ACTA INFOLOGICA, 2018; 2(1): 12-21
Research Article

ACTA INFOLOGICA
ISSN: 2602-3563

İdeal Steganografi Senaryosu: Taşıyıcı Resimlerin Kapasitelerinin Hesaplanması, Frekans Tabanlı Steganografide OPA Yöntemi

Ferdi Sönmez*, Faruk Takaoğlu, Oğuz Kaynar

ÖZ

Bu çalışmada steganografi'nin bir dalı olan dijital resim steganografisinden ve onunda bir alt dalı olan frekans tabanlı steganografi yöntemlerinden olan AKD (Ayrık Kosinüs Dönüşümü) ve ADD (Ayrık Dalgacık Dönüşümü)'nden bahsedilmiştir. Steganografik yöntemlerin performans hesaplama parametreleri olan OHK(Ortalama Hataların Karesi) ve TSGO (Tepe Sinyali Gürültü Oranı), gibi yöntemler açıklanmış ve bu parametrelerin değerlerinin arttırılması için resim kapasitesi hesaplama yöntemleri olan Kullback-Leibler Iraksaması, Jensen-Shannon Iraksaması ve DAS (Dörtlü Ağaç Segmentasyonu)'ndan bahsedilmiştir. Sonuç olarak resimlerdeki var olan kapasitenin daha da arttırılmasını sağlayan OPAİ (Optimal Piksel Ayarlama İşlemi) yönteminden bahsedilmiş ve ideal bir steganografi senaryosu belirtilmiştir. Çalışmamıza ek olarak bu senaryo denemesi gerçekleştirilmiş ve sonuç olarak DAS'na göre daha yüksek veri gizleme kapasitesi olan resimlerin daha yüksek TSGO değerleri verdiği sonucuna ulaşılıştır.

Anahtar Kelimeler: Ayrık Kosinüs Dönüşümü, Ayrık Dalgacık Dönüşümü, Kullback-Leibler Iraksaması, Jensen-Shannon Iraksaması, Bilgi Teknolojileri Güvenliği, Veri Güvenliği, Veri Gizleme, Frekans Tabanlı Steganografi.

Ideal Steganography Scenario: Calculation of Capacities of Carrier Images, OPA Method in Frequency-Based Steganography

ABSTRACT

In this study, digital image steganography, a branch of steganography, and DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform), frequency-based steganography methods that are a sub-branch of it, are mentioned. Methods such as MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) which are performance calculation parameters of steganographic methods are explained and the methods of calculating image capacity like Kullback-Leibler Divergence, Jensen-Shannon Divergence and QTS (Quard Tree Segmentation) for increasing the values of these parameters are mentioned. This study explains the OPAP (Optimal Pixel Adjustment Process) method, which allows the existing capacity in the pictures to be further increased, in detail and provides an ideal steganography scenario. Additionally, this scenario has been tried and consequently reached the result that the images with higher data concealment capacity than QTS have higher PSNR values.

Keywords: Discrete Cosine Transform, Discrete Wavelet Transform, Kullback-Leibler Divergence, Jensen-Shannon Divergence, Information Technology Security, Data Security, Data Hiding, Frequency Based Steganography.

Information of Author(s):

Ferdi Sönmez
ORCID: 0000-0002-5761-3866
ferdisonmez@hotmail.com

Faruk Takaoğlu
ORCID: -
faruktakaoglu@stu.aydin.edu.tr
İstanbul Aydın Üniversitesit

Oğuz Kaynar
ORCID: 0000-0003-2387-4053
okaynar@cumhuriyet.edu.tr
Cumhuriyet Üniversitesi, İİBF, YBS Bölümü

DOI: 10.30801/acin.358076

Submit Date: 26.11.2017
Accept Date: 14.06.2018
Publish Date: 26.06.2018

(*) Contact Author
Address: İstanbul Arel Üniversitesi, İstanbul, Türkiye ● **Telephone Number:** +90 850 27 35 - 1299

ACTA INFOLOGICA
ISSN: 2602-3563

1. GİRİŞ

Steganografi eski çağlardan bu yana farklı formlarda ve uygulama alanlarında gördüğümüz bir bilimdir [1]. Şahısların sahip oldukları değerli bilgileri saklamak için kullandıkları bu bilim günümüzde dijital formlar üzerinden veri transferi ve iletişimi sağlamak için kullanılmaktadır. Steganografi veri güvenliği biliminin alt dallarından biri olsa da asıl icraatı verinin içeriğinin korunmasından çok verinin içeriğinin gizlenmesidir [2]. Bu da aslında steganografinin verinin korunması ile ilgilenen kriptoloji bilimine karşı avantajıdır. Kriptoloji bilimi var olan verinin içeriğinin korunmasını ve başka şahıslarca içeriğinin okunamaması veya çözülememesini amaçlar ancak steganografinin asıl amacı verinin başka şahıslarca görünmemesini sağlamaktır. Görünen ancak içeriği belli olmayan bir bilgi elbet yetenekli kişilerce ve ilerleyen teknolojilerce çözülebilir. Ancak, verinin varlığından haberdar olunamaması durumunda, kişilerin yetenekleri ve sahip oldukları teknolojiler bir anlam ifade etmez [1]. Diğer bir steganografi benzeri uygulama ise Watermarking (filigran)'dır [3]. Multimedya unsurlarının aitliklerinin ispatlanması için kullanılan yöntemdir. Bu yöntem çok benzer sistemler kullanarak var olan ve üzerinden kazanç elde edilen veya edilebilecek multimedya unsurlarının aitliklerinin ispatlanması için bu unsurların içerisine bazı imza niteliğinde bozulmalar "signature" eklemektir. Üçüncü şahısların gerekli izin veya bedeli ödemeden görsel unsurları kullanmasını engellemek için yapılmıştır. Çoğu zaman imzalar flu veya gölgeli biçimde multimedya unsurlarının üzerinde gözükür halde bulunur. Bu tarz bir uygulanış hem uygulama hemde mantık olarak steganografiye aykırıdır. Watermarking'de amaç görseldeki imza niteliğindeki bozulmayı göstermek ve resmin korunduğunu ve hatta kime ait olduğunu ispatlamakken, steganografi'de amaç veri gizlenmesinden kaynaklanan bozulmaları minimize etmek, olabildiğince göstermemektir. Steganografi bu bahsettiğimiz yönlerinden diğer benzer bilimlerden ayrılmakla birlikte, beraber de kullanılabilir. Steganografide kullanılacak gizli mesajların önce kriptolanarak sonrasında veri gizleme işlemine tabii tutulduğu uygulamalar çokça mevcuttur[2]. Bu tarz melez uygulamalar güvenliği ve gizliliği arttırıcı yöntemlerdir. Tüm bu bilgilerden sonra steganografinin kullanıldığı bazı terimler şunlardır [4]:

- Taşıyıcı Unsur / Masum Obje: Veri gömülümü yapılacak ve gizli mesajı taşıyacak çoklu ortam unsuruna verilen addır. Çalışmamız resim steganografisi olduğu için buradaki taşıyıcı objemiz resim unsurlarıdır.
- Gizli Mesaj: 3.Şahıslardan saklamak istediğimiz ve değerli olan bilgilerdir. Bu bilgiler taşıyıcı unsurların içerisine saklanır.
- Stego Key / Steganografik Anahtar: Veri gizlemesi bazen karşılıklı anlaşılarak bazen de algoritma ve yöntemler kullanılarak belirli bir düzen içerisinde yapılır. Böyle durumlarda karşılıklı olarak anlaşma sağlanmadığı için her iki tarafta veri gizlenmesini çözecek bir anahtar üzerinde anlaşırlar.
- StegObje / Steganografik Obje: Taşıyıcı resim içerisine gizli mesajın saklanmasından sonra oluşan taşıyıcı objeye çok benzeyen mültimedya unsurlarına verilen ad.
- Steganografik Analiz / StegAnaliz: Steganografik unsurların denetlenmesi ve içlerindeki gizlenmiş verilen bulunmaya çalışılması işlemine verilen addır.
- StegAnalist: Steganografik analiz işlemini gerçekleştiren uzmana verilen addır.

Güvenilir bir steganografi sistemi inşa ederken dikkat edilmesi gereken unsurlar şunlardır [5]:

- Görünmezlik: Steganografik sistemin insanlar tarafından (insan gözüyle) farkına varılamaz olmasıdır. Steganografik mesajın taşıyıcı unsur üzerine gömülümü işleminden sonra resimde meydana gelecek değişimler insan çıplak gözüyle farkına varılamaz olmalıdır.
- Güvenlik: Saldırgan taşıyıcı obje üzerinde gizli mesajın varlığını farketse bile mesajı ortaya çıkarmasının imkansıza yakın olması durumudur. TSGO (Tepe Sinyalinin Gürültüye Oranı) ölçü birimi ne kadar yüksek değerli olursa sistemimiz o kadar güvenli demektir.
- Kapasite: Önemli mesajın kapasitesinin taşıyıcı mesajın kapasitesinden fazla olmaması durumudur. Bu yaklaşık olarak maksimum %51 'lik kısımı geçmemesi tavsiye edilir aksi durumda, steganografinin unsurlarından olan görünmezlik unsuru delinmiş olur.
- Sağlamlık: Steganografinin taşıyıcı unsuru resim, video vb. üzerinde yapılan filtreleme, kesme-kırpma, yön değiştirme ve sıkıştırma gibi manipülasyonlara karşı dayanıklı olması durumudur.

ACTA INFOLOGICA
ISSN: 2602-3563

1.1. İlgili Çalışmalar

Önceki ve ilerleyen bölümlerde yer yer belirtildiği gibi watermarking filigran yazılımları ve yöntemleri steganografi ile aynı branşta kabul edilse de, yaptıkları işler ve sistemsel bakış açılarından farklılık gösteririler. Yaghmaee ve Jamzad, çalışmalarında resim kapasitelerinin hesaplanması konusunda eğitici bir yayın çıkarıldığı görüşmektedir [3]. İlk olarak resimde kapasiteyi belirleyen faktörler hakkında geniş ve kronolojik bir bilgi serisi sunulmuş daha sonrasında resimlerin kapasitelerinin ölçülmesini sağlayan yöntemler anlatılmıştır.

N. Verma'nın çalışmasında; EAB (En Az Ağırlıklı Bit), ADD (Ayrık Dalgacık Dönüşümü) ve DS (Dalgacık Steganografi) yöntemleri, geniş resim verileri üzerinde uygulanmış, avantaj ve dezavantaj'ları açısından karşılaştırılmıştır [6]. Bu 3 popüler yöntem aynı materyaller üzerinde uygulanmış ve analiz aşamasında SGO, (Sinyal Gürültü Oranı) ve Histogram analizinden faydalanılmıştır. Sonuç olarak ADD'nün daha başarılı olduğu görülmüştür. Makale renkli resimler üzerinde çalışılarak geliştirilebilir. Steganografi hakkında bilgi sahibi olmak isteyenler için uygun bir çalışmadır.

Steganografi önemli olduğu kadar onun analizinde kullanılan steganaliz metodları da araştırılmıştır [2]. İlgili bir çalışmada, steganografi platformu olan yazılımların performans analizi yapılmakta ve steganografi algoritmaları hakkında bilgilendirilme yapılmaktadır [7]. NÇK, (Normalize Çapraz Korelasyon) yönteminin steganografik sistemlerin güvenilirliğini ve algoritmalarının sağlamlığını ölçmekte kullanıldığını ve önceki çalışmalarda TSGO, dikkate alınarak yüksek değerli güçlü sinyaller içeren mesajlarda, gizli mesaj gömebilmek için alanın daha da arttığı gözlemlenmiştir. Bir steganografi işleminin kabul edilebilir olması İGS (İnsan Görüş Sistemi) tarafından anlaşılamamasına bağlıdır. Bunun için OHK (Ortalama Hataların Karesi) 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.

Hemalatha ve arkadaşlarının 2012 yılında gerçekleştirdikleri çalışmada renkli resimlerde steganografi uygulaması yapılmıştır [8]. İnsan gözü parlaklık değişimlerini algılamada kuvvetli iken renk tonlarının değişiminde zayıftır. Bu bilgiden yola çıkarak araştırmacı renkli steganografi de "YCbCr" parlaklık değeri tutan 'Y' değerinin yerine 'Cb' mavi renk ton değerleri ve 'Cr' kırmızı renk ton değerleri üzerinde veri gizleme işlemi gerçekleştirmiştir. Veri gizleme işlemi dönüşüm formülleri kullanılarak renklerin sayısal değerleri üzerinde gerçekleştirilmiştir. 256x256 boyutunda bir renkli resim içerisine 128x128 boyutunda bir siyah beyaz resim gizlenmiştir. ADD kullanılarak resimler alt band'lara ayrılmıştır. En düşük seviyeli band olan LL bandında veri gizleme işlemi yapılmıştır. EAB, bir piksel tabanlı dönüşüm sağlayan yöntemdir.

Suvarna ve Chandel çalışmalarında TSGO, değerlerine göre beş Wavelet Dalgacık türünün performans analizini yapmışlardır [9]. Buradaki önemli olan bilgi yeni başlayanlar için Matlab platformundaki Wavelettools'un yöntemleri olduğu gibi dalgacık türlerinin de kendi içinde yöntemleri olduğudur. Bu türler yapılacak işlemlerin veya işlenecek sinyallerin özelliklerine göre farklı performans gösterebilirler. Bu yüzden performanslı işlem yapacakların bu türlere dikkat etmesi gerekmektedir. Çalışmada, tüm Matlab-Wavelettools türleri anlatılmış ve steganografi işlemi adımları ile açıklanmıştır. Testlerin sonucuna göre ise Dört Seviyeli Haar ADD diğer Dalgacık türlerine göre daha başarılı bir TSGO değeri vermiştir.

Dhawale ve arkadaşları, steganografinin uygulama platformlarından biri olan dijital resim steganografisi alanında tanıtıcı yönü ağır basan özet makaleye benzer bir çalışma yapmışlardır [10]. Bu makalede piksel tabanlı veri gizleme yöntemlerinden olan EAB, TDA (Tekil Değer Ayrışımı), YS (Yayılı Spektrum) yöntemleri kullanılmış, frekans tabanlı steganografi yöntemleri olarak; ADD, AKD, AFD (Ayrık Fourier Dönüşümü) ve TDD (Tamsayı Dalgacık Dönüşümü) yöntemleri ele alınmıştır. Çalışmanın amacı bir masum taşıyıcı resim verisi içerisine bir papatya resmini gizlemek ve yukarıda bahsi geçen yöntemlerin performans parametrelerince test edilerek hangisinin daha başarılı olduğunun bulunmasıdır. Çalışmada steganografi bilimi hakkında yeni bilgi edilecekler için çokca bilgi mevcut iken bu alanda çalışma sahibi olanlar için sığ denilebilecek veriler içermektedir. Çalışmada kullanılan materyal çeşitliliği arttırılmalı ve güçsüz oldukları bir bedahet olan yöntemler rastgelelik veya sinyal düzeltmeyi sağlayan hamming kod gibi uygulamalarla güçlendirilerek frekans tabanlı olan ve başarı oranları bilinen yöntemlerle tekrar kıyaslanmalıdır.

ACTA INFOLOGICA
ISSN: 2602-3563

2. YÖNTEM

Resimlerde veri gizlemeye uygun olan bölgelerin ve bu bölgelerin kenar noktalarının iyileştirilmesi üzerinde durulmuş, matrisler kullanılarak gruplar halinde veri gizleme işlemlerinin yapılmasının rastgele veri gizleme işlemi yapılmasından daha etkili olduğu keşfedilmiştir. Frekanslar üzerinden işlemler yaparken elimizdeki gizlenecek verinin büyüklüğüne göre hangi frekans band'larında veri gizlemesi yapılması gerektiği (çok verinin düşük band'larda, az veri yüksek band'larda saklanmalıdır) belirlenmiştir. Steganografi yapılırken kullanılan resimlerin dokusal özelliklerinin veri gizleme kapasitesini etkilediği anlaşılmıştır. Frekans tabanlı işlemlerde steganografinin anlaşılmaması için bazı durumlarda gürültü ekleme veya gürültü temizleme işlemleri yapılarak steganografi uygulanmış ve elde edilen sonuçlar not edilmiştir. Veri madenciliği yöntemleri kullanılarak steganaliz çalışmaları da yapılmıştır [11]. Resimlerin olası enerji seviyeleri hesaplanarak eşik değerleri belirlenmiş ve bu değerlerden yola çıkarak steganaliz yöntemleri geliştirilmiştir.

2.1. Frekans Tabanlı Steganografi

Frekans tabanlı steganografi yöntemleri daha karmaşık ve anlaşılması zor yöntemler olduklarından daha güvenli ancak daha az tercih edilen yöntemlerdir [12]. Bu yöntemlerde diğer piksel bazlı değişim yöntemlerinde olduğu gibi resim içerisinde yer alan ancak değişiminin resmin bütününde çokça bir fark oluşturmayacağı bit'lerin bulunması ve bunların üzerinde değişim yapılmasını hedefler. Kısacası mantık olarak diğer yöntemlerle aynıdır ancak izlediği yollar daha karmaşık ve resimde daha az etki oluşturur [11]. AKD yönteminde resim 8x8 boyutunda matris'lere bölünür ve her bir matris bloğundan 64 adet AKD katsayısı elde edilir. EAB mantığında olduğu gibi burada da resimlerin parlaklık değerlerini içermeyen ve minimum bozulmaya sebebiyet verecek olan bit'ler artık bit'lerdir ve bunların üzerinde değişim yapılabilir. Genel bilgi olması açısından resim uzantıları aslında resimlerin sıkıştırılma yöntemlerini sembolize eder ve JPEG uzantısında olduğu gibi bir grup veya kuruluşun önderliğinde yapılmaktadır. GIF uzantılı resimlerde veri saklamada kullanılan platformlardan biri olsada GIF resimlerin renk histogramında denge içermesi ve veri gizlemenin bozulmalara yol açmasıyla kolaylıkla bulunabilmesi söz konusudur bu yüzden JPEG veri saklama yöntemlerinde çokca kullanılan bir resim uzantısıdır. Çünkü en performanslı sıkıştırma yöntemine sahiptir. Bu yöntemde [13], sıkıştırılması yapılmış resimlerin değerleri üzerinde oynamak, resim üzerinde bozulmalara elbette sebebiyet verecektir. Ancak en az etkiye sahip değerler üzeriden değişim yapıldığında, resimlerin parlaklık değerlerinden ziyade tonlamaları değişebileceğinden fark edilmesi zor olacaktır. Steganaliz yöntemlerinden olan ve resimlerin bölgesel olarak histogram ve entropi analizleri yapıldığında buradaki resimlerin bozulmaları takip edilerek veri gizlenmesi anlaşılabilir. ADD yönteminde de AKD mantığıyla resim değerleri frekans değerlerine çevrilmekte ve farklı frekans bandlarının farklı özelliklerine uygun veri gömülümü yapılabilmektedir [14][11][12]. Örneğin, yüksek frekans bandında az, düşük frekans bandında çok veri gizlemek.

i) AKD - Ayrık Kosinüs Dönüşümü

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

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

Formüldeki;

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

AKD'nde [10], kosinüs sinyallerini kullanan ve resimleri uzaysal tabandan frekans tabanlı matris yapısına kosinüs dönüştürücüsü ile dönüştüren bir yapıdır.

ii) ADD - Ayrık Dalgacık Dönüşümü

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

W, sürekli bir fonksiyon / j, skala parametresi / k, öteleme parametresidir [15].

Bu yöntem dalgacık olarak tabir ettiğimiz ana sinyalin 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. AFD'nde, olduğu gibi sinyali sadece tek bir frekans bandında incelemez, daha ufak ve ayrıntılı

ACTA INFOLOGICA
ISSN: 2602-3563

dalgacıklarda incelenerek daha iyi gözlemler yapabilmemize olanak sağlar. AKD'nde olduğu gibi ADD uygulanırken taşıyıcı resim ve mesaj frekans boyutuna dönüştürülmektedir [16][17].

2.2. Steganografide Performans Parametreleri

Steganografik algoritmaların performansları, gizli mesajı içerisine sakladığımız steganografik resim ve bu resmin içerisine mesaj iletisi eklenmeden önceki hali olan taşıyıcı resmin karşılaştırılması ile belirlenmektedir [12][11]. Bu karşılaştırmaya dayalı analiz ise bazı matematiksel parametrelerin bulunması ile tamamlanmış olur. Bu parametrik değerler; TSGO, OHK, NÇK, OF (Ortalama Farkı), Yİ (Yapısal İçerik), MF (Maksimum Fark) ve NMH (Normalleştirilmiş Mutlak Hata)'dır. Bu parametreler taşıyıcı obje ile steganografik obje arasındaki farkı değerlendirmemizi sağlayan matematiksel fonksiyonlar içermektedir [18].

i) OHK - Ortalama Hataların Karesi

OHK, 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 formüle göre OHK, benzerlik bulmaya çalışmaktadır [10].

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

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 OHK değeri düşük ise bu benzerliğin az olduğunu ve algoritmanın başarılı olduğunu göstermektedir. Tersi durumlarda ise algoritmamız başarısız sayılacaktır.

ii) TSGO - Tepe Sinyalinin Gürültüye Oranı

TSGO, logaritmik desibel ölçütü ile tanımlanır, ölçümlendirilir. Steganografik resmin görüntüsünün bozulumuna sebebiyet veren en üst seviye sinyal ile bozuluma sebebiyet veren gürültü değerinin arasındaki orana TSGO denir. Düşük TSGO ölçümü görsel kalitede düşüklük ve bilgi sıkıştırmada kalitesizlik anlamına gelir. Tersine durumda yani TSGO'nun yüksek ölçüldüğü durumda, resim kalitesi, sıkıştırması ve yeniden yapılandırılmasının kaliteli ve başarılı olduğu anlaşılır. TSGO değeri aşağıdaki formül ile hesaplanmaktadır [10].

$$\text{TSGO} = \log_{10}\left(\frac{MAX_1^2}{MSE}\right)$$

TSGO formülü görüldüğü üzere başka bir ölçüm parametresi olan OHK değerine bağlı olarak hesaplanır. MAXı değeri var olan en yüksek piksel değeridir.

2.3. Resimlerin Veri Gizleme Kapasiteleri

Dijital resimlerin kapasiteleri, çözünürlükleri ve hafızada kapladıkları alanla doğru orantılı olarak değişse de steganografide bunların haricinde renk, bit derinliği ve dinamik değer aralığı değerleri de önem kazanmaktadır. Bir resmin çözünülürlüğü Uzaysal Çözünürlük ve Tonal Çözünürlük olarak iki kısımda incelenir. Uzaysal Çözünürlük .dpi (dots per inch, inç başına nokta) değerinde var olan nokta sayısı veya .ppi (pixel per inch, piksel hassasiyeti) değeri gibi yöntemlerle ölçülebilir. Her iki yöntemde resimlerde detayı yakalayabilmek olarak adlandırılan görüntü kalitesinin ölçümü için gereklidir. Steganografide bu detay parametresi önemli olduğu gibi aynı zamanda Tonal Çözünürlük denilen renk çeşitliliği ve geniş bir yelpaze içermesi ve tüm bu değerlerin yüksek değerlikli olması hem resim için kalite unsurunu arttırıcı hem de steganografi için veri gömülümü kapasitesini arttırıcı özellik içerir. Resmin kendi çözünürlük değerleri dpi gibi parametreler ile resim boyutunun orantısının düzgün kurulmasına bağlı olduğundan (4800x6000 piksel boyutu 8x10 inç'lik baskı boyutunda 600 dpi çözünürlük içerip 28.8 MB (mega-bayt) boyuta sahipken, yine aynı piksel boyutunun 4x5'lik baskı boyutunda 1200 dpi çözünürlük oluşturması ve 86.4 MB'lık boyuta sahip olması gibi.) önemli olanın uygun çözünülürlükte uygun boyut değerleri ile seçilim yapılmalı ve steganografi için kapasiteli resimler oluşturulmalıdır [19]. Aksi durumda, boyutu düzgün olmayan resimlerde uygulanan steganografi görsel bozulmalar göstereceğinden kolayca anlaşılabilmektedir.

ACTA INFOLOGICA
ISSN: 2602-3563

i) Kullback-Leibler Iraksama Yöntemi

Yapacağımız bu çalışmada resimlerin veri saklama kapasitesini ölçmek için KL-Iraksama yöntemini kullanacağız. Bu yöntem, Liu ve arkadaşları çalışmalarında [12] aktarıldığı gibi kapasite ölçme yöntemleri ile ters orantı göstermektedir. Yani resimlerde ölçüm yapılırken, OPA (Optimal Piksel Ayarı) veya GKM (Gauss Karışımı Modeli) ve FBM (Fisher Bilgi Matrisi)'nden elde edilen değerlerin yüksek çıkması beklenirken, KL-Iraksama değerlerinin olabildiğince düşük çıkması istenilmektedir. KL-Iraksama değeri en az olan resimler bize resim saklama kapasitesinin en yüksek olduğu resimleri gösterecektir. Böylelikle yüksek kapasiteli resimlere ulaşılabilecek ve amacımız doğrultusunda resim saklama kapasitesi hesaplanmamış resimlerle Stegnografi yöntemleri üzerindeki etkileri ölçülebilecektir. Aşağıda KL-Iraksama yönteminin formülü yer almaktadır:

$$D_{KL}(P||Q) = \int_{\mathbf{X}} P \, ln\left(\frac{P}{Q}\right) d\mathbf{X}$$

Bu denklemde P(X|O) Masum X objesinin dağılım olasılığı değeri, Q(Y|O) değeri ise Steganografik resim olan Y'nin dağılım olasılığı değeridir. KL-Iraksama yöntemi bu iki dağılım/serpilme olasılıklarının farkının hesaplanmasıdır.

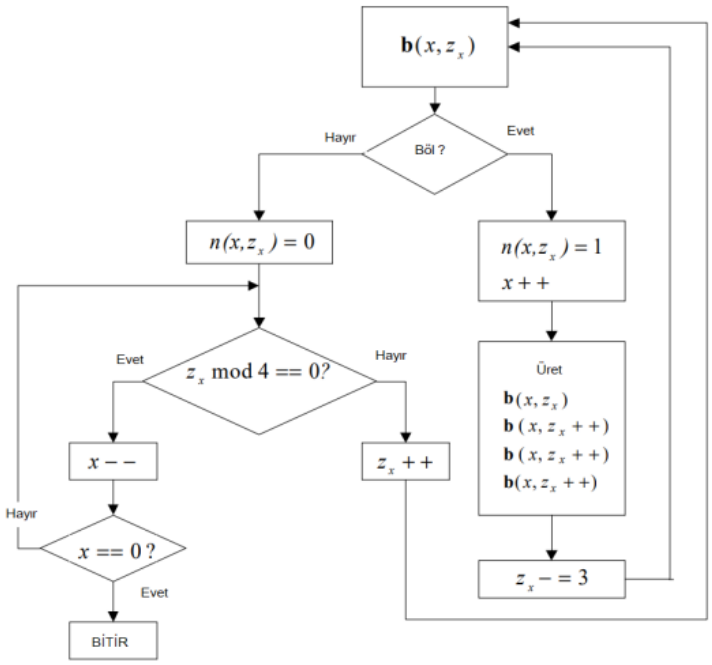
ii) Jensen-Shannon Iraksama Yöntemi

$$\mathrm{ICC}(X) = H(X) - \sum_{S=1}^{R} \frac{n_s}{N} H(I_s),$$

$$H(X) = -\sum_{i=1}^{N} p_i \log p_i,$$

Burada, N = Tüm piksel sayısı, X = Orijinal Resim, R = Toplam Segment Sayısı, n_s = Segment'deki piksel sayısı, Is = Segmentle bağıntılı histogram değerinin rastgele yoğunluk değeri, H = Entropi Fonksiyonu

Görsellik açısından farkına varılabilirliğin zor olması için heterojenlik değeri resim içerisinde sağlanmalıdır. Böylelikle, bozulmaların farkına varılması zor olacaktır [7]. Resim içindeki her bir segment de JS-Iraksama formülü rastgele dağılım ile bu hesaplamayı yapmaya çalışmaktadır.



Şekil 1. Dörtlü Ağaç Segmentasyonu Algoritması

ACTA INFOLOGICA
ISSN: 2602-3563

iii) DAS - Dörtlü Ağaç Segmentasyonu

Bu yöntemin amacı resim içerisindeki parlaklık "kontrast" değerlerinin düşük olduğu pikselleri bulmaktır. Bunun tercih edilmesinin sebebi [20] 1.1.İlgili Çalışmalar bölümünde bahsedilen İGS, insan gözünün parlaklık değerlerine karşı duyarlı olmasıdır. Yüksek kontrast değerlerine veri gizleme işlemi yapıldığında oluşan bozulmalar insan gözüyle farkına varılabilir. Bu yüzden bu kısımlara fazla veri gizlenemez. Ancak parlaklık "kontrast" değerleri daha düşük olan piksellere veri gizlenmesi daha uygundur. Buna bağlı olarak, bu yöntem resimleri piksel gruplarına bölerek her bir bölgede düşük parlaklık değerli pikselleri işaretler. Bu işaretlenmiş yerlerin sayısı resimdeki veri gizleme kapasitesini belirtmektedir [21]. Şekil 1'de DAS yönteminin bir algoritması verilmiştir.

2.4. OPAS - Optimal Piksel Ayarlama Süreci

OPAS (Optimal Piksel Ayarlama Süreci) veya sadece OPA, steganografide mesaj gömülümü gerçekleştikten sonra uygulanan bir yöntemdir. Asıl amacı steganografik resim ile orijinal resim arasındaki farklılıkları veya hataları gidermek, en aza indirmektir [22]. Örneğin elimizde taşıyıcı orijinal mesajın bir bölümünün binary değeri olsun. Bu değerin 10000 olduğunu farz edelim (10'luk sayı tabanındaki değeri 16). Sonrasında bu noktaya gizlemek istediğimiz gizli mesajın değerinin 1111 (10'luk tabanda değer karşılığı 15) olduğunu farz edelim. Bu iki değerin steganografi sonucunda birleşmesi ile elde edilecek değer 11111'dir (10'luk sayı tabanındaki değeri 31). Sonuç olarak 10'luk sayı tabanında hesaplandığında eski orijinal resim ile steganografik resim arasında 16 fark olduğu gözlemlenir. OPA algoritması bu 11111 sayı bloğunun EAB değerini değiştirerek 01111 yani 15'e çeker ve sonuç olarak taşıyıcı medya/orijinal resimle arasındaki farkı 1'e indirir. Bu uygulama yapılarak resimlere daha fazla gizli mesaj yüklenebilir ve dolayısıyla kapasiteler arttırılmış olur [23].

3. BULGULAR: DENKLEM ÖRNEĞİ

Bu çalışmadaki amacımız ideal bir steganografi senaryosu veya prosedürü belirlemektir. Şekil 2'de senaryonun adımları gözükmektedir.

Şekil 2. İdeal Steganografi Senaryosu

ACTA INFOLOGICA
ISSN: 2602-3563

Burada,

*1= Seçilen resime ADD "haar" yönteminin uygulanması ve LL "low" bandın seçilimi –değerlerin bulunması,

*2= Low band değerlerine AKD yöntemiyle öznitelik katsayılarının 8x8 matris bloklarından çıkarılması öznitelik tablosunun oluşumu,

*3= EAB mantığıyla en az değer içeren bit'lerin yani artık bit'lerin bulunması,

*4= Gizli mesaj ve gizli mesaj uzunluğunun birleştirilip eş sayı tabanına çevrilerek artık bit'lere eklenmesi ve gizlenmiş veri içeren öznitelik tablosunun oluşumu,

*5= Gizlenmiş öznitelik tablosundan OPA algoritmasının uygulanarak hataların minimize edilmesi ve kapasitenin arttırılması,

*6= Kalan masum değerleri içeren öznitelik değerleri ile gizli veri içeren öznitelik değerlerinin birleşimi,

*7= Ters ADD uygulanarak özniteliklerin frekans bandına, sonrasında da steganografik resime dönüşümü,

*8= Orijinal resim ile steganografik resim kullanılarak bulunan KL-Iraksama, JS-Iraksama yöntemlerinin veya DAS yönteminin uygulanması.

Yukarıdaki adımlarda ideal bir steganografi senaryosu verilmiştir. 8. adımda KL/JS-Iraksama yöntemlerinden çıkan sonuçlarda en ufak değerlerin aslında en yüksek veri saklama kapasitesi resimleri olduğunun işaretidir. Sonuç olarak bu işlem aynı anda birden fazla resme uygulanıp ve en sonunda bu hesaplama yöntemleri test edilirse minimum değerli resim en yüksek kapasiteli resim olarak anlaşılır ve sonuç olarak gizlenmiş verinin aktarımında o resim tercih edilebilir. Diğer bir yöntem olan DAS seçilerek steganografi işlemi yapılmadan önce resimlerin veri gizlemeye uygun olan blokları seçilerek bu bloklara veri gizlenmesi için özel bir kodlama işlemi yapılabilir veya doğrudan hangi resimde daha fazla uygun bloğu varsa o resme veri gizlemesi uygulanarak daha yüksek TSGO değerleri elde edilebilir. Aşağıdaki resimlere DAS uygulanmış ve sonuç olarak ADD steganografi sisteminden sonraki elde edilen TSGO değerleri verilmiştir.

Şekil 3. Taşıyıcı Resim 1

Şekil 4. Taşıyıcı Resim 2

Şekil 5. Taşıyıcı Resim 3

Tablo 1. Taşıyıcı Resimlerin DAS Uygun Blok Sayıları

DENEMELER	ADD-TSGO
Taşıyıcı Resim 1	16.252
Taşıyıcı Resim 2	16.096
Taşıyıcı Resim 3	16.072

Tablo 2. Taşıyıcı Resimlerin ADD sonrası TSGO değerleri

DENEMELER	ADD-TSGO
Taşıyıcı Resim 1	50,3908 dB
Taşıyıcı Resim 2	47,0555 dB
Taşıyıcı Resim 3	46,0858 dB

ACTA INFOLOGICA
ISSN: 2602-3563

Elde edilen tablolardan anlaşılacağı gibi DAS yöntemine göre veri gizlemeye uygun olarak belirtilen veri bloklarının sayıca fazla olduğu resimlerde daha fazla TSGO değerleri elde edildiği görülmektedir. Bazı araştırmacılar [24][25][26] çalışmalarında benzer yöntemler ve metotlar kullanmıştır. Çalışmamızda daha fazla sayıda veri gizlenmesine rağmen bu çalışmalara yakın TSGO değerleri elde edilmiştir.

4. TARTIŞMA VE SONUÇ

Bu çalışmada, AKD ve ADD frekans tabanlı Steganografi yöntemlerinin birlikte kullanımını ele alınmıştır. Çalışmamızda ADD'nün alçak frekanslı ve veri gizlemeye müsait bandları çıkarma özelliği ve bu bantlarda AKD'nin öznitelik katsayılarını elde ederek EAB yöntemini uygulamasından faydalanılmıştır. Bu hibrid yöntemler ek olarak diğer çalışmalardan farklı olması için gizli mesaja uygulanan veri sıkıştırma yöntemleri kullanılmadan, OPA algoritması tercih edilmiş ve taşıyıcı unsur üzerindeki değişimleri minimize etme yoluna gidilmiştir. Çalışmamızda son olarak resimlerin kapasitelerinin ölçülmesi alanına değinilmiştir. Steganografi alanında resimlerin gizli veri taşıma kapasiteleri üzerinde halen tam bir görüş birliği bulunmamaktadır. Bu alanda denenen yöntemler olan Iraksama Yöntemlerinin yerine DAS yöntemi kullanılmış, taşıyıcı resimlerinin başarılı TSGO değerlerinin DAS yönteminden çıkan taşıma kapasiteleri ile doğru orantılı olduğu görülmüş ve kapasitesi yüksek taşıyıcı resimlere veri gizleme işlemi uygulandığında daha başarılı TSGO değerleri alınacağı anlaşılmıştır. Bazı araştırmacılar çalışmalarında benzer yöntemler ve metotlar kullanmıştır. Çalışmamızda daha fazla sayıda veri gizlenmesine rağmen bu çalışmalara yakın TSGO değerleri elde edilmiştir.

Çalışmamızda, AKD ve ADD beraber kullanımı ile hibrid bir yöntem sunması ve ayrıca OPA, DAS gibi yöntemlerle bağdaşması güvenilirliğini ve sağlamlığını arttırmaya yönelik avantajlar olarak gözükse de sadece siyah beyaz resimlerde çalışması ve renkli resimlerde uygulanmaya başlandıkça uygulama alanında karmaşıklık ve hataların artması açısından dezavantajlar göstereceğini düşünmekteyiz. Bu dezavantajların önüne geçmek ileriki çalışmalar için ayrı bir motivasyon ve araştırma konusu olarak görülmektedir.

KAYNAKLAR

[1] Holub, V., Fridrich, J., Denemark, T. (2014). Universal distortion function for steganography in an arbitrary domain, EURASIP Journal on Information Security, 2014(1), ss.11-19.

[2] Sajedi, H. (2016). Steganalysis based on steganography pattern discovery. Journal of Information Security and Applications, 30, 3-14.

[3] Yaghmaee, F., Jamzad M.(2010). Estimating watermarking capacity in gray scale ımages based on ımage complexity , EURASIP Journal on Advances in Signal Processing, ss. 20102010:851920, doi: 10.1155/2010/851920.

[4] Subhedar, M.S., Mankar, V.H. (2014). Current status and key issues in image steganography: A survey, Computer Science Review, 13, ss. 95-113.

[5] Challita, K., Farhat, H. (2011). Combining steganography and cryptography: new directions. International Journal on New Computer Architectures and Their Applications, 1(1), ss.199-208.

[6] Verma, N.(2011). Review of steganography techniques, International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)–TCET, Mumbai, India

[7] Zeki, A.M., Ibrahim, A.A., Manaf, A.A.(2012). Steganographic software:analysis and implementation, International Journal Of Computers And Communications, 6(1).

[8] Hemalatha, S., Acharya U. D., Renuka, A., Kamath, P.R.(2012). A Novel color image steganography using discrete wavelet transform, CCSEIT-12, October 26-28, 2012, Coimbatore, India.

[9] Suvarna P., Chandel, G.S.(2013). Performance analysis of steganography based on 5-wavelet families by 4 levels -dwt suvarna, International Journal of Advance Research in Computer Science and Management Studies, 1(7), ss. 20-33.

[10] Dhawale, C. A., Hegadi, R., Jambhekar, N.D.(2014). Performance analysis of digital ımage steganographic algorithm. ICTCS '14, Kasım 14 – 16, 2014, Udaipur, Rajasthan, India, ACM 978-1-4503-3216-3/14/11.

ACTA INFOLOGICA
ISSN: 2602-3563

[11] Sujatha, P., Purushothaman, S., Rajeswari, R. (2014). Performance study of combined artificial neural network algorithms for ımage steganalysis, In Proceedings of International Conference on Internet Computing and Information Communications, ss. 441-451, Springer India.

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

[13] Hemalatha, S., Acharya, U.D., Renuka, A.(2015). Wavelet transform based steganography technique to hide audio signals in image, Procedia Computer Science, 47, ss.272-281.

[14] Provos, N., Honeyman, P. (2001). Detecting steganographic content on the internet, Center for Information Technology Integration, NDSS 2002, San Diego.

[15] Haşiloğlu, A. (2001). Dalgacık dönüşümü ve yapay sinir ağları ile döndürmeye duyarsız doku analizi ve sınıflandırma, Turk J. Engin Environ Sci, 25, ss.405-413.

[16] Dalvi, A., Kamathe, R.S. (2015). Color ımage steganography by using dual wavelet transform (DWT SWT). International Journal of Scientific Engineering and Research (IJSER), 3(7), ss.25-41.

[17] Bera, S., Dewangan, U., Sharma, M. (2013). Development and analysis of stego ımage using discrete wavelet transform, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[18] Cheddad A., J. Condell, K., Kevitt, P.(2010). Digital ımage steganography: survey and analysis of current methods, Signal Processing, 90(3), ss.727-752.

[19] Peterson, A.K. (2005). Introduction to Basic Measures of a Digital Image for Pictorial Collections, Prints & Photographs Division, Library of Congress, Washington, DC, ss. 20540-4720.

[20] Muhsin, Z. F., Rehman, A., Altameem, A., Saba, T., & Uddin, M. (2014). Improved quadtree image segmentation approach to region information. The Imaging Science Journal, 62(1), ss. 56-62.

[21] Lin,Y-C, Li, T-S (2011). Reversible image data hiding using quad-tree segmentation and histogram shifting, Journal of Multimedia, 6 (4), ss. 349-358.

[22] Kaur, S., Goel, N. (2015). Segmentation and block based image steganography using optimal pixel adjustment process and identical approach, 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), Chandigarh, 2015, ss. 1-5.

[23] Nithya , R. K., Nehru, C.P., Ubramanıam, T.B.(2014). Optimal pixel adjustment based reversible steganography, (IJITR) International Journal Of Innovatıve Technology And Research, 2 (3), 2014, ss. 963–966.

[24] Demirci, B. (2016). Görüntü steganografi metotları ve performanslarının karşılaştırılması (Doktora Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü).

[25] Kaya, H. V. (2015). Watermarking in medical images by using DWT, DCT, DFT and lSB algorithms (Doktora Tezi, Çankaya Üniversitesi).

[26] Şahin A. (2007). Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri. (Doktora Tezi, Selçuk Üniversitesi).

Bu çalışma 4. Uluslararası Yönetim Bilişim Sistemleri konferansında sunularak, özeti konferans özet kitabında yayınlanmıştır.