YALOVA ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

GÖRÜNTÜLERDE SAYISAL DAMGALAMA VE VERİ GİZLEME

YÜKSEK LİSANS TEZİ

Sinan AY
(105105014)

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Müfit ÇETİN

Ortak Danışman: Dr. Ali DURSUN

EKİM 2013

YALOVA Üniversitesi Fen Bilimleri Enstitüsü'nün 105105014 numaralı Yüksek Lisans Öğrencisi **Sinan AY,** ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"GÖRÜNTÜLERDE SAYISAL DAMGALAMA VE VERİ GİZLEME"** başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Müfit ÇETİN** Yalova Üniversitesi	.....
Eş Danışman :	**Dr. Ali DURSUN** TÜBİTAK UEKAE	.....
Jüri Üyeleri :	**Prof. Dr. Yaşar BECERİKLİ** Yalova Üniversitesi	.....
	Doç. Dr. Müfit ÇETİN Yalova Üniversitesi	.....
	Yrd. Doç. Dr. Abdulkadir TEPECİK Yalova Üniversitesi	.....
	Dr. Ali DURSUN TÜBİTAK UEKAE	.....

Teslim Tarihi : **20 Eylül 2013**

Savunma Tarihi : **24 Ekim 2013**

Aileme,

ÖNSÖZ

Tez danışmanlarım sayın Doç. Dr. Müfit ÇETİN ve Dr. Ali DURSUN hocalarıma, tez çalışma sürecimde yaptığı değerli katkılardan dolayı teşekkür ediyorum. Özellikle beni yetiştiren annem ve babam başta olmak üzere zor zamanlarımda yanımda olan herkese minnetlerimi sunarım.

Ekim 2013

Sinan AY
(Bilgisayar Mühendisi)

İÇİNDEKİLER

Sayfa

KISALTMALAR

ADD **:** Ayrık Dalgacık Dönüşümü
AFD **:** Ayrık Fourier Dönüşümü
AKD **:** Ayrık Kosinüs Dönüşümü
ASCII **:** AmericanStandardCharacterInterchange
CCD **:** ChargeCoupled Device
DCT **:**DiscreteCosineTransform
EXE **:**Executable(Çalıştırılabilir)
HFD **:** Hızlı Fourier Dönüşümü
HTML **:**HyperTextMarkupLanguage
KZFD **:** Kısa Zamanlı Fourier Dönüşümü
LSB **:**LeastSignificant Bit
MSE **:**MeanSquaredError
PSNR **:**PeakSignaltoNoiseRatio
RMSE **:** RootMeanSquaredError
XML **:**ExtensibleMarkup Language

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

GÖRÜNTÜLERDE SAYISAL DAMGALAMA VE VERİ GİZLEME

ÖZET

Bu tezde sayısal damgalama ve steganografi yöntemleri açıklandı ve bu yöntemlerle ilgili bir uygulama gerçekleştirildi.

Dijital teknolojinin gelişmesiyle dijital ürünlerin kullanımı oldukça artmıştır ve video dosyaları, ses dosyaları ve resim gibi multimedya içerikleri çok kolay bir şekilde oluşturulabilir, iletilebilir, çoğaltılabilir ve değiştirilebilir hale gelmiştir. Fakat bu kolaylık sayısal ürününün içeriğinin değiştirilmesi gibi sorunlara neden olmuştur. Bu durum özellikle kritik sayısal ürünlerde çok ciddi sorunlara neden olmaktadır.

Araştırmacıların çoğu telif hakları, görüntünün içeriğinin korunması ve sahiplik ispatı gibi sorunların farkındadır. Bu şekildeki sorunları gidermek adına birçok yöntem sunulmuştur. Sayısal damgalama yöntemi de bu yöntemlerden biridir. Bu yöntem, sayısal verinin içine fark edilmeyecek şekilde bilgi yerleştirilmesi temeline dayanmaktadır ve gizli bilgi yerleştirilmiş olan dosyaya bakanlar, bilginin varlığından habersizdirler. Sayısal damgalama yöntemi video, ses ve resim gibi çoklu ortam dosyalarının içine veri yerleştirme yöntemi olarak sunulmaktadır.

Steganografi, gizli bilginin varlığından haberdar olmadan iletişimin gerçekleştirilmesi sanatı ya da bilimi olarak tanımlanabilir. Steganografi de amaç; gizli bilgiyi birbirlerine aktaran kişiler arasında güvenli ve kimsenin fark edemeyeceği şekilde iletişimin sağlanmasıdır. Gizli bilgiye sadece içeriğini bilen kişi tarafından ulaşılabilir, diğer kişiler gizli bilginin içeriğinden haberdar değildir ve içeriğe ulaşamamaktadırlar.

Steganografi ve sayısal damgalama yöntemleri birbirlerine oldukça benzemektedirler. Ancak ikisinin arasında belirgin fark vardır. Sayısal damgalamada temel amaç çoklu ortam dosya içeriğinin değiştirilmesinin engellenmesidir, amacına uygun olarak damga verisi insanlar tarafından fark edilebilir olması sorun teşkil etmemektedir. Ancak steganografi de çoklu ortam dosyasına bakan üçüncü kişinin, multimedya içeriğinde gizli bir verinin varlığından haberdar olmaması gerekmektedir. Eğer üçüncü kişi çoklu ortam dosyasında ki gizli bilgiyi görebiliyorsa ideal bir uygulama gerçekleştirilmemiştir.

Tezde önerdiğimiz metot bu iki yöntemi tek bir sayısal resimde gerçekleştirmektir. Sayısal damgalama ile resmin içinde gizli mesaj var ya da yok ayrımı yapılmaktadır. Steganografi yöntemiyle de gizli haberleşmeyi sağlamaktayız.

WATERMARKING AND STEGANOGRAPHY IN IMAGES

SUMMARY

In this thesis, digital watermarking and steganography techniques had been explained and an application had been applied.

Due to the rapid development of the digital technologies, digital products become very popular and it is easy to create, transmit, duplicate, and manipulate digital videos, photos, voices, and so on. Such convenience however leads to a problem, that is, it is also easy to tamper with the content of a digital product. The situation can be very serious especially when the media content is critical.

Many researchers are aware of the issues of copyright protection, image authentication, proof of ownership, etc. Hence, there are many solutions that have been proposed. The watermarking technique is one of the solutions. This technique embeds information so that it is not easily perceptible; that is, the viewer cannot see any information embedded in the contents. Digital watermarking refers to specific information hiding techniques whose purpose is to embed secret information inside multimedia content, like images, video, or audio data.

Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists.

Steganography and digital watermarking are very similar; however one big distinction must be highlighted between the two. In digital watermarking, the focus is on ensuring that nobody can remove or alter the content of the watermarked data, even though it might be plainly obvious that it exists. Steganography on the other hand, focuses on making it extremely difficult to tell that a secret message exists at all. If an unauthorized third party is able to say with high confidence that a file contains a secret message, then steganography has failed.

Proposed method in this thesiswe appliedto an image both methods. Digitalwatermarking detects whether or notthe data inimage. And steganography isusedto transmitthe secret message.

1. GİRİŞ

Hızla ilerleyen teknolojiinsan hayatına birçok kolaylıklar getirmiştir. Teknolojik gelişmeler sayesinde günümüzdeçok daha hızlı ve ucuz bilgi paylaşımı ortamına kavuşulmuştur.İnsanlar kolay bir şekilde internet üzerinden birçok veriye ulaşabilmekte ve bunları teknolojinin sunmuş olduğu imkânlar sayesinde hızla çoğaltabilmektedir. Ancak bu kolaylıklar insanları iki önemli sorunla baş başa bırakmıştır.

Bu sorunlardan birincisi internet ortamında güvenli veri iletişimidir.İnternetinsağladığı olanaklar sayesinde çok kolay bir şekilde her konu hakkında bilgiye ulaşılabilmekte ve bu bilgiler paylaşılabilmektedir. Ancak internetciddi güvenlik açıkları da beraberinde getirmiştir. Birbiriyle haberleşen iki kişi arasındaki iletişim bir üçüncü kişi tarafından erişilebilir ve değiştirilebilir hale gelmiştir.

Bu sorunu ortadan kaldırmak için farklı metotlar geliştirilmiştir. Bu metotlardan en çok bilineni şifreleme (kriptoloji) yöntemidir. Şifrelemede korunmak istenen veri şifreleme algoritmasıyla anlaşılmaz hale dönüştürülür ve bu şekilde istenen kişiye gönderilir. Fakat şifrelerin de zaman içinde kırılması mümkündür.

Şifrelerin kırılabilme ihtimaline karşı gönderilmek istenen bilgiyi kimsenin dikkatini çekmeden karşı tarafa aktarma metodu olan steganografi yöntemi geliştirilmiştir. Steganografi, taşınmak istenen mesajın başka bir ortamda saklanarak üçüncü şahısların iletilen mesajın varlığından haberdar olmasının engellenmesi yöntemidir.Bu yöntem sayesinde gizli bilgi herhangi bir şüphe uyandırmadan istenilen kişiye gönderilebilir.

Teknolojinin günümüzde getirdiği diğer bir sorunda çoklu ortam dosyalarının telif hakkının korunmasıdır. İnternet üzerinden yapılan iletişim, gönderilen bilgi ya da çalışmaların kolaylıkla yetkisiz kişilerin eline geçmesine; bu çalışmaların hızlı bir şekilde kopyalanmasına ve kopyaların hızla dağıtılabilmesine sebep olmaktadır. Bundan dolayı sayısal ortamda yapılan çalışmalarıntelif haklarının korunması sorunu ortaya çıkmıştır.

Çoklu ortam dosyalarının yetkisiz kişiler tarafından kopyalanması ve dağıtılması problemiher geçen gün büyümektedir. Bu sorun için önerilen çözümlerden biri sayısal damgalama yöntemidir. Sayısal damgalama; resim, video, ses ve metin gibi çoklu ortam dosyalarına gizli bir telif hakkı bilgisi yerleştirilmesi yöntemidir.

Bu çalışmada güvenli veri iletişimini sağlamak için geliştirilen steganografi yöntemi ile telif hakkının korunması amacıyla geliştirilen sayısal damgalama tekniği incelenmiştir.

1.1 Taşıyıcı Üzerinde Veri SaklamaYönteminin Tarihçesi

Tarih boyunca bilginin önemi kadar güvenli bir şekilde istenilen kişiye iletilmesi de önemli bir yer işgal etmiştir. Sayısal damgalama ve steganografi yöntemlerimetin, resim, video ve ses gibi çoklu ortam dosyalarına bilgi ekleme temeline dayanmaktadır.Bir taşıyıcı üzerinde ve bilgiyi gönderen kişi dışında kimsenin fark edemeyeceği şekilde taşınması yöntemi çok eskilere dayanmaktadır.

Tarihte bilinen ilk örtülü veri gizleme olayı milattan önceki yıllara dayanmaktadır. M.Ö. 485-525 yıllarında yaşayan Heredot bir çalışmasında Pers İmparatorluğu ile Yunan şehir devleti arasındaki savaş esnasında; Pers İmparatoruna iletilecek bilginin örtülü gizleme metodunun kullanıldığını aktarmıştır. Pers kralına gizli planı aktarmak için önceplanı taşıyacak kişinin kafası tıraş edilir. Daha sonra plantaşıyıcı kişinin kafasına yazılır ve saçları uzadıktan sonra yola koyulur. Gizli bilgiyi taşıyan kişi yolculuk boyunca kimsenin şüphesini çekmeden Pers kralına ulaşır.Pers kralına ulaşan taşıyıcısaçlarını tıraş ettirerek gizli bilgiyi aktarmış olur[1].

Eski tarihten bilinen diğer bir örnekte milattan sonra yaşayan PlinytheElder tarafından aktarılmıştır. PlinytheElder' in aktarmış olduğu bilgiye göre insanlar bir bitkinin sütünü kullanarak kâğıda saydam bir şekilde yazı yazmışlardır. Daha sonra saydam olarak yazılmış olan kâğıt ısıtıldığında kâğıtta yer alan yazıların kahverengine dönüşerek yazılan bilgiye ulaşılabildiğini aktarmıştır[1].

1518' de JohannesTrithemius, kriptoloji çalışmalarının bulunduğu kitabını yayımlamıştır. Bu kitabında steganografikşifreleme yöntemi kullanmıştır. Belli bir sıraya göre alınan harfler ile oluşturulan kelimeleringizlibir bilgi oluşturduğu ortaya çıkmıştır[1].

Eski Yunanistan'da, insanlar mesajları tahtaya yazıp üzerini mumla kaplarlardı. Böylece cisim kullanılmamış bir tablete benzerdi.Daha sonra mumun eritilmesiyle birlikte içindeki gizli mesaj okunabilirdi[2].

II. Dünya Savaşı sırasında, New York'taki bir Japon ajanı oyuncak bebek pazarlamacısı kılığı altında saklanmaktaydı. Bu ajan, Amerikan ordusunun hareketlerini bebek siparişi içeren mektuplar içine saklayarak Güney Amerika'dakiadreslere gönderiyordu [2].

1.2 Literatür Araştırması

Bu bölümde sayısal damgalama ve steganografi yöntemleri ile ilgili geçmite yapılan çalışmalar hakkında genel bilgiler verilecektir.

1.2.1 Sayısal damgalama ile ilgili yapılan çalışmalar

Sayısal damgalama Muzak Şirketi'nin [3], almış olduğu patentle tarihteki yerini almıştır. Gerçekleştirilenbu patent çalışmasındamüzik dosyalarına,telif haklarını korumak amacıylabir kimlik kodu yerleştirilebileceği gösterilmiştir.

Schyndel ve diğ. [4], resmin en anlamsız bitinde yapmış oldukları değişikliklerle damgalama işlemini gerçekleştirmişlerdir. Uzay düzleminde gerçekleştirilen bu yöntem kolay bir şekilde gerçekleştirilmesine rağmen saldırılara karşı oldukça dayanıksızdır.

Koch ve diğ. [5], çoklu ortam çalışmalarının telif hakkını koruma amaçlı yapmış oldukları çalışmada öncelikle orijinal görüntüyü 8x8'lik bloklara bölmüştür. Daha sonra her bir bloğun Ayrık Kosinüs Dönüşümünü (AKD) alıpdamga bilgisine göre orta frekans bölgesinde gerekli değişikleri yaparak damgalama işlemini gerçekleştirmiştir.

Cox ve diğ. [6], çoklu ortam dosyalarında uygulanabilecek sağlamlığı yüksek sayısal damgalama yöntemi önermiştir.

Kutter ve diğ. [7], uzay düzleminde orijinal görüntüye ihtiyaç duymadan damga bilgisinin geri elde edilebileceğini gösterenbir çalışma gerçekleştirmişlerdir. Bu çalışmada renkli görüntünün mavi piksel değerlerindeyapılan değişikliklerle damgalama işlemi gerçekleştirilmiştir.

Yeung ve Mintzer[8],imge doğrulamaamaçlı görünmez sayısal damgalama yöntemi gerçekleştirmiştir. Yapılan çalışmada damga eklenen görüntünün içeriğinde herhangi bir değişikliğin meydana gelip gelmediğinin tespiti yapılabilir.

Mohanty ve diğ. [9], yapmış oldukları çalışma ile sayısal görüntülerde telif haklarını korumak amacıyla görünür ve görünmez damgalama yöntemlerini birlikte kullanmışlardır.

Hsu ve Wu[10], imgenin doğruluğunu kanıtlamak amacıyla frekans düzlemindeDCT tabanlı bir damgalama algoritması önermişlerdir.

Takai ve Mifune[11], yapmış oldukları çalışmayla Fourier hologram tekniğini kullanarak damgalama işlemini gerçekleştirmişlerdir.

Shih ve Wu[12], uzay düzlemi ve frekans düzlemi yöntemlerini bir arada kullanarak sayısal görüntülerin kalitesinde daha az bozulma meydana getiren damgalama yöntemikullanmışlardır. Bu yöntemdedaha yüksek kapasiteli damgalamagerçekleştirmek için filigran iki parçaya ayrılmıştır. Filigranın bir bölümü uzay düzleminde en az değerlikli bitlerin değiştirilmesi ile görüntüye eklenmiştir. Ardından uzay düzleminde damgalanmışbu görüntüye frekans düzleminde filigranın diğer bölümü eklenmiştir.

Shieh ve diğ. [13], DCT yöntemini kullanarak yapmış olduklarıdamgalama yönteminde üzerinde değişiklik yapılacak frekansların seçimi için genetik algoritma yöntemini kullanılmışlardır. Çalışmada imgeye görünmez ve dayanıklı damgalanma işlemi gerçekleştirilmiştir.

Cai ve diğ. [14], faz kaydırmalı interferometre kullanarak gerçekleştirmiş oldukları çalışmada güvenlik seviyesi yüksek bir damgalama yöntemi sunmuşlardır.

1.2.2 Steganografi yöntemiyle ile ilgili yapılan çalışmalar

Kurak ve McHugh[15], resim dosyalarının piksel değerlerini oluşturan en az değerlikli bitinde değişiklik yapma temeline dayanan bir steganografi çalışmasıgerçekleştirmişlerdir.

Bender ve diğ. [16], yapmış oldukları çalışma ileresim, yazı ve ses gibi çoklu ortam dosyalarına bilgi gizlenebileceğini açıklamışlardır.

Marvel ve diğ. [17], hata kontrol kodlaması, görüntü işleme ve yayılı spektrum yöntemlerini kullanarak steganografi işlemi gerçekleştirmişlerdir. Yapılan çalışmada orijinal resme ihtiyaç duymadan gizli bilgiyi elde edilebilmektedir. Ayrıca alıcı ve göndericide aynı anahtarın bulunması gerekmektedir.

Lee ve Chen[18], LSB tekniğini kullanarak gri tonlu resimlerin piksel değerlerini oluşturan ilk dört bitinde yapılan değişiklikle yüksek kapasiteli steganografi işlemi gerçekleştirmişlerdir.Bu yöntemde %50' ye yakın kapasite artışı gözlenmiştir.

Tsengve Chang[19], jpeg uzantılı resimlerdeyüksek saklamakapasitesiileverisaklanabileceğini gösteren biryöntem geliştirmişlerdir. Yapılan çalışmada klasik yöntemlerde kullanılan AKD bileşenlerine sabit büyüklükte bilgi gizleme yerine; kapasite tahmin tablosuna göre veri gizleme yöntemi önerilmiştir. Böylece %20 civarında kapasite artışı sağlanmıştır.

Reddy ve Raja[20], çalışmalarında ADD kullanarak güvenli ve yüksek kapasiteli steganografi yöntemi kullanmışlardır. Çalışma taşıyıcı ve gizlenecek bilginin ADD'si alınıp güçlendirme katsayısı kullanılması temeline dayanmaktadır.

2. SAYISAL DAMGALAMA VE STEGANOGRAFİ

Sayısal damgalama ve stenografi ilk bakışta birbirlerine benzer görünseler de bu iki yöntem özellikle amaç bakımından oldukça farklıdır. Stenografide temel amaç gizli bilgiyi başkalarından koruyarak alıcıya ulaştırmaktır. Sayısal damgalamada ise temel amaç telif hakkını korumaktır.

Steganografi ve sayısal damgalama uygulamalarıçoklu ortam dosyalarınıniçeriklerini bu dosyalara zarar vermeden bir dereceye kadar değiştirilebilmesi ve insan görme sisteminin ses, görüntü ve renk kalitesindeki ufak değişiklikleri fark edememe özelliklerinden faydalanarak gerçekleştirilmektedirler.

Bu bölümde sayısal damgalama ve steganografi ile ilgili bilgiler yer alacaktır.

2.1 Sayısal Damgalama

Sayısal damgalamaçoklu ortam dosyalarınınizinsiz kopyalanarak çoğaltılmasını ve internetin sunmuş olduğu imkânlarla dağıtılmasını engellemek amacıyla önerilmiş yöntemlerden biridir. Sayısal damgalama yönteminde çoklu ortam dosyalarınaçeşitli amaçlarla bilgi saklanır. Saklanan bilginin, istediğinde gerielde edilip tekrar kullanılması amaçlanır.

Bilinen ilkfiligran örnekleri 1282 yılında İtalya'da kullanılmıştır.Bu filigranlar kâğıt kalıplar üzerine ince metal modeller eklenerek yapılmıştır. Yapılan işlem sonucunda kâğıt, metalin bulunduğu yerde daha ince ve saydam hale gelmiştir[21].

Filigranlar 18. yüzyıla kadar günümüzdeki kullanım amaçlarından farklı olarak kullanılmıştır. Bu zamana kadar filigranlar, kâğıt yaprakların yapıldığı kalıpları teşhis etmek, gizemli işaretleri temsil etmek veya dekorasyon olarak kullanılmışlardır. 18. yüzyıldan itibaren ise filigranlar Avrupa ve Amerika'da ticari marka oluşturmak ve para üzerinde sahtekârlığı önlemek amacıyla kullanılmaya başlanmıştır [22].

Sayısal görüntüler üzerindeki ilk damgalama uygulamaları piksellerin en az değerlikteki bitinin değiştirilmesiyle yapılmıştır.Her bir pikselin 24 bit ile temsil edildiği renkli resmedamga bilgisine ait 3 bitlik bilgi yerleştirilebilir. Bu işlem gerçekleştirilirken taşıyıcının en düşük değerlikli bitlerinin; damgalanacak bilgiye göre değiştirilmesi ile en basit görünmez damgalama gerçekleştirilir. Örneğin: "A" harfini ikilik sayı sisteminde "10000011" ile temsil edilir. Bu harfi damgalamak için üç pikselin son bitlerini Şekil 2.1'de görüldüğü gibi değiştirilir[2].

P_1(00100111	11101001	11001000)
P_2(00100111	11001000	11101001)
P_3(11001000	00100111	11101001)

(a) Orijinal resmin piksel değerleri.

P_1'(00100111	1110100**0**	11001000)
P_2'(0010011**0**	11001000	1110100**0**)
P_3'(11001000	00100111	11101001)

(b) Damgalanmış resmin piksel değerleri.

Şekil 2. 1: En az değerlikli bitin değiştirilmesiyle yapılan damgalama örneği.

Burada P_1, P_2 ve P_3 orijinal görüntünün piksel değerleridir. P_1', P_2' ve P_3' ise damgalama sonucu oluşan görüntüye ait piksel değerleridir. Bu yöntemde damga görüntünün en az değerlikli bitlerine saklandığından orijinal görüntüde yapılan değişiklerfark edilmemektedir.Ancak yapılacak saldırılar sonucu görüntü içindeki bilgi kolayca kaybedilebilir. Gizli bilginin damgalanacağı piksel değerliğinin arttırılması ile dayanıklılık arttırılabilir fakat görüntüde meydana gelen bozulmalar çok daha fazla olur.

2.1.1 Sayısal damgalamanın temelleri

Sayısal damgalamandatemel amaç bir damga sinyalinin taşıyıcı sinyale eklenmesi olarak söylenebilir. Taşıyıcı sinyal; resim, ses, video ya da metin gibi çoklu ortam dosyaları olabilir. Damga bilgisi yazı, resim, logo vb. şeyler olabilir.

Sayısal damgalama sisteminin tasarlanmasında üç temel unsur vardır. Bunlar aşağıdaki gibidir[23]:

(i) Taşıyıcı sinyale eklenecek olan damga sinyali *W*'nun tasarlanması. Damga sinyali genellikle *K* anahtarına ve damga bilgisi *I*'ya bağlıdır.

$$\boldsymbol{W = f_0(I, K)} \quad \textbf{(2.1)}$$

Kimi zaman taşıyıcı sinyal olan *X*'e de bağlı olabilir.

$$\boldsymbol{W = f_0(I, K, X)} \quad \textbf{(2.2)}$$

(ii) Damgalı veri *Y*'ninelde edilmesini sağlayacak olan taşıyıcı bilgi*X*'e; damga sinyali *W*'nunekleme yönteminin tasarlanması.

$$\boldsymbol{Y = f_1(X, W)} \quad \textbf{(2.3)}$$

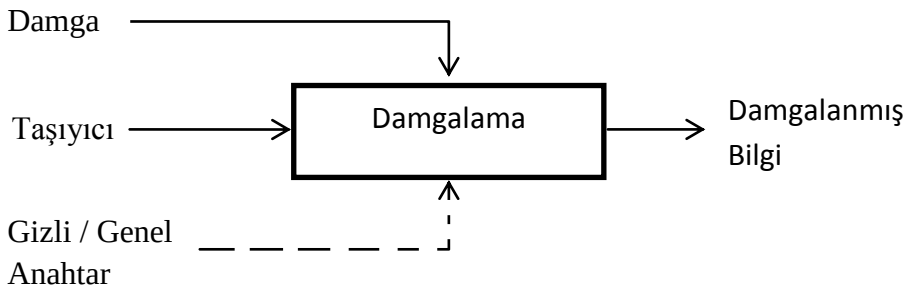
(iii) Damga bilgisinin geri elde etme işleminin tasarlanması. Bazen bu işlemi gerçekleştirirken kullanılan *K* anahtarı ve taşıyıcı sinyalin orijinal hali olan *X* gerekebilir.

$$\boldsymbol{I' = g(X, Y, K)} \quad \textbf{(2.4)}$$

Bazen de taşıyıcı sinyale ihtiyaç duyulmaz.

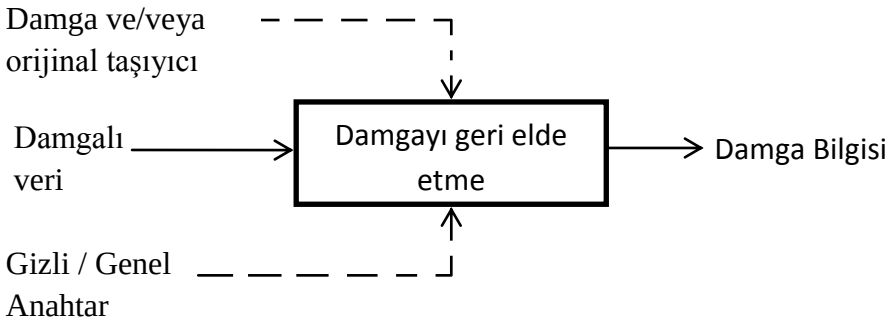
$$\boldsymbol{I' = g(Y, K)} \quad \textbf{(2.5)}$$

Şekil 2.2'de damgalama işlemi genel hatları ile görülmektedir.Damga ve taşıyıcıyı giriş verisi olarak kullanarak damgalama işlemi gerçekleştirilir. İsteğe bağlı olarak gizli veya genel bir anahtar da kullanılabilir. Bu anahtar güvenliği güçlendirmek amacıyla kullanılmaktadır. Belirlenen damgalama algoritmasına göre damga bilgisi taşıyıcı nesneye eklenir[23].



Şekil 2. 2: Genel sayısal damgalama işlemi.

Şekil 2.3'de ise damgayı geri elde etme işlemi yer almaktadır. Burada damgalamış veri, kullanılmış ise genel veya özel anahtar ve geri elde algoritmasının türüne göre taşıyıcının orijinal hali gerekmektedir. İşlemin sonucunda damga bilgisi elde edilmektedir[23].



Şekil 2. 3: Genel damgayı geri elde işlemi.

2.1.2 Sayısal damgalama türleri

Literatürde çeşitli amaçlara yönelik birçok damgalama yöntemi yer almaktadır. Şekil 2.4'de görüldüğü gibi damgalama yöntemleri; damganın saklandığı veri ortamının türüne, damgalama algoritmasının düzlemine ve insan görme sistemi tarafından görünüp görünmemesine göre farklı sınıflarda incelenebilir.

2.1.2.1 Algoritma düzlemine göre sayısal damgalama

Sayısal damgalama algoritma düzlemine göre uzay düzleminde ve frekans düzleminde olmak üzere iki gruba ayrılmaktadır. Frekans düzleminde gerçekleştirilen damgalama işlemleri uzay düzlemine göre daha sağlamdır [24].

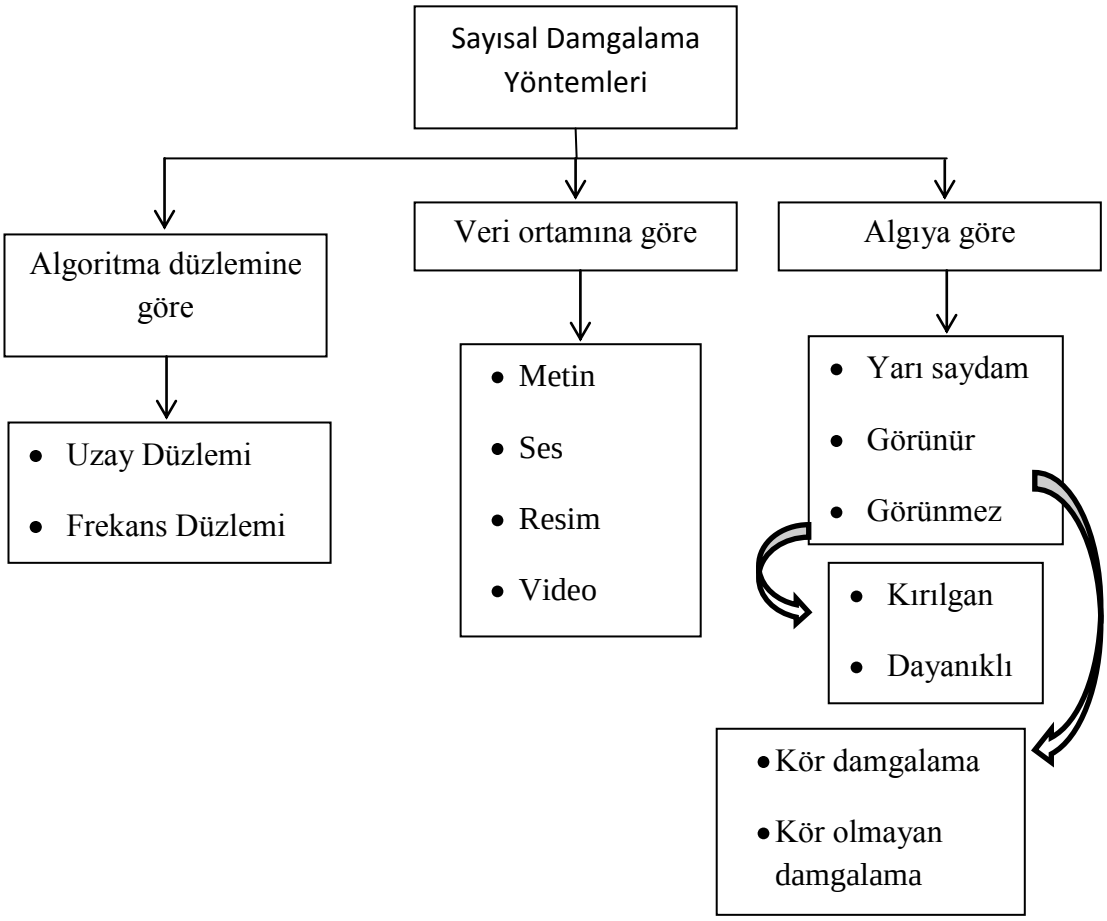
Uzay düzleminde sayısal damgalama

Uzay düzleminde gerçekleştirilen damgalama işlemlerinde resmin pikselleri üzerinde değişiklikler yapılır. En az değerlikli bit (LeastSignificant Bit, LSB) yöntemi uzay düzleminde sayısal damgalamada en çok kullanılan yöntemdir. Bu yöntem resmi oluşturan piksel değerlerinin son biti gizli verinin değerlerine göre değiştirilerek gerçekleştirilir.

Frekans düzleminde sayısal damgalama

Frekans düzleminde damgalama yapılırken taşıyıcı obje öncelikle frekanslarına ayrılır. Frekans dönüşümünü gerçekleştirmek adına Ayrık Kosinüs Dönüşümü (AKD), Ayrık Fourier Dönüşümü (AFD), Ayrık Dalgacık Dönüşümü (ADD) ve Hızlı Fourier Dönüşümü (HFD) literatürde yoğun bir şekilde kullanılmaktadır.

Frekans düzleminde yapılan damgalama işlemleri uzay düzlemiyle kıyaslandığında saldırılara karşı daha dayanıklıdır [24].



Şekil 2. 4: Sayısal damgalama türleri.

2.1.2.2 Veri ortamına göre sayısal damgalama

Veri ortamına göre damgalama görüntü, metin, ses ve video olmak üzere dört ana grupta gerçekleştirilmektedir[25]. Bunlardan görüntünün kopyalanması ve üzerinde değişiklik yapılması diğerlerine göre daha kolay olduğu için literatürde daha çok uygulaması yer almaktadır.

Metin damgalama;yönteminde damga düz bir metine belirlenen algoritmaya göre yerleştirilebilir. Kelimelerle satırlar arasındaki boşluklara, font şekillerinegöre yerleştirilebilir. Metinde yapılacak değişim sonucunda damganın geri elde edilmesi zordur.

Görüntü damgalama; damga bilgisinin resim dosyasına eklendiği damgalama türüdür. Resim dosyası renkli veya gri tonlu olabilir.

Ses damgalama ile ilgili yapılan çalışmada, damga doğrudan ses işaretine eklenmektedir.

Video damgalama; görüntü damgalama uygulamaları ile benzerdir.

2.1.2.3 Algıya göre sayısal damgalama

Damgalama yöntemleri algılama düzeyine göre üçe ayrılır. Bunları sıralayacak olursak;

- Yarı saydam damgalama,
- Görünür damgalama,
- Görünmez damgalamadır.

Yarı saydam damgalama;taşıyıcı üzerinde yarı saydam olarak görünen damgalama şeklidir. Bu damgalama türüne örnek olarak bazı haber videolarının ortasında yer alan haber ajanslarının logosu gösterilebilir.Bu damgalama türü genelde çoklu ortam dosyasının kime ait olduğunu tespit etmek amaçlı kullanılır.Şekil 2.5'de yarı saydam damgalı Lena resmi yer almaktadır.

Görünür damgalama; insan görme sistemi tarafından çok açık bir şekilde fark edilebilen damgalama türüdür. Telif hakkı koruma ve sahiplik tespiti uygulamaları için kullanılabilir [25].

Şekil 2. 5: Yarı saydam damgalı Lena resmi.

Görünmez damgalama;taşıyıcıya gözle algılanamayacak bir şekilde damgayı yerleştirme işlemidir. Görünmez damgalama yöntemi ile damgataşıyıcı nesne içerisine belli bir algoritma ile dağıtılır ve uygulanan algoritmanın tersi ile taşıyıcıdan geri elde edilir. Bu damgalama türünde damgalanmış taşıyıcıya bakan biri objede çok küçük değişikler meydana geldiği için her hangi bir şey fark edemez.

Çoklu ortam dosyalarının kötüye kullanılıp kullanılmadığının tespiti ve sahiplik ispatı için kullanılabilir [25].

Görünmez damgalamada kendi içinde dayanıklı ve kırılgan damgalama olmak üzere ikiye ayrılır.

Dayanıklı damgalama algoritmalarında damgalanmış veriye dışarıdan gelen sıkıştırma, gürültü ekleme gibi saldırılara karşı dayanıklı olması ve geri elde etme işleminden sonra geri elde edilmesi amaçlanmaktadır.

Kırılgan damgalamada ise damgalı veriye yapılacak olan değişiklikte damga bilgisi zarar görecek şekilde tasarlanır.Kırılgan damgalama daha çokiçerik doğrulama (contentauthentication) amacıyla kullanılır.

Geri elde etme algoritmasına göre sayısal damgalama

Sayısal damgalama tekniklerinde damga bilgisini elde etmek için kimi zaman taşıyıcı objeye ihtiyaç duyulurken kimi zamanda taşıyıcı obje ihtiyaç duyulmaz.

Damgalanmış görüntüden damgalama verisinin geri elde edilmesi için orijinal görüntüye ihtiyaç duyuluyorsa bu yönteme **kör olmayan damgalama**, eğer orijinal görüntüye ihtiyaç duyulmuyorsa bu yönteme **kör damgalama** yöntemi denir[26].

2.1.3 Sayısal veri damgalama tekniklerinin kullanım alanları

Sayısal damgalama yöntemi oldukça yaygın bir kullanım alanına sahiptir. Temel kullanım alanları aşağıdaki gibi sıralanabilir.

2.1.3.1 Telif haklarının korunması (Copyright)

Çoklu ortam dosyalarına eklenen sayısal damga sayesinde telif hakkı iddia eden kişi iddiasını kanıtlayabilir. Sayısal damgalama telif hakkı saklı olan çoklu ortam dosyalarını internet veya P2P (Peer topeer)gibi güvenli olmayan ağ üzerinden dağıtımına karşı korumak için kullanılabilir [27].

2.1.3.2 İçerik arşivleme

Resim, video ve ses dosyaları gibi sayısal ürünlerin arşivlenmesine yardımcı olmak amacıyla tanıtıcı bir nesne veya seri numarası ürüne yerleştirerek sayısal damgalama kullanılabilir. Bu yöntem aynı zamanda sayısal ürünlerin sınıflandırmasında ve düzenlenmesinde de kullanılmaktadır [27].

2.1.3.3 Meta-data ekleme

Meta-data bir verinin içeriğini tanımlayan veri anlamına gelmektedir. Bu uygulama alanında damgalama yöntemi ile resimler içeriğiyle birlikte etiketlenebilir ve arama motorlarında kullanılabilir;ses dosyaları şarkı sözleri ile birlikte veya sarkıcının adıyla taşınabilir;gazeteciler bir olaya ait fotoğraflara ilgili haberin kapak konusunuekleyebilir;tıbbi röntgenlere hasta kayıtları eklenebilir[27].

2.1.3.4 Yayın izleme

Sayısal damgalama yöntemi yayın izleme amaçlı olarak da kullanılmaktadır. Bir işletmenin ticari reklam yayınlarının uygun zamanda ve uygun sürede yayında olup olmadığını izlemek amaçlı kullanılmaktadır [27].

2.1.3.5 Değişiklik tespiti

Sayısal ürünün içeriğinde değişiklik yapılıp yapılmadığını tespit etmek amacıyla kırılgan damga yerleştirilebilir. Eğer kırılgan damga bozulmuşsa üründe bir değişiklik meydana gelmiştir. Bundan dolayı içeriğin doğrululuğuna güvenilemez. Değişiklik tespiti uydu görüntüleri ve sağlık görüntüleri gibi son derece hassas bilgiler içeren uygulamalar için çok önemlidir. Ayrıca mahkemelerde sayısal görüntülerin içeriğinde bir değişiklik olup olmadığını kanıtlamak için adli bir araç olarak da kullanılabilir[27].

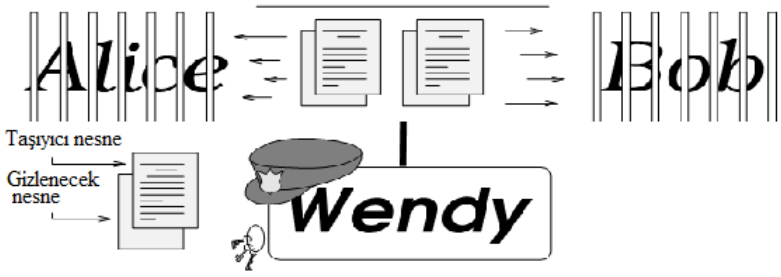
2.1.3.6 Sayısal parmak izi

Sayısal parmak izi sayısal içiriğin sahibini tespit etmek amacıyla kullanılmaktadır. Parmak izi sayısal içeriğin sahibine özeldir. Bundan dolayı sayısal bir ürünün farklı kullanıcılara ait farklı parmak izleri olabilir [27].

2.2 Steganografi

Steganografi sözcüğü, "örtü" veya "sır" anlamına gelen "steganos" ile "yazı" anlamına gelen "graphy" kelimelerinin bir araya gelmesiyle oluşmuştur. Steganografi adından da anlaşıldığı gibi gizli yazı anlamına gelmektedir.

Steganografi, Simons'un 1983 yılında literatüre kazandırmış olduğu mahkûmlar problemiyle özdeşleşmiştir.Bu senaryo Şekil 2.6'da görülmektedir[28].Mahkumlar planında Alice ile Bobhapishane içindedir ve kaçma planı hazırlamak istiyorlar. Ancak aralarındaki bütün haberleşme gardiyan Wendy'nin gözetiminde gerçekleşmektedir.Wendy, Alice ile Bob arasındaki tüm mesajlaşmaları gözetleyebilir, inceleyebilir ve dilerse değiştirebilir. Bu yüzden Alice ve Bob planlarını Wendy'nin dikkatini çekmeden masum görünümlü bir içerikle yapmalıdırlar[29].



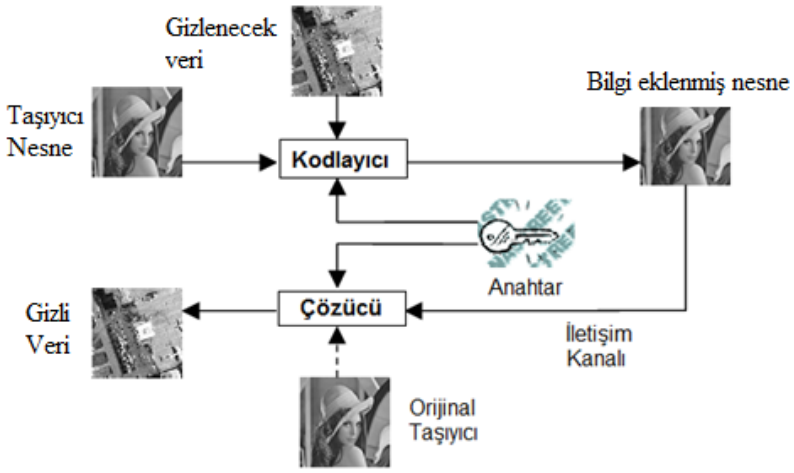
Şekil 2. 6: Steganografi ile özdeşleşmiş olan mahkûmlar problemi.

Almanlar, 2. Dünya Savaşı'nda birbirlerine yolladıkları sıradan bir metnin içindeki her sözcüğün baştan ikinci harflerine veriyi gizlemişler, metindeki ikinci harfleri yan yana getirince oluşan cümleyle gizli haberleşmeyi kimsenin dikkatini çekmeden gerçekleştirmişlerdir. Aşağıda bir Alman casusun 2.Dünya Savaşı'nda gönderdiği bir metin örneği yer almaktadır[30].

"Apparentlyneutral's protest is throughlydiscountedandignored. Isman hard it Blockadeissueaffectspretextforembargo on byproducts,ejectingsuetsandvegetableoils."

Her kelimenin ikinci harflerini aldığımızda oluşan mesaj şu şekildedir: "Pershingsailsfrom NY June 1."

Steganografi uygulamalarında gizli bilgitaşıyıcı objenin içine eklenerek istenen kişiye iletilir. Basit bir steganografi yapısı Şekil 2.7'de görülmektedir [31]. Burada gizli veri, taşıyıcı objeye veri gömme algoritmasıyla yerleştirilir ve iletişim kanalı ile alıcıya gönderilir. Steganografi yöntemlerinde güvenliği arttırmak adına genel veya özel anahtar da kullanılabilir. Alıcı steganografik objeye veri çıkarma algoritmasını uygulayarak gizli veriye ulaşabilir.



Şekil 2. 7: Steganografi yapısı.

2.2.1 Steganografiteknikleri

Steganografi yönteminde gizli veri resimden düz metine kadar çeşitli ortamlarda saklanabilmektedir. Bu bölümde farklı steganografi işlemleri hakkında bilgiler verilecektir.

2.2.1.1 Metin tabanlı steganografi

Bilgi gizlenecek ortamın metin olduğu steganografi yöntemidir. Metin tabanlı steganografi yöntemide kendi içerisinde şu şekilde sınıflandırılmaktadır[16]:

- Açık alan yöntemleri (Open Space Methods)
- Yazımsal yöntemler (SyntacticMethods)
- Anlamsal yöntemler (SemanticMethods)

Açık alan yöntemleri

Bu yöntem iki kelime arasında boşluklardan ve satır sonlarındaki boşluklardan faydalanarak gerçekleştirilir. Gerçekleştirilirken ASCII kodlarının kullanılması daha uygun olmaktadır. Üç farklı uygulama şekli vardır[16].

- **Cümleler arasında boşluk bırakma yöntemi**

Bu yöntemde metin içine her bir ifade sonlandırma karakterinden sonra bir ya da iki boşluk bırakarak ikili (binary) kod yerleştirilir. İfade sonlandırma karakteri olarak C programlama dilinde noktalı virgül kullanılırken; metin yazılar için nokta kullanılmaktadır.Ancak bu yöntemde her bir cümleye sadece bir bitlikbilgi yerleştirilebilecektir[16].

- **Kelimeler arasına boşluk bırakma yöntemi**

Bu yöntem kelimelerin arasına ekstra boşluk bırakarak gerçekleştirilir. Kelimeler arası bir boşluk "0" olarak, iki boşlukta "1" olarak değerlendirilir. Bu metotla her bir satıra birkaç bit yerleştirilebilir [16].

- **Satır sonuna boşluk bırakma yöntemi**

Bu yöntemde bilgiyi kodlamak için her bir satır sonuna boşluk bırakarak gerçekleştirilir. Bilgi kodlama işlemi, satır sonuna önceden belirlenmiş sayıda boşluk bırakarak yapılır. Her satırdaiki boşluk ile bir bitlik kodlama, dört boşluk ile iki bitlik kodlama ve sekiz boşluk ile üç bitlik kodlama yapılabilir. Bu yöntemde önceki yönteme göre daha fazla miktarda veri gizlenebilir [16].Şekil 2.8'de normal metin ve kodlanmış metin örneği yer almaktadır.

1	0		t	ü	r		i	n	s	a	n		v	a	r	d	ı	r	,
i	k	i	l	i	k		s	i	s	t	e	m	i		b	i	l	e	n
v	e		b	i	l	m	e	y	e	n	.								

(a)

1	0		t	ü	r		i	n	s	a	n		v	a	r	d	ı	r	,	
i	k	i	l	i	k		s	i	s	t	e	m	i		b	i	l	e	n		
v	e		b	i	l	m	e	y	e	n	.									

(b)

Şekil 2. 8: (a) Normal metin, (b) kodlanmış metin.

Yazımsal yöntemler

Bu metotta veriyi kodlamak için noktalama işaretleri kullanılır [16]. Örneğin *"ekmek, yağ, ve süt"* ifadesi ile *"ekmek, yağ ve süt"* ifadesi ilk bakışta benzer görünmektedir. Ancak ilk ifadede fazladan virgül bulunmaktadır. Belirlenen yönteme göre ifadelerin biri "1" değeride "0" olarak kodlanabilir.

Anlamsal Yöntemler

Bu yöntemde kelimenin kendisi değiştirilmektedir. Eş anlamlı kelimelere birincil ve ikincil değerler atanır [16]. Daha sonra bu değerler "1" ve "0" değerlerine dönüştürülür. Örneğin eşanlamlı olan "yetenekli" kelimesi birincil ve "kabiliyetli" kelimesi ikincil olarak seçilmiş olsun. Birincil kelime "1", ikincil kelime "0" olarak ikili koda dönüştürülür.

2.2.1.2 Görüntü steganografi

Taşıyıcı nesne olarak en yaygın olarak kullanılan steganografi yöntemidir. Çoğu özel amaçlı uygulamalar için kullanılan farklı sayısal görüntü türleri bulunmaktadır. Bu farklı görüntü türleri içinde farklı steganografi algoritmaları yer almaktadır[32].

Görüntüye bilgi gizlemek için uzay düzlemi, dönüşüm düzlemi, yayılı spektrum ve istatistiksel yöntemler gibi teknikleri kullanarak görüntü dosyalarında değişiklikler yapılır[33].

2.2.1.3 Ses steganografi

Bu yöntemde taşıyıcı nesne olarak ses dosyaları kullanılmaktadır. İnsan işitme sistemi 1/1000'den büyük frekans değerlerine karşı hassastır. Aynı zamanda rasgele olarak gerçekleşen seslere karşı da oldukça duyarlıdır [16]. Bu saydığımız nedenlerden dolayı ses dosyalarına veri gizlemek uğraş gerektiren bir konudur.

Ses dosyalarına bilgi gizlemek amacıyla kullanılan yöntemler şu şekildedir: düşük bit kodlaması (Low-bit encoding), aşama kodlaması (phasecoding), yayılım spektrumu (spreadspectrum) ve yankı veri gizlemesi (echo data hiding) [16].

2.2.1.4 Kullanılabilecek diğer ortamlar

Steganografi işlemini gerçekleştirmek için metin, ses ve görüntü dosyaları dışında kullanılabilecek başka ortamlarda bulunmaktadır. Sabit disklerdeki kullanılmayan alanlar, IP (Internet Protocol) paketlerindeki ileride kullanılmak üzere ayrılmış bölümler, XML, HTML veEXE dosyaları veri saklamak için kullanılabilmektedir.

2.3 Sayısal Damgalama ve Steganografi Tekniklerinin Kıyaslanması

Steganografi ve sayısal damgalama uygulamaları birbirlerine çok benzemektedirler. Her iki yöntemde de bir taşıyıcı ortam üzerine bilgi eklenmektedir. Ancak bu iki yöntem kullanım amacı bakımından birbirlerinden ayrılmaktadır. Steganografi de temel amaç bilgi gizlemek iken sayısal damgalama çoğunlukla telif hakkını koruma amaçlıdır. Ayrıca kimi zaman damgalama uygulamalarında damga bilgisi görünür bir şekilde taşıyıcıya eklenebilmektedir fakat steganografi uygulamalarında gizlenen içerik görünür olmamalıdır.

Çizelge 2.1'deWang ve Wang[34], tarafından derlenmiş steganografik ve sayısal damgalama yöntemlerinin benzerlikleri ve farklılıklarının yer aldığı çizelgeden derlenmiş bir özet yer almaktadır.

Çizelge 2. 1: Damgalama ile steganografi uygulamalarının karşılaştırılması.

	İhtiyaçlar	Damgalama		Steganografi
		Özel	Açık	
Amaç	Entelektüel hakların korunumu	++++		-
	Şüpheye mahal vermeden gizli veri iletimi	-		++++
Şartlar	İnsan duyuları açısından görünmezlik	++++		+++++
	İstatistiki ve algoritmasal görünmezlik	+		+++++
	Saldırıya, hileye ve çıkarıma dayanıklılık	+++++		-
	Normal sinyal işlemeye karşı dayanıklılık	++++		+
	Sıkıştırmaya karşı dayanıklılık	++++		++
	Yüksek gömme kapasitesi	++		++++
Geri elde etme	Orijinal görüntüye ihtiyaç olmayan	-	++++	++++
	Orijinal görüntüye ihtiyaç olan	++++	-	-
	Az işlem gücü ile kestirim	++		+++
Çok önemli:+++++ Gerekli:++++ Önemli:+++ İstenir++ İşe yarar:+ Gereksiz:-				

2.4 Kullanılan Performans Analizi Yöntemleri

Görüntüde ki değişim oranın belirlenmesi için çeşitli ölçme yöntemleri önerilmiştir. Bunlardan en çok bilinenleri: MSE (MeanSquaredError: Ortalama Karesel Hata), RMSE (RootMeanSquaredError: Ortalama Karesel Hatanın Karekökü) ve PSNR (PeakSignaltoNoiseRatio: Doruk Sinyal Gürültü Oranı) yöntemleridir.

MSE hataların kareleri toplamının ortalamasıdır ve genellikle σ^2 ile gösterilir. Matematiksel olarak ifadesi Eşitlik 2.6'da görülmektedir[35]. RMSE ise MSE'nin kareköküdür.

$$\boldsymbol{\sigma^2 = \frac{1}{N}\sum_{n=1}^{N}(x_n - y_n)^2} \quad \textbf{(2.6)}$$

Resimdeki bozulma oranını belirleme adına MSE yerine hata büyüklüğünün orijinal piksel değerinin en büyüğü (peak-tepe) ile olan ilişkisi ile ilgilenilir. Böyle durumlarda PSNR yöntemi kullanılmaktadır. PSNR yönteminin matematiksel ifadesiEşitlik 2.7'de yer almaktadır[35].

$$\boldsymbol{PSNR(dB) = 10log_{10}\frac{x_{peak}^2}{\sigma_d^2}} \quad \textbf{(2.7)}$$

Genel olarak MSE sonucunun düşük; PSNR değerinin yüksek değerli olması görüntüdeki bozulmanın az olduğu anlamına gelmektedir. PSNR değerinin kabul edilebilir olması için 30dB'den yüksek olması gerekmektedir [36].

3. TEORİK YÖNTEMLER

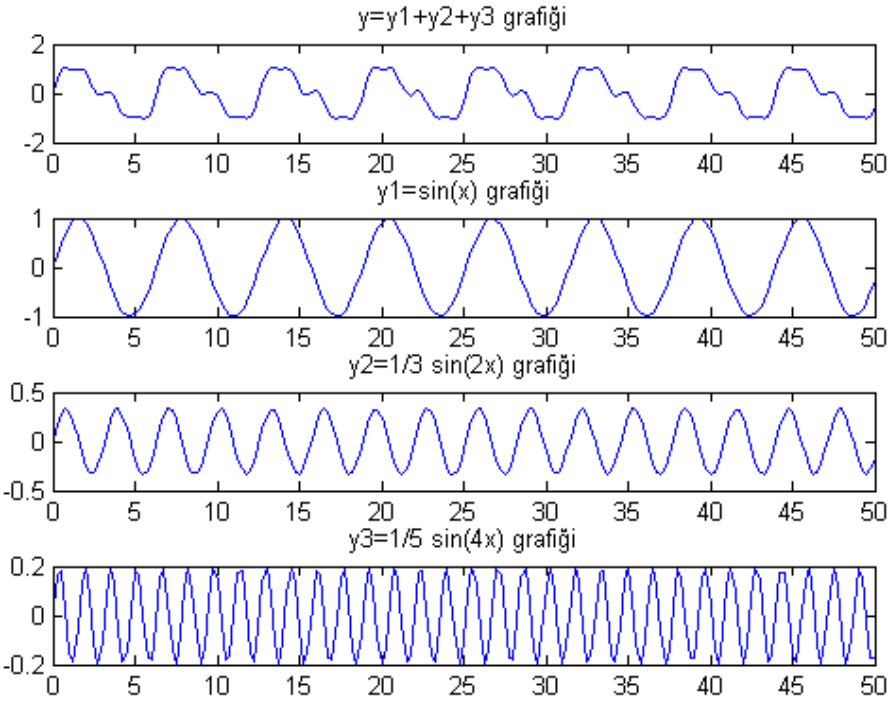
Tezin bu bölümünde sayısal damgalama ve steganografi uygulamalarını gerçekleştirirken kullanılan yöntemlerin teorik altyapısı incelenmiştir. İlk olarak steganografiişlemini gerçekleştirirken kullanılan ayrık dalgacık dönüşümü incelenecektir. Daha sonra damgalama işleminde kullanılan sayısal hologram konusuna değinilecektir.

3.1 Fourier Dönüşümü

Sinyaller temsil edilirken birçok yöntem kullanılabilir. Ham halde bulunan sinyaller çoğunlukla zaman düzlemindedir. Ancak sinyallerin zaman düzlemindeki temsili sinyalin özellikleri hakkında yetersiz bilgi içermektedir. Yapılacak dönüşüm işlemleri sonucunda karmaşıklığı daha az olan sonuçlar elde edilebilir ve elde edilen bu verilerle problem çözümleri daha basit bir şekilde gerçekleştirilebilir [37]. Bu nedenle sinyallere dönüşüm işlemlerini uygulayarak karakteristiği hakkında daha iyi yorumlar yapılabileceğifarklı düzlemde temsil edilmektedirler. Sinyalin temsil edilebileceği düzlemlerden biri frekans düzlemidir.Fourier dönüşümü de zaman düzleminden frekans düzlemine geçiş için kullanılan dönüşümlerden biridir.

Analiz işlemlerinde yaygın olarak kullanılan Fourier dönüşümü, herhangi bir periyodik fonksiyonun sinüzoidal bileşenlerine ayrıştırılması temeline dayanmaktadır. Bu yöntem ismini Fransız matematikçi ve fizikçi Joseph Fourier'den almıştır. Joseph Fourier yapmış olduğu çalışmada sinyallerin düzgün seçilmiş sinüzoidal bileşenlerinin toplamı şeklinde yazılabileceğini göstermiştir[38].

Şekil 3.1'de$y = \sin x + \frac{1}{3}\sin 2x + \frac{1}{5}\sin 4x$ fonksiyonunun Fourier dönüşümü ile sinüzoidal bileşenlerine ayrıştırılması gösterilmiştir.



Şekil 3. 1: Sinyalin sinüzoidal bileşenlerine ayrıştırılması.

Bir $x(t)$ sinyalinin Fourier dönüşümü olan $X(\omega)$, Eşitlik 3.1'de gösterilmiştir.

$$X(\omega) = \int_{-\infty}^{\infty} x(t).e^{-j\omega t}\,dt \qquad \textbf{(3.1)}$$

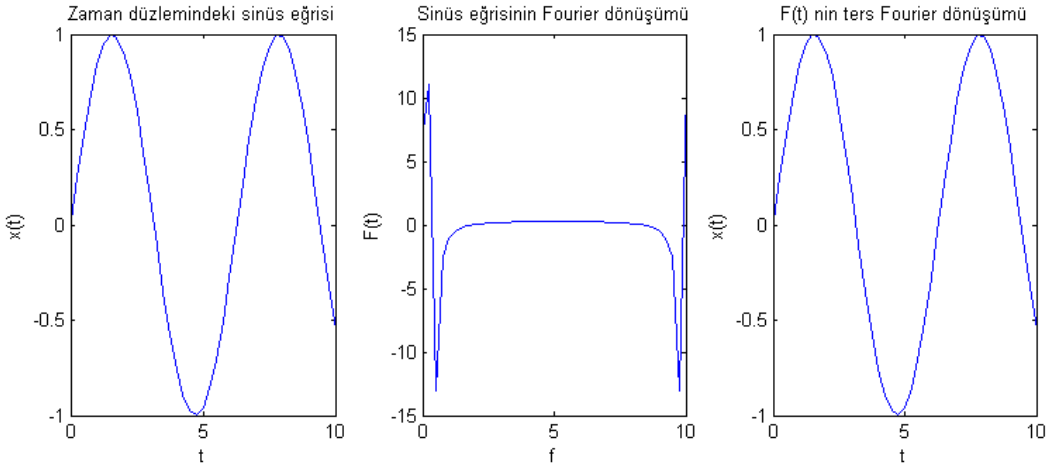
Eşitlik 3.1'de yer alan ω, açısal frekansı temsil etmektedir ve T, sinyalin periyodu olmak üzere Eşitlik 3.2'de ki gibi hesaplanmaktadır.

$$\omega = \frac{2\pi}{T} \qquad \textbf{(3.2)}$$

$X(\omega)$fonksiyonuna ters Fourier dönüşümü uygulanarak tekrar $x(t)$ sinyali elde edilebilir.

$$x(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} X(\omega).e^{j\omega t}\,d\omega \qquad \textbf{(3.3)}$$

Bir sinüs eğrisinin Fourier ve ters Fourier dönüşümü sonuçları Şekil 3.2'deyer almaktadır. Burada görüldüğü gibisinüs eğrisinin Fourier dönüşümü alındıktan sonrasinyal artık frekans düzleminde temsil edilmektedir. Eğer sinyal tekrar zaman düzleminde temsil edilmek isteniyorsa ters Fourier dönüşümü gerçekleştirilir. Böylece sinyalin tekrar zaman düzlemindeki temsili elde edilmiş olur.



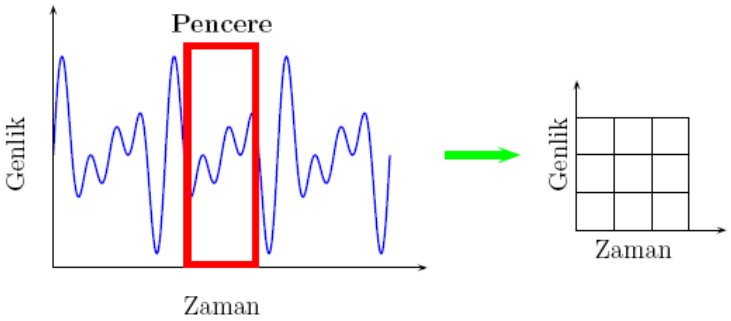
Şekil 3. 2: Sinüs eğrisinin Fourier ve ters Fourier dönüşümleri.

3.1.1 Kısa zamanlı Fourier dönüşümü

Kısa zamanlı Fourier dönüşümü (KZFD), pencerelenmiş Fourier dönüşümü olarak da bilinir. Fourier dönüşümü durağan sinyaller için yani zamanla frekans değerleri değişmeyen sinyaller için kullanışlı bir yöntemdir. Ancak durağan olmayan sinyallerde hangi frekans değerinin hangi zamanda gerçekleşmiş olduğu bilgisi önemli olduğundan bu sinyaller için kullanışlı olmamaktadır. Fourier dönüşümünün bu eksikliğini gidermek için DenisGabor, durağan olmayan sinyallerin analizi adına Fourier dönüşümüne yeni bir boyut kazandırarak KZFD yöntemini ortaya atmıştır. Aslında KZFD, Fourier dönüşümünü değiştirilmiş halidir.

KZFD'de sinyalin tamamına tek seferde Fourier dönüşümü uygulanmamaktadır. Sinyal parçalara bölünerek bloklar halinde getirilir. Daha sonra bloklara Fourier dönüşümü uyuglanır[39].

Şekil 3.3'deKZFD'nin temsili gösterimi ve Zaman-Genlik ilişkileri yer almaktadır.



Şekil 3. 3: KZFD gösterimi.

Eşitlik 3.4 ile bir sinyalin KZFD'si hesaplanabilir.

$$X_{KZFD}(\tau,\omega) = \int_{-\infty}^{\infty} x(t)\, w(t-\tau) e^{-j\omega t} dt \qquad \textbf{(3.4)}$$

Burada yer alan τ, zaman parametresini;ω ise frekansı temsil etmektedir. $w(t-\tau)$ise pencere fonksiyonu olarak adlandırılır.

KZFD'de pencere fonksiyonu, zaman ve frekans ayrışması açısından önemlidir. Seçilecek olan dar pencere ile iyi bir zaman çözümlemesi elde edilirken, frekans çözümlemesinde kötü bir sonuç elde edilir. Geniş pencere seçimi ile bir önceki durumun tersi gerçekleşmektedir[39].

3.2 Dalgacık Dönüşümü

Sinyalin frekans bileşenlerinin analizi için Fourier dönüşümü yoğun bir şekilde kullanılmaktadır. Fakat Fourier dönüşümünde frekans bilgisi ile zaman veya konum bilgisi eşzamanlı olarak gösterilememektedir. Frekansa bağlı olarak gelişen olayın zaman veya konuma bağlı olarak gösterilmesi için KZFD yöntemi önerilmiştir. Seçilen pencere fonksiyonunun tüm sinyal boyunca sabit bir pencere ile gezdirme temeline dayanan KZFD'de ayrı bir sorun ortaya çıkmıştır.Bu yöntemde karşılaşılan sorun ise pencere fonksiyonun sabit büyüklükte olmasıdır. Sinyal, KZFD'de sabit zaman ve frekans bileşenlerine göre analiz edilir. Bundan dolayı farklı zaman-frekans bileşenleri içeren sinyaller için etkili sonuçlar vermemektedir[40].

Dalgacık dönüşümü bu sorunu çözme adına önerilmiş bir yöntemdir. Çünkü: KZFD'de kullanılan sabit pencere boyutunun aksine dalgacık dönüşümünde pencere fonksiyonu sinyali farklı frekans ve zaman bileşenlerinde analiz etmek amacıyla çeşitli boyutlarda olabilir[41].

3.2.1 Sürekli dalgacık dönüşümü

Sürekli dalgacık dönüşümü (SDD), ana dalgacık fonksiyonunu bütün bir sinyal boyunca ölçeklendirilip, öteleyerek sinyalin analiz edilmesi işlemidir [42].

Bir $x(t)$ sinyalinin SDD'si Eşitlik 3.5 ile hesaplanabilir.

$$X_{DD}(s,\tau) = \frac{1}{\sqrt{s}} \int_{-\infty}^{\infty} x(t)\, \psi^*\left(\frac{t-\tau}{s}\right) dt \qquad \textbf{(3.5)}$$

Eşitlik 3.5'de yer alan s, ölçekleme parametresi; τ ise öteleme parametresi olarak adlandırılır. ψ^*, ana dalgacık fonksiyonu olan ψ' nin karmaşık konjügasyonudur.

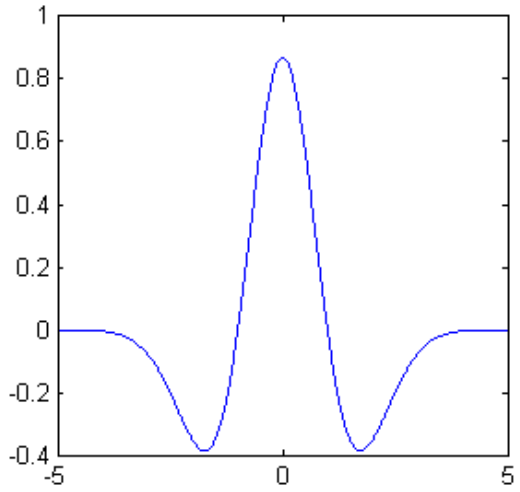
Öteleme, dalgacık fonksiyonunun zaman düzleminde gezdirilmesi işlemidir. Ölçekleme ise seçilen ana dalgacığın genişletilip daraltılması olarak tanımlanabilir ve frekansla ilgili bilgi üretir. Dalgacık dönüşümündeki ölçekleme parametresi haritalardaki ölçeğe benzemektedir. Haritalarda olduğu gibi yüksek ölçek sinyalle ilgili detaylı olmayan genel bir görünüm; düşük ölçek ise detaylı bir görünüm verir. Benzer şekilde düşük frekans yani yüksek ölçek sinyalle ilgili genel bilgiler verirken yüksek frekans sinyalin detay bilgilerini vermektedir [43].

3.2.1.1 Dalgacık türleri

Dönüşüm işlemlerini gerçekleştirirken seçilebilecek farklı dalgacık türleri bulunmaktadır. Bu bölümde bunlardan bazıları gösterilecektir.

Meksika şapkası (Mexican hat) dalgacığı

Meksika şapkası,Gaussian fonksiyonunun normalize edilmiş halidir.Meksika şapkası dalgacığı genellikle jeofizikte sismik verileri modellemede kullanılır[44]. Şekil 3.4' de meksika şapkası dalgacığı görülmektedir.



Şekil 3. 4: Meksika şapkası.

Matematiksel olarak Eşitlik 3.6' daki gibi ifade edilebilir:

$$\psi(t) = \frac{1}{\sqrt{2\pi\sigma^3}}\left(1 - \frac{\sigma^2}{t^2}\right)e^{\frac{r^2}{2\sigma^2}} \qquad (3.6)$$

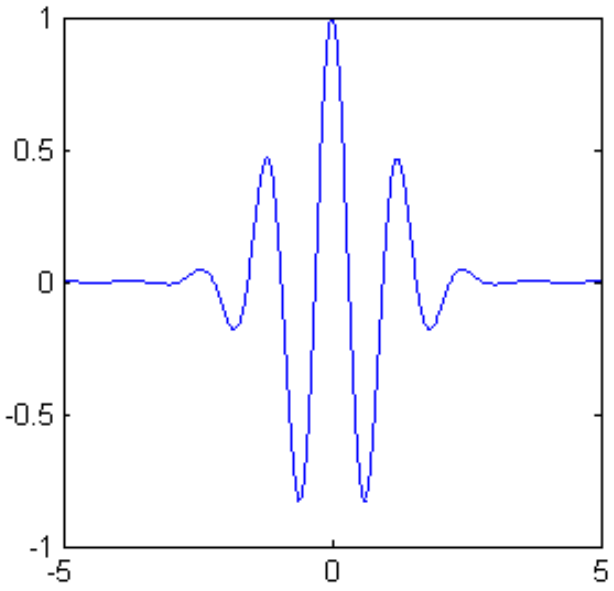
Morlet dalgacığı

Morlet dalgacığı matematiksel Eşitlik 3.7'deki gibi ifade edilebilir[45]. Eşitlikte bulunan f_b, bant genişliğini; f_c ise dalgacığın frekans merkezini temsil etmektedir.

Morlet dalgacığı genellikle sinyalin uyarılma halleri gibi kısa süreli bileşenlerini belirlemek için kullanılır[46].

$$\psi(t) = \frac{1}{\sqrt{2\pi f_b}} e^{j2\pi f_c t} e^{\frac{t^2}{f_b}} \quad \textbf{(3.7)}$$

Şekil 3.5' de Morlet dalgacığı görülmektedir.



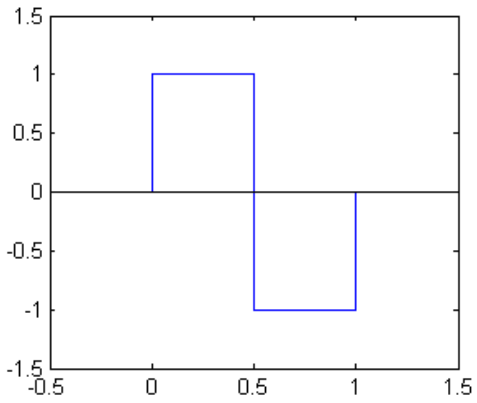
Şekil 3. 5: Morlet dalgacığı.

Haar dalgacığı

Haar fonksiyonları kenar belirleme, imge kodlama ve ikili mantık tasarımı uygulamalarında kullanışlıdır. Matematiksel ifadesi Eşitlik 3.8'de yer almaktadır[47].

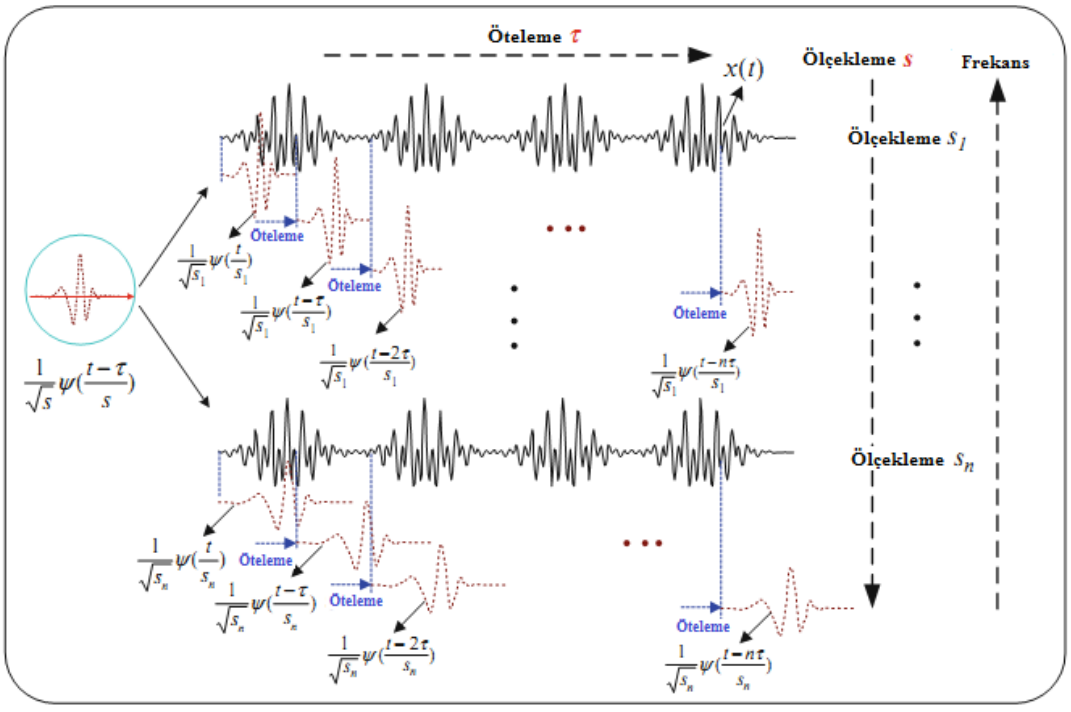
$$\psi(t) = \begin{cases} 1 & 0 < t < \frac{1}{2}; \\ -1 & \frac{1}{2} < t < 1; \\ 0 & diğer. \end{cases} \quad \textbf{(3.8)}$$

Şekil 3.6'daHaar dalgacığı görülmektedir.



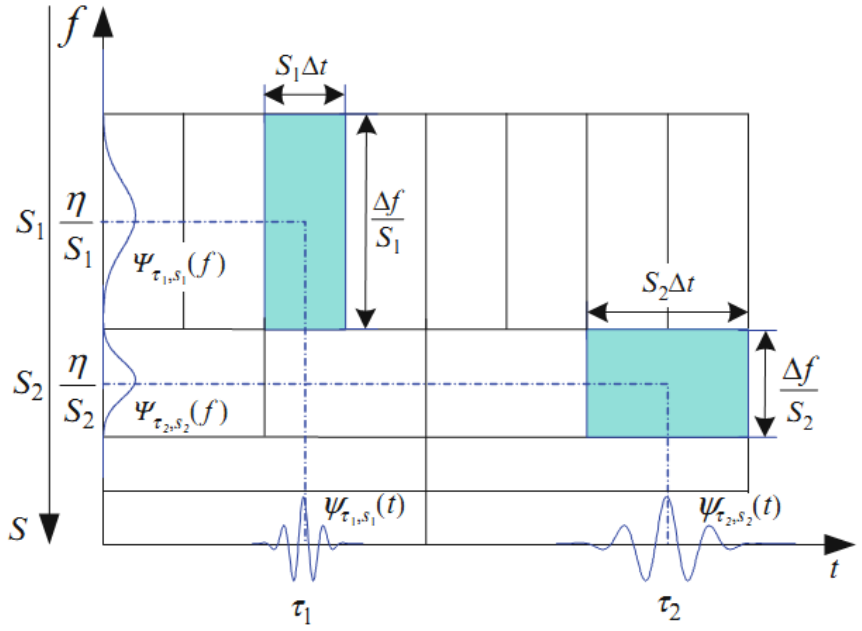
Şekil 3. 6: Haar dalgacığı.

SDD'de yapılan işlemler Şekil 3.7'de görülmektedir[48]. Burada seçilen ana dalgacık bütün sinyal boyunca farklı ölçeklerde gezdirilmektedir.



Şekil 3. 7: Dalgacık dönüşümünde öteleme ve ölçeklendirme.

Dalgacık dönüşümünün zaman-frekans analizi Şekil 3.8'degörülmektedir[48].Burada ölçek parametresi s değerinins_1'den s_2'ye ($s_2 = 2s_1$) çıkarılmasıyla birlikte; frekans çözünürlüğü iki katına çıkarken, zaman çözünürlüğü yarıya düşmektedir. Bu şekilde sinyal boyunca yüksek frekanslı bileşenlerin tespiti için küçük ölçek; alçak frekanslı bileşenlerin tespiti içinde büyük ölçek kullanılması dalgacık dönüşümün önemli bir özelliğidir[48].



Şekil 3. 8: Zaman-frekans çözümlemesi $s_2 = 2s_1$.

3.2.2 Ayrık dalcık dönüşümü

SDD işleminde ölçekleme ve öteleme parametrelerinin sürekliolmasından dolayı gereğinden fazla bilgi üretilmektedir. Gereksiz bilgilerin hesaplanması ciddi bir zaman kaybına neden olmaktadır. Dalgacık dönüşümündeki yapılan işlem sayısını düşürmek içinAyrık Dalgacık Dönüşümü (ADD) yöntemi kullanılmaktadır[49].

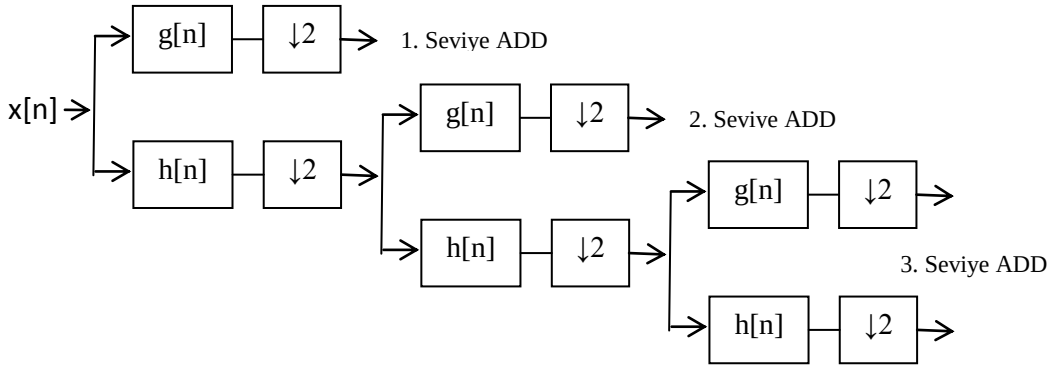
ADD, sinyali belirli ölçek grupları tespit ederek, tespit edilen bu ölçek gruplarında analiz işlemini gerçekleştirme temeline dayanmaktadır. Ölçekleme ve öteleme parametreleri ikinin üsleri şeklinde seçilmektedir. Eşitlik 3.5'deSDD formülü yer almaktadır. SDD'de yer alan ölçekleme ve öteleme parametreleri sırasıyla $s \epsilon R^+ - \{0\}$ ve $\tau \epsilon R$aralıklarında hesaplanmaktadır. Fakat ADD'de j ve k tamsayı olmak üzere $s = 2^j$ ve $\tau = k.2^j = k.a$olacak şekilde hesaplama yapılır.

ADD'de çoklu çözünürlük analizini elde edebilmek için ayrık işarete sırayla alçak ve yüksek geçiren filtreler uygulanmaktadır. Daha sonra ortaya çıkan değerler örnek azaltma işlemine tabi tutularak yarıya indirilir. Bir x[t] sinyalinin ADD çözümlemesinde, g[n] yüksek geçiren; h[n] alçak geçiren filtre olmak üzere aşağıdaki fonksiyonlar kullanılmaktadır.

$$\mathbf{y_{yüksek}[k] = \sum_n x[n]g(2k - n)} \quad \textbf{(3.9)}$$

$$\boldsymbol{y_{alçak}[k] = \sum_n x[n]h(2k - n)} \quad \textbf{(3.10)}$$

ADD işlemi Şekil 3.9'da görülmektedir. Her seviyede alçak ve yüksek geçiren filtreleme işlemleri uygulayarak farklı frekans sonuçları elde edilir[50].



Şekil 3. 9: Üç seviyeli dalgacık analizi.

Şekil 3.9'da x[n] ayrık sinyali temsil etmektedir. g[n], yüksek geçiren filtreyi; h[n] ise alçak geçiren filtreyi göstermektedir. Her seviyede, yüksek geçiren filtre sonucunda detay bilgileri; alçak geçiren filtre sonucunda yaklaşım (approximation) bilgileri üretilir. Ayrıca yapılan her filtreleme işleminden sonra çıkış sinyalinin boyutu yarıya düşürülmektedir.

3.3 Sayısal Holografi

Bu bölümde sayısal holografi konusunda temel bilgiler yer almaktadır.Holografiye genel olarak bakıldıktan sonra sayısal holografi ile ilgili bilgiler verilecektir.

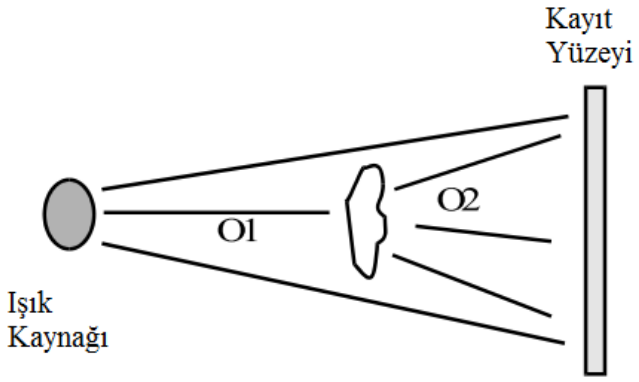
3.3.1 Holografinin temelleri

Holografi, Yunanca “bütün” anlamına gelen “holos” ile “yazı” anlamına gelen “graphy” kelimelerinin bir araya gelmesiyle oluşmuş bir terimdir. Holografi, cisimden gelen dalga bilgilerini belirli bir şekilde depo edip, bu bilgide hiçbir kayıp olmadan tekrar ortaya çıkartmayı sağlayan bir tekniktir.

Bu konuyla ilgili ilk çalışmaları yapan kişiDenisGabor’dur.DenisGabor holografi yöntemini 1947 yılında elektron mikroskopunun çözünürlüğünü artırmak için yapmış olduğu çalışmanın neticesinde bulmuştur. Yapmış olduğu çalışmanın sonucunda elektron mikroskopunun çözünürlüğünü artırmak yerine; elektron dalgaların oluşturduğu kırınım deseninde, bu deseni oluşturan dalgaların faz ve genliklerinin tüm bilgilerini yer aldığını anlamıştır.

Bu buluştan sonra holografi, bir görüntü kaydetme ve görüntüleme tekniği olarak kullanılmaya başlanmıştır. Bulunduğu yıllardaki teknolojik imkânsızlıklardan dolayı günümüzdeki kadar iyi görüntüleme yapılamamaktaydı. Lazerlerin keşfi ve Leithve Upatnieks[51]’in geliştirmiş olduklarıoff-axis aydınlatmasayesinde daha iyi bir görüntüleme metodu olarak günümüzde kullanılmaktadır[52].

Gabor’un çalışmasında kullanmış olduğu yöntem on-axis holografi olarak bilinmektedir. Şekil 3.10’da görüldüğü gibi saydam bir nesne, ışık kaynağından çıkan ışınlar ile aydınlatılır. Daha sonra nesneden yansıyan ve saçılan ışınlar ikinci bir ışın demetioluşturur.Referans demeti olarak adlandırılan ışık kaynağından gelen ışınlar ile nesneden yansıyan ve saçılan bu ışınlar bir kayıt ortamında çakıştırılarak kaydetme işlemigerçekleştirilir [53].

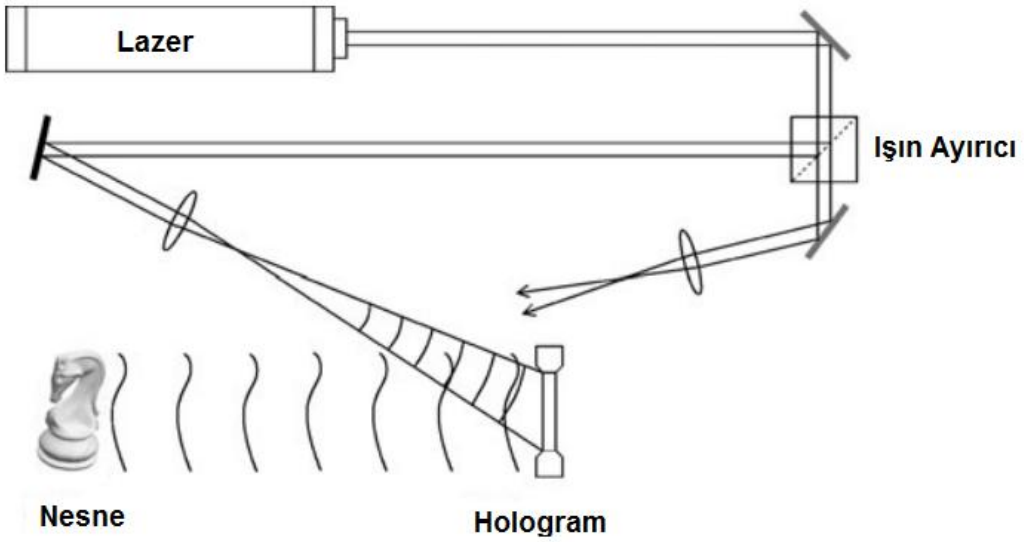


Şekil 3. 10: Gabor hologramın kaydedilmesi. (O1=Referans demeti; O2=Nesne demeti)

Holografide iki temel işlem yer almaktadır. Bunlar: hologram kaydetme ve hologramı yeniden yapılandırma işlemleridir.

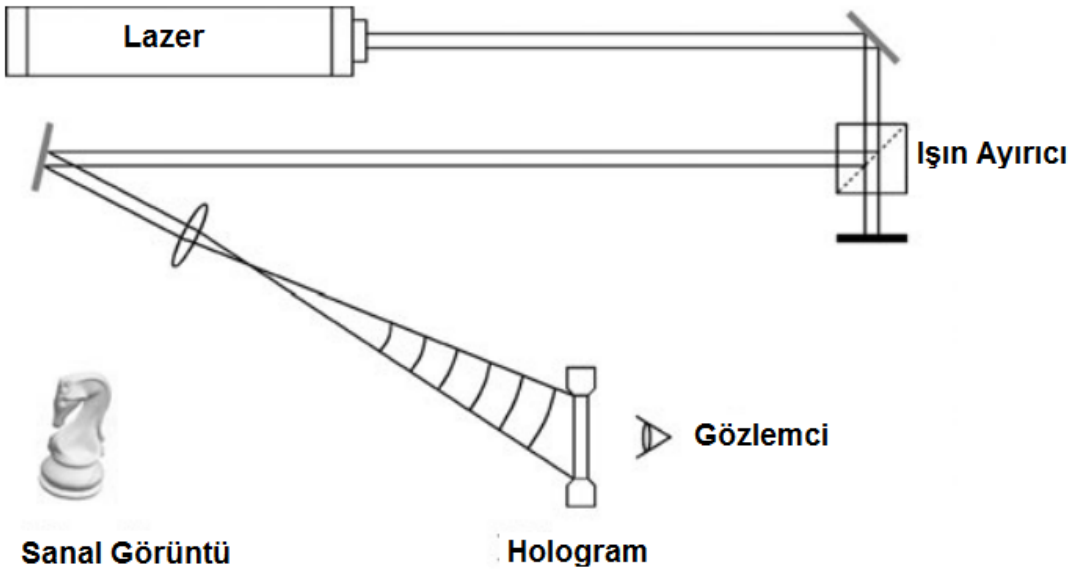
Off-axis hologram kaydının temel prensipleri Şekil 3.11'de yer almaktadır[54]. Şekil 3.11'de görüldüğü gibi eş fazlı ışık kaynağından çıkan ışınlar, ışın kırıcı vasıtasıyla ikiye ayrılmaktadır. Bunlardan biri direk olarak nesneyi aydınlatarak nesneden yansıma yapar ve yansıyan bu ışınlar plakanın üzerine düşer. Referans demeti olarak adlandırılan ikinci demet ise doğrudan plakayı aydınlatır. Bu iki ışın demetinin girişimi sağlanır ve girişim deseni kaydedilir. Oluşan bu girişim desenine hologram denilir[54].

Hologram genellikle düz bir ortama kaydedilmesine rağmen nesnenin üç boyutlu bilgilerini içermektedir.



Şekil 3. 11: Hologramın kaydedilmesi.

Hologram, Şekil 3.12'de görüldüğü gibi referans demetini kullanarak aydınlatıldığında orijinal nesne dalgaları tekrar oluşturabilir. Bu işlem sonucunda gözlemci sanal bir görüntü görmektedir. Ancak hologram kaydı ile oluşturulmuş olan bu sanal görüntünün gerçek nesneden bir farkı yoktur.



Şekil 3. 12: Hologramın yeniden yapılandırılması.

Hologramı oluştururken kullanılan nesne demeti $O(x,y)$ ve referans demeti $R(x,y)$'nin gösterimleri şu şekildedir:

$$O(x,y) = o(x,y)\exp\left(\mathrm{i}\varphi_o(x,y)\right) \quad \textbf{(3.11)}$$

$$R(x,y) = r(x,y)\exp\left(\mathrm{i}\varphi_r(x,y)\right) \quad \textbf{(3.12)}$$

Eşitlik 3.11'de yer alan $O(x,y)$ nesneden yansıyan ışık demetinin karmaşık genliğini; o, reel genliği ve φ_o, fazı temsil etmektedir.Eşitlik 3.12'de yer alan $R(x,y)$ referans demetinin karmaşık genliğini; o, reel genliği ve φ_r, fazı temsil etmektedir.

Bu iki dalga demetinin bir plaka üzerindeki girişimleri Eşitlik 3.13 ile hesaplanır.

$$I(x,y) = |O(x,y) + R(x,y)|^2$$

$$= (O(x,y) + R(x,y))(O(x,y) + R(x,y))^*$$

$$= R(x,y)R^*(x,y) + O(x,y)O^*(x,y) +$$

$$O(x,y)R^*(x,y) + R(x,y)O^*(x,y) \quad \textbf{(3.13)}$$

Bu denklemde yer alan * işareti karmaşık konjugesinitemsil etmektedir. Oluşturulmuş fotoğrafik yüzeyin genlik iletimi (amplitudetransmission) olan$h(x,y)$ile $I(x,y)$birbiri ile uyumludur.

Eşitlik 3.14'de bulunan $h(x,y)$, hologram fonksiyonu olarak adlandırılır. Denklemde yer alan β sabit bir sayıdır. τ, zamanı temsil ederken; h_0, yüzeyin genlik iletimidir.

$$\boldsymbol{h(x,y) = h_0 + \beta\tau I(x,y)} \quad \textbf{(3.14)}$$

Hologramın yeniden oluşturulması içingenlik iletimi(amplitudetransmission) ile referans demetinin karmaşık genliğinin çarpılması gerekmektedir.

$$R(x,y)h(x,y) = [h_0 + \beta\tau(r^2 + o^2)]R(x,y)$$
$$+\beta\tau r^2 O(x,y) + \beta\tau R^2(x,y)O^*(x,y) \quad \textbf{(3.15)}$$

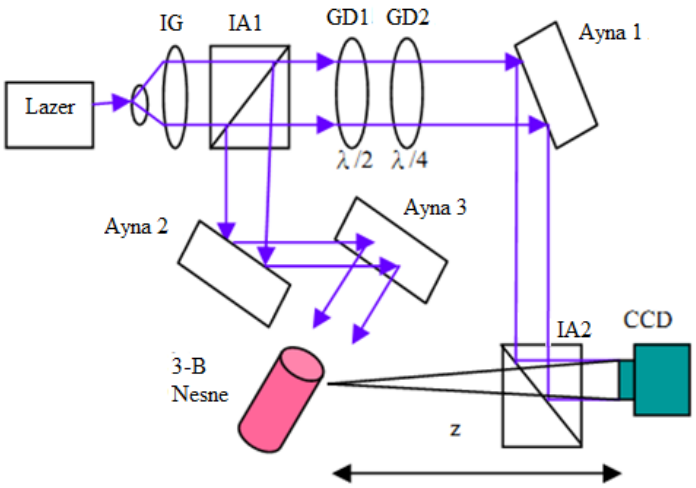
Eşitliğin sağ tarafındaki ilk terim referans dalgasıdır. Bu terim hologram boyunca kırınıma uğramamış dalgayı temsil etmektedir. İkinci terim sanal haldeki yeniden yapılandırılmış nesne dalgasını temsil eder. $\beta\tau r^2$katsayısı, sadece görüntünün parlaklığına etki eder. Üçüncü terim ise saptırılmış (distorted) gerçek görüntüyü temsil etmektedir.

3.3.2 Sayısal holografinin kaydedilmesi ve yeniden yapılandırılması

DenisGabor tarafından keşfedilen holografi, lazerin keşfi ve off-axis holografinin geliştirilmesi ile daha pratik ve güçlü bir araç haline gelip kendine birçok dalda uygulama alanı bulmuştur. Ancak geleneksel holografide fotoğrafik yüzeyin kullanımı maliyet ve zaman noktasında olumsuzluklara neden olmaktadır.

Son zamanlarda CCD kameraların kullanılmaya başlanmasıyla holografi farklı bir boyut kazanmıştır. Holografi, ışık demetinin faz ve genlik bilgilerinin kaydedilmesiyle üç boyutlu görüntüleme yapmayı sağlayan tekniktir. Sayısal holografi yönteminde CCD kameralar sayesinde klasik yöntemler göre holografik desen daha hızlı bir şekilde sayısal olarak oluşturulabilir ve yeniden yapılandırılabilir[55].

Sayısal hologram kaydetme işlemi Şekil 3.13'de yer alan Mach-Zendergirişimölçeri ile gerçekleştirilebilmektedir. Referans demeti ile nesneden yansıyan ışınlar cisimdenz kadar uzakla yer alan CCD kamera üzerinde girişime uğratılır. Bu girişim deseninin kaydedilmesi ile sayısal hologram oluşmuş olur.



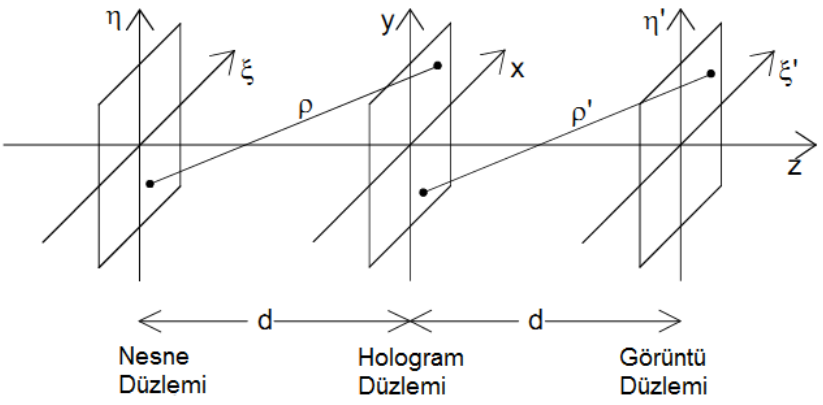
Şekil 3. 13: Sayısal hologram kaydetme işlemi (IG: Işın Genişletici, IA: Işın Ayırıcı, GD: Geciktirme Düzlemi).

Hologramın yeniden yapılandırılma işlemi referans demeti ile aydınlatılmasıyla gerçekleştirilir. Bu işlemin sonucunda üç boyutlu görüntü oluşur. Yeniden yapılandırma işlemin gerçekleştirebilmek için Fresnel-Kirchhoff integralinden faydalanarak elde edilen Eşitlik 3.16 kullanılır [56].

$$\Gamma(\xi',\eta') = \frac{i}{\lambda}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} h(x,y)E_R(x,y)\frac{\exp\left(-i\frac{2\pi}{\lambda}p\prime\right)}{p\prime}dxdy \qquad \textbf{(3.16)}$$

$$p' = \sqrt{(x-\xi)^2+(y-\eta)^2+d^2} \qquad \textbf{(3.17)}$$

Eşitlik 3.16'da yer alan $h(x,y)$, hologram fonksiyonunu temsil etmektedir. p'ise hologram düzlemindeki bir nokta ile yeniden yapılandırma düzlemindeki bir nokta arasındaki mesafeyi temsil etmektedir. Şekil 3.14'de bu durum görülmektedir.



Şekil 3. 14: Koordinat sistemleri arasındaki ilişki.

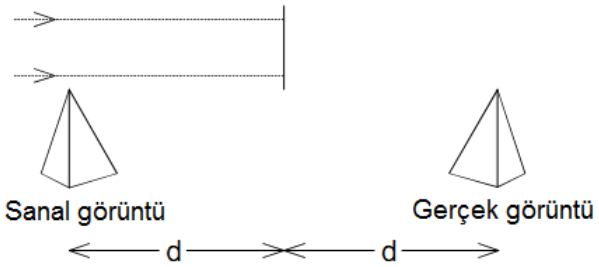
Eşitlik 3.18'deayrık Fresnel dönüşümü yer almaktadır.

$$\Gamma(m,n) = \frac{i}{\lambda d} exp\left(-i\frac{2\pi}{\lambda}d\right) exp\left[-i\pi\lambda d\left(\frac{m^2}{N^2\Delta x^2} + \frac{n^2}{N^2\Delta y^2}\right)\right]$$

$$\sum_{k}^{N-1}\sum_{l}^{N-1} U^*(k,l)U_h(k,l)exp\left[-i\frac{\pi}{\lambda d}(k^2\Delta x^2 + l^2\Delta y^2)\right] \exp\left[i2\pi\frac{(km+ln)}{N}\right]$$

(3.18)

Yeniden yapılandırma sonucunda oluşan sanal görüntü orijinal nesnenin konumunda yer alırken; gerçek görüntü CCD'nin ters yönünde ve *d* kadar uzaklıkta yer alır. Bu durum Şekil 3.15' de görülmektedir.



Şekil 3. 15: Referans demeti ile yeniden yapılandırma.

4. ÖNERİLEN YÖNTEM

Bu bölümde tez adına önerilen sayısal damgalama ve steganografi yöntemlerinin nasıl gerçekleştirildiği hakkında bilgi verilecektir.

4.1 Steganografi Yöntemi

Literatürde önceki bölümlerde anlatıldığı üzere steganografi adına birçok yöntem yer almaktadır. Yapılan uygulamada steganografi işlemleri frekans düzleminde gerçekleştirilmiştir. ADD yöntemini kullanarak elde edilen katsayılarda belirlediğimiz algoritmaya göre değişiklikler yaparak gizlenecek veri yerleştirilmiştir.

Steganografi işlemi için taşıyıcı resim olarak 512x512 boyutunda gri tonlu resim ve gizli bilgi olarak 64x64 boyutunda siyah-beyaz resim kullanılmıştır.

4.1.1 Gizli bilgiyi ekleme işlemi

Sayısal resme bilgi gizleme işlemi aşağıdaki yol takip edilerek gerçekleştirilmiştir.

- Taşıyıcı resmin ADD' si alınarak birinci seviye her biri 256x256 boyutunda olan LL_1, LH_1, HL_1, HH_1 katsayılarıelde edilir.
- LL_1 matrisi de ADD işleminden geçilerek ikinci seviye 128x128' lik LL_2, LH_2, HL_2, HH_2 katsayıları elde edilir. Daha sonra LL_2, ADD işleminden geçilerek 64x64' lük LL_3, LH_3, HL_3, HH_3 katsayıları elde edilir.
- Boyutu 64x64 olan gizli bilgi, 4096x1'lik satır matrisi haline getirilir.
- Taşıyıcı resme uygulanan üç seviye ADD sonucunda oluşan matrislerden sırasıyla HH_3, HL_3, LH_3, LL_3, HH_2, HL_2, LH_2, LL_2, HH_1, HL_1, LH_1 matrisleri 8x8'lik matrisler halinde bloklara ayrılır.
- Oluşan 8x8' lik her bir bloğa gizli bilginin bir piksellik bilgisi yerleştirilir.

- Gizlenecek bilgi siyah-beyaz resimden oluştuğu için 4096x1' lik satır matrisini değerleri 0 veya 1 olacaktır. Gizlenecek bilginin piksel değeri 0' a eşitse ve 8x8'lik matrisin (5,2) ve (4,3) değerlerine bakılır. Eğer (5,2) değeri, (4,3)'den büyükse ise blok üzerinde herhangi bir değişiklik yapılmaz. Ancak matrisin (5,2) değeri, (4,3)'den küçükse matris üzerinde gerekli işlemler yapılarak (5,2) > (4,3) şekline dönüştürülür.
- Eğer mesaj 1'e eşitse mesajın 0'a eşit olduğunda yapılan işlemlerin tersi yapılır. Yani (5,2)< (4,3) şekline dönüştürülür.
- Bu işlemlerden sonra 8x8' lik matrisin (5,2) ile (4,3) değerleri arasındaki fark belirlemiş olduğumuz eşik değeri *k*'danküçük ise fark eşik değerine uygun olarak yeniden yapılandırılır.

Bu işlemler gizli verinin tüm pikselleri için gerçekleştirildikten sonra ters ADD işlemi uygulanarak gizli bilgi eklenmiş resim elde edilir.

Şekil 4.1'de ADD' si alınmış olan resmin 8x8'lik bir bloğu görülmektedir. Eklenecek gizli bilginin sıradaki piksel değerinin 0' a eşit olduğu durumda bilgi gizleme işlemi tamamlandıktan sonraki durumu Şekil 4.2'deki gibi olacaktır. Burada görüldüğü gibi bloğun (5,2) ve (4,3) değerleri veri gömme algoritmasına göre değişmiştir.

3.2500	20.0000	12.0000	2.2500	24.7500	18.2500	31.3750	110.1250
4.5000	4.0000	2.6250	5.3750	27.5000	4.0412e-14	37.3750	91.6250
2.2500	1.0000	6.7500	23.8750	0.3750	9.0000	33.1250	85.0000
2.5000	2.3750	0.6250	21.3750	8.6250	8.2500	14.7500	102.5000
3.0000	0.8750	9.8750	1.1250	14.6250	0.7500	17.7500	100.7500
0.8750	12.5000	22.0000	3.7500	15.6250	3.2500	22.8750	107.8750
0.7500	18.2500	53.7500	8.8750	44.1250	4.5000	27.0000	104.8750
23.7500	41.6250	95.1250	91.3750	39.0000	6.7500	25.2500	116.1250

Şekil 4. 1:ADD'si alınmış taşıyıcı resmin 8x8' lik bir bloğu.

3.2500	20.0000	12.0000	2.2500	24.7500	18.2500	31.3750	110.1250
4.5000	4.0000	2.6250	5.3750	27.5000	4.0412e-14	37.3750	91.6250
2.2500	1.0000	6.7500	23.8750	0.3750	9.0000	33.1250	85.0000
2.5000	2.3750	-1.8750	21.3750	8.6250	8.2500	14.7500	102.5000
3.0000	3.3750	9.8750	1.1250	14.6250	0.7500	17.7500	100.7500
0.8750	12.5000	22.0000	3.7500	15.6250	3.2500	22.8750	107.8750
0.7500	18.2500	53.7500	8.8750	44.1250	4.5000	27.0000	104.8750
23.7500	41.6250	95.1250	91.3750	39.0000	6.7500	25.2500	116.1250

Şekil 4. 2:ADD'si alınmış taşıyıcı resmin veri gömüldükten sonraki görünümü.

4.1.2 Gizli bilgiyi geri elde etme işlemleri

Veri gömme işleminin ardından oluşan görüntünün içerisinde artık gizlenmiş bilgi yer almaktadır.Oluşan bu resme aşağıdaki işlemler uygulanırsa gizli bilgi tekrar elde edilmiş olacaktır.

- Gizli verinin gömülü olduğu resim dosyasının üç seviye ADD' si alınır.
- Ayrıştırma sonucunda oluşan HH_3, HL_3, LH_3, LL_3, HH_2, HL_2, LH_2, LL_2, HH_1, HL_1, LH_1 katsayılarını sırasıyla 8x8' lik bloklara bölünür.
- Oluşan her bir blok için (5,2) ile (4,3) değerleri arasında kıyaslama yapılır.
- Eğer (5,2) > (4,3) ise mesajın ilgili pikseli 0'a eşit olur.
- Eğer (5,2) < (4,3) ise mesajın ilgili pikseli 1'e eşit olur.Yapılan işlemler sonucunda 0 ve 1'lerden oluşan satır matrisini, 64x64' lük matris haline getirilir ve gizlenen bilgi geri elde edilmiş olur.

4.2 Sayısal Damgalama Yöntemi

Tez için yapılan uygulamada sayısal damgalama işlemi holografik damgalama yöntemi ile gerçekleştirilmiştir. Taşıyıcı resim ve damga bilgisi için 512x512'lik gri tonlu resimler kullanılmıştır.

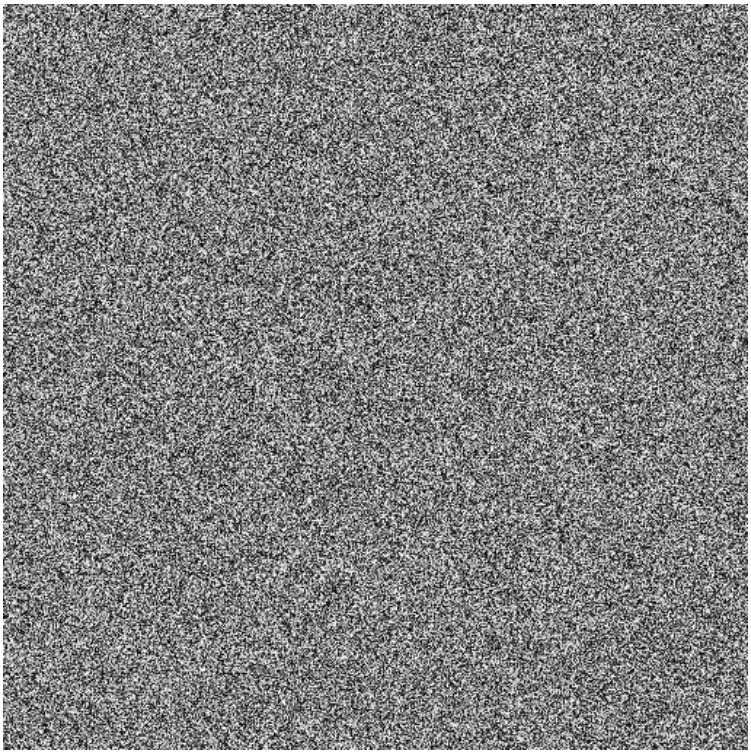
4.2.1 Holografik damgalamanın gerçekleştirilmesi

Hologram kaydetme işleminde ışının dalga boyu ve nesne ile kayıt ortamı arasındaki uzaklık bilgileri ekstra bir güvenlik anahtarı oluşturmaktadır. Doğru dalga boyu ve uzaklık bilgisi olmadan damga bilgisi doğru bir şekilde çıkarılamayacaktır. Buda damga bilgisine yetkisiz kişilerin ulaşamaması adına bir güvenlik oluşturacaktır.Hologram kaydetme işlemi aşağıdaki gibi gerçekleştirilmektedir.

- Hologram kaydetme ve yeniden yapılandırma işlemleri için kullanılacak ışının dalga boyu, nesne ile kayıt ortamı arasındaki uzaklık mesafesi ve cisim ile kayıt ortamı arasındaki açı bilgileri belirlenir.
- Belirlenen değerlere göre damga bilgisinin hologram kaydı elde edilir. Oluşan hologram Şekil 4.3'de yer almaktadır.

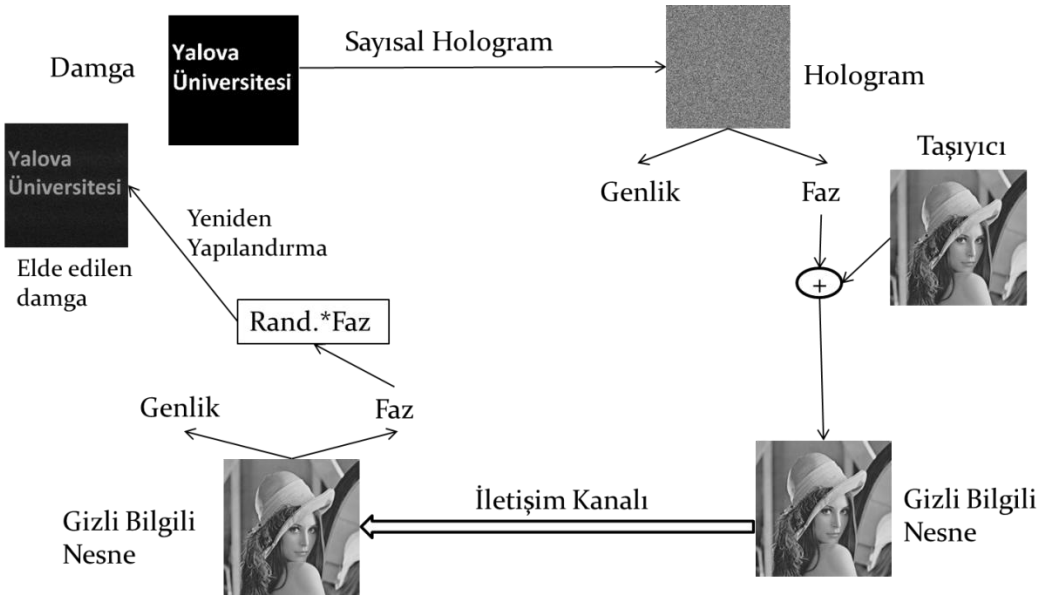
- Taşıyıcı belirlenen ağırlık katsayısı ile çarpılır. Ardından hologramın faz bilgisi ile bir araya getirilir.Böylece sayısal damgalama işlemi gerçekleştirilmiş olur.

Damga bilgisinin tekrar elde edilme işlemi için alıcının hologram oluştururken kullanılan dalga boyu, uzaklık ve açı mesafelerini bilmesi gerekmektedir. Bu bilgiler ile optik transfer fonksiyonunu oluşturup; hologramı yeniden yapılandırarak damga bilgisi elde edilebilir. Yapılandırma işlemi gerçekleştirilir ve damga bilgisi elde edilmiş olur.Bu işlemler Şekil 4.4'de yer almaktadır.



Şekil 4. 3: Oluşturulan hologram.

Damga bilgisini elde edebilmek için damgalı bilginin faz bilgisine rasgele değerlerden oluşan genlik bilgisi eklenir. Ardından doğru değerlerle yeniden yapılandırarak damga bilgisi elde edilir. Doğru bir şekilde yeniden yapılandırılan hologram Şekil 4.5'de yer almaktadır. Şekilde görüldüğü gibi doğru yapılandırılan hologramda damga bilgisi net bir şekilde görülebilmektedir.



Şekil 4. 4: Sayısal holografi ile damgalama işleminin gerçekleştirilmesi.

Şekil 4. 5: Hologramın yeniden yapılandırılması.

5. SİMÜLASYON SONUÇLARI

Tez için Matlab Simülasyon programını kullanarak, sayısal damgalama ve steganografi uygulaması gerçekleştirilmiştir.Gerçekleştirilen uygulama ile tek bir sayısal resme gizli bilgi ekledikten sonra damgalama işlemini geçekleştirilebilmektedir.

Tezde kullanılan steganografi yöntemi ile gizli haberleşme işlemi yapılırken sayısal damgalama sayesinde alıcı, mesajın içeriğinde herhangi bir bilginin var olup olmadığını anlayabilecek ve gizli bilgi var ise damga bilgisine göre gönderici hakkında bilgi sahibi olabilecektir.

5.1 Steganografi Yönteminde Elde Edilen Sonuçlar

Steganografi metodunun adımları Bölüm 4.1'de anlatılmıştır. Bu bölümde gerçekleştirilen uygulamanın sonuçları yer almaktadır.

Kullanılan yönteme göre Şekil 5.1(a)'da yer alan taşıyıcı resmin üzerine Şekil 5.2 (a)'da yer alan bilgi eklenirse elde edilen yeni resim Şekil 5.1(b)'de yer almaktadır.Şekil 5.1 (a) ve Şekil 5.1 (b)'de görüldüğü gibi her iki resim birbirine benzemesine rağmen oluşan yeni görüntüde gizli bilgi yer almaktadır.

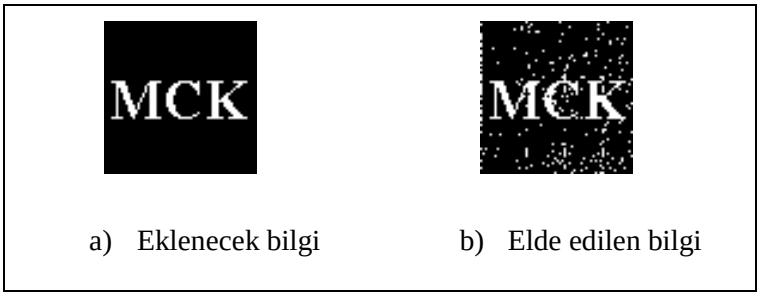
Bilgiyi ekleyen kişi dışındaki kimseler resimde gizli bilginin varlığından haberdar olmayacaktır.Gizli bir şekilde haberleşmek isteyen iki kişini bu yöntemle hiçbir şüphe çekmeden haberleşebilir. Bu özellik steganografi yönteminin diğer bilgi gizleme yöntemlerinden ayıran en önemli özelliklerinden biridir.

Steganografi yönteminde üçüncü kişilerin gizli bilgiyi elde edebilmesi için önce gizli bilginin yerleştirildiği taşıyıcıyı tespit etmesi gerekmektedir. Taşıyıcıyı tespit ettikten sonra veriyi geri elde etme algoritmasını bilmesi gerekmektedir. Bundan dolayı istenmeyen kişilerin steganografi yöntemiyle yapılan haberleşmeyi tespit etmesi oldukça güçtür.

a) Taşıyıcı resim b) Gizli bilgi eklenmiş resim

Şekil 5. 1: Kız resminin karşılaştırılması.

Gizli bilgi eklenmiş olan resme geri dönüşüm algoritması uygulandığında elde edilen bilgi ise Şekil5.2 (b)' de yer almaktadır.



a) Eklenecek bilgi b) Elde edilen bilgi

Şekil 5. 2: Taşıyıcı resme eklenen ve geri elde edilen bilgi.

5.1.1 Steganografi yöntemindeki görüntüdeki kalite değerlendirmeleri

Her ne kadar steganografi yönteminde orijinal resim ile bilgi eklenmiş resim arasındaki farkı insan görme sistemi fark edemese de orijinal resimde bazı değişiklikler olmaktadır. Meydana gelen değişiklikleri tespit etme adına en çok kullanılan yöntemler PSNR ve MSE yöntemleridir.

Bu bölümde uygulanan steganografi yönteminin farklı resimlerdeki kalite değerlendirilmesi yapılacaktır. Değerlendirmede gizli bilgi ekleme sırasında belirlenen *k* eşik değerinin farklı resimlerdeki *k*=(1, 2, 5, 10, 20) değerleri için elde edilen PSNR ve MSE sonuçları yer alacaktır.

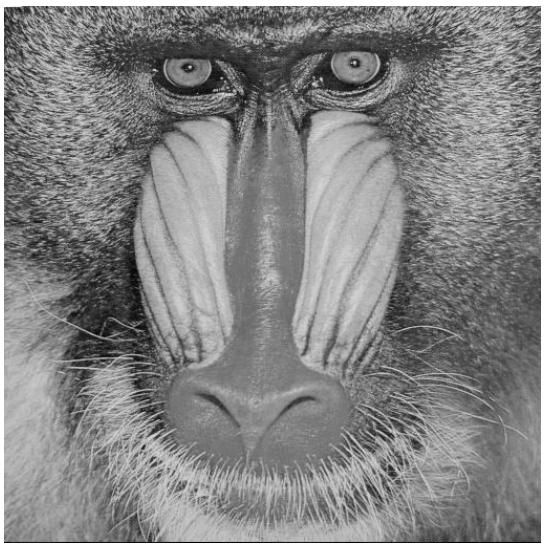
Taşıyıcıya eklenecek bilgi Şekil 5.2 (a)' da yer alan 64x64 boyutundaki 'MCK' yazılı siyah-beyaz resim kullanılacaktır.Uygulamada kullanılacak görüntüler Şekil 5.3'de yer alan her biri 512x512 boyutlu gri tonlu Kız, Baboon, Göl ve Barbara resimleridir.

Gerçekleştirilen uygulama sonucunda elde edilen PSNR ve MSE değerleri Çizelge 5.1'de yer almaktadır. Çizelge5.1'de görüldüğü gibi *k* değerinin artmasıyla birlikte görüntülerin PSNR değeri azalmakta ve MSE değeri artmaktadır. Bu sonuçlar kapsamında belirlenen *k* değerinin görüntü kalitesinin değişiminde önemli bir rol oynadığı tespit edilmiştir.

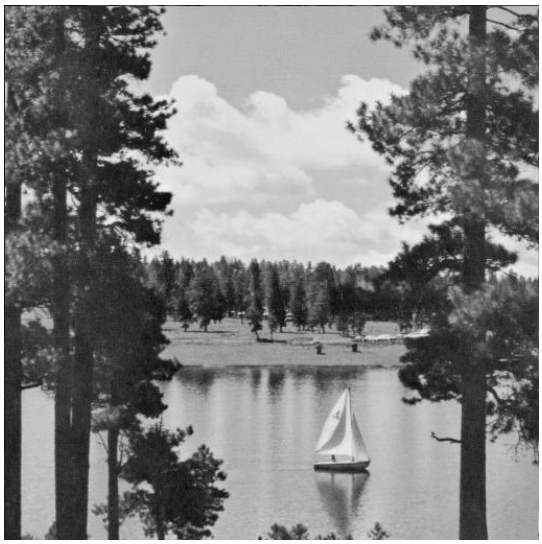
Çizelge 5. 1: Farklı resimlerin farklı *k* değerindeki PSNR ve MSE değerleri

	Kız		Baboon		Göl		Barbara	
	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE
k = 1	44.34	1.55	39.48	2.71	39.57	2.68	39.51	2.70
k = 2	44.29	1.56	39.47	2.72	39.56	2.69	39.50	2.71
k = 5	43.93	1.62	39.40	2.74	39.45	2.72	39.39	2.74
k = 10	42.90	1.83	39.02	2.86	39.03	2.85	39.01	2.86
k = 20	40.38	2.44	37.57	3.38	37.68	3.34	37.65	3.35

a) Kız



b) Baboon



c) Göl

d) Barbara

Şekil 5. 3: Bilginin ekleneceği resimler

5.2 Damgalama Yönteminde Elde Edilen Sonuçlar

Holografik damgalama işleminde kullanılan 512x512'lik gri tonlu taşıyıcı ve damgalanmış resimler sırasıyla Şekil 5.4 (a) ve (b)'de yer almaktadır. Şekil 5.4 (c) ve (d)'de ise sırasıyla 512x512'lik gri tonlu damga bilgisi ve geri elde edilen damga bilgileri yer almaktadır.

a) Lena.

b) Damgalı Lena.

c) Damga bilgisi.

d) Elde edilen damga.

Şekil 5. 4: Damgalama işlemi.

5.2.1 Dalga boyu, uzaklık mesafesi ve açının yeniden yapılandırmadaki yeri

Bölüm 4.2'de sayısal hologramı oluştururken belirlenen dalga boyu, uzaklık mesafesi ve açı bilgilerinin hologramı yeniden yapılandırırken ekstra güvenlik sağladığından bahsedilmişti. Bu bölümde bu değerlerin değişmesiyle damga bilgisinin geri elde edilmesinde ne tür değişiklerin meydana geldiği incelenecektir.

5.2.1.1 Kullanılan dalga boyu ve uzaklık mesafesi değerlerinin ikisinin de yanlış olma durumu

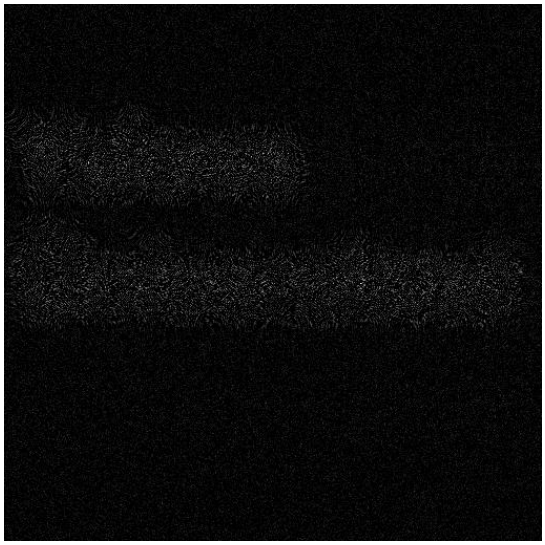
İlk olarak hologramı kaydederken kullanılan uzaklık mesafesi ve açı bilgilerinin her ikisini de yanlış olarak giren kullanıcının yeniden yapılandırma sonucunda elde edeceği damga bilgisini inceleyelim. Uygulamada kullanılan uzaklık mesafesi değeri z=0.3 ve dalga boyu l_d= $0.6x10^{-6}$ olarak belirlenmişti. Damgalanmış görüntüyü alan kullanıcının z=0.2 ve l_d= $0.5x10^{-6}$ iken elde edeceği sonuç Şekil 5.5'de yer almaktadır. Burada görüldüğü gibi damga bilgisi oldukça zor bir şekilde algılanmaktadır.

a) z=0.3 ve l_d= $0.6x10^{-6}$ b) z=0.2 ve l_d= $0.5x10^{-6}$

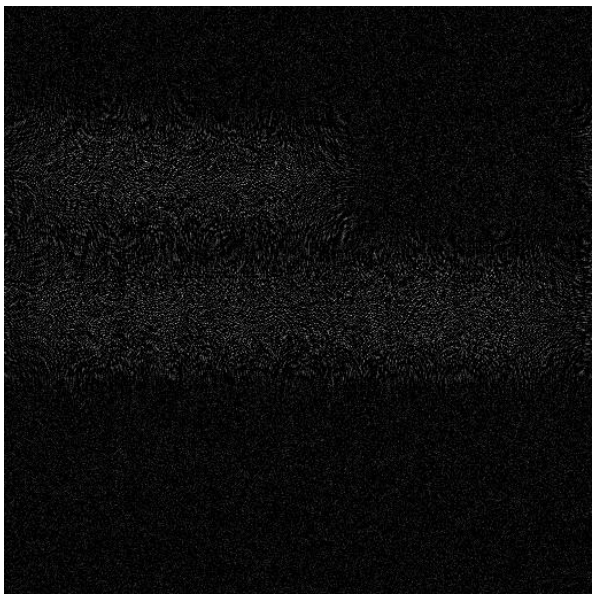
Şekil 5. 5: Dalga boyu ve uzaklık mesafesi değerlerinin yanlış girilme durumu-1.

Yeniden yapılandırma için girilen değerleri z=0.1 ve ve l_d= $0.4x10^{-6}$ olarak ve z=0.1 ve l_d= $0.4x10^{-6}$ olarak belirlendiğinde elde edilen simülasyon sonuçları Şekil 5.6'da yer almaktadır.

a) z=0.3 ve l_d= $0.6x10^{-6}$



b) z=0.1 ve l_d= $0.4x10^{-6}$



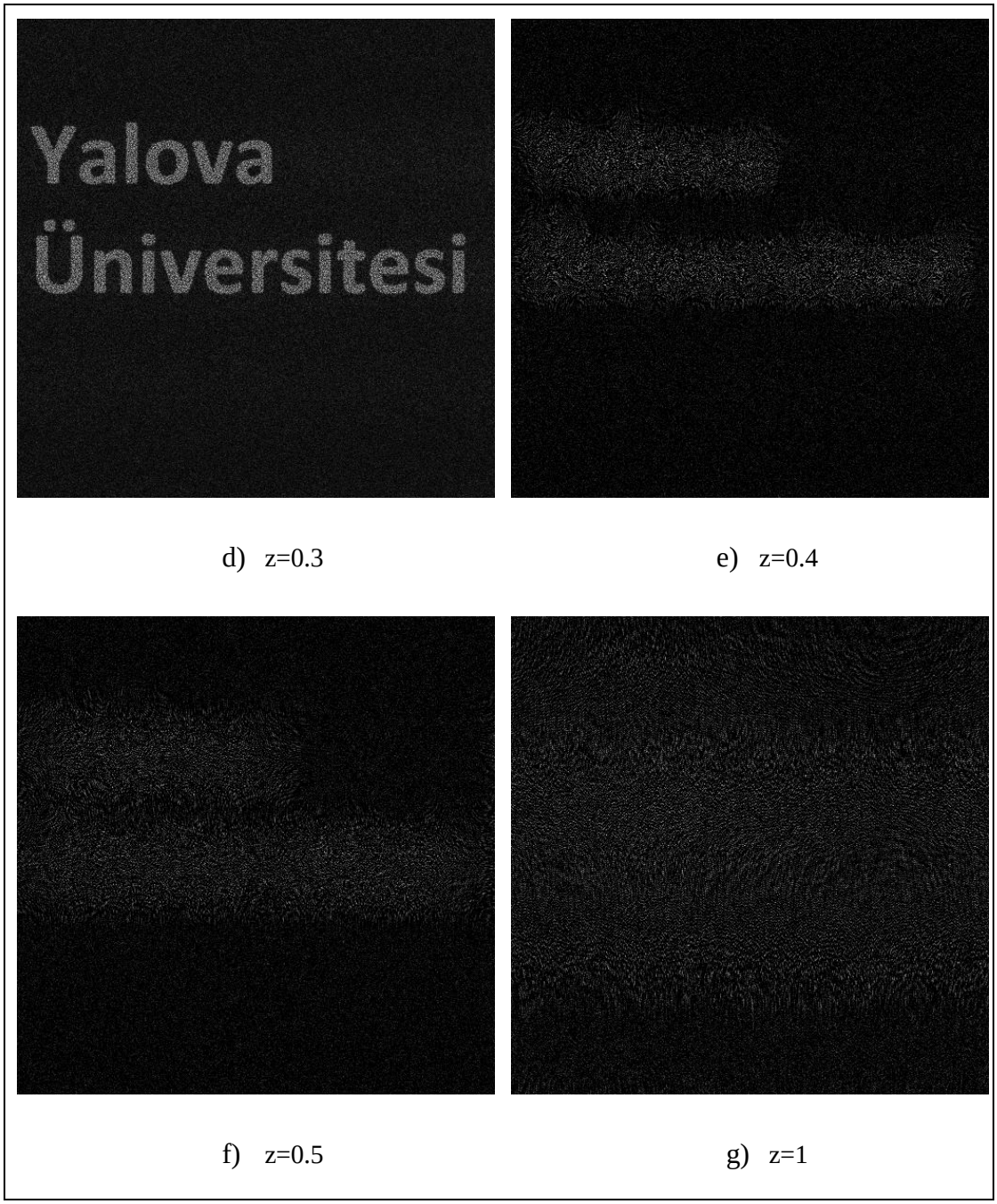
c) z=0.1 ve l_d= $0.2x10^{-6}$

Şekil 5. 6: Dalga boyu ve uzaklık mesafesi değerlerinin yanlış girilme durumu-2.

Elde edilen sonuçlara göre yeniden yapılandırma değerleri ile kaydetme değerleri arasındaki mesafe arttıkça görüntü giderek anlamsızlaşmaktadır.

5.2.1.2 Kullanılan uzaklık mesafesi değerinin yanlış olma durumu

Damgalama işleminde hologram kaydetme esnasında kullandığımız uzaklık mesafesi z=0.3 iken hologramı yeniden yapılandırırken sırasıyla z=0.4, z=0.5 ve z=1 için oluşan yeniden yapılandırma simülasyonsonuçları Şekil 5.7'de yer almaktadır. Burada görüldüğü gibi uzaklık mesafesi yanlış girildiğinde damga bilgisi okunaksız hale gelmektedir.



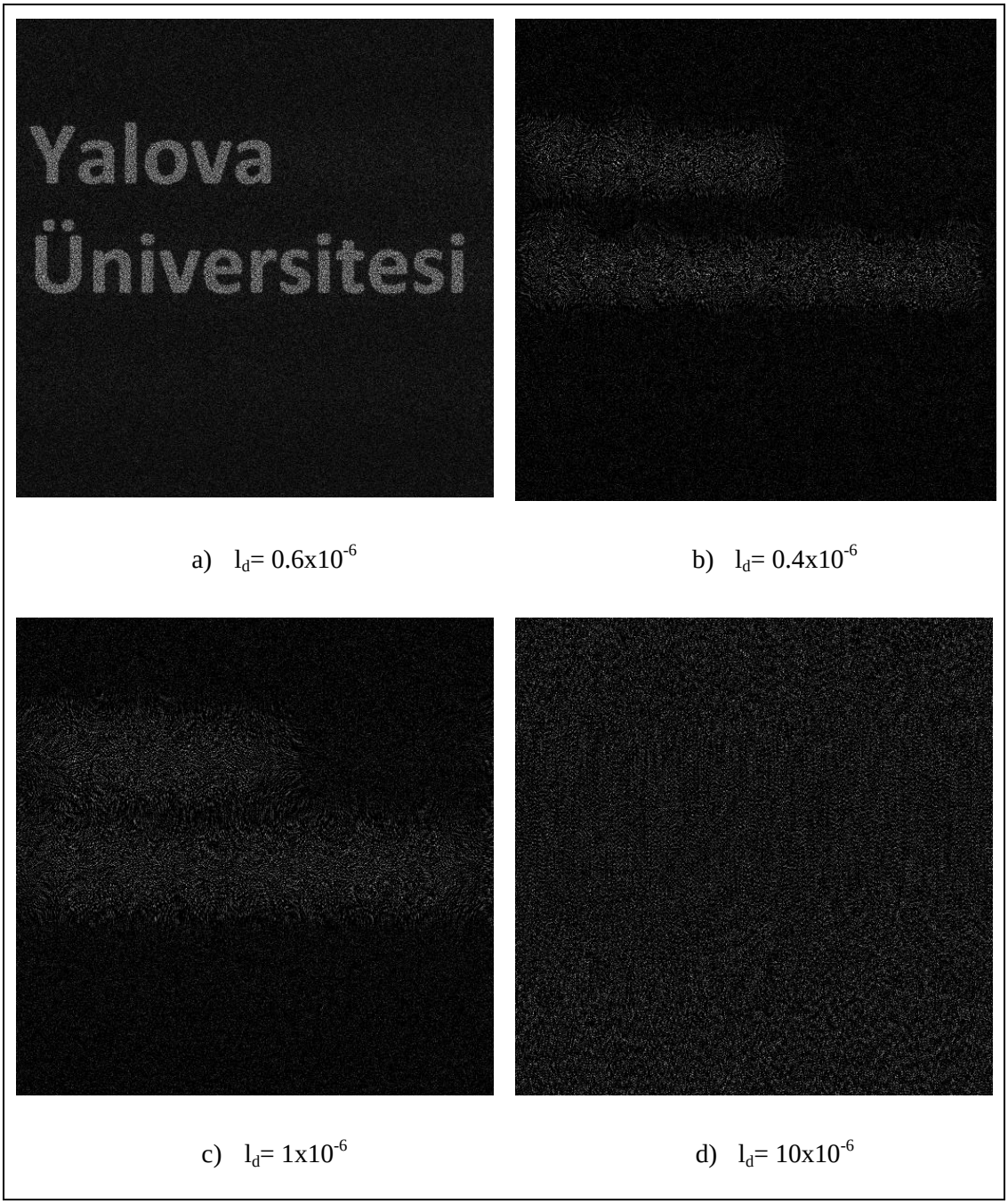
d) z=0.3 e) z=0.4

f) z=0.5 g) z=1

Şekil 5. 7: Farklı uzaklık mesafeleriyle yeniden yapılandırmada elde edilen damga bilgileri.

5.2.1.3 Kullanılan dalga boyu değerinin yanlış olma durumu

Aynı şekilde eğer dalga boyu hologram kaydetme esnasında kullanılan dalga boyunda farklı değerler alırsa damga bilgisi elde edilemeyecektir. Hologramı oluştururken kullandığımız damga boyu $l_d= 0.6x10^{-6}$ iken sırasıyla $l_d= 0.4x10^{-6}$, $l_d= 1x10^{-6}$, $l_d= 10x10^{-6}$ olduğu durumlardaki sonuçları inceleyelim. Şekil 5.8'de elde edilen simülasyon sonuçları yer almaktadır.



a) $l_d= 0.6x10^{-6}$ b) $l_d= 0.4x10^{-6}$

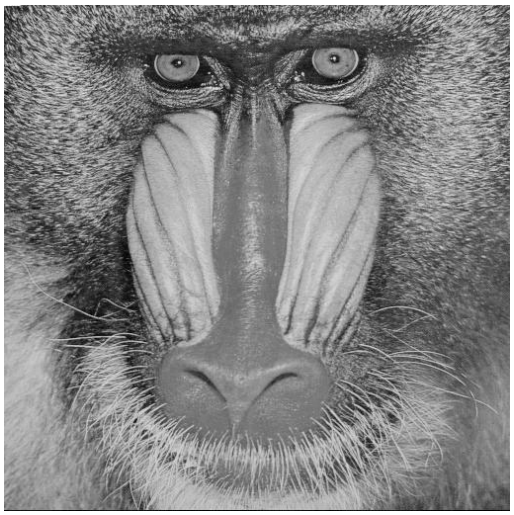
c) $l_d= 1x10^{-6}$ d) $l_d= 10x10^{-6}$

Şekil 5. 8: Farklı dalga boylarındaki yeniden yapılandırmada elde edilen damga bilgileri.

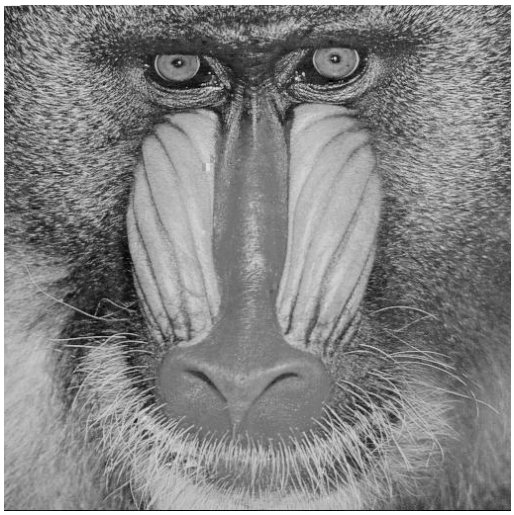
Elde edilen simülasyon sonuçlarına göre dalga boyu ve uzaklık mesafesi değerleri damgayı elde etmede oldukça büyük öneme sahiptir. Hologramı oluştururken kullanılan değerlere çok yakın değerlerde bile yeniden yapılandırma sonuçları anlamsız görüntüler oluşturmaktadır. Netice olarak bu değerler damgalama işleminin güvenliğini daha da artırmaktadır.

5.3 Tek bir imge üzerinde bilgi gizleme ve damgalama

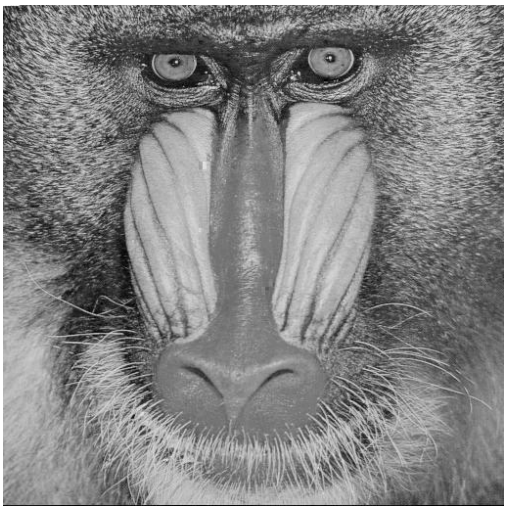
Bu bölümde bir imgeye bilgi gizleme ve damgalama işlemi sonuçları incelenecektir. Uygulamada önce taşıyıcı resme steganografi yöntemiyle bilgi eklenecek daha sonra oluşan gizli bilginin yer aldığı resme damgalama işlemi gerçekleştirilecektir. Şekil 5.9'da bu işlem sonucunda oluşan görüntüler yer almaktadır.



a) Orijinal Baboon



b) Gizli bilgi eklenmiş Baboon



c) Gizli bilgi eklenmiş ve damgalanmış Baboon

Şekil 5. 9: Bir imgede bilgi gizleme ve damgalama.

Şekil 5.9 (a) ve Şekil 5.9 (c) arasındaki görüntü kalite değerlendirme sonuçları: PSNR=38.88 ve MSE=2.91 olarak belirlenmiştir. Şekil 5.9 (c)'de bulunangörüntüden tekrar damga bilgisi ve gizli bilgi elde edilmek istendiğinde oluşan sonuçlar Şekil 5.10 ve Şekil 5.11'de yer almaktadır.

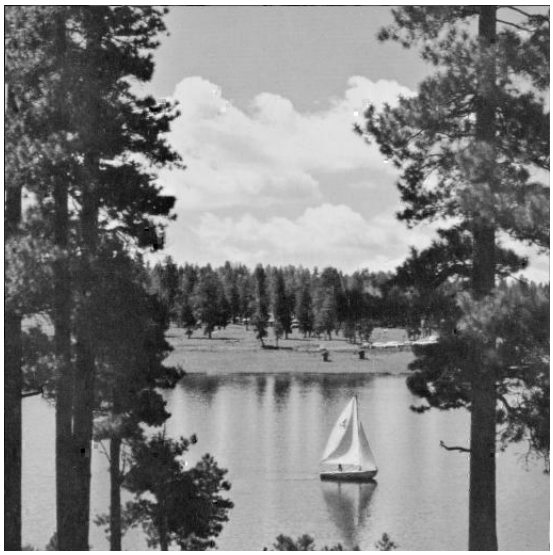
Şekil 5. 10: Elde edilen damga.

Şekil 5. 11: Elde edilen gizli bilgi.

Aynı işlemler Göl resmi için gerçekleştirildiğinde elde edilen sonuçlar Şekil 12'de yer almaktadır. Elde edilen damgalı ve gizli bilgili Göl resmi ile orijinal Göl resminin kalite değerlendirme sonuçları PSNR ve MSE değerleri sırasıyla 39.32 ve 2.76 olarak gerçekleşmiştir.

a) Orijinal Göl

b) Gizli bilgi eklenmiş Göl



c) Gizli bilgi eklenmiş ve damgalanmış Göl.

Şekil 5. 12: Bir imgede bilgi gizleme ve damgalama.

Damga ve gizli bilgiyi tekrar elde edilmek istendiğinde oluşan sonuçlar Şekil 5.13 ve Şekil 5.14' de görülmektedir.

Şekil 5. 13: Elde edilen gizli bilgi.

Şekil 5. 14: Elde edilen damga.

5.4 Kullanılan Yöntemlerin Zaman Karmaşıklığı

Bu bölümde kullanılan sayısal damgalama ve steganografi yöntemleri için gereken süreyle ilgili test sonuçları yer almaktadır. Test ortamı için kullanılan ortamın özellikleri şu şekildedir: işletim sistemi, Windows 7 Ultimate 64 bit; işlemci, Intel Core i3 2.27 GHz; kullanılan simülasyon programı Matlab.

Yukarıda verilen ortamda 512x512'lik gri tonlu bir resmin Fourier dönüşümünü almak için gereken süre 0.0135 saniyedir. Bu bilgiler altında tez uygulamasında gerçekleştirilen damgalama yönteminde 512x512 boyutlu damga bilgisinin hologram olarak elde edilip 512x512 boyutlu taşıyıcı resme eklenmesi için gereken süre 0.9075 saniyedir.

Steganografi işlemi için 512x512'lik gri tonlu resim taşıyıcı; 64x64'lük siyah-beyaz resim de gizli bilgi olarak kullanıldığı takdirde gizli bilgiyi taşıyıcıya eklemek için gereken süre 0.2980 saniyedir.

6. SONUÇ

Tezde günümüzde bilgi güvenliği adına önerilen önemli yöntemlerden olan sayısal damgalama ve steganografi işlemleri tek bir resim üzerinde gerçekleştirilmiştir.Uygulamada ilk olarak steganografi yöntemi ile imgenin içerisine karşı tarafa aktarılmak istenen bilgi eklenmektedir. Daha sonra bu imgeye kim tarafından gönderildiğini gösterecek damga bilgisi eklenmektedir. Böylece alıcı imgenin damga bilgisine bakarak kimden geldiğini anlayabilecektir.

Uygulamanın steganografi kısmı dalgacık dönüşümünü kullanarak frekans düzleminde gerçekleştirilmiştir. Steganografiile bilgi eklerken belirlediğimiz eşik değerinin görüntü kalitesinin değişiminde rol oynadığı tespit edilmiştir. Kullanılan algoritma da gizli bilgiyi geri elde etmek için orijinal görüntüye ihtiyaç duyulmamaktadır. Yani alıcı kişi eğer resmin içinde gizli bilginin varlığından haberdar ise ve geri elde etme algoritmasını biliyorsa bilgi saklı olan resimden saklanmış veriyi elde edebilir.

Damgalama yönteminde ise holografik damgalama yöntemi kullanılmıştır. Elde edilen uygulama sonuçlarına göre: damga bilgisinin elde edilebilmesi için hologram kaydetme aşamasında belirlenen dalga boyu ve uzaklık mesafelerinin oldukça kritik bir önem taşıdığı tespit edilmiştir. Hologram kaydetme esnasında belirlenen dalga boyu ve uzaklık mesafesi değerlerine çok yakın değerlerde bile yeniden yapılandırma sonrasında oluşan görüntünün anlamsız olmasına neden olmaktadır. Buda yetkisi olmayan kişilerin damga bilgisine ulaşmasını oldukça güçleştiriyor. Yani damgayı elde etmek isteyen kişinin bu değerleri muhakkak bilmesi gerekmektedir.

Bu tarz tek bir imgeye damgalama ve steganografi işlemini gerçekleştiren uygulamalar ihtiyaca göre farklı amaçlar içinde kullanılabilir. Mesela steganografi uygulanmış bir imgeye eklenen kırılgan bir damga sayesinde imgenin içeriğinde herhangi bir değişiklik meydana gelip gelmediğinin tespiti yapılabilir. Eğer damga bilgisinde bir değişiklik varsa steganografi ile elde edilen bilgiye şüpheyle bakılmalıdır.

KAYNAKLAR

[1] Anonymous, Image Steganography and Steganalysis, Alındığı tarih:10.01.2013 adres:http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf

[2] N. F. Johnson ve S. Jajodia, 1998: Exploring Steganography: Seeing the Unseen, *Computer*, pp. 26-34,.

[3] E. F. Hembrooke, 1954: United States Patent 3,004,104.

[4] R. G. Schyndel, A. Z. Tirkel ve C. F. Osborne, 1994: A digital watermark.

[5] E. Koch, J. Rindfrey ve J. Zhao, 1996: Copyright protection for multimedia data, *Digital Media and Electronic Publishing*, pp. 203-213.

[6] I. Cox, J. Kilian, F. Leighton ve T.Shamoon,1997: Secure spread spectrum watermarking for multimedia.

[7] M. Kutter, S. Voloshynovskiy ve A. Herrigel, 1997: The watermark copy attack, *Security and Watermarking of Multimedia Content*.

[8] M.Yeung ve F. Mintzer, 1997: An invisible watermarking technique for Image verification, *International Conf on Image Processing*.

[9] S. P. Mohanty, K. Ramakrishnan, Kankanhalli ve M., 1999: A dual watermarking technique for images, *Proceedings of the 7th ACM International Multimedia Conference (ACMMM).*

[10]C.T. Wu ve H. Ja-Ling, 1999: Hidden digital watermarks in images, *IEEE Transactions on Image Processing*, pp. 58-68.

[11]N. Takai ve Y. Mifune, 2002: Digital watermarking by a holographic technique.

[12]F. Y. Shih ve S. Y. Wu, 2003: Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*, p. 969 – 975.

[13]C. Shieh, H. Huang, F. Wang ve J. Pan, 2004: Genetic watermarking based on transform-domain techniques, *Pattern Recognition*, pp. 555-565.

[14]L. Cai, M. Z. He, Q. Liu ve X. L. Yang, 2004: Digital image encryption and watermarking by phase-shifting interferometry.

[15]C. Kurak ve J. McHugh, 1992: A cautionary note on image downgrading, *Proceedings of the IEEE 8th Annual Computer Security Applications Conference*.

[16]W. Bender, D. Gruhl, N. Morimoto ve A. Lu, 1996: Techniques for data hiding, *IBM Systems Journal*, pp. 313-336.

[17]L. M. Marvel, C. G. Boncelet ve C. T. Retter, 1999: Spread Spectrum Image Steganography, *IEEE Transactions on Image Processing*, pp. 1075-1083.

[18]Y. Lee ve L. Chen, 2000: High capacity image steganographic model, *IEE Proceedings - Vision, Image and Signal Processing*, p. 288 – 294.

[19]H. Tseng ve C. Chang, 2004: Steganography using JPEG-compressed images, *The Fourth International Conference on Computer and Information Technology* , China.

[20]H. S. M. Reddy ve K. B. Raja, 2009: High capacity and security steganography using discrete wavelet transform, *International Journal of Computer Science and Security*, pp. 462-472.

[21]D. Hunter, 1967: Handmade Paper and Its Watermark: A Bibliography.

[22]I. J. Cox, M. L. Miller ve J. A. Bloom, 2002: Digital Watermarking, San Francisco: Morgan Kaufmann Publishers.

[23]F. Hartung ve M. Kutter, 1999: Multimedia watermarking techniques, *Proceedings of the IEEE*, pp. 1079-1107.

[24]S. M. Thampi,2004: Information hiding techniques: a tutorial review, *ISTE-STTP on Network Security & Cryptography*.

[25]S. P. Mohanty, 1999: Digital watermarking : a tutorial review, Bangalore.

[26]S. Hajjara, M. Abdallah ve A. Hudaib, 2009: Digital image watermarking using localized, *European Journal of Scientific Research*, pp. 594-608.

[27]V. M. Potdar, S. Han ve E. Chang, 2005: A survey of digital image watermarking techniques, *3rd IEEE International Conference on Industrial Informatics (INDIN).*

[28]S. Katzenbeisser ve F. A. P. Petitcolas, 2000: Information hiding techniques for steganography and digital watermarking, Boston: Artech House.

[29]R. J. Anderson ve F. A. Petitcolas, 1998: On the limits of steganography, *IEEE Journal of Selected Areas in Communications*, pp. 474-481.

[30]D. Kahn, 1967: The Codebreakers, New York: The Macmillan Company.

[31]Jonathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett, 2004: Steganography and digital watermarking, *School of Computer Science, The University of Birmingham*, 2004.

[32]T. Morkel, J. Eloff ve M. Olivier, 2005: An overview of image steganography, *Proceedings of the fifth annual information security South Africa conference*, Sandton.

[33]N. Hamid, A. Yahya, R. B. Ahmad ve O. M. Al-Qershi, 2012: Image steganography techniques: an overview, *International Journal of Computer Science and Security*, pp. 168-187.

[34]H. Wang ve S. Wang, 2004: Cyber warfare: steganography vs. steganalysis, *Communications of the ACM*, pp. 76-82.

[35]K. Sayood, 2006: Introduction to data compression, Morgan Kaufmann.

[36]V. S. Jabade ve S. R. Gengaje, 2011: Literature review of wavelet based digital image watermarking techniques, *International Journal of Computer Applications*, pp. 28-35.

[37]E. O. Brigham, 1974: The Fast Fourier Transform, New Jersey: Prentice-Hall.

[38]A. V. Oppenheim ve A. S. Willsky, 1997: *Signals and Systems*, Prentice-Hall.

[39]S. Qian ve D. Chen, 1999: Understanding the nature of signals whose power spectra change with time, *IEEE Signal Processing Magazine*, pp. 53-67.

[40]S. Mallat, 2008: A Wavelet Tour of Signal Processing.

[41]O. Rioul ve M. Vetterli, 1991: Wavelets and signal processing, *IEEE SP Magazine*, pp. 14-38.

[42]A. W. Galli, G. T. Heydt ve P. F. Ribeiro, 1996: Exploring the power of wavelet analysis, *IEEE Computer Applications in Power*, pp. 37-41.

[43]R. Polikar, The wavelet tutorial, Alındığı tarih: 13.02.2013, Adres: http://users.rowan.edu/~polikar/WAVELETS/WTpart3.html.

[44]G. Erlebacher ve D. Yuen, 2004: A wavelet toolkit for visualization and analysis of large data sets in earthquake research, *Pure Appl Geophys,* pp. 2215-2229.

[45]A. Grossmann ve J. Morlet, 1984: Decomposition of hardy functions into square integrable wavelets of constant shape, *SIAM J Math Anal,* pp. 3307-3315.

[46]J. Lin ve L. Qu, 2000: Feature extraction based on Morlet wavelet and its application for mechanical fault diagnosis, *J Sound Vib,* pp. 135-148.

[47]R. S. Stankovic ve B. J. Falkowski, 2003: The Haar wavelet transform: its status and achievements, *Computers and Electrical Engineering,* pp. 25-44.

[48]R. X. Gao ve R. Yan, 2011: Wavelets Theory and Applications for Manufacturing, New York: Springer.

[49]O. Rioul ve P. Duhamel,1992: Fast algorithms for discrete and continuous wavelet transforms, *IEEE,* pp. 569-586, 1992.

[50]M. Vetterli ve C. Herley, 1990: Wavelets and filter banks: relationships and new results,*IEEE,* pp. 1723-1726.

[51]E. N. Leith ve J. Upatnieks, 1962: Reconstructed wavefronts and communication theory, *JOSA,* pp. 1123-1128.

[52] M. K. Kim, 2010: Principles and techniques of digital holographic microscopy, SPIE Reviews.

[53] J. Shamir, 1999: Optical Systems and Processes, SPIE.

[54] U. Schnars ve W. P. O. Jüptner, 2002: Digital recording and numerical reconstruction of holograms, *Meas. Sci. Technol.*, pp. R85-R101.

[55] M. K. Kim, L. Yu ve C. J. Mann, 2006: Interference techniques in digital holography, *Journal of Optics A: Pure and Optics,* no. 8, pp. S518-S523**.**

[56] U. Schnars ve W. Jueptner, 2005: Digital Holography, Springer.

ÖZGEÇMİŞ

Ad Soyad: Sinan AY

Doğum Tarihi: 10.04.1986

Doğum Yeri: İstanbul

Lisans: Kocaeli Üniversitesi Bilgisayar Mühendisliği