



**SAYISAL GÖRÜNTÜ İŞLEMEDE DAMGALAMA TEKNİKLERİ VE KAOS
TEMELLİ YENİ BİR YAKLAŞIM**

Yusuf SELİMDAROĞLU

YÜKSEK LİSANS TEZİ

Mekatronik Mühendisliği Anabilim Dalı

Dr. Öğr. Üyesi Levent GÖKREM

Eş Danışman Dr. Öğr. Üyesi Uğur ERKAN

Şubat - 2022

T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MEKATRONİK MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

**SAYISAL GÖRÜNTÜ İŞLEMEDE DAMGALAMA TEKNİKLERİ
VE KAOS TEMELLİ YENİ BİR YAKLAŞIM**

YUSUF SELİMDAROĞLU

TOKAT
Şubat - 2022

ETİK SÖZLEŞME

Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre, Dr. Öğr. Üyesi Levent Gökrem danışmanlığında hazırlamış olduğum “Sayısal Görüntü İşlemede Damgalama Teknikleri ve Kaos Temelli Yeni Bir Yaklaşım” adlı Yüksek Lisans tezinin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımını kabul edeceğimi beyan ederim.

2/02/2022

Tez Yazarı (Yusuf Selimdaroğlu)



JÜRİ KABUL VE ONAY

Yusuf Selimdaroglu tarafından hazırlanan “**Sayısal Görüntü İşlemede Damgalama Teknikleri ve Kaos Temelli Yeni Bir Yaklaşım**” adlı tez çalışmasının savunma sınavı 2 Şubat 2022 tarihinde yapılmış olup aşağıda verilen Jüri tarafından Oy Birliği ile Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü Mekatronik Mühendisliği Anabilim Dalı’nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri (Unvanı, Adı Soyadı)

İmzası

Üye (Başkan) :Prof. Dr. Mahmut HEKİM

.....

Üye :Doçent Dr. Kemal ADEM

.....

Üye :Doktora Öğr. Üyesi Levent GÖKREM

.....

ONAY

...../...../.....

Prof. Dr. Mehmet GÜNEŞ
Lisansüstü Eğitim Enstitüsü Müdürü

ÖNSÖZ

Yaklaşık üç yıldır öğrenim gördüğüm süre boyunca tezimi hazırlama esnasında değerli fikirleri ve yorumlarıyla beni yönlendiren tez danışmanlarım Dr. Öğr. Üyesi Levent Gökrem ve Dr. Öğr. Üyesi Uğur Erkan'a çalışmama kattıkları ilgi ve yardımlarından dolayı ve maddi manevi desteklerini benden esirgemeyen aileme ve dostlarıma teşekkür ediyorum.

Yusuf SELİMDAROĞLU

2 Şubat 2022

ÖZET
SAYISAL GÖRÜNTÜ İŞLEMEDE DAMGALAMA TEKNİKLERİ VE KAOS
TEMELLİ YENİ BİR YAKLAŞIM

Selimdaroğlu, Yusuf
Yüksek Lisans, Mekatronik Mühendisliği Anabilim Dalı
Tez Danışmanı: Dr. Öğr. Üyesi Levent Gökrem
İkinci Danışman: Dr. Öğr. Üyesi Uğur Erkan
Şubat 2022, xiii + 71 sayfa

Son yıllarda gündeme gelen en önemli konulardan birisi dijital görüntüler üzerindeki telif haklarıdır. Dijital görüntüleri korumanın en etkili yöntemlerinden birisi dijital damgalamadır. Dijital damgalama, görüntüye size ait olduğu gösteren bir imza atma işlemidir. Bu işlemin görünür ve görünmez dijital damgalama olmak üzere iki türü vardır. Görünür dijital damgalama daha çok videolar ve görüntüler üzerine, damganın açık şekilde görülebileceği şekilde basılmasıdır. Bu damgalama türünde amaç, daha çok telif değil, görüntü yayılırken görüntünün sahibinin de belli olması amaçlanmaktadır. Görünmez dijital damgalamada, görüntüye eklenen damganın, görüntüye bakanlar tarafından fark edilmemesi amaçlanmaktadır. Bu damgalama türünde, genelde farklı boyutlarda kare kodlar kullanılmaktadır. Bu çalışmada, 3 farklı boyutta toplam 12 adet kare kodla test edilen görünmez bir dijital damgalama tekniği önerilmektedir. İlk olarak görüntü ve dijital damga ikilik sisteme çevrilmektedir. Daha sonra, görüntüdeki her bir 8 bitlik pikselin düşük 4 biti damgalama için kullanılmaktadır. Böylelikle, damgalanmış görüntüdeki değişim mümkün olduğu kadar en aza indirilmeye çalışılmaktadır. Dijital damga görüntüye uygulanırken, kolaylıkla çıkarılmaması için yeni önerilen bir kaotik haritayla piksel konumları karıştırılmıştır. Ayrıca, yeni önerilen kaotik harita, dijital damga görüntüye yerleştirilirken de kullanılmaktadır. Bu çalışmada, dijital damgalama ve görüntü şifrelemede kullanılmak için bir boyutlu yeni bir kaotik harita önerilmiştir. Yeni önerilen kaotik harita, yapılan tüm kaotik ölçme testlerinde yüksek başarı göstermiştir. Sonuç olarak, önerilen dijital damgalama tekniği, dijital damgayı görüntüye yerleştirirken pik sinyal-gürültü oranı (Peak signal-to-noise ratio, PSNR) ve yapısal benzerlik (structural similarity, SSIM) testleriyle de görüntüdeki bozulma ölçülmüştür. PSNR ve SSIM sonuçlarının çoğu sırasıyla, 50'den büyük ve 1'e çok yakındır. Buda önerilen damgalama yönteminin çok başarılı olduğunu göstermektedir.

Anahtar Kelimeler: Sayısal Görüntüleme, Damgalama, Telif Hakkı, Multimedya Koruması, Dijital Damga, Kaotik Harita, Kaos Kavramı, PSNR, SSIM

ABSTRACT
**STAMPING TECHNIQUES IN DIGITAL IMAGE PROCESSING AND A NEW
APPROACH BASED ON CHAOS**

Selimdaroglu, Yusuf
Master's Thesis, Division of Mechatronics Engineering
Advisor: : Assit.Prof.Dr. Levent Gökrem
Second Advisor: Assit.Prof.Dr. Uğur Erkan
February 2022, xiii + 71 pages

One of the most crucial issues that have occurred in recent years is the copyrights on digital images. One of the most effective approaches of preserving digital images is digital watermarking. Digital watermarking is the process of signing the image as your own. There are two kinds of this process, one of which visible and the other one is invisible digital watermarking. Visible digital watermarking is the printing of videos and images in such a way that the watermarked is clearly visible. In this sort of watermarked, the objective is not only copyright, but also to unearth the owner of the image while spreading the image. In invisible digital watermarking, it is aimed that the stamp added to the image is not realized by the watchers. In this genre of stamping, QR codes of different sizes are mostly used. In this study, an invisible digital watermarking technique tested with a total of 12 QR codes in 3 different sizes is recommended. Initially, the image and the digital watermarking are transformed into the binary system. The lower 4 bits of each 8-bit pixel in the image are then used for watermarked. Hence the change in the watermarked image is tried to be minimized. When applying the digital watermarking to the image, pixel positions are mixed with a newly proposed chaotic map so that it is not easily removed. Besides, the newly proposed chaotic map is also used when placing a digital watermarking on the image. In addition, in this study, a new one-dimensional chaotic map is proposed for use in digital watermarking and image encryption. This newly proposed chaotic map has displayed high success in all tests. As a result, while the proposed digital watermarking technique places the digital watermarking on the image, the distortion in the image was also measured by the peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) tests. Most PSNR and SSIM results are greater than 50 and very close to 1, respectively. This shows that the proposed watermarked method is very successful.

Keywords: Digital Image, Watermarked, Copyright, Multimedia Protection, Digital Watermarked, Chaotic Map, PSNR, SSIM

İÇİNDEKİLER

Sayfa

ETİK SÖZLEŞME.....	i
JÜRİ KABUL VE ONAY	ii
ÖNSÖZ	iii
ÖZET	iv
ABSTRACT.....	v
İÇİNDEKİLER	vi
TABLolar LİSTESİ.....	ix
ÇİZELGE LİSTESİ	x
ŞEKİL LİSTESİ.....	xi
KISALTMALAR.....	xiii
1. GİRİŞ	1
2. GENEL BİLGİLER	3
2.1. Sayısal Görüntü İşleme	3
2.2. Dijital Steganografi.....	7
2.3. Sayısal Damgalama.....	10
2.4. Damgalama Teknikleri ve Sınıflandırılması.....	12
2.4.1. Algıya göre sınıflandırma	14
2.4.2. Veri ortamına göre sınıflandırma.....	18
2.4.3. Algoritma düzlemine göre sınıflandırma	20
2.5. Sayısal Damgalama Yöntemleri	21
2.5.1. LSB yöntemi	22
2.5.2. DCT yöntemi	26
2.5.3. DFT Yöntemi	29
2.5.4. DWT Yöntemi	29

2.6. Saldırı Türleri.....	32
2.6.1. Alt küme ekleme saldırısı	32
2.6.2. Alt küme değiştirme saldırısı	33
2.6.3. Bit değiştirme saldırısı	33
2.6.4. Alt küme silme saldırısı	33
2.6.5. Sahte sahiplik saldırısı	33
2.6.6. Satır bazlı çoklu saldırı	34
2.6.7. Sıralama saldırısı.....	34
2.6.8. Alan bazlı çoklu saldırı	34
2.6.9. Element sıra karıştırma saldırısı	34
2.6.10. Alan silme veya karıştırma saldırısı.....	34
2.6.11. Etiket ad karıştırma saldırısı	35
2.7. İlgili Alanda Yapılan Çalışmalar	35
3. MATERYAL VE YÖNTEM.....	38
3.1. Damgalama İşlemlerinde Kullanılan Materyaller.....	38
3.2. Yeni Önerilen Kaotik Harita.....	40
3.2.1. Çatallanma Diyagramı ve Lyapunov üssü	41
3.2.2. Permütasyon entropi	43
3.2.3. Örnek Entropi	44
3.2.4. 0-1 Testi	45
3.3. Yeni Önerilen Dijital Damgalama Yöntemi	45
4. BULGULAR.....	50
4.1. LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ Damgası Test Sonuçları.....	51
4.2. YUSUF SELİMDAROĞLU Damgası Test Sonuçları	52
4.3. LEVENT GÖKREM Damgası Test Sonuçları	55
4.4. UĞUR ERKAN Damgası Test Sonuçları	56

5. SONUÇ VE ÖNERİLER.....	58
KAYNAKLAR	61
EKLER.....	68
Ek 1. Matlab Uygulama Görüntüleri	68



TABLÖLAR LİSTESİ

Sayfa

Tablo 3.1. SHA – 512 Hash kodları.....	40
Tablo 3.2. Kaotik harita karşılaştırma tablosu.....	41
Tablo 4.1. PSNR ve SSIM sonuçları 1	52
Tablo 4.2. PSNR ve SSIM sonuçları 2	54
Tablo 4.3. PSNR ve SSIM sonuçları 3	56
Tablo 4.4. PSNR ve SSIM sonuçları 4	58



ÇİZELGE LİSTESİ

Sayfa

Çizelge 2.1. Algıya göre sınıflandırmanın özellikleri.....	14
--	----



ŞEKİL LİSTESİ

Sayfa

Şekil 2.1. Lena görüntüsü	6
Şekil 2.2. Görünür damga	11
Şekil 2.3. Damgalama işlemi	13
Şekil 2.4. Sayısal damgalama teknikleri	Hata! Yer işareti tanımlanmamış.
Şekil 2.5. DWT ile damgalama yöntemi.....	16
Şekil 2.6. ASCII tablosunda “b” harfinin, bir filigran bit dizisi olarak bir başka veri dizisinin içine kodlanması	23
Şekil 2.7. RGB görüntüdeki kırmızı, yeşil ve mavi katmanlar	23
Şekil 2.8. Ses sinyalinin örneklenmesi ve kuantalanması	25
Şekil 2.9. LSB yöntemiyle video damgalama blok diyagramı	26
Şekil 2.10. DCT uygulanması (Orijinal ve damgalanmış medyada)	28
Şekil 2.11. Dikey ve yatay DWT	31
Şekil 3.1. Bu çalışmada kullanılan QR kodlar	39
Şekil 3.2. Bu çalışmada kullanılan test görüntüleri	39
Şekil 3.3. 1D-koatik Harita Çatallanma ve Lyapunov Üssü Diyagramı a) Çatallanma, b) Lyapunov Üssü	42
Şekil 3.4. Lyapunov Üssü	43
Şekil 3.5. Permütasyon entropi	44
Şekil 3.6. Örnek entropi	45
Şekil 3.7. 0-1 Test sonucu.....	45
Şekil 4.1. Lena, Einstein, Parrot ve Pirate görüntüleri için “LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ” dijital damgalaması görsel sonuçları	51
Şekil 4.2. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalaması görsel sonuçları.....	53
Şekil 4.3. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalaması görsel sonuçları.....	55
Şekil 4.4. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalama görsel sonuçları	57
Şekil 7.1. Matlab uygulama ana ekran görüntüsü	68
Şekil 7.2. Matlab uygulama görüntü al ekran görüntüsü.....	69

Şekil 7.3. Matlab uygulama damga al ekran görüntüsü.....	69
Şekil 7.4. Matlab uygulaması damga ekleme ekran görüntüsü.....	70
Şekil 7.5. Matlab uygulaması damga çıkarma ekran görüntüsü	70



KISALTMALAR

Akt: Aktaran

DCT :Ayrık Kosinüs Dönüşümü

DFT: Ayrık Fourier Dönüşümü

DWT: Ayrık Dalgacık Dönüşümü

EML: Extensible Markup Language

FOA: Meyve Sineği Algoritması

HD: Hessenberg Ayrıştırması

İİS: İnsan İşitme Sistemi

İGS: İnsan Görme Sistemi

ISO: Uluslararası Standardizasyon Organizasyonu

JPEG: Birleşik Fotoğraf Uzmanları Grubu

NC: Normalleştirilmiş Korelasyon

PSNR: Tepe Sinyal Gürültü Oranı

RGB: Kırmızı Yeşil Mavi

SSIM: Yapısal Benzerlik İndeksi Ölçüsü

SVD: Tekil Değer Ayrıştırması

TSGO: Tepe Sinyalinin Gürültüye Oranı

1. GİRİŞ

Teknolojinin gelişmesi ve yaygın internet kullanımı sonucunda bilgi ve veri paylaşımının hızla artması telif hakkını doğuran en büyük sebeplerden birisidir. Sayısal görüntü damgalama verilerinin (fotoğraf, video, ses) korunmasında bize öncülük yapabilen bir tekniktir. Damgalamayı iki farklı konuda ele alınabilir. Bu kapsamda görülebilen ve görülemeyen damgalama çeşitlerini inceleyeceğiz.

Görülebilen damgalama çeşidi olarak televizyon kanallarını örnek verebiliriz. Her bir kanaldaki yayın akışının belli bir noktasında kanal logosunu yayın süresince görebilmemize imkân sağlayan bir damgalama türüdür. Bu tür bir damgalama bize yayının hangi yayın kuruluşuna ait olduğunu göstermektedir. Bir örnek olarak da haber ajansının web üzerinde paylaşmış olduğu video veya fotoğrafın üzerinde ajansın isminin damgalanması ve bu ismin gözle görülebilmesi o ajansın hem telif hakkına hem de web üzerinde popüler olmasına sebep olacaktır.

Görülemeyen damgalama çeşidinde ise verinin (fotoğraf, video, ses) içerisine gizli bir algoritma ile veri (fotoğraf, video, ses) ekleyebilir ve yine aynı yöntemle bu veri kusursuz bir şekilde çıkarılabilmektedir. Haberleşme sisteminde kullanılan bu teknik sayesinde bir resmin içerisine damgalanacak mesaj ile iletişim de kullanarak üçüncü kişilerin bunu bir resim dosyası olarak algılaması sağlanabilir. Webde dolaşan bir resim dosyasının sadece bize ait olduğunu bu teknikle mümkün kılınabilir. Üçüncü kişiler telif hakkının bizde olduğunu bilemez ve webde dolaşan resim dosyamızın kimler tarafından kullanıldığını bu damgalama tekniği ile takip edilebilir.

Sayısal damgalama yöntemleri, ajanslar tarafından yaygın olarak kullanılması yazılım korsanlarının damgalanan damgayı çalıp, damga üzerindeki oynamaları sonucunda programcılarının sağlam ve kusursuz damgalama teknikleri geliştirmelerine sebebiyet vermiştir.

Sayısal damgalama ile ilgili ilk çalışmaların 1954 yıllarında Emil Hembrooke'un Murac Corporation adına aldığı "Identification of sound and like signals" başlıklı patent ile başladığı düşünülmektedir.

Bu patentte sayısal damgalama “Bu buluş, bir müzikal sunumun kökeninin pozitif olarak tanımlanması mümkün kılınır ve bu şekilde korsanlığı önlemek için etkili bir araç teşkil eder, yani kâğıda basılan bir filigrana benzetilir.” biçiminde belirtilmektedir.

Sayısal damgalama yöntemleri üzerindeki çalışmalar, yoğunlukla görüntü, ses ve videonun dünya genelinde yayılması ile beraber 2002 yılından sonra hızla yükselişe geçmiştir. Ancak sayısal görüntü işlemede damgalama terimi ilk olarak 1992 yılında Andrew Z. Tirkel ve Charles F. Osbourne tarafından ortaya çıkarılmıştır. 1993 senesinde, 512*512 boyutundaki 8-bit siyah-beyaz bir görüntü üzerine insan algısı tarafından görülemeyen sayısal damgalama yöntemi Andrew Z. Tirkel, Charles F. Osbourne, R.M. van Schyndel, W.J. Ho, N.R.A. Mee ve Gerard Rankin tarafından ortak bir proje olarak bilim dünyasına tanıtılmıştır.

Sayısal görüntü damgalama teknikleri ile yerleştirilen damganın orijinal veride kullanımı etkileyebilecek düzeyde bozulmaya neden olmamalıdır. Aksi halde güvenliği sağlanmış olmakla birlikte kullanılamaz durumda bir veri elde edilecektir. Güvenlik ile birlikte yüksek damgalama kapasitesinin olması da kullanılabilirlik alanlarının artmasına yardımcı olacaktır. Damgalama tekniklerinin damga verisini orijinal verinin kullanılabilirliği bozulmadan yerleştirmesi beklenir.

Bu kapsamda çalışmada giriş bölümünden sonra genel bilgilere yer verilecektir. Sayısal damgalama kavramı, sayısal damgalama teknikleri ve sınıflandırılması, saldırı türleri kapsamlı şekilde ele alınacaktır. Çalışmanın üçüncü bölümünde ise sayısal damgalama alanında yapılmış çalışmalara yer verilecektir.

2. GENEL BİLGİLER

2.1. Sayısal Görüntü İşleme

Sayısal görüntü işleme, verilerin yakalanarak ölçme değerlendirme işleminin sonrasında bir başka aygıtta okunabilir duruma dönüştürülmesi veya elektronik bir ortamdan bir başka elektronik ortama aktarılmasını kapsayan sinyal işleme çalışmasından farklıdır (Gonzalez ve Woods, 2006). Belirli bir hedefe yönelmiş olan görüntü kaynağından alınan görüntülerin içerikleri farklıdır. Bunlar elektro mikroskop, ultrason, bilgisayar içerikli görüntüler şeklindedir. Görüntü işlemede görüntüler için uygulanan ön hazırlık aşamasında kötü görüntü, netlik, görüntü bulanıklığı azaltılmaktadır. Görüntülere uygulanan işlemler düşük, orta ve yüksek düzeyde olmaktadır. Giriş çıkış görüntülerinin gerçekliği filtreleme düşük düzeydeki işlemlerle sağlanır. Görüntülerde olan nesnelerin tanınması, sınıflandırılması için bölme ve tanıma ise orta düzeydeki işlemlerle sağlanır. Görüntülerde olan nesneleri tanıma için görüntülerin analizi ise yüksek düzeydeki işlemlerle sağlanır. Bilgisayar ortamında görüntülerin analiz edilmesi sonucunda nesnelerin görüntüleri detaylandırılır. Bu aşama sonucunda görüntü işleme yapılmış olur (Jahne, 2005).

Sayısal görüntü işleme, görüntü içeriğinin sayısal olarak tanımlanmasını ifade etmektedir. Sayısal görüntü işleme, analog görüntünün sayısal biçime dönüştürülmesini, ardından iyileştirme, sınıflandırma, onarma, anlama, yorumlama, sıkıştırma gibi farklı amaçlar için sayısal bilgisayarlara işlenmesine ilişkindir. Bu şekilde görüntülerin içeriği ile görüntüde bulunan nesnelerin niteliklerine ilişkin bilgiler elde edilmektedir. Sayısal görüntü işleme teknikleri ile görüntülerin anlamlı bilgileri ve özellikleri çıkarılabilir. Bu uygulama yazılımlar tarafından 2B ve 3B sayısal görüntülerin işlenmesiyle gerçekleştirilmektedir. Sayısal görüntü işleme teknikleri günümüzde teknik alanların tamamına yakını etkilemiştir. Pek çok alanda sayısal görüntü işleme uygulamalarının kullanıldığı görülmektedir. Sayısal görüntü işleme tekniklerinin kullanıldığı alanlar görüntülerin kaynaklarına göre; X ışını görüntüleme (Tomografi, Radyografi, Anjiyografi vb.), Gama ışını görüntüleme (PET, kamera, gama, SPECT), Görüntü ve kızılötesi bantlarda görüntüleme (optik görüntüleme sistemleri, ışık mikroskopisi), Mikrodalga bandındaki görüntüleme (Radar), Morötesi bandında görüntüleme (lazerler, biyolojik görüntüleme, Litografi), diğer görüntüleme yöntemleri (Taramalı elektron mikroskobu, Geçirimli elektron mikroskobu) şeklinde kategorize edilebilmektedir (Gonzalez ve Woods, 2006).

Sayısal görüntü işlemeye ilişkin temel aşamalar aşağıdaki gibi sıralanmaktadır:

1. Görüntü elde etmek (Image Acquisition): Fotoğraf makinesi, tarayıcı, kamera, tıbbi görüntüleme cihazları, telefon gibi cihazlardan görüntüyü elde etmek. Görüntünün gerçek dünyadan bir hafıza birimine ya da film tabakasına alınmasını sağlayıcı resim alıcılarıdır. Cihazlarda resim algılayıcısı ile algılanan resmin sayısal duruma dönüştürülmesini sağlayan sayısallaştırıcı birim vardır. Resim algılayıcısının resmin doğrudan sayısal duruma dönüştürememesi durumunda, algılayıcı ile sağlanan analog resim dönüştürücü ile sayısal duruma dönüştürülür. Sayısal fotoğraf makinesi, tarayıcı, sayısal kamera analog resimleri sayısal duruma dönüştüren yapılar arasında gösterilebilir.
2. Görüntünün iyileştirilmesi (Image Enhancement): Görüntülerin filtreleme, kontrast gibi yöntemlerle daha iyi duruma getirilmesi.
3. Görüntünün onarılması (Image Restoration): Gürültülü görüntünün ya da bozulmuş görüntünün ya da görüntünün içerisindeki nesnelerin girdisinin tahmin edilmesi.
4. Morfolojik işlemler: Görüntüde aşındırma, genişletme, iskelet oluşturma, sınır belirleme gibi işlemlerin yapılması.
5. Segmentasyon: Görüntünün kendisini meydana getiren nesnelere, parçalara ayrılmasıdır. Bunun yanı sıra görüntünün arka planının istenmesi durumunda görüntü girdi halinden uzaklaştırılabilmektedir.
6. Tanıma: Retina tanıma, parmak izi, yüz tanıma gibi nesnenin tanımlayıcılarının görüntüde belirlenmesini kapsar.
7. Şablon eşleme: Görüntü içindeki bir şablon görüntüyle eşleşen bölgenin ya da bölgelerin karşılaştırılmasıdır (Pratt, 2001; Gonzalez ve Woods, 2006).

Sayısal görüntü işleme yazılımları arasında OpenCV, GNU Octave, MATLAB, Obj, GIMP, Aforge, FIJI, NET, Python, OpenGL, VTK gibi çok sayıda yazılım gösterilebilir.

Medikal açıdan görüntüleme yöntemleri ele alındığında, hastalık şüphesi olan ve/veya belirli bir anomaliye sahip olan bölgeleri fizyolojik ve anatomik olarak 2B, 3B, 4B olarak gerçek zamanlı incelemek ve görüntülemek önem arz etmektedir. Bu şekilde görüntülenecek bölgelerin konumu, şekli, büyüklüğü, çevre bölgelere yakınlığı gibi parametreleri belirlenerek, tıbbi tanı ve/veya tedaviye yön verilmesi mümkün olabilmektedir. Medikal görüntülemede olan bu yenilikler, tanı ve tedavinin doğru

yapılabilmesi yanında medikal arařtırmalara da olumlu katkı yapabilmektedir (Landini vd., 2008).

Sayısal görüntü işlemede, nesne özelliklerinin ve bunların görünürlüğü ile ölçülebilirliğinin belirlenmesi amacıyla çeşitli yöntemler bulunmaktadır. Görüntülemede bilimsel hedef; toplama, görselleştirme, işleme, hacim kaplama, yüzey kaplama, biyomedikal görünümünün nicel analizini kapsamaktadır (Landini vd., 2008). Görüntülemenin biyomedikal uygulamadaki temel amacı ise tekrarlanabilir şekilde, doğru görüntüleme yapılabilmesidir (Jolesz ve Shtern, 1992).

Sayısal görüntü işlemede ilk aşama gürültüyü kaldırmak, radyometrik düzeltme, geometrik düzeltme gibi adımları kapsayan ön işlemedir. Görüntü işlemede düşük, orta, yüksek düzeyde olmak üzere görüntülere işlemler uygulanmaktadır. Filtreleme işlemi düşük düzeydeki işlemlerdendir. Objelerin sınıflandırılması, çıkarılması ve segmentasyon ise görüntüde yapılan orta düzeydeki işlemlerdir. Görüntü analizi ve görüntüden nesne tanıma ise yüksek düzeydeki işlemlerdir. Bunların yanı sıra görüntü dönüşümlerinden interpolasyon işlemlerinde tekrar örnekleme yapılabilir. Bu yöntemlerde genel olarak görüntüde hesaplanmış olan yeni piksel değerlerini çevresindeki komşu pikseller ile tekrar hesaplanır. İnterpolasyon yöntemlerinde farklı yaklaşımlar bulunmaktadır. Bu yaklaşımlardan en fazla kullanılanları ise doğrusal (bilinear), en yakın komşu (nearest neighbour), kübik spline (cubic spline), çift kübik (bi-cubic) yöntemleri olarak sıralanabilir (Siddharth vd., 2015).

Görüntü işlemede insan algılama sistemi, görüntüyü yakalama, görüntünün gruplanması ve analizi açısından en karmaşık bilinen sistemdir. Gözlerle başlayan insan görme sisteminde göz, fotoğraf makinesinin yaptığı gibi, beyindeki görme kısımları da analog temele dayalı görüntü işleme sistemi şeklinde kabul edilebilir. Sayısal görüntü işleme teknikleri, tıbbi tanı, askeri gözetim ve keşif, güvenlik, endüstriyel denetleme, hukuk gibi alanlarda kullanılmaktadır.



Şekil 2.0.. Lena görüntüsü

Sayısal görüntü üzerinde yapılan işlemler

Görüntü işlemede tüm işlemler görüntüyü meydana getiren piksellerde yani piksellerin gri seviye değerlerinin üzerinde gerçekleştirilmektedir. Bu işlemler; yerel işlemler, nokta işlemleri ile bütünsel işlemler olarak sınıflandırılabilir.

Nokta işlemlerde, bir noktada olan çıkış gri seviyesinin sadece benzer noktada olan giriş gri seviyesine bağlı olmaktadır. Diğer bir anlatımla nokta işlemleri, kendine komşu piksellerden bağımsız şekilde pikselin gri seviyesini değiştirme ile ilgilidir.

Yerel işlemlerde, bir noktada çıkış gri seviyesi noktanın komşuluğunda olan giriş gri seviyelerine bağlı olmaktadır. Yerel işlemlerde uzay domeninde farklı boyutlarda maskelerden yararlanılır. Maskeler görüntüde olan piksellerin tümü üzerinde kaydırılır ve görüntü filtrelenmesi için kullanılır. Buna göre yerel işlemlere görüntünün

bulanıklaşmasının giderilmesi, görüntü temizliği, bölge ve kenar özelliklerinin belirlenmesi örnek olarak gösterilebilir.

Bütünsel işlemlerde ise, bir noktada olan çıkış gri seviyesi, giriş gri seviyelerin tümüne bağlı olmaktadır.

Sayısal görüntü işleminin faydaları kullanım tekniklerine bağlı olarak farklılık göstermektedir. Görüntü işlemede kullanılan tekniklerin görüntüye yaklaşımı farklıdır. Görüntü işleme alanında yapılan çalışmaların temelinde görüntünün çözülmesi yani sayısallaştırma bulunmaktadır. Günümüzde sayısal görüntü işleme, elektronik, tıp, tasarım, güvenlik, imalat, jeodezi, mimari gibi pek çok farklı alanda kullanılmaktadır. Bu alanların çeşitliliği göz önüne alındığında, yapılan çalışmalar da artmaktadır. Bu bağlamda sayısal görüntü işleme alanındaki çalışmalar için genel bir değerlendirme yapılması mümkün olmamaktadır.

2.2. Dijital Steganografi

Bilgi gizleme yöntemleri arasında steganografi önemli bir alt daldır (Petitcolas vd., 1999). Steganografi, bir nesne içine verinin gizlenmesi şeklinde tanımlanabilir. Bu yöntemle veri, ses, resim, video, sayısal resim görüntüleri üzerinde saklanabilir. Görüntü dosyalarına gizlenecek veriler metin dosyası yanında, herhangi bir görüntüye gizlenmiş bir başka görüntü de olabilir. Burada içerisine bilgi gizlenen ortam örtü verisi, oluşan ortam ise stego- metin ya da stego- nesnesi olarak tanımlanmaktadır.

Steganografi, Yunanca gizli, saklı anlamına gelen “steganos” sözcüğü ile çizim, yazım anlamındaki “grafi” sözcüklerinden gelmektedir. Steganografinin tarihi Antik Yunanlılara ve Herodot dönemine kadar uzanmaktadır. Bilinen ilk steganografi uygulaması, İran savaşlarında kafasını kazıtarak kafa derisine gizli mesaj dövmesi yapılan ulak ile başlamıştır. Mesaj yazıldıktan sonra saçın uzaması beklenerek, ulak tarafından mesaj ulaştırılmaktadır. Bu aşamada ulağın saçı yeniden tıraş edilerek, mesaj açığa çıkarılmaktadır. İlerleyen dönemlerde harflerle müzik notalarının atanması, mors kodları, görünmez mürekkepler gibi uygulamalar ile steganografi kullanılmıştır (Katzenbeisser ve Petitcolas, 2000).

Steganografi görüldüğü gibi eski çağlardan itibaren farklı uygulama alanlarında ve formlarda görülebilen bir bilimdir (Sujatha vd., 2014). Kişilerin değerli bilgilerini gizlemek amacıyla kullandıkları steganografi, günümüzde dijital formlardan veri

transferini, veri iletimini sağlamak amacıyla kullanılmaktadır. Steganografinin esas işlevi veri içeriğini korumaktan ziyade veri içeriğinin gizlenmesini sağlamasıdır (Liu vd., 2015).

Görünen fakat içeriği belirli olmayan bilgi yetenekli kişiler ve ilerleyen teknolojilerin yardımıyla çözülebilir. Fakat verinin mevcudiyetinden haberdar olunamaması halinde teknolojileri ve kişilerin yetenekleri önem arz etmez (Sujatha vd., 2014).

Steganografide kullanılan terimler genel olarak aşağıdaki gibidir (Provos ve Honeyman, 2001):

1. Taşıyıcı unsur: Verinin gizleneceği ve gizli mesajın taşınacağı çoklu ortam unsurudur. Örnek vermek gerekirse resim steganografisinde taşıyıcı obje resim unsurları olmaktadır.
2. Gizli mesaj: Üçüncü kişilerden saklanmak istenen değerli bilgilerdir. Bunlar taşıyıcı unsurlar içinde saklanır.
3. Steganografik anahtar: Veri gizleme karşılıklı anlaşarak ya da yöntemler ve algoritma kullanımı ile belli bir düzende yapılabilir. Bu durumlarda karşılıklı anlaşma sağlanmadığından dolayı iki taraf veri gizlenmesini çözebilecek olan anahtar üzerinde anlaşma sağlamaktadırlar.
4. Steganografik obje: Taşıyıcı resimde gizlenmiş mesajın saklanması sonrasında taşıyıcı obje ile benzerlik gösteren multimedya unsurlarıdır.
5. Steganografik analiz: Bu işlem steganografik unsurların denetlenmesini, içlerine gizlenmiş olan verilerin bulunmasını içermektedir.
6. StegAnalist: Bu steganografik analiz işlemini yapan uzman için tanımlanan addır.

Steganografi sisteminin güvenilir şekilde inşa edilmesi için gereken unsurlar aşağıdaki gibi sıralanmaktadır (Haşiloğlu, 2001):

Görünmezlik (Algılanamazlık): Steganografik sistemin performans değerlendirmesinde bazı özelliklere bakılmaktadır. Bu özellikler arasında algılanamazlık en önemli olanıdır. Bu özellik gizli verinin iyi gizlendiğini ifade eder. Bu steganografik sistemin insan gözü ile fark edilemez olmasıyla ilişkilidir. Taşıyıcı unsurun üzerine steganografik mesajın gömülmesi sonrasında resimdeki değişimlerin insan gözü ile fark edilemez olması gerekmektedir.

Güvenlik: Saldırganın taşıyıcı objeye gizlenmiş mesajı fark etmesi durumunda dahi mesajı açığa çıkarmasının olanaksızla yakın olması gerekmektedir. Tepe Sinyalinin Gürültüye Oranı (TSGO) değeri ne kadar yüksek olur ise sistem o derece güvenli olmaktadır.

Kapasite (Veri yükü): Performans değerlendirmesinde steganografik veri yükü (kapasite) diğer bir kriterdir. Bu özellik kapak verisinin taşıyabileceği gizli veriyi ifade etmektedir. Kapak verisi boyutunun artması, taşınacak veri boyutunun azalması steganografik yöntemin başarısını artıracaktır. Steganografi çalışmaları genelde küçük boyutlu kapak verisinde büyük boyutlu gizli verinin fark edilmeden başarıyla taşıyabilecek algoritmalara odaklanmaktadır. Ayrıca iletim ortamında transfer edilen verinin artması, stego verilerin belirlenme olasılığını da azaltacaktır (Eggers vd., 2002). Veri yükü taşıyıcı mesaj kapasitesine göre önemli mesaj kapasitesinin daha fazla olmasını ifade etmektedir. Bu oranın en fazla %51 olması tavsiye edilmektedir. Zira bu oranın üzerinde olması durumunda steganografinin unsurları arasında bulunan görünmezlik unsuru ihlal edilmiş olur.

Sağlamlık: Steganografide taşıyıcı unsur olan video, resim gibi unsurların üzerine yapılan kesme- kırpma, filtreleme, sıkıştırma, yön değiştirme gibi manipülasyonlardaki dayanıklılık durumunu ifade etmektedir.

Günümüzde steganografi uygulamaları dijital nesneler üzerinde yapılmaktadır. Teknolojinin gelişmesiyle birlikte verilerin korunması için son yıllarda bu tür uygulamalar giderek yaygınlaşmaktadır. Steganografi, temel olarak gizli veri, kapak verisi ve gizleme fonksiyonu elemanlarından oluşmaktadır. Gizli veri, göndericinin alıcıya güvenli bir ortamda aktarmak istediği veriyi kapsamaktadır. Kapak verisi, gizli verinin gömüleceği ve iletim ortamında şüpheye yer bırakmayacak herhangi bir veriyi içermektedir. Gizleme fonksiyonu ise, göndericinin gizli veriyi gizleme yöntemini ve anahtarını içermektedir (Kutucu vd., 2015). Steganografik yöntemde öncelikle gizli verinin doğru yerleştirilmesi amacıyla kapak verisinde yeterince veri alanı bulmak amaçlanır (Liu vd, 2011). Kapak verisinin uygun olmaması durumunda ise veri gizleme işleminin yapılması mümkün olmaz.

Steganografik yöntemler

Steganografik yöntemler ses, metin ve resim olarak üç grup halinde ele alınmaktadır.

Ses steganografisi; yöntemi en önemsiz bite gömme, faz kodlama, eşlik kodlama, yaygın spektrum, yankı saklamadan oluşmaktadır (Baker vd., 2011).

Metin steganografisi; bu steganografi yönteminde bilginin saklanacağı nesne metindir. Bu yöntemde veri miktarı kısıtlı miktarda saklanabilmektedir. Metin steganografisi aşağıdaki gibi sınıflandırılabilir (Papa, 1998):

a. Yazımsal yöntemler

b. Açık alan yöntemleri

c. Anlamsal yöntemler

Görüntü steganografisi; bu steganografide en fazla kullanılan yöntemdir. Görüntünün içerisine bilgi gizleme şeklinde uygulanır. Gizleme fonksiyonu, gizlenecek veri ve verinin gizleneceği taşıyıcı ortam olarak iki parametreyi içermektedir (Westfeld ve Pfitzmann, 2000). Görüntü dosyalarına bir metin gizlenebilir veya başka bir resmin gizlenmesi de mümkün olabilir. Görüntü steganografide resim içerisine verinin gizlenmesinde farklı yöntemler kullanılmaktadır. Bu yöntemler maskeleyme ve filtreleme, en önemsiz bite ekleme ile algoritmalar ve dönüşümler olabilmektedir (Sellers, 1999).

2.3. Sayısal Damgalama

Bilgisayarlar ile bilgisayar ağlarındaki gelişmeye paralel olarak güvenlik ve telif haklarının korunması için geliştirilen sayısal damgalama teknikleri steganografi uygulamalarına benzemektedir. Fakat sayısal damgalamanın amacı çalışmayla birlikte damgalanan bilginin taşınmasını da içerir. Bu sebeple bilgisayar ortamında olan çalışmalara telif hakkı, logo, lisans gibi bilgiler damgalanmaktadır. Damgalama tekniklerinin geliştirilmesinde öncelikle sayısal çalışmalar için damgalanan bilginin sıkıştırma, gürültü, yeniden boyutlandırma, kesme gibi çeşitli işaret işleme işlemleri gibi saldırılara karşı dayanıklı olması göz önüne alınır. Steganografi uygulamalarında bu tür bir beklenti bulunmaz.

Sayısal damgalama yöntemi, izinsiz olarak çoklu ortam dosyalarının kopyalanarak çoğaltılmasını, internet olanakları ile dağıtılmasını önleyebilmek için önerilen bir

yöntemdir. Çoklu ortam dosyalarına çeşitli amaçlarla sayısal damgalama yöntemi kullanılarak bilgi saklanır. Burada amaç, saklanan bilginin gerek duyulduğunda yeniden kullanılmasıdır. Sayısal dosyalarda metin, video, görüntü, ses dosyaları gibi filigranlar kullanılır (Mesut, 2019).

Bir diğer tanımlamada ise sayısal damgalama, sayısal multimedya içeriğine bilginin eklenmesi işlemidir (Memon, Holliman ve Yeung, 1999). Sayısal damgalama, damga olarak nitelendirilen bilginin daha sonradan kopya kontrolü ve kopya önleme gibi çeşitli amaçlar için algılanabileceği ya da çıkarılabileceği biçimde sayısal multimedya içeriğine gömülme işlemidir. Sayısal damgalama, bu tekniklerin geliştirilmesi, ticarileştirilmesi için sayısal içeriğin hızla yayılımını zorlaştıracak engellerin üstesinden gelmeye yardımcı olacak önemli ve aktif olan araştırma alanı durumuna gelmiştir (Swanson, Kobayashi ve Tewfik, 1998).



Şekil 2.1. Görünür damga

Genel olarak damgalama, şifreleme ile şifre çözme işlemleri için önemli bir gelişmedir. İçeriğe doğrudan gizlenebilen, insanların duysal olarak algılayamadığı, sadece bilgisayar tarafından okunabilen bilgi parçası, sayısal damgalama olarak tanımlanmaktadır. Bu işlemin en önemli avantajı, içerik ile damganın ayrılmaz şekilde olmasıdır. Damga formlarının aşağıdaki gibi çeşitleri vardır (Srivadana, 2013):

Parmak izi: Damgalar, içeriğin alıcılarını belirlemek için parmak izi ile yardımcı olur. Aynı zamanda yasadışı şekilde kopyaların kaynağının izlenmesi için de yardımcı olur. İmzalar ile parmak izi arasındaki fark ise, damgayı imzalamada içerik sahibini, parmak izinde ise bilgisayarlar ile otomatik sistemler içeriği tanımlamaktadır. Yasal olarak içeriğin sahibine dağıtımını sağlar (Arnold, Schmucker ve Wolthusen, 2003).

İmzalar: Damga içeriğin sahibini belirler. Bilgi, kullanıcı tarafından içeriğin sahibi tarafından yayınlamak amacıyla yasal hakların elde edilmesi için kullanılır.

Kopya kontrolü: Damga, içeriğin sahibinin istediği kopyalama ve kullanım kurallarının hakkında bilgiler içermektedir. Bilgileri içeren cümlelerin kopyalanması mümkün olmaz.

İçerik koruma amacıyla geliştirilen çeşitli algoritmalar bulunmaktadır. Ancak algoritmalarda sağlamlık ve gürültü en önemli sorunları olmaktadır. Bu sebeple damgalama tekniklerini içerik korumada önemi artmaktadır. Bu yöntemle sayısal formata şifrelenen bilgilere sadece yetkili kişilerin ulaşabileceğinden emin olunabilir. Yetkili kişiler dışındakilerin orijinal verileri yok etmeden verilere erişebilmesi daha zor olur. Bu kırılğan, steganografi, eşleştirme, kırılğan, görünür gibi damgalama olarak bilinen yaklaşıma benzerdir.

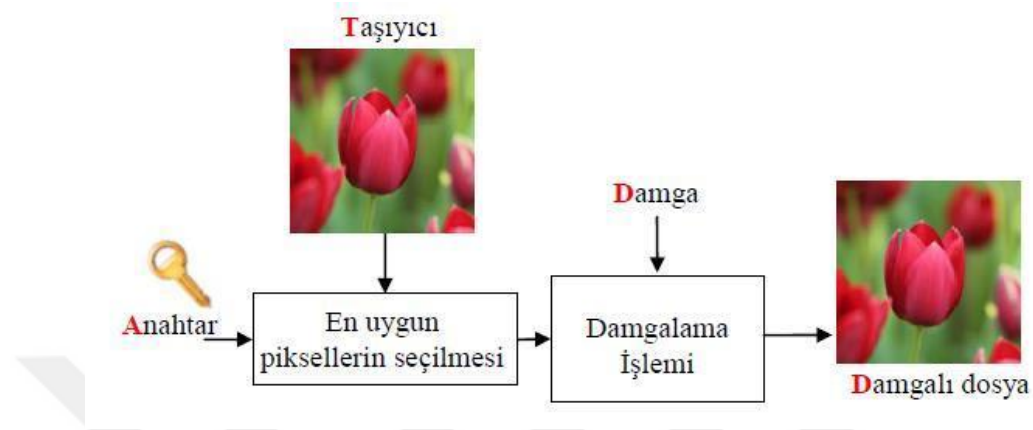
Görünür damga tekniği, içeriği kodlanmayan ve herkesin kolaylıkla okuyabileceği ya da kopyalayabileceği tanıdık bir yöntemdir. Bu yöntemle gizlilik sürdürülemez. İçerikle beraber görünür damgalar oluşturulur. Kodlana içeriği konuşlandırılması ile ihlal edilen telif hakkı olan içeriğini belirleme yeteneğine karşı çalışan sayısal damga, telif hakkı içeriğine kimliği doğrulanmış olan kullanıcıların kolay erişmesini sağlar. Buna kolay dönüştürülemeyen, işlenemeyen sayısallaştırılmış veri tanımlaması yapılabilir. Resim, metin gibi formatlara gömülmeleri mümkündür. Videolar, sesler gibi damgalar, verilerin aralarında tanımlanmasını ve içeriğin arasındaki bilgiyi sağlar. Damganın insanlar tarafından algılanması mümkün değildir. Sadece bilgisayarlar damgayı okuyabilir (Anderson, 1996).

Makinenin okuyabildiği damgalar daha fazla tercih edilirler. Bu damgalar daha iyi kodlama için eylemlerin okunmasına yardımcı olacak aktif işaretlemeye izin verdiğinden, genellikle gerekli olmayan okunabilir, içerik kaybı yaşanmadan damga çıkarılamaz. Yakın zamanda bu sayısal damgaların film ve müziklerin telif hakkı korunması hususunda pek çok uygulaması bulunmaktadır. Veri kaybına, değişimlere, alt seçim türünde olan problemlere karşı dayanıklılığı deneysel analizler ile onaylanmış olan pek çok iyileştirme, alternatif teknik bulunmaktadır (Srivadana, 2013).

2.4. Damgalama Teknikleri ve Sınıflandırılması

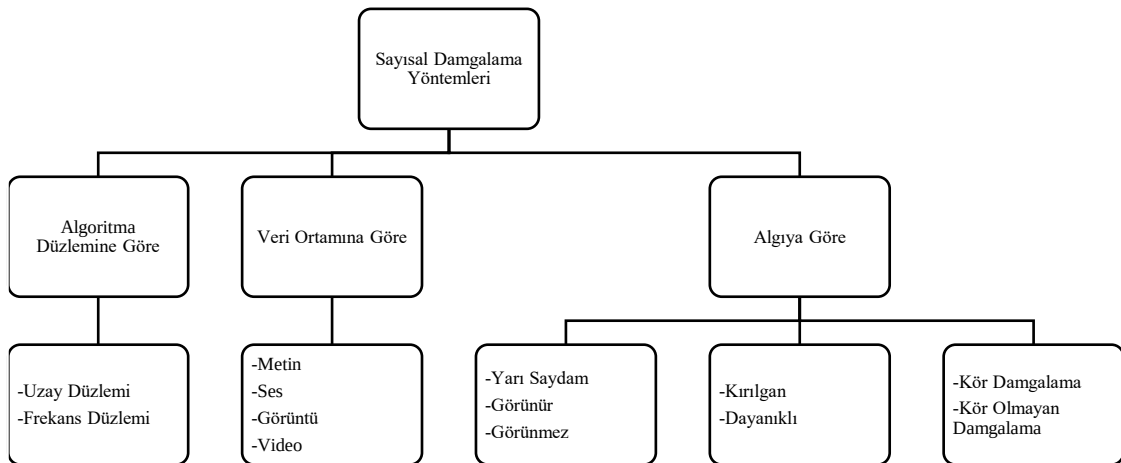
Damgalama tekniği, Şekil 2.1.'de görüldüğü üzere görüntüyü ya da verileri multimedya dosyası benzeri sayısal bir nesneye yerleştirme işlemidir. Bu logo ya da işaret ardından gömme işlemi için kullanılan damgalama tekniğini tersine çevirerek algılanabilir ya da çıkarılabilir. Kapak resmi, orijinal görüntüler ya da kaynak görüntüsü olarak tanımlanan

bu logoyu ya da işareti gerçekleştirmek amacıyla kullanılır. Bir damgalama tekniği sadece görüntünün telif hakkının korunması amacıyla kapak resmi içerisine bir logo ya da işaret koyabilmek için kullanılan işlemdir (Alasafi, 2016).



Şekil 2.2. Damgalama işlemi

Damgalama tekniğinin güvenilir olduğunu düşündüren en önemli koşullarından biri, bir logonun ya da işaretin saldırganlar tarafından kolay tespit edilememesi ya da çıkarılamaması ya da bir kapak görüntüsündeki logo ya da işaretin saldırılardan etkilenmesinin daha az olmasıdır. Damgalama teknikleri, kullanılan kapak görüntüsü, çalışma türü, logo ya da işaret türü gibi gömülü işlemin modüle edilen ya da modüle edilen doğasını işlemek amacıyla kullanılan yöntemlere göre sınıflandırılmaktadır. Aynı zamanda kullanılan uygulamalara ve insan algısına göre sınıflandırılmaları mümkündür (Le, Nguyen ve Le, 2010). Sayısal damgalama tekniklerinin sınıflandırılması ve kendi içerisindeki alt grupları Şekil 2.2’de gösterilmektedir.



2.4. Sayısal damgalama yöntemleri

2.4.1. Algıya göre sınıflandırma

Sayısal damgalama tekniklerinin algıya göre sınıflandırılması görünür damgalama, görünmez damgalama ve yarı saydam damgalama olarak yapılmaktadır.

Çizelge 2.1. Algıya göre sınıflandırmanın özellikleri

	Görünür Damgalama	Görünmez Damgalama
Özellikler	Yasa dışı olarak telif hakkı kaldırılmaz Telif hakkı ihlalleri için medyada kullanılır Esas olarak marka ya da logo etiketinde kullanılır Kimlik doğrulamayı sağlar	İnsan gözünün algılayamayacağı şekildedir Genellikle görünmez damgalama tercih edilir Genelde ticari gereklilik durumunda kullanılır
Avantajları	Hızlı işlem sağlar Doğrudan damgalama ekleme olasılığı	Orijinali küçültmede dayanıklılık özelliği vardır
Dezavantajları	Onur kırıcı orijinal kalite Saldırgan kırılabilirliği	Orijinal görüntü değiştirilebilir

Görünür damgalama

Görünür damgalama, görüntünün gözle görülebilecek bir yerine damgalanacak olan damganın yerleştirilme işlemidir. Bu damgalar sadece yasal yöntemlerle çıkarılabilir. İçeriği ya da görüntüyü doğrulamak için tescil etiketleri ve logo şeklinde kullanılır. Görünür damgalama tekniği, bir logo ya da işaretin gözle görülebildiği her tekniği içermektedir. Bu tekniğin yaygın olarak kullanıldığı alan medya kanallarıdır (Swanson vd., 1998).

Yapılan bazı araştırmalarda görünür ve görünmeyen damgalar birlikte kullanılarak, görünmeyen damganın görünür damganın yedeği şeklinde kullanılabileceği ortaya konmuştur (Amit Kumar, 2015). İnternette yayımlanan imgelerin bir köşesinde hangi sitede yayınlandığı ve televizyon ekranında kanal logosu gibi uygulamalar vardır. Doğrudan uygulandığı için hızlı ve kolay olur. Ancak saldırılara karşı kırılandır ve asıl görüntü kalitesini düşürür. Eserlerin mülkiyetinin tanımlanması, izleyicilerin sınırlı kopya haklarının dışında izinsiz kullanımını önlemek için görünür damgalar kullanılır (Hu ve Kwong, 2001).

Görünür basma teknikleri genel olarak ayrılmaz ve çıkarılabilir olarak iki tür olarak ele alınabilir. Ayrılmaz olanlar öncelikle damganın kaynak resmine ya da videoya uyumlu olmasını gerektirir. Diğer bir ifade ile uygun damga gerektirir. Sayısal içerikte damga görünebilir. Fakat orijinal resmin kalitesini etkilememesi gerekir. Bunun dışında gömülü damga, kötü amaçlı saldırılara ve istenmeyen düzenlemelere karşı oldukça dayanıklı olmalıdır. Çıkarılabilir olanlar ise, telif hakkı koruma sorunlarına etkili bir çözüm

sunmaktadır. Dağıtım öncesi orijinal sayısal içerik telif hakkı bildirimine benzer silinebilir özellikte bir desen ile işaretlenir ya da ücretsiz olarak internette görüntüleme olarak bırakılır. Görünür damgalama teknikleri aşağıdakiler gibi uygulamalara uygundur (Yang vd., 2007):

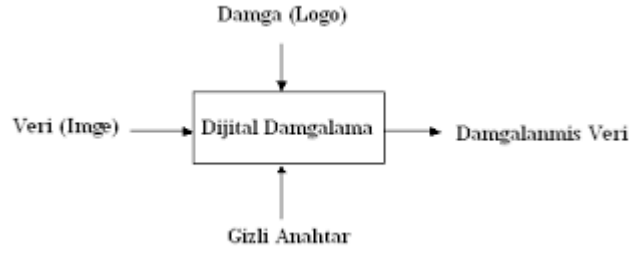
-İnsanların yaşamında sayısal görüntülerin ve videoların önemli bir rolü bulunmaktadır. Bunlar zaman içinde klasik analog ürünlerin yerine geçmeye başlamıştır. İçerik sağlayıcıların bilgisayar ağlarının üzerinden ücretsiz ön izleme sağlama, indirmeleri dağıtma ya da paylaşma ile görünür telif hakkı bilgisiyle alabilir. İçeriğiyle ilgilenenler telif hakkı bilgilerini kaldırabilmek için üreticiden satın aldıkları gizli anahtar ile iyi sürümlere ulaşabilirler.

-Bir şirket ticari bir ortamda kullanıcılarına ücretsiz deneme yazılımını sınırlı süre serbest bırakarak kara geçebilir. Fakat yazılımın deneme süresi sonunda çalışmayı kesebilir. Bunun için yazılım bağımlı olan sayısal içerik görünür damgalama ile kısıtlanabilir. Kullanıcı yazılımı kullanabilmek için etkinleştirmesi, sayısal içerikten damgayı lisans anahtarı yardımıyla kaldırması gerekir.

Çıkarılabilir görünür damgalama gerektiren pek çok uygulama bulunmasına rağmen, literatürde genelde geri alınamaz tekniklerin daha fazla geliştirilmesine odaklanılmaktadır. Fakat iki damgalama algoritması farklı uygulamalar için farklı gereklilikleri karşılaması için üretildiğinden, az sayıda görünür damga tekniği çıkarılabilmektedir (Yang vd., 2007).

Görünmez damgalama

Görünmez ya da etkilenmeyen damga, bir logo ya da işaretin görsel algılanmayacağı damgalama tekniğini içermektedir. Özel bir yazılım kullanılmadan Ayırık Kosinüs Dönüşümü (DCT) ve Ayırık Dalgacık Dönüşümü (DWT) teknikleri ile logolar ya da işaretlerin çıkartılması söz konusu değildir. Şekil 2.3.'te DWT ile damgalama işlemi görülmektedir. Görünmez damgalama tekniği dayanıklılığına göre kırılğan ve dayanıklı olarak iki tür ele alınmaktadır. Veri doğrulamak için dayanıklı damgalar kullanılırken, sayısal içeriği orijinalliğini ve bütünlüğünü kontrol etmek için kırılğan damgaların kullanılması amaçlanmıştır (Vleeschouwer vd., 2001).



Şekil 2.5. DWT ile damgalama yöntemi

Dayanıklı Damga: Görünmez damgalama tekniğinde dayanıklı damgalama, gizli olarak taşıyıcı görüntüye damgalanan bilgi görüntü kalitesini ciddi oranda bozmadan saldırılara karşı dayanıklı olmasına, çıkarıldığında ise tanınabilir nitelikte olması amaçlanır. Dayanıklı damga, gömülü logo ya da işaretin piksel bitlerinde değişikliğe neden olduğu ve gözlenemediğini ifade eder. Bunun yanında veri çıkarma için sadece uygun kod çözme mekanizmalarının kullanılması gerekmektedir (Petitcolas vd., 1999).

Kırılğan Damga: Bu teknik logo ya da markanın gömülü olduğu kapak resminde ortaya çıkan herhangi bir saldırı ya da değişiklikte logo ya da markanın tahribine yol açacağı anlamına gelmektedir (Stein, 2000).

Görüntü değiştirilmiş ise değiştirilenlere karşılık gelen içerik ve damga eşleştirilemez. Bu şekilde değiştirilmiş blokların algılanması sağlanır. Kırılğan damgalama şemalarının bazıları, görüntüyü küçük bloklara bölerek, her bloğa işareti yerleştirir. Gömülü verilerin kapak bloklarının ana içeriğinin karması olması mümkündür. Görüntü değiştirilmiş ise değiştirilenlere karşılık gelen damga ve görüntü içeriği, bu değiştirilen blokların algılanması amacıyla eşleştirilememektedir. Saldırganın sahte damgayı içeren yasal olmayan bir görüntüyü sahtekarlık amacıyla damgalı görüntüden uygun olan blokları seçse dahi, bu damgalama yöntemi saldırılara karşı güvenliği sağlayabilmek için her bloğa kırılğan damga üretmek amacıyla iki aynı endeks bilgisi kullanılır (Zhao ve Cui, 2009).

Blok biçimindeki kırılğan damgalama şemaları, sadece değiştirilmiş olan blokları tanımlar, değiştirilmiş pikselleri ise tanımlayamaz. Bunu aşabilmek için ana piksellerin gri değerlerinden üretilen damga bilgisinin ana pikseller içine gömülen bazı piksellerde kırılğan damga şemaları önerisi yapılmıştır (Vleeschouwer vd., 2002). Bu bağlamda değiştirilmiş pikseller, taşımış oldukları damga bilgisi olmamasından dolayı tanımlanabilir. Aynı zamanda yöntemlerde yeni piksel değerlerinden türetilmiş olan bazı

bilgilerin damga ile akıřabilmesi nedeniyle, deęiřtirilmiř piksellerin yeri tamamlanmamıř, ayrıca deęiřtirme modelinin belirlenmesi hatalıdır. Bunu özümleyebilmek iin, konak görüntüsüne hassas damga düzenleme řeması özel kimlik doęrulama verisini yerleřtirir, görüntüyü doęrulamak iin istatistiksel mekanizma sunar. Deęiřiklik mukavemetinin tahmin edilmesiyle, deęiřtirilmiř piksellerin bulunması amacıyla orijinal ve deęiřtirilmiř piksellere karřılık olan farklı iki daęılım kullanılabilir.

Saęlam ya da kırılğan görünmez damga, piksel deęerindeki modifikasyonların algısal fark edilemeyecek olan, sadece uygun kod özme mekanizması yardımıyla geriye kazanılabilecek biimde gömölür (Mohanty, 2008). oklu damgalarda, ierik doęrulaması, telif hakkı koruması ya da resim yazısına iki ya da üç damga gömölü olur. Görünmez damga teknięinde saęlamlık özellięi sadece ierik korumasının garanti edilmesi iin yeterli deęildir. Özel damgalama tekniklerinin multimedya cihazlarında olan standart kod özücü sistemleriyle geliştirilmesi gerekmektedir. Standart gelişimleri olan bir kurum kurulmalıdır (Eskicioęlu ve Delp 2001).

Sayısal multimedya aęı ile görüntü ierięinin daęıtımı ve yaratılmasına eřitli avantajlar saęlanmıřtır. Fakat düzenleme ve kopyalama kolaylıęının olması nedeniyle yetkisiz kullanım, yanlış beyan ve yanlış kullanım kolaylařmaktadır. Bu konuda ierik saęlayıcıların endiřeleri bulunmaktadır. Bir görüntüye sinyal yerleřtirme eylemi olarak tanımlanabilen damga, sahip haklarını korumak amacıyla önerilmektedir (Lin ve Delp, 2005). Saydam ya da görünmez iřaretler, damgalanan görüntüde algısal bozulmayı asgariye indirmek amacıyla insan görsel sistemi özelliklerini kullanmaktadır (Lin ve Delp, 2005).

Yarı Saydam Damgalama

Görünür veya görünmez damgalama dıřındaki dięer yöntem ise logonun görüntünün büyük bölümünün üzerine yarı saydam eklenmesi řeklinde uygulanan yarı saydam damgalama yöntemi bulunmaktadır. Bu yöntemle logonun görüntüden ayrılmıř olması görüntünün anlamsızlařmasına neden olacaęından daha avantajlıdır. Fakat kullanıcıya bu řekilde görüntüyü sunmak dezavantajdır.

2.4.2. Veri ortamına göre sınıflandırma

Sayısal damgalama tekniklerinin veri ortamına göre sınıflandırması, ana bilgisayar ve gömme için kullanılan nesne türüne göre ses, görüntü, metin ve video şeklinde sınıflandırmaya tabi tutulabilmektedir (Alasafi, 2016).

Ses damgalama

Bilgi sistemleri ile ağ tabanlı veri tabanlarında olan gelişmelerle birlikte sayısal medyada örnek olarak video, görüntü ve ses gibi büyüme hızlanmıştır. Sayısal ortamdaki kaynaklanan yüksek verimdeki manipülasyon, erişim ve çoğaltma da kısmen bunda etkilidir. Veri gizleme, verilerdeki küçük değişimlerle görüntü, ses ya da video gibi sayısal verilerde olan ekstra bilgileri kodlamayı ifade etmektedir. Bir sesi ya da görüntüyü, ek bilgiler ile destekleme ya da ses veya görüntünün bütünlüğünün doğrulanması için görüntüler ya da seslerde olan bilgilerin gizlenmesi tercih edilebilmektedir. Gizli bilgiler görüntü verileri, ses, metin ya da köprüler olabilir. Örnek olarak, bir resimde olan binaları ve yüzleri etiketlemek amacıyla metin başlıklarının kullanılması mümkündür. Bir köprü ile görüntü bölgesi diğer bir belgeye ya da veri kaynağına bağlanabilir (Boney vd.,1996).

Gömülü veriler iletildiğinde ya da saklandığında görüntüde kalır. Bunları son kullanıcının çıkarması ya da son kullanıcıya gizlenmesi hedeflenebilir. Örnek olarak, gömülü verileri bir tüketici çıkarabilir, bunları bilgi ihtiyacının karşılanması amacıyla kullanabilir. Diğer durumda gömülü veriler damga olabilir. Damga, diğer bilgilerle telif hakkını temel verilere gizlemek suretiyle sayısal medyayı etiketlemek amacıyla kullanılır. Saklanan verilerin tersine damga ile kullanıcı gömülü bilgiye erişim sağlayamaz (Boney vd., 1996).

Damga kullanımının yararlı olabilmesi için bazı gereklilikleri karşılaması gerekir. Bu gereklilikler damganın sağlam olması ve duyulmuyor olmasıdır. Tüm kriterler önem arz etse de elde edilen verilerin sağlam olması ve elde edilemezlik aralarında en önemli olanlardır. Ana veri sağlam olduğunda, gizli veriler duyulamaz. Bunun aksi durumunda ses kalitesinde düşme olur. Ayrıca sağlamlık gerekliliğinde ise, gizli verilerin gömüldüğü ortamda hayatta kalması durumu söz konusudur. Genel olarak ses verileri, yeniden örnekleme, filtreleme, gürültü, sıkıştırma, ses- sayısal, kırpma, sayısal- ses dönüşümü gibi bazı sinyal işleme işlemlerine tabi olur. Ana bilgisayar verilerinin her daim manipülasyona açık olması nedeniyle, gömülü verinin sağlam olması gerekmektedir.

Diğer bir ifade ile host verileri, gömülü veriler sinyal işleme işlemlerinden sonra da hayatta kalmalıdır (Boney vd., 1996).

Görüntü damgalama

Siyah beyaz ve renkli görüntülerin damgalanması sırasında doğrudan orijinal görüntüye damga eklenir. Görünmezliğin artırılması damganın asıl işarete bağlı olarak ölçeklenmesini gerektirir. Görüntülü damgalama tekniğinde damga, filtreleme, sıkıştırma, kırpmaya, ölçeklendirme, döndürme, A/D dönüşüm, geometrik bozulma, D/A dönüşüm gibi sıkça kullanılan işaret işleme saldırılarına dayanıklılığını koruyabilmelidir.

Metin damgalama

Bilgi güvenliği araştırma alanında sayısal damgalama 1990'lı yıllarda önerilen sayısal ürün telif hakkı koruma tekniğidir. Multimedya verileri, seri numarası, sayısal, resim, metin, logo ile diğer bilgi türlerinde yerleşik olup, telif hakkının korunmasında etkili olur. Ürünü işaretleyerek, gizli iletişimi sağlar, veri doğruluğunu belirler ve ait olduğu verileri onaylar (Ruia ve Jinqiaob, 2013). Ana metin algoritmalarının sınıflandırılması aşağıdaki gibidir:

- İçeriğe dayalı metin damgalama,
- Biçime dayalı metin damgalama,
- Doğal dile dayanan metin damgalama,
- Gösterilen önemsiz biti kaynak alan damgalama (Zhao ve Cui, 2009).

İçeriğe dayalı olan metin damgalamada daha iyi güvenlik ve sağlamlık sağlayan gömme aracına ulaşabilmek için karakter kodlaması ile değişim yapılır. Biçime dayalı metin damgalama en fazla kullanılan algoritmadır. Başlangıçtan karakter kaydırma, satır kaydırma, rengi, yazı tipini ve diğer yöntemleri değiştirebilen ilerlemeye kodlama, biçime dayalı metin damgalama oldukça etkindir (Ruia ve Jinqiaob, 2013).

İngilizce harfler yerine benzeyen Yunan harfleri kullanılır. Fakat bu teknik İngilizce için uygun olup, damgalama alanı küçük olur ve damga bilgisi daha azdır. Çince karaktere dayalı metin damgalama ise en iyi damgalama algoritmasıdır (Zhao ve Cui, 2009). Temsil edilemeyen esaslarla yapılan metin damgalamada, damgayı gömmede önemsiz boşluklar ya da noktalar kullanıldığında görüntü damgası kararsız olur. İletimde damga bilgisinin

kaybedilmesi olasıdır. Bunun yanı sıra güvenlik ve sağlamlık biçime dayalı metin damgalamaya göre iyi değildir (Ruia ve Jinqiaob, 2013). Damgalama algoritmalarının aşağıdaki gibi pek çok sorunu vardır (Ruia ve Jinqiaob, 2013):

-Güvenlik yetersizdir. Damgalama algoritması bilindiği takdirde damga çıkarılabilir.

-Sağlamlık oranı düşüktür. Damga bilgilerinin değiştirilmesi için Word menüsünden işlem yapılabilir.

-İngilizce ve Çincenin karışık metinlerde geçerliliği yoktur.

-Damga kapasitesi düşüktür.

Video damgalama

Multimedya uygulamaları, yasadışı kopyalama ve sayısal video dağıtımının önlenmesi amacıyla telif hakkı korumayı zorunlu kılmaktadır. Telif hakkı koruması, korumak istenen sayısal video için logo ve sahiplik bilgileri gibi verilerin kimlik doğrulama verisi olarak eklenmesini ifade etmektedir. Videodan çıkarılabilen kimlik doğrulama verileri mülkiyetin kanıtlanması için kanıt olarak kullanılabilir. Sayısal video damgalama, bu sebeple araştırma alanında yeni bir telif hakkı koruma yöntemidir. Video damgalamada bilgiler video karelerine yerleştirilmektedir (Emek, 2006). Damgalamanın uzantısı görüntüdür. Bu nedenle görüntü damgalama tekniklerinin video damgalama içeriğine uygulanması mümkündür. Video damgalama frekans ya da uzaysal boyutta yapılabilir. Frekans boyutta olan video damgalamaya göre uzaysal boyutta video damgalama daha basit olsa da frekans boyutta yapılan damgalama daha sağlam olur ve saldırılara karşı dayanıklılığı daha iyidir (Emek, 2006).

2.4.3. Algoritma düzlemine göre sınıflandırma

Damgalama amacıyla kullanılan algoritmalar, istenen algı seviyesi ve ortam bakımından uzay düzleminde sayısal damgalama ve frekans düzleminde sayısal damgalama şeklinde sınıflandırılmaktadır. Frekans düzleminde yapılan sayısal damgalama, uzay düzleminde yapılan sayısal damgalama işlemlerinden sağlamlık bakımından daha üstündür (Thampi, 2004).

Uzay düzleminde sayısal damgalama

Uzay düzleminde sayısal damgalama işleminde damga yapılacak çalışmanın bilgisinin üzerinde değişiklik yapılmaktadır. Bu işlemlerde amaç damganın algılanmasının zor olmasıdır. Bu nedenle görüntü pikselleri parlaklık değerleri üzerine küçük değişimler yapılmaktadır. Pikselin parlaklık değerine damga doğrudan eklenebilir veya damga parlaklık değerinin düşük anlamlı bitine ek yapılabilir (Oğuz, 2006).

Uzaysal teknikler, piksellerde değiştirilmiş bitler ya da piksellerin sayısının değiştirilmesi gibi, görüntü içerisindeki karakteristik özelliklerin değiştirilmesi ve kapak görünümüne bir logo ya da işaret yerleştirilmek için kullanılan tekniklerdir (Le vd., 2010). Bu amaçla pek çok teknik kullanılmıştır. Bir logo veya işaretin gizlenmesi amacıyla kullanılan en güçlü tekniklerden biri bu olmasına rağmen, görüntünün görselliğini olumsuz şekilde etkileyebilir.

Frekans düzleminde sayısal damgalama

Frekans düzleminde sayısal damgalama, bu alandaki araştırmaların önemli bir kısmını oluşturmaktadır. Bu işlemde damgalama yapılacak çalışma ilk aşamada frekans bileşenlerine ayrılmaktadır. Çalışmanın frekans bileşenlerine ayrılması için ayırık dalga dönüşümü, ayırık kosinüs dönüşümü, hızlı fourier dönüşümü gibi dönüştürme araçlarından yararlanılır. Damgalama yapılacak bilginin görüntüde JPEG gibi kayıplı sıkıştırmaya daha dayanıklı olması amacıyla ayırık dalga dönüşümü tercih edilmektedir. Bu şekilde elde edilen katsayılar ve frekanslarda değişiklik yapılarak, ters dönüşüm formülü ile damgalanmış ürün elde edilir (Oğuz, 2006).

2.5. Sayısal Damgalama Yöntemleri

Bilgisayar ortamında bulunan verilerin damgalanması amacıyla pek çok yöntem geliştirilmiştir. Sayısal damgalama yöntemleri, çalışmanın türüne, algoritma düzlemine ve algıya göre üç ana başlıkta ele alınabilir. Bu yöntemler de kendi içerisinde alt gruplara ayrılmaktadır. Damgalama yöntemlerinin her birinin kendisine özgü özellikleri vardır. Bu başlık altında sayısal damgalama yöntemleri hakkında bilgilere yer verilecektir.

2.5.1. LSB yöntemi

LSB, damgalamanın en yaygın şekilde uygulanan yöntemidir. Bu yöntem orijinal medyada önemsiz bitlere filigran gizleme mantığına dayanmaktadır (Sharma ve Rajni, 2012). LSB yönteminde filigran bit dizisine dönüştürülerek, her bit orijinal medyadaki piksel değerlerinden en az önemsiz olan bit değeri ile değiştirilmektedir. Bu yöntemin karmaşık işlemlerinin az olması, İnsan Görme Sistemi (İGS) ve İnsan İşitme Sistemi (İİS) ile algılanamazlığının yüksek olmasından dolayı sayısal damgalamada en fazla tercih edilen yöntemdir (Simmons, 1984; Doğan, 2011). Fakat LSB yöntemi, sağlamlık ve algılanamazlık arasında bulunan ters orantı nedeniyle, ortalama filtreleme, bit silme gibi saldırılara karşı dayanıksızdır (Abdülkhaev, 2016). Aynı zamanda Birleşik Fotoğraf Uzmanları Grubu (JPEG) sıkıştırmasına da dayanıklı değildir (Patel vd.,2013). Uygulamaların bazılarında daha fazla veri yükünün elde edilmesi amacıyla orijinal medyada her blokta veri en önemsiz olan iki ya da üç bitine gömülmektedir. Fakat bu veri yükünü arttırmakta, orijinal medyada bozulmaya neden olmakta ve algılanamazlığı ise düşürmektedir (Geetha ve Muthu, 2010).

LSB damgalama yöntemi diğer adı ile en önemsiz bite ekleme yöntemi, uygulaması basit olan ve yaygın kullanılan bir yöntemdir (Johnson ve Katzenbeisser, 2000). Gömülecek olan veri bilginin gizleneceği görüntüdeki her pikselin en önemsiz bitine belli bir algoritmada değil, sıralı şekilde gömülür. Gömülen verinin ortaya çıkarılması sırasında metnin karakter sayısı bilinemeyeceğinden, işaret karakteri sonuna eklenir.

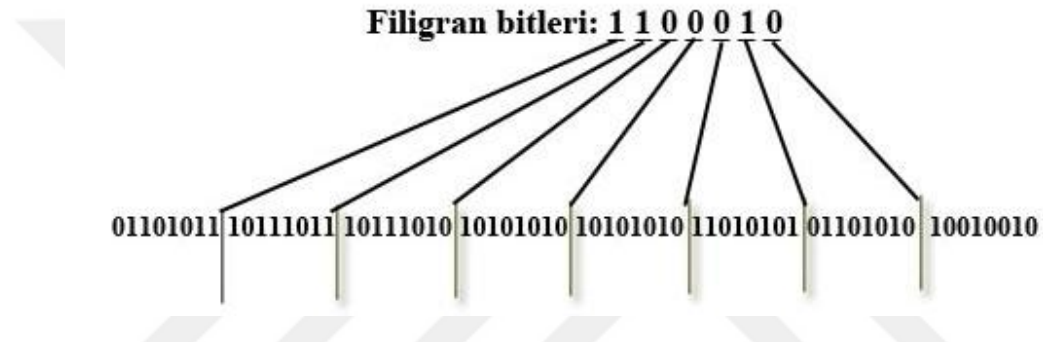
LSB damgalama yönteminin aşamaları aşağıdaki şekildedir:

- 1.Aşama: Bilgi gizlenecek ve saklanacak metni almak.
- 2.Aşama: Saklanacak olan metni ikili olarak dönüştürmek.
- 3.Aşama: Metnin bitleri bitinceye kadar 4. ve 5. adımlarını uygulamak.
- 4.Aşama: Bilgi gizlenecek metnin piksellerinin ikilik sistemde yazılması.
- 5.Aşama: Verinin gömüleceği resmin piksellerinde en önemsiz biti ile saklanacak verinin sıradaki biti ile değiştirmek.
- 6.Aşama: Stego bilgiyi yazarak, işlemi sonlandırmak.

LSB yönteminde resmin boyutuna göre belli miktarda veri gizlenmesi mümkündür. Piksel boyutu 256X256 olan bir resimde her pikselin kırmızı, yeşil, mavi renk

değerlerinde 3X256X256 uzunlukta olan bit dizisi gizlenebilmektedir. Bit dizisinin bütün renk kanalına gizlenmesi gibi tercih edilen bir renk kanalına gizlenmesi de mümkündür (Öztürk vd., 2011).

LSB damgalama yöntemi, video, ses ve resim medyalarının üzerine filigran yerleştirme işlemi yapabilmektedir. Şekil 2.4’de görüldüğü üzere her birinde orijinal medyayı farklı yöntemler ile bit dizilerine ayrılmakta, her dizine ait LSB değeri ve filigrandaki sıradaki bit yer değiştirilir (Hilewitz ve Lee, 2008).



Şekil 2.6. ASCII tablosunda “b” harfinin, bir filigran bit dizisi olarak bir başka veri dizisinin içine kodlanması

Gri tonlamalı olan görüntülerde her pikselin alabileceği 8 bit (0-255 arası tamsayı) değeri 1 bayt ile temsil edilir. Piksel sayısı küçük ise koyu, büyük ise açık tonla gösterilmektedir (Oğuz, 2006). LSB yönteminde gri onlamalı görüntünün her pikselindeki son bitine filigran biri gömülebilir. Diğer bir ifade ile gri tondaki bir görüntünün bit taşıma kapasitesi piksel sayısı kadar olduğu belirtilebilir. Renkli görüntüler üç katmanlı olup, her pikselde renk değeri ise Şekil 2.5’de görüldüğü gibi kırmızı yeşil mavi (RGB) olarak farklı üç renk tonuyla ifade edilir. Bu en fazla kullanılan RGB üç katmanlı yapıdır (Çetin ve Özcerit, 2009).

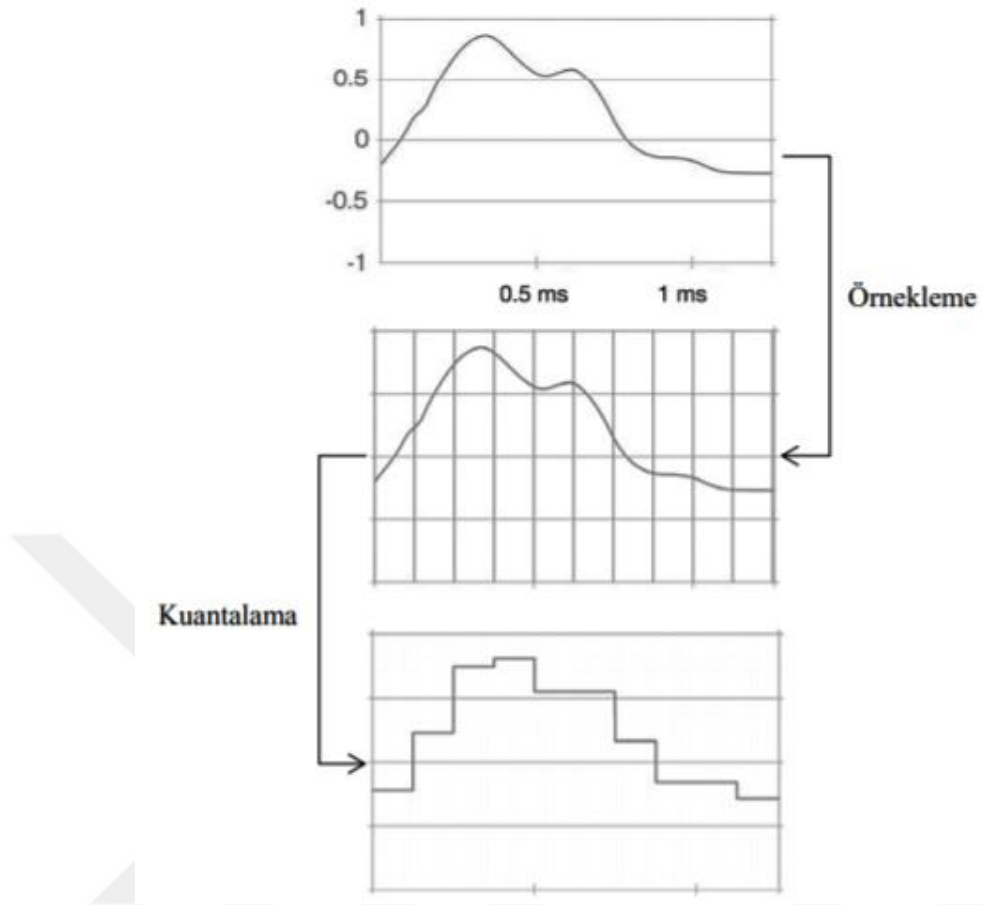


Şekil 2.7. RGB görüntüdeki kırmızı, yeşil ve mavi katmanlar

LSB yöntemi ayrı ayrı üç katmanlı görüntüdeki her katmana uygulanabilir. Bu sayede gri tonlamalı görüntüye göre üç kat veri yükü ile aynı bozulma oranıyla elde edilebilir (Tunçkanat ve Sağıroğlu, 2002). Fakat RGB görüntüdeki rastgele pikselin son bitine +1 değerli bozulma saldırısı uygulandığında, renk değeri İGS'nin algılanamayacağı oranda değişse de o pikselde filigranın biti kaybolacaktır. Bu tür saldırılarla karşı LSB yöntemi dayanıksızdır (Uçar, 2014).

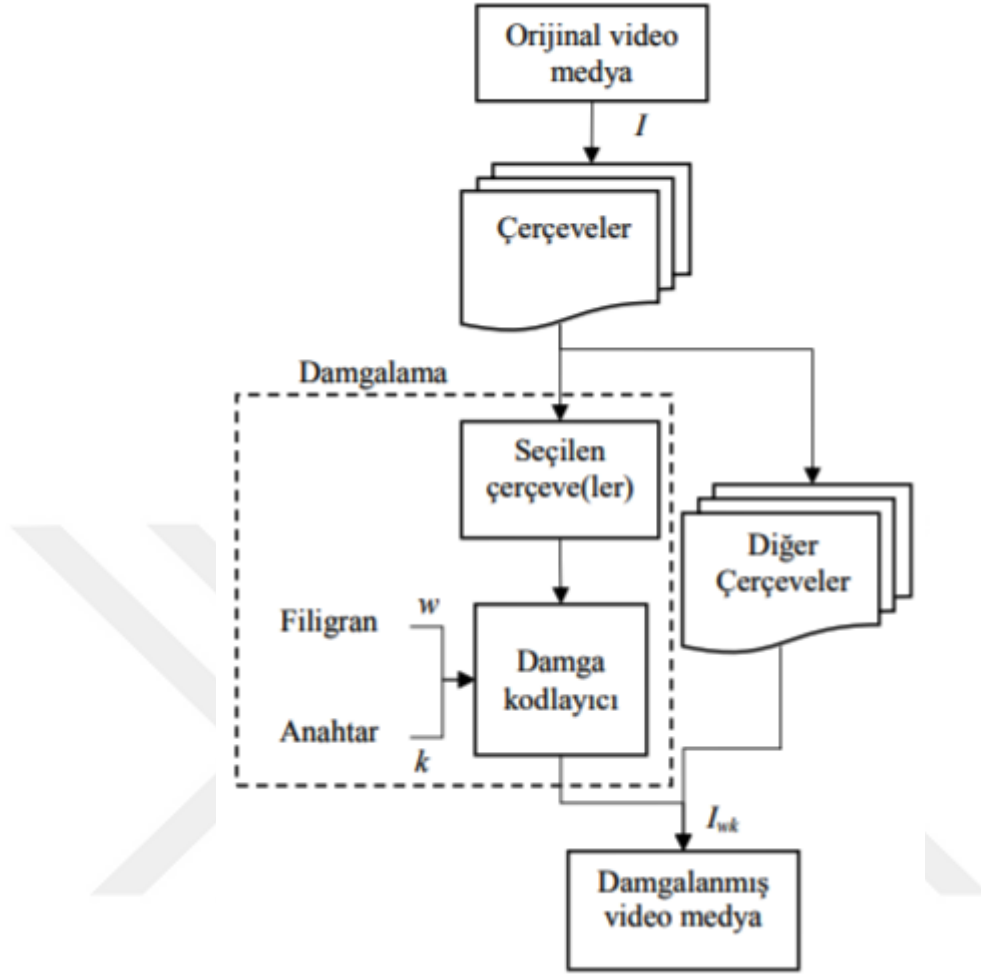
Orijinal medyanın bir ses medyası olması durumunda LSN damgalama yöntemi ile yüksek oranlarda filigran verisi gömülebilir. Bu durumda kodlama kapasitesine bağlı olarak veri yükü değişmektedir. Kodlama kapasitesinin yüksek olması halinde filigran iletim kanalında oluşan görüntüden kolay etkilenecek bozulabilir. Fakat sayısal iletim yapılacak alanlarda ses analog yerine ikili tabana dönüştürülerek iletildiğinden, gürültü ve bozulma olmayacak, LSB yöntemi fayda sağlayacaktır (Raggo ve Hosmer, 2012).

Analog bir sinyale LSB uygulanması için öncelikle sinyalin sayısal veri dizisine dönüştürülmesi gerekmektedir. Bunu yapabilmek için ses sinyalinin istenen frekans değerine örneklenmesi gerekir. Şekil 2.6'da olduğu gibi örneklenen ses sinyali daha sonra β bit sayısı kuantalama yardımıyla ikili veri dizisine dönüştürülmektedir (Koyun ve Macit, 2018). Bu şekilde β bitlik veri blokları elde edilir. LSB her bloğa uygulanarak, aynı algoritmanın tersi ile damgalanmış ses sinyali oluşturulur.



Şekil 2.8. Ses sinyalinin örneklenmesi ve kuantalanması

Video medyalarında da LSB yöntemi sıkça kullanılmaktadır. Video medyası LSB için durağan bir imge şeklinde kullanılabilir. Bunu sağlayabilmek için video çerçevelere bölünmektedir. Bu çerçevelerin her biri görüntü olup, istenenler LSB için seçilir (Al-Salihi ve Koç, 2017). Şekil 2.7’de görüldüğü üzere filigran ve seçilen çerçeveler sayısal formdaki veri dizisine dönüştürülmektedir. Filigranın hangi renge ve çerçeveye gömüldüğü alıcı tarafa bir anahtar ile bildirilmelidir (Dasgupta vd., 2012).



Şekil 2.9. LSB yöntemiyle video damgalama blok diyagramı

Durağan bir imgeye göre videoların veri yükünün daha fazla olmasından dolayı farklı yöntemler geliştirilmesi mümkündür. Sağlamlığın artırılması amacıyla genelde seçilen çerçevelerin sadece bir renk paletine filigran gömülmesi tercih edilir. Ardından çerçevelere birleştirilir ve damgalanmış video oluşturulur.

2.5.2. DCT yöntemi

Ayrık Kosinüs Dönüşümü (DCT) yönteminin damgalama için kullanımı ilk olarak Koch ve Zhao tarafından önerilmiştir (Koch ve Zhao, 1995). Bilgi sıkıştırma kapasitesinden ve giriş verilerinden bağımsız olduğundan damgalamada DCT yöntemi sıklıkla kullanılır. Özellikle sıkıştırma ve hesaplama verimliliği, frekans uzayında enerji dağılımının uygunluğundan dolayı, MPEG, JPEG gibi çok sayıda video ve görüntü kodlamada temel aşama olmuş, görüntü işlemede yaygın kullanılan dönüşüm yöntemidir (Ling vd., 2010). DCT yöntemi kosinüs dalga formu ile orijinal sayısal veriyi frekans alanına eşlemekte,

Ters Ayırık Kosinüs Dönüşümü ile frekans etki alanında verileri uzamsal alana geriye aktarır (Tsai ve Yang, 2017).

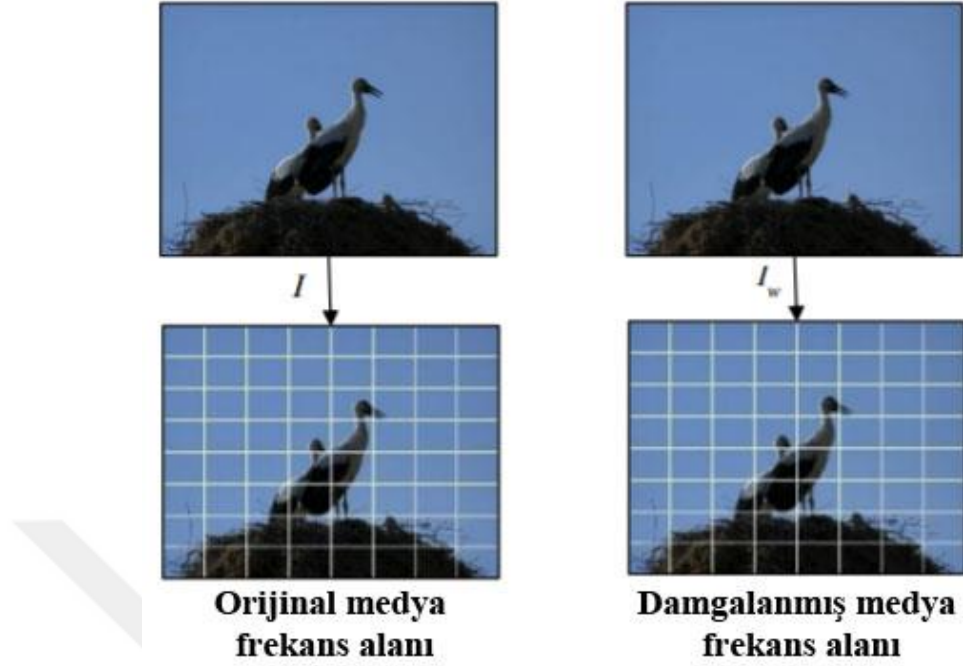
İki boyutlu DCT iki boyutlu NxM piksel görüntüye uygulanır ve NxM boyutunda olan DCT katsayıları elde edilmektedir (Barni vd., 1998). Damgalamada genelde medya 8x8 piksel büyüklüğünde olan bloklara ayrılır, her bloğa ayrı DCT uygulanır. Dönüşüm ile enerjinin önemli bir kısmı az miktardaki dönüşüm katsayısında toplanır (Baskut, 1990). Dönüşüm katsayılarının kullanımı damgalama, sıkılaştırma ya da farklı uygulamalarda olabilir (Doğan, 2011). DCT yöntemi, analog bir sinyali frekans bileşenlerine dönüştürmektedir. DCT, her imgeyi farklılaşan frekanslar ve büyüklüklerden meydana gelen sinüzoidler olarak görmektedir.

$$y(i, j) = \sqrt{\frac{2}{M}} \sqrt{\frac{2}{N}} a_i a_j \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} x(m, n) \cos \frac{(2m+1)i\pi}{2M} \cos \frac{(2n+1)j\pi}{2N} \quad (2.1)$$

Yukarıdaki denklemde x; NxM piksel giriş sinyali olduğundan, DCT yardımıyla elde edilen çıkış sinyali katsayıları y olarak hesaplanmıştır. x(m,n): n sütunda ve m satırda olan piksel yoğunluğu, y(i,j): DCT matrisinin j sütundaki ve i satırdaki DCT katsayısıdır (Alzaid, 2009).

DCT yöntemi, görüntü işlemede insan gözünün hassaslığının daha az olduğu düşük frekans aralıklarındaki, sinyalin enerjisinin yoğunlaştırılması açısından Fourier Dönüşümü ile ilgilidir. Bu sebeple Uluslararası Standardizasyon Organizasyonu (ISO) komitesi, görüntü sıkıştırmadaki bloke edici etkinin azaltılmak için DCT yöntemini 8X8 blok boyutlu olan JPEG standardına uyarlamıştır. Temel JPEG görüntü kodlaması ise üç prosedürden oluşmaktadır. Bunlar görüntü dönüştürme, kodlama ve nicelemedir (Tsai ve Yang, 2017).

DCT yöntemi ile damgalamada, Şekil 2.8.'de görüldüğü gibi damgalanmış nesne yanında orijinal nesneye de ihtiyaç bulunmaktadır. DCT damgalanmış nesne ile orijinal nesneye uygulanmakta ve ikisi de frekans alanına dönüştürülmektedir.



Şekil 2.10. DCT uygulanması (Orjinal ve damgalanmış medyada)

Düşük ve yüksek frekans DCT bileşenlerinden kurtularak, filigranın gömülü olduğu ve filigranla eşit olan $M1 \times M2$ piksel boyutunda olan kırpılmış alan oluşturulur. Orjinal medyadan oluşturulan kırpılmış alan ve damgalanmış medyadan oluşturulan kırpılmış alan farkı ise çıkarılan filigranı vermektedir.

DCT yöntemi, görüntülerin içine filigran eklenmesi ile bunların doğruluğunun alıcı tarafından teyit edilmesi için de kullanılmaktadır. Görüntünün içine filigran yerleştirilmesi amacıyla dijital görüntü bloklara ayrılmaktadır. Bu görüntünün üzerine DCT uygulanır. Bu aşamanın sonunda DC bileşeni elde edilerek, bununla filigran birleştirilir ve görüntü içerisine filigran yerleştirilir. Görüntünün alıcı ile paylaşılması aşamasında filigranın görüntüdeki bütünlüğü kontrol edilerek, manipülasyon olup olmadığının teyidi yapılır.

Gürültü eklenmesi ve JPEG sıkıştırılmaları uygulanan görüntülerde DCT yönteminin etkin olduğu bilinmektedir. Frekans dönüşüm fonksiyonlarını geliştirme, analizlerdeki hesaplama karmaşıklığına yol açan özelliklerin azaltılmasında etkili olmaktadır (Cochran vd., 1967).

2.5.3. DFT Yöntemi

Ayrık Fourier Dönüşümü (DFT) yöntemi, insan gözü görme duyarlılığına bağlı olarak damga spektrumu her frekans bandında şekillendirebilmeyi sağlar. DFT yöntemi ile yapılan damgalama uygulaması özellikle ötelemede dayanıklılığı sağlamaktadır. İlk aşamada DFT görüntüye uygulanır ve frekans uzayında temsil edilmektedir. Damga görüntüde DFT katsayılarının gerçel veya genliğine eklenebilir (Solachidis ve Pitas, 2001). Damga ekleme amacıyla DFT katsayılarının fazının kullanılmamasının temel nedeni ise insan gözünün fazda olan değişimlere oldukça duyarlı olmasıdır. Diğer aşamada DFT katsayıları değiştirilmiş olan görüntüye ters DFT uygulanır ve damgalanmış görüntünün elde edilmesi sağlanır.

2.5.4. DWT Yöntemi

Ayrık Dalgacık Dönüşümü (DWT) yöntemi, dalgacık olarak tanımlanan ana sinyali matematiksel, frekans ve zaman bandında küçük dalgalara bölerek, bunlarla işlem yapar. Dalgacıkların diğer damgalama yöntemlerine göre üstünlüğü, daha küçük zaman dilimlerinde oluşan küçük ama sonucu etkileyebilen dalgalanmaları incelemeye olanak sağlamasıdır. Dalgacıklar, veriyi frekans bileşenlerine ayıran, kendi ölçekleri ile eşleştirilen çözünürlüğe sahip bileşenlerde çalışan matematiksel fonksiyonlar olarak tanımlanabilir. Dalgacık dönüşümüyle fonksiyon frekans bileşenlerine bölünerek, imgeler ya da fonksiyonlar farklı bileşenlere ayrılarak, her bileşen üzerinde ayrı çalışılabilir (Elmas, 2006). Dalgacık dönüşümü, Joseph Fourier tarafından geliştirilmiş olan FT'ye dayanmaktadır (Doğan, 2011).

DWT yöntemi, sürekli dalgacık dönüşümünde işlem ve veri kapasitesinin büyük olmasından dolayı işlem verimliliğinin artırılması amacıyla ölçek ve konumların ikili kuvvetlerinin alınması işlemi olarak tanımlanmaktadır. Sürekli dalgacık dönüşümünde her ölçek ve öteleme değerinde hesaplama gerektiğinden, gereksiz işlemlerden kaçınılması için ölçek ve öteleme değerleri ayrıştırılır ve sürekli dalgacık dönüşümünden ayrık dönüşüme geçiş sağlanır (Misiti vd., 1996).

Mallat tarafından 1988'de filtreler kullanılarak ayrık DWT geliştirilmiştir. Pek çok işarete, işarete ait olan bilgi önemli oranda düşük frekanslı bileşenlerde tutulmaktadır. Ayrıntı ve/veya gürültüyü temsil eden bilgi ise yüksek frekanslı bileşenlerde tutulmaktadır. Örnek vermek gerekirse, insan sesinden yüksek frekanslar çıkarıldığında

ses deęiřimi olurken, kiřinin syledięi anlařılabilmektedir. Ancak dřk frekansların ıkarılması durumunda ise anlamsız ses duyulması rneęinden dřk ve yksek frekansların ierdikleri bilgi daha aık anlařılabilir (Misiti vd., 1996).

Ayrık Kosins Dnřmnde DWT uygulaması sırasında mesaj ve resim frekans boyuna dnřtrlmektedir. DWT tařıyıcı resmi alak frekans ve yksek frekans olarak iki frekans dalgasına ayrıřtırmaktadır. Az veri saklanacak ise nitelik, zellik tařıyan yksek frekans idealdir. Zira bu blgedeki deęiřimler tařıyıcı resmin insan gz ile belirlenebilecek bozulmalara neden olabilir. Yoęun bilgi saklamada dřk bant tařıyıcı olarak seilebilir. Bu blmde ok veri bulunduęundan, bu ok veriyi saklayabilme anlamına gelmektedir. Ancak kapasitenin ařılmaması ve bozulmalara dikkat edilmesi gerekmektedir. Fakat dřk frekans olarak tařıyıcı bant seilmesinin dezavantajları da bulunmaktadır. Bunların yksek frekans kadar saęlamlıęı yoktur. Yksek frekansta veri saklanmasının fark edilebilirlięi azdır. Bu nedenle blgedeki deęiřimler enerji deęerlerinin deęiřmesine yol amaktadır (Dalvi ve Kamathe, 2014: 4).

DWT yntemi grnt damgalamada İGS'nin yn baęımlı olan zelliklerini yansıtmaktadır. İnsan gz, grntdeki yumuřak alanlarda olan bozulmalara, kenarlar ve dokulu kısımlarda olan bozulmalara gre daha duyarlı olur. Bu nedenle damganın grntnn kenarları ve dokulu kısımlarına eklenmesi uygun olacaktır (ztrk, 2009). Aynı zamanda uzamsal alana gre zellikle ses damgalamadaki dalgacık dnřml olan damgalama yntemleri daha iyi sonular vermektedir (Rachid, 2014).

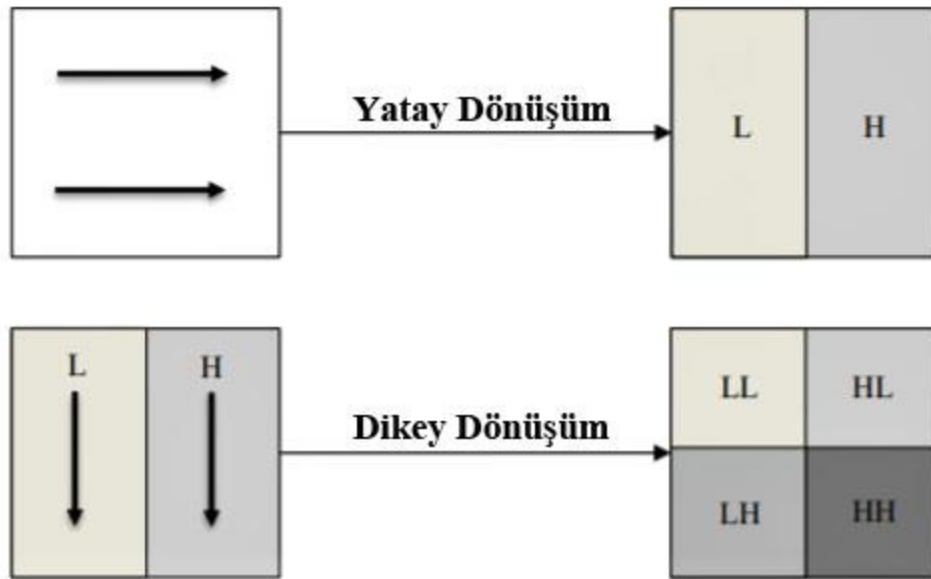
DWT yntemi, frekans ve uzamsal alanda damgalamanın zelliklerini beraber tařır (Mehta vd., 2013). Orijinal medyadaki dřk ve yksek frekans alanların ayrıřtırılması ve grntnn grltden temizlenmesi amalanmaktadır. Bu sayede filigran grntye ait olan, grlt olmayan blgeye gmlebilir. nemli ve nemsiz katsayılar eřik deęeri ile ayırt edilerek, filigranın gmleceęi katsayılar belirlenebilir (Elmas, 2006).

DWT yntemi genelde her katmanın boyutunun azaltılması iin kullanılır. Bir grntnn $2^i \times 2^i$ pikselde olan boyutu sonraki katmanda $2^{i/2} \times 2^{i/2}$ piksel olacak řekilde azaltılmaktadır. Bu yntemde grnt drt alt grntye dnřtrlmekte, alt grntler ise LL, LH, HL, HH olarak tanımlanmaktadır. Bu iřlemden sonra BXB bloęu olan sonu grntsne ulařılır, grnt sol st kředen saę alt křeye doęru taranarak, DWT hesaplaması yapılır. Her blok iin A matrisindeki bir satırda DWT tutarsızlıkları sıralanır.

Buna göre matris $(M-B+1) \times (N-B+1)$ satır ile $B \times B$ sütundan meydana gelecektir. N ve M girdi görüntüsü sütun ve satır sayısını ifade etmektedir. A matrisindeki satırlarda sıralama işlemi yapılır. DWT tutarsızlıkları doğrultusunda her blok aralarında karşılaştırılarak, benzer piksel alanları işaretlenir ve yazılım yardımıyla gösterilir (Yadav ve Rathore, 2012).

DWT yöntemi ile giriş sinyali Şekil 2.9’da görüldüğü gibi dört farklı frekans alt bandına ayrıştırılmaktadır:

1. Düşük – Düşük alt bandı yaklaşık orijinal kapak verisinin aynısı olmaktadır.
2. Yüksek – Yüksek alt bandı yüksek frekansları göstermektedir.
3. Düşük – Yüksek alt bandı dikey yüksek frekanslarla orijinal sinyal detayları olur.
4. Yüksek – Düşük alt bandı yatay yüksek frekanslarla orijinal sinyal detayları olur (Abdülkhaev, 2016).



Şekil 2.11. Dikey ve yatay DWT

Bu dört frekans katsayısı filigran kapak verisine değiştirilerek gömülür. Fakat gerekirse yeniden DWT uygulanır ve her defasında kendini temsil eden dört farklı alt banda yapıştırılabilir. Bu sayede çok seviyeli DWT uygulanabilir. N seviyedeki dönüşümde $3N+1$ adet toplam adet bant olur (Yavuz, 2008).

Damganın gömüleceği katsayıların seçimi DWT yöntemindeki en önemli hususlardan biridir (Pereira vd., 2001). Algılanamazlık ve sağlamlık özelliklerinin ortasında bir sonuç

istendiğinde, filigran orta frekans bölgesine gömülür (Hsieh vd., 2001). Görüntü medyalarında sağlam bir damgalama istendiğinde ise filigran genelde yüksek frekanslı olan bileşenlere gömülmektedir (Xia vd., 1997). Sıkıştırma algoritmalarının kullanımında ise filigran algoritmalarından sonra zarar görebileceğinden HH bandı tercih edilmez, ancak bu bandın keskinleştirme, kırpma, gamma düzeltme, kontrast değiştirme, histogram denkleştirme gibi saldırılara dayanıklı olduğu da bilinmektedir (Sverdlov vd., 2005).

Dokuya bağlı gerçekleştirilen manipülasyon tespiti yöntemlerinde, bu oranın artırılması önem arz etmektedir. Doku özelliklerini ortaya çıkarmak amacıyla DWT fonksiyonu kullanılmaktadır. Sınıflandırma tekniği ise blokların oluşturulmasında kullanılır. Sınıflandırma teknikleri manipüle edilmiş ve orijinal olan görüntülere ilişkin piksel boyutlarını üretmektedir. Görüntü manipülasyon tespiti yöntemlerinin dayanağı dijital görüntünün en az içerik özelliğidir. Dijital görüntüde renk özelliği, şekil boyutu özelliği ve doku özelliği olmak üzere üç temel özellik bulunmaktadır. Görüntü manipülasyon tespitinde doku özelliği en önemli olan özelliktir. Bu özelliklerin çıkarılması amacıyla özellik çıkaran algoritmalar kullanılmaktadır. Genelde özellik çıkarımında DWT kullanılması tercih edilmektedir. Bilinen en iyi doku özelliği çıkarıcısı DWT'dir. DWT, temelde yüksek frekans ile düşük frekansın birleşimi durumuna gelmektedir (Ujjiniya ve Chugh, 2016).

2.6. Saldırı Türleri

Damgalanan veri tabanının izinsiz olarak kullanımı hedefleyen saldırganların damga verisinin tümünü ya da olumsuz olarak damga çıkarım sürecini etkileyecek kadar miktarını bozma amacıyla çeşitli saldırılar düzenlemektedir. Saldırıların bir kısmı damga verisini yok etmeyi amaçlarken, bazı saldırıların amacı veriye kendi damga verilerini ekleme amacını taşımaktadır (Arnold vd., 2003). Saldırı türleri veri tabanındaki veri türüne göre farklılık göstermektedir (Patel ve Alpesh, 2014).

2.6.1. Alt küme ekleme saldırısı

Bu saldırıda saldırgan damga verisini yok edebilmek için verisini rastgele olarak oluşturduğu sütun ya da satırları veri tabanına ekleyerek saldırıyı gerçekleştirmektedir. Damganın çıkarılmasında yerleştirilmemiş olan damganın çıkartılarak, bu aşamanın başarısının azaltılması amaçlanmaktadır. Alt küme ekleme saldırısı, veri tabanındaki veriden bağımsız şekilde yapılabilecek olan saldırı türüdür (Patel ve Alpesh, 2014).

2.6.2. Alt küme değiştirme saldırısı

Bu saldırıda saldırgan tarafından belirlenen satırların sütun değerlerinde gerçekleştirdiği değişim saldırısı söz konusudur. Saldırının damga yerleştirilmiş değerlerde gerçekleştirdiği değişimde, damgalamada damga çıkarma başarısının azalması amaçlanmaktadır. Alt küme değiştirme saldırısı, veri tabanındaki veriden bağımsız şekilde yapılabilir (Patel ve Alpesh, 2014).

2.6.3. Bit değiştirme saldırısı

Bu saldırıda saldırgan belirlediği değerlerde bit düzeyinde değişiklik yapmaktadır. Saldırgan tarafından değiştirilecek olan bit sayısı ve değişimin türü belirlenmektedir. Saldırı bit değeri ya da değerleri rastgele veya bit değerlerinin tersi şeklinde gerçekleştirilebilmektedir. Bit değiştirme saldırısı, sayısal alanlar üzerinde yapılan bir saldırıdır (Patel ve Alpesh, 2014). Bit değiştirme saldırısının alt küme silme saldırısına oranla daha dayanıklı olmasına rağmen, saldırı oranının artmasıyla birlikte kaybedilen damga verisi oranının da artacağı belirtilebilir.

2.6.4. Alt küme silme saldırısı

Alt küme silme saldırısı, saldırgan tarafından veri tabanında belirlenen satırları silme ile damga verisinin yok edilmesi amacıyla gerçekleştirilmektedir. Saldırıda damga çıkarma aşamasının başarısının azaltılması amaçlanır. Bu saldırı türü damga yerleştirme yöntemlerini etkilemede en üst düzeyde başarıya sahiptir. Damgaman yerleştirildiği alanın ya da satırın yok edilmesiyle birlikte damga verisinin tam olarak kaybedilmesine neden olabilmektedir. Bu saldırı veri tabanındaki veriden bağımsız olarak yapılabilecek bir saldırıdır (Patel ve Alpesh, 2014).

2.6.5. Sahte sahiplik saldırısı

Bu saldırıda saldırgan sahiplik iddiasında bulunabilmek için kendi damgasının bulunduğu satırları veri tabanına eklemektedir. Saldırgan tarafından eklenen satırların, içerik sahibi tarafından eklenmiş damganın çıkarma başarısını düşürmesi, kendi damgasının veri sahipliği iddiasında bulunabilmesi amacıyla yapılmaktadır. Bu saldırı veri tabanındaki veriden bağımsız olarak yapılabilir (Patel ve Alpesh, 2014).

2.6.6. Satır bazlı çoklu saldırı

Bu saldırı, birden fazla saldırının arka arkaya gerçekleştirilmesi ile oluşmaktadır. Öncelikle yanlış olan damganın çıkarılması için alt küme ekleme saldırısı yapılmaktadır. Bunun neticesinde yeni veri tabanına yerleştirilen satırların yok edilebilmesi amacıyla alt küme silme saldırısı gerçekleştirilir. Bu şekilde oluşturulan veri tabanına bir değiştirme saldırısı yapılarak, damga çıkarım başarısının azaltılması amaçlanmaktadır. Tek tür saldırıları başarılı olamadığında, komplike saldırı türü satır bazlı çoklu saldırı ile damganın yok edilmesinin başarı sağladığı görülmektedir (Patel ve Alpesh, 2014).

2.6.7. Sıralama saldırısı

Veri tabanına yerleştirilen damganın bütünlüğünü bozmak amacıyla sütunların ya da satırların yerinin değiştirilmesi ile gerçekleştirilen bir saldırıdır. Damgalama yöntemlerinden bazıları damga çıkarımında sütun ya da satırların damga yerleştirmede kendi sıralarında olmaları ile başarılı bir şekilde tamamlanabilir. Sütun ya da satırlarının değiştirilmesi ile damağa çıkarımı başarısı olumsuz olarak etkilenmektedir. Sıralama saldırısı, veri tabanındaki veriden bağımsız olarak gerçekleştirilebilmektedir (Patel ve Alpesh, 2014).

2.6.8. Alan bazlı çoklu saldırı

Alt küme değiştirme ve bit değiştirme saldırılarının arka arkaya uygulanması ile alan bazlı çoklu saldırı gerçekleştirilmektedir. Bu saldırı türünde de birden fazla seviyeli saldırı sonucunda dayanıklı damga yerleştirmeye karşılık damganın yok edilmesi amaçlanır (Patel ve Alpesh, 2014).

2.6.9. Element sıra karıştırma saldırısı

Extensible Markup Language (XML) veri tutan veri tabanlarında element sıra karıştırma saldırısı gerçekleştirilmektedir. XML'nin yapısından dolayı aynı seviyede olan düğüm sıralarının değiştirilmesi ile XML verinin bütünlüğünü bozmaz. Element sıra karıştırma saldırısı ile XML veride olan düğümlerin sıraları değiştirmekte ve sıralamaya bağımlı damgalama yöntemlerine karşı başarılı olmayı amaçlamaktadır (Patel ve Alpesh, 2014).

2.6.10. Alan silme veya karıştırma saldırısı

Bu saldırı XML düğümünün alan değerlerinin silinmesi ya da düğümde sırasının değiştirilmesi üzerine kuruludur. Alan silme saldırısının amacı XML verileri tutan veri

tabanlarındaki damgalamada düğüm alanlarını kullanan diğer yöntemleri etkilemektedir (Patel ve Alpesh, 2014).

2.6.11. Etiket ad karıştırma saldırısı

XML etiketlerinin küçük- büyük harflere duyarlılığı bulunmaktadır. XML verinin bütünlüğü bozulmadan devam etmesi için veri düğümünün başlangıç ile bitiş etiketinin aynı karakterlerde olması gerekmektedir. Ancak bu sadece damga verisini etikette saklayan damgalama yöntemlerinde etkili olmakta, damga çıkarım aşamasını olumsuz olarak etkilemektedir (Patel ve Alpesh, 2014).

2.7. İlgili Alanda Yapılan Çalışmalar

İnternet erişim hızında ve internete erişen cihaz sayısının artmasıyla birlikte veri hareketliliğinin de aynı paralellikte arttığı görülmektedir. Her geçen gün küçük boyutta resim, doküman ve videolar yanında büyük boyutta olan veri tabanlarının paylaşımında artış olmaktadır. Yapıları gereği veri tabanları kolay çoğaltılabilir, içeriğinde değişiklikler yapılabilir ve tekrar yayınlanabilir. Bunun yanı sıra kullanım alanlarına bağlı olarak içeriklerin değişmesi ya da silinmesi söz konusudur. Bu gibi durumlardan dolayı veri tabanlarında sahiplik ve bütünlük kontrolü sağlanması bir sorun olarak karşımıza çıkmaktadır. Bu bağlamda alanyazında veri tabanı güvenliğinin sağlanması amacıyla sayısal görüntü damgalama üzerine çeşitli araştırmaların yapıldığı görülmektedir. Alanyazındaki çalışmalar incelendiğinde pek çoğunun sayısal alan/alanlar ile damgalama yapıldığı dikkat çekmektedir. Sayısal olmayan alanlardaki çalışmaların daha az olduğu belirtilebilir. Bu amaçla damganın değiştirilmesi ya da yok edilmesi amaçlı saldırıların çoğunun sayısal verilere odaklandığı belirtilebilir.

Muzak Şirketi tarafından alınan patent ile sayısal damgalama tarihte yerini almıştır (Hembrooke, 1954). Bu patent çalışması ile müzik dosyalarının telif hakkını koruma amacıyla kimlik kodu yerleştirilebileceği ortaya konmuştur.

Koch ve arkadaşları (1996), çoklu ortamlarda telif hakkı koruma amaçlı olarak yaptıkları çalışmalarında, orijinal görüntüyü öncelikle 8x8'lik bloklara ayırmışlardır. Her bloğa ait ayrıık kosinüs dönüşümünü alarak, damga bilgisi doğrultusunda orta frekans alanında gereken değişikliklerle damgalama işlemini yapmışlardır (Koch vd., 1996).

Yeung ve Mintzer (1997) tarafından imge doğrulama için görünmez sayısal damgalama tekniği gerçekleştirilmiştir. Bu çalışmada görüntüye damga eklenerek, içerikte herhangi bir değişimin olup olmadığının tespiti yapılmıştır.

Takai ve Mifune (2002) tarafından yapılan çalışmada damgalama işlemi Fourier hologram tekniği ile gerçekleştirilmiştir.

Shih ve Wu (2003) tarafından yapılan çalışmada frekans düzlemi ve uzay düzlemi yöntemleri bir arada kullanılmıştır. Bu şekilde sayısal görüntülerde kalitenin daha az bozulduğu damgalama tekniği kullanılmıştır. Yüksek kapasiteli damgalama için filigran ikiye ayrılmıştır. Uzay düzleminde filigranın bir bölümü az değerlikli bitlerin değişimiyle görüntüye eklenmiş, ardından uzay düzlemine damgalanan görüntüye frekans düzleminde diğer filigran bölümü eklenmiştir.

Shieh ve diğ. (2004) tarafından çalışmada DCT yöntemi ile damgalama tekniğinde değişiklik yapılacak olan frekansların belirlenmesi amacıyla genetik algoritma yöntemi kullanılmıştır. Çalışmada dayanıklı ve görünmez damgalama işlemi yapılmıştır.

XML veri saklayan alanlarda uygulanabilen yeni bir damgalama tekniği önerilmiştir. Kullanıcı tarafından belirlenen algılanabilirlik oranı ve gizliliğin önem arz ettiği veri tabanlarındaki algılanamazlığın, kapasitenin önem arz ettiği veri tabanlarındaki damgalamanın daha yüksek olmasına neden olmuştur. Alanyazında XML veri alanlarına damga yerleştiren Inoue vd., (2001), Yao vd., (2006), Darwish, (2010), Romaric, (2012) tarafından yapılmış çalışmalarda damgalama sonrasında veri üzerindeki değişim karşılaştırıldığında, uygulanan yöntem fark edilemez, orijinal veride değişime neden olmamaktadır. Bu yöntemin karakterler üzerindeki Homoglif dönüşüme neden olduğundan fark edilemezlik oranı yüksektir. Damganın çıkarılmasından sonra orijinal verinin elde edilmesi mümkündür. Ayrıca saldırılara karşı dayanıklılık düzeyi oldukça yüksektir.

Prasannakumari (2009) tarafından yapılan çalışmada damgalama işlemi veri tabanına sahte alan ekleyerek gerçekleştirilmiştir. Damga verisini içeren yeni alanın değerleri, orijinal veri alanının değerleri üzerindeki toplama işlemiyle belirlenmektedir.

Camara vd. (2014) tarafından yapılmış çalışmada orijinal veri tabanında değişikliğe neden olmadan damgalama gerçekleştirilmektedir. Önerilen yöntemde veri tabanı

gruplara ayrılmakta, her grupta yapılan matematiksel işlemlerle damga verisi oluşturulmaktadır.

Gupta ve Pieprzyk (2008) tarafından fark genişleme tabanlı damgalama tekniği kullanılarak sayısal görüntü damgalama yapılmıştır. Bu yöntem ortalama değerin genişlemesini sağlayarak, damganın sağlanmasına neden olmaktadır. Yöntem ilk defa Alattar (2004) yılında önermiştir. Resimlerde uygulanabilen, orijinal veriye geri dönmek mümkün olduğu yöntemde, komşu olan iki pikselin aralarındaki farkı değiştirme ile damgalama gerçekleştirilmektedir. Damganın çıkarılmasından sonra pikseller orijinal değerlerine sorunsuz olarak döndürülebilmektedir. Damga yerleştirilecek satırda iki alan değeri, piksel değerinin yerine kullanılmaktadır.

Darwish (2010) tarafından daha önce yapılmış çalışma kendisi tarafından geliştirilerek, damgalamada veri metnindeki karakterlerin büyütülmesinin yerine XML verisi kapatma etiketi sonuna boşluk eklemiştir (Darwish, 2012).

Romarić vd. (2012) tarafından yapılmış çalışmada rastgele üretilmiş olan damga bitlerinin veri içine gömmek amacıyla boşluk ekleme tekniği kullanılmıştır. Veri üzerindeki sorgular göz önüne alınarak, en önemli olan etiketin belirlenmesine çalışılmıştır. Bu şekilde belirlenen etiketteki veriye damga bir değerinin “0” olması durumunda boşluk eklenirken, “1” olması durumunda ise veride değişiklik yapılmamıştır.

3. MATERYAL VE YÖNTEM

3.1. Damgalama İşlemlerinde Kullanılan Materyaller

Kare kod (Quick Response, QR) bilgisayarlarda veya mobil cihazlarda okutulabilen iki boyutlu bir matristir. QR, beyaz arka plan üzerine siyah motifler konularak oluşturulmaktadır. QR mobil cihazlara internet adreslerine, e-posta içeriklerine, iletişim bilgileri gibi verileri yönlendirmede kullanılmaktadır. Görüntü damgalamada ise, görüntü içerisine imza yerleştirmede veya bilgi gizlemede kullanılmaktadır.

Bu çalışmada 12 adet kare kod (Quick Response, QR) ile damgalama işlemi yapılmıştır. Kullanılan QR kodlar ve damga yazıları şekil 3.1’de gösterilmiştir.

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ			
Boyut	29 × 29	64 × 64	128 × 128

YUSUF SELİMDAROĞLU			
Boyut	25 × 25	64 × 64	128 × 128

LEVENT GÖKREM			
Boyut	21 × 21	64 × 64	128 × 128

UĞUR ERKAN



Boyut

25 × 25

64 × 64

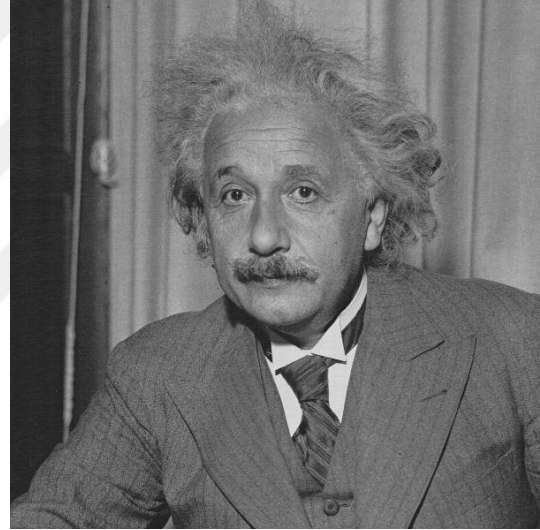
128 × 128

Şekil 3.1. Bu çalışmada kullanılan QR kodlar

Bu tez çalışması için 4 adet literatürde en çok bilinen ve boyutları birbirinden farklı “Lena-512 × 512”, “Einstein-600 × 600”, “Parrot-512 × 768” ve “Pirate-1024 × 1024” görüntüleri kullanılmıştır. Kullanılan görüntüler Şekil 3.2’de gösterilmiştir.



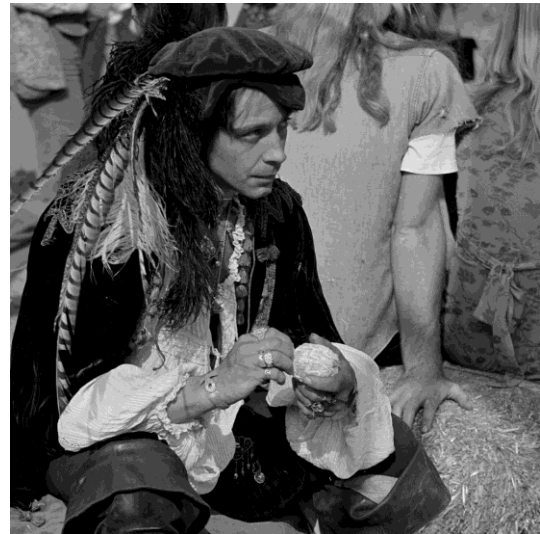
Lena



Einstein



Parrot



Pirate

Şekil 3.2. Bu çalışmada kullanılan test görüntüleri

Bu çalışmada ayrıca her görüntü için farklı SHA – 512 Hash kodları kullanılmıştır. SHA – 512 Hash kodları her yazı için Hash algoritması kullanılarak oluşturulmuştur. Oluşturulan SHA – 512 Hash kodları Tablo 3.1’de gösterilmiştir.

Tablo 3.1. SHA – 512 Hash kodları

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ	77FC46935F4327C8B01BED47E185D04EAC970909697B818B50E09A A8112C92987B3267A63EBBD2ABF4F876B6C46576D6C34928642FE 30CCAED46CF9ECE3DA3A3
YUSUF SELİMDAROĞLU	A06E6811661812595950F0040BB5AA2200BEEAABCB7FC9D7A5CF 714ED559F893C530D6C93C066EF8E9EA30C0D9CE50BBC77CC481 B562FF983B71F5B2184C0E24
LEVENT GÖKREM	07D13A476C3057D5306DD50D4ADDF52E93EF7702A0B1C4BDDCB F77E942A2D3AC9FC8219614E4FBEE8C82785E7BA44C1F17AAA8A 0E1C49D09BBF4BA197A618F71
UĞUR ERKAN	1B838F419BF3E878B3B17BE72B70A060C100075EE1A16E256894CD AB9F55F77E75B58F95B65E961786428615AC83B510F01B44046422D 2E8BCE7B3DC30243A5A

3.2. Yeni Önerilen Kaotik Harita

Euler sayısı veya matematikte ki adıyla e sayısı mühendislik ve doğa bilimlerinde çok kullanılan bir gerçel sayıdır. e sayısının tam değeri sonlu sayıda rakam ile yazılamamaktadır. e sayısı, türevi kendine eşit olan tek sayıdır. Yaklaşık değeri, 16 basamak için $e = 2.7182818284590452 \dots$ ’dir. π sayısı ise, bir dairenin çevresinin çapına bölümü ile elde edilen irrasyonel bir sayıdır. Yaklaşık değeri, 16 basamak için $\pi = 3.1415926535897932 \dots$ ’dir. e ve π sayısı ondalık kısımdan sonra bilinen bir tekrar oluşturmamaktadır. Bu iki sayı, bu yönleriyle bir kaotik dizi oluşturmak için ideal görünmektedir. Bu çalışmada, e ve π sayılarına dayanan bir boyutlu kaotik harita (One-Dimensional Map, 1D Map) önerilmiştir. Bu kaotik harita e ve π sayılarının ondalık kısımlarının öngörülemezliğinden yararlanarak iyi bir kaotik performans göstermektedir. Önerilen kaotik harita için matematiksel ifade Eşitlik 3.1’de verilmiştir.

$$x_{i+1} = \frac{(u + e^{10})x_i e^{x_i}}{\pi^{x_i}} \bmod 1 \quad (3.1)$$

Burada u kontrol parametreleridir. Bu çalışma için $u \in [0,10]$ arasında alınmıştır. Koatik haritanın performansını değerlendirmek için çatallanma (Bifurcation Diagram, BD) ve Lyapunov üssü (Lyapunov exponent, LE), permütasyon entropisi (Permutation entropy, PE), Örnek Entropisi (Sample entropy, SE) ve 0-1 testi karşılaştırmaları yapılmıştır. Karşılaştırmalarda kullanılacak 1D Map'ler Tablo 3.2'de gösterilmiştir. Tablo 3.2'de gösterilen karşılaştırma numarası, grafiklerdeki numarayı temsil etmektedir.

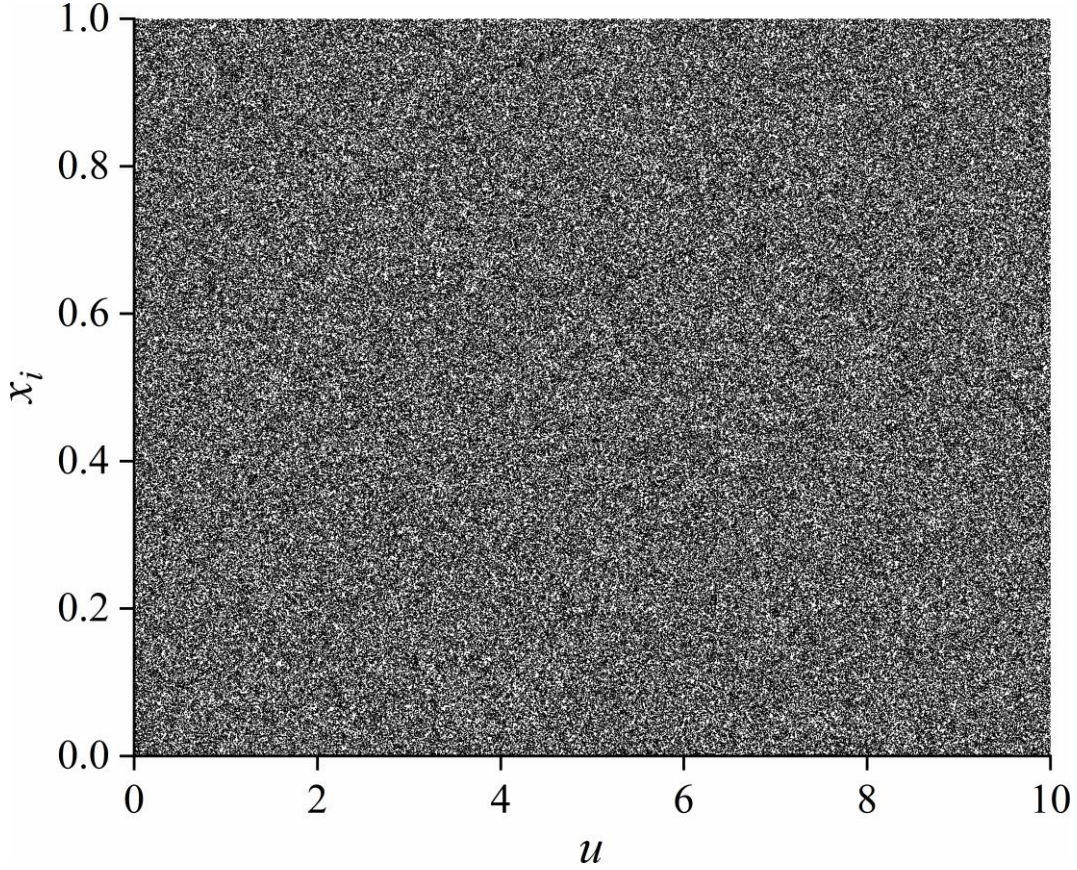
Tablo 3.2. Kaotik harita karşılaştırma tablosu

Karşılaştırma Numarası	Yıl	Kaotik Üretici	Referans
[1]	2019	$x_{i+1} = ux_i(1 - x_i)(1 - x_i^2)$	(Hanis ve Amutha, 2019)
[2]	2020	$x_{i+1} = (x_i(u + 1))^{\sin(\beta\pi + x_i)}$	(Mansouri ve Wang, 2020)
[3]	2020	$x_{i+1} = (u(3 + 2\lambda)(1 - \sin(\pi x_i))) \bmod 1$	(Wang ve Liu, 2020)
[4]	2021	$x_{i+1} = \frac{\cos((ux_i + 1)^2 + 1)}{\sin((ux_i + 1)^2 + 1) + 2}$	(Midoun ve Wang, 2021)
[5]	2021	$x_{i+1} = \begin{cases} \frac{1}{x_i^2 + \alpha} - \beta x_i & \text{if } x_i \in [0, \frac{1}{\alpha}] \\ \frac{-1}{x_i^2 + \alpha} - \beta x_i & \text{if } x_i \in [\frac{-1}{\alpha}, 0) \end{cases}$	(Talhaoui ve Wang, 2021)
[6]	2022	$x_{i+1} = ue^{x_i^3} + (1 - u)e^{x_i} \bmod 1$	(Yahi ve Bekkouche, 2022)
[7]	2022	$x_{i+1} = \frac{(u + e^{10})x_i e^{x_i}}{\pi^{x_i}} \bmod 1$	Yeni Önerilen

3.2.1. Çatallanma Diyagramı ve Lyapunov üssü

Çatallanma diyagramı, doğrusal olmayan sistemlerin kaotik davranışlarını izlemekte kullanılan, kaotik haritanın kontrol parametrelerine karşı duyarlılığını gösteren görsel bir araçtır. Çatallanma diyagramı oluşturmak için, kontrol parametresi belli aralıklara bölünür. Daha sonra kontrol parametresinin her bir değeri için bir kaotik dizi üretilir. Kontrol parametresi değerlerine karşılık gelen kaotik dizilerin grafiği çizilerek çatallanma diyagramı oluşturulmaktadır. Eğer çatallanma diyagramında belli bir yerde toplanma varsa ve belli bölgeler boşsa, bu durumda kaotik harita iyi bir kaotik performans göstermiyordur. Yeni önerilen haritaya ait çatallanma diyagramı Şekil 3.3'de gösterilmiştir. Çatallanma diyagramından görüldüğü gibi, yeni önerilen kaotik harita kontrol parametresinin $u \in [0,10]$ aralığı için hiçbir bölgede toplanma yapmamıştır. Tüm

bölgeleri doldurmuştur. Bu durum yeni önerilen kaotik haritanın yüksek bir kaotik performans sergilediğini göstermektedir.



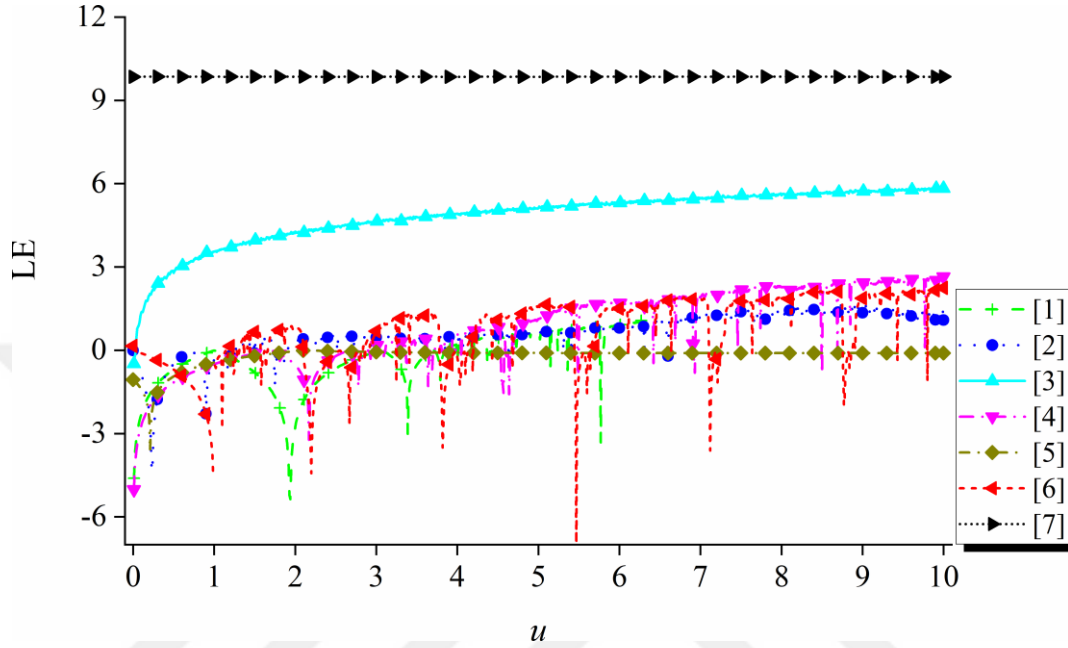
Şekil 3.3. 1D-kaotik Harita Çatallanma ve Lyapunov Üssü Diyagramı a) Çatallanma, b) Lyapunov Üssü

Lyapunov Üssü (Lyapunov Exponent, LE) kaotik sinyali incelemede en temel araçlardan birisidir. LE, bir sistemin öngörülebilirliği ve başlangıç parametrelerine duyarlılığını ölçmektedir (K. Briggs, 1990). LE matematiksel olarak;

$$\lambda = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^{n-1} \ln|f'(x_i)| \quad (3.2)$$

burada $f(x_i) = x_{i+1}$ ve n kontrol parametresinin belirli bir değeri için yineleme sayısıdır. Pozitif bir λ 'nın anlamı, başlangıç koşullarında ufak bir değişikliğin üretilen kaotik haritada büyük değişikliğe yol açacağını göstermektedir. Eğer $\lambda > 0$ ise sistem kaotiktir ve başlangıç koşullarına duyarlıdır. $\lambda < 0$ ise sistem kaotik değildir. Şekil 4.4'de yeni önerilen kaotik harita ve literatürdeki güncel 1D kaotik haritaların LE grafikleri verilmiştir. Yeni önerilen kaotik harita en yüksek λ değerlerine sahiptir. $u \in [0,10]$ kontrol parametresinin tüm değerleri için sistem kaotik davranış sergilemektedir. Yeni

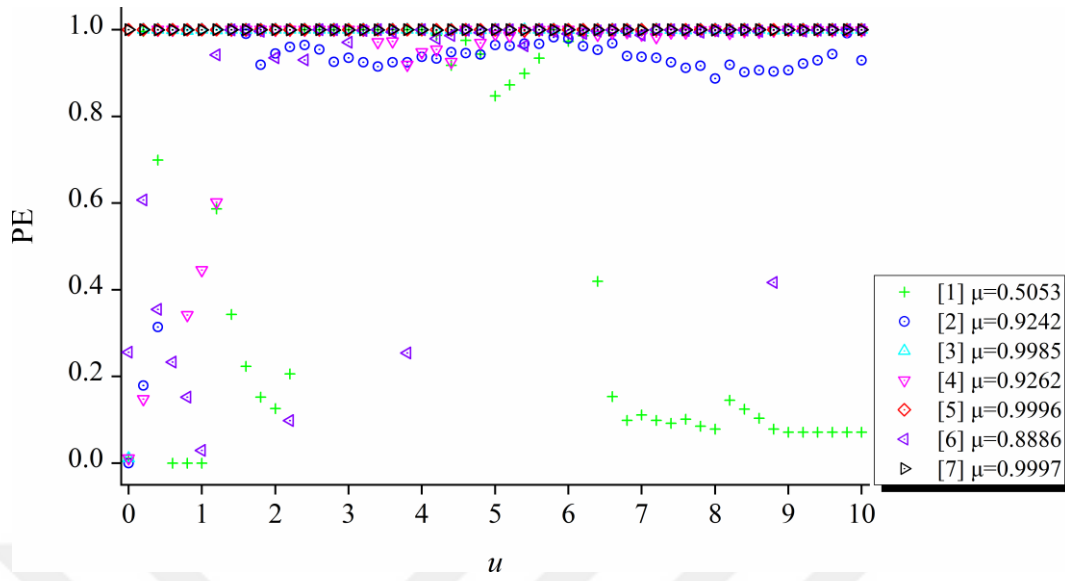
geliştirilen kaotik harita daha karmaşık yörüngelere sahiptir ve bu nedenle çıktıları daha tahmin edilemezdir.



Şekil 3.4. Lyapunov Üssü

3.2.2. Permütasyon entropi

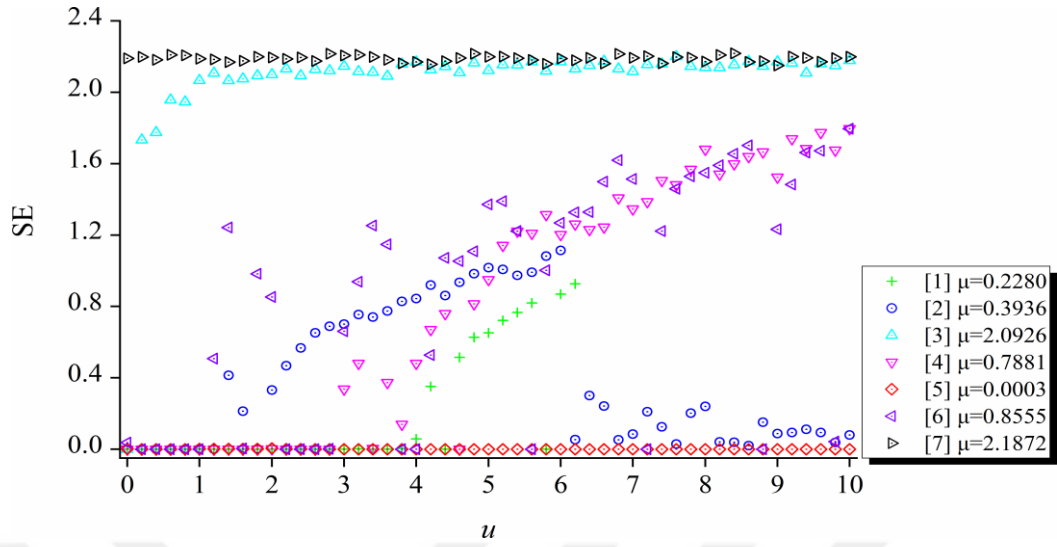
Permütasyon entropi (Permutation Entropy, PE), zaman serilerinin karmaşıklığını ölçmek için geliştirilmiş bir ölçüsüdür. PE kaotik haritaların oluşturduğu kaotik dizilerin içerisindeki değerlerin sıraları arasındaki ilişkilere bakmaktadır. Daha sonra bu ilişkilerin olasılık dağılımını çıkararak, kaotik bir dizinin karmaşıklığının nicel ölçümünü sağlayan güçlü bir araçtır. Yeni önerilen kaotik harita ve literatürdeki karşılaştırmalı sonuçlar için PE sonuçları, Şekil 4.5’de gösterilmektedir. Ortalama değeri gösteren μ değerine göre, en yüksek PE değerini (0.9997) yeni önerilen kaotik harita üretmiştir. Permütasyon entropi değerlerine göre, yeni önerilen kaotik haritanın ürettiği kaotik diziler kendi içerisinde sağlam bir permütasyona sahiptir.



Şekil 3.5. Permütasyon entropi

3.2.3. Örnek Entropi

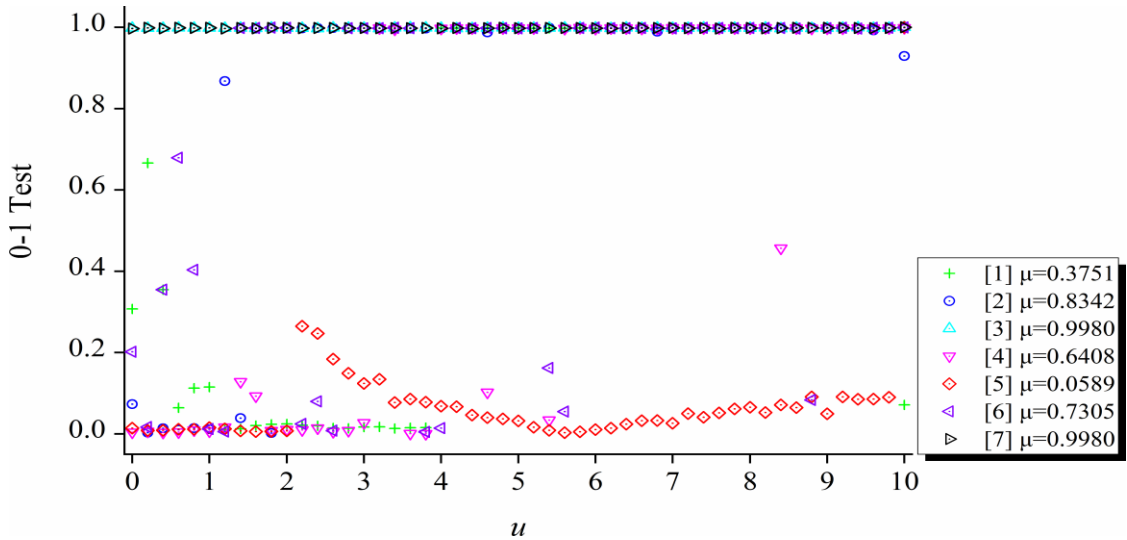
Örnek entropi (Sample Entropy, SE), zaman serilerindeki karmaşıklık seviyesini ölçmekte kullanılan entropinin bir türüdür. Kaotik bir sistemin çıktılarının karmaşıklığını nicel olarak ölçmektedir. Pozitif bir SE, üretilen dizilerin sıradan bir düzene sahip olmadığı ve kaotik davranışlar gösterdiği anlamına gelir. Daha büyük bir SE, dizinin daha yüksek bir karmaşıklığa sahip olduğunu gösterir (J.S. Richman ve J.R. Moorman, 2000). Yeni önerilen kaotik harita ve literatürdeki karşılaştırmalı sonuçları Şekil 4.6'da gösterilmektedir. Ortalama değeri gösteren μ değerine göre, en yüksek SE değerini (2.1872) yeni önerilen kaotik harita üretmiştir. Örnek entropi analizine göre, yeni önerilen kaotik haritanın ürettiği kaotik diziler yüksek düzeyde tahmin edilemezlik göstermektedir.



Şekil 3.6. Örnek entropi

3.2.4. 0-1 Testi

0–1 testi, dinamik sistemlerin kaotik durumunu belirlemek için nicel bir değerlendirme aracıdır. 0-1 testi, kaotik bir sistemin yörüngesinin büyüme oranlarını ölçmek için geliştirilmiştir. Önerilen harita ve karşılaştırmalı sonuçları Şekil 3.7’de gösterilmektedir. Yeni önerilen harita, 0.9980’lik ortalama değer ile en başarılı performansı gösteren iki haritadan biridir.



Şekil 3.7. 0-1 Test sonucu

3.3. Yeni Önerilen Dijital Damgalama Yöntemi

Bu çalışma boyunca, $A := [a_{ij}]_{m \times n}$ 8-bit gri ölçekli bir görüntüyü temsil etmektedir. Burada $i \in \{1, 2, \dots, m\}$, $j \in \{1, 2, \dots, n\}$ ve a_{ij} , $0 \leq a_{ij} \leq 255$ arasındadır. Bir

görüntünün veya kaotik dizinin tam sayı alt değerlere yuvarlanmış şekli, $\text{floor}(A) := \lfloor \text{floor}(a_{ij}) \rfloor$ ile ifade edilmektedir. $(D)_t$, D 'nin t sayı tabanında ifade edilmiştir. $\hat{A} := [\hat{a}_{ij}]_{m \times n}$, A matrisinin 2'lik sayı tabanında yazılışı göstermektedir. Algoritmalarda dijital damga uygulanacak görüntü A ve dijital damga W ile gösterilmiştir. $\dot{A} := [\dot{a}_{ij}]_{mn \times 1}$, A matrisinin sütun vektörüne dönüşmüş şeklidir. $\dot{A}^8 := [\dot{a}_{ij}^8]_{mn \times 8}$, $\dot{A}$ sütun vektörüne her bir bileşeninin 8 bite dönüştürülmüş şeklidir. $\dot{A}_{i,1:4}^8 := [\dot{a}_{i,1:4}^8]_{mn \times 4}$, $\dot{A}$ matrisinin ilk düşük 4 bitinin alınması ile elde edilen matrisi göstermektedir. $\text{reshape}(A, r_1, r_2)$, A matrisinin $r_1 \times r_2$ olarak yeniden boyutlandırılmış halini ifade etmektedir.

Bu tez çalışmasında dijital damgalama işlemi üç aşamalı bir şekilde gerçekleştirilmiştir. İlk olarak, Sha-512 koddan başlangıç değerlerinin üretilmesidir. İkinci aşama, uygulanacak dijital damganın karıştırılmasıdır. Son aşama ise, dijital damganın görüntüye uygulanmasıdır.

İlk olarak, dijital damgalama yönteminde kullanılacak kaotik haritalar için başlangıç değerleri ve kontrol parametreleri SHA – 512'lik koddan üretilmelidir. Bu çalışmada kullanılan yöntem, dijital damganın karıştırılması ve görüntüye eklenmesinde kaotik harita kullanmaktadır. Bu nedenle ikişer adet başlangıç ve kontrol parametresine ihtiyaç duyulmaktadır. Bunları üretmek için gerekli yöntem Algoritma 1'de gösterilmektedir. İlk olarak, $C = (B)_{10}$ üretilen SHA – 512 kod, onluk sisteme çevrilmektedir. 10'luk sisteme dönüşüm yapılırken 8 bitlik parçalar halinde dönüşüm yapılmaktadır. 8 bitlik bir parçanın alabileceği minimum ve maksimum değer 0 ve 255 'dir. Böylelikle $C := [c_{ij}]_{1 \times 64}$ matrisi oluşmaktadır (Algoritma 1: Satır→3). Daha sonra C matrisi içerisindeki değerler $T = \text{sum}(C)$ toplanmaktadır (Algoritma 1: Satır→4). C matrisi 4 parçaya ayrılmaktadır. Her birisi üretilecek iki kaotik haritayı oluşturmakta kullanılacaktır (Algoritma 1: Satır→5:7). Son olarak iki adet başlangıç parametresi (x_1, x_2) ve iki adet kontrol parametresi (u_1, u_2) üretilmektedir (Algoritma 1: Satır→8:11). Kaotik dizinin üretilmesi adımları Algoritma 2'de gösterilmiştir. Bir başlangıç ve kontrol parametresi alan algoritma, istenilen uzunlukta bir kaotik dizi üretmektedir.

İkinci aşama, dijital damganın görüntüye uygulanmadan önce karıştırılmasıdır. Bu karıştırma işlemi, görüntüden dijital damganın çıkarılmasını zorlaştırmak içindir. Eğer

dijital damga karıştırılmadan görüntüye eklenirse, çeşitli görüntü işleme veya saldırı metotlarıyla dijital damga görüntüden çıkarılabilir. Bu nedenle damganın piksel konumları karıştırılarak görüntüye eklenmektedir. Görüntüdeki piksellerin yerlerini karıştırmak için kaotik haritanın ürettiği dizi kullanılmaktadır. Teklif edilen kaotik harita ile bir dizi oluşturmak için, bir başlangıç değerine (x) $[0,1]$ ve birde $[0,10]$ kontrol parametresine (u) ihtiyaç duyulmaktadır. Bu değerler Algoritma 1 ile üretilmiştir. Bir görüntüdeki piksellerin yerleri değiştirilirken, ilk olarak kaotik haritanın ürettiği dizi küçükten büyüğe sıralanmaktadır (Algoritma 3: Satır→4). Sıralama yapılırken, sıralanan değerlerin indeksleri P matrisinde tutulmaktadır. Bu değerlere göre görüntü karıştırılmaktadır. Örneğin, kaotik dizi sıralandığında, Kaotik dizi sıralanırken, 15. Sıradaki değer 4. sıraya geliyorsa, görüntüdeki 15. değer 4. sıraya getirilmektedir. Kaotik dizinin indisleri kullanılarak dijital damgadaki piksellerin yerleri değiştirilmektedir (Algoritma 3: Satır→5:8).

Son aşamada, damgayı görüntüye yerleştirme kısmıdır. Dijital damga, görüntüye yerleştirilirken, görüntüdeki düşük seviye olan 4 bit kullanılmaktadır. Bunun sebebi, dijital damganın görüntüde olabildiğince az değişikliğe sebep olması içindir. Düşük 4 bir seviyesinde yapılan bir değişiklik, görüntüdeki piksel değerinde 8 azalma veya artma yapacaktır. Aynı işlem yüksek 8 bitte olsaydı, 128 azalma veya artma olarak kendini gösterecekti. Buda görüntüde büyük değişimlere yol açacak ve görüntüde değişim olduğu belli olacaktı. Bu nedenle dijital damga, pikselin düşük 4 biti kullanılarak yerleştirilmiştir (Algoritma 3: Satır→9:11). Görüntünün düşük 4 biti ile işlem yapma adımları Algoritma 3: Satır→9:12 gösterilmiştir. Damgalama işlemi yapılmadan, görüntü ve dijital damga binary (2'lik sistem) olarak yazılmaktadır. Dijital damga, görüntüde en az değişime sebep olması için bir zıplama parametresi belirlenerek yerleştirilmektedir (Algoritma 3: Satır→9:12). Görüntünün düşük 4 bitlik boyutu, dijital damganın boyutuna bölünerek $f = \text{floor}(mn/yz)$ zıplama parametresi oluşturulmuştur (Algoritma 3: Satır→14). Üretilen kaotik dizi, bu zıplama parametresi ile çarpılarak $X^3 = f * X^2$ kaotik dizi değiştirilmiştir (Algoritma 3: Satır→15). Böylelikle dijital damganın yerleştirileceği piksel konumları belirlenmiştir. Son olarak zıplama parametresine göre dijital damga görüntüye yerleştirilmiştir (Algoritma 3: Satır→16:19).

Algoritma 1: Başlangıç değerlerinin ve kontrol parametrelerinin elde edilmesi (ALG1)

```
1  Çıkış X, U
2  B =SHA-512 kod üret
3  C = (B)10
4  T = sum(C)
5  for i = 1: 4
6       $D_i = C^{16(i-1)+1:16i}$ 
7  end
8   $x_1 = T \left( \frac{\text{sum}(D_1)}{16 * 255} \right) \bmod 1$ 
9   $x_2 = T \left( \frac{\text{sum}(D_3)}{16 * 255} \right) \bmod 1$ 
10  $u_1 = 10T \left( \frac{\text{sum}(D_2)}{16 * 255} \right) \bmod 1$ 
11  $u_2 = 10T \left( \frac{\text{sum}(D_4)}{16 * 255} \right) \bmod 1$ 
```

Algoritma 2: Kaotik dizinin elde edilmesi (ALG2(x_1, u))

```
1  Giriş  $x_1, u$ 
2  Çıkış X
3  for i = 1 to mn
4       $x_{i+1} = \frac{(u + e^{10})x_i e^{x_i}}{\pi^{x_i}} \bmod 1$ 
5  end
```

Algoritma 3: Görüntüye dijital damganın yerleştirilmesi (ALG3)

```
1  ALG1 çalıştır
2   $A := [a_{ij}]_{m \times n}$  ve  $W := [w_{ij}]_{y \times z}$  oku
3   $X^1 = \text{ALG2}(x_1^1, u_1)$ 
4   $[L_1 P] = \text{sort}(X^1)$ 
5  for  $i = 1$  to  $yz$ 
6       $k = p_{1i}$ 
7       $\hat{w}_{1i}^1 = \hat{w}_{1k}$ 
8  end
9   $\hat{A} := [\hat{a}_{ij}]_{mn \times 1}$  hesapla
10  $\hat{A}^8 := [\hat{a}_{ij}^8]_{mn \times 8}$  hesapla
11  $\hat{A}_{i,1:4}^8 := [\hat{a}_{i,1:4}^8]_{mn \times 4}$  hesapla
12  $D \leftarrow \text{reshape}(\hat{A}_{i,1:4}^8, 1, 4mn)$ 
13  $X^2 = \text{ALG2}(x_1^2, u_2)$ 
14  $f = \text{floor}(mn/yz)$ 
15  $X^3 = f * X^2$ 
16 for  $i = 1$  to  $yz$ 
17      $g = x_i^3 + (i - 1)f$ 
18      $d_{1g} = \hat{w}_{1i}$ 
19 end
20  $\hat{A}_{i,1:4}^8 \leftarrow \text{reshape}(D, mn, 4)$ 
```

4. BULGULAR

Bu bölümde 4 adet QR kod için (“LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ”, “YUSUF SELİMDAROĞLU”, “LEVENT GÖKREM” VE “UĞUR ERKAN”) her bir test görüntüsündeki damgalama sonuçları verilecektir. Damgalama sonuçlarına ilave olarak pik sinyal-gürültü oranı (Peak signal-to-noise ratio, PSNR) ve yapısal benzerlik (structural similarity, SSIM) oranı sonuçları verilmektedir. PSNR ve SSIM, Eşitlik 4.1, 4.2 ve 4.3’de tanımlanmıştır.

$$PSNR := 10 \log \left(\frac{255^2}{MSE} \right) \quad (4.1)$$

burada MSE ortalama kare hata(mean squared error, MSE) yi temsil etmektedir. MSE şu şekilde hesaplanmaktadır:

$$MSE := \frac{1}{mn} \sum_{i=1}^m \sum_{j=1}^n (e_{ij} - f_{ij})^2 \quad (4.2)$$

burada $E := [e_{ij}]$ is the orijinal görüntü ve $F := [f_{ij}]$ damgalama yapılmış görüntüdür. SSIM [9] aşağıdaki gibi hesaplanmaktadır.

$$SSIM(E, F) := \frac{(2\mu_E\mu_F + C_1) + (2\sigma_{EF} + C_2)}{(\mu_E^2 + \mu_F^2 + C_1) + (\sigma_E^2 + \sigma_F^2 + C_2)} \quad (4.3)$$

burada μ_E ve μ_F ortalama piksel yoğunluğudur. σ_E ve σ_F , standart sapma ve σ_{EF} çapraz kovaryansdır. Ek olarak, $C_1 := (K_1L)^2$ ve $C_2 := (K_2L)^2$ iki sabittir. Bu çalışma için literatürde genelde kullanılan değerler olan $K_1 = 0.01$, $K_2 = 0.03$ seçilmiştir. $L = 255$ ise 8-bit gri tonlamalı görüntüdür.

PSNR ne kadar yüksek olursa iki görüntü o kadar birbirine benzerdir. PSNR için 40 ve yukarısı bir sayı, iki görüntünün neredeyse aynı olduğu anlamına gelmektedir. SSIM için ise, eğer iki görüntü aynı ise 1 değerini almaktadır. Yani SSIM değeri maksimum 1 olmaktadır. SSIM değeri 1’e ne kadar yakınsa iki görüntü o kadar birbirine benzemektedir. Bu çalışmada, orijinal test görüntüsü ile damga eklendikten sonraki görüntü arasındaki PSNR ve SSIM sonuçları verilmektedir. Dijital damgalamada en önemli hususlardan birisi, damga eklendikten sonra görüntünün çok az bir değişikliğe uğramasıdır. Bunu sağlamak için 8-bitlik bir görüntüdeki ilk 4-bit değil son 4-bit kullanılmıştır. Görüntü damgalamanın diğer kullanıldığı alanlardan birisi olan görüntüde bilgi gizleme alanında da orijinal görüntüde çok az değişiklik olması istenmektedir.

4.1. LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ Damgası Test Sonuçları

Bu bölümde “LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ” yazısı ile 3 adet 29×29 , 64×64 ve 128×128 boyutlarında QR kod üretilmiştir. Bu üretilen kodlar bu tez çalışmasında kullanılan 4 adet farklı boyuttaki test görüntüsüne önerilen algoritma ile eklenmiştir. Orijinal ve dijital damga eklenmiş görüntüler Şekil 4.1’de verilmiştir. Digital damganın boyutu büyüdükçe orijinal görüntüye benzerlik azalmaktadır. Ama 128×128 gibi büyük boyuttaki bir dijital damga eklenmiş görüntüde nerdeyse orijinal görüntüyle aynıdır.



Şekil 4.1. Lena, Einstein, Parrot ve Pirate görüntüleri için “LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ” dijital damgalaması görsel sonuçları

“LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ” QR koduna ait PSNR ve SSIM sonuçları Tablo 4.1’de verilmiştir. Tüm test görüntülerinde 29×29 damga boyutu için PSNR ve SSIM sonuçları yüksektir. PSNR ve SSIM sonuçlarının ortalaması 56.09 ve 0.9986’dır. Bu sonuçlara göre orijinal görüntüyle damgalı görüntü nerdeyse aynıdır. 64×64 boyutundaki damga için, PSNR ve SSIM sonuçlarının ortalaması 49.20 ve 0.9948’dir. Bilgi gizlemede genelde 64×64 boyutu kullanılmaktadır. Bu sonuçlara göre, önerilen algoritma bu damga boyutu için hem damgalamada hem de bilgi gizlemede kullanılabilir. 128×128 boyutu için PSNR ve SSIM ortalama sonuçları 43.35 ve 0.9741’dir. Önerilen damgalama yöntemi Yüksek damga boyutunda da tüm test görüntüleri için iyi sonuçlar vermiştir. Örneğin 512×512 ’lik düşük boyutlu “Lena” görüntüsünde 128×128 ’lik büyük boyutlu bir damgada PSNR ve SSIM sonuçları 40.85 ve 0.9609 ile tatmin edicidir.

Tablo 4.1. PSNR ve SSIM sonuçları 1

Görüntü	Damga boyutu	PSNR	SSIM
Lena	29×29	53.72	0.9978
	64×64	46.81	0.9894
	128×128	40.85	0.9609
Einstein	29×29	55.15	0.9986
	64×64	48.51	0.9939
	128×128	43.25	0.9802
Parrot	29×29	55.75	0.9982
	64×64	48.70	0.9980
	128×128	42.58	0.9643
Pirate	29×29	59.75	0.9996
	64×64	52.80	0.9978
	128×128	46.72	0.9909
Ortalama	29×29	56.09	0.9986
	64×64	49.20	0.9948
	128×128	43.35	0.9741

4.2. YUSUF SELİMDAROĞLU Damgası Test Sonuçları

Bu bölümde “YUSUF SELİMDAROĞLU” yazısı ile 3 adet 25×25 , 64×64 ve 128×128 boyutlarında QR kod üretilmiştir. Bu üretilen kodlar tüm test görüntülerine eklenmiştir. Orijinal ve dijital damga eklenmiş görüntüler Şekil 4.2’de verilmiştir. Görsel sonuçlara göre, damga eklenmiş görüntüler ile orijinal görüntü arasında görsel herhangi bir fark görünmemektedir. Damga eklenmiş görüntülerde, damgaya dair görsel bir iz bulunmamaktadır.

Original Görüntü



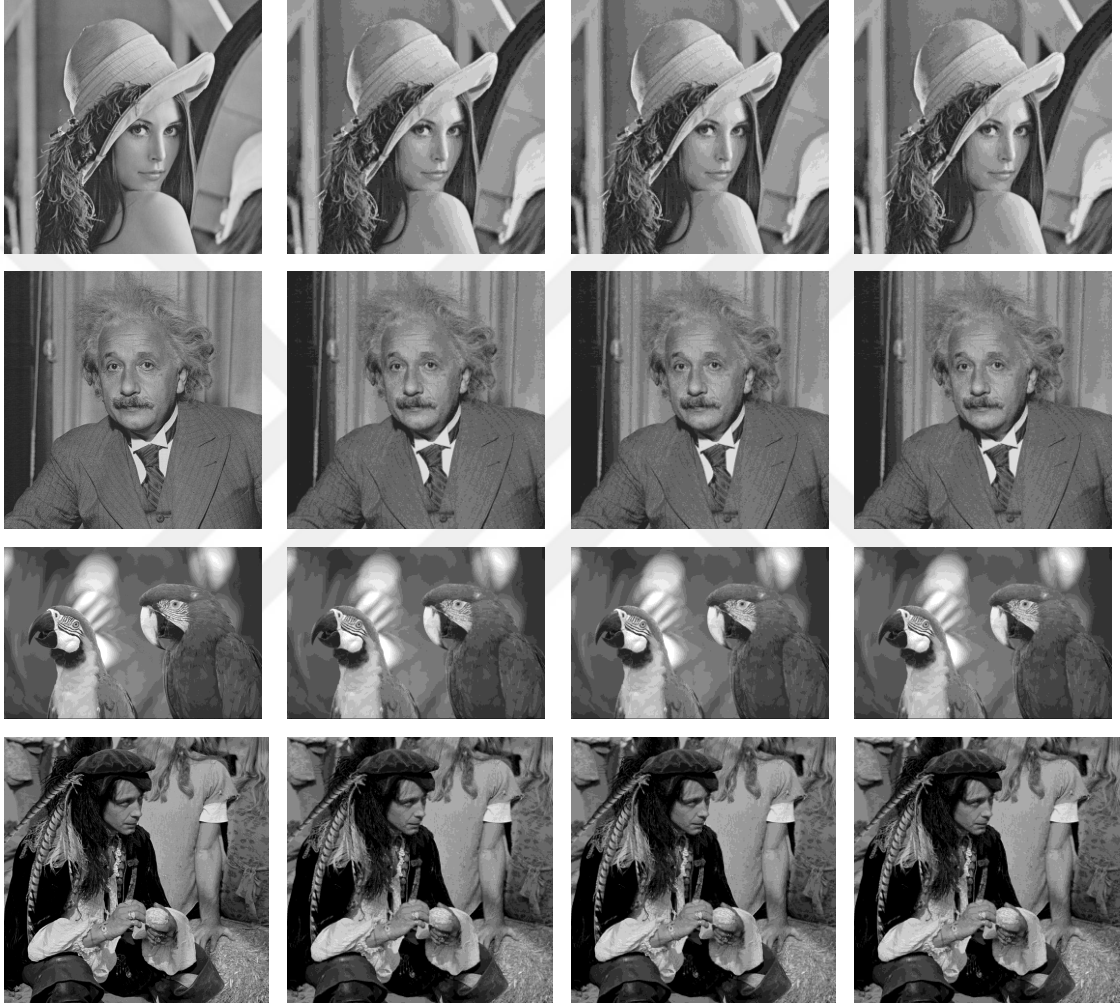
25 × 25



64 × 64



128 × 128



Şekil 4.2. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalaması görsel sonuçları

“YUSUF SELİMDAROĞLU”, QR koduna ait PSNR ve SSIM sonuçları Tablo 4.2’de verilmiştir. Tüm test görüntülerinde, 25 × 25 damga boyutu için PSNR sonuçları 50’den yüksek ve SSIM sonuçları 1’e çok yakındır. PSNR ve SSIM sonuçlarının 25 × 25 damga boyutunda ortalaması 57.38 ve 0.9989’dır. Bu sonuçlar ideal sonuçlar olan > 50 ve 1’e çok yakındır. Bu damga boyutu için önerilen algoritma gayet başarılı görünmektedir. 64 × 64’lik dijital damga için, PSNR ve SSIM sonuçlarının ortalaması 49.21 ve 0.9930’dur. PSNR sonucu ideal sonuca nerdeyse eşittir. SSIM sonucu ise 1’e 0.0070

kadar yakınlıktadır. 128×128 boyutun da ki dijital damga için PSNR ve SSIM ortalama sonuçları 43.24 ve 0.9740'dır. Bu sonuçlara göre, tüm damga boyutları için önerilen yöntem başarılıdır. Örneğin 600×600 boyutundaki "Einstein" test görüntüsünde 64×64 damga boyutunda PSNR ve SSIM sonuçları 48.54 ve 0.9939'dur. Bu sonuçlar ideal PSNR ve SSIM sonuçlarına çok yakındır.

Tablo 1.2. PSNR ve SSIM sonuçları 2

Görüntü	Damga boyutu	PSNR	SSIM
Lena	25×25	55.18	0.9984
	64×64	46.82	0.9895
	128×128	40.08	0.9606
Einstein	25×25	56.51	0.9990
	64×64	48.54	0.9939
	128×128	43.26	0.9804
Parrot	25×25	56.83	0.9986
	64×64	48.67	0.9907
	128×128	42.85	0.9641
Pirate	25×25	61.00	0.9997
	64×64	52.79	0.9978
	128×128	46.75	0.9910
Ortalama	29×29	57.38	0.9989
	64×64	49.21	0.9930
	128×128	43.24	0.9740

4.3. LEVENT GÖKREM Damgası Test Sonuçları

Bu bölümde “LEVENT GÖKREM” yazısı ile 3 adet 21×21 , 64×64 ve 128×128 boyutlarında QR kod üretilmiştir. Orijinal ve dijital damga eklenmiş görüntüler Şekil 4.3’de gösterilmiştir. Damga boyutu küçük olduğunda görsel sonuçlara göre, örneğin 21×21 boyutunda dijital damgada, damgalı görüntünün orijinal görüntüden farkı anlaşılamamaktadır. İki görüntü aynı görünmektedir.



Şekil 4.3. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalaması görsel sonuçları

“LEVENT GÖKREM”, QR koduna ait PSNR ve SSIM sonuçları Tablo 4.3’de verilmiştir. Tüm test görüntülerinde, 21×21 damga boyutu için 1024×1024 boyutunda “Pirate” görüntüsü için PSNR sonuçları 62.58 ve SSIM sonucu 0.9998 ile orijinal görüntüyle nerdeyse aynıdır. PSNR ve SSIM sonuçlarının 21×21 damga boyutunda tüm test görüntülerindeki ortalaması 58.84 ve 0.9992’dir. Bu sonuç önerilen yöntemin damgalama ve bilgi gizlemede gayet başarılı olduğunu gösteriyor. 768×512 boyutundaki “Parrot” test görüntüsünde 21×21 damga boyutunda PSNR ve SSIM sonuçları 58.57 ve 0.9990’dir. Önerilen damgalama yöntemi, tüm görüntü boyutlarında yüksek başarı ile çalışmaktadır.

Tablo 4.3. PSNR ve SSIM sonuçları 3

Görüntü	Damga boyutu	PSNR	SSIM
Lena	21×21	56.41	0.9988
	64×64	48.81	0.9895
	128×128	40.80	0.9604
Einstein	21×21	57.81	0.9993
	64×64	48.57	0.9940
	128×128	43.27	0.9803
Parrot	21×21	58.57	0.9990
	64×64	48.68	0.9908
	128×128	42.62	0.9645
Pirate	21×21	62.58	0.9998
	64×64	52.81	0.9978
	128×128	46.79	0.9911
Ortalama	29×29	58.84	0.9992
	64×64	49.72	0.9930
	128×128	43.37	0.9741

4.4. UĞUR ERKAN Damgası Test Sonuçları

Bu bölümde “UĞUR ERKAN” yazısı ile 3 adet 25×25 , 64×64 ve 128×128 boyutlarında QR kod ile tüm test görüntülerine uygulanmıştır. Şekil 4.4’de, orijinal ve dijital damga eklenmiş görüntüler verilmiştir. Şekil 4.4’e göre, dijital damgalar eklendikten sonra test görüntülerinde görsel bir değişiklik görülmemektedir.

Original Görüntü



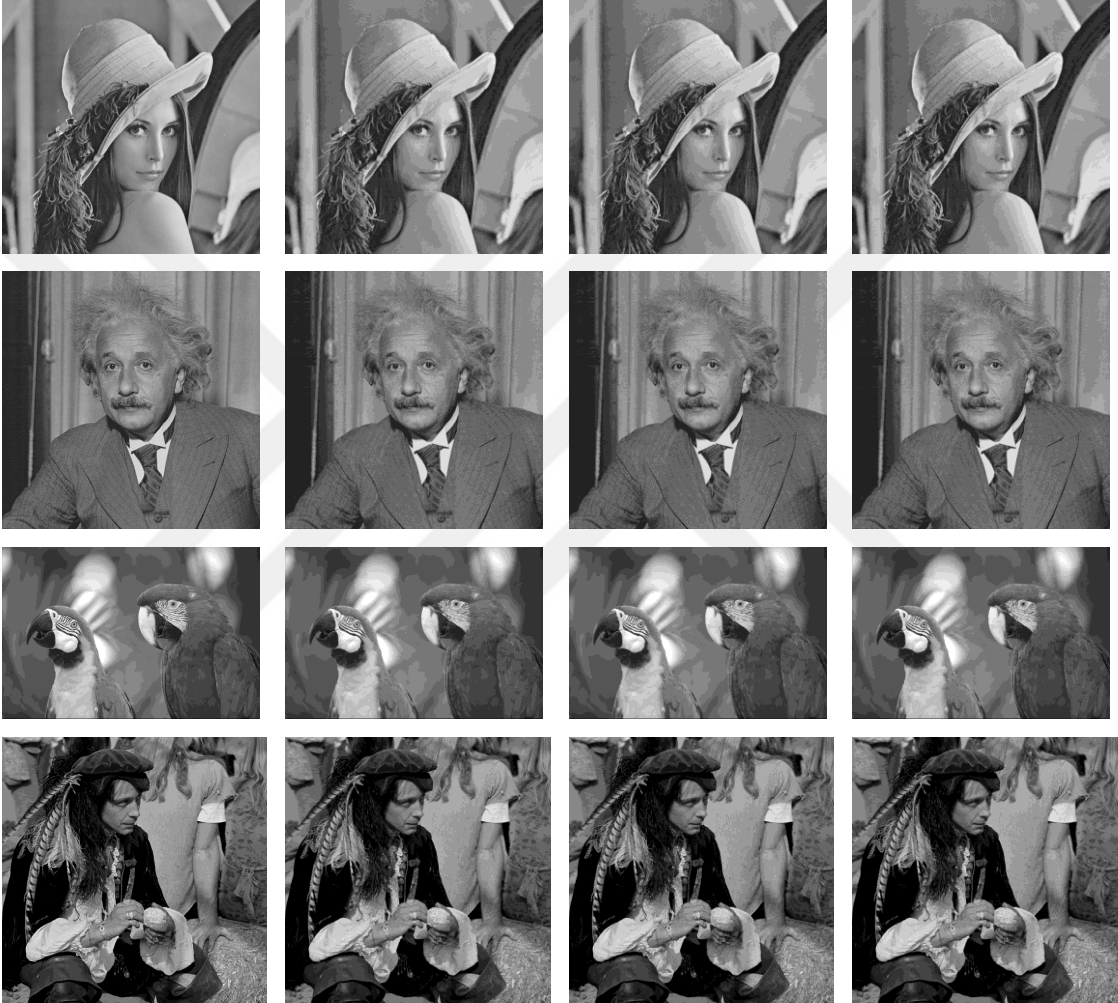
25 × 25



64 × 64



128 × 128



Şekil 4.4. Lena, Einstein, Parrot ve Pirate görüntüleri için “YUSUF SELİMDAROĞLU” dijital damgalama görsel sonuçları

“UĞUR ERKAN”, QR koduna ait PSNR ve SSIM sonuçları Tablo 4.4’de verilmiştir. PSNR ve SSIM sonuçlarının 25×25 damga boyutunda ortalaması 57.28 ve 0.9989’dur. Bu sonuçlar ideal sonuçlar olan > 50 ve 1’e çok yakındır. Bu sonuçlara göre, tüm damga boyutları için önerilen yöntem başarılıdır. Örneğin 1024×1024 boyutundaki “Pirate” test görüntüsünde 128×128 damga boyutunda PSNR ve SSIM sonuçları 43.43 ve 0.9740’dur. Görüntü boyutu yüksek olduğunda, dijital damga boyutu büyük bile olsa, önerilen yöntem başarılı sonuçlar vermektedir.

Tablo 4.4. PSNR ve SSIM sonuçları 4

Görüntü	Damga boyutu	PSNR	SSIM
Lena	25 × 25	55.10	0.9984
	64 × 64	46.97	0.9898
	128 × 128	40.88	0.9604
Einstein	25 × 25	56.31	0.9989
	64 × 64	48.45	0.9937
	128 × 128	43.25	0.9795
Parrot	25 × 25	56.71	0.9985
	64 × 64	48.71	0.9907
	128 × 128	42.67	0.9644
Pirate	25 × 25	61.01	0.9997
	64 × 64	52.93	0.9979
	128 × 128	46.94	0.9917
Ortalama	29 × 29	57.28	0.9989
	64 × 64	49.26	0.9930
	128 × 128	43.43	0.9740

Sonuç olarak, bu bölümde 4 adet test yapılmıştır. Her bir test için 3 adet damga ve 4 adet test görüntüsü kullanılmıştır. Önerilen yöntem tüm testlerde görsel sonuçlara ilave olarak PSNR ve SSIM sonuçlarıyla da doğrulanan gayet başarılı sonuçlar üretmektedir. Görüntü boyutu büyüdükçe, sabit damga boyutu için görsel kalitesi ve sayısal sonuçları artmaktadır. Bu testlerde kullanılan en büyük test görüntüsü 1024×1024 boyutunda “Pirate” görüntüsüdür. Bu boyutlarda, damga boyutu büyük bile olsa görsel ve PSNR-SSIM sonuçlarına göre sonuçlar ideale yakındır. Günümüzde dijital ve mobil teknolojilerin gelişimi ile bu boyutlar küçük olarak ifade edilmektedir. Günümüzde mobil telefonlar ile çekilen görüntülerin boyutları bu çalışmada kullanılan görüntülerden çok yüksektir. Bu çalışmada önerilen algoritma kullanılarak hem dijital damgalama hem de görüntülere bilgi gizleyerek bilgi iletimi yapılabilir. Önerilen algoritma ile eklenen bilgileri görsel olarak fark etmek çok zordur. Dijital damga permütasyon ile karıştırılarak eklendiği için hash-512’lik kodu bilmeden görüntüden çıkarmak çok zordur. Damga direk olarak görüntüye eklenmediği için ve görüntüde atlama yapılarak eklendiği için görsel veya sayısal sonuçlarla damga eklendiğini fark etmek zordur.

5. SONUÇ VE ÖNERİLER

Bu çalışmada yeni bir boyutlu bir kaotik harita önerilmiş ve bu kaotik harita kullanılarak yeni bir görünmez dijital damgalama tekniği önerilmiştir. İlk olarak önerilen yeni harita, literatürde ki bir boyutlu güncel haritalarla Çatallanma Diyagramı, Lyapunov üssü, Permütasyon Entropi (PE), Örnek Entropi (SE) ve 0-1 Test ile karşılaştırılmıştır. Yapılan

bütün testlerde yeni önerilen kaotik harita, $LE \approx 10$, $PE = 0.9997$, $SE = 2.1872$ ve $0 - 1$ Test = 0.9980 değerleri ile diğer bir boyutlu kaotik haritalara göre daha başarılı olmuştur.

Kaotik harita kullanarak dijital damga, görüntüye 2 aşamada uygulanmaktadır. İlk olarak, dijital damganın piksel konumları karıştırılmaktadır. Böylece uygulanan dijital imza görüntüden çıkarılsa bile anlamlı bir sonuç ifade etmeyecektir. Bu nedenle önerilen algoritma bilgi gönderiminde de kullanılabilir. Bu karıştırma işlemi, kaotik dizi küçükten büyüğe sıralandıktan sonra, sıralamadaki indisleri kullanılarak yapılmaktadır. İndislere göre dijital damganın piksel konumları yeni, yerlerine taşınmaktadır. İkinci olarak, dijital damga görüntünün piksellerin düşük 4 bitlik kısmına uygulanmaktadır. Bu işlem yapılırken, dijital damganın bütün piksellere homojen bir şekilde uygulanabilmesi için bir zıplama değeri hesaplanmaktadır. Daha sonra, görüntüye ait piksellerin 4 bitlik düşük kısımları alınmaktadır. Bunun sebebi, görüntünün dijital damgadan en az etkilenmesidir. Görüntünün düşük 4 bitlik piksellerine kaotik harita ve zıplama sayısı yardımıyla dijital damga uygulanmaktadır. En son, dijital damga uygulanmış 4-bitlik düşük kısım diğer 4-bitlik yüksek kısım ile birleştirilmektedir. Böylelikle dijital damgalı görüntü elde edilmektedir.

Bu çalışma için, “LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ”, “YUSUF SELİMDAROĞLU”, “LEVENT GÖKREM” VE “UĞUR ERKAN” metinlerinin her biri için 3'er adet olmak üzere toplam 12 adet kare kod üretilmiştir. Bu kare kodları eklemek için en bilinen 4 adet test görüntüsü kullanılmıştır. Her kare kod her bir görüntüye uygulanmıştır. Dijital damganın görüntüleri ne kadar değiştirdiğini ölçmek için pik sinyal-gürültü oranı (PSNR) ve yapısal benzerlik oranı (SSIM) ölçütleri kullanılmıştır. Görüntüde en az değişikliğe sebep olması için görüntüdeki piksellerin düşük 4 bitlik kısımları dijital damga uygulamada kullanılmıştır. Dijital damganın görsel etkisini en aza indirmek için, dijital damga sırayla piksellere uygulanmamıştır. Bir sıçrama katsayısı belirlenmiştir. Bu sıçrama katsayısına göre göre görüntüye dijital damganın değerleri yerleştirilmiştir. PSNR sonuçlarının çoğunluğu 50'nin üzerindedir. Dijital damga boyutu 128×128 iken 40'ın üzerine çıkmaktadır. Büyük dijital damga boyutunda bile görüntüdeki etkisi çok az olmaktadır. SSIM değerleri 128×128 dışındaki kare kod boyutlarında neredeyse 1'dir. 128×128 boyutunda ise, ortalama değerleri yaklaşık

0.9700'nin üzerindedir. Bu deęerler, grntnn grsel olarak dijital damgadan ok az etkilendięini gstermektedir.

Bu yapılan alıřmada, grnt boyutu damga boyutuna blnerek bir sırama katsayısı oluřturulmuřtur. Bu nedenle, damga boyutu ne kadar kk olursa, grnt ierisinde fark edilmesi o kadar zor olacaktır. Damga boyutu grnt boyutundan byk olduęunda damgayı yerleřtirmek imknsız olacaktır. Grnt boyutu ile damga boyutu arasında ters orantı vardır. Grnt boyutu ne kadar byk olur ve damga boyutu ne kadar kk olursa, damgalama bařarısı o kadar artmaktadır.

Gelecek alıřmalarda, ilk olarak dijital damganın etkisini daha aza indirecek yntemler geliřtirilecektir. 4 bitlik dřk bitler yerine bařka bitler semenin grnt zerindeki etkilerine bakılacaktır. Ayrıca, pikselin 8 bitlik tamamını kullanarak, bit semeye dair yntemler geliřtirilecektir. Daha ilerisinde, bu alıřmada nerilen yntem, grnt zerine bilgi gizlemede kullanmak iin daha detaylı analizler yapılacaktır.

KAYNAKLAR

- Abdülkhaev, A., (2016). *A New Approach for Video Watermarking*, Gaziantep Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Gaziantep.
- Alasafi, L. (2016). *Güvensiz Haberleşme Ortamlarında Telif Hakkı Koruma Amaçlı Dayanıklı İmge Damgalama*. (Yüksek Lisans Tezi). Süleyman Demirel Üniversitesi/Fen Bilimleri Enstitüsü/Elektrik Elektronik Mühendisliği Anabilim Dalı, Isparta.
- Al-Salihi, I., Kayhan Koç, S., (2017). A Comparative Study of LSB Based Video Steganography Techniques, *Proceedings of 12th IASTEM International Conference*, Tehran, Iran, 1-5.
- Alattar, A.M., (2004). Reversible watermark using the difference expansion of a generalized integer transform, *IEEE transactions on image processing*, 13,8, 1147-1156.
- Alzaid, A.S.A., (2009). *Digital Image Watermarking*, Brno Technical University, Faculty of Electrical Engineering and Communication, Bachelor Thesis.
- Amit Kumar, S. (2015). Robust and Imperceptible Dual Watermarking for Telemedicine Applications. *Wireless Personal Communications*, 80(4), 1415-1433.
- Anderson, R. (Ed.) (1996). *Information Hiding*. Berlin: Springer-Verlag.
- Arnold, M., Schmucker, M. ve Wolthusen, S. D., 2003, “Techniques and Applications of Digital Watermarking and Content Protection”, *Artech House*, 273, London.
- A. Mansouri, X. Wang, 2020. A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme, *Inf. Sci. (Ny)*. 520 46–62. [https://doi.org/10.1016/j.ins.2020.02.008-\(10.09.2022\)](https://doi.org/10.1016/j.ins.2020.02.008-(10.09.2022)).
- A. Yahi, T. Bekkouche, 2022. M. El Hossine Daachi, N. Diffellah, A color image encryption scheme based on 1D cubic map, *Optik (Stuttg)*. 249 168290. [https://doi.org/10.1016/J.IJLEO.2021.168290-\(03.09.2021\)](https://doi.org/10.1016/J.IJLEO.2021.168290-(03.09.2021)).
- Baker, J., Lin, T., Shahi, S. ve Jayaram, N. (2011). Draft: New ground motion selection procedures and selected motions for the PEER transportation research program.
- Barni, M., Bartolini, F., Cappellini, V., Piva, A., (1998). A DCT-Domain System for Robust Image Watermarking. *Signal Processing*, (66), 357-372.
- Baskut, A., (1990). Numerical Image Compression using The Discrete Cosine Transform, *Signal Processing*, 19(4), 346.
- Boney, L., Tewfik, A., Hamdy, K. (1996). Digital Watermarks for Audio Signals. *IEEE Int. Conf., on Multimedia Computing and Systems*, 473- 480.
- Camara, L., Li, J., Li, R. ve Xie, W., (2014). Distortion-free watermarking approach for relational database integrity checking, *Mathematical problems in engineering*.

- Cochran, WT, Cooley, JW, Favon, DL, Helms, HD, Kaenel, RA, Lang, WW, Maling, GC, Nelson, DE, Rader, CM, Welch, PD (1967). What is the fast fourier transform. *IEEE Transactions on Audio and Electroacoustics*, AU-15: 45-55.
- Çetin Ö., Özcerit A. T., (2009). A new steganography algorithm based on color histograms for data embedding into raw video streams, *Computers & Security*, (28), 670-682.
- Dalvi, A. ve Kamathe, R. S. (2015). "Color image steganography by using dual wavelet transform (dwt, swt)", *International Journal of Scientific Engineering and Research (IJSER)*, 3(7): 1-6.
- Darwish, S.M., (2010). An optimized fingerprinting system for tamper proof and copy control of XML documents, *Soft Computing and Pattern Recognition (SoCPaR), 2010 International Conference of*, 454-457.
- Darwish, S., (2012). New system to fingerprint extensible markup language documents using winnowing theory, *IET signal processing*, 6,4, 348-357.
- Dasgupta, K., Mandal, J.K., Dutta, P., (2012). Hash Based Least Significant Bit Technique For Video Steganography (HLSB), *International Journal of Security, Privacy and Trust Management (IJSPTM)*, (1)2, 1-11.
- Doğan, Ş., (2011). *Yeni bir sayısal damgalama tekniği ile biyometrik uygulamalar*, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, Elâzığ.
- Eggers, J.J., Bauml, R., Girod, B., (2002). A Communications Approach to Image Steganography, *Proceedings of SPIE (4675) Security and Watermarking of Multimedia Contents IV San Jose, California, USA*.
- Elmas, A., (2006). *Zaman-Frekans Yaklaşımı Kullanılarak Görüntü Damgalama*, İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.
- Emek, Serkan ,2006, "Sabit Görüntüler ve Video İşaretleri için Ayrık Dalgacık Dönüşümü, Ayrık Kosinüs Dönüşümü Tabanlı Sayısal Damgalama Yöntemi", Doktora Tezi, Yıldız Teknik Üniversitesi.
- Eskicioğlu A. M., Delp, E. J. (2001). An Overview of Multimedia Content Protection in Consumer Electronics Devices. *Elsevier Signal Processing: Image Communication* 16, 681–699.
- Geetha, K., Muthu, P.V., (2010). Implementation of ETAS (Embedding Text in Audio Signal) Model to Ensure Secrecy, *International Journal on Computer Science and Engineering*, (2)4, 1308-1313.
- Gonzalez RC, Woods RE. (2006). *Digital Image Processing*. 3rd ed. USA: *Prentice-Hall, Inc.*, p: 1-1022.
- Gupta, G. ve Pieprzyk, J., (2008). Reversible and blind database watermarking using difference expansion, *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, 24.
- Haşiloğlu, A. (2001). Dalgacık dönüşümü ve yapay sinir ağları ile döndürmeye duyarsız doku analizi ve sınıflandırma, *Türk J. Engin Environ Sci*, 25, ss.405-413.
- Hembrooke, E. F., (1954). United States Patent 3,004,104.

- Hilewitz, Y., Lee, R., (2008). Fast Bit Gather, Bit Scatter and Bit Permutation Instructions for Commodity Microprocessors, *Signal Processing Systems*, (53), 145-169.
- Hsieh, M., Tseng, D., Huang, Y., (2001). Hiding Digital Watermarks Using Multiresolution Wavelet Transform, *IEEE Trans., on Industrial Electronics*, 48(5), 875-882.
- Hu, Y. ve S. Kwong, S., (2001). “Wavelet domain adaptive visible watermarking,” *Electronics Letters*, vol. 37, pp. 1219-1220.
- Inoue, S., Makino, K., Murase, I., Takizawa, O., Matsumoto, T. ve Nakagawa, H., (2001). A proposal on information hiding methods using XML, The 1st Workshop on NLP and XML, 707-710.
- Jahne, B. (2005). Digital Image Processing, Springer, 6th Ed., (pp. 7-19), Berlin, 2005.
- Johnson, N., ve Katzenbeisser, S. (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Boston: Artech House.
- Jolesz F, Shtern F. (1992). The operating room of the future. Report of the national cancer institute workshop, imaging-guided stereotactic tumor diagnosis and treatment. *Invest Radiol.*; 27(4): 326-328.
- J.S. Richman, J.R. Moorman, 2000. Physiological time-series analysis using approximate and sample entropy, *Am. J. Physiol. - Hear. Circ. Physiol.* 278 2039–2049. [https://doi.org/10.1152/ajpheart.2000.278.6.h2039-\(12.12.2021\)](https://doi.org/10.1152/ajpheart.2000.278.6.h2039-(12.12.2021)).
- Katzenbeisser, S. ve Petitcolas, F.A.P., (2000). “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, INC. 685 Canton Street Norwood, MA 02062.
- Koch, E. ve Zhao, J., (1995). Toward Robust and Hidden Image Copyright Labeling, Nonlinear Signal Processing Workshop, *Thessaloniki*, Yunanistan, 1-4.
- Koch, E., Rindfrey J. ve Zhao J., (1996). Copyright protection for multimedia data, *Digital Media and Electronic Publishing*, pp. 203-213.
- Koyun, A., Macit, H. B., (2018). Generating a stego-audio data using LSB technique and robustness test, *Journal of Engineering Sciences and Design*, 6(1), 87-92.
- Kutucu, H., Dişli, A., Akça, M., (2015). Çok Katmanlı Steganografi Tekniği Kullanılarak Mobil Cihazlara Haberleşme Uygulaması, Akademik Bilişim Konferansı, Eskişehir.
- K. Briggs, 1990. An improved method for estimating Liapunov exponents of chaotic time series, *Phys. Lett. A.* 151 27–32. [https://doi.org/10.1016/0375-9601\(90\)90841-B-\(03.10.2021\)](https://doi.org/10.1016/0375-9601(90)90841-B-(03.10.2021)).
- Landini L, Positano V, Santarelli M.F. (2008). 3D Medical Image Processing. In: Neri E, Caramella D. Bartolozzi C, eds. *Image Processing in Radiology. Medical Radiology (Diagnostic Imaging)*. 1st ed. Berlin: Springer,; p:67-85.
- Le, T.H.N., Nguyen, K.H., Le, H.B. (2010). Literature Survey on Image Watermarking Tools, Watermark Attacks and Benchmarking Tools. *Second International Conferences on Advances in Multimedia (MMEDIA)*, 67-73.

- Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B., Su, J., (2011). Thwarting Audio Steganography Attacks in Cloud Storage Systems, *International Conference on Cloud and Service Computing*, 259-265.
- Liu, Y., Liu, Y., Wu, S., Zhong, S. (2015). What Makes the Stego Image Undetectable? ICIMCS '15, Ağustos 19-21, 2015, Zhangjiajie, Hunan, China, ACM. ISBN 978-1-4503-3528-7/15/08.
- Lin, E.T., Delp, E.J. (2005). A Review of Fragile Image Watermarks. *Video and Image Processing Laboratory (VIPER) School of Electrical and Computer Engineering Purdue University West Lafayette, Indiana*.
- Ling, L., Xinde, S., Leiting, C., (2010). A robust image watermarking based on DCT by arnold transform and spread spectrum, 3rd International Advanced Computer Theory and Engineering Conference, Chengdu, Çin, 20-22.
- Luo Yuling, (2019). *An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain*
- Mehta, S., Nallusamy, R., Marawar, R. V., Prabhakaran, B., (2013). A study of DWT and SVD based watermarking algorithms for patient privacy in medical images, *IEEE International Healthcare Informatics Conference*, Philadelphia, US, 9-11.
- Memon, N., Holliman, M., Yeung. M. (1999). On the Need for Image Dependent Keys in Watermarking. *Proceedings of the Second Workshop on Multimedia*.
- Mesut, A.Ş. (2019). Bilgi Gizleme Teknikleri Yüksek Lisans Dersi Notları. <https://personel.trakya.edu.tr/andacs#.XRjIz-gzY2w> adresinden 18 Kasım 2020 tarihinde erişildi.
- Misiti, M., Misiti, Y., Oppenheim, G. ve Poggi, J. (1996). Wavelet toolbox user guide, The MathWorks Inc., Natick, MA.
- Mohanty, S.P. (2008). Invisible Watermarking Based on Creation and Robust InsertionExtraction of Image Adaptive Watermarks. *Article in ACM Transactions on Multimedia Computing Communications and Applications*, 5(2), 12:1-12:22.
- M.A. Midoun, X. Wang, M.Z. Talhaoui, (2021), A sensitive dynamic mutual encryption system based on a new 1D chaotic map, *Opt. Lasers Eng.* 139 106485.
- M.Z. Talhaoui, X. Wang, 2021. A new fractional one dimensional chaotic map and its application in high-speed image encryption, *Inf. Sci. (Ny)*. 550 13–26. [https://doi.org/10.1016/J.INS.2020.10.048-\(05.08.2021\)](https://doi.org/10.1016/J.INS.2020.10.048-(05.08.2021)).
- Oğuz, C., (2006). *Görüntü İşaretleri İçin Yeni Bir Damgalama Yöntemi*, (Yüksek Lisans Tezi), İstanbul Üniversitesi/Fen Bilimleri Enstitüsü/Elektrik-Elektronik Mühendisliği Anabilim Dalı, İstanbul.
- Öztürk, S., (2009). *Kırılgan ve Dayanıklı Resim Damgalama Tekniklerinin Başarımının Zeki Optimizasyon Yöntemleriyle Artırılması*, Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, Kayseri.
- Öztürk, E., Şahin Mesut, A., ve Mesut, A. (2011). LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri. 4. Ağ ve Bilgi Güvenliği Sempozyumu, Atılım Üniversitesi, Ankara.

- Patel, M., Sajja, P.S., Sheth, R., (2013). Analysis and Survey of Digital Watermarking Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, (3)10, 203-210.
- Patel, M., Alpesh, S. (2014). The Study of Various Attacks on Digital Watermarking Technique. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 3(5), 1567-1570.
- Pereira, S., Voloshyoskiy, Y., Pun, T., (2001). Optimal transform domain watermark embedding via linear programming, *Signal Processing*, (81)6, 1251-1260.
- Petitcolas, F., Anderson, R., Kuhn, M. (1999). Information Hiding – a Survey. *Proc. of the IEEE*, 87(7), 1062-1078.
- Popa, R. (1998). *An Analysis of Steganographic Techniques*. (Master's thesis). The "Polytechnic" University of Timisoara, Timisoara, Romania.
- Prasannakumari, V., (2009). A robust tamperproof watermarking for data integrity in relational databases, *Research Journal of Information Technology*, 1,3, 115- 121.
- Pratt WK. (2001). Digital Image Processing: PIKS Inside. 3rd. ed. USA: John Wiley & Sons, Inc;, p:1-756.
- Provos, N. ve Honeyman, P. (2001). Detecting steganographic content on the internet, Center for Information Technology Integration, NDSS 2002, San Diego.
- Rachid, R.S., (2014). *Binary Image Watermarking on Audio Signal Using Wavelet Transform*, Çankaya Üniversitesi, Matematik-Bilgisayar Bilimleri Bölümü, Yüksek Lisans Tezi, Ankara.
- Raggo, M. ve Hosmer, C., (2012). Data Hiding, Syngress, 350s, Elsevier.
- Romaric, T., Damiani, E. ve Bennani, N., (2012). Robust XML watermarking using fuzzy queries, Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual, 433-438.
- Ruia, X., Jinqiaob, C.X.S. (2013). A multiple watermarking algorithm for texts mixed Chinese and English. *Proc. Comput. Sci.*, 17, 844-851.
- S. Hanis, R. Amutha, (2019) A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure, *Nonlinear Dyn.* Vol. 95 421–432.
- Sellers, D. (1999). An Introduction to Steganography.
- Sharma, P.K., Rajni, C., 2012. Analysis of Image Watermarking Using Least Significant Bit Algorithm, *International Journal of Information Sciences and Techniques (IJIST)*, (2)4, 95-101.
- Shieh, C., Huang,H., Wang, F. ve Pan, J., (2004). Genetic watermarking based on transform-domain techniques, *Pattern Recognition*, pp. 555-565.
- Shih F. Y. ve Wu, S. Y., (2003). Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*, p. 969 – 975.
- Siddharth V, Saeed SH, Dua H. (2015). Image standardisation using interpolation. *International Journal of Enhanced Research in Science Technology & Engineering.*; 4(4); 272-278.

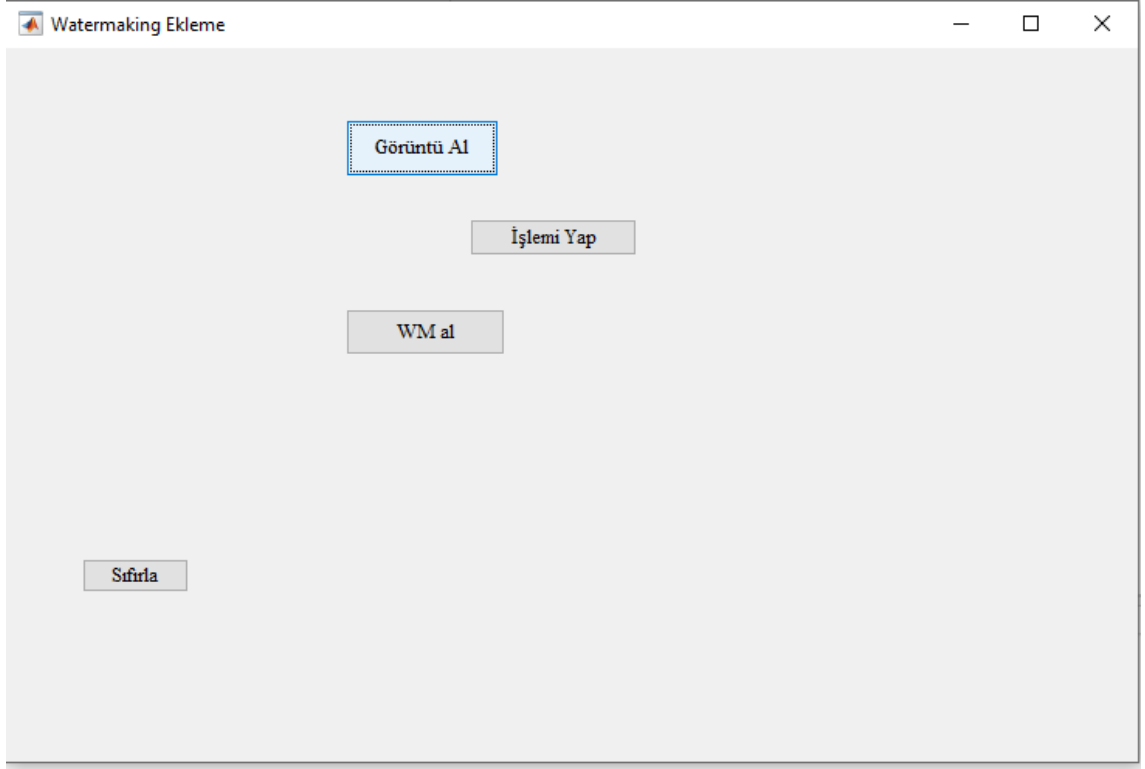
- Simmons G. J., (1984). The prisoners' problem and the subliminal channel, Chaum, D., (Ed), *Advances in Cryptology* 1nd edition, 489s, Springer US.
- Solachidis, V. ve Pitas, L., (2001). Circularly Symmetric Watermark Embedding in 2-D DFT Domain *IEEE Transactions On Image Processing*, vol. 10, No. 11.
- Srivadana, N. (2013). Digital Watermarking. *International Journal For Technological Research In Engineering*, 1(3), 13-17.
- Stein, J.Y. (2000). *Digital Signal Processing: a Computer Science Perspective*. New York: Wiley-Interscience.
- Sujatha, P., Purushothaman, S., Rajeswari, R. (2014). Performance study of combined artificial neural network algorithms for image steganalysis, In *Proceedings of International Conference on Internet Computing and Information Communications*, ss. 441-451, Springer India.
- Swanson, M.D., Kobayashi, M., Tewfik, A.H. (1998). Multimedia Data Embedding and Watermarking Technologies. *Proc., of the IEEE*, 86(6), 1064-1087.
- Sverdllov, A., Dexter, S., Eskicioglu, A.M., (2005). Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequency, 13th European Signal Processing Conference, Antalya.
- Takai, N. ve Mifune, Y., (2002). Digital watermarking by a holographic technique.
- Thampi, S. M., (2004). Information hiding techniques: a tutorial review, *ISTESTTP on Network Security & Cryptography*.
- Tsai, S.E., Yang, S.M., (2017). A Fast DCT Algorithm for Watermarking in Digital Signal Processor, *Hindawi Publishing Corporation Mathematical Problems in Engineering*, Article ID 7401845, 1-7.
- Tunçkanat, M., Sağıroğlu, Ş., (2002). Güvenli İletişim İçin Yeni Bir Yaklaşım: İmge İçerisine Doküman Gizleme, GAP IV. *Mühendislik Kongresi*, 665-668.
- Uçar, A., (2014). *Gezgin Ortamda Görüntü Damgalama Uygulaması*, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Kocaeli.
- Ujjiniya, U. ve Chugh, S., (2016). Digital image forgery detection based on texture feature and clustering technique. *International Journal of Computer Applications*, 147: 21-24.
- Vleeschouwer, C.D., Delaigle, J.F., Macq, B., (2001). "Circular interpretation on histogram for reversible watermarking", *Proc, of IEEE International Multimedia Signal Processing Workshop*, France, 345–350.
- Westfeld, A. ve Pfitzmann, A. (2000). Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned. *Attacks on Steganographic Systems*. 1-16.
- Xia, X.G., Boncelet, C.G., Arce, G.R., (1997). A multiresolution watermark for digital images, *IEEE International Conference on Image Processing*, (3), 548- 551.
- X. Wang, P. Liu, 2020 A new image encryption scheme based on a novel one-dimensional chaotic system, *IEEE Access*. 8 174463–174479. <https://doi.org/10.1109/ACCESS.2020.3024869>-(15.09.2021).

- Yadav, P. ve Rathore, Y., (2012). Detection of copy-move forgery of images using discrete wavelet transform. *International Journal on Computer Science and Engineering (IJCSE)*, 4: 565-570.
- Yang, L.H., Kleinman, A., Link, B.G., Phelan, J.C., Lee, S. and Good, B., (2007), “Culture and Stigma: Adding Moral Experience to Social Theory”, *Social Science & Medicine*, 64: 1524- 1535.
- Yao, R., Zhao, Q. ve Lu, H., (2006). A novel watermark algorithm for integrity protection of XML documents, *International Journal of Computer Science and Network Security*, 6,2B, 202-207.
- Yavuz, E., (2008). *Duruk İmgelerde Damgalama ve Veri Saklama*, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, Ankara.
- Yeung, M. ve Mintzer, F., (1997). An invisible watermarking technique for Image verification, *International Conf on Image Processing*.
- Zhao, L., Cui, D.W. (2009). Text watermark algorithm based on tone of Chinese characters. *Comput. Eng.* 35(10), 142–144.
- Z. Wang, A.C. Bovik, H.R. Sheikh, E.P. Simoncelli, 2004. Image quality assessment: From error visibility to structural similarity, *IEEE Trans. Image Process.* 13 600–612. <https://doi.org/10.1109/TIP.2003.819861>-(19.11.2021).

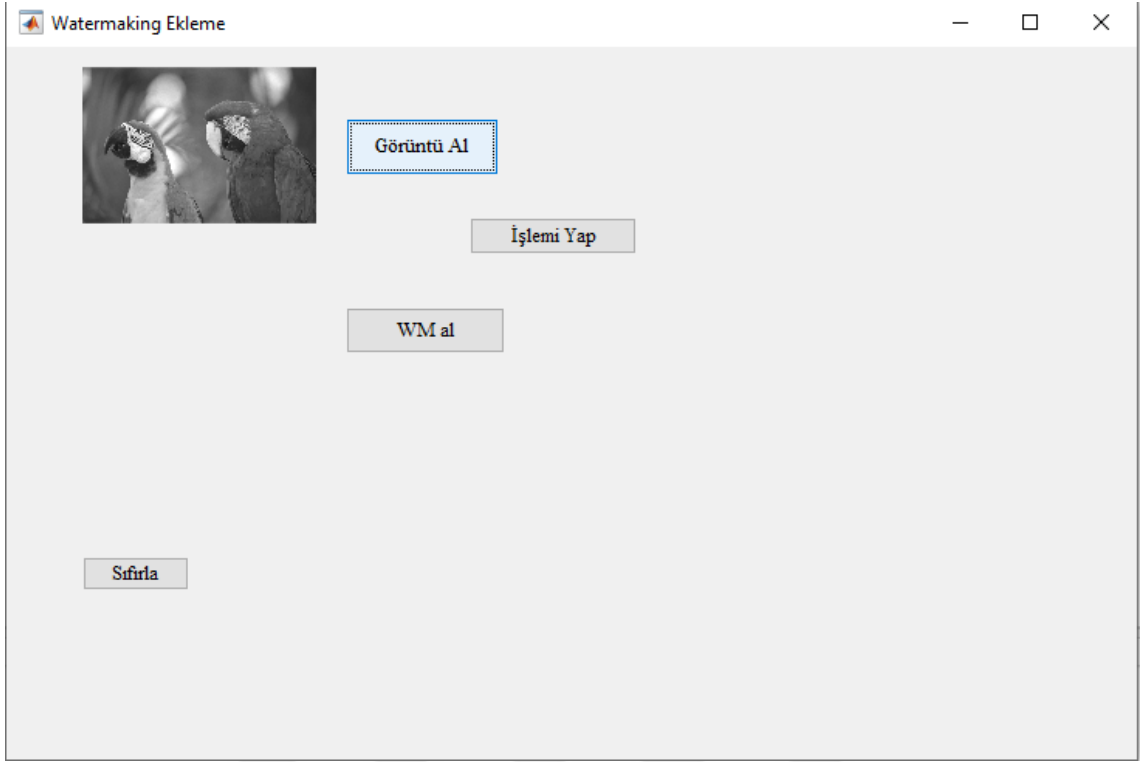
EKLER

Ek 1. Matlab Uygulama Görüntüleri

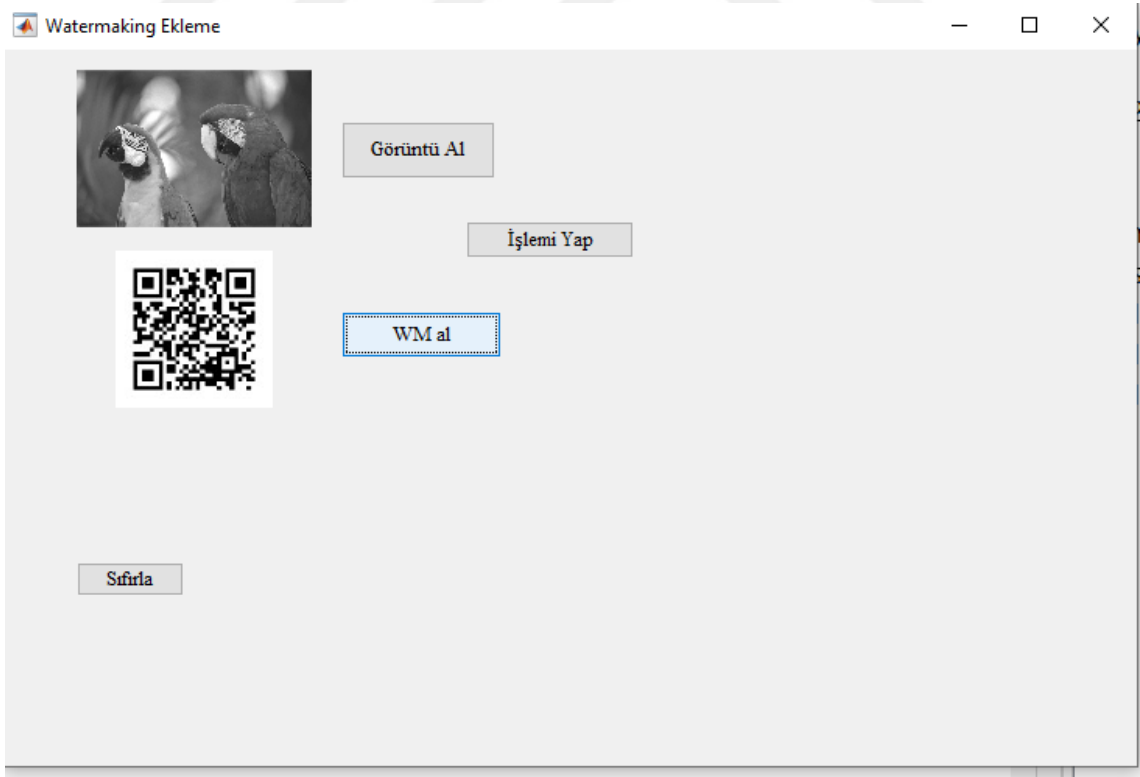
Sayısal görüntü işlemede kaos temelli yeni bir damgalama yaklaşımı matlab uygulamasında programlanarak ekran görüntüleri elde edilmiştir.



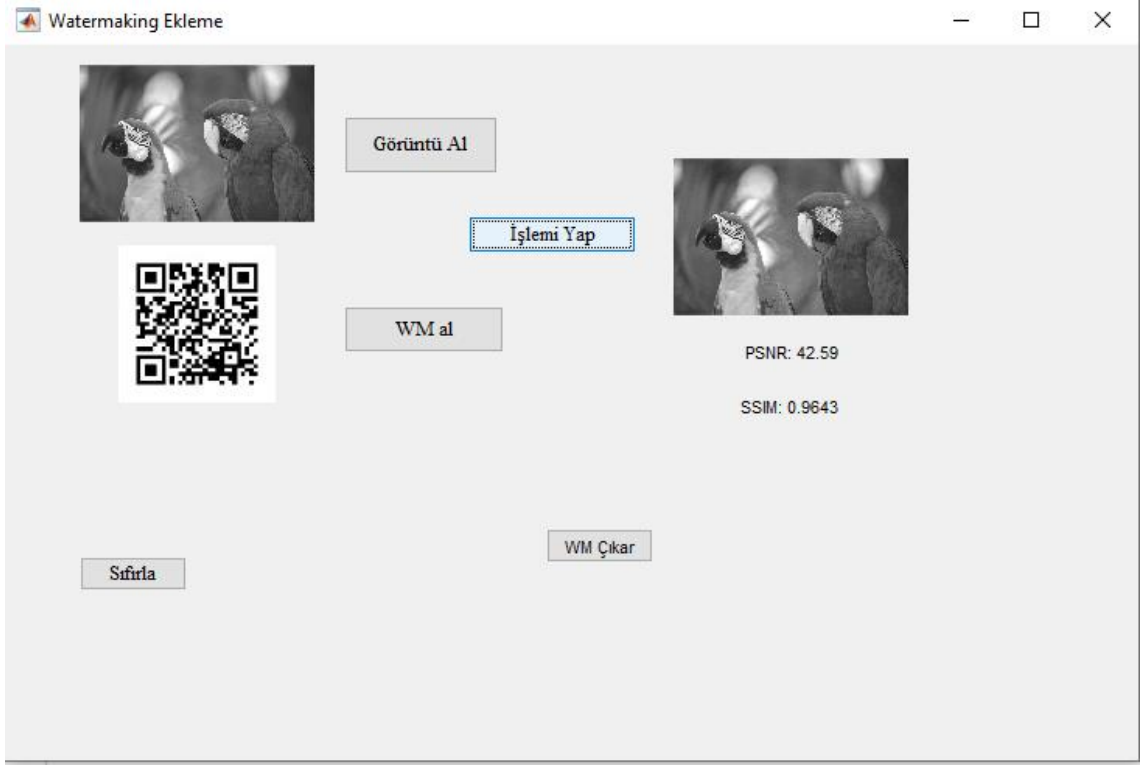
7.1. Matlab uygulama ana ekran görüntüsü



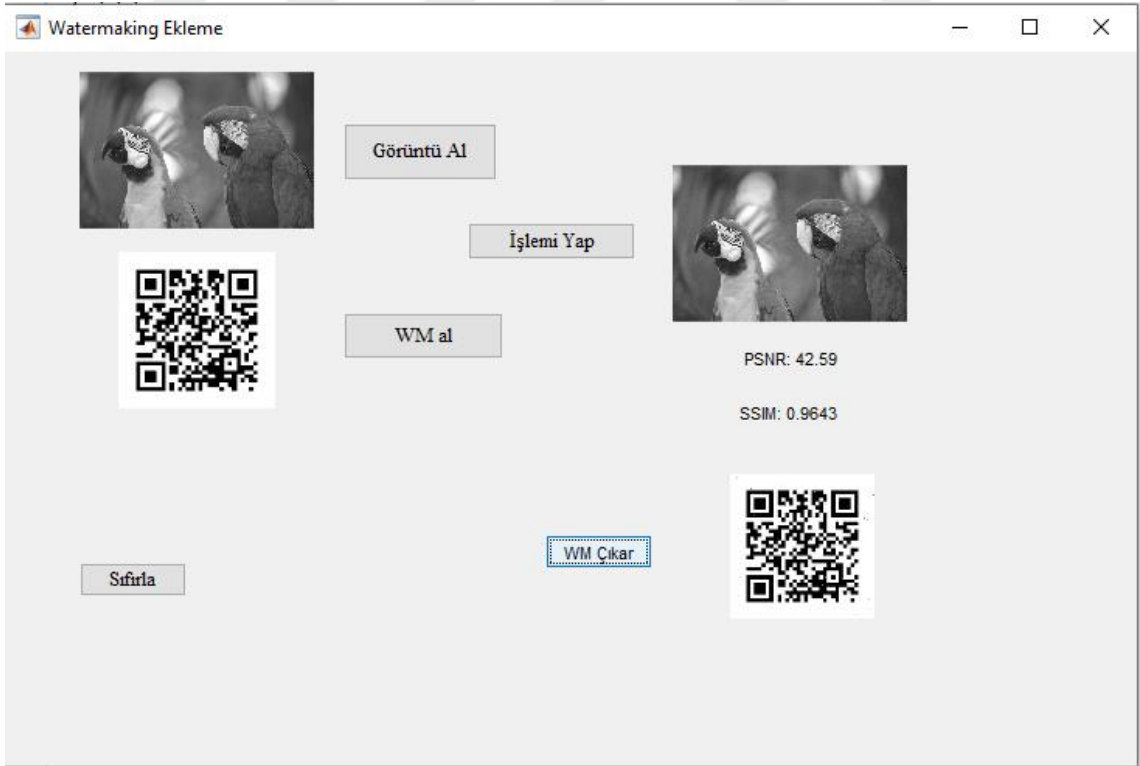
7.2. Matlab uygulama görüntü al ekran görüntüsü



7.3. Matlab uygulaması damga al ekran görüntüsü



7.4. Matlab uygulaması damga ekleme ekran görüntüsü



7.5. Matlab uygulaması damga çıkarma ekran görüntüsü