Avrupa Bilim ve Teknoloji Dergisi
Sayı 18, S. 683-694, Mart-Nisan 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 18, pp. 683-694, March-April 2020

Research Article

Yakın Histogramlar Temelli Yeni Bir Hibrit Veri Gizleme Yöntemi

Harun Kurnaz[1], Mehmet Zeki Konyar[2*], Adnan Sondaş[3]

[1]Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilişim Sistemleri Mühendisliği A.B.D., Kocaeli, Türkiye
[2]Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği, Kocaeli, Türkiye (ORCID: 0000-0001-8914-5553)
[3]Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği, Kocaeli, Türkiye (ORCID: 0000-0003-4559-3463)

(İlk Geliş Tarihi 1 Şubat 2020 ve Kabul Tarihi 19 Mart 2020)

(**DOI:** 10.31590/ejosat.695672)

ATIF/REFERENCE: Kurnaz, H., Konyar, M. Z. & Sondaş, A. (2020). Yakın Histogramlar Temelli Yeni Bir Hibrit Veri Gizleme Yöntemi. *Avrupa Bilim ve Teknoloji Dergisi*, (18), 683-694

Öz

Sayısallaşan dünyada veri aktarım hızlarının artması, iletişim yöntemlerinin çeşitlenmesi gibi özellikler sonucunda bilgi gizleme çalışmalarının önemi artmıştır. Gizli bilginin üçüncü şahıslar tarafından algılanamaması, sadece istenen kişilerin ilgili gizli veriyi ortaya çıkarabilmesi bu çalışmalardaki temel amaçtır. Gizlenen veri kapasitesinin artırmak, örtü görüntüsündeki değişimi azaltmak ve gizli verinin tespitini zorlaştırmak veri gizleme (steganografi) uygulamalarındaki en önemli hedeflerdir. Histogram, sayısal bir resmin renklerinin hangi tonlarda olduğunu gösteren bir dağılım grafiğidir. Verinin gizlenmesi farklı ortamlar üzerinde sıklıkla yapılmakta ve bu alanda ki çalışmalar oldukça ilgi görmektedir. Önerilen yöntem, histogram dağılımını kullanarak veri gizleme yapılacak piksel değerlerini tespit etmektedir. Veri üzerindeki değişimi minimize ederek histogram değerlerinin korunması sağlanmıştır. Önerilen yöntemde veri gizleme için kullanılacak görüntünün histogram dağılımındaki tepe noktası tespit edilmektedir. Tepe noktasının tek veya çift olmasına göre veri gizleme için kullanılacak komşu değer çiftleri belirlenmektedir. Görüntü taranarak ilgili piksel çiftlerine gizleme yapılmaktadır. Önerilen çalışmada kapasite ve dayanıklılık artırılarak görüntü üzerindeki değişikliğin minimize edilmesi amaçlanmaktadır. Bu amaçla gizleme kapasitesinin daha fazla olması istendiğinde görüntüdeki kırmızı, mavi ve yeşil renk kanallarının tamamı kullanılabilmektedir. Veri gizleme işlemi sonucunda histogram dağılımının çok fazla değişmemesi oldukça önemlidir. Önerilen yöntem ile yapılan veri gizlemede elde edilen taşıyıcı (stego) görüntünün görsel kalitesi oldukça yüksektir. Görsel kalitenin bu kadar iyi olmasının en önemli sebebi geliştirilen yaklaşımdan kaynaklanmaktadır. Daha önceki histogram tabanlı yöntemlerde tepe noktasının etrafını boşaltmak için histogramda tepe değeri hariç tüm pikseller ötelenmektedir. Diğer bir deyişle geçmiş histogram temelli yöntemlerde bir harf bile gizlemek istendiğinde histogram da bir boşluk açılması ve tüm piksellere müdahale edilmesi gerekmektedir. Oysaki önerilen yöntemde herhangi bir ötelemeye ihtiyaç duyulmadığı için stego görüntülerin görsel kalitesi büyük oranda korunmaktadır. Önerilen yöntem görsel kalite, gizli mesajın çıkartımı, kapasite, görünmezlik ve dayanıklık açısından, literatürdeki benzer çalışmalara göre üstünlük sağlamaktadır.

Anahtar Kelimeler: Hibrit yöntem, Histogram, LSB, Stego Görüntü, Veri Gizleme.

A New Hybrid Data Hiding Method Based on Near Histograms

Abstract

As a result of features such as increased data transfer rates and diversification of communication methods in the digital world, the importance of data hiding has increased. The main purpose in data hiding studies is that the secret information could not detected by third parties, only the desired people can extract secret data. The most important goals in steganography applications are increasing the hidden data capacity, reducing the change in the cover image and making it difficult to detect hidden data. The histogram is a distribution that showing the shades of a digital image. Data hiding is often done on different cover media datas, and studies in this area attract much attention. The proposed method determines the pixel values by histogram distribution to hide data. Histogram values were preserved by minimizing the change in the cover data. In the proposed method, the peak value is determined in the histogram distribution of the

* Sorumlu Yazar: Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği, Kocaeli, Türkiye (ORCID: 0000-0001-8914-5553) mzeki.konyar@kocaeli.edu.tr

image to be used for data hiding. Depending on whether the peak value is odd or even, adjacent pairs of values are determined for data hiding. The image is scanned and data hiding is done to the respective pixel pairs. In the proposed study, it is aimed to minimize the change in the image by increasing the capacity and durability. For this purpose, when it is desired to increase the hiding capacity, all the red, blue and green color channels in the image can be used. It is very important that the histogram distribution does not change much after data hiding. The visual quality of the carrier (stego) image obtained by hiding data with the proposed method is quite high. The most important reason why the visual quality is so good is because of the developed method. Previous histogram-based methods open a space around the peak value of the histogram by shifting all pixels except the peak. In other words, when it is desired to hide even a letter in previous histogram-based methods, a gap must be opened in the histogram and all pixels must be intervened. However, since no shifting is required in the proposed method, the visual quality of stego images is largely preserved. The proposed method provides superiority over similar studies in the literature in terms of visual quality, secret message extraction, capacity, invisibility and durability.

Keywords: Data Hiding, Histogram, Hybrid method, LSB, Stego Image.

1. Giriş

Steganografi ya da gizli yazı, bir görünmez haberleşme yöntemidir. Veri gizlemede, gizli mesajın ekleneceği bir taşıyıcı nesneye (ortam/medya) ihtiyaç duyulmaktadır. Taşıyıcı nesne verinin gizleneceği dosyadır ve örtü (cover) nesnesi olarak isimlendirilir. Örtü nesnesine gizlenecek olan veri (gömü verisi) metin, görüntü ya da ses dosyası olabilir. Örtü nesnesi içine veri gömüldükten sonra elde edilen yeni taşıyıcı nesne ise stego nesnesi (örtülü nesne) olarak adlandırılmaktadır (Patel & Gadhiya, 2015; Konyar vd., 2018).

Günümüzde sayısal verinin çeşitlenmesiyle birlikte gizleme işlemi için görüntü ve grafik dosyalarının yanısıra, IP paketleri, exe uygulamaları, html ve xml dosyaları, videolar gibi birçok farklı yapı tercih edilmektedir. Günümüzde, medya dosyaları (video, ses) büyük boyutları ve yüksek oranda bilgi içermeleri nedeniyle en sık tercih edilen saklama alanları olarak karşımıza çıkmaktadır. Steganografik tekniklerin başarılı olabilmesi için üç önemli gereksinimi sağlaması gerekmektedir. Bunlar; gizli haberleşmenin güvenliği, veri gizleme kapasitesi ve kasıtlı veya kasıtsız olarak yapılan saldırılara karşı dayanıklılık olarak sıralanabilir. Yapılan çalışmalarda, daha fazla veri gizleme kapasitesine sahip olan, taşıyıcı görüntü de daha az değişim oluşturan ve görsel ataklara karşı dayanıklı bir yöntemin geliştirilmesi amaçlanmaktadır (Yalman vd, 2014; Kurnaz & Sondaş, 2018).

Görüntüye veri gizlemek için farklı yaklaşımlar mevcuttur. Görüntünün renk (RGB) kanallarına ağırlık tabanlı (Chrysochos vd., 2007) veya RGB kanalları rastgele değiştirilerek (Gutup vd., 2008) veri gizlenmektedir. Histogram değerlerini kullanan diğer bir çalışmada (Ni vd., 2006), histogram bilgisinin dairesel bir çevrimde dizilimi esas alarak veri gizleme yapmaktadır. Bu çalışmada görüntü histogramının en yüksek frekanslı değeri boşaltılmakta ve boşaltılan bu bölgeye gizli bilgiyi içeren yeni veriler eklenmektedir. Alıcı tarafta gizli veri çıkartıldıktan sonra histogram eski haline getiren tersinir bir yöntem önerilmektedir. Meiamai vd., (2013) tarafından yapılan çalışmada, görüntüyü oluşturan renk bileşenlerinin histogram değerleri ayrı ayrı oluşturularak bileşenler üzerine veri gizleme işlemi yöntemi uygulanmıştır. Bu yöntemde piksel kanalındaki pikseller için ortalama hesaplanarak en az önemli bit (LSB) kullanılarak gizleme işlemi gerçekleştirilmiştir. LSB kullanan diğer bir çalışmada (Mohammed vd., 2015) orijinal örtü görüntüsünün ve stego görüntünün histogramları arasındaki farkları en aza indirmek için görüntüdeki her bir renk değerinin frekansına zıt değişiklikler yaparak renklerin değişmeden korunmasını sağlayan yöntem önerilmektedir.

Histogram değişikliğiyle kayıpsız bir veri gizleme öneren Xuan vd., (2007) oluşturulan algoritma ile belli aralıktaki histogram parlaklık değerlerini algoritmanın çalıştırılmasında kullanmışlardır. Görüntüdeki parlaklık değerinin histogramının tekrarlanma sayısına (frekansına) göre veri gizleyen bir yöntem de mevcuttur (Yalman & Ertürk, 2009). Oradaki yöntemde görüntü histogramı oluşturularak parlaklık değer aralığı ve tekrarlanma sayıları belirlenir. Daha sonra gömülecek bit değerine göre tekrarlanma sayıları kullanılarak veri gizleme işlemi gerçekleştirilir. Chang vd, (2008) tarafından önerilen yöntemde histogram bilgisi oluşturulup, en fazla tekrar eden parlaklık değerine göre bir algoritma oluşturarak veri gizlenmektedir. Benzer biçimde farklı veri gizleme yöntemleri de histogram dağılımını kullanarak veri gizlemektedirler (Lin & Li, 2011; Kuo vd., 2008; Hwang vd., 2006).

Veri gizlemede histogram dağılımı kullanan Islamy & Ahmad (2019) yönteminde gizli mesaj doğrudan tepe noktasına veya tepe noktasının sağındaki değere gizlenmektedir. Wu vd. (2015) çalışmasında karşıtlık düzeltme yaklaşımlarından faydalanılmıştır. Önerilen çalışmada ilk olarak görüntünün histogramı çıkartılmaktadır. Görüntüdeki en yüksek iki histogram değeri alınıp, onlardan büyük olanın sağı, küçük olanın solu boşaltılır. Gizli mesaj işte bu iki histogram değerine eklenir. Bu iki değerin bilgisi de resimdeki ilk piksellere eklenmektedir. Veri çıkartımı ise bu iki değere bakılarak yapılır. Kapasiteyi arttırmak için bütün bu işlemler oluşan yeni görüntüde yeniden tekrar edilir. Böyece veri gizleme yapılırken karşıtlık azaltma da yapılmış olur. Bu yöntemde hem gizleme yerlerinin alıcıya gönderilmesine ihyiyaç duyulmakta, hem de histogramda kaydırma işlemi yapılmaktadır. Chen vd. (2015) histogram kaymasından dolayı ortaya çıkan hatayı düzeltmek için bir yöntem önermişlerdir. Bu amaçla, gradiyen ayarlı tahmin ve histogram kaymasına dayanarak bir yönlendirilmiş tahmin şeması tasarlanmıştır. Böylece hem gizleme kapasitesi artırılmakta hem de kaymadan dolayı oluşan hata azaltılmaktadır. Pan vd. (2015) çalışmasında varlık frekansı en fazla olan histogram değeri yerine onun sağ ve sol komşularına gizleme yapılır. Böylece anahtar bilgisi göndermeye gerek kalmamaktadır. Ayrıca düşük kapasite problemini aşmak için de örtü resmi bloklara bölünerek oradaki histogramlara bakılarak veri gizlenmektedir. Bu yöntemde kapasite arttırılmış olmakla beraber yine histogramda kaydırma işlemi yapılmaktadır.

Literatürdeki mevcut histogram temelli veri gizleme yöntemlerinin büyük bir kısmı histogramda boşluk oluşturmayı önermektedirler ve tepe değerini alıcıya göndermeyi zorunlu kılmaktadırlar. Tepe değerini göndermeyen çalışmalarda ise histogramdaki

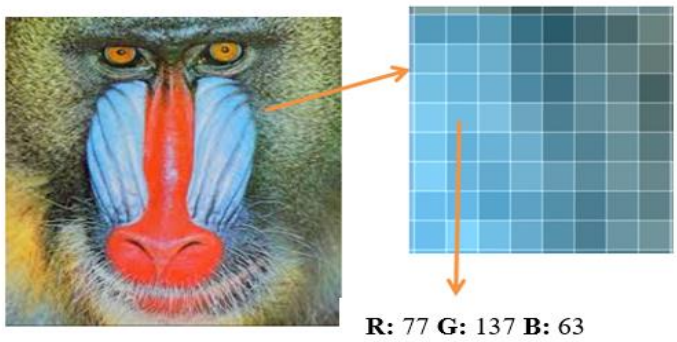
tepe değerinin sağında ve solunda boşluklar oluşturmak için resime müdahale etmek gerekmektedir. Kaydırma yapmayan ve tepe değeri gönderim ihtiyacı duymayan yöntemler de ise ya düşük kapasite problemi ya da tepe değerinin değiştirilmesi problemi öne çıkmaktadır.

Bütün bunlar göz önüne alınarak bu makalede önerilen yöntemin en önemli üstünlükleri ve literatüre katkısı değerlendirildiğinde çeşitli özellikler öne çıkmaktadır. İlk olarak önerilen yöntem, tepe noktasına müdahale etmemektedir. Ayrıca gizleme sonrası değişen piksellerin histogram değerinin tepe değerini aşması önlenmektedir. Böylece alıcıya bir tepe değeri bilgisi gönderme zorunluluğu ortadan kalmaktadır. Çalışmanın ikinci katkısı ise histogram dağılımında boşluk oluşturma ihtiyacını ortadan kaldırmaktır. Çalışmanın üçüncü katkısı ise benzer yöntemlere göre düşük kapasite problemini gidermektir. Bu amaçla tepe noktasının sağ veya sol tarafına veri gizlenmesi önerilmektedir. Ayrıca yüksek kapasite ihtiyacı için renkli görüntüdeki tüm renk kanallırnın histogram dağılımları kullanılabilmektedir dolayısıyla veri gizleme kapasitesi artırılmaya uygundur. Son olarak önerilen yöntem bütün bu katkıları sağlarken stego görüntünün görsel kalitesini önemli ölçüde korumaktadır. Bu özellikler göz önüne alındığında, önerilen yöntemin benzerlerine göre belirgin üstünlükleri vardır.

Sunulan çalışmanın 2. Bölümünde histogramın görüntü steganografisinde kullanımı, 3. Bölümünde önerilen komşuluk temelli hibrit yöntem anlatılmaktadır. Deneysel çalışmalar ve literatür çalışmalarıyla karşılaştırma sonuçları 4. Bölümde, steganaliz ve görünmezlik testleri ise 5. Bölümde verilmektedir. 6. Bölümde önerilen çalışmanın sonuçları verilmektedir.

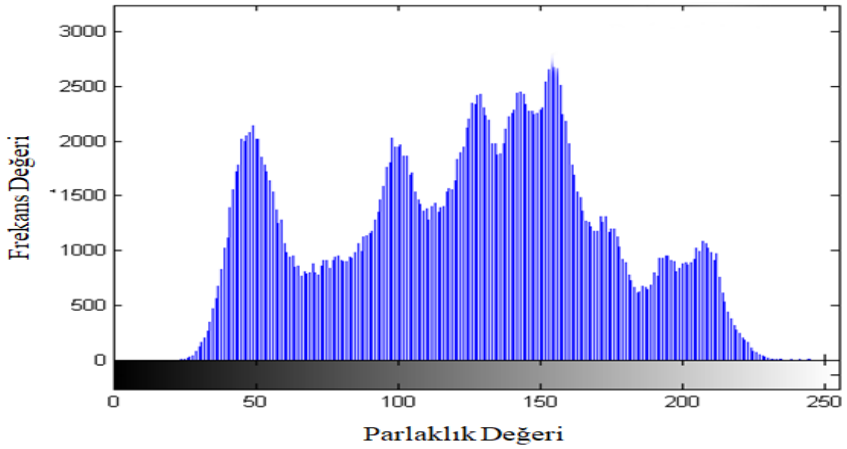
2. Görüntülerde Veri Gizlemede Histogram Kullanımı

Sayısal renkli görüntülerin en küçük üçlü nokta grubuna piksel denir. Gri seviyeli görüntülerde her piksel, 0 ile 255 arasında (8 bitlik) parlaklık seviyesi değerleri alırken, renkli görüntülerde ise her pikselin rengi Kırmızı (Red), Yeşil (Green), Mavi (Blue) olmak üzere üç ana renkten (RGB) elde edilir. Her renk değeri 0 ile 255 arasında değişen 8 bitlik değere sahiptir ve her renkli piksel değeri 24 bitten (3-Byte) meydana gelmektedir. Şekil 1'de renkli piksellerin farklı oranlarda RGB bileşiminden oluştuğu görselleştirilmiştir.



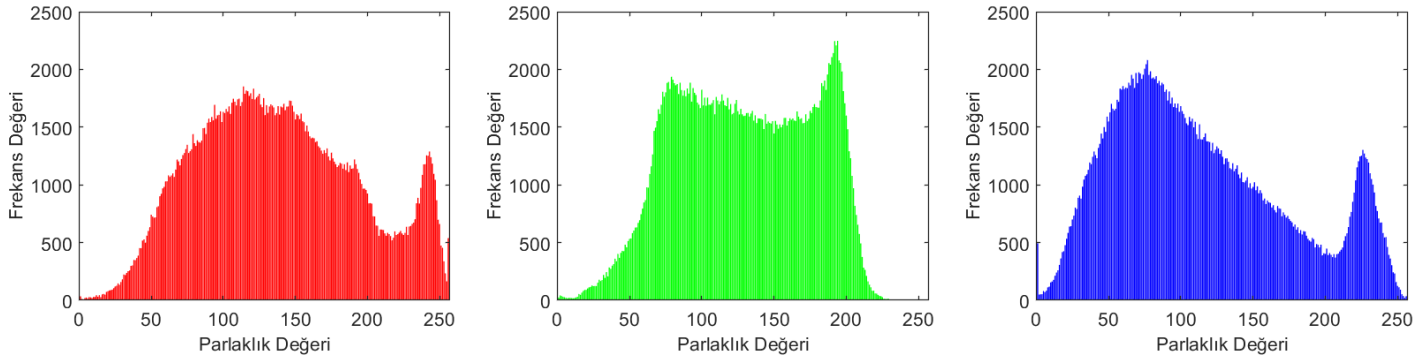
Şekil 1. 24-bit bir resmin piksel haritasındaki renk değerleri

Histogram, görüntüdeki piksel değerlerinin dağılımını ifade etmektedir. Her değerin görüntü içerisinde ne kadar bulunduğu bilgisi varlık frekansı olarak tutulmaktadır ve histogram dağılımı görüntü hakkında bilgi vermektedir. Örneğin histogram değerlerinin farklı noktalarda dağılımı görüntünün o kadar fazla renk veya ton içermekte olduğunu belirtir. Renk aralığının daralması ise yakın tonların ağırlıkta olduğu bilgisini vermektedir. Şekil 2' de örnek bir görüntü histogramı gösterilmektedir.



Şekil 2. Örnek bir histograma ait parlaklık ve frekans değerleri

Histogram grafikleri her renk değeri için elde edilebileceği gibi ortak renk karışımı değerlerine göre de oluşturulabilmektedir. Renkli görüntülerde R, G, B bileşenleri göz önüne alınarak üç adet ayrı histogram dağılım grafiği elde edilebilir. Şekil 3'te Baboon test görüntüsü için üç ayrı renk kanalının histogram dağılımları verilmiştir. Kullanılan yöntemlerde histogram değerleri R, G, B bileşenleri için ayrı ayrı oluşturulup uygun bileşen belirlenmiştir.



Şekil 3. Baboon görüntüsüne ait renk kanallarının histogram dağılımları. (a) R kanalı, (b) G kanalı, (c) B kanalı

Görüntüler üzerinde gerçekleşen steganografi uygulamaları, resmin sayısal değerlerinde küçük değişimler yapılarak gerçekleştirilmektedir. Sayısal değerlerdeki farklılıklar ya da bozulmalar insan gözü tarafından algılanamayacak seviyelerdedir.

Klasik veri gizleme yöntemlerinde histogram tabanlı veri gizleme çalışmalarından daha farklı bir bakış açısı kullanılmaktadır. Örtü dosyası olarak alınan görüntünün gri değerlerinin histogramı oluşturulmaktadır. Histogramda tepe (P) noktası tespit edilip P+1 ile 254 arasındaki değerlerin tamamını bir arttırarak histogramda bir boşluk oluşturulmaktadır. Örneğin P=120, ise [121-254] değerleri [122-255] aralığına kaydırılmaktadır. Daha sonra görüntü en baştan taranmaya başlayarak her P değerindeki piksellere gizli mesajın bir biti gizlenmektedir. Eğer gizli bit 0 ise P değerli piksel değişmez. Eğer gizli bit 1 ise, P değerli piksel P+1 yapılır. Zaten ilgili piksel değeri olan P+1 boş olduğu için (yukarıdaki örnekte 121 değeri) gizleme işlemi diğer pikselleri bozmamaktadır (Ni vd., 2006; Yalman & Ertürk, 2009).

Veri gizlerken alıcı tarafa P değerinin de gönderilmesi gerekmektedir. Alıcı tarafta stego görüntüden veri çıkartırken yine benzer şekilde piksel değerlerinde tarama yapılır. Öncelikle P değeri çıkartılır. Daha sonra pikseller içerisinde P değerine sahip olanlardan 0, piksel değeri P+1 olanlardan ise 1 çıkartılarak veri çıkartma tamamlanır. Son olarak sağa kaydırılan pikseller (P+2 ile 255 arasında olan pikseller) yeniden sola (P+1 ile 254 aralığına) geri çekilir ve görüntü eski haline çevrilir. Bu şekilde yapılan veri gizleme yönteminde maksimum veri gizleme kapasitesi başlık bilgileri dâhil olmak üzere P kadar olmaktadır (Ni vd., 2006).

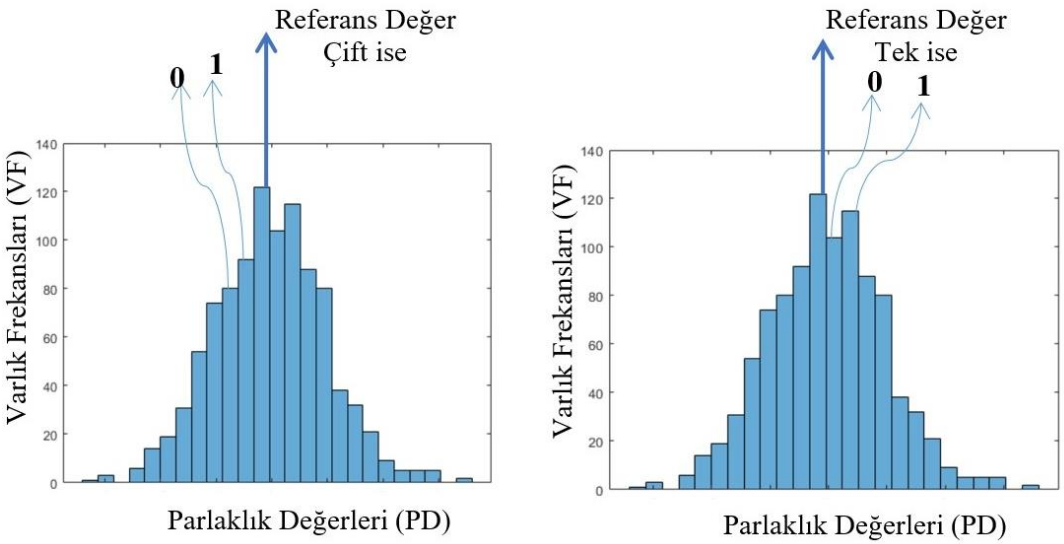
3. Önerilen Komşuluk Temelli Hibrit Veri Gizleme Yöntemi

Bu çalışmada önerilen yöntem histogram dağılımını kullanarak geliştirilen yeni bir hibrit algoritmaya dayanmaktadır. Verinin gizleneceği alanların tespiti için görüntünün histogram bilgisinden yararlanılmaktadır. Histogram değerinde değişiklik yapmak için daha önceki çalışmalarda olduğu gibi en düşük anlamlı bit (LSB) yöntemi kullanılmaktadır (Akbay vd., 2018). Hibrit yapıda olan bu yöntemin algoritmasında öncelikle histogram dağılım grafiği taranmakta ve LSB yöntemi ile gizleme işlemi yapılmaktadır. Önerilen çalışmada kapasite ve dayanıklılık artırılarak görüntü üzerindeki değişikliğin minimize edilmesi amaçlanmaktadır. Veri gizleme işlemi sonucunda histogram grafiğinin mümkün olduğunca az bozulması önemlidir. Gizleme işlemi sonucunda oluşan görüntü üzerindeki değişikliğin histogram üzerine yansımaması temel amaçlardandır.

Önerilen yöntemde öncelikle görüntü histogramında varlık frekans değeri en yüksek parlaklığın (P) değeri tespit edilmektedir. Referans alınan P değerine göre verinin gizleneceği piksel parlaklık değerleri tespit edilmektedir. Eşitlik (1)'de veri gizleme için kullanılacak piksellerin (p_g) seçimi verilmiştir. Veri gizleme işleminde referans P değerinin parlaklık değeri çift ise histogramın sol tarafındaki 2 parlaklık değeri, tek ise sağ tarafındaki 2 parlaklık değeri verinin gizlenmesi için kullanılmaktadır.

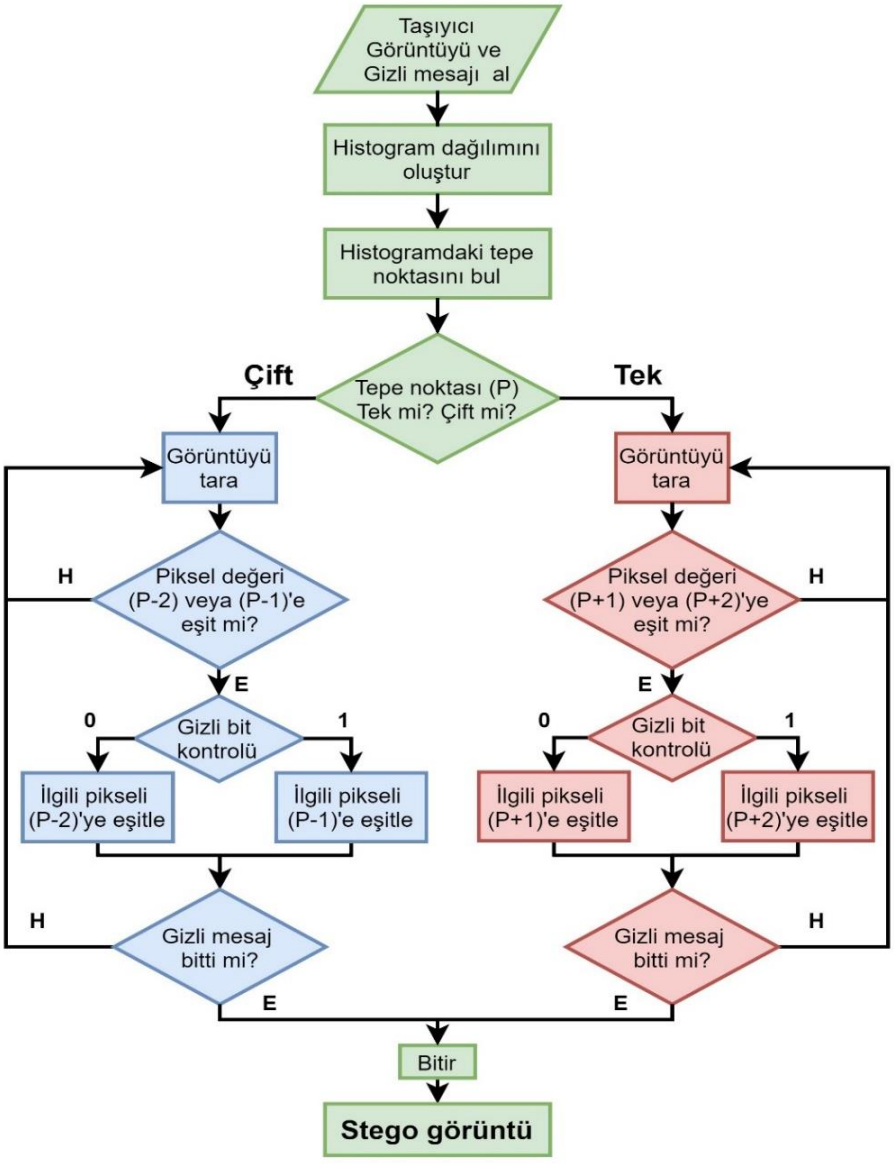
$$p_g = \begin{cases} P-1 \; ve \; P-2, & eğer \;\; P \; mod(2) = 0 \\ P+1 \; ve \; P+2, & eğer \;\; P \; mod(2) = 1 \end{cases} \quad (1)$$

Referans değerin çift veya tek olma durumunda gizlenecek veri için kullanılacak parlaklık değerleri Şekil 4'te gösterilmektedir. Referans olarak seçilen P değerine göre önerilen algoritma gizleme yapılacak pikselleri tespit etmektedir. Histogram bilgileri kullanılarak en fazla tekrar eden parlaklık değerinin çift veya tek olma durumuna göre gömülecek verilerin hangi parlaklık değerlerine gizleneceği tespit edilir. Önerilen yöntemin en önemli özelliklerinden birisi, P değerinin alıcıya gönderilme ihtiyacını ortadan kaldırmasıdır.



Şekil 4. Önerilen yöntemde gizleme için kullanılacak bitlerin parlaklık değerinin tespiti

RGB gibi üç kanallı görüntülerde bu algoritma her kanal için histogram dağılımları hesaplanarak aynı işleme tabi tutulması ile gerçekleştirilmektedir. Şekil 5'te önerilen yakın histogramlar yöntemiyle veri gizlemenin akış şeması verilmiştir.



Şekil 5. Yakın histogramlar yöntemi veri gizleme akış şeması

Önerilen yöntemle gömülen veri içerisindeki her karakterin ASCII karşılığı ikili sayı sistemine çevrilir. Türkçe karakterlerin olma durumu göz önünde bulundurularak her karakter 10 bitlik sayılarla ifade edilir. Önerilen yöntemde veri gizlemek için kullanılan yakın histogramlar yöntemi (YHY) için uygulanan işlem adımları aşağıdaki gibidir:

Adım 1. Taşıyıcı görüntünün histogramı oluşturulur.
Adım 2. Histogram dağılımından yararlanılarak en fazla tekrarlanma sayısına (varlık frekansına) sahip değer olan P elde edilir.
Adım 3. P değerinin tek veya çift olma durumuna bakılır.
Adım 4. Eşitlik 1'den yararlanılarak gizleme için kullanılacak olan pikseller tespit edilir.
Adım 5. P'nin tek olduğu durumlarda P+1 ve P+2 parlaklık değerine sahip olan pikseller, P'nin çift olduğu durumlarda ise P-1 ve P-2 parlaklık değerine sahip olan pikseller gizleme için kullanılır.
Adım 6. Gizlenecek bit değeri alınır.
Adım 7. Görüntü piksel değerleri taranmaya başlanır.
Adım 8. Gizlenecek bit değeri 1 ise karşılaşılan ilk komşuluk (P+1, P+2 veya P-1, P-2) değerinin P-1 veya P+2 olması sağlanır. Eğer piksel değeri P-1 veya P+2 ise değiştirilmez. Eğer piksel değeri P-2 veya P+1 ise ilgili pikselin değeri bir arttırılarak P-1 veya P+2 elde edilir.
Adım 9. Gizlenecek bit değeri 0 ise karşılaşılan komşuluk (P+1, P+2 veya P-1, P-2) değerinin P-2 veya P+1 olması sağlanır. Eğer piksel değeri P-2 veya P+1 ise değiştirilmez. Eğer piksel değeri P-1 veya P+2 ise ilgili pikselden ilgili pikselin değeri bir azaltılarak P-1 veya P+2 elde edilir.
Adım 10. Gömü verisi sonlanıncaya kadar sonraki gizli bit değeri için görüntüde son gizlemenin yapıldığı piksel adres bilgisi alınıp tekrar Adım 6'ya gidilir.
Adım 11. Gömü verisi sonuna NULL $(0000000000)_2$ kodu eklenerek stego görüntü elde edilir.

Gizlenmek istenen mesajın ilk harfi için 10 bit değeri $(1011101110)_2$ olarak kabul edilsin. Veri gizleme için Şekil 2'de verilen örnek histogram dağılımına sahip görüntüyü kullandığımızı varsayalım. Örtü dosyası olarak kullanılacak bu görüntünün histogramı incelendiğinde, varlık frekansı en yüksek olan parlaklık değeri ve komşu değerlerinin tekrarlanma sayıları Tablo 1'deki gibidir.

Tablo 1. Örnek görüntüdeki maksimum histogram değeri ve komşu değerleri

	P-2	**P-1**	**P**	**P+1**	**P+2**
Parlaklık Değeri	*158*	*159*	*160*	*161*	*162*
Varlık frekansı	*2420*	*2575*	*2730*	*2550*	*2480*

Önerilen yöntemde ilk olarak görüntünün histogramından yararlanılarak en fazla tekrarlanan değer P=160 olarak tespit edilir. P değeri çift olduğundan veri gizlemek için solda kalan parlaklık değerine (158 ve 159) sahip olan pikseller kullanılacaktır. Bu değerlikli pikseller sırayla ele alınır ve gizelenecek olan değer "0" ise ilgili pikselin değeri "158" olarak, gizlenecek değer "1" ise piksel değeri "159" olarak ayarlanır. İlk olarak gömü verisinin (yani $(1011101110)_2$) ilk biti olan 1 değerinden başlanır. İlk bit değeri olan "1" alınarak örtü görüntüsündeki piksel değeri "158" veya "159" olan piksellerden herhangi birine ulaşılıncaya kadar görüntü okunur. Karşılaşılan ilk değer "159"ise değişiklik yapılmaz, "158"ise parlaklık değeri "159"olarak değiştirilir. Sonraki gizli bit olan "0" değeri için kalındığı yerden itibaren görüntü okunmaya devam edilir. Karşılaşılan ilk "158" veya "159" parlaklık değeri için, piksel değeri "158" ise değişiklik yapılmaz. Piksel değeri "159" ise "158" olarak piksel parlaklık değeri değiştirilir. Gömü verisi sonlanıncaya kadar bu döngü devam eder. Gizleme bitince stego görüntü elde edilerek alıcıya gönderilir. Burada dikkat edilmesi gereken husus, gizleme işlemi sonucunda en fazla tekrarlanan parlaklık değerinin (P) değişmemiş olması gerekmektedir. P değerinin aşılmaması için bir sayaç kullanılmaktatır. Bu sayaç verinin gizleme sonrası komşu historam değerlerinin P'den küçük değerlerde kalması sağlanmaktadır.

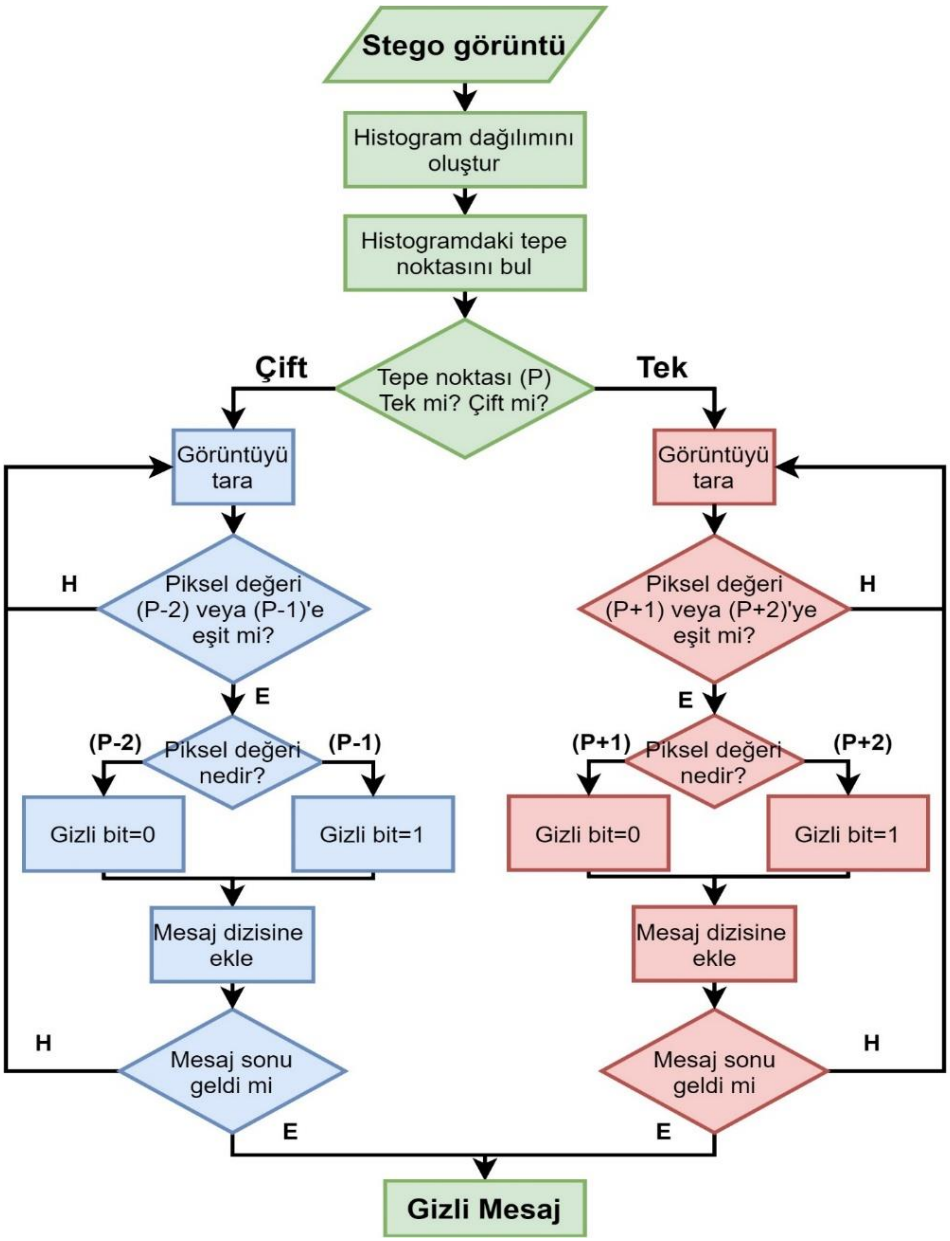
Alıcı tarafında, sadece stego görüntü ve gizleme algoritmasına uyumlu veri çıkartma algoritması kullanılarak gizli bit dizisi tekrar elde edilebilmektedir. Şekil 6'da önerilen yakın histogramlar yöntemiyle veri çıkartmanın akış şeması yer almaktadır. Gizli bit dizisinin i. sırasındaki elemanı b_i ve tarama sırasında karşılaşılan piksel değeri p_t olmak üzere veri çıkartımı Eşitlik (2)'ye göre yapılmaktadır.

$$b_i = \begin{cases} 0\,, & eğer\ \ P\ çift\ ve\ p_t = P-2\ ise \\ 1\,, & eğer\ \ P\ çift\ ve\ p_t = P-1\ ise \\ 0\,, & eğer\ \ P\ tek\ \ ve\ p_t = P+1\ ise \\ 1\,, & eğer\ \ P\ tek\ \ ve\ p_t = P+2\ ise \end{cases} \tag{2}$$

Önerilen yakın histogramlar yönteminde veri çıkartmak için uygulanan işlem adımları aşağıdaki gibidir:

Adım 1. Alıcıya gelen, gizli mesajı içeren stego görüntünün histogramı oluşturulur.
Adım 2. Histogram dağılımında varlık frekansı en yüksek değer olan tepe değeri P elde edilir.
Adım 3. P değerinin tek veya çift olma durumuna bakılır.
Adım 4. Eşitlik (1)'den yararlanılarak gizli mesaj içeren pikseller tespit edilir.

Adım 5. P'nin tek olduğu durumlarda gizli bitler P+1 ve P+2 parlaklık değerinde olan piksellerde, P'nin çift olduğu durumlarda ise gizli bitler P-1 ve P-2 parlaklık değerine sahip olan piksellerde bulunur.
Adım 6. Görüntü piksel değerleri taranmaya başlanır.
Adım 7. Eşitlik (2)'ye göre gizli bitler çıkarılır ve bit dizisine sırayla eklenir.
Adım 8. Gömü verisi sonu kodu olan NULL $(0000000000)_2$ değeri elde edilince kadar Adım 5'e gidilir.
Adım 9. Elde edilen metin dizisi 10 bitlik gruplara ayrılarak gizli mesaj elde edilir.

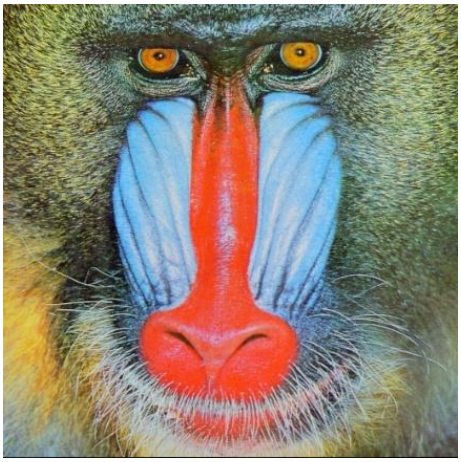


Şekil 6. Yakın histogramlar yöntemi gizli veriyi çıkarma akış şeması

4. Deneysel Çalışmalar

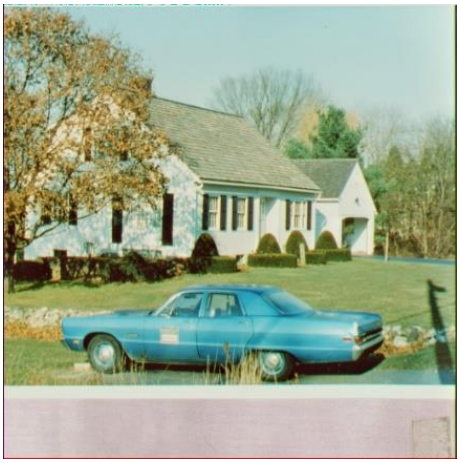
Önerilen yöntem çeşitli örtü dosyaları üzerinde test edilmiştir. Standart örtü dosyaları olarak kullanılan 512×512 boyutundaki renkli görüntülerden Airplane, Baboon, Fruits, House, Peppers ve Sailboat Şekil 7'de verilmektedirler. Yapılan testlerde gizli mesaj olarak çeşitli uzunluklardaki metinler kullanılmıştır.

Airplane



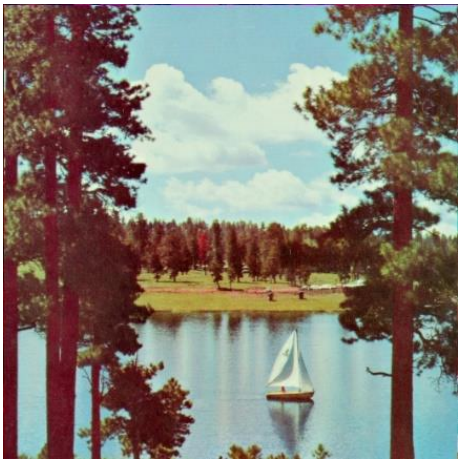
Baboon

Fruits



House

Peppers



Sailboat

Şekil 7. Örtü dosyası olarak kullanılan bazı test görüntüleri.

Önerilen veri gizleme yöntemin sonuçları kapasite ve görsel kalite üzerinden değerlendirilmiştir. Stego görüntülerin görsel kalitelerini değerlendirmek için tepe sinyal-gürültü oranı (peak signal to noise ratio-PSNR) sonuçlarına bakılmaktadır.

$$PSNR = 10 \times log_{10}(\frac{255^2}{MSE(I_O, I_S)}) \tag{3}$$

$$MSE(I_O, I_S) = \frac{1}{M \times N} \times \sum_{m=1}^{M-1} \sum_{n=1}^{N-1} [I_O(m,n) - I_S(m,n)]^2 \tag{4}$$

Eşitlik (3) ve (4)'teki I_O ve I_S sırasıyla orijinal ve stego görüntülerini, M ve N ise görüntü boyutlarını göstermektedir. Ortalama karesel hata (Mean squared error, MSE), işlem sonucu stego görüntüdeki piksellerin değişmesinden kaynaklanan karesel hatayı göstermektedir. Eğer iki görüntü aynı ise MSE değeri sıfır olmakta, en yüksek bozulma durumunda ise MSE değeri 1 olmaktadır (Sencar vd., 2004).

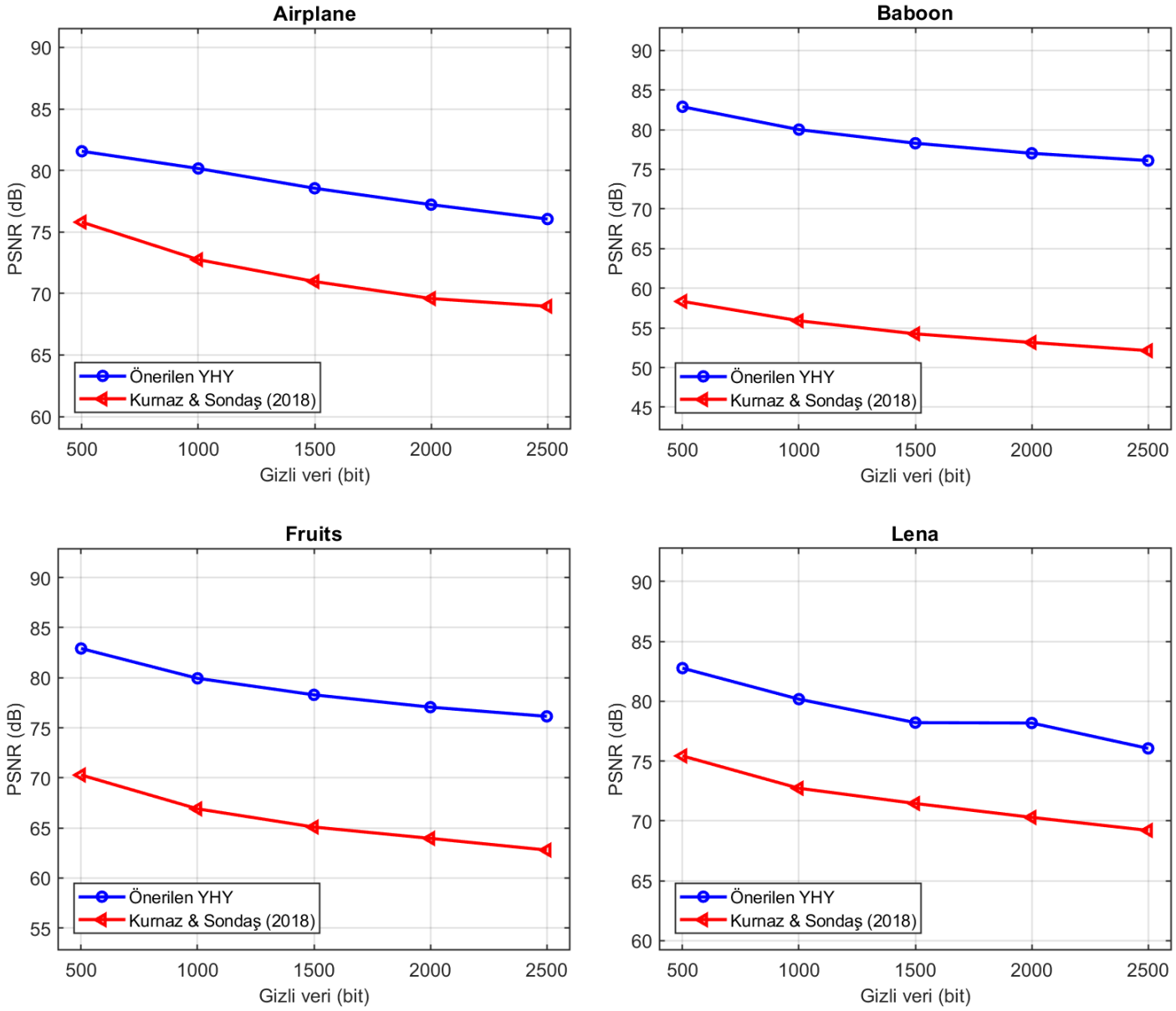
PSNR değeri görsel kaliteyi ifade etmekte olup MSE ile arasında ters orantılı bir ilişki bulunmaktadır. Düşük MSE daha az hata yani daha yüksek kalite anlamına gelmektedir. İki görüntü arasındaki benzerlik arttıkça PSNR değeri de yükselmektedir. Orijinal ve stego görüntüleri aynı olduğunda PSNR değeri sonsuz olmaktadır.

Önerilen yakın histogramlar temelli veri gizleme yönteminin taşıyıcı görüntüde meydana getirdiği görsel kalite değişimi daha önce geliştirilen benzer bir çalışmayla (Kurnaz & Sondaş, 2018) birlikte gösterilmektedir. Tablo 2'de önerilen yöntemin PSNR başarımı verilmiştir.

Tablo 2. Önerilen yöntemin PSNR değerleri

	PSNR(dB)	
Görüntü	**Önerilen YHY**	**Kurnaz & Sondaş (2018)**
Airplane	*79,87*	*72,62*
Baboon	*79,99*	*55,84*
Fruits	*79,94*	*66,90*
House	*80,27*	*70,19*
Peppers	*80,16*	*70,27*
Sailboat	*80,19*	*72,65*

Önerilen yöntemin görsel kalitesi taşıyıcı görüntülere farklı miktarlardaki veri gizleme sonucunda tekrar incelenmiştir. Şekil 8'de önerilen yöntemin benzer yönteme göre çok daha iyi görsel kaliteye sahip olduğu görülmektedir.



Şekil 8. Önerilen yöntemin farklı kapasitedeki gizli veriler için görsel kalite değerlendirmesi.

Göndericinin yolladığı stego nesneden gizli mesajın doğru çıkartılması gerekmektedir. Aksi durumda gizli mesajda hatalar ortaya çıkmaktadır. Gömülen ve çıkarılan iki mesaj arasındaki hata miktarını kontrol etmek için kullanılan bit hata oranı için BER (bit error rate) değeri eşitlik (5)'teki gibi hesaplanmaktadır.

$$BER(\%) = \sum_{k=1}^{K} \frac{[M_g(k) \oplus M_c(k)]}{K} \times 100 \quad (5)$$

burada M_g ve M_c gizlenen ve çıkarılan gizli mesajları göstermektedir. K gizli mesaj uzunluğu, $\oplus$ ise özel veya (ex-or) mantıksal ifadesidir. BER değeri en iyi durumda 0 olmaktadır. BER değeri gizli mesajın alıcı tarafından ne kadar hangi oranda bozulduğunu göstermektedir. Tablo 3'te dört test görüntüsü için değişik uzunluklarda gizlenen mesajın BER değerleri gösterilmektedir. Görüldüğü üzere, gizlenen mesaj alıcı tarafında herhangi bir bozulmaya uğramadan elde edilebilmiştir.

Tablo 3. Önerilen yöntemin BER değerleri

	500 bit	**1000 bit**	**1500 bit**	**2000 bit**	**2500 bit**
Airplane	*%0*	*%0*	*%0*	*%0*	*%0*
Baboon	*%0*	*%0*	*%0*	*%0*	*%0*
Fruits	*%0*	*%0*	*%0*	*%0*	*%0*
Lena	*%0*	*%0*	*%0*	*%0*	*%0*

Bu çalışma kapsamında geliştirilen yöntemin literatür yöntemlerine göre önemli oranda üstünlüğü bulunmaktadır. Tablo 4 ve Tablo 5' te veri gizleme sonucu elde edilen Lena ve Baboon stego görüntülerinin literatürdeki çalışmalarla kıyaslanması gösterilmektedir.

Tablo 4. Önerilen yöntemin literatür çalışmalarıyla PSNR karşılaştırma sonuçları (2500 bitlik gizli mesaj için)

	PSNR(dB)	
Veri gizleme yöntemi	**Baboon**	**Lena**
Önerilen YHY	***76,10***	***76,06***
Islamy & Ahmad (2019)	*68,81*	*66,77*
Solak (2019)	*53,69*	*50,47*
Kurnaz & Sondaş (2018)	*52,13*	*69,21*
Lin & Li (2011)	*52,75*	*50,51*
Ni vd. (2006)	*53,67*	*57,94*
Kuo vd. (2008)	*48,20*	*48,20*
Hwang vd. (2008)	*48,20*	*48,20*

Tablo 4'te verilen sonuçlar değerlendirildiğinde, önerilen yöntem benzer yöntemlere göre ciddi oranda görsel kapasiteyi korumaktadır. Benzer gizleme kapasiteleri için önerilen yöntem en yakın PSNR değerine sahip çalışma olan Islamy & Ahmad (2019) yönteminden yaklaşık 8 dB daha üstün PSNR değerine sahiptir. Tablo 5'te 1000 bitlik veri gizleme için önerilen yöntem en yakın değerlere sahip yöntemler olan Kurnaz & Sondaş (2018) ve Yalman & Ertürk (2009) çalışmalarından çok daha yüksek PSNR değerlerine sahiptir. Önerilen yöntemdeki PSNR değerlerinin bu derece yüksek olmasının en önemli sebebi, geliştirilen hibrit yaklaşımdan kaynaklanmaktadır. Daha önceki histogram tabanlı yöntemler tepe noktasının etrafını boşaltmak için histogramda tepe değeri hariç tüm pikselleri ötelemekteydi. Oysaki önerilen yöntemde herhangi bir ötelemeye ihtiyaç duyulmadığı için stego görüntülerin görsel kalitesi büyük oranda korunmaktadır.

Tablo 5. Önerilen yöntemin literatür çalışmalarıyla PSNR karşılaştırma sonuçları (1000 bitlik gizli mesaj için)

	PSNR(dB)	
Veri gizleme yöntemi	**Baboon**	**Lena**
Önerilen YHY	***79,99***	***80,17***
Kurnaz & Sondaş (2018)	*55,84*	*72,73*
Yalman & Ertürk(2009)	*59,25*	*62,75*
Lin & Li (2011)	*53,33*	*53,43*
Ni vd. (2006)	*53,78*	*58,08*
Kuo vd. (2008)	*51,35*	*51,21*
Hwang vd. (2008)	*48,20*	*48,20*

5. Steganaliz ve Görünmezlik Testleri

Veri gizleme yöntemlerinin kalitesinin kontrol edildiği bir başka yön ise steganaliz testleri ve istenmeyen kişiler tarafından tespit edilemezlik durumudur. Tablo 6'da ilk olarak önerilen yöntemin orijinal histogram dağılımında herhangi bir öteleme ve değişim meydana getirip getirmediği incelenmektedir.

Tablo 6. Baboon görüntüsü için histogram test sonuçları

Veri gizleme yöntemi	Histogram Değişimi
Önerilen YHY	*Dağılım değişmez (sadece2 değerin dağılımı değişir)*
Yalman & Ertürk(2009)	*Dağılım Değişir*
Klasik LSB	*Dağılım Değişir*

Piksel bozulma oranı için görüntüde değişen piksellerin tüm piksellere oranına bakılmaktadır. Piksel bozulma oranlarını karşılaştırması Tablo 7'de verilmektedir. Önerilen yöntemin pikselleri bozma oranı diğer çalışmalara göre oldukça düşük düzeyde kalmaktadır.

Tablo 7. Baboon görüntüsü için piksel değişim oranları

Veri gizleme yöntemi	Piksel bozulma oranı
Önerilen YHY	$2{,}1 \times 10^{-5}$
Kurnaz & Sondaş (2018)	$11{,}8 \times 10^{-5}$
Yalman & Ertürk(2009)	$11{,}9 \times 10^{-5}$
Klasik LSB	$10{,}9 \times 10^{-5}$

Son olarak önerilen yöntemle elde edilen stego görüntülerin görünmezlik durumları kontrol edilmiştir. Görünmezlik veri gizleme yöntemlerini tespit etmek için hazırlanan iki farklı uygulama ile test edilmiştir. Tablo 8'de "StegSpy" ve "StegDetect" uygulamalarının sonuçları verilmektedir. Her iki uygulama da stego görüntü içerisinde yakın histogram temelli yöntemle gizlenen verinin varlığını tespit edememiştir.

Tablo 2. Baboon görüntüsü için steganaliz test sonuçları

Veri gizleme yöntemi	StegSpy testi	StegDetect testi
Önerilen YHY	*Tespit Edilmedi*	*Tespit Edilmedi*
Kurnaz & Sondaş (2018)	*Tespit Edildi*	*Tespit Edildi*
Yalman & Ertürk(2009)	*Tespit Edildi*	*Tespit Edildi*
Klasik LSB	*Tespit Edildi*	*Tespit Edildi*

6. Sonuç

Bu çalışmada, görüntülere veri gizlemek için kullanılabilecek yakın histogramlar temelli bir veri gizleme yöntemi önerilmektedir. Önerilen yöntemde, histogram dağılımındaki tepe noktasının tek veya çift olma durumuna göre gizli mesaj görüntü içerisine gizlenmektedir. Böylece histogram dağılımında herhangi bir kaydırmaya ihtiyaç duyulmamaktadır. Bununla birlikte histogramdaki tepe noktası bilgisini alıcıya gönderme ihtiyacını ortadan kaldırmak için tepe noktasının komşularına gizleme yapılmaktadır. Ayrıca yüksek kapasiteli gizlemeye uyumlu olması için tüm renk kanallarının histogramı ayrı ayrı kullanılabilmektedir. Deneysel sonuçlar incelendiğinde önerilen yöntemle veri gizlenen görüntülerin görsel kalitesinin literatürdeki çalışmalara göre daha yüksek olduğu görülmektedir. Bunun en önemli sebebi önerilen yöntemin histogramda boşluk açmaya ihtiyaç duyulmamasıdır. Dolayısıyla histogram dağılımında çok fazla bir değişiklik olmamaktadır. Önerilen yöntemde farklı oranlarda gizlenen veri miktarlarında da görsel kalite korunmaktadır. Başarılı bir veri gizleme uygulamasında stego nesnenin görüntü kalitesi, gizlenen mesajın haberleşme kanalında tespit edilememesi ve gizli mesajın alıcı tarafından doğru çıkartılması önemlidir. Önerilen yakın histogramlar temelli yöntemin kullanılması kapasite, dayanıklılık ve taşıyıcıdaki değişim ilişkisini iyi koruduğu ortaya konulmuştur. Ayrıca gizli mesaj herhangi bir bozulmaya uğramamakta ve alıcıda tamamen doğru bir biçimde elde edilmektedir. Gelecekte yapılacak çalışmalarda, örtü dosyasının bloklara ayrılması sonucunda yapılacak gizlemeler önerilen yöntemin kapasitesinin daha da artırılmasını sağlayacaktır. Ayrıca geliştirilen uygulamada veriler şifrelenmeden görüntü üzerine gömülmektedir. Daha güvenli biçimde veri gizleme ihtiyacı olduğunda gömü verisinin şifrelenip gömülmesi dayanıklılığa katkı sağlayacaktır.

Kaynakça

Chang C. C., Tai W. L. & Chen K. N. (2008). Lossless Data Hiding Based on Histogram Modification for Image Authentication, *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Shanghai, 506-511.

Chen, X., Sun, X., Sun, H., Xiang, L. & Yang, B., (2015). Histogram shifting based reversible data hiding method using directed-prediction scheme, *Multimed Tools Appl,* 74, 5747–5765.

Chrysochos E., Fotopoulos V., Skodras A. & Xenos M. (2007, May). Reversible Image Watermarking Based on Histogram Modification, *11th Panhellenic Conference on Informatics with international participation*, Patras, Greece.

Gutub A., Ankeer M., Abu-Ghalioun M., Shaheen A. & Alvi A. (2008, March). Pixel Indicator High Capacity Technique for RGB Image Based Steganography, *WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E.

Hwang, J. H., Kim, J. W. & Choi, J. U. (2006). A reversible watermarking based on histogram shifting. In: Y.Q. Shi, B. Jeon. (Eds.) *Digital Watermarking. IWDW 2006. Lecture Notes in Computer Science*, (4283, 348-361) Berlin, Heidelberg: Springer

Islamy, C. C. & Ahmad, T. (2019). Histogram-based multilayer reversible data hiding method for securing secret data, *Bulletin of Electrical Engineering and Informatics*, 8(3), 1128-1134.

Konyar, M. Z., Akbulut, O., & Öztürk, S. (2018, Sept). Matrix Encoding Based Data Hiding in HEVC, *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, Sarajevo, 662-665.

Kuo, W. C., Jiang, D. J. & Huang, Y. C. (2008). A reversible data hiding based on block division, *Congress on Image and Signal Processing*, Sanya, Hainan, 365-369.

Kurnaz H. & Sondaş A. (2018, Nov). Histogram Temelli Bir Veri Gizleme Yönteminin Uygulanması, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi*, Kocaeli, Türkiye.

Lin, Y. C. & Li, T. S. (2011). Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting, *Journal of Multimedia*, 6(4), 349-358

Meiamai V., Minu A. & Anushia Devi R. (2013). Histogram Technique with Pixel Indicator For High Fidelity Steganography, *International Journal of Engineering and Technology*, 3(5), 0975-4024.

Mohammed A. & Al-Husainy F. (2015). Image Steganography Method Preserves the Histogram Shape of Image, *European Journal of Scientific Research*, 1(130), 101-106.

Ni Z., Shi Y.Q., Ansari N., Su W. (2006). Reversible Data Hiding, *IEEE Transactions on Circuits and Systems for Video Technology*, 16(3), 354-362.

Pan, Z., Hu, S., Ma, X. & Wang, L., (2015). Reversible data hiding based on local histogram shifting with multilayer embedding, *J. Vis. Commun. Image R.,* 31, 64-74.

Patel Z. V. & Gadhiya S. A. (2015). A Survey Paper on Steganography and Cryptography, *International Multidisciplinary Research Journal (RHIMRJ)*, 2(5), 1-5.

Sencar H.T., Ramkumar M., & Akansu A.N. (2004). *Data Hiding Fundamentals and Applications*, New York: Elsevier, Academic Press.

Solak, S. (2019, April). Görüntü Histogramında Yer Alan En Yüksek Değere Verilerin Kayıpsız ve Geri Dönüşümlü Gizlenmesi, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi Bildiriler Kitabı*, Cilt I, 323-327, Kocaeli, Turkiye.

StegSpy, Erişim Adresi: *http://www.spy-hunter.com/stegspy* (Son Erişim tarihi: 20.12.2019)

StegDetect, Erişim Adresi: *https://stegdetect.apponic.com/* (Son Erişim tarihi: 20.12.2019)

Xuan G., Shi Y. Q., Chai P., Cui X., Ni Z. & Tong X. (2007, 3- 5 December). Optimum Histogram Pair Based Image Lossless Data Embedding, in Proc. *Int. Workshop Digit. Watermarking Ser. Springer Lect. Notes Comput. Sci*., Guangzhou, China.

Yalman, Y., Çetin, Ö., Ertürk İ. & Akar, F. (2014). Veri gizleme. İstanbul: Beta Yayınevi.

Yalman Y., Ertürk İ. (2009, February). İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulaması, *XI. Akademik Bilişim Konferansları*, Harran Üniversitesi, Şanlıurfa.

Wu, H., Dugelay, J & Shi, Y. (2015). Reversible Image Data Hiding with Contrast Enhancement, *IEEE Signal Processing Letters*, 22(1), 81-85.