MUSTAFA KEMAL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ
ANABİLİM DALI

SAYISAL ORTAMLARDA VERİ DAMGALANMASI VE GERİ ELDESİ

MURAT FURAT

YÜKSEK LİSANS TEZİ

ANTAKYA

ŞUBAT–2006

Mustafa Kemal Üniversitesi

Fen Bilimleri Enstitüsü Müdürlüğüne,

Yrd. Doç. Dr. Mustafa ORAL danışmanlığında, Murat FURAT tarafından hazırlanan bu çalışma 01.02.2005 tarihinde aşağıdaki jüri tarafından, Elektrik-Elektronik Mühendisliği Anabilim Dalında yüksek lisans tezi olarak kabul edilmiştir.

Başkan:	Yrd.Doç. Dr. Mustafa ORAL	İmza…….
Üye	: Prof. Dr. Semir ÖVER	İmza…….
Üye	: Yrd.Doç. Dr. Ersin ÖZDEMİR	İmza…….

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Kod No:

İmza
01.02.2006

Prof. Dr. Abdurahman YİĞİT
Enstitü Müdürü

İÇİNDEKİLER

ÖZET

SAYISAL ORTAMLARDA VERİ DAMGALANMASI VE GERİ ELDESİ

Sayısal ürünlerin telif haklarının korunması, sayısal ortamın önemli sorunlarından biridir. Özellikle kopyalama ve çoğaltma işlemlerinde sayısal ortamın sağladığı kolaylık, bu sorunun önemini daha da arttırmıştır. Üzerinde değişiklik yapılması, kopyalanması ve çoğaltılması belki de en kolay olan ürünler sayısal görüntülerdir. Sayısal görüntülerdeki bu sorunun çözümü için yapılan çalışmalardan biri, görüntülere çalışmanın sahibi, yapım yılı ya da firma logosu gibi bir bilginin damgalanmasıdır. Bu bilgi, taşıyıcı görüntü üzerine görünür bir şekilde damgalanabileceği gibi görüntüye insan gözünün algılayamayacağı bir teknikle de yapılabilir.

Bu çalışmada, taşıyıcı görüntülere bir bilgi damgalamak için yeni bir yöntem önerilmiştir. Bu yöntem ile görüntüye görünmez ve dayanıklı filigran damgalanmaktadır. Damgalama işleminde uzay ve frekans düzlemi bileşenlerinin bir arada kullanılmaktadır. Damgalama DCT (Discrete Cosine Transform) ile elde edilen frekans bileşenlerine yapılırken, referans noktası olarak uzay düzleminden elde edilen enerji kullanılmıştır. Filigranın, çeşitli görüntü işleme saldırılarına karşı dayanıklılığı, kullanılan damgalama ağırlığı ile arttırılabilmektedir. Damgalama işleminden önce filigrana uygulanan permutasyon ile filigranın görüntü işleme saldırılarına karşı dayanıklılığı bir kat daha arttırılmıştır.

Önerilen yöntemin test edilmesi amacıyla literatürdeki damgalama çalışmalarında sıkça kullanılan üç ayrı görüntü, taşıyıcı olarak seçilmiştir. Bu görüntülere 26 farklı ağırlıkla yapılan damgalama sonucu görüntülerdeki değişim hata ve kalite bazında ölçülmüştür. Damgalanan görüntülere JPEG kayıplı sıkıştırması, gürültü ekleme, kesme, filtreleme ve döndürme gibi saldırılar çeşitli oranlarda uygulanmış ve filigran geri elde edilmiştir. Saldırılar sonunda elde edilen filigranın aslına benzerliği ölçülmüş, böylece saldırılara karşı dayanıklılığı tespit edilmiştir.

2006, 75 sayfa

Anahtar Kelimeler: İmge damgalama, sayısal ürünlerde telif haklarının korunması ve güvenlik, DCT

ABSTRACT

WATERMARKING OF DIGITAL MEDIA

Copyright protection of the digital products is one of the problems of digital media. Easy copying and multiplication processes provided by the technology have increased the importance of the problem.

Digital images are the products which can be easily modified, copied and duplicated. One of the studies to solve copyright protection on the digital images is to embed some information about the author, production year or logo. This information can be embedded into an image where it can be perceptually either visible or invisible.

In this work, a method is proposed to embed watermarks into the host images invisibly and robust. Both spatial and frequency domain components are used to embed watermark. While watermark is embedded into the frequency domain components provided by DCT (Discrete Cosine Transform), spatial domain energy is selected as the reference point. The resistance of the embedded watermark to image processing attacks can be enhanced by increasing the embedding weight. By permuting the watermark before embedding, the watermark resistance is increased.

Three images, used in the literature frequently, were selected to test the proposed method. These images are watermarked with 26 different weights. The distortion and quality of the watermarked images are measured. After JPEG lossy compression, noise, cropping, filtering and rotation attacks with different ratios, the watermarks were extracted. Similarities of the extracted watermarks were measured to determine the resistance against such attacks.

2006, 75 pages

Key Words: Digital watermarking, copyright protection of digital products and security, DCT

ÖNSÖZ

Yüksek Lisans tez konumun belirlenmesinde ve çalışmamın her aşamasında yardımlarını esirgemeyen, değerli fikir ve katkıları çalışmama yön veren danışmanım Yrd. Doç. Dr. Mustafa ORAL'a çok teşekkür ederim. Maddi ve manevi desteğini esirgemeyen, bölüm başkanımız Yrd. Doç. Dr. Emin ÜNAL'a teşekkür ederim. Ayrıca teknik bilgi ve desteklerini esirgemeyen Öğr. Gör. Mustafa BAYRAMOĞLU ve Öğr. Gör. Mustafa YENİAD ile değerli çalışma arkadaşlarım Serkan GÜLER, Ahmet GÖKÇEN ve Tarık SERİNDAĞ'a çok teşekkür ederim.

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

1. GİRİŞ

Son yıllarda ilerleyen teknoloji, hayatımıza birçok kolaylık getirmiştir. Özellikle bilgisayar alanında yaşanan gelişmeler, bilgi paylaşımının daha ucuz ve kolay olmasını sağlamıştır. Dünya üzerindeki bilgisayarların birbirlerine bağlanmasını ve karşılıklı bilgi alışverişinde bulunabilmesine olanak sağlayan Internet ağı da teknolojinin getirdiği diğer bir ürün olarak karşımıza çıkmaktadır. Son birkaç yıl içinde büyüyen talep karşısında Internet altyapısına yapılan yatırımların artması ve bunun sonucu olarak hızlanan veri iletişimi sayesinde, dünyanın herhangi bir yerindeki bir bilgiye erişmek artık sorun olmaktan çıkmıştır.

Bu gelişmelere paralel olarak, bilgisayar yazılımlarında da, birçok yeniliği beraberinde getiren ilerlemeler görülmüştür. Bilgisayar ortamına aktarılan ses, video, görüntü ve metin verileri, geliştirilen yazılımlarla daha kolay işlenebilmektedir. Hem maliyet hem de zaman açısından kazandırdığı avantajların büyük olması nedeniyle, günümüzdeki birçok çalışma artık bilgisayar ortamında gerçekleştirilmektedir. Bunun sonucu olarak, bilgisayar kullanılarak yapılan ürünler günlük hayatımızda daha fazla yer almıştır (SHIEH ve ark., 2004).

CD, DVD gibi depolama araçlarının üretim maliyetlerinin düşmesi, verilerin saklanmasında bu araçların kullanımını arttırdığı gibi, depolanan verilerin kopyalanıp çoğaltılmasını popüler hale getiren diğer bir etken olmuştur (EGGERS ve ark., 2001).

Teknolojinin sağladığı kolaylıklar beraberinde sorunların da ortaya çıkmasına sebep olmuştur. Bunlardan ilki; bilgisayar ortamına alınan çalışmaların aslından hiçbir şey kaybetmeden çoğaltılabilmesidir (ZHAO ve KOCH, 1995). Özellikle Internet altyapısının getirdiği hız ve paylaşımdaki kolaylık nedeniyle bilgisayar ortamındaki çalışmaların birçok kopyası çok hızlı ve kalitesinde herhangi bir kayıp olmadan kolay bir şekilde dağıtılabilmektedir. Ortaya çıkan diğer bir sorun da, bu çalışmalar üzerinde bilgisayar yazılımları ile kolaylıkla değişiklikler yapılabilmesi ve bunların yeni bir çalışma gibi sunulabilmesidir. Sonuç olarak, çalışmanın asıl sahibinin telif hakları yok sayılmaktadır (HSU ve WU, 1999).

Bilgi paylaşımının hızlı ve kolay yapılabilmesinin sonucu olarak, güvenli iletişimin sağlanabilmesinde yaşanan zorluklar da teknoloji ile birlikte gelen bir başka sorun olarak karşımıza çıkmaktadır. Özellikle Internet üzerinden yapılan iletişim,

gönderilen bilgi ya da çalışmaların kolaylıkla yetkisiz kişilerin eline geçmesine ve kopyaların hızla dağıtılabilmesine sebep olabilmektedir. Bu da, Internet üzerinden yapılan iletimde güvenlik sorunlarının olduğunu göstermektedir. Bilgisayar ortamına aktarılan çalışmaların, yetkisi olmayan kişiler tarafından kopyalanması ve dağıtılmasıyla ortaya çıkan problem, gün geçtikçe daha da büyümektedir. Bu sorun için önerilen çözümlerden biri, bu çalışmalara, amaca uygun bir bilgi eklemek ve çalışmayı bu bilgi ile birlikte bilgisayar ortamında tutmak ve takip etmektir.

Bilgisayar ortamında bilginin gizli bir şekilde gönderilmesi için önerilen yöntemlerden biri, herhangi bir sayısal ortama; sese, videoya, görüntüye ya da yazıya, bu bilginin görünmez bir şekilde saklanması bilginin masum görünümlü bir taşıyıcı aracılığıyla yollanmasıdır. Steganography adı verilen bu yöntemde, gönderilecek bilgi seçilen sayısal ortama fark edilebilir bir değişikliğe sebep olmayan bir yöntem kullanılarak eklenir (JOHNSON ve JAJODIA, 2005). Böylece gönderilen sayısal ortam içinde herhangi bir bilginin bulunduğuna dair hiç bir ize rastlanmaz. Kriptolojiden farklı olarak bilgi, üzerinde herhangi bir deşifre işlemine gerek duyulmadan anlaşılır bir şekilde geri elde edilir. Kriptoloji de ise, bilginin kendisi bir algoritma ile şifrelenir. Şifrelenmiş bilgi, herhangi bir taşıyıcı olmaksızın iletilir. İletim boyunca bilgi şifrelidir. İletimin sonunda alıcı, deşifre algoritmasını kullanarak şifrelenmiş bilgiyi çözer. Böylece üçüncü bir kişi iletimin herhangi bir yerinde şifrelenmiş bilgiyi elde etse bile çözmek için deşifre algoritmasını bilmediği için asıl bilgiye ulaşamaz (BARNI ve BARTOLONI, 2004).

Çalışma sahiplerinin telif haklarının korunması amacıyla yapılan araştırmalarda, steganography uygulamalarına benzer bilgi saklama yöntemleri geliştirilmiştir. Bunlardan bazıları, çalışma ya da sahibinin hakkında bilgi içeren sayısal imza (digital signature), etiket (label) ya da sayısal damga (watermark) olarak gösterilebilir (MOHANTY, 1999). Sayısal damgalama bir çeşit steganography olarak da tanımlanabilir. Aralarındaki fark şöyle açıklanabilir: Steganography uygulamalarında, saklanması istenen mesaj bir sayısal ortama eklenir. Ancak sadece taşıyıcı görevi üstlenen bu ortam üzerinde yapılacak değişikliklere karşı dayanıklı olması beklenmez. Damgalamada ise amaç, bir sayısal ortama saklanan bilginin bu ortam üzerinde yapılacak çeşitli işlemlere karşı dayanıklı olması ve sonunda tanınabilir bir şekilde geri elde edilebilmesidir. Damgalama algoritmaları bu amaç çerçevesinde geliştirilir ve

bilgisayar ortamındaki çalışmaların telif haklarının korunmasında son yıllarda en çok önerilen bilgi saklama çeşididir. Telif haklarının korunması ve bilgi saklanması ile ilgili olarak daha ayrıntılı açıklama ikinci bölümde verilecektir.

Bu çalışma ile bilgisayar ortamındaki görüntülere gizli bir filigran damgalanması amaçlanmıştır. Bu amaçla siyah-beyaz bir logo filigran olarak seçilmiştir. Damgalanacak taşıyıcı görüntü gri seviyeli bir görüntü olup, damgalama sonunda görüntüdeki bozulmanın en az olması ve logonun çeşitli resim işleme saldırıları sonunda tanınabilir şekilde geri elde edilmesi hedeflenmiştir.

Tez düzeni genel hatlarıyla şu şekildedir: Veri damgalama yöntemleri, tarihi ve terminolojisinin anlatıldığı birinci bölümde, veri saklama yöntemleri arasındaki farklar ile uygulama alanlarına yer verilmiştir. İkinci bölüm, tezin oluşturulmasında kullanılan araçların tanıtıldığı "Materyal" ile geliştirilen damgalama algoritmasının ayrıntılı açıklamasına yer verildiği "Yöntem" bölümünü içermektedir. Yapılan testler ile çeşitli değerlendirmeler grafik, tablo ve görüntü olarak "Araştırma Bulguları ve Tartışma" bölümünde yer almaktadır. Dördüncü bölümde ise, bu çalışmadan elde edilen sonuçlar değerlendirilmiş ve gelecekteki çalışmalar için çeşitli öneriler yapılmıştır. Ayrıca tezde önerilen yöntem için hazırlanan bilgisayar yazılımının kaynak kodu ekler bölümünde sunulmuştur.

2. ÖNCEKİ ÇALIŞMALAR

2.1. Veri Saklama Yöntemlerinin Tarihçesi

Veri saklama yöntemlerinin tarihi veri iletişimi kadar eskilere dayanır. MÖ 485 – 525 yıllarında yaşayan ilk Yunan tarihçisi Heredot, bir çalışmasında Pers İmparatorluğu ile ondan çok daha küçük Yunan şehir devleti arasında geçen savaş sırasında yapılan gizli iletişim metodunu anlatmıştır. Buna göre Pers kralına gizli planı götürecek olan kişinin kafası tıraş edilip mesaj kafasına dövme ile yazılmış ve taşıyıcının saçları tekrar uzayıncaya kadar beklenmiştir. Böylece mesaja bir çeşit doğal kamuflaj hazırlanmıştır. Görünürde yanında hiçbir şey bulunmayan taşıyıcı, özgürce seyahat edebilmiş ve ulaşması gereken yere vardığında kafasını tıraş edip taşıdığı mesajı göstermiştir (ANONYMOUS, 2005).

Günümüzde de kullanılan görünmez mürekkep uygulamaları bilinen tarih kadar eskidir. MS 23-79 yıllarında yaşayan Pliny the Elder, saydam bir yazı için, bir bitkinin sütü kullanılarak kağıda yazı yazıldığını, ama kağıdın sonradan ısıtıldığında uygulanan sütün kağıt üzerinde kahverengiye doğru koyulaştığını anlatmıştır. Bu da, tarihte kullanılan ilk görünmez mürekkep uygulaması olarak karşımıza çıkmaktadır (ANONYMOUS, 2005).

Rönesans döneminde yaşayan Johannes Trithemius ilk kriptoloji kitabını yazmıştır (Şekil 2.1.). Aynı dönemde Giovanni Battista Porta, gizli bir mesajın çok kaynamış bir yumurta ile nasıl taşınabileceğini tanımlamıştır (ANONYMOUS, 2005). Bunların yanında steganography alanında bilinen ilk eser, Johannes Trithemius tarafından yazılmış kitaptır (KATZENBEISSER ve PETITCOLAS, 2000). "Örtülü yazı" anlamındaki Steganography kelimesi, eski Yunanca'dan gelen bir kelimedir (JOHNSON ve JAJODIA, 2005). *Steganographia* terimi ilk olarak Trithemius'un el yazması kitabında geçmiştir (ARNOLD ve ark., 2003).

Bu konuda geçmişte kullanılan çok sayıda tekniği rapor eden Æneas the Tactician, gizli mesajları taşıyan mektupların, kadınların küpelerinde saklanıp taşındığını bildirmiştir. Bildirilen diğer bir yöntem ise, yollanan mektuptaki yazı karakterlerinin boyunu değiştirerek gizli mesajın kodlanması, mektubun üstüne ya da

altına küçük delikler açarak gizli mesajın saklanmasıdır. Sonradan bu yöntem, 17. yüzyılda Wilkins (1614–1672) tarafından geliştirilerek küçük delikler yerine görünmez mürekkep kullanılarak mikro noktalar ile işaretlenmiştir (KATZENBEISSER ve PETITCOLAS, 2000). Görünmez mürekkep yöntemi II. Dünya Savaşı'nın başlarında kullanılmıştır. Görünmez mürekkep ile masum gibi görünen mektupların satır aralarında farklı mesajlar taşınmıştır. Ayrıca şifrelenmemiş bir mektubun metni, taşınacak mesajı gizlemek için bir ortam olarak kullanılmıştır. II. Dünya Savaşı'nda bir Alman ajanı tarafından gönderilen mektupta bu yöntem kullanılmıştır (CHEN, 1999; JOHNSON ve JAJODIA, 2005). Mesaj, mektubun şifrelenmemiş metni içinde gizlenmiştir. Normal cümle düzenindeki mektubun aşağıdaki metni, masum bir metin olarak görünmektedir:

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

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

Bilgisayar ve bilgisayar ağlarının gelişmesiyle ortaya çıkan güvenlik ve telif hakları sorunu için sayısal damgalama fikri ilk olarak 1990 yılının başında ortaya atılmıştır. O günden beri artarak hızlanan bir tempo ile konu üzerinde araştırmalar yapılmaktadır. Sayısal görüntülerin damgalanması üzerine ilk akademik konferans 1996 yılında organize edilmiştir. Bu konudaki ilk yayınlar TANAKA ve ark. tarafından 1990 yılında, CARONNI ve ark. tarafından 1993 yılında yapılmıştır. 1995 yılından itibaren yayınlanan araştırmaların sayısında büyük bir artma görülmüştür. Sayısal görüntülerdeki damgalama çalışmaları, sonradan, ses ve video görüntüleri üzerine de yapılarak genişleyerek artmıştır (KUTTER ve PETITCOLAS, 1999).

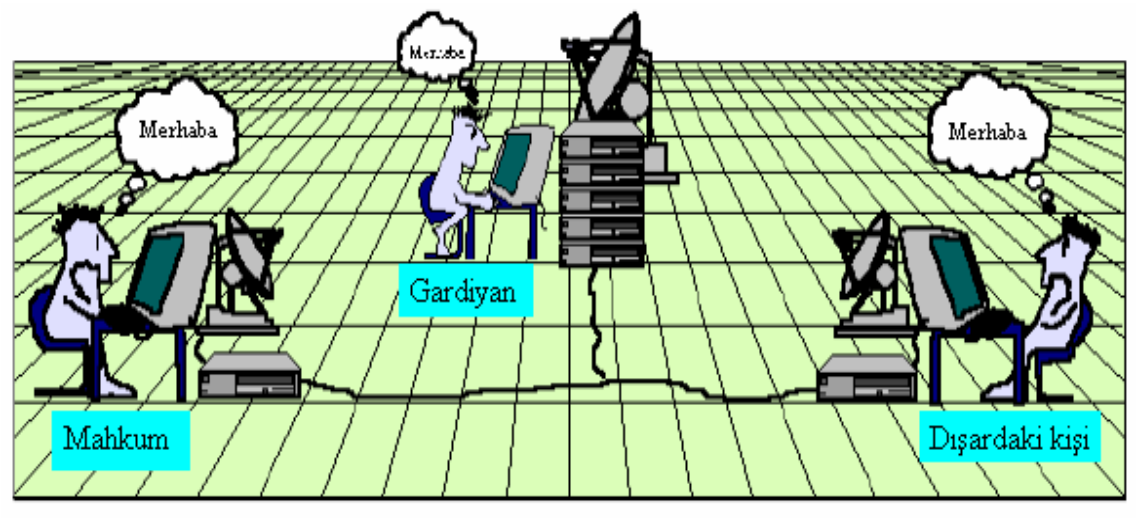
Sayısal görüntüler üzerinde yapılan bilgi gizleme işlemleri amacına uygun olarak farklı yöntemlerle yapılmaktadır. Çoğu zaman bu yöntemler birbirleriyle karıştırılmaktadır. Bu amaçla takip eden bölümde veri gizleme terminolojisi kısaca anlatılacak ve ardından literatürde karşılaşılan veri damgalama çalışmaları hakkında geniş bir özet Bölüm 2.5.'de sunulacaktır.

2.2. Veri Gizleme Terminolojisi

2.2.1. Steganography

Örtülü yazı anlamına gelen "Steganography", adından da anlaşılacağı gibi bir taşıyıcıya gizli mesajın eklenmesi ile yapılan iletişim türüdür. Gizli mesaj doğrudan ya da şifrelenerek değil, taşıyıcı aracılığı ile karşı tarafa iletilir. Mesajın taşıyıcı üzerinde yapılacak saldırılara karşı dayanıklı olması beklenmez. Buradaki amaç, taşıyıcıya fark edilmeyecek bir yöntem ile mesajı saklamak ve iletmektir. Mesaj, taşıyıcı içinde küçük bir değişiklikle yok olabilecek kırılgan bir yapıya sahiptir.

Örtülü mesaja örnek olarak, dışarıda bir partiye gitmek isteyen hapishanedeki mahkumun durumu modellenmiştir (BARNI ve BARTOLONI, 2004). Şekil 2.1.'de gardiyan, yasadışı bir iletişim olmaması için dışarıdaki kişilerden mahkuma gelen her mesajı okumakta ve içinde gizli bir bilgi olup olmadığını araştırmaktadır. Anlama kabiliyeti olmasa bile, gizli bir bilgi bulduğundan şüphelendiği her mesajı yasaklamaktadır. Bu durumda dışarıdaki kişilerin kriptolu bir mesajı mahkuma göndermeleri gardiyanın dikkatini çekecektir ve yasaklanacaktır. Dolayısıyla mahkuma gönderilecek mesajın masum bir metnin içine gizlenerek yollanması uygun çözüm olarak ortaya çıkmaktadır.



Şekil 2.1. Gizli bilgi iletişimi için bir model: mahkumların problemi

2.2.2. Kriptoloji

Bir veri gizleme yöntemi olan kriptolojide, örtülü mesajın aksine bir taşıyıcı kullanılmaz. Gizlenmesi gereken mesaj, bir algoritma kullanarak şifrelenir ve şifreli mesajın kendisi herhangi bir taşıyıcı kullanılmadan gönderilir. Alıcı, aldığı mesajı deşifre ederek asıl mesaja ulaşır. Üçüncü kişiler, şifrelenmiş mesajı elde etse bile deşifre algoritmasını bilmedikçe mesajın aslını elde edemezler.

2.2.3. Sayısal Damgalama (Digital Watermarking)

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

2.2.4. Parmak İzi Ekleme ve Etiketleme (Fingerprinting, Labeling)

Etiketleme olarak da adlandırılan parmak izi, bir sayısal çalışmanın belli bir müşteriye dağıtılma öncesinde, telif haklarının korunması amacıyla, yalnızca o müşteriyi temsil eden bilginin çalışmaya görünmez bir şekilde damgalanması işlemidir. Etiketleme için kullanılan yöntemde bilgi, dışardan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her müşteriye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir (ARNOLD ve ark, 2003). Parmak izi ekleme, amaç bakımından sayısal damgalamadan farklı ancak yöntem olarak sayısal damgalama ile aynı özellikler gösterir.

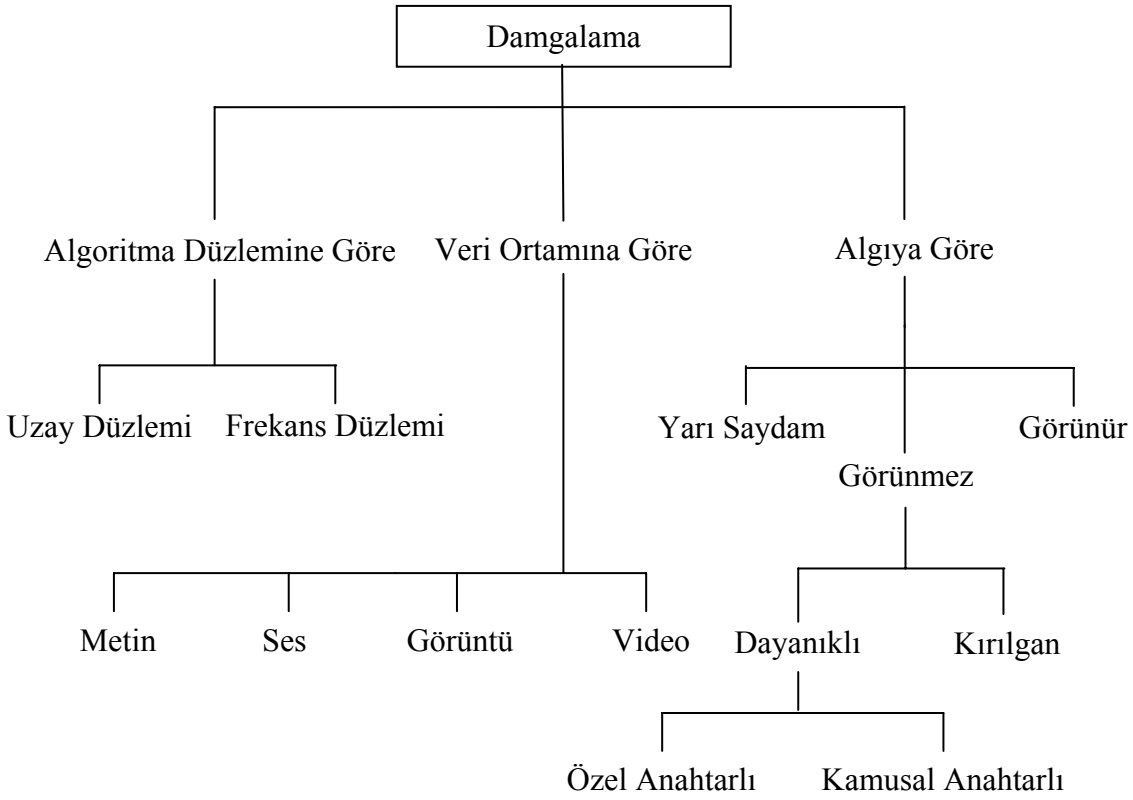
2.2.5. Sayısal İmzalama (Digital Signature)

Sayısal imzalama, bir doküman sahibinin kendi kişisel anahtarı (private key) ile dokümanı imzalaması yani şifrelemesidir. Bu kişisel anahtardan üretilen kamusal anahtar (public key), dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır. Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Bir kişisel anahtar ile imzalanan doküman, sahibi hakkında bilgi de birlikte taşımış olur. Bazı otoritelerin, sayısal damgalama ile sayısal imzalamanın eş anlamlı olduğuna dair görüşlerine karşın bunları birbirinden ayrı tutan görüşler de vardır (MOHANTY, 1999).

Uygulamada sayısal dokümanların imzalanması için çeşitli yazılımlar mevcuttur. Her kişi için oluşturulan kamusal ve kişisel imzalar, kendisine elektronik kartlarda verilir. Bu konuda, birçok yerde yasal düzenlemelerin ve teknik altyapının henüz sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır, göndericinin kişisel imzası kullanılarak şifrelendiğinden gönderici tarafından inkar edilemez ve göndericinin imzası taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan üzerinde değişiklik yapamaz (TOPALSAN, 2004).

2.3. Veri Damgalama Yöntemleri

Bilgisayar ortamındaki verilerin damgalanması için birçok yöntem geliştirilmiştir. Damgalama yöntemleri, algoritma düzlemine göre, çalışmanın türüne göre ve algıya göre olmak üzere öncelikle üç ana başlıkta incelenebilir. Bunlar da kendi içerisinde alt gruplara ayrılır. Buna göre Şekil 2.2.'de sayısal damgalamanın çeşitleri görülmektedir.



Şekil 2.2. Damgalama yöntemlerinin sınıflandırılması

Damgalama algoritmaları, üzerinde çalışılan düzleme göre ikiye ayrılır. Uzay düzleminde yapılan damgalama işlemlerinde doğrudan damgalanacak çalışmanın bilgisi üzerinde değişiklik yapılır. Frekans düzleminde yapılan damgalama işlemlerinde, damgalanacak çalışma öncelikle frekans bileşenlerine ayrılır. Bu amaçla DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform), FFT (Fast Fourier Transform) gibi dönüştürme araçları kullanılarak, çalışma frekans düzlemine taşınır. Burada, elde edilen frekanslar ve katsayıları üzerinde değişiklik yapıldıktan sonra ters dönüştürme uygulanarak damgalanmış ürün elde edilir.

Damgalanacak çalışmanın türüne göre, damgalama yöntemleri dört alt başlıkta incelenebilir. Bunlar yazı, ses, görüntü ve videodur.

Algıya göre damgalama algoritmaları üç grupta incelenebilir. Damgalanacak filigranın, görüntünün bir yerine gözle görülebilecek bir şekilde yerleştirilmesine "görünür damgalama" adı verilir. Görünür damgalamaya örnek olarak televizyon ekranında bulunan kanal logosu ya da Internet'te yayınlanan görüntülerin altında bulunan yayıncı sitenin adresi verilebilir. Bu yöntemde her ne kadar logo görüntünün

üzerinde belirgin bir şekilde yerleştirilse de, kırpma (cropping) yoluyla görüntüden kolaylıkla ayrılabilir ve hatta yerine başkası yerleştirilebilir.

Görüntü içine gözle algılanamayacak bir şekilde filigranı yerleştirme işlemine "görünmez damgalama" adı verilir. Bu yöntem ile damgalanan görüntülerde filigran, görüntü içine yetkili kişi tarafından bilinen bir algoritma ile dağıtılır ve başka bir algoritma ile görüntüden geri elde edilir. Filigranın görüntü içindeki yeri belli olmadığından kırpma işlemi ile görüntüden ayrılamaz. Damgalama ve geri elde etme algoritmaları sadece yetkili kişi tarafından bilindiğinden yetkisi olmayan kişilerin görüntüdeki filigrana ulaşmaları neredeyse imkansızdır.

Görünür ya da görünmez damgalamanın yanında sayılabilecek üçüncü bir yöntem ise, logonun görüntünün büyük bir bölümü üzerine yarı saydam olarak eklenmesidir. Bu yolla eklenen logonun görüntüden ayrılması, görüntüyü anlamsız kılacağından avantajlıdır. Ancak görüntüyü kullanıcıya bu şekilde sunmak bir dezavantajdır.

Görünmez damgalama yöntemleri kendi içinde "dayanıklı" ve "kırılgan" olmak üzere ikiye ayrılır. Dayanıklı damgalama yöntemleriyle yapılan damgalamada, taşıyıcı görüntüye gizli bir şekilde damgalanan bilginin, görüntünün kalitesinde ciddi bir bozulmaya neden olmayan çeşitli görüntü işleme saldırılarına karşı dayanıklı ve geri çıkarıldığında tanınabilir nitelikte olması amaçlanır. Kırılgan damgalama yöntemlerinin amacı görüntünün gerçekliği ya da doğruluğunun tespiti olduğundan, görüntüde yapılacak en küçük bir değişikliğin damgalanan bilgiyi yok etmesi istenir.

Dayanıklı görünmez damgalama algoritmaları kendi içlerinde iki grupta incelenebilir. Bunlar "kişisel anahtarlı" ve "kamusal anahtarlı" olarak adlandırılır. Bu tür damgalama yöntemlerinin temel prensibi, damgalama ve geri elde etme sırasında kullanılan anahtarlara bağlıdır. Eğer taşıyıcı görüntüden filigranın çıkarılması için gerekli anahtar herkes tarafından biliniyorsa, bu yöntem "kamusal anahtarlı görünmez dayanıklı damgalama" olarak adlandırılır. Diğer taraftan, kullanılan anahtar sadece görüntünün sahibi tarafından biliniyorsa, yani gizli tutuluyorsa, bu "kişisel anahtarlı görünmez dayanıklı damgalama" olarak adlandırılır (ARNOLD ve ark., 2003).

Sayısal görüntülere gizli filigran damgalama yöntemlerinin sınıflandırılmasında kullanılan bir diğer kriter ise geri elde algoritmasında görüntünün aslının kullanılıp kullanılmamasıdır. Filigranın geri elde edilmesinde eğer görüntünün ya da filigranın aslı

kullanılmıyorsa, bu tür yöntemlere “kör damgalama” adı verilir. Eğer görüntünün ya da filigranın aslından biri kullanılıyorsa, bu tür yöntemlere “kör olmayan damgalama” denir.

2.4. Filigran Damgalama Yöntemlerinde Dikkat Edilmesi Gereken Hususlar

Sayısal görüntülerde telif haklarının korunması ve güvenlik için filigran damgalanması üzerine birçok çalışma yapılmıştır. Kullanılan algoritmalar ve düzlemler birbirinden farklı olsa da, temelde belli başlı amaçlar etrafında toplanmıştır. Filigranın algılanmaması ve dayanıklılığı göz önünde bulundurularak damgalama algoritmalarından beklenen özellikler aşağıdaki gibi sıralanabilir (MOHANTY, 1999).

2.4.1. Görünür Filigran Damgalamanın Özellikleri

- Görünür bir şekilde damgalanan filigran hem renkli hem de monokrom görüntülerde açıkça belli olmalıdır.
- Filigranı resim kırpma işlemine karşı korumak için, görüntüde geniş bir alana yayılmalı ya da görüntünün önemli bir bölümü üzerine yerleştirilmelidir.
- Filigran yarı saydam olarak görüntü üzerine eklenecekse görünebilecek seviyede saydam olmalı fakat orijinal görüntünün ayrıntıları korunmalıdır.

2.4.2. Görünmez Dayanıklı Filigran Damgalamanın Özellikleri

- Görünmez bir şekilde görüntüye damgalanmış filigran, ne görüntüde tespit edilebilmeli ne de görüntü içeriğinin kalitesini düşürmelidir.
- Görünmez bir şekilde görüntüye damgalanmış filigran, görüntü kalitesinde gözle görülür bir bozulmaya sebep olmayan çeşitli işlemlere karşı dayanıklı olmalıdır.
- Yüksek kaliteli görüntülerin ve sanat çalışmaların damgalanmasında en az sayıda piksel değiştirilmelidir.

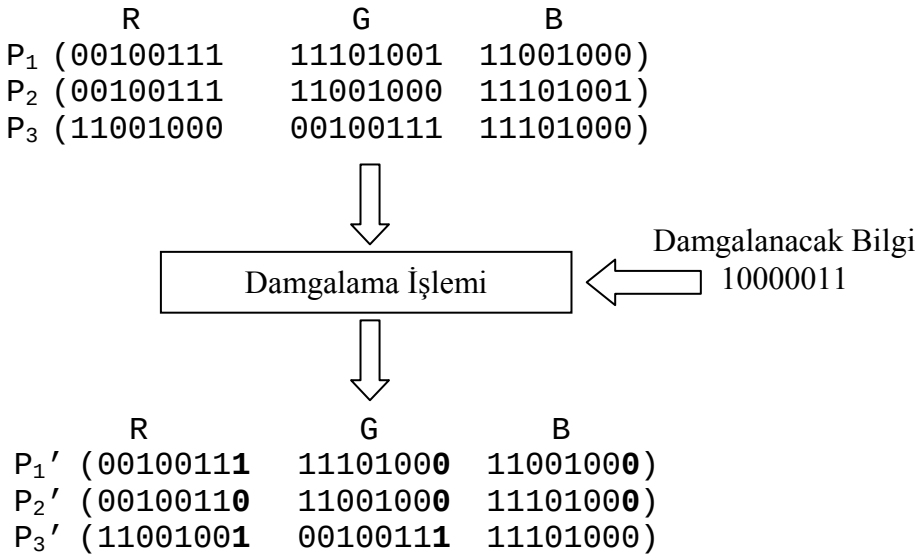
- Filigran damgalanması ve geri görüntüden elde edilmesi işlemi kolay ve hızlı bir şekilde yapılabilmelidir.
- Görüntüye damgalanan filigranın geri çıkarılmasında kullanılacak yazılım bilgisayar ve işletim sistemlerinden bağımsız çalışabilmelidir.
- Görüntü içindeki filigran, JPEG gibi çeşitli kayıplı sıkıştırma işlemlerine karşı dayanıklı olmalıdır.

2.4.3. Görünmez Kırılgan Filigran Damgalamanın Özellikleri

- Görünmez bir şekilde görüntüye damgalanmış filigran, ne görüntüde tespit edilebilmeli ne de görüntü içeriğinin kalitesini düşürmelidir.
- Görüntü pikselleri üzerinde yapılacak bir değişiklik filigranın kolayca bozulmasına neden olmalıdır.
- Filigran güvenli olmalıdır. Bunun anlamı, sık kullanılan görüntü işlemleri ile görüntü üzerinde yapılacak herhangi bir değişiklik sonucu bozulan filigran, tekrar düzeltilebilecek niteliğe sahip olmamalı ve tanınabilir bir düzeyde geri elde edilmesi mümkün olmamalıdır.
- Filigran damgalanması ve geri görüntüden elde edilmesi işlemi kolay ve hızlı bir şekilde yapılmalıdır.

2.5. Sayısal Görüntülerde Damgalama Çalışmaları

Sayısal görüntüler üzerindeki ilk damgalama çalışmaları uzay düzleminde piksellerini en az değerlikte değiştirilmesi ile yapılmıştır (JOHNSON ve JAJODIA, 2005). 24-bit renk derinliğine sahip bir görüntüde her piksel üç temel renk kanalı (Kırmızı – Yeşil – Mavi) ile temsil edilir. Her kanal 256 renk tonuna sahiptir ve 8 bitlik binary sayı ile temsil edilir. En düşük değerlikli bitlerin görüntüye damgalanacak bilgiye göre değiştirilmesi ile en basit görünmez damgalama gerçekleştirilir. Örneğin "A" harfinin ikilik sayı sisteminde 10000011 ile temsil edilir ve bu harfi damgalamak için 3 pikselin en az değerlikli bitleri Şekil 2.3'de görüldüğü gibi değiştirilir.



Şekil 2.3. Görüntünün piksellerinin en az değerlikli bitinin değiştirilmesi ile yapılan damgalama algoritması örneği

Burada P1, P2 ve P3 orijinal görüntünün herhangi üç elemanıdır. P1', P2' ve P3' ise damgalama sonucu oluşan görüntüye ait elemanlardır.

Bu yöntemle damga bilgisi, görüntünün en az değerlikli bitlerine saklandığından gözle görülemeyecek bir değişiklikle damgalama yapılmış olur. Ancak yapılacak saldırılar sonucu görüntü içindeki bilgi kolayca kaybedilebilir. Gizli bilginin damgalanacağı piksel değerliğinin arttırılması ile dayanıklılık arttırılabilir fakat orijinal görüntü üzerinde oluşan bozulma da üstel olarak artar.

Görünmez dayanıklı filigran damgalama yöntemlerinde, filigranın görüntü içinde ağırlığının az tutulması onun algılanması olasılığını azaltıp görünmezliğini arttırır. Ancak, dayanıklılığının sağlanması için filigranın görüntüdeki ağırlığının arttırılması gereklidir. Dolayısıyla, birbirine ters orantılı olarak ortaya çıkan bu durumda bir denge bulunarak, filigranın her iki özelliği de sağlayan en uygun ağırlık tespit edilerek görüntüye damgalanmalıdır.

Uzay düzleminde piksellerin değerlerin değerlerinin değiştirilmesine bağlı bir yöntem KUTTER ve ark. (1997) tarafından geliştirilmiştir. Bu yöntem ile, üç kanallı renkli görüntülerin mavi kanalı kullanılarak görünmez, kör damgalama gerçekleştirilmiştir. Burada mavi kanalın kullanılmasının nedeni, renkli görüntülerde parlaklığa katkısının diğer kanallara göre az olmasıdır. Damgalanacak bilgi, her pikselin mavi kanalının yoğunluğunun belli bir ağırlık oranında arttırılması ya da azaltılması

yoluyla yapılmıştır. Bu oranın tespitinde, bilginin görüntü içindeki dayanıklılığı ile buna ters orantılı olan görünmezliğinin sağlanmasının göz önünde bulundurulmasına dikkat çekilmiştir. Ancak, görüntüye damgalanan bilginin geri alınmasında performansı arttırmak için, görüntüye birden fazla damgalanması gerektiği vurgulanmıştır. Bu yöntem daha sonra ULUDAĞ ve ark. (2001) tarafından, geri alma performansının arttırılması amacıyla, damgalama formülüne standart sapma (Standard Deviation) ve eğim büyüklüğü (Gradient Magnitude) eklenerek geliştirilmiştir. Geliştirilen bu yöntemi, GÜNSEL ve ark. (2002) parmak izi görüntülerinin damgalanmasında kullanmışlardır. Benzer bir yöntem kullanarak JAIN ve ULUDAĞ (2002), bir parmak izinin sahibinin görüntüsüne damgalanarak yollanmasını ya da kişinin parmak izinin damgalandığı fotoğrafın güvenlik gerektiren kartlarda kullanılmasını önermiştir.

Görünür ve görünmez damgalamanın birlikte kullanıldığı bir yöntem MOHANTY ve ark. (1999) tarafından sunulmuştur. MINTZER ve ark. (1997) tarafından listelenen görünür damgalamanın özelliklerini sağlamaya yönelik yapılan çalışmada, insan gözü ile görülebilen bir filigran görüntü üzerine damgalanmakta ve ardından ancak bir bilgisayar yazılımı ile belki geri elde edilebilecek bir görünmez damgalama yapılmaktadır. Buna göre, “Dual Watermarking” olarak adlandırılan yöntem ile görüntü öncelikle görünür bir şekilde damgalanmaktadır. Ardından görünür olarak damgalanmış görüntüye görünmez bir damgalama uygulanmaktadır.

Uzay düzleminde yapılan birçok damgalama araştırmalarının yanında, yayınlanan araştırmaların önemli bir bölümünü de frekans düzleminde yapılan araştırmalar oluşturmaktadır. Görüntü bilgisinin frekanslarına ayrılmasında DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), DFT (Discrete Fourier Transform), FFT (Fast Fourier Transform) gibi dönüştürme araçları kullanılmaktadır. Bunların yanında Hadamard ve Chirp-Z dönüştürme araçlarının da kullanılarak geliştirilen damgalama yöntemleri önerilmiştir (FOTOPOULOS ve ark, 2000). Damgalanan bilginin görüntü içinde JPEG gibi kayıplı sıkıştırmaya karşı dayanıklılığının sağlanması amacıyla birçok çalışmada DCT kullanılmıştır.

HSU ve WU (1999) DCT tabanlı bir filigran damgalama algoritması önermişlerdir. Öncelikle filigran ikilik bir desene dönüştürülüp sonrasında permutasyon uygulanarak filigran, kendi içinde karıştırılmıştır. Damgalanacak görüntü DCT kullanılarak frekans düzlemine aktarılmış ve damgalama için kullanılacak frekanslar

belirlenmiştir. Bunların belirlenmesinde önemli rol oynayan iki etken, insan gözünün görüntünün alçak frekanslarındaki değişikliklere duyarlı olması ve yüksek frekansların JPEG gibi kayıplı sıkıştırma algoritmalarında dikkate alınmamasıdır. Bu nedenlerden dolayı, damgalama işlemi için orta frekans bandındaki frekanslar seçilmiştir. Blok tabanlı DCT uygulanan yöntemde, görüntü 8×8 piksel boyutlarına bloklara bölünmüş ve her blok ayrı ayrı frekanslarına ayrılmıştır. Bu bloklar da filigran gibi kendi içinde karıştırılarak, damgalanan filigranın görünmezlik özelliğinin artması amaçlanmıştır. Her blok içinden seçilen orta frekans katsayıları, komşu blokta aynı koordinattaki katsayılar ile karşılaştırılır. Bu karşılaştırma sonucunda 1 ve 0'lardan oluşan bir binary polarite tablosu, damgalanacak binary filigran ile XOR işlemine alınmıştır. Elde edilen yeni polarite tablosuna göre DCT ile hesaplanan frekans bileşenleri üzerinde değişiklik yapılmıştır. Kör olmayan, görünmez ve dayanıklı özelliklere sahip yöntem ile daha görünmez ve düşük seviyedeki JPEG kayıplı sıkıştırma saldırılarına karşı dayanıklı bir damgalama amaçlanmıştır. Görüntüden filigranın geri elde edilmesi için görüntünün aslı kullanılmıştır. Damgalanmış ve asıl görüntü frekans düzlemine dönüştürüldükten sonra seçilen frekanslardaki fark XOR işlemi ile bulunmuştur. Elde edilen binary değerlere ters-permutasyon uygulanarak filigran geri elde edilmiştir.

DCT kullanılarak yapılan bir başka damgalama yönteminde de üzerinde değişiklik yapılacak frekansların seçimi için genetik algoritma kullanılmıştır (SHIEH ve ark., 2004). Kör damgalama yöntemleri sınıfına giren bu algoritma ile bir görüntüye görünmez, dayanıklı filigran damgalanması gerçekleştirilmiştir. Blok tabanlı DCT kullanılan yöntemde, her bloğun DC değerinin AC frekansların katsayılarına oranının toplamından oluşan bir referans tablosu öncelikle oluşturulmuştur. Bir polarite kümesi de, her blok için, seçilen AC frekansın katsayısının ona karşılık gelen referans tablosundaki değerin çarpımı sonucunun aynı bloğun DC katsayısı ile karşılaştırılması ile elde edilmiştir. Her blok için bu kümenin elemanları, AC frekans katsayısı ve daha önce bir anahtar sayıya bağlı olarak permutasyon uygulanan ikilik filigranın değeri kullanılarak damgalama yapılmıştır. Geri elde etme algoritmasında da damgalama yapıldığı gibi referans tablosu ile polarite kümesi oluşturulmuştur. Sonra, her blok için bu kümenin elemanları ile filigranın arandığı AC değerin referans tablosundaki ilgili değerle çarpımından gelen sonuç o bloğun DC katsayısı ile karşılaştırılmasından ikilik filigranın bilgisi elde edilmiştir. Damgalamadan önce filigran, bir anahtar sayıya bağlı

olarak permutasyon uygulandığından, filigranın oluşturmak için elde edilen filigran bilgisine aynı anahtar sayı kullanılarak ters-permutasyon uygulanmıştır.

SHIH ve WU (2003) hem uzay düzlemi hem de frekans düzlemini birlikte kullanarak, sayısal görüntülere, kalitesinde daha az bozulma ile filigran damgalamak için bir yöntem önermişlerdir. Bu yöntemde, görüntüye daha büyük bir filigranın damgalanması için öncelikle filigran iki parçaya ayrılmıştır. Filigranın bir bölümü uzay düzleminde en az değerlikli bitlerin değiştirilmesi ile görüntüye damgalanmıştır. Ardından damgalanan görüntüye, frekans düzleminde filigranın diğer bölümü damgalanmıştır.

3. MATERYAL VE YÖNTEM

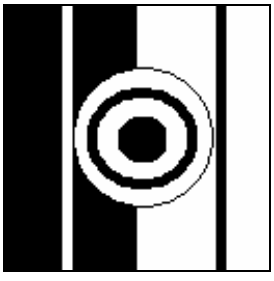
3.1. Giriş

Bu bölümde, sayısal görüntülere filigran damgalanması amacıyla ilk kez önerilen bir yöntem ayrıntılarıyla anlatılmaktadır. Yöntemin geliştirilmesinde kullanılan araçlar 'Materyal' alt başlığı altında yer almaktadır. Damgalama ve geri alma algoritmalarının yapısı ile çalışması hakkında ayrıntılı bilgi 'Yöntem' alt başlığı altında ele alınmıştır.

3.2. Materyal

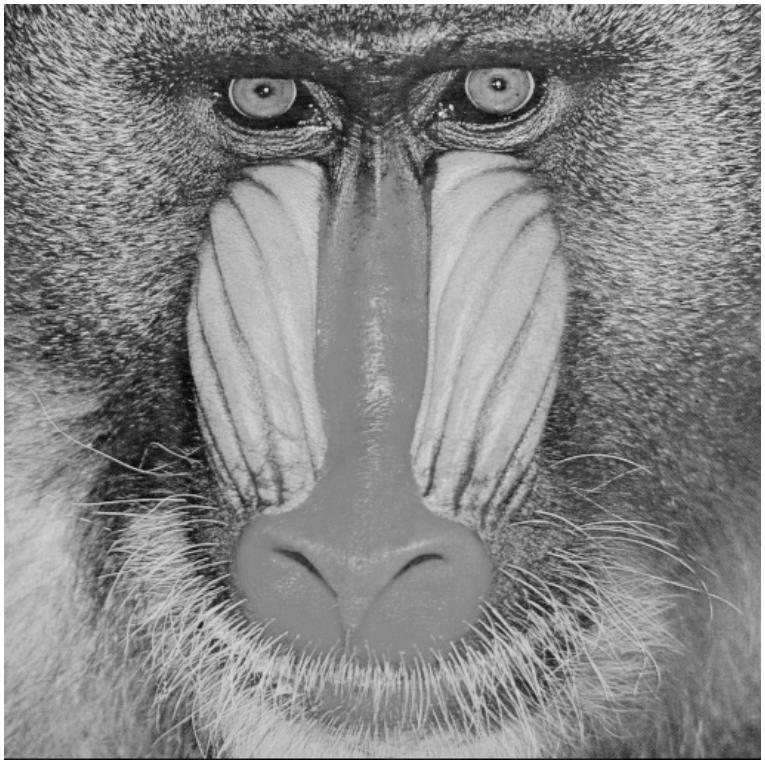
Bu çalışmada bilgisayar ortamına aktarılan görüntülere filigran damgalaması ve geri eldesi amacıyla geliştirilen yöntem için bir bilgisayar yazılımı hazırlanmıştır. Bu yazılım için Borland™ Delphi 7 görsel programlama dili kullanılmıştır. Yazılımın hazırlandığı ve testlerin yapıldığı bilgisayar, Intel™ Pentium IV 3.0 GHz işlemcili, üzerinde 1 GByte RAM ve 128 MB ekran kartı bulunan bir masaüstü bilgisayarıdır.

Testler için kullanılan filigran, Şekil 3.1.'de görülen 128×128 piksel boyutlarındaki siyah–beyaz bir logodur. Bu logo, sayısal görüntü işleme ve damgalama yöntemlerinin testleri için oldukça yaygın olarak kullanılan 512×512 piksel boyutlarındaki Lena, Baboon ve Peppers görüntülerine damgalanmıştır (Şekil 3.2.). Testlerde kullanılan tüm görüntüler gri seviyede Bitmap formatındadır.



Şekil 3.1. Taşıyıcı görüntüye damgalanacak 128×128 piksel boyutlarındaki filigran

(a)



(b)

Şekil 3.2. Testler için seçilen taşıyıcı görüntüler, a) Lena, b) Baboon, c) Peppers.

(c)

Şekil 3.2. (Devam) Testler için seçilen taşıyıcı görüntüler, a) Lena, b) Baboon, c) Peppers

3.3. Yöntem

Literatürde; sayısal görüntülere gizli bir bilginin damgalanması için önerilen yüzlerce farklı algoritma vardır. Bu algoritmaların yapılarına göre sınıflandırılması Şekil 2.2.'de görülmektedir. Bu çalışma ile; sayısal görüntülere görünmez ve dayanıklı bir şekilde damgalama işlemi için uzay ve frekans düzlem bileşenlerinin bir arada kullanıldığı hibrit bir yöntem önerilmiştir. Damgalama işlemi frekans düzlemi bileşenleri kullanılarak yapılırken referans noktasının tayininde uzay düzlemi enerjisi görevlendirilmiştir. Farklı düzlemlerin bir arada kullanılmasının literatürde mevcut olan yöntemlere göre daha dayanıklı damgalama işlemi yapacağı öngörülmüştür.

Literatürde uzay ve frekans düzlemlerinin bir arada kullanıldığı damgalama yöntemleri (SHIH ve WU, 2003) olmakta beraber, bu metotlarda damgalama işlemi her iki düzleme ayrı ayrı yapılmıştır. Filigranın bir kısmı frekans düzlemine damgalanırken, diğer bir kısmı da uzay düzlemine doğrudan damgalanmıştır. Bu çalışma ile önerilen

yöntemde bunların aksine damgalama ve geri elde etme algoritmaları her iki düzlemden elde edilen parametreleri kullanarak damgalama işlemi gerçek anlamda iki düzleme de bağıl olması sağlanmıştır.

Önerilen yöntemin ayrıntıları 3.3.1 ve 3.3.2 bölümlerinde açıklanacaktır. Damgalama için görüntü ile filigran üzerinde yapılan ön işlemler, damgalama algoritması ve damgalanmış görüntünün oluşturulması yöntemin ilk aşamasını oluşturmaktadır. İkinci aşamada ise filigranın geri elde edilmesi için sırasıyla ön işlemlerin yapılmasının ardından geri elde etme algoritmasının çalıştırılması ve son olarak filigranın oluşturulması hakkında ayrıntılarıyla bilgi verilecektir.

3.3.1. Damgalama İşlemi

Damgalanmış bir görüntüye yapılan saldırıların türleri düşünüldüğünde, saldırılara karşı algoritmaların frekans düzlemini sıklıkla kullandıkları görülmektedir (HARTUNG ve KUTTER, 1999). Bu amaçla, Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) ve Discrete Cosine Transform (DCT) en çok kullanılan dönüştürme araçlarıdır. JPEG kayıplı sıkıştırma algoritmasında da kullanılan DCT, yaygın bir kullanım sağlamış ve pek çok çalışmada damgalama için DCT katsayıları üzerinde değişiklik yapılmıştır. Bu nedenle, çalışmamızda, taşıyıcı görüntü ilk olarak JPEG sıkıştırma algoritmasında kullanıldığı gibi, 8×8 piksel boyutlarında bloklara ayrılmıştır. Ardından, DCT dönüştürme aracı ile frekans bileşenleri hesaplanmıştır. Damgalama işlemi, DCT ile elde edilen frekans katsayıları üzerinde yapılan değişiklikle gerçekleştirilmiştir. Taşıyıcı görüntüye damgalanacak filigranın dayanıklılığının ve görünmezliğinin arttırılması amacıyla, damgalama öncesinde filigrana permutasyon uygulanmıştır.

Damgalama işlemi yapılmadan önce taşıyıcı ve filigran görüntülerine bir dizi ön işlem uygulanması gerekmektedir.

Taşıyıcı görüntüye blok tabanlı DCT uygulanarak her bloğun DC ve AC frekans katsayıları hesaplanır. Görüntü kalitesine yönelik yapılan saldırılar sonunda DC ile uzay (spatial) düzleminden elde edilen enerjinin arasındaki farkın değişimi (Çizelge 3.1.), frekans düzleminden elde edilen enerjiye (Çizelge 3.2.) göre daha az olmaktadır.

Dolayısıyla, uzay düzleminde her bir bloğun enerjisi hesaplanarak damgalama işlemi sırasında hayati öneme sahip referans noktası olarak tayin edilir.

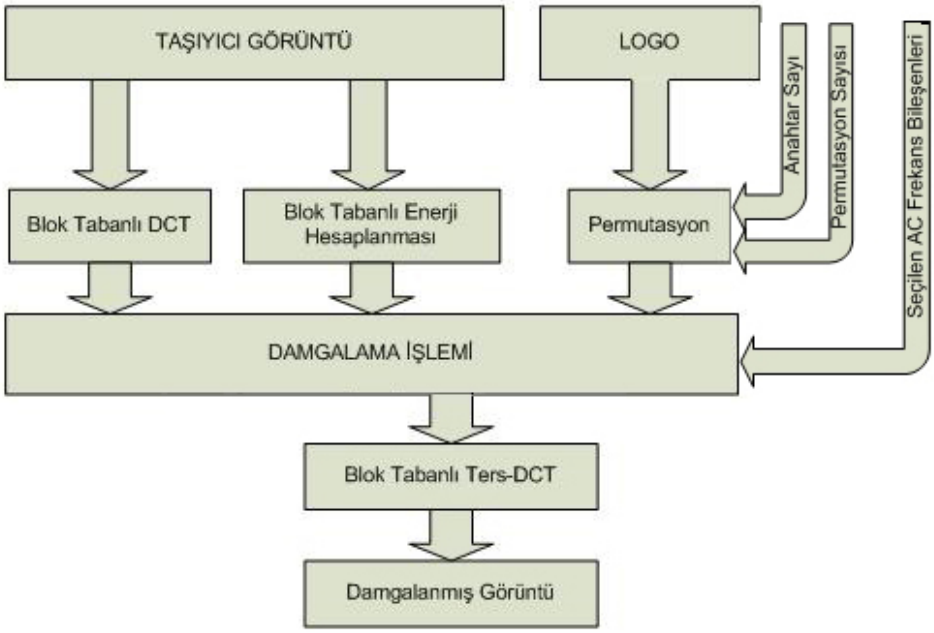
Çizelge 3.1. DC ile uzay düzleminden elde edilen enerji arasındaki farkın, kaliteye yönelik saldırılar sonundaki değişimi

TESTLER	ORTALAMA DEĞİŞİM (DC-Uzay Enerjisi)		
	Lena	Baboon	Peppers
Gaussian LPF	2,009	13,198	2,752
LPF	2,385	14,775	3,243
HPF	19,858	120,044	30,691
MEDIAN	1,375	11,412	1,576
JPEG (%80)	0,328	0,869	0,404

Çizelge 3.2. DC ile frekans düzleminden elde edilen enerji arasındaki farkın, kaliteye yönelik saldırılar sonundaki değişimi

TESTLER	ORTALAMA DEĞİŞİM (DC-Frekans Enerjisi)		
	Lena	Baboon	Peppers
Gaussian LPF	12,868	64,114	16,872
LPF	14,277	72,825	18,278
HPF	91,201	305,429	139,272
MEDIAN	9,361	55,643	13,259
JPEG (%80)	2,468	2,292	2,786

Filigran görüntüsü ise görüntü işleme saldırılarına karşı dayanıklılığını arttırmak için permutasyona uğratılır. Bölüm 3.3.1.4.'de detayları verilen damgalama algoritması ile taşıyıcı görüntü damgalanır ve uygulanan ters DCT ile damgalanmış görüntü elde edilir (Şekil 3.3.).



Şekil 3.3. Damgalama algoritmasının blok diyagramı

Takip eden alt bölümlerde damgalama algoritması ile birlikte kullanılan ara işlemlerin detayları verilmiştir.

3.3.1.1. DCT Dönüşümü

H'ın $N_1 \times N_2$ piksel boyutlarında, tüm pikselleri 0–255 renk aralığına sahip taşıyıcı görüntü olduğunu varsayalım.

$$H = \{h(x,y), 0 \le x < N_1, 0 \le y < N_2\} \tag{3.1.}$$

H taşıyıcı görüntüsü öncelikle 8×8 piksellik bloklara ayrılarak bu görüntünün frekans analizi için Denklem 3.2. ile her bloğa ayrı ayrı DCT uygulanır.

$$\tilde{H}_b(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} h_b(x,y)\cos\left(\frac{(2x+1)u\pi}{2\times 8}\right)\cos\left(\frac{(2y+1)v\pi}{2\times 8}\right) \tag{3.2.}$$

Burada; *b* blok numarası olup $0 \le b \le \frac{N_1}{8} \times \frac{N_2}{8} - 1$ arasında değer alabilir. *u* ve *v* frekans düzlemine taşınan bloğun frekans bileşenlerinin koordinatlarını, $\tilde{H}_b(u,v)$ bu koordinatlardaki bileşenin değerini gösterir. $\alpha(u)$ ile $\alpha(v)$ aşağıdaki denklem kullanılarak bulunur.

$$\alpha(i) = \begin{cases} \sqrt{\frac{1}{8}}, & i = 0 \quad için \\ \sqrt{\frac{2}{8}}, & i = 1,2,...,7 \quad için \end{cases} \tag{3.3.}$$

3.3.1.2. Enerji Hesabı

Uzay düzleminde her bloğun enerjisini hesaplamak için Denklem 3.4. kullanılır.

$$E_b = \sum_{x=0}^{7} \sum_{y=0}^{7} [h_b(x,y)]^2 \tag{3.4.}$$

3.3.1.3. Permutasyon

Damgalama sonucu sayısal görüntüde oluşan bozulma, kullanılan filigranın büyüklüğü ile doğru orantılıdır. Renkli ya da gri seviyeli bir filigran yerine taşıyıcı görüntüye damgalamak için Şekil 3.1.'de görülen 128×128 piksel boyutlarındaki siyah-beyaz logo, *W,* seçilmiştir. Bu logoda, beyaz rengin piksel yoğunluğu "1" atanarak ikilik (binary) logoya, W_b, dönüştürülür. Böylece logonun büyüklüğü, taşıdığı bilgi değiştirilmeden en az seviyeye indirilir. Ayrıca, taşıyıcı görüntünün kırpılmasıyla kaybedilen bilginin logonun geneline yayılması için, damgalama işleminden önce ikilik logoya permutasyon uygulanır (Denklem 3.5.). Bu amaçla, bir anahtar sayı *K*, kullanılarak 0 ile logonun piksel sayısı arasında olan rasgele sayılar üretilir. Logonun pikselleri, önce soldan sağa, sonra yukardan aşağıya olmak üzere numaralandırılır. Daha sonra, üretilen her rasgele sayı, logonun bir pikselinin numarasını temsil etmek üzere, sırasıyla yan yana olan sayıların gösterdiği pikseller yerleri değiştirilerek permutasyon işlemi gerçekleştirilir. Bu işlem birden fazla da uygulanabilir.

$$W_p = P(W_b, K, M_1 \times M_2) \tag{3.5.}$$

Burada; $M_1 \times M_2$, ikilik filigranın boyutlarını,

K, rasgele sayı üretmek için seçilen anahtar sayıyı,

W_b, ikilik filigranı,

W_p, permutasyon uygulanmış ikilik logoyu göstermektedir.

Permutasyon işleminin ardından logo, taşıyıcı görüntü ile aynı sayıda bloklara ayrılır. Görüntünün her bloğuna logonun bir bloğu damgalanacaktır. Damgalama sonucu görüntü üzerinde oluşacak bozulma logo bloklarının büyüklüğü ile doğru orantılıdır.

3.3.1.4. Damgalama Algoritması

Damgalama için kullanılacak AC frekansların seçimi, taşıyıcı görüntüye logonun getirdiği bozulma ve logonun çeşitli resim işleme saldırılarına karşı olan dayanıklılığı ile yakından ilgilidir. Damgalama işlemi, eğer alçak frekans bandında bulunan frekanslar üzerinde yapılırsa, görüntü üzerinde gözle görülür bir bozulmaya neden olur. Ancak, kullanılacak AC frekanslar, yüksek frekanslar arasından seçilirse, JPEG kayıplı sıkıştırma algoritmasının, kuantalama sırasında, bu banttaki frekansları göz ardı etmesinden dolayı damgalanan logo kaybedilebilir. Bu iki nedenden dolayı, birçok çalışmada olduğu gibi bu çalışmada da, damgalama için orta frekans bandından seçilen frekanslar kullanılmıştır.

DCT ile frekanslarına ayrılan 8×8 piksel boyutlarındaki her blok içinde 63 AC frekansın katsayısı ile bir DC katsayısı bulunur. Şekil 3.4.'de zikzak numaralandırılmış bir görüntü bloğu görülmektedir. Sol üstte yer alan 0 numaralı hücre DC, diğerleri AC frekans katsayılarını göstermektedir. Gri renk ile doldurulmuş hücreler orta frekans bandıdır.

0	1	5	6	14	15	27	28
2	4	7	13	**16**	26	29	42
3	8	12	17	**25**	30	41	43
9	11	18	**24**	31	40	44	53
10	**19**	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Şekil 3.4. Zikzak numaralandırılmış görüntü bloğu

Bu çalışmada, yapılan testler sonucu, yukarıdaki şekilde orta frekans bandı içinde vurgulanan 16, 19, 24 ve 25 numaralı frekanslar damgalama için seçilmiştir.

Sabit renk yoğunluğuna sahip bir görüntünün 8×8 piksel boyutlarındaki her bloğu için hesaplanan DC katsayısı, aynı bloğun enerjisinin karekköüne eşittir. Ancak gerçek görüntülerde bu eşitlik bozulmakta ve aradaki fark AC frekansların katsayılarının yüksekliği ile orantılı olmak üzere artmaktadır. Bu nedenle, damgalama işlemi için bir referans noktası belirlemek gereklidir. Önerdiğimiz yöntemde, enerjinin karekökü referans olarak alınmıştır (Denklem 3.6.). Bu sayı, aynı bloğun DC değeri ile kullanılacak AC frekansın katsayısının toplamı ile karşılaştırılarak damgalama gerçekleştirilecektir. AC bileşeninin katsayısındaki değişiklik en fazla kullanılan ağırlık kadar olacaktır.

$$R = \sqrt{E} \tag{3.6.}$$

Damgalama algoritması ayrıntıları ile şöyle açıklanabilir: Bir görüntü bloğu için kullanılacak referans *R,* damgalama ağırlığı λ, damgalanacak ikilik filigranın bilgisi *f*, *DC* ve *AC* ise hesaplanan frekans katsayılarını temsil etmek üzere, aşağıdaki denklem ile öncelikle *n* değişkeni hesaplanır.

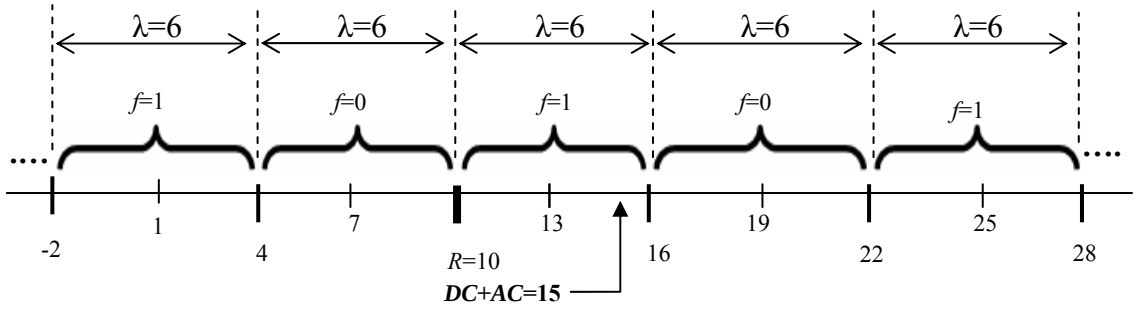
$$n = \begin{cases} R + \dfrac{4n-1}{2}\lambda < DC + AC \le R + \dfrac{4n+3}{2}\lambda, & f = 1 \quad ise \\ R + \dfrac{4n-3}{2}\lambda < DC + AC \le R + \dfrac{4n+1}{2}\lambda, & f = 0 \quad ise \end{cases} \tag{3.7.}$$

Denklem 3.7.'den elde edilen *n,* Denklem 3.8.'de yerine konularak yeni AC katsayısı, AC' bulunur.

$$AC' = \begin{cases} R + \dfrac{4n+1}{2}\lambda - DC, & f = 1 \quad ise \\ R + \dfrac{4n-1}{2}\lambda - DC, & f = 0 \quad ise \end{cases} \tag{3.8.}$$

Damgalama algoritması bir örnek ile daha iyi anlaşılabilir. Görüntünün bir bloğunda *R*=10, *DC*=11 ve seçilen *AC*=4 olsun. Damgalama ağırlığı *λ*=6 ve damgalanacak filigran bilgisi *f*=1 olmak üzere, ilk olarak Denklem 3.7. kullanılarak *n* değişkeni 0 olarak hesaplanır. Hesaplanan *n,* Denklem 3.8.'de yerine konularak AC'=2 olarak bulunur. Eğer *f*=0 ise Denklem 3.7. kullanılarak *n*=1 bulunur. Yeni *AC* katsayısı için Denklem 3.8.'den 8 olarak bulunur.

Yukarıda formüllerle ifade edilen damgalama algoritması Şekil 3.5.'deki dönüşüm cetveli kullanılarak daha basit bir şekilde uygulanabilir.



Şekil 3.5. Damgalama algoritması oluşturulan dönüşüm cetveli

Bir dönüşüm cetveli üzerinde referans noktasının bulunduğu yerden başlayarak cetvel, her iki yöne doğru her biri λ kadar uzunlukta birimlere bölünür. Her birime, kullanılacak ikilik filigranın alacağı değerler (0 ve 1) ardışık olarak atanır. DC ile AC katsayılarının toplamının aldığı değerin bu cetvel üzerindeki yeri tespit edilir. Damgalanacak filigranın bilgisine (0 ya da 1) göre, DC ile AC katsayılarının toplamı en yakın ilgili birimin orta noktasına gelecek şekilde yeni AC belirlenir.

Verilen örnekte λ=6 olduğundan, dönüşüm cetveli referans noktasından itibaren 6 birimlik bölümlere ayrılır. Cetvel üzerinde DC+AC=15 olarak aldığı değer işaretlenir. Buna göre, filigran bilgisi f=1 için AC değeri DC+AC=13 olacak şekilde tekrar hesaplanır. Buradan yeni AC değeri 2 olarak saptanır. Eğer filigran bilgisi f=0 ise, yeni AC değeri DC+AC=19 olacak şekilde hesaplanır ve 8 olarak bulunur.

Görüntünün tüm bloklarında seçilen AC frekanslarına damgalama işlemi uygulandıktan sonra ters DCT (Denklem 3.9.) ile yeni piksel yoğunlukları, $h_b^w(x,y)$, hesaplanır.

$$h_b^w(x,y)=\sum_{u=0}^{7}\sum_{v=0}^{7}\alpha(u)\alpha(v)\tilde{H}_b(u,v)\cos\left(\frac{(2i+1)u\pi}{2\times 8}\right)\cos\left(\frac{(2j+1)v\pi}{2\times 8}\right) \qquad (3.9.)$$

Burada; $\tilde{h}_b(u,v)$ bloğun (u,v) koordinatındaki frekansının katsayısını, $h_b^w(x,y)$ bloğun uzay düzleminde (x,y) koordinatında bulunan pikselinin yeni renk yoğunluğunu temsil etmektedir. Denklemde yer alan $\alpha(u)$ ile $\alpha(v)$ aşağıdaki gibi hesaplanır.

$$\alpha(i) = \begin{cases} \sqrt{\frac{1}{8}}, & i = 0 \quad için \\ \sqrt{\frac{2}{8}}, & i = 1,2,...,7 \quad için \end{cases} \tag{3.10.}$$

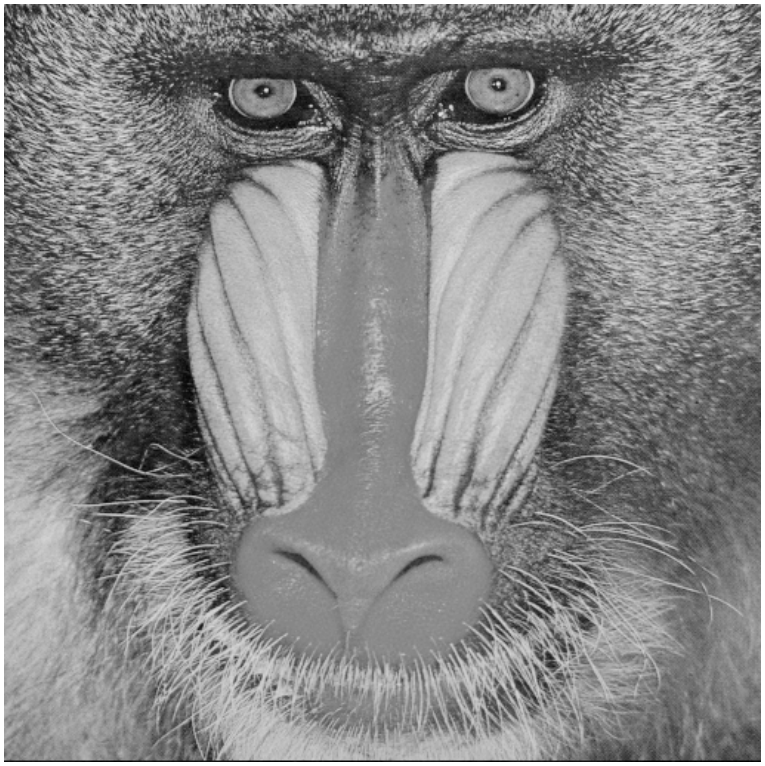
Frekans düzleminden uzay düzlemine geri dönüştürülen blokların birleştirilmesi ile damgalanmış görüntü elde edilir.

$$H_w = \left\{ h_b^w(x,y), 0 < x \le N_1, 0 < y \le N_2 \right\} \tag{3.11.}$$

Şekil 3.6.'da λ=10 ağırlıkla filigran damgalanan Lena, Baboon ve Peppers görüntüleri yer almaktadır.

(a)

Şekil 3.6. λ=14 ağırlıkla filigran damgalanan taşıyıcı görüntüler, a) Lena, b) Baboon, c) Peppers



(b)

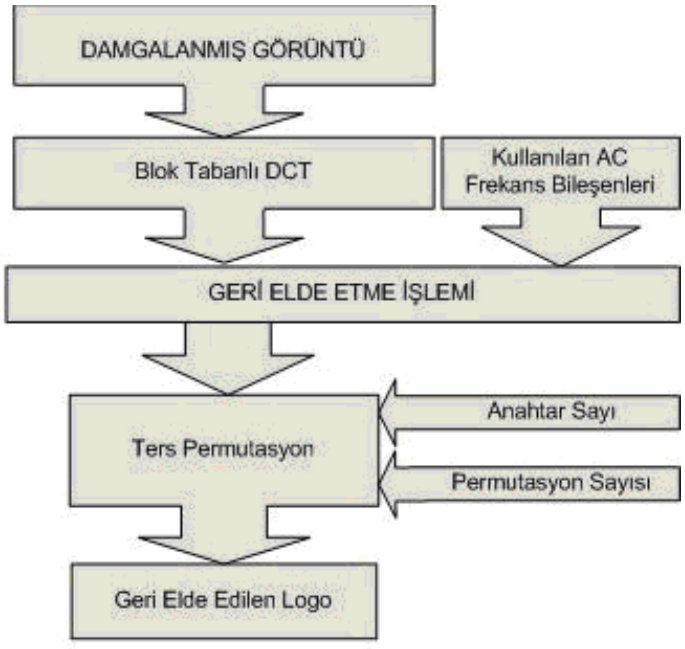
(c)

Şekil 3.6. (Devam) λ=14 ağırlıkla filigran damgalanan taşıyıcı görüntüler, a) Lena, b) Baboon, c) Peppers

3.3.2. Filigranın Geri Elde Edilmesi

Taşıyıcı görüntüye damgalanan filigranın geri elde edilmesi için asıl görüntü ya da filigranın kendisi kullanılmaz. Görüntüden filigranın elde edilmesinde, damgalama işleminde kullanılan AC frekansları, damgalama ağırlığı ile filigranın permutasyonunda seçilen anahtar sayı kullanılır. Şekil 3.7.'de geri elde etme algoritmasının blok diyagramı görülmektedir.

Öncelikle damgalanmış görüntü 8×8 piksel boyutlarında bloklara ayrılarak her bloğun frekans bileşenleri Denklem 3.2., enerjisi ise Denklem 3.4. kullanılarak hesaplanır.



Şekil 3.7 Geri elde etme algoritmasının blok diyagramı

Filigranın taşıyıcı görüntüden geri elde edilmesi damgalanma algoritmasına benzer şekilde yapılır. Blok bazında aranacak filigran bilgisi için damgalama algoritmasında olduğu gibi, bloğun enerjisinin karekökü, *R,* referans alınarak DC ve *AC* katsayılarının toplamı ile karşılaştırılır. Buna göre, Denklem 3.12. kullanılarak öncelikle n' tespit edilir.

$$n' \Leftarrow R + n'\lambda < DC + AC \leq R + n'\lambda \qquad (3.12.)$$

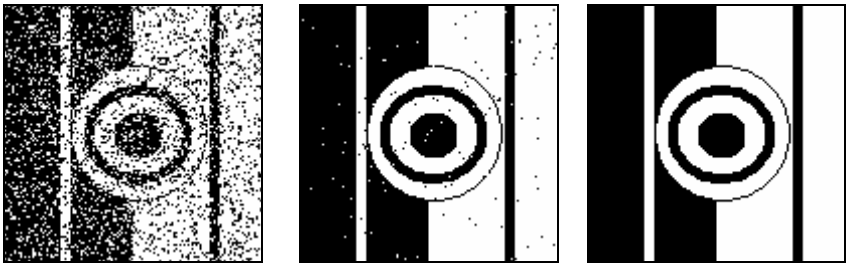
Bulunan n' değeri çift sayı ise buraya damgalanan filigran bilgisi "1", tek ise "0" olarak elde edilir (Denklem 3.13.).

$$f' = \begin{cases} 1, & n' \ \ çift \ \ ise \ \ (...,-2,0,2,4,...) \\ 0, & n' \ \ tek \ \ ise \ \ (...,-3,-1,1,3,...) \end{cases} \tag{3.13.}$$

Taşıyıcı görüntüden elde edilen ikilik desen, permutasyon uygulanmış filigran verisidir. Filigrana, taşıyıcı görüntüye damgalanmadan önce bir anahtar sayı kullanılarak permutasyon uygulandığından, elde edilen filigran verisine de aynı anahtar sayı ile aynı sayıda ters-permutasyon uygulanır (Denklem 3.14.). Böylece ikilik filigranın aslı elde edilir. Son olarak elde edilen ikilik filigranda beyaz renk "1" ile temsil edildiğinden yoğunluğu "1" olan pikseller "255" atanarak siyah-beyaz logo elde edilir.

$$W'_p = P^{-1}(W'_b, K, M_1 \times M_2) \tag{3.14.}$$

Şekil 3.8.'de, en düşük üç damgalama ağırlığı olan λ=2, 4 ve 6 ağırlıkla damgalanmış Lena görüntülerinden geri elde edilen logolar gösterilmektedir. Az ağırlık oranıyla (λ=2 ve λ=4) görüntüye damgalanan logolar, DCT dönüşümü, damgalama ve ters DCT işlemlerindeki yuvarlamalardan kaynaklanan veri kaybından dolayı bir miktar bozulma ile geri elde edilirken, λ=6 ve üzeri ağırlıklarla yapılan damgalamalarda bu bozulma görülmemektedir.



(a) (b) (c)

Şekil 3.8. Lena görüntüsünden geri elde edilen logolar, a) λ=2 ağırlıkla damgalanmış görüntüden, b) λ=4 ağırlıkla damgalanmış görüntüden, c) λ=6 ağırlıkla damgalanmış görüntüden

4. ARAŞTIRMA BULGULARI VE TARTIŞMA

4.1. Giriş

Sayısal görüntülere yapılan gizli filigran damgalama çalışmalarında öngörülen hedefler; görünmezliğin sağlanması, damgalamanın taşıyıcı görüntüye getirdiği bozulmanın en az seviyede tutulması ve damgalanan filigranın çeşitli görüntü işleme saldırılarına karşı dayanıklı olması olarak özetlenebilir.

Damgalama sonucu filigranın taşıyıcı görüntüde yarattığı bozulma taşıyıcı görüntünün kalitesini düşürdüğü gibi, hedeflenen görünmezliği de olumsuz olarak etkilemektedir. Bu amaçla damgalama ağırlığı en az seviyede tutulmaktadır. Ancak, çeşitli görüntü işleme saldırılarına karşı filigranın tanınabilir nitelikte geri elde edilmesinin sağlanması damgalama ağırlığının arttırılması ile mümkündür. Her iki amaca uygun bir damgalama ağırlığı bulmak için taşıyıcı görüntüler 2 – 46 arasında değişen 23 farklı ağırlıkta damgalanmıştır. Aralarından seçilen çeşitli ağırlıklarla damgalanan görüntülere filigranı yok etmeye yönelik saldırılar yapılmış, geri elde edilen filigranın aslına benzerliği ölçülmüştür. Görüntü işleme saldırıları hakkında bilgi takip eden bölümde yer almaktadır.

4.2. Damgaya Karşı Yapılabilecek Saldırı Çeşitleri

4.2.1. Basit Saldırılar

Gizli ve dayanıklı bir şekilde damgalanan filigranın yok edilmesi amacıyla yapılan basit saldırılar, görüntü kalitesinde fark edilmeyecek derecede değişiklik yapabilen çeşitli görüntü işleme algoritmalarıdır. Saldırı sonucu taşıyıcı görüntüdeki filigran bozulabilir ya da filigran geri elde edilemeyecek derecede zarar görebilir (ARNOLD ve ark., 2003).

4.2.1.1. JPEG Kayıplı Sıkıştırması

JPEG, günümüzde en yaygın olarak kullanılan sıkıştırma yöntemlerinden biri olmasının yanında, görüntü boyutunun küçülmesine ters oranla koruduğu görüntü kalitesi nedeniyle de tercih edilen bir sıkıştırma yöntemidir. JPEG sıkıştırması DCT kullanılarak yapılan blok tabanlı bir dönüştürme algoritmasına dayanmaktadır. Temel olarak JPEG kayıplı sıkıştırması, DCT ile dönüştürülen görüntünün yüksek frekanslı bileşenlerinin istenen sıkıştırma oranında silinmesine dayanır. JPEG algoritmasının bu özelliğinden faydalanılarak damgalanmış görüntüden filigranın yok edilmesi amaçlanır. Eğer filigran bilgisi taşıyıcı görüntünün yüksek frekans bileşenlerine saklanmışsa, JPEG kayıplı sıkıştırması sonucu filigran tanınabilir benzerlikte elde edilemeyecek şekilde yok olabilir. Böylece görüntü kalitesinde önemli bir düşmeye sebep olmadan filigran yok edilebilir.

4.2.1.2. Kırpma (Cropping)

Kırpma, taşıyıcı görüntünün bir bölümünün kesilmesi ile gerçekleştirilir. Taşıyıcı görüntülere yapılan gizli ve dayanıklı damgalama işleminde damganın yeri belli değildir. Kırpma işlemi ile görüntüden ayrılan bölümde var olabilecek filigran bilgisinin yok edilmesi ve böylece filigranın geri elde edilemeyecek derecede zarar görmesi amaçlanır. Eğer damga taşıyıcı görüntüye görünür bir şekilde yerleştirilmişse, damganın yok edilmesi için yapılabilecek en kolay saldırı kırpmadır. Bununla birlikte, damganın kırpılıp görüntüden ayrılması görüntünün bütünlüğünde ciddi bir etki bozulmaya sebep olacaksa, kırpma saldırısının yapılması, geriye kalan görüntü değerlendirildiğinde anlamsız olmaktadır.

4.2.1.3. Gürültü Ekleme

Taşıyıcı görüntülere yapılacak gizli filigran damgalama işlemleri sonunda görüntü piksellerinin önemli bir bölümü ya da hepsi değişikliğe uğramaktadır. Dolayısıyla görüntünün değişen her pikseli damganın bilgisini taşımaktadır. Gürültü ekleme saldırısı gizli damgalama yöntemlerinin bu özelliğini hedef alır. Görüntü

kalitesinde önemli bir düşmeye sebep olmayacak bir şekilde, görüntünün her pikselinin rasgele arttırılması ya da azaltılması ile gürültü ekleme saldırısı gerçekleştirilir. Böylece görüntü içindeki damga, bu saldırı sonucu değişen piksel yoğunluklarından dolayı tanınamayacak bir nitelikte bozulmuş olarak elde edilebilir.

4.2.1.4. Tekrar Damgalama

Taşıyıcı görüntüye yapılabilecek saldırılardan bir diğeri de başka bir damgalama algoritması kullanarak görüntünün tekrar damgalanmasıdır. Böylece pikseller üzerinde yapılacak ikinci değişiklik, taşıyıcı görüntüye damgalanan ilk bilgiyi yok edebileceği gibi saldırganın da aynı görüntü üzerinde kendi haklarını savunabileceği bir bilgiyi görüntüye eklenmesine sebep olur.

4.2.2. Geometrik Saldırılar

4.2.2.1. Yatay Eksende Döndürme

Bu işlem, görüntünün yatay eksen etrafında 180^0 döndürülmesi ile yapılır. Görüntünün yatay eksende döndürülmesi kayıpsız bir şekilde gerçekleşeceğinden damgalanmış bir taşıyıcı görüntü yatay eksende tekrar döndürüldüğünde görüntünün aslı geri elde edilebilir. Böylece damgalanan bilgi bir bozulmaya uğramamış olur.

4.2.2.2. Dikey Eksende Döndürme

Görüntünün dikey bir eksen etrafında 180^0 döndürülmesi ile kayıpsız bir biçimde yapılabilir. Görüntünün kendisini elde etmek için dikey eksen etrafında tekrar döndürülmesi gerekir. Böylece görüntüye damgalanan bilgi kayıpsız bir şekilde geri elde edilebilir.

4.2.2.3. Açılı Döndürme

Genelde küçük bir açı oranında taşıyıcı görüntünün saat yönünde ya da tersi yönde döndürülmesi ile görüntü içindeki filigranın yok edilmesi amaçlanır. Yatay ve dikey eksende döndürmenin aksine açılı döndürme işleminde görüntü ebadı değişmekte ve orijinal ebat için görüntüye sonradan kırpma işlemi de uygulanmaktadır. Birçok damgalama algoritması bu saldırı türüne karşı hassastır.

4.2.2.4. Ölçekleme

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

4.2.2.5. Satır ya da Sütunların Silinmesi

Satır ya da sütunların silinmesi, uzay düzleminde yapılan en yaygın saldırılardan biridir. Satırlar ile sütunlar sonrakilerle yer değiştirilerek ya da silinenlerin yerine yanındakilerin kopyalanması ile gerçekleştirilen bir saldırı türüdür. Görüntü piksellerinin orijinal koordinatlarından ayrılmasıyla yapılan bu değişiklik, gözle fark edilemeyecek derecede olmasına rağmen görüntüye gizli bir şekilde damgalanan filigranın bozulmasına yol açabilmektedir.

4.2.2.6. StirMark

PETITCOLAS ve ark. (1998) tarafından geliştirilen bir dizi görüntü işleme saldırılarının birleşiminden oluşan damgalama algoritmaları için bir test yöntemidir. Sinyal arttırma, sıkıştırma, ölçekleme, kırpma, döndürme, geometrik dönüştürme ve görüntüyü geometrik olarak rasgele bozma işlemlerinden oluşan bu test yöntemi damgalama algoritmalarının dayanıklılığının test edilmesi için önerilmiştir.

4.2.3. Yok Etme Saldırısı

Yok etme işlemi, taşıyıcı görüntüye damgalanan bilgiyi sadece geri elde edilemeyecek şekilde bozmaya yönelik olmayıp onun yerinin tahmin edilip görüntüden ayrılması için yapılan saldırı türüdür. Bu saldırı ile damgalanan bilginin görüntüde sebep olduğu değişikliğin geri alınması ve böylece orijinal görüntünün elde edilmesi amaçlanır.

4.2.4. Kaliteye Yönelik Saldırılar

4.2.4.1. Filtreleme

Median filtresi ile alçak ve yüksek geçiren filtreler, sıklıkla kullanılan filtreleme çeşitleri arasında yer almaktadır. Median filtresi bir görüntünün ayrıntılarını koruyarak, üzerindeki gürültüyü yok etmek amacıyla kullanılır. Alçak geçiren filtre ile görüntünün yüksek frekanslı bileşenleri görüntüden ayrılır. Böylece daha düz ve yumuşak bir görüntü elde edilir. Yüksek geçiren filtre ise alçak frekans bileşenlerini görüntüden ayırarak daha keskin bir görüntü elde edilmesinde kullanılır. Filtreler ile yapılan saldırılarla, onların görüntü kalitesi üzerinde yaptığı değişiklikler göz önünde bulundurularak, taşıyıcı görüntüdeki filigranın bozulması hedeflenir.

4.2.4.2. Kontrast

Birçok görüntü işleme yazılımında standart olarak bulunan bir fonksiyondur. Görüntünün kontrastında yapılacak değişiklik ile yapılacak saldırı bazı damgalama algoritmaları için başarılı olabilmektedir.

4.2.4.3. Renk Kuantalama

Renk kuantalama, taşıyıcı görüntünün genelde Internet'te yayınlanacağı zaman GIF (Graphic Interchange Format) biçimine dönüştürülmesinde uygulanır.

4.3. Damgalama Algoritması Performans Değerlendirme Metotları

Hazırlanan filigran, λ=2 ile λ=46 arasında değişen 23 farklı ağırlık ile test görüntülerine damgalanmıştır. Elde edilen sonuçların değerlendirilmesinde, ölçüm kriteri olarak literatürde önerilen ve birçok damgalama yönteminin testlerinde kullanılan Mean Square Error (MSE), Peak-to-Signal Noise Ratio (PSNR) ile Normalized Correlation (NC) kullanılmıştır.

2 ile 46 arasında değişen 23 farklı ağırlıkla yapılan her damgalama sonunda, filigranın taşıyıcı görüntülerde oluşturduğu bozulma Mean Square Error (MSE) (Denklem 4.1.) ile ölçülmüştür. MSE, en basit ve en yaygın olarak kullanılan ölçümdür (WANG ve ark., 2004).

$$MSE_{XX'} = \frac{1}{N}\sum_{i=1}^{N}(X - X')^2 \qquad (4.1.)$$

Burada X damgalama öncesi görüntü elemanının orijinal piksel değerini, X' damgalama sonrası resim elemanının değerini, N ise toplam piksel sayısını belirtmektedir. Her pikselin orijinal değeri ile sapma miktarının farkının karesinin bir toplama eklenmesiyle yapılan toplam hata miktarı bulunur. Burada oluşan farkın karesinin alınması, negatif yönde olan farkın genel toplamdaki azaltma etkisini önlemektir.

Damgalama sonunda elde edilen görüntü X' ile orijinal görüntü X arasındaki kalite, Denklem 4.2.'de yer alan Peak-to-Signal Noise Ratio (PSNR) kullanılarak hesaplanmıştır.

$$PSNR_{XX'} = 10\log(\frac{255^2}{MSE_{XX'}}) \text{ (dB)} \qquad (4.2.)$$

Yukarıdaki denklemle ifade edilen kalite ölçütü birimi desibeldir (dB). Denklemde yer alan 255 sabit sayısı, görüntü piksellerinin alacağı en yüksek değeri göstermektedir.

λ=14, 18, 26 ve 38 ağırlıkları ile damgalanan test görüntülerine JPEG kayıplı sıkıştırması, kırpma, gürültü ekleme, alçak geçiren filtre (LPF-Low Pass Filter), Gaussian LPF, yüksek geçiren filtre (HPF-High Pass Filter), Median filtrelemeleri ile karalama, döndürme, kontrast ve tekrar damgalama saldırıları yapılmıştır. Saldırıların yapıldığı taşıyıcı görüntülerden filigranlar geri elde edilmiştir. Elde edilen filigranların

benzerliği Denklem 4.3.'de verilen Normalized Correlation (NC) kullanılarak ölçülmüştür.

$$NC = \frac{\sum_{i=1}^{N}(X \times X')}{\sum_{i=1}^{N}(X)^2} \tag{4.3.}$$

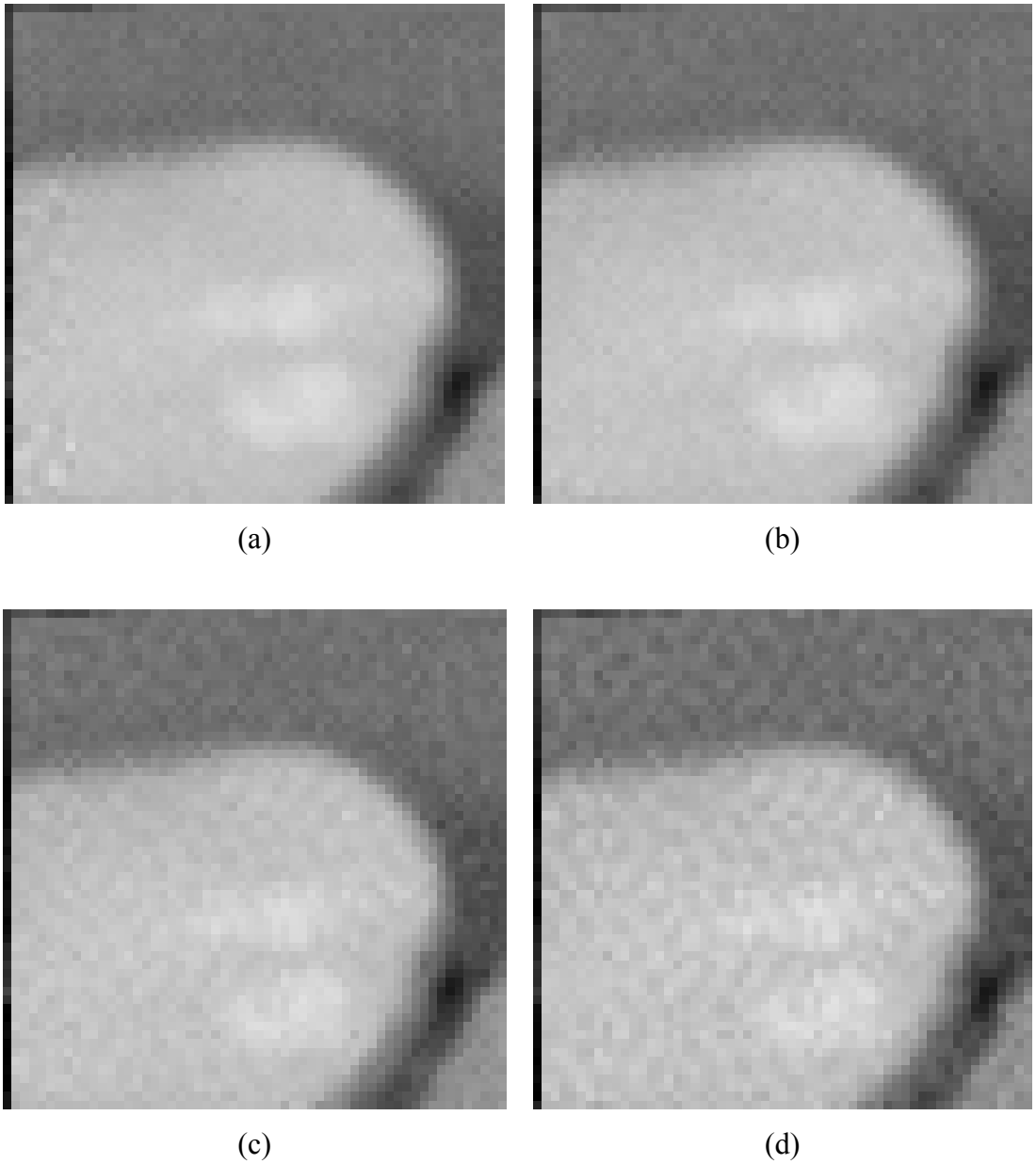
Burada X damgalama öncesi resim elemanının orijinal piksel değerini, X' damgalama sonrası resim elemanının değerini, N ise hesaplanan piksel sayısını göstermektedir.

4.4. Performans Değerlendirme Testleri

4.4.1. Damgalama Ağırlığının Görüntü Kalitesine Etkisi

Sayısal görüntülerin damgalanması ile görüntü kalitesinde bir bozulma görülmektedir. Oluşan bozulmanın nedenlerinden biri kullanılan damgalama ağırlığıdır. Şekil 4.1.'de 4 farklı ağırlıkla damgalanmış taşıyıcı Peppers görüntülerinin sol üst bölümünden alınan kesitler yer almaktadır. Bu kesitler incelendiğinde, damgalama ağırlığının artması ile birlikte görüntü üzerinde oluşan bozulmanın da arttığı görülmektedir.

Test için seçilen Lena, Peppers ve Baboon görüntüleri, 23 farklı ağırlık ile damgalandıktan sonra elde edilen görüntülerde oluşan bozulma MSE ile ölçülmüş, sonuçlar aşağıdaki Çizelge 4.1.'de verilmiştir.



(a) (b)

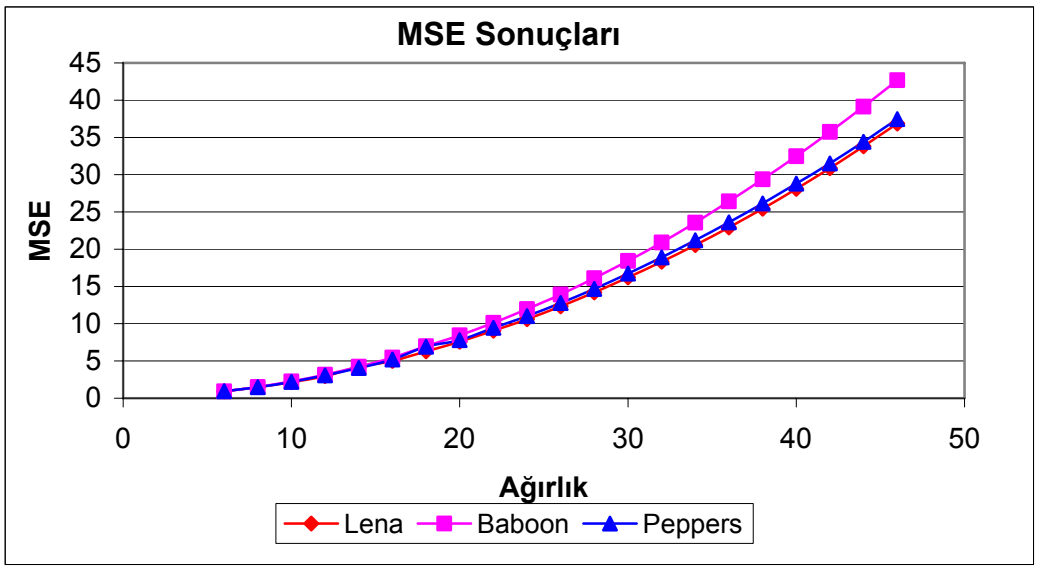
(c) (d)

Şekil 4.1. Çeşitli ağırlık oranlarıyla damgalanan Peppers görüntülerinden alınan kesitler, a) λ=6, b) λ=14, c) λ=26, d) λ=42

Çizelge 4.1.'deki sonuçlar, Şekil 4.2.'deki grafikle birlikte analiz edildiğinde, damgalama ağırlığının artmasıyla birlikte taşıyıcı görüntüler üzerinde oluşan bozulma da artmıştır. Lena ile Peppers görüntülerinde oluşan bozulma yaklaşık eşit olarak ölçülürken, Baboon görüntüsündeki bozulma diğerlerine göre daha hızlı artmıştır. Bunun gerekçesi, Baboon görüntüsündeki doku (texture) bilgisinin (tüyler) daha hızlı değişim göstermesidir.

Çizelge 4.1. λ=2 ile λ=46 arasında değişen 23 farklı ağırlık ile filigran damgalanan test görüntülerinde oluşan bozulmanın MSE ile ölçüm sonuçları

Ağırlık	Lena	Peppers	Baboon
2	0,3197	0,8144	0,4776
4	0,5512	0,5509	0,5620
6	0,9337	0,9349	0,9277
8	1,4734	1,4921	1,5029
10	2,1562	2,2003	2,2476
12	2,9656	3,0793	3,1569
14	4,2188	4,0549	4,2251
16	4,9972	5,1875	5,4597
18	6,2901	6,9111	6,9875
20	7,5896	7,8035	8,4463
22	9,0652	9,4437	10,1216
24	10,6115	11,0085	11,9660
26	12,3377	12,7909	13,9187
28	14,2028	14,6776	16,1012
30	16,2092	16,7420	18,4239
32	18,3240	18,9033	20,8956
34	20,5587	21,1940	23,5646
36	22,9272	23,6096	26,4225
38	25,4263	26,1436	29,3790
40	28,0969	28,8069	32,4690
42	30,8750	31,5175	35,7460
44	33,8102	34,4185	39,1371
46	36,8657	37,4678	42,6824



Şekil 4.2. Çeşitli ağırlıklarla filigran damgalanmış taşıyıcı görüntülerde oluşan bozulmanın ağırlığa göre grafiği

Orijinal görüntülerle çeşitli ağırlıklarda damgalanmış görüntüler arasındaki kalite PSNR ile ölçülmüş, sonuçlar aşağıdaki Çizelge 4.2.'de verilmiştir. 30–40 dB arasındaki PSNR sonuçları normal olarak kabul edilmektedir (SHIEH ve ark, 2004). PSNR değerinin düşmesi, görüntü kalitesindeki bozulmanın arttığını göstermektedir.

Çizelge 4.2. 2–46 arasında değişen 23 farklı ağırlık ile filigran damgalanan test görüntüleri ile orijinal görüntüler arasındaki kalite ölçümü, PSNR (dB) sonuçları

Ağırlık	Lena	Peppers	Baboon
2	53,083	49,022	51,340
4	50,718	50,720	50,633
6	48,429	48,423	48,457
8	46,448	46,393	46,362
10	44,794	44,706	44,614
12	43,410	43,246	43,138
14	41,879	42,051	41,872
16	41,144	40,981	40,759
18	40,144	39,735	39,688
20	39,329	39,208	38,864
22	38,557	38,379	38,078
24	37,873	37,714	37,351
26	37,218	37,062	36,695
28	36,607	36,464	36,062
30	36,033	35,893	35,477
32	35,501	35,365	34,930
34	35,001	34,869	34,408
36	34,527	34,400	33,911
38	34,078	33,957	33,450
40	33,644	33,536	33,016
42	33,235	33,145	32,599
44	32,840	32,763	32,205
46	32,465	32,394	31,828

SHIEH ve ark. (2004), geliştirdikleri damgalama algoritmasıyla kullandıkları λ=10 ile λ=30 ağırlıklarla damgalanan Lena görüntüsünden elde ettikleri en iyi kalite oranları ile bu çalışmada aynı oranlarda yapılan damgalama sonucu elde edilen kalite oranları Çizelge 4.3.'de verilmiştir. Çizelge 4.3. incelendiğinde, bu çalışmada önerilen yöntem kullanılarak hem kendi seçtiğimiz frekanslarda hem de SHIEH ve ark. (2004) tarafından önerilen frekanslarda, aynı ağırlıklarla yapılan damgalamalar sonucunda daha

yüksek PSNR, yani daha kaliteli görüntüler elde edilmiştir. Bunun nedeni, SHIEH ve ark. (2004) tarafından önerilen yöntemde kullanılan ağırlık, taşıyıcı görüntünün damgalanacak her AC frekansına sabit olarak eklenmesi ya da çıkarılmasıdır. Ancak bizim çalışmamızda, damgalama algoritmasında kullanılan ağırlık, görüntünün AC frekanslarında yapılabilecek en büyük değişiklik miktarı olarak işlem görmektedir. Yani, damgalama için seçilen AC frekansların 0-λ arasında değişikliğe uğraması nedeniyle, sabit ağırlık ile yapılan çalışmalara göre taşıyıcı görüntü üzerindeki bozulma daha az, dolayısıyla kalite daha yüksek olmaktadır.

Çizelge 4.3. SHIEH ve ark. (2004) yaptıkları çalışmada elde ettikleri PSNR sonuçları ile bu çalışmada elde edilen PSNR sonuçlarının karşılaştırılması

	Seçilen AC Frekanslar	PSNR (dB) λ=10	PSNR (dB) λ=30
SHIEH ve ark.(2004)	6, 9, 11, 12	34,790	34,090
Kendi çalışmamız	6, 9, 11, 12	44,725	36,002
Kendi çalışmamız	16, 19, 24, 25	44,794	36,033

Genetik algoritma ile AC frekansları seçen SHIEH ve ark. (2004), saldırılara karşı dayanıklı ancak kaliteyi de düşürmeyen AC frekansları seçmeye çalışmışlardır. Buna göre, damgalama için seçilen AC frekans grubundan diğer AC frekanslara göre daha iyi kalitede bir sonuç vermesi beklenmektedir. λ=10 ve 30 ağırlıkla yaptıkları testlerde, yukarıdaki şartlara uygun frekansların bulunması için yaklaşık 400 dakikalık bir işlem yapılmaktadır.

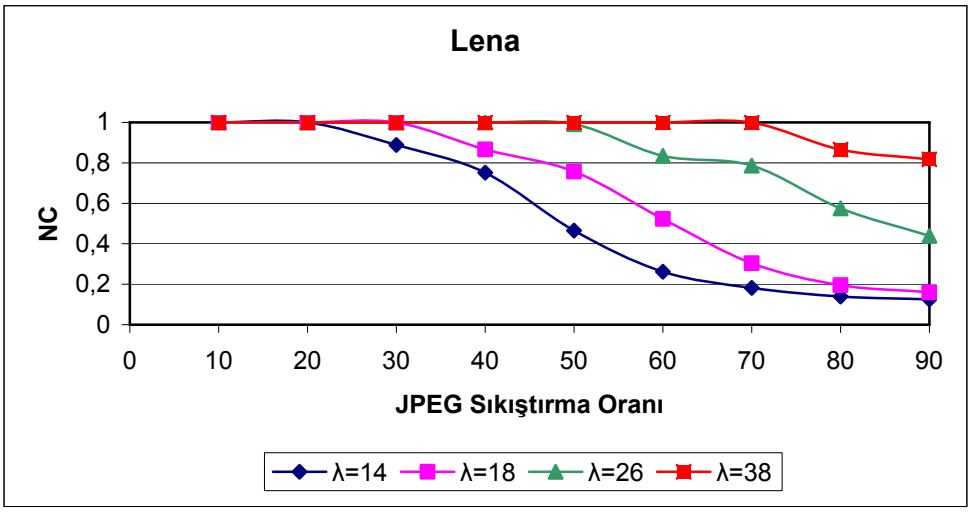
Orta frekans bandından seçilen çeşitli frekans kombinasyonları kullanılarak Lena görüntüsü λ=10 ve 30 ağrılıklarda damgalanmış ve kalite ölçümleri yapılmıştır (Çizelge 4.4.). PSNR ölçümleri incelendiğinde, damgalamalar sonucu ölçülen kalite değerleri ile SHIEH ve ark. (2004) tarafından genetik algoritma kullanılarak elde edilen kaliteler arasında gözle görülecek derecede bir fark oluşmadığı tespit edilmiştir. Ayrıca burada, ağırlığın artmasıyla birlikte aynı frekanslarda yapılan damgalamalarda kalitenin de aynı oranda düştüğü gözlenmiştir.

Çizelge 4.4. Orta frekans bandından rasgele seçilen AC frekanslar kullanılarak λ=10 ve 30 ağırlıklarla Lena görüntüsüne yapılan damgalama sonucu ölçülen PSNR sonuçları

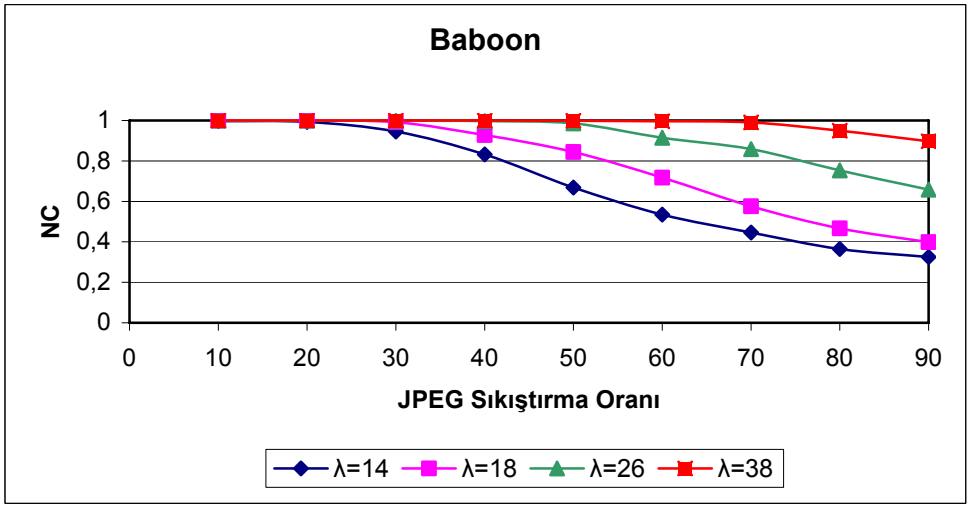
Orta frekans bandından rasgele seçilen AC frekanslar	PSNR (dB) λ=10	PSNR (dB) λ=30
16, 17, 18, 19	44,7917	36,0502
15, 17, 23, 34	44,7682	36,0946
18, 25, 32, 33	44,8109	36,1458
20, 23, 30, 32	44,8177	36,1377
16, 21, 24, 30	44,8184	36,1171
17, 30, 31, 34	44,8648	36,1567
15, 18, 21, 31	44,8056	36,1297
23, 27, 30, 32	44,8090	36,1365
22, 23, 24, 25	44,8281	36,1203
17, 26, 27, 32	44,7831	36,1308
15, 19, 22, 32	44,8354	36,1415
25, 26, 29, 30	44,8034	36,1413
22, 27, 30, 33	44,8368	36,1482
21, 31, 32, 33	44,8340	36,1382
18, 24, 31, 32	44,8252	36,1071
19, 16,26, 34	44,8115	36,1433
23, 25, 30, 31	44,8143	36,1449
17, 25, 29, 31	44,7987	36,1214
17, 19, 32, 34	44,8515	36,1622
27, 29, 30, 32	44,8143	36,1312

4.4.2. JPEG Kayıplı Sıkıştırması

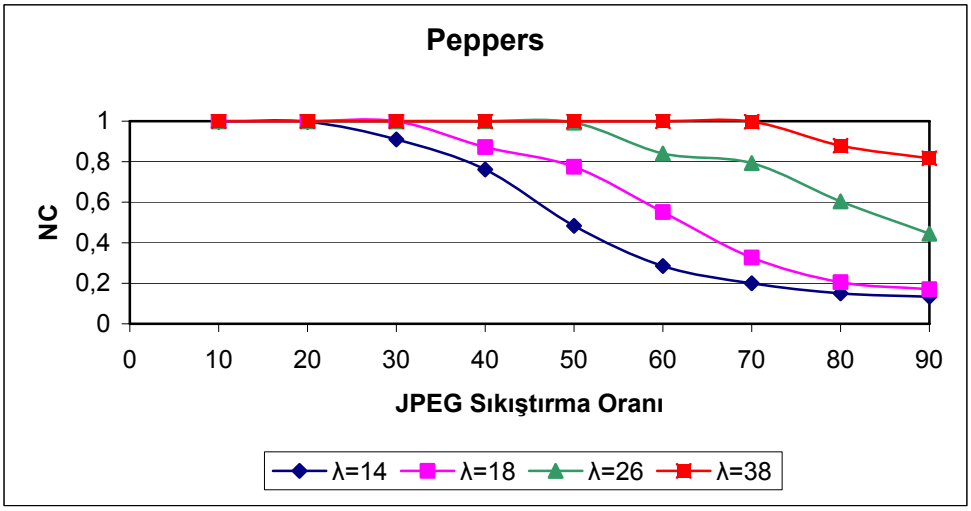
Taşıyıcı görüntüye damgalanan filigranın JPEG kayıplı sıkıştırmasına karşı dayanıklılığının sağlanması amacıyla damgalama işlemi DCT kullanılarak frekans düzleminde gerçekleştirilmiştir. JPEG algoritması ile basit olarak, blok tabanlı DCT ile frekans düzlemine taşınan görüntülerin istenen sıkıştırma oranında yüksek frekanslı AC bileşenlerinin silinmesiyle yapılır. Bu nedenle, filigranın uygulanacağı AC frekansların seçiminde Şekil 3.5.'de gösterilen orta frekans bandı kullanılmıştır. Farklı ağırlıklarda filigran damgalanan taşıyıcı görüntüler, ACDSee 6 yazılımı kullanılarak 9 farklı oranda (%10-…-%90) sıkıştırılmıştır. Ardından, geri elde etme algoritması ile JPEG kayıplı sıkıştırması uygulanan taşıyıcı görüntülerden filigranlar geri elde edilmiştir. Elde edilen filigranın aslına benzerlikleri NC ile ölçülmüş, sonuçlar her taşıyıcı görüntü için ayrı ayrı grafik olarak aşağıda verilmiştir.



Şekil 4.3. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Lena görüntülerine JPEG kayıplı sıkıştırması uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü



Şekil 4.4. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Baboon görüntülerine JPEG kayıplı sıkıştırması uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü



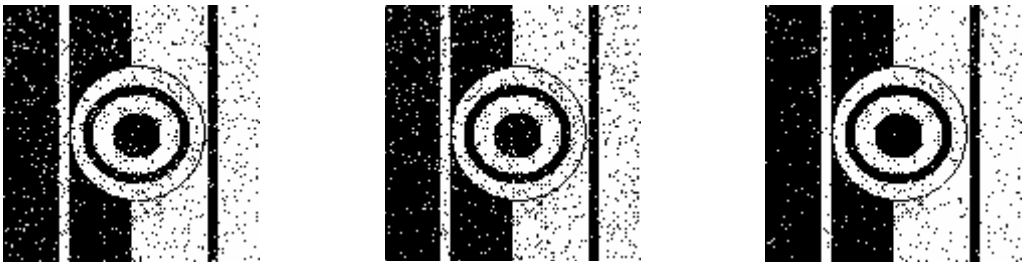
Şekil 4.5. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Peppers görüntülerine JPEG kayıplı sıkıştırması uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü

Şekil 4.3., Şekil 4.4. ve Şekil 4.5.'de görülen, λ=14, 18, 26 ve 38 ağırlıklarda filigran damgalanan taşıyıcı görüntülerden geri elde edilen filigranların benzerliği, JPEG kalitesiyle doğru orantılı olarak artmaktadır. Bununla birlikte, damgalama ağırlığının yüksek olması, düşük kalitedeki JPEG sıkıştırmalarına karşı taşıyıcı görüntüdeki filigranın dayanıklılığının artmasını sağlamıştır. Her 3 görüntüde de, 18 ağırlıkla damgalanan taşıyıcı görüntülerden elde edilen filigranlar, %40 sıkıştırma oranına kadar yaklaşık 0,9 benzerlikle geri elde edilmiştir. Aynı benzerlik oranı, λ=38 ağırlıkla damgalanan taşıyıcı görüntülerin %70 orana kadar yapılan sıkıştırılmasından sonra geri elde edilen filigranlarda ölçülmüştür.

Sonuç olarak, kullanılan ağırlığın artması ile birlikte görüntü içindeki filigranın JPEG kayıplı sıkıştırmasına karşı gösterdiği direnç de artmıştır. Şekil 4.6.'da çeşitli ağırlıklarla damgalanmış Baboon görüntülerinden geri elde edilen filigranlardan benzerlik ölçümü (NC) yaklaşık 0,9 olan filigranlar görülmektedir.

HSU ve WU (1999) önerdikleri yöntemle Lena görüntüsünü damgalamış ve JPEG kayıplı sıkıştırmasına karşı test yapmışlardır. %10,74 oranında sıkıştırılan damgalanmış görüntüden elde edilen filigranın benzerliği 0,413 olarak ölçülmüştür. Bu çalışmada önerilen yöntemle, en düşük test ağırlığı (λ=14) ile damgalanan Lena görüntüsü %10 oranında sıkıştırılmıştır. Bu görüntüden, NC=0,999 benzerlikle filigran

geri elde edilmiştir. Dolayısıyla JPEG sıkıştırmasına karşı daha yüksek direnç göstermiştir.



(a) λ=18, % 40 sıkıştırılmış (b) λ=26, % 60 sıkıştırılmış (c) λ=38, % 80 sıkıştırılmış

Şekil 4.6. Damgalanmış Baboon görüntüsünden JPEG kayıplı sıkıştırmasının ardından geri elde edilen filigranlar

Şekil 4.6.'daki logolar incelendiğinde JPEG sıkıştırmasının getirdiği bozulma, logo üzerine bir gürültü olarak yansımıştır. Logonun yapısında bulunan siyah ve beyaz bloklar, bu saldırısının getirdiği gürültüye karşı logonun tanınmasını kolaylaştırmıştır. Eğer taşıyıcı görüntülere damgalanan logonun yapısı ince çizgilerden ya da art arda tekrar eden bir yazının oluşturduğu görüntü olsaydı, saldırılar sonunda geri elde edilen logonun tanınması daha zor olacaktı. Dolayısıyla, damgalamada kullanılan logoyu oluşturan renklerin büyük bloklarda olması, saldırılar sonunda geri elde edildiğinde tanınma olasılığını da arttırmaktadır.

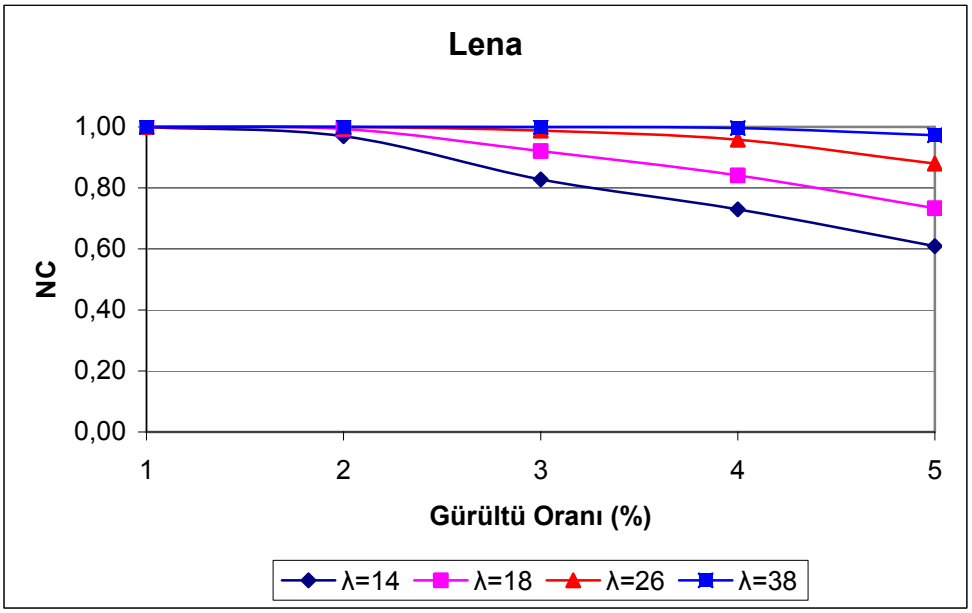
4.4.3. Gürültü Ekleme

Çeşitli amaçlarla gizli ve dayanıklı filigran damgalanan görüntülere yapılan saldırılardan biri de görüntünün kalitesinde önemli bir düşmeye sebep olmadan yapılan gürültü ekleme saldırısıdır. Bu saldırı, görüntünün tüm piksellerinin yoğunluğunun belli oranda değiştirilmesi ile gerçekleştirilir. Böylece, görüntü içindeki filigranın geri elde edilmesini sağlayacak bilginin yok olmasına sebep olacak değişiklikler yapılır.

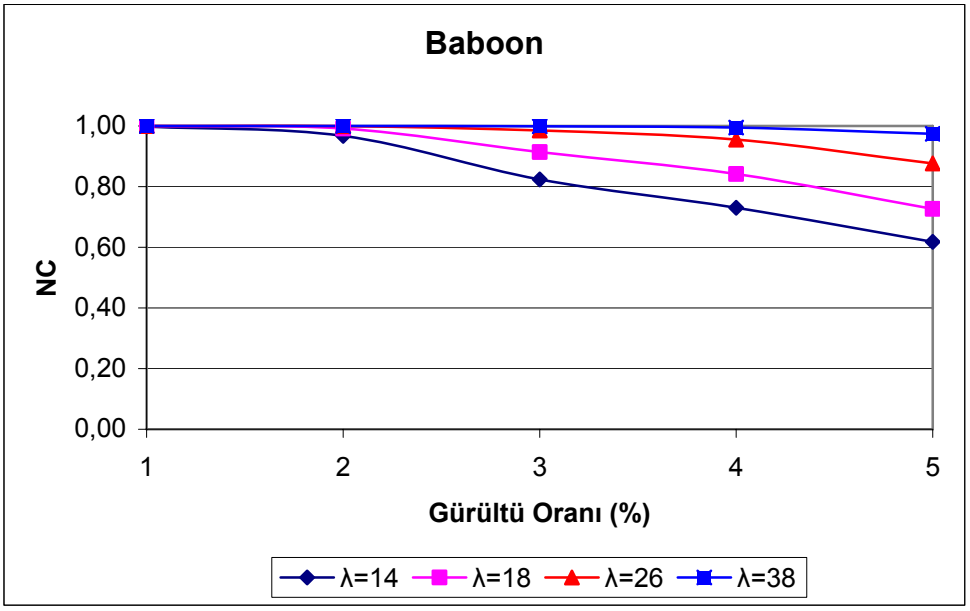
Bu tezde önerilen yöntem ile damgalanan taşıyıcı görüntülerin her pikseline, %1 ile %5 arasında değişen 5 farklı oranda rasgele gürültü eklenmiş ve ardından bu görüntülerdeki filigranlar geri elde edilmiştir. Elde edilen filigranların NC ile ölçülen benzerlikleri Çizelge 4.5.'de verilmiştir.

Çizelge 4.5. Çeşitli oranlarda gürültü eklenen taşıyıcı görüntülerden geri elde edilen filigranların benzerliklerinin ölçüm sonuçları

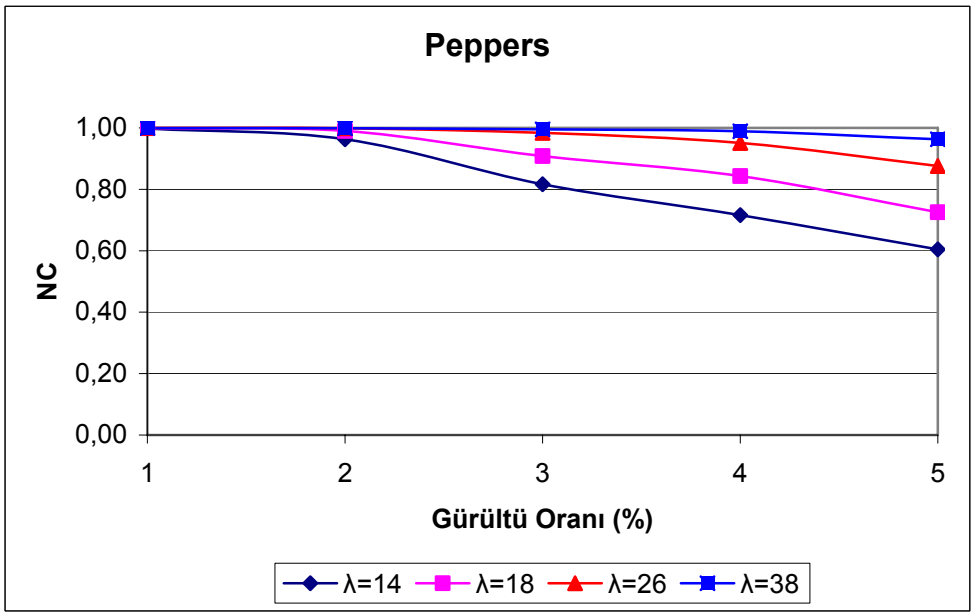
Gürültü Oranı (%)	Baboon				Lena				Peppers			
	λ=14	**λ=18**	**λ=26**	**λ=38**	**λ=14**	**λ=18**	**λ=26**	**λ=38**	**λ=14**	**λ=18**	**λ=26**	**λ=38**
1	0,997	0,999	1,000	1,000	0,999	0,999	1,000	1,000	0,997	0,998	1,000	0,999
2	0,967	0,991	0,999	1,000	0,969	0,993	0,999	1,000	0,962	0,989	0,998	0,998
3	0,823	0,914	0,985	0,998	0,828	0,920	0,988	0,999	0,816	0,908	0,983	0,995
4	0,730	0,841	0,955	0,994	0,729	0,841	0,957	0,996	0,715	0,843	0,950	0,988
5	0,617	0,726	0,876	0,973	0,609	0,733	0,879	0,972	0,604	0,725	0,875	0,963



Şekil 4.7. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Lena görüntülerine %1 ile %5 oranları arasında gürültü uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü



Şekil 4.8. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Baboon görüntülerine %1 ile %5 oranları arasında gürültü uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü



Şekil 4.9. λ=14, 18, 26 ve 38 ağırlıklarla filigran damgalanan Peppers görüntülerine %1 ile %5 oranları arasında gürültü uygulandıktan sonra geri elde edilen filigranların benzerlik ölçümü

Uygulanan gürültünün etkisi Şekil 4.10a'da λ=26 ağırlıkla damgalanan Lena görüntüsünden alınan kesit, Şekil 4.10b'de %5 oranında gürültü uygulanan aynı görüntüden alınan kesit ve Şekil 4.10c'de %5 oranında gürültü uygulanmış görüntüden geri elde edilen logo görülmektedir.

(a) (b) (c)

Şekil 4.10. a) λ=26 ağırlıkla damgalanmış Lena görüntüsünden alınan kesit, b) Aynı görüntüye %5 oranında gürültü uygulandıktan sonra alınan kesit, c) %5 oranında gürültü uygulanan Lena görüntüsünden geri elde edilen logo

Gürültü ekleme ile yapılan saldırılarda görüntü kalitesindeki bozulmanın en az seviyede tutulması ancak bunun yanında da görüntünün içine saklanan filigranın da geri elde edildiğinde tanınamayacak derecede bozulması amaçlanır. Şekil 4.10b'de görülen kesitte, %5 oranında gürültü uygulanan Lena görüntüsündeki bozulma, görüntü kalitesinde gözle görülür derecede değişikliğe neden olmasına karşın, bu görüntüden elde edilen logo (Şekil 4.10c) orijinaline tanınabilir derecede (NC=0,879) benzerlik göstermektedir. Bu da, uygulanan damgalama algoritmasının, görüntü kalitesinde önemli bir düşüş yaratan gürültü saldırılarına karşı dayanıklı bir damgalama gerçekleştirdiğini göstermektedir. JPEG kayıplı sıkıştırmasında oluğu gibi gürültü saldırısında da logonun tanınabilir olmasında renk bloklarının büyüklüğü önemli rol oynamıştır.

4.4.4. Kırpma İşlemi

Taşıyıcı görüntülerdeki filigrana yapılan saldırılardan bir diğeri kırpma işlemidir. Bu saldırıya karşı önerilen yöntemin test edilmesi amacıyla λ=14 ağırlıkla damgalanmış taşıyıcı görüntüler %10 ile %90 aralığında kırpılmış ve kırpılan bölüm düz beyaz renkle doldurulmuştur. Düz renk dolgusu herhangi bir bilgi saklayamayacağından buradan elde edilecek filigran siyah olarak çıkacaktır. Kırpılmış görüntülerden geri elde edilen filigranların benzerliği (NC) ile görüntünün kalan bölümü arasındaki ilişki Çizelge 4.6.'da verilmiştir. Çizelge incelendiğinde, kırpma saldırısına uğrayan taşıyıcı görüntülerden elde edilen filigranın benzerliği, görüntünün kalan bölümü ile yaklaşık doğru orantılı olarak azalmaktadır.

Çizelge 4.6. Damgalanmış taşıyıcı görüntülere uygulanan kırpma saldırısı sonucu kalan bölümün oranı ile kalan bölümden geri elde edilen filigranların benzerliklerinin (NC) ölçüm sonuçları

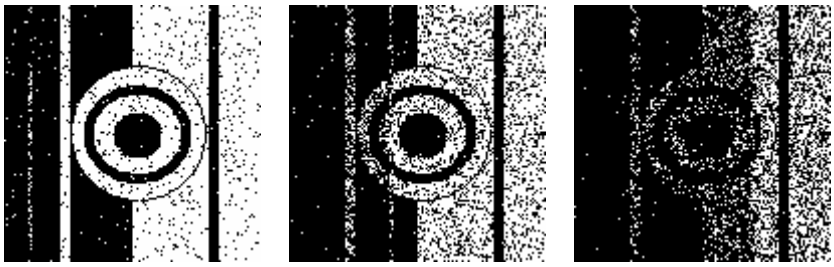
Kırpma sonunda kalan bölüm (%)	**Baboon λ=14**	**Lena λ=14**	**Peppers λ=14**
90	0,936	0,935	0,934
80	0,880	0,879	0,881
70	0,774	0,772	0,780
60	0,701	0,701	0,702
50	0,600	0,601	0,602
40	0,496	0,495	0,495
30	0,377	0,369	0,378
20	0,246	0,242	0,258
10	0,137	0,138	0,139

Kırpma saldırısı sonunda, görüntünün kalan bölümü ile ondan elde edilen filigranın benzerliği arasındaki doğru orantının daha iyi tespit edilmesi amacıyla bu değerler arasında regresyon analizi yapılmıştır (Çizelge 4.7.). Regresyon sonucunun 1'e yakın olması bu değerlerin doğrusallığını göstermektedir.

Çizelge 4.7. Kırpma saldırısı sonunda elde edilen filigranların benzerliği (NC) ile taşıyıcı görüntünün kalan bölümü arasında yapılan regresyon analizi sonuçları

Regresyon Analizi		
Baboon λ=14	**Lena λ=14**	**Peppers λ=14**
0,996	0,996	0,996

Saldırı sonucu kırpılan bölümde yer alan filigran tamamen kaybedilmektedir. Kaybedilen filigran bilgisi uygulanan permutasyondan dolayı filigran üzerine gürültü olarak yansımaktadır. Damgalanan filigranın seçiminde ya da oluşturulmasında kullanılan renk bloklarının büyüklüğü nedeniyle, yüksek kesme oranlarında bile tanınabilirlik sağlanmıştır (Şekil 4.11.).



(a) (b) (c)

Şekil 4.11. λ=26 ağırlıkla damgalanan Lena görüntüsüne çeşitli oranlarda yapılan kesme saldırıları sonunda geri elde edilen filigranlar, a) %10, b) %40, c) %70

Damgalama öncesinde filigrana uygulanan permutasyonun etkisinin görülmesi amacıyla Şekil 4.12a.'da λ=10 ağırlıkla damgalanmış 512×512 boyutlarındaki Lena görüntüsü dıştan 80 piksel kalınlığında kırpılarak yerine siyah renk ile dolgu yapılmıştır. Kırpılan görüntü ile bu görüntüden geri elde edilen filigran Şekil 4.12b.'de yer almaktadır. Damgalama işlemi öncesinde filigrana uygulanan permutasyon sonucu, taşıyıcı görüntünün kırpılan bölümünden tamamen kaybedilen bilgi, filigranın genelinde bir gürültü oluşturmuştur. Böylece filigranın bir bölümü tamamen kaybedilmemiş ve tanınmasında kolaylık sağlanmıştır.

Aynı görüntüye permutasyon uygulanmadan λ=10 ağırlıkla filigran damgalanmıştır. Ardından yukarıdaki gibi bir kırpma saldırısına uğratılmış ve filigran geri elde edilmiştir (Şekil 4.13). Görüntünün geriye kalan bölümü ile bu bölümden elde edilen filigran Şekil 4.14b'de görülmektedir. Geri elde edilen filigranın, taşıyıcı görüntünün kırpılan bölümüne damgalanan kısmı permutasyon uygulanmadığından tamamen kaybedilmiştir.

(a) (b)

Şekil 4.12. a) Çevresinden 80 piksel genişliğinde alan kırpılıp beyaz renk ile doldurulmuş, λ=10 ağırlıkla permutasyon uygulanıp filigran damgalanan Lena görüntüsü, b) Görüntünün kalan bölümünden geri elde edilen filigran

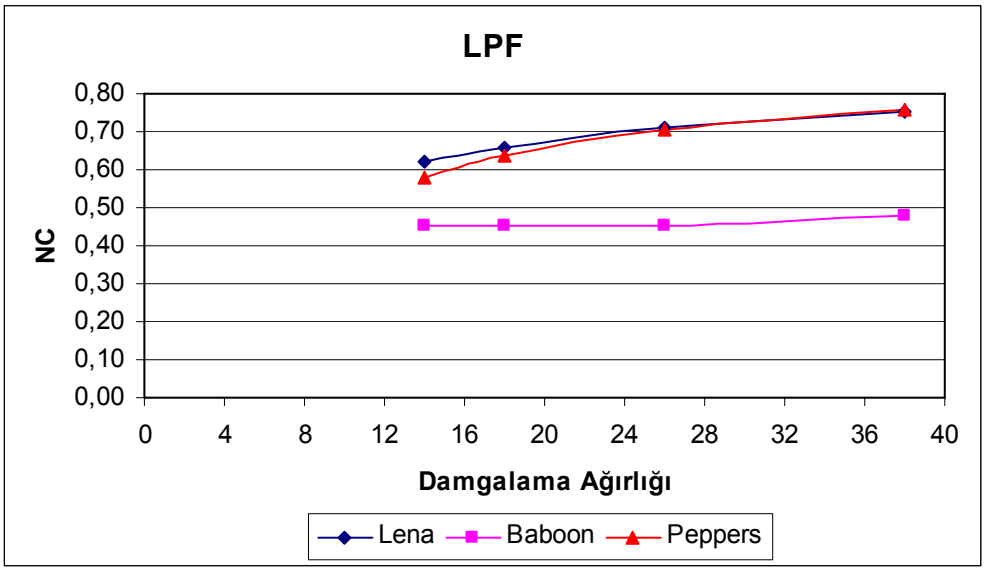
(a) (b)

Şekil 4.13. a) Permutasyon uygulanmadan λ=10 ağırlıkla damgalanan, çevresinden 80 piksel genişliğinde alan kırpılıp beyaz renk ile doldurulmuş Lena görüntüsü, b) Kesilen görüntüsünün kalan bölümünden geri elde edilen filigran

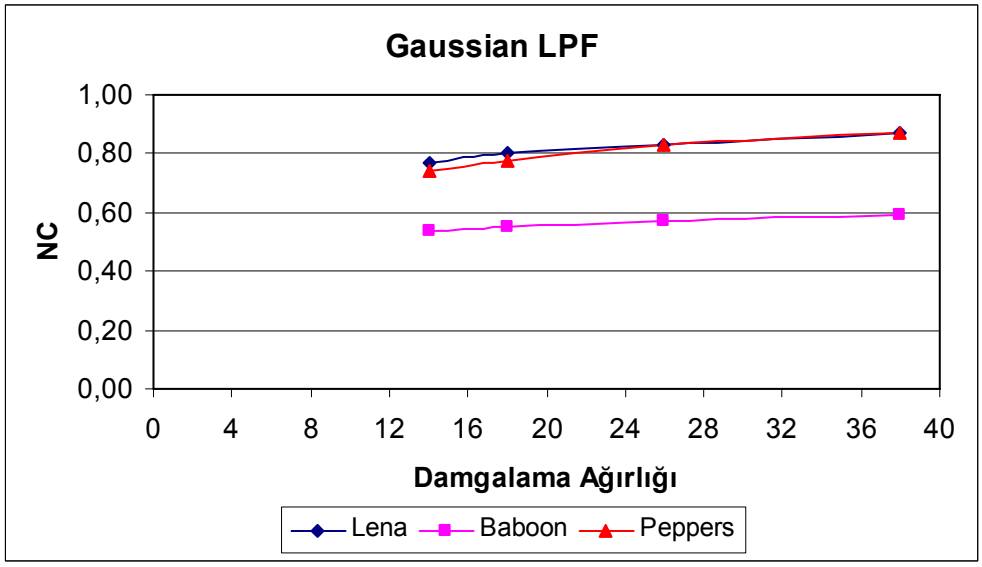
4.4.5. Filtreleme

Test için seçilen ağırlıklarda, λ=14, 18, 26, 38, filigran damgalanan görüntülere alçak geçiren filtre (LPF-Low Pass Filter), Gaussian LPF, yüksek geçiren filtre (HPF-High Pass Filter) ve Median filtrelemeleri ile saldırılar yapılmıştır. Saldırıların ardından görüntülerin geri elde edilen filigranların aslına benzerlikleri her filtreleme saldırısı için ayrı ayrı ölçülmüştür.

LPF (Şekil 4.14.) ve Gaussian LPF (Şekil 4.15) saldırısının ardından Lena, Baboon ve Peppers görüntülerinden elde edilen filigranların benzerlikleri yer almaktadır. LPF saldırısı sonucu, damgalama ağırlığının benzerliğin artmasında çok etkili olmadığı tespit edilmiştir. Düz alanların yoğun olarak bulunduğu Lena ve Peppers görüntülerinde, damgalama ağırlığına bağlı olarak filigran benzerliğinde artış görülmüştür. Ancak düz alanın neredeyse bulunmadığı Baboon görüntüsünde damgalama ağırlığı görüntüden elde edilen filigranın benzerliğini etkilememiştir.

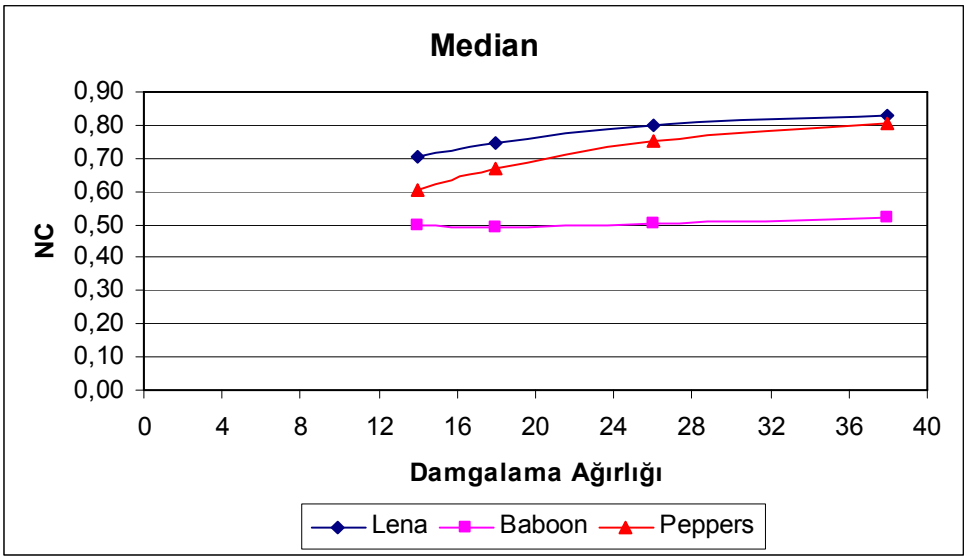


Şekil 4.14. Alçak frekans filtrelemesi (LPF) uygulanan test görüntülerinden elde edilen filigranların damgalama ağırlığına göre benzerlik ölçümü



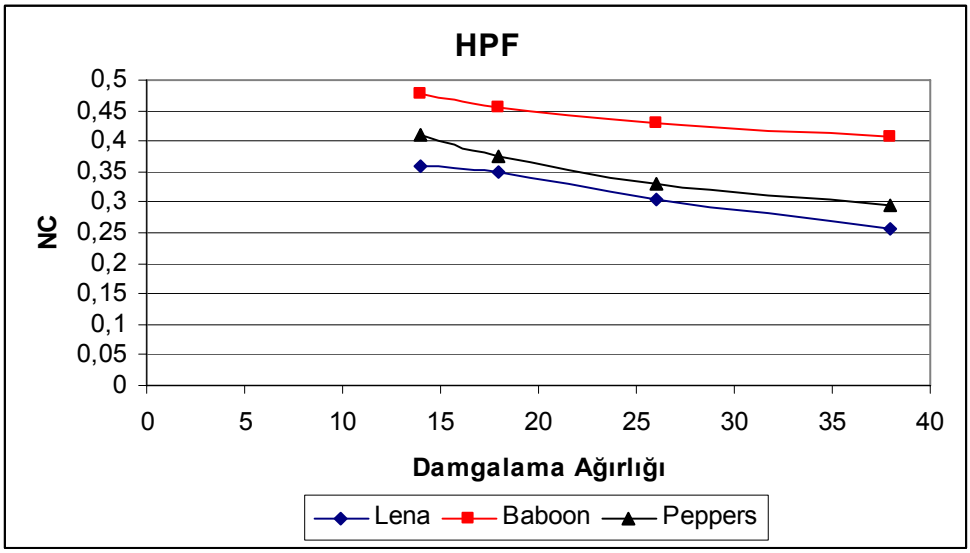
Şekil 4.15. Gaussian LPF uygulanan test görüntülerinden elde edilen filigranların damgalama ağırlığına göre benzerlik ölçümü

Taşıyıcı görüntülere yapılan saldırılardan Median filtrelemesi sonucu elde edilen filigranların benzerliği, LPF ve Gaussian LPF saldırıları ile aynı karakteristiği göstermiştir (Şekil 4.16.).



Şekil 4.16. Median filtresi uygulanan test görüntülerinden elde edilen filigranların damgalama ağırlığına göre benzerlik ölçümü

Yüksek damgalama ağırlığının kullanılması, taşıyıcı görüntülerin AC frekans bileşenleri üzerindeki değişimi de arttırmıştır. Buna bağlı olarak HPF uygulanan görüntülerde bu değişim daha da artarak gözle görülür derecede bozulmalara sebep olmuştur. Özellikle Lena ve Peppers görüntülerinde yüksek damgalama ağırlığının meydana getirdiği değişimin belirgin olması, HPF saldırısından bu görüntülerin daha fazla etkilenmesine neden olmuştur. Dolayısıyla, damgalama ağırlığının yüksek olduğu görüntülerdeki bu bozulma, geri elde edilen filigranın benzerliğini zıt yönde etkilemiş, HPF saldırısına uğrayan taşıyıcı görüntülerden elde edilen filigranların benzerliği, diğer saldırılardan elde edilen sonuçların aksine damgalama ağırlığına ters oranda ölçülmüştür. Damgalama ağırlığının artmasına karşın filigranın benzerliğinde azalma görülmüştür. Düz alanların yoğun olarak bulunduğu Lena ve Peppers görüntülerindeki filigranlar, Baboon görüntüsündeki filigrana göre HPF saldırısına karşı daha az dayanıklılık göstermiştir (Şekil 4.17.).



Şekil 4.17. HPF filtresi uygulanan test görüntülerinden elde edilen filigranların damgalama ağırlığına göre benzerlik ölçümü

4.4.6. Döndürme

Frekans düzleminde damgalanan görüntülerdeki filigranın yok edilmesinde başarılı olan döndürme saldırısı Lena görüntüsüne uygulanmıştır. Bu saldırı sonucu, Lena görüntüsüne damgalanan filigran tamamen kaybedilmiştir. Şekil 4.18.'de λ=14 ağırlıkla damgalanan ve 1^0 saat yönünde döndürülen Lena görüntüsü ile bu görüntüden elde edilen filigran yer almaktadır.

(a) (b)

Şekil 4.18. a) λ=14 ağırlıkla damgalanan ve 1^0 saat yönünde döndürülen Lena görüntüsü, b) Geri elde edilen filigran

4.4.7. Karalama

Taşıyıcı Lena görüntüsüne çeşitli oranlarda, 8 piksel kalınlığındaki bir çizgi ile karalama yapılmıştır. Karalanan görüntüler ve onlardan elde edilen filigranlar aşağıdaki şekillerde gösterilmiştir (Şekil 4.19.).

(a)

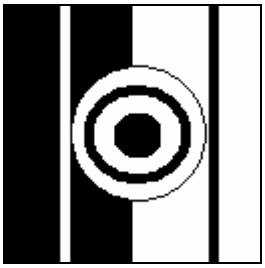
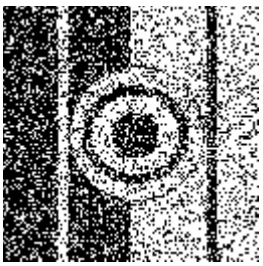
(b)

(c)

Şekil 4.19. Çeşitli oranlarda yapılan karalanan Lena görüntüsü ve elde edilen filigranlar, a) NC=0,849, b) NC=0,736, c) NC=0,624

4.4.8. Tekrar Damgalama

Damgalanmış görüntülerin tekrar damgalanması, ilk damgalamadaki bilginin yok olmasına neden olabilir. Bu tür bir saldırının ilk damgalanan filigrana etkisini tespit etmek amacıyla, λ=14 ağırlıkla damgalanmış Lena görüntüsü aynı ağırlıkla fakat farklı anahtar sayı ile permutasyon uygulanarak tekrar damgalanmıştır (Şekil 4.20.).

Damgalama Frekansları	Geri Elde Edilen Filigran	Benzerlik (NC)
15, 18, 26, 33 (Tamamen farklı frekanslar)		1
15, 18, 19, 25		0,789
16, 19, 24, 25 (Tamamen aynı frekanslar)		0,639
(a)	(b)	(c)

Şekil 4.20. a) Tekrar damgalama için seçilen frekanslar, b) Geri elde edilen ilk damgalanan filigranlar, c) Benzerlik (NC)

Tekrar yapılan damgalama işleminde, seçilen frekans bileşenleri ilk yapılan damgalamada kullanılanlardan tamamen farklı olduğunda, ilk filigranda bozulma olmamıştır. Tamamen ya da bir miktar aynı frekans kullanılarak yapılan tekrar damgalama işlemleri sonucunda ilk damgalanan filigranda veri kaybı olmuştur. Bunun sebebi olarak, ikinci damgalama işleminin ilk damgalamada kullanılan frekans bileşenleri üzerinde yaptığı değişim ile açıklanabilir.

4.4.9. Kontrast Artırma

Damgalanmış görüntülerin kontrastının değiştirilmesi ile yapılacak saldırı, görüntülere damgalanan filigranın yok olmasına neden olabilir. Bu saldırıya karşı filigranın dayanıklılığını test etmek amacıyla, damgalanmış görüntüler Adobe Photoshop^{TM} CS2 yazılımı ile kontrastı 10 arttırılmış ve saldırıya uğrayan görüntülerden filigran geri elde edilmiştir. Elde edilen filigranların benzerliği NC ile ölçülmüştür (Çizelge 4.8.). Ölçümler sonunda filigranlar +10 kontrasta karşı başarılı dayanıklılık göstermiştir. Saldırıların çoğunda olduğu gibi, damgalama ağırlığının artması filigranın kontrast saldırısına karşı gösterdiği direnci de arttırmıştır.

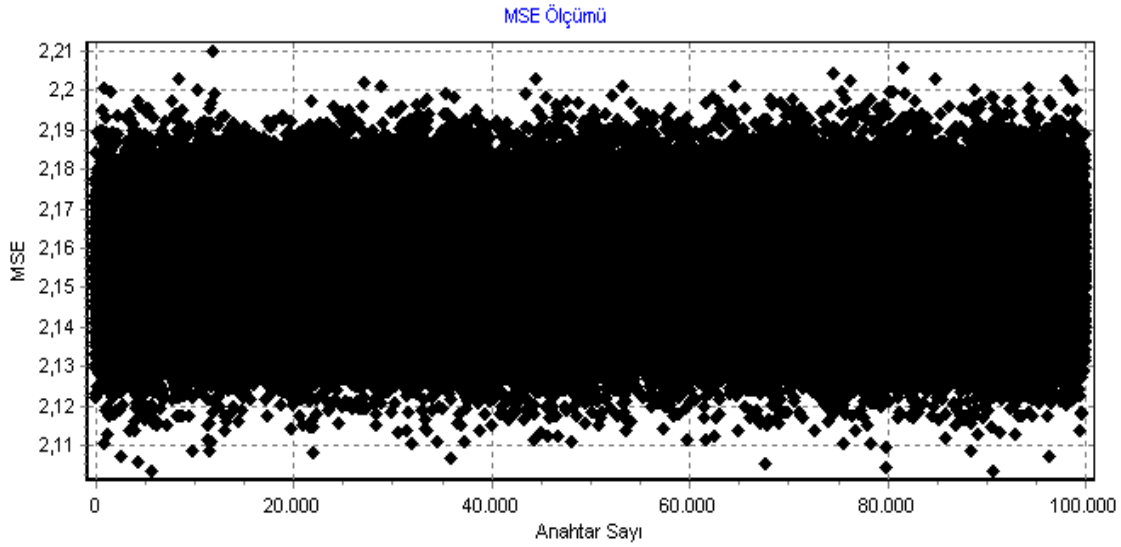
Çizelge 4.8. Kontrastı 10 arttırılan taşıyıcı görüntülerden geri elde edilen filigranların bezerlik ölçümü (NC)

Damgalama Ağırlığı	Lena	Peppers	Baboon
14	0,894	0,884	0,671
18	0,921	0,899	0,733
26	0,956	0,917	0,845
38	0,978	0,934	0,929

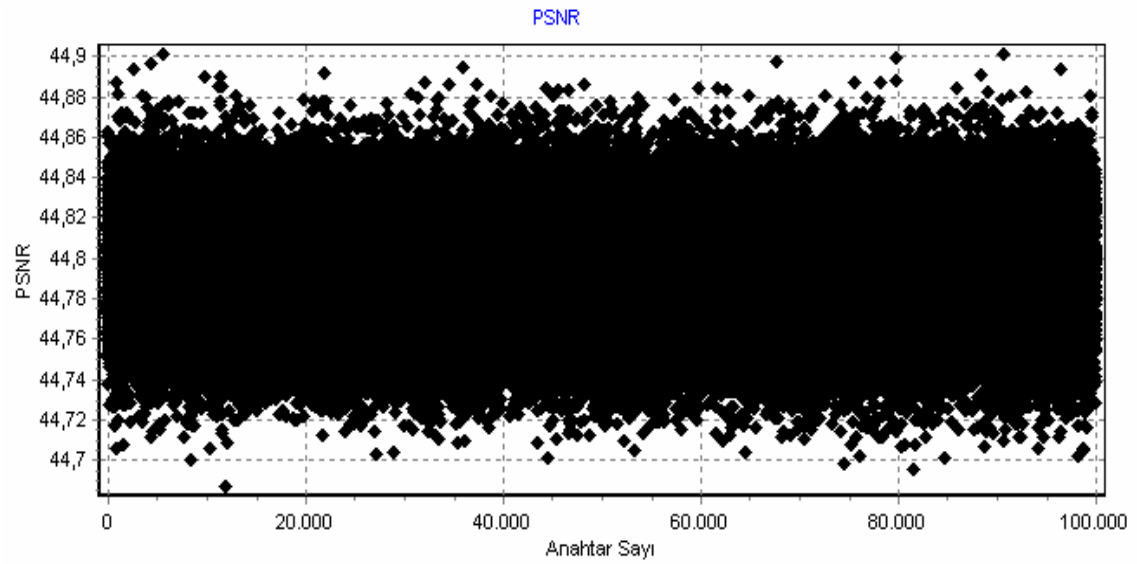
4.4.10. Anahtar Sayısının Damgalama Üzerindeki Etkisi

Bu çalışma ile geliştirilen damgalama algoritmasında damgalama ağırlığı, görüntünün frekanslarında yapılacak değişikliğin en büyük miktarı olarak işlem görmektedir. Ayrıca, bir anahtar sayı ile yapılan permutasyon sonucu, filigranın pikselleri kendi içinde dağıtılmaktadır. Bu dağıtma sonucu, permutasyonda kullanılan sayının görüntünün AC bileşenlerinin değiştirilmesinde bir etkisinin olabileceği ve her taşıyıcı görüntüye göre seçilecek belli bir anahtarın bozulmayı minimuma indirebileceği düşünülmüştür. Bu amaçla, kullanılan anahtar sayı ile damgalama sonucu oluşan bozulma arasındaki ilişkinin belirlenmesi için 1 ile 100.000 arasındaki tüm sayılar kullanılarak filigrana permutasyon uygulanmış ve λ=10 ağırlıkla Lena görüntüsü damgalanmıştır. Elde edilen sonuçlardaki değişim çok küçük bir oranda olduğundan, filigranın permutasyonunda kullanılan anahtar sayının, damgalama sonrasında görüntüde oluşan bozulma ve görüntü kalitesi üzerinde gözle görülür bir etkisi tespit

edilememiştir. Görüntü kalitesindeki bozulma Şekil 4.21.'de gösterilmiştir. Bu değerler arasında anahtar sayı olarak 5611 en düşük hata değerini verirken (MSE= 2,103565216) 11899 anahtar sayısı en yüksek hata değerini (MSE= 2,209945679) vermiştir. Ancak en yüksek hata ile en düşük arasındaki fark kalite üzerinde gözle görülebilecek derecede bir değişime yol açmamıştır. En düşük hata değerindeki kalite PSNR= 44,90124 ile en yüksek değerini alırken, en yüksek hata değerindeki kalite PSNR= 44,68698 olarak ölçülmüştür (Şekil 4.22.).



Şekil 4.21. 1–100.000 arasındaki anahtar sayılar kullanılarak Lena görüntüsüne λ=10 ağırlıkla yapılan damgalamalar sonucu taşıyıcı görüntüde oluşan bozulmanın (MSE) ölçümü



Şekil 4.22. 1–100.000 arasındaki anahtar sayılar ile Lena görüntüsüne λ=10 ağırlıkla yapılan damgalamalar sonucunda görüntüdeki kalitenin (PSNR) ölçümü

4.4.11. Damgalanan Görüntülerde DC ile Uzay Düzlemi Enerjisinin ve Frekans Düzlemi Enerjisinin Karşılaştırılması

Damgalama işlemi için referans olarak uzay düzlemi enerjisi seçilmiştir. Bunun nedeni, kaliteye yönelik yapılan saldırılarda DC ile uzay düzlemi enerjisi arasındaki değişimin frekans düzleminden elde edilen enerjiye göre çok daha az olmasıdır.

Çeşitli ağırlıklarla damgalanan görüntülere aynı saldırılar yapılmış ve elde edilen görüntülerdeki DC-Uzay Düzlemi Enerjisi ve DC-Frekans Düzlemi Enerjisi karşılaştırmaları aşağıdaki çizelgelerde gösterilmiştir. Çizelgeler incelendiğinde, referans olarak seçilen uzay düzlemi enerjisinin ile DC arasındaki fark, frekans düzlemi enerjisine göre çok daha az olduğu görülmektedir. Dolayısıyla, referans noktasının tayininde uzay düzlemi enerjisinin kullanılması daha uygun olmuştur.

Çizelge 4.9. Damgalanan görüntülerde, DC ile uzay düzleminden elde edilen enerji arasındaki farkın, kaliteye yönelik saldırılar sonundaki değişimi

TESTLER	ORTALAMA DEĞİŞİM (DC-Uzay Enerjisi)		
	Lena	Baboon	Peppers
Gaussian LPF	1,011	1,277	1,104
LPF	0,894	1,154	1,034
HPF	21,850	18,594	19,306
MEDIAN	1,335	2,247	1,582
JPEG	2,650	6,265	3,079

Çizelge 4.10. Damgalanan görüntülerde, DC ile frekans düzleminden elde edilen enerji arasındaki farkın, kaliteye yönelik saldırılar sonundaki değişimi

TESTLER	ORTALAMA DEĞİŞİM (DC-Frekans Enerjisi)		
	Lena	Baboon	Peppers
Gaussian LPF	6,8525	6,0122	6,3852
LPF	5,0261	5,0541	4,8986
HPF	102,0562	54,9614	74,6547
MEDIAN	9,8227	14,6045	10,2241
JPEG	35,6337	35,5421	34,3170

5. SONUÇ VE ÖNERİLER

Bu çalışmada, sayısal görüntülerde telif haklarının korunması amacıyla yapılan filigran damgalama için bir yöntem önerilmiştir. Önerilen yöntemde taşıyıcı görüntülere görünmez ve dayanıklı filigran damgalanmasıdır. Geri elde etme algoritmasında damgalanan görüntünün ya da filigranın aslı kullanılmadığından kör damgalama yapılmıştır.

Dayanıklı ve görünmez damgalama yöntemlerinin amacı, taşıyıcı görüntüye damgalanan filigranın çeşitli saldırılara karşı direncini arttırmaktır. Bu amaç çerçevesinde geliştirilen yöntem ile filigranın dayanıklılığı JPEG kayıplı sıkıştırması, gürültü ekleme, kesme, filtreleme ve döndürme saldırıları karşısında test edilmiştir. Yapılan saldırılarda görüntünün kalitesinde gözle görülür bir düşüşe neden olmamıştır.

Taşıyıcı görüntülerin damgalanmasında kullanılan ağırlık, görüntü kalitesi ile saldırılara karşı filigranın dayanıklılığının sağlanmasında önemli rol oynamıştır. Damgalama ağırlığının artmasıyla birlikte görüntüdeki bozulmanın da arttığı tespit edilmiştir. Bununla birlikte yapılan testlerde, yüksek ağırlıklar ile damgalanan taşıyıcı görüntülerdeki filigranlar, saldırılara karşı daha fazla direnç göstermiş, daha yüksek benzerlik oranlarında geri elde edilmiştir.

Taşıyıcı görüntülere damgalanan filigrana, damgalama öncesinde bir anahtar sayı kullanılarak permutasyon uygulanmıştır. Permutasyon ile filigran pikselleri kendi içinde dağıtılmış ve böylece taşıyıcı görüntünün her yerine homojen bir şekilde dağılımı amaçlanmıştır. Kesme saldırısı ardından geri elde edilen filigranlarda, görüntünün kesilen bölümünde yer alan filigran bilgisi kaybedilmiş, ancak, kaybedilen bu bilgi filigrana bir gürültü olarak yansımıştır. Kesilen bölümün büyüklüğü ile doğru orantılı olarak filigranda oluşan gürültü de artmıştır.

Seçilen filigranı oluşturan renk bloklarının büyüklüğü, saldırılar sonunda filigranın tanınabilir olmasında rol oynayan önemli etkenlerden biridir. Bu çalışmada olduğu gibi, büyük renk bloklarından oluşan filigran, saldırılar sonunda geri elde edildiğinde daha iyi tanınabilmekte ve gürültünün etkisi daha az olmaktadır.

Literatürde yer alan birçok çalışmada kullanılan damgalama ağırlığı, görüntünün değiştirilecek pikselinde ya da frekans bileşeninde sabit bir değişikliğe yol açmaktadır. Ancak, bu çalışmada önerilen yöntemde ise, ağırlık, yapılabilecek en büyük değişiklik

sınırı olmakta, görüntüdeki değişiklikler 0 ile kullanılan ağırlık arasında pozitif ya da negatif yönde olmaktadır. Böylece önceki çalışmalara bağlı olarak görüntü kalitesi daha yüksek oranda korunmaktadır.

Sonuç olarak, geliştirilen damgalama algoritması ile görünmez ve dayanıklı olarak taşıyıcı görüntülere filigran damgalanmıştır. Filigranın kesme, JPEG kayıplı sıkıştırması, gürültü ekleme, filtreleme, karalama ve döndürme saldırılarına karşı dayanıklılığı test edilmiştir. HPF saldırısında geri elde edilen filigranın benzerliği önemli oranda azalmıştır. Döndürme sonucu filigran kaybedilirken diğer saldırılarda sonuçlar başarılı olmuştur. Döndürme ve HPF için, damgalama ağırlığı ve frekans bileşenleri seçimi dışında başka bir değişken kullanılarak bu saldırıların filigran üzerindeki etkinliği azaltılabilir.

KAYNAKLAR

ANONYMOUS, 2005. Image Steganography and Steganalisys. http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf

ARNOLD, M., SCHMUCKER, M. and WOLTHUSEN, S. D., 2003. **Techniques and Applications of Digital Watermarking and Content Protection,** Artech House, 273, London.

BARNI, M. and BARTOLONI, F., 2004. **Watermark System Engineering: Enabling Digital Assets Security and Other Applications**, Marcel Dekker, 485 s, United States of America.

CHEN, P.C., 1999. **On the Study of watermarking Application in WWW – Modeling, Performance Analysis and Application of Digital Image Watermarking Systems.** Master Thesis, National Tsing Hua University, 127 s, Hesinchu, Taiwan.

EGGERS, J. J., BAUML, R., TZSCHOPPE, R. and HUBBER, J., 2001 **Applications of Information Hiding and Digital Watermarking.** ECDL WS Generalized Documents (Publication)

HARTUNG, F. and KUTTER, M., 1999. **Multimedia Watermarking Techniques. Proceedings of IEEE,** 1079-1107.

FOTOPOULOS, V., KAVATHAS, P. and SKODRAS, A. N., 2000. Bit Signature Casting in the DCT Domain, Technical Report, Computer Technology Institute.

GÜNSEL, B., ULUDAĞ, U. and TEKALP, A. M., 2002. **Robust Watermark of Fingerprint Images,** The Journal of Pattern Recognition Society, 35, 2739-2747.

HSU, C. T. and WU, J.W., 1999. **Hidden Digital Watermarks in Images,** IEEE Transaction on Image Processing, 8 (1): 58-68.

JAIN, A. K. and ULUDAĞ, U., Hiding Fingerprint Minutiae in Images, **Proceedings AutoID 2002 3. Workshop on Authomatic Identification Advanced Technologies,** 2002, 97-102, New York, USA.

JOHNSON, N. F. and JAJODA, S., 1998, Exploring Steganography: Seeing the Unseen. **IEEE Computing Practices,** 2: 26-34.

KATZENBIESSER, S. and PETITCOLAS, F., 2000. **Information Hiding Techniques for Steganography and Digital Watermarking.** Artech House, 237, London.

KUTTER, M. and PETITCOLAS, F. A. P., 1999. **A Fair Benchmark for Image Watermarking Systems,** Electronic Imaging'99 Security and Watermarking of Multimedia Contents, 3657: 25-27.

KUTTER, M., JORDAN, F. and BOSSEN, F., 1997. Digital Signature of Color Images Using Amplitude Modulation, **Proceedings of SPIEEI97**, 518-526, Litvia.

MINTZER, F., BRAUDAWAY, G. W. and YEUNG, M. M., Effective and Ineffective Digital Watermarks, **IEEE INTERNATIONAL Conference on Image Processing, ICIP-97,** 1997, 9-12, Washington.

MOHANTY, S. P., Digital Watermarking: A Tutorial Review, Technical Report, Department of Electrical Engineering, Indian Instute of Science, Bangalore, India, 1999 (Unpublished).

MOHANTY, S. P., RAMAKRISHNAN, K. R. and KANKANHALLI, M., 1999. A Dual Watermarking Technique for Images, **Proceedings of 7th ACM International Multimedia Conference, ACMM-MM'99,** 49-51, Orlando, USA.

PETITCOLAS, A. P., ANDERSON, R. J. and KUHN, M. G., Attacks on Copyright Marking Systems, **Second International Workshop, IH'98,** 1998, 219-239, Oregon, USA.

SHIEH, C. S., HUANG, H. C., WANG, F. H. and PAN, J. S., 2004. **Genetic Watermarking Based on Transform Domain Techniques,** The Journal of the Pattern Recognition, 37 (2004): 555-565.

SHIH, F. Y. and WU, S. Y. T., 2003. **Combinational Image Watermarking in the Spatial Domain and Frequency Domains,** The Journal of Pattern Recognition, 36 (2003): 969-975.

TOPLASAN, M., 2004. **Sayısal İmza ve Şifreleme.** Lisans Tezi (Basılmamış), Mustafa Kemal Üniversitesi, 68, Hatay.

ULUDAĞ, U., GUNSEL, B. and TEKALP, A.M., 2001. Robust Watermarking of Busy Images, **Proceedings of SPIE Electronic Imaging 2001 Conference, Security and Watermarking of Multimedia Contents III**, 18-25, California, USA.

WANG, Z., BOVIK, A. C., SHEIK, H. R. and SIMONCELLI, E. P., 2004. **Image Quality Assesment: From Error Visibility to Structural Similarity**, IEEE Transaction on Image Processing, 13(4): 600-612.

ZHAO, J. and ECKHARD, K. Embedding Robust Labels into Images for Copyright Protection. **Proceeding of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies**, August 1995: 1-10, Vienna.

ÖZGEÇMİŞ

1977 yılında Kilis'te doğdum. İlk, orta ve lise öğrenimimi Bursa'da tamamladım. 1996 yılında Gaziantep Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nü kazandım. 2002 yılında mezun olduktan sonra aynı yıl Mustafa Kemal Üniversitesi'nde araştırma görevlisi olarak göreve başladım. 2003 yılında Mustafa Kemal Üniversitesi Fen Bilimleri Enstitüsü Elektrik Elektronik Anabilim dalında yüksek lisansa başladım. Halen Mustafa Kemal Üniversitesi Mühendislik Mimarlık Fakültesinde Araştırma görevlisi olarak görev yapmaktayım.