

**T.C.
ERCIYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**TERSİNİR VE KIRILGAN SAYISAL DAMGALAMA İÇİN
YENİ BİR YÖNTEM**

**Hazırlayan
Gökhan AZİZOĞLU**

**Danışman
Dr. Öğr. Üyesi Ahmet Nusret TOPRAK**

Yüksek Lisans Tezi

**Temmuz 2021
KAYSERİ**

**T.C.
ERCIYES ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI**

**TERSİNİR VE KIRILGAN SAYISAL DAMGALAMA İÇİN
YENİ BİR YÖNTEM
(Yüksek Lisans Tezi)**

**Hazırlayan
Gökhan AZİZOĞLU**

**Danışman
Dr. Öğr. Üyesi Ahmet Nusret TOPRAK**

**Temmuz 2021
KAYSERİ**

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Gökhan AZİZOĞLU

İmza

“Tersinir ve Kırılgan Sayısal Damgalama İçin Yeni Bir Yöntem” adlı Yüksek Lisans Tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesi 'ne uygun olarak hazırlanmıştır.

Hazırlayan

Gökhan AZİZOĞLU

İmza

Danışman

Dr. Öğr. Üyesi Ahmet Nusret TOPRAK

İmza

Bilgisayar Mühendisliği ABD Başkanı

Prof. Dr. Veysel ASLANTAŞ

TEŞEKKÜR

Tez çalışması sırasında bilgi, birikim ve tecrübeleri ile bana yol gösteren ve ayrıca çalışma disiplini, çalışkanlığı, üretkenliği ve insani ilişkileri ile örnek aldığım, güvenini ve desteğini hiçbir zaman esirgemeyen değerli danışman hocam, sayın Dr. Öğr. Üyesi Ahmet Nusret TOPRAK’a teşekkürü bir borç bilirim.

Çalışmalarında fikir alışverişlerinde bulunduğum, desteklerini eksik etmeyen, bana yol gösteren, kıymetli hocalarım, Dr. Öğr. Üyesi Emre ÜNSAL, Dr. Öğr. Üyesi Rukiye KARAKIŞ, Dr. Öğr. Üyesi Sibel ARSLAN ve Dr. Öğr. Üyesi Yakup EMÜL’e teşekkür ederim.

Beni bugünlere getiren, her konuda destek veren, yanımda olan çok değerli aileme ve yıllardır manevi desteğini esirgemeyen sevgili eşim Fatma AZİZOĞLU’na çok teşekkür ederim.

Gökhan AZİZOĞLU

Temmuz 2021, KAYSERİ

TERSİNİR VE KIRILGAN SAYISAL DAMGALAMA İÇİN YENİ BİR YÖNTEM

Gökhan AZİZOĞLU

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü
Yüksek Lisans Tezi, Temmuz 2021
Danışman: Dr. Öğr. Üyesi Ahmet Nusret TOPRAK

ÖZET

Son yıllarda, bilgi teknolojilerindeki büyük gelişmeler ile tıbbi görüntülerin depolanması ve dağıtımı kolay bir hale gelmiştir. Fakat bununla birlikte bu gelişmeler, görüntülerin yetkisiz kişiler tarafından kopyalanmasına, değiştirilmesine ve yasa dışı dağıtımına imkân sağlamıştır. Tıbbi görüntüler, yasa dışı kullanımlar ile maddi zararlar meydana getirebileceği gibi bu görüntüler üzerinde yapılan kurcalamaların uzman hekimin hastalığın teşhisi sırasında vereceği kararı etkileyebileceğinden hastaların hayatlarını tehlikeye atabilir. Bu yüzden, tıbbi görüntülerin doğrulama, bütünlük ve güvenliğinin sağlanması çok önemlidir.

Tez kapsamında, bu problemlere çözüm getirecek tıbbi görüntülerde kurcalama yer tespiti yapabilen yeni bir tersinir kırılgen sayısal damgalama yöntemi önerilmiştir. Geliştirilen yöntemde, görüntü 8×8 boyutunda bloklara ayrıldıktan sonra Ayrıık Dalgacık Dönüşümü ile frekans uzayına taşınarak damga bilgisi gömülmüştür. Daha sonra, görüntü frekans uzayından, resim uzayına dönüştürülmüştür. Bu dönüşüm sırasında, meydana gelen yuvarlama hatalarının düzeltilmesi ve en yüksek farkedilmezlik değerine sahip damgalanmış görüntünün elde edilmesinde zeki optimizasyon algoritmalarından faydalanılmıştır. Damgalanmış görüntü üzerine uygulanan kurcalamaların tespiti için iki farklı yöntem önerilmiş ve yüksek doğrulukta kurcalama tespit performansı elde edilmiştir. Ayrıca önerilen yöntem, tıbbi görüntü uygulama alanlarında hayati öneme sahip olan orijinal görüntüyü, damga çıkarma aşamasında kayıpsız bir şekilde sunmuştur.

Anahtar Kelimeler: Sayısal Damgalama, Tıbbi Görüntü Damgalama, Kurcalama Yer Tespiti

A NOVEL REVERSIBLE FRAGILE DIGITAL WATERMARKING METHOD

Gökhan AZİZOĞLU

Erciyes University, Graduate School of Natural and Applied Sciences

Master Thesis, July 2021

Supervisor: Asst. Prof. Ahmet Nusret TOPRAK

ABSTRACT

In recent years, storing and distributing medical images have become more accessible with significant advances in information technologies. However, these developments allowed the illegal copying, modification, and illegal distribution of images by unauthorized people. Medical images can cause financial damage by illegal use, and endangering the lives of patients, as changes made to these images can affect the decision of a specialist doctor during the diagnosis of the disease. Therefore, it is essential to ensure the verification, integrity, and security of medical images.

Within the scope of the thesis, a new reversible fragile digital watermarking method was proposed that could detect changes in medical images that would solve these problems. After the image is divided into 8×8 size blocks in the developed method, the watermark information is embedded by moving to the frequency domain by Discrete Wavelet Transform. Later, the image was converted from the frequency domain to the spatial domain. During this transformation, intelligent optimization algorithms were used to correct the rounding errors that occurred and obtain the watermarked image with the highest value of imperceptibility. Two different methods have been proposed for detecting changes applied to the watermarked image, and high accuracy of tamper detection performance has been achieved. In addition, the proposed method presented the original image, which is vital in medical image application areas, without loss in the watermark extraction phase.

Keywords: Digital Watermarking, Medical Image Watermarking, Tamper Detection

İÇİNDEKİLER

TERSİNİR VE KIRILGAN SAYISAL DAMGALAMA İÇİN YENİ BİR YÖNTEM

BİLİMSEL ETİĞE UYGUNLUK	ii
YÖNERGEYE UYGUNLUK.....	iii
KABUL VE ONAY	iv
ÖNSÖZ	v
ÖZET.....	vi
ABSTRACT	vii
İÇİNDEKİLER	viii
KISALTMALAR	xii
TABLolar LİSTESİ.....	xiv
ŞEKİLLER LİSTESİ	xv
GİRİŞ	1

1. BÖLÜM

GENEL BİLGİLER

1.1. Sayısal Görüntü Damgalama	4
1.2. Sayısal Görüntü Damgalama Uygulama Alanları	6
1.2.1. Telif Hakkının Korunması	6
1.2.2. Veri Doğruluğunun İspatı	7
1.2.3. Veri Bütünlüğünün İspatı	7
1.2.4. Yayın Takibi	7
1.2.5. Parmak İzi Takibi	7
1.2.6. Tıbbi Görüntü Damgalama.....	8

1.3. Sayısal Görüntü Damgalama Özellikleri	8
1.3.1. Farkedilmezlik.....	8
1.3.2. Dayanıklılık.....	9
1.3.3. Veri Gömme Kapasitesi.....	9
1.3.4. Güvenlik.....	10
1.3.5. Hesaplama Karmaşıklığı	10
1.4. Sayısal Görüntü Damgalama Yöntemlerinin Sınıflandırılması	10
1.4.1. Algılanabilirliğine Göre	11
1.4.1.1. Görünür Damgalama.....	11
1.4.1.2. Görünmez Damgalama.....	11
1.4.2. Damgalama Uzayına Göre	12
1.4.2.1. Resim Uzayında Damgalama	12
1.4.2.2. Frekans Uzayında Damgalama.....	14
1.4.3. Dayanıklılığına Göre.....	16
1.4.3.1. Dayanıklı Damgalama	16
1.4.3.2. Kırılğan Damgalama.....	19
1.4.3.3. Yarı-Kırılğan Damgalama.....	22
1.4.3.4. Hibrit Damgalama	22
1.5. Görüntü Damgalamada Karşılaşılan Saldırıları	23
1.6. Görüntü Kalite Metrikleri.....	24
1.6.1. Ortalama Karesel Hata.....	25
1.6.2. Tepe Sinyal Gürültü Oranı	25
1.6.3.Yapısal Benzerlik İndeksi.....	25
1.6.4. Bit Hata Oranı	26

1.7. Zeki Optimizasyon Algoritmaları.....	26
1.7.1. Parçacık Sürü Optimizasyon Algoritması	27
1.7.2. Genetik Algoritma.....	28
1.7.3. Yapay Arı Koloni Algoritması	29
1.7.4. Diferansiyel Gelişim Algoritması.....	30

2. BÖLÜM

TERSİNİR KIRILGAN SAYISAL DAMGALAMA

2.1. Giriş.....	33
2.2. Tersinir Kırılğan Sayısal Damgalama.....	33
2.2.1. Damganın Gömülmesi	35
2.2.2. Damganın Çıkarılması.....	42
2.2.3. Kurcalama Yer Tespiti	44

3. BÖLÜM

BULGULAR

3.1. Kullanılan Araçlar ve Veri Seti	48
3.2. Optimizasyon Algoritması Seçimi	48
3.2.1. Parçacık Sürü Optimizasyon Algoritması	50
3.2.2. Genetik Algoritma.....	51
3.2.3. Yapay Arı Koloni Algoritması	54
3.2.4. Diferansiyel Gelişim Algoritması.....	56
3.3. Farkedilmezlik Analizi	58
3.4. Kurcalama Yer Tespiti Performans Değerlendirmesi.....	60

4. BÖLÜM

SONUÇ-TARTIŞMA ve ÖNERİLER

4.1. Sonuç	66
4.2. Tartışma ve Öneriler	67
KAYNAKÇA	68
ÖZGEÇMİŞ.....	73



KISALTMALAR

EHK: Elektronik Hasta Kaydı
 PACS: Görüntü Arşivleme ve İletişim Sistemleri
 ADD: Ayrık Dalgacık Dönüşümü
 PSNR: Tepe Sinyal Gürültü Oranı
 MSE: Ortalama Karesel Hata
 YB: Yapısal Benzerlik İndeksi
 BHO: Bit Hata Oranı
 EAB: En Anlamsız Bit
 YİÖ: Yerel İkili Örüntü
 AKD: Ayrık Kosinüs Dönüşümü
 TDA: Tekil Değer Ayrışımı
 LL: Düşük-Düşük
 LH: Düşük-Yüksek
 HL: Yüksek-Düşük
 HH: Yüksek-Yüksek
 dB: Desibel
 ROI: En İlgili Alan
 RONI: İlgili Olmayan Alan
 MR: Manyetik Rezonans
 NK: Normalleştirilmiş Korelasyon
 TDD: Tamsayı Dalgacık Dönüşümü
 bpp: Bit Per Pixel (Piksel Başına Düşen Bit Sayısı)
 ABC: Yapay Arı Koloni
 BT: Bilgisayarlı Tomografi
 DGA: Diferansiyel Gelişim Algoritması
 PSO: Parçacık Sürü Optimizasyon
 GA: Genetik Algoritma
 PB: Popülasyon Büyüklüğü
 Ort: Ortalama

Std: Standart Sapma

MD5: Message Digest 5

PB: Popölasyon Büyüklüğü



TABLOLAR LİSTESİ

Tablo 2.1. Özet tıbbi görüntü formatları	39
Tablo 3.1. PSO algoritması popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler	52
Tablo 3.2. PSO algoritması popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler	52
Tablo 3.3. GA popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler	53
Tablo 3.4. GA popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler	54
Tablo 3.5. ABC algoritması koloni büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler	55
Tablo 3.6. ABC algoritması koloni büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler	55
Tablo 3.7. DGA popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler	56
Tablo 3.8. DGA popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler	57
Tablo 3.9. Optimizasyon algoritmalarının farkedilmezlik analizi	57
Tablo 3.10. Optimizasyon algoritmalarının hesaplama maliyetleri	58
Tablo 3.11. Damgalanmış görüntülerin farkedilmezlik değerleri	59
Tablo 3.12. Geliştirilen yöntemin, literatürdeki bazı yöntemler ile farkedilmezlik karşılaştırması	59

ŞEKİLLER LİSTESİ

Şekil 1.1. Bilgi güvenliği yöntemlerinin sınıflandırması	5
Şekil 1.2. Damgalama sistemi karakteristiği.....	6
Şekil 1.3. Geliştirilen damgalama yönteminde, uygulamanın ihtiyacına göre kurulan dayanıklılık, farkedilmezlik ve kapasite arasındaki denge üçgeni.....	10
Şekil 1.4. Görünür damgalama örneği	11
Şekil 1.5. En Anlamsız Bit damgalama yöntemi	13
Şekil 1.6. Ayırık Kosinüs Dönüşümünün alt bantları	14
Şekil 1.7. İki seviyeli Ayırık Dalgacık Dönüşümünün alt bant görünümü	16
Şekil 1.8. Lena görüntüsü üzerine uygulanmış bazı yaygın kullanılan ataklar.....	24
Şekil 1.9. PSO algoritması akış diyagramı.....	28
Şekil 1.10. Genetik Algoritma akış şeması	29
Şekil 1.11. ABC algoritması temel işlem adımları	30
Şekil 1.12. Diferansiyel Gelişim Algoritması akış şeması.....	31
Şekil 2.1. Geliştirilen damgalama yönteminin genel şeması	34
Şekil 2.2. İki seviyeli ADD dönüşüm katsayıları.....	36
Şekil 2.3. 2×2 boyutundaki katsayı matrisi.....	37
Şekil 2.4. Örnek bir alt banda damga bilgisinin gömülme süreci	38
Şekil 2.5. Damgalama sonrası görüntü piksel değişimi	38
Şekil 2.6. Tam sayı yuvarlama sonrası görüntü piksel değişimi.....	41
Şekil 2.7. Damga gömülme sürecine ait blok diyagram	41
Şekil 2.8. Damga çıkarma sürecine ait blok diyagram.....	44
Şekil 2.9. Birinci yönteme ait doğrulama bitleri	45
Şekil 2.10. Blok sağlama bitlerinin elde edilmesi.....	45
Şekil 2.11. Birinci yöntem kullanılarak blok doğrulama bitlerinin elde edilmesi	46
Şekil 2.12. İkinci yöntem kullanılarak blok doğrulama bitlerinin elde edilmesi.....	47
Şekil 3.1. Damgalamada kullanılan görüntüler.....	49
Şekil 3.2. Optimizasyon algoritması seçimi için kullanılan giriş görüntüsü ve damga ..	50
Şekil 3.3. PSO algoritması için; a) örnek çözüm kümesi, b) dönüşüm matrisi.....	50

Şekil 3.4. GA için; a) örnek bir birey, b) dönüşüm matrisi.....	51
Şekil 3.5. 128×96 boyutundaki siyah-beyaz damga	58
Şekil 3.6. Giriş görüntüsü ile çıkarılmış görüntünün histogramı	60
Şekil 3.7. Barbara görüntüsüne uygulanan içerik değişim saldırısı	61
Şekil 3.8. Yöntemlerin, kırpma ve döndürme saldırılarına karşı performansları.....	61
Şekil 3.9. Yöntemlerin, alçak geçiren filtre, JPEG ve JPEG2000 sıkıştırma saldırılarına karşı performansları	62
Şekil 3.10. Yöntemlerin, Gaussian ve tuz-biber saldırılarına karşı performansları	63
Şekil 3.11. Yöntemlerin, histogram eşitleme, bulanıklaştırma ve keskinleştirme saldırılarına karşı performansları	64
Şekil 3.12. Yöntemlerin, kopyala-yapıştır, metin ekleme ve şekil ekleme saldırılarına karşı performansları	65

GİRİŞ

Son yıllarda, bilgi teknolojilerindeki büyük gelişmeler ile tıbbi görüntülerin sayısal olarak depolanması ve dağıtımı oldukça kolay bir hale gelmiştir. Fakat bununla birlikte bu gelişmeler, görüntülerin yetkisiz kişiler tarafından kopyalanmasına, değiştirilmesine ve yasa dışı dağıtımına imkân sağlamıştır. Tıbbi görüntülerin değiştirilmesi uzman hekimin hastalığın teşhisi sırasında vereceği kararı etkileyebileceğinden, tıbbi görüntülerin doğrulama, bütünlük ve güvenliğinin sağlanması çok önemlidir [1].

Elektronik hasta kaydı (EHK), hastanın kimlik bilgilerini, klinik ve tanı raporlarını, reçeteleri, tedavi geçmişi, histolojik ve patolojik bulguları, aşıları, laboratuvar verilerini, radyolojik görüntüleri, EEG, EKG veya EMG gibi biyolojik sinyalleri ve bunların raporlarını içerebilmektedir. EHK yerel ve geniş ağlarda siber saldırılara uğrama riski altındadır. Bu tıbbi verilerin, açık ağ ortamlarında yetkisiz kişiler tarafından ele geçirilmesi, sigortası olmayanlara bazı ilaç veya tıbbi ekipman alımı gibi yasadışı kullanıma imkân tanımaktadır. Bu verilerin değiştirilmesi veya yok edilmesi ise hastaların, hayatlarını tehdit eden durumlara girmesine neden olabilir [2].

Tıbbi görüntülerin saklanması, erişimi, dağıtımı ve geri çağırılması için Görüntü Saklama ve İletişim Sistemleri (PACS) geliştirilmiştir. Tıbbi görüntülerin boyutları ortalama 1 MB ile 100 MB arasındadır ve her yıl bu görüntülerin saklanması için ihtiyaç duyulan depolama miktarı %10 ile %20 arasında değişmektedir. Bu artış ile birlikte bant genişliği kapasite tüketiminin azaltılmasına olan ihtiyaç önem kazanmıştır [2].

Sayısal damgalama, tıbbi görüntü güvenliğinin sağlanması gibi problemleri çözmek için yaygın olarak kullanılan yöntemlerden biridir. Sayısal damgalama, damga adı verilen sayısal bir verinin başka bir sayısal verinin içerisine gizlenmesi temeline dayanmaktadır. Telif hakkı koruması, yayın takibi, veri doğrulama ve bütünlük

kontrolü, parmak izi takibi, tıbbi görüntü damgalama gibi çeşitli uygulamalarda kullanılmaktadır [3].

Literatürde önerilen birçok sayısal damgalama yöntemi bulunmasına rağmen tıbbi görüntülerde güvenliği sağlayarak hasta haklarını koruma altına alan, bant genişliği kapasitesini azaltan ve kurcalama tespiti yapabilen bir yöntem olan ihtiyaç hâlâ devam etmektedir.

Bu tez çalışmasında, tıbbi görüntülerde doğrulamayı, bütünlüğü ve yapılan kurcalamaları tespit edebilen yüksek farkedilmezliğe sahip damgalanmış görüntü sunan yeni bir tersinir kırılğan sayısal damgalama yöntemi önerilmiştir. Yapılan çalışmada, orijinal görüntü 8×8 boyutunda örtüşmeyen bloklara ayrılmaktadır. Daha sonra, görüntü bloklarına iki seviyeli Ayırık Dalgacık Dönüşümü (ADD) uygulanarak damga bilgisi dönüşüm sonrasında elde edilen katsayılara gömülmektedir.

Yüksek görüntü kalitesine sahip damgalanmış görüntü elde etmek için orijinal görüntüde meydana gelecek olan bozulmayı minimum oranda tutmak gereklidir. Bunu sağlayabilmek için önerilen yöntemde yüksek ve orta frekanslı ADD alt bantları tercih edilmiştir. Elde edilen sonuçlar, önerilen yöntemin yaygın olarak karşılaşılan içerik değişimi, kırpma, metin ekleme, kopyala yapıştır, döndürme ve gürültü ekleme gibi saldırılarda yüksek doğrulukta kurcalama yer tespiti yapabildiğini göstermektedir. Ayrıca önerilen yöntem, tıbbi görüntüler gibi orijinal görüntünün hayati öneme sahip olduğu uygulama alanları için tersinir özellik sağlamaktadır.

Tezin Organizasyonu:

Birinci bölümde, sayısal damgalama, damgalanmış görüntüye uygulanan saldırılar, görüntü kalite metrikleri ve zeki optimizasyon yöntemleri ile ilgili genel bilgilere ve literatür çalışmalarına yer verilmiştir.

İkinci bölümde, önerilen sayısal damgalama yöntemine ait damga gömme, damga çıkarma ve kurcalama yer tespiti süreçleri detaylı bir şekilde açıklanmıştır.

Üçüncü bölümde, zeki optimizasyon algoritması seçimi, farkedilmezlik analizi ve kurcalama yer tespiti performans değerlendirmesi sonunda elde edilen bulgular paylaşılmıştır.

Son olarak, dördüncü bölümde deneysel çalışmalar sonunda elde edilen sonuçlar tartışılmıştır.



1. BÖLÜM

GENEL BİLGİLER

1.1. Sayısal Görüntü Damgalama

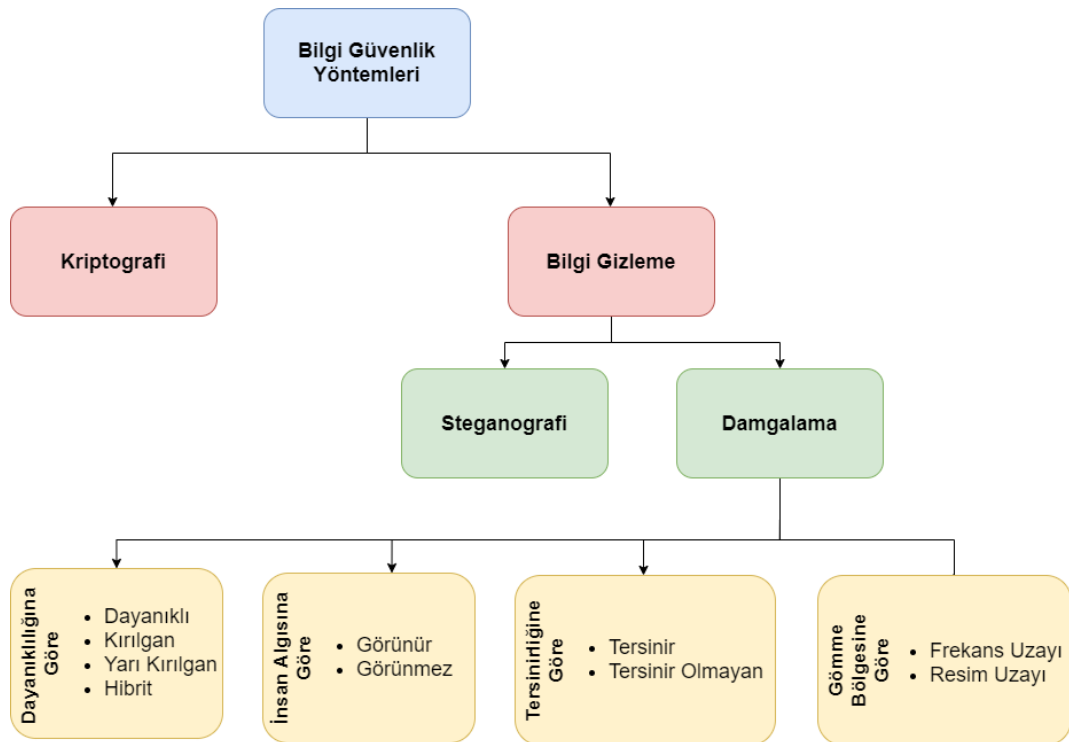
Son yıllarda gelişen görüntü işleme araçları ile birlikte insan gözü algısı ile görüntü üzerinde yapılan kurcalamaları fark etmek neredeyse imkânsız hale gelmiştir [4]. Hatanın ciddi zararlara yol açabileceği tıbbi ve askeri uygulama alanları gibi sahalar için görüntü üzerinde meydana gelen kasti veya kasti olmayan kurcalamaların tespiti büyük önem arz etmektedir. Bu yüzden, görüntünün telif haklarının korunmasını, doğruluğunu ve bütünlüğünü sağlayacak bir çözüme ihtiyaç vardır. Bu problemi çözmek için sayısal görüntü damgalama yöntemleri geliştirilmiştir. Sayısal görüntü damgalama, damga adı verilen görünmeyen gizli bir sahiplik bilgisinin (hastane logosu ve hasta bilgileri gibi) taşıyıcı veya orijinal görüntü olarak isimlendirilen görüntüye gömülmesine denir [5]. Sayısal damgalama yöntemleri, telif hakkı koruması, yayın takibi, parmak izi takibi, tıbbi görüntü damgalama, veri doğruluğunun ispatı ve veri bütünlüğünün ispatı gibi uygulamalarda kullanılmaktadır [6,7].

Sayısal damgalamadan daha eski olan bir diğer alan ise steganografidir. Damgalama ve steganografi birbiriyle ilişkili alanlardır. Her iki alanda da verinin gömülmesinde steganografi teknikleri kullanılmaktadır. Sayısal damgalama, hak sahipliği ve telif haklarının korunması gibi uygulamalarda steganografinin ticari bir uygulamasını temsil etmektedir [8].

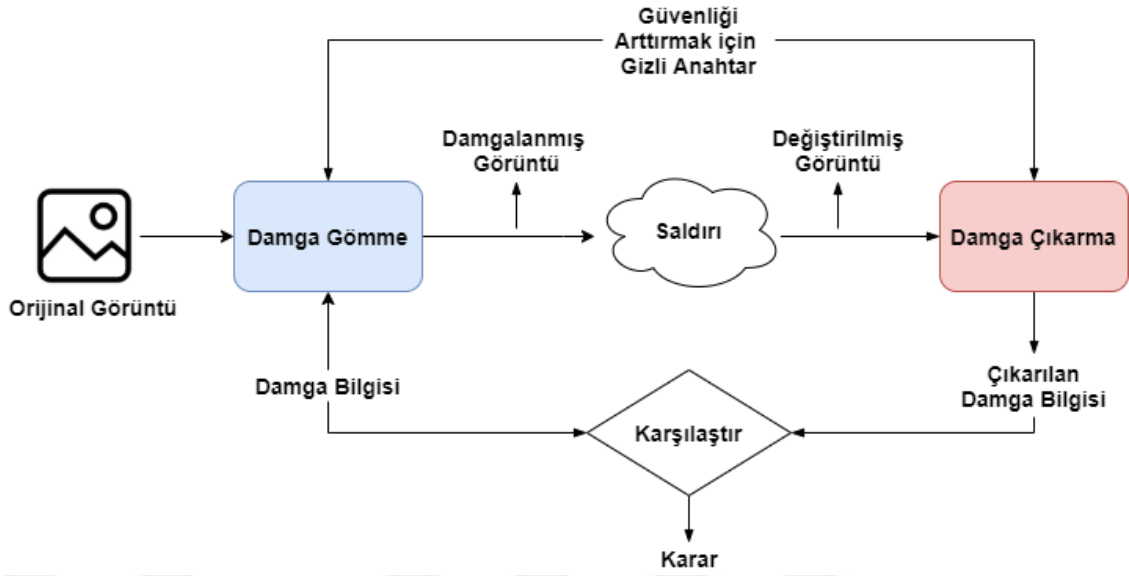
Steganografi, “gizli, saklı (stegano-)” ve “yazı (-grafi)” kelimelerinden türetilmiş eski Yunancaya dayanan bir ifadedir. Steganografi ile damgalama arasındaki fark: steganografide gizli bilgi, taşıyıcı bilgi ile ilişkili değilken, damgalamada taşıyıcı ile gömülen veri birbiri ile ilişkilidir. Ayrıca steganografide gizlenecek olan mesajın gizli kalması büyük öneme sahipken, görüntü damgalamada damganın görünür ya da

görünmez olduğu durumlar bulunmaktadır. Stegonagrafide, saldırganın veriyi fark edemeyeceği şekilde gizlenmesi hedeflenirken, damgalamada verinin saldırgan tarafından silinemeyecek veya değiştirilemeyecek şekilde gizlenmesi hedeflenmektedir [7]. Bu sebeplerle sayısal görüntülerin güvenliğini sağlamada ve korumada görüntü damgalama yöntemleri tercih edilmektedir.

Bilgi güvenlik yöntemleri, Şekil 1.1’de gösterildiği gibi kriptografi ve bilgi gizleme olarak iki ana alt dala ayrılmaktadır [7]. Kriptografi, şifreleme ve şifre çözme mekanizmalarına sahip çeşitli şifreleme yöntemleri ile verinin korunmasını sağlamaktadır [9]. Kriptografi tekniklerinde mesaj, iletim hattına girmeden önce gizli bir anahtar yardımı ile şifrelenir ve anlaşılmaz hale getirilir. Böylece iletim hattında bir saldırı olsa dahi gizli anahtara sahip olmadan orijinal mesaja erişim sağlanamayacaktır. İletim hattından alıcıya gelen şifreli mesaj ve gizli anahtar kullanılarak orijinal mesaja ulaşılır. Kriptografi, mesajın korunmasında güçlü bir yöntem olsa da orijinal içerik ile ilişkilendirilemediği için telif haklarının korunması gibi uygulamalarda kullanılamamaktadır. Kriptografi, görüntü damgalama yöntemlerinde genellikle, verinin gizlenmeden önce şifrelenmesi ve böylece daha yüksek güvenlik sağlanması amacıyla kullanılabilmektedir [5].



Şekil 1.1. Bilgi güvenliği yöntemlerinin sınıflandırması [7]



Şekil 1.2. Damgalama sistemi karakteristiği [7]

Bir damgalama yöntemi, genel olarak damga gömme ve damga çıkarma süreçlerinden oluşur (Şekil 1.2) [7]. Damga gömme sürecinde, damga taşıyıcı görüntüye gömülür. Bu işlem sırasında, gizli bir anahtar yardımı ile şifreleme yöntemleri kullanılarak güvenlik artırılabilir [5,10]. Damga çıkarma sürecinde ise görüntü içerisine gömülmüş olan damga, çıkarma algoritması kullanılarak görüntüden elde edilir. Elde edilen görüntü, orijinal damga ile kıyaslanarak görüntü doğrulanır.

1.2. Sayısal Görüntü Damgalama Uygulama Alanları

Sayısal görüntü damgalama, güvenliği sağlamak veya arttırmak için birçok farklı alanda uygulanabilmektedir. Bu uygulamalardan en önemli olanları, telif hakkının korunması, yayın takibi, parmak izi takibi, tıbbi görüntülerde damgalama, veri doğruluğunun ispatı ve veri bütünlüğünün ispatı olarak sınıflandırılabilir [6].

1.2.1. Telif Hakkının Koruması

Telif hakkı koruması, sayısal görüntü damgalama alanında en çok kullanılan uygulamalardan biridir. Sayısal damgalama, gelişen teknoloji ile ortaya çıkan eser sahibinin telif haklarının korunması problemine çözüm getirmektedir.

Sayısal damgalama ile görüntü içerisine sahiplik bilgileri gömülerek, sayısal verinin sahipliğinin doğrulanması ve korunması sağlanmaktadır. Böylece damgalanmış görüntü

telif hakkı davalarında mülkiyetin ispatlanması için hukuki olarak kullanılabilir [11].

Bu uygulamalarda, görüntü içerisinde saklanacak olan veriler dayanıklı bir şekilde gömülerek saldırılara karşı bozulmaması ve görüntü sahibi olmayanların hak sahipliği iddia etmelerinin önüne geçilmesi sağlanmaktadır.

1.2.2. Veri Doğruluğunun İspatı

Bu uygulamalarda, görüntünün orijinali ile aynı olduğunu doğrulamak için taşıyıcı görüntü üzerine bir damga gömülmektedir. Gömülen damga, daha sonra çıkarılıp orijinal damga ile kıyaslanarak görüntünün doğrulanması sağlanmaktadır. Bu damgalar orijinal görüntüde bir bitlik en ufak bir değişimde bile bozularak görüntünün değiştiğini göstermektedir. Görüntünün orijinali ile aynı olduğunu doğrulamak için çeşitli kriptografi teknikleri de kullanılabilir. Fakat kriptografi tekniklerinde, şifrelenmiş görüntü ile bir anahtarın iletilmesi dezavantajı vardır. Bu uygulamalar için genel olarak kırılğan ve yarı-kırılğan damgalama yöntemleri kullanılmaktadır [6].

1.2.3. Veri Bütünlüğünün İspatı

Bütünlük uygulamalarında, görüntünün yetkisiz kişiler tarafından değiştirilmediği garanti edilmesi ve kurcalama yapılan yerlerin bulunması hedeflenir. Bu uygulamalarda, en küçük kurcalamalar bile alıcı tarafından tespit edilebilmelidir. Veri bütünlüğünün ispatı uygulamalarında, kırılğan damgalama yöntemleri tercih edilmektedir [4].

1.2.4. Yayın Takibi

Yayın takibi uygulamalarda içerik sahipleri, ses veya videoları yayın kuruluşuna göndermeden önce içerisine zaman bilgilerini de içeren bir damga gömerek hangi sürelerde başlayıp biteceğini, kaç tekrar gösterileceğini, ne kadar süre yayımlanacağını, izinsiz yayın yapan kuruluşların tespitini ve telif haklarının korunmasını sağlamaktadır [6].

1.2.5. Parmak İzi Takibi

Parmak izi uygulamalarında, yasal olmayan kopyaların takibini yapabilmek için her bir müşteriye gönderilecek kopya için genellikle o müşteriye ait kimlik bilgisi veya seri

numarası gibi özel bilgileri içeren damgalar gömülür [6,7]. Böylece görüntünün yasadışı kopyalarının takibi yapılabilir ve ihlal yapan müşterilerin tespiti sağlanabilir. Bu uygulamalarda kullanılacak olan damganın dayanıklı ve görünmez olması gereklidir [7].

1.2.6. Tıbbi Görüntülerde Damgalama

Son yıllarda sağlık endüstrisi, hastaların ihtiyaçlarını karşılamak için en son bilgi ve iletişim teknolojilerini kullanmaya odaklanmıştır [12]. Bununla birlikte teletıp ve e-sağlık çözümlerinin hızla büyümesi, tıbbi görüntülerin teşhis amaçlı kullanım oranlarını arttırmıştır. Tanı, tedavi ve araştırmadaki önemi nedeniyle tıbbi görüntüler son derece değerli ve hassas verilerdir. Tıbbi verilerin güvenli olmayan bir ağ üzerinden iletilmesi değiştirme, kaldırma, kopyalama ve yetkisiz erişim gibi güvenlik sorunlarına yol açabilmektedir [5,13]. Bu sebeple, tıbbi bilgilerin korunması oldukça büyük öneme sahiptir.

Tıbbi görüntülerde damgalama, görüntüler için yüksek güvenlik ve gizlilik sağlamaktadır. Tıbbi görüntülerde, küçük bozulma veya kurcalamalar yanlış tanıya yol açabileceği için görüntülerin güvenliği sağlarken, orijinalliğinin korunması gereklidir. Orijinal görüntünün korunmasının gerektiği bu tip uygulamalarda genellikle tersinir görüntü damgalama teknikleri kullanılmaktadır. Tersinir damgalama yöntemlerinde, görüntü içerisine gömülen damga çıkarıldıktan sonra orijinal görüntü kayıpsız bir şekilde elde edilebilmektedir [13].

1.3. Sayısal Görüntü Damgalama Özellikleri

Sayısal damgalama yöntemlerinin, kullanım amaçlarına göre sahip olmaları beklenen bazı temel özellikleri bulunmaktadır. Sayısal damga yöntemleri ile geliştirilen uygulamalar, bu temel özellikleri karşılama oranlarına göre farkedilmezlik, dayanıklılık, veri gömme kapasitesi, güvenlik ve hesaplama karmaşıklığı olarak sınıflandırılmaktadır.

1.3.1. Farkedilmezlik

Damgalanmış görüntülerin, orijinal görüntüye algısal olarak benzer olması, damgalanan görüntüdeki piksel değişimlerinin minimum düzeyde olması ve damgalama neticesinde orijinal görüntüde meydana gelen değişimlerin gözle fark edilemiyor olması

beklenmektedir. Farkedilmezlik, orijinal görüntü ile damgalanmış görüntü arasındaki benzerlik ölçüsünü yani damganın görünmezlik derecesini ifade etmektedir [7].

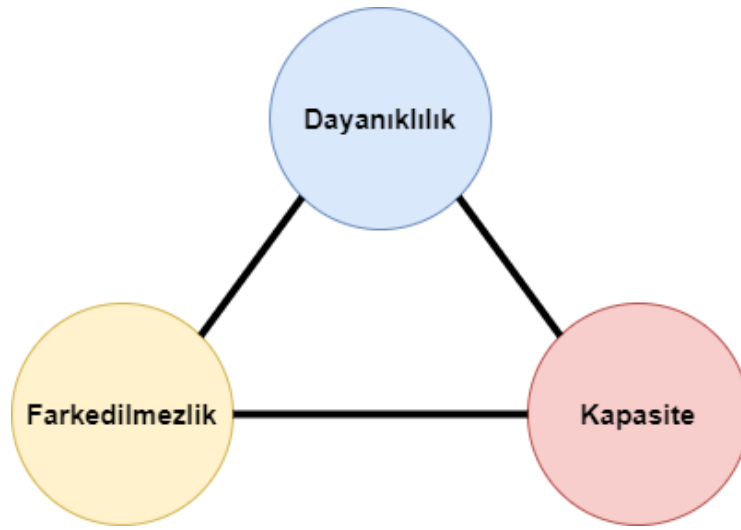
Damgalama yöntemlerinde farkedilmezliği ölçmek için çeşitli kalite metrikleri kullanılmaktadır. Bu kalite metrikleri, orijinal görüntü ile damgalanmış görüntü arasındaki bozulmayı gösterir. Farkedilmezliği ölçmek için Tepe Sinyal Gürültü Oranı (PSNR), Ortalama Karesel Hata (MSE), Yapısal Benzerlik İndeksi (YB) ve Bit Hata Oranı (BHO) gibi kalite metrikleri yaygın olarak kullanılmaktadır.

1.3.2. Dayanıklılık

Dayanıklılık, bir damganın dışarıdan uygulanacak her türlü atak veya dönüşüme karşı ayakta kalabilme yeteneğidir [5]. İyi bir damgalama yönteminde, damga yetkisiz kişiler tarafından çıkarılamamalı veya kaldırılamamalıdır [6]. Bu ataklar, genellikle çıkarma, geometrik, protokol ve kriptografik saldırılar olarak olmak üzere dört gruba ayrılmaktadır [4].

1.3.3. Veri Gömme Kapasitesi

Veri gömme kapasitesi, orijinal görüntü içine veri gömülmeye uygun olan boş alanı ve gömülmeye uygun veri miktarını ifade eder [4]. Veri gömme kapasitesine olan ihtiyaç, geliştirilecek olan uygulamanın türüne göre değişmektedir. Sayısal damgalama sistemlerinde kapasite, dayanıklılık ve farkedilmezlik arasında bir denge vardır (Şekil 1.3) [6]. Bu dengede yer alan özelliklerden birinde iyileştirme sağlandığında diğer özelliklerde azalma olacaktır. Örneğin, yüksek kapasiteli bir damgalama yöntemi geliştirilmek istendiğinde mevcut bütün uygun boş alanların kullanılması gerekecektir. Fakat bununla beraber, damganın gömüldüğü görüntüde bozulma artacak yani farkedilmezlik azalacak ve saldırılar karşısında dayanıklılık daha düşük olacaktır [7]. Bu yüzden, geliştirilecek olan damgalama yönteminde, uygulamanın ihtiyacına göre uygun denge sağlanmalıdır.



Şekil 1.3. Geliştirilen damgalama yönteminde, uygulamanın ihtiyacına göre kurulan dayanıklılık, farkedilmezlik ve kapasite arasındaki denge üçgeni [4]

1.3.4. Güvenlik

Bir damgalama yönteminde yetkisiz erişim minimum düzeyde olmalıdır [5]. Damgalama yönteminde güvenlik, kasıtlı yapılan saldırılara karşı mücadele edebilme yeteneğini ifade eder [4]. Saldırgan, damga gömme ve çıkarma yöntemlerini bilse dahi damga bilgisine ulaşamamalıdır. Bu güvenliğini sağlamak için genel olarak bir gizli anahtar yardımı ile şifreleme yöntemleri kullanılır. Güvenlik, sahiplik doğrulama ve tıbbi görüntü paylaşım uygulamalarında aranan bir özelliktir.

1.3.5. Hesaplama Karmaşıklığı

Damganın gömülmesinden, çıkarılmasına kadar geçirilen süre ve ihtiyaç duyulan kaynaklar hesaplama karmaşıklığı olarak tanımlanır [4]. Damgalama yönteminin, hesaplama karmaşıklığının yüksek olması kullanılan kaynak miktarını arttıracak gibi geçirilen süreyi de arttıracaktır. Özellikle gerçek zamanlı uygulamalarda hesaplama karmaşıklığının düşük olması arzu edilen bir özelliktir [7].

1.4. Sayısal Damgalama Yöntemlerinin Sınıflandırılması

Sayısal damgalama yöntemleri, geliştirilecek uygulamanın türüne ve gereksinimlerine göre genellikle algılanabilirliğine, damgalama uzayına ve dayanıklılığına göre sınıflandırılmaktadır.

1.4.1. Algılanabilirliğine Göre

Sayısal damgalama yöntemleri, insan görsel algısına göre sınıflandırıldığında görünür ve görünmez damgalama olmak üzere ikiye ayrılmaktadır [14].

1.4.1.1. Görünür Damgalama

Görünür damgalama, genellikle telif hakkı korunması uygulamalarında kullanılmaktadır [6]. Görüntü üzerine, insan görsel algısı ile tespit edilebilen (Şekil 1.4) bir damga yerleştirilmektedir. Bu damgalama yönteminin farkedilmezliği düşüktür ve görüntü üzerinden çıkarılması kolaydır. İçerik sahipliğini göstermek için video veya televizyon kanallarının köşesine yerleştirilen logo, popüler görünür damgalama yöntemi uygulamalarındandır [15].



Şekil 1.4. Görünür damgalama örneği

1.4.1.2. Görünmez Damgalama

Görünmez damgalama, damga bilgisinin insan görsel algısı tarafından fark edilemediği damgalama yöntemidir. Damgalama uzayına göre, damga bilgisi frekans uzayında çeşitli dönüşümler ile elde edilen katsayılar veya resim uzayında piksel değerlerine farklı damga gömme yöntemleri kullanılarak gömülebilmektedir. Bu damgalama yöntemleri ile taşıyıcı giriş görüntüsü, damga bilgisi ile ilişkilendirilerek görünmez damgalama gerçekleştirilmektedir [16]. Genellikle telif hakkı korunması, yasal olmayan kopyalamalar ve sahtecilik uygulamalarında koruma sağlamak için kullanılmaktadır [5].

1.4.2. Damgalama Uzayına Göre

Damganın gömülme ve çıkarılma işlemi için birçok teknik kullanılmaktadır. Kullanılan algoritmalara ve damgayı gömmek için kullanılan yola göre damgalama teknikleri resim uzayında damgalama ve frekans uzayında damgalama olmak üzere iki sınıfa ayrılmaktadır [6].

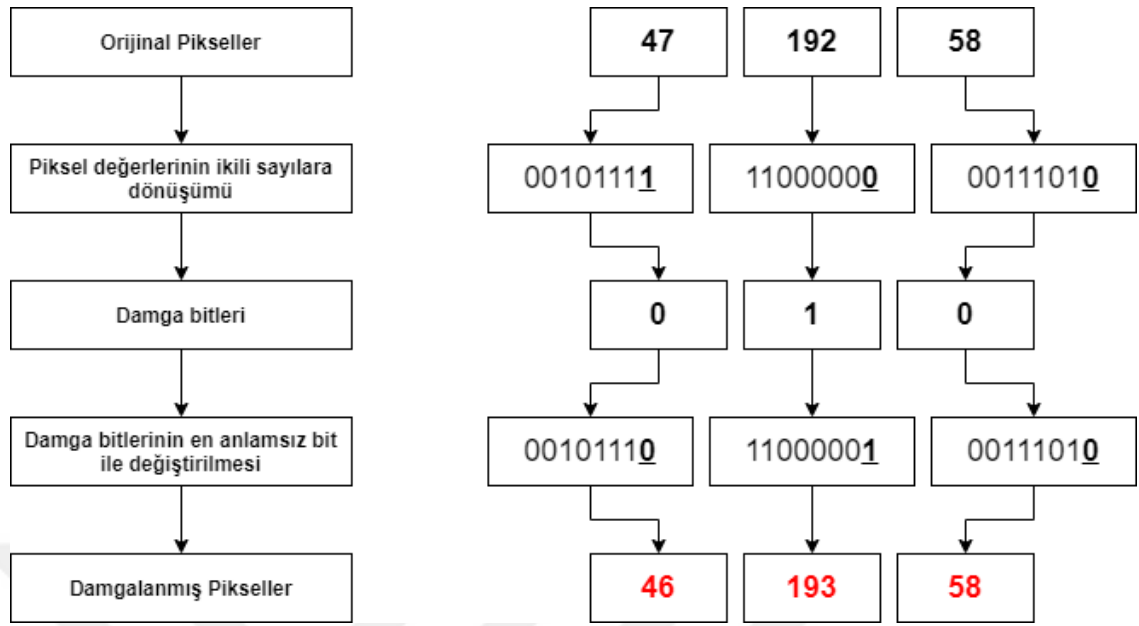
1.4.2.1. Resim Uzayında Damgalama

Resim uzayı kullanılarak gerçekleştirilen damgalama yöntemlerinde, damga bilgisi doğrudan taşıyıcı görüntü piksel değerleri değiştirilerek gömülmektedir [4]. Resim uzayı teknikleri, düşük hesaplama maliyeti ve yüksek kapasiteye sahiptir. Ancak damga, özellikle gürültü ve sıkıştırma gibi geometrik saldırılarda kolayca değişebilmektedir. Bu yöntemler, saldırılar karşısında dayanıklı olmadığı için daha çok kırılğan damgalama uygulamalarında tercih edilmektedirler [6,7].

Resim uzayı kullanılarak gerçekleştirilen birçok damgalama yaklaşımı vardır. Bunlardan en yaygın olarak kullanılanları, En Anlamsız Bit (EAB), Yerel İkili Örüntü (YİÖ) ve Histogram Değiştirme yöntemleridir [4].

En Anlamsız Bit:

EAB yöntemi, en eski ve en basit resim uzayı damgalama tekniklerinden biri olarak bilinmektedir. Şekil 1.5'te gösterildiği gibi giriş görüntüsünün piksellerinin en anlamsız bitleri, gömülecek verinin bitleri ile değiştirilerek gerçekleştirilir. EAB üzerinde yapılan kurcalama, insan gözü tarafından algılanamamaktadır. EAB yönteminde, görüntü pikselleri ilk olarak sekiz bit ikili sayılara dönüştürülür, daha sonra en anlamsız bit (son bit) damga biti (0 veya 1) ile değiştirilir. Oluşturulan yeni sekiz bit, ondalık sayıya dönüştürülerek, yeni piksel değeri elde edilir. Bu yöntem, gürültü, döndürme ve sıkıştırma gibi saldırılara karşı son derece hassastır [4].



Şekil 1.5. En Anlamsız Bit damgalama yöntemi [4]

Yerel İkili Örüntü:

YİÖ, doku analiz ve sınıflandırmasında kullanılan bir yaklaşımdır. Bu yöntemde, görüntü öncelikle örtüşmeyen bloklara bölünür, daha sonra her bloktaki merkezi piksel ve bitişik pikseller arasındaki yerel piksel farklılıkları hesaplanır. Yerel piksel farkı, damganın gömülmesi ve çıkarılması için kullanılır ve eşik olarak kabul edilir. YİÖ tabanlı yöntemler, parlaklık ve kontrast değişimine karşı dayanıklıdır. Ancak bulanıklık ve filtreleme gibi diğer işlemlere karşı kırılgandır. Bu yöntemler yarı-kırılgan damgalama yöntemleri için uygundur [7].

Histogram Değiştirme:

Resim uzayındaki bir başka damgalama tekniği, histogram değiştirmedir. Gri seviye histogramı düşünecek olursak, görüntüdeki her bir gri seviyeye karşılık, ilgili gri seviyedeki piksel sayısını veren fonksiyonu ifade etmektedir. Damga, histogramın maksimum ve minimum noktaları arasındaki değerler değiştirilerek gömülür. Kolay bir damgalama imkânı sağlar. Fakat maksimum nokta sayısındaki kısıtlamadan dolayı sınırlı kapasiteye sahiptir [4].

1.4.2.2. Frekans Uzayında Damgalama

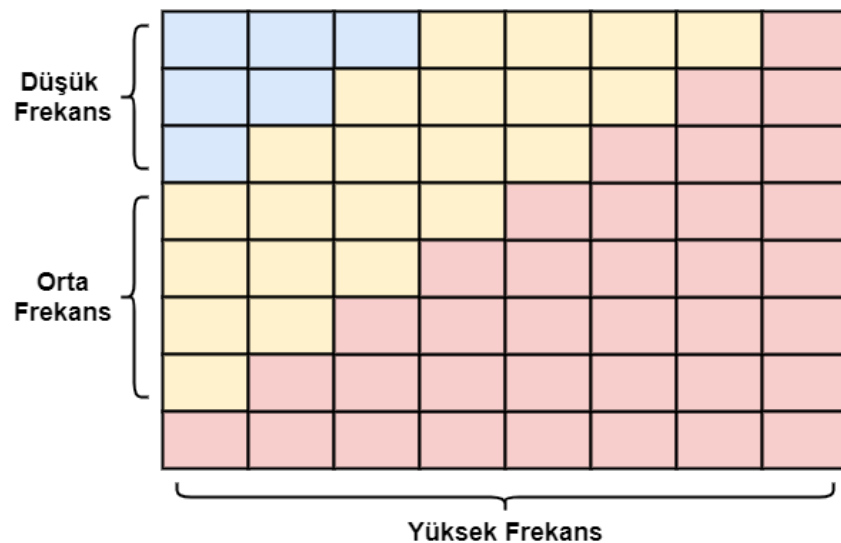
Frekans uzayı damgalama yöntemlerinde, görüntü üzerine çeşitli dönüşümler uygulandıktan sonra damga gömme işlemleri gerçekleştirilir. Frekans uzayı damgalama yöntemleri, resim uzayı damgalama yöntemlerine kıyasla daha yüksek dayanıklılık sağlamaktadır. Fakat hesaplama karmaşıklığı daha yüksektir [5].

Frekans bölgesi damgalama yöntemlerinde, yaygın olarak Ayırık Kosinüs Dönüşümü (AKD), Ayırık Dalgacık Dönüşümü (ADD) ve Tekil Değer Ayırışımı (TDA) dönüşümleri kullanılmaktadır.

Ayrık Kosinüs Dönüşümü:

Ayrık kosinüs dönüşümünde, görüntü resim uzayından frekans uzayına taşınır. AKD, JPEG gibi görüntü sıkıştırmada kullanılan önemli yöntemlerden biridir. Sıkıştırma saldırılarına karşı dayanıklıdır. Fakat döndürme, kırpma ve ölçekleme gibi geometrik dönüşüm saldırılarına karşı kırılgandır [6].

Birinci seviye AKD, görüntüyü Şekil 1.6'da görüldüğü gibi düşük, orta ve yüksek frekans alt bantlarına bölmektedir [7]. Düşük frekans alt bandı, görüntü ile ilgili büyük miktardaki bilgiyi barındırırken, yüksek frekanslı alt bantta, görüntünün ayrıntıları mevcuttur [4]. AKD tabanlı uygulamalarda, genellikle orta frekans bandı tercih edilmektedir [7].



Şekil 1.6. Ayrık Kosinüs Dönüşümünün alt bantları [7]

Ayrık Dalgacık Dönüşümü:

ADD, insan görsel sisteminin teorik modellerine benzer çok çözünürlüklü özelliklere sahip ve uygun mekânsal lokalizasyon sağlayan güçlü bir matematiksel araçtır. ADD yöntemi, Denklem 1.1 ve Denklem 1.2 görüntü üzerine uygulandığında, Düşük-Düşük (LL), Düşük-Yüksek (LH), Yüksek-Düşük (HL) ve Yüksek-Yüksek (HH) olmak üzere farklı frekanslardan oluşan dört alt bant elde edilmektedir[4].

Bir $x[n]$ sinyali için ADD fonksiyonu, takip eden denklemler ile verilir [6]:

$$W_{\phi}[j_0, k] = \frac{1}{\sqrt{M}} \sum_n x[n] \phi_{j_0 k}[n] \quad (1.1)$$

$$j \geq j_0 \text{ için; } W_{\psi}[j, k] = \frac{1}{\sqrt{M}} \sum_n x[n] \psi_{jk}[n] \quad (1.2)$$

Elde edilen dört alt banda, birden fazla seviyede dönüşüm uygulanarak yeni alt bantlar elde edilebilmektedir. Bu yaklaşım, Denklem 1.3'te yer alan ters dönüşüm fonksiyonu uygulanarak tersine çevrilebilir.

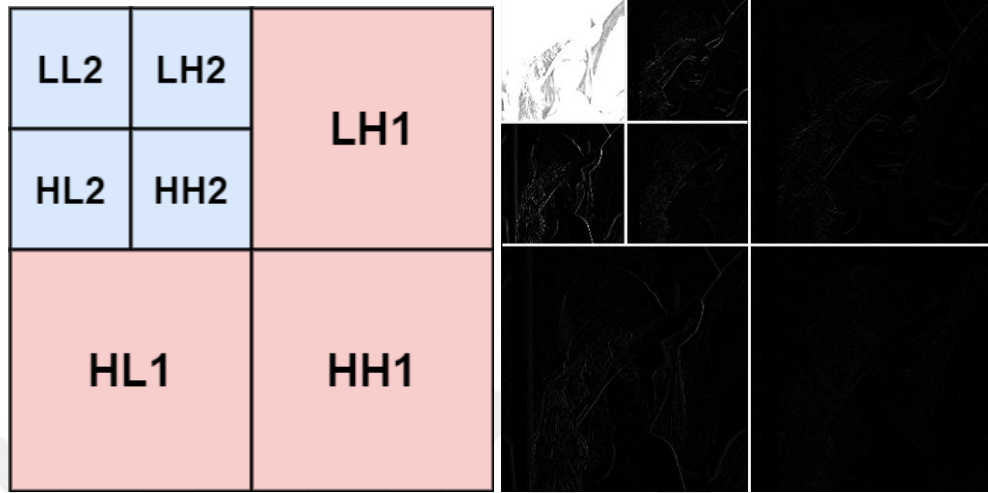
$$x[n] = \frac{1}{\sqrt{M}} \sum_k W_{\phi}[j_0, k] \phi_{j_0 k}[n] + \frac{1}{\sqrt{M}} \sum_{j=j_0}^J \sum_k W_{\psi}[j, k] \psi_{j,k}[n] , \quad (1.3)$$

burada $W_{\phi}[j_0, k]$ yaklaşım katsayıları, $W_{\psi}[j, k]$ detay katsayıları, M transfer edilecek örnek sayısı, J transfer seviyelerinin sayısı, $\phi_{j_0 k}[n]$ ve $\psi_{j,k}[n]$ iki temel fonksiyon, $\phi[n]$ ölçekleme fonksiyonu ve $\psi[n]$ dalgacık fonksiyonudur. Ayrıca ADD dönüşümlerinde yer alan n, j ve k katsayıları aşağıda verilmiştir:

$$n = 0, 1, 2, \dots, M - 1, \quad j = 0, 1, 2, \dots, J - 1, \quad k = 0, 1, 2, \dots, 2^j - 1 \quad (1.4)$$

Şekil 1.7'de iki seviyeli ADD uygulanmış bir görüntü matrisi verilmiştir. ADD uygulanmış görüntü alt bantlarından LL, insan algısı ile fark edilebilen ayrıntılar içermektedir. Bu yüzden bu alt bantta uygulanacak işlemler, insan gözü ile algılanabilmektedir. LL alt bandına damga gömülmesi, farkedilmezliği düşürse de dayanıklılık özelliği yüksek olduğu için dayanıklı damgalama yöntemlerinde tercih edilmektedir. Damga gömülmesinde, HH alt bandı tercih edildiğinde ise düşük

dayanıklılık, iyi bir farkedilmezlik elde edildiğinden kırılğan damgalama yöntemlerinde daha çok kullanılmaktadır [5,19].



Şekil 1.7. İki seviyeli Ayırık Dalgacık Dönüşümünün alt bant görünümü

Tekil Değer Ayrışımı:

TDA, bir matrisi U ve V ortogonal matris ile S diyagonal matrisine dönüştürür. Bir köşegen matrisi olan S tekil değerleri tutmaktadır. Damgalama sırasında damga bilgisinin gömülmesinde bu tekil değerler kullanılmaktadır. Yüksek hesaplama maliyeti olmasına rağmen, iyi enerji sıkıştırma özellikleri sunar ve bu tekil değerlerdeki küçük değişiklikler görüntünün kalitesini çok az etkiler [7].

Bir $m \times n$ boyutundaki X görüntüsünün, TDA dönüşümü Denklem 1.5'te gösterilmektedir [5].

$$X = USV^T \quad (1.5)$$

1.4.3. Dayanıklılığına Göre

Sayısal damgalama yöntemleri, gömülen damganın kasti veya kasti olmayan saldırılar karşısında ayakta kalabilme durumuna göre dayanıklı, kırılğan, yarı kırılğan ve hibrit damgalama olmak üzere dört sınıfta incelenmektedir [18].

1.4.3.1. Dayanıklı Damgalama

Görüntü içerisine gömülen damganın, görüntü işleme ve geometrik dönüşüm saldırılarına karşı ayakta kalabildiği damgalama yöntemidir. Damga, uygulanan

saldırıları sonrasında aynı özelliklerini koruyarak doğrulama işlemlerinde kullanılabilir. Bu damgalama yöntemi, telif hakkı koruması, yayın takibi, kopyalama kontrolü ve parmak izi uygulamalarında kullanılmaktadır [6].

Literatürde, dayanıklı damgalama yöntemi kullanılarak geliştirilmiş çeşitli çalışmalar mevcuttur.

Liu vd. [19], çeşitli tıbbi görüntülere hastane logosu ve görüntünün en ilgili alanı (ROI) kullanılarak elde edilen damgayı tüm görüntü üzerine gömerek kurcalama tespiti yapabilen, yapılan değişikliği kurtarabilen ve tersinir bir dayanıklı damgalama yöntemi geliştirmiştir. Geliştirilen yöntemde, özyinelemeli renk değişim modülasyonu, Slantlet dönüşümü ve Tekil Değer Ayrışımı birlikte kullanılmıştır. Yapılan çalışma sonunda 41.2995 dB PSNR ve 0.9607 YB değerleri elde edilmiştir. Önerilen yöntemde tersinirlik sağlayabilmek için orijinal tekil değerlerin saklanması ihtiyacı vardır.

Swaraja vd. [17], elektronik hasta kaydı ve ROI'den oluşan damgayı, Lempel-Ziv-Welch algoritmasını kullanarak sıkıştırmışlardır. Sıkıştırılan damga, kurcalama tespitini ve güvenliği sağlamak için damganın parlaklığına ait RONI bölgesine gizlenmiştir. Damgalama yönteminde, ADD, Schur dönüşümü ve bakteriyel besin arama optimizasyonu ile Parçacık Sürü Optimizasyon (PSO) algoritmasının birleşiminden oluşan hibrit bir algoritma kullanılmıştır. Damganın gömülmesinde, ADD'nin orta alt bantları tercih edilmiştir. Ataklara karşı en dayanıklı ve farkedilmezliği en yüksek damgalanmış görüntüyü elde edebilmek için optimizasyon algoritmasından faydalanılmıştır. Kurcalama tespiti yapabilen ve yapılan değişikliği kurtarabilen, dayanıklı damgalama kullanılarak gerçekleştirilen çalışma, çeşitli gri seviye ve renkli tıbbi görüntüler üzerinde denenmiş ve en yüksek 37.24 dB PSNR değeri elde edilmiştir.

Thakur vd. [12], hasta kimlik bilgisi ve hasta raporundan oluşan damgayı, manyetik rezonans (MR), X-Ray ve ultrason gibi çeşitli tıbbi görüntüleri kullanarak tüm giriş görüntüsü üzerine ADD, AKD ve TDA dönüşümlerini peş peşe uygulayarak gömmüşlerdir. Çalışmada, gömme sırasında bir kazanç faktörü kullanılmıştır. Bu kazanç faktörü düştükçe damgalanmış görüntünün görsel kalitesi yükselmektedir. Ayrıca, daha iyi gizlilik sağlayabilmek için damgalanmış görüntü üzerine kaos tabanlı şifreleme algoritması uygulanmıştır. 512×512 boyutundaki MR görüntüsü ile yapılan deneysel çalışma sonunda, deney içerisindeki en iyi normalleştirilmiş korelasyon (NK)

değeri 0.9989 olarak, 0.09 kazanç faktöründe elde edilmiştir. Bu kazanç faktöründe, PSNR 34.6099 ve YB 0.9967 olarak elde edilmiştir. Damganın çıkarılması esnasında, damga gömülmesinde kullanılan tekil değer matrisine ihtiyaç duyulmaktadır.

Selvam vd. [13], yaptıkları çalışmada tıbbi görüntülerde geleneksel yöntemlerde ihtiyaç duyulan anahtar bilgisi olmadan uygulanabilen, tersinir bir damgalama yöntemi önermişlerdir. Anahtar bilgisi ihtiyacı probleminin üstesinden gelebilmek için kapasiteyi arttırmayı hedeflemişlerdir. Bunun için, Tamsayı Dalgacık Dönüşümü (TDD) ve Ayırık Gould Dönüşümü birleşiminden oluşan hibrit bir dönüşüm yöntemi geliştirmişlerdir. Yapılan deneysel çalışmada, 2×2 'lik blok kullanımında en iyi kapasite değeri 0.25 bpp (Bit Per Pixel) olarak elde edilmiştir. 796 bit damga, 512×512 boyutundaki Lena görüntüsü üzerine gömüldüğünde 65.81 PSNR elde edilmiştir.

Ansari vd. [20], yaptıkları çalışmada ideal kayıpsız damgalama yönteminin beş temel gereksinimini (dayanıklılık, tersine çevrilebilirlik, farkedilmezlik, güvenlik ve kapasite), en üst düzeye çıkarabilen kayıpsız tersinir damgalama yönteminin geliştirmeyi hedeflemişlerdir. Geliştirilen yöntemde damga güvenliğini arttırmak için öncelikle Arnold dönüşümü uygulanmıştır. Daha sonra yüksek kapasite elde edebilmek ve dayanıklı bir damgalama yöntemi geliştirmek için Slantlet dönüşümü kullanmışlardır. Ayrıca farkedilmezlik, dayanıklılık ve kapasite arasındaki en uygun dengeyi sağlayabilmek için Yapay Arı Koloni (ABC) algoritması kullanmışlardır. Geliştirilen çalışma, yuvarlamalar sonucu meydana gelen piksellerdeki taşma ve aşağı kalma problemi için bu durumun meydana geldiği pikselleri ve yerlerini yan bilgi olarak tutmaktadır. Bu yan bilginin damganın çıkarılması sırasında alıcı tarafında bulunması gereklidir. 512×512 boyutundaki Lena görüntüsü ve 128×128 boyutundaki siyah-beyaz damga kullanılarak gerçekleştirilen deneysel çalışmada, gömme güç faktörü 3 için 8×8 'lik blok kullanımında 44.0372 PSNR elde edilmiştir.

Parah vd. [21], yapmış oldukları çalışmada tıbbi görüntülerin güvenliğini sağlamak için iki farklı damgalama yöntemi önermiştir. İlk yöntem, damgayı ve hasta kayıt bilgisini ROI ve RONI bölgesine gömerken, ikinci yöntemde ROI bölgesi korunurken RONI bölgesine damga ve hasta kayıt bilgisi gömülmüştür. İki yöntem içinde 8×8 'lik bloklar ve AKD katsayıları kullanılmıştır. 10 farklı 512×512 boyutundaki bilgisayarlı tomografi (BT) görüntüsü, damga olarak 32×32 ve 47×47 boyutunda logo ve 1024 bit hasta kaydı

kullanılarak gerçekleştirilen deneysel çalışma sonunda, ortalama PSNR değeri 40 dB üzerinde, gömme faktörü 10 için YB 0.9857 ve gömme faktörü 20 için YB 0.94064 elde edilmiştir.

Lei vd. [22], tıbbi görüntülerin saklanması ve transfer edilmesi sırasında meydana gelen güvenlik problemini çözebilmek için tersinir bir damgalama yöntemi önermiştir. Kimlik bilgisi ve metin verisi orijinal tıbbi görüntü içerisine, dalgacık dönüşümü ve TDA'nın ardından özyinelemeli renk değişikliği modülasyonu uygulanarak gömülmüştür. Ayrıca Diferansiyel Gelişim Algoritması (DGA), uygun örnekleme adımları elde edebilmek için damganın gömülme faktörünü belirlemede kullanılmıştır. 512×512 boyutundaki X-Ray, MR ve ultrason görüntüleri ile birisi metin diğeri logo olmak üzere iki 64×64 boyutundaki damga ile deneysel çalışmalar gerçekleştirilmiştir. Deneylerde dalgacık dönüşümleri ve TDA dönüşümü ile kombinasyonları için ayrı ayrı sonuçlar paylaşılmış ve en iyi farkedilmezlik değerinin TDD ile TDA dönüşümünün birleşiminden oluşan hibrit yöntemde elde edildiği görülmüştür. X-Ray görüntüsü için hibrit yöntemde, PSNR 48.39 dB ve ortalama YB 0.9934 elde edilmiştir.

Das ve Kundu [23], JPEG ve JPEG2000 sıkıştırma algoritmalarına karşı yüksek dayanıklılık sağlayabilen ve tıbbi görüntülerin güvenliğini sağlamayı amaçlayan bir kör tıbbi görüntü damgalama yöntemi önermişlerdir. Geliştirilen yöntemde, Contourlet dönüşümünün düşük frekanstaki alt bantları kullanılmıştır. Yapılan deneysel çalışmalarda, 512×512 boyutunda çeşitli tıbbi görüntülere, EHK, doktor kimlik bilgisi, anahtar kelime indeksi ve opsiyonel olarak ROI bölgesini içeren bir damga gömülmüştür. 512×512 boyutundaki karın bölgesine ait BT görüntüsü için PSNR 34.8498 ve ortalama YB 0.7887 elde edilmiştir.

1.4.3.2. Kırılğan Damgalama

En ufak değişimde gömülen damganın bozulduğu, genellikle görüntünün bütünlüğünün ve içeriğinin doğrulandığı uygulamalarda kullanılan damgalama türüdür [4]. Kırılğan damgalama, görüntü üzerinde kurcalama olup olmadığı ile ilgili bilgi sağlayabilmektedir [6].

Literatürde, kurcalama yer tespiti, veri doğruluğunun ispatı ve veri bütünlüğünün ispatı gibi amaçlara yönelik geliştirilmiş birçok çalışma mevcuttur.

Gül ve Öztürk [24], giriş görüntüsünü 16×16 boyutundaki bloklara bölerek, damga bilgisini, iki en anlamsız bit kullanarak gömmüştür. Yaptıkları çalışma ile görüntüde, kurcalama yer tespiti yapabilen ve %75 oranına kadarki yapılan değişiklikleri kurtarabilen, kırılğan bir damgalama yöntemi geliştirmiştir. Çalışmada, iki en anlamsız bit kullanılması farkedilmezlik değerini düşürmüştür. Lena görüntüsü ile yapılan deney sonunda, 44.127 dB PSNR ve 0.9785 YB elde edilmiştir.

Hurrah vd. [25], kullandıkları beyin MR görüntüsü içerisine ikili sayı değerlerinden oluşan bir logoyu, EAB yöntemi ile tüm görüntü üzerine gömmüştür. Damga gömülmeden önce, Arnold haritası ve Gelişmiş Şifreleme Standardı ile şifrelenmiştir. Kurcalama yer tespiti yapabilen tersinir ve kırılğan damgalama yöntemi kullanılmıştır. Önerilen yöntemin gömme kapasitesi, 512×512 boyutundaki giriş görüntüsü ve 8×8 bloklar için 4096 bittir. 512×512 boyutundaki 30 farklı tıbbi görüntü, 64×64 boyutundaki siyah-beyaz damga görüntüsü ve 8×8 boyutundaki bloklar kullanılarak yapılan deneysel çalışmalar sonunda ortalama 61.17 PSNR elde edilmiştir.

Gül ve Öztürk [26], giriş görüntüsünü öncelikle 32×32 boyutundaki bloklara bölmüştür. Daha sonra bu 32×32 blokları, 16×16 büyüklüğündeki dört bloğa ayırmıştır. SHA-256 kullanarak dört bloğun üçünden elde etmiş oldukları özet bilgiyi dördüncü bloğa EAB yöntemi yardımı ile gömmüşlerdir. Yaptıkları çalışma ile görüntüde kurcalama yer tespiti yapabilen, kırılğan bir damgalama yöntemi geliştirmişlerdir. Çalışmada, 16×16 büyüklüğünde bloklar kullanılması kurcalama yer tespitinin hassasiyetini düşürmüştür. 512×512 boyutundaki Lena görüntüsü ile yapılan deney sonunda, 57.196 dB PSNR elde edilmiştir.

Tai ve Liao [27], veri doğrulama ve bütünlüğünü sağlamak amacı ile kurcalama yer tespiti yapabilen ve yapılan değişikliği kurtarabilen kırılğan bir damgalama yöntemi önermiştir. Damga olarak, her 4×4 'lük blok için 4 biti doğrulama ve 28 biti kurtarma biti olmak üzere, toplam 32 bit kullanılmıştır. Kurcalamadan etkilenen blokları yüksek oranda kurtarabilmek için blokların kurtarma bilgileri değişikliğin yapıldığı yerden uzak eş bloklara gömülmektedir. Bu amaç ile oluşturulan blok haritası Arnold haritası yardımı ile oluşturulmaktadır. Ayrıca, her bloğun farklı bölgelerde yer aldığından emin olmak için blok haritası, anahtar tabanlı sözde rastgele permütasyon algoritması kullanılarak tekrar oluşturulmuştur. Damganın gömülmesinde TDD ve EAB yöntemleri

birlikte kullanılmıştır. Yapılan deneysel çalışmalarda, kolaj saldırıları, sürekli ortalama saldırıları ve büyük oranda yapılan kurcalamalar sonunda elde edilen sonuçlar paylaşılmış ve kıyaslanan blok tabanlı çalışmalara göre daha iyi sonuçlar elde edilmiştir. 512×512 boyutundaki Lena görüntüsü ile yapılan deneysel çalışmada, 44.14 PSNR değeri elde edilmiştir.

Parah vd. [28], nesnelerin interneti odaklı bir sağlık sisteminde, tıbbi görüntülerde tersinir, yüksek kapasiteli, güvenli ve etkili hesaplama maliyetli bir elektronik sağlık kaydı gizleme yöntemi önermiştir. Yapılan çalışmada, piksel yineleme metodu ve modüler aritmetik yöntemleri kullanılmıştır. Piksel yineleme metodu ile giriş görüntüsü iki katına çıkarılarak damgalama işlemi gerçekleştirilmektedir. 512×512 boyutundaki Lena görüntüsü ile yapılan deneysel çalışmada, 39.09 PSNR ve 2.25 bpp kapasite elde edilmiştir. Damgalanmış görüntünün boyutu iki katına çıkarılması hem orijinal görüntüde bozulmaya sebep olmuş hem de ihtiyaç duyulan depolama alanını arttırmıştır.

Rahman vd. [29], tıbbi görüntülerde gizliliği sağlamak, yapılan kurcalamaları tespit etmek ve yapılan kurcalamaları kurtartmak amacı ile tersinir bir damgalama yöntemi önermişlerdir. Gizli bir anahtar yardımı ile orijinal görüntüden kaotik olarak üretilen damga, görüntü üzerinde kaotik olarak seçilen piksellere döngüsel artıklık denetimi ve xor lojik operasyonu yöntemleri kullanılarak gömülmektedir. 348×314 boyutundaki MR ve ultrason görüntülerine, 55×55 boyutundaki damga kullanılarak yapılan deneysel çalışma sonunda 72.98 dB PSNR elde edilmiştir.

Parah vd. [30], e-sağlık uygulamalarında kullanılabilecek yüksek kapasiteli ve tersinir bir damgalama yöntemi önermiştir. Yapılan çalışmada, tüm görüntü üzerine 4×4'lük bloklardan hesaplanmış sağlama toplamı ve hasta bilgisi ortanca EAB yöntemi kullanılarak gömülmüştür. Damga bilgisi, doğrusal olmayan kaos algoritması ile şifrelenerek gömülen verinin güvenliği artırılmıştır. Damga gömülmeden önce giriş görüntüsünün boyutu iki katına çıkarılmaktadır. Çeşitli X-Ray görüntüleri üzerine yapılan deneysel çalışmalar sonunda, ortalama PSNR 46.3698 dB, ortalama YB 0.9827 ve 0.75 bpp kapasite elde edilmiştir. Damgalanmış görüntünün boyutu iki katına çıkarılması hem orijinal görüntüde bozulmaya sebep olmuş hem de ihtiyaç duyulan depolama alanını arttırmıştır.

Shih vd. [31], veri doğrulama ve bütünlüğünü sağlamak amacı ile kullanılacak uygulama türüne göre ayarlanabilen, tersinir ve kırılğan bir damgalama yöntemi önermişlerdir. Görüntü ROI ve RONI bölgesi olarak ayrıldıktan sonra damga bilgisi, Parçacık Sürü Optimizasyon algoritmasının sunduğu en uygun çözüme göre RONI bölgesine gömülmektedir. Damga bilgisi, RONI bölgesine ADD, TDA ve AKD dönüşümlerinin birlikte kullanılması ile gömülmektedir. 500×300 boyutundaki bir doğa görüntüsüne, siyah-beyaz damga gömülmesi ile 57.33 PSNR elde edilmiştir.

Nguyen vd. [32], görüntü doğrulama amacı ile tersinir ve yüksek doğrulukta yer değişikliği tespiti yapabilen bir yöntem önermişlerdir. Yapılan çalışmada, damga bilgisi iki seviyeli ADD ve 8×8 boyutunda bloklar kullanılarak gömülmüştür. Fakat çalışmada, damgalanmış görüntü pikselleri reel sayı değerlerinden, tam sayı değerlerine dönüştürülmemiştir. Bu yüzden yöntem, reel sayı veri tiplerini desteklemeyen uygulama alanlarında kullanılamamaktadır. 512×512 boyutundaki Lena görüntüsü üzerinde yapılan deneysel çalışmalar sonunda, 83.52 PSNR değeri elde edilmiştir.

1.4.3.3. Yarı-Kırılğan Damgalama

Yarı-kırılğan damgalama yöntemleri, gömülen damgayı kasti olan saldırılara karşı dayanıklı davranırken, kötü amaçlı saldırılara karşı kırılğan davranmaktadır. Burada bahsi geçen kasti saldırılara resmi keskinleştirme, koyulaştırma, histogram eşitleme, parlaklığını arttırma gibi uygulamalar örnek verilebilir. Yarı-kırılğan damgalama yöntemlerinde, bu tür bilinçli yapılan uygulamalarda damganın bozulmaması arzu edilirken kötü amaçlı yapılan belirgin saldırılarda bozulması istenir [5].

Cui [33], görüntünün ROI bölgesinin doğrulaması ve kurcalama yer tespitini sağlayan bir damgalama yöntemi önermiştir. Damga, RONI bölgesinin ADD katsayıları kullanılarak gömülmüştür. Lena görüntüsü üzerine yapılan deneysel çalışmalarda, 36.61 PSNR elde edilmiştir.

1.4.3.4. Hibrit Damgalama

Hibrit damgalama yöntemi, kırılğan damgalama ve dayanıklı damgalamanın birleşimi olarak geliştirilmiştir. Aynı anda veri doğruluğunun ispatı, veri bütünlüğünün ispatı ve telif hakkı korumasını sağlayabilmektedir [7,18].f

Memon vd. [18], tıbbi görüntülerde güvenlik, gizlilik ve bütünlüğü sağlamak için hibrit bir yöntem önermişlerdir. Bu yöntemde güvenlik ve gizliliği sağlamak amacı ile görüntü içerisine ROI bölgesinin en anlamsız bitleri, hasta kayıt bilgileri, doktor kimlik numarasından oluşan dayanıklı bir damga gömülürken, bütünlük kontrolünü sağlamak için ROI bölgesinden oluşan kırılğan bir damga gömülmüştür. 256×256 boyutundaki 8 bit gri seviyeli BT, ultrason, X-Ray ve MR görüntüleri kullanılarak yapılan deneysel çalışmalar sonunda elde edilen sonuçlar PSNR alternatifi ağırlıklandırma faktörü içeren bir kalite ölçüm metriği olan ağırlıklandırılmış PSNR ile gösterilmiştir. Ağırlıklandırılmış PSNR değeri en yüksek 60.9420 dB olarak elde edilmiştir. Çalışmada veri kapasitesi ile ilgili bilgi verilmemiştir.

1.5. Görüntü Damgalamada Karşılaşılan Saldırıları

Görüntü üzerine uygulanan yaygın ataklar çıkarma, geometrik, protokol ve kriptografik saldırılar olmak üzere dört grupta incelenmektedir [4]. Bu saldırılar görüntünün transferi sırasında kasıtlı veya kasıtlı olmadan gerçekleştirilebilir. Özellikle dayanıklı damgalama uygulamalarında dayanıklılığı ölçmek için, damgalanmış görüntü üzerine çeşitli ataklar uygulandıktan sonra damga çıkarılarak orijinal olan görüntü ile kıyaslanır. Dayanıklı damgalama sistemlerinde, çıkarılan damganın saldırılara direnmiş ve damgalanmış görüntü kalitesini korumuş olması beklenir [6].

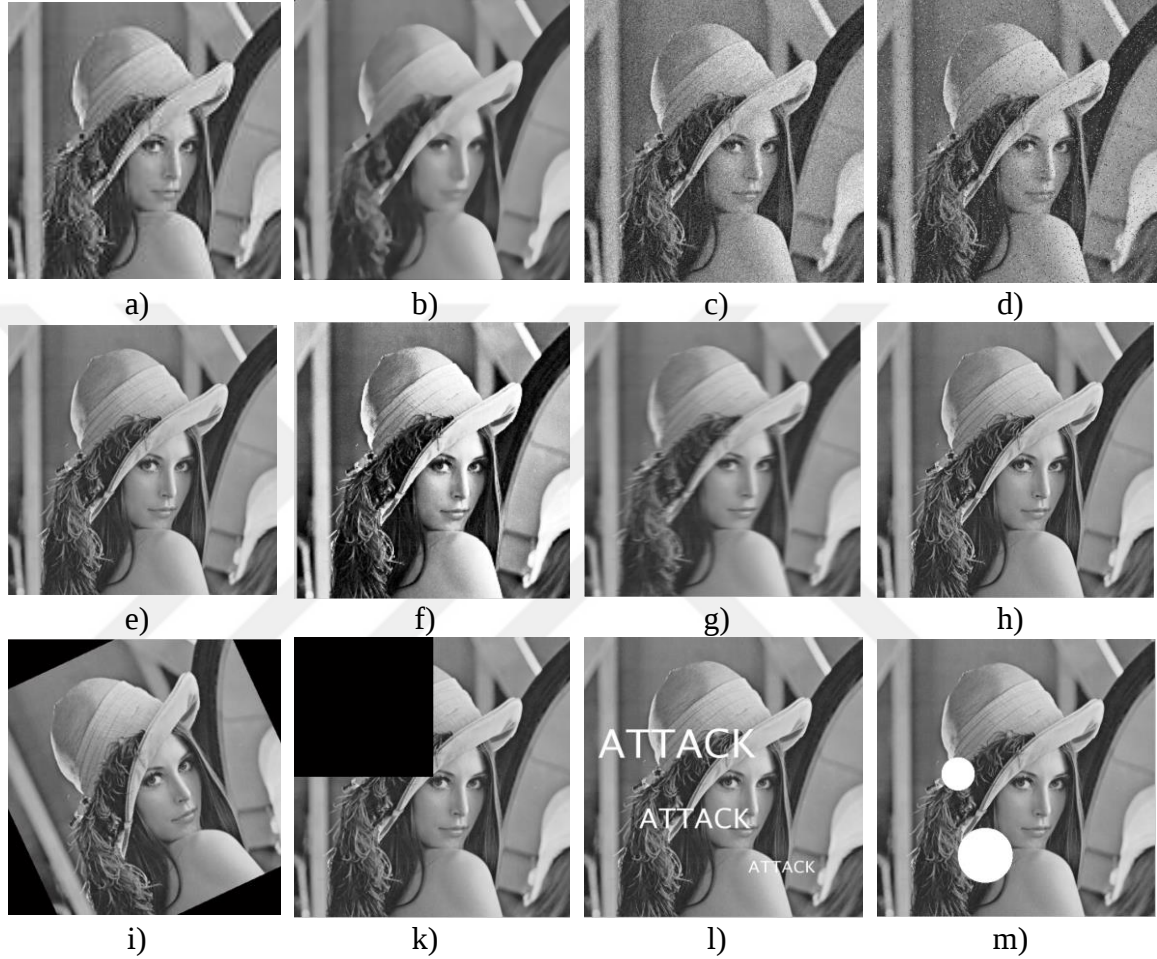
Çıkarma atakları, damgalamada kullanılan damgayı, gizli anahtar olmadan çıkarmak veya bozmak amacı ile yapılan ataklardır. Bu ataklar damgayı tamamen kaldıramasa da damga üzerinde ciddi bozulmalar meydana getirir [6].

Geometrik dönüşüm saldırıları, sıkıştırma, kırpma, döndürme, ölçekleme gibi görüntünün geometrik yapısını bozacak damgaya zarar verme amacı ile yapılan saldırılardır [6].

Protokol saldırıları, belirsizlik oluşturma veya kopyalama amaçları ile gerçekleştirilebilir. Belirsizlik saldırılarında, saldırgan tarafından sahipliğini iddia etmek ve belirsizlik oluşturmak için damgalanmış görüntü içerisinden kendine ait bir damga çıkarılmaktadır. Kopyalama saldırılarında ise damga tahmin edilerek tahrip edilmeden başka bir veri üzerine kopyalanması ile oluşturulan saldırılardır [6].

Kriptografik saldırılar, damgalama yönteminde kullanılan anahtara zarar vermeye yönelik yapılan saldırılardır [6].

Görüntü üzerine uygulanan yaygın ataklar Şekil 1.8’de verilmiştir.



Şekil 1.8. Lena görüntüsü üzerine uygulanmış bazı yaygın kullanılan ataklar;

- a) Orijinal Görüntü, b) Medyan, c) Gaussian Gürültü, d) Tuz-Biber Gürültüsü, e) JPEG Sıkıştırma, f) Histogram Eşitleme, g) Bulanıklaştırma, h) Keskinleştirme, i) Döndürme, k) Kırpma, l) Metin Ekleme, m) Şekil Ekleme

1.6. Görüntü Kalite Metrikleri

Literatürde damgalama yöntemlerinin başarılarının ölçülmesi için birçok farklı görüntü kalite metrikleri kullanılmaktadır. Kalite metrikleri, değerlendirme için referans görüntüye ihtiyaç duyma durumlarına göre sınıflandırılmaktadır. Referans görüntüye

ihtiyaç duyan kalite metrikleri referans tabanlı, referans görüntüye ihtiyaç duymayan kalite metrikleri ise objektif metrikler olarak adlandırılmaktadır [34].

Gömülen damganın görüntü üzerine olan etkisini değerlendirmek için damgalı görüntü ile orijinal görüntü kullanılırken, damgalama yönteminin dayanıklılığının ölçülmesinde çıkarılan damga ile orijinal damga kullanılmaktadır.

1.6.1. Ortalama Karesel Hata:

MSE, iki görüntü piksel değerleri arasındaki ortalama kare farkını ölçmektedir. İki görüntü birbirine ne kadar yakınsa MSE o kadar düşük olmaktadır. $m \times n$ boyutundaki orijinal görüntü I ve damgalanmış görüntü I_w için MSE, Denklem 1.6'da verilmiştir [7].

$$MSE(I, I_w) = \frac{1}{mn} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} (I(i, j) - I_w(i, j))^2 \quad (1.6)$$

1.6.2. Tepe Sinyal Gürültü Oranı:

PSNR, orijinal görüntü ile damgalanmış görüntü arasındaki benzerliğin ölçülmesinde kullanılmaktadır. Yüksek PSNR değeri, iki görüntü arasındaki benzerlik miktarının arttığını göstermektedir [4]. PSNR desibel (dB) olarak ifade edilmektedir.

$$PSNR(I, I_w) = 10 * \log_{10} \frac{\max_I^2}{MSE(I, I_w)} \quad (1.7)$$

Denklemde I ve I_w sırasıyla giriş görüntüsü ve damgalanmış görüntüyü temsil etmekte, $\max_I$ ise giriş görüntüsünün maksimum piksel değerini ifade etmektedir. Tez çalışmasında yapılan deneylerde görüntüler gri seviyede 8 bit olarak kodlandığı için $\max_I$ değeri 255 olarak alınmıştır.

1.6.3. Yapısal Benzerlik İndeksi:

Görüntülerin birbirine yapısal olarak benzerliğini ölçmekte kullanılmaktadır. Referans tabanlı bir kalite metriğidir. Diğer kalite metriklerinin insan göz algısına uygun olmadığı için geliştirilmiş bir kalite metriğidir. Yapısal benzerlik ölçümünde parlaklık, kontrast ve yapısal bilgi olmak üzere üç bileşen kıyaslanmaktadır. YB değeri -1 ile 1

arasında değişmektedir. YB değerinin 1 olması damgalanmış görüntünün orijinal görüntü ile birebir benzer olduğunu ifade etmektedir [35].

$$YB(I, I_w) = \frac{(2\mu_I\mu_{I_w} + c_1)(2cov + c_2)}{(\mu_I^2 + \mu_{I_w}^2 + c_1)(\sigma_I^2 + \sigma_{I_w}^2 + c_2)}$$

$$\begin{cases} c_1 = (k_1L)^2 & k_1 = 0.01 \\ c_2 = (k_2L)^2 & k_2 = 0.03 \end{cases} \quad (1.8)$$

Denklemde yer alan, μ_I ve μ_{I_w} sırası ile orijinal ve damgalanmış görüntülerin ortalama değerleri, σ_I^2 ve $\sigma_{I_w}^2$ sırası ile orijinal ve damgalanmış görüntülerin varyans değerleri, cov damgalanmış görüntünün kovaryansı, c_1 ve c_2 bölümü dengelemek için kullanılan sabitler, L ise dinamik parametre aralığıdır. Tez çalışmasında 8 bit gri seviyeli görüntü kullanıldığı için 255 olarak alınmaktadır ($L=2^{\text{piksel başına düşen bit sayısı}}-1$) [4].

1.6.4. Bit Hata Oranı (BHO):

BHO, damgalama yönteminde iletilen toplam bit sayısının, yanlış çözülmüş bitlere oranının yüzde olarak ifade etmektedir. İdeal bir damgalama yönteminde BHO sıfır olmalıdır [4].

$$BHO = \frac{(\text{Hatalı çözülmüş Bit Sayısı})}{(\text{Toplam Bit Sayısı})} \quad (1.9)$$

1.7. Zeki Optimizasyon Algoritmaları

Sayısal damgalama yöntemlerinin geliştirilmesinde, Parçacık Sürü Optimizasyon (PSO) algoritması, Genetik Algoritma (GA), Yapay Arı Koloni (ABC) algoritması ve Diferansiyel Gelişim Algoritması (DGA) gibi zeki optimizasyon algoritmaları kullanılabilir.

Zeki optimizasyon algoritmaları, sayısal damgalama yöntemlerinde ataklara karşı direncin artırılması [18,22], gömülecek damga miktarının belirlenmesi [31] ve yüksek fark edilebilirlik elde edebilmek için damganın gömüleceği konumun belirlenmesi [36] gibi farklı amaçlar ile kullanılarak damgalama yönteminin geliştirilmesine katkı sağlamaktadır.

1.7.1. Parçacık Sürü Optimizasyon Algoritması

PSO algoritması, sürü halinde hareket eden kuş veya balık gibi hayvanların davranışlarından esinlenerek 1995 yılında Kennedy ve Eberhart tarafından geliştirilen popülasyona dayalı bir sezgisel optimizasyon tekniğidir [37].

PSO algoritması, optimal çözümü bulmak için arama yapan bireyleri (parçacıklar) içeren sürü adı verilen bir popülasyon oluşturur. Arama bölgesinde, bu popülasyon içindeki tüm parçacıklar birbirleri ile bilgi paylaşımı yapar. Bu bilgi paylaşımını esas alarak her parçacık, önceki uygunluk değerlerini kullanarak sürüdeki optimum pozisyonunu belirlemeye çalışır. Bu da parçacığın, kendi en iyi çözümüne ve global en iyi çözümüne yönelmesini sağlar.

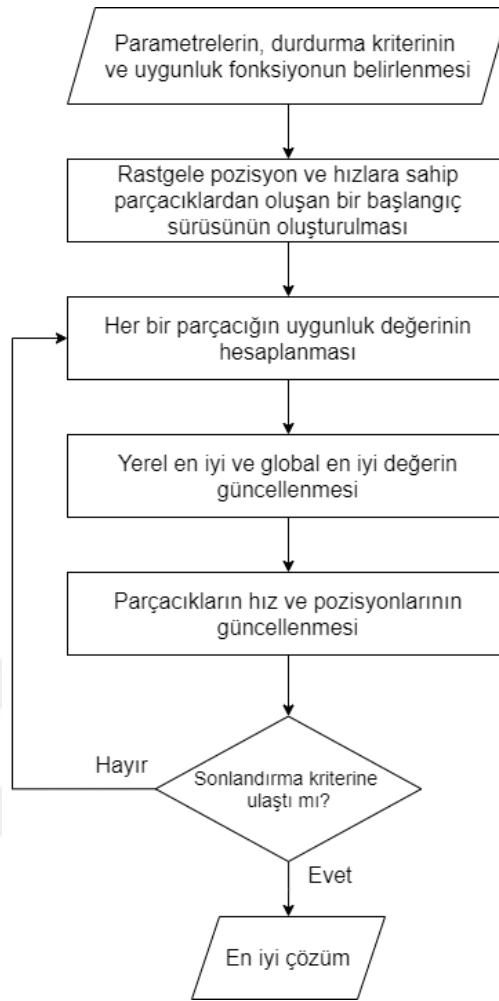
PSO algoritmasında, öncelikle başlangıç sürüsü oluşturulur. Süredeki çözümü arayacak olan parçacıkların pozisyonları ve hızları rastgele olarak belirlenir. Her bir iterasyonda, parçacıkların hızları (L_i) ve pozisyonları (P_i) sırası ile Denklem 1.10 ve Denklem 1.11 kullanılarak güncellenir.

$$L_i(i + 1) = \omega L_i(i) + C_1 \Phi_1 (y_{eni yi} - P_i(n)) + C_2 \Phi_2 (g_{eni yi} - P_i(n)) \quad (1.10)$$

$$P_i(i + 1) = P_i(i) + L_i(i + 1) \quad (1.11)$$

Denklem 1.10'da yer alan C_1 ve C_2 sırasıyla $y_{eni yi}$ ve $g_{eni yi}$ için ivmelenme sabitlerini, Φ_1 ve Φ_2 [0 1] aralığında düzgün dağıtılmış rastgele üretilen değerler, ω parçacığın momentumunu kontrol eden eylemsizlik ağırlığını ifade etmektedir.

Her iterasyonda amaç fonksiyonu kullanılarak parçacıkların uygunluk değerleri hesaplanır. Tüm parçacıklar içerisindeki en iyi uygunluk değerine sahip olan parçacık global en iyi ($g_{eni yi}$) olarak tanımlanır. Her bir parçacığın almış olduğu değerler içindeki en iyi uygunluk değeri ise yerel en iyi ($y_{eni yi}$) olarak tanımlanır. Daha sonra parçacıkların yapacakları hareket belirlenerek değişim hızları ve yeni pozisyonları atanır. İterasyonlar, sonlandırma kriterine ulaşıncaya kadar devam eder [17]. PSO algoritmasına ait akış diyagramı Şekil 1.9'da gösterilmiştir.

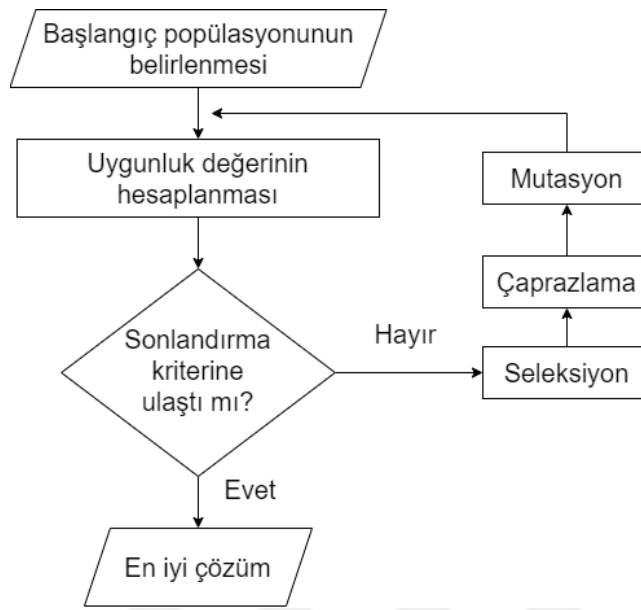


Şekil 1.9. PSO algoritması akış diyagramı

1.7.2. Genetik Algoritma

GA, doğal seleksiyon ilkelerine dayanan, 1975 yılında Holland [38] tarafından ilk kez ortaya atılan bir arama ve optimizasyon yöntemidir.

GA, belirli bir problemin olası aday çözümlerini içeren rastgele popülasyonlar oluşturur. Popülasyondaki her birey kromozom olarak adlandırılmaktadır. Oluşturulan popülasyondaki her bir birey için amaç fonksiyonu kullanılarak uygunluk değerleri hesaplanır. Bu uygunluk değerlerine göre doğal seleksiyon, çaprazlama ve mutasyon genetik operatörleri kullanılarak her iterasyonda çözümler geliştirilerek problemin en uygun çözümü aranır. Bu iterasyonlar sonlandırma kriteri sağlanana kadar devam eder ve iterasyonlar sonunda elde edilen çözüm en iyi (optimal) çözüm olarak atanır [39]. Basit bir GA akış şeması Şekil 1.10'da gösterilmiştir.

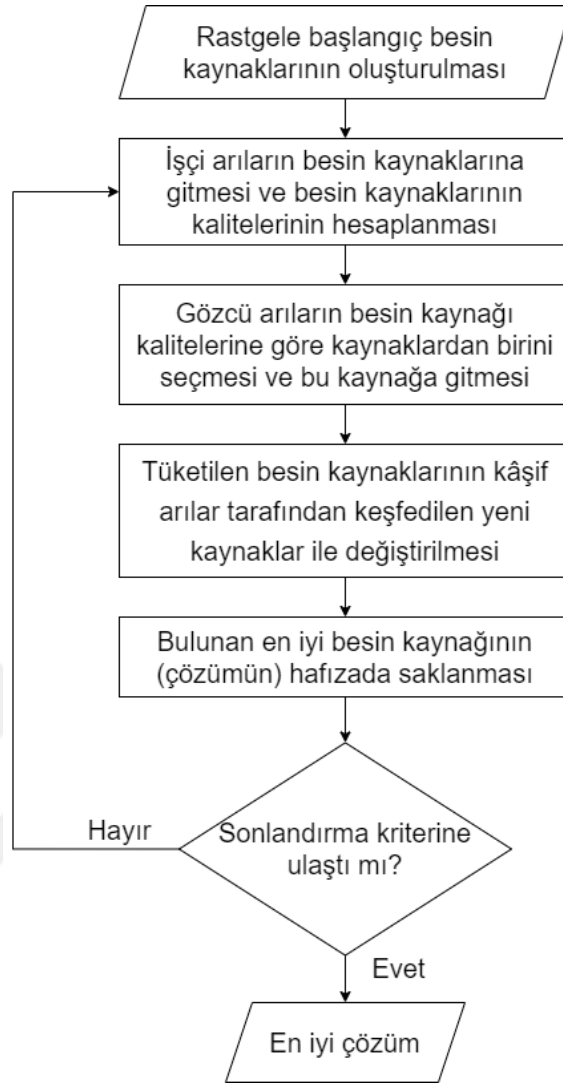


Şekil 1.10. Genetik Algoritma akış şeması

1.7.3. Yapay Arı Koloni Algoritması

ABC algoritması, arı kolonilerinin besin arama sırasında göstermiş oldukları zeki davranışları modelleyen Karaboğa tarafından 2005 yılında literatüre kazandırılmıştır [40].

ABC algoritmasında işçi, gözcü ve kâşif olmak üzere üç tip arı sınıfı bulunmaktadır. ABC algoritması modellenirken bazı varsayımlar kullanılır. Bu varsayımlara göre, kovadaki işçi arıların sayısı kovanın çevresindeki besin kaynaklarının sayısına eşittir. Böylece, başlangıç kolonisinin yarısı işçi arılardan oluşurken diğer yarısı gözcü arılardan oluşmaktadır. Besin kaynaklarının konumları araştırılan olası muhtemelen aday çözümleri, kaynakların besin miktarları ise ilgili çözümlerin kalitesini ifade etmektedir. Her bir kaynak tek bir işçi arı tarafından tüketilir ve bu işçi arılar kovana geri döndüklerinde bekleyen gözcü arılara gerçekleştirdikleri dans hareketleri ile kaynağın kalitesi ve konumu hakkında bilgi verir. Gözcü arılar aldıkları kalite bilgisine göre kaynak seçimi yapar ve seçilen kaynağa komşu kaynak arayışları gerçekleştirir. Kaynak arayışları, belirlenen limit “ L ” parametre değeri boyunca mevcut kaynağın komşu kaynaklar ile değiştirilip değiştirilemeyeceğine bakılır. Değiştirilebilecek daha iyi bir kaynak bulunamaması kaynağın tükenmiş olduğunu ifade eder ve işçi arılar kaynağı terk ederek kâşif arı olarak yeni kaynak arayışına girerler. ABC algoritmasının temel işlem adımları Şekil 1.11’de gösterilmiştir [40].



Şekil 1.11. ABC algoritması temel işlem adımları

1.7.4. Diferansiyel Gelişim Algoritması

DGA, temelinde GA'ya dayanan 1996 yılında Storn ve Price [41] tarafından geliştirilen popülasyon tabanlı sezgisel bir optimizasyon algoritmasıdır. Doğrusal olmayan gerçel değerli fonksiyonları optimize etmek ve birden fazla yerel minimuma sahip problemlerde yaklaşık çözüm bulmak için DGA kullanılmaktadır. Ayrıca DGA, az sayıda kontrol parametresi gerektirme, dayanıklılık, hızlilik, kolay kullanılabilirlik, türev işlemleri gerektirmeme ve paralel hesaplama kolay uyum sağlayabilme özelliklerine sahiptir [42].

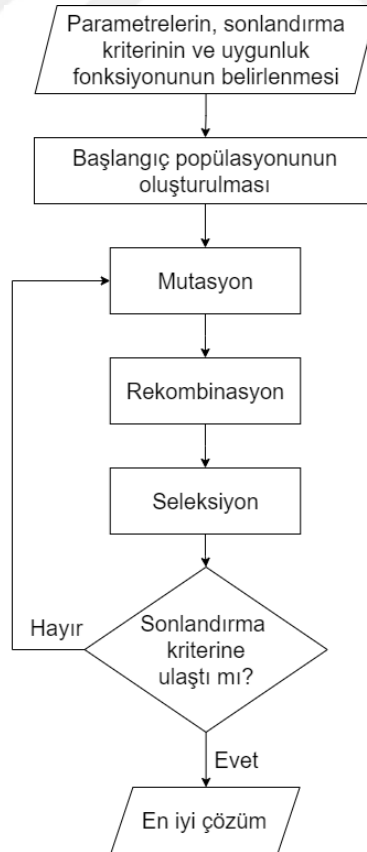
GA'da kullanılan seleksiyon, çaprazlama ve mutasyon bu algorithmada farklı olarak kromozomlara tek tek uygulanarak daha iyi bireyler üretilmeye çalışılır [42].

DGA, başlangıç parametreleri, amaç fonksiyonu ve sonlandırma kriteri tamamlandıktan sonra arama uzayındaki başlangıç popülasyonunun rastgele oluşturulması ile başlar. Popülasyon, mutasyon, seleksiyon ve rekombinasyon ile sonlandırma kriteri sağlanana kadar geliştirilir. Mutasyon operatörü, daha önce elde edilmemiş çözümleri üretmek için kullanılır. Rekombinasyon operatörü ise daha önceki nesillerden gelen kaliteli çözümleri birleştirmek için kullanılır. DGA'ya ait akış şeması Şekil 1.12'de gösterilmiştir.

Başlangıç popülasyonunun büyüklüğü NP ve değişken sayısı (Kromozomdaki gen sayısı) D için başlangıç çözümlerinin popülasyonu Denklem 1.11 ile üretilir.

$$x_{j,i,G} = x_j^U + rand_j[0,1](x_j^U - x_j^L), \quad i = (1, \dots, NP), \quad j = (1, \dots, D) \quad (1.11)$$

Denklemde, G indis değeridir ve 0 ile başlar. Popülasyona kaç nesil boyunca mutasyon, rekombinasyon ve seleksiyon uygulanacağını belirtir. x_j^L ve x_j^U sırasıyla alt ve üst başlangıç sınırlarını ($x_j^L \leq x_{j,i,0} \leq x_j^U$) ifade etmektedir.



Şekil 1.12. Diferansiyel Gelişim Algoritması akış şeması

Arama uzayını genişletmek ve farklı çözümler elde etmek için kromozomlara mutasyon uygulanır. Mutasyon ile mevcut kromozomun genleri üzerinde rastgele belirlenmiş miktarda değişiklikler yapılır. Böylece tek bir noktada takılıp kalmanın önüne geçilmiş olur. Mutasyon uygulanacak kromozom dışında birbirlerinden farklı olan üç kromozom seçilir ($r_{1,2,3}$) ve çaprazlamada kullanılacak mutant kromozomu elde etmek için Denklem 1.12 uygulanır.

$$v_{i,G+1} = x_{r_1,G} + F \cdot (x_{r_2,G} - x_{r_3,G}) \quad (1.12)$$

$$r_1, r_2, r_3 \in \{1, 2, \dots, NP\}, r_1 \neq r_2 \neq r_3 \neq i, F \in [0, 2], \quad (1.13)$$

burada, F parametresi ölçekleme faktörüdür ve seçilen iki kromozom arasındaki farkın etkisini kontrol eden sabit bir değerdir. F değerinin küçülmesi yakınsamanın hızlanmasını sağlarken, değerinin yükselmesi popülasyondaki farklılaşmayı arttıracaktır.

Rekombinasyon ile önceki nesillerden elde edilmiş olan başarılı çözümler çaprazlanarak daha iyi çözümlere ulaşılmaya çalışılır. Aday çözüm $u_{j,i,G+1}$ Denklem 1.14 kullanılarak elde edilir.

$$u_{i,G+1} = \begin{cases} rand_{j,i}[0,1] \leq CR \text{ veya } j = j_{rand} \text{ için } u_{j,i,G+1} \\ rand_{j,i}[0,1] > CR \text{ ve } j \neq j_{rand} \text{ için } x_{j,i,G} \end{cases}, \quad (1.14)$$

burada, $j = [1, 2, \dots, D]$, $rand_{j,i} \in [0, 1]$ rastgele üretilen sayı, $u_{j,i,G+1}$ mutasyon sonucu elde edilen vektörün parametre değeri, $x_{j,i,G}$ hedef vektörün parametre değeri, yeni vektörde hangi oranda çaprazlama yapılacağını belirleyen $CR \in [0, 1]$ çaprazlama sabiti ve $j_{rand} \in [1, 2, \dots, D]$ rastgele seçilen indis değerini ifade eder.

Üretilen yeni çözümün yeni nesle dâhil edilip edilmeyeceğine, üretilen çözümün mevcut nesil ile aç gözlü bir yaklaşım kullanılarak karar verilir. Kıyaslanan çözümlerden uygunluk değeri yüksek olan çözüm yeni nesle dâhil edilir. Seleksiyon işlemi Denklem 1.15 kullanılarak gerçekleştirilir.

$$x_{i,G+1} = \begin{cases} f(u_{i,G+1}) \leq f(x_{i,G}) \text{ için } u_{i,G+1} \\ \text{diğer durumlar için } x_{i,G} \end{cases}, \quad (1.15)$$

burada, $f()$ optimize edilmeye çalışan amaç fonksiyonunu ifade etmektedir [43].

2. BÖLÜM

TERSİNİR KIRILGAN SAYISAL DAMGALAMA

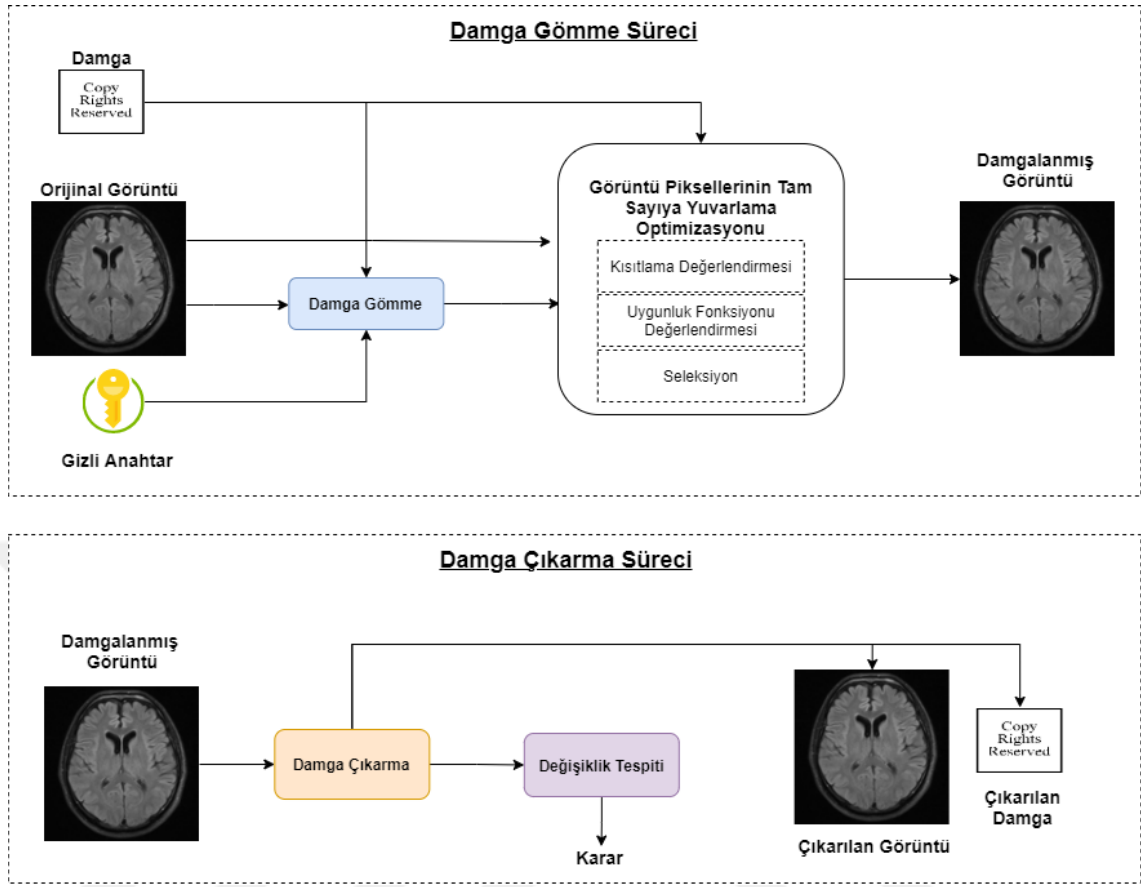
2.1. Giriş

Tıbbi görüntüler, tanı ve tedavide kullanılan, hayati öneme sahip verilerdir. Bu sebeple, geliştirilecek görüntü damgalama yönteminin, görüntüye gömülen damganın çıkarılmasının ardından orijinal tıbbi görüntüye kayıpsız bir biçimde geri dönebilmesi önemli bir husustur. Görüntü damgalama ve damga çıkartma süreçlerinin ardından kayıpsız bir şekilde orijinal görüntüyü elde edebilen bu türden görüntü damgalama yöntemleri, tersinir yöntemler olarak adlandırılmaktadır. Bu tez çalışmasında, damgalanmış görüntü üzerine uygulanan kasti veya kasti olmayan kurcalamaları tespit edebilen, kırılğan ve tersinir yeni bir görüntü damgalama yöntemi önerilmektedir.

Bu bölümde, önerilen tersinir kırılğan sayısal damgalama yöntemi detaylı bir şekilde açıklanmıştır.

2.2. Tersinir Kırılğan Sayısal Damgalama

Önerilen sayısal damgalama yöntemi, yüksek farkedilmezliğe sahip damgalanmış görüntü, damga çıkarma sonrasında kayıpsız orijinal görüntü sunma ve damgalanmış görüntü üzerinde yapılan kurcalamaların tespiti özelliklerine sahiptir. Geliştirilen yöntemin genel şeması Şekil 2.1'de gösterilmiştir. Genel damgalama sistemi karakteristiğinden farklı olarak, damganın gömülmesi sırasında arzu edilen en uygun damgalanmış görüntüyü elde etmek için zeki optimizasyon algoritmalarından faydalanılmıştır. Ayrıca, geliştirilen yöntem ile kurcalama yer tespiti için gömülen damganın alıcıya gönderilmesine veya damganın depolanmasına gerek kalmamaktadır.



Şekil 2.1. Geliştirilen damgalama yönteminin genel şeması

Geliştirilen yöntemde, öncelikle güvenliğin artırılmasında kullanılan anahtar tabanlı karıştırma algoritması ile damganın gömüleceği bloklar karıştırılmaktadır. Aynı gizli anahtar, alıcı tarafında damganın çıkarılması sürecinde blok haritasının oluşturulmasında kullanılmaktadır.

Karıştırılmış görüntü bloklarına damganın gömülmesi, her bir kaynak görüntü bloğuna, Ayrık Dalgacık Dönüşümü (ADD) uygulanarak dönüşüm katsayılarının elde edilmesi ve ardından bu dönüşüm katsayılarının değiştirilmesi ile gerçekleştirilmektedir. Damga gömme işlemi tamamlandıktan sonra, damgalanmış görüntü frekans uzayından, resim uzayına dönüştürülür. Dönüşüm sonrasında, reel sayılardan oluşan piksel değerleri elde edilir. Fakat görüntü formatlarının birçoğu tam sayı piksel değerleri ile ifade edilmektedir. Bu yüzden, reel sayılardan tam sayıya dönüşüm işlemi uygulanır. Uygulanan dönüşümde, reel sayılardan tam sayılara çevirme işlemi sırasında yuvarlama hataları meydana gelmektedir.

Önerilen yöntemde, meydana gelen yuvarlama hatası problemlerini çözebilmek için zeki optimizasyon algoritmalarından faydalanılmıştır. Optimizasyon algoritması yardımı ile elde edilebilecek en yüksek farkedilmezlik değeri gözetilerek, reel sayılar ile tanımlanan dönüşüm katsayılarından, tam sayı ile ifade edilen resim uzayına dönüşüm gerçekleştirilmiştir.

Son olarak, elde edilen damgalanmış görüntüden, damga çıkarma algoritması kullanılarak orijinal görüntünün kayıpsız bir şekilde çıkarılması ve damgalanmış görüntü üzerine yapılan kurcalamaların tespiti sağlanmıştır.

Geliştirilen damgalama yöntemi, damganın gömülmesi, damganın çıkarılması ve yapılan kurcalamaların tespit edilmesi olmak üzere üç işlem adımından oluşmaktadır.

2.2.1. Damganın Gömülmesi

Damga gömülme işleminde, öncelikle damga $1 \times N$ boyutunda bir vektöre dönüştürülür, damgalanacak gri seviyeli görüntü ise 8×8 boyutunda bloklara ayrılarak blok haritası adı verilen bir matris oluşturulur. Ardından damga bilgisi bu matris içerisinde saklanır. Daha sonra damgayı çıkarırken kullanılacak olan bu blok haritası, güvenliği sağlamak adına anahtar tabanlı modern bir yöntem olan Knuth karıştırma algoritması ile karıştırılmaktadır.

Ronald Fisher ve Frank Yates [44], orijinal formunu 1938 yılında sundukları, sonlu dizilerin rastgele olarak karıştırılmasını sağlayan, Fisher-Yates karıştırma algoritmasını sunmuşlardır. Daha sonra Donald Knuth, bu algoritmayı modernize ederek Knuth karıştırma algoritmasını geliştirmiştir [45]. Algoritma 2.1’de Knuth karıştırma algoritmasının sözde kodu verilmiştir [46].

Algoritma 2.1: Knuth karıştırma algoritması sözde kodu

Giriş: n boyutlu dizi (arr)

Çıkış: Karıştırılmış dizi (arr)

for $i=2$ to n do

a) $j \leftarrow 1 \leq j \leq i$ aralığında rastgele tam sayı seç

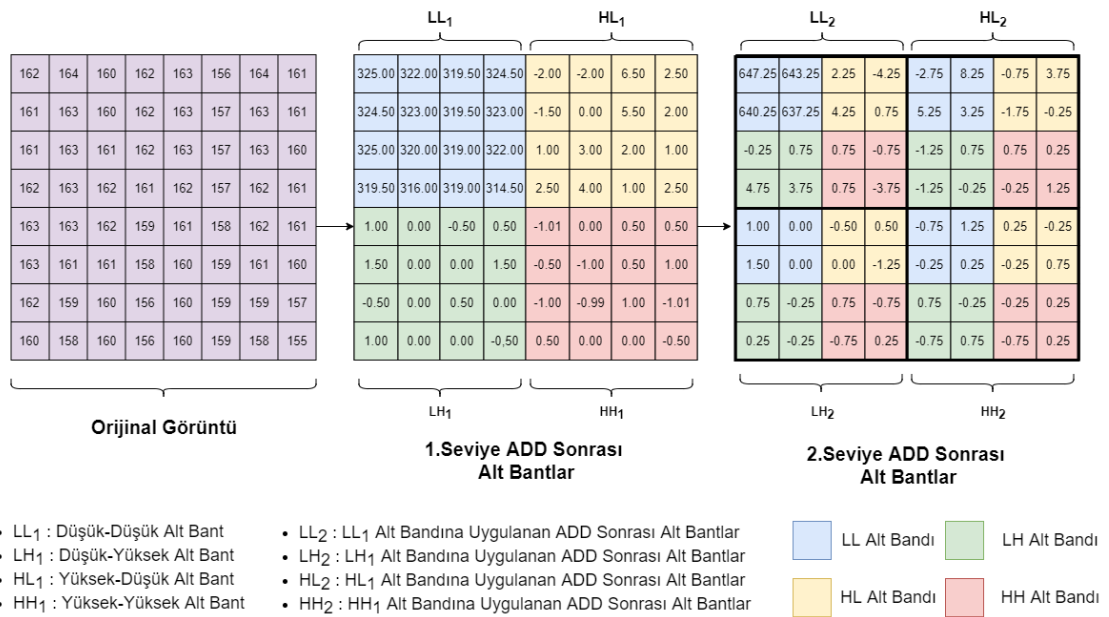
b) $arr[i]$ ve $arr[j]$ değiştir

end for

Görüntü damgalanmadan önce, damga bilgisinin gömüleceği bloklar, Knuth karıştırma algoritması kullanılarak gizli bir anahtar yardımı ile karıştırılmaktadır.

Damga bilgisini görüntü içerisine gömmek için öncelikle, karıştırılmış görüntü bloklarının her birine, frekans uzayı damgalama yöntemlerinde kullanılan ADD ile iki seviyeli dönüşüm uygulanmaktadır. ADD'ye ait detaylı bilgi "1.4.2.2 Frekans Uzayında Damgalama" başlığı altında verilmiştir.

ADD sonrasında, LL, LH, HL ve HH olmak üzere dört alt bant elde edilmektedir. Damga bilgisi LL bandına gömüldüğünde daha dayanıklı bir damgalama elde edilirken, HH bandına gömüldüğünde daha yüksek bir farkedilmezlik elde edilmektedir [17]. Yapılan çalışmada, yüksek farkedilmezlik elde edilmesi hedeflendiği için HH alt bandı ve orta bantlar kullanılmıştır. Görüntü üzerindeki 8×8'lik bloklara iki seviyeli ADD uygulandığında, Şekil 2.2'de gösterildiği gibi 2×2 boyutunda dönüşüm katsayıları elde edilmektedir.



Şekil 2.2. İki seviyeli ADD dönüşüm katsayıları

Görüntüde minimum bozulma elde edebilmek için, damga bilgisi, Denklem 2.1 kullanılarak elde edilen mutlak mesafe değerine gömülmektedir.

$$M = | (a + b + c)/3 - s | \quad (2.1)$$

Denklemden yer alan M , mutlak mesafe değeri, s 2×2 boyutundaki katsayı matrisi içerisinde seçilen katsayı, a , b ve c ise seçilen katsayıya komşu olan katsayıları ifade etmektedir. Denklem 2.1’de yer alan katsayıları değerlerini gösteren 2×2 boyutundaki örnek bir katsayı matrisi Şekil 2.3’te verilmiştir.

s	a
b	c

Şekil 2.3. 2×2 boyutundaki katsayı matrisi

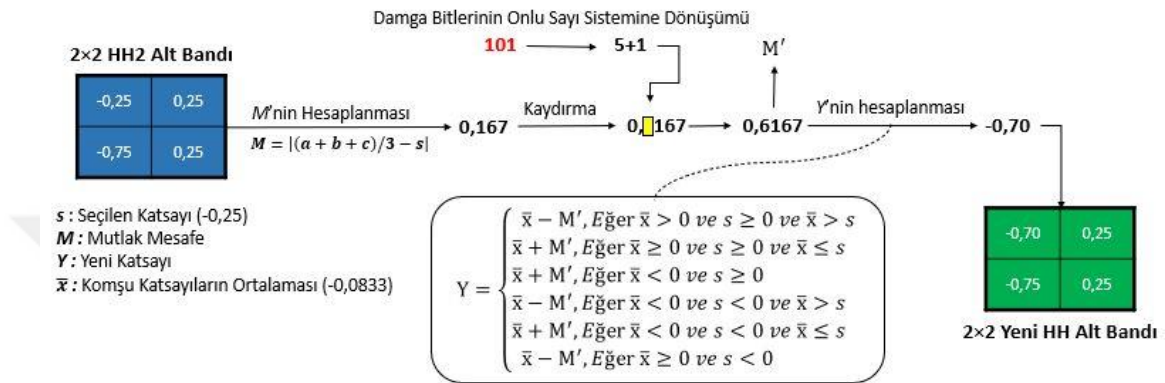
Her bloğa iki seviyeli ADD uygulandıktan sonra, bir blok içerisinde HH, LH ve HL alt bantlarının her birine üç bit olmak üzere toplamda dokuz bit gömülmektedir. Damga bilgisini gömmek için hesaplanan mutlak mesafenin virgülden sonraki ilk hanesi kullanılmaktadır. Önerilen yöntemde, her bir alt banda kapasiteyi arttırmak amacı ile bir bit yerine üç bit veri gömülmesini sağlayacak bir yöntem önerilmiştir. Bunu sağlamak için üç bitlik veri öncelikle ondalık olarak ifade edilir. Daha sonra virgülden sonraki rakamlar bir birim sağa kaydırılarak elde edilen ondalık sayı virgülden sonraki ilk haneye yerleştirilir. Bu işlem sırasında, ondalık sayının sıfır etkisiz eleman olma özelliğinden kaynaklanan bir problem meydana gelmemesi için sayının değeri bir artırılarak oluşabilecek sayılar bir ile sekiz aralığına taşınır. İki seviyeli ADD alt bantlarından HH bandına üç bit damga bilgisi, kurcalama tespitinde kullanılacak dört bitlik doğrulama bilgisi LH ve HL orta bantlarına gömülmektedir.

Verilerin mutlak mesafeye gömülmesinden sonra yeni katsayının elde edilmesi için Denklem 2.2 kullanılmaktadır.

$$Y = \begin{cases} \bar{x} > 0 \text{ ve } s \geq 0 \text{ ve } \bar{x} > s \text{ için,} & \bar{x} - M' \\ \bar{x} \geq 0 \text{ ve } s \geq 0 \text{ ve } \bar{x} \leq s \text{ için,} & \bar{x} + M' \\ \bar{x} < 0 \text{ ve } s \geq 0 \text{ için,} & \bar{x} + M' \\ \bar{x} < 0 \text{ ve } s < 0 \text{ ve } \bar{x} > s \text{ için,} & \bar{x} - M' \\ \bar{x} < 0 \text{ ve } s < 0 \text{ ve } \bar{x} \leq s \text{ için,} & \bar{x} + M' \\ \bar{x} \geq 0 \text{ ve } s < 0 \text{ için,} & \bar{x} - M' \end{cases} \quad (2.2)$$

Denklemden yer alan, $\bar{x}$ komşu katsayıların (a , b ve c) ortalaması, M' verinin gömüldüğü yeni mutlak mesafe değeri ve Y ise elde edilen yeni katsayı değeridir.

Elde edilen yeni katsayı (Y), 2×2 'lik bloktaki seçilen katsayı (s) ile yer değiştirilir ve ters ADD dönüşümleri ile veri gömülmüş görüntü bloğu elde edilir. Tüm bloklara damga bilgisi gömüldükten sonra bloklar birleştirilerek damgalanmış görüntü elde edilir. Şekil 2.4'te örnek bir alt banda üç bitlik damga bilgisinin gömülme süreci gösterilmiştir.



Şekil 2.4. Örnek bir alt banda damga bilgisinin gömülme süreci

Damgalama sonrasında piksel değişimini gösterimi için önerilen damgalama yöntemi kullanılarak, bir giriş görüntüsü üzerine ADD uygulanarak frekans uzayına taşınmış, daha sonra elde edilen dönüşüm katsayılarına üç bit damga ve dört doğrulama biti gömülmüştür. Damgalama sonrasında, görüntü frekans uzayından, resim uzayına taşınmıştır. Giriş görüntüsünde yer alan piksellerin, önerilen yöntem ile damgalandıktan sonraki piksel değerlerindeki değişim Şekil 2.5'te gösterilmiştir.

162	164	160	162	163	156	164	161
161	163	160	162	163	157	163	161
161	163	161	162	163	157	163	160
162	163	162	161	162	157	162	161
163	163	162	159	161	158	162	161
163	161	161	158	160	159	161	160
162	159	160	156	160	159	159	157
160	158	160	156	160	159	158	155

162,0375	164,0375	159,9625	161,9625	163,0000	156,0000	164,0000	161,0000
160,9625	162,9625	160,0375	162,0375	163,0000	157,0000	163,0000	161,0000
160,9625	162,9625	161,0375	162,0375	163,0000	157,0000	163,0000	160,0000
162,0375	163,0375	161,9625	160,9625	162,0000	157,0000	162,0000	161,0000
163,0000	163,0000	162,0000	159,0000	161,1125	157,8875	161,8875	161,1125
163,0000	161,0000	161,0000	158,0000	160,0375	158,9625	160,9625	160,0375
162,0000	159,0000	160,0000	156,0000	159,8875	159,1125	159,1125	156,8875
160,0000	158,0000	160,0000	156,0000	159,9625	159,0375	158,0375	154,9625

Şekil 2.5. Damgalama sonrası görüntü piksel değişimi

Tıbbi görüntüler, sayısal ortamda Analyze, Nifti, Minc ve Dicom olmak üzere beş yaygın formatta bulunmaktadır. Tablo 2.1'de görülebileceği üzere, bu formatlar yaygın

olarak tamsayı veri tiplerini desteklemekte, bazı formatlar reel sayılardan oluşan veri tiplerini desteklememektedir [47].

Şekil 2.5'te de görüleceği üzere damgalanmış görüntü, reel sayılardan oluştuğu için tüm tıbbi görüntü formatlarında kullanılamayacaktır. Bu problemi çözmek için görüntü pikselleri tam sayıya, gömülmüş olan verinin tekrar elde edilebileceği şekilde yuvarlanması gereklidir. Literatürde yer alan bazı yöntemlerde [25,34,35] elde edilen yüksek farkedilmezlik değerlerine bu problem göz ardı edilerek ulaşılmıştır. Fakat geliştirilen frekans tabanlı damgalama yönteminin tüm pratik uygulamalarda kullanılabilmesi için bu problemin üstesinden gelinmelidir.

Tablo 2.1. Özet tıbbi görüntü formatları [47]

Format	Başlık	Uzantı	Veri Tipleri
Analyze	Sabit uzunluk: 348 bayt ikili	.img ve .hdr	• İşaretsiz tamsayı (8-bit) • İşaretsiz tamsayı (16-bit,32-bit) • Float (32-bit,64-bit) • Karmaşık (64-bit)
Nifti	Sabit uzunluk: 352 bayt ikili	.nii	• İşaretsiz ve işaretsiz tam sayı (8- den 64-bit'e kadar) • Float (32- den 128-bit'e kadar) • Karmaşık (64- den 256-bit'e kadar)
Minc	Genişletilebilir ikili format	.mnc	• İşaretsiz ve işaretsiz tam sayı (8- den 32-bit'e kadar) • Float (32- den 64-bit'e kadar) • Karmaşık (32- den 64-bit'e kadar)
Dicom	Değişken uzunluklu ikili format	.dcm	• İşaretsiz ve işaretsiz tam sayı (8-bit, 16-bit; 32-bit sadece radyoterapi dozlarında), • Float desteklenmiyor

Aslantaş vd. [48], yapmış oldukları çalışmada AKD ve EAB yöntemi kullanılan kırılğan damgalama yöntemlerinde, damgalanmış görüntü elde edilirken oluşan yuvarlama

hatalarını ortaya koymuş ve bu yuvarlama hatalarının zeki optimizasyon algoritmaları ile çözülebileceğini göstermiştir.

Yapılan çalışmada, görüntüye AKD uygulandıktan sonra elde edilen katsayılarla EAB yöntemi kullanarak damga bilgisi gömülmektedir. Daha sonra zeki optimizasyon algoritması yardımı ile gömülen damganın elde edilebileceği ikili sayılardan oluşan bir dönüşüm matrisi, orijinal görüntüye eklenerek damgalanmış görüntü elde edilmiştir. 256×256 boyutundaki Lena görüntüsü üzerine, 64×64 boyutunda siyah-beyaz damga gömülerek yapılan deneysel çalışma sonunda, 55.5 dB üzerinde PSNR ve 1 NK elde edilmiştir.

Tez çalışması kapsamında önerilen damgalama yönteminde, [48]'de yer alan çalışmada kullanılan yöntemden faydalanılarak dönüşüm matrisi oluşturulmuş ve yuvarlama hatalarından kaynaklanan problemin çözümünde kullanılmıştır.

Geliştirilen yöntemde, optimizasyon algoritması, görüntü içerisine gömülen damgayı çıkarabilen ve en yüksek farkedilmezlik değerini sunan tam sayı piksel değerlerinin elde edilmesini hedeflemektedir. Bunun için, OKH görüntü kalite metriğinden faydalanan, Denklem 2.3'te yer alan amaç fonksiyonunu kullanılarak, orijinal görüntü bloklarına eklenecek olan bir dönüşüm matrisi elde edilir. Tüm bloklardan elde edilen dönüşüm matrisleri birleştirilerek 512×512 boyutunda 0 ve 1 değerlerinden oluşan bir matris olarak saklanır. Elde edilen matris, orijinal görüntünün elde edilmesinde kullanılabilmesi için damganın çıkarılması esnasında alıcıda bulunması gereklidir.

$$F(\text{uygunluk}) = OKH(\text{Damgalanmış blok}) \quad (2.3)$$

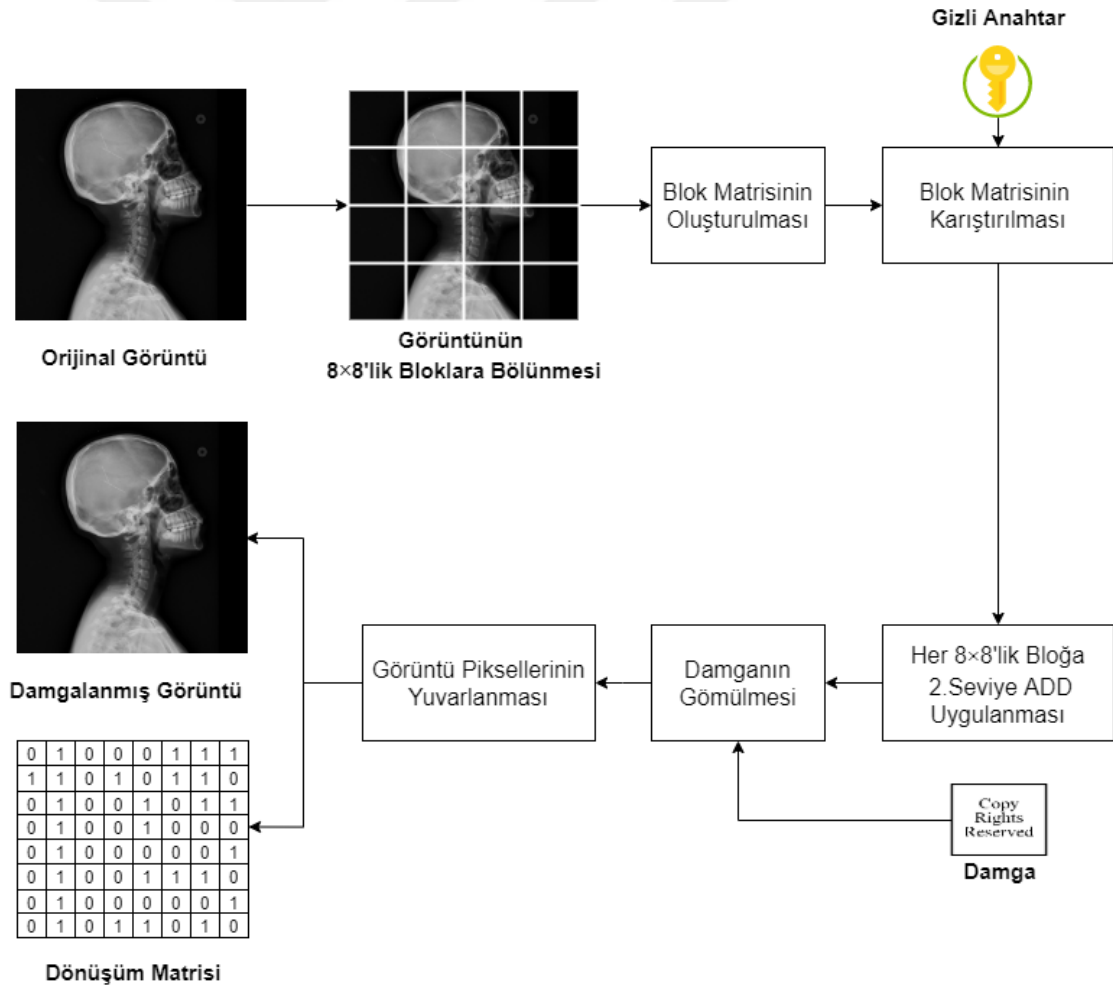
Her bir damgalanmış 8×8 boyutundaki görüntü bloğunun kendine ait bir çözümü mevcuttur. Optimizasyon algoritması ile elde edilen en iyi dönüşüm matrisleri, orijinal görüntü bloklarına eklenerek tam sayıya yuvarlanmış damgalanmış görüntünün son hali elde edilir. Şekil 2.5'te yer alan reel sayılardan oluşan damgalanmış görüntüye ait piksel değerlerinin, optimizasyon algoritması ile tam sayıya yuvarlanması sonucu elde edilen piksel değerlerinin değişimi Şekil 2.6'da gösterilmiştir.

162,0375	164,0375	159,9625	161,9625	163,0000	156,0000	164,0000	161,0000
160,9625	162,9625	160,0375	162,0375	163,0000	157,0000	163,0000	161,0000
160,9625	162,9625	161,0375	162,0375	163,0000	157,0000	163,0000	160,0000
162,0375	163,0375	161,9625	160,9625	162,0000	157,0000	162,0000	161,0000
163,0000	163,0000	162,0000	159,0000	161,1125	157,8875	161,8875	161,1125
163,0000	161,0000	161,0000	158,0000	160,0375	158,9625	160,9625	160,0375
162,0000	159,0000	160,0000	156,0000	159,8875	159,1125	159,1125	156,8875
160,0000	158,0000	160,0000	156,0000	159,9625	159,0375	158,0375	154,9625

162	164	160	162	163	156	164	161
161	163	160	162	163	157	163	161
161	163	161	162	163	157	163	160
162	163	162	161	162	157	162	161
164	163	162	159	161	158	162	161
164	161	161	158	160	159	161	160
162	160	161	156	161	159	160	157
160	158	160	156	160	159	158	155

Şekil 2.6. Tam sayı yuvarlama sonrası görüntü piksel değişimi

Damga bilgisi ve doğrulama bitlerinin görüntü içerisine gömülmesinde kullanılan algoritmanın temel işlem adımları Algoritma 2.2’de ve damganın gömülme sürecine ait blok diyagram Şekil 2.7’de gösterilmiştir.



Şekil 2.7. Damga gömülme sürecine ait blok diyagram

Algoritma 2.2: Damga gömme algoritması

Giriş: Giriş görüntüsü, siyah-beyaz damga

Çıktı: Damgalanmış görüntü, dönüşüm matrisi

- 1: Damganın, $1 \times N$ boyutuna dönüştürülmesi
 - 2: Giriş görüntüsünün, 8×8 'lik bloklara ayrılması
 - 3: Blok haritasının oluşturulması
 - 4: Gizli anahtar kullanarak blok haritasının karıştırılması
 - 5: Her bir blok için iki seviyeli ADD uygulanarak 2×2 boyutunda katsayı matrisinin edilmesi
 - 6: 2×2 boyutundaki katsayı matrisi içinden katsayı seçiminin yapılması
 - 7: Seçilen katsayıya komşu olan katsayıların ortalamasının alınması
 - 8: Denklem 2.1 kullanılarak mutlak mesafenin hesaplanması
 - 9: Blok içerisine gömülecek olan üç bitlik verinin, ondalık sayıya dönüştürülmesi
 - 10: Ondalık sayının sıfır olma durumuna karşı bir birim artırılması
 - 11: Sayının, mutlak mesafenin virgülden sonraki rakamlarının sağa bir birim ötelenerek ilk hanesine yerleştirilmesi
 - 12: Elde edilen yeni mutlak mesafe değeri ile Denklem 2.2 kullanılarak yeni katsayı değerinin elde edilmesi
 - 13: Yeni katsayı değerinin, 2×2 'lik blokta seçilen katsayı ile yer değiştirilmesi
 - 14: Ters ADD dönüşümleri ile görüntü bloğunun frekans uzayından, resim uzayına taşınması
 - 15: Tüm bloklar damgalandıktan sonra blokların birleştirilerek damgalanmış görüntünün elde edilmesi
 - 16: Damgalanmış görüntü piksellerinin, optimizasyon algoritması kullanılarak tam sayıya yuvarlanması
-

2.2.2. Damganın Çıkarılması

Damganın çıkarılması aşamasında, damganın gömülme işlemlerine benzer olarak damgalanmış görüntü, öncelikle 8×8 'lik bloklara ayrılmaktadır. Daha sonra, damganın gömülmesinde kullanılan gizli anahtar yardımı ile blok haritası oluşturulur ve bu blok haritasına göre her bloğa iki seviyeli ADD uygulanarak 2×2 boyutunda katsayı matrisleri elde edilir. 2×2 katsayı matrisi içerisinden katsayısı seçilir ve Denklem 2.1 ile mutlak mesafe hesaplanır. Mutlak mesafenin virgülden sonraki ilk hanesine gömülen

veriyi içeren sayı alınır. Alınan sayının değeri bir azaltılarak ikili sayı sistemine dönüştürülür ve gömülen veriye ulaşılır. $1 \times N$ boyutundaki damga bilgisi orijinal boyutuna dönüştürülerek gömülen damga elde edilir. Orijinal görüntüyü elde etmek için ise damga gömme sırasında elde edilen dönüşüm matrisi damgalanmış görüntüden çıkarılarak orijinal görüntüye kayıpsız bir şekilde ulaşılır.

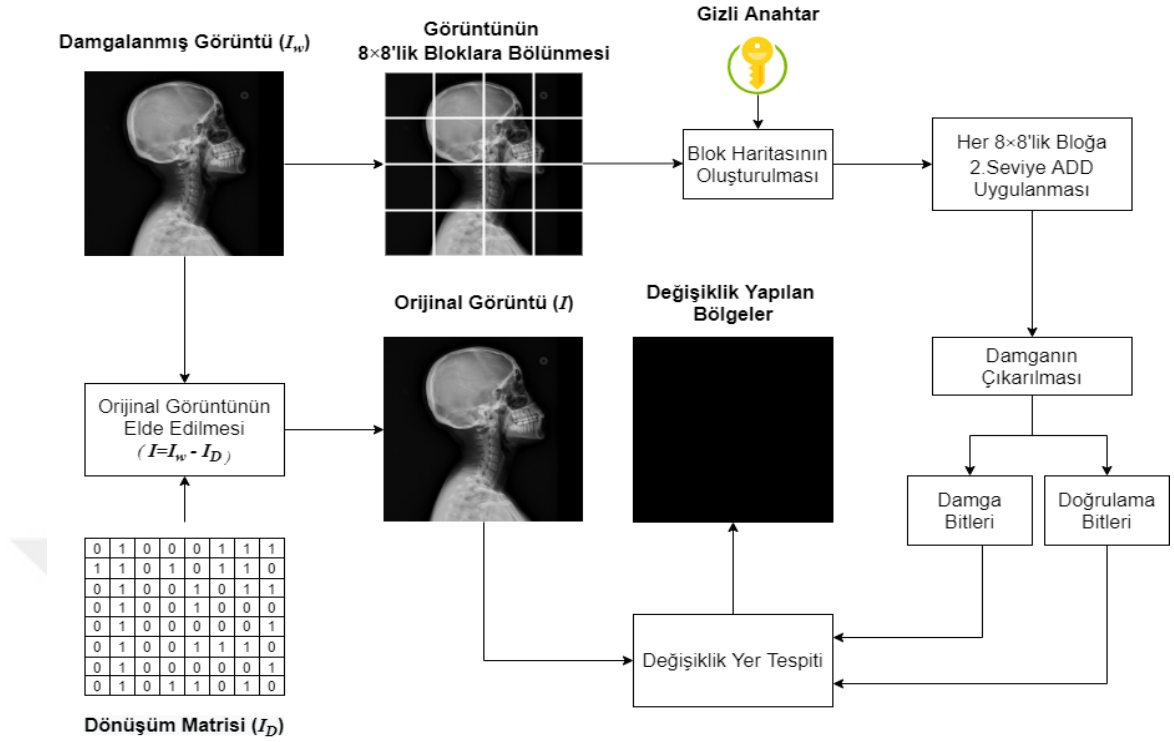
Dönüşüm matrisi, damga ile ilgili herhangi bir bilgi içermemektedir. Bu yüzden ele geçirilmesi herhangi bir güvenlik zafiyetine sebep olmayacaktır. Damganın çıkarılmasında kullanılan algoritmanın temel işlem adımları Algoritma 2.3'te ve damga çıkarma sürecine ait blok diyagram Şekil 2.8'de gösterilmiştir.

Algoritma 2.3: Damga çıkarma algoritması

Giriş: Damgalanmış görüntü, dönüşüm matrisi, gizli anahtar

Çıktı: Orijinal Görüntü, çıkarılmış damga

- 1: Damgalanmış görüntünün 8×8 'lik bloklara ayrılması
 - 2: Gizli anahtar ile blok haritasının oluşturulması
 - 3: Her bir blok için iki seviyeli ADD uygulanarak 2×2 boyutunda katsayı matrislerinin edilmesi
 - 4: 2×2 boyutundaki katsayı matrisi içerisinde katsayının seçilmesi
 - 5: Seçilen katsayıya komşu olan katsayıların ortalamasının alınması
 - 6: Denklem 2.1 kullanılarak mutlak mesafenin hesaplanması
 - 8: Mutlak mesafenin virgülden sonraki ilk hanesindeki sayı alınarak gömülen verinin elde edilmesi
 - 10: Çıkarılan sayının değerinin bir birim azaltılması ve ikili sayı sistemine dönüştürülmesi
 - 11: Elde edilen $1 \times N$ boyutundaki verinin orijinal damga boyutuna dönüştürülerek çıkarılmış damganın elde edilmesi
 - 12: Damgalanmış görüntüden dönüşüm matrisinin çıkarılarak orijinal görüntünün elde edilmesi
-



Şekil 2.8. Damga çıkarma sürecine ait blok diyagram

2.2.3. Kurcalama Yer Tespiti

Damgalama yöntemlerinde, saklanacak veri miktarının artması ile hafıza ve bununla ilişkili kaynaklara olan ihtiyaç artmaktadır. Özellikle ağ uygulamalarında, transfer edilen veri miktarı, sınırlı olan bant genişliğinin verimli kullanımı için çok önemlidir [7, 25].

Bu tez kapsamında, kurcalama tespitinde kullanılacak doğrulama bitlerinin üretimi için iki farklı yöntem önerilmiştir. Bu yöntemler, kurcalama yer tespitini gerçekleştirebilmek için alıcı tarafında orijinal damgaya ihtiyaç duymamaktadır. Yönetimin, orijinal görüntü ve damga bilgisi saklama gereksiniminin olması depolama alanı, transfer edilecek veri miktarı ve bant genişliğinin verimli kullanımı açısından avantaj sağlamaktadır.

Önerilen iki yöntemde, kurcalama yer tespiti için her 8x8'lik bloğa üç bit damga ile birlikte dört doğrulama biti gömülmektedir.

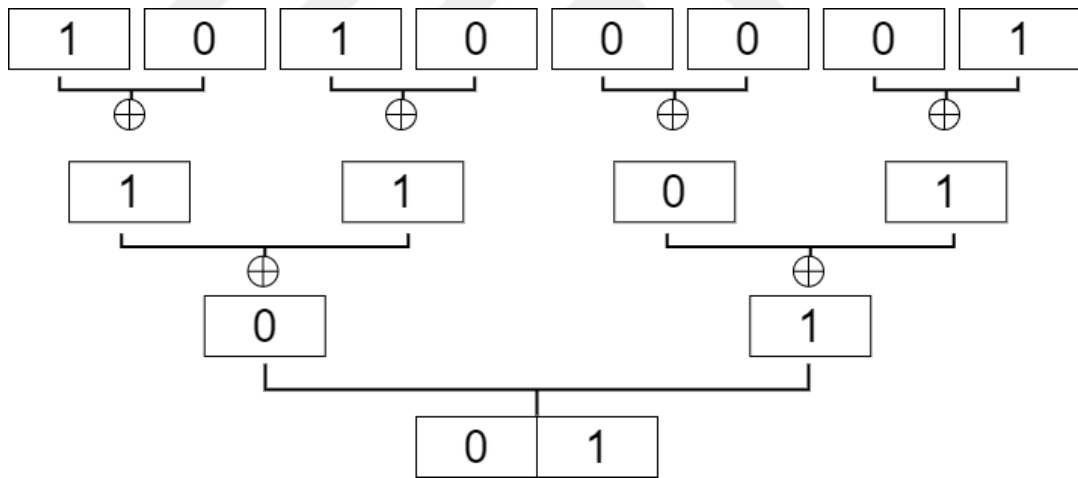
Birinci önerilen yöntemde, Şekil 2.9'da gösterildiği gibi doğrulama bitleri, damga doğrulama, blok sağlama ve sıfır doğrulama bitlerinden oluşmaktadır.

Damga Doğrulama	Blok Sağlama	Blok Sağlama	Sıfır Doğrulama
-----------------	--------------	--------------	-----------------

Şekil 2.9. Birinci yönteme ait doğrulama bitleri

Damga doğrulama, bir bitten oluşmaktadır ve gömülen üç bitlik damgayı doğrulamak için tutulmaktadır. Damga doğrulama biti, üç bitlik damga verisinin onluk sisteme dönüştürüldükten sonra çift veya tek olma durumuna göre belirlenmektedir. Elde edilen sayı çift ise damga doğrulama biti “0” değilse “1” olarak atanmaktadır.

Blok sağlama iki bitten oluşmaktadır ve orijinal görüntü bloklarında değişme olmadığının sağlanmasını yapmak için tutulmaktadır. Bu iki biti hesaplamak için öncelikle 8×8’lik orijinal görüntü bloğundaki tüm piksellerin ortalaması alınır. Daha sonra elde edilen sayı ikili sayı sistemine dönüştürülür. Elde edilen 8 bitlik sayıya Şekil 2.10’da gösterildiği gibi iki bite düşene kadar xor lojik operasyonu uygulanır.



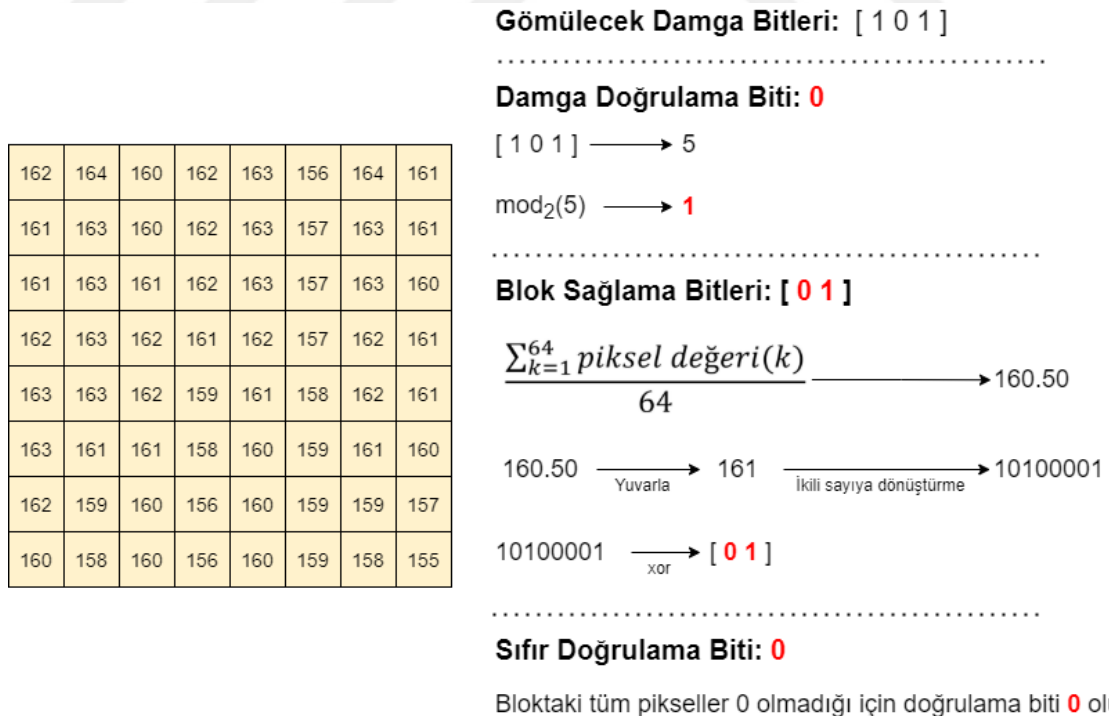
Şekil 2.10. Blok sağlama bitlerinin elde edilmesi

Damga çıkarma aşamasında, damgalanmış görüntüden dönüşüm matrisi çıkarılarak orijinal görüntü bloğu elde edilir. Çıkarılan orijinal görüntü bloğundan elde edilen blok sağlama bitleri ile damgalı görüntü bloğundan çıkarılan blok sağlama bitleri kıyaslanarak blokta kurcalama olup olmadığı kontrol edilir.

Sıfır doğrulama, bir bitten oluşmaktadır ve kırpma saldırılarında doğru yer kurcalama tespiti yapabilmek için kullanılmaktadır. Görüntü üzerine kırpma saldırısı uyguladığında çıkarılan damga doğrulama biti “0” ve blok sağlama bitleri “00” olacaktır. Bu durumda geliştirilen sistem, gömülen damganın “000” yani çift olduğunu

düşünerek gömülen damganın değiştirilmediğine karar verecektir. Aynı şekilde, dönüşüm matrisi çıkarıldığında elde edilen orijinal görüntü blok piksellerinin tümü sıfır olacağı için elde edilen blok sağlama bitleri “00” olacaktır ve bu doğrulama aşamasından da geçecektir. Bu yüzden kırpma saldırılarında iki doğrulamada işe yaramayacak ve başarısız olacaktır. Meydana gelen bu belirsizlik problemi, damganın gömülmesi sırasında gömülen piksellerin tümü sıfırsa, sıfır doğrulama biti “1” değilse “0” atanarak çözülmektedir. Böylece damga çıkarıldığında sıfır doğrulama biti “1” beklenirken çıkarılan değer “0” olacağı için kurcalamanın yapıldığı doğru bir şekilde tespit edilebilecektir.

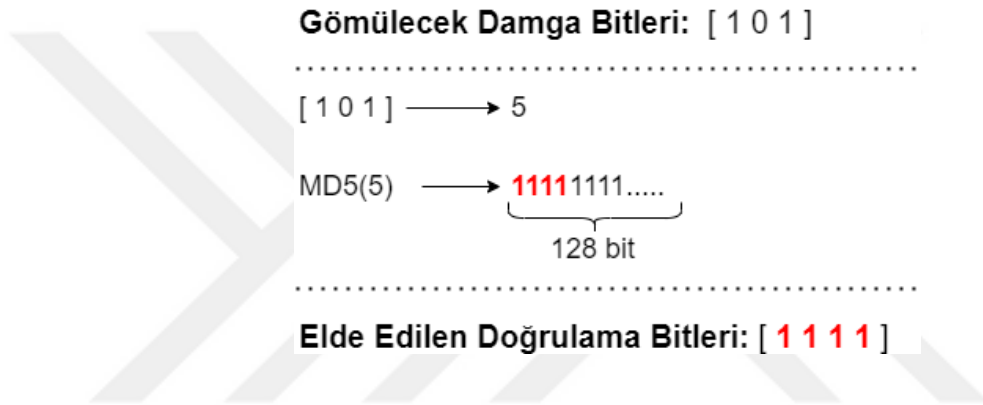
Oluşturulan doğrulama bitleri, gömülen damga, gömülen blok pikselleri ve kırpma gibi özel durumları içeren geometrik dönüşüm saldırıları dikkate alınarak oluşturulmuştur. Birinci yöntem kullanılarak, örnek bir 8×8 boyutundaki bloktan, doğrulama bitlerinin elde edilmesi Şekil 2.11’de gösterilmiştir. İkinci yöntemde ise, doğrulama bitleri yaygın olarak kullanılan hash fonksiyonlarından biri olan Message Digest 5 (MD5) hash algoritması kullanılarak oluşturulmuştur.



Şekil 2.11. Birinci yöntem kullanılarak doğrulama bitlerinin elde edilmesi

MD5 hash algoritması, MD4'ün bir üst sürümü olarak Ron Rivest tarafından geliştirilmiştir. MD5 algoritması, değişken uzunluktaki mesajın özetini oluşturarak 128 bit uzunluğunda sabit bir çıktı üretir [49].

Doğrulama bitleri üretilirken, üç bitlik damga bilgisi ondalık sayı sistemine dönüştürülür. Daha sonra elde edilen sayı MD5 hash fonksiyonu kullanılarak 128 bit uzunluğunda bir çıktı elde edilir. Elde edilen 128 bitin ilk dört biti doğrulama biti olarak kullanılır. Şekil 2.12'de ikinci yöntem kullanılarak örnek doğrulama bitlerinin elde edilmesi gösterilmiştir.



Şekil 2.12. İkinci yöntem kullanılarak doğrulama bitlerinin elde edilmesi

3. BÖLÜM

BULGULAR

Bu bölümde, tez kapsamında yapılan deneysel çalışmalar ve elde edilen bulgular ayrıntıları ile anlatılmaktadır. Yapılan deneysel çalışmalar, kullanılacak olan optimizasyon algoritmasının seçilmesi, görüntülerin farkedilmezlik analizleri ve damgalanmış görüntü üzerine saldırılar uygulanması ile elde edilen kurcalama yer tespiti performanslarının değerlendirilmesi bölümlerinden oluşmaktadır.

3.1. Kullanılan Araçlar ve Veri Seti

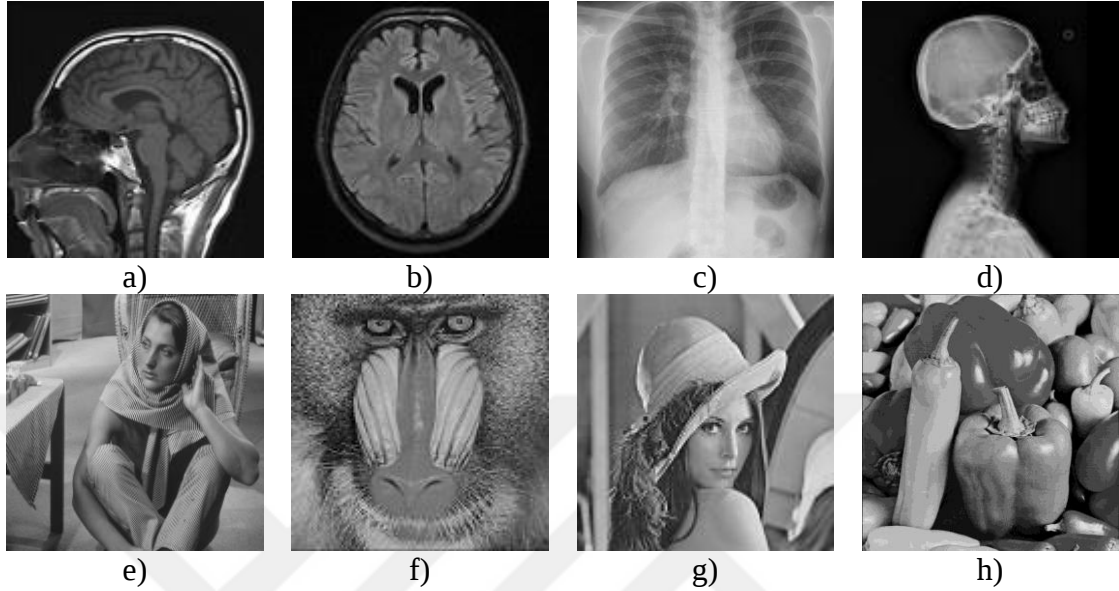
Yöntemin geliştirilmesinde, MATLAB 2020b platformu kullanılmıştır. Yöntemin geliştirildiği ve testlerin yapıldığı Macbook Pro dizüstü bilgisayar, Intel 2.3 GHz i9 işlemci ve 16 GB RAM özelliklerine sahiptir.

Önerilen damgalama yöntemi ile yapılan deneysel çalışmalarda, 512×512 boyutunda MR ve X-Ray gri seviye tıbbi görüntüleri kullanılmıştır. Ayrıca, sayısal damgalama uygulamalarında sıklıkla kullanılan, “Barbara”, “Baboon”, “Lena” ve “Peppers” görüntüleri kullanılarak saldırılara karşı elde edilen performansları paylaşılmıştır (Şekil 3.1).

3.2. Optimizasyon Algoritması Seçimi

Geliştirilen sayısal damgalama yönteminde, frekans uzayı damgalama yöntemlerinden yaygın olarak kullanılan ADD tercih edilmiştir. ADD kullanılarak gerçekleştirilen damgalama sonrasında, reel sayı değerlerine sahip piksellerden oluşan damgalanmış görüntü elde edilmektedir. Fakat Tablo 2.1’de gösterildiği gibi, tüm tıbbi görüntü formatları reel sayı tipini desteklememektedir. Bu yüzden, damgalanmış görüntünün tam sayıya dönüştürülmesi gerekmektedir. Uygulanan dönüşümde, reel sayılardan tam sayılara çevirme işlemi sırasında yuvarlama hataları meydana gelmektedir.

Önerilen yöntemde, meydana gelen yuvarlama hatası problemlerini çözebilmek için zeki optimizasyon algoritmalarından faydalanılmıştır.

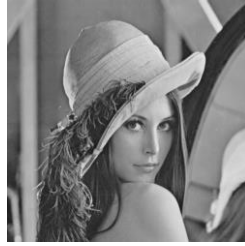


Şekil 3.1. Damgalamada kullanılan görüntüler; a) Beyin MR1, b) Beyin MR2, c) Göğüs X-Ray, d) Boyun X-Ray, e) Barbara, f) Baboon, g) Lena, h) Peppers

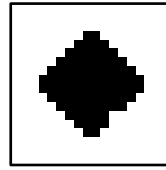
Damgalanmış görüntüyü, tam sayıya dönüştürmede kullanılacak zeki optimizasyon algoritması seçimi için yapılan deneysel çalışmalarda, yaygın olarak kullanılan Parçacık Sürü Optimizasyon (PSO) algoritması, Genetik Algoritma (GA), Yapay Arı Koloni (ABC) algoritması ve Diferansiyel Gelişim Algoritması (DGA) tercih edilmiştir.

Algoritmaların performans karşılaştırması için yapılacak deneylerde, eşit şartların sağlanması için amaç fonksiyonun değerlendirme sayısı 8000 olarak belirlenmiş ve sabit tutulmuştur. Değerlendirme sayısını sabit tutmak için popülasyon büyüklüklerinin (PB) 20 ve 40 olduğu durumlarda sırasıyla çevrim sayıları 400 ve 200 olarak belirlenmiştir. Algoritmaların kararlılığını göstermek için koşma sayısı, 30 olarak tercih edilmiştir. Kullanılan amaç fonksiyonu Denklem 2.3 ile verilmiştir. Ayrıca, geliştirilen çözümler ile istenilen damga bilgisinin çıkarılamadığı durumlarda yüksek penaltı değerleri verilerek en iyi çözüm olma olasılığından uzaklaşması sağlanmıştır. Şekil 3.2, ilgili deneylerde kullanılan 512×512 boyutunda Lena görüntüsünü ve damga olarak kullanılan 18×18 boyutunda siyah-beyaz görüntüyü göstermektedir.

Lena (512×512 px)



Damga (18×18 px)



Şekil 3.2. Optimizasyon algoritma seçimi için kullanılan giriş görüntüsü ve damga

3.2.1. Parçacık Sürü Optimizasyon Algoritması:

Tamsayıya yuvarlama işleminde çözüm kümesi, 8 gerçel değerli parametre ($P = p_1, p_2, \dots, p_8$) ile temsil ederek PSO algoritması uygulanmıştır. Bu gerçel değerlerin, tam sayıya yuvarlanmış halleri ikili sayıya dönüştürülerek, 8×8 boyutunda dönüşüm matrisi elde edilmiştir. Elde edilen dönüşüm matrisi, orijinal görüntü blok piksel değerlerine eklenerek, damgalanmış piksel değerleri olarak amaç fonksiyonunun hesaplanmasında kullanılmıştır. Şekil 3.3'te çözüm kümesi ve dönüşüm matrisi gösterilmiştir.

p_1	0.03
p_2	5.07
p_3	38.27
p_4	65.92
p_5	94.06
p_6	192.35
p_7	234.42
p_8	254.72

a)

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

b)

Şekil 3.3. PSO algoritması için; a) örnek çözüm kümesi, b) dönüşüm matrisi

PSO algoritması ile yapılan deneyde eylemsizlik ağırlığı (ω) ve ivmelenme sabitleri ($C1, C2$) için en uygun değerlerin tespit edilmesi adına yapılan çalışmalara yer verilmiştir. İvmelenme sabitlerinin değerleri eşit tutulmuştur. Ayrıca, elde edilen en uygun değerler için damgalanmış görüntünün farkedilmezlik değerleri paylaşılmıştır.

Elde edilen sonuçlar, Tablo 3.1 ve Tablo 3.2’de gösterilmiştir. Eylemsizlik ağırlığının ve ivmelenme sabitlerinin büyük olduğu değerlerde algoritma daha iyi farkedilmezlik değerleri sunmuştur. Popülasyon büyüklüğü 20, eylemsizlik ağırlığı 1.8 ve ivmelenme sabitleri 0.9 için algoritma en uygun değerleri PSNR 69.7289 ve MSE 0.0069 olarak elde etmiştir. Tablolarda yer alan standart sapma değerleri, algoritmanın kararlı olduğunu göstermektedir. Popülasyon büyüklüğü arttıkça, farkedilmezlik değerinde azalma olduğu gözlemlenmiştir.

3.1.2. Genetik Algoritma:

GA ile yapılan deneyde, çözüm kümesi (kromozom), ikili sayılardan oluşan 64 bireyden (genden) oluşmaktadır. Bu 64 birey 8×8 boyutunda bir dönüşüm matrisi ile temsil edilmiştir ve orijinal görüntü bloğuna eklenerek amaç fonksiyonunun hesaplanmasında kullanılmıştır. Şekil 3.4’te örnek bir bireyin (G) dönüşüm matrisi karşılığı gösterilmiştir.

a)
$$G = [\begin{matrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}]$$

b)

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

Şekil 3.4. GA için; a) örnek bir birey, b) dönüşüm matrisi

Tablo 3.1. PSO algoritması popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler

PB=20			ω					
			1.6		1.8		2.0	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
$C1=C2$	0.5	Ort	69,5363	0,0072	69,6500	0,0071	69,6722	0,0070
		Std	0,0628	0,0001	0,0655	0,0001	0,0649	0,0001
	0.6	Ort	69,5512	0,0072	69,6927	0,0070	69,7034	0,0070
		Std	0,0570	0,0001	0,0620	0,0001	0,0671	0,0001
	0.7	Ort	69,5688	0,0071	69,6721	0,0070	69,6439	0,0074
		Std	0,0620	0,0001	0,0070	0,0001	0,0071	0,0001
	0.8	Ort	69,5640	0,0072	69,6396	0,0071	69,5034	0,0073
		Std	0,0634	0,0001	0,0699	0,0001	0,0642	0,0001
	0.9	Ort	69,5226	0,0073	69,7289	0,0069	69,6481	0,0071
		Std	0,0677	0,0001	0,0575	0,0001	0,0623	0,0001

Tablo 3.2. PSO algoritması popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler

PB=40			ω					
			1.6		1.8		2.0	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
$C1=C2$	0.5	Ort	69,5804	0,0072	69,6977	0,0070	69,6550	0,0070
		Std	0,0679	0,0001	0,0642	0,0001	0,0667	0,0001
	0.6	Ort	69,5447	0,0072	69,7140	0,0070	69,5628	0,0072
		Std	0,0625	0,0001	0,0687	0,0001	0,0680	0,0001
	0.7	Ort	69,5579	0,0072	69,6680	0,0070	69,5556	0,0072
		Std	0,0625	0,0001	0,0673	0,0001	0,0653	0,0001
	0.8	Ort	69,5495	0,0072	69,6977	0,0070	69,5094	0,0073
		Std	0,0612	0,0001	0,0645	0,0001	0,0640	0,0001
	0.9	Ort	69,6506	0,0071	69,5852	0,0072	69,4909	0,0073
		Std	0,0652	0,0001	0,0668	0,0001	0,0637	0,0001

GA'nın en uygun çözümü verecek kontrol parametrelerinin belirlenmesi için çaprazlama oranı (ÇO) ve mutasyon oranı (MO) değerleri değiştirilerek simülasyonlar uygulanmıştır. Elde edilen sonuçlar, Tablo 3.3 ve Tablo 3.4'te gösterilmiştir. Popülasyon büyüklüğü 40, çaprazlama oranı 0,9 ve mutasyon oranı 0,03 için en iyi farkedilmezlik değerleri PSNR 72.7272 ve MSE 0.0035 olarak elde edilmiştir. Tablolarda yer alan standart sapma değerleri algoritmanın kararlı olduğunu göstermektedir. Popülasyon büyüklüğü arttıkça farkedilmezlik değerinde artma olduğu gözlemlenmiştir. Çaprazlama oranı arttıkça farkedilmezlik değeri artmaktadır. Mutasyon oranını düşük değerlerinde daha iyi farkedilmezlik değerleri sağlamış ve değişimlerinin farkedilmezlik üzerine etkisi düşük olmuştur.

Tablo 3.3. GA popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler

PB=20			ÇO					
			0.7		0.8		0.9	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
MO	0.01	Ort	70,3591	0,0060	70,8799	0,0847	71,1491	0,0050
		Std	0,0961	0,0001	0,0053	0,0001	0,0939	0,0001
	0.02	Ort	71,9231	0,0042	72,1549	0,0040	72,2514	0,0039
		Std	0,0899	0,0001	0,0948	0,0001	0,0982	0,0001
	0.03	Ort	72,0273	0,0041	72,1944	0,0039	72,3066	0,0038
		Std	0,0935	0,0001	0,0900	0,0001	0,0918	0,0001
	0.04	Ort	71,4173	0,0047	71,7349	0,0044	72,1058	0,0040
		Std	0,0946	0,0001	0,0911	0,0001	0,0925	0,0001
	0.05	Ort	70,4152	0,0059	70,9377	0,0052	71,3530	0,0048
		Std	0,0933	0,0001	0,0934	0,0001	0,0938	0,0001

Tablo 3.4. GA popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler

PB=40			ÇO					
			0.7		0.8		0.9	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
MO	0.01	Ort	70,3823	0,0966	70,3699	0,0060	71,0672	0,0051
		Std	0,0059	0,0001	0,0939	0,0001	0,0957	0,0001
	0.02	Ort	71,1674	0,0050	71,4377	0,0047	71,7780	0,0043
		Std	0,0945	0,0001	0,0949	0,0001	0,0929	0,0001
	0.03	Ort	72,6247	0,0036	72,6961	0,0035	72,7272	0,0035
		Std	0,0946	0,0001	0,0924	0,0001	0,0914	0,0001
	0.04	Ort	69,5237	0,0073	69,9312	0,0066	70,1330	0,0063
		Std	0,0972	0,0001	0,0956	0,0001	0,0981	0,0001
	0.05	Ort	69,3627	0,0075	69,4572	0,0074	69,7666	0,0069
		Std	0,0922	0,0001	0,0970	0,0001	0,0923	0,0001

3.1.3. Yapay Arı Koloni Algoritması:

ABC algoritması kullanılarak yapılan tam sayı yuvarlama işleminde, PSO algoritmasına benzer olarak 8 gerçel değerli sayının ikili sayılara çevrilmesi ile dönüşüm matrisi oluşturulmuştur. Yapılan deneyde limit (L) için en uygun değerlerinin tespit edilmesi adına yapılan çalışmalara yer verilmiştir.

Elde edilen sonuçlar, Tablo 3.5 ve Tablo 3.6.'da gösterilmiştir. Tüm sayısal sonuçlar değerlendirildiğinde, koloni büyüklüğü 40 ve limit 80 için en iyi farkedilmezlik değerleri PSNR 72.8002 ve MSE 0.0034 olarak elde edilmiştir. Koloni büyüklüğü arttıkça farkedilmezlik değerleri yükselmiştir.

Limit parametresi, işçi ve gözcü arıların her iterasyon sonunda çözüm üretememe sayaçlarını temsil eder. Limit değeri aşılmış yani belirli bir iterasyon sonunda artık iyi çözümler üretilmemeye başlandıysa, bu bölge terk edilir. Yapılan deneyde limit parametresi [10 100] aralığında değiştirilerek gerçekleştirilmiştir. Limitin düşük olduğu değerlerde düşük farkedilmezlik değerleri elde edilmiş ve limit değeri yükseldikçe farkedilmezlik yükselmiştir.

Tablo 3.5. ABC algoritması koloni büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler

PB=20		<i>L</i>	
		PSNR	MSE
50	Ort	72,4660	0,0037
	Std	0,0812	0,0001
60	Ort	72,4825	0,0037
	Std	0,0799	0,0001
70	Ort	72,4790	0,0037
	Std	0,0826	0,0001
80	Ort	72,5794	0,0036
	Std	0,0819	0,0001
90	Ort	72,5397	0,0036
	Std	0,0831	0,0001

Tablo 3.6. ABC algoritması koloni büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler

PB=40		<i>L</i>	
		PSNR	MSE
50	Ort	72,4144	0,0037
	Std	0,0782	0,0001
60	Ort	72,6514	0,0035
	Std	0,0825	0,0001
70	Ort	72,6984	0,0035
	Std	0,0830	0,0001
80	Ort	72,8002	0,0034
	Std	0,0824	0,0001
90	Ort	72,6255	0,0036
	Std	0,0764	0,0001

3.1.4. Diferansiyel Gelişim Algoritması:

DGA ile yapılan tam sayı yuvarlama için çözüm kümesi 8 gerçel değerli parametre ile temsil edilmiştir. Çözüm kümesindeki bu parametreler tam sayıya yuvarlanarak, elde edilen sayıların ikili kodlamayla 64 bitlik dönüşüm matrisi oluşturulmuştur. Bu dönüşüm matrisi, orijinal görüntü bloklarına eklenerek amaç fonksiyonunun hesaplanmasında kullanılmıştır.

Yapılan deneyde, en iyi farkedilmezlik değerini sunan DGA'nın sahip olduğu adım büyüklüğü (F) ve çaprazlama oranı (ÇO) parametrelerinin araştırılması adına yapılan çalışmalara yer verilmiştir. Yapılan deneyler sonunda elde edilen farkedilmezlik değerleri, Tablo 3.7 ve Tablo 3.8'de gösterilmiştir. Popülasyon büyüklüğü 40, adım büyüklüğü 0.9 ve çaprazlama oranı 0.5 için en iyi farkedilmezlik değerleri PSNR 76.8710 ve MSE 0.0013 olarak elde edilmiştir. GA'ya benzer olarak DGA'da da çaprazlama oranı arttıkça farkedilmezlik değeri yükselmiştir. Tablolarda yer alan standart sapma değerleri algoritmanın kararlı olduğunu göstermektedir. Popülasyon büyüklüğü arttıkça farkedilmezlik değerinde artma olduğu gözlemlenmiştir.

Tablo 3.7. DGA popülasyon büyüklüğü 20 ve 400 çevrim ile elde edilen sayısal metrikler

PB=20			F					
			0.7		0.8		0.9	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
ÇO	0.3	Ort	75,3325	0,0019	75,8755	0,0017	76,2816	0,0015
		Std	0,1485	0,0001	0,1532	0,0001	0,1578	0,0001
	0.4	Ort	75,4251	0,0019	76,0792	0,0016	76,2887	0,0015
		Std	0,1536	0,0001	0,1548	0,0001	0,1524	0,0001
	0.5	Ort	75,2113	0,0020	75,7178	0,0017	76,4725	0,0015
		Std	0,1489	0,0001	0,1501	0,0001	0,1540	0,0001
	0.6	Ort	75,4674	0,0019	75,6435	0,0018	76,1711	0,0016
		Std	0,1590	0,0001	0,1557	0,0001	0,1455	0,0001
	0.7	Ort	75,3545	0,0019	75,7836	0,0017	76,0525	0,0016
		Std	0,1455	0,0001	0,1496	0,0001	0,1494	0,0001

Tablo 3.8. DGA popülasyon büyüklüğü 40 ve 200 çevrim ile elde edilen sayısal metrikler

PB=40			F					
			0.7		0.8		0.9	
			PSNR	MSE	PSNR	MSE	PSNR	MSE
ζO	0.3	Ort	76,1477	0,0016	76,3177	0,0015	76,5664	0,0014
		Std	0,1672	0,0001	0,1516	0,0001	0,1564	0,0001
	0.4	Ort	76,1108	0,0016	76,4441	0,0015	76,6327	0,0014
		Std	0,1411	0,0001	0,1568	0,0001	0,1471	0,0001
	0.5	Ort	76,1609	0,0016	76,5000	0,0015	76,8710	0,0013
		Std	0,1477	0,0001	0,1562	0,0001	0,1330	0,0001
	0.6	Ort	75,9640	0,0017	76,0250	0,0016	76,2300	0,0016
		Std	0,1693	0,0001	0,1536	0,0001	0,1596	0,0001
	0.7	Ort	75,6143	0,0018	76,0419	0,0016	76,1665	0,0016
		Std	0,1465	0,0001	0,1672	0,0001	0,1481	0,0001

Tablolarda yer alan parametre değeri dışındaki değerler için benzer veya daha kötü sonuçlar elde edilmiştir.

3.1.5. Algoritmaların Karşılaştırılması:

Gerçekleştirilen tüm deneylerde, Şekil 3.2’de gösterilen 512×512 boyutunda Lena giriş görüntüsü ve 18×18 boyutunda siyah-beyaz damga kullanılmıştır. Yapılan deneyler sonunda, algoritmaların farkedilmezlikleri analiz edilmiştir ve algoritmaların sunmuş olduğu en iyi farkedilmezlik değerlerinin karşılaştırması Tablo 3.9’da gösterilmiştir. Elde edilen sonuçlar, en iyi farkedilmezlik değeri sunan algoritmanın DGA olduğunu göstermektedir.

Tablo 3.9. Optimizasyon algoritmalarının farkedilmezlik analizi

Optimizasyon Algoritması	PSNR (dB)	MSE
Parçacık Sürü Optimizasyon Algoritması	69,7289	0,0069
Genetik Algoritma	72,7272	0,0035
Yapay Arı Koloni Algoritması	72,8002	0,0034
Diferansiyel Gelişim Algoritması	76,8710	0,0013

Algoritmaların damganın gömülmesinden, damganın çıkarılmasına kadar geçen süreleri hesaplanmış ve elde edilen hesaplama maliyetleri Tablo 3.10’da gösterilmiştir. Hesaplama maliyeti en düşük çıkan algoritmanın, GA olduğu görülmüştür.

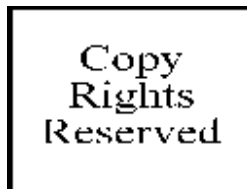
Tablo 3.10. Optimizasyon algoritmalarının hesaplama maliyetleri

Optimizasyon Algoritması	Hesaplama Maliyeti (dk)
Parçacık Sürü Optimizasyon Algoritması	44.93
Genetik Algoritma	42.21
Yapay Arı Koloni Algoritması	95.77
Diferansiyel Gelişim Algoritması	44.7

3.2. Farkedilmezlik Analizi

Farkedilmezlik analizinde, damgalanmış ve çıkarılmış olan görüntülerin algısal kalite ölçümleri, PSNR, MSE ve YB sayısal görüntü kalite metrikleri kullanılarak gerçekleştirilmiştir.

Görüntünün damgalanmasında, Şekil 3.1’de yer alan medikal görüntüleri de içeren birçok farklı görüntü, giriş görüntüsü olarak kullanılmıştır. Giriş görüntüsüne, geliştirilen yöntemin sağlamış olduğu maksimum kapasitede (12288 bit) damgalanmayı sağlayacak, Şekil 3.5’te gösterilen 128×96 boyutundaki siyah-beyaz damga kullanılmıştır.



Şekil 3.5. 128×96 boyutundaki siyah-beyaz damga

Görüntülerin damgalama sonrasında elde edilen algısal kaliteleri, önerilen iki farklı kurcalama tespit yöntemi için Tablo 3.11’de gösterilmiştir. Damgalanmış görüntülerin, ortalama farkedilmezlik değerleri, özel olarak oluşturulan birinci yöntem ile PSNR 59.2739, MSE 0.0787 ve YB 0.9994 olarak elde edilmiştir. MD5 hash fonksiyonu

kullanılan ikinci yöntemde ise PSNR 59.9562, MSE 0.0659 ve YB 0.9994 olarak elde edilmiştir.

Tablo 3.11. Damgalanmış görüntülerin farkedilmezlik değerleri

Görüntü	PSNR (dB)		MSE		YB	
	1.Yöntem	2.Yöntem	1.Yöntem	2.Yöntem	1.Yöntem	2.Yöntem
Baboon	58.4858	60.2082	0.0922	0.0620	0.9998	0.9998
Barbara	58.3912	60.2069	0.0942	0.0620	0.9996	0.9997
Lena	60.6327	60.1466	0.0562	0.0629	0.9996	0.9995
Peppers	60.3011	60.2501	0.0607	0.0614	0.9996	0.9996
Beyin MR-1	59.9085	59.7141	0.0664	0.0695	0.9993	0.9992
Beyin MR-2	58.1611	59.7284	0.0993	0.0692	0.9991	0.9993
Boyun X-Ray	59.8873	59.1695	0.0667	0.0787	0.9990	0.9987
Göğüs X-Ray	58.4237	60.2256	0.0935	0.0617	0.9991	0.9994
Ortalama	59.2739	59.9562	0.0787	0.0659	0.9994	0.9994

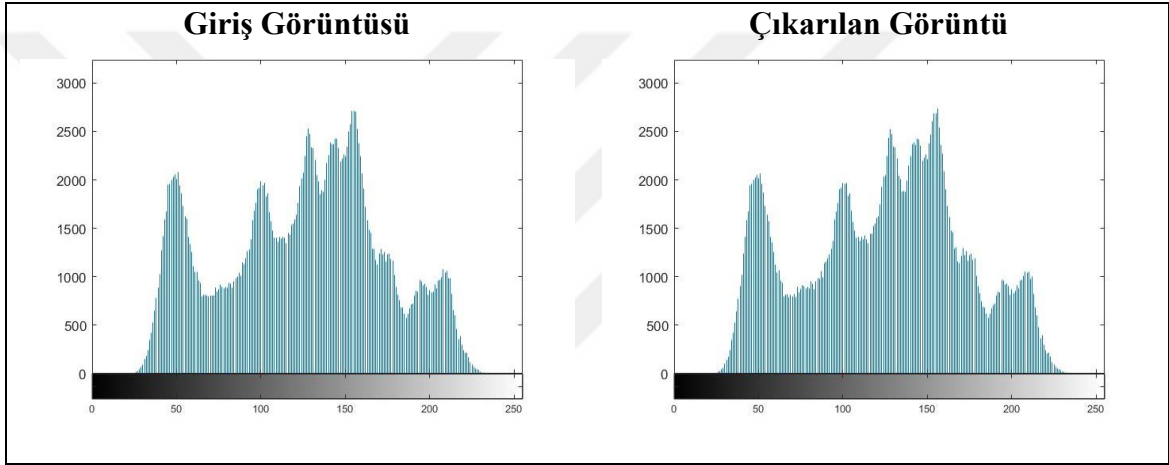
Geliştirilen yöntemin, 512×512 boyutundaki Lena görüntüsü için literatürdeki kurcalama yer tespiti yapabilen, tersinir ve tersinir olmayan bazı yöntemler ile farkedilmezlik değerlerinin karşılaştırması Tablo 3.12’de gösterilmiştir.

Tablo 3.12. Geliştirilen yöntemin, literatürdeki bazı yöntemler ile farkedilmezlik karşılaştırması

Yöntem	Blok Boyutu	Damgalanmış Görüntü PSNR (dB)	Tersinirlik
Gül ve Öztürk [50]	2×4, 4×2	38.3545	Yok
Parah vd. [28]	2×2	39.1735	Var
Gül ve Öztürk [24]	16×16	44.1270	Yok
Tai ve Liao [27]	4×4	44.1400	Var
Raj vd. [51]	8×8	44.1600	Yok
Lee vd. [52]	4×4	47.2000	Yok
Lo ve Hu [53]	4×4	51.4540	Var
Gül ve Öztürk [26]	32×32	57.1960	Yok
Birinci Yöntem	8×8	60.6327	Var
İkinci Yöntem	8×8	60.1466	Var

Önerilen yöntemlerin, literatürdeki tersinir ve tersinir olmayan birçok kırılğan damgalama yönteminden daha iyi farkedilmezlik değeri sunduğu görülmüştür.

Geliştirilen damgalama yöntemi, orijinal görüntünün, damga çıkarma işlemi sırasında kayıpsız bir şekilde elde edilmesini sağlayan tersinir bir özelliğine sahiptir. Damgalanmış görüntüden elde edilen görüntü ile giriş görüntüsünün histogramlarının karşılaştırması Şekil 3.6.'da gösterilmiştir. Çıkarılmış görüntü ile giriş görüntüsünün karşılaştırması, görüntülerin birbirleri ile aynı olduğunu ve görüntünün kayıpsız bir şekilde edilebildiğini göstermektedir.



Şekil 3.6. Giriş görüntüsü ile çıkarılmış görüntünün histogramı

3.3. Kurcalama Yer Tespiti Performans Değerlendirmesi

Geliştirilen yöntemin, saldırılara karşı kurcalama yer tespiti performansını belirlemek için damgalanmış görüntüye içerik değiştirme, kırpma, kopyala-yapıştır, metin ekleme, döndürme ve gürültü ekleme gibi yaygın kullanılan ataklar uygulanmıştır.

İçerik değiştirme saldırısı, damgalanmış bir görüntü içesinden iki parça alarak bunların kendi aralarında yerinin değiştirilmesi ile gerçekleştirilmektedir. Önerilen iki yöntem ile damgalanmış 512×512 boyutundaki Barbara görüntüsüne uygulanan 50×50 boyutunda içerik değiştirme saldırısı sonrası elde edilen sonuçlar Şekil 3.7'de gösterilmiştir.

Önerilen yöntemlerin, geometrik dönüşüm saldırılarından kırpma ve döndürme saldırılarına karşı göstermiş oldukları performans Şekil 3.8'de gösterilmiştir. Kırpma saldırısında, görüntüye %15 oranında kırpma işlemi uygulanmıştır. Döndürme saldırısında, görüntü 10 derece döndürülmüştür.

Yöntem	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem				
2.Yöntem				

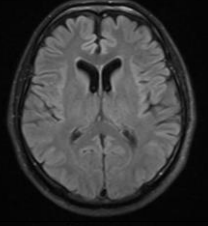
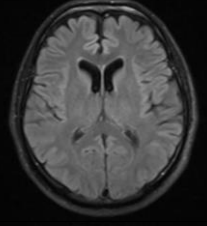
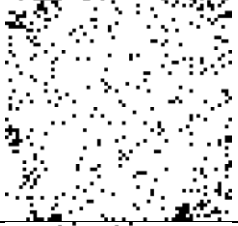
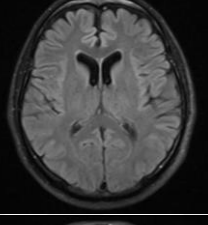
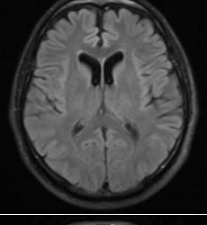
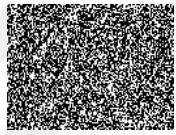
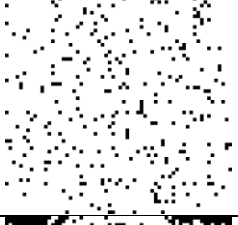
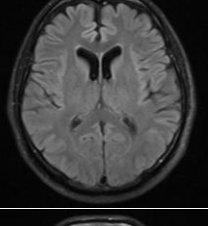
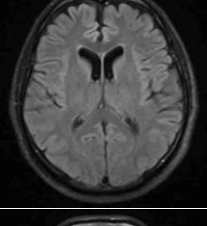
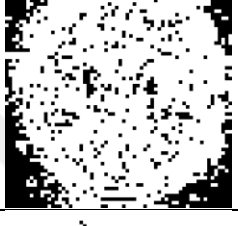
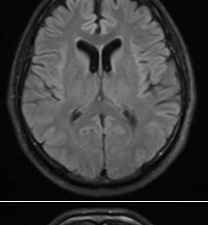
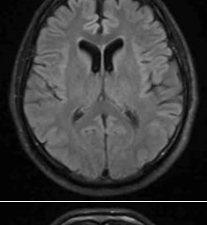
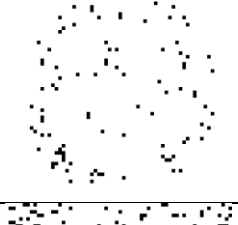
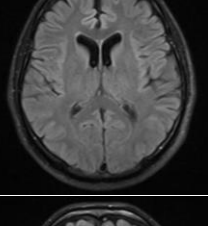
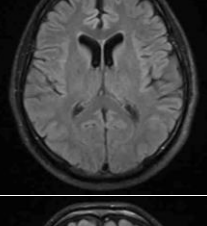
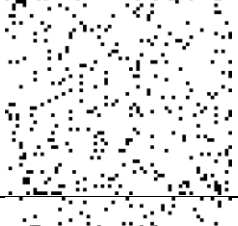
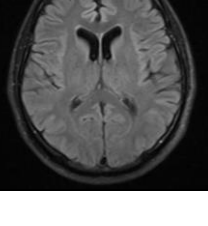
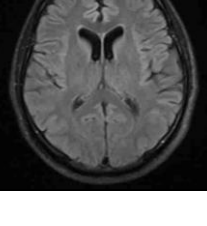
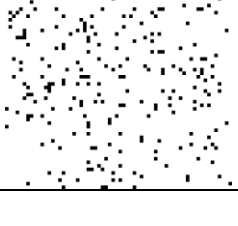
Şekil 3.7. Barbara görüntüsüne uygulanan içerik değişim saldırısı

Sonuçlar, uygulanan kırpma saldırılarını tespit edebildiğini ve döndürme saldırılarında damganın kırılman olduğunu göstermektedir.

Yöntem – Saldırı	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem – Kırpma Saldırısı				
2.Yöntem – Kırpma Saldırısı				
1.Yöntem – Döndürme Saldırısı				
2.Yöntem – Döndürme Saldırısı				

Şekil 3.8. Yöntemlerin, kırpma ve döndürme saldırılarına karşı performansları

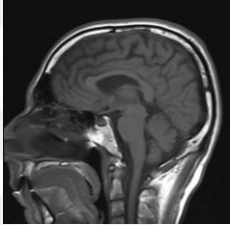
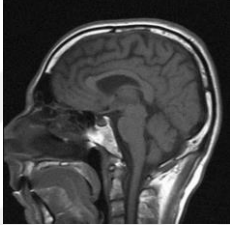
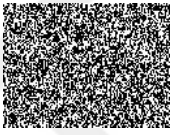
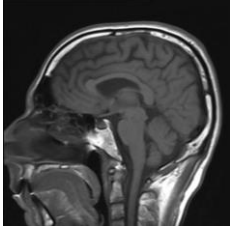
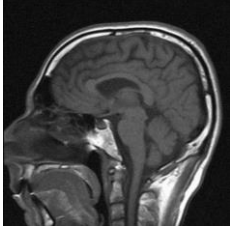
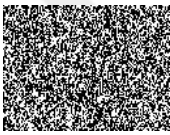
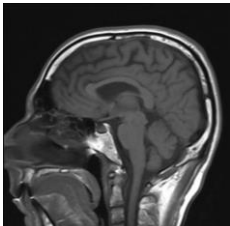
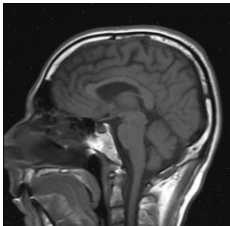
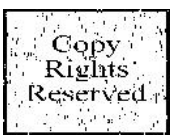
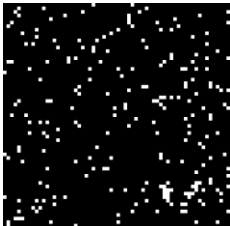
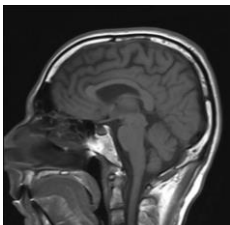
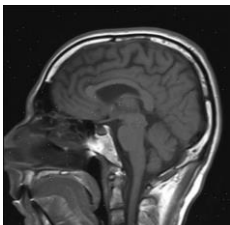
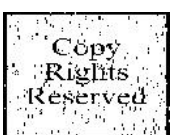
Filtreleme ve sıkıştırma saldırılarından, alçak geçiren filtre, JPEG ve JPEG2000 saldırı sonucu elde edilen sonuçlar Şekil 3.9’da gösterilmiştir.

Yöntem – Saldırı	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem – Alçak Geçiren Filtre Saldırısı				
2.Yöntem – Alçak Geçiren Filtre Saldırısı				
1.Yöntem – JPEG Sıkıştırma Saldırısı				
2.Yöntem – JPEG Sıkıştırma Saldırısı				
1.Yöntem – JPEG2000 Sıkıştırma Saldırısı				
2.Yöntem – JPEG2000 Sıkıştırma Saldırısı				

Şekil 3.9. Yöntemlerin, alçak geçiren filtre, JPEG ve JPEG2000 sıkıştırma saldırılarına karşı performansları

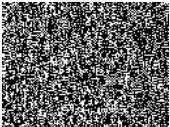
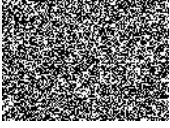
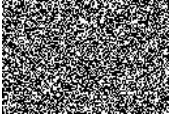
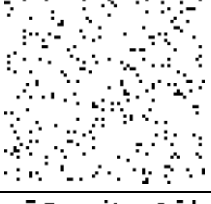
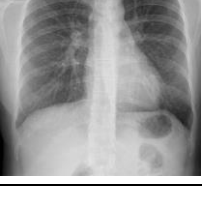
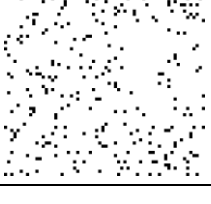
Alçak geçiren filtre saldırısında, 3×3 boyutunda Gaussian alçak filtre, JPEG sıkıştırma saldırısında kalite faktörü 20 ve JPEG2000 sıkıştırma saldırısında sıkıştırma oranı 8 olarak tercih edilmiştir. Elde edilen sonuçlar, önerilen yöntemlerin filtreleme ve sıkıştırma saldırılarına karşı kırılkan olduğunu göstermektedir.

Önerilen yöntemlerin, gürültü ekleme saldırılarından, Gaussian ve tuz-biber saldırılarına karşı göstermiş oldukları performans Şekil 3.10'da gösterilmiştir. Gaussian gürültü ekleme ve tuz-biber saldırıları için gürültü oranı 0.001 olarak seçilmiştir.

Yöntem – Saldırı	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem – Gaussian Gürültü Saldırısı				
2.Yöntem – Gaussian Gürültü Saldırısı				
1.Yöntem – Tuz-Biber Gürültü Saldırısı				
2.Yöntem – Tuz-Biber Gürültü Saldırısı				

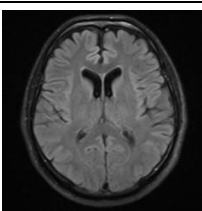
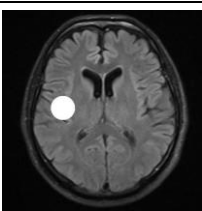
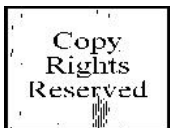
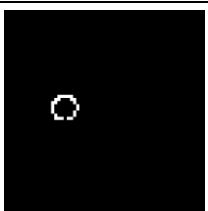
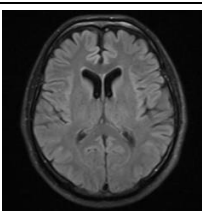
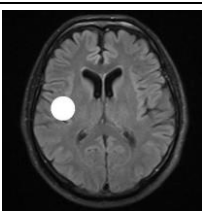
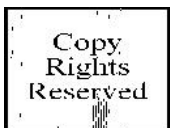
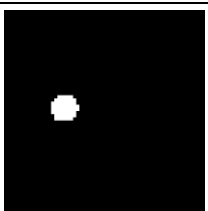
Şekil 3.10. Yöntemlerin, Gaussian ve tuz-biber saldırılarına karşı performansları

Göğüs bölgesine ait X-Ray görüntüsüne, histogram eşitleme, bulanıklaştırma ve 0.8 miktarında keskinleştirme uygulanmıştır. Elde edilen sonuçlar, Şekil 3.11’de gösterilmiştir.

Yöntem – Saldırı	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem – Histogram Eşitleme Saldırısı				
2.Yöntem – Histogram Eşitleme Saldırısı				
1.Yöntem – Bulanıklaştırma Saldırısı				
2.Yöntem – Bulanıklaştırma Saldırısı				
1.Yöntem – Keskinleştirme Saldırısı				
2.Yöntem – Keskinleştirme Saldırısı				

Şekil 3.11. Yöntemlerin, histogram eşitleme, bulanıklaştırma ve keskinleştirme saldırılarına karşı performansları

Yaygın olarak kullanılan, kopyala-yapıştır, metin ekleme ve şekil ekleme saldırılarının MR ve X-Ray görüntülerine uygulanması ile elde edilen sonuçlar Şekil 3.12’de gösterilmiştir.

Yöntem – Saldırı	Damgalanmış Görüntü	Saldırı Uygulanmış Görüntü	Çıkarılan Damga	Kurcalama Tespiti
1.Yöntem – Kopyala- Yapıştır Saldırısı				
2.Yöntem – Kopyala- Yapıştır Saldırısı				
1.Yöntem – Metin Ekleme Saldırısı				
2.Yöntem – Metin Ekleme Saldırısı				
1.Yöntem – Şekil Ekleme Saldırısı				
2.Yöntem – Şekil Ekleme Saldırısı				

Şekil 3.12. Yöntemlerin, kopyala-yapıştır, metin ekleme ve şekil ekleme saldırılarına karşı performansları

4. BÖLÜM

SONUÇ, TARTIŞMA VE ÖNERİLER

4.1. Sonuç

Bu tez çalışmasında, tıbbi görüntülerde doğrulamayı, bütünlüğü ve yapılan kurcalamaları tespit edebilen yüksek farkedilmezliğe sahip damgalanmış görüntü sunan, yeni bir tersinir kırılğan sayısal damgalama yöntemi önerilmiştir.

Yapılan deneysel çalışmalar, önerilen yöntemin yüksek farkedilmezliğe sahip damgalanmış görüntü sunduğunu ve orijinal görüntüyü kayıpsız bir şekilde çıkarabildiğini göstermektedir. Ayrıca, önerilen iki farklı kurcalama tespit yöntemi, yaygın olarak kullanılan kırpma, döndürme, kopyala-yapıştır, metin ekleme ve şekil ekleme gibi saldırılar ile yapılan kurcalamaları yüksek doğrulukta tespit edebilmiş, görüntü üzerine uygulanan filtreleme, sıkıştırma, bulanıklaştırma, keskinleştirme ve gürültü ekleme gibi geometrik dönüşüm saldırılarına karşı kırılğan özellik sergilemiştir.

Kurcalama tespiti için, alternatif iki farklı yöntem ile yüksek doğrulukta kurcalama tespiti yapılması hedeflenmiştir. Önerilen yöntemlerden, doğrulama bitlerinin elde edilmesinde MD5 kullanılan ikinci yöntemde daha yüksek farkedilmezlik ve daha yüksek doğrulukta kurcalama tespiti performansı elde edilmiştir. Ayrıca, MD5 ile elde edilen 128 bitin tamamı yerine belirli sayıda bitini kullanarak kurcalama tespiti yapılabileceği görülmüştür. Farklı yöntemler ile kurcalama tespiti yapılmaya çalışılsa da, doğrulama biti için dört bitlik kapasite olması kurcalama tespiti performansın artırılmasında kısıt oluşturduğu, deney sonuçları ile gösterilmiştir.

Tez çalışmasında, dönüşüm tabanlı yöntemlerde karşılaşılan reel sayı piksel değerlerinden, tam sayı piksel değerlerine dönüşüm sırasında meydana gelen yuvarlama

hataları da vurgulanmış ve bu problemin çözümünde zeki optimizasyon algoritmalarının kullanılabileceği gösterilmiştir.

4.2. Tartışma ve Öneriler

Önerilen sayısal damgalama yöntemi, tıbbi görüntülerin kullanıldığı uygulama alanlarına yönelik hazırlanmıştır. Bu yüzden, orijinal görüntü ve damga saklama ihtiyacını ortadan kaldırmak için görüntü içine gömülecek veri kapasitesinden feragat edilmiştir. Farklı uygulama alanları için, üç bit damga bilgisi ve dört bit damga bilgisini görüntü içerisine gömmek yerine, tüm bitler damga bilgisi olarak gömülebilir. Böylece, orijinal damga bilgisi ve çıkarılan damga bilgisi kıyaslanarak daha yüksek kurcalama tespit performansı elde edilebilir.

Görüntü damgalama süresinin azaltılması için yapılan çalışmada paralel hesaplamadan faydalanılmıştır. Fakat buna rağmen, kullanılan optimizasyon algoritması çalışma süresini uzatmaktadır. Hesaplama maliyetinin azaltılmasına yönelik iyileştirmeler yapılabilir.

KAYNAKÇA

1. Agung, B.W. T., Adiwijaya, Permana, F. P., 2012. Medical image watermarking with tamper detection and recovery using reversible watermarking with LSB modification and Run Length Encoding (RLE) compression. *IEEE International Conference on Communication, Networks and Satellite*, 2012, Indonesia, IEEE, 161-171.
2. Karakis, R., Guler, I., 2018. Steganography and Medical Data Security, 627-660. In: *Cryptographic and Information Security* (Eds: Ramakrishnan, S.), CRC Press, Boca Raton.
3. Abdulrahman, A. K., Ozturk, S., 2019. A novel hybrid DCT and DWT based robust watermarking algorithm for color images. **Multimedia Tools and Applications**, **78.12**: 17027–17049.
4. Qasim, A. F., Meziane, F., Aspin, R., 2018. Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. **Computer Science Review**, **27**: 45–60.
5. Anand, A., Singh, A. K., Watermarking techniques for medical data authentication: a survey. **Multimedia Tools and Applications**, 1–33.
6. Begum, M., Uddin, M. S., 2020. Digital Image Watermarking Techniques: A Review. **Information**, **11.2**: 110.
7. Mousavi, S. M., Naghsh, A., Abu-Bakar, S. A. R., 2014. Watermarking Techniques used in Medical Images: a Survey. **Journal of Digital Imaging**, **27.6**: 714-729.
8. Katzenbeisser, S., Petitolas, F., 2000. Information Hiding Techniques for Steganography and Digital Watermarking. **Artech House Computer Security Series**, **28.6**: 1–2.
9. Coron, J. S., 2006. What is cryptography?. **IEEE Security and Privacy**, **4.1**: 70–73.
10. Gull, S., Loan, N. A., Parah, S. A., Sheikh, J. A., Bhat, G. M., 2020. An efficient watermarking technique for tamper detection and localization of medical images. **Journal of ambient intelligence and humanized computing** **11.5**: 1799–1808.

11. Potdar, V. M., H. Song, and C. Elizabeth, 2005. A survey of digital image watermarking techniques. *3rd IEEE International Conference on Industrial Informatics*, 2005, Perth, Australia, IEEE, 709–716.
12. Thakur, S., Singh, A. K., Ghrera, S. P., Elhoseny, M., 2019. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. **Multimedia Tools and Applications**, **78.3**: 3457–3470.
13. Selvam, P., Balachandran, S., Iyer, S. P., Jayabal, R., 2017. Hybrid transform based reversible watermarking technique for medical images in telemedicine applications. **Optik**, **145**: 655–671.
14. Kumar, C., Singh, A. K., Kumar, P., 2018. A recent survey on image watermarking techniques and its application in e-governance. **Multimedia Tools and Applications**, **77.3**: 3597–3622.
15. Aslantas, V., Ozer, S., Ozturk, S., 2007. A novel clonal selection algorithm based fragile watermarking method. *International Conference on Artificial Immune Systems*, 2007, Berlin, Heidelberg, Springer, 358–369.
16. Zhang, X., Wang, S., 2004. Steganography using multiple-base notational system and human vision sensitivity. **IEEE signal processing letters**, **12.1**: 67–70.
17. Swaraja, K., Meenakshi, K., Kora, P., 2020. An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. **Biomedical Signal Processing and Control**, **55**: 101665.
18. Memon, N. A., Chaudhry, A., Ahmad, M., Keerio, Z. A., 2011. Hybrid watermarking of medical images for ROI authentication and recovery. **International Journal of Computer Mathematics**, **88.10**: 2057–2071.
19. Liu, X., Lou, J., Fang, H., Chen, Y., Ouyang, P., Wang, Y., Zou, B., Wang, L., 2019. A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images. **IEEE Access**, **7**: 76580–76598.
20. I Ansari, I. A., Pant, M., Ahn, C. W., 2017. Artificial bee colony optimized robust-reversible image watermarking. **Multimedia Tools and Applications**, **76.17**: 18001-18025.
21. Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., Bhat, G. M., 2017. Information hiding in medical images: a robust medical image watermarking system for E-healthcare. **Multimedia Tools and Applications**, **76.8**: 10599-10633.

22. Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., Lei, H., 2014. Reversible watermarking scheme for medical image based on differential evolution. **Expert Systems with Applications**, **41.7**: 3178–3188.
23. Das, S., Kundu, M. K., Effective management of medical information through a novel blind watermarking technique. **Journal of medical systems**, **36.5**: 3339-3351.
24. Gul, E., Ozturk, S., 2020. A novel triple recovery information embedding approach for self-embedded digital image watermarking, **Multimedia Tools and Applications**, **79.41**: 31239-31264.
25. Hurrah, N. N., Parah, S. A., Sheikh, J. A., 2020. Embedding in medical images: an efficient scheme for authentication and tamper localization. **Multimedia Tools and Applications**, **79.29**: 21441-21470.
26. Gul, E., Ozturk, S., 2019. A novel hash function based fragile watermarking method for image integrity, **Multimedia Tools and Applications**, **78.13**: 17701-17718.
27. Tai, W. L., Liao, Z. J., 2018. Image self-recovery with watermark self-embedding. **Signal Processing: Image Communication**, **65**: 11-25.
28. Parah, S. A., Sheikh, J. A., Akhoon, J. A., Loan, N. A., 2020. Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. **Future Generation Computer Systems**, **108**: 935-949.
29. Rahman, A., Sultan, K., Aldhafferri, N., Alqahtani, A., Mahmud, M., 2018. Reversible and fragile watermarking for medical images. **Computational and mathematical methods in medicine**.
30. Parah, S. A., Ahad, F., Sheikh, J. A., Bhat, G. M., 2017. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. **Journal of biomedical informatics**, **66**: 214-230.
31. Shih, F. Y., Zhong, X., Chang, I. C., Satoh, S., 2018. An adjustable-purpose image watermarking technique by particle swarm optimization. **Multimedia Tools and Applications**, **77.2**: 1623-1642.
32. Nguyen, T. S., Chang, C. C., Yang, X. Q., 2016. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain. **AEU-International Journal of Electronics and Communications**, **70.8**: 1055-1061.

33. Cui, D., 2008. A semi-fragile watermarking for ROI image authentication. *2008 International Conference on MultiMedia and Information Technology*, 2008, United States, IEEE, 302-305.
34. Aslantas, V., Toprak, A. N., 2014. A pixel based multi-focus image fusion method. **Optics Communications**, **332**: 350-358.
35. Wang, Z., Bovik, A. C., Skeikh, H.R., Simoncelli, E.P., 2004. Image quality assessment: from error visibility to structural similarity. **IEEE transactions on image processing**, **13.4**:600-612.
36. Balasamy, K., Ramakrishnan, S., An intelligent reversible watermarking system for authenticating medical images using wavelet and PSO. **Cluster Computing**, **22.2**: 4431-4442.
37. Kennedy, J., Eberhart, R., 1995. Particle swarm optimization. *Proceedings of ICNN'95-international conference on neural networks*, 1995, IEEE, 1942-1948.
38. Holland, J. H., 1975. Adaptation in natural and artificial systems. Ann Arbor: University of Michigan Press, 183.
39. Holland, J. H., 1992. Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence. MIT press.
40. Karaboğa, D., 2005. An idea based on honey bee swarm for numerical optimization. **Technical report-tr06, Erciyes university, engineering faculty, computer engineering department. 200**: 1-10.
41. Storn, R., Price, K., 1997. Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces. **Journal of global optimization**, **11.4**: 341-359.
42. Keskintürk, T., 2006. Diferansiyel gelişim algoritması. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 2006, İstanbul Ticaret Üniversitesi, 85–99.
43. Price, K. V., Storn, R. M., Lampinen, J. A., 2006. Differential evolution: a practical approach to global optimization. **Springer Science & Business Media**.
44. Fisher, R. A., Yates, F., 1938. Statistical tables for biological, agricultural and medical research. Oliver and Boyd.
45. Knuth, D. E., 1969, The art of computer programming, volume 2: seminumerical algorithms (3rd Edition).

46. Agarwal, S., 2019. Fractal based image cipher using knuth shuffle method and dynamic diffusion. *The International Journal of Computer Networks & Communications*, 2019, Korea, 81–100.
47. Larobina, M., Murino, L., 2014. Medical image file formats. **Journal of Digital Imaging**, **27.2**: 200-206.
48. Aslantas, V., Ozer, S., Ozturk, S., 2009. Improving the performance of DCT-based fragile watermarking using intelligent optimization algorithms. **Optics Communications**, **282.14**: 2806-2817.
49. Rivest, R., 1992. The MD5 message-digest algorithm. Internet Activities Board.
50. Gul, E., Ozturk, S., 2021. A novel pixel-wise authentication-based self-embedding fragile watermarking method. **Multimedia Systems**, **27.3**: 531-545.
51. Neena, R.N. R., Shreelekshmi, R., 2018. Blockwise fragile watermarking schemes for tamper localization in digital images. *2018 International CET Conference on Control, Communication, and Computing*, 2018, IEEE, India, 441-446.
52. Lee, C. F., Shen, J. J., Chen, Z. R., Agrawal, S., 2019. Self-embedding authentication watermarking with effective tampered location detection and high-quality image recovery. **Sensors**, **19.10**: 2267.
53. Lo, C. C., Hu, Y. C., 2014. A novel reversible image authentication scheme for digital images. **Signal Processing**, **98**: 174–185.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı: Gökhan AZİZOĞLU

Uyruğu: Türkiye (T.C)

EĞİTİM

Derece	Kurum	Mezuniyet Tarihi
Yüksek Lisans	Erciyes Üniversitesi Bilgisayar Mühendisliği	-
Lisans	Erciyes Üniversitesi Bilgisayar Mühendisliği	2019
Lisans	Erciyes Üniversitesi Biyomedikal Mühendisliği	2015
Lise	Midyat Anadolu Lisesi, Mardin	2010

İŞ DENEYİMLERİ

Yıl	Kurum	Görev
2020-Halen	Sivas Cumhuriyet Üniversitesi	Araştırma Görevlisi
2020-2020	Kapadokya Üniversitesi	Araştırma Görevlisi
2017-2020	Kayseri Ulaşım A.Ş.	Mühendis

YABANCI DİL

İngilizce

YAYINLAR

1. Azizoğlu, G., Toprak, A.N., 2021. A novel reversible fragile watermarking in DWT domain for tamper localization and digital image authentication. *9th International Symposium on Digital Forensics and Security*, 2021, IEEE.