



**T.C.  
GAZİ ÜNİVERSİTESİ  
BİLİŞİM ENSTİTÜSÜ**

**DOKTORA  
TEZİ**

**EPİLEPTİK MRG VE EEG VERİLERİ  
İÇİN BULANIK MANTIK TABANLI  
STEGANOĞRAFI UYGULAMASI**

**RUKİYE KARAKIŞ**

**ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ  
ANABİLİM DALI**

**HAZİRAN 2015**



**EPİLEPTİK MRG VE EEG VERİLERİ İÇİN  
BULANIK MANTIK TABANLI STEGANOĞRAFİ UYGULAMASI**

**Rukiye KARAKIŞ**

**DOKTORA TEZİ  
ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ  
BİLİŞİM ENSTİTÜSÜ**

**HAZİRAN 2015**

Rukiye KARAKIŞ tarafından hazırlanan “EPİLEPTİK MRG VE EEG VERİLERİ İÇİN BULANIK MANTIK TABANLI STEGANOĞRAFI UYGULAMASI” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Gazi Üniversitesi Elektronik ve Bilgisayar Anabilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

**Danışman :** Prof. Dr. İnan GÜLER

Elektronik ve Bilgisayar Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/~~onaylamıyorum~~.....

**Başkan :** Prof. Dr. O. Ayhan ERDEM

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/~~onaylamıyorum~~.....

**Üye :** Doç. Dr. H. Şakir BİLGE

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/~~onaylamıyorum~~.....

**Üye :** Doç. Dr. Cengiz KOÇUM

Biyomedikal Mühendisliği Anabilim Dalı, Başkent Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/~~onaylamıyorum~~.....

**Üye :** Doç. Dr. İsa NAVRUZ

Elektrik ve Elektronik Mühendisliği Anabilim Dalı, Ankara Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum/~~onaylamıyorum~~.....

Tez Savunma Tarihi: 29./06/2015

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....  
Doç. Dr. Nurettin TOPALOĞLU  
Bilişim Enstitüsü Müdürü

## ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

  
Rukiye KARAKIŞ

29.06.2015

EPİLEPTİK MRG VE EEG VERİLERİ İÇİN BULANIK MANTIK TABANLI  
STEGANOĞRAFI UYGULAMASI  
(Doktora Tezi)

Rukiye KARAKIŞ

GAZİ ÜNİVERSİTESİ  
BİLİŞİM ENSTİTÜSÜ  
Haziran 2015

ÖZET

Günümüzde, medikal veriler İnternet ve açık ağlarda tehlike altındadır. Medikal verilerin ele geçirilmesi veya değiştirilmesi, hasta haklarının ihlal edilmesine ve hastaların hayatlarının tehlikeye girmesine sebep olabilir. Bu nedenle, medikal verilerin ve özellikle medikal görüntülerin güvenliği sağlanmalıdır. Medikal verilerin güvenliği için kriptoloji ya da steganografi teknikleri kullanılmaktadır. Bu çalışmada, medikal verilerin tek bir ortamda birleştirilerek güvenliğinin sağlanması için iki yeni steganografi yöntemi önerilmiştir. Bu sebeple, Elektroensafolagram (EEG) gizlenecek mesaj olarak, Manyetik Rezonans (MR) görüntüleri taşıyıcı görüntü olarak kullanılmıştır. EEG'nin yanısıra mesaj, doktor yorumu ve görüntülerin başlık kısmında yer alan hasta kişisel bilgilerinden oluşturulmuştur. En az ağırlıklı bite (Least Significant Bit-LSB) veri gizleme, literatürde en çok kullanılan yöntemdir. Aynı zamanda, bu yöntem basit ve oldukça hızlıdır. Bu çalışmada, benzerlik tabanlı (Similarity-SM) ve bulanık mantık tabanlı (Fuzzy Logic-FL) iki yeni steganografi yöntemi önerilmektedir. Bu yöntemler, piksellerin LSB'lerini sıralı olmadan seçmektedir ve seçilen piksellerin LSB'leri ile mesaj bitlerini yer değiştirmektedir. Mesaj gizlemek için piksellerin gri seviyelerinin benzerlik değerleri kullanılmaktadır. SM-LSB algoritması, mesaj gizlemek için piksellerin LSB'lerini deneme-yanılma ile belirlenen bir eşik değerine göre seçmektedir. FL-LSB algoritması, sıralı olmadan seçilen piksellerin LSB'lerinde bir eşik değeri olmaksızın mesaj gizlemektedir. Mesaj, saldırıları engellemek için kayıpsız sıkıştırma ve simetrik şifreleme algoritmaları kullanılarak korunmaktadır. Taşıyıcı ve gömülü görüntülerin performansı, istatistiksel analiz yöntemleri olan hataların kareleri ortalaması (Mean Square Error-MSE), sinyalin tepe değerinin gürültüye oranı (Peak Signal to Noise Ratio-PSNR), evrensel kalite indeksi (Universal Image Quality Index-UQI), yapısal benzerlik (Structural Similarity-SSIM) ve korelasyon katsayısı (R) ile ölçülmüştür. Elde edilen analiz sonuçlarına göre FL-LSB yöntemi, LSB algoritmasını güçlendirmiş ve medikal verileri tek bir ortamda birleştirilerek güvenliğini sağlamıştır. Aynı zamanda, MR görüntüleri ve EEG sinyallerinin iletim kapasitesi ve kayıt alan miktarları azaltılmıştır ve MR görüntülerinin başlık kısımlarındaki hastaların kişisel bilgilerinin güvenliği de sağlanmıştır.

Bilim Kodu : 704.3.013  
Anahtar Kelimeler : Medikal görüntü steganografi, medikal veri güvenliği, bulanık mantık algoritması, benzerlik tabanlı algoritma  
Sayfa Adedi : 106  
Danışman : Prof. Dr. İnan GÜLER

A FUZZY LOGIC-BASED STEGANOGRAPHY APPLICATION FOR MRI AND EEG  
DATA OF EPILEPSY  
(Ph. D. Thesis)

Rukiye KARAKIŞ

GAZİ UNIVERSITY  
INFORMATICS INSTITUTE

June 2015

ABSTRACT

Today, there are risks for electronic medical data in open networks and Internet. If medical data is captured or altered, it may cause to be violated of patient's rights and to be changed treatment. Hence, the security of all patient records and especially medical images must be ensured. Cryptography and steganography techniques are used to secure medical data. In this study, two new image steganography methods are proposed to secure medical data by combining them into one file format. Hence, the Electroencephalogram (EEG) is selected as hidden data, and Magnetic Resonance (MR) images are used as the cover image. In addition to the EEG, the message is composed of the doctor's comments and patient information in the file header of images. Least significant bit (LSB) embedding is the most widely used method in the literature. It is also simple and operate more rapidly. In this study, two new image steganography methods that are based on fuzzy-logic and similarity are proposed. These methods select the non-sequential least significant bits (LSB) of image pixels and alter these selected LSBs of the pixels with the bits of the message. The similarity values of the gray levels in the pixels are used to hide the message. SM-LSB algorithm selects the LSBs of pixels to embed the message by a threshold value which is determined by trial and error. FL-LSB algorithm hides the message with selecting randomly LSB pixels without a threshold value. The message is secured to prevent attacks by using lossless compression and symmetric encryption algorithms. The performance between stego image and cover image was measured by statistical analysis methods such as mean square of error (MSE), peak signal-to-noise ratio (PSNR), structural similarity measure (SSIM), universal quality index (UQI), and correlation coefficient (R). According to the obtained result, the proposed FL-LSB method ensured both to secure medical data by combining them into one file format and to reinforce LSB embedding technique. It also ensured the confidentiality of the patient information in the file header of images, and reduces data repository and transmission capacity of both MR images and EEG signals.

Science Code : 704.3.013

Key Word : Medical image steganography, medical data security, fuzzy logic algorithm,  
similarity based algorithm

Page Number : 106

Supervisor : Prof. Dr. İnan Güler

## TEŞEKKÜR

Yüksek lisans ve doktora eğitimim süresince, bilgisi ve değerli yorumları ile her zaman yanımda olan, çalışma disiplinini hep örnek alacağım çok değerli hocam ve danışmanım Prof. Dr. İnan GÜLER'e, doktora sürecim boyunca desteğini esirgemeyen Prof. Dr. O. Ayhan ERDEM'e ve Doç. Dr. H. Şakir BİLGE'ye, veri elde etme sürecindeki katkılarından dolayı Prof. Dr. Erhan BİLİR ve Öğr. Gör. Dr. İrem ÇAPRAZ'a teşekkür ederim. Geliştirdiği kaynak kodlarını öğrencileriyle alçakgönüllükle paylaşan, bilginin paylaştıkça çoğaldığı öğrendiğim Prof. Dr. Recep DEMİRCİ'ye teşekkürü borç bilirim.

Ankara'ya geldiğim ilk günden itibaren bana abla ve aile olan, tezimin veri elde etme sürecince de katkısını esirgemeyen, güler yüzünü hiç unutmayacağım sevgili Nihal YENİDÜNYA'ya ve ailesine sonsuz teşekkür ederim. Tezim boyunca maddi ve manevi katkılarını, dostluklarını eksik etmeyen, sevgili yol arkadaşlarım Meral ÖZARSLAN YATAK, Bayram KÜÇÜK, Gürcan ÇETİN, Osman ÖZKARACA, Adem TEKEREK'e ve bilhassa tez sürecim boyunca program kodlamadaki fikir ve yardımlarından ötürü Mutlu YAPICI'ya teşekkürü borç bilirim. Tez sürecim boyunca yardımlarını ve güler yüzlerini esirgemeyen Kurban KOÇAK, Zerrin MİT, Rahime TAPIŞ KARA ve Adeviye AYDIN'a çok teşekkür ederim.

Uzun öğrencilik ve doktora yıllarımızı Ankara'da birlikte geçirdiğimiz, bana çalışmanın, azimli olmanın ne olduğunu öğreten, evimizi baba evi yapan ve bana aile olan sevgili kız kardeşim Serap KARAKIŞ'a en derin teşekkürlerimi sunarım. Bu uzun yolda en büyük dayanağım ve yoluma devam etme sebebim olan, maddi ve manevi tüm destekleri ile hep yanımda olan canım annem Sultan KARAKIŞ'a, sevgili ablam Bilge ŞİMŞEK'e ve biricik kardeşim Necmettin KARAKIŞ'a en içten teşekkürlerimi sunarım. Yanımda olmasalar da, birlikte geçirdiğimiz o çok az zaman diliminde bana doğruları gösteren ve doğru olmayı öğreten, çalışma ahlakını aşılaman, varlıklarını hayatımın sonuna kadar kalbimde hissedeceğim, rahmetli babam Mehmet KARAKIŞ ve dedem Necmettin HÜLAGÜ'ye sonsuz teşekkür ederim.

Tezimi destekleyen Gazi Üniversitesi Bilimsel Araştırma Projeleri Birimine (Proje No: 07/2012-45) katkılarından dolayı ayrıca teşekkür ederim.



## İÇİNDEKİLER

	<b>Sayfa</b>
ÖZET .....	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER .....	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ.....	x
SİMGELER VE KISALTMALAR.....	xiii
<b>1. GİRİŞ.....</b>	<b>1</b>
1.1. Literatür Araştırması .....	3
<b>2. MATERYAL VE METOT .....</b>	<b>15</b>
2.1. Medikal Veri Güvenliği .....	15
2.2. Sayısal Görüntü.....	17
2.3. DICOM (Digital Imaging and Communications in Medicine).....	19
2.4. Steganografi Teknikleri.....	23
2.4.1. Görüntü steganografi teknikleri .....	26
2.5. Bulanık Mantık .....	29
2.6. Sıkıştırma Teknikleri.....	33
2.7. Veri Seti ve Kullanılan Yazılımlar .....	35
<b>3. ÖNERİLEN YÖNTEMLER.....</b>	<b>39</b>
3.1. Medikal Görüntü Steganografi için Önerilen Yöntemler .....	43
3.1.1. Benzerlik-tabanlı LSB (SM-LSB) algoritması.....	43
3.1.2. Bulanık mantık-tabanlı LSB (FL-LSB) yöntemi .....	47
3.2. Karşılaştırma Yöntemleri.....	51
<b>4. BULGULAR VE TARTIŞMA .....</b>	<b>53</b>
4.1. Önerilen Yöntemlerle Elde Edilen Sonuçlar.....	57
4.2. Önerilen Yöntemlerle Elde Edilen Sonuçların Karşılaştırması .....	68
4.3. Önerilen Yöntemin Literatürdeki Çalışmalar ile Karşılaştırılması .....	80
<b>5. SONUÇ VE ÖNERİLER .....</b>	<b>85</b>
KAYNAKLAR .....	89
EKLER.....	101

	<b>Sayfa</b>
EK-1. Etik kurul.....	102
ÖZGEÇMİŞ.....	104

## ÇİZELGELERİN LİSTESİ

<b>Çizelge</b>	<b>Sayfa</b>
Çizelge 2.1. DICOM başlık kısmında yer alan temel veri eleman özellikleri .....	23
Çizelge 2.2. Epilepsi veri setindeki MR ve EEG verilerinin tanımlamaları ve kapasiteleri.....	36
Çizelge 4.1. SM-LSB algoritması ile elde edilen performans sonuçları.....	69
Çizelge 4.2. FL-LSB algoritması ile elde edilen performans sonuçları.....	73
Çizelge 4.3. Önerilen algoritmaların gizlediği mesaj kapasitelerinin karşılaştırılması .....	76
Çizelge 4.4. Önerilen algoritmaların farklı görüntü boyutlarına göre gizlediği mesaj kapasiteleri.....	79
Çizelge 4.5. Tez çalışması ile literatürdeki uzay tabanlı yöntemlerin karşılaştırması.....	80
Çizelge 4.6. Tez çalışması ile literatürdeki dönüşüm tabanlı yöntemlerin karşılaştırması..	82

## ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Medikal bilgilerin gizliliği için kullanılan güvenlik araçları.....	15
Şekil 2.2. Medikal bilgilerin sağlamlığı için kullanılan güvenlik araçları.....	16
Şekil 2.3. Sayısal görüntünün temel yapısı.....	17
Şekil 2.4. PACS sistematik şeması .....	20
Şekil 2.5. DICOM veri elemanının özellikleri.....	22
Şekil 2.6. Görüntü dosyaları için bir steganografik şifreleme sistemi.....	25
Şekil 2.7. Bulanık mantık sisteminin akış diyagramı .....	31
Şekil 2.8. Klasik küme örneği.....	31
Şekil 2.9. Bulanık küme örneği ve üçgen üyelik fonksiyonu .....	32
Şekil 3.1. Önerilen yöntemler için mesaj gizleme aşaması. ....	39
Şekil 3.2. DICOM görüntü için oluşturulan mesaj .....	40
Şekil 3.3. Mesaj gizleme aşamasının akış diyagramı .....	41
Şekil 3.4. Önerilen yöntemler için gizlenen mesajı elde etme blokları. ....	42
Şekil 3.5. Mesajı elde etme aşamasının akış şeması.....	42
Şekil 3.6. Benzerlik-Tabanlı LSB (SM-LSB) yönteminin akış şeması .....	44
Şekil 3.7. Görüntünün 3x3 komşu pikselleri .....	45
Şekil 3.8. 3x3 pencerede komşu piksellerin benzerlik matrisi.....	46
Şekil 3.9. Bulanık Mantık-Tabanlı LSB (FL-LSB) yönteminin akış diyagramı .....	48
Şekil 3.10. Komşu piksellerin renk bileşenlerinin bulanıklaştırılması için tanımlanan bulanık üçgen kümeler (ÇAB: Çok Az Benzer, AB: Az Benzer, OB: Orta Benzer, ÇB: Çok Benzer ve YB: Yüksek Benzer).....	49
Şekil 4.1. DICOM serisinden kişisel bilgilerin seçilmesini sağlayan pencere .....	53
Şekil 4.2. Hastaya ait DICOM serisinin yüklenilmesini sağlayan pencere .....	54
Şekil 4.3. Hastanın EEG verisinin yüklenilmesini sağlayan pencere. ....	55
Şekil 4.4. Oluşturulan mesajın DICOM serisine gizlenmesini sağlayan pencere.....	55

<b>Şekil</b>	<b>Sayfa</b>
Şekil 4.5. Gizlenen mesajın elde edilmesi ve görüntülenmesini sağlayan pencere .....	56
Şekil 4.6. Taşıyıcı ve gömülü görüntülerin karşılaştırılmasını sağlayan pencere.....	57
Şekil 4.8. 256x256 boyutlu taşıyıcı ve gömülü görüntülerin histogramı a) taşıyıcı görüntü histogramı b) SM-LSB ile oluşturulan gömülü görüntü histogramı c) FL-LSB ile oluşturulan gömülü görüntü histogramı.....	59
Şekil 4.9. 512x512 boyutlu taşıyıcı ve gömülü görüntülerin histogramı a) taşıyıcı görüntü histogramı b) SM-LSB ile oluşturulan gömülü görüntü histogramı c) FL-LSB ile oluşturulan gömülü görüntü histogramı.....	61
Şekil 4.10. 256x256 boyutlu gömülü görüntülerdeki değişen pikseller a) SM-LSB ile değişen pikseller b) FL-LSB ile değişen pikseller .....	63
Şekil 4.11. 512x512 boyutlu gömülü görüntülerdeki değişen pikseller a) SM-LSB ile değişen pikseller b) FL-LSB ile değişen pikseller .....	64
Şekil 4.12. Görüntü boyutlarına göre bölütlenen EEG verisi. ....	65
Şekil 4.13. a) EEG verisi, b) SM-LSB ile gizlenen EEG, c) FL-LSB ile gizlenen EEG.....	66
Şekil 4.14. MR görüntü kesiti a) Taşıyıcı MR, b) Taşıyıcı MR kesiti, c) SM-LSB ile elde edilen gömülü MR kesiti d) FL-LSB ile elde edilen gömülü MR kesiti ...	67
Şekil 4.15. MR görüntü kesiti a) Taşıyıcı MR, b) Taşıyıcı MR kesiti, c) SM-LSB ile elde edilen gömülü MR kesiti d) FL-LSB ile elde edilen gömülü MR kesiti ...	68
Şekil 4.16. SM-LSB ile elde edilen gömülü görüntülerin PSNR değerleri .....	70
Şekil 4.17. SM-LSB ile elde edilen gömülü görüntülerin MSE değerleri .....	70
Şekil 4.18. SM-LSB ile elde edilen gömülü görüntülerin SSIM, UQI ve R değerleri .....	71
Şekil 4.19. SM-LSB ile elde edilen gömülü görüntülerin değişen ortalama piksel oranı (PR) değerleri.....	71
Şekil 4.20. SM-LSB ile elde edilen gömülü görüntülerin PSNR-HVS ve PSNR-HVSM değerleri .....	72
Şekil 4.21. FL-LSB ile elde edilen gömülü görüntülerin PSNR değerleri .....	73
Şekil 4.22. FL-LSB ile elde edilen gömülü görüntülerin MSE değerleri .....	74
Şekil 4.23. FL-LSB ile elde edilen gömülü görüntülerin SSIM, UQI ve R değerleri .....	74
Şekil 4.24. FL-LSB ile elde edilen gömülü görüntülerin PSNR-HVS ve PSNR-HVSM değerleri .....	75
Şekil 4.25. FL-LSB ile elde edilen gömülü görüntülerin PR değerleri .....	75

<b>Şekil</b>	<b>Sayfa</b>
Şekil 4.26. Önerilen algoritmaların gizlediği mesaj kapasitelerinin karşılaştırılması .....	77
Şekil 4.27. SM-LSB algoritması ile elde edilen veri gizleme kapasitelerinin yüzdesi .....	78
Şekil 4.28. FL-LSB algoritması ile elde edilen veri gizleme kapasitelerinin yüzdesi .....	78

## SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

<b>Simgeler</b>	<b>Açıklamalar</b>
$\Delta K$	Piksellerin kırmızı renk bileşenleri için gri seviye değer farkı
$\Delta M$	Piksellerin mavi renk bileşenleri için gri seviye değer farkı
$\Delta Y$	Piksellerin yeşil renk bileşenleri için gri seviye değer farkı
$\mu$	Bulanık mantıkta üyelik işlevi
$c$	Taşıyıcı görüntünün boş olmayan alt kümeleri
$C$	Piksel benzerlik değeri
$d$	Öklid uzaklığı
$dB$	Desibel
$D_n$	Normalizasyon katsayısı
$M$	Sütun sayısı
$N$	Satır sayısı
$p$	Eşlik biti
$P$	Görüntü pikseli
$S$	Lokal piksel benzerlik değeri
$T_h$	Eşik değeri
$z$	Üyelik fonksiyonunun merkezi

<b>Kısaltmalar</b>	<b>Açıklamalar</b>
<b>BMP</b>	Bitmap
<b>BT</b>	Bilgisayarlı Tomografi
<b>DCT</b>	Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform)

<b>Kısaltmalar</b>	<b>Açıklamalar</b>
<b>DFT</b>	Ayrık Fourier Dönüşümü (Discrete Fourier Transform)
<b>DICOM</b>	Tıpta Sayısal Görüntüleme ve Haberleşme (Digital Imaging and Communications in Medicine)
<b>DWT</b>	Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform)
<b>EEG</b>	Elektroensafolagram
<b>EKG</b>	Elektrokardiyogram
<b>ESK</b>	Elektronik Sağlık Kaydı
<b>FL-LSB</b>	Bulanık MantıkTabanlı-LSB
<b>GIF</b>	Grafik Değişirme Biçimi (Graphics Interchange Format)
<b>HIPAA</b>	Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Talimatı (Health Insurance Portability and Accountability Act)
<b>HVS</b>	İnsan Görme Sistemi (Human Visual System )
<b>JPEG</b>	Birleşik Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group)
<b>LSB</b>	En Az Ağırlıklı Bit (Least Significant Bit)
<b>MR</b>	Manyetik Rezonans
<b>MSE</b>	Hataların Kareleri Ortalaması (Mean Square Error)
<b>MSSIM</b>	Ortalama Yapısal Benzerlik (Mean Structural Similarity)
<b>NEMA</b>	Ulusal Elektrik Üreticileri Derneği (National Electrical Manufacturers Association)
<b>PACS</b>	Görüntü Arşivleme ve Haberleşme Sistemi (Picture Archiving and Communication System)
<b>PNG</b>	Taşınabilir Ağ Grafiği (Portable Network Graphics)
<b>PR</b>	Piksel Oranı (Pixel Ratio)
<b>PSNR</b>	Sinyalin Tepe Değerinin Gürültüye Oranı (Peak Signal to Noise Ratio)
<b>PSNR-HVS</b>	İnsan Görme Sistemine göre Sinyalin Tepe Değerinin Gürültüye Oranı (Peak Signal to Noise Ratio-Human Visual System)



**Kısaltmalar****Açıklamalar****PSNR-HVSM**

İnsan Görme Sistemine göre Düzenlenmiş Sinyalin Tepe Değerinin Gürültüye Oranı (Modified Peak Signal to Noise Ratio-Human Visual System)

**R**

Korelasyon Katsayısı (Correlation Coefficient )

**RGB**

R: Kırmızı (Red), G: Yeşil (Green), B: Mavi (Blue)

**RGBA**

R: Kırmızı (Red), G: Yeşil (Green), B: Mavi (Blue), A: Alfa (Alpha)

**ROI**

İlgi Bölgesi (Region of Interest)

**RONI**

İlgi Olmayan Bölge (Region of Non Interest )

**SM-LSB**

Benzerlik Tabanlı- LSB

**SSIM**

Yapısal Benzerlik (Structural Similarity)

**UQI**Evrensel Kalite İndeksi  
(Universal Image Quality Index)**VF**

Değer Alanı (Value Field)

**VL**

Değer Uzunluğu (Value Length)

**VPN**

Sanal Özel Ağlar (Virtual Private Networks)

**VR**

Değer Temsili (Value Representation)

**YCbCr**Y: Parlaklık (Luminance), Cb: Mavi Renk Parlaklığı  
(Chrominance Blue), Cr: Kırmızı Renk Parlaklığı  
(Chrominance Red)

## 1. GİRİŞ

Günümüzde, medikal verilerin kayıt edilmesi, ulaşılması ve dağıtılması ile ilgili tanımlamalar bilgi ve haberleşme teknolojilerindeki gelişmeler ile değişmektedir. Medikal veriler, açık ağlarda ve İnternet'te risk altındadırlar. Son yıllarda, en sık rastlanılan siber saldırılar medikal verilerin ele geçirilmesi üzerinedir. Medikal verilerin ele geçirilmesi ya da değiştirilmesi hasta haklarının ihlal edilmesine ve aynı zamanda hastaların hayatlarının tehlikeye girmesine sebep olabilir [1-3].

Elektronik sağlık kaydı (ESK), doğum öncesinden ölüm sonrasına kadar geçen sürede, kişilerin sağlık bilgilerinin sistematik olarak bir araya getirilmesi ile oluşmaktadır [4]. ESK, hastanın kimlik bilgilerini, hastalık özgeçmişini, tanı, teşhis ve tedavi süreçlerini, reçetelerini, histolojik ve patolojik bulgularını, laboratuvar sonuçlarını, radyolojik görüntülerini ve bunların raporlarını içermektedir [2]. Bu kayıtlar, sağlık kurumlarında, sigorta firmalarında ya da klinik araştırmalarda ve epidemiyolojik çalışmalarda toplanabilmektedir. ESK sistemleri şu özelliklere sahip olmalıdır: hastalar tek bir kayıt numarasına sahiptir, tüm hasta bilgilerine kurumun her yerinden ulaşılabilir, hastaların tüm sağlık süreçleri kayıt edilmelidir, sistemden istekler iletilmeli ve sonuçlar görülmelidir, verilere hızlı ve kolayca erişilmelidir. Ayrıca ESK sistemleri, hasta randevularını ve yönetim işlemlerini gerçekleştirmelidir [5].

Yakın zamana kadar hastane bilgi sistemlerinin içerisinde sadece metinsel veriler saklanmaktaydı. Ancak hastaya ait tüm verilerin sayısal ortama aktarılma zorunluğu, medikal görüntülerin de sayısallaştırılarak arşivlenmesini gerektirmiştir [6]. Medikal görüntülerin kapasitesi ortalama 10MB~100MB arasında değişmektedir [7-9]. Bu sebeple, ESK sisteminde yapılan işlemlerin % 90'ını medikal görüntülerin arşivlenmesi aşamaları oluşturmaktadır [10]. Her yıl medikal görüntülerin kayıt edilmesi için gerekli alan miktarı % 10 ile % 20 arasında büyümektedir [7]. Yüksek kayıt kapasitesi gerektiren medikal görüntülerin arşivlenmesi için, görüntü arşivleme ve haberleşme sistemi (Picture Archiving and Communication System- PACS) geliştirilmiştir. Hastanelerdeki Sayısal Bilgi Yönetimi (Hospital Information System-HIS)'nin en önemli parçalarından birini Radyoloji Bilgi Sistemi (Radiology Information System-RIS) ve PACS oluşturmaktadır.

Medikal görüntülerin (X-ray, Bilgisayarlı Tomografi-BT, Manyetik Rezonans-MR, Ultrason vb.) oluşturulması, kayıt edilmesi, yazdırılması, iletilmesi ve geri çağırılması için Tıpta Sayısal Görüntüleme ve Haberleşme (Digital Imaging and Communications in Medicine-DICOM) standardı geliştirilmiştir [11-15]. Ulusal Elektrik Üreticileri Derneği (National Electrical Manufacturers Association-NEMA) tarafından desteklenen DICOM standardı tıbbi görüntüleme ve sağlık bakımı alanında çalışan bilgi teknolojisi üreticileri ve kullanıcılarının bir araya gelmesi ile NEMA standardı (PS3) ve ISO standardı (12052:2006) kullanılarak geliştirilmektedir. DICOM, PACS içinde farklı cihazların, yazılımların ve platformların birbirleriyle entegre çalışması için gerekli olan tanımlamaları içermektedir.

DICOM görüntü dosyası, başlık kısmında hastanın kişisel bilgilerini (ad, soyad, yaş, ağırlık, medikal özgeçmiş gibi), kurum, cihaz ve görüntüye ait (görüntünün boyutu, veri tipi, sunumu gibi) bilgileri tutmaktadır [7, 16]. Görüntü verisi ise dosya başlık kısmından sonra gelmektedir. MRICron, MRICro, MicroDicom, 3DSlicer, dicom2, ezDICOM, ImageMagick, AMIDE, Medcon/XMedcon, ImageJ, dicom2pgm, Offis dcmtk gibi çeşitli yazılımlar, DICOM dosyalarının hem görüntü verilerini, hem de dosyaların başlık kısmında yer alan bilgileri görüntülemektedir ve bu yazılımlar İnternet aracılığıyla kolaylıkla elde edilebilmektedir [16, 17]. Bu sebeplerle, hastanın kişisel haklarının korunması için DICOM dosyasının başlık kısmında yer alan kişisel bilgilerinin ele geçirilmeye ve yasadışı yollarla kopyalanmaya karşı mutlaka korunması gerekmektedir.

Medikal bilgi güvenliği hasta haklarını ve sağlık alanındaki kurum ve kuruluşların ve kişilerin sorumluluklarını ortaya koymaya çalışmaktadır. Medikal bilgi güvenliği medikal standartları ve talimatları oluşturulan katı etik kurallar ve yasalarca korunmaktadır. En temel standart olan ISO27799; medikal bilginin korunmasını sağlayan talimatları ISO17799/ISO27002 standartlarındaki tanımlamalara göre ortaya koymaktadır. Bazı ülkeler ise kendi sağlık bilgi yönetim politikalarını oluşturmuşlardır. Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Talimatı (Health Insurance Portability and Accountability Act- HIPAA), Federal Yönetmelikler Sayı 45 (Code of Federal Regulations number 45-CFR 45), Avrupa Yönergesi 95/46/EC (Europe's Directive 95/46/EC) bu politikalarından bazılarıdır. HIPAA hasta haklarını korumak için gerekli sağlık planlamasını ve medikal görüntülerin güvenliğinin sağlanması için gereken adımları içermektedir. CFR 45 medikal verilerin korunması ile ilgili standartları içermektedir [18].

HIPAA'ya göre medikal kayıtların güvenliği için gizlilik (confidentiality), güvenilirlik (reliability) ve kullanılabilirlik (availability) adımları sağlanmalıdır [1]. Gizlilik; “ önceden planlanmış koşullar altında sadece yetkili kullanıcıların bilgiye erişebileceğini” ifade etmektedir. Güvenilirlik (reliability); sağlamlık (integrity) ve kimlik denetleme (authentication) alt alanlarına sahiptir. Sağlamlık; bilgi, yetkisi olmayan kişilerce değiştirilemez. Kimlik Denetleme; bilgilerin doğru kaynaktan alınmasını ve doğru hastaya ait olmasını kanıtlar. Kullanılabilirlik; yetkili kullanıcıların bilgiye ulaşma ve bilgiyi kullanmaları için gereken tanımlamaları ve durumları belirler [1, 18].

Sağlık bilgi sistemlerinde medikal veri güvenliği; güvenlik duvarı, sanal özel ağlar (Virtual Private Networks- VPN) ve kriptografik yöntemler (simetrik, asimetrik ya da özet şifreleme) ile gerçekleştirilmektedir. Ancak, kullanılan güvenlik araçları sınırlıdır ve güvenlik duvarları korsanlarca kolaylıkla durdurulabilmektedir. Aynı zamanda, kullanılan şifreleme teknikleri tek başına yetersiz kalmaktadır. Çünkü şifreli metinler, taşınma ve iletilme esnasında oluşabilecek bit hatalarına karşı hassastır, işlem maliyetini ve yükünü de artırmaktadır. Ayrıca medikal verilerin dosya başlıkları düz metin formatında kolaylıkla ele geçirilebilmektedir [1, 4, 16, 18, 19].

Bu tez çalışmasında, medikal veri güvenliği için yeni steganografik yöntemlerin geliştirilmesi hedeflenmiştir. Çalışmada; farklı medikal sinyalleri tek bir ortamda birleştirmek, medikal veri güvenliği için yeni yaklaşımlar ortaya koymak, olası saldırılara karşı hasta kişisel bilgilerinin sıkıştırma ve şifreleme yöntemleri ile korunmasını sağlamak, verilerin kayıt alan miktarlarının ve medikal sinyallerin iletilmesi için gereken bant genişliği kapasitesinin azaltılması amaçlanmıştır.

### **1.1. Literatür Araştırması**

Son yıllarda medikal veri güvenliği için kriptolojiye alternatif olarak steganografik yaklaşımlarda kullanılmaktadır. Bu sebeple geliştirilen dönüşüm tabanlı yaklaşımlar saldırılara karşı daha dayanıklı olmalarına karşılık veri gizleme miktarları az, işlem maliyetleri yüksektir. Görüntü uzayında geliştirilen yöntemler ise daha fazla veri gizlemektedir, ancak bu yöntemler saldırılara karşı dayanıklı değildir.

Steganografi gizli olmayan sayısal medya ortamlarında (metin, ses, video gibi) üçüncü şahısların haberi olmayacak şekilde, verilerin gizlenmesini sağlamaktadır [19-43]. Steganografinin temel özellikleri: algılanamamazlık, dayanıklılık ve kapasitedir [20, 21, 44]. İnsan görme ya da işitme sistemi; dosyalarda yapılan küçük değişimleri fark edememektedir. Steganografi ile insandaki bu eksiklikten yararlanılarak dosyaların başlıkları, boşluk kısımları, sıkıştırma sonrasında açılan boşluk kısımları ya da dosyanın ham verisi içerisine, istenilen verilerin gizlenmesi sağlanmaktadır [20, 45].

Literatürde medikal veri güvenliği için steganografi tabanlı pek çok yaklaşım önerilmiştir [1, 18, 46-79]. Bu yöntemler; mesaj gizlemek için kullanılan düzleme göre dönüşüm tabanlı ve uzay tabanlı teknikler olarak ikiye ayrılmaktadır [80-84]. Uzay tabanlı yöntemler, en az ağırlıklı bite (Least Significant Bit-LSB) gizleme, yayılım, nicemleme, histogram gibi tekniklerden yararlanmaktadır. Bu yöntemlerin uygulanması kolaydır ve işlem maliyetleri oldukça azdır. Ancak uzay tabanlı yöntemler, sıkıştırmaya, geometrik bozulmalara ve filtrelemeye karşı dayanıksızdır. Dönüşüm tabanlı teknikleri; ayrık kosinüs dönüşümü (Discrete Cosine Transform- DCT), ayrık Fourier dönüşümü (Discrete Fourier Transform- DFT) ve ayrık dalgacık dönüşümü (Discrete Wavelet Transform- DWT) gibi yöntemleri dönüşüm uzayında kullanmaktadır. Bu yöntemler sıkıştırmaya, geometrik bozulmalara (döndürme, ölçekleme, öteleme, kırpma) ve filtrelemeye karşı dayanıklıdır. Ancak bu yöntemler, yüksek hesaplama maliyetine ve karmaşıklığına sahiptirler. Uzay tabanlı tekniklerin, özellikle LSB yönteminin, veri gizleme kapasitesi oldukça yüksektir [63-69]. Uzay tabanlı ve dönüşüm tabanlı tekniklerin her ikisinde de insan görme ya da işitme sisteminin eksikliği istismar edilmektedir [1, 19-43]. Bu sebeple, bu tez çalışmasında LSB yönteminin veri gizleme kapasitesinden yararlanan ve onun geliştirilmesini sağlayan iki yeni yöntem önerilmektedir.

Literatürde, farklı yapılardaki medikal görüntülerin (MR, BT, PET, X-ray vb.) ya da biyolojik sinyallerin içinde kişisel bilgilerin saklanması için pek çok yöntem önerilmiştir [1, 18, 46-93].

Medikal görüntülerin güvenliğini sağlamak için dönüşüm tabanlı steganografi yöntemlerinden de yararlanılmıştır [49-54].

Joshi ve arkadaşı yaptıkları çalışmada 512x512 boyutlu iki adet BT ve MR görüntüsü içerisine, hastane logosundan ve hastanın kişisel bilgilerini gösteren görüntüden oluşturulan mesajı, DWT kullanarak dönüşüm uzayında gizlemiştir. Mesaj gizlenmeden önce Arnold dönüştürme tekniği ile şifrelenmiştir. Çalışmada sinyallerin tepe değerinin gürültüye oranı (Peak Signal to Noise Ratio- PSNR) değerleri sırasıyla 53,37 dB ve 56,76 dB olarak elde edilmiştir. Ancak çalışmada gizlenen veri miktarı ile ilgili bilgi verilmemiştir [49].

Mavudila ve arkadaşları iki farklı medikal görüntü içerisine, şifrelenen logoları gizlemek için çok bantlı çift ağaç dalgacık dönüşümü yöntemini uygulamıştır. Çalışmada bant genişliği artırıldıkça daha yüksek kapasitede veri gizlenmiştir. PSNR değerleri sırasıyla 40,2 dB ve 42,0 dB olarak elde edilmiştir. Ancak çalışmada, gerçekleştirilen işlemlerin maliyeti ile ilgili bilgi verilmemiştir [50].

Giakoumaki ve arkadaşları farklı yapılarıdaki 30 medikal görüntünün ağ üzerinden aktarılırken güvenliğini sağlamak için DCT katsayılarına veri gizlemiştir. 4 000 bayt veri için PSNR değerleri en az  $52,78 \pm 0,08$  dB ve en fazla  $62,32 \pm 0,04$  dB olarak elde edilmiştir [51].

Li ve arkadaşları yaptıkları çalışmada mamografi görüntüleri içerisinde hasta bilgilerini şifreleyerek damgalama teknikleri ile saklamışlardır [52]. Jiao ve arkadaşı X-ray görüntülerinde DCT yöntemini kullanarak, hasta kişisel verilerini görüntü içerisine gizlemiştir [53]. Fakhari ve arkadaşları dönüşüm uzayında genetik ve karınca koloni algoritmaları ile damgalama tekniğini birleştirmişlerdir [54].

Medikal veri güvenliği için literatürde görüntünün ilgi bölgeleri (Region of Interest-ROI) ya da ilgili olmayan bölgeleri de (Region of Non Interest-RONI) kullanılmıştır. ROI bölgeleri tanı koyarken etkin olarak kullanıldığından, buralarda veri gizleme konusunda dikkatli olunması gerekmektedir. Ravali ve arkadaşları medikal görüntülerin bölütleme sonrası belirlenen RONI'lerinin DCT katsayılarına veri gizlenebileceğini göstermiştir. PSNR değerleri altı farklı görüntü için 38,3485 dB ile 60,8781 dB aralığında elde edilmiştir. Ancak, RONI bölgeleri az olduğunda, EEG ya da EKG (Elektrokardiyogram) gibi verilerinin gizlenmesi zordur. Aynı zamanda yüksek çözünürlüklü görüntülerde bu işlemler maliyeti de artırmaktadır [56].

Rahimi ve arkadaşı medikal görüntülerin ROI'lerinin tekil değer ayrışımını kullanarak hesapladıkları katsayılarında, hasta kişisel bilgilerini (230 karakter-660 bayt) saklamışlardır. PSNR ve yapısal benzerlik (Structural Similarity-SSIM) değerleri sırasıyla 60 dB ve 0,997'den fazla olarak elde edilmiştir. Ancak çalışmada az miktarda veri gizlenmiştir [57].

Memon ve arkadaşı önerdikleri yöntemde Otsu eşik değeri ile bölütledikleri görüntünün RONI'lerinde hasta bilgilerini, hastane logosunu ve mesaj doğrulama kodunu saklamışlardır. Yaklaşık 8 000 bayt veri için PSNR değerini 51 dB olarak elde etmişlerdir [58].

Zain ve arkadaşları ROI ve RONI'lerde 480 000 bit veriyi LSB ile gizlemişlerdir. PSNR değerleri yaklaşık olarak 54,15 dB olarak elde edilmiştir. Çalışmada ROI ve RONI'lerde ayrı ayrı ya da bir arada veri gizledikten sonra da radyologların tanı sonuçlarının değişmediği ortaya konulmuştur [59].

Shukla ve arkadaşları geliştirdikleri yöntemde görüntülerin ROI'lerini seçerek RONI'lerde dalgacık dönüşüm kullanarak mesaj gizlemişlerdir. Ancak çalışmanın performans analizleri verilmemiştir [60].

Nyeem ve arkadaşları medikal görüntülerin RONI'lerinde LSB ile veri gizlemişlerdir. RONI bölgeleri seçiminde, medikal görüntü değerlendirirken etkilerinin olmamasına, gizlenecek kapasite miktarını karşılamalarına, bozulmalara karşı dirençli olmalarına ve bilgisayar hesaplama maliyetinin düşürmelerine dikkat edilmiştir. 370 medikal görüntünün ortalama SSIM (Mean Structural Similarity- MSSIM) değerleri 0,999'dan büyüktür. Yaklaşık 100,40 kilo bit veri için MSSIM değeri 0,9974 olarak elde edilmiştir [61].

Fatemizadeh ve arkadaşı medikal görüntülere, üçüncü seviye dalgacık dönüşüm uygulayarak ROI'lerin ve arka planın bölütlenmesini sağlamıştır. ROI'lerde gizleme ile ilgili bilgileri gizlemişlerdir. RONI'lerin 3 seviye dalgacık katsayılarında ise veri gizlemişlerdir [62].

Görüntü uzayı tabanlı steganografi yöntemleri, DICOM görüntü dosyalarında daha fazla miktarda verinin gizlenmesini sağlamaktadır [63-69, 86-88]. Zaim ve arkadaşı iki ultrason görüntüsü içerisine LSB yöntemi ile logo yerleştirmişlerdir. Ancak çalışmada kullanılan yöntem, kapasite ve analizler açıklanmamıştır [63].

Kuang ve arkadaşları medikal görüntü içerisinde sayısal imzaların (Digital Signature Arithmetic- DSA) LSB tekniği ile gizlenmesini sağlamışlardır. Ancak çalışmada kapasite ve performans analizleri verilmemiştir [10].

Raul ve arkadaşları 3 farklı 512x512 boyutlu medikal görüntüde, merkezden başlayıp, spiral çizerek LSB seçimini gerçekleştirmişlerdir. Bunun için 3x3'lük pencerede piksellerin varyanslarını hesaplamışlardır. Varyans değeri belli bir eşik değerinin üzerinde ise bu piksellerin LSB'lerinde veri gizlenmiştir. Ancak çalışmada gizlenen veri miktarı ile ilgili bilgi yoktur. 3 görüntü için PSNR değerleri sırasıyla 41,1 dB, 43,6 dB ve 38,9 dB'dir [64].

Pandey ve arkadaşları şifreledikleri veriyi görüntü içerisine LSB tekniği ile gizlemişlerdir. Ancak çalışmada görüntü kapasiteleri ve performans analizleri verilmemiştir [65].

Mortazavian ve arkadaşları LSB yöntemini geliştirerek en az ağırlıklı bitlerin görüntü piksellerinin ortalama değerlerine göre sıralı olmayacak şekilde seçmişlerdir. Ancak yöntemde görüntü piksel değerleri 0 ile 255 arasına normalize edilmiştir. PSNR değeri ise maksimum 51 dB olarak elde edilmiştir [66].

Viswanathan ve arkadaşı geliştirdikleri bit tabanlı yaklaşımla 128 bit veriyi görüntü içerisinde gizlemişlerdir. Yöntemde 255 üzeri piksellerde gizleme yapılmamıştır ve çalışmanın performans analiz sonuçları verilmemiştir [67].

Navas ve arkadaşlarının geliştirdikleri yöntemde; 128x128 medikal görüntü pikselleri 3x3 bloklara ayrılmış ve bu bloklardaki varyans değerleri hesaplanmıştır. Bu varyans değerlerine göre elde edilen doğru gürültü görünebilirlik piksellerinin LSB'lerinde veri gizlenmiştir. Çalışmada, pikselin 7 farklı LSB'sine veri gizlediklerinde özellikle 4., 5., ve 6. seviye LSB'lerin gömülü görüntülerinde ciddi bozulmalar ortaya çıkmıştır. 1. seviye LSB'lerde gizleme yapıldığında PSNR değeri 49,4 iken 6. seviyede 19,8 dB'dir [68].

Koley ve arkadaşlarının geliştirdikleri yöntemde, medikal görüntülerin RGB değerleri, YCbCr (Y: Luminance-Parlaklık, Cb: Chrominance Blue- Mavi Renk Parlaklığı, Cr: Chrominance Red-Kırmızı Renk Parlaklığı) uzayına dönüştürülmüştür. Hasta ve doktor isimlerinden oluşan mesaj bu uzayda gizlenmiştir. Gizlenen mesajın az olmasına rağmen, gri seviye görüntüler için PSNR değerleri 53,883 dB ile 57,654 dB aralığındadır [69].



Umeda ve arkadaşları  $512 \times 512 \times 100$  adet 16 bitlik BT görüntüsünü 7-Zip sıkıştırma yazılımı ile sıkıştırarak kayıt etmişlerdir ve bu klasörde yer alan bir örtü görüntü içerisinde bu BT görüntüsünü gizlemişlerdir. SSIM ve PSNR değerleri sırasıyla 0,99 ve 65,3 dB olarak elde edilmiştir. Buna göre, birden fazla taşıyıcı görüntü kullanmak kapasiteyi artıracaktır [70].

Doğan ve arkadaşları hasta bilgilerinin önce sıkıştırılmasını ve görüntü piksellerinin LSB'leri ile bu sıkıştırılan verilerin bitlerinin yer değiştirilmesini sağlamışlardır [87].

Literatürde önerilen geri alınabilir (reversible) veri gizleme teknikleri, görüntü kimlik denetleme ve telif hakkı koruma uygulamaları için iyi bir çözümdür. Bu yöntemlerde amaç, gizli veri elde edildikten sonra, orijinal taşıyıcı görüntünün hiçbir bozulma olmadan geri oluşturulmasıdır [71].

Ni ve arkadaşları görüntü histogramı öteleme tabanlı geri alınabilir veri gizleme tekniği önermiştir. Yöntemde maksimum noktadaki piksel değeri 1 ile diğerleri 0 ile yer değiştirilir. Önerilen yöntem oldukça basittir ve görüntüde çok az bozulmaya sebep olmaktadır. Ancak yöntemin veri gizleme kapasitesi düşüktür [72].

Tseng ve arkadaşlarının geliştirdikleri yöntemde ise zirve noktalar değişmeden kalırken, veriler zirve noktalarının etrafındaki komşu piksellerin içerisinde saklanmaktadır [73].

Lin ve arkadaşları ise çoklu seviyeli geri alınabilir veri gizleme tekniğini önermişlerdir. Bu yöntemde, görüntü histogramında piksellerin değer farklarına göre belirlenen zirve tepe noktalarına mesaj gizlenmiştir [74].

Huang ve arkadaşları önerdikleri geri alınabilir veri gizleme tekniği ile yüksek veri saklama kapasitesini medikal görüntüde fark edilebilir bozulma olmadan sağlamışlardır. İki farklı medikal görüntüde sırasıyla 10 672 ve 18 910 bayt veri için PSNR değerleri 49,49 ve 50,39 dB olarak elde edilmiştir [71]. Aynı görüntülerde Ni ve arkadaşları 4 792 bit veri için PSNR değerini 49,71 dB ve 16 591 bit veri için PSNR değerini 49,23 dB olarak elde etmişlerdir [72]. Lin ve arkadaşları seviye 1 de 65 349 bit veri için PSNR değerini 48,67 dB olarak elde ederken, Huang ve arkadaşları 81 274 bit veri için PSNR değerini 48,87 dB olarak bulmuşlardır [74].

Huang ve arkadaşları medikal görüntüler için histogram öteleme tabanlı bir steganografi tekniğini önermişlerdir. Çalışmada, görüntüler önce bloklara bölünmüştür ve sonrasında blokların histogram farkları hesaplanmıştır. Bu değerler önceden belirlenen eşik değerinden büyükse, bu piksellerde veri gizleme gerçekleştirilmiştir. Yöntem ile orijinal görüntü geri getirilse de eşik değeri her görüntü için optimize edilmelidir. Çalışmada blok sayısı azaldıkça kapasite artmıştır. Ayrıca piksellerin iki seviye LSB'si veri gizlemek için kullanıldığında PSNR değerleri azalmıştır [75, 76].

Lou ve arkadaşları görüntü bit uzayında medikal görüntülerde çok katmanlı veri gizleme tekniği ile daha fazla veri gizlenmesini sağlamışlardır. Yöntemde, yatay ve dikeydeki piksel çiftlerinin ortalaması ve farkı hesaplandıktan sonra, gizleme yapılan piksel bitinin logaritmik değerinin, piksellerin ortalama ve farkına dâhil edilerek elde edilen yeni değerlerinde mesaj gizlenmektedir. Çalışmada PSNR değerleri yaklaşık olarak 14 954 bayt veri için 48,86 dB ve 16 862 bayt veri için 42,91 dB olarak elde edilmiştir [77].

Fallahpour ve arkadaşları yaptıkları çalışmada, histogram öteleme tabanlı geri dönüştürme yapabilen yeni bir yöntem önermiştir. Görüntülerin RONI'lerinin yüksek frekans değerlerine veri gizlemişlerdir. Veri gizleme kapasitesini % 30 ile % 200 arasında arttırmışlardır. PSNR değerleri 265 bayt ve 9 416 bayt veri için sırasıyla 37 dB ile 57 dB aralığında elde edilmiştir [78].

Tan ve arkadaşları geliştirdikleri çift katmanlı geri alınabilir teknik ile görüntülerin 2x2 blok pencerelerinde belirledikleri piksellerin LSB'lerine veri gizlemişlerdir. 512x512 çözünürlüklü 8 bit görüntüde, 15 885 bayt veri gizledikten sonra PSNR değerini 34,7 dB olarak elde etmişlerdir [79].

Son yıllarda, literatürde medikal EKG sinyallerinin içerisinde hasta bilgilerinin gizlenmesiyle ilgilenen çalışmaların sayısı da artmıştır [93-105].

Ibadia ve arkadaşları büyüyen nüfus ile birlikte kardiyak hastalıklarının artması sebebiyle, mobil EKG verilerinin güvenliğini sağlamak için dalgacık tabanlı steganografi tekniğini geliştirmişlerdir. Yöntem ile hastaların kişisel bilgileri sinyal içinde geliştirilen karıştırma algoritması ile şifrelenerek gizlenmiştir. Tekrar oluşturulan sinyallerde % 1'den daha az bozulma görülmüştür [94].

Mekala ve arkadaşları yaptıkları çalışmada dalgacık tabanlı steganografi teknikleri ile hasta verilerinin şifrelenerek taşınmasını sağlamışlardır. Ancak çalışmada, örtü ve gömülü sinyaller arasındaki istatistiksel karşılaştırma sonuçları verilmemiştir [95].

Mai ve arkadaşları yaptıkları çalışmada, EKG verileri içerisinde hastaların genel bilgilerinin ve medikal bilgilerinin (alerji, diğer tedavi, aile hikâyesi, kalp ile ilgili geçmişi ve test sonuçları gibi) 32 bitlik anahtar aracılığıyla şifreleyerek gizlenmesini sağlamışlardır [96].

Ibadi ve arkadaşları EKG verileri içerisinde hasta bilgilerini nicemeleme indeks modülasyonu (QIM) yöntemi ile gizlemiştir. Veride önce ön işlem, ardından LSB ile damgalama gerçekleştirilmiştir. EKG içerisine maksimum 10 000 bit (1 250 bayt) veri kaydedilmiştir. Ibadi ve arkadaşları [98] EKG içerisine, minimum bozulma olacak şekilde hasta isim, yaş, kimlik numarası gibi verileri steganografi teknikleri ile gizlemiştir. Normal ve anormal EKG için, kalan fark yüzdesi (PRD) sırasıyla % 0,0247 ve % 0,0678 olmuştur [97].

Suganya ve arkadaşları EKG verilerinin içine hasta bilgilerinin kaotik şifreleme yöntemleri (XOR algoritması ile) kullanılarak şifreli olarak gizlenmesini sağlayan steganografi tekniği önermişlerdir. DWT ile alt bantlara ayrılan yüksek frekanslı sinyalin katsayıları ile mesaj bitleri LSB yöntemi ile yer değiştirilmiştir. Şifre çözülerek veri kolaylıkla elde edilebilmiştir [99].

Keerthana ve arkadaşları da benzer yöntemleri kullanmışlardır. Ancak çalışmada, istatistiksel kıyaslama sonuçlarını vermemişlerdir [93].

Zheng ve Xu yaptıkları çalışmada, EKG sinyallerinin QRS bileşenlerini bozmayacak şekilde, Haar dalgacık dönüşümü ile sinyalin yüksek frekanslı alt bileşenlerinin katsayıları içinden seçim yapmışlardır. QRS sinyallerinin belirlenmesi için öncelikle B-spline dalga dönüşümü uygulanmıştır ve R dalgaları belirlenmiştir. Ardından QRS bileşenleri için eşik değerleri ayarlanmıştır. Tekrar orijinal veri okunarak Haar dalgacık dönüşümü ile yüksek frekans alt bileşenleri oluşturulmuştur ve buralarda gizleme işlemi gerçekleştirilmiştir. Normalize RMSE hatası 5 farklı sinyal için 0,09 ile 0,12 arasında elde edilmiştir. Ancak, veriler üzerinde herhangi bir şifreleme işlemi yapılmamıştır [100].

Sankari ve arkadaşları EKG verileri için de hasta verilerinin steganografi teknikleri ile gizlendiği bir çalışma önermişlerdir. Çalışmada, DWT yöntemi ve asimetrik şifreleme kullanılmıştır. Ancak çalışmanın istatistiksel karşılaştırma sonuçları verilmemiştir [101].

Nambakhsh ve arkadaşları yaptıkları çalışmada, DICOM formatlı MR ve BT görüntüleri içerisinde tek kanallı EKG verilerinin taşınmasını sağlamışlardır. Hastalara ait olan verilerin daha güvenli ve daha az kayıt maliyetine sahip olarak iletilmesini amaçlamışlardır. 2B dalgacık dönüşümü ile dalgacık katsayıları belirlenmiş ve belli bir eşik değerinin üzerinde olan katsayıların bitleri ile mesaj bitleri yer değiştirilmiştir. PSNR değerleri, 512 ve 8192 bayt veriler için 35 dB'den fazla olarak elde edilmiştir ve geliştirilen yöntem ile resmin detayları korunmuştur [102].

Matam yaptığı çalışmasında tek kanallı EEG sinyali içerisinde hasta bilgilerini dalgacık dönüşümü ile gizlemiştir. Doğru katsayıları bulmak için sinyalin bağımsız bileşenlerini elde etmiştir. Ancak EEG verisinin tek kanallı olması sistemin kullanılabilirliğini etkilemektedir [103].

Kong ve arkadaşı EEG sinyallerini AR (Auto-Regressive) yöntemiyle önce sıkıştırmış ve sıkıştırılan sinyallerin LSB'lerine veri gizlemiştir [104].

Ibaida ve arkadaşları tele-tıp uygulamalarında EKG verilerinin boyutlarının çok yüksek olması sebebiyle sıkıştırılarak gönderilmesi gerektiğini ifade etmiştir. Bu sebeple, EKG sinyallerinin sıkıştırılması için; sinyallerin temel bileşenler analizi ile özniteliklerin çıkarılmasını ve k-ortalama yöntemi ile de normal ve anormal olarak ayrıştırılmasını sağlamışlardır [105].

Literatürdeki bazı çalışmaların amaçları ise bu çalışmanınkine benzerlik göstermektedir [82-84, 106-109]. Bu çalışmalarda medikal görüntü içerisinde mesaj gizlenmektedir. Gizlenecek olan mesaj, hastanın kişisel bilgilerinden (hastanın adı ve soyadı, yaşı, doğum tarihi, ağırlığı, cinsiyeti, adresi vb.) ve biyolojik sinyallerinden oluşmaktadır. Ancak çalışmalarda, sınırlı sayıda görüntü ve sınırlı miktarda biyolojik sinyal kullanılmıştır. Bu sebeple gizlenen mesaj kapasitesi düşüktür.

Miaou ve arkadaşları yaptıkları çalışmada medikal görüntü içerisinde EKG sinyalini, doktor yorumunu ve doktor mührünü gizlemeye çalışmıştır. Veri gizlemek için standart LSB tekniğini kullanmışlardır. PSNR değerleri 33 dB ile 43 dB aralığındadır. Çalışmada gizlenen veri kapasitesi hakkında bilgi verilmemiştir [106].

Giakoumaki ve arkadaşları geliştirdikleri dalgacık tabanlı algoritmayı 512x512x20 adet görüntü ile test etmişlerdir. Ortalama PSNR değerleri, yaklaşık 668 bayt (5 348 bit) veri için  $46,66 \pm 0,2$  dB'dir [107].

Nambakhsh ve arkadaşları önerdikleri dalgacık tabanlı algoritma ile EKG verilerini 256x256 çözünürlüklü 25 adet PET görüntüsü içerisinde gizlemişlerdir. PSNR değerleri 2 kilo bayt (KB) mesaj için  $48,15 \pm 0,22$  dB şeklindedir [82, 83].

Anand ve Niranjana görüntü bit uzayında LSB tekniği ile medikal görüntüler içerisinde mesaj gizlemiştir. EKG ya da EEG gibi sinyalleri içerecek text dosyalarını aralıklı olarak seçilen görüntü LSB'lerine saklamışlardır. Ancak bu çalışmanın da, gizlenen mesaj kapasite miktarı çok düşüktür [108].

Acharya ve arkadaşları LSB yöntemi ile hasta bilgilerini ve hastanın EKG ya da EEG biyolojik sinyallerini medikal görüntü içerisinde gizlemişlerdir. Mesaj, Rijndael simetrik algoritması ile şifrelenmiştir [84].

Acharya ve arkadaşları farklı bir çalışmalarında frekans düzleminde DCT katsayılarına LSB yöntemi ile veri gizlemişlerdir. Katsayıları RLE (Run Length) kullanarak şifrelemişlerdir. Huffman sıkıştırma kullanarak da verilerin kayıt alanını azaltmaya çalışmışlardır. Ancak, frekans düzleminde gerçekleştirilen işlemlerin maliyeti görüntü bit uzayına göre daha fazladır. Aynı zamanda saklanan mesaj kapasitesi de daha düşüktür. Ayrıca çalışmada, taşıyıcı ve gömülü görüntülerin histogramlarındaki değişim göze çarpmaktadır [109].

Bu çalışmada görüntü uzayında veri gizlemede en çok kullanılan yöntem olan LSB yönteminin daha da geliştirilmesi amaçlanmaktadır. LSB yönteminin uygulanması kolay, mesaj gizleme kapasitesi yüksek ve maliyeti düşüktür. Tez çalışmasında LSB tekniğini mevcut haline nazaran daha da geliştiren iki yeni yöntem önerilmektedir. Bunlar; benzerlik-tabanlı LSB (SM-LSB) ve bulanık mantık-tabanlı LSB (FL-LSB) olarak isimlendirilmiştir.

Bu tez çalışması beş bölümden oluşmaktadır. Çalışmanın 2. bölümünde; medikal veri güvenliği, PACS sistemleri, DICOM dosya uzantısı ve görüntü steganografi ile ilgili genel bilgiler aktarılmaktadır. Çalışmada önerilen bulanık mantık algoritmasının detaylarının anlaşılması için yöntem ile ilgili bilgiler de 2. bölümde sunulmaktadır. Gizlenecek verinin güvenliğinin sağlanmasında kullanılacak kayıpsız sıkıştırma algoritmaları ile ilgili genel bilgilerde burada aktarılmıştır. Ayrıca çalışma için oluşturulan medikal veri seti ve kullanılan yazılımlar ile ilgili açıklamalar da 2. bölümde yer almaktadır. 3. bölümde geliştirilen FL-LSB ve SM-LSB yöntemleri, örtü ve gömülü görüntüler arasındaki karşılaştırmalar için kullanılan MSE, PSNR, R, SSIM, UQI yöntemlerinin açıklamaları verilmiştir. 4. bölümde geliştirilen yöntemlerin test veri setiyle test edilmesi sonrasında elde edilen kapasite ve karşılaştırma bulguları sunulmuştur. Ayrıca tartışma 4. bölümde verilmiştir. Son bölümde ise sonuç ve öneriler yer almaktadır.



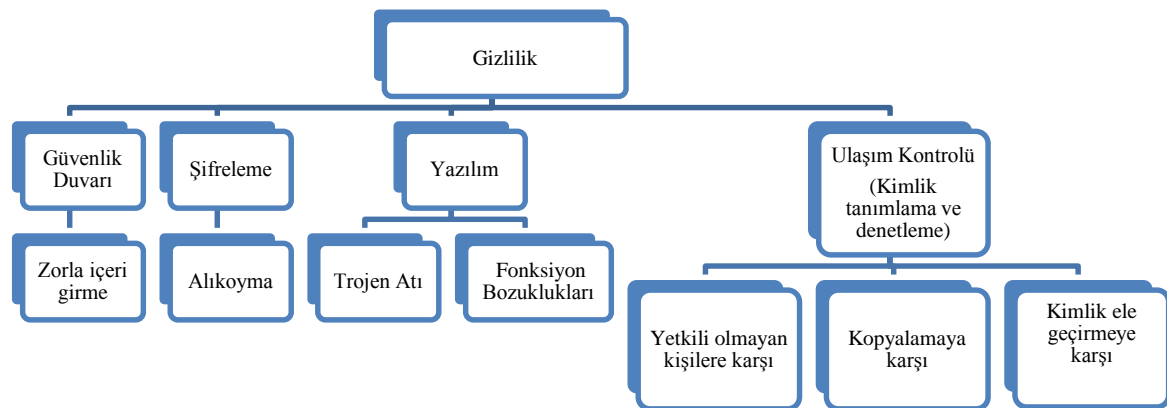
## 2. MATERYAL VE METOT

Bu bölümde medikal veri güvenliği, görüntü steganografi teknikleri, bulanık mantık ve çalışmada kullanılan veri seti ve yazılımlar ile ilgili bilgiler verilecektir.

### 2.1. Medikal Veri Güvenliği

Günümüzde, bilgisayar sistemlerinin gelişmesi sağlık sektörünü de etkilemiştir. Sayısal olan ya da olmayan tüm elektronik kayıtlar gizli tutulmalıdır. HIPAA'ya göre medikal bilgi güvenliğinde, gizlilik, güvenilirlik ve kullanılabilirlik aşamaları zorunlu olarak sağlanmalıdır. Bununla ilgili ayrıntılar ve tanımlamalar giriş bölümünde verilmiştir.

Güvenlik araçları, bir ağa bağlı olan ya da olmayan bilgisayar sistemleri içerisinde bilginin gizliliği ve sağlamlığını gerçekleştirmek için hastane bilgi sistemi içerisinde kullanılmaktadır. Gizlilik, bilgi açığa çıkarılarak ve yönü değiştirilerek tehdit edilebilir. Şekil 2.1'de görüldüğü gibi bu tehditler veri transfer edilirken (Örneğin; kötü niyetli kişilerce alıkoyma ya da dosyaların/kayıtların yasal olmayan yollarla kopyalanması şeklinde olabilir) ya da veri tabanında (İçeri sızma, kimlik gasp etme ya da Trojen atı virüsü kullanımı) gerçekleşebilir [1]. Gizlilik tehditlerini engellemek için ulaşım kontrolü ve güvenli iletim protokolleri oluşturulmalıdır. Ayrıca, güvenli iletim protokolleri bağımsız masaüstü ya da taşınabilir cihazlar içinde kullanılabilir. Açık ağ ortamında ise güvenlik duvarı ile gizlilik tehditleri kontrol edilebilir ve veriler transfer edilirken şifrelenebilir.



Şekil 2.1. Medikal bilgilerin gizliliği için kullanılan güvenlik araçları



Güvenlik araçları aynı zamanda medikal bilgilerin sağlamlığı içinde kullanılmaktadır. Şekil 2.2’de görüldüğü gibi, sağlamlık tehditleri veri ve kayıtların tahrip edilmesi ve değiştirilmesi şeklinde olmaktadır [1]. Bu sebeple, kullanılan ana makinelerde veriyi silme, kayıt etme, değiştirme yetkilerine kimlerin sahip olacağı mutlaka tanımlanmalıdır. Virüslere karşı anti virüsler ve akredite olan güvenlik yazılımları kullanılmalıdır. Aynı zamanda, güvenlik duvarları saldırılara karşı da sistemi koruyabilmelidir. Ayrıca, veri transfer edilirken verilerin sağlamlığı sayısal imzalarla garanti edilebilir.



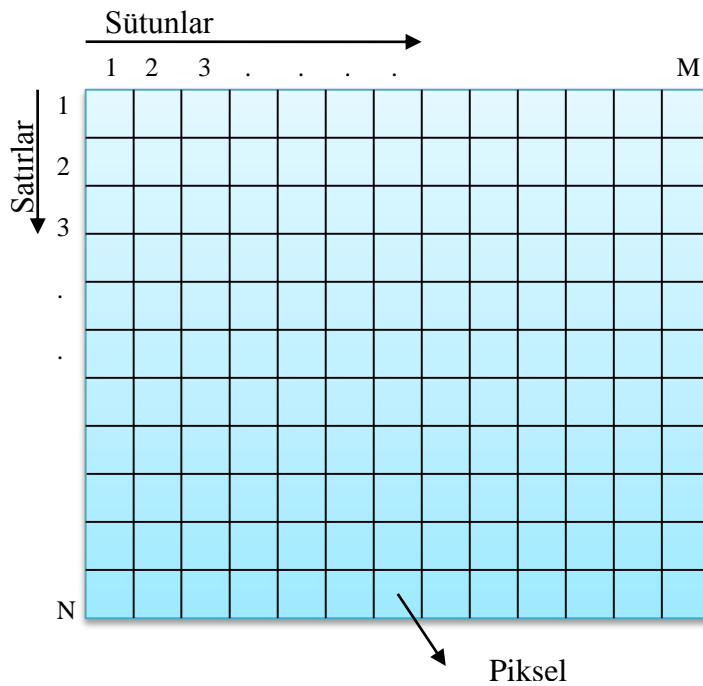
Şekil 2.2. Medikal bilgilerin sağlamlığı için kullanılan güvenlik araçları

Kullanılabilirlik tehditleri; dosya yönetim sistemlerinin engellenmesi, sabit disklerin yok edilmesi ya da verinin tahrip edilmesi gibi kötü niyetli saldırılarla gerçekleştirilebilir. Oluşturulan güvenlik sistemlerinde, veriyi elde tutma kuralları da (ulaşım, denetleme vs.) mutlaka oluşturulmalıdır.

Sağlık bilgi sistemlerinde medikal veri güvenliğini sağlamak için güvenlik duvarı, sanal özel ağlar ve kriptografik yöntemler kullanılır. Ancak, kullanılan güvenlik araçlarının sınırları mevcuttur ve güvenlik duvarları korsanlarca aşılabilmektedir. Aynı zamanda, şifrelenen medikal veriler, taşınma ve iletilme esnasında oluşabilecek bit hatalarına karşı hassas olup, işlem maliyeti ve yükünü artırmaktadır [4, 16, 19]. Ayrıca, medikal verilerin dosya başlıkları düz metin formatında kolaylıkla ele geçirilebilmektedir [1, 18]. HBS içinde medikal verilerin ele geçirilmesi tehdidi dışındaki diğer bir sorun da elle yanlış kayıtların girilmesidir.

## 2.2. Sayısal Görüntü

Sayısal görüntü N satır ve M sütunluk bir dizi ile temsil edilir. Bir görüntü dizisinin elemanlarına piksel denir. Bu pikseller 1 ya da 0 değerlerini içeriyorsa, oluşan resimlere ikili (binary) görüntü denir. 1 ve 0 değerleri sırasıyla aydınlık ve karanlık bölgeleri veya nesne ve zemini temsil ederler. Renkli sayısal görüntü dosyalarında pikseller genellikle 24 ya da 8 bit; gri-seviye görüntülerde pikseller 1-2-4-6 ya da 8 bit olabilirler. 24 bit renk içeren bir resim  $2^{24}$  renkten birine sahiptir. Bunlar 8 bit (256 değer) tarafından verilen üç temel rengin (K-Kırmızı, Y-Yeşil, M-Mavi) farklı miktarlarını içermektedir. 8 bit renk içeren bir resimde her piksel  $2^8$  (256) renkten birine sahiptir ve renkler bir tablo ya da bir paletten seçilmektedir. 8 bit gri seviyeli bir resim  $2^8$  (256) gri noktanın birleşiminden oluşmaktadır. Şekil 2.3'de sayısal bir görüntünün temel yapısı gösterilmektedir [19, 34, 41, 110].



Şekil 2.3. Sayısal görüntünün temel yapısı

Sayısal bir görüntüdeki yatay ve dikey piksel sayısı görüntünün çözünürlüğünü vermektedir. Örneğin 256x512 çözünürlüğe sahip görüntü yatayda 256 piksele ve dikeyde 512 piksele sahiptir. Sayısal bir görüntünün kapladığı alan ise görüntünün boyutları (yükseklik, genişlik) ve renk derinliği ile hesaplanır (Dosya Boyutu (bayt)= (Yükseklik × Genişlik × Renk Derinliği) / 8) [26].

Sayısal görüntü dosyalarının kapladıkları dosya boyutlarını azaltmak için kayıplı ve kayıpsız olarak iki tür sıkıştırma mevcuttur. Kayıpsız sıkıştırma, orijinal görüntüdeki bilgilerin korunması gerektiğinde kullanılır. Grafik değiştirme biçimi (Graphics Interchange Format-GIF), taşınabilir ağ grafiği (Portable Network Graphics –PNG) ve 8 bit Bitmap (BMP) formatları kayıpsız sıkıştırma ile elde edilir. GIF 8 bit renk derinliğine sahiptir ve 256 rengi destekler. Düşük renk derinliği sebebiyle genellikle grafik gösterimlerinde kullanılır, sayısal fotoğrafçılık uygulamalarında tercih edilmez. PNG ise gri ya da kırmızı, yeşil ve mavi renkli kanalların yanı sıra bir saydamlık kanalını da destekler [26, 29].

Kayıplı sıkıştırma ile dosyaların büyüklüğü büyük ölçüde azaltılır, ancak bu yöntem ile görüntü bütünlüğü korunamaz. Birleşik fotoğraf uzmanları grubu (Joint Photographic Experts Group- JPEG) resimlerinde kayıplı sıkıştırma gerçekleştirilir. Kullanılan kayıplı sıkıştırma algoritmasına bağlı olarak JPEG formatı, yüksek kaliteli dijital resimlere yakın sonuç vermektedir. İnsan retinası, bir görüntüdeki renk verisinin parlaklığının daha az çözünürlükte örneklenmesini hissedemez. Bu sebeple, JPEG görüntü dosyası oluşturulurken ilk işlem, piksellerin renk değer vektörlerinin farklı bir uzaya taşınmasıdır. Sayısal görüntüde renk değeri; RGB (R:Red-Kırmızı, G:Green-Yeşil, B:Blue-Mavi) renk uzayında kırmızı, yeşil ve mavi renklerinin ağırlıklandırılmış değerlerinden oluşmaktadır. YCbCr olarak ifade edilen diğer bir uzayda Y parlaklığı, Cb (Chrominance Blue- Mavi Renk Parlaklığı) ve Cr (Chrominance Red-Kırmızı Renk Parlaklığı) renklilik bilgilerini temsil eder. JPEG görüntü formatı oluşturulurken öncelikle renk vektörü RGB, YCbCr uzayına dönüştürülmektedir (Eş. 2.1). İkinci aşamada ise bloklara ayrılan renk bileşenlerine DCT uygulanır, görüntünün enerjisi daha az sayıda pikselde yoğunlaştırılır ve tekrar nicemleme gerçekleştirilir. Nicemleme sonrasında görüntü blokları daha az sayı ile ifade edilir [37].

$$\begin{aligned}
 Y &= 0,299R + 0,587G + 0,114B \\
 Cb &= 0,5 + (B - Y) / 2 \\
 Cr &= 0,5 + (R - Y) / 1,6
 \end{aligned}
 \tag{2.1}$$

Eş. 2.1’de verilen C; görüntünün her pikselinin (x,y) renk vektörü için atanan ayrık fonksiyonu olan  $c(x,y)$ ’dir.

### Bitmap (BMP) görüntü özellikleri

BMP, kayıplı ya da kayıpsız sıkıştırma yapılmaksızın görüntü özelliklerini tutan dosya biçimidir. Bu sebeple sıkıştırma uygulanan PNG, JPEG gibi dosya türlerine göre hafıza alanlarında daha fazla yer kaplar. Sayısal görüntü dosyalarının özelliklerinin anlaşılması için bu kısımda BMP dosya yapısının özellikleri verilmiştir.

Bitmap resim dosyası: resim dosya başlığı (bitmap file header), resim bilgi başlığı (bitmap info header), renk haritası (color map), resim bilgisi bölümlerinden oluşmaktadır. Resmin sahip olduğu toplam veri alanı, örneğin, 100x100 piksel ve 256 renk bilgisine sahip bir resim için resmin satır genişliği ile hesaplanır. 256 renk bilgisi renk haritası (colormap) alanında saklanır. Resim dosya başlığı 14 bayt boyutunda olup, içerisinde dosya tipi, dosya boyutu, reserve edilmiş boş alanlar ve başlığın dosyanın neresinde bittiğini işaret eden bir değer bulunmaktadır [20, 111].

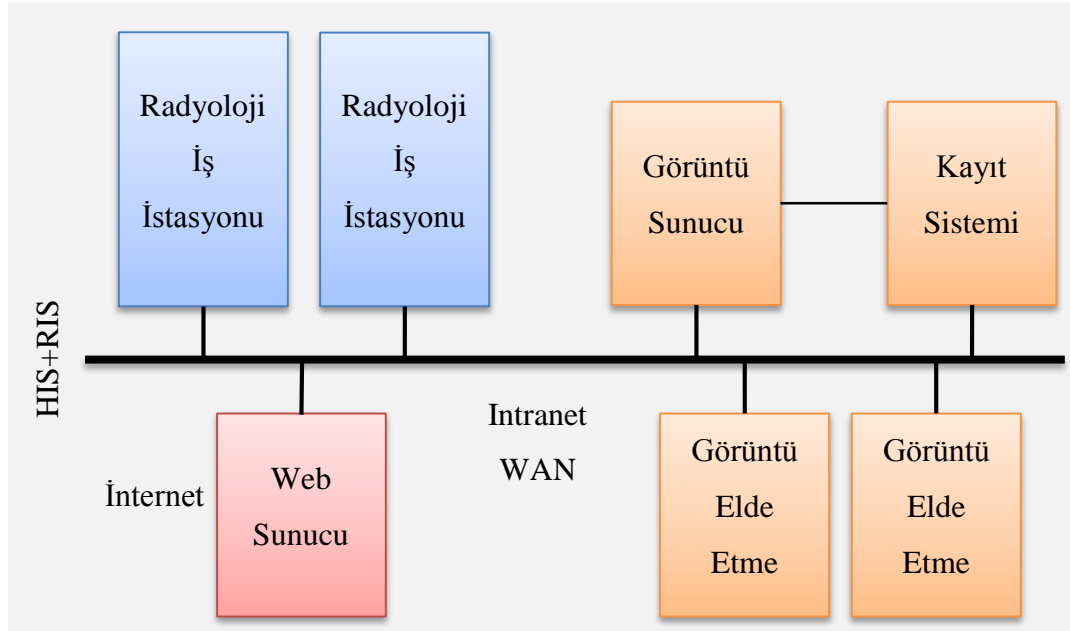
Resim bilgi başlığı 40 bayt yer kaplamaktadır. Bu alan içerisinde yığının kapladığı alan değeri, resmin genişliği, yüksekliği, renk planı, 1 piksel için ayrılan veri alanı (1, 4, 8, 16, 24, 32), resmin sıkıştırılmış ya da sıkıştırılmamış olduğu bilgisi, metre başına düşen X piksel genişliği ve yüksekliği, renk sayısı ve önemli olan renk sayısı gibi bilgiler bulunmaktadır.

Renk haritası RGBA (R:Red-Kırmızı, G:Green-Yeşil, B:Blue-Mavi, A:Alpha-Alfa) her piksel 4 baytlık alan içerecek şekilde oluşturulmaktadır. Renk haritası kullanılarak, renk geçişleri hassasiyetinden ödün verilirken, dosya boyutları azaltılmaktadır. Resim dosya başlığı, resim bilgi başlığı, renk haritası resim dosyasından alındıktan sonra kalan bilgi ise resim verisinin bilgisidir [20, 111].

### **2.3. DICOM (Digital Imaging and Communications in Medicine)**

PACS, medikal görüntülerin elde edilmesi, saklanması, dağıtımı ve geri çağırılması için gerekli yazılım ve platformları yönetmek amacıyla geliştirilmiştir. Şekil 2.4'de görüldüğü gibi PACS, radyoloji ve hastane bilgi sistemleri ile entegre çalışmaktadır ve görüntülerin yönetilmesini sağlamaktadır [7].

PACS herhangi bir yerel ağ (Local Area Network-LAN) ya da geniş ağ (Wide Area Network-WAN) üzerinde merkezde ana sunucu ve ana sunucuya görüntü sağlayan ya da mevcut görüntüleri kullanan iş istasyonlarından (istemciler) oluşmaktadır. Ana sunucu görüntü kayıt etme, çağırma ve yedekleme gibi işlemleri yönetmektedir. Radyoloji iş istasyonları görüntü çağırma, işleme ve görüntülemeyi sağlamaktadırlar. PACS sisteminde hasta bilgileri kolaylıkla HIS ve RIS üzerinden elde edilebilmektedir. İnternet üzerinden haberleşmek için ise Web sunucular gerekmektedir. PACS sisteminde web için görüntülere web adresi (Uniform Resource Locator- URL) verilmektedir. PACS sistemi arşivindeki tüm görüntülere sorgu yapılarak ulaşılabilir [8].



Şekil 2.4. PACS sistematik şeması

PACS içerisinde peta bayt seviyelerinde yer kaplayan medikal görüntülerin boyutlarını azaltmak için sıkıştırma algoritmalarından yararlanılmaktadır. Verinin tekrar elde edilmesini sağlayan kayıpsız sıkıştırma yöntemleri 2:1 ya da 3:1 oranında sıkıştırma yaparken, verinin tekrar elde edilmesinin olanaksız olduğu kayıplı sıkıştırma yöntemleri de 10:1-50:1 ve daha fazla miktarda sıkıştırma gerçekleştirebilir. Ancak mevcut standartlara göre kayıplı sıkıştırılan görüntülerdeki kayıplar radyolojik değerlendirmeyi etkileyebilir. Bu sebeple kayıpsız sıkıştırma yöntemleri (Run Length Coding- RLE, JPEG 2000 vs.) veri boyutlarını azaltmak için tercih edilir.

DICOM, PACS içinde farklı cihazların, yazılımların ve platformların birbirleriyle uyumlu çalışması için gerekli olan tanımlamaları da içermektedir. Amerikan Radyoloji Koleji'nin (American College of Radiology-ACR) ve Ulusal Elektrik Üreticileri Derneği'nin (NEMA, National Electrical Manufacturers Association) bir araya gelmesi ile 1983 yılında geliştirilmeye başlanmıştır. Komitenin ilk hedefi sayısal tıbbi görüntüleme sistemini, cihaz üreticilerinden bağımsız hale getirmektir. Pek çok hata içeren ve kılavuz şeklinde olan ilk sürüm ACR-NEMA 1.0 1985 yılında, ikinci sürüm ise 1988 yılında ACRNEMA 2.0 ismi ile yayınlanmıştır. Bilgisayar ağlarının yaygınlaşması ile de 1993 yılından itibaren DICOM 3.0 standardı PACS içerisinde kullanılmaktadır. Günümüzde, standart üzerinde güncellemeler ve değişiklikler devam etmektedir ve en güncel sürüm 2008 yılında yapılmıştır. DICOM standardı; NEMA standardı (PS3) ve ISO standardı (12052:2006) kullanılarak geliştirilmektedir [8].

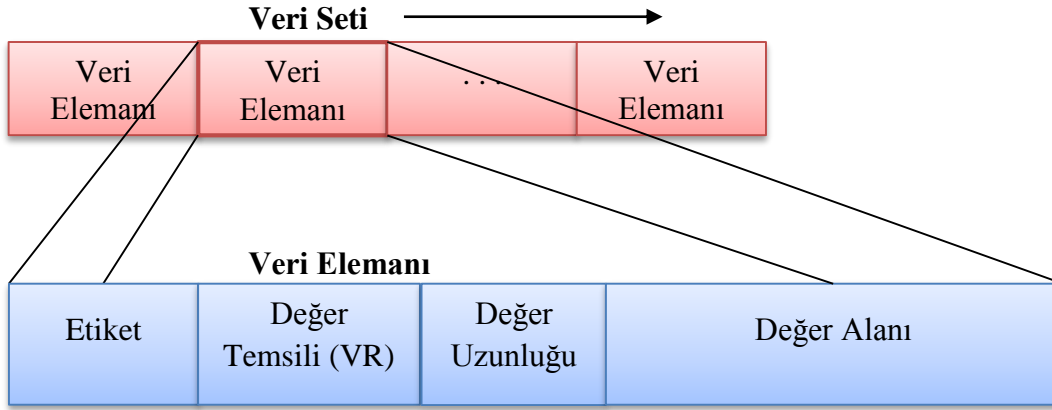
Hasta görüntüleri DICOM'da oluşturulurken hasta, çalışma, seriler ve görüntü basamaklarına göre oluşturulur. Buna göre her hastanın birden çok çalışması olabilmektedir. Her çalışma bir ya da daha fazla görüntü serisine sahip olmaktadır. Her seri ise hastaya ait bir ya da daha fazla görüntü içermektedir.

DICOM dosyası, JPEG, BMP gibi görüntü dosya formatlarından farklılık gösterir. Diğer görüntü dosya formatları dosya başlık kısmında görüntü dışında bilgi içermez. DICOM dosya yapısı ise iki kısımdan oluşur. İlk kısımda hasta (ad, soyad, adres, doğum tarihi vs.), enstitü, doktora ait veriler, çalışma, serilere ait bilgiler ve görüntülere ait kayıt türü, format, çekim özellikleri gibi veriler tutulmaktadır. İkinci kısımda görüntüye ait piksel verileri saklanmaktadır [11-17]. Ticari ya da bedava yazılımlar aracılığıyla DICOM dosyaları kolaylıkla görüntülenmektedir. Bu sebeplerle, bu tez çalışmasında hastanın kişisel haklarının korunması için DICOM dosyasının başlık kısmında yer alan hastaya ait kişisel bilgilerin saldırılara karşı güvenliğinin sağlanması amaçlanmıştır. Tezde hastanın kişisel bilgilerinin elde edilme sürecinin anlaşılması için aşağıda DICOM dosya yapısının özellikleri verilmiştir.

DICOM dosya yapısı 4 farklı alana sahiptir. Bunlar; 128 baytlık boş tutulan açıklama alanı olan önsöz (Preamble), dosyanın bir DICOM dosyası olduğunu belirten ön bildirim alanı ön ek (Prefix), DICOM etiketleri ve etiketler ile birlikte gelen verileri içeren veri elemanları

(Data Elements), resim bilgisinin saklandığı piksel verisi (Pixel Data) alanlarıdır [11-17]. DICOM dosyaları üzerinde okuma ve yazma onaltılık sayı sistemi ile yapılmaktadır.

DICOM dosyasında veriler (karakter, tam sayı, ondalıklı sayı, tarih gibi) 27 tane temel veri tipi kullanılarak, çift sayı uzunlukta olacak şekilde saklanır. DICOM içinde okuma ve yazma işlemleri için DICOM veri sözlüğü oluşturulur. Sözlük içine veriler sıralı olarak yerleştirilir. Her veri elemanı, etiket (Tag), değer temsili (Value Representation-VR), değer uzunluğu (Value Length - VL) ve değer alanına (Value Field -VF) sahiptir [11-14]. Şekil 2.5’de DICOM veri elemanının standart yapısı görülmektedir.



Şekil 2.5. DICOM veri elemanının özellikleri

Şekil 2.5’te görüldüğü gibi, her veri elemanı içinde yer alan etiket “(grup, eleman)” çifti ile numaralandırılır. Örneğin hasta ismi ve doğum tarihi etiket içinde “Patient Name” (0010,0010), “Patient Birth Date” (0010, 0030) şeklinde tutulur. Buradaki 0010 grup numarasını, 0010 ve 0030 ise eleman özelliklerini göstermektedir.

Çizelge 2.1’de dosya başlık kısmında yer alan temel veri eleman özellikleri verilmiştir. VR içerisinde 2 harften oluşan kısaltılmış bir isim ve isimle ilgili tanım, verinin uzunluğu ve içerebileceği karakterler ile ilgili açıklama yer almaktadır. Bu tez çalışmasında DICOM sözlüğü içerisinde yer alan veri elemanlarından hasta kişisel bilgilerini taşıyan veriler geliştirilen yazılım aracılığıyla elde edilmiştir.

Çizelge 2.1. DICOM başlık kısmında yer alan temel veri eleman özellikleri

Özellik İsmi	Etiket (grup, eleman)	Tip	Özellik Açıklaması
Patient's Name	(0010,0010)	2	Hastanın tam adı
Patient ID	(0010,0020)	2	Hasta için verilen kimlik numarası
Patient's Birth Date	(0010,0030)	2	Hastanın doğum tarihi
Patient's Sex	(0010,0040)	2	Hastanın Cinsiyeti M = erkek F = kadın O = diğer
Study Instance UID	(0020,000D)	1	Çalışmanın tekil tanımlayıcı numarası
Study Date	(0008,0020)	2	Çalışmanın başladığı tarih
Study Time	(0008,0030)	2	Çalışmanın başladığı saat
Study ID	(0020,0010)	2	Kullanıcı ya da cihazın ürettiği çalışma numarası
Modality	(0008,0060)	1	Serideki görüntüleri tanımlayan terimler
Series Instance UID	(0020,000E)	1	Serinin tekil tanımlayıcı numarası
Series Number	(0020,0011)	2	Seri için verilen numara

#### 2.4. Steganografi Teknikleri

Günümüzde, bilgi ve bilgi güvenliğinin sağlanması sistemlerin, kurum ve kuruluşların en önemli sorunudur. Gelişen teknoloji sonucunda sayısal ortamdaki (metin, ses, görüntü ve video dosyaları) verilerin korunması gerekmektedir. Verilerin korunmasında ve gizlenmesinde; mesajın içeriğinin korunmasını sağlayan şifreleme yöntemleri ve mesajın varlığının gizlenmesini sağlayan steganografi yöntemleri kullanılmaktadır.

Kriptoloji hem şifre bilimi (Kriptografi) hem de şifre analizini (Kriptanaliz) inceleyen matematiğin alt dalıdır. Kriptografi paylaşılan, gönderilen ve alınan verinin güvenliğini sağlar. Kriptanaliz de ise şifreyi çözmeye ve şifreli verileri açığa çıkarmaya çalışır [29, 112, 113].

Steganografi kelimesi Yunan alfabesine göre “steganos: gizli, saklı” ve “grafi: çizim ya da yazım” kelimelerinden türetilmiştir. Antik Yunan ve Herodot zamanından beri kullanılan oldukça eski bir yöntemdir. M.Ö. 480 yılında Yunanlılar ve Persler arasındaki savaş sırasında ilk kez kullanılmıştır. İran’da bulunan bir Yunanlı, Yunanlılara karşı düzenlenmesi



planlanan Pers istilasını kölesinin başına kazıtarak, kafa derisinin üzerine dövme ile yazdırmıştır. Kölenin saçları uzadıktan sonra Atina'ya gönderilmiştir. Kölenin saçlarının tekrar kazıtılması ile mesaj elde edilmiştir ve Yunanlılar savaşı kazanmıştır [29, 41, 112-113].

Steganografi ile ilgili tarihte farklı örnekler mevcuttur (Yumurta üzerine civa ile yazı yazma, mesajın yazıldığı kâğıdın balmumu ile kaplanarak yutulması vb.). Tarihte steganografi ve kriptoloji özellikle I. ve II. Dünya Savaşlarında bir arada kullanılmıştır. Örneğin; mors kodları, mikro nokta, mor ötesi boya ile yazı yazan spreylere ve kalemler vb.[29, 41, 112-113].

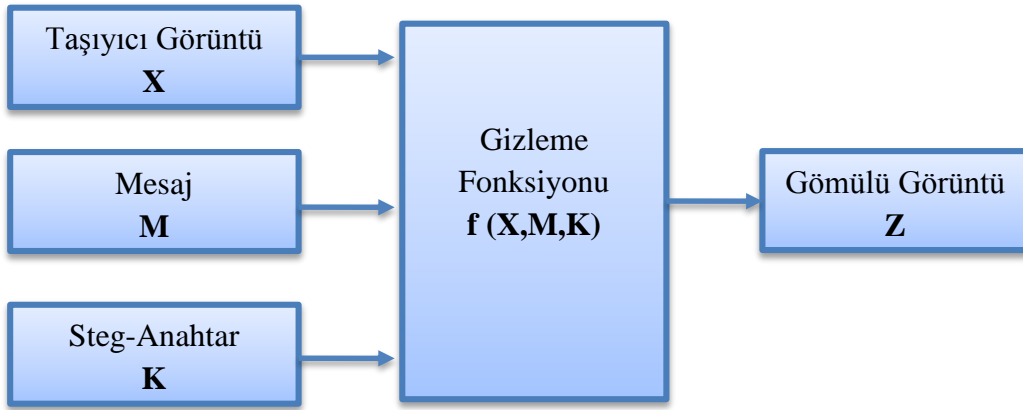
Günümüzde ise bilgisayar teknolojilerinin gelişmesi ile steganografinin uygulama alanları da değişmiştir. Steganografi ile sayısal ortamda tutulan ses, metin, görüntü ve video gibi dosyalara veri saklanarak dikkat çekmeden iletilmesi sağlanmaktadır. Bu sistemde gizli verilerin açığa çıkma ihtimaline karşılık ise veriler şifrelenmektedir.

Steganografi, gizli olan herhangi bir verinin, üçüncü şahısların haberi olmayacak şekilde, gizli olmayan sayısal medya ortamları (ses, metin, görüntü, video gibi) içerisinde gizlenmesi ve elde edilmesi işlemidir. Steganografi de araç olarak kullanılan gizleme ortamına taşıyıcı-nesnesi (cover-object), oluşan ortama da gömülü-nesnesi (stego-object) denilmektedir. İnsan görme sistemi resim dosyalarındaki küçük değişimleri fark edememektedir. Aynı şekilde insan ses sistemi de müzik dosyası üzerindeki küçük değişimleri algılayamamaktadır [19, 45].

Steganografi teknikleri insan sistemindeki bu eksiklikten yararlanarak verilerin multimedya dosyaları içerisine gizlenilmesini sağlamaktadır. Aynı zamanda dosya içerisinde mevcut olan boşluklara ya da sıkıştırma sonrasında açılan boşluklara veri gizlenilebilmektedir [29, 41, 112-113].

Steganografinin en temel özellikleri; algılanamamazlık, sağlamlık ve kapasitedir. “Algılanamamazlık”; gizli verinin gömülü nesne üzerinde fark edilmemesini, “kapasite”; gizlenen verinin bit miktarını, “sağlamlık”; gizli verinin elde edilmeye karşı dirençli olmasını ifade etmektedir [20, 21, 44].

Bu tez çalışmasının da konusu olan görüntü dosyaları için bir gizli anahtar aracılığıyla şifrelenen verinin gizlenmesini sağlayan bir steganografik sistem Şekil 2.6'da gösterilmektedir [21]. Şekil 2.6'da görüldüğü gibi, gönderici bir gizleme fonksiyonu kullanarak veriyi gizlemektedir. Gizleme fonksiyonu, veriyi saklayan taşıyıcı ortam ve gizlenecek veriden oluşmaktadır. Literatürde gizleme işlemi için görüntü uzayı ve dönüşüm uzayı tabanlı yöntemler kullanılmaktadır. Görüntü uzayını kullanan yöntemleri, görüntü piksel değerlerinin en az ağırlıklı bitlerini (Least Significant Bit- LSB) ya da maskeleyme ve filtreleme tekniklerini kullanırlar. Dönüşüm uzayı tabanlı yöntemlerde ise görüntü frekans uzayına dönüştürülür ve veri gizleme işlemi burada gerçekleştirirler. Dönüşüm uzayında en yaygın olarak kullanılan dönüşümler; ayrık kosinüs dönüşümü (Discrete Cosine Transform- DCT), ayrık fourier dönüşümü (Discrete Fourier Transform- DFT) ve ayrık dalgacık dönüşümüdür (Discrete Wavelet Transform-DWT) [20, 29, 41, 45, 112, 113].



Şekil 2.6. Görüntü dosyaları için bir steganografik şifreleme sistemi

Görüntü uzayında yapılan işlemlerin işlem maliyetleri düşüktür. Aynı zamanda daha basit tekniklerdir. Ancak, bu yöntemler görüntü üzerinde gerçekleştirilecek ufak değişmelere (filtreleme, sıkıştırma, boyut değiştirme, döndürme, kırpma vb.) karşı hassastırlar. Dönüşüm uzayında gerçekleştirilen gizleme işlemleri sonucunda oluşan gömülü görüntüler ise saldırılara karşı daha dayanıklıdır. Ancak dönüşüm uzayını kullanan yöntemler, görüntü uzayı yöntemlerine göre daha az veri saklarlar, işlem maliyetini ve yükünü artırırılar [29, 41, 112-113].

Steganografi yöntemlerinde güvenlik çok önemlidir. Eğer taşıyıcı görüntü ile gömülü görüntü arasındaki entropi değeri sifira yakın ise steganografi işlemi güvenlidir, ancak bu

değeri elde etmek zordur [29, 41, 112-113]. Bu sebeple kullanılan steganografik yöntemlerde saklanacak olan bilginin boyutları taşıyıcı nesnesinin boyutlarına uygun olacak şekilde belirlenmelidir. Ayrıca, gizli mesaj taşıyıcı görüntüye eklenirken bazı gürültüler ve bozulmalar oluşturmaktadır. Gömülü görüntüde oluşan bu değişimler olabildiğince şeffaf olmalıdır ve gömülü görüntünün kapasitesinde artış gerçekleştirmemelidir.

#### **2.4.1. Görüntü steganografi teknikleri**

Görüntü steganografisi için literatürde pek çok yöntem önerilmiştir. Bunlar, yer değiştirme sistemleri, dönüştürme teknikleri, yayılı spektrum teknikleri, istatistiksel yöntemler, bozulma teknikleridir [37]. Yer değiştirme teknikleri içerisinde en sık kullanılanı en az ağırlıklı bite ekleme ve bit düzlem araçlarıdır.

##### En az ağırlıklı bite şifreleme (LSB)

En az ağırlıklı bite (LSB) ekleme yöntemi literatürde yaygın olarak kullanılır ve yöntemin uygulanması da kolaydır. LSB yönteminde, görüntüyü oluşturan her pikselin her baytının en az ağırlıklı biti olan son biti o bitin yerine gizlenmesi istenilen verinin bitleri ile sırasıyla değiştirilmektedir. Pikselin sekiz bitinden en az ağırlıklı olan bir biti değiştirildiğinde oluşan bu değişim insan gözü tarafından algılanamamaktadır. LSB yöntemi görüntünün başından ya da sonundan olmak üzere sıralı bir şekilde yapılabilir ya da bir rastgele fonksiyon aracılığıyla gerçekleştirilebilir [16, 29, 34, 37, 41, 112, 113].

Steganografide gizlenen verinin saldırılara karşı güvenliği gizli anahtarlarla sağlanabilir. Steganografik anahtarlar; verinin görüntü içine gizlenmesi ve çıkartılması işlemini kontrol ederken, kriptografik anahtarlar; mesajın gizlenmeden önce şifrelenmesi ve elde edilirken de çözülmesinde kullanılırlar. Örneğin renk değeri 182 (10110110) olan gri seviyeli bir görüntünün pikselinin içine 1 değeri saklandığında 183 (10110111) değeri oluşmaktadır. Oluşan bu renk değeri gözle fark edilememektedir [34].

LSB yönteminin kapasitesi görüntü boyutları ile ilişkilidir ve gücünü algılanamazlık özelliğinden alır. Ancak veriyi elde etmek için gerçekleştirilen saldırılara ve değişimlere (ölçeklendirme, döndürme, kırpma, gürültü ekleme) karşı sağlam değildir.

### Taşıyıcı bölgeler ve eşlik bitleri

Taşıyıcı bölgeler görüntünün altkümeleridir ve bu bölgeler farklı şekillerde oluşturulabilmektedir. Bir bölgenin eşlik biti Eş. 2.2'deki gibi hesaplanmaktadır.

$$p(I) = \sum_{j \in I} LSB(c_j) \bmod 2 \quad (2.2)$$

Eş. 2.2.'de  $c$  taşıyıcı görüntünün boş olmayan alt kümelerini,  $p(I)$  eşlik bitlerini ifade etmektedir. Mesaj gizleme yapılırken, mesaj bitleri görüntü bölgelerinin eşlik bitine göre yerleştirilir. Çözme işleminde ise görüntünün tekrar eşlik bitleri hesaplanmaktadır ve mesaj bitleri sıralı bir şekilde çıkartılmaktadır [37].

### Palet tabanlı gizleme

Palet tabanlı görüntüler, görüntü renk bilgisini gösteren renk uzayından oluşan renk altkümesine sahiptir. Her palet tabanlı görüntü; özelleştirilmiş  $N$  tane renge ve palet içinde her pikseli ifade eden renk verisine sahiptir. Resmin dosya boyutunu azaltabilmek için renk sayısını azaltma yoluna giderek sıkıştırma yapılmaktadır. Palet tabanlı gizleme işlemlerinde genellikle GIF ve TIFF uzantılı görüntüler tercih edilmektedir. Bilgi gizleme işleminde ya palet ya da resim verisi üzerinde değişiklikler yapılmaktadır. Renk vektörünün LSB değerlerinde ya da farklı şekillerde sıralanan renk paletiyle de veri gizlenilebilir. İnsan göz sistemi, paletteki farklı bir sıralamayı fark etmeyecektir.  $N!$  değerinde palet sıralaması yapılabildiğinden veri taşımak için yeterli alan oluşmaktadır. Bu yöntemde her renk değeri için Öklid uzaklık değeri hesaplanmaktadır (Eş. 2.3) ve bu değerler sıralanmaktadır.

$$d = \sqrt{K^2 + Y^2 + M^2} \quad (2.3)$$

Eş. 2.3'deki K: Kırmızı, Y: Yeşil, M: Mavidir. Sıralanan renk paletinden sonra renk indislerinin LSB'leri mesaj bitleri ile değiştirilmektedir. Mesajı elde etmek için ise önce sıralı paletteki rengin sıra numarasına ulaşılmaktadır, sıra numarasının son basamağındaki sayı ile gizlenen mesaj elde edilmektedir. Yapılan bazı çalışmalarda palet sıralamasına gerek kalmadan her pikselin en yakın renk değerleri Öklid normu ile hesaplanmış ve bu değerlerin eşlik bit değeri hesaplanarak mesaj bitlerinin buralarda yerleştirilmesi sağlanmıştır. Farklı

çalıřmalarda ise resmin renk deęerlerinin azaltılması ile mesaj gizlenmesi gerekleřtirilmiřtir [37]. Grnt uzayında gerekleřen bu iřlemler LSB yntemi gibi saldırılara karřı saęlam deęildir.

### Dnřm uzayı teknikleri

Mesajları grnt ierisine gizlemek iin dnřm uzayı teknikleri de kullanılmaktadır. Bunun iin genellikle DCT, DFT, DWT yntemleri tercih edilmektedir.

DCT ile grnt, zaman blgesi yerine frekans blgesine tařınarak burada gizleme yapılmaktadır [37]. Bu yntemde, tařıyıcı grntnn DCT katsayılarına mesaj bitleri yerleřtirilerek nicemleme gerekleřtirilir. Ardından grntnn ters kosins dnřm alınarak tekrar zaman uzay eksenine geilmektedir ve grnt tekrar elde edilmektedir. JPEG dosya formatı oluřturulurken de DCT dnřm kullanılmaktadır. DCT ile bir grntnn kosins katsayıları elde edilmektedir ve yksek frekanslı katsayılar atılıp ters dnřm yapılarak grnt zellikleri korunmaktadır.

DWT dnřm ise JPEG-2000 algoritmasında tercih edilmiřtir. Bir grntnn dalgacık dnřm, ok lekli uzamsal frekans analizi yapılarak gerekleřtirilir. Bir grntde 2-Boyutlu DWT dnřm yapıldıęında, grnt farklı yksek ve alak frekanslı alt bileřenleri temsil eden znrlk seviyelerine ayrıřtırılır. Bu ayrıřma iin eřitli filtreler (Haar, Daubechies Ortogonal filtresi, Daubechies Bi- Ortogonal filtresi vb.) kullanılmaktadır [29].

Grntlere farklı seviyelerdeki ayrıřtırma uygulandıktan sonra, dřk frekanslı ancak byk genlikli DWT katsayıları ve yksek frekanslı ancak dřk genlikli DWT katsayıları elde edilir. Her znrlk seviyesi iin iki ortogonal kanal bant geiren filtre baęlanarak alt-rnekleme gerekleřtirilir. Filtreleme iřlemi ise iteratif olarak grnty ayrıřtırır. Ayrıřtırılan bu alt znrlk seviyelerinde ise veri gizlenerek grnt tekrar elde edilir [29].

### İstatistiksel yöntemler

İstatistiksel yöntemlerde taşıyıcı görüntü bloklara ayrılır ve gizleme yapılacak bloklar 1 işareti ile işaretlenir. Bu işaretleme gerçekleştirilirken içinde bulunan görüntü bloğuna farklı hipotez testleri ile istatistiksel analizler yapılır ve gizleme yapılacak piksel seçilir. Bu seçim işlemi için piksellerin dağılımı, varyans değerleri, minimum, maksimum, ortalama gibi tanımlayıcı istatistiksel değerleri kullanılır [37].

### Algısal maskeleye sistemleri

Steganografik teknikler veriyi örtü nesnesi içerisine kayıt ederken algılanmamasını hedeflemektedir. Bu amaçla kullanılan maskeleye teknikleri en önemsiz bitleri algısal olarak seçerek gizleme işleminin daha güvenli hale getirilmesini sağlamaktadır. Maskeleye ile bir sinyal içinde farklı bir sinyalin varlığı fark edilmemektedir. Maskeleye işlemi gizlenecek verinin boyutu ve görüntünün karakterine göre değişir [20, 39].

### Geliştirilen bazı programlar

Farklı steganografi tekniklerinden yararlan pek çok yazılım geliştirilmiştir. Bunlar StegoDos, S-Tools, MondelSteg, EzStego, Hide and Seek, Hide4PGP, White Noise Storm, Stegonos vb.dir [20, 39]. Bu yazılımlar DICOM dışındaki görüntü dosyalarında veri gizleme ve veriyi açığa çıkarmak için kullanılmaktadır.

## **2.5. Bulanık Mantık**

Bu tez çalışmasında LSB yönteminin güçlendirilmesi için Bulanık Mantık (Fuzzy Logic-FL) algoritmasından yararlanılmıştır. Görüntü piksellerinin benzerlik derecelerinin belirlenmesinde FL algoritması kullanılmıştır. Benzerlik, pikseller arasındaki uzaklığın Öklid norm ile hesaplanması sonucunda belirlenmektedir. Ancak Öklid norm uzaklığı algısal olarak piksel benzerliğini hesaplayamaz. Bu sebeple, görüntü piksel benzerliğinin elde edilmesi problemi belirsiz ve karmaşıktır.

FL klasik yöntemlerle analiz edilemeyen, karmaşık, belirsiz ve kesin olmayan problemleri çözmek için kullanılır [114]. Bu yöntem ilk kez 1956 yılında Amerika Birleşik Devletlerinde

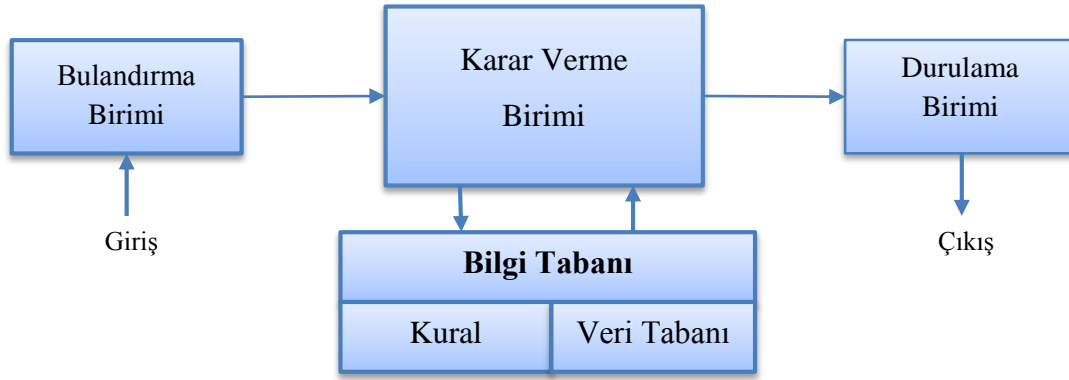
düzenlenen bir konferansta sunulmuş olmakla birlikte, kuramın detaylarını Lotfi A. Zadeh 1965 yılında yayınladığı makalede ortaya koymuştur. Buna göre insan düşüncesi bulanıktır ve boolean mantığı insan düşünce sisteminin ihtiyaçlarını ortaya koyamamaktadır. Zadeh tarafından ortaya konulan bulanık mantık kuramının genel özellikleri şöyledir:

- FL'de yaklaşık düşünme kesin düşünmenin yerini alır.
- FL'de her durum  $[0, 1]$  aralığında tanımlanan derecelerle ifade edilir.
- FL'de bilgi büyük, küçük, orta, çok az, daha az gibi çeşitli dilsel ifadelerle dönüştürülür.
- FL'de bulanık çıkarım dilsel ifadeleri kapsayan kurallar ile gerçekleştirilir.
- Her mantıksal sistem ve problem bulanık olarak tanımlanabilir.
- FL özellikle matematiksel modeli zor olan sistemlerin sorunlarını çözebilmektedir [114].

FL'in temeli bulanık küme ve alt kümelerle dayanır. Bulanık kümede, klasik kümeden farklı olarak ara değerler mevcuttur ve varlıklar biraz soğuk, biraz sıcak, biraz karanlık gibi dilsel ifadelerle tanımlanırlar. Bulanık varlık kümesinde, her bir varlığın  $[0-1]$  aralığında herhangi bir değer alabilen üyelik derecesi mevcuttur [114-116].

FL'de öncelikle problemin durum, giriş ve çıkış değişken dizileri tanımlanır. Bulanık alt kümelerin her bir değişkeni için aralıklar belirlenir ve her birine dilsel bir etiket atanır. Her bulanık alt küme için üyelik işlevi tanımlanır. Sistemi ve problemi iyi bilen uzmanlarca kural tabanı oluşturulur. Giriş bilgileri bulanık kümeler (üçgen, yamuk, çan eğrisi gibi) aracılığıyla bulandırılır. Bulanık kurallar kullanılarak bulanık çıkarım yapılır. Sistem tarafından algılanamayacak olan bulanık ifadeler durulaştırılarak, tekrar sistemin anlayacağı sayısal ifadelerle dönüştürülür [114-116]. Şekil 2.7'de bulanık mantık sisteminin akış diyagramı görülmektedir.

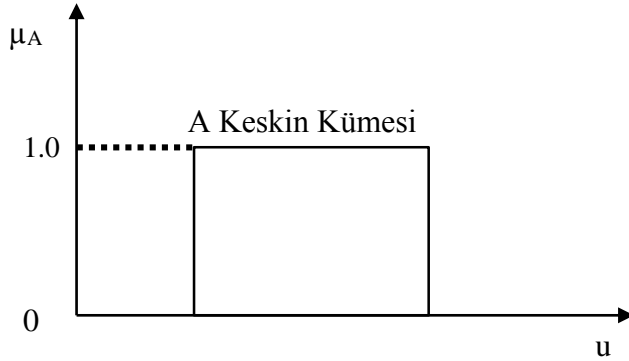
Bu çalışmada görüntü piksel değerlerinin benzerliği problemi FL ile analiz edilmiştir. Görüntü piksel değerleri bulanık kümeler aracılığıyla bulandırılarak, üçgen kümelerle üyelik değerleri hesaplanmıştır. Ardından kural tabanı kullanılarak bulanık çıkarım gerçekleştirilmiş, elde edilen bulanık ifadeler durulaştırılarak piksel benzerlik değerleri hesaplanmıştır. Yöntemin anlaşılması için FL algoritmasının detayları hakkında bilgiler verilmiştir.



Şekil 2.7. Bulanık mantık sisteminin akış diyagramı

### Bulanık küme kavramı

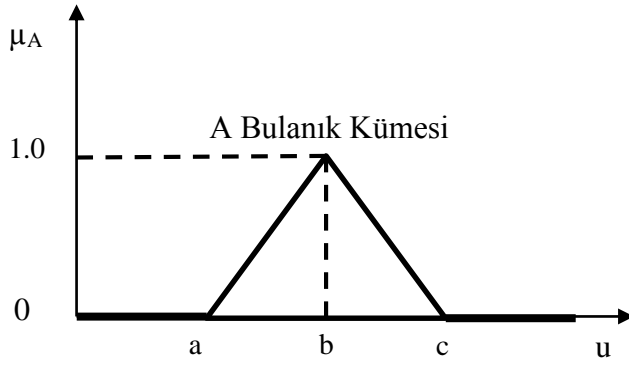
Klasik küme kavramında bir eleman o kümenin elemanıdır (0) ya da değildir (1), kısmi üyelik söz konusu değildir  $\{0,1\}$ . Klasik küme örneği Şekil 2.8’de verilmiştir [114-116].



Şekil 2.8. Klasik küme örneği

Bulanık kümelerde kısmi üyelik söz konusudur ve bulanık kümenin elemanlarının alacağı üyelik değerleri  $[0-1]$  aralığındadır. Bulanık küme, keskin bir kümenin genelleştirilmiş halidir. Bulanık küme elemanlarının üyelik değerini belirlemek için üyelik fonksiyonu olarak adlandırılan üçgen, yamuk, çan eğrisi vb. fonksiyonlar kullanılır. Şekil 2.9’da bulanık küme ve üçgen üyelik fonksiyonu verilmiştir. Üyelik işlevleri 3 (küçük, orta, büyük), 5 (küçük, orta küçük, orta, orta büyük, büyük) ve 7 (çok küçük, küçük, az küçük, sıfır, az büyük, büyük, orta büyük) gibi farklı dilsel ifadelerle tanımlanmaktadır [114-116].





Şekil 2.9. Bulanık küme örneği ve üçgen üyelik fonksiyonu

Bir bulanık küme, küme elemanları ve onların üyelik dereceleri ile oluşturulabilir. A bir bulanık küme olmak üzere Eş. 2.6'daki gibi tanımlanabilir.

$$A = \{u/\mu_A(u) | u \in U\} \quad (2.6)$$

Eş. 2.6'daki u, A kümesinin elemanı, U ise A kümesinin tanımlandığı evrendir [114-116].  $\mu_A(u)$  ise üyelik işlevini ifade etmektedir.

Üyelik işlevi bir kümenin elemanlarının kümeye üyelik derecesini hesaplar ve  $[0,1]$  arasında değer alır. Eş. 2.7 üyelik işlevi tanımlanmaktadır [114-116].

$$\mu_A(u): U \rightarrow [0,1]; \mu_A(u) \in [0,1] \quad (2.7)$$

Eş. 2.7'deki A bir bulanık kümenin elemanı,  $\mu_A(u)$  üyelik işlevi, U ise A kümesinin tanımlandığı evrendir.

### Bulandırma birimi

Bulandırma birimi giriş bilgilerini dilsel niteleyiciler aracılığıyla sembolik değerlere dönüştürür. Üyelik fonksiyonları aracılığıyla giriş bilgilerinin az küçük, küçük, çok küçük gibi dilsel ifadeler için kullanılan bulanık kümelere üyelik derecesi hesaplanmaktadır.

### Bilgi tabanı

Karar verme birimi içinde kullanılır, sistem ile ilgili bilgilerin kurallar halinde tutulduğu veri tabanı ya da kural tabanı kısımlarına sahiptir [114-116]. FL sistemlerinde girişler ve çıkışlar arasındaki bağlantılar kurallar aracılığıyla belirlenir.  $A$  ve  $B$  giriş,  $C$  çıkış olmak üzere FL sistemi için örnek bir kural: EĞER  $A=x$  ve  $B=y$  ise O HALDE  $C=z$  şeklindedir.

### Karar verme birimi

FL sistemlerinin merkezini oluşturur ve bulanık kavramların işlenmesini ve çıkarım yapılmasını sağlar. Literatürde yaygın olarak Mamdani ve Sugeno bulanık çıkarım mekanizmaları kullanılmaktadır. Mamdani tip çıkarım yapılırken minimumların maksimumu (Min-Max) ve maksimum çarpım (Max-Dot) yöntemleri kullanılmaktadır. Max-Dot yönteminde her bir giriş değeri ait olduğu bulanık kümelerin üyelik derecesine göre tekrar ölçeklendirilir. Çıkış değeri ölçeklenen bulanık kümelerin maksimum değeri alınarak bulunur. Min-Max yönteminde ise bulanık kümelerin girişlerinin üyelik derecelerinin üzerindeki kısımları kesilir. Çıkış değeri elde edilen bulanık kümelere örneğin ağırlıklı ortalama yöntemi uygulanarak elde edilir. Sugeno çıkarım yönteminde ise kuralların çıkışları giriş değerlerinin doğrusal birleşimi ile elde edilir, keskin çıkış içinde ağırlıklı ortalama kullanılır [114-116].

### Durulama birimi

Karar verme işlemi sonrasında bulanık kümeler elde edilir. FL sisteminin çalışabilmesi için bulanık ifadeler durulanarak sayısal ifadelere dönüştürülür. Durulamada; maksimum üyelik, ağırlık merkezi, ağırlık ortalaması ya da mean-max gibi farklı yöntemler kullanılır. Yaygın olarak kullanılan ağırlık ortalaması yönteminde Eş. 2.8'de verilen hesaplamalar gerçekleştirilir [114-116].

$$z^* = \frac{\sum \mu_c(\bar{z})\bar{z}}{\mu_c(\bar{z})} \quad (2.8)$$

Eş. 2.8'de verilen  $z$  her bir üyelik fonksiyonunun merkezidir.

## **2.6. Sıkıştırma Teknikleri**

Veri sıkıştırma yöntemleri, kayıplı ve kayıpsız sıkıştırma yöntemleri olmak üzere ikiye ayrılırlar. Kayıplı sıkıştırma yöntemleri, verinin bütünlüğünü en az etkileyecek kısımların atılarak kalan kısımlara kayıpsız sıkıştırma uygulanarak gerçekleştirilir. Bu yöntemde sıkıştırma sonrasında verinin tamamı geri getirilemez. Kayıplı sıkıştırma yöntemleri görüntü, video ve ses dosyalarının sıkıştırılmasında kullanılır. İnsan gözü ve kulağı yüksek frekans değerlerine hassas olmadığı için genellikle eleme yüksek frekans üzerinde gerçekleştirilir. Kayıpsız sıkıştırma yöntemleri, orijinal verinin sıkıştırıldıktan sonra geri getirilmesini sağlar ve hızlı çalışır, ancak yöntemlerin sıkıştırma oranı azdır. Ses ve video verileri sıkıştırılırken yüksek sıkıştırma oranı sağladığından genellikle kayıplı sıkıştırma yöntemleri tercih edilir. Görüntü verilerinde ise fotoğraflarda kayıplı, düşük frekanslı görüntülerde kayıpsız sıkıştırma yöntemleri kullanılır [30].

Kayıpsız sıkıştırma yöntemleri olasılık tabanlı ve sözlük tabanlı yöntemler olarak iki gruba ayrılmaktadır. Olasılık tabanlı yöntemlerde veri içinde daha sık tekrar eden semboller daha küçük boyutta kodlarla saklanır. Sözlük tabanlı yaklaşımlarda ise sık tekrarlanan sembol öbekleri tek bir sembol ile kodlanır.

Bu tez çalışmasında medikal verilerdeki ayrıntılar önemli olduğundan kayıpsız sıkıştırma teknikleri ile gizlenecek mesaj kapasitesinin artırılması için kayıpsız sıkıştırma teknikleri kullanılmıştır. Bu sebeple aşağıdaki başlıklarda çalışmada kullanılan Huffman ve LZW algoritmalarından bahsedilmiştir.

### Huffman kodlaması

1952 yılında David Huffman tarafından geliştirilen entropi kodlama yöntemidir. Bu yöntemde verilerin frekansına bakılarak en az kullanılan karakter için en uzun, en çok kullanılan karakter için en kısa kod üretilerek sıkıştırma gerçekleştirilir. % 10 ile % 90 arasında sıkıştırma gerçekleştirebilir [30, 117, 118].

İşlem adımları:

- Veri setine ait karakterlerin frekanslarını gösteren bir ağaç hazırlanır.
- Ağacın en tepesinden aşağıya doğru sola ayrılan kola “0”, sağa ayrılan kola “1” kodu verilir.
- En küçük iki frekans toplanarak frekans tablosu yeniden düzenlenir.
- Tek bir ağaç oluşturulana kadar en küçük frekanslar toplanır.

### LZW algoritması

Lempel–Ziv–Welch (LZW) algoritması Abraham Lempel, Jacob Ziv ve Terry Welch tarafından oluşturulmuştur. 1984 yılında Welch, LZW algoritmasını 1978 yılında Lempel ve Ziv tarafından geliştirilen LZ78 algoritmasından uyarlamıştır. Algoritma sözlük tabanlıdır ve mümkün olan en fazla karakteri içeren kodu sözlüğe ekler. Açma işlemi için sözlüğün saklanması zorunluluğu yoktur. Algoritmanın sözde kodu aşağıdaki gibidir [30, 119, 120].

1. Veri dizisinden bir karakter alınır.
2. Sözlükte karakter aranır.
3. Sözlükte karakter varsa veri dizisinden karakter alınmaya devam edilir ve karakterler genişletilir.
4. Sözlükte karakter yoksa şimdiye kadar uyan sözlük değeri çıkışa verilir.
5. Sözlükte olmayan yeni karakter şimdiye kadar uyan sözlük kaydı ile birlikte, sözlüğe eklenir.
6. Veri dizisi bitmedi ise yukarıdaki işlemler tekrar edilir.

### **2.7. Veri Seti ve Kullanılan Yazılımlar**

Bu çalışmada Gazi Üniversitesi Tıp Fakültesi Nöroloji Bölümü'ne başvuran 22 epilepsi hastasına ait MR görüntüleri ve EEG verileri kullanılmıştır. Oluşturulan veri setinde bulunan 11 erkek ve 11 kadın hastanın yaş aralığı 18 ile 55 arasındadır ve yaş ortalaması  $32 \pm 7.9$ 'dır. Veri setinin detayları ve gizlenecek mesajı oluşturan verilerin kapasiteleri Çizelge 2.2'de verilmektedir. Ayrıca, veri setinin elde edilmesi için Gazi Üniversitesi Tıp Fakültesi'nden alınan Etik Kurul belgesi Ek 1'de verilmiştir.

Çizelge 2.2'den görüldüğü gibi 22 epilepsi hastasına ait farklı boyutlardaki MR görüntüleri mesaj gizlemek için kullanılmıştır. MR görüntüleri 16 bitliktir, ancak yapılan çalışmada

önerilen yöntemlerin kapasitelerini tam olarak ortaya koymak için 2 bayt olan piksellerin yalnızca ilk baytları veri gizlemek için kullanılmıştır. Gizlenecek mesaj MR görüntülerinde yer alan hasta kişisel bilgilerinden, doktor yorumundan ve her görüntü için bölütlenen EEG verilerinden ve EEG dosyasına ait dosya başlık bilgilerinden oluşturulmuştur. Çizelge 2.2 de her hasta için MR görüntülerinde yer alan hasta kişisel bilgilerinin boyutu (EPR), EEG dosyasının başlık bilgilerinin boyutu, EEG verisinin toplam boyutu ve doktor yorumunun boyutu görülmektedir.

Hasta kişisel bilgileri (hastanın adı, verilen numarası, hasta doğum tarihi, cinsiyeti, yaşı, ağırlığı ve adresi, çekim tarihi, saati, numarası, görüntünün yapısı ve tanımı, serinin tarihi, saati ve tanımı) her DICOM dosyasının başlık kısmından ayrı ayrı elde edilmiştir. EEG, 21 yüzey elektrot aracılığıyla uluslararası 10-20 sistemine göre kayıt edilmiştir. EEG verileri yapılan çalışmada “short” veri yapısı ile her karakter 4 bayt yer kaplayacak şekilde aktarılmıştır. Verilerde herhangi bir kayıp söz konusu olmamıştır. Çizelge 2.2’de toplam EEG boyutu Eş. 2.9 kullanılarak hesaplanmıştır.

$$\text{Toplam EEG Boyutu} = \text{Elektrot sayısı} * \text{EEG zaman uzunluğu} * 4 \quad (2.9)$$

Klinikte tanı ve teşhis için kullanılan rutin EEG verisinin kayıt süresi 20 ile 40 dakika arasındadır. EEG dosyaları başlık kısmında zaman boyutu, elektrot sayısı, örnekleme aralığı, başlangıç zamanı ve elektrotların ismi gibi başlık bilgilerini içermektedir.

Çalışma için MR görüntülerinin analizi, EEG verisinin analizi için gereken kodlamalar, önerilen steganografi yöntemlerinin kodlamaları ve taşıyıcı görüntüler ile gömülü görüntüler arasındaki karşılaştırmalar için gerekli kodlamalar Visual Studio. NET 2010 platformunda gerçekleştirilmiştir. İstatistiksel karşılaştırmalar için MATLAB platformu da kullanılmıştır.

Çizelge 2.2. Epilepsi veri setindeki MR ve EEG verilerinin tanımlamaları ve kapasiteleri

Hastalar	MR Görüntüleri	Toplam MR sayısı	EPR* Kapasitesi (bayt)	EEG Bilgi kapasitesi (bayt)	EEG Zaman Uzunluğu	Toplam EEG kapasitesi (bayt)	Doktor Yorumu (bayt)
Hasta-1 (P1)	256x256x113 512x512x119	232	224	334	21X275800	23 167 200	44
Hasta-2 (P2)	256x256x156 512x512x119	275	224	344	21X239400	20 109 600	44
Hasta-3 (P3)	256x256x89 512x512x120	209	220	344	21X246400	20 697 600	44
Hasta-4 (P4)	256x256x115 512x512x119	234	224	344	21X243200	20 428 800	34
Hasta-5 (P5)	256x256x101 512x512x119	220	220	344	21X214600	18 026 400	34
Hasta-6 (P6)	256x256x101 512x512x120	221	216	344	21X225800	18 967 200	34
Hasta-7 (P7)	176x176x138 248x320x20 320x320x40 448x448x20 464x512x20 512x512x3	241	284	344	21X223400	18 765 600	34
Hasta-8 (P8)	176x176x139 248x320x22 320x320x40 448x448x20 464x512x20 512x512x3	243	280	344	21X290600	24 410 400	34
Hasta-9 (P9)	176x176x138 320x320x71 448x448x20 424x512x24 464x512x20	273	284	344	21X268600	22 562 400	34
Hasta-10 (P10)	256x256x111 512x512x119	230	220	344	21X255000	21 420 000	34
Hasta-11 (P11)	176x176x138 320x320x49 448x448x40 464x512x40	267	284	344	21X223400	18 765 600	44
Hasta-12 (P12)	256x256x60 512x512x40	100	260	344	21X217200	18 244 800	14
Hasta-13 (P13)	256x256x60 512x512x40	100	264	344	21X249200	20 932 800	14
Hasta-14 (P14)	256x256x75 512x512x42	117	260	344	21X228600	19 202 400	14
Hasta-15 (P15)	256x256x60 512x512x40	100	260	344	21X190800	16 027 200	14
Hasta-16 (P16)	256x256x60 512x512x40	100	272	344	21X206400	17 337 600	14
Hasta-17 (P17)	256x256x60 512x512x40	100	264	344	21X223800	18 799 200	14
Hasta-18 (P18)	256x256x60 512x512x40	100	268	344	21X329000	27 636 000	14
Hasta-19 (P19)	256x256x60 512x512x40	100	260	344	21X200800	16 867 200	14
Hasta-20 (P20)	256x256x60 512x512x40	100	264	344	21X242800	20 395 200	14
Hasta-21 (P21)	256x256x60 512x512x40	100	264	344	21X230200	19 336 800	14
Hasta-22 (P22)	256x256x60 512x512x40	100	264	344	21X211200	17 740 800	14

\*EPR=DICOM başlık kısmında yer alan hasta kişisel bilgilerini ifade etmektedir.

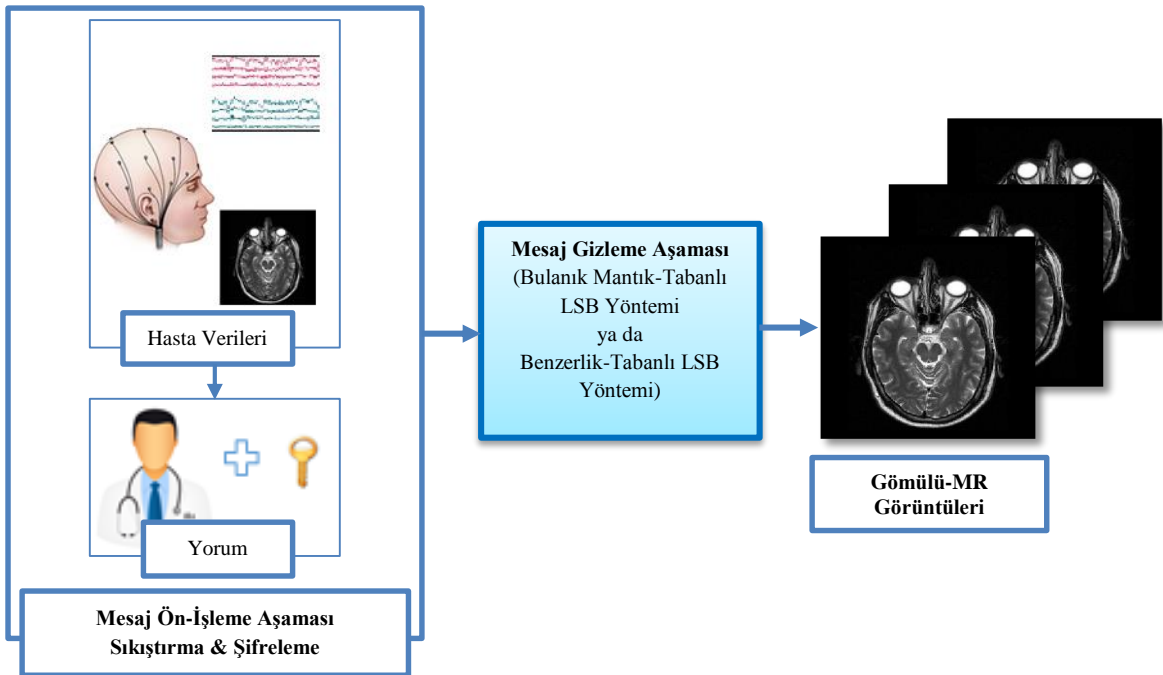


### 3. ÖNERİLEN YÖNTEMLER

Bu çalışmada epileptik hastalara ait medikal verilerin steganografi teknikleri ile güvenliğinin sağlanması amaçlanmıştır. Görüntü uzayında en çok tercih edilen LSB yöntemi, hızlı ve basit bir veri gizleme tekniğidir. LSB ile gizlenen veri gözle fark edilmez ve yöntemin gizleme kapasitesi yüksektir. Bu sebeplerle, bu tez çalışmasında 2. Bölüm’de Çizelge 2.2’de ayrıntıları verilen medikal verilerin güvenliğinin sağlanması için LSB yöntemini geliştiren 2 yöntem önerilmektedir. Tez kapsamında yapılan analizler iki aşamada gerçekleştirilmiştir. Bunlar mesaj gizleme ve gizli mesajı geri elde etme şeklindedir.

#### Mesaj gizleme aşaması

Tez çalışmasında kullanılan mesaj gizleme aşamasının temel blokları Şekil 3.1’den görülmektedir. İlk olarak, epilepsi hastalarının kişisel bilgileri DICOM serisindeki her bir dosyadan ayrı olarak elde edilmektedir. Görüntülerin boyutuna göre EEG verisi bölütlenmektedir. EEG dosyasının başlık bilgileri ve bölütlenen EEG verisi ve onun zaman uzunluğu bir araya getirilmektedir. EEG’ye ait olan bilgilere, görüntüde yer alan kişisel bilgiler ve doktor yorumundan oluşan ön bilgi eklenmektedir. Her görüntü için kişisel bilgiler, EEG verisi ve doktor yorumu birleştirilerek gizlenecek mesaj oluşturulmaktadır.



Şekil 3.1. Önerilen yöntemler için mesaj gizleme aşaması



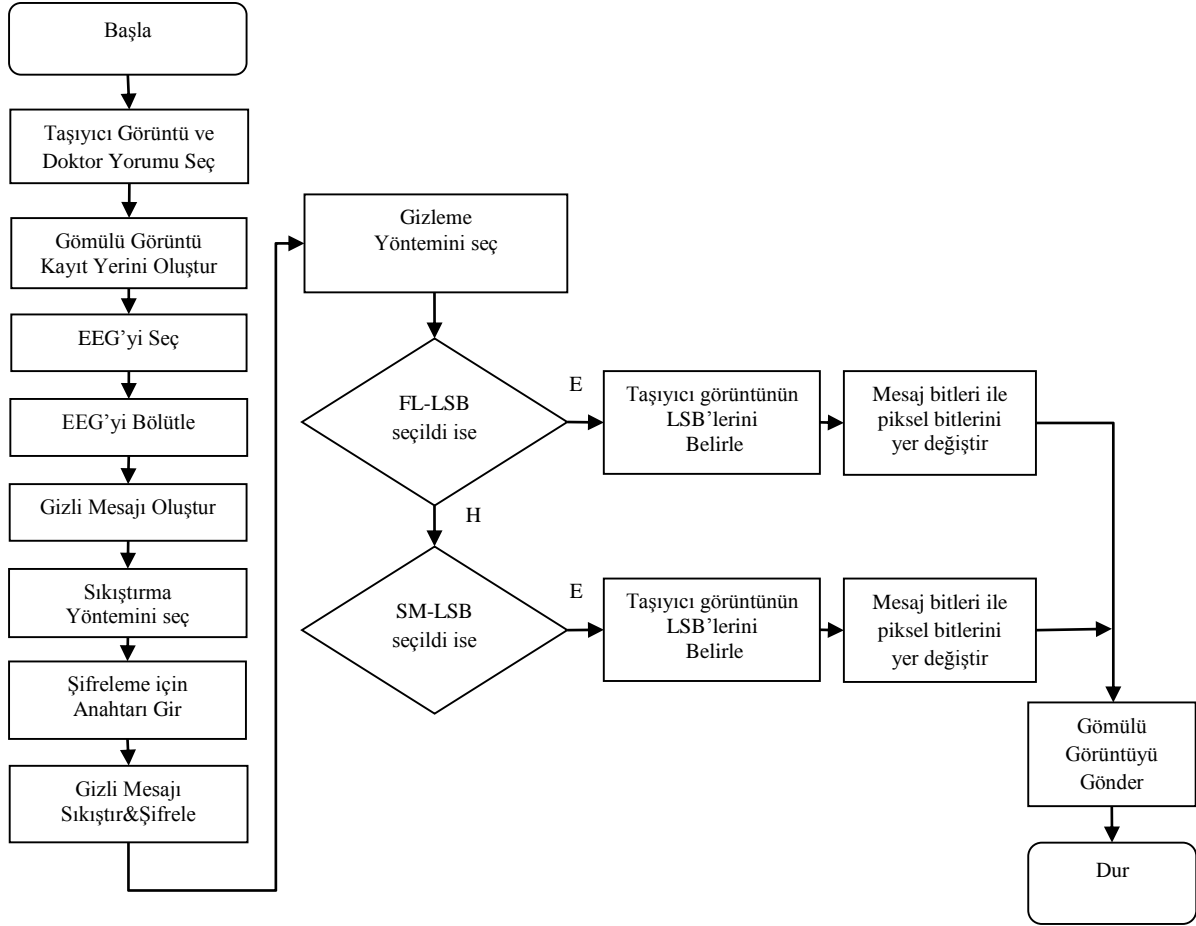
Şekil 3.2’de her DICOM görüntü için oluşturulan mesaj dizisi görülmektedir. Burada EPR DICOM’dan elde edilen hasta kişisel bilgileridir. EEG bölütleme için ((Görüntü Yükseklik\*Görüntü Genişlik\*8)-(EPR+DoktorYorum+EEG Başlık Boyut))/(EEG Elektrot Sayısı) formülasyonu kullanılmaktadır.

<b>Toplam Boyut</b>	EPR	Doktor Yorum	EEG Başlık Bilgileri	Bölütlenen EEG Verisinin Boyutu	Bölütlenen EEG Verisi
---------------------	-----	--------------	----------------------	---------------------------------	-----------------------

Şekil 3.2. DICOM görüntü için oluşturulan mesaj

Mesaj ön işleme aşamasında, kayıpsız sıkıştırma algoritmaları olan LZW ve Huffman yöntemleri saklanacak mesajın kapasitesinin artırılması için kullanılmaktadır [120, 121]. Ayrıca mesajın saldırılara karşı güvenliğini artırmak için Rijndael simetrik şifreleme algoritması ile 128-bitlik anahtar aracılığıyla mesaj şifrelenmektedir.

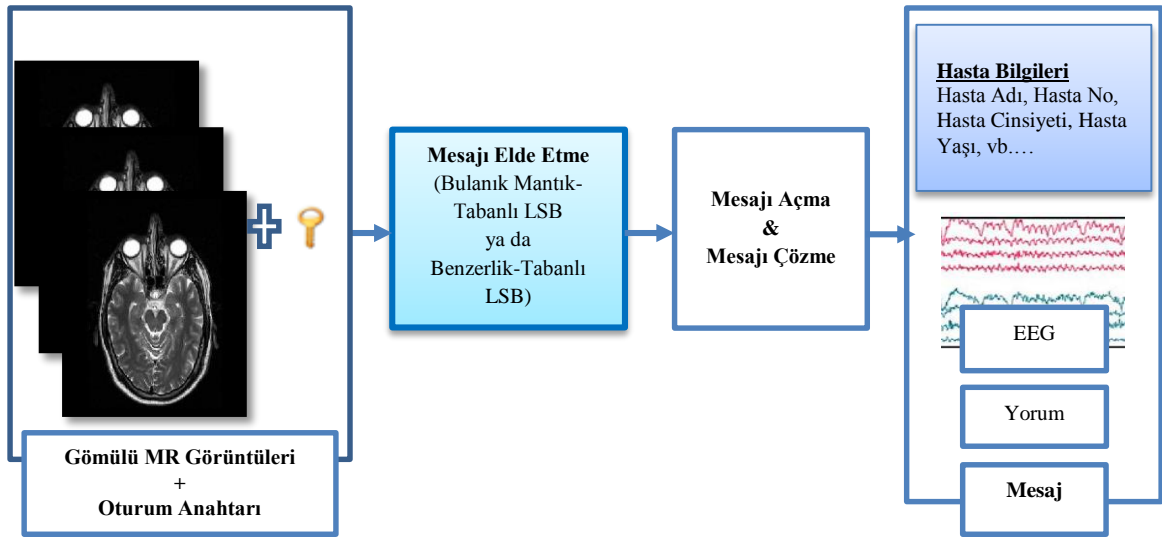
Şekil 3.1’de görüldüğü gibi ikinci olarak, geliştirilen yöntemler olan benzerlik-tabanlı LSB (SM-LSB) ve bulanık mantık-tabanlı LSB (FL-LSB) aracılığıyla görüntü piksellerinin gri seviye farkı hesaplanarak mesajın gizleneceği LSB’ler belirlenmektedir. Önerilen yöntemlerin detayları aşağıdaki başlıklarda verilmiştir. Mesaj gizlemenin son aşamasında ise seçilen görüntü piksellerinin LSB’leri ile mesajın bitleri yer değiştirilmektedir ve gömülü DICOM görüntüleri oluşturulmaktadır. Çalışmada, bilgisayar hesaplama ve işlem maliyetini azaltmak için mesaj gizleme işlemleri hastaya ait tüm DICOM görüntülerinde eş zamanlı olarak gerçekleştirilmektedir. Mesaj gizleme işleminin detayları ise Şekil 3.3’de verilen akış şemasından görülmektedir.



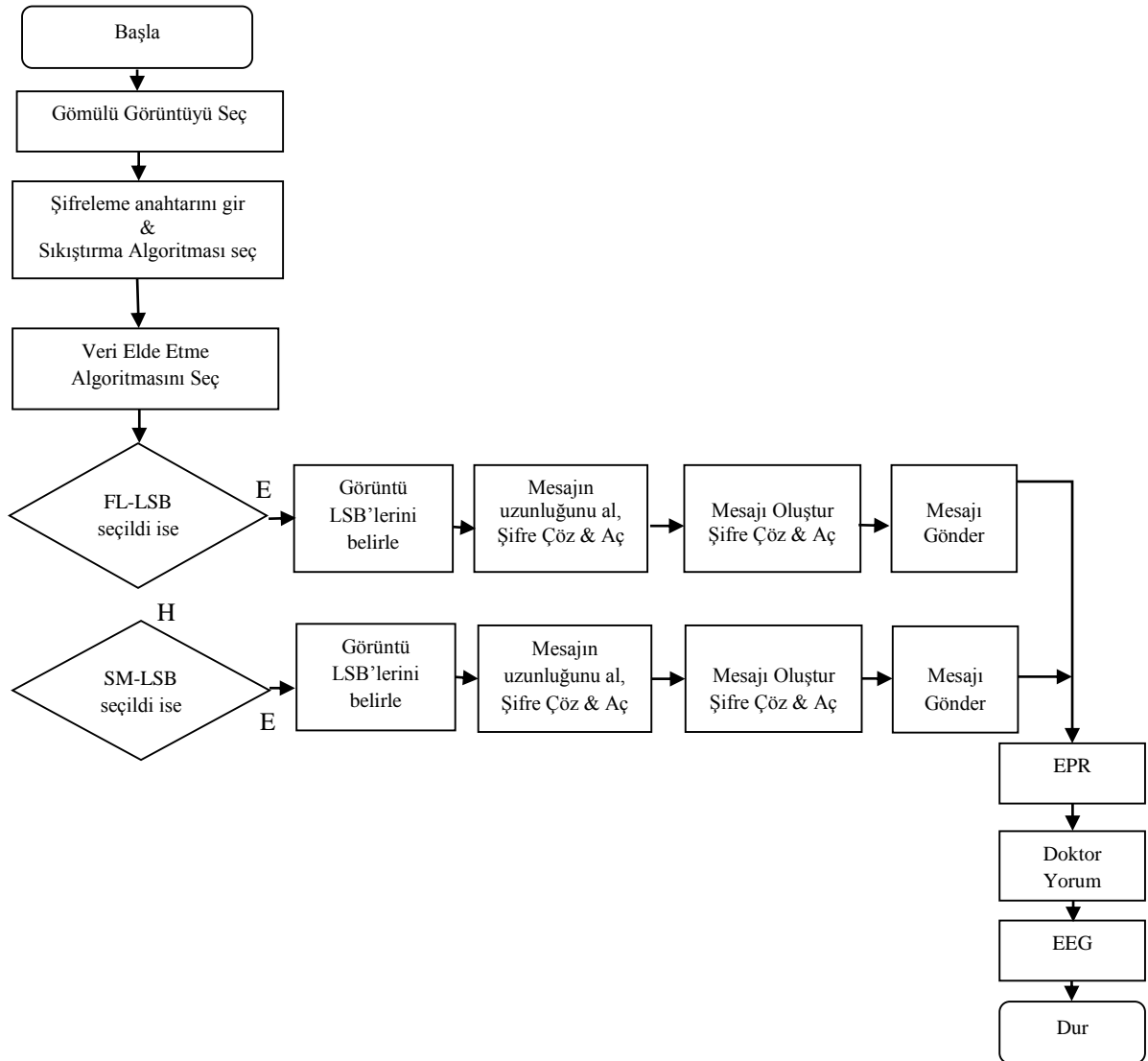
Şekil 3.3. Mesaj gizleme aşamasının akış diyagramı

### Mesaj elde etme aşaması

Mesaj elde etme aşaması Şekil 3.4'de verilen bloklar ile açıklanmaktadır. Burada, Şekil 3.1'de mesaj gizleme aşamalarının tersi bir durum meydana gelmektedir. Mesajı elde etmek için gömülü DICOM görüntüleri ve şifreli mesajı çözmek için stego-anahtar (oturum anahtarı) gerekmektedir. Öncelikle, önerilen yöntemler ile mesajın gizlendiği piksel koordinatları elde edilmektedir. Ardından her görüntü için bu piksellerin LSB'leri kullanılarak mesaj bir araya getirilmektedir. Mesajın içinden hasta kişisel bilgileri, bölütlenen EEG ve doktor yorumu ayırt edilerek grafik ara yüz (Graphical User Interface-GUI) penceresine aktarılmaktadır. Ayrıca, gizlenen EEG verisi tüm DICOM serisindeki görüntülerden bir araya getirilebilmektedir. Mesajı elde etme işleminin detayı ise Şekil 3.5'de verilen akış diyagramı ile anlatılmaktadır.



Şekil 3.4. Önerilen yöntemler için gizlenen mesajı elde etme blokları



Şekil 3.5. Mesajı elde etme aşamasının akış şeması

Bu tez çalışmasında, mesaj gizlemek için kullanılan taşıyıcı MR görüntüleri ile mesaj gizlendikten sonra oluşturulan gömülü MR görüntüleri arasındaki karşılaştırmalar için hataların karelerinin ortalaması (Mean square error-MSE), sinyalin tepe değerinin gürültüye oranı (Peak signal to noise ratio-PSNR), evrensel kalite indeksi (Universal Image Quality Index-UQI), yapısal benzerlik (Structural Similarity-SSIM) ve korelasyon katsayısı (R) değerleri kullanılmıştır. Bu tekniklerin uygulanması ile elde edilen istatistiksel analiz sonuçlarını karşılaştırmak suretiyle yorumlar yapılmıştır.

Aşağıdaki başlıklarda önerilen yöntemlerin ayrıntıları verilmiştir ve karşılaştırma için kullanılan yöntemler ile ilgili bilgiler sunulmuştur.

### **3.1. Medikal Görüntü Steganografi için Önerilen Yöntemler**

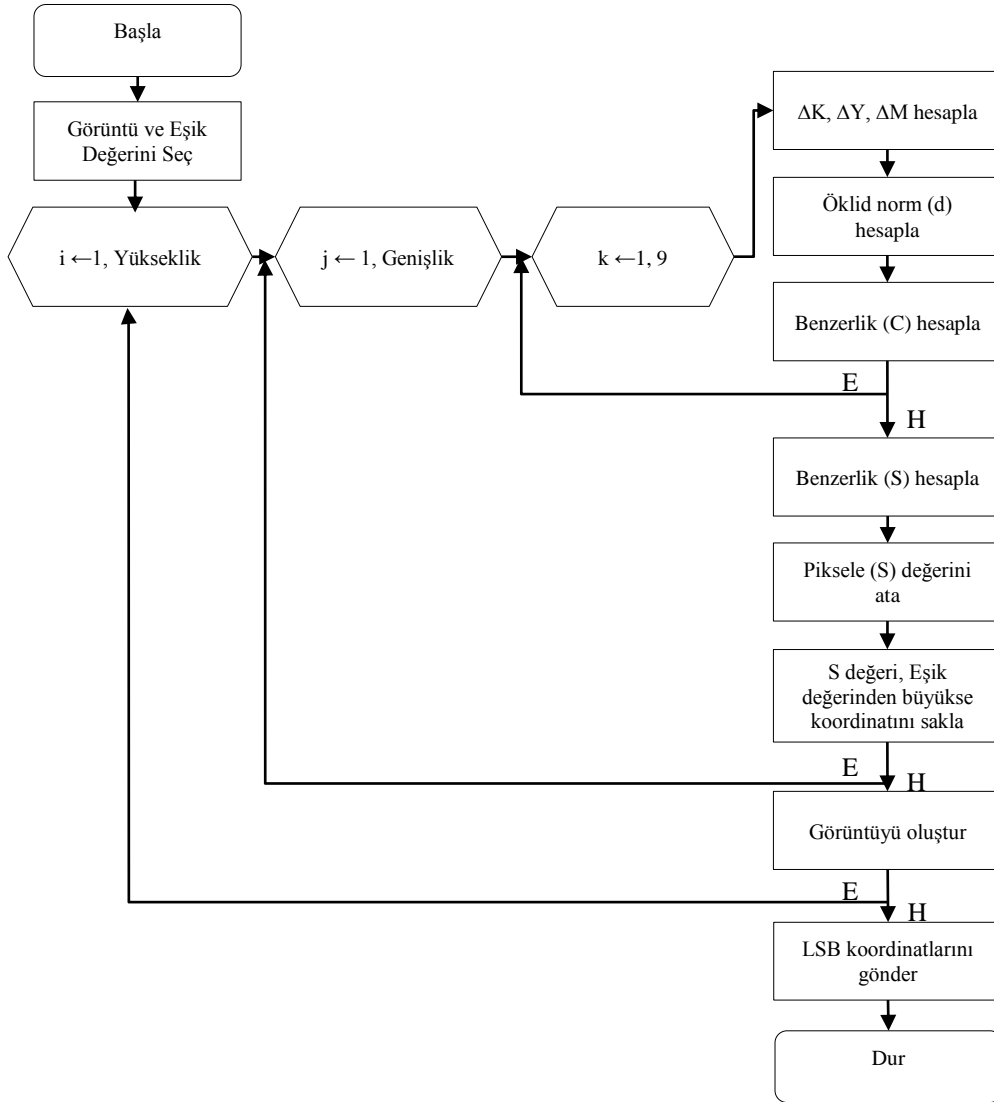
Bu tez çalışmasında, medikal görüntü steganografi için benzerlik tabanlı ve bulanık mantık tabanlı iki yeni algoritma önerilmektedir.

#### **3.1.1. Benzerlik-tabanlı LSB (SM-LSB) algoritması**

Sayısal bir görüntü pikseller ile örneklenir. Gri-ölçekli görüntülerde, pikseller gri seviye yoğunluğa sahiptir. Renkli görüntülerde ise pikseller üç renk bileşeni (kırmızı, yeşil ve mavi) ya da dört renk bileşeni (cyan, eflatun, sarı ve siyah) ile oluşturulmaktadır [122]. Benzerlik iki grup ya da nesne arasındaki benzerlik derecesi ile belirlenmektedir.

Görüntü işlemede, iki piksel arasındaki benzerlik ölçümü Öklid uzaklığı kullanılarak belirlenmektedir [123-125]. Demirci kenar tespiti için benzerlik tabanlı bir yöntem önermiştir [123]. Ayrıca, literatürde görüntü histogramı üzerinde komşu piksel farkına (Pixel Value Differencing-PVD) göre belirlenen piksellerde mesaj gizlenmiştir. Bu yöntemlerde pikseller arasındaki uzaklık yerine farkları alınarak (Örneğin; fark sıfır olan piksellere) veri gizlenmektedir. Bu yöntemlerdeki en dikkat çekici özellik, yüksek mesaj gizleme kapasitelerinin olması ve yüksek PSNR değerleri elde etmiş olmalarıdır [16, 126, 127]. Bu sebeplerle, bu tez çalışması literatürdeki çalışmalardan farklı olarak gömme kapasitesini artırmak için görüntünün histogramını kullanmadan, görüntüdeki her pikselin komşu piksellerinin gri seviye farkına dayalı yeni bir benzerlik-tabanlı LSB (SM-LSB) algoritması önermektedir.

Önerilen algoritmanın en temel fikri, piksel değerleri  $[0 \ 1]$  aralığında gerçel sayılardan oluşan yeni bir görüntü oluşturmaktır. SM-LSB yönteminin akış diyagramı Şekil 3.6'da verilmiştir. Şekil 3.6'dan görüldüğü gibi, her pikselin  $3 \times 3$  pencerede komşularıyla Öklid uzaklığı ve benzerliği hesaplanmaktadır. Ardından lokal benzerlik değerleri bulunarak, görüntüye piksel değeri olarak atanmaktadır. Yöntemde, elde edilen yeni görüntünün gerçel değerleri eğer belli bir eşik değerinin ( $T_h$ ) üzerinde ise mesaj gizlemek için seçilmektedir.



Şekil 3.6. Benzerlik-Tabanlı LSB (SM-LSB) yönteminin akış şeması

SM-LSB algoritması, MR görüntünün her pikselinin  $3 \times 3$  pencerede komşu piksellerinin bulunmasını sağlar. Şekil 3.7'de, görüntü piksellerinin  $3 \times 3$  penceredeki komşulukları görülmektedir. Şekil 3.7'de görülen  $P_1, P_2, \dots, P_9$  üç renk bileşenine (R, G, B) sahip görüntü piksellerini ifade etmektedir. Örneğin  $P_{1(K_1, Y_1, M_1)}$  şeklinde ifade edilmektedir.

P1	P2	P3
P4	<b>P9</b>	P5
P6	P7	P8

Şekil 3.7. Görüntünün 3x3 komşu pikselleri

Şekil 3.6'da verilen akış semasından görüldüğü gibi, yöntemin ilk aşamasında görüntünün pikselleri arasındaki farklılıklar hesaplanmıştır ve bu farklılıklar pikseller arasındaki uzaklığın hesaplanması için kullanılmıştır. Bu sebeple, öncelikle Eş. 3.1'de görüntüdeki komşu piksellerin her renk bileşeni için gri seviye değer farkları elde edilmiştir.

$$\begin{aligned}
 \Delta K &= |P_{1(K_1)} - P_{2(K_2)}| \\
 \Delta Y &= |P_{1(Y_1)} - P_{2(Y_2)}| \\
 \Delta M &= |P_{1(M_1)} - P_{2(M_2)}|
 \end{aligned} \tag{3.1}$$

Eş. 3.1'de görüldüğü gibi, K: kırmızı, Y: yeşil ve M: mavi olarak ifade edilmiştir. Eş. 3.1 ile iki piksel arasındaki renk farkları kullanılarak piksellerin gri seviye farklarının Öklid uzaklığı hesaplanmıştır. Eş. 3.2'de Öklid norm verilmiştir [16, 123-125].

$$d_{i,j} = \frac{1}{\sqrt{3}} (\Delta K^2 + \Delta Y^2 + \Delta M^2) \tag{3.2}$$

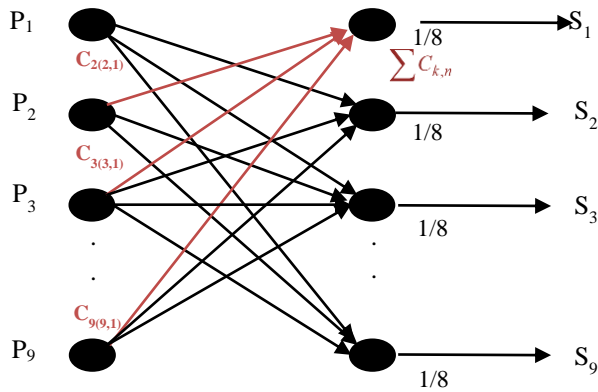
İkinci aşamada, iki piksel arasındaki benzerlik Eş. 3.2 ve Eş. 3.3'e göre hesaplanmıştır. Literatürde, pikseller arası benzerlik; üssel ya da Gauss fonksiyonu kullanılarak belirlenebilmektedir [123-125]. Bu sebeple çalışmada, piksel benzerliği Eş. 3.3 üssel fonksiyonu ile hesaplanmıştır. Gauss fonksiyonu, mesajın geri elde edilmesini sağlayamadığından, çalışmada üssel fonksiyon tercih edilmiştir.

$$C_k(x_i, x_j) = \exp\left(\frac{-d_{ij}^q}{D_n}\right) \tag{3.3}$$

Eş. 3.3’de geçen  $D_n$  normalizasyon katsayısıdır.  $D_n$  değeri tez çalışmasında deneme yanılma yolu ile belirlenmiştir ve 128 olarak atanmıştır [16]. Bu değer gizli mesajın geri getirilmesinde başarılı olduğu için seçilmiştir. Eş. 3.3’de geçen  $C_k$  değeri ise piksellerin 3x3 pencerede hesaplanan benzerlik değerleridir.

Algoritmada üçüncü aşamada, piksellerin yerel benzerlik değerleri hesaplanmıştır. Her pikselin komşu piksellere göre hesaplanan benzerlik değerleri Eş. 3.4’de görüldüğü gibi önce toplanmış ve sonrasında bölme işlemi ile normalize edilmiştir. Şekil 3.8’de, SM-LSB algoritması ile piksel değerlerinin benzerlik değerlerine dönüştürülme aşamaları gösterilmektedir. Burada, 3x3 pencerede görüntünün piksel değerleri ( $P_1, P_2, \dots, P_9$ ) SM-LSB algoritmasının girişlerini oluşturmaktadır. Eş. 3.3 ile pikseller arasındaki benzerlik hesaplanmaktadır. Eş. 3.4 ile de piksellerin lokal benzerlik değerleri ( $S_1, S_2, \dots, S_9$ ) elde edilmektedir. Bu lokal benzerlik değerleri ise yeni görüntünün piksel değerlerini oluşturmaktadır. Demirci geliştirdiği yöntemde elde ettiği benzerlik değerlerini 0-255 arasındaki piksel değerlerine dönüştürmüştür, elde ettiği bu görüntüde ise kenarların tespitini sağlamıştır [123]. Bu tez çalışmasında ise benzerlik değerleri bu çalışmadan farklı olarak gerçel sayılar halinde tutulmuştur.

$$S_k = \frac{1}{8} \sum_{n=1}^9 C_{k,n} \quad \text{for } k \neq n \quad (3.4)$$



Şekil 3.8. 3x3 pencerede komşu piksellerin benzerlik matrisi

Yöntemin son aşamasında, görüntünün benzerlik değerleri, eğer belli bir eşik değerinin üzerinde ise mesaj gizlemek için seçilmiştir ve bu seçilen değerlerin koordinatları bir matris içinde tutulmuştur. Çalışmada  $T_h=0,5$  olarak atanmıştır. Bu değer deneme yanılma yolu ile tespit edilmiştir. Algoritma mesaj elde etme aşamasında da aynı şekilde çalışmaktadır. Yöntemin veriyi geri elde edilmesi için aynı eşik değerinin seçilmesi gerekmektedir. Öncelikle, gömülü görüntüler geliştirilen programın GUI'sinden seçilmektedir ve görüntülerin benzerlik değerleri elde edilmektedir. Eşik değerinin üzerinde olan benzerlik değerleri kullanılarak gizli mesaj, bu piksellerin LSB'lerinden açığa çıkarılmaktadır ve bir araya getirilmektedir.

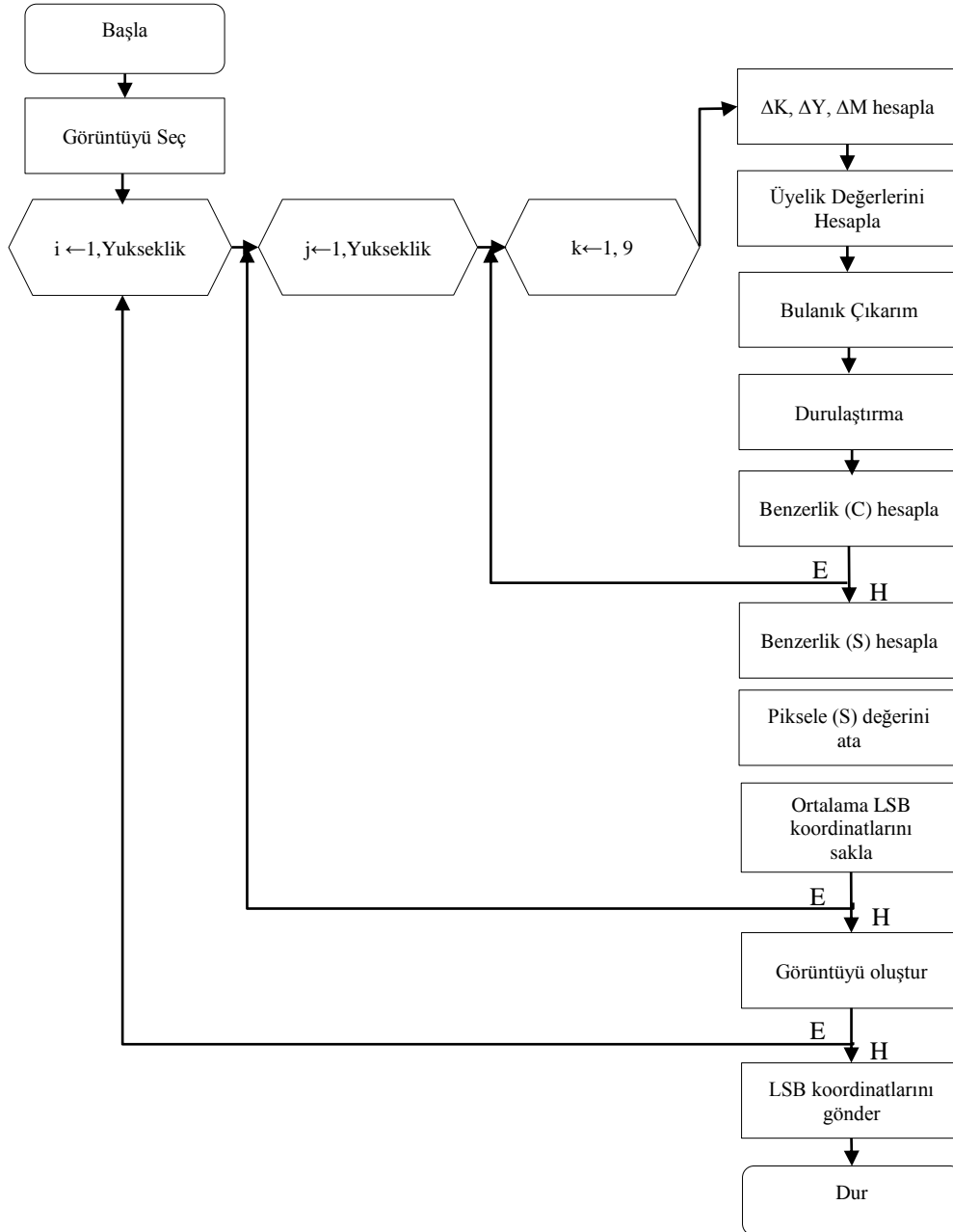
### 3.1.2. Bulanık mantık-tabanlı LSB (FL-LSB) yöntemi

Görüntü işlemede, Öklid normu piksellerin arasındaki uzaklığı hesaplamak için kullanılmaktadır. Ancak literatürdeki çalışmalar, algısal renk yakınsaklığının Öklid uzaklığı ile belirlenemeyeceğini ve kural tabanlı yaklaşımlar ile bu problemin aşılacağını göstermiştir. Literatürde kural tabanlı yaklaşımlar renkli görüntü bölütleme ve filtrelemede kullanılmıştır [19, 123-125, 128, 129]. Bu sebeplerle, bu tez çalışmasında bulanık mantık-tabanlı LSB (FL-LSB) algoritması mesaj gizlemek için görüntü piksellerinin LSB'lerini seçmiştir. Geliştirilen yöntemin SM-LSB yönteminden en önemli farkı adaptif olarak çalışması, kullanıcı tarafından belirlenecek bir eşik değerine ihtiyaç duymamasıdır. Şekil 3.9'da FL-LSB yönteminin akış diyagramı verilmiştir. Şekil 3.9'da görüldüğü gibi her bir pikselin komşularına göre gri seviye farklılıkları önce bulandırılmış, bulanık çıkarım işleminin ardından durularak benzerlik değerleri elde edilmiştir. Ardından bu değerlerden lokal benzerlik değerleri hesaplanarak görüntünün piksel değeri olarak atanmıştır.

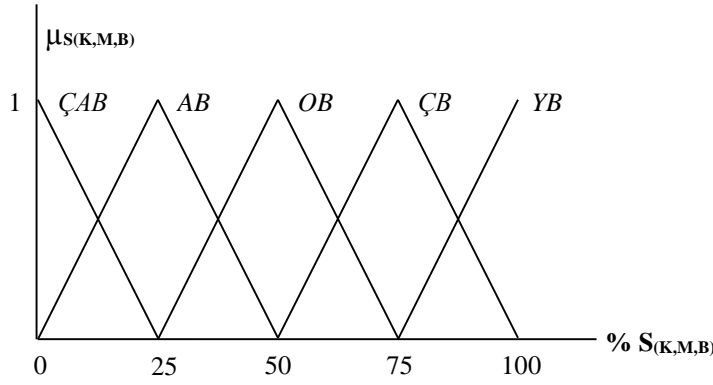
İlk aşamada, 3x3 pencerede piksellerin gri seviye farkı hesaplanmıştır. Bu işlem Eş. 3.1 kullanılarak her renk bileşeni için gerçekleştirilmiştir. FL-LSB algoritmasında, SM-LSB'den farklı olarak benzerlik değerlerini hesaplamak için Öklid norm kullanılmamıştır. Elde edilen gri seviye fark değerleri FL-LSB yönteminin bulanık kümelerinin girişlerini oluşturmuştur. Çalışmada, bu gri seviye fark değerleri ( $\Delta K$ ,  $\Delta Y$  ve  $\Delta M$ ) 3 dilsel tanımlama ile ifade edilmiştir. Bunlar: Sıfır: ZE; Orta: MD ve Büyük: LR şeklindedir [19]. Şekil 3.10'da görüldüğü gibi bulanıklaştırma işlemi tüm renk bileşenleri için gerçekleştirilmektedir. Çetin ve arkadaşları [124] geliştirdikleri kural tabanlı filtrede 7 bulanık küme kullanmışlardır.



Bu çalışmada ise 7 bulanık küme işlem maliyetini artırmamak için tercih edilmemiştir, 3 bulanık küme kullanıldığında ise elde edilen benzerlik değerleri görüntü içinde hep aynı olmuştur ve bu sebeple aynı pikseller seçilmiştir [19].



Şekil 3.9. Bulanık Mantık-Tabanlı LSB (FL-LSB) yönteminin akış diyagramı



Şekil 3.10. Komşu piksellerin renk bileşenlerinin bulanıklaştırılması için tanımlanan bulanık üçgen kümeler (ÇAB: Çok Az Benzer, AB: Az Benzer, OB: Orta Benzer, ÇB: Çok Benzer ve YB: Yüksek Benzer).

Çalışmada, görüntüdeki komşu piksellerin, renk bileşenlerinin gri seviye değerlerine göre benzerliklerini ifade etmek için, 5 üçgen bulanık küme tanımlanmıştır. Bunlar: *Çok Az Benzer (ÇAB)*, *Az Benzer (AB)*, *Orta Benzer (OB)*, *Çok Benzer (ÇB)*, *Yüksek Benzer (YB)* şeklindedir.

Üçüncü aşamada, bulanık çıkarım işlemi gerçekleştirilmiştir. Bunun için oluşturulan kural tabanı aşağıdaki gibidir [19, 124]. Çalışmada toplam 27 kural oluşturulmuştur. Bu kurallar aşağıda verilmiştir.

Kural 1: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Sıfır}$  ise  $P_1$  ve  $P_2$  *Yüksek Benzer*'dir.

Kural 2: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Orta}$  ise  $P_1$  ve  $P_2$  *Yüksek Benzer*'dir.

Kural 3: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Büyük}$  ise  $P_1$  ve  $P_2$  *Çok Benzer*'dir

Kural 4: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Orta}$  ve  $\Delta M = \text{Sıfır}$  ise  $P_1$  ve  $P_2$  *Yüksek Benzer*'dir

Kural 5: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Orta}$  ve  $\Delta M = \text{Orta}$  ise  $P_1$  ve  $P_2$  *Çok Benzer*'dir

Kural 6: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Orta}$  ve  $\Delta M = \text{Büyük}$  ise  $P_1$  ve  $P_2$  *Orta Benzer*'dir

Kural 7: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Büyük}$  ve  $\Delta M = \text{Sıfır}$  ise  $P_1$  ve  $P_2$  *Çok Benzer*'dir

Kural 8: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Büyük}$  ve  $\Delta M = \text{Orta}$  ise  $P_1$  ve  $P_2$  *Orta Benzer*'dir

Kural 9: Eğer  $\Delta K = \text{Sıfır}$  ve  $\Delta Y = \text{Büyük}$  ve  $\Delta M = \text{Büyük}$  ise  $P_1$  ve  $P_2$  *Az Benzer*'dir

Kural 10: Eğer  $\Delta K = \text{Orta}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Sıfır}$  ise  $P_1$  ve  $P_2$  *Yüksek Benzer*'dir

Kural 11: Eğer  $\Delta K = \text{Orta}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Orta}$  ise  $P_1$  ve  $P_2$  *Çok Benzer*'dir

Kural 12: Eğer  $\Delta K = \text{Orta}$  ve  $\Delta Y = \text{Sıfır}$  ve  $\Delta M = \text{Büyük}$  ise  $P_1$  ve  $P_2$  *Orta Benzer*'dir

- Kural 13: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Orta$  ve  $\Delta M = Sıfır$  ise  $P_1$  ve  $P_2$  Çok Benzer'dir
- Kural 14: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Orta$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Orta Benzer'dir
- Kural 15: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Orta$  ve  $\Delta M = Büyük$  ise  $P_1$  ve  $P_2$  Az Benzer'dir
- Kural 16: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Sıfır$  ise  $P_1$  ve  $P_2$  Orta Benzer'dir
- Kural 17: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Az Benzer'dir
- Kural 18: Eğer  $\Delta K = Orta$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Büyük$  ise  $P_1$  ve  $P_2$  Çok Az Benzer'dir
- Kural 19: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Çok Benzer'dir
- Kural 20: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Orta Benzer'dir
- Kural 21: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Az Benzer'dir
- Kural 22: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Orta Benzer'dir
- Kural 23: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Az Benzer'dir
- Kural 24: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Sıfır$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Çok Az Benzer'dir
- Kural 25: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Sıfır$  ise  $P_1$  ve  $P_2$  Az Benzer'dir
- Kural 26: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Orta$  ise  $P_1$  ve  $P_2$  Çok Az Benzer'dir
- Kural 27: Eğer  $\Delta K = Büyük$  ve  $\Delta Y = Büyük$  ve  $\Delta M = Büyük$  ise  $P_1$  ve  $P_2$  Çok Az Benzer'dir

Dördüncü aşamada, komşu piksellerin benzerlik yüzdeleri ağırlık merkezi yöntemi ve çarpım ile Eş. 3.5 kullanılarak hesaplanmıştır [124].

$$C = \frac{\sum_{j=1}^Z S_j \mu_{prem}^j(L)}{\sum_{j=1}^Z \mu_{prem}^j(L)} \quad (3.5)$$

Eş. 3.5 deki  $S_j$ : j. kuralda elde edilen benzerlik yüzdesinin orta değeri ve Z ise toplam kural sayısıdır.  $\mu_{prem}^j(L)$  ise Eş. 3.6 kullanılarak hesaplanmaktadır [124].

$$\mu_{prem}^j(L) = \mu_K^j(\Delta K) \mu_Y^j(\Delta Y) \mu_M^j(\Delta M) \quad (3.6)$$

Beşinci aşamada, 3x3 pencerede bulanık mantık tarafından hesaplanan benzerlik değerleri Eş. 3.4 kullanılarak tüm komşu değerler için toplanmış ve normalize edilerek ağırlıklı ortalamaları hesaplanmıştır. Elde edilen yeni gerçel değerler ise yeni görüntünün piksel değeri olarak atanmıştır. 3x3 pencerede bu benzer değerlerin orta değeri ise mesaj gizlenecek LSB olarak seçilmiştir. FL-LSB yönteminde de, SM-LSB yönteminde olduğu gibi gizleme yapılacak LSB'lerin koordinatlarını içeren bir matris oluşturulmaktadır. Son olarak mesaj bitleri ile bu matriste yer alan piksellerin LSB'leri ile yer değiştirilmektedir. Veri elde etme aşamasında, gömülü görüntüler üzerinde aynı işlemler uygulanmaktadır, elde edilen koordinat matrisinde yer alan piksellerden mesaj bitleri çıkarılmaktadır ve mesaj bu bitlerden tekrar bir araya getirilmektedir.

### 3.2. Karşılaştırma Yöntemleri

Bu tez çalışmasında, taşıyıcı ve gömülü görüntüler 5 farklı yöntem ile analiz edilmiştir. Hataların kareleri ortalaması olan MSE fonksiyonu Eş. 3.7'de verilmiştir [110].

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (f(x_i, y_j) - g(x_i, y_j))^2 \quad (3.7)$$

Eş. 3.7'deki  $f(x,y)$  ve  $g(x,y)$  sırasıyla taşıyıcı ve gömülü görüntülerini sembolize etmektedir.  $M$  ve  $N$  ifadeleri ise görüntünün boyutlarını göstermektedir. Sinyalin tepe değerinin gürültüye oranı olan PSNR fonksiyonu Eş. 3.8'de verilmiştir [110].

$$PSNR = 10 \log \left( \frac{255 \times 255}{MSE} \right) \quad (3.8)$$

MSE ve PSNR değerleri, insan görme sistemini (Human Visual System-HVS) ifade edememektedir. Bu sebeplerle HVS dikkate alınarak geliştirilen evrensel kalite indeksi (Universal Image Quality Index-UQI) ve yapısal benzerlik (Structural Similarity-SSIM) teknikleri de kullanılarak, görüntüler arasındaki ilişki ortaya konulmuştur [130, 131]. SSIM ve UQI değerleri Eş. 3.9 ve Eş. 3.10'da verilmiştir. UQI; görüntüdeki korelasyonun azalmasını, parlaklık ve kontrast bozulmalarını değerlendirmektedir. SSIM ise yapısal bilgideki azalmaları ortaya koymaktadır. Bu sebeple SSIM ve UQI karşılaştırmaları MSE ve PSNR'ye göre karşılaştırmalarda daha iyi sonuçlar vermektedir.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (3.9)$$

$$UQI(x, y) = \frac{(4\mu_x\mu_y 2\sigma_{xy})}{(\mu_x^2 + \mu_y^2)(\sigma_x^2 + \sigma_y^2)} \quad (3.10)$$

Eş. 3.9 ve Eş. 3.10'da,  $\mu_x$  :  $X$ 'in ortalaması,  $\mu_y$  :  $Y$ 'nin ortalaması,  $\sigma_x$  :  $X$ 'in varyansı,  $\sigma_y^2$  :  $Y$ 'nin varyansı,  $\sigma_{xy}$  :  $X$  ve  $Y$ 'nin kovaryansını ifade etmektedir.  $c_1 = (k_1L)^2$  ve  $c_2 = (k_2L)^2$  bölme işleminde paydayı dengede tutmak için kullanılır.  $k_1$  ve  $k_2$  'nin varsayılan değerleri 0,01 ve 0,03'dür.  $L$  ise piksel değerlerinin arasındaki dinamik aralıktır [130, 131].

Korelasyon katsayısı ( $R$ ) görüntü karşılaştırma iki görüntüyü karşılaştırır ve Eş. 3.11 kullanılarak hesaplanır [132].

$$R = \frac{\sum \sum (f_{MN} - \bar{f}) - (g_{MN} - \bar{g})}{\sqrt{\left( \sum \sum (f_{MN} - \bar{f})^2 \right) \left( \sum \sum (g_{MN} - \bar{g})^2 \right)}} \quad (3.11)$$

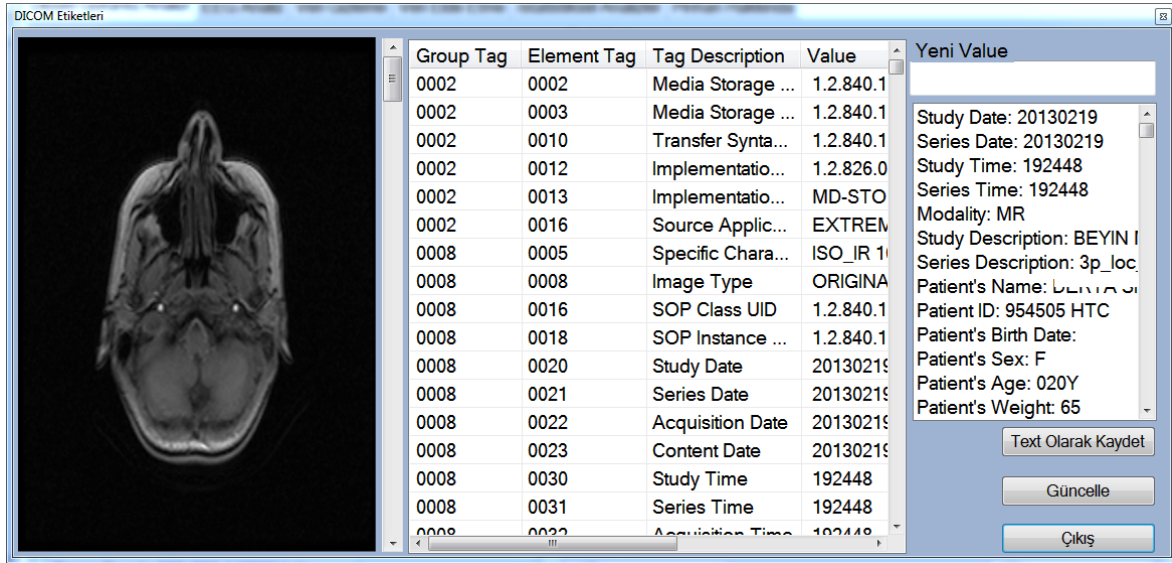
Eş. 3.11'deki  $\bar{f}$  taşıyıcı görüntü piksellerinin ortalaması ve  $\bar{g}$  ise gömülü görüntü piksellerinin ortalamasıdır.

Ayrıca çalışmada frekans düzleminde taşıyıcı ve gömülü görüntülerin 8x8 pencerede DCT katsayılarına göre karşılaştırılmasını sağlayan insan görme Sistemine göre düzenlenmiş sinyalin tepe değerinin gürültüye oranı (Peak Signal to Noise Ratio-Human Visual System-PSNR-HVS) ve insan görme sistemine göre düzenlenmiş sinyalin tepe değerinin gürültüye oranı (Modified Peak Signal to Noise Ratio-Human Visual System-PSNR-HVSM) yöntemleri de kullanılmıştır. Yöntemlerin detaylarına kaynaklardan ulaşılabilir [133, 134].

#### 4. BULGULAR VE TARTIŞMA

Bu bölümde, bu tez çalışmasında önerilen yöntemlerin Çizelge 2.2’de ayrıntıları verilen Gazi Üniversitesi Nöroloji Bölümü’nden toplanılan verilerle test edilmesi ile elde edilen sonuçlar verilmiştir. Tez çalışması kapsamında Visual Studio .NET 2010 platformu kullanılarak geliştirilen DicomPinhan adlı programın pencereleri aşağıda görülmektedir.

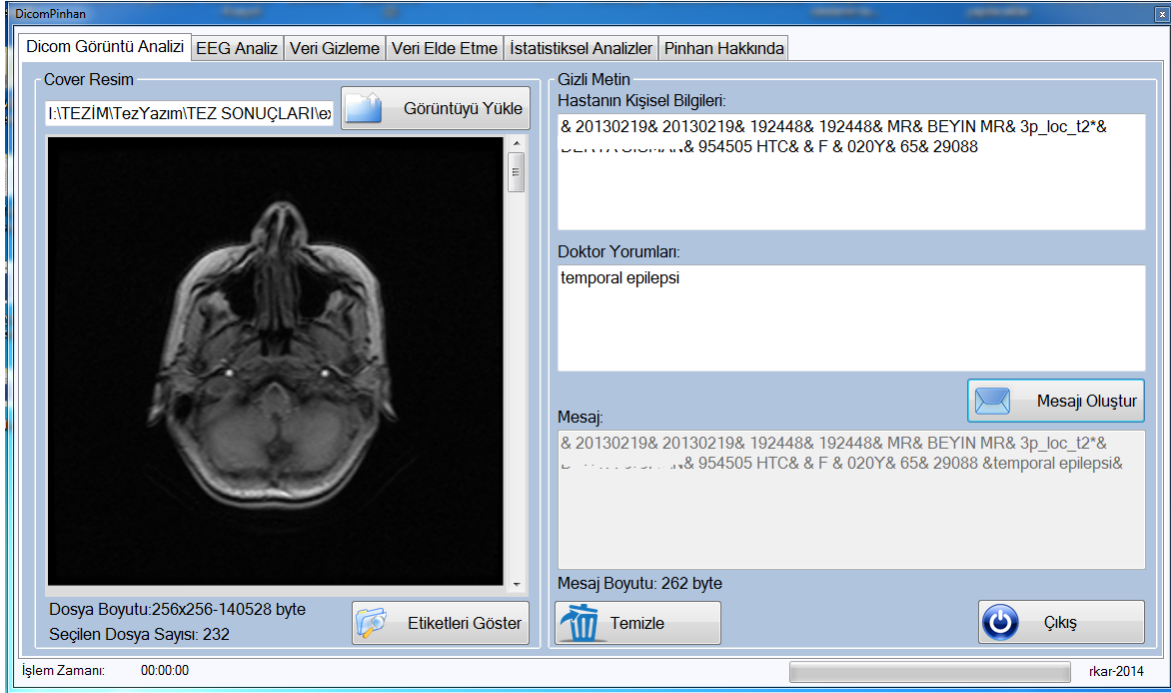
Şekil 4.1’de görülen program penceresi ile hastaya ait DICOM serisi yüklendikten sonra, dosya başlık kısmında yer alan tüm bilgiler görüntülenmektedir ve güncellenebilmektedir. Bu pencere aracılığıyla hastanın kişisel bilgileri elde edilmektedir. Çalışma kapsamında hasta kişisel bilgileri: hastanın adı, verilen numarası, hasta doğum tarihi, cinsiyeti, yaşı, ağırlığı ve adresi, çekim tarihi, saati, numarası, görüntünün yapısı ve tanımı, serinin tarihi, saati ve tanımı şeklindedir. Şekil 4.1’deki pencereden istenirse mevcut kişisel bilgiler değiştirilebilmektedir. Ancak çalışma için hastaların mevcut bilgileriyle analiz yapılmıştır.



Şekil 4.1. DICOM serisinden kişisel bilgilerin seçilmesini sağlayan pencere

Şekil 4.2’de hastanın DICOM görüntülerinin seçildiği ve doktor yorumunun ara yüzden girilmesinin sağlandığı pencere görülmektedir. DICOM dosyalarının başlık kısmının görüntülenmesi için “Etiketleri Göster” butonu kullanılmaktadır. Aynı zamanda görüntü yüklenirken gömülü görüntülerin kayıt edilmesi için gereken yol da seçilmektedir.

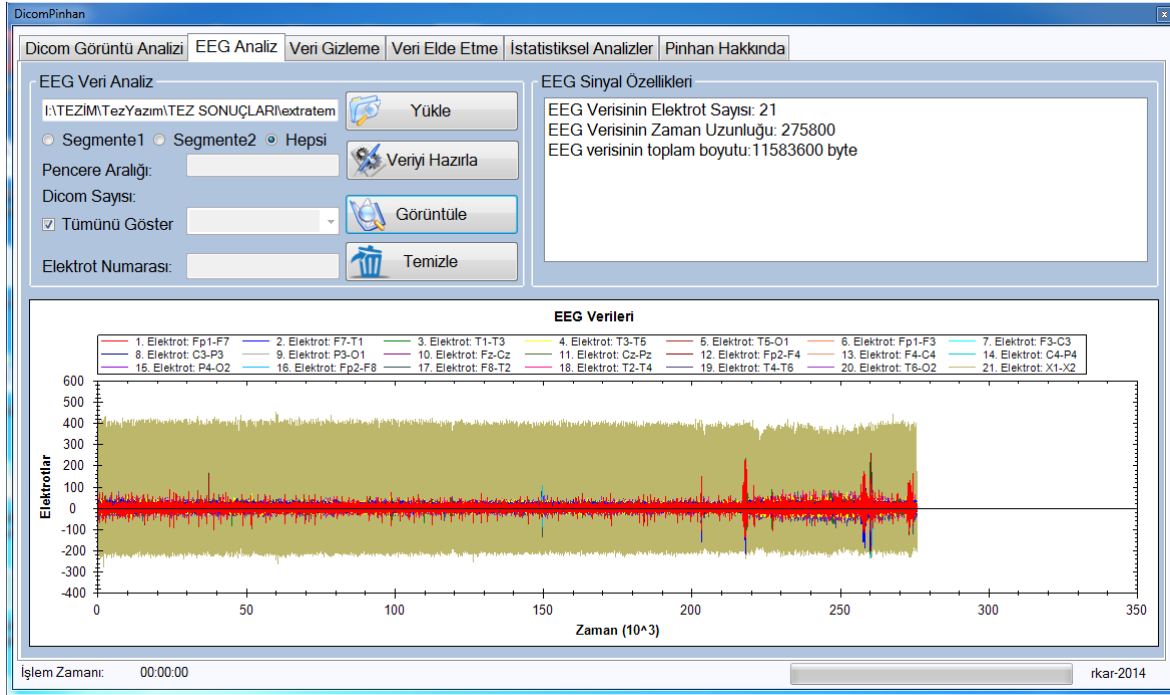
Çalışmada EEG verisi olmaksızın da kişisel bilgiler ve doktor yorumundan oluşan mesaj gizlenilmektedir ve ilk mesajın oluşturulması sağlanmaktadır. Oluşturulan bu ilk mesajın boyut bilgisi de Şekil 4.2’deki pencereden görülebilmektedir.



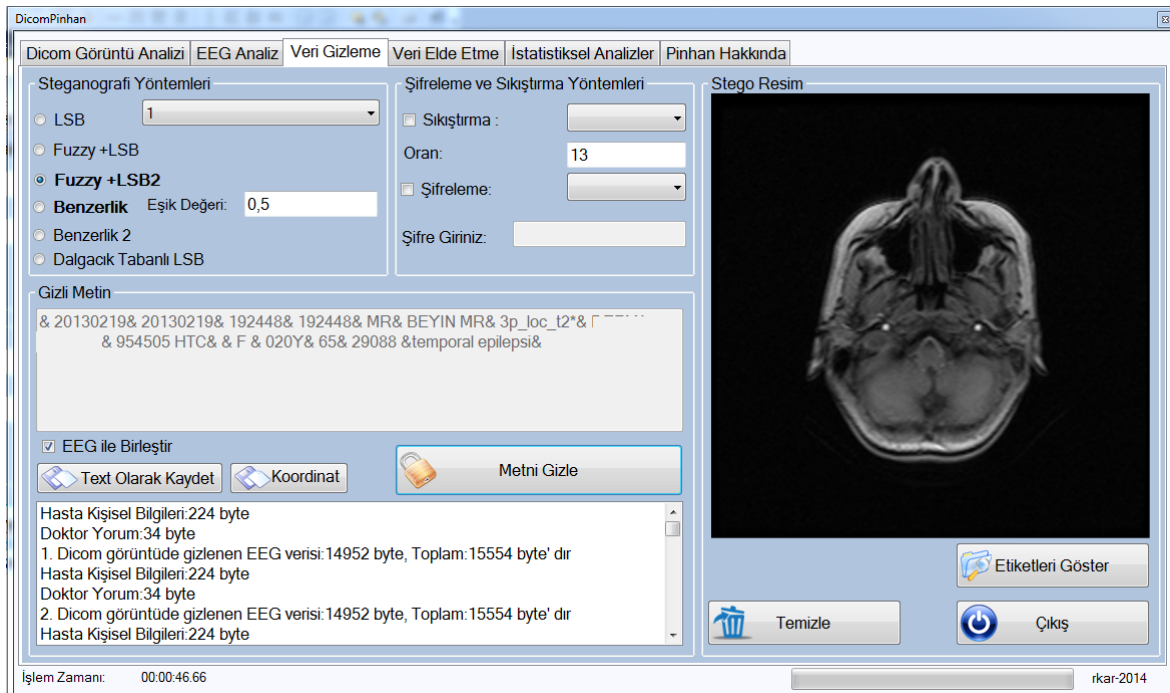
Şekil 4.2. Hastaya ait DICOM serisinin yüklenilmesini sağlayan pencere

Şekil 4.3’de verilen pencere ile hastaya ait EEG dosyasının sisteme yüklenmesi ve dosyaya ait başlık bilgilerinin elde edilmesi sağlanmaktadır. Aynı zamanda, pencereden EEG verisi toplu olarak ya da her bir elektrot için ayrı olarak görüntülenmektedir. DICOM görüntüsünden elde edilen kişisel bilgiler, doktor yorumu ve EEG verisi birleştirilerek gizlenecek mesaj oluşturulmaktadır. Mesaj oluşturmak için yapılanlar 3. Bölüm’de, Şekil 3.1 ve Şekil 3.2’de verilmiştir.

Şekil 4.4’te verilen pencereden öncelikle mesajın EEG’li ya da EEG’siz olarak oluşturulması sağlanmaktadır. Veri gizlemek için geliştirilen pencereden gizleme yöntemi, sıkıştırma algoritması ve şifreleme algoritması seçilmektedir. Şifreleme için gereken anahtar da girilmektedir.



Şekil 4.3. Hastanın EEG verisinin yüklenilmesini sağlayan pencere



Şekil 4.4. Oluşturulan mesajın DICOM serisine gizlenmesini sağlayan pencere

Şekil 4.5'te verilen pencere ile gizlenen mesajın elde edilmesi ve görüntülenmesi sağlanmaktadır. Gömülü görüntülerin, gizlemede kullanılan yöntemin, sıkıştırma ve şifreleme algoritmalarının öncelikle seçilmesi gerekmektedir. Şifreleme için girilen anahtar girişi de yapılmalıdır. Geliştirilen yöntem mesajı ekrana aktarmaktadır. Mesaj alındıktan

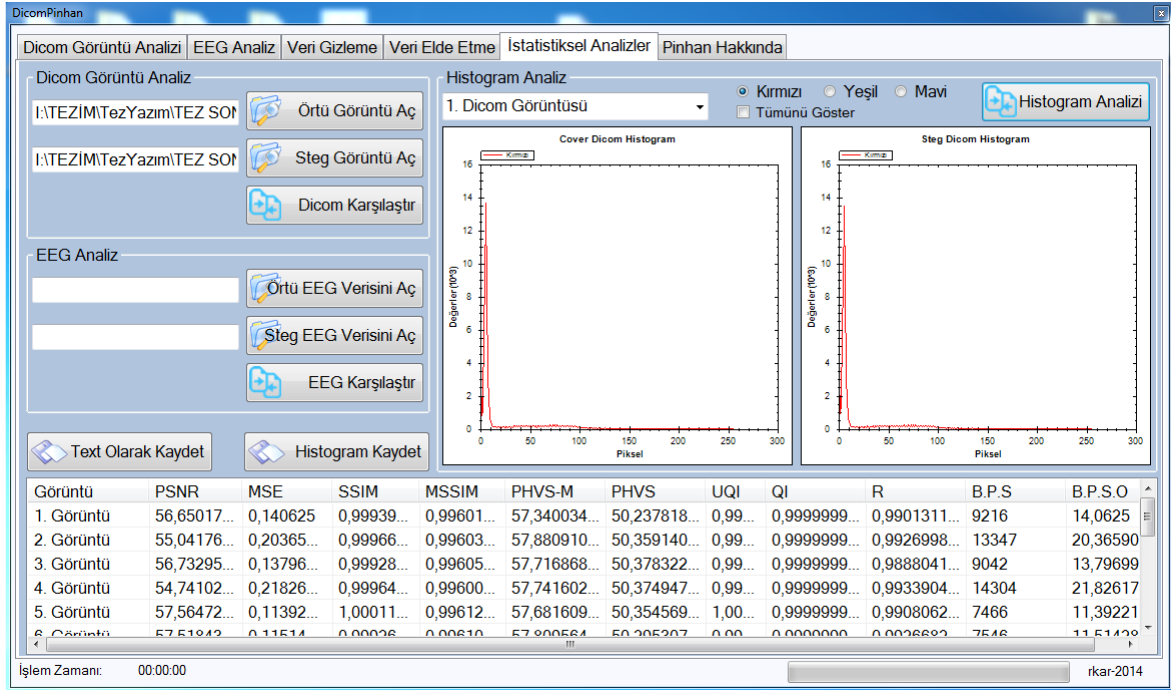


sonra kişisel bilgiler, doktor yorum ve EEG verileri ayrıştırılmaktadır. Her görüntüde gizlenen EEG verisi ayrı ayrı ya da toplu olarak görüntülenmektedir.



Şekil 4.5. Gizlenen mesajın elde edilmesi ve görüntülenmesini sağlayan pencere

Şekil 4.6'daki pencere ile taşıyıcı ve gömülü görüntülerin karşılaştırılması sağlanmaktadır. Bu pencereden görüntüler arasındaki MSE, PSNR, SSIM, UQI ve R değerleri liste halinde görülebilmektedir ve kayıt edilebilmektedir. Ayrıca görüntülerin her renk bileşeni için normalize histogramları da incelenebilmektedir.



Şekil 4.6. Taşıyıcı ve gömülü görüntülerin karşılaştırılmasını sağlayan pencere

#### 4.1. Önerilen Yöntemlerle Elde Edilen Sonuçlar

Şekil 4.7’de 256x256 ve 512x512 boyutlu MR taşıyıcı görüntüler ve önerilen FL-LSB ve SM-LSB yöntemleri ile elde edilen gömülü görüntüler verilmiştir. Şekil 4.7’den de görüldüğü gibi, gömülü görüntülerde veri gizleme sonrasında gözle görülür bir farklılık bulunmamaktadır. Gömülü görüntüler herhangi bir DICOM görüntüleyici ile görüntülendiklerinde hastaya ait kişisel bilgiler görülmemelidir. Bu sebeple, Şekil 4.7’de verilen görüntüler MicroDicom yazılımı ile görüntülenmiştir. Şekil 4.7.a’da 256x256 ve 512x512 boyutlu iki taşıyıcı MR görüntüsü verilmiştir. Şekil 4.7.b ve Şekil 4.7.c’de sırasıyla SM-LSB ve FL-LSB yöntemleri ile elde edilen gömülü görüntüler görülmektedir. Gizleme işlemi sonrasındaki gömülü görüntülerde kişisel bilgiler görüntü içerisine gizlendiğinden DICOM görüntüleyici bu verileri göstermemiştir. Hasta kişisel bilgileri ancak yetkililerce elde edilebilmektedir.

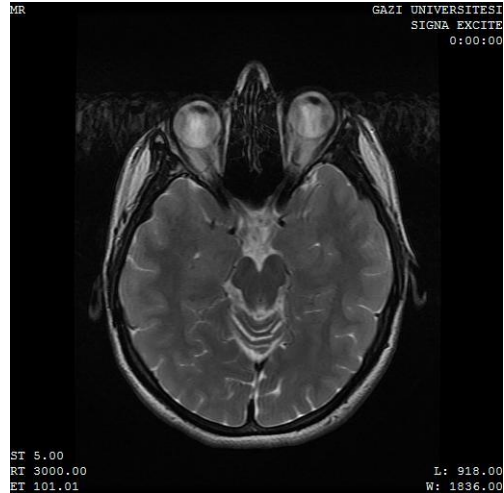
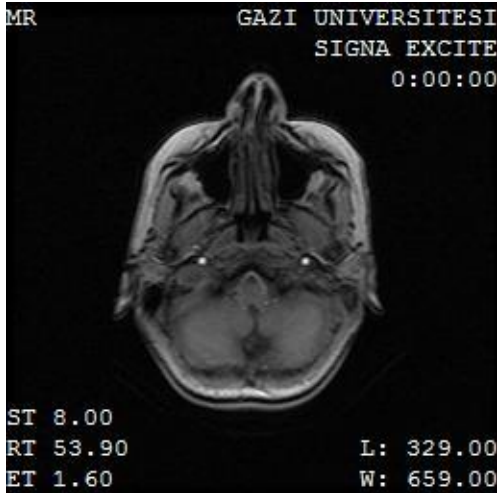
Şekil 4.8 ve Şekil 4.9’da taşıyıcı ve gömülü görüntülerin histogramları verilmiştir. Şekil 4.8.a ve Şekil 4.9.a’de sırasıyla 256x256 ve 512x512 boyutlu taşıyıcı MR görüntülerine ait histogramlar, Şekil 4.8.b ve Şekil 4.9.b’de SM-LSB ile elde edilen gömülü görüntülere ait histogramlar, Şekil 4.8.c ve Şekil 4.9.c’de FL-LSB ile elde edilen gömülü görüntülerin histogramları görülmektedir.



a)

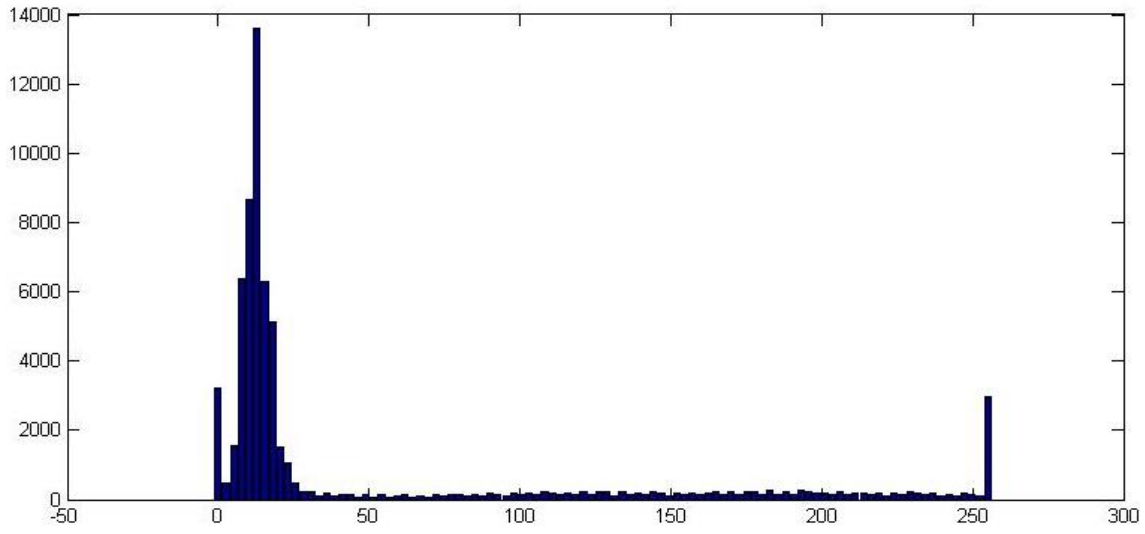


b)

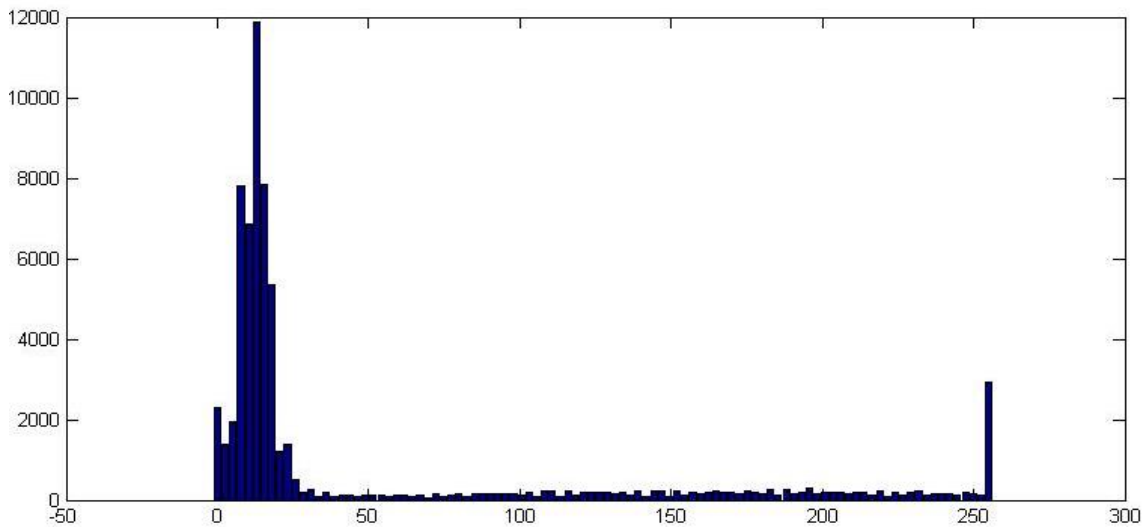


c)

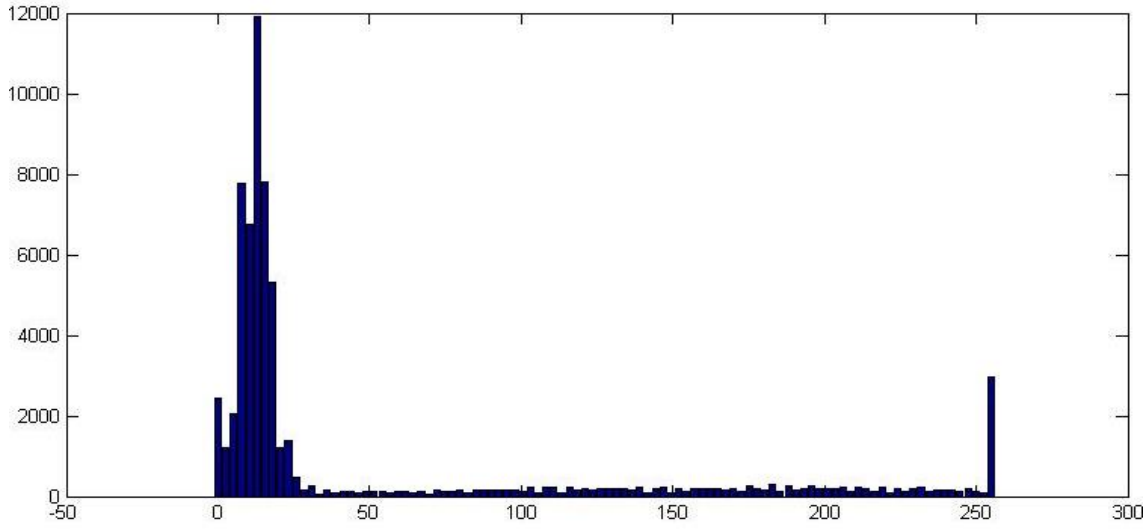
Şekil 4.7. 256x256 ve 512x512 boyutlu taşıyıcı ve gömülü görüntüler a) taşıyıcı görüntüler b) SM-LSB ile oluşturulan gömülü görüntüler, c) FL-LSB ile oluşturulan gömülü görüntüler



a)



b)



c)

Şekil 4.8. 256x256 boyutlu taşıyıcı ve gömülü görüntülerin histogramı a) taşıyıcı görüntü histogramı b) SM-LSB ile oluşturulan gömülü görüntü histogramı c) FL-LSB ile oluşturulan gömülü görüntü histogramı

Şekil 4.8.b, Şekil 4.9.b, Şekil 4.8.c ve Şekil 4.9.c’de, yöntemlerle veri gizleme sonrasında histogramlarda değişim söz konusudur. SM-LSB yöntemi ile FL-LSB yönteminin histogram sonuçları ise birbirine benzerdir. Özellikle histogramda arka planı ifade eden 0 ile 50 arasındaki piksellerin frekans dağılımlarında, veri gizlemede piksellerin en az ağırlıklı bitleri (0 ya da 1) değiştiğinden farklılıklar oluşmuştur.

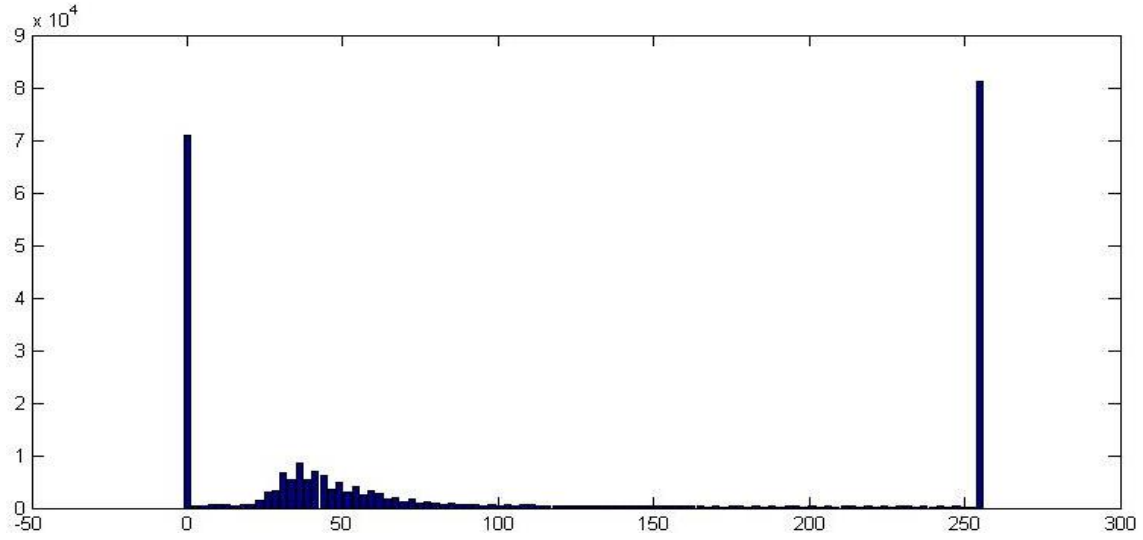
Şekil 4.8.a’da görüldüğü gibi taşıyıcı görüntünün histogramı Rayleigh dağılım özelliği göstermektedir. Şekil 4.8.a ve Şekil 4.8.b’den de görüldüğü gibi, SM-LSB yöntemi ile elde edilen gömülü ve taşıyıcı görüntülerin histogramlarının ortalama değerleri 655,36 olarak elde edilmiş ve değişim oluşmamıştır.

SM-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının standart sapma değerleri sırasıyla 18,851 ve 18,502 şeklindedir. Taşıyıcı ve gömülü görüntülerin histogramlarının çarpıklık değerleri sırasıyla 4,7978 ve 4,7603 şeklindedir. SM-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının basıklık değerleri ise sırasıyla 28,1977 ve 27,9100 şeklindedir. İstatistiksel analizlere göre, histogramlar arası oluşan farklar oldukça düşüktür.

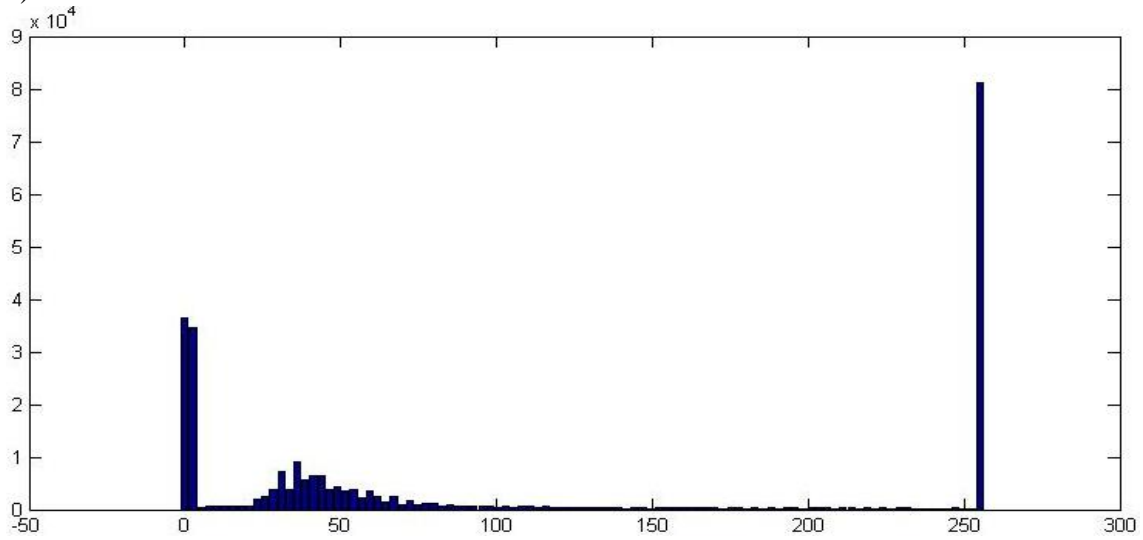
Şekil 4.8.a ve Şekil 4.8.c’den de görüldüğü gibi, FL-LSB yöntemi ile elde edilen gömülü ve taşıyıcı görüntülerin histogramlarının ortalama değerleri 655,36 olarak elde edilmiş ve benzer şekilde değişim oluşmamıştır.

FL-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının standart sapma değerleri sırasıyla 18,851 ve 18,468 şeklindedir. Taşıyıcı ve gömülü görüntülerin histogramlarının çarpıklık değerleri sırasıyla 4,7978 ve 4,7247 şeklindedir.

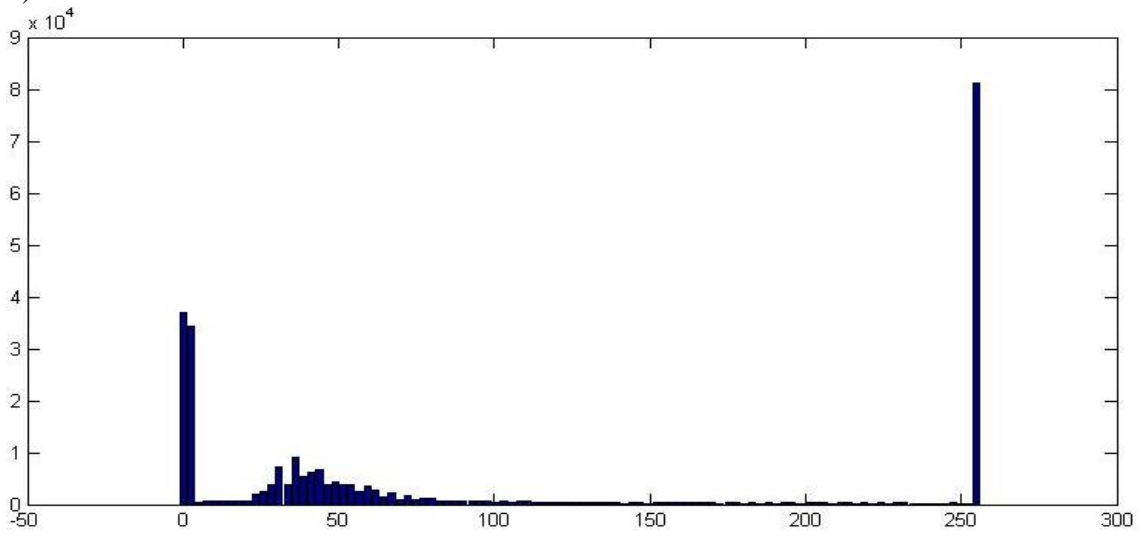
FL-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının basıklık değerleri ise sırasıyla 28,1977 ve 27,4645 şeklindedir. Buna göre, FL-LSB yöntemi ile de, histogramlar arası oluşan farklar oldukça düşüktür.



a)



b)



c)

Şekil 4.9. 512x512 boyutlu taşıyıcı ve gömülü görüntülerin histogramı a) taşıyıcı görüntü histogramı b) SM-LSB ile oluşturulan gömülü görüntü histogramı c) FL-LSB ile oluşturulan gömülü görüntü histogramı

Şekil 4.9.a ve Şekil 4.9.b'den görüldüğü gibi, SM-LSB yöntemi ile elde edilen gömülü ve taşıyıcı görüntülerin histogramlarının ortalama değerleri 655,36 olarak elde edilmiş ve değişim oluşmamıştır. Taşıyıcı ve gömülü görüntülerin histogramlarının standart sapma değerleri sırasıyla 15,144 ve 14,972 şeklindedir.

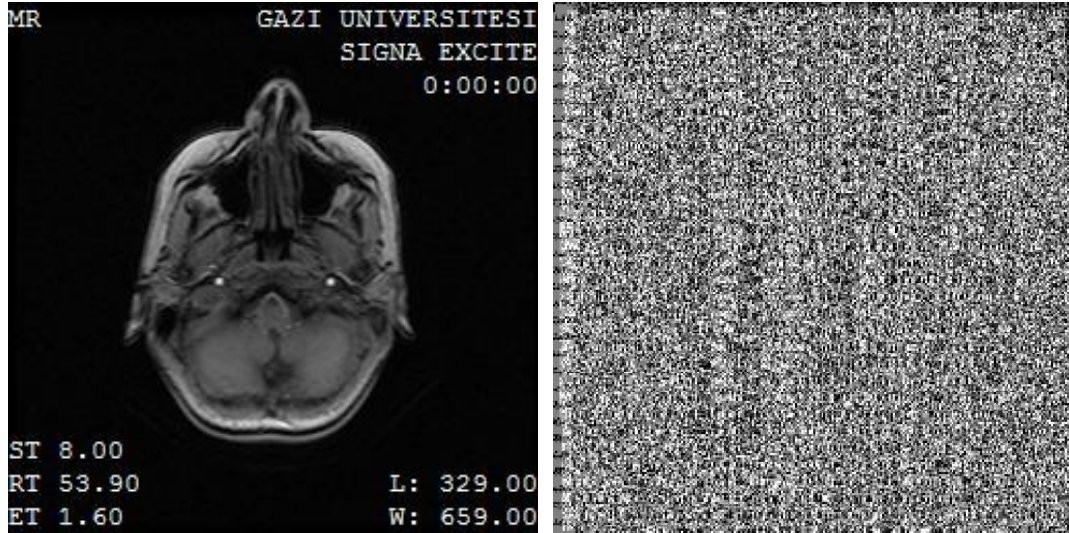
SM-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının çarpıklık değerleri sırasıyla 4,1587 ve 4,2432 şeklindedir. SM-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının basıklık değerleri ise sırasıyla 24,8819 ve 25,9201 şeklindedir (Şekil 4.9.a ve Şekil 4.9.b).

Şekil 4.9.a ve Şekil 4.9.c'den görüldüğü gibi, FL-LSB yöntemi ile elde edilen gömülü ve taşıyıcı görüntülerin histogramlarının ortalama değerleri 655,36 olarak elde edilmiş ve değişim oluşmamıştır. Taşıyıcı ve gömülü görüntülerin histogramlarının standart sapma değerleri sırasıyla 15,144 ve 15,029 şeklindedir.

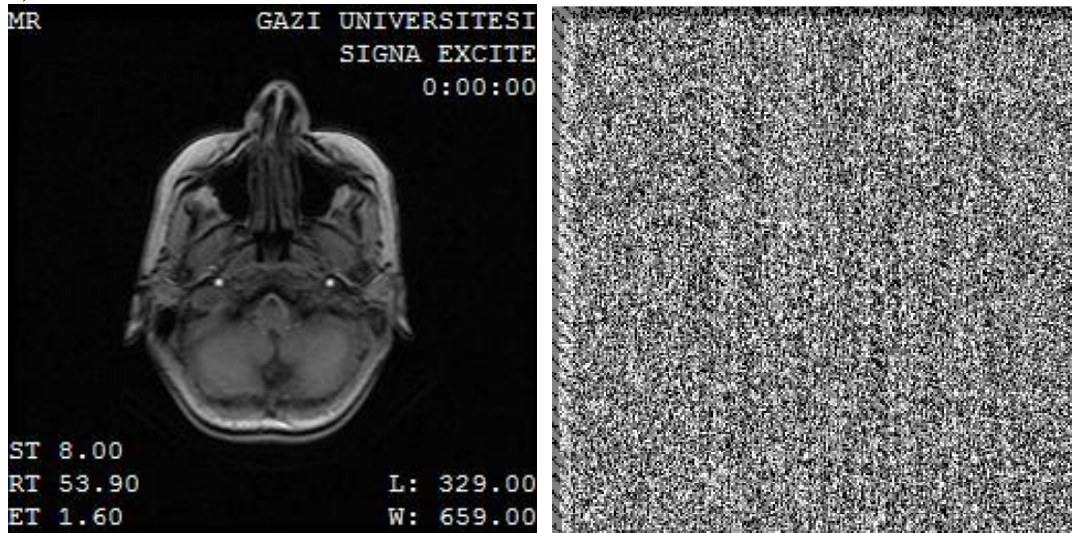
FL-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının çarpıklık değerleri sırasıyla 4,1587 ve 4,2156 şeklindedir. FL-LSB yöntemi ile elde edilen taşıyıcı ve gömülü görüntülerin histogramlarının basıklık değerleri ise sırasıyla 24,8819 ve 25,5435 şeklindedir (Şekil 4.9.a ve Şekil 4.9.c).

Buna göre, SM-LSB ve FL-LSB yöntemleri ile elde edilen görüntüler ve taşıyıcı görüntülerin histogramları arasındaki farklar oldukça düşüktür.

Şekil 4.10 ve Şekil 4.11'de sırasıyla 256x256 ve 512x512 boyutlu MR gömülü görüntülerinde mesaj gizleme sonrası değişen pikseller görülmektedir. Şekil 4.10.a, Şekil 4.11.a'da SM-LSB ile elde edilen sonuçlar, Şekil 4.10.b, Şekil 4.11.b'de FL-LSB ile elde edilen sonuçlar verilmiştir.



a)

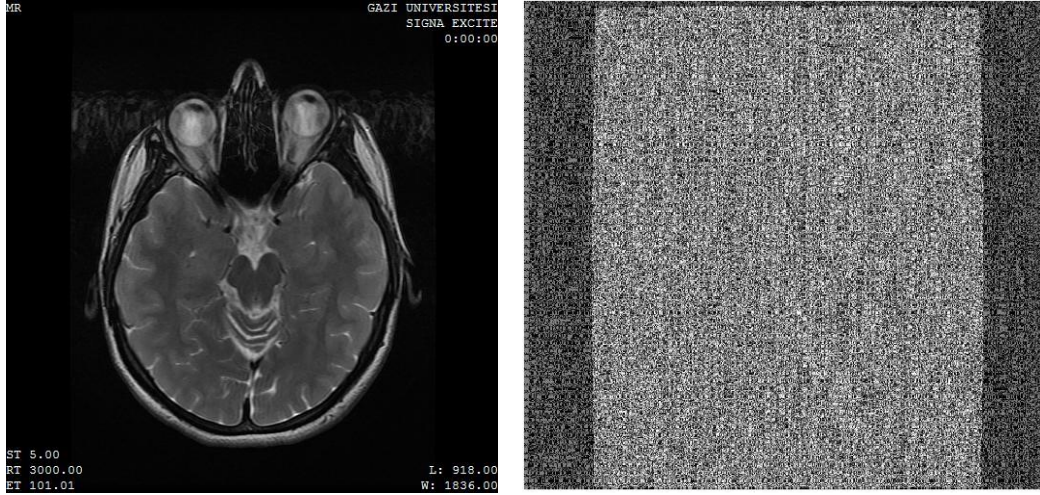


b)

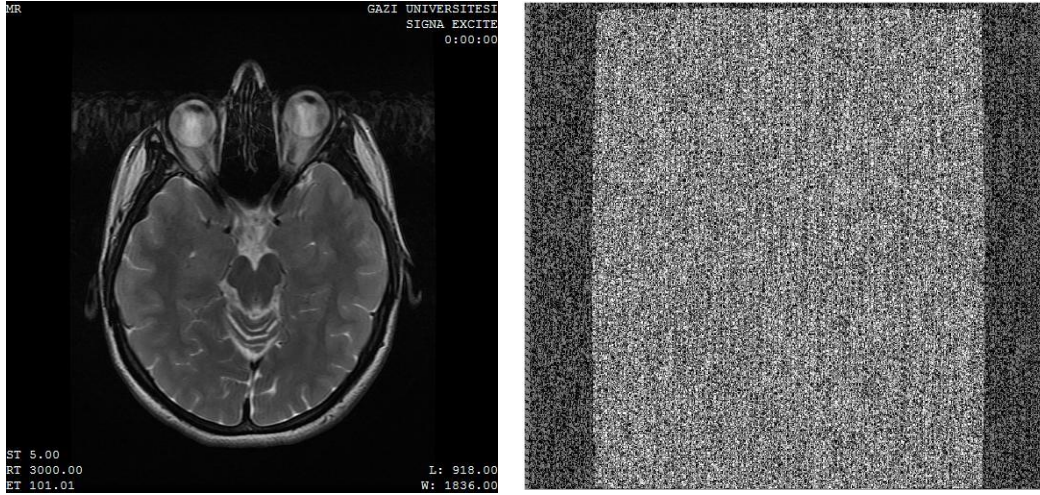
Şekil 4.10. 256x256 boyutlu gömülü görüntülerdeki değişen pikseller a) SM-LSB ile değişen pikseller b) FL-LSB ile değişen pikseller

Bu çalışmanın temel amacı tüm görüntü üzerine dağılacak şekilde veri gizlemektir. Bu sebeple Şekil 4.10 ve Şekil 4.11’de görüntüye gizlenen verinin ilgi ya da ilgi olmayan bölgelerde değil tüm görüntü üzerine dağıldığı görülmektedir. Ancak görüntü değişince FL-LSB ve SM-LSB algoritmalarının seçtiği LSB’lerde değişeceğinden mesajın gizlendiği yerlerde değişecektir. Aynı zamanda farklı bir mesaj gizlendiğinde de görüntü üzerindeki dağılım farklılaşacaktır.





a)

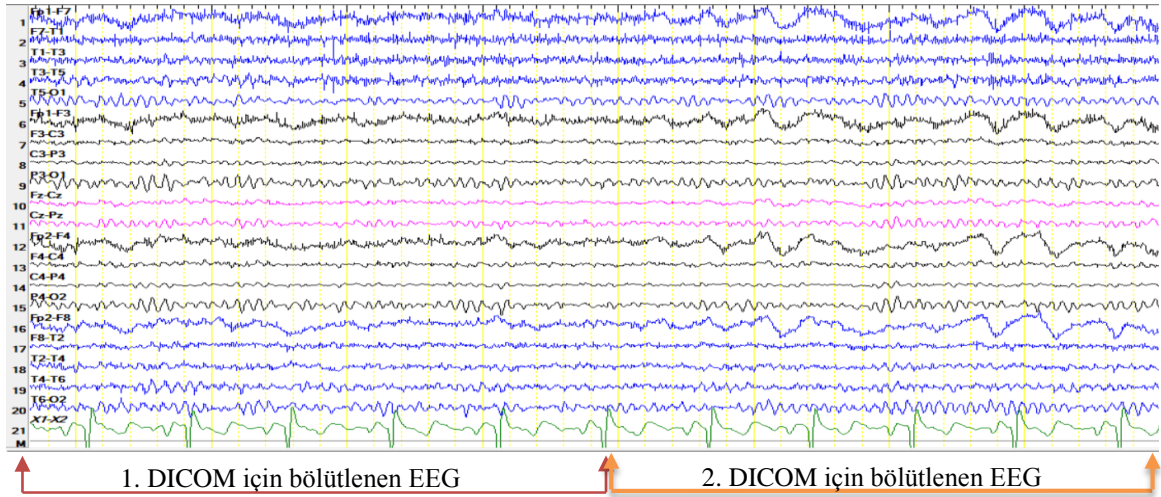


b)

Şekil 4.11. 512x512 boyutlu gömülü görüntülerdeki değişen pikseller a) SM-LSB ile değişen pikseller b) FL-LSB ile değişen pikseller

Şekil 4.11'de verilen MR görüntüsüne sahip olan hastanın tüm DICOM serisindeki görüntülerinin yükseklik ve genişliğine göre bölütlenen EEG işaretleri Şekil 4.12'de verilmiştir.

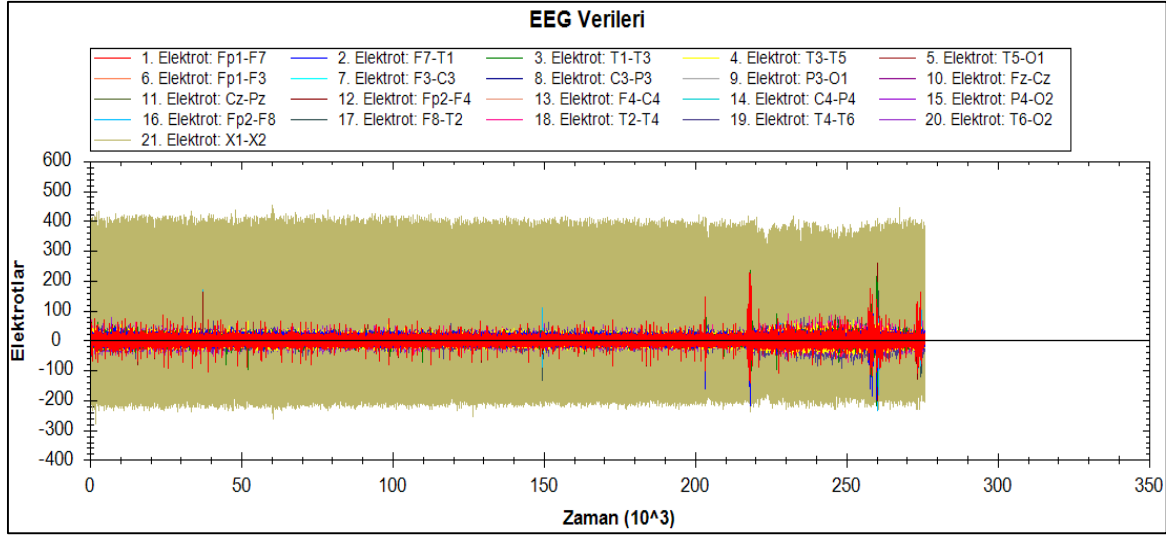
Şekil 4.13'de ise epilepsi hastasına ait EEG verilerinin geliştirilen yöntemler ile gizlenen miktarları gösterilmiştir. Tüm DICOM serisinde sırayla bölütlenen EEG verisi; EEG'nin zaman boyutu, EEG başlık bilgileri, görüntülerin dosya başlık kısmında yer alan kişisel bilgiler ve doktor yorumuyla birleştirilmiştir.



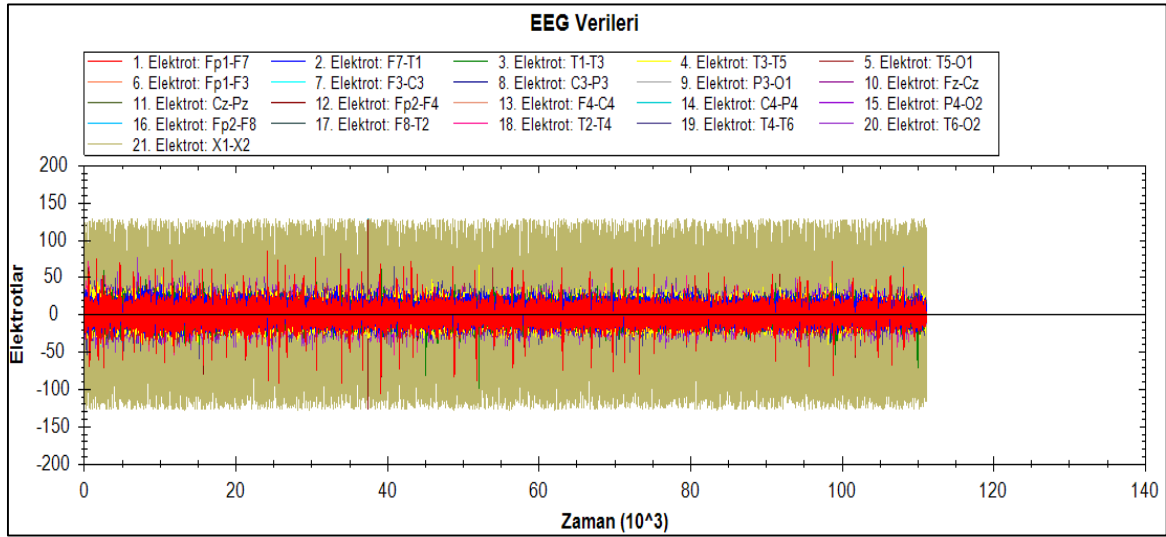
Şekil 4.12. Görüntü boyutlarına göre bölütlenen EEG verisi

Şekil 4.14 ve Şekil 4.15’de sırasıyla 256x256 ve 512x512 boyutlu taşıyıcı MR görüntülerinin belli bir kesitin bilgi gizlemeden önceki ilk hali verilmiştir. Aynı zamanda FL-LSB ve SM-LSB ile aynı kesitte bilgi gizlendikten sonraki görüntüleri gösterilmiştir.

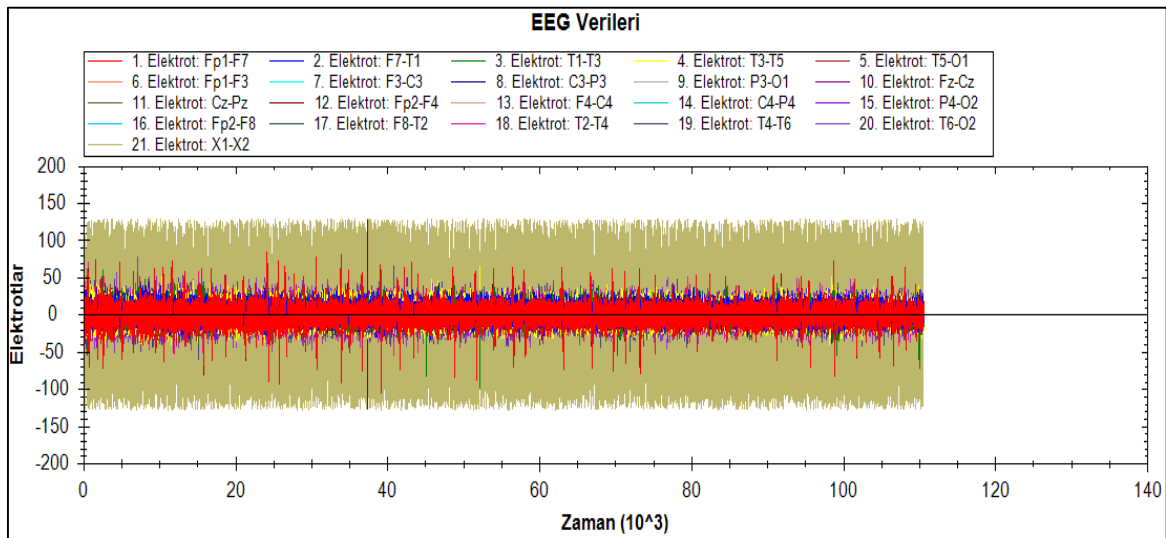
Şekil 4.14 ve Şekil 4.15’e göre, 1000 kez büyütülerek incelenen kafatası ve beyne ait kesit görüntülerin öncesi ve veri gizleme sonrası görüntülerinde, göze çarpan büyük değişimler ya da mozaikleşme söz konusu değildir. Bunun sebebi piksellerin yalnızca en az ağırlıklı tek bitlerinin değişmesidir. Bu işlem diğer bitlerde yapıldığında göze çarpan değişimler olabilir. Buna göre, bu tez çalışmasında önerilen, SM-LSB ve FL-LSB yöntemleri LSB yönteminin algılanamazlık özelliğini sağlamıştır.



a)



b)



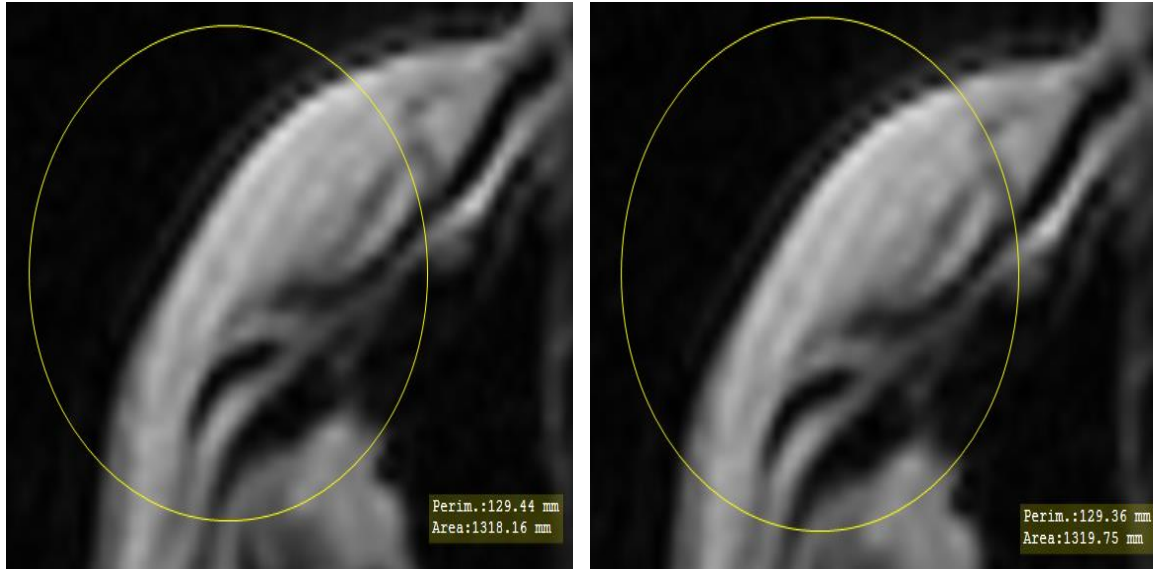
c)

Şekil 4.13. a) EEG verisi, b) SM-LSB ile gizlenen EEG, c) FL-LSB ile gizlenen EEG



a)

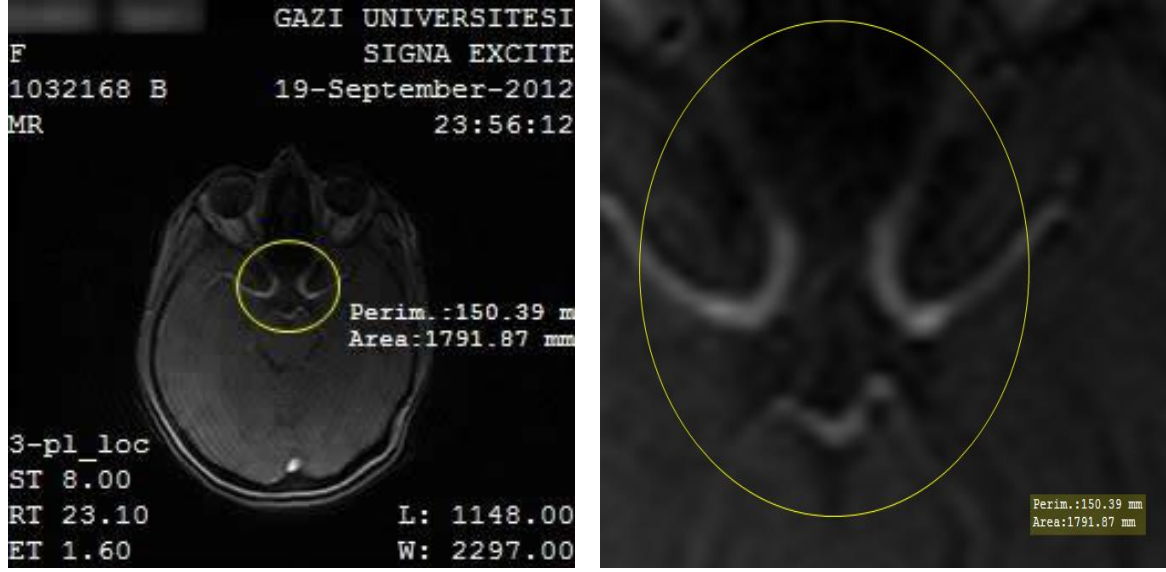
b)



c)

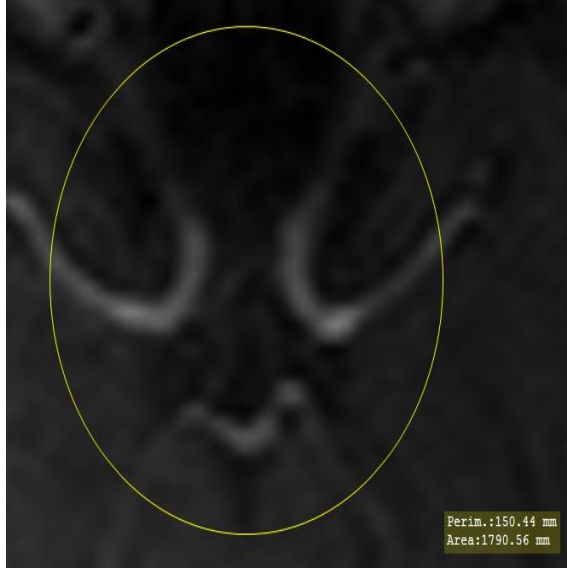
d)

Şekil 4.14. MR görüntü kesiti a) Taşıyıcı MR, b) Taşıyıcı MR kesiti, c) SM-LSB ile elde edilen gömülü MR kesiti d) FL-LSB ile elde edilen gömülü MR kesiti

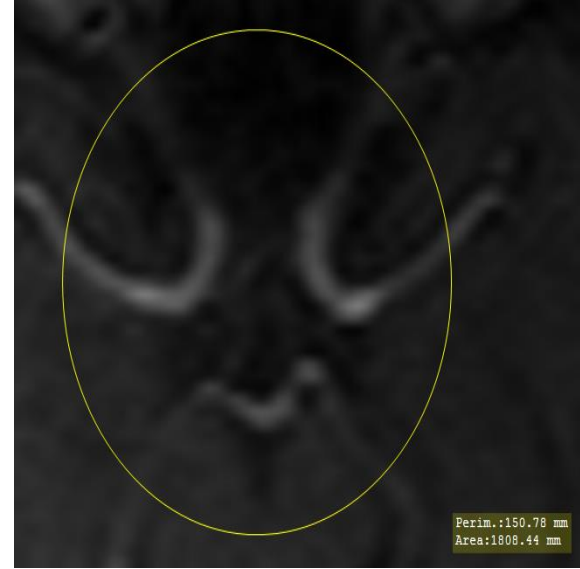


a)

b)



c)



d)

Şekil 4.15.MR görüntü kesiti a) Taşıyıcı MR, b) Taşıyıcı MR kesiti, c) SM-LSB ile elde edilen gömülü MR kesiti d) FL-LSB ile elde edilen gömülü MR kesiti

#### 4.2. Önerilen Yöntemlerle Elde Edilen Sonuçların Karşılaştırması

Çizelge 4.1’de SM-LSB algoritması ile elde edilen gömülü görüntüler ile taşıyıcı görüntüler arasındaki PSNR, MSE, SSIM, UQI ve R ile hesaplanan performans analiz sonuçları verilmiştir. Epilepsi veri setinde 22 hastanın farklı boyutta olan görüntüleri bulunmaktadır. Çizelge 2.2’de her hastanın sahip olduğu farklı çözünürlükteki görüntülerin boyutları ve sayıları verilmiştir. Bu sebeple analiz sonuçları hastaların farklı çözünürlükteki görüntülerinin elde ettiği sonuçların ortalaması alınarak gerçekleştirilmiştir.

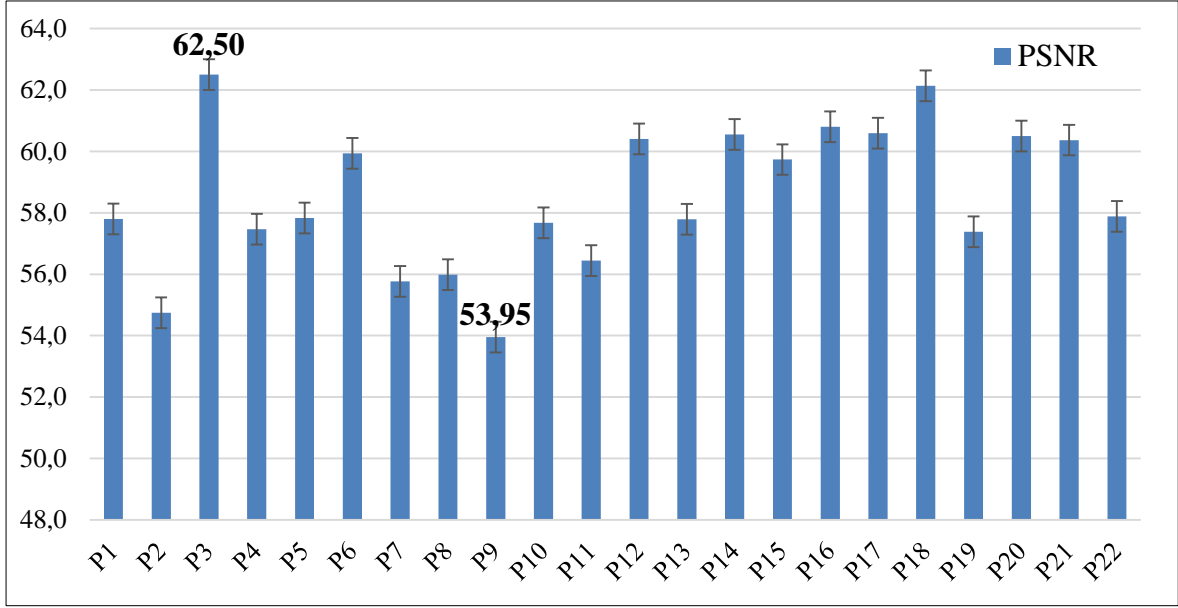
Yapılan çalışmada, veri gizleme işlemi görüntünün alacağı maksimum veri gizleme sınırına göre gerçekleştirilmiştir ve istatistiksel analizlerin hepsi maksimum veri gizleme sonrasında oluşan gömülü görüntüler ve taşıyıcı görüntüler arasında yapılmıştır. Görüntüler içerisine istenilirse maksimum sınırdan daha az veri gizlenebilir. Bunun sonucunda tüm istatistiksel analiz sonuçları daha iyi olacaktır ve gömülü görüntülerle taşıyıcı görüntüler arasındaki benzerlik de artacaktır.

Çizelge 4.1. SM-LSB algoritması ile elde edilen performans sonuçları

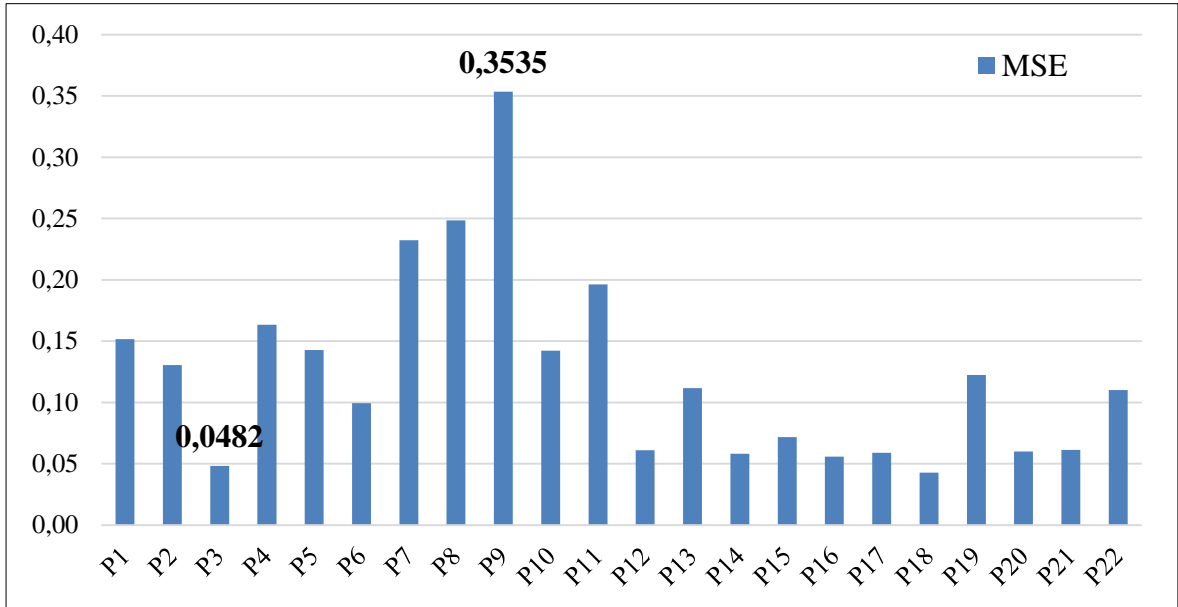
Hasta	PSNR	MSE	SSIM	UQI	R	PSNR-HVS	PSNR-HVSM	% PR
P1	57,7964	0,1515	0,999712	0,999684	0,9982	53,8331	46,4596	13,1255
P2	54,7430	0,1303	0,999792	0,999775	0,9973	52,1328	45,4109	10,6588
P3	62,5025	0,0482	0,999669	0,999630	0,9992	54,3996	45,9084	4,8219
P4	57,4631	0,1635	0,999459	0,999378	0,9975	54,0714	46,4826	13,8005
P5	57,8316	0,1427	0,999714	0,999698	0,9982	54,0485	46,5100	12,9147
P6	59,9360	0,0993	0,999631	0,999561	0,9989	53,7075	46,6281	9,0406
P7	55,7668	0,2323	0,999811	0,999806	0,7173	53,6300	47,0060	17,3619
P8	55,9870	0,2486	0,999743	0,999737	0,7359	53,8101	47,0248	16,5165
P9	53,9520	0,3535	0,999803	0,999797	0,8406	51,2358	44,4351	27,4140
P10	57,6764	0,1421	0,999707	0,999681	0,9977	54,3096	46,5148	11,9838
P11	56,4447	0,1962	0,999898	0,999896	0,8392	50,9367	45,5517	15,7279
P12	60,4063	0,0610	0,999924	0,999923	0,9148	53,6616	46,2436	6,1044
P13	57,7866	0,1117	0,999883	0,999881	0,9212	51,6043	43,9419	11,1691
P14	60,5455	0,0581	0,999872	0,999870	0,9190	54,2426	46,4334	5,8072
P15	59,7319	0,0716	0,999889	0,999887	0,8837	53,5532	46,2750	7,1569
P16	60,8035	0,0558	0,999922	0,999921	0,9243	53,3478	46,2635	5,5806
P17	60,5941	0,0589	0,999894	0,999892	0,8953	53,3487	46,2738	5,8856
P18	62,1346	0,0428	0,999911	0,999909	0,9253	53,8443	46,8480	4,2810
P19	57,3811	0,1223	0,999871	0,999869	0,9054	50,2328	43,2155	12,2341
P20	60,5006	0,0599	0,999932	0,999931	0,9119	53,2875	46,2771	5,9898
P21	60,3670	0,0612	0,999915	0,999913	0,9150	53,4422	46,2618	6,1192
P22	57,8782	0,1100	0,999893	0,999891	0,9229	50,3436	43,2421	10,9998
<b>Min.*</b>	<b>53,9520</b>	<b>0,0428</b>	<b>0,999459</b>	<b>0,999378</b>	<b>0,7173</b>	<b>50,2328</b>	<b>43,2155</b>	<b>4,2810</b>
<b>Mak.*</b>	<b>62,5025</b>	<b>0,3535</b>	<b>0,999932</b>	<b>0,999931</b>	<b>0,9992</b>	<b>54,3996</b>	<b>47,0248</b>	<b>27,4140</b>
<b>S.S.*</b>	<b>2,3441</b>	<b>0,0786</b>	<b>0,000122</b>	<b>0,000143</b>	<b>0,0795</b>	<b>1,3170</b>	<b>1,1339</b>	<b>5,5042</b>

\* Min.=Minimum, Mak.=Maksimum, S.S.=Standart Sapma

Şekil 4.16'dan görüldüğü gibi, ortalama PSNR değerleri en az 53,9520 dB ve en çok 62,5025 dB  $\pm$  2,3441 aralığında elde edilmiştir. Şekil 4.17'den görüldüğü gibi, ortalama MSE değerleri 0,0428 ile 0,3535  $\pm$  0,0786 aralığında bulunmuştur.



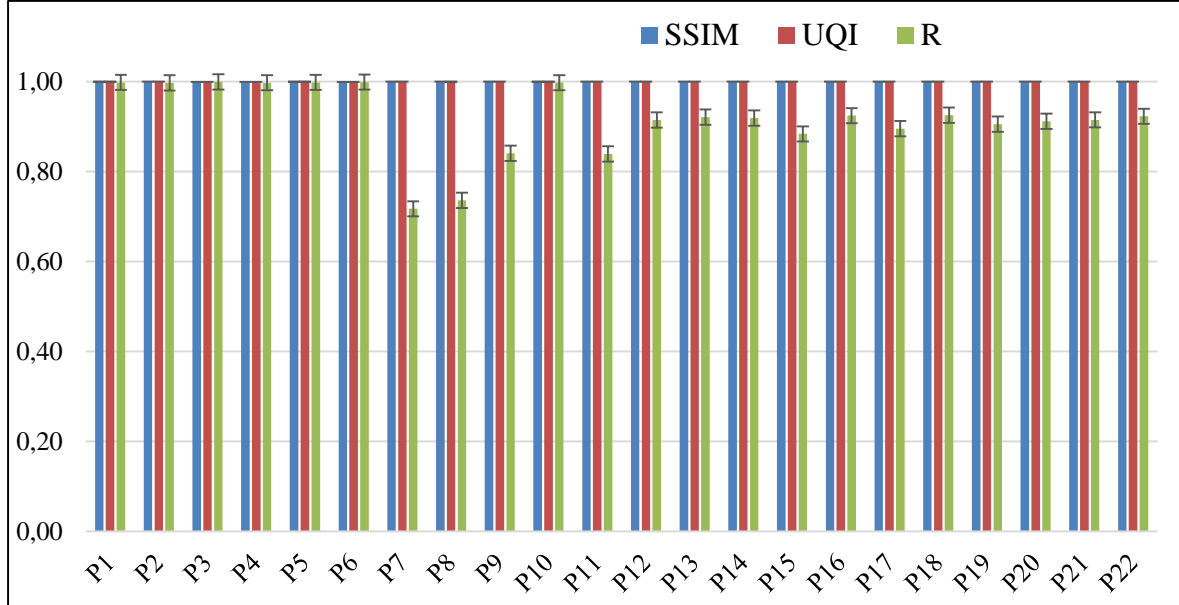
Şekil 4.16. SM-LSB ile elde edilen gömülü görüntülerin PSNR değerleri



Şekil 4.17. SM-LSB ile elde edilen gömülü görüntülerin MSE değerleri

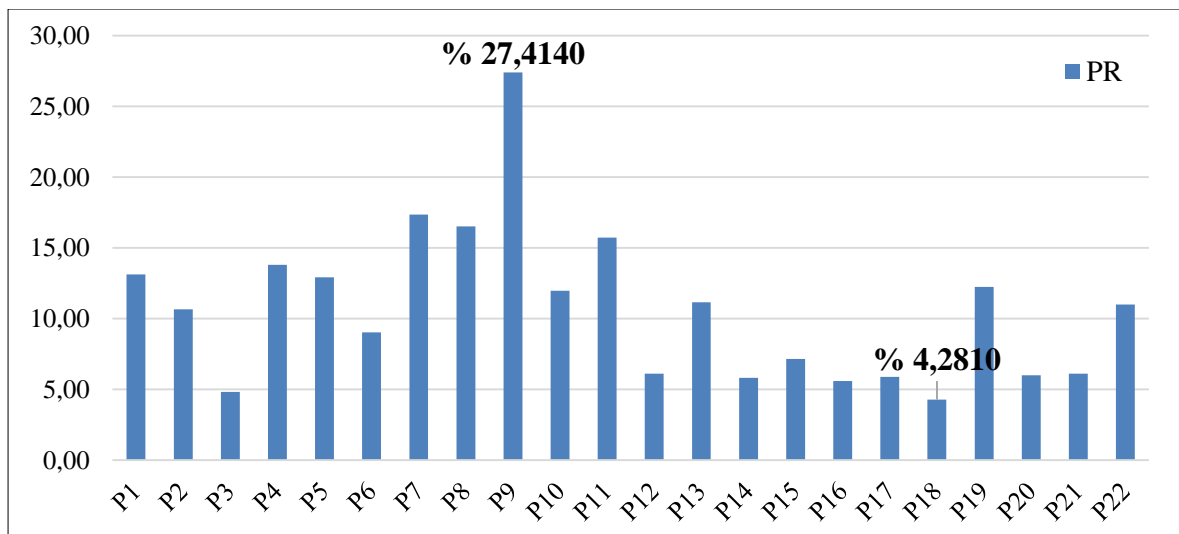
Şekil 4.18'den görüldüğü gibi ortalama korelasyon katsayısı (R) değerleri 0,7173 ile 0,9992  $\pm$  0,0795 arasında bulunmuştur (Şekil 4.17). Ancak görüntü analizinde, insan görme sistemini daha iyi yansıtan SSIM ve UQI analizleri, R analizinden daha yaygın olarak kullanılmaktadır.

Çalışmada, ortalama SSIM ve UQI değerleri ise 0,9994 ve 0,9999 aralığındadır. SSIM değerleri 0,999459 ile 0,999932  $\pm$  0,000122 aralığında ve UQI değerleri ise 0,999378 ile 0,99993  $\pm$  0,000143 aralığında elde edilmiştir. Elde edilen sonuçlara göre gömülü görüntüler ve taşıyıcı görüntüler arasındaki farklılık gözle görülmeyecek kadar çok küçüktür.



Şekil 4.18. SM-LSB ile elde edilen gömülü görüntülerin SSIM, UQI ve R değerleri

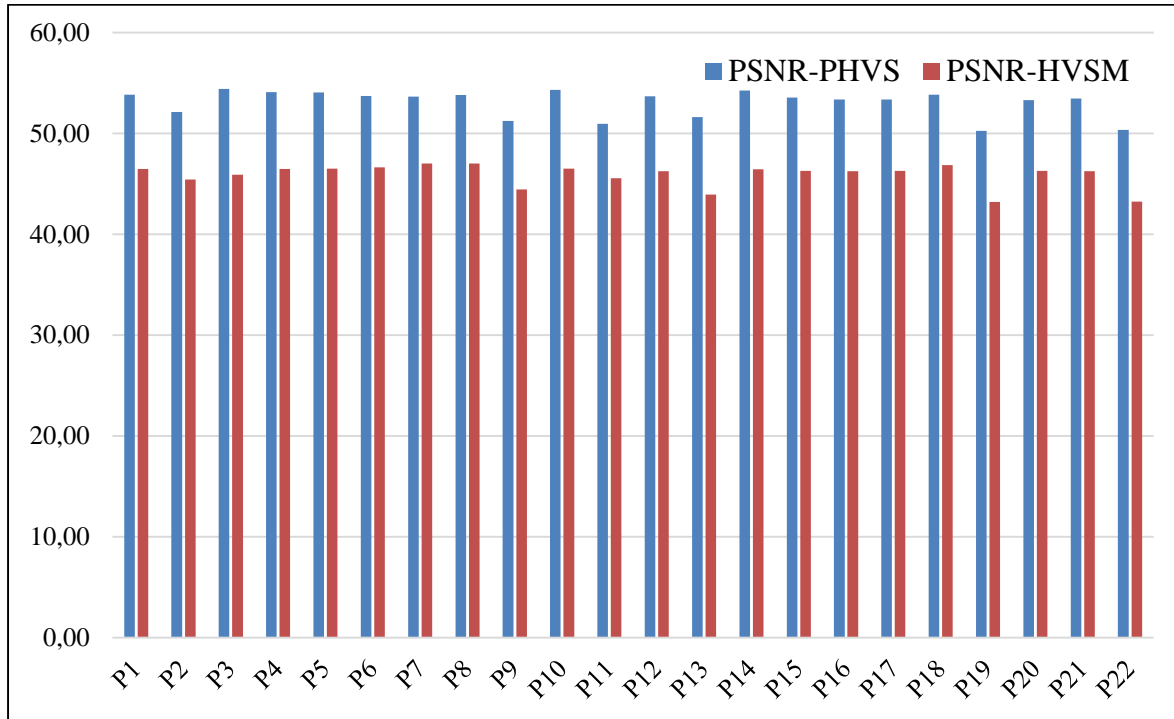
Çalışmada aynı zamanda her görüntü için ortalama değişen piksel oranı (PR) değişen piksel sayısı/gömülü görüntüdeki piksel sayısı ile elde edilmiştir. Çizelge 4.1’de ve Şekil 4.19’da görüldüğü gibi, ortalama PR değerleri en az % 4,2810 ve en fazla % 27,4140’dır.



Şekil 4.19. SM-LSB ile elde edilen gömülü görüntülerin değişen ortalama piksel oranı (PR) değerleri



Çalışmada, gömülü ve taşıyıcı görüntüler arasındaki karşılaştırmayı frekans düzleminde yapan PSNR-HVS ve PSNR-HVSM istatistiksel analizleri de kullanılmıştır. Şekil 4.20’de görüldüğü gibi, PSNR-HVS değerleri 50,2328 ile 54,3996  $\pm$  1,3170 aralığındadır. PSNR-HVSM değerleri ise 43,2155 ile 47,0248  $\pm$  1,1339 aralığında bulunmuştur. Literatüre göre bu değerlerin tıpkı PSNR’de olduğu gibi 35 dB’den yüksek olması gerekmektedir. Maksimum veri gizleme ile elde edilen sonuçlara göre gömülü görüntüler ve taşıyıcı görüntüler arasındaki farklılıklar çok azdır.



Şekil 4.20. SM-LSB ile elde edilen gömülü görüntülerin PSNR-HVS ve PSNR-HVSM değerleri

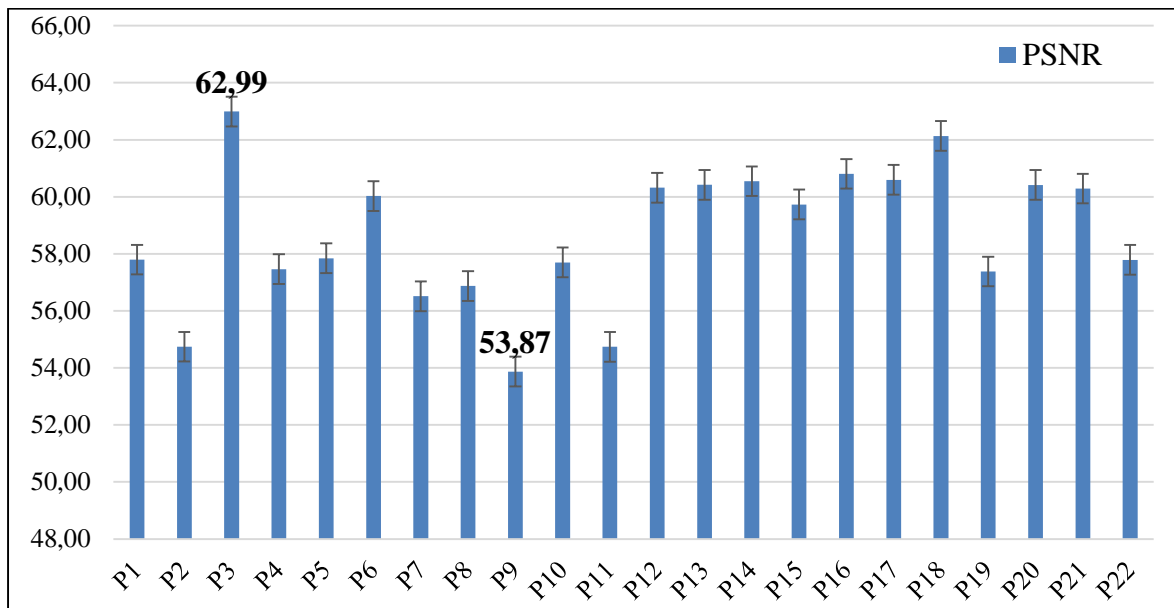
Çizelge 4.2’de FL-LSB algoritması ile elde edilen istatistiksel karşılaştırma analiz sonuçları verilmiştir. Çizelge 4.2 ve Şekil 4.21’den görüldüğü gibi, ortalama PSNR değerleri 53,8708 dB ve 62,9892 dB  $\pm$  2,4389 aralığındadır. PSNR değerleri literatürdeki sınır olan 35 dB değerinden çok yüksektir.

Şekil 4.22’de görüldüğü gibi ortalama MSE değerleri 0,0428 ve 0,3598  $\pm$  0,08123 olarak bulunmuştur. Elde edilen ortalama MSE değerleri sıfıra çok yakındır. Buna göre gömülü ve taşıyıcı görüntüler arasındaki farklılık çok azdır.

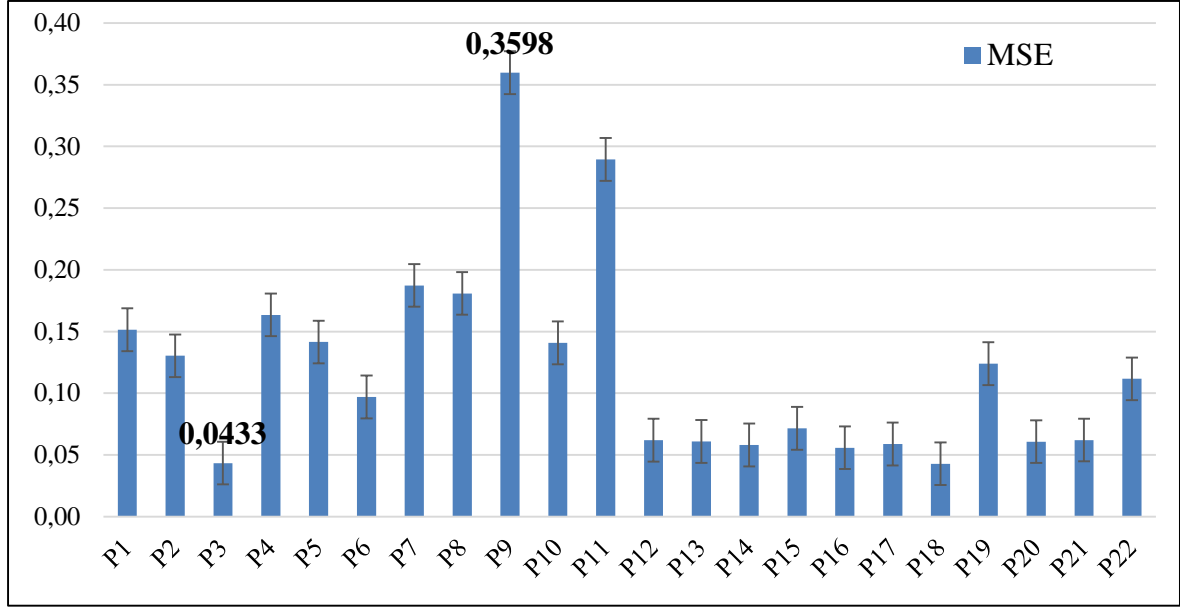
Çizelge 4.2. FL-LSB algoritması ile elde edilen performans sonuçları

Hasta	PSNR	MSE	SSIM	UQI	R	PSNR-HVS	PSNR-HVSM	PR %
P1	57,7964	0,1515	0,999712	0,999684	0,9982	53,8331	46,4596	13,12552
P2	54,7430	0,1303	0,999792	0,999775	0,9973	52,1328	45,4109	10,65882
P3	62,9892	0,0433	0,999696	0,999658	0,9993	55,3289	47,0047	4,330891
P4	57,4631	0,1635	0,999459	0,999378	0,9975	54,0714	46,4826	13,80047
P5	57,8434	0,1415	0,999716	0,999700	0,9983	54,0859	46,5128	12,82817
P6	60,0257	0,0969	0,999639	0,999569	0,9990	53,7148	46,6274	8,802772
P7	56,5125	0,1873	0,999883	0,999880	0,8141	54,0836	47,0112	15,52878
P8	56,8729	0,1808	0,999843	0,999840	0,8621	54,4503	47,0753	14,23622
P9	53,8708	0,3598	0,999801	0,999795	0,8371	51,1623	44,4052	28,02354
P10	57,7006	0,1408	0,999711	0,999684	0,9977	54,3307	46,5113	11,85890
P11	54,7384	0,2895	0,999881	0,999878	0,8405	51,1639	44,7846	23,89260
P12	60,3198	0,0619	0,999923	0,999922	0,9134	53,8538	46,2800	6,194917
P13	60,4180	0,0609	0,999884	0,999882	0,9200	53,9051	46,3073	6,087525
P14	60,5455	0,0581	0,999872	0,999870	0,9190	54,2426	46,4334	5,807245
P15	59,7319	0,0716	0,999889	0,999887	0,8837	53,5532	46,2750	7,156903
P16	60,8035	0,0558	0,999922	0,999921	0,9243	53,3478	46,2635	5,580629
P17	60,5941	0,0589	0,999894	0,999892	0,8953	53,3487	46,2738	5,885576
P18	62,1346	0,0428	0,999911	0,999909	0,9253	53,8443	46,8480	4,280992
P19	57,3811	0,1240	0,999867	0,999865	0,9040	50,3448	43,2412	12,39595
P20	60,4156	0,0607	0,999933	0,999933	0,9105	53,4105	46,3028	6,073809
P21	60,2887	0,0620	0,999908	0,999907	0,9135	53,5700	46,2915	6,203587
P22	57,7906	0,1116	0,999894	0,999892	0,9216	50,4658	43,2681	11,16233
<b>Min.*</b>	<b>53,8708</b>	<b>0,0428</b>	<b>0,999459</b>	<b>0,999378</b>	<b>0,8141</b>	<b>50,3448</b>	<b>43,2412</b>	<b>4,28099</b>
<b>Mak.*</b>	<b>62,9892</b>	<b>0,3598</b>	<b>0,999933</b>	<b>0,999933</b>	<b>0,9993</b>	<b>55,3289</b>	<b>47,0753</b>	<b>28,02354</b>
<b>S.S.*</b>	<b>2,4389</b>	<b>0,0812</b>	<b>0,000119</b>	<b>0,000140</b>	<b>0,0586</b>	<b>1,3461</b>	<b>1,1013</b>	<b>6,128659</b>

\* Min.=Minimum, Mak.=Maksimum, S.S.=Standart Sapma

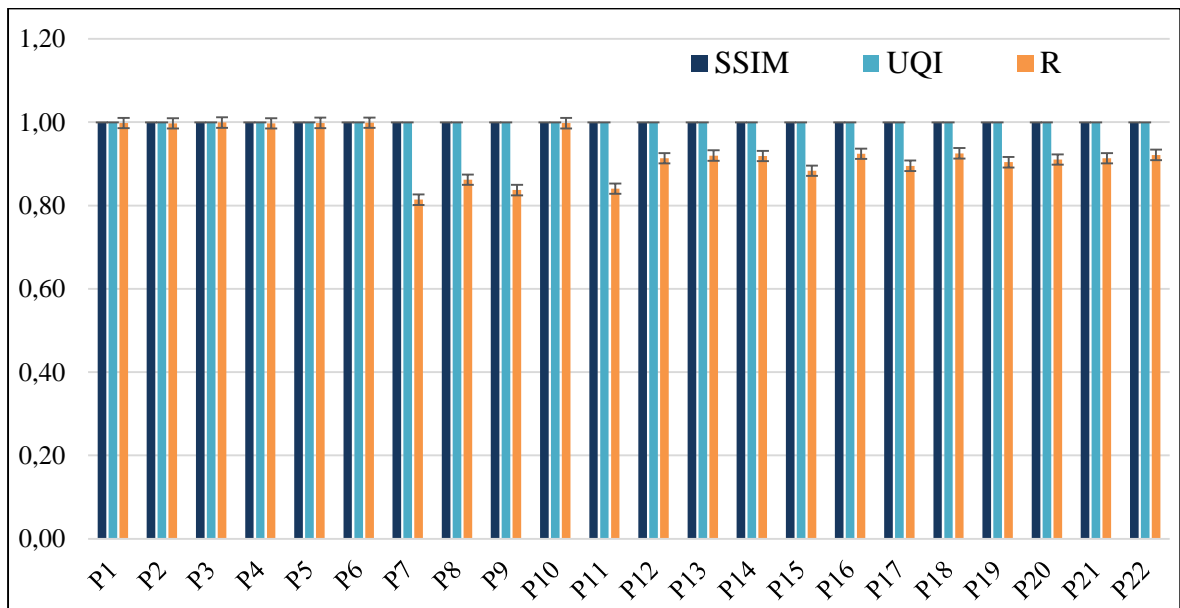


Şekil 4.21. FL-LSB ile elde edilen gömülü görüntülerin PSNR değerleri



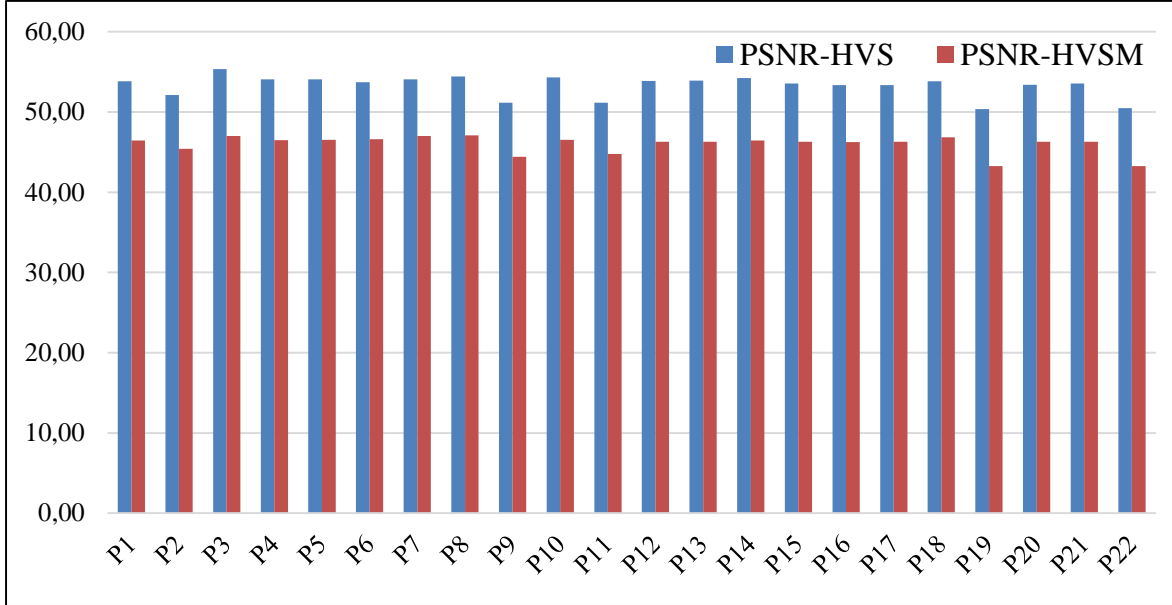
Şekil 4.22. FL-LSB ile elde edilen gömülü görüntülerin MSE değerleri

Çizelge 4.2 ve Şekil 4.23'den görüldüğü gibi ortalama SSIM değerleri, 0,999459 ile 0,999933  $\pm$  0,000119 aralığında ve UQI değerleri, 0,999378 ile 0,999933,  $\pm$  0,000140 aralığında elde edilmiştir. Ortalama R değerleri 0,8141 ile 0,9993  $\pm$  0,0586 arasındadır. R değerleri daha düşük olarak elde edilmiş olsa da insan görme sistemini daha iyi yansıtan SSIM ve UQI değerleri çalışmada çok yüksektir. Elde edilen sonuçlara göre gömülü görüntüler ve taşıyıcı görüntüler arasındaki farklılık gözle görülmeyecek kadar çok küçüktür.

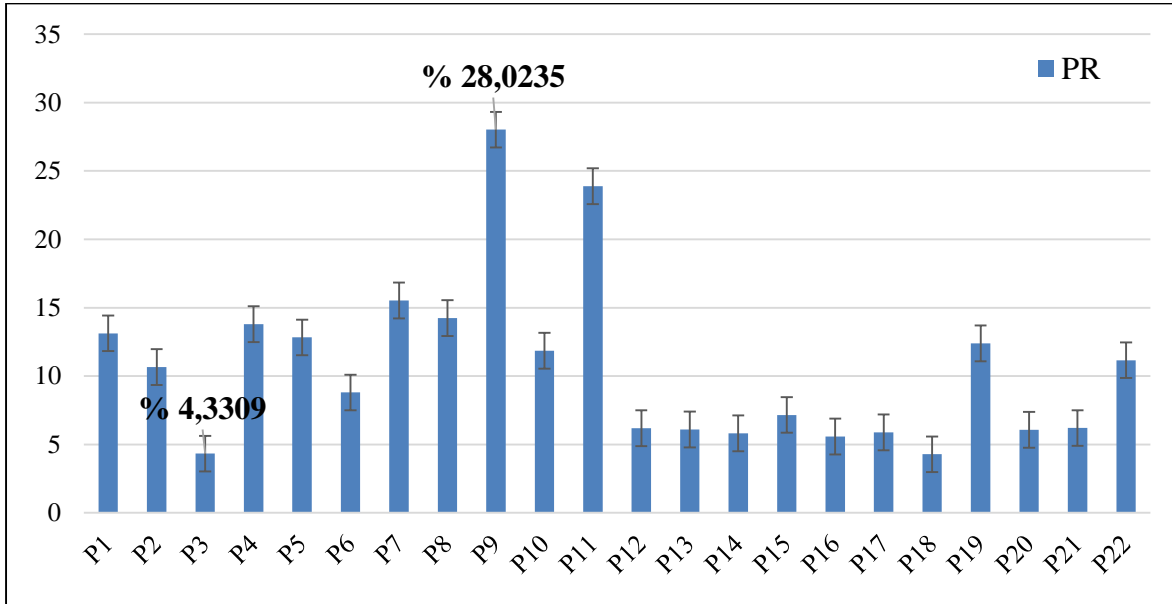


Şekil 4.23. FL-LSB ile elde edilen gömülü görüntülerin SSIM, UQI ve R değerleri

Çizelge 4.2 ve Şekil 4.24'den görüldüğü gibi, ortalama PSNR-HVS değerleri 50,3448 ile 55,3289  $\pm$  1,3461, PSNR-HVSM 43,2412 ile 47,0753  $\pm$  1,1013 arasında bulunmuştur. Bu değerler alt sınır olan 35 dB'den çok yüksektir. Çizelge 4.2 ve Şekil 4.25'den, ortalama PR değerleri % 4,280 ve % 28,0235  $\pm$  6,128659 aralığındadır.



Şekil 4.24. FL-LSB ile elde edilen gömülü görüntülerin PSNR-HVS ve PSNR-HVSM değerleri



Şekil 4.25. FL-LSB ile elde edilen gömülü görüntülerin PR değerleri

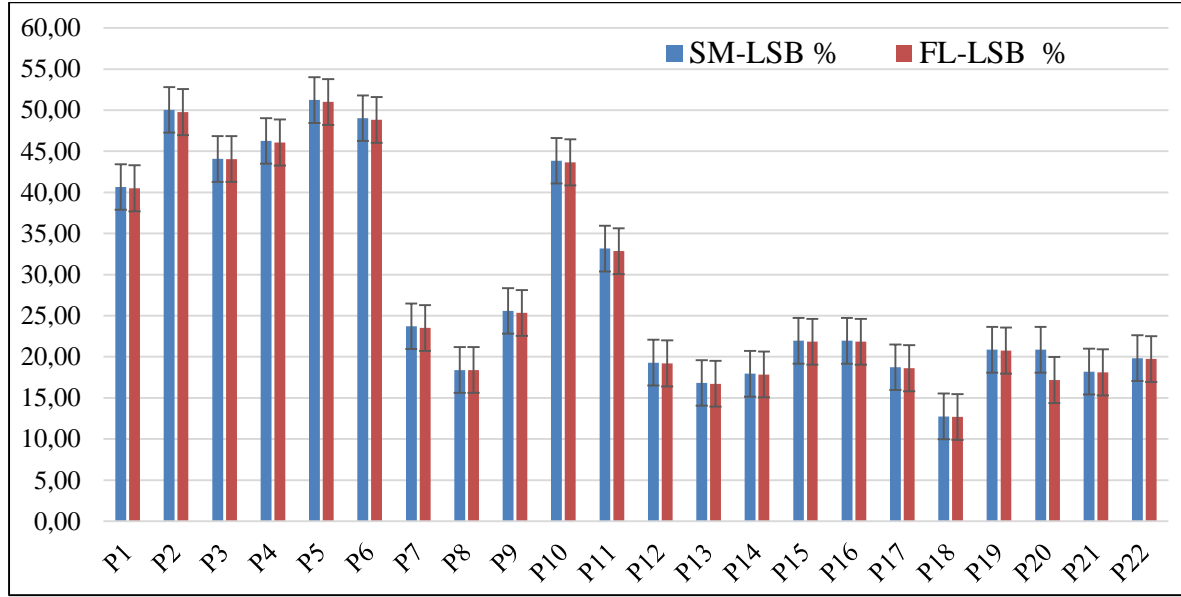
Çizelge 4.1 ve Çizelge 4.2’de, SM-LSB ve FL-LSB yöntemlerinin 22 epilepsi hastasına ait farklı çözünürlükteki (176x176, 256x256, 448x448, ... , 512x512) taşıyıcı görüntüleri ile gömülü görüntüleri arasındaki istatistiksel karşılaştırma analizleri verilmiştir. Bu analizlere göre, geliştirilen iki yöntemde birbirlerine yakın değerler elde etmiştir.

Yapılan çalışmada, önerilen yöntemlerin LSB yönteminin en önemli özelliklerinden biri olan yüksek kapasite özelliğini sağlama durumu da incelenmiştir. Bu sebeple, Çizelge 4.3’de önerilen algoritmaların sıkıştırma yöntemleri kullanılmaksızın elde ettiği toplam mesaj kapasiteleri verilmiştir.

Çizelge 4.3. Önerilen algoritmaların gizlediği mesaj kapasitelerinin karşılaştırılması

Hastalar	Toplam Data (bayt)	Gizlenen Verinin Kapasitesi		Gizlenen Verinin Yüzdesi	
		SM-LSB (bayt)	FL-LSB (bayt)	SM-LSB (%)	FL-LSB (%)
P1	23 309 184	9 477 996	9 438 516	40,66	40,49
P2	20 277 900	10 147 080	10 090 884	50,04	49,76
P3	20 824 672	9 177 232	9 174 796	44,07	44,06
P4	20 570 604	9 514 758	9 478 620	46,25	46,07
P5	18 166 332	9 305 592	9 263 676	<b>51,22</b>	<b>50,99</b>
P6	19 098 474	9 361 866	9 322 386	49,02	48,81
P7	18 925 142	4 488 314	4 449 254	23,72	23,51
P8	24 570 294	4 520 418	4 520 418	18,40	18,40
P9	22 743 126	5 817 210	5 763 450	25,58	25,34
P10	21 557 540	9 453 560	9 410 804	43,85	43,65
P11	18 945 024	6 283 032	6 224 904	33,16	32,86
P12	18 306 600	3 531 000	3 514 200	19,29	19,20
P13	20 995 000	3 531 400	3 511 240	16,82	16,72
P14	21 005 574	3 767 514	3 749 454	17,94	17,85
P15	16 089 000	3 531 000	3 512 520	21,95	21,83
P16	16 090 200	3 532 200	3 513 720	21,95	21,84
P17	18 861 400	3 531 400	3 511 240	18,72	18,62
P18	27 698 600	3 531 800	3 511 640	<b>12,75</b>	<b>12,68</b>
P19	16 929 800	3 531 800	3 513 320	20,86	20,75
P20	16 929 400	3 531 400	3 512 920	20,86	17,17
P21	19 399 000	3 531 400	3 512 920	18,20	18,11
P22	17 803 000	3 531 400	3 512 920	19,84	19,73

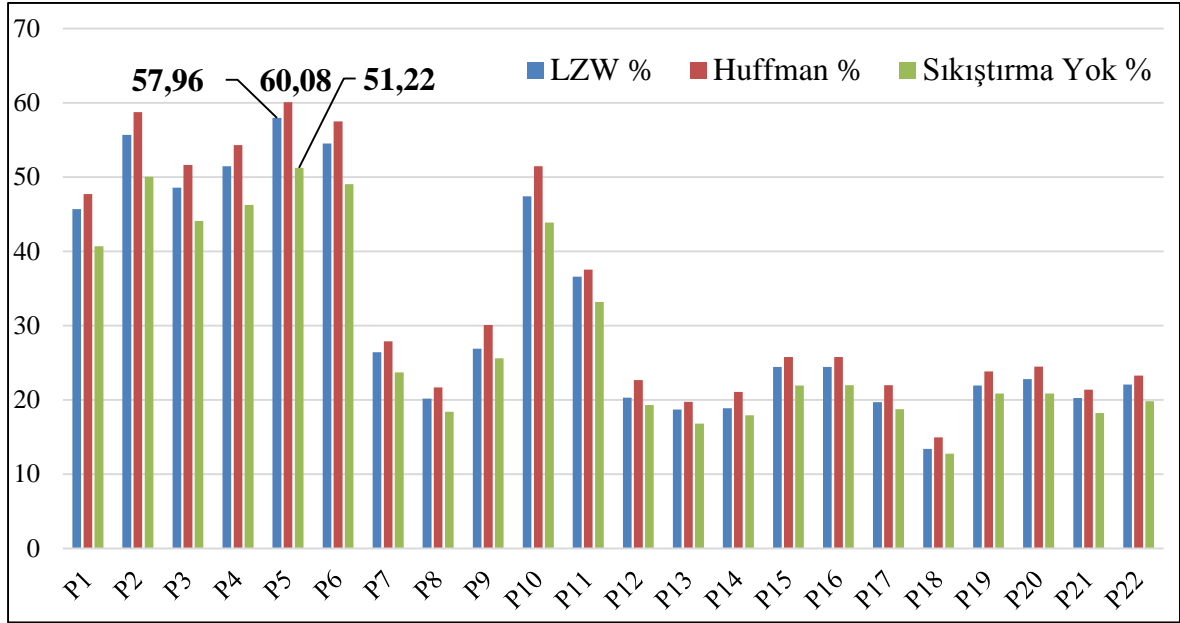
Çizelge 4.3 ve Şekil 4.26'da görüldüğü gibi, SM-LSB yöntemi ile toplam verinin en az % 12,75'i ve en fazla % 51,22'si gizlenmiştir. Çizelge 4.3 ve Şekil 4.26'da görüldüğü gibi, FL-LSB yöntemi ise toplam verinin en az % 12,68'ini ve en fazla % 50,99'unu gizlemiştir. Çizelge 4.3'ten görüldüğü gibi geliştirilen yöntemlerin veri gizleme kapasiteleri birbirine yakındır ancak SM-LSB yöntemi daha fazla veri gizlemiştir.



Şekil 4.26. Önerilen algoritmaların gizlediği mesaj kapasitelerinin karşılaştırılması

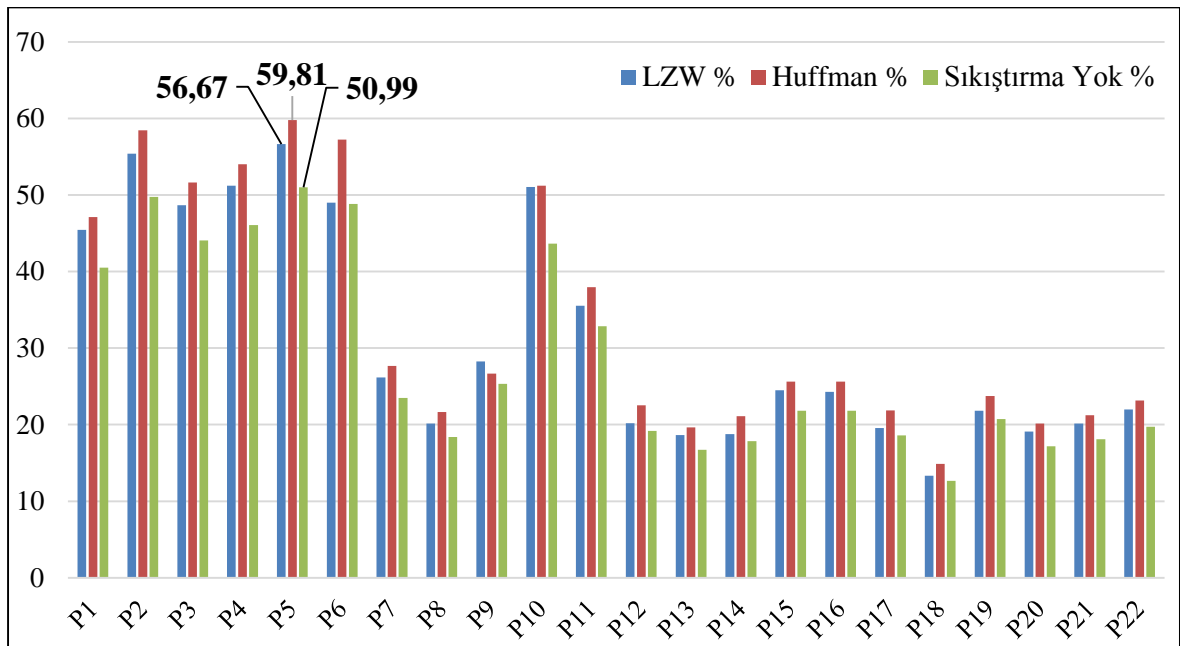
Bu çalışmada sıkıştırma algoritmalarının veri gizleme kapasitesine etkisi de araştırılmıştır. Kayıplı sıkıştırma algoritmaları veri üzerinde kayıplar oluşturacağından, hastalığın tanı ve teşhisi bu durumdan etkilenebilir. Bu sebeple, çalışmada kayıpsız Huffman ve LZW algoritmaları kullanılmıştır. Yöntemler veri gizleme kapasitesini artırmıştır.

Şekil 4.27'de SM-LSB algoritmasının sıkıştırma yöntemleri kullanıldığında gizlenen mesajın yüzde değerleri verilmiştir. Huffman sıkıştırma ile toplam verinin en az % 14,97'si ve en fazla % 60,08'si gizlenmiştir. LZW sıkıştırma ile toplam verinin en az % 13,41'i ve en fazla % 57,96'sı gizlenmiştir. Huffman kayıpsız sıkıştırma kullanılarak daha fazla veri gizlendiği Şekil 4.27'den de görülmektedir.



Şekil 4.27. SM-LSB algoritması ile elde edilen veri gizleme kapasitelerinin yüzdesi

Şekil 4.28’de ise FL-LSB algoritmasının elde ettiği veri gizleme kapasitelerinin yüzdeleri verilmiştir. Benzer şekilde burada da Huffman sıkıştırma algoritması ile daha fazla veri saklanmıştır. LZW sıkıştırma ile toplam verinin en az % 5,38’i ve en fazla % 56,67’si saklanırken, Huffman sıkıştırma ile en az % 14,88’i ve en fazla % 59,81’i gizlenmiştir. Şekil 4.27 ve Şekil 4.28’den görüldüğü gibi kayıpsız sıkıştırma algoritmaları kapasiteyi artırmıştır.



Şekil 4.28. FL-LSB algoritması ile elde edilen veri gizleme kapasitelerinin yüzdesi

Geliştirilen yöntemlerin, mesaj gizleme sınırlarını etkileyen en önemli faktör taşıyıcı görüntülerin boyutlarıdır. Çizelge 4.3'den görüldüğü gibi, EEG kayıtlarının süresinin 20-40 dakika olması sebebiyle toplam veri miktarının hepsi gizlenememiştir. Ancak çalışmada, her görüntünün kişisel bilgileri, EEG verisinin genel özellikleri öncelikli olarak mutlaka gizlenmiştir.

Çizelge 4.4'de geliştirilen yöntemlerin farklı görüntü boyutlarında gizlediği mesaj kapasiteleri verilmiştir. Buna göre, SM-LSB yöntemi ile 176x176 boyutlu görüntüde 6 962 bayt ve 512x512 boyutlu görüntüde 64 838 bayt veri gizlenmiştir. LZW sıkıştırma kullanıldığında aynı boyuttaki görüntülerde sırasıyla 7 802 bayt ve 72 734 bayt veri gizlenmiştir. Huffman sıkıştırma ile aynı boyuttaki görüntülerde sırasıyla 8 222 bayt ve 76 010 bayt veri saklanmıştır.

Çizelge 4.4'den görüldüğü gibi FL-LSB algoritması ile 176x176 boyutlu görüntüde 6 794 bayt ve 512x512 boyutlu görüntüde 64 586 bayt mesaj gizlenmiştir. LZW sıkıştırma kullanıldığında aynı boyuttaki görüntülerde sırasıyla 7 550 bayt ve 72 482 bayt veri gizlenmiştir. Huffman sıkıştırma kullanıldığında ise aynı boyuttaki görüntülerde 8 054 bayt ve 75 086 bayt veri saklanmıştır. Geliştirilen yöntemler görüntü boyutlarına göre veri gizlediğinden, boyutlar ve görüntü sayısı arttıkça veri gizleme kapasitesi de artmıştır.

Çizelge 4.4. Önerilen algoritmaların farklı görüntü boyutlarına göre gizlediği mesaj kapasiteleri

Görüntü Boyutları	SM-LSB (bayt)			FL-LSB (bayt)		
	Sıkıştırma Yok	LZW	Huffman	Sıkıştırma Yok	LZW	Huffman
<b>176x176</b>	<b>6 962</b>	<b>7 802</b>	<b>8 222</b>	<b>6 794</b>	<b>7 550</b>	<b>8 054</b>
256x256	15 698	17 714	18 470	15 614	17 546	18 218
248x320	14 606	16 286	17 210	14 522	16 202	17 126
320x320	24 854	27 626	29 222	24 686	27 458	28 970
424x512	44 174	46 442	51 818	44 090	46 274	49 046
448x448	49 466	54 926	57 950	49 214	54 674	57 698
464x512	53 078	58 958	62 234	52 994	58 874	62 066
<b>512x512</b>	<b>64 838</b>	<b>72 734</b>	<b>76 010</b>	<b>64 586</b>	<b>72 482</b>	<b>75 086</b>



Veri gizleme kapasitelerine ve karşılaştırma sonuçlarına bakıldığında önerilen algoritmaların sonuçlarının birbirine yakın değerler elde ettiği görülmektedir. SM-LSB algoritması, FL-LSB yöntemine göre daha fazla veri gizleyebilmiştir. Ancak bu yöntemde oluşturulan benzer görüntü içinden LSB seçilmesi için eşik değeri kullanılmıştır. Bu değer, çalışmada 0,5 olarak alınmıştır. Farklı değerler kullanıldığında ise gizli mesaj geri elde edilememiştir. Bu sebeple eşik değerinin optimize edilme zorunluğu vardır.

### 4.3. Önerilen Yöntemin Literatürdeki Çalışmalar ile Karşılaştırılması

Literatürde medikal verilerin güvenliğinin steganografi ile sağlanması ile ilgili çok fazla çalışma önerilmiştir. Bu sebeple, tez çalışmasının sonuçlarının karşılaştırılması için literatürden hastaya ait fizyolojik verileri görüntü içerisine saklayan benzer amaca sahip çalışmalar seçilmiştir. Çizelge 4.5’de tez çalışması ile literatürdeki uzay tabanlı yöntemlerin karşılaştırılması verilmiştir.

Çizelge 4.5. Tez çalışması ile literatürdeki uzay tabanlı yöntemlerin karşılaştırması

Yayınlar	Yöntem	PSNR (dB)	MSE	Görüntü	Gizli Mesaj	Şifreleme	Kapasite
Miaou ve ark. [106]	LSB	33 - 43		-	Hasta Bilgi+ EKG+Yorum+ Doktor Mührü	Var	-
Anand ve Niranjan [108]	LSB		0,009 0,002 0,008	128x128x3	Hasta Bilgi +EEG	Var	2 KB
Acharya ve ark. [84]	LSB	-	-	128x128x3 MR, Ultrason, Ang.	Hasta Bilgi+ EKG	Var	-
<b>Bu Tez Çalışması</b>	<b>SM-LSB</b>	<b>53,95- 62,50± 2,34</b>	<b>0,04 - 0,35 ± 0,08</b>	<b>176x176 256x256 248x320 320x320 424x512 448x448 464x512 512x512</b>	<b>Hasta Bilgi+ EEG+ Yorum</b>	<b>Var</b>	<b>6,80 KB* 15,33 KB 14,26 KB 24,27 KB 43,14 KB 48,31 KB 51,83 KB 63,32 KB</b>
<b>Bu Tez Çalışması</b>	<b>FL-LSB</b>	<b>53,87- 62,99± 2,44</b>	<b>0,04 - 0,36 ± 0,08</b>	<b>176x176 256x256 248x320 320x320 424x512 448x448 464x512 512x512</b>	<b>Hasta Bilgi+ EEG+ Yorum</b>	<b>Var</b>	<b>6,63 KB 15,25 KB 14,18 KB 24,11 KB 43,06 KB 48,06 KB 51,75 KB 63,07 KB</b>

\*KB=Kilo Bayt

Miaou ve arkadaşları yaptıkları çalışmada EKG verisi, doktor yorumu ve doktor mührünü medikal görüntü içerisinde gizlemeye çalışmıştır. Veri gizlemek için standart LSB tekniğini kullanmışlardır. PSNR değerleri 33-43 dB aralığındadır. Çalışmada gizlenen veri kapasitesi hakkında bilgi verilmemiştir [106]. Çizelge 4.5'te görüldüğü gibi bu tez çalışmasında önerdiğimiz SM-LSB yöntemi ile elde ettiğimiz PSNR değerleri 53,9520 dB ve 62,5025 dB aralığındadır. FL-LSB yöntemi ile elde ettiğimiz PSNR değerleri ise 53,8708 dB ve 62,9892 dB şeklindedir. Bu sonuçlar farklı çözünürlükteki görüntülerdeki maksimum veri gizleme sınırına göre elde edilmiştir. Daha az veri gizlendiğinde daha iyi sonuçlar elde edilecektir.

Acharya ve arkadaşları LSB yöntemi ile hasta bilgilerini, EKG ya da EEG biyolojik sinyallerini medikal görüntü içerisine gizlemişlerdir. Mesaj, Rijndael simetrik algoritması ile şifrelenmiştir [84].

Anand ve Niranjana görüntü bit uzayında LSB tekniği ile medikal görüntüler içerisinde mesaj gizlemiştir. EKG ya da EEG gibi sinyalleri içerecek metin dosyalarını aralıklı olarak seçilen görüntü LSB'lerine saklamışlardır. Ancak gizlenen mesajın kapasite miktarları çok düşüktür [108]. Bu tez çalışmasında oluşturulan veri setinde 128x128 çözünürlükte görüntü bulunmamaktadır. Ancak en düşük çözünürlükteki 176x176 boyutlu görüntülerde sırasıyla SM-LSB yöntemi ile 6,80 kilo bayt (KB), FL-LSB yöntemi ile 6,63 KB veri saklanmıştır. Elde edilen istatistiksel karşılaştırmalara göre LSB yöntemini geliştirmek için önerilen SM-LSB ve FL-LSB yöntemleri fazla miktarda veriyi yüksek PSNR değerleri elde ederek saklamıştır.

Çizelge 4.6'da ise çalışmada önerilen yöntemler ile literatürde benzer amaca sahip olan dönüşüm tabanlı yöntemleri kullanan çalışmalar karşılaştırılmıştır. Bu çalışmada dönüşüm tabanlı yöntemler mesaj gizleme kapasitelerinin azlığı ve yüksek işlem maliyetleri sebebiyle tercih edilmemiştir. Çizelge 4.6'dan da görüldüğü gibi çalışmada önerdiğimiz SM-LSB ve FL-LSB yöntemleri dönüşüm tabanlı yöntemlere göre çok fazla veri gizlemiştir.

Giakoumaki ve arkadaşları geliştirdikleri dalgacık tabanlı algoritmayı 512x512x20 adet görüntü ile test etmişlerdir. Ortalama PSNR değerleri, yaklaşık 668 bayt (5 348 bit) mesaj için  $46,66 \pm 0,2$  dB'dir [107].

Çizelge 4.6. Tez çalışması ile literatürdeki dönüşüm tabanlı yöntemlerin karşılaştırması

Yayımlar	Yöntem	PSNR (dB)	MSE	Görüntü	Gizli Mesaj	Şifreleme	Kapasite
Giakoumaki ve ark. [107]	DWT	46,66±0,2	-	512x512x20 MR, PET	Hasta Bilgi + ASCII text veri	Var	668 bayt (5 348 bit)
Nambakhsh ve ark. [82, 83]	DWT	48,15±0,22	-	256x256x25 PET	Hasta Bilgi + EKG	Var	2 KB
Acharya ve ark. [109]	DCT	-	0,70 0,53 0,50	196x260 MR 200x265 Ang. 200x265 Ultrason	Hasta Bilgi+ EKG	Var	-
<b>Bu Tez Çalışması</b>	<b>SM-LSB</b>	<b>53,95-62,50±2,34</b>	<b>0,04 - 0,35 ± 0,08</b>	<b>176x176 256x256 248x320 320x320 424x512 448x448 464x512 512x512</b>	<b>Hasta Bilgi+ EEG+ Yorum</b>	<b>Var</b>	<b>6,80 KB 15,33 KB 14,26 KB 24,27 KB 43,14 KB 48,31 KB 51,83 KB 63,32 KB</b>
<b>Bu Tez Çalışması</b>	<b>FL-LSB</b>	<b>53,87-62,99±2,44</b>	<b>0,04 - 0,36 ± 0,08</b>	<b>176x176 256x256 248x320 320x320 424x512 448x448 464x512 512x512</b>	<b>Hasta Bilgi+ EEG+ Yorum</b>	<b>Var</b>	<b>6,63 KB 15,25 KB 14,18 KB 24,11 KB 43,06 KB 48,06 KB 51,75 KB 63,07 KB</b>

Nambakhsh ve arkadaşları dalgacık tabanlı algoritma ile EKG verilerini 256x256x25 PET görüntüleri içerisinde gizlemişlerdir. PSNR değerleri 2 kilo bayt mesaj için 48,15±0,22 şeklindedir [82, 83]. Bu çalışmada ise 256x256 boyutlu görüntülerde sırasıyla SM-LSB yönteminde 15,33 KB ve FL-LSB yönteminde 15,25 KB veri saklanmıştır. Yaptığımız çalışmada ise PSNR değerleri SM-LSB yönteminde sırasıyla en az 53,95 dB ve FL-LSB yönteminde 53,87 dB olarak elde edilmiştir.

Acharya ve arkadaşları farklı bir çalışmalarında da frekans düzleminde DCT katsayılarına LSB yöntemi ile veri gizlemişlerdir. Katsayıları RLE (Run Length) kullanarak şifrelemişlerdir. Huffman sıkıştırma kullanarak da verilerin kayıt alanını azaltmaya çalışmışlardır. Ancak, frekans düzleminde gerçekleştirilen işlemlerin maliyeti görüntü bit uzayına göre daha fazladır. Aynı zamanda saklanan mesaj kapasitesi de daha azdır. Ayrıca çalışmada verilen taşıyıcı ve gömülü görüntülerin histogramlarındaki değişim göze çarpmaktadır [109].

Bu tez çalışmasında Çizelge 2.2’de verilen her bir hastanın farklı çözünürlükteki DICOM görüntülerinin tümünde eş zamanlı olarak mesaj gizlenmiştir. Çalışmanın en temel amacı medikal verileri bir ortamda birleştirmektir. Bu sebeple mesaj gizleme kapasitesi daha fazla olan görüntü bit uzayında gerçekleştirilen LSB tekniğinin geliştirilmesi üzerine çalışılmıştır.

LSB yönteminde pikseller sıralı olarak seçilmektedir ve geliştirilen SM-LSB ve FL-LSB yönteminde ise sıralı olmayan bir seçim söz konusudur. Gizlenen mesajın saldırılar sonucunda ele geçirilmesini engellemek için ise simetrik şifreleme ve sıkıştırma yöntemleri kullanılmıştır. Her DICOM görüntü içerisinde hasta kişisel bilgileri, doktor yorumu, bölütlenen EEG, EEG zaman boyutu ve EEG dosya başlığında yer alan bilgiler gizlenmiştir.

Gizlenen EEG verileri tüm DICOM serisinden toplanarak görüntülenmiştir. Oluşturulan gömülü DICOM görüntülerinin başlık kısımlarında hastanın kişisel bilgileri bulunmamaktadır ve bu kişisel bilgilere ancak yetkisi olan kullanıcılar erişebilmektedir. Çalışmada önerilen SM-LSB ve FL-LSB yöntemleri istatistiksel analizler sonucunda birbirine yakın değerler elde etmiştir. Ancak SM-LSB yönteminde kullanılan normalizasyon katsayısının ve piksel seçiminde kullanılan eşik değerinin optimize edilmesi gerekmektedir. Bu sebeple herhangi bir optimizasyon gerektirmeyen FL-LSB yöntemi çoklu medikal sinyallerin bir ortamda birleştirilmesi ve medikal veri güvenliğinin sağlanması için önerilmiştir.

Geliştirilen FL-LSB yöntemi ile literatürdeki çalışmalara göre daha fazla veri, daha yüksek PSNR değerleri ile gizlenmiştir. Ortalama PSNR değerleri 53,8708 dB ve 62,9892 dB  $\pm$  2,4389 aralığındadır. Ortalama R değerleri 0,8141 ile 0,9993  $\pm$  0,0586 arasındadır. Ayrıca HVS sistemi dikkate alınarak geliştirilen SSIM, UQI karşılaştırmaları da yapılmıştır. Bu çalışmada gömülü görüntülerin SSIM değerleri, 0,999459 ile 0,999933  $\pm$  0,000119 aralığında ve UQI değerleri, 0,999378 ile 0,999933  $\pm$  0,000140 aralığında elde edilmiştir. Buna göre gömülü görüntüler ve taşıyıcı görüntüler arasındaki benzerlik çok yüksektir. Çalışmada gömülü ve taşıyıcı görüntülerin frekans düzleminde karşılaştırmasını sağlayan PSNR-HVS ve PSNR-HVSM analizleri de gerçekleştirilmiştir. Ortalama PSNR-HVS değerleri 50,3448 ile 55,3289  $\pm$  1,3461, PSNR-HVSM ise 43,2412 ile 47,0753  $\pm$  1,1013 arasında bulunmuştur.

Ancak alıřmada nerilen SM-LSB ve FL-LSB algoritmalarının mesaj saklama sınırı kullanılan grntnn boyutuna baėlıdır. Bu sebeple yaklaşık 20-30 dakika arasında kayıt edilen EEG verilerinin hepsi gizlenememiřtir.

## 5. SONUÇ VE ÖNERİLER

Medikal veriler açık ağlarda, İnternet'te ya da özel ağlarda tehdit altındadır. Günümüzde, medikal veri güvenliği kriptoloji ve steganografi teknikleri kullanılarak sağlanmaktadır. Ancak şifrelenen veriler veri iletimindeki bit değişimlerine ve kayıplarına karşı hassastırlar.

Bu çalışmada medikal veri güvenliği için Benzerlik-Tabanlı LSB (SM-LSB) ve Bulanık Mantık-Tabanlı LSB (FL-LSB) isimli iki yeni algoritma önerilmiştir. Çalışmanın temel amacı çoklu medikal sinyallerin tek bir ortamda birleştirilmesini sağlamaktır. Bunun için Gazi Üniversitesi Nöroloji Bölümü'ne başvuran 22 epilepsi hastasına ait EEG ve MR görüntüleri toplanmıştır. Çalışmada Visual Studio. NET 2010 platformu kullanılarak geliştirilen DicomPinhan isimli yazılım ile önerilen yöntemlerle veri gizleme ve veriyi elde etme aşamalarının gerçekleştirilmesi, analiz ve karşılaştırmaların yapılması sağlanmıştır.

Çalışmada 22 epilepsi hastasına ait farklı çözünürlükteki (176x176, 256x256, ... , 512x512) DICOM görüntüler, taşıyıcı görüntüler olarak kullanılmıştır. Gizli mesaj ise hastaya ait bu görüntülerin her birinin başlık kısmından elde edilen kişisel bilgiler (hastanın adı, verilen numarası, hasta doğum tarihi, cinsiyeti, yaşı, ağırlığı ve adresi, çekim tarihi, saati, numarası, görüntünün yapısı ve tanımı, serinin tarihi, saati ve tanımı), doktor yorumu ve her görüntünün boyutuna göre bölütlenen EEG verisi şeklindedir. Aynı zamanda geliştirilen yazılım ile sadece kişisel bilgiler ve doktor yorumundan oluşan mesaj da görüntülere gizlenebilmektedir. Çalışmada, her bir DICOM görüntüden, hasta kişisel bilgileri ayrı ayrı alınmıştır. Bölütlenen EEG verisi, uzunluğu ve EEG başlık bilgileri de mesaja eklenmiştir. Oluşturulan gizli mesaj, saldırılara karşı LZW ve Huffman kayıpsız sıkıştırma algoritmaları ile önce sıkıştırılmış, ardından Rijndael simetrik şifreleme algoritması ile 128 bitlik anahtar aracılığıyla şifrelenmiştir. Veri gizleme sonucunda oluşturulan gömülü görüntülerin başlık kısımlarından hasta kişisel bilgileri silinmiştir. Bu bilgilere ancak yetkili olan kullanıcıların erişmesi sağlanmıştır.

Bu tez çalışmasında önerilen SM-LSB ve FL-LSB algoritmalarının temel amacı [0 1] aralığında piksellerin gri seviye farklarına göre yerel benzerlik değerlerini tespit etmektir ve bu benzerlik değerlerini LSB seçiminde kullanmaktır.

SM-LSB yöntemi ile Öklid uzaklığı kullanılarak hesaplanan benzerlik değerleri, eğer belli bir eşik değerinin üzerinde ise LSB olarak seçilmiştir. FL-LSB yönteminde ise eşik değeri olmaksızın LSB seçimi gerçekleştirilmiştir. Çalışmada taşıyıcı ve gömülü görüntülerin karşılaştırılması için MSE, PSNR, SSIM, UQI ve R istatistiksel analizleri gerçekleştirilmiştir. İstatistiksel analizlerin hepsi farklı çözünürlükteki görüntülerdeki maksimum veri gizleme kapasitesine göre yapılmıştır.

SM-LSB yöntemi ile ortalama PSNR değerleri en az 53,9520 dB ve en çok 62,5025 dB  $\pm$  2,3441 aralığında elde edilmiştir. MSE değerleri 0,0428 ile 0,3535  $\pm$  0,0786 aralığında bulunmuştur. Ortalama R değerleri 0,7173 ile 0,9992  $\pm$  0,0795 arasındadır. Ancak görüntü analizinde, insan görme sistemini daha iyi yansıtan SSIM ve UQI analizleri, R analizinden daha yaygın olarak kullanılmaktadır. SSIM değerleri 0,999459 ile 0,999932  $\pm$  0,000122 aralığında ve UQI değerleri ise 0,999378 ile 0,99993  $\pm$  0,000143 aralığında elde edilmiştir.

FL-LSB yönteminde ortalama PSNR değerleri 53,8708 dB ve 62,9892 dB  $\pm$  2,4389 aralığındadır. Ortalama MSE değerleri 0,0428 ve 0,3598  $\pm$  0,08123 olarak bulunmuştur. Ortalama R değerleri 0,8141 ile 0,9993  $\pm$  0,0586 arasındadır. Ortalama SSIM değerleri, 0,999459 ile 0,999933  $\pm$  0,000119 aralığında ve UQI değerleri, 0,999378 ile 0,999933,  $\pm$  0,000140 aralığında elde edilmiştir. Ortalama R değerleri 0,8141 ile 0,9993  $\pm$  0,0586 arasındadır. R değerleri daha düşük olarak elde edilmiş olsa da insan görme sistemini daha iyi yansıtan SSIM ve UQI değerleri çok yüksektir. Elde edilen sonuçlara göre gömülü görüntüler ve taşıyıcı görüntüler arasındaki farklılık gözle görülmeyecek kadar çok küçüktür. Çalışma dahilinde gerçekleştirilen histogram analizleri de bunu desteklemektedir. Ayrıca çalışmadaki tüm analizler maksimum veri gizleme kapasitesine göre gerçekleştirilmiştir. Daha az veri gizleme gerçekleştirildiğinde tüm istatistiksel analiz değerleri de yükselecektir.

Çalışmada 176x176 çözünürlükteki MR görüntülerinde sırasıyla SM-LSB yöntemi ile 6,80 KB ve FL-LSB yöntemi ile 6,63 KB veri gizlenmiştir. 512x512 çözünürlükteki MR görüntülerinde sırasıyla SM-LSB yöntemi ile 63,32 KB ve FL-LSB yöntemi ile 63,07 KB veri gizlenmiştir.

Çalışmada LSB yöntemini geliştirmek için önerilen SM-LSB ve FL-LSB yöntemlerinin elde ettiği istatistiksel sonuçlar birbirine çok yakındır. İki yöntemde LSB tekniğinin genel özellikleri olan algılanamamazlık ve yüksek kapasiteyi sağlamıştır. Ancak SM-LSB yöntemi LSB seçiminde kullanılan ve optimize edilmesi gereken eşik değerine sahiptir. Bu sebeple, çalışmada FL-LSB yöntemi farklı medikal verilerin bir ortamda güvenliklerinin sağlanarak birleştirilmesi için önerilmiştir.

Geliştirilen FL-LSB yönteminin analiz sonuçları ve kapasitesi literatürde önerilen benzer amaca sahip olan çalışmalarından daha yüksektir. Önerilen FL-LSB yöntemi ile elde edilen sonuçlar ışığında, kişisel bilgilerin güvenilirliği sağlanmış, medikal veriler tek bir ortamda birleştirildiğinden gereken veri kayıt miktarı ve veri iletimi için kullanılan bant genişliği azaltılmıştır.

Gelecekte, EEG verisi üzerinde gürültü giderme ve veri azaltma teknikleri (Temel Bileşenler Analizi, Bağımsız Bileşenler Analizi, vb.) kullanılarak FL-LSB yöntemi ile EEG verisinin tam olarak gizlenilmesi sağlanabilir.





## KAYNAKLAR

1. Coatrieux, G., Maitre, H., Sankur, B., Rolland, Y., and Collorec, R. (2000). *Relevance of Watermarking in Medical Imaging*. Paper presented at the Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 IEEE EMBS International Conference on, Arlington, VA, 250-255.
2. İnternet: Electronic Health Records Overview. URL: <http://www.himss.org/files/HIMSSorg/content/files/Code%20180%20MITRE%20Key%20Components%20of%20an%20EHR.pdf>, Son Erişim Tarihi: 01.07.2015.
3. İnternet: Sherley, L. Medical Data Has Become the Next Cybersecurity Target. URL: <https://www.benton.org/headlines/medical-data-has-become-next-cybersecurity-target>, Son Erişim Tarihi: 01.07.2015.
4. İnternet: Electronic Health Record. URL: [http://en.wikipedia.org/wiki/Electronic\\_health\\_record](http://en.wikipedia.org/wiki/Electronic_health_record), Son Erişim Tarihi: 01.07.2015.
5. İnternet: EHR (Electronic Health Record) - ESK (Elektronik Sağlık Kaydı). URL: <http://www.saglik.gov.tr/DH/belge/1-29721/ehr-electronic-health-record---esk-elektronik-saglik-ka-.html>, Son Erişim Tarihi: 01.07.2015.
6. Boyacı, A., Ulaş, M. (2007, Şubat). *PACS ve Medikal Görüntülerin Sayısal Olarak Arşivlenmesi*. Akademik Bilişim 2007 Sempozyumunda sunuldu, Dumlupınar Üniversitesi, Kütahya, 305-310.
7. Haidekker, M.A. (2011). *Image Storage, Transport, and Compression (Edition: 1)*. Wiley-IEEE Press, 386-412.
8. Tasbas, E. (2011). *Sağlık Bakanlığı Standartlarına Uygun PACS Teknik Sarnamesi Hazırlama Yazılımı*, Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü, İzmir, 5-10.
9. Onbay, T.U. (2009). *Dağıtık PACS Sistemleri Üzerinden Tıbbi Görüntülere Erişimin Sağlanması*, Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir, 1-63.
10. Kuang, L.-Q., Zhang, Y., Han, X. (2009). *Watermarking Image Authentication in Hospital Information System*. Paper presented at the Information Engineering and Computer Science, 2009. ICIECS 2009. International Conference on, 1-4.
11. İnternet: DICOM. URL: <http://en.wikipedia.org/wiki/DICOM>, Son Erişim Tarihi: 01.07.2015.
12. İnternet: DICOM. URL: <http://medical.nema.org/>, Son Erişim Tarihi: 01.07.2015.
13. Ulaş, M., Boyacı, A. (2007). *DICOM Görüntü Standardı*. Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı Bildirileri Sempozyumunda sunuldu, Dumlupınar Üniversitesi, Kütahya, 69-74.

14. İnternet: Oosterwijk, H. (2010). The DICOM standard, overview and characteristics. URL: [http://www.ringholm.com/docs/02010\\_en.htm](http://www.ringholm.com/docs/02010_en.htm), Son Erişim Tarihi: 01.07.2015.
15. İnternet: About Dicom, The National Electrical Manufacturers Association (NEMA). URL: <http://medical.nema.org/Dicom/about-DICOM.html>, Son Erişim Tarihi: 01.07.2015.
16. Karakiş, R., Güler, İ., Çapraz, İ., ve Bilir, E. (2015). *Medikal Sinyaller için Benzerlik Tabanlı Görüntü Steganografi Uygulaması*. Akademik Bilişim Sempozyumunda sunuldu, Eskişehir.
17. İnternet: An introduction to the DICOM single-file format. URL: <http://www.cabiatl.com/mricro/dicom/index.html>, Son Erişim Tarihi: 01.07.2015.
18. Nyeem, H., Wageeh Boles, W., and Boyd, C. (2013). A Review of Medical Image Watermarking Requirements for Teleradiology. *J. Digit. Imaging*, 26, 326-343.
19. Karakiş, R., Güler, İ., Çapraz, İ., ve Bilir, E. (2015). *A New Method of Fuzzy Logic-Based Steganography for the Security of Medical Images*. Paper presented at the Signal Processing and Communications Applications Conference (SIU), 2015 23rd, Malatya, 176-179.
20. Cheddad, A., Condell, J., Curran, K., and McKeivitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, 90, 727-752.
21. Lin, E.T., Delp, E.J. (1999). A review of data hiding in digital images. *CERIAS Tech Report 2001-139*. 1-5.
22. Şahin, A. (2007). *Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri*, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, 7-90.
23. Doğan, F. (2012). *Medikal Görüntüler İçerisine Hasta Bilgilerinin Gizlenmesi*, Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya, 1-39.
24. Ünlü, O. (2012). *Ortam ve Yöntem Bağımsız Steganografik Kütüphane Tasarımı*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 1-30.
25. Kurtuldu, Ö. (2008). *İmge Steganografisi için Yeni Yöntemler*, Yüksek Lisans Tezi, Deniz Harp Okulu Deniz Bilimleri ve Mühendisliği Enstitüsü, İstanbul, 1-23.
26. Yalman, Y. (2010). *Sayısal Görüntüler için Histogram Temelli Veri Gizleme Yöntemi ve Uygulama Yazılımı*, Doktora Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Kocaeli, 1-48.
27. Tuncer, T. (2011). *Resimler için Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları*, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ, 1-35.

28. Rathi, S.C. (2012). *Medical Image Authentication through Watermarking Preserving ROI*, Master Thesis, Department of Computer Engineering and Information Technology College of Engineering, Pune, 1-27.
29. Yalman, Y., Özdemir, Ç., Ertürk, İ., ve Akar, F. (2014). *Veri Gizleme*. Beta Basım A.Ş., İstanbul, ISBN 978-605-333-141-4, 1-107.
30. Şatır, E. (2013). *Bilgi Güvenliği için Metin Steganografisinde Yeni bir Yaklaşım*, Doktora Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya, 1-80.
31. Li, B., He, J., Huang, J., and Shi, Y.Q. (2011). A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, 2 (2), 142-172.
32. Yalman, Y., Ertürk, İ. (2009). *İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulaması*. XI. Akademik Bilişim Konferansları Sempozyumunda sunuldu, Harran Üniversitesi, Şanlıurfa, 537-544.
33. Petitcolas, F.A.P, Anderson, R.J., and Kuhn, M.G. (1999). *Information Hiding-A Survey*. Paper presented at the Proceedings of the IEEE, special issue on protection of multimedia content, 87 (7), 1062–1078.
34. Şahin, A., Buluş, E., ve Sakallı, M.T. (2006). *Gri Seviye Resimler Üzerinde Rasgele LSB Yöntemini ve Sayı Teorisini Kullanarak Bilgi Gizleme ve Steganaliz*. Akademik Bilişim Konferansları 2006-AB2006 Sempozyumunda sunuldu, Denizli-Türkiye.
35. Yalman, Y., Akar, F., and Erturk, I. (2012). *Recent Advances in Steganography, (Chapter 4: Contemporary Approaches To The Histogram Modification Based Data Hiding Techniques)*, InTech Open Access Publisher, ISBN: 978-953-51-0840-5, 53-74.
36. Johnson, N.F., Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. *IEEE Computer*, 31 (2), 26-34.
37. İnternet: Johnson, N.F., Katzenbeisser, S.C. Chapter 3. A survey of steganographic techniques. URL: <http://www.artechhouse.com/uploads/public/documents/chapters/petitcolas035-ch03.pdf>, Son Erişim Tarihi: 01.07.2015.
38. Hamid, N., Yahya, A., Ahmad R.B., and Al-Qershi, O.M. (2012). Image Steganography Techniques: An Overview. *International Journal of Computer Science and Security (IJCSS)*, 6 (3), 168-187.
39. Amirtharajan, R., Akila, R., and Deepikachowdavarapu, P. (2010). A Comparative Analysis of Image Steganography. *International Journal of Computer Applications (0975 – 8887)*, 2 (3), 41-47.

40. Cetin, O., Ozcerit, A.T. (2009). A new steganography algorithm based on color histograms for data embedding into raw video streams. *Computers & Security*, 28, 670-682.
41. Şahin, A., Buluş, E., Sakallı, M.T. (2006). 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. *Trakya Univ. J. Sci.*, 7 (1), 17-22.
42. Arica, N., Kurtuldu, Ö. (2009). Image steganography by wavelet matching. *Journal of Electronic Imaging*, 18 (3), 033013-1-9.
43. Kurtuldu, Ö., Arica, N. (2009). İmge Kareleri Kullanan Yeni Bir Steganografi Yöntemi. *Journal of Naval Science and Engineering*, 5 (1), 107-118.
44. Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R. (2003). *Information hiding using steganography*. Paper presented at the Telecommunication Technology 2003. NCTT 2003 Proceedings. 4th National Conference on, 21-25.
45. Karakiş, R., Güler, I. (2014). *An Application of Fuzzy Logic-Based Image Steganography*. Paper presented at the Signal Processing and Communications Applications Conference (SIU), 2014 22nd, Trabzon, 156-159.
46. Coatrieux, G., Lecornu, L., Sankur, B., and Roux, C. (2006). *A Review of Image Watermarking Applications in Healthcare*. Paper presented at the Engineering in Medicine and Biology Society, 2006. EMBS '06. 28th Annual International Conference of the IEEE, 4691-4694.
47. Navas, K. A., Sasikumar, M. (2007). *Survey of Medical Image Watermarking Algorithms*. Paper presented at the SETIT 2007 4rth International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, TUNISIA, 1-6.
48. Abdullatif, M., Zeki, A.M., and Chebil, J. (2013). *Wavelet Watermarking On Medical Images*. Paper presented at the Proceeding of the International Conference on Artificial Intelligence in Computer Science and ICT(AICS 2013), 147-156.
49. Joshi, I., Pawar, V.N. (2014). Secure Medical Image Watermarking. *International Journal of Research in Advent Technology*, 2 (42), 266-42.
50. Mavudila, R., Masmoudi, Lh., Cherkaoui, M., Hamri, M., and Hassanain, N. (2012). Medical Image Watermarking Based on M-band Wavelet Transform. *International Journal of Modern Engineering Research (IJMER)*, 2 (4), 2711-2718.
51. Giakoumaki, A., Perakis, K., Banitsas, K., Giokas, K., Tachakra, S., and Koutsouris, D. (2010). Using Digital Watermarking to Enhance Security in Wireless Medical Image Transmission. *Telemedicine and E-Health*, 16 (3), 306-313.
52. Li, M., Narayanan, S., and Poovendran, R. (2004). *Tracing medical images using multi-band watermarks*. Paper presented at the Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE, 2, 3233-3236.

53. Jiao, S., Goutte, R. (2010). Secure Transfer of Identification Information in Medical Images by Steganocryptography. *Int. J. Communications, Network and System Sciences*, 3, 801-804.
54. Fakhari, P., Vahedi, E., and Lucas, C. (2011). Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. *Digital Signal Processing*, 21, 433-446.
55. Yang, M., Song, L., Trifas, M., Buenos-Aires, D., Chen, L., and Elston, J. (2010). Secure Patient Information and Privacy in Medical Imaging. *Systemics, Cybernetics And Informatics*, 8 (3), 63-66.
56. Ravali, K., Kumar A.P., and Asadi, S., (2011). Carrying Digital Watermarking for Medical Images using Mobile Devices. *IJCSET*, 1 (7), 366-369.
57. Rahimi, F., Rabbani, H. (2011). A dual adaptive watermarking scheme in contourlet domain for DICOM image., *BioMedical Engineering OnLine*, 10 (53), 1-18.
58. Memon, N.A., Gilani, S.A.M. (2011). Watermarking of chest CT scan medical images for content authentication, *International Journal of Computer Mathematics*, 88 (2), 265-280.
59. Zain, J.M., Fauzi, A.R.M., and Aziz, A.A. (2006). *Clinical Evaluation of Watermarked Medical Images*. Paper presented at the Proceedings of the 28th IEEE EMBS Annual International Conference, New York City, USA, 5459- 5462.
60. Shukla, A., Singh, C. (2014). Medical Image Authentication Through Watermarking. *International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)*, 2 (2), 292-295.
61. Nyeem, H., Boles, W., and Boyd, C. (2015). Content-independent embedding scheme for multi-modal medical image watermarking. *BioMedical Engineering OnLine 2015*, 14 (7), 1-19.
62. Fatemizadeh, E., Maneshi, M. (2012). A New Watermarking Algorithm Based On Human Visual System For Content Integrity Verification of Region of Interest. *Computing and Informatics*, 31, 877-899.
63. İnternet: Zaim, J.M., İstepanian, R.S.H. Digital Watermarking in Wireless Telemedical Environment. 1-3. URL: [http://umpir.ump.edu.my/928/1/13\\_JMZ\\_digital.pdf](http://umpir.ump.edu.my/928/1/13_JMZ_digital.pdf), Son Erişim Tarihi: 01.07.2015.
64. Raul, R.-C., Claudia, F.-U., and Trinidad-Bias, G.J. (2007). *Data Hiding Scheme for Medical Images*. Paper presented at the Electronics, Communications and Computers, CONIELECOMP '07. 17th International Conference on, 32-37.
65. Pandey, V., Singh, A., and 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.

66. Mortazavian, P., Jahangiri, M., and Fatemizadeh, E. (2004). *A Low-Degradation Steganography Model for Data Hiding in Medical Images*. Paper presented at the Proceeding of the Fourth IASTED International Conference Visualization, Imaging, and Image Processing, 914-920.
67. Viswanathan, P., Venkata Krishna, P. (2009). *Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication*. Paper presented at the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, 585-589.
68. Navas, K.A, Sasikumar, M., and Sreevidya, S. (2007). *A Benchmark for Medical Image Watermarking*. Paper presented at the Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services., 14th International Workshop on, 237- 240.
69. Koley, S., Pal, K., Ghosh, G., and Bhattacharya, M. (2014). Secure Transmission and Recovery of Embedded Patient Information from Biomedical Images of Different Modalities through a Combination of Cryptography and Watermarking. *I.J. Image, Graphics and Signal Processing*, 3, 18-31.
70. Umeda, T., Okawa, A., and Gomi, T. (2014). *Security Model for Secure Transmission of Medical Image Data Using Steganography*. Integrating Information Technology and Management for Quality of Care, IOS Press, doi:10.3233/978-1-61499-423-7-311.
71. Huang, S.-C., Lin, M.-S. (2010). A High-capacity Reversible Data-hiding Scheme for Medical Images. *Journal of Medical and Biological Engineering*, 30(5), 289-296.
72. Ni, Z., Shi, Y.Q., Ansari N., and Su, W. (2006). Reversible data hiding. *IEEE Trans.Circ.Syst.Video Technol.*, 16, 354-362.
73. Tseng, H.W., Hsieh, C.P. (2008). Reversible data hiding based on image histogram modification. *Imaging Sci. J.*, 56, 271-278.
74. Lin, C.C., Tai W.L., and Chang, C.C. (2008). Multilevel reversible data hiding based on histogram modification of difference images. *Pattern Recognit.*, 41, 3582-3591.
75. Huang, L.-C., Tseng, L.-Y., and Hwang, M.-S. (2012). The Study on Data Hiding in Medical Images. *International Journal of Network Security*, 14 (6), 301-309.
76. Huang, L.-C., Tseng, L.-Y., and Hwang, M.-S. (2013). A reversible data hiding method by histogram shifting in high quality medical images, *The Journal of Systems and Software*, 86, 716-727.
77. Lou, D.-C., Hu, M.-C., and Liu, J.-L. (2009). Multiple layer data hiding scheme for medical images, *Computer Standards & Interfaces*, 31, 329-335.
78. Fallahpour, M., Megias, D., and Ghanbari, M. (2011). Reversible and high capacity data hiding in medical images. *Image Processing- IET*, 5 (2), 190-197.

79. Tan, C.-K., Changwei Ng, J., Xu, X., Poh, C.L., Guan, Y.L., and Sheah, K. (2011). Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability. *Journal of Digital Imaging*, 24 (3), 528-540.
80. Ulutas, M., Ulutas, G., and Nabiyev, V.V. (2011). Medical image security and EPR hiding using Shamir's secret sharing scheme. *The Journal of Systems and Software*, 84, 341-353.
81. Usha, B.A., Srinath, N.K., Nanjangud, A., Deshpande, A.M., and Rebello, A. (2014). A Survey on Patient Information Protection Using Cryptographic and Data Hiding Techniques. *International Journal of Advanced Research in Computer and Communication Engineering*, 3 (4), 6334-6336.
82. Nambakhsh, M.S., Ahmadian, A., and Zaidi, H. (2011). A contextual based double watermarking of PET images by patient ID and ECG signal, *Computer Methods and Programs in Biomedicine*, 104 (3), 418-425.
83. Nambakhsh, M.S., Ahmadian, A., Ghavami, M., Dilmaghani, R.S., and Karimi-Fard, S. (2006). A Novel Blind Watermarking of ECG Signals on Medical Images Using EZW Algorithm. Paper presented at the Proceedings of the 28th IEEE-EMBS Annual International Conference New York City, USA, 3274-3277.
84. Acharya, R.U., Bhat, P.S., Kumar, S., and Min, L.C. (2003). Transmission and storage of medical images with patient information. *Computers in Biology and Medicine*, 33, 303-310.
85. Usha, B.A., Srinath, N.K., Nanjangud, A., Deshpande, A.M., and Rebello, A. (2014). A Survey on Patient Information Protection Using Cryptographic and Data Hiding Techniques. *International Journal of Advanced Research in Computer and Communication Engineering*, 3 (4), 6334-6336.
86. Li, Y., Li, C.-T., and Wei, C.-H. (2007). *Protection Of Mammograms Using Blind Steganography and Watermarking*, Paper presented at the Information Assurance and Security, IAS 2007. Third International Symposium on, 496-500.
87. Doğan, F., Güzeldereli, E.A., ve Çetin, Ö. (2013). Medikal görüntü içerisine tıbbi bilgilerin gömülmesi için yeni bir yaklaşım, *SAÜ. Fen Bil. Der.*, 17 (2), 277-286.
88. Öksüzoğlu, S. (2009). *Radyografik Görüntülere Veri Gizleme Uygulaması*, Elektrik-Elektronik-Bilgisayar ve Biyomedikal Mühendisliği 13. Ulusal Kongresi ve Fuarı Sempozyumunda sunuldu.
89. Nambakhsh, M.S., Ahmadian, A., and Zaidi, H. (2011). A contextual based double watermarking of PET images by patient ID and ECG signal. *Comput. Methods Programs Biomed.*, 104 (3), 418-25.
90. Lou, D.-C., Hu, M.-C., and Liu, J.-L. (2009). Multiple layer data hiding scheme for medical images. *Computer Standards & Interfaces*, 31, 329-335.



91. Puech, W. (2008). *Image Encryption and Compression for Medical Image Security*. Paper presented at the Image Processing Theory, Tools and Applications, 2008. IPTA 2008. First Workshops on, 1-2.
92. Pandey, V., Shrivastava, M. (2012). Secure Medical Image Transmission using Combined Approach of Data-hiding. Encryption and Steganography. *International Journal of Advanced Research in Computer Science and Software Engineering*, 2 (12), 54-57.
93. Keerthana, L., Venkataramanaiah, Mr.B. (2014). ECG Steganography Based Privacy Protection of Medical Datas for Telemedicine Application. *OSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, 4 (2), 46-51.
94. Ibaida, A., Khalil, I. (2013). Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems. *IEEE Transactions on Biomedical Engineering*, 60 (12), 3322-3330.
95. Mekala, R., Vanitha, S. (2014). Privacy Protection of Medical Datas Using ECG Steganography. *International Journal of Innovations in Scientific and Engineering Research (IJISER)*, 1 (4), 1-5.
96. Mai, V., Khalil, I., and Ibaida, A. (2013). *Steganography-based Access Control to Medical Data Hidden in Electrocardiogram*. Paper presented at the 35th Annual International Conference of the IEEE EMBS, Osaka, Japan, 1302- 1305.
97. Ibaida, A., Khalil, I., and Van, S.R. (2011). *A Low Complexity High Capacity ECG Signal Watermark for Wearable Sensor-Net Health Monitoring System*. Paper presented at the Proceedings of the Computing in Cardiology; Hangzhou, China, 393-396.
98. Ibaida, A., Khalil, I., and Al-Shammary, D. (2010). *Embedding Patients Confidential Data in ECG Signal For HealthCare Information Systems*. Paper presented at the 32nd Annual International Conference of the IEEE EMBS, Buenos Aires, Argentina, 3891-3894.
99. Suganya, N., Marimuthu, M. (2014). ECG Steganography Based Privacy Protecting of Medical Data for Telemedicine Application. *International Journal of Innovative Research in Computer and Communication Engineering*, 2 (1), 794-800.
100. Zheng, K., Qian. Xu. (2008). *Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms*. Paper presented at the 2008 International Conference on Computational Intelligence and Security, 295-299.
101. Sankari, V., Nandhini, K. (2013). Sharing of Patient confidential data using ECG steganography, *International Journal of Scientific & Engineering Research*, 4 (12), 2132-2137.

102. Nambakhsh, M.S., Ahmadian, A., Ghavami, M., Dilmaghani, R. S., and Karimi-Fard, S. (2006). *A Novel Blind Watermarking of ECG Signals on Medical Images Using EZW Algorithm*. Paper presented at the Proceedings of the 28th IEEE-EMBS Annual International Conference New York City, USA, 3274-3277.
103. Matam, B.R. (2009). *Watermarking biomedical time series data*. Phd Thesis, Aston University, 1-200.
104. Kong, X., Feng, R. (2001). Watermarking Medical Signals for Telemedicine. *IEEE Transactions on Information Technology in Biomedicine*, 5 (3), 195-201.
105. Ibaida, A., Khalil, I., and Sufi, F. (2009). *Cardiac Abnormalities Detection from Compressed ECG in Wireless Telemonitoring using Principal Components Analysis (PCA)*. Paper presented at the Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009 5th International Conference on, 207-212.
106. Miaou, S.-G., Hsu, C.-M., Tsai, Y.-S., and Chao, H.-M. (2000). *A secure data hiding technique with heterogeneous data-combining capability for electronic patient records*. Paper presented at the Engineering in Medicine and Biology Society, Proceedings of the 22nd Annual International Conference of the IEEE, 1, 280-283.
107. Giakoumaki, A., Pavlopoulos, S., and Koutsouris, D. (2006). Secure and efficient health data management through multiple watermarking on medical images. *Medical and Biological Engineering and Computing*, 44 (8), 619-631.
108. Anand, D., Niranjana, U.C. (1998). *Watermarking medical images with patient information*. Paper presented at the Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th Annual International Conference of the IEEE, 2, 703-706.
109. Acharya, U.R., Niranjana, U.C., Iyengar, S.S, Kannathal, N., and Min, L.C. (2004). Simultaneous storage of patient information with medical images in the frequency domain. *Computer Methods and Programs in Biomedicine*, 76 (1), 13-19.
110. Gonzalez, R.C, Woods R.E. (1993). *Digital Image Processing*. Reading, MA: Addison-Wesley.
111. İnternet: BMP file format. URL: [https://en.wikipedia.org/wiki/BMP\\_file\\_format](https://en.wikipedia.org/wiki/BMP_file_format), Son Erişim Tarihi: 01.07.2015.
112. İnternet: Şeker, Ş.E. Steganografi ve LSB. URL: <http://bilgisayarkavramlari.sadievrenseker.com/2009/06/05/steganografi-ve-lsb/>, Son Erişim Tarihi: 01.07.2015.
113. Çimen, C., Akleylek, S., ve Akyıldız, E. (2008). *Şifrelerin Matematiği Kriptografi*. Odtü Yayıncılık, Ankara, 1-50.
114. Elmas, Ç. (2007). *Yapay Zeka Uygulamaları*. Seçkin Yayıncılık Ankara, ISBN 9750206146, 261-316.

115. İnternet: Bulanık Mantık. URL: [http://tr.wikipedia.org/wiki/Bulan%C4%B1k\\_mant%C4%B1k](http://tr.wikipedia.org/wiki/Bulan%C4%B1k_mant%C4%B1k), Son Erişim Tarihi: 01.07.2015.
116. Baykal, N., Beyan, T. (2004). *Bulanık Mantık İlke ve Temelleri*, Bıçaklar Kitabevi, Ankara, ISBN 975-8695-08-8, 335-387.
117. İnternet: Huffman Kodu. URL: [https://tr.wikipedia.org/wiki/Huffman\\_kodu](https://tr.wikipedia.org/wiki/Huffman_kodu), Son Erişim Tarihi: 01.07.2015.
118. İnternet: Huffman Kodlaması (Huffman Encoding). URL: <http://bilgisayarkavramlari.sadievrenseker.com/2009/02/25/huffman-kodlamasi-huffman-encoding/>, Son Erişim Tarihi: 01.07.2015.
119. İnternet: LZW Sıkıştırma algoritması. URL: <http://bilgisayarkavramlari.sadievrenseker.com/2010/01/04/lzw-sikistirma-algoritmasi/>, Son Erişim Tarihi: 01.07.2015.
120. İnternet: Lempel–Ziv–Welch. URL: <https://en.wikipedia.org/wiki/Lempel%E2%80%93Ziv%E2%80%93Welch>, Son Erişim Tarihi: 01.07.2015.
121. İnternet: Huffman, D. (1952). *A Method for the Construction of Minimum-Redundancy Codes*. Paper presented at the Proceedings of the IRE 40 (9): 1098-1101. URL: [http://compression.ru/download/articles/huff/huffman\\_1952\\_minimum-redundancy-codes.pdf](http://compression.ru/download/articles/huff/huffman_1952_minimum-redundancy-codes.pdf), Son Erişim Tarihi: 01.07.2015.
122. İnternet: Pixel. URL: <http://en.wikipedia.org/wiki/Pixel>, Son Erişim Tarihi: 01.07.2015.
123. Demirci, R. (2007). Similarity relation matrix-based color edge detection. *Int. J. Electron. Commun. (AEÜ)*, 61, 469-477.
124. Elmas, Ç., Demirci, R., and Güvenç, U. (2013). Fuzzy diffusion filter with extended neighborhood, *Expert Systems with Applications*, 40, 866-872.
125. Güvenç, U. (2008). *Uyarlanabilir Görüntü Filtre Tasarımı*. Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara. 54-108.
126. Wu, D.-C., Tsai, W.-H. (2003). A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24 (9-10), 1613-1626.
127. Li, Y.C., Yeh, C.-M., and Chang, C.C. (2010). Data hiding based on the similarity between neighboring pixels with reversibility. *Digital Signal Processing*, 20 (4), 1116-1128.
128. Güler, İ., Toprak, Demirhan, A., ve Karakış, R. (2008). MR images restoration with the use of fuzzy filter having adaptive membership parameters. *Journal of Medical Systems*, 32 (3), 229-234.

129. Demirhan, A., Güler, İ. (2014). *Automatic Segmentation Of Tumor, Edema And Healthy Tissues Of Brain Using Neuro Fuzzy Inference System*, Paper presented at the 2014 IEEE 22nd Signal Processing and Communications Applications Conference (SIU 2014), Trabzon, 120-123.
130. İnternet: Structural similarity. URL: [http://en.wikipedia.org/wiki/Structural\\_similarity](http://en.wikipedia.org/wiki/Structural_similarity), Son Erişim Tarihi: 01.07.2015.
131. Wang, Z., Bovik, A.C. (2002). A Universal Image Quality Index. *IEEE Signal Processing Letters*, 9 (3), 81-84.
132. İnternet: Miranda Neto, A., Correa Victorino, A., Fantoni, I., Zampieri, D. E., Ferreira, J.V., and Lima, I.D.A. (2013). Image Processing Using Pearson's Correlation Coefficient: Applications on Autonomous Robotics. URL: [https://hal.inria.fr/file/index/docid/860912/filename/Image\\_Processing\\_Using\\_Pearson\\_s\\_Correlation\\_Coefficient\\_-\\_Applications\\_on\\_Autonomous\\_Robotics\\_final.pdf](https://hal.inria.fr/file/index/docid/860912/filename/Image_Processing_Using_Pearson_s_Correlation_Coefficient_-_Applications_on_Autonomous_Robotics_final.pdf), Son Erişim Tarihi: 01.07.2015.
133. Egiazarian, K., Astola, J., Ponomarenko, N., Lukin, V., Battisti, F., and Carli, M. (2006) *New full-reference quality metrics based on HVS*. Paper presented at the Proc. of the II. International Workshop on VPQM, 4, 1-4.
134. İnternet: TID2008 page. URL: <http://www.ponomarenko.info/tid2008.htm>, Son Erişim Tarihi: 01.07.2015.



**EKLER**

## EK-1. Etik kurul



**GAZİ ÜNİVERSİTESİ (GİRİŞİMSEL OLMAYAN) KLİNİK ARAŞTIRMALAR ETİK KURULU  
DEĞERLENDİRME FORMU**

DEĞERLENDİRME KURULUNUN ADI	Gazi Üniversitesi Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu
AÇIK ADRES	Gazi Üniversitesi Tıp Fakültesi Dekanlık Binası 06500 Beşevler/Ankara
TELEFON	0312 202 69 58
FAKS	0312 202 46 73
E-POSTA	tipetikkurul@gazi.edu.tr

BAŞVURU BİLGİLERİ	ARAŞTIRMANIN AÇIK ADI	Epileptik Odakların Elektroensefalogram ve Manyetik Rezonans Görüntüsü Verileri ile Lokalize Edilmesi		
	SORUMLU ARAŞTIRMACI ÜNVANI/ADI/SOYADI	Prof.Dr.Erhan BİLİR		
	UZMANLIK TEZİ/AKADEMİK AMAÇLI	UZMANLIK TEZİ <input type="checkbox"/>	AKADEMİK AMAÇLI <input type="checkbox"/>	
		DİĞER <input type="checkbox"/>	<b>Doktora Tezi</b>	
	İLAÇ DIŞI ARAŞTIRMA	<input checked="" type="checkbox"/>	<input type="checkbox"/> İLAÇ DIŞI GİRİŞİMSEL <input checked="" type="checkbox"/> İLAÇ DIŞI GİRİŞİMSEL OLMAYAN 3-Dosya ve görüntü kayıtları kullanılarak yapılan retrospektif çalışmalar ve arşiv taramaları 4-Rutin takip ve tedavi sırasında elde edilmiş materyallerle yapılacak araştırmalar	

DEĞERLENDİRİLEN BELGELER	Belge Adı	Tarihi	Versiyon No	Dili
	ARAŞTIRMA PROTOKOLÜ			
BİL. GÖNÜLLÜ OLUR FORMU				Türkçe <input checked="" type="checkbox"/> İngilizce <input type="checkbox"/> Diğer <input type="checkbox"/>
DEĞERLENDİRİLEN DİĞER BELGELER	Belge Adı	Açıklama		
	ARAŞTIRMA BÜTÇESİ	<input checked="" type="checkbox"/>		
	SİGORTA	<input type="checkbox"/>		

KARAR BİLGİLERİ	Karar No: <b>327</b>	Toplantı tarihi: 26.09.2012
	<p>Üniversitemiz Tıp Fakültesinde <b>Prof.Dr.Erhan Bilir</b>'in sorumluluğunda yapılması tasarlanan ve yukarıdaki künyede kayıtlı başvuru bilgileri verilen, <i>Doktora Tezi</i> olan klinik araştırma başvuru dosyası ve ilgili belgeler araştırmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelenmiş ve araştırmanın gerçekleştirilmesinde etik sakınca bulunmadığına ve "bütçesi dışında" uygun olduğuna G.Ü.T.F. Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu üyelerinin oybirliği ile karar verilmiştir.</p> <p>Etik Kurulun kararı, projenin bütçesi BAP tarafından kabul edildiği takdirde yürürlüğe girecek olup, BAP kararının Kurulumuza bildirilmesi gerekmektedir.</p>	

ETİK KURUL BİLGİLERİ	
ÇALIŞMA ESASI	Dünya Tıp Birliği Helsinki Bildirgesinin son versiyonu, İyi Klinik Uygulamaları (Uluslararası ICH-GCP) kılavuzu ve bununla ilgili 2001/20/EC ve 2005/28/EC sayılı Avrupa Birliği direktifleri, Biyoloji ve Tıbbın uygulanması bakımından İnsan Hakları ve İnsan haysiyetinin korunması sözleşmesi ve İnsan Hakları ve Biyotıp Sözleşmesinin onaylanmasının uygun bulunduğu dair kanun (9.12.2003 tarihli 25311 sayılı Resmi Gazete), 2547 sayılı Yükseköğretim Kanunu (06.11.1981 tarihli 17506 sayılı Resmi Gazete), Klinik Araştırmalar Hakkında Yönetmelik , İyi Klinik Uygulamaları Kılavuzu
ETİK KURUL BAŞKANI UNVANI/ADI/SOYADI: Prof.Dr.Canan ULUOĞLU	

## EK-1. Etik kurul (devam)

Unvanı/Adı/Soyadı	Uzmanlık Alanı	Kurumu	Cinsiyet	İlişki *		Katılım **		İmza
				E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Canan ULUOĞLU BAŞKAN	Tıbbi Farmakoloji	G.Ü.T.F Tıbbi Farmakoloji A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Doç.Dr.Arzu BAKIRTAŞ BAŞKAN YRD.	Çocuk Sağ.ve Hast. Çocuk Allerji	Çocuk Sağlığı ve Hastalıkları A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Gonca AKBULUT RAPORTÖR	Fizyoloji	G.Ü.T.F Fizyoloji A.D.	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	Katılmadı
Prof.Dr.Fusun BOZKIRLI ÜYE	Anesteziyoloji ve Reanimasyon	G.Ü.T.F Anest.ve Rea. A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Emin TÜRKÖZ ÜYE	Restoratif Diş Tedavisi ve Endodonti	G.Ü.D.F Restoratif Diş Ted. ve Endodonti A.D	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	Katılmadı
Prof.Dr.Seyhan ERSAN ÜYE	Farmasötik Kimya	G.Ü.E.F (Ecz. Mes. Bil.) Farmasötik Kimya A.D.	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Sefer AYCAN ÜYE	Halk Sağlığı	G.Ü.T.F Halk Sağlığı A.D	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Mustafa KAVUTÇU ÜYE	Tıbbi Biyokimya	G.Ü.T.F Tıbbi Biyokimya A.D	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Öznur L.BOYUNAĞA ÜYE	Radyoloji	G.Ü.T.F Radyoloji A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Galip GÜZ ÜYE	İç Hastalıkları Erişkin Nefroloji	G.Ü.T.F İç Hastalıkları A.D.	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	Katılmadı
Prof.Dr.Aylar POYRAZ ÜYE	Tıbbi Patoloji	G.Ü.T.F Tıbbi Patoloji A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Metin YILMAZ ÜYE	Kulak-Burun-Boğaz Hast.	Kulak-Burun-Boğaz Hast. A.D	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Prof.Dr.Nesrin ÇOBANOĞLU ÜYE	Tıp Etiği ve Tıp Tarihi	G.Ü.T.F Tıp Etiği ve Tıp Tarihi A.D	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	Katılmadı
Doç.Dr.Birol DEMİREL ÜYE	Adli Tıp	G.Ü.T.F Adli Tıp A.D.	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	
Öğr.Gör. Adem GELİR ÜYE	Hukukçu Üye	Rektörlük Hukuk Müşavirliği	E	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	Katılmadı
Emine ŞEKER ÜYE	Sivil Temsilci	Sivil Temsilci	K	E <input type="checkbox"/>	H <input checked="" type="checkbox"/>	E <input checked="" type="checkbox"/>	H <input type="checkbox"/>	

\* :Araştırma ile İlişki  
\*\* :Toplantıda Bulunma



## ÖZGEÇMİŞ

### Kişisel Bilgiler

Soyadı, adı : Karakış, Rukiye  
 Uyuğu : T.C.  
 Doğum tarihi ve yeri : 1980, Sivas  
 Medeni hali : Bekâr  
 Telefon : 0 (312) 202 85 80  
 E-mail : rukiyekarakis@gazi.edu.tr



Eğitim Derecesi	Okul/Program	Mezuniyet Yılı
Doktora	Gazi Üniversitesi- Bilişim Enstitüsü Elektronik ve Bilgisayar Eğt. A.B.D.	2009-halen
Yüksek Lisans	Gazi Üniversitesi –Bilişim Enstitüsü Elektronik ve Bilgisayar Eğt. A.B.D.	2006-2009
Lisans	Ondokuz Mayıs Üniversitesi-Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (Bölüm İkinciliği)	1998-2002
Lise	Sivas Kongre Lisesi (YDA)	1994-1998

İş Deneyimi, Yıl	Çalıştığı Yer	Görev
2002- 2005	Milli Eğitim Bakanlığı	Öğretmen
2005- 2006	Cumhuriyet Üniversitesi	Araştırma. Gör.
2006- 2015	Gazi Üniversitesi (Madde 35.)	Araştırma. Gör.

### Yabancı Dil

İngilizce

### Yayınlar

#### SCI, SCI-EXP., SSCI, AHCI Tarafından Taranan Makaleler:

- Güler, İ., Toprak, A., Demirhan, A., **Karakış, R.** (2008). MR images restoration with the use of fuzzy filter having adaptive membership parameters, *J. Med. Syst*, 32 (3), 229-34.
- Güler, İ., Demirhan, A., **Karakış, R.** (2009). Interpretation of MR images using self-organizing maps and knowledge-based expert systems, *Digital Signal Processing*, 19 (4), 668–677.

3. **Karakış, R.**, Tez, M., Kılıç, Y.A., Kuru, B., Güler, İ. (2013). A genetic algorithm model based on artificial neural network for prediction of the axillary lymph node status in breast cancer, *Engineering Applications of Artificial Intelligence*, 26 (3), 945–950.
4. **Karakış, R.**, Guler, İ., Çapraz, İ., Bilir, E. (2013). A Novel Fuzzy Logic-Based Image Steganography Method To Ensure Medical Data Security, *Computers in Biology and Medicine (Hakem İncelemesinde)*.

#### **Diğer İndeksler Tarafından Taranan Makaleler:**

1. Işık, A.H. **Karakış, R.**, Güler, İ. (2010). Postgraduate students'attitudes towards distance learning (The case study of Gazi University), *Procedia - Social and Behavioral Sciences*, 9, 218-222.
2. Çetin, G., **Karakış, R.**, Çetin, A. (2013). Semantic Wiki: A Tool for Collaborative Learning Environment in Computer Engineering Education, *Journal of Education and Future*, 4, 77-86.
3. **Karakış, R.**, Çapraz, İ., Bilir, E., Guler, İ. (2013). EEG Source Localization Using a Genetic Algorithm-Based Artificial Neural Network, *Recent Patents on Biomedical Engineering*, 6 (3), 188-194.

#### **Bilimsel Toplantı - Kongre ve Görevler:**

1. **Karakış, R.**, Tez, M., Güler, İ. (2011). Meme Kanseri Hastalarının Koltuk Altı Lenf Nod Durumunun Örüntü Tanıma Analiz Teknikleri ile Sınıflandırılması, *IEEE 19. Sinyal İşleme ve İletişim Uygulamaları Kurultayı Antalya*, 988 - 991 (2011).
2. Işık, A.H., **Karakış, R.**, Güler, İ. (2011). Gazi Üniversitesi Bilişim Enstitüsü Web Sayfasının Kullanılabilirlik Analizi, *2nd International Conference on New Trends in Education and Their Implications ICONTE 2011 Antalya*, 607-614.
3. Çetin, G., **Karakış, R.** (2012). A wiki application for artificial neural network course in engineering education, *Interactive Collaborative Learning (ICL), 2012 15th International Conference on*, 1-4 (2012).
4. **Karakış, R.**, Işık, A.H., Güler, İ. (2013). Feature selection in pulmonary function test data with machine learning methods, **Signal Processing and Communications Applications Conference (SIU), 2013 21st**, 1- 4.
5. İnternet: **Karakış, R.**, Güler, İ. (2014). Medikal Dicom Görüntüler için Steganografi Uygulaması, *7th International Conference on Information Security and Cryptology, İstanbul, Poster*, <http://www.iscturkey.org/iscold/>.
6. **Karakış, R.**, Güler, İ. (2014). An Application of Fuzzy Logic-Based Image Steganography, *Signal Processing and Communications Applications Conference (SIU), 2014 22nd*, 156-159.
7. **Karakış, R.**, Güler, İ., Çapraz, İ., Bilir, E. (2015). Medikal Sinyaller için Benzerlik Tabanlı Görüntü Steganografi Uygulaması, Akademik Bilişim (Kabul Edildi).
8. **Karakış, R.**, Güler, İ., Çapraz, İ., Bilir, E. (2015). A New Method of Fuzzy Logic-Based Steganography for the Security of Medical Images -Medikal Görüntülerin Güvenliği için Bulanık Mantık Tabanlı Steganografi Yöntemi, *Signal Processing and Communications Applications Conference (SIU), 2015 23rd*, 176-179.

#### **Yer Alınan Bilimsel Projeler:**

1. “MR Görüntülerinin Bilgi Tabanlı Yapay Zekâ Teknikleri Kullanılarak Yorumlanması”, G.Ü. Rektörlüğü Bilimsel Araştırma Projesi (07/2007-06), Araştırmacı.

2. “Beyin Fonksiyonlarının Oluştuđu Yerlerin İmge Çakıştırma ve Örüntü Tanıma Teknikleri ile fMRG İmgelerinden Belirlenmesi”, G.Ü. Rektörlüğü Bilimsel Araştırma Projesi (07/2012-45), Araştırmacı.

**Hobiler**

Yamaç ve serbest paraşüt, model uçak, doğa yürüyüşü, yüzme, deneme yazma.



*GAZİ GELECEKTİR..*

