DCT VE DWT TEKNİKLERİ İLE GÖRÜNTÜ VE METİN VERİSİ GİZLEME

Faruk TAKAOĞLU
İstanbul Aydın Üniversitesi, Türkiye
faruktakaoglu@gmail.com
https://orcid.org/0000-0003-0828-2017

Mustafa TAKAOĞLU
İstanbul Aydın Üniversitesi, İstanbul
mustafatakaoglu@aydin.edu.tr
https://orcid.org/0000-0002-1634-2705

ÖZ

Steganografi tarihte gizli yazma sanatı olarak bilinmektedir. Günümüzün gelişen teknolojik ilerlemesi içerisinde kendisine iletişim alanında yer bulmuştur. Herhangi bir mesajı içeriğinin görünmesini istemediğimiz durumlarda steganografi kullanılır. Diğer bir güvenlik unsuru olan kriptoloji bilimi ile birçok zaman karıştırılmaktadır. Kriptoloji bilimi mesajın içeriğini veya unsurlarını okunamaz hale getirmekle uğraşırken steganografi mesajın görünemez, farkına varılamaz olmasına gayret sarf etmektedir. Bu doğrultuda makalemizdeki amacımız, steganografi ve onun en çok kullanılan yöntemlerinde olan ayrık kosinüs dönüşümü "DCT" ve ayrık dalgacık dönüşümü "DWT" yöntemlerinin uygulanması ve sonuçların karşılaştırılmasıdır. Bu amaca erişmek için MATLAB platformunda DCT ve DWT yöntemleri kodlanmış ve steganografi yapmaları sağlanmıştır. Makalenin ikinci bölümünde yüksek sinyalin gürültüye oranı "PSNR", ortalama hataların kareleri toplamı "MSE" ve Z skor "Z-score" yöntemleri aynı platformda performanslarını ölçmek için kodlanmıştır. Bu performans parametrelerinden elde edilen değerler sonuç bölümümüzde gösterilmiş ve DWT yönteminin DCT yöntemine göre daha başarılı sonuçlar verdiği saptanmıştır.

Anahtar Kelimeler: *Steganografi, DCT, DWT, Z-skor*

Geliş Tarihi: 14.04.2020, Kabul Tarihi: 30.04.2020, DOI NO: 10.17932/IAU.IAUD.2009.002/iaud_v12i3001
Araştırma Makalesi-Bu makale Turnitin programıyla kontrol edilmiştir.

HIDING IMAGE AND TEXT DATA WITH DCT AND DWT TECHNIQUES

ABSTRACT

Steganography has been known as secret writing in history. It has found a place for itself in the communication technology area with the help of the rapid growing of our era's technological developments. It has more applications in different fields in recent years. If we don't want to show the inside of any message, then we must use steganography. Most of the time, it is confused by cryptography. While cryptology is trying to make the content or elements of the message unreadable, steganography strives to make the message invisible, unnoticeable. Accordingly, our purpose in this article is to explain the steganography, and it's mostly used branches, which are Discrete Cosinus Transformation, simply DCT, and Discrete Wavelet Transformation, simply DWT. To reach that purpose, we described both DCT and DWT in the MATLAB platform. After that, we coded Peak Signal to Noise Ratio, simply PSNR, Mean Square Error, simply MSE, and Z score for estimating the performances of DCT and DWT. According to those performances, we decided which one of the steganography branches are more successful. After performance analyses, it has been determined that the success of DWT is better than the success of DCT.

Keywords: *Steganography DCT, DWT, Z-Score*

GİRİŞ

Steganografi Latincede gizli anlamındaki steganos ve yazma anlamındaki graphein kelimelerinden türetilmiştir. Gizli yazma anlamındaki bu bilimin amacı, gizli olduğuna inanılan tüm verilerin masum bir taşıyıcı içerisine, sadece alıcının farkına varabileceği bir şekilde yerleştirmektir. Tarih boyunca gizli haberleşme, çeşitli yöntemlerle önemli olduğuna inanılan tüm bilgiler için kullanılmıştır. Eski Yunan uygarlığında Pers İmparatorluğu istilasına karşı haberleşme ihtiyacı, kafaları kazınan kölelerin kafa derisine yazılan mesajlarla yapılmaktaydı. Köleler saçları uzadıktan sonra mesajın iletilmesi gereken yerlere doğru seyahat ederler ve böylelikle mesajlar hedeflere ulaşırdı. İlerleyen zamanlarda gizli mesajlar gazete, dergi gibi yazılı medya unsurlarının gelişmesi ile haberleşme metinler arasına saklanarak gönderilmeye başlandı. Son zamanlarda ise sosyal medya aracılığı ile gizli haberleşmelerin sıkça yapıldığı bilinmektedir. Günümüzde birçok sektörde legal veya illegal amaçlarla steganografi içeren haberleşme yöntemleri kullanılmaktadır. Legal kullanıma örnek, devletlerin istihbarat teşkilatlarının, iletişim kanallarının dinlenme olasılığına karşı bu yöntemi kullanmasıdır. Diğer bir taraftan, illegal örgütler steganografi yardımı ile güvenlik güçlerinin haberleşmelerinin farkına varmasını engellemeye çalışmaktadır. Steganografinin alt dalları aynı zamanda dijital ürünlerin sahiplik veya aitliklerinin ispatlanması

için de günümüzde yaygın olarak kullanılmaktadır. Ancak çağımızda hızla ilerleyen iletişim teknolojileri ve ürünlerinin önem kazanması ile gizli haberleşme yöntemlerinin daha da önem kazanacağı düşünülmektedir. Bu yüzden bu makale çalışmamızda steganografi biliminin ana uygulama alanı olan gizli haberleşme yönteminden bahsedeceğiz (Anderson ve Petitcolas, 1998: 478).

Steganografi yapılması için öncelikle bir gizli veri ve taşıyıcı unsur belirlenmelidir. Gizli verimiz bir metinsel veri veya ufak bir resim verisi seçilebilir. Bu verilerin büyüklükleri taşıyıcı unsurun büyüklüğü ile doğru orantılıdır. Eğer hedefine ulaşmasını umduğumuz gizli verinin, taşıyıcı verisi, boyut olarak ufak ise gizli verimiz bu taşıyıcı verinin yarısından ufak olmalıdır. Taşıyıcı verimiz veya bir diğer adı ile masum veri, günlük olarak internette çokça gördüğümüz multimedya unsurlarından biri olabilir. Bu ögeler resim dosyaları, ses ve müzik dosyaları veya video dosyaları olabilir. Taşıyıcı unsur ve gizli veri belirlendikten sonra yapılması gereken şey steganografi algoritması kullanarak gizli verinin taşıyıcı veri içerisine eklenmesidir. Taşıyıcı unsur üzerinde, içerisine eklenen gizli veriden dolayı bazı değişimler meydana gelecektir. Bu değişimlerin insan gözü ile farkına varılamaz olması steganografinin temel kuralıdır. Bu yüzden özellikle resim olacak taşıyıcı unsurlarda steganografi işlemi uygulanırken resimlerdeki parlaklık değerleri kesinlikle değiştirilmemelidir. Çünkü insan gözü renklerdeki tonlama farklılıklarını algılamada zayıf iken parlaklık değerlerini algılamada çok kuvvetlidir. Farkına varılan herhangi bir steganografi analiz yöntemleri kullanılarak çözülmeye çalışılabilir. Bu işleme steganaliz, bu işlemi yapana da steganalist denilmektedir. Tüm bu bilgiler ışığında, DCT algoritmasında 40KB'lık bir metin verisini resim dosyasının içerisine, DWT algoritmasında 40KB'lık bir resim verisini yine başka bir resim dosyası içerisine gizlenmiştir. Makalenin bundan sonraki ikinci bölümde, DCT ve DWT algoritmalarımızı ve kullanım senaryoları anlatılacaktır. Üçüncü bölümümüzde steganografi sistemlerimizin performanslarını ölçen parametler tanıtılacaktır. Makalemizin sonuç bölümünde ise performans parametrelerinin sonuçları gösterilecek ve bu sonuçlara göre hangi steganografi sisteminin daha performanslı olduğu ispatlanacaktır (Pfitzman, 2004: 348).

DCT VE DWT YÖNTEMLERİ

Çalışmamızda uygulanan DCT ve DWT yöntemlerini ve senaryolarımızı anlatmadan önce steganografinin dallarından bahsetmek gerekmektedir. Steganografi uygulandıkları platformlara göre altı alt dala ayrılmaktadır. Bunlardan biri olan dijital medya unsurları steganografisi, uzaysal-resim tabanlı steganografi ve frekans-dönüşümü tabanlı steganografi olmak tekrar üzere ikiye ayrılır. Çalışmamız frekans dönüşümlü steganografinin alt dalları olan DCT ve DWT'nin performanslarının incelenmesidir. Bu konuyu seçmemizin sebebi

frekans tabanlı steganografinin diğer türlere göre yüksek güvenilirliği ve DCT, DWT'nin en çok kullanılan yöntemler olmasıdır. Steganografi yöntemleri kullanılırken asıl amacımız sistemimizin güvenilir ve görünmez olmasıdır. Bunu yaparken sistemimizin sağlamlığı için kapasiteye ve önemli bitleri değiştirmemeye dikkat edeceğiz.

DCT

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 geçer. Aşağıdaki resimde DCT, Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)'un matematiksel formulasyonunu 2.1 ve 2.2'de görmekteyiz (Dhawale, Hegadi ve Jambhekar, 2014: 5).

$$F(u,v) = \frac{c(u)c(v)}{4}\sum_{i=0}^{7}\sum_{j=0}^{7}\cos\left(\frac{(2i+1)u\pi}{16}\right)\cos\left(\frac{(2j+1)u\pi}{16}\right)f(i,j) \quad (2.1)$$

$$c(e) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if } e = 0 \\ 1 & \text{if } e \neq 0 \end{cases} \quad (2.2)$$

Formüldeki;

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

Ayrık kosinüs dönüşümünde, kosinüs sinyallerini kullanan ve resimleri uzaysal tabandan frekans tabanlı matris yapısına kosinüs dönüştürücüsü ile dönüştüren bir yapıdır (Dhawale, Hegadi ve Jambhekar, 2014: 5).

Taşıyıcı obje her iki metotta 512x512 boyutunda bir resimdir. İki metodun performanslarının kıyaslanabilmesi için taşıyıcı objeler ve gizli mesajın KB, Kilobayt, cinsinden aynı olması gerekmektedir. Bu yüzden gizli mesaj, 40KB değerindeki bir resim veya metin verisinden seçilebilir. DCT metodunda ise gizli mesaj olarak 40KB'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. Bir sonraki bölümde Hamming kodlama ile ilgili ayrıntılı bilgi verilecektir. Taşıyıcı resmin de 8x8 boyutunda bir matrise çekilmesiyle DCT'nin uygulanması için tüm hazırlıklar tamamlanmış olur. 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 oluşturulmuş olur. DCT frekanslar üzerinde çalışma yapılırken dikkat edilmesi gereken unsur üzerinde işlem yapılan bit değerlinin en önemli bit değeri olmamasına "MSB-Most significant bit" dikkat etmektir. Bu bit değerleri piksellerin parlaklık değerlerini taşımaktadırlar ve üzerinde gerçekleştirilecek değişimler insan gözüyle dahi farkına varılabilir. Bizim çalışmamızda resimleri siyah beyaz formatına dönüştürerek bu önemli ayrıntı kaldırılmıştır. Renkli resimlerde ise "LSB-Least Significant Bit" en önemsiz bit anlayışına göre hareket edilmelidir.

HAMMİNG KODLAMASI

Telekomünikasyon sektöründe çalışan Richard Hamming'in geliştirdiği bir yöntemdir. Sinyallerin hatlarda gönderimi esnasında meydana gelen çeşitli etkiler neticesinde göndericiden alıcıya giderken değişimlere uğradığı saptanmış ve bunun çözülümü için geliştirilmiştir. Makalemizde 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. Elimizde 4 bit'lik 1001 verisi olduğunu farz edelim. Bu verinin alıcıya düzgün bir şekilde ulaşmasını sağlayabilmek için veriye kontrol amaçlı 3 adet kontrol bit'i eklenir ve sonuna bu kontrol bit'lerini eşitleyecek Parity bit'i eklenir. 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 bitlerdir. 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 değeler 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 veriler üzerinde gerçekleşen toplama işlemidir. 8 bit'lik bir veri kümesinde her bir 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. Buradaki amacımız, Hamming kodlama kullanarak düzeltilmiş mesajı, ikili sayısal tabanlı değerlerinin DCT özniteliklerine en az bozulmayı verebilmesini sağlamaktır (Medeni ve Souidi, 2009: 46).

DWT

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 dalgalanmaları inceleyebilmemize olanak sağlamasıdır. Ayrık Kosinüs Dönüşümünde, DCT, olduğu gibi DWT uygulanırken taşıyıcı resim ve mesaj frekans boyutuna dönüştürülür. DWT taşıyıcı resmi 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 resmin 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 bu da çokça veriyi saklayabiliriz anlamı taşımaktadır. Tabii ki kapasite değerleri aşılmamalı ve bozulmalara dikkat edilmelidir. Ancak taşıyıcı bandın düşük frekans seçilmesinin bazı dezavantajları vardır. Yüksek frekans gibi sağlam değillerdir. Çünkü yüksek frekansta veri saklamak fark edilirliği az olan bir işlemdir ve dolayısıyla bu bölgede yapılan değişimler enerji değerlerinde değişime sebebiyet vermektedir. JPEG standartlarında bahsedilene göre resimler en düşük enerji düzeyine göre ayarlanmıştır. Bu piksel kümesinde, matrisinde, meydana gelen her türlü değişim resmin ortalama enerjisini üstel yönde etkileyecek bir değişim olur ve bu değişimler histogram ve entropi analizlerinde kolayca açığa çıkabilir (Dalvi ve Kamathe, 2014: 4).

Bu bölümde, ikinci olarak oluşturduğumuz DWT algoritması adımlarından bahsedeceğiz. Aynı DCT'de olduğu gibi, işlemlerimiz öncelikle taşıyıcı resmin ve gizli mesajın seçilimi ile başlamakta ve DWT dönüşümünün uygulanması ile devam etmektedir. DWT iş akış diyagramı aşağıdaki DCT'de olduğu gibi DWT senaryosunda taşıyıcı objemiz 512x512 formatında bir resim ve gizli mesajımızın boyutu da 40KB'dır. Burada DCT Hamming kodlamasındaki etki gibi bir etki oluşturmak için 40KB'lık resim verisinin siyah beyaz formatındaki taşıyıcı resme 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 özelliği de 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 resmin orijinal hali ile DWT ile oluşturulmuş steganografik resmimizi kıyaslayarak PSNR değerlerini elde edip DCT ile kıyaslayacağız.

STEGANOGRAFİ PERFORMANS PARAMETRELERİ: MSE, PSNR, Z-SCORE

MSE

MSE, Hata Karelerinin Ortalaması, genellikle sinyallerde iki sinyalin birbirilerine olan benzerliklerini ölçmek için kullanılan bir yöntemdir. Steganografide buna benzer olarak taşıyıcı resim ile steganografik resmin benzerliklerini ölçmek için kullanılır. Aşağıdaki 2.3. formülüne göre MSE, benzerlik bulmaya çalışır (Dhawale,Hegadi ve Jambhekar, 2014: 5).

$$\text{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (2.3)$$

Formüldeki;

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

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

PSNR

PSNR, Yüksek Sinyalin Gürültüye Oranı, logaritmik desibel ölçütü ile tanımlanır, ölçümlendirilir. Steganografik resmin 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 2.4'deki formül ile hesaplanır (Dhawale, Hegadi ve Jambhekar, 2014: 5).

$$\text{PSNR} = \log_{10()} \qquad (2.4)$$

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

SONUÇ

512x512 boyutundaki resimlere DCT ve DWT metotlarında 40KB büyüklüğündeki gizli mesajlar resim ve metin verisi olarak yüklenilmiştir. Yüklemeler sonrasında yeni oluşan siyah beyaz steganografik resimler ve orijinal halleri ile kıyaslanmasından sonra çıkan PSNR değerleri Tablo 1'deki gibidir.

Çizelge 1: DCT-DWT PSNR değerleri

DENEMELER	DWT- PSNR	DCT - PSNR
DENEME1	50,1016	38,1549
DENEME4	50,2364	40,1903
DENEME7	50,7428	40,4352

Makalemizin performans parametreleri bölümlerinde bahsettiğimiz, düşük PSNR değeri başarıda azlığı göstermektedir. Bu bilgiden yola çıkarak oluşturduğumuz bu senaryoda PSNR değeri düşük olan DCT algoritmasının steganografi oluşturmada DWT algoritmasına göre daha az başarılı olduğunu söylemek mümkündür. DWT yöntemi tüm deneme resimlerinde DCT yöntemine göre daha yüksek PSNR değerleri elde etmiş yani daha başarılı olmuştur. Bunu ispatlayan çalışma sonuçlarımız Tablo 1. DCT-DWT PSNR değerlerinde gösterilmiştir. Z-skor çalışmamızda ise farkına varılmayı kıyaslayan PSNR değerlerinden farklı olarak, istatistiksel olarak benzerliği ölçmekteyiz. Z-skor bölümümüzdeki tabloda da gösterildiği gibi, eğer steganografimiz farkına varılırsa DCT istatiksel olarak verinin bulunmasını daha da zorlaştıran bir yapıya sahiptir. Aşağıda gösterilen deneme7 isimli resimli uygulamamızda DCT senaryosu istatistiksel olarak DWT'den daha başarılı olmuş ve diğer tüm denemelere göre daha başarılı bir değer almıştır.

Şekil 1: Deneme7 Taşıyıcı Resim

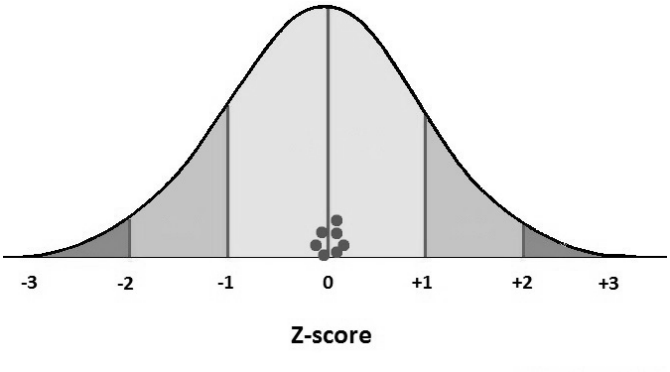
Şekil 2: Deneme7 Steganografik Resim

Z-SCORE

Bilinen Z-skor uygulamaları gibi ilk önce standartlaştırma yapılmıştır. Tüm verilerin ortalama değeri elde edilmiştir. İlk olarak taşıyıcı veri ve steganografik veri matrislerden dizi formatına çekilmiştir. Daha sonrasında bu iki dizinin elemanlarının, sayısal değerler açısından farkları alınmıştır ve daha öncesinden bulunmuş olan standart sapma değerine bölünmüştür. Elde edilen sonuçlar aşağıdaki tabloda yer almaktadır. Tablo 2'deki sonuçlar her bir deneme resmi için elde edilen ortalama değerlerdir. Bu değerler Z-skor eğrisinde dağılımı göstermektedir (Göçmen, 2011).

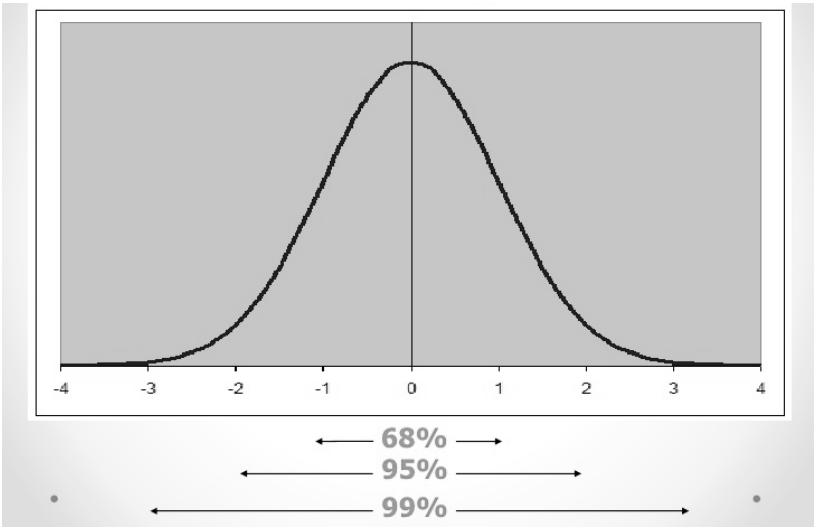
Çizelge 2: DWT ve DCT Z-Score Değerleri

DENEMELER	DWT- Zscore	DCT - Zscore
DENEME1	3,1734	1,2705e-04
DENEME4	2,1127	-1,5367e-04
DENEME7	2,4425	0,7676e-04



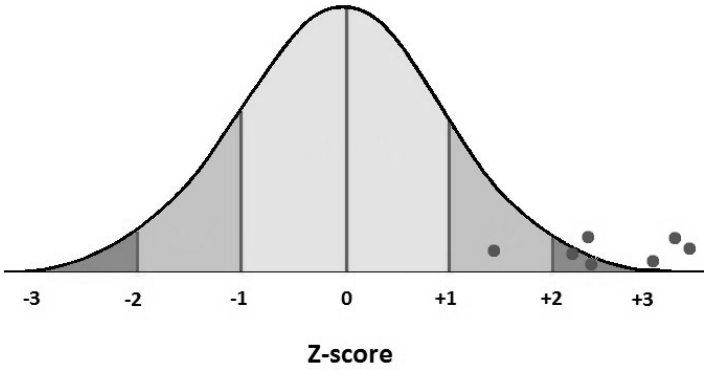
Şekil 3: Z-skor Eğrisinde DCT Verilerinin Dağılımı

Yukarıdaki resimde DCT verilerinin Z-skor eğrisindeki dağılımın özet bir kısmı gözükmektedir. Yukarıdaki tablo değerleri her steganografik deneme resmi için bulunan ortalama Z-skor değeridir. DCT sistemi için elde edilen tüm değerler 0.08 ile 0.02 arasında değişmektedir. Aşağıdaki Şekil 4›deki Z-skor eğrisinden anlaşılacağı üzere, DCT'nin verilerin dağılımını istatistiksel olarak sıkışık topladığını göstermektedir.



Şekil 4: Z-skor Eğrisi Üzerinde DCT Verilerinin Dağılımı

DCT sistemi gizli veriyi taşıyıcı resmin istatistiksel olarak %68'lik bir kısmında saklayabilmiş ve bu durum PSNR değerlerinin düşük çıkmasına sebebiyet vermiştir. Aşağıdaki Şekil 5›de DWT'nin ortalama piksellerinin dağılımını göstermektedir. Buradaki dağılım DCT algoritmasına göre daha rastgeleliği yüksek ve geniştir.



Şekil 5: DWT Ortalama Piksel Dağılımı

Yukarıdaki Şekil 5'de gösterdiğimiz Z-skor eğrisinde gösterdiğimiz değerlere göre DWT taşıyıcı resmin %99'luk bir kısmına veri gizleme işlemi yapmaktadır. Daha fazla alanda veri saklaması MSE değerinin düşmesine ve PSNR değerlerinin yüksek çıkmasını sağlar. Z-skor çalışmamız DCT ve DWT sistemlerinin veri gizlerkenki veri dağılımlarını istatiksel olarak göstermektedir. DWT sistemimizin neden daha yüksek PSNR değerine sahip olduğunu istatistiksel dağılım açısından ispatlamaktadır.

KAYNAKÇA

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.

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

Dhawale, C. A., Hegadi, R. ve Jambhekar, N. D. (2014). "Performance Analysis of Digital Image Steganographic Algorithm", *ICTCS '14*, November 14 – 16, 2014, pp. 1-7.

Medeni, M. B. O. ve Souidi, M. (2009). "A Steganography Schema and Error-Correcting Codes", *Journal of Theoretical and Applied Information Technology,* 18(1): 42-47.

Dalvi, A. ve Kamathe, R. S. (2015). "Color image steganography by using dual wavelet transform (dwt, swt)", *International Journal of Scientific Engineering and Research (IJSER),* 3(7): 1-6.

Göçmen, M. (2011). "Z-Score Sunumu". http://www.slideshare.net/mgocmen37/z-skorzscore adresinden alındı. (Erişim Tarihi: 22/06/2016)