GÖRÜNTÜ HİSTOGRAMINDA YER ALAN EN YÜKSEK DEĞERE VERİLERİN KAYIPSIZ VE GERİ DÖNÜŞÜMLÜ GİZLENMESİ

Dr. Serdar SOLAK
Kocaeli Üniversitesi, Enformatik Bölümü
serdars@kocaeli.edu.tr

Özet
Verilerin, görüntü dosyaların içerisine üçüncü kişiler tarafından fark edilmeyecek biçimde saklanması Görüntü Steganografisi olarak adlandırılmaktadır. Görüntü Steganografisi çalışmalarında temel amaç, örtü görüntü ile stego görüntü benzerlik oranı, veri gizleme kapasitesi, stego görüntü kalitesi gibi değerlendirme ölçütlerinin yüksek olmasını sağlamaktır. Ayrıca, stego görüntü içerisinde yer alan veri elde edildikten sonra orijinal örtü görüntünün kayıpsız bir şekilde elde edilmesi tıp, sanat ve askeri uygulamalarda önemlidir. Çalışmada, örtü görüntülere kayıpsız ve geri dönüşümlü veri gizlenme yapılabilmesi için görüntü histogramı yöntemi kullanılmıştır. Gizlenecek olan veriler, görüntü histogramında en fazla yer alan değerin değiştirilmesi ile saklanmaktadır. Deneysel çalışmalarda, verilerin görüntüye gizlenmesi ve tekrar elde edilmesi %100 başarımla gerçekleştirilmiştir. Ayrıca, örtü görüntü orijinal hali kayıpsız bir şekilde elde edilmiştir.

Anahtar Kelimeler: Görüntü Histogramı, Görüntü Steganografisi, Güvenlik, Veri Gizleme

HISTOGRAM-BASED REVERSIBLE DATA HIDING METHOD USING MAXIMUM HISTOGRAM VALUE

Abstract
It is called Image Steganography to store data in an image file that will not be noticed by third parties. The main purpose of image steganography studies is to ensure that the evaluation criteria are high, such as similarity ratio between cover image and stego image, data hiding capacity and stego image quality. Furthermore, it is important to obtain the cover image lossless in many applications as medical, art and military, after the data in the stego image is extracted. In this study, the image histogram-based reversible data hiding method was used to conceal data into cover image. The secret data is concealed by changing the value that is most commonly found in the image histogram. In experimental studies, the concealment and retrieval of secret data was performed at a rate of 100%. In addition, the original cover image was obtained lossless.

Keywords: Image Histogram, Image Steganography, Reversible Data Hiding, Security

1. GİRİŞ

Verilerin görüntülerin içerisine anlaşılmayacak şekilde saklanması Görüntü Steganografisi olarak bilinmektedir. Görüntü Steganografisinde, gizlenecek veri, veriyi saklayacak örtü görüntü, veri gizleme yöntemi ve verinin örtü görüntüye gizlenmesi sonucunda elde edilen stego görüntü kavramları yaygın olarak kullanılmaktadır. Görüntü Steganografisi konusunda yapılan çalışmalarda, stego görüntü içerisinden verinin elde edilmesi (Non-Reversible Data Hiding) ve stego görüntü içerisinde yer alan verinin çıkarılmasından sonra, orjinal örtü görüntüsünün tamamen elde edilmesi kayıpsız ve geri dönüşümlü veri gizleme (Reversible Data Hiding (RDH)) olarak iki farklı sınıfta incelenmektedir. Sadece verinin örtü görüntüye gizlenmesi ve stego görüntüden çıkarılmasına yönelik yapılan çalışmalarda en düşük anlamlı bitlere verilerin gömülmesi (Solak ve Altınışık, 2019), görüntü pikselleri arasındaki fark değerleri (Prasad ve Pal, 2017) yöntemleri ve iki yöntemin birleşimi ile oluşan metodlar kullanılmaktadır (Jung, 2018; Pradhan ve Ark., 2018). RDH çalışmalarında, fark genişlemesi (Oruganti ve Ark., 2019), tahmin hatası genişlemesi (He ve Ark., 2018; Yi ve Ark., 2018), çift stego görüntü (Lu ve Ark., 2015; Chi ve Ark., 2018) ve histogram kaydırma tabanlı (Li ve Li, 2017) olmak üzere dört grupta incelenmektedir. Fark genişlemesi yönteminde, iki komşu piksel arasındaki fark dikkate alınarak veri gömülmesi sağlanmaktadır. Fark genişleme algoritmaları kullanılarak yapılan veri gizleme işlemi sonrasında elde dilen stego görüntüde ciddi oranda görsel bozulmalar oluşmaktadır. Tahmin hatası genişleme yönteminde, bu bozulmaları aza indirmek ve engellemek amacıyla, kenar tespit yöntemleri

kullanılmış ve örtü görüntü için tahmin değerleri üretilmiştir. Genel olarak yöntemin kullanılmasında, örtü görüntü ile tahmini değeri arasındaki hata veri gömme işlemi için genişletilmektedir. Bu yöntemin kullanılması soncunda görüntüde stego görüntüdeki bozulmalar aza indirgenmiş olmaktadır. Çift stego görüntü yönteminde ise, örtü görüntünün kopyaları yaratılmakta ve veri kopyalarının içerisine gizlenmektedir. Bu yöntemde, üçüncü kişilerin gizli veriyi elde etmesi için iki stego görüntüye de sahip olması gerektiğinden daha güvenli bir yöntemdir. Genellikle çift stego görüntü yöntemi, gizlenecek veri kapasitesini arttırmak amacıyla kullanılmaktadır. Histogram tabanlılarda yöntemlerde, örtü görüntüyü oluşturan piksel değerlerine ait histogram oluşturulmaktadır. Elde edilen histogramda maksimum ve minimum değerler bulunarak bu değerlere göre histogram kaydırma işlemi uygulanmaktadır.

2. MATERYAL VE METOD

Çalışmada örtü görüntülere verilerin kayıpsız ve geri dönüştürülebilir bir şekilde gizlenmesi amacıyla histogram tabanlı veri gizleme yöntemi kullanılmaktadır. Örtü görüntüye ait histogramda en büyük değere sahip renk değerinin komşu iki piksel değerine dağıtılması ile gerçekleştirilmektedir. Gizlenecek olan veride yer alan bit sayısı kadar, en yüksek sayıdaki piksel değerinden histogramda yer alan diğer komşu iki piksele aktarım gerçekleşmektedir. Bu aktarma işlemi, gizlenecek olan verideki bit değerinin 0 veya 1 olmasına göre alt komşu veya üst komşu değerinin histogramdaki dağılımını arttırmaktadır. Histogramda yer alan sadece en yüksek değerin değiştirilmesi kullanılarak, en fazla elde edilen histogramda yer alan maksimum değer kadar bit gizlenebilmektedir. Ancak yöntemde veri gizleme kapasitesinin arttırılması amacıyla farklı sayıda yer alan renk dağılımları da dikkate alınabilir. Önerilen yöntemin veri gizleme algoritması maddeler halinde sunulmaktadır.

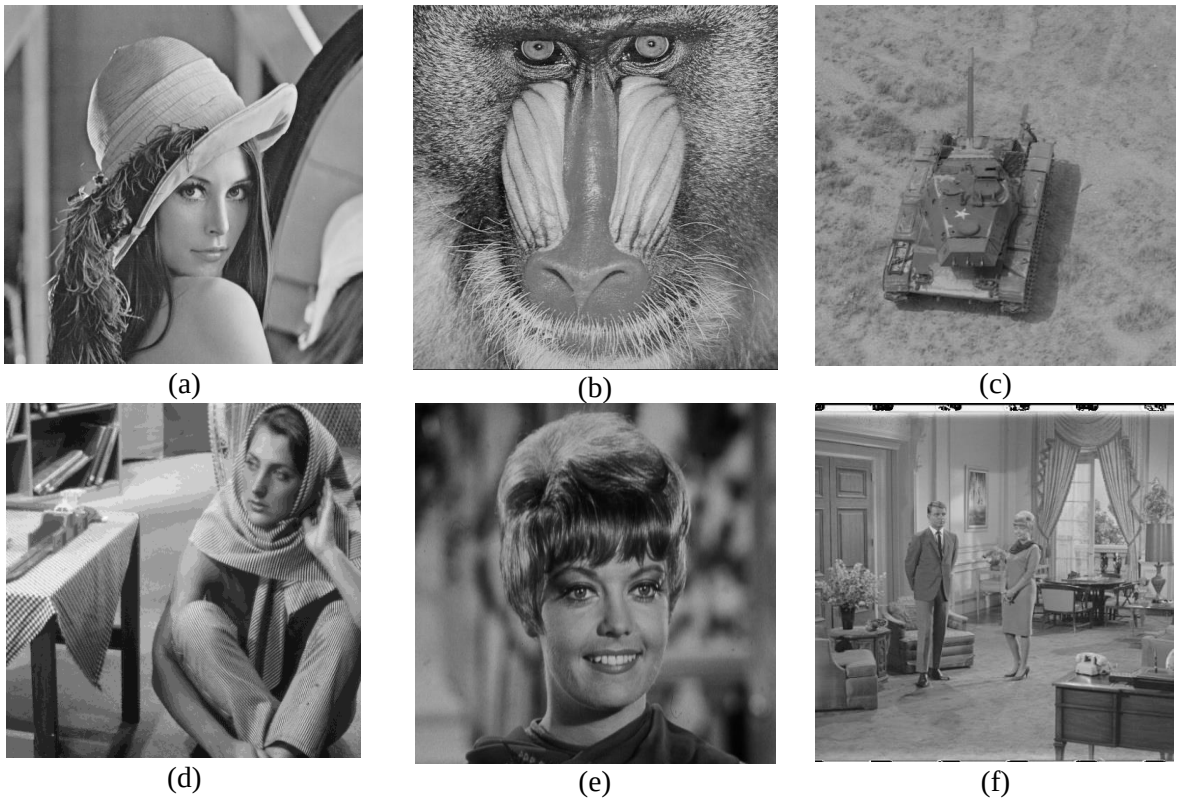
1. Örtü görüntüye ait histogramı oluştur.
2. Histogramda yer alan maksimum ve minimum değerleri ve hangi renge değerine ait olduklarını bul.
3. Histogramda yer alan maksimum renk adetine sahip renk değerine en yakın komşu minimum renk değerleri bul.
4. Örtü görüntü histogramını maksimum-minimum renk değerleri arasında kaydır.
5. Gizlenecek olan veriyi kullanıcıdan al ve ikili sayı sistemine çevir
6. Histogramı kaydırılmış görüntü içinden renk değerini al maksimum değere eşitse;
    a. Gizlenecek veri bitinin değeri 1 ise görüntüye ait ilgili pikselin değerini 1 arttır veya azalt (max ve min piksel değerlerine göre değişmektedir.).
    b. Gizlenecek veri bitinin değeri 0 ise görüntüye ait ilgili pikseli aynı bırak
7. Gizlenecek veri bitene kadar 6. Adımı uygula ve stego görüntüyü elde et.

İlgili basamaklar uygulandıktan sonra veri, örtü görüntü içerisine güvenli bir şekilde gizlenmiş olmaktadır. Histogram tabanlı veri gizleme yönteminde tepe sinyal gürültü oranı değeri düşük ancak kabul edilebilir seviyede çıkmaktadır. Veri gizleme işlemi sonucunda elde edilen stego görüntüden gizli veri ve orijinal örtü görüntünün elde edilmesi işlemi için veri çıkarım işlemi uygulanmaktadır. Veri çıkarım işleminin uygulanması aşamasında, orijinal örtü görüntü histogramından elde edilen maksimum ve minimum değerler ve gizli verinin uzunluk bilgileri bilinmesi gerekir. Veri çıkarım işlemine ait algoritma adımlar halinde verilmektedir.

1. Stego görüntü, maksimum, minimum renk değerleri ve gizli verinin uzunluğunu al.
2. Maksimum ve minimum piksel değerlerini değerlendir.
3. Stego görüntü ilgili pikselini al.
    a. Piksel değeri maksimum değere eşitse gizli veriye 0 ekle
    b. Piksel değeri (maksimum+1) veya (maksimum-1) değerlerine eşitse gizli veriye 1 ekle
4. Gizlenmiş olan verinin tamamı çıkarılana kadar 3. Adımı tekrarla ve gizli veriyi oluştur
5. Elde edilen gizli veriyi karakterlere çevir.
6. Veri çıkarıldıktan sonra maksimum ve minimum pikseller kullanılarak histogramı orijinal haline getir.
7. Orijinal görüntüyü elde et.

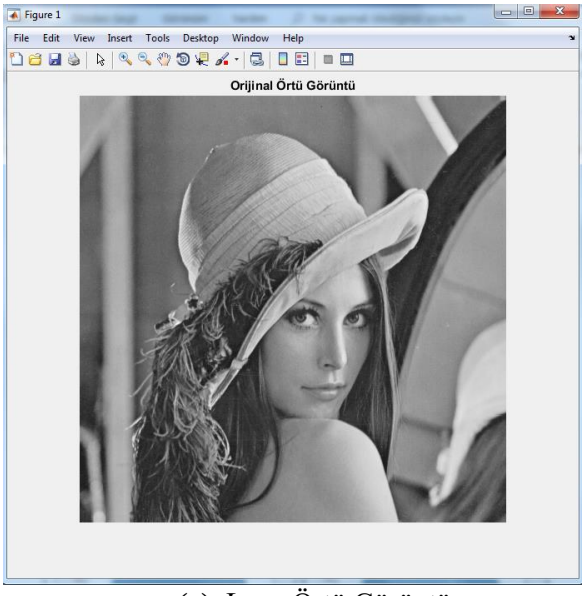
3. DENEYSEL ÇALIŞMALAR VE SONUÇLAR

Deneysel çalışmada, görüntü işleme veri tabanlarında yer alan 512 x 512 boyutlarında Lena, Baboon, Tank, Barbara, Zelda ve Couple resimlerinin gri ölçekli örtü görüntüleri kullanılmaktadır. Şekil 1'de kullanılan örtü görüntüler sunulmaktadır. Deneysel çalışmaların başarımında örtü görüntü ile stego görüntü arasındaki benzerlik durumunu gösterene Tepe Sinyal Gürültü Oranı (Peak Signal Nose Ratio - PSNR) kullanılmaktadır.

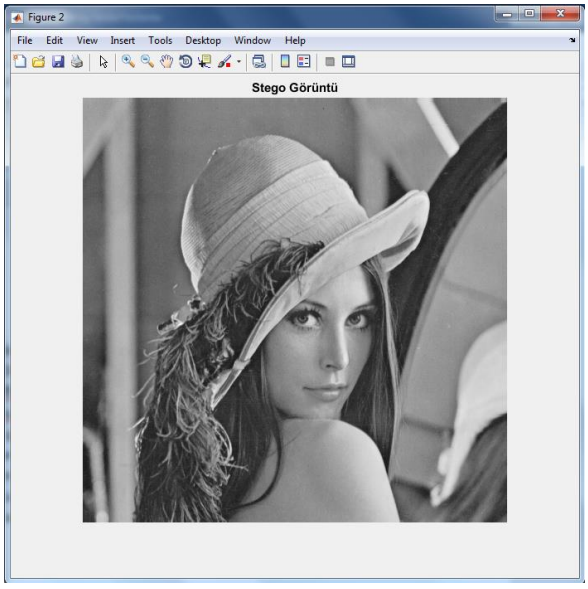


Şekil 1: Deneysel çalışmalarda kullanılan örtü görüntüler, (a) Lena, (b) Baboon, (c) Tank, (d) Barbara, (e) Zelda ve (f) Couple

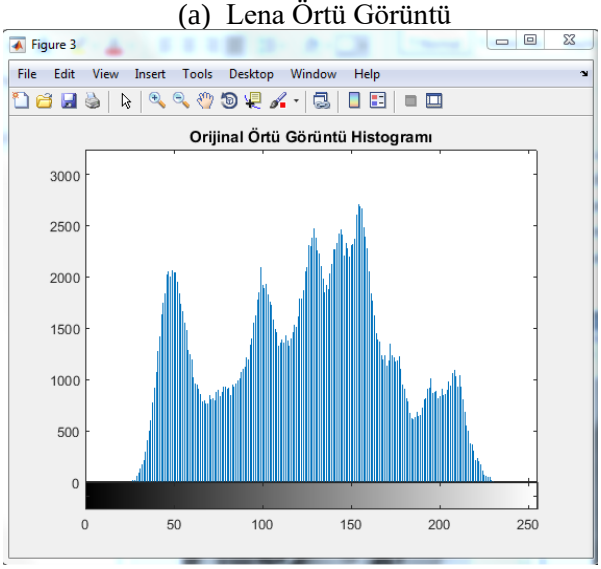
Örtü görüntülerin içerisine 272 bit uzunluğunda "HistogramBasedReversibleDataHiding" kelimesi gizlenerek sonuçlar elde edilmiştir. Ayrıca, rastgele üretilen maksimum renk değeri adetinde bit örtü görüntülere gizlenmiştir. Şekil 2'de Lena örtü görüntüsüne 272 bit uzunluğunda bu bilginin gizlenmesi sonucunda elde edilen stego görüntü, stego görüntü histogramı, örtü görüntü ve örtü görüntü histogramları sunulmaktadır. Orijinal örtü görüntüsünde maksimum değere sahip renk adetinin azaldığı gözlenmektedir. Veri gizleme işlemi maksimum değere göre yapıldığından histogramın, stego görüntü histogramında farklılaşma görülmektedir. Ancak stego görüntü üzerinde insan gözü ile algılanamayacak değişiklik gerçekleşmektedir.



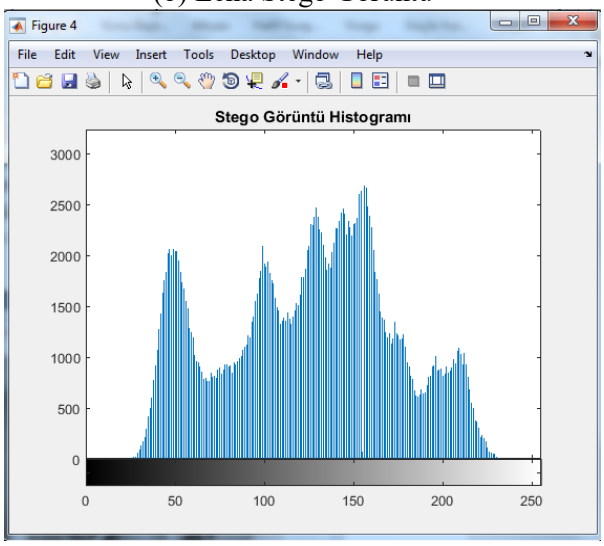
(a) Lena Örtü Görüntü



(b) Lena Stego Görüntü



(c)Orijinal Görüntü Histogramı



(d) Stego Görüntü Histogramı

Şekil 2: "HistogramBasedReversibleDataHiding" verisinin Lena örtü görüntüye gizlenmesi sonucunda elde edilen; (a) Örtü görüntü, (b) Stego görüntü, (c) Örtü görüntü histogramı, (d) Stego görüntü histogramı

Tablo 1'de örtü görüntülerin histogramlarından elde edilen en büyük ve en küçük renk değeri, en büyük renk değerinin adeti, 272 bitlik verinin gizlenmesi sonucunda elde edilen PSNR değeri ve en büyük renk değerinin adeti kadar rastgele üretilmiş verinin gizlenmesi sonucunda elde edilen PSNR değerleri sunulmaktadır. Gizlenecek veri bit değerinde ciddi artışlar olmasına rağmen PSNR değerleri arasında yüksek farklılıklar gözlenmemektedir.

Tablo 1'de sunulan minimum renk değeri ile maksimum renk değerleri veri gömülmeden önce örtü görüntüye uygulanacak olan histogram kaydırma işlemine ait değerleri göstermektedir. Histogram kaydırma işleminden sonra, veri gömülmeden önce elde edilen PSNR değerleri Lena için 53,7018, Baboon için 50,4768, Tank için 100, Barbara için 54,1316, Zelda için 53,5613 ve Couple için 50,6123 olarak elde edilmiştir.

Histogram kaydırma işlemi yapıldıktan sonra elde edilen psnr değerleri ile veri gömüldükten sonra elde edilen psnr değerlerinin birbirine çok yakın olduğu gözlenmektedir. Kısacası görüntüdeki bozulmanın histogram kaydırma işleminden kaynaklandığı görülmektedir.

Tablo 1: Deneysel çalışmalarda kullanılan örtü görüntülerin başarım analizi

Örtü Görüntü	Minimum Renk Değeri	Maksimum Renk Değeri	Maksimum Adet	PSNR (272 bit)	PSNR (Maksimum Adet)
Lena	236	154	2716	53,6940	53,6217
Baboon	225	121	2759	50,4732	50,4382
Tank	146	147	16729	81,1768	63,0848
Barbara	247	159	2217	54,1230	54,0595
Zelda	186	120	2588	53,5538	53,4857
Couple	133	22	3858	50,6085	50,5549

4. TARTIŞMA

Çalışmada, histogram kaydırma yöntemi kullanılarak kayıpsız ve geri dönüştürülebilir veri gizleme yöntemi önerilmektedir. Önerilen yöntemde sadece histogramda yer alan maksimum değer adetinde veri gizleme işlemi gerçekleştirilmiştir. Bu sebepten dolayı kapasitenin düşük olduğu gözlenmektedir. Farklı renk değer adetine sahip diğer renklerde kullanılarak kapasite rahatlıkla arttırılabilir. Ayrıca, histogram kaydırma yöntemi ile beraber piksel renk değerleri değişim yöntemi ve en düşük anlamlı bitlere verilerin gizlenmesi kullanılarak yeni geri dönüşümlü ve kayıpsız veri gizleme yöntemleri önerilebilir.

KAYNAKLAR

Chi, L. P., Wu, C. H., & Chang, H. P. (2018). Reversible data hiding in dual Stegano-image using an improved center folding strategy. *Multimedia Tools and Applications*, *77*(7), 8785-8803.

He, W., Xiong, G., Weng, S., Cai, Z., & Wang, Y. (2018). Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion. *Information Sciences*, *467*, 784-799.

Jung, K. H. (2018). Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. *Journal of Real-Time Image Processing*, *14*(1), 127-136.

Li, M., & Li, Y. (2017). Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding. *Signal Processing*, *130*, 190-196.

Lu, T. C., Wu, J. H., & Huang, C. C. (2015). Dual-image-based reversible data hiding method using center folding strategy. *Signal Processing*, *115*, 195-213.

Oruganti, M., Sabitha, C., Ghosh, B., Neeraja, K., & Hemanath, K. (2019). Difference Expansion based Near Reversible Data Hiding Scheme. In *First International Conference on Artificial Intelligence and Cognitive Computing* (pp. 613-619). Springer, Singapore.

Prasad, S., & Pal, A. K. (2017). An RGB colour image steganography scheme using overlapping block-based pixel-value differencing. *Royal Society open science*, *4*(4), 161066.

Pradhan, A., Sekhar, K. R., & Swain, G. (2018). Digital image steganography using LSB substitution, PVD, and EMD. *Mathematical Problems in Engineering*, *2018*.

Solak, S., & Altınışık, U. (2019). A new approach for steganography: bit shifting operation of encrypted data in LSB (SED-LSB). *International Journal of Informatics Technologies*, *12*(1).

Yi, S., Zhou, Y., & Hua, Z. (2018). Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion. *Signal Processing: Image Communication*, *64*, 78-88.