

**YENİ BİR SAYISAL DAMGALAMA TEKNİĞİ İLE
BİYOMETRİK UYGULAMALAR**

Şengül DOĞAN

**Doktora Tezi
Elektrik-Elektronik Mühendisliği Anabilim Dalı
Danışman: Yrd. Doç. Dr. Arif GÜLTEN**

Eylül-2011

**T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**YENİ BİR SAYISAL DAMGALAMA TEKNİĞİ
İLE BİYOMETRİK UYGULAMALAR**

DOKTORA TEZİ

Şengül DOĞAN

(06213201)

**Tezin Enstitüye Verildiği Tarih: 23 Ağustos 2011
Tezin Savunulduğu Tarih: 12 Eylül 2011**

Tez Danışmanı : Yrd. Doç. Dr. Arif GÜLTEN (F.Ü)
Diğer Jüri Üyeleri : Prof. Dr. Mustafa POYRAZ (F.Ü)
Prof. Dr. Hanifi GÜLDEMİR (F.Ü)
Doç. Dr. Serdar Ethem HAMAMCI (İ.Ü)
Yrd. Doç. Dr. Mustafa TÜRK (F.Ü)

EYLÜL-2011

ÖNSÖZ

Bu tez çalışması süresince bilgi ve tecrübelerinden faydalandığım, bana yol gösteren ve destek olan danışman hocam, Sayın Yrd. Doç. Dr. Arif GÜLTEN'e teşekkürlerimi sunarım.

Çalışmalarında bilgi ve tecrübesini benden hiçbir zaman esirgemeyen Sayın Prof. Dr. Hanifi GÜLDEMİR'e, tez çalışması sırasında bana destek olan Sayın Türker TUNCER'e ve tüm değerli hocalarıma teşekkürü bir borç bilirim.

Başta bir tanecik annem ve tez süresi boyunca neşe kaynağım olan yeğenim Elifnur ÇOLAKOĞLU olmak üzere her zaman desteklerini hissettiğim aileme gösterdikleri sabır ve anlayıştan dolayı şükranlarımı sunarım.

Şengül DOĞAN
ELAZIĞ-2011

İÇİNDEKİLER

Sayfa No

ÖNSÖZ	II
İÇİNDEKİLER	III
ÖZET	V
SUMMARY	VI
ŞEKİLLER LİSTESİ	VII
TABLOLAR LİSTESİ	XI
KISALTMALAR LİSTESİ	XII

1. GİRİŞ	1
1.1. Tezin Amacı	4
1.2. Tezin Bölümleri	4
2. BİYOMETRİK YÖNTEMLER VE UYGULAMALARI	6
2.1. Parmak İzi Tanıma	8
2.2. Yüz Tanıma	9
2.3. İris Tanıma	10
2.4. El Geometrisi Tanıma	11
2.5. Retina Tanıma	12
2.6. Ses Tanıma	12
2.7. DNA Tanıma	13
2.8. İmza, Yürüyüş, Tuş Vuruşu ve Konuşma Tanıma	14
3. VERİ GİZLEME YÖNTEMLERİ VE TARİHÇESİ	16
3.1. Steganografi	18
3.2. Kriptoloji	20
3.3. Sayısal Damgalama	22
3.4. Etiketleme	23
3.5. Sayısal İmzalama	24
4. SAYISAL DAMGALAMA SİSTEMLERİ	25
4.1. Sayısal Damgalama Türlerinin Sınıflandırılması	26
4.1.1. Algoritma Düzlemine Göre Damgalama	27
4.1.2. Algılanabilirlik Özelliğine Göre Damgalama	28
4.1.3. Uygulama Alanına Göre Damgalama	30
4.1.4. Doküman Türüne Göre Damgalama	30
4.1.4.1. Resim ve Video Damgalama	30
4.1.4.2. Metin Damgalama	31
4.1.4.3. Ses Damgalama	31
4.2. Sayısal Damgalama Sistemlerinin Özellikleri	32
4.2.1. Algılanamamazlık	32
4.2.2. Kapasite	33
4.2.3. Güvenlik	33
4.2.4. Dayanıklılık	33
4.2.5. Kapasite	33
4.2.6. Güvenlik	33
4.3. Sayısal Damgalama Sistemlerine Yapılan Saldırıları	33
4.3.1. Basit Saldırıları	33
4.3.1.1. JPEG Kayıplı Sıkıştırma	34

4.3.1.2.	Gürültü Ekleme	34
4.3.1.3.	Kırpm.....	34
4.3.2.	Geometrik Saldırıları	34
4.3.2.1.	Yatay Eksende Döndürme	35
4.3.2.2.	Dikey Eksende Döndürme.....	35
4.3.2.3.	Açılı Döndürme.....	36
4.3.2.4.	Ölçekleme.....	36
4.3.2.5.	Satır veya Sütunların Yer Değiştirmesi/ Silinmesi.....	37
4.3.3.	Silici Saldırıları.....	37
4.3.4.	Kriptografik Saldırıları	37
4.3.5.	Protokol Saldırıları	38
4.4.	Damga Ekleme ve Çıkarma İşlemi.....	38
4.5.	Veri Gizleme Yöntemlerinin Kıyaslanması	41
5.	SAYISAL DAMGALAMA UYGULAMALARINDA KULLANILAN YÖNTEMLER.....	43
5.1.	Sayısal Resim Bileşenleri ve Formatları	43
5.1.1.	Resim (İmge).....	43
5.1.1.1.	Gerçek Renk	44
5.1.1.2.	Gri Seviye.....	44
5.1.1.3.	İndeksli Renk.....	44
5.1.2.	Piksel	44
5.1.3.	Nokta ve Nokta Aralığı	45
5.1.4.	Çözünürlük	45
5.1.5.	LPI.....	46
5.1.6.	DPI.....	46
5.2.	Sayısal Damgalama Uygulamalarında Kullanılan Yöntemler	46
5.2.1.	En Önemsiz Bit Yöntemi	46
5.2.2.	Ayrık Dalgacık Dönüşümü.....	49
5.2.3.	Ayrık Kosinüs Dönüşümü	54
5.2.4.	Ayrık Fourier Dönüşümü	59
5.2.5.	Tekil Değer Ayrışımı Yöntemi.....	60
6.	RENKLİ RESİMLER İÇİN GERÇEKLEŞTİRİLEN SAYISAL DAMGALAMA UYGULAMALARI	62
6.1.	ADD ile Sayısal Damgalama Uygulaması	64
6.2.	AKD ile Sayısal Damgalama Uygulaması	70
6.3.	TDA Yöntemi ile Sayısal Damgalama Uygulaması	77
7.	GELİŞTİRİLEN YÖNTEM İLE SAYISAL DAMGALAMA UYGULAMASI.....	84
7.1.	AKD ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması	90
7.2.	ADD ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması	93
7.3.	TDA ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması	95
8.	SONUÇLAR VE DEĞERLENDİRME.....	99
	KAYNAKLAR.....	104
	ÖZGEÇMİŞ	

ÖZET

Bilgisayar ve elektronik teknolojisindeki gelişmeler ve internet kullanımının yaygınlaşması akıllı ve uzaktan kontrollü güvenlik sistemlerinin günlük hayatımıza yaygın olarak girmesine de imkân sağlamıştır. Biyometrik sistemler kişilerin yanında herhangi bir araç taşımadan kendi biyometrik özelliklerinin sorgulanmasıyla oluşturulan kişi tanımaya yönelik geliştirilen güvenlik sistemleridir. Bu sistemlerin gelişimi hem bilgisayar ve ağ teknolojisi hem de elektronik teknolojisindeki gelişmeler paralelinde her geçen gün artmaktadır. Sistem tasarımında güvenlik ve başarımlar düzeyinin artırılması amacıyla sayısal damgalama yöntemleri yaygın olarak kullanılmaktadır. Biyometrik bir sistemin amacı ve kullanım yerine göre sayısal damgalama alanında geliştirilen yöntemler tek başına veya birbirleriyle ilişkili olarak kullanılabilirlerdir.

Bu tez çalışmasında renkli biyometrik resimler için yeni bir sayısal damgalama yöntemi sunulmuştur. Geliştirilen yöntemin başarımlarını Ayrık Kosinüs Dönüşümü, Ayrık Dalgacık Dönüşümü, Tekil Değer Ayrışımı Yöntemi gibi literatürde yoğun olarak kullanılan yöntemlerle karşılaştırılmıştır. PSNR, BER, NC oranı, hesaplama süresi ve histogram eğrisi gibi ölçütler ile kıyaslanarak sonuçlar değerlendirilmiştir.

Anahtar Kelimeler: Biyometrik Sistemler, Veri Gizleme, Sayısal Damgalama, Ayrık Kosinüs Dönüşümü, Ayrık Dalgacık Dönüşümü, Tekil Değer Ayrışımı.

SUMMARY

A New Digital Watermarking Method for Biometric Applications

Advancement in computer and electronic technology and the spread of internet use have led the intelligent and remote controlled safety systems to enter daily life. Biometric safety systems use biometric properties which do not require to carry any tool to recognize people. The developments of these systems are increasing every day with the advancements parallel to computer, network and electronic technologies. Digital watermarking techniques are widely used in the system design to increase the safety and performance level. The developed digital watermarking techniques can be combined to be used with the other techniques depending on the aim and place of use of the biometric system.

In this thesis, a new digital watermarking method is proposed for the color images. The performance of the proposed method is compared with that of Discrete Cosine Transform, Discrete Wavelet Transform and Singular Value Decomposition which are widely used in digital watermarking. In the comparisons the PSNR, BER, NC rate, computing time and histograms are obtained and used as the criteria.

Keywords: Biometric Systems, Data Hiding, Digital Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Singular Value Decomposition.

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 2.1.	Bir biyometrik sistemin genel yapısı	7
Şekil 2.2.	Parmak izi örnekleri.....	8
Şekil 2.3.	Yüz resmi örnekleri	9
Şekil 2.4.	İris resmi örnekleri.....	10
Şekil 2.5.	El geometrisi örnekleri	11
Şekil 2.6.	Retina örnekleri	12
Şekil 2.7.	Ses örnekleri	13
Şekil 2.8.	DNA örnekleri	14
Şekil 3.1.	Veri gizleme tekniklerinin damgalama ile olan ilişkisi	17
Şekil 3.2.	Veri gizleme tekniklerinin türleri	18
Şekil 3.3.	Steganografik sistemin yapısı	19
Şekil 3.4.	Steganografik yöntemlerin sınıflandırılması	19
Şekil 3.5.	Şifreleme ve şifre çözme basamakları	21
Şekil 3.6.	Temel damgalama işlemi	22
Şekil 3.7.	Damga çıkarma işlemi	23
Şekil 4.1.	Damgalama yönteminin blok diyagramı	25
Şekil 4.2.	Sayısal damgalama türlerinin sınıflandırılması	27
Şekil 4.3.	Algılanabilirlik özelliğine göre damgalama türleri.....	28
Şekil 4.4.	Görünür damgalama türleri.....	29
Şekil 4.5.	Sayısal damgalama sistemlerinin özellikleri	32
Şekil 4.6.	Damgalanmış nesnenin yatay ekseninde döndürülmesi	35
Şekil 4.7.	Damgalanmış nesnenin dikey ekseninde döndürülmesi	35
Şekil 4.8.	Damgalanmış nesnenin 30° döndürülmesi	36
Şekil 4.9.	Ölçeklendirme türleri.....	36
Şekil 4.10.	Görünür damgalamada damgayı yok etme	37
Şekil 4.11.	EÖB yöntemi tabanlı damga ekleme işleminin blok diyagramı	39
Şekil 4.12.	EÖB yöntemi tabanlı damga çıkarma işleminin blok diyagramı.....	40
Şekil 5.1.	Resmin sayısallaştırılması	43
Şekil 5.2.	Görüntünün piksellerinin açığa çıkarılması.....	45

Şekil 5.3. Resimlerde piksel boyut ilişkisi.....	45
Şekil 5.4. EÖB yöntemi ile veri gizleme	47
Şekil 5.5. Renkli bir resmin RGB katmanları	49
Şekil 5.6. Dalgacık dönüşümü ile bir işaretin frekans bileşenlerine ayrılması.....	50
Şekil 5.7. ADD ile resmin alt bantlarına ayrılması.....	51
Şekil 5.8. Tek seviyeli ADD ile resmin alt bantlarına ayrılması	52
Şekil 5.9. İki seviyeli ADD ile resmin alt bantlarına ayrılması	52
Şekil 5.10. AKD işlem basamakları.....	55
Şekil 6.1. ADD tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı	64
Şekil 6.2. ADD tabanlı damga çıkarma sisteminin iris ve yüz resimleri için blok diyagramı	65
Şekil 6.3. ADD ile damgalama işlemi	66
Şekil 6.4. ADD tabanlı sistemden elde edilen sonuçlar.....	66
Şekil 6.5. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	67
Şekil 6.6.a. Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	68
Şekil 6.6.b. Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	68
Şekil 6.6.c. 1° döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	69
Şekil 6.6.d. Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	69
Şekil 6.7 AKD ile damgalama işlemi	70
Şekil 6.8.a. AKD ile resmin ayrıştırılması.....	71
Şekil 6.8.b.AKD tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı	72
Şekil 6.9. AKD tabanlı sistemde damga çıkarma için sisteminin blok diyagramı	73
Şekil 6.10. AKD tabanlı sistemden elde edilen sonuçlar.....	73
Şekil 6.11. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	74

Şekil 6.12.a. Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	75
Şekil 6.12.b. Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	75
Şekil 6.12.c. 1° döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	76
Şekil 6.12.d. Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	76
Şekil 6.13. TDA tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı.....	78
Şekil 6.14. TDA tabanlı damga çıkarma sisteminin iris ve yüz resimleri için blok diyagramı.....	79
Şekil 6.15. TDA tabanlı sistemden elde edilen sonuçlar	79
Şekil 6.16. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	80
Şekil 6.17.a. Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	81
Şekil 6.17.b. Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	81
Şekil 6.17.c. 1° döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	82
Şekil 6.17.d. Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	82
Şekil 7.1. Geliştirilen yöntem ile sistemin renkli iris ve yüz resimleri için damgalama blok diyagramı	84
Şekil 7.2. Geliştirilen yöntem ile iris ve yüz resimleri için damga çıkarma sisteminin blok diyagramı	85
Şekil 7.3. Geliştirilen yöntem ile sistemden elde edilen sonuçlar	86
Şekil 7.4. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	87
Şekil 7.5.a. Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	88

Şekil 7.5.b. Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	88
Şekil 7.5.c. 1° döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	89
Şekil 7.5.d. Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması	89
Şekil 7.6. AKD ve geliştirilen yöntem ile sisteminin blok diyagramı	91
Şekil 7.7. AKD ve geliştirilen yöntem ile sistemden elde edilen sonuçlar	92
Şekil 7.8. ADD ve geliştirilen yöntem ile sisteminin blok diyagramı	94
Şekil 7.9. ADD ve geliştirilen yöntem ile sistemden elde edilen sonuçlar	95
Şekil 7.10. TDA ve geliştirilen yöntem ile sisteminin blok diyagramı	97
Şekil 7.11. TDA ve geliştirilen yöntem ile sistemden elde edilen sonuçlar	98

TABLÖLAR LİSTESİ

	<u>Sayfa No</u>
Tablo 1.1. Çoklu ortam ve biyometrik verilerin ortak amaçları	2
Tablo 2.1. Biyometrik yöntemlerin karşılaştırılması	15
Tablo 6.1. Renkli iris ve yüz resimleri için ADD tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları.....	70
Tablo 6.2. Renkli iris ve yüz resimleri için AKD tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları.....	77
Tablo 6.3. Renkli iris ve yüz resimleri için TDA tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları.....	83
Tablo 7.1. Geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları	90
Tablo 7.2. Damganın geliştirilen yöntem ile saldırılara dayanıklılığı	90
Tablo 7.3. AKD ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları	92
Tablo 7.4. Damganın AKD ve geliştirilen yöntem ile saldırılara dayanıklılığı	92
Tablo 7.5. ADD ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları	95
Tablo 7.6. Damganın ADD ve geliştirilen yöntem ile saldırılara dayanıklılığı	95
Tablo 7.7. TDA ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları	98
Tablo 7.8. Damganın TDA ve geliştirilen yöntem ile saldırılara dayanıklılığı	98

KISALTMALAR LİSTESİ

ADD	: Ayrık Dalgacık Dönüşümü
AFD	: Ayrık Fourier Dönüşümü
AKD	: Ayrık Kosinüs Dönüşümü
BER	: Bit Hata Oranı
EÖB	: En Önemsiz Bit
İDS	: İnsan Duyuş Sistemi
İGS	: İnsan Görme Sistemi
JPEG	: Birleşik Fotoğraf Uzmanları Grubu
MSE	: Ortalama Karesel Hata
NC	: Normalizasyon Katsayısı
PSNR	: Tepe İşaret Gürültü Oranı
TADD	: Ters Ayrık Dalgacık Dönüşümü
TAKD	: Ters Ayrık Kosinüs Dönüşümü
TDA	: Tekil Değer Ayrışımı

1. GİRİŞ

Biyometrik sistemler bireylerin birbirinden farklılık gösteren fiziksel ve davranışsal özelliklerini kullanarak kimlik tanımaya yönelik geliştirilen bilgisayar tabanlı sistemlerdir. Biyometrik sistemlerde kişi, nüfus cüzdanı, şifre, imza gibi harici herhangi bir araç kullanmadan kendi biyometrik özellikleri ile sisteme erişmektedir. İşte biyometrik sistemlerin temel amacı bu anlamda ortaya çıkmaktadır. Biyometrik özellikler kişiye özgüdür ve nüfus cüzdanı, şifre gibi kişiden kişiye aktarılacak yapıda değildirler. Bu nedenle günümüzde güvenlik gerektiren uygulamalarda biyometrik sistemler tercih edilmektedir. Başlangıçta bir biyometrik sistem denilince akla parmak izi ile kişi tanıyan sistemler gelmekteydi. Fakat farklı güvenlik seviyesi gerektiren uygulamalar için farklı biyometrik sistemler geliştirme yoluna gidilerek çeşitli biyometrik sistemler oluşturulmuştur. En yaygın kullanılan biyometrik tanıma sistemleri aşağıdaki gibi sıralanabilir:

- Parmak İzi Tanıma
- Yüz Tanıma
- İris Tanıma
- Ses Tanıma
- Retina Tanıma
- El Geometrisi Tanıma
- İmza Tanıma

Bu sistemlerin kullanılma oranı amacına göre değişmektedir. Örneğin yüksek güvenlik gerektiren uygulamalarda iris tanıma sistemleri yoğun olarak tercih sebebi iken gerektirdiği özel görüntüleme donanımları ve yüksek maliyeti sebebiyle, kullanımı performansının gerektirdiği ölçüde yaygın değildir. Aynı şekilde günümüzde yaygın bir şekilde kullanılan parmak izi tanıma sistemleri ise parmak izinin taklit edilebilmesi ve bu girişimler ile aşılacak güvenlik sınırları nedeniyle yüksek güvenlik gerektiren uygulamalarda yoğun olarak tercih edilmemektedir. Sistemlere ait bu dezavantajlar biyometrik sistemlerde yeni arayışlara sebep olmuş ve geliştirilecek biyometrik sistemde birden fazla biyometrik özellik sorgulanarak tanıma sistemlerinin güvenlik düzeyinin artırılması amaçlanmıştır [1]. Ayrıca günümüzde teknoloji büyük bir hızla gelişmektedir. Bu gelişim olumlu açıdan incelenirse güvenlik, yaşam kalitesini artırma, hız gibi hayatımızı kolaylaştıracak pek çok avantajlara sahiptir. Fakat teknolojiye bu gelişmeler sahtecilik uygulamalarında da

kendine yer bulmuş ve bu uygulamaların artmasına sebep olmuştur. Bilgisayar tabanlı bu tür sistemlerde sahtecilik uygulamalarına çözüm olarak her geçen gün yeni yazılımlar ve araçlar geliştirilerek bu soruna çözüm yolları bulmaya çalışılmaktadır. Biyometrik tanıma sistemlerinde de sayısal damgalama uygulamalarında da temel amaç aitliğin belirlenmesidir. Bu nedenle biyometrik sistemlerin güvenlik sorunlarının tespitinde ve çözümünde sayısal damgalama yöntemleri geniş bir kullanım alanı bulmuştur. Sayısal damgalama yöntemleri bir nesnenin kime ait olduğunun belirlenmesinde kullanılan bir yöntemdir ve başlangıçta çoklu ortam verileri üzerinde kullanım alanı bulsa da Tablo 1.1.'de gösterildiği gibi ortak amaçlara sahip olduklarından biyometrik sistemlere de uyarlanabilmektedir [2].

Tablo 1.1. Çoklu ortam ve biyometrik verilerin ortak amaçları

Çoklu ortam verileri	Biyometrik veriler
Çoklu ortam verilerinin kime ait olduğunun belirlenmesi ve telif hakkının korunması	Biyometrik verilerin kime ait olduğunun belirlenmesi
Sadece izin verilen şahsın verileri kullanmasını sağlamak	Sadece biyometrik özelliği sorgulanan ve doğrulanan kişinin sisteme erişim hakkının tanınması
Çoklu ortam verilerinde yasal olmayan çoğaltılmanın engellenmesi	Veritabanına eklenen biyometrik özelliklerin istenmeyen şahısların eline geçmemesi, sisteme erişim için kullanılmaması
Çoklu ortam verilerinin iletiminde sistemin bant genişliğini en verimli şekilde kullanmasını sağlamak	Biyometrik verilerin iletiminde sistemin bant genişliğini en verimli şekilde kullanmasını sağlamak
İletim kanalında verilerde bozulmanın olup olmadığının tespiti	İletim kanalında verilerde bozulmanın olup olmadığının tespiti

Tüm bu alanlarda sayısal damgalama uygulamaları aitliğin belirlenmesi ve güvenliğin sağlanması amacıyla kullanılabilir. Sayısal damgalama yanında veri gizleme üzerine pek çok yöntem mevcuttur ve bunlar kullanım amacına göre birbirinden ayrılır. Eldeki verinin herhangi bir örtü nesnesi içerisine eklenmeden doğrudan şifrelenerek göndericiye ulaştırılması kriptoloji, verinin şifrelenmesinin zorunlu olmadığı fakat bir örtü nesnesi içerisine eklenerek iletilmesi ise steganografi olarak adlandırılmaktadır. Steganografide eklenecek damganın örtü nesnesi ile ilişkili olması beklenmemektedir. Ancak damgalamada örneğin bir eserin kim tarafından yapıldığını tespit etmek için yapan

kişiyeye özgü bir özellik eklemek amaçlanmaktadır. Yani örtü nesnesi ile eklenecek damga birbiriyle ilişkili olmalıdır [3].

Sayısal damgalama uygulamalarında çeşitli yöntemler mevcuttur. Bu yöntemler uzay ve dönüşüm bölgesinde olmak üzere iki şekilde yapılabilmektedir. En Önemli Bit (EÖB) yöntemi [4] ile damgalama uygulamaları uzay bölgesinde yapılmaktadır. Başarımları yüksek olmasına rağmen saldırılara karşı hassastır. Ayrık Fourier Dönüşümü (AFD) [5, 6], Ayrık Dalgacık Dönüşümü (ADD) [7, 8] ve Ayrık Kosinüs Dönüşümü (AKD) [9-11] gibi dönüşüm bölgesinde yapılan damgalama yöntemleri ise saldırılara karşı daha dayanıklıdır. Günümüzde bu yöntemler güvenli, sağlam ve saldırılara dayanıklı bir damgalama sistemi geliştirilebilmek için birbirleriyle ilişkili olarak kullanılmakta ve yapay zekâ teknikleri ile başarımlarının artırılmasına çalışılmaktadır. Aslantaş ve diğerkleri [12] AKD yöntemini ve akıllı optimizasyon tekniklerini (genetik algoritma, parçacık sürü optimizasyonu, diferansiyel gelişim algoritması) kullanarak resimler üzerindeki değışimin PSNR ve NC oranlarını sunmuşlardır. Huang ve Guan [13] yaptıkları damgalama uygulamasında TDA ve AKD yöntemlerini bir arada kullanmışlardır. Bu çalışmada, TDA yöntemi ile damganın tekil değerkleri elde edilerek orijinal görüntüye eklenmiştir. Ayrıca damganın en yüksek enerji değerkleri orijinal görüntünün AKD ile elde edilen ayrıntı boyutuna eklenerek geliştirilen yöntemin sağlamlığı artırılmaya çalışılmış ve yerel PSNR oranları ile yöntemin geçerliliğı sunulmuştur. Bhatnagar ve Raman [14] ise ADD ve TDA yöntemleri ile telif haklarının korunmasına yönelik bir yarı kör damgalama yapısı önermişlerdir. Hazırlanan sistem gri seviye resimler üzerine uygulanmıştır. JPEG sıkıştırma, kesme, yeniden boyutlandırma döndürme gibi bir takım geometrik saldırılara karşı sistemin başarımları PSNR ve NC oranları ile açıklanmıştır. Tsai ve arkadaşları [15] renkli resimler üzerinde ADD yöntemi tabanlı olarak yeni bir damgalama yöntemi önermişlerdir. Piksel haritası çıkarılan resme renk kuantalama tekniğı ile damganın eklenmesi sağlanarak sistemin başarımları PSNR oranları ile açıklanmıştır. Voloshynovskiy ve diğerkleri [16] pek çok çalışmaya referans olan ve damgalama uygulamalarında damganın korunması üzerine bir yöntem önermişlerdir. Olası saldırıların mekanizmalarının daha iyi anlaşılması ile damgalama yapısının başarımlarının daha yüksek olabileceğini savunan Voloshynovskiy ve arkadaşları, iki aşamalı bir damga çözme yöntemi önermişlerdir. İlk aşamada damgalanmış nesnede damganın tahmini yapılmakta, ikinci aşamada ise istatistiksel hesaplamalarla damganın bütünlüğü sağlanmaktadır. Damgalanmış nesnede PSNR oranı, çıkarılan damga da ise İGS (İnsan Görme Sistemi) baz

alınarak sonuçlar sunulmuş ve başarımı Benchmark testlerindeki yöntemlerle elde edilen sonuçlarla kıyaslanmıştır. Chang ve arkadaşları [17] ise ADD, AKD, AFD yöntemlerinden farklı olarak damgalanacak nesnenin parlaklık değerlerini içeren tekil değerlerinin elde edildiği TDA yöntemi ile bir damgalama yöntemi önermişlerdir. Gri seviye resimler üzerinde test edilen sistemde çeşitli saldırılara karşı damgalanmış resmin değişim oranı tespit edilmeye çalışılmıştır.

1.1. Tezin Amacı

Bu tez çalışmasının amacı, bir biyometrik sistem tasarımında güvenlik düzeyini artırmaya yönelik, hem uzay hem de dönüşüm bölgesinde uygulanabilecek ve aynı zamanda başarımlar ölçütlerindeki gerekli kriterleri sağlayacak yeni bir sayısal damgalama yöntemi geliştirmektir. Sayısal damgalama uygulamalarında İnsan Görme Sistemi (İGS) ve İnsan Duyma Sistemi (İDS) yanında bilgisayar üzerinde yapılan analizler (PSNR, NC, Histogram Eğrileri, BER oranı gibi) başarımlar ölçütü olarak kullanılmaktadır. Bu çalışmanın hedefi sayısal damgalama uygulamalarında yaygın olarak kullanılan ADD, AKD ve TDA ile geliştirilen yöntemin PSNR, BER, NC oranları, hesaplama süreleri ve histogram eğrileri ile kıyaslanması ve başarımlar oranlarının incelenmesidir. Bu hedef doğrultusunda biyometrik verilerden renkli 20 yüz (896x592) ve 20 iris (50x38) resmi üzerinde bahsedilen başarımlar ölçütleri incelenecektir.

1.2. Tezin Bölümleri

Bu tez çalışması yedi bölüm olarak düzenlenmiştir. Bölüm 2’de biyometrik sistemlerin kullanım amaçları, çeşitleri ve hangi alanlarda kullanıldığı araştırılmıştır.

Bölüm 3’de veri gizleme yöntemleri ve kullanım alanları verilmiştir. Ayrıca veri gizleme yöntemlerinin hangi alanlarda birbirinden ayrıldıkları araştırılmıştır.

Bölüm 4’de sayısal damgalama sistemlerinin yapısı, sınıflandırılması, sahip olması gereken özellikleri ve bu sistemler üzerine yapılan saldırılar açıklamıştır. Bir sayısal damgalama sisteminde damga ekleme ve damga çıkarma işlemleri sunulmuştur. Ayrıca bu bölümde veri gizleme yöntemleri kıyaslanmıştır.

Bölüm 5’de tez kapsamında biyometrik verilerin resim formatı kullanıldığı için sayısal resim bileşenleri açıklanmıştır. Ayrıca sayısal damgalama uygulamalarında

kullanılan yöntemler (EÖB, ADD, AKD, TDA, AFD) açıklanarak bu yöntemlerin sayısal damgalama uygulamalarında kullanılma nedenleri, avantajları ve dezavantajları irdelenmiştir.

Bölüm 6’da bu tez çalışmasında geliştirilen yöntemin değerlendirilmesine yer verilmiştir. Başarım ölçütü olarak kullanılan değerlerin sayısal damgalama uygulamalarında taşıdığı anlam ve denklemleri verilerek ADD, AKD, TDA ve geliştirilen yöntemden elde edilen PSNR, BER, NC oranları, hesaplama süreleri ve histogram eğrileri sunulmuştur. Bölüm 7’de elde edilen sonuçlar değerlendirilmiş ve önerilen yöntemin uygunluğu tartışılmıştır. Bunun sonucunda ileride yapılabilecek çalışmalarla ilgili bazı öneriler sunulmuştur.

2. BİYOMETRİK YÖNTEMLER VE UYGULAMALARI

Biyometri insanları birbirinden ayırt edebilecek fiziksel ve davranışsal özellikleri inceleyen bilim dalıdır. Biyometrik sistemler teknolojinin gelişmesiyle bir ihtiyaç olarak doğmuştur [18, 19]. Geleneksel kişi tanıma sistemleri, kimliğin tanınması için belge, şifre vb. çeşitli tanıma araçları kullanırlar [20]. Bu araçlar yetkili olmayan üçüncü şahısların eline geçebilecek yapıda olduklarından gelişen teknolojiye ayak uyduramamaktadırlar. Bu anlamda çalınamayan, kaybolmayan, zamanla değişmeyen özellikleri kullanan biyometrik sistemler devreye girmişlerdir [21].

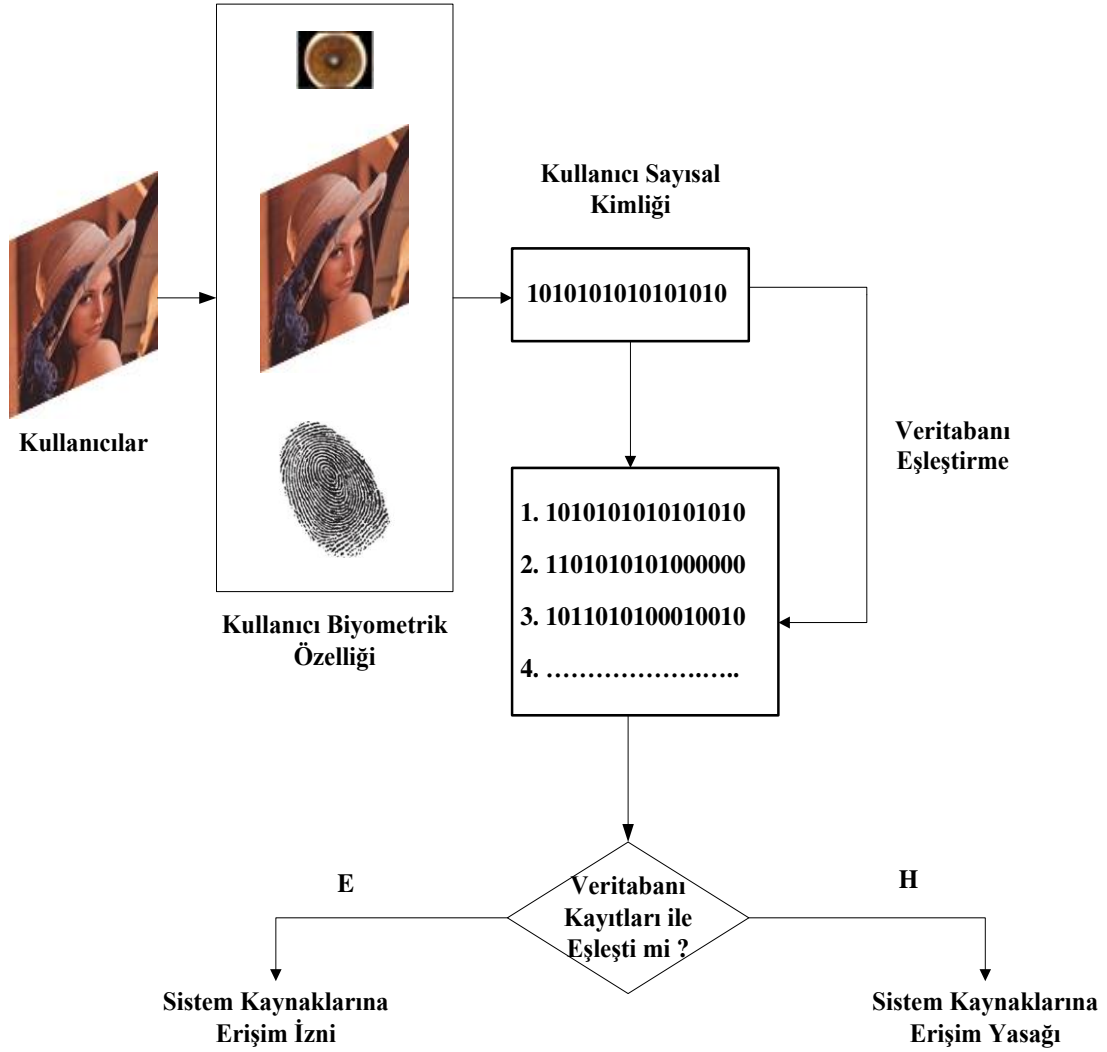
Biyometrik sistemler, bireyleri birbirinden ayıran ölçeklenebilir fiziksel, psikolojik ve davranışsal özellikleri kullanarak kimlik tespiti yapan bilgisayar kontrollü sistemlerdir. Gelişen teknoloji paralelinde geliştirilen sistemlerin güvenliğinin en üst düzeyde olması istenmektedir. Biyometrik sistemler kişiye özgü bilgileri kullandıkları için son yıllarda bu yöntemlere olan ilgi büyük bir hızla artmaktadır [22]. Bu sistemler:

- Havalimanlarında
- Askeri kaynak takibinde
- Polis teşkilatında
- Personel devam/takip işlemlerinde
- Çağrı merkezlerinde
- Online/bireysel bankacılık işlemlerinde
- Kurumsal ve kişisel ağ güvenliğinde
- E-ticaret uygulamalarında
- Satış noktası terminallerinde
- Hasta takip ve kimlik saptama
- Para çekme makinalarında

gibi alanlarda son derece etkin bir şekilde kullanılmaktadırlar [23, 24].

Şekil 2.1.'de yapısı verilen bir biyometrik sistemin tasarımında sırasıyla aşağıdaki adımlar takip edilir [25]:

- Sistemin oluşturulması için gereken veriler toplanır.
- Her veri kişiye özgü bir koda dönüştürülerek veritabanına kaydedilir.
- Sorgulanacak kişi veritabanındaki kayıtlarla karşılaştırılarak sonuca varılır.



Şekil 2.1. Bir biyometrik sistemin genel yapısı

Kimlik belirleme uygulamalarında, biyometri tabanlı sistemler yüksek güvenlik sağlarlar. Günümüzde kullanılan sistemlerde bir tek biyometrik özellik yerine birden fazlası kullanılarak güvenlik ve başarı düzeyinin artırılması amaçlanmıştır. Biyometrik sistemler kullanılan verinin çeşidine göre 4 sınıfa ayrılırlar:

- **Tekli Biyometrik Sistem:** Tek biyometrik özelliğin kullanıldığı sistemlerdir.
- **Tekli Model Biyometrik Sistem:** Tek bir örnek ve tek bir tanımlamaya uygun şeklinde tasarlanacak bir biyometrinin altkümesi olarak ifade edilebilecek bir sistemdir.
- **Çoklu Biyometrik Sistem:** Aynı kişiden elde edilen birden fazla tanımlayıcının tek başlarına veya birbirleriyle ilişkileri zayıf olan tek biyometrik tanımlayıcıların kullanılması prensibine dayanır.

- **Çoklu Model Biyometrik Sistem:** Birbirleriyle ilişkileri kuvvetli olan birden fazla biyometrik özelliğin kullanılması şeklinde tanımlanabilir [23]. Bu tür sistemlerde birden fazla biyometrik özellik sorgulanır [26-28].

Günümüzde kullanılan biyometrik sistemler fiziksel ve davranışsal özelliklerine göre ikiye ayrılmaktadır [29].

Fiziksel özelliklere göre biyometrik sistemler:

- Parmak izi tanıma
- Yüz tanıma
- İris tanıma
- El geometrisi tanıma
- Retina tanıma
- Ses tanıma
- DNA tanıma

Davranışsal özelliklere göre biyometrik sistemler:

- İmza tanıma
- Yürüyüş tanıma
- Tuş vuruşu tanıma
- Konuşma tanıma

2.1. Parmak İzi Tanıma

Parmak izi, parmak uçlarının yüzeyinde bulunan izlerden oluşan desendir [30,31]. Günümüzde biyometrik sistem denince ilk akla gelen ve en yaygın kullanılan parmak izi tanıma sistemleridir. Parmak izi taklit edilemez bir biyometrik bilgi olduğundan ve kolay elde edilebildiğinden polis merkezlerinde, pasaport ve vize başvurularında kullanılır [32]. Şekil 2.2.'de farklı parmak izi örnekleri verilmiştir [33-35].



Şekil 2.2. Parmak izi örnekleri

Parmak izi tanıma sistemlerinin avantajları:

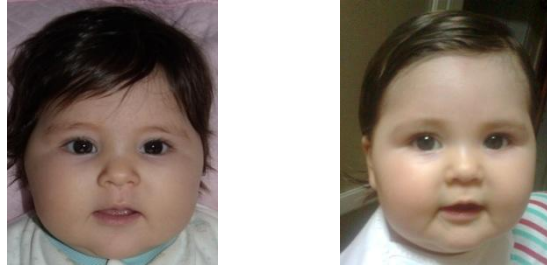
- Parmak izi kolay elde edilebilir.
- Parmak izi tanıma sistemleri pahalı sistemler değildir.
- Her insanda (%95 aynı olabilse de tek yumurta ikizleri de dahil) farklılık gösterir.
- Parmak izi tanıma sistemleri çok hızlı çalışırlar.

Dezavantajları:

- İnsanların % 3-7'sinin parmak izi kullanılamamaktadır.
- Parmak izi örneği alınan kişinin parmağının yıpranması ya da kişinin kilo alıp vermesi gibi değişiklikler sonucu aynı iz tekrar elde edilemeyebilir.
- Parmak izi kalıbı ile sistem, istenmeyen kişiler tarafından kullanılabilir [36, 37].

2.2. Yüz Tanıma

İnsan beyninin kişi tanıma mantığına benzer şekilde çalışan yüz tanıma sistemleri kullanımı en kolay ve kabul edilebilir yöntemlerden biri olarak görülmektedir [38]. Ancak bu yöntemde de bazı sorunlar yer almaktadır. Özellikle, otomatik olarak görüntü alma, alınan görüntü içerisinde yüz olup olmadığını tespit etme ve belirli bir noktadan yüzü tanıma işlemleri sırasında zorluklar yaşanabilmektedir [39]. Yüz resmi örnekleri Şekil 2.3.'de verilmiştir.



Şekil 2.3. Yüz resmi örnekleri

Yüz tanıma sistemlerinin avantajları:

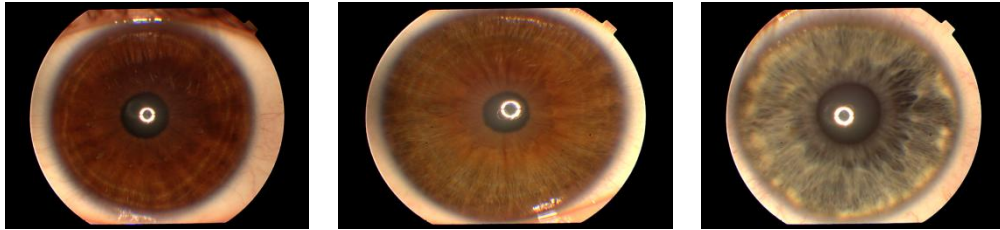
- Parmak izi kadar kolay taklit edilemeyecek şekilde çok sayıda özellik barındırırlar.
- İnsan yüzü tek yumurta ikizleri haricinde birbirinden farklılık gösterir.
- Veritabanının oluşturulması kolaydır.
- Yüz tanıma sistemleri pahalı sistemler değildir.

Dezavantajları:

- Uygulanması ve algoritmasının oluşturulması zordur.
- Kişinin yüzünde bulunan aksesuarlarla kişinin sistemdeki kaydının eşleşmesi zordur.
- Kişinin yüzünde oluşabilecek küçük bir yaralanma ve hasarda tanıma olumsuz etkilenir [36, 40].

2.3. İris Tanıma

Güvenilirliği ve doğruluğu bayağı yüksek olan iris tanıma sistemleri maliyeti yüksek olan biyometrik sistemler arasındadır. İnsanların embriyo dönemlerinde oluşan ve hayatları boyunca değişmeyen iris tabakası bir biyometrik karakteristiktir [41]. İris tabakası ömür boyu değişikliğe uğramaz ve dış ortamdan izole edilmiş olup cerrahi müdahalelerle bile değiştirilememektedir. Sistemin en büyük zorluğu, iris görüntüsü alınması sırasında tarayıcıdan yayılan belirli bir miktar ışığın günlük yaşantıda insanları rahatsız edici boyutunun olmasıdır. Görüntünün tanıma için uygun formatta alınabilmesi için tarayıcının gözden belirli bir uzaklıkta bulunması ve oldukça kaliteli olması gerekmektedir. Bunun da maliyeti arttırması nedeniyle günümüzde tercih edilmemesindeki en önemli engellerden biridir [42, 43]. İris örnekleri Şekil 2.4.'de verilmiştir [44].



Şekil 2.4. İris resmi örnekleri

İris tanıma sistemlerinin avantajları:

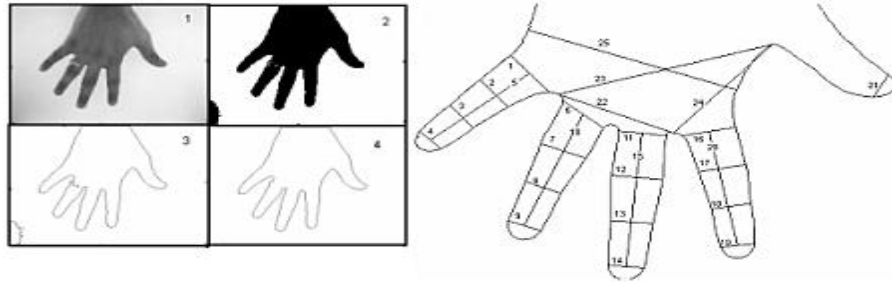
- İris vücudun dışındaki bir organ olmadığından zarar görme olasılığı düşüktür.
- Tek yumurta ikizleri dahil iris izi tüm kişilerde farklılık gösterir.
- Göz, insanın ölümünden sonra en kısa sürede değişime uğrayan organlardan biridir.

Dezavantajları:

- Sistemde veritabanı oluşturulurken iris görüntüsünün alınabilmesi için kullanılan cihazların çözünürlüğünün ve kalitesinin çok iyi olması gerekmektedir.
- İris tanıma sistemleri pahalı sistemlerdir [36].

2.4. El Geometrisi Tanıma

Elin belli bir kısmının veya tamamının taranması ile oluşturulan sistemde; elin şekli, parmakların uzunluğu, genişliği gibi biyometrik karakteristikleri kullanarak tanıma işlemini gerçekleştiren ve çok kullanılan biyometrik bir yöntemdir [45]. El geometrisi örnekleri Şekil 2.5.'de verilmiştir [46].



Şekil 2.5. El geometrisi örnekleri

El geometrisi tanıma sistemlerinin avantajları:

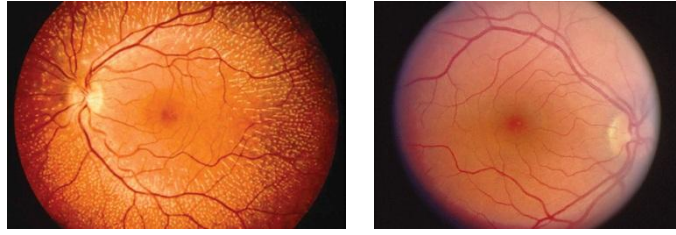
- Sistemin uygulanması ve algoritmasının oluşturulması kolaydır.
- Sistem güvenilir ve doğruluğu yüksektir.

Dezavantajları:

- Sistem fazla yer kaplar. Özellikle diz üstü bilgisayarlarda kullanılmak istendiğinde, kaplayacağı alanın en azından bir el büyüklüğünde olması gerektiğinden oldukça fazla fiziksel alana ihtiyaç vardır.
- El şekli kalıcı bir biyometrik özellik değildir. Özellikle kilo almayla veya vermayla beraber parmakların genişliği değişebileceğinden mevcutta tanımlı olan taslak bilgilerle giriş bilgilerin uyuşmasını engelleyecektir.
- Resmin alınma süresi uzundur [36].

2.5. Retina Tanıma

Retina tabakasında bulunan retinal damarlar oldukça sabit bir yapıya sahip olup retinal desen olarak adlandırılır. Bu desenin dijital görüntüsü göz bebeğine az miktarda ışık yansıtılarak elde edilebilir. Bu da retina tanıma sistemlerinin kullanımını kolaylaştırmaktadır. Retinal desen dış ortamdan izoledir ve bu özelliği karakteristik yapısının korunabilmesi açısından oldukça önemlidir [18]. Retina örnekleri Şekil 2.6.'da verilmiştir [47, 48].



Şekil 2.6. Retina örnekleri

Retina tanıma sisteminin avantajları:

- En güvenilir yöntemler arasındadır.
- Doğruluk oranı oldukça yüksektir.
- Bu zamana kadar retina tanıma sistemlerinde sahteciliğe rastlanmamıştır.

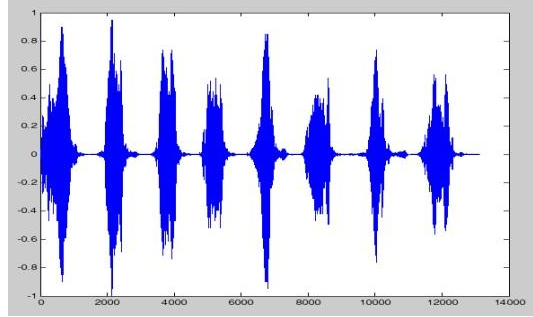
Dezavantajları:

- Maliyeti yüksektir.
- Damar ve göz hastalıkları damar yapısını etkiler. Bu da sistemdeki eşleşmeyi güçleştirir [36].

2.6. Ses Tanıma

Biyometride ses sistemi, ağız, burun çukurları ve diğer insan konuşma mekanizmalarının bütünü ses izi olarak adlandırılır. Ses izi her insanda tektir ve bu özellikler diğer insanlardan farklıdır. Ses izi tanımanın en büyük sıkıntısı, kapasitesi yüksek olan sistemlerde doğruluk oranının düşmesidir. Özellikle, çok fazla tanımlı insan olması durumunda ses izlerinin benzer olması nedeniyle yanlış eşleştirmeler söz konusu olabilmektedir. Bununla beraber, kullanıcının o andaki duygusal veya fiziksel durumundan

kaynaklanan ses deęiřiklięi de bařarının dūřmesine neden olabilmektedir [49]. Ses rnekleri řekil 2.7.'da verilmiřtir.



řekil 2.7. Ses rnekleri

Ses tanıma sistemlerinin avantajları:

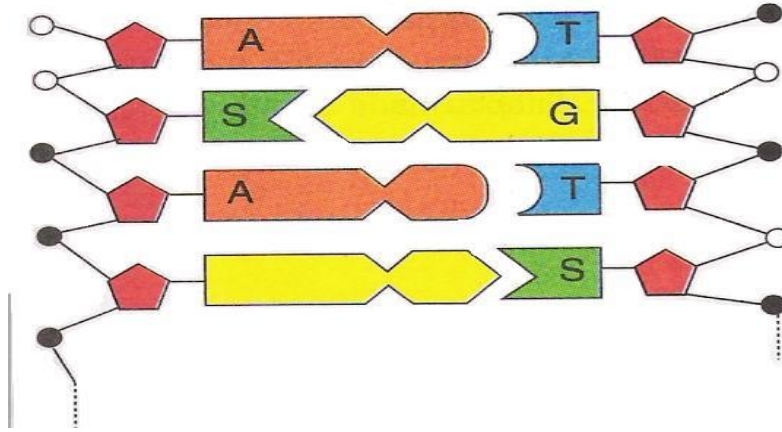
- Kullanımı kolaydır.

Dezavantajları:

- Fiziksel ortamdaki grltlerden etkilenir.
- İnsan sesinin bir cihaz yardımıyla kopyalanması ve sistemde kullanılması kolaydır.
- Grip, nezle vs. gibi hastalıklar sesi etkiledięinden sistemin performansını da etkiler [36].

2.7. DNA Tanıma

Biyometride bir bireyi tanımlamanın en kesin karřılıęı DNA haritasının oluřturulmasıdır. Bu yntemde DNA molekllerinin dizilimine gre doęruluk kontrol edilir. DNA yapısı, tek yumurta ikizleri hari kiřiden kiřiye farklılık gstermekte ve kan, kan lekesi, sa, tırnak, vb. pek ok farklı kaynaktan elde edilebilmektedir [50]. DNA rnekleri řekil 2.8.'da verilmiřtir [51].



Şekil 2.8. DNA örnekleri

DNA tanıma sistemlerinin avantajları:

- Son derece güvenilir ve doğruluğu üst düzeyde bir yapıdır.
- DNA yapısı kişinin pek çok özelliğinden elde edilebilir.

Dezavantajları:

- Pahalı sistemlerdir.
- DNA yapısı uzman kişiler tarafından hazırlanmazsa yanlış sonuçlar elde edilebilir.
- Tek yumurta ikizlerinde aynıdır.
- İşlem süresi 24 saat gibi bir zaman dilimini kapsadığı için hız gerektiren durumlarda bir dezavantaj olarak görülmektedir [36].

2.8. İmza, Yürüyüş, Tuş Vuruşu ve Konuşma Tanıma

Bu tanıma sistemleri biyometride davranışsal tanıma sistemleri arasında yer almaktadırlar. Her insanın davranışsal özellikleri kişiden kişiye belirli noktalarda farklılıklar göstermektedir. Bu özellikleri ortaya çıkaracak uygun algoritmalarla tanıma sistemleri oluşturulabilir [19].

Tablo 2.1.'de biyometrik yöntemlerin uygulamaları ile ilgili bir karşılaştırma yer almaktadır [36, 52].

Tablo 2.1. Biyometrik yöntemlerin karşılaştırılması

Biyometrik Yöntem	Benzersizlik	Performans	Yaygınlık	Değişmezlik	Elde Edilebilirlik	Kullanım Oranı
Parmak izi	Yüksek	Yüksek	Orta	Orta	Orta	Yüksek
Yüz	Düşük	Düşük	Yüksek	Orta	Yüksek	Yüksek
İris	Yüksek	Yüksek	Düşük	Yüksek	Orta	Orta
El Geometrisi	Orta	Orta	Orta	Orta	Yüksek	Yüksek
Retina	Yüksek	Yüksek	Düşük	Orta	Düşük	Düşük
DNA	Yüksek	Yüksek	Düşük	Yüksek	Düşük	Düşük
Ses	Düşük	Düşük	Yüksek	Düşük	Orta	Yüksek

Biyometrik yöntemler kullanım amaçlarına göre doğrulama, tanıma ve sınıflandırma olmak üzere üç ayrı alana ayrılır.

Doğrulama: Doğrulama işlemi iki adımdan oluşur. Birinci adımda veritabanının oluşturulması için her bir kişinin biyometrik özellikleri algoritmalar yardımıyla benzersiz bir koda dönüştürülerek veritabanına kaydedilir. İkinci adımda ise sisteme giriş yapılmak istendiğinde, girdi olarak alınan verinin veritabanında kayıtlı biyometrik özellikleri ile benzerlik yüzdesi belirlenir. Benzerlik oranı belirli bir değerin üzerinde ise sistemde kabul görülür ve bu durumda giriş izni verilir.

Tanıma/Algılama: Kimlik tespiti yapmayı amaçlayan bu yöntem girdiyi veritabanındaki kayıtlar ile eşleştirebilmektedir. Doğrulama işleminde kayıtlar arasındaki benzerlik yüzdesine bakılır ve girdinin kime ait olduğu ile ilgilenilmez. Tanıma/Algılama işleminde ise eşleştirme yapılır. Böylelikle kişi takibi gerektiren uygulamalarda kullanılabilir.

Sınıflandırma: Sınıflandırma biyometrik girdilerin benzer özelliklerine göre gruplandırılmasıdır. Bu adım özellikle işlem hızı gerektiren durumlarda kullanılır. Örneğin tanıma sırasında veritabanının tamamına değil de ortak sınıfa ait kayıtlar arasında karşılaştırma yapılır ve böylelikle büyük ölçüde performans artışı sağlanır [19].

3. VERİ GİZLEME YÖNTEMLERİ VE TARİHÇESİ

Veri gizleme yöntemleri günümüzde çok popüler alanlardan biri olmasına rağmen veri gizleme uygulamaları veri iletişimi kadar eskilere dayanır. İlk Yunan tarihçisi Herodot'un bir çalışmasında anlattığı gizli mesaj yollama tekniğinde; Histiaius, Pers işgali altındaki İyonya şehri Milet'e yolladığı kölesinin kafa derisine bir mesaj dövmelettirir. Zamanla kölenin saçı uzar ve mesaj saçın altında gizli kalır ve köle Milet valisi Aristogoras'a yollanır. Aristogoras, kölenin saçını traşlatır ve "Persliler'e karşı ayaklanma başlatın" gizli mesajını alarak bir ayaklanma çıkartır. Bu yöntem steganografik veri gizleme olarak adlandırılır. Steganografik veri gizlemede amaç veriyi gizli, güvenilir ve saldırılara karşı sağlam bir şekilde iletilmesi gereken yere gönderebilmektir. Mesaj "Bu köle Histiaius'undur" şeklinde köle ve sahibi hakkında bilgi içerecek şekilde dövmelettirilmiş olsaydı bu bir damgalama tekniği olacaktı [53].

MS 23-79 yılları arasında yaşayan Pliny the Elder, bitki sütü kullanarak kâğıt üzerine yazı yazmıştır. Kâğıt ancak ısıtıldığında yazı görülebilmıştır. Bu mektuplar kadınların küpelerinde taşınmıştır. İlerleyen zamanlarda yollanan mektuplardaki yazı karakterleri boyutu değiştirilerek mesajın kodlanması amaçlanmıştır [54].

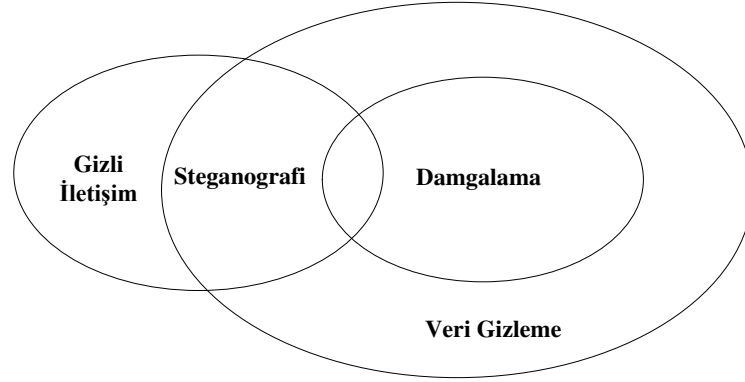
II. Dünya Savaşı'nın başlarında görünmez mürekkep ile görünen mektup satırlarına başka mesajların saklanarak iletilmesi sağlanmış ve bir anlamda şifreleme yapılmıştır. II. Dünya Savaşı'nda bir Alman ajanı bu yöntemi kullanarak aşağıda verilen normal cümle düzenindeki mektubu iletmiştir.

"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 harfleri dikkate alınarak "*Pershing sails from NY June I*" şeklinde ortaya çıkmaktadır [55, 56].

İlk kriptoloji ve steganografi kitabı Johannes Trithemius tarafından yazılmıştır [57]. Örtülü yazı anlamına gelen Steganografi kelimesi ilk olarak el yazması şekilde basılan Trithemius'un kitabında geçmiştir [58]. Veri gizleme alanındaki bir diğer yöntem olan damgalama ise ilk olarak 1990 yılında ortaya atılmış ve bu alanda ilk akademik konferans

1996 yılında düzenlenmiştir. Veri gizleme tekniklerinin damgalama ile olan ilişkisi Şekil 3.1.'de gösterilmiştir [59].

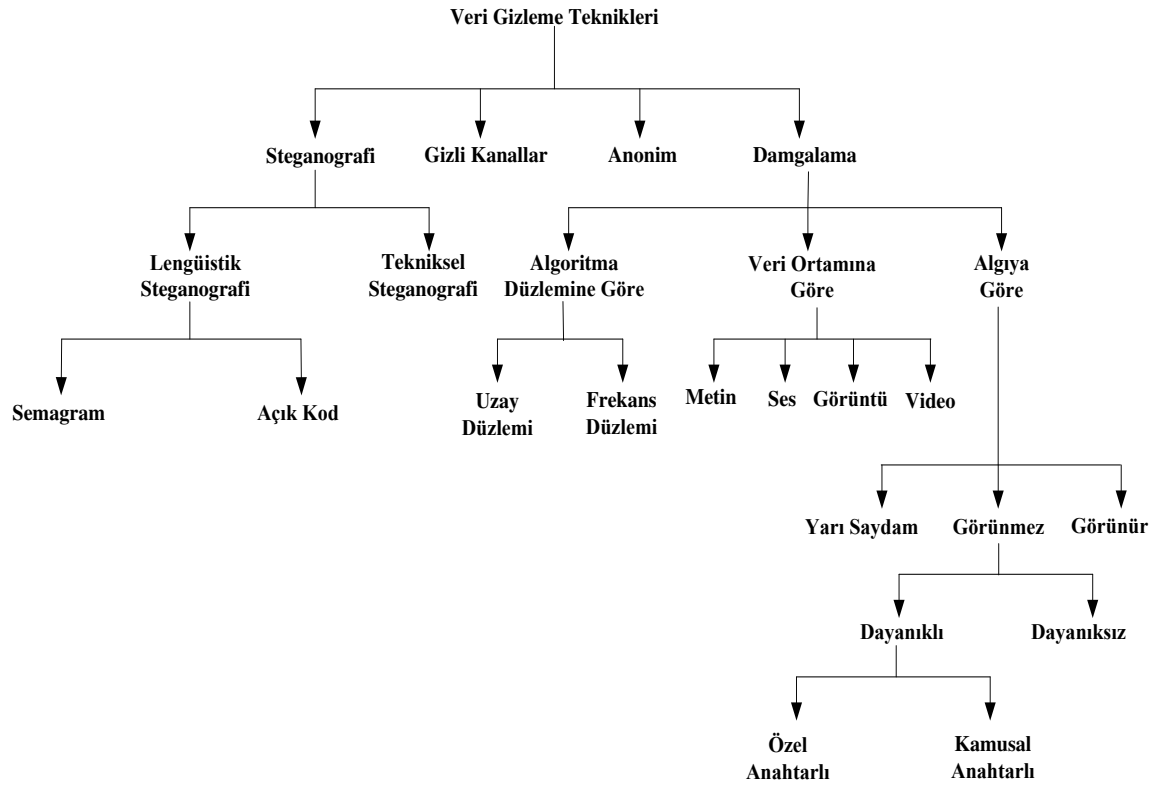


Şekil 3.1. Veri gizleme tekniklerinin damgalama ile olan ilişkisi

Günümüzde bilgi saklamaya ihtiyaç duyulmasının başlıca sebepleri aşağıda sıralanmıştır.

- Resim kullanarak gizli haberleşme
- Sayısal resimlerin sahipliği ve doğrulanması
- Veri bütünlüğünün sağlanması
- Sahtekârlık tespiti
- Videokasetlere parmak izi ekleme
- Resimlere başlık ekleme
- Akıllı tarayıcılar
- Videolara altyazı/ses gibi ilave bilgi ekleme
- Otomatik telif hakkı bilgisi
- Kopyalama kontrol

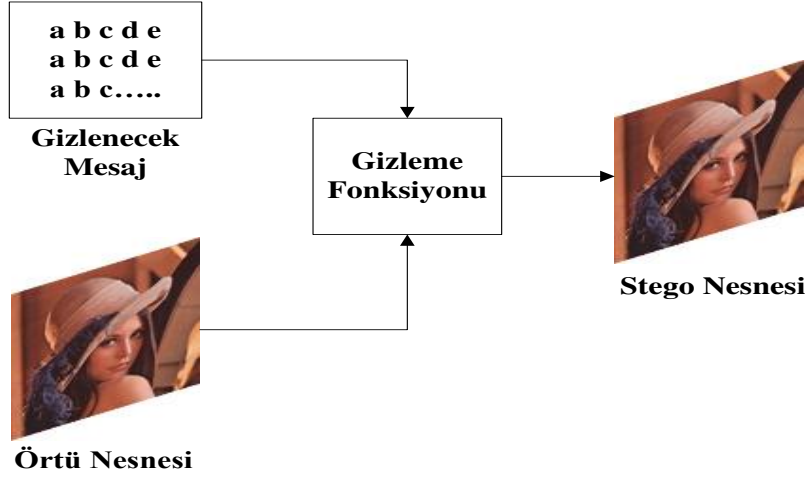
Tüm bu ihtiyaçların yanında veri gizleme işlemi yapılırken 2 temel sorunla karşılaşmaktadır. Eklenen bilginin algılanamaz yapılması ve gizlenen bilginin bütünlüğünün korunmasıdır. Veri gizleme teknikleri farklı uygulama alanları bulmuş ve çeşitli yöntemler geliştirilmiştir. Bu yöntemlerin sınıflandırılması Şekil 3.2.'de gösterilmiştir [60].



Şekil 3.2. Veri gizleme tekniklerinin türleri

3.1. Steganografi

Bir taşıyıcı ortama gizli mesajın eklenmesi ile yapılan iletişim türü olarak bilinen Steganografi, örtülü yazı anlamına gelmektedir [61]. Bir veri şifrelenerek ya da doğrudan gizlenerek taşıyıcı aracılığı ile karşı tarafa iletilir. Mesajın taşıyıcı üzerinde yapılacak değişikliklere karşı dayanıklı olması beklenmez. Buradaki amaç, fark edilmeyecek bir yöntem ile mesajı saklamak ve taşıyıcıya iletmektir [62,63]. Şekil 3.3.'de Steganografi yapısı gösterilmiştir. Mesaj, taşıyıcı içinde küçük bir değişiklik ile yok olabilecek kırılgan bir yapıya sahiptir. Steganografide, örtü nesnesinin insan algısı ile fark edilmeyecek ölçüde bozulmasına izin verilebilir [64,65].

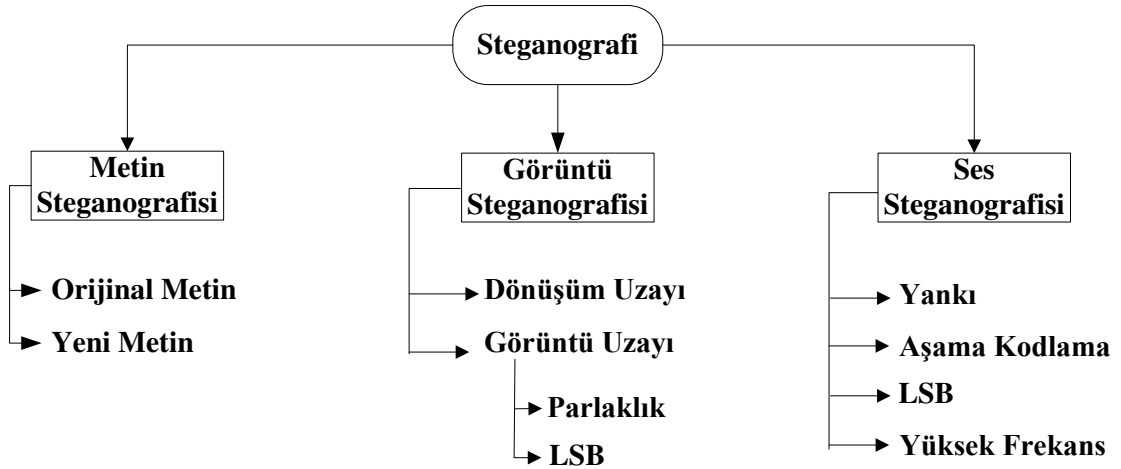


Şekil 3.3. Steganografik bir sistemin yapısı

Steganografinin uygulama alanları aşağıda sıralanmıştır.

- **Görünmez mürekkep:** Görünmez mürekkeple yazma yöntemidir.
- **Gizli yerler:** Fark edilmeyecek şekilde küpe, bavul vb. yerlere saklama
- **Microdotlar:** Noktalar halinde bilgiyi sayfaya gizleme
- **Bilgisayar tabanlı yöntemler:** Metin, ses, video, resim dosyalarını kullanarak veri gizleme yöntemleridir [66].

Steganografi kullanım alanları açısından üçe ayrılmaktadır. Bilgi gizlenecek ortam metin ise metin steganografisi olarak adlandırılmaktadır. Ortam olarak görüntü kullanılırsa görüntü steganografisi, ses kullanılırsa ses steganografisi denir. Bu sınıflandırma Şekil 3.4.'de verilmiştir.



Şekil 3.4. Steganografik yöntemlerin sınıflandırılması

Steganografi şifrelemeye yakın olmasına rağmen şifrelemeden farklıdır. Şifreleme mesajın içeriğinin korunması ile ilgilenirken steganografi mesajın varlığının gizlenmesi ile ilgilenmektedir. Dolayısıyla steganografi bir şifreleme yöntemi değil şifrelemeyi tamamlayıcı bir öğedir [67]. Steganografi birçok alanda ve çeşitli amaçlar için kullanılmaktadır. Bunlar şöyle belirtilebilir [68]:

– **Askeri:** Askeri durumlarda iletişimin şifrelenmesi her zaman yeterli olmamaktadır. Şifrelenmiş bir bilginin gönderildiği düşman tarafından fark edilebilir. Buna karşılık iletişim steganografik yöntemlerle yapılırsa çok daha başarılı olacaktır. Bu nedenle şifrelemeye alternatif olarak kullanılabilir.

– **Filigran ve parmak izi:** Hem filigranlar hem de parmak izleri gizlendiğinde bunun belli olmamasına ve güvenli olmasına ihtiyaç duyarlar. Bu nedenle, bu işlemde steganografiden yararlanılmaktadır.

– **Sağlık alanı:** Bazı sağlık sistemleri görüntüleri ve bunlar hakkındaki açıklamaları bir yere gönderebilir ve orada saklayabilir. Bazen bu görüntüler ve açıklamalar birbirinden ayrılabilir ve bu da tehlikeli sonuçlara yol açabilir. Eğer açıklama bilgileri görüntünün içine saklanırsa böyle bir durum ortadan kaldırılır. Bu işlem için de steganografi kullanılmaktadır [69].

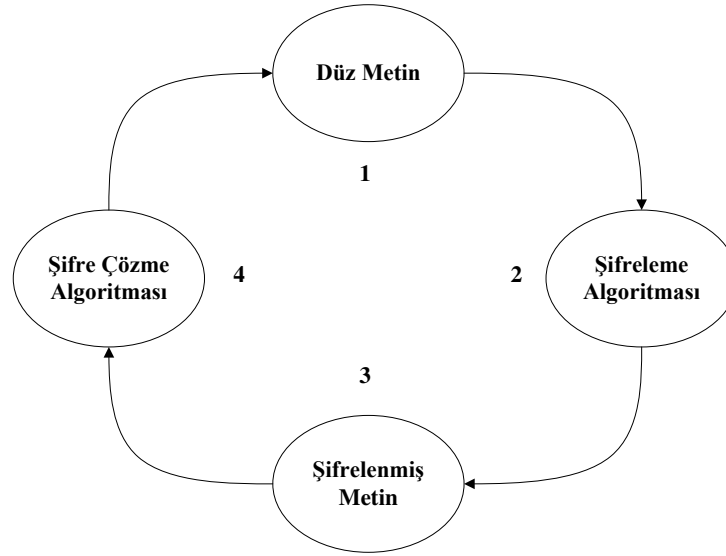
3.2. Kriptoloji

Veri gizleme yöntemlerinden biri olan kriptoloji şifreli belgeler bilimi olarak adlandırılmaktadır. Kriptografi ve Kriptoanaliz olmak üzere iki alana ayrılır. Metin şifrelemek için kullanılan teknikleri inceleyen bilim dalına Kriptografi denir. Şifrelenmiş bir metnin şifrelenmemiş hale getirilmesiyle ilgilenen bilim dalına ise Kriptoanaliz adı verilir [70, 71]. Bir kriptolojik sistem dört ana fonksiyona sahip olmalıdır:

- **Gizlilik:** Bilgi istenmeyen üçüncü şahısların eline geçmemelidir. İletim kanalında fark edilemeyecek yapıda olmalıdır.
- **Bütünlük:** Bilgi şifrelendikten sonra iletim kanalında değiştirilmemeli ve şifre çözme işleminden sonra bilgi bütünlüğü bozulmamalıdır.
- **Reddedilemezlik:** Bir kriptolojik sistem bilgiyi gönderen kişinin daha sonra gönderdiği bilgiyi inkâr etmemesi için bilgi gönderim işlemi tamamlandıktan sonra alındı onayını sağlamalıdır.

- **Kimlik Belirleme:** Kimlik belirleme işlemi, bilginin doğru kaynaktan alındığını doğrulamak için kullanılır.

Şekil 3.5.'de şifreleme ve şifre çözme adımları gösterilmiştir [72,73].



Şekil 3.5. Şifreleme ve şifre çözme basamakları

Kriptoloji kullanılan algoritma, anahtar sayısı ve şifrelenecek mesajın tipine göre sınıflandırılabilir.

Kullanılan algoritmaya göre kriptoloji

- Algoritması gizli olan kriptoloji
- Algoritması açık olan kriptoloji

Anahtar sayısına göre kriptoloji

- Simetrik kriptoloji
- Asimetrik kriptoloji

Mesaj tipine göre kriptoloji

- Akan şifre algoritmaları
- Blok algoritmaları şeklinde sınıflandırılabilir [73].

Simetrik ve asimetrik kriptoloji arasındaki fark; simetrik algoritmada şifreleme ve şifre çözme için aynı anahtar kullanılırken asimetrik algoritmada farklı anahtar kullanılır. Genel olarak simetrik kriptoloji, asimetrik kriptolojiden daha hızlı çalışır.

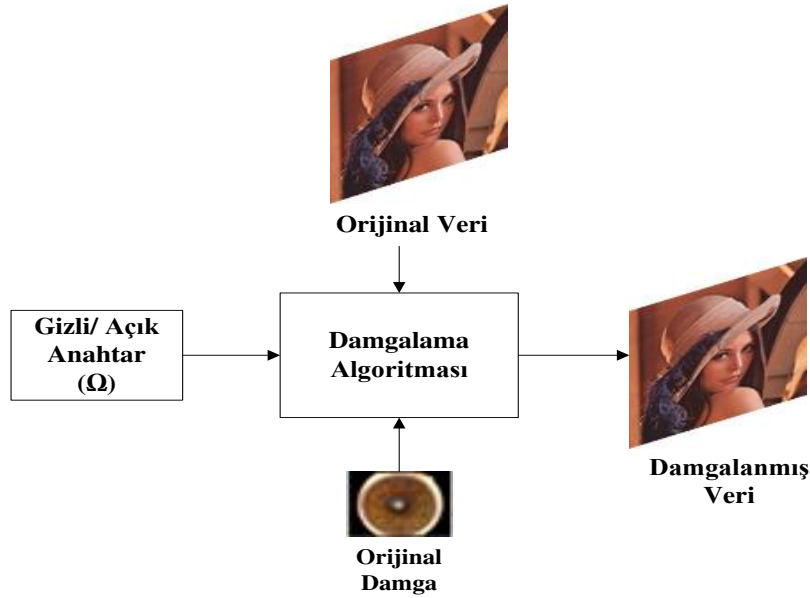
Akan şifre algoritmalarında ise şifrelenecek metindeki her bit ayrı ayrı şifrelenir. Blok algoritmalarında ise bit gurubu tek parçaymış gibi şifrelenir.

Kriptolojide steganografiden farklı olarak herhangi bir taşıyıcı kullanılmaz. Gizlenmesi gereken mesaj, bir algoritma kullanılarak şifrelenir ve şifreli mesajın kendisi herhangi bir taşıyıcı kullanılmadan gönderilir. Alıcı, aldığı mesajı deşifre ederek asıl mesaja ulaşır [74]. Sayısal içeriğe erişimi yetkisiz kişiler şifrelenmiş mesajı elde etse bile deşifre algoritmasını bilmedikçe mesajın aslını elde edemezler [75].

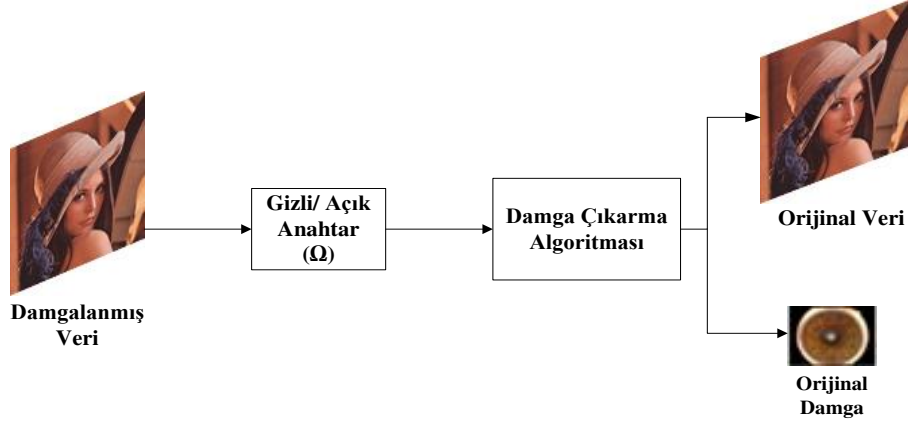
3.3. Sayısal Damgalama

Bilgisayar ve bilgisayar ağlarının gelişmeye başlaması ile birlikte verilerin (çoklu ortam, biyometrik vb.) kopyalanması, dağıtılması ve değiştirilmesi kolaylaşmıştır. Verilere aitlik özelliğinin kazandırılması ve korunmasında veri gizleme tekniklerinden damgalama kullanılmaktadır [76].

Damgalama, steganografi uygulamaları ile benzer yapıdadır. Ancak damgalamada steganografiden farklı olarak damganın aitliğinin belirlenmesi sağlanmalıdır. Bu nedenle bilgisayar ortamındaki çalışmalara telif hakkı, lisans, logo vb. bilgiler damgalanır [77]. Temel damgalama işlemi Şekil 3.6.'da damga çıkarma işlemi ise Şekil 3.7.'de gösterilmiştir [78, 79].



Şekil 3.6. Temel damgalama işlemi



Şekil 3.7. Damga çıkarma işlemi

Damgalama işlemi uygulama alanına göre aşağıda belirtilen alanlarda kullanılmaktadır:

- **Ürünün yasal olarak sahibini belirleme:** Ürün içerisine ürünü oluşturan kişiye ait bir bilgi eklenir ve böylece yasal sahibin tescillenmesi amacıyla kullanılır.
- **Yasal olmayan kopyalamanın kaynağını belirleme:** Her ürüne farklı damgalar yerleştirilerek ürünü çoğaltan kaynağın tespit edilebilmesi için kullanılır.
- **İçeriğin çoğaltılmasını engelleme:** İçeriğin çoğaltılmasını engelleyecek yapıda bir damga eklenerek yasal olmayan kopyalamalar önlenir.
- **Ürün takibi:** Ürünün adedi, çalıntı olup olmadığı hakkında bilgi edinebilmek için kullanılır.
- **Ürünün orijinalliğinin tespiti:** Bir kaynaktan iletilen bilginin ulaştığı andaki veri ile eşleşme kontrolünü sağlar.
- **Tıp sektöründe hastaya ait bilgilerin muhafazası:** Hastaya ait bir anahtar yardımıyla hasta bilgilerinin gizlenmesi sağlanır.
- **Veri gizleme:** İki kullanıcı haberleşirken aynı zamanda veri gizlenerek özel mesajların saklanması amacı ile kullanılabilir [76].

3.4. Etiketleme

Etiketleme, sayısal bir çalışmanın belli bir tüketiciye dağıtılması öncesinde, telif haklarının korunması amacıyla, yalnızca o tüketiciyi temsil eden bilginin çalışmaya görünmez bir şekilde damgalanması işlemidir.

Etiketlemede kullanılan yöntemde bilgi, dışardan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her tüketiciye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir. Etiketleme, amaç bakımından sayısal damgalamadan farklı ancak yöntem olarak sayısal damgalama ile aynı özellikleri gösterir [80].

3.5. Sayısal İmzalama

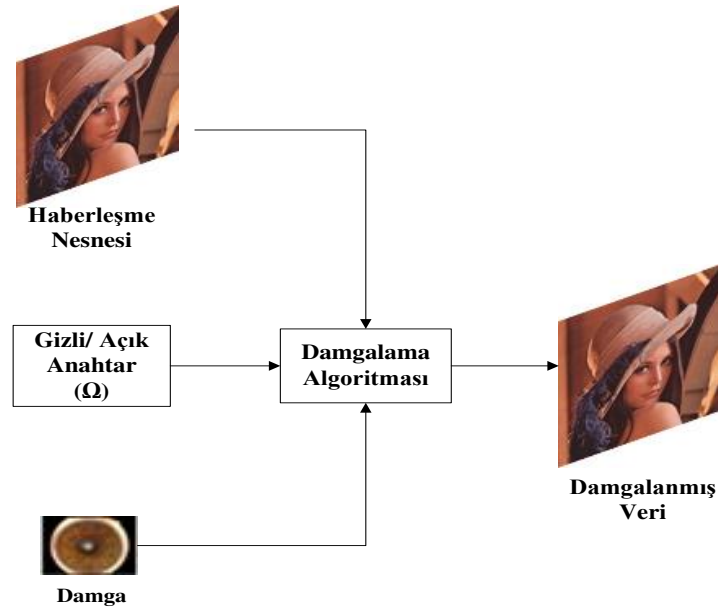
Sayısal imzalama, doküman sahibinin kendi kişisel anahtarı ile dokümanı imzalaması, yani şifrelemesidir. Bu kişisel anahtardan üretilen kamusal anahtar, dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır.

Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Kişisel bir anahtar ile imzalanan doküman, sahibi hakkındaki bilgiyi de birlikte taşımış olur. Sayısal damgalama ile sayısal imzalamanın eş anlamlı olduğuna dair görüşlere karşın bunları birbirinden ayrı tutan görüşler de vardır.

Sayısal dokümanların imzalanması için uygulamada çeşitli yazılımlar vardır. Herhangi birisi için oluşturulan kamusal ve kişisel imzalar, kendisine elektronik kartlarda verilir. Ancak birçok yerde yasal düzenlemelerin ve teknik altyapının tamamen sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır. Göndericinin kişisel imzası kullanılarak şifrelendiğinden inkâr edilemez ve imza taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan doküman üzerinde değişiklik yapamaz [81].

4. SAYISAL DAMGALAMA SİSTEMLERİ

Sayısal damgalama, kişiye ait bir eserin içine kişi ya da eserin konusuyla ilgili bir mesajın yerleştirilmesi amacıyla eserin algılanamayacak şekilde değiştirilmesidir [82]. Sayısal damgalamada amaç bir ses ya da görüntü dosyası içerisine bir damganın eklemek değil bir kişiye ait olduğunu belirtmektir [60]. Şekil 4.1.'de damgalama yönteminin blok diyagramı verilmiştir. Şekilden de görülebileceği gibi haberleşme nesnesi ve damga birbirleriyle ilişki içerisindedirler [83, 84].



Şekil 4.1. Damgalama yönteminin blok diyagramı.

Damgalama, bilgisayar teknolojisinin gelişmesi ile beraber sayısal verilerin kopyalanması, çoğaltılması, değiştirilmesi işlemlerinin kolay bir hal alması sonucu bir ihtiyaç olarak doğmuştur. Ayrıca damgalama sadece sayısal verilere değil kâğıt para, kâğıt, kumaş, giysi etiketleri gibi fiziksel nesnelere de uygulanabilmektedir. Fiziksel nesnelere bu nesnelerin yapım aşamasında damga eklenerek uygulanır. [53, 85].

Sayısal damgalama uygulamaları aşağıda belirtilen farklı amaçlar için kullanılmaktadır ve gelişen teknoloji paralelinde kendisine yeni uygulama alanları bulmaktadır [86- 88].

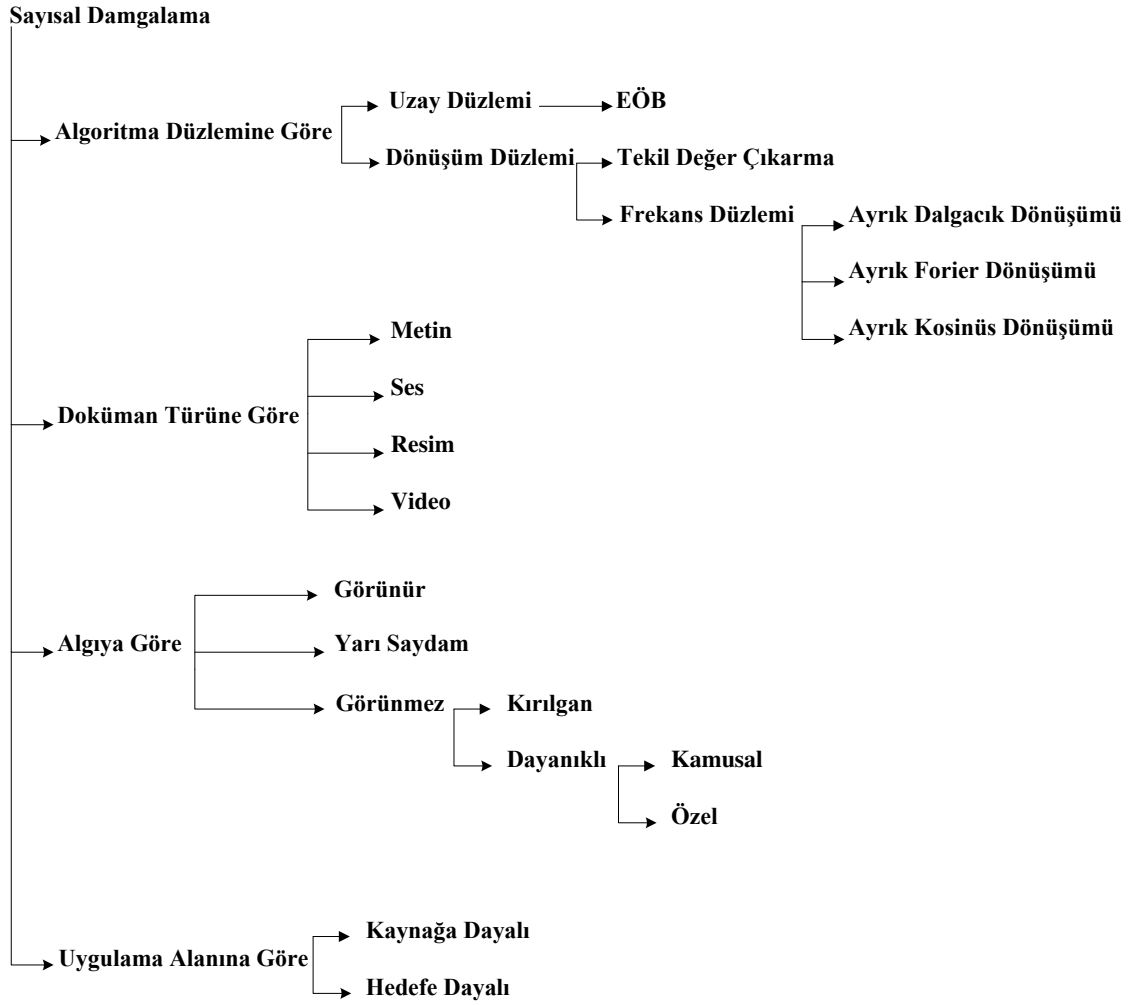
- **Eser sahibinin belirlenmesi:** Telif haklarının korunması için verinin sahibi hakkında herhangi bir bilginin orijinal nesne içerisine yerleştirilmesi

uygulamalarında kullanılır. Sanat eserlerinde, çoklu ortam uygulamalarında görünür ya da görünmez damga şeklinde kullanılabilir.

- **Yayın takibi:** Yayın süresinin belirlenmesi için kullanılır.
- **İşlem takibi:** Eserin yasal satışında alıcı kaydedilir. Böylelikle yasal olmayan dağıtımların kaynağı bulunur. Bunun için her yasal kopyaya farklı bir damga eklenerek hangi yasal kopyanın kime dağıtıldığı takip edilebilir.
- **İçeriğin doğrulanması:** Çoklu ortam verilerinin kolayca kopyalanabilmesi, çoğaltılabilmesi ve hatta değiştirilebilmesi gibi sorunlardan dolayı alıcı ile gönderici arasında iletilen herhangi bir verinin iletim kanalında değiştirilmediğinin teyidi için, damgalama yöntemleri kullanılır.
- **Cihaz takibi-kontrolü:** Belirlenen hedefe göre cihazların kontrol edilmesi gibi uygulamalarda yer alırlar.
- **Arşivleme:** Sayısal arşivlerin elde edilmesi için kullanılır.
- **Kopya kontrolü/ takibi/ belirlenmesi:** Yasal olmayan kopyalamaların engellenmesi için kullanılır. Gönderici ile alıcı taraftaki anahtar/damga uyuşmazsa iletim işlemi gerçekleştirilmez.

4.1. Sayısal Damgalama Türlerinin Sınıflandırılması

Kullanım alanlarına göre sayısal damgalama Şekil 4.2.'de gösterildiği gibi algoritma düzlemi, doküman türü, uygulama alanı ve algıya göre dört sınıfa ayrılabilir [85].



Şekil 4.2. Sayısal damgalama türlerinin sınıflandırılması

4.1.1. Algoritma Düzlemine Göre Damgalama

Algoritma düzlemine göre damgalama ikiye ayrılır [89].

- Uzay bölgesinde damgalama
- Dönüşüm bölgesinde damgalama

Uzay bölgesinde yapılan damgalama işleminde damgalanmak istenen nesnenin bitleri gizlenecek nesnenin en önemsiz bitine eklenir. Böylece damga nesneye kaydedilir. Uzay bölgesinde saklanabilecek bilgi miktarı sınırlıdır. Bu nedenle bu bölgede yapılan damgalama, saldırılara karşı dayanıksızdır. Damgalanmış nesnenin en önemsiz bitleri silinerek damga kolaylıkla yok edilebilir. Bu tür zorlukların aşılabilmesi için dönüşüm bölgesinde damgalama teknikleri geliştirilmiştir [90]. Bir resim farklı frekans bantlarına

ayrılarak matematiksel fonksiyonlarla damga ekleme işlemi yapılır. Böylelikle damganın dayanıklılığı artırılmış olur [85].

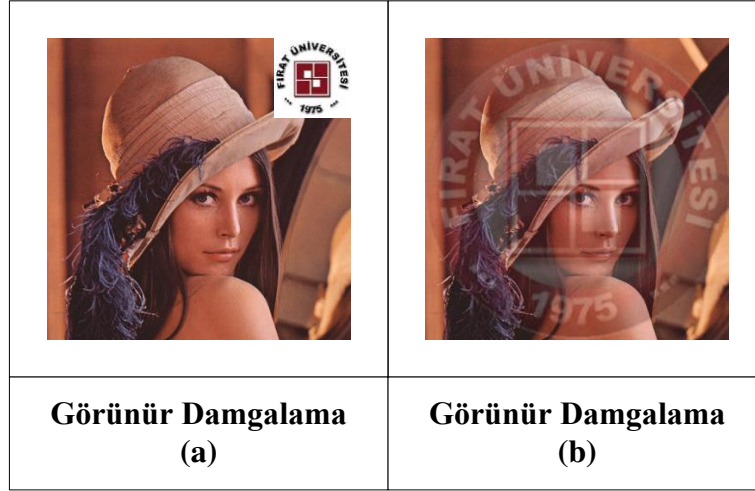
4.1.2. Algılanabilirlik Özelliğine Göre Damgalama

Algılanabilirlik özelliğine göre damgalama Şekil 4.3.'de gösterildiği gibi görünür ve görünmez damgalama olmak üzere iki alanda incelenebilir [91].



Şekil 4.3. Algılanabilirlik özelliğine göre damgalama türleri

Görünür damgalamada asıl nesne içerisine eklenen damga, hem renkli hem de tek renk uygulamalar için görünür yapıdadır. Görünür damgalama uygulamaları Şekil 4.4.'de gösterildiği gibi farklı şekillerde kullanılabilir. Şekil 4.4.a.'da gösterilen damgalama türünde damga resimden kolaylıkla kesip çıkarılabilir. Bu tür damgalama uygulamalarında damga görüntü üzerinde önemli bir bölüme yerleştirilmeli ve böylece görüntü üzerinden ayrılması zor olmalıdır. Şekil 4.4.b.'deki gibi yarı saydam şekilde eklenen damgada ise orijinal görüntünün ayrıntıları korunmalıdır.



Şekil 4.4. Görünür damgalama türleri

Yapılan çalışmaların çoğu görünmez damgalama üzerine yoğunlaşsa da, görünür damgalama pek çok alanda kendine uygulama alanı bulmuştur.

Görünür damgalama

- Logo ve tescil şeklinde olduğundan dolayı kanuni sahibi belli olması ve illegal olarak çıkarılamaması,
- Kullanım haklarını göstermesi
- Hızlı olması,
- Haberleşme nesnesine doğrudan uygulanması

gibi birçok olumlu özelliğe sahip olmasına rağmen, haberleşme nesnesinin kalitesini azaltması ve saldırılara karşı dayanıksız olması gibi olumsuzlukları da mevcuttur.

Görünmez damgalamanın görünür damgalamadan en önemli farkı görüntü kalitesinde değişikliğe izin vermemesidir. Ayrıca bu damgalama uygulamalarının görüntü kalitesinde gözle fark edilebilecek bozulmalara karşı dayanıklı yapıda olması için çeşitli yöntemler geliştirilmiştir. Bu tür uygulamalarda insan görme sistemi baz alınır ve tüm bu özelliklerinden dolayı steganografi uygulamalarını da kapsar. Ayrıca görünmez damgalama, görünür damgalama uygulamalarına göre saldırılara karşı daha dayanıklıdır ve daha yaygın olarak kullanılır.

Yüksek kalitedeki görüntüler ve sanat eserlerinde yapılan görünmez damgalama uygulamalarında görüntü kalitesinin değişmemesi çok önemlidir. Bunun için kullanılacak yöntem iyi tespit edilmeli ve değişen piksel sayısının çok az olması sağlanmalıdır.

Yarı saydam damgalamada ise haberleşme nesnesinde gözle görülür küçük bir değişim kabul edilebilir. Örneğin kayıplı sıkıştırma uygulamalarında yarı saydam damgalama kendine uygulama alanı bulmuştur.

Tüm bu damgalama uygulamaları, damganın geri çıkarılması işlemi için bilgisayar ve işletim sistemlerinden bağımsız çalışmalıdırlar [83, 87].

4.1.3. Uygulama Alanına Göre Damgalama

Kaynağa dayalı damgalama işleminde tüm orijinal kopyalara aynı damga eklenir. Böylelikle dağıtılan öğelerin ya kopyalanması engellenmeye çalışılır ya da bu öğelerin orijinal olup olmadığı tespit edilebilir. Hedefe dayalı damgalama işleminde ise dağıtılacak tüm kopyalara farklı damga eklenir. Böylelikle müşteri takibi sağlanmış olup kopyalama işleminin kim tarafından yapıldığı tespit edilebilir [92].

4.1.4. Doküman Türüne Göre Damgalama

4.1.4.1. Resim ve Video Damgalama

Sabit veya hareketli görüntülerin içerisine gizli verinin eklenmesi işlemine resim/video damgalama denir. Damgalama uygulamaları en çok sabit görüntüler üzerinde kullanılmıştır. Siyah-beyaz veya renkli görüntüler, kullanılan yöntemle göre belli formata dönüştürülür. Dönüştürülmüş görüntünün parlaklık değerine veya renk bileşenlerine işlenmiş damga eklenir. Kullanım alanına göre damga görünür veya görünmez olabilir. Görünmez damgalama uygulamalarında insan görme sistemi baz alınır. Damgalanmış resim; sıkıştırma, ölçeklendirme, kırpma, bulanıklaştırma, keskinleştirme, Analog/Dijital dönüşüm, Dijital/Analog dönüşüm, gürültü ekleme gibi yaygın saldırılara karşı dayanıklılığını korumalıdır.

Görüntü damgalama uygulamalarında damga ve asıl görüntü belirli bir yöntemle göre işlenir ve damga, asıl görüntüye ya da işlenmiş haline doğrudan eklenir. Damga, asıl görüntüyle ilişkili bir bilgidir ki bu özellik, steganografi ve damgalama arasındaki en önemli farktır. Steganografide, örtü nesnesi ile gizlenecek veri arasında bir ilişki aranmaz. Damgalamada ise asıl görüntü ile damga birbiriyle ilişkili öğelerdir. Video damgalama görüntü damgalama uygulamalarının devamıdır. Görüntü damgalama ve damga çıkarma

için kullanılan yöntemler, video damgalama uygulamaları için yeniden düzenlenmiş ve kullanılmıştır. [92, 93].

4.1.4.2. Metin Damgalama

Sayısal damgalama, ilk olarak metin damgalama alanında kullanılmıştır. Metin damgalama işleminde damga, metin aralarındaki boşluklara ya da font şekillerinin içine yerleştirilir. Bu damgalama şeklinde font tipi değiştirilirse veya metin boşlukları silinirse damga yok olabilir.

Elektronik ve bilgisayar alanlarındaki gelişmeler paralelinde hemen hemen tüm bilgilerin sayısal ortamda saklanması mümkün olmuştur. Bununla beraber metin damgalama işlemi de elektronik ortamda yapılmaya başlanmıştır. Elektronik metin damgalama, beraberinde satır ve kelime ötelemeye dayalı metin damgalama yöntemlerinin gelişmesine yol açmıştır. Bu yöntemlerde metnin ikili yazı bölgelerinde damgalanması sağlanarak, saldırılara karşı dayanıklılığı artırılmıştır [94].

4.1.4.3. Ses Damgalama

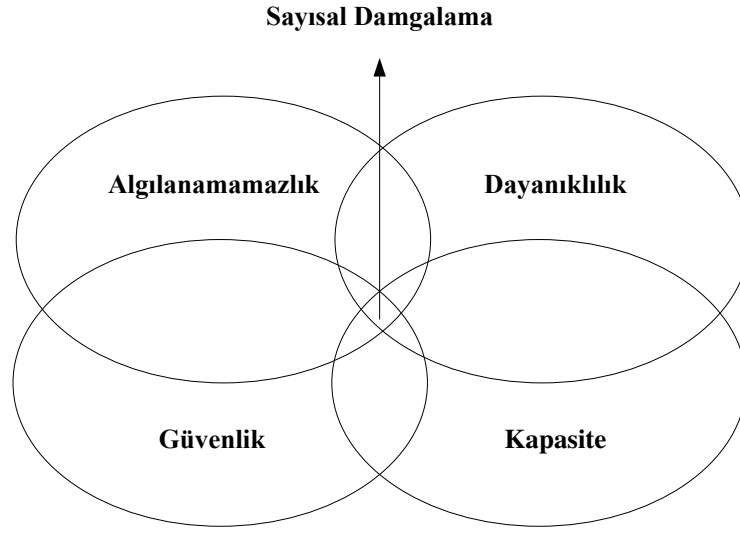
Yeni nesil taşınabilir müzik aletlerinde telif haklarının korunması ve sayısal müziklerin güvenliğinin sağlanması, izinsiz çoğaltılmasının engellenmesi için çeşitli ses damgalama yöntemleri geliştirilmiştir. Ses damgalama işleminde, damga ya doğrudan ses işaretine, ya da sıkıştırılmış ses paketinin bitlerine eklenir. Bu yöntemde ölçüt insan duyma sistemidir. Haberleşme nesnesine damga eklendikten sonra insan duyma sistemi tarafından algılanamayacak yapıda olmalıdır.

Ses işaretlerinin damgalanması işlemi tıpkı video ve resim damgalanmasında olduğu gibi sıkıştırma, algılanamamazlık, filtreleme gibi pek çok saldırılara karşı dayanıklılık göstermelidir.

Ses damgalama için genişletilmiş spektrum, yansıma kodlaması ve faz kodlaması gibi yöntemler geliştirilmiştir. Haberleşme nesnesi ve damganın sayısallaştırılıp frekans bantlarına ayrılarak uygun algoritmalar ile insan duyma sisteminin algılayamayacağı şekilde birbirine eklenmesi bu tür yöntemlerdeki ortak noktadır [92].

4.2. Sayısal Damgalama Sistemlerinin Özellikleri

Sayısal damgalama uygulamaları, Şekil 4.5.'de gösterildiği gibi algılanamamazlık, güvenlik, kapasite ve dayanıklılık olmak üzere 4 özelliğe göre değerlendirilebilir. Bu dört özellik birbirleriyle etkileşim içerisindedir [92]. Örneğin çok dayanıklı bir damgalama sistemi için asıl görüntünün her biti üzerinde değişiklikler yapılmalıdır. Bununla beraber asıl görüntünün her biti üzerinde yapılan değişiklik damganın algılanamamazlık özelliğini azaltır. Bu dört özellik birbirini etkilediğinden dolayı bir damgalama sistemi tasarlanırken kullanım amacı ve yerine göre en uygun karakteristik özellikler belirlenmelidir [93].



Şekil 4.5. Sayısal damgalama sistemlerinin özellikleri

4.2.1. Algılanamamazlık:

Görünmez damgalama uygulamalarında; damga, asıl görüntünün kalitesini değiştirmeyecek nitelikte olmalıdır. İnsan algısı tarafından damgalanmış görüntü ile asıl görüntü arasında bir fark sezilmemelidir. Ancak asıl görüntünün sadece gönderici ve alıcıda olduğu damgalama uygulamaları için belirli bir sınırdan bozulma, görünmez damga uygulamalarında sorun teşkil etmemektedir [94].

4.2.2. Kapasite:

Asıl görüntünün içerisine eklenebilecek bilgi miktarıdır. Asıl görüntüde bozulmaya yol açmadan kullanılacak uygulama ve yönteme göre bu miktar değişebilmektedir. Eklenecek bilgi miktarı ne kadar az ise asıl görüntü saldırılara karşı o kadar güçlü ve güvenli olur. Günümüz damgalama uygulamalarında eklenecek bilgi miktarının artırılması yanında saldırılara karşı dayanıklılığının da aynı oranda korunması amaçlanmaktadır [95].

4.2.3. Güvenlik:

Saldırlara karşı dayanabilme becerisine denir. Damgalama sistemlerinin güvenlik ölçüsü, gönderilen gizli bilginin yetkisiz kişilere ulaşmamasına, sadece alıcı ve gönderici arasındaki iletişiminin sağlanmasına bağlıdır [96].

4.2.4. Dayanıklılık:

İletişim sırasında yapılan tüm uygulamalara rağmen asıl içeriğin varlığını sürdürebilme yeteneğidir. Tüm damgalama uygulamaları dayanıklılık özelliği göstermek zorunda değildir. Bu damgalama sistemlerine kırılğan damgalama denir ve kırılğan damgalama uygulamaları küçük bir değişiklikte bile zarar görecektir. Kırılğan damgalama, gizli veri üzerinde değişiklik olup olmadığının tespiti için kullanılır [97].

4.3. Sayısal Damgalama Sistemlerine Yapılan Saldırıları

Sayısal damgalama alanındaki gelişmeler beraberinde bu yöntemlerin başarımını azaltmaya ve gönderilecek bilginin engellenmesine yönelik saldırı yöntemlerinin de artmasına sebep olmuştur. Damgalama saldırıları farklı şekillerde sınıflandırılabilir [98].

4.3.1. Basit Saldırıları

Görüntü işleme ve sıkıştırma uygulamaları olarak bilinir. Buradaki amaç görüntü üzerinde yapılan değişikliklerle damganın sezilmesi ve hedefe uygun olarak silinmesi ya

da değiştirilmesinin sağlanmasıdır. Sıkıştırma, gürültü ekleme, kuantalama bu saldırılara örnek olarak verilebilir [99].

4.3.1.1. JPEG Kayıplı Sıkıştırma

JPEG, görüntü kalitesindeki değişikliği minimuma indirebildiği için sıkıştırma uygulamalarında en çok kullanılan yöntemlerin başında yer alır. JPEG sıkıştırma, Ayrık Kosinüs Dönüşümü tabanlı olarak görüntünün yüksek frekanslı bileşenlerinin belirlenen sıkıştırma oranında silinmesine dayanır. Bu özelliği nedeniyle JPEG sıkıştırma, iletim kanalında nesnede damganın silinmesi ya da zarar görmesi amacıyla yaygın olarak kullanılmaktadır [98].

4.3.1.2. Gürültü Ekleme

Damgalama işlemlerinde asıl nesne çeşitli yöntemlerle işlenecek duruma getirilir ve damga asıl nesneye eklenir. Bu durumda asıl nesnenin pikselleri büyük oranda değişikliğe uğramış olur. Gürültü ekleme işlemi, damgalanmış nesnenin insan algısının algılamayacağı oranda piksellerini rastgele değiştirme işlemidir. Böylelikle damga zarar görmekte ve alıcı tarafa istenilen şekilde ulaşamamaktadır [99].

4.3.1.3. Kırpma

Damgalanmış resmin belli bir kısmı kesilip çıkarılarak damganın zarar görmesi amaçlanır. Görünür damgalama işlemlerinde damga, nesnenin belli bir kesimine yerleştirilmiş ise bu saldırı kolaylıkla hedefine ulaşmış olur. Nesnenin tümüne yayılmış görünür yada görünmez damgalama uygulamalarında hedeflenen bir kısım kesip çıkarılarak damganın alıcı tarafa anlamlı bir şekilde ulaşması engellenir [100].

4.3.2. Geometrik Saldırıları

Damgalanmış nesne ile asıl görüntü arasındaki uyum bozularak damganın alıcı tarafa ulaşması engellenmeye çalışılır. Boyutlandırma, kırpma, öteleme gibi saldırılarda

damganın zarar görmesi amaçlanır. Bu saldırılar geri alındığında damga yeniden elde edilebilir [98].

4.3.2.1. Yatay Eksende Döndürme

Damgalanmış nesne Şekil 4.6.'da gösterildiği gibi yatay eksende döndürülür. Nesnenin piksel oranları üzerinde değişiklik yapılmadığı için nesne ters yönde yatay olarak döndürülürse damgalanmış nesneden damga yeniden elde edilebilir.



Şekil 4.6. Damgalanmış nesnenin yatay eksende döndürülmesi

4.3.2.2. Dikey Eksende Döndürme

Bu işlemle damgalanmış nesne Şekil 4.7.'de gösterildiği gibi dikey eksende döndürülür. Yatay eksende döndürme işleminde olduğu gibi nesnenin piksel oranları üzerinde değişiklik yapılmadığı için nesne ters yönde dikey olarak döndürülürse damgalanmış nesneden damga yeniden elde edilebilir.



Şekil 4.7. Damgalanmış nesnenin dikey eksende döndürülmesi

4.3.2.3. Açılı Döndürme

Damgalanmış nesne Şekil 4.8.'de gösterildiği gibi saat yönünde ya da tersi yönünde döndürülerek damganın zarar görmesi amaçlanır. Bu durumda damgalanmış nesne döndürüldüğü yönün tersi ya da asıl nesne damgalanmış nesnenin döndürüldüğü yönde döndürülürse damga orijinal haliyle yeniden elde edilebilir. Açılı döndürme, yatay ve dikey yönde döndürme saldırılarına karşı daha hassastır.



Şekil 4.8. Damgalanmış nesnenin 30° döndürülmesi

4.3.2.4. Ölçekleme

Damgalanmış nesneye eşit oranda yatay ve dikey ölçeklendirme yapılabileceği gibi farklı oranlarda yatay ve dikey ölçeklendirme de yapılabilir. Farklı oranda yapılan ölçeklendirmede, damganın esas haliyle alıcı tarafta elde edilmesi orantılı ölçeklendirmeye göre daha zordur. Şekil 4.9.'da ölçeklendirme türleri verilmiştir [100].



Şekil 4.9. Ölçeklendirme türleri

4.3.2.5. Satır veya Sütunların Yer Değiřtirmesi/ Silinmesi

Damgalanmış nesnenin iletim kanalında piksel yoğunluklarına göre, satır/sütunlarının bir sonraki/önceki satır/sütunlarla yer deęiřtirmesi/silinmesi ile damgaya zarar verme uygulamalarıdır.

4.3.3. Silici Saldırıları

Bu saldırıların amacı damgalanmış nesnedeki damgayı yok etmektir. Örneęin, En Önemsiz Bit yöntemi ile eklenen damga silinmesi en kolay damgalama çeşididir. Sayısallaştırılmış damganın her biti, sayısallaştırılmış asıl görüntünün her bir byte'nın son bitine eklenir. En Önemsiz Bit yöntemiyle damgalanmış görüntünün son bitleri silinirse görüntüdeki damga yok edilmiş olur. Şekil 4.10'da Görünür Damgalama için damga yok etme örneęi verilmiştir [101].

		
Damgalanmış Görüntü	Damganın Silinmesi	Çeşitli Resim Programlarıyla Çıkarılan Damganın Doldurulması

Şekil 4.10. Görünür damgalamada damgayı yok etme

4.3.4. Kriptografik Saldırıları

Damgalama işleminde kullanılan anahtar kriptografik saldırılarda hedefdir. Damgalanmış nesnedeki anahtarın bulunması ve böylece nesne içerisindeki damganın elde edilmesi amaçlanmaktadır [102].

4.3.5. Protokol Saldırıları

Gönderici ve alıcı arasında bilgi gönderilirken eklenen damganın iletişim kanalında çıkarılıp yerine yenisinin eklenmesi işlemi protokol saldırıları olarak alınır. Bu saldırılar telif hakkı uygulamaları için önemli bir zorluktur [98].

4.4. Damga Ekleme ve Çıkarma İşlemi

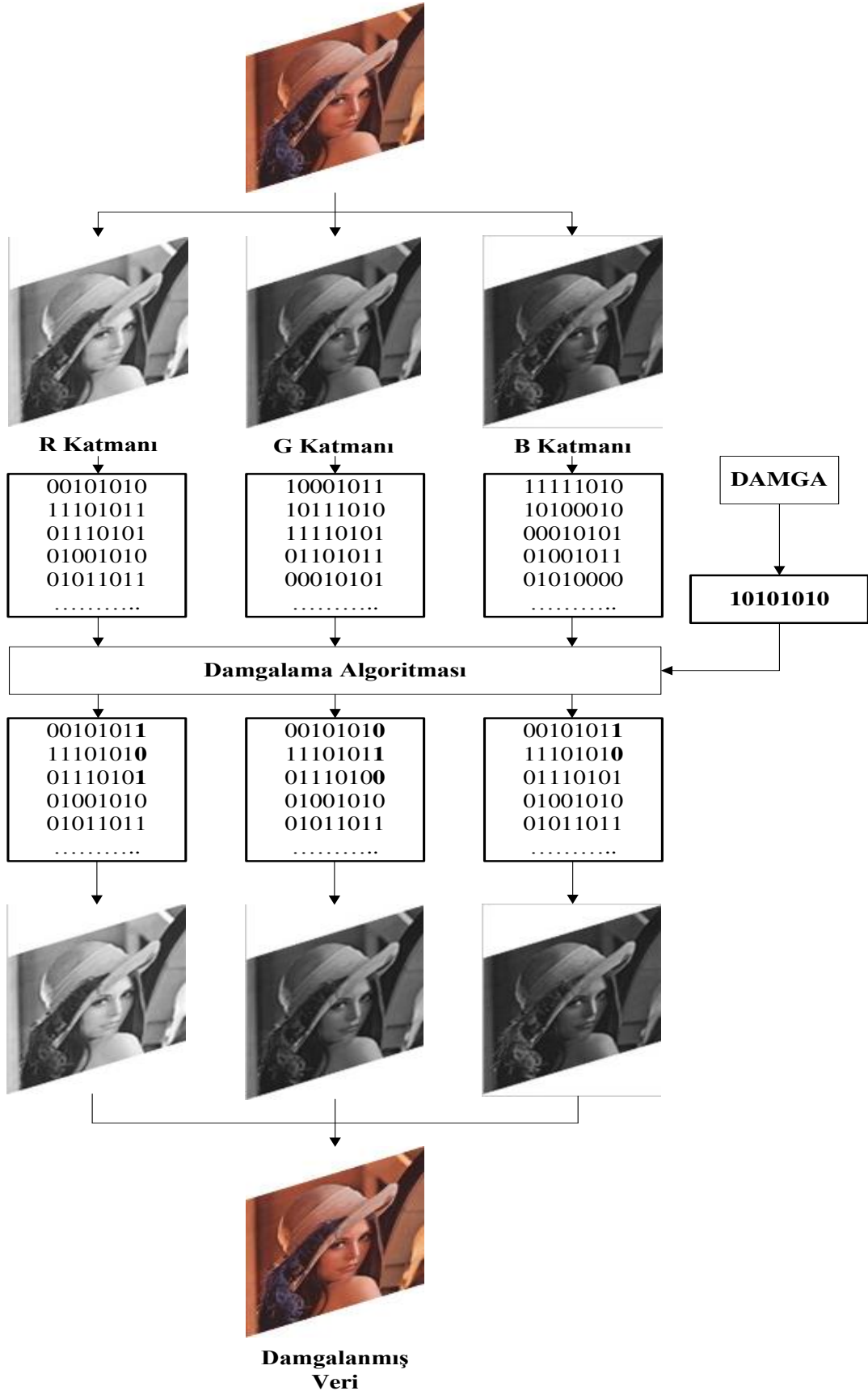
Damgalama, sayısal bir nesnesinin sahibi hakkındaki bir bilgiyi üzerinde saklamaya yönelik yapılan çalışmalardır. Bu alanda yapılan ilk çalışmalar sayısal görüntülerin en önemsiz bitinin değiştirilmesi üzerine yapılmıştır [93]. En Önemsiz Bit yöntemi baz alınarak bir damga ekleme işlemi Şekil 4.11.'de, damga çıkarma işlemi ise Şekil 4.12.'de gösterilmiştir.

Sayısal bir görüntüye damga ekleme işleminde

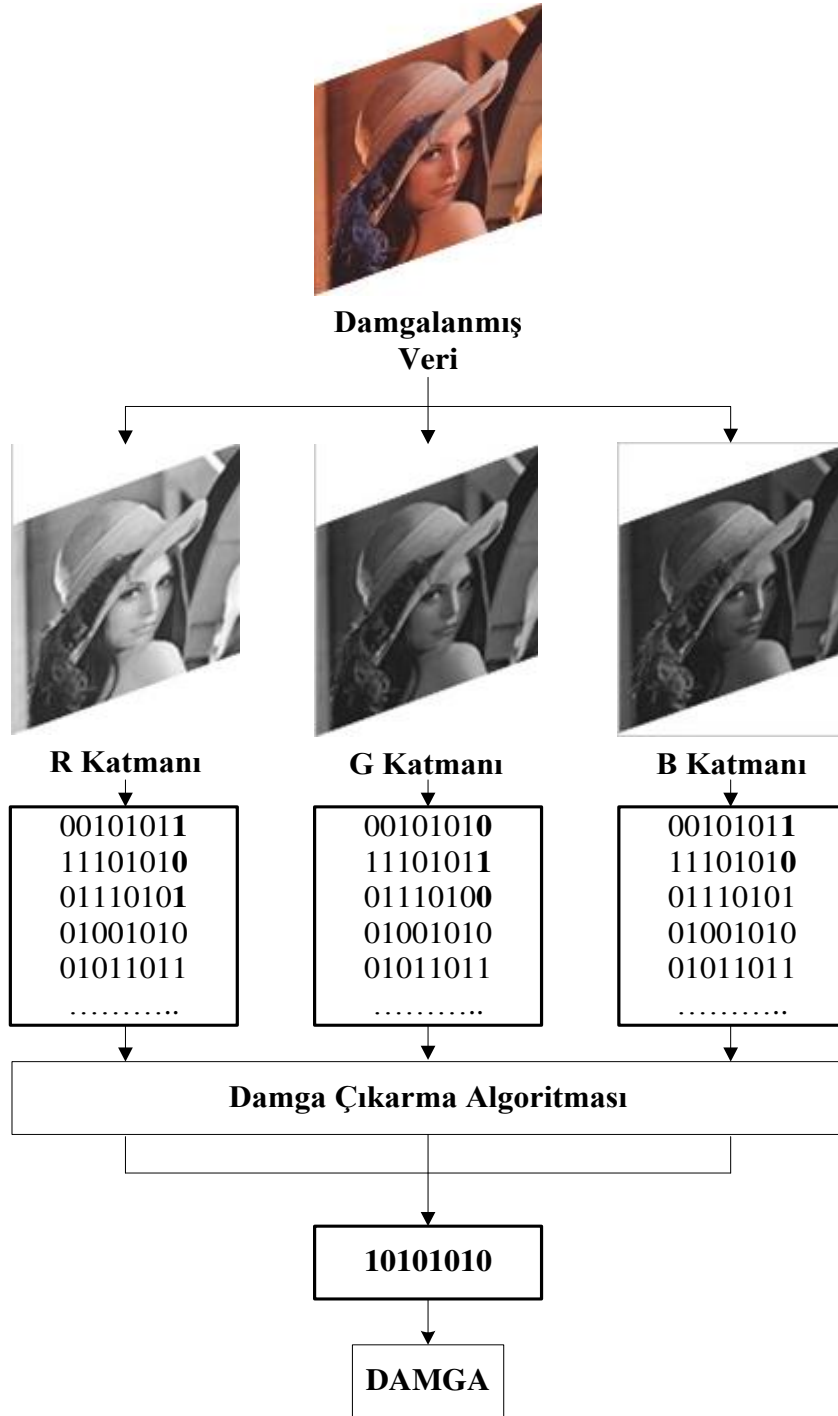
- Asıl nesne sayısallaştırılır.
- Damga sayısallaştırılır.
- Kullanım amacı ve yerine göre damgalama yöntemi belirlenir.
- Damganın alıcı tarafta çıkarılması için bir anahtar (gizli/açık) belirlenir.
- Seçilen yönteme ve anahtara göre damga asıl nesneye eklenir.

Damga çıkarma işleminde

- Damgalanmış nesne sayısallaştırılır.
- Damgalanmış sayısal nesnedeki anahtar (gizli/açık) keşfedilir.
- Belirlenen anahtara göre damgalanmış nesneden damga çıkarılır.
- Damga ve asıl nesne kendi formatlarına dönüştürülür.



Şekil 4.11. EÖB yöntemi tabanlı damga ekleme işleminin blok diyagramı



Şekil 4.12. EÖB yöntemi tabanlı damga çıkarma işleminin blok diyagramı

4.5. Veri Gizleme Yöntemlerinin Kıyaslanması

Veri gizleme uygulamalarında steganografi, damgalama ve kriptografi gibi farklı yöntemler kullanılır. Bu yöntemlerin seçimi uygulama ve kullanım alanına göre farklılıkları aşağıda sıralanmıştır [93, 103-107].

Damgalama uygulamalarında

- Amaç mesajın sahibini belirlemektir.
- Damga bulunduğu taşıyıcı ile ilişki içerisindedir.
- İnsan algısı baz alınarak tasarlanır.
- Asıl görüntüde bozulmaya izin verilmez.
- Gizlenecek mesaj önce şifrenip sonra ortam içerisine gizlenebilir.
- Damga oluşturmada kılıf asıl nesnedir.
- Saldırlara karşı dayanıklı olması beklenir.
- Gizlenmiş nesne görsel olarak kılıf nesnesi ile aynı olmalıdır.
- Asıl nesneye gizlenecek veri miktarı ne kadar az olursa saldırılara karşı o kadar güçlü ve güvenli olur.
- Hiç kimsenin damgalanmış nesnedeki damgayı kaldırmaması ve kendi damgasını eklememesi hedeflenir.

Steganografi uygulamalarında

- Amaç mesajın varlığını saklamaktır.
- Gizlenen mesaj taşıyıcı ile ilişki içerisinde olmak zorunda değildir.
- İnsan algısı baz alınarak tasarlanır.
- İnsan algısının fark edemeyeceği ölçüde asıl görüntüde bozulmaya izin verilebilir.
- Gizlenecek mesaj önce şifrenip sonra ortam içerisine gizlenebilir.
- Steganografi uygulamalarında kılıf asıl nesne veya gizlenen mesaj olabilir.
- Saldırlara karşı dayanıklı olması beklenmez.
- Damgalanmış nesne görsel olarak kılıf nesnesi ile aynı olmalıdır.
- Steganografik yöntemlerin ticari uygulamaları sayısal damgalama içerisinde yer alır.

Kriptografi uygulamalarında

- Amaç mesajın içeriğinin saklanmasıdır.

- Bir veri gönderilmek üzere şifrelendiğinde orijinal halinden farklı bir duruma gelebilir.
- Gizli mesajın iletilmesi için kılıfa ihtiyaç duyulmaz.
- Saldırlara karşı dayanıklı olması beklenir.

5. SAYISAL DAMGALAMA UYGULAMALARINDA KULLANILAN YÖNTEMLER

Bilgisayarlı sistemlerin gelişmesi günümüzde hemen hemen tüm verilerin bilgisayar ortamında tutulmasına olanak sağlamıştır. Bu veriler saklanırken ya da iletimi sırasında güvenliği ve bütünlüğünün sağlanması, sahibinin belirlenmesi gibi işlemler için çeşitli yöntemler geliştirilmiştir. Bu bölümde alt başlıklarda geliştirilen yöntemler ve bu yöntemlerde ortak kullanılan terimler açıklanmıştır.

5.1. Sayısal Resim Bileşenleri ve Formatları

5.1.1. Resim (İmge)

Doğa veya hayal gücü ile beyin tarafından benzetimi yapılabilecek nesnelerin görüntüsel olarak nitelendirilmesine resim (imge) denir. Günümüzde görüntü, resim ve ses gibi çoklu ortam öğeleri bilgisayar destekli olarak işlendiklerinden dolayı sayısallaşmışlardır. Şekil 5.1.'de resmin tek katman için sayısallaştırma örneği verilmiştir.

	<pre>198 195 191 184 160 121 100 102 195 193 190 184 160 122 100 101 191 191 189 184 161 122 99 100 ... 188 188 188 184 161 122 98 99 ... 186 186 187 184 161 122 97 97 ... 185 186 187 184 161 121 97 97 ... 186 187 187 184 161 121 96 96 ... 187 187 188 184 160 121 96 96 ... 188 187 191 185 162 124 88 83 ... 189 188 192 185 161 123 87 82 ... 190 189 192 184 160 122 85 80 ... 192 190 192 184 159 120 84 78 ... 193 190 192 183 158 119 83 77</pre>
Örnek Resim	Sayısallaştırılmış İmge (Bir Katman Değerleri)

Şekil 5.1. Resmin sayısallaştırılması

İdeal bir resim

- Yüksek çözünürlük
- Küçük dosya boyutu
- Çalıştığı bilgisayar ve işletim sisteminden bağımsız olması gibi özelliklere sahip olmalıdır.

Resim, iki boyutlu ışık-yoğunluk ($r(\alpha,\beta)$) fonksiyonu olarak ifade edilebilir. $r(\alpha,\beta)$ fonksiyonunun değeri (α,β) noktasındaki pikselin ışıklılık değerini temsil eder [108]. Literatürde kullanılan resim tipleri aşağıda sıralanmıştır.

5.1.1.1. Gerçek Renk

Gerçek renk olarak adlandırılan ve bu tez kapsamında kullanılan resim tipi RGB formatındadır. RGB renk sisteminde görüntü derinliği 24 bittir. Her piksel Kırmızı (Red=R), Yeşil (Green=G) ve Mavi (Blue=B) oranlarını belirleyen üç farklı renk değerine sahiptir.

5.1.1.2. Gri Seviye

Bu resim tipleri gri formattaki resimlerdir. Bu tipteki resimlerde her piksel tek bir değere sahiptir. Piksellerin gri seviye değerleri ya $[0, 1]$ aralığında “double” sayılarla ya da “uint8-uint16” olarak ifade edilen $[0, 255]$ veya $[0, 65535]$ aralığında değişen değerlerle temsil edilirler.

5.1.1.3 İndeksli Renk

RGB resim tipinden farklı olarak indeksli renk resim tipinde, bir renk değeri üç farklı (RGB) değerle temsil edilmek yerine “double” tek bir değerle temsil edilir.

5.1.2. Piksel

Bilgisayar ekranında oluşan görüntüler noktalardan oluşur ve her bir nokta kare şeklindedir. Bu noktalar görüntünün normal boyutunda fark edilemez. Ancak Şekil 5.2.’de gösterildiği gibi imge büyütüldüğünde bu noktalar fark edilebilir.

	
Normal Boyuttaki Görüntü	32 Kat Büyütülmüş Görüntü

Şekil 5.2. Görüntünün piksellerinin açığa çıkarılması

Ekranda kontrol edilebilen ve belirli renk bilgilerini barındıran en küçük noktalara piksel denir. Her bir piksel kırmızı, yeşil ve mavi renklerin karışımından oluşur. Bir görüntünün içerdiği piksel miktarı ne kadar fazla olursa görüntü kalitesi o oranda artar. Ancak Şekil 5.3.'de gösterildiği gibi piksel sayısının artması dosyanın boyutunun da büyümesine neden olur [109].

			
512x512 piksel 768 KB	256x256 piksel 192 KB	64x64 piksel 12.0 KB	32x32 piksel 3.05 KB

Şekil 5.3. Resimlerde piksel boyut ilişkisi

5.1.3. Nokta ve Nokta Aralığı

Bir pikseli meydana getiren kırmızı, mavi veya yeşil renklerinden her birine nokta denir. Bir pikseldeki renklerin birbirine olan mesafesi ise nokta aralığı olarak adlandırılır.

5.1.4. Çözünürlük

Ekranda bir defada görüntülenebilen ve birbirinden ayırt edilebilen nokta sayısına çözünürlük denir.

5.1.5. LPI

Her inç başına düşen satır veya çizgi sayısına LPI (line per inch) denir.

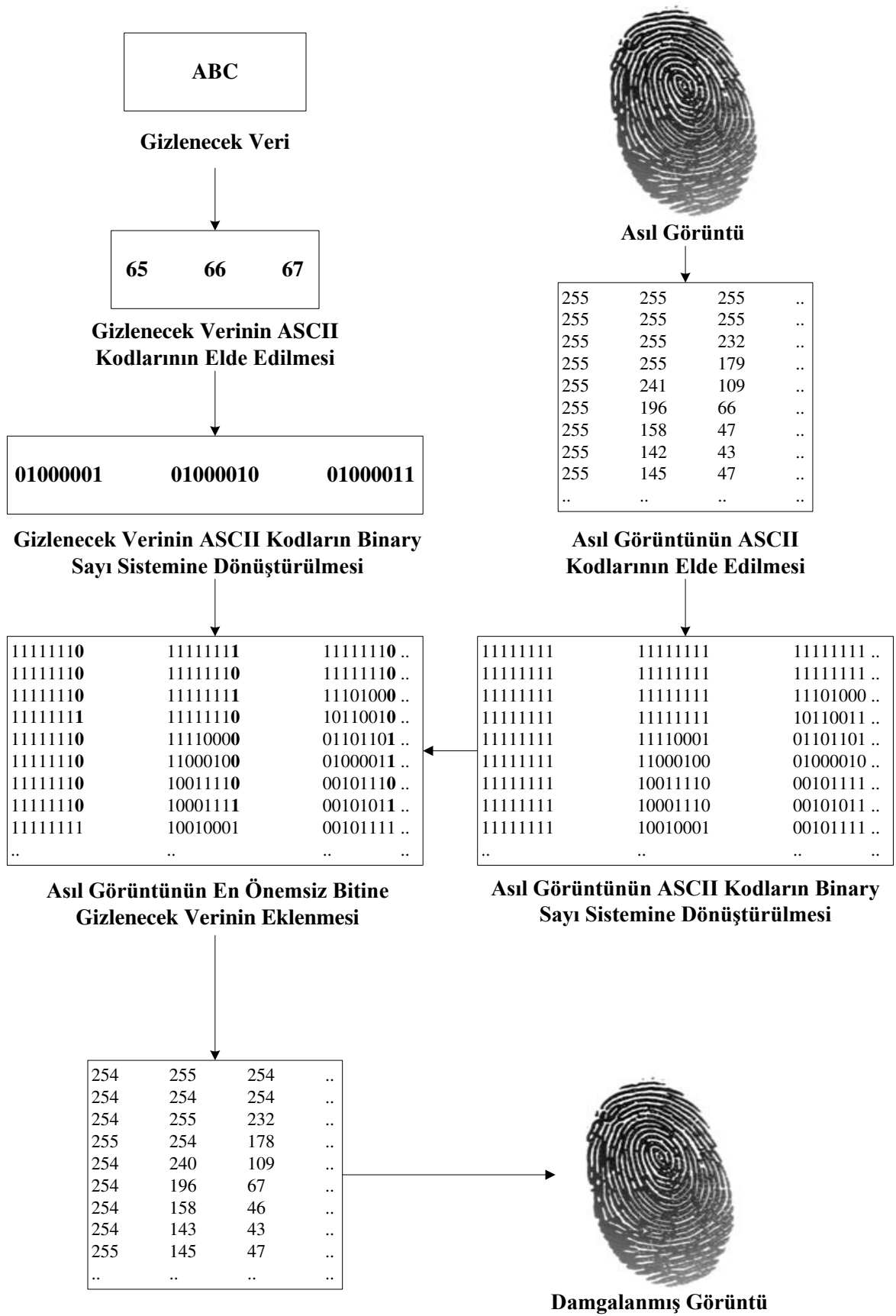
5.1.6. DPI

Her inç başına düşen nokta sayısına DPI (Dot per inch) denilmektedir [108].

5.2. Sayısal Damgalama Uygulamalarında Kullanılan Yöntemler

5.2.1. En Önemsiz Bit Yöntemi

Veri gizleme alanında kullanılan en basit ve yaygın yaklaşım En Önemsiz Bit (EÖB) yöntemidir. Bu yöntemde Şekil 5.4.'de gösterildiği gibi her nesnenin ikili sayı sistemindeki karşılığının değerine en az katkıda bulunan en sağdaki biti üzerinde değişiklik yapılarak asıl nesnenin en az değişikliğe uğraması sağlanır. Uygun bir algoritmayla nesnenin her baytındaki son bite, gizlenecek verideki her bitin eklenmesi ile veri gömülebilmektedir [110].



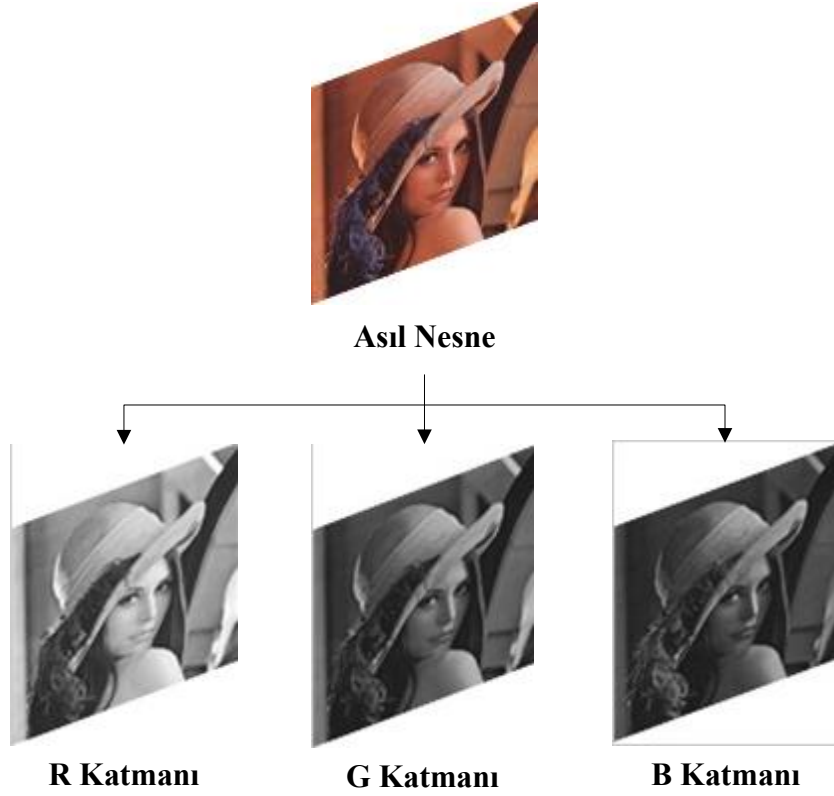
Şekil 5.4. EÖB Yöntemi ile Veri Gizleme

EÖB yöntemi uygulanması kolay bir yöntem olmasının yanında asıl nesnedeki bozulmanın İGS tarafından kolayca fark edilememesinden dolayı damgalama uygulamalarında yoğunlukla tercih edilmektedir [111]. Bu avantajlarının yanında EÖB yöntemi kesme, ölçeklendirme, döndürme, sıkıştırma gibi basit saldırılara karşı çok hassastır. Bu saldırılara karşı dayanıklılığın artırılması amacıyla asıl nesne ön işlemlere tabi tutulur. Böylelikle asıl nesnedeki bozulma azaltılıp güvenlik seviyesinin artırılması amaçlanır. Ancak yine de kesme, kırpma, yapıştırma gibi basit işlemler sonucunda gizli veride kayıplar olabilmektedir [112].

Gönderici ve alıcı arasındaki iletim kanalında bir nesnenin en önemsiz bitlerinin silinmesi ile gizlenmiş nesne kolaylıkla yok olabilmektedir. Aynı zamanda gizlenecek veri, asıl nesne içerisine amaca uygun bir algoritma ile sıralı değil de rastgele bir düzenle gömülürse damga saldırılarına karşı daha dayanıklı olmaktadır [113]. EÖB yönteminin dayanıklılığının artırılması amacıyla veri gizleme işlemi esnasında Fibonacci serileri de kullanılmıştır. Bu yöntemde seçilen pikseller ilk önce Fibonacci değerlerine dönüştürülmekte ve gizli veri bu dönüşüm sonucunda ilgili pikselde saklanmaktadır [114]. Geliştirilen yöntemde gizli verinin saklanması esnasında İGS'nin algılayamadığı hızlı değişen yerlerin kullanılması [115] yerine farklı bir algoritma kullanılarak yerel varyans değerleri için uygun olan bölgeler seçilmiştir.

Veri gizleme uygulamalarında kullanılan tek katmanlı bir nesne için veri saklama kapasitesi, genel olarak asıl görüntünün kapasitesinin yaklaşık %15'i kadardır. Eğer asıl görüntü, Şekil 5.5.'de gösterildiği gibi renkli bir resim dosyası ise bu oran üçe katlanabilir. Çünkü renkli resimlerde kullanılan yöntem ve algoritmaya göre her katman ayrı bir resim olarak değerlendirilirse 3 katmana da veri gömülebilir. Böylelikle asıl nesnenin veri gizleme kapasitesi artırılmış olur [116].

Bir nesne içerisinde verinin gizlenip gizlenmediğinin algılanması için eşit boyutlu bölümlere ayrılan her bir katman ve her bir bölümün karmaşıklığı hesaplanır. Her bölüm için elde edilen karmaşıklık seviyelerinin belirlenen bir eşik değerinde olup olmadığı kontrol edilir. Karmaşıklık istenilen düzeyde ise bu katmanın seçilen bölümüne bir verinin gizlenmiş olduğu tespit edilir [117].



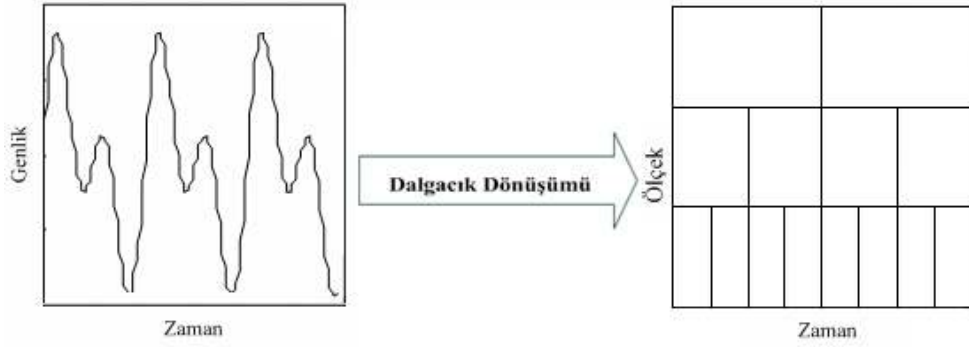
Şekil 5.5. Renkli bir resmin RGB katmanları

EÖB yönteminde amaca uygun farklı algoritmalar geliştirilerek damgalanmış görüntünün dayanıklılığı ve sağlamlığı artırılmak istense de bu yöntem basit saldırılara karşı çok hassastır. Geliştirilen algoritmaların bir bölümü iletim kanalında üçüncü şahısların gizlenmiş veriyi elde edememeleri üzerine, diğer bölümü ise kuantalama özelliklerini kullanarak veri gizlemede fazladan güvenlik sağlama üzerine odaklanmıştır [118].

5.2.2. Ayrık Dalgacık Dönüşümü

Dalgacık dönüşümü, verilen bir fonksiyonu farklı frekans bileşenlerine bölerek her bileşenin kendi yapısına uygun olarak işlenmesine olanak sağlar. Bu dönüşümün temeli Joseph Fourier tarafından geliştirilen Fourier Dönüşümüne dayanmaktadır. Fourier Dönüşümü, karmaşık işaretlerin yaklaşık olarak daha basit işaretlerin toplamı şeklinde ifade edilebileceğini öne sürmüş ve böylelikle frekans dönüşümünün de temelini atmıştır. Dalgacık dönüşümünde, verilen bir işaretin düşük ve yüksek frekanslarda farklı boyutlarda

pencereler kullanılarak Şekil 5.6.'da gösterildiği gibi zaman düzlemindeki karşılığı elde edilir. Böylelikle amaca uygun olarak, düşük frekans bilgilerinin geniş zaman aralığında, yüksek frekans bilgilerinin ise küçük zaman aralığında işlem yapılmasına olanak sağlar.



Şekil 5.6. Dalgacık dönüşümü ile bir işaretin frekans bileşenlerine ayrılması

Günümüzde Dalgacık dönüşümü, Fourier dönüşümü ile incelenen durağan işaretlerin yanı sıra durağan olmayan işaretlerin işlenmesinde de kullanılır.

Dalgacık dönüşümü;

- Ayrık Dalgacık Dönüşümü (ADD)
- Sürekli Dalgacık Dönüşümü (SDD)

olarak 2 sınıfta incelenebilir. Hem ADD hem de SDD sürekli zaman sinyallerini temsil etmek için kullanılırlar. SDD elde edilebilir ölçeklenmiş ve ötelenmiş değerler üzerinde çalışır. Bu dönüşümde ölçekleme ve dönüşüm parametreleri sürekli değiştiğinden dolayı dalgacık katsayılarının hesaplanması işlemi sürekli tekrarlanmalıdır. ADD ise belirli ölçeklenmiş ve ötelenmiş değerlerin altkütmesi ya da grid gösterimini elde etmek için kullanılır. SDD'nin belirtilen dezavantajından dolayı ADD uygulamalarda daha sık tercih edilmektedir [119].

ADD görüntü işleme uygulamalarında da büyük oranda kullanılır. Dalgacık dönüşümü bir resmi yatay, dikey ve diyagonal olarak üç boyuta ayrıştırır. Bundan dolayı, dalgacıklar İGS'nin yön bağımlı özelliklerini çok dikkatli bir şekilde yansıtır. ADD'nin çoklu çözünürlük özeliğinden dolayı, ölçeklenebilirlik ve alçaltmaya dayanıklılık gerektiren uygulamalarda sıklıkla tercih edilir ve bu özelliğinden dolayı resimlerin aşamalı iletimine izin verir. Yüksek çözünürlük alt-bantları, resmin içindeki kenar ve doku örüntülerinin kolay bir şekilde bulunmalarını sağlar.

Bir resme tek seviyeli ADD uygulandığında resim Şekil 5.7.'de gösterildiği gibi DD, DY, YD ve YY olmak üzere 4 alt banda ayrılmaktadır. Her ayrıştırma seviyesindeki düşük

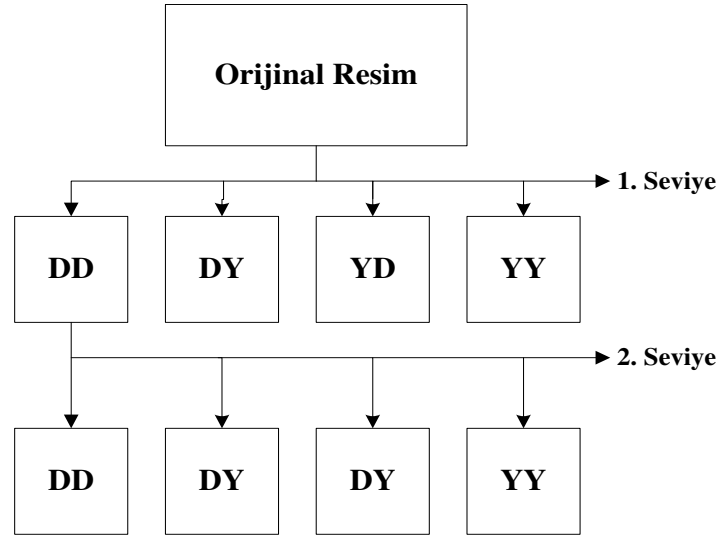
(DD) alt-bantların ADD genlik katsayıları daha büyük olur. ADD'nin genlik katsayıları diğer (DY, YD, YY) alt-bantlarda daha küçük olur. ADD ile elde edilen 4 alt bant

DD= Yaklaşık resim

DY= Dikey detay

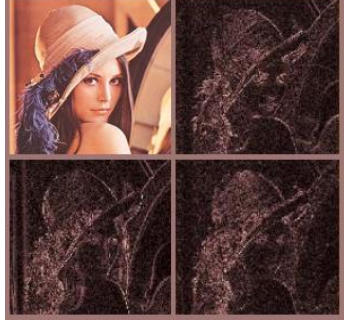
YD= Yatay detay

YY= Köşegen resim olarak temsil edilmektedir. Damgalama uygulamalarında damga genellikle YD ve DY alt bantlarına eklenir. Sağlamlığı artırmak maksadı ile DD bandına da damga ekleme yapılabilir. Damga, sıkıştırma sonrası zarar göreceği için genellikle YY alt bandına eklenmez. Fakat YY alt bandı kırpma, keskinleştirme, kontrast değiştirme, histogram denkleştirme, gamma düzeltme gibi saldırılara karşı sağlamdır [120].



Şekil 5.7. ADD ile resmin alt bantlarına ayrılması

Amaca ve kullanım yerine uygun olarak bir resme ayrık dalgacık dönüşümü birden fazla uygulanabilir. Orijinal bir resmin tek seviyeli ADD Şekil 5.8.'de, iki seviyeli ADD ise Şekil 5.9.'da verilmiştir [119].

	
Orijinal Resim	ADD ile Orijinal Resmin Altbantları

Şekil 5.8. Tek seviyeli ADD ile resmin alt bantlarına ayrılması

	
Orijinal Resim	İki Seviyeli ADD ile Orijinal Resmin Altbantları

Şekil 5.9. İki seviyeli ADD ile resmin alt bantlarına ayrılması

Denklem 5.1 ve 5.3’de Dalgacık dönüşümünün karşılığı verilmiştir. Burada $\alpha > 0$ ve $\beta \in \mathbb{R}$ olmak üzere α parametresi frekansı, β parametresi zamanı, δ dalgacık fonksiyonunu ve $DD(\alpha, \beta)$ dalgacık dönüşümünü temsil etmektedir.

$$DD(\alpha, \beta) = \frac{1}{\sqrt{\alpha}} \int_{-\infty}^{+\infty} f(t) \delta\left(\frac{t-\beta}{\alpha}\right) dt \quad 5.1$$

ve

$$\delta_{\alpha, \beta}(t) = \frac{1}{\sqrt{\alpha}} \delta\left(\frac{t-\beta}{\alpha}\right) \quad 5.2$$

olmak üzere

$$DD(\alpha, \beta) = \int_{-\infty}^{+\infty} f(t) \overline{\delta_{\alpha, \beta}(t)} dt \quad 5.3$$

Denklem 5.4.'de verilen uygunluk şartını sağlamak üzere Denklem 5.5.'de Ters Dalgacık Dönüşümü verilmiştir. Bu denklemde c_δ bir dalgacık sabitidir ve kullanılan dalgacık türüne bağlıdır.

$$c_\delta = \int_{-\infty}^{\infty} \frac{|\delta(a)|^2}{|a|} dw < \infty \quad 5.4$$

$$TDD(t) = \frac{1}{c_\delta} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{1}{\alpha^2} DD(\alpha, \beta) \delta_{\alpha, \beta}(t) d\alpha d\beta \quad 5.5$$

ADD aşağıda belirtilen bazı özellikleri nedeniyle damgalama uygulamalarında yaygın olarak kullanılmaktadır.

- a. ADD, çok çözünürlüklü doğasından dolayı ölçeklendirme ve kabul edilebilir bozulmaya ihtiyaç gösteren, dayanıklılık gerektiren uygulamalar için uygundur.
- b. Büyük genlikli ADD katsayıları damga gömmek için uygundur.
- c. Düşük çözünürlükte damga algılama işlemlerinde hesapsal olarak etkilidir. Çünkü her ardışık çözünürlük seviyesinde sadece birkaç frekans bandı ile ilgilenilmektedir.
- d. Çok çözünürlüklü damgalama, zaman veya frekans boyutunda iki veya ikinin katları şeklinde yapılan aşağı örnekleme karşı dayanıklıdır.
- e. İGS, görüntüdeki köşeler ve dokulu alanlardaki bozulmalara yumuşak alanlardaki bozulmalardan daha duyarsızdır. Yüksek çözünürlüklü alt bantlarda asıl görüntüye ait köşe ve doku desenlerini kolaylıkla ortaya çıkardığından damga, İGS tarafından daha zor algılanabilmektedir.
- f. Dalgacık dönüşümü hesapsal olarak etkilidir, basit süzgeç dönüşümleri kullanılarak uyarlanabilir.
- g. İletim ve kod çözme hatalarına karşı daha dayanıklıdır.
- h. ADD katsayılarının genliği her seviyede temel bileşende daha büyüktür. Diğer yatay, düşey ve köşegensel bileşenlerde temel bileşene göre daha küçüktür.

Sayısal damgalama uygulamalarında ADD kullanırken yöntemin sahip olduğu belirli avantajlarının yanında aşağıda belirtilen bir takım dezavantajları da mevcuttur.

Avantajları:

- a. ADD, resmin farklı çözünürlüklerinde işlem yapabilir. Bu özelliği ile AKD'den avantajlıdır.

- b. ADD'nin gerçekleştirilmesi için geliştirilen hızlı algoritmalar vardır.
- c. ADD, iyi enerji sıkıştırma özelliğine sahiptir. Bu nedenle ADD çok sayıda görüntü işleme probleminin çözümünde kullanılmıştır.
- d. Bloklara ayırmaya gerek kalmadan yüksek sıkıştırma oranı sağlanmakta, dolayısıyla blok kenarlarının doğurduğu sıkıntılardan sakınılmaktadır.
- e. Dalgacık fonksiyonu kullanıcıya bağlı olarak serbestçe seçilebileceğinden yüksek esneklik özelliğine sahiptir.

Dezavantajları:

- a. Yönsel seçicilik özelliği, amaca uygun olarak aynı yönde sıralanmış özelliklere karşı güçlü cevap vermesi, diğer özellik yönlerine karşı cevabının zayıf olabileceği anlamına gelir. ADD'nin yönsel seçicilik özelliği iyi değildir.
- b. ADD ötelemeden bağımsız değildir [93].

5.2.3. Ayırık Kosinüs Dönüşümü

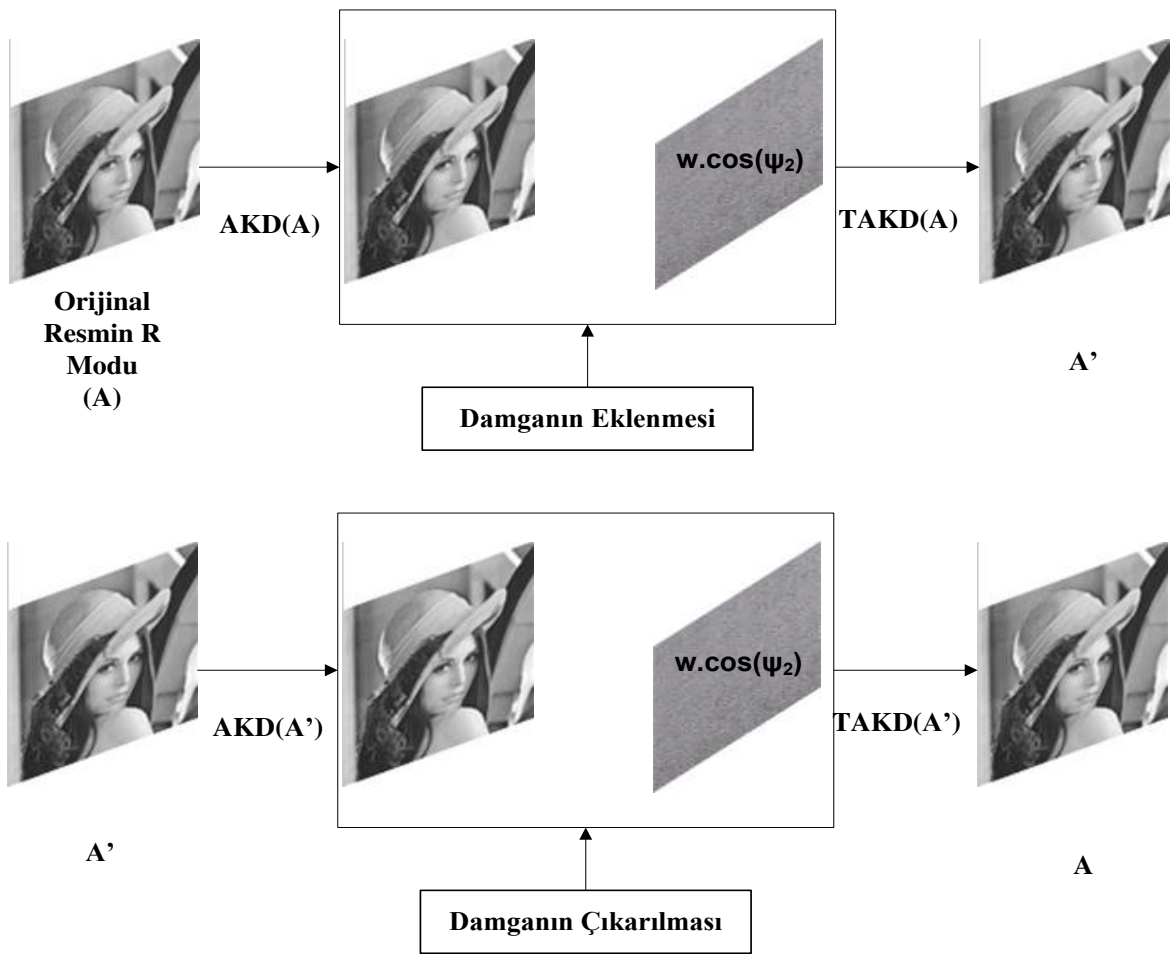
AKD, bilgi sıkıştırma kapasitesi ve giriş verilerinden bağımsız olması özelliklerinden dolayı yaygın olarak kullanılmaktadır. 8x8 boyutundaki görüntü parçası bire bir dönüşüm kullanılarak frekans boyutuna taşınır. Bu dönüşüm sonucunda enerjinin büyük bir bölümü az miktarda dönüşüm katsayısında toplanır. Dönüşüm katsayıları genelde sıkıştırma veya daha özel olarak damgalama ve farklı birçok amaçla saklanır, kuantalama işlemine tabi tutulduktan sonra kodlanır. Basitlik ve hesaplama karmaşıklığını azaltmak için ayırık dönüşümler kullanılır [121].

Ayrık Fourier Dönüşümü (AFD), karmaşık işareti karmaşık uzayda dönüştürür. Ancak işaret gerçel sayılardan oluşuyorsa yani sanal kısmı sıfır ise spektrumda gerçel ve sanal kısımlar birbirinin aynısı olur. Bu da elde edilen dönüşümün yarısının kendisini tekrar edeceği anlamına gelir. AKD, gerçel işareti gerçel spektruma dönüştürerek AFD'nin tekrar problemini çözer.

AKD sinyalleri değişken frekanslardaki sinüslerin toplamına dönüştürür. Resimler için ise 2 boyutlu AKD (2B AKD) kullanılır ve resmin bir matris eşitliği elde edilir. NxM boyutundaki bir resme 2B AKD uygulanarak NxM boyutunda AKD katsayıları elde edilir. Elde edilen bu matrisin sol üst köşesinde bulunan katsayılar enerjinin çok büyük bir kısmını tutarlar. Dolayısıyla bilginin büyük bir kısmı da bu alandadır. Uygun tarama

yöntemleri ile matris tek boyutlu dizilere taşınır ve geliştirilen algoritmalarla bu bilgiler daha ayrıntılı, sağlam ve güvenli olarak işlenebilir [122].

AKD resmin tamamına uygulanırsa bu tür dönüşüme Global AKD denir. Bu durumda resmin tüm noktaları arasındaki ilişki kodlanmaya çalışılır. Resmin belirli bölgesi ile ilgili ayrıntı elde edilmek istenirse Global AKD istenilen sonucu veremeyebilir. Bu eksikliği gidermek için yerel AKD ile resmin belirli bir bölgesinin katsayılarının elde edilmesi amaçlanmıştır. Yerel AKD’de de resim küçük bölgelere ayrılır ve her bir bölgeye ayrı ayrı AKD uygulanır. AKD’nin işlem basamakları Şekil 5.10.’da verilmiştir [123].



Şekil 5.10. AKD işlem basamakları

Gerçek bir dizinin AKD’sini bulmak için öncelikle bir işaret oluşturulur.

$$\begin{aligned}
 x'[m] &\triangleq \{x[m]\} & (0 \leq m \leq N-1) \\
 x'[m] &\triangleq \{x[-m-1]\} & (-N \leq m \leq -1)
 \end{aligned}
 \tag{5.6}$$

İşaret ($-N \leq m \leq N-1$) aralığı dışında tekrar edecek şekilde oluşturulur. Böylelikle oluşturulan dizi $x'[m]$, $2N$ periyoduyla periyodik ve $m = -\frac{1}{2}$ için simetriktir. Dolayısıyla Denklem 5.7'deki eşitliği sağlamalıdır.

$$x'[m] = x'[-m - 1] = x'[2N - m - 1] \quad 5.7$$

Eğer $x'(m)$ işareti, sağa ya da sola doğru $\frac{1}{2}$ kadar kaydırılırsa $x'[m] = x'[m - \frac{1}{2}]$ ifadesi $m=0$ için simetrik olur. $x'[m]$, $x[m]$ olarak ifade edilecek olursa, $2N$ noktalı simetrik ifadenin AFD şu şekilde bulunur:

$n=0, \dots, 2N-1$ olmak üzere

$$X[n] = \frac{1}{\sqrt{2N}} \sum_{m'=-N+\frac{1}{2}}^{N-\frac{1}{2}} e^{-\frac{j2\pi m'n}{2N}} x\left[m' - \frac{1}{2}\right] \quad 5.8$$

m yerine $m + \frac{1}{2}$ konulursa $n=0, \dots, N-1$ olmak üzere Denklem 5.9 elde edilir.

$$X[n] = \frac{1}{\sqrt{2N}} \sum_{m'=-N+\frac{1}{2}}^{N-\frac{1}{2}} x\left[m' - \frac{1}{2}\right] \cos\left(\frac{2\pi m'n}{2N}\right) \quad 5.9$$

Denklem 5.9 düzenlenirse Denklem 5.10 elde edilir.

$$X[n] = \sqrt{\frac{2}{N}} \sum_{m=0}^{N-1} x[m] \cos\left(\frac{(2m+1)n\pi}{2N}\right) \quad 5.10$$

Denklem 5.10'un kosinüsler cinsinden yazılabilmesinin sebebi $x[m]$ 'in gerçel ve simetrik olmasıdır. Aynı nedenle dönüşümden elde edilen değerlerin sadece ilk kısmı saklanır, ikinci kısmı simetrik olduğu için atılır. Elde edilen dönüşüm $n=0, \dots, N-1$ olmak üzere Denklem 5.11'deki gibidir.

$$X[n] = \sqrt{\frac{2}{N}} \sum_{m=0}^{N-1} x[m] \cos\left(\frac{(2m+1)n\pi}{2N}\right) = \sum_{m=0}^{N-1} c[n, m] x[m] \quad 5.11$$

Burada nxm'lik dönüşüm matrisi:

$$c[n, m] \triangleq \sqrt{\frac{2}{N}} \cos\left(\frac{(2m+1)n\pi}{2N}\right) \quad 5.12$$

olarak tanımlanabilir. Bu AKD matrisinin sütun vektörlerinin hepsi ortagonal ve ilki hariç normaldir:

$$X[n] = \sqrt{\sum_{m'=0}^{N-1} c^2[n, m']} \quad 5.13$$

Denklem 5.12, Denklem 5.13'de yerine yazılırsa

$$X[n] = \sqrt{\sum_{m'=0}^{N-1} \frac{2}{N} \cos^2\left(\frac{(2m'+1)n\pi}{2N}\right)} = \begin{cases} \sqrt{2} & n = 0 \\ 1 & n = 1, 2, \dots, N-1 \end{cases} \quad 5.14$$

elde edilir.

O halde AKD'yi birim dikgen hale getirecek katsayı Denklem 5.15'de belirtildiği şekilde tanımlanabilir.

$$a[n] = \begin{cases} \sqrt{\frac{1}{N}} & n = 0 \\ \sqrt{\frac{2}{N}} & n = 1, 2, \dots, N-1 \end{cases} \quad 5.15$$

Sonuç olarak n=0, ..., N-1 olmak üzere AKD Denklem 5.16'de verildiği gibi elde edilir.

$$X[n] = a[n] \sum_{m=0}^{N-1} x[m] \cos\left(\frac{(2m+1)n\pi}{2N}\right) = \sum_{m=0}^{N-1} x[m] c[n, m] \quad 5.16$$

TAKD ise n=0, ..., N-1 olmak üzere Denklem 5.17 belirtildiği gibi elde edilir [124].

$$x[m] = \sum_{n=0}^{N-1} a[n] X[n] \cos\left(\frac{(2m+1)n\pi}{2N}\right) \quad 5.17$$

AKD ařağıda belirtilen bazı zellikleri nedeniyle damgalama uygulamalarında yaygın olarak kullanılmaktadır.

- a. 8x8 blokluk AKD katsayılarından DC katsayısının genliğı ilgili bloğun ortalama gri seviyesi ile orantılıdır.
- b. Bir kaç katsayı ile mkemmel iřaret yaklařımı sağılanabilir. DC ve bir kaç AC katsayı ile grnt yeniden anlařılabilir řekilde oluřturulabilir.
- c. Katsayılar zig-zag olarak sıralandıklarında dřk frekanstan yksek frekansa ve yksek genlikten dřk genliğıe sıralanmıř olurlar.
- d. Eğıer bir bloktaki yksek frekanslı katsayıların oğı sıfırsa o blok yumuřak bir grnt bloğuna aittir, kře iermez.
- e. Eğıer bir bloktaki dřk frekanslı AC katsayıları yksek genlik değıerine sahipse, bunlar o blokta yer alan křeleri temsil ederler.
- f. AKD hızlı bir dnřmdr.

Sayısal damgalama uygulamalarında AKD kullanırken yntemin sahip olduğı belirli avantajlarının yanında ařağıda belirtilen bir takım dezavantajları da mevcuttur.

Avantajları:

- a. Karmařık bileřenler iermez. Diğıer bir avantajı ise grntleri kk değıerlere evirir.
- b. Bundan dolayı kk katsayıların yuvarlanması ve bunlardan tekrar grntnn elde edilmesindeki hatalar ok nemsenmez. İstenen grnt kalitesine gre katsayılar seilir.
- c. Periyodiktir ve periyodik olma zelliğıinden dolayı sreksizliğı kısmen ortadan kaldırır ve sıkıřtırma sonrası oluřabilecek blok etkisini byk lde azaltır.
- d. Yksek değıerliğıe sahip bilgiyi, daha dřk değıerli bilgiye dnřtrerek pikseller arası fazlalığın giderilmesine imkn verir. Bu zelliğıe enerji sıkıřtırma denilmektedir.
- e. AKD'nin diğıer bir stnlğı de dnřm sonucunda ok sayıda kk değıerli katsayılar oluřturmasıdır. Kk değıerli katsayılar sıfıra yuvarlanıp, değıřtirilmiř katsayılardan grntnn geri elde edilmesi sonucunda oluřan hatalar byk olmaz. Gerekli grnt kalitesi, hangi katsayıların sıfıra yuvarlanacağıını belirler.
- f. AKD ve ADD'ye dayalı sıkıřtırma yntemleri ok yaygın kullanılmaktadır. Bu yntemler řu anda durağıan grntlerin sıkıřtırılmasında en ok istifade edilen

sıkıştırma standartları olan JPEG (AKD'ye dayalı) ve JPEG2000 (dalgacık dönüşümüne dayalı) standartlarında kullanılmaktalar. Fakat son zamanlarda özellikle düşük bit hızlarında ADD' ye dayalı olan algoritmalarından daha çok istifade edilmektedir. Bunun başlıca sebepleri AKD'den doğan sıkıntılar ve ADD'nin sağlamış olduğu avantajlardır.

Dezavantajları:

- a. AKD'de sadece tek bir bloğun içindeki pikseller arası korelasyon ele alınmakta ve diğer komşu bloklardaki piksellerin korelasyonu ihmal edilmektedir.
- b. AKD kullanılarak blokların sınırlara tamamen uygulanması bir zorluk teşkil etmektedir.
- c. Blok kenarlarının doğurduğu sıkıntılar özellikle yüksek sıkıştırma oranlarında veya düşük bit hızlarında yeniden düzenlenmiş görüntüyü etkilemektedir.
- d. Kaynak veriye göre ayarlanamayan değişmez bir fonksiyona sahiptir.
- e. İkili (binary) görüntüler (faks veya parmak izi şekilleri) için verimli bir uygulamaya sahip değildir [93].

5.2.4. Ayırık Fourier Dönüşümü

Fourier Dönüşümü temel mantığını Fourier analizinden almaktadır. Fourier analizine göre bir periyodik sinyal farklı genlik ve frekanstaki birden fazla sinüzoidal sinyalin toplamı şeklinde ifade edilebilir. En düşük frekanslı sinüzoidal sinyal temel dalga (birinci harmonik) diğerleri ise harmonik bileşenler olarak kabul edilir [125].

Periyodik ve periyodik olmayan sinyallerin harmonik analizlerinin yapılabilmesi amacıyla AFD kullanılmaktadır. AFD'nin işlem süresinin uzun olması nedeniyle Hızlı Fourier Dönüşümü (HFD) geliştirilmiştir. HFD'de hızlı bir algoritma ile hedeflenen verinin harmonik analizinin yapılması sağlanmıştır. HFD, ayırık fourier hesabı için faz faktörünün simetri ve periyodiklik özelliğinden yararlanarak AFD'ye göre daha hızlı bir hesaplama sağlar [126].

AFD'nin $k=0,1,..., N-1$ olmak üzere N adet ayırık frekans değeri için hesabı Denklem 5.18'de verilmiştir.

$$X_k = \sum_{n=0}^{N-1} x[n]e^{-j2\pi kn/N} \quad 5.18$$

Ters ayrık fourier dönüşümü ise $n=0,1,\dots,N-1$ olmak üzere Denklem 5.19 ile temsil edilir [127].

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{j2\pi kn/N} \quad 5.19$$

AFD aşağıda belirtilen bazı özellikleri nedeniyle damgalama uygulamalarında yaygın olarak kullanılmaktadır.

- AFD, insan görme duyarlılığına göre damga spektrumunu her frekans bandına şekillendirmeyi mümkün kılar. AFD kullanılarak yapılan damgalama özellikle ötelemeye karşı dayanıklılığı sağlar.
- Ruanaidh, Dowling ve Boland, (1996) tarafından önerilen damgalama yönteminde damga, görüntünün algısal olarak önemli AFD faz bileşenlerine gömülür. AFD’de faz bileşenleri genlik bileşenlerinden görüntünün aşılabilirliği açısından daha önemlidir. Faz bileşenlerinin kullanılmasının bir başka nedeni haberleşme teorisinden iyi bilindiği gibi faz modülasyonunun genlik modülasyonu ile karşılaştırıldığında gürültü performansı açısından daha iyi sonuç vermesidir.
- Dönüşüm ve ötelemeyele değişmezlik özelliklerinden dolayı AFD genlik bileşenleri kullanılmıştır.
- Damga, AFD dönüşümü alınan görüntünün algısal olarak önemli faz bileşenlerine gömülür.
- Büyük genlikli dönüşüm katsayıları tercih edilir.
- AFD dönüşüm ve ötelemeyele değişmezlik özelliklerinden dolayı genlik bileşenleri damgalanır [93].

5.2.5. Tekil Değer Ayrışımı

Tekil Değer Ayrışımı (TDA) bir lineer cebir metodudur. Verilen bir matristeki problemleri belirleyip nümerik cevaplar bulmaya yarar [128]. Bir A matrisi $A = USV^T$ olmak üzere üç ayrı matrisin çarpımına ayrıştırılabilir. Burada U, $M \times N$ ve V^T , $N \times N$ boyutunda ortagonal matrislerdir. S ise $N \times N$ boyutlarında bir köşegen matristir. S matrisinin sıfıra karşılık gelmeyen köşegen elemanları A matrisinin tekil değerleri olarak adlandırılır ve aşağıdaki gibi ifade edilebilir [129]:

$$S = \begin{bmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{bmatrix}$$

A matrisinin rankı r ise $S = \text{diag}(\beta_1, \beta_2, \dots, \beta_n)$ değeri $\beta_1 \geq \beta_2 \geq \dots \beta_r \geq \beta_{r+1} = \beta_n = 0$ özelliğini sağlar.

TDA yönteminde resim damgalama işlemi yapılırken damga resmin köşegen matrisine eklenir [130].

$$A = \sum_{i=0}^r \beta_i u_i v_i^T \quad 5.20$$

TDA aşağıda belirtilen bazı özellikleri nedeniyle damgalama uygulamalarında yaygın olarak kullanılmaktadır [129].

- a. TDA; AFD, AKD ve ADD gibi saldırılara karşı daha dayanıklı olan dönüşüm bandında yapılan damgalama yöntemlerinden biridir.
- b. TDA tabanlı damgalama uygulamalarında, damga resmin TDA işleminden sonra elde edilen tekil değerlerine gömülmektedir. Tekil değerler üzerinde yapılan küçük değişiklikler resim kalitesini çok fazla etkilemez.
- c. Resme uygulanan görüntü işleme teknikleri tekil değerleri az oranda değiştirir. Bu nedenle TDA yöntemi saldırılara karşı daha fazla dayanıklıdır.

6. RENKLİ RESİMLER İÇİN GERÇEKLEŞTİRİLEN SAYISAL DAMGALAMA UYGULAMALARI

Bu tez çalışmasında renkli resimlere veri gizlemek için bir biyometrik sistemde kullanılabilecek sayısal damgalama uygulamaları yapılmıştır. Hazırlanan sistemde 896x592 boyutunda 20 farklı renkli resme (10 erkek+10 kadın) [131], 50x38 boyutunda renkli 20 iris resmi [132] gizlemek için ADD, AKD, TDA gibi yöntemler ile sayısal damgalama uygulamaları gerçekleştirilmiştir. Ayrıca geliştirilen yeni bir yöntemle diğer bahsedilen metotlar karşılaştırılmıştır. Aynı zamanda orijinal resmin bulanıklaştırma, keskinleştirme, ve döndürme gibi görsel saldırılara karşı değişimi kontrol edilmiştir. Kriter olarak İşaret-Gürültü Oranı (PSNR), Bit Hata Oranı (BER), Histogram Eğrileri ve Normalizasyon Katsayısı (NC) baz alınmıştır.

PSNR, orijinal nesne ile işlenmiş nesne arasındaki kalite ölçümü için kullanılmaktadır. İki nesne arasındaki PSNR ölçümü desibel olarak ifade edilir ve bu oran ne kadar yüksek olursa işlenmiş nesnenin kalitesinin de o oranda yüksek olduğu söylenebilir. NxN boyutundaki bir resim ile işlenmesi sonrası elde edilen resim arasındaki PSNR hesabı Denklem 6.1. ile ifade edilebilir.

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \quad 6.1$$

PSNR denklemindeki MSE ile temsil edilen değer orijinal nesne ile damgalanmış nesne arasında birbirine uymayan noktaların oranı olarak ifade edilmekte ve Denklem 6.2.'ye karşılık gelmektedir. PSNR değeri gibi MSE değerine bakılarak da damgalanmış nesnenin kalitesi üzerine yorum yapılabilmektedir. Denklem 6.1. göz önüne alındığında yüksek PSNR oranı düşük MSE değerine karşılık gelmektedir. Böylelikle bu sonuçlar elde edildiğinde bir damgalama sisteminde orijinal nesne ile damgalanmış nesne arasındaki kalite değişim oranının az olduğunu söylenebilmektedir.

$$MSE = \frac{1}{N \times N} \sum_{i=1}^N \sum_{j=1}^N [I_1(i,j) - I_2(i,j)]^2 \quad 6.2$$

Denklem 6.2'de, $I_1(i,j)$ orijinal resim ve $I_2(i,j)$ 'de damgalanmış resmi temsil etmektedirler. Renkli görüntülerin PSNR değerleri R, G, B katmanları dikkate alınarak

Denklem 6.3. veya 6.4'ten biri kullanılarak, MSE formülleri ise denklem 6.5.'deki gibi hesaplanır [133].

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{MSE(R)+MSE(G)+MSE(B)}{3}} \quad 6.3$$

$$PSNR = \frac{PSNR_R + PSNR_G + PSNR_B}{3} \quad 6.4$$

$$MSE_r = \frac{1}{N} \sum_{i=1}^N (r_1 - R_1)^2$$

$$MSE_g = \frac{1}{N} \sum_{i=1}^N (g_1 - G_1)^2 \quad 6.5$$

$$MSE_b = \frac{1}{N} \sum_{i=1}^N (b_1 - B_1)^2$$

Damgalanmış resim ile orijinal resim (damgalanmış resimden çıkarılan damga ile orijinal damga) arasındaki benzerliği ölçmek için normalizasyon katsayısı (NC) kullanılır. NC değerinin en yüksek değeri birdir ve NC değeri bire ne kadar yakın olursa damgalanmış resim orijinal resme o kadar benzerdir denilebilir [134].

$$NC = \frac{\sum_{i=1}^N \sum_{j=1}^N [X(i,j) * X'(i,j)]}{\sum_{i=1}^N \sum_{j=1}^N [X(i,j)]^2} \quad 6.6$$

Denklem 6.5'de, X (i,j) damgalama öncesi toplam bit sayısı, X'(i,j) damgalama sonrası resim elemanlarının değeri ve N ise hesaplanan piksel sayısıdır.

Bit hata oranı (BER), sayısal bilgi iletiminde gönderilen veri içindeki bozulan ya da yanlış algılanan bit oranını ifade eder. Damgalama uygulamalarında ise orijinal veri ile damgalanmış veri arasındaki değişen bit oranı BER değeri olarak ifade edilir [135].

$$BER = \frac{\text{Hatalı Bit Sayısı}}{\text{Toplam Bit Sayısı}} \quad 6.7$$

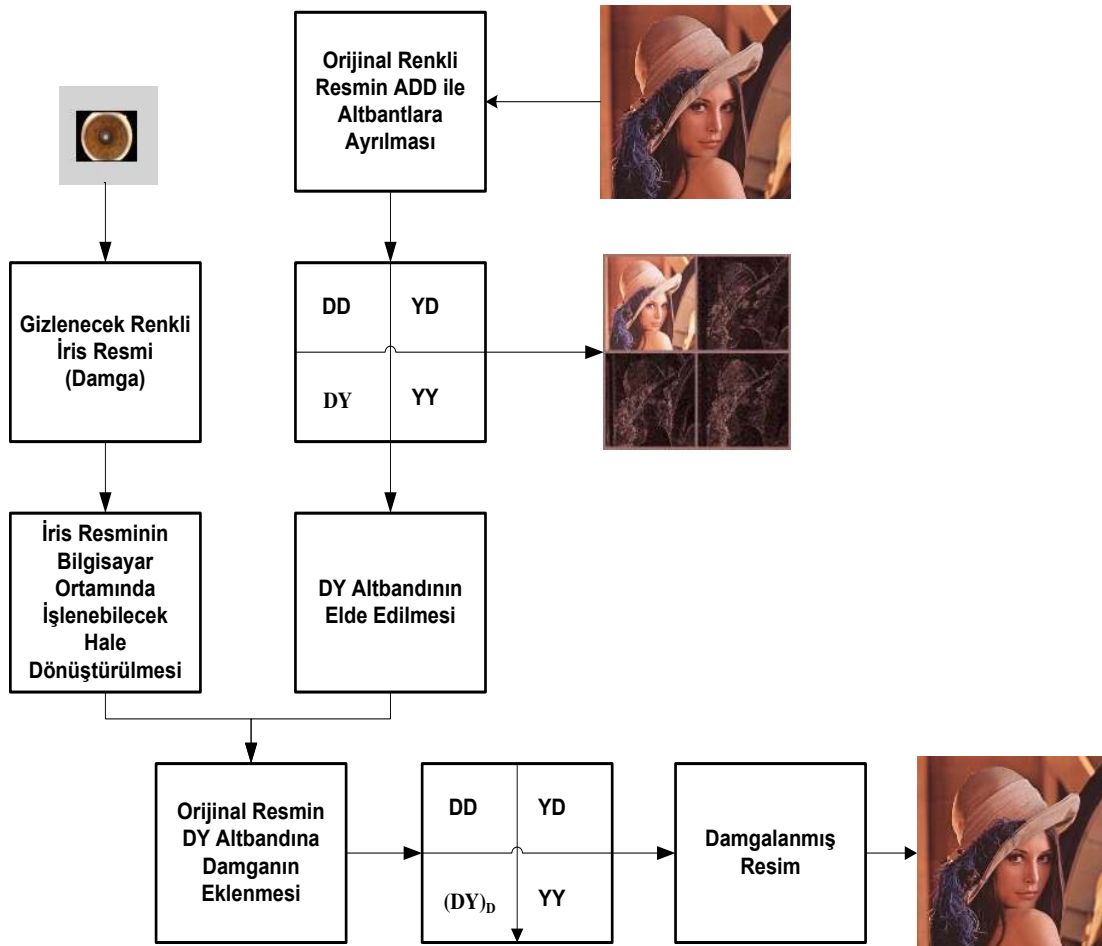
Veri gizleme uygulamalarında damgalanmış nesnenin orijinal nesneden farkını ortaya çıkarmak için kullanılan yöntemlerden bir diğeri de histogram eğrileridir. Histogram

eğrileri sayısal bir resimdeki renk dağılımını gösterir. Orijinal resim ve damgalanmış resmin histogram eğrileri arasındaki farkın İGS tarafından algılanamayacak yapıda olması beklenir [136].

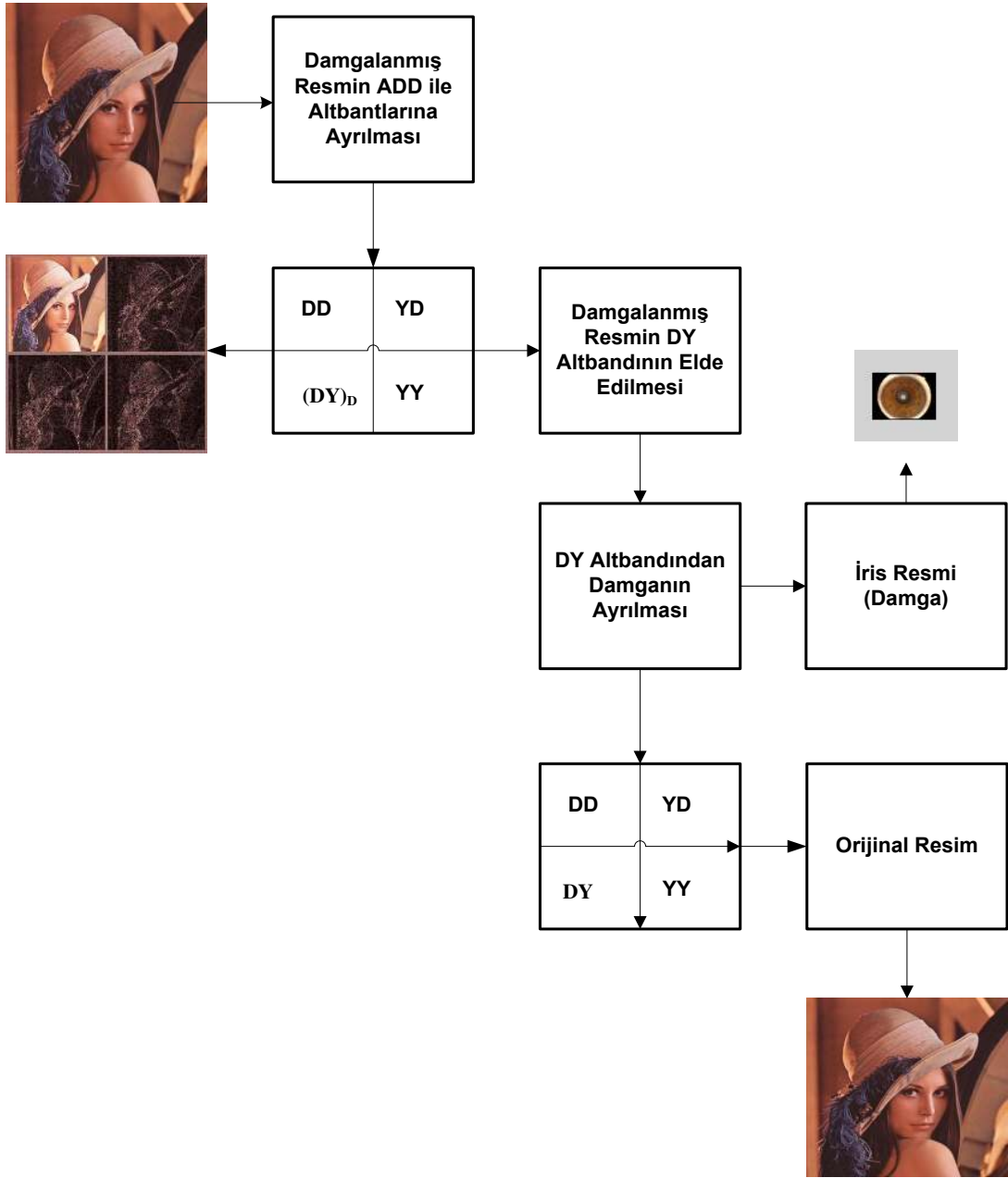
Tez çalışmasında kullanılan yöntemler ve elde edilen sonuçlar alt başlıklar halinde aşağıda verilmektedir.

6.1. ADD ile Sayısal Damgalama Uygulaması

Sistemde iris resminin orijinal resme eklenmesi işleminin blok şeması Şekil 6.1’de, damgalanan verilerin yeniden elde edilmesi işlemi için kullanılan yapının blok şeması ise Şekil 6.2’de verilmiştir.



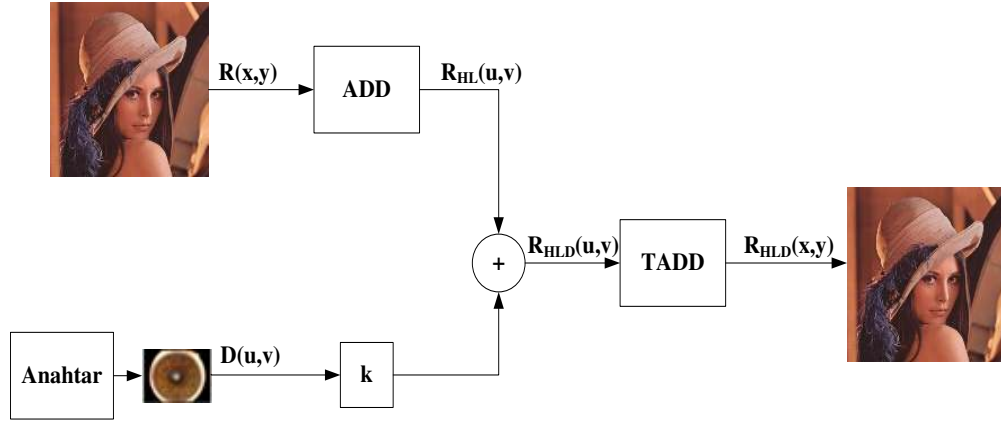
Şekil 6.1. ADD tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı



Şekil 6.2. ADD tabanlı damga çıkarma sisteminin iris ve yüz resimleri için blok diyagramı

Şekil 6. 3.'de görüldüğü gibi orijinal resme ADD ile damga eklenirken

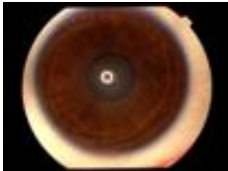
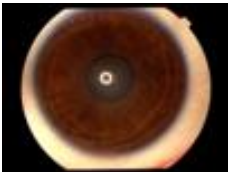
1. Orijinal resim ADD ile alt bantlarına ayrılır.
2. Damga eklenecek alt bant/bantlar seçilir.
3. Damga yapısı ve kullanım yerine uygun olarak algoritmada, damga olarak seçilen rastlantısal işaret k gibi bir katsayı ile orantılanarak alt banda eklenir. Ayrıca değişen ADD katsayılarının indisi ve damganın boyutu bir anahtarda tutulur.
4. TADD ile alt bantlar bir araya getirilerek Şekil 6.4.'de gösterilen damgalanmış resim elde edilir.



Şekil 6.3. ADD ile damgalama işlemi

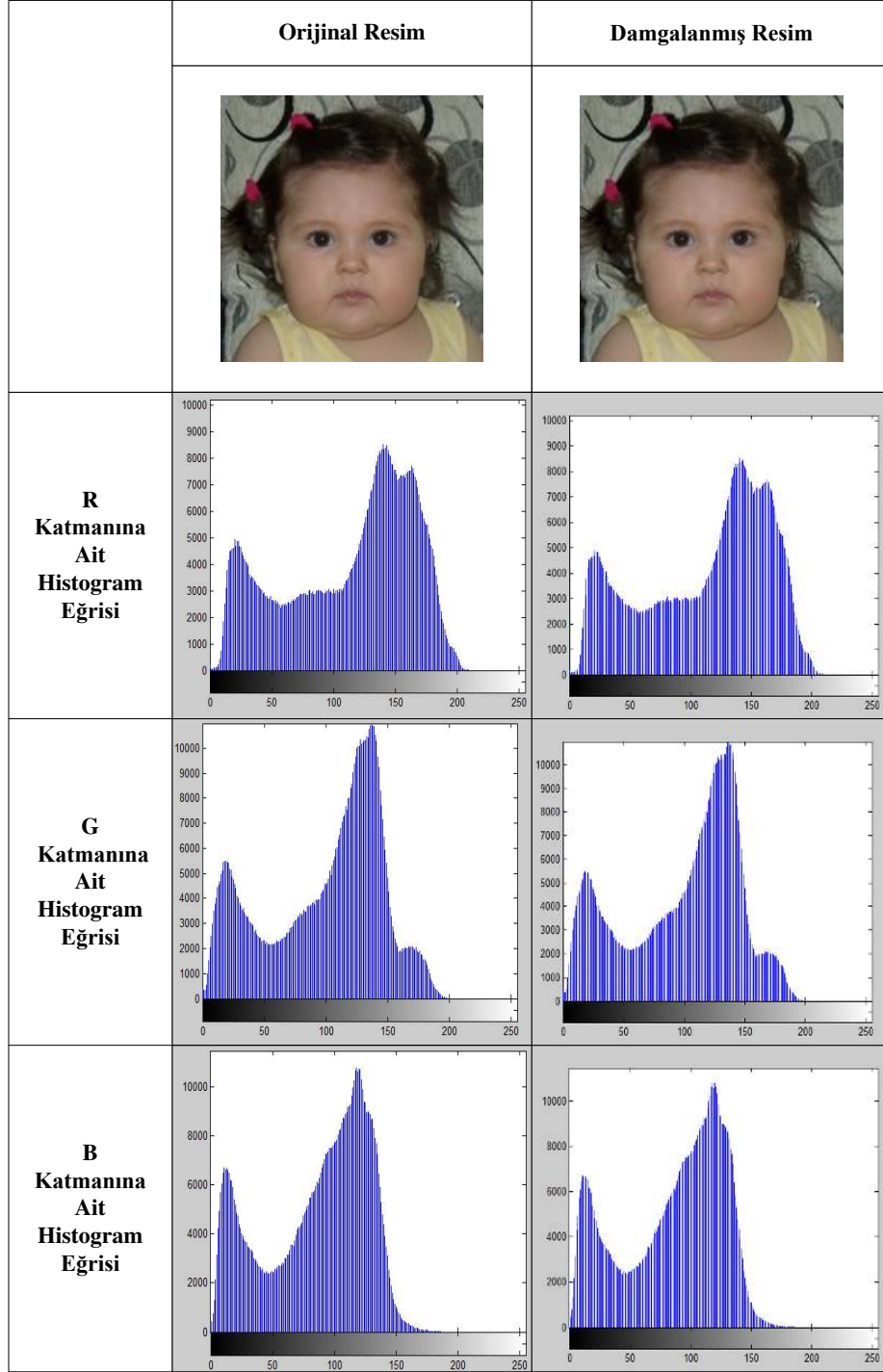
Damganın geri elde edilmesi için

1. Damgalanmış resme ADD uygulanır.
2. Damgalanmış resmin ADD katsayıları ve anahtar değerler baz alınarak damganın bit dizisi oluşturulur. Bu işlem damga boyutu anahtar değerle eşleşinceye kadar devam eder.
3. Damga görüntü formatına dönüştürülür.

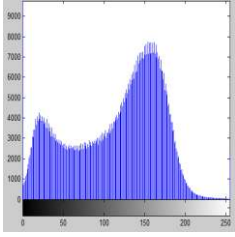
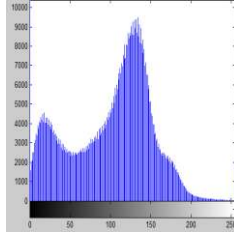
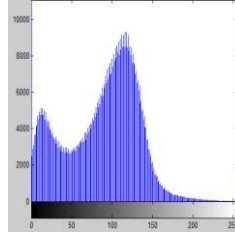
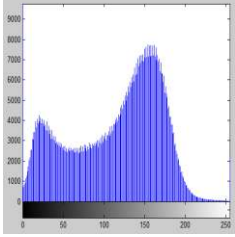
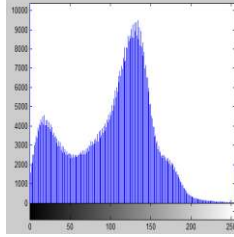
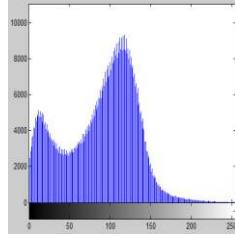
Orjinal Resim	Damga
	
Damgalanmış Resim	Damganın Damgalanmış Resimden Elde Edilmesi
	

Şekil 6.4. ADD tabanlı sistemden elde edilen sonuçlar

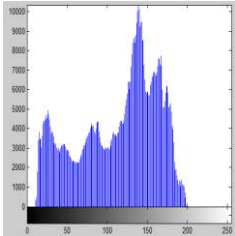
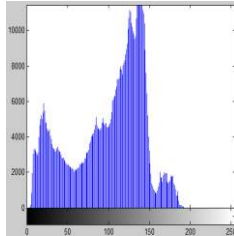
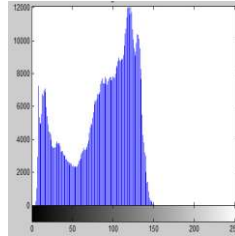
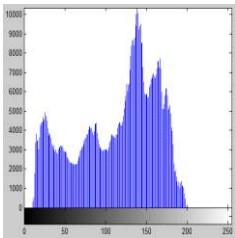
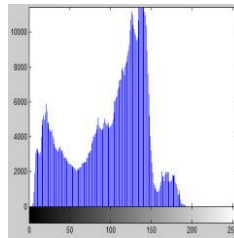
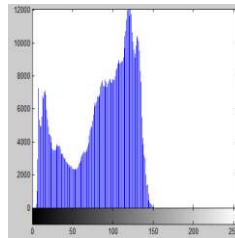
Şekil 6.4. (a)'da verilen örnek resmin damga eklenmesi işlemi ile hesaplanan PSNR değeri 42.6083, BER değeri 0.0269, NC oranı 1 ve hesaplama süresi 52.216691 sn olarak bulunmuştur. Damgalanmış resim ile orijinal resmin histogram eğrileri Şekil 6.5'de, yapılan saldırılar sonucu elde edilen histogram eğrileri ise Şekil 6.6.(a), (b), (c), (d)'de verilmiştir.



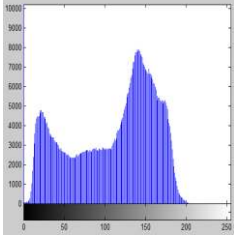
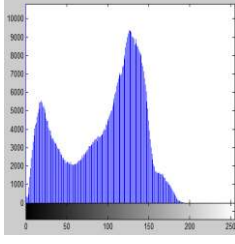
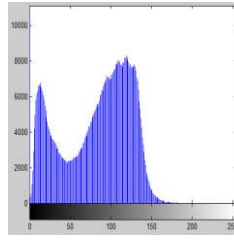
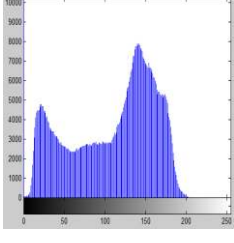
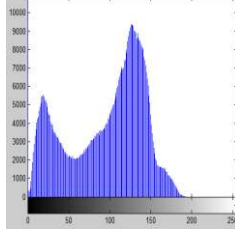
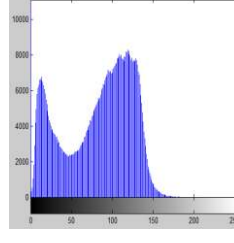
Şekil 6.5. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Keskinleştirilmiş Orijinal Resim	Keskinleştirilmiş Orijinal Resmin R Katmanı	Keskinleştirilmiş Orijinal Resmin G Katmanı	Keskinleştirilmiş Orijinal Resmin B Katmanı
			
Keskinleştirilmiş Damgalanmış Resim	Keskinleştirilmiş Damgalanmış Resmin R Katmanı	Keskinleştirilmiş Damgalanmış Resmin G Katmanı	Keskinleştirilmiş Damgalanmış Resmin B Katmanı
			

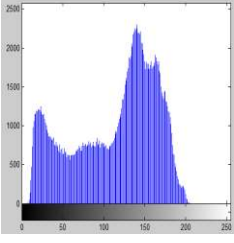
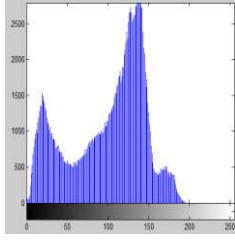
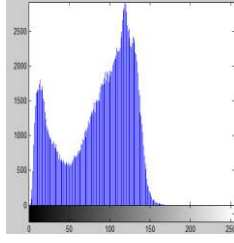
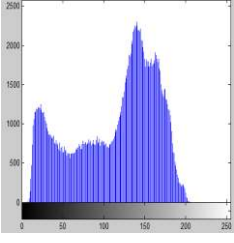
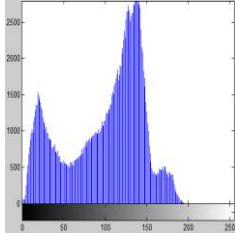
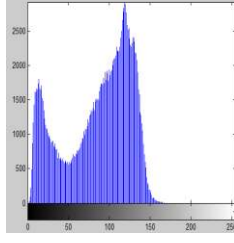
Şekil 6.6.(a) Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Bulanıklaştırılmış Orijinal Resim	Bulanıklaştırılmış Orijinal Resmin R Katmanı	Bulanıklaştırılmış Orijinal Resmin G Katmanı	Bulanıklaştırılmış Orijinal Resmin B Katmanı
			
Bulanıklaştırılmış Damgalanmış Resim	Bulanıklaştırılmış Damgalanmış Resmin R Katmanı	Bulanıklaştırılmış Damgalanmış Resmin G Katmanı	Bulanıklaştırılmış Damgalanmış Resmin B Katmanı
			

Şekil 6.6.(b) Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

1^o Döndürülmüş Orijinal Resim	1^o Döndürülmüş Orijinal Resmin R Katmanı	1^o Döndürülmüş Orijinal Resmin G Katmanı	1^o Döndürülmüş Orijinal Resmin B Katmanı
			
1^o Döndürülmüş Damgalanmış Resim	1^o Döndürülmüş Damgalanmış Resmin R Katmanı	1^o Döndürülmüş Damgalanmış Resmin G Katmanı	1^o Döndürülmüş Damgalanmış Resmin B Katmanı
			

Şekil 6.6.(c) 1^o döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Ölçeklendirilmiş (x0.5) Orijinal Resim	Ölçeklendirilmiş (x0.5) Orijinal Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin B Katmanı
			
Ölçeklendirilmiş (x0.5) Damgalanmış Resim	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin B Katmanı
			

Şekil 6.6.(d) Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 6.1.'de verilmiştir.

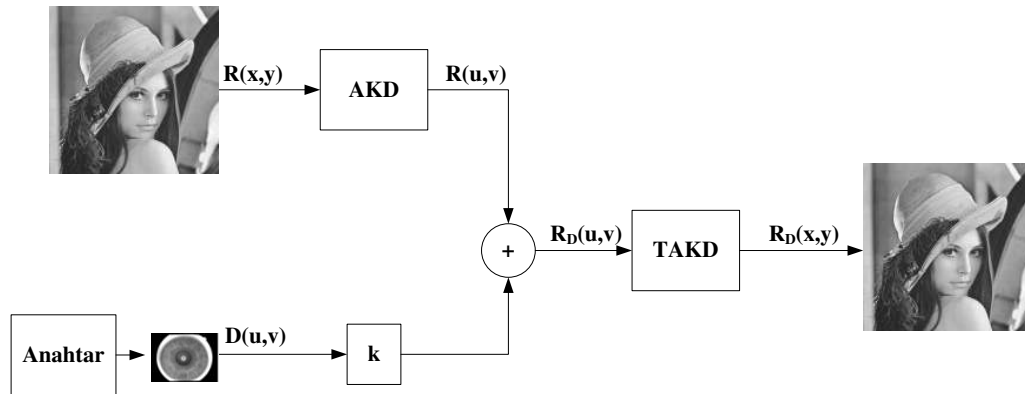
Tablo 6.1. Renkli iris ve yüz resimleri için ADD tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları

Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	42.8140	1	0.0257	52.729798

6.2. AKD Yöntemi ile Sayısal Damgalama Uygulaması

AKD, damgalama uygulamalarında damganın sağlamlığını ve saldırılara karşı dayanıklılığını artırdığı için geniş kullanım alanı bulmuştur. AKD ile damga ekleme işlemi Şekil 6.7.'de gösterildiği gibi

1. Orijinal resmin yaklaşık boyutu AKD ile elde edilir.
2. Algoritmada damga olarak seçilen rastlantısal işaret k gibi bir katsayı ile orantılanarak yaklaşık boyuta eklenir. Ayrıca değişen AKD katsayılarının indisi ve damganın boyutu bir anahtarda tutulur.
3. Görüntünün TAKD alınarak damgalanmış resim elde edilir.



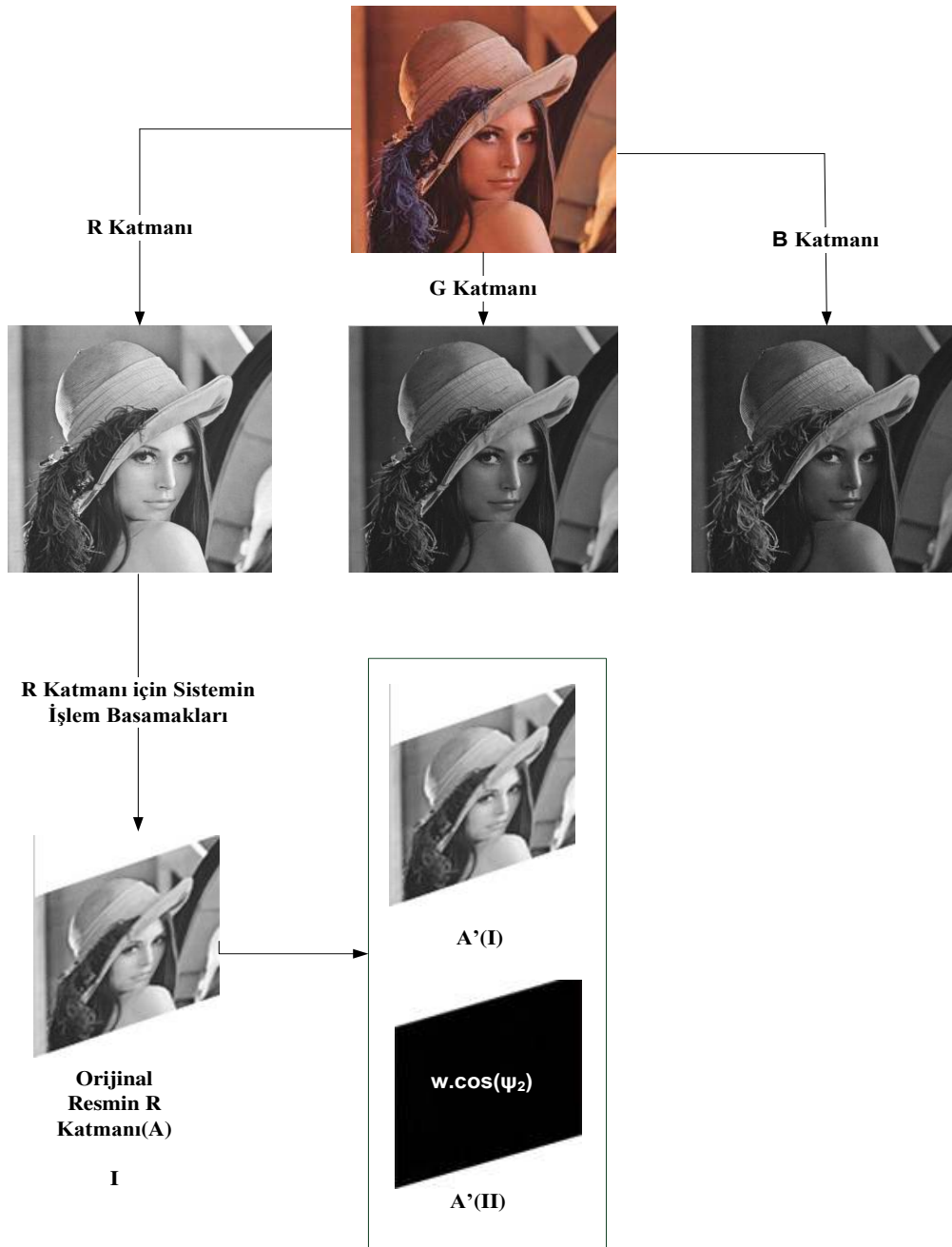
Şekil 6.7. AKD ile damgalama işlemi

Damga çıkarma işleminde ise

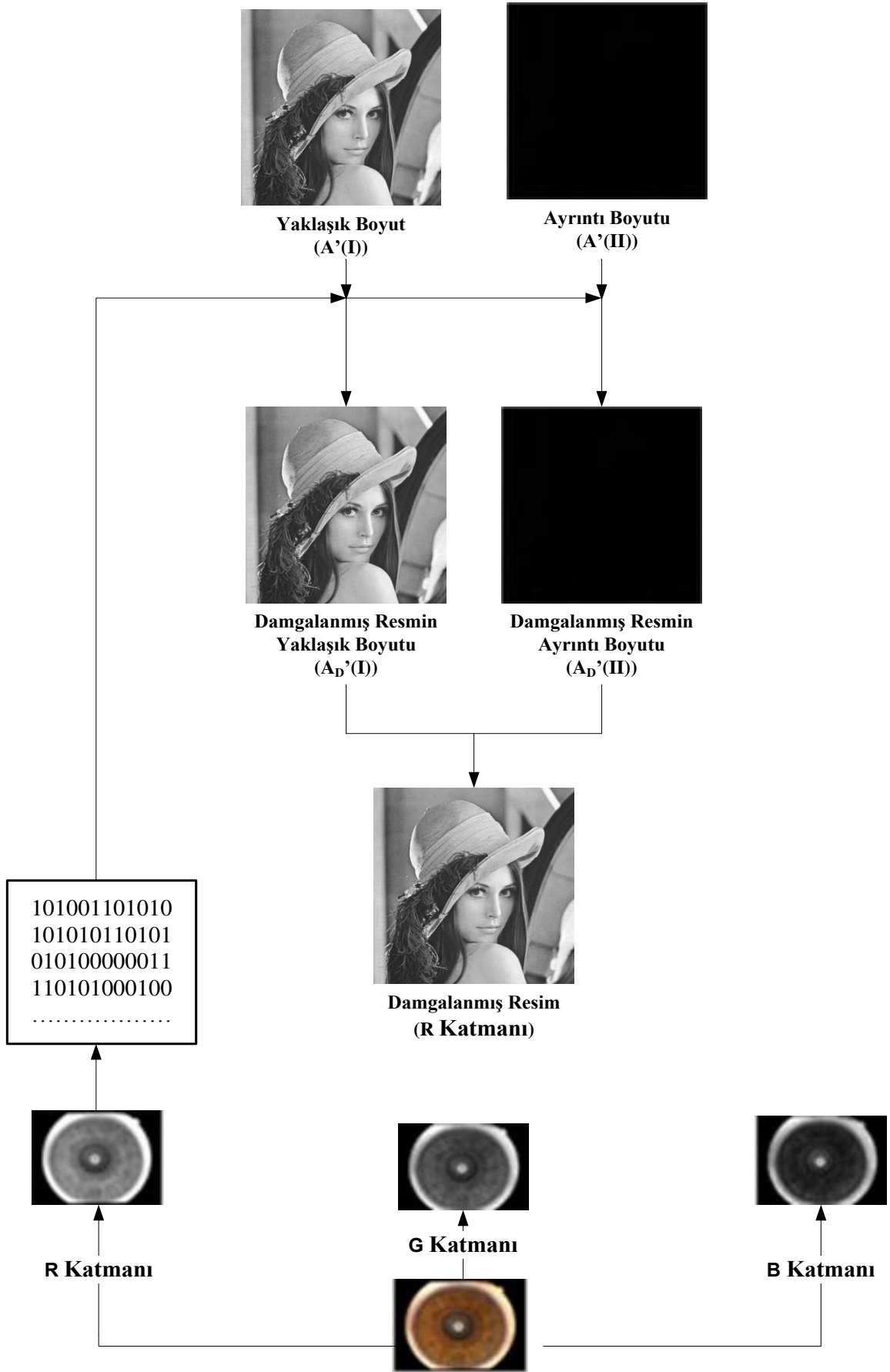
1. Damgalanmış resmin AKD alınır.

2. Damgalanmış resmin AKD katsayıları ve anahtar değerler baz alınarak damganın bit dizisi oluşturulur. Bu işlem damga boyutu anahtar değerle eşleşinceye kadar devam eder.
3. Damga görüntü formatına dönüştürülür.

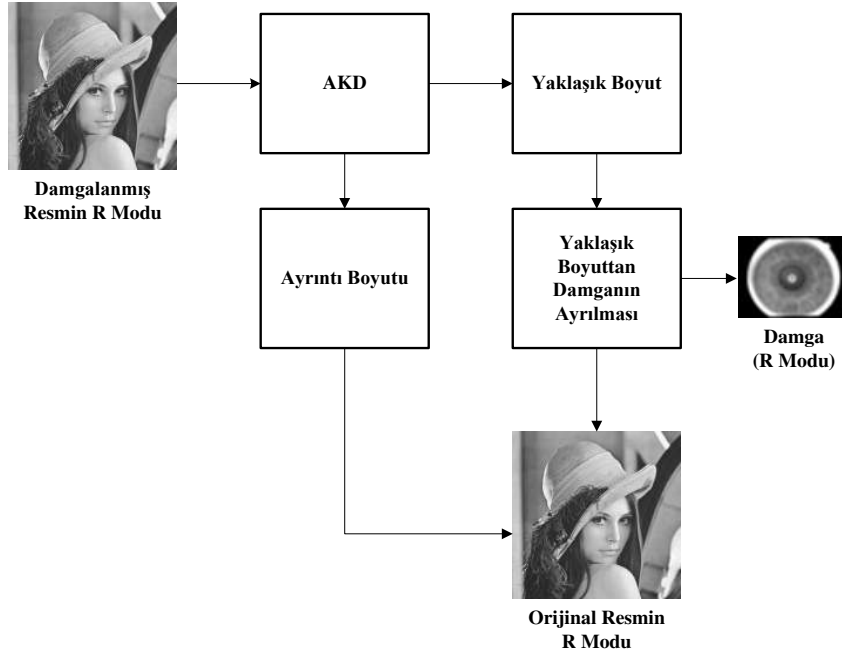
AKD yöntemi ile orijinal resim üzerine iris resminin damgalaması işleminin blok şeması Şekil 6.8.a ve b.'de, damgalanan resmin yeniden elde edilmesi işleminin blok şeması ise Şekil 6.9'de verilmiştir.



Şekil 6.8.a. AKD ile resmin ayrıştırılması



Şekil 6.8.b. AKD tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı

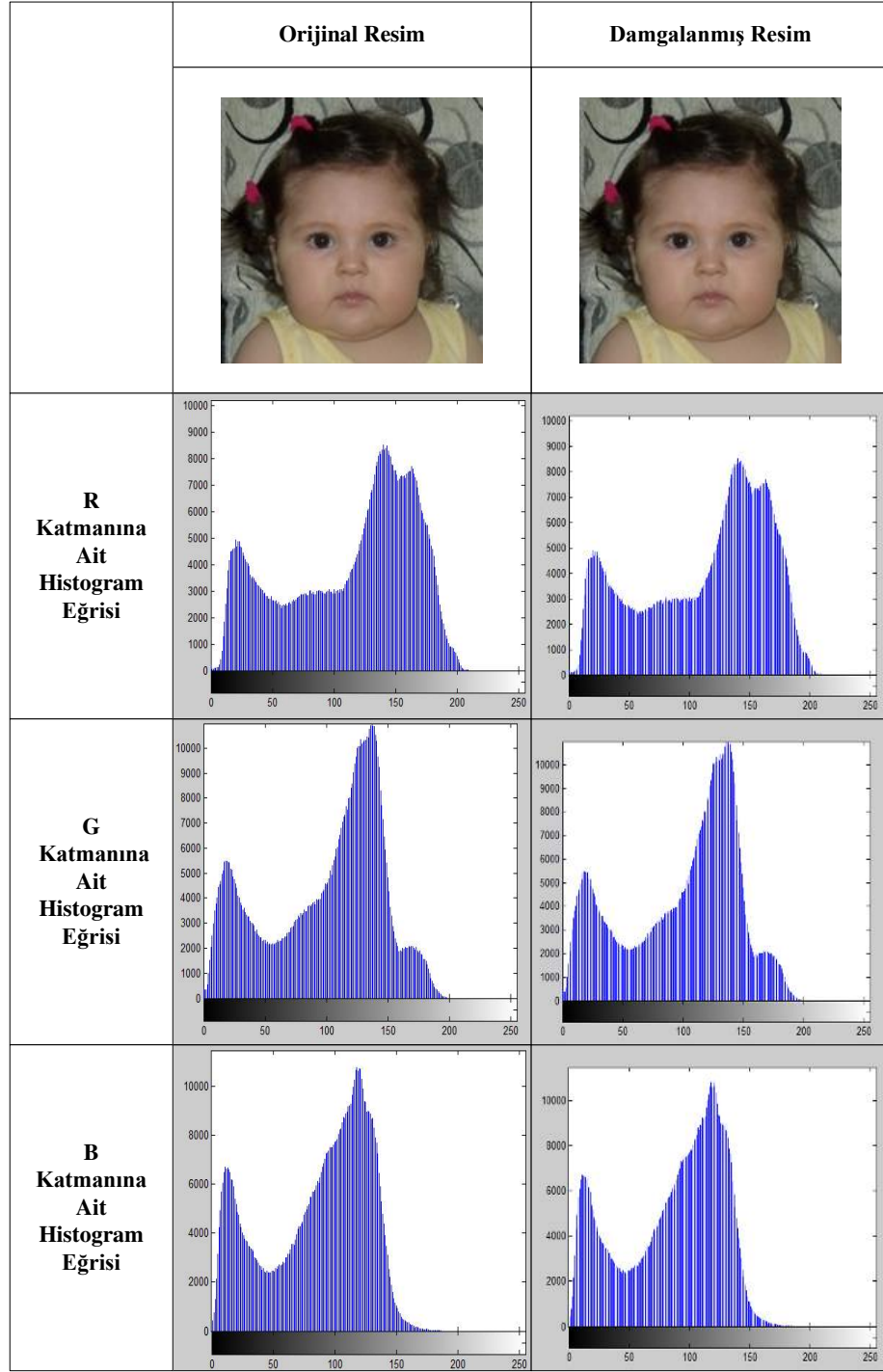


Şekil 6.9. AKD tabanlı sistemde damga çıkarma için sisteminin blok diyagramı

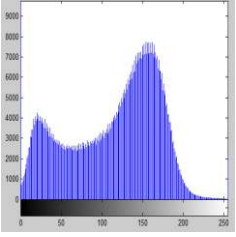
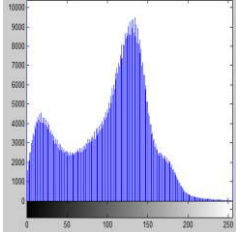
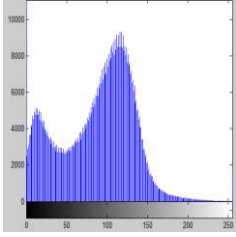
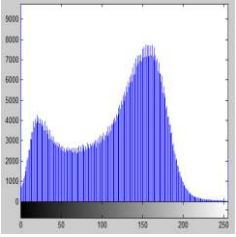
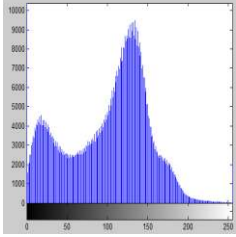
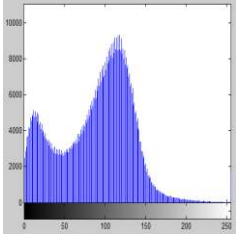
Orijinal Resim (a)	Damga (b)	Damgalanmış Resim (c)	Damganın Damgalanmış Resimden Elde Edilmesi (d)

Şekil 6.10. AKD tabanlı sistemden elde edilen sonuçlar

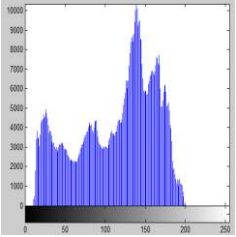
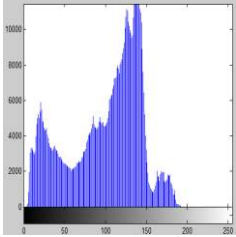
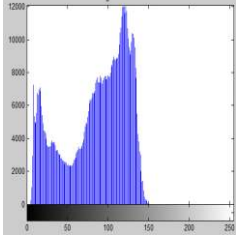
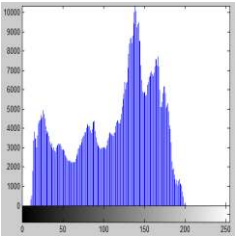
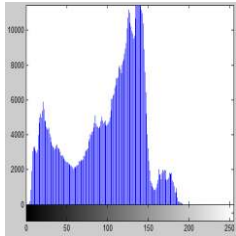
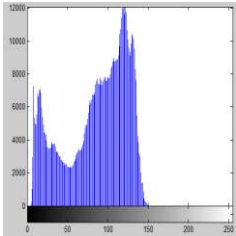
Sistemde Şekil 6.10.(a)'nın, Şekil 6.10.(b) ile damgalanması sonucu elde edilen PSNR değeri 39.7061, BER değeri 0.0144, Hesaplama Süresi 23.626921 sn ve NC oranı 1 olarak hesaplanmıştır. Damgalanmış resim ile orijinal resmin histogram eğrileri Şekil 6.11.'de, yapılan saldırılar sonucu elde edilen histogram eğrileri ise Şekil 6.12.(a), (b), (c), (d)'de verilmiştir.



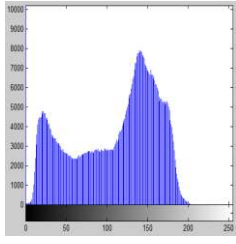
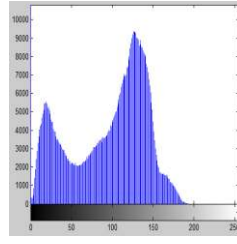
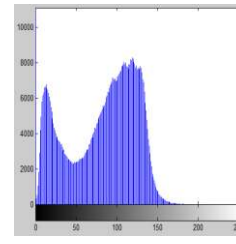
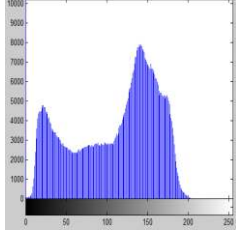
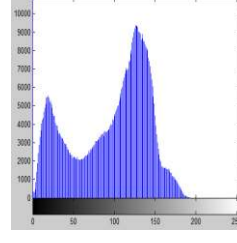
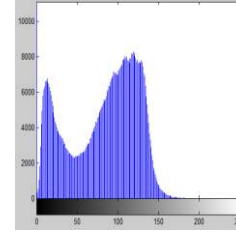
Şekil 6.11. Orijinal resim ile damgalanmış resmin R,G,B katmanlarının histogram eğrilerinin karşılaştırılması

Keskinleştirilmiş Orijinal Resim	Keskinleştirilmiş Orijinal Resmin R Katmanı	Keskinleştirilmiş Orijinal Resmin G Katmanı	Keskinleştirilmiş Orijinal Resmin B Katmanı
			
Keskinleştirilmiş Damgalanmış Resim	Keskinleştirilmiş Damgalanmış Resmin R Katmanı	Keskinleştirilmiş Damgalanmış Resmin G Katmanı	Keskinleştirilmiş Damgalanmış Resmin B Katmanı
			

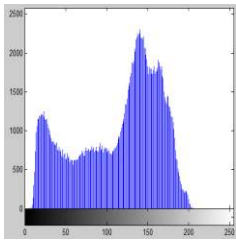
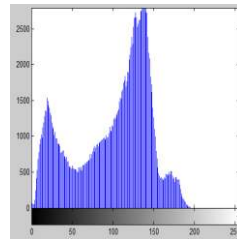
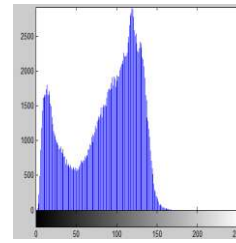
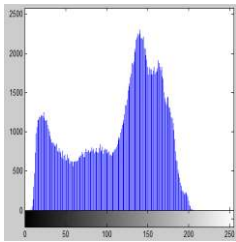
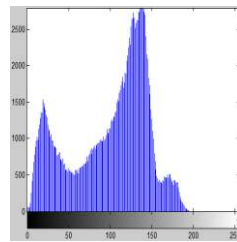
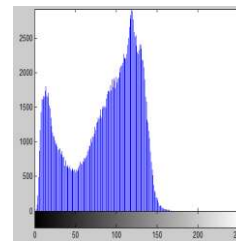
Şekil 6.12.(a) Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Bulanıklaştırılmış Orijinal Resim	Bulanıklaştırılmış Orijinal Resmin R Katmanı	Bulanıklaştırılmış Orijinal Resmin G Katmanı	Bulanıklaştırılmış Orijinal Resmin B Katmanı
			
Bulanıklaştırılmış Damgalanmış Resim	Bulanıklaştırılmış Damgalanmış Resmin R Katmanı	Bulanıklaştırılmış Damgalanmış Resmin G Katmanı	Bulanıklaştırılmış Damgalanmış Resmin B Katmanı
			

Şekil 6.12.(b) Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

1^o Döndürülmüş Orijinal Resim	1^o Döndürülmüş Orijinal Resmin R Katmanı	1^o Döndürülmüş Orijinal Resmin G Katmanı	1^o Döndürülmüş Orijinal Resmin B Katmanı
			
1^o Döndürülmüş Damgalanmış Resim	1^o Döndürülmüş Damgalanmış Resmin R Katmanı	1^o Döndürülmüş Damgalanmış Resmin G Katmanı	1^o Döndürülmüş Damgalanmış Resmin B Katmanı
			

Şekil 6.12.(c) 1^o döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Ölçeklendirilmiş (x0.5) Orijinal Resim	Ölçeklendirilmiş (x0.5) Orijinal Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin B Katmanı
			
Ölçeklendirilmiş (x0.5) Damgalanmış Resim	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin B Katmanı
			

Şekil 6.12.(d) Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 6.2.'de verilmiştir.

Tablo 6.2. Renkli iris ve yüz resimleri için AKD tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları

Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	40.1649	1	0.0145	24.143840

6.3. TDA Yöntemi ile Sayısal Damgalama Uygulaması

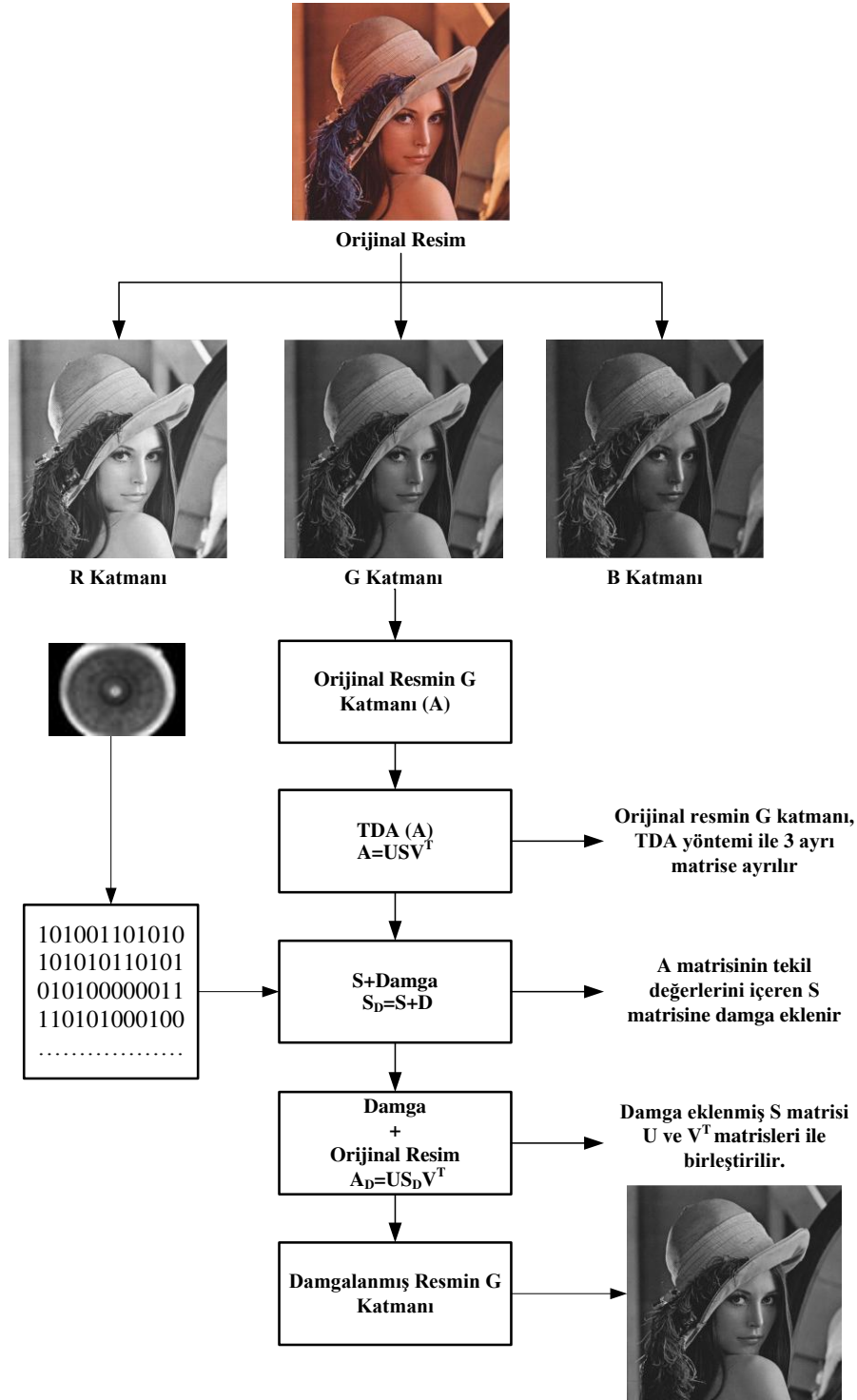
TDA ile damga ekleme işleminde

1. Orijinal resmin TDA yöntemi ile tekil değerleri elde edilir ($A=USV^T$).
2. Elde edilen tekil değer matrisine k ile ölçeklenmiş damga eklenir ($S_D=S+k.D$). Ayrıca değişen TDA katsayılarının indisi ve damganın boyutu bir anahtarda tutulur.
3. Damgalanmış tekil değer matrisi ile diğer iki matris birleştirilerek damgalanmış resim oluşturulur ($A_D=US_DV^T$).

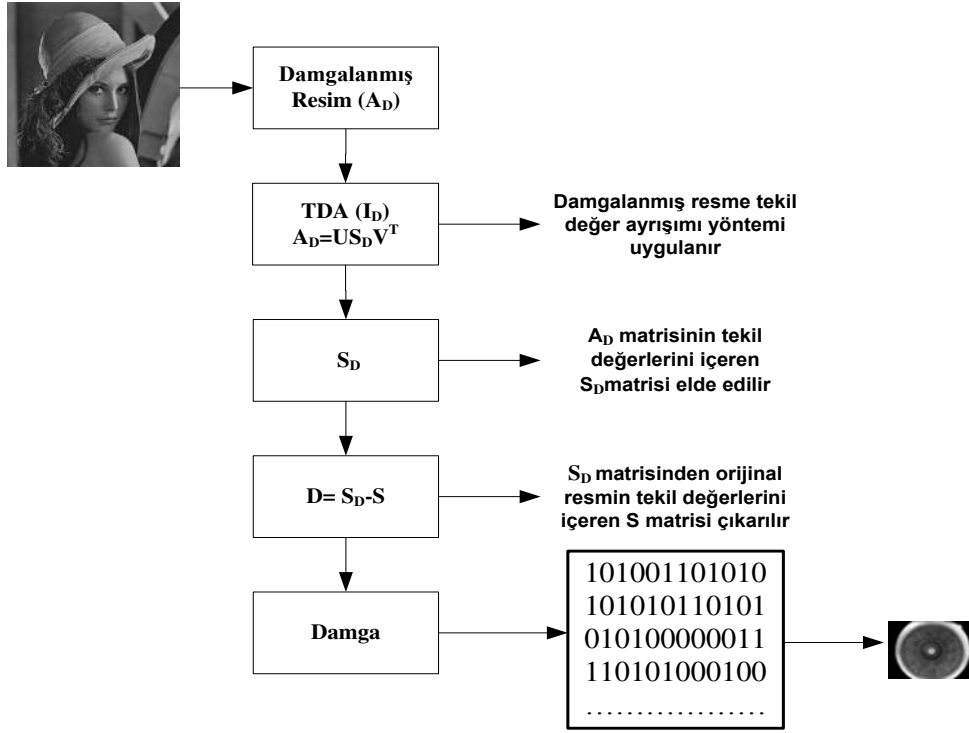
Damgalanmış resimden damganın çıkarılması için

1. Damgalanmış resme TDA yöntemi uygulanır ($A_D=US_DV^T$).
2. Damgalanmış resmin tekil değerleri ve anahtar değerler baz alınarak damganın bit dizisi oluşturulur. Bu işlem damga boyutu anahtar değerle eşleşinceye kadar devam eder.
3. Damga görüntü formatına dönüştürülür.

TDA yöntemi ile orijinal resim üzerine damganın eklenmesi işleminin blok şeması Şekil 6.13.'de, damgalanan verilerin yeniden elde edilmesi işlemi için sistemin blok şeması ise Şekil 6.14.'de verilmiştir.



Şekil 6.13. TDA tabanlı damgalama sisteminin renkli iris ve yüz resimleri için blok diyagramı

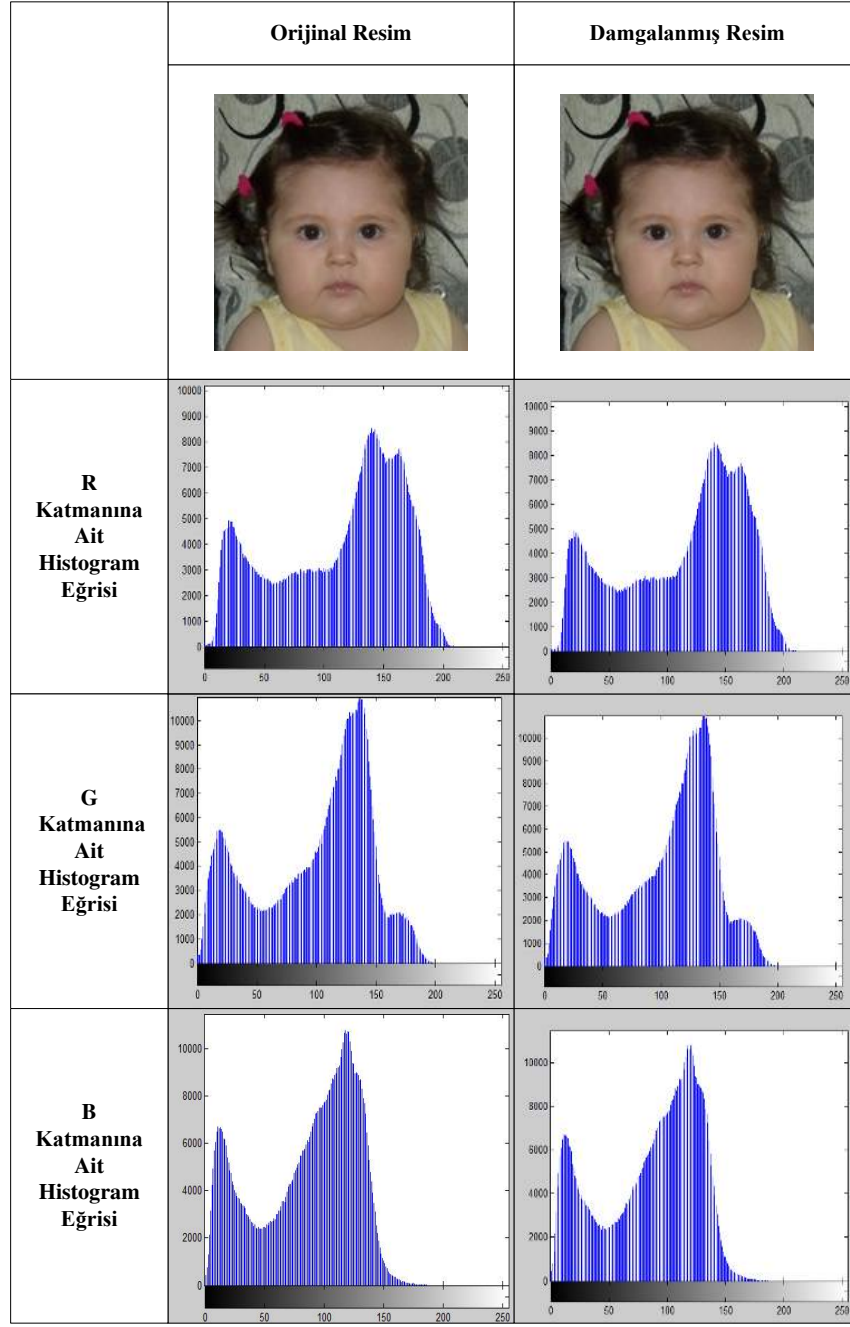


Şekil 6.14. TDA tabanlı damga çıkarma sisteminin iris ve yüz resimleri için blok diyagramı

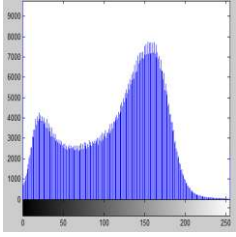
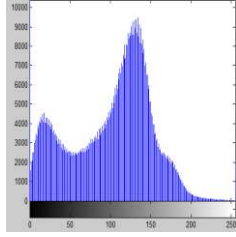
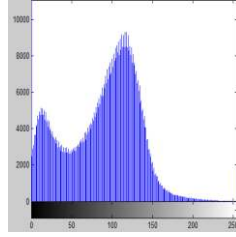
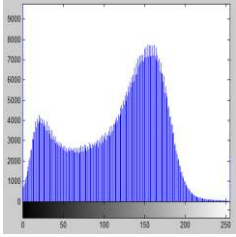
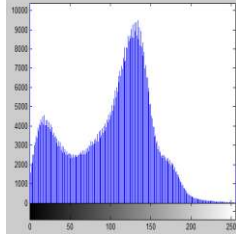
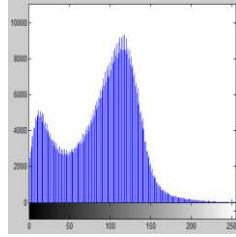
Orijinal Resim (a)	Damga (b)
Damgalanmış Resim (c)	Damganın Damgalanmış Resimden Elde Edilmesi (d)

Şekil 6.15. TDA tabanlı sistemden elde edilen sonuçlar

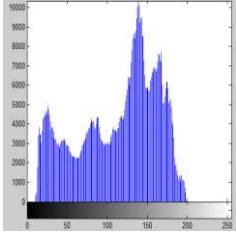
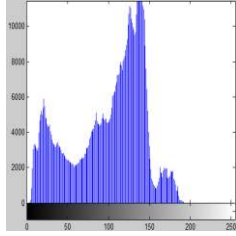
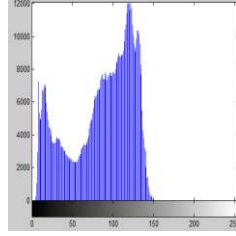
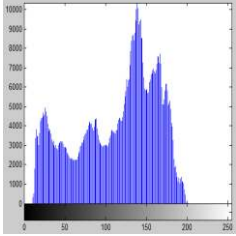
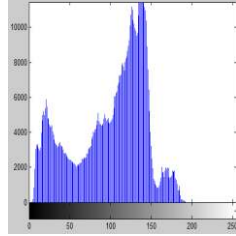
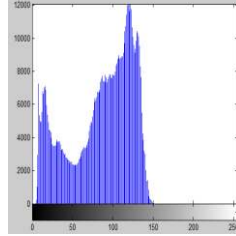
Şekil 6.15. (c)'de verilen damgalanmış resimden elde edilen PSNR değeri 42.2094, BER değeri 0.0472, hesaplama süresi 47.171945 sn ve NC oranı 1 olarak hesaplanmıştır. Damgalanmış resim ile orijinal resmin histogram eğrileri Şekil 6.16'de, yapılan saldırılar sonucu elde edilen histogram eğrileri ise Şekil 6.17.(a), (b), (c), (d)'de verilmiştir.



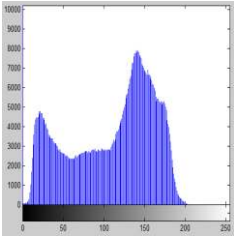
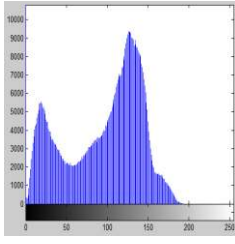
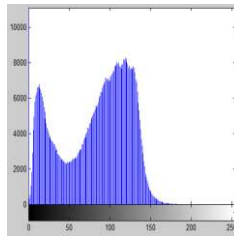
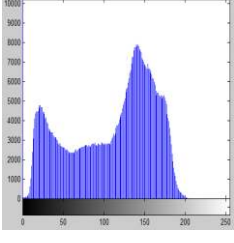
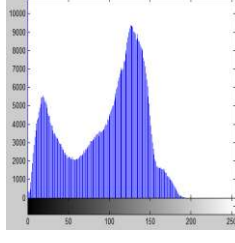
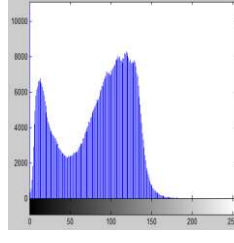
Şekil 6.16. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Keskinleştirilmiş Orijinal Resim	Keskinleştirilmiş Orijinal Resmin R Katmanı	Keskinleştirilmiş Orijinal Resmin G Katmanı	Keskinleştirilmiş Orijinal Resmin B Katmanı
			
Keskinleştirilmiş Damgalanmış Resim	Keskinleştirilmiş Damgalanmış Resmin R Katmanı	Keskinleştirilmiş Damgalanmış Resmin G Katmanı	Keskinleştirilmiş Damgalanmış Resmin B Katmanı
			

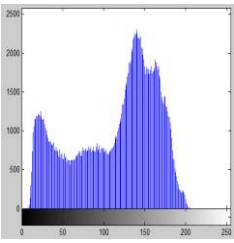
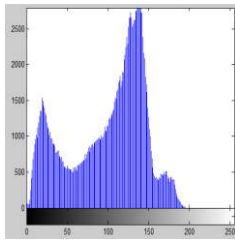
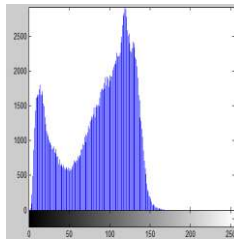
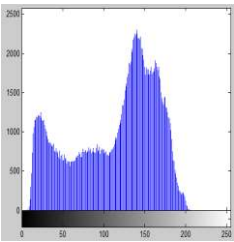
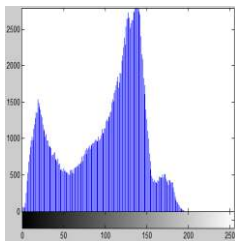
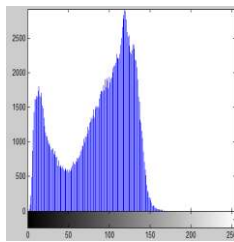
Şekil 6.17.(a) Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Bulanıklaştırılmış Orijinal Resim	Bulanıklaştırılmış Orijinal Resmin R Katmanı	Bulanıklaştırılmış Orijinal Resmin G Katmanı	Bulanıklaştırılmış Orijinal Resmin B Katmanı
			
Bulanıklaştırılmış Damgalanmış Resim	Bulanıklaştırılmış Damgalanmış Resmin R Katmanı	Bulanıklaştırılmış Damgalanmış Resmin G Katmanı	Bulanıklaştırılmış Damgalanmış Resmin B Katmanı
			

Şekil 6.17.(b) Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

1^o Döndürülmüş Orijinal Resim	1^o Döndürülmüş Orijinal Resmin R Katmanı	1^o Döndürülmüş Orijinal Resmin G Katmanı	1^o Döndürülmüş Orijinal Resmin B Katmanı
			
1^o Döndürülmüş Damgalanmış Resim	1^o Döndürülmüş Damgalanmış Resmin R Katmanı	1^o Döndürülmüş Damgalanmış Resmin G Katmanı	1^o Döndürülmüş Damgalanmış Resmin B Katmanı
			

Şekil 6.17.(c) 1^o döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Ölçeklendirilmiş (x0.5) Orijinal Resim	Ölçeklendirilmiş (x0.5) Orijinal Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin B Katmanı
			
Ölçeklendirilmiş (x0.5) Damgalanmış Resim	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin B Katmanı
			

Şekil 6.17.(d) Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

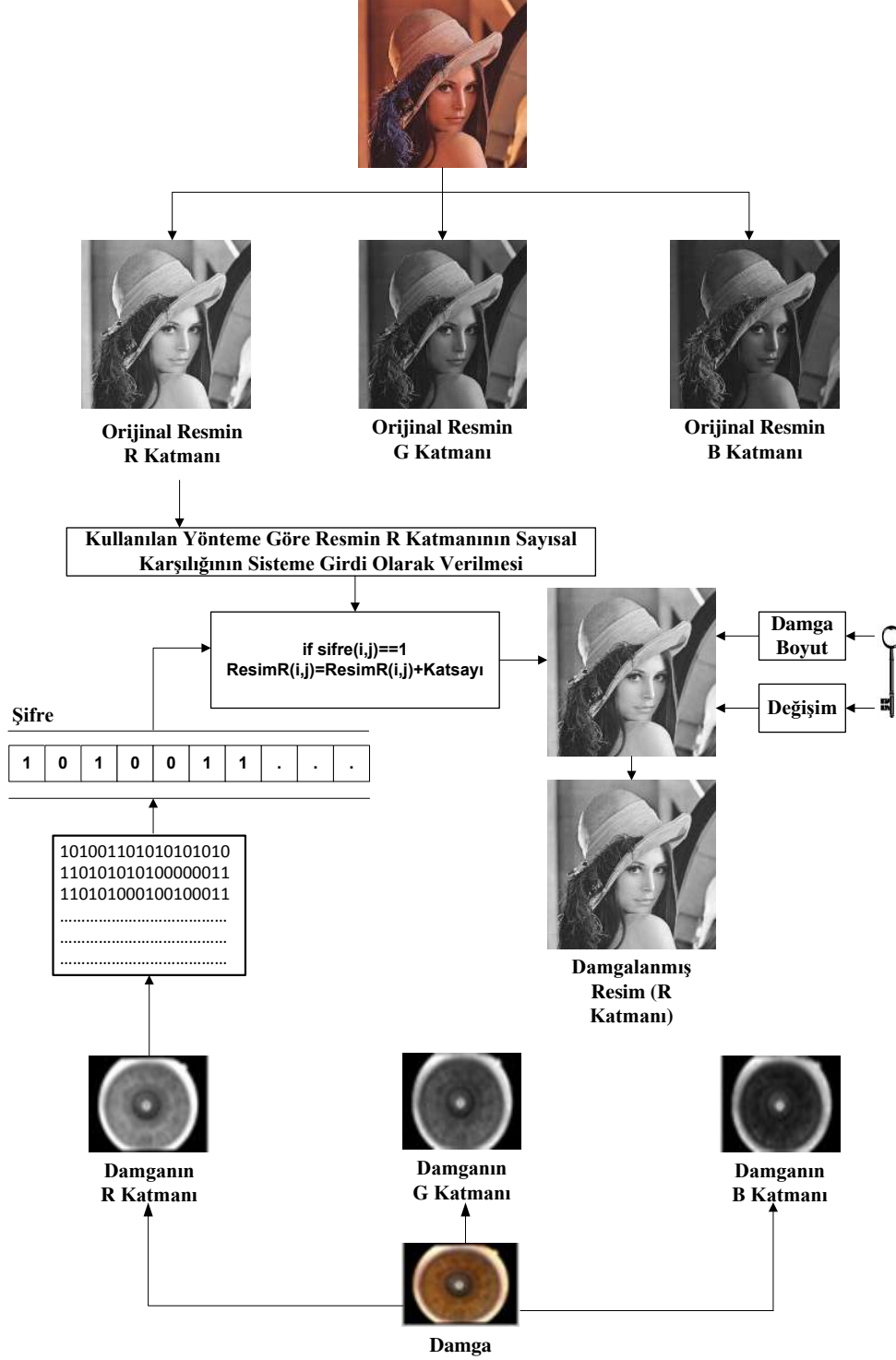
Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 6.3.'de verilmiştir.

Tablo 6.3. Renkli iris ve yüz resimleri için TDA tabanlı damgalama sisteminde elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları

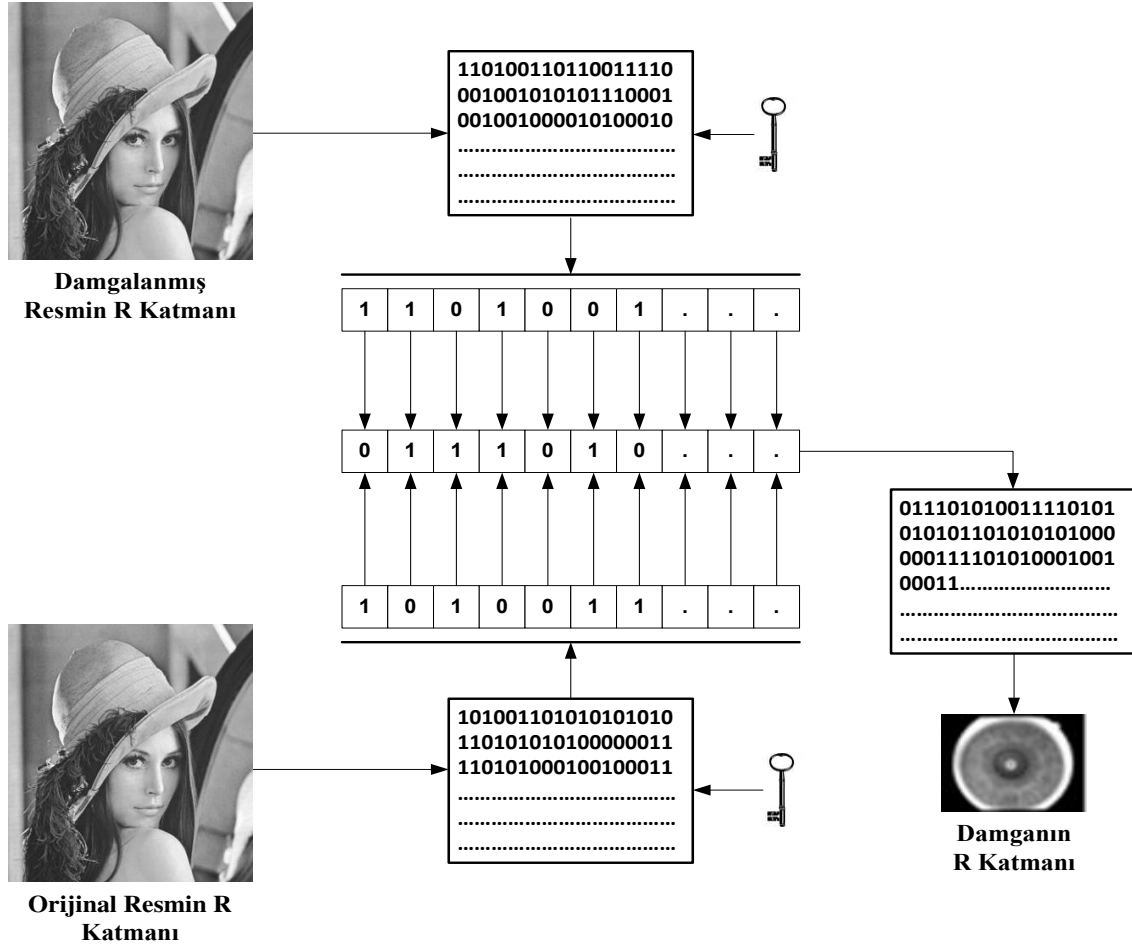
Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	42.0421	1	0.0451	47.757082

7. GELİŞTİRİLEN YÖNTEM İLE SAYISAL DAMGALAMA UYGULAMASI

Geliştirilen yöntem ile iris resminin orijinal resmin üzerine damgalanması işleminin blok şeması Şekil 7.1.'de, damganın damgalanmış resimden elde edilmesi için sistemin blok şeması Şekil 7.2.'de verilmiştir.



Şekil 7.1. Geliştirilen yöntem ile sisteminin renkli iris ve yüz resimleri için damgalama blok diyagramı

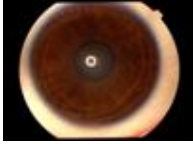
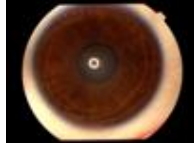


Şekil 7.2. Geliştirilen yöntem ile iris ve yüz resimleri için damga çıkarma sisteminin blok diyagramı

Şekil 7.1.'de verildiği gibi damga ve orijinal resim R, G ve B katmanlarına ayrılarak amaca göre işlenebilecek kodları (ASCII kodları, double karşılığı) elde edilir. Geliştirilen sistemde damganın orijinal resme eklenmesinde damga baz alınır. Damganın ikili kodları elde edildikten sonra aldığı değere göre sistemin belirleyeceği katsayı orijinal resmin değerine eklenir. Damgalanmış resimden elde edilecek damganın NC değerinin 1 olması dikkate alınarak belirlenen katsayı değeri orijinal resmin piksel değerini bozmayacak kadar küçük, aynı zamanda damganın geri elde edilebilmesine olanak sağlayacak kadarda büyük olmalıdır. Damganın resme eklenmesi tamamlandıktan sonra anahtar değerler eklenir. Sistem iki anahtar değer içermektedir. Bunlardan birincisi damganın boyutu ikincisi ise değişim oranının yüzdesidir. Bu işlemlerin sonucunda Şekil 7.3.(c)'deki damgalanmış resim elde edilir.

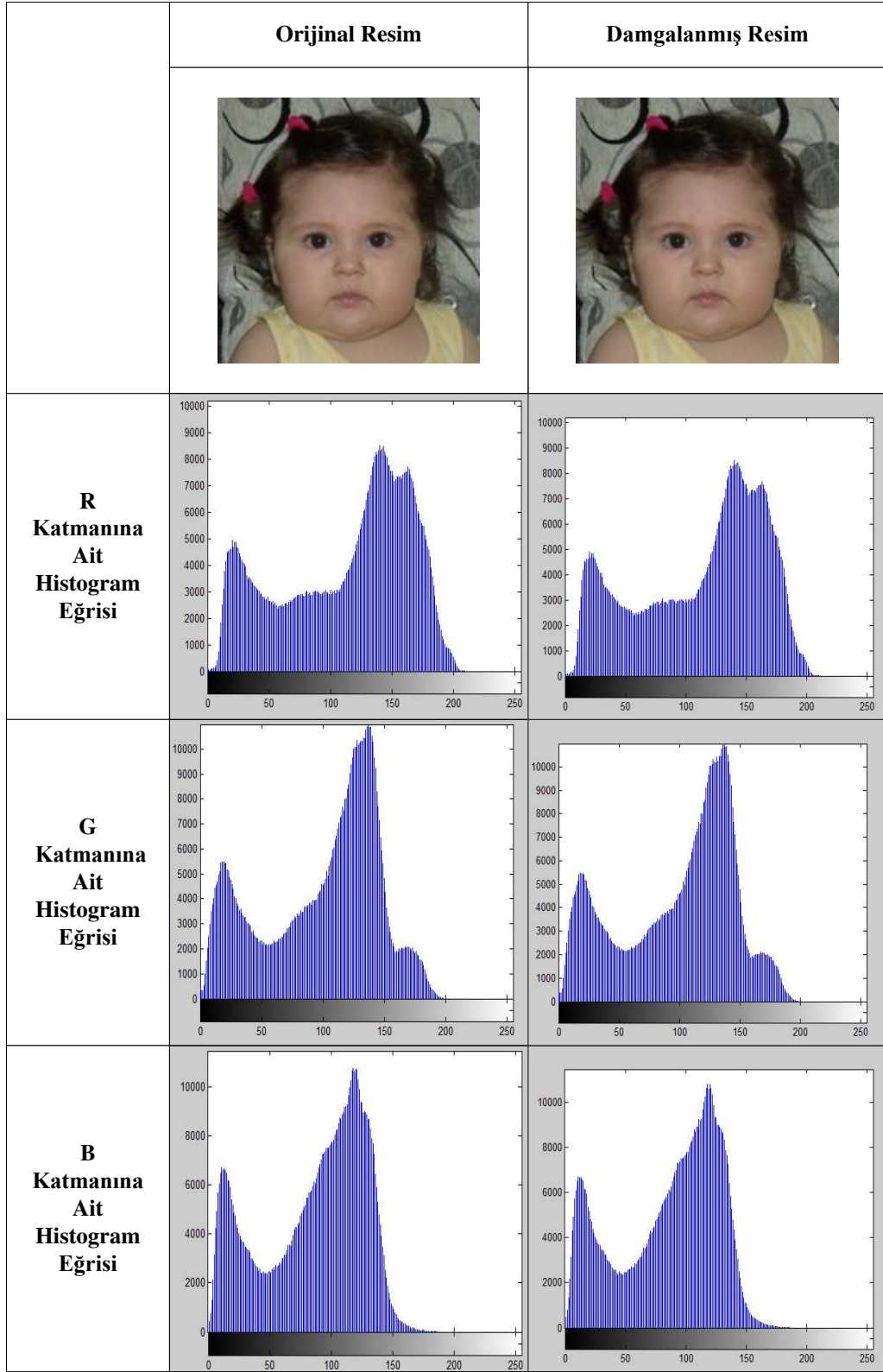
Damgalanmış resimden damga çıkarma işleminde orijinal resim ve ayrıca damgalanmış resimden elde edilen anahtar değerler dikkate alınır. Damgalanmış resimdeki anahtar değerlerden damga boyutu baz alınarak Şekil 7.2.'de verilen blok şemasında

gösterildiği gibi orijinal resim ve damgalanmış resim arasında eşleştirme yapılır. Eşleştirmenin hangi indise kadar süreceği ilk anahtar değeri ile belirlenir. Böylelikle damganın ikili kodları elde edilerek Şekil 7.3.(d)'de verilen damga elde edilir. Orijinal resim ile damgalanmış resim arasındaki değişimin yüzde karşılığı ikinci anahtar değerdir ve bu değer iletim kanalında herhangi bir saldırı olup olmadığının tespiti için kullanılır. Damga çıkarma işleminde değişim oranı eşleşmez ise damgalanmış resmin yeniden iletilmesi istenir.

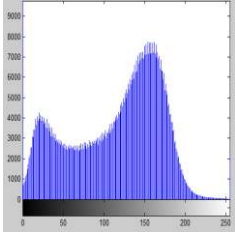
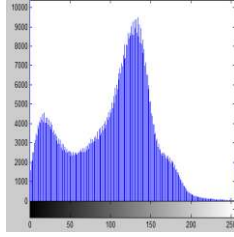
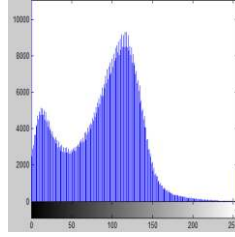
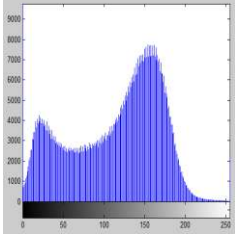
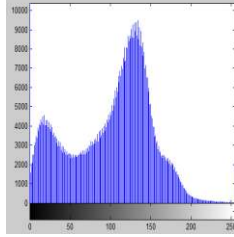
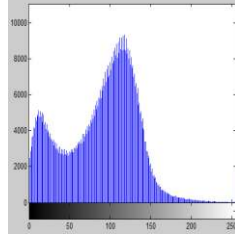
Orijinal Resim (a)	Damga (b)	Damgalanmış Resim (c)	Damganın Damgalanmış Resimden Elde Edilmesi (d)
			

Şekil 7.3. Geliştirilen yöntem ile sistemden elde edilen sonuçlar

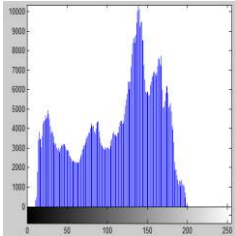
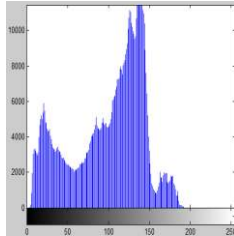
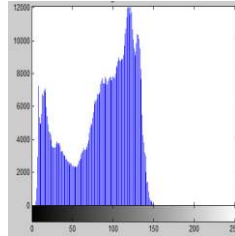
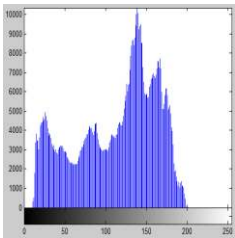
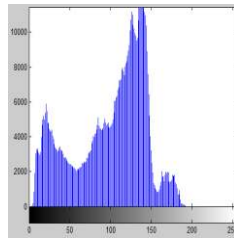
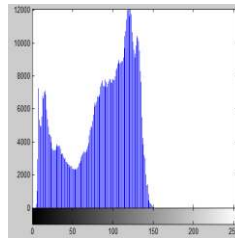
Sistemde verilen örnek resim için hesaplanan PSNR değeri 51.7964, BER değeri 0.0025, hesaplama süresi 22.516435 sn ve NC oranı 1 olarak bulunmuştur. Damgalanmış resim ile orijinal resmin histogram eğrileri Şekil 7.4.'de, yapılan saldırılar sonucu elde edilen histogram eğrileri ise Şekil 7.5.(a), (b), (c), (d)'de verilmiştir.



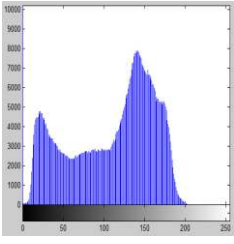
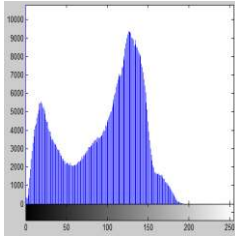
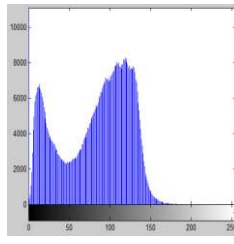
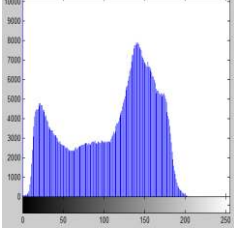
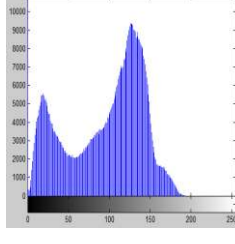
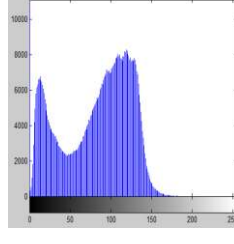
Şekil 7.4. Orijinal resim ile damgalanmış resmin R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Keskinleştirilmiş Orijinal Resim	Keskinleştirilmiş Orijinal Resmin R Katmanı	Keskinleştirilmiş Orijinal Resmin G Katmanı	Keskinleştirilmiş Orijinal Resmin B Katmanı
			
Keskinleştirilmiş Damgalanmış Resim	Keskinleştirilmiş Damgalanmış Resmin R Katmanı	Keskinleştirilmiş Damgalanmış Resmin G Katmanı	Keskinleştirilmiş Damgalanmış Resmin B Katmanı
			

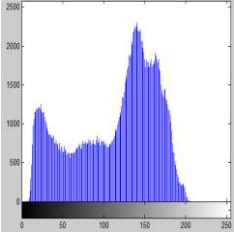
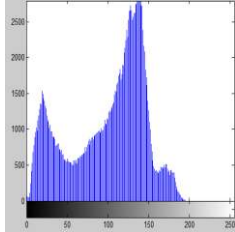
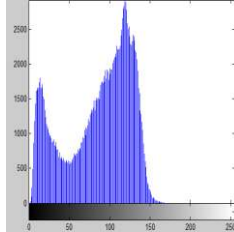
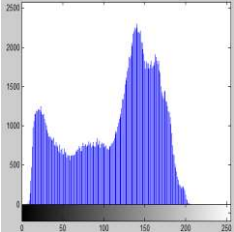
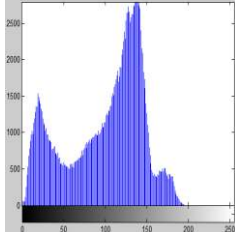
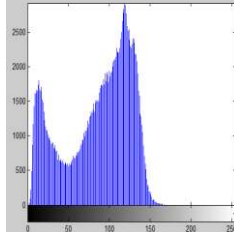
Şekil 7.5.(a) Keskinleştirme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Bulanıklaştırılmış Orijinal Resim	Bulanıklaştırılmış Orijinal Resmin R Katmanı	Bulanıklaştırılmış Orijinal Resmin G Katmanı	Bulanıklaştırılmış Orijinal Resmin B Katmanı
			
Bulanıklaştırılmış Damgalanmış Resim	Bulanıklaştırılmış Damgalanmış Resmin R Katmanı	Bulanıklaştırılmış Damgalanmış Resmin G Katmanı	Bulanıklaştırılmış Damgalanmış Resmin B Katmanı
			

Şekil 7.5.(b) Bulanıklaştırma işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

1^o Döndürülmüş Orijinal Resim	1^o Döndürülmüş Orijinal Resmin R Katmanı	1^o Döndürülmüş Orijinal Resmin G Katmanı	1^o Döndürülmüş Orijinal Resmin B Katmanı
			
1^o Döndürülmüş Damgalanmış Resim	1^o Döndürülmüş Damgalanmış Resmin R Katmanı	1^o Döndürülmüş Damgalanmış Resmin G Katmanı	1^o Döndürülmüş Damgalanmış Resmin B Katmanı
			

Şekil 7.5.(c) 1^o döndürme işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Ölçeklendirilmiş (x0.5) Orijinal Resim	Ölçeklendirilmiş (x0.5) Orijinal Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Orijinal Resmin B Katmanı
			
Ölçeklendirilmiş (x0.5) Damgalanmış Resim	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin R Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin G Katmanı	Ölçeklendirilmiş (x0.5) Damgalanmış Resmin B Katmanı
			

Şekil 7.5.(d) Ölçeklendirme (x0.5) işlemi sonrası R, G, B katmanlarının histogram eğrilerinin karşılaştırılması

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 7.1.'de verilmiştir.

Tablo 7.1. Geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi ortalama sonuçları

Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	51.5839	1	0.0024	21.638468

Damgalanmış resme uygulanan keskinleştirme, bulanıklaştırma ve döndürme saldırıları sonrası elde edilen damganın NC oranları Tablo 7.2.'de gösterilmiştir.

Tablo 7.2. Damganın geliştirilen yöntem ile saldırılara dayanıklılığı

Saldırı	Ortalama NC
Yok	1
Keskinleştirme (1 kez)	0.8137
Bulanıklaştırma (20 %)	0.7049
Döndürme (1°)	0.6382

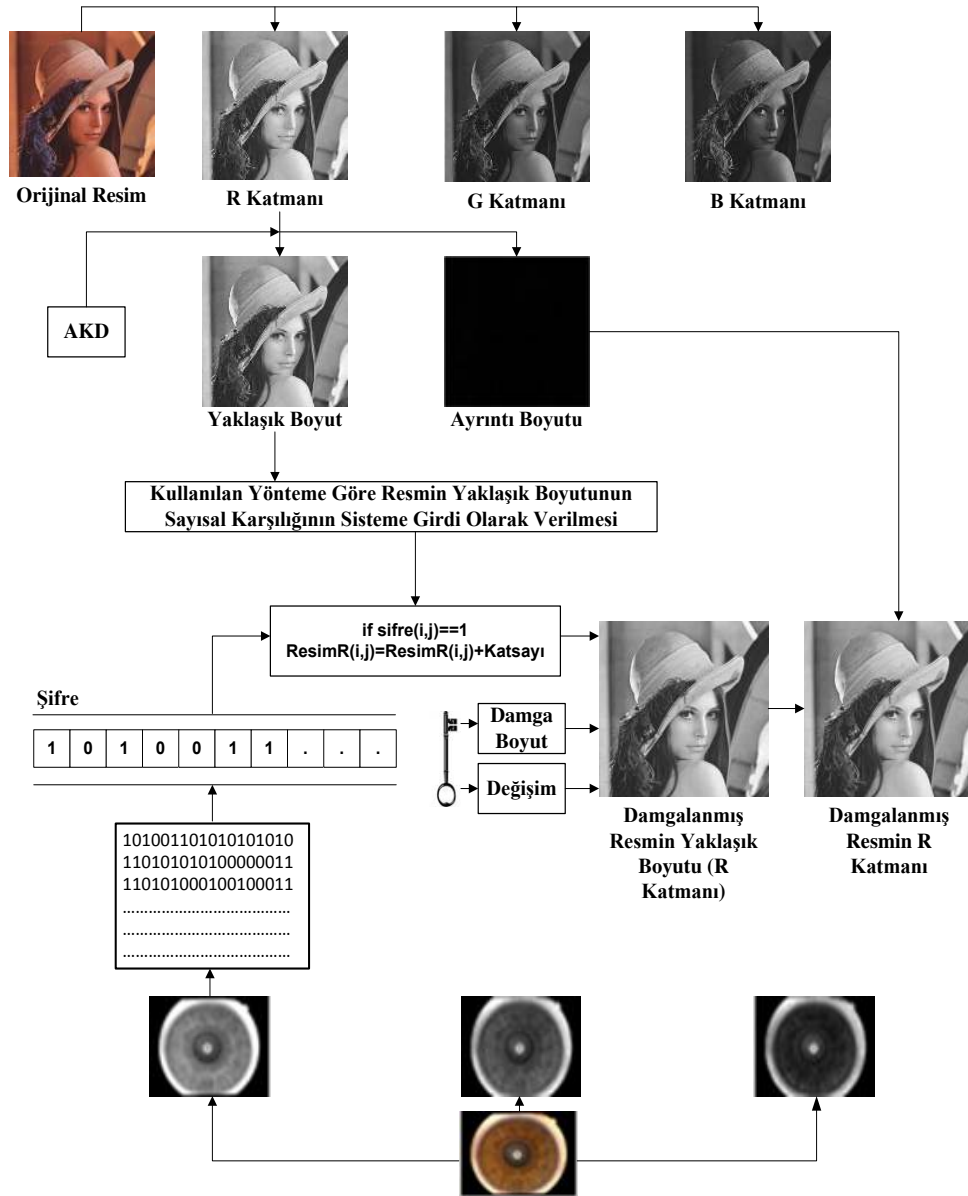
7.1. AKD ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması

Geliştirilen yöntem ve AKD tabanlı sistemde Şekil 7.6.'da gösterildiği gibi iris resminin orijinal resme damgalanması işleminde:

1. Orijinal resmin AKD'si alınarak yaklaşık boyutu elde edilir.
2. Damga olarak belirlenen resim alınıp ikilik kodlara çevrildikten sonra Şifre adındaki matrise atanır.
3. Şifrenin boyutu ilk anahtar olarak kaydedilir.
4. Şifrenin tüm elemanları resimdeki şifre boyutu kadar taranır.
5. Şifrenin kontrol edilen indisi değeri 1 ise, resmin aynı indisli elemanı sistemin belirleyeceği katsayı ile artırılır.
6. Damga eklenmiş yaklaşık boyut ile orijinal resmin ayrıntı boyutu birleştirilir.
7. Orijinal resim ile damgalanmış resmin bit düzeyinde değişimi yüzde olarak hesaplanır. İkinci anahtar olarak kaydedilir.

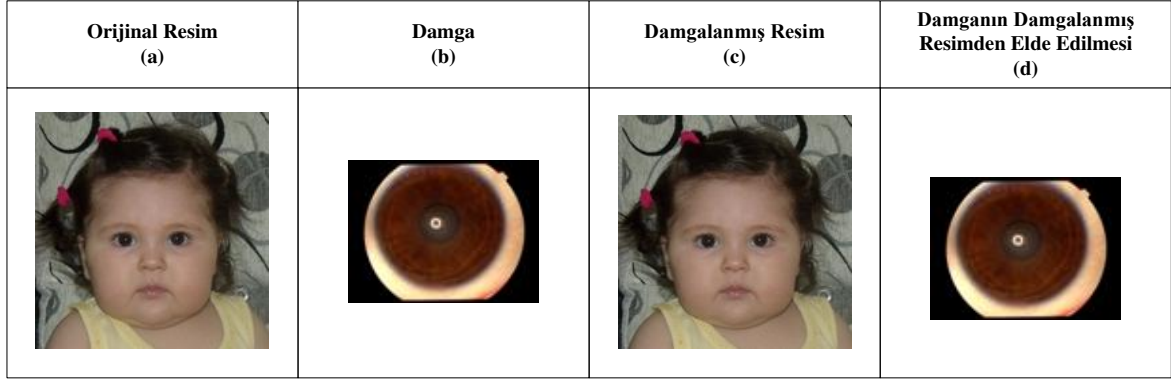
Damganın damgalanmış resimden elde edilmesi işlemi Şekil 7.2. ile aynı yapıdadır. Damganın çıkarılması işleminde:

1. Anahtarlar tespit edilir.
2. Damgalanmış resim ve orijinal resmin değişim oranı tespit edilir. İkinci anahtar değerle değişim oranı uyuşmaz ise damgalanmış resim yeniden istenir.
3. İlk anahtar değere göre şifre adlı bir boş matris oluşturulur.
4. AKD ile orijinal resim ve damgalanmış resmin yaklaşık boyutu elde edilir.
5. Yaklaşık boyut anahtardaki boyut kadar taranır ve karşılaştırılır.
6. Farklı olan indisler için boş matrise 1 aynı olan bitler için 0 atanır.
7. Şifre adlı matris görüntü formatına dönüştürülür.



Şekil 7.6. AKD ve geliştirilen yöntem ile sistemin blok diyagramı

Sistemde verilen örnek resim için hesaplanan PSNR değeri 43.7426, BER değeri 0.0028, hesaplama süresi 23.126346 sn ve NC oranı 1 olarak hesaplanmıştır. AKD ve geliştirilen sistemden elde edilen damgalanmış resim Şekil 7.7. (c)'de, damga ise Şekil 7.7. (d)'de verilmiştir.



Şekil 7.7. AKD ve geliştirilen yöntem ile sistemden elde edilen sonuçlar

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 7.3.'de verilmiştir.

Tablo 7.3. AKD ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları

Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	44.6784	1	0.0025	21.924404

Damgalanmış resme uygulanan keskinleştirme, bulanıklaştırma ve döndürme saldırıları sonrası elde edilen damganın NC oranları Tablo 7.4.'de gösterilmiştir.

Tablo 7.4. Damganın AKD ve geliştirilen yöntem ile saldırılara dayanıklılığı

Saldırı	Ortalama NC
Yok	1
Keskinleştirme (1 kez)	0.8509
Bulanıklaştırma (20 %)	0.7324
Döndürme (1°)	0.6786

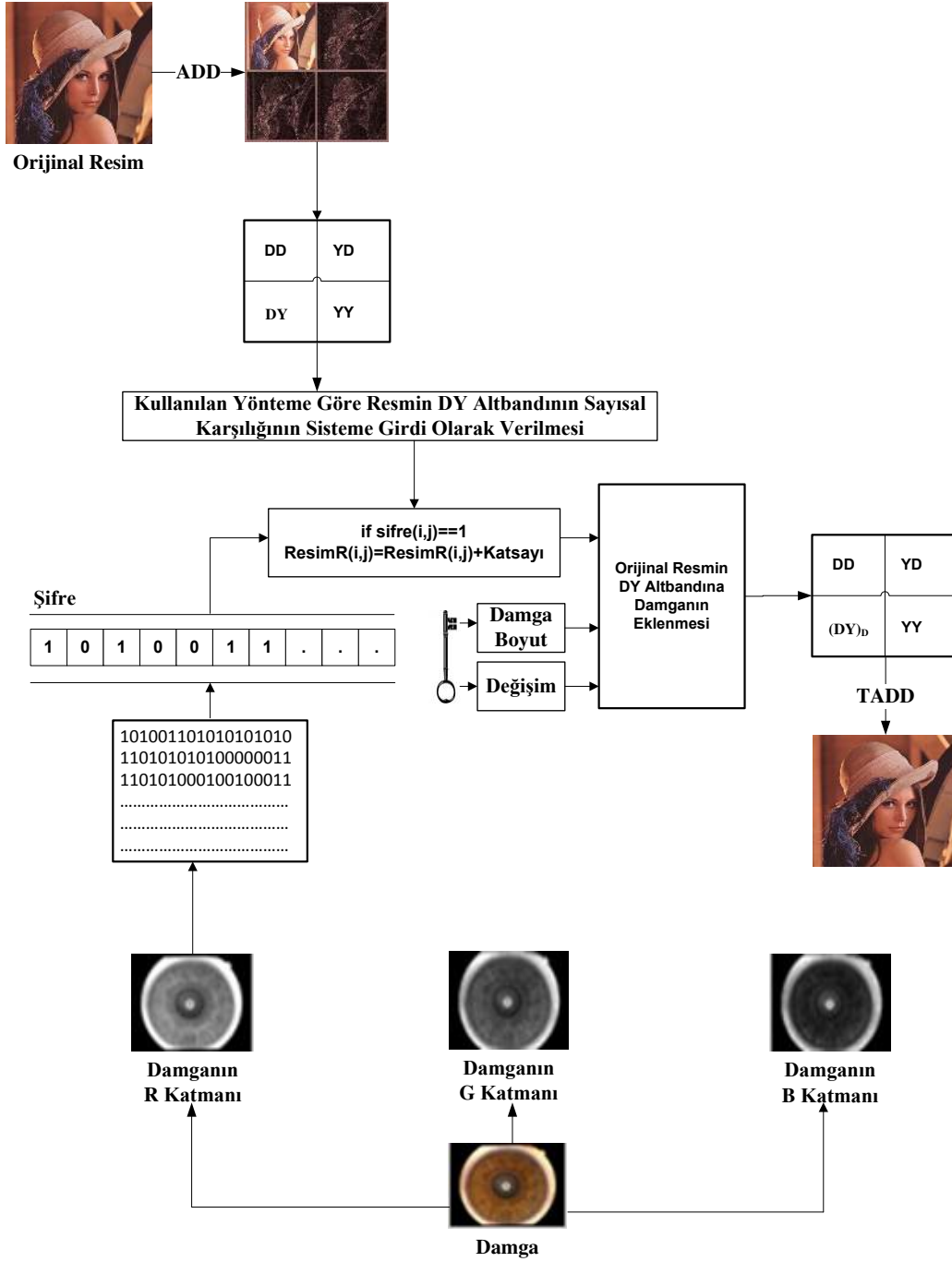
7.2. ADD ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması

Geliştirilen yöntem ve ADD tabanlı sistemde Şekil 7.8.'de gösterildiği gibi iris resminin orijinal resme damgalanması işleminde

1. Orijinal resmin ADD alınarak DY alt bandı elde edilir.
2. Damga olarak belirlenen resim alınıp ikilik kodlara çevrildikten sonra Şifre adındaki matrise atanır.
3. Şifrenin boyutu ilk anahtar olarak kaydedilir.
4. Şifrenin tüm elemanları resimdeki şifre boyutu kadar taranır.
5. Şifrenin kontrol edilen indisi değeri 1 ise, resmin aynı indisli elemanı sistemin belirleyeceği katsayı ile artırılır.
6. Damga eklenmiş DY alt bandı orijinal resmin diğer alt bantları ile TADD ile birleştirilir.
7. Orijinal resim ile damgalanmış resmin bit düzeyinde değişimi yüzde olarak hesaplanır. İkinci anahtar olarak kaydedilir.

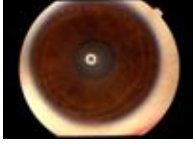
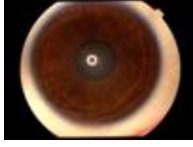
Damganın damgalanmış resimden elde edilmesi işlemi Şekil 7.2. ile aynı yapıdadır. Damganın çıkarılması işleminde

1. Anahtarlar tespit edilir.
2. Damgalanmış resim ve orijinal resmin değişim oranı tespit edilir. İkinci anahtar değerle değişim oranı uyumsuz ise damgalanmış resim yeniden istenir.
3. İlk anahtar değere göre şifre adlı bir boş matris oluşturulur.
4. Orijinal resim ile damgalanmış resmin ADD ile DY alt bandı elde edilir.
5. DY alt bantları anahtardaki boyut kadar taranır ve karşılaştırılır.
6. Farklı olan indisler için boş matrise 1 aynı olan bitler için 0 atanır.
7. Şifre adlı matris görüntü formatına dönüştürülür.



Şekil 7.8. ADD ve geliştirilen yöntem ile sisteminin blok diyagramı

Sistemde verilen örnek resim için hesaplanan PSNR değeri 46.1693, BER değeri 0.0192, hesaplama süresi 46.264817 sn ve NC oranı 1 olarak hesaplanmıştır. ADD ve geliştirilen sistemden elde edilen damgalanmış resim Şekil 7.9. (c)'de, damga ise Şekil 7.9. (d)'de verilmiştir.

Orjinal Resim (a)	Damga (b)	Damgalanmış Resim (c)	Damganın Damgalanmış Resimden Elde Edilmesi (d)
			

Şekil 7.9. ADD ve geliştirilen yöntem ile sistemden elde edilen sonuçlar

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 7.5.'de verilmiştir.

Tablo 7.5. ADD ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları

Birey Sayısı	Orjinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	45.8809	1	0.0195	47.512490

Damgalanmış resme uygulanan keskinleştirme, bulanıklaştırma ve döndürme saldırıları sonrası elde edilen damganın NC oranları Tablo 7.6.'de gösterilmiştir.

Tablo 7.6. Damganın ADD ve geliştirilen yöntem ile saldırılara dayanıklılığı

Saldırı	Ortalama NC
Yok	1
Keskinleştirme (1 kez)	0.8551
Bulanıklaştırma (20 %)	0.7395
Döndürme (1°)	0.6847

7.3. TDA ve Geliştirilen Yöntem Tabanlı Sayısal Damgalama Uygulaması

Geliştirilen yöntem ve TDA tabanlı sistemde Şekil 7.10.'da gösterildiği gibi iris resminin orijinal resme damgalanması işleminde

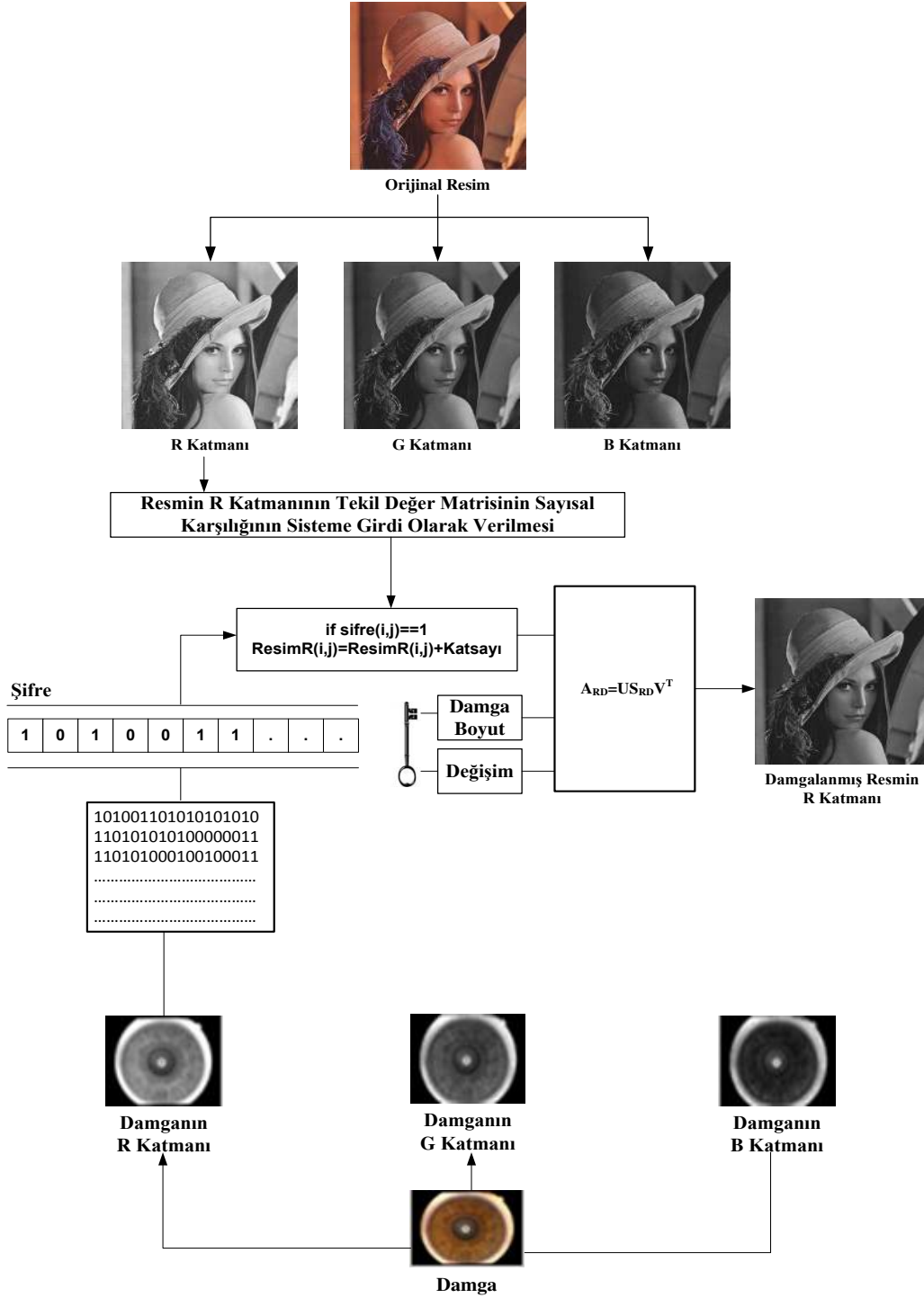
1. Orijinal resmin TDA alınarak tekil değer matrisi elde edilir.

2. Damga olarak belirlenen resim alınıp ikilik kodlara çevrildikten sonra Şifre adındaki matrise atanır.
3. Şifrenin boyutu ilk anahtar olarak kaydedilir.
4. Şifrenin tüm elemanları resimdeki şifre boyutu kadar taranır.
5. Şifrenin kontrol edilen indisi değeri 1 ise, resmin aynı indisli elemanı sistemin belirleyeceği katsayı ile artırılır.
6. Damga eklenmiş tekil değer matrisi orijinal resmin diğer iki matrisi ile birleştirilir.
7. Orijinal resim ile damgalanmış resmin bit düzeyinde değişimi yüzde olarak hesaplanır. İkinci anahtar olarak kaydedilir.

Damganın damgalanmış resimden elde edilmesi işlemi Şekil 7.2. ile aynı yapıdadır.

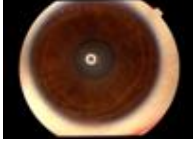
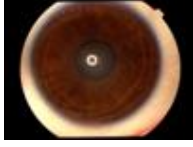
Damganın çıkarılması işleminde

1. Anahtarlar tespit edilir.
2. Damgalanmış resim ve orijinal resmin değişim oranı tespit edilir. İkinci anahtar değerle değişim oranı uyumsuz ise damgalanmış resim yeniden istenir.
3. İlk anahtar değere göre şifre adlı bir boş matris oluşturulur.
4. Orijinal resim ile damgalanmış resmin TDA ile tekil değerleri elde edilir.
5. Tekil değer matrisleri anahtardaki boyut kadar taranır ve karşılaştırılır.
6. Farklı olan indisler için boş matrise 1 aynı olan bitler için 0 atanır.
7. Şifre adlı matris görüntü formatına dönüştürülür.



Şekil 7.10. TDA ve geliştirilen yöntem ile sisteminin blok diyagramı

Sistemde verilen örnek resim için hesaplanan PSNR değeri 46.5013, BER değeri 0.0021, hesaplama süresi 43.596274 sn ve NC oranı 1 olarak hesaplanmıştır. TDA ve geliştirilen sistemden elde edilen damgalanmış resim Şekil 7.11. (c)'de, damga ise Şekil 7.11. (d)'de verilmiştir.

Orijinal Resim (a)	Damga (b)	Damgalanmış Resim (c)	Damganın Damgalanmış Resimden Elde Edilmesi (d)
			

Şekil 7.11. TDA ve geliştirilen yöntem ile sistemden elde edilen sonuçlar

Sistemde 20 birey için hesaplanan PSNR, BER, NC ve sistemin toplam hesaplama süresi ortalamaları Tablo 7.7.'de verilmiştir.

Tablo 7.7. TDA ve geliştirilen yöntem ile elde edilen PSNR, NC, BER ve hesaplama süresi sonuçları

Birey Sayısı	Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	NC	BER	Hesaplama Süresi (saniye)
20	Yüz Resmi + İris	46.3054	1	0.0017	42.132521

Damgalanmış resme uygulanan keskinleştirme, bulanıklaştırma ve döndürme saldırıları sonrası elde edilen damganın NC oranları Tablo 7.8.'de gösterilmiştir.

Tablo 7.8. Damganın TDA ve geliştirilen yöntem ile saldırılara dayanıklılığı

Saldırı	Ortalama NC
Yok	1
Keskinleştirme (1 kez)	0.8674
Bulanıklaştırma (20 %)	0.7552
Döndürme (1°)	0.6897

8. SONUÇLAR VE DEĞERLENDİRME

Bu tez çalışmasında biyometrik sistemlerin güvenliğini artırılması için yeni bir damgalama yöntemi önerilmiştir. Geliştirilen sistemde biyometrik verilerden renkli 20 yüz resmi (10 erkek ve 10 bayan), damga olarak ise renkli 20 iris resmi kullanılmış ve geliştirilen yöntem ile ADD, AKD ve TDA yöntemlerinin başarımları düzeyleri karşılaştırılmıştır. Ayrıca geliştirilen yöntemin ADD, AKD ve TDA ile birlikte kullanılabileceği de gösterilmiş ve buna ilişkin başarımları düzeyleri de incelenmiştir.

Günümüzde gelişen teknoloji paralelinde biyometrik sistemlerin güvenliğini artırılması için yapılan çalışmalar artmaktadır. Başlangıçta biyometrik sistem denilince akla parmak izi tanıma sistemleri gelmekteydi. Fakat parmak izi tanıma sistemlerinin kolay aşılabilen güvenlik sınırları nedeniyle kişiye ait başka biyometrik veriler (iris, yüz, el geometrisi, ses tanıma v.b.) kullanılarak yeni sistemler geliştirilmiştir. Bu tür biyometrik sistemler tekli model biyometrik sistemler olarak adlandırılmaktadır. Bu biyometrik sistemlerin ya bir güvenlik açığının mevcut olması ya da yüksek maliyetleri nedeniyle birden fazla biyometrik özellik birleştirilerek tekli model biyometrik sistemlerden çoklu model biyometrik sistemlere geçiş sağlanmıştır. Çoklu model biyometrik sistemler kullanılan alana uygun olarak kişinin birden fazla biyometrik özelliğini kontrol eder. Böylelikle yüksek güvenlik düzeyinin sağlanması gereken uygulamalarda çoklu model biyometrik sistemler kullanılmaktadır.

Bir biyometrik sistem tasarımında başlangıçta her bir kişiye ait veriler bir veritabanında toplanarak sisteme erişim hakkı tanınır. Daha sonra sistemin uygulanması aşamasında sisteme giriş yapmaya çalışan kişilerin biyometrik örnekleri alınarak önceden oluşturulan veritabanı ile karşılaştırılıp kişiye erişim izni verilir ya da verilmez. Damgalama uygulamalarında biyometrik sistemlerden elde edilen veriler yoğunlukla kullanılmaktadır. Çünkü biyometrik sistemlerde de damgalama uygulamalarında da esas amaç sahiplik faktörünün belirlenmesidir. Örtüşen bu faktörler nedeni ile damgalama uygulamaları biyometrik alanda geniş kullanım alanına sahiptir.

Damgalama uygulamalarında, damgalanan verinin sistemin hedefine uygun olarak muhafaza edilmesinin sağlanması ve iletiminin başarıyla gerçekleştirilmesi temel amaç olarak nitelendirilebilir. Ayrıca tüm bu işlemler yapılırken haberleşme sistemlerinde iletilecek olan verinin sistemin bant genişliğini en verimli şekilde kullanması damgalama yöntemleri için önemli bir ayırt edici faktördür.

Damgalama yöntemleri üzerine yapılmış çalışmaların büyük bir kısmını görünmez damgalama uygulamaları kapsamaktadır. Orijinal verinin içine damga eklenmesi ile verideki bozulmaların minimuma indirgenmesi ve damgalanmış verinin saldırılara karşı direncinin artırılması amacıyla görünmez damgalama üzerine her geçen gün yeni algoritmalar geliştirilmekte ve önerilmektedir. Bir damgalama sisteminin değerlendirilmesinde göz önünde tutulan etmenler damgalanmış verinin orijinal veriyi ne kadar değiştirdiği, orijinal verinin saklayabileceği bilgi miktarı ve damga saldırılarına karşı ne kadar dayanıklı olduğunun incelenmesidir. Bu anlamda bir damgalama sistemlerinin başarımını ölçmek için PSNR, MSE, NC, BER, Histogram eğrileri gibi ölçütler kullanılmaktadır.

PSNR değeri desibel olarak ölçülür ve literatürde yaygın olarak kullanılır. Bu değer orijinal resim ile damgalanmış resim arasındaki kalite farkını tespit etmek için kullanılır ve ne kadar büyük olursa damgalanmış resmin kalitesinin bozulma oranı o kadar az olur.

Damgalanmış resim ile orijinal resim veya damgalanmış resimden çıkarılan damga ile orijinal damga arasındaki benzerliği belirlemek için NC kullanılır. NC değeri en fazla 1 olabilir. NC değeri 1'e yaklaştıkça orijinal resim ile damgalanmış resim veya orijinal damga ile damgalanmış resimden çıkarılan damga o oranda benzer kabul edilir.

Bir resimdeki renk değerlerinin sayısını gösteren grafiğe histogram denir. Bir resmin histogram eğrisi o resmin kontrast düzeyi veya tonları hakkında bilgi edinilmesini sağlar.

Damgalama yöntemlerde orijinal resim ile damgalanmış resim arasındaki değişen bit sayısının toplam bit sayısına oranı BER olarak ifade edilir. BER değeri 0'a ne kadar yakınsa damgalama sisteminde damgalanmış resmin aslına o kadar yakın olduğu söylenebilir.

Yukarıda bahsedilen başarımların ölçütlerinin istenilen seviyede olması için farklı damgalama yöntemleri mevcuttur. Bu yöntemler uzay ve dönüşüm bölgesinde damgalama olmak üzere ikiye ayrılır. Uzay bölgesinde yapılan damgalama uygulamaları EÖB tekniği tabanlıdır. Dönüşüm bölgesinde ise ADD, AKD, TDA gibi yöntemler kullanılmaktadır. Bu yöntemler birbirleriyle ilişkili olarak kullanılabilirler. Örneğin ADD ile bir resmin elde edilen 4 alt bandından hangi bandına ya da bantlarına damga eklenecekse EÖB yöntemi yardımı ile damga ekleme işlemi yapılabilir. EÖB yöntemi ile damgalama da gizlenecek veri miktarı sınırlıdır ve saldırılara karşı hassastır. Yukarıda bahsedildiği gibi EÖB yönteminin diğer yöntemler ile kaynaştırılması sonucu EÖB yönteminin bu dezavantajlarının giderilmesi amaçlanmıştır.

Bu tez kapsamında, uzay ve dönüşüm bölgesinde kullanılabilecek, mevcut yöntemlerin başarımlarını artıracak bir damgalama yöntemi önerilmiştir. ADD, AKD ve TDA metotları kullanılarak elde edilen sonuçlar, önerilen yöntemin sonuçları ile PSNR, NC Histogram Eğrileri ve BER değerleri referans alınarak kıyaslanmıştır. Bölüm 6. ve 7.'de tablolar halinde verilen sonuçların ortalamaları Tablo 8.1.'de verilmiştir.

Tablo 8.1. Renkli iris ve yüz resimleri için elde edilen PSNR, BER ve hesaplama süresi ortalama değerleri

Orijinal Resim (896x592) Gizlenecek Resim (50x38)	PSNR	BER	NC	Hesaplama Süresi (sn)
ADD	42.8140	0.0257	1	52.729798
AKD	40.1649	0.0145	1	24.143840
TDA	42.0421	0.0451	1	47.757082
Geliştirilen Yöntem (GY)	51.5839	0.0024	1	21.638468
ADD ve GY	45.8809	0.0195	1	47.512490
AKD ve GY	44.6784	0.0025	1	21.924404
TDA ve GY	46.3054	0.0017	1	42.132521

Tablo 8.1.'de verilen sonuçlar irdelendiğinde

- Geliştirilen yöntemin literatüre kattığı en büyük avantaj, tez kapsamında uygulanan yöntemlerden farklı olarak damgalanmış resim ile orijinal resim arasındaki PSNR oranının daha yüksek elde edilmesidir. Ancak ADD, AKD, TDA gibi yöntemler ile bir arada kullanılmaz ise saldırılara karşı bu yöntemlere nazaran daha az dayanıklıdır.
- Damga gizleme işleminde ADD, AKD veya TDA yöntemleri ve geliştirilen yöntem bir arada kullanılırsa daha yüksek PSNR değerlerine ulaşılmaktadır. Buda geliştirilen yöntemin literatürde yaygın olarak kullanılan yöntemlerle (ADD, AKD, TDA, AFD vb.) bir arada kullanılabileceğini ve ayrıca ortak kullanım sonucu sistemlerin başarımlarını artırdığını göstermektedir. Böylelikle damgalama sistemlerinde kullanılan yöntemlerin avantajları tespit edilerek önerilen yöntem ile birleştirilip, başarı ve güvenlik düzeyi daha yüksek sistemler geliştirilebilir.
- Sistemde orijinal resim ve damgalanmış resim çeşitli saldırılara (keskinleştirme, bulanıklaştırma ve döndürme) maruz bırakılmış ve damgalanmış resimden elde

edilen damganın NC değeri kontrol edilmiştir. Elde edilen sonuçlar dikkate alındığında geliştirilen yöntem diğer yöntemler ile bir arada kullanılırsa saldırılara karşı dayanıklı olduğu gözlemlenmiştir.

- Geliştirilen yöntemde renkli biyometrik resimler kullanılmıştır. Böylelikle resmin 3 katmanına (R, G ve B) damga gizlenmiş ve gri seviye yani tek katmanlı resimlerdeki damga ekleme uygulamalarına göre veri gizleme kapasitesinin yüksek olması sağlanmıştır.
- Geliştirilen yöntem ve bu yöntemin diğer yöntemler ile beraber kullanılmasıyla, daha düşük BER değerleri elde edilmiştir. Böylelikle geliştirilen yöntemin damga ekleme işleminde bit değişimini azalttığı sonucuna varılabilir.
- Bölüm 6 ve 7.'de verilen histogram eğrileri yakından incelendiğinde resmin renk değerleri hakkında önemli bilgiler içermektedir. Tezde incelenen yöntemlerle geliştirilen yöntemin histogram eğrileri kıyaslandığında birbirine paralel sonuçlar elde edilmiştir.
- Bütün çalışmalar Intel(R) Core (TM)2 Duo CPU P8800 @2.66 Ghz işlemcili, 3.00 GB RAM ve Windows Vista 32 bit işletim sistemli bir bilgisayarla yapılmıştır. Hesaplama süresi dikkate alındığında en iyi sonuca geliştirilen yöntemle ulaşılmıştır.
- Önerilen yöntem damgalanmış resimden damganın yeniden elde edilebilmesi için orijinal resme ihtiyaç duyduğundan geliştirilen damgalama algoritması kör olmayan damgalama yöntemi olarak nitelendirilebilir. Böylelikle alıcı ve gönderici taraf orijinal veriye sahip olmazsa damgalanmış veriden damganın aslına uygun olarak elde edilmesi zorlaşmaktadır.

Bu tez çalışmasında geliştirilen yöntem ile renkli iris resmi, renkli yüz resmi içerisine damgalanmıştır. Bundan sonraki çalışmalarda çoklu model biyometrik sistemlerin amacına uygun olarak birden fazla biyometrik özellik kullanılarak sistem genişletilebilir. Örneğin geliştirilen sistem ile parmak izi resmi, iris resmi içine gömüldükten sonra damgalanmış iris resmi ise yüz resmi içerisine eklenerek biyometrik sistemlerde kullanılabilir. Böylelikle biyometrik özellikler artırılarak kullanım amacına göre sistemin güvenlik düzeyi ve başarımı artırılabilir. Ayrıca literatürde damgalama sistemleri üzerine yapılan çalışmalar damgalanmış nesnenin ve damganın varlığını koruyucu, değişimini engelleyici ve bütünlüğünü muhafaza etmeye yönelik olarak yapılmaktadır. Bu amaçlar doğrultusunda pek çok yöntem kullanılmakta (ADD, AFD, AKD, TDA, EÖB v.b.) ve bunlarla beraber

her geen gn yeni yaklařımlar nerilmektedir. Tm bu yntemler kullanım amacı ve kullanım yerine gre farklı stn zelliklere sahip olmakla beraber bařarım oranı akıllı optimizasyon teknikleri ile glendirilebilmektedir. Bu nedenle damgalama uygulamalarında var olan yntemler iin “en iyi sonucu verir” yada “daha stndr” gibi bir genelleme yapılamamaktadır. Bir damgalama sisteminde bařarımını artırmak iin hedef belirlendikten sonra, var olan yntemler bir arada kullanılabileceėi gibi var olan yntemlerden elde edilen zellikler yeni yaklařımlarla glendirilebilmektedir. Tm bu anlatılanlardan yola ıkarak geliřtirilen damgalama sisteminin eldeki bulgularda bařarılı sonular verdiėi grlmekte, var olan damgalama yntemleri ve akıllı optimizasyon teknikleri ile glendirilerek daha bařarılı sonulara ulařılabileceėini de gstermektedir.

KAYNAKLAR

- [1] **Kim, W., Lee, H.**, 2009. Multimodal Biometric Image Watermarking using Two-Stage Integrity Verification, *Signal Processing*, **89 (12)**, 2385–2399.
- [2] **Jain, A. K., Uludag, U., Hsu, R.**, 2002. Hiding a Face in a Fingerprint Image, *Pattern Recognition*, **3**, 52–54.
- [3] **Jain, A. K., Uludag, U.**, 2003. Hiding Biometric Data, *IEEE Transactions on. Pattern Recognition and Machine Intelligence*, **25(11)**, 1494–1498.
- [4] **Wang, F.H., Jain, L.C., Pan, J.S.**, 2002. Genetic Watermarking Techniques Based on Spatial Data, *Proceedings of the Sixth International Conference on Knowledge-Based Intelligent Information Systems*, Milano, Italy, IOS Press, 417-421
- [5] **Fan, A., Sun, Q.**, 2008. Simultaneous Calculation of DFT and IDFT of Real Two-Dimensional Sequences and Its Application in Digital Image Watermark, *Congress on Image and Signal Processing, CISP '08*, **5**, 730–733.
- [6] **Kang, X., Huang, J., Shi, Y. Q., Lin, Y.**, 2003. A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression, *Circuits and Systems for Video Technology, IEEE Transactions on*, **13 (8)**, 776-786.
- [7] **Kundur, D., Hatzinakos, D.**, 1997. A Robust Digital Image Watermarking Scheme using Wavelet-Based Fusion, *Proc. ICIP 97, IEEE Int. Conf. Image Processing*, Santa Barbara, CA, 544-547.
- [8] **Wang, X., Qi, W., Niu, P.**, 2007. A New Adaptive Digital Audio Watermarking Based on Support Vector Regression, *Audio, Speech and Language Processing, IEEE Transactions on*, **15 (8)**, 2270-2277.
- [9] **Chang, C.C., Chang, Y.C., Shen, J.J.**, 2006. A Heuristic Method for Extracting Enhanced Watermarks from Digital Images, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IHH-MSP '06*, 453-456.
- [10] **Barni, M., Bartolini, F., Cappellini, V., Piva, A.**, 1998. A DCT-Domain System for Robust Image Watermarking, *Signal Processing*, **66 (3)**, 357-372.
- [11] **Choi, H.-J., Seo, Y.-H., Yoo, J.-S., Kim, D.-W.**, 2008. Digital Watermarking Technique for Holography Interference Patterns in a Transform Domain, *Optics and Lasers in Engineering*, **46 (4)**, 343-348.

- [12] **Aslantaş, V., Ozer, S., Ozturk, S.,** 2009. Improving the Performance of DCT-Based Fragile Watermarking using Intelligent Optimization Algorithms, *Optics Communications*, **282 (14)**, 2806-2817.
- [13] **Huang, F., Guan, Z.-H.,** 2004. A Hybrid SVD-DCT Watermarking Method based on LPSNR, *Pattern Recognition Letters*, **25 (15)**, 1769-1775.
- [14] **Bhatnagar, G., Raman, B.,** 2009. A New Robust Reference Watermarking Scheme based on DWT-SVD, *Computer Standards & Interfaces*, **31 (5)**, 1002-1013.
- [15] **Tsai, P., Hu, Y.-C., Chang, C.-C.,** 2004. A Color Image Watermarking Scheme based on Color Quantization, *Signal Processing*, **84 (1)**, 95-106.
- [16] **Voloshynovskiy, S., Pereira, S., Iquise, V., Pun, T.,** 2001. Attack Modelling: Towards A Second Generation Watermarking Benchmark, *Signal Processing*, **81 (6)**, 1177-1214.
- [17] **Chang, C.-C., Tsai, P., Lin, C.-C.,** 2005. SVD-Based Digital Image Watermarking Scheme, *Pattern Recognition Letters*, **26 (10)**, 1577-1586.
- [18] **El-Abed, M., Giot, R., Hemery, B., Rosenberger, C.,** 2010. A Study of Users' Acceptance and Satisfaction of Biometric Systems, *Security Technology (ICCST), 2010 IEEE International Carnahan Conference on*, 170-178.
- [19] **Bilgin, M.,** 2008. Biyometrik Seçim Sistemi Tasarımı ve Gerçekleştirilmesi, Yüksek Lisans Tezi, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Konya.
- [20] **El Saddik, A., Orozco, M., Asfaw, Y., Shirmohammadi, S., Adler, A.,** 2007. A Novel Biometric System for Identification and Verification of Haptic Users, *Instrumentation and Measurement, IEEE Transactions on*, **56 (3)**, 895-906.
- [21] **Conti, V., Militello, C., Sorbello, F., Vitabile, S.,** 2010. A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems, *IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications And Reviews*, **40 (4)**, 384-395.
- [22] **Marsico, M., D., Nappi, M., Riccio, D., Tortora, G.,** 2009. A Multiexpert Collaborative Biometric System for People Identification, *Journal of Visual Languages and Computing*, **20**, 91–100.
- [23] **Eren, B.,** 2009. Biyometrik Teknolojilerin Etkili Tasarlanması ve Uygulanmasında Yeni Bir Öneri: Multimodel Teknoloji, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstanbul.

- [24] **Çelebi Taşyapı, A.**, 2008. Biyometrik Tanıma, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, Kocaeli.
- [25] **Önen Yıldız, H., G.**, 2010. Avuçiçi Esaslı Biyometrik Kimlik Tanımlama ve Doğrulama, Yüksek Lisans Tezi, Fen Bilimleri Enstitüsü, İstanbul.
- [26] **Doroteo T. Toledano, D., T., Pozo, R., F., Trapote, A., H., Go'mez, L., H.**, 2006. Usability Evaluation of Multi-Modal Biometric Verification Systems, *Interacting with Computers*, **18**, 1101-1122.
- [27] **Kumar, P., Mittal, A., Kumar P.**, 2010. Addressing Uncertainty in Multi-Modal Fusion for Improved Object Detection in Dynamic Environment, *Information Fusion*, **11 (4)**, 311-324.
- [28] **Roberts, C.**, 2007. Biometric Attack Vectors and Defences, *Computers & Security*, **26 (1)**, 14-25.
- [29] **Ross, A., Jain, A.K.**, 2003. Information Fusion in Biometrics, *Pattern Recognition Letters*, **24-13**, 2115-2125.
- [30] **Cummins, H., Mildo, C.**, 1961. Finger Prints, Palm and Soles, Dover Publication Inc., New York.
- [31] **Galton, F.**, 1961. Finger Prints, Da Capo Pres, New York.
- [32] **Chang, J., H., Fan, K., C.**, 2002. A New Model for Fingerprint Classification by Ridge Distribution Sequences, *Pattern Recognition*, **35 (6)**, 1209-1223.
- [33] http://www.talhabilgisayar.net/parmak_izi_sistemleri.asp, Güvenlik ve Alarm Sistemleri, 19.05.2011.
- [34] <http://www.artelektronik.com/parmak-izi.html>, Parmaz İzi Tanıma Sistemleri, 19.05.2011 .
- [35] <http://parmakizi-okuyucu.blogspot.com/2011/02/parmak-izi-nedir.html>, Parmak İzi Okuyucuları, 19.05.2011.
- [36] <http://www.ahmetkakici.com/genel/biyometrik-tanima-sistemleri/> 16.05.2011.
- [37] **Yang, J., Liu, L., Jiang, T., Fan, Y.**, 2003. A Modified Gabor Filter Design Method for Fingerprint Image Enhancement, *Pattern Recognition Letters*, **24 (12)**, 1805-1817.
- [38] **Chellappa,R., Wilcon, C., Sirohey,A.**, 1995. Human And Machine Recognition Of Faces:A Survey, *Proceedings of the IEEE*, **83 (5)**, 705-740.

- [39] **Adler, A., Schuckers, M.E.**, 2007. Comparing Human and Automatic Face Recognition Performance, Systems, *Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, **37 (5)**, 1248-1255.
- [40] **Turk, M.A., Pentland, A.P.**, 1991. Face Recognition using Eigenfaces, *Computer Vision and Pattern Recognition*, Proceedings CVPR '91., IEEE Computer Society Conference on, 586-591.
- [41] **Newhan, E.**, 1995. The Biometric Report, SJB Services, New York.
- [42] **Daugman, J.G.**, 1993. High Confidence Visual Recognition Of Persons By A Test Of Statistical Independence, *IEEE Trans.Pattern Analysis and Machine Intell.*, **15 (9)**, 1148-1161.
- [43] **Abhyankar, A., Schuckers, S.**, 2010. A Novel Biorthogonal Wavelet Network System for Off-Angle Iris Recognition, *Pattern Recognition*, **43 (3)**, 987-1007.
- [44] <http://phoenix.inf.upol.cz/iris/download/>, 03.02.2010.
- [45] **Polat, Ö., Yıldırım, T.**, 2008. Hand Geometry Identification without Feature Extraction by General Regression Neural Network, *Expert Systems with Applications*, **34 (2)**, 845-849.
- [46] <http://www.egmguvenlik.net/page/11>, EGM Güvenlik, 19.05.2011.
- [47] <http://www.aktuelgazete.com/haber/ve-bir-devrim-gerceklesti-kok-hucrenden-retina-elde-edildi-1342.html>, Aktuel Gazete, 19.05.2011.
- [48] <http://webvision.med.utah.edu/book/part-i-foundations/simple-anatomy-of-the-retina/>, 19.05.2011.
- [49] **Campbell, Jr. J.**, 1997, Speaker Recognition A Tutorial, *Proceedings Of IEEE*, **85 (9)**, 1437-1462.
- [50] **Jain, A.K., Ross, A., Prabhakar, S.**, 2004. An Introduction to Biometric Recognition, 14 (1), 4-20.
- [51] <http://turuncukafa.blogcu.com/>, 19.05.2011.
- [52] **Prabhakar, S., Pankanti, S., Jain, A. K.**, 2003. Biometric Recognition: Security and Privacy Concerns, *IEEE Security Privacy Mag.*, **1 (2)**, 33-42.
- [53] **Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G.**, 1999. Information Hiding: A Survey, *Proceedings of the IEEE*, **87 (7)**, 1062-1078
- [54] **Mohanty, S. P.**, 1999. Digital Watermarking: A Tutorial Review, Indian Institute of Science, Bangalore, India

- [55] **Chen, P.C.**, 1999. On The Study of Watermarking Application in WWW – Modeling, Performance Analysis and Application of Digital Image Watermarking Systems, Master Thesis, National Tsing Hua University, Hsinchu, Taiwan.
- [56] **Johnson, N. F., Jajoda, S.**, 1998. Exploring Steganography: Seeing the Unseen, *IEEE Computing Practices*, **2**, 26-34.
- [57] **Katzenbiesser, S. and Petitcolas, F.**, 2000. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, 237, London.
- [58] **Arnold, M., Schmucker, M., Wolthusen, S. D.**, 2003. Techniques and Applications of Digital Watermarking and Content Protection, Artech House, 273, London.
- [59] **Hamza, Y. A.**, 2008. Blok Kırpma Kodlamasına ve Ayrık Dalgacık Dönüşümüne Dayalı Dijital Renkli Resim Damgalama Sistemi, Yüksek Lisans Tezi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Eskişehir.
- [60] **Furat, M.**, 2006. Sayısal Ortamlarda Veri Damgalanması ve Geri Eldesi, Yüksek Lisans Tezi, Mustafa Kemal Üniversitesi, Fen Bilimleri Enstitüsü, Antakya.
- [61] **Elmas, A.**, 2006. Zaman-Frekans Yaklaşımı Kullanılarak Görüntü Damgalama, Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.
- [62] **Canbek, G., Sağiroğlu, S.**, 2006. Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri, Grafiker, Ankara, 1-50.
- [63] **Tuncer, T., Doğan, Ş., Avcı, E.**, 2011. A Steganography Application for Determination of Reliability against Visual Attacks of Hidden Data in Color Image, *IATS'11*, **3**, 32-36.
- [64] **Chou, J., Ramchandran, K., Ortega, A.**, 2001. High Capacity Audio Data Hiding for Noisy Channels. Information Technology: Coding and Computing, Proceedings. *International Conference*, Las Vegas, 108-112.
- [65] **Cvejic, N., Seppanen, T.**, 2002. Increasing The Capacity of LSB-Based Audio Steganography, *Multimedia Signal Processing*, 2002 IEEE Workshop , St. Thomas, Virgin Islands, USA, 336- 338.
- [66] **Şahin, A.**, 2007. Görüntü Steganografisinde Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.
- [67] **Bender W., Gruhl D., Morimoto N., Lu A.**, 1999. Techniques for Data Hiding, *IBM Systems Journal*, **35**, NOS 3&4.
- [68] **Biryukov A.**, 1999. Methods of Cryptanalysis, PHd Thesis.

- [69] **Chaum D.**, 1981. Untraceable Electronic Mail, Return DWTresses and Digital Pseudonyms, *Communications of the ACM*, **24 (2)**, 84-88.
- [70] **Şen,Ş.**, 2006. İndirgenmiş SPN(Substitution Permutatin Network) Algoritması için Lineer Kriptanaliz Uygulaması, Yüksek Lisans Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.
- [71] **Ülker,E. ve ark**, 2006. Selçuk Üniversitesinde Sayısal İmza Uygulaması, Ulusal Elektronik İmza Sempozyumu, 123 – 129.
- [72] **Chang T. Y.**, 2011. An ID-Based Multi-Signer Universal Designated Multi-Verifier Signature Scheme, *Information and Computation*, **209 (7)**, 1007-1015.
- [73] **Yılmaz, R.**, 2010. Kriptolojik Uygulamalarda Bazı İstatistik Testler, Yüksek Lisans Tezi, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Konya.
- [74] **Farid, H.**, 2001. Detecting Steganographic Message in Digital Images. Technical Report TR2001-412, Dartmouth College, 1-9.
- [75] **Fridrich, J., Goljan, M.**, 2002. Practical Steganalysis of Digital Images State of The Art. Proc. SPIE Photonics West, 4675:1–13.
- [76] **Akhaee, M. A., Kalantari, N. K., Marvasti F.**, 2010. Robust Audio and Speech Watermarking using Gaussian and Laplacian Modeling, *Signal Processing*, **90 (8)**, 2487-2497.
- [77] **Chamlawi, R., Khan, A.**, 2010. Digital Image Authentication and Recovery: Employing Integer Transform based Information Embedding and Extraction, *Information Sciences*, **180 (24)**, 4909-4928.
- [78] **Doğan, Ş., Tuncer, T., Avci, E., Gulten, A.**, 2011. A Robust Color Image Watermarking with Singular Value Decomposition Method, *Advances in Engineering Software*, **42(6)**, 336-346.
- [79] **Doğan, Ş., Tuncer, T., Avci, E., Gulten, A.**, 2011. A Watermarking Application for Color Image with Singular Value Decomposition Method, IATS'11, **3**, 27-31.
- [80] **Fridrich, J., Du, R., Long, M.**, 2000. Steganalysis of LSB Encoding in Color Images, Multimedia and Expo, ICME 2000. 2000 IEEE International Conference , New York, USA , **3**, 1279-1282.
- [81] **Fridrich, J.**, 2006. Minimizing The Embedding Impact in Steganography, Proceeding of the 8th Workshop on Multimedia and Security, Geneva- Switzerland, 2-10.

- [82] **Suhail, M. A., Obaidat, M. S., Ipson, S. S., Sadoun, B.,** 2003. A Comparative Study of Digital Watermarking in JPEG and JPEG 2000 Environment, *Information Sciences*, **151**, 93-105.
- [83] **Hsu, C. T., Wu, J.W.,** 1991. Hidden Digital Watermarks in Images, *IEEE Transaction on Image Processing*, **8 (1)**, 58-68.
- [84] **Amornraksa, T., Janthawongwilai K.,** 2006. Enhanced images Watermarking based on Amplitude Modulation, *Image and Vision Computing*, **24 (2)**, 111-119.
- [85] **Hamza, Y. A.,** 2008. Ayrık Dalgacık Dönüşümüne Dayalı, Dayanıklı Dijital Renkli Resim Damgalama Sistemi, Yüksek Lisans Tezi, Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Eskişehir.
- [86] **Yavuz, E. and Telatar, Z.** 2006. SVD Adapted DCT Domain DC Subband Image Watermarking against Watermark Ambiguity, *Lecture Notes on Computer Science*, 4105, 66-73.
- [87] **Öz, A.,** 2008. Çoklu Ortam Verilerinin Damgalanmasına Yeni Yaklaşımlar, Yüksek Lisans Tezi, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Kayseri.
- [88] **Kazan, S.,** 2009. Moment Tabanlı Normalleştirmeye Dayalı Sayısal Görüntü Damgalama Yöntemleri, Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya.
- [89] **Barni, M., Bartolini, F., Cappellini, V., Piva, A.,** 1998. A DCT-Domain System for Robust Image Watermarking, *Signal Processing*, **66**, 357-372.
- [90] **Stankovic, S., Djurovic, I., Pitas, Ioannis,** 2001. Watermarking in the Space/Spatial-Frequency Domain Using Two-Dimensional Radon-Wigner Distribution, *IEEE Transactions On Image Processing*, **10 (4)**, 650-658.
- [91] **Elbasi, E., Eskicioglu, A. M.,** 2006. A DWT-Based Robust Semi-blind Image Watermarking Algorithm Using Two Bands, IS&T/SPIE's 18th Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, Ocak 15-19.
- [92] **Öztürk, S.,** 2009. Kırılgan ve Dayanıklı Resim Damgalama Tekniklerinin Başarımının Zeki Optimizasyon Yöntemleriyle Artırılması, Doktora Tezi, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Kayseri.
- [93] **Emek, S.,** 2006. Sabit Görüntüler ve Video İşaretleri için Ayrık Dalgacık Dönüşümü Ayrık Kosinüs Dönüşümü Tabanlı Sayısal Damgalama Yöntemi, Doktora Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul..

- [94] **Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G.,** 1998. Attacks on Copyright Marking Systems. Proceedings of the Second Workshop on Information Hiding, Portland, Oregon, USA..
- [95] **Brassil, J., Low, S., Maxemchuk, N., O' Gorman, L.** 1995. Hiding Information in Document Images. Proceedings of the 29th Annual Conference on Information Sciences and Systems, pp. 482-489.
- [96] **Fridrich, I., Goljan, M.** 1999. Comparing Robustness of Watermarking Techniques, Interantional Society for Optical Enginnering, Security, and Wateramrking of Multimedia Contents, **3657**, 214-225, San Jose CA, Jan 25-25.
- [97] **Swanson, M.D., Kobayashi, M., Tewfik, A.H.** 1998. Multimedia Data-Embedding and Watermarking Technologies, *Proc. IEEE*, **86**, 1064-1087.
- [98] **Oğuz, C.,** 2006. Görüntü İşaretleri için Yeni Bir Sayısal Damgalama Yöntemi, Yüksek Lisans Tezi, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.
- [99] **Gürocak, İ.,** 2010. Görüntü Damgalama Kullanılarak İnternet Üzerinden Dosya Paylaşımı, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.
- [100] **Yavuz, E.,** 2008. Duruk İmgelerde Damgalama ve Veri Saklama, Doktora Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.
- [101] **Petitcolas, F.A.P.** 2000. Watermarking Schemes Evaluation. *IEEE Signal Processing*, **17(5)**, 58-64.
- [102] **Arnold, M., Schmucker, M., Wolthusen, S. D.,** 2003, Techniques and Applications of Digital Watermarking and Content Protection, Artech House, 273, London.
- [103] **Nikolaidis N., Pitas, I.,** 1999. Digital Image Watermarking: An Overview. ICMCS 99, Florence, Italy, **1**, 1-6.
- [104] **Ozaktas, H.M., Arikan, O., Kutay, M.A. and Bozdagi, G.** 1996. Digital computation of the fractional Fourier transforms. *IEEE Transactions on Signal Processing*, **44**, 2141-2150.
- [105] **Franz, E., Jerichow, A., Moller, S., Pfitzmann, A., Stierand, I.,** 1996. Computer Based Steganografik: How It Works and Why Therefore Any Restrictions on Cryptography are Nonsense, at Best, Proc. Information Hiding Workshop, 7–21.

- [106] **Craver, S., Memon, N., Yeo, B., Yeung, N.M.,** 1997. Resolving Rightful Ownerships with Invisible Watermarking Techniques, Research Report RC 20755 (91985), Computer Science/Mathematics, IBM Research Division.
- [107] **W. Diffie, W., Hellman, M. E.,** 1976. New Directions in Cryptography, *IEEE Transactions on Information Theory*, **22**, 644–654.
- [108] **Russ, J. C.,** 1999. The Image Processing Hand Book, Third Edition, CRC Press, ISBN:0-8493-2532-3.
- [109] **Güven M.,** 2001. Macromedia Fireworks 4, Dost Kitabevi.
- [110] **Sellars D.,** 1999. An Introduction to Steganography, Online book.
- [111] **Simmons G.,** 1984. The Prisoners' Problem and the Subliminal Channel, CRYPTO83 Advances in Cryptology, pp. 51-67.
- [112] **Stinson D.R.,** 2002. Cryptography: Theory and Practice, Second Edition, CRC Press.
- [113] **Swanson M., Kobayashi M., Tewfik A.,** 1998. Multimedia Data Embedding and Watermarking Technologies, *Proc. of IEEE*, **86** (6), 1064-1087.
- [114] **Şahin A., Buluş E., Sakallı M.T.,** 2006. 24-Bit Renkli İmgeler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme, Trakya Üniversitesi Fen Bilimleri Dergisi, Edirne-Türkiye.
- [115] **Şahin A., Buluş E., Sakallı M.T.,** 2006. Gri Seviye İmgeler Üzerinde Rasgele LSB Yöntemini ve Sayı Teorisini Kullanarak Bilgi Gizleme ve Steganaliz, *Akademik Bilişim Konferansları 2006-AB2006*, Denizli-Türkiye.
- [116] **Tunçkanat M., Sağıroğlu Ş.,** 2002. Güvenli İletişim İçin Yeni Bir Yaklaşım: İmge İçerisine Döküman Gizleme, GAP IV. Mühendislik Kongresi ,**1**, 665-668.
- [117] **Wang H., Wang S.,** 2004. Cyber Warfare: Steganography vs. Steganalysis, *Communications of the ACM*, **47** (10), 76-82.
- [118] **Westfeld, A.,** 2001. High Capacity Despite Better Steganalysis, In: Moskowitz, I.S.: Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, **2137**. Springer-Verlag, Berlin Heidelberg New York, 289–302.
- [119] **Regentova, E., Latifi, S., Deng, S.,** 2001. Images Similarity Estimation by Processing Compressed Data, *Image and Vision Computing*, **19** (7), 485-500.
- [120] **Soltani, S., Simard, P., Boichu D.,** 2004. Estimation of The Self-Similarity Parameter using The Wavelet Transform, *Signal Processing*, **84** (1), 117-123.
- [121] **Baskut, A.,** 1990. Numerical Image Compression using The Discrete Cosine Transform, *Signal Processing*, **19**(4), 346.

- [122] **Barni, M., Bartolini, F., Cappellini, V. and Piva, A.** 1998. A DCT-Domain System for Robust Image Watermarking. *Signal Processing*, **66**, 357-372.
- [123] **Liu, F. and Liu, Y.** 2008. A Watermarking Algorithm for Digital Image based on DCT and SVD. *Congress on Image and Signal Processing*, 380-383.
- [124] **Ustaoglu, U.**, 2008. Kesirli Fourier dönüşümü analiziyle ilinti tabanlı iki boyutlu damgalama, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.
- [125] **Herrigel, A., et al.**, 1998. Secure Copyright Protection Techniques for Digital Images, in Information Hiding, LNCS 1525, 169-190.
- [126] **Sherlock B. G.**, 1999. Windowed Discrete Fourier Transform for Shifting Data, *Signal Processing*, **74(2)**, 169-177.
- [127] **Pereira, S., et al.**, 1999. Template Based Recovery of Fourier-Based Watermarks Using Log-Polar and Log-Log Maps, Proc. IEEE Multimedia Systems 99, Int. Conf. Multimedia Computing and Systems, Florence, Italy, 870-874..
- [128] **Aslantas, V.**, 2008. A Singular-Value Decomposition-based Image Watermarking using Genetic Algorithm, *AEU - International Journal of Electronics and Communications*, **62 (5)**, 386-394.
- [129] **Fan, M.-Q., Wang, H.-X., Li, S.-K.**, 2008. Restudy on SVD-Based Watermarking Scheme, *Applied Mathematics and Computation*, **203(2)**, 926-930.
- [130] **Chandra, D.V.S.** 2002. Digital Image Watermarking using Singular Value Decomposition, *Midwest Symposium on Circuits and Systems*, **3**, 264-267.
- [131] <http://www.vision.caltech.edu/html-files/archive.html>, Computational Vision, 2010.
- [132] <http://phoenix.inf.upol.cz/iris/>, Index of Iris Download, 02.01.2010.
- [133] **Karaca, N.**, 2007. Alçak Çözünürlüklü Fotoğrafların Görüntülenmesi ve Bunların Optimizasyonu ile İlgili Bir Çalışma, Yüksek Lisans Tezi, Ege Üniversitesi, Fen Bilimleri Enstitüsü, İzmir.
- [134] **Chiang, W.-Y., Wang, S.-J., Weng, C.-Y., Yang, C.-H.**, 2009. Robustness-Set in Watermarking Embedding Systems using Codebook Classifications. *ICUIMC 2009*: 207-215.
- [135] http://cygm.meb.gov.tr/modulerprogramlar/kursprogramlari/bilisim/moduller/goruntu_isleme1.pdf, 12.05.2011.

- [136] **Yalman, Y., Ertürk, İ.**, 2009. İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniğı Tasarımı ve Uygulaması, Akademik Bilişim Konferansı Bildirileri, Harran Üniversitesi, Şanlıurfa.

ÖZGEÇMİŞ

Şengül DOĞAN

sdogan@firat.edu.tr

Tlf: 424 2370000 / 4350

Fırat Üniversitesi Teknik Eğitim Fakültesi

Elektronik ve Bilgisayar Eğitimi Bölümü

ELAZIĞ

1980 yılında Elazığ'da doğdu. İlk, orta ve lise öğrenimini Elazığ'da tamamladı. 1998 yılında Fırat Üniversitesi Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bilgisayar Öğretmenliği Bölümü'nü kazandı. 2002 yılında bu bölümden mezun olup Milli Eğitim Bakanlığında Bilgisayar Öğretmeni olarak göreve başladı (2002- Elazığ/Karakoçan YİBO, 2003- Elazığ/Yücel İÖÖ, 2005- Elazığ/Merkez Anadolu Lisesi). 2004 yılında Fırat Üniversitesi Fen Bilimleri Enstitüsü Biyomühendislik Ana Bilim Dalı'nda yüksek lisans eğitimine başladı. 2007 yılında yüksek lisans eğitimini tamamlayarak aynı yıl Fırat Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Ana Bilim Dalı'nda doktora eğitimine başladı. 2010 yılında Teknik Eğitim Fakültesi Elektronik Bilgisayar Eğitimi Bölümü Bilgisayar Öğretmenliği Bölümü'nde açılan araştırma görevliliği sınavını kazanarak göreve başladı. Halen bu görevi sürdürmektedir. Yabancı dili İngilizcedir.