011000110100
e	0010010000000100001000001110101010100100010101111000100101111000
f	0001000000011000101010110000100011010101000110100010110101100010
g	0000010100110010100001111101001010000000101100001001001100100110
h	0100000001000100010011110001000011000001111101001010011000111000

Farklı boyutlardaki örtü görüntülerinin 8×8 boyutunda alt bloklara bölünmesi sonucu oluşacak blok sayıları ve LSB dizileri bilgileri Tablo 3.3.'de verilmektedir. Örtü görüntüsü boyutu arttıkça, alt blok sayısı ve LSB dizi adeti de artmaktadır.

Tablo 3.3. Farklı boyuttaki örtü görüntülerine 8×8 boyutunda bloklara bölündüğünde elde edilen LSB dizi adeti

Örtü Görüntüsü Boyutu	8×8 Blok Sayısı	LSB Dizi Adeti
16×16	4	32
32×32	16	128
64×64	64	512
128×128	256	2048
256×256	1024	8192
512×512	4096	32768

Veri hazırlama işleminde yapılan alt bloklara bölme ve tarama sıralarının kullanılarak LSB dizilerinin oluşturulması geliştirilen yöntemi diğer yöntemlerden ayıran en önemli noktadır. Geliştirilen yöntemde gizli veri grupları farklı bloklarda gizlenmektedir. Bloklardaki verilerin bütünlüğünün sağlanması için her bir blokta gizli veriye ek olarak bir sonraki gizli veri gruplarının bilgileri de yer almaktadır. Bunu bir bağlı doğrusal bir liste olarak düşünebiliriz. Burada kullanılan alt blokların boyutunun 8×8'den daha küçük olması durumunda, alt blok sayısı artmakta ve buna bağlı olarak iş yükü artarak işlem süresi uzamaktadır. Ayrıca verilerin gizlenmesinde kullanılabilecek bit sayısında azalma olmaktadır. Alt blokların boyutunun 8×8'den

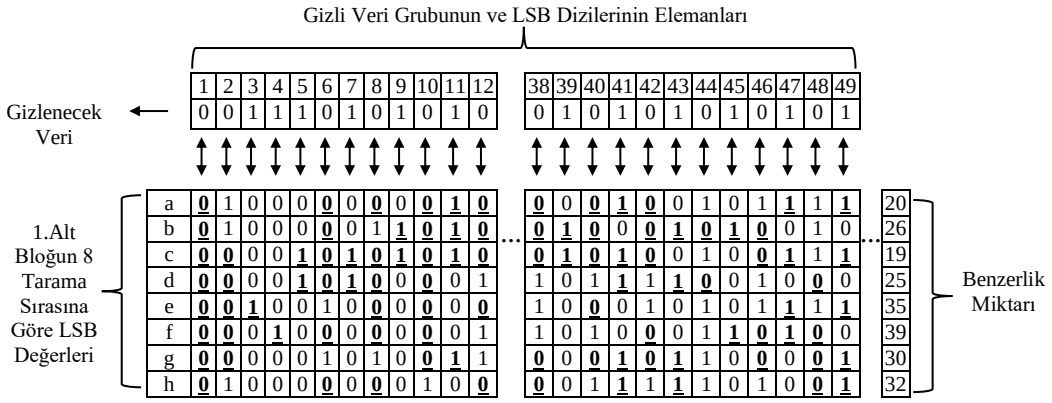
daha büyük olması durumunda ise benzerlik miktarının azalması söz konusudur. Çünkü karşılaştırılacak veri miktarı artmaktadır. Tarama sırası sayısının arttırılması ile örtü görüntüsünde gizlenebilecek yer sayısı/piksel sayısı çoğaltılmaktadır. Böylece en uygun yerin bulunma olasılığı arttırılmıştır.

3.2.2. Benzerlik miktarı hesaplanması

Veri hazırlama süreci sonunda örtü görüntüsünün elde edilen her LSB dizisi ile gizlenecek veri grupları arasındaki benzerlik miktarı bulunur. Böylece verilerin örtü görüntüsü içerisindeki en benzer alt bloklara gizlenmesi sağlanmaktadır.

Benzerlik miktarı; gizlenecek veri grubu bitlerinin, LSB dizisi içerisindeki sıralı olarak aynı olan bit sayısıdır.

Tespit edilen benzerlik miktarı, gizlenecek veri grubunun sıra numarası, LSB dizisinin ait olduğu blok numarası ve LSB dizisi oluşturulurken kullanılan tarama sırasının numarası bilgileri ile benzerlik tablosu oluşturulur. Şekil 3.6.'da benzerlik miktarının hesaplanmasına ait bir örnek verilmektedir. Burada gizlenecek 1.veri grubuna ait olan 64 elemanlı binary biçimindeki değerlerinin bir bölümü görülmektedir. Ayrıca örtü görüntüsünün 1. alt bloğuna ait Şekil 3.4.'deki tarama sıralarına göre ve Tablo 3.1.'deki değerlere göre elde edilmiş olan piksellerin R renk kanalına ait LSB dizisi değerlerinin bir bölümü görünmektedir. Gizlenecek veri grubunun her bir elemanı sırasıyla LSB dizilerinin elemanları ile karşılaştırılmıştır. LSB dizilerindeki aynı sırada aynı değere sahip olan elemanlar kalın ve altı çizgili olarak belirtilmiştir. 64 eleman içerisinde aynı olanların adeti her bir LSB dizisi için benzerlik miktarını oluşturmaktadır. Elde edilen bu benzerlik miktarları kullanarak benzerlik tablosu elde edilmektedir.



Şekil 3.6. Benzerlik miktarının hesaplanması

Tablo 3.4.'de ilk gizlenecek veri grubunun örtü görüntüsündeki ilk alt bloktaki tarama sırasına ve Şekil 3.6.'da verilen örneğe göre elde edilen örnek bir benzerlik tablosu çıktısı verilmiştir. Tablo 3.4.'deki verilere göre eğer ilk gizlenecek veri grubu 1. alt bloğun 1. tarama sırasına göre gizlenirse bu bloktaki 20 pikselin değeri değiştirilmeyecek yani 44 pikselin değeri değiştirilecektir. Eğer aynı alt bloğa 6.tarama sırasına göre veri gizleme yapılırsa 39 pikselin değeri değiştirilmeyecek yani sadece 25 pikselin değeri değiştirilecektir. Görüldüğü gibi 1.tarama sırasına göre eğer 6.tarama sırası seçilirse 19 pikselin değeri değiştirilmeyecektir.

Tablo 3.4. Örnek bir benzerlik tablosu çıktısı

Benzerlik Tablosu				
Sıra Numarası	Gizlenecek Veri Grubu Sıra Numarası	LSB Dizisinin Ait Olduğu Alt Blok Numarası	Benzerlik Miktarı	LSB Dizisinin Tarama Sırası
1	1	1	20	1
2	1	1	26	2
3	1	1	19	3
4	1	1	25	4
5	1	1	35	5
6	1	1	39	6
7	1	1	30	7
8	1	1	32	8

Tablo 3.5.'de farklı boyutlardaki örtü görüntülerine ait blok sayısı, bloklardan oluşturulan LSB dizisi sayısı, gizlenecek veri miktarının en az-en fazla bit olarak

miktarı ve bu verilerin bölüneceği en az-en fazla grup sayısı ve benzerlik tablosunun oluşturulduğundaki kayıt bilgileri verilmektedir. Gizlenecek veri 30 bitlik bir veri olsa dahi bu 30 bitlik verinin işgal edeceği blok sayısı 1'dir. Bundan dolayı tabloda gizlenecek en az bit sayısı 1 bloğa karşılık gelecek 64 bit olarak ifade edilmiştir. Gizlenecek en fazla veri miktarı ise örtü görüntüsünün sadece 1 renk kanalına gizlenebilecek veri miktarını belirtmektedir. Örneğin, 128×128 boyutunda 24 bpp renkli görüntüde 128×128=16384 adet piksel bulunmaktadır. Veri gizlemenin sadece R renk kanalına LSB yöntemiyle yapıldığı düşünülürse bu örtü görüntüsüne en fazla gizlenebilecek veri miktarı 16384 bit değerindedir. Bu 2048 bayt (2 KB) büyüklüğünde bir veriye karşılık gelmektedir. Tablodaki en fazla veri miktarları bu prensibe göre verilmiştir. Tabloda yer alan gizlenecek en fazla veri grubu sayısı ise örtü görüntüsünün 8×8 boyutunda alt bloklarının sayısından fazla olamaz.

Tablo 3.5. Örtü görüntüsü boyutlarına göre oluşacak benzerlik tablosu bilgileri

Örtü Görüntü Boyutu	8×8 Blok Sayısı	LSB Dizi Adeti	Gizlenecek Veri Miktarı				Benzerlik Tablosundaki Kayıt Sayısı	
			En Az (bit)	En Az Veri Grubu Sayısı	En Fazla (bit)	En Fazla Veri Grubu Sayısı	En Az	En Fazla
16×16	4	32	64	1	256	4	32	128
32×32	16	128	64	1	1024	16	128	2048
64×64	64	512	64	1	4096	64	512	32768
128×128	256	2048	64	1	16384	256	2048	524288
256×256	1024	8192	64	1	65536	1024	8192	8388608
512×512	4096	32768	64	1	262144	4096	32768	134217728

3.2.3. Veri gizleme

Gizlenecek ilk veri grubu için benzerlik tablosunda benzerlik miktarı yani bloktaki, gizlenecek veri grubu ile aynı sıradaki aynı eleman değeri adeti bilgisi, en yüksek olan satır seçilir. Tablo 3.4.'de verilen örneğe göre 6. sırada olan benzerlik miktarı bilgisi 39 olan satır 1. veri grubu için seçilir (Bu örnekte şuna dikkat edilmelidir; Tablo 3.4.'de sadece 1 adet gizlenecek veri grubunun 1 adet alt blok için benzerlik

tablosu verilmiştir). Bu seçme işlemi gizlenecek aynı veri grubunun bütün alt bloklardaki benzerlik miktarı en büyük olanının seçilmesi ile yapılacaktır. Gizlenecek veri grubundan sadece bir tanesinin gizlenecek bloğu bulunurken, örtü görüntülerinden 16×16 boyutundaki için 32 adet, 32×32 boyutundaki için 128 adet, 64×64 boyutundaki için 512 adet, 128×128 boyutundaki için 2048 adet, 256×256 boyutundaki için 8192 adet ve 512×512 boyutundaki için 32768 adet farklı benzerlik miktarı bilgisinden en büyük olan seçilecektir. Bu sayede klasik LSB yönteminde zorunlu olarak sadece 1 başlangıcı olan veri gizleme yerinin olasılık değeri arttırılmıştır.

Benzerlik tablosundan seçilen bu satır geçici yeni bir tabloda saklanır. 1. alt blok 1. veri grubu için kullanılacağından bir sonraki veri grupları için 1. blok seçilemez. 2. veri grubu için benzerlik tablosunda en büyük değerli satır seçilirken 1. bloğun olduğu satırlar bundan sonra dikkate alınmaz. Bu işlem en sonuncu veri grubuna kadar yapılır. Tablo 3.6.'da örnek olarak verilerin gizleneceği blok bilgileri verilmiştir.

Gizlenecek veri grubu sayısına göre, benzerlik tablosuna bakılarak elde edilen Tablo 3.6.'da tablonun ilk satırından itibaren gizli veri grupları örtü görüntüsünün ilgili alt bloğuna piksellerin LSB değeri değiştirilerek gizlenecektir. Tablo 3.6.'da verilen bilgiler kaynak alındığında gizlenecek 1. veri grubu, örtü görüntüsünün 54. alt bloğuna gizlenecektir. Gizleme işlemi yapılırken 6. tarama sırası yani Şekil 3.4'de "f" ile temsil edilen tarama sırasına göre veriler bloğun piksellerine gizlenecektir. Bu gizleme işlemi sırasında 64 pikselden sadece 25 pikselin LSB değeri değiştirilecektir. Aynı şekilde Tablo 3.6.'nın 6. satırına bakıldığında gizlenecek 6. veri grubu örtü görüntüsünün 134. alt bloğuna 8. tarama sırasına göre gizleme işlemi gerçekleştirilecektir. Bu gizleme işlemi sonucunda sadece 28 pikselin LSB değeri değiştirilecektir.

Tablo 3.6. 512×512 boyutundaki örtü görüntüsüne gizlenecek verilere ait bilgilerin bir kısmı

Gizlenecek Veriler Tablosu				
Sıra Numarası	Gizlenecek Veri Grubu Sıra Numarası	LSB Dizisinin Ait Olduğu Alt Blok Numarası	Benzerlik Miktarı	LSB Dizisinin Tarama Sırası
1	1	54	39	6
2	2	1000	37	6
3	3	1174	36	2
4	4	1649	38	8
5	5	3308	37	2
6	6	134	36	8
7	7	2745	35	5
8	8	3974	34	1
9	9	2767	37	7
10	10	3330	37	3
11	11	3943	36	4
12	12	3311	36	7
13	13	79	37	3
14	14	1344	37	4
15	15	2019	35	4
16	16	2685	38	7

İlk veri grubu örtü görüntüsünün alt bloğuna gizlenirken gizli veriye ek olarak, ikinci veri grubunun gizleneceği blok numarası ve gizlenirken takip edilecek tarama sırası bilgisi de bu bloğa gizlenir. Bloğa gizlenen bu veriler toplam 64 bit uzunluğundadır. Bölüm 3.2.1.'de anlatıldığı üzere gizlenecek veriler alt gruplara ayrılırken, alt grupların her birinin eleman sayısı L olacak şekilde belirlenmiştir. L değeri örtü görüntüsünün bölüneceği alt blok sayısına göre değişmektedir. Veri gizleme işlemi bit seviyesinde yapıldığı için, verilerin gizleneceği blok numarası ve gizlemede kullanılan tarama sırası bilgileri de ikili sayı sistemine çevrilerek gizleme işlemi yapılır.

Tablo 3.7.'de 8 farklı tarama sırasının veri gizlenirken kullanılan bit değerleri görünmektedir. Tarama sıralarının ondalık değerlerinden 1 çıkartılarak 1 bit tasarruf edilmiştir. Tarama sırasını örtü görüntüsünde saklayabilmek için her bir blokta 3 bitlik alan kullanılmaktadır.

Tablo 3.7. Veri gizlenirken kullanılan tarama sırası bilgileri

Tarama Sırası Numarası	İkili Sayı Sisteminde İfade Edilebilecek Değeri	Gizlenirken Temsil Edilen Ondalık Değeri	Gizlenirken Temsil Edilen İkili Sayı Sistemindeki Değeri
1	0001	0	000
2	0010	1	001
3	0011	2	010
4	0100	3	011
5	0101	4	100
6	0110	5	101
7	0111	6	110
8	1000	7	111

Tablo 3.8.'de ise alt blok numaralarını saklayabilmek için gerekli bilgiler verilmektedir. Tarama sırasında olduğu gibi burada da 1 bit tasarruf yapılabilmesi için blok adetlerinden 1 çıkartılmıştır. Böylelikle 512×512 boyutundaki örtü görüntüsünde 0000 0000 0000 bilgisi 1. alt bloğu temsil ederken 1111 1111 1111 bilgisi 4096. bloğu temsil etmektedir. Böylelikle 512×512 boyutundaki örtü görüntüsündeki 8×8 boyutunda oluşturulabilecek en fazla blok âdeti bilgileri temsil edilebilmektedir. 512×512 boyutundaki örtü görüntüsünü için gizlenecek verilerin blok numaralarının saklanabilmesi için her bir alt blokta tarama sırasına ek olarak 12 bitlik bir alan ayrılmalıdır.

Tablo 3.9.'da örtü görüntüsünün alt bloklarına gizlenecek verilerin tarama sırası ve blok numaralarına göre ihtiyaç duyulan bit sayıları verilmektedir. 512×512 boyutundaki örtü görüntüsünde her bir bloktaki gizlenen verilerin 49 biti asıl gizli mesajı oluştururken 15 bit ise bir sonraki verinin gizlenecek bloğun bilgisini içermektedir. Bu bir sonraki veriye ulaşmak için hazırlanan başlık bilgisi değeridir. 256×256 boyutundaki örtü görüntüsünün her bir alt bloğunda 13 bitlik başlık bilgisi

var iken 128×128 boyutundaki bir görüntüde bu değer 11 bit'dir. Başlık bilgisi uzunluğu ne olursa olsun örtü görüntüsünün her bir alt bloğuna toplamda 64 bit veri gizlenmektedir.

Tablo 3.8. Veri gizlenirken kullanılan alt blok numarası bilgileri

Örtü Görüntüsü Boyutu	Kullanılabilecek 8×8 Blok Sayısı		Temsil edilen bit değeri		Alabilecek farklı değer adeti	İhtiyaç duyulan bit adeti
	En Az	En Fazla	En Az	En Fazla		
16×16	1	4	00	11	4	2
32×32	1	16	0000	1111	16	4
64×64	1	64	00 0000	11 1111	64	6
128×128	1	256	0000 0000	1111 1111	256	8
256×256	1	1024	00 0000 0000	11 1111 1111	1024	10
512×512	1	4096	0000 0000 0000	1111 1111 1111	4096	12

Tablo 3.9. Gizli veri gruplarının eleman sayısının belirlenmesi

Örtü Görüntüsü Boyutu	Kullanılabilecek 8×8 Blok Sayısı		Alt Bloklar İçin İhtiyaç Duyulan Bit Adeti	Tarama Sırası İçin İhtiyaç Duyulan Bit Adeti	İhtiyaç Duyulan Toplam Bit Adeti	Gizlenecek Veri Gruplarındaki *L* Eleman Sayısı	Toplamda Gizlenecek Veri Miktarı (bit)
	En Az	En Fazla					
16×16	1	4	2	3	5	59	64
32×32	1	16	4	3	7	57	64
64×64	1	64	6	3	9	55	64
128×128	1	256	8	3	11	53	64
256×256	1	1024	10	3	13	51	64
512×512	1	4096	12	3	15	49	64

3.2.3.1 Veri gizleme sırasında karşılaşılabilecek özel durumlar

Bu bölümde veri gizleme işlemi başlamadan önce veya veri gizleme işlemi gerçekleştirilirken karşılaşılacak özel durumlar hakkında bilgi verilmektedir.

3.2.3.1.1. Anahtarlı ve anahtarsız veri gizleme

Bölüm 2.5.3.'de anlatıldığı ve Şekil 2.15.'de gösterildiği üzere bir steganografi sistemin genel yapısı içerisinde anahtar kullanımı olabilir. Geliştirilen yöntemde veri gizleme işlemi anahtarlı ve anahtarsız olarak 2 farklı biçimde gerçekleştirilmektedir. Eğer veri gizleme işlemi yapılırken anahtar kullanılacaksa, ilk veri grubunun hangi bloğa hangi tarama sırasına göre saklanacağı bilgisi bu anahtarı oluşturacaktır. Yani ilk veri grubunun başlık bilgisi anahtar olarak belirlenir. Tablo 3.9.'a bakıldığında örtü görüntüsünün boyutuna göre alt blok sayısı değişeceğinden bu başlık bilgisi en az 5 bit en fazla 15 bit uzunluğunda olacaktır. Bu anahtarın son 3 biti tarama sırasını vermektedir.

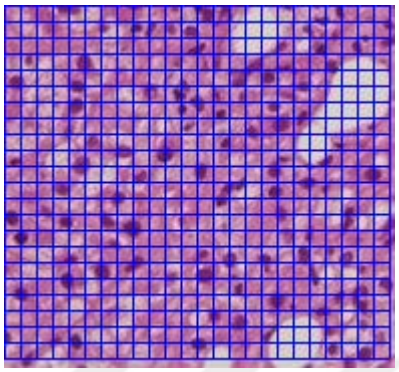
Eğer anahtar kullanılmadan veri gizleme işlemi yapılacaksa ilk veri grubunun saklanacağı blok bilgisinin nerede tutulacağı bir problem olarak ortaya çıkar. Bu problemi çözmek için anahtarsız veri gizleme yapılırken örtü görüntüsünün 1. alt bloğu gizlenecek 1. veri grubu için ayrılır. Anahtarsız veri gizleme ve çıkarma işleminde daima 1. bloktan 1. tarama sırası kullanılıp işlemler başlayıp yapılır. Anahtarsız veri gizlemede, benzerlik tablosu oluşturulurken örtü görüntüsünün 1. bloğu üzerinde işlemler yapılmaz.

3.2.3.1.2. Örtü görüntüsü boyutu ayarlanması

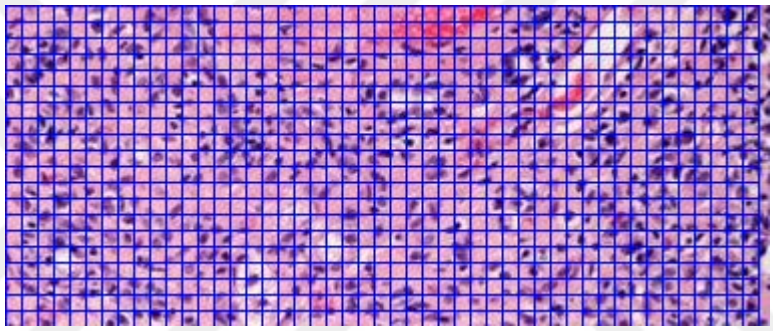
Geliştirilen yöntemin sağlıklı bir biçimde uygulanabilmesi, örtü görüntüsünün 8×8 boyutunda alt görüntülere ayrılabilmesi için örtü görüntüsünün boyutunun 8×8 matrisine uygun olması gerekmektedir. Eğer örtü görüntüsünün boyutu bu matrise uygun değilse bu boyuta en uygun küçük değerler sınır olarak alınır. Örneğin boyu 519×512 boyutunda bir örtü görüntüsü olursa, 8×8 boyutunda alt bloklara bölme işlemi sol üst köşeden (0,0) koordinatından başladığında 7 piksel değerinde örtü görüntüsünün genişliği kullanılamayacaktır.

Şekil 3.7. ve 3.8.'de boyutları 8'in katı olmayan görüntülere örnek verilmiştir. Görüntüler 8×8 boyutunda alt bloklara uygun bir biçimde bölündüklerinde sağ

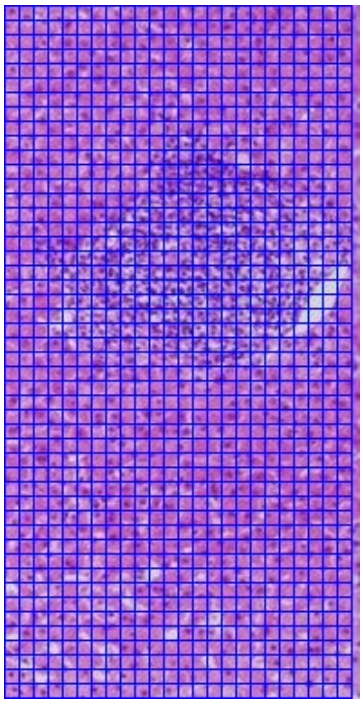
taraflarında veya alt taraflarında veri gizlemede kullanılmayan alanlar olabilmektedir. Veri gizlemede kullanılan alanlar mavi kenarlıklı olarak belirtilmişlerdir.



a

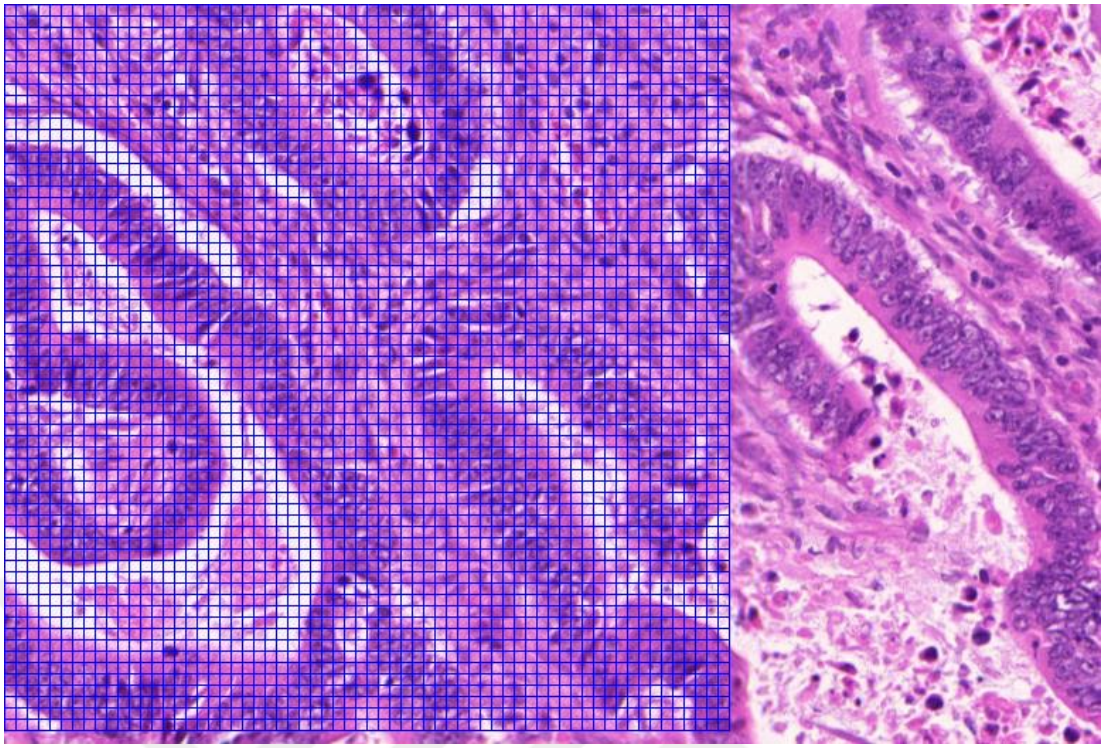


b



c

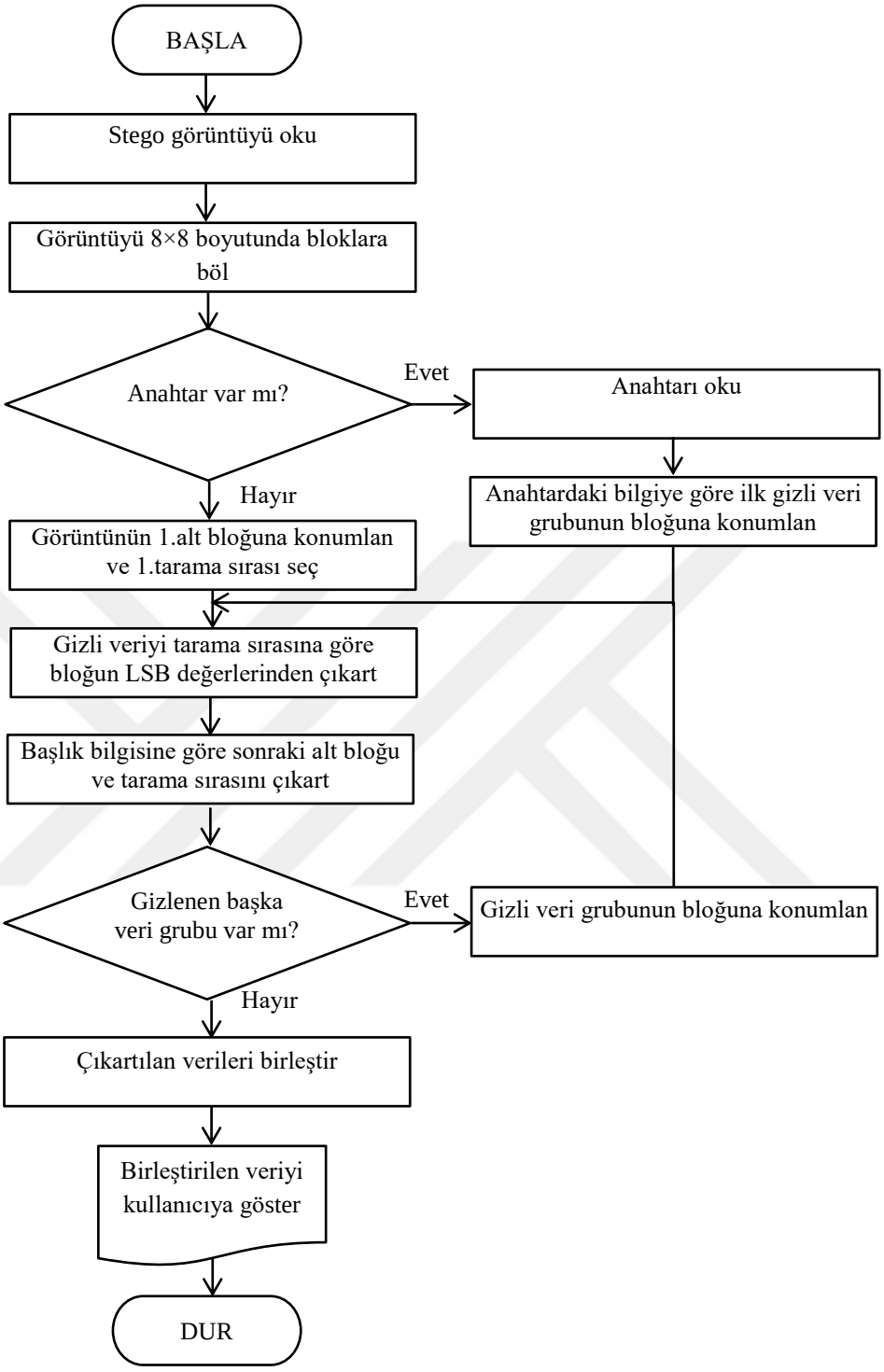
Şekil 3.7. Örtü görüntüsü 8×8 boyutunda alt bloklara ayrıldığında kullanılan blokların belirlenmesi a) 195×181 boyutunda, b) 382×160 boyutunda, c)197×385 boyutunda



Şekil 3.8. 775×522 boyutundaki örtü görüntüsü 8×8 boyutunda alt bloklara ayrıldığında kullanılan blokların belirlenmesi

3.2.4. Veri çıkartılması

Şekil 3.9.'da verilen veri çıkartma akış diyagramına göre stego görüntü okunduktan sonra görüntü 8×8 boyutunda alt bloklara bölünür. Veri gizlemede kullanılan anahtar bilgisine göre ilk veri grubunun gizli olduğu alt bloğa konumlama yapılarak uygun tarama sırasına göre gizli veri bitleri bloktan çıkarılır. Bloğun en sonunda yer alan bir sonraki bloğun konum ve tarama sırası bilgileri çıkartılarak gizlenen en son bloğa kadar veri çıkarma işlemi gerçekleştirilir. Çıkartılan verilerden başlık bilgileri dışındaki veriler birleştirilerek gizlenen veri geri elde edilir.



Şekil 3.9. Veri çıkartma akış diyagramı

3.3. Geliştirilen Veri Gizleme Yazılımı

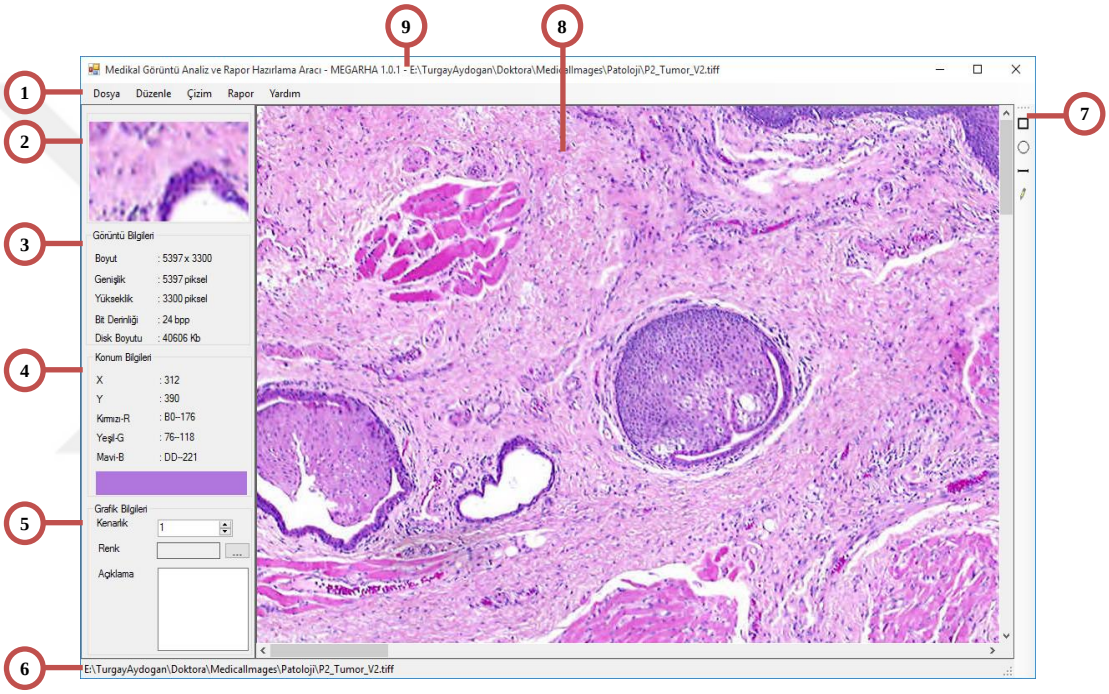
Tez çalışmasında geliştirilen veri gizleme yöntemini kullanan "Medikal Görüntü Analiz ve Rapor Hazırlama Aracı (MEGARHA)" adında bir uygulama yazılımı geliştirilmiştir. Bu uygulama yazılımı ile renkli (24 bpp) ve gri seviyeli (8 bpp) görüntüler için grafiksel ve metin içerikli rapor hazırlanıp aynı görüntü içerisine bu rapor gizlenebilmektedir. Gerçekleştirilen yazılım Visual Studio 2015 editöründe C# programlama dili kullanılarak geliştirilmiştir. Geliştirilen yazılımın ana ekran görüntüsü Şekil 3.10.'da görülmektedir. Ana ekran 9 kısımdan meydana gelmektedir. Bu kısımlar ve işlemleri;

1. Menü Çubuğu: Şekilde 1 ile numaralandırılmış kısımdır. Dosya, Düzenle, Çizim, Rapor ve Yardım adında ana menüleri içermektedir.
    a. Dosya ana menüsü altında Aç, Rapor Anahtarı Gir, Raporu Görüntü İçerisine Gizle, Son Belgeler ve Çıkış adında alt menüler bulunmaktadır. Aç menüsü ile raporu hazırlanacak veya içerisine önceden rapor gizlenen görüntü bilgisayarın depolama biriminden seçilerek program içerisinde ekranda gösterilir. Rapor Anahtarı Gir menüsü ile içerisine önceden rapor girilen görüntü açıldıktan sonra raporun gösterilebilmesi için rapor anahtarı var ise bu menü yardımıyla veri girişi yapılır ve girilen anahtarın doğrultusunda rapor görüntü üzerinde gösterilir. Üzerinde işlem yapılan son 10 tıbbi görüntüye hızlı ulaşmak için Son Belgeler adındaki menü kullanılır. Çıkış adındaki menü ile program sonlandırılır.
    b. Düzenle ana menüsü altında Hepsini Seç, Sil, Geri ve İleri adında alt menüler bulunmaktadır. Bu menüler raporu hazırlanacak olan tıbbi görüntü üzerinde çizilmiş olan grafiksel çizimlerin düzenlenmesi için kullanılmaktadır. Görüntü üzerinde yer alan bütün grafiksel çizimleri seçmek için Hepsini Seç menüsü kullanılır. Seçili olan çizimi silme işlemi Sil adındaki menü ile gerçekleştirilir. Geri menüsüyle çizim işlemlerinde yapılan en son işlem iptal edilmektedir. İleri menüsü ise tam tersi işlemle geri alınan işlemi yenileme gerçekleştirilir.

c. Çizim menüsü altında Dikdörtgen, Elips, Çizgi ve Kalem adında görüntü üzerine çizilebilecek çizimleri belirleyebildiğimiz alt menüler vardır. Görüntü üzerine dikdörtgen çizmek için Dikdörtgen adındaki menü, elips çizmek için Elips adındaki menü, çizgi çizmek için Çizgi adındaki menü ve serbest çizimler yapmak için ise Kalem adındaki menü kullanılır.
d. Rapor ana menüsü altında Raporu Ekran Üzerinde Gizle, Raporu Ekran Üzerinde Göster, Raporu Görüntü İçerisine Gizle ve Hasta-Rapor Bilgileri adında alt menüler yer almaktadır. Görüntü üzerindeki raporu anlık olarak ekrandan gizlemek ve göstermek için ilk iki alt menü kullanılır. Hasta-Rapor Bilgileri menüsü ile tıbbi görüntünün ait olduğu hasta bilgileri ve tıbbi görüntüye ait metin içerikli rapor bilgilerinin veri girişinin yapılacağı pencere açılmaktadır. Raporu görüntüye gizlemek için ise Raporu Görüntü İçerisine Gizle menüsü kullanılır.
e. Yardım ana menüsü altında ise Hakkında menüsü bulunur. Bu menü ile açılan yeni pencerede program hakkında bilgi verilir.

2. Yakınlaştırma: Şekilde 2 ile numaralandırılmış kısımdır. Raporu hazırlanacak görüntü üzerinde çizim işaretçisinin üzerinde bulunduğu görüntünün 140×70 piksel boyutunda parçasını alıp daha büyük bir oranda görüntülenmesini sağlar. Bu sayede rapor hazırlayacak uzman kişiye detayların daha iyi görünmesini sağlamaktadır.
3. Görüntü Bilgileri: Şekilde 3 ile numaralandırılmış kısımdır. Açılan tıbbi görüntünün temel dosya bilgilerinin verildiği kısımdır.
4. Konum Bilgileri: Şekilde 4 ile numaralandırılmış kısımdır. Raporu hazırlanacak görüntü üzerinde çizim işaretçisinin üzerinde bulunduğu piksel ile ilgili konum ve renk bilgilerinin verildiği bölümdür.
5. Çizim Bilgileri: Şekilde 5 ile numaralandırılmış kısımdır. Raporda yer alacak çizimlere ait bilgilerin ulaşıldığı ve değiştirilebildiği kısımdır.
6. Durum Çubuğu: Şekilde 6 ile numaralandırılmış kısımdır. Raporu hazırlanacak görüntünün bilgisayarda bulunduğu fiziksel adresin yolunu göstermektedir.

7. Çizim Araç Çubuğu: Şekilde 7 ile numaralandırılmış kısımdır. Görüntü üzerinde şekillerin çiziminin yapılabilmesi için kullanılan araç çubuğudur. Bu araç çubuğu sayesinde görüntü üzerinde dikdörtgen, elips, çizgi ve serbest çizim yapılabilmektedir.
8. Rapor Alanı: Şekilde 8 ile numaralandırılmış kısımdır. Raporu hazırlanacak görüntünün programda görüntülendiği ve çizimlerin yapıldığı alandır.
9. Başlık Çubuğu: Şekilde 9 ile numaralandırılmış kısımdır. Programın adı ve üzerinde işlem yapılan belgenin adının görüntülendiği alandır.



Şekil 3.10. Veri gizleme ve çıkarma işleminde kullanılan uygulama yazılımı

3.3.1. Geliştirilen veri gizleme yazılımı ile verinin gizlenmesi

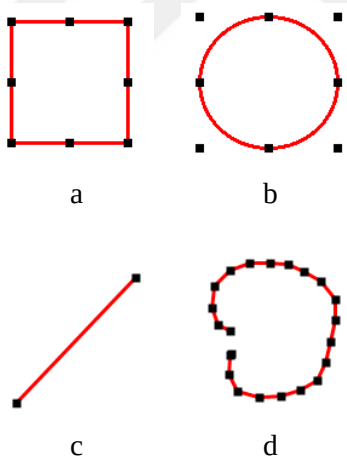
Geliştirilen yazılım ile görüntüler üzerinde yapılan geometrik şekilsel işaretlemeler, bu şekillere ait açıklamalar ve hasta ile ilgili temel bilgileri barındıran bir sınıf tasarlanmıştır. Bu sınıfta şekillere ait başlangıç koordinatı, bitiş koordinatı, genişlik, uzunluk, kenarlık kalınlığı, kenarlık çizgi rengi, açıklama bilgisi ve hasta bilgileri uygun veri tiplerine göre bir sınıf içerisinde oluşturulmuştur. .Net Framework'ün sağladığı İkili Serileştirme (Binary Serialization) sayesinde bu sınıf kullanılırken oluşturulan nesne byte tipinde bir diziye dönüştürülmektedir. Gizleme işlemi

sırasında bu dizi binary biçime dönüştürülüp gizlenecek veri grupları oluşturulmaktadır.

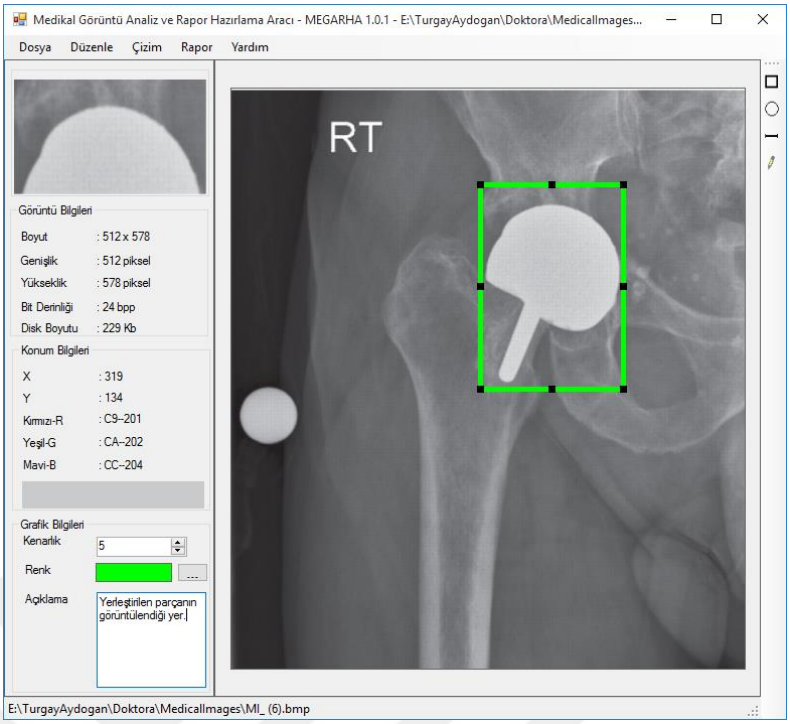
Geliştirilen program ile veri gizleme işlemi 3 adımda yapılmaktadır;

1. Görüntünün Açılması: Bu adımda Dosya ana menüsü altındaki Aç menüsü ile raporu hazırlanacak veya içerisine önceden rapor gizlenen görüntünün bilgisayarın depolama biriminden seçilerek program içerisinde ekranda gösterilir.
2. Raporun Hazırlanması: Tıbbi görüntüye ait olan raporun hazırlanması için Şekil 3.11.'de gösterilen çizimler görüntü üzerine eklenebilmektedir. Eklenen bu çizimler menüler yardımı ile silinip, şekillere ait kenarlık kalınlığı, renk değeri ve metin açıklamaları değiştirilebilmektedir. Şekil 3.12.'de tıbbi bir görüntüye eklenen örnek bir şekil ve açıklaması görünmektedir. Buna benzer şekiller ve açıklamalar geliştirilen yazılım sayesinde tıbbi görüntülere rahatlıkla eklenebilmektedir. Ayrıca çizim alanında çizim işaretçisi kullanılarak şekil seçildikten sonra Şekil 3.12.'de görüldüğü gibi şekle özgü olarak şekillerin üzerinde beliren siyah kareler kullanılarak konumu ve ölçüleri değiştirilebilmektedir. Şekil 3.13.'de görüldüğü gibi hasta ve tıbbi görüntüye ait bazı bilgilerin veri girişi yapılabilir.
3. Veri Gizleme: Hazırlanan raporun görüntüye gizlenebilmesi için veri gizleme seçeneklerinin belirlenmesi gerekmektedir. Bu seçeneklere ulaşmak için Rapor ana menüsü altında Raporu Görüntü İçerisine Gizle menüsü kullanılarak Şekil 3.14.a.'daki pencere açılır. Açılan bu pencerede Sıkıştırma, Şifreleme, Veri Gizleme Anahtarı, Veri Gizleme Yöntemi, Raporu Görüntüye Gizle ve Analiz adında bölümler yer almaktadır. Kullanıcı isteğe göre tıbbi görüntü içerisine gizlenecek rapor verisini gizleme işleminden önce yaygın olarak kullanılan GZip algoritması ile sıkıştırabilir veya kendisinin belirleyeceği şifre ile 3DES algoritmasını kullanarak şifreleyebilir. Veri Gizleme Anahtarı bölümünde rapora göre elde edilecek olan stego anahtarını görüntü içerisine gizleme veya görüntü dışında kalması ile ilgili seçenekler yer almaktadır. Stego anahtarı görüntü içerisine gizlenmesi seçeneği işaretlenirse örtü görüntüsünün ilk bloğu sadece stego anahtarı için ayrılır.

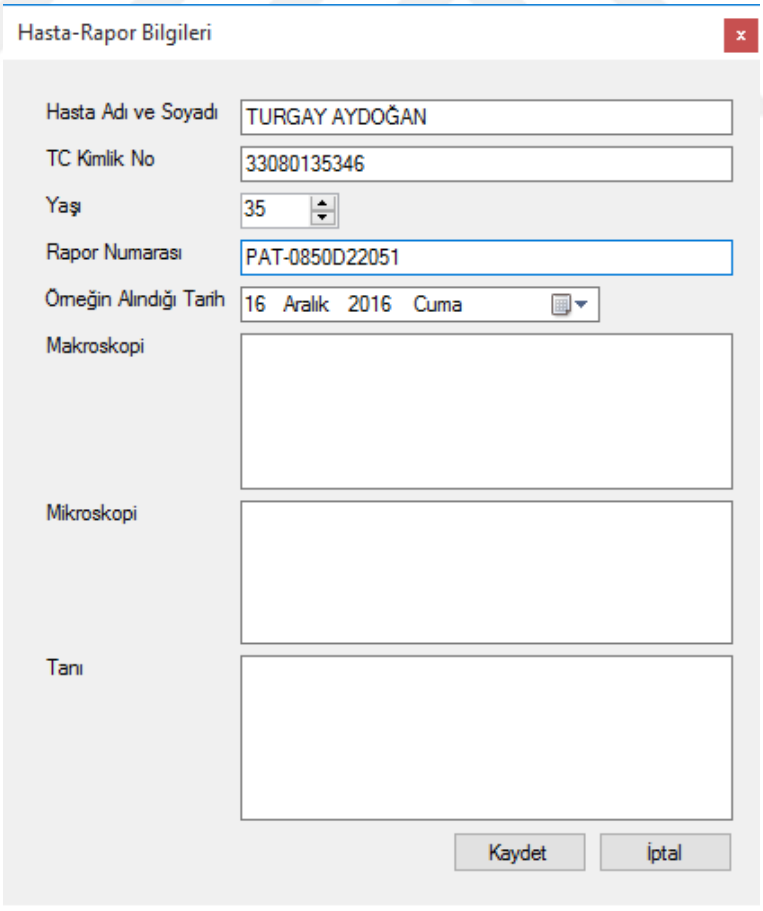
Fakat diğer seçenek işaretlendiğinde stego anahtar veri gizleme işlemi sonunda kullanıcıya karakter dizisi olarak gösterilir. Son olarak kullanıcı istediği veri gizleme yöntemlerinden bir tanesini seçip üzerinde Raporu Görüntüye Gizle yazan düğme ile işlemi sonlandırır. Veri gizleme işlemi gerçekleştirilirken Şekil 3.14.b.'deki ekran görüntüsündeki işlem çubuğu ile kullanıcıya işlemlerin bitirilme oranlarıyla ilgili görsel bilgi verilir. Veri gizleme işlemi tamamlandıktan sonra işlem çubuğu olan pencere kapanır ve veri gizleme işlemi gerçekleştirilmiş olunur. İşlem sonucunda program tarafından, içerisinde raporun bulunduğu stego görüntüsü ve bazı istatistiksel bilgilerin yer aldığı belgeler üretilir. Bu belgeler programın bilgisayarda kurulu olduğu fiziksel adreste, üzerinde işlem yapılan tıbbi görüntünün adı ve işlem tarihinden oluşan bir adla klasör içerisine kaydedilir. Ayrıca Analiz bölümünde stego görüntüsü ile ilgili bazı istatistiksel bilgiler gösterilmektedir. Bunlar hakkında bir sonraki bölümde detaylı bilgi verilmektedir.



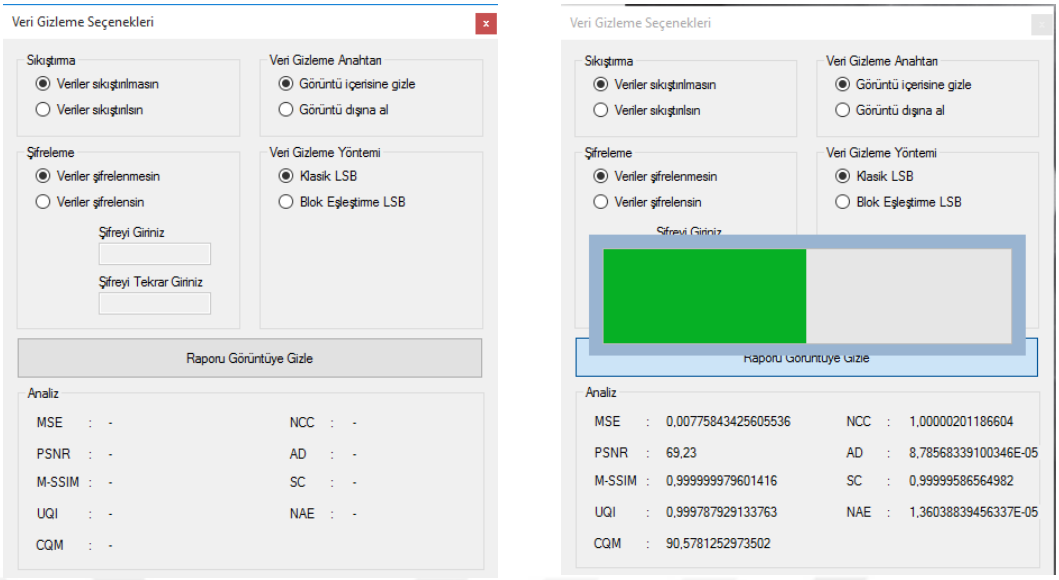
Şekil 3.11. Rapor hazırlama esnasında kullanılan geometrik şekiller a)Dikdörtgen, b) Elips, c) Çizgi ve d) Serbest çizim yapılabilen Kalem



Şekil 3.12. Örnek bir tıbbi görüntü ile üzerine eklenen çizim bilgisi ve bu çizimlere ait metin bilgisi



Şekil 3.13. Örnek bir tıbbi görüntüye ait hasta bilgileri



a b

Şekil 3.14. Veri gizleme seçeneklerinin olduğu pencereye ait ekran görüntüsü. a) Veri gizleme işlemi gerçekleşmeden önce istenilen seçeneklerin belirlendiği ekran görüntüsü, b) Seçenekler belirlendikten sonra veri gizleme işlemi gerçekleşirken programın ekran görüntüsü

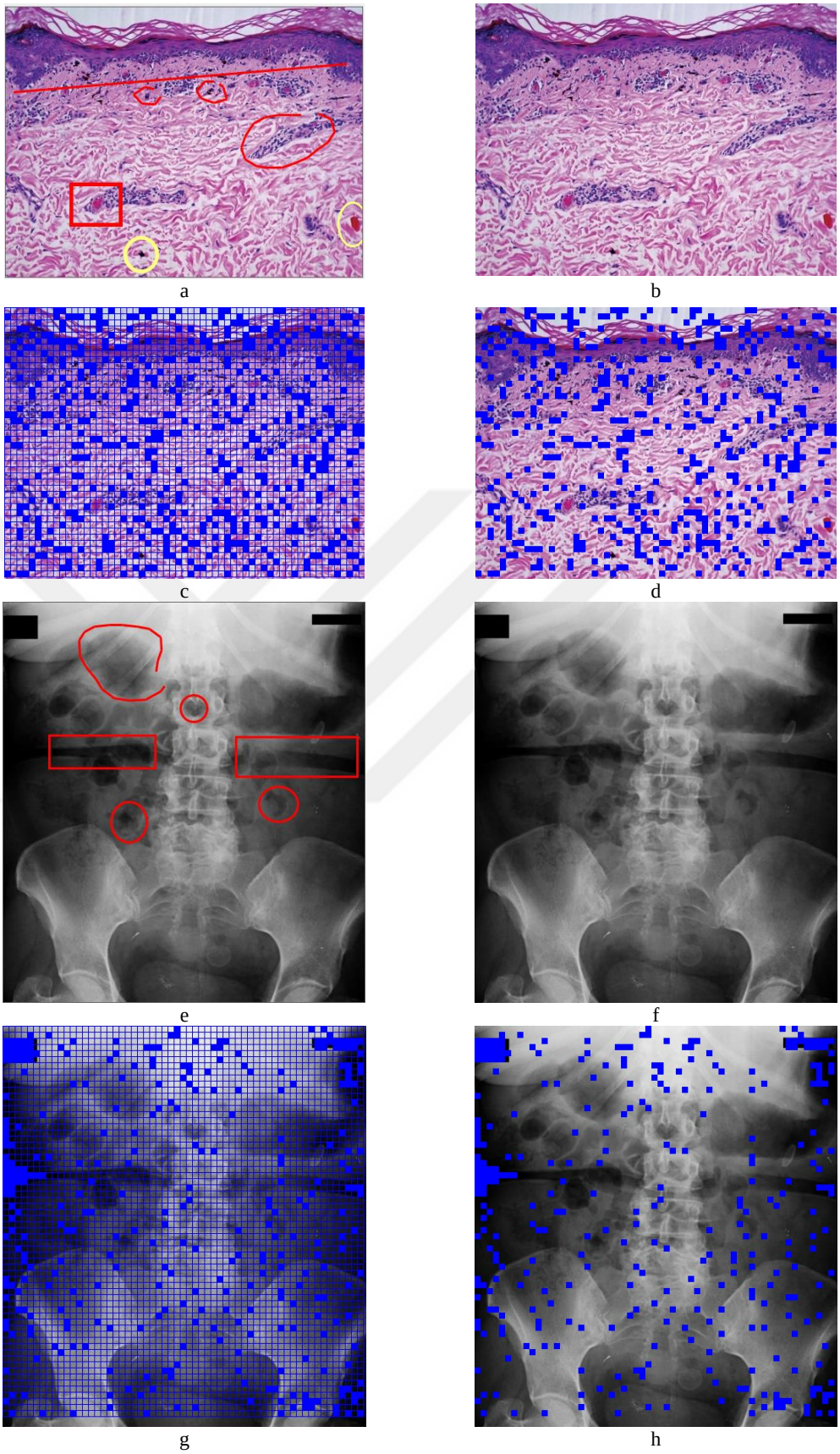
Veri gizleme sonucu içerisinde rapor bulunan stego görüntülere ait bazı örnekler Şekil 3.15.'de görülmektedir. Şekil 3.15.a.'da örnek bir patoloji görüntüsü üzerine hazırlanan rapor görünmektedir. Veri gizleme işleminden sonra raporu içerisinde barındıran stego görüntü Şekil 3.15.b.'de görünmektedir. Stego görüntüde değişiklik yapılan piksellerin blokları ise Şekil 3.15.c. ve Şekil 3.15.d.'de görünmektedir. Şekil 3.15.e.'de ise başka bir tıbbi görüntüye ait rapor görülmektedir. Şekil 3.15.f.'de raporu içerisinde barındıran tıbbi görüntü, Şekil 3.15.g. ve Şekil 3.15.h.'de rapor verisinin gömüldüğü bloklar gösterilmektedir.

Geliştirilen yazılım ile üst bölümlerde anlatıldığı üzere veri sıkıştırma, veri şifreleme ve farklı veri gizleme algoritmalarının kullanılması gibi seçeneklerin kullanıcı tarafından belirlenmesi istenilmektedir. Seçeneklerin belirlenmesinden sonra rapor bilgisi örtü görüntüsüne gizlenmektedir. Bu gizleme işleminde hangi seçeneklerin kullanıldığı bilgisine, stego görüntüden verileri çıkartırken yani raporu geri elde ederken ihtiyaç duyulacaktır. İhtiyaç duyulacak bu bilgiler için "*Başlık Bilgisi*" adı altında bir anahtar oluşturulmaktadır. Bu anahtar kullanıcının veri gizleme işlemini gerçekleştirmeden önce veri gizleme seçeneklerinde "Görüntü içerisine gizle" veya "Görüntü dışına al" olarak iki farklı biçimde sorulmaktadır. Eğer kullanıcı "Görüntü

içerisine gizle” seçeneğini seçerse örtü görüntüsünün ilk bloğu sadece başlık bilgisi için ayrılır. Fakat “Görüntü dışına al” seçeneği işaretlendiğinde ise başlık bilgisi bir stego anahtar olarak veri gizleme işlemi sonunda kullanıcıya karakter dizisi olarak verilir. Kullanıcı bu stego anahtara ulaşmak için görüntünün kaydedildiği bilgisayarın fiziksel adresinde “StegoKey.txt” dosyası içerisinden ulaşabilmektedir. Oluşturulacak bu başlık bilgisinin bit değerleri Tablo 3.9.’da verilmiştir. Fakat Tablo 3.9.’da verilen başlık bilgisi bit değerleri geliştirilen veri gizleme yönteminin genel kullanımı içindir. Bu kullanıma ek olarak geliştirilen veri gizleme yazılımının veri sıkıştırma, veri şifreleme ve farklı veri gizleme algoritmaları gibi seçenekleri de dahil edildiğinde yeni başlık bilgisi bit değerleri Tablo 3.10.’da verilmiştir.

Başlangıç bloğunun numarasını belirtmek için en az 2 en fazla 12 bite ihtiyaç vardır. 8 farklı tarama sırasından hangisinin kullanıldığı temsil etmek için 3 bite ihtiyaç duyulmakta, veri sıkıştırıldıysa “1” sıkıştırılmadıysa “0” ile ifade edilecektir, bundan dolayı veri sıkıştırma için başlık bilgisinde 1 bite ihtiyaç vardır. Aynı biçimde şifreleme işlemi yapıldıysa bunu “1” ile ifade edip yapılmadıysa “0” ile ifade edilmiştir.

Kaç blokta veri gizleme yapılacağı bilgisi için en az 2 en fazla 12 bite ihtiyaç vardır. Her blokta 64 bitin gizlenebildiği için veri gizleme yapılan en son blokta kaç bitin kullanıldığı bilgisini en fazla 6 bit ile temsil edilmektedir. Böylece örtü görüntüsünün boyutuna göre başlık bilgisi toplamda en az 16 bit, en fazla ise 36 bit değerinde olmaktadır.



a b c d e f g h

Şekil 3.15. Geliştirilen yazılım kullanılarak hazırlanan rapor, elde edilen stego görüntü örnekleri ve verilerin gizlendiği alt bloklar

Tablo 3.10. Geliştirilen yazılımda kullanılan başlık bilgisi bit değerleri

Açıklama	Değerler					
Örtü Görüntüsü Boyutu	16×16	32×32	64×64	128×128	256×256	512×512
Başlangıç Bloğunu Numarası	2	4	6	7	10	12
Tarama Sırası Numarası	3	3	3	3	3	3
Veri Sıkıştırma Bilgisi	1	1	1	1	1	1
Şifreleme Bilgisi	1	1	1	1	1	1
Veri Gizleme Yöntemi Numarası	1	1	1	1	1	1
Kaç Blok Gizleme Yapılacak Bilgisi	2	4	6	7	10	12
En Son Blokta Kaç Bit Veri Gizlenecek Bilgisi	6	6	6	6	6	6
İhtiyaç Duyulan Toplam Bit Âdeti	16	20	24	26	32	36

Tablo 3.11., Tablo 3.12. ve Tablo 3.13.'de gösterilen başlık bilgisi Tablo 3.10.'da belirtilen seçeneklere göre elde edilmiş bazı başlık bilgileri gösterilmiştir. Bu başlık bilgileri bir sonraki bölümde anlatılacak olan veri çıkarma işleminde kullanılarak stego görüntü içerisinden raporun okunmasına olanak sağlayacaktır. Tablo 3.11.'de 128×128 boyutundaki örtü görüntüsü için elde edilen başlık bilgisi görünmektedir. Tablo 3.10.'a bakıldığında 128×128 boyutundaki örtü görüntüsü için 26 bit değerinde bir başlık bilgisine ihtiyaç vardır. Tablo 3.11., Tablo 3.12. ve Tablo 3.13.'e bakıldığında ise Başlangıç Bloğu Numarası, Tarama Sırası Numarası, Kullanılan Veri Gizleme Yöntemi Numarası, Kaç Blok Gizleme Yapılacak Bilgisi ve En Son Blokta Kaç Bit Veri Gizlenecek Bilgisi değerlerinden 1 çıkartılmaktadır. Böylelikle her birinden birer bit tasarruf edilerek başlık bilgisinin gereksiz yere uzamasının önüne geçilmiştir.

Tablo 3.11. 128×128 boyutundaki örtü görüntüsünün başlık bilgisine bir örnek

	Değeri	Ondalık Değeri	Bit Değeri
Başlangıç Bloğunu Numarası	95	95−1 = 94	101 1111
Tarama Sırası Numarası	8	8−1 = 7	111
Veri Sıkıştırma Olacak mı?	Evet	1	1
Şifreleme Olacak mı?	Hayır	0	0
Kullanılan Veri Gizleme Yöntemi Numarası	1	1−1 = 0	0
Kaç Blok Gizleme Yapılacak Bilgisi	15	15−1 = 14	000 1110
En Son Blokta Kaç Bit Veri Gizlenecek Bilgisi	20	20−1 = 19	01 0011
Başlık Bilgisi	1011111 −111− 1− 0 − 0 − 0001110 − 010011		

Tablo 3.12. 256×256 boyutundaki örtü görüntüsünün başlık bilgisine bir örnek

	Değeri	Ondalık Değeri	Bit Değeri
Başlangıç Bloğunu Numarası	2	2−1 = 1	00 0000 0001
Tarama Sırası Numarası	1	1−1 = 0	000
Veri Sıkıştırma Olacak mı?	Hayır	0	0
Şifreleme Olacak mı?	Hayır	0	0
Kullanılan Veri Gizleme Yöntemi Numarası	2	2−1 = 1	1
Kaç Blok Gizleme Yapılacak Bilgisi	250	250−1 = 249	1111 1001
En Son Blokta Kaç Bit Veri Gizlenecek Bilgisi	30	30−1 = 29	01 1101
Başlık Bilgisi	0000000001− 000 − 0− 0 −1 − 11111001− 011101		

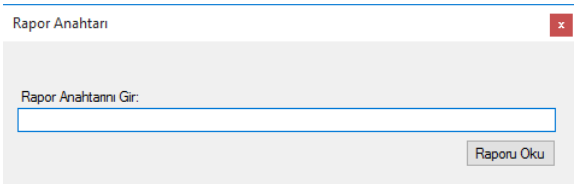
Tablo 3.13. 512×512 boyutundaki örtü görüntüsünün başlık bilgisine bir örnek

	Değeri	Ondalık Değeri	Bit Değeri
Başlangıç Bloğunu Numarası	260	260−1 = 259	0001 0000 0011
Tarama Sırası Numarası	5	5−1 = 4	100
Veri Sıkıştırma Olacak mı?	Evet	1	1
Şifreleme Olacak mı?	Evet	1	1
Kullanılan Veri Gizleme Yöntemi Numarası	2	2−1 = 1	1
Kaç Blok Gizleme Yapılacak Bilgisi	60	60−1 = 59	0 0011 1011
En Son Blokta Kaç Bit Veri Gizlenecek Bilgisi	15	15−1 = 14	00 1110
Başlık Bilgisi	000100000011−100 −1− 1 − 1 − 000111011− 001110		

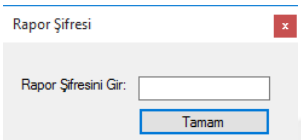
3.3.2. Geliştirilen veri gizleme yazılımı ile gizli verinin çıkarılması

Uygulama yazılımı ile açılan bir görüntüdeki raporu ekranda görüntülemek için Dosya ana menüsü altındaki Aç, alt menüsü kullanılarak rapor içeren bir görüntü açıldığında Şekil 3.16.'daki pencere açılır. Bu pencerede eğer başlık bilgisi anahtar olarak var ise bu bilgi girilir ve girilen anahtara göre rapor stego görüntü içerisinden çıkartılıp ekranda gösterilir. Eğer anahtar bilgisi yok ise her hangi bir veri girişi yapılmasına ihtiyaç olmadan görüntü açılır. Bu işlem ile stego görüntünün ilk bloğundan başlık bilgisi okunur ve stego görüntü içerisindeki rapor çıkartılıp ekranda gösterilir. Girilen anahtara veya ilk blokta okunan başlık bilgisine göre eğer şifreleme kullanılmışsa Şekil 3.17.'deki pencere kullanıcının karşısına çıkar ve

kullanıcıdan şifre girmesi istenir. Kullanıcı doğru şifreyi girer ise stego görüntü içerisindeki rapor çıkartılıp ekranda gösterilir.



Şekil 3.16. Stego görüntüye ait anahtar bilgisinin girileceği ekran görüntüsü



Şekil 3.17. Okunan başlık bilgisine göre eğer şifreleme yapılmış ise ekrana çıkan şifre girme penceresine ait ekran görüntüsü

3.4. Sonuç

Bu bölümde geliştirilen veri gizleme yöntemi ve bu yöntemi kullanılarak oluşturulan yazılım hakkında bilgi verilmiştir. Gizleme işlemi için ilk önce gizlenecek veriye en uygun yer bulunması ile ilgili adımlar gerçekleştirilmiş ve bulunan en uygun yerlere göre LSB yöntemi kullanılarak veri gizleme işlemi gerçekleştirilmiştir.

Geliştirilen yöntemin kullanılabilirliği ve test işlemleri için Visual Studio 2015 editöründe C# programlama dili kullanılarak bir yazılım geliştirilmiştir. Bu yazılım sayesinde ister patolojik görüntü olsun ister farklı cihazlar ile elde edilmiş tıbbi görüntüler olsun bu görüntüler üzerinde inceleme, analiz ve geometrik şekilsel çizimler yapılmasına olanak sağlayan bir araç oluşturulmuştur. Bu yazılım sayesinde 24 bpp değerindeki tıbbi görüntülere 2 farklı veri gizleme yöntemi kullanılarak veri gizleme işlemi gerçekleştirilebilmektedir.

Geliştirilen yöntemlerin başarım analizleri yine programda sayısal olarak gösterilmektedir. Bu başarım analizleri ile ilgili detaylı bilgi bir sonraki bölümde verilmiştir.

BÖLÜM 4. GELİŞTİRİLEN ALGORİTMAYA AİT BAŞARIM DEĞERLENDİRMELERİ

4.1. Giriş

Sayısal bir görüntü içerisine yapılan veri gizleme işlemi sonunda, veri gizlenen sayısal görüntüde ilk haline göre bozulmaların oluşması kaçınılmaz bir sonuçtur. Veri gizleme yöntemi uygulanırken bu bozulmaların en az olması ve fark edilememesi amaçlanır. Literatürde yer alan veri gizleme çalışmalarında bozulmaların sayısal olarak incelenmesi ve değerlendirilmesi adına MSE ve PSNR sayısal ölçütleri kullanılmaktadır (Yalman, 2010).

Geliştirilen yöntem/algoritma ilk olarak insan görme sistemine odaklanan görsel karşılaştırma ile orijinal ve stego görüntüler kıyaslanmıştır. Sonrasında, histogram grafiklerinin incelenmesi, Piksel Bozulma Oranlarının hesaplanması yapılmış ve sayısal içerikli olan istatiksel görüntü kalite ölçütlerinden MSE, PSNR, Evrensel Görüntü Kalite İndeksi, Ortalama Yapısal Benzerlik, Renkli Görüntü Kalite Ölçütü, Ortalama Fark, Yapısal İçerik, Normalize Karşıt Korelasyon ve Normalize Mutlak Hata değerleri analiz edilmiştir. Ayrıca, geliştirilen veri gizleme algoritmasının steganaliz ataklarına/saldırılarına karşı olan başarımı ise Stegdetect ve Stegspy araçları kullanılarak yapılmıştır.

Bu tez çalışmasında kullanılan patoloji görüntüleri ve diğer tıbbi görüntüler Amerika Birleşik Devleti'nde bulunan Ulusal Sağlık Enstitüsü (National Institutes of Health − NIH) biyomedikal araştırma merkezinin bünyesinde yer alan OPENI (Open Access Biomedical Image Search Engine) biyomedikal görüntü arama motorundan elde edilmiştir. Bu biyomedikal görüntü arama motoruna https://openi.nlm.nih.gov/ web adresinden ulaşılabilmektedir. Ayrıca görüntü işleme çalışmalarında literatürde yaygın olarak kullanılan Lena, Tiffany, Baboon, F16, Sailboat on Lake (Lake),

Peppers ve House adındaki standart test görüntülerine Güney Kaliforniya Üniversitesi (University of Southern California) bünyesinde yer alan ve 1977'den bu yana kullanılan USC-SIPI Görüntü Veritabanı (USC-SIPI Image Database)'ndan ulaşılmıştır. USC-SIPI Görüntü Veritabanı'na http://sipi.usc.edu/database/ web adresinden ulaşılabilmektedir. Test işlemlerinde 24 bit ve 8 bit renk derinliğinde 32×32, 64×64, 128×128, 256×256 ve 512×512 boyutunda görüntüler kullanılmıştır. 24 bit renk derinliğindeki renkli görüntülerin sadece kırmızı (R) renk kanalına veri gizleme yapılmıştır. Başarım değerlendirmesine ait olan bütün test işlemlerinde kullanılan gizlenecek veriler ise rastgele olarak üretilmiştir.

4.2. Görüntü Görsel Analizi

Görüntüye uygulanan veri gizleme işlemi sonucunda meydana gelecek bozulmaların insan görme sistemi tarafından fark edilememesi istenilen sonuçlardandır. Stego görüntüsü üzerinde meydana gelen bu bozulmaların insan görme sistemi tarafından tespit edilebilmesi için ya orijinal görüntü ile kıyaslama yapılır ya da stego görüntünün yaklaştırılması ile detaylı inceleme yapılır (Yalman, 2010).

Şekil 4.1., 4.2., 4.3., 4.4. ve 4.5.'de, geliştirilen veri gizleme yönteminin görsel analizi ile ilgili sonuçlar verilmektedir. Şekil 4.1. ve 4.2.'de literatürde çok yaygın olarak kullanılan "Lena" isimli görüntünün veri gizleme yapılmadan önceki orijinal hali ile veri gizleme işlemi yapıldıktan sonraki stego görüntüsü sunulmaktadır. Şekil 4.3. incelendiğinde geliştirilen yöntemin renkli patoloji görüntülerine ve standart test görüntülerine uygulandığı zaman elde edilen stego görüntüleri görülmektedir. Şekil 4.3.a., 4.3.b., 4.3.c., 4.3.g., 4.3.h. ve 4.3.ı.'da veri gizleme işlemi yapılan örtü görüntüleri görünmektedir. Şekil 4.3.d., 4.3.e., 4.3.f., 4.3.i., 4.3.j. ve 4.3.k.'da ise veri gizlenmiş stego görüntüler sunulmaktadır. Aynı şekilde gri seviyeli test görüntülerine ait olan veri gizleme işlemi yapılan örtü görüntüleri de Şekil 4.4.a., 4.4.b., 4.4.c., 4.4.g., 4.4.h. ve 4.4.ı.'da görünmektedir. Şekil 4.4.d., 4.4.e., 4.4.f., 4.4.i., 4.4.j. ve 4.4.k.'da ise gri seviyeli test görüntülerinin veri gizlenmiş hali olan stego görüntüler görünmektedir. Elde edilen sonuçlar ele alındığında insan görme sistemi tarafından

yapılan inceleme de stego görüntüler ile orijinalleri arasında her hangi bir görsel fark göze çarpmamaktadır.

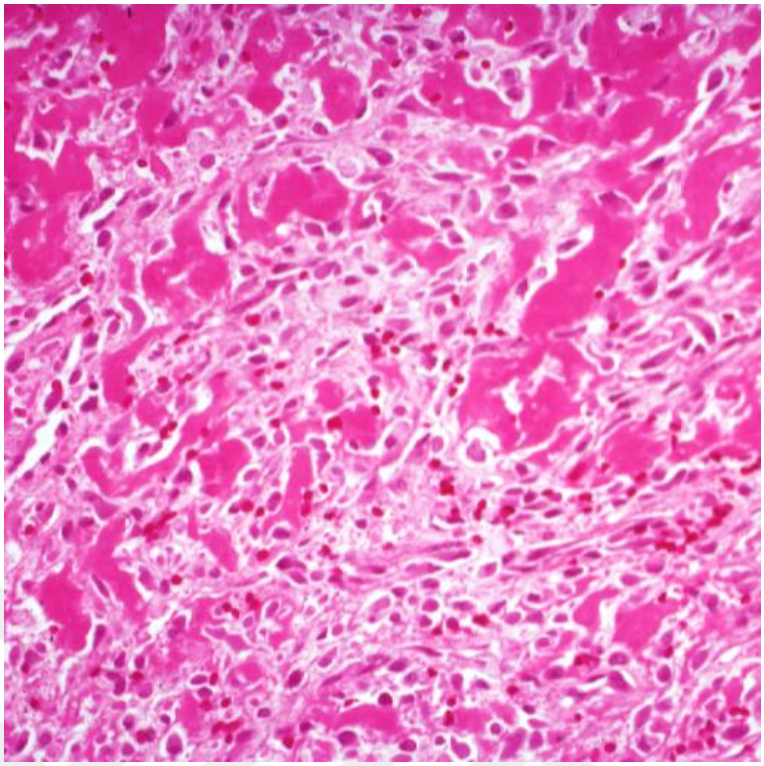
Yapılan bu incelemeyi daha detaylandırmak için Şekil 4.5.'de test görüntülerinden kırpılan ve yakınlaştırılan bölütler verilmektedir. Şekil 4.5.a., 4.5.c. ve 4.5.e.'de orijinal görüntülerin bölütleri yer almaktadır. Görüntülere veri gizlendikten sonra elde edilen stego görüntülerin bölütleri ise Şekil 4.5.b., 4.5.d. ve 4.5.f.'de görülmektedir. Yakınlaştırma sonucunda insan görme sistemi tarafından yapılan incelemede veri gizlenmiş olan görüntülerde görsel bir farkın olmadığı anlaşılmaktadır.

Tez çalışmasındaki en önemli amaç veri gizleme işlemi yapılırken en az değişimi yaparak, yapısal olarak görüntüde orijinaline göre en az görsel farkı oluşturmaktır. Şekil 4.1., 4.2., 4.3., 4.4. ve 4.5.'de görüldüğü gibi insan görme sistemi tarafından yapılan incelemede her hangi bir fark tespit edilememiştir. Bu incelemeyi detaylandırmak için görüntülerin histogram grafikleri elde edilip histogram grafikleri incelenerek yapısal farklılığın olup olmadığı tespit edilmeye çalışılmıştır.

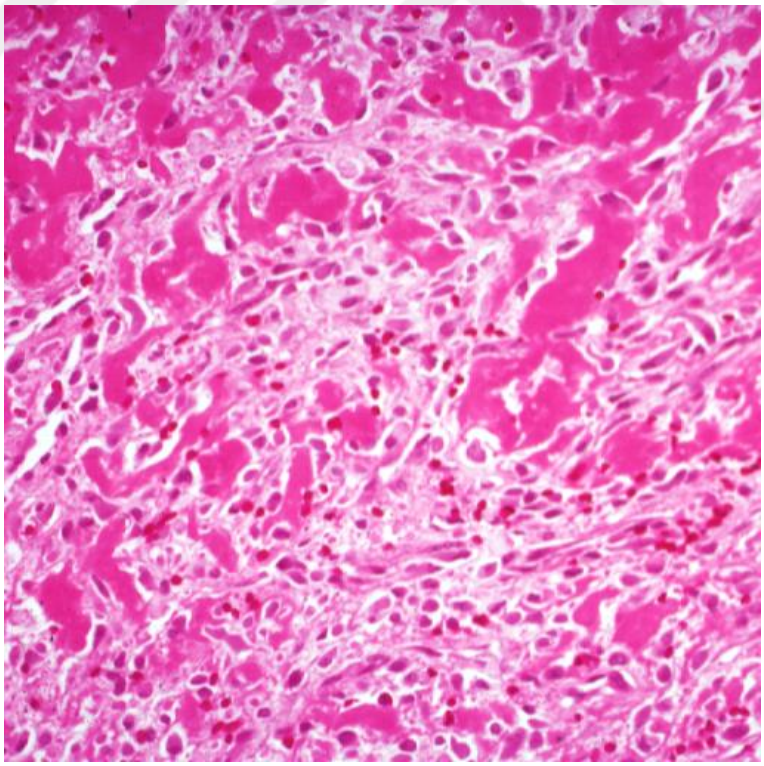
a

b

Şekil 4.1. Lena isimli test görüntüsü a) orijinal görünümü b) Önerilen yöntem kullanılarak içerisine veri gizlenmiş görünümü

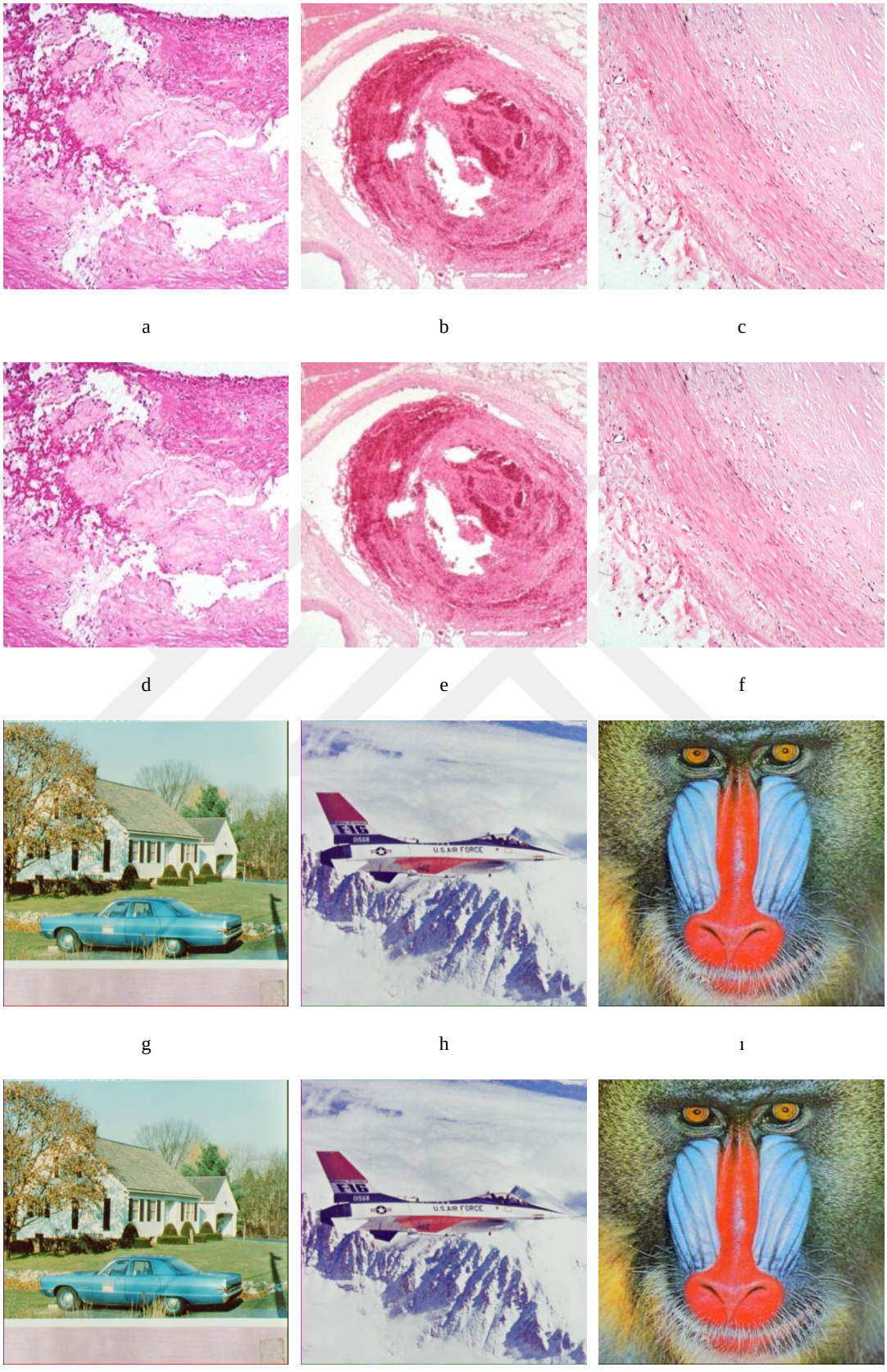


a



b

Şekil 4.2. Tıbbi test görüntüsü a) orijinal görünümü b) Önerilen yöntem kullanılarak içerisine veri gizlenmiş görünümü



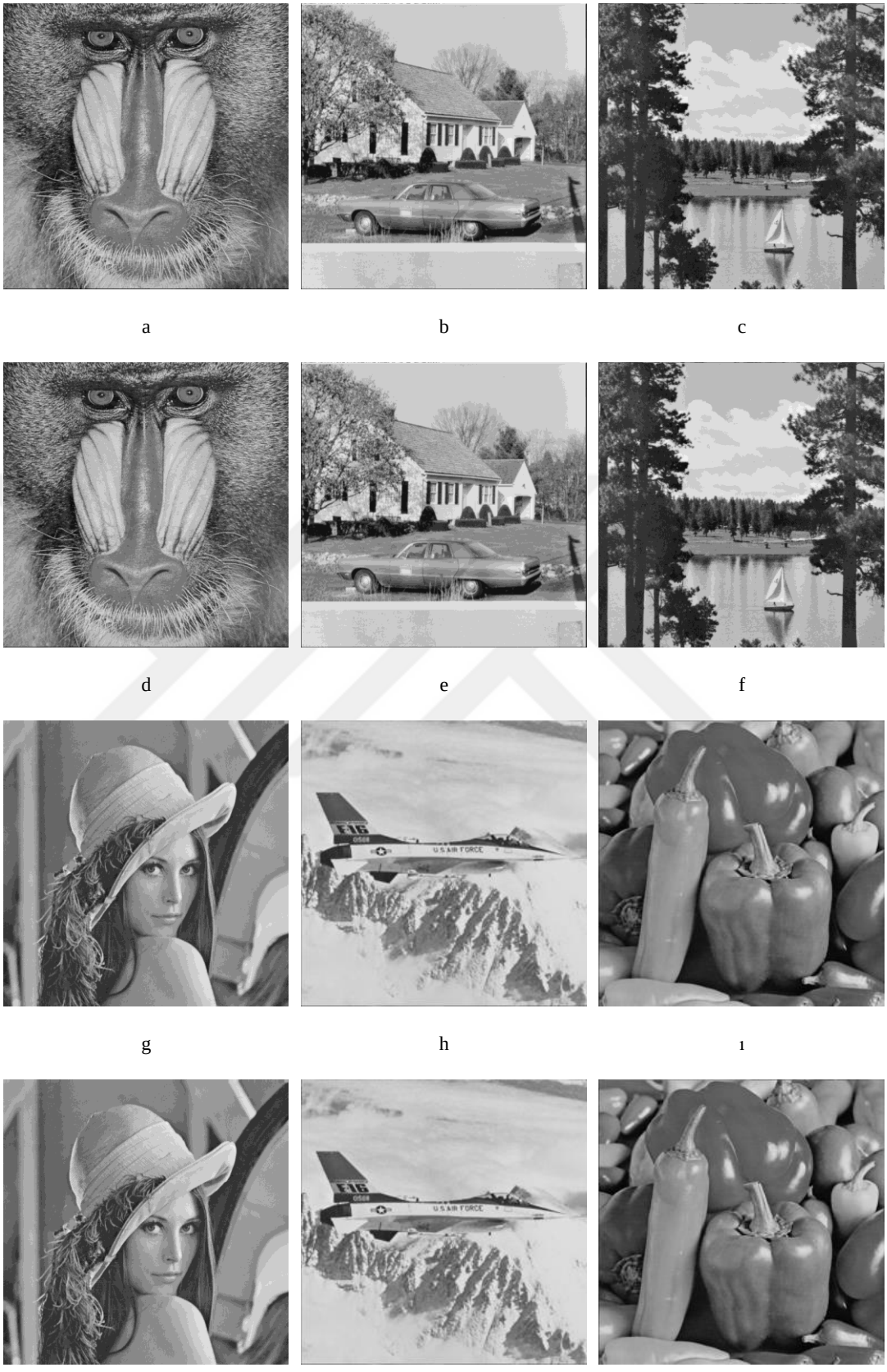
a b c

d e f

g h ı

i j k

Şekil 4.3. Veri gizleme yapılmış renkli görüntülerin orijinal ve veri gizlenmiş görünümleri



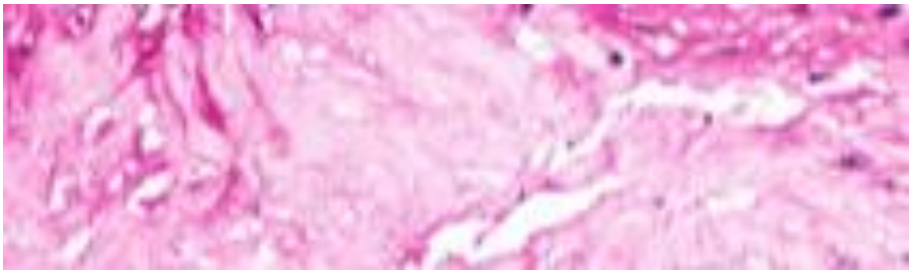
a b c

d e f

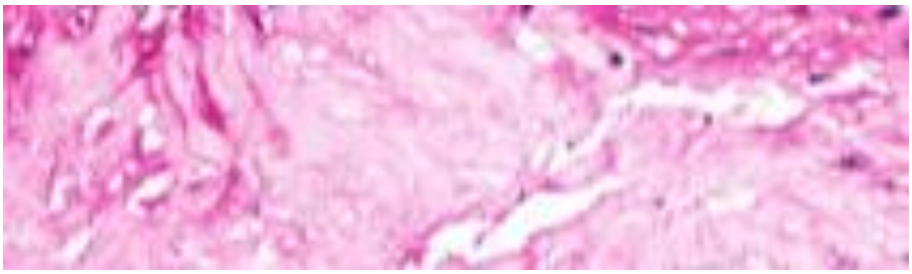
g h ı

i j k

Şekil 4.4. Veri gizleme yapılmış gri seviyeli görüntülerin orijinal ve veri gizlenmiş görünümleri



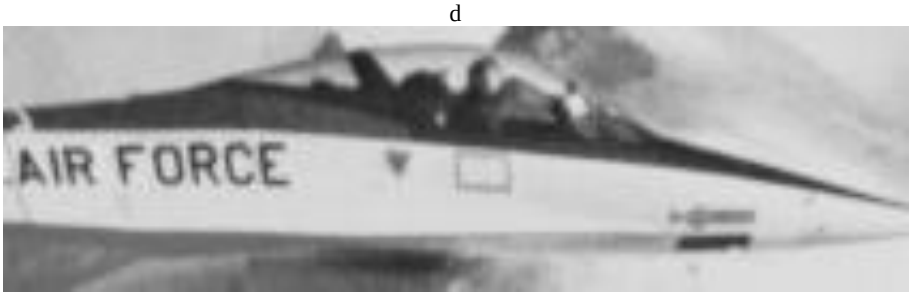
a



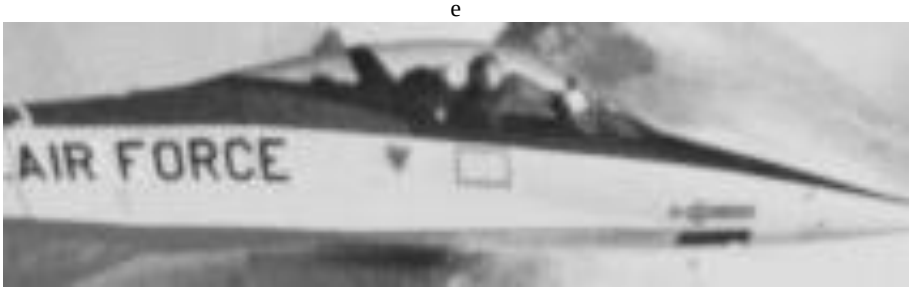
b

c

d



e



f

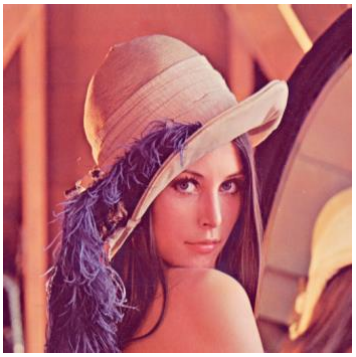
Şekil 4.5. Görüntülerin orijinal ve veri gizlendikten sonraki görünümlerinin kırpılıp yakınlaştırılmış görünümleri

Bir görüntüye ait histogram grafiği, görüntünün piksellerinin sahip olduğu renk değerlerinin kaçar tane olduğu bilgisini vermektedir. Grafiğin yatay ekseninde her bir pikselin alabileceği renk değeri olan 0–255 aralığında değerler (gri seviye, piksel parlaklık frekansları, yoğunluk değerleri) yer alır. Grafiğin düşey ekseninde ise yatayda yer alan her bir gri seviyenin görüntünün piksellerinde kaçar tane olduğu bilgisi yer almaktadır (Şirvan, 2010; Özkan, 2011; İkibaş, 2012).

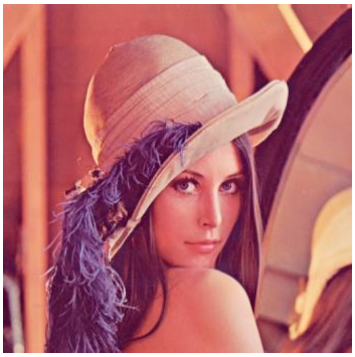
Görüntü üzerinde yapılan değişikler sonucunda piksellerin gri seviye değerlerinin değiştirilmesi ile görüntünün histogramında değişimler olmaktadır. Bu değişimler görüntünün orijinaline göre grafiğin dengesiz dağılımı ve grafikteki değerlerde ani değişimler olarak meydana gelmektedir. Bu değişimler görüntünün istatistiksel olarak dengesiz bir dağılıma yol açmakta ve gizlenen veriyi içeren stego görüntüler için risk oluşturmaktadır. Bu risk ile steganaliz ataklara karşı stego görüntünün güvenliği azalmaktadır (Yalman, 2010).

Histogram grafiği renkli görüntüler için R, G ve B renk kanalları için ayrı ayrı elde edilebilirken, 8 bit gri seviyeli görüntüler için sadece bir adet histogram grafiği elde edilebilmektedir. Şekil 4.6., 4.7.'de 24 bit değerindeki renkli görüntülerin sadece R renk kanalına ait, Şekil 4.8.'de ise 8 bit değerindeki gri seviyeli görüntülere ait, veri gizleme öncesi ve sonrası histogram grafikleri verilmektedir. Şekil 4.6.a., 4.7.a. ve 4.8.a.'da veri gizleme işleminde kullanılan görüntülerin orijinalleri görünmektedir. Bu görüntülere ait olan histogram grafikleri

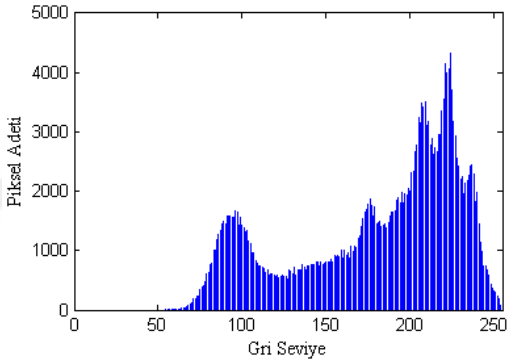
Şekil 4.6.c., 4.7.c. ve 4.8.c.'de yer almaktadır. Tez çalışmasında önerilen veri gizleme yöntemi kullanılarak elde edilen stego görüntüler ise Şekil 4.6.b., 4.7.b. ve 4.8.b.'de görünmektedir. Bu stego görüntülere ait histogram grafikleri ise Şekil 4.6.d., 4.7.d. ve 4.8.d.'de verilmiştir.



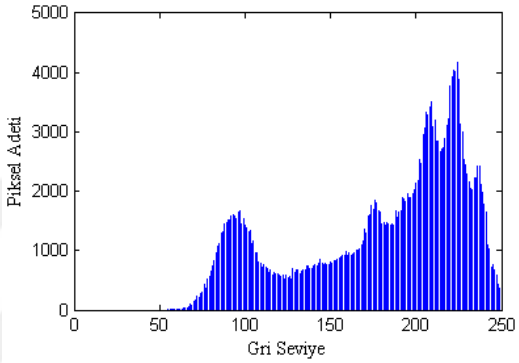
a



b

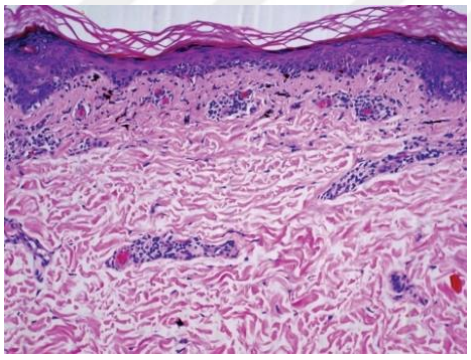


c

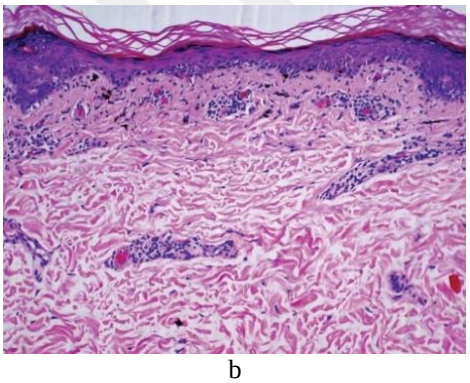


d

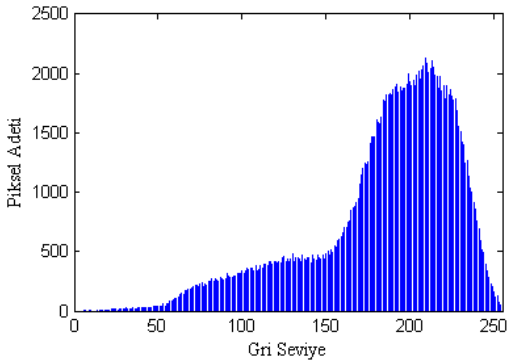
Şekil 4.6. Lena isimli görüntünün orijinal ve veri gizlenmiş durumlarına ait histogram grafiği



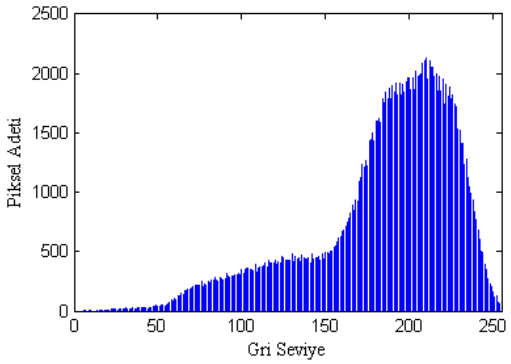
a



b

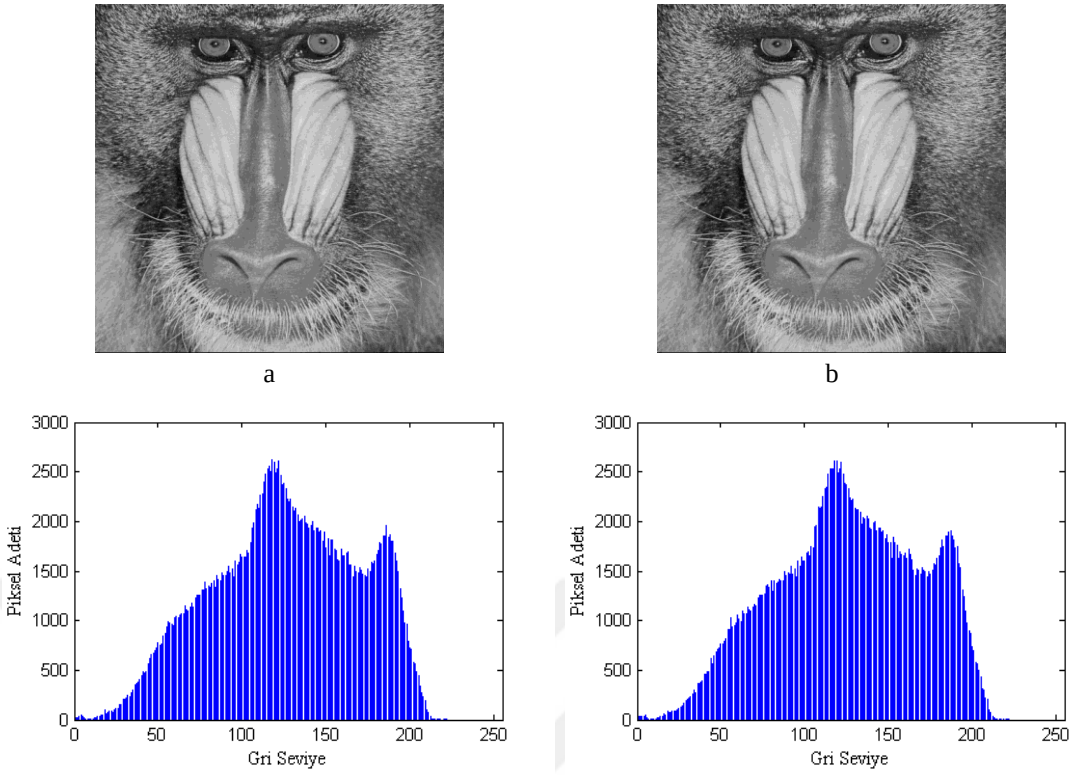


c



d

Şekil 4.7. Patolojik görüntünün orijinal ve veri gizlenmiş durumlarına ait histogram grafiği



Şekil 4.8. Baboon isimli görüntünün orijinal ve veri gizlenmiş durumlarına ait histogram grafiği

Orijinal görüntü ve stego görüntülerin histogram grafikleri incelendiğinde çok fazla değişimin veya ani değişimlerin olmadığı gözlenmektedir. Sadece bazı gri seviye değerlerinin tepe değerlerinde az değişimler olduğu fark edilmektedir. Önerilen yöntemle yapılan veri gizleme işlemi sonucundaki orijinal görüntü histogram grafiği ile stego görüntülerin histogram grafikleri birbirine çok yakın sonuçlar vermektedir. Böylece gizli veriye sahip görüntüler istatiksel olarak üçüncü kişilerce incelendiğinde her hangi bir şüphe uyandırmayacak ve bu sayede steganaliz ataklarına karşıda güvenlik elde edilmiş olunacaktır.

4.3. Piksel Bozulma Oranı

Tez çalışmasında geliştirilen yöntem ile veri gizlenecek görüntü (piksellerinde) üzerinde en az değişim amaçlanmaktadır. Bu değişim yani görüntünün piksellerinin bozulma miktarı ne kadar az olursa o görüntü orijinal görüntüye o kadar yakındır denilebilir. Görüntü üzerinde meydana gelen bu bozulmaları gürültü olarak ifade edebiliriz. Eğer bir görüntüde ne kadar az gürültü var ise bu gürültülerin insan görme

sistemi tarafından algılanması da o kadar zor olacaktır. Görüntüye ne kadar fazla veri saklanması çalışılırsa doğal olarak daha çok pikselde değişim yapılacağı için piksellerin bozulma oranı artacaktır.

Tablo 4.1. ve 4.2.'de geliştirilen veri gizleme yöntemi ile literatürde çok yaygın olarak kullanılan klasik LSB yönteminin veri gizleme işlemi sonucunda görüntülerin piksellerinde meydana getirdiği bozulma miktarları verilmektedir. Tablo 4.1.'de 24 bit değerinde renkli görüntülere ait test sonuçları ve Tablo 4.2.'de ise 8 bit değerinde gri seviyeli görüntülere ait test sonuçları görünmektedir. Tablo 4.1. ve 4.2.'de ki her bir satıra ait sonuçlar gizlenen aynı veri grupları kullanılarak elde edilen test sonuçlarına aittir. Farklı görüntü boyutlarına, görüntülerin sahip olduğu toplam piksellerin yaklaşık %10, %20, %25, %50, %75, %90 ve %100'ü kullanılarak veri gizleme işlemi gerçekleştirilmiştir.

Tablo 4.1. test verileri incelendiğinde 512×512 boyutundaki renkli örtü görüntüsünün 262144 pikseline yani piksellerin hepsine 32 KB kapasitesindeki veriye eşit olan 262144 bit veri tez çalışmasında önerilen yöntemle gizlendiğinde, örtü görüntüsünün sadece %28,78 oranında piksellerinde bozulma/değişim meydana gelmiştir. Bu orana denk gelen piksel sayısı ise 75448'dir. Aynı veriler kullanılarak klasik LSB yöntemi ile yapılan veri gizleme işlemi sonucunda ise değişim oranı %50,04 olmuştur. Klasik LSB yöntemi kullanıldığında örtü görüntüsünün yarısının değişime uğradığı anlaşılmaktadır. Bu iki oran kıyaslandığında önerilen yöntemin klasik LSB yöntemine göre görüntü üzerinde oldukça az bozulma/değişim yaptığı görülmektedir.

Tablo 4.1. RGB görüntülerde veri gizleme sonucu elde edilen piksel bozulma miktarı ve oranları

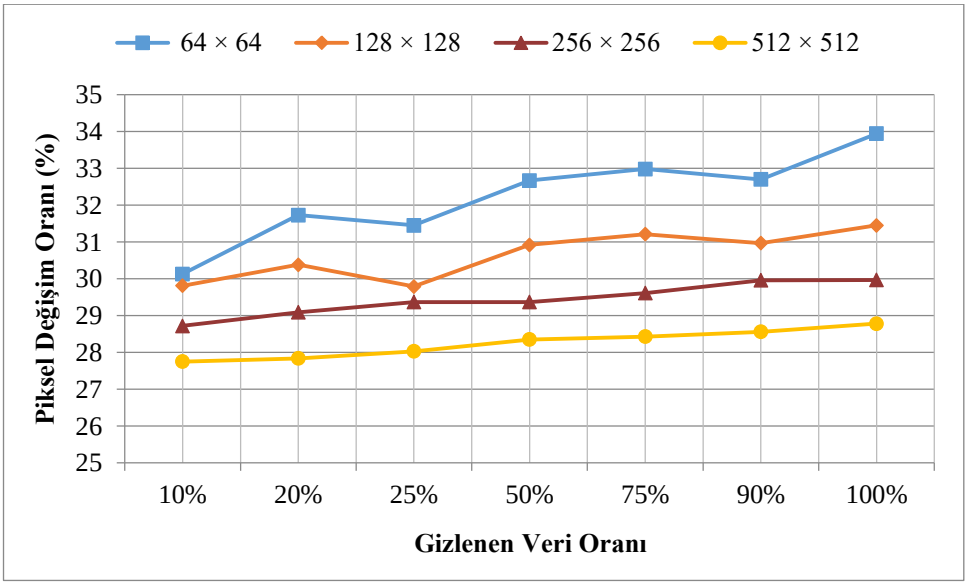
Görüntü Boyutu	Toplam Piksel Sayısı	Gizlenen Veri Oranı	Gizlenen Veri Miktarı (bit)	Veri Gizlenen Piksellerde Değişim Değerleri				Toplam Boyuta Göre Piksellerdeki Değişim Oranı
				Klasik LSB		Önerilen Yöntem		
				Sayısı	Oranı	Sayısı	Oranı	
32 × 32	1024	12,5	128	61	47,66	40	31,25	3,91
32 × 32	1024	25	256	135	52,73	82	32,03	8,01
32 × 32	1024	50	512	266	51,96	170	33,2	16,60
32 × 32	1024	75	768	401	52,21	257	33,46	25,10
32 × 32	1024	94	960	480	50	326	33,96	31,84
32 × 32	1024	100	1024	513	50,1	355	34,67	34,67
64 × 64	4096	10	448	215	47,99	135	30,13	3,30
64 × 64	4096	20	832	419	50,36	264	31,73	6,45
64 × 64	4096	25	1024	533	52,05	322	31,45	7,86
64 × 64	4096	50	2048	1055	51,51	669	32,67	16,33
64 × 64	4096	75	3072	1582	51,5	1013	32,98	24,73
64 × 64	4096	90	3712	1864	50,22	1214	32,7	29,64
64 × 64	4096	100	4096	2127	51,93	1390	33,94	33,94
128 × 128	16384	10	1664	842	50,6	496	29,81	3,03
128 × 128	16384	20	3328	1681	50,51	1011	30,38	6,17
128 × 128	16384	25	4096	2060	50,29	1220	29,79	7,45
128 × 128	16384	50	8192	4200	51,27	2533	30,92	15,46
128 × 128	16384	75	12288	6252	50,88	3835	31,21	23,41
128 × 128	16384	90	14784	7529	50,93	4579	30,97	27,95
128 × 128	16384	100	16384	8279	50,53	5153	31,45	31,45
256 × 256	65536	10	6592	3375	51,2	1893	28,72	2,89
256 × 256	65536	20	13120	6568	50,06	3817	29,09	5,82
256 × 256	65536	25	16384	8335	50,87	4812	29,37	7,34
256 × 256	65536	50	32768	16512	50,39	9624	29,37	14,69
256 × 256	65536	75	49152	24682	50,22	14556	29,61	22,21
256 × 256	65536	90	59008	29734	50,39	17681	29,96	26,98
256 × 256	65536	100	65536	32855	50,13	19644	29,97	29,97
512 × 512	262144	10	26240	13146	50,1	7281	27,75	2,78
512 × 512	262144	20	52480	26264	50,05	14612	27,84	5,57
512 × 512	262144	25	65536	32883	50,18	18369	28,03	7,01
512 × 512	262144	50	131072	65953	50,32	37159	28,35	14,18
512 × 512	262144	75	196608	98513	50,11	55895	28,43	21,32
512 × 512	262144	90	235968	118296	50,13	67404	28,56	25,71
512 × 512	262144	100	262144	131171	50,04	75448	28,78	28,78

Tablo 4.2. Gri seviyeli görüntülerde veri gizleme sonucu elde edilen piksel bozulma miktarı ve oranları

Görüntü Boyutu	Toplam Piksel Sayısı	Gizlenen Veri Oranı	Gizlenen Veri Miktarı (bit)	Veri Gizlenen Piksellerde Değişim Değerleri				Toplam Boyuta Göre Piksellerdeki Değişim Oranı
				Klasik LSB		Önerilen Yöntem		
				Sayısı	Oranı	Sayısı	Oranı	
32 × 32	1024	12,5	128	61	47,66	37	28,91	3,6
32 × 32	1024	25	256	116	45,31	73	28,52	7,1
32 × 32	1024	50	512	256	50	174	33,98	17,0
32 × 32	1024	75	768	399	51,95	258	33,59	25,2
32 × 32	1024	94	960	476	49,58	332	34,58	32,4
32 × 32	1024	100	1024	529	51,66	368	35,94	35,9
64 × 64	4096	10	448	236	52,68	133	29,69	3,2
64 × 64	4096	20	832	434	52,16	268	32,21	6,5
64 × 64	4096	25	1024	532	51,95	327	31,93	8,0
64 × 64	4096	50	2048	1030	50,29	675	32,96	16,5
64 × 64	4096	75	3072	1518	49,41	1013	32,98	24,7
64 × 64	4096	90	3712	1867	50,3	1208	32,54	29,5
64 × 64	4096	100	4096	2051	50,07	1365	33,33	33,3
128 × 128	16384	10	1664	861	51,74	506	30,41	3,1
128 × 128	16384	20	3328	1676	50,36	1038	31,19	6,3
128 × 128	16384	25	4096	2095	51,15	1268	30,96	7,7
128 × 128	16384	50	8192	4124	50,34	2589	31,6	15,8
128 × 128	16384	75	12288	6160	50,13	3779	30,75	23,1
128 × 128	16384	90	14784	7423	50,21	4594	31,07	28,0
128 × 128	16384	100	16384	8274	50,5	5166	31,53	31,5
256 × 256	65536	10	6592	3323	50,41	1930	29,28	2,9
256 × 256	65536	20	13120	6700	51,07	3851	29,35	5,9
256 × 256	65536	25	16384	8311	50,73	4758	29,04	7,3
256 × 256	65536	50	32768	16446	50,19	9706	29,62	14,8
256 × 256	65536	75	49152	24700	50,25	14573	29,65	22,2
256 × 256	65536	90	59008	29625	50,21	17621	29,86	26,9
256 × 256	65536	100	65536	32947	50,27	19729	30,1	30,1
512 × 512	262144	10	26240	13210	50,34	7201	27,44	2,7
512 × 512	262144	20	52480	26278	50,07	14730	28,07	5,6
512 × 512	262144	25	65536	32940	50,26	18530	28,27	7,1
512 × 512	262144	50	131072	65654	50,09	36825	28,1	14,0
512 × 512	262144	75	196608	98447	50,07	55789	28,38	21,3
512 × 512	262144	90	235968	118195	50,09	67285	28,51	25,7
512 × 512	262144	100	262144	131487	50,16	75520	28,81	28,8

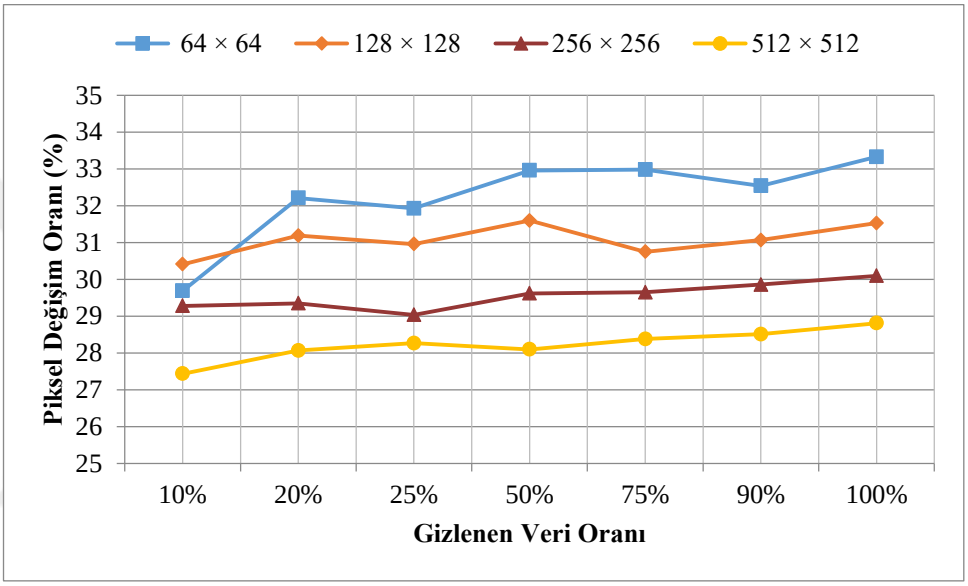
Tablo 4.2.'de 8 bit renk derinliğindeki örtü görüntülerinin test sonuçları incelendiğinde 512×512 boyutundaki örtü görüntüsüne 32 KB kapasitesindeki veri olan 262144 bit veri gizleme sonucunda, önerilen yöntem ile görüntünün piksellerinde %28,81 oranında piksel bozulması gerçekleşirken, klasik LSB yöntemi ile aynı veriler gizlendiğinde bu oranın %50,16 olduğu hesaplanmıştır. Önerilen yöntemle sadece 75520 piksel değeri değişime uğramıştır. Renkli görüntülerde olduğu gibi gri seviyeli görüntülerde de önerilen yöntem oldukça daha az piksel bozulma oranına sahiptir.

Şekil 4.9. ve 4.10.'da farklı görüntü boyutlarına ve farklı veri gizleme oranlarına göre görüntülerde meydana gelen piksel bozulma oranlarının grafiksel gösterimi yer almaktadır. Renkli görüntülerde yapılan veri gizleme işlemi sonucunda önerilen yöntemin kullanılmasıyla veri gizlemenin yapıldığı piksellerin %27,75 − %33,94 oranında piksel bozulmasına neden olduğu görülmektedir. Klasik LSB yöntemi kullanılarak yapılan veri gizleme işlemiyle ise veri gizlemenin yapıldığı piksellerin bozulma oranları %47,66 − %52,73 değerleri arasındadır. Renkli görüntülerde veri gizlemenin yapıldığı piksellerin ortalama bozulma oranı önerilen yöntem için %30,66 iken klasik LSB yöntemi kullanıldığında ise ortalama piksel bozulma oranının %50,57 olduğu hesaplanmıştır.



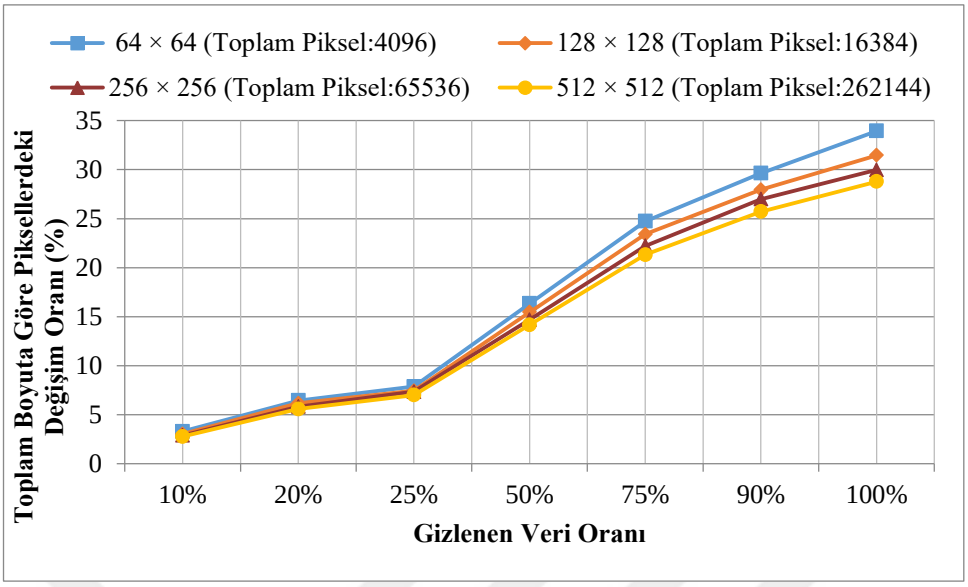
Şekil 4.9. Önerilen yöntem kullanılarak RGB görüntülerde veri gizleme sonucu elde edilen piksel bozulma oranları

Gri seviyeli görüntüler de elde edilen test sonuçlarında önerilen yöntem ile veri gizlemenin yapıldığı piksellerde elde edilen bozulma oranları %27,44 – %33,33 değerleri arasındadır. Klasik LSB yöntemi uygulandığında ise veri gizlemenin yapıldığı piksellerin bozulma oranlarının %45,31 – %52,68 değerleri arasında değiştiği hesaplanmıştır. Önerilen yöntem için veri gizlemenin yapıldığı piksellerde ortalama piksel değişim oranı %30,68 iken klasik LSB yöntemi uygulandığında bu oran %50,34 seviyesindedir.



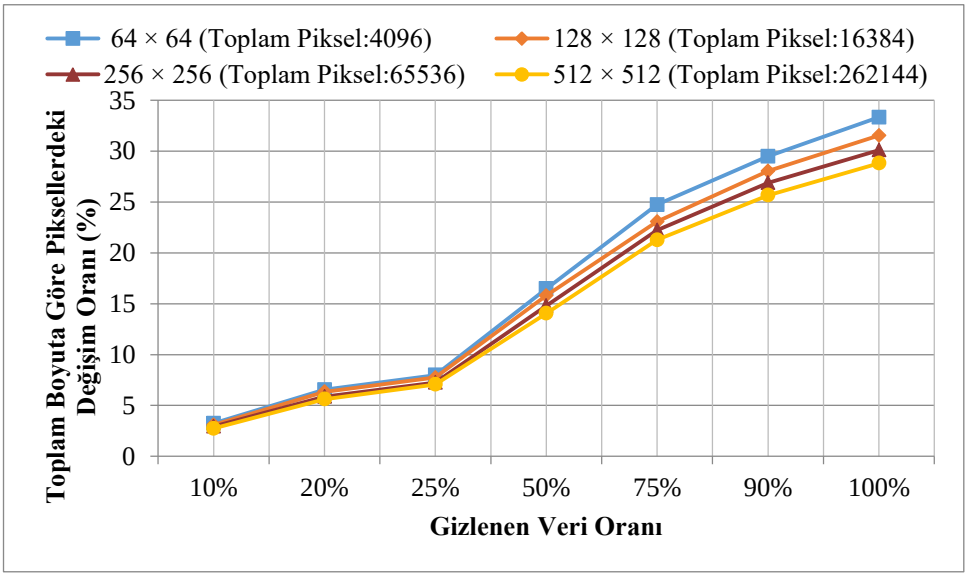
Şekil 4.10. Önerilen yöntem kullanılarak Gri seviyeli görüntülerde veri gizleme sonucu elde edilen piksel bozulma oranları

Şekil 4.11. ve 4.12.'de önerilen yöntem uygulandığında örtü görüntüsünün toplam piksel sayısına göre piksellerdeki bozulma/değişim oranı verilmektedir. Şekil 4.11. incelendiğinde renkli görüntülerde görüntünün toplam pikseline göre %2,78 – %33,94 oranları arasında değişim meydana gelmiştir. En az değişim değeri incelendiğinde ise örtü görüntüsünün toplam 262144 pikselinin 26240 tanesine 1 bit veri gizlenmek istendiğinde sadece 7281 pikselin değeri değiştirilmiştir. Klasik yöntemle bu gizleme işlemi yapıldığında ise 13146 pikselin değerinin değişime uğradığı tespit edilmiştir.



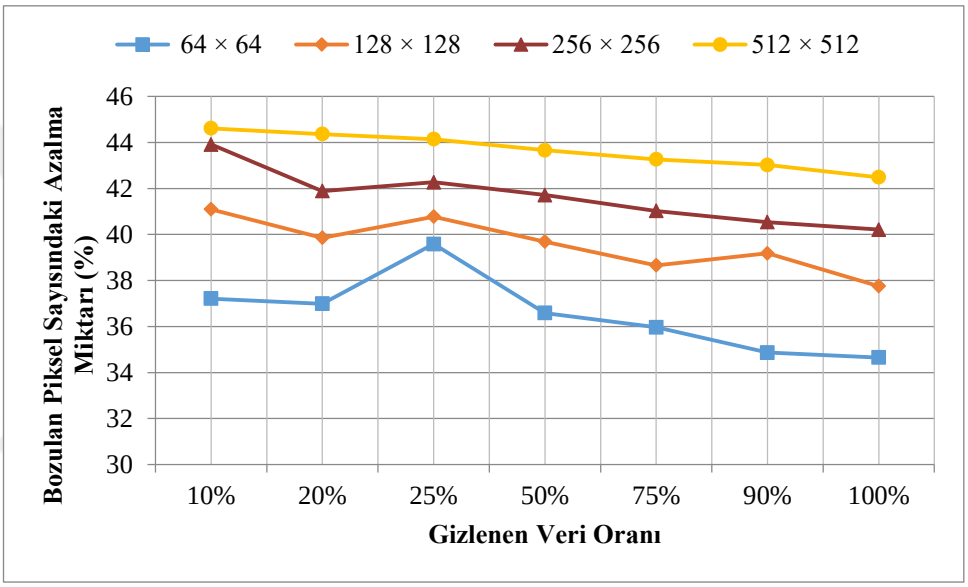
Şekil 4.11. Önerilen yöntem kullanılarak renkli görüntülerde veri gizleme sonucu elde edilen piksel değişim miktarının toplam piksel sayısına oranları

Şekil 4.12.'de ise gri seviyeli görüntülerde toplam piksel sayısına göre olan bozulma/değişim oranı verilmektedir. Değişim oranı renkli görüntülerdeki değişim oranına benzer değer içermektedir. Buradaki aralık %2,75 – %33,33 oranları arasındadır. En az değişimin, toplam 262144 pikselin 26240 tanesine 1 bit gizlenmek istendiğinde sadece 7201 pikselin değeri değiştiğinde olduğu hesaplanmıştır. Klasik yöntemle bu gizleme işlemi yapıldığında ise 13210 pikselin değeri değişime uğradığı tespit edilmiştir.



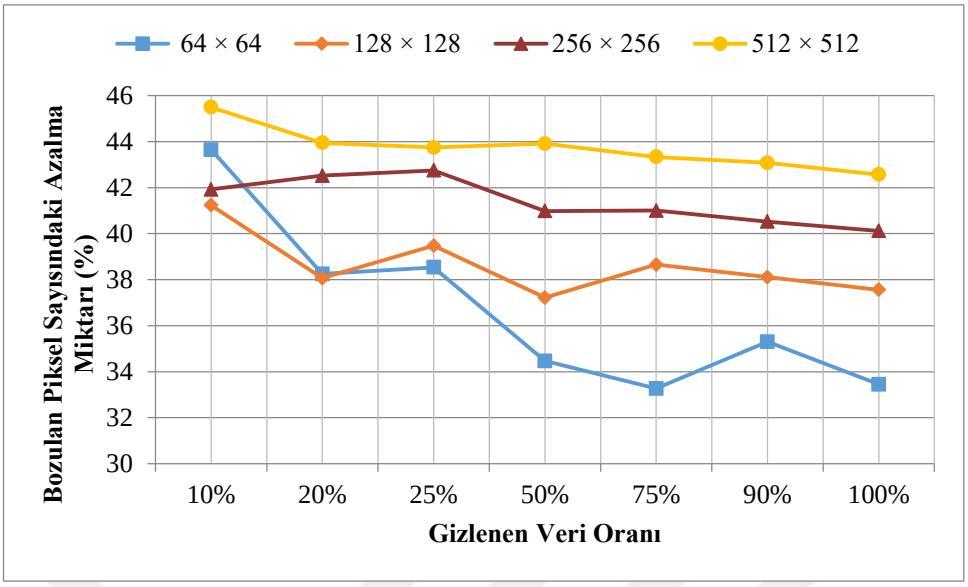
Şekil 4.12. Önerilen yöntem kullanılarak gri seviyeli görüntülerde veri gizleme sonucu elde edilen piksel değişim miktarının toplam piksel sayısına oranları.

Şekil 4.13. ve 4.14.'de önerilen yöntemin klasik LSB yöntemine göre piksellerin bozulma miktarındaki azalma oranı yani kazanç oranı verilmektedir. Şekil 4.13.'e göre renkli görüntülerde %34,65 − %44,61 değerleri arasında klasik LSB yöntemine göre bozulan piksel sayısında azalma olmuştur. 512×512 renkli örtü görüntüsüne 26240 bit yaklaşık 3,2 KB veri gizlenirken klasik LSB yönteminin kullanılması ile 13146 piksel değişime uğrarken aynı veri ile önerilen yöntemle 7281 piksel değişime uğramıştır. Geliştirilen yöntemin kullanımı ile piksel değişim miktarının %44,61 oranında azaldığı görülmektedir.



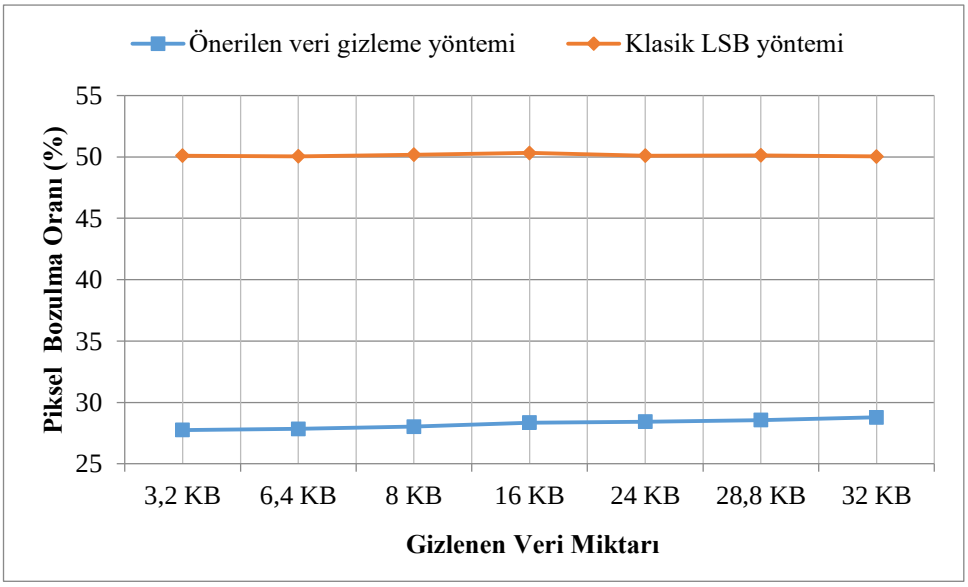
Şekil 4.13. RGB görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu klasik LSB yöntemine göre değişime uğrayan piksel sayısındaki azalmanın oranları

Şekil 4.14.'de gri seviyeli görüntüler için elde edilen piksel değişimindeki azalma oranları görülmektedir. Klasik LSB yöntemine göre %33,27 − %45,49 değerleri arasında bozulan piksel sayısında azalma olmuştur. 512×512 gri seviyeli örtü görüntüsüne 26240 bit yaklaşık 3,2 KB veri gizlenirken klasik LSB yönteminin kullanılması ile 13210 piksel değişime uğrarken aynı veri ile önerilen yöntemle 7201 piksel değişime uğramıştır. Böylece %45,491 oranında piksel değişim miktarı azalmıştır.

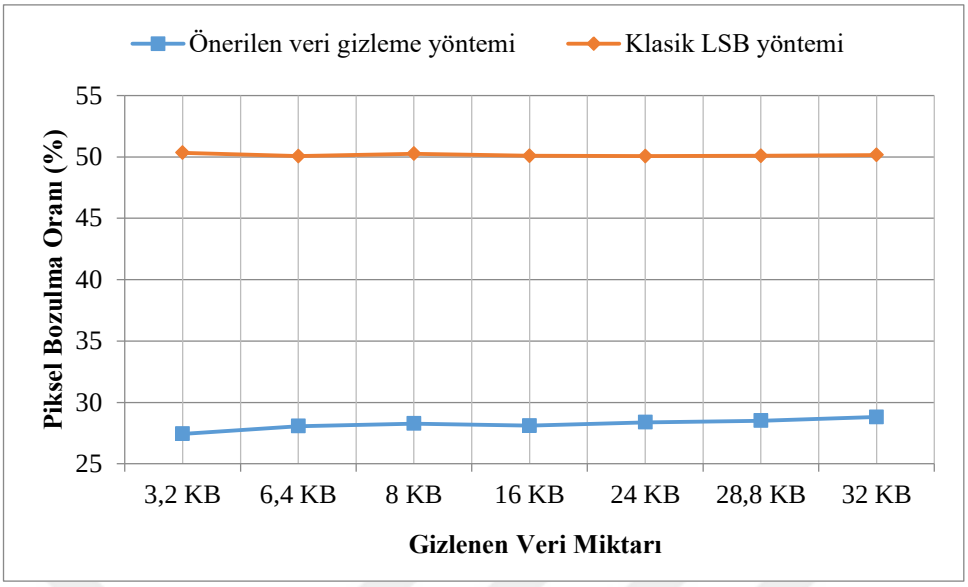


Şekil 4.14. Gri seviyeli görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu klasik LSB yöntemine göre değişime uğrayan piksel sayısındaki azalmanın oranları

Şekil 4.15. ve 4.16.'da 512×512 boyutundaki renkli ve gri seviyeli görüntülerde geliştirilen yöntem ve klasik LSB yöntemine göre gizlenen veri miktarının kapasite birimi gösterimlerine karşın piksel değişim oranları verilmektedir. Bütün veri miktarlarında klasik LSB yöntemi kullanılması sonucu örtü görüntüsünün piksellerinin yaklaşık %50'i bozulmaya uğrarken, önerilen yöntem kullanıldığında bu oranın yaklaşık %28 olduğu görülmektedir.

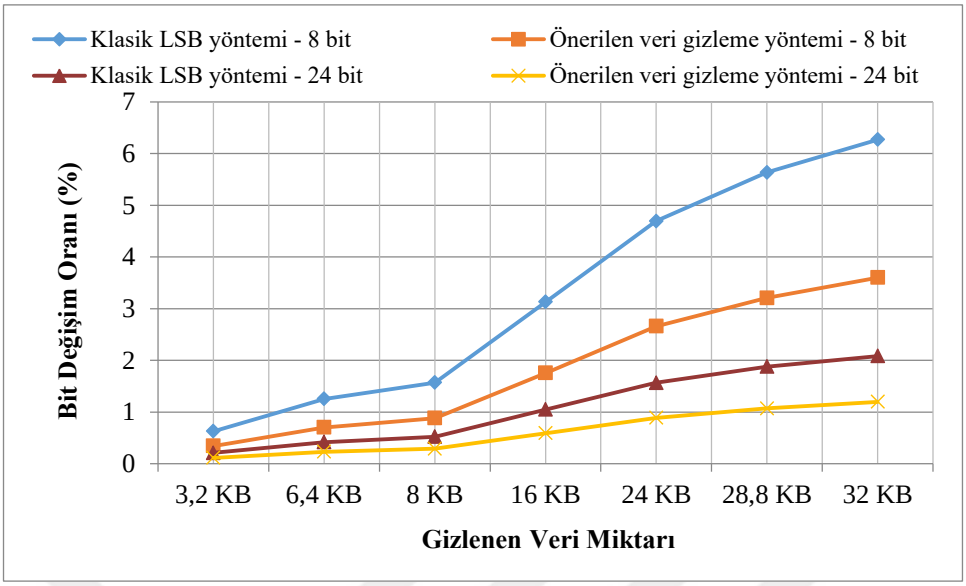


Şekil 4.15. RGB görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu ve klasik LSB yöntemine kullanılarak yapılan veri gizleme sonucu elde edilen piksel değişim oranları



Şekil 4.16. Gri seviyeli görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu ve klasik LSB yöntemine kullanılarak yapılan veri gizleme sonucu elde edilen piksel değişim oranları

Şekil 4.17.'de geliştirilen yöntem ve klasik LSB yönteminin 512×512 boyutundaki renkli ve gri seviyeli görüntülerde veri gizlenmesi sonucu meydana gelen bit değişiminin görüntülerdeki toplam bit sayısına göre, değişim oranları verilmektedir. Renkli görüntülerde önerilen yöntem, görüntüdeki toplam 6291456 bitin %0,12 – %1,20 oranında değişime uğratırken klasik LSB yönteminde bu oranlar %0,21 – %2,08 aralığındadır. Gri seviyeli görüntülerde ise toplam 2097152 bitin önerilen yöntem kullanıldığında, bit değişim oranı %0,34 – %3,60 aralığında iken klasik LSB yöntemi ile bu aralık %0,63 – %6,27 değerlerindedir. Önerilen yöntemle, renkli görüntülerde 32 KB kapasitesindeki veri gizlendiğinde görüntünün toplam bit sayısının sadece %1,20'i değiştirilmiştir. Bu değer görüntü üzerinde oldukça az bir değişim olduğunu göstermektedir.



Şekil 4.17. RGB ve Gri seviyeli görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu ve klasik LSB yöntemine kullanılarak yapılan veri gizleme sonucu elde edilen bit değişim oranları

Yapılan test işlemleri neticesinde elde edilen sonuçlar incelendiğinde tez çalışmasında geliştirilen yöntem kullanılarak yapılan veri gizleme işleminde görüntünün veri gizlenecek piksellerinde bozulma/değişim oranı klasik LSB yöntemine göre oldukça az olmaktadır. Buradaki en önemli özellik ise geliştirilen yöntemin veri gizleme işleminden önce gizlenecek veriye en uygun yani en benzer pikselleri bloklarda bulup, bu yerlere verileri gizlemesidir. Böylelikle istenilen sonuç olan görüntüde en az değişim miktarı elde edilmektedir. Bu değişim bundan sonra yapılacak olan başarım değerlendirmelerini de doğrudan etkilemektedir.

4.4. Ortalama Karesel Hata (MSE) ve Tepe Sinyal Gürültü Oranı (PSNR)

Gizli verinin örtü görüntüsüne gizlenmesi sonucu oluşan stego görüntüde meydana gelen bozulmaları ölçmek için kullanılan Ortalama Karesel Hata (MSE) ve Tepe Sinyal Gürültü Oranı (PSNR) bilgileri, literatürde çok yaygın kullanılan iki hata tespit ölçütüdür. PSNR değerlerinin hesaplanabilmesi için ilk önce MSE değerinin hesaplanması gerekmektedir (Hong, 2013; Tyagi ve ark., 2015).

MSE değerini hesaplamak için Denklem 4.1. kullanılır (Rabbani ve Jones, 1991).

$$\mathrm{MSE} = \frac{1}{\mathrm{m} \times \mathrm{n}} \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} \|\mathrm{O}(\mathrm{i},\mathrm{j}) - \mathrm{S}(\mathrm{i},\mathrm{j})\|^2 \quad (4.1)$$

Burada O ve S aralarındaki bozulmanın hesaplanacağı birbiriyle kıyaslanan görüntüler olmak üzere; O orijinal görüntüyü, S ise içerisine veri gizlenmiş stego görüntüyü temsil etmektedir. m ve n değerleri ise görüntülerin boyutlarını temsil etmektedir. Denklem 4.2.'de ise MSE değeri hesaplandıktan sonra bulunacak olan PSNR değerinin denklemi yer almaktadır (Rabbani ve Jones, 1991).

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \right) \quad (4.2)$$

Burada yer alan MAX değeri görüntünün pikselinde kullanılabilen en büyük sayısal değeri temsil etmektedir. 24 bit renk derinliğindeki renkli görüntülerin her pikseli R (kırmızı), G (yeşil) ve B (mavi) renk kanallarından oluşmakta ve her biri 8 bit değerinde değer alabilmektedir. Yani her renk kanalının alabileceği en büyük değer 255'dir. 8 bit değerindeki gri seviyeli görüntülerde ise pikselde alınabilecek en büyük değer 255'dir. Denklem 4.2.'de yer alan MAX değeri bundan dolayı 255 olarak alınmaktadır. Bulunan PSNR değeri desibel (dB) ölçü birimi ile ifade edilir. Renkli görüntüler için MSE değeri her renk kanalı için ayrı ayrı hesaplanır ve ortalama MSE değeri hesaplanır. İstenirse her renk kanalı için ayrı ayrı MSE ve PSNR değerleri hesaplanabilir (Rendy, 2015; Tyagi ve ark., 2015).

Renkli görüntülerin renk kanalları için MSE değerlerini ayrı ayrı hesaplamak istenildiğinde Denklem 4.3. kullanılır.

$$\mathrm{MSE}_{R,G,B} = \frac{1}{\mathrm{m} \times \mathrm{n}} \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} \left\| \mathrm{O}_{R,G,B}(\mathrm{i},\mathrm{j}) - S_{R,G,B}(\mathrm{i},\mathrm{j}) \right\|^2 \quad (4.3)$$

Burada yer alan $\mathrm{MSE}_{\mathrm{R,G,B}}$ değeri ilgili renk kanalının MSE değerini temsil etmektedir. $\mathrm{O}_{\mathrm{R,G,B}}$ orijinal görüntüyü, $\mathrm{S}_{\mathrm{R,G,B}}$ ise stego görüntüyü belirtmektedir. R

(kırmızı) renk kanalını, G (yeşil) renk kanalını ve B (mavi) renk kanalını temsil etmektedir.

Eğer renkli görüntüde ortalama PSNR değeri bulunması istenirse ilk önce Denklem 4.4. ile R, G, B renk kanallarına ait MSE değerlerinin ortalamasının bulunması gerekmektedir. Daha sonra Denklem 4.2. ile renkli görüntünün PSNR değeri hesaplanır.

$$\mathrm{MSE} = \frac{\mathrm{MSE}_R + \mathrm{MSE}_G + \mathrm{MSE}_B}{3} \tag{4.4}$$

Renkli görüntüler için PSNR değerleri ayrı ayrı hesaplamak istenildiğinde Denklem 4.5. kullanılır.

$$\mathrm{PSNR}_{R,G,B} = 10 \log_{10} \left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}_{R,G,B}} \right) \tag{4.5}$$

Burada yer alan $\mathrm{PSNR}_{\mathrm{R,G,B}}$ ve $\mathrm{MSE}_{\mathrm{R,G,B}}$ değeri sırasıyla ilgili renk kanalının PSNR ve MSE değerlerini temsil etmektedir. MAX değeri ise her bir renk kanalında kullanılabilecek en büyük değer olan 255 olarak alınır.

Orijinal görüntü ve stego görüntü kullanılarak hesaplanan PSNR değeri ne kadar yüksek çıkarsa stego görüntünün görüntü kalitesi o kadar iyidir. Bunun aksine, elde edilen PSNR değeri küçük ise stego görüntü kalitesi düşüktür. Stego görüntü kalitesi yüksek olması görüntünün orijinale yakın olmasıyla elde edilebilir (Chang ve ark., 2008). Eğer iki görüntü arasında hesaplanan PSNR değeri 30 dB − 50 dB arasında ise bu değer literatürdeki görüntü işleme çalışmalarında kabul edilmiş değer olarak ele alınmaktadır (Netravali ve Haskell, 1995; Chang ve ark., 2008; Coşkun ve ark., 2013).

Literatürde yer alan veri gizleme çalışmalarında, stego görüntüsü içerisindeki gizli veri miktarını ölçmek ve karşılaştırmak için kullanılan gömü kapasitesi (embedding capacity − EC) veya diğer adıyla gömü yükü (embedding payload) Denklem 4.6.'da

verilmektedir. Stego görüntüsünde piksel başına düşen gizli bit sayısı (bits per pixel − bpp) bu denklem aracılığı ile hesaplanır (Zhang ve ark., 2013; Nayak ve Bhagvati, 2013).

$$EC = \frac{N_{SB}}{m \times n} \text{ bpp} \tag{4.6}$$

Burada EC gömü kapasitesini, N_{SB} (number of secret bits) stego görüntüde yer alan gizli veri bitlerinin sayısını, m ve n değerleri ise stego görüntünün boyutunu yani sahip olduğu toplam piksel sayısını vermektedir.

Tablo 4.3.'de 24 bit renkli görüntülerin R (kırmızı) renk kanalına ait deneysel sonuçları yer almaktadır. Farklı boyuttaki örtü görüntülerine, değişken veri miktarına göre aynı veri gruplarının klasik LSB ve önerilen yöntem kullanılıp yapılan veri gizleme işlemi sonucunda elde edilen MSE ve PSNR değerleri Tablo 4.3.'de yer almaktadır. Önerilen yöntem 52,59 dB – 63,70 dB aralığında PSNR değerine sahip iken, klasik LSB yönteminin aynı verilerin gizlenmesi sonucunda 50,96 dB – 61,14 dB aralığında PSNR değerinin hesaplandığı gözlenmektedir. Önerilen yöntemin klasik LSB yöntemine göre her durumda daha iyi sonuç verdiği gözlenmektedir.

Tablo 4.4.'de 8 bit gri seviyeli görüntülere ait MSE ve PSNR değerleri verilmektedir. Önerilen yöntemin en düşük 52,55 dB değerinde PSNR değeri hesaplanırken buna karşın klasik LSB yönteminin aynı veri gurubunun gizlenmesi sonucunda hesaplanan PSNR değeri 50,93 dB'dir. Önerilen yöntemin hesaplanan en yüksek PSNR değeri ise 63,74 dB iken klasik LSB yönteminin değeri 61,11 dB'dir. Renkli görüntülerde olduğu gibi gri seviyeli görüntülerde de önerilen yöntemin daha iyi sonuç verdiği görülmektedir.

Tablo 4.3. RGB görüntülerde veri gizleme sonucu elde edilen MSE ve PSNR değerleri

Görüntü Boyutu	Toplam Piksel Sayısı	Gizlenen Veri				Klasik LSB		Önerilen Yöntem		Fark
		Oranı (%)	Bit Sayısı	Miktar (KB)	Miktar (bpp)	MSE	PSNR	MSE	PSNR	
32 × 32	1024	12,5	128	0,0156	0,13	0,0713	59,60	0,0400	62,11	2,51
32 × 32	1024	25	256	0,0313	0,25	0,1318	56,93	0,0801	59,10	2,17
32 × 32	1024	50	512	0,0625	0,50	0,2500	54,15	0,1621	56,03	1,88
32 × 32	1024	75	768	0,0938	0,75	0,3916	52,20	0,2510	54,13	1,93
32 × 32	1024	94	960	0,1172	0,94	0,4688	51,42	0,3184	53,10	1,68
32 × 32	1024	100	1024	0,1250	1,00	0,5215	50,96	0,3584	52,59	1,63
64 × 64	4096	20	832	0,1016	0,20	0,1052	57,91	0,0647	60,02	2,11
64 × 64	4096	25	1024	0,1250	0,25	0,1301	56,99	0,0786	59,18	2,19
64 × 64	4096	50	2048	0,2500	0,50	0,2537	54,09	0,1619	56,04	1,95
64 × 64	4096	75	3072	0,3750	0,75	0,3833	52,30	0,2444	54,25	1,95
64 × 64	4096	90	3712	0,4531	0,91	0,4753	51,36	0,3018	53,33	1,97
64 × 64	4096	100	4096	0,5000	1,00	0,5059	51,09	0,3369	52,86	1,77
128 × 128	16384	10	1664	0,2031	0,10	0,0496	61,17	0,0295	63,43	2,26
128 × 128	16384	20	3328	0,4063	0,20	0,1026	58,02	0,0617	60,23	2,21
128 × 128	16384	25	4096	0,5000	0,25	0,1283	57,05	0,0761	59,32	2,27
128 × 128	16384	50	8192	1,0000	0,50	0,2535	54,09	0,1545	56,24	2,15
128 × 128	16384	75	12288	1,5000	0,75	0,3770	52,37	0,2300	54,51	2,14
128 × 128	16384	90	14784	1,8047	0,90	0,4574	51,53	0,2825	53,62	2,09
128 × 128	16384	100	16384	2,0000	1,00	0,5053	51,10	0,3145	53,15	2,05
256 × 256	65536	10	6592	0,8047	0,10	0,0515	61,01	0,0289	63,52	2,51
256 × 256	65536	20	13120	1,6016	0,20	0,0993	58,16	0,0577	60,52	2,36
256 × 256	65536	25	16384	2,0000	0,25	0,1261	57,12	0,0737	59,46	2,34
256 × 256	65536	50	32768	4,0000	0,50	0,2520	54,12	0,1469	56,46	2,34
256 × 256	65536	75	49152	6,0000	0,75	0,3766	52,37	0,2221	54,67	2,30
256 × 256	65536	90	59008	7,2031	0,90	0,4530	51,57	0,2688	53,84	2,27
256 × 256	65536	100	65536	8,0000	1,00	0,5013	51,13	0,2997	53,36	2,23
512 × 512	262144	10	26240	3,2031	0,10	0,0500	61,14	0,0277	63,70	2,56
512 × 512	262144	20	52480	6,4063	0,20	0,1002	58,12	0,0557	60,67	2,55
512 × 512	262144	25	65536	8,0000	0,25	0,1264	57,11	0,0707	59,64	2,53
512 × 512	262144	50	131072	16,0000	0,50	0,2498	54,15	0,1406	56,65	2,50
512 × 512	262144	75	196608	24,0000	0,75	0,3750	52,39	0,2126	54,86	2,47
512 × 512	262144	90	235968	28,8047	0,90	0,4504	51,60	0,2560	54,05	2,45
512 × 512	262144	100	262144	32,0000	1,00	0,4999	51,14	0,2881	53,54	2,40

Tablo 4.4. Gri seviyeli görüntülerde veri gizleme sonucu elde edilen MSE ve PSNR değerleri

Görüntü Boyutu	Toplam Piksel Sayısı	Gizlenen Veri				Klasik LSB		Önerilen Yöntem		Fark
		Oranı (%)	Bit Sayısı	Miktar (KB)	Miktar (bpp)	MSE	PSNR	MSE	PSNR	
32 × 32	1024	12,5	128	0,0156	0,13	0,0664	59,91	0,0400	62,11	2,20
32 × 32	1024	25	256	0,0313	0,25	0,1133	57,59	0,0713	59,60	2,01
32 × 32	1024	50	512	0,0625	0,50	0,2500	54,15	0,1699	55,83	1,68
32 × 32	1024	75	768	0,0938	0,75	0,3896	52,22	0,2520	54,12	1,89
32 × 32	1024	94	960	0,1172	0,94	0,4648	51,46	0,3242	53,02	1,56
32 × 32	1024	100	1024	0,1250	1,00	0,5244	50,93	0,3613	52,55	1,62
64 × 64	4096	20	832	0,1016	0,20	0,1060	57,88	0,0654	59,97	2,09
64 × 64	4096	25	1024	0,1250	0,25	0,1299	57,00	0,0798	59,11	2,11
64 × 64	4096	50	2048	0,2500	0,50	0,2498	54,16	0,1594	56,11	1,95
64 × 64	4096	75	3072	0,3750	0,75	0,3730	52,41	0,2444	54,25	1,84
64 × 64	4096	90	3712	0,4531	0,91	0,4558	51,54	0,2949	53,43	1,89
64 × 64	4096	100	4096	0,5000	1,00	0,5007	51,13	0,3333	52,90	1,77
128 × 128	16384	10	1664	0,2031	0,10	0,0505	61,10	0,0302	63,33	2,23
128 × 128	16384	20	3328	0,4063	0,20	0,1023	58,03	0,0634	60,11	2,08
128 × 128	16384	25	4096	0,5000	0,25	0,1267	57,10	0,0762	59,31	2,21
128 × 128	16384	50	8192	1,0000	0,50	0,2471	54,20	0,1529	56,29	2,09
128 × 128	16384	75	12288	1,5000	0,75	0,3726	52,42	0,2330	54,46	2,04
128 × 128	16384	90	14784	1,8047	0,90	0,4531	51,57	0,2804	53,65	2,08
128 × 128	16384	100	16384	2,0000	1,00	0,5050	51,10	0,3153	53,14	2,05
256 × 256	65536	10	6592	0,8047	0,10	0,0502	61,12	0,0291	63,49	2,36
256 × 256	65536	20	13120	1,6016	0,20	0,1022	58,03	0,0588	60,44	2,41
256 × 256	65536	25	16384	2,0000	0,25	0,1268	57,10	0,0726	59,52	2,42
256 × 256	65536	50	32768	4,0000	0,50	0,2499	54,15	0,1465	56,47	2,32
256 × 256	65536	75	49152	6,0000	0,75	0,3769	52,37	0,2224	54,66	2,29
256 × 256	65536	90	59008	7,2031	0,90	0,4533	51,57	0,2679	53,85	2,29
256 × 256	65536	100	65536	8,0000	1,00	0,5027	51,12	0,3010	53,34	2,23
512 × 512	262144	10	26240	3,2031	0,10	0,0504	61,11	0,0275	63,74	2,64
512 × 512	262144	20	52480	6,4063	0,20	0,0997	58,14	0,0557	60,67	2,53
512 × 512	262144	25	65536	8,0000	0,25	0,1257	57,14	0,0707	59,64	2,50
512 × 512	262144	50	131072	16,0000	0,50	0,2505	54,14	0,1405	56,65	2,51
512 × 512	262144	75	196608	24,0000	0,75	0,3749	52,39	0,2121	54,87	2,47
512 × 512	262144	90	235968	28,8047	0,90	0,4509	51,59	0,2567	54,04	2,45
512 × 512	262144	100	262144	32,0000	1,00	0,5005	51,14	0,2870	53,55	2,42

Tablo 4.5.'de literatürde çok sık kullanılan standart haline gelmiş test görüntülerine ait PSNR değerleri görülmektedir. Önerilen yöntem kullanılarak farklı boyutlardaki görüntülere ve rastgele üretilmiş farklı veri miktarlarında gizlemeler yapılmıştır. Yapılan gizlemeler sonucunda PSNR değerlerinin 57,16 dB – 68,47 dB aralığında değiştiği hesaplanmıştır.

Tablo 4.5. RGB standart test görüntülere ait PSNR değerleri

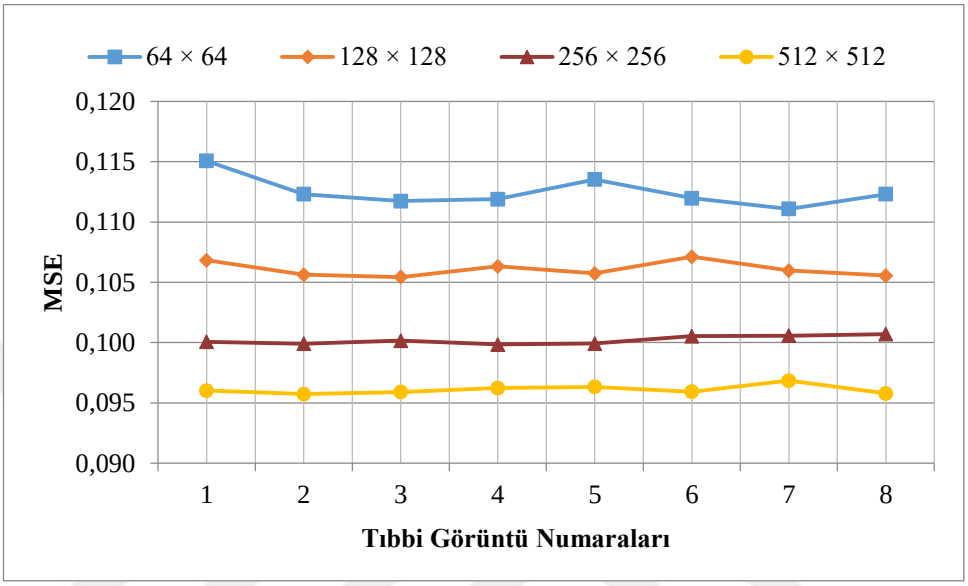
Boyut	Oran	Bit	Miktar		Test Görüntüleri						
			KB	bpp	Lena	Pepper	House	Baboon	F-16	Lake	Tiffany
64 × 64	20	832	0,10	0,20	64,74	64,79	64,88	64,73	64,66	64,78	64,57
64 × 64	25	1024	0,13	0,25	63,88	63,92	63,78	63,89	63,76	63,87	63,80
64 × 64	50	2048	0,25	0,50	60,70	60,79	60,81	60,80	60,75	60,77	60,66
64 × 64	75	3072	0,38	0,75	58,97	58,96	58,98	58,93	58,96	59,00	58,96
64 × 64	90	3712	0,45	0,91	58,07	58,11	58,08	58,18	58,09	58,11	57,87
64 × 64	100	4096	0,50	1,00	57,63	57,57	57,66	57,62	57,60	57,68	57,18
128 × 128	10	1664	0,20	0,10	68,02	67,89	67,86	67,90	67,91	67,88	67,84
128 × 128	20	3328	0,41	0,20	65,00	64,92	64,97	64,89	65,02	64,91	64,92
128 × 128	25	4096	0,50	0,25	64,08	64,04	64,08	63,97	64,07	64,03	64,03
128 × 128	50	8192	1,00	0,50	61,03	60,98	60,99	61,00	60,99	60,97	60,87
128 × 128	75	12288	1,50	0,75	59,24	59,25	59,22	59,21	59,19	59,24	59,01
128 × 128	90	14784	1,80	0,90	58,44	58,36	58,37	58,37	58,32	58,37	57,80
128 × 128	100	16384	2,00	1,00	57,90	57,93	57,86	57,85	57,88	57,83	57,23
256 × 256	10	6592	0,80	0,10	68,22	68,18	68,30	68,29	68,28	68,33	68,13
256 × 256	20	13120	1,60	0,20	65,25	65,21	65,24	65,22	65,22	65,29	65,09
256 × 256	25	16384	2,00	0,25	64,23	64,28	64,24	64,21	64,27	64,20	64,11
256 × 256	50	32768	4,00	0,50	61,20	61,19	61,25	61,18	61,22	61,20	61,07
256 × 256	75	49152	6,00	0,75	59,44	59,41	59,43	59,41	59,41	59,40	59,02
256 × 256	90	59008	7,20	0,90	58,61	58,62	58,60	58,59	58,60	58,61	57,85
256 × 256	100	65536	8,00	1,00	58,11	58,14	58,12	58,09	58,12	58,12	57,22
512 × 512	10	26240	3,20	0,10	68,45	68,47	68,47	68,41	68,41	68,38	68,28
512 × 512	20	52480	6,41	0,20	65,40	65,42	65,40	65,38	65,40	65,37	65,27
512 × 512	25	65536	8,00	0,25	64,44	64,44	64,41	64,42	64,42	64,45	64,29
512 × 512	50	131072	16,00	0,50	61,40	61,39	61,41	61,40	61,39	61,38	61,26
512 × 512	75	196608	24,00	0,75	59,61	59,61	59,61	59,61	59,60	59,61	58,96
512 × 512	90	235968	28,80	0,90	58,79	58,80	58,80	58,79	58,79	58,82	57,79
512 × 512	100	262144	32,00	1,00	58,31	58,30	58,31	58,32	58,31	58,32	57,16

Tablo 4.6.'da ise aynı test görüntülerin 8 bit gri seviye dönüştürülmüş biçimlerine ait PSNR değerleri verilmektedir. Farklı boyutlardaki görüntülere ve farklı veri miktarlarının, önerilen yöntem kullanılarak gizlenmesi sonucunda PNSR değerlerinin en düşük 52,76 dB olduğu en yüksek ise 63,74 dB olduğu hesaplanmıştır.

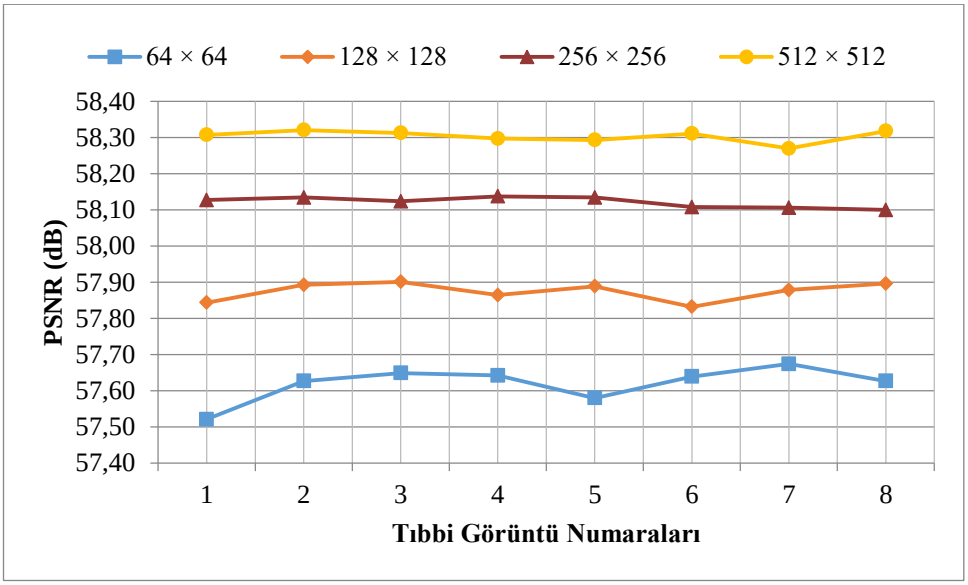
Tablo 4.6. Gri seviyeli standart test görüntülere ait PSNR değerleri

Boyut	Oran	Bit	Miktar		Test Görüntüleri						
			KB	bpp	Lena	Pepper	House	Baboon	F-16	Lake	Tiffany
64 × 64	20	832	0,10	0,20	59,91	59,91	59,89	59,80	59,97	59,91	59,74
64 × 64	25	1024	0,13	0,25	59,11	59,00	59,06	59,10	59,06	59,08	59,04
64 × 64	50	2048	0,25	0,50	56,01	56,01	56,05	55,96	55,99	56,11	55,91
64 × 64	75	3072	0,38	0,75	54,12	54,25	54,05	54,19	54,16	54,20	54,27
64 × 64	90	3712	0,45	0,91	53,30	53,43	53,29	53,33	53,34	53,34	53,35
64 × 64	100	4096	0,50	1,00	52,76	52,83	52,90	52,86	52,86	52,84	52,90
128 × 128	10	1664	0,20	0,10	63,17	63,14	63,19	63,29	63,10	63,33	63,23
128 × 128	20	3328	0,41	0,20	60,08	60,08	60,09	60,24	60,11	60,16	60,10
128 × 128	25	4096	0,50	0,25	59,27	59,26	59,22	59,30	59,31	59,24	59,27
128 × 128	50	8192	1,00	0,50	56,24	56,28	56,19	56,29	56,20	56,14	56,19
128 × 128	75	12288	1,50	0,75	54,38	54,40	54,46	54,42	54,50	54,43	54,42
128 × 128	90	14784	1,80	0,90	53,62	53,60	53,59	53,57	53,65	53,58	53,63
128 × 128	100	16384	2,00	1,00	53,10	53,11	53,14	53,10	53,15	53,11	53,13
256 × 256	10	6592	0,80	0,10	63,44	63,45	63,43	63,49	63,41	63,48	63,47
256 × 256	20	13120	1,60	0,20	60,42	60,45	60,38	60,42	60,47	60,44	60,45
256 × 256	25	16384	2,00	0,25	59,50	59,47	59,45	59,48	59,48	59,47	59,52
256 × 256	50	32768	4,00	0,50	56,47	56,44	56,42	56,43	56,43	56,41	56,40
256 × 256	75	49152	6,00	0,75	54,64	54,65	54,66	54,66	54,66	54,66	54,68
256 × 256	90	59008	7,20	0,90	53,84	53,85	53,83	53,82	53,84	53,84	53,81
256 × 256	100	65536	8,00	1,00	53,33	53,34	53,34	53,34	53,35	53,32	53,34
512 × 512	10	26240	3,20	0,10	63,65	63,62	63,62	63,61	63,74	63,66	63,70
512 × 512	20	52480	6,41	0,20	60,67	60,61	60,64	60,64	60,65	60,61	60,63
512 × 512	25	65536	8,00	0,25	59,65	59,64	59,64	59,64	59,64	59,65	59,66
512 × 512	50	131072	16,00	0,50	56,65	56,64	56,62	56,62	56,64	56,63	56,62
512 × 512	75	196608	24,00	0,75	54,84	54,85	54,83	54,87	54,84	54,83	54,85
512 × 512	90	235968	28,80	0,90	54,04	54,04	54,04	54,03	54,02	54,04	54,03
512 × 512	100	262144	32,00	1,00	53,54	53,55	53,55	53,55	53,54	53,55	53,52

Şekil 4.18. ve 4.19.'da verilen grafiklerde önerilen yöntem kullanılarak farklı çözünürlüklerdeki 8 farklı patoloji görüntüsüne 1 bpp değerinde veri gizleme işlemi sonucunda elde edilen MSE ve PSNR değerleri görülmektedir. PSNR değerlerinin 57,52 dB – 58,32 dB aralığında değiştiği görülmektedir.



Şekil 4.18. Tıbbi görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu elde edilen MSE başarımları



Şekil 4.19. Tıbbi görüntülerde önerilen yöntem kullanılarak yapılan veri gizleme sonucu elde edilen PSNR başarımları

Tablo 4.7.'de tez çalışmasında geliştirilen veri gizleme yöntemi ile literatürde yer alan bazı veri gizleme çalışmalarının başarım sonuçları karşılaştırmaları olarak verilmektedir. Tablo 4.7.'de yer alan literatürdeki yöntemlerin yapmış olduğu başarım değerlendirmelerine benzer örtü görüntüsü ve veri miktarı kullanılmıştır. Tablo 4.7.'de yer alan literatür çalışmalarının yaklaşık %65'indeki aynı örtü görüntüsü ve veri miktarı kullanılmıştır. Sonuçlar incelendiğinde geliştirilen yöntemin kullanılmasıyla elde edilen PSNR değeri daha yüksek çıkmaktadır. Buda geliştirilen yöntemin daha iyi sonuç verdiği ve stego görüntünün örtü görüntüsüne daha benzer yani daha az bozulduğunu göstermektedir.

Tablo 4.7. Önerilen yöntemin literatürdeki diğer veri gizleme yöntemlerine karşı PSNR başarım sonuçları

Yöntemler	Yöntemlerin Sonuçları			Önerilen Yöntem Sonuçları		
	Görüntü Bilgisi	Veri Miktarı	PSNR (dB)	Görüntü Bilgisi	Veri Miktarı	PSNR (dB)
Toony ve ark., 2009	(1)	32768 bit	47,03	(1)	32768 bit	62,73
Luo ve ark., 2010	(1)	%10	61,9	(1)	%10	63,74
Luo ve ark., 2010	(1)	%50	54,1	(1)	%50	56,65
Lou ve Hu, 2012	(1)	262144 bit	50,51	(1)	262144 bit	53,55
Lou ve Hu, 2012	(1)	%90	50,51	(1)	%100	53,55
Amirtharajan ve Rayappan, 2012	Lena(1)	65536 bit	52,25	Lena(1)	65536 bit	53,33
Amirtharajan ve Rayappan, 2012	Baboon(1)	65536 bit	52,25	Baboon(1)	65536 bit	53,34
Amirtharajan ve Rayappan, 2012	F16(1)	65536 bit	52,28	F16(1)	65536 bit	53,35
Iranpour ve Farokhian, 2013	(1)	0,1 bpp	62	(1)	0,1 bpp	63,66
Akar ve ark., 2013	Lena(1)	32 KB	51,16	Lena(1)	32 KB	53,54
Hong, 2013	Lena(1)	1 bpp	52,4	Lena(1)	1 bpp	53,54
Hong, 2013	F16(1)	1 bpp	52,38	F16(1)	1 bpp	53,54
Hong, 2013	Peppers(1)	1 bpp	52,39	Peppers(1)	1 bpp	53,55
Hong, 2013	Baboon(1)	1 bpp	52,38	Baboon(1)	1 bpp	53,55
Bedi ve ark., 2013	F16(1)	131072 bit	45,38	F16(1)	131072 bit	56,64
Bedi ve ark., 2013	Lake(1)	131072 bit	45,67	Lake(1)	131072 bit	56,63
Bedi ve ark., 2013	Baboon(1)	131072 bit	44,31	Baboon(1)	131072 bit	56,62
Lavania ve ark., 2014	Lena(2)	49152 bit	49,09	Lena(2)	49152 bit	54,67

Tablo 4.7. (Devamı)

Yöntemler	Yöntemlerin Sonuçları			Önerilen Yöntem Sonuçları		
	Görüntü Bilgisi	Veri Miktarı	PSNR (dB)	Görüntü Bilgisi	Veri Miktarı	PSNR (dB)
Kanan ve Nazeri, 2014	F16[(1)]	32768 bit	54,3	F16[(1)]	32768 bit	56,43
Kanan ve Nazeri, 2014	F16[(1)]	0,5 bpp	54,3	F16[(1)]	0,5 bpp	56,65
Kanan ve Nazeri, 2014	Peppers[(1)]	32768 bit	54,28	Peppers[(1)]	32768 bit	56,44
Kanan ve Nazeri, 2014	Baboon[(1)]	32768 bit	54,25	Baboon[(1)]	32768 bit	56,43
Sarreshedari ve Akhaee, 2014	Lena[(1)]	0,5 bpp	52,91	Lena[(1)]	0,5 bpp	56,65
Sajasi ve Moghamad, 2015	Baboon[(1)]	262144 bit	52,72	Baboon[(1)]	262144 bit	53,55
Sajasi ve Moghamad, 2015	Baboon[(1)]	131072 bit	54,11	Baboon[(1)]	131072 bit	56,62
Sajasi ve Moghamad, 2015	Lena[(1)]	131072 bit	54,33	Lena[(1)]	131072 bit	56,32
Li ve ark., 2015	[(1)]	10000 bit	63,88	[(1)]	16384 bit	65,69
Al-Dmour var ark.,2015	[(1)]	%10	61,86	[(1)]	%10	63,49
Al-Dmour var ark.,2015	[(1)]	%25	57,83	[(1)]	%25	59,52
Ou ve ark., 2015	F16[(2)]	50000 bit	60,13	F16[(2)]	52480	65,4
Al-Dmour ve Al-Ani,2016	[(1)]	%20	58,96	[(1)]	%20	60,67
Al-Dmour ve Al-Ani,2016	[(1)]	%25	57,99	[(1)]	%25	59,68
Tuncer ve Avcı, 2016	[(2)]	1 bpp	56	[(2)]	1 bpp	58,32
Tuncer ve Avcı, 2016	[(2)]	0,5bpp	59	[(2)]	0,5bpp	61,42

[(1)] 8 bit renk derinliğindeki gri seviyeli stego görüntüdür, [(2)] 24 bit renk derinliğindeki renkli stego görüntüdür.

Tablo 4.7.'de yer alan bazı literatür çalışmalarında tez çalışmasında önerilen yönteme kıyasla, aynı boyutta örtü görüntüsü kullanılmasına karşın daha az veri gizlenmesi sonucu elde edilen PSNR değerleri daha düşük çıkmıştır. Buda geliştirilen yöntemin daha iyi olduğunun bir göstergesidir.

4.5. Evrensel Görüntü Kalite İndeksi (UQI)

Wang ve Bovik (2002) tarafından geliştirilen Evrensel Görüntü Kalite İndeksi orijinal görüntüler ve bozulmaya uğramış görüntüler arasında insan görme sistemine dayalı bir görüntü kalite ölçütüdür. Görüntüdeki korelasyon kaybı, parlaklık

bozulması ve kontrast bozulmasına dayalı olarak üç etkene göre hesaplanmaktadır (Wang ve Bovik, 2002; Sun, 2016). Bu görüntü kalite ölçütünün alacağı değer aralığı [-1, 1] olarak ifade edilmiştir (Jindal ve Singh, 2014). UQI Denklem 4.7.'e göre elde edilmektedir.

$$\mathrm{UQI}(o,s) = \frac{(4\mu_s\mu_o 2\sigma_{so})}{(\mu_s^2 + \mu_s^2)(\sigma_s^2 + \sigma_s^2)} \tag{4.7}$$

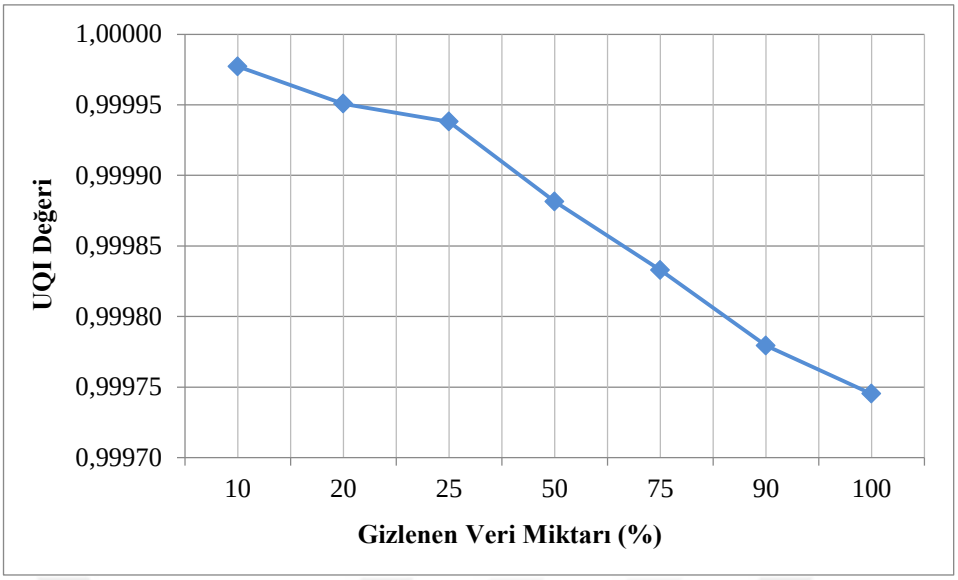
Burada, O orijinal görüntüyü ve S ise stego görüntüyü ifade etmektedir. μ_o orijinal görüntünün ortalaması, μ_s stego görüntünün ortalaması, σ_o orijinal görüntünün standart sapması, σ_s stego görüntünün standart sapması, σ_{os} orijinal görüntü ve stego görüntünün kovaryansı (covariance) olarak ifade edilir (Wang ve Bovik, 2002).

Tablo 4.8. incelendiğinde 24 bit renkli ve 8 bit gri seviyeli görüntülerde farklı boyuttaki stego görüntülere ait farklı veri miktarlarındaki UQI değeri görülmektedir. Her test satırı için UQI değerinin en iyi sonuç olan 1 değerine yakın olduğu hesaplanmıştır. Görüntü boyutuna göre gizlenecek veri miktarı arttığında UQI değerinin küçüldüğü fark edilmektedir. Buda görüntüdeki bozulma miktarının arttığını ifade etmektedir. Her ne kadar bozulma oranı artsa da UQI değerlerinde en yüksek ve en düşük değer arasında sayısal olarak fazla bir fark olmadığı görülmektedir.

Şekil 4.20.'de 512×512 boyutundaki 24 bit renkli görüntülere %10 − %100 oranında veri gizlenmesi sonucu elde edilen UQI değerleri görülmektedir. En yüksek değer %10 veri miktarı ile 0,999977 olarak hesaplanırken, en düşük değer %100 veri miktarında 0,999745 olarak hesaplanmıştır. Bu iki değer arasında 0,000232 gibi bir fark vardır. Her piksele veri gizlense de yapılan değişim az olmasından dolayı çok az bir fark oluştuğu gözlenmektedir.

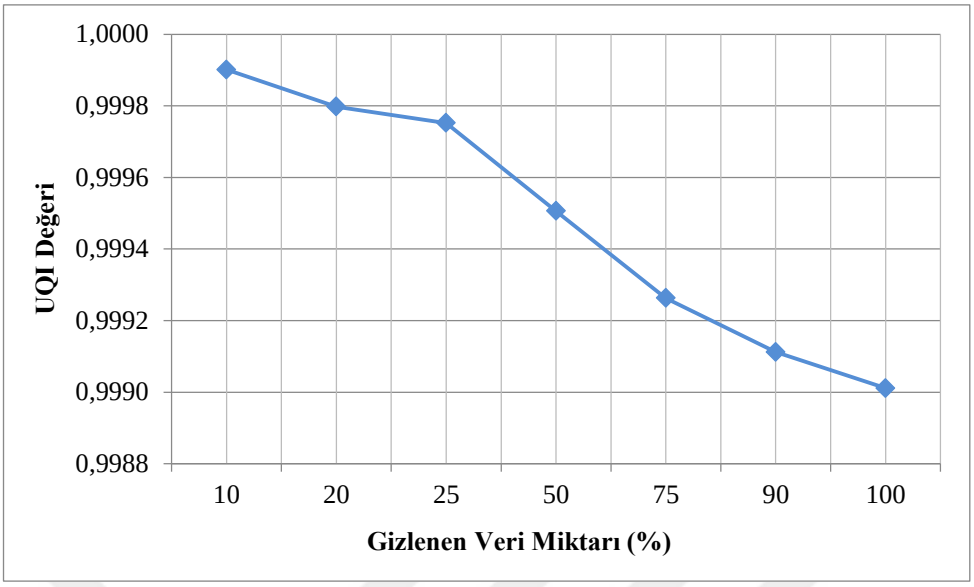
Tablo 4.8. Önerilen yöntemin kullanılması ile elde edilen UQI değerleri

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	UQI (24 bit)	UQI (8 bit)
32 × 32	12,5	128	0,02	0,13	0,999997	0,999985
32 × 32	25	256	0,03	0,25	0,999992	0,999973
32 × 32	50	512	0,06	0,50	0,999979	0,999901
32 × 32	75	768	0,09	0,75	0,999970	0,999870
32 × 32	94	960	0,12	0,94	0,999963	0,999843
32 × 32	100	1024	0,13	1,00	0,999964	0,999807
64 × 64	10	448	0,05	0,11	0,999994	0,999969
64 × 64	20	832	0,10	0,20	0,999990	0,999938
64 × 64	25	1024	0,13	0,25	0,999982	0,999896
64 × 64	50	2048	0,25	0,50	0,999968	0,999793
64 × 64	75	3072	0,38	0,75	0,999946	0,999616
64 × 64	90	3712	0,45	0,91	0,999934	0,999510
64 × 64	100	4096	0,50	1,00	0,999930	0,999437
128 × 128	10	1664	0,20	0,10	0,999995	0,999943
128 × 128	20	3328	0,41	0,20	0,999989	0,999843
128 × 128	25	4096	0,50	0,25	0,999989	0,999809
128 × 128	50	8192	1,00	0,50	0,999976	0,999620
128 × 128	75	12288	1,50	0,75	0,999964	0,999400
128 × 128	90	14784	1,80	0,90	0,999956	0,999293
128 × 128	100	16384	2,00	1,00	0,999950	0,999219
256 × 256	10	6592	0,80	0,10	0,999992	0,999911
256 × 256	20	13120	1,60	0,20	0,999984	0,999821
256 × 256	25	16384	2,00	0,25	0,999976	0,999766
256 × 256	50	32768	4,00	0,50	0,999953	0,999555
256 × 256	75	49152	6,00	0,75	0,999926	0,999281
256 × 256	90	59008	7,20	0,90	0,999916	0,999114
256 × 256	100	65536	8,00	1,00	0,999905	0,999034
512 × 512	10	26240	3,20	0,10	0,999977	0,999901
512 × 512	20	52480	6,41	0,20	0,999951	0,999798
512 × 512	25	65536	8,00	0,25	0,999938	0,999752
512 × 512	50	131072	16,00	0,50	0,999881	0,999506
512 × 512	75	196608	24,00	0,75	0,999833	0,999263
512 × 512	90	235968	28,80	0,90	0,999779	0,999112
512 × 512	100	262144	32,00	1,00	0,999745	0,999011



Şekil 4.20. 512×512 boyutundaki 24 bit renkli görüntülerin farklı veri miktarına göre UQI değerinin değişim grafiği

Şekil 4.21.'de 512×512 boyutundaki 8 bit renkli görüntülere %10 − %100 oranında veri gizlenmesi sonucu elde edilen UQI değerleri görülmektedir. En yüksek değer ile en düşük değer arasındaki fark yaklaşık olarak 0,0008 seviyesindedir. Bu farkın aynı görüntünün aynı boyuttaki farklı veri miktarı için olduğu göz önüne alınırsa geliştirilen yöntemin oldukça başarılı bir görsel kalite sunduğu anlaşılmaktadır. Çok veri miktarı ile stego görüntüde az UQI değişimi sağlanmıştır. Bu durum stego görüntünün örtü görüntüsüne olan benzerliğinin en üst seviyede korunduğunu göstermektedir.



Şekil 4.21. 512×512 boyutundaki 8 bit renkli görüntülerin farklı veri miktarına göre UQI değerinin değişim grafiği

4.6. Ortalama Yapısal Benzerlik (M−SSIM)

Wang ve ark. (2004) tarafından geliştirilen Ortalama Yapısal Benzerlik bir görüntü kalite ölçütü olarak kullanılmaktadır. Orijinal görüntü ile bozulma meydana gelmiş iki görüntü arasındaki görsel kalite miktarını ölçmek için kullanılmaktadır. M–SSIM değeri en alt 0 ve en üst değer olarak 1 ile ifade edilir. [0 – 1] aralığındaki en iyi değer 1'dir. M–SSIM değeri SSIM ölçütünden elde edilmektedir. Denklem 4.8.' e göre SSIM ölçütünün alacağı değer hesaplanır.

$$\mathrm{SSIM}(o,s) = \frac{(2\mu_s\mu_o + C_1)(2\sigma_{so} + C_2)}{(\mu_s^2 + \mu_s^2 + C_1)(\sigma_s^2 + \sigma_s^2 + C_2)} \tag{4.8}$$

Burada, O orijinal görüntüyü ve S ise stego görüntüyü ifade etmektedir. μ_o orijinal görüntünün ortalamasını, μ_s stego görüntünün ortalamasını, σ_o orijinal görüntünün standart sapmasını, σ_s stego görüntünün standart sapmasını, σ_{os} orijinal görüntü ve stego görüntünün kovaryansını (covariance) göstermektedir. $C_1=(K_1L)^2$ ve $C_2=(K_2L)^2$ olarak ifade edilir. C_1 ve C_2 bölme işleminde paydayı dengede tutmak için kullanılan değişkenlerdir. L sabiti bir pikselin alabileceği dinamik değer aralığını belirtmektedir (8 bit ile ifade edilebilen bir pikseldeki değer için 2^8-1 = 255 olarak

alınır ve bu varsayılan değerdir), K_1 sabiti 0,01 ve K_2 sabiti 0,03 olarak alınır. Bu değerler varsayılan değerlerdir. M–SSIM değerinin hesaplandığı formül Denklem 4.9.'da görülmektedir (Wang ve ark., 2004; Karakış ve ark., 2015).

$$M - SSIM(o, s) = \frac{1}{M}\sum_{j=1}^{M} SSIM(o_j, s_j) \tag{4.9}$$

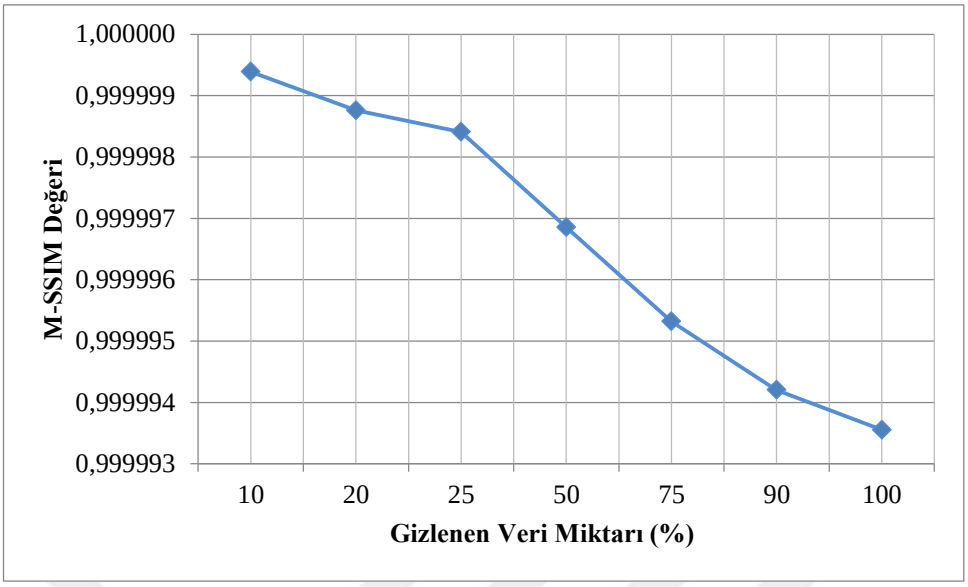
Burada O orijinal görüntüyü, S bozulmaya uğramış (işlem görmüş) görüntüyü, M değeri SSIM değerinin bulunmasında kullanılan yerel (local) pencere sayısını, o_j, s_j M adet yerel penceredeki *j.* görüntü içeriğini temsil etmektedir. M–SSIM görüntünün elde edilen M adet pencereye ait olan SSIM değerlerinin ortalaması olarak hesaplanır (Wang ve ark., 2004).

Tablo 4.9.'da 24 bit renkli ve 8 bit gri seviyeli görüntülere ait M–SSIM değerleri yer almaktadır. Farklı boyuttaki görüntülerin farklı veri miktarlarına ait olan M–SSIM değerleri incelendiğinde değerlerin M–SSIM'in en üst değeri olan 1'e çok yakın olduğu gözlenmektedir. Buda önerilen yöntemin orijinal görüntüye göre görsel kalitesinde az değişim yaptığını ifade etmektedir. Böylece stego görüntünün kalitesinin örtü görüntüsüne oldukça yakın olduğu sonucu elde edilmektedir.

Şekil 4.22.'de 512×512 boyutundaki 24 bit renkli görüntülere %10 − %100 oranında veri gizlenmesi sonucu elde edilen M–SSIM değerleri görülmektedir. Örtü görüntüsüne gizlenecek veri miktarı arttıkça görsel kalitesinde düşme olduğu gözlenmektedir. En yüksek değer 0,99999939 iken en düşük değer 0,99999355 olarak hesaplanmıştır. En düşük ve yüksek değer arasındaki fark 0,00000584 olarak hesaplanmaktadır. En düşük değerin bile M–SSIM'in en iyi değeri olan 1'e çok yakın olduğu görülmektedir. Önerilen yöntem ile yapılan gizlemenin görüntünün görsel kalitesinde çok fazla değişim yapmadığı anlaşılmaktadır.

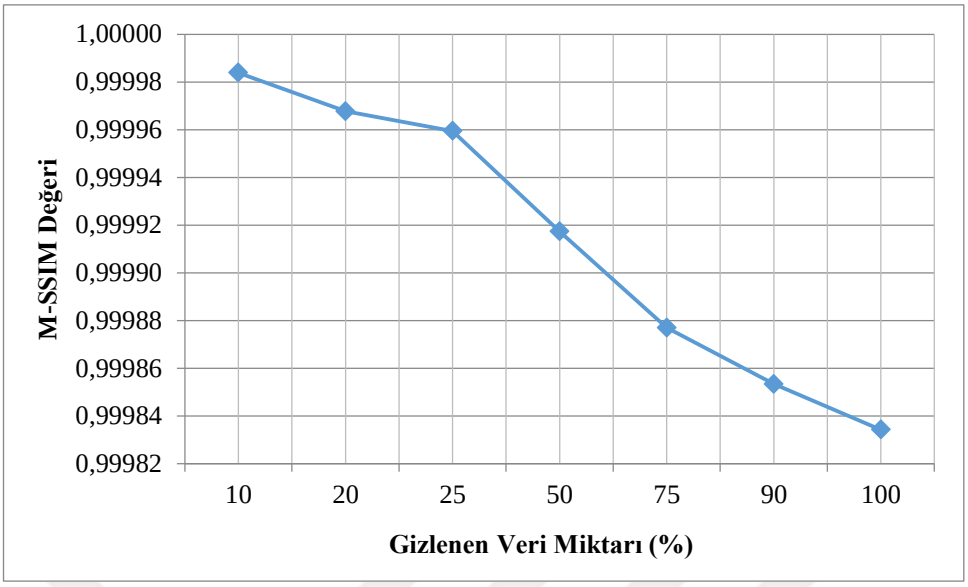
Tablo 4.9. Önerilen yöntemin kullanılması ile elde edilen M − SSIM değerleri

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	M – SSIM (24 bit)	M – SSIM (8 bit)
32 × 32	12,5	128	0,02	0,13	0,99999998	0,99999819
32 × 32	25	256	0,03	0,25	0,99999924	0,99998941
32 × 32	50	512	0,06	0,50	0,99999606	0,99994243
32 × 32	75	768	0,09	0,75	0,99999594	0,99992394
32 × 32	94	960	0,12	0,94	0,99999347	0,99989689
32 × 32	100	1024	0,13	1,00	0,99999205	0,99988758
64 × 64	10	448	0,05	0,11	0,99999862	0,99997975
64 × 64	20	832	0,10	0,20	0,99999708	0,99993268
64 × 64	25	1024	0,13	0,25	0,99999555	0,99990525
64 × 64	50	2048	0,25	0,50	0,99999017	0,99983164
64 × 64	75	3072	0,38	0,75	0,99998658	0,99969834
64 × 64	90	3712	0,45	0,91	0,99998328	0,99961189
64 × 64	100	4096	0,50	1,00	0,99998157	0,99958680
128 × 128	10	1664	0,20	0,10	0,99999858	0,99995120
128 × 128	20	3328	0,41	0,20	0,99999638	0,99986310
128 × 128	25	4096	0,50	0,25	0,99996691	0,99983662
128 × 128	50	8192	1,00	0,50	0,99999203	0,99969354
128 × 128	75	12288	1,50	0,75	0,99998874	0,99951594
128 × 128	90	14784	1,80	0,90	0,99998601	0,99941471
128 × 128	100	16384	2,00	1,00	0,99998436	0,99935362
256 × 256	10	6592	0,80	0,10	0,99999743	0,99992744
256 × 256	20	13120	1,60	0,20	0,99999494	0,99986268
256 × 256	25	16384	2,00	0,25	0,99999372	0,99982406
256 × 256	50	32768	4,00	0,50	0,99998610	0,99964988
256 × 256	75	49152	6,00	0,75	0,99997957	0,99946112
256 × 256	90	59008	7,20	0,90	0,99997591	0,99932395
256 × 256	100	65536	8,00	1,00	0,99997238	0,99926177
512 × 512	10	26240	3,20	0,10	0,99999939	0,99998391
512 × 512	20	52480	6,41	0,20	0,99999876	0,99996774
512 × 512	25	65536	8,00	0,25	0,99999841	0,99995946
512 × 512	50	131072	16,00	0,50	0,99999686	0,99991731
512 × 512	75	196608	24,00	0,75	0,99999532	0,99987702
512 × 512	90	235968	28,80	0,90	0,99999420	0,99985342
512 × 512	100	262144	32,00	1,00	0,99999355	0,99983429



Şekil 4.22. 512×512 boyutundaki 24 bit renkli görüntülerin farklı veri miktarına göre M – SSIM değerinin değişim grafiği

Şekil 4.23.'de 512×512 boyutundaki 8 bit gri seviyeli görüntülere %10 − %100 oranında veri gizlenmesi sonucu elde edilen M–SSIM değerleri görülmektedir. Örtü görüntüsüne gizlenecek veri miktarı arttıkça görsel kalitesinde düşme olduğu gözlenmektedir. En yüksek değer 0,99998391 iken en düşük değerin %100 veri miktarında 0,99983429 olarak hesaplanmıştır. En düşük ve yüksek değer arasındaki fark 0,00014962 olarak hesaplanmaktadır. Renkli görüntülerde olduğu gibi en düşük değerin bile M–SSIM'in en iyi değeri olan 1'e çok yakın olduğu görülmektedir. Bu sonuç önerilen yöntemin kullanıldığı veri gizleme işlemlerinde, stego görüntünün görsel kalitesinde çok fazla değişimin yapılmadığını göstermektedir.



Şekil 4.23. 512×512 boyutundaki 8 bit renkli görüntülerin farklı veri miktarına göre M – SSIM değerinin değişim grafiği

4.7. Renkli Görüntü Kalite Ölçütü (CQM)

Yalman ve Ertürk (2013) tarafından geliştirilen yöntem renkli görüntülerde kullanılan bir görüntü kalite ölçütüdür. Parlaklık ve renklilik değerleri ile ifade edilen YUV renk modeline ve PSNR değerine dayalı bir görüntü kalite ölçütüdür. Denklem 4.10. kullanılarak hesaplanır (Yalman ve Ertürk, 2013).

$$\mathrm{CQM} = (\mathrm{PSNR_Y} \times \mathrm{R_W}) + \left(\frac{\mathrm{PSNR_U} + \mathrm{PSNR_V}}{2}\right) \times \mathrm{C_W} \qquad (4.10)$$

Burada $\mathrm{PSNR_Y}$, $\mathrm{PSNR_U}$ ve $\mathrm{PSNR_V}$ değerleri görüntünün Y, U ve V renk kanallarına ait PSNR değerlerini ifade etmektedir. $\mathrm{R_W}$ ve $\mathrm{C_W}$ ise sırasıyla değerleri 0,9449 ve 0,0551 olan insan görme sistemi algılayıcıları ile bağlantılı ağırlıklardır. Bu görüntü kalite ölçütü hesaplanırken RGB renk modelindeki görüntünün ilk önce YUV renk modeline dönüşümünün yapılması gerekmektedir. En iyi sonuç olarak 100 dB değerini vermektedir. Yani çıkan sonuç ne kadar büyükse görüntü kalitesi o kadar iyi denebilir (Yalman ve Ertürk, 2013).

Tablo 4.10.'da 24 bit renkli görüntülere ait farklı veri miktarındaki farklı boyuttaki stego görüntülerin hesaplanan en iyi CQM değerleri görülmektedir. En iyi sonuçta 100 dB olan CQM değerinde Tablo 4.10. incelendiğinde her test için sonuçların iyi olduğu gözlenmektedir. En düşük değer 97,7435 dB iken en iyi sonuç 99,9998 dB olduğu hesaplanmıştır. Geliştirilen veri gizleme yönteminin CQM görüntü kalite ölçütünde de iyi sonuç verdiği görülmektedir.

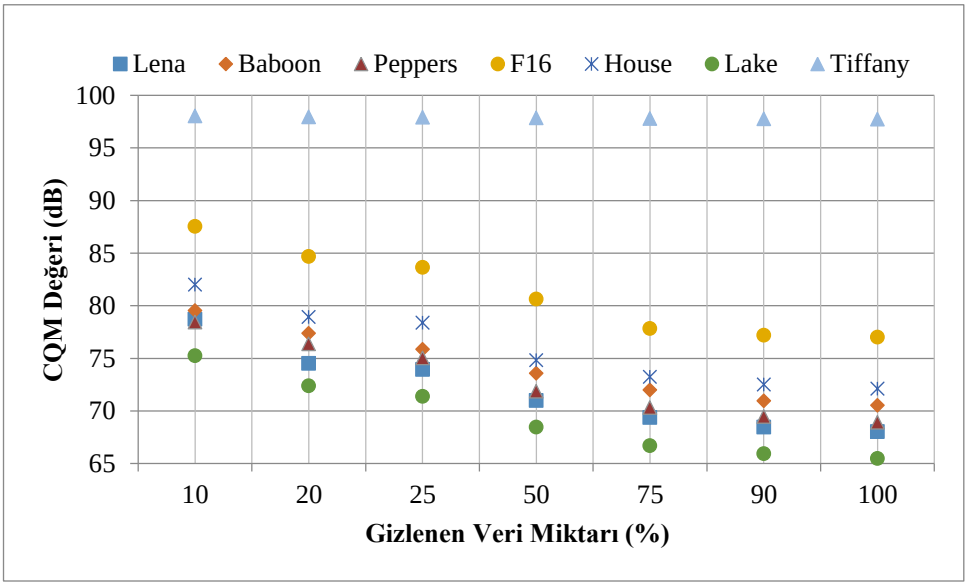
Şekil 4.24.'de 512×512 boyutundaki 24 bit renkli standart test görüntülerinin %10 − %100 oranında veri gizlenmesi sonucunda hesaplanan CQM değerleri verilmektedir. En iyi sonucun Tiffany test görüntüsüne ait olduğu görülmektedir. Diğer test görüntülerinin kendi arasındaki oranlara kıyasla CQM sonuçları incelendiğinde CQM değerlerinin en alt değer ile en üst değer arasında yaklaşık 10 dB fark olduğu görülmektedir.

Tablo 4.10. Önerilen yöntemin kullanılması ile renkli stego görüntülere ait CQM değerleri

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	CQM (dB)
32 × 32	12,5	128	0,02	0,13	99,000000
32 × 32	25	256	0,03	0,25	98,063620
32 × 32	50	512	0,06	0,50	98,020944
32 × 32	75	768	0,09	0,75	97,938011
32 × 32	94	960	0,12	0,94	97,892186
32 × 32	100	1024	0,13	1,00	97,886868
64 × 64	10	448	0,05	0,11	98,223921
64 × 64	20	832	0,10	0,20	98,208626
64 × 64	25	1024	0,13	0,25	98,116484
64 × 64	50	2048	0,25	0,50	98,010451
64 × 64	75	3072	0,38	0,75	97,776587
64 × 64	90	3712	0,45	0,91	97,753699
64 × 64	100	4096	0,50	1,00	97,743565
128 × 128	10	1664	0,20	0,10	98,033274
128 × 128	20	3328	0,41	0,20	97,946533
128 × 128	25	4096	0,50	0,25	97,928895
128 × 128	50	8192	1,00	0,50	97,835728
128 × 128	75	12288	1,50	0,75	97,789553

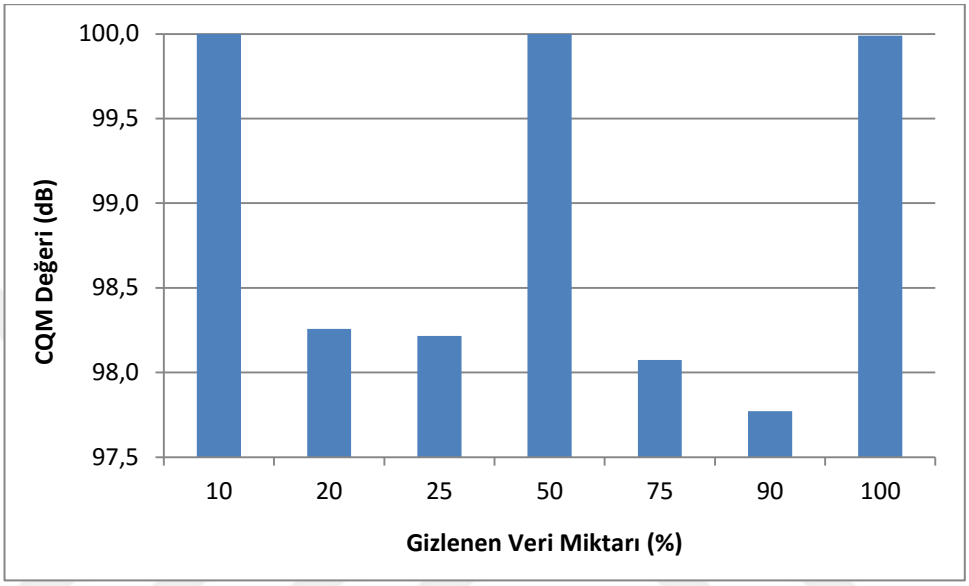
Tablo 4.10. (Devamı)

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	CQM (dB)
128 × 128	90	14784	1,80	0,90	97,759696
128 × 128	100	16384	2,00	1,00	97,751032
256 × 256	10	6592	0,80	0,10	98,039222
256 × 256	20	13120	1,60	0,20	97,949892
256 × 256	25	16384	2,00	0,25	97,933336
256 × 256	50	32768	4,00	0,50	97,847882
256 × 256	75	49152	6,00	0,75	97,797988
256 × 256	90	59008	7,20	0,90	97,768062
256 × 256	100	65536	8,00	1,00	97,754523
512 × 512	10	26240	3,20	0,10	99,999889
512 × 512	20	52480	6,41	0,20	98,256724
512 × 512	25	65536	8,00	0,25	98,216622
512 × 512	50	131072	16,00	0,50	99,998999
512 × 512	75	196608	24,00	0,75	98,074714
512 × 512	90	235968	28,80	0,90	97,771826
512 × 512	100	262144	32,00	1,00	99,989987



Şekil 4.24. 512×512 boyutundaki 24 bit renkli standart test görüntülerin farklı veri miktarına göre CQM değerinin değişim grafiği

Şekil 4.25.'de 512×512 boyutundaki 24 bit renkli görüntülere %10 − %100 oranında gizli veri gizlenmesi sonucu elde edilen en iyi CQM değerleri görülmektedir. Değerlerin hepsi 97,77 dB üzerindedir. Sonuçlar geliştirilen yöntem ile elde edilen stego görüntünün örtü görüntüsüne benzer olduğunu ispatlamaktadır. Böylece örtü görüntüde veri gizleme işlemi yapılırken bozulmanın az olduğu anlaşılmaktadır.



Şekil 4.25. 512×512 boyutundaki 24 bit renkli görüntülerin farklı veri miktarına göre CQM değerinin değişim grafiği

4.8. Ortalama Fark (AD)

Ortalama Fark (Average Difference – AD) orijinal görüntü ve bozulmaya maruz kalmış görüntü arasında farkı hesaplamak için kullanılan istatistiksel yöntemlerden biridir (Eskicioğlu ve Fisher, 1995; Santoso ve ark., 2016;). Hesaplanırken kullanılacak olan formül Denklem 4.11.'de verilmektedir.

$$AD = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| O_{i,j} - S_{i,j} \right| \tag{4.11}$$

Burada O ve S aralarındaki bozulmanın hesaplanacağı birbiriyle kıyaslanan görüntüler olmak üzere; O orijinal görüntüyü, S ise içerisine veri gizlenmiş stego

görüntüyü temsil etmektedir. M ve N değerleri ise görüntülerin boyutlarını temsil etmektedir. Orijinal görüntü ve stego görüntünün farklarının mutlak değeri toplamının ortalaması olan AD değerinin alabileceği en düşük ve en yüksek değerler sırasıyla 0 ve 255 değerleridir. AD'nin küçük çıkması görüntülerin birbirine benzer olduğunu, büyük çıkması ise görüntülerin farklı oldukları anlamına gelmektedir (Sivakumar ve ark., 2010; Debnath ve ark., 2015).

Tablo 4.11.'de 24 bit renkli görüntüler ve 8 bit gri seviyeli görüntüler için elde edilmiş farklı boyutlardaki ve farklı miktarlardaki verilerin gizlenmesi sonucu elde edilen en iyi AD değerleri verilmektedir. Değerler incelendiğinde hem 24 bit renkli görüntülerde hem de 8 bit gri seviyeli görüntülerde AD değerlerinin 0'a yakın olduğu görülmektedir. Bu sonuç orijinal görüntü ve stego görüntünün birbirine benzer olduğunu ifade etmektedir.

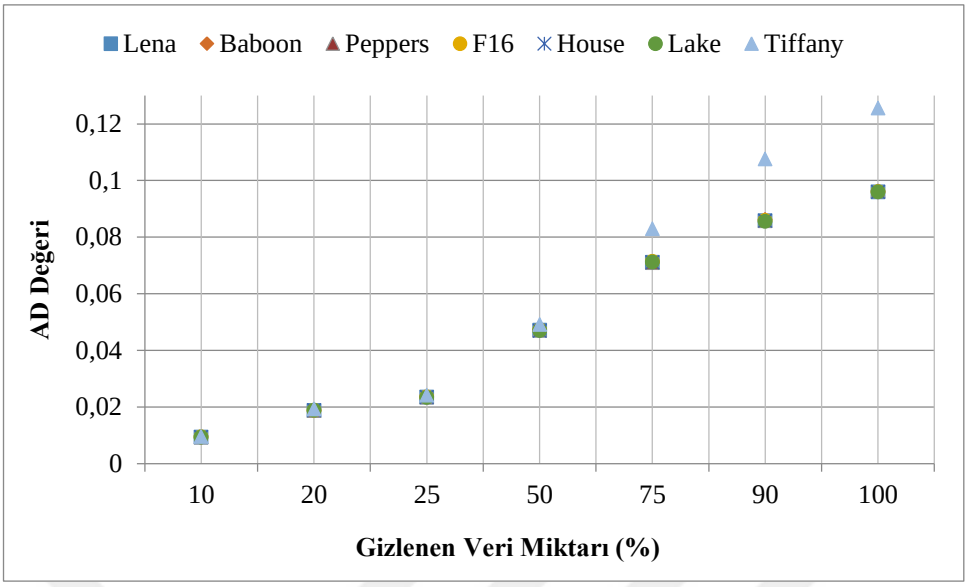
Tablo 4.11. Önerilen yöntemin kullanılması ile elde edilen AD değerleri

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	AD (24 bit)	AD (8 bit)
32 × 32	12,5	128	0,02	0,13	0,012370	0,038086
32 × 32	25	256	0,03	0,25	0,025716	0,083008
32 × 32	50	512	0,06	0,50	0,055664	0,166016
32 × 32	75	768	0,09	0,75	0,085612	0,258789
32 × 32	94	960	0,12	0,94	0,107422	0,325195
32 × 32	100	1024	0,13	1,00	0,115885	0,346680
64 × 64	10	448	0,05	0,11	0,010742	0,034424
64 × 64	20	832	0,10	0,20	0,020833	0,062256
64 × 64	25	1024	0,13	0,25	0,025228	0,076904
64 × 64	50	2048	0,25	0,50	0,053385	0,158203
64 × 64	75	3072	0,38	0,75	0,081217	0,239990
64 × 64	90	3712	0,45	0,91	0,098877	0,295166
64 × 64	100	4096	0,50	1,00	0,110026	0,333984
128 × 128	10	1664	0,20	0,10	0,010071	0,029236
128 × 128	20	3328	0,41	0,20	0,020467	0,061096
128 × 128	25	4096	0,50	0,25	0,025024	0,074585
128 × 128	50	8192	1,00	0,50	0,051066	0,152527
128 × 128	75	12288	1,50	0,75	0,078471	0,230835

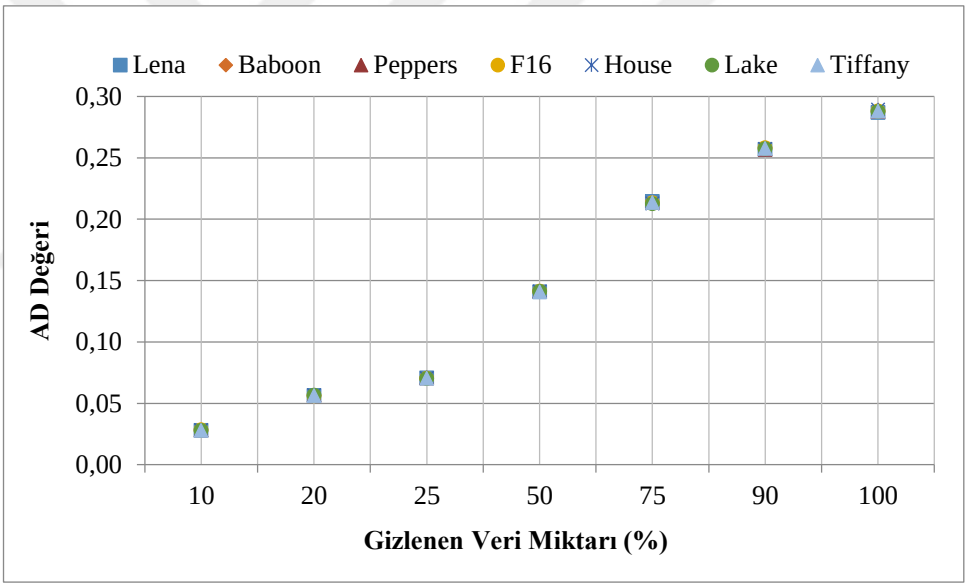
Tablo 4.11. (Devamı)

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	AD (24 bit)	AD (8 bit)
128 × 128	90	14784	1,80	0,90	0,094238	0,281494
128 × 128	100	16384	2,00	1,00	0,104696	0,313904
256 × 256	10	6592	0,80	0,10	0,009603	0,029099
256 × 256	20	13120	1,60	0,20	0,019287	0,058578
256 × 256	25	16384	2,00	0,25	0,024180	0,073273
256 × 256	50	32768	4,00	0,50	0,048843	0,146698
256 × 256	75	49152	6,00	0,75	0,073893	0,221466
256 × 256	90	59008	7,20	0,90	0,089249	0,267715
256 × 256	100	65536	8,00	1,00	0,099706	0,300064
512 × 512	10	26240	3,20	0,10	0,009296	0,027828
512 × 512	20	52480	6,41	0,20	0,018631	0,056103
512 × 512	25	65536	8,00	0,25	0,023327	0,070057
512 × 512	50	131072	16,00	0,50	0,046815	0,140759
512 × 512	75	196608	24,00	0,75	0,070844	0,212444
512 × 512	90	235968	28,80	0,90	0,085496	0,256725
512 × 512	100	262144	32,00	1,00	0,095556	0,286945

Şekil 2.26.'da 512×512 boyutundaki standart test görüntülerine farklı veri miktarlarında yapılan gizleme sonucunda hesaplanan AD değerleri görülmektedir. Şekil 2.27.'de ise aynı test görüntülerinin 8 bit gri seviyeli olanlarına ait sonuçlar yer almaktadır. İki grafikte incelendiğinde sonuçların en iyi değer olan 0'a çok yakın oldukları görülmektedir. Önerilen yöntem ile yapılan veri gizleme işlemi sonucunda örtü görüntüsünün orijinal halinin büyük ölçüde korunduğu anlaşılmaktadır.



Şekil 4.26. 512×512 boyutundaki 24 bit renkli standart test görüntülerin farklı veri miktarına göre AD değerinin değişim grafiği



Şekil 4.27. 512×512 boyutundaki 8 bit gri seviyeli standart test görüntülerin farklı veri miktarına göre AD değerinin değişim grafiği

4.9. Yapısal İçerik (SC)

Orijinal görüntünün piksel değerlerinin karesi toplamının değişime uğrayan görüntünün piksellerinin karesinin toplamına bölümü ile bulunan Yapısal İçerik (Structural Content – SC) Denklem 4.12.'de verilmektedir. Özdeş olan görüntüler için bu değer 1 olarak ifade edilmektedir. SC değeri 1'e yakın ise karşılaştırılan

görüntüler benzerdir sonucu çıkarılmaktadır (Varnan ve ark., 2011; Sivakumar ve ark., 2010).

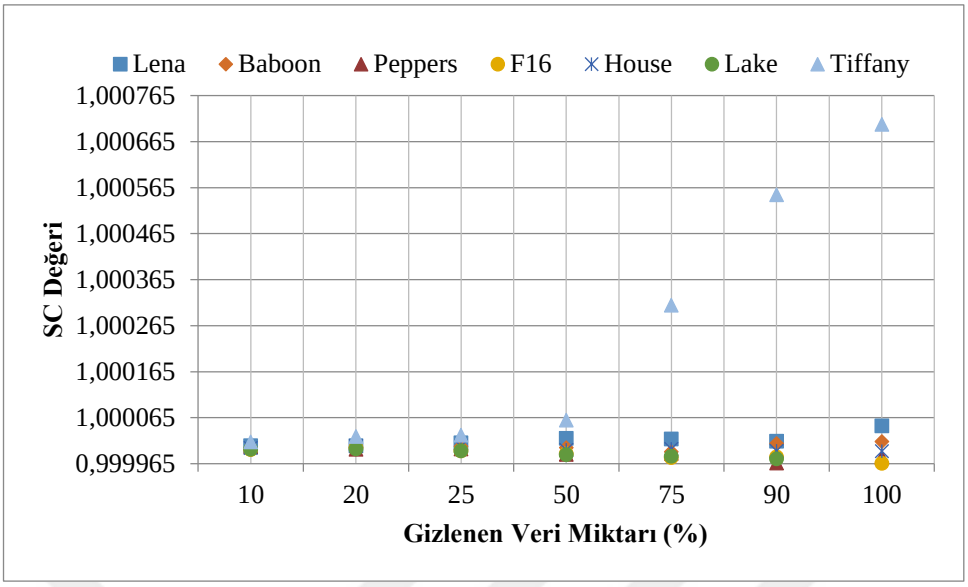
$$SC = \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}\left(O_{i,j}\right)^2}{\sum_{i=0}^{M}\sum_{j=0}^{N}\left(S_{i,j}\right)^2} \tag{4.12}$$

Burada O ve S aralarındaki bozulmanın hesaplanacağı birbiriyle kıyaslanan görüntüler olmak üzere; O orijinal görüntüyü, S ise içerisine veri gizlenmiş stego görüntüyü temsil etmektedir. M ve N değerleri ise görüntülerin boyutlarını temsil etmektedir.

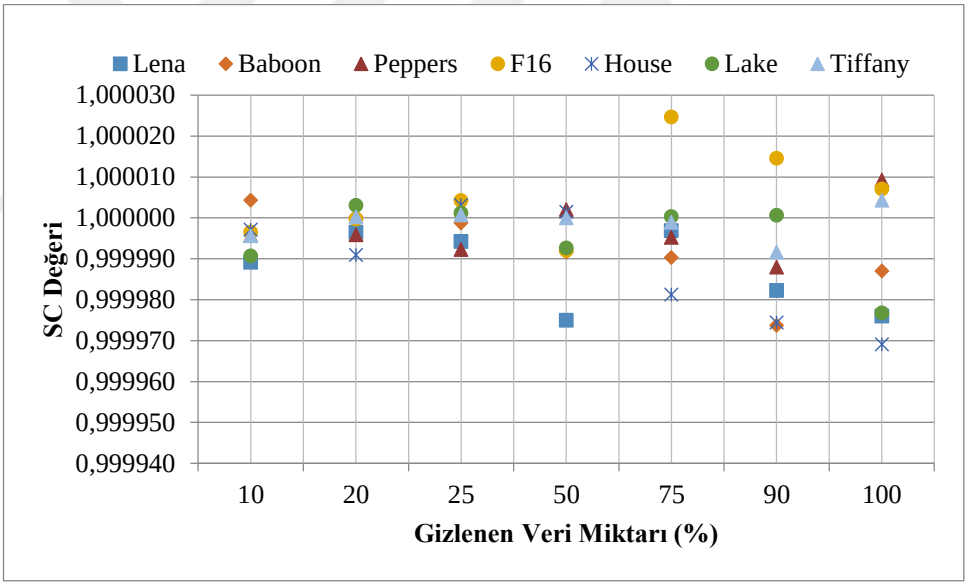
Tablo 4.12.'de 512×512 boyutundaki 24 bit renkli ve 8 bit gri seviyeli standart test görüntülerine farklı oranlarda veri gizlenmesi sonucu elde edilen SC değerleri verilmektedir. Tablo 4.12. incelendiğinde bütün test işlemlerinde elde edilen SC değerinin bire çok yakın olduğu görülmektedir.

Tablo 4.12. Önerilen yöntemin kullanılması ile elde edilen SC değerleri

Görüntü Bilgileri		Veri Miktarı (%)						
		10	20	25	50	75	90	100
Lena	(24 bit)	1,000003	1,000004	1,000010	1,000020	1,000018	1,000013	1,000047
	(8 bit)	0,999989	0,999996	0,999994	0,999975	0,999997	0,999982	0,999976
Baboon	(24 bit)	0,999996	1,000000	1,000002	1,000000	0,999990	1,000009	1,000013
	(8 bit)	1,000004	1,000000	0,999999	0,999992	0,999990	0,999974	0,999987
Peppers	(24 bit)	1,000002	0,999996	0,999997	0,999985	0,999987	0,999966	0,999979
	(8 bit)	0,999996	0,999996	0,999992	1,000002	0,999995	0,999988	1,000009
F16	(24 bit)	0,999996	1,000000	0,999992	0,999986	0,999978	0,999980	0,999965
	(8 bit)	0,999996	1,000000	1,000004	0,999992	1,000025	1,000015	1,000007
House	(24 bit)	0,999999	1,000003	1,000003	0,999995	0,999997	0,999992	0,999992
	(8 bit)	0,999997	0,999991	1,000003	1,000001	0,999981	0,999974	0,999969
Lake	(24 bit)	0,999996	0,999996	0,999993	0,999984	0,999981	0,999975	0,999965
	(8 bit)	0,999991	1,000003	1,000001	0,999993	1,000000	1,000001	0,999977
Tiffany	(24 bit)	1,000012	1,000024	1,000026	1,000059	1,000309	1,000549	1,000702
	(8 bit)	0,999996	1,000000	1,000001	1,000000	0,999999	0,999992	1,000004



Şekil 4.28. 512×512 boyutundaki 24 bit renkli standart test görüntülerin farklı veri miktarına göre SC değerinin değişim grafiği



Şekil 4.29. 512×512 boyutundaki 8 bit gri seviyeli standart test görüntülerin farklı veri miktarına göre SC değerinin değişim grafiği

Şekil 4.28. ve 4.29.'da ve Tablo 4.12.'de verilen değerden elde edilen grafiksel gösterim yer almaktadır. Tiffany test görüntüsü dışında diğer test görüntülerinin en iyi sonuç olan bire oldukça çok yakın olduğu görülmektedir.

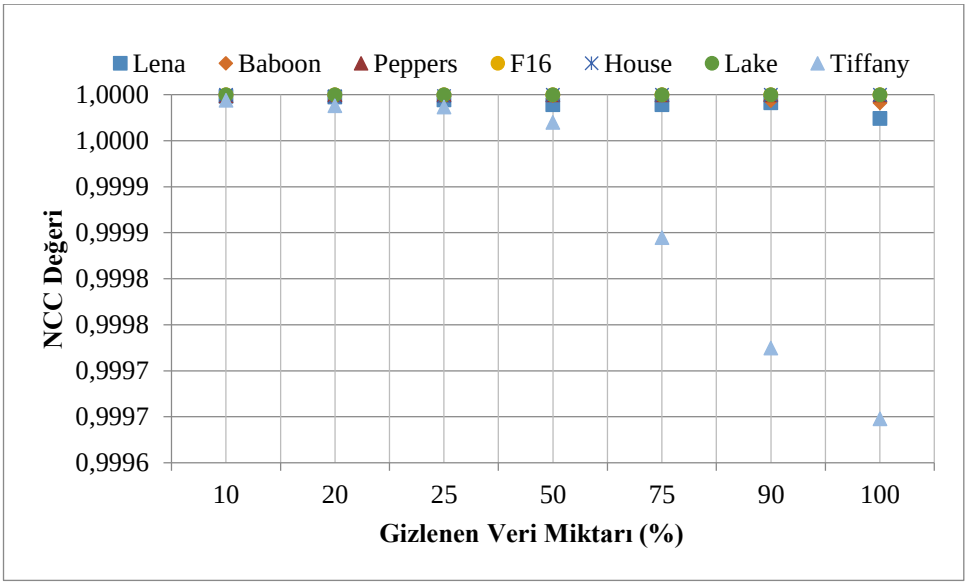
4.10. Normalize Karşıt Korelasyon (NCC)

İki görüntü arasındaki yakınlığı ifade etmek için kullanılan yöntemlerden biri olan Normalize Karşıt Korelasyon (Normalized Cross Correlation – NCC) hesaplanırken Denklem 4.13. kullanılır. Birbirine yakın olan görüntülerde bu değer 1 olarak hesaplanmaktadır (Sivakumar ve ark., 2010; Alzubaydi ve Alshibani, 2014).

$$NCC = \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}(O_{i,j})(S_{i,j})}{\sum_{i=0}^{M}\sum_{j=0}^{N}(O_{i,j})^2} \tag{4.13}$$

Burada O ve S aralarındaki bozulmanın hesaplanacağı birbiriyle kıyaslanan görüntüler olmak üzere; O orijinal görüntüyü, S ise içerisine veri gizlenmiş stego görüntüyü temsil etmektedir. M ve N değerleri ise görüntüleri boyutlarını temsil etmektedir.

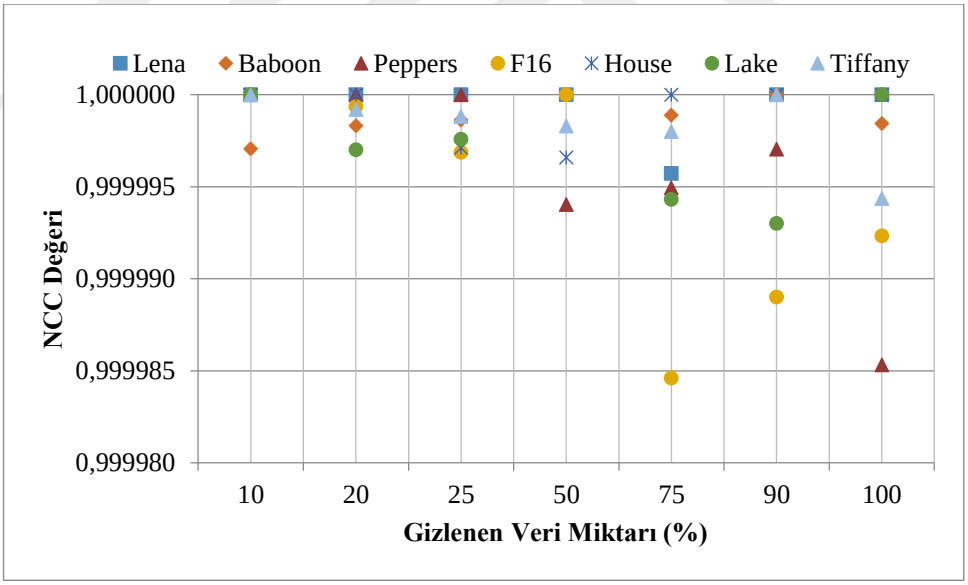
Tablo 4.13.'de 512×512 boyutundaki 24 bit renkli ve 8 bit gri seviyeli standart test görüntülerine farklı oranlarda gizli veri gizlenmesi sonucu elde edilen NCC değerleri verilmiştir. NCC değerlerinin, bütün test görüntülerindeki veri gizleme işlemi sonucunda, en iyi sonuç olan bire yakın olduğu görülmektedir.



Şekil 4.30. 512×512 boyutundaki 24 bit renkli standart test görüntülerin farklı veri miktarına göre NCC değerinin değişim grafiği

Tablo 4.13. Önerilen yöntemin kullanılması ile elde edilen NCC değerleri

Görüntü Bilgileri		Veri Miktarı (%)						
		10	20	25	50	75	90	100
Lena	(24 bit)	0,999998	0,999997	0,999994	0,999989	0,999989	0,999991	0,999974
	(8 bit)	1,000000	1,000000	1,000000	1,000000	0,999996	1,000000	1,000000
Baboon	(24 bit)	1,000000	0,999999	0,999998	0,999999	1,000000	0,999993	0,999991
	(8 bit)	0,999997	0,999998	0,999999	1,000000	0,999999	1,000000	0,999998
Peppers	(24 bit)	0,999999	1,000000	1,000000	1,000000	1,000000	1,000000	1,000000
	(8 bit)	1,000000	1,000000	1,000000	0,999994	0,999995	0,999997	0,999985
F16	(24 bit)	1,000000	1,000000	1,000000	1,000000	1,000000	1,000000	1,000000
	(8 bit)	1,000000	0,999999	0,999997	1,000000	0,999985	0,999989	0,999992
House	(24 bit)	1,000000	0,999998	0,999998	1,000000	1,000000	1,000000	1,000000
	(8 bit)	1,000000	1,000000	0,999997	0,999997	1,000000	1,000000	1,000000
Lake	(24 bit)	1,000000	1,000000	1,000000	1,000000	1,000000	1,000000	1,000000
	(8 bit)	1,000000	0,999997	0,999998	1,000000	0,999994	0,999993	1,000000
Tiffany	(24 bit)	0,999994	0,999988	0,999987	0,999970	0,999845	0,999725	0,999648
	(8 bit)	1,000000	0,999999	0,999999	0,999998	0,999998	1,000000	0,999994



Şekil 4.31. 512×512 boyutundaki 8 bit gri seviyeli standart test görüntülerin farklı veri miktarına göre NCC değerinin değişim grafiği

Şekil 4.30. ve 4.31.'de ise Tablo 4.13.'de verilen değerlerden elde edilen grafiksel gösterim yer almaktadır. Önerilen yöntem ile yapılan veri gizleme sonucunda orijinal görüntü ile stego görüntü arasındaki farkın az olduğu hesaplanmaktadır.

4.11. Normalize Mutlak Hata (NAE)

Normalize Mutlak Hata (Normalized Absolute Error – NAE) görüntünün hata tahmin doğruluğunu ölçmek için kullanılan bir metriktir. NAE'nin alacağı değer aralığı 0 ve 1'dir. Düşük değerin olması orijinal görüntü ile değişime uğramış olan görüntü arasındaki hatanın küçük olduğunu belirtmektedir (Sakuldee ve Udomhunsakul, 2007; Sivakumar ve ark., 2010). Denklem 4.14.'de NAE hesaplanmasında kullanılan formül verilmektedir.

$$NCC = \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}\left|O_{i,j} - S_{i,j}\right|}{\sum_{i=0}^{M}\sum_{j=0}^{N}O_{i,j}} \tag{4.14}$$

Burada O ve S aralarındaki bozulmanın hesaplanacağı birbiriyle kıyaslanan görüntüler olmak üzere; O orijinal görüntüyü, S ise stego görüntüyü temsil etmektedir. M ve N değerleri ise görüntülerin boyutlarını temsil etmektedir.

Tablo 4.14.'de 512×512 boyutundaki 24 bit renkli ve 8 bit gri seviyeli standart test görüntülerine farklı oranlarda veri gizlenmesi sonucu elde edilen NAE değerleri verilmektedir. Tablo 4.14. sonuçları incelendiğinde bütün test görüntülerindeki veri gizleme işlemi sonucunda hesaplanan NAE değerinin en iyi sonuç olan sıfıra yakın olduğu görülmektedir.

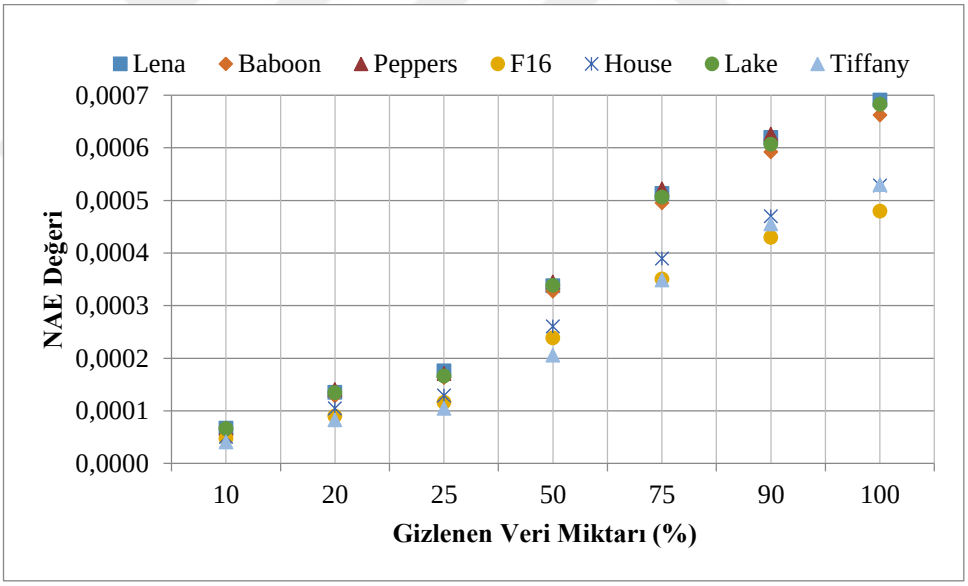
Tablo 4.14. Önerilen yöntemin kullanılması ile elde edilen NAE değerleri

Görüntü Bilgileri		Veri Miktarı (%)						
		10	20	25	50	75	90	100
Lena	(24 bit)	0,000067	0,000135	0,000175	0,000337	0,000513	0,000619	0,000690
	(8 bit)	0,000219	0,000436	0,000550	0,001098	0,001668	0,002007	0,002248
Baboon	(24 bit)	0,000065	0,000129	0,000163	0,000327	0,000496	0,000592	0,000662
	(8 bit)	0,000224	0,000445	0,000560	0,001123	0,001682	0,002039	0,002275
Peppers	(24 bit)	0,000066	0,000141	0,000171	0,000345	0,000522	0,000626	0,000708
	(8 bit)	0,000256	0,000512	0,000640	0,001278	0,001930	0,002327	0,002601
F16	(24 bit)	0,000047	0,000090	0,000116	0,000238	0,000350	0,000430	0,000480
	(8 bit)	0,000151	0,000309	0,000389	0,000777	0,001175	0,001420	0,001587

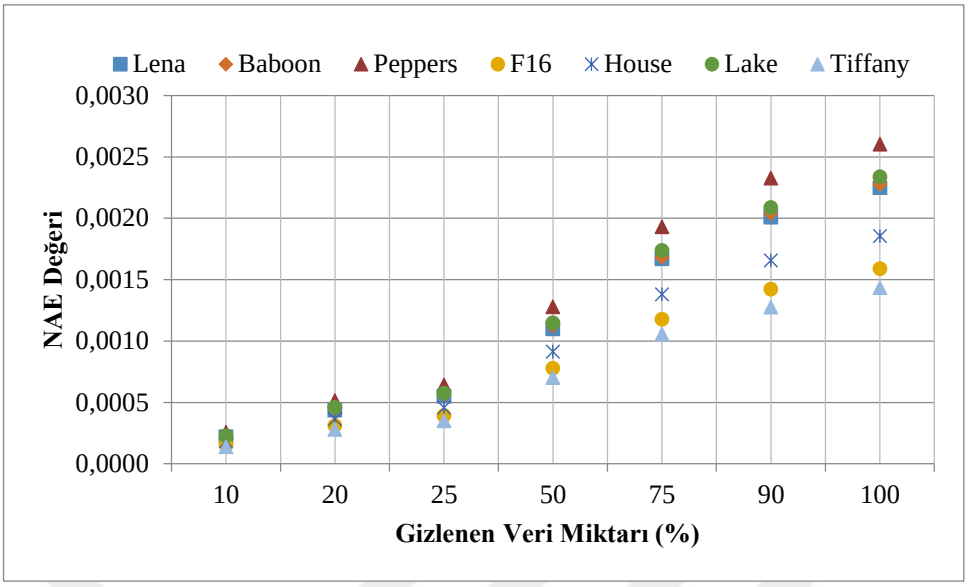
Tablo 4.14. (Devamı)

Görüntü Bilgileri		Veri Miktarı (%)						
		10	20	25	50	75	90	100
House	(24 bit)	0,000050	0,000104	0,000129	0,000261	0,000389	0,000470	0,000528
	(8 bit)	0,000182	0,000362	0,000456	0,000913	0,001380	0,001656	0,001854
Lake	(24 bit)	0,000066	0,000134	0,000166	0,000338	0,000506	0,000606	0,000683
	(8 bit)	0,000227	0,000459	0,000573	0,001147	0,001736	0,002086	0,002335
Tiffany	(24 bit)	0,000041	0,000082	0,000105	0,000206	0,000349	0,000455	0,000530
	(8 bit)	0,000137	0,000278	0,000348	0,000701	0,001055	0,001274	0,001433

Şekil 4.32. ve 4.33.'de 512×512 boyutundaki 24 bit renkli ve 8 bit gri seviyeli standart test görüntüleri ile orijinal görüntüleri arasındaki NAE değerlerinin grafiksel gösterilimi verilmektedir. Önerilen yöntem ile yapılan veri gizleme sonucunda orijinal görüntü ile stego görüntü arasındaki hata değerinin az olduğu hesaplanmaktadır.



Şekil 4.32. 512×512 boyutundaki 24 bit renkli standart test görüntülerin farklı veri miktarına göre NAE değerinin değişim grafiği



Şekil 4.33. 512×512 boyutundaki 8 bit gri seviyeli standart test görüntülerin farklı veri miktarına göre NAE değerinin değişim grafiği

4.12. Steganaliz Başarımı

Steganografi örtü nesnesi üzerinde az değişim yaparak veriyi gizlerken, gizli verinin fark edilmemesini amaçlar. Fakat her ne kadar örtü nesnesinde az değişim yapılsa da oluşan stego nesnesinin istatiksel özelliklerinde değişime neden olunur (Provos ve Honeyman, 2003). İşte meydana gelen bu değişimleri tespit eden yani stego görüntü içerisindeki gizli verinin var olup olmadığı ile uğraşan alana steganaliz denir (Ker ve Pevny, 2014).

Farklı veri gizleme algoritmaları kullanılarak yapılan veri gizlemeleri tespit etmek için istatistiksel yöntemler ile çalışan birkaç steganaliz aracı vardır. Stegdetect, 24 bit renkli görüntülerdeki gizli veriyi ortaya çıkarmak için kullanılan bir araçtır. Stegdetect analiz ettiği görüntülerde gizli veri tespit ettiğinde, bu verinin doğruluğunu birden üçe kadar "*" (yıldız) işareti ile belirtmektedir (Warkentin ve ark., 2008; Khalind ve ark., 2013). İçerisinde gizli veri tespit ettiği görüntülerde "positive", tespit edemediği görüntülerde "negative" mesajlar vermektedir. Ayrıca verdiği "skipped (false positive likely)" mesajı ile görüntüde yanlışlık ile gizli veri bulduğunu ifade etmektedir (Khalind ve ark., 2013). Stegdetect aracı https://github.com/abeluck/stegdetect web adresinden ücretsiz indirilip kullanılabilir.

Steganaliz için kullanılan diğer bir araç ise Stegspy yazılımıdır. Bu yazılım ile görüntü içerisinde gizli verinin olup olmadığı tespit edilir (Singh ve ark., 2013; Ntalianis ve Tsapatsoulis, 2016). Stegspy aracı "detected" mesajı ile gizli veriyi bulduğunu, "no steg found" mesajı ile gizli veri bulamadığını belirtmektedir. Gizli veriyi bulduğunda ise gizli verinin başlangıç adresini vermektedir (Yalman ve ark., 2014). Stegspy aracı http://www.spy-hunter.com web adresinden ücretsiz indirilip kullanılabilir.

Tablo 4.15.'de geliştirilen yöntem ile farklı boyuttaki görüntülere farklı veri miktarları gizlenmesi sonucu elde edilen stego görüntülerinin Stegdetect ve Stegspy steganaliz araçları tarafından test edilmesi sonucunda elde edilen sonuçlar verilmektedir. Stegtedect 64×64 boyutundaki görüntülerin bir kısmı dışında bütün görüntülerde elde edilen sonuç "negative" dir. Yani örtü görüntülerinde gizli veri tespit edilememiştir. Stegspy ile yapılan testlerde ise görüntülerin hiç birinde gizli veri varlığı tespit edilememiştir. Bu sonuçlar geliştirilen yöntemin steganaliz ataklarına karşı başarılı olduğunu göstermektedir. Böylece örtü görüntüsünün iletiminde gizli verinin üçüncü şahıslara karşın korunabildiği anlaşılmaktadır.

Tablo 4.15. Stegdetect ve Stegspy steganaliz araçları sonuçları

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	Stegdetect Sonucu	Stegspy Sonucu
32 × 32	12,5	128	0,02	0,13	(1)	(3)
32 × 32	25	256	0,03	0,25	(1)	(3)
32 × 32	50	512	0,06	0,50	(1)	(3)
32 × 32	75	768	0,09	0,75	(1)	(3)
32 × 32	94	960	0,12	0,94	(1)	(3)
32 × 32	100	1024	0,13	1,00	(1)	(3)
64 × 64	10	448	0,05	0,11	(2)	(3)
64 × 64	20	832	0,10	0,20	(1)	(3)
64 × 64	25	1024	0,13	0,25	(1)	(3)
64 × 64	50	2048	0,25	0,50	(2)	(3)
64 × 64	75	3072	0,38	0,75	(2)	(3)
64 × 64	90	3712	0,45	0,91	(2)	(3)
64 × 64	100	4096	0,50	1,00	(1)	(3)

Tablo 4.15. (Devamı)

Görüntü Boyutu	Gizlenen Veri Oranı	Gizlenen Bit Sayısı	Gizlenen Veri Miktarı (KB)	Gizlenen Veri Miktarı (bpp)	Stegdetect Sonucu	Stegspy Sonucu
128 × 128	10	1664	0,20	0,10	(1)	(3)
128 × 128	20	3328	0,41	0,20	(1)	(3)
128 × 128	25	4096	0,50	0,25	(1)	(3)
128 × 128	50	8192	1,00	0,50	(1)	(3)
128 × 128	75	12288	1,50	0,75	(1)	(3)
128 × 128	90	14784	1,80	0,90	(1)	(3)
128 × 128	100	16384	2,00	1,00	(1)	(3)
256 × 256	10	6592	0,80	0,10	(1)	(3)
256 × 256	20	13120	1,60	0,20	(1)	(3)
256 × 256	25	16384	2,00	0,25	(1)	(3)
256 × 256	50	32768	4,00	0,50	(1)	(3)
256 × 256	75	49152	6,00	0,75	(1)	(3)
256 × 256	90	59008	7,20	0,90	(1)	(3)
256 × 256	100	65536	8,00	1,00	(1)	(3)
512 × 512	10	26240	3,20	0,10	(1)	(3)
512 × 512	20	52480	6,41	0,20	(1)	(3)
512 × 512	25	65536	8,00	0,25	(1)	(3)
512 × 512	50	131072	16,00	0,50	(1)	(3)
512 × 512	75	196608	24,00	0,75	(1)	(3)
512 × 512	90	235968	28,80	0,90	(1)	(3)
512 × 512	100	262144	32,00	1,00	(1)	(3)

(1) sonucun “negative” olduğunu, (2) sonucun “skipped (false positive likely)” olduğunu, (3) sonucun “no steg found” olduğunu belirtmektedir.

4.13. Sonuç

Görüntü içerisine yapılan veri gizleme işlemi neticesinde mutlaka görüntüde değişimler meydana gelmektedir. Bu aşamada veri gizleme yöntemi ile amaçlanan, değişimlerden dolayı meydana gelen bozulmaların en alt seviyede olması ve bu bozulmaların gizli veriyi inceleyen kişiler tarafından fark edilememesidir. Önerilen yöntemin tam da bu amaçlara ulaşıp ulaşmadığı göstermek adına literatürde veri gizleme yöntemlerinin analizi için en sık kullanılan teknikler ile testler yapılmıştır.

İlk olarak orijinal görüntü ile stego görüntünün arasındaki görsel fark insan görme sistemi ile test edilmiş ve herhangi bir farkın algılanamadığı görülmüştür. Hatta görüntülerin belli kısımlarının yakınlaştırılması ile yapılan görsel incelemede piksellerdeki bozulmalar fark edilememektedir. Görsel farkı detaylandırmak için görüntülerin histogram grafikleri elde edilmiş ve bu grafikler incelendiğinde çok fazla değişimin veya ani değişimlerin olmadığı gözlenmiştir. Bununla birlikte, bazı gri seviye değerlerinin tepe değerlerinde ufak değişimler olduğu fark edilmektedir. Önerilen yöntemle yapılan veri gizleme işlemi sonucundaki orijinal görüntü histogram grafiği ile stego görüntülerin histogram grafikleri birbirine çok yakın sonuçlar vermektedir.

Literatürde veri gizleme yöntemlerinde en sık kullanılan karşılaştırma ve başarım ölçütleri MSE ve PSNR değerleridir. Önerilen yöntem için 24 bit renkli görüntülerde sadece R kanalına veri gizleme yapıldığında PSNR değerinin 52,59 dB – 63,70 dB aralığında olduğu, 8 bit gri seviyeli görüntülerde ise 52,55 dB – 63,74 dB aralığında olduğu hesaplanmıştır. Eğer iki görüntü arasında hesaplanan PSNR değeri 30 dB − 50 dB arasında ise bu değer literatürdeki görüntü işleme çalışmalarında kabul edilmiş değer olarak ele alınmaktadır (Netravali ve Haskell, 1995; Chang ve ark., 2008; Coşkun ve ark., 2013). Önerilen yöntem ile yapılan veri gizleme işlemi neticesinde elde edilen PSNR değerinin kabul edilen değerlerin oldukça üzerinde olduğu anlaşılmaktadır. Ayrıca son zamanlarda geliştirilen veri gizleme yöntemleri ile yapılan PSNR karşılaştırılmasında da önerilen yöntemin daha yüksek PSNR değerine sahip olduğu görülmektedir.

İstatiksel hesaplamalara dayalı görüntü kalite ölçütleri olan UQI, M−SSIM, CQM, AD, SC, NCC ve NAE kalite ölçütleri kullanılıp orijinal görüntü ile stego görüntü arasındaki yapısal benzerlik test edilmiştir. UQI, M−SSIM, SC ve NCC ölçütleri için en iyi değerin 1 olması, CQM için en iyi değerin 100 olması, AD ve NAE için ise en iyi değerin 0 olması beklenmektedir. Önerilen yöntem ile yapılan veri gizleme işlemi sonucunda hesaplanan değerlerin hepsinde en iyi değer veya en iyi değere yakın sonuçlar çıkmıştır. Bu sonuç önerilen yöntemin örtü görüntüsü üzerinde çok az değişim/bozulma yaptığını ispatlamaktadır.

Görüntüde meydana getirilen en az değişim ile gizli verinin fark edilmesi en aza indirgenmiştir. Bunu test etmek için ise geliştirilen yöntem ile veri gizleme yapılmış görüntülere steganaliz testleri yapılmıştır. Stegdetect ve Stegspy araçları kullanılarak yapılan steganaliz ataklarına karşı önerilen yöntemin başarılı olduğu gözlenmiştir.

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

Bilişim teknolojilerinin hızlı gelişimi ve yaygın kullanımı ile sayısal veri ve doküman elde edilmesi, arşivlenmesi ve paylaşımı her ortamda kolaylıkla yapılabilmektedir. Verilerin gerek arşivlenmesi gerekse paylaşımı sırasında, veriler yetkisi dışında kişilerin erişimine yani yetkisiz veri elde edilmesi tehlikesine maruz kalmaktadır. Böylelikle veri gizliliği ihlal edilmiş olunur. Bu durumda gerek kurumsal verilerin, gerek kişisel verilerin korunması ve güvenliği oldukça önem arz etmektedir. Bu bölümde tez çalışması kapsamında geliştirilen algoritmanın sonuçları ve iyileştirilmesi adına öneriler verilmektedir.

5.1. Sonuçlar

Bu tez çalışmasının bilime katkısı, bir örtü görüntüsü üzerinde en az değişiklik ile görüntü kalitesini en üst seviyede tutan ve böylece gizli verinin fark edilmesini güçleştiren, blok eşleştirme, tarama sırası seçime dayalı ve LSB yöntemini kullanan yeni bir veri gizleme algoritması tasarlanması ve algoritmanın tıbbi görüntüler üzerine bir uygulama arayüzünün geliştirilmesidir. Tez çalışmasının sonuçları;

1. 24 bit renkli ve 8 bit gri seviyeli görüntülerde kullanılabilecek blok eşleştirme ve tarama sırası seçimli yeni bir LSB tabanlı veri gizleme algoritması tasarlanmıştır,
2. Geliştirilen veri gizleme algoritması sayesinde örtü görüntüsünde en az bozulma/değişim sağlanmıştır,
3. Literatürde yapılan veri gizleme yöntemlerine kıyasla örtü görüntüsünde oluşan bozulma seviyesi en aza indirilmiş ve stego görüntüde yüksek kalite elde edilmiştir,
4. Tıbbi alanda kullanmak amacıyla örtü görüntüsüne metin bilgilerine ek, görüntü üzerinde yapılan geometrik şekilsel işaretlemeler ve bu şekillere ait

açıklamaların gizlenebilmesi için bir uygulama yazılımı geliştirilmiştir. Uygulama yazılımı ile gizlenecek verilerini boyutunun arttığı durumlarda ise veri sıkıştırma yöntemi kullanılarak gizlenecek veriler ilk önce sıkıştırılarak veri boyutu azaltılmaktadır. Veri gizleme işleminin güvenliğini arttırmak adına gizlenecek bilgilere şifreleme yapılabilmektedir. Ayrıca yazılım sayesinde veriler tasarlanan algoritma ile veya klasik LSB yöntemi kullanılarak görüntü içerisine gizlenebilinmiştir,

5. Tasarlanan algoritmanın başarımlarına ait aşağıdaki sonuçlara ulaşılmıştır:
    a. Başarımlarının değerlendirilmesi için tıbbi görüntülerin yanında görüntü işleme çalışmalarında standart olarak kullanılan Lena, Tiffany, Baboon, F16, Sailboat on Lake (Lake), Peppers ve House test görüntüleri 24 bit ve 8 bit renk derinliğinde 32×32, 64×64, 128×128, 256×256 ve 512×512 boyutunda kullanılmıştır. İlk olarak görsel analiz edilen görüntülerde orijinal görüntü ile stego görüntü arasında herhangi bir farkın olmadığı gözle görülmektedir. Hatta görüntüler yakınlaştırıldığında bile insan görme sistemi bu iki görüntü arasındaki farkı anlayamamaktadır. Görüntülerin histogram sonuçları incelendiğinde histogram grafiklerinde keskin bir değişimin olmadığı görülmekte ve sadece en üst seviyelerde çok az değişimin olduğu fark edilmiştir.
    b. Gizli veri için en uygun yerin bulunması prensibine dayanan önerilen algoritmanın uygulanması sonucu, klasik LSB yöntemine göre görüntünün piksellerinde ve bitlerinde yapmış olduğu bozulma oranları azdır. Bu durum doğrudan literatürde veri gizleme uygulamalarında en çok kullanılan karşılaştırma ölçütü olan PSNR değerini etkilemektedir. 512×512 boyutundaki 24 bit renkli örtü görüntüsüne 32 KB kapasitesinde veri gizlenmesi sonucunda elde edilen stego görüntünün PSNR değeri 58,32 dB olarak hesaplanmıştır. Aynı boyuttaki 8 bit gri seviyeli görüntüye 32 KB kapasitesinde veri gizlendiğinde ise PSNR değeri 53,55 dB olarak ölçülmüştür. Klasik LSB yöntemine göre yaklaşık 2 dB daha iyi sonuç alındığı hesaplanmaktadır. Literatürdeki çalışmalar ile karşılaştırma

yapıldığında ise önerilen algoritmanın daha iyi PSNR değeri verdiği görülmüştür.

c. İstatiksel hesaplamalara dayalı olan UQI, M–SSIM, CQM, AD, SC, NCC ve NAE kalite ölçütleri kullanılıp orijinal görüntü ile stego görüntü arasındaki yapısal benzerlik test edildiğinde ise tüm metriklerde en iyi değer veya en iyi değere yakın sonuçlar verdiği hesaplanmıştır.
d. Son olarak gizli verinin üçüncü şahıslar tarafından fark edilmesine yönelik yapılan steganaliz ataklarına karşın Stegdetect ve Stegspy araçlarına karşıda başarılı olduğu görülmüştür.

5.2. Tartışma ve Öneriler

Literatür incelendiğinde veri gizleme işleminde kullanılan birçok veri gizleme yöntemi vardır. Bu veri gizleme yöntemlerinden bazıları gizlenecek veri miktarını arttırmayı amaçlarken bazıları da fark edilmemeyi amaçlamaktadır. Bu kıstaslar ve tez çalışmasında tasarlanan algoritmanın sunmuş olduğu katkıları değerlendirildiğinde elbette yapılan çalışmanın geliştirilmesi ve farklı çalışmalardan esinlenerek yeni veri gizleme çalışmaları geliştirilmesi mümkündür. Bundan sonra yapılabilecekler aşağıdaki gibi listelenebilir:

1. Tez çalışmasında veri gizleme işlemi için 24 bit renkli görüntülerde sadece R renk kanalı kullanılmıştır. Diğer renk kanallarının kullanımını da kapsayacak biçimde araştırma genişletilebilir.
2. Yöntemin test işlemlerinde sadece 24 bit renkli ve 8 bit gri seviyeli görüntüler kullanılmıştır. İstenildiği takdirde her türlü sayısal görüntüde bu algoritma uygulanabilir.
3. Önerilen algoritma LSB tabanlı olup pikselin sadece en son bitinde değişim yapmıştır. Gizli veri miktarını arttırmak için en son bitten ayrı en son ikinci veya üçüncü bitte de veri gizleme işlemi yapılabilmesi durumundaki verimlilik araştırılabilir.
4. Renk değişimlerinin keskin olduğu kenarlarda daha fazla bitte değişim yapılarak veri miktarı artışı gerçekleştirilebilir.

5. Literatürde gizlenecek veriye uygun veritabanından örtü görüntüsü eşleştirilerek yapılan veri gizleme yöntemleri mevcuttur. Bu yöntemlerde genelde öznitelikler çıkartılarak yapay zeka algoritmaları veya sınıflandırma algoritmaları kullanılmaktadır. Bu çalışmada bulunan benzer blokların bulunmasında yapay zeka algoritmaları veya sınıflandırma algoritmalarının kullanılabilirliği incelenebilir.
6. İşlemlerin daha hızlı yapılabilmesi için paralel programlama teknikleri kullanılabilir.
7. Tez çalışmasında sadece görüntüler kullanılmıştır. Buna ek olarak hareketli görüntü kaydı olan video kayıtlarında da bu algoritma kullanılıp geliştirilebilir.
8. Tasarlanan algoritmanın kullanılması için bir arayüz geliştirilmiştir. Bu arayüz sadece masaüstü bilgisayarlarda kullanılabilmektedir. Bu arayüzün her ortamdan rahatlıkla kullanılabilmesi için web ortamındaki versiyonu geliştirilebilir.
9. Geliştirilen arayüz daha kapsamlı hale getirilerek bir sayısal medikal yönetim sistemi geliştirilebilir. Ayrıca hastane bilgi sistemleri içerinde yer alan görüntü arşivleme ve iletişim sistemlerine geliştirilen yazılım entegre edilip kullanılabilir.
10. Veri gizleme işlemlerinde geometrik şekilsel işaretlemeler ve metin bilgileri görüntülere gizlenmiştir. Önerilen yöntem sayısal biçime dönüştürülecek her türlü sayısal verinin, örtü nesnesine gizlenebilmesi için geliştirilebilir.

KAYNAKLAR

Ahani, S., Ghaemmaghami, S. 2014. Colour Image Steganography Method Based On Sparse Representation. IET Image Processing, 9(6): 496-505.

Akar, F. 2009. Şablon Eşleme Yöntemi İle Plaka Tanıma Ve Değerlendirme Sistemi. Atatürk Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı, Doktora Tezi.

Akar, F., Yalman, Y., Varol, H. S. 2013. Data Hiding In Digital Images Using A Partial Optimization Technique Based On The Classical LSB Method. Turkish Journal of Electrical Engineering and Computer Science, 21: 2037-2047.

Akgün, F. 2011. Mobil İletişim Teknolojilerinin Yapısı Ve Bu Teknolojilerde Kullanılan Veri Şifreleme Algoritmalarının Güvenirliklerinin Analizi. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Akkoyunlu, B., Yılmaz, M. 2005. Türetimci çoklu ortam öğrenme kuramı. Hacettepe Üniversitesi Eğitim Fakültesi Dergisi, 28:9-18.

Al-Ani, Z. K., Zaidan, A. A., Zaidan, B. B., Alanazi, H. 2010. Overview: Main Fundamentals For Steganography. Journal Of Computing, 2(3):158-165.

Al-Dmour, H., Al-Ani, A. 2015. Quality Optimized Medical Image Steganography Based On Edge Detection And Hamming Code. In 2015 IEEE 12th International Symposium on Biomedical Imaging, 1486-1489.

Al-Dmour, H., Al-Ani, A. 2016. A steganography embedding method based on edge identication and XOR coding. Expert Syst Appl, 46: 293-306.

Al-Dmour, H., Al-Ani, A., Nguyen, H. 2014. An efficient steganography method for hiding patient confidential information. 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 222-225.

Al-Husainy, M. A. 2009. Image Steganography By Mapping Pixels To Letters. Journal Of Computer Science, 5(1): 33-38.

Alzubaydi, D., Alshibani, D. R. 2014. New Image Broadcasting based on Visual Cryptography and Steganography. International Journal of Computer Applications, 108(9).

Amirtharajan, R., Rayappan, J. B. B. 2012. An Intelligent Chaotic Embedding Approach To Enhance Stego-İmage Quality. Information Sciences, 193: 115-124.

Anderson, R. J., Petitcolas, F. A. 1998. On The Limits Of Steganography. IEEE Journal On Selected Areas In Communications, 16(4): 474-481.

Aslan, B. 2013. Blok Şifreler İçin Cebirsel İkili Doğrusal Dönüşüm Tasarımı Ve Modern Bir Blok Şifreye Uygulanması. Trakya Üniversitesi , Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Ataklı, A., Kaplan, A. 2016. Tıbbi Dokümantasyon ve Sekreterlik, Güneş Tıp Kitapevleri, 1-111.

Aydoğan, T., Bayılmış, C., Çetin, Ö., Mete, M. 2011. Patolojik Görüntülere Metin ve Grafik Bilgilerinin Gömülmesi. Tıp Teknolojileri Ulusal Kongresi, TIPTEKNO'11, Antalya, 1-4.

Aydoğan, T., Bayılmış, C. 2016. A new efficient block matching data hiding method based on scanning order selection in medical images. Turkish Journal of Electrical Engineering and Computer Science, 1-13.

Baraklı, B., Vural, C. 2012. A new reversible video watermarking method based on motion compensated interpolation. Signal Processing and Communications Applications Conference (SIU), IEEE, 1-4.

Bajpai, S. Saxena, K. 2012. Techniques of Steganography for Securing Information: A Survey. International Journal on Emerging Technologies 3(1): 48-54.

Bedi, P., Bansal, R., Sehgal, P. 2013. Using PSO In A Spatial Domain Based Image Hiding Scheme With Distortion Tolerance. Computers & Electrical Engineering, 39(2): 640-654.

Borse, G., Anand, V., Patel, K. 2013. Steganography: Exploring an ancient art of Hiding Information from Past to the Future. International Journal of Engineering and Innovative Technology, 3(4): 192-94.

Bourbakis, N., Rwabutaza, A., Yang, M., Skodras, A. N., Ewing, R. 2009. A synthetic stegano-crypto scheme for securing multimedia medical records and their associations. In 2009 16th International Conference on Digital Signal Processing, 1-8.

Chang, C. C., Lin, C. C., Chen, Y. H. 2008. Reversible Data-Embedding Scheme Using Differences Between Original And Predicted Pixel Values. IET Information Security, 2(2): 35-46.

Chang, C. C., Lin, C. C., Tseng, C. S., Tai, W. L. 2007. Reversible Hiding in DCT-Based Compressed Images. Information Sciences, 177(13): 2768-2786.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P. 2010. Digital Image Steganography: Survey And Analysis Of Current Methods. Signal processing, 90(3): 727-752.

Chhajed, G. J., Shinde, S. A. 2010. Efficient embedding in B&W picture images. In Information Management and Engineering (ICIME), 525-528.

Chen, S. K., Wang, R. Z. 2010. High-Payload Image Hiding Scheme Using K-Way Block Matching. In Intelligent Information Hiding and Multimedia Signal Processing, 2010 Sixth International Conference, 70-73.

Coşkun, A., Ülker, Ü. 2013. Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti. International Journal Of Informatics Technologies, 6(2): 31-39.

Coşkun, İ., Akar, F., Çetin, Ö. 2013. A new digital image steganography algorithm based on visible wavelength. Turkish Journal of Electrical Engineering & Computer Sciences, 21(2): 548-564.

Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T. 2007. Digital Watermarking and Steganography, 1-624.

Çetin, Ö. 2008. Hareketli Görüntü Uygulamaları İçin Sırörtme Yaklaşımı İle Veri Gömme Algoritması Tasarımı. Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Çetin, Ö., Akar, F., Özcerit, A. T., Çakıroğlu, M., Bayılmış, C. 2012. A blind steganography method based on histograms on video files. The Imaging Science Journal, 60(2): 75-82.

Debnath, D., Deb, S., Kar, N. 2015. An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher & RGB Image Steganography. In Computational Intelligence and Networks (CINE), 2015 International Conference, 178-183.

Djebbar, F., Ayad, B., Hamam, H., Abed-Meraim, K. 2011. A View On Latest Audio Steganography Techniques. In Innovations in Information Technology (IIT) International Conference, 409-414.

Doğan, Ş. 2011. Yeni Bir Sayısal Damgalama Tekniği İle Biyometrik Uygulamalar. Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Dunbar, B. 2002. A Detailed Look At Steganographic Techniques And Their Use İn An Open-Systems Environment. Sans Institute, 1-9.

El Safy, R. O., Zayed, H. H., El Dessouki, A. 2009. An adaptive steganographic technique based on integer wavelet transform. In Networking and Media Convergence International Conference,111-117.

Eskicioğlu, A. M., Fisher, P. S. 1995. Image quality measures and their performance. IEEE Transactions on communications, 43(12): 2959-2965.

Fazli, S., Kiamini, M. 2008. A high performance steganographic method using JPEG and PSO algorithm. In IEEE International Multitopic Conference. INMIC 2008, 100-105.

Fındık, O. 2010. Yapay Zeka Teknikleri Kullanarak Sabit Görüntüler İçin Sayısal Damgalama. Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Fridrich, J. 2010. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press,1-437.

Ghebleh, M., Kanso, A. 2014. A Robust Chaotic Algorithm For Digital Image Steganography. Communications in Nonlinear Science and Numerical Simulation, 19(6): 1898-1907.

Gonzalez, R. C., Woods, R. E. 2002. Digital image processing, Third Edition, 1-954.

Gutub, A., Fattani, M. 2007. A Novel Arabic Text Steganography Method Using Letter Points And Extensions. World Academy of Science, Engineering and Technology, 27: 28-31.

Hong, W. 2013. Adaptive Image Data Hiding In Edges Using Patched Reference Table And Pair-Wise Embedding Technique. Information Sciences, 221: 473-489.

Iranpour, M., Farokhian, F. 2013. Minimal Distortion Steganography Using Well-Defined Functions. In 2013 High Capacity Optical Networks and Emerging/Enabling Technologies, 21-24.

İkibaş, C. 2012. Retinal İmgelerde Optik Disk Ve Makulanın Tespiti Ve Değerlendirilmesi. Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

İncetaş, O., Sağıroğlu, Ş. 2015. Kuantum Kriptografide Gönderilen Foton Sayısının, Gürültüsüz Ortamda Elde Edilen Anahtar Uzunluklarına Etkisi. SDÜ Mühendislik Bilimleri ve Tasarım Dergisi, 3(1): 29-42.

Jamil, T. 1999. Steganography: The Art Of Hiding Information In Plain Sight. IEEE potentials, 18(1):10-12.

Jayaram, P., Ranganatha, H. R., Anupama, H. S. 2011. Information Hiding Using Audio Steganography–A Survey. The International Journal of Multimedia & Its Applications (IJMA) 3: 86-96.

Ji, R., Yao, H., Liu, S., Wang, L. 2006. Genetic algorithm based optimal block mapping method for LSB substitution. IEEE International Conference on Intelligent Information Hiding and Multimedia, 215-218.

Jindal, B., Singh, A. P. 2014. Image steganography with multilayer security using moderate bit substitution. Journal of Applied Sciences, 14(8): 738-747.

Kafri, N. M., Suleiman, H. Y. 2009. Bit-4 of Frequency Domain-DCT Steganography Technique. IEEE International Conference on Networked Digital Technologies, 286-291.

Kanan, H. R., Nazeri, B. 2014. A Novel Image Steganography Scheme With High Embedding Capacity And Tunable Visual Image Quality Based On A Genetic Algorithm. Expert Systems with Applications, 41(14): 6123-6130.

Kao, D. Y., Wang, S. J., Goyal, D., Liu, J. 2011. A Trustworthy Computing of ADAPT Principle Guaranteeing Genuine Medical Image. In Parallel and Distributed Systems, 17th International Conference, 618-623.

Karakış, R., Güler, İ., Çapraz, İ., Bilir, E. 2015. A novel fuzzy logic-based image steganography method to ensure medical data security. Computers in biology and medicine, 67, 172-183.

Karakuş, D. 2006. Görüntü Analiz Yöntemleri İle Kayaçların Yapısal Özelliklerinin Tanımlanması. Dokuz Eylül Üniversitesi, Fen Bilimleri Enstitüsü, Maden Mühendisliği Bölümü Maden İşletme Anabilim Dalı, Doktora Tezi.

Kazan, S. 2009. Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Ker, A. D., Pevny, T. 2014. The steganographer is the outlier: realistic large-scale steganalysis. IEEE Transactions on Information Forensics and Security, 9(9): 1424-1435.

Khalind, O. S., Hernandez-Castro, J. C., Aziz, B. 2013. A study on the false positive rate of Stegdetect. Digital Investigation, 9(3): 235-245.

Khalind, O., Aziz, B. 2013. Single-Mismatch 2LSB Embedding Steganography. In IEEE International Symposium on Signal Processing and Information Technology, 283-286.

Kipper, G. (2003). Investigator's Guide to Steganography. CRC Press, 1-240.

Kumar, A., Pooja, K. 2010. Steganography- A Data Hiding Technique. International Journal of Computer Applications. 9(7): 19-23.

Kurtulmuş, F. 2012. Olgunlaşmamış Şeftali Meyvesini Doğal Bahçe Koşullarında Alınmış Görüntülerde Görüntü İşleme Teknikleri Ve Yapay Sınıflandırıcılarla Saptayarak Sayan Algoritmaların Geliştirilmesi. Uludağ Üniversitesi, Fen Bilimleri Enstitüsü, Tarım Makinaları Anabilim Dalı, Doktora Tezi.

Kuzay, D. 2014. Radyo Frekans Radyasyon Ve Oldukça Düşük Frekanslı Manyetik Alanların Diyabetik Ve Diyabetik Olmayan Sıçanların Testis Dokusunda Oksidan Stres Üzerine Etkisi. Gazi Üniversitesi, Tıp Fakültesi, Fizyoloji Anabilimdalı, Uzmanlık Tezi.

Lavania, S., Matey, P. S., Thanikaiselvan, V. 2014. Real-Time Implementation Of Steganography In Medical Images Using Integer Wavelet Transform. In Computational Intelligence and Computing Research, IEEE International Conference, 1-5.

Lerch-Hostalot, D., Megías, D. 2013. LSB Matching Steganalysis Based On Patterns Of Pixel Differences And Random Embedding. Computers & Security, 32: 192-206.

Li, X., Zhang, W., Gui, X., Yang, B.2015. Efficient Reversible Data Hiding Based On Multiple Histograms Modication. IEEE T Inf Foren Sec, 10: 2016-2027.

Li, Y., Li, C. T., Wei, C. H. 2007. Protection of mammograms using blind steganography and watermarking. In Third International Symposium on Information Assurance and Security,496-500.

Liu, J., Tang, G., Sun, Y. 2013. A secure steganography for privacy protection in healthcare system. Journal of medical systems, 37(2): 1-10.

Lou, D. C., Hu, C. H. 2012. LSB Steganographic Method Based On Reversible Histogram Transformation Function For Resisting Statistical Steganalysis. Information Sciences, 188: 346-358.

Lou, D. C., Hu, M. C., Liu, J. L. 2009. Multiple layer data hiding scheme for medical images. Computer Standards & Interfaces, 31(2): 329-335.

Luo, W., Huang, F., Huang, J. 2010. Edge Adaptive Image Steganography Based On LSB Matching Revisited. IEEE Transactions on Information Forensics and Security, 5(2): 201-214.

Luo, X., Cheng, Q., Tan, J. 2003. A lossless data embedding scheme for medical images in application of e-diagnosis. Proceedings of the 25th Annual International Conference of the IEEE, 1:852-855.

Mantos, P. L., Maglogiannis, I. 2016. Sensitive Patient Data Hiding using a ROI Reversible Steganography Scheme for DICOM Images. Journal of medical systems, 40(6): 1-17.

Martiri, E., Baxhaku, A., Barolli, E. 2011. Steganographic Algorithm Injection in Image Information Systems used in Healthcare Organizations. In Intelligent Networking and Collaborative Systems, Third International Conference, 408-411.

Mevzuat Bilgi Sistemi, 1998. Hasta Hakları Yönetmeliği. Resmi Gazete, 23420.

Mohanty, S. P. 1999. Digital watermarking: A tutorial review, in http://www. csee. usf. edu/~ smohanty/research/Reports/WMSurvey1999Mohanty. pdf.

Naji, A. W., Gunawan, T. S., Hameed, S. A., Zaidan, B. B., Zaidan, A. A. 2009. Stego-Analysis Chain, Session One Investigations on Steganography Weakness vs Stego-Analysis System for Multimedia File. In Computer Science and Information Technology-Spring Conference, 405-409.

Nayak, D. K., Bhagvati, C. 2013. A Threshold-LSB Based Information Hiding Scheme Using Digital Images. In Computer and Communication Technology (ICCCT), 2013 4th International Conference, 269-272.

Nergui, M., Acharya, U. S., Acharya, R., Yu, W. 2010. Reliable and robust transmission and storage techniques for medical images with patient information. Journal of Medical systems, 34(6): 1129-1139.

Netravali, A. N., Haskell, B. G. 1995. Digital Pictures: Representation. Compensation, and Standards. 2nd Edition, Plenum Press.

Nishad, P.M., Chezian, R.M. 2013. Various Colour Spaces And Colour Space Conversion Algorithms. Journal of Global Research in Computer Science, 4(1): 44-48

Ntalianis, K., Tsapatsoulis, N. 2016. Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks. IEEE Transactions on Emerging Topics in Computing, 4(1): 156-174.

Ou, B., Li, X., Zhao, Y., Ni, R. 2015. Efficient color image reversible data hiding based on channel-dependent payload partition and adaptive embedding. Signal Processing, 108: 642-657.

Özkan, H. 2011. Bilgisayarlı Tomografi Anjiyografi Görüntülerinde Pulmoner Embolilerin Bilgisayar Destekli Tespiti. Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik-Bilgisayar Eğitimi Anabilim Dalı, Doktora Tezi.

Öztürk, S. 2009. Kırılgan Ve Dayanıklı Resim Damgalama Tekniklerinin Başarımının Zeki Optimizasyon Yöntemleriyle Artırılması. Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Pandey, V., Shrivastava, M. 2012. Secure Medical Image Transmission using Combined Approach of Datahiding, Encryption and Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 2(12): 54-57.

Pandey, V., Singh, A., Shrivastava, M. 2012. Medical Image Protection by Using Cryptography Data-Hiding and Steganography. International Journal of Emerging Technology and Advanced Engineering, 2(1): 106-109.

Pavani, M., Naganjaneyulu, S., Nagaraju, C. 2013. A Survey On LSB Based Steganography Methods. International Journal Of Engineering And Computer Science, 2(8): 2464-2467.

Prabakaran, G., Bhavani, R., Rajeswari, P. S. 2013. Multi secure and robustness for medical image based steganography scheme. In Circuits, Power and Computing Technologies International Conference, 1188-1193.

Provos, N., Honeyman, P. 2003. Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3): 32-44.

Qiao, M., Sung, A. H., Liu, Q. 2013. MP3 Audio Steganalysis. Information Sciences, 231: 123-134.

Rabbani, M., Jones, P. W. 1991. Image Compression Theory And Applications. SPIE Press.

Raj, S. A., Soumya, T. 2013. A Youthful Procedure for Spatial Domain Steganography. In Advances in Computing and Communications (ICACC) 2013 Third International IEEE Conference, 300-303.

Ramaiya, M. K., Hemrajani, N., Saxena, A. K. 2013. Security Improvisation In Image Steganography Using DES. In Advance Computing Conference (IACC) IEEE 3rd International, 1094-1099.

Reddy, V. L. 2015. Novel Chaos Based Steganography for Images Using Matrix Encoding and Cat Mapping Techniques. Information Security and Computer Fraud, 3(1): 8-14.

Rosaline, S. I., Raj, M. A. 2013. Adaptive Pixel Pair Matching Based Steganography for Audio Files. In Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System 2013 IEEE International Conference, 1-5.

Sabokdast, M., Mohammadi, M. 2013. A Steganographic Method For Images With Modulus Function And Modified LSB Replacement Based On PVD. In Information and Knowledge Technology (IKT) 5th Conference, 121-126.

Sajasi, S., Moghadam, A. M. E. 2015. An Adaptive İmage Steganographic Scheme Based On Noise Visibility Function And An Optimal Chaotic Based Encryption Method. Appl Soft Comput 2015, 30: 375-389.

Sakallı, M. T. 2006. Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Sakuldee, R., Udomhunsakul, S. 2007. Objective performance of compressed image quality assessments. International Journal of Computer Science, 2(4): 258-267.

Santoso, A. W., Bayuaji, L., Lim, T. S., Habibah, L., Jasni, M. Z. 2016. Comparison of Various Speckle Noise Reduction Filters on Synthetic Aperture Radar Image. International Journal of Applied Engineering Research (IJAER), 11(15): 8760-8767.

Sarreshtedari, S., Akhaee, M. A. 2014. One-Third Probability Embedding: A New ±1 Histogram Compensating Image Least Significant Bit Steganography Scheme. IET Image Processing, 8(2): 78-89.

Sharif, A., Mollaeefar, M., Nazari, M. 2016. A Novel Method For Digital Image Steganography Based On A New Three-Dimensional Chaotic Map. Multimedia Tools and Applications, 1-19.

Shirali-Shahreza, M., Shirali-Shahreza, M. H. 2007. Text Steganography In SMS. In Convergence Information Technology International Conference, 2260-2265.

Shrikalaa, M., Mathivanan, P., Jasmine, J. L. 2013. Conversion of 2D Stegano Images Into A 3D Stereo Iniage Using RANSAC. In Information & Communication Technologies (ICT) 2013 IEEE Conference, 686-690.

Singh, V., Aman, M., Gupta, V., Parashar, M. 2013. Techniques of defeating steganography: a state of art survey. International Journal Of Engineering And Computer Science. 2(5): 1479-1486.

Sivakumar, R., Gayathri, M. K., Nedumaran, D. 2010. Speckle filtering of ultrasound B-Scan Images-a comparative study between spatial and diffusion filters. In Open Systems (ICOS), 2010 IEEE Conference, 80-85.

Srinivasan, Y., Nutter, B., Mitra, S., Phillips, B., Ferris, D. 2004. Secure transmission of medical records using high capacity steganography. In Computer-Based Medical Systems Proceedings 17th IEEE Symposium, 122-127.

Sun, S. 2016. A novel edge based image steganography with 2 k correction and Huffman encoding. Information Processing Letters, 116(2): 93-99.

Sümbüllüoğlu, K., Akdağ, B. 2010. Hasta Dosyaları Bilimsel Yaklaşım, Pamukkale Üniversitesi yayınları, 1-555.

Şahin, A. 2007. Görüntü Steganografide Kullanılan Yeni Metodlar Ve Bu Metodların Güvenilirlikleri. Trakya Üniversitesi , Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Şahin, A., Buluş, E., Sakallı, M.T. 2005. 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. Trakya Univ J Sci, 7(1): 17-22.

Şatır, E. 2013. Bilgi Güvenliği İçin Metin Steganografisinde Yeni Bir Yaklaşım. Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Şatır, E., Işık, H. 2012. A Compression-Based Text Steganography Method. Journal of Systems and Software, 85(10): 2385-2394.

Şatır, E., Işık, H. 2014. A Huffman Compression Based Text Steganography Method. Multimedia Tools And Applications, 70(3): 2085-2110.

Şirvan, O. 2010. Yapay Sinir Ağları Kullanılarak Retina Görüntülerinden Hastalık Tanılama Sistemi Tasarımı Ve Gerçekleştirimi. Ege Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Taghipour, H., Taghipour, J., Esmaili, H. A. 2014. Embedding of Pathology Reports in Pathology Images. Annual Research & Review in Biology, 4(13): 2228-2241.

Tang, M., Hu, J., Fan, M., Song, W. 2013. A Steganalysis By Adjacency Pixel Bits Structure. Computers & Electrical Engineering, 39(2): 488-496.

Tang, M., Hu, J., Fan, M., Song, W. 2013. A Steganalysis By Adjacency Pixel Bits Structure. Computers & Electrical Engineering, 39(2): 488-496.

Taşkın, D. 2007. Sıkıştırılmış Video Akımının Düzensiz Haritalar Ve Başlangıç Kodlarına Dayalı Şifrelenmesi. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Toony, Z., Sajedi, H., Jamzad, M. 2009. A High Capacity Image Hiding Method Based On Fuzzy Image Coding/Decoding. In Computer Conference, 2009 14th International CSI, 518-523.

Tuncer, T., Avci, E. (2016). A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images. Displays, 41: 1-8.

Tüzün, S., Akan, A. 2005. Yüz Uzayının Dikleştirilmesine Dayanan Yeni Bir Yüz Tanıma Yöntemi. Elektrik-Elektronik-Bilgisayar Mühendisliği 11. Ulusal Kongresi, İstanbul, 1-4

Tyagi, A., Roy, R., Changder, S. 2015. High Capacity Image Steganography Based on Pixel Value Differencing and Pixel Value Sum. In Advances in Computing and Communication Engineering (ICACCE) 2015 Second International Conference, 488-493.

Ulutas, M., Ulutas, G., Nabiyev, V. V. 2011. Medical image security and EPR hiding using Shamir's secret sharing scheme. Journal of Systems and Software, 84(3): 341-353.

Umeda, T., Okawa, A., Gomi, T. 2014. Security model for secure transmission of medical image data using steganography,311.

Üstübioğlu, A., Ulutaş, G., Ulutaş, M. 2015. A New Watermark Algorithm Resistance To Geometric Transformations. In 2015 23nd Signal Processing and Communications Applications Conference,1525-1528.

Varnan, C.S., Jagan, A., Kaur, J., Jyoti, D., Rao, D.S. 2011. Image Quality Assessment Techniques in Spatial Domain, IJCST, 2(3): 177-184.

Vashishtha, L. K., Dutta, T., Sur, A. 2013. Least Significant Bit Matching Steganalysis Based On Feature Analysis. In Communications (NCC) 2013 IEEE National Conference, 1-5.

Wang, H., Wang, S. 2004. Cyber Warfare: Steganography vs. Steganalysis. Communications Of The ACM, 47(10): 76-82.

Wang, J., Sun, Y., Xu, H., Chen, K., Kim, H. J., Joo, S. H. 2010. An Improved Section-Wise Exploiting Modification Direction Method. Signal Processing, 90(11): 2954-2964.

Wang, R. Z., Chen, Y. S. 2006. High-Payload Image Steganography Using Two-Way Block Matching. IEEE Signal Processing Letters, 13(3): 161-164.

Wang, R. Z., Lin, C. F., & Lin, J. C. 2001. Image hiding by optimal LSB substitution and genetic algorithm. Pattern recognition, 34(3): 671-683.

Wang, R. Z., Tsai, Y. D. 2007. An image-hiding method with high hiding capacity based on best-block matching and k-means clustering. Pattern Recognition, 40(2): 398-409.

Wang, Z., Bovik, A. C. 2002. A universal image quality index. IEEE Signal Processing Letters, 9(3): 81-84.

Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P. 2004. Image quality assessment: from error visibility to structural similarity. IEEE Transactions On Image Processing, 13(4): 600-612.

Warkentin, M., Bekkering, E., Schmidt, M. B. 2008. Steganography: Forensic, Security, and Legal Issues. The Journal of Digital Forensics, Security and Law: JDFSL, 3(2): 17.

Yalman, Y. 2010. Sayısal Görüntüler İçin Histogram Temelli Veri Gizleme Yöntemi Ve Uygulama Yazılımı. Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim Dalı, Doktora Tezi.

Yalman, Y., Çetin, Ö., Ertürk, İ., Akar, F. 2014. Veri Gizleme. Beta Basım Yayım, İstanbul, 1-267

Yalman, Y., Ertürk, İ. 2011. Kişisel Bilgi Güvenliğinin Sağlanmasında Steganografi Biliminin Kullanımı. ÜNAK 2009, 215-226.

Yalman, Y., Ertürk, İ. 2013. A new color image quality measure based on YUV transformation and PSNR for human vision system. Turkish Journal of Electrical Engineering & Computer Sciences, 21(2): 603-612.

Yaman, K., Sarucan, A., Atak, M., Aktürk, N. 2001. Dinamik Çizelgeleme İçin Görüntü İşleme Ve Arıma Modelleri Yardımıyla Veri Hazırlama. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 16(1):19-40.

Yargıçoğlu, A.U. 2010. Düşük Veri Hızlarında Çalışan Konuşma Kodlayıcılarına Gürbüz Bilgi Saklama Ve Damgalama. Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Yavuzer Aslan, F., Sakallı, M. T., Aslan, B. 2012. Önemli Blok Şifrelerde Kullanılan Doğrusal Dönüşümlerin İncelenmesi. Akademik Bilişim, 46-56.

Yerlikaya, T. 2006. Yeni Şifreleme Algoritmalarının Analizi. Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi.

Yerlikaya, T., Buluş, E., Buluş, N. 2006. Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri. Akademik Bilişim.

Yıldız, Y., Özcerit, A.T. 2015. 24 bit renkli hareketli resimler (video) üzerinde geliştirilen sırörtme yöntemi. SAÜ Fen Bil Der 19(1): 1-6.

Yılmaz, İ. 2002. Renk Sistemleri, Renk Uzayları Ve Dönüşümler. Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30. Yıl Sempozyumu, Konya.

Yılmaz, İ., Güllü, M., Baybura, T., Erdoğan, A. O. 2002. Renk Uzayları ve Renk Dönüşüm Programı (RDP). Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 2(2): 19-35.

Yürüklü, E. 2013. Kaotik Özelliklerin Konuşma Sesleri Steganalizinde Kullanımı. Uludağ Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Mühendisliği Anabilim Dalı, Doktora Tezi.

Zhang, L., Wang, H., Wu, R. 2009. A High-Capacity Steganography Scheme For JPEG2000 Baseline System. IEEE Transactions on Image Processing, 18(8): 1797-1803.

Zhang, Y., Jiang, J., Zha, Y., Zhang, H., Zhao, S. 2013. Research On Embedding Capacity And Efficiency Of Information Hiding Based On Digital Images. International Journal of Intelligence Science, 3(02): 77-85.

Zhou, X. Q., Huang, H. K., Lou, S. L. 2001. Authenticity and integrity of digital mammography images. IEEE transactions on medical imaging, 20(8): 784-791.

Zhu, Z., Zhang, T., Wan, B. 2013. A Special Detector For The Edge Adaptive Image Steganography Based On LSB Matching Revisited. In 2013 10th IEEE International Conference on Control and Automation (ICCA), 1363-1366.

ÖZGEÇMİŞ

Turgay AYDOĞAN 1982 yılında Erzincan'da doğdu. İlköğretimini sırasıyla İstanbul'da 60.Yıl Sarıgazi İlkokulu, Gazimağusa/KKTC'de Canbulat İlkokulu ve Bodrum/Muğla'da Turgutreis İlköğretim Okulunda tamamladı. Ortaöğretim eğitimini 1993−2000 yılları arasında Milas Anadolu Lisesi'nde aldı. 2001 yılında Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilgisayar Sistemleri Öğretmenliği programını kazandı ve 2005 yılında sınıf birincisi olarak mezun oldu. 2005−2008 yılları arasında Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'nda Yüksek Lisans öğrenimini tamamladı. 2009 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'nda Doktora öğrenimine başladı. 2006 yılında Milli Eğitim Bakanlığı'nda Bilişim Teknolojileri Öğretmeni olarak öğretmenlik mesleğine başladı. 2009 yılında Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı'nda uzman olarak, yazılım biriminde göreve başladı. 2010 yılından itibaren bu kurumdaki görevine okutman olarak devam etmektedir. Evli ve iki çocuk babasıdır.