**T.C.**
**SAKARYA ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

# TIBBİ GÖRÜNTÜ GÜVENLİĞİ İÇİN YENİ BİR SAYISAL DAMGALAMA YÖNTEMİ

**YÜKSEK LİSANS TEZİ**

**Maimaitiming MAMUTI**

| | | |
|---|---|---|
| **Enstitü Anabilim Dalı** | **:** | **BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ** |
| **Tez Danışmanı** | **:** | **Dr. Öğrt. Üyesi Serap KAZAN** |

**Eylül 2019**

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

# TIBBİ GÖRÜNTÜ GÜVENLİĞİ İÇİN YENİ BİR SAYISAL DAMGALAMA YÖNTEMİ

**YÜKSEK LİSANS TEZİ**

**Maimaitiming MAMUTI**

| | |
|---|---|
| **Enstitü Anabilim Dalı** | **BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ** |

**Bu tez 13./09/2019 tarihinde aşağıdaki jüri tarafından ~~oybirliği/oyçokluğu~~ ile kabul edilmiştir.**

| | | |
|---|---|---|
| Prof. Dr. Razit Kökter | Dr. Öğrt. Üyesi Serap Kazan | Doç.Dr. Nilüfer Yurtay |
| **Jüri Başkanı** | **Üye** | **Üye** |

## BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm veri ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Maimaitiming MAMUTI

01.09.2019

# TEŞEKKÜR

Çalışmamın başından beri danışmanım Dr. Öğretim Üyesi Serap Kazan'dan çok destek aldım, sabırla beni yönlendirdi. Aileme, özellikle de her zaman yanımda olan anneme şükranlarımı sunarım.

# İÇİNDEKİLER

# SİMGELER VE KISALTMALAR LİSTESİ

| | |
|---|---|
| DCT | : Ayrık Kosinüs Dönüşüm |
| DWT | : Ayrık Dalgacık Dönüşümü |
| LSB | : En Değersiz Bit |
| MSE | : Ortalama Kare Hatası |
| NC | : Normalleştirilmiş Korelasyon |
| PSNR | : Tepe Sinyal Gürültü Oranı |
| IDCT | :Ters Ayrık Kosinüs Dönüşümü |
| IDWT | :Ters Ayrık Dalgacık Dönüşümü |

# ŞEKİLLER LİSTESİ

# ÖZET

Anahtar kelimeler: LSB, DWT, DCT, Arnold Scrambling, RGB Görüntü, Tıbbi Görüntü Damgalama, NC, PSNR

Dünya her geçen gün giderek sayısallaşmaktadır, teknolojinin ilerlemesi ile tıbbi görüntülerin internet üzerinde depolanması ve paylaşılması gibi işlemler mümkün hale gelmiştir. Ancak görüntülerin iletilmesi sırasında ve sonrasında oluşabilecek veri güvenliğini tehdit eden olasılıklar da dikkat çekmektedir. Bundan dolayı, tıbbi görüntülerin gerçekliğini ve bütünlüğünü nasıl koruyacağımız aciliyetle değinilmesi gereken bir husus olmuştur. Bu tezde, tıbbi görüntülerin karakteristiği ve niteliğini göz önünde bulundurarak, daha önce yapılmış ilgili araştırmalarla beraber, çeşitli sayısal görüntü damgalama algoritmalarını değerlendirdikten sonra, literatür taramasına dayanarak damgalama algoritmasını daha da saldırıya dayanıklı hale getirme çabasıyla, tıbbi görüntü için yeni sayısal damgalama algoritması geliştirilmiştir.

Bu çalışmada, RGB renkli görüntü kapak resmi olarak seçilip, R, G ve B renk kanallarına ayrıştırılmıştır. Daha sonra R kanalından oluşan R matrisine Ayrık Dalgacık Dönüşümü (DWT) damgalama algoritması, G kanalına Ayrık Kosinüs Dönüşümü (DCT) algoritması uygulanmış, son olarak B kanal ise En Değersiz Bit (LSB) damgalama algoritması ile işlem görmüştür. Tıbbi görüntü okunduktan sonra, sayısal damgalama algoritmasına bir güvenlik düzeyi daha katmak amacıyla Arnold Scrambling kullanılarak piksel yerleri değiştirilmiştir. Önerilen sayısal damgalama algoritmasının performansı, yaygın olarak kabul edilen Normalleştirilmiş Korelasyon (NC) ve Tepe Sinyal Gürültü Oranı (PSNR) kullanılarak değerlendirilmiş ve analiz edilmiştir.

Deneysel sonuçlar, önerilen algoritmanın başarılı olduğunu ve yeni yaklaşımın kabul edilebilir bir görüntünün elde edilmesinde başarılı olduğunu ortaya koymuştur.

# A NOVEL WATERMARKING METHOD FOR MEDICAL IMAGE SECURITY ENHANCEMENT

## SUMMARY

Keywords: LSB, DWT, DCT, Arnold Scrambling, RGB Image, Medical Image Watermarking, NC, PSNR

As the world is becoming increasingly digitized, with the advancement of technology, storing and transmitting medical images via internet has been made possible. And tampering of the images has come to the attention. So how to keep authenticity and integrity of medical images is a question that should be addressed with urgence. This thesis takes into consideration of characteristic and nature of medical images and throughly studies, evaluates digital image watermarking algorithms, and based on literature review develops a new watermarking algorithm for medical image as an effort to make watermarking scheme more attack-resistant.

In this study, the color image is chosen as cover image and decomposed into R, G, and B color channels, then DWT watermarking algorithm is applied on R matrix, which consists of R channel, DCT is applied on G channel, last channel B is processed with LSB watermarking algorithm. After reading the watermark image, which is a medical image, Arnold Scrambling is used to jumble pixels of watermark image in order to provide another level of security to the whole watermarking scheme. The performance of proposed watermark algorithm is evaluated and analysed using widely accepted Normalized Correlation and Peak Signal to Noise Ratio.

The experimental results show that imperceptibility of proposed watermarking scheme is relatively high, suggesting that the new approach is considered successful in achieving acceptable image quality.

# BÖLÜM 1. GİRİŞ

Çok eskiden beri, insanlar sürekli olarak daha hızlı ve daha etkili iletişim yolları icat etmek için çalışmaktadırlar. En eski mağara çizimleri, şenlik ateşi sinyalizasyonu, davul alarmları, metinler, telgraflar, telefonlar ve televizyonlar bunlara örnek olarak verilebilir. Şimdi de, veri çağının ortaya çıkmasıyla, özellikle internet teknolojisinin yaygın kullanılması ile, verinin iletimi gittikçe daha elverişli hale gelmiştir ve iletilen veri gittikçe artmaktadır. Sonuç olarak, veri güvenliği koruması konusu giderek daha belirgin hale gelmiştir.

Geleneksel veri güvenliği teknolojileri öncelikle şifreleme için veri şifrelemesi kullanırlar. Bununla birlikte, birçok alanda, kriptografi uygulaması sınırlamalarını giderek daha fazla ortaya çıkarmıştır: kriptografi, şifreli metnin anlaşılmazlığı yoluyla verilerin içeriğini korurken, şifreli metnin anlaşılmazlığı da veriyi ortaya çıkarmaktadır. Bu, saldırganın dikkatini kolayca çekebilir, böylece saldırganın, iletişimin içeriğini deşifre etmek veya iletişim sürecini tahrip etmek için çeşitli yollar kullanması ve bunun sonucunda da veri aktarımının başarısız olmasına yol açmasına neden olabilir. Bilgisayar sistemlerinin yetenekleri artmaya devam ettikçe, bir anahtar sistemi veya bir genel anahtar sistemi kullanıp kullanmadığına bakılmaksızın, anahtar uzunluğunu artırarak sistem güvenliğini artıran geleneksel şifreleme yöntemleri giderek güvenilmez hale gelmiştir. Bu nedenle, kamuflaj özelliklerine sahip yeni ortaya çıkan veri güvenliği teknolojisi olan verinin gizlenmesi yöntemi ortaya çıktmıştır. Bu, gizli iletişimin etkili bir aracı haline gelmiştir ve uluslararası araştırmalarda hızla sıcak bir araştırması konusu haline geldmiştir.

Veri gizleme teknolojisi geleneksel kriptografiden farklıdır, çünkü çoklu ortam verilerinin fiziksel görünümünde önemli değişikliklere neden olmadan, çoklu ortam verilerindeki gizli verileri gizlemek için çoklu ortam verisinin her yerde bulunan

yedekliliğini kullanır. Engellenen kişi gizli verinin varlığını bilse bile, izinsiz olarak veriye erişmesi zordur, böylece gizli verilerin gizliliği ve güvenliği sağlanır. Şu anda, veri gizleme teknolojisi temel olarak aşağıdaki alanlarda kullanılmaktadır:

- Veriyi gizleme gizli bir iletişim yöntemidir ve askeri, istihbarat ve ulusal güvenlik açısından büyük bir öneme sahiptir. Artık bilgisayar saldırısı teknolojisi, çeşitli ülkelerin askeri alanına girmiştir ve bazı ülkeler ağ araştırmaları, izleme ve diğer ülkelerin istilalarını önlemek için açıkça ağ güçleri kurmuştur. İletişim kurmak için veri gizleme teknolojisini kullanarak, bu casusluk davranışlarından kaçınmak çok iyidir, böylece ulusal güvenlik açısından önem taşıyan gizli veriler kolayca sızdırılmaz.
- İsimsiz (anonim) iletişim. Birçok ülke ve finans kurumu, elektronik seçimlerde, elektronik para programlarında ve adsız posta protokollerinde üçüncü şahıslar tarafından izlenmesi zor olan anonim iletişim teknolojilerini kullanır, böylece kullanıcıların gizliliği etkin bir şekilde korunur.
- Telif hakkı koruması. Dijital teknoloji, multimedya verilerinin (resimler, metin, ses, video vb.) saklanmasını, kopyalanmasını ve dağıtılmasını kolaylaştırır. Ortaya çıkan korsanlık sorunları ve telif hakkı tartışmaları giderek daha ciddi sosyal problemler haline gelmiştir. Önemli bir veri gizleme teknolojisi dalı olan sayısal damgalama, sahibinin telif hakkı verilerini multimedyaya yerleştirmek için kullanılan bir yöntemdir. Yasadışı ihlali tespit etmek ve asıl sahibi ile kovuşturmak için bir kanıt olarak kullanılır, böylece fikri mülkiyet haklarının korunmasında etkili bir araç haline gelmiştir.
- Printed Basılı maddelerin sahteciliğini tespit etme ve önleme. Basılı maddelerin sahteciliği önlemek için kullanılan veri gizleme teknolojisi, son yıllarda önerilen yeni bir konudur ve birçok yayıncı ve ilgili ürün veren tarafından benimsenmiştir. Yöntem, sayısal görüntüyü yazdırmadan önce bazı gizli verileri yerleştirir. Yazdırılan kağıt giriş için tekrar taranabilir ve görüntü çalışmasının gerçekliği belirli bir kurtarma ve ayırt etme algoritması ile doğrulanır.

Teknolojinin hızlı gelişimi ile dijitalleşme her gün yaşamımızda her yerde bulunur. Görüntüler gibi birçok sayısal veri, birçok avantaj nedeniyle ağ üzerinden giderek daha fazla paylaşılmaktadır. Birçok kolaylık sağlamanın yanı sıra, sayısallaştırma, özellikle iletilen verilerin orijinalliğini ve bütünlüğünü kurcalama ve yetkisiz erişim gibi saldırılara karşı korumak açısından da yeni zorluklar getirmektedir. Kötü amaçlı saldırıları önlemek için her zamankinden daha güçlü bir sayısal veri koruma mekanizmasına ihtiyaç duyulmaktadır.

Sayısal görüntü damgalama çeşitli şekillerde yapılabilir. Bu çalışmada damga olarak kullanılan sayısal veriler, kapak veri adı verilen başka bir sayısal veride gizlemek için kullanılmıştır. Gömme işlemi sırasında kapak verinin hiçbir şekilde bozuk olmamasına dikkat edilmelidir. Yukarıda belirtildiği gibi, sayısal damgalama işlemi iki girdi verisini; kapak veriyi ve damgayı içerir. Sayısal veri herhangi bir veri türü olabilir. Temel sayısal görüntü damgalama iki işlem içerir: gömme işlemi ve çıkarma yada kurtarma işlemi.

Gömme işlemi, belirli bir gömme algoritması kullanarak damga verisini kapak verisine ekler. Gizli sayısal verileri damgalı verilerden çıkarmak için bir algoritma kullanmak gerekir.

### 1.1. Veri Gizleme Teknolojisi Araştırması

Veri gizleme [1,2,3] stegnografi olarak bilinmektedir, kısaca bir verinin diğer bir veri içinde gizlenmesi olarak tanımlanabilir ve gizlenmiş veri sadece hedef alıcı tarafından kurtarılabilir. Hedef alıcı hariç insanlar veri gizlenmiş olduğunu bilemez. Buradaki temel amaç verinin varlığını saklamaktır.

Veri gizleme teknolojisi uzun bir geçmişe sahiptir. Uzun zaman önce insanlar, verileri yabancılardan veya düşmanlardan saklamak amacıyla çeşitli yöntemler geliştirmişlerdir. Örneğin, MÖ 440'da, Histaieus adlı bir kişi, gizli verisini iletmek için saç maskeleme yöntemi kullanmıştır; 17. yüzyıl görünmez mürekkebi: belirli harfler üzerinde çok küçük lekeler yapmıştır, 19. yüzyıl mikrofilm, kimyasal olarak uygulanan

ileri steganografi tekniği - iyot suyunun püskürtülmesinden sonra kahverengi fontu gösteren, kalem lekeli nişasta suyuyla beyaz kağıda yazılmış; Çin edebiyatındaki Tibet şiiri, veri gizleme teknolojisinin klasik bir uygulamasıdır.

Bununla birlikte, internet tarafından temsil edilen veri çağında, veri işleme teknolojisi, sinyal işleme ve yayılı spektrum iletişimi gibi çok-profesyonel teknolojilerin araştırma yönünü kapsayan algısal bilim, veri teorisi ve şifreleme gibi birçok alanda yer almıştır. Küresel veri teknolojisinin hızlı bir şekilde gelişmesiyle birlikte, fikri mülkiyet haklarını koruma ihtiyacının artması ve şifreleme teknolojisinin kullanımındaki sınırlamalar nedeniyle, dünyadaki veri gizleme teknolojisi araştırmaları hızla artmıştır. Akademik değişimleri kolaylaştırmak için, 30 Mayıs - 1 Haziran 1996 tarihleri arasında Cambridge, İngiltere'de düzenlenen ilk uluslararası veri gizleme seminerinde saklanan bazı İngilizce terminoloji ve disiplin veri dallarının birleştirilmesi ve standardizasyonu ile ortaya çıkan disiplinler arası konu - veri gizleme resmen doğar. Uluslararası akademik topluluk aynı zamanda veri gizleme teknolojisi üzerine birçok makale yayınlamıştır. Birçok etkili uluslararası konferans (IEEE ICIP, IEEE ICASSP, ACM Multimedya, vb.) ve bazı uluslararası yetkili akademik dergilerde veri gizleme teknolojisiyle ilgili başlıklar yayınlanmıştır.

Veri gizleme teknolojisinin çeşitli uygulama alanları için, Cambridge Üniversitesi, NEC Amerikan Enstitüsü ve MIT Araştırma Üniversitesi'ndeki uzmanlar ve araştırmacılar birçok etkili algoritma önermişlerdir. Günümüzde, veri gizleme teknolojisi üzerine çok fazla araştırma yapılmaktadır. Avrupa'daki TALISMAN ve OCTALIS gibi bazı uluslararası standart projeler, önemli bir araştırma konusu olarak veri gizleme teknolojisini de içermektedir. Hedef, Avrupa'daki büyük ölçekli ticari ihlal ve korsanlık için telif hakkı koruma mekanizması ve koşullu erişim mekanizmaları sağlamaktır.

### 1.2. Damgalama Tarihi

Damgalama konsepti, ilk önce 1200'lerde kağıt üreticileri tarafından icat edilmiştir ve kağıt üreticisini ve kağıt boyutunu tanımlamak için kullanılmıştır [4]. 18. yüzyılda para

biriminin ve diğer belgelerin sahteciliğini önlemek için damgalama kullanılmaya başlanmıştır. Sahteciliği önlemek amacıyla para birimlerine veya belgelere gömülebilecek desenleri tespit etmek için Szepnaski [5] tarafından ilk sayısal damgalama yöntemi ortaya konulmuştur. Daha sonra, verileri bir ses sinyaline gömme işlemi Holt et al. [6] tarafından geliştirilmiştir. O zamandan beri, yıllar geçtikçe ilgili teknolojilerin gelişmesi ile damgalama yönemleri geliştmiştir ve sayısal verileri koruma amaçlı bir çok yeni damgalama yöntemi ortaya konulmuştur.

### 1.3. Problem Bildirimi ve Motivasyon

Sayısal görüntü damgalamanın tıbbi görüntüye uygulanması o kadar da kolay değildir. Çoğu uygulamada sadece tek bir algoritma kullanılarak piksel uzayında ya da frekans uzayında bazı yöntemler ortaya konulmuştur. Bu çalışmada her iki uzayda sıkça kullanılan damgalama algoritmaları birleştirilmiştir.

Bu çalışmada ana motivasyon tıbbi görüntü için daha sağlam bir damgalama şeması geliştirmektir. Tıbbi görüntü için gerekli güvenliğini sağlamak amacıyla, her iki uzayın geleneksel olarak kullanılmış algoritmalarını birleştirerek yeni bir damgalama şeması geliştirilmiştir. Tıbbi görüntü, her bir renk bileşenine farklı algoritmalar uygulayarak bir RGB görüntüsüne gizlenmiştir. Bu, karmaşıklığı artırmaktadır ancak saldırılara karşı güvenlik sağlamıştır.

### 1.4. Kullanılan Materyaller

Bu çalışmada, kapak görüntüsü olarak RGB görüntüleri ve damga görüntüsü olarak tıbbi görüntü kullanılmıştır. Kodlama ve simülasyon ise Matlab2016 ortamında yapılmıştır. Görüntüler kullanıma açık sitelerden indirilmiştir.

### 1.5. Tez Hedefleri ve Ozganizasyonu

Tıbbi görüntü için bir sayısal görüntü damgalama şeması geliştirmek, bu görüntü araştırmasının temel amacıdır. Bunun yanı sıra;

- Yeni sayısal görüntü damgalama düzeninin görüntüler üzerindeki etkisini ve algılanabilirliğini değiştirip değiştirmediğini incelemek
- Arnold Scrambling algoritmasının tıbbi görüntü üzerindeki etkisini ve güvenliği nasıl arttırdığını tespit etmek
- PSNR ve NC gibi performans ölçüm faktörlerini karşılaştırarak saldırılara karşı dayanıklılığı ve saldırıların etkisi üzerinde analiz yapmak

Tezin devamı aşağıdaki gibi düzenlenmiştir. 2. Bölümde, tıbbi görüntüler için sayısal görüntü damgalama yöntemleri açıklanmıştır. 3. Bölümde, bu çalışmada kullanılan damgalama algoritması ayrıntılı olarak açıklanmıştır. Önerilen sayısal görüntü damgalama şeması test edilmiş ve simülasyon sonunda elde edilen sonuçların analizi yapılmıştır. Son bölümde, önerilen damgalama tekniği ile ilgili sonuçlar incelenmiş ve gelecekteki olası çalışmalar için öneriler ortaya konulmuştur.

# BÖLÜM 2. KAYNAK ARAŞTIRMASI

## 2.1. Tıbbi Görüntü İçin Sayısal Görüntü Damgalama

Teknolojinin ilerlemesiyle tıbbi görüntü paylaşımı yaygınlaşmış ve daha da sık kullanılmaya başlamıştır [7,8]. Wong et al 1995 yılında tıbbi görüntü gerçekliği ve bütünlüğü üzerindeki çalışmasıyle ilgili makale yayınlamıştır [9].

Sayısal görüntü damgalama, veri güvenliğini koruma amaçlı geliştirildiğinden yaygınlık kazanmıştır. Sayısal görüntü damgalama, tıbbi görüntünün depolandığı ve internet üzerinden paylaşıldığı görüntü kalitesini ve orijinalliğini korumayı amaçlar. Tıbbi görüntü kalitesi her ne pahasına olursa olsun korunmalıdır çünkü hastayla ilgili tıbbi veriler gizlilik içeriyor olabilir. Tıbbi görüntü damgalama veri sahibi doğrulama, indeksleme, erişim kontrolü, veri kaynak tanımlama gibi birçok amaçlı kullanılabilir [10].

Sayısal görüntü damgalamanın tıbbi görüntü işlemede oynadığı rol, görüntünün kalitesini kaybetmeden içeriğinin güvenliğini artırmaktır. Bu nedenle, tıbbi görüntü işlemede sağlam bir sayısal görüntü damgalama algoritması çok önemlidir. Ancak, muayeneyle ilgili alan tıbbi görüntüler için son derece önemlidir, bu nedenle sağlam sayısal görüntü damgalama, kötü amaçlı saldırıların etkisini en aza indirmeye yardımcı olabilir.

## 2.2. RGB Görüntü

RGB görüntüsü, üç boyutlu bir matristen oluşur. Örneğin, 200 x 100 x 3 gibi bir matristen oluşan görüntüde 200, sütün sayısını, 100 satır sayısını, 3 ise R, G ve B bilişenleri temsil eder.

Her katman matrisi (200x100x1/2/3), R / G / B'nin gri değerine karşılık gelir ve buradaki matris, renkli görüntüyü değil, yalnızca tek renkli ışığa karşılık gelen gri değeri temsil eder.

Sayısal görüntü çok boyutlu bir matristen oluşur. 8 bitlik bir görüntü için matris elemanı 0-255 (0 - 2 ^ 8-1) arasındadır. Matris içindeki öğeler piksel değerine karşılık gelir: Değer, pikselin gri değeridir, değer ne kadar büyükse, pikselin rengi o kadar beyaz / açıktır, değer ne kadar küçükse, pikselin rengi o kadar koyu / karanlıktır.

Görüntünün her bileşeni, gri tonlamalıdır, renkten bahsetmek anlamsızdır. Görüntünün R bileşenini kırmızı kanalı, B bileşenini mavi kanalı, G bileşeni yeşil kanalı göstermektedir. Bir dizi işlemden sonra, ekrandaki görüntü, renkli olarak gösterilir.

### 2.3. Sayısal Damgalama Yöntemleri

Sayısal damgala yöntemleri işlem yapıldığı uzaya göre piksel uzayı ve frekans uzayı olmak üzere ikiye ayrılır.

#### 2.3.1. Piksel uzayı

Piksel uzayında veri saklama, veriyi gizleme amacına ulaşmak için karşılık gelen piksel noktalarının değerlerini uygun şekilde değiştirmektir. Piksel uzayında en sık kıllanılan damgalama algoritması, En Değersiz Bit (LSB) algoritmasıdır.

##### 2.3.1.1. En değersiz bit (LSB)

LSB algoritması, kapak görüntüsünün en değersiz bitinde veriyi gizler. Bu teknoloji, yüksek kapasiteli verileri gizleyebilir ve uygulaması basittir. Ancak saldırı önleme özelliği yeterince güçlü değildir. Kapak görüntüde gizli verilerin gizlenip gizlenmediğini çözmek kolaydır, böylece güvenliği azaltır [11]. Güvenliği artırmak için başka algoritmalar geliştirilebilir.

Deshpande Neeta ve arkadaşları tarafından önerilen LSB, çıplak insan gözüyle fark edilemez, kapak veri görüntüsünün en değersiz bitleri verileri gizlemek için kullanılır [12].

Bu yöntemde, gizlenmesi amaçlanan verinin her biti, kapak verinin bir baytının son bitine yazılırak veri gizleme gerçekleştirilir. LSB yönteminde genel olarak ekleme en son bitlerde yapıldığından gizli veri içeren verinin değişim oranı çok yüksek değildir.

Bu yöntemin çeşitli versiyonu vardır, sadece son bitinde değil başka bitlerde de değişim yapılabilmektedir. Bu, gizli veri kapasitesini artırmayı amaçlar, ama kapak veride oluşan büyük değişiklikten dolayı algılayabilme olasılığı artar.

### 2.3.2. Frekans uzayı

Frekans uzayında veri gizlemeyi gerçekleştirmek için görüntü verileri bir dönüşüm işlemine tabi tutulur. Bir görüntünün düşük frekans bileşeni değiştirilirse, görüntünün görsel özellikleri büyük ölçüde değişecektir. Bu nedenle, gizli veri kodlaması için görüntünün orta ve yüksek frekans bileşenlerinde gizlenmesi daha uygundur. Ayrık Kosinüs Dönüşüm (DCT) ve Ayrık Dalgacık Dönüşümü (DWT) gibi dönüşüm yöntemleri vardır.

#### 2.3.2.1. Ayrık kosinüs dönüşümü (DCT)

DCT ilk olarak Ahmed, Natarajan ve Rao tarafından geliştirilmiştir [13]. Bu yöntem JPEG sıkıştırmasında da kullanılan bir dönüşüm yöntemidir. Temeli kosinüs dönüşümüne dayanır. Dönüştürülen sonuç sadece kosinüs terimini içerecektir, bu yüzden ayrık kosinüs dönüşümü olarak adlandırılır. Bir görüntüdeki ayrık kosinüs dönüşümü, görüntü hakkında birçok önemli görsel verinin DCT dönüşümünün katsayılarının küçük bir bölümünde toplanması özelliğine sahiptir. Görüntü işleme ve görüntü verisi gizleme teknikleri sadece iki boyutlu ayrık kosinüs dönüşümünü kullanır. İki boyutlu DCT dönüşümü denklem 3.1'de gösterilmiştir.

$$F(p,q) = a(p)a(q)\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2q+1)q\pi}{2N}\right] \quad (3.1)$$

Burada, $p = 0,1,\cdots,M-1; q = 0,1,\cdots,N-1$, Ters DCT ise Denklem 3.2'deki gibidir:

$$f(m,n) = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} a(p)a(q)F(p,q)\cos\left[\frac{(2m+1)p\pi}{2M}\right]\cos\left[\frac{(2n+1)q\pi}{2N}\right] \quad (3.2)$$

Burada ise, $m = 0,1,\cdots,M-1; n = 0,1,\cdots,N-1$, Yukarıda bahsedilen denklemlerde $a(p), a(q)$ Denklem 3.3'deki gibi ifade edilebilir:

$$a(p) = \begin{cases} \sqrt{1/M}, & p = 0 \\ \sqrt{2/M}, & p = 1,2,\cdots,M-1. \end{cases}, \quad a(q) = \begin{cases} \sqrt{1/N}, & q = 0 \\ \sqrt{2/N}, & q = 1,2,\cdots,N-1. \end{cases} \quad (3.3)$$

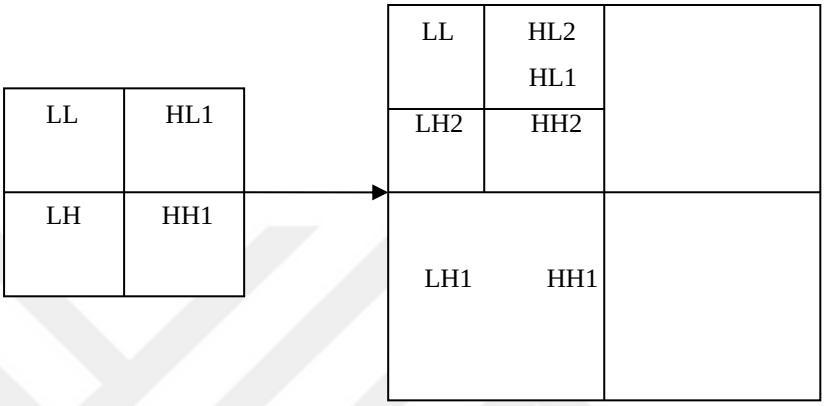
Bir görüntü üzerinde bir DCT dönüşümü gerçekleştirilir ve görüntüyle ilgili birçok önemli görsel veri, dönüştürülmüş katsayının (düşük frekans katsayısı) küçük bir bölümünde toplanır. DCT gizlemede, orijinal görüntü 8 × 8 piksel bloklara bölünür ve daha sonra her bir blok DCT dönüşümüne tabi tutulur [14]. Elde edilen katsayı matrisinde, görünmezliği ve dayanıklılığı sağlamak için orta frekans katsayısı tercih edilebilir.

### 2.3.2.2. Ayrık dalgacık dönüşümü (DWT)

DWT son yıllarda ortaya çıkan yeni bir sinyal analizi teorisidir. Frekans uzayında lokalizasyonunu sağlayabilen ve birçok alanda yaygın olarak kullanılan yeni yöntemdir. Sayısal görüntüler ayrık sinyallerdir, bu nedenle bu çalışmada DWT kullanılmıştır. DWT yöntemi ile kapak görüntüsü bloklara bölünür ve daha sonra her görüntü bloğu farklı dalgacık katsayıları seviyelerini elde etmek için tekrar DWT'ye tabi tutulur. Ayrıştırma işleminden sonra, görüntü kenarı ayrıntıları HH, HL ve LH alt bantlarında yoğunlaştırılır [15]. Bu alt bantlardaki daha büyük katsayılar genellikle

görüntünün kenarlarını temsil eder, bu nedenle damga yerleştirildikten sonraki algılanabilirlik daha iyidir, ancak bu alt bantların sayısı arttığında katsayının kaybolma olasılığı göreceli olarak büyüktür, bu nedenle gizli verileri orta ve düşük frekans katsayılarına gömmek daha avantajlıdır.

2D-DWT Şekil 3.1.'deki gibi gösterilebilir.




Şekil 2.1. 2D-DWT

Dönüşüm alanına gömülü olan gizli görüntü enerjisi, alandaki tüm piksellere eşit olarak dağıtılabilir; bu, gizlenen verinin görünmezliğini sağlamada faydalıdır. Ayrıca, gizli veriler çeşitli gürültü saldırılarına ve sıkıştırma işlemlerine etkili bir şekilde direnebilir ve bu nedenle dayanıklılık açısından nispeten güçlüdür [16]. Bununla birlikte, gizli veri kapasitesi sınırlıdır ve bu da büyük veri gizleme işlemini zorlaştırmaktadır.

## 2.4. Sayısal Görüntü Damgalama Özellikleri

Sayısal damgalama özellikleri aşağıdaki gibi özetlenebilir.

- Görünmezlik: Veri gizleme tekniği ile işlenen görüntünün, insan görsel sistemleri ile algılanılmaması anlamına gelen görünmezlik, verilerin belirgin bir şekilde bozulmaması ve gizli verilerin görülmemesi gerekir. veya yapay olarak duyulduğunda, bir kişinin görsel veya işitsel algısı, kapak verisi ile gizli veri arasında ayrım yapamaması gerekmektedir. Bu veri gizleme teknolojisinin

en temel özelliği ve şartıdır. Görüntü verisinin gizlenmesi için, görünmezlik oldukça önemlidir.

- Belirlenemezlik: Gizli verilerin örtük verilerle aynı matematiksel özelliklere sahip olduğu anlamına gelir; bu, tutarlı bir istatistiksel gürültü dağılımına sahip olmasını sağlar, böylece yasadışı işlemleri önler, çünkü veri özelliklerinin matematiksel analizi sırasında bile gizli verilerin olup olmadığı bilinmez.
- Sağlamlık: Gürbüzlük olarak da bilinir. Gizli veri dosyasında yapılan bazı değişiklikler nedeniyle gizli verilerin kaybolmasına karşı koybilme kabiliyetini ifade eder. Burada bahsedilen değişiklikler şunları içerir: iletim sırasındaki kanal gürültüsü, filtreleme işlemleri, yeniden ölçekleme, kırpma, kayıplı sıkıştırma, döndürme ve kesme.
- Asimetri: Bazı durumlarda, veriyi gizleme teknolojisinin amacı, kapak verisine bazı verileri yerleştirmektir ve veri erişiminin zorluğunu arttırmak istenmez. Bu nedenle, erişim zorluğunun arttırılmadığından emin olmak için asimetrik gizli veri kodlamasının kullanılması tercih edilir.
- Kendini kurtarma: Bazı işlemlerden veya dönüşümlerden sonra, önemli verilere daha fazla zarar görebilir. Fakat kalan küçük bir parça ile veri kurtarma işlemi yapılabilir, gizli veri hala kurtarılabilir ve kurtarma işlemi ana veri sinyalini gerektirmez. Buna kendini kurtarma denir.

Bir özellik bir başkasıyla karşı karşıya kalabilir. Artan damgala gücü sağlamlığı artırabilir ancak orjinalına uygunluğunu azaltır [17].

Araştırma süresinin sınırlı olması gibi çeşitli nedenlerle, bu makalede temel olarak sayısal görüntü gizleme teknolojisinin önemli özelliklerinden, görünmezliği, belirlenemezliği ve sağlamlığı üzerinde, simülasyon sonuçlarına göre analiz yapılır

### 2.5. Arnold Dönüşümü

Arnold dönüşümü, Arnold'un genel olarak Arnold'un kedi haritası dönüşümü olarak bilinen ergodik teoride önerdiği bir dönüşümdür.

Verileri gizlemeden önce karıştırmak, verileri düzensiz ve sistematik hale getirir ve bu nedenle iletim daha güvenli olacaktır [18]. Damgalama için ekstra güvenlik sağlamak amacıyla Arnold, ön işlemlerde kullanılır. Kedi haritası olarak da bilinen Arnold periyodik bir süreçtir. Ve görüntünün piksel pozisyonlarını değiştirerek bir şifreleme tekniği olarak hareket eder. Daha da önemlisi, saldırgan, şifreleme algoritması hakkında yeterli veriye sahip olmadan damgalamayı çıkaramaz. Bu yüzden Arnold damgalamaın güvenliğini arttırır ve önerilen yöntemin sağlamlığını arttırır. İki boyutlu çırpma aşağıdaki gibi tanımlanabilir:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{3.4}$$

Burada x, y∈ {0,1,2 ,. . . , N-1}, (x, y), görüntü matrisinin bir elemanı dönüştürülmeden önceki ve (x ', y') dönüşümden sonraki yeni bir pozisyonu temsil ettiği konumu temsil eder. F görüntüsündeki tüm pikseller üzerinde bir Arnold dönüşümü gerçekleştirmek bir Arnold dönüşümü tamamlar.

# BÖLÜM 3. KULLANILAN YÖNTEM VE SİMÜLASYON ANALİZİ

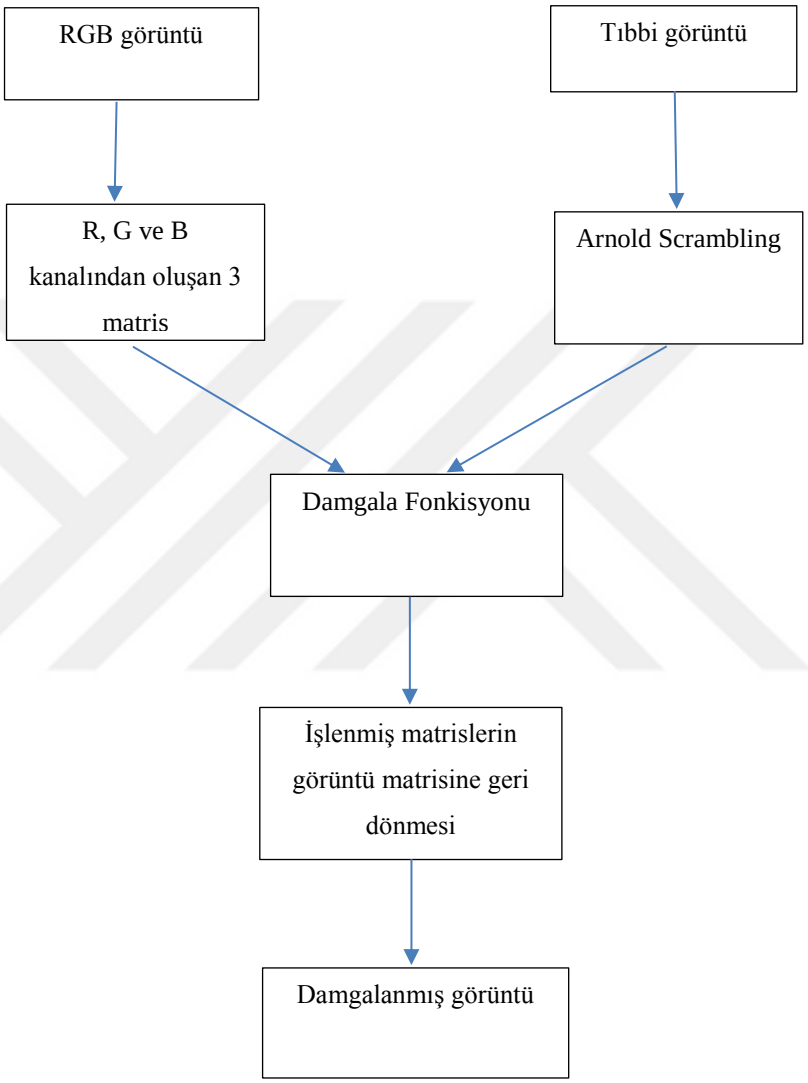
## 3.1. Damgalama İşlemi

Önerilen sayısal görüntü damgalama şeması iki görüntüden oluşur; bunlardan biri damga görüntüsü olarak seçilen tıbbi görüntü ve damga görüntüsünün gömüleceği kapak görüntüsüdür. Bunlar Şekil 3.1. ve Şekil 3.2.'de gösterilmiştir. Kapak görüntüsü 512x512 boyutunda, tıbbi görüntü ise 39x39 boyutunda seçilmiştir.

Şekil 3.1. Kapak görüntüsü

Şekil 3.2. Damga görüntüsü

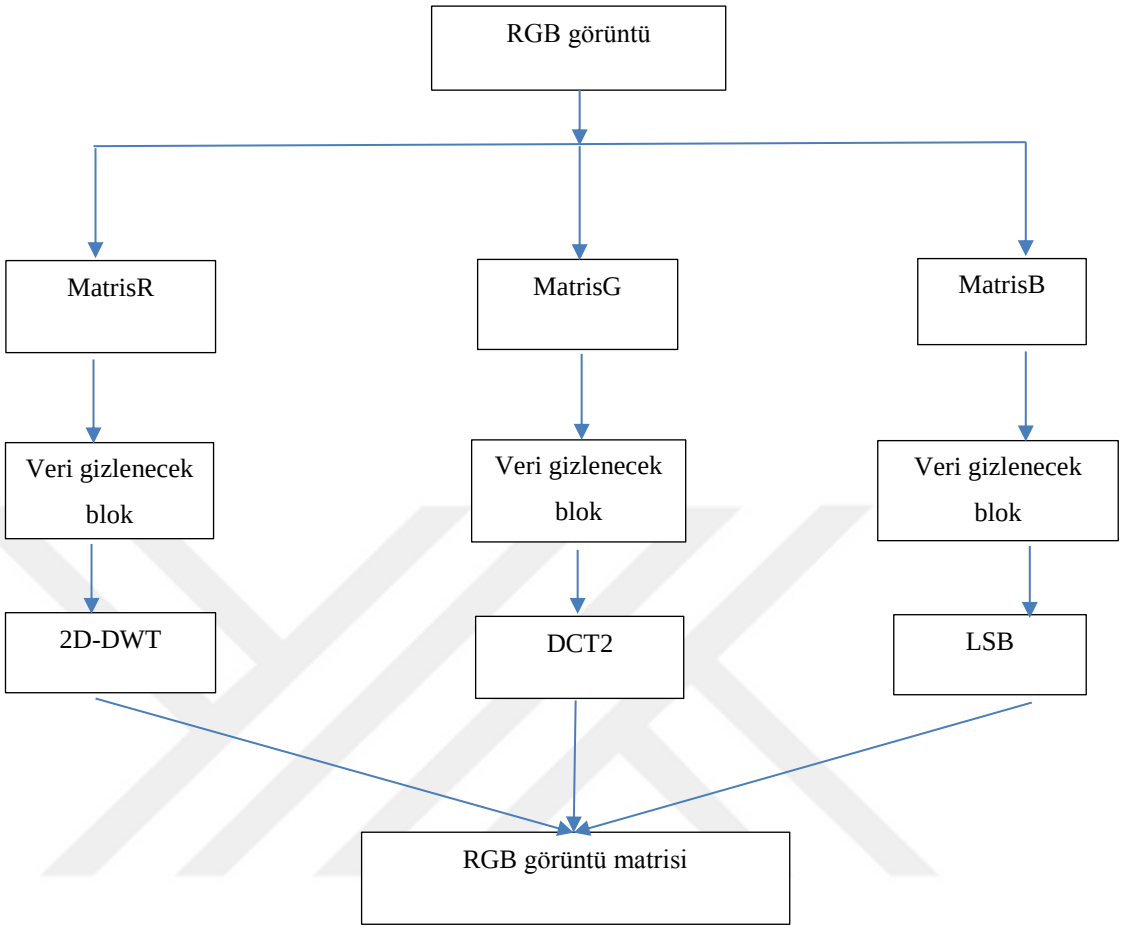
Sayısal damga oluşturma işlemi Şekil 3.3.'teki blok diagramı ile gösterilmiştir. İlk olarak seçilen tıbbi görüntü gri seviyeli görüntüye dönüştürülür. Bu görüntünün boyutu isteğe bağlı olarak değiştirilebilir. RGB kapak görüntüsü, R, G ve B kanallarına ayrıştırılır ve her kanal bir matrisi temsil eder.




Şekil 3.3. Damgala

Damgalama Fonkisyonu daha detayli bir şekilde açıklayacak olursak Şekil 3.4.'teki diyagram ile gösterilebilir.

Bir sonraki adımda, kapak görüntüsünün her pikseli 8 bit değerindeki ikili görüntüye dönüştürülür. Ve bu birleşenler R, G ve B'den oluşan üç boyutlu matrislerde saklanır.



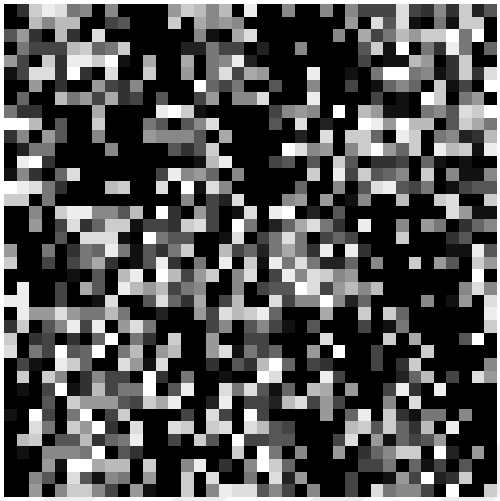

Şekil 3.4. Fonkisyon

Gömme işlemi ise renkli kapak görüntünün üç kanalından oluşan üç tane iki boyutlu matrislerde yapılır. Daha da açacak olursak, tıbbi görüntünün ilk 64x64 bitleri R matrisine gömülür, daha sonra DWT işlemine tabi tutulur ve MatrisR olarak kaydedilir. İkinci 64x64 bitleri ise G matrisine gizlenir, DCT işlemi yapıldıktan sonra MatrisG olarak adlandırılır. Geri kalan bitler de G kanaldan oluşan matrise gömülür. LSB ile veri gizleme işlemi yapıldıktan sonra MatrisB olarak kaydedilir. Şekil 3.5.'te kapak görüntüsünün R, G ve B kanallarına ayrılmış hali gösterilmiştir.


Şekil 3.5. Kapak görüntüsünün R, G ve B kanallarına ayrılmış hali

Bir sonraki adıma geçmeden önce Arnold algoritması ile tıbbi görüntünün piksellerinin yerleri değiştirilir ve gri seviyeli bir görüntü olarak kaydedilir (Şekil 3.6.).

Arnold algoritmasının iterasyon sayısı 250 olarak seçilmiştir. Daha sonra bu matris 64x64'lük matrislere dönüştürülür.



Şekil 3.6. Tıbbi görüntünün Arnold algoritması uygulandıktan sonraki hali

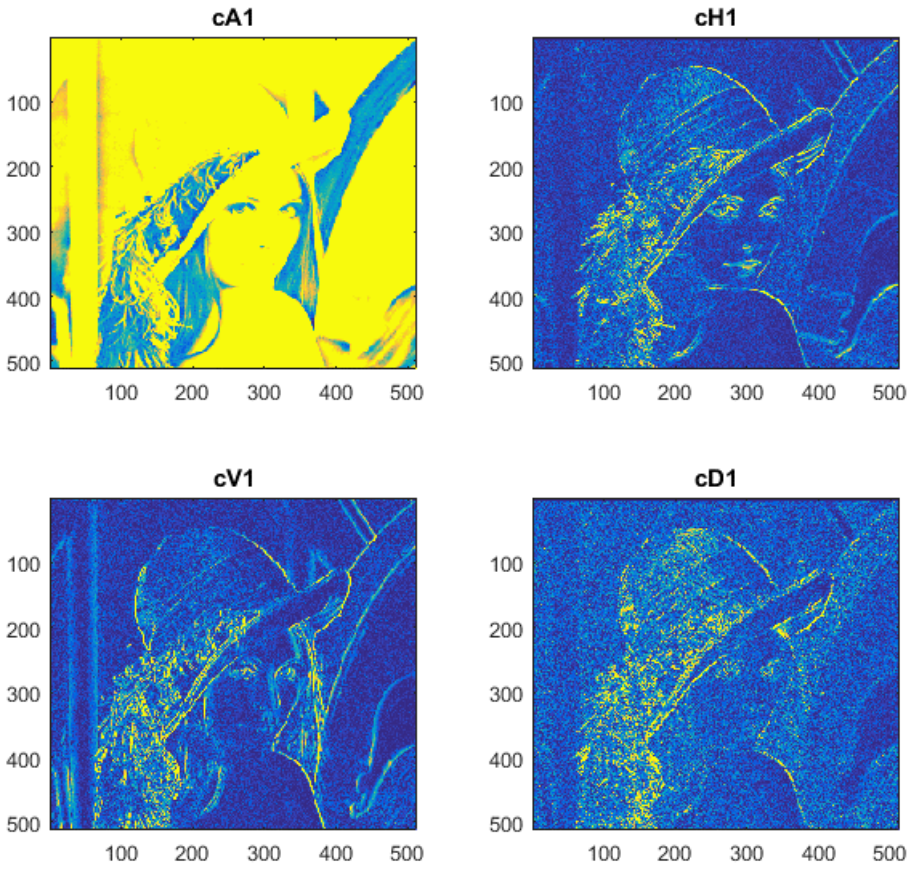
Son olarak, üç matrisin birleşimi kapak görüntüsünün kurtarılması için bir matrise konulur.

Şekil 4.4.'teki diyagram üç tane gömme işlemi içerir. Bunlardan DWT algoritmasının MatrisR'de uygulanması aşağıdaki gibi ifade edilebilir. Kapak görüntü 8 bloğa bölünür ve veri gizlenmek üzere seçilen blok tek seviyeli 2-D ayrık dalgacık dönüşümü (DWT) haar dalgacık kullanılarak işleme tabi tutulur. Bu işlem, cA katsayıları matrisini ve cH, cV ve cD matrislerini ayrıntı katsayılarını oluşturmak için yapılır (sırasıyla yatay, dikey ve çapraz).

Aşağıdaki Matlab kodu ile görüntü bloklara ayrılır.

```
[cA1,cH1,cV1,cD1]=dwt2(block,'haar')
```

İşlem sonunda Şekil 3.7.'deki sonuçlar elde edilir.

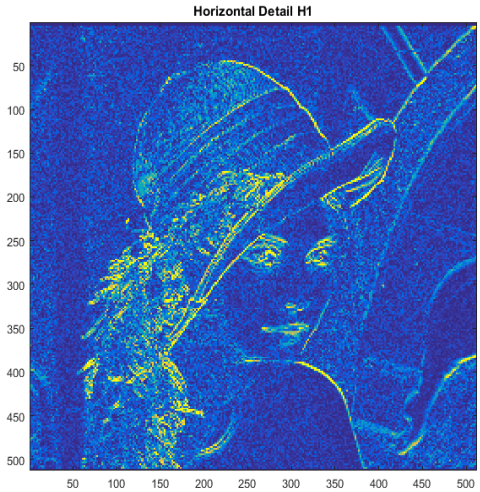



Şekil 3.7. Coefficiencies

Aşağıdaki matlab kodu ile ikinci DWT, Haar dalgacıkını kullanarak bloğun cH1 değerine uygulanır.

[cA2,cH2,cV2,cD2]=dwt2(cH1,'haar');

Bu işlemin sonucunda Şekil 3.8.'deki görüntü ortaya çıkar.



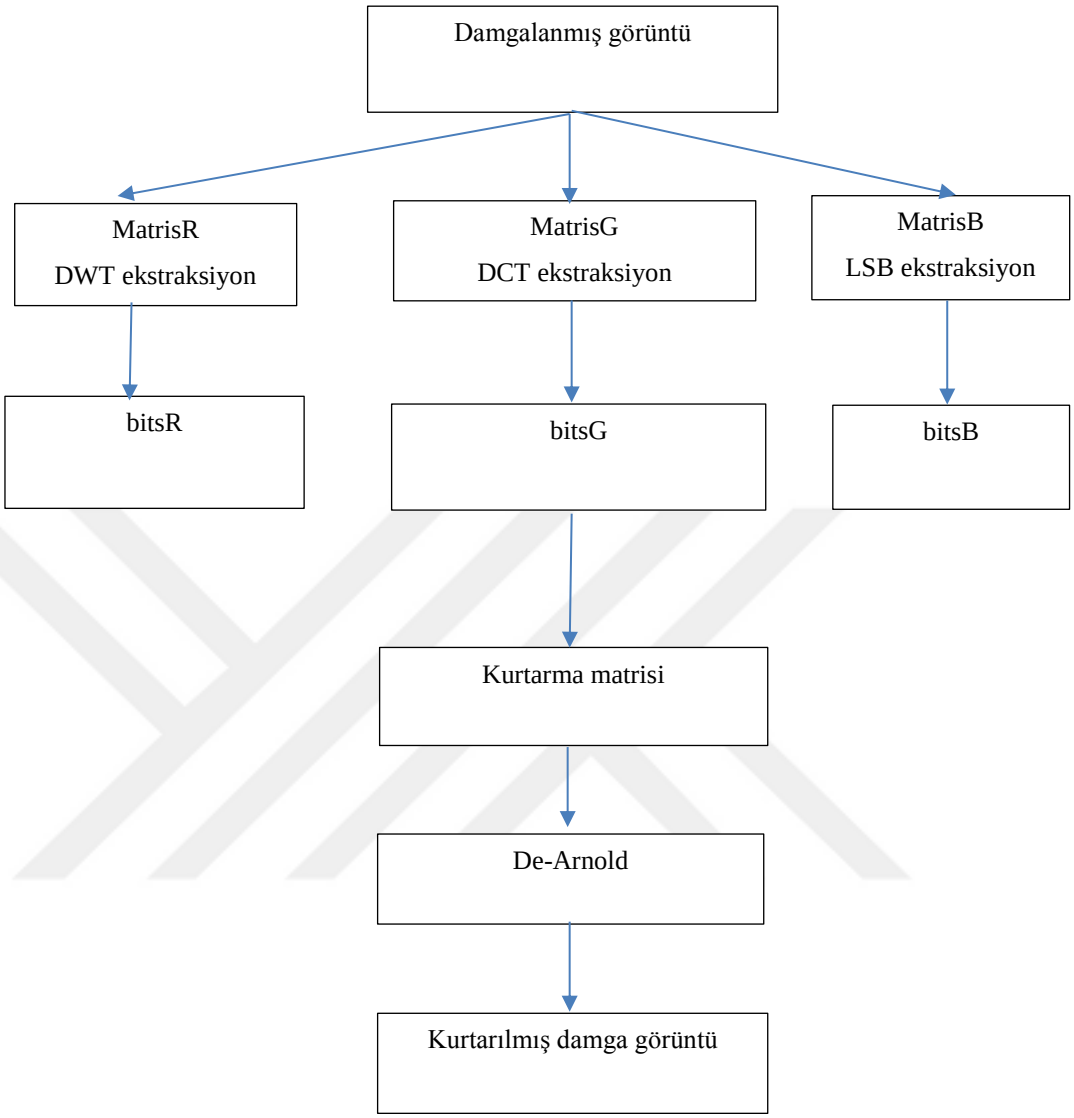

Şekil 3.8. cH1

Damgalama işlemi tamamlandıktan sonra Şekil 3.9.'daki damgalanmış görüntü elde edilmiştir.

Şekil 3.9. Damgalanmış görüntü

### 3.2. Damga Kurtarma

Damgalama işlemi bittikten sonra çıkarma yapılarak gömülen görüntü kurtarılır. Bu işlem Şekil 3.10.'deki diyagramda gösterilmiştir.




Şekil 3.10. Damga kurtarma

İlk olarak, damgalanmış görüntü R, G ve B'den oluşan matrislere ayırılır, veri gizleme işlemi sırasında ugulanan algoritmaların ekstraksiyon fonkisyonu ile orjinal görüntünin R, G, B kanalından olurşan matrislere dönüştürülür.

Asıl götüntüyü oluşturmak amacı ile, 64x64'lük bir boyutlu bitsR, bitsG ve bitsB matrisleri elde edilir. Yani üç asıl renk kanalından oluşan matrislerin değeri bir boyutlu matrislere konulur ve elde edilen 8 bitlik ikili birleşenler ondalık birleşenlere dönüştürülerek kurtarma matrisine konulur.

Ters Ayrık Dalgacık Dönüşümü (IDWT), orjinal görüntünün gömme işlemini bitirmeden önce dönüştürülmüş katsayıları yeniden elde etmek için IDWT gerçekleştirilir.

DCT gömme işleminde sayısal damga ile aynı boyutta matris göz önünde bulundurulur ve seçilen blokta DCT uygulanılarak gömme işlemi gerçekleştirilir. DCT'nin uygulandığı blokta Ters Kosinüs Dönüşümü (IDCT) gerçekleştirilir.

LSB'nin uygulanacağı matris 8x8 büyüklüğünde bloklara bölünmüştür. Farkın hesaplanması için son ikinci bit ve seçilen bloğun son biti alınır. Daha sonra sayısal damga gömülü matris orijinal matrise geri dönüştürülür.

Gömme esnasında işlem yapılmadan önce Arnold ile piksellerin yerleri değiştilidiği için, kurtarma aşamasında da yukardaki adımlardan sonra elde edilen görüntünün de aynı şekilde pikselleri dağılmış haldedir. Pikselleri asıl yerlerine getirmek için de De-Arnold yapılır ve böylece gömülem tıbbi görüntü yani damgaya Şekil 3.11.'deki gibi erişilebilir.

Şekil 3.11. Kurtarılan damga görüntüsü

### 3.3. Damgalama Kalite Değerlendirme Yöntemleri

Damga kurtarma işleminin uygunlanması sonucunda elde edilen görüntü kalitesinin belli yöntemlerle belirlenmesi birçok açıdan önem arzetmektedir. Sık kullanılan ve kabul edilen yöntemler aşağıdaki gibi gösterilmektedir.

#### 3.3.1. Tepe sinyal gürültü oranı (PSNR)

PSNR, tanınmış bir görüntü kalitesi göstergesidir. Görüntünün PSNR'si Denklem 3.1 kullanılarak gerçekleştirilir. PSNR (Tepe Sinyal Gürültü Oranı), bir sinyalin mümkün olan maksimum gücünün doğruluğunu etkileyen yıkıcı gürültü gücüne oranını temsil eden bir terimdir.

PSNR en yaygın sinyal kalitesi değerlendirme göstergesidir. Veri gizleme sistemi modeli iletişim sistemi modeliyle yakından ilişkili olduğundan, orijinal görüntü için, gizli veri rastgele gürültü olarak kabul edilebilir ve gürültü orijinal görüntünün kalitesini etkileyecektir. Teorik PSNR, sinyal gücü ve gürültü gücü için kullanılır. Görüntü verisini gizleme sistemi performansının değerlendirmesinde, PSNR değeri hesaplanır ve aşağıdaki gibi tanımlanabilir.

$$PSNR(dB) = 10\log_{10}\frac{D^2 MN}{\sum_{x=1}^{M}\sum_{y=1}^{N}(I(x,y) - I'(x,y))^2} \tag{3.1}$$

*D*, sinyalin tepe değeridir.

PSNR desibel (*dB*) cinsinden ölçülür. *PSNR*, aynı görüntü ile kurtarılan görüntünün sonuçlarını karşılaştırmak için iyi bir ölçüdür. *PSNR* değeri ne kadar büyük olursa, damga o kadar iyi gizlenmiş demektir [19].

### 3.3.2. Normalleştirilmiş korelasyon (NC)

Normalleştirilmiş korelasyon Denklem 3.2'deki gibi tanımlanabilir.

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j) - W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W'(i,j)]^2}} \tag{3.2}$$

Burada, $W$ orjinal görüntü, $W'$ ise damgalanmış görüntüdür ve $M_1$, $M_2$ ise görüntünün boyutudur. Normalleştirilmiş Çapraz Korelasyonun (*NC*) değeri 0 ve 1 arasında değişir ve Denklem 4.2 kullanılarak hesaplanır. $NC = 1$ ise gömülen damga ve çıkarılan damga aynıdır. Genel olarak, $NC > 0.7500$ ise önerilen yöntem kabul edilebilir [20]. Böylece $W'$nin kurtarılmış damga olduğu ve $W'$nin orjinal damga olduğu tespit edilir.

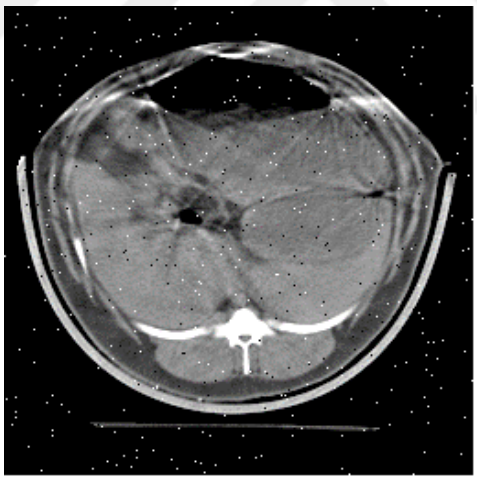
Önerilen yöntem Matlab ile uygulandıktan sonra elde edilen *dNC* değeri 0,9799 ve PSNR (*dB*) değeri 55,9463118 şeklindedir. Yani bu çalışmada geliştirilmiş yöntemin daha sağlam ve nispeten güvenli olduğu tespit edilmiştir. Orjinal damga görüntüsünün ve kurtarılan görüntüsünün görsel olarak aynı olduğu ifade edilebilir.

Yukarıdakı sonuç ise ideal ortamda, yani herhangi bir saldırıya maruz bırakılmadan elde edilmiştir. Fakat damgalamanın ne kadar dayanıklı olduğunu tespit etmek için damgalanmış görüntü bir takım saldırılara maruz bırakılarak PSNR ve dNC değerleri tekrar ölçülmelidir. Bu sebepten dolayı geliştirilmiş yöntem bir sonraki aşamada sıkça kullanılan saldırılara tabi tutularak performans kalitesi ölçülebilir.

Damgalanmış görüntüye tuz biber gürültüsü, kesme, döndürme ve ölçekleme gibi saldırılar uygulanmıştır. Tuz biber saldırısı uygulanırken parametre olarak 0.01 seçilmiştir. İşlem sonrası elde edilen görüntü Şekil 3.12.'de gösterilmiştir.

Şekil 3.12. Tuz biber saldırısı

Saldırıya maruz bırakılan görüntü kurtarma işlemine tabi tutulmuştur ve Şekil 3.13.'teki görüntü elde edilmiştir. İşlem sonucunda elde edilen görüntünün *dNC* değerinin 0.7684 olduğu tespit edilmiştir. Bu sonuç, önerilen yöntemin bu tür saldırıya kaşı dayanıklı olduğunu göstermektedir.



Şekil 3.13. Tuz biber saldırı sonrası kurtarılan görüntü

Damgalama işlemi yapıldıktan sonra elde edilen görüntüye kesme saldırısı uygulanmıştır. İşlem sonucunda elde edilen görüntü Şekil 3.14.'te gösterilmektedir.

Şekil 3.14. Kesme

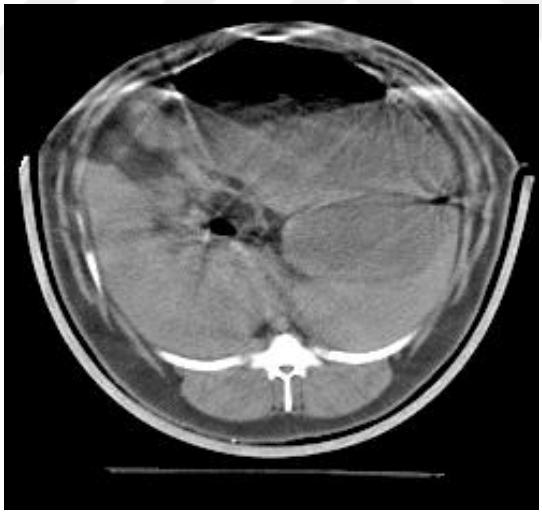
Kesme saldırısı uygulandıktan sonra kurtarılan tıbbi görüntü (Şekil 3.15.) ‘nün *dNC* değeri 0.77’dur. Bu da önerilen yöntemin kesme saldırısına karşı nispeten dayanıklı olduğunu göstermiştir.

Şekil 3.15. Kesme sonrası kurtarılan görüntü

Daha sonra, damgalanmış görüntü döndürme saldırıya maruz bırakılmıştır ve Şekil 3.16.’daki görüntü kaydedilmiştir.

Şekil 3.16. Döndürme

Saldırı sonrası kurtarma işlemi yapılmıştır ve kurtarılan tıbbi görüntü Şekil 3.17.'de gösterilmiştir. Elde edilen *dNC* değeri 0.76'dir. Bir önceki saldırı sonucu ile karşılaştırıldığında önerilen yöntemin yine bu tür saldırıya karşı da nispeten dayanıklı olduğu tespit edilmiştir.

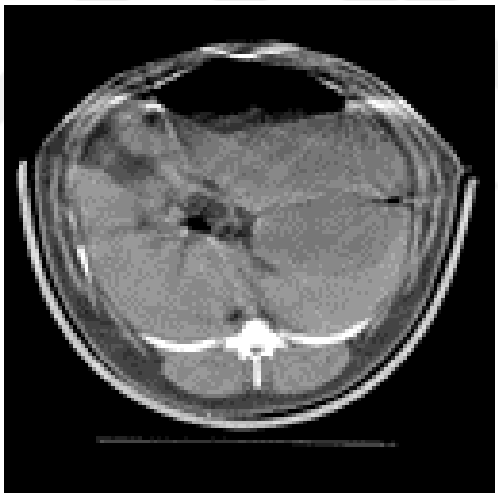


Şekil 3.17. Döndürme sonrası kurtarılan görünrü

Son olarak, damgalanmış görüntü ölçekleme saldırısı ile işlem yapılmıştır ve parametre olarak 0.75 seçilmiştir. İşlem sonunda Şekil 3.18.'deki görüntü elde edilmiştir.

Şekil 3.18. Ölçekleme

Ölçekleme saldırısı sonrası kurtarma işlemi yapılarak elde edilen görüntü Şekil 3.19.'da gösterilmiştir. Kurtarılan görüntünün *dNC* değerinin 0.77 olduğu tespit edilmiştir.



Şekil 3.19. Ölçekleme sonrası kurtarılan görüntü

Saldırı parametreleri isteğe göre seçilebilir ve elde edilen sonuç saldırı kuvvetine göre değişiklik gösterebilir.

# BÖLÜM 4. SONUÇ VE ÖNERİLER

## 4.1. Sonuçlar

Tezde tıbbi görüntü koruması için yeni bir sayısal görüntü damgalama algoritması ele alınmıştır. Önerilen damgalama şeması, RGB görüntüsünün her bir renk kanalından tam olarak faydalanarak, LSB, DWT ve DCT kullanarak frekans alanına gömülü damga sağlar.

Önerilen damga düzenlemesinin temel avantajları şunlardır:

- En çok kullanılan geleneksel algoritmalar birleştirilmiştir.
- Ek güvenlik sağlamak için Arnold işlemi damgalama esnasında kullanılmıştır.
- Hem dNC hem de PSNR kalite göstergesi olarak kullanılmıştır.

İnternet üzerinden paylaşılan tıbbi görüntü için yüksek seviye güvenliği, önerilen şema ile elde edilebilir, çünkü damga RGB görüntüsünün her bir bileşenine gömülüdür, bu da önerilen yöntemin saldırılara karşı daha dayanıklı olduğunu göstermektedir. Çıkarılan tıbbi görüntünün *dNC* değeri 0.95'ten büyüktür; bu, kurtarılan tıbbi görüntü ile aslının benzer olduğu anlamına gelir.

Önerilen damgalama yönteminin tespit edilmiş dezavantajları ise, bazı saldırılara karşı dayanıklılığın güçlü olmamasıdır. Saldırısız durumda kurtarılan görüntü 50 *db*'den daha büyük bir *PSNR* değerine sahiptir.

## 4.2. Öneriler

Önerilen yöntem, damga işlemi sırasında ekstra güvenlik artırıcı yöntemler eklenerek daha da iyileştirilebilir. Bazı saldırılara karşı dayanıklılığı artırmak için hem kapak görüntüsü hem de tıbbi görüntü daha küçük bloklara bölünebilir. Kurtarılan tıbbi görüntü küçük boyutludur, çünkü bu görüntü kurtarma esnasında kullanılan katsayıların yaklaşık değeridir. Tıbbi görüntü boyutu daha büyük ölçeklendirilebilir, böylece kurtarılan görüntünün boyutu da büyük olabilir.

## KAYNAKÇA


[1] N. F. Johnson and S. Katzenbeisser," .A survey of steganographic techniques", in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, pp.43-78. Artech House, Norwood, MA, 2000.

[2] Lou, D. C. and Liu, J. L. 2002. "Steganography Method for Secure Communications". Elsevier Science on Computers& Security, 21, 5: 449-460.

[3] J. Fridrich and M. Goljan, .Practical steganalysis of digital images-state of the art., Proc. SPIE Photonics West, Vol. 4675, pp. 1-13, San Jose, California, Jan. 2002.

[4] C. Ingemar, M. Matthew, B. Jeffrey. "Digital Watermarking", Morgan Kaufmann Publishers Inc. San Francisco, CA, USA © 2008.

[5] W. Szepanski. " A Signal Theoretic Method for Creating Forgery-proof Documents for Automatic Verification", in J. S. Jackson, editor, 1979 Carnaham Conference on Crime Countermeasures, pp. 101 - 109, 1979.

[6] L. Holt, B. G. Maufe, and A. Wiener. "Encoded Marking of a Recording Signal", U.K. Patent GB 2196167A, 1988.

[7] S. Calcote, "Developing a Secure Healthcare Information Network on the Internet," Healthcare Financial Manage, vol. 51, no. 1, pp. 68 - 76, 1997.

[8] H. Munch, U. Englemann, A. Schroter and H. P. Meinzer, "The Integration of Medical Images with the Patient Record and their Web Based Distribution", Journal of Academic Radiology, vol. 11, no. 6, pp. 661 – 668, 2004.

[9] S. T. C. Wong, M. Abundo, and H. K. Huang, "Authenticity Techniques for PACS images and Records," Proceedings of SPIE, vol. 2435, pp. 68 – 79, 1995.

[10] T. H. N. Le, K.H. Nguyen, H. B. Le, " Literature Survey on Image Watermarking Tools, Watermark Attacks, and Benchmarking Tools", Proceedings of the Second IEEE International Conferences on Advanced in Multimedia, pp. 67 – 73, 2010.

[11] Saravanan Chandran, Koushik Bhattacharyya “Performance Analysis of LSB, DCT, and DWT for Digital Watermarking application using Steganography”, EESCO,2015

[12] Frank Y.Shih, “Digital Watermarking and Steganography- Fundamentals and Techniques”, CRC Press 2008.

[13] Juan RH: Statistical analysis of watermarking schemes for copyright protection of image. IEEE. (1999).

[14] Y. Qianli, C. Yanhong, “A Digital picture watermarking Algorithm Based on Discrete Wavelet Transform and Discrete Cosine Transform2012, pp. 1102-1105.

[15] W. Hong and M. Hang, "Robust Digital Watermarking Scheme for Copy Right Protection," IEEE Trans. Signal Process, 2006.

[16] S. Mallat, “A Theory for Multiresolution Signal Decomposition: The Wavelet Representation”, IEEE Pattern Analysis and Machine Intelligence, vol. 11, no. 7, pp. 674 -693, 1989.

[17] Katzenbeisser S. and Petitcolas F. A. P., (2000) “Information Hiding Techniques for Steganography and Digital Watermarking”, Artech House, UK

[18] Razieh Keshavarziana; Ali Aghagolzadehb “ROI based robust and secure image watermarking using DWT and Arnold map" published in Int. J. Electron. Commun. (AEÜ) 70 (2016) 278–288.

[19] Chandra Mohan B., Veera Swamy K. and Srinivas Kumar S., (2011) “A Comparative performance evaluation of SVD and Schur Decompositions for Image Watermarking ”, IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI) (14), pp 25–29.

[20] Yusuf Perwej, Firoj Parwej and Asif Perwej., “An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection” , The International Journal of Multimedia & Its Applications (IJMA) Vol.4, No.2, April 2012

# ÖZGEÇMİŞ

MAIMAITIMING MAMUTI, Çinde doğdu. Üniversite eğitimini Pekin'de tamamladı. Halen Sakarya Üniversitesinde Bilgisayar Mühendisliği bölümünde yüksek lisans yapmaktadır.