

**BLOK KIRPMA KODLAMASINA VE
AYRIK DALGACIK DÖNÜŞÜMÜNE
DAYALI, DAYANIKLI DİJİTAL RENKLİ
RESİM DAMGALAMA SİSTEMİ**

Yasir A. HAMZA

Yüksek Lisans Tezi

Bilgisayar Mühendisliği Anabilim Dalı

Mayıs - 2008

JÜRİ VE ENSTİTÜ ONAYI

Yasir A. HAMZA'nın "Blok Kırpma Kodlamasına ve Ayrık Dalgacık Dönüşümüne Dayalı, Dayanıklı Dijital Renkli Resim Damgalama Sistemi" başlıklı **Bilgisayar Mühendisliği** Anabilim Dalındaki, Yüksek Lisans Tezi 28.04.2008 tarihinde, aşağıdaki jüri tarafından Anadolu Üniversitesi Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

Adı-Soyadı	İmza
Üye (Tez Danışmanı) : Prof. Dr. YAŞAR HOŞCAN	
Üye : : Doç. Dr. ÖMER NEZİH GEREK	
Üye : : Yard. Doç. Dr. CÜNEYT AKINLAR	

Anadolu Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
.....tarih ve sayılı kararıyla onaylanmıştır.

Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

BLOK KIRPMA KODLAMASINA VE AYRIK DALGACIK DÖNÜŞÜMÜNE DAYALI, DAYANIKLI DİJİTAL RENKLİ RESİM DAMGALAMA SİSTEMİ

Yasir A. HAMZA

**Anadolu Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı**

Danışman: Prof. Dr. Yaşar HOŞCAN

2008, 92 sayfa

Son zamanlarda, dijital çoklu ortam içeriğinin dağıtılması için İnternet'in platform olarak kullanılması gittikçe artmaktadır. İnternet gibi açık bir ortamın kullanılması, işlemdeki dijital içeriğin zihinsel mülkiyet haklarının korunmasına ve uygulanmasına dair tehlikeleri artırmaktadır. Zihinsel mülkiyet haklarının korunması için çoklu ortam verilerin içine dijital filigran gömme metodu mevcuttur.

Bu tez çalışmasında, dijital resimlerde telif hakları korumak için, yeni bir görünmez ve dayanıklı dijital renkli resim damgalama yöntemi önerilmiştir. Önerilen yöntem blok kırpma kodlamasına ve ayrik dalgacık dönüşümüne dayalıdır. Resim damgalama işleminde, 24-bitlik renkli Bitmap formatında resim kullanılmaktadır. Resme damgalanacak filigran, 1-bitlik siyah-beyaz Bitmap formatında resimdir. Resim damgalama algoritmasının dayanıklılığını artırmak için resim damgalama işleminden önce, damgalanacak filigrana gizli bir anahtar kullanılarak, permütasyon işlemi uygulanır. Kullanılan gizli anahtar hem resme filigran damgalama işleminde hem de resimden filigran çıkarma işleminde kullanılır.

Önerilen damgalama yöntemini test etmesi için, damgalanmış resim, orijinal resim ve çıkarılmış filigranların üzerlerinde, üç performans değerlendirme ölçütü kullanılmıştır. Ayrıca önerilen yöntemin dayanıklılığını ispatlamak için, farklı türde saldırılar damgalanmış resimlerin üzerinde denenmiştir. Elde edilen sonuçlar, önerilen damgalama yöntemini, JPEG kayıplı sıkıştırma, gürültü ekleme, filtreleme, histogram eşitleme, mozaik, gama düzeltme, kontrast ayarlama, ölçekleme, rastgele çizme, sahte filigran ekleme, filigran çarpıştırma, morfolojik ve JPEG2000 kayıplı sıkıştırma gibi işlemlere ve saldırılara karşı dayanıklı olduğunu göstermiştir.

Anahtar Sözcükler: Resim Damgalama, Dayanıklı, Filigran, Ayrik Dalgacık Dönüşümü, Blok Kırpma Kodlaması

ABSTRACT**Master of Science Thesis****BLOCK TRUNCATION CODING AND DISCRETE WAVELET
TRANSFORM BASED ROBUST DIGITAL COLOR IMAGE
WATERMARKING SYSTEM****Yasir A. HAMZA****Anadolu University
Graduate School of Sciences
Computer Engineering Program****Supervisor: Prof. Dr. Yaşar HOŞCAN****2008, 92 pages**

Recently, Internet is being increasingly used as the platform for distribution of digital multimedia content. The use of an open medium like Internet gives rise to concerns about protection and enforcement of intellectual property rights of the digital content involved in the transaction. One of the methods for the protection of intellectual property rights is the embedding of digital watermarks into multimedia data.

In this thesis work, new invisible and robust digital color image watermarking method is proposed for protection of copyrights of digital images. The proposed method is based on block truncation coding and discrete wavelet transform. In the image watermarking process, 24-bit color bitmap image is used. The watermark that is embedded in image is 1-bit black and white bitmap image. To increase robustness of the image watermarking method; by using a secret key, a watermark permutation process is performed on watermark that will be used for embedded process before image watermarking process. The selected secret key is used in watermark embedding process and watermark extraction process from image.

Three performance evaluation measurements are used on watermarked image, original image and extracted watermark, for testing proposed watermarking method. Various types of attacks are applied on watermarked image to prove the robustness of proposed method. The results have shown that the proposed watermarking method is robust against attacks and processes such as JPEG lossy compression, noise addition, filtering, histogram equalization, mosaic, gamma correction, contrast adjustment, scaling, randomize drawing, fake watermark addition, watermark collision, morphologic and JPEG2000 lossy compression.

Keywords: Image Watermarking, Robust, Watermark, Discrete Wavelet Transform, Block Truncation Coding

TEŞEKKÜR

Geleceğime yol gösterenler ve hayatım boyunca onlara borçlu olacağım değerli rahmetli babam Ahmet BEYATLI'ya ve değerli anneme, içtenlikle teşekkür ederim.

Bu tez çalışmasının başından sonuna kadar her aşamasında benden yardımlarını esirgemeyen, beni yönlendiren ve motive eden değerli tez danışmanım Prof. Dr. Yaşar HOŞCAN'a sonsuz teşekkürlerimi sunarım.

Tez konusu seçimimde ve çalışmam süresince bana yardım ettiği için Sayın Doç. Dr. Ömer Nezih GEREK'e çok teşekkür ederim.

Anadolu Üniversitesi Bilgisayar Mühendisliği Bölümü'nde öğrenim ve tez çalışma süremce tanıştığım sayın hocalarıma ve arkadaşlarıma çok teşekkür ederim.

Tezin çalışma süresince bana yardım ettiği için Sayın Öğr. Gör. Muzaffer DOĞAN'a çok teşekkür ederim.

Tezin çevirme ve metin düzeltmelerinde bana yardım eden arkadaşım Uğur KURUKAFA'ya çok teşekkür ederim.

Hayatımın her anında olduğu gibi, tez çalışmalarım sırasında da anlayışları, sevgileri ve sabırlarıyla beni destekleyen sevgili aileme ve bütün arkadaşlarıma çok teşekkür ederim.

Son olarak beni her zaman destekleyen ve yüreklendiren eşim Necla BEYATLI'ya ve çocuklarım Ammar ve Ezhar'a içtenlikle teşekkür ederim.

Yasir A. HAMZA

Mayıs, 2008

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	i
ABSTRACT	ii
TEŞEKKÜR	iii
İÇİNDEKİLER.....	iv
ŞEKİLLER DİZİNİ	vii
ÇİZELGELER DİZİNİ.....	xii
SİMGELER VE KISALTMALAR DİZİNİ.....	xiv
1. GİRİŞ	1
2. VERİ GİZLEME	5
2.1. Veri Gizleme Tarihçesi	5
2.2. Veri Gizleme Terminolojisi	8
2.2.1. Steganografi	8
2.2.1.1. Algılamaya Karşı Koruma..	8
2.2.1.2. Kaldırmaya Karşı Koruma	9
2.2.2. Kriptoloji.....	11
2.2.3. Dijital Damgalama.....	11
2.2.4. Parmak İzi.....	11
2.2.5. Dijital İmzalama.....	12
2.3. Damgalama.....	12
2.3.1. Dijital Damgalama Nedir.....	13
2.3.2. Dijital Damgalamanın Gereksinimleri.....	14
2.3.2.1. Aslına Sadakat (Fark Edilmezlik).....	15
2.3.2.2. Dayanırılık.....	15
2.3.2.3. Damgalamanın Yararlı Yüğü.....	15
2.3.2.4. Güvenlik.....	16
2.3.2.5. Kör ve Kör Olmayan Damgalama.....	16
2.3.3. Dijital Damgalama Türleri.....	17
2.3.3.1.Uzamsal Bölge ve Dönüşüm Bölge Damgalaması.....	18

2.3.3.2. Görünebilir ve Görünmez Damgalama.....	19
2.3.3.3. Dayanıklı ve Kırılgan Damgalama.....	19
2.3.3.4. Kamusal ve Kişisel Damgalama.....	19
2.3.3.5. Kaynağa Dayalı ve Hedefe Dayalı Damgalama.....	20
2.3.4. Dijital Damgalama Uygulamaları.....	20
2.3.4.1. Telif Hakkı Koruma.....	21
2.3.4.2. Parmak İzi.....	21
2.3.4.3. Veri Asılama.....	21
2.3.4.4. Tıbbi Bilgiler Güvenliği.....	21
2.3.4.5. Bilgi Gizleme.....	22
2.3.4.6. Kopyalama Koruması.....	22
2.3.4.7. Yayın Gözetleme.....	22
3. DALGACIK DÖNÜŞÜMÜ VE BLOK KIRPMA KODLAMASI	23
3.1. Giriş.....	23
3.2. Ayrık Dalgacık Dönüşümü	24
3.2.1.1. Haar Ayrık Dalgacık Dönüşümü.....	25
3.2.1.2. Haar ADD'nin Dijital Resimler Üzerine Uygulanması....	27
3.2.1.3. Haar ADD Algoritması.....	29
3.2.2. ADD'nin Karakteristikleri.....	30
3.3. Blok Kırpma Kodlaması	32
3.3.1. Blok Kırpma Kodlamasının Temel Algoritması.....	32
3.3.2. BKK Algoritma'sının Özellikleri.....	35
4. MATERYAL VE YÖNTEM	36
4.1. Giriş.....	36
4.2. Materyal.....	36
4.3. Yöntem.....	38
4.4. Resim Damgalama İşlemi.....	39
4.4.1. Filigran Permutasyon İşlemi.....	41
4.4.2. Önerilen Damgalama Algoritması.....	41
4.4.3. Filigran Çıkarma Algoritması.....	46

5. ARAŞTIRMA BULGULARI VE TARTIŞMA	50
5.1. Giriş.....	50
5.2. Filigrana Karşı Yapılabilecek Saldırıların Çeşitleri.....	50
5.2.1. Basit Saldırıların.....	51
5.2.2. Filigran Algılamayı Devre Dışı Bırakan Saldırıların.....	51
5.2.3. Sahte Filigran Ekleme Saldırıları.....	51
5.2.4. Filigran Kaldırma Saldırıları.....	52
5.3. Damgalama Algoritmasının Performans Değerlendirme Ölçütleri.....	52
5.4. Performans Değerlendirme Testleri.....	53
5.4.1. Orijinal Resim ile Damgalanmış Resmin Arasındaki Farklılık.....	53
5.4.2. Damgalama Güçlendirme α Değerinin Damgalanmış Remin Kalitesine Etkisi.....	54
5.4.3. JPEG Kayıplı Sıkıştırması.....	58
5.4.4. Gürültü Ekleme.....	59
5.4.5. Kırpma İşlemi.....	61
5.4.6. Filtreleme.....	63
5.4.7. Döndürme İşlemi.....	67
5.4.8. Histogram Eşitleme.....	69
5.4.9. Mozaik İşlemi.....	70
5.4.10. Gama Düzeltme İşlemi.....	72
5.4.11. Kontrast Ayarlama İşlemi.....	74
5.4.12. Ölçekleme İşlemi.....	76
5.4.13. Rastgele Çizme.....	77
5.4.14. Sahte Filigran Ekleme Saldırısı.....	78
5.4.15. Filigran Çarpıştırma Saldırısı.....	80
5.4.16. Morfolojik İşlemler.....	82
5.4.17. JPEG2000 Kayıplı Sıkıştırması.....	84
6. SONUÇ VE ÖNERİLER	86
KAYNAKLAR.....	89

ŞEKİLLER DİZİNİ

2.1. Veri gizleme tekniklerin dalları.....	6
2.2. Damgalama tekniği ile diğer gizleme tekniklerin arasındaki ilişkiler.....	7
2.3. Steganografi türleri.....	8
2.4. Simmons'un tarafından formüle edilen Mahkumlar Problem'i.....	9
2.5. Damgalama sistemin genel yapısı.....	14
2.6. Dijital damgalamanın gereksinimlerin arasındaki ortak ilişkiler.....	17
2.7. Damgalama sistemin temel gereksinimlerin arasındaki bedel ilişkileri.....	17
2.8. Dijital damgalamanın türleri.....	18
3.1. Filtreme işleminden sonra sinyalin spektrum ayrışımı.....	25
3.2. $x[n]$ Tek boyutlu sinyali üzerinde ADD işleminin uygulanması, (a) sinyalin üzerine ADD ayrıştırma işlemi, (b) sinyali geri çatma işlemi.....	27
3.3. Resmin üzerine ADD işleminin uygulanması, (a) resmin üzerine ADD ayrıştırma işlemi, (b) resmi geri çatma işlemi.....	28
3.4. Yatay işleminin resmin birinci satırı üzerine uygulanması.....	29
3.5. Dikey işleminin resmin sütunları üzerine uygulanmasını.....	30
3.6. Lena resmi üzerinde Haar ADD birinci ve ikinci seviye ayrıştırma işlemi.....	31
3.7. BKK algoritması resmin bir bloğun üzerine uygulanması, (a) Orijinal resim bloğu, ortalaması=159, (b) Kodlama işlemi uygulandıktan sonra bilgiler, ML=182 ve MH=136. (c) Çözücüde bloğu yeniden kurma işlemi, (d) OKH =128,5.....	34
4.1. Resimlere damgalanacak filigran.....	37
4.2. Testler için kullanılan resimler, (a) Lena, (b) Baboon.....	37
4.2. (Devam)Testler için kullanılan resimler, (a) Lena, (b) Baboon.....	38
4.3. Damgalama işleminin blok diyagramı.....	40
4.4. Önerilen damgalama algoritması.....	44
4.5. (0.1) α değeriyle damgalanmış resimler, (a) Lena , (b) Baboon.....	45
4.6. Filigran çıkarma algoritmasının blok diyagramı.....	46
4.7. Damgalanmış resimden filigran çıkarma algoritması.....	48

4.8. Lena resminden çıkarılan filigranlar, (a) DD1'den çıkarılan filigran, (b)DY1'den çıkarılan filigran, (c) YD1'den çıkarılan filigran, (c) YY1'den çıkarılan filigran.....	49
4.9. Baboon resminden çıkarılan filigranlar, (a) DD1'den çıkarılan filigran, (b) DY1'den çıkarılan filigran, (c) YD1'den çıkarılan filigran, (c) YY1'den çıkarılan filigran.....	49
5.1. Test resimleri, (a) orijinal Lena resmi ile damgalanmış resmin arasındaki mutlak farklılık resmi, (b) orijinal Baboon resmi ile damgalanmış resmin arasındaki mutlak farklılık resmi.....	54
5.2. Farklı α değerleriyle damgalanmış resimlerde oluşan bozulmanın α değerine göre grafiği.....	55
5.3. Farklı α değerleriyle damgalanmış resimler ile orijinal resimler arasındaki DSGO kalite ölçümünün, α değerine göre grafiği.....	56
5.4. Farklı α değerleriyle damgalanmış resimlerden çıkarılmış filigranlar ile orijinal filigran arasındaki NK benzerlik ölçümünün, α değerine göre grafiği.....	57
5.5. (0.2) α değeriyle damgalanmış Baboon resmin JPEG kayıplı sıkıştırması uygulandıktan sonra çıkarılmış filigranların NK sonuçları.....	58
5.6. (0.2) α değeriyle damgalanmış Lena resmin üzerine JPEG kayıplı sıkıştırması uygulandıktan sonra çıkarılmış filigranların NK sonuçları.....	59
5.7. (0.1) α değeriyle damgalanmış Lena resmin üzerine %5 oranla Gauss gürültüsü eklendikten sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	61
5.8. (0.1) α değeriyle damgalanmış Lena resmin üzerine %10 oranla Gauss gürültüsü eklendikten sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	61
5.9. (0.1) α değeriyle damgalanmış Lena resmi üzerine kırpma işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	62

- 5.10. (0.1) α değeriyle damgalanmış Lena resminin üzerine ortanca filtresi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....64
- 5.11. (0.1) α değeriyle damgalanmış Lena resminin üzerine Gauss bulandırması 3×3 boyutlarıyla DGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....65
- 5.12. (0.1) α değeriyle damgalanmış Lena resminin üzerine Gauss bulandırması 5×5 boyutlarıyla DGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....65
- 5.13. (0.1) α değeriyle damgalanmış Lena resmi üzerine %95 oranla keskinleştirme YGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....67
- 5.14. (0.1) α değeriyle damgalanmış Lena resmin üzerine 1° saat yönünde döndürme uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....68
- 5.15. (0.1) α değeriyle damgalanmış Lena resminin üzerine histogram eşitleme işlemi uygulandıktan sonra, (a) Lena resmi (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....69
- 5.16. (0.1) α değeriyle damgalanmış Lena resmin üzerine 2 blok değeriyle mozaik işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....71
- 5.17. (0.1) α değeriyle damgalanmış Lena resmin üzerine 3 blok değeriyle mozaik işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den

çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	72
5.18. (0.1) α değeriyle damgalanmış Lena resmin üzerine 0.5 gama değeriyle gama düzeltme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	73
5.19. (0.1) α değeriyle damgalanmış Lena resmin üzerine 5 gama değeriyle gama düzeltme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	74
5.20. (0.1) α değeriyle damgalanmış Lena resmi üzerine -05 değeriyle kontrast işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	75
5.21. (0.1) α değeriyle damgalanmış Lena resmi üzerine +05 değeriyle kontrast işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	76
5.22. (0.1) α değeriyle damgalanmış ve 256×256 boyutlarında ölçeklenmiş Lena resminden çıkarılmış filigranlar (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran.....	77
5.23. (0.1) α değeriyle damgalanmış Lena resmin üzerine rastgele çizgi çizmek, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	78
5.24. İkinci damgalama işleminde kullanılan filigran.....	79
5.25. (0.1) α değeriyle ve aynı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran.....	79
5.26. (0.1) α değeriyle ve farklı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran,	

(b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran.....	80
5.27. (0.1) α değeriyle ve aynı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran.....	81
5.28. (0.1) α değeriyle ve farklı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran.....	81
5.29. (0.1) α değeriyle damgalanmış Lena resmi üzerine genişleme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	83
5.30. (0.1) α değeriyle damgalanmış Lena resmi üzerine aşındırma işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran.....	84
5.31. (0.1) α değeriyle damgalanmış Lena resmin JPEG2000 kayıplı sıkıştırması uygulandıktan sonra, resimden çıkarılmış filigranların NK sonuçları.....	85

ÇİZELGELER DİZİNİ

2.1. Steganografi ve damgalamanın arasındaki farklılıklar.....	10
2.2. Dijital damgalama uygulamaların sınıflandırmasını.....	20
3.1. $x[n]$ Örnek sinyalin ayrıştırma işlemi üzerine uygulandıktan sonra, frekansların katsayıları ve çözünürlük değerleri.....	26
5.1. $\alpha=0.1$ ile $\alpha=0.01$ arasında değişen 10 farklı α değeriyle damgalanmış test resimlerinde oluşan bozulmanın OKH ile ölçüm sonuçları.....	55
5.2. $\alpha=0.1$ ile $\alpha=0.01$ arasında değişen 10 farklı α değeriyle damgalanmış resimler ile orijinal resimler arasındaki kalite ölçümü, DSGO sonuçları.....	56
5.3. $\alpha=0.1$, $\alpha=0.01$, $\alpha=0.001$ ve $\alpha=0.0001$ arasında α değerleriyle damgalanmış resimlerden çıkarılmış filigranlar ile orijinal filigran arasındaki benzerlik değeri, NK sonuçları.....	57
5.4. $\alpha=0.1$ değeriyle damgalanmış lena resmi ve %5 ve %10 oranla Gauss gürültüsü eklendikten sonra çıkarılmış filigranların NK sonuçları.....	60
5.5. (0.1) α değeriyle damgalanmış ve kırılmış lena resminden çıkarılmış filigranların NK sonuçları.....	62
5.6. (0.1) α değeriyle damgalanmış ve üzerine ortanca filtresi uygulanan lena resminden çıkarılmış filigranların NK sonuçları.....	63
5.7. (0.1) α değeriyle damgalanmış ve üzerine DGF uygulanan lena resminden çıkarılmış filigranların NK sonuçları.....	65
5.8. (0.1) α değeriyle damgalanmış ve üzerine YGF uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	68
5.9. (0.1) α değeriyle damgalanmış ve üzerine döndürme işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	66
5.10. (0.1) α değeriyle damgalanmış ve üzerine histogram eşitleme işlemi uygulanmış Lena resminden çıkarılmış filigranların NK sonuçları.....	69
5.11. (0.1) α değeriyle damgalanmış ve üzerine 2 ve 3 blok değeriyle mozaik işlemi uygulanmış Lena resminden çıkarılmış filigranların NK sonuçları.....	70
5.12. (0.1) α değeriyle damgalanmış ve üzerine 0.5 ve 5 gama değeriyle gama düzeltme işlemi uygulanan Lena resminden çıkarılmış	

filigranların NK sonuçları.....	73
5.13. (0.1) α değeriyle damgalanmış ve üzerine -50 ve +50 değerleriyle kontrast işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	75
5.14. (0.1) α değeriyle damgalanmış ve üzerine ölçekleme işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	77
5.15. (0.1) α değeriyle damgalanmış ve üzerine aynı ve farklı gizli anahtar kullanarak tekrar üzerine damgalama işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	79
5.16. (0.1) α değeriyle damgalanmış ve üzerine aynı ve farklı gizli anahtarlar kullanarak üzerine tekrar damgalama işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları.....	81
5.17. (0.1) α değeriyle damgalanmış ve üzerine genişleme ve aşındırma işlemleri uygulandıktan sonra Lena resminden çıkarılmış filigranların NK sonuçları.....	83

SİMGELER VE KISALTMALAR DİZİNİ

No.	Türkçe	Kısaltması	İngilizce	Kısaltması
1	Ayrık Dalgacık Dönüşümü	ADD	Discrete Wavelet Transform	DWT
2	Blok Kırpma Kodlaması	BKK	Block Truncation Coding	BTC
3	Dijital Haklar Yönetimi	DHY	Digital Rights Management	DRM
4	Doruk Sinyalin ile Gürültü Oranı	DSGO	Peak Signal to Noise Ratio	PSNR
5	Düşük-Düşük Alt-bant	DD	Low-Low Sub-band	LL
6	Düşük-geçiren Filtre	DGF	Low-pass Filter	LPF
7	Düşük-Yüksek Alt-bant	DY	Low-High Sub-band	LH
8	Normalleştirme Kolerasyonu	NK	Normalized Correlation	NC
9	Orijinal Düşük- Düşük	ODD	Original Low-Low	OLL
10	Orijinal Düşük-Yüksek	ODY	Original Low-High	OLH
11	Orijinal Yüksek-Düşük	OYD	Original High-Low	OHL
12	Orijinal Yüksek-Yüksek	OYY	Original High-High	OHH
13	Ortalama Kare Hatası	OKH	Mean Square Error	MSE
14	Sürekli Dalgacık Dönüşümü	SDD	Continuous Wavelet Transform	CWT
15	Ters Ayrık Dalgacık Dönüşümü	TADD	Inverse Discrete Wavelet Transform	IDWT
16	Yüksek-Düşük Alt-bant	YD	High-Low Sub-band	HL
17	Yüksek-geçiren Filtre	YGF	High-pass Filter	HPF
18	Yüksek-Yüksek Alt-bant	YY	High-High Sub-band	HH
19	Zihinsel Mülkiyet	ZM	Intellectual Property	IP

1. GİRİŞ

Son zamanlarda, dijital çoklu ortam içeriğinin dağıtılması için İnternet'in platform olarak kullanılması gittikçe artmaktadır. İnternet'in kalıtsal esnekliği, kullanıcıların dijital içeriğin farklı formlarını (örneğin metin dokümanlar, veritabanı, elektronik-kitap (e-kitap), resim, ses, video, bilgisayar yazılımı ve oyun) kurmak, dağıtmak, kayıt etmek, tekrar kullanmak, abone olmak, arttırmak, değiştirmek ve alışveriş yapmak amacıyla birbirleriyle iletişim kurmalarını kolaylaştırır.

İnternet gibi açık bir ortamın kullanılması, işlemdeki dijital içeriğin zihinsel mülkiyet (ZM) haklarının korunmasına ve uygulanmasına dair tehlikeleri artırır. Üstelik dijital içeriğin yetkisiz kopyalanması ve işlenmesi nispeten önemsiz ve ucuz araçlar kullanılarak yapılabilir. Bu işlem geleneksel analog çoklu ortam içeriğine benzemez. Dijital haklar yönetim (DHY) sistemleri dijital içeriğin mülkiyet haklarına ait konuları belirtmektedir. DHY sistemleri dijital içeriğin ZM haklarının yetkisiz kullanımını, kopyalanmasını ve dijital içeriğin dağıtımını engellemeye, tarif ederken, tanımlarken, ticaret yaparken, korurken, izlerken ve takip ederken yardımcı olur.

Moving Pictures Expert Group (MPEG), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C) gibi çeşitli organizasyonlar, DHY sistemlerini standardize etmeye çalışıyorlar. DHY'e yönelik önemli ölçüde ilgi ve çalışma olmasına rağmen, ZM hakları ve içeriği koruma konusu yasal karışıklıklar ve anlaşmazlıklarla doludur [1]. Farklı grupları; örneğin içeriği inşa edenler, müzik kayıt şirketleri, film üretme evleri, kitap yayım evleri, açık-kaynaklı yazılım geliştirme toplulukları, tüketim elektronik mallar sanayisi, yazılım şirketleri, hükümet organizasyonları ve kullanıcılar, ZM hakları yönetiminde ve korumasında farklı bakışları ve görüşleri vardır. Bu yüzden, bu günlerde ZM hakları çok tartışılan bir konu haline gelmiştir.

Bundan dolayı DHY sistemlerin geniş bir şekilde uygulanmasındaki en büyük sorunlar, DHY sistemlerin çerçevesinin ve alanının belirtilen tüm gruplar tarafından kabul gören bir tanımının yapılması ve DHY ile ilgilenen yasal, politik, iş ve yayın çevrelerine hitap etmesidir. DHY sistemleri içerik yönetimin farklı

yönlerine hitap etmektedir, örneğin (içerik tanımlama, içerik depolama, içerik gösterim, içerik dağıtım ve ZM haklar yönetimi).

Bu günlerde, çoklu ortam ürünleri ve dağıtımları, yetki vasıtaları kullanan içerik sağlayıcılardan alıcılara kadar, hepsi dijital ortamdadırlar. Dijital işlemenin ve dağıtımının gürültüsüz aktarma, donanım işlemenin yerine yazılım ve sistemleri yeniden yapılandırma yeteneğini ispatlama gibi avantajları, herkese belli ve açıktır. Çok açık olmamakla beraber, dijital medya dağıtımının dezavantajları da vardır. Örneğin medya üreticileri ve içerik sağlayıcıları açısından bakılırsa, dijital verilerin asıllarına sadakati kaybetmeden sınırsız kopyalamaları istenilmeyen bir durumdur. Çünkü bu işlem büyük bir parasal kayba neden olabilir.

Dijital kopyalama koruması ve kopyalama engelleme mekanizmalarının sınırlı bir değeri vardır. Çünkü korunmuş verilerin orijinal sürümlerine erişmek, en azından karşılığını ödeyen alıcılara verilir. Bundan sonra, alıcı yasa dışı kopyaları üretilip dağıtabilir. Kopyalama engellemesine yönelik tekniksel denemeler daima engellenmiştir. Zihinsel mülkiyet haklarının korunması için çoklu ortam verilerin içine dijital filigranlar gömme metodu mevcuttur.

Filigran kaldırılmayan, dayanıklı ve fark edilmez bir dijital koddur. Bu kod örtülü veri içine gömülür ve genellikle kaynak hakkında, konum ve/veya verilerin hedef bilgilerini kapsar. Buna rağmen damgalama, kopyalama koruması için direkt bir şekilde kullanılmaz. Ama en azından çoklu ortam verilerinin kaynağını ve hedefini tanımlayabilir ve mülkiyet hakkının ihlal edilmesinden şüphelendiği durumda son savunma hattı gibi uygun takip etme hareketleri sağlar.

Telif hakkını korumak, damgalama tekniklerinin en önemli uygulamasıyken, var olan diğer uygulamalar da verinin asılmasını gerektirmektedir [27]. Veri asılama uygulamalarında kırılğan filigranlar kullanılır. Eğer damgalanmış veri işlendiyse, o zaman gömülen kırılğan filigranlar ya bozulurlar ya da yok olurlar. Böylece çoklu ortam verilerinin aktarılmasına değerli bir ek hizmet sunar. Bazı uygulamalarda, veri gözetleme ve takip etme gibi, verilerin etiketini gömmek gerekmektedir. Veri gözetleme sistemine bir örnek, otomatik kayıt etme ve gözetleme yayın radyo programlarıdır.

Damgalama metotları geliřtirmek, bazı tasarım bedellerine baėlıdır. Damgalanan filigran, standart veri řlemelerine karřı dayanıklı olmalıdır. Örneėin; dijitalden analoga çevirme řlemi ile dijital formata çevirme řlemi. Güvenlik, damgalama metotlarının çok önemli bir gereksinimidir ve damgalanan filigran, bilgili bireylerin yeltenme saldırılarına bile direnmelidir. Ayrıca, damgalanan filigran fark edilmez olmalı ve taşıdığı bilgi miktarı mümkün olduėunca çok olmalıdır. Genel olarak, filigran gömme ve çıkarma řleminin karmařıklığı düşük olmalıdır. Çünkü bazı uygulamalar için gerçek zamanlı damgalama metodu istenebilir.

Bu tez çalışmasında, dijital resimlerde telif haklarını korumak için yeni bir görünmez ve dayanıklı dijital renkli resim damgalama yöntemi önerilmiřtir. Önerilen yöntem blok kırpma kodlamasına ve ayrık dalgacık dönüşümüne dayalıdır. Resim damgalama řleminde, 24-bitlik renkli Bitmap formatında resim kullanılmaktadır. Resme damgalanan filigran, 1-bitlik siyah-beyaz Bitmap formatında resimdir. Resim damgalama algoritmasının dayanıklılıėını artırmak için resim damgalama řleminden önce, damgalanacak filigrana gizli bir anahtar kullanarak, permütasyon řlemi uygulanır. Seçilen gizli anahtar hem resme filigran damgalama řleminde hem de resimden filigran çıkarma řleminde kullanılır.

Önerilen damgalama yöntemini test etmek için, damgalanmıř resim, orijinal resim ve çıkarılmıř filigranların üzerlerinde, üç performans deėerlendirme ölçütü kullanılmıřtır. Ayrıca önerilen yöntemin dayanıklılıėını ispatlamak için, farklı türde saldırılar damgalanmıř resimlerin üzerinde denenmiřtir. Elde edilen sonuçlar, önerilen damgalama yönteminin, Joint Photographic Experts Group (JPEG) kayıplı sıkıřtırma, gürültü ekleme, filtreleme, histogram eřitleme, mozaik, gama düzeltme, kontrast ayarlama, ölçekleme, rastgele çizme, sahte filigran ekleme, filigran çarpıřtırma, morfolojik ve JPEG2000 kayıplı sıkıřtırma gibi řlemlere ve saldırılara karřı dayanıklı olduėunu göstermiřtir.

Tez düzeni genel hatlarıyla řu řekildedir: Veri gizleme yöntemleri, veri gizleme tarihçesi, terminolojisinin, dijital damgalama ve dijital damgalamanın türleri ve uygulamaları anlatıldığı ikinci bölümde, yöntemlerin arasındaki farklar ile uygulama alanlarına yer verilmiřtir. Üçüncü bölüm, ayrık dalgacık dönüşümün

teorinin geliştirme süresi, Haar ayrık dalgacık dönüşümü ve blok kırpma kodlaması ayrıntılı bir şekilde açıklanmıştır. Dördüncü bölümde, tezin oluşturulmasında kullanılan araçların tanıtıldığı “Materyal” ile geliştirilen damgalama algoritmasının ayrıntılı açıklamasına yer verildiği “Yöntem” bölümünü içermektedir. Yapılan testler ile çeşitli değerlendirmeler grafik, çizelge ve resim olarak “Araştırma Bulguları ve Tartışma” bölümünde yer almaktadır. Beşinci bölümde ise, bu çalışmadan elde edilen sonuçlar değerlendirilmiş ve gelecekteki çalışmalar için çeşitli önerilerde bulunulmuştur.

2. VERİ GİZLEME

2.1. Veri Gizlemenin Tarihçesi:

Gizli iletişim fikri çok eski bir iletişim yöntemidir. En erken ima gizli yazmaya Homer'in İlayda'sında görülmüştür [1,2]. Birkaç yüzyıldan sonra, steganografik yöntemler Herodotos tarafından, yazdığı çeşitli hikâyelerde görülmüştür. Steganografiyi tarif eden ilk dokümanlar Herodotos tarafından oluşturulmuştur. Herodotos bu tür faaliyetleri birkaç durumda vermiştir. Harpagus isimli bir adam yabani bir tavşan öldürmüştür ve mektubu tavşanın karnında saklamıştır. Sonra tavşanı habercisiyle göndermiştir. Haberciyi görenler avcı olduğunu sansınlar diye bu hileyi yapmıştır. Metler ve Farslara karşı devrimin başlangıç zamanını arkadaşlarına bildirmek için Histaieus, güvendiği kölelerinden birinin başının saçını tıraş ettirdi. Mektubu onun kafasına dövme şeklinde yaptırdı ve saç ı uzayıncaya kadar onu bekletti. Sonra, onunla birlikte saç kesim emri ile gönderdi ve böylece arkadaşları mektubu aldılar

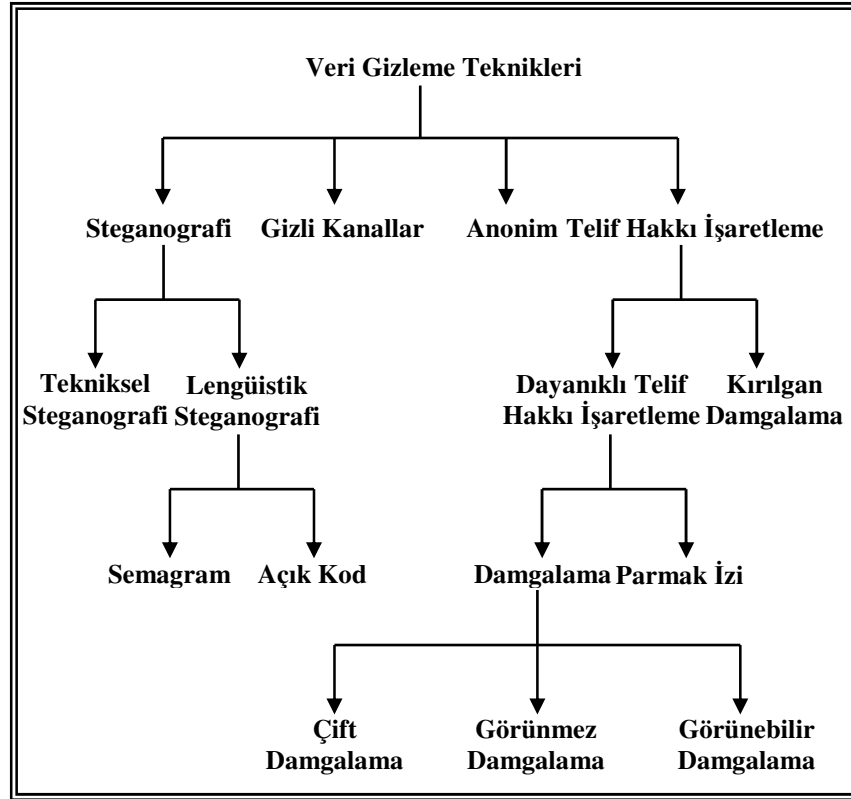
Hint Edebiyatı'ndan birkaç ünlü eser olan Kautilya's Arthasa'stra ve LalitaVista'ra ve Vatsa'yana's Ka'masu'tra'da gizli yazma (steganografi) kullanılmıştır. Ovid "Art of Love" 'ında görölmez yazı yazmak için süt kullanmayı önerir [1,3]. Bu konuda geçmişte kullanılan çok sayıda tekniğı rapor eden Æneas the Tactician, gizli mesajları taşıyan mektupların, kadınların küpelerinde saklanıp taşındığını bildirmiştir. Bildirilen diğeri bir yöntem ise, yollanan mektuptaki yazı karakterlerinin boyunu değıştirerek gizli mesajın kodlanması, mektubun üstüne ya da altına küçük delikler açarak gizli mesajın saklanmasıdır.

Sonradan bu yöntem, 17. yüzyılda Wilkins (1614–1672) tarafından geliştirilerek küçük delikler yerine görünmez mürekkep kullanılarak mikro noktalar ile işaretlenmiştir. Görünmez mürekkep yöntemi II. Dünya Savaşı'nın başlarında kullanılmıştır. Görünmez mürekkep ile masum gibi görünen mektupların satır aralarında farklı mesajlar taşınmıştır. Ayrıca şifrelenmemiş bir mektubun metni, gönderilecek mesajı gizlemek için bir ortam olarak kullanılmıştır. II. Dünya Savaşı'nda bir Alman ajanı tarafından gönderilen mektupta bu yöntem kullanılmıştır. Mesaj, mektubun şifrelenmemiş metni içinde gizlenmiştir. Normal cümle düzenindeki mektubun aşağıdaki metni, masum bir metin olarak görünmektedir:

Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Metnin sakladığı asıl bilgi, metindeki her kelimenin ikinci harflerinin birleştirilmesi ile ortaya “*Pershing sails from NY June 1*” olarak çıkar.

Steganografi terimi M.Ö 1500 yılında kullanılmaya başlanmıştır. O da Trithemius'in "Steganographia" konusunu içeren kitabında kullanılmasından sonradır. Linguistik steganografi diğer steganografi dallarından biridir. Bu steganografi dalı linguistik veya gizli yazma dil yapılarını içerir. Linguistik steganografinin iki türü Semagram ve Açık kod vardır. Semagram yazılı halde olmayan gizli bir mesajdır. Örneğin, insanlar harfler için müzik notalarını kullandılar. Ama bunlar hiç bir şekilde müziğe benzemez ve müzik hissini vermez. Açık kod yöntemi kodlu kelimeleri kullanır. Şekil 2.1.'de veri gizleme tekniklerinin dalları gösterilmektedir.

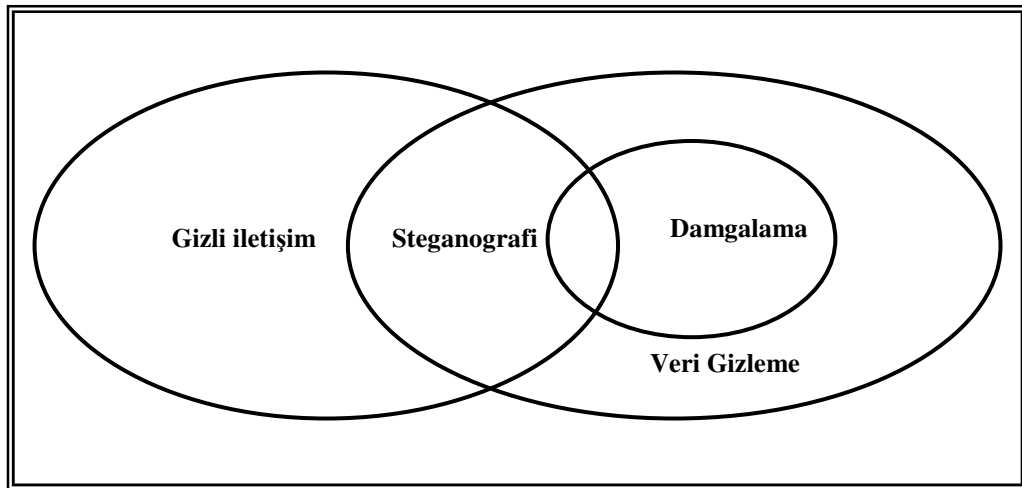


Şekil 2.1. Veri gizleme tekniklerinin dalları

Örneğin, Birinci Dünya Savaşı'nda, farklı türlerde İngiliz kruvazör savaş gemileri ve destroyerlerini temsil etmek için Alman casuslar sahte puro siparişlerini kullandılar. Böylece, Portsmouth'de 5000 puro ihtiyacı, beş kruvazörün Portsmouth'ta olduğu anlamına geliyordu.

Damgalama tekniği steganografiden evrilmiştir. Damgalamanın kullanılışı neredeyse kâğıt üretimi kadar eskidir. Eskiden yarı-dolu bulamaç gibi lifi ve suyu şebeke kalıplar üzerine boşaltarak lifi biriktirirlerdi. Sonra şekil ve tekdüzelik eklemek için bulamaç ile el kalıbının çerçeveleri kırılır ve son olarak, suyu ve yapışmış lifi çıkartmak için yüksek basınç uygulanırdı. Bu işlem 2000 yıldan beri pek fazla değişmedi. Damgalama bu işlemin ürünüdür. Kâğıt damgalama orta yüzyılların sonundan beri geniş bir şekilde kullanılmıştır. En erken kullanım olarak, ürün üzerine üretim patentini kayıt etmek için damgalama görünmüştür. Böylece stok estetiklerini ve kullanılabilirliğini alçaltmadan asılama belirli olarak kurulabilirdi. Son zamanlarda, kâğıt düzenini belgelendirmek için damgalama kullanılır.

Bu günlerde, çok gelişmiş ülkeler kendi kâğıtlarının, paralarının ve posta pullarının sahte üretimini zorlaştırmak için damgalamayı kullanırlar. Şekil 2.2.'de damgalama tekniği ile diğer veri gizleme teknikleri arasındaki ilişkiyi gösterilmektedir.

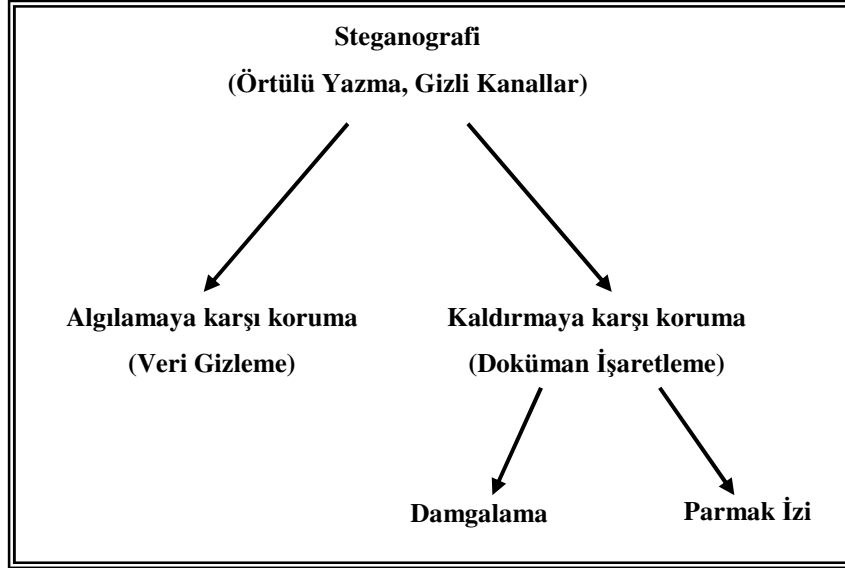


Şekil 2.2. Damgalama tekniği ile diğer veri gizleme tekniklerin arasındaki ilişkiler

2.2. Veri Gizleme Terminolojisi

2.2.1. Steganografi

Steganografi kelimesi Yunan örtülü yazma (στεγανω) kelimesinden gelir [1, 2, 3]. Mektubun zararsız olduğunu gösteren steganografi eski bir özel mektuplar gömme sanatıdır. Böylece üçüncü tarafın gizli mektubu algılamasını engeller. Başka bir deyişle, steganografi gizli kanallar kurma anlamına gelir. Gizli kanallar, bilgi aktarmak için kullanılan bir gizli iletişim kanalıdır. Şekil 2.3.'te gösterildiği gibi, steganografi iki genel türe ayrılır.



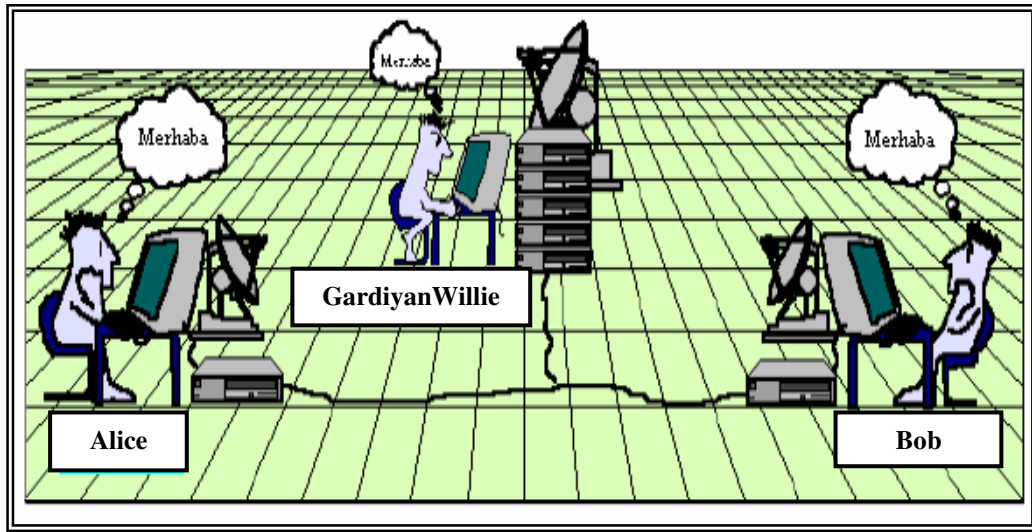
Şekil 2.3. Steganografi türleri

2.2.1.1. Algılamaya Karşı Koruma

Bu yaklaşım, Mahkûmlar Problem'i kullanılarak izah edilebilir [3, 4, 11]. Mahkûmlar Problem'i, 1983'te Simmons tarafından formüle edildi. Bu senaryoya dayalı, Alice ve Bob hapislanededirler ve bir kaçma planı hazırlamak isterler. Onların bütün iletişimleri gardiyan Willie 'den geçmektedir. Eğer Willie herhangi bir şifreli mektup veya şüpheli mektup algılsa, o zaman onların planlarını bozulacaktır. Ayrıca Alice ve Bob mektuplarında gizli mesajlarını saklamak

amacıyla, mektupların örtü metninde zararsız görünen bazı gizleme yöntemleri bulunmalıdır. Alice ve Bob'un kriptolojide olduğu gibi güvenliğin sadece kendisine bağlı olduğu o anahtarı paylaşmayı bir şekilde başardıklarını varsayalım.

Ayrıca, mahkumların ikisinin resim göndererek anlaştıklarını varsayılrsa, o zaman kullanılan genel model Alice'in resme ekstra oranda gürültü eklemesi ve resmin kalitesini etkilememesidir. Willie de aynı şeyleri yapabilir. Ama gürültü miktarı kısıtlıdır. Çünkü resimde alçaltma tanımlanmış. Değiştireceği bitleri seçmek için temel anahtarını kullanarak, Alice böylece bilgilerini nereye koyduğunu keşif etmeden Willie'yi durdurabilir. Ayrıca, eğer Willie resme ekstra gürültü eklemek isterse, o zaman gürültüyü resimdeki bütün mümkün yerlere eklemelidir ve böylece resim bozulur. Şekil 2.4.'te Mahkumlar Problem'i gösterilmektedir.



Şekil 2.4. Simmons'un tarafından formüle edilen Mahkumlar Problem'i

2.2.1.2. Kaldırmaya Karşı Koruma

Kaldırmaya karşı koruma yaklaşımı, doküman işaretleme için kullanılır. Yazar hakkında bilgi gömmek veya seri numara gömmek için bu metot kullanılır. Başka bir deyişle, telif hakkı bilgisi gömmek için kullanılır. Böyle durumlarda,

amaç kaldırmaya karşı korunmaktır. Damgalama metodu, damgalama okuyucu aracını kullanan kullanıcıya görünür ya da görünmez olabilir.

Bilgi gizlemenin iki ana dalı steganografi ve damgalamadır. Bu iki dal birçok ortak karakteristiklere sahiptir [22]. Ancak damgalama ve steganografinin birtakım yöntemlerde farklılıkları da olur. Örneğin; amaçta, tanımlamada ve algılama/çıkarma metodlarında. Çizelge 2.1.'de bu iki dalın arasındaki farklılıklar gösterilmektedir.

Çizelge 2.1. Steganografi ve damgalamanın arasındaki farklılıklar

	Gereksinimler	Damgalama		Steganografi
		Kişisel	Kamusal	
Amaç	Zihinsel Mülkiyet Haklarının Korunması	+ + + +		-
	Şüphe uyandırmadan gizli mesaj aktarımı	-		+ + + +
Tanımlama	Algısal görünmezlik	+ + + +		+ + + + +
	Statiksel veya algoritmik görünmezlik	+		+ + + + +
	Kaldırmaya, yok etmeye ve sahtesini yapmaya karşı dayanıklılık	+ + + + +		-
	Normal sinyal işlemeye karşı direnme	+ + + +		+
	Genel sıkıştırma kodlamasına dayanma yeteneği	+ + + +		+ +
	Yüksek yararlı yük miktarı	+ +		+ + + +
Algılama / Çıkarma	Taşıyıcı obje olmadan Algılama/çıkarma işlemi	-	+ + + +	+ + + +
	Sadece Taşıyıcı objeyi kullanarak Algılama/çıkarma işlemi	+ + + +	-	-
	Algılama/çıkarma işleminde düşük karmaşıklık ihtiyacı	+ +		+ + +
	İsteğe bağlı otomatik obje indirme yeteneği	+		+ +
Sembollerin Açıklamaları: Çok önemli: (+ + + + +) , Gerekli: (+ + + +) , Önemli : (+ + +) , İstenebilir: (+ +) , Faydalı : (+) , Önemli olmayan veya konu dışı : (-)				

2.2.2. Kriptoloji

Bir veri gizleme yöntemi olan kriptolojide, steganografi aksine bir örtü veri kullanılmaz. Gizlenmesi gereken verilerin, bir algoritma kullanarak şifrelenir ve şifrelenmiş veriler hiç örtü veri kullanılmadan gönderilir [1, 3]. Alıcı, aldığı verileri deşifre ederek orijinal verileri elde eder. Üçüncü kişiler, şifrelenmiş verileri elde etseler bile, deşifre algoritmasını bilmedikçe verilerin orijinaline elde edemezler.

2.2.3. Dijital Damgalama

Bilgisayarların ve bilgisayar ağlarının gelişmeye başlaması ile birlikte, güvenlik ve telif haklarının korunması amacıyla ortaya atılan dijital damgalama yöntemleri de steganografi uygulamalarına benzer. Ancak amaç bakımından dijital damgalamada, çalışma ile birlikte çalışmaya damgalanan bilginin taşınması da istenir. Bu nedenle bilgisayar ortamındaki çalışmalara telif hakkı, lisans, vb. bilgiler damgalanır. Damgalama yöntemlerinin geliştirilmesinde, dijital çalışmalara damgalanan bilginin çeşitli saldırılara karşı dayanıklı olması öncelikli amaç olarak göz önünde tutulur. Ancak steganografi uygulamalarında böyle bir beklenti yoktur.

2.2.4. Parmak İzi

Bazı yazarlar parmak izi tekniğini etiketleme olarak adlandırırlar [1]. Parmak izi, bir dijital çalışmanın belli bir müşteriye dağıtılma öncesinde, telif haklarının korunması amacıyla, yalnızca o müşteriye temsil eden bilginin çalışmaya görünmez bir şekilde damgalanması işlemidir. Etiketleme için kullanılan yöntemde bilgi, dışarıdan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her müşteriye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir. Parmak izi ekleme, amaç bakımından dijital damgalamadan farklı ancak yöntem olarak dijital damgalama ile aynı özellikler gösterir.

2.2.5. Dijital İmzalama

Dijital imzalama, bir doküman sahibinin kendi kişisel anahtarı ile dokümanı imzalaması yani şifrelemesidir [1]. Bu kişisel anahtardan üretilen kamusal anahtar dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır. Dijital imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Bir kişisel anahtar ile imzalanan doküman, sahibi hakkında bilgi de birlikte taşımış olur. Bazı otoritelerin, dijital damgalama ile dijital imzalamanın eş anlamlı olduğuna dair görüşlerine karşın bunları birbirinden ayrı tutan görüşler de vardır

Uygulamada dijital dokümanların imzalanması için çeşitli yazılımlar mevcuttur. Her kişi için oluşturulan kamusal ve kişisel imzalar, kendisine elektronik kartlarda verilir. Dijital imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır, göndericinin kişisel imzası kullanılarak şifrelendiğinden gönderici tarafından inkâr edilemez ve göndericinin imzası taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan üzerinde değişiklik yapamaz

2.3. Damgalama

700 yıl önce, İtalya’da kâğıdın markasını ve kâğıdı üreten fabrikayı bildirmek için damgalama kullanılmıştır. 18’inci yüzyılda, parayı ve diğer dokümanları taklit etmeye karşı bir ölçüt olarak damgalama kullanmaya başlanmıştır. Damgalama terimi 18’inci yüzyılın sonuna doğru ortaya atıldı [5]. Bu işleme böyle bir adın verilmesinin nedeni, muhtemelen damgaların etkisinin suyun kâğıt üzerindeki etkilerine benzetilmesidir.

Dijital damgalamaya benzeyen ilk örnek, 1954 yılında Emil Hembrooke’ın hazırladığı ve müzik çalışmalarını tanıtmak için kullandığı dosyalanmış patenttir. 1988’de, Komatsu ve Tominaga “dijital damgalama” terimini ilk kullanan kişiler olarak ortaya çıktılar.

1990'ların başlarında, dijital damgalama araştırma alanı yavaşça büyümeye başladı ve araştırma alanının bu şekilde büyümesi 1990'ların sonuna kadar devam etti. Ancak 2000 yılının başlangıcından bu yana, dijital damgalama araştırma alanına yönelik ilgide bir patlama yaşandı.

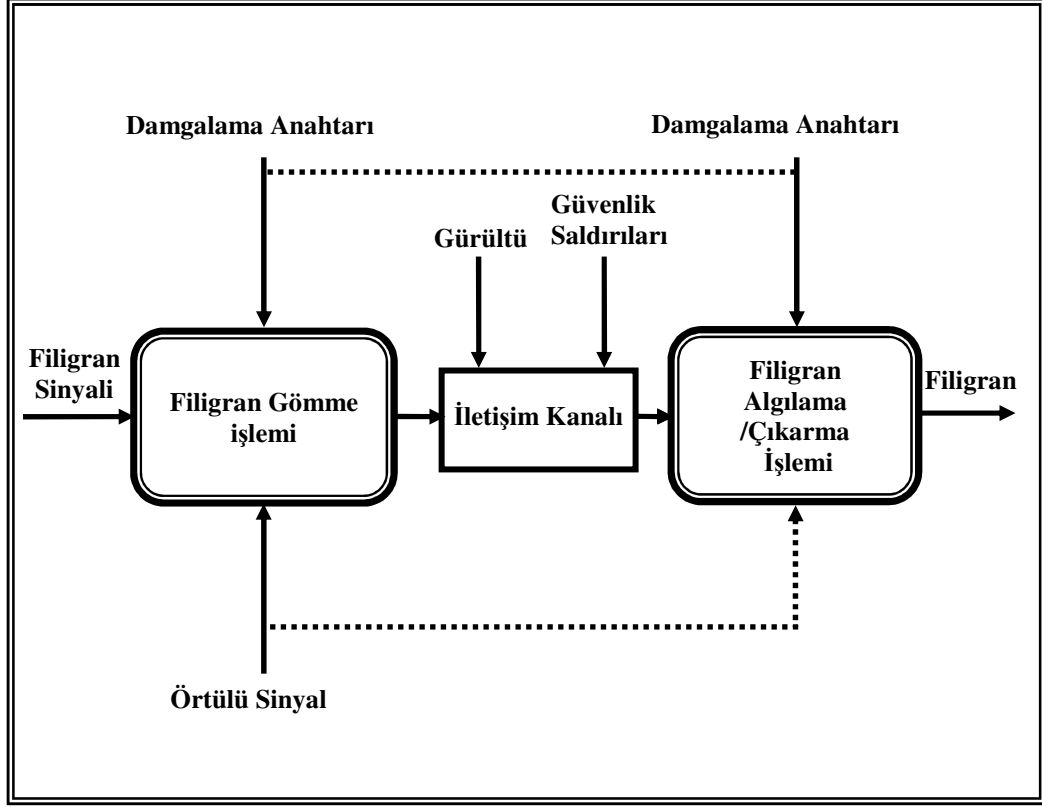
2.3.1. Dijital Damgalama Nedir

Telif hakkının korunmasını güçlendirmek için geliştirmekte olan metotlar dijital damgalamayı ortaya çıkardı. Dijital damgalama, gizli bir koddur. Bu gizli kod çoklu ortam verilerinin içinde gömülür ve sahibinin ve/veya içeriğinin verilerini doğrulamak için izin verir. Damgalama steganografi tekniğinin özel bir durumudur. Steganografi (resim, ses kayıtları ve hatta disklerdeki) kullanılmayan veya önemsiz veri alanlarından faydalanan bu alanları başka bir bilgi ile değiştirir [6].

Dijital damgalama fiziksel objelerin damgalamasına benzer[7]. Fakat kullanılan damgalama tekniği dijital içeriğin yerine fiziksel objelerdir. Dijital damgalamada düşük-enerjili bir sinyal fark edilmeyecek bir şekilde başka bir sinyalde gömülür. Düşük-enerji sinyaline filigran denilir ve bazı meta veriyi temsil eder (örneğin ana sinyalin hakkında ya güvenlik ya da mülkiyet hakları bilgileri). Filigranın gömüldüğü ana sinyale örtü sinyal denilir ve örtü sinyal filigranı örter. Örtü sinyal genel olarak dijital formatta resim, ses klipi, video veya metin dokümanıdır.

Dijital damgalama sistemi temel olarak filigranı gömme işlemi ve filigranı algılama işlemi içerir. Filigranı gömme işleminde filigranı örtü sinyal içine ekler ve filigran algılama işleminde filigranın sinyalin varlığını algılar. Şekil 2.5.'te damgalama sisteminin yapısı genel gösterilmektedir. Damgalama anahtarı hem Filigranı gömme işleminde ve filigran algılama işleminde kullanılır. Damgalama anahtarı ile damgalama sinyali birebir benzerliğe sahiptir (örneğin her damgalama sinyali için ayrı bir damgalama anahtarı vardır). Damgalama anahtarı özeldir ve sadece yetkili kişilere aittir ve sadece yetkili kişilerin damgalanan filigranı algılayabilmelerini sağlar. Ayrıca, iletişim kanalı gürültülü ve tehlikeli

olabilir. Yani dijital damgalama teknikleri hem gürültüye hem de güvenlik saldırılarına karşı esnek olmalıdır.



Şekil 2.5. Dijital damgalama sistemin genel yapısı

2.3.2. Dijital Damgalamanın Gereksinimleri

Dijital damgalama birtakım önemli karakteristikler kapsayabilir [5]. Bu karakteristikler; damgalanmış filigranın fark edilmesinin zor olması, farklı bozulma durumlarında damgalanmış filigranın kendisini koruması, kötü niyetli saldırılara direnmesi, çok sayıda bilgi bitleri taşıması, başka damgalarla birlikte bulunabilmesi ve filigranın çok az bir gömme veya algılama işlemi hesaplaması gerektirmesidir. Bu karakteristiklerin önemi uygulamaya dayalıdır. [5, 6, 7]'de bahsedilen dijital damgalama gereksinimleri gösterilmiştir.

2.3.2.1. Aslına Sadakat (Fark Edilmezlik)

Damgalanmış filigran ne izleyici tarafından fark edilebilir olmalıdır ne de içeriğin kalitesini düşürmelidir. Böyle durumlarda “Fark Edilmezlik” terimi kapsamlı olarak kullanılır. Ancak, eğer sinyal gerçekten fark edilemez özellikteyse, o zaman algıya dayalı kayıplı sıkıştırma algoritması, ya görünürlük eşiğini ortak olarak geçen daha fazla değişiklik sunar ya da böyle bir sinyali kaldırır.

2.3.2.2. Dayanıklılık

Uygulamaya dayanarak, dijital damgalama tekniği, damgalanmış içeriğe karşı değişikliklere yönelik farklı dayanıklılık seviyelerini destekleyebilir. Eğer dijital damgalama mülkiyeti tanımlamak için kullanılırsa, o zaman damgalanmış filigran olası değiştirmelere karşı dayanıklı olmalıdır. Damgalama filigranı kasıtsız veya kötü niyetli ve geometrik bozulmalar sonucu ne alçaltılmalı ne de yok edilmeli (örneğin analogtan dijitala çevirme, dijitalden analoga çevirme, kırpma, yeniden örnekleme, kırırtı, nicemleme, ölçekleme ve içeriği sıkıştırma).

Diğer taraftan, dijital damgalama içerik asılama için kullanılırsa, damgalama kırılmalı olmalıdır ki içeriğe yönelik herhangi bir değiştirmede damgalama filigranı yok olabilsin. Böylece içeriğe yönelik herhangi bir değiştirme müdahalesi algılanabilir.

2.3.2.3. Damgalamanın Yararlı Yüğü

Damgalamada saklanabilen bilgi miktarı kullanılan uygulamaya dayalıdır. Örneğin kopyalama koruma amaçları için kullanılan damgalamada, bir bitlik yararlı yük çoğunlukla yeterlidir.

ZM haklarının korunması için; bir kişinin, International Standard Book Numbering (ISBN) için kullanılaben benzer (kabaca 10 sayı) bir miktar bilgiyi gömmek istediğini farz etmek mantıklı görünüyor. Bunun başında, ayrıca telif hakkının tarihi, çalışma için verilmiş izinler ve iş için yapılan değerlendirmeler

yazılmalıdır. Bu, yaklaşık (60) veya (70) bit bilginin örtülü veride, resimde, video karesinde ya da işitsel bir parçacıkta gömülmesi gerektiği anlamına gelir [8].

2.3.2.4. Güvenlik

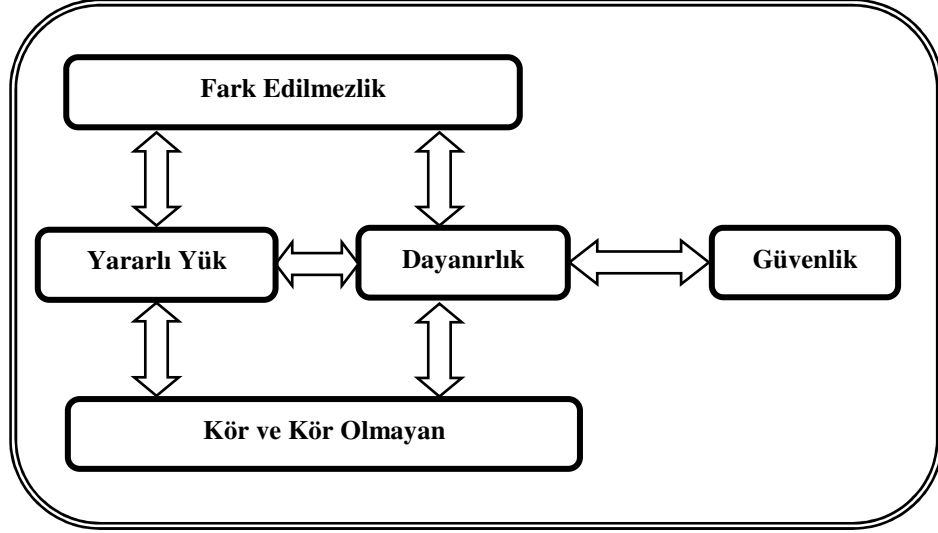
Damgalama tekniklerinin güvenliği şifreleme tekniklerin güvenliği ile aynı şekilde yorumlanabilir. Dolayısıyla; bir damgalama tekniği, ancak filigran gömme ve algılama işlemi için gerekli olan algoritmaları tam olarak bilmekle, damgalama filigranının yetkili olmayan bir gruba varlığını algılamada yardımcı olmaması veya onu kaldırması ile güvenlidir.

2.3.2.5. Kör ve Kör Olmayan Damgalama

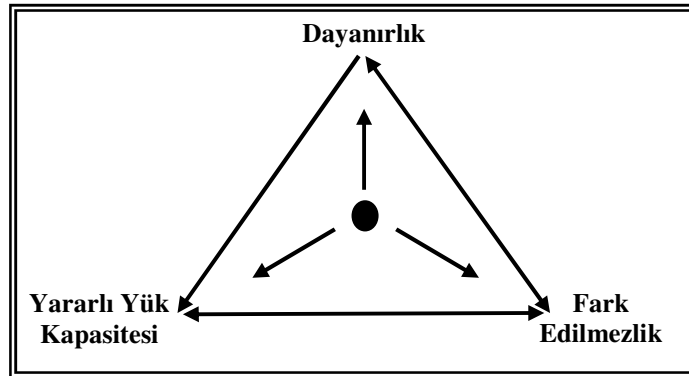
Bazı uygulamalarda, telif hakkı koruma ve veri gözetleme gibi, filigran çıkartma algoritmaları damgalanmış filigranı bulmak için damgalanmamış orijinal veriyi kullanabilir. Buna kör olmayan veya kişisel damgalama denir. Başka birçok uygulamada, kopyalama korunması ve indeksleme gibi, damgalama çıkartma algoritmalarının orijinal damgalanmamış veriye erişimi yoktur. Bu, filigran çıkartma algoritmasını daha zor hale getirir. Bu tür damgalama algoritmaları; kör veya kamusal algoritmaları olarak adlandırılır.

Şekil 2.6.'da dijital damgalamanın gereksinimleri arasındaki ortak ilişkiler gösterilmiştir. Yukarıda bahsedilen gereksinimlerin çoğu, ayrıntılı damgalama yöntemi sisteminin kalıtsal özelliklerine veya tasarımına dayalıdır [26]. Ancak fark edilmezlik, dayanırlık ve yararlı yük kapasitesi gereksinimleri, her damgalama sistemine uygulanabilen bir bedel oluşturmaktadır. Bu bedel, ayrıntılı damgalama sisteminde kurulabilen işlem türünü gösteren bir üçgen şeklinde temsil edilebilir. Şekil 2.7.'de gösterilmektedir. Örneğin, yüksek yararlı yük kapasiteli damgalama sistemi, yararlı yük kapasitesini artırmak için aynı zamanda sistemin dayanırlığını düşürür. Aynısı, aslına daha az sadık bir sistemin dayanırlık derecesine asla ulaşamayacak mükemmel biçimde görünmez olan bir başka damgalama sistemine uygulanabilir. Zihinsel Mülkiyet Haklarını

Damgalama Sistemleri'nin yüksek dayanırlık derecesine sahip olması istenirse, yararlı yük kapasitesi düşürülmelidir. Yayın gözetleme damgalama sistemi, yüksek yararlı yük kapasitesi gerektirirse, dayanırlık derecesi ve/veya fark edilmezlik göz önüne alınmaz.



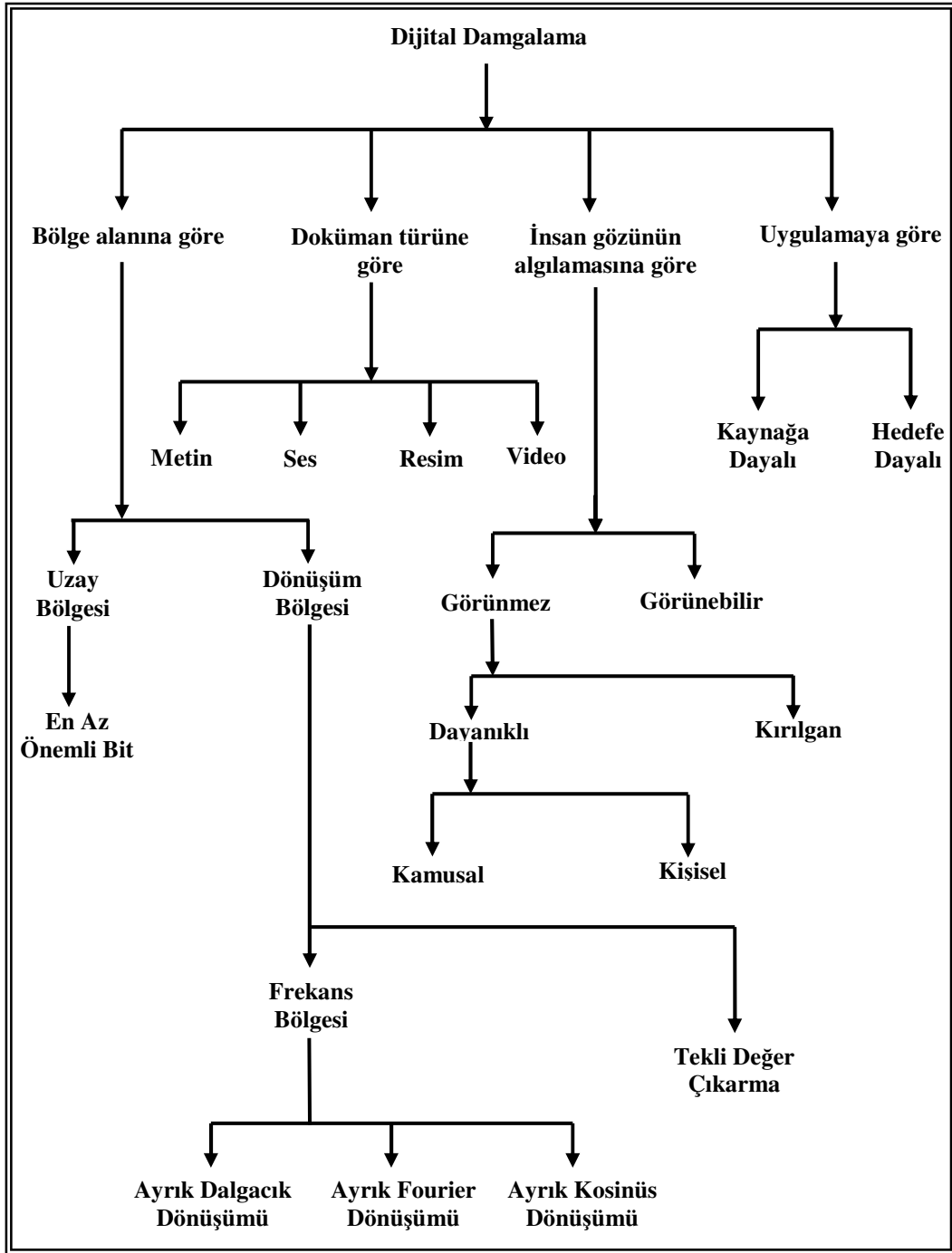
Şekil 2.6. Dijital damgalamanın gereksinimlerin arasındaki ortak ilişkiler



Şekil 2.7. Damgalama sisteminin temel gereksinimlerinin arasındaki bedel ilişkileri

2.3.3. Dijital Damgalama Türleri

Dijital damgalama teknikleri ve damgalama filigranları, farklı yollardan farklı kategorilere bölünebilir [1]. Şekil 2.8.'de farklı dijital damgalama tekniklerinin türleri gösterilmektedir.



Şekil 2.8. Dijital damgalamanın türleri

2.3.3.1. Uzamsal Bölge ve Dönüşüm Bölge Damgalaması

Damgalama, uzamsal bölgede uygulanabilir. Uzamsal bölge damgalamasında, damgalamak istenen filigranın bitleri, örtülü resmin en az önemli seçilen piksellerin bitlerinde kaydedilir ve damgalanır [10]. Uzamsal bölge

damgalamasında saklanabilen bilgi miktarı sınırlıdır. Bu yüzden bu damgalama yöntemi, saldırılara karşı çok zayıftır. Bütün saldırganlar, damgalanmış resimden filigran çıkarmak için damgalanmış resimdeki bütün en az öneme sahip piksellerin bitlerini yok etmeye çalışırlar. Uzamsal bölge damgalamasına alternatif bir damgalama türü ise dönüşüm bölge damgalamasıdır. Bu metodun fikri, resmi farklı frekans seviyelerine dönüştürecek bazı matematiksel fonksiyonlara tabi tutmaktır. Bu tür bir dönüşüme örnek, ayrık dalgacık dönüşümüdür. Dönüşüm bölge damgalaması metotları, uzamsal bölge damgalaması metotlarından daha dayanıklıdır [1].

2.3.3.2. Görünebilir ve Görünmez Damgalama

Görünebilir filigranlar; görsel dijital içerik içine, içeriğe bakıldığı zaman görülebilecek biçimde gömülen filigranlardır. Görünmez filigranlar fark edilmezlerdir ve sadece dijital içeriğe bakarak algılanamazlar.

2.3.3.3. Dayanıklı ve Kırılğan Damgalama:

Dayanıklı damgalama tekniğinde damgalanmış içeriğe değiştirmeler yapılsa bile, damgalanmış filigran etkilenmez. Bunun tam tersine; kırılğan damgalamada, damgalanmış filigranın içeriği değiştirilir veya kurcalanırsa, damgalanmış filigran yok olur.

2.3.3.4. Kamusal ve Kişisel Damgalama:

Kamusal damgalamada, damgalanmış filigranı algılamak için, damgalanmamış içeriğe gerek yoktur [1,7]. Kamusal damgalama ve kör damgalama aynı anlamdadır [9]. Ayrıca, damgalanmış içerik kullanıcılarının filigran algılama işlem yetkileri vardır. Ama kişisel damgalamada, her kullanıcının filigran algılama işlem yetkisi yoktur. Ayrıca damgalanmış filigranı algılamak için, damgalanmamış filigrana veya orijinal içeriğe gerek vardır. Kişisel damgalama ve kör olmayan damgalama da aynı anlamdadır [9].

2.3.3.5. Kaynağa Dayalı ve Hedefe Dayalı Damgalama:

Kaynağa dayalı damgalama, dağıtılmakta olan bütün orijinal kopyalara verilen eşsiz mülkiyet filigranını tanımlamak veya asılamak için kullanılan bir damgalama türüdür [1]. Hedefe dayalı damgalamada, her dağıtılmış orijinal kopya, eşsiz filigran ile damgalanır ve bu filigran müşteriyi tanımlamak için kullanılır. Yasa dışı tekrardan satış durumlarında, hedefe dayalı damgalama müşteriyi takip edebilir.

2.3.4. Dijital Damgalama Uygulamaları:

Dijital damgalama tekniklerinin farklı ve geniş alanlı uygulamaları vardır. Ayrıca, dijital damgalama uygulamalarının birtakım farklı senaryoları da vardır. Bu uygulamaların senaryoları farklı yöntemlerle sınıflandırılabilir. Sınıflandırma, damgalanmış filigranın taşıdığı bilgi türüne dayalıdır. Çizelge 2.2.'de damgalama uygulamalarının sınıflandırılması gösterilmektedir.

Çizelge 2.2. Dijital damgalama uygulamalarının sınıflandırılması

Uygulama Sınıfı	Damgalanmış filigranın amacı	Uygulama Senaryosu
Zihinsel Mülkiyet Haklarını Koruma	Taşıdığı bilgiler içerik sahibi ve zihinsel mülkiyet hakları hakkındadır.	-Telif hakkı koruma. -Kopyalamayı koruma. -Parmak izi.
İçerik Asılama	Orijinal çoklu ortam içeriğinin değiştirilmediğini garanti eder ve/veya değiştirilmiş bilgilerin türünü ve yerini belirlemeye yardımcı olur.	-Asılama. -İçeriğin bütünlüğünü kontrol etme.
Bilgi Gizleme	Ek bilgi taşımak için kullanılan yan-kanalı temsil eder.	-Yayın Gözetleme. -Sistem Artırma.

2.3.4.1. Telif Hakkı Koruma

Dijital damgalama telif hakkı tanımlamada ve korunmada kullanabilir. Zihinsel mülkü korumak için, veri sahibi verilerine telif hakkı bilgilerini temsil eden bir filigran gömebilir [8]. Birisi onun telif hakkını ihlal ettiği zaman, damgalanmış filigran kendi mülkiyetini mahkemelerde ispatlayabilir.

2.3.4.2. Parmak İzi

Yasal olmayan kopyaların kaynağını takip etmek için, mülkiyet sahibi parmak izi tekniğini kullanabilir. Bu durumda, farklı müşterilere dağıtılmak istenen verilerin kopyalarına, mülkiyet sahibi farklı filigranlar gömebilir. Parmak izi metodunda, kopya verilerin içine, müşteriye ait olan tanımlama seri numarası gömülebilir. Parmak izi metodu, lisans anlaşmalarının bilgilerini kıran ve üçüncü kişilere veren müşterileri, mülkiyet sahibinin zihinsel haklarını tespit etmeyi sağlar [8,11].

2.3.4.3. Veri Asılama

Kırılğan damgalar, verilerin asılmasını kontrol etmek için kullanılabilir [8]. Kırılğan damga, verilerin değişip değişmediğini gösterir. Ayrıca değiştirilen verilerin hakkında, verilerin neresinde değişme olduğu gibi, lokalizasyon bilgileri sunar.

2.3.4.4. Tıbbi Bilgilerin Güvenliği

Tıbbi resimlerde hastanın adı ve tarihini gömmek, faydalı bir güvenlik ölçüsü olabilir.

2.3.4.5. Bilgi Gizleme

Damgalama teknikleri, gizli kişisel mesajlar aktarmak için kullanılabilir. Bazı devletlerin hükümetleri şifreleme hizmetlerinin kullanılmasını yasaklıyor. Bu yüzden, insanlar mesajlarını başka verilerde gizleyebilirler.

2.3.4.6. Kopyalama Koruması

Damgalamada kaydolan bilgiler, kopyalama koruma amaçları için direkt dijital kaydedici cihazları kontrol edebilir. Bu durumlarda, damgalanmış filigran yasaklama kopya bitini temsil eder ve kaydedici cihazdaki damgalanmış filigran algılayıcı, kaydedici cihaza sunulan verilerin kaydolup olmadığını tespit eder.

2.3.4.7. Yayın Gözetleme

Damgalama, yayın içeriğinin izlenmesi için kullanılabilir (örneğin televizyon ve yayınlanmış radyo sinyalleri). Yayına hazırlanan her video veya ses klip içine eşsiz filigran koyulur. Bundan sonra, otomatik izleme istasyonları yayını alır ve o filigranları arar, her klip yayınlandığı zaman filigran tanımlaması yapılır [11].

3. DALGACIK DÖNÜŞÜMÜ VE BLOK KIRPMA KODLAMASI

3.1. Giriş

Dalgacık dönüşümü, matematiksel bir işlemdir. x Bölgesinde olan f sinyali veya fonksiyonu, bir $u : F \rightarrow f$ dönüşümü ile F bölgesinde başka bir sinyal veya fonksiyona dönüştürülür. f Fonksiyonu, önce u dönüşümü ile F alanına dönüştürülür ve bu alan içerisinde gerekli kodlama işlemleri yapıldıktan sonra, u dönüşümünün ters dönüşümü kullanılarak sinyal tekrar f alanına geri dönüştürülür.

Dalgacık teorisinin tarihsel gelişimi, 20. yüzyılın başlarında Macaristanlı matematikçi Alfred Haar'ın çalışmalarıyla başlamıştır. 1975'te *Sürekli Dalgacık Dönüşümü'nü* (SDD) keşfeden Zweig; 1982'de SDD'yi formüle eden Pierre Goupillaud, Grossmann ve Morlet; 1983'te *Ayrık Dalgacıklar* üzerinde çalışan Jan-Olov Strömberg; 1988'de *Dik Dalgacıklar* üzerinde çalışan Daubechies; 1989'da çoklu çözünürlük çerçevesiyle Mallat; 1991'de SDD'nin zaman-frekans çeviricisiyle Nathalie Delprat; 1993'te *Harmonik Dalgacık Dönüşümü* ile Newland dalgacık teorisine dikkate değer katkılarda bulunmuşlardır [13].

Dalgacık, bir matematiksel fonksiyon türüdür. Dalgacık fonksiyonu, verilen fonksiyonu veya sürekli zaman sinyalini, farklı frekans bileşenlerine böler ve her bileşeni kendi ölçeğine uygun çözünürlükle okumayı sağlar. Dalgacık dönüşümü dalgacıklar fonksiyonu ile temsil edilir. Dalgacıklar, sonlu-uzunluklu kız kardeş dalgacıklar olarak bilinen ölçeklenmiş ve ötelenmiş kopyalardır veya hızlı-yok olan salınma ana dalgacığı olarak bilinen dalga biçimidir. Dalgacık Dönüşümü, duraklamaları ve keskin dorukları olan fonksiyonların temsilinde ve doğru bir şekilde analiz ve tekrar kurulmalarında sonlu, periyodik olmayan ve/veya durağan olmayan sinyallerde, *Fourier Dönüşümü*'nden daha üstün avantajlara sahiptir [13].

Dalgacık Dönüşümü, *Ayrık Dalgacık Dönüşümü* (ADD) ve *Sürekli Dalgacık Dönüşümü* (SDD) olarak sınıflandırılır. Hem ADD hem de SDD sürekli-zaman (analog) dönüşümleridir. Bunlar sürekli-zaman sinyallerini temsil etmek için kullanılabilirler. SDD muhtemel olan her ölçeklenmiş ve ötelenmiş değerlerin

üzerinde çalışır. Ancak ADD, belirli ölçeklenmiş ve ötelenmiş değerlerin altkümesi veya grid gösterimi olarak kullanılır.

3.2. Ayrık Dalgacık Dönüşümü

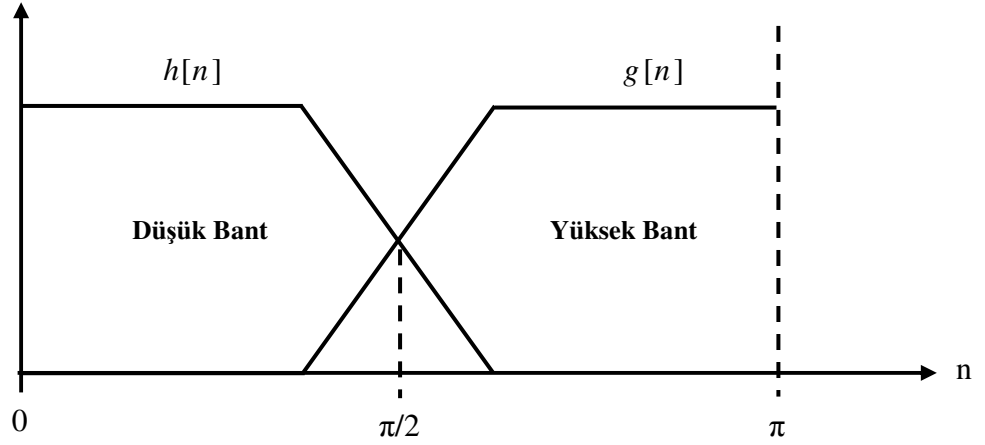
ADD'nin temel fikri, tek boyutlu sinyaller üzerine uygulandığında daha kolay anlaşılabilir [14,15]. ADD, verilen sinyali iki alt-banda böler ve bunlar genellikle *yüksek frekans* ve *düşük frekans* alt-bantlarıdır. Bu bölme işlemine *ayrıştırma* denilir. Sinyalin kenar bileşenleri, büyük ölçüde yüksek frekans alt-bandına ayrıştırılır. Sinyalin yüksek ve düşük frekans alt-bantlarına ayrıştırılması için sinyal sırasıyla bir dizi *yüksek-geçiren (YGF)* ve *düşük-geçiren(DGF)* filtrelerden geçirilir. Sinyalin farklı çözünürlükler üzerinde analiz edilmesi için farklı kesik frekans filtreleri kullanılır.

Orijinal $x[n]$ sinyali yüksek-geçiren $g[n]$ ve düşük-geçiren $h[n]$ filtrelerinden geçirilir ve iki ile aşağı örneklenir. Aşağı örnekleme sonunda alt-sinyallerin örnek sayıları yarıya düşer. Böylece, sinyalin en yüksek frekans bandı $\pi/2$ olur. Şekil 3.1.'de $x[n]$ sinyalinin spektrum ayrışım işleminin sonucu gösterilmektedir. Bu işlem birinci seviyeli ayrıştırmayı oluşturur ve elde edilen yüksek-geçiren sinyalle düşük-geçiren sinyaller matematiksel olarak sırasıyla şu şekilde ifade edilebilirler:

$$Y_{Yüksek}[n] = \sum_k x[k] g[2n - k] \quad (3.1)$$

$$Y_{Düşük}[n] = \sum_k x[k] h[2n - k] \quad (3.2)$$

Sinyal üzerinde birden fazla ayrıştırma yapılmak istenirse, yukarıdaki işlem alt-sinyaller üzerinde tekrarlanır. Yüksek-geçiren filtre ve düşük-geçiren filtrenin çıktılarına, *ADD katsayıları* denir ve bu ADD katsayıları kullanılarak orijinal sinyal yeniden geri çatılabilir. Yeniden geri çatma işlemine *Ters Ayrık Dalgacık Dönüşümü (TADD)* denir.



Şekil 3.1. Filtreleme işleminden sonra sinyalin spektrum ayrışımı

TADD işlemi, sinyali geri çatmak için ters bir sırada çalışır. Sinyaller her seviyede iki ile yukarı örneklenir ve yüksek-geçiren $g'[n]$ ve düşük-geçiren $h'[n]$ sentez filtrelerinden geçirilir ve sonra elde edilen her iki sinyal toplanır. Analiz ve sentez filtreleri birbirleriyle uyumlu bir *filtre bankası* oluştururlar. Bundan dolayı, her katman için geri çatma formülü şu şekilde olur:

$$x[n] = \sum_{k=-\infty}^{\infty} (Y_{Düşük}[k] h[2n-k] + Y_{Yüksek}[k] g[2n-k]) \quad (3.3)$$

Filtre bankasını oluşturan $h[n]$ ve $g[n]$ filtrelerinin Fourier dönüşümleri olan $H(\omega)$ ve $G(\omega)$ fonksiyonları, dikgenlik koşulunu sağlamalıdır:

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \quad (3.4)$$

3.2.1.1. Haar Ayrık Dalgacık Dönüşümü

Dalgacık dönüşümünün nasıl çalıştığı basit bir örnekle açıklanabilir. $x[n]$, tek boyutlu bir resim ve piksel değerleri sırasıyla (9, 7, 5, 3) olsun. Resmi

temsil etmek için resmin dalgacık dönüşümü hesaplanır ve Haar dalgacık tabanı kullanılabilir. Bu işlem için her iki komşu pikselin ortalaması alınır ve her bir ortalama sonucu, bir piksel değerini temsil eder. İki ile aşağı örnekleme sonunda elde edilen düşük çözünürlüklü resmin piksel değerleri (8, 4) olur. Bu ortalama işleminde resmin bazı bilgileri kaybolur.

Resmin yüksek-geçiren filtreden geçirilmesi, komşu piksellerin değerlerinin birbirinden çıkartılıp ikiye bölünmesiyle olur. Elde edilen resmin iki ile aşağı örneklenmesi ile oluşan resmin piksel değerleri (1, -1) bulunur.

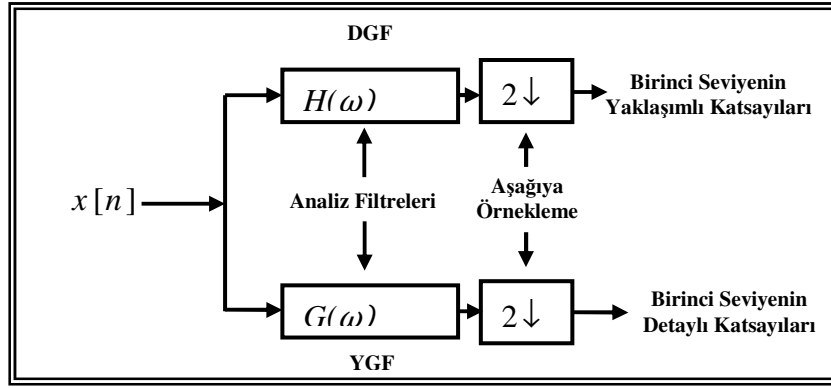
Orijinal resmin geri çatılması için düşük çözünürlüklü resim ve ikinci aşamada bulunan detay katsayıları kullanılır. Bu örnekte, $(8+1, 8-1, 4+1, 4-1) = (9, 7, 5, 3)$ hesaplamasıyla orijinal resim elde edilebilir.

Ayrıştırma işleminin elde edilen resimler üzerinde tekrarlanması sonucunda tam ayrıştırma olur. Çizelge 3.1.'de $x[n]$ tek boyutlu resmin ve bu resmin düşük çözünürlüklü sürümlerinin ayrıştırma işlemi sonunda elde edilen frekansların katsayıları gösterilmektedir.

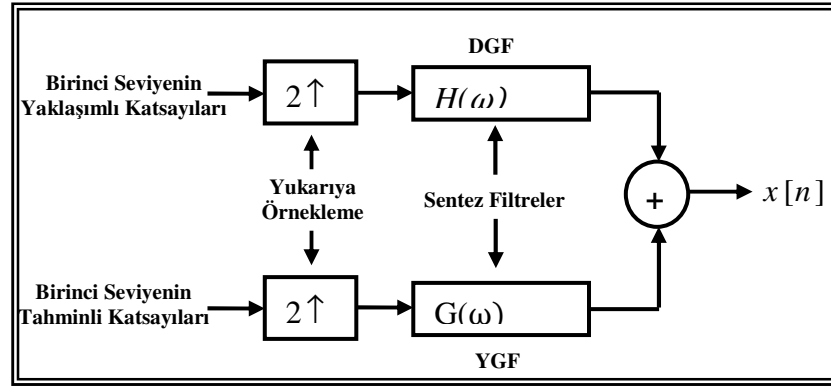
Çizelge 3.1. $x[n]$ Örnek sinyalinin ayrıştırma işlemi üzerine uygulandıktan sonra, frekansların katsayıları ve çözünürlük değerleri

Çözünürlük	Ortalama	Detaylı Katsayıları
4	(9, 7, 5, 3)	-
2	(8,4)	(1 -1)
1	6	2

Böylece, tek-boyutlu Haar tabanı için, orijinal dört pikseli resmin dalgacık dönüşümü $(6 \ 2 \ 1 \ -1)$ şeklinde elde edilir. Ortalama katsayıları ve çıkarma katsayılarını tekrarlı bir şekilde hesap eden dalgacık dönüşümüne filtre bankası denir. Tek-boyutlu sinyalin Haar ADD ayrıştırma ve Haar TADD geri çatma işlemleri şekil 3.2.'de gösterilmiştir.



(a)



(b)

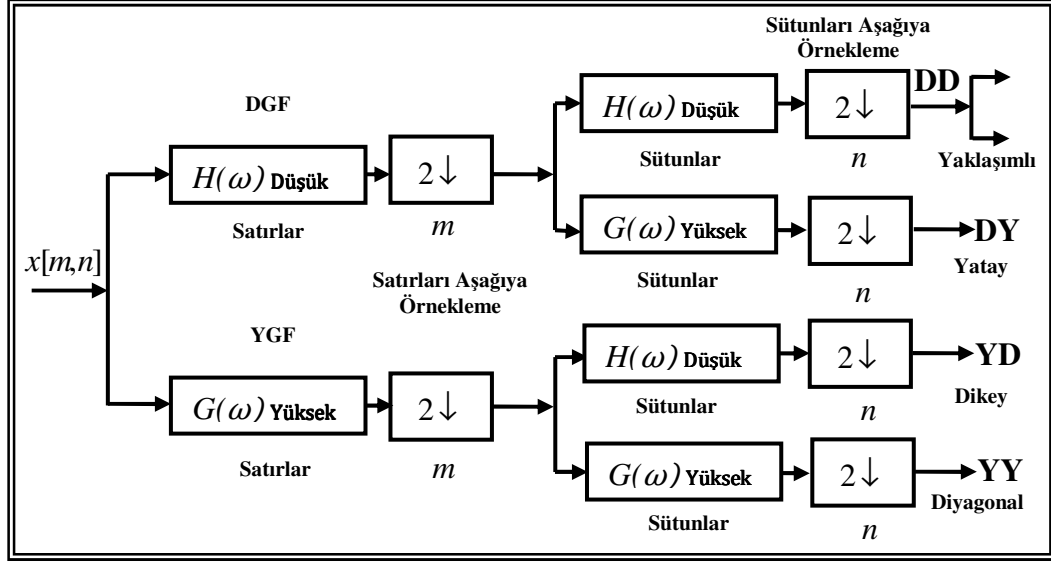
Şekil 3.2. $x[n]$ tek-boyutlu sinyali üzerinde ADD'nin uygulanması, (a) sinyalin üzerine ADD ayrıştırma işlemi, (b) sinyali geri çatma işlemi

3.2.1.2. Haar ADD'nin Dijital Resimler Üzerine Uygulanması

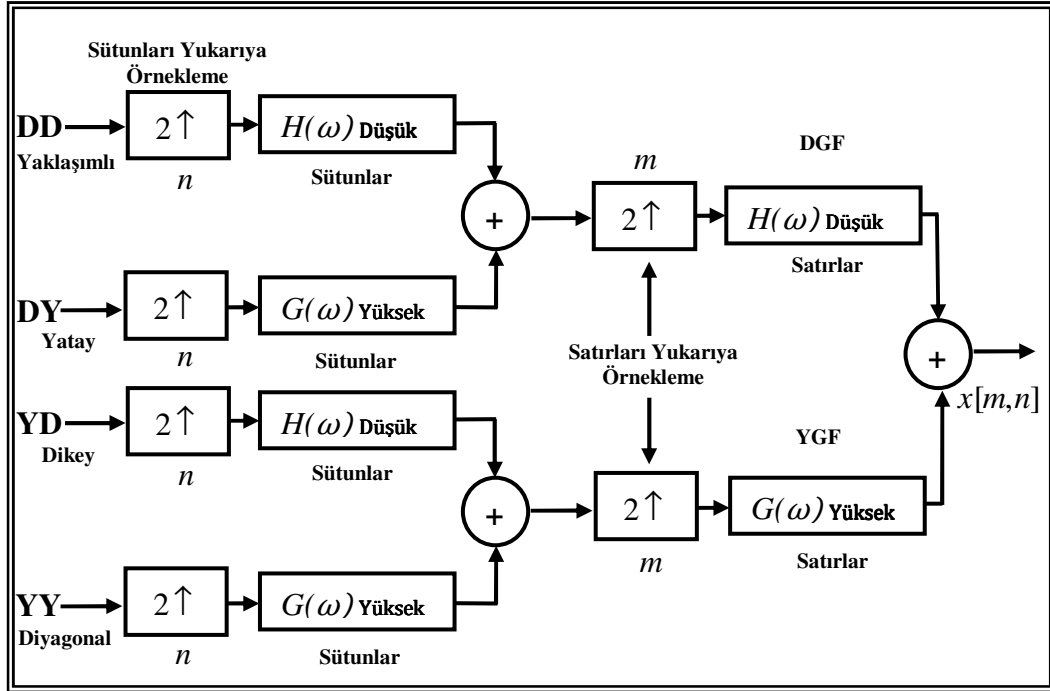
İki boyutlu bir resmin ADD'si, tek boyutlu dönüşümler kullanılarak hesaplanır. Bunun için dönüşüm önce tüm satırlar üzerinde ayrı ayrı uygulanır, arkasından aynı işlem bu sefer sütunlar üzerinde yapılır. Bu işlem dört kanallı geri çatma filtre bankasıyla temsil edilir. Yüksek-geçiren ve düşük-geçiren filtrelerin yukarıda belirtilen şekilde kullanılmasıyla resmin yatay bileşenleri dikey bileşenlerinden ayrıştırılır ve sonuçta resmin *Düşük-Düşük (DD)* frekans alt-bantlı yaklaşımının yanında her çözünürlük için üç detaylı resim daha elde edilir:

- ❖ *Düşük-Yüksek* frekans alt-bantlı resim (DY).
- ❖ *Yüksek-Düşük* frekans alt-bantlı resim (YD).
- ❖ *Yüksek-Yüksek* frekans alt-bantlı resim (YY).

Bu işlemler (DD) alt-bandı üzerinde tekrarlanarak özdeşlikli filtre bankasının ikinci aşaması kullanılır. Şekil 3.4.'te Haar ADD birinci aşamasının resim üzerine uygulanması ve onun TADD'si gösterilmektedir.



(a)



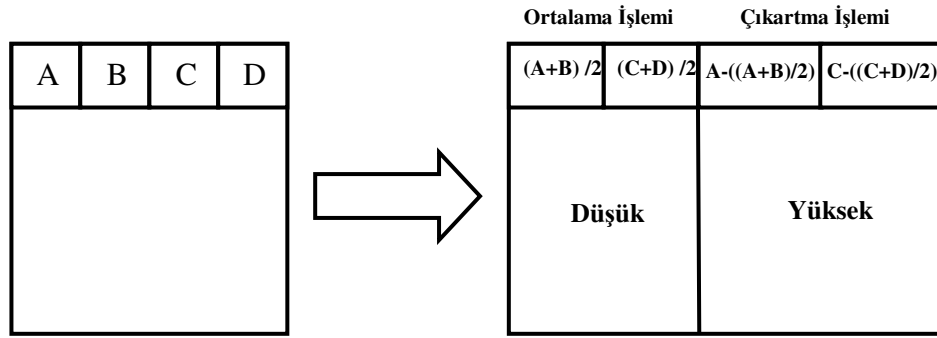
(b)

Şekil 3.4. Resmin üzerine ADD işleminin uygulanması, (a) resmin üzerine ADD ayrıştırma işlemi, (b) resmi geri çatma işlemi

3.2.1.3. Haar ADD Algoritması

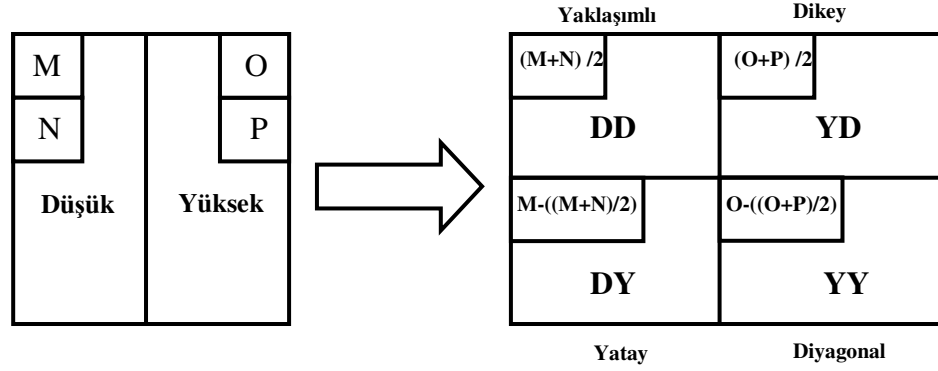
Resmin Haar ADD'sini hesaplamak için şu adımlar resmin üzerine uygulanmalıdır [16]:

İlk Adım: Yatay yönde resmin pikselleri soldan sağa taranır. Sonra, her iki komşu pikselin üzerine ortalama ve çıkartma işlemi uygulanır. Ortalama işleminin sonucu Şekil 3.5.'te gösterildiği gibi tablonun sol tarafına kaydedilirken, çıkarma işleminin sonucu sağ tarafa kaydedilir. Bu işlem resmin bütün satırları üzerinde uygulanır. Piksellerin ortalama değerleri, düşük frekansların katsayılarının alt-bandını temsil eder ve piksellerin çıkartma sonuçları yüksek frekansların katsayılarının alt-bandını temsil eder. Şekil 3.5.'te yatay işleminin resmin birinci satırı üzerine uygulanması gösterilmektedir.



Şekil 3.5. Yatay işleminin resmin birinci satırı üzerine uygulanması

İkinci Adım: Resmin pikselleri dikey yönde yukarıdan aşağıya taranır. Sonra her iki komşu pikselin üzerine ortalama ve çıkartma işlemi uygulanır. Ortalama işleminin sonucu yukarıda kaydedilir ve çıkartma işleminin sonucu aşağıda kaydedilir. Bu işlem resmin bütün sütunları üzerinde uygulanır. Son olarak (DD, DY, YD, YY) sırasıyla, dört alt-bantlı resim elde edilir. (DD) alt-bantlı resim, orijinal resme çok benzer. Şekil 3.6.'da dikey işlemin sütunlar üzerine uygulanması gösterilmektedir. Şekil 3.7.'de Lena resmi üzerinde Haar ADD'nin birinci ve ikinci seviye ayrıştırma işlemi gösterilmektedir.



Şekil 3.6. Dikey işleminin resmin sütunları üzerine uygulanması

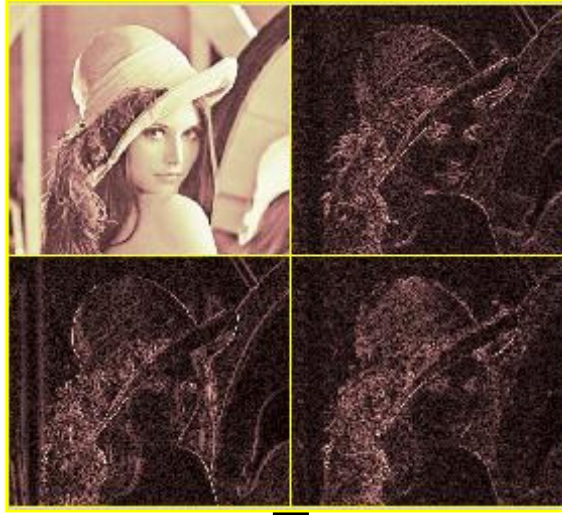
3.2.2. ADD'nin Karakteristikleri:

Dalgacık ayrışımı resmi üç yönlü –yatay, dikey ve diyagonal– uzamsala ayrıştırır. Bundan dolayı, dalgacıklar insan görsel sisteminin (İGS) yön bağımlı özelliklerini çok dikkatli bir şekilde yansıtır [20]. Çoklu çözünürlük özeliğinden dolayı, ölçeklenebilirlik ve alçaltmaya dayanıklılık gerektiren uygulamalar için uygun olur. Bu yüzden, resimlerin aşamalı iletimine izin verir. Yüksek çözünürlük alt-bantları, resmin içindeki kenar ve doku örüntülerinin kolay bir şekilde bulunmalarını sağlar.

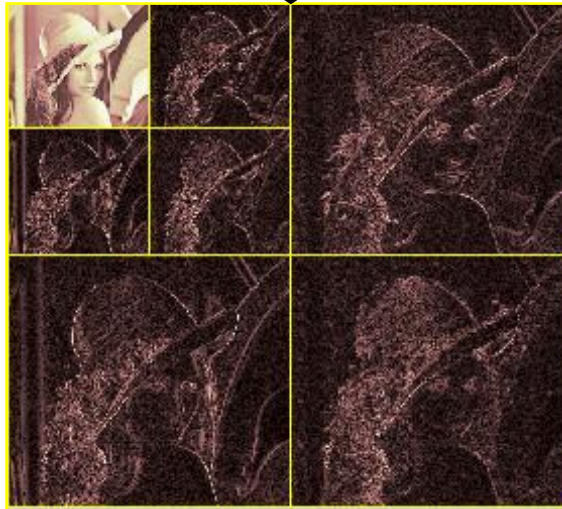
Dalgacık dönüşümü hesaplama yönünden etkindir ve basit evrişim filtresi kullanılarak uygulanabilir. Ayrıca dayanıklılık yönünden, iletime ve kod çözme hatalarına karşı daha dayanıklıdır. Her ayrıştırma seviyesindeki düşük (DD) alt-bantların ADD genlik katsayıları daha büyük olur. ADD'nin genlik katsayıları diğer (DY, YD, YY) alt-bantlarda daha küçük olur. ADD'nin hesaplama karmaşıklığı doğrusaldır. Yani ADD algoritması $O(n)$ zamanda çalışır [12]. ADD resmin hem uzamsal hem de frekans bilgilerini içerir.



Birinci seviyeli Haar ADD



İkinci seviyeli Haar ADD



Şekil 3.7. Lena resmi üzerinde Haar ADD birinci ve ikinci seviye ayrıştırma işlemi

3.3. Blok Kırpma Kodlaması

Blok Kırpma Kodlaması (BKK), moment koruma nicemlemesine dayalı bir bloğa uyarlanabilen ikili kodlayıcı bir şemadır. BKK algoritması resmin uzamsal bölgesinin (resmin pikselleri) üzerinde uygulanır. BKK'nın temel kavramı, 17 Mart 1979 tarihinde Purdue Üniversitesi'nde O.Robert Mitchell ve Edward J. Delp tarafından ortaya atıldı [18, 19, 20]. BKK üzerine ilk çalışmalar, 1978 ve 1979 yıllarında IEEE Uluslararası İletişim Konferansı'nda ortaya çıktı. 1987 yılında BKK, JPEG sıkıştırma standardı için kesin aday oldu.

Temel BKK algoritması sabit uzunluklu kayıplı bir sıkıştırma metodudur. Bu algoritma, resmin yerel alanını nicemlemek için Q seviyeli bir nicemleyici kullanır. Nicemleyici seviyeleri, nicemlenmiş çıktıda muhafaza edilen resimdeki yerel alanın momentlerinin sayısı kadar seçilir. BKK algoritması en basit şekliyle, gri seviyeli resmin standart sapmasını ve ortalamasını korumayı hedefler. Yüksek dereceli momentleri korumak için BKK algoritmasına ek kısıtlamalar eklenebilir. Bu yüzden BKK algoritması, uyarlanabilen bir korunmuş moment blok nicemleyicidir [18].

3.3.1. BKK Temel Algoritması

BKK algoritmasının birinci adımı, resmi çakışmayan dikdörtgen biçiminde bloklara bölmektir. Resmin blok bölme işleminin daha kolay bir şekilde yapılması için bloklar ($n \times n$) boyutlarında karelere bölünür. Genellikle n değeri 4 veya 8 seçilir [20]. İki seviyeli (1 bit eşlemi) nicemleyiciyi elde etmek için temel fikir, bloktaki her pikseli temsil edecek iki parlaklık değeri seçmektir. Bu değerler, geri çatılan bloğun gri seviyeli ortalaması ve standart sapması, orijinal bloğun değerleri ile aynı olacak biçimde seçilir.

Bundan sonra bir $n \times n$ bit eşlemi, piksel parlaklık değerinin, belirlenmiş eşik değerinin üstünde mi yoksa altında mı olduğunu belirlemek için kullanılır. BKK algoritması bloğu temsil edecek bir bit eşlemi ürettiği için, *ikili örüntü resim kodlama metodu* olarak sınıflandırılır [18]. BKK eşikleşme işlemi; insan görsel sisteminin yerel uzamsal bütünleşmesini ve maske hataları üzerinde uygulanma

yeteneği avantajını kullanarak, yeniden yüksek aslına sadakatli bir keskin kenar üretme imkânı sağlar. Resim üzerine BKK algoritmasının uygulanması şu adımlarla yapılır [18, 20, 21]:

Adım 1: Orijinal resim çakışmayan bloklara bölünür. Bloğun boyutu ya 4×4 ya da 8×8 olabilir. Her bloğun gri seviyeli ortalamasını hesaplamak için aşağıdaki denklem kullanılır:

$$M = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n x(i, j) \quad (3.5)$$

Burada $x(i, j)$ bloğun piksellerini, n ise seçilen blok boyutunu temsil etmektedir.

Adım 2: Bloktaki resmin pikselleri, piksellerin gri seviyelerinin bloğun gri seviyeli ortalamasından daha büyük oluşlarına göre, iki sınıfa ayrılır. Bu iki tür pikselin gri seviyeli ortalamaları şöyle hesaplanır:

$$ML = \frac{1}{k} \sum_{x(i, j) < M} x(i, j) \quad (3.6)$$

$$MH = \frac{1}{n^2 - k} \sum_{x(i, j) \geq M} x(i, j) \quad (3.7)$$

K: M ortalamasından büyük olan gri seviyeli piksellerin sayısı

ML: Düşük ortalama değeri

MH: Yüksek ortalama değeri

Adım 3: Her bloğun bit eşlemini hesaplamak için şu denklem kullanılır:

$$B(i, j) = \begin{cases} 1 & \text{eğer } x(i, j) > M \\ 0 & \text{eğer } x(i, j) \leq M \end{cases} \quad (3.8)$$

$B(i, j)$ her bloğun bit eşlemini temsil eder.

Eğer bloğun piksel değeri bloğun ortalamasından büyük ise, bit eşlemin değeri 1 olacaktır. Aksi halde, bit eşlemin değeri 0 olacaktır.

Adım 4: Kodlayıcı, resmin bütün blokları için ML ve MH değerlerini ve bit eşlemini resim dosyasına yazar. Çünkü bu bilgiler resmin geri çatma işleminde gereklidirler.

Adım 5: Çözücü, her resim bloğunu geri çatmak için bloğun 1 değerine sahip olan alanını bloğun ML değeriyle; 0 değerine sahip olan alanını ise bloğun MH değeriyle değiştirir. Şekil 3.8.'de BKK algoritmasının resmin bir bloğu üzerine uygulanması gösterilmektedir.

181	173	156	141
192	180	138	118
188	183	141	116
185	176	157	123

(a)

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

(b)

182	182	136	136
182	182	136	136
182	182	136	136
182	182	136	136

(c)

-1	-9	20	5
10	-2	2	-18
6	1	5	-20
3	-6	21	-13

(d)

Şekil 3.8. BKK algoritmasının resmin bir bloğu üzerine uygulanması, (a) Orijinal resim bloğu, ortalaması=159, (b) Kodlama işlemi uygulandıktan sonra bilgiler, $ML=182$ ve $MH=136$. (c) Çözücüde bloğun geri çatma işlemi, (d) Ortalama kare hatası (OKH) =128,5

3.3.2. BKK Algoritma'sının Özellikleri:

BBK algoritması az hesaplama gerektirir. Bu yüzden bu algoritmayı gerçekleyen yazılımlar ve donanımlar kolaylıkla oluşturulabilir [18, 23]. Algoritmanın uygulanması basittir. İstenen oranda sıkıştırma sağlanabilir. Geri çatma işleminin sonucunun kalitesi orta seviyededir. Resmin kenarlarını muhafaza eder. Her bloğun ortalamasının ve standart sapmasının değerlerini kullanarak ayrı bir şekilde sıkıştırır [24]. Sabit bölmeyi kullandığı için yerel karakteristiklerden faydalanmayı başaramaz [23].

4. MATERİYAL VE YÖNTEM

4.1. Giriş

Bu bölümde, dijital renkli resimlere filigran damgalanması amacıyla ilk kez önerilen bir damgalama yöntemi ayrıntılarıyla anlatılmaktadır. Damgalama yönteminin geliştirilmesinde kullanılan araçlar ‘Materyal’ alt başlığı altında yer almaktadır. Resme filigran damgalama ve resimden filigran algılama/çıkarma yönteminin yapısı ile çalışması hakkında ayrıntılı bilgi ‘Yöntem’ alt başlığı altında ele alınmıştır.

4.2. Materyal

Bu tez çalışmasında bilgisayar ortamına aktarılan renkli resimlere filigran damgalanması ve filigranın çıkarılması amacıyla geliştirilen yöntem için bir bilgisayar yazılımı hazırlanmıştır. Yazılım hazırlanmasında kullanılan işletme sistemi, Windows® XP Service Pack 2’dir. Önerilen algoritmanın tasarımında ve kodlamasında, Matlab® 7.1 (R14) Service Pack 3 tekniksel hesaplamalar dili kullanılmıştır. Yazılımın hazırlandığı ve testlerin yapıldığı bilgisayar, Intel® Pentium IV 1.73 GHz işlemcili, üzerinde 1.5 GByte RAM ve 256 MB ekran kartı bulunan bir Dell™ dizüstü bilgisayardır.

Önerilen damgalama yönteminin testleri için kullanılan filigran, Şekil 4.1.’de görülen (128×128) piksel boyutlarındaki siyah–beyaz bir resimdir. Bu filigran, (512×512) piksel boyutlarındaki Lena⁽¹⁾, Baboon⁽²⁾ resimlerine damgalanmıştır (Şekil 4.2.’de). Testlerde kullanılan resimler renkli Bitmap formatındadır.

(1) Lena resmi, orijinal olarak Kasım 1972’de Playboy™’ın dijitalleştirme merkezince yayımlandı. Bu resimde, görünebilir bozulma eklenmeden filigran gömme işlemi zorlaşır. Çünkü bu resmin omuz bölgeleri yumuşak ve arka planının kontrastı keskindir. Ancak, resmin tüylü olan bölgesinin işlenmesi kolaydır.

(2) Baboon resmi fazla doku içerdiği için üzerinde damgalama işlemi yapılması daha kolaydır.

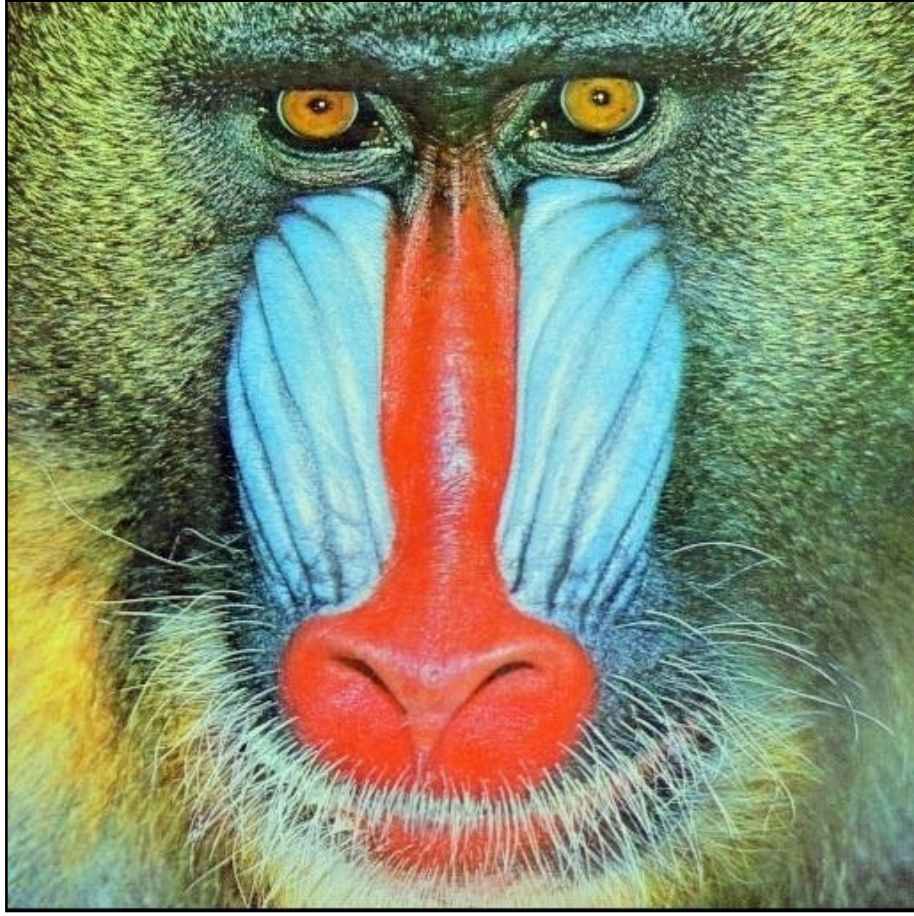


Şekil 4.1. Resimlere damgalanacak filigran



(a)

Şekil 4.2. Testler için kullanılan resimler, (a) Lena, (b) Baboon



(b)

Şekil 4.2. (Devam)Testler için kullanılan resimler, (a) Lena, (b) Baboon

4.3. Yöntem

Dijital resimlere gizli bir telif hakkı bilgisi damgalanması için önerilen yüzlerce farklı yöntem vardır. Bu yöntemlerin yapılarına göre sınıflandırılması Şekil 2.8.'de görülmektedir. Bu tez çalışması, yeni bir damgalama yöntemi sunmaktadır. Çünkü hem ADD hem de BKK bir arada kullanılmaktadır. ADD oldukça yaygın bir frekans bölge damgalama yöntemidir. Bu yöntemin hakkında birden fazla makale ve tez çalışması vardır. Blok kırpma kodlamasının damgalama yöntemi olarak kullanılması, oldukça nadirdir. Çünkü BKK algoritması bir resim kayıplı sıkıştırma algoritmasıdır. [19]'daki makalede gri seviyeli resme bir filigran gömmek için BKK algoritması kullanılmıştır. ADD ve

BKK'nin bir arada kullanılması, sadece bir sıkıştırma metodu olarak [28]'de sunulmuştur.

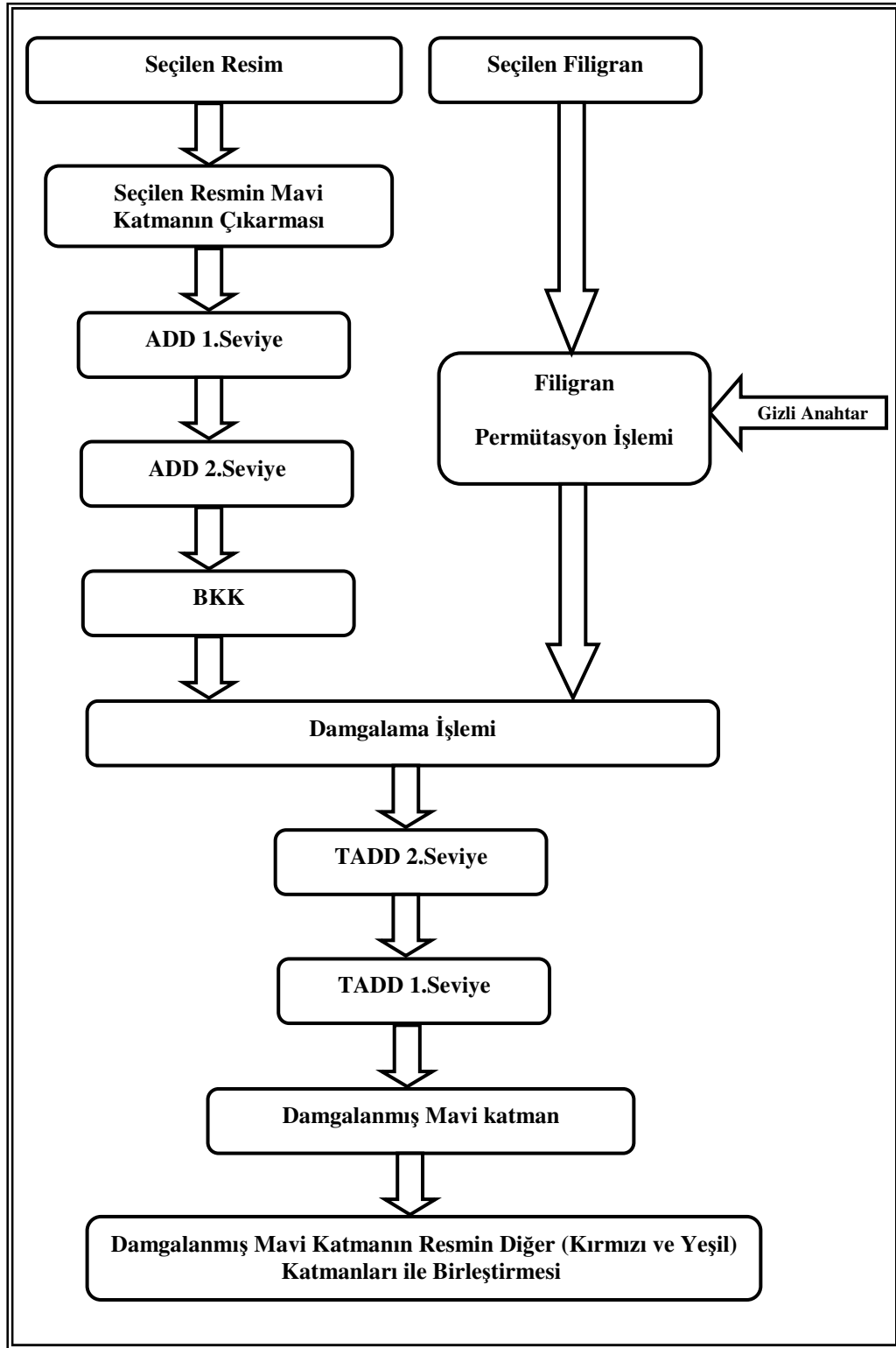
Bu tez çalışmasında dijital renkli resimlerde görünmez ve dayanıklı damgalama işlemi yapmak için dönüşüm bölge damgalama ve uzamsal bölge damgalama türü kullanılmıştır. Resme bir filigran gömmek için resmin üzerine hem ADD ve BKK uygulanır. İlk olarak, resmin birinci seviye ve ikinci seviye ADD'si hesaplanır, elde edilen ikinci seviyenin (DY1, YD1 ve YY1) alt-bantlarının frekans katsayıları üzerine BKK algoritması ayrı ayrı uygulanır. Ancak ikinci seviyenin (DD1) alt-bantının üzerinde BKK algoritması kullanılmadığı için bu alt-bantın damgalama işlemi sadece ADD kullanılarak yapılır.

ADD ve BKK'nin bir arada kullanılmasının amacı, daha dayanıklı bir damgalama işlemi elde etmektir. Ayrıca resme filigran damgalama işlemi ve filigran çıkarma işleminin dayanıklılığını artırmak için önerilen damgalama yöntemi, damgalanacak filigrana gizli anahtar kullanarak permütasyon işlemi uygulamaktır.

Önerilen yöntemin ayrıntıları **3.3.1** ve **3.3.2** bölümlerinde açıklanacaktır. Damgalama için resim ile filigran üzerinde yapılan ön işlemler, damgalama algoritması ve damgalanmış resmin oluşturulması yönteminin ilk aşamasını oluşturmaktadır. İkinci aşamada ise damgalanmış resimden filigranların çıkarılması için sırasıyla ön işlemlerin yapılmasının ardından filigran çıkarma algoritmasının çalıştırılması ve son olarak filigranın oluşturulması hakkında ayrıntılarıyla bilgi verilecektir.

4.4. Resim Damgalama İşlemi

Dijital renkli resme filigranı gömmek için renkli resmin ilk olarak mavi katmanı hesaplanır, sonra mavi katmanlı resmin üzerine ADD ve BKK uygulanır. Bu tez çalışmasında ADD ve BKK kullanılmasının nedeni, her iki algoritmanın **3.2.2.** ve **3.3.2.** bölümlerinde gösterilen özelliklerinden kaynaklanıyor. Damgalama işlemi yapmadan önce filigran permütasyon işlemi vardır. Şekil 4.3.'te damgalama işleminin blok diyagramı gösterilmektedir.



Şekil 4.3. Damgalama işleminin blok diyagramı

4.4.1. Filigran Permütasyon İşlemi

Damgalanacak filigrana permütasyon işlemi uygulamak için bu adımlar takip edilir:

Adım 1: (0 ile $2^{32}-1$) Pozitif tam sayısı seçilir. Seçilen tam sayı, damgalama gizli anahtarını temsil eder. Bu anahtar gizli tutulmalıdır. Çünkü filigran çıkarma işleminde de gereklidir.

Adım 2: Seçilen gizli anahtar, Matlab'ta bulunan (*rand('state',seed)*) fonksiyonunun, *seed* değerini temsil eder.

Adım 3: Aynı filigranın boyutlarında ve rastgele değerlere sahip bir matris oluşturmak için aşağıdaki fonksiyonların çağırılması gerekir.

(*rand('state',seed)*)

imark= rand (size (filigran))

imark:rand fonksiyonunun ürettiği bütün rastgele sayılar, bu matrisin değerlerini temsil eder.

Adım 4: *Imark* matrisin bütün değerleri, reel formattadır. Bu değerleri, 0 ve 1 şekline dönüştürmek için, aşağıdaki fonksiyon kullanılır.

imark'=im2bw(imark)

im2bw: bu fonksiyonun sonucu, matrisi siyah-beyaz formatta bir resme çevirir.

Adım 5: Son olarak damgalanacak filigranın üzerine permütasyon işlemi uygulamak için, elde edilen *imark'* resmi ile damgalanacak filigrana (XOR) mantıksal işlemi uygulanır. Elde edilen sonuç resmi, hem resim damgalama işleminde hem de resimden filigran çıkarma işleminde kullanılır.

4.4.2. Önerilen Damgalama Algoritması

[32]'de ADD'ye dayalı damgalama yöntemi, damgalama filigranının resmin bütün (DD1, DY1, YD1 ve YY1) alt-bantlarında gömülmesi önerilmiştir.

Böylece damgalanmış resmin farklı tür saldırılara daha dayanıklı olduğu gösterilmiştir. Çünkü (DD1) alt-bandında damgalanmış resimde damgalanan filigranı filtrelemeye, JPEG kayıplı sıkıştırmaya ve geometrik bozulmalara dayanıklılığını artırır.

Fakat damgalanmış resimde damgalanan filigran, resmin histogramında değişikliklere daha duyarlı hale gelir. Örneğin; kontrast ayarlama, gama düzeltme, histogram eşitleme. (DY1, YD1 ve YY1) alt-bantlarında damgalanmış resimde damgalanan filigranın, düşük-geçiren filtrelemeye, kayıplı sıkıştırmaya ve küçük geometrik bozulmalara dayanıklılık seviyesi azdır. Fakat damgalanan filigranın gürültü ekleme işlemine karşı dayanıklılığı yüksektir. ADD'nin bütün alt-bantlarının avantajları ve dezavantajları ve BKK algoritmasının avantajları da göz önüne alındığında, önerilen damgalama algoritmasının daha dayanıklı olacağı öngörülmüştür. Resme bir telif hakkı filigranı gömmek için damgalama algoritması şu adımlarda yapılır.

Adım 1: (24) bitlik, Bitmap formatında bir renkli resim seçilir.

Adım 2: (1) bitlik, Bitmap formatında siyah-beyaz resim seçilir. Bu resim filigranı temsil eder. Seçilen resmin üzerine filigran permütasyon işlemi uygulanır.

Adım 3: Seçilen resimde mavi rengin katmanı hesap edilir. Çünkü damgalama işlemi sadece resmin mavi katmanının üzerinde yapılır. Mavi katmanın seçilme nedeni, mavi katmanın frekanslarının resmin diğer (kırmızı ve yeşil) katmanlarının frekanslarından daha büyük olması ve mavi katmanın frekanslarında olan değişimlerin, insan gözünde kolay bir şekilde fark edilememesidir. Işığın mavi spektrumu, kırmızı ve yeşil spektrumdan daha düşük duyarlılıktadır [29]. Çünkü insan gözünün retinası fovea bölümünde, (mavi ışığı idrak edilmesi için ilk olarak sorumlu olan bölge) α konilerinin yoğunluğu düşüktür.

Adım 4: Mavi katmanın üzerine 1.seviyeli Haar ADD uygulanır. Bu işlemten sonra resim dört alt-banda bölünür (DD, DY, YD ve YY). Bu alt-bantlar resmin frekans katsayılarını temsil eder. Haar ADD algoritması 3.2.1.3. bölümünde ayrıntılı bir şekilde açıklanmıştır.

Adım 5: (DD) alt-bandı üzerine Haar ADD algoritması uygulanır. Bu işlemten sonra (DD) alt-bandı dört alt-banda (DD1, DY1, YD1 ve YY1) bölünür.

Adım 6: (DD1) alt-bandına filigran gömmek için denklem (4.2) kullanılır.

$$DD1(i, j) = DD1(i, j) + (gizlifiligran(i, j) * \alpha) \quad (4.2)$$

Gizlifiligran: Üzerine permütasyon uygulanan filigran. $(1 \leq j \leq M)$, $(1 \leq j \leq N)$ ve $(M \times N)$:Üzerine permütasyon uygulanan filigranın boyutlarıdır. α : Reel sayıdır. Damgalama güçlendirme değerini temsil eder.

Adım 7: Elde edilen (DY1, YD1 ve YY1) alt-bantların sonuçları üzerine ayrı bir şekilde, (4×4) blok değeriyle BKK algoritmasının sadece kodlayıcı işlemi uygulanır. BKK algoritmasının kodlayıcı işlemi 3.3.1. bölümünde ayrıntılı bir şekilde açıklanmıştır.

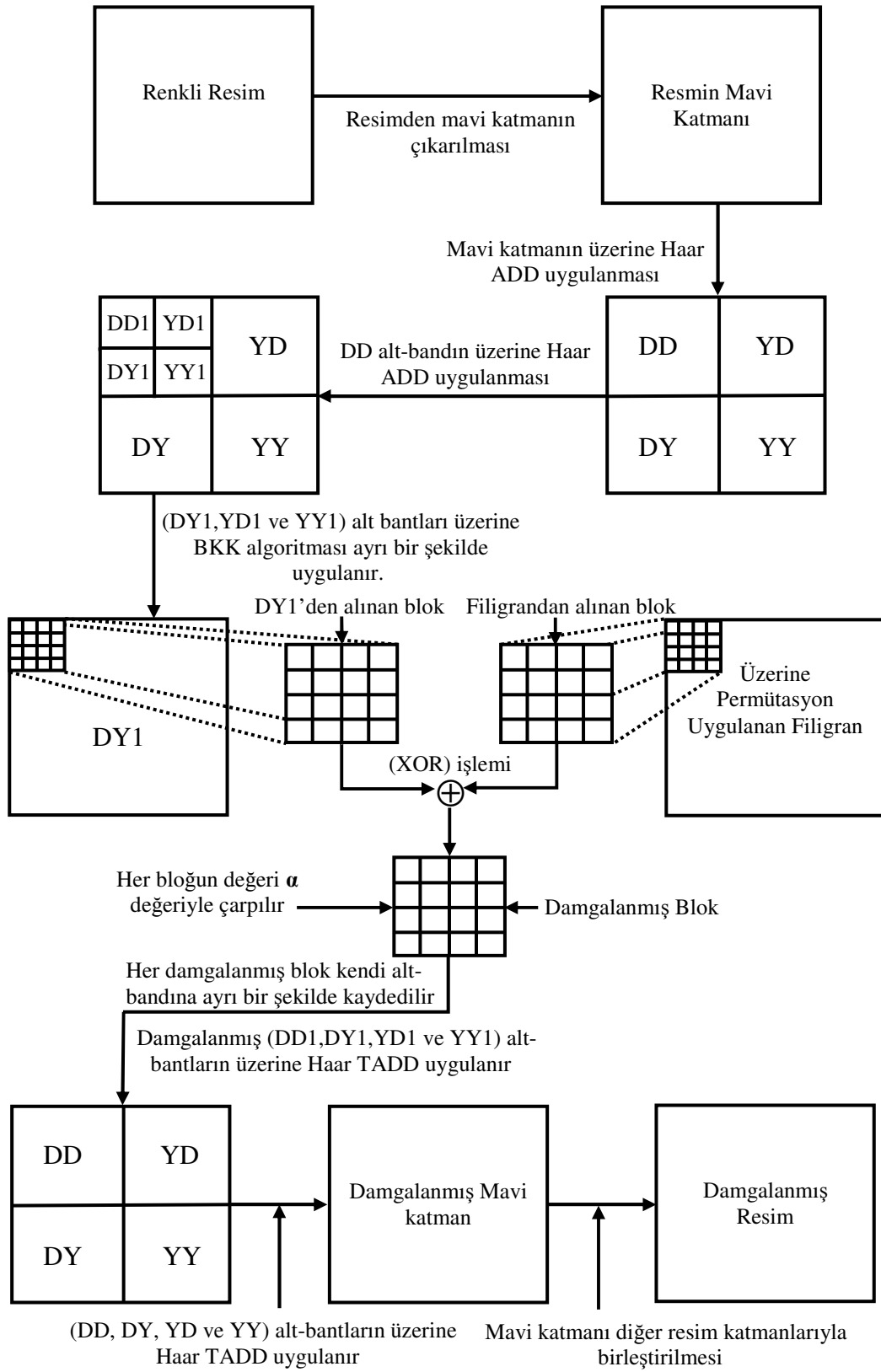
Adım 8: Her bir (DY1, YD1 ve YY1) alt-banda filigran gömmek için elde edilen alt bandın BKK algoritmasının blokları, filigranın aynı boyutta bölünmüş bloklarıyla (XOR) işlemine tabi tutulur ve sonuç blok damgalama güçlendirme değeriyle çarpılır. Bu işlem bütün alt-bandın ve filigran resmin bölünmüş blokları üzerinde uygulanır.

Adım 9: (DD1, DY1, YD1 ve YY1) alt-bantları damgalandıktan sonra Haar TADD uygulanır. Bu işlemten sonra (DD1, DY1, YD1 ve YY1) tek bir (DD) alt-bant şeklinde olacaktır.

Adım 10: (DD, DY, YD ve YY) alt-bantları üzerine Haar TADD uygulanır. Bu işlemten sonra (DD, DY, YD ve YY) alt-bantları tek bir damgalanmış mavi katman şeklinde olacaktır.

Adım11: Damgalanmış mavi katman resmin diğer (kırmızı ve yeşil) katmanlarıyla birleştirilir.

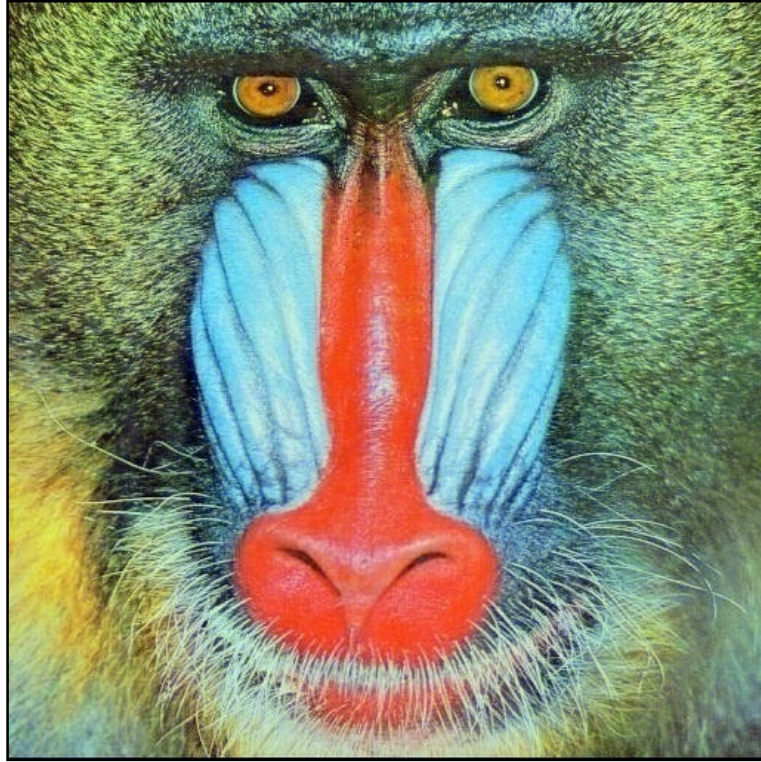
Adım 12: Birleştirme işleminden sonra elde edilen resim, damgalanmış resmi temsil eder. Şekil 4.4.'te resim damgalama algoritması gösterilmektedir. Şekil 4.5.'te $(0.1) \alpha$ damgalama güçlendirme değeriyle damgalanmış resimleri gösterilmektedir.



Şekil 4.4. Önerilen damgalama algoritması



(a)

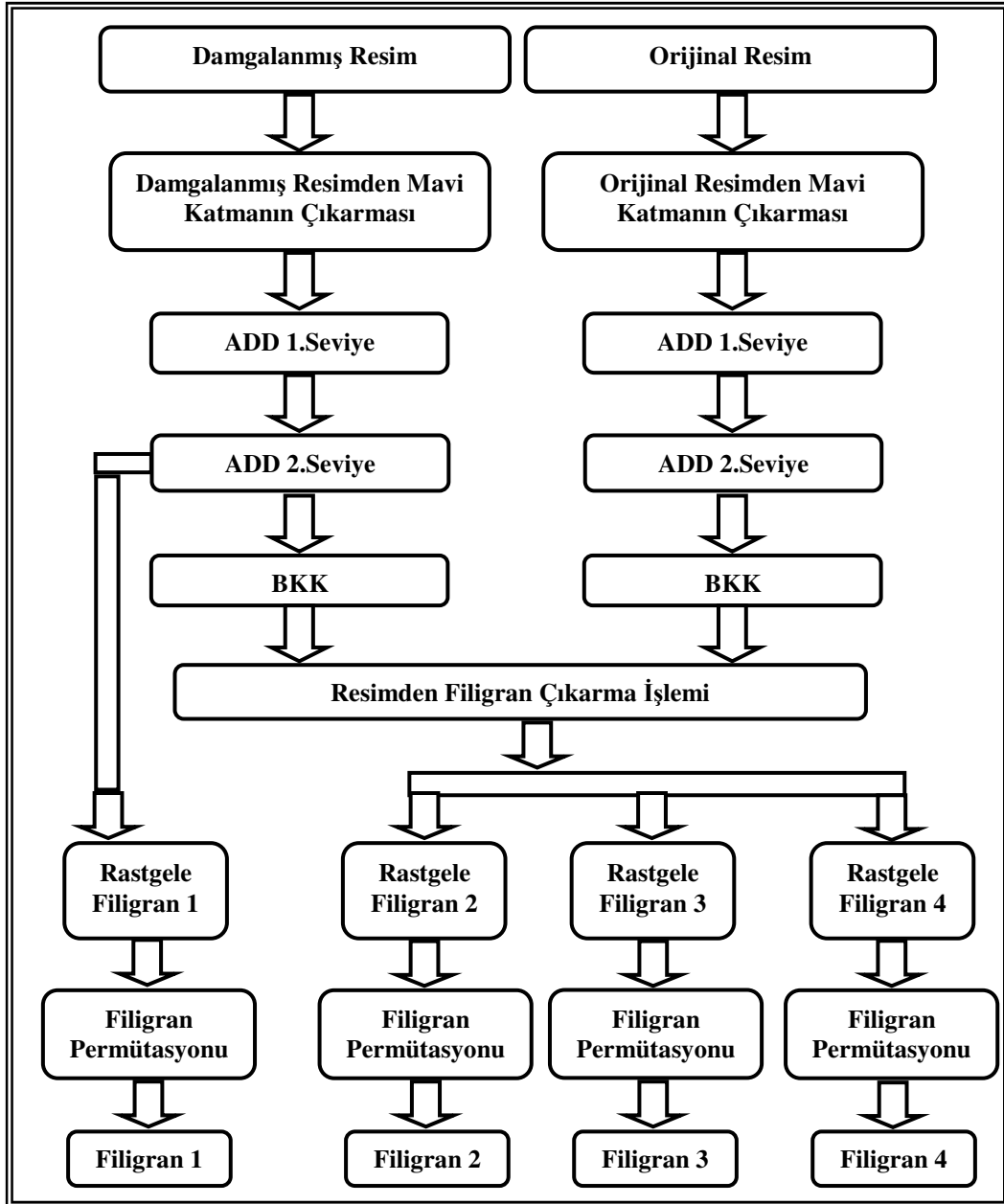


(b)

Şekil 4.5. (0.1) α değeriyle damgalanan resimler, (a) Lena , (b) Baboon

4.4.3. Filigran Çıkarma Algoritması

Damgalanmış resimden damgalanan filigranın çıkarılması için orijinal taşıyıcı resim kullanılır. Bu yüzden bu tür damgalama yöntemi, kişisel damgalama yöntemi olarak tanımlanır. Damgalanmış resimden filigranları çıkarmak için damgalama işleminde kullanılan ADD (1. ve 2. Seviyesi), BKK algoritması ve filigran permütasyon işlemleri sırasıyla kullanılır. Şekil 4.6.'da filigran çıkarma algoritmasının blok diyagramı gösterilmektedir.



Şekil 4.6 Filigran çıkarma algoritmasının blok diyagramı

Damgalanmış resimden damgalanan filigranları çıkarmak için filigran çıkarma algoritması şu adımlarda yapılır.

Adım 1: Damgalanmış resim ve orijinal resim seçilir.

Adım 2: Seçilen damgalanmış resmin ve orijinal resmin, mavi katmanı ayrı ayrı alınır.

Adım 3: Damgalanmış resimden alınan mavi katmanın ve orijinal resimden alınan mavi katmanın üzerine 1.seviyeli Haar ADD ayrı ayrı uygulanır. Bu işlemden sonra damgalanmış resimden alınan mavi katman (DD, DY, YD ve YY) alt-bantlarına ve orijinal resimden alınan mavi katman (ODD, ODY, OYD ve OYY) alt-bantlarına bölünür.

Adım 4: (DD) ve (ODD) alt-bantların üzerine Haar ADD algoritması uygulanır. Bu işlemden sonra (DD) alt-bandı (DD1, DY1, YD1 ve YY1) alt-bantlarına ve (ODD) alt-bandı (ODD1, ODY1, OYD1 ve OYY1) alt-bantlarına bölünür.

Adım 5: (DD1) alt-bandında damgalanan filigranı çıkarmak için denklem (4.3) kullanılır.

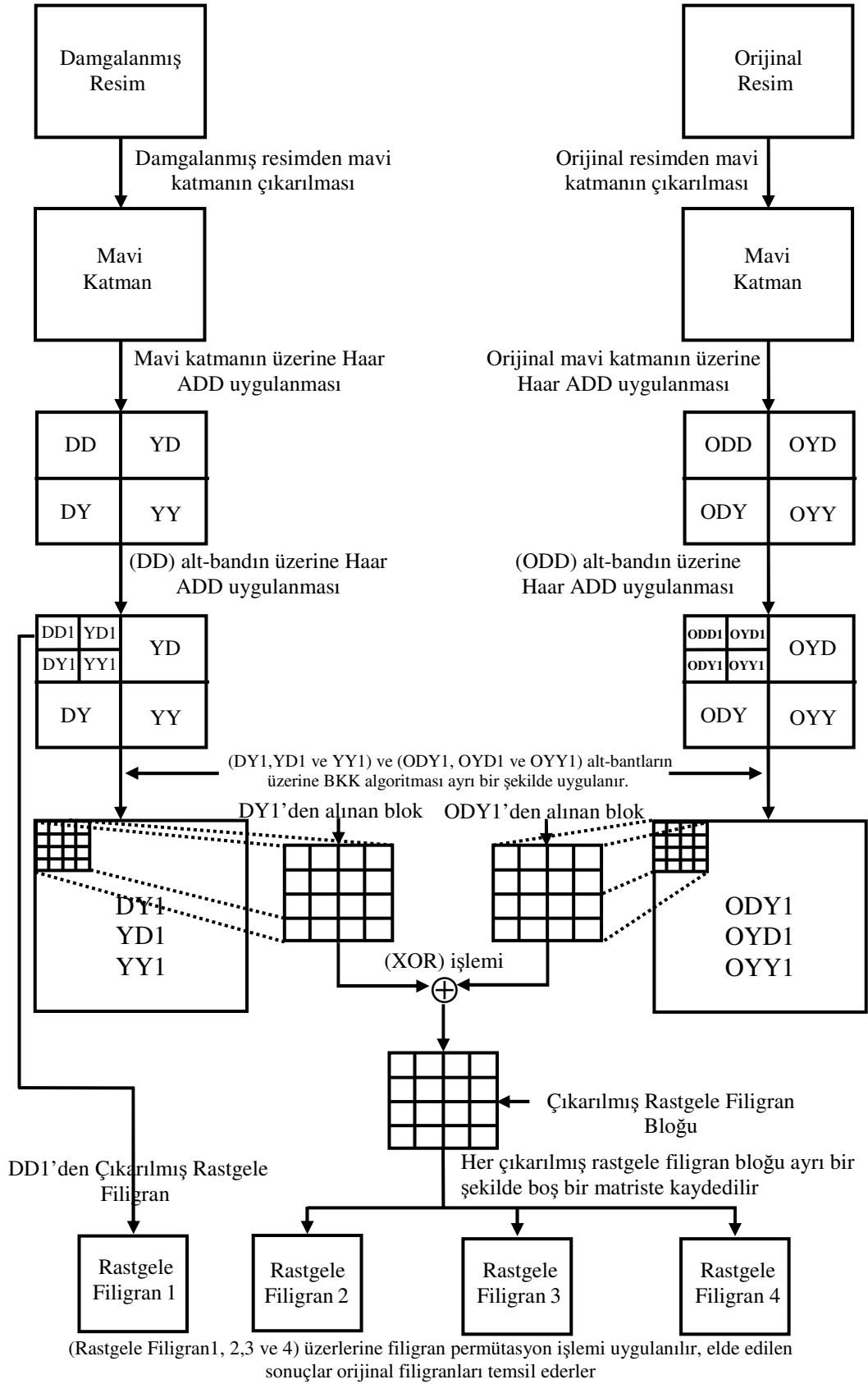
$$fark = (DD1(i, j) - ODD1(i, j)) / \alpha \quad (4.3)$$

Eğer $fark > 0.5$ ise (rastgele filigran1) matrisinin değeri 1 olur. Aksi halde 0 olur. $(1 \leq i \leq M)$, $(1 \leq j \leq N)$ ve $(M \times N)$ filigran resminin boyutlarıdır.

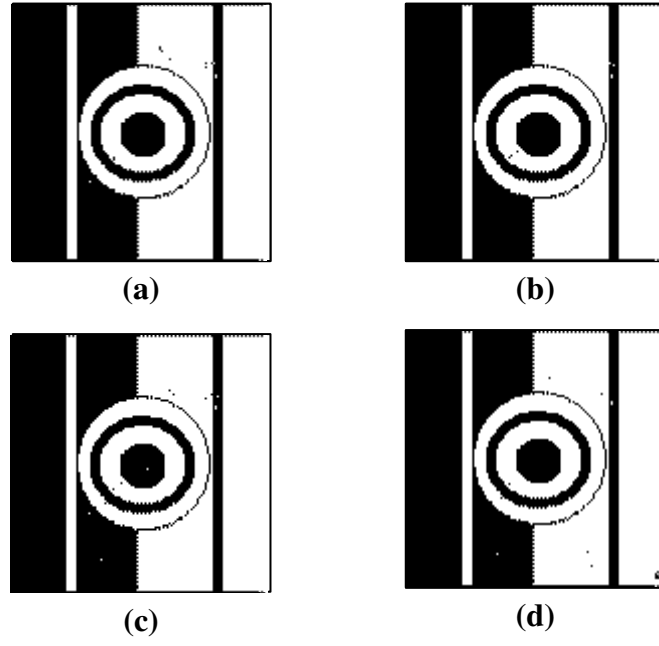
Adım 6: Elde edilen (DY1, YD1 ve YY1) ve (ODY1, OYD1, OYY1) alt-bantlarının üzerine ayrı ayrı BKK algoritması uygulanır.

Adım 7: Her bir (DY1, YD1 ve YY1) alt-bandın filigranını çıkarmak için elde edilen alt bandın BKK algoritmasının böldüğü bloklar ile aynı şekilde BKK algoritmasıyla orijinal (ODY1, OYD1, OYY1) alt-bantlarının aynı boyutta bölünmüş blokları arasında (XOR) işlemi yapılır. Bu işlemden sonra (rastgele filigran 2,3 ve 4) elde edilir.

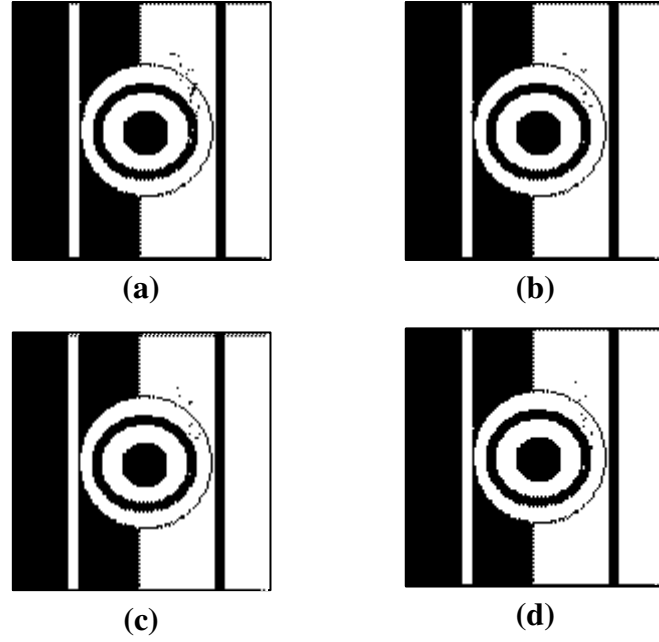
Adım 8: Son olarak, elde edilen filigranlar rastgele filigranları temsil ederler. Bu filigranları orijinal şekline dönüştürmek için filigran permütasyon işlemi gizli anahtar ile filigranlar uygulanır. Şekil 4.7.'de damgalanmış resimden filigran çıkarma algoritması gösterilmektedir.



Şekil 4.7. Damgalanmış resimden filigran çıkarma algoritması



Şekil 4.8. Damgalanmış Lena resminden çıkarılan filigranlar, (a) DD1'den çıkarılan filigran, (b) DY1'den çıkarılan filigran, (c) YD1'den çıkarılan filigran, (c) YY1'den çıkarılan filigran



Şekil 4.9. Damgalanmış Baboon resminden çıkarılan filigranlar, (a) DD1'den çıkarılan filigran, (b) DY1'den çıkarılan filigran, (c) YD1'den çıkarılan filigran, (c) YY1'den çıkarılan filigran

5. ARAŞTIRMA BULGULARI VE TARTIŞMA

5.1.Giriş

Dijital resimde damgalanan filigran fark edilmez, güvenilir ve saldırılara karşı dayanıklı olmalıdır. Damgalanan filigran yetkisiz algılamaya, çözmeye ve işlenmeye çok güçlü bir şekilde direnmelidir [30]. Ayrıca resim sıkıştırmaya, sinyal işlemeye, filtrelemeye ve diğer tekniklere karşı da dayanıklı olmalıdır. Damgalanmış resim dosyasına yapılan herhangi bir işlem, damgalanan filigrana bir saldırı yapmaya neden olabilir.

Damgalama işleminin sonucu filigranın damgalanmış resme yarattığı bozulma damgalanmış resmin kalitesini düşürdüğü gibi, hedeflenen görünmezliği de olumsuz olarak etkilemektedir. Bu amaçla damgalama güçlendirme α değeri en az seviyede tutulmalıdır. Ancak, çeşitli görüntü işleme saldırılarına karşı filigranın tanınabilir nitelikte çıkarılması, α değerinin artırılması ile mümkündür. Her iki amaca uygun bir damgalama güçlendirme α değeri bulmak için (0.01-0.1) arasında değişen 10 farklı α değerinde resimler damgalanmıştır. Önerilen damgalama yönteminin, farklı α değerlerinde damgalanmış resimlerin ile orijinal resimlerin arasındaki kalite ve değişim hatasını ölçmek için ortalama kare hatası (OKH) ve doruk sinyali ile gürültü oranı (DSGO) ölçütleri kullanılmıştır. Damgalanmış resimden çıkarılmış filigranların orijinal filigranla benzerliğini ölçmek için normalleştirme kolerasyonu (NK) ölçütü kullanılmıştır. Damgalanmış resimlere ve damgalanan filigranlara yönelik saldırılar yapmak için ACDSee®, Adobe Photoshop® ve XnView® yazılımları kullanılmıştır.

5.2. Filigrana Karşı Yapılabilecek Saldırı Çeşitleri

Görüntü işleme saldırılarına karşı dayanıklılık, damgalama sistemin majör gereksinimdir. Bütün olası saldırılara karşı damgalama sisteminin mutlak dayanıklılığına ulaşması mümkün olmayabilir [27]. Bunun için, pratiksel gereksinimini başarılı bir şekilde yapılan saldırı, damgalanan filigrana zarar vermeden damgalanmış resmin kalitesini düşürmeye çalışmalıdır. Bazı tür

saldırılarda damgalanan filigranın çıkarılması ya da algılanması çok zordur. Damgalama sistemi iyi bir şekilde tasarlanırsa, yüksek dayanıklılık derecesine ulaşabilir. Fakat dayanıklılık, fark edilmezlik ve yararlı yük kapasitesi arasında bedeller vardır ve her zaman bu nokta göz önüne alınmalıdır. Damgalama sistemine karşı yapılabilecek saldırılar dört kategoriye ayrılır.

5.2.1. Basit Saldırıları

Bazen bu tür saldırılar, gürültü saldırıları olarak adlandırılır. Bu tür saldırılarda damgalanmış resimde damgalanan filigranı zayıflatmak için damgalanmış resim ve damgalanan filigran üzerinde işlem yapmaya çalışıyorlar. Ancak damgalanan filigranı tanımlamaya ve izole etmeye uğraşmıyorlar. Bu tür saldırı örnekleri filtreleme, JPEG kayıplı sıkıştırması, gürültü ekleme, kırpma, analoga çevirme ve gama düzeltmedir.

5.2.2. Filigran Algılamayı Devre Dışı Bırakan Saldırıları

Bazen bu tür saldırılar eşzaman saldırıları olarak adlandırılır. Bu tür saldırılarda resimde damgalanan filigranın kolerasyonunu kırmaya ve filigranı çıkarmaya/algılamaya çalışıyorlar. Böylece filigran algılayıcıda filigranı çıkarma/algılama işlemi olanaksız olur. Bu tür saldırılar genellikle geometrik bozulmalar ile yapılır. Örneğin; döndürme, kırpma, kaykılma, uzamsal yönde kaydırma, resme pikseller ekleme, silme ve diğer geometrik dönüşüm metotları.

5.2.3. Sahte Filigran Ekleme Saldırıları

Bazen bu tür saldırılar, kilitlenme saldırıları olarak adlandırılır. Bu tür saldırılarda damgalanmış resme, damgalanan filigranı bozmak için damgalanmış resim üzerine başka bir filigran damgalanır. Bu tür saldırıların örneği, resme damgalanan filigranın yetkisini düşürmek için damgalanmış resme bir veya birkaç filigran damgalanır. Böylece hangi filigranın birinci olduğunu belli olmaz.

5.2.4. Filigran Kaldırma Saldırıları

Bazen bu tür saldırılar, hile saldırıları olarak adlandırılır. Bu tür saldırılarda damgalanmış resmi analiz edip damgalanan filigranı tahmin etmeye çalışıyorlar. Sonra damgalanmış resmi, orijinal resim ve filigran olarak birbirinden ayırt ederler ve damgalanmış resimden filigranı atarlar. Bu tür saldırıların örnekleri, gürültü çıkarma ve kesin lineer olamayan filtreleme işlemidir.

5.3. Damgalama Algoritması Performans Değerlendirme Ölçütleri

Hedeflenen resim kalitesinin ölçümünün, dijital resim damgalama sistemlerinde önemli bir rolü vardır. Damgalama algoritmasının performansını ve damgalama algoritmasından elde edilen test sonuçlarını değerlendirmek için birkaç ölçüt vardır. Doruk sinyali ile gürültü oranının (DSGO) ölçümü, orijinal resim ile damgalanmış resim arasındaki kalite farkını hesaplamak için kullanılır. Ortalama kare hatası (OKH) ölçümü, damgalanmış resmin piksel değerleri ile orijinal resmin piksel değerleri arasındaki kare farkı ortalamasını bulmak için kullanılır. Damgalanmış resimden çıkarılmış filigran ile orijinal filigranın arasındaki benzerlik değerini hesaplamak için normalleştirme kolerasyon (NK) ölçümü kullanılır. Damgalanmış resim ile orijinal resmin OKH'nı hesaplamak için denklem (5.1) kullanılır.

$$OKH = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [O(i, j) - D(i, j)]^2 \quad (5.1)$$

$O(i, j)$: Orijinal resmin piksel değeri

$D(i, j)$: Damgalanmış resmin piksel değeri

$M \times N$: Resmin boyutlarını temsil eder.

Damgalanmış resim ile orijinal resim arasındaki DSGO'nı hesaplamak için denklem (5.1)'den elde edilen sonuç, denklem (5.2)'de kullanılır.

$$DSGO = 10 * \log(255^2 / OKH) \text{ (dB)} \quad (5.2)$$

255: Sabit sayıdır. Resmin piksellerinin alacağı en yüksek değeri göstermektedir.
(dB): Kalite ölçü birimi desibeldir.

DSGO gerçek değeri bir anlam ifade etmez. Fakat farklı α değerlerinde damgalanmış resimlerin DSGO değerleri karşılaştırıldığı zaman, DSGO bir resim kalite ölçütü olur. Damgalanmış resimden çıkarılan filigran ile orijinal filigran arasındaki benzerliği ölçmek için denklem (5.3) kullanılır.

$$NK = \frac{\sum_{i=1}^M \sum_{j=1}^N [OF(i, j) * CF(i, j)]}{\sum_{i=1}^M \sum_{j=1}^N [OF(i, j)]^2} \quad (5.3)$$

$OF(i, j)$: Orijinal filigranın piksel değeri.

$CF(i, j)$: Çıkarılmış filigranın piksel değeri.

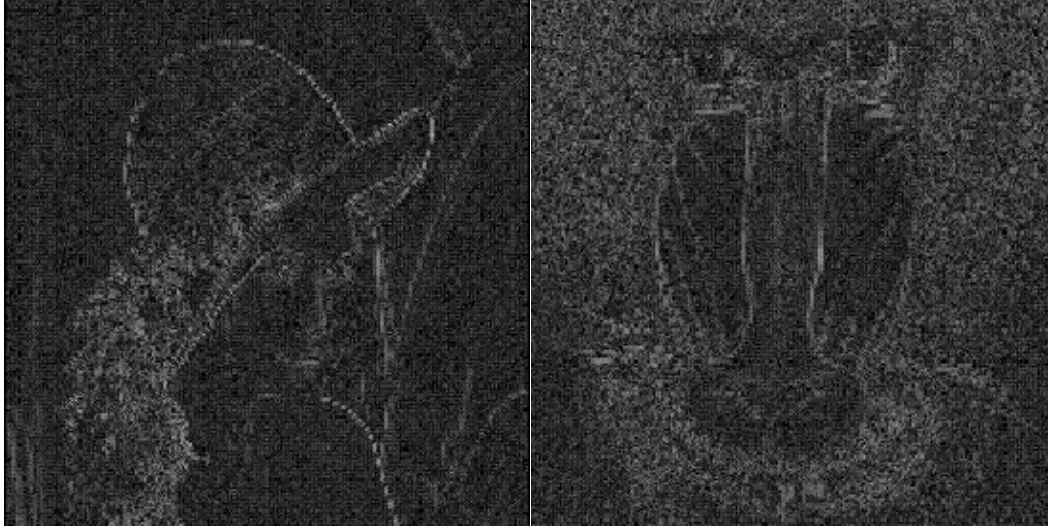
NK ölçümün en yüksek değeri 1'dir. Eğer orijinal filigran ile çıkarılmış filigranın NK değeri 1 ise, o zaman çıkarılmış filigran ile orijinal filigran tamamen aynıdır.

5.4. Performans Değerlendirme Testleri

5.4.1. Orijinal Resim ile Damgalanmış Resmin Arasındaki Farklılık

Önerilen damgalama algoritması, resmin mavi katmanını damgalama işleminde kullanıldığı için, damgalanmış resim ile orijinal resme mutlak farklılık işlemi uygulandığında, damgalama işlemi sadece damgalanacak resmin mavi

katmanının piksel deęerleri üzerine uygulanır. Damgalanmış resmin dięer (kırmızı ve yeşil) katmanlarının piksel deęerlerinde hiçbir deęişiklik olmaz. Şekil 5.1.'de Lena resmin ve Baboon resmin (0.1) α deęeriyle damgalandıktan sonra, her resmin mutlak farklılık resmi ayrı ayrı gösterilmektedir.



(a)

(b)

Şekil 5.1. (a) Orijinal Lena resmi ile damgalanmış resmin arasındaki mutlak farklılık resmi, (b) orijinal Baboon resmi ile damgalanmış resmin arasındaki mutlak farklılık resmi

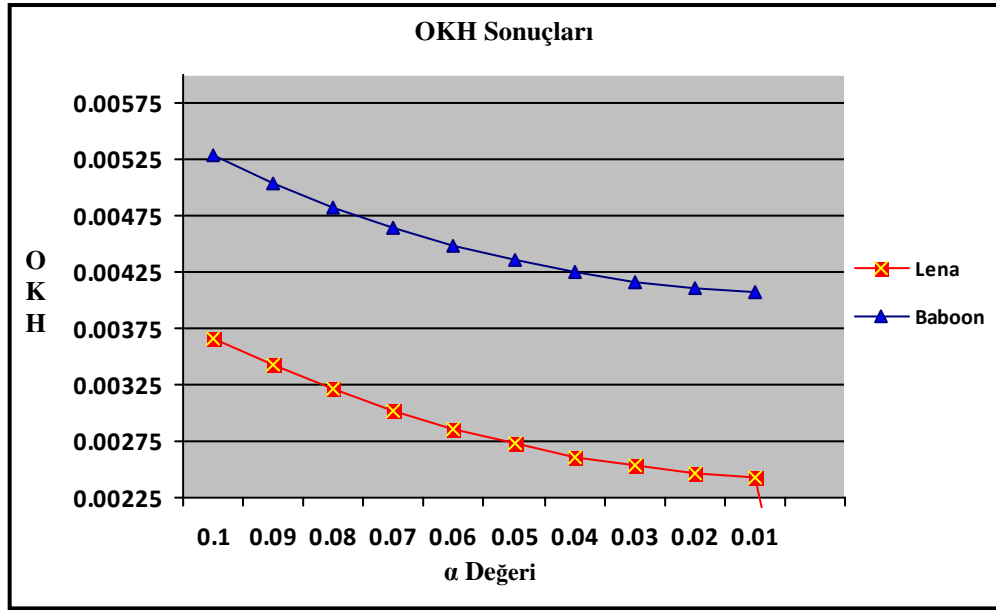
5.4.2. Damgalama Güçlendirme α Deęerinin Resim Kalitesine Etkisi

Dijital resimlerin damgalanması ile resim kalitesinde bir bozulma meydana gelmektedir. Oluşan bozulmanın nedenlerinden birisi, kullanılan damgalama güçlendirme α deęeridir.

Test için seçilen Lena ve Baboon resimleri, 10 farklı α deęeriyle ile damgalandıktan sonra elde edilen resimlerde oluşan bozulma OKH ile ölçülmüş, sonuçlar aşağıdaki Çizelge 5.1.'de verilmiştir.

Çizelge 5.1. $\alpha=0.1$ ile $\alpha=0.01$ arasında değişen 10 farklı α değeriyle damgalanmış test resimlerinde oluşan bozulmanın OKH ile ölçüm sonuçları

α Değeri	Lena	Baboon
0.1	0.00366	0.00528
0.09	0.00342	0.00504
0.08	0.00321	0.00483
0.07	0.00302	0.00465
0.06	0.00286	0.00449
0.05	0.00273	0.00436
0.04	0.00261	0.00425
0.03	0.00253	0.00416
0.02	0.00247	0.00410
0.01	0.00243	0.00407



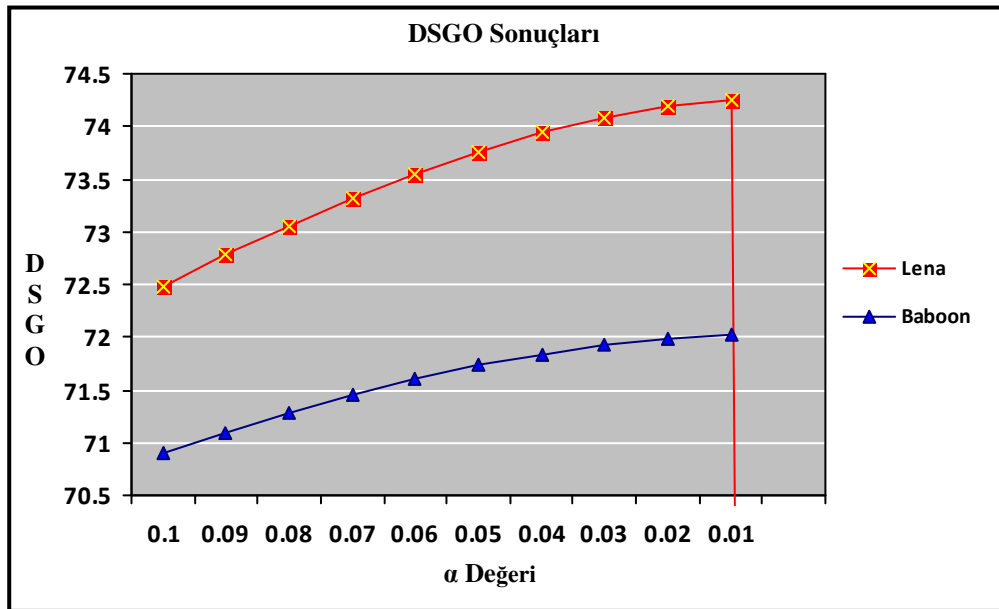
Şekil 5.2. Farklı α değerleriyle damgalanmış resimlerde oluşan bozulmanın α değerine göre grafiği

Çizelge 5.1.'deki sonuçlar kullanılarak, Şekil 5.2.'deki grafikte birlikte analiz edildiğinde, damgalama güçlendirme α değerinin artmasıyla birlikte resimler üzerinde oluşan bozulmanın da arttığı görülmektedir. Lena resminde oluşan bozulma miktarı Baboon resmindeki bozulma miktarından daha azdır.

Bunun nedeni, Baboon resminin Lena resmine göre daha fazla doku içerikli olmasıdır. Orijinal resimlerle, farklı α değerinde damgalanmış resimler arasındaki kalite DSGO ile ölçülmüş, sonuçlar aşağıdaki Çizelge 5.2.'de verilmiştir. DSGO değerinin düşmesi, resim kalitesindeki bozulmanın arttığını göstermektedir.

Çizelge 5.2. $\alpha=0.1$ ile $\alpha=0.01$ arasında değişen 10 farklı α değeriyle damgalanmış resimler ile orijinal resimler arasındaki kalite ölçümü, DSGO sonuçları

α Değeri	Lena	Baboon
0.1	72.49	70.90
0.09	72.78	71.10
0.08	73.06	71.28
0.07	73.31	71.45
0.06	73.55	71.60
0.05	73.76	71.73
0.04	73.95	71.84
0.03	74.09	71.93
0.02	74.20	71.99
0.01	74.26	72.03

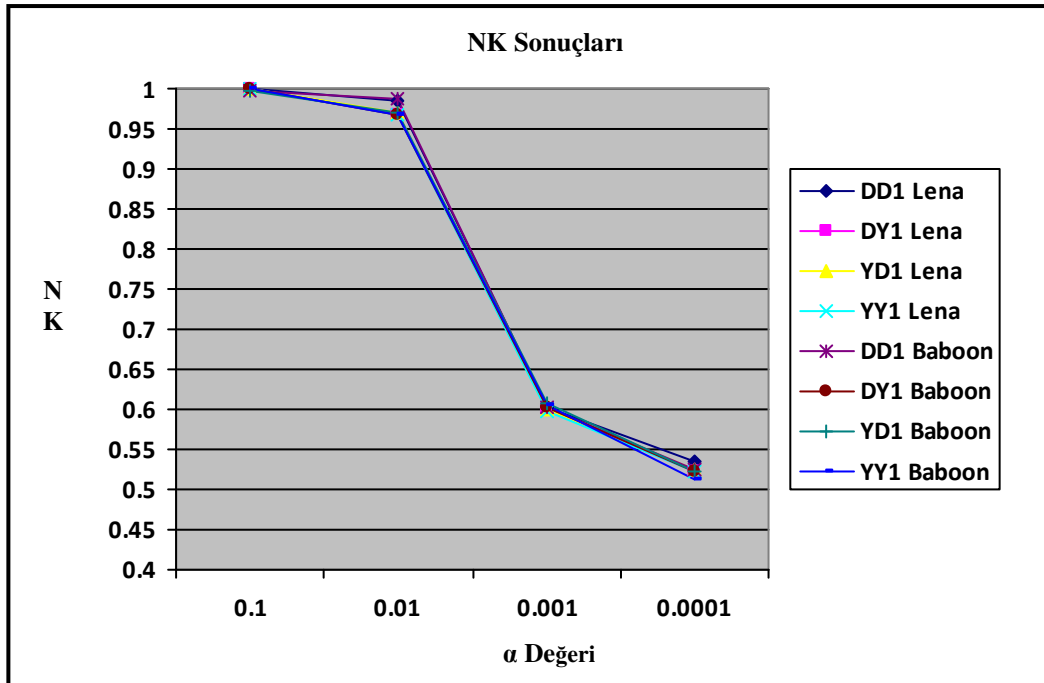


Şekil 5.3. Farklı α değerleriyle damgalanmış resimler ile orijinal resimler arasındaki DSGO kalite ölçümünün, α değerine göre grafiği

Farklı α değerinde damgalanmış resimlerden çıkarılmış filigranlar ile orijinal filigran arasındaki benzerlik testi, NK ile ölçülmüş, sonuçlar aşağıdaki çizelge 5.3.'te verilmiştir. NK değerinin düşmesi, çıkarılmış filigranlar ile orijinal filigran arasındaki benzerlik farkını göstermektedir. Ayrıca α değerinin artmasıyla, çıkarılmış filigranların NK benzerlik değeri de artmaktadır.

Çizelge 5.3. $\alpha=0.1$, $\alpha=0.01$, $\alpha=0.001$ ve $\alpha=0.0001$ arasında α değerleriyle damgalanmış resimlerden çıkarılmış filigranlar ile orijinal filigran arasındaki benzerlik değeri, NK sonuçları

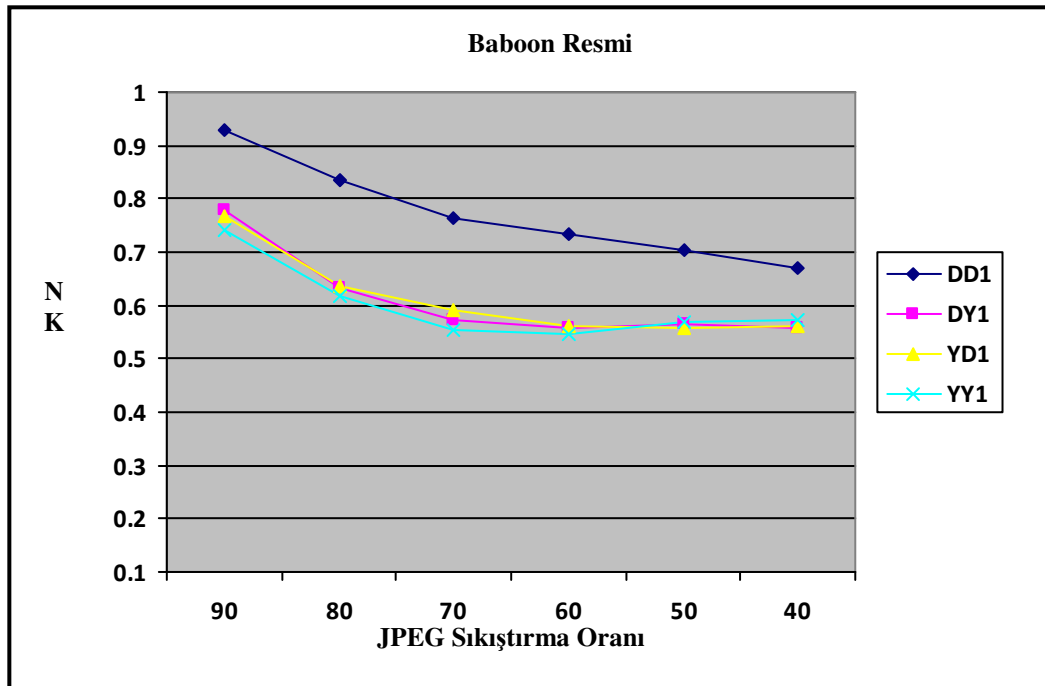
α Değeri	Lena				Baboon			
	DD1	DY1	YD1	YY1	DD1	DY1	YD1	YY1
0.1	0.9991	0.9991	0.9994	0.9992	0.9980	0.9992	0.9982	0.9988
0.01	0.9861	0.9675	0.9703	0.9675	0.9886	0.9684	0.9689	0.9685
0.001	0.6024	0.6005	0.6005	0.5986	0.6024	0.6022	0.6075	0.6044
0.0001	0.5338	0.5231	0.5254	0.5213	0.5248	0.5223	0.5237	0.5137



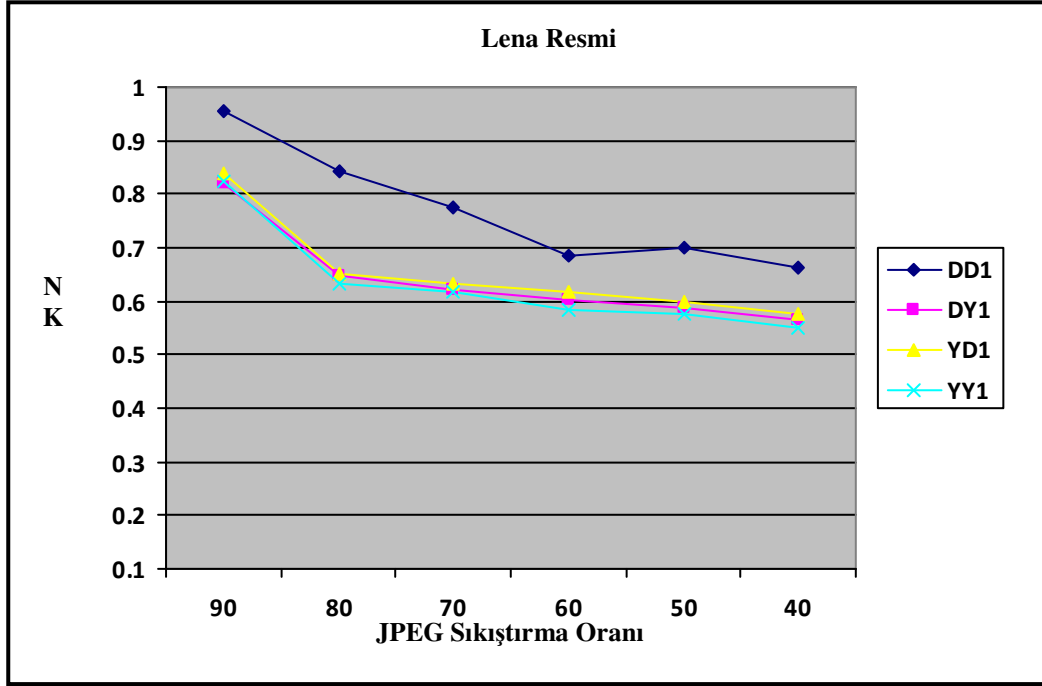
Şekil 5.4. Farklı α değerleriyle damgalanmış resimlerden çıkarılmış filigranlar ile orijinal filigran arasındaki NK benzerlik ölçümünün, α değerine göre grafiği

5.4.3. JPEG Kayıplı Sıkıştırması

JPEG kayıplı sıkıştırması günümüzde en çok kullanılan resim sıkıştırma yöntemidir. Her damgalama yönteminin dayanıklılığını ölçmek için JPEG sıkıştırma algoritması bir ölçüt olarak kullanılır. Eğer damgalanmış resmin üzerine JPEG sıkıştırması düşük oranla uygulanırsa, resimde damgalanan filigranın yok olmasına neden olabilir. Bu yüzden damgalama algoritması bütün sıkıştırma oranlarına dayanıklı olmalıdır [31]. (0.2) α değeriyle damgalanmış Lena ve Baboon resimleri, ACDSee yazılımı kullanılarak 6 farklı oranda (%40-...-%90) sıkıştırılmıştır. Ardından, filigran çıkarma algoritması ile JPEG kayıplı sıkıştırması uygulanan damgalanmış resimlerden filigranlar çıkarılmıştır. Elde edilen filigranların orijinal filigrana benzerlikleri NK ile ölçülmüş, sonuçlar her damgalanmış resim için ayrı bir şekilde grafik olarak şekil 5.5.'te ve şekil 5.6.'da gösterilmiştir.



Şekil 5.5. (0.2) α değeriyle damgalanmış Baboon resmin JPEG kayıplı sıkıştırması uygulandıktan sonra, resimden çıkarılmış filigranların NK sonuçları



Şekil 5.6. (0.2) α değeriyle damgalanmış Lena resmin üzerine JPEG kayıplı sıkıştırması uygulandıktan sonra, resimden çıkarılmış filigranların NK sonuçları

Lena ve Baboon resimlerin üzerine farklı sıkıştırma oranıyla JPEG kayıplı sıkıştırması uygulandığında, elde edilen resimlerden çıkarılmış filigranlar, sadece (DD1) alt-bandından çıkarılmış filigran, diğer alt-bantlardan çıkarılmış filigranlardan hem daha yüksek bir NK benzerlik değerine sahip hem de JPEG kayıplı sıkıştırmasına karşı daha dayanıklıdır. Fakat damgalanmış resimlerin (DY1, YD1 ve YY1) alt-bantları, JPEG kayıplı sıkıştırmasına %60 oranına kadar damgalanan filigranları koruyabilmektedirler.

5.4.4. Gürültü Ekleme

Damgalama algoritmasının dayanıklılık derecesini ölçmek için damgalanmış resme gürültü ekleme işlemi uygulanır. Farklı türlerde gürültü ekleme işlemleri vardır. Ancak damgalanmış resme ve damgalanan filigrana en çok zarar verebilen gürültü ekleme işlemi, Gauss gürültü ekleme işlemidir. Bu

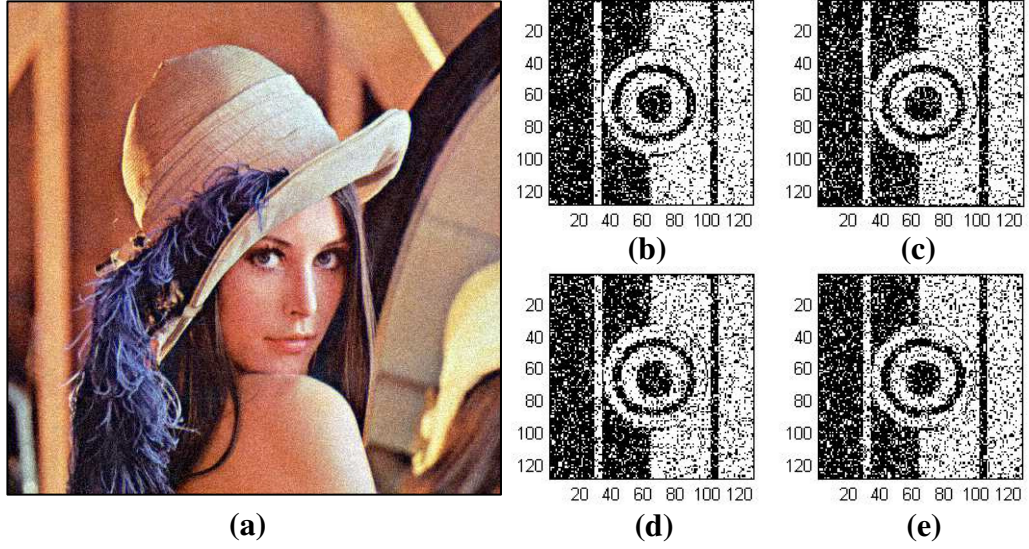
işlem damgalanmış resmin üzerine uygulandığında, hem damgalanmış resmin kalitesinin düşmesine hem de damgalanan filigranın yok olmasına neden olabilir.

Önerilen damgalama yönteminin, bu tür işleme dayanıklı olup olmadığını test etmek için, Adobe Photoshop yazılımı kullanarak, Gauss gürültü ekleme işlemi %5 ve %10 oranla damgalanmış Lena resmi üzerine uygulanmıştır. Ardından damgalanmış resme filigran çıkarma işlemi uygulanmıştır. Elde edilen filigranların NK değerleri ölçülmüştür. Çizelge 5.4.'te (0.1) α değeriyle damgalanmış Lena resmi ve %5 ve %10 oranla Gauss gürültüsü eklendikten sonra çıkarılmış filigranların NK sonuçları verilmiştir. Şekil 5.7'de Lena resmi üzerine %5 oranla Gauss gürültüsü eklendikten sonra ve resminden çıkarılmış filigranlar gösterilmektedir. Şekil 5.8'de Lena resmi üzerine %10 oranla Gauss gürültüsü eklendikten sonra ve resminden çıkarılmış filigranlar gösterilmektedir.

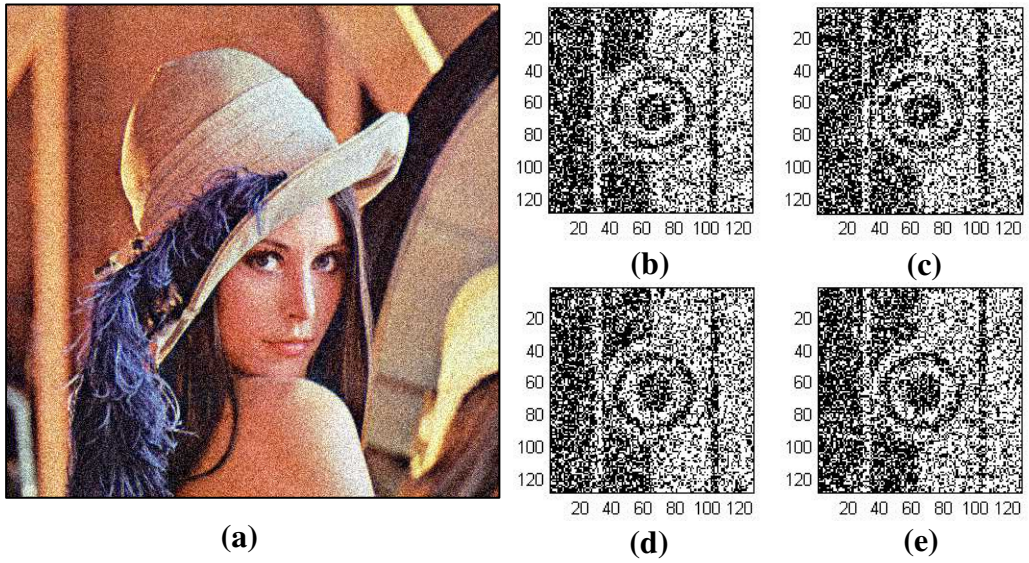
Çizelge 5.4. $\alpha=0.1$ değeriyle damgalanmış lena resmi ve ve %5 ve %10 oranla Gauss gürültüsü eklendikten sonra çıkarılmış filigranların NK sonuçları

Gauss Gürültüsün Oranı	DD1	DY1	YD1	YY1
%5	0.8507	0.8218	0.8238	0.8197
%10	0.6872	0.6764	0.6783	0.6812

Elde edilen NK sonuçları incelendiğinde, damgalanmış resmin bütün (DD1, DY1, YD1 ve YY1) alt-bantlarından çıkarılmış filigranların NK değerleri yaklaşık olarak eşittir. Demek ki önerilen damgalama algoritması uygulanmış resmin bütün alt bantlarında damgalanan filigranlar, Gauss gürültüsü ekleme işlemine karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bandında damgalanan filigranda Gauss gürültüsü ekleme işlemine karşı dayanıklıdır. Blok kırpma kodlamasının ayırık dalgacık dönüşümüyle bir arada kullanılması, önerilen damgalama algoritmasının dayanıklılık yeteneğini arttırmaktadır.



Şekil 5.7. $(0.1) \alpha$ değeriyle damgalanmış Lena resmin üzerine %5 oranla Gauss gürültüsü eklendikten sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) DD1'den çıkarılmış filigran



Şekil 5.8. $(0.1) \alpha$ değeriyle damgalanmış Lena resmin üzerine %10 oranla Gauss gürültüsü eklendikten sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) DD1'den çıkarılmış filigran

5.4.5. Resim Kırpma İşlemi

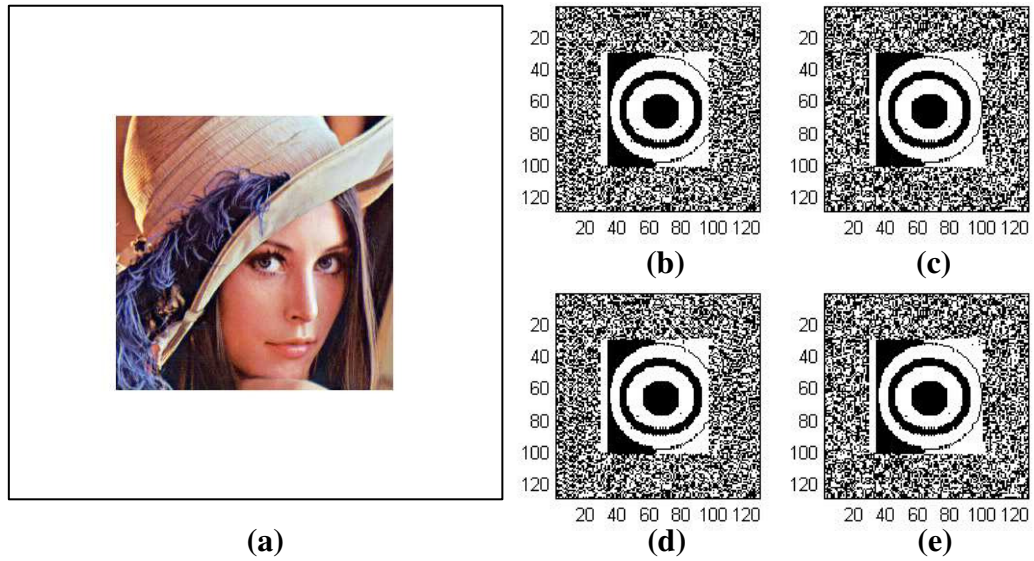
Resim Kırpma işlemi, damgalanmış resmin aynı boyutta ya da farklı boyutta resmin bir bölümünün kesilmesi ile yapılır. Görünmez bir şekilde

damgalanmış resme damgalanan filigranın yeri belli değildir. Damgalanmış resme kırpma işlemi yüksek bir ölçüde uygulandığında, damgalanan filigrana yüksek derecede zarar verebilir veya filigranın yok olmasına neden olabilir.

Önerilen damgalama yönteminin bu tür işleme karşı dayanıklı olup olmadığını test etmek için Adobe Photoshop yazılımını kullanarak, (0.1) α değeriyle damgalanmış Lena resmi üzerine kırpma işlemi tam resmin ortasından uygulanmıştır. Elde edilen resimden damgalanan filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.5.'te verilmiştir. Şekil 5.9.'da elde edilen damgalanmış ve kırpılmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.5. (0.1) α değeriyle damgalanmış ve kırpılmış lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.6721	0.6579	0.6729	0.6851



Şekil 5.9. (0.1) α değeriyle damgalanmış Lena resmi üzerine kırpma işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları inceliğinde, damgalanmış resme kırpma işlemi uygulandığında, resmin bütün (DD1, DY1, YD1 ve YY1) alt-bantları yaklaşık

olarak aynı NK değerine sahiptir. Önerilen damgalama algoritması uygulanmış resmin bütün alt bantlarında damgalanan filigranlar, kırpma işlemine karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bandında damgalanan filigran, kırpma işlemine karşı dayanıklıdır. Blok kırpma kodlamasının ayırık dalgacık dönüşümüyle bir arada kullanılması, önerilen damgalama algoritmasının dayanıklılık yeteneğini arttırmaktadır.

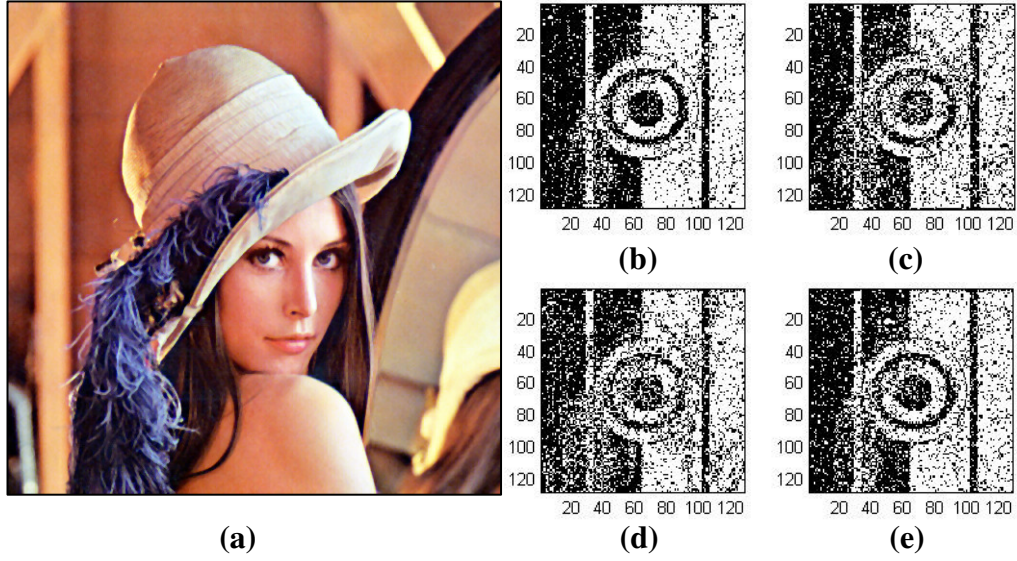
5.4.6. Filtreleme

Filtreleme işlemi aslında damgalanmış resmin kalitesini yükseltmek için kullanılan bir işlemdir. Fakat bu işlem damgalanmış resmin kalitesini yükselttiğinde, damgalanan filigrana büyük ölçüde zarar verebilir. Genellikle en çok kullanılan ortanca, düşük-geçiren DGF ve yüksek-geçiren YGF filtreleridir. Ortanca filtresi resimdeki gürültüyü yok etmek için kullanılır. DGF'de, Haar ADD'de açıklandığı gibi, resmin düşük frekansları resmin yüksek frekanslarından ayrılır. Böylece elde edilen resim daha düz ve yumuşak olur. YGF'de de, Haar ADD'de açıklandığı gibi, resmin yüksek frekansları resmin düşük frekanslarından ayrılır. Böylece elde edilen resim daha keskin olur.

Önerilen damgalama algoritmasının, filtreleme işlemine karşı dayanıklı olup olmadığını test etmek için XnView ve Adobe Photoshop yazılımları kullanılarak damgalanmış Lena resminin üzerine filtreleme işlemi uygulanmıştır. Damgalanmış lena resminin üzerine ortanca filtresi ile 3×3 boyutta uygulanması için XnView yazılımı kullanılmıştır. Elde edilen Lena resminden çıkarılmış filigranların NK sonuçları çizelge 5.6.'te verilmiştir. Şekil 5.10.'da elde edilen damgalanmış ve üzerine ortanca filtresi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.6. (0.1) α değeriyle damgalanmış ve üzerine ortanca filtresi uygulanan lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.8697	0.7755	0.7983	0.8348



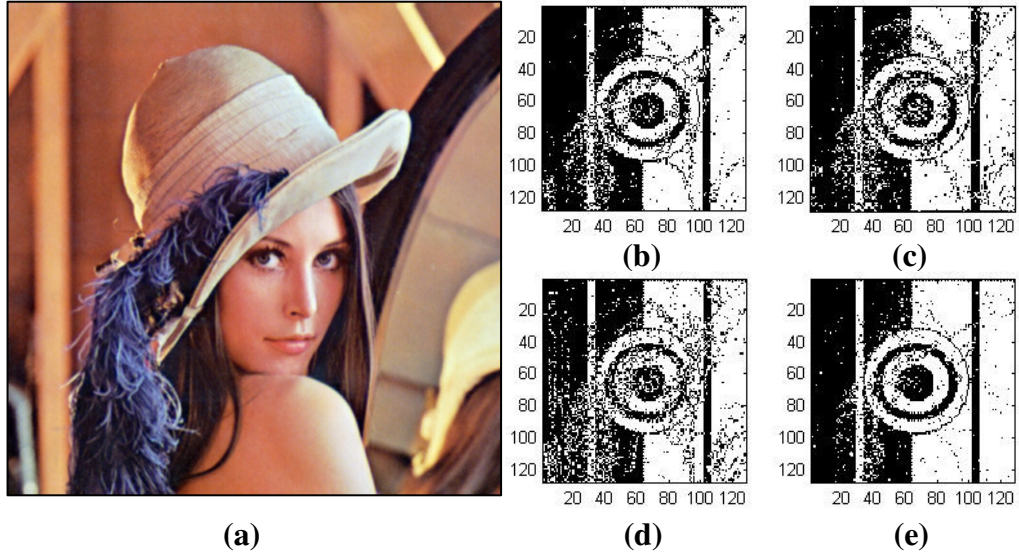
Şekil 5.10. (0.1) α değeriyle damgalanmış Lena resminin üzerine ortanca filtresi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelendiğinde, damgalanmış Lena resmine ortanca filtresi uygulandığında, resmin (DD1 ve YY1) alt-bantları resmin diğer (DY1 ve YD1) alt-bantlarından daha yüksek NK değerlerine sahip olmuşlardır. Önerilen damgalama algoritması uygulanmış resmin bütün (DD1, DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, ortanca filtreleme işlemine karşı dayanıklıdır. Blok kırpma kodlamasının ayrık dalgacık dönüşümüyle bir arada kullanması önerilen damgalama algoritmasına yeni bir dayanıklılık yeteneği katmaktadır.

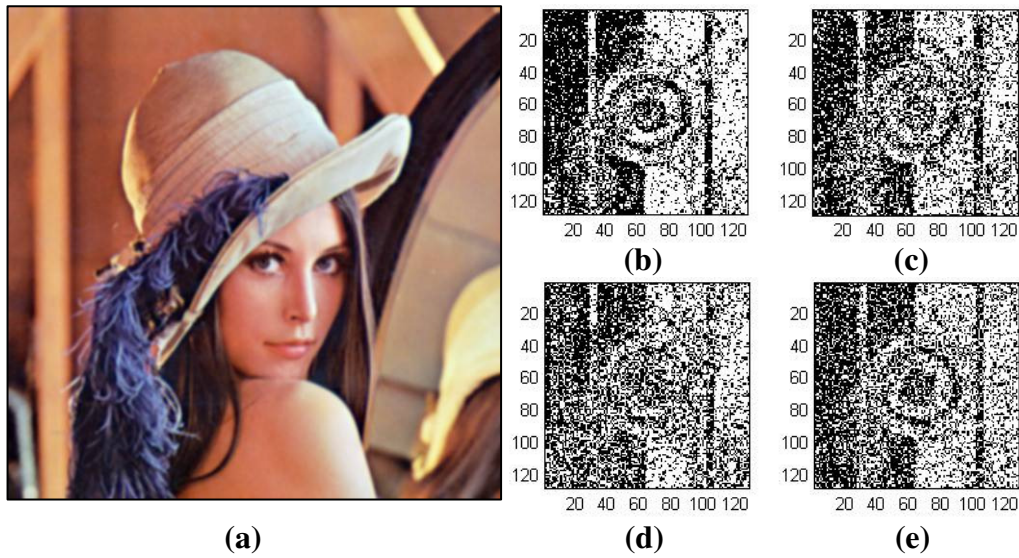
Damgalanmış lena resminin üzerine DGF uygulamak için Gauss bulandırması 3×3 ve 5×5 boyutlarında kullanılmıştır. Elde edilen Lena resminden çıkarılmış filigranların NK sonuçları çizelge 5.7.'de verilmiştir. Şekil 5.11.'de damgalanmış Lena resmi üzerine Gauss bulandırması 3×3 boyutlarda DGF uygulandıktan sonra ve çıkarılmış filigranlar gösterilmektedir. Şekil 5.12.'de damgalanmış Lena resmi üzerine Gauss bulandırması 5×5 boyutlarda DGF uygulandıktan sonra ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.7. (0.1) α değeriyle damgalanmış ve üzerine DGF uygulanan lena resminden çıkarılmış filigranların NK sonuçları

Gauss Bulandırma Boyutu	DD1	DY1	YD1	YY1
3×3	0.9071	0.8503	0.8886	0.9522
5×5	0.7694	0.6568	0.6895	0.6999



Şekil 5.11. (0.1) α değeriyle damgalanmış Lena resminin üzerine Gauss bulandırması 3×3 boyutlarıyla DGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran



Şekil 5.12. (0.1) α değeriyle damgalanmış Lena resminin üzerine Gauss bulandırması 5×5 boyutlarıyla DGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmine Gauss bulandırması 3×3 boyutlarında resmin üzerine uygulandığında resmin (DD1 ve YY1) alt-bantlarının diğer (DY1 ve YD1) alt-bantlarından daha yüksek NK değerlerine sahip oldukları görülmektedir. Fakat Gauss bulandırması 5×5 boyutlarında resmin üzerine uygulandığında, resmin (DD1) alt-bantının diğer (DY1, YD1 ve YY1) alt-bantlarından daha yüksek NK değerine sahip olduğu görülmektedir. Diğer alt-bantların ise NK değerleri yaklaşık olarak birbirine eşittir. Önerilen damgalama algoritması uygulanan resmin bütün alt-bantlarında damgalanan filigranlar, DGF işlemine karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bandında damgalanan filigran, DGF işlemine karşı dayanıklıdır. Blok kırpma kodlamasının ayrık dalgacık dönüşümüyle bir arada kullanması, önerilen damgalama algoritmasına yeni bir dayanıklılık yeteneği katmaktadır.

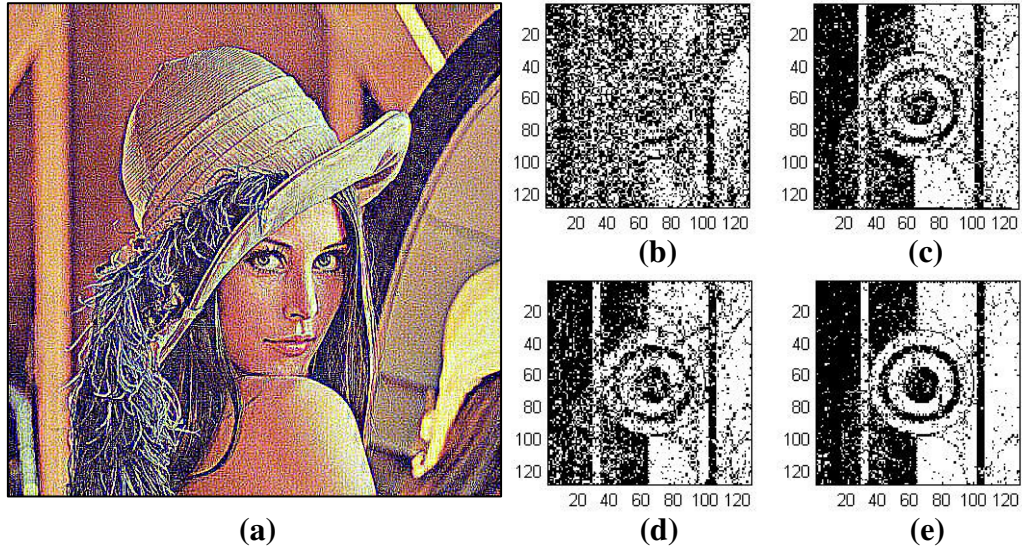
Damgalanmış resmin üzerine YGF işlemi uygulamak için XnView yazılımı kullanılarak, damgalanmış Lena resminin üzerine %95 oranla keskinleştirme işlemi uygulanmıştır. Elde edilen Lena resminden çıkarılmış filigranların NK sonuçları çizelge 5.8.'de verilmiştir. Şekil 5.13.'te elde edilen damgalanmış ve üzerine YGF uygulanan Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.8. (0.1) α değeriyle damgalanmış ve üzerine YGF uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.6370	0.8098	0.8344	0.9089

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmine YGF işlemi uygulandığında, resmin (YY1) alt-bantının, diğer (DD1, DY1 ve YD1) alt-bantlarından daha yüksek bir NK değerine sahip olduğu görülmektedir. Fakat (DY1 ve YD1) alt-bantlarının NK değerleri yaklaşık olarak eşittir. Önerilen damgalama algoritması uygulanmış resmin bütün alt-bantlarında damgalanan filigranlar, YGF işlemine karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bandında damgalanan filigranı, YGF

işlemine karşı dayanıklı kılmaktadır. Blok kırpma kodlamasının ayırık dalgacık dönüşümüyle bir arada kullanılması, önerilen damgalama algoritmasına yeni bir dayanıklılık yeteneği katmaktadır.



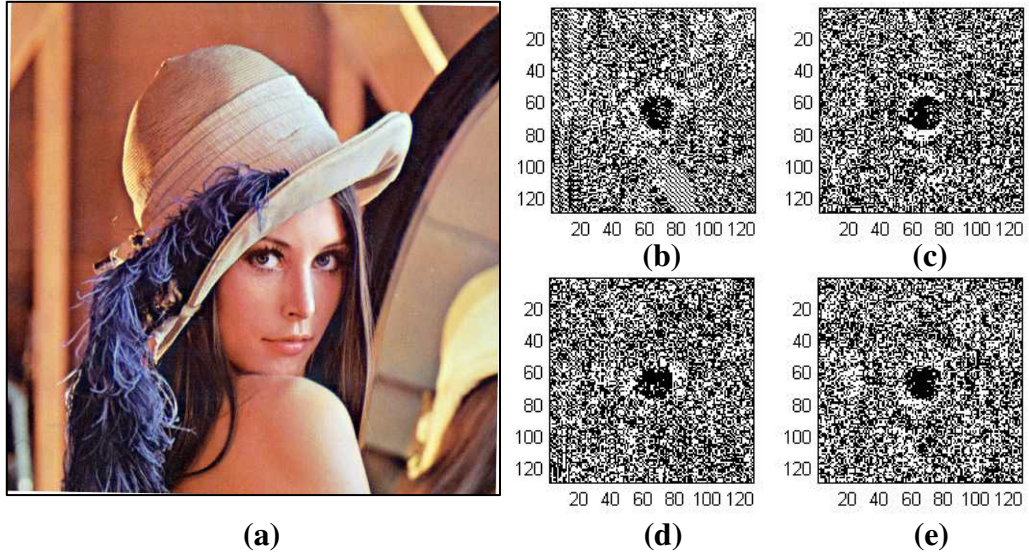
Şekil 5.13. (0.1) α değeriyle damgalanmış Lena resmi üzerine %95 oranla keskinleştirme YGF uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

5.4.7. Döndürme İşlemi

Damgalanmış resimlere uygulanan geometrik saldırılardan birisi de, açılı döndürme işlemidir. Bu tür saldırının damgalanmış resmin kalitesine bir etkisi yoktur. Fakat damgalanan filigranın yok olmasına neden olabilir. Önerilen damgalama algoritmasının bu tür saldırıya dayanıklılığını test etmek için, (0.1) α değeriyle damgalanmış Lena resminin üzerine, Adobe Photoshop yazılımı kullanılarak, 1° saat yönünde döndürme işlemi uygulanmıştır. Ardından elde edilen resimden damgalanan filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.9.'da verilmiştir. Şekil 5.14.'te elde edilen damgalanmış ve üzerine döndürme işlemi uygulanan Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.9. (0.1) α değeriyle damgalanmış ve üzerine döndürme işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.5457	0.5050	0.5050	0.4890



Şekil 5.14. (0.1) α değeriyle damgalanmış Lena resmin üzerine 1 saat yönünde döndürme uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

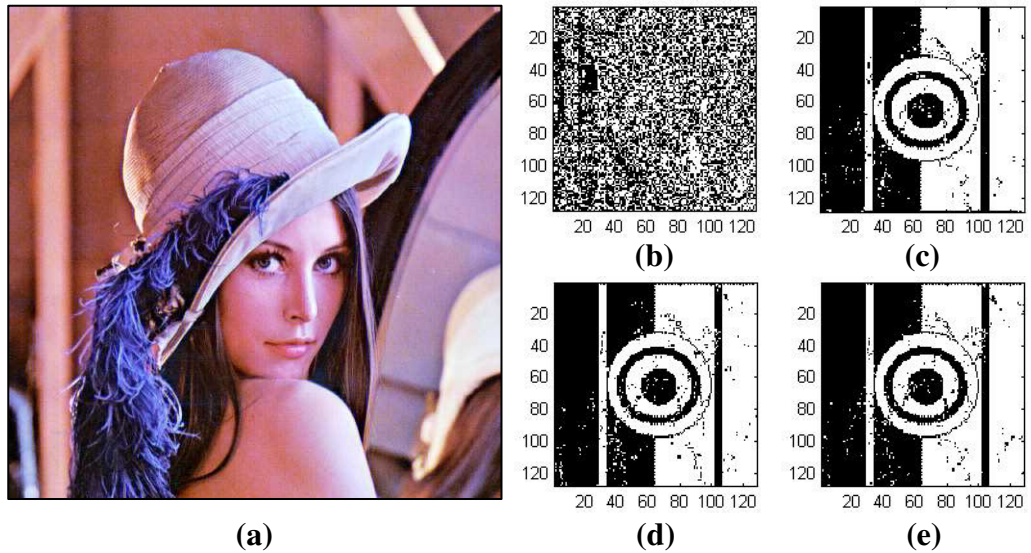
Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmine 1° saat yönünde döndürme işlemi uygulandığında, resmin (DD1) alt-bandının diğer (DY1, YD1 ve YY1) alt-bantlarından daha yüksek bir NK değerine sahip olduğu görülmektedir. Önerilen damgalama algoritması uygulanan resmin bütün alt-bantlarında damgalanan filigranlar, döndürme işlemine karşı yüksek dayanıklılık derecesine sahip değildirler. Çünkü 1° saat yönünde döndürme işlemi uygulandığında, neredeyse damgalanmış filigranlar yok olmaktadır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bandında damgalanan filigran, döndürme işlemine karşı dayanıklıdır.

5.4.8. Histogram Eşitleme

Resim üzerine histogram eşitleme işlemi uygulandığında, resmin kontrastını artırır. Histogram eşitleme işlemi, resmin histogram değerlerini eşit bir şekilde dağıtır. Damgalanmış resme uygulanan saldırılardan birisi de histogram eşitleme saldırısıdır. Önerilen damgalama algoritmasını bu tür saldırıya karşı dayanıklı olup olmadığını test etmek için (0.1) α değeriyle damgalanmış Lena resmi üzerine Matlab kullanarak, histogram eşitleme işlemi uygulanmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.10.'da verilmiştir. Şekil 5.15.'te elde edilen damgalanmış ve üzerine histogram eşitleme işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.10. (0.1) α değeriyle damgalanmış ve üzerine histogram eşitleme işlemi uygulanmış Lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.5335	0.9681	0.9751	0.9704



Şekil 5.15. (0.1) α değeriyle damgalanmış Lena resminin üzerine histogram eşitleme işlemi uygulandıktan sonra, (a) Lena resmi (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelediğinde, damgalanmış resme histogram eşitleme işlemi uygulandığında, resmin (DY1, YD1 ve YY1) alt-bantları yüksek bir NK değerine sahiptirler. Fakat (DD1) alt-bandında damgalanan filigran yok olmuştur. Önerilen damgalama algoritması, resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, histogram eşitleme işlemine karşı yüksek bir seviyede dayanıklılığa sahiptirler. Fakat [32]'de önerilen damgalama algoritmasında, resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, histogram eşitleme işlemine karşı orta derecede bir dayanıklılık seviyesine sahiptirler.

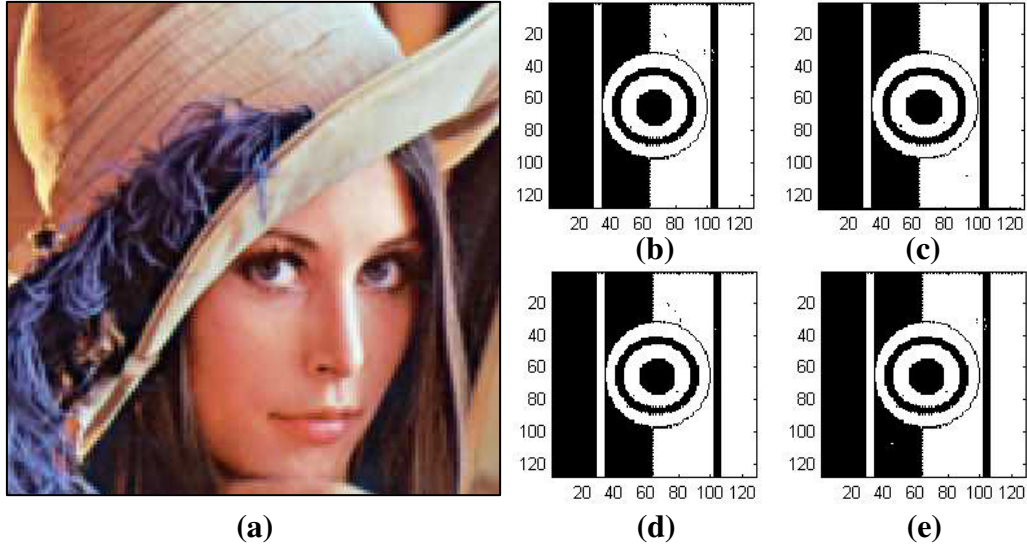
5.4.9. Mozaik İşlemi

Resmi verilen blok değerine göre bloklara böler ve her bloğa tek bir renk yaparak resmi mozaikten yapılmış gibi bir görünüme kavuşturur. Bu tür işlemler damgalanmış resmin piksel değerlerini değiştirirler. Böylece resimde damgalanan filigranın yok olmasına neden olur. Önerilen damgalama algoritmasının, bu tür işleme dayanıklı olup olmadığını test etmek için Adobe Photoshop yazılımı kullanılarak, damgalanmış resmin üzerine, 2 ve 3 blok değeriyle mozaik işlemi uygulanmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.11.'de verilmiştir. Şekil 5.16.'da elde edilen damgalanmış ve üzerine 2 blok değeriyle mozaik işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir. Şekil 5.17.'de elde edilen damgalanmış ve üzerine 3 blok değeriyle mozaik işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

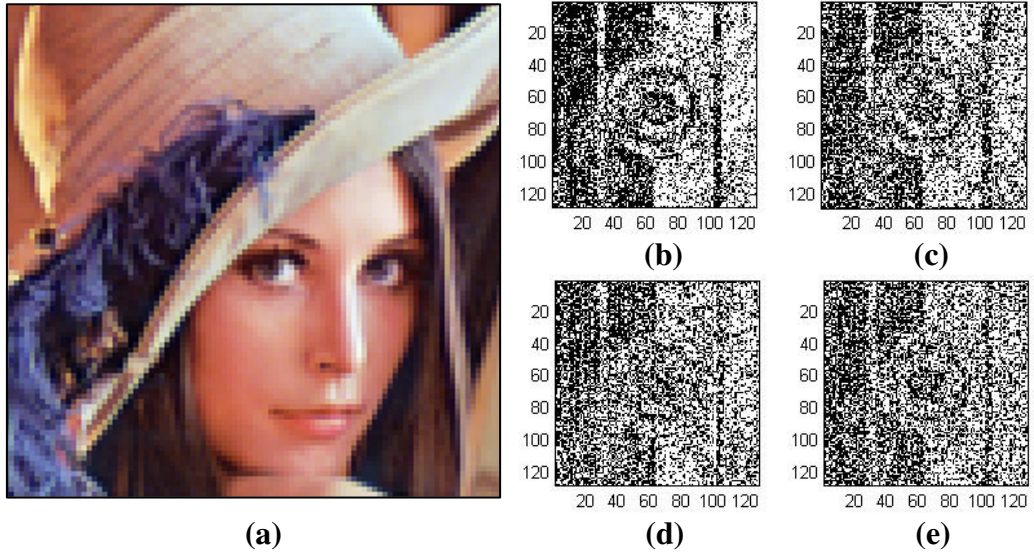
Çizelge 5.11. (0.1) α değeriyle damgalanmış ve üzerine 2 ve 3 blok değeriyle mozaik işlemi uygulanmış Lena resminden çıkarılmış filigranların NK sonuçları

Blok Değeri	DD1	DY1	YD1	YY1
2	0.9991	0.9990	0.9995	0.9992
3	0.7165	0.6426	0.6572	0.6298

Elde edilen NK sonuçları incelediğinde, damgalanmış resme 2 blok değeriyle mozaik işlemi uygulandığında, resmin bütün alt-bantları yüksek ve eşit NK değerlerine sahip oldukları görülmektedir. Fakat mozaik işlemi 3 blok değeriyle uygulandığında, (DD1) alt-bantının NK değeri, resmin diğer alt-bantlarının değerlerinden daha yüksektir. Önerilen damgalama algoritması uygulanmış resmin (DY1, DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, 2 ve 3 blok değerinde mozaik işlemine karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, resmin bütün alt-bantlarında damgalanan filigranlar, 2 blok değerinde mozaik işlemine karşı dayanıklıdır.



Şekil 5.16. (0.1) α değeriyle damgalanmış Lena resmin üzerine 2 blok değeriyle mozaik işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran



Şekil 5.17. (0.1) α değeriyle damgalanmış Lena resmin üzerine 3 blok değeriyle mozaik işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

5.4.10. Gama Düzeltme İşlemi

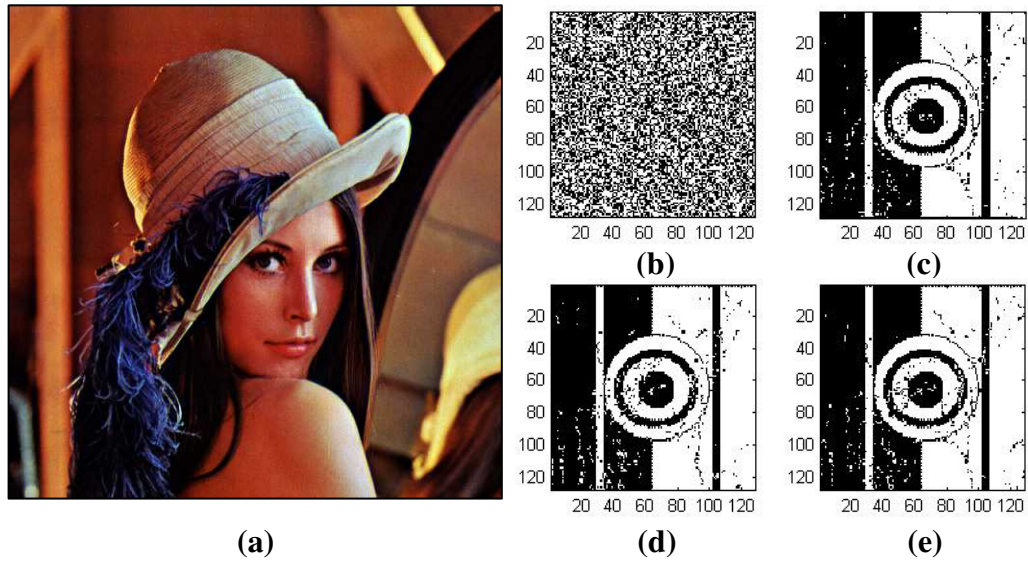
Resmin üzerine gama düzeltme işlemi uygulandığında, elde edilen resmin parlaklık derecesi daha yüksek olacaktır. Bu işlem gama değerine bağlıdır. Gamanın saptanmış değeri 1'dir. Eğer gama değeri 1'den yüksek ise, resmin parlaklığı da daha yüksek olacaktır. Aksi halde resmin parlaklık seviyesi daha az olacaktır.

Önerilen damgalama algoritmasının bu işleme dayanıklı olup olmadığını test etmek için XnView yazılımı kullanılarak, resmin üzerine 0.5 ve (en yüksek değer) 5 gama değeriyle gama düzeltme işlemi uygulanmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.12.'de verilmiştir. Şekil 5.18.'de elde edilen damgalanmış ve üzerine 0.5 gama değeriyle gama düzeltme işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir. Şekil 5.19.'da elde edilen damgalanmış ve üzerine 5 gama değeriyle gama düzeltme işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

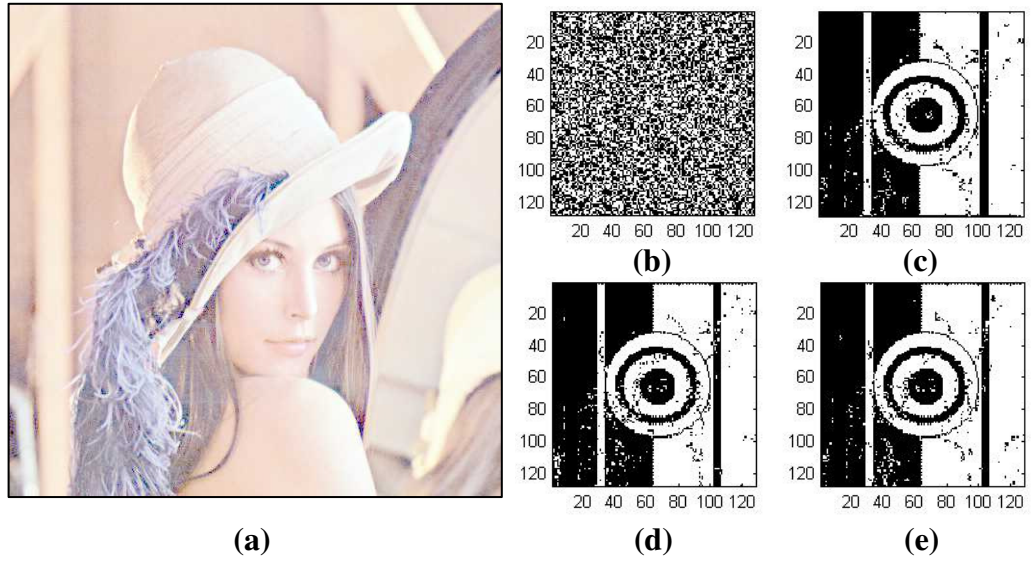
Çizelge 5.12. (0.1) α değeriyle damgalanmış ve üzerine 0.5 ve 5 gama değeriyle gama düzeltme işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

Gama değeri	DD1	DY1	YD1	YY1
0.5	0.5073	0.9689	0.9677	0.9697
5	0.4927	0.9664	0.9678	0.9681

Elde edilen NK sonuçları incelediğinde, damgalanmış resme 0.5 ve 5 gama değerleriyle gama işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigran yok olmuştur. Fakat resmin diğer (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar hem yüksek NK değerlerine sahiptirler hem de yüksek derecede bu işleme karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, resmin sadece (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigran, 1.5 gama değerinde gama düzeltme işlemi uygulandığında, (DY1, YD1 ve YY1) alt-bantlarının NK değerleri sırasıyla (0.828, 0.782 ve 0.888) olmuştur ve (DD1) alt-bandında damgalanan filigran yok olmuştur.



Şekil 5.18. (0.1) α değeriyle damgalanmış Lena resmin üzerine 0.5 gama değeriyle gama düzeltme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran



Şekil 5.19. (0.1) α değeriyle damgalanmış Lena resmin üzerine 5 gama değeriyle gama düzeltme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

5.4.11. Kontrast Ayarlama İşlemi

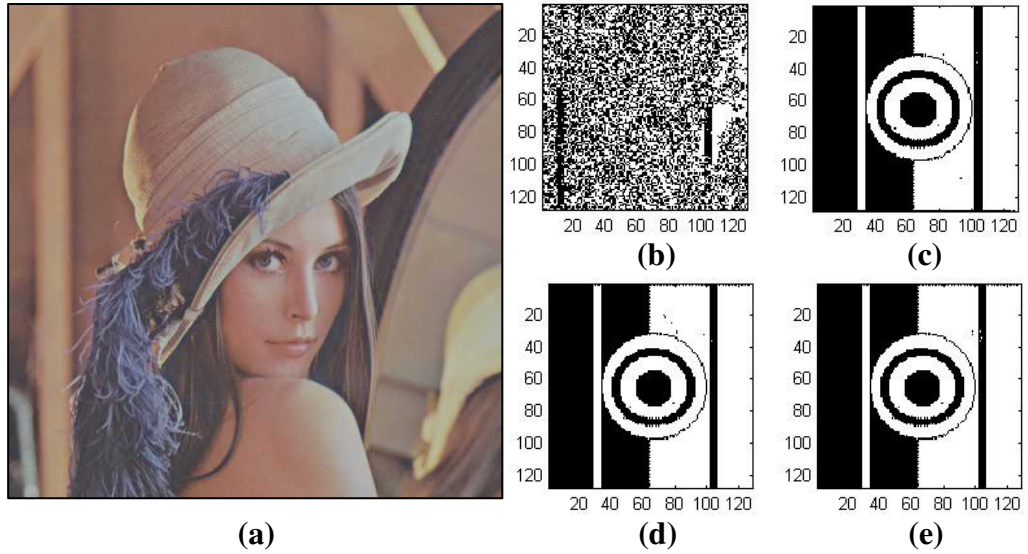
Bu işlem resmin kontrastını yükseltmek veya azaltmak için kullanılır. Eğer bu işleme verilen değer pozitifse, o zaman resmin kontrastı artacaktır. Fakat verilen değer negatifse, o zaman resmin kontrastı azalacaktır. Bu işlem resmin üzerine uygulandığı zaman resimde damgalanan filigranın yok olmasına neden olabilir.

Önerilen damgalama algoritmasının bu işleme dayanıklı olup olmadığını test etmek için Adobe Photoshop yazılımı kullanılarak resmin üzerine -50 ve +05 değerleriyle kontrast işlemi uygulanmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.13.'de verilmiştir. Şekil 5.20.'de elde edilen damgalanmış ve üzerine -50 değeriyle kontrast işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir. Şekil 5.21.'de elde edilen damgalanmış ve üzerine +05 değeriyle kontrast işlemi uygulanmış Lena resmi ve çıkarılmış filigranlar gösterilmektedir.

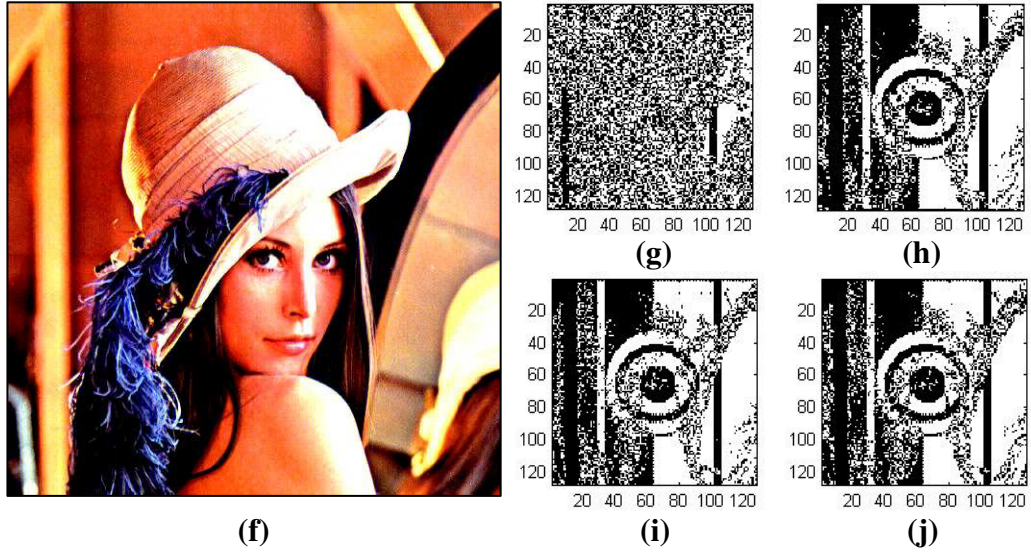
Çizelge 5.13. (0.1) α değeriyle damgalanmış ve üzerine -50 ve +50 değerleriyle kontrast işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

Kontrast Değeri	DD1	DY1	YD1	YY1
-50	0.5187	0.9990	0.9994	0.9991
+50	0.5648	0.8491	0.8496	0.8479

Elde edilen NK sonuçları incelediğinde, damgalanmış resme -05 ve +05 değeriyle kontrast işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigran yok olmuştur. Fakat diğer (DY1, YD1 ve YY1) alt-bantlarda damgalanan filigranlar hem yüksek NK değerlerine sahiptirler hem de yüksek derecede bu işleme karşı dayanıklıdır.



Şekil 5.20. (0.1) α değeriyle damgalanmış Lena resmi üzerine -05 değeriyle kontrast işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran



Şekil 5.21. (0.1) α değeriyle damgalanmış Lena resmi üzerine +05 değeriyle kontrast işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

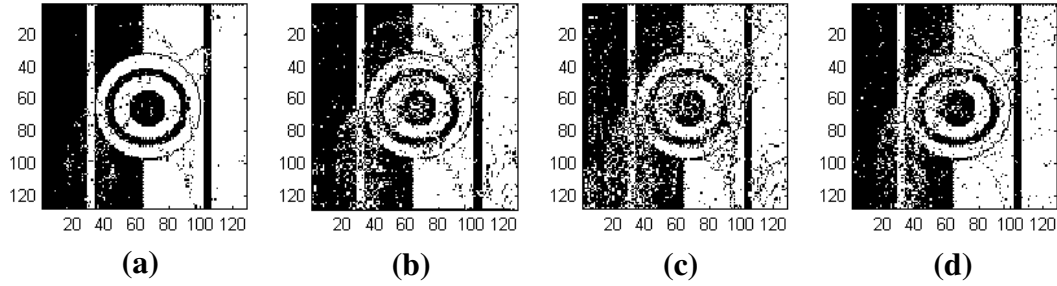
5.4.12. Ölçekleme İşlemi

Bu durum kağıda basılmış bir resmin, bir tarayıcıda taranması ya da Internet'te yayınlanmak üzere resmin çözünürlüğünün azaltılmasıyla yapılır. Ölçekleme, yatay ve dikey yönde aynı oranda yapılan ölçekleme ile farklı oranlarda yapılan ölçekleme olarak iki gruba ayrılır. Birçok dijital damgalama algoritması aynı oranda yapılan ölçeklemeye karşı dayanıklıdır.

Önerilen damgalama algoritmasının, bu tür işleme karşı dayanıklı olup olmadığını test etmek için, XnView yazılımı kullanılarak damgalanmış Lena resmine (512×512) boyutlarından (256×256) boyutlarına ölçekleme işlemi uygulanmıştır. Elde edilen resimden filigran çıkarma işlemi uygulanmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.22.'de verilmiştir. Şekil 5.19.'da elde edilen damgalanmış ve ölçeklenmiş Lena resminden çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.14. (0.1) α değeriyle damgalanmış ve üzerine ölçekleme işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

DD1	DY1	YD1	YY1
0.9709	0.8676	0.9045	0.9303

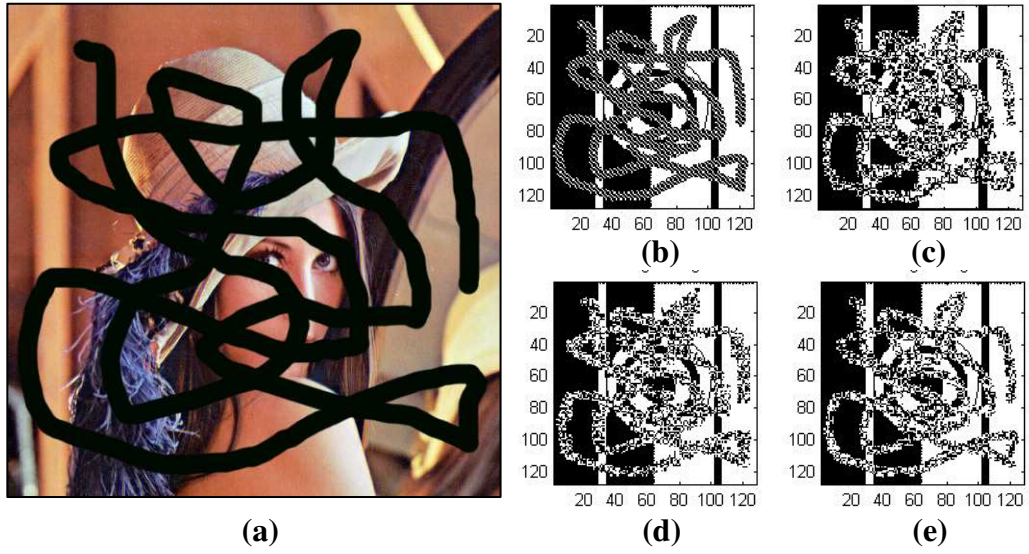


Şekil 5.22. (0.1) α değeriyle damgalanmış ve 256×256 boyutlarında ölçeklenmiş Lena resminden çıkarılmış filigranlar (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmine ölçekleme işlemi uygulandığında, resmin bütün alt-bantları bu işleme karşı dayanıklıdır. Fakat [32]'de önerilen damgalama algoritmasında, sadece resmin (DD1) alt-bantında damgalanan filigran bu işleme karşı dayanıklı olmuştur. Blok kırpma kodlamasının ayırık dalgacık dönüşümüyle bir arada kullanılması, önerilen damgalama algoritmasına yeni bir dayanıklılık yeteneği katmaktadır.

5.4.13. Rastgele Çizme

Adobe Photoshop yazılımında 20 piksel değerinde çizme fırçası kullanılarak, damgalanmış Lena resminin üzerine rastgele bir şekilde siyah bir çizgi çizilmiştir. Elde edilen resim ve resimden çıkarılmış filigranlar şekil 5.23.'te gösterilmiştir. Damgalanmış Lena resmi üzerine rastgele çizim yapıldığında, çizilen çizim hem resmi hem de damgalanan filigranları aynı oranda etkilemektedir.



Şekil 5.23. (0.1) α değeriyle damgalanmış Lena resmin üzerine rastgele çizgi çizmek, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

5.4.14. Sahte Filigran Ekleme Saldırısı

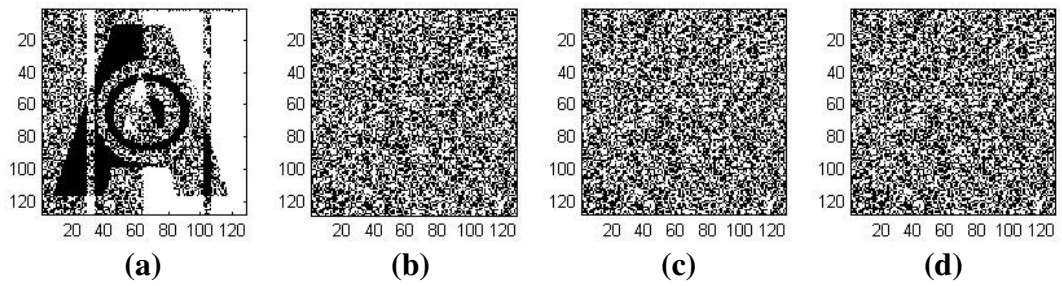
Önerilen damgalama algoritmasının bu tür saldırıya karşı dayanıklı olup olmadığını test etmek için (0.1) α değeriyle ve (123) değeriyle gizli anahtar kullanılarak, damgalanmış Lena resmine, aynı gizli anahtar ve farklı (12345) gizli anahtar kullanarak, fakat farklı filigranla tekrar damgalama işlemi uygulanmıştır. Elde edilen resimden birinci damgalanan filigranı çıkarmak için filigran çıkarma işlemi uygulanmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.15.'te verilmiştir. İkinci damgalama işleminde kullanılan filigran şekil 5.24.'te gösterilmektedir. Aynı gizli anahtar kullanılarak, tekrar damgalanmış resimden çıkarılmış filigranlar şekil 5.25.'te gösterilmiştir. Farklı gizli anahtar kullanılarak, tekrar damgalanmış resimden çıkarılmış filigranlar şekil 5.26.'da gösterilmiştir.

Çizelge 5.15. (0.1) α değeriyle damgalanmış ve üzerine aynı ve farklı gizli anahtar kullanarak tekrar üzerine damgalama işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

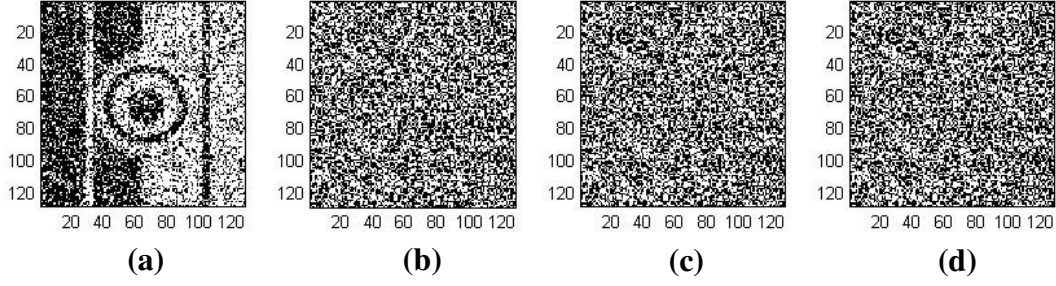
Aynı Gizli Anahtar Kullanarak				
Gizli Anahtar Değeri	DD1	DY1	YD1	YY1
123	0.7811	0.5083	0.5082	0.5081
Farklı Gizli Anahtar Kullanarak				
Gizli Anahtar Değeri	DD1	DY1	YD1	YY1
123, 12345	0.7390	0.4884	0.4889	0.4889



Şekil 5.24. İkinci damgalama işleminde kullanılan filigran



Şekil 5.25. (0.1) α değeriyle ve aynı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran



Şekil 5.26. (0.1) α değeriyle ve farklı gizli anahtarlar tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran

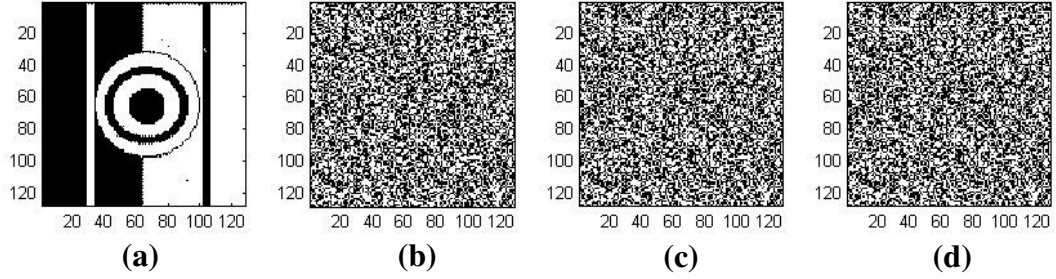
Elde edilen NK sonuçları incelediğinde, damgalanmış resme farklı filigran kullanarak, tekrar damgalama işlemi uygulandığında, resmin sadece (DD1) alt-bandı bu işleme karşı dayanıklıdır. Fakat diğer alt-bantlarda damgalanan filigranlar yok olmuştur. Bunun nedeni, birden fazla filigran permütasyon işlemi uygulanmasıdır.

5.4.15. Filigran Çarpıştırma Saldırısı

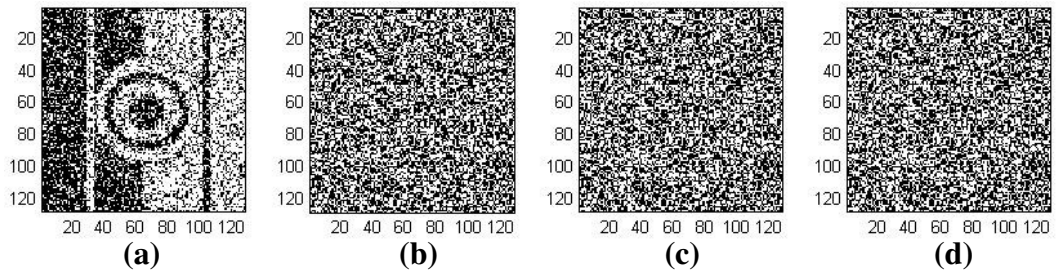
Bu tür saldırıda, damgalama işleminde kullanılan filigran, ikinci kez aynı resmi damgalamak için kullanılır. Böylece resmin birinci damgalama işleminde damgalanan filigran, ikinci damgalama işleminde damgalanan filigranla çarpışır. Böylece resimde damgalanan filigranın yok olmasına neden olur. Önerilen damgalama algoritmasının bu tür saldırıya karşı dayanıklı olup olmadığını test etmek için, aynı filigran resme iki kez damgalanmıştır. Fakat bu damgalama işlemi iki defa ayrı ayrı uygulanmıştır. Birincide, aynı gizli anahtar, ikincisinde farklı gizli anahtar kullanılmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.16.'da verilmiştir. Şekil 5.27.'de aynı gizli anahtarı kullanarak iki kez üzerine damgalama işlemi uygulanan resimden çıkarılmış filigranlar gösterilmektedir. Şekil 5.28.'de farklı gizli anahtar kullanarak iki kez üzerine damgalama işlemi uygulanan resimden çıkarılmış filigranlar gösterilmektedir.

Çizelge 5.16. (0.1) α değeriyle damgalanmış ve üzerine aynı ve farklı gizli anahtarlar kullanarak üzerine tekrar damgalama işlemi uygulanan Lena resminden çıkarılmış filigranların NK sonuçları

Aynı Gizli Anahtar Kullanarak				
Gizli Anahtar Değeri	DD1	DY1	YD1	YY1
12	0.9994	0.5077	0.5083	0.5082
Farklı Gizli Anahtar Kullanarak				
Gizli Anahtar Değeri	DD1	DY1	YD1	YY1
12, 12345	0.7395	0.4898	0.4899	0.4899



Şekil 5.27. (0.1) α değeriyle ve aynı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran



Şekil 5.28. (0.1) α değeriyle ve farklı gizli anahtarla tekrar damgalanan Lena resminden çıkarılmış filigranlar, (a) DD1'den çıkarılmış filigran, (b) DY1'den çıkarılmış filigran, (c) YD1'den çıkarılmış filigran, (d) YY1'den çıkarılmış filigran,

Elde edilen NK sonuçları incelediğinde, damgalanmış resme aynı filigran ve aynı gizli anahtarı kullanarak, tekrar damgalama işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigranda hiçbir değişiklik olmamıştır. Fakat resmin diğer alt-bantlarında damgalanan filigranlar yok olmuşlardır. Fakat damgalanmış resme aynı filigran ancak farklı gizli anahtarı kullanarak, tekrar damgalama işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigranda değişiklik olmuştur ve diğer alt-bantlarda damgalanan filigranlar yok olmuşlardır. Bunun nedeni, birden fazla filigran permütasyon işleminin kullanmasıdır. Fakat [32]'de önerilen damgalama algoritmasının, filigran çarpıştırma saldırısına karşı hiçbir dayanıklılığı olmamıştır.

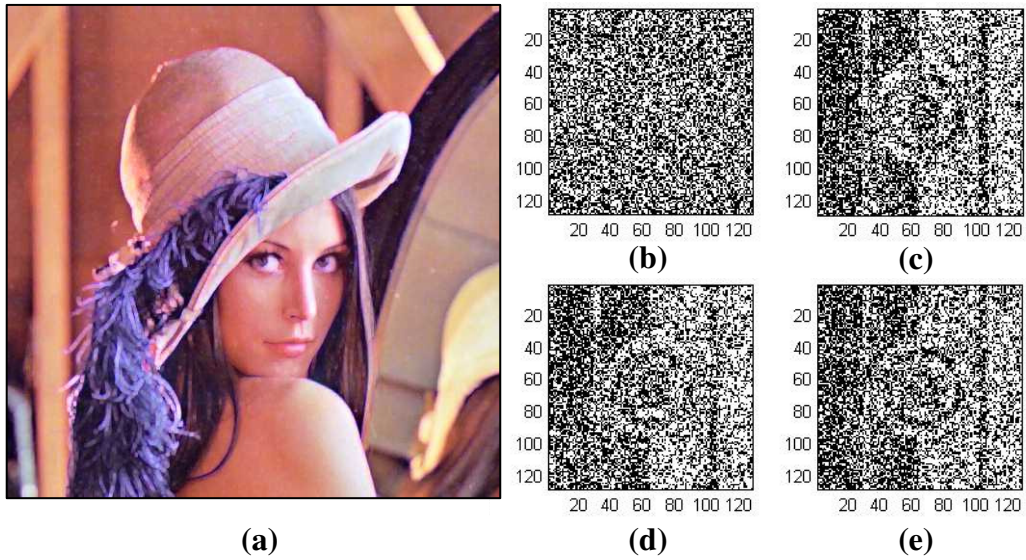
5.4.16. Morfolojik İşlemler

Genişleme ve aşındırma işlemleri, morfolojiksel işlemlerin temelidir. Genişleme işlemi, resimdeki objelerin kenarlarına pikseller eklemek için kullanılır. Aşındırma işlemi ise, resimdeki objelerin kenarlarından pikselleri silmek için kullanılır. Resimdeki objelere eklenecek ve objelerden silinecek piksellerin sayısı, resim işlenmesinde kullanılan yapı elementinin boyutuna ve şekline dayalıdır.

Önerilen damgalama algoritmasının bu tür işlemlere karşı dayanıklı olup olmadığını test etmek için, damgalanmış Lena resmi üzerine hem genişleme hem de aşındırma işlemi, 3×3 yapı elementi boyutuyla uygulanmıştır. Elde edilen resimden filigranlar çıkarılmıştır. Çıkarılmış filigranların NK sonuçları çizelge 5.17.'de verilmiştir. Şekil 5.29.'da damgalanmış Lena resmi üzerine genişleme işlemi uygulandıktan sonra resimden çıkarılmış filigranlar gösterilmektedir. Şekil 5.30.'da damgalanmış Lena resmi üzerine aşındırma işlemi uygulandıktan sonra resimden çıkarılmış filigranlar gösterilmektedir.

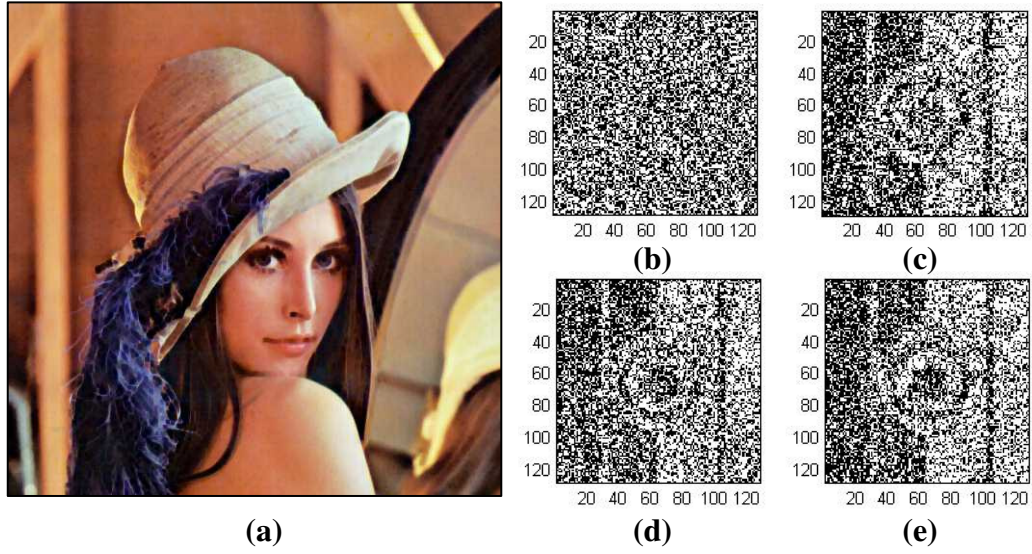
Çizelge 5.17. (0.1) α değeriyle damgalanmış ve üzerine genişleme ve aşındırma işlemleri uygulandıktan sonra Lena resminden çıkarılmış filigranların NK sonuçları

Genişleme İşlemi				
Yapı Elementin Boyutu	DD1	DY1	YD1	YY1
3×3	0.4929	0.6395	0.6559	0.6231
Aşındırma İşlemi				
Yapı Elementin Boyutu	DD1	DY1	YD1	YY1
3×3	0.5076	0.6342	0.6604	0.6624



Şekil 5.29. (0.1) α değeriyle damgalanmış Lena resmi üzerine genişleme işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmi üzerine genişleme işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigran yok olmuştur. Fakat resmin diğer (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranların hem NK değerleri eşit hem de genişleme işlemine karşı dayanıklıdır.



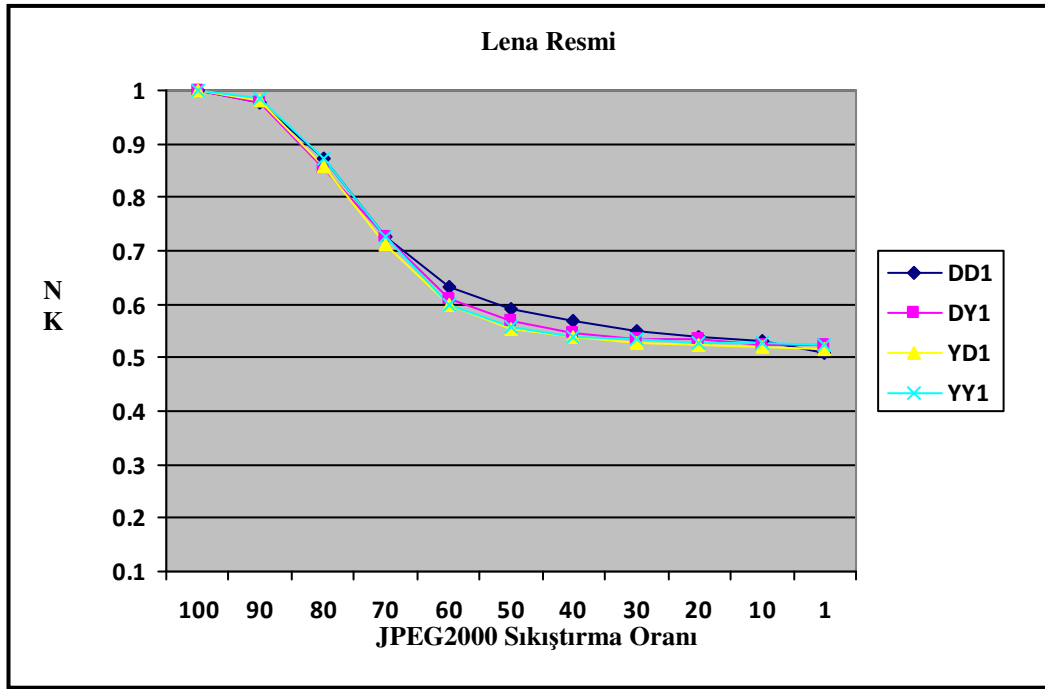
Şekil 5.30. (0.1) α değeriyle damgalanmış Lena resmi üzerine aşındırma işlemi uygulandıktan sonra, (a) Lena resmi, (b) DD1'den çıkarılmış filigran, (c) DY1'den çıkarılmış filigran, (d) YD1'den çıkarılmış filigran, (e) YY1'den çıkarılmış filigran

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmi üzerine aşındırma işlemi uygulandığında, resmin (DD1) alt-bandında damgalanan filigran yok olmuştur. Fakat resmin diğer (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranların hem NK değerleri eşit hem de genişleme işlemine karşı dayanıklıdır.

5.4.17. JPEG2000 Kayıplı Sıkıştırması

JPEG2000 de JPEG gibi (Joint Photographic Experts Group) adlı komite tarafından geliştirilmiştir [33]. Ayrık dalgacık dönüşümü teknolojisini temel olarak, bilinen en iyi sıkıştırma teknolojilerinin kullanılmasıyla oluşturulmuş bir kodlama sistemidir. JPEG standardının kısıtlamalarını gidermek ve düşük bit-oranlarında yüksek kalitede resimler elde etmek amacıyla tasarlanmıştır. ADD teknolojisinin avantajı sayesinde, Ayrık Kosinüs Dönüşümü'nde olduğu gibi sadece kayıplı sıkıştırma değil, kayıpsız sıkıştırma da yapabilmektedir. Ayrıca JPEG2000, istemci/sunucu resim uygulamaları için ve sınırlı kaynağa sahip olan kablosuz cihazlar için ilave fonksiyonel özelliklere sahiptir.

Önerilen damgalama algoritmasının bu tür sıkıştırma metoduna karşı dayanıklı olup olmadığını test etmek için (0.1) α değeriyle damgalanmış Lena resmi, XnView yazılımı kullanılarak 11 farklı oranda (%1-...-%100) sıkıştırılmıştır. Ardından, filigran çıkarma algoritması ile JPEG2000 kayıplı sıkıştırması uygulanan damgalanmış Lena resimden filigranlar çıkarılmıştır. Elde edilen filigranların orijinal filigrana benzerlikleri NK ile ölçülmüş, sonuçları grafik olarak şekil 5.31.'de gösterilmektedir.



Şekil 5.31. (0.1) α değeriyle damgalanmış Lena resmin JPEG2000 kayıplı sıkıştırması uygulandıktan sonra, resimden çıkarılmış filigranların NK sonuçları

Elde edilen NK sonuçları incelediğinde, damgalanmış Lena resmi üzerine (%1-...-%100) oranda JPEG2000 kayıplı sıkıştırması uygulandığında, resmin (DD1, DY1, YD1 ve YY1) alt-bantlarında damgalanan filigran hem NK değerleri eşit hem de JPEG2000 kayıplı sıkıştırmasına karşı dayanıklıdır. Önerilen damgalama algoritmasında ADD kullanıldığı için JPEG2000 kayıplı sıkıştırmasına karşı yüksek derecede dayanıklıdır.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, dijital renkli resimlerin telif haklarının korunması amacıyla yeni bir damgalama yöntemi önerilmiştir. Önerilen yöntemde damgalanacak resimlere görünmez dört filigran gömülür. Damgalanmış resimden damgalanan filigranları çıkarmak için filigran çıkarma algoritmasının orijinal resme ihtiyacı olduğu için önerilen damgalama yöntemi, kör olmayan damgalama yöntemi olarak adlandırılır.

Dayanıklı ve görünmez damgalama yöntemlerinin amacı, damgalanmış resme damgalanan filigranın çeşitli görüntü işlemelerine ve saldırılara karşı direncini arttırmaktır. Bu amaç çerçevesinde geliştirilen yöntem ile damgalanan filigranların dayanıklılığı JPEG kayıplı sıkıştırması, gürültü ekleme, kırpma, filtreleme, döndürme, histogram eşitleme, mozaik, gama düzeltme, kontrast ayarlama, ölçekleme, rastgele çizme, sahte filigran ekleme saldırısı, filigran çarpıştırma saldırısı, morfolojik işlemler ve JPEG2000 kayıplı sıkıştırması karşısında test edilmiştir.

Resimlerin damgalanmasında kullanılan damgalama güçlendirme değeri, damgalanmış resmin kalitesi ve filigranların dayanıklılığının, bazı saldırılara karşı sağlanmasında önemli bir rol oynamıştır. Damgalama güçlendirme değerinin artmasıyla birlikte damgalanmış resimdeki bozulmanın da arttığı tespit edilmiştir. Fakat önerilen damgalama yöntemi için en iyi damgalama güçlendirme değeri (0.1)'dir. Çünkü resme damgalanmış filigranların dayanıklılıklarını test etmek için bu değer, resimlerin damgalanmasında kullanılmıştır. Böylece bu değere, önerilen damgalama yöntemi için en iyi damgalama güçlendirme değeri denilebilir.

Damgalanmış resimlere damgalanan filigranlara, damgalama öncesinde gizli bir anahtar kullanılarak, permütasyon işlemi uygulanmıştır. Permütasyon işlemi ile her bir filigranın pikselleri rastgele dağıtılmış ve bununla damgalanmış resmin her bir alt-bandında rastgele dağılması amaçlanmıştır. Kırpma işlemi damgalanmış resmin üzerine uygulandığında, ardından çıkarılmış filigranlarda, resimden kırılan bölümünde yer alan filigran bilgisi kaybedilmiş, ancak kaybedilen bu bilgi, filigrana bir gürültü olarak yansımıştır. Kırılan bölümün büyüklüğü ile doğru orantılı olarak filigranda oluşan gürültü de artmıştır.

Blok kırpma kodlamasının, ayrık dalgacık dönüşümüyle bir arada kullanılması, ayrık dalgacık dönüşümüne dayalı damgalama algoritmalarının aşağıdaki dayanıklılık yeteneklerini artırmaktadır.

1. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, gürültü ekleme işlemine karşı dayanıklıdır.
2. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, kırpma işlemine karşı dayanıklıdır.
3. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, ortanca filtrelemesine karşı dayanıklıdır.
4. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, DGF filtrelemesine karşı dayanıklıdır.
5. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, YGF filtrelemesine karşı dayanıklıdır.
6. Damgalanmış resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, histogram eşitleme işlemine karşı yüksek bir dayanıklılık seviyesine sahiptirler.
7. Damgalanmış resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, 2 ve 3 blok değerinde mozaik işlemine karşı dayanıklıdır.
8. Damgalanmış resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, yüksek derecede gama düzeltme işlemine karşı dayanıklıdır.
9. Damgalanmış resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, yüksek derecede kontrast ayarlama işlemine karşı dayanıklıdır.
10. Damgalanmış resmin bütün alt-bantlarında damgalanan filigranlar, ölçekleme işlemine karşı dayanıklıdır.
11. Damgalanmış resmin (DD1) alt-bantında damgalanan filigran, filigran çarpıştırma saldırısına karşı dayanıklıdır.
12. Damgalanmış resmin (DD1) alt-bantında damgalanan filigran, sahte filigran ekleme saldırısına karşı dayanıklıdır.

- 13.** Damgalanmış resmin (DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, 3×3 yapı element boyutunda genişleme ve aşındırma işlemlerine karşı dayanıklıdırlar.
- 14.** Damgalanmış resmin (DD1, DY1, YD1 ve YY1) alt-bantlarında damgalanan filigranlar, JPEG2000 kayıplı sıkıştırmasına karşı dayanıklıdırlar.

Bu çalışmada resimlerin telif haklarını korumak için resimlere siyah-beyaz filigranlar damgalanmıştır. İlerdeki çalışmalarımda renkli filigranlar kullanılarak çalışılacaktır. Ayrıca, önerilen damgalama yöntemi döndürme işlemine karşı kayda değer bir dayanıklılık göstermemiştir. Bu yüzden; önerilen damgalama yönteminin, başka bir değişken kullanarak döndürme işlemine karşı dayanıklılığının artırılması amaçlanacaktır. Son olarak, önerilen damgalama yöntemi kör olmayan veya kişisel bir damgalama yöntemidir. Kör olmayan damgalama yöntemini kör veya kamusal hale dönüştürmek hedeflenen amaçlar arasındadır.

KAYNAKLAR

- [1] Mohanty, S. P., "Digital Watermarking: A Tutorial Review", Indian Institute of Science, Bangalore, India, 1999.
<http://www.cs.unt.edu/~smohanty/research/Reports/MohantyWatermarkingSurvey1999.pdf>
- [2] Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G., "Information Hiding: A Survey", *Proceedings of the IEEE*, **87** (7), 1062-1078, 1999.
- [3] Popa, R., "An Analysis of Steganographic Techniques"
http://ad.informatik.unifreiburg.de/mitarbeiter/will/dlib_bookmarks/digital-watermarking/popa/popa.pdf
- [4] Kharrazi, M., Sencar, H. T. and Memon, N., "Image Steganography: Concepts and Practice", *WSPC/Lecture Notes Series: 9in x 6in*, 1-31, Polytechnic University, Brooklyn, A.B.D., 2004.
- [5] Serge, A. N. N., "Digital Watermarking". www.sec.informatik.tu-darmstadt.de/pages/lehre/SS07/sem_misc/papers/nguepi.pdf
- [6] Pedroncelli, A., *Secure Multimedia Databases*, Master Thesis, Rand Afrikaans University, 2002.
- [7] Anonim, "Digital Watermarking: A Technology Overview", 2001.
http://www.securitytechnet.com/resource/security/application/Digital_Watermarking_Tech_Overview.pdf
- [8] Langelaar, G. C., Setyawan, I. and Lagendijk, R. L. "Watermarking Digital Image and Video Data: A State-of-the-Art Overview", *IEEE signal processing magazine*, 20-46, 2000.
- [9] Anonim, "Watermarking World", 2008.
<http://www.watermarkingworld.org/faq.html>
- [10] Nasir, I., Weng, Y. and Jiang, J., "A New Robust Watermarking Scheme for Color Image in Spatial Domain", <http://www.ist-live.org/intranet/school->

[of-informatics-university-of-bradford001-3/a-new-robust-watermarking-scheme-for-color-image-in-spatial-domain.pdf/view](http://www.informatics-university-of-bradford001-3/a-new-robust-watermarking-scheme-for-color-image-in-spatial-domain.pdf/view)

- [11] Cox, I. J., Miller, M. L. and Bloom, J. A., “Watermarking Applications and Their Properties”, *Published in the International Conference on Information Technology’2000*, Las Vegas, A.B.D., 2000.
- [12] Anonim, “Discrete Wavelet Transform”, 2008.
http://en.wikipedia.org/wiki/Discrete_wavelet_transform
- [13] Anonim, “Wavelet”, 2008. <http://en.wikipedia.org/wiki/Wavelet>
- [14] Terzija, N., Repges, M., Luck, K. and Geisselhardt, W., “Digital Image Watermarking Using Discrete Wavelet Transform: Performance Comparison of Error Correction Codes”, *2nd IASTED International Conference, Visualization, Imaging and Image Processing*, Benalmadena, Malaga, Spain, 2002.
- [15] Talukder, K. H and Harada, K., “Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image”, *IAENG International Journal of Applied Mathematics*, **36** (1), 2007.
- [16] Chen, P. Y. and Lin, H. J., “A DWT Based Approach for Image Steganography”, *International Journal of Applied Science and Engineering*. **4** (3), 275-290, 2006.
- [17] Anonim, “Watermarking World”, 2008.
<http://www.watermarkingworld.org/WMLArchive/0509/msg00005.html>
- [18] Delp, E. J., Saenz, M. and Salama, P., “Block Truncation Coding (BTC)”, *Handbook of Image and Video Processing: BTC*.
- [19] Tu, S. F. and Hsu, Ch. Sh., “BTC-Based Watermarking Scheme for Digital Images”, *Information and Security, An International Journal*, **15** (2), 216-228, 2004.
- [20] Franti, P., Nevalinen, O. and Kaukoranta T., “Compression of Digital Images By Blok Truncation Coding: Survey”, *The Computer Journal*, **37** (4), 308-332, 1994.

- [21] Anonim, "Block Truncation Coding", 2008.
http://www.ee.latrobe.edu.au/%7Edennis/teaching/ELE42IPC/ELE42IPC_imgpro/node14.html
- [22] Wang, H. and Wang, S., "Cyber Warfare: Steganography vs. Steganalysis", *Communications of the ACM*, **47** (10), 76-82, 2004.
- [23] Anonim, "Block Truncation Coding", 2008.
<http://sparc.nfu.edu.tw/~lyc/dc/D09.pdf>
- [24] Peleg, N., "Block Truncation Coding (BTC)", 2006.
<http://cs.haifa.ac.il/~nimrod/Compression/Image/I5btc2005.pdf>
- [25] Muharemagic, E. and Furht, B., "Multimedia Security: Watermarking Techniques".
<http://www.cse.fau.edu/~borko/MulChapter,%20Watermarking%20IEC2004.pdf>
- [26] Neubauer, Ch. and Herre, J., "Advanced Watermarking and its Applications", *Presented at the 109th Convention 2000 September*, Los Angeles, California, A.B.D., 2000.
- [27] Hartung, F. and Kutter, M., "Multimedia Watermarking Techniques". Invited Paper. *Proceedings of the IEEE*, **87** (7), 1079-1107, 1999.
- [28] Venkateswaran, N., Arunkumar, J. and Deepak, T. K., "A BTC-DWT Hybrid Image Compression Algorithm".
<http://ieeexplore.ieee.org/iel5/4286642/4286643/04286696.pdf>
- [29] Genov, E. P., "Digital Watermarking of Bitmap Images" *International Conference on Computer Systems and Technologies-CompSysTech'07*, **285** (37), 1-6, 2007.
- [30] Cacciaguerra, S. and Ferretti, S., "Data Hiding: Steganography and Copyright Marking".
http://www.cs.unibo.it/~scacciag/home_files/teach/datahiding.pdf
- [31] Bhatt, N., "Digital Watermarking", 2008.
http://users.on.net/~neerav/temp/digital_watermarking.pdf

- [32] Taoa, P. and Eskicioglu, A. M., “A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform domain”, 2004.
<http://www.sci.brooklyn.cuny.edu/~eskicioglu/papers/OE2004.pdf>
- [33] Mesut, A. ve Carus, A. , “Kayıpsız Görüntü Sıkıştırma Yöntemlerinin Karşılaştırılması”, *II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi (MBGAK)*. İstanbul, 2005.