T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DWT ve DCT Steganografide Performans Analizi

YÜKSEK LİSANS TEZİ

Faruk TAKAOĞLU

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Programı

AĞUSTOS - 2016

T.C.

İSTANBUL AYDIN ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

DWT ve DCT Steganografide Performans Analizi

YÜKSEK LİSANS TEZİ

Faruk TAKAOĞLU

(Y1413.010017)

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Zafer ASLAN

Ağustos, 2016

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

Yüksek Lisans Tez Onay Belgesi

Enstitümüz Bilgisayar Mühendisliği Ana Bilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı **Y1413.010017** numaralı öğrencisi **Faruk TAKAOĞLU**'nun **"DWT VE DCT STEGANOGRAFİDE PERFORMANS ANALİZİ"** adlı tez çalışması Enstitümüz Yönetim Kurulunun 19.07.2016 tarih ve 2016/19 sayılı kararıyla oluşturulan jüri tarafından oybirliği ile Tezli Yüksek Lisans tezi olarak kabul edilmiştir.

Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi :11.08.2016	
1)Tez Danışmanı: Prof. Dr. Zafer ASLAN	.....
2) Jüri Üyesi : Yrd. Doç. Dr. Metin ZONTUL	.....
3) Jüri Üyesi : Yrd. Doç. Dr. Ferdi SÖNMEZ	.....

Not: Öğrencinin Tez savunmasında **Başarılı** olması halinde bu form **imzalanacaktır**. Aksi halde geçersizdir.

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "DWT ve DCT Steganografide Performans Analizi" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (..../08/2016)

Faruk TAKAOĞLU

Sevgili Babama,

ÖNSÖZ

Steganografi birçok alanda etkin olarak kullanılan anlamca Steganos (gizli) ve Graphein (yazma) anlamına gelen iki latince kelimenin birleşmesinden oluşmuştur. Günümüzde elektronik aitlik/sahiplik damgasından parmak ve göz tanımlama sistemlerine, replikasyon ve sahtecilikten en önemlisi olan gizli ve güvenilir haberleşmeye kadar bir çok alanda kullanılan önemli bir bilim dalıdır. Günümüz internet çağının kontrol edilemez yaygınlığı, özellikle haberleşme sektöründe kötü niyetli şahıslar tarafından suistimal edilebilmektedir. Bu şahıslar art niyetli amaçlar için Steganografi kullanmaktadırlar. Steganografi diğer tüm güvenlik unsuru olan bilim ve yazılımlar gibi test edilip araştırılıp bulunabilmekte ve steganografik sistemler çözülebilmektedir. Yüksek lisans tezimde amacım bir steganografi sistemi oluşturup bu sistemi MATLAB simulasyon ortamında, Matlab fonksiyonlarından; Discreate Wavelet Transform ve Discreate Cosine Transform yöntemlerini kullanarak, bu yöntemlerin performanslarını birbirileri ile test etmektir. Tez çalışmamda bana engin bilgileri ile yol gösteren saygıdeğer Hocam Prof. Dr. Zafer ASLAN'a ve kıymetli abim Mustafa TAKAOĞLU'na teşekkürlerimi borç bilirim.

Ağustos, 2016 Faruk TAKAOĞLU
Bilgisayar Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

AD : Avarage Difference (Ortalama Fark)
ASCII : American Standart Code for Information Interchange (Bilgi Değişimi İçin Amerikan Standart Kodu)
BMP : Bitmap Image File (Bitmap Resim Dosyası)
DCT : Discrete Cosine Transform (Ayrık Kosünüs Değişimi)
DES : Data Encryption Standard (Veri Şifreleme Standardı)
DFT : Discrete Fourier Transform (Ayrık Fourier Değişimi)
DRFRFT : Discrete Fractional Fourier Transform (Ayrık Kesirli Fourier Dönüşümü)
DWT : Discrete Wavelet Transform (Ayrık Dalgacık Dönüşümü)
FFT : Fast Fourier Transform (Hızlı Fourier Dönüşümü)
GIF : Graphics Interchange Format (Grafik Değişim Formatı)
GMM : Gaussian Mixture Model (Gauss Karışım Modeli)
HVS : Human Visual System (İnsan Görsel Sistemi)
IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)
JPEG : Joint Photographic Experts Group (Birleşmiş Fotoğraf Uzmanları Grubu)
KB : Kilobyte (Kilobayt)
LL : Low Band (Düşük Bant)
LSB : Least Significant Bit (En Az Anlamlı Bit)
MATLAB : Matrix Labratory (Matris Laboratuarı)
MD : Maximum Difference (Maksimum Fark)
MDC : Message Digest Cipher (Özet Mesaj Şifreleme)
MPSO-TVAC: Modified PSO With Time Varying Inertial Weight (Zamanla Değişen Atalet Ağırlığına Göre Değiştirilmiş PSO)
MSB : Most Significant Bit (En Önemli Bit)
MSE : Mean Squared Error (Ortalama Kare Hatası)
NAE : Normalized Absolute Error (Normalize Mutlak Hata)
NCC : Normalized Cross-Correlation (Normalize Çapraz Korelasyon)
OPA : Optimum Pixel Adjustment (Optimal Piksel Ayarı)
PNG : Portable Network Graphics (Taşınabilir Ağ Grafikleri)
PoV : Pair of Values (Değerlerin Çifti)
PSNR : Peak Signal to Noise Ratio (Tepe Sinyali Gürültü Oranı)
PSO : Particle Swarm Optimization (Parçacık Sürü Optimasyonu)
PVD : Pixel Value Differencing (Piksel Değeri Farkı)
RGB : Gaussian Noise, Rotation Salt And Oeooer Noise, Gamma Correction, Blurring and Median (Gauss Gürültü Yöntemi, Tuz ve Karabiber

Gürültü Rotasyonu, Gama Düzeltme, Bulanıklaştırma ve Medyan Filtreleme Yöntemleri)

SC : Structural Content (Yapısal İçerik)
SNR : Signal to Noise Ratio (Sinyal Gürültü Oranı)
SSIM : Structural Similarity Index (Yapısal Benzerlik İndeksi)
SVM : Support Vector Machine (Destek Vektör Makinesi)
SVD : Singular Value Decomposition (Tekil Değer Ayrışımı)
SWT : Stationary Wavelet Transform (Sabit Dalgacık Dönüşümü)
TDES : Triple DES (Üçlü Des Algoritması)
UNIWARD : Universal Wavelet Relative Distortion (Evrensel Dalgacık Bağıntılı Bozulma)
WAV : Waveform Audio File Format (Waveform Ses Dosyası Biçimi)

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

DWT VE DCT STEGANOGRAFİDE PERFORMANS ANALİZİ

ÖZET

Günümüzde veri güvenliği teknolojik gelişimler ve internetin geniş kullanımıyla birlikte daha önemli bir hal almıştır. Şahıslar gerek gizlilik ilkelerinin sorumlu kurum ve kuruluşlarca ulusal güvenlik amaçlı ihlal edilmesi, gerekse art niyetli ve yasadışı işlemlerinin açığa çıkmasından korktukları için birbirileri ile gizli haberleşmeyi tercih etmektedirler. Gizli haberleşme, mesajın içeriğinin anlaşılmasını engellemeye çalışan "Kriptoloji" ve mesajın varlığının bilinmesini ve görünmesini engellemeye çalışan "Steganografi" kullanılarak yapılmaktadır. Sadece mesajın içeriğini okunmaz hale getiren kriptoloji bilimi, meraklı çevrelerce dikkati cezbetmektedir. İçeriğinden bağımsız olarak herhangi bir mesajın okunuşunun ve anlaşılmasının zorlaştırılması, dikkat çekmesinin artmasına sebep vermekte ve sonuç olarak meraklı çevrelerce şifre sisteminin çözülümü hızlanmaktadır. Steganografi bilimi tüm bu dezavantajlardan bağımsız olarak, mesajın varlığının gizlenmesi ile uğraşmaktadır. Göremediğiniz veya varlığından dahi haberdar olmadığınız bir nesne veyahutta bilginin içeriğine ulaşma isteğiniz, çabanızda olamaz. Günümüz tarihinden önceki dönemlerde, atalarımız kurmuş oldukları devletlerde, haberleşmeyi yukarıda bahsettiğim avantajından dolayı steganografi ile gerçekleştirmişlerdir. Bu konu ile ilgili çokça yöntemler ve sistemler geliştirmiş ve ciddi ilerlemeler kaydetmişlerdir. Ancak çağımız teknolojisine uyarlanan steganografide ülke bireylerinin çoğu bu bilimden uzak kalmışlardır. Yukarıda bahsedilen tüm bu avantaj ve tarihsel geçmişi bir motivasyon kabul ederek, bu tez çalışmasındaki ana amaç, steganografi sistemlerini iyi bir seviyede öğrenip, test edebilmektir. Tezin spesifik amaçları ise; veri saklama yöntemleri konusunda deneyim kazanmak, gerek görsel, gerek yazılı metin verilerinin saklanması işlemi konusunda en uygun yöntemleri belirleyebilmektir. Bu hedeflere yönelik olarak tez çalışmasında da frekans tabanlı steganografi yöntemlerinden olan DWT, Discrete Wavelet Transform (Ayrık Dalgacık Dönüşümü), ve DCT, Discrete Cosinus Transform (Ayrık Kosinüs Dönüşümü), yöntemleri kullanılmıştır. Bu yöntemlerin birbirilerine karşı olan işlemsel üstünlüklerinin kıyaslanabilmesi için, DCT yöntemi kullanılarak bir resim verisi arkasına LSB yöntemiyle metinsel veri, DWT yöntemi kullanılarak matlab platformunda resim verisi arkasına boyutsal olarak daha ufak başka bir resim verisi eklenmiştir. Sonuç olarak bu iki yöntem, PSNR, Peak Signal to Noise Ratio (Yüksek Sinyalin Gürültüye Oranı), verisine göre kıyaslanmıştır. Oluşturulan bu test senaryosunda, hangi yöntemin bir diğerine daha üstün olduğu sayısal verilerle saptanmaya çalışılmıştır.

Anahtar Kelimeler : Veri saklama, Veri güvenliği, Wavelet, Steganografi, DWT, DCT, Kriptoloji.

PERFORMANCE ANALYSIS OF DWT AND DCT ON STEGANOGRAPHY

ABSTRACT

Nowadays, data security has become more important than ever because of technological developments and widely usage of internet. People prefer to use secret communication due to breaking their social life privacy by responsible institutions or they concern about their illegal activities. Secret communication has done by the Cryptology, which converts the content of message to unreadable situation, or has done by Steganography, which hides the existence of the message itself. Cryptology takes attention of curious parties of community by making the messages itself unreadable.On the other hand, making the messages itself unreadable situation, accelerates cracking of cyrpto systems security by technology community. But on the other side, steganography only hides of the existence of message itself. This can not be cause of curiosity of cracking any security systems to reach it's content. Because, you can not have any ambitious about solving a complex security algorithms or trying to crack any security system which can not be seen. The time before our technological era, our encestors of Turkish Republic citizents and at the our encestors old and past goverments, they used old fashioned – according to our age- steganographical communication ways, effectively. According to history tellers they developed their own ways and conduct this science and art branch. But nowadays, we are unfamiliar with steganography itself and it's terminologies. We have to reach the same level which our encestors accomplished in steganography. With the help of the steganography main advantage and taking motivation from this historical background of our community, my master thesis main purpose, to efficiently learn steganography and gain experience about it. To accomplish this purpose, I am going to go to learn and use frequency based steganography algorithms which are DCT, Discrete Cosinus Transform and DWT, Discrete Wavelet Transform. And also to learn them in effective way, I created a scenario about secret data communication. I've hidden a text message in a carrier object with DCT and I've hidden a small picture in a carrier object with DWT. According to this scenario, I've matched these well known frequency based steganography techniques based on their PSNR, Peak Signal to Noise Ratio values. The result going to go to show us which way is the most successfull way of our scenario. With this work, I have experienced about DWT, DCT and LSB, Least Significant Bit which is widely used and known technique to embed secret messages in pictures and used in our work with DCT algorithm. I hope this master thesis paper work will be helpfull for all readers to carry this science to the next level.

Keywords : Information Security, Informatin Hiding, Matlab Wavelet, Steganography, DCT, DWT, Cryptology.

1. GİRİŞ

Gizli, kelime anlamı olarak; başkalarından saklanan, duyurulmayan, mahrem anlamını taşımaktadır. Bu anlamın eyleme dönüştürülmüş haline ise gizlilik denilmektedir (URL1). İnsanlar tarih boyunca değerli olduklarına inandıkları her türlü maddi ve manevi nesneyi saklamış ve gizlemişlerdir. Gizlilik yöntemlerinin zamanla açığa çıkması ve öğrenilmesi ile daha karmaşık ve ilk bakışta anlaşılması zor sistemler geliştirmişlerdir. Zamanla bu sistemler gelişmişlikleri ile hayranlık uyandırmaya başlamış ve böylelikle gizlilik ile gizleme işlemleri bir sanat ve bilim dalı halini almıştır (Cachin, 1998). Latincede gizli manasındaki "steganos" ve yazmak manasındaki "graphein" kelimelerinden türetilmiş ve gizli yazma anlamına gelen bu terim dilimize Steganografi olarak geçmiştir. Bu bilimin amacı, ikinci ya da üçüncü şahıslardan önemli olan nesnenin varlığının gizlenmesidir (Challita ve Farhat, 2011). Steganografi diğer bir veri güvenliği bilimi olan Kriptoloji ile birçok zaman birlikte kullanılmakta, zaman zaman ise birbirileri ile karıştırılmaktadır. Bu iki aynı amaca hizmet veren bilimlerin farkı ise Kriptolojinin mesajın içeriğine ulaşmayı engellemesi ve bunun içinde içeriği okunamayacak bir hale getirmesidir. Ancak Steganografinin amacı mesajın varlığını gizlemektir. Kriptolojik metinlerde mesajlar farklı algoritmalar ile ikinci ve üçüncü şahısların fikir yürüterek ya da benzerlik kurarak anlayamayacakları biçimlere dönüştürülür. Böylelikle mesajın güvenliği sağlanmış olduğu düşünülsede, görsel bir karmaşa ile sağlanmış gizlilik her zaman şahıslar tarafından bir ilgi ve merak uyandırır. Sonuç olarak, Kriptoloji zamanla ve belirli bir uğraşla çözülebilmektedir. Steganografi bilimi ise değerli nesnenin varlığını gizlediği için, mesaj insan gözüyle görünmez bir hal alır ve şahıslarda merak uyandırmaz. Görünemeyen bir mesajda çözülemez olduğundan mantıken daha sağlam bir yapı içermektedir.

Bu doğrultuda Steganografi tarihte çokça kullanılmış ve teknoloji çağının başlaması ve gelişmesiyle beraber çağımıza kıyasla ilkel sayılabilecek yöntemlerinden sıyrılıp daha karmaşık ve düşünsel zorluklar içeren yöntemlerle uygulanmaya başlanmıştır.

Steganografi, antik Yunanistan'da kölelerin kafasına gönderilen mesajları kazıyarak mesajın alıcısına kölelerin saçları uzadıktan sonra gönderilerek, Pers istilası yıllarında sıkça güvenli haberleşme yöntemi olarak kullanılmıştır. Ayrıca Yunanlar XERXES istilası esnasında, tahta tabletlere gizli mesajı yazıldıktan sonra, tablet üzerine eritilmiş mumla kaplar ve yeni bir tablet görüntüsü verilirdi. Alıcı mumu eriterek gizli mesaja ulaşır ve böylelikle güvenli haberleşmeyi sağlamış olurlardı (Challita ve Farhat, 2011). Amerika Birleşik Devletlerinin kuruluşundaki Amerikan Kolonisi özgürlükçü savaşçılarının kullandıkları görünmez mürekkeple yazılan mesajlarla steganografiyi ve aynı yöntemle II. Dünya Savaşında haberleşmeyi sağlayan Alman ordusu steganografiyi aktif olarak kullanmışlardır (Al-Shatrawi, 2012). Steganografi İngiltere başbakanı Margaret Thatcher tarafından 1980 yılında bakanlar kurulu dökümanlarının basına sızdırılmasından sonra kullanılmaya başlanmıştır. Duyurularda kelime aralarına bakanların kimliklerini şifreleyen kelime işlemcileri programlatmış ve basına duyuruları sızdıranları bulmaya çalışmıştır (Çivicioğlu ve Alçı, 2003). 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'daki adreslere gönderiyordu. Yakın zamanda ise verilmek istenilen mesaj çoğu zaman global yayın organları kullanılarak hedeflere ulaştırılıyordu. Örneğin Ron Howard'ın "Akıl Oyunları" adlı filminde, John Nash karakterinin gazete ve dergilerde gizli mesajlar araması (URL2). Bu yöntem daha çok anlamları metinlerin içeriğinden çıkarılabilecek, örneğin bir paragraftaki her kelimenin ikinci harfinin alınması ile meydana gelicek anlamlı mesaj gibi, kolay ancak bulması zor ve muhtemelen farkına varıldığı anda mesajın hedefe çoktan ulaştığı veya mesajın ilk anki değerini yitirdiği durumlarda tercih edilir. Çok okunan bir gazetenin bir haber içeriğinden dahi bir operasyon ihbarı verilebilir veya saldırı emri hedeftekilere ulaştırılabilir. Steganografi'nin sağladığı gizlilikle iletişim kurma yöntemleri günümüzde de çokça kullanılmaktadır. Birçok kurum önemli pozisyonlardaki çalışanları ile ticari bilgi içeren mesajlarını gönderirken, legal veya illegal örgütler kendi içlerinde haberleşme sağlarken, istihbarat örgütleri ve siyasi kimlik sahipleri devletler arası veya siyasi önemi bulunan bilgileri iletirken steganografi ile haberleşme yöntemlerini sıkça kullanmaktadırlar (Anderson ve Petitcolas, 1998). Steganografi sadece haberleşme

alanında kullanılmamaktadır. Günümüzde dijital medyanın sağladığı imkanların gelişmesi ile birçok ürün ve ürün tasarımları internet mecraları üzerinden müşteri beğenisine sunulmaktadır veya tasarlanmaktadır. Bu durum beraberinde ürünlerin veya kaynakların üreticilerin farkına varmadan değiştirilmesi, kopyalanması veya silinmesi gibi sorunlara yol açabilir.

Böyle durumların önüne geçmek ve üretilen objelerin ilk sahiplerinin belirlenmesi için "watermarking" ve "fingerprinting" denilen Steganografi sistemleri geliştirilmiştir. Bu sistemlerde üreticinin imzası dijital ürünün daha önceden belirlenmiş bölümüne bir logo, imza veya bit sırası şeklinde yerleştirilir ve yasa dışı kullanımının tespiti durumunda ürün sahipliğinin delili olarak sunulur (Bloom, Cox, Fridrich, Kalker ve Miller, 1991).

Günümüz steganografisi eski yöntemlere kıyasla daha fazla teknolojik terimler içerir ve daha karmaşık bir haldedir. Steganografi ile iletimde kullanılan terimler şunlardır; gizlenecek mesaj (Secret Message), taşıyıcı obje veya taşıyıcı mesaj (Cover Message); gizli mesajı iletmek için kullanılacak video, resim, ses kaydı gibi, kullanılacağımız çoklu medya platformu üyeleri, Steganografi algoritmasının çözülümünü sağlayan anahtar (key) gibi. Bu anahtar steganografi algoritmasının başkaları tarafından çözülmesini engelleyecek olan taraflarca belirlenmiş ve yine taraflara özgü özel bir değerdir.

Bu terminolojilerin dışında eğer steganografi, kriptoloji gibi başka disipliner bilimlerle çalışırsa, kullanılan bilimin veya yöntemin terminolojileride sisteme dahil olmaktadır. Kriptoloji için kripto algoritması ve anahtarı örnek verilebilir (Pfitzman, 2004).

1.1. Çalışma Konusu

Yukarıda bahsedilen bilgilerin ışığında bu tez çalışmamızda öncelikli olarak haberleşme alanında Steganografinin nasıl kullanıldığından ayrıntılı olarak bahsedeceğiz. Ana hikayemiz bu alanda çalışma yürüten herkesin çok iyi bildiği Simmons'un hapishane mahkumları problemidir. Bu problemde, adını bizim belirlediğimiz iki mahkum hapisten kaçmak için bir plan yaparlar ve bu planı birbirlerine ulaştırabilecekleri tek kanal hapisane gardiyanıdır. Birbirlerine gönderecekleri mesaj, gardiyan üzerinden ve gardiyanın dikkatini çekmeden gizli bir şekilde nasıl gönderilmelidir sorusunun cevabı bizim oluşturacağımız ve test edeceğimiz Steganografi yöntemidir (Bloom, Cox, Fridrich, Kalker ve Miller, 1991). Gardiyan gerçek hayatta iletişim kanalımızı takip eden, bizi dinleyen kurum, kuruluş veya yetkililer ya da bizden şüphelenen herhangi bir kişidir. Bu kişi bizim oluşturduğumuz gizli iletişim ağını çözebilmek için gözlemlemeler yapar bu işleme Steganografinin analizi ya da "Steganaliz" denir. Steganaliz yöntemleri steganografi sistemlerini çözmek, gizli bilgileri açığa çıkarmak üzerine adeta steganografi ile yarışırlar. Bu yarış veri gizleme bilimi ve sanatının gelişmesine katkıda bulunur. Steganalizcilerin çözdüğü herbir sistemden sonra Steganograficiler sistemlerini modernize eder ve farkına varılması daha güç sistemler oluştururlar. Bazı durumlarda tam bir güvenlik sağlamak için steganografik sistemin içerisindeki mesaj kriptolanır ve güvenlik iki katmanlı olmuş olur. Ancak günümüzdeki geliştirilen süper bilgisayarlar ve güçlü kuantum bilgisayarlar sayesinde bu güvenlik katmanlarınında kolayca aşılabileceği bir zamana gelmiş bulunmaktayız. Bu süper güçlü bilgisayarların şifreleme sistemleri karşısındaki en önemli avantajı şifreleme havuzu adıyla tabir edilen tüm olası şifreleri "brute force" kaba kuvvet yöntemiyle hızlı bir şekilde çözmesidir. Steganografinin farkına varıldığı ve kripto sisteminin çözülebildiği bir senaryoda, bir grup araştırmacı buna önlem olarak Görsel Bal Şifrelemesi (Visual Honey Encryption) adlı bir sistem geliştirmişlerdir. Bu sistem her yanlış şifre denemesinden sonra deneyeni reddetmek yerine, ana metin ile benzerliği bulunmayan ancak mantıksal tutarlılık gösteren metinleri göstererek, bu tarz sistemlerin yanıltılmasını hedeflemektedir (Jo, Kim, Lee, Lee ve Yoon, 2015). Tez çalışmasında tüm bu bilgiler ışığında, bir steganografi senaryosu oluşturacağız. Bu senaryo farklı veri türlerinin güncel veri

saklama yöntemleri ile uygulanmasını içerecek ve bu uygulamaların test edilmesi ile performanslarının kıyaslanmasını içerecektir. Bu amaçla tezimizde, DCT; Discrete Cosinüs Transform (Ayrık Kosinüs Dönüşümü) yöntemi ve DWT; Dsicrete Wavelet Transform (Ayrık Dalgacık Dönüşümü) yöntemlerini taşıyıcı objeler olarak adlandırdığımız masum resimlerin içerisine metin ve görsel veri saklamasında kullanacağız.

Bu yöntemlerin kullanımı esnasında, yapılan çalışmaya özellik ve orjinallik katmak için DCT yöntemi Hamming Kod yaklaşımı, DWT yöntemi ise rastgelelik yaklaşımı ile güçlendirilecektir. Ayrıca bu yöntemlerden bağımsız olarak kullanılan ve ileri bölümlerde ayrıntılı bir biçimde bahsedeceğimiz LSB; Least Significant Bit (En önemsiz bit değeri) yöntemi DCT ile birlikte kullanılacaktır.

1.2. Tezin Amacı

Bu tez çalışmasındaki amacımız; günümüzde kullanılan veri saklama yöntemlerinde yüksek seviyede bilgi sahibi olmak ve sonuçlarını sunduğumuz belgeleri okuyan ikinci şahısların, bu konuda ilgi ve alakalarını arttırmak ve bilgi sahibi yapabilmektedir. Bu amaçları desteklemek ve geliştirmek için öğrenilip test edilen steganografi sistemlerinden detaylıca bahsedilecektir. Steganografinin kullanımı ve tarihsel gelişiminden sonra verilecek veri gizleme ve analiz yaklaşımları, oluşturulan sistemlerin performans testlerinin nasıl yapıldığı ayrıntılı olarak anlatılacaktır.

Son olarak bu amacımızı pekiştirmek için, yukarıda bahsettiğimiz ve ilerideki bölümlerde daha ayrıntılı anlattığımız DCT ve DWT yöntemleri ile bir steganografik sistem oluşturup bunların birbirilerine göre performansları kıyaslanacaktır.

1.3. Literatür Taraması

Bu bölümde, tez yazımına başlanmadan önce yapılan araştırmalar esnasında incelenen ve faydalanılan makaleler hakkında bilgiler verilmiştir. Her makalenin tezimizle alakalı olan yanı ya da faydalanılan noktaları literatür taramasında açıklanmıştır.

StegTrack: Tracking images with hidden content (StegTrack: Gizli içerik görüntüleri izleme)

Makalede dört Hindistanlı araştırmacının kendi oluşturdukları StegTrack adında, bilgisayara kurulumu yapıldıktan sonra sürekli olarak aktif kalan ve bilgisayarın içerisindeki tüm multimedya unsurlarını steganaliz yöntemleri ile inceleyen ve daha sonrasında gelen yeni multimedya unsurlarını inceleyen ve uyarı veren kendi yazılımları hakkında bilgi vermektedir. Bu yazılım, steganografi ile bilgisayarlara sızma yapmaya çalışan virüs programlarını engellemeye çalışmaktadır. Ayrıca içerisinde birden fazla steganografi algoritmaları içermekte (LSB, JPHide, JSteg vb.) ve resimlerin hareket trafiklerini hafızasına kaydederek dinamik olarak steganaliz yapmaktadır. Yazılımın özelliği, daha önce denenmemiş olan birden çok analiz yöntemi ve algoritmanın birden çok medya platformu üzerinde anlık olarak çalıştırılmasıdır. Makaleden; Steganografinin, resimlerin istatistik değerlerinde değişime neden olduğu ve burdan yola çıkılarak bulunabileceği, bununla beraber model tanımlama, Pattern-Recognition, yöntemlerinin steganalizdeki resimler üzerinde nasıl kümeleme algoritmaları ile beraber kullanılacağı hakkında bilgi sahibi olunmuştur (JPEG uzantılı bir resim dosyası için Markov tabanlı veya NJD, Neighbouring Joint Density Probabilities, yaklaşımlarının kullanımının uygun olacağı gibi) (Bedi, Bhasin, Goel ve Gupta, 2015).

Review of steganography techniques (Steganografi yöntemlerini gözden geçirmek)

N. Verma'nın yazmış olduğu bu makalede; LSB, DCT ve Wavelet Steganografi yöntemleri, geniş resim verileri üzerinde uygulanmış ve avantaj-dezavantaj'ları açısından karşılaştırılmıştır. LSB, Least Significant Bit, yönteminin nasıl kullanıldığı gösterilmiş, ayrıca basit oluşundan dolayı kullanımının kolaylığı, avantajı ve aynı zamanda bit'lerin yer değiştirmesi esasına dayandığı içinde uygun bit sıralamasına sahip bir taşıyıcı mesaj, resim veya müzik bulunması dezavantajından bahsedilmiştir. Bu makalede LSB ile ilgili olarak Lossy Compression Algorithm'den ve öneminden bahsedilmiş. LSB ile veri aktarımı yapılırken veri kanalı gürültüsünden dolayı veri kayıbı yaşanabileceği ve bunun için Lossy algoritmasının kullanılması gerektiği öğrenilmiştir.

Ayrıca makaleden DCT, FFT, DWT tanımlamaları ve çalışmaları hakkında bilgi edinilmiştir. Bu methodları, gri resimler üzerinde steganografi uygulayıp, SNR vs Entropy analizi ve histogram analizinde karşılaştırılınca DWT'nin aralarında en iyisi olduğu görülmüştür (Verma, 2011).

Secured image steganography using different transform domain (Farklı dönüşüm alanı kullanımıyla güvenli görüntü steganografisi)

A. Kaushal ve V. Chaudhary'nin yazmış oldukları bu makalede; DFT, Discrete Fourier Transform, DCT, Discrete Cosine Transform, ile DrFrFt, Discrete Freactional Fourier Transform, yöntemleri steganografi performansları açısından kıyaslanmıştır. Çalışmada PSNR, Peak Signal Noise Rratio, ve Mean Square Error metotları daha güvenli ve geliştirilmiş bir iletişim kanalı oluşturmak için kullanılmıştır.

Bu makalede resim steganografisinin çeşitleri olan İmage Spatial Domain, İmage Frequency Domain ve Adaptive Steganography'den sadece ilk ikisinden bahsedilmiş ve Spatial Domain'den ziyade Frequency Domain tercih edilmesinden bahsedilmiştir. Çalışmamız için faydalı bir bilgi sunmuştur. Taşıyıcı bir resim içerisine mesaj olan bir resim yerleştirilmiş ve steganalizinde 3 yöntem arasından DrFrFT'un en iyisi olduğu gözlemlenmiştir. Bu makaleden tezimizde çokça faydalanılmıştır (Chaudhary ve Kaushal, 2013).

Steganographic software: Analysis and implementation (Steganografi yazılımı: Analiz ve uygulama)

Bu makalede, steganografi platformu olan yazılımların performans analizi yapılmakta ve steganografi algoritmaları hakkında bilgi verilmektedir. Normalized Cross Correlation, NCC, yönteminin steganografik sistemlerin güvenilirliğini ve algoritmalarının sağlamlığını ölçmekte kullanıldığını ve önceki çalışmalarda SNR, Signal Noise Ratio, dikkate alınarak yüksek değerli güçlü sinyaller içeren mesajlarda, gizli mesaj gömebilmek için alanın daha da arttığı gözlemlenmiştir. Bir steganografi işleminin kabul edilebilir olması HVS, Human Visual System, tarafından anlaşılamamasıdır. Bunun için MSE, Mean Squared Error, gibi yöntemler kullanılarak taşıyıcı ve steganografik resim arasındaki farklılıklar ölçülür ve belli değerlerin üzerinde olmamasına dikkat edilir. Bu makalede tüm bu sistemler göz önünde bulundurularak, steganografi uygulamaları belirli

veri blokları üzerinde test edilmiş ve sonuç olarak “Invisible Secrets 4” ve “S-Tools” en verimli programlar olarak bulunmuştur. Bu makaleden MSE kullanımı hakkında faydalanılmıştır (Ibrahim, Manaf ve Zeki, 2012).

Color image steganography by using dual wavelet transform (DWT-SWT) (Çift dalgacık dönüşümü kullanarak renkli görüntü steganografisi DWT-SWT)

Bu makalede, taşıyıcı ve mesajın ikiside resim olmakla beraber biri renkli diğeri siyah beyaz resimdir. Her iki resimde DWT ve SWT yöntemleri kullanılarak bileşenlerine ayrılır ve bu bileşenlerin değerleri tekrar DWT ve SWT ile fizyon (birleştirme) yapılarak (mavi renk bileşeni ile siyah beyaz resim) tekrar tek bir resim haline dönüştürülür. Bu yöntemde DWT ve SWT’nin farklı kombinasyonları ile kullanılarak steganografinin görsel kalitesi ve güvenilirliğinin güçlendirilmesi amaçlanmaktadır.

Makaleden DWT steganografide çalışma esasını ve frekanslarındaki farklılıklarını öğrendik. Düşük frekans sinyalin, çoğunluğunu barındırırken, yüksek frekans ise sinyalin değerli ve kaliteli kısımını barındırır. Bahsedilen fusion yöntemi ilgi çekicidir ve kendi çalışmamızda değerlendirilebilir (Dalvi ve Kamathe, 2014).

Performance evaluation of dct and dwt features for blind image steganalysis using neural networks (Sinir ağları kullanarak kör görüntü steganalizinde DCT ve DWT performans değerlendirmesi)

Bu makalede, 72 DWT özelliği ve 274 DCT özellik kümesi MSE, Mean Square Error, zaman ve doğruluk açısından karşılaştırılmıştır. Veriler Steghide ve Outguess ile hazırlanmıştır. Bu makalede steganalizin çeşitleri olan Target ve Blind steganalizden bahsedilmiştir. Burada bir yapay zeka kurulmuş ve resimlerden ilk başta bahsettiğimiz özellikler sayesinde çıkarılan öz nitelikler, yapay zeka sistemine entegre edilerek steganaliz yapılması istenmiştir. Deney sonucunda DCT daha verimli çalıştığı gözlemlenmiştir. Bu makaleden DCT ve DWT‘nin frekansa dayalı çalışması ile igili bilgi edinilmiştir (Chhikara ve Saini, 2015).

Mp3 steganography techniques (Mp3 steganografi teknikleri)

Bu makalede, steganografinin PNG, JPEG ve GIF versiyonlarından farklı olarak, Mp3 ses dosyalarında yapılmasında kullanılan araçlar ve sistematiği üzerine bilgiler verilmiştir. Makalede ek olarak yazarlar kendi oluşturdukları MP3STEG adındaki yazılımlarından ve bu yazılımın mimarisinden bahsetmişlerdir. Yazılım 200 adet MP3 dosyası üzerinden test edilmiş ve sonuç olarak steganografi yönteminin güvenilir olduğu kanıtlanmıştır. Makale çalışması teknik açıdan çok faydalı olup, ses dosyaları üzerinden ilerlediği için tez çalışmamızda kullanılamamıştır (Zaturenskiy, 2013).

Digital audio steganography using DWT with reduced embedding error and better extraction compared to DCT (DCT'ye kıyasla azaltılmış gömme hatalası ve daha iyi ekstraksiyon ile DWT kullanarak dijital ses steganografisi)

Makalede ses dosyaları üzerinde veri saklama ve veri bulma çalışmaları yapılmıştır. Bu doğrultuda DCT ve DWT'nin performansları karşılaştırılmış ve sonuç olarak DWT'nin ses dosyaları üzerinde ve resim dosyalarında Haar wavelet yöntemi kullanılarak ayrıştırılmış. PSNR ve MSE değerleri açısından DWT'nin daha iyi bir performans gösterdiği ispatlanmıştır. PSNR ve MSE parametlerinin elde edilmesi ve resim verileri haricinde başka bir multimedya unsuru üzerinde denenmesinden dolayı çalışmamıza bilgi anlamında fayda göstermiştir (Nehete, Sawarkar ve Sohani, 2011).

A Novel color image steganography using discrete wavelet transform (Ayrık dalgacık dönüşümü kullanarak yeni renkli görüntü steganografisi)

Bu makalede, renkli resimlerde steganografi çalışması yapılmıştır. Diğer çalışmalardan farklı olarak, resimlerdeki sadece renklilik değerleri üzerinde değişim yapılmıştır. Bunun sebebi insan gözünün parlaklık değerlerine karşı hassas ve duyarlı olmasıdır. Frekans analizinde kullanılan DWT ile taşıyıcı resimler ve şifreli resimler frekanslarına ayrılıp bulunması zor ve güvenilir bir sistem olması için düşük frekanslı alt bandlara gömülmüştür. Şifreli metinler için ise anahtar LSB yöntemi kullanılarak taşıyıcı sisteme entegre edilmiştir. Sistem Matlab'da denenmiş ve PSNR, MSE açısından değerlendirilerek diğer yöntemlere nazaran kaliteli sonuçlar alınmıştır. Sistemin

dezavantajı ise, şifreli mesajı LSB ile sisteme yerleştirdiklerinden dolayı frekans analizinden LSB'ye rastlanabilmesidir. LSB çalışma yöntemlerinin anlaşılması anlamında tez çalışmamıza büyük katlı sağlamıştır (Acharya, Kamath, Prabhu ve Shama, 2012).

Steganography using cuckoo optimized wavelet coefficients (Guguklu optimize dalgacık katsayılarını kullanarak steganografi)

Bu makalede yazarlar, guguk kuşunun doğadaki yumurtlama yönteminden esinlenerek oluşturdukları bir yöntemle alakalıdır. Çalışmada DWT kullanılarak resim frekans kanallarına ayırılmış ve bu kanallardan biri seçilerek Cuckoo algoritmasında işlenmiştir. Gizli mesaj Huffman kodlama yöntemiyle kısaltılmış ve DWT frekansına uygun olarak DWT ile frekansa eklenmiştir. Son olarak Steganaliz yapılmış ve PSNR, Peak Signal Noise Ratio, ve SSIM, Structural Similarity Index, ile test edilmiştir. Bu makalede Cuckoo algoritması, DWT ile frekanslardaki ortak etmen veya uygun katsayıları bulmak için kullanılmıştır. Tez çalışmasında DWT ve PSNR işlemlerinin incelenmesi açısından faydalı olmuştur (Bedi ve Singhal, 2015).

A New paradigm hidden in steganography (Steganografide gizli yeni paradigma)

Bu makalede, yazarlar kendi geliştirdikleri steganografik bir yöntemden bahsetmektedirler. Bu yöntemin süreksiz matematiksel modellerle ve algılanan gürültünün etkileyici olmadığı durumlarda geçerli olduğu varsayılarak yapılmıştır. Teori Catastrope teorisinden alıntı yaparak süreksiz atlamalar mantığını steganografiye entegre etmeyi içermektedir. Ek olarak sisteme White Noise, masum-beyaz, gürültü eklemeyi denemişler ancak yapılan testlerde bu aldatmacanın çok bariz olduğu ve anlaşılır olduğu için yanlış bir tercih olduğu kanısına varmışlardır. Konu teorik açıdan tezimize uzak olduğu için faydalanılmamıştır (Chang, Longdon ve Moskowitz, 2000).

On the limits of steganography (Steganografi sınırları hakkında)

Bu makalede, Steganografinin kapsamı ve steganografi ile yapılabilecekler ayrıntılı olarak anlatılmıştır. Dijital damgalama ve sahiplik kanıtlaması, güvenli ve şifreli kanallar aracılığıyla gizli iletişim yöntemlerinin en basitinden, en yeni ve gelişmişine kadar bahsedilmiştir. Steganografi teknikleri, zayıflıkları ve avantajları ile ele alınmıştır.

Shannon teorisinden esinlenerek aktif dinleyicilere karşı açık anahtarlı steganografinin nasıl kullanılacağı anlatılmış ve yöntemleri kendi deneylerinin sonuçlarıyla test etmişlerdir. Bu çalışma steganografi hakkında bilgi haznemizi geliştirmiş ancak tez aşamasında kullanılmamıştır (Anderson ve Petitcolas, 1998).

Combining steganography and cryptography: New directions (Steganografi ve kriptolojinin birleştirilmesi: Yeni yöntemler)

Bu makalede, öncelikli olarak Steganografinin tarihi gelişimi anlatılmış, sonrasında bilinen yöntemler ve onların steganaliz yöntemlerinden bahsedilmiştir. Yazarlar asıl olarak kendi geliştirdikleri sistemi son kısımlarda anlatmışlardır. Bir gizli mesajı, birden fazla parçalara ayırıp, herbir parçayı farklı bir taşıyıcı resim içerisine yükleyerek literatüre yeni bir sistem kazandırmaya çalışmışlardır. İki taraf önceden bilip ve anlaşıp (algoritma ve şifreleme üzerinde ve resimler hakkında), önce mesajı şifreleyip, sonra birden fazla resim üzerinde şifreli mesajın bit sırlamasına yakın veya benzer olanlar seçilerek, mesaj bir çok resime gizleyerek iletilir. Steganografinin kriptoloji ile ilgisi ve uygulanması konusunda bu kaynak tezimizde çokça kullanılmıştır (Challita ve Farhat, 2011).

Digital image steganography using universal distortion (Evrensel bozulma kullanarak dijital görüntü steganografisi)

Bu makale, steganaliz yöntemi olarak kullanılan bozulumun keşfedilmesi veya saptanması ile engellemeye veya minimize etmeye yarayan kendi oluşturdukları UNIWARD, Universal Wavelet Relative Distortion ile alakalıdır. Uniward aslında bir fonksiyondur. Bir JPEG resiminde, gizli mesaj saklayabilmek için, bir pixel değiştirildiği zaman JPEG resiminde 8x8 matrislik bir pixel bloğu etkilenir. DWT veya DCT ‘de öznitelik veya katsayısal olarak 23x23 pixellik bir etkilenme gözlemlenir. UNIWARD bunu engellemek yani bozulum miktarını minimum seviyede tutmak için resim üzerinde hesaplamalar yaparak; gürültü çokluğu, temiz köşe-kenar-sınırlar, kompleks bölgeler bulur ve bu bölgelere veri gömülümünün yapılmasını gösterir. Böylelikle veri bozunumu saptanması mümkün olduğunca azaltılır. Bu makale tezimizin steganografi analizi kısımındaki yazılarımızda faydalı bir kaynak olmuştur (Fridrich ve Holub, 2013).

Support vector machine based intelligent watermark decoding for anticipated attack (Beklenen saldırıya karşı destek vektör makinesi tabanlı akıllı fligran çözme)

Bu makalede, steganografinin bir alt dalı olan watermarking'in sahiplik veya aitlik imzası SVM, Support Vector Machine, adındaki sınıflandırıcı kullanılarak multimedya unsurlarının watermarking'den kaynaklanan bozulmalarını tahmin etmeye çalışmışlardır. Tahmin aşamasında bir yapay zeka sistemi kurulup, SVM ile istatistiksel katsayılar incelenerek bozulmalar bulunmaya çalışılmıştır. Çalışmalar Hernandez Scheme ile karşılıklı olarak test edilmiştir. Kurulan SVM tabanlı yapay zeka sistemi daha iyi sonuçlar göstermiş ve filigranların yerini bit olarak saptamıştır. Alternatif yollar geliştirme ve tez çalışmasında yenilik oluşturma amacı ile incelenmiş ancak tezimizde kullanılamamıştır (Khan, Majid, Mirza ve Tahir, 2008).

Performance comparison of various particle swarm optimizers in DWT–SVD watermarking for RGB image (RGB görüntüsü için DWT-SVD filigranının çeşitli parçacık sürüsü optimizasyonlarının performans karşılaştırması)

Bu makale, steganografinin bir alt dalı olan watermarking ile alakalıdır. Makalede watermarking algoritması bilinmekte, orijinal resim ve gömülecek bilgi ellerinde bulunmakta ve bu algoritmaya karşılık atak yapılmaktadır. Böylelikle "Particle Swarm Optimization" PSO türlerinin performansları karşılaştırmaktadır. Öncelikli olarak çalışmanın temellerini oluşturan SVD, DWT ve Particle Swarm Optimization makaledeki kullanımları doğrultusunda anlatılmıştır. DWT ile Haar Wavelet'de kullanılarak resim sinyallerine ve frekanslarına ayırılmış ve aitlik sembolu LL, Low Band, gömülümü gerçekleşmiştir. Atak yöntemleri olarak Gaussian Noise, Rotation Salt And Oeooer Noise, Gamma Correction, Blurring and Median filtreleme, bir çok PSO türüne uygulanmıştır ve sonuç olarak MPSO-TVAC, Modified PSO with Time varying inertial weight, türü en güvenilir sistem olarak bulunmuştur. Bu çalışma; tezimizin DWT ve Haar dalgacık türünün anlaşılması konusunda çok faydalı olmuştur (Srivastava, 2015).

An efficient data hiding scheme using Hamming error correcting code (Hamming hata düzeltme kodu kullanarak etkili veri saklama)

Bu makalede, LSB yöntemi kullanılarak resimin içerisine mesaj gizlenip, tersine steganografi yapılarak gizli mesajın yeri bulunması üzerine çalışılmıştır. Resimin içerisine mesaj ve şifresi gizlenildikten sonra bunların Hamming Error Correction yöntemi kullanılarak bulunabilmesi için bazı tek/benzersiz bozulmalar yerleştirlerek bir nevi iz bırakılmaktadır. Hamming Code bu bozulmaları takip ederek şifreli mesaja ve anahtara ulaşmaktadır. Çalışmalar sonunda entropy analizide yapılmış ve gömülen mesaj arttıkça, farkına varılabilirlikte artmakta olduğu ispatlanmıştır. Tezimize eklenen Hamming kodlama bu araştırmadan esinlenerek gerçekleştirilmiştir (Giri, Jana ve Mondal, 2015).

Performance analysis of digital image steganographic algorithm (Steganografik algoritma dijital görüntüsünün performans analizi)

Bu makalede, steganografinin çeşitlerinden olan Spatial ve Frequency Domain tarzlarının her birini anlatıp, karşılıklı performanslarının analizi üzerine çalışılmıştır. Test aşamasında MSE ve PSNR değerleri esas alınarak sonuca varılmış ve performans analizi yapabilmek için steganografik resimlerin veri gizlemeden önce ve sonraki halleri karşılaştırılmıştır. Sonuç olarak, testlerden DWT'nin daha etkin bir yöntem olduğu anlaşılmıştır. Bu çalışma ve iç unsurları, tezimizin steganografi ve alt dallarını anlatırken çokça faydalanılan bir kaynak olmuştur (Dhawale, Hegadi ve Jambhekar, 2014).

Zero distortion technique: An approach to image steganography on color images using strenght of chaotic sequence (Sıfır bozulma tekniği: Kaotik dizinin gücünü kullanarak renkli görüntüler üzerinde görüntü steganografisi yaklaşımı)

Bu makalede, steganografinin bir çeşidi olan Spatial Domain tarzından LSB ile ilgili bir çalışma yapılmıştır. Ancak buradaki çalışmanın farkı; LSB yönteminin farklı bir çeşidi olan Zero Distortion tekniğinin kullanılmasıdır. Bu teknik resimlerdeki değişimlerinin meydana getireceği bozulmaları engellemek için mesajın bit'leri ve resimin bit'lerini tarama işleminden geçirir ve benzer olan bit'lere veri gömülümünü gerçekleştirir. Buradan mesajı çıkarabilmek için ise her gömülüm yaptığı pixel'in kordinatını bir

matrisde saklar ve bu matrisin bulunup çözülmemesi için Chaotic Sequence, Kaotik Sıralama, denilen bir rastgeleleştirme yöntemi ile matris şifrelenir. Bu çalışma LSB yönteminin kavranması konusunda tezimizde faydalandığımız bir çalışma olmuştur (Batham, Sharma ve Yadav, 2014).

Locating secret messages in images (Görüntülerdeki gizli mesajların yerininin saptanması)

Bu makalede, Data Mining'in bir konusu olan ve sınıflandırma, kümeleme, alakalandırma ve regresyon analizi gibi konularda kullanılan Outlier Detection, steganografinin bir resim içerisinde bulunup bulunmadığını anlamak için kullanılmıştır. Outlier Detection iki çeşittir. Bunlar; Distance Based ve Distribution Based'dir. Mesafe tabanlı olan Outlier Detection'da Öklid uzaklığı formulü kullanılarak kümeler arası ve küme içinde merkez noktasına aykırılık gösteren noktalar bulunur. Distribution tabanlı olan Outlier Detection'da ise parametrik bir model oluşturulur ve küme içerisindeki herbir nokta tekrar çıkarılarak parametrik model hesap güncellemesi yapılır. Değişime sebep olan nokta, outlier olarak tespit edilir. Resimlerde bu işlemleri gerçekleştirmek zor olduğu ve güncel efektif bir kullanımı olan parametrik model olmadığı için makale yazarlar resim restorasyonu yapan programları kullanarak kendi ellerindeki steganografik resimleri restore etmiş ve programın düzelttiği bölgelerin izlerini sürerek steganografik mesaja ulaşmaya çalışmışlardır. Parametrik olmayan dağıtım/dağılım fonksiyonları kullanılmıştır. Resim restorasyonundan esinlenen bu fonksiyonlar, resimlerdeki enerji değerlerini hesaba katmaktadır. JPEG kurallarına göre, resiminlerin herbir pikselinin diğer piksellere konfigrasyonu ve bağıntısı bulunmakta, bu bağıntı resimlerin en az enerjili olmasını sağlamaktadır. Eğer bu pikseller üzerinde oynama yapılırsa, enerji bağınıtısı bozulur ve artış gösterir. Test aşamasında enerjisi artan piksellerin %87'sinin mesaj taşıdığı saptanmış ve kesin olarak yerleri bulunmuştur. Tezimizde doğrudan bir katkısı bulunmasada, uyguladıkları yöntem ve bakış açısı ile steganaliz mantığının kavranmasına çok yardımı dokunmuştur (Davidson ve Paul, 2004).

What makes the stego image undetectable (Steganografik görüntüyü ne saptanamaz yapar)

Bu makalede steganografik yöntem ve uygulamalardan çok steganografinin uygulandığı taşıyıcı resimlerin nasıl seçilmesi gerektiği ve bu seçilimin belli başlı metod ve kurallara uygun olması gerektiği üzerine çalışılmıştır. Resimlerin mesaj taşıma kapasitesinin ölçülmesi için GMM, Gaussian Mixture Model, ve formule edilmesi için Fisher Information Matrix kullanılmıştır. Sonuç olarak resim içi dağınıklığın, resimde fazla doku bulunmasının ve az karmaşıklık bir steganografi gömülümü için ideal resmi belirlemektedir. Tezimizde kullanılmamış ancak bir taşıyıcı resim seçiminde nelerin önemli olduğunu anlamamızı sağlayan faydalı bir çalışma olmuştur (Liu, Liu, Wu ve Zhong, 2015).

Development and anlaysis of stego image using discrete wavelet transform (Ayrık dalgacık dönüşümü kullanılarak steganografik görüntünün gelişim ve analizi)

Bu makalede Discrete Wavelet Transform yapılırken OPA, Optimum Pixel Adjustment, algoritması kullanılarak taşıyıcı resimlerin taşıma kapasitesi hesaplanmış ve buna uygun olarak resimin içerisine rastgele yerleşimlerle mesaj yerleştirilmiş ve sonucu test edilmiştir. Sonuç olarak rastgelelik içeren sistem, belirli bir sıra ve sıklıkla yerleştirilene göre daha fazla güvenilir olduğu bulunmuştur. Bu çalışmadaki rastgelelik kavramı tez çalışmamızdaki DWT rastgelelik işlemine zemin oluşturmuştur (Bera, Dewangan ve Sharma, 2013).

How to bootstrap anonymous communication (Anonim iletişime nasıl bootstrap yapılır)

Bu makale, Steganografinin teknolojik veya algoritmik uygulamalarından farklı olarak, steganografinin iletişim kanalları üzerinde nasıl uygulanabileceği ve anonim bir steganografik iletişim kanalının nasıl oluşturulması gerektiği ile alakalıdır. Makale tüm iletişim kanallarının takip edilmesi ve şahıs hayatlarının gizliliğinin ihlal edilmesinden ilham alınarak hazırlanmıştır. Bu sorundan dolayı bir protokol ve iş akış şeması geliştirmişler ve bunun güvenilirliğini test etmişlerdir. Herhangi biri blog sitesinde verileri taşıyıcı mesaj içerisine yerleştirip, daha sonrasında mesajları şifreledikleri

anahtar veriyi birbirilerine steganografi ile direk olarak gönderip, public olan yani herkesin görünümüne açık olan şifreli bilgileri almaları istenmiştir. Teorik açıdan oldukça faydalı olmasına rağmen şuanki tez çalışmamızda kullanılmamıştır (Jakobsen ve Orlandi, 2016).

Reversible data hiding scheme based on histogram shifting using edge direction predictor (Kenar yönü tahmini kullanılarak histogram kaydırması temel alınarak tersinir veri saklama)

Makalede taşıyıcı resim pikselleri matrise aktarılır. Tek ve çift sayılı satırlara ayrı olarak veri gömülümü işlemi gerçekleştirilir. Her satırdaki herbir piksel için "Edge Direction" tahmini yapılır ve hata değeri hesaplanır. Ardından "histogram shifting" yapılır ve gömülecek mesajda uygun gelen nokta ile birleştirilir. Bu işlem hem tek sayılı, hemde çift sayılı matris elemanlarının herbiri için yapılır ve gömülüm tamamlanmış olur. Sonuç olarak testlerde ortalamanın üzerinde bir başarı göstermiştir. Bu çalışmadan tezimizde faydalanılmamıştır (Kim, Lee ve Yoo, 2014).

Visual honey encryption: Application to steganography (Görsel bal şifreleme: Steganografide uygulanması)

Bu makalede Honey şifreleme yöntemi steganografi ile birlikte kullanılmıştır. Honey şifrelemesinin özelliği şudur; şifreli mesajı bulan ve mesajı çözmek için şifre giren kişilere karşı bu şifreleme her girilen yanlış mesajdan sonra anlam taşıyan yanlış metinler gösterir ve böylelikle kişiyi şaşırtmayı amaçlar. Yazarlar, klasik Honey şifrelemesini steganografi ile birlikte resimler ve diğer multimedya öğeleri üzerinde deneyeceklerdir ancak resimler için yeni bir honey şifreleme sistemi oluşturmaları gereklidir. Bunun için Markovian işlemini, Bayesian şeması ile birlikte kullanıp resimlerin suni yapısı oluşturulur. Bu işlemlerden sonra Honey şifrelemesi görsel alanlarda uygulanabilir hale gelir ve ismi "Visual Honey Encryption" olur. Bunun steganografide uygulanmasına ise "Honey Steganography" denir. Sonuç olarak yapılan steganografi aşılabilir ve şifreli mesaja ulaşılabilir. Ancak bu sistemi kırmak daha zor ve şaşırtıcı bir hal almıştır.

Bu çalışma sayesinde steganografi ve kriptoloji haricinde üçüncü ve yeni katman bir yaklaşım sunumunu öğrenmiş olduk ve tezimizin giriş ve sonuç kısımlarında çıkarımlarımızı aktarırken bu çalışmadan ilham aldık (Jo, Kim, Lee, Lee ve Yoon, 2015).

An information-theoretic model for steganography (Steganografi için bir bilgi-teorik modeli)

Bu makalade Steganografinin teori kısımından, algoritmalardan ve olası senaryolardan bahsedilerek, bunlara göre steganografi aşamaları geliştirilmiş, bu aşamalar matematiksel olarak gösterilmiş ve hesaplanmıştır. Bu çalışmadan tezimizde faydalanılmamıştır (Cachin, 2004).

Attacks on steganographic systems (Steganografik sistemlerde saldırılar)

Bu makalede yazarlar bir steganografi sistemi oluşturmaktan çok, bilinen steganografi platformlarının ve kullandıkları steganografi sistemlerinin yapısını ayrıntılı olarak incelemiş ve makalede anlatmışlardır. Ardından ise tüm bu sistemlere karşı ataklar yani steganaliz yöntemi gerçekleştirmişlerdir. Herbir yöntem ve atak tarzları gösterilmiş ve sistemlerin keşfedilen zayıf noktalarından şemalar ile bahsedilmiştir. (Pfitzmann ve Westfeld, 2000).

Improving steganographic security by synchronizing the selection channel (Seçim kanalı senkronizasyonu ile steganografik güvenliğin arttırılması)

Bu makalede Gibbs yapılandırılması kullanılarak taşıyıcı resime LSB'nin güçlendirilmiş bir yöntemiyle steganografi yapılmaktadır. Araştırmacılar deneyler sonucu random piksellerin şifreli mesajlarla değiştirilmesinin kanal ve taşıyıcıdaki bozulma ve ek gürültü değerlerini yükselttiğini ancak aksine birbirileri ile bitişik piksellerin veri değişiminde kullanılmasının daha az gürültü ve bozulmaya neden olduklarını bulmuş ve bunu çalışmalarına bu makale ile eklemişlerdir. Makalede ayrıca LSB yönteminin farklı bir kullanımı öğrenilmiştir (Denemark ve Fridrich, 2015).

Performance analysis of steganography based on 5 wavelet families by 4 levels DWT (4 seviye DWT'e göre 5 dalgacık ailesine dayandırılmış steganografi performans analizi)

Bu makalede araştırmacılar PSNR, Peak Signal Noise Ratio, değerine göre beş Wavelet türünün performans analizini yapmışlardır. Tüm dalgacık analizi türleri anlatılmış ve Steganografi işlemi adımları ile açıklanmıştır. Testlerin sonucuna göre ise 4-level Haar Discreate Wavelet Transform diğer dalgacık analizi türlerine göre daha başarılı bir PSNR değeri vermiştir. Bu makale sayesinde, DWT yöntemimizde Haar yöntemini DCT yöntemine karşı seçildi ve çokca faydalı bilgiler edinildi (Chandel, Gupta ve Patil, 2014).

2. MATERYAL VE METOD

Tezimizin bu bölümünde, metot olarak dijital resim steganografisi yapacağımız için öncelikle dijital resim steganografisine kadar olan bölümlerden bahsedip, daha sonrasında, bu yöntemin metotlarına değineceğiz. Bu bölümde önce Uzaysal/Resim tabanlı steganografi ve alt dallarını ayrıntılı bir şekilde anlatacağız ve ardından Transform (Değişim)/Frekans tabanlı steganografi ve alt dallarından ayrıntılı bir şekilde bahsedeceğiz. Bir diğer başlığımız olan materyal konusunda ise kullanılan taşıyıcı resimlerden ve gizli mesajdan bahsedilecektir.

2.1. Materyal

Tez çalışmamızdaki materyallerimiz, içerisine veri gizlemesi yaptığımız taşıyıcı resimlerdir. Performans ölçümlerinin daha düzgün ve kesin yapılabilmesi için bu bölümde kullanılan resimlerimizin hepsi aynı boyutlarda ve aynı resim uzantılarındadır. Kullandığımız taşıyıcı resimler ve DWT yönteminde taşıyıcı resimlerin arkasına gizlediğimiz gizli mesaj olan diğer resimler aşağıdaki gibidir. Tezimizin senaryosu gereği DCT yönteminde gizli mesaj olarak kullanıdığımız metinsel veriler ise EK A ve EK E'de yer almaktadır. Aşağıdaki Şekil 2.1-2.7 aralığında, kullandığımız orjinal taşıyıcı resimler verilmiştir. Bu taşıyıcı resimlerin boyutları ortalama 300 Kb değerindedir.

Şekil 2.1 : Taşıyıcı Resim 1

Şekil 2.2 : Taşıyıcı Resim 2

Şekil 2.3 : Taşıyıcı Resim 3

Şekil 2.4 : Taşıyıcı Resim 4

Şekil 2.5 : Taşıyıcı Resim 5

Şekil 2.6 : Taşıyıcı Resim 6

Şekil 2.7 : Taşıyıcı Resim 7

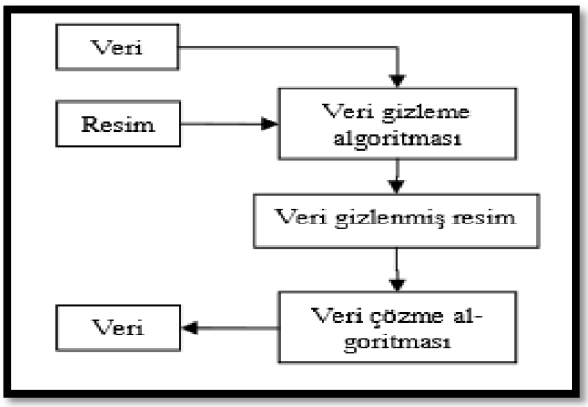
Aşağıda verilen Şekil 2.8-2.9'da, kullandığımız gizli mesaj görüntüleri bulunmaktadır. Kullandığımız diğer gizli mesaj verilerimiz olan metin dosyaları ise daha önce belirtildiği gibi EK A ve EK E'de verilmiştir.

Şekil 2.8 : Gizli Mesaj 1

Şekil 2.9 : Gizli Mesaj 2

2.2. Metod

Bu bölümde, tezimizin uygulama aşamasında kullandığımız metotlardan ve iş akış diagramlarımdan adım adım bahsedeceğiz. Tezimizin amacı; görsel veri analizinde kullanılan iki popüler metodun, MATLAB platformu üzerinde test edilerek hangisinin steganografi uygulaması olarak daha başarılı olduğunun çıkarımına erişmektir. Bu doğrultuda steganografi performans ölçüm parametrelerinden biri olan PSNR değerini belirleyici faktör olarak seçip, DCT ve DWT metotlarını bu parametre üzerinden karşılaştıracağız. İlk olarak en sade hali ile steganogragfi sistemi nasıldır ve iyi bir steganografi sistemi oluşturmak için hangi esaslara dikkat etmek gereklidir sorularının cevapları verilecektir. En sade hali ile bir steganografi sistemi Şekil 2.10'daki gibidir (Esin ve Güvenoğlu, 2012);



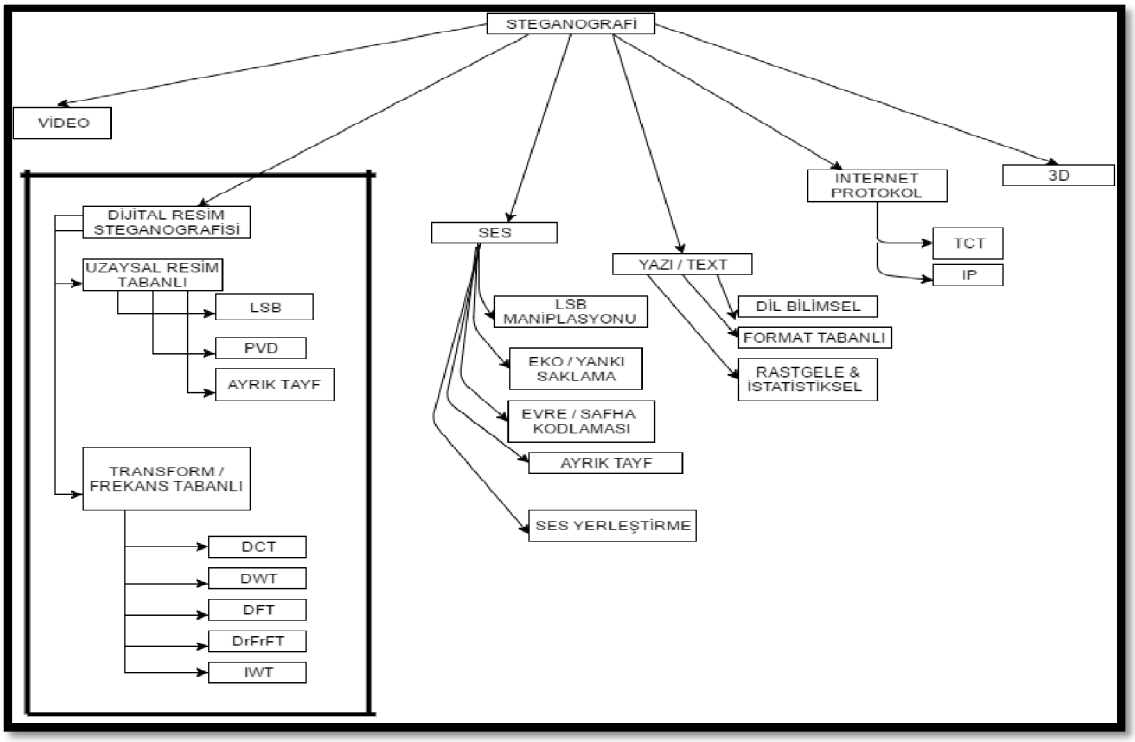
Şekil 2.10 : Temel Steganografi sistemi

Güvenilir bir steganografi sistemi inşaa edilirken;

- **Görünmezlik:** Steganografik sistemin insanlar tarafından (insan gözüyle) farkına varılamaz olmasıdır. Steganografik mesajın, taşıyıcı unsur üzerine gömülümü işleminden sonra resimde meydana gelecek değişimler, insan gözüyle farkına varılamaz olmalıdır. İnsan gözü parlaklık ve bulanıklık gibi görsel değerlere karşı duyarlı olduğu için bu değerlerin değişim göstermemesine dikkat edilmesi gerekmektedir.
- **Güvenlik:** Saldırgan, taşıyıcı obje üzerinde gizli mesajın varlığını farketse bile mesajı ortaya çıkarmasının imkansıza yakın olması durumudur. PSNR, Peak Signal Noise Ratio baş harflerinden oluşturulmuştur. Bu ölçü birimi ne kadar yüksek değerli olursa sistemimiz o kadar güvenli demektir.
- **Kapasite:** Önemli mesajın kapasitesinin, taşıyıcı mesajın kapasitesinden fazla olmaması durumudur. Bunun yaklaşık olarak maksimum %51'lik kısımının geçmemesi tavsiye edilir. Aksi taktirde, steganografinin unsurlarından olan görünmezlik unsuru delinmiş olur.
- **Sağlamlık:** Steganografinin taşıyıcı unsuru resim, video vb. üzerinde yapılan filtreleme, kesme-kırpma, yön değiştirme ve sıkıştırma gibi maniplasyonlara karşı dayanıklı olması durumudur (Acharya, Kamath, Prabhu ve Shama, 2012).

Bu gibi değerlere dikkat edilmelidir. Buradaki değerlerin uygunluğu bizim sistemimizin ne kadar güvenilir olduğunu göstermektedir. Bahsedilen değer unsularının haricinde, dikkat edilmesi gereken bir diğer unsur ise kullanacağımız steganografik metotlardır. Birçok steganografik metot mevcuttur ancak herbirini dilediğimiz gibi

kullanamamaktayız. Gizli mesajımızı taşıyan taşıyıcı unsurun türüne göre steganografik metodumuzu belirleyebilir veya bunların kombinasyonlarını kullanabiliriz. Unsurlara göre steganografi metotları aşağıdaki Şekil 2.11'de gösterilmiştir (Dhawale, Hegadi ve Jambhekar, 2014).



Şekil 2.11 : Steganografi Metotları

Tez çalışmamızda steganografi uygulayacağımız metot, dijital resim steganografisidir. Başarılı bir dijital resim steganografisinde dikkat edilmesi gereken unsur, steganografi yapılacak taşıyıcı resimin görüntü ve içerik özellikleridir. Bu özellikler taşıyıcı resiminizin taşıma kapasitesini belirlemede kullanılır. Bu kapasiteyi belirlemek için GMM, Gaussian Mixture Model, ve Fisher Information Matrix gibi bilimsel yöntemlerden faydalanılabilir ve taşıma kapasitesini hesaplama işlemi tamamlanabilir. Yapılan bilimsel araştırmalarda resim içi renk dağınıklığı, fazla katman ve doku bulunmasının ve az karmaşıklığın ideal bir steganografik resimi belirleyen unsurlar olduğu belirlenmiştir (Liu, Liu, Wu ve Zhong, 2015).

Literatür taramasından sonra tezimizin ikinci bölümünde; kullanılan materyaller, platformlar ve steganografik veri tabanını oluşturan resimler hakkında bilgi verilecektir.

Üçüncü bölümümüzde kullanılacağımız steganografik analiz yöntemleri ve steganografi uygulamaları hakkında ayrıntılı bilgi verilecek ve ardından dördüncü bölümümüzde tezimizin ana teması olan sistemimizin bilimsel yöntemi ayrıntılı olarak anlatılacak ve en son olarak sonuç bölümüyle bitirilecektir.

2.2.1. Uzaysal/resim tabanlı steganografi

Sptaial Domain, Uzay / Resim tabanlı steganografi'de asıl amaç taşıyıcı resimin pikselleri ile ASCII tablosuna göre oluşturulmuş gizli mesajın bit'lerini yer değiştirmektir. Kullanacağımız resim siyah beyaz bir resim olursa, böyle bir durumda her bir byte'a bir veri saklamamız önerilir. Eğer taşıyıcı resimimiz renkli bir resim ise bu durumda Red-Green-Blue üç ana renk kuralına göre 3 byte yani 24 bit'lik bir değişim bloğumuz bulunur ve böylelikle veri saklama alanımız genişler. Bu metodun avantajı, anlaşılması basit ve kolay uygulanabilir olması iken dezavantajı ise ustaca kullanılmadığı taktirde histogram veya entropy analizi ile kolayca bulunabilmesidir (Verma, 2011). Ustaca kullanımdan kastedilen, byte yapısına hakim olunması ve yapılan bozulumlara gürültü süsü verilebilmesidir. Bilindiği üzere bir byte bloğundaki en baştaki ve en sondaki bitler Most Significant Bit, MSB ve Least Significant Bit, LSB'dir. Algoritmanın adında anlaşılacağı gibi kesinlikle LSB'ler mesaj bitleri ile değişime uğramalıdır. Buradaki istisnai durum, bazı byte'ların resimin parlaklık değerleri ile alakalı olabilmesidir. İnsan gözü ayrıntıyı ayırt etmede ne kadar başarısız olursa olsun, parlaklığı ayırt etmede gayet hassas ve başarılıdır. Bit değişimleri yapılırken kesinlikle parlaklık değelerini değiştirmemeye özen gösterilmelidir. Son yıllarda resim kanalları seçimi ve bit'lerin yer değişimi ile ilgili birçok sistemi kuvvetlendirmeye yönelik çalışmalar olmuştur. Bu çalışmalar sonucunda, rastgelelik ve bitişik değerlerin değişiminin daha faydalı olduğu gözlemlenmiş ve sıfır bozunum, kaotik sıralama gibi fonksiyonlarla hata payı ve güvenilirliği arttırılmıştır (Batham, Virendra ve Yadav, 2014).

2.2.1.1. LSB yöntemi

En çok kullanılan veri saklama yöntemidir. Dezanatajlarına nazaran bu kadar çok popüler olmasının sebebi kolay tanıtılabilir ve kullanılabilir bir sistem olmasıdır (Verma, 2011). Bu yöntemdeki amaç, şifreli mesajın bit'leri ile taşıyıcı mesajın bit'lerini

değiştirerek, şifreli mesajı taşıyıcı mesaj platformuna eklemektir. Bu ekleme işlemi, steganografi yapılacak taşıyıcı platform ögesinin (resim, müzik veya ses kaydı) değerlerinin, bilgisayarın işlem yapabileceği format olan ikili sayı sistemine dönüştürülmesi ile başlar. Bilgisayardaki ASCII (tüm harflerin ve karakterlerin bilgisayardaki sayısal değerlerinin tutulduğu tablo) tablosu kullanılarak şifrelenilecek mesaj sayısal değerlere dönüştürüldükten sonra mesajımız istenilirse kriptoloji algoritmasından geçirilerek şifrelenebilir. Bundan sonraki aşama LSB algoritmasının uygulanmasıdır.

Algoritmanın temel prensibi mesajın bitlerinin platformdaki 8 bit'lik blokların en az etki değerine sahip bit'lerle değiştirilmesi esasıdır. Bu bit'lere İngilizcede Least Significant Bit denilmektedir ve algoritmamız bu tanımın baş harflerinden oluşmaktadır, LSB. Steganografiyi taşıyacak olan platform herhangi bir çoklu ortam medya unsuru olabilir (multimedya öğesi). Herbirinin dikkat edilmesi gereken önemli noktaları vardır. Bu noktalar resim formatı için "monochrome" denilen, resimdeki tek renkli piksellerdir. Bu piksellerin bit'leri ile kesinlikle şifreli mesaj değişimi yapılmaz çünkü tek renkli piksel şifreli mesajla değiştirildiği anda farklı bir renk tonunu alır ve bu da çıplak gözle dahi anlaşılabilecek bir hataya yol açar. LSB'nin matematiksel gösterimi aşağıdaki denklem 2.1 gibidir;

$$x'_i = x_i - x_i \bmod 2^k + m_i \qquad \textbf{(2.1)}$$

Bu denklemde;

- x'_i steganografik resimin i sayılı pikselini,
- x_i buna karşılık gelen değiştirelecek taşıyıcı resimin pikselini,
- m_i değeri i'ninci blok'taki güvenilir data'yı,
- Formüldeki mod değer üzerinde ki "k" sayısı LSB'de değiştirilecek işlem sayısını gösterir.

  Tüm bu çıkarılan bit'ler veya çıkarım işlemleri k değerindeki en sağ değerin değişimlerini sağlamak içindir. Matematisel olarak mesaj aşağıdaki denklem 2.2 gibidir;

$$m_i = x_i \bmod 2^k \qquad \textbf{(2.2)}$$

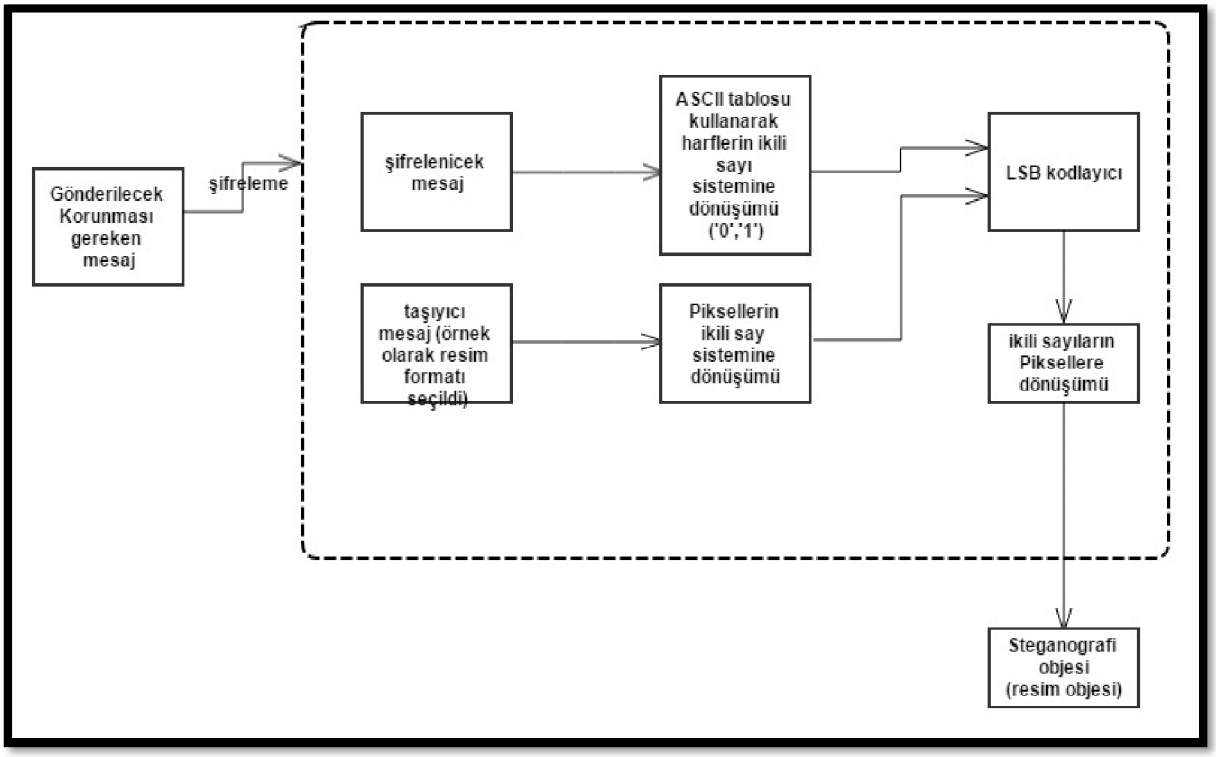
Aynı durum ses ögeleri için de geçerlidir. Desibel değerlerinin ses dosyalarındaki değişimde belirli bir eşik değerinin altında tutulması gerekir. Bunun üstüne çıkan değişimlerde, şahıslar herhangi bir yazılıma ihtiyaç duymadan farklılık olduğunu anlayabilir ve gizlememiz açığa çıkabilir (Bender, Gruhl, Lu ve Marimoto, 1999). En az değişim sağlayan, en değersiz bit'lerin değişimi, platformun genelinde gözle görülebilen bir değişim sağlamadığından analizcilerin dikkatine takılmamış olur. Aksi taktirde resimlerdeki renk ve parlaklık, ses kayıdı ve videolarda görüntü ve ses bozuklukları herhangi bir program kullanılmadan farkına varılabilir. Bu yüzden genellikle renk değişimi problemine takılmamak için siyah beyaz resimler ile veri aktarımı yapılması daha kolay ve sorunsuz olduğundan tavsiye edilmektedir (Verma, 2011). Asıl amaç aşağıdaki Şekil 2.12'de görüldüğü gibi farkedilemez olmaktır.

(Normal Resim) *(Steganografi içeren Resim)*

Şekil 2.12 : Normal Steganografik Resim Karşılaştırması

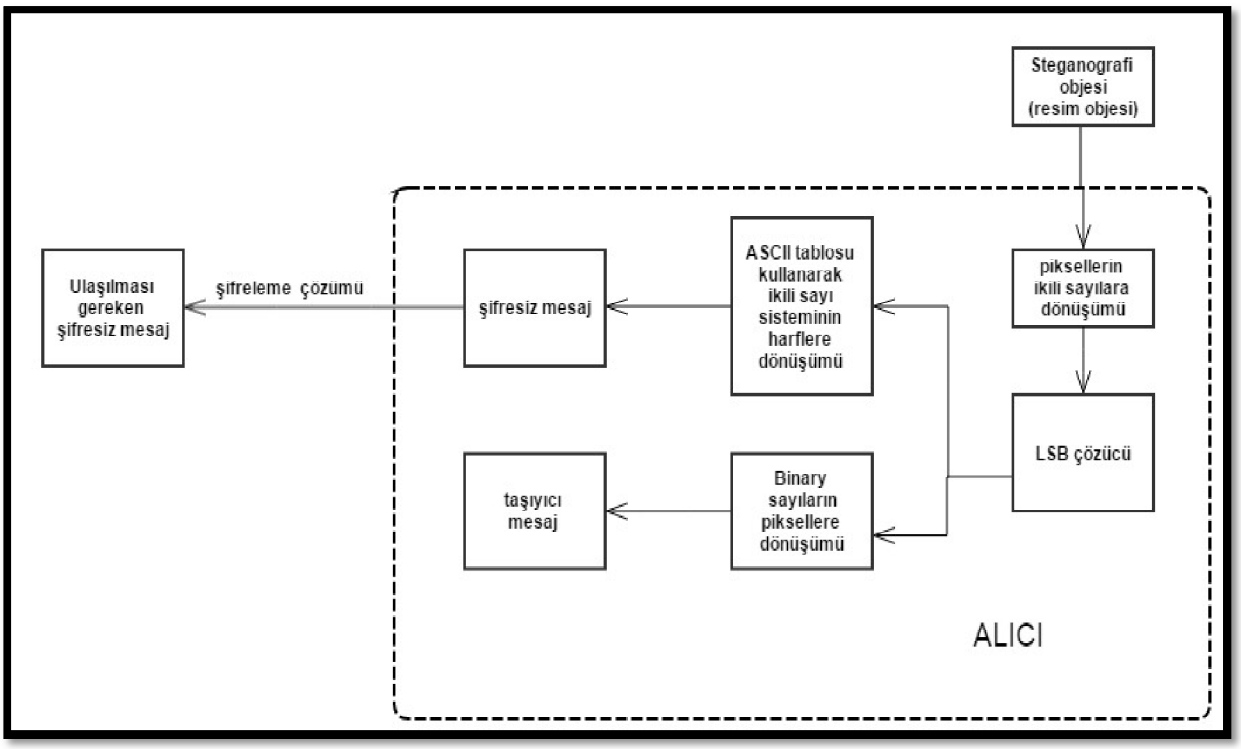
Günümüzde veri optimizasyonu giderek artmakta ve gelişen veri sıkıştırma yöntemleri ile birlikte geniş mesajları gönderebileceğimiz büyüklükte resimlerin kullanılırlığı azalmaktadır. 800x600'lük bir resimin internet üzerinden gönderimini yapmak gayet dikkat çekici bir durum olduğundan, LSB gibi bit'ler üzerinde değişim yapan algoritmaların farkına varılabilirliği giderek artmaktadır. Ancak tüm bu dezavantajlarına rağmen halen en çok tercih edilen yöntemlerden biridir. LSB steganografinin bu basitliğini gösteren olay döngüsü Gönderen ve Alıcı tarafları açısından ayrı ayrı şematize edilmiştir. Tez çalışmamızda LSB yöntemi DCT yönteminin içinde kullanılmıştır. Bu yüzden tezin bu kısımında ayrıntılı olarak anlatılmaktadır. DCT yönteminin daha ayrıntılı anlatıldığı ilerki bölümlerde LSB kullanımını anlatan şekil ve metinsel verileri

görebilirsiniz. Aşağıda bu tez kapsamında hazırlanmış olan Şekil 2.13'de, gönderen için LSB steganografi aşamaları gösterilmektedir.



Şekil 2.13 : Gönderici için LSB Steganografi Aşamaları

Aşağıda tezimiz kapsamında hazırlanmış olan Şekil 2.14'de, alıcı için LSB steganografi adımları gösterilmektedir:



Şekil 2.14 : Alıcı için LSB Steganografi adımları

2.2.1.2. Piksel Değeri Farkı

PVD, Pixel Value Differencing, algoritması LSB yöntemine kıyasla taşıyıcı resim üzerine daha fazla veri gömme kapasitesine sahiptir. Bunu gerçekleştirirken, resim üzerinde bir iz bırakmadan ve çözünürlük kalitesi yüksek resimler yaparak gerçekleştirir. Bu metot 8 bit'lik siyah beyaz resimlere veri saklama işlemi yapılırken geliştirilmiş bir yöntemdir. Bu yöntemde taşıyıcı resimin sol üst köşesinden başlayarak tüm resimin üzerinde zig zag şeklinde ilerler. Resimi birbirine karşımayacak piksel bloklarına böler. Bu bloklardan ilk ikisi resimin pürüzsüzlüğünü oluşturduğu için herbir satırdaki pürüzsüzlük bloklarına veri gömülümü yapılmaz. Ancak bu blok piksellerin diğer piksellerle aralarında ki farklılıklar ölçülür. Bu farklılık ne kadar yüksek ise bu satırdaki bloklara o kadar fazla veri gömülümü yapılabilir (Verma, 2011).

2.2.1.3 Ayrık tayf/spekturum

Spread Spectrum, Dağınık/Ayrık Spekturum metodu gizli mesajı, taşıyıcı resimin heryerine dağıtmayı amaçlar ve bu yüzden zor bir metotdur. Öncelikle mesaj noise adı verilen resime kanal içinde eklenen gürültü içersine yerleştirilir. Bu gürültü/ses taşıyıcı

resime eklenir. Böylelikle steganografik resim oluşmuş olur. Sinyal frekansı açısından mesaj taşıyıcı resime göre düşük bir sinyal içerir. Bu yüzden resim üzerindeki değişimler gözle veya uzman bir steganalizci tarafından anlaşılamaz. Bu yöntemi istatistiksel olarak güçlü, pratikte ise güvenilir bir yöntem olduğu akademik çalışmalarda bahsedilmiştir (Dhawale, Hegadi ve Jambhekar, 2014).

2.2.2. Transform/frekans tabanlı steganografi

Dijital resim/görsel steganografinin bir dalı olan bu yöntemde amaç, mesajı taşıyıcı resimin spesifik ve belirlenmiş önemli bir bölgesine gömülümünü gerçekleştirmektir. Bunun için resimler piksel tabanından frekans tabanına çekilir ve gömülüm frekans tabanında gerçekleştirilir. Taşıyıcı resimin birden fazla frekans bandı bulunur ve gizli mesaj bu bandlardan istenilen bir tanesine eklenir. Bu yöntemle sistem steganografik algoritmayı dıştan gelen gürültülere daha fazla tolere edilebilir bir hale getirir. Buda güvenliği arttırıcı bir etmendir. Tüm bu nedenler ve ileride anlatacağımız ek özellikler ile bu sistemin daha güvenilir olduğu kabul edilmektedir. Sistem ne kadarda kuvvetli olsada, karmaşıklık ve sistemin entegre edilmesinin uzun sürmesi ve yavaş olması bu yöntemin dezavantajlarındandır (Chaudhary ve Kaushal, 2013). Tezimizin bu bölümünde frekans tabanlı steganografi yöntemlerinden olan Discrete Wavelet Transform, DWT, Discrete Cosine Transform, DCT, Discrete Fourier Transform, DFT den bahsedeceğiz.

2.2.2.1 Ayrık fourier dönüşümü

Joseph Baptiste Fourier tarafından oluşturulan DFT, Discrete Fourier Transform (Ayrık Fourier Dönüşümü), frekans analizi zaman tabanlı dizilerin analizinde en çok kullanılan ve en çok bilinen yöntemlerin başında gelir. Fourier dönüşümü steganografide öncelikle uzay tabanlı görsel bir resimi frekans tabanına çekmek için kullanılır. Fourier'in diğer kullanım alanlarında bahsedilen dezavantaj, zaman dizisinden frekans dizisine geçilme esnasında tüm zaman bilgilerinin yok olması durumudur. Ancak steganografik uygulamasında zaman ölçütü bizim için tolere edilebilecek bir alandır. Çünkü zamansal incelemeler, sinyallerde değişim anının incelenmesine olanak sağlarken, veri gizleme işleminde böyle bir ihtiyaç bulunmaz.

Fourier dönüşümü diğer dönüşümler gibi öncelikle uzay tabanlı taşıyıcı resimin ve mesajın, frekans tabanına çekilmesi ile başlar. Frekans tabanına dönüştürülen resim 2x2 piksel bloklarına çevirilir ve LSB mantığına göre en az değişime sebep olacak piksellerin frekansları ile mesaj frekansları yer değiştirilir. Tüm mesajın gizlenmesi tamamlandıktan sonra tüm frekans bandları tekrar uzay tabanlı piksellere dönüştürülerek steganografik resim elde edilmiş olunur.

Ayrık Fourier dönüşümü tezimizin kullanılan yöntemlerinden biri değildir, ancak bu yöntem tüm diğer yöntemlerden eski bir tarihsel alt yapıya sahip olduğu ve ilk kullanılan yöntem olduğu için kuramsal karşılaştırma yapabilmek açısından tezimizde yer almaktadır.

2.2.2.2. Ayrık kosinüs dönüşümü

Bütün frekans tabanlı dönüşüm steganografilerinde resimler, image/resim, spatial/uzaysal tabandan frekans tabanına çekilir. Bunun için NxN olarak adlandırılan genel olarak 8x8 matris bloğuna aktarılan bir sistematik işlem düzeneğinden geçirilir. Bu işlem düzeneği kısaca "converter" dönüştürücü olarak adlandırılır.

Dönüştürücü çeşitleri arasındaki farklar ise resimi işlemek ve incelemek için kullandıkları sinyal türleri ve dönüştürücü mekanizmasındaki matematiksel formulasyon farklarıdır. Aşağıdaki resimde DCT, Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)'un matematiksel formülasyonunu 2.3 ve 2.4'de görmekteyiz (Dhawale, Hegadi ve Jambhekar, 2014).

$$F(u,v) = \frac{c(u)c(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} \cos\left(\frac{(2i+1)u\pi}{16}\right) \cos\left(\frac{(2j+1)u\pi}{16}\right) f(i,j) \qquad \textbf{(2.3)}$$

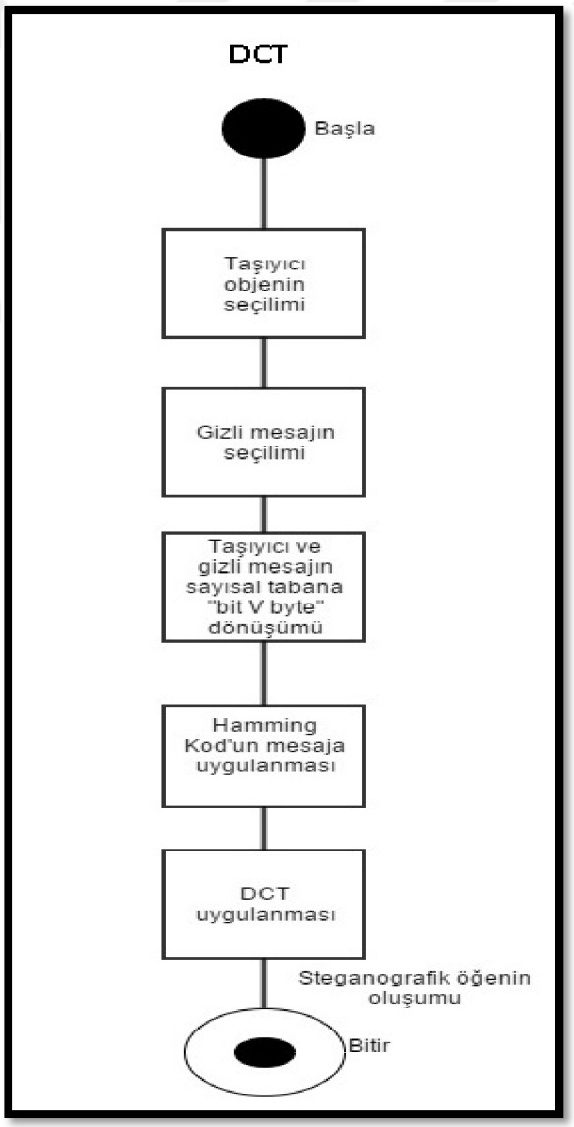
$$c(\acute{\varepsilon}) = \begin{cases} 1^{1/\sqrt{2}} & \acute{\varepsilon} = 0 \text{ ise} \end{cases} \qquad \textbf{(2.4)}$$

Formüldeki;

- F(u,v) fonksiyonu bir DCT'nin (u,v) kordinatındaki,
- f(i,j) fonksiyonu bir DCT'nin (i,j) kordinatındaki piksel değerlerini göstermektedir.

Ayrık Kosinüs Dönüşümünde, kosinüs sinyallerini kullanılmakta ve resimleri uzaysal tabandan frekans tabanlı matris yapısına kosinüs dönüştürücüsü ile dönüştürülmektedir(Dhawale, Hegadi ve Jambhekar, 2014).

Bu bilgiler ışığında tez çalışmamızda, tezimizin amacına uygun bir şekilde oluşturduğumuz DCT senaryosundan bahsedeceğiz. Başlangıç olarak bir taşıyıcı resim ve gizli mesajın program arayüzünden seçilmesi ve daha sonrasında arka planda gerçekleştirilen adımlar anlatılacak ve en son olarakta steganografik resim ve orijinal taşıyıcı resimin kıyaslanması ile PSNR değeri hesaplanacaktır. Bu iş akışının sembolik olarak gösterildiği diagram Şekil 2.15 gibidir.



Şekil 2.15 : DCT Senaryosu

Taşıyıcı obje her iki metodda 512x512 boyutunda bir resimdir. İki metodun performanslarının kıyaslanabilmesi için taşıyıcı objeler ve gizli mesajın KB, Kilobyte, cinsinden aynı olması gerekmektedir. Bu yüzden gizli mesaj, 40 KB değerindeki bir resim veya "text" metin verisinden seçilebilir. DCT metodunda ise gizli mesaj olarak 40 KB'lık bir metin verisi seçilmiştir. Bu metin verisi ASCII tablosundan faydalanılarak sayısal tabanlı verilere dönüştürülmüştür ve 8x8 boyutunda bir matrise atanmıştır. Daha sonrasında bu matris değerlerinde, bir düzeltme ve güvenilirliği arttırma amacıyla Hamming kodlama yapılmıştır. Taşıyıcı resminde 8x8 boyutunda bir matrise çekilmesiyle DCT'nin uygulanması için tüm hazırlıklar tamamlanmıştır. Daha öncesinde steganografik iletişimin temellerinde bahsedildiği gibi tezimizin bu bölümünde de gizli verinin alıcı tarafından elde edilmesi için karşılıklı bilgi paylaşımı yapılmıştır. Bu bilgi paylaşımı verinin taşıyıcı mesajın hangi bölümlerinde yer aldığı ile ilgilidir.

Resimlerin her 8x8 boyutunda oluşturulan veri bloklarında, veri değişimi için kullanılan frekans değerleri (2,2) ve (6,1) koordinatlarıdır. Alıcı sadece bu bilgiye sahip olarak alınan resimden bu spesifik kordinatlardaki verileri alarak gizli mesaja ulaşabilir. Kullanmış olduğumuz bu yöntem örnekleme yöntemlerinden sistematik örneklemenin uygulanmış şeklidir. DCT algoritması kendi içerisinde bu matris bloklarını kendi öznitelik tablosu ve transpoze edilmiş yani tersi alınmış matrisleri birleştirerek görsel verileri frekans tabanına çekmek işlemini gerçekleştirmektedir. Böylelikle frekans tabanına çekilmiş gizli ve taşıyıcı veri birleştirilmiş ve steganografik resim oluşturulmuştur. Burada daha önceki bahsettiğimiz LSB yöntemi, veri değişimleri esnasında uygulanmıştır ve insan gözünün parlaklık değerlerine karşı duyarlı olmasından dolayı sistem DCT algoritmasını siyah beyaz formatta gerçekleştirmiştir. Ayrıca DCT algoritmasının pseudo kodu EK B'de verilmiştir.

2.2.2.3. Hamming kodlaması

Telekominikasyon sektöründe çalışan Richard Hamming'in geliştirdiği bir yöntemdir. 1940 yılında bir dizi testlerden sonra matematiksel ve algoritmik ispatları ile kamuoyuna sunulmuştur. Sunulduğu dönemlerde büyük bir ihtiyacı gidermiştir. Sinyallerin hatlarda gönderimi esnasında meydana gelen çeşitli etkiler neticesinde göndericiden alıcıya giderken değişimlere uğradığı saptanmış ve bunun çözülümü için geliştirilmiştir.

Günümüzde halen farklı alanlarda kullanılmaktadır. Tezimizde ise; metinsel veri olan gizli mesajın 2 tabanındaki sayısal dönüşümünden sonra meydana gelebilecek hatalarının düzeltilmesi için kullanılmıştır.

Hamming kodlama lineer veri hattı üzerinde çalışır. Hata bulabilir ve hatayı düzeltebilir. Hatayı sadece saptayıp uyarı gönderebilir veya hatayı bulamaz. Farklı senaryolarda bu bahsettiğimiz olaylar gerçekleşebilir. Tezimizdeki kullanım amacına uygun olmasından dolayı sadece genel Hamming kodlaması bilgisi verecek ve (7,4) olarak adlandırılan basit adımlısından bahsedeceğiz. Elimizde 4 bit'lik 1001 verisi olduğunu farzedelim. Bu verinin alıcıya düzgün bir şekilde ulaşmasını sağlayabilmek için veriye kontrol amaçlı 3 adet kontrol bit'i ekliyor ve sonuna bu kontrol bit'lerini eşitleyecek Parity bit'i tanımlıyoruz. Buradaki genel amaç, bilgi içeren ilk 4 mesaj bitinin verilerinin, sonradan eklenen Hamming kontrol bitleri ile sürekli olarak çift yapılmaya çalışılmasıdır. Mesaj Hamming kodlamaya sokulduktan sonra görüntüsü $1001H_1H_2H_3P$'dir. Sırasıyla H verileri 5'inci, 6'ıncı, ve 7'inci bit'lerdir. H_1 1. 2. ve 3. verilerin 2 sayı tabanındaki matematiksel toplamıdır. Bu toplam H_2 için 1'inci, 3'üncü ve 4'üncü, H_3 için 2'inci, 3'üncü ve 4'üncü bit değerleridir. H değerleri bahsedilen matematiksel toplamın sürekli olarak 2 sayı tabanında 0 sonucunu vermesine uygun değerler alırlar.

Sonuç olarak bu eklenen değerler, gönderilen veri alıcıdan alınıncaya kadarki farkları ile kıyaslanır ve hatanın yeri saptanmış olur. Bu saptanmaya göre ise veri üzerinde düzeltme yapılır. Bu düzeltme işlemi Syndrome adı verilen ve S ile sembolize edilen başka bir veriler üzerinde gerçekleşen toplama işlemidir. 8 bit'lik bir veri kümesinde herbir H değeri Hamming mantığının eşitliğini sağlayan, bilgi içeren diğer bitler ile toplanır ve sonucunun sıfır olması beklenir. Aksi durumlarda veri üzerinde değişim olmuş demektir ve 1 sonucunu veren veriler düzeltilir. İlk başta bahsettiğimiz (7,4)'lük sistem, en sona veri bloğunu tamamlayan son bit hariç toplam 7 bit'lik veriden, 4 tanesinin veri içerdiğini sembolize ettiği için bu tarz bir tanımlama yapılarak anlatılmaktadır.

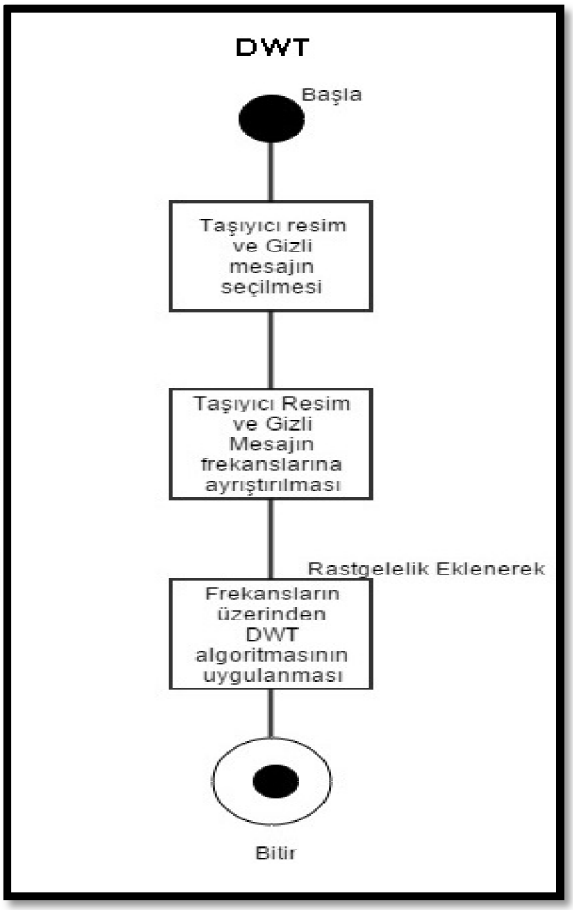
Hamming kodlama steganografi çalışmamızda gizli metinsel mesajın 2 tabanlı sayısal verilere dönüşümü sırasında meydana gelebilecek hatalı sıralamaların düzeltilmesi ve önüne geçilmesi amacı ile kurduğumuz sisteme eklenilmiştir. Hamming kodlama ile ilgili çalışmamızda ayrıntılarını vermiş olduğumuz kodlar EK D bölümünde yer

almaktadır. Buradaki amacımız, Hamming kodlama kullanarak düzeltilmiş mesajı, ikili sayısal tabanlı değerlerinin DCT özniteliklerine en az bozulmayı verebilmesini sağlamaktır (URL3).

2.2.2.4. Ayrık dalgacık dönüşümü

Ayrık Dalgacık Dönüşümü, DWT, Discrete Wavelet Transform, sinyal işlemede aitlik/sahiplik işlemleri olan ve Türkçesi Filigran olan ancak çoğunlukla İngilizce ismiyle kullanılan Watermarking işleminde ve görüntü, veri sıkıştırmada kullanılan bir yöntemdir. Bu yöntem dalgacık olarak tabir ettiğimiz ana sinyali matematiksel, zaman ve frekans bandında ufak dalgalara böler ve bu bandlarda işlem yapar. Bu dalgacıkların diğer yöntemlere kıyasla üstünlüğü daha ufak zaman dilimlerinde meydana gelen ufak ama sonucu etkileyebilecek dalgalanmarı inceleyebilmemize olanak sağlamasıdır. Ayrık Fourier Dönüşümünde, DFT, olduğu gibi sinyali sadece tek bir frekans bandında incelemez, daha ufak ve ayrıntılı dalgacıklarda incelenerek daha iyi gözlemler yapabilmemize olanak sağlar. Ayrık Kosinüs Dönüşümünde, DCT, olduğu gibi DWT uygulanırken taşıyıcı resim ve mesaj frekans boyutuna dönüştürülür. DWT taşıyıcı resimi yüksek ve alçak frekans olmak üzere iki frekans dalgasına ayrıştırır. Yüksek frekans nitelik, özellik taşıyan frekanstır. Eğer az veri saklanacaksa bu kısımda veri saklanması idealdir. Çünkü bu bölgede yapılan fazla değişimler taşıyıcı resimin insan gözüyle tespit edebileceği bozulmalara yol açabilir. Diğer bir olasılık olan yoğun bir bilgi saklama işleminde ise düşük band taşıyıcı olarak seçilmelidir. Bu kısımda çokça veri bulunmakta ve buda çokça veriyi saklayabiliriz anlamına gelmektedir. Tabiki kapasite değerleri aşılmamalı ve bozulmalara dikkat edilmelidir. Ancak taşıyıcı bandın düşük frekans seçilmesinin bazı dezavantajları vardır. Yüksek frekans gibi sağlam değillerdir. Çünkü yüksek frekansda veri saklamak farkedilirliği az olan bir işlemdir ve dolayısıyla bu bölgede yapılan değişimler enerji değerlerinde değişime sebebiyet verir. JPEG standartlarında bahsedilene göre resimler en düşük enerji düzeyine göre ayarlanmıştır. Bu piksel kümesinde, matrisinde, meydana gelen her türlü değişim resimin ortalama enerjisini üstel yönde etkileyecek bir değişim oluşturur ve bu değişimler histogram ve entropi analizlerinde kolayca açığa çıkabilir (Dalvi ve Kamathe, 2015).Bu bölümde, ikinci olarak oluşturduğumuz DWT algoritması adımlarından geçmişte verdiğimiz bilgiler doğrultusunda ayrıntılı olarak bahsedeceğiz. Aynı DCT'de

olduğu gibi, işlemlerimiz öncelikle taşıyıcı resimin ve gizli mesajın seçilimi ile başlamakta ve DWT dönüşümünün uygulanması ile devam etmektedir. DWT iş akış diagramı aşağıdaki Şekil 2.16 gibidir.



Şekil 2.16 : DWT Senaryosu

DCT'de olduğu gibi DWT senaryosunda taşıyıcı objemiz 512x512 formatında bir resim ve gizli mesajımızın boyutuda 40 KB'dır. Burada DCT Hamming kodlamasındaki etki gibi bir etki oluşturmak için 40 KB'lık resim verisinin siyah beyaz formatındaki taşıyıcı resime dengeli ve rastgele dağılmasını sağlamak için kod ile müdahale yapılmış ve daha sonrasında DWT uygulanarak resim ve mesaj verileri matrislerde frekans tabanına çekilerek birleştirilmiştir. Hamming kodlama, görsel olarak veri analizi sinyal gösterimlerinde gözüken kırılmaları adeta tıraşlayarak bozulmaları önler iken DWT'de kod ile eklediğimiz rastgelelik özelliğide sıralı ya da periyodik olarak tabir edebileceğimiz bozulma ve kırılmaların analizinin engellenmeye çalışmaktadır. DWT ile frekans tabanında birleştirilen ve tekrar görselliğe kavuşturulan yeni oluşturulmuş

resmimiz steganografik bir obje olmuştur. Bundan sonra taşıyıcı resimin orijinal hali ile DWT ile oluşturulmuş steganografik resmimizi kıyaslayarak PSNR değerlerini elde edip DCT ile kıyaslayacağız. Ayrıca DWT algoritmasının pseudo kodu EK C'de verilmiştir. DWT algoritmasında kullanılan dalgacık fonksiyonu 2.5'deki gibidir.

$$W_{j,k}(t) = 2^{-j/2} W(2^{-j} t - k) \quad \textbf{(2.5)}$$

W, sürekli bir fonksiyon,

j, skala parametresi,

k, öteleme parametresidir (Haşiloğlu, 2001).

2.2.3. Matlab platformu

Matris laboratuvarı kısaltması olan MATLAB, dördüncü nesil bir programlama dili ve platformudur. Dünya üzerindeki birçok mühendis ve bilim adamının sistem ve ürün dizayn etmek ve analiz etmek için kullandıkları kullanışlı bir platformdur. Otomobil güvenlik, uzay mekikleri vb. oluşturulması için planlanan tüm sistem ve ürünlerin dizaynı ve simülasyonu üzerinde kullanılmaktadır (URL4). Sinyal ve görsel işlem, yapay zeka uygulamaları, derin-makine öğrenme uygulamaları, robotik dizayn ve iletişim sistemleri gibi birçok alanda aktif olarak kullanılmaktadır. Bilim insanlarının en önemli materyallerinden biri haline gelmiştir. MATLAB platformu matematiksel olarak matrisler üzerinden işlemler görebilmekte ve var olan veri kümlerinin bu matrisler üzerinden görselleştirilmesi ve çıkarımlar bulunmasında kolaylıklar sağlanılmasında en önemli faktördür. Cleve Moler adındaki New Mexico Üniversitesi Bilgisayar Bölüm Başkanı, 1970'li yıllarında sonunda MATLAB'ı geliştirmeye başladı. Bu bilim insanı önce LINPACK ve EISPACK adında iki program tasarlayarak uygulamalı matematik alanında öğrencilerine katkı sağlamayı amaçlamıştır. 1983 yılında Stanford Üniversitesinden Jack Little ile tanışmış ve daha sonrasında bu programdaki ticari potansiyeli gören Stece Bangert'in gruba katılması ile MATLAB programını ürün olarak sunan MathWorks şirketini kurmuşlardır. Program şimdiki hali ve yenilikleri ile günümüze ulaşmıştır. Günümüzde özellikle veri analizi ve resim işleme alanlarında oldukça popülerdir (URL5). Çalışma alanımız olan steganografi'nin MATLAB kullanımı oldukça avantajlıdır. Öncelikle sunulan ek paket programlar sayesinde birçok analiz türünü zaman harcamadan kullanabilir ve hızlı bir ilerleme kaydedilebilir. Bununla

birlikte MATLAB farklı programlama dilleri bilenlerin kendi bildikleri programlama dillerinde programlar yazmasına ve bunları MATLAB platformuna entegre etmelerine yazılımsal olarak izin vermektedir. Ayrıca öğrenciler için uyguladıkları indirimli ve deneme sürümlü kullanım politikaları ve açık kaynak kod içeren platform ve kütüphaneleri ile bilimsel açıdan kendini geliştirme isteğinde olan öğrencilerin tercih edebileceği bir uygulamadır. Bu tez çalışmasında MATLAB bir metod olarak seçilmiş ve uygulama aşamalarında MATLAB hakkında bilgi birikimi ve deneyim kazanılmıştır.

2.2.4. R programlama platformu

Steganografi'de kullanılan metodlar genellikle matrisler üzerinde çalışmakta ve görsel verilerin istatistiksel kıyaslanmasını ve incelenmesini içerdiği için veri inceleme alanında faliyet gösteren R programlama alternatif bir materyal olarak gösterilebilir. R programlama, Yeni Zellanda Auckland Üniversitesinden Ross Ihaka ve Robert Gentleman taradından çıkarılmış ve R geliştirme ekibi tarafından geliştirilmektedir. S programlama dilinin açık kaynaklı versiyonu olduğundan GNU S olarak da anılır. R açık kaynak kodlu bir yazılım olduğundan, ana geliştirme ekibi haricinde dünya üzerindeki bir çok bilgisayar mühendisinin oluşturduğu topluluk tarafından geliştirilmekte ve güncellenmektedir. R programlama komut arayüzü ve grafik arayüzünü birlikte kullanmaktadır. Bu yüzden ülkemizde kodlama ve bilgisayar yetileri çok kuvvetli olmayan kişilerce kullanımı zor olabilir. R programlama, MATLAB 'da olduğu gibi C, C++ ve Fortran yazılım dilleri ile ek kodlamalar yapmaya ve ana programa dahil etmeye izin vermektedir. Tamamen ücretsizdir ve ağırlıklı olarak istatistiksel incelemelere dayalı kütüphane ve fonksiyonlar içermektedir (URL6). Tezimizde R programlama kullanılmamıştır. Ancak neden MATLAB platformunu seçtiğimizin anlaşılması ve karşılaştırılmasının daha iyi yapılabilmesi için burada anlatılmaktadır.

2.2.5. Steganografi programları ve steganaliz yöntemleri

2.2.5.1. Steganografi programları

Steganaliz, tezimizin en başında bahsettiğimiz gibi steganografik sistemlere karşı geliştirilmiş, steganografik sistemlerin açıklarını bulmaya ve onları çözmeye çalışan steganografik bir sanat ve bilim dalıdır. Steganaliz steganografi ile birlikte büyür ve ilerler. Aralarındaki ilişki adeta bir yarış gibidir ve sürekli olarak bu iki bilim dalı

birbirini geçmeye çalışır. Steganalizin tek amacı steganografik iletinin içerisindeki gizli mesajı elde etmektir. Bunu yaparken steganografik resimi istatistiksel veya görsellik unsurlarına göre inceler. Bu incelemelere steganalizde atak denir. Atakları gerçekleştiren şahıslar ise steganalizci veya steganaliz uzmanı olarak adlandırılır.

Steganalizciler hedeflerine ulaşmak için farklı atak yöntemleri kullanırlar. Bunlardan bir tanesi Known Cover Attack, bilgi taşıdığı bilinen taşıyıcı objeye yapılan atak yöntemidir. Bu yöntemde steganaliz uzmanı, hali hazırda steganografik resim ve taşıyıcı resimin orijinal haline sahiptir. Bu iki resimi birbirleri ile kıyaslayarak aradaki farkları bulmaya çalışır. Bu karşılaştırmadan ortaya çıkan farklılıklar varsa not edilir. Bu notlar ışığında steganografik sistem çözülmeye uğraşılır.

Steganografik sistem çözüldükten sonra uygulanılan adımlar bir sıralamayla sistematize edilir ve bu işlemler sonucunda spesifik bir steganografi algoritmasına karşılık, onu çözecek steganaliz yöntemi oluşmuş olur (Challita ve Farhat, 2011).

Başka bir yöntem ise Blind Steganalysis, kör steganaliz olarak çevirebileceğimiz yöntemdir. Bu yöntemde steganaliz uzmanı, steganografi sistemi hakkında herhangi bir bilgi sahibi olmamakla birlikte, bir önceki yöntemin aksine steganografik resim bilinmeksizin yapılır. Chi-square, x^2-test gibi test yöntemleri kullanılarak ya da resim üzerine kesme, kırpma, yön ve doğrultu değiştirme, sıkıştırma gibi işlemler yapılır. Bu işlemler sonucunda resimdeki bozulmalar ve özellik vektöründeki değişimler gözlemlenerek taşıyıcı resimin steganografik içerip içermediği anlaşılmaya çalışılır (Challita ve Farhat, 2011).

Diğer bir yöntem ise, istatistiksel incelemeler yardımı ile steganografik iletilerin incelenmesidir. Bu yönteme örnek olarak Maximum Likelihood yöntemi gösterilebilir (Pfitzmann ve Westfeld, 2000). Tezimizin bu bölümünden sonra başlıca steganografi programları ve bu programlara karşı gerçekleştirilen steganaliz yöntemlerinden bahsedilecektir.

JSteg

Steganografi sistemi olarak halkın kullanımına açılan ilk sistemdir. Veri saklama işlemi LSB yöntemi kullanılarak yapılır. Bu sistemde DCT katsayıları LSB yöntemi mantığıyla mesaj verileri ile yer değiştirilir. Bu değişim esnasında düşük veya yüksek band'a veri

aktarımı önemsenmez. Mesaj 1 ve 0 bit'lerine dönüştürülür ve DCT frekans katsayılarına eklenerek tamamlanır. JSteg yönteminde, mesaj veya mesaj sıralaması şifrelenmez. Bu yüzden gizlenmiş mesaj üzerinde herhangi bir şüpheye kapılan analizci bozulmaları yakaladığı anda gizli mesajada ulaşabilir. LSB kullanımının kolay ve yaygın olmasından dolayı JSteg yöntemi halen günümüzde de yaygın olarak kullanılmaya devam etmektedir. Şifreli mesajın orijinal taşıyıcı resimine ulaşıldığı taktirde, histogram analizinden rahatlıkla gizli mesaja ulaşılabilir. $_X^2$ test yöntemi, gizli mesaja ulaşmamıza yardımcı olan bir diğer yöntemdir. Bu yöntem histogram analizine benzer bir analiz yöntemi izler. JSteg, JPEG resim objeleri üzerine uygulanmak için tasarlanmıştır ve JPEG objeleri veri diziliminde simetri içerirler. LSB yöntemi kullanılarak veri gömülümü gerçekleştiği zaman bu simetride bozulmalar meydana gelir. Dolayısıyla analiz eden yöntemler bu simetri bozukluğunu ararlar. JPEG içerisine sıkıştırma yapan JSteg yöntemi genel resime oranla %12'lik bir bozuluma kadar toleranslıdır. Bu oranın aşağısında kalan veri gömülümü işlemleri görsel ataklara karşı bağışıklığa sahiptirler. Bu görsel ataklar resim üzerinde yapılan işlemleri sembolize eder. Resim üzerinde kırpma, yön değiştirme, yüksek sıkıştırmaya tabi tutma gibi işlemlerle resim üzerindeki bozulumlara bakılır. Bu tarz ataklardan etkilenmeyen JSteg yöntemi, istatistiksel ataklara karşı yukarıda belirttiğimiz nedenden ötürü etkisiz kalmaktadır (URL7).

$| N_{2i} - N_{2i-1}| \geq |N^*_{2i} - N^*_{2i-1}|$ Bu formül yukarıdaki kısımlardan bahsettiğimiz piksel kıyaslama ve incelemeyi sembolize eden bir formuldür. "N" değeri "i" indek değerine bağlı olarak değişen pikseli sembolize eder. Mesaj gömülümü esnasında piksellerin renk olarak tuttuğu değerler değişir bu denklem ise değişimin miktarını ve dengesini ölçmektedir. N* değeri mesaj gömülümü gerçekleştikten sonraki objenin piksel değerini sembolize etmektedir (URL8).

OutGuess

Niels Provos tarafından geliştirilmiş bu sistem JSteg yönteminin gelişmiş bir üst versiyonu gibidir. Bu yöntemde JSteg yönteminden farklı olarak PRNG (Pseudo Random Number Generator) kullanılır. PRNG sistemi DCT katsayılarını veya özniteliklerini seçme işleminde kullanılır. Rastgele üretilen sayılar yardımıyla rastgele DCT katsayıları seçilir ve şifrelenmiş mesaj LSB yöntemiyle bu DCT değerleriyle değiştirilir.

Input: *message, shared secret, cover image*

Output: *stego image*

initialize PRNG with shared secret

while *data left to embed* ***do***

get pseudo-random DCT coefficient from cover image

if *DCT ≠ 0 and DCT ≠ 1* ***then***

get next LSB from message

replace DCT LSB with message LSB

end if

insert DCT into stego image

end while

Yukarıdaki pseudo kodda bulunan adımlar sırasıyla şöyledir;

İlk olarak girdi değerimiz belirtilir, bu da taşıyıcı resim, mesaj ve paylaşılan sır değerleridir. Sonrasında bu paylaşılan sır değeri ile rastgele sayı üretimi başlatılır. While döngüsünde belirtilen koşul değeri ise veri gömülümü gerçekleştirilecek, veri kaldığı sürece devam edilecektir demektir. While döngüsünün herbir adımında taşıyıcı resimden DCT katsayı/ortak etmen alınır. Bu değerin seçimi, rastgele üretilen sayının gösterdiği değerdir. Bu sayının 1 veya 0 değeri olmamasına özen gösterilir ve bunu kontrol eden bir "if" koşul komudu yerleştirilmiştir. DCT'den gelen her bir değer ile mesajdan LSB yöntemine göre bir bit çekilir ve piksel değeri ile yer değiştirilir. Tüm mesajın LSB ile DCT katsayılarıyla değişimi tamamlandıktan sonra steganografik öğemiz oluşmuş olur ve döngü tamamlanır.

Böylelikle JSteg yöntemindeki sıralı yer değiştirme ile simetri oluşturan ve farkındalığı kolaylaştıran bu dezavantajdan kurtulmuş olunur. Görsel ataklara karşı dayanıklı olmakla beraber son eklemelerle istatistiksel ataklara karşı dayanıklı bir hal almıştır. JSteg yönteminde kullanılan X^2 testlerden belirli koşullar altında etkilenmemektedir. Bu

koşullar veri gizleme sınırı kısıtlamalarıdır. JSteg yöntemine göre daha kısıtlı kapasitede veri saklama işlemi yapılabilir. Eğer bu sınır aşılırsa, sistemin güvenilir olduğu yanları düşer ve genel analizlere karşı duyarlı hale gelir. Veri saklama kapasitesinin düşük olması OutGuess yönteminin başlıca zaafiyetidir. Diğer bir zayıf noktası ise başlangıçta steganografi steganaliz ilişkisini kısımında bahsettiğimiz olaydan dolayı meydana gelen geliştirilmiş X^2 test yöntemidir. Başlangıçtaki testlerden geçebilen OutGuess yöntemi sonrasında geliştirilen bu testte yakalanabilmektedir. X^2 testinde algoritma birden fazla resimde tek bir alandaki bozulmaları test ederken genişletilmiş, X^2 testinde tek bir örnek resim üzerinde birden fazla alan kaydırılarak kontrol edilir. Bu yeni yöntem sayesinde rastgelelikle resimin içerisine karışık olarak eklenen mesaj ve onun sebebiyet verdiği bozulumlar bölge bölge taranarak tek tek bulunur ve açığa çıkarılır.

$$Y_i^* = \frac{n_{2i-1}+n_{2i}}{2} \quad \textbf{(2.6)}$$

Yukarıdaki 2.6 formülünde "n" değerleri "i" indeks değerine bağlı olarak değişen piksel değerlerinin yerini tutmaktadır. DCT katsayı veya ortak etmenlerinin aritmetik Mean ortalama değerlerini bulmaktansa, iki bağımsız ortak etmenin aritmetik ortalaması alınıyor. Yukarıda anlattığımız genişletilmiş X^2 testinin matematiksel formulü böylelikle tanımlanmıştır (URL9).

S-Tools

S-Tools Steganografi programı Andy Brown tarafından yapılmıştır. Benzer programların aksine birkaç farklı platform formatında veri saklama işlemi yapabilmektedir. Bu formatlar GIF, BMP ve WAV dosyalarıdır. 8 bit'lik veya 24 bit'lik kayıpsız veri saklama işlemi yapabilmektedir. Bu bit değişimi, taşıyıcı platform formatının ana renklerini oluşturan kırmızı, yeşil ve mavi renkler veya siyah beyaz olmasından kaynaklanan bir değişimdir. Veri saklama işlemini LSB algoritmasına göre yapar ve ayrıca şifreleme sistemide kullanır. Bu şifreleme sisteminin güvenlik anahtarınıda taşıyıcı resime LSB yardımıyla yerleştirir. Kullandığı şifreleme sistemleri DES, Data Encryption Standard, Veri Şifreleme Standartı, IDEA, International Data Encryption Algorithm, Uluslararası Veri Şifreleme Algoritması, MDC, Message Digest Cipher, Özet Mesaj Şifreleme ve TDES, Triple DES, Üçlü veya Üç kat Des Algoritması yöntemleridir. Bu program internetten bedava elde edilebilir. Dikkat edilmesi gereken

temel unsur, kullanılan taşıyıcı objelerin içerisine gömülecek mesajların boyutlarının taşıyıcıdan fazla olmaması durumudur. Her ne kadar sistemin bunları dikkate alarak düzeltmeler yaptığı söylenilse bile eşik değerinden fazla veri eklenmesi her zaman insan gözüyle olmasa bile analizler yardımıyla ortaya çıkma durumunu arttırmaktadır (URL10).

2.2.5.2. Görsel atak ve analiz yöntemleri

Görsel ataklardaki temel ölçüt birimi, taşıyıcı resim üzerine ekleme yapıldıktan sonra oluşan steganografik resimin bozulmalar içermemesidir. Bu bozulmalar en öncelikli olarak insan gözüyle görülmemeli, bunun için parlaklık değerleri ile değişim yapılmamalıdır. İkinci önemli mevzu olarak, analiz yöntemleri ile fark edilemeyecek konumda bulunmasıdır.

Analiz programlarının çokça gelişmiş olması bir dezavantaj gibi görünse de, ileti kanalındaki veri aktarım çokluğu ve gürültü etmeninin iletiye etkisi göz önünde bulundurularak belirli bir oranda veri gizlenmesi sağlanılabilir. Önemli olan bu eşik değerinin aşılmaması durumudur. Önceki yıllarda parlaklık değerlerinin dijital resim içerisinde tamamiyle rastgele, dağınık olduğu ve bu yüzden LSB yöntemi ile değişime tabi tutulabileceği sunulmuştur. Ancak yapılan çalışmalar sonrasında bunun yanlış olduğu ispatlanmıştır (Pfitzmann ve Westfeld, 2000).

Steganaliz uzmanları görsel açıdan bir analiz ya da atak yapacakları zaman öncelikli olarak şüpheli resimin orijinal halini elde etmeye çalışır. Daha sonrasında orijinal hali ile veri gizlenmiş hali karşılıklı olarak kıyaslanılır. Görsel bozulumlar çeşitli programlarla test edilir. Analizler sonucunda bariz bir bozulumaya rastlanılmadığı taktirde, resim üzerinde yüksek veri sıkıştırması, kırpma, yön ve doğrultularını değiştirme gibi işlemlerle iki resimin üzerinde meydana gelebilecek bozulmalar test edilir. İki resimin birbirine farklı bozulmalar göstermesi durumunda, analiz uzmanı şüpheli resimde farklı ve aykırı bozulmaların olduğu kısımlarda veri taraması yapmaya başlayabilir.

Son dönemlerdeki çalışmalarda, gizli mesaj şifrelenip taşıyıcı resim üzerinde şifrelenmiş bit bloğuna benzerlik gösteren yerler ile değiştirilir ve şifre anahtarı resim içerisinde belirli bir bölgeye gizlenir. Bu durumda analizcinin şifreli mesajın yerini ilk aşamada bulması zorlaşır. Ancak şifre anahtarının bozuluma sebebiyet verdiği blok veya bölüm

elde edilebilir ise mesaja ulaşmak daha kolay olur. Çünkü bu tarz uygulamalarda anahtar veri bloğunun içerisine aynı zamanda verinin yer aldığı koordinatlarda eklenir. Önceki çalışmalarda gizli anahtar verilerinin resim içerisine rastgele olarak dağıtılmasının güvenliği arttıracağı bir fikir gibi görülüp uygulansada, araştırmalar sonucu benzer veya yakın veri bloklarında çiftler halinde saklanmasının daha az bozuluma ve analiz dalgalanmalarına sebebiyet verdiğine, dolayısıyla daha güvenli olduğu kanıtlanmıştır.

Steganalizcilerin yol haritası öncelikle taşıyıcı ortam öğesine saldırmaktır. Bu objenin filtrelemelere ve değişimlere vereceği tepkiler steganalizci tarafından gözlemlenir ve varsa orijinal hali ile kıyasa tabi tutulur. Değişimlerden kasıt, renkli bir resimin siyah beyaza, siyah beyaz bir resimin ise renkli bir resime çevirilmesi ve daha sonrasında bunların veri gizlediğinden şüphelenilmeyen ve aynı uygulamalara tabi tutulan objelerle kıyaslanmasıdır. Analizler sonucunda bozulmaların görüldüğü bölgeler muhtemel veri bölgeleridir. Bu bölgeler çıkarılarak ayrıntılı olarak incelenir. Sonuçta varsa şifrelemeler çözülmeye çalışılarak asıl mesaja ulaşılır (Denemark ve Fridrich, 2015).

2.2.5.3. İstatistiksel atak ve analiz yöntemleri

İstatistiksel tabanlı ataklar veya analizler uzman kişinin şüphelendiği objenin bulunması, bulunan objenin uzay-piksel tabanlı gösterimden frekans tabanlı gösterime çekilmesi ve zaman, olay ve frekans tabanlı incelemelerle bozulumların bulunması ve en sonunda bozulum gösteren yerler ve bunların periodik olarak tekrarlanması gibi emareler sonucunda mesajın yerinin ve içeriğinin saptanması ile tamamlanır. Daha önceki bölümlerde de anlattığımız gibi frekans tabanlı veri gömülüm işlemleri, LSB gibi uzay tabanlı en basit bit yer değişimine dayalı sistemlerden daha güvenilirdir. Dezavantajları, daha az veri gönderim kapasitesi, yavaş çalışması ve karmaşık olmasıdır.

Bu sistemler frekanslar ve frekans band'ları üzerinden veri aktarımı sağlar. Analiz aşamaları tekrar bu platformlar üzerinde olur. Şüphelenilen resim, frekans tabanına tekrar dönüştürülüp analize tabi tutulduğunda, tahmini veya benzer resimin frekans değerleri ile kıyaslamaya başlanılır. Frekans verilerindeki periodik bozulmalar incelenir.

Veri aktarım esnasında ve kanalda veri aktarımı esnasında bozulmalar meydana gelebilir. Ancak bunların periodik olması, içerisinde gizli bir mesaj olabileceği ihtimallerini arttırır ve Chi-square atağı denilen yöntemin mantığında bu yöntem yer

almaktadır. PoV, Pair of Values, denilen değer çiftleri olarak tercüme edebileceğimiz bu değer veri bloğundaki tek ve çift rakamlı satır ve sütünların değerlerinin eş olması durumudur. Bu eşler belirli benzerlikler gösterilirler ve bu benzerliklerin bozulum gösterdiği durumlar analiz yönteminin temel başlangıcıdır (URL11).

2.2.6. Steganografi performans parametreleri

Steganografik algoritmaların performansları, gizli mesajı içerisine sakladığımız steganografik resim ve bu resimin içerisine mesaj iletisi eklenmeden önceki hali olan taşıyıcı resimin karşılaştırılması ile belirlenir. Bu karşılaştırmaya dayalı analiz ise bazı metamatiksel parametrelerin bulunması ile tamamlanmış olur.

Bu parametrik değerler; PSNR, Peak Signal to Noise Ratio, MSE, Mean Squared Error, NCC, Normalized Cross-Correlation, AD, Average Difference, SC, Structural Content, MD, Maximum Difference ve NAE, Normalized Absolute Error'dür. Bu parametreler taşıyıcı obje ile steganografik obje arasındaki farkı değerlendirmemizi sağlayan matematiksel fonksiyonlar içerir.

2.2.6.1. MSE ortalama kare hatası

MSE, Ortalama Kare Hatası, genellikle sinyallerde iki sinyalin birbirilerine olan benzerliklerini ölçmek için kullanılan bir yöntemdir. Steganografide buna benzer olarak taşıyıcı resim ile steganografik resimin benzerliklerini ölçmek için kullanılır. Aşağıdaki 2.7 formulüne göre MSE, benzerlik bulmaya çalışır (Dhawale, Hegadi ve Jambhekar, 2014).

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad \textbf{(2.7)}$$

Formuldeki;

- I(i,j) değeri orijinal taşıyıcı resimi temsil etmektedir.
- K(i,j) değeri steganografik resimi temsil etmektedir.
- m,n değerleri ise resimin boyutlarını göstermektedir.

Formulün sonucunda eğer MSE değeri düşük ise bu benzerliğin yüksek olduğunu ve algoritmanın başarılı olduğunu göstermektedir. Tersi durumlarda ise algoritmamız başarısız sayılacaktır.

2.2.6.2. PSNR tepe sinyali gürültü oranı

PSNR, Yüksek Sinyalin Gürültüye Oranı, logaritmik desibel ölçütü ile tanımlanır, ölçümlendirilir. Steganografik resimin görüntüsünün bozulumuna sebebiyet veren en üst seviye sinyal ile bozuluma sebebiyet veren gürültü değerinin arasındaki orana PSNR denir. Düşük PSNR oranı ölçümü görsel kalitede düşüklük ve bilgi sıkıştırmada kalitesizlik anlamına gelir. Tersine durumda yani, PSNR oranının yüksek ölçüldüğü durumda resim kalitesi, sıkıştırması ve yeniden yapılandırılmasının kaliteli ve başarılı olduğu anlaşılır. PSNR değeri aşağıdaki 2.8'deki formul ile hesaplanır (Dhawale, Hegadi ve Jambhekar, 2014);

$$\text{PSNR} = \log_{10}\left(\frac{MAX_1^2}{MSE}\right) \quad \textbf{(2.8)}$$

PSNR formulü görüldüğü üzere başka bir ölçüm parametresi olan MSE değerine bağlı olarak hesaplanır. MAX_I değeri var olan en yüksek piksel değeridir.

3. ANALİZ

Bir önceki bölümde bahsedilen 2.2.2.2. Ayrık Kosinüs Dönüşümü, 2.2.2.3. Hamming Kodlaması, 2.2.2.4. Ayrık Dalgacık Dönüşümü, 2.2.6.1.MSE ve 2.2.6.2.PSNR senaryoları 3.1. DCT Steganografik Resim Analizleri ve 3.2. DWT Steganografik Resim Analizleri bölümlerinde gösterilen resimler üzerinde doğrudan ve dolaylı olarak kullanılmıştır. 512x512 boyutundaki Şekil 2.1-2.7 aralığındaki taşıyıcı resimlere DCT ve DWT metotlarında Şekil 2.8 ve Şekil 2.9'da verilen 40KB büyüklüğündeki gizli mesajlar yüklenmiştir. Yüklemeler sonrasında yeni oluşan siyah beyaz steganografik resimler ve orijinal halleri arasında kıylaslamalar yapılmıştır.

Elde ettiğimiz PSNR değerlerinin başarısı yorumlanırken, çalışmamıza benzer bir yüksek lisans tezi olan, "DCT, DWT, DFT ve LSB algoritmaları kullanılarak medikal resimlerde dijital damgalam" çalışmasında araştırmacı arkadaşımız, kullandığı görsellerin PSNR değerlerini hesaplamış ve elde ettiği sonuçlar bizim çalışmamızda elde ettiğimiz sonuçlara büyük benzerlikler göstermiştir (Kaya, 2015).

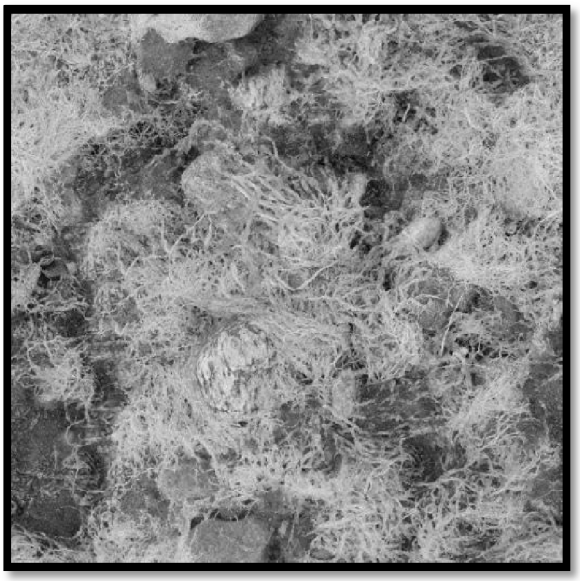
Tezimizde kullandığımız ve içerisine veri gizlediğimiz Şekil 2.7'deki resim ile alakalı Yüksek Lisans Tezinde benzer bir çalışma yapan Selçuk Üniversitesinden Barış Demirci, tezinin 17. sayfasında bizim tezimizdeki Şekil 2.7'deki aynı resime veri gizlemiş ve sonuç olarak elde ettiği değerler, bizim tezimizde bulduklarımızla paralellik göstermiştir. Hem kendi tezimizdeki sonuçlarda, hemde araştırmacı arkadaşımızın tezindeki sonuçlarda elde edilen sonuçlar, görüntüde çok ufak farklılıklar oluştuğunu göstermiş ve birbirine paralellik göstermiştir (Demirci, 2016).

Son olarak tezimizde ele aldığımız konular ve açıklanan başlıklarda verilen bilgilerin tutarlılığını görebilmek açısından, Andaç Şahin'in doktora tezi olan; "Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri" adlı çalışması incelenmiştir. Yapılan incelemeler sonucunda öncelikle Şahin'in doktora tezinde ele aldığı konular içerik olarak büyük benzerlik göstermiştir. Çalışmasında

bulunan alt başlıklar incelendiğinde, verilen bilgilerin tezimizde yaptığımız literatür araştırmaları sonucu elde ettiğimiz bilgilerle büyük benzerlik gösterdiği görülmüştür. Kullandığımız materyal ve metodların seçiminde vermiş olduğumuz kararların doğruluğunun teyit edilmesi açısından çok faydalı bir kıyaslama olmuştur (Şahin, 2007).

3.1. DCT Steganografik Resim Analizleri

Bu bölümde DCT algoritması, taşıyıcı resimler olan Şekil 2.1-2.7 aralığındaki orjinal resimlere incelenmek üzere tek tek uygulanmıştır. Uygulama sonucunda Şekil 3.1-3.7 arasındaki görüntüler elde edilmiştir. Bu görüntülere DCT ile EK A'da belirttiğimiz 40 KB'lık gizli mesaj olan metin dosyası gizlenmiştir. Oluşan görüntülerin PSNR değerleri hesaplanmıştır. Ayrıca EK E'de bulunan EK A'dan farklı metin dosyası olan gizli mesajı, çalıştığımız orjinal görüntüler olan Şekil 2.1-2.7 arasındaki görüntülere DCT algoritması ile gizlenmiştir. Oluşan görüntüler EK F'de verilmiş olup, PSNR değerleri hesaplanmıştır. Aşağıda Şekil 3.1-3.7 arasındaki verilen görüntüler; EK A'da bulunan metin dosyasının gizlendiği DCT steganografik resimleridir.



Şekil 3.1 : DCT Steganografik Resim 1

Şekil 3.2 : DCT Steganografik Resim 2

Şekil 3.3 : DCT Steganografik Resim 3

Yukarıdaki Şekil 3.1-3 aralığında verilen görüntüler, DCT algoritması uygulanmış taşıyıcı resimleri göstermektedir. Bu görüntülerin PSNR değerleri sırasıyla şöyledir: 38,1549 dB, 36,0315 dB, 36,8739 dB.

Şekil 3.4 : DCT Steganografik Resim 4

Şekil 3.5 : DCT Steganografik Resim 5

Şekil 3.4 ve Şekil 3.5'de verilen görüntüler, DCT algoritması uygulanmış taşıyıcı resimleri göstermektedir. Bu görüntülerin PSNR değerleri sırasıyla şöyledir: 40,1903 dB ve 40,4821 dB.

Şekil 3.6 : DCT Steganografik Resim 6

Şekil 3.7 : DCT Steganografik Resim 7

Yukarıdaki Şekil 3.6 ve Şekil 3.7'de verilen görüntüler, DCT algoritması uygulanmış taşıyıcı resimleri göstermektedir. Bu görüntülerin PSNR değerleri sırasıyla şöyledir: 40,3033 dB ve 40,4352 dB.

DCT algoritması uygulandıktan sonra elde edilen yukarıdaki görüntüler çıplak gözle incelendiğinde bir fark görülmemektedir. Bu uygulamanın sonucunda hesapladığımız PSNR değeri ayrıca Çizelge 3.1'de verilmiştir.

Çizelge 3.1 : DCT PSNR Değerleri 1

DENEMELER	DCT-PSNR
DENEME1	38,1549 dB
DENEME2	36,0315 dB
DENEME3	36,8739 dB
DENEME4	40,1903 dB
DENEME5	40,4821 dB
DENEME6	40,3033 dB
DENEME7	40,4352 dB

DCT algoritmasını aynı EK A'da izlediğimiz adımları izleyerek EK E'de bulunan gizli mesaj olan metin dosyası için de uyguladık. Elde ettiğimiz görseller EK F'de verilmiştir. Oluşan görüntülerin PSNR değerleri Çizelge 3.2'de verilmiştir. Bu uygulamada oluşan görüntüler incelendiğinde herhangi bir tespit farklılık görülmemiştir. Ayrıca Şekil 3.1-3.7 arasında bulunan görüntülerden EK F'de bulunan görüntüleride ayırt edebilmek imkansızdır.

Çizelge 3.2 : DCT PSNR Değerleri 2

DENEMELER	DCT-PSNR
DENEME1	38,1530 dB
DENEME2	36,0442 dB
DENEME3	36,8705 dB
DENEME4	40,2141 dB
DENEME5	40,4835 dB
DENEME6	40,3021 dB
DENEME7	40,4373 dB

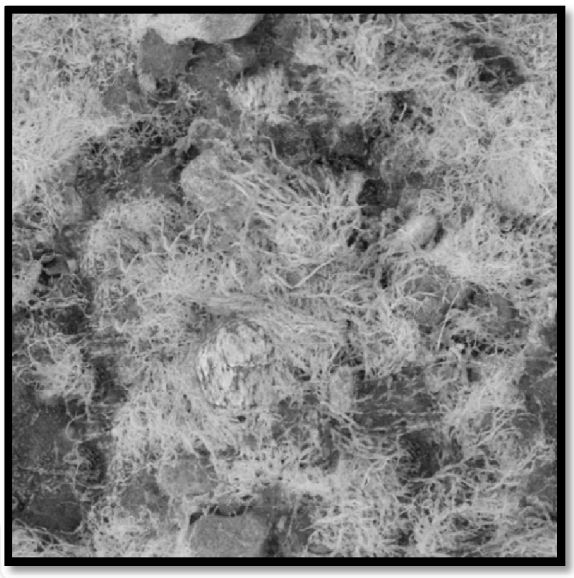
Çizelge 3.1 ve Çizelge 3.2'de elde ettiğimiz PSNR değerlerini incelediğimizde, her iki gizli mesajın Şekil 3.1-3.7 arasındaki görüntülere uygulanması sonucu elde edilen PSNR değerlerinin, puan olarak aynı, ondalık kısımda ise çok ufak farklılıklar gösterdiğini görüyoruz. Her iki çizelgede de bulunan DENEME1 sonuçlarına bakarsak; 38,1549 dB-38,1530 dB gibi büyük bir benzerlik görüyoruz. En aykırı olduğu durum olan DENEME4'de ise elde edilen değerler 40,1903 dB-40,2141 dB olarak karşımıza çıkıyor. Her iki çizelgeyi kendi içinde incelediğimizde, sırasıyla 5, 7 ve 6. denemelerde kullanılan taşıyıcı resimlerin, her iki çizelgede de yapılan çalışmalar sonucunda elde edilen PSNR değerlerine göre, diğer kullanılan taşıyıcı resimlere oranla daha başarılı veri gizlendiğini görüyoruz.

Sonuç olarak bütün demelerde elde edilen PSNR değerleri, elde edilen başarının benzerliği açısından paralellik göstermektedir. Ancak elde edilen bu PSNR değerleri başarılıdır ancak çok yüksek değerler değildir. Çünkü PSNR değeri ne kadar yüksekse, oluşan görüntülerin kalitesi o kadar yüksektir. Bu açıdan bakıldığında DCT performans ve verimini DWT ile kıyaslarken dikkat edeceğimiz temel değişken PSNR değerlerindeki başarı oranlarıdır. Çünkü her iki algoritma 40 KB'lık veriler ile denenmiştir. Burada önemli olan gizlenilen verinin boyutudur. DCT ve DWT algoritmalarının bu verileri gizlemedeki başarıları, iki algoritmanın karşılaştırılmasındaki en önemli faktördür.

3.2. DWT Steganografik Resim Analizleri

Bu bölümde kullandığımız DWT algoritması, taşıyıcı resimler olan Şekil 2.1-2.7 aralığındaki orjinal resimlere, DWT algoritmasının başarısını incelemek için tek tek uygulanmıştır. Uygulama sonucunda Şekil 3.8-3.14 arasındaki görüntüler elde edilmiştir. Bu görüntülere DWT ile Şekil 2.8'de belirttiğimiz 40 KB'lık gizli mesaj olan görüntü gizlenmiştir. Oluşan görüntülerin PSNR değerleri hesaplanmıştır. Ayrıca Şekil 2.9'da bulunan ve Şekil 2.8'den farklı olan gizli mesajımızı, çalıştığımız orjinal görüntüler olan Şekil 2.1-2.7 arasındaki görüntülere DWT algoritması kullanılarak gizlenmiştir. Oluşan görüntüler EK G'de verilmiş olup, PSNR değerleri hesaplanmıştır.

Aşağıda Şekil 3.8-3.14 arasındaki verilen görüntüler; Şekil 2.8'de bulunan gizli mesajın gizlendiği DWT steganografik resimleridir. Aşağıdaki Şekil 3.8 ve Şekil 3.9'da verilen görüntülerin hesaplanmış PSNR değerleri sırasıyla şöyledir: 50,1016 dB ve 51,3603 dB.



Şekil 3.8 : DWT Steganografik Resim 1

Şekil 3.9 : DWT Steganografik Resim 2

Şekil 3.10 : DWT Steganografik Resim 3

Şekil 3.11 : DWT Steganografik Resim 4

Yukarıdaki Şekil 3.10 ve Şekil 3.11'de verilen görüntülerin DWT algoritması uygulandıktan sonra hesaplanmış PSNR değerleri sırasıyla şöyledir: 51,4908 dB ve 50,2364 dB.

Şekil 3.12: DWT Steganografik Resim 5

Şekil 3.13 : DWT Steganografik Resim 6

Şekil 3.14 : DWT Steganografik Resim 7

Yukarıdaki Şekil 3.12-3.14'de verilen görüntülerin DWT algoritması uygulandıktan sonra hesaplanmış PSNR değerleri sırasıyla şöyledir: 51,1106 dB, 51,2060 dB ve 50,7428 dB. Sonuç olarak DWT algoritması uygulandıktan sonra elde edilen tüm görüntüler yukarıda verilmiştir. Bu görüntülerin incelenmesi sonucunda gözle görülebilen herhangi bir farklılık tespit edilememiştir. DWT algoritmasının uygulanması sonucunda hesapladığımız PSNR değerleri aşağıdaki Çizelge 3.3'de verilmiştir.

Çizelge 3.3 : DWT PSNR Değerleri 1

DENEMELER	DWT-PSNR
DENEME1	50,1016 dB
DENEME2	51,3603 dB
DENEME3	51,4908 dB
DENEME4	50,2364 dB
DENEME5	51,1106 dB
DENEME6	51,2060 dB
DENEME7	50,7428 dB

Yukarıda açıkladığımız adımların aynısı, Şekil 2.9'da gizli mesajımız olan görüntü verimiz için de uygulanmıştır. DWT algoritması, elimizdeki orijinal görüntüler olan

Şekil 2.1-2.7 arasındaki görüntülere uygulanmış ve elde edilen görüntüler EK G'de verilmiştir. Oluşan görüntülerin incelenmesi sonucunda herhangi bir farklılık tespit edilememiştir. Bu görüntülerin PSNR değerleri hesaplanmış ve aşağıdaki Çizelge 3.4'de verilmiştir.

Çizelge 3.4 : DWT PSNR Değerleri 2

DENEMELER	DWT-PSNR
DENEME1	45,9511 dB
DENEME2	47,2097 dB
DENEME3	47,3403 dB
DENEME4	46,0858 dB
DENEME5	46,9600 dB
DENEME6	47,0555 dB
DENEME7	46,5923 dB

DWT algoritmasının Şekil 2.8 ve Şekil 2.9'da bulunan gizli mesaj görüntülerini, elimizdeki orjinal görüntülere gizlemesi sonucu elde edilen PSNR değerleri yukarıda hesaplanmıştır. Elde edilen PSNR değerleri birbirlerine yakındır. Ortalama olarak her iki denemede elde edilen PSNR değerleri arasında 4 puanlık bir fark vardır. Bu sonuçlar doğrultusunda, Şekil 2.8'de bulunan gizli mesajımızın Şekil 2.9'da bulunan gizli mesaja oranla daha başarılı bir şekilde gizlendiği görülmüştür. Aynı şekilde DWT kalitesinin belirlenmesinde kullandığımız PSNR değerinin yüksek olmasıyla doğru orantılı olarak kalitesininde artmasından dolayı, Şekil 2.8'de bulunan gizli mesajımızın Şekil 2.9'da bulunan gizli mesaja göre kalitesi daha yüksektir. Yukarıda verilen iki çizelgenin kendi içinde incelenmesi sonucunda sırasıyla 3, 2 ve 6. denemelerinde kullanılan taşıyıcı resimlerin, yapılan çalışmalar sonucunda elde edilen PSNR değerlerine göre hazırlanmış çizelgelerde görüldüğü üzere, 3, 2 ve 6. taşıyıcı resimlerde diğer kullanılan taşıyıcı resimlere oranla daha başarılı veri gizlendiğini görüyoruz.

Sonuç olarak elde ettiğimiz görüntüleri ve PSNR değerlerini inceleyecek olursak; elde ettiğimiz her iki denemedeki görüntülerin, hem olarak bir farklılık göstermediğini hemde iki farklı mesajı taşıyan aynı görüntülerin birbirlerinden herhangi bir şekilde ayırt edilemediğini görürüz. Elde edilen PSNR değerleri gayet başarılıdır ancak çok yüksek değerler değildir. DCT ile kıyaslama yaparken kullanacağımız bu değerler, DCT'ye oranla daha yüksektir. Uygulama aşamalarında, her iki algoritmaya 40 KB'lık veriler

gizlenmiş ve farklı PSNR değerleri elde edilmiştir. Çıkan sonuçlar üzerinden 4.1. Sonuç bölümünde DCT ve DWT algoritmalarının kıyaslamaları yapılacaktır.

4. SONUÇ VE ÖNERİLER

4.1. Sonuç

Tezin analiz bölümünde DCT ve DWT algoritmaları, elimizdeki orjinal veriler olan; Şekil 2.1-2.9 arasındaki taşıyıcı görüntüler ve gizli mesajlar ile EK A ve EK E'de bulunan gizli mesajlar üzerinde tek tek denenerek PSNR değerleri hesaplanmıştır. Elde ettiğimiz tüm PSNR değerleri 30-50 dB aralığındadır. Değerlerimiz bu aralıkta olması, çalışmamız sonucunda elde ettiğimiz sonuçların, genel kabul görmüş başarı aralığında bulunduğunu göstermektedir.

DCT uygulamasında kullanılan taşıyıcı resimlerin işlenmesi sonucu elde edilen PSNR değerleri Çizelge 3.1 ve Çizelge 3.2'de incelendiğinde, her iki çizelge için de 5, 7 ve 6. denemelerdeki taşıyıcı resimlerin veri gizlemede kullanılan diğer taşıyıcı resimlere kıyasla daha başarılı sonuçlar verdiği görülmüştür. DCT'de elde edilen sonuçlar aşağıdaki gibi sıralanabilir:

Şekil 2.1'de bulunan orjinal resim öncelikle DCT algoritmasında denenmek amacıyla ele alınmıştır. Bu görüntünün içine EK A'da bulunan gizli mesaj, yani metin dosyası gizlenmiştir. Elde edilen PSNR değeri: 38,1549 dB olmuştur. Oluşan görüntü Şekil 3.1'de verilmiştir. Yine Şekil 2.1'de bulunan orjinal resimimize bu sefer EK E'de bulunan gizli mesaj DCT algoritmasıyla gizlenmiştir. PSNR değeri olarak 38,1530 dB hesaplanmıştır. Oluşan görünyü EK F'de verilmiştir. Bu iki durumda ortaya çıkan değerler birbirlerine çok yakın olup EK A için yapılan çalışma daha başarılı olmuştur. Çünkü PSNR değeri ile algoritmanın başarısı doğru orantılıdır.

Şekil 2.2'de bulunan orjinal resimimiz incelenmek için ele alınmıştır. Bu görüntüye DCT algoritmasıyla, EK A'da bulunan gizli mesajımız olan metin dosyası gizlenmiştir. Elde ettiğimiz PSNR değeri 36,0315 dB olmuştur. Oluşan görüntümüz ise Şekil 3.2'de verilmiştir. Oluşan görüntü görsel olarak incelendiğinde herhangi bir değişiklik görülmemiştir. Yine Şekil 2.2'de bulunan orjinal resimimize, EK E'de bulunan gizli

mesajı gizlemek amacıyla DCT algoritması uygulanmıştır. Oluşan görüntü EK F'de verilmiştir. Elde ettiğimiz PSNR değeri 36,0442 dB olmuştur. Bu görünütü görsel olarak incelendiğinde herhangi bir farklılık tespit edilememiştir. Elde edilen PSNR değerleri incelendiğinde Şekil 2.2 için en verimli DCT denemesinin, EK E'de bulunan gizli mesaj ile yapıldığı görülmüştür.

Şekil 2.3'de bulunan orjinal resimimiz incelenmek üzere ele alınmıştır. Görüntü DCT algoritmasına EK A'da bulunan gizli mesaj ile işleme sokulmuş ve mesaj gizlenmiştir. Bu işlem sonucunda oluşan görüntü Şekil 3.3'de verilmiştir. Elde ettiğimiz görüntünün görsel olarak incelenmesinde herhangi bir farklılığa rastlanmamıştır. Bu işlem sonucunda elde ettiğimiz PSNR değeri 36,8739 dB olmuştur. Aynı işlemler EK E'de bulunan gizli mesajımız ile Şekil 2.3'de bulunan orjinal resmimize uygulanmıştır. Oluşan görüntü EK F'de verilmiştir. Görüntü görsel olarak incelendiğinde gizli mesajı tespit edebileceğimiz herhangi bir değişiklik fark edilmemiştir. Elde ettiğimiz PSNR değeri 36,8705 dB olmuştur. PSNR değerlerine göre bir kıyaslama yaptığımızda EK A'da bulunan gizli mesaj ile yapılan DCT gizlemesinin daha başarılı olduğu görülmektedir.

Şekil 2.4'de bulunan orjinal resimimiz DCT algortimasıyla incelenmek üzere ele alınmıştır. EK A'da bulunan gizli mesaj DCT algoritması sayesinde Şekil 2.4'de bulunan resime başarı ile gizlenmiştir. Oluşan görüntü incelendiğinde herhangi bir fark edilirlik söz konusu değildir. Elde ettiğimiz yeni görüntü Şekil 3.4'de verilmiştir. Yapılan hesaplamalarda elde edilen PSNR değeri 40,1903 dB olmuştur. Şekil 2.4'de bulunan resimimizin, EK E'de bulunan gizli mesajımız ile DCT algoritmasına sokulup, incelenmesi sonucunda PSNR değeri hesaplanmıştır. Oluşan görüntü incelendiğinde hiçbir farklılık görülememiştir. Elde edilen görüntü EK F'de verilmiştir. Hesaplanan PSNR değeri 40,2141 dB olmuştur. Bu hesaplamalar sonucu elde edilen PSNR değerlerine göre EK E ile yapılan DCT çalışması daha başarılı olmuştur.

Şekil 2.5'de bulunan orjinal resimimiz incelenmek üzere ele alınmıştır. Bu görüntüye DCT algoritmasında EK A'da verdiğimiz gizli mesaj olan metin dosyası gizlenmiştir. Gizleme işlemi sonucunda oluşan görüntü Şekil 3.5'de verilmiştir. Görüntünün görsel olarak incelenmesi sonucu herhangi bir değişim fark edilmemiştir. PSNR değeri 40,4821 dB olarak bulunmuştur. EK E'de bulunan gizli mesajımızın Şekil 2.5'de DCT algoritması

ile saklanması sonucunda EK F'de verilen görüntü elde edilmiştir. Bu görüntü incelendiğinde herhangi bir farklılığa rastlanılmamıştır. Oluşan görüntünün PSNR değeri 40,4835 dB olarak hesaplanmıştır. DCT algoritması ile gizlenen mesajlarımızın her iki görüntü üzerinde elde ettiği PSNR başarısı incelendiğinde EK E'de bulunan gizli mesajımızın daha başarılı bir şekilde gizlendiği görülmektedir.

Şekil 2.6'da bulunan orjinal resimimiz DCT algoritmasında incelenmek üzere ele alınmıştır. EK A'da bulunan metin dosyamız gizlenecek mesaj olarak kullanılmıştır. Gizleme işleminin DCT algoritması ile gerçekleştirilmesi sonucunda oluşan görüntü Şekil 3.6'da verilmiştir. Bu görüntü incelendiğinde herhangi bir farklılık tespit edilememiştir. Görüntünün PSNR değeri 40,3033 dB olarak hesaplanmıştır. EK E'de bulunan gizli mesajın DCT algoritması ile Şekil 2.6'da bulunan orjinal resime gizlenmesi sonucu oluşan görüntü EK F'de verilmiştir. Görüntünün görsel olarak incelenmesi sonucu herhangi bir değişime rastlanılmamıştır. Elde edilen her iki gizli mesaj için PSNR değerleri karşılaştırıldığında EK A'da ki mesajın daha başarılı bir şekilde gizlendiği görülmüştür.

Şekil 2.7'de bulunan orjina resim incelenmek üzere ele alınmıştır. Bu görüntüye DCT algoritması ile EK A'da bulunan gizli mesaj saklanmıştır. Oluşan görüntü incelendiğinde herhangi bir farklılık görülmemiştir. Oluşan görüntü Şekil 3.7'de verilmiştir. Görüntünün hesaplanan PSNR değeri 40,4352 dB'dir. EK E'de bulunan metin dosyası olan gizli mesajımız için de aynı adımlar uygulanmıştır. Şekil 2.7'nin DCT algoritması ile EK E'de bulunan gizli mesajın saklanması sonucu EK F'de verilen görüntü elde edilmiştir. Bu görüntü incelendiğinde herhangi bir farklılık görülmemiştir. Oluşan görüntünün hesaplanan PSNR değeri 40,4373 dB olmuştur. Her iki çalışmada da elde edilen PSNR değerleri karşılaştırıldığında EK E'de bulunan gizli mesajın daha başarılı bir şekilde gizlendiği görülmüştür.

DCT algoritması ile yapılan ve iki metin dosyasının gizli mesaj olarak kullanıldığı çalışmalarda elde edilen görüntülerin PSNR değerleri birbirlerine benzerlik göstermektedir. Her iki gizli mesaj için de elde edilen başarılar neredeyse aynıdır. Bu açıdan bakıldığında DCT algoritmasının 40 KB'lık metin verilerini gizlerken göstermiş olduğu başarının istikrarlı olduğu söyleyebilir. Tezin 2.2.6.2. bölümünde PSNR

değerleriyle ilgili ayrıntılar sunulmuştur. Bu bilgilere göre düşük PSNR değerleri, kullanılan yöntemin başarı oranındaki düşüklüğü göstermektedir. Her ne kadar elde ettiğimiz rakamlar birbirlerine çok yakın da olsa, yukarıda yapılan açıklamalarda hangi gizli mesajın daha iyi gizlendiği, tezin 2.2.6.2. bölümünde belirttiğimiz bilgiler ışığında açıklanmıştır.

DWT algoritmasının uygulanmasında kullanılan taşıyıcı resimlerin işlenmesi sonucu elde edilen PSNR değerleri Çizelge 3.3 ve Çizelge 3.4'de incelendiğinde, her iki çizelge için de sırasıyla 3, 2 ve 6. denemelerdeki taşıyıcı resimlerin veri gizlemede kullanılan diğer taşıyıcı resimlere kıyasla daha başarılı sonuçlar verdiği görülmüştür. DWT algoritması ile elde edilen sonuçlar aşağıdaki gibi özetlenebilir:

Şekil 2.1'de bulunan orjinal resim incelenmek üzere ele alınmıştır. Bu görüntü içine Şekil 2.8'de bulunan gizli mesaj gizlenmiştir. Gizleme işlemini yapmak için DWT algoritması kullanılmıştır. Elde edilen görüntü Şekil 3.8'de verilmiştir. Bu görüntünün incelenmesi sonucunda gözle görülebilecek herhangi bir değişim tespit edilmemiştir. Görüntünün hesaplanan PSNR değeri 50,1016 dB olmuştur. Şekil 2.1'de bulunan resimimiz yine incelenmek üzere ele alınmış ve DWT algoritması ile içerisine Şekil 2.9'da bulunan gizli mesajımız yüklenmiştir. Gizli mesajın yüklenmesi sonucu oluşan görüntü EK G'de verilmiştir. Bu görüntünün incelenmesi sonucunda hiçbir farklılığa rastlanılmamıştır. Elde edilen bu görüntünün PSNR değeri 45,9511 dB olarak hesaplanmıştır. Yapmış olduğumuz DWT algoritması ile veri gizleme sonucunda elde edilen PSNR değerleri üzerinden Şekil 2.8'de bulunan gizli mesaj daha başarılı bir şekilde gizlenmiştir.

Şekil 2.2'de bulunan orjinal resim DWT algoritması ile incelenmek üzere ele alınmıştır. Bu görüntünün içine gizlenmesi amacıyla Şekil 2.8'de bulunan gizli mesaj DWT algoritması ile başarıyla saklanmıştır. Elde edilen görünütünün incelenmesi sonucunda herhangi bir değişiklik görülmemiştir. Şekil 3.9'da oluşan görüntü verilmiştir. Bu görüntünün PSNR değeri 51,3603 dB olarak hesaplanmıştır. Şekil 2.2'de bulunan orjinal resimimiz bu kez Şekil 2.9'da bulunan gizli mesajın gizlenmesi amacıyla ele alınmıştır. DWT algoritması ile Şekil 2.9'da bulunan gizli mesaj başarı ile gizlenmiş ve oluşan görüntü EK G'de verilmiştir. Görüntünün incelenmesi sonucunda farkedilir bir

değişikliğe rastlanılmamıştır. Görüntünün hesaplanan PSNR değeri 47,2097 dB olmuştur. Elde ettiğimiz iki PSNR değeri incelendiğinde Şekil 2.8'de bulunan gizli mesajın daha başarılı bir şekilde gizlendiği görülmüştür.

Şekil 2.3'de bulunan ve üzerinde hiçbir işlem yapılmamış orjinal resimimiz incelenmek üzere ele alınmıştır. Bu görüntüye DWT algoritması uygulanmıştır. Şekil 2.8'de bulunan gizli mesaj DWT algoritması sayesinde saklanmıştır. Oluşan görüntü incelendiğinde herhangi bir farklılık gözlemlenememiştir. Elde ettiğimiz görüntü Şekil 3.10'da verilmiştir. Hesaplanan PSNR değeri 51,4908 dB olmuştur. Şekil 2.9'da bulunan diğer gizli mesajımız, Şekil 2.3'de bulunan orjinal resimi DWT algoritması sayesinde gizlenmiştir. Oluşan görüntü EK G'de verilmiştir. Görüntü incelendiğinde farkedilir bir değişiklik görülmemiştir. Oluşan görüntünün hesaplanan PSNR değeri 47,3403 dB olmuştur. Bu iki gizli mesajın DWT ile gizlenmesi sonucu elde edilen PSNR değerleri karşılaştırıldığında Şekil 2.8'de bulunan gizli mesajın daha başarılı bir şekilde gizlendiği görülmüştür.

Şekil 2.4'de bulunan orjinal resim incelenmek üzere ele alınmıştır. DWT algoritması ile birlikte çalıştırılmıştır. Şekil 2.8'de bulunan gizli mesaj, DWT algoritması ile Şekil 2.4'ün içine gizlenmiştir. Bu işlem sonucu oluşan görüntü incelendiğinde herhangi bir farklılık görülmemiştir. Oluşan görüntü Şekil 3.11'de verilmiştir. Hesaplanan PSNR değeri 50,2364 dB olmuştur. Şekil 2.4'de bulunan orjinal resim bu kez Şekil 2.9'da bulunan gizli mesajın saklanmasında kullanılmıştır. Gizleme işlemi DWT algoritması ile yapılmıştır. Oluşan görüntü EK G'de verilmiştir. Bu görüntünün incelenmesi sonucunda herhangi bir değişiklik saptanamamıştır. Hesaplanan PSNR değeri 46,0858 dB olmuştur. Her iki DWT denemesinin sonucunda oluşan görüntülerde ki PSNR değerleri karşılaştırıldığında Şekil 2.8'de bulunan gizli mesajın daha başarılı bir şekilde gizlendiği görülmektedir.

Şekil 2.5'de bulunan resimimiz incelenmek üzere ele alınmıştır. DWT algoritması ile Şekil 2.8'deki gizli mesaj görüntümüze gizlenmiştir. Bu işlem sonucunda PSNR değerleri hesaplanmıştır. Oluşan görüntü Şekil 3.12'de verilmiştir. Görüntünün incelenmesi sonucu herhangi bir değişiklik bulunamamıştır. Hesaplanan PSNR değeri 51,1106 dB olmuştur. Aynı senaryo bu kez Şekil 2.9'da bulunan gizli mesajımız için

tekrar edilmiştir. DWT algoritmasının Şekil 2.5'de bulunan orjinal resime gizli mesajı gizlemesi sonucu elde edilen görüntü EK G'de verilmiştir. Hesaplanan PSNR değeri 46,9600 dB olmuştur. Hesaplanan bu PSNR değerleri karşılaştırıldığında Şekil 2.8'de bulunan gizli mesaj daha başarılı bir şekilde gizlenmiştir.

Şekil 2.6'da bulunan ve üzerinde herhangi bir değişiklik yapılmamış orjinal verimiz incelenmek üzere ele alınmıştır. DWT algoritması uygulanan görüntümüzün içine Şekil 2.8'de verilen gizli mesaj saklanmıştır. Oluşan görüntü Şekil 3.13'de verilmiştir. Bu görüntünün incelenmesi sonucu herhangi bir farklılık gözlemlenememiştir. Hesaplanan PSNR değeri 51,2060 dB olmuştur. Yapılan bu adımlar bu kez Şekil 2.9'da verilen gizli mesajın gizlenmesi amacıyla tekrar yapılmıştır. Şekil 2.9'da ki gizli mesaj DWT algoritması sayesinde Şekil 2.6'da bulunan orjinal resmimize gizlenmiştir. Oluşan görüntü EK G'de verilmiştir. Görüntüde herhangi bir değişiklik bulunmamıştır. Hesaplanan PSNR değeri 47,0555 dB olmuştur. Elde ettiğimiz PSNR değerlerini karşılaştırdığımızda Şekil 2.8'de verilen görüntünün daha başarılı bir şekilde gizlendiği görülmüştür.

Son olarak Şekil 2.7'de bulunan resimimiz ele alınmıştır. Bu görüntünün içine DWT algoritması ile Şekil 2.8'de bulunan gizli mesaj saklanmıştır. Elde edilen görüntü incelendiğinde herhangi bir değişim saptanamamıştır. Şekil 3.14'de elde ettiğimiz görüntü verilmiştir. Yapılan hesaplamalar sonucunda ise görüntünün PSNR değeri 50,7428 dB olarak hesaplanmıştır. Şekil 2.9'da bulunan ikinci gizli mesajımız da aynı adımlardan geçmiş ve EK G'de verdiğimiz görüntü elde edilmiştir. Hesaplanan PSNR değeri 46,5923 dB olmuştur. Bu PSNR değerleri karşılaştırıldığında Şekil 2.8'de bulunan gizli mesajın daha başarılı bir şekilde gizlendiği anlaşılmaktadır.

Yukarıda açıkladığımız sonuçlar ışığında, DWT algoritması ile gizlenen iki gizli mesajın PSNR değerleri hesaplanmıştır. DWT algoritmasında veri saklama yaparken, kullandığımız gizli mesajlar resim dosyası seçilmiştir. Yani DWT işlemi sonucunda elde ettiğimiz görsellerin içinde saklanan veri, yine bir görseldir. PSNR değerleri üzerinden bakıldığında, her iki gizli mesaj için elde edilen sonuçlar birbirlerine yakın ve başarılı değerlerdir. Tezimizin 2.2.6.2. bölümünde PSNR değerleriyle ilgili bilgiler sunulmuştur. Bu bilgilere göre düşük PSNR değerleri, kullanılan yöntemin başarı oranındaki

düşüklüğü göstermektedir. Bu bilgi esas alınarak ve elde edilen PSNR değerleri dikkate alınarak, yukarıda belirttiğimiz ve başarılı kabul ettiğimiz gizli mesajlar belirlenmiştir.

Tezin karşılaştırdığı DWT ve DCT algoritmalarına, çalışacakları aynı taşıyıcı resimler ve aynı büyüklükteki gizli mesajlar verilmiştir. Bu verilerin işlenmesi sonucunda her iki algoritma için de PSNR değerleri elde edilmiştir. Tezin 2.2.6.2. bölümünde PSNR sonuçlarıyla ilgili ayrıntılar sunulmuştur. Düşük PSNR değerleri, kullanılan yöntemin başarı oranındaki düşüklüğü göstermektedir. Buna dayalı olarak, yukarıda sunulan uygulamalarda DCT'nin DWT algoritmasına göre daha az PSNR değerlerine ulaşabildiği görülmüştür. Tüm DWT senaryolarında elde edilen PSNR değerleri DCT'den daha yüksek çıkmıştır. Bu değerlendirmeler sonucunda DCT ve DWT algoritmalarının karşılaştırılması sonucu DWT algoritması daha başarılı bulunmuştur.

4.2. Öneriler

Bu bölümde, tez çalışması süresince öğrendiklerimiz ve edindiğimiz genel bilgilerden faydalanarak, steganografi ve yan dallarından bahsedecek ve steganografiyle ilgili yüksek lisans tezimize ek olarak ileriki dönem çalışmalarımızda neler üzerinden ilerleyeceğimize değineceğiz.

Öncelikle steganografi, günümüzde kullandığı taşıyıcı iletişim unsurlarının herkese açık olması ve içeriğindeki gizli mesajların ise farkına varılamaz olmasından dolayı devletlerin önemli teşkilatlarında, haber alma ve istihbarat amaçlı kullanılmaktadır. Bu ve diğer birçok açıdan steganografi çok önemli bir çalışma konusudur.

Ayrıca günümüz haberleşme sistemlerinde, iletişim hatlarında birçok sebepten ötürü meydana gelebilen gürültü etmeni bulunmaktadır. Gürültü etmeni özellikle görsel ve işitsel veriler üzerinde farkına varılması güç bozulmalara sebep verebilir. Steganografide bu bozulma, gizli veri aktarımında bir avantaj konumundadır. Gönderdiğimiz gizli verinin taşıyıcı mesaj üzerindeki bozulumunun, gürültüye oranı bize avantaj kazandırmaktadır. Bu oranı ölçen PSNR değeri ise kurmuş olduğumuz sistemin ne kadar düzgün çalıştığının en önemli göstergesidir.

Tez çalışmamızın sonucunda elde ettiğimiz DWT algoritmasının DCT algoritmasına nazaran daha başarılı olması durumu, ileride bu alanda yapılacak araştırmalarda, veri

gizleme seçimi yapılırken, metin verisi yerine görsel veri tercihinin daha güvenilir sonuçlar verebileceği düşünülmektedir. Steganografi günümüzde çok daha özel ve hibrit teknolojiler ile birlikte kullanılan bir iletişim kanalı konumundadır. Birçok legal veya illegal oluşumlar, iletişim ihtiyaçlarının karşılanmasında belirli ölçülerde steganografiyi kullanmaktadırlar. Her gün en çok kullandığımız internet siteleri, haber mecraları ve hatta Twitter ve Facebook gibi sosyal medya unsuları üzerinde takip ettiğimiz ve popüler konularda karşılaştığımız multimedya unsurları steganografi barındırıyor olabilir. DeepWeb yani karanlık internet ağı olarak çevirebileceğimiz, internet tarayıcıları tarafından adreslenmemiş internet ağı bile şuan içerisinde bulunduğumuz ve hatta DeepWeb'den çok daha ufak olan indeksli internet belkide daha fazla steganografi unsuru içermektedir. Ancak veri akış trafiğinin çok yüksek olması ve giderek artmasından dolayı steganografinin kolayca takip edilemeyeceği gibi bir imkan oluşsa dahi, geliştirilen yeni sistemlerle dahi farkına varılması zor bir durumda olduğu mutlak bir gerçektir.

Bu tez çalışmamızdan çıkarımımız; günümüzde yavaş yavaş birçok alanda kendini göstermeye başlayan yapay zeka veya derin öğrenme uygulamalarının daha aktif bir şekilde steganografide kullanılma zorunluğudur. Zira bu kadar büyük bir trafiğin insanlar tarafından kontrol edilmeye çalışılması artık neredeyse imkansız bir hal almıştır. Bu yüzden gelecek zamanlardaki bilimsel çalışmalarımızın derin öğrenme, Deep Learning, veya Machine Learning yöntemlerinin steganografi ile sentezlenmesi üzerine olacaktır. Bu nedenle bahsetmiş olduğumuz bu konuda ayrıntılı bir araştıma yapılabilir ve yeni bakış açıları getirilebilir. Ayrıca steganografi algoritmalarının Watermarking adındaki aitlik ve sahiplik belirtmeye yarayan çalışmalarda kullanılması, dijital medya unsurlarının haklarının korunması konusunda ayrıntılı bir bilgi ve tecrübe kaynağı olmuştur. Steganografi üzerine çalışmalarımız sayesinde replikasyon ürünlerin incelenmesi ve sahtecilik analizi, görsel veri işleme algoritma ve yöntemleri, mesajlaşma ve iletişim prosedürleri ve şifreleme üzerinde ufkumuzu genişletmiş ve bu alanlarda daha çok çalışmanın yapılmasına gereksinim duyulduğu görülmüştür.

KAYNAKLAR

Acharya,U. D., Kamath, P. R., Prabhu, R. ve Shama, H. (2012). A Novel ColorImage Steganography using Discrete Wavelet Transform. CCSEIT-12, October 26-28, 2012, Coimbatore [Tamil nadu, India], ACM 978-1-4503-1310-0/12/10, Pages 223-226.

Alçı, M. ve Çivicioğlu, P. (2003). Güvenli İletişim İçin Veri Gizleme Tekniklerinin Kullanımı. Elektrik-Elektronik, Bilgisayar Mühendisliği 10. Ulusal Kongresi

Anderson, R. J. ve Petitcolas, F. A. P. (1998). On The Limits of Steganography. IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998. ISSN 0733-8716.

Batham, S., Sharma, S. ve Ya dav, V. K. (2014). Zero distortion technique: An approach to image steganography on color images using strenght of chaotic sequence. J. Lloret Mauri at al. (Eds.): SSCC 2014, CCIS 467, pp. 407-416 2014.

Bedi, P., Bhasin, V.,Goel, A. ve Gupta, S. (2015). StegTrack: Tracking images with hidden content. WCI '15, August 10 - 13, 2015, Kochi, India, ACM. ISBN 978-1-4503-3361-0/15/08, Pages 318-323.

Bedi, P. ve Singhal, A. (2015). Steganography using Cuckoo Optimized Wavelet Coefficients. WCI '15, August 10 - 13, 2015, Kochi, India, ACM. ISBN 978-1-4503-3361-0/15/08, Pages 365-370.

Bender, W., Gruhl, D., Lu, A. ve Morimoto N. (1999). Techniques for data hiding. IBM Syst. Journal vol.35 nos:3-4 1999, pp: 315-331.

Bera, S., Dewangan, U. ve Sharma, M. (2013). Development and Analysis of Stego Image Using Discrete Wavelet Transform. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064pp:142-148.

Bloom, J., Cox, I., Fridrich, J., Kalker, T. ve Miller, M. (1991). Digital Watermarking and Steganography Book. Paper: 12 - 25

Cachin, C. (2004). An information-theoretic model for steganography. Information and Computation Volume 192, Issue 1, 1 July 2004, Pages 41–56.

Challita, K. ve Farhat, H. (2011). Combining Steganography and Cryptography: New Directions. International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208 The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

Chandel, G. S., Gupta, R. ve Patil, S. (2014). Performace Analysis of Steganography Based on 5-wavelet Families by 4 levels – dwt. IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.12, December 2014. Page: 56 - 61.

Chang, L., Longdon, G. E. ve Moskowitz, I. S. (2000). A new paradigm hidden in steganography. NSPW '00 Proceedings of the 2000 workshop on New security paradigms, Pages 41 - 50, ACM New York, NY, USA, ACM ISBN: 1-58113-260-3.

Chaudhary, V. ve Kaushal, A. (2013). Secured image steganography using different transform domain. International Journal of Computer Applications (0975 – 8887) Volume 77– No.2, September 2013, pp: 24-28.

Chhikara, R. ve Saini, M. (2015). Performance evaluation of dct and dwt features for blind image steganalysis using neural networks. International Journal of Computer Applications (0975 – 8887) Volume 114 – No. 5, March 2015, pp: 20-23.

Dalvi, A. ve Kamathe, R. S. (2014). Color image steganography by using dual wavelet transform (dwt, swt). International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878, Impact Factor (2014): 3.05.

Davidson, I. ve Paul, G. (2004). Locating Secret Messages in Images. KDD'04, August 22-25, 2004, Seattle, Washington, USA, ACM 1-58113-888-1/04/0008.

Denemark, T. ve Fridrich, J. (2015). Improving Steganographic Security by Synchronizing the Selection Channel. IH&MMSec '15 Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. Pages 5 - 14. ACM, New York, NY, USA. ISBN: 978-1-4503-3587-4.

Dhawale, C. A., Hegadi, R. ve Jambhekar, N. D. (2014). Performance Analysis of Digital Image Steganographic Algorithm. ICTCS '14, November 14 - 16 2014, Udaipur, Rajasthan, India, ACM 978-1-4503-3216-3/14/11.

Esin, E.M. ve Güvenoğlu, E. (2012). Resim İçine Yazı Gizlenmesi Amacıyla Kullanılan LSB Ekleme Yönteminin Shuffle Algoritmasıyla İyileştirilmesi.

Fridrich, J. ve Holub,V. (2013). Digital Image Steganography Using Universal Distortion. IH&MMSec'13, June 17–19, 2013, Montpellier, France, ACM 978-1-4503-2081-8/13/06.

Giri, D., Jana, B. ve Mondal, S. K. (2015). An Efficient Data Hiding Scheme using Hamming Error Correcting Code. ICCCT '15 Proceedings of the Sixth International Conference on Computer and Communication Technology 2015. Pages 360 - 065 ACM New York, USA, ACM ISBN: 978-1-4503-3552-2.

Haşiloğlu, A. (2001). Dalgacık Dönüşümü ve Yapay Sinir Ağları ile Döndürmeye Duyarsız Doku Analizi ve Sınıflandırma. Turk J Engin Environ Sci 25 (2001) , 405-413. @TÜBİTAK

Ibrahim, A. M., Manaf, A. A. ve Zeki, A. M. (2012). Steganographic Software: Analysis and Implementation. INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Issue 1, Volume 6, 2012

Jakobsen, S. K. ve Orlandi, C. (2016). How to bootstrap anonymous communication. ITCS '16 Proceedings of the 2016 ACM Conferance on Innovations in Theoretical Computer Science. Pages 333 - 344. ACM, New York, NY, USA. ISBN: 978-1-4503-4057-1.

Jo, H. J., Kim, H., Lee, K., Lee, H. ve Yoon, J. W. (2015). Visual honey encryption: Application to steganography. IH&MMSec '15 Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security. Pages 65 - 74. ACM, New York, NY, USA. ISBN: 978-1-4503-3587-4.

Khan, A., Majid, A., Mirza, A. M. ve Tahir, S. F. (2008). Support Vector Machine based Intelligent Watermark Decoding for Anticipated Attack. World Academy of Science, Engineering and TechnologyInternational Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:2, No:9, 2008.

Kim, D. S., Lee, G. J. ve Yoo, K. Y. (2014). Reversible data hiding scheme based on histogram shifting using edge direction predictor. RACS '14 Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems. Pages 126 - 131. ACM, New York, NY, USA. ISBN: 978-1-4503-3060-2.

Liu, Y., Liu, Y., Wu, S. ve Zhong, S. (2015). What Makes the Stego Image Undetectable? ICIMCS ’15, August 19-21, 2015, Zhangjiajie, Hunan, China, ACM. ISBN 978-1-4503-3528-7/15/08.

Nehete, S., Sawarkar, S. D. ve Sohani, M. (2011). Digital Audio Steganography using DWT with Reduced Embedding Error and Better Extraction Compared to DCT. ICWET’11, February 25–26, 2011, Mumbai, Maharashtra, India, ACM 978-1-4503-0449-8/11/02.

Pfitzman, B. (2004). Information Hiding Terminology in Information Hiding. Springer Lecture Notes in Computer Science, vol:1174, pp:347-350.

Pfitzmann, A. ve Westfeld, A. (2000). Attacks on steganographic systems: Breaking the steganographic utilities EzStego,JSteg,Steganos and Stools – and some lessons learned. Information Hiding Volume 1768 of the series Lecture Notes in Computer Science pp 61-76.

Srivastava, A. (2015). Performance comparison of various particle swarm optimizers in dwt – svd watermarking for rgb image. ICCCT '15 Proceedings of the Sixth International Conference on Computer and Communication Technology 2015. Pages 244 - 250 ACM New York, USA, ACM ISBN: 978-1-4503-3552-2.

Verma, N. (2011). Review of steganography techniques. *ICWET’11*, February 25–26, 2011, Mumbai, Maharashtra, India, ACM 978-1-4503-0449-8/11/02.

Zaturenskiy, M. (2013). Mp3 steganography techniques. RIIT'13, October 10-12, 2013, Orlando, Florida, USA, ACM 978-1-4503-2494-6/13/10.

Internet Kaynakları

Demirci, B. (2016). Görüntü Steganografi Metodları ve Performanslarının Karşılaştırılması. (Yüksek Lisans Tezi) Adres: https://tez.yok.gov.tr/UlusalTezMerkezi/giris.jsp

Kaya, H. V. (2015). Watermarking in medical images by using DCT, DWT, DFT and LSB algorithms. (Yüksek Lisans Tezi) Adres:http://earsiv.cankaya.edu.tr:8080/xmlui/handle/123456789/392

Şahin A. (2007). Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri. (Doktora Tezi) Adres: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

URL-1<http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.57506379399758.18050380 >, Alındığı Tarih: 2.4.2016.

URL-2<https://tr.wikipedia.org/wiki/Steganografi>, Alındığı Tarih: 4.4.2016.

URL-3<http://www.jatit.org/volumes/research-papers/Vol18No1/7Vol18No1.pdf>, Alındığı Tarih: 9.5.2016.

URL-4<https://tr.wikipedia.org/wiki/MATLAB>, Alındığı Tarih: 10.5.2016.

URL-5<http://www.mathworks.com/products/matlab/>, Alındığı Tarih: 10.5.2016.

URL-6<http://www.garykessler.net/library/fsc_stego.html>, Alındığı Tarih: 11.5.2016.

URL-7<http://www.guillermito2.net/stegano/jsteg/>, Alındığı Tarih: 14.5.2016.

URL-8<https://tr.scribd.com/doc/48764974/Steganography-Data-hiding-using-LSB-algorithm>, Alındığı Tarih: 14.5.2016.

URL-9<http://niels.xtdnet.nl/papers/practical.pdf>, Alındığı Tarih: 16.5.2016.

URL-10<http://www.garykessler.net/library/fsc_stego.html>, Alındığı Tarih: 18.5.2016.

URL-11<http://www.isites.info/pastconferences/isites2014/isites2014/papers/A6-ISITES2014ID136.pdfl>, Alındığı Tarih: 20.5.2016.

URL-12<http://www.mathworks.com/help/comm/ug/error-detection-and-correction.html#bsxti8o>, Alındığı Tarih: 22.5.2016.

EKLER

EK A : Gizlenen Text Dosyası: İstiklal Marşı

EK B : DCT Pseudo Kodu

EK C : DWT Pseudo Kodu

EK D : Hamming Matlab Kodu

EK E : Gizlenen Text Dosyası: Gençliğe Hitabe

EK F : DCT Steganografik Resimleri

EK G : DWT Steganografik Resimleri

EK A

A.1. Gizlenen Text Dosyası: İstiklal Marşı

Korkma, sönmez bu şafaklarda yüzen al sancak;
Sönmeden yurdumun üstünde tüten en son ocak.
O benim milletimin yıldızıdır, parlayacak;
O benimdir, o benim milletimindir ancak.
Çatma, kurban olayım, çehrene ey nazlı hilal!
Kahraman ırkıma bir gül... Ne bu şiddet, bu celal?
Sana olmaz dökülen kanlarımız sonra helal;
Hakkıdır, Hakk'a tapan, milletimin istiklal.
Ben ezelden beridir hür yaşadım, hür yaşarım.
Hangi çılgın bana zincir vuracakmış? Şaşarım!
Kükremiş sel gibiyim: Bendimi çiğner, aşarım;
Yırtarım dağları, enginlere sığmam taşarım.
Garb'ın afakını sarmışsa çelik zırhlı duvar;
Benim iman dolu göğsüm gibi serhaddim var.
Ulusun, korkma! Nasıl böyle bir imanı boğar,
"Medeniyet!" dediğin tek dişi kalmış canavar?
Arkadaş! Yurduma alçakları uğratma sakın;
Siper et gövdeni, dursun bu hayasızca akın.
Doğacaktır sana va'dettiği günler Hakk'ın...
Kim bilir, belki yarın, belki yarından da yakın.
Bastığın yerleri "toprak!" diyerek geçme, tanı!
Düşün altındaki binlerce kefensiz yatanı.
Sen şehid oğlusun, incitme, yazıktır, atanı:
Verme, dünyaları alsan da, bu cennet vatanı.
Kim bu cennet vatanın uğruna olmaz ki feda?
Şüheda fışkıracak toprağı sıksan, şüheda!
Canı, cananı, bütün varımı alsın da Huda,

Etmesin tek vatanımdan beni dünya da cüda.
Ruhumun senden İlahi şudur ancak emeli:
Değmesin ma'bedimin göğsüne namahrem eli;
Bu ezanlar ki şehadetleri dinin temeli
Ebedi, yurdumun üstünde benim inlemeli.
O zaman vecd ile bin secde eder varsa taşım;
Her cerihamda, İlahi, boşanıp kanlı yaşım,
Fışkırır ruh-i mücerred gibi yerden na'şım!
O zaman yükselerek Arş'a değer, belki, başım.
Dalgalan sen de şafaklar gibi ey şanlı hilal!
Olsun artık dökülen kanlarımın hepsi helal.
Ebediyyen sana yok, ırkıma yok izmihlal:
Hakkıdır, hür yaşamış, bayrağımın hürriyet;
Hakkıdır, Hakk'a tapan, milletimin istiklal.
Mehmet Akif ERSOY

EK B

B.1. DCT Pseudo Kodu

```
// DCT pseudo kodu
BEGIN DCT PSEUDO
//Taşıyıcı obje ve mesajın okunması
        READ CoverImage;
        READ SecretMessage;
//gizli mesajın binary formatına dönüşümü
        SET S = SecretMessage;
        SET A = CALL dec2bin(S);
// Hamming Kodlamanın binary formata dönüşmüş gizli mesaja uygulanması
        SET A1 = CALL HammingCode(A);
//Taşıyıcı resim üzerinde 8x8 grid oluşumu
        SET X,Y = size(CoverImage);
        SET Counter=0;
        FOR endof X,
        SET X1 = Counter:Counter+8;
                FOR endof Y
                        SET Y1 = Counter:Counter+8;
                        SET BLOK (X1,Y1);
                        SET FREQ = dct2(BLOK);
```

```
                SET RAW = dec2bin(FRE);
                CALL LSB(RAW,A1);
            END FOR
        END FOR
CALL idct2(FRE);
END DCT PSEUDO
```

EK C

C.1. DWT Pseudo Kodu

```
// DWT Pseudo Kodu
BEGIN DWT PSEUDO
// Taşıyıcı ve gizli objelerin okunması
    READ CoverImage;
    READ SecretImage;
// Taşıyıcı ve gizli objenin frekanslarında işlem yapılması için sayısal tabana çekilmesi
    SET T = CALL im2double(CoverImage);
    SET S= CALL im2double(SecretImage);
// DWT kullanılarak 3. Katman yani en düşük katmanda veri bandlarının elde edilmesi
    //Taşıyıcının banlarına ayrışması
        // Haar bu alanda kullanılan popüler ve verimli bir yöntem olduğu için
        // seçilmiştir.
    SET K1 = CALL dwt2('T','haar');
    SET K2 = dwt2('K1','haar');
    SET K3 = dwt2('K2','haar');
    //Gizli mesajın bandlarına ayrışması
    SET L1 = dwt2('S','haar');
    SET L2 = dwt2('L1','haar');
    SET L3 = dwt2('L2','haar');
```

// Rastgelelik eklemek için sabit sayı tanımlıyoruz. Bu sayı bizim belirlediğimiz bir sayı
// olucak ve taşıyıcı mesaja eklenecektir.Böylelikle basit bir rastgelelik sağlanacaktır.

SET C = CALL Random();

SET StegoImage = (K3+L3)*C;

SET FinalImage = CALL idwt2(StegoImage); // x3 kez tekrarlanarak

END DWT PSEUDO

EK D

D.1. Hamming Matlab Kodu

(URL12)

// Hamming Matlab kodları

Hamming Chunk kodu – Ana program

```
function [bin_send] = hamming_encode_chunk(bin)
% Bulunan 3 adet tepe noktasına veya yığına hamming kodlama yapılır. Bu kod bloğu bu 3 yığını sınırları ile oluşturup encode algoritmasını programa çağırır
len = floor(length(bin)/3);
bin_send = zeros(6, len);
bin = bin(1:len*3);
bin = reshape(bin, 3, len);
for i = 1:len
   bin_send(:,i) = hamming_encode(bin(:,i)')';
end
bin_send = reshape(bin_send, 1, 6 * len);
end
```

Hamming Encode Fonksiyonu

```
function [bin_send, nbp] = hamming_encode(bin)
% hamming_encode() verilen binary veri bloğuna hamming kodlama yapar
% INPUTLAR
%   bin - Binary string, örn: [1 0 0 1 0 1 1 0]
% OUTPUTLAR
%   bin_send – hamming kodlaması tamamlanmış array
%Programa çağırılan nbp fonksiyonu kaç adet parity bit ekleneceğinin hesabını yapar
nbp = hamming_nbp(length(bin), false);
%Elde edilen parity bit sayısını bu fonksiyona gönderip verilen array'e parity bit ekletiriz
bin_send = insert_parity_bits(bin,nbp);
end
```

Hamming NBP Fonksiyonu

```
function [nbp] = hamming_nbp(l, inc_parity)
% nbp() Calculates number of parity bits for given message length
% INPUTS
%   l         - verilen mesajın uzunluğu
%   inc_parity – mesajın önceden parity bit içerip içermediğini belirten logical değerdir. Flase ise nbp yapılacak true ise nbp değerleri verilmiş çözülme işlemi yani tersine nbp yapılacak demektir.
% OUTPUT
%   nbp – Kaç adet parity bit kullanılacağını belirten rakam
if inc_parity == true
```

```
   nbp = ceil(log2(l));
else
   nbp = floor(log2(l + ceil(log2(l)))) + 1;
end
end
```

insert_parity_bits Fonksiyonu

```
%Parity bitleri hesaplar ve doğru noktalara yerleştirir
function E=insert_parity_bits(message,nbp)
nbp=nbp;
A=message;
E=insert_parity_spots(A,nbp);
P=generate_hamming_matrix(E,nbp);
%Mesaj bloğundaki değeri 1 olan verileri saptar
for V=1:nbp
   Q(V,:)=P(V,:).*E;
end
Q;
%Herbir parity satırında bitlerin toplamının tek mi çift mi olduğunu bulur. 1 veya 0.
for U=1:nbp
   R(U,:)=mod(length(find(Q(U,:))),2);
end
R;
%Gerekli olan yerlere parity bit eklemesi yapar
for S=0:nbp-1
   E(1,2^S)=R(S+1,1);
end
E;
```

insert_parity_spots Fonksiyonu

```
%Bu fonksiyonun amacı parity bitlerin olacağı yerlere O sıfır yerleştirmektir.
function E=insert_parity_spots(message,nbp)
clearvars D E
nb_bits_parity=nbp;
D=message;
E=ones(1,length(D)+nb_bits_parity);
%matris'in 2^n pozisyonlarına 0 ekleme
for I=0:nb_bits_parity
   E(1,2^I)=0;
   E=E(1,1:length(D)+nb_bits_parity);
end
E;
%message vector
for M=1:length(E)
   if E(1,M)==1
      count=floor(log2(M)+1);
      E(1,M)=D(1,M-count);
   end
```

```
    end
    E;
     generate_hamming_matrix Fonksiyonu
% Bu kod bloğunda mesaj verisi ve parity bitler bir matris içerisine toplanmaktadır.
function P=generate_hamming_matrix(coded_message,nbp)
P=zeros(nbp,length(coded_message));
stop_z=length(P);
for X=1:nbp
   for Y=0:length(P)-1
      if Y<stop_z/2^X
        P(X,((2^X)*Y+2^(X-1)):((2^X)*Y+(2^X)-1))=1;
      end
   end
end
P=P(:,1:stop_z);
```

EK E

E.1. Gizlenen Text Dosyası: Gençliğe Hitabe

Ey Türk Gençliği!

Birinci vazifen, Türk istiklâlini, Türk Cumhuriyetini, ilelebet, muhafaza ve müdafaa etmektir.

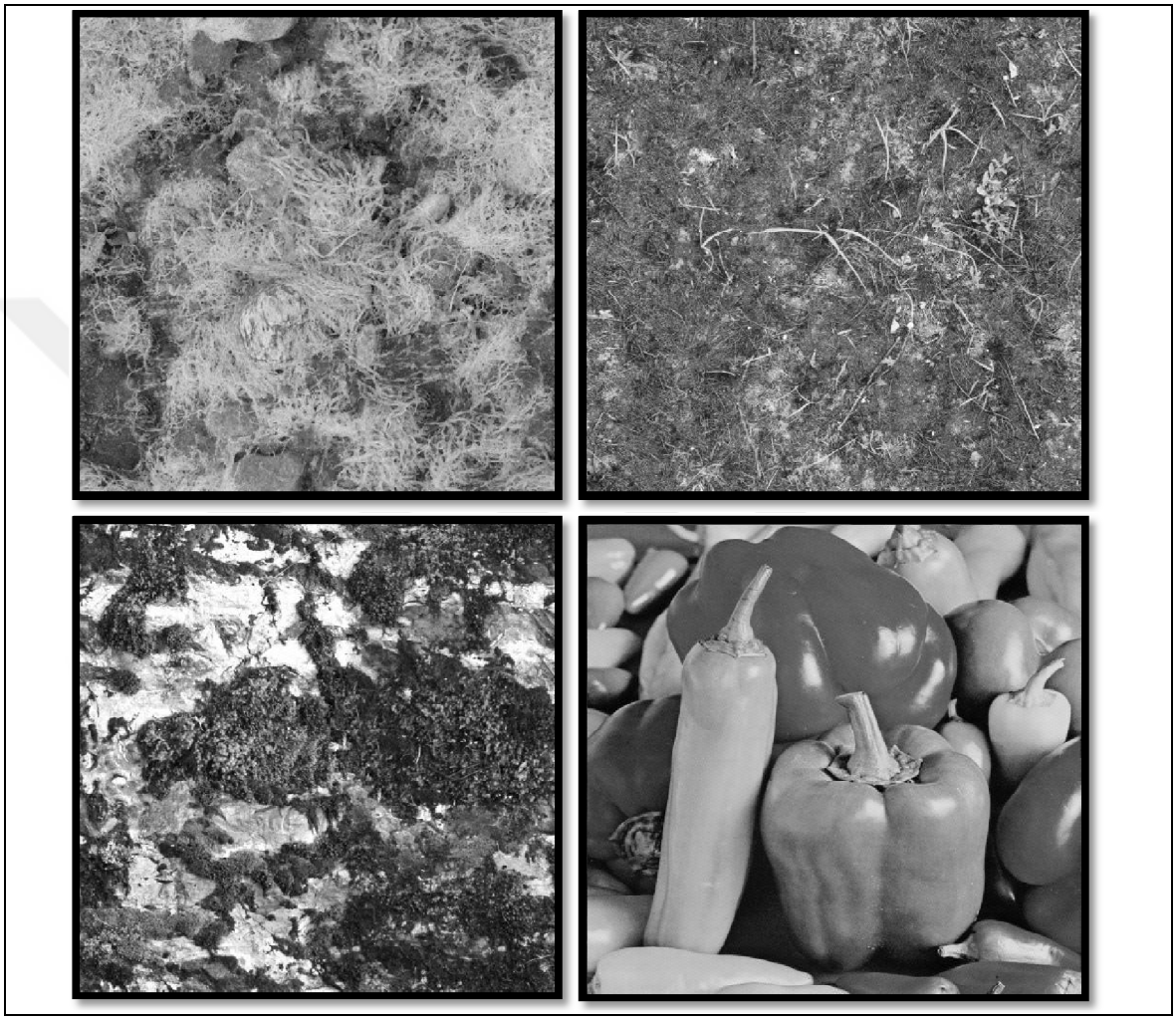
Mevcudiyetinin ve istikbalinin yegâne temeli budur. Bu temel, senin, en kıymetli hazinendir. İstikbalde dahi, seni bu hazineden mahrum etmek isteyecek, dahilî ve haricî bedhahların olacaktır. Bir gün, İstiklâl ve Cumhuriyeti müdafaa mecburiyetine düşersen, vazifeye atılmak için, içinde bulunacağın vaziyetin imkân ve şerâitini düşünmeyeceksin! Bu imkân ve şerâit, çok nâmüsait bir mahiyette tezahür edebilir. İstiklâl ve Cumhuriyetine kastedecek düşmanlar, bütün dünyada emsali görülmemiş bir galibiyetin mümessili olabilirler. Cebren ve hile ile aziz vatanın, bütün kaleleri zaptedilmiş, bütün tersanelerine girilmiş, bütün orduları dağıtılmış ve memleketin her köşesi bilfiil işgal edilmiş olabilir. Bütün bu şerâitten daha elîm ve daha vahim olmak üzere, memleketin dahilinde, iktidara sahip olanlar gaflet ve dalâlet ve hattâ hıyanet içinde bulunabilirler. Hattâ bu iktidar sahipleri şahsî menfaatlerini, müstevlilerin siyasi emelleriyle tevhit edebilirler. Millet, fakr ü zaruret içinde harap ve bîtap düşmüş olabilir.

Ey Türk istikbalinin evlâdı! İşte, bu ahval ve şerâit içinde dahi, vazifen; Türk İstiklâl ve Cumhuriyetini kurtarmaktır! Muhtaç olduğun kudret, damarlarındaki asil kanda mevcuttur!

M. Kemal ATATÜRK

EK F

F.1. DCT Steganografik Resimleri

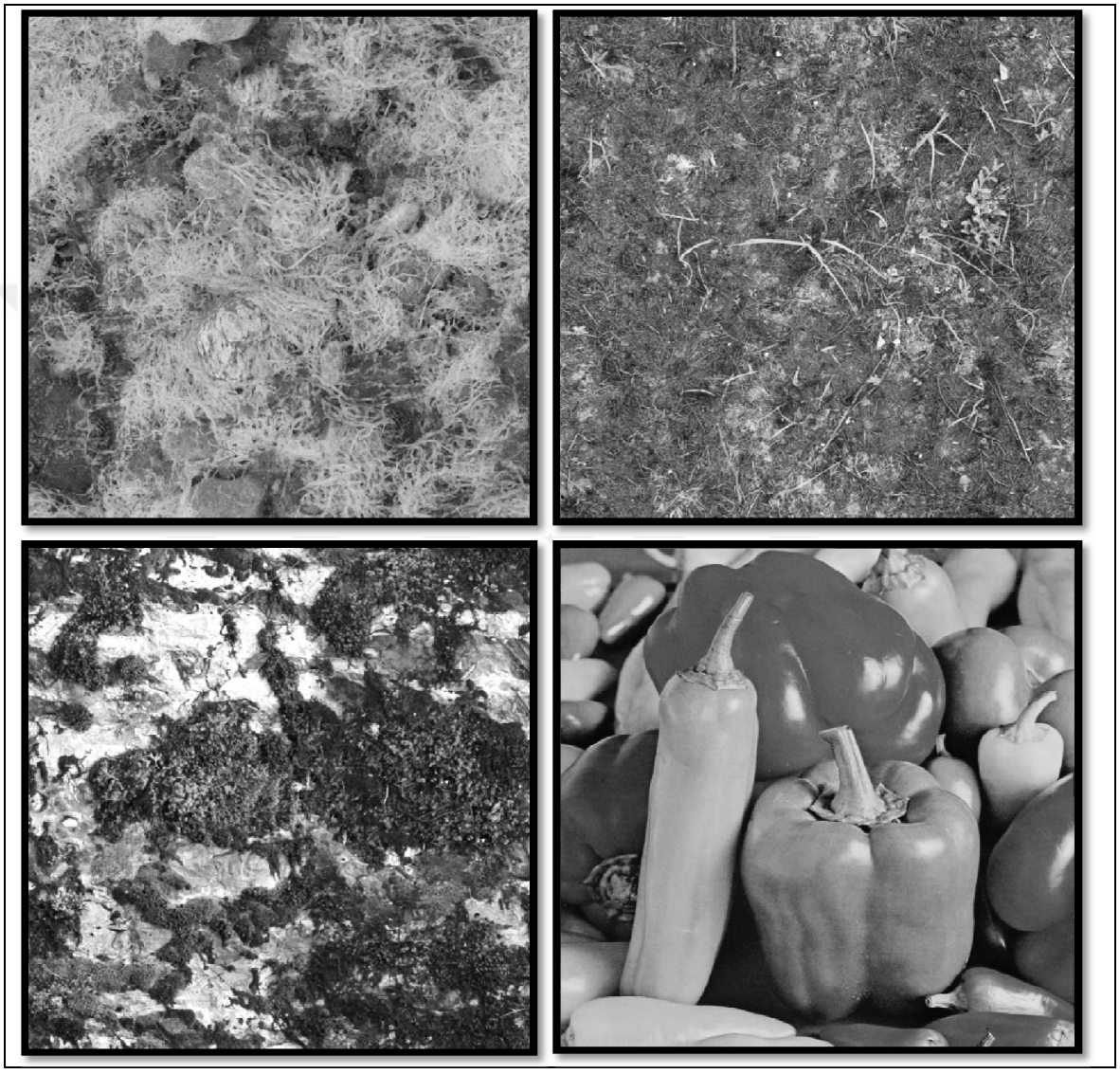


Şekil F.1 : DCT Uygulanmış Steganografik Resimler 1

Şekil F.2 : DCT Uygulanmış Steganografik Resimler 2

EK G

G.1. DWT Steganografik Resimleri



Şekil G.1 : DWT Uygulanmış Steganografik Resimler 1

Şekil G.2 : DWT Uygulanmış Steganografik Resimler 2

ÖZGEÇMİŞ

Ad - Soyad : Faruk Takaoğlu

Doğum Tarihi ve Yeri : 11.08.1991

E-posta : faruktakaoglu@gmail.com

Tel : 0542 454 69 61

ÖGRENİM DURUMU : Yüksek Lisans (Devam Etmekte)

- **LİSANS** : İstanbul Aydın Üniversitesi - Mühendislik Mimarlık Fakültesi - Bilgisayar Mühendisliği (2009-2014)
- **YÜKSEK LİSANS** : İstanbul Aydın Üniversitesi - Bilgisayar Mühendisliği Ana Bilim Dalı - Bilgisayar Mühendisliği Programı

MESLEKİ DENEYİMLER

Tarih : 2012

Meslek veya Pozisyonu : Stajyer

İşyeri Adı : İstanbul Aydın Üniversitesi

Tarih : 2013-2014

Meslek veya Pozisyonu : Stajyer Öğrenci

İşyeri Adı : Tübitak Bilgem İltaren (Ankara - Türkiye)

ÖDÜLLER

İstanbul Aydın Üniversitesi 2010-2011 eğitim yılı bilgisayar mühendisliği bölüm birinciliği ve yüksek onur sertifikası

İstanbul Aydın Üniversitesi 2011-2012 eğitim yılı bilgisayar mühendisliği bölüm birinciliği ve yüksek onur sertifikası

İstanbul Aydın Üniversitesi 2012-2013 eğitim yılı bilgisayar mühendisliği bölüm birinciliği ve yüksek onur sertifikası

İstanbul Aydın Üniversitesi 2013-2014 eğitim yılı bilgisayar mühendisliği bölüm birinciliği ve yüksek onur sertifikası

İstanbul Aydın Üniversitesi 2013-2014 eğitim yılı Mühendislik Fakültesi birinciliği