ESNEK RESİM DAMGALAMA: BLOK TABANLI DAMGALAMA ANALİZİ, VEKTÖR DAMGASI KULLANIMI VE DOĞRULAMA DAMGALAMASININ GELİŞTİRİLMESİ

RESILIENT IMAGE WATERMARKING: BLOCK-BASED IMAGE WATERMARKING ANALYSIS, USING VECTOR IMAGE AS WATERMARK AND IMPROVING AUTHENTICATION PURPOSE WATERMARKING

AHMET ŞENOL

PROF. DR. HAYRİ SEVER
Tez Danışmanı

Hacettepe Üniversitesi
Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliğinin
Bilgisayar Anabilim Dalı için Öngördüğü
DOKTORA TEZİ olarak hazırlanmıştır

2018

Ahmet ŞENOL'un hazırladığı "Esnek Resim Damgalama: Blok Tabanlı Damgalama Analizi, Vektör Damgası Kullanımı Ve Doğrulama Damgalamasının Geliştirilmesi" adlı bu çalışma jüri tarafından BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI'nda DOKTORA TEZİ olarak kabul edilmiştir.

(Prof.Dr.Erkay SAVAŞ)
Başkan .....

(Prof.Dr. Hayri Sever)
Danışman .....

(Yrd.Doç.Dr.Murat AYDOS)
Üye .....

(Doç.Dr.Ahmet Burak CAN)
Üye .....

(Doç.Dr. Reza ZARE HASSANPOUR)
Üye .....

Bu tez Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tarafından DOKTORA TEZİ olarak onaylanmıştır.

Prof.Dr. Menemşe GÜMÜŞDERELİOĞLU
Fen Bilimleri Enstitüsü Müdürü

YAYINLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

☐ **Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.**
(Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etseniz ve kütüphane bu talebinizi yerine getirse bile, tezinin arama motorlarının önbelleklerinde kalmaya devam edebilecektir.)

☑ **Tezimin/Raporumun 16.01.2019 tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.**
(Bu sürenin sonunda uzatma için başvuruda bulunmadığım taktirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı ve ya tamamının fotokopisi alınabilir)

☐ **Tezimin/Raporumun ..... tarihine kadar erişime açılmasını istemiyorum, ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.**

☐ **Serbest Seçenek/Yazarın Seçimi**

16 / 01 / 2018

Ahmet ŞENOL

Sevgili Anneme, Aileme…

ETİK

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

03/01/2018

Ahmet ŞENOL

ÖZET

ESNEK RESİM DAMGALAMA: BLOK TABANLI DAMGALAMA ANALİZİ, VEKTÖR DAMGASI KULLANIMI VE DOĞRULAMA DAMGALAMASININ GELİŞTİRİLMESİ

AHMET ŞENOL

Doktora, Bilgisayar Mühendisliği Bölümü

Tez Danışmanı : Prof. Dr. Hayri SEVER

Ocak 2018, 130 Sayfa

Dijital bir çağda yaşamakla beraber verilerin korunması, başkası tarafından sahiplenilmesinin engellenmesi, dosyanın orijinali ile aynı olduğunun, bize gönderilen dosyanın iletim ortamında değiştirilmediğinin teyidi daha önem kazanmıştır. Dijital ortamdaki resimlerin ve videoların telif haklarının korunması, değişikliğe uğrayıp uğramadığının kontrol edilebilmesi amacıyla dijital damgalama tekniği geliştirilmiştir.

Sahiplik ispatı veya orijinalliğin teyidi amacıyla yapılan damgalama işlemlerinde resim bir bütün olarak ele alınıp başka bir uzaya çevrilmekte, yeni uzayda damgalanmakta, uzay dönüşümünün ters işlemi ile tekrar piksel uzayına dönülüp damgalı resim elde edilmektedir. Bu tez kapsamında yapılan bir çalışmada, resmi bütün olarak diğer uzaya alma ile bloklara ayırdıktan sonra diğer uzaya alma arasında ne gibi farklar olduğu, blok büyüklüğünün dayanıklı damgalamaya etkisi araştırılmış ve ortaya konmuştur. Buna göre, blok tabanlı çalışmaların dayanıklı damgalamada daha başarılı sonuçlar verdiği ancak işlemci kaynağını daha fazla

kullandığı ve damga ekleme ve çıkarma işleminin daha uzun sürdüğü tespit edilmiştir.

Mevcut çalışmalar incelendiğinde damgalama işlemlerinde damga olarak resmin özet değeri, sözde rastgele sayı dizisi, siyah beyaz resim logosu v.b. kullanıldığı görülmektedir. Damgalama işleminde vektör resmi formatındaki firma logosunun damga olarak uygulanması bilindiği kadarı ile bu çalışmadan önce denenmemiştir. Vektör resmi, siyah beyaz resimden farklı olarak, piksel değerlerinden oluşan bir matris değil, nokta, çizgi, bezir eğrisi, poligon gibi geometrik şekillerin pozisyon ve özelliklerinin girildiği dosya biçimidir. Vektör resimlerinin özelliği, resmin büyüme ve küçültülmesinde kalite kaybına uğramamasıdır. Bu tez çalışması kapsamında yapılan çalışmada, ana resme damga olarak vektör resmi dayanıklı damgalama yaklaşımı ile DWT uzayında damgalanmış, kesme ve döndürme saldırıları hariç kayıplı sıkıştırma, histogram eşitleme, 3x3 alçak geçirgen filtreleme gibi birçok saldırıya karşı dayanıklı olarak damgalama yapılabildiği gösterilmiştir.

Resmin orijinalliğini ispatlamak için yapılan damgalama işlemlerine doğrulama amaçlı damgalama denir. Resme yapılan her türlü değişikliğe karşı hassas olan, yapılan değişikliği masum veya kötü niyetli olarak ayırmayıp doğrulama işleminin neticesini olumsuz olarak neticelendiren damgalama işlemlerine kırılgan damgalama işlemleri denir. Bu tezde DWT uzayında damgalama yapan kırılgan bir doğrulama yöntemi geliştirilmiştir. Söz konusu yöntem, resimde değişikliğe uğramış bölümleri başarılı bir şekilde ortaya çıkarması, uygulama kolaylığı getirmesi ile öne çıkmaktadır.

İdeal doğrulama damgalama algoritması masum resim işleme operasyonlarına karşı dayanıklı, kötü niyetli resim hilelerine karşı kırılgan olmalıdır. Resmin kayıplı sıkıştırmaya uğraması, büyüklüğünün değiştirilmesi, keskinleştirme veya alçak geçirgen filtreye maruz kalması, histogram eşitleme v.b. işlemler masum işlemlere örnek verilebilir. Resimdeki bir kişinin resimden çıkarılması, kişinin yüzünün değişmesi, aracın plakasının değiştirilmesi, araya girme saldırı yöntemi ile gönderilen asıl resmin yerine başka resim gönderilmesi v.b. işlemler kötü niyetli işlemlere örnek verilebilir. Yarı kırılgan damgalama yöntemleri masum resim işlemlerine uğramış resimleri doğrulayacak, kötü niyetli olan işlemleri ortaya çıkaracak olan ideal yarı kırılgan yönteme yaklaştığı ölçüde başarılı sayılır. Tez çalışması kapsamında DWT ve DCT uzayını kullanan, doğrulama ve telif hakkı

damgalama amaçlarının ikisini de gerçekleştiren yarı kırılgan bir damgalama yöntemi geliştirilmiştir. Geliştirilen yarı kırılgan yöntem, kötü niyetli değişiklikleri başarılı şekilde tespit etmekle beraber, kayıplı %75 kalitede jpeg sıkıştırmasına maruz kalmış resmi başarılı olarak doğrulamakta, diğer mevcut yarı-kırılgan yöntemlerden üstün olarak, histogram eşitleme, şiddet ayarlama, gamma düzeltmesi işlemlerine maruz kalmış resimleri de doğrulayabilmektedir. Geliştirilen yöntem, kolaj saldırılarına karşı da dayanıklıdır.

Anahtar Kelimeler: Resim damgalama, blok analizi, resim uzayı, dönüşüm, ayrık dalgacık dönüşümü, DWT, ayrık kosinüs dönüşümü, DCT, vektör resmi, scalable vector graphics SVG, doğrulama, telif hakkı, korelasyon, sözde rastgele sayı dizisi, PRNS, benzerlik, gürbüzlük, yarı kırılgan

ABSTRACT

RESILIENT IMAGE WATERMARKING: BLOCK-BASED IMAGE WATERMARKING ANALYSIS, USING VECTOR IMAGE AS WATERMARK AND IMPROVING AUTHENTICATION PURPOSE WATERMARKING

AHMET ŞENOL

Doctor of Philosophy, Department of Computer Science

Supervision: Prof. Dr. Hayri SEVER

Ocak 2018, 130 Pages

As we live in a digital World, protecting our digital property and to be sure that the data we receive is the same as original has become more important. Digital watermarking emerged as a discipline to ensure copyright ownership and authenticating digital data.

The image is transformed into another domain, watermarked in this new domain and restransformed into pixel domain by applying inverse transform in most of the copyright protection and authentication type of watermarking algorithms. In the scope of this thesis, it is searched if it makes a difference between transforming an image to the new domain as a whole or dividing the image into blocks and transforming each block to new domain separately. It is examined if using block-based approach affects watermarking performance for different block sizes for DWT-based watermarking. It is revealed by this study that dividing the image into blocks beforehand, transforming each block to new domain separately, and then watermarking the blocks improves robustness drastically. It is also revealed by this

study that as block size decreased, robustness increased with the cost of extra cpu time needed.

In most of the previous image watermarking studies, an image digest, a pseudo random number sequence, a binary image logo etc is inserted as a watermark. To the best of our knowledge a vector image is not used as a watermark before. A vector image is different from a binary image in that it does not consist of pixels but consists of points, circles, polygons, lines, beziers etc. All those items have their own attributes. For example, a circle has center point coordinates (x,y), diameter, line color, line width etc. Vector images' quality does not suffer from scaling operations. In this thesis a vector image is embedded as a watermark in a robust way in DWT domain that survived jpeg compression, histogram equilization, 3x3 low-pass filter except cropping and rotation attacks.

The type of watermarking that pursues proving the image's geunineness is image authentication type of watermarking. Fragile type of authentication purpose image watermarking is sensitive to every type and amount of change and does not discriminate the changes as ill purposed or innocent. In the scope of this thesis, a new fragile DWT-based authentication type of image watermarking algorithm is introduced. The method detects the changed region of the image successfully and it is easy to implement.

The ideal authentication type of watermarking is expected to be robust against innocent type of changes applied to the image and to be fragile against ill-purpose changes performed on the image. Lossy image compression applied to the image, scaling, sharpening, blurring, histogram equilization that affect all of the image can be given as examples of innocent type of operations to be performed on an image. Removing an existing person from an image, changing one's face, changing a car's licence plate, perform "man in the middle attack" can be given examples for the ill-purpose operations that can be performed on an image. The semi-fragile authentication watermarking method will approach the ideal form as the type of ill-purpose attacks it detects increases and authenticates the images that are subjected to innocent operations. In the scope of this thesis, a new semi-fragile authentication image watermarking method is built up that uses DCT and DWT domains, that embeds two watermarks to the image for copyright protection and authentication purposes. The built-up method authenticates %75 quality jpeg

compressed images and in addition to the existing methods, authenticates images that are subjected to histogram equilization, intensity adjustment and gamma correction. The new method is also immune to collage attacks.

Keywords: Image watermarking, block analysis, domain, transformation, discrete wavelet transform DWT, discrete cosine transform DCT, vector image, scalable vector graphics SVG, authentication, copyright protection, correlation, pseudo random number sequence PRNS, fidelity, robustness, semi-fragile

TEŞEKKÜR

Tez danışmanım sayın Prof. Dr. Hayri SEVER'e, doktora programının her aşamasındaki kıymetli desteklerinden, tez çalışmamın hedefe ulaşmasındaki çok değerli katkılarından dolayı minnettarım.

Sayın Yrd. Doç. Dr. Ersin ELBAŞI'na resim damgalama konusunda bana verdiği çok kıymetli desteğin yanısıra hazırladığımız bildirilerdeki çok değerli katkılarından dolayı teşekkürü borç bilirim.

Sayın Prof. Dr. Erkay SAVAŞ ve Sayın Yrd. Doç. Dr. Murat AYDOS'a tez süresince değerli vakitlerini ayırmaları ve değerli katkılarından dolayı şükranlarımı sunarım.

Hacettepe Üniversitesi Bilgisayar Mühendisliği çok kıymetli öğretim üyelerine teşekkürü borç bilirim.

Dr. Âdem MÜLAYİM'e görüntü işleme ve tez konusunu seçme hususunda verdiği değerli katkılarından dolayı teşekkür ederim.

Doç.Dr. Mehmet ÇİYDEM'e benim için bulduğu benzer tez örnekleri ve akademik çalışmalar hakkında verdiği bilgilerden dolayı teşekkür ederim.

Ramazan UĞURLU'ya tezin yazım kurallarına uygunluğu ve hata düzeltmeleri konusundaki katkılarından dolayı teşekkür ederim.

Âdem TOSUN'a vektör resimleri konusundaki katkılarından dolayı teşekkür ederim.

Değerli eşime ve çocuklarıma bana doktora çalışmaları boyunca katlandıkları ve desteklerinden dolayı teşekkür ederim.

İÇİNDEKİLER

Sayfa

TABLOLAR

Sayfa

ŞEKİLLER

Sayfa

KISALTMALAR

SVG Scalable Vector Graphics

DCT Discrete Cosine Transform

DWT Discrete Wavelet Transform

PSNR Peak Signal to Noise Ratio

SR Similarity Raito

PRNS Pseudo Random Number Sequence

PDF Portable Document Format

CD Compact Disc

DVD Digital Versatile Disc

QR Quick Response

FFT Fast Fourier Transform

RMSE Rounded Mean Square Error

BCH Bose, Chaudhuri ve Hocquenghem

JPEG Joint Photographic Experts Group

RSA Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman

AES Advanced Encryption Standard

RC4 Ron's Code 4 (RSA Variable-Key-Size Encryption Algorithm by Ron Rivest)

EXIF Exchangeable Image File Format

LPC Linear Predictive Coding

ISO International Standard Organization

XML e**X**tensible **M**arkup **L**anguage

RGB Red Green Blue

IWT Integer Wavelet Transform

1. GİRİŞ

Bilgisayar teknolojilerinin gelişmesi, veri depolama kapasitelerinin artması ve ucuzlaması, iletişim imkânlarının inanılmaz derecede artması ile birlikte insanlığın sahip olduğu ve paylaştığı dijital verilerde büyük artış olmuştur. 2016 yılı itibarı ile üretilen çalışmaların büyük çoğunluğu dijital ortamdadır. 2010 yılında Google CEO'su Eric Schmidt, Lake Tahoe'deki Techonomy Konferansında her iki günde bir insanlığın başlangıçtan 2003 yılına kadar oluşturduğu veri kadar veri (5 exabayt ≈ 1 milyon terabayt) oluşturduğumuzu ifade etmiştir [1].

Bir amatör fotoğrafçının veya bir foto muhabirinin çektiği çok özel ve eşsiz bir fotoğraf, bir grafik artistinin çizdiği bir vektör logosu, büyük emeklerle oluşturulmuş bir kitabın elektronik hali, milyon dolarlar harcanarak çekilmiş bir film; hepsi dijital ortamdadır ve kolaylıkla çalınma veya izinsiz kullanılma riski altındadır. Fiziksel olarak çalma fiiline karşı daha kolay korunabilen bir kitap, dijital ortama girdiğinde kolaylıkla kopyalanabilmektedir. Bir kitabın üzerine veya sayfalarının arasına tükenmez kalemle adı soyadı yazılarak, en azından o sayfaların imzalı kısımları yırtılmazsa, kişi o kopyanın sahipliğini ispatlayabilir. Ancak elektronik ortamda bir kitaba sahipliği damgalamak o kadar kolay değildir. Kitaplar dijital ortamda değilken de korsan bir şekilde bastırılabilmekle beraber hem bastırılan kopya genelde daha kalitesiz olmakta, hem de en azından korsan kopya için korsan kullanıcı bir miktar ücret ödemek zorunda kalmaktadır. Ayrıca korsan da olsa risk alarak basım yapacak bir matbaa, ciltleme donanımı gerekmektedir. Bir kitabın dijital kopyasına korsan olarak erişmek genellikle maliyetsiz olmaktadır. Her ne kadar internet üzerinde korsan içeriğin edinilmesine yardımcı olan siteler mahkeme kararı ile kapatılıyor ise de torrent programları ile uçtan uca iletişim yolu ile insanlar genel olarak dijital dosyaları izinsiz ve kanunsuz olarak paylaşmaktadır. İzinsiz kopyalamanın önüne geçilmesi, dijital bir verinin sahipliğinin ispatlanması, uzlaşmazlık durumunda mahkemede delil kabul edilebilmesi önem kazanmaktadır.

Dijital varlıkların korunması için zaman içerisinde çeşitli yöntemler geliştirilmiştir. Kriptolama dijital varlıkları koruma yöntemlerinden birisidir. Bir dosya bir depolama ünitesinde şifrelenmiş olarak bulunabilir. Bir yerden başka bir yere şifreli olarak gönderilebilir. Söz konusu dijital varlığın sadece kişisel amaçlarla kullanıldığı durumlarda kriptolama bir sorun olarak görünmemektedir. Kripto anahtarına ve

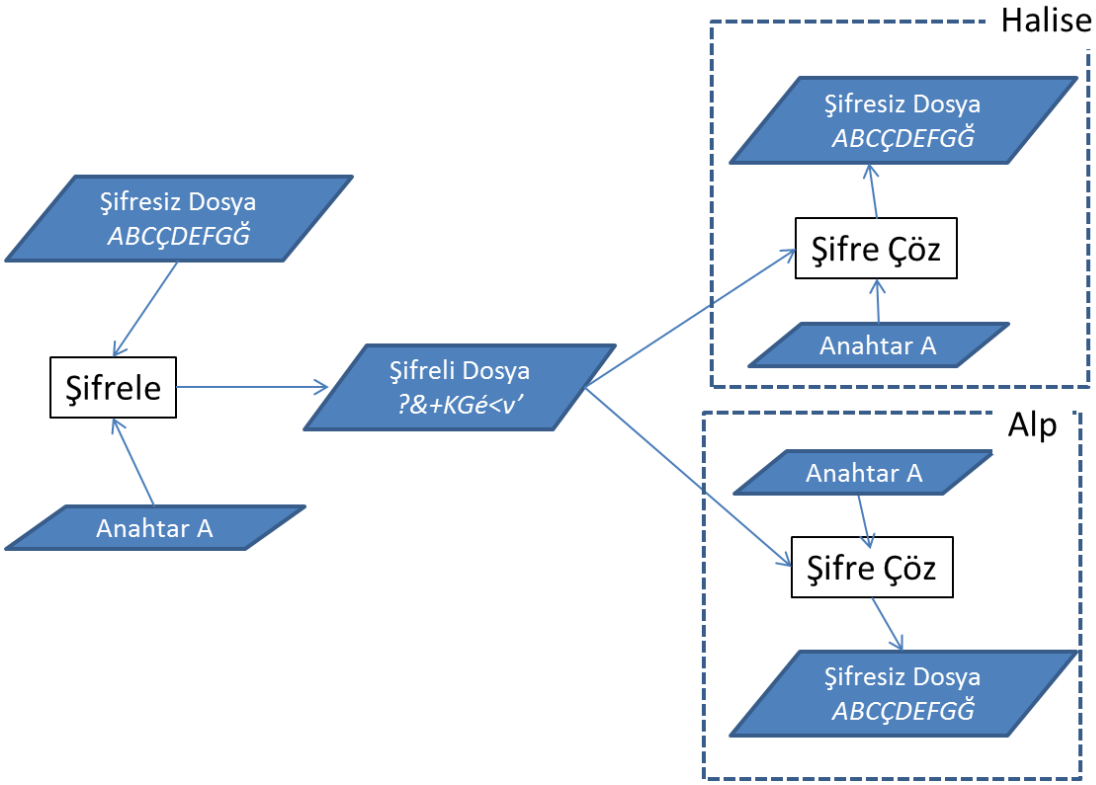
çözücü programa sahip olmayan bir kişinin şifreli içeriği görmesi neredeyse imkânsızdır. Paar'a göre bilgisayar teknolojisinin mevcut ivmeyle gelişmeye devam etmesi halinde önümüzde ve daha on yıllarca 112 bit ve daha üstü uzunlukta anahtarlarla doğru algoritma ile şifrelenmiş dokümanlar güvende olacaklardır[2]. Şifrelenmiş dosyanın kıymeti kalmayana veya kritikliği ortadan kalkana kadar şifrenin çözülmesi mümkün görülmemektedir. Kriptolama çözümünde, bir dijital içeriği birden fazla kişinin kullanması durumunda anahtarın, şifre çözüm programının veya algoritmasının da her bir kullanıcı tarafından bilinmesi gereklidir. Algoritmanın gizli olmasının faydaları olsa da esas olarak güvenliği anahtarın gizliliğinin belirlemesi gerekir. 1883 yılında Auguste Kerckhoff tarafından Kerckhoff yasaları belirlenmiştir [3].

1. Sistem matematiksel olarak kırılabilse de pratikte kırılamamalıdır.
2. Algoritma gizli olmamalı, düşmanın eline geçmesinden endişe edilmemelidir.
3. Anahtar yazılı kâğıtlara bağımlı olmadan tarafların rızası ile değiştirilebilmelidir.
4. Sistem iletişim araçları ile uyumlu olmalıdır.
5. Taşınabilir olmalı ve çalışması için birden fazla kişinin biraraya gelmesine ihtiyaç duyulmamalıdır.
6. Sistemin kullanımı kolay olmalı, bir seri kuralın gözetildiği ve kullananın zihinsel gerilimine yol açmayacak şekilde olmalıdır.

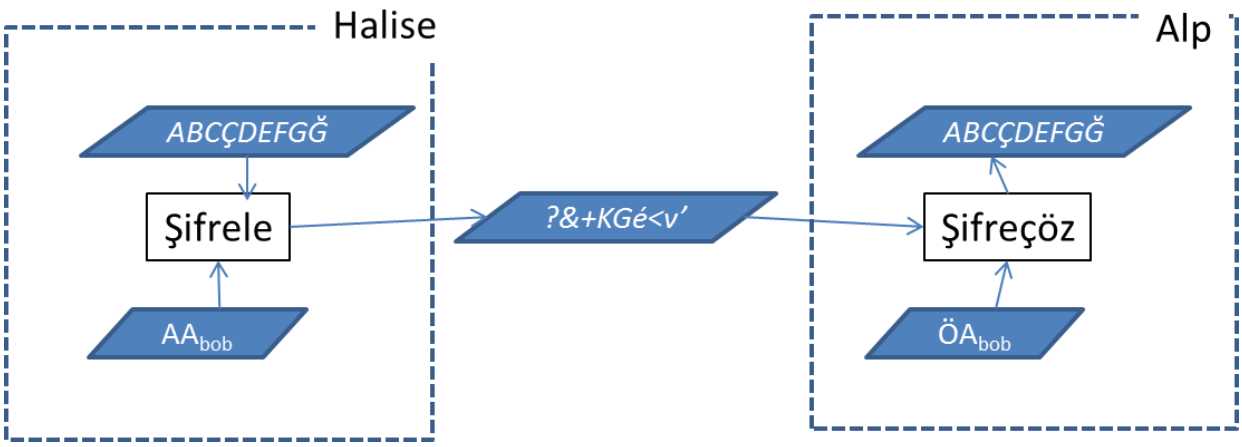
Şifreleme işlemleri simetrik ve simetrik olmayan şifrelemeler olarak sınıflanabilir.

Şekil 1.1' de simetrik şifreleme yöntemi görülmektedir. Simetrik şifrelemede dosya şifrelendiği anahtar ile açılır. Anahtar elinde bulunan kişi hem şifreleyebilir, hem de şifreli dosyayı açabilir. Bundan dolayı dosyayı kullanan tüm kullanıcılarda şifrenin bulunması gereklidir. Hemen hemen tüm kriptolama sistemlerinde temel problem anahtarın güvenli bir şekilde nasıl paylaşılacağıdır. Dosyanın veya içeriğin durağan olmaması ve anahtarın belli aralıklarla değişmesi durumunda anahtarın tüm kullanıcılara güvenli olarak ulaştırılması önemli bir güvenlik sorunu olarak ortaya çıkmakta ve bu sorun genellikle şifreli dosya ile anahtarın farklı iletim ortamlarından gönderilmesi ile aşılmaya çalışılmaktadır. Şifreli dosyanın e-posta ekinde gönderilip şifrenin SMS olarak gönderilmesi bu duruma bir örnek olarak gösterilebilir.

Simetrik şifreleme performans olarak hızlı olsa da, anahtar paylaşımındaki sorunları gidermek için asimetrik şifreleme yöntemi geliştirilmiştir. Asimetrik şifrelemede her kişinin bir özel (private), bir de anonim (public) anahtarı vardır. Anonim anahtar tüm kullanıcılarla paylaşılmakta, özel şifre kimse ile paylaşılmamaktadır. Şekil 1.2 de görüldüğü gibi Halise (Alice) Alp'e (Bob) bir mesaj gönderirken Alp'in anonim anahtarını (AA_{alp}) kullanarak dosyayı şifreler. Şifrelenmiş dosyayı Halise dâhil Alp'in özel anahtarına ($ÖA_{alp}$) sahip olmayan hiç kimse açamaz. Sadece Alp kendi özel anahtarı ile açabilir. Alp de Halise'ye şifreli bir dosya göndereceği zaman Halise'nin anonim anahtarını (AA_{halise}) kullanarak dosyayı şifreleyip Halise'ye gönderir. Halise aynı şekilde kendi özel anahtarını kullanarak ($ÖA_{halise}$) şifreli dosyayı açar.



Şekil 1.1. 'ABCÇDEFGĞ harf dizesinin simetrik şifreleme yöntemi ile gönderimi



Şekil 1.2. 'ABCÇDEFGĞ' harf dizesinin özel anahtar ve anonim anahtar kullanarak gönderimi

Şifreleme her ne kadar noktadan noktaya dosyanın iletilmesini sağlasa da işlemesi için anahtar paylaşımına ihtiyaç duymaktadır. Şifrelemenin asıl zayıf tarafı, şifre çözüldükten sonra dosyanın tamamen savunmasız kalmasıdır. Bir film yapımcısı Halise, bir film yorumcusu Alp'e daha gösterime girmemiş filmini değerlendirmesi için şifreli olarak gönderdiğinde, Alp'in şifreyi çözdükten sonra kötü niyetli olarak filmin internete düşmesini sağladığı düşünülsün. Halise, filmin Alp tarafından yayıldığını ispat edemeyecektir. Alp, filmin kendisinden değil, Halise'den şifresiz olarak yayıldığını iddia edecektir.

Dijital damgalama, bahse konu problemlere çözüm olarak bulunan yöntemlerden biridir. Dijital damgalama, dijital bir veri veya dosyanın içerisine normal duyu organlarıyla varlığı anlaşılamayacak şekilde damga yerleştirmek, istendiğinde de geri çıkartabilmektir.

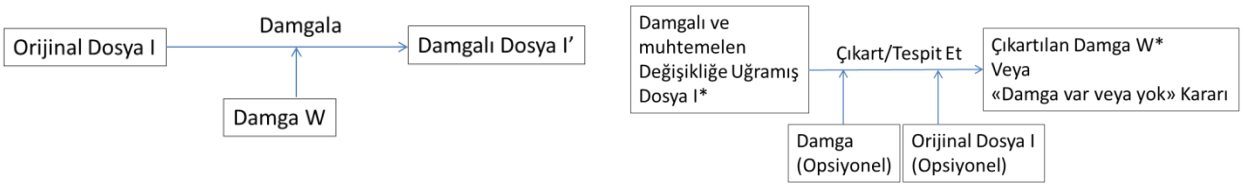
Dijital damgalama, bir dijital dosyanın sahipliğini ispatlamak için kullanıldığında, damga, ana çalışma olan dosyadan kolay çıkartılamayacak şekilde damgalanır ve dosya silininceye kadar dosyanın bir parçası olarak kalmaya devam eder. Bir film dosyası içerisine yerleştirilmiş damga, film dosyası şifreli olmasa bile dosyanın sahibinin kim olduğunu açığa çıkarır.

Damganın yerleştirildiği ve asıl korunmak istenen çalışmaya ana çalışma, ana çalışmanın içerisine yerleştirilen veriye de damga denir. Ana çalışma resim, video, ses dosyası olabildiği gibi bir word dokümanı, metin dosyası da olabilir. İçine fark edilmeyecek şekilde damga yerleştirilebilen her dosya tipi bir ana dosya olabilir.

Pdf dokümanları da görünmez damga ile damgalanabilmektedir [4], [5]. Damgalamanın amacına göre damga olarak siyah beyaz bir firma logosu, dosyanın sahibinin siluet resmi, oldukça büyük bir bit uzunluğunda bir sayı dizisi, kişinin kendi sesi veya belirli bir ses vb. konabilmektedir.

Damgalama işleminde damganın eklenmesi ve geri çıkarılması söz konusudur. Sahipliği ispat maksadıyla damgalanmak istenen orijinal I dosyası W damgası ile damgalanıp damgalı I' dosyası elde edilir. Damgalama işlemi Şekil 1.3.a da görülmektedir. Şekil 1.3.a'da damga dışardan sisteme verilen girdi gibi görünse de bazen orijinal dosyanın kendisinden de türetilebilir. Orijinal dosyadan damga üretirken dışarıdan girilecek bir anahtara göre damga üreten sistemler de vardır. Şekil 1.3.b'de ise damgalı olup olmadığı tespit edilmeye çalışılan bir I* dosyasından damganın çıkarılmaya çalışılması görülmektedir. I* dosyası damgalı ve damgalandıktan sonra hiçbir değişikliğe uğramamış bir dosya olabilir, damgalı bir dosya olup bilinçli veya biliçsiz şekilde değişikliğe uğramış bir dosya olabilir veya damga ihtiva etmeyen bir dosya olabilir. Bazı algoritmalar, "damga var" veya "damga mevcut değil" kararını kendisi verebildiği gibi, bazı algoritmalar damgayı çıkarıp kararı kullanıcıya bırakabilir. Damga çıkarma işlemi esnasında eldeki karar verilecek dosyaya ilaveten orijinal dosyaya ihtiyaç duymayan algoritmalara kör damgalama algoritmaları, orijinal dosyaya ihtiyaç duyan algoritmalara kör olmayan damgalama algoritmaları adı verilmiştir. Damganın kendisini orijinal dosyadan üreten algoritmalar damganın mevcut olup olmadığına karar verirken damgalama esnasında eklenen orijinal damgaya ihtiyaç duymayabilir.

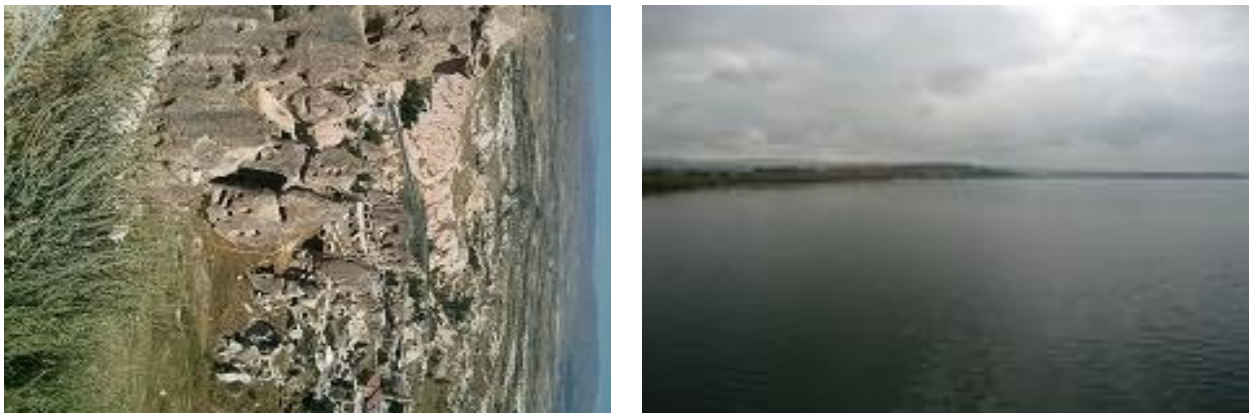
Damgalı dosyanın bir resim olduğu ve bu dosyanın sahibi olan Halise tarafından kendi web sitesine konduğu, bu siteden Alp'in resmi indirdiği, yukardan ve kenardan biraz kırpıp izinsiz olarak kendi sitesinde kullandığı düşünülsün. Bu durumda I* dosyası damgalı ve değişikliğe uğramış bir dosya olacaktır. Hiçbir değişikliğe uğratmayıp olduğu gibi kullanılması durumunda I' ile I* birbirine eşit olacaktır. Dosyanın gerçek sahibi kendi dosyasının başka web sitesinde olduğunu fark edip o dosyayı indirerek, indirdiği I* dosyasından kendi damgasını çıkartabilir. Dosyanın gerçek sahibi, korsan kullanıcı sitedeki dosyasından çıkarttığı damga W*'nin orijinal damgası W ile aynı olduğunu göstererek site sahibini önce uyarmak sureti ile dosyayı kaldırtacak, kaldırılmazsa hukuk yoluna başvurabilecektir.



a.Resim Damgalama b.Damga Çıkartma/Tespit Etme

Şekil 1.3. Damgalama ve Çıkartma İşlemleri

Ana dosyanın damgayı barındırabilecek ve damganın varlığını fark ettirmeyecek bir sığasının olması önemlidir. Sadece 10 kelimeden oluşan bir metin dosyasına fark edilmeyecek bir damga konulması pek olası değildir ancak 15000 kelimeden oluşan bir metin dosyasının bir damgayı barındırma kapasitesi çok daha yüksektir. 3264*2448 boyutlarındaki renkli bir resimde 3264*2448*3*8= 191.766.528 bit bulunmakta, fark edilmeyecek şekilde bir damga barındırma kapasitesi yüksek bulunmaktadır. Ana dosyanın boyutunun büyük olması sığasını artıracağı gibi, bir dosyanın içindeki içeriğin karakteristik özellikleri de önemlidir. İçerisinde ağaçların bulunduğu karmaşık bir manzara resminin, bembeyaz ve dümdüz bir gökyüzü resminden çok daha iyi damga saklama kapasitesi vardır çünkü resimde yapılan değişiklik düz bir zeminde yapılacak değişiklik kadar fark edilmeyecektir. Şekil 1.4'de boyutları aynı ancak damgalama sığası farklı 2 resim görülmektedir



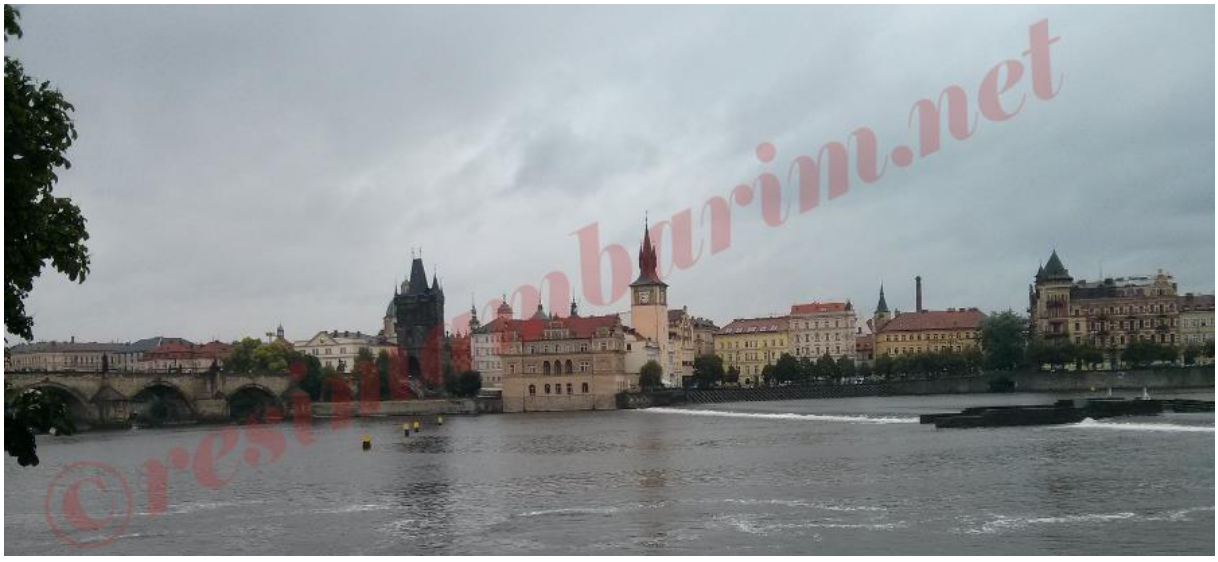
a. Damga sığası yüksek detaylı resim b. Damga sığası düşük daha düz bir resim

Şekil 1.4. Damga sığası farklı resimler

Damganın, sahipliği ispatlayacak ve damganın ana çalışmadan çıkartılmasını tesadüfle açıklanmasına izin vermeyecek büyüklükte olması önemlidir. 2 bit uzunluğunda bir damganın bir resimden çıkartılması sahipliği ispat etmekte

yetersiz kalacaktır çünkü 2^2 = 4 ihtimalden birinin gerçekleşmesi her durum için 25% olasılık demektir ve damganın çıkarılma durumunu tesadüfle açıklamaya kapı aralayacaktır. 100*100 lük bir siyah beyaz resim damgasının bir ana resimden çıkartılması durumunda 1/20,000 olasılığı olan bir durum olmuş demektir ve sahipliği ispatlayacak yeterlikte sayılabilir. Çıkartılan siyah beyaz damganın yerleştirilen damga ile birebir aynı olması şart koşulmazsa genel olarak bir hata payı oranı kullanılır. %5 hata payı verilmesi durumunda ihtimal dâhilindeki 20,000 damgadan 1000 tanesi şartı sağlayabilecektir. Resmin sığasının büyük olması durumunda damga boyutu artırılarak da şans faktörü azaltılabilecektir.

Şekil 1.5'de görüldüğü gibi bazı uygulamalarda damga görünür olarak eklenebilmektedir. Adobe Systems ve Microsoft firmaları Pdf ve Word dokümanları üzerine görünür damgalar ekleme imkânı sunmaktadır. Pek çok kelime işlem veya doküman üreten firma, yazılımına bu imkânı kazandırmıştır. Damganın görünür olması durumunda damganın ortadan kaldırılması mümkün olduğundan, görünür damgalama her ne kadar kullanılsa da dijital damgalamada asıl istenilen damganın belirli olmamasıdır. Resim damgalama yapılmışsa damgalı resme çıplak gözle bakıldığında bir damgalama olduğu hissedilmemelidir. Ses damgalama yapılmışsa damgasız orijinal ses ile damgalı ses arasında insan kulağının duyarlılık sınırları içinde hissedilir bir fark olmamalıdır.



Şekil 1.5. Görünür damga ile damgalanmış bir resim

1.1 Problem

Damga çalışmalarının pek çoğu farklı dönüşüm uzaylarında yapılmaktadır. Resim başka bir dönüşüm uzayına alınmakta, dönüştüğü uzayda damgalanmakta ve tekrar piksel uzayına geri dönüştürülmektedir. Dönüşüm uzayları daha detaylı olarak bölüm 2.3'de açıklanmaktadır. Farklı uzaylarda damgalama yapan algoritmaların bir bölümü resmi bütün olarak diğer uzaya çevirmekte, bazıları ise resmi önce bloklara böldükten sonra blokları bağımsız olarak ayrı ayrı dönüşüm uzayına çevirmektedir. Damgalama konusunda yapılan çalışmalarda her ne kadar bu iki yaklaşımdan biri seçilse de, iki yaklaşım arasında yapılacak seçimin damgalamaya ne tür bir etkisi olacağı, gürbüzlüğü olumlu veya olumsuz etkileyip etkilemeyeceği, blok ebatının bir etkisinin olup olmayacağı, damgalanmış resmin orijinal resme benzerliğinin iki yaklaşımdan birinin seçiminden etkilenip etkilenmeyeceği konularında yapılmış bir çalışma mevcut değildi. Bu tezde bu sorulara yanıt arayacak şekilde aşağıdaki işlemlerin yapılması hedeflenmiştir:

- Resmin bütün olarak DWT uzayına alınarak damgalanması,
- Resmin bloklara bölünerek her bir bloğun DWT uzayına bağımsız olarak alındıktan sonra damgalanması,
- Bloklu olarak yapılan damgalamanın farklı blok büyüklükleri ile de yapılması,
- Farklı blok büyüklüğü ile damgalanmış resimlerin her birinin orijinal resme benzerliğinin(PSNR değerlerinin) hesaplanması,
- Damgalanmış resimlere farklı resim operasyonları düzenlenmesi (kayıplı sıkıştırma, histogram eşitleme, Gauss gürültüsü, Gamma Düzeltmesi v.b.),
- Her bir blok büyüklüğü ve her bir farklı resim operasyonu uygulanmış damgalı resimlerden damganın geri çıkarılması,
- Çıkarılan her bir damganın orijinal damga ile karşılaştırılarak orijinal damgaya benzerliğinin hesaplanması,
- Her blok büyüklüğünde yapılan damgalama ve damga geri çıkarmanın işlemci zamanı gereksiniminin kaydedilmesi,
- Değişik blok büyüklerinde yapılan damgalama ve damga çıkarma operasyonlarının aşağıdaki yönlerden karşılaştırılıp analiz edilerek,
    - Resmin orijinaline benzerliği (PSNR) yönünden karşılaştırılması,

- Geri çıkartılan damganın orijinal damgaya benzerliği yönünden karşılaştırılması,
- Damgalama ve geri çıkarma işlemlerine harcanan işlemci zamanı yönünden karşılaştırılması.

Resim damgalama çalışmalarında damga olarak sözde rastgele sayı dizisi, siyah beyaz resim, resim hakkında meta veri v.b. kullanan birçok çalışma yapılmıştır. Firma logoları genel olarak vektör resmi olarak tasarlandığı halde siyah beyaz resme çevrilerek konulduğunda hem renk bilgisi kaybolmakta, hem de siyah beyaz resmin boyutu vektör resmine göre nisbi olarak daha fazla yer tutmaktadır. Vektör resimlerini sahipliği ispatlamak için damga olarak kullanmak daha önce denenmemişti. Firma logosu olarak 256x256 boyutlarında bir siyah beyaz resim 65536 bitlik veri ile tutulabilirken aynı boyutlarda bir vektör resmi yaklaşık 2 kilo byte yani 16384 bitlik veri ifade etmektedir. Vektör resminin boyutunun büyüdüğünde kalitesinde düşme olmaması, renk bilgisi de ihtiva etmesi ilave artılarıdır. Tez kapsamında aşağıdaki işlemlerin yapılması hedeflenmiştir:

- Bir vektör resim formatı seçilmesi,
- Vektör resminin ana resme nasıl damgalanacağının belirlenmesi
- Vektör resminin ana resimden nasıl çıkarılacağının belirlenmesi
- Vektör resmi ile damgalanan resmin orijinal resme benzerliğinin (PSNR) hesaplanması
- Damgalı resme bilinen resim operasyonları uygulanması
- Resim operasyonları uygulanan damgalı resimlerden vektör damgasının geri çıkartılması
- Vektör damgalarının birbiri ile karşılaştırılması yönünde yeni metrik geliştirilmesi
- Geri çıkartılan vektör damga ile orijinal vektör damgasının karşılaştırılması
- Vektör damgalamanın başarı metriklerinin belirlenmesi

Resim damgalamanın en çok kullanıldığı alanlardan birisi de resim doğrulamadır. Resmin bir yerden diğerine gönderilmesi durumunda resmi alan, resmin gönderildiği hali ile aynı olduğunu teyit etmek isteyebilir. Resim damgalamadan önce bu konuda kriptografik resim özeti kullanılmakta idi. Resimden bir anahtara bağlı olarak bir resim özeti çıkarılmakta, resim ile beraber veya başka bir iletim

vasıtası ile anahtar ve resim özeti de karşı tarafa gönderilmektedir. Resimden ayrı olarak anahtar ve resim özeti gönderilmek zorunda kalınması ve resim doğrulanırken kriptografik özetin resmi bütünüyle doğrulaması veya doğrulamaması, araştırmacıları farklı arayışlara yönlendirmiş, bu amaçla resim damgalama da kullanılmaya başlanmıştır. Doğrulama amaçlı resim damgalamada hedef öncelikle resimde bir değişiklik yoksa resmin doğrulanması, resimde değişiklik var ise değişen yerlerin işaretlenebilmesidir. Resimdeki en ufak bir değişikliğin resmin doğrulanamamasına yol açan damgalama çeşitlerine tam kırılgan damgalama çeşidi denir. Çok yüksek güvenlik isteyen bazı işlemlerde bu derece katı olmak gerekebilir. Zaman içerisinde resim doğrulama için farklı kıstaslar da ortaya çıkmıştır. Resme yapılan ve resmin yorumunu değiştirmeyecek türde değişikliklerin resmin doğrulanmasını engellememesi, buna karşılık resmin anlamını değiştirecek türde değişikliklerin ortaya çıkarılabilmesi istenmiştir. Resmin büyütülmesi veya küçültülmesi, resmin kayıplı sıkıştırma ile sıkıştırılması, parlaklığın ayarlanması v.b. işlemler resmin anlamını değiştirmeyecek türden değişikliklerdir ve resmin doğrulanmasına mani teşkil etmemelidir. Bunun yanında resimde olmayan bir nesnenin resme sonradan ilave edilmesi, resimdeki bir kişinin yüzünün değiştirilmesi, resimde olan bir kişinin resimden silinmesi, resimdeki bir aracın plaka numarasının değiştirilmesi v.b. işlemler de doğrulama damgalaması açısından resmin kötü amaçlı olarak değiştirilmesi olarak algılanmalı ve değişiklik yapılan bölüm tespit edilip işaretlenebilmelidir. Mevcut doğrulama damgalama algoritmaları tüm kötü niyet barındırmayan işlemlere toleranslı, bunun yanında tüm kötü niyetli değişiklikleri de tespit etme noktasından epey uzaktır. Şimdiye kadar geliştirilen algoritmalar kötü niyetli değişiklikleri genelde tespit ederken, tolere edebildikleri masum resim operasyonları çoğunluk itibarı ile tektir. Genel olarak tolere edilebilen masum işlem çeşidi sayısı birdir. Bu konuda en çok kayıplı sıkıştırmayı tolere edebilen doğrulama damgalama algoritmaları geliştirilmiştir. Tez kapsamında mevcut doğrulama algoritmaları hakkında kısa bilgi verilerek,

- Kötü amaçlı değişiklikleri tespit edebilecek,
- Mevcut algoritmalardan daha fazla masum resim işlemini tolere edebilecek,
- Yapılan değişikliği gerekli hassasiyet seviyesinde tespit edebilecek,
- Damgalı resmin orijinal resme benzerliği ilkesini gözetecek,

- Doğrulama damgalama algoritmalarına yapılabilecek kolaj saldırılarına (bakınız bölüm 3.3.1.3.1) karşı önlem almış yeni algoritma veya algoritmalar geliştirilmeye çalışılacaktır.

1.2 Amaç

Dijital damgalamada uzun süredir resim piksel uzayından farklı uzaylara alınarak damgalanmakta, pek çok çalışmada resim bir bütün halinde dönüşüme alınmakta, bazılarında ise resim bloklara bölündükten sonra dönüşüm uzayına alınmaktadır. Blok tabanlı çalışmalar mevcut olsa da DWT uzayında blok tabanlı çalışmanın damgalama gürbüzlüğüne etkisi, blok ebadının damgalama çalışmasının başarısına etkisi daha önceden araştırılmamış idi. Tez kapsamında resmin bloklara ayrılması ile resmin bir bütün olarak ele alınması arasındaki farkların ortaya konması, blok ebadının bir fark yaratıp yaratmadığının, damgalı resme yapılacak saldırılara karşı blok ebadının gürbüzlüğe etkisinin olup olmadığının ve işlemci zamanı yönünden blok ebadının etkisinin araştırılması ve bu yönde testler yapılarak açıklığa kavuşturulması hedeflenmiştir.

Resim damgalamada öncelikle sözde rastgele sayı dizileri damga olarak kullanılmış, daha sonra siyah beyaz firma logoları, sahibin siyah beyaz resmi daha yaygın olarak kullanılmaya başlamıştır. Az da olsa damga olarak meta veri, sahibinin sesini damgalayan çalışmalar da mevcuttur. Vektör resimleri bir firmanın logosu olarak yaygın kullanımı olan bir resim formatıdır. Vektör resimleri piksel olarak gösterilmez. Çizgiler, poligonlar, bezir eğrileri v.b. resmi meydana getiren objelerdir. Vektör resimdeki tüm nesnelerin merkezi koordinatı, kenar kalınlığı rengi v.b. pek çok özelliği vardır. Vektör resimleri renkli olmaları, büyütüldüğünde ve küçültüldüğünde kalite kaybına uğramamaları ile bilinirler. Vektör resim formatlarından svg resim formatı, bu formatın web tarayıcı programları tarafından tanınması ve gösterilebilmesi, bu formattaki resmin kaynak kodunun okunabilir xml formatında olması nedenleriyle tercih edilmiştir. 256x256 boyutlarında siyah beyaz resim damgası 65536 bitlik bir veri meydana getirirken, boyutunu istediğimiz kadar büyütebileceğimiz bir svg formatında renkli resim logosu yaklaşık 2 kilobit yani 16384 bitlik bir damga verisine karşılık gelmektedir. Damganın veri boyutunun küçülmesi, damgayı ana resme veri tekrarı yaparak daha gürbüz şekilde damgalayabilmemizi sağlayabilecek, çıkardığımız damga isteğimiz boyuta büyütülebilecek, aynı zamanda renkli olması sahipliğin ispatı yönünden çok daha

kuvvetli bir şekilde yapılabilecektir. Neredeyse bütün firmaların logoları renklidir. Dolayısı ile sahipliği ispat ederken çıkardığımız logonun renkli olması sahipliği çok daha güçlü şekilde vurgulayacaktır. Bütün bu saydığımız sebepler damga olarak vektör damgası kullanmanın damgalamaya önemli bir katkıda bulunabileceği yönünde bir istek oluşturmuş ve tez çalışması kapsamında bu konu üzerinde testler ve deneyler yapmamızı sağlamıştır.

Resim damgalamanın en önemli kullanım alanlarından biri de damgalamanın doğrulama amaçlı kullanımıdır. Uydudan gönderilen bir görüntünün yolda yakalanıp değiştirilerek gönderilme ihtimaline karşı önlem olarak resim damgalama kullanılabilmektedir. Resmin gönderildiği orijinal hali ile aynı olduğunu doğrulamak için damgalamadan önce kriptografik özet yöntemi kullanılmakta idi. Resmin kriptografik özeti resimle beraber bir anahtar kullanılarak üretilmekte, resimle beraber karşı tarafa gönderilmekte idi. Resmi alan taraf da aynı anahtarı ve aldığı resmi kullanarak dosya özeti çıkarmakta, karşı taraftan aldığı özet ile aynı ise resmi doğrulamakta idi. Her ne kadar kriptografik özet yöntemi denenmiş ve güvenilir bir doğrulama yöntemi olsa da asıl dosyadan ayrı bir özet dosyasının gönderilmek zorunda kalınması bir işletim zorluğu getirmektedir. İlave olarak, kriptografik özet yönteminde resim bir bütün halinde doğrulanmakta, resmin belli bölümünde yapılan değişiklikler belirlenememektedir. Her ne kadar kriptografik özet yönteminde resim bloklara bölünüp resmin hangi bloklarında değişiklik yapıldığı tespit edilebilse de, her bir bloğun özetinin ayrı olarak hesaplanıp gönderilmesi ayrı bir işletim zorluğu getirmektedir. Kriptografik özet yönteminin dezavantajlarından biri de, resmi doğrulama yönünden hiç bir esnekliği olmamasıdır. Resimde bir piksel değerinin sadece bir biti değişse dahi tamamen farklı bir kriptografik özet çıkacağından, yöntemin resimde en ufak bir değişikliğe toleransı yoktur. Resim doğrulama maksadıyla resim damgalama yapmak, resimle ayrı bir özet dosyası göndermek zorunda kalınmaması, resimde yapılan ve resmin anlamını değiştirmeyecek küçük masum değişiklikleri tolere edebilmesi nedeniyle geliştirilmiştir. Resim doğrulama da kriptografik özette olduğu gibi hiç bir değişikliği tolere etmeyecek şekilde tam doğrulama yapabildiği gibi resimdeki bazı değişikliklere esnek de davranabilir. Tam doğrulama algoritmaları hariç esnek doğrulama damgalama algoritmalarının ana hedefi resimlerdeki masum değişiklikleri tolere etmek, kötü niyetli değişiklikleri de tespit etmektir. Tam

doğrulama algoritmalarının diğer adı kırılgan doğrulama, esnek doğrulama algoritmalarının diğer adı yarı-kırılgan doğrulama algoritmalarıdır. Yarı kırılgan damgalama algoritması ile damgalanmış bir resmin kayıplı sıkıştırma veya parlaklığını artırma-azaltma gibi resmin tamamını etkileyen genel bir işlemden sonra da resmi doğrulaması istenir. Resimde bir kişinin yüzünün değiştirilmesi, bir aracın plakasının değiştirilmesi, resimde olan bir nesnenin yok edilmesi v.b. işlemleri yarı-kırılgan algoritmanın tespit edebilmesi istenir. Şimdiye kadar geliştirilen yarı kırılgan algoritmalardan ideal duruma ulaşan bir algoritma yoktur. Geliştirilen yarı kırılgan algoritmalar genel olarak kayıplı sıkıştırma işlemine dayanıklı olmakla birlikte diğer masum sayılabilecek işlemlere dayanıklılığı konusunda fazla bir çalışma yoktur. İdeal yarı kırılgan doğrulama algoritmasına yaklaşmaya çalışan algoritmalar geliştirilmeye devam etmektedir. Bu tez çalışması kapsamında mümkün olduğunca çok masum resim işlemine karşı dayanıklı olabilen, bunun yanında kötü niyetli resim işlemlerini tespit edebilen yeni algoritma ve yaklaşımlar geliştirilmesine çalışılmıştır.

1.3 Özgünlük

DWT uzayında yapılan mevcut damgalama çalışmalarında genellikle resim bir bütün halinde DWT uzayına alındıktan sonra damgalama yapılmakta, ayrışma seviyesi ile damgalama bantları konusunda farklı yaklaşımlar olduğu görülmektedir. Örneğin, Tao ve Eskicioğlu çalışmalarında resmi bütün olarak ele alıp LL, LH, HL and HH bantlarından her birine siyah beyaz resim damgası eklemiş, LL bandı için damga şiddet değeri diğer üç banda göre daha yüksek bir değer uygulamıştır [6]. Ancak DWT uzayında yapılan damgalamada resmin bloklara bölünerek damgalama yapılmasının ve bu yöntemle yapılan damgalamada blok boyutlarının performans ve damgalama başarısına etkilerinin incelendiği bir çalışma bulunmamaktadır. Bu çalışmada söz konusu eksiklik giderilmeye çalışılmış, DWT uzayında yapılan damgalamada, resmi bloklara bölerek her bir bloğun bağımsız olarak DWT uzayına alınması ve ardı sıra yapılan damgalama işleminin, resmi bütün olarak DWT uzayına alma ile arasındaki başarı oranı ve blok ebadının başarıya etkisi araştırılmıştır. Daha küçük blok ebadı ile daha başarılı damgalama yapılabilirken, daha fazla işlemci zamanına ihtiyaç duyulduğu, gerekli işlemci zamanının sıkıntı yaratmayacağı uygulamalar için bloklu DWT damgalamanın uygulanmasının faydalı olacağı ortaya konmuştur.

Alanyazın incelendiğinde damgalama uygulamalarında amaç ne olursa olsun genellikle pixel uzayında tanımlanmış bir resmin (dosya formatından farklılıkları dikkate alınmaksızın) damga olarak kullanıldığı gözlenmektedir. Damgalamada, damga olarak bir vektör resminin kullanıldığı örneğe ise rastlanmamıştır. Bu çalışmada damga olarak vektör resmi kullanılması olanakları incelenerek damgalama alanyazına katkı sağlanmaya çalışılmıştır. Bu amaçla bir vektör resmi, ana resme DWT-tabanlı kör olmayan gürbüz bir yöntemle damgalanmış, yapılan damgalamanın özellikleri incelenmiş, kırılganlığı test edilmiş, mevcut damgalama teknikleri ile vektör damgalama yöntemi kıyaslanarak olası kullanım alanları ortaya konmuştur.

Bu çalışma kapsamında biri kırılgan diğeri yarı kırılgan olmak üzere resim doğrulama amaçlı iki farklı damgalama algoritması geliştirilmiştir. Orijinal resme ihtiyaç duymayan, uygulaması kolay, yüksek PSNR değerine sahip, doğrulama amaçlı bir damgalama algoritması olan ilk algoritmanın gerekli performans ve başarı testleri yapılmıştır. Test sonuçları incelendiğinde geliştirilen yeni damgalama algoritmasının mevcut algoritma seçenekleri arasında uygulanması kolay, PSNR değeri yüksek, değerli bir alternatif olarak öne çıktığı görülmüştür.

İkinci olarak bu çalışma ile temel hedefi resim doğrulama olan, bunun yanında sahipliğin ispatı amacıyla da resmi ikinci bir damga ile damgalayan yarı kırılgan bir damgalama algoritması geliştirilmiştir. Bu yöntemde ana resim orta kısım ve kenar kısım olmak üzere iki kısım olarak ele alınmış, orta kısma sahipliğin ispatı için kullanılacak damga uygulanmıştır. Elde edilen damgalanmış orta kısım kendi içinde bloklara bölünmüş, her bir parça kenar kısmın bölünmesi ile elde edilen bir blok ile bir gizli anahtar yardımıyla eşlenmiştir. Daha sonra her bir orta kısım bloğundan elde edilen damga kullanılarak eşleniği olan kenar kısım bloğu damgalanmıştır. Eşleme işlemi için kullanılacak kenar kısım bloklarının seçiminde baştan ve sondan bazı bloklar hariç tutularak damganın yüksek geçirgen ve alçak geçirgen işlemlere karşı belli oranda gürbüz olması hedeflenmiştir. Resmin orta kısım ve kenar kısım olarak değerlendirilmesi, orta kısım ve kenar kısım büyüklüklerinin farklı olması bu algoritmayı özgün kılan ana yaklaşımlardır. Kenar kısım bloklarının daha büyük olması, damga saklayabilme kapasitesini ve saklanan damganın gürbüzlüğünü artırmaktadır. Orta kısım bloklarının daha küçük olması, daha önemli kişi veya objelerin bulunduğu orta kısımda yapılan

değişikliklerin (varsa) daha hassas tespitini sağlamaktadır. Damgalama yönteminin doğrulama algoritmaları için istenen bir özellik olan yarı kırılgan olması, masum resim işlemleri olan kayıplı sıkıştırma, histogram eşitleme, gamma düzeltmesi, parlaklık ayarlaması gibi işlemlerden etkilenmeyerek resmi doğrulayabilmesi, resme sonradan konan nesneleri veya silinen kısımları tespit edebilmesi önemli katkılar olarak görülmektedir. Geliştirilen damgalama algoritması, mevcut doğrulama algoritmalarından farklı olarak histogram eşitleme, gamma düzeltmesi, parlaklık ayarlaması gibi masum işlemlerin sonunda da resmi doğrulayabilmesi sayesinde önceki çalışmalardan öne çıkmaktadır. Ayrıca damgalama yapılırken sabit bir damga kullanılmaması, damganın ana resime dayalı olarak üretilmesi, algoritmanın Holliman ve Memon'un çalışmasında [7] belirtilen kolaj (collage) ataklarına karşı da başarılı olmasını sağlamıştır.

1.4 Tez Organizasyonu

Devam eden kesimler şu şekilde tasarlanmıştır:

İkinci bölümde "Alan Bilgisi ve Alan Yazın Özeti" başlığı altında, genel olarak damgalama konusunda şimdiye kadar yapılmış çalışmalardan bahsedilmiş, damgalama işleminde kullanılan temel alan bilgisi verilerek, devamında damgalama çeşitleri, iyi bir damgalamanın özellikleri ile damgalamanın başarı kıstasları üzerinde durulmuştur.

Üçüncü bölümde ilk olarak "DWT Uzayında Bloklu Damgalama ve Blok Büyüklüğü Analizi" başlığı altında blok damgalama yöntemi açıklanarak farklı blok büyüklükleri ile yapılan damgalamaların başarıları analiz edilmiştir. İkinci olarak "Ana Resme Damga Olarak Vektör Resmi Damgalamak" başlığı altında vektör resim formatında oluşturulmuş SVG formatındaki bir resim dosyasının damga olarak kullanılarak bir resmin damgalanmasına yönelik bir algoritma verilmiştir. Bu bölümde geliştirilen damgalama algoritmasının performansı, başarısı ve dayanıklılığı da incelenmiştir. Üçüncü olarak "Doğrulama Amaçlı Damgalama" başlığı altında damgalamanın doğrulama amaçlı kullanımı, doğrulama amaçlı damgalamanın türleri ve özellikleri incelenmiş bu konudaki mevcut uygulamalardan bahsedilerek, geliştirilen doğrulama amaçlı kırılgan bir damgalama algoritması açıklanmıştır. Aynı bölümde bölümde geliştirilen algoritmaların test sonuçları verilerek mevcut yöntemlere olan üstünlük ve

zayıflıkları tartışılmış ve geliştirilen yöntemlerin pratik uygulamalarının neler olabileceğinden bahsedilmiştir.

Dördüncü ve son bölümde ise tez çalışması kapsamında geliştirilen algoritmaların artı ve eksileri özetlenerek, alanyazına katkıları belirtilmiş, bu tez çalışmasının devamında yapılabilecek akademik çalışmaların neler olabileceğinden bahsedilmiştir.

2. ALAN BİLGİSİ VE ALAN YAZIN ÖZETİ

Metin belgelerini damgalamak için kayda değer çalışmalar yapılmıştır. Bilgisayarlar yokken de pek çok yazar veya şairin dize ve paragraflara gizli bilgi sakladığı söylenir. Örneğin paragrafların başındaki veya sayfaların başındaki kelimelerin ilk harfleri yan yana getirildiğinde şairin yazarın kendi adı veya sevdiği kişinin adı gibi anlamlı bir şeyler ortaya çıktığı görülür. HTML belgelerinde tag'lerde büyük küçük harf ayrımı olmadığından şifrelenecek bilgiye göre tag'lerin bazı harflerini büyük, bazılarını küçük harfle yazarak da damgalama yapanlar vardır [8]. Bazı çalışmalarda kodlanacak bilgiye göre bazı kelimeler için kısaltma kullanarak damgalama yapılmıştır [9]. Kelimelerin arasına veya paragraf sonlarına konan fazladan boşluk karakterlerine bilgi saklayarak damgalama yapan çalışmalar mevcuttur [9][10]. Bu tip çalışmalar, fazladan boşlukları otomatik kaldıran kelime işlemcilere karşı dayanıksızdır. Damga bir anda ortadan kalkabilir. Bir takım uygulamalarda bazı kelimelerin yerine eşanlamlıları kullanılarak damgalama yapılmaya çalışılmaktadır [11], [12] . Eşanlamlı yöntemi her ne kadar zor ve bilgi saplama kapasitesi sınırlı bir yöntem olsa da ekstra boşluk veya sağa sola metni kaydırma gibi kolay ortadan kaldırılabilecek bir damga çeşidi değildir. Shirali M. bazı kelimelerin Amerika Birleşik Devletleri (ABD) ve Birleşik Krallık (UK) yazılışlarının farklı olmalarını kullanarak metin içerisine bilgi saklamışlardır [13]. Eşanlamlı yöntemi tespiti güç ve kelime işlemcilerin otomatik yaptığı işlemlere göre (fazladan boşlukları kaldırmak gibi) dayanıklı olsa da uygulanabilmesi için İngilizce metin olması ve nispeten uzun bir ana dosya gerektirmesi nedeniyle ancak kısıtlı bir kullanım alanı olabilecektir. Ayrıca kelimeler için dosyanın belli bölümlerinde ABD, belli bölümlerinde Birleşik Krallık (UK) yazılışlarının kullanılması dikkat çekebilecektir.

Tablo 2-1 ABD ve UK yazılışları farklı bazı kelimeler

ABD yazılışı	**UK yazılışı**
Favorite	Favourite
Criticize	Criticise
Fulfill	Fulfil
Center	Centre

Fujitsu firması ürün resimlerine ürün ile ilgili bilgi ihtiva eden bilginin indeksini tutan Ian kod veya QR kod damgalamış, cep telefonlarına indirilebilen bir uygulama ile ürünün resmi telefon ile görüntülendiğinde resimdeki damgalanmış kod çıkarılmış, internet üzerinden veri tabanına bağlanılarak ve ürün indeksi kullanılarak bilgi ekrana getirilmiştir [14]. Sistemin genel işleyişi Şekil 2.1'de görülmektedir.

Şekil 2.1. Fujitsu firmasının ürün bilgilerini meta veri damgalama yöntemiyle saklaması

Tezin çalışma konusu özellikle resim damgalama ile olduğundan tezin bundan sonraki kısmında dijital damgalamanın resim damgalama ile ilgili bölümü üzerinde çalışılacaktır.

Resim damgalamanın ilk örnekleri piksel uzayında 1990'lı yıllarda verilmeye başlanmıştır. 1994 yılında Tirkel ve arkadaşları gri seviyeli bir resmin en değersiz bitlerine (LSB) damgalama yaparak doğrulama, sahipliği ispat ve resim hakkında bilgileri resim içine saklama (tagging) amaçlı resim damgalama yapmışlardır[15].Tipik bir gri seviyeli resimde, her piksel için 8 bitlik bir değer tutulmaktadır(0-255 arası). En önemsiz bitler değiştiğinde resimdeki değişiklik fark edilmeyecek kadar küçük olmaktadır.

En önemsiz bitlerle yapılan damgalama basit olarak aşağıdaki formülle yapılır (en önemsiz 2 bitin kullanıldığı varsayılmıştır). Eş.1.1.'de orijinal resim 4'e bölünüp 4 ile çarpılırken aslında en önemsiz 2 biti sıfırlanmış olmaktadır. *w / 64* kısmında ise gri seviyeli damga resminin en önemli 2 bitinin en önemsiz 2 bite kaydırılması ile ve sonraki toplama işlemi ile damga resminin en önemli 2 bitinin ana resmin en önemsiz 2 bitine yerleştirilmesi sağlanmış olmaktadır.

$$f_w = 4(f / 4) + w / 64 \quad (1.1)$$

f: orijinal resim

w: gri tonlu damga resmi

f_w : damgalı resim

Damganın geri çıkartılması ise aşağıdaki yöntemle yapılır:

En önemli 6 biti sıfırla

Kalan bitlerdeki değeri tüm gri seviye değer aralığına (0-255) genişlet

Dorairangaswamy ve Padhmavathi piksel uzayını kullanarak, siyah beyaz bir damga resminin her bir bit değerini ana resimden 4 piksele damgalayarak ana resmin sahipliğini ispatlar [16].

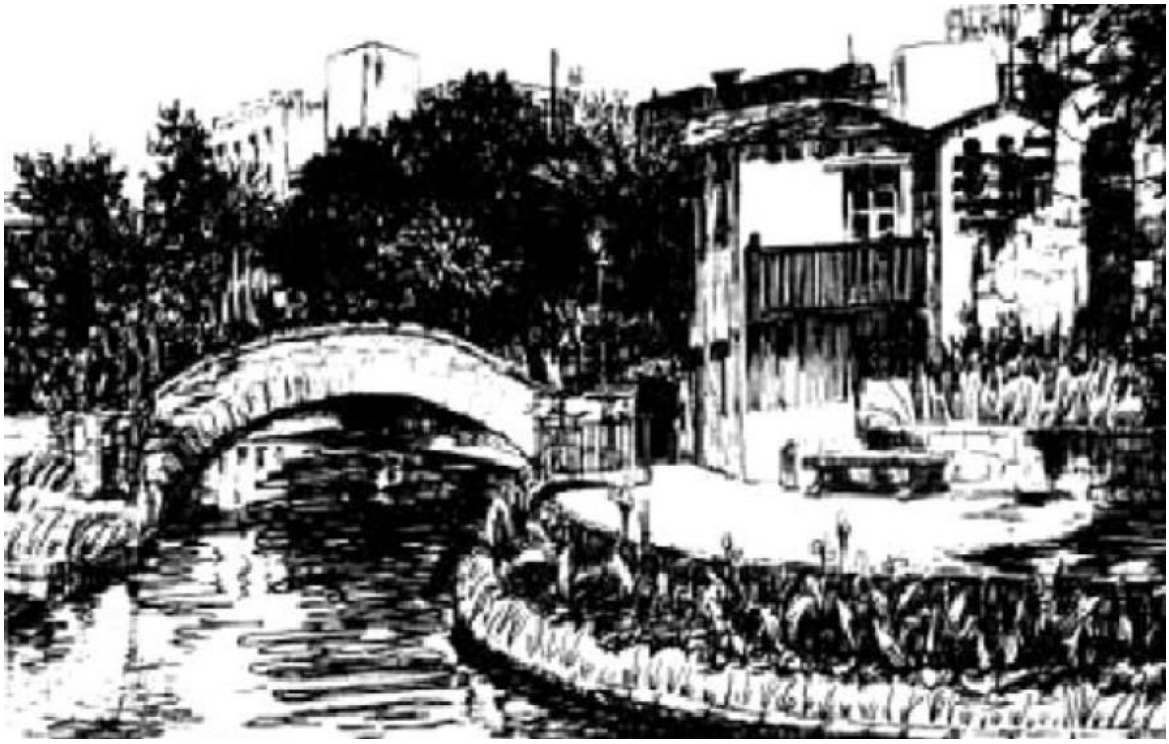
Piksel uzayındaki damgalama en önemsiz bitlerin sıfırlanması ile kolaylıkla ortadan kaldırılabilmektedir. Başkasının dijital resim çalışmasını alan biri en önemsiz bitlerin tamamına 0 veya 1 veya sözde rastgele bit dizisi (SRBD) koyduğunda damga ortadan kalkacak, çalışmanın asıl sahibi sahipliğini ispatlayamaz duruma düşecektir. Bu nedenle zamanla yeni teknikler ortaya çıkmıştır.

Resmi piksel uzayından farklı bir uzaya alma, resmi alınan yeni uzayda damgalama, daha sonra resmi tekrar piksel uzayına döndürme yaklaşımı daha sonra ağırlık kazanmıştır.

2.1 Damgalama, Steganografi ve Kriptografi

Dijital damgalamanın bilgi gizleme (steganografi) ile benzeşen ve ayrışan yönleri vardır. Steganografi, fark edilmeyecek şekilde genelde karşı tarafa bilgi iletmek için yine bir ana ortama bilgi gizleme işlemidir. Tarihte bilinen kayıtlı ilk steganografi uygulaması tarihçi Herodot'un "Tarihçeler" kitabında anlatılmaktadır[17]. Histiæus'un Miletus Kralı Aristagoras'a gizli bir mesaj iletmek için kölesinin saçlarını kazıtarak mesajı kölenin kafasına dövme yaptırdığını, kölenin saçları uzamış olarak Aristagoras'a ulaştığını, ulaşmasını müteakip saçların tekrar kazınarak mesajın okunduğunu anlatır. 1945'de Şekil 2.2'deki resim içerisine mors alfabesi kullanılarak bilgi gizlenmiştir [14]. Gizli bilgi derenin kenarındaki çayır resimlerine gömülmüştür. Uzun çayır çizgiyi, kısa çayır noktayı temsil etmekte idi. Mesajda ‘‘Compliments of CPSA MA to our chief Col Harold R.

Shaw on his visit to San Antonio May 11th 1945'' yani CPSA MA şefimiz Albay Harold R.Shaw'a 11 Mayıs 1945 deki ziyaretlerinden dolayı övgülerini sunar yazmaktadır. Gizli mürekkeple yazı yazma da bir nevi steganografi olarak değerlendirilebilir.



Şekil 2.2. 2nci Dünya Savaşında 1945'te kullanılmış ve mors alfabesi ile içine mesaj gizlenmiş resim

Steganografi kötü amaçlı olarak da kullanılabilmektedir. 11 Eylül saldırıları sonrasında El Kaide terör örgütünün dünya ticaret merkezine yaptığı saldırılarını steganografi teknikleri kullanarak koordine ettiği iddia edilmiş, ancak milyonlarca resim incelenmesine rağmen bu yönde ciddi bir veriye ulaşılamamıştır [18]. Çocuk pornografisinin ve uyuşturucu trafiğinin iletişimi için steganografi teknikleri kullanıldığı yönünde de ciddi duyumlar bulunmaktadır [18].

Steganografide iletişim bir noktadan karşı noktaya düşünülürken, damgalamada damgalanan içeriğin birçok kişiye ulaşması hedeflenir. Damgalanmış bir resmin bir örün(web) sitesinde yayımlanması gibi. Steganografide karşı tarafa gönderilen mesajdan sadece gönderen ve alanın bilgisi olduğu düşünüldüğünden, mesajın ortadan kaldırılmasına yönelik bir değişiklik beklenmez. Bu durumda steganografide, değişikliklere karşı dayanıklılıktan söz edilmez. Ancak dijital

damgalamada örneğin örün sitesine konan bir damgalı resmin, değişikliklere karşı dayanıklı olması beklenir. Örün sitesinde bulunan damgalı resmi birileri alıp, resmin kalitesinde çok bozulma olmadan değişiklik yaparak damgayı ortadan kaldırabiliyorsa, örün sitesi sahibi resmi izinsiz kullanan kişiye karşı sahiplik iddia edemeyecektir. Özellikle sahipliğin ispatlanması amacıyla yapılan damgalama işlemlerinde, damgalı resmin standart resim değişikliklerine karşı dayanıklı olması beklenir. Steganografide ana dosya içerisine gizlenen mesaj, genelde ana dosya ile ilintili değildir. Örneğin bir mektubun paragraflarının ilk harflerini birleştirince bir sonraki saldırının hangi şehirden yapılacağı ile ilgili bir mesajın, içinde saklandığı mektup içeriğiyle bir ilgisi bulunmayabilir. Dijital damgalamada ise dosya içerisine konulan damga, dosyanın kendisinin sahipliğini ispatlamada kullanılmakta, aralarında bir ilişki bulunmaktadır. Steganografi ve damgalama karşılaştırması Tablo 2-2 de görülmektedir.

Tablo 2-2. Steganografi ve Damgalama karşılaştırma tablosu

Bakış Açısı	**Steganografi**	**Dijital Damgalama**
İletişim cinsi	Noktadan noktaya	Bir noktadan çok noktaya
Mesajın varlığının Duyurulması	Gizli mesaj olduğu bilakis gizlenir	Gizli mesajın (damga) varlığı çoğunlukla duyurulur, korsan kullanıma karşı caydırıcılık hedeflenir
Değişikliklere Karşı Dayanıklılık	Geçerli değildir (Dayanıklılık aranmaz)	Sahipliğin ispatı amaçlanıyorsa dayanıklılık istenir, gerekir
Mesajın ana ortam ile ilişkisi	Bir ilişki aranmaz. Ana taşıyıcı ortamn tek görevi gizli mesajı saklamaktır.	Damga, yerleştirildiği ana ortam ile ilişkilidir. Örneğin bir resim dosyasının içinde sahibinin firma logosu vardır. Logo, bizzat içinde bulunduğu resmin sahipliğini sağlar.

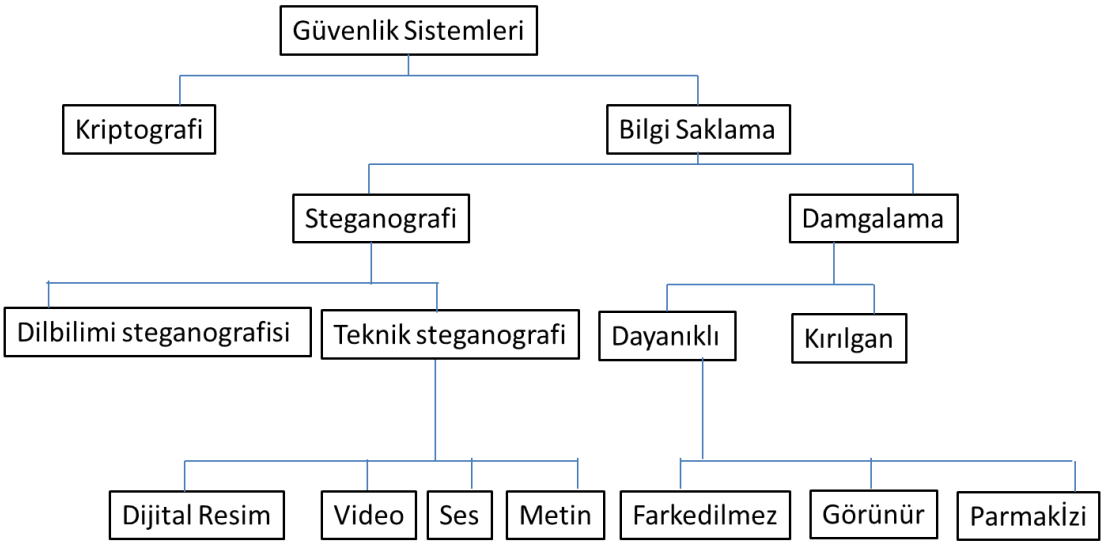
Damgalama işlemi, şifreleme (kriptografi) ile de karşılaştırılabilir. Steganografide karşı tarafa mesaj gönderirken, ana bilgi içerisinde gizli bir mesaj olduğu bilgisi saklanarak güvenlik sağlanırken, kriptografide bilgi şifrelenerek karşı tarafa gönderilir ve bilginin şifreli olduğu üçüncü şahıslarca da bilinir. Kriptografide bilgi karşı tarafa ulaşıp şifresi çözüldükten sonra bilgi tamamen kopyalama ve izinsiz kullanıma karşı korumasız hale gelir. Damgalı bir dosyada ise damga dayanıklı bir şekilde hazırlanmışsa damga her zaman dosya ile beraber kalmaya devam ederek, izinsiz bir kullanımda sahipliği ispatlayabilecektir. Şifrelenmiş bir çalışma şifresi çözülmediği sürece kimsenin işine yaramayacaktır ancak damgalı bir

çalışma damgalı haliyle de işe yarayabilir, kullanılabilir. Damgalı çalışmayı izinsiz kullananlar, kullandıkları izinsiz kopyadan damganın çıkarılması durumunda yasal olarak sorumlu olacaklardır. Kriptografi ve damgalama işlemleri Tablo 2-3 de karşılaştırılmıştır.

Tablo 2-3. Kriptografi ve Damgalama Karşılaştırma Tablosu

Bakış Açısı	**Kriptografi**	**Dijital Damgalama**
İzinsiz Kullanım	Şifre çözülmediği sürece şifreli dosya hiçbir işe yaramaz	Damgalı da olsa dosyada kalite kaybı olmayacağından damgalı dosya kullanılabilir
Güvenlik	Şifre çözüldükten sonra çalışma tamamen korumasız kalır	Damga daima çalışmanın bir parçası olarak kalmaya devam eder.

Cheddad v.d. kriptografi, steganografi ve damgalamayı Şekil 2.3'de görüldüğü gibi ilişkilendirmiş ve kategorize etmişlerdir [14]. Steganografi ve damgalama bilgi saklama kategorisi altına alınmıştır.



Şekil 2.3. Cheddad v.d. nin Güvenlik Sistemleri Taksonomisi

2.2 Damgalamanın Kullanım Alanları

Dijital damgalama değişik amaçlarla kullanılmaktadır. Bu bölümde her kullanım alanının genel olarak damgalama olmadan nasıl yapılmaya çalışıldığı ve damgalama ile birlikte nasıl bir yöntem değişimine uğradığı alt başlıklar halinde gösterilmektedir.

2.2.1 Sahipliğin İspatı, telif haklarının korunması

2.2.1.1 İlgili Mevzuat

Türkiye'de telif hakları 5846 sayılı fikir ve sanat eserleri kanunu ile korunmaktadır. "Fikir ve sanat eserleri üzerindeki haklar eserin üretilmesiyle birlikte doğar. Telif hakkının doğması için tescile gerek yoktur." [19]. 5846 sayılı kanunun eser sahipliğiyle ilgili 11 nci maddesi önemlidir ve aşağıda verilmiştir. Her ne kadar bir eseri üreten kişi veya kurum o eseri tescil ettirmek zorunda olmasa ve doğal sahibi olsa bile tereddüte mahal bırakmamak isterse noter aracılığı veya Kültür ve Turizm Bakanlığına başvurarak eseri tescil ettirebilmektedir. Müzik eseri içeren yerli ve ithal yapımlar, sinema eseri içeren yerli ve ithal yapımlar, yerli ve ithal bilgisayar oyunları için tescil işlemi yaptırmak zorunludur.

> *"**Madde 11 –** Yayımlanmış eser nüshalarında veya bir güzel sanat eserinin aslında, o eserin sahibi olarak adını veya bunun yerine tanınmış müstear adını kullanan kimse, aksi sabit oluncaya kadar o eserin sahibi sayılır."*

5846 sayılı kanuna 1995 yılında **4110/5 maddesi ile "**Umumi yerlerde veya radyo-televizyon aracılığı ile verilen konferans ve temsillerde, mutat şekilde eser sahibi olarak tanıtılan kimse o eserin sahibi sayılır" değişikliği getirilmiş, ancak madde 11'in önceliği olduğu belirtilmiştir.

Bir eserden elde edilecek kopyalarla ilgili, kanunun aşağıdaki maddesi de önemlidir.

> ***"Madde 15 –**Bir güzel sanat eserinden çoğaltma ile elde edilen kopyelerle bir işlenmenin aslı veya çoğaltılmış nüshaları üzerinde asıl eser sahibinin ad veya alametinin, kararlaştırılan veya adet olan şekilde belirtilmesi ve vücuda getirilen eserin bir kopye veya işlenme olduğunun açıkça gösterilmesi şarttır."*

2004 yılı tarihli 5101 nolu kanunun 24ncü maddesiyle 5846 sayılı Kanunun 81 inci maddesi aşağıdaki şekilde değiştirilmiştir. Madde bahsedilen bandroller, çıkarılmak istendiğinde yırtılan, üzerinde holografik resim barındıran özel etiketlerdir.

> *"**Madde 81. -** Musiki ve sinema eserlerinin çoğaltılmış nüshaları ile süreli olmayan yayınlara bandrol yapıştırılması zorunludur. Ayrıca, kolay kopyalanmaya müsait diğer eserlerin çoğaltılmış nüshalarına da eser veya hak sahibinin talebi üzerine bandrol yapıştırılması zorunludur. Bandroller, Bakanlıkça bastırılır ve satılır."*

Hukukla ilgili hususlar konunun uzmanlarına bırakılarak bu kadarla iktifa edilmektedir.

2.2.1.2 Sahipliğin İspatının Damgalama ile Yapılması

Dijital ortamdaki varlıklar ortaya çıkalı beri insanlar bu varlıklarını korsan kullanım elinden korumak için yöntemler geliştirmişlerdir. Resimlerin üzerine Şekil 1.5'de olduğu gibi görünür © işaretleri ve sahibini gösterecek logo veya metin konarak sahiplik korunmaya çalışılmıştır. Kısmi bir işlev yerine getirse de görünür damgaların ortadan kaldırılması mümkündür ve çoğunlukla basit bir şekilde yapılabilmektedir. Tape şeklindeki ses/müzik barındıran bantlarda veya CD-DVD lerin üzerinde telif hakları ile ilgili etiketler bu amaçla konulmuştur.

Şekil 2.4 ve Şekil 2.5'de örnekleri görülmektedir. Bu örneklerde görüleceği üzere ilgili etiketler ambalajın veya medyanın içindeki ürünün telif haklarını korumaktan ziyade kullanıcıya veya ürünü eline alan kişiye telif haklarını hatırlatmaktadır. Korsan kullanıma karşı sadece bu etiketler kullanıldığında, kolaylıkla ürünün bir kopyası elde edilip kullanılabilecek, ancak ürün bizzat kopyalanırken yakalanırsa veya bandrolsüz ürün satılırken suçüstü yapılması durumunda yasal işlem yapılabilecektir. Ürünün sahipliğini ispatlayacak kısmının, asıl üründen bu kadar kolay ayrılabilmesi problem teşkil etmektedir.

Şekil 2.4. Tape üzerine yerleştirilmiş bandrol

Şekil 2.5. CD kabı üzerine yerleştirilmiş bandrol

Bir ürünün birine ait olduğunu göstermek o ürünün o kişiye ait olduğunu ispatlamak anlamına gelmemektedir. Bir resmin üzerine yerleştirilmiş görünür © işareti ve firma ismi görüntü işleme programları vasıtası ile kaldırılıp yerine korsan kişinin kendi firma adı kolaylıkla konabilir. Ürünlere tescil kaydı akla gelebilir ancak bu işlem de hem bir süreç gerektirdiği, hem de çoğunlukla maddi külfet getirmesi nedeniyle tercih edilmemektedir.

Dijital damgalama, etiket, denetim pulu (bandrol), telif hakkı © işareti gibi temel konvansiyonel araçların dijital ortamdaki değerler için sahipliği kalıcı olarak ispatlayamaması nedeniyle bir disiplin olarak ortaya çıkmıştır. Korunmak istenen dosya damgalandıktan sonra damga, dosyanın kullanım ömrü boyunca o dosyanın ayrılmaz bir parçası olur ve sadece yerleştiren veya yetki verilen kişi damgayı geri çıkarabilir. Alev(Eve) Halise'nin kendi damgası ile damgaladığı damgalı resimden Halise'nin damgasını çıkartamaz çünkü damga görünür değildir, damgalama algoritması ve damgalama anahtarı elinde değildir. Alev, Halise'nin çalışmasının kendi çalışması olduğunu iddia ettiğinde ve olay mahkemeye taşındığında Halise, Alev'in elindeki kendi damgasını taşıyan dosyadan damga çıkarma algoritmasını kullanarak kendi damgasını çıkartabildiğinde, dosyanın kendi çalışması olduğunu ispatlamış olacaktır.

2.2.2 Reklam Yayını Takibi

Damgalama reklam takibi amacıyla da yapılabilir. Bir yayıncı kuruluş ile reklamlarının yayımlanması için anlaşan ticari bir firma, reklamlarının kendisine

taahhüt edilen tarihlerde, tekrar sayısınca ve süresince yayımlandığını takip etmek için 3 yolu olabilir [20].

1. Ekran başına bir kişiyi oturtup manuel olarak reklam başlangıç ve bitişlerinin kaydını tutturmak
2. Reklam yayınını birebir eşleştirme ile tespit etmeye çalışmak
    a. Reklam yayınının başına ve sonuna fark edilmeyecek özel kareler ekleyerek, reklamın başına ayrı ve bitişine ayrı kareler koyarak işaretlenir
    b. Bir TV kartı vasıtası ile yayın ekran yakalama programı ile kaydedilir veya anlık olarak yakalanır
    c. Yayın karesi reklamın başlangıç karesi veya bitiş karesi ile karşılaştırılır. Eğer bir eşitlik veya uyuşma tespit edilirse başlangıç veya bitiş hangisi ise zamanı kaydedilir
3. Reklam yayınını damgalama ile takip etmek
    a. Reklam yayınına damga yerleştirilir
    b. Bir TV kartı vasıtası ile yayın ekran yakalama programı ile kaydedilir veya anlık olarak yakalanır
    c. Yayın karelerinde damga tespit edildiği sürece veri tabanına veya dosyaya zaman kaydı düşülür.

Zorunlu olmadıkça birinci yol olan manuel takibi kimse tercih etmek istemeyecektir. İkinci yolda reklam filmi içeriğinin en azından başlangıç ve bitiş karelerinin birebir karşılaştırılması söz konusudur. İkinci alternatifin dezavantajı, yayıncı kuruluşun algoritmadaki açığı fark edip, kendi yayınına reklamın başlangıç kısmı ve bitiş kısmı karelerinden serpiştirmesi ve müşteriden aldığı para karşılığı olan reklamı yayımlamadığı halde reklam takip programını yanıltabilmesidir. Reklam yayımlanmadığı halde reklamın sahibi ticari firma aldatılmış olacaktır. İkinci yolda reklamın başlangıç veya bitişi değil de tüm reklam içeriğinin karşılaştırılması yapılabilir ancak bu durumda karşılaştırılacak veri çok büyük olacağından sağlıklı bir netice çıkması güç olacaktır. Reklam yayını kısa olsa bile video içeriğinin çakıştırılıp karşılaştırılması, özellikle kaymalar ve gürültü düşünüldüğünde ve veri büyüklüğü hesaba katıldığında zor bir işlemdir. Son seçenek olan damgalama yolu ile reklam takibi ise mantıklı bir çözümdür. Veri karşılaştırılması yerine karelerden çıkarılan damga referans damga ile karşılaştırılacağından çok daha küçük bir veri

karşılaştırılması söz konusu olacaktır. Ayrıca damgalama yöntemlerinde ileride değinileceği gibi gürültü veya resmin sağa sola kayması gidi durumlarda da damga geri çıkartılabilmektedir.

2.2.3 Parmak İzi takibi:

İngiltere Başbakanı Margaret Thatcher'ın 1981 yılında, bakanlar kurulundan dışarı bilgi sızdıran kişiyi ortaya çıkarmak için aynı metni farklı sayıda boşluk karakterleri kullanarak, görünürde aynı ancak boşluk pozisyonu ve sayısı birbirinden farklı olan metinleri kişilere vermek sureti ile metin dosya damgalama örneği sergilediği iddia edilmektedir [21]. Metin dosyaları damgalanırken genelde kelimeler arasındaki boşluk karakterlerinin sayısı ve pozisyonu kullanılarak bilgi saklama ve damgalama yapılır[2],[3],[24]. Margaret Thatcher'ın yaptığı bu uygulama aynı zamanda parmak izi takibi türünde bilgi sızmasının kimden olduğunu bulma yönünde bir damgalama tekniğidir.

Evrak güvenliğinin önemli olduğu kurumlarda evraktan alınan her çıktıya ayrı bir numara filigran olarak konur ve çıktı o şekilde alınır. Şekil 2.6'de filigranlı alınmış bir evrak görülmektedir. Evrakın gizli olması ve dışarı sızması durumunda, hangi numaralı filigranın kime teslim edildiğinin sağlıklı tutulması kaydıyla, evrakın hangi personelin kopyasından sızdığı tespit edilebilecektir.

Dijital damgalama dijital verilerin izini takip etmek için kullanılabilecek iyi bir çözümdür. Bir film yapımcısı gösterime girmemiş bir filmini belli sayıda film eleştirmenine geri besleme almak için gönderdiğinde her kopyayı farklı bir damga ile damgalar. Her film yapımcısı farklı damgalı bir film kopyası almış olur. Film eleştirmeni, kötü niyetli olarak filmin İnternet'ten indirilebilmesini sağlayacak şekilde bir sunucuya koyarsa veya konmasını sağlarsa, internetten indirilebilen kopyada kimin damgası çıkartılabiliyorsa onun tarafından suistimal yapıldığı anlaşılacak ve adli işlem başlatılabilecektir. Film DVD'leri için üretilen her kopya için ayrı damga damgalanır ve kime satıldığının takibi seri numarası ile takip edilebilirse, internete düşen yasal olmayan kopyaların kimin kopyasından dağıtıldığı meydana çıkarılabilecektir.

MADDE 2.–26.5.1981 tarihli ve 2464 sayılı Belediye Gelirleri Kanununun 21 inci maddesinin son fıkrası aşağıdaki şekilde değiştirilmiştir.¶

(I) numaralı bendin (1) ve (2) numaralı alt bentleri ile yerli ve yabancı film gösterimlerine ilişkin belirlenen vergi bu Kanunun 22 nci maddesinin (1) numaralı bendinde öngörüldüğü şekilde hesaplanarak her ayın onbeşinci günü akşamına kadar mahallin mal müdürlüğüne veya muhasebe müdürlüğüne emaneten yatırılır. Ödemenin yapıldığına dair banka dekontunun ibrazı üzerine belediye tarafından biletlere özel damga konulur. Ödeme yapmayanlar hakkında 6183 sayılı Amme Alacaklarının Tahsil Usulü Hakkında Kanun hükümleri uygulanır. Bahsi geçen yerlerde toplanan meblağın %75'i Kültür ve Turizm Bakanlığı Merkez Saymanlık hesabına, %25'i ilgili belediyeye tahsilini takip eden ayın onbeşinci günü akşamına kadar aktarılır.¶

MADDE 3.–26.5.1981 tarihli ve 2464 sayılı Belediye Gelirleri Kanununun 52 nci maddesine aşağıdaki fıkra eklenmiştir.¶

5846 sayılı Fikir ve Sanat Eserleri Kanunu kapsamında korunan eser, icra ve yapımların tespit edildiği kitap, kaset, CD, VCD ve DVD gibi taşıyıcı materyallerin birinci fıkrada bahsi geçen yerlerde satışına izin verilmez.¶

MADDE 4.–13.4.1994 tarihli ve 3984 sayılı Radyo ve Televizyonların Kuruluş ve Yayınları Hakkında Kanunun 3 üncü maddesinin (v) bendi aşağıdaki şekilde değiştirilmiştir.¶

v) Eser ve/veya bağlantılı hak sahipleri: Eser, icra, fonogram ve yapımlar üzerindeki manevî ve malî hakları, 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile düzenlenen gerçek veya tüzel kişileri,¶

MADDE 5.–3984 sayılı Kanunun 4 üncü maddesinin ikinci fıkrasının (o) bendi aşağıdaki şekilde değiştirilmiştir.¶

o) Yayınlarda, eser ve bağlantılı hak sahiplerine 5846 sayılı Fikir ve Sanat Eserleri Kanunu ile tanınan hakların ihlâl edilmemesi.¶

MADDE 6.–3984 sayılı Kanunun 37 nci maddesi başlığı ile birlikte aşağıdaki şekilde değiştirilmiştir.¶

Radyo-Televizyon Kuruluşlarınca Yayınlanan ve/veya İletilen Eser, Icra, Fonogram ve Yapımların Kullanımına İlişkin Esaslar¶

Madde 37.–Radyo-televizyon kuruluşları, yayın ve/veya iletimlerinde eser, icra, fonogram ve yapımları kullanabilmek için, eser sahipleri, bağlantılı hak sahipleri veya bu kişilerin üyesi oldukları meslek birlikleri ile izin almak üzere sözleşme yaparlar ve bu sözleşme ile belirlenen malî hak bedellerini öderler. Bu sözleşme ve ödemeler, 5846 sayılı Fikir ve Sanat Eserleri Kanununun ilgili hükümleri çerçevesinde yapılır. Bu madde hükümlerini ihlâl eden yayın kuruluşları hakkında ayrıca bu Kanunun 33 üncü madde hükümleri uygulanır.¶

MADDE 7.–23.1.1986 tarihli ve 3257 sayılı Sinema, Video ve Müzik Eserleri Kanununun 6 ncı maddesinin son fıkrasının birinci ve ikinci cümleleri aşağıdaki şekilde değiştirilmiştir.¶

Şekil 2.6. Filigranlı çıktı alınmış bir evrak

2.2.4 Doğruluğunu Kanıtlama

İnsanlar bir şeyin orijinal olduğunu, sahte olmadığını, değiştirilmediğini anlamak için değişik teknikler geliştirmişlerdir. Paralardaki belli resimlerin sadece özel durumlarda (güneşe tutulduğunda) görünmesi ve paranın gerçek olduğunu (orijinal) ispatlamada kullanılması fiziksel bir damgalama örneği sayılabilir(Bakınız Şekil 2.7). Pek çok ürünün ambalajında görünmez boya ile yazılan yazılar veya logolar vardır. Evrakların üzerine konulan filigranlar da iz takibi maksatlı olduğu gibi doğrulama maksatlı da kullanılabilir.

Şekil 2.7. Filigranlı 50 lira

Görüntü işleme programları sayesinde resimlerde fark edilemeyecek değişiklikler yapılabilmektedir. Şekil 2.8'da solda orijinal resimde kapı kolunu açmaya çalışan bir kişi varken sağdaki resimde bu kişinin görüntü işleme programı ile kaldırıldığını görüyoruz. Adli vakalarda, askeri ve medikal uygulamalarda bir dosyanın orijinali ile aynı olduğu çok önemli olabilir. Havadan gönderilen uydu verisinin havada birileri tarafından yakalanarak değiştirilmediğinden emin olmak gerekir.

a. Orijinal Resim

b. Üzerinde Oynanmış Resim

Şekil 2.8. Orijinal ve Değiştirilmiş Resimler

Bir dijital dosyanın orijinali ile aynı olduğunu sağlamak için damgalama yöntemlerinden önce kriptografiden yararlanılmakta idi. Dosyanın dijital özeti gizli bir anahtar ile çıkarılıyor, dosyaya ilave olarak karşı tarafa gönderiliyordu. Karşı taraf dosyayı ve özeti aldıktan sonra aynı gizli anahtarla dosyadan özet çıkarıyor, kendisine gelen özet ile karşılaştırıyor, iki özet aynı ise dosyanın değiştirilmemiş olduğuna hükmediyordu.

Doğrulama amaçlı kriptografik özet kullanımında dosya özeti hesaplanırken gerek duyulan anahtarın değişebilmesi, dosya ile beraber dosya özetinin de iletilmek zorunda kalınması işletim zorluğu getirmekte idi. Bu dezavantajlara sahip olmayan damgalama doğrulama amaçlı da kullanılmaya başlanmıştır. Kriptografik özet yönteminde, doğrulanması hedeflenen dosyanın iletim ortamındaki gürültüye hiç toleransı yoktur. İletilen dosyanın bir biti bile değişse bambaşka bir özet çıkacak, doğrulama özeti ile aynı olmadığından dosya *orijinal değil* olarak değerlendirilecektir. İlerde anlatılacağı üzere damgalama yoluyla doğrulamada belli bir esneklik söz konusu olabilmektedir.

Doğrulama amaçlı damgalama, kriptografik özet yönteminin dezavantajlarını gidermek üzere geliştirilmiştir. Doğrulama bilgisi doğrudan dosyanın içerisine damgalandığından özet dosyasını göndermek gerekmeyecek, alınan dosyadan çıkartılan özet ile karşıdan gönderilen özeti eşleştirmek gibi sorunlar olmayacaktır. Ayrıca damgalama yönteminin kriptografik özet yöntemine göre bir avantajı da, dosyanın bloklara bölünüp blokların ayrı ayrı damgalanması suretiyle dosyanın neresinde değişiklik yapıldığının tespit edilebilmesidir.

Doğrulama amaçlı damgalamada ideal hedef doğrulama damgasının masum olan basit resim operasyonlarını (kayıplı resim sıkıştırma, başka resim formatına dönüştürme v.b.) "resim değişikliğe uğradı" diye algılamayıp, resimdeki bir araç plaka numarası veya bir kişinin yüzünün değişmesi gibi kötü niyetli değişiklikleri tespit etmesidir. Bu çeşit doğrulama damgalaması yapmak zordur. Doğrulama amaçlı damgalama bölüm 3.3'te daha detaylı açıklanacaktır.

2.2.5 Meta Veri Saklama

Internet'te resim arama yapıldığında girilen anahtar kelimelere göre kıstasları sağlayan resimler gelir. Gelen bu resimler, resimler hakkında veri tabanında kaydedilmiş bilgilere göre gelir. Arama motoru internet sitelerinden bu resimleri toparlayıp kaydederken resimlerin başlık (header) kısımlarında veri varsa bunları, dosya isimlerini, alındığı site bilgilerini, dosyanın tarih bilgilerini v.b. ne toparlayabilirse veri tabanına kaydeder.

Sadece arama motorları değil, fotoğraf ve resim hizmeti veren bir site, veri tabanındaki resimlerle ilgili bir sorgu yaptığında ilgili resimleri getirebilmesi için meta verileri sisteme kaydeder. Söz konusu meta verilerden bazıları: Fotoğrafın/resmin ne ile ilgili olduğu, gündüz mü gece mi çekildiği, hangi tarihte hangi coğrafi noktada çekildiği, kim tarafından çekildiği v.b.'dir.

Söz konusu meta verinin resmin içerisine damga olarak gömülüp resmin bir parçası olması ve resimle birlikte gitmesi sağlanabilir. Resimlerin başlıklarına meta veriyi saklamak ve geri almak damgalamadan daha kolay görünmektedir. Her ne kadar resimlerin başlık kısımları meta veri için daha uygun gibi görünse de, resim format değişikliklerinde meta veriler genelde kaybolmaktadır. Ayrıca herkesin nüfuz etmesi istenmeyen meta veriler damgalama yoluyla daha güvenli saklanmış olacaktır.

2.3 Damgalamada Kullanılan Dönüşüm Uzayları

Bu bölümde resim damgalamada resmin piksel uzayından dönüştürüldüğü, daha sonra piksel uzayına geri dönüştürüldüğü, en çok kullanılan dönüşüm uzayları genel hatları ile anlatılacaktır.

2.3.1 Ayrık Kosinüs Dönüşümü (Discrete Cosine Transform: DCT)

Resim sıkıştırmasında çok kullanılan bir dönüşümdür. 1..N değerleri arasında tanımlı bir f(j) fonksiyonunun DCT uzayına alınması Eş.1.2 ile gerçekleşir. F(j) değerleri DCT dönüşümü gerçekleştikten sonraki değerlerdir. DCT uzayından tekrar f(j) fonksiyonu Eş.1.3 ters işlemi ile gerçekleşir.

$$F(k) = \frac{2c(k)}{N}\sum_{j=0}^{N-1} f(j)cos\left[\frac{((2j+1))k\pi}{2N}\right],\ \text{k= 0,1, ….., N-1} \tag{1.2}$$

$$f(j) = \sum_{k=0}^{N-1} c(k)F(k)cos\left[\frac{(2j+1)k\pi}{2N}\right],\ \text{j= 0,1, ….., N-1} \tag{1.3}$$

$$k = 0\ için\ c(k) = \frac{1}{\sqrt{2}}$$

$$k = 1,2,\ldots.,N-1\ için\ c(k) = 1$$

2.3.2 Fourier Dönüşümü, Hızlı Fourier Dönüşümü (Fast Fourier Transform: FFT)

Piksel uzayındaki bir resmin kesikli fourier dönüşümü aşağıdaki Eş.1.4 ile hesaplanır. MxN boyutlarındaki bir resmin FFT dönüşüm uzayındaki karşılığı yine MxN boyutlarında olup *f(x,y)* değerleri resmin *(x,y)* noktasındaki piksel değerleridir [25]. *F(u,v)* değerlerine Fourier katsayıları da denir.

$$F(u,v) = \frac{1}{MN}\ \sum_{x=0}^{M-1}\ \ \sum_{y=0}^{N-1} f(x,y)\exp(\ -j2\pi(\frac{ux}{M} + \frac{vy}{N})\ ) \tag{1.4}$$

Fourier dönüşümü değerleri karmaşık sayılardır. Bu sayıların büyüklük ve faz açısı değerleri Eş.1.5 ve Eş.1.6 da belirtilmiştir.

$$|F(u,v)| = \sqrt{R^2(u,v) + I^2(u,v)} \tag{1.5}$$

$$\Phi(u,v) = tan^{-1}\left[\frac{I(u,v)}{R(u,v)}\right]$$

(1.6)

FFT'si elde bulunan bir resmin piksel uzayına geri alınması için Eş.1.7 uygulanır.

$$f(x,y) = \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v)\exp(j2\pi(\frac{ux}{M} + \frac{vy}{N}))$$

(1.7)

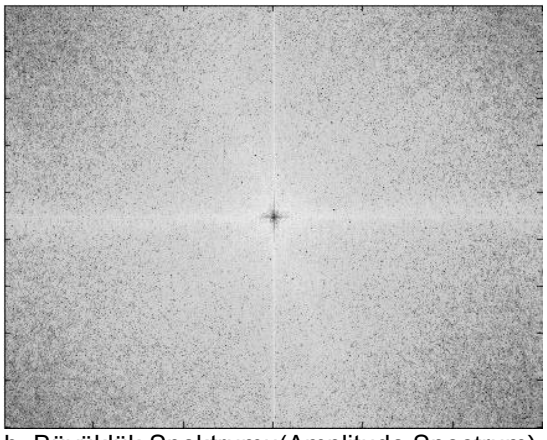
Fourier dönüşümünde, asıl resim kaydırılırsa (translation) fourier transform büyüklük değerleri değişmez, fazda bir kayma olur. Asıl resim döndürülürse Fourier spectrum'u da aynı açıyla döner, büyüklük değerleri aynı kalır. Asıl resim x,y eksenlerinde a,b çarpanları ile büyütülürse, Fourier katsayıları Eş.1.8'e göre değişir [26] .

$$\Im[f(ax,by)] = \frac{1}{ab}F(\frac{u}{a},\frac{v}{b})$$

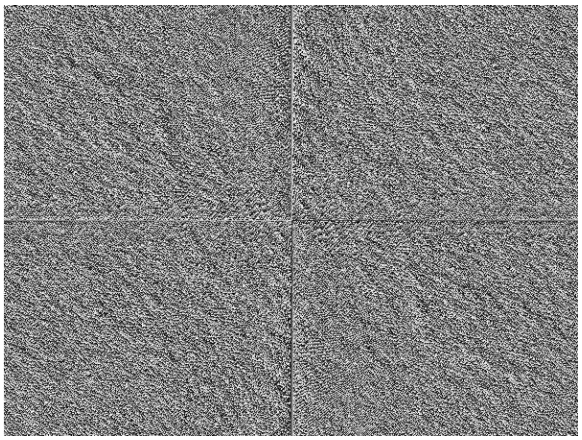
(1.8)

Şekil 2.9.a.'da ana resim, b.'de Fourier dönüşümü büyüklük değerleri spektrumu, c.'de faz spektrumu görülmektedir. Aynı resmin ç. karesinde Fourier dönüşümünün sadece büyüklük değerleri kullanılarak yapılan geri dönüşümden elde edilen resim görülmektedir. Fourier dönüşümünün sadece faz değerleri kullanılarak yapılan geri dönüşümden elde edilen resim d. karesinde görülmektedir. ç ve d kareleri incelendiğinde, resmin sadece büyüklük dönüşüm değerleri kullanıldığında ana resmi çağrıştıracak bir görüntü elde edilemeyip sadece faz dönüşüm değerleri kullanıldığında resmin siluetinin elde edilebildiği görülmektedir. Resmin ana çatısının faz dönüşüm değerlerince muhafaza edildiği gözlemlenmektedir.

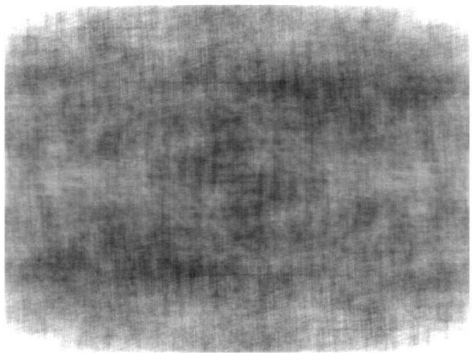
a. Ana Resim



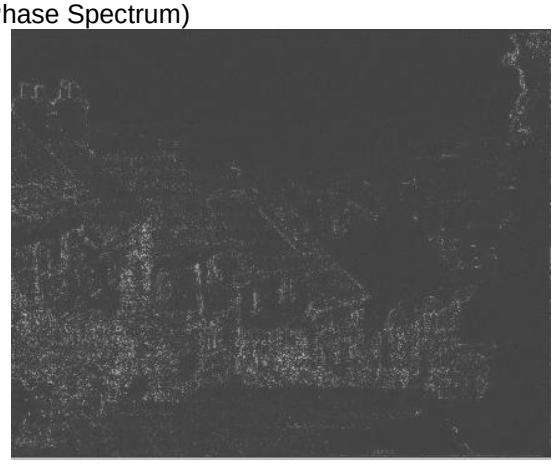
b. Büyüklük Spektrumu(Amplitude Spectrum)



c. Faz spektrumu (Phase Spectrum)



ç. Fourier dönüşümünün sadece büyüklük değerleri kullanılarak yapılan geri dönüşümden elde edilen resim



d. Fourier dönüşümünün sadece faz değerleri kullanılarak yapılan geri dönüşümden elde edilen resim

Şekil 2.9. Fourier Dönüşüm Özellikleri

2.3.3 Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform : DWT)

Fourier dönüşümünde temel fonksiyonlar sinüzoidler iken dalgacık dönüşümünde sınırlı süreli değişken frekanslı dalgacıklardır (wavelets) [25]. Dalgacık dönüşümü resmi farklı çönünürlüklerde inceleme ve üzerinde işlem yapma imkânı verir.

Dalgacık Dönüşümü Eş.1.11 ile belirtilirken ters dalgacık dönüşümü Eş.1.14 ile verilmiştir. ψ anne dalgacık olmak üzere;

$$\psi_{a,b(t)=\frac{1}{\sqrt{a}}}\,\psi\left(\frac{t-b}{a}\right),\ (t\ \in\ R)$$

(1.9)

$$\left\|\psi_{a,b}\right\| =\ \|\psi\|$$

(1.10)

f fonksiyonunun dalgacık dönüşümü olan F(a,b) dönüşümü:

$$F(a,b) = \left(f, \psi_{a,b}\right) = \frac{1}{\sqrt{a}} \int_{-\infty}^{\infty} f(t)\ \psi\left((t-b)/a\right) dt,\ (t\ \in\ R) \qquad (1.11)$$

$$\left(f, \psi_{a,b}\right) = \frac{1}{2\pi}\ (\hat{f},\ \hat{\psi}_{\ a,b}) \qquad (1.12)$$

$$\hat{\psi}_{a,b}\ (\omega) = \sqrt{a}\ e^{-i\omega b}\hat{\psi}(a\omega) \qquad (1.13)$$

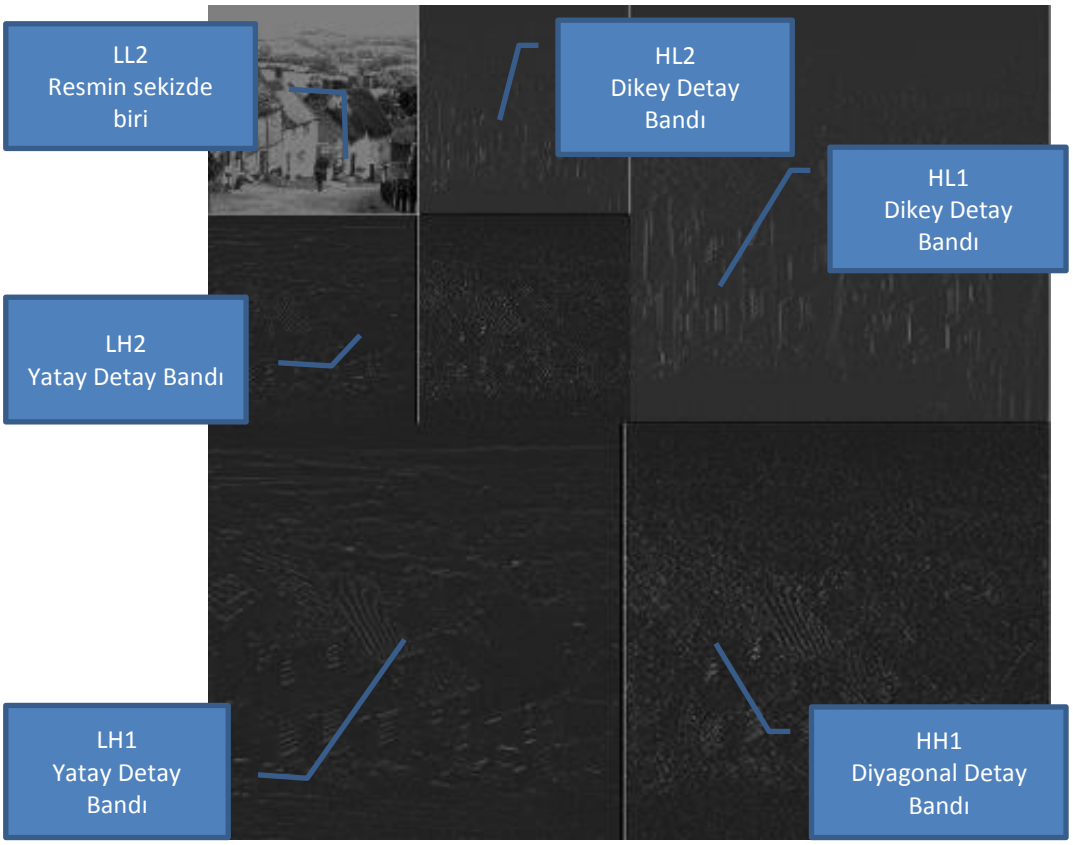
Ters Dalgacık Dönüşümü

$$f(t) = C_{\psi}^{-1} \int_{-\infty}^{\infty}\int_{0}^{\infty} \frac{1}{a^2} F(a,b)\ \psi_{a,b}\ (t) da\ db \qquad (1.14)$$

$$C_{\psi} = \int_{0}^{\infty} \frac{\left|\hat{\psi}\ (\omega)\right|^2}{\omega}\ d\omega \qquad (1.15)$$

$$\int_{-\infty}^{\infty} \psi\ (t)\ dt\ = 0 \qquad (1.16)$$

Ayrık dalgacık dönüşümünde resim, orijinal resmin dörtte biri olan dört bölüme ayrılır. Bu işlem birinci seviye ayrışmada gerçekleşir. Şekil 2.10'te görüldüğü üzere birinci seviye ayrışmalardan sol alttaki LH1 bandı yatay kenarları, sağ kenardaki HL1 bandı dikey kenarları, sağ alt köşedeki HH1 bandı diyagonal kenarları barındırır. Sol üstteki LL1 bandı ise normal resmin dörtte bir küçültülmüş halini muhafaza eder. LL1 bandı bir seviye daha ayrışmaya uğrayıp HL2, LH2, HH2 ve LL2 bantları oluşmuştur. LL2 bandı istense kendi kenar büyüklüğü piksel sayısı cinsinden dördün katı olmak kaydıyla birkaç defa daha ayrışmaya uğrayabilir. Ancak damgalamada genel olarak bir veya 2 seviye ayrışma yeterli kabul edilmektedir.



Şekil 2.10 Resmin 1 nci seviye ve 2 nci seviye DWT ayrışması

2.3.4 Tekil Değer Ayrışması (Singular Value Decomposition SVD)

Lineer cebirin konusu olan tekil değer ayrışmasında bir A matrisi üç matrisin çarpımı biçiminde ifade edilebilir.

$$A = U\,S\,V^{T} \qquad (1.17)$$

U ortogonal matris, S köşesel (diagonal) matris, V yine bir ortogonal matrisdir. V matrisinin transpose'u alınarak matris çarpımı gerçekleşmektedir. U, S ve V matrislerinin elemanları reel değerlerdir.

Eğer A k kenar uzunluğuna sahip bir kare matris ise, Eş.1.18 sağlanır. U'nun sütunları ve V'nin sütunları A'nın sol ve sağ tekil değer vektörleridir ve A'nın geometrik özelliklerini taşır. U'nun sütunları $U\ U^{T}$ nun ortonormal eigen vektörleridir. V'nin sütunları $A^{T}A$ nın ortonormal vektörleridir. S, U ve V'nin eigen değerleri karelerini küçükten büyüğe sıralı olarak ihtiva eden köşesel matrisdir. S'nin köşesel verilerine A'nın tekil değerleri denir ve A Eş.1.19'daki gibi de yazılabilir. u_i ve v_i U ve V'nin i'nci eigen vektörü, σ_i ise i'nci tekil değerdir. Eş.1.19' daki k değeri, A matrisinin rütbesidir.

$$U\,U^T = I_k, \qquad V\,V^T = I_k \tag{1.18}$$

$$A = \sum_{i=1}^{k} \sigma_i u_i {v_i}^T \tag{1.19}$$

SVD, aşağıdaki özelliklerinden dolayı damgalamada tercih edilmektedir [27]

- A matrisi ile α açı kadar döndürülmüş A_α matrisinin tekil değerleri aynıdır.
- A ve A^T aynı sıfır olmayan tekil değerlere sahiptir.
- A'nın iki satırı birbiri ile yer değiştirirse veya iki sütunu birbiri ile yer değiştirirse A'nın tekil değerleri değişmez
- A matrisi sıfır değerlere sahip (siyah) satırlarla ve sütunlarla genişletilirse, elde edilen A_g matrisi A ile aynı tekil değerlere sahip olur.

SVD tabanlı damgalamada genelde tekil değerlere damgalama yapılır [22],[27]–[32]. Az da olsa bazı SVD tabanlı damgalama çalışmalarında U ve V bölümlerine de damgalama yapılmıştır [33].

2.3.5 LU Ayrışması

Her bir kare A matrisi, Eş.1.20'de görüldüğü gibi L ve U matrislerinin çarpımı olarak ayrıştırılabilir. L matrisinde köşegen değerler 1, köşegen altındaki değerler çarpan değerleridir. U matrisinde ise köşegende ve üzerinde çarpan değerleri vardır. Eş.1.20'nin diğer bir yazılış şekli de Eş.1.21'dir.

$$A = L \times U = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & u_{12} & u_{13} \\ 0 & d_2 & u_{23} \\ 0 & 0 & d_3 \end{bmatrix} \tag{1.20}$$

$$A = L \times D \times U = \begin{bmatrix} 1 & 0 & 0 \\ l_{21} & 1 & 0 \\ l_{31} & l_{32} & 1 \end{bmatrix} \times \begin{bmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{bmatrix} \times \begin{bmatrix} 1 & {u_{12}}/{d_1} & {u_{13}}/{d_1} \\ 0 & 1 & {u_{23}}/{d_2} \\ 0 & 0 & 1 \end{bmatrix} \tag{1.21}$$

2.4 Frekans Uzayında Yapılan Çalışmalar

1997'de Cox, Kilian, Leighton, ve Shamoon geniş spektrum iletişimi yaklaşımı ile damgayı geniş bir frekans aralığına yayarak damgalama yapmışlardır[34]. Geniş spektrumlu iletim ortamı olarak damgayı barındıracak ana dosyayı, iletilen sinyal

olarak da damganın kendisini anlamışlardır. NxN büyüklüğündeki bir resim dosyasına damgalama yaparken, resmi önce kesikli kosinüs dönüşümüne (DCT) tabi tutmuşlar, damgayı DC komponenti hariç en önemli N dönüşüm değerine damgalamışlardır. Algoritma aşağıdaki şekildedir:

D: Damgalanacak resim

V: $v_1, v_2, \ldots, v_n$: D'nin içerisinde X damgasının damgalanacağı bir dizi değer

X Damgası (bir dizi reel sayı) ***:*** $x_1, x_2, \ldots, x_n$ where x_i değerleri ***N(0,1)'***e göre bağımsız olarak seçilmiştir***,*** ***(N(μ, σ²)*** , ***μ ortalaması σ²*** *varyansına sahip bir dağılımdır*.)

V' : $v'_1, v'_2, \ldots, v'_n$ ***: V*** 'ye ***X*** damgası eklendikten sonraki ***V*** değerleri

D' : Damgalı doküman

D* : Damgalı dokümanın (D') saldırıya uğramış veya gürültü eklenmiş hali.

X* : *D** dokümanından çıkarılmış, bozulmuş ihtimali olan damga

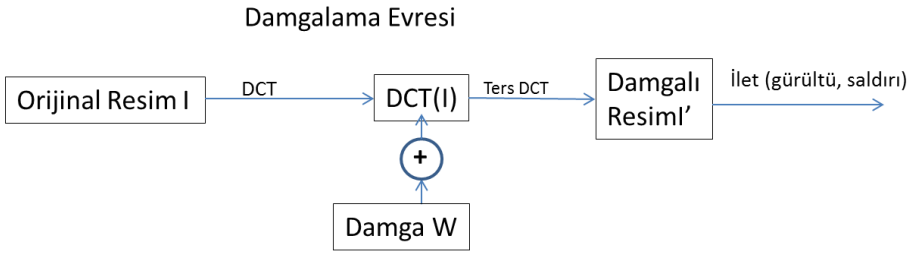
V' değerlerini hesaplarken ***X*** damgasının V değerlerini hangi ölçekle değiştireceğini belirten bir α değeri vardır ve aşağıdaki formülle ***V'*** değerleri hesaplanır.

$$V'_i = v_i + \alpha\, v_i\, x_i$$

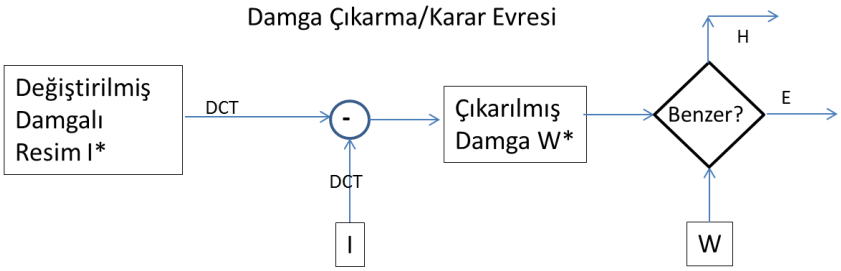
Yazarlar **α =0.1** olarak kullanmışlardır. Ayrıca aşağıdaki gibi her değer için farklı α_i değeri de kullanılabileceğini belirtmişlerdir.

$$V'_i = v_i + \alpha_i\, v_i\, x_i.$$

Damgalama ve damga çıkarma işlemleri Şekil 2.11 ve Şekil 2.12'de görülmektedir.



Şekil 2.11 Cox v.d. Damgalama İşlemi



Şekil 2.12 Cox v.d. Damga Çıkarma ve Tespit İşlemi

Piva, Barni, Bartolini ve Capellini de benzer bir yöntem kullanmıştır[35]. Damgalama DCT uzayında yapılmış, damga olarak ortalaması 0, varyansı 1 olan bir sözde rastgele sayı dizisi (pseudo random number sequence-PRNS) kullanılmıştır. Cox v.d.'nden farklı olarak, damga DC hariç ilk 1000 değere damgalanmak yerine, ilk L değer damgalanmayıp sonraki M değer damgalanmıştır. Damga tespit evresinde orijinal resmi kullanmaması nedeniyle çalışma kör damgalama örneği sayılmaktadır. İlk L değeri kullanmamalarının sebebi olarak, yazarlar damgalı resmin histogram eşitleme, gamma düzeltmesi gibi yüksek-geçirgen filtrelerden etkilenmemesini sağlamak olduğunu belirtmişlerdir. Makalede L=25000, M=16000 değerleri kullanılmıştır. M değeri damga boyutu olarak da anlaşılmaktadır. Damga düşük frekanslı ve yüksek frekanslı değerler yerine orta frekanslı değerlere damgalanarak damgalı resmin yüksek-geçirgen ve alçak-geçirgen filtrelere karşı dayanıklı olması hedeflenmiştir.

2.5 Kör ve Kör Olmayan Damgalama

Damga çıkarma esnasında algoritma damgalı ve muhtemelen değişikliğe uğramış resme ilaveten orijinal resme ve damga damgalama esnasında kullanılan veya üretilen damgaya ihtiyaç duyuyorsa, bu tip damgalama algoritmalarına kör olmayan damgalama algoritmaları denir.

Orijinal resme damga geri çıkartma esnasında ihtiyaç duymayan algoritmalara kör algoritma denir. Kör olmayan algoritmalar ile damgalanan resimler kör algoritmalara göre damgalanan resimlere göre orijinal resme benzerlik yönünden genellikle daha iyidir. Kör damgalamada genel olarak damga gürbüzlük katsayısının biraz daha güçlü tutulması gerekir. Asla benzerlik yönünden dezavantajı olsa da kör damgalama kör olmayan damgalamaya göre çok daha

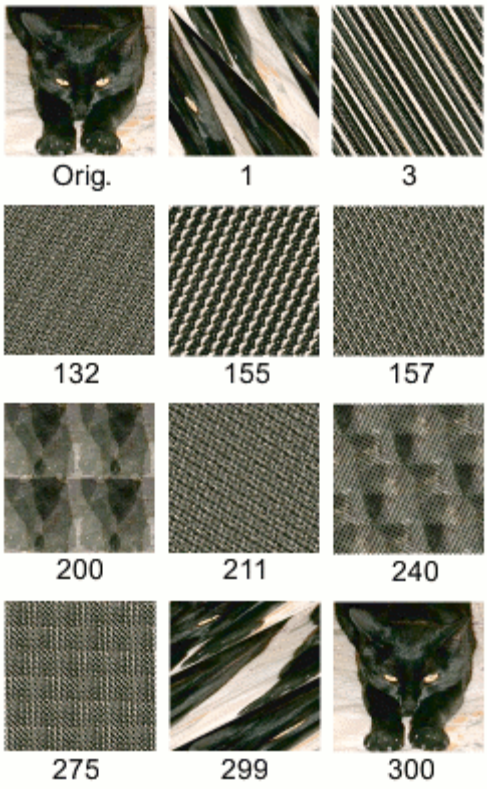
fazla tercih edilir çünkü damga çıkartma esnasında orijinal resmin de bulunmasını beklemek büyük bir dezavantajdır. Doğrulama amaçlı damgalama algoritmalarında orijinal resmin doğrulama işlemini yapmaya çalışan kişinin elinde olmadığı varsayılmaktadır.

2.6 Kullanılan Damga Çeşitleri

İlk yapılan damgalama çalışmaları resimlere sözde rastgele sayı dizileri damgalamışlardır (Pseudo random number sequence-PRNS). PRNS uzunlukları genel olarak uzun denebilecek büyüklüklerde olmuştur. PRNS'ler üretilirken resimdeki gürültünün normal dağılıma sahip olduğundan yola çıkılarak resimlere damgalanan PRNS'ların ortalamasının 0, varyansının bir olması genel kabul gören yaklaşım olmuştur. PRNS şeklinde eklenen damgalar çıkartılırken genel olarak damgalı resmin değerleri ile PRNS damgasının değerleri arasındaki korelasyon hesaplanmış, korelasyon belli bir sınır değerinden büyükse resmin damgalı olduğuna karar verilmiştir. Korelasyon hesaplamalarında değişik formüller kullanılmış olup 2.7.2 bölümünde detaylı olarak anlatılmaktadır.

Bazı çalışmalarda resim hakkında meta veriler resme damgalanmıştır. Pek çok çalışmada ise resme siyah beyaz resim damgası damgalanmıştır. Damgalanan siyah beyaz damga bir firma logosu, bir kişinin yüzü gibi sabit bir damga olabildiği gibi örneğin resmin kendisinin düşük çözünürlüklü bir hali de olabilmektedir. Bazı çalışmalarda kişinin kendi sesi de damgalanabilmektedir.

Pek çok çalışma damgayı ana resme damgalamadan önce bir şifre ile şifrelemekte veya Arnold Cat Map algoritması gibi geri alınabilir bir yöntem ile karıştırdıktan sonra damgalamaktadır. Şekil 2.13'de Arnold Cat Map algoritması ile resmin karıştırılma adımları görülmektedir [36]. Birinci karede kedi resminin orijinal ilk hali görülmekte, resmin ara adımlardaki hallerinin altındaki numara ise algoritmanın kaçıncı defa uygulanışında resmin o hale geldiğini göstermektedir. Kaçıncı adımındaki halini ana resme damgaladığını ancak resmi damgalayan ve damgayı çıkartacak yetkili kullanıcı bilecektir. Algoritma bu resim için 300 adımda tekrar resmin orijinal haline geri dönmektedir.



Şekil 2.13. Arnold cat map yöntemi ile karıştırılan resim 300 adım sonra orijinal haline dönmektedir

2.7 Damgalamanın Başarı Kriterleri

Damgalamanın başarısı damgalamanın amacına göre değişebilir. Sahipliğin ispatı amacıyla geliştirilen bir damgalama çalışmasında damgayı kötü amaçlı olarak yok etme amacıyla yapılmış resim operasyonlarına karşı damganın dayanıklı olması istenirken, resmin orijinali ile aynı olduğunu teyit etmek maksadıyla yapılan doğrulama algoritmasında resimde belli oranda değişiklikten daha fazlası yaplması durumunda damganın bozulmak sureti ile değişikliği bize bildirmesi istenebilir. Bu bölümde damgalamanın başarısında kullanılan metrikler alt başlıklar halinde açıklanmaktadır.

2.7.1 Damgalı Resmin Orijinal Resme Benzerliği (Fidelity), Ayırtedilmezliği

Damgalama işleminin başarısını belirleyen kıstaslardan birincisi benzerlik kıstasıdır. Benzerlik, damgalı resim ile orijinal resmin çıplak gözle ayırt edilemeyecek kadar birbirine benzemesi, resimde damgalamadan dolayı dalgalanmalar, kusurlar görünmemesidir. Şekil 2.14.a'da orijinal resim, b'de damgalı resim görünmektedir. Damgalı resim orijinal resme ne kadar çok benzerse, damgalama işlemi benzerlik ölçütüne göre o kadar başarılı sayılır.

Orijinal resim ile damgalı resim arasındaki benzerlik genelde en yüksek sinyalin gürültüye oranı (Peak-signal-to-Noise-Ratio (PSNR)) değeri ile ölçülür.

$$PSNR = 20 \log_{10}(255/RMSE) \quad (1.22)$$

Orijinal resim ve damgalı resimler arasındaki piksel değerleri farklarının kareleri toplamının karekökü olarak RMSE Eş.1.23 ile hesaplanır.

$$RMSE = \text{sqrt}((\sum_{i,j}(I^*_{ij} - I_{ij})^2)/ (NxN)) \quad (1.23)$$

I*: damgalı resim, I: orijinal resim

Orijinal Resim Damgalı resim

Şekil 2.14 Orijinal ve Damgalı Resim

Ellinas, PSNR değerinin insan görme sistemini (Human Visual System HVS) dikkate almadığını söyleyerek ağırlıklı PSNR (weighted PSNR: wPSNR) formülünü kullanmıştır (Eş.1.24) [37]. Eş.1.25'de wPSNR hesaplanırken kullanılan ağırlıklı RMSE değeri olan wRMSE verilmektedir.

$$wPSNR = 10 \log_{10}(255 * 255/wMSE) \quad (1.24)$$

$$wRMSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{x(i,j)-y(i,j)}{1+var(i,j)}\right]^2 \quad (1.25)$$

var(i,j) varyans değeri olup Eş.1.26'da verilmiştir. x(i,j) orijinal resim değerleri, y(i,j) damgalı resim değerleri, $Y'_{u,v}$ değerleri damgalı ve değişikliğe uğramış resmin DWT dönüşüm uzayındaki kullanılan değerleridir.

$$\text{Var(i,j)} = \frac{1}{(MN)^2} \sum_{u=0}^{M-1} \quad \sum_{v=0}^{N-1} (Y'u, v)^2 \tag{1.26}$$

$$\sigma^2 = \frac{1}{(MN)^2} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{x(i,j)-y(i,j)}{1+var(i,j)}\right]^2$$

$$wMSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{x(i,j)-y(i,j)}{1+var(i,j)}\right]^2$$

Kutter ve Petitcolas benzerliği PSNR yerine MPSNR değeri ile ölçmüşlerdir [38] . Bu metriğin PSNR yerine kullanılması van den Branden Lamprecht ve Farrell tarafından önerilmiştir [39] .

MPSNR hesaplanırken önce resmin daha detaysız segmentasyonu yapılır, filtrelerle orijinal resim görsel komponentlere ayrılır. Her piksel için tespit sınır değeri (treshold) orijinal resim bir maske gibi kullanılarak belirlenir, tüm renk kanalları üzerine biriktirmek suretiyle filtrelenmiş hata sınır değeri ile bölünür. Sınır değeri üzerindeki değerlere JND (Just Noticable Difference) denir.

$$\text{MPSNR} = 10 \log_{10} \frac{255^2}{E^2}$$

E hesaplanan sapma değeridir. Bu değerin ölçü birimi dB (decibel) değil, görünür decibel (visual decibel) vdB'dir. Değer normalize edilirse

$$\text{Q} = \frac{5}{1+N\ x\ E}$$

N normalize sabit değeridir.

2.7.2 Çıkarılan Damganın Orijinal Damgaya Benzerliği

Sahipliğin ispatı türündeki damgalamalarda söz konusu resimden çıkarılan damganın ana resme eklenen damgaya benzerliği karar vermede ölçüt olacaktır.

Bu konuda benzerlik oranı (Similarity Ratio SR) metriği en fazla kullanılan metriklerdendir.

2.7.2.1 Similarity Ratio SR değeri

SR değeri daha çok siyah beyaz damgalarının benzerlik ölçütü olarak kullanılır. S değeri orijinal damga ile çıkartılan damga arasında aynı koordinatlardaki siyah beyaz değer birbirine eşit olanların sayısı, D ise aynı olmayanların sayısı olmak üzere Eş.1.27'de verilmiştir.

$$SR = S / (S + D) \quad (1.27)$$

2.7.2.2 Normalize SR (NSR)

Bazı çalışmalarda Eş.1.28'de verilen normalize edilmiş SR değeri kullanılmaktadır.

$$NSR = \frac{SR - \min(SR)}{1 - \min(SR)} \quad (1.28)$$

2.7.2.3 Doğrusal Korelasyon (Linear Correlation)

Doğrusal korelasyon, Eş.1.29'daki gibi hesaplanır.

$$Z = \frac{1}{M*N} \sum_x \sum_y W(x,y) * W'(x,y) \quad (1.29)$$

W: orijinal damga

W': çıkartılan damga

M,N: damga boyutları

Eğer Z > Tz , ise damganın varlığına hükmedilir. Tz korelasyon sınır değeridir.

$Tz = \frac{\propto}{3M} \sum_{x=1}^{M} \sum_{y=1}^{N} W'(x,y)$, Piva v.d. leri[35]da $\alpha = 0.2$ kullanmıştır.

2.7.2.4 Normalize Korelasyon (Normalized Correlation)

Lineer korelasyondaki problem, resimdeki genel parlaklık değişikliklerinden etkilenmesidir.

Bu problem, lineer korelasyondaki paydanın resim boyutları çarpımı değil resimlerdeki değerlerin kareleri toplamının karekök değeri şeklinde her iki resimden elde edilen değerin çarpımı ile yer değiştirmesi ile çözülmekte, resimdeki genel parlaklık azalması veya artmasından etkilenmesinin önüne geçilmiş olmaktadır.

$$Z_{NC} = \frac{1}{\sqrt{\sum\sum W(x,y)^2}\ \sqrt{\sum\sum W\prime(x,y)^2}} \sum_x \quad \sum_y \quad W(x,y) * W'(x,y)$$

2.7.2.5 Korelasyon Katsayısı (Correlation Coefficient)

Normalize korelasyonun problemi, DC komponent'a yapılan bir değişiklikten etkilenmesidir. Bu sakıncayı ortadan kaldırmak için korelasyon katsayısı formülü geliştirilmiştir. Normalize korelasyondan farkı, payda kısmında değerlerden değer ortalaması çıkarıldıktan sonra kareler toplamı alınarak karekök alınmasıdır.

$$Z_{CC} = \frac{1}{\sqrt{\sum\sum(W(x,y)-\overline{W(x,y)})^2} * \sqrt{\sum\sum(W\prime(x,y)-\overline{W\prime(x,y)})^2}} \sum_x \quad \sum_y \quad W(x,y) * W'(x,y)$$

$\overline{W(x,y)}$: $W(x,y)$ ortalamasıdır.

2.7.3 Saldırılara Karşı Gürbüzlük (Robustness)

Sahipliği ispat etmek için yapılan damgalamalarda damgalı resim içindeki gömülü damganın basit resim işlemleri ile ortadan kalkmaması istenir. Bir fotoğraf sanatçısının fotoğraflarını damgaladıktan sonra kendi web sitesine koyduğu düşünülsün. Bu fotoğrafı indirdikten sonra fotoğrafın %80'lik kısmı indiren kişinin işini görüyorsa ve kesme işlemi (crop) sonucunda %80'lik kalan kısımdan damga çıkartılamıyorsa, damgalama işlemi kesme işlemine göre dayanıklı değildir demektir. Bu durumda fotoğrafı indirip kesme işlemi yaparak kullanan kişi bedel ödemeden fotoğrafı kullanmış olacaktır.

Kesme işlemine benzer şekilde, bir kişi damgalı olarak piyasaya sunulan bir dosyayı damgayı tekrar geri çıkartamayacak şekilde değiştirip bedelsiz kullanmak isteyebilir. Sahipliğin ispatı amaçlanan damgalama işleminin, resme yapılacak bu tür değişikliklerde dahi damgayı muhafaza etmesi, diğer bir deyişle damganın değişikliklere rağmen dosyadan geri çıkartılabilmesi istenir. Damgalı çalışmayı bedelsiz kullanmak isteyen kişinin damgayı ortadan kaldırmak için resme yaptığı işlemler, resmi korsan kullanmak isteyen kişinin dahi işine yaramayacak şekilde resmi bozuyorsa bu aşamadaki resim değişikliklerinde damga geri çıkartılamasa da amaca ulaşılmış demektir.

Damgalı resme yapılabilecek resim operasyonları bölüm 2.8 de kategorize edilmiştir. Damgalı resmin kayıplı sıkıştırmaya maruz kalması, histogram eşitleme, bulanıklaştırma, belli bir açıyla döndürülmesi, resmin belli oranda büyütülmesi veya küçültülmesi v.b. işlemler genel olarak kötü maksatlı olmayan, damgayı

ortadan kaldırmayı amaçlamadan yasal kullanan kişinin de yapabileceği resim işlemleri olabilir. Bir resmin karşı tarafa gönderilirken iletim ortamından kaynaklı belli oranda gürültüye maruz kalması da doğal bir değişiklik olarak görülebilir. Bu tür resim değişiklikleri kötü amaçlı olarak damgalı resim içindeki damgayı yok etmeye yönelik de olabilir.

Damgalı resme yapılan bazı değişikler ise büyük olasılıkla veya kesin olarak kötü amaçlıdır. Damgalı bir resme kendi damgalama algoritmasını kullanarak kendi damgasını da ekleyen kişi yeniden damgalama saldırısı yapmış olur. Halise'nin damgalı çalışmasına kendi damgasını yeniden damgalayan Alp, işin yargıya intikal etmesi durumunda mahkeme bilirkişisi huzurunda Halise'nin damgalı resminden kendi damgasını çıkararak kafa karıştırmak veya Halise'nin çalışmasının kendine ait olduğunu ispatlamak istemektedir. Bu durumda Halise'nin bilirkişiye sadece Halise'nin elinde bulunan orijinal damgasız resmini vererek Alp'in bu resimden kendi damgasını çıkartmasını istemesi durumunda Alp damgayı çıkartamayacak ve Halise'nin haklılığı ortaya çıkacaktır. Craver, Memon, Yeo ve Yeung'un çalışmasında Halise'nin damgalama algoritmasını belli esaslara dikkat etmeden yapması durumunda Alp'in damgayı Halise'nin orijinal damgasız resminden de çıkartabileceği, bu durumu önlemek için Halise'nin damgalamayı hangi esaslara uyarak yapması gerektiği anlatılmaktadır[40].

Reklam takibi amaçlı yapılan bir damgalamada, damganın hava yayını veya yayın ortamında yayına eklenmesi olası gürültülere rağmen yayından geri çıkartılabilmesi, damgalamanın bu tür gürültülere dayanıklı olması beklenir.

Damgalamada gürbüzlük ile benzerlik ters ilişkili özelliklerdir. Gürbüzlüğü artırırken benzerlik azalır. Gürbüzlük genel olarak damga çarpanı artırılarak sağlanır. Damgalama eklemeli (additive) bir işlem olduğu ve Eş. (1.30)'daki gibi uygulandığı için damgalı resim I* elde edilirken W damgasının resme hangi katsayıyla ekleneceğini α katsayısı belirler. α katsayısı arttıkça benzerlik azalır. Bir çok çalışmada α katsayısının en iyi değeri optimizasyon teknikleri kullanılarak bulunmaya çalışılır [28][41][42][29][33][32] .

$$I^* = I + \alpha * W \qquad (1.30)$$

Bazı damgalama çeşitlerinde gürbüzlük istenen bir durum değildir. Doğruluğunu ispatlama (authentication) tarzı damgalamalarda resimde bir değişiklik olması

durumunda hemen tespit edilebilmesi için damgalama işlemi kırılgan bir şekilde yapılır. Bir değişiklik durumunda damganın geri kazanılamayacağı şekilde damgalama ve geri çıkarma algoritması düzenlenir. Özellikle askeri çalışmalarda, medikal görüntülerde, delil niteliği taşıyan dokümanlarda en ufak bir değişikliğin fark edilmesi istenir. Buna benzer "doğruluğunu ispatlama" tarzı damgalama yöntemlerinin bazılarında bir dosyada yapılacak en ufak bir bit değişikliğinde dosya "orijinal değil" şeklinde kategorize edilmek istenir. Bu tür damgalama uygulamalarına "tam doğrulama damgalaması" veya "tam kırılgan damgalama" uygulamaları denir.

Doğrulama tarzı damgalamaların bazılarının ise yarı kırılgan olması arzulanır. Uydudan gönderilen resimlerin havadan gönderiminde ortamdan kaynaklı bir gürültüden etkilenmeyecek şekilde gürbüz, ancak resimde oynama tarzı diğer değişikliklerde damganın ortadan kalktığı seçici kırılgan bir damgalama istenebilir. Normal ve olağan karşılanan değişikliklerde damganın bozulmadığı, ancak kötü niyetli değişikliklerde damganın ortadan kalktığı bir damgalama yöntemi doğrulama tarzı damgalamalar için idealdir. Bu şekilde seçici kırılgan damgalama yöntemi üretmek zordur. Şimdiye kadar yapılan uyguamalar belli tip değişikliklere karşı gürbüz, belli değişikliklere kırılgan olacak şekilde ideal duruma yaklaşmaya çalışmakta iselerde ideal durumdan uzaktadırlar.

2.8 Damganın Ortadan Kaldırılmasına Yönelik Saldırılar

Damgalı bir resime yapılan bazı işlemler resimdeki damganın geri çıkarılamayacak şekilde bozulmasına yol açabilir. Bu tür işlemler damgayı ortadan kaldırmayı hedeflemeyen masum normal işlemler olabileceği gibi, resmin kalitesini fazla bozmadan sahipliği ispatlamayı önleyecek veya resmin anlamını değiştirecek değişiklikler olabilir. Resmin damgalama işlemi hangi amaçlı yapıldıysa algoritmanın damga gürbüzlük katsayısını ona göre düzenlemesi beklenir. Damgayı etkileyebilecek genel işlemler aşağıdaki gibi sıralanabilir. Bu listede olmayan değişiklikler olabilir ancak en sık yapılanlar sıralanmıştır.

2.8.1 Kötü Maksatlı Olma İhtimali Az Olan Değişiklikler(Daha yaygın)

- Kayıplı sıkıştırma
- Lineer - lineer olmayan filtreleme (alçak geçirgen-yüksek geçirgen v.b.)
- Büyültme-küçültme (x' = x.a, y' = y.b)

- Resmin tamamına uygulanan parlaklık azaltma veya artırma
- Histogtam eşitleme, Gamma düzeltmesi v.b.
- İletim ortamında doğal olarak gürültü eklenmesi

2.8.2 Maksatlı Olma İhtimali Orta Seviye Olan Değişiklikler

- Kesme (Cropping)
- Resmi belli açıyla döndürme
- Resmi aşağı-yukarı veya sağa-sola kaydırma (x’ = x + x0 , y’ = y + y0)

2.8.3 Maksatlı Yapılan Değişiklikler

- Resmi kağıda bastırıp basılı olanı taratmak(Rescanning)
- İlave 2nci damga eklemek
- Kesme yapıştırma işlemi beraber yapılması

3. DAMGALAMA YÖNTEMİ

3.1 DWT Uzayında Bloklu Damgalama ve Blok Büyüklüğü Analizi

Ayrık dalgacık dönüşümü genel hatları ile bölüm 2.3.3 de açıklanmıştır. DWT uzayında damgalama konusunda daha önce pek çok çalışma yapılmıştır.

Ganic ve Eskicioğlu resmi DWT uzayında bir seviye ayrışıma tabi tuttuktan sonra her bir bandı SVD ayrıştırmasına tabi tutmuşlardır[27] . Damga resmini de SVD ayrıştırmasına tabi tuttuktan sonra Eş.1.31'de ifade edildiği gibi damganın tekil (singular) değerlerini belli bir katsayı ile çarparak her bir bandın tekil değerlerine ekleyerek ve işlemlerin tersini uygulayarak damgalı resmi elde etmişlerdir. λ_i^* Damgalanmış DWT bandı tekil değerini, λ_i DWT bandı tekil değerini, α katsayı değerini, λ_{wi} damganın tekil değerini ifade etmektedir.

$$\lambda_i^* = \lambda_i + \alpha\lambda_{wi} \quad (1.31)$$

Zhu, Xiong ve Zhang çalışmalarında resmi DWT uzayında birkaç seviye ayrışmaya tabi tuttuktan sonra her bir DWT ayrışma seviyesinin HL, LH, HH bantlarına o seviyenin çözünürlüğüne uygun büyüklükte bir sözde rastgele sayı dizisi damgalamışlardır [43].

Dugad, Ratakonda ve Ahuja [44], resimle aynıt boyutta bir damgayı, resimle beraber DWT dönüşümüne sokarak, LL bandı haricindeki bantlarda T1 sınır değerinden büyük değerlere damgalama yapmışlar, damgayı geri çıkartırken T1 sınır değerinden daha büyük T2 sınır değeri belirleyerek T2 sınır değerinden daha büyük değerlerin damgalanan damga ile korelasyonuna bakmışlardır. Damgayı damgalarken Eş.1.32' deki gibi ana resmin dönüşüm değerlerinin skalar büyüklüğü ile de çarptıkları için, eklenen damga orijinal değerin büyüklüğü ile orantılı olmaktadır. λ_w damga değerleri ortalaması sıfır, varyansı 1 olan rastgele sayı dizisidir. Orijinal damga ile eldeki çalışma arasındaki korelasyon Eş.1.33 de görüldüğü gibi, λ_i^* damgalı olup olmadığı kontrol edilen çalışmanın ilgili dönüşüm değerleri, λ_{wi} ise eklenen damga olacak şekilde hesaplanır. Korelasyon hesabından sonra Eş.1.34'de görüldüğü gibi bir sınırı S değeri belirlenerek S değerinden korelasyon büyük çıktığı taktirde çalışmada damganın bulunduğuna karar verilir. Benzer bir çalışma olan [35] de ise Eş.1.34'deki sınır değer payda olarak 2M değil, 3M kullanılmıştır.

$$\lambda_i^* = \lambda_i + \alpha|\lambda_i| \lambda_{wi} \quad (1.32)$$

$$z = \frac{1}{M}\sum_i \lambda_i^* \lambda_{wi} \quad (1.33)$$

$$S = \frac{\alpha}{2M}\sum_i|\lambda_i^*| \quad (1.34)$$

Elbaşı ve Eskicioğlu resmi DWT uzayına alıp LL1 bandı hariç LH1, HL1 ve HH1 bandlarının belli bir sınır değerinden büyük değerlerine damgayı damgalamış, damganın varlığını test ettikleri aşamada Naive Bayes kullanarak yarı-kör damgalama denemişlerdir[45]. Damganın varlığının kontrol edildiği aşamada, T2 sınır değerinden büyük band değerlerinin ortalama, değer aralığı, varyans, değer sayısı v.b. istatistiksel değerlerini öznitelik olarak kullanarak Naive Bayes sınıflayıcısına karar verdirmişlerdir. Naive Bayes sınıflayıcısının, önceden sınıfları belli olan bir eğitim setinde eğitildiği ifade edilmiştir.

Elbaşı ve Eskicioğlu, DWT uzayında sadece LL ve HH bantlarına her banda değişik damga gücü faktörü kullanarak, bazı saldırı çeşitlerinde LL bandındaki damganın dayanıklı olduğunu, bazı saldırılarda ise HH bandındaki damganın dayanıklı olduğunu tespit etmişlerdir[46].

Jane ve Elbaşı damgalama yaparken DWT, LU, SVD ayrışmalarını beraber kullanmışlardır[47] . Resmi DWT seviye 1 ayrıştırdıktan sonra LL bandını LU ayrışması ile Eş.1.21'de olduğu gibi L, D, U bantlarına ayrıştırmışlar, daha sonra D bandını SVD ayrıştırmasına tabi tutarak damgayı SVD ayrışımının tekil değerlerine damgalamışlardır.

Barni, Bartolini, ve Piva resmi 4 seviye DWT ayrışmasına tabi tuttuktan sonra damgayı LH, HL ve HH bantlarına damgalamışlardır [48]. Damgalama esnasında, insan görü sisteminin Lewis ve Knowles [49] tarafından tespit edilen aşağıdaki prensiplerine uymak sureti ile damgalama katsayısı hesaplayarak uygulamışlardır.

- İnsan gözü yüksek frekanslı bantlardaki, özellikle 45 derece açıya sahip bantlardaki (HH bandı) gürültüye daha az hassastır.
- Parlaklığın çok yüksek veya çok düşük olduğu yerlerdeki gürültüye daha az duyarlıdır.
- Yüksek dokuya sahip bölgelere daha az duyarlı iken, kenarlara karşı daha hassastır.

Peining ve Eskicioğlu DWT uzayında 1 ve 2 seviye ayrışma yaparak farklı ayrışma seviyelerinde LL, LH, HL, HH bantlarına damgalama yapmışlardır[6]. Çalışmalarında aşağıdaki bulgulara ulaşmışlardır.

- Farklı ayrışım seviyelerine ve farklı bantlara farklı damga katsayısı uygulanırsa daha iyi sonuçlar elde edilebilmektedir. Daha iyi sonuç, benzerlikten fazla ödün vermeden elde edilen dayanıklılığın artmasıdır. Birinci seviye DWT ayrışımında LL bandına katsayı olarak 8, LH, HL, HH bantlarına 2 katsayısı uygulanmıştır. İkinci seviye DWT ayrışımında LL2 bandına 20, LH2, HL2, HH2 bantlarına 3 katsayısı uygulanmıştır.
- Pek çok DWT tabanlı damgalama çalışmasında LL bandına yapılacak damgalamanın orijinal resme benzerlik özelliğine fazla olumsuz etkisi olduğu söylenmesine rağmen durumun böyle olmadığı, LL bandına yapılan damgalamanın başarılı sonuçlar verdiği gözlemlenmiştir. LL bandına yapılan damgalamanın, yüksek frekans değerleri ortadan kaldıran kayıplı sıkıştırma, bulanıklaştırma, Gauss gürültüsü gibi saldırıların haricinde büyüklük değiştirme, döndürme, kesme, keskinleştirme saldırılarında da diğer üç banda yapılan damgalamadan daha dayanıklı olduğu gözlemlenmiştir.
- Orta frekanslara yapılan damgalama histogram eşitleme, gamma düzeltmesi, parlaklık aralığı ayarlama gibi resim operasyonlarına daha dayanıklıdır.
- İleri DWT ayrışma seviyelerine damgalama yapmak mümkün olsa da damgalama yapılabilecek yüzeyin küçülmesi bir dezavantaj olarak durmaktadır.

Ellinas resmi DWT uzayına aldıktan sonra her bir banttaki kenarları sobel kenar bulucu ile bulmakta, daha sonra morfolojik bir yayma operasyonuyla kenarların etrafında damgalanacak bölümü belirleyip damgayı bu alana damgalamaktadır [50].

Liu, Huang ve Shi damgaya BCH (Bose, Chaudhuri, ve Hocquenghem) hata düzeltme kodu ve 2 boyutlu araya girme (2-D interleave) kullanmak sureti ile DWT uzayında LL bandı dâhil olmak üzere tüm bantları kullanacak şekilde kör damgalama yöntemi geliştirmişlerdir[51].

Kaur ve Jindal resme öncelikle 2x2 lik medyan filtre uyguladıktan sonra resmi 1nci seviye DWT ayrışmasına tabi tutmuş, HH bandının ve damga resminin SVD dönüşümünü alıp HH bandının tekil değerlerine damganın tekil değerlerini bir damga gücü katsayısı ile çarparak eklemişler, ters işlemleri uygulayarak damgalı resmi elde etmişlerdir[52].

3.1.1 Bloklu Damgalama

Yapılan çalışma, Tao ve Eskicioğlu'nun [6] çalışmasının bloklu olarak yapılması ve değişik blok büyüklükleri ile analiz edilmesidir. DWT uzayı tabanlı, LL, LH, HL, HH tüm bantlara damgalama yapan bir damgalama çalışması yapılmıştır. Tao ve Eskicioğlu resmin bir bütün olarak DWT dönüşümünü alırken buradaki çalışmada resim bloklara ayrıldıktan sonra her bir blok kendi içinde DWT uzayına çevrilmiştir. Resim Tao ve Eskicioğlu çalışmasında olduğu gibi bir bütün olarak DWT uzayına alınarak damgalandığı gibi, 64x64, 32x32, 16x16, 8x8 büyüklüğündeki blok büyüklükleri ile ayrı ayrı damgalama yapılarak sonuçlar elde edilmiştir. Bu çalışmaya özgü olarak, damga resminin kendisi de aynı şekilde bloklara ayrılmıştır. Her bir blok için, o bloğun en ve boy olarak yarısı olan damga resmi bloğu LL, HL, LH, HH bloklarına damgalanmaktadır. Her bir blok büyüklüğü için damgalı resim ile orijinal resim arasındaki benzerlik değeri olan PSNR değeri hesaplanmıştır.

PSNR = 20 $\log_{10}$(255/RMSE)

RMSE ise original ve damgalı resimler arasındaki farkların karelerinin toplamının karekökünün resim boyutuna bölünmesi ile bulunur.

RMSE =sqrt(($\sum_{i,j}(I^*_{ij} - I_{ij})^2$)/ (NxN))

Damga ekleme algoritması aşağıda verilmiştir. Algoritma 64x64 lük bloklar için verilmiştir ancak blok büyüklüklüğü parametriktir ve diğer blok ebatları için de çalıştırılmıştır.

3.1.1.1 Damga Ekleme Algoritması:

1. Orjinal resim 64x64'lük eşit parçalarına bölünür (Her bir bloğa Ipo densin)

2. Siyah beyaz damga resmi W 32x32'lik Wp bloklarına bölünür

3. Her 64x64 Ipo bloğu için

    a. (Ipt_LL, Ipt_LH, Ipt_HL, Ipt_HH) ← DWT(Ipo),

b. Damganın 32x32lik denk gelen Wp kısmını Ipt_LL, Ipt_LH, Ipt_HL, Ipt_HH her birine damgala

i) $Ipt\_LL'_{ij} \leftarrow Ipt\_LL_{ij} + \alpha\, Wp_{ij}$, LL bandı için α=8 for LL, diğer üç band için α=2

c. Ipw ← IDWT(Ipt_LL', Ipt_LH', Ipt_HL', Ipt_HH') ,Ipw damgalı bloğunu elde et

ç. Damgalı Ipw bloklarını birleştirip Iw damgalı resmini elde et.

3.1.1.2 Damga Çıkartma Algoritması:

1. Damgalanmış ve Muhtemelen Saldırıya Uğramış Resmi 64x64 lük Eşit Ip* Bloklarına Böl

2. Orjinal resmi 64x64 eşit parçalara böl, (Her bir bloğa Ipo densin)

3. (Ipt_LL*, Ipt_LH*, Ipt_HL*, Ipt_HH*) ← DWT(Ip*)

(Ipt_LL, Ipt_LH, Ipt_HL, Ipt_HH) ← DWT(Ipo)

4. Tüm Ip* ve Ipo Blokları için

Wp_LL* ← (Ipt_LL*- Ipo_LL)/coll; (Wp_LL* : LL bandından çıkarılan damga bloğu, coll değeri 8)

Wp_LLb* ← Wp_LL* > 0.5; (Wp_LLb* : Wp_LL'in siyah beyaz {0,1} değerlerine çevrilmiş hali)

Wp_LH* ← (Ipt_LH*- Ipo_LH)/coll; (coll değeri 2)

Wp_LHb* ← Wp_LH* > 0.5;

Wp_HL* ← (Ipt_HL*- Ipo_HL)/coll; (coll değeri 2)

Wp_HLb* ← Wp_HL* > 0.5;

Wp_HH* ← (Ipt_HH*- Ipo_HH)/coll; (coll değeri 2)

Wp_HHb* ← Wp_HH* > 0.5;

5. Wp* bloklarını birleştirerek LL, LH, HL, HH bantları için ayrı ayrı çıkarılmış damgaları elde et.

3.1.2 Deneyler

Yapılan damgalama çalışmalarında Şekil 3.1' deki siyah beyaz resim damga olarak kullanılmıştır.

Şekil 3.1 Bloklu Damgalama Siyah Beyaz Damga (BC harfi yan yana)

Algoritma, 64x64, 32x32, 16x16, 8x8'lik blok büyüklükleri ile ayrı ayrı çalıştırılmıştır. Her bir bloğun DWT ayrışımı bağımsız olarak yapılmış, damga LL, LH, HL, HH bantlarına ayrı ayrı damgalanmıştır. Her bir durum için damgalanmış resimler, orijinal resimler ile damgalanmış resimler arasındaki PSNR değerleri kaydedilmiştir.

Algoritmanın resim saldırılarına dayanıklılığını ölçebilmek için damgalı resimler damgalama işleminden sonra değişik işlemlere tabi tutulmuştur. Resimlere %75, %50, %25 kalitesinde jpeg kayıplı sıkıştırma, 3x3 bulanıklaştırma filtresi, 0 ortalamasında ve 0.001 varyansında Gauss gürültüsü, 0.5 ve 2 çarpanı ile küçültme-büyültme, histogram eşitleme, [0 0.8] aralığından [0 1] aralığına parlaklık şiddeti ayarlama, gamma düzeltmesi, yeniden damgalama saldırı ve işlemleri uygulanmıştır. İkinci damga saldırısında eklenen damga Şekil 3.2'de görülmektedir.

Şekil 3.2 Bloklu damgalamada kullanılan ikinci siyah-beyaz damga (Büyük A harfi)

Algoritma tarafından damgalı ve saldırıya maruz kalmış resimler **Şekil 3.3**'te görülmektedir. **Şekil 3.4** - **Şekil 3.11** 'de ise damgalama algoritması ile farklı blok büyüklükleri uygulayarak damgalandıktan sonra çeşitli resim operasyonlarına maruz kalmış resimlerin LL, LH, HL, HH bantlarından elde edilmiş damgalar görülmektedir. **Şekil 3.4** - **Şekil 3.11** incelendiğinde, damgalı ve saldırıya maruz kalmış resimlerden çıkarılan damgaların kalitesinin, blok ebadı küçüldükçe bariz bir şekilde arttığı gözlemlenmektedir. Bu durum, çıkartılan damgaların SR değerleri incelendiğinde de görülmektedir. En belirsiz damgalar, resim 64x64'lük

bloklara bölündüğünde, gerçeğine en yakın damgalar ise blok ebadı 8x8 olduğunda elde edilmiştir. Esasında gerçeğinden en uzak damga, resim herhangi bir bloğa bölünmeden bütün halinde DWT ayrışmasına alınıp damgalandığında elde edilmiştir. Çıkartılan damgalar ile yerleştirilen damga arasında hesaplanan SR değerleri Tablo 3-1 de verilmiştir. Tao ve Eskicioğlu çalışmasında belirtilen sonuçlar 8x8 blok ebadı sonuçlarının olduğu sütunun hemen yanında verilmiştir. Bu çalışma yapılırken kullanılan resim ve damga, Tao ve Eskicioğlu'nun çalışmalarında kullandığı resim ve damga ile aynıdır. Yapılan çalışmalar ve elde edilen SR değeri sonuçları, bloklu DWT damgalamanın bloksuz Tao ve Eskicioğlu DWT damgalamasına göre bazı saldırı çeşitlerinde daha iyi sonuçlar verdiğini göstermiştir. Tao ve Eskicioğlu'nun çalışması ile bazı saldırı tipleri yönünden kıyaslama yapılamamaktadır çünkü döndürme açısı, kesme oranı gibi bazı parametreler kendi çalışmalarında belirtilmemiştir.

Damgalanmış, Saldırı Yok

JPEG Sıkıştırma.75%.

JPEG Sıkıştırma.50%.

JPEG Sıkıştırma.25%.

0.5 küçült tekrar 2 katı büyült 2

Histogram Eşitleme.

3x3 Bulanıklaştırma

Parlaklık Ayarı [0 0.8]→ [0 1]

Gamma Düzeltmesi

Gauss Gürültüsü

Döndür-Düzelt 20o

Kes 50.4%

İkinci Damgalama

Şekil 3.3. Bloklu damgalama, damgalanmış ve çeşitli saldırılara maruz kalmış resimler

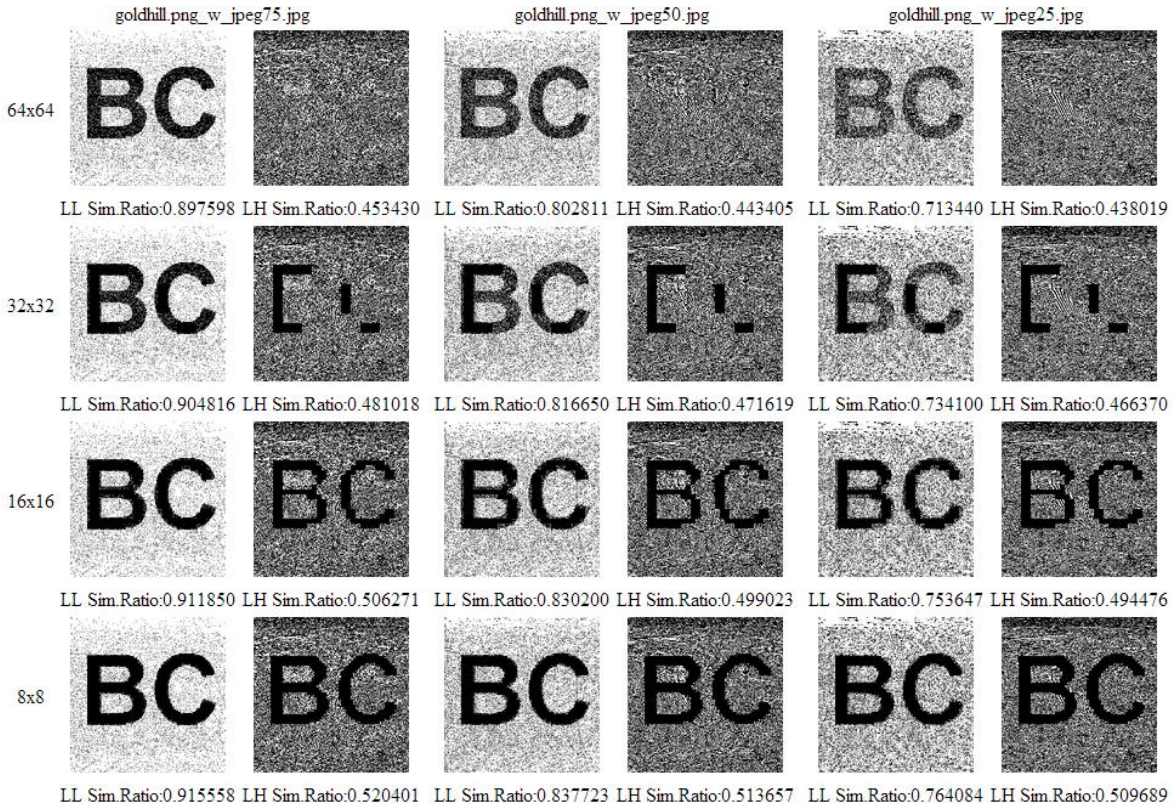
Algoritmaya, orijinal resme benzerlik yönüyle baktığımızda, küçük blok ebatlarında daha kaliteli damgalar çıkartabilmemize rağmen, damgalanan resmin benzerlik değerinin blok büyüklüğünden etkilenmediğini gözlemliyoruz. Yani 64x64 lük blok ebadı ile damgalanmış resim ile 8x8 blok ebadı kullanılarak damgalanmış resmin benzerlik değeri arasında bir farklılık görünmemektedir. Bu sonuç şöyle açıklanabilir: Orijinal resme damgaladığımız damga bir siyah beyaz resimdir ve damgalamadan etkilenen DWT uzayı değeri sayısı, siyah beyaz damgadaki 1 değerlerinin sayısı kadar olacaktır. PSNR değerinin farklı olduğu sadece Gauss gürültüsü etkisi durumudur. Gauss gürültüsü etkisinin her uygulanışında farklı bir rastgele gürültü eklendiğinden ve her blok ebadı için resme farklı bir gürültü eklenmekte olduğundan, PSNR değerinin farklı çıkması doğal bir durum olarak görünmektedir.

Damga gücü α değerini LL bandı için 12, LH, HL, HH bandları için 5 yaptığımızda çıkartılan damgaların SR değerleri daha iyi olmakta ancak eklenen damga belirgin hale gelmeye başlamakta, damgalamanın benzerlik ilkesi zedelenmeye başlamaktadır.

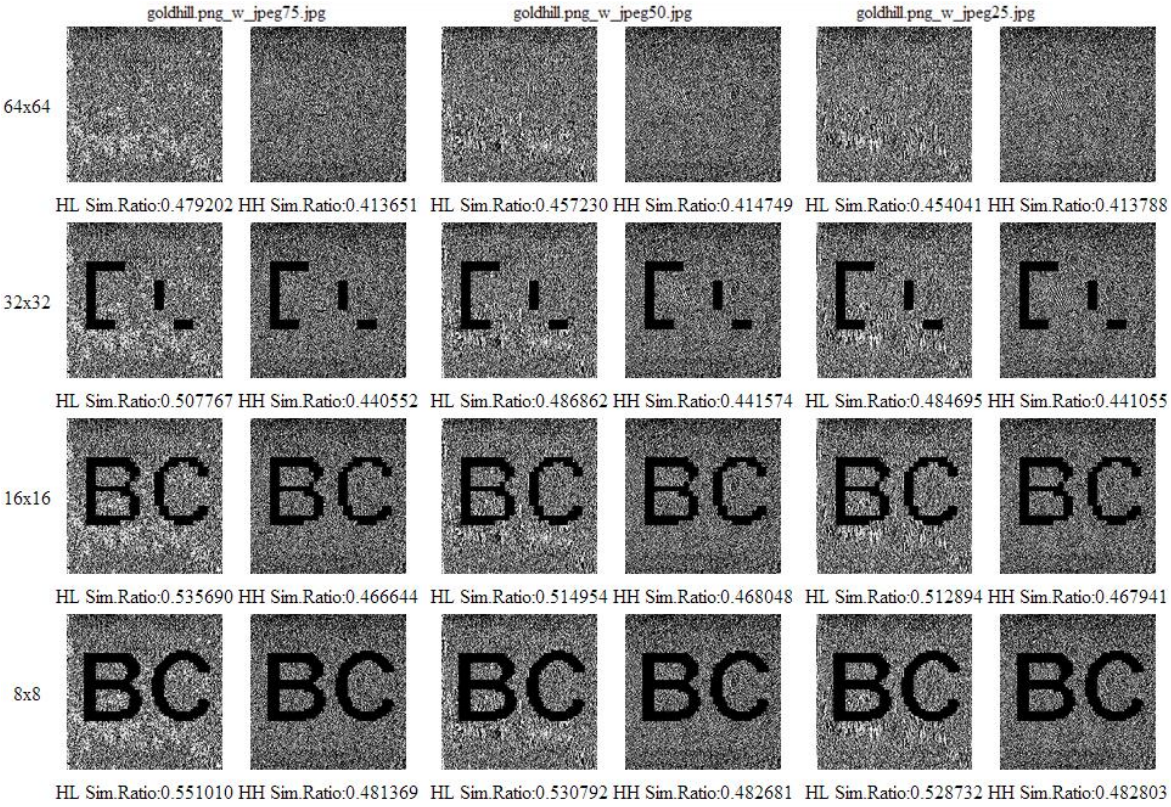
En iyi sonuçlar 8x8 büyüklüğündeki blok durumunda elde edilmesinin yanında, bu blok ebadlarıyla sadece 1nci seviye DWT ayrışması gerçekleştirilebilmektedir. Söylenmesi gereken diğer bir husus ise, blok ebadı küçüldükçe harcanan işlemci zamanı artmaktadır. Damga yerleştirme evresi ve değişik blok büyüklükleri için harcanan işlemci zamanları Tablo 3-2 ve **Şekil 3.12**'de, damga çıkartma evresi için Tablo 3-3 ve **Şekil 3.13**'te verilmiştir. Damga yerleştirme işlemci zamanları

incelendiğinde, blok büyüklüğü 64x64'den 32x32'e düştüğünde, yani 4 kat düştüğünde harcanan işlemci zamanı 1.8 kat artmış, 32x32'den 16x16'a düştüğünde 2.7 kart artmış, 16x16'dan 8x8'e düştüğünde 3.05 kat artmıştır. İşlemci zamanının artış hızı ise 32x32'lik bloktan 16x16'lık bloğa düşerken 1.54, 16x16'lık bloktan 8x8'lik bloğa düşerken 1.099'dur. Blok ebadı 4 kat düştükçe işlemci zamanı lineer olmayan şekilde ivmesi artmaktadır. Çıkartma evresi içinde benzer durum vardır.

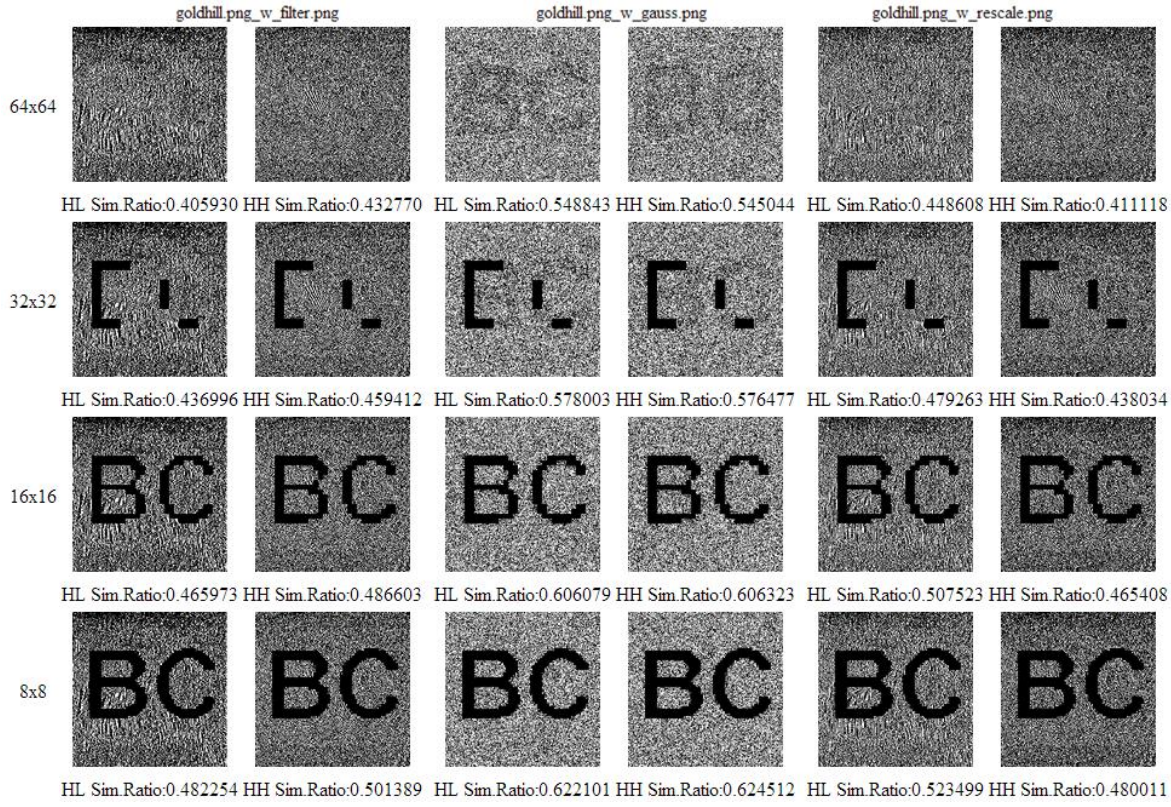
Reel zamanlı işlemlerde işlemci zamanı kritik olabilir ancak ekstra işlemci zamanını talere edebilen sistemlerde bloklu DWT ayrışma algoritmaları resmi tüm olarak ele alıp DWT ayrışmasına tabi tutan algoritmalara göre avantajlı durmaktadır.



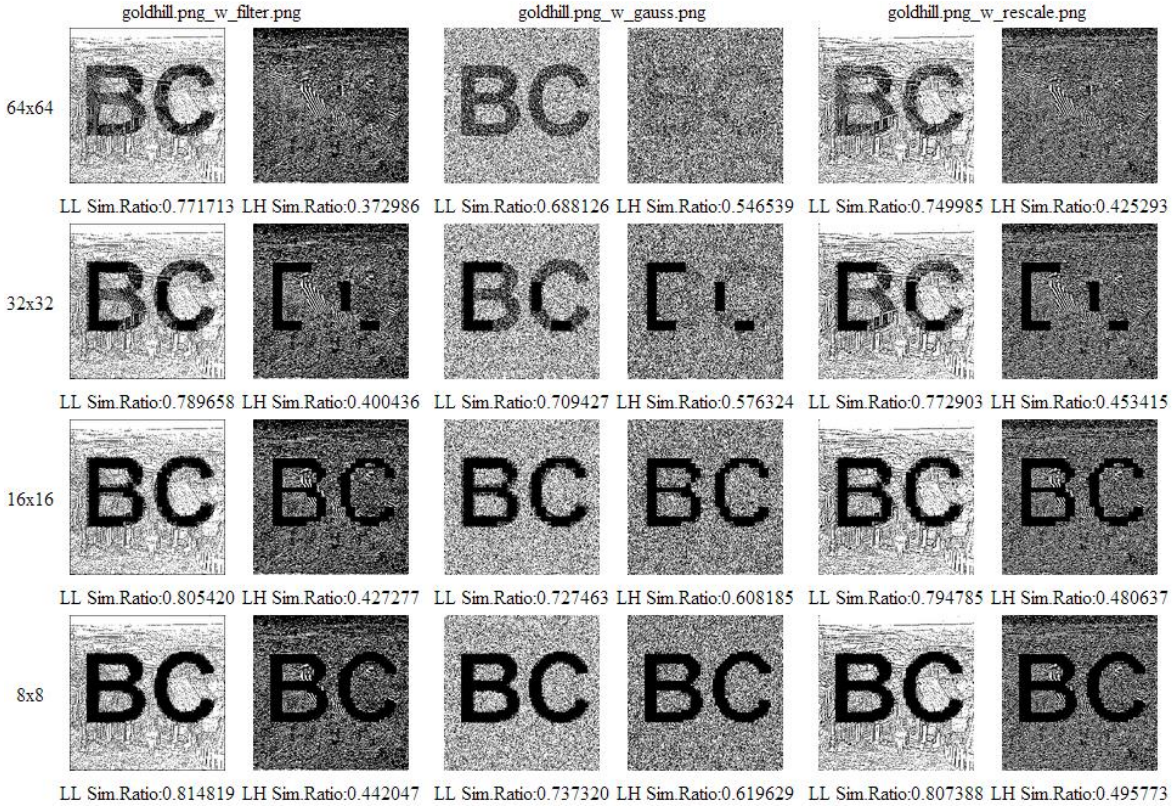
Şekil 3.4. Farklı blok büyüklükleri ile DWT tabanlı damgalandıktan sonra JPEG kayıplı sıkıştırmasına maruz kalmış resimlerin LL, LH bantlarından çıkartılan damgalar. Soldaki değerler blok büyüklüğüdür.



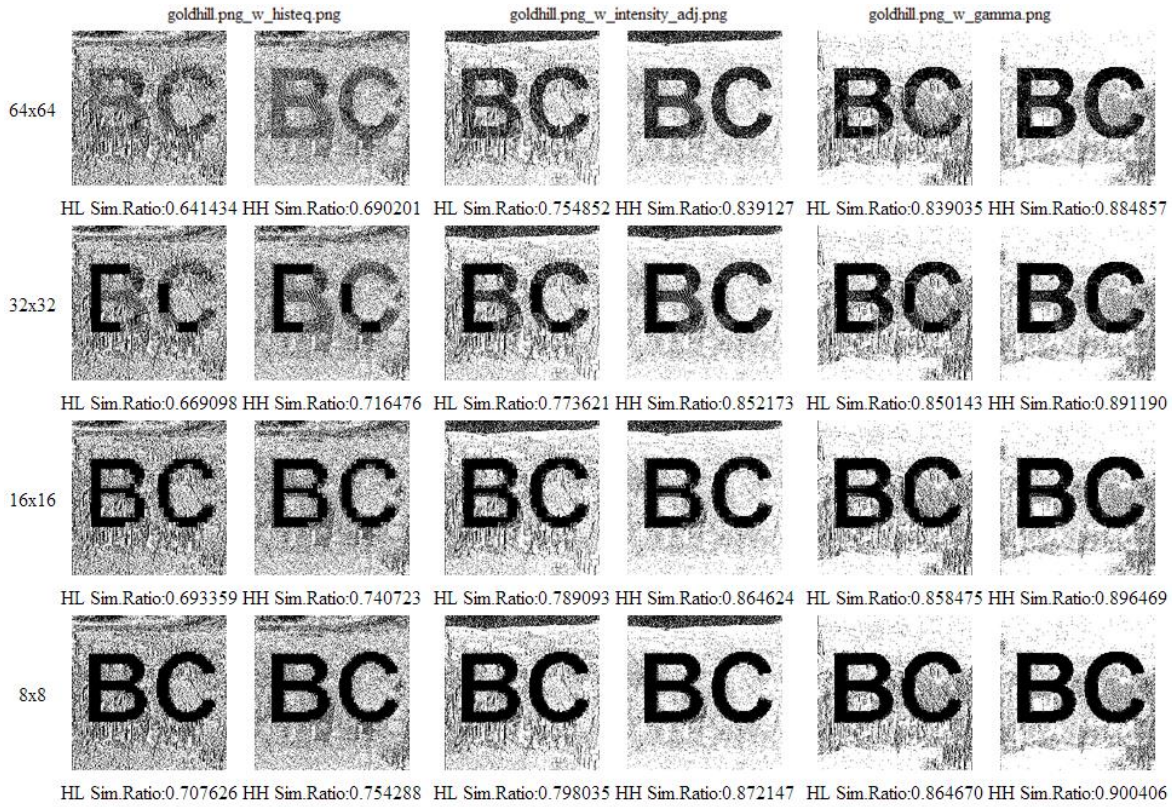
Şekil 3.5. JPEG kayıplı sıkıştırmasına maruz kalmış resimlerin HL, HH bantlarından çıkartılan damgalar.



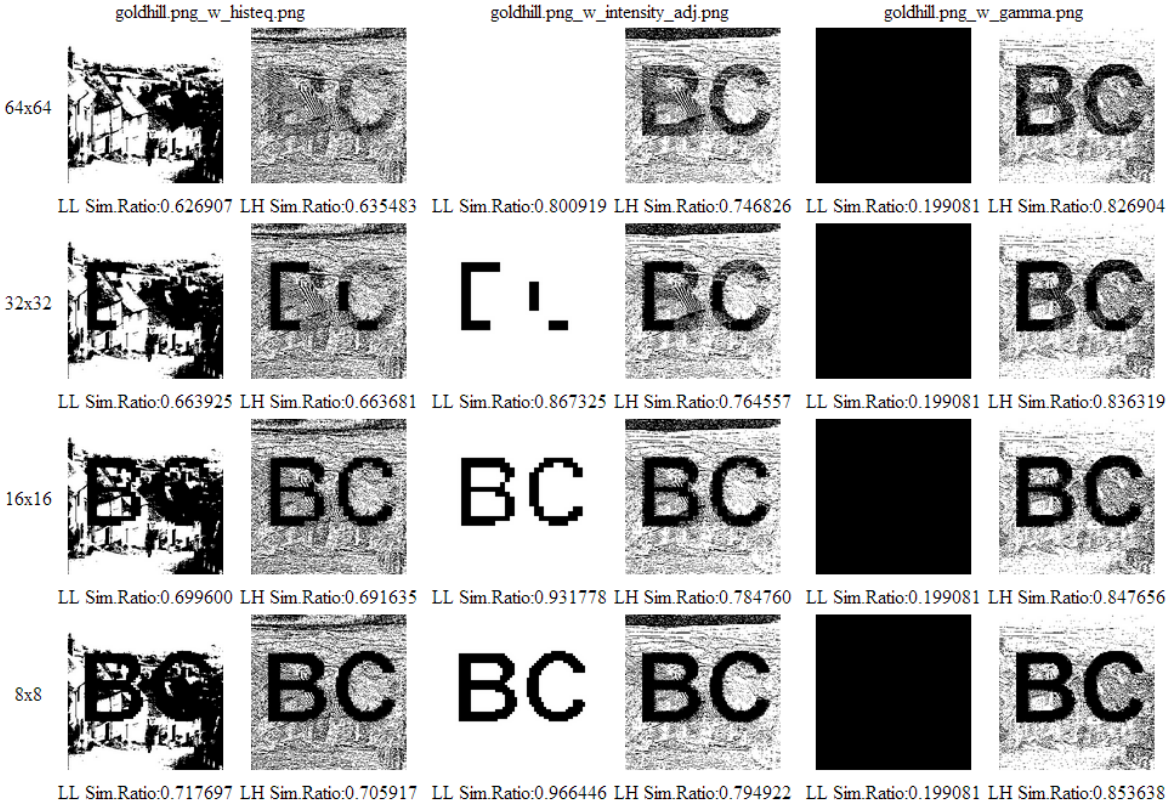
Şekil 3.6. Bulanıklaştırma filtresi, Gauss Gürültüsü, Büyültme-Küçültme işlemlerine maruz kalmış resimlerin HL, HH bantlarından çıkartılan damgalar



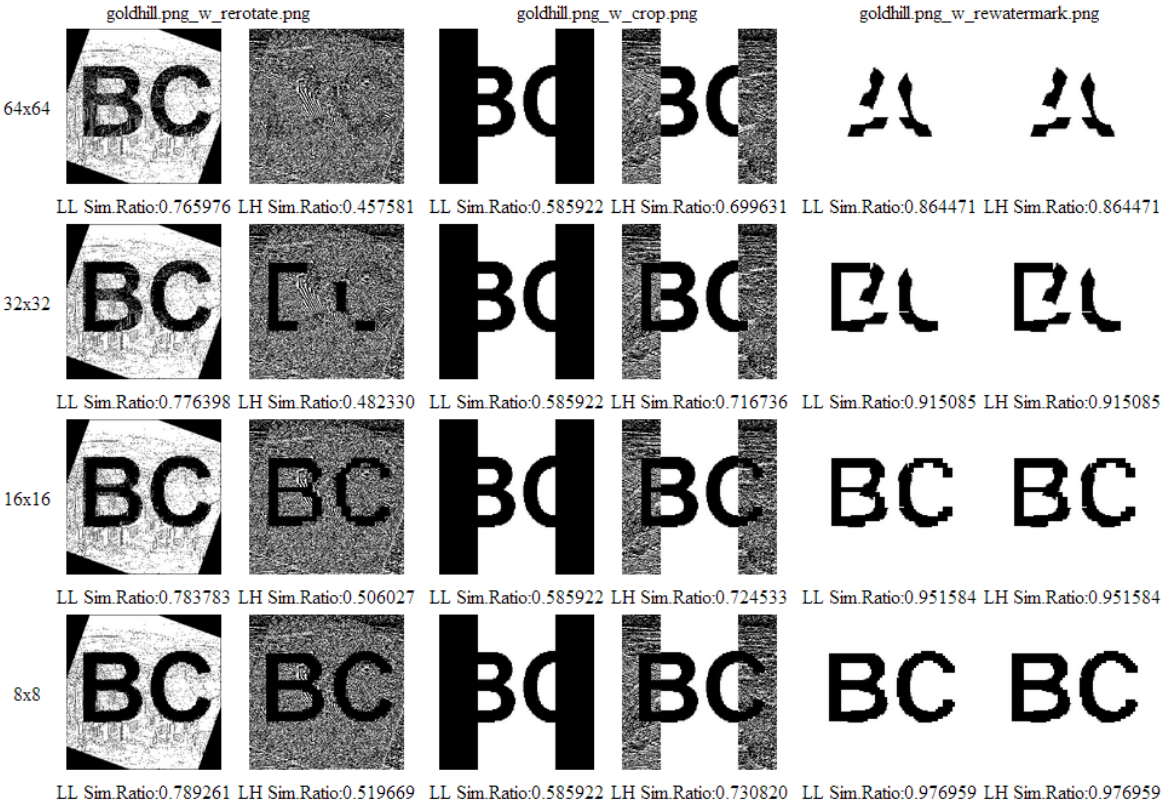
Şekil 3.7. Bulanıklaştırma filtresi, Gauss Gürültüsü, Büyültme-Küçültme işlemlerine maruz kalmış resimlerin LL, LH bantlarından çıkartılan damgalar



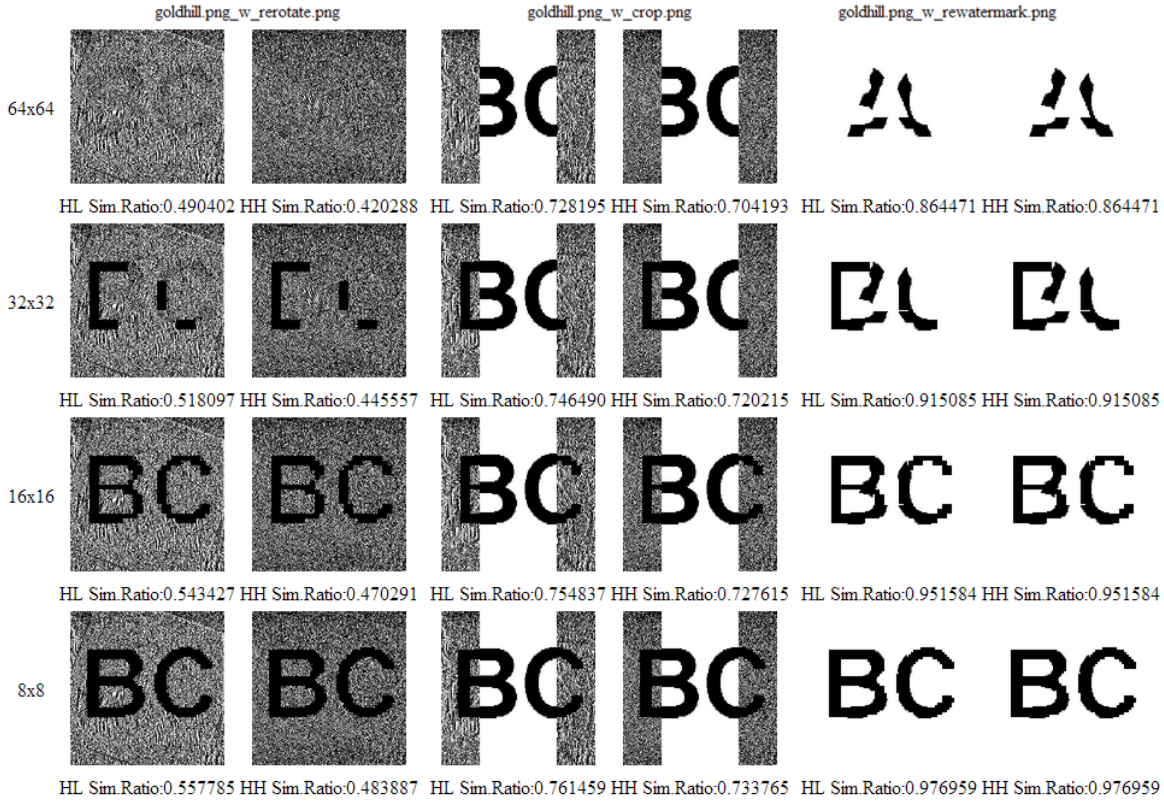
Şekil 3.8.Histogram eşitleme, parlaklık aralığı düzeltme, gamma düzeltmesi işlemlerine maruz kalmış resimlerin HL, HH bantlarından çıkartılan damgalar



Şekil 3.9.Histogram eşitleme, parlaklık aralığı düzeltme, gamma düzeltmesi işlemlerine maruz kalmış resimlerin LL, LH bantlarından çıkartılan damgalar



Şekil 3.10. Döndürme, kesme, ikincil damgalama işlemlerine maruz kalmış resimlerin LL, LH bantlarından çıkartılan damgalar



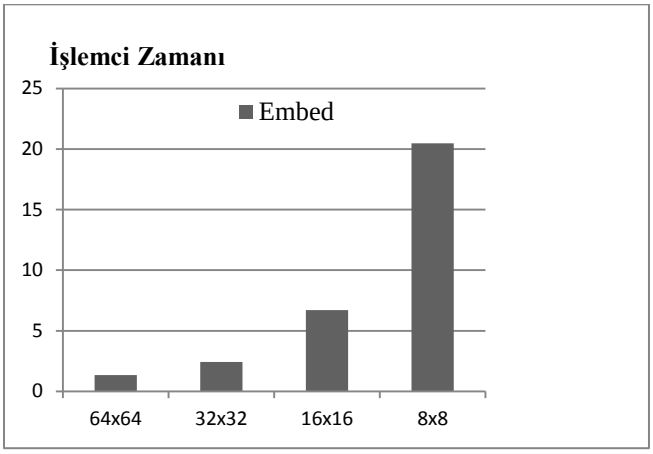
Şekil 3.11. Döndürme, kesme, ikincil damgalama işlemlerine maruz kalmış resimlerin HL, HH bantlarından çıkartılan damgalar

Tablo 3-1. Bloklu Damgalamada Damgalı ve Değişikliğe Uğramış Resimlerden Çıkartılan Damgaların SR Değerleri

	LL						**LH**						**HL**						**HH**					
	512x512	**64x64**	**32x32**	**16x16**	**8x8**	**Tao&Esk**	**512x512**	**64x64**	**32x32**	**16x16**	**8x8**	**Tao&Esk**	**64x64**	**32x32**	**16x16**	**8x8**	**Tao&Esk**	**64x64**	**32x32**	**16x16**	**8x8**	**Tao&Esk**
JPEG 75	0,898	0,898	0,905	0,912	0,916	0,920	0,453	0,453	0,481	0,506	0,520	0,619	0,479	0,508	0,536	0,551	0,632	0,414	0,441	0,467	0,481	0,617
JPEG 50	0,803	0,803	0,817	0,830	0,838	0,840	0,443	0,443	0,472	0,499	0,514	0,600	0,457	0,487	0,515	0,531	0,610	0,415	0,442	0,468	0,483	0,616
JPEG 25	0,713	0,713	0,734	0,754	0,764	0,747	0,438	0,438	0,466	0,494	0,510	0,595	0,454	0,485	0,513	0,529	0,598	0,414	0,441	0,468	0,483	0,615
FILTER	0,772	0,772	0,790	0,805	0,815	0,822	0,373	0,373	0,400	0,427	0,442	0,596	0,406	0,437	0,466	0,482	0,605	0,433	0,459	0,487	0,501	0,622
GAUSS	0,685	0,688	0,709	0,727	0,737	0,717	0,545	0,547	0,576	0,608	0,620	0,563	0,549	0,578	0,606	0,622	0,564	0,545	0,576	0,606	0,625	0,564
BÜYÜT-KÜÇÜLT	0,750	0,750	0,773	0,795	0,807	0,780	0,425	0,425	0,453	0,481	0,496	0,604	0,449	0,479	0,508	0,523	0,599	0,411	0,438	0,465	0,480	0,623
HIST. EŞ..	0,627	0,627	0,664	0,700	0,718	0,421	0,635	0,635	0,664	0,692	0,706	0,662	0,641	0,669	0,693	0,708	0,654	0,690	0,716	0,741	0,754	0,703
PARLAKLIK AYARLAMA	0,801	0,801	0,867	0,932	0,966	0,197	0,747	0,747	0,765	0,785	0,795	0,799	0,755	0,774	0,789	0,798	0,787	0,839	0,852	0,865	0,872	0,883
GAMMA	0,199	0,199	0,199	0,199	0,199	0,803	0,827	0,827	0,836	0,848	0,854	0,863	0,839	0,850	0,858	0,865	0,857	0,885	0,891	0,896	0,900	0,908
DÖNDÜRME-	0,766	0,766	0,776	0,784	0,789	0,910	0,458	0,458	0,482	0,506	0,520	0,654	0,490	0,518	0,543	0,558	0,665	0,420	0,446	0,470	0,484	0,645
KESME	0,586	0,586	0,586	0,586	0,586	0,996	0,700	0,700	0,717	0,725	0,731	0,913	0,728	0,746	0,755	0,761	0,919	0,704	0,720	0,728	0,734	0,922
YENİDEN-DAMGALA	0,864	0,864	0,915	0,952	0,977	0,905	0,864	0,864	0,915	0,952	0,977	0,905	0,864	0,915	0,952	0,977	0,904	0,864	0,915	0,952	0,977	0,904
TOPLAM	7,878	7,881	8,149	8,390	**8,526**	**8,062**	6,208	6,210	6,510	6,798	**6,954**	**7,475**	6,383	6,700	6,979	**7,144**	**7,460**	6,330	6,617	6,885	**7,040**	**7,700**

Tablo 3-2. İşlemci Zamanı – Blok Ebadı Tablosu, Damga Yerleştirme Safhası için

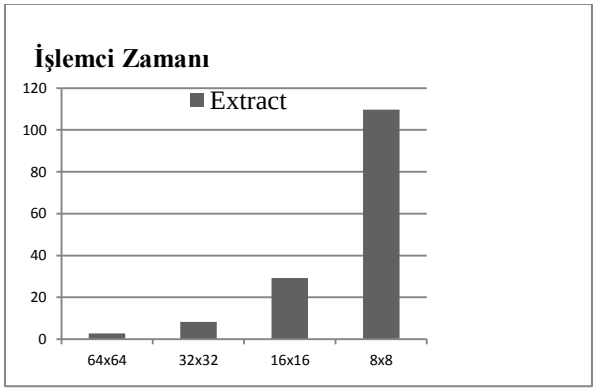
Blok Ebadı	Damga Yerleştirme İşlemci Zamanı	Blok Ebadı 4 Kat Küçüldükçe İşlemci Zamanı Artışı Oranı	Blok Ebadı 4 Kat Küçüldükçe İşlemci Hızı Artış Hızı Oranı
64x64	1.342		
32x32	2.418	1.801788376	
16x16	6.708	2.774193548	1.539688892
8x8	20.467	3.051132976	1.099827003



Şekil 3.12. İşlemci Zamanı – Blok Ebadı Grafiği, Damga Yerleştirme Safhası için

Tablo 3-3. İşlemci Zamanı – Blok Ebadı Tablosu, Damga Çıkarma Safhası için

Blok Ebadı	Damga Çıkarma İşlemci Zamanı	Blok Ebadı 4 Kat Küçüldükçe İşlemci Zamanı Artışı Oranı	Blok Ebadı 4 Kat Küçüldükçe İşlemci Hızı Artış Hızı Oranı
64x64	2.777		
32x32	8.237	2.966150522	
16x16	29.313	3.558698555	1.199770048
8x8	109.747	3.743970252	1.052061644



Şekil 3.13. İşlemci Zamanı – Blok Ebadı Grafiği, Damga Çıkarma Safhası için

3.1.3 Katkılar

Önceki DWT uzayında yapılan çalışmalarda genel olarak resim bir bütün halinde DWT uzayına alındıktan sonra damgalama yapılmakta, kaç seviye ayrışma uygulandığı ve hangi bantlara damgalama yapıldığı konusunda değişik uygulamalar görülmektedir. Tao ve Eskicioğlu çalışmasında resmi bütün olarak ele alıp LL, LH, HL and HH bantlarından her birine siyah beyaz resim damgası eklemiş, LL bandı için damga şiddet değeri diğer üç banda göre daha yüksek bir değer uygulanmıştır [6].

Bu çalışmada DWT uzayında yapılan çalışmalarda resmi bloklara bölerek her bir bloğun bağımsız olarak DWT uzayına alınması ve ardı sıra yapılan damgalama işleminin, resmi bütün olarak DWT uzayına alma ile arasındaki başarı oranı ve blok ebadının başarıya etkisi araştırılmıştır. Yapılan deneyler sonunda aşağıdaki çıkarımlara ulaşılmıştır.

1. Resmi birbiri ile çakışmayan bloklara bölerek her bir bloğu ayrı ayrı DWT uzayına alarak yapılan damgalamanın resmi bir bütün olarak değerlendirip DWT uzayına alarak yapılan damgalamadan daha başarılı sonuçlar verdiği, sahipliğin ispatı için gürbüzlüğün arttığı görülmüştür.
2. Blok ebadı küçüldükçe damgalamanın başarısının yükseldiği gözlemlenmiştir.

3. Daha küçük blok ebatlarında damga gürbüzlüğü artarken, orijinal resme benzerlikte olumsuz bir yansıma bulunmadığı, PSNR değerinin aynı kaldığı tespit edilmiştir.
4. Daha küçük blok ebadı ile daha başarılı damgalama yapılabilirken, daha fazla işlemci zamanına ihtiyaç duyulduğu, gerekli işlemci zamanının sıkıntı yaratmayacağı uygulamalar için bloklu DWT damgalamanın uygulanmasının faydalı olacağı görülmüştür.

3.2 Ana Resme Damga Olarak Vektör Resmi Damgalamak

Resim damgalamada ana resmin içine orijinalinden çıplak gözle ayırt edilmeyecek şekilde bir damga eklemek gerekmektedir. Resim damgalamada amaca göre damga kullanılır. Amaç sahipliği ispatlamak ise bir firma logosu, kişinin sesi, sahip olan kişinin resmi ana resme eklenebilecektir.

Damgalama ile ilgili ilk yapılan çalışmalarda, damgalamanın benzerlik ilkesine sadık kalmak amacıyla sözde rastgele sayı dizileri kullanılmıştır. Cox v.d. ve Piva v.d. resmin ayrık kosinüs dönüşümünü (DCT) aldıktan sonra ortalaması 0 ve varyansı 1 olan yeterli uzunlukta rastgele sayı dizisini (PRNS) DC elemanı hariç PRNS uzunluğundaki katsayıya ekleyip ters DCT ile damgalı resmi elde etmiştir [34][53]. Swanson, Zhu ve Tewfik [54], Elbaşı ve Eskicioğlu [46] [45], Barni ve Bartolini [48], Ruanaidh ve diğerleri [55], Alattar [56] resme damga olarak sözde rastgele sayı dizisi damgalamışlardır.

Schyndel, Trkel ve Osborne, resme damga olarak m-serisi (m-sequence) eklemişlerdir [15]. M-serileri lineer kaydırma register'ları kullanılarak Fibonacci kendini çağıran (recursion) ilişkisindeki bir başlangıç vektöründen üretilir. Otokorelasyon fonksiyonu ve spektral dağılımı Gauss rastgele gürültüsü gibidir.

Eskicioğlu ve Tao resmi ayrık dalgacık dönüşümüne(DWT) aldıktan sonra LL, LH, HL, HH bant değerlerine damga olarak siyah-beyaz resim değerlerini eklemişlerdir[6]. Lang ve Zhang Fourier dönüşümünün genel bir sürümü olan ve sinyalin biraz zaman biraz da frekans bileşenlerini ihtiva edebilen Kısmi Fourier Dönüşümü uzayında siyah-beyaz resim logosunu damga olarak yerleştirmişlerdir[57]. Jane, İlk ve Elbaşı resmi ayrık dalgacık dönüşümüne tabi tuttuktan sonra seçtikleri bant veya bileşenlere sırası ile LU ve SVD ayrışmalarını da uygulayarak siyah-beyaz resim damgasını eklemişlerdir [58]. Kannammal ve Rani, doğal bir resmin içerisine siyah-beyaz tıbbi resmi yerleştirdikten sonra,

damgalı resmi RSA, AES veya RC4 şifreleme algoritmalarından biri ile şifreleyerek resmin iletim ortamında şifreli gitmesini sağlamıştır. Şifrenin açılmasından sonra asıl gizli resmin doğal bir manzara resmi içerisinde kalmasını sağlayarak hastane içinde de güvenli kalmasını hedeflemişlerdir[59]. Hsieh ve Tseng[60] , Tao ve Eskicioğlu [6], Wang ve Cui [61], Aggarwal, Kaur ve Anantdeep [62], Biad, Bouden, Nibouche ve Elbaşı [63] da çalışmalarında resme siyah beyaz resim damga resmi eklemişlerdir.

Pereira ve Pun damga olarak değer kümesi {-1, 1} olan iki değerli bir sinyal dizisi kullanmışlardır. İki değerli sinyal sözde rastgele sayı dizesini andırmakla birlikte değerler {-1, 1} değerlerinden biri olmaktadır [64].

Huang ve Fang resme DCT uzayında EXIF üstverisi (meta-veri) ve BCH(Bose-Chaudhuri-Hocquenghem) hata düzeltme kodları eklemişlerdir[65]. EXIF üstverisi JPEG ve TIFF resimlerinin başlık(header) kısımlarına konan, resmin çekildiği tarih, coğrafi konum, kamera modeli, ISO hız değeri gibi değerlerden oluşan yaklaşık 150 byte'lık değerdir.

Inamdar ve Rege resmi dalgacık paket dönüşümüne alıp resme Gabor yüzü, sıkıştırılmış ses (Linear Predictive Coding LPC sıkıştırması uygulanmış) ve görünür imza olmak üzere üç biyometrik damga birden ekleyen bir yöntem geliştirmişlerdir[66].

Jinland ve Kim ana resimden kuantalama yöntemiyle elde edilen bir hologramı damga olarak kullanmışlardır [67].

3.2.1 SVG Vektör Resmi Damgası

Daha önceki damgalama çalışmalarında ne tür damgalar kullanıldığı açıklanmış, bilindiği kadarı ile ana resme damga olarak vektör resmi eklemenin denenmediği görülmüştür. Bu çalışmada gri seviyeli bir resme renkli vektör resminin damga olarak eklenmesi ve çıkarılması yapılmıştır. Çalışma, bloklu DWT-tabanlı, gürbüz damgalama çeşididir. Vektör resmin damga olarak kullanılmasının, vektör resminin renkli olması, damganın kayıpsız çıkarılma durumunda resmin sahipliğini ispatlama yönünden daha tereddütsüz sonuç vermesi yönünden önemli olduğu düşünülmektedir. Gerçek hayatta firma logoları çok büyük oranda renklidir. Ayrıca vektör resminin büyütme-küçültme işlemlerinde kalite kaybına yol açmaması onu siyah-beyaz resim damgasına karşı daha avantajlı kılmaktadır.

Çalışmaya başlarken vektör tabanlı resim formatları incelenmiş, hangi vektör resim formatının uygun olduğu araştırılmıştır. SVG vektör resim formatının yaygın olarak kullanıldığı, içeriğine kolay nüfuz edilebilir ve okunabilir XML formatında olduğu için SVG vektör resim formatı tercih edilmiştir. Svg vektör resimlerinin bir özelliği de resim dosya boyutlarının 2 kilobyte civarında olacak şekilde küçük olmasıdır. Damganın boyutunun küçük olması, damganın daha gürbüz olarak ana resme eklenmesine imkân tanıyacaktır. Şekil 3.14 de örnek bir vektör resmi ve vektör resminin SVG formatındaki içeriğinin bir kısmı görülmektedir.

3.2.2 Damgalama Ön İşlemi

Ana resme gömülecek vektör resmi önce bir sadeleştirme işleminden geçirilir. Bu işlemde, resmin görünümünü elde etmeyi engellemeyen geri uyumlulukla ilgili kısımları atılır, vektör resminin içindeki objelere verilen id alanları atılır. Vektör logo resminin içindeki rakamlar otomatik olarak parse edilerek bir dizi içine doldurulduktan sonra, svg dosyasının rakamları ihtiva etmeyen bir iskelet dosyası svgns uzantılı olarak kaydedilir. Vektör resim dosyası olan svg dosyasından çıkarılan nümerik değer dizisi svgnn uzantılı olarak kaydedilir ve damga gömme safhasında kullanılır. Ön işlemin parse adımı sonucunda oluşan bir dizi de svg dosyasından çıkartılan nümerik değerlerin tipini ihtiva eden dizidir ve svgng uzantılı olarak kaydedilmektedir. Svgng dosya içeriğinde svgnn dosyasındaki her bir nümerik değer için “tamsayı”, “RGB parlaklık değeri”, “tamsayı kısmı 0 olmayan bir reel değer”, “tamsayı kısmı 0 olan bir reel değer” anlamlarından birine karşılık gelecek bir kod konmaktadır. Bu dosya damga gömme ve damgayı geri çıkartma işlemlerinde kullanılmaktadır.

```
<g
   inkscape:label="Layer 1"
   inkscape:groupmode="layer"
   id="layer1">
  <path
     sodipodi:type="arc"
     style="fill:#002b3d;fill-opacity:0.75392671;stroke:none"
     id="path3981"
     sodipodi:cx="247.48738"
     sodipodi:cy="412.93561"
     sodipodi:rx="203.04066"
     sodipodi:ry="203.04066"
     d="m 450.52805,412.93561 a 203.04066,203.04066 0 1 1 -
406.081334,0 203.04066,203.04066 0 1 1 406.081334,0 z"
     transform="matrix(-0.81024417,-0.13180993,0.13180993,-
0.81024417,482.6141,838.79671)" />
```

Şekil 3.14. Vektör resmi görüntüsü ve XML kaynak kodundan bir kesit

Damgalama ön işlemi sırasında svgnn dizisindeki nümerik değerler analiz edilir. Svgnn nümerik değerlerindeki tamsayı olan sayıların ve RGB bant değerlerinin birleşim kümesi olan sayıların mutlak değerlerinin en büyüğü bulunur, bu sayının negatifsiz (unsigned) ikili sayı sisteminde kaç bit ile ifade edilebileceği hesaplanır ve ibc değerine atanır. Örneğin bu sayı 384 ise ibc değişkenine 9 atanır. Nümerik değerler analiz edilirken reel olan sayıların tamsayı kısımlarının da en büyüğü bulunarak yine sayının negatifsiz ikili sayı sisteminde sığabileceği bit sayısı hesaplanır ve ribc değerine atanır. Nümerik değerlerdeki reel sayıların tamsayı kısmı 0 olanların ondalık kısımlarının (iki basamağa yuvarlanmıştır) mutlak değerlerinin en büyüğü bulunup yüzle çarpılır, aynı şekilde sığabileceği bit sayısı bulunup rfbc değişkenine atanır. Bulunan bu üç değer de svgng dizisinin sonuna üç nümerik değer olarak dosyaya yazdırılmadan önce eklenir. Bulunan bu numaralar, damga ekleme ve çıkarma işleminde kullanılmaktadır.

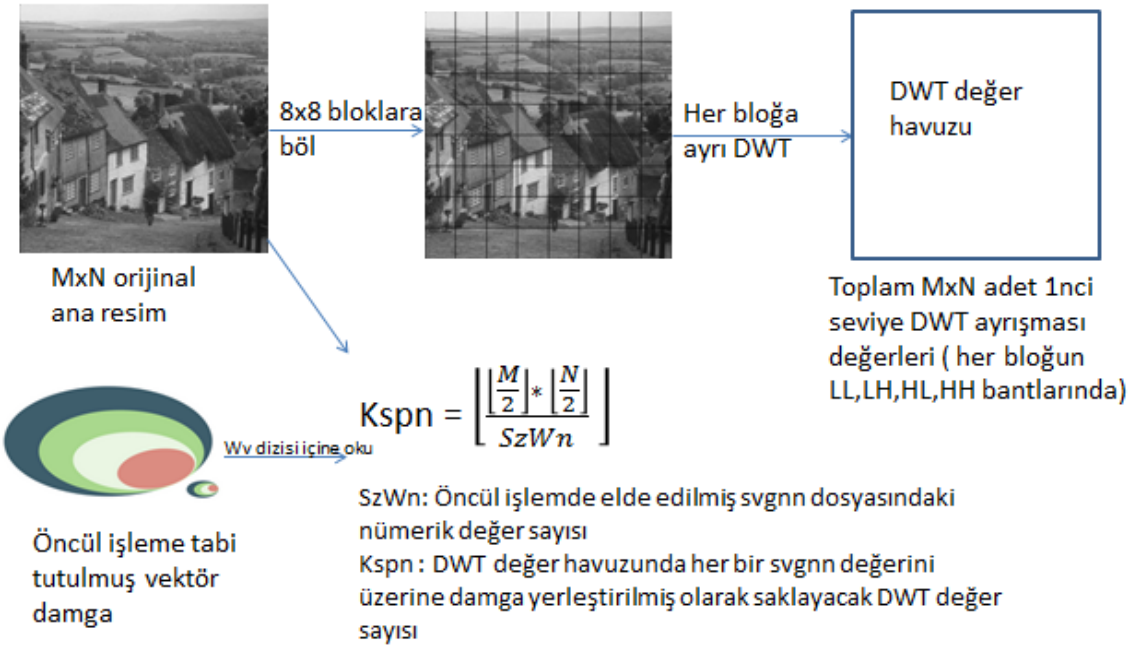
3.2.3 Damgalama İşlemi

Orijinal resim hafızaya alındıktan sonra ön işlem safhasında oluşmuş olan svgnn, svgng dosyaları dizilere okunur. ibc, ribc, rfbc değişkenlerine değerleri svgng dizisinin son üç değerinden aktarılır.

Ana resim 8x8'lik bloklara ayrılarak her bir parçanın ayrık dalgacık dönüştürmesi (DWT) yapılır. Resmi önce bloklara ayırmanın amacı, yapılacak damgalamanın daha gürbüz olmasını sağlamaktır. Resmin DWT dönüşümü sonrası Şekil 3.15'de görüldüğü gibi DWT değerler havuzu oluşur. Resim MxN boyutunda ise, LL, LH, HL ve HH bantlarının her birinde M/2*N/2 değer vardır. Svgnn dizisindeki nümerik değerler LL, LH, HL, HH bantlarının her birine ayrı ayrı yerleştirileceğinden, her bir nümerik değer, Eş.3.1' de belirtilen kspn sayısınca DWT değerine damgalanır. Her bir nümerik değerin DWT değerlerine nasıl yerleştirileceği (ekleneceği) bir sonraki adımda açıklanmaktadır.

$$Kspn = \lfloor \ (\lfloor M/2 \rfloor * \lfloor N/2 \rfloor)/SzWn \ \rfloor \qquad (3.1)$$

Her bir nümerik değerin kaç DWT değerine damgalanacağı belirlendikten sonra, nümerik değerlerin DWT değerlerine nasıl damgalanacağı belirlenmiştir. Nümerik değerler "tamsayı", "RGB parlaklık değeri", "tamsayı kısmı sıfır olmayan reel sayı", "tamsayı kısmı sıfır olan reel sayı" diye sınıflanmış ve svgng dizisine bu sınıflar okunmuştur. Sayıları 0 veya 1'lerden oluşan bit dizileri olarak düşünüp, sayının her bir bit değeri için değer 1 ise belli uzunlukta bir prsn dizisi eklemek, bit değeri 0 ise aynı uzunlukta prsn değeri çıkartmak sureti ile damgalama yapmak düşünülmüştür. Burada kod bölüşümlü çoğullama (code division multiplexing) yaklaşımı kullanılmıştır çünkü aynı DWT değerlerine 1 değeri de 0 değeri de damgalanabilmektedir [20].



Şekil 3.15. Vektör Damgası Yerleştirme

Damgalamada başarımızı resme damgaladığımız nümerik değerleri gerçeklerine ne kadar yakın elde ettiğimiz belirleyeceğinden, her bit basamağına hak ettiği önemi verme yaklaşımı benimsenmiştir. Tamsayı değerlerini damgalamada her bit değeri kaç DWT değerine damgalanacak, diğer bir deyişle her bit değeri ne uzunluktaki bir PRNS ile damgalanacak, bu bilgi prns_bc dizisinde tutulacaktır. Prns_bc dizisinin boyutu ibc olacak, Prns_bc(1) Eş.3.1.'deki ilk ve en önemsiz bit basamağının, Prns_bc(ibc) en önemli bit basamağının damgalama PRNS uzunluğunu tutacaktır. Öncelikle önemsiz önemli ayırt etmeden tüm bit basamaklarına 20 uzunluğu verilmekte, daha sonra önemli bit'lere basamağının önemi ve kspn nispetinde Eş.3.2.'deki gibi ekstra uzunluk verilmektedir. prns_r_bc dizisi tamsayı kısmı sıfırdan büyük olan reel sayılar için bit basamaklarına karşılık gelen prns uzunluklarını tutmakta; hesaplanması Eş.3.3'de görülmektedir. Tamsayı kısmı 0 olan reel sayılar için bit prns uzunlukları prns_f_bc dizisinde tutulmakta ve Eş.3.4'de hesaplanmaktadır. Kspn değerinin 1969, ibc değerinin 8 olduğu durumda prns_bc dizisi Tablo 3-4'de görülmektedir.

Tablo 3-4. Kspn=1969 olması durumunda örnek prns_bc değerleri

Bit Basamağı	7	6	5	4	3	2	1	0
Prns uzunluğu	924	472	246	133	76	48	34	27

$$kspn\_r = kspn - 20 * ibc ;$$

$$prns\_bc(y) = 20 + floor(2(y-1)/2ibc)*kspn\_r; \{ y=1..ibc\} \quad (3.2)$$

$$rbc=ribc + rfbc;$$

$$kspn\_r = kspn - 20 * rbc;$$

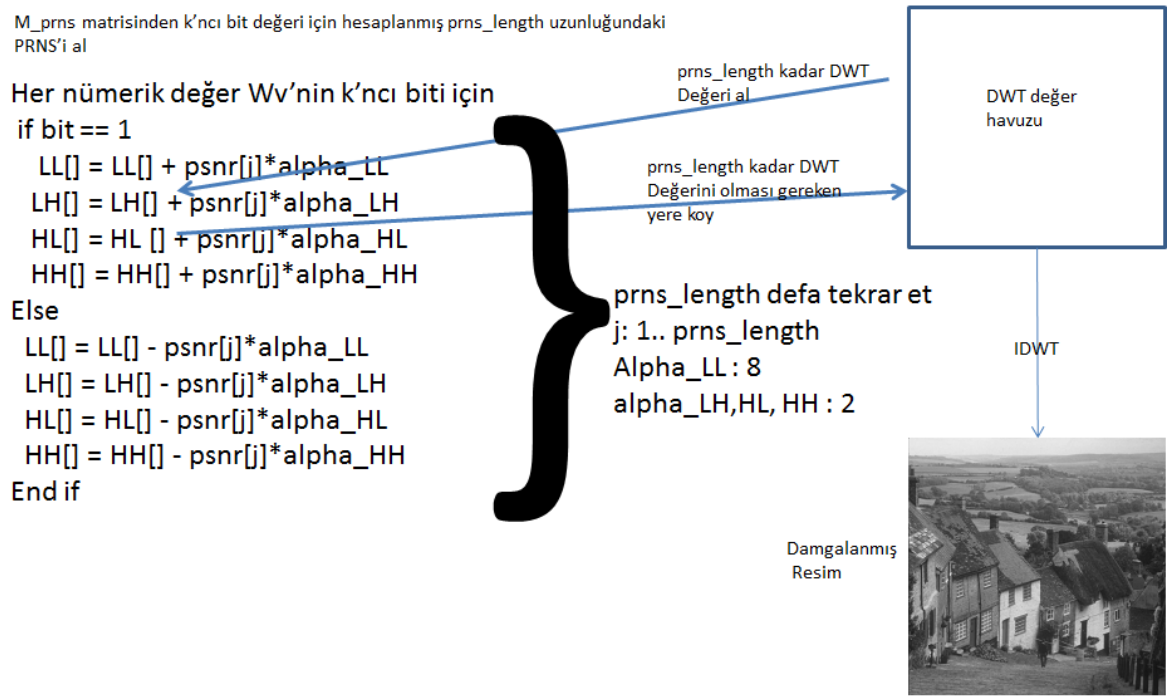
$$prns\_r\_bc(y) = 20 + floor(2(y-1)/2rbc)*kspn\_r; \{y=1..rbc\} \quad (3.3)$$

$$kspn = kspn - 20 * rfbc;$$

$$prns\_f\_bc(y) = 20 + floor(2(y-1)/2rfbc)*kspn\_r; \{ y=1..rfbc\} \quad (3.4)$$

Bit basamak prns uzunlukları hesaplandıktan sonra bu uzunluklardaki prns değerleri damga yerleştirme safhasında üretilmekte, m_prns matrisinde saklanmakta, damga geri çıkartma safhasında kullanılmak üzere dosyaya

yazılmaktadır. Damga yerleştirmenin yerleştirilen her bir bit değeri için nasıl yapıldığı Şekil 3.16'de görülmektedir.



Şekil 3.16. Vektör Damgası PRNS Ekleme

3.2.4 Deneyler ve Önerilen Vektör Damga Başarı Metriği

Kullanılan ana resim, damga olarak eklenen vektör resmi Şekil 3.17'de görülmektedir. Şekil 3.17'deki ana resim ve vektör resmi ve algoritma kullanılarak elde edilen damgalı resim Şekil 3.18 te görülmektedir.

Benzerlik yönünden ana resim ve damgalı resim arasındaki tepe sinyalin gürültüye oranı (PSNR) değeri 35.301'dir. Bu PSNR değeri resme EXIF üst-verisi damgalandığı Huang ve Fang'ın çalışmasına göre göre daha düşüktür ancak Huang ve Fang'ın çalışmasında sadece JPG %80 kalitesinde sıkıştırma, 3x3 medyan ve LP filtreleme saldırıları uygulanmıştır [65]. Bu çalışmada ise JPG%25 kalitesinde sıkıştırma ve fazladan 7 saldırı daha uygulanmış ve ikisi hariç damga başarılı olarak çıkarılmıştır. Söz konusu saldırılar damgayı geri çıkartmayı zorlaştıran ve diğerlerine göre damgaya daha zarar verici saldırılardır.

a. Orjinal Resim **b.** Vektör Resim Damgası

Şekil 3.17. Orijinal resim ve vektör damga resmi

Şekil 3.18 Vektör damgası ile damgalanmış resim. PSNR : 35.301

Vektör damgası damgalandıktan saldırılara maruz kalmış damgalı resimlerden çıkartılan vektör damgaları iki ayrı deney ve vektör damgası için Şekil 3.19 ve Şekil 3.20' da görülmektedir.

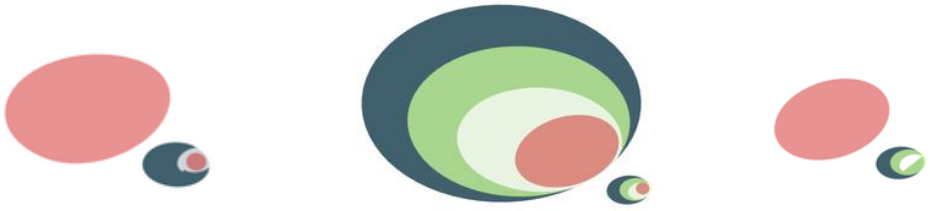
Vektör resminin damgalanmasında vektör resminden rakamların çıkarılarak resme eklenmesi söz konusu olduğundan algoritmanın başarısı iki türlü ölçülebilir: Birincisi, orijinal vektör resmini ve resimden çıkartılan vektör resmini renkli piksel tabanlı resme dönüştürdükten sonra YUV formatında parlaklık değerleri üzerinden Eş.1.7.' de verilen benzerlik değeri SR ile başarıyı ölçmek. SR değeri diğer çalışmalarda siyah-beyaz resim logosu olacağı düşünülmüştür. Bu çalışmada damga renkli vektör resmi olduğundan orijinal vektör resminin piksel değeri ile çıkartılan resmin karşılık gelen piksel değeri arasındaki farkın mutlak değeri 10'dan küçükse aynı piksel değeri kabul edilmektedir. İkinci yöntemde ise eklenen ve çıkartılan sayı dizisinin Eş.1.23' de verilen RMSE değeri başarı ölçüsü olarak alınabilir. RMSE ne kadar küçük ise başarı o kadar yüksek demektir.

Şekil 3.19’deki damga ile damgalanmış resme yapılmış değişik saldırı çeşitleri için hesaplanan SR ve RMSE değerleri

Tablo 3-5’de görülmektedir.

JPEG %50 JPEG %25 Bulanıklaştırma

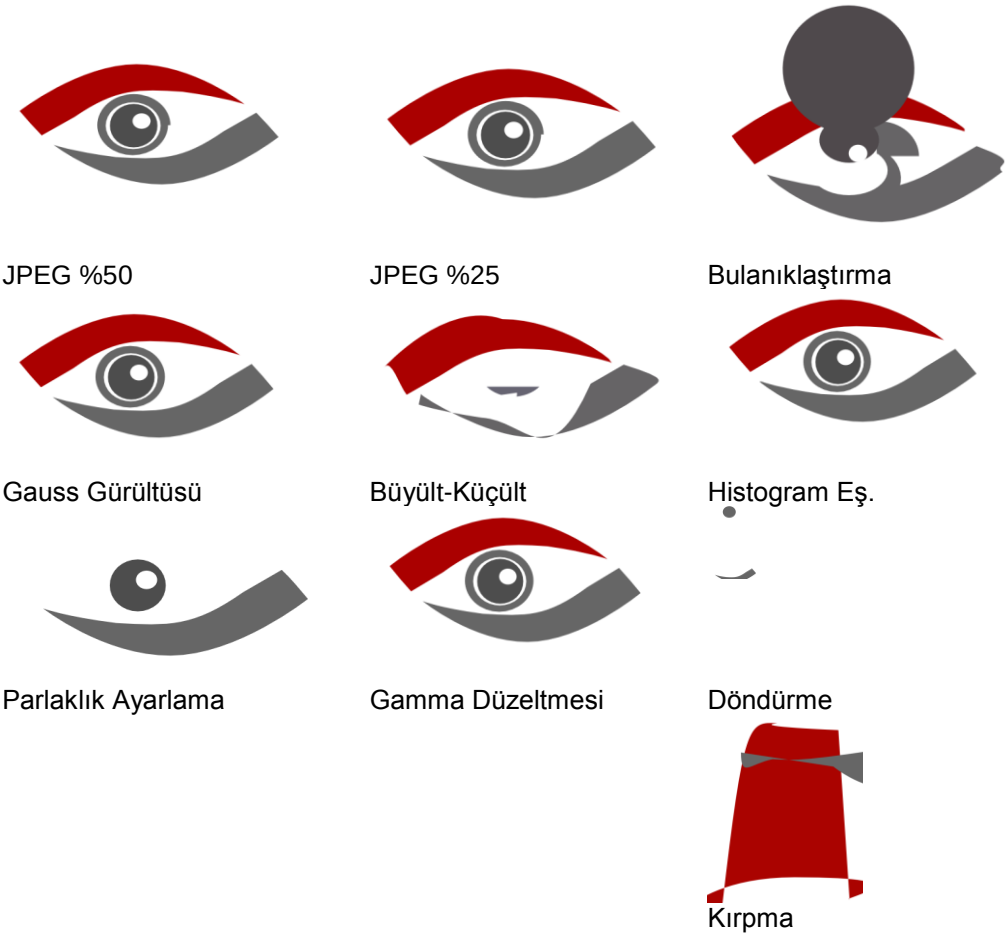
Gauss Gürültüsü Büyült-Küçült Histogram Eşitleme.



Parlaklık Ayarlama Gamma Düzeltmesi Döndürme

Kırpma

Şekil 3.19. Değişik saldırılara maruz kalmış damgalı resimlerden elde edilen vektör damgalar



Şekil 3.20. Değişik bir damga vektörü için saldırı sonrası elde edilen sonuçlar

Tablo 3-5. Vektör Damgalama Algoritması Başarı değerleri

Saldırı Çeşidi	Saldırı Yok	Jpeg %50	Jpeg %25	3x3 Filtre	Gauss Gürültüsü	Büyüt Küçült	Histogram Eşitleme	Parlaklık Ayarlama	Gamma Düzeltmesi	Döndürme	Kırpma
SR	0.982	0.982	0.794	0.95	0.982	0,546	0.982	0.471	0.982	0.725	0.598
RMSE	0.000	0.000	0.001	0.017	0.000	0.044	0.000	0.148	0.000	0.140	0.069

3.2.5 Katkılar

Damga olarak daha önce hiç denenmemiş olan vektör resmi ana resme DWT-tabanlı kör olmayan gürbüz bir yöntemle damgalanmış, değişik saldırılara uğrayan damgalanmış resimden vektör resim damgası iki saldırı cinsi hariç (kırpma, döndürme) geri çıkartılabilmiştir.

Siyah beyaz resim damgasında bir pixel bir bitlik değere karşılık gelmekte, o pikselin yanlış tespiti sadece bir pikseli etkilemekte, çıkartılan damga resminin silüeti yine de elde edilebilmektedir. Vektör resminde objelerin özelliklerinin nümerik değerleri damgalandığından değerlerin doğru elde edilememesi tamamen farklı bir görüntüde damga çıkartmamıza yol açabilmektedir. Bu haliyle vektör resmi damgalama yarı kırılgan doğrulama damgalama işlemleri için de bir potansiyel taşımaktadır. Belirli bir oranın üzerinde değişiklik uygulandığında damga bambaşka bir görüntüye bürüneceğinden yarı kırılgan damgalama için değerlendirilebileceği düşünülmektedir.

Geliştirilen yöntem döndürme ve kesme saldırılarına karşı daha kırılgandır. Damga resminin vektör resmi olması resmin sahipliğini daha tereddütsüz biçimde sağlarken resim damgalamada yeni bir açılım yapma potansiyeli taşımaktadır.

3.3 Doğrulama Amaçlı Damgalama

3.3.1 Doğrulama Amaçlı Damgalama Genel Bilgiler

Askeri alanda, sağlık alanında uydu haberleşmesinde, istihbaratta, havacılıkta, bazı ticari işletmelerde karşı taraftan gönderilen dokümanın orijinali ile aynı olduğu çok büyük önem taşıyabilmektedir.

Bilim dünyasında da resimlerde sahtecilik görülebilmektedir. 2004 yılında Güney Koreli Profesör Woo-Suk Hwang ve arkadaşları kök hücre araştırması ile ilgili önemli ilerlemeler içeren sonuçlarla ilgili bir makale yayımlamışlardır. Bir yıl sonra, yapılan araştırma sonucu makalede yayımlanan 11 resimden dokuzunun türetme ve oynama suretiyle orijinal iki tanesinden elde edildiği açığa çıkmıştır [68]. Yapılan bazı araştırmalara göre yayıma kabul edilen makalelerden yaklaşık %20'sinin manipüle edilmiş sonuçlar ihtiva ettiği, %1'nin ise sahtekârca oynamalar ihtiva ettiği tahmin edilmektedir [69], [70].

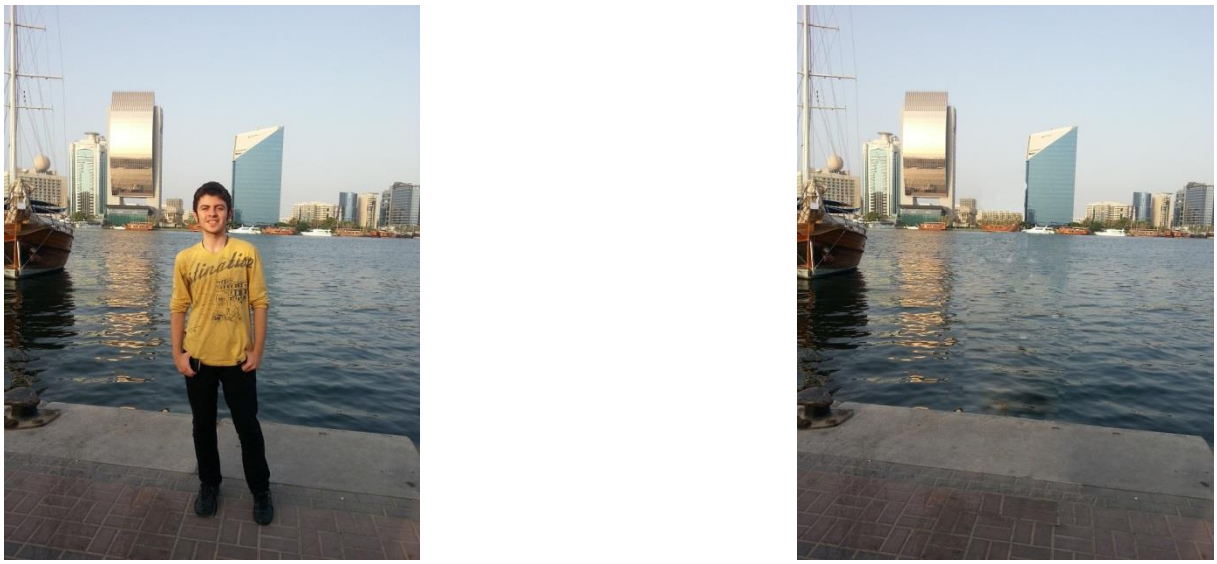
ABD'de 2004 yılının başkanlık seçim kampanyaları esnasında bazı gazetelerde John Kerry ve şarkıcı Jane Fonda 1970'lerdeki bir savaş karşıtı gösteride yan yana gösterilmiştir[68]. Fotoğraf fotomontajla elde edilmiştir. John Kerry'nin fotoğrafı 13 Haziran 1971'de fotoğrafçı Ken Light tarafından çekilmiş, Fonda'nın fotoğrafı ise Ağustos 1972'de Miami plajında bir konuşma yaparken Owen Franken tarafından çekilmişti. Şekil 3.21'da ortada fotomontaj olan resim, sol tarafta Associated Press tarafından ve sağ tarafta Owen Franken tarafından sağlanan gerçek resimler görülmektedir.

Şekil 3.21. John Kerry ve Jane Fonda'nın 1970'de bir savaş karşıtı gösteride yan yana dururken gösteren fotomontaj resim ve yanlardaki gerçek resimler.

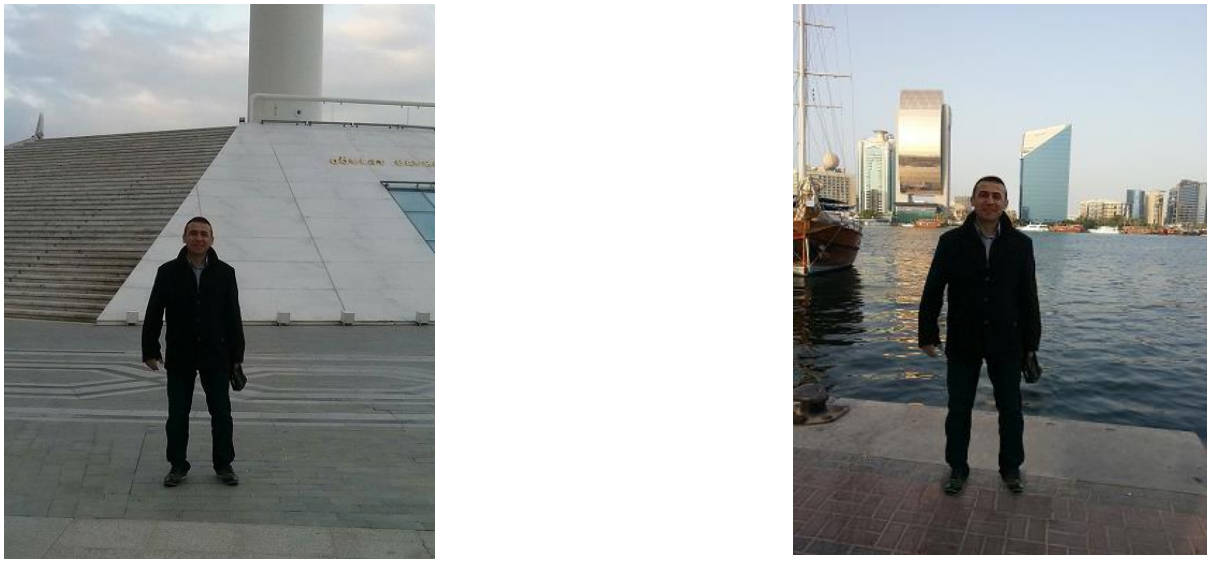
2007 sonbaharında Rusya'daki bir programda politik analist Mikhail Delyagin'in konuşması Vladimir Putin hakkındaki keskin söylemleri nedeniyle programdan silinmiş, ancak bir karede el ve ayaklarının silinmesi unutulmuştur [71].

Şekil 3.22. Rusya'da 2007 yılındaki bir tartışma programındaki görüntüsü dijital olarak silinen Mikhail Delyagin'in silinmesi unutulmuş el ve ayakları

Günümüzün katmanlı resim işleme programları ve teknolojileri ile resimlerde oynamalar yapmak oldukça kolaylaşmıştır. Şekil 3.23'de oğlum Bedirhan'ın ve Şekil 3.24'da oğlum Batuhan'ın Photoshop programı ile klonlama, kes, büyült, yapıştır, yumuşak geçiş yap gibi operasyonlarla yaptıkları resim manipülasyonları görülmektedir.

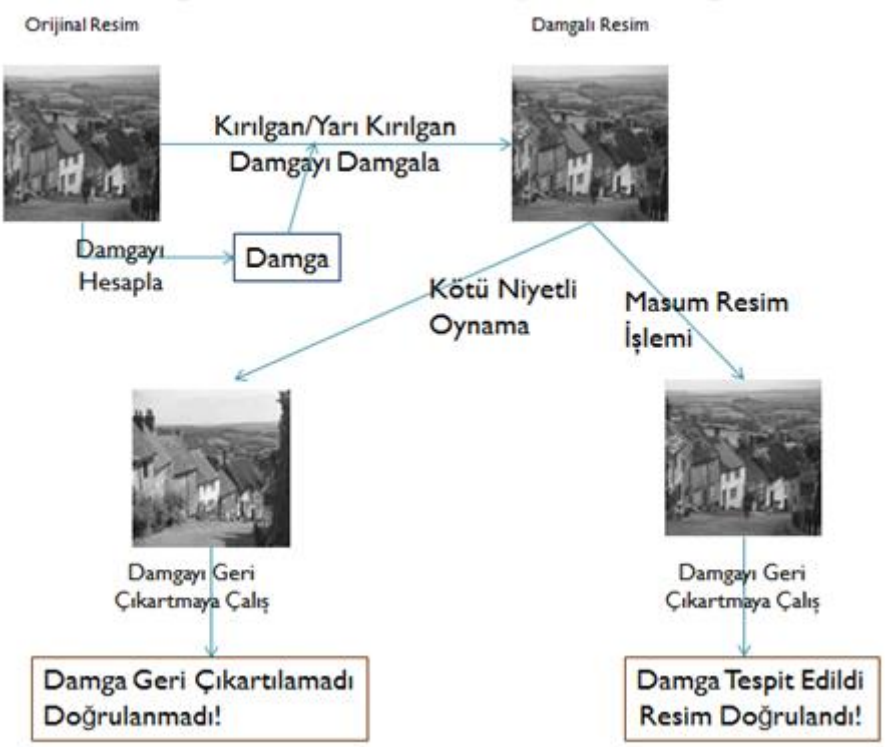


Şekil 3.23. Kopyalayarak resimde sahtecilik örneği. Solda orijinal resimde oğlum Bedirhan kopyalama yöntemiyle sağdaki resimde yokmuş gibi görülmektedir.



Şekil 3.24. Kes, yapıştır, büyüt, yumuşak geçiş yap operasyonarı ile sahtecilik örneği. Solda Azerbaycan Bakü'deki Bayrak Anıtı önünde çekilmiş orijinal resim, sağ tarafta ise aslında olmadığım bir fotoğrafa yerleştirilmiş görüntüm görülmektedir.

Doğrulama damgalaması öncelikle resimlerin orijinalleri ile aynı olduğunu tespit edebilmek amacıyla geliştirilmiştir. Doğrulama amaçlı damgalama genel hatları ile Şekil 3.25'de görülmektedir.



Şekil 3.25. Doğrulama Amaçlı Damgalama Genel Hatları

Doğrulama amaçlı damgalama aşağıdaki hedefleri gerçekleştirmeye çalışır. Bu hedeflerden bazıları bazı çalışmalarda hedeflenmeyebilir.

- Resim nasıl bir cihazla elde edildi, hangi marka, model cihaz ile çekilmiştir?
- Resim, çekildiği iddia edilen cihazla mı çekilmiştir?
- Resme uygulanan görüntü işleme operasyonları varsa hangileridir?
- Resim orijinal bir resim mi, fotomontaj mıdır?
- Resmin hangi kısımları ne tür operasyonlara maruz kalmıştır?
- Resimde değişiklik varsa resmin genel yorumunu değiştirecek bir değişiklik midir?

Doğrulama amaçlı damgalamada damga kırılgan veya yarı kırılgan olarak ana resme damgalanır. Doğrulama damgalamaları tam kırılgan ve yarı kırılgan olmak üzere ikiye ayrılır:

3.3.1.1 Tam Kırılgan Damgalama

Tam kırılgan damgalamada resme yapılacak en küçük bir değişiklikte damga geri çıkarılamaz şekilde bozulur. Dosyanın bir biti dahi değişse damga geri çıkarılamaz. Bu durumda resim doğrulanmamış olacaktır. Yüksek seviyeli güvenlik

isteyen, sözgelimi bir ülkenin güvenliğini ilgilendiren bir durumda bu hassasiyet gerekebilir.

Tam kırılgan damgalamada genel uygulama, resmin bir bölümünden bir özet (hash) değer hesaplanması, hatta bu işlem yapılırken bir anahtar değer kullanılması, sonra elde edilen bu özet değerin, resmin geri kalanına damgalanması şeklinde olmaktadır. Resmi "özet hesaplanan" ve "özetin damgalandığı" kısımlara ayırmada değişik yöntemler kullanılmıştır. Bazıları resmi piksel uzayında en önemsiz bir bit veya iki bitini önceden sıfırlayarak resmi en önemsiz iki bit değerleri, en önemli 6 bit değerleri olmak üzere iki parçaya ayırmayı yeğlemişlerdir. Ayrılan bit sayısı uygulayana göre değişebilmektedir. Dolayısıyla, en önemli 6 bit değerlerinden ve kullanılan özel anahtardan hesaplanan özet değeri, en önemsiz iki bitlere yerleştirilerek damgalama gerçekleştirilmektedir. Bazı yöntemlerde ise resim bloklara ayrılarak bazı bloklardan hesaplanan özet değeri, diğer blok üzerine damgalanmak sureti ile damgalama yapılmaktadır.

3.3.1.2 Yarı Kırılgan Damgalama

Yarı kırılgan damgalamada resme yerleştirilen damganın en ufak değişiklikte bozulması değil, resimde belirgin bir değişiklik yapıldığında bozulması hedeflenir. Resimde yapılacak masum denebilecek değişikliklerin damgayı bozmaması istenir. Damgalı bir resmi alan bir şahıs resmi yarı boyutlarına getirdikten sonra bir başka şahsa göndermek isteyebilir. Resimde keskinleştirme, koyulaştırma, parlaklığı artırma, resmin belli bir bölgesini kullanmak üzere kesme, histogram eşitleme, gamma düzeltmesi gibi işlemler içinde kötü niyet barındırmayan işlemler olarak görülebilir.

Delil sayılabilecek bir resimde olan bir kişinin resimden profesyonel resim araçları kullanılarak belli olmayacak şekilde kaldırılması veya olmayan bir kişinin o resme eklenmesi kötü niyet taşıyan işlemlerden sayılır. Bir resim veya görüntüdeki kişinin yüzünün değiştirilmesi, bir plaka yerine başka bir plaka numarasının resme konulması yine bu tür kötü niyetli işlemlerden sayılabilir. Uydudan gönderilen görüntü yakalanarak onun yerine başka bir görüntü gönderilmesi de yine kötü niyetli işlemlerden sayılabilir.

3.3.1.3 Önceki Çalışmalar

Doğrulama amaçlı ilk algoritmalardan birini Yeung ve Mintzer geliştirdi [72]. Yeung ve Mintzer'in çalışmasında [0..255] aralığındaki gri seviye değerleri {0, 1}

kümesindeki değerlere eşleştirilerek dönüştürüldü. Hangi değerin sıfır değerine hangi değerin 1 değerine izdüşümünün alındığı algoritmanın anahtarı sayıldı ve damga çıkartma-doğrulama aşamasında kullanıldı. Tablo 3-6'de örnek bir izdüşüm görünmektedir. Damga yerleştirme aşamasında yerleştirilecek 0 veya 1 bit değeri damga yerleştirilecek piksel değerinin anahtara göre karşılık geldiği bit değeri ile aynı ise piksel değeri aynı bırakılır, aynı değilse damgalanacak bit değerine karşılık gelen, anahtara göre en yakın piksel değeri ile değiştirilir. Bu hali ile algoritma piksel uzayında çalışan kırılgan bir algoritmadır. Örneğin resme yapılacak bir kayıplı sıkıştırmada veya bir filtre uygulama sonunda piksel değerleri bambaşka {0,1} değerlerine karşılık gelecek, resim doğrulanamayacaktır.

Tablo 3-6. Yeung ve Mintzer yöntemi ile yapılan piksel değerlerini siyah beyaz değerlere eşleştirmeye bir örnek

Piksel değeri	0	1	2	3	4	5	7	8	…..	251	252	253	254	255
Eşlenik Bit değeri	0	0	1	0	1	1	0	0	…..	0	0	1	1	0

Birçok doğrulama amaçlı damgalama çalışmasında damga en önemsiz bitlere (LSB) yerleştirilmiştir. Lin, Hsieh ve Huang resmi 4x4 boyutlarında birbiri ile çakışmayan bloklara böldükten sonra 4x4'lük her bloğu da 2x2'lik alt bloklara bölmüşlerdir [73]. Daha sonra resmin en önemsiz 2 biti sıfırlanmış, alt blokların ortalama piksel grilik seviyeleri arasındaki farklar hesaplanmıştır. 4x4'lük bloklar kendi arasında eşleştirilmiş, eşleştirme için Eş.3.5 kullanılmaktadır. Bloklar 1..N arası numaralandırılıp, (X, Y) blok ikilisi oluşturulurken bir k asal sayısı kullanılmaktadır. K asal sayısı 1..N-1 arasında bir asal sayı olmalıdır. Şekil 3.26'da damgayı barındıran 2x2'lik bloğun piksel değerlerinin bit yapısı görülmektedir. En önemsiz 2 biti daha önce sıfırlandığından, bu 2 bitlik alanın 2 bitine doğrulama ve parity bitleri, kalan 6 bite ise eşleştiği bloğun en önemli bitleri yerleştirilir. Doğrulama biti *v*, parity biti *p*, en önemli düzeltme ve restorasyon bitleri *r* ile gösterilmektedir. Resimde doğrulama ve oynanan yerleri restore işlemi güzel özellikler olsa da damgalama işlemi tam kırılgandır. Resmin tamamına uygulanacak bir keskinleştirme veya bulanıklaştırma işleminden veya kayıplı sıkıştırma işleminden sonra resmin tamamını oynanmış olarak nitelendirecek, tüm bloklar etkilendiği için restorasyon işlemi de yapılamayacaktır.

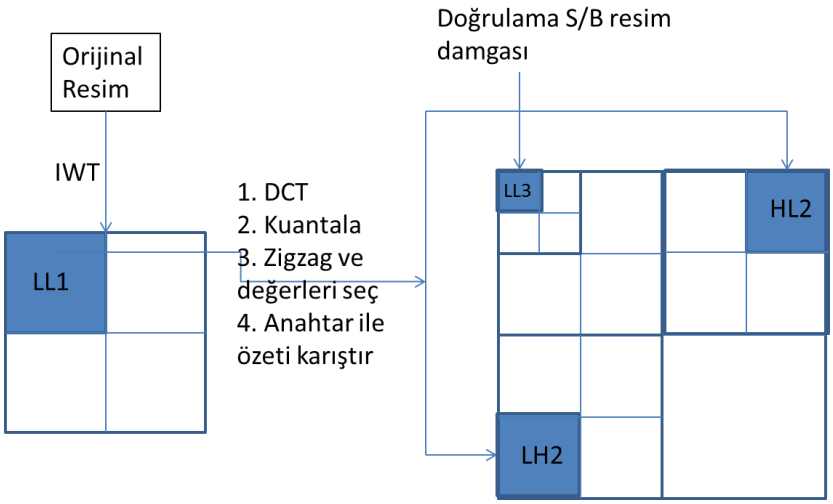
$$Y = (k * X \bmod N) + 1 \quad (3.5)$$

	Orginal Resim Verisi						Damga	
	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8
Pixel 1							*v*	*r*
Pixel 2							*p*	*r*
Pixel 3							*r*	*r*
Pixel 4							*r*	*r*

Şekil 3.26 4x4 lük blok çiftinin damgasını taşıyacak 2x2 lik 4 pikselin bit yapısı

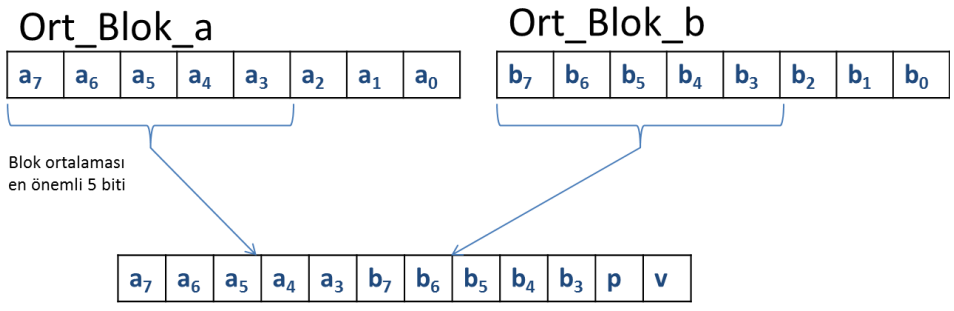
Chamlawi, Khan, Idris ve Munir DWT uzayını ve DCT dönüşümünü kullanan doğrulama ve restorasyon amaçlı yarı kırılgan bir damgalama algoritması geliştirmişlerdir. Damga olarak 2 damga birden eklemişler, doğrulama amaçlı siyah beyaz bir resim, restorasyon amaçlı ise resmin kendisinin bir özetini çıkarıp resme damgalamışlardır. Resmin özetini çıkarırken, öncelikle resmi kuantalama (quantization) işlemine tabi tuttuktan sonra zig zag gezinimiyle DC değeri hariç M adet değer seçip bir *v* vektörü içine yerleştirdikten sonra *Eş.3.6' da* olduğu gibi bir büyültme işlemine tabi tutmuşlardır. r(i) değerleri [-0.5 .. 0.5] aralığında olup α kuvvet çarpanıdır. Damgalama algoritması Şekil 3.27'de görülmektedir. Doğrulama damgasını LL3 bandına damgalarken restorasyon damgasını HL2 ve LH2 bandına damgalamışlardır. Yarı kırılgan özelliği sayesinde %70 kalite JPEG sıkıştırmasına tabi tutulmuş damgalı resmi doğrulayabilmekte olduğu yönünde sonuçlar verilmiştir.

$$V_{büyüt}(i) = v(i)\ \alpha\ log(i + 2 + r(i)) \quad (3.6)$$



Şekil 3.27. Chamlawi et.al. damgalama şeması

Lee ve Lin damgalama çalışmalarında doğrulama ve restorasyonu hedeflemişlerdir [74]. Resmi 2x2 lik bloklara böldükten sonra blokları ikişerli çiftler yaptıktan sonra her blok çiftini diğer blok çifti ile eşleştirmişlerdir. Bir blok çiftinin ortalamasının en önemli bitleri ve hesaplanan parite biti *p* ve düzeltme biti *v* ile beraber 12 bit yapmakta, bu 12 bitlik veri ise diğer eşlenik blok çiftinin her birinin en önemsiz 3 bitine yerleştirilmektedir. p ve v değerleri Eş.3.7'de görüldüğü gibidir. Hazırlanan 12 bitlik damga eşlenik 2x2 büyüklüğündeki iki bloktan her birine Şekil 3.29'deki gibi damgalanır. Her ne kadar çalışmada damgalamanın yanında restorasyon önemli bir artı ise de çalışma resimdeki piksel değerlerinin en önemsiz 3 bitini sıfırlama yöntemiyle kolaylıkla restorasyon yapabilme ve resimdeki değişiklik yapılan blokları tespit etme kabiliyetini yitirmektedir.



Şekil 3.28. Lee ve Lin çalışması 12 bitlik blok damgası oluşturma aşaması

p = a7 a6 a5 a4 a3 b7 b6 b5 b4 b3 (3.7)

$$v=\begin{cases}1 & eğer\ p=0\ ise\\ 0 & eğer\ p\neq 0\ ise\end{cases}$$

					a_7	a_6	a_5
					a_4	a_3	b_7
					b_6	b_5	b_4
					b_3	p	v

Şekil 3.29. Lee ve Lin çalışması 2x2'lik 4 pikselden oluşan bloğun 3 en önemsiz bitine 12 bitlik damganın yerleştirilmesi

Liu, Lin ve Yuan renkli bir resmi YCbCr uzayına alıp, Y kanalının DWT LL1 bandını 8x8'lik bloklara bölüp, her bloğu bir parlaklık quantalama tablosu ile işleme tabi tutarak kuantalanmış LL1 değerleri Y kanalının HH1 bandı değerlerinin yerini almıştır [75]. DWT işleminin tersi alınarak gürbüz damgalı resim elde edilmiş olur. Dayanıklı damgalı resim RGB uzayına alındıktan sonra R, G, B kanalları kırılgan damga ile damgalanır. Kırılgan damgalama piksel uzayında damgalanır. Sıfır ve birlerin rastgele dizilişlerinden oluşan damga 3^n tabanlı bir formüle göre 10'lu tabana alınır. N burada bir parametredir. Elde edilen her sayı basamağı bir bit dizisi olarak en önemsiz bitlere yerleştirilir.

Pillai ve Theagarajan doğrulama ve restorasyon amaçlı iki adet damga ekleyen bir yöntem geliştirmişlerdir[76]. Doğrulama damgası resmin DWT LL1 bandından elde edilmiştir. LL1 bandı bloklara bölündükten sonra bloklar A ve B olmak üzere iki gruba ayrılmıştır. Bir blok A'dan bir blok B'den olmak üzere bloklar çiftleşmişlerdir. Her bloğun DCT dönüşümü alındıktan sonra DCT blok değerleri diğer blok değerleri karşılaştırılmış, '<' (küçüktür) karşılaştırmasına göre 0 veya 1 değerleri almışlardır. Önemli DCT değerlerine karşılık gelen bit değer dizisi doğrulama damgası olarak hesaplanmıştır. Ana resmin DWT HL1 bandının 2nci seviye DWT ayrışması sonucu LH2 ve HL2 değerleri damgalanacak bit değerinin 0 veya 1 olmasına göre α değerine bölünmüş veya α değeri ile çarpılmıştır. Restorasyon damgası, resmin DWT LL3 bandının quantalanması sonucu elde edilmiş, resmin HL1 bandının en önemsiz bitlerine damgalanmıştır. Çalışmada restorasyon

damgasından ve damgalanmasından bahsedilse de restorasyon kısmı ile ilgili deneyler ve sonuçlar paylaşılmamıştır.

3.3.1.3.1 Blok Tabanında Bağımsız Damgalama Türlerine Yapılabilen Saldırılar

Holliman ve Memon, bloklara ayrıldıktan sonra blokların birbirinden bağımsız biçimde damgalandığı damgalama algoritmalarının nasıl saldırıya uğrayabileceğini, elde damgalama algoritması ve anahtar olmadan doğrulama damgası ihtiva etmeyen bir resmin doğrulama damgası ihtiva eder hale nasıl getirilebiceği üzerine bir çalışma yapmıştır [7]. Saldırının genel sistematiği şöyle çalışmaktadır. X resmi {X1, X2, … Xn} bloklarından oluşur ve Xi bloğuna Wi damgasını Ki anahtarını kullanarak damgalar. Blok tabanında bağımsız damgalama demek, damgalı Xi' bloğu damgalanırken sadece orijinal Xi bloğu, Wi damga bloğu ve Ki anahtarına bağımlıdır ve aşağıdaki şekilde damgalanır.

for i=1 to blok_sayisi

Xi' = Damgala (Xi, Wi, Ki)

Verilen bir K anahtarı için Xi ve Xj bloklarından geri çıkartılan damga Eş.3.8'i sağlayacak şekilde eşit ise Xi ve Xj blokları K-eşit sayılır.

$$Damga\_cikarK(Xi) = Damga\_cikarK(Xj) = W \quad (3.8)$$

Bu durumda resim bloklarından elde edilen birbirinden değişik m adet damga var ise, {C1, C2, …, Cm} şeklinde K-eşit grupları vardır. Bu durumda Xi' ve Xj' aynı K-eşit grubunda ise Xi' ile Xj' resimde değiştirildiğinde resmin doğrulanmasında sıkıntı olmayacaktır. Aşağıdaki algoritma kullanılarak anahtara gerek olmadan damgasız resim damgalı hale getirilebilecektir. Elde damgalı olduğu bilinen resim sayısı ne kadar fazla ise, her bir K-eşit grubundaki değişik blok sayısı o kadar fazla olacak, bu bloklardan Yi ye daha çok benzeyen damgalı Xj' bloğu bulma olasılığı artacak, bu yolla elde edilen damgalı resmin orijinaline benzerlik değeri (PSNR) artacaktır.

X' = {X1', X2', … Xn'} :W damgalı resim

Y = {Y1, Y2, … Yn} : Elde anahtar ve algoritma olmadan damgalı hale getireceğimiz resim

For i = 1 to blok_sayisi

Xi' bloğunun K-eşit grubunu tespit et

Yi ye benzeyen Xi' bloğunun K-eşit grubundan Yi' bul

Yi nin yerine Yi' yi koy

Yeung ve Mintzer'in çalışması ile damgalanmış bir resimde blok büyüklüğü 1x1 yani 1 piksel gibi düşünülüp 2 adet K-eşit {C0, C1} grubu oluşacaktır. Yani sıfır değerine karşılık gelen piksel değerleri ile 1 değerine karşılık gelen piksel değerleri. Saldırganın elinde doğrulama programı mevcut ise ve elinde bir adet doğrulanmış resim var ise, bir pikselin değerini her defasında 0.255 arası farklı bir piksel değerine set edip doğrulama algoritmasını tekrar çalıştırmak sureti ile 0..255 arasındaki tüm piksel değerlerinin damga olarak sıfıra mı bire mi karşılık geldiği bulunmuş olacak, 255 denemede gizli olduğu iddia edilen anahtar açığa kavuşturulmuş olacaktır. Elde hangi pikselin damgalı halde sıfıra veya bire karşılık geldiği bulunduktan sonra, damgasız bir resimdeki piksel değeri eğer olması gereken damga değerine {0 veya 1} karşılık geliyorsa değiştirilmeyip olduğu gibi bırakılacak, değiştirilmesi gerekiyorsa olması gereken damga değerine karşılık gelen en yakın piksel değeri ile yer değiştirecektir.

Söz konusu saldırı çeşidine önlem olarak, daha büyük bloklara ayırmak ve damgalamanın blok-bağımsız olmasını engellemek sayılabilir. Eşitlik 3.9'da görüldüğü gibi Xi bloğunun damgalı Xi' bloğuna dönüşmesi için bloğun kendisi Xi, damga Wi, anahtar Ki nin yanı sıra, Xj bloğundan elde edilen bir değer de olacaktır. Bu duruma örnek olarak blokların gizli bir anahtar ile birbiri ile eşleştirilmesi, bir bloğun damgalanması esnasında eşleştiği diğer bloğun piksel ortalamasının da kullanılması örnek verilebilir

Xi' = Damgala (Xi, Wi, Ki, f(Xj)) (3.9)

Wolfgang ve Delp bir çalışmalarında doğrulama amaçlı bir tam kırılgan, bir de yarı-kırılgan damga geliştirilmişlerdir [77].Tam kırılgan damgalamada, resmin özet değeri ve zaman damgası kullanılması ile bir bitlik bir değişiklik bile resmin doğrulanamamasına yol açmaktadır. İki boyutta değişken damgalı VW2D adını verdikleri çalışmalarında, çalışma resimlerini "orijinal", "hafif oynanmış", "orijinal resimden türemekle birlikte epey oynanmış", "original resimden türeyemeyecek şekilde tamamen değişmiş" şeklinde sınıflandırma yapabilmektedir.

Wong, değişiklikleri piksel düzeyinde tespit edebilen bir çalışma geliştirmiştir [78]. Resmi bloklara böldükten sonra resmin M,N ebatlarını, özet değerini tutacak diğer bloğun içeriğini, damgalama yapan kişinin güvenlik anahtarını kullanarak MD5 değeri hesaplamıştır. Doğrulama yapacak tarafta ise, resmin ebatları, göndericinin public anahtarı, MD5 içeriğini barındıran blok içeriği bulunmaktadır. MD5 barındıran bloğun en düşük öneme sahip basamaklarında diğer bloğun MD5 özet değeri barındırılmaktadır.

Tez çalışmaları kapsamında iki adet doğrulama algoritması geliştirilmiştir. Bu algoritmalar bölüm 4.2 ve bölüm 4.3'te açıklanmıştır.

3.3.2 Doğrulama Damgalama Algoritması KırılganDoğKenarTopOrtDWT

KırılganDoğKenarTopOrtDWT algoritması resmi 8x8'lik bloklara böldükten sonra her bir bloğu birbirinden bağımsız olarak 1nci seviye DWT dönüşüm uzayına alıp blokları çiftler haline getirip çiftlerden ikinci bloğun HL, LH, HH bantlarından hesaplanan değeri birinci bloğun LL1 bandına damgalar. Algoritmanın damga yerleştirme kısmı 4.2.1 bölümünde, damga doğrulama kısmı 4.2.2.'de açıklanmıştır.

3.3.2.1 Damga Ekleme Algoritması

1. Resmi birbiri üzerine binmeyen 8x8 büyüklüğünde bloklara böl

2. Her parçanın DWT dönüşümünü herbiri kendi içinde ayrı olmak üzere yap

3. 8x8'lik blokları birbiri ile eşleştir

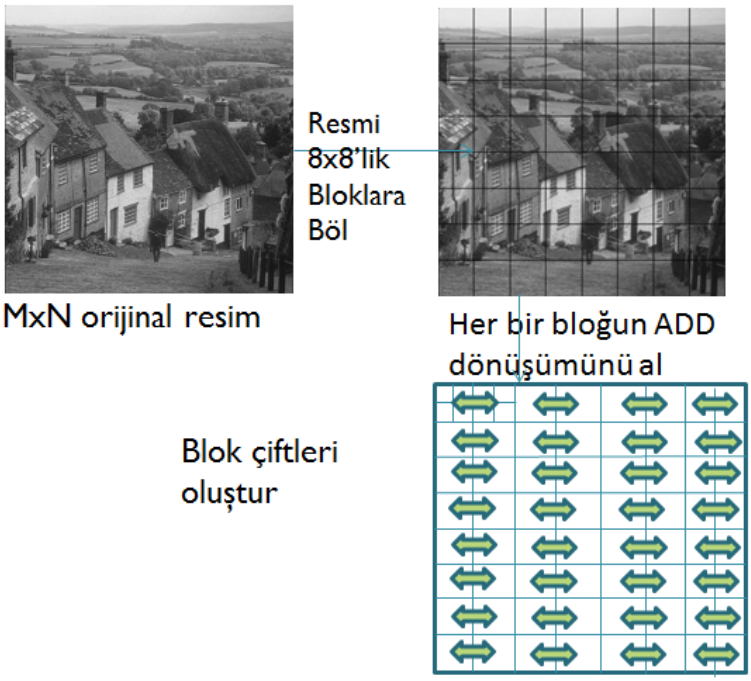
Eşleştirilen çiftlerdeki her bir ikinci blokda her bir (i,j) DWT değeri için

```
If toplam (HL_2(i,j)+ LH_2(i,j)+ HH_2(i,j) ) <= Sınır_değer
    LL_1(i,j) = zemin(LL_1(i, j )/10)*10 + 2; /* zemin : floor fonksiyonu
else
    LL_1(i,j) = zemin(LL_1(i, j )/10)*10 + 7;
```

4. DWT ters düşümü yap ve damgalı resmi elde et.

Burada resmi parçalara bölmekteki maksadımız, resimde yapılan değişikliklerin yerini belirleyebilmektir. Eşleştirilen bloklarda bir blokta hesaplanan değer, diğer bloktaki karşılık gelen değere damgalanmaktadır. Damgalama işlemi Şekil 3.30 de görülmektedir. LL değerini 10'a bölüp bu değeri Zemin (floor) fonksiyonuna

soktuktan sonra tekrar 10 ile çarparak LL değeri ondalık son basamağı sıfırlanmaktadır. Daha sonra bu basamak değerine 2 değerini atayarak LL değerine sıfır değeri damgalamış oluyoruz. Diğer durumda ise LL değerinin ondalık son basamağına 7 değeri atanmış olmaktadır. 2 değeri {0,1,2,3,4} değerleri için ortalama ve medyan değeri, 7 değeri ise {5,6,7,8,9} değerleri için ortalama ve medyan değeridir. Bu şekilde ortalama değerler kullanılarak, resimde yapılabilecek küçük çaplı değişikliklere karşı dayanıklılık ve belirli bir esneklik sağlanmaya çalışılmaktadır.



Şekil 3.30. KırılganDoğKenarTopOrtDWT Damga Yerleştirme Safhası

3.3.2.2 Doğrulama Algoritması

Algoritmanın doğrulama adımları aşağıda verilmiştir. Doğrulama algoritması Şekil 3.32'de görülmektedir.

1. Resmi birbiri üzerine örtüşmeyen 8x8 lik bloklara böl

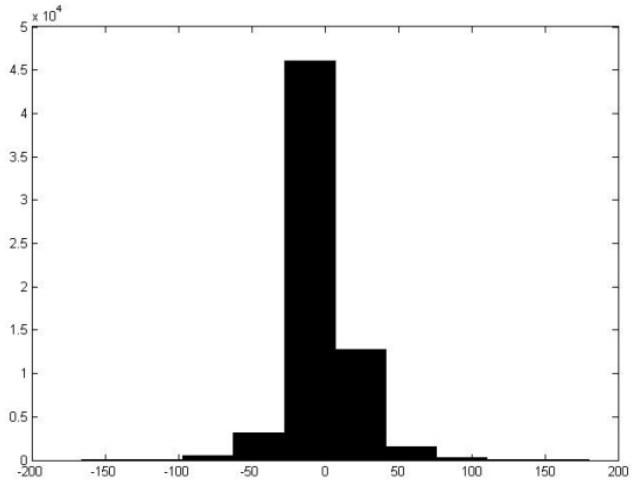
2. Her bloğu kendi içinde DWT dönüşümüne al

3. 8x8'lik blokları ikişerli eşleştir

   a. İkinci bloktaki her bir (i,j) DWT değeri için

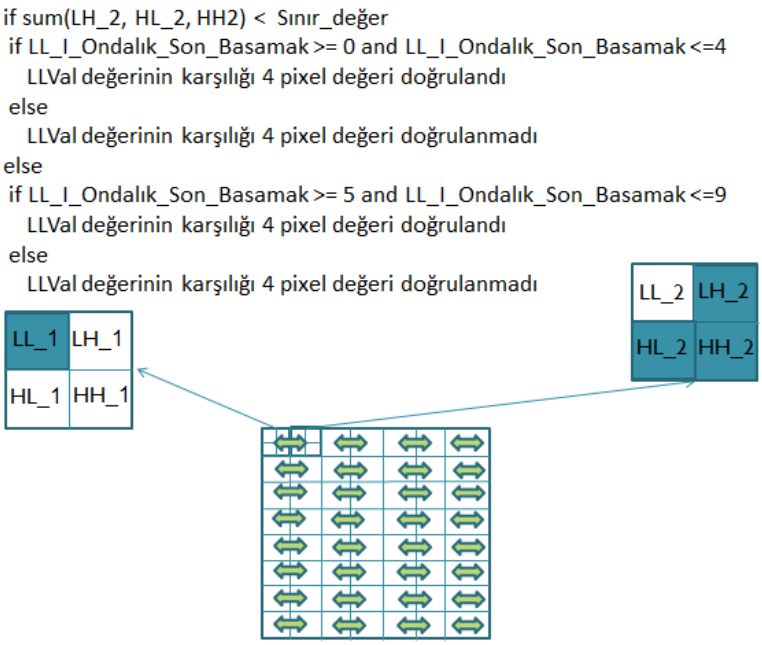
      toplam= (HL_2(i,j)+ LH_2(i,j)+ HH_2(i,j))

```
if ( toplam <= Sınır_değer  )
    if (LL_1(i,j) >=0 and  LL_1(i,j) <=4        )
            bu LLVal değerine karşılık gelen 4 piksel değeri doğrulanmıştır.
    else
            bu LLVal değerine karşılık gelen 4 piksel değeri doğrulanamamıştır.
    end if
else
    if (LL_1(i,j) >=5 and  LL_1(i,j) <=9 )
             bu LLVal değerine karşılık gelen 4 piksel değeri doğrulanmıştır.
    else
             bu LLVal değerine karşılık gelen 4 piksel değeri doğrulanamamıştır.
    end if
end if
```



Şekil 3.31. Örnek bir resmin toplam(LH, HL, HH) değerleri histogramı

Sınır değeri belirlerken, toplam (LH, HL, HH) değerleri analiz edilmektedir. Bu değerlerin histogramı Şekil 3.31'de görülmektedir. Histogram analiz edildiğinde sıfır ve bir atanacak damga değerlerinin birbirine yakın olması hedeflendiğinden her bir blok için toplam (LH, HL ,HH) değerine karşılık gelecek {0,1} değeri bulunurken kıyaslanacak sınır değeri 8.13 olarak hesaplanmıştır.



Şekil 3.32. KırılganDoğKenarTopOrtDWT Resim Doğrulama Safhası

3.3.2.3 Deneyler

Deneylerde gri seviyeli resimler kullanılmıştır ancak algoritma renkli resimlerin YUV formatına alınması ile veya renkli resimlerin her renk bandının ayrı ayrı damgalanması ile rahatlıkla uygulanabilecektir. Şekil 3.33.'de orijinal ve damgalanmış resim görülmektedir. Damgalanmış resmin PSNR değeri 45.738338 oldukça yüksek bir değer olup algoritmanın orijinal resme benzerlik yönünden iyi olduğunu göstermektedir. Algoritma 8x8 blok büyüklüğü ile denenmiştir ancak 128x128, 64x64, 32x32, 16x16 blok ebatlarıyla da kolaylıkla çalıştırılabilmektedir. Blok büyüklüğü arttıkça resim üzerinde yapılan oynamaların hangi kısımda yapıldığına dair hassasiyet de o oranda azalacaktır.

Damgalı resim, resimdeki iki adet bacanın kopyala yapıştır yöntemi ile ortadan kaldırıldığı bir şekilde değiştirilmiştir. Değişikliğe uğrayan resim Şekil 3.34.a.'da görülmektedir. Doğrulama algoritması değişikliğe uğrayan resim üzerinde çalıştırılmıştır. Doğrulama hedefli damgalama algoritmalarında original damgasız resmin elde olmadığı varsayıldığından, yapılan doğrulama deneylerinde original resim kullanılmamıştır. Doğrulama işlemi sonucu Şekil 3.34.b.'de görülmektedir. Algoritma değişiklik tespit ettiği blokların dörtte birine beyaz (255) piksel değerini atamaktadır. Değişikliğe uğrayan bacaların olduğu yerler Şekil 3.34.b.'de işaretlenmiş olarak görülmektedir. Kaldırılan bacaların yerine konan bazı blok

çiftleri şans eseri damgalama kıstasını sağladığından değişmemiş gibi görülmekte, ancak bu durumda olanların oranı oldukça az olduğundan resimde değişmiş kısım rahatlıkla ayırt edilebilmektedir.

a. b.

Şekil 3.33. Doğrulama Algoritma1 a.orijinal resim b. damgalanmış resim PSNR:45.79

a. b.

Şekil 3.34. a. İki bacası ortadan kaldırılmış damgalı resim b. Üzerinde oynanmış resmin doğrulama işlemi sonucu

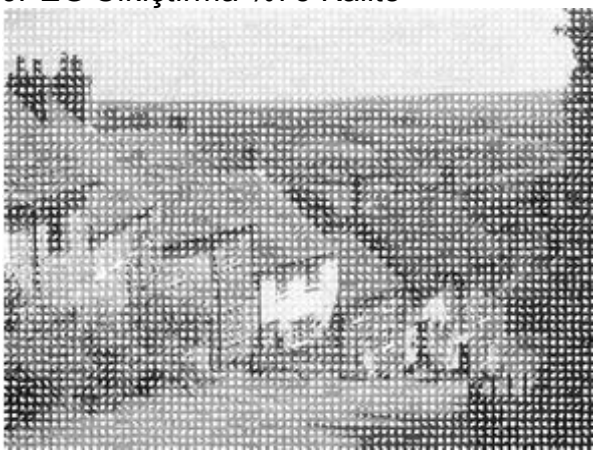
Doğrulama algoritması resme yapılabilecek genel değişikliklere karşı nasıl doğrulama yapacağı ile ilgili de denenmiştir. Şekil 3.35'da doğrulama sonuçları gösterilmektedir. Kayıplı sıkıştırma, 3x3'lük bulanıklaştırma filtresi, Gauss gürültüsü, büyültme-küçültme, histogram eşitleme, gamma düzeltmesi gibi kötü amaçlı değerlendirilemeyecek işlemlerde resmin tamamı değişmiş gibi blokların işaretlendiği görülmektedir. Kırpma işlemlerinde ise kırpılan bölüm

işaretlenebilmektedir. Alınan sonuçlar algoritmanın kırılgan tipte bir doğrulama damgalama algoritması olduğunu göstermektedir.

Algoritma başka iki resimle daha denenmiş, Şekil 3.36 ve Şekil 3.37'de görüleceği gibi başarılı bir şekilde değişiklik yapılan kısımlar işaretlenmiştir.

JPEG Sıkıştırma %75 Kalite

Bulanıklaştırma 3x3 filtre

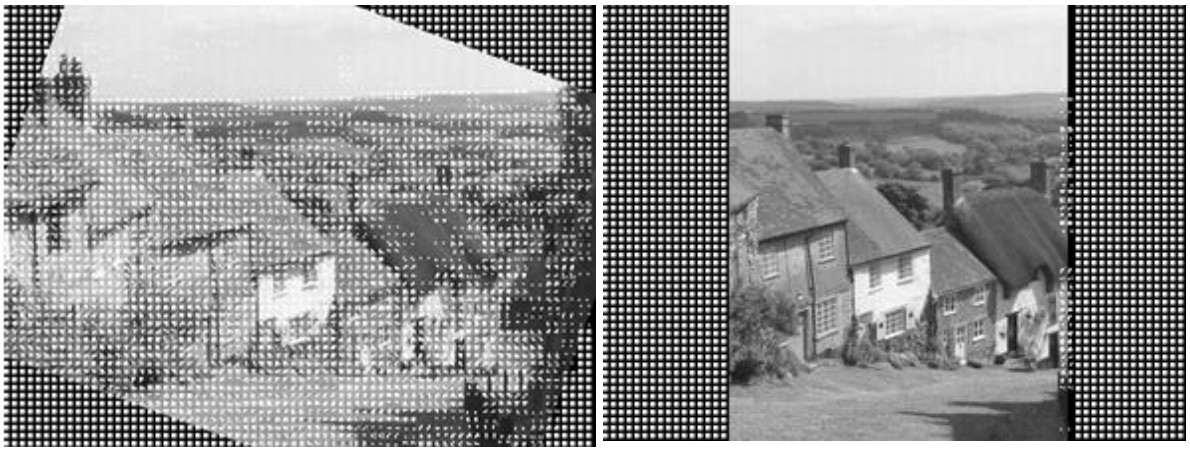


Gauss Gürültüsü

Büyültme-Küçültme

Histogram Eşitleme

Gamma Düzeltmesi

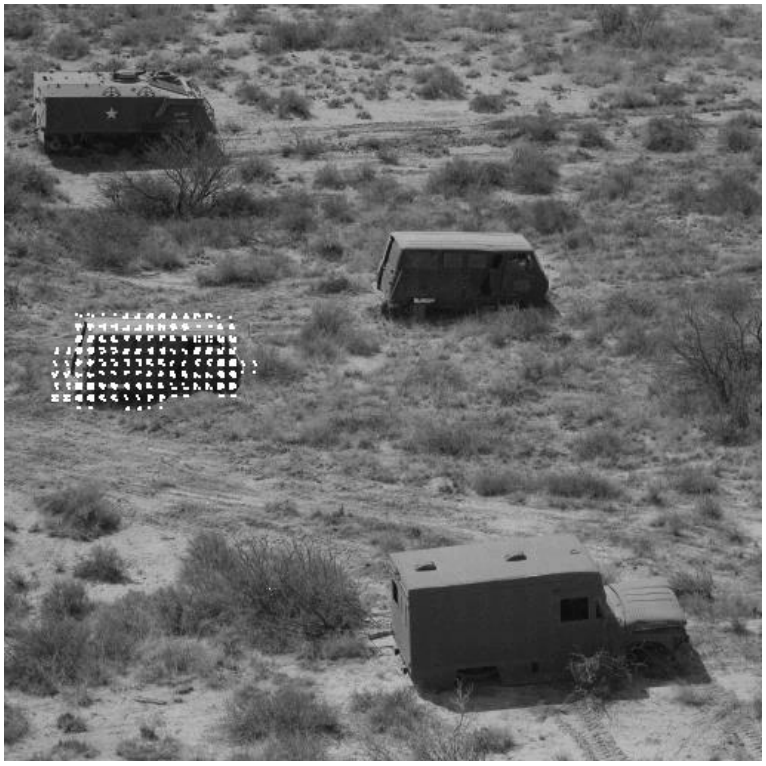


Döndürme Kırpma

Şekil 3.35. KırılganDoğKenarTopOrtDWT farklı değişikliklere maruz kalmış resimlere yapılan doğrulama sonuçları

a. Orijinal damgalı resim(PSNR 45.693)

a. Üzerinde oynanmış resim



c. Doğrulama sonucu

Şekil 3.36. Araçlar resmi doğrulama sonuçları.

a. Orijinal damgalı resim(PSNR 45.777)

b. Üzerinde oynanmış resim

c. Doğrulama sonucu

Şekil 3.37. Lena resmi doğrulama sonuçları. a. Orijinal damgalı resim(PSNR 45.777) b. Üzerinde oynanmış resim c. Doğrulama sonucu

3.3.2.4 Benzer Çalışmalar ile Kıyaslama

KırılganDoğKenarTopOrtDWT algoritması kırılgan dört adet doğrulama algoritması ile kıyaslanmıştır. Yeung ve Mintzer [72], Lin, Hsieh [73], Liu, Lin, Yuan [75], Lee ve Lin[74] algoritmaları ile yapılan kıyaslama **Tablo 3-7** de görülmektedir. Bahsi geçen algoritmaların tamamı değerlerin ikili sayı sisteminde en önemsiz bir 1-3 bitlerini kullanarak damgalama yaparken KırılganDoğKenarTopOrtDWT yöntemi DWT LL değerlerinin ondalık sayı halinin son basamağına damgalama yapmıştır. Yeung ve Mintzer'in çalışması blok tabanlı değil piksel tabanlı iken diğer yöntemler ve KırılganDoğKenarTopOrtDWT blok tabanlıdır. Blok tabanlı iki algoritma blok eşleştirmesini anahtar kullanarak yaparken Liu, Lin, Yuan [75] çalışması ve KırılganDoğKenarTopOrtDWT yönteminde anahtar kullanılmamaktadır. Doğrulanmaya çalışılan resimde değiştirilen kısımların tespitindeki hassasiyete bakıldığında Yeung ve Mintzer [72] yöntemi piksel hassasiyetine kadar değişikliği tespit etmekte, Liu, Lin, Yuan [75]'ın yöntemi 1x4 blok alanını tespit edebilirken diğer iki yöntem ile beraber KırılganDoğKenarTopOrtDWT algoritması 4x4'lük blok alanı hassasiyetinde değişiklik tespiti yapabilmektedir. Lin, Hsieh [73] ve Lee ve

Lin[74] çalışmaları doğrulamanın yanında restore yeteneğine de sahipken diğer iki yöntem ve KırılganDoğKenarTopOrtDWT yöntemi restore yeteneğine sahip değildir. KırılganDoğKenarTopOrtDWT yöntemi doğrulama yapabilmek için bir anahtara ihtiyaç duymazken diğer yöntemlerin hepsi anahtar veya anahtarlara ihtiyaç duymaktadır. Yeung ve Mintzer [72]'in anahtarının nasıl kırılacağı yönünde makaleler mevcuttur [79].

KırılganDoğKenarTopOrtDWT yöntemi yüksek PSNR değeri ile Yeung ve Mintzer yöntemi hariç diğer tüm yöntemlerden daha başarılıdır. 4x4'lük değişiklik tespit hassasiyeti ile başarı olarak ortamalanın üzerindedir. Orijinal resme benzerlik PSNR yönünden [72] hariç diğer tüm yöntemlerden oldukça yüksek bir değer olan 45.8 PSNR değerine sahiptir. Doğrulama esnasında doğrulanmaya çalışılan resim haricinde başka hiçbir bilgiye ihtiyaç duymaması kullanımını pratik kılmaktadır.

Tablo 3-7. Benzer Kırılgan Doğrulama Çalışmaları ile Kıyas

	Yeung ve Mintzer [72]	**Lin, Hsieh** [73]	**Liu, Lin, Yuan** [75]	**Lee ve Lin**[74]	**KırılganDoğKenar-TopOrtDWT**
Kullanılan Uzay	Piksel uzayı, piksel değerleri {0,1} kümesine eşleme	Piksel uzayı, Iki en önemsiz bit (LSB)	DWT, en önemsiz bit	Piksel uzayı, en önemsiz 3 bit	DWT, Ondalık son rakam
Blok çiftleme var mı? anahtar tabanlı mı?	Blok tabanlı değil	Var, K (Asal sayı)	Var, Anahtar yok	Var, K (Asal sayı)	Var, anahtar yok
Değiştirilen yer tespit hassasiyeti	1 piksel	4x4 blok alanı	1x4 blok alanı	4x4 blok alanı	4x4 blok alanı
Hata düzeltmesi, Değiştirilen yeri onarma	☒	☑	☒	☑	☒
Damgalanan resmin PSNR değeri	≈ 52	≈ 44.3	≈ 40	≈ 40	≈ 45.8
Doğrulama metodu neye ihtiyaç duyar	0-255 arası piksel değerlerini siyah beyaz değerlere eşleştiren anahtar	Eşleştirme anahtarı K	Damga N Parametresi	Eşleştirme anahtarı K	-
Algoritma anahtarının kırılma durumu	Kırılmıştır	-	-	-	-

3.3.2.5 Katkılar

Bu çalışmada, kırılgan bir doğrulama algoritması geliştirilmiştir. Geliştirilen algoritma, resmin geneline uygulanan bir filtre, histogram eşitleme, kayıplı sıkıştırma v.b. işlemlerde resmin neredeyse tamamını değiştirilmiş olarak işaretlemekte, resmin geneline bir işlem yapıldığını tespit etmektedir. Bu özelliği ile algoritma kırılgan doğrulama algoritmasına bir örnek teşkil etmektedir.

Algoritma doğrulama esnasında orijinal çalışmaya ihtiyaç duyulmamaktadır. Algoritma resimde yapılan değişiklikleri tespit edebilmekte, değişikliğin yerini 4x4 piksel duyarlılığında sınırlayabilmektedir. Kırpma işlemi uygulanması durumunda yine kırpılan kısımlar algoritma tarafından tespit edilebilmektedir.

Algoritma kullanılarak elde edilen damgalı resimlerin PSNR değerleri 45.7 civarında seyretmekte, bu değer, algoritmanın orijinal resme benzerlik yönünden çok güçlü olduğunu göstermektedir.

Algoritmanın basit ve kolaylıkla uygulanabilir olması da algoritmanın pozitif yönlerindendir.

Algoritmanın zayıf tarafı, blok eşleştirmelerinin bir anahtara bağlı olmadan yapılması, düz ve tahmin edilebilir olmasıdır. Holliman ve Memon'un makalelerinde belirttiği gibi, aynı yöntemle damgalandığını ve doğrulamadan geçtiğini bildiğimiz başka resimlerden o blok çiftine benzeyen bir blok çifti bulunması durumunda bloklar doğrulanmış resimden doğrulanacak resme kopyalandığı taktirde resmin o blokları doğrulama testinden geçecektir [7]. Her ne kadar Holliman ve Memon'un bahsettiği saldırı türü mümkün olsa da, hem elde bol miktarda damgalı ve doğrulanmış resmin olması hem de doğrulanmış resimlerden değiştirilmek istenilen bloklara benzer blok çiftlerin bulunması gerekmekte, bunların sonucunda da yapılan sahteciliğin işe yaraması ihtimali de hayli zayıf görünmektedir.

Geliştirilen algoritmanın orijinal resme ihtiyaç duymaması, uygulanmasının kolaylığı, damgalanmış resimlerin PSNR değerinin yüksek oluşu, algoritmanın mevcut algoritma seçeneklerinin arasında değerli bir alternatif olarak yer almasını sağlamaktadır.

3.3.3 Doğrulama Damgalama Algoritması YarKırDoğDCTDWTOrtaKenar

Bu çalışmada doğrulama amaçlı yarı-kırılgan damgalamanın yanı sıra sahipliğin ispatı amaçlı damgalama yapılmak sureti ile iki çeşit damgalama uygulanmıştır.

Geliştirilen Yöntem, resmi iki ana kısımdan ibaret görmektedir: Orta kısım ve çevre kısım. Genellikle resimlerde önemli görülen nesneler veya kişiler Şekil 3.38'de de görüldüğü gibi resmin orta kısmına veya orta kısmına yakın kısımlara denk gelir. Bu çalışmada resmin orta kısmına resmin asla benzerliğini kötü etkilemeyecek şekilde dayanıklı damga yerleştirilmek sureti ile sahipliğin ispatı hedeflendikten sonra kenar bloklara da doğrulama amaçlı damganın yerleştirilmesi ana düşüncedir. Orta kısım kendi içerisinde, kenar kısım kendi içerisinde bloklara bölündükten sonra orta bloklar çevre bloklar ile eşleştirilip, orta bloğun özet değeri kenar bloğa damgalanacaktır.

Şekil 3.38. Resmin orta ve çevre kısımlara ayrıldıktan sonra bloklara bölünmesi

Algoritmayı bilen birinin resmin orta kısmını kesip izinsiz kullanmasını önlemek için öncelikle resmin orta kısmına sahipliği ispat damgası dayanıklı olarak damgalanır. Orta kısım, bölüm 3.1.'de anlatılan DWT uzayındaki algoritma ile damgalanır. Genel olarak damgalamanın ana adımları Eş 3.10 ile Eş.3.11' de gösterilmiştir. Bölüm 2.1.'den farklı olarak, sadece LL1 bandı damgalanmıştır. Orta kısma sahipliğin ispatı için yapılan damgalama, asla benzerliği olumsuz etkilememektedir. Sahipliğin ispatı için orta kısma yapılan damgalama sonrası elde edilen resmin PSNR değeri 57 civarında olup çok yüksek bir değerdir. Bu çalışmada asıl odak noktası doğrulama amaçlı damgalama olduğu için ve

sahipliğin ispatı için yapılan damgalama bölüm 2.1.'de anlatıldığı için, orta kısma yapılan damgalama ile ilgili ayrıntılı bilgi ve sonuç verilmeyecektir.

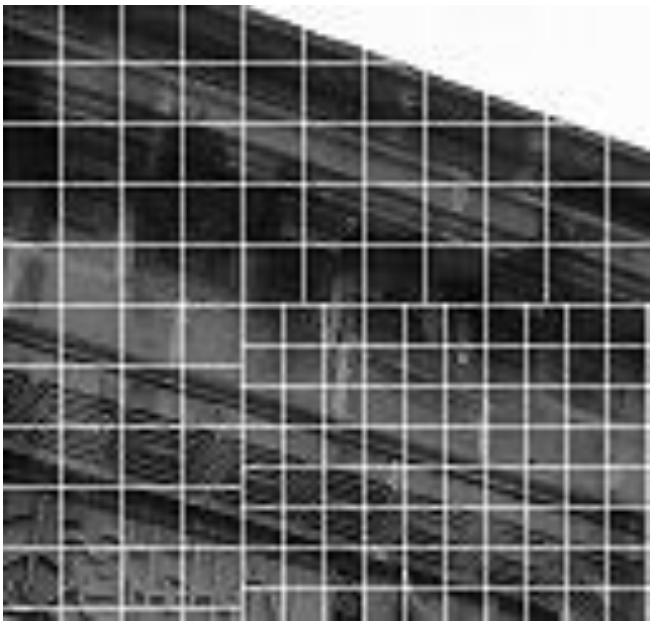
[LL1, LH HL1, HH1] ← DWT (Orta_Resim_Blok) (3.10)

LL1 ← LL1 + α * SiyahBeyazResimDamgası (3.11)

İkinci aşama olarak, orta blokların LL1 bantları siyah beyaz resme çevrilir. Bunun için bir sınır değer belirlenir ve LL1 değeri sınır değerden büyükse 1, değilse 0 değeri verilir. Sınır değer dinamik olarak belirlenir ve tüm orta kısmın değerleri dikkate alınarak oluşacak siyah beyaz resimde sıfır ve birlerin sayısının birbirine yakın olması hedeflenir. Bunu yapmaktaki maksat, damgayı daha dengeli yerleştirerek asıl resme benzerlik ilkesini daha az olumsuz etkilemektir.

Şekil 3.38'de orta kısım kalın bir çerçeve içine alınmıştır. Orta kısım blokları kenar kısım bloklarına göre daha küçük yüzeye sahiptir. Orta kısım blokları ile kenar kısım bloklarının eşleştirilmesinin nasıl yapıldığı bölüm 4.3.3'de açıklanmıştır. Bu eşleştirme algoritması bir K1 asal sayısı anahtarına bağlıdır. Doğrulama programını kullanacak olan karşı tarafa bu anahtarın verilmesi gerekecektir.

Orta kısım ile kenar kısım blokları birbiri ile eşleştirildikten sonra, orta kısım bloğundan bir siyah beyaz resim hesaplanıp eşleştiği kenar bloğa damgalanır. Kenar bloklar orta bloklara göre daha büyüktür. Bu bize daha önemli olan orta kısımda yapılan değişiklikleri daha hassas bir şekilde tespit etme olanağı vermektedir. Kenar blokların ebat olarak daha büyük yüzeye sahip olması, damga barındırabilme kapasitesini artırmakta, yarı kırılganlığı sağlayacak şekilde seçici olarak bazı resim operasyonlarından damganın etkilenmemesini sağlayacaktır. Şekil 3.39'de orta kısım ile kenar kısım blokları arasındaki büyüklük farkı daha yakından görülebilmektedir.



Şekil 3.39. Orta kısım blokları kenar kısım bloklarına göre daha küçüktür.

3.3.3.1 Damga Ekleme Algoritması

Damgalama kısmının algoritması aşağıda verilmiştir.

1. Resim orta kısım ve kenar kısım olmak üzere iki kısma ayrılır.
    a. Orta ve kenar kısımlar bir döngü içerisinde kenar kısmını döngünün her dönüşünde büyütmek sureti ile yapılır. iii fıkrasında yazılan durum meydana geldiğinde döngü sona erer.
        i. Kenar kısım blok ebadı BS_O,
        ii. Orta kısım blok ebadı BS_I
        iii. Orta_kisim_blok_sayisi / Kenar_kisim_blok_sayisi > 0.9
2. Bir önceki bölümde anlatıldığı gibi orta kısma sahipliğin ispatı damgası yerleştirilir
3. (B_Ik, B_Ok) çiftleri oluşturulur, B_Ik orta kısımdan, B_Ok kenar kısımdan olmak üzere S_K anahtarı kullanılarak bölüm 3.3.3.3 deki eşleştirme algoritması kullanılır.
4. Prns_uzunluk ← (BS_O * BS_O – 2 * V_haricBirak) / (BS_I /2 * BS_I /2)
5. Prns ← prns_random (Prns_uzunluk) ; % ortalama 0, varyans 1
6. Orta kısımdaki her B_Ik bloğu için
    a. DWT (B_Ik)

b. Bin_LL1_B_Ik Siyah beyaz resmini DWT (B_Ik) LL1 bandından elde et
c. DCT_ B_Ok _M ← DCT(B_Ok), B_Ok kenar kısımda eşleştiği blok
d. Z_DCT_ B_Ok ← zigzagscan(DCT_ B_Ok _M)
e. V_DCT_B_Ok ← Z_DCT_ B_Ok'den değerler al, baştaki ve sondaki V_ haricBirak değerlerini hariç bırak (Asıla benzerlik ve kayıplı sıkıştırmaya dayanıklılık için)
f. Bin_LL1_B_Ik'nin her bir bit_val bit değeri için
    i. Val_prns ← V_DCT_B_Ok'den Prns_length sayısınca değer al
    ii. If bit_val==1

        Val_prns* ← Val_prns + Prns * alpha

    Else

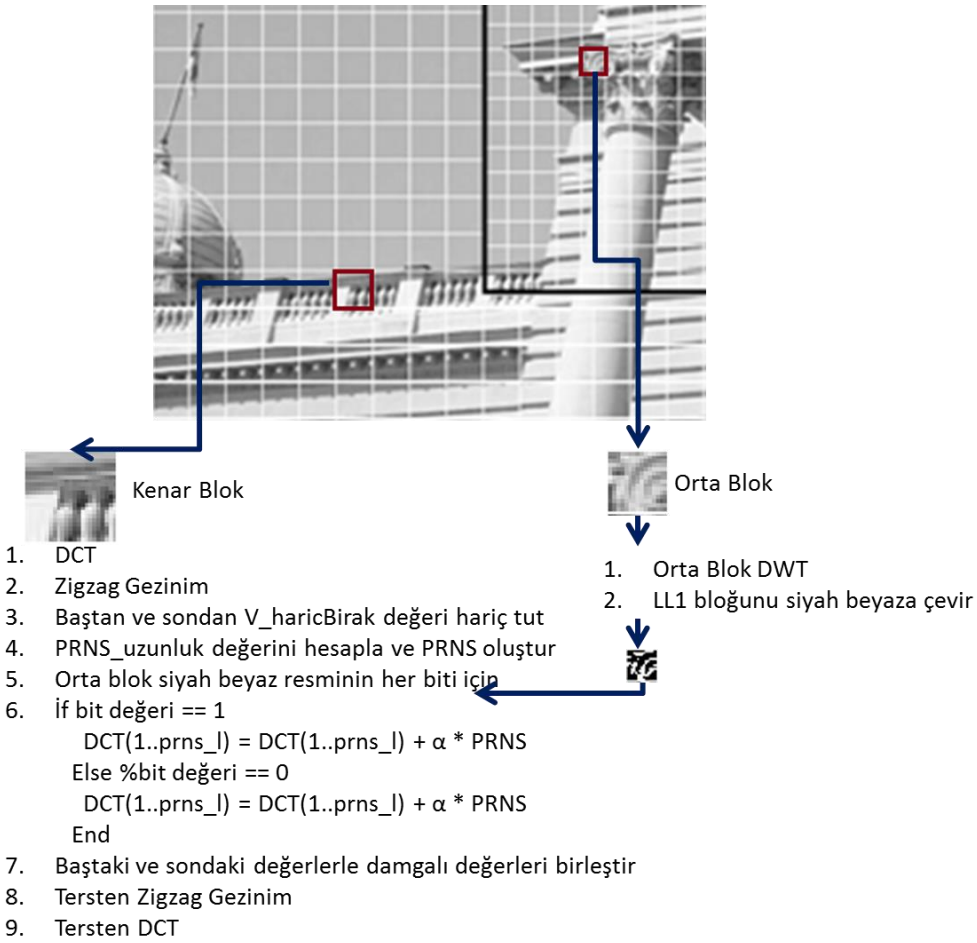
        Val_prns* ← Val_prns - Prns * alpha

g. B_Ok* ← Inverse_DCT(InverseZigzag(V_excluded + V_DCT_B_Ok* + V_HaricBirak))

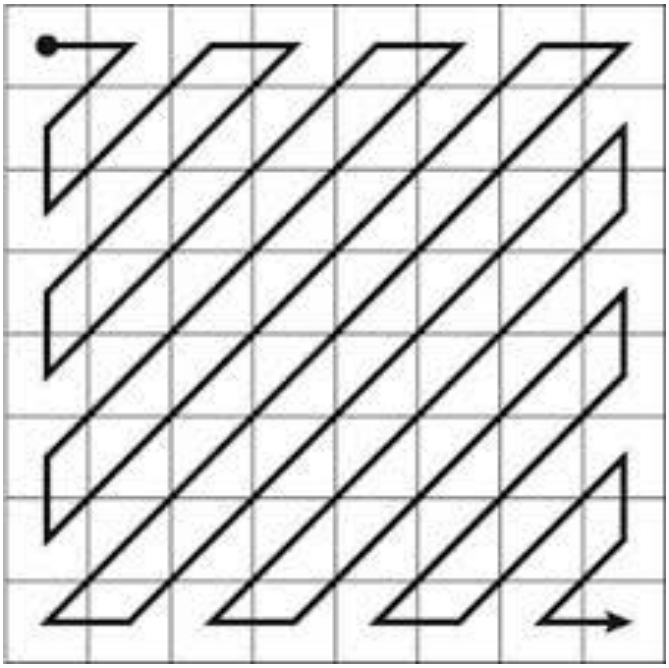
İşlem adımı 1.a.iii 'de orta kısım ile kenar kısım blok sayısı resmin yükseklik ve genişliğine bağlı olduğundan birbirinden farklı olabilecektir. Orta kısımdaki blokların en az %90'nının kenar bloklarla eşleşmesi yeterli sayılmıştır. %100 de denebilirdi ancak döngünün her dönüşünde kenar kısım kalınlığı arttığından, orta kısmı da fazla küçük bırakmamak adına %90 yeterli görülmüştür. Diğer bir deyişle, orta kısım bloklarından en fazla %10'u kenar bloklar ile eşleşmemiş olabilecektir. Bu oran söz gelimi %97 de olabilecektir. Orta kısım bloklarının tamamı daha önceden sahiplik damgası ile damgalandığından, orta kısım blokları için büyük sorun olmayacaktır. Algoritmayı bilen birinin, orta kısım blokları ile eşleşmemiş blokları tespit edip bu bloklarda değişiklik yaptığı halde doğrulama algoritmasının bunu tespit edememesi bir risk oluşturmaktadır. Öncelikle, eşleştirme gizli bir anahtar değer üzerinden yapıldığı için orta bloklarla eşleşmeyen blokları tespit etmek kolay değildir. Blok analizleri ile üzerinde damga bulunmayan kenar blokların tespiti çok zor olmasına rağmen yapılabilse bile büyük çoğunlukla bu bloklar birbiri ardı sıra veya bitişik değildir. Bir kenar bloğun içeriğini fark edilmeyecek şekilde değiştirmek tek başına sahtecilik yapan kişinin amacına

hizmet etmeyecektir. Resim sahteciliğinde amaç yapılan sahteciliğin fark edilememesi, tespit edilememesi olduğu gibi resmin genel yorumunu değiştirmeye yönelik olmalıdır. Sonuç olarak orta kısım bloklarının göreceli az bir kısmının kenar kısım blokları ile eşleşmemesi büyük bir sorun çıkarmayacaktır.

İşlem adımı 4, Prns_uzunluk hesaplanırken kenar blokların kenar uzunluğu olan BS_O değerini dikkate almaktadır. Bir kenar bloğunun barındırdığı piksel sayısı BS_O * BS_O değeridir. İşlem adımı 6.b.'de LL1 değerleri siyah beyaz {0,1} değerlerine dönüştürülürken, değeri 1 olan piksel değerleri ile değeri 0 olan piksel değerleri sayısının birbirine yakın olması gözetilmiştir. İşlem adımı 6.c.'de gösterildiği gibi, kenar bloğun DCT dönüşümü elde edilmektedir. Zigzag geziniminden sonra elde edilen değer vektöründe baştan ve sondan v_HaricBirak kadar değer damgalamadan hariç birakılmaktadır. Zigzag gezinimi, DCT transformuna maruz kalmış bir kare bloğun en düşük frekanslı ve önemli değeri olan DC komponenti en başta olmak üzere en düşük frekans değerinden en yüksek frekans değerine sıralanmak sureti ile sıralı bir vektör haline geçmek için kare blok üzerinde yapılan gezinimdir. Bir 8x8'lik kare blok üzerinde yapılan zigzag gezinimi Şekil 3.41'de görülmektedir. Böyle yaparak, DC elemanı dâhil düşük frekanslı ve değiştirildiği takdirde resimde farkedilir değişikliklere yol açacak frekanslar damgalanmamış olacaktır. Yüksek frekanslı DCT değerlerine de damgalama yapılmayarak, yüksek frekanslı değerlerde deformasyona yol açacak kayıplı sıkıştırma gibi işlemlere karşı dayanıklılık ve esneklik gözetilmektedir. Damga damgalama süreci Şekil 3.40'de görülmektedir.



Şekil 3.40. Damga Ekleme algoritması



Şekil 3.41. Zigzag gezinimi

3.3.3.2 Doğrulama Algoritması

Doğrulama algoritması aşağıda görülmektedir.

1. Damga yerleştirmede olduğu gibi resim orta ve kenar kısımlara ayrılır
2. S_K anahtarı kullanan karıştırma algoritması Blok çiftlerini (B_Ik, B_Ok) oluşturur, B_Ik orta kısımdan, B_Ok kenar kısımdan
3. Damgalama esnasında kullanılan PRNS okunur
4. Prns_uzunluk ← Length(PRNS)
5. Orta kısımdaki her bir B_Ik bloğu için
    a. DWT (B_Ik)
    b. DWT (B_Ik) den LL1'in SiyahBeyaz resmini Bin_LL1_B_Ik'e ata
    c. DCT_ B_Ok _M ← DCT(B_Ok), B_Ok kenar kısımdaki eşlenik blok
    d. Z_DCT_ B_Ok ← zigzagscan(DCT_ B_Ok _M)
    e. V_DCT_B_Ok ← Z_DCT_ B_Ok'den baştan ve sondan V_haricBirak kadar değeri hariç bırakarak diğer değerleri ata
    f. Islenmis_baslangic ← 1
    g. While (Islenmis_baslangic <= (Length(V_DCT_B_Ok) - Prns_uzunluk))
        i. Val_prns ← V_DCT_B_Ok'den Prns_length kadar değer al
        ii. Correlation_deger1 = correlation_coefficient(Val_prns, Prns)
        iii. Correlation_deger2 = correlation_coefficient(Val_prns, -Prns)
        iv. If Correlation_deger1 >= Correlation_deger2

            bit_val ← 1

        v. Else

            bit_val ← 0

        vi. Extracted_Bitmap ← Elde edilen biti olması gereken konuma yerleştir
        vii. Processed_Start = Processed_Start + Prns_length
    h. Bit_Diff_Sum ← Sum(abs (Extracted_Bitmap - Bin_LL1_B_Ik))
    i. BitMapImageNumberOfBits ←(Row_Length(Bin_LL1_B_Ik) * Column_Length(Bin_LL1_B_Ik))

j. If (Bit_Diff_Sum / BitMapImageNumberOfBits) > 0.15 /*Threshold=0.15 */

Orta ve Kenar bloğu değiştirilmiş olarak işaretle

6. Doğrulama resmini son işleme tabi tut
   a. Değişti olarak işaretlenen her blok için
   b. Eğer etrafında değişmiş olarak işaretlenen blok yoksa

Bloğu değişmedi olarak işaretle

3.3.3.3 Karıştırma ve Eşleştirme Algoritması

Doğrulama amaçlı damgalama algoritmalarının pek çoğunda resim bloklara bölünür ve bloklar (B1,B2) şeklinde birbiri ile eşleştirilir. B1 bloğundan hesaplanan değerler veya resim B2 bloğuna gömülür veya tam tersi yapılır. Blok eşleştirmesini gizli tutmak gerekir çünkü kötü niyetli kişiler blok çiftini doğrulamadan geçmiş başka bir resimdeki blok çifti ile değiştirip doğrulama aşamasını başarı ile geçebilir [7].

Lan, Hsieh ve Huang [73] bu tür eşleştirmeler için Torus oto-morfizmlerinin kullanılabileceğini belirtmiştir. Bir Torus oto-morfizmi Eş.3.12'de belirtildiği gibi başlangıç durumu olan, t zaman aralıklarında değişen dinamik bir sistemdir.

$$S_{t+1} = f(S_t),\ t \in \{0, 1, 2..\} \qquad (3.12)$$

İki boyutlu bir oto-morfizm şu şekilde tanımlanabilir:

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},\quad \begin{pmatrix} x_{t+1} \\ y_{t+1} \end{pmatrix} = A \times \begin{pmatrix} x_t \\ y_t \end{pmatrix} mod\ N \qquad (3.13)$$

$a_i \in Z$, $determinant(A)=1$,

$A\ \lambda_{1,2} \in R - \{-1, 0, 1\}$ eigen değerlerine sahiptir

Sistem kaotiktir ve her R zaman adımında kendini tekrarlar, yani $S_R = S_0$.

Votayzis ve Pitas, Eş.3.13 için Eş.3.14'te belirtilen özel bir A matrisi önermiştir [80]. A matrisi tek bir k değerinden kurulabilmektedir.

$$A = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \qquad (3.14)$$

Doğrulama algoritması-2'de [73] 'de bahsedilen ve Eş.3.15'te verilen tek boyutlu karıştırma algoritması kullanılmaktadır.

$$X' = (k \times X \, mod \, N) + 1 \quad (3.15)$$

X, X' ∈ {0, 1, .., N-1} t ve t+1 zamanlarındaki blok numaralarıdır. K bir asal sayıdır ve gizli anahtardır, N ise blok sayısıdır.

Orta blokların kümesi S1, eleman(blok) sayısı N1 olsun, kenar blokların kümesi S2, eleman(blok) sayısı N2 olsun. Algoritma S1 kümesindeki elemanları S2 kümesindeki elemanlara bire bir eşleştirir.

3.3.3.4 Deneyler

Orijinal resim Şekil 3.42'da, damgalanan sahiplik siyah beyaz damgası Şekil 3.43'de, sahiplik ve doğrulama damgaları ile damgalanmış resim Şekil 3.44'de görülmektedir. PSNR değeri olarak 40.577 biraz düşük gibi görünse de, yarı kırılganlık için asıl resme benzerlikten biraz feda edilmiştir. Resme yapılan işlemlere göre algoritma ile yapılan doğrulama işlemleri sonucu Tablo 3-8'de görülmektedir.

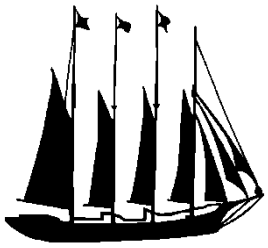
Tablo 3-8. YarKırDoğDCTDWTOrtaKenar saldırılara göre başarı durumu

Saldırı Tipi	**PSNR**	**(Değişmiş blok) / Toplam Blok Sayısı**	**Başarı %**
-	40.577	0/2932	100
Değiştirme	30.902	54/2932	100
Jpeg 75% sıkıştırma	35.107	4/2932	99.86
Jpeg 50% sıkıştırma	33.346	177/2932	-
Jpeg 25% sıkıştırma	31.640	625/2932	-
Gauss Gürültüsü	29.981	16/2932	99.5
Histogram Eşitleme	17.458	0/2932	100
Parlaklık ayarlama	22.114	3/2932	99.9
Büyültme Küçültme	29.071	178/2932	-
3x3 ortalama filtresi	29.748	127/2932	-
Gamma Düzeltmesi	18.704	10/2932	99.66
Yanlış anahtar	-	2111/2932	-

Şekil 3.45.a.'da caminin üzerinde orijinalinde bulunmayan bir kabartma sütunun caminin üzerinde varmış gibi eklenerek oynama yapılan resim görülmektedir. Şekil 3.45.b.'de ise üzerinde oynama yapılmış resme yapılan doğrulama sonucu

görülmektedir. Resimden de görüleceği gibi, doğrulama algoritması sonradan eklenen kabartma sütunun olduğu bölümü başarılı bir şekilde işaretlemiştir.

Şekil 3.42. Orijinal Resim



Şekil 3.43. Resmin Orta Kısmına Damgalanan Siyah Beyaz Damga

Şekil 3.46.a.'da görüleceği üzere %75 kalite kayıplı sıkıştırmaya maruz kalmış bir resim 3 blok çifti hariç neredeyse tamamında doğrulanabilmiştir. Şekil 3.46.b.'de ise Jpeg %50 kalite sıkıştırmaya uğramış bir damgalı resmin doğrulanmasında değiştirildiği tespit edilen blok sayısı önemli ölçüde artmaktadır (177 blok). Şekil

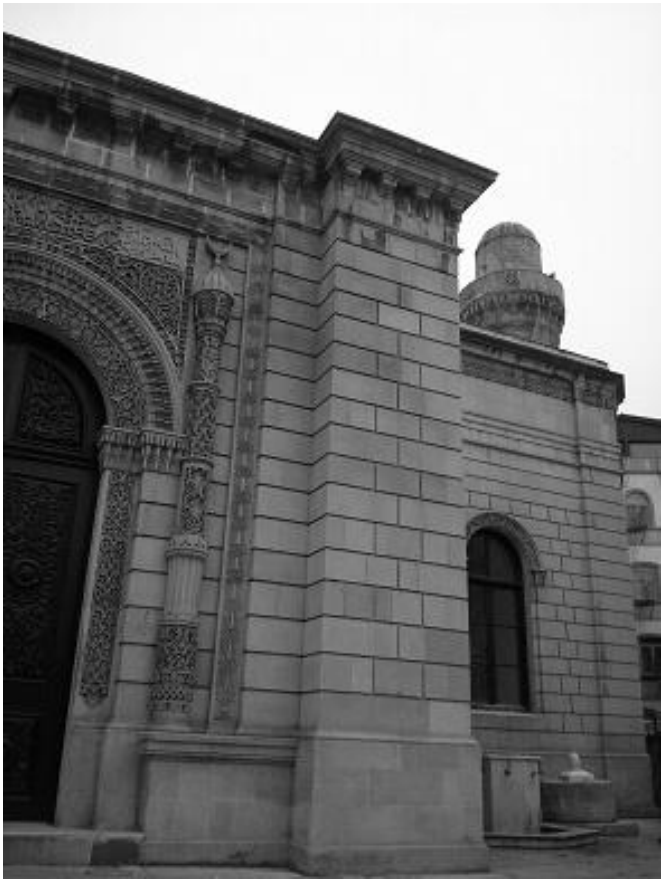
3.46.c.'de ise Jpeg %25 sıkıştırmaya uğramış resimde resmin çok önemli bir kısmı doğrulamadan geçememektedir (625 blok).

Şekil 3.47 a.'da ve b.'de kötü amaçlı yapılmayan parlaklık ayarlama ve histogram eşitleme işlemlerinden sonra da resmin doğrulanabildiği görülmektedir. Parlaklık ayarlamasında değişti olarak işaretlenen 3 blok resmin doğrulanmasına mani olmayacaktır.

Şekil 3.48 a.'da damgalanmış ve K anahtarı ile blokları birbirine eşleştirilen blokların K anahtarından farklı bir anahtar ile bloklar eşleştirilerek doğrulama yapılmak istendiğinde blokların %80'inden fazlası değişmiş gibi işaretlenmektedir. Anahtar elde olmadan doğrulama yapılamadığı bu şekilde görülmektedir. Anahtar elde olmadan doğrulama yapılabilse idi, algoritmayı devre dışı bırakacak kolaj (collage) saldırılarına açık hale gelebilirdi.

Şekil 3.48.b.'de ise büyültme küçültme işlemine tabi tutulmuş bir damgalı resmin doğrulama işlemi sonunda kayda değer sayıda değiştirilmiş blok tespit etmesidir. Büyültme-küçültme genel olarak kötü niyet barındırmayan bir işlem sayıldığından algoritma ile damgalanmış resimdeki damganın büyültme veya küçültme işleminden etkilenmemesi tercih edilirdi ancak bu işlemden etkilendiği görüldü.

Şekil 3.49.a.'da Gauss gürültüsü uygulanmış damgalı resme yapılan doğrulama sonucu görülmektedir. Doğrulamadan geçemeyen blok sayısı 16 olsa da toplam blok sayısının 2932 olduğu düşünüldüğünde ve değişen blokların hepsinin yanyana olmaması algoritmanın Gauss gürültüsüne karşı gürbüz olduğu sonucunu vermektedir. Gauss gürültüsünün tüm resmi etkileyen ve kötü niyetli değerlendirilmeyen bir durum olması nedeniyle algoritmanın Gauss gürültüsüne karşı gürbüz olması yarıl kırılganlık adına olumlu bir durumdur.



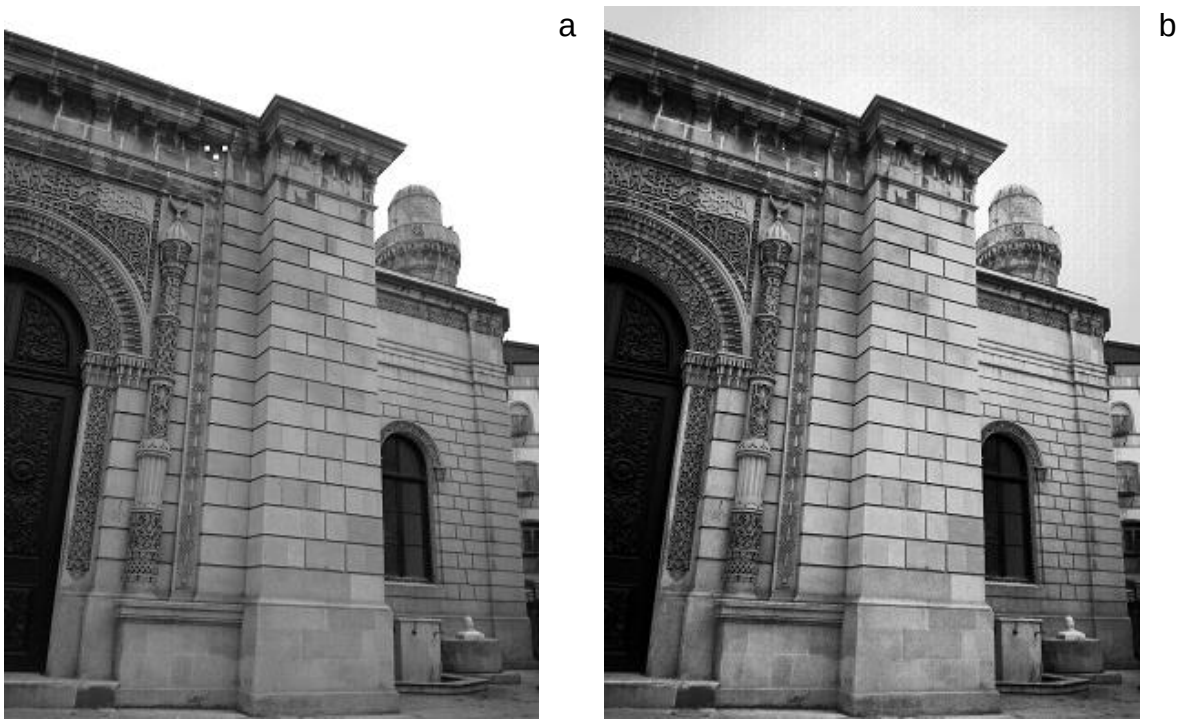
Şekil 3.44. Sahiplik ve doğrulama damgası ile damgalanmış resim. PSNR : 40.577

Şekil 3.49.b.'de 3x3 bulanıklaştırma işlemine tabi tutulmuş damgalı resme yapılan doğrulama sonucu görülmektedir. 2932 blokdan 127'si damgasını yitirmiş ve değiştirilmiş olarak işaretlense de resim değiştirilmiş olarak değerlendirilmektedir. Algoritma bulanıklaştırma filtresine karşı belli bir esnekliği olsa da yarı kırılganlık için yeterli değildir.

Şekil 3.45. a.Üzerinde oynanmış damgalı resim b. Oynanmış resmin doğrulaması

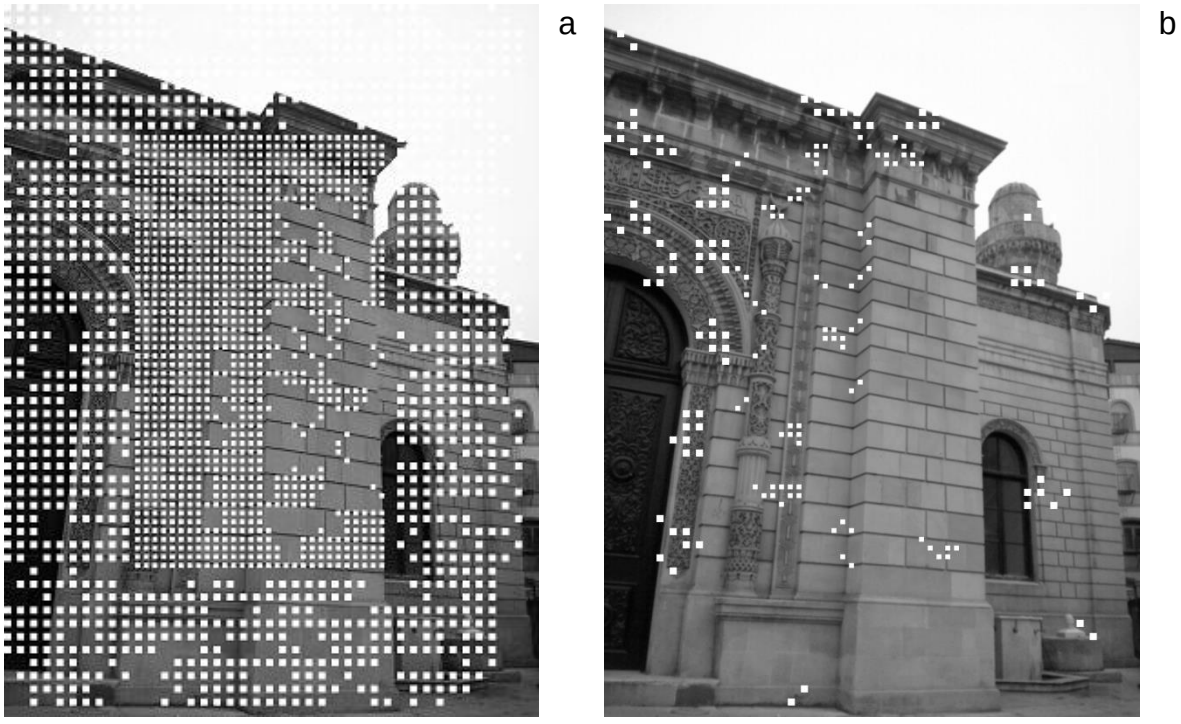
Şekil 3.46. Jpeg kayıplı sıkıştırmaya uğramış damgalı resimlerin doğrulaması a. %75 kalite b. %50 kalite c. %25 kalite

a b

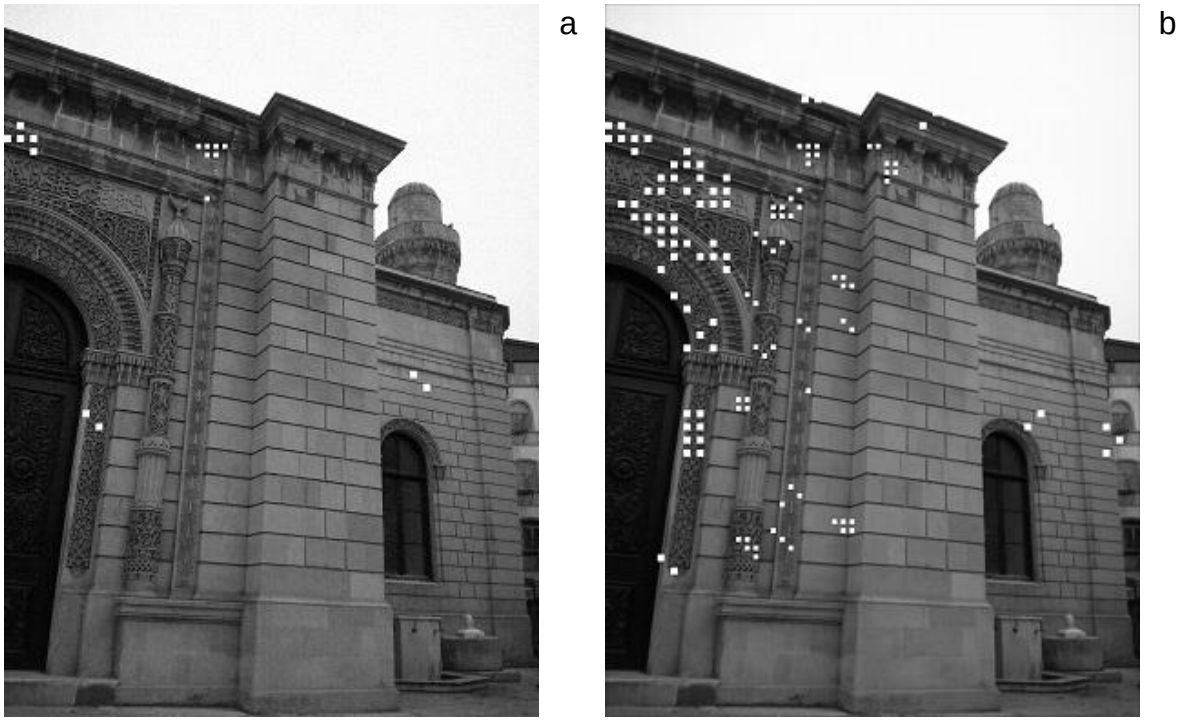


Şekil 3.47. Resim işlemlerine uğramış damgalı resimlerin doğrulaması a. Parlaklık ayarlaması b. Histogram Eşitleme

a b



Şekil 3.48. a. Yanlış anahtarla doğrulanmaya çalışılmış, üzerinde işlem yapılmamış damgalı resim b. Büyültme-küçültme uygulanmış damgalı resme yapılan doğrulama işlemi



Şekil 3.49. a. Gauss gürültüsü uygulanmış damgalı resim doğrulaması
b. 3x3 ortalama filtresine maruz kalmış damgalı resim doğrulaması

3.3.3.5 Benzer Çalışmalar ile Kıyaslama

Tablo 3-9'de çalışmamıza benzer dört çalışma ile geliştirilen YarKırDoğDCTDWTOrtaKenar algoritmasını kıyasladığımız verileri ihtiva etmektedir. Önceki çalışmaları incelediğimizde, bazı çalışmaların resmi bloklara böldükten sonra damgalama yaptığı görülmektedir. Çalışmaların çoğunda blokları birbiri ile eşleştirirken bir gizli anahtara dayalı bir algoritma kullanıldığı, resimler doğrulanırken bu anahtarın doğrulayacak tarafa verilmesi gerektiği, birbiri ile eşleşmiş bloklardan birinden hesaplanan değerlerin diğer bloğa damgalandığı görülmektedir.

Yarı kırılgan yöntemlerle karşılaştırıldığında, Chamlawi v.d. [81] %75 kalite ile sıkıştırılmış damgalı bir resmi doğrulayabildiğini belirtmekte, ancak başka bir iyi niyetli resim işlemine karşı yöntemin toleranslı olup olmadığını açıklamamaktadır. Geliştirilen YarKırDoğDCTDWTOrtaKenar yöntemi, %75 kalite ile jpeg sıkıştırması yapılmış damgalı resmi doğrulamanın yanında, histogram eşitleme, gamma düzeltmesi, parlaklık ayarlaması, gauss gürültüsü işlemlerine maruz kalmış damgalı resimleri de doğrulamaktadır.

Resimde değişikliğe uğramış bölgenin tespiti hassasiyetine gelince, yöntemimiz 8x8 ‘lik blok alanı hassasiyetinde değiştirilmiş alan tespiti yapabilmektedir.

Resmin aslına benzerlik yönünden PSNR değeri olan 40 değeri, kabul edilebilir bir PSNR değeridir ve karşılaştırılan yöntemlerden sadece ikisi PSNR yönünden yöntemimizden daha iyi görünmektedir.

Yöntemimiz doğrulama yapabilmek için blok eşleştirme anahtarı olan K asal sayı değerine ve sözde rastgele sayı dizisi PRNS’e ihtiyaç duymaktadır. Algoritmanın güvenliği açısından bu değerlerin doğrulama yapan tarafa güvenli bir yoldan aktarılması gerekmektedir. Karşılaştırılan diğer dört yönteme baktığımızda, tüm yöntemlerin doğrulama kısmında benzer şekilde anahtar veya değerleri doğrulama tarafına aktarması gerektiği görülmektedir.

Tablo 3-9.Önceki Benzer Doğrulama Damgalama Çalışmaları ile Kıyas

	Lin, Hsieh [73]	**Chamlavi** [81]	**Liu, Lin, Yuan** [75]	**Pillai, Theagarajan** [76]	**Kendi Yöntemimiz**
Blok çiftleme anahtar tabanlı mı?	K (Asal sayı)	Blok tabanlı değil	Anahtar yok	K (Tohum anahtar)	K (Asal sayı)
Kırılgan / Yarı kırılgan	Kırılgan	Yarı-kırılgan	Kırılgan	Yarı-kırılgan	Yarı-kırılgan
Gürbüz Olunan Resim İşlemleri	-	70% jpeg	-	90% jpeg	75% jpeg Histogram eşitleme Parlaklık ayarlama Gamma düzeltmesi
Değiştirilen Yer Tespit Hassasiyeti	4x4 blok alanı	64x64 blok alanı	1x4 blok alanı	16x16 blok alanı	8x8 blok alanı
Hata düzeltmesi, Kendi kendini onarma	☑	☑	☒	Restorasyon bilgisi gömülüyor ancak restorasyon ile ilgili deney sonucu yazılmamış	☒
Damgalanan resmin PSNR değeri	≈ 44.3	≈ 38	≈ 40	≈ 48	≈ 40 Orta kısım daha az etkilenir
Kullanılan uzay	Piksel uzayı, Iki en önemsiz bit (LSB)	IWT, DCT, 5 en önemsiz bitler	DWT, en önemsiz bit	DWT, DCT, 5 en önemsiz bitler	DWT, DCT
Doğrulama yöntemi neye ihtiyaç duyar	Eşleştirme anahtarı K	Üç anahtar, PRN matrisi, Damga	Damga N Parametresi	Eşleştirme tohum anahtarı K R vektörü (HL1_HL/HL1_LH oranı)	Eşleştirme anahtarı K, PRNS

3.3.3.6 Katkılar

Bu çalışma ile temel hedefi resim doğrulama olan, bunun yanında sahipliğin ispatı amacıyla da resmi ikinci bir damga ile damgalayan yarı kırılgan bir damgalama algoritması geliştirilmiştir. Resim orta kısım ve kenar kısım olmak üzere iki kısımdan ibaret olarak düşünülmüştür. Orta kısım sahipliğin ispatı damgası ile öncelikle damgalanmıştır. Daha sonra orta kısım kendi içinde bloklara bölünmüş, kenar kısım kendi içinde bloklara bölünerek orta bloklar ile kenar bloklar birbiri ile bir gizli anahtar kullanılarak eşleştirilmiştir. Orta kısım bloklarından elde edilen damga kenar kısım eşlenik bloğuna damgalanmaktadır.

Orta kısım bloklarının DWT ayrışımının LL1 bandından bir sınır değer kullanılarak elde edilen siyah beyaz resim damgaları kenar blokların DCT dönüşümü alındıktan sonra baştan ve sondan belli sayıda değer hariç bırakmak üzere damgalanmaktadır. Böylelikle damganın yüksek geçirgen ve alçak geçirgen işlemlere karşı belli oranda gürbüz olması hedeflenmiştir.

Resmin orta kısım ve kenar kısım olarak değerlendirilmesi, orta kısım ve kenar kısım büyüklüklerinin farklı olması bu çalışmayı özgün kılan ana yaklaşımlardır. Kenar kısım bloklarının daha büyük olması, damga saklayabilme kapasitesini ve saklanan damganın gürbüzlüğünü artırmaktadır. Orta kısım bloklarının daha küçük olması, daha önemli kişi veya objelerin bulunduğu orta kısımda yapılan değişikliklerin (varsa) daha hassas tespitini sağlamaktadır.

Damgalama yönteminin doğrulama algoritmaları için istenen bir özellik olan yarı kırılgan olması, masum resim işlemleri olan kayıplı sıkıştırma, histogram eşitleme, gamma düzeltmesi, parlaklık ayarlaması gibi işlemlerden etkilenmeyerek resmi doğrulayabilmesi, resme sonradan konan nesneleri veya silinen kısımları tespit edebilmesi önemli katkılar olarak görülmektedir. Geliştirilen damgalama algoritması kıyaslanan doğrulama algoritmalarına ilave olarak histogram eşitleme, gamma düzeltmesi, parlaklık ayarlaması gibi masum işlemlerin sonunda da resmi doğrulayabilmesi, yarı kırılgan algoritmalar açısından algoritmamızın diğerlerine göre üstünlüğüdür.

Damgalama yapılırken sabit bir damga kullanılmaması, damganın ana resime dayalı olarak üretilmesi, algoritmanın Holliman ve Memon'un çalışmasında [7] belirtilen kolaj (collage) ataklarına karşı da başarılı olmasını sağlamaktadır.

4. SONUÇ VE KATKILAR

Tez çalışması kapsamında ayrık dalgacık dönüşümü kullanan gürbüz damgalama algoritmalarına bloklu yaklaşımın etkisi araştırılmış, daha önce damga olarak hiç kullanılmamış vektör damgası damgalanması analiz edilmiş, yarı kırılgan damgalama algoritmalarına daha iyi sonuçlar veren yeni algoritmalar eklenmeye çalışılmıştır.

Daha önceden resimleri bloklara ayırarak yapılan damgalama çalışmaları mevcut olsa da resmi bloklara ayırmadan bütün olarak farklı uzaya alınarak yapılan damgalama ile bloklara ayırdıktan sonra diğer uzaya alınarak yapılan damgalama arasında başarı yönünden fark olup olmadığı, bloklu damgalama yapmak daha iyi sonuçlar veriyor ise blok ebadının bu başarıyı etkileyip etkilemediği, etkiliyor ise ne oranda etkilediği tez kapsamında yapılan çalışma ile net bir şekilde ortaya konmuştur. Yapılan çalışma neticesinde elde edilen sonuçlar aşağıdaki gibidir.

- Bloklu damgalama gürbüzlük açısından çok daha başarılı sonuçlar vermiştir.
- Blok ebadı küçüldükçe gürbüzlük artmıştır.
- Artan gürbüzlüğe karşın damgalı resmin orijinal resme benzerliği olan PSNR değerinde bir düşme olmamıştır.
- Gürbüzlükteki olumlu iyileşmeye karşın işlemci zamanı yönünden bloklu damgalama daha fazla işlemci zamanına ihtiyaç duymaktadır.
- Artan işlemci zamanına toleransın olduğu durumlarda blok tabanlı damgalama gürbüzlüğü artırmak maksadıyla kullanılabilecektir.

Önceki damgalama çalışmalarında damga olarak sözde rastgele sayı dizisi, siyah beyaz firma logo resmi, resim hakkında meta veri, sahibinin sesi v.b. kullanılmıştır. Vektör resmini damga olarak resme damgalamak daha önce denenmemiştir. Firma logoları büyük oranda vektör resmi olarak tasarlanmaktadır. Vektör resimleri renkli olmaları, büyültme küçültme işleminde kalite kaybına uğramamaları, piksel tabanlı resimlere göre boyut olarak çok daha küçük olmaları nedeniyle siyah beyaz resme göre avantajlara sahiptir. Vektör resimlerinden svg formatı resmi okunabilir xml kaynak kodunda sakladığından ve yaygın kullanımından dolayı tercih edilmiştir. 256x256 ebatlarında bir siyah beyaz resim 65536 bitlik veri alanı, aynı boyutlardaki renkli piksel resmi 524288 bitlik veri alanı, aynı boyutlardaki bir vektör resmi yaklaşık 2 kilobit yani 16384 bitlik bir veriye karşılık gelmektedir. Vektör

damgasının boyutu küçüldükçe ana resimde bir biti damgalayabileceğimiz değer sayısı ve buna paralel olarak olarak gürbüzlük artacaktır. Bu düşünceyle yola çıkılarak tez kapsamında yapılan çalışmada svg formatındaki vektör damgası kullanılmasına karar verilmiştir. İlk yapılan çalışmalarda svg dosyasının tamamı bir dosya gibi düşünülerek bit bazında damgalanmış, ancak bu şekilde yapılan damgalamada svg formatının kaynak kodu olan xml kodundaki rezerve kelimelerde bir bozulma olduğunda svg dosyasının görüntülendiği program hata vermiş ve dosyayı gösterememiştir. Daha sonra svg dosyasında vektör resmi görüntüsünü etkilemeyecek şekilde gereksiz kısımlar elenerek tekrar damgalama yapılmış, yine saldırı durumunda çıkartılan vektör dosyası bozuk olarak nitelendirilerek görüntülenememiştir. Tezde belirtilen vektör ön işleminde olduğu gibi vektör dosyasını nümerik kısımları ayrılarak ana resme damgalandığında vektör svg dosyası damgalama başarı ile uygulanmış, JPEG %75 ve JPEG %50 kaliteli sıkıştırmalarda damga tam doğru olarak geri çıkartılabilmiş, JPEG %25 kalite sıkıştırmada vektör objelerinden sadece bir tanesinde kısmi bozulma olmuştur. Gauss gürültüsü, Histogram eşitleme, Gamma düzeltmesi saldırılarına uğramış damgalı resimlerden vektör resmi hatasız şekilde geri çıkartılabilmiştir. Bulanıklaştırma saldırısına uğramış resimden de tam doğruya yakın şekilde vektör damgası geri çıkartılabilmiştir. Algoritma büyültme-küçültme, parlaklık ayarlama, döndürme ve kırpma saldırılarına karşı gürbüzlüğünü koruyamamıştır. Vektör damgası kullanma, tereddüte yol açmayacak şekilde sahipliği ispatlayacak logonun renkli olması, büyüdüğünde kalite kaybına uğramaması, 10 değişik saldırı çeşidinden sekiz tanesine karşı gürbüzlüğü muhafaza edebilmesi nedeniyle özellikle siyah beyaz damgaya göre tercih edilebilecektir.

Resim damgalamanın en çok kullanıldığı alanlardan birisi de resim doğrulamadır. Bize gönderilen resimle elimize geçenin aynı olduğunu tespit edebilmek için resim doğrulama damgalaması kullanılmaktadır. Bazı durumlarda resimdeki bir bit değişikliği bile resmin doğrulanmamasını gerektirebilir. Ülke güvenliğini tehdit edebilecek durumlar, çok önemli kişilerin medikal görüntüleri gibi. Resimdeki değişiklikleri tolerans göstermeden ortaya çıkaran damgalama yöntemlerine tam kırılgan damgalama yöntemleri denir. Bu tez çalışması kapsamında kırılgan bir damgalama yöntemi geliştirilmiştir. Resim eşit ebatlarda bloklara ayrılmış, bloklar çiftler haline getirilmiş, çiftlerden her iki bloğun da DWT dönüşümü yapılmış, 2nci

bloğun kenar bilgilerini içeren HL, LH, HH bantlarındaki aynı koordinattaki değerler toplanmış, dinamik olarak hesaplanan bir sınır değerle kıyaslanarak bu değer toplamı {0,1} değerlerinden birine eşlenmiştir. 1nci Bloğun LL1 bandında aynı koordinata gelen değerin onluk sayı düzenine göre son basamağı sıfırlanarak 2nci bloktan 0 değeri dönmüşse LL1 bandındaki değerin ondalık son basamağı 2, 1 değeri dönmüşse ondalık son değeri 7 yapılmıştır. Geliştirilen kırılgan doğrulama algoritması 45.7 gibi yüksek PSNR değerine sahip, resimde yapılan değişiklikleri 4x4 piksel hassasiyetinde tespit edebilen, uygulanması pratik bir algoritma olarak mevcut kırılgan resim damgalama uygulamalarına değerli bir alternatif oluşturmaktadır. Algoritmanın zayıf tarafı, blok eşleştirmelerinin her bloğun hemen yanındaki blok ile yapılması, bu hali ile Holliman ve Memon'un [7] bahsettiği kolaj saldırılarına açık olmasıdır. Kolaj saldırısının yapılabilmesi için:

- Blok büyüklüğünün ve blok eşleştirmelerinin tahmin edilebilmesi,
- Elde oldukça fazla miktarda aynı algoritma ile damgalanmış ve doğrulanmış resim bulunması,
- Resimdeki bloklarla damgalı resimlerden kopyalanarak resme ihtal edilecek blokların yapay durmaması ve istenilen kötü amaçlı değişikliğe hizmet edecek bir görüntü elde edilebilmesi

gibi pek çok durumun biraraya gelmesini gerektirmektedir. Çok çok kritik bir faaliyet değil ise, kolaj saldırılarının yapılmasının pratikte tercih edilme ihtimali düşüktür. Algoritmaya damga ekleme aşamasında bir anahtar eklemek sureti ile daha güvenilir hale getirilerek orta güvenlikli ve yüksek PSNR isteyen işlerde algoritmanın kullanılabileceği değerlendirilmektedir.

Doğrulama amaçlı damgalamaların büyük çoğunluğunda tam kırılganlık istenen bir durum değildir. Resme yapılan ve resmin yorumunu etkilemeyen değişiklikleri tolere edebilen, resmin yorumunu etkileyebilecek değişiklikleri ise tespit edebilen yarı kırılgan damgalama algoritmaları tercih edilir. Bütün masum resim işlemlerini doğrulayıp kötü amaçlı tüm değişiklileri ortaya çıkarabilen bir algoritma mevcut değildir. Geliştirilen yarı kırılgan resim damgalama algoritmaları genelde tek bir resim değişikliği çeşidini, örneğin kayıplı resim sıkıştırmasını tolere edecek, bunun yanında resimdeki kes yapıştır tarzı oynamaları tespit edebilecek şekilde geliştirilmiştir. Yarı kırılgan damgalama algoritması, resimdeki bir nesnenin ortadan kaldırılması veya olmayan bir nesnenin konması veya kopyala yapıştır türü kötü

niyetli değişiklikleri tespit edebilmek kaydıyla, tolere edebildiği masum işlem kümesi ne kadar geniş ise o kadar başarılı sayılmaktadır. Bunun yanında, resmin asıl resme benzerliği ilkesi aşırı ihlal edilmemeli, kendisini devre dışı bırakma saldırılarına da algoritma savunma geliştirmiş olmalıdır. Doğrulama damgalama algoritmalarının büyük kısmı resmi bloklara ayırarak damgalama yapmaktadır. Bölüm 3.3.1.3.1 de anlatılan kolaj saldırılarına karşı, algoritma kapsamında yapılan blok çiftleştirme işlemi bir anahtar ve karıştırma algoritması kullanılarak hangi bloğun diğeriyle eşleştiği gizli tutulması gerekmektedir. Bahsi geçen hedeflerden yola çıkılarak, resim orta kısım ve kenar kısım olarak iki ana parçadan oluştuğu düşünülmüş, orta kısımlar küçük ebatlı bloklara, kenar kısımlar daha büyük ebatlı bloklara bölünmüştür. Resmin ana odak noktasının genelde orta kısım civarında olduğu varsayılmış, orta kısım blokları küçük tutularak buralarda yapılacak değişikliklerin daha hassas olarak saptanması, aynı zamanda orta bloklardan hesaplanacak blok resim özetlerinin de boyutlarının küçük olması sağlanmıştır. Orta bloklar daha sonra karıştırma algoritması ve anahtar kullanılarak kenar bloklarla eşleştirilmiştir. Daha büyük ebatlı kenar blokların damga sığası da geniş olacak şekilde orta bloklardan hesaplanan blok resim özetleri kenar bloklara damgalanmıştır. Orta blokların olduğu resim parçasının kesilip kullanılma ihtimaline karşı da, ilk olarak orta blokların olduğu bölüme sahiplik damgası uygulanmıştır. Geliştirilen algoritma, önceki geliştirilen yarı kırılgan damgalama algoritmalarına göre kayıplı sıkıştırma işlemine ilaveten gamma düzeltmesi, histogram eşitleme, parlaklık ayarlaması işlemlerini de tolere edebildiği görülmüştür. Damgalama yapılırken sabit bir damga kullanılmaması, damganın ana resime dayalı olarak üretilmesi, algoritmanın Holliman ve Memon'un çalışmasında [7] belirtilen kolaj (collage) ataklarına karşı da başarılı olmasını sağlamaktadır. Kolaj saldırılarına karşı dayanıklı, yapılan kötü niyetli değişiklikleri ortaya çıkarıp hassas bir şekilde sınırlarını tespit edebilen, hem sahiplik ispatı hem doğrulama damgalama amaçlarının ikisini de gerçekleştiren, DWT ve DCT uzaylarını kullanan yarı kırılgan başarılı bir algoritma geliştirilmiştir.

4.1 İlave Yapılabilecek Çalışmalar

Vektör resminin ana resme damga olarak eklenmesi ile ilgili yeni yöntemler geliştirilebilecektir. Tezdeki çalışmada svg dosyasının nümerik kısımları svg dosyasından ayrılarak ana dosyaya damgalanmakta, svg dosyasının nümerik

değerleri ihtiva etmeyen diğer kaynak kod çatısı ve kullanılan rastgele sayı dizileri adeta bir anahtar gibi karşı tarafa gönderilmek sureti ile karşı tarafta vektör resim damgası tekrar elde edilmeye çalışılmaktadır. Tezdeki yöntemimizden farklı olarak, svg formatındaki vektör resmin tamamen hafızada parse edilerek her bir nesne tipinin ve özelliklerinin farklı bir nümerik kodla ana resme damgalanması, nesne tipi ve önemli özellikler için daha vurgulu damgalama yapılması, görünüşü fazla değiştirmeyecek özellikler için damga gücünün daha az kullanılması denenebilecektir. Örneğin bir çember objesi için çemberin merkez koordinat değerleri ve yarıçapı çok önemlidir ancak çember çizgisinin renk değerleri (renkli durumda 3 tamsayı değeri) damga katsayısı daha küçük olarak damgalanabilir. İkinci olarak, vektör resminin damga olarak kullanılması tezde yapılmışken, vektör resminin ana resim olarak kendisinin damgalanması ayrı bir çalışma konusudur. Svg vektör resim formatının kaynak kodu metin tabanlı XML kodu olduğundan, metin dosyalarına daha önce uygulanmış olan damgalama metodları SVG dosyası için de geçerli olacaktır. Fazladan konulacak boşluk karakterleri kullanılabileceği gibi, xml dosyalarının da büyük-küçük harf duyarlı olmaması değerlendirilerek yine damgalama yapılabilecektir. Metin tabanlı damgalamanın pek çoğunun kolaylıkla ortadan kaldırılabildiği gibi svg xml kaynak kodunu metin dosyası yaklaşımıyla damgalamak ta aynı saldırılara maruz kalabilecektir. Svg xml kaynak kodu içerisindeki resim objelerinin kaynak kodu içerisinde hangi sıra ile bulunacağı, resim objelerinin özellikleri detaylı incelenmek sureti ile bu özelliklerde vektör resminin görünümünü fazla etkilemeyecek değişiklikler yaparak bir damgalama yönteminin geliştirilebileceği düşünülmektedir.

Doğrulama algoritmalarından ilki olan KırılganDoğKenarTopOrtDWT yönteminde blok eşleştirmesi gizli bir anahtara dayalı bir karıştırma algoritması ile yapılabilir, blok eşlerinden HL, LH, HH bantlarının toplamından elde edilen ikili değer yine gizli bir anahtar ile Xor işlemine tabi tutulduktan sonra damgalanabilir, böylelikle yöntem daha güvenli bir hale getirilebilir. İkinci olarak geliştirilen YarKırDoğDCTDWTOrtaKenar yöntemi ise KırılganDoğKenarTopOrtDWT yöntemindeki olabilecek güvenlik zafiyetlerini barındırmamaktadır.

Resim damgalama video damgalamanın da temelini oluşturmakta, bu konularda araştırma, geliştirme, iyileştirme devam etmektedir. Ülkemizde sayısal damgalama, hususi ile resim damgalama hukuk sistemimizde henüz delil olarak

kabul edilmemekte, pratikte yasal dayanağında eksiklikler bulunmaktadır. Öncelikle bu konuda yasal düzenleme yapılmasının telif hakları yönünden, orijinalliğin ispatı yönünden önemli olduğu düşünülmektedir.

KAYNAKLAR

[1] E. (Google C. Schmidt, “Every 2 Days We Create As Much Information As We Did Up To 2003,” 2010. [Online]. Available: https://techcrunch.com/2010/08/04/schmidt-data/.

[2] P. (Department of E. E. A. I. S. Christof, “APPLIED CRYPTOGRAPHY AND DATA SECURITY (Ruhr-Universitat Bochum Germany).” [Online]. Available: http://faculty.kfupm.edu.sa/ics/muhamadi/Richfiles/crypto-notes.pdf.

[3] “Auguste Kerckhoff Laws.” [Online]. Available: http://financialcryptography.com/mt/archives/000195.html.

[4] A. W. . A.-A. H. . A. Kunhu, “A new watermarking algorithm for scanned grey PDF files using DWT and hash function,” in *Communication Systems, Networks & Digital Signal Processing (CSNDSP), 9th International Symposium*, 2014, pp. 690–693.

[5] A. ;H. A. M. ; H. A.-A. Mahmoud, “A new watermarking algorithm for scanned colored PDF files using DWT and hash function,” in *Information and Communication Technology Research (ICTRC), International Conference*, 2015.

[6] P. Tao, A. M. Eskicioglu, and I. Science, “A robust multiple watermarking scheme in the Discrete Wavelet Transform domain,” in *Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference Philadelphia, PA*, 2004, pp. 133–144.

[7] M. Holliman and N. Memon, “Counterfeiting Attacks on Oblivious Block-wise Independent Invisible Watermarking Schemes,” *IEEE Trans. Image Process.*, vol. 9, no. 3, pp. 432–441, 2000.

[8] M. H. Shirali-shahreza and S. Mohammad, “A New Approach to Persian / Arabic Text Steganography,” in *5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR’06)*, 2006, pp. 1–6.

[9] W. Bender, N. Morimoto, and A. Lu, “Techniques for data hiding,” *IBM Syst. J.*, vol. 35, pp. 313–336, 1996.

[10] D. Huang and H. Yan, “Interword Distance Changes Represented by Sine Waves for Watermarking Text Images,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 11, no. 12, pp. 1237–1245.

[11] K. Bennett, “Linguistic Steganography: Survey,Analysis, and Robustness Concerns for Hiding Informationin Text,” 2004.

[12] M. Niimi, S. Minewaki, H. Noda, and E. Kawaguchi, “A Framework of Text-based Steganography Using SD-Form Semantics Model,” in *Pacific Rim*

Workshop on Digital Steganography,Kyushu Institute of Technology, Kitakyushu, Japan.

[13] M. Shirali-shahreza, “Text Steganography by Changing Words Spelling,” in *ICACT 2008*, pp. 1912–1913.

[14] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[15] R. G. Van Schyndel, a. Z. Tirkel, and C. F. Osborne, “A digital watermark,” *Proc. 1st Int. Conf. Image Process.*, vol. 2, pp. 86–90, 1994.

[16] M.A.Dorairangaswamy and B.Padhmavathi, “An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images,” in *IEEE international conference TENCON 2009*, 2009.

[17] S. de Audrey, *Herodotus-The Histories*. London: Penguin Books, 1996.

[18] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, “Vision of the unseen,” *ACM Comput. Surv.*, vol. 43, no. 4, pp. 1–42, Oct. 2011.

[19] Wikipedia, “Telif Hakkı.” [Online]. Available: https://tr.wikipedia.org/wiki/Telif_hakkı.

[20] I. J. M. L. . B. J. A. Cox, *Digital Watermarking*. Academic Press, 2002.

[21] A. R., “Information Hiding,” *Lect. Notes ın Comput. Sci.*, vol. 1174, 1996.

[22] B. J. ;Lo. S. T., “Copyright protection for the electronic distribution of text documents,” *Proc. IEEE*, vol. 87, no. 7, pp. 1181–1196, 1999.

[23] Q. G. M. ; E. K. W. ; N. D. Memon, “Data hiding in binary text documents,” *Proc. SPIE*, vol. 4314, pp. 369–375, 2001.

[24] A. M. A. O. M. Alattar, “Watermarking electronic text documents containing justified paragraphs and irregular line spacing,” *SPIE Proc.*, vol. 5306, 2004.

[25] G. R. C. and W. R. E., *Digital Image Processing*. Pearson International Edition, 2008.

[26] D. Zheng, Y. Liu, and J. Zhao, “A survey of RST invariant image watermarking algorithms,” *Can. Conf. Electr. Comput. Eng.*, vol. 39, no. 2, pp. 2086–2089, Jul. 2007.

[27] A. M. ; G. E. Eskicioglu, “Robust DWT-SVD Domain Image Watermarking : Embedding Data in All Frequencies,” 2004.

[28] S. R. V., R. S. Shekhawat, and V. K. Srivastava, “A DWT-DCT-SVD based digital image watermarking scheme using particle swarm optimization,” in

Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, 2012, pp. 1–4.

[29] M. Ali and C. Wook, "An optimized watermarking technique based on self-adaptive DE in DWT – SVD transform domain," *Signal Processing*, vol. 94, pp. 545–556, 2014.

[30] O. Jane, H. Gökhan, and E. Elbaşı, "A Secure and Robust Watermarking Algorithm Based on the Combination of DWT , SVD , and LU Decomposition with Arnold ' s Cat Map Approach," in *2013 8th International Conference on Electrical and Electronics Engineering (ELECO)*, 2013, no. 3, pp. 306–310.

[31] O. Jane, E. Elbaşi, and H. G. Ilk, "Hybrid non-blind watermarking based on DWT and SVD," *J. Appl. Res. Technol.*, vol. 12, no. 4, pp. 750–761, 2014.

[32] V. Aslantas, a. L. Dogan, and S. Ozturk, "DWT-SVD based image watermarking using Particle Swarm Optimizer," *2008 IEEE Int. Conf. Multimed. Expo*, pp. 241–244, 2008.

[33] H. H. Tsai, Y. J. Jhuang, and Y. S. Lai, "An SVD-based image watermarking in wavelet domain using SVR and PSO," *Appl. Soft Comput. J.*, vol. 12, no. 8, pp. 2442–2453, 2012.

[34] I. J. Cox, S. Member, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," in *Image Processing, IEEE Transactions*, 1997, vol. 6, no. 12, pp. 1673–1687.

[35] C. V. Piva, A., Barni M.,Bartolini F., "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image," pp. 520–523, 1997.

[36] "Arnold'a Cat Map Wiki Page." [Online]. Available: https://en.wikipedia.org/wiki/Arnold's_cat_map.

[37] J. N. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection," vol. 1, no. 10, pp. 2964–2969, 2007.

[38] M. Kutter and F. a P. Petitcolas, "A fair benchmark for image watermarking systems," *SPIE 3657, Secur. Watermarking Multimed. Contents*, vol. 3657, no. January, pp. 25–27, 1999.

[39] C. J. V. Den, B. Lambrecht, and J. E.Farrel, "Perceptual quality metric for digitally coded color images," in *EUSIPCO*, p. 1175.

[40] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 573–586, 1998.

[41] H. Modaghegh, K. R. Hossein, and M. R. Akbarzadeh-T, "A new adjustable blind watermarking based on GA and SVD," *2009 Int. Conf. Innov. Inf.*

Technol. IIT '09, no. December, pp. 6–10, 2009.

[42] M. M. Soliman, A. E. Hassanien, N. I. Ghali, and H. M. Onsi, "An adaptive watermarking approach for medical imaging using swarm intelligent," *Int. J. Smart Home*, vol. 6, no. 1, pp. 37–50, 2012.

[43] W. Zhu, Z. Xiong, and Y. Q. Zhang, "Multiresolution watermarking for images and video," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 9, no. 4, pp. 545–550, 1999.

[44] R. Dugad, K. Ratakonda, and N. Ahuja, "A new wavelet-based scheme for watermarking images," *Proc. 1998 Int. Conf. Image Process. ICIP98 (Cat. No.98CB36269)*, vol. 2, pp. 1–5, 1998.

[45] E. Elbasi and A. M. Eskicioglu, "Naïve Bayes Classifier Based Watermark Detection in," pp. 232–240, 2006.

[46] E. Elbasi and A. M. Eskicioglu, "A DWT-based robust semi-blind image watermarking algorithm using two bands," in *Proc. of SPIE-IS&T Electronic Imaging*, 2006, vol. 6072, pp. 1–11.

[47] E. E. Jane Onur, "A New Approach in Non-blind watermarking method based on DWT and SVD via LU decomposition," *Turkish J. Electr. Eng. Comput. Sci.*, pp. 1354–1366, 2014.

[48] M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 783–791, 2001.

[49] L. A. S. K. G. G, "Image Compression Using 2d Wavelet transform," vol. I, no. 2, 1992.

[50] J. N. Ellinas, "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection," *Proc. World Acad. Sci. Eng. Technol. Vol 25*, vol. 25, no. 10, pp. 438–443, 2007.

[51] H. L. H. Liu, J. L. J. Liu, J. H. J. Huang, D. H. D. Huang, and Y. Q. Shi, "A robust DWT-based blind data hiding algorithm," *2002 IEEE Int. Symp. Circuits Syst. Proc. (Cat. No.02CH37353)*, vol. 2, pp. 672–675, 2002.

[52] C. Technologies, "Robust Digital Image Watermarking in High Frequency Band Using Median Filter Function Based on DWT-SVD," pp. 47–52, 2014.

[53] a. Piva, M. Barni, F. Bartolini, and V. Cappellini, "DCT-based watermark recovering without resorting to the uncorruptedoriginal image," *Proc. Int. Conf. Image Process.*, vol. 1, pp. 520–523, 1997.

[54] M. Swanson, B. Zhu, and A. Tewfik, "Transparent Robust Image Watermarking," *Image Process. 1996. …*, pp. 211–214, 1996.

[55] J. J. K. O. Ruanaidh and T. Pun, “Rotation , scale and translation invariant spread spectrum digital image watermarking,” vol. 66, no. 5003, pp. 303–317, 1998.

[56] A. M. Alattar and D. Corporation, “REVERSIBLE WATERMARK USlNG DIFFERENCE EXPANSION OF TRIPLETS,” *Reading*, pp. 501–504.

[57] J. Lang and Z. Zhang, “Blind digital watermarking method in the fractional Fourier transform domain,” *Opt. Lasers Eng.*, vol. 53, pp. 112–121, 2014.

[58] O. Jane, H. G. İ, and E. Elba, “A Robust Transform Domain Watermarking Technique by Triangular and Diagonal Factorization,” in *36th International Conference on Telecommunications and Signal Processing, Roma, Italy, 2-4 July*, 2013, pp. 867–871.

[59] A. Kannammal and S. S. Rani, “Two Level Security for Medical Images Using Watermarking / Encryption Algorithms,” *Int. J. Imaging Syst. Technol. 24(1)*, 2014.

[60] M. S. Hsieh, D. C. Tseng, and Y. H. Huang, “Hiding digital watermarks using multiresolution wavelet transform,” *IEEE Trans. Ind. Electron.*, vol. 48, no. 5, pp. 875–882, 2001.

[61] X. Y. Wang, H. Y. Yang, and C. Y. Cui, “An SVM-based robust digital image watermarking against desynchronization attacks,” *Signal Processing*, vol. 88, no. 9, pp. 2193–2205, Sep. 2008.

[62] E. D. Aggarwal, E. S. Kaur, and E. Anantdeep, “An Efficient Watermarking Algorithm to Improve Payload and Robustness without Affecting Image Perceptual Quality,” vol. 2, no. 4, pp. 105–109, 2010.

[63] S. Amira-biad, T. Bouden, M. Nibouche, and E. Elbasi, “A Bi-Dimensional Empirical Mode Decomposition Based Watermarking Scheme,” *Int. Arab J. Inf. Technol.*, vol. 12, no. 1, pp. 24–31, 2015.

[64] S. Pereira and T. Pun, “Robust template matching for affine resistant image watermarks,” *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123–1129, 2000.

[65] H.-C. Huang and W.-C. Fang, “Metadata-based image watermarking for copyright protection,” *Simul. Model. Pract. Theory*, vol. 18, no. 4, pp. 436–445, Apr. 2010.

[66] V. S. Inamdar and P. P. Rege, “Dual watermarking technique with multiple biometric watermarks,” *Sadhana*, vol. 39, no. February, pp. 3–26, 2014.

[67] J. Li, H. M. Liu, and J. W. Huang, “A Robust Watermarking Scheme for City Image,” *Int. J. Secur. Its Appl.*, vol. 10, no. 1, pp. 303–314, 2016.

[68] A. Rocha, W. Scheirer, T. Boult, and S. Goldenstein, “Vision of the Unseen :

Current Trends and Challenges in Digital," vol. 43, no. 4, pp. 1–42, 2011.

[69] H. FARID, "Exposing digital forgeries in scientific images," in *Proceedings of the Multimedia and Security Workshop ACM*, 2006.

[70] H. PEARSON, "Image manipulation: CSI: Cell biology," *Nature*, no. 434, pp. 952–953, 2005.

[71] W. WANG, "Digital video forensics. Ph.D. dissertation. Department of Computer Science, Dartmouth College, Hanover, NH.," 2009.

[72] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," *Proc. Int. Conf. Image Process.*, vol. 2, pp. 680–683, 1997.

[73] P. Lin, C. Hsieh, and P. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery," *Pattern Recognit.*, vol. 38, no. 12, pp. 2519–2529, 2005.

[74] T. Lee and S. D. Lin, "Dual watermark for image tamper detection and recovery," vol. 41, 2008.

[75] X. Liu, C. Lin, and S. Yuan, "Blind dual watermarking for color images ' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 8215, no. c, pp. 1–9, 2016.

[76] J. S. Pillai and P. Theagarajan, "Semi Fragile Watermarking for Content based Image Authentication and Recovery in the DWT-DCT domains," *Int. Arab J. Inf. Technol.*, vol. 6.

[77] R. B. Wolfgang and E. J. Delp, "Fragile Watermarking Using the VW2D Watermark," *Proc. SPIE/IS&T Int. Conf. Secur. Watermarking Multimed. Contents*, vol. 3657, pp. 204–213, 1999.

[78] P. W. Wong and W. Road, "A Public Key Watermark for Image Verification and Authentication," *Image Process. 1998. ICIP 98. Proceedings. 1998 Int. Conf.*, vol. 1, pp. 455–459, 1998.

[79] J. Wu, B. B. Zhu, S. Liz, and F. Lin, "Efficient Oracle Attacks on Yeung-Mintzer and Variant Authentication Schemes *," in *IEEE International Conference on Multimedia and Expo (ICME)*, 2004, pp. 931–934.

[80] I. P. G. Voyatzis, "Chaotic mixing of digital images and applications to watermarking," in *Proceedings of the European Conference on Multimedia Applications Services and Techniques (ECMAST'96)*, 1996, pp. 687–689.

[81] R. Chamlawi, A. Khan, A. Idris, and Z. Munir, "A Secure Semi-Fragile Watermarking Scheme for Authentication and Recovery of Images based on Wavelet Transform," vol. 2, no. 2, pp. 727–731, 2008.

ÖZGEÇMİŞ

Kimlik Bilgileri

Adı Soyadı : Ahmet ŞENOL

Doğum Yeri : Bor-NİĞDE

Medeni Hali : Evli, 2 çocuk babası

E-posta : asenol@gmail.com

Adresi : Park Çiftlik Konutları CK4-48 Gayret Mah. Ymah. ANKARA

Eğitim

Lise : Maltepe Askeri Lisesi, İzmir (1985-1989)

Y.Lisans : Ortadoğu Teknik Üniversitesi Bilgisayar Mühendisliği, ANKARA (1989-1993)

Y.Lisans : Ortadoğu Teknik Üniversitesi Bilgisayar Mühendisliği, ANKARA (1993-1997)

Doktora : Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı, Ankara (2011-2018)

Yabancı Dil

İngilizce : KPDS, Yıl:2008, Not: 86

İş Deneyimi

09.1993-12.2017 : Kamu kurumunda veritabanı yöneticiliği, veritabanı ve web uygulamaları sistem analiz ve tasarımı, uygulama programcılığı, lojistik ve eğitim bilgi sistemlerinde yazılım ve alan bilgisi tecrübesi, lisans düzeyinde ders verme(işletim sistemleri, veritabanı yönetim sistemleri, kesikli matematik)

Deneyim Alanları

Veritabanı Yönetim Sistemleri, Programlama Dilleri, Web Programlama, Görüntü İşleme, Örüntü Tanıma, Resim Damgalama, Bilgi Güvenliği

Tezden Üretilmiş Projeler ve Bütçeleri

-

Tezden Üretilmiş Yayınlar

[1] Ahmet ŞENOL , Hayri Sever, “Dijital Damgalamaya Genel Bir Bakış”, Savunma Faaliyetleri ve Teknolojileri Bülteni , pp 17-20, Haziran 2016

[2] Ahmet ŞENOL , Hayri Sever, “Block Size Analysis for Discrete Wavelet Watermarking and Embedding a Vector Image as a Watermark”, International Arab Journal of Information Technology, Status : Under reviewing, PaperId : 15728, sent on 23 March 2017

[3] Ahmet ŞENOL , Hayri Sever, “A Semi-fragile Authentication and Proving Ownership Image Watermarking Using DWT, DCT”, Electronic Journal of University of Malaya EJUM, sent on 19th October 2017

Tezden Üretilmiş Tebliğ ve/veya Poster Sunumu ile Katıldığı Toplantılar

[1] A. Şenol, E. Elbaşı, K. Dinçer, and H. Sever, “A Block Size Analysis for Blocked Discrete Wavelet Watermarking,” 2014 International Conference on Information Security and Cryptology

[2] A. Şenol, E. Elbaşı, K. Dinçer, and H. Sever, “Blocked-DWT based Vector Image Watermarking,”, IEEE 23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı, pp. 0–3.

[3] A. Şenol, E. Elbaşı, K. Dinçer, and H. Sever, “A Blind Authentication Purpose Discrete Wavelet Watermarking” 30-31 October 2015 International Conference on Information Security and Cryptology

HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA TEZ ÇALIŞMASI ORJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 14/01/2018

Tez Başlığı / Konusu: **Esnek Resim Damgalama: Blok Tabanlı Damgalama Analizi, Vektör Damgası Kullanımı Ve Doğrulama Damgalamasının Geliştirilmesi**

Yukarıda başlığı/konusu gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler d) Sonuç kısımlarından oluşan toplam 122 sayfalık kısmına ilişkin, 05/Ocak/2018 tarihinde şahsım/tez danışmanım tarafından *Turnitin* adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 9 'dur.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar ~~hariç~~/dâhil
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

14.01.2018

Adı Soyadı:	Ahmet ŞENOL
Öğrenci No:	N10343920
Anabilim Dalı:	Bilgisayar Mühendisliği
Programı:	Bilgisayar Mühendisliği
Statüsü:	☐ Y.Lisans ☒ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

Prof.Dr.Hayri SEVER