Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, 34, S. 305-310, Mart 2022

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 34, pp. 305-310, March 2022

Research Article

Uzamsal Alan Görüntü Steganografisi için Blok Veri Gizlemede Kanal Seçimi

Zeynep Sarı[1*], Mehmet Yıldırım[2]

[1*] Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, Kocaeli, Türkiye, (ORCID: 0000-0003-2834-3745), zeynep.sari@kocaeli.edu.tr
[2 *] Kocaeli Üniversitesi, Teknoloji Fakültesi, Bilişim Sistemleri Mühendisliği Bölümü, Kocaeli, Türkiye (ORCID: 0000-0003-1676-1560), myildirim@kocaeli.edu.tr

(2nd International Conference on Applied Engineering and Natural Sciences ICAENS 2022, March 10-13, 2022)

(**DOI:** 10.31590/ejosat.1081746)

ATIF/REFERENCE: Sarı, Z. & Yıldırım, M. (2022). Uzamsal Alan Görüntü Steganografisi için Blok Veri Gizlemede Kanal Seçimi. *Avrupa Bilim ve Teknoloji Dergisi*, (34), 305-310

Öz

İnternetin yaygın kullanılması ile birlikte veri iletimi kolaylaşmıştır. Bütün iletişim biçimlerinde, özellikle gizli iletişimde, veri güvenliği en önemli unsurdur. Bu nedenle, verinin güvenliğini sağlamak için verinin şifrelenmesi en eski yöntemdir ve buna kriptografi adı verilmektedir. Kriptografi, bilgiyi güvence altına almak için kullanılan etkili bir yöntem olsa da bilginin varlığını belli eder. Steganografi ise, bilginin varlığını istenmeyen kişilerden gizler. Steganografi verinin varlığını kamufle etmek için kapak adı verilen taşıyıcı medya kullanır. Kapak medya; video, görüntü veya ses dosyası olabilir. Uzamsal alanda görüntü steganografisinde, veriler bir kapak görüntünün piksellerine doğrudan yerleştirilir. Literatürde, birçok araştırmacı tarafından geliştirilmiş çeşitli görüntü steganografi teknikleri yer almaktadır. Bu çalışmada, uzamsal alanda görüntü steganografisinde, blok veri gizleme için güvenli kanal seçimi tekniği önerilmektedir. Veri gizlemede kullanılacak pikseli tespit etmek için iki yöntem kullanılmıştır. Birincisinde, kapak görüntü bloklara bölündükten sonra, blok içerisindeki her bir pikselin komşuları ile arasındaki ortalama farkı yani gradyan değeri kullanılmaktadır. İkincisinde, pikselin sayısal değeri doğrudan kullanılmaktadır. Tespit edilen piksellerin en az anlamlı bitleri (1-lsb, 2-lsb, 3-lsb), gizlenecek mesajın bitleri ile değiştirilmektedir. Her iki yöntemde de PSNR ve SSIM değerlerinin birbirlerine yakın olduğu tespit edilmiştir. Üretilen stego görüntülerin 1-lsb için ortalama PSNR değeri 63.2631 ve bpp değeri 0,007, 2-lsb için PSNR değeri 56.8598 ve bpp değeri 0.015, 3-lsb için PSNR değeri 50.5023 ve bpp değeri 0.03 bulunmuştur, bu değerlerin oldukça başarılı olduğu görülmüştür.

Anahtar Kelimeler: Blok Veri Gizleme, Görüntü Steganografisi, Kanal Seçimi, k-lsb, Uzamsal Alan

Channel Selection in Block Data Embedding for Spatial Domain Image Steganography

Abstract

With the widespread use of the Internet, data transmission has become easier. In all forms of communication, especially confidential communication, data security is the most important issue. Therefore, encryption of data is the oldest method toensure the security of data and it is called cryptography. Although cryptography is an effective method used to secure information, it reveals the presence of information. Steganography, on the other hand, hides the presence of information from unwanted people. Steganography uses carrier media, called covers, to camouflage the presence of data. Cover media; can be a video, an image or an audio file. In image steganographyfor the spatial-domain, data is placed directly into the pixels of a cover image. In the literature, there are various image steganography techniques developed by many researchers. In this study, a secure channel selection technique is proposed for block data hiding in spatial image steganography. Two methods were used to detect the pixel to be used in data hiding. In the first, after the cover image is divided into blocks, the average difference between each pixel and its neighborsin the block, that is the gradient value, is used. In the second, the numerical value of the pixel is used directly. The least significant bits (1-lsb, 2-lsb, 3-lsb) of the detected pixels are replaced with the bits of the message to be hidden. PSNR and SSIM values were found to be close to each other in both methods. The mean PSNR value for 1-lsb was 63.2631 and the bpp value was 0.007, the PSNR value for 2-lsb was 56.8598 and the bpp value was 0.015, the PSNR value for 3-lsb was 50.5023 and the bpp value was 0.03. These values were found to be quite successful.

Keywords: Block Data Hiding, Image Steganography, Channel Selection, k-lsb, Spatial Domain

[*] Sorumlu Yazar: zeynep.sari@kocaeli.edu.tr

1. Giriş

Son yıllarda internetin yaygınlaşmasıyla birlikte, hassas verilerin internet ortamında aktarımında güvenlik ihtiyacı da artmıştır. Steganografi bu güvenli iletimi sağlamak için kullanılmaktadır. Dijital görüntülerin yaygın olması ve sık kullanılması, onların steganografi yöntemleri için güncel medya formatı olarak kullanılabilmesini sağlamaktadır (Nguyen, 2015a). Steganografide, taşıyıcı görüntüye "kapak görüntü", içine veri gizlenmiş görüntüye "stego görüntü" denilmektedir (Sabeti, 2013).

Steganografi verinin varlığını gizlerken, steganaliz, taşıyıcı medyadaki gizlenmiş verilerin varlığını ortaya çıkaran bilim alanıdır (Cheddad, 2010). Bu nedenle görüntü steganografisinin en belirgin ihtiyacı, steganaliz yöntemlerine karşı dayanıklı olmasıdır. Literatürde steganaliz ataklarına dayanıklılığı arttırmak için etkili olan iki yöntem vardır (Chen,2010; Fridrich,2006); blok tabanlı steganografi ve kanal seçim yaklaşımlarıdır. Matris yaklaşımlı veri gizleme, ilk olarak Crandall tarafından ortaya atılmıştır (Crandall, 1998; Nguyen, 2015b). Crandall matris bloklarını "hücre" olarak ele alıp veri gömme işlemini önermiştir. Kanal seçimi yaklaşımı ile hedeflenen öncelikle steganaliz saldırılarına dayanaklı olabilmek, bir diğeri de minimum görünürlükte bozulmaya neden olacak pikselleri seçebilmektir.

Kanal seçiminde güvenliği arttırmak için çeşitli metotlar ve şemalar sunulmuştur. Sabeti ve arkadaşları tarafından sekizli karmaşıklık ölçüsüne dayalı lsb (ing: least significant bit) eşleştirme yöntemi önerilmiştir. Bu yöntem bir pikselin ve sekiz komşuluğunun arasındaki farkların toplamını ele almaktadır. Önerilen yöntemlerin etkinliğini ölçmek için, gizlenen veri ile çıkartılan verinin aynı olması gerekmektedir. Veri çıkarma işleminin başarılı olduğunu belirleyebilmek için yaygın olarak bit hata oranı (BER-bit error rate) ölçütü kullanılmaktadır (Shah,2021).

Bu çalışmada, stego görüntülerin kalitesini ve güvenliğini arttırmak için kanal seçim kuralı kullanılmıştır. Bölüm II'de bu çalışmaya temel olan ve literatürde yer alan yöntemlerden kısaca bahsedilmiş, Bölüm III'te önerilen yöntem açıklanmıştır. Bölüm IV'te önerilen yöntem ile elde edilen deneysel sonuçlardan bahsedilmiş olup, Bölüm V'te çalışmaya dair genel sonuçlar verilmiştir.

2. Materyal ve Metot

2.1. Block Veri Gizleme Algoritması

Blok veri gizleme (block data hiding-BDH) algoritmasında, ek vektör veya matris kullanılmasına gerek kalmadan veri gizleme işlemi yapılmaktadır. Bu işlem kanal seçimi metoduyla birlikte uygulanabilir. Bloklara bölme işleminde araştırmacılar çalışmalarında farklı matris boyutları seçerek, kapak görüntüsünü bölmüşlerdir.

2.2 Kanal Seçim Kuralı

Verinin algılanabilirliğini azaltmak için kapak görüntünün her bir bloğunda seçilen piksel veya piksellerin bitleri ile k bit uzunluğundaki bir mesajın bitlerinin değiştirilmesi önerilmektedir (Nguyen, 2015a; Sabeti, 2013; Cheddad, 2010; Chen, 2010; Crandall, 1998).

Steganaliz teknikleri ile verinin varlığının ortaya çıkmasını engellemek için gizlenecek bitler, keskin kenar geçişlerinin olduğu piksel değerlerine gizlenmelidir. Bunun nedeni, insan görme sisteminin (HVS-human vision system) görüntü içindeki küçük değişikliklere karşı daha az duyarlı olmasıdır (Nguyen,2015b).

Steganografide güvenlik, kullanılan metotlardan ve veri gizleme değişikliklerinin sayısından etkilenir (Fridrich,2006); bu da kanal seçimi yaparken renk yoğunluğunun fazla olduğu bölgeleri seçmenin önemini ortaya çıkarmaktadır. Kenar pikselleri, pikselin komşuları ile arasındaki fark alınarak tespit edilebilir. Gradyan değerinin büyük olması görüntüde keskin geçişlerin olduğunu, küçük gradyan değeri ise, görüntünün daha yumuşak geçişleri olduğunu göstermektedir.

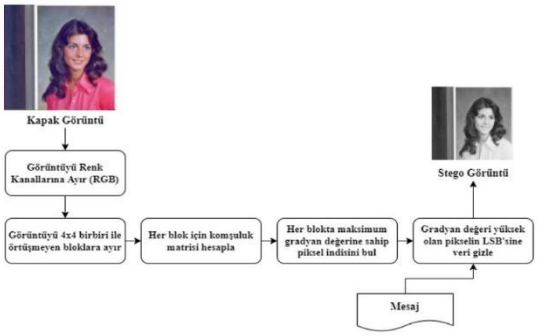
Bir pikselin en az iki, en fazla dört komşusu olabilir. Ortalama gradyan hesaplanırken pikselin komşuları ile farkları alınır ve kaç komşusu var ise o sayıya bölünür. Denklem 1'de 4 komşusu olan bir pikselin ortalama gradyan hesabı verilmektedir.

$$\boldsymbol{G(i,j)} = \frac{\left((\mathbf{m_{i,j}-m_{i,j-1}})+(\mathbf{m_{i,j}-m_{i,j+1}})+(\mathbf{m_{i,j}-m_{i-1,j}})+(\mathbf{m_{i,j}-m_{i+1,j}})\right)}{\mathbf{4}} \quad (1)$$

Gradyan hesabında çıkarma işlemlerinde mutlak değer alınmaması, incelenen blok içerisinde birden fazla en büyük gradyan tespit edilmesini engellemekte ve o pikselin keskin renk geçişinde olduğu bilgisini vermektedir.

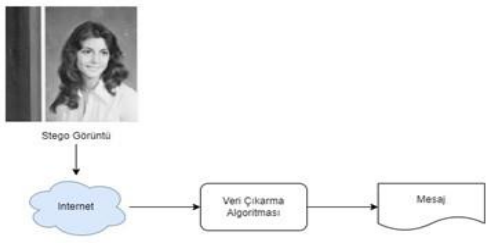
3. Önerilen Yöntem

Bu bölümde, gizlenecek mesajın bitlerini kenar piksellere gizleyebilmek için blok veri gizleme ve kanal seçimi kuralı sunulmaktadır. Bu şemada, uzamsal alanda kanal seçim kuralı ile gizli verinin gizleneceği pikseller belirlenmektedir.



Şekil 1. Önerilen şema veri gizleme algoritması

Şekil 1'de gösterildiği gibi, mesaj, bir kapak görüntünün piksellerine gizlenmiştir. Şekil 2'deki gibi, daha sonra stego görüntü internet üzerinden alıcıya iletilmiş ve alıcı herhangi bir işlem yapmadan gizli veriyi çıkartmıştır.



Şekil 1. Veri Çıkartma Algoritması

Önerilen yöntemde kanal seçimi için, 2 farklı yol izlenmiştir.

Kanal seçimi yapmadan önce her iki yöntemde de renkli görüntü üzerinde çalışılmıştır. Ancak mesaj tek renk kanalına gizlenmiştir. Bu sebeple, kapak görüntünde kanal seçimi yapmadan önce, görüntü renk kanallarına (RGB) ayrılmıştır.

3.1. Önerilen Kanal Seçimi

Önerilen kriterde, verinin algılanabilirliğini minimumda tutmak için görüntüde keskin kenarları bulabilmek önem taşımaktadır. Renkli görüntünün bir kanalı için, görüntü birbirleri ile örtüşmeyen 4x4 alt bloklara bölünür. Her blok içinde, piksellerin komşuları ile arasındaki farklılıkları Denklem 1'de verilen formül ile komşuluk sayısına göre ayrı ayrı hesaplanır ve bu gradyan değeri olarak bir matriste tutulur. Her blok içerisinde, Gradyan değeri en yüksek olan indisteki piksel veri gizlemek için seçilmektedir.

Aynı şekilde, görüntünün gradyan matrisine ihtiyaç duyulmadan sadece her bloktaki en yüksek değerlikteki piksel değeri seçilerek de veri gizleme işlemi yapılmıştır. Çalışmada, gradyan kullanarak yapılan kanal seçimine "Yöntem_1", yüksek değerlikteki piksel değeri kullanılarak yapılan kanal seçimine de "Yöntem_2" isimleri verilmiştir. Yöntem_2'nin uygulama şekli, standart lsb yer değiştirmesi ile benzerlik göstermektedir. Bu çalışmadaki farkı ise, bloklara ayırma ve ayrılan blok içerisinde en yüksek piksel değerine veri gizleme işlemi yapılmasıdır. Bu, yöntemi güvenlik açısından klasik lsb yer değiştirme yöntemlerinden daha güçlü kılmaktadır.

3.2 Önerilen Yöntemin Uygulanması

Önerilen yöntemde, görüntünün bir renk kanalı 4x4 bloklara ayrılmakta ve her bloktan seçilen tek bir piksele gizli mesajın bitleri yerleştirilmektedir.

3.2.1 Veri Gizleme Adımları

Lsb yönteminde görüntü matrisi üzerinde pikseller satır satır (Kanan, 2010), sol baştan başlayarak taranmaktadır ve her bir pikselin lsb bit/bitlerine mesaj bit/bitleri gizlenmektedir. Çalışmamızda ise, görüntünün gradyan matrisinde 4x4 blok içerisinde en yüksek gradyan değerine sahip indisteki piksel veri gizlenecek piksel olarak seçilmektedir. En yüksek değeri bulurken aramada, sol baştan başlanır ve ilk en yüksek gradyan değerli piksel seçilir.

164	63	75	95
120	135	55	75
99	132	60	54
64	150	113	50

(a)

72,5	-61,667	4	20
-12,667	42,5	-31,25	7
-6,3333	21	-28,5	-7,6667
-60,5	47	26,3333	-33,5

(b)

Şekil 3. (a) Kapak görüntüye ait 4x4 blok piksel değerleri, (b) Aynı blok için gradyan değerleri

Şekil 3(a)'da kapak görüntünün herhangi bir 4x4 blok görüntüsündeki piksel değerleri, (b)'de ise aynı bloktaki komşuluk matrisindeki gradyan değerleri verilmektedir.

Burada en yüksek gradyan değerinin 72.5 olduğu görülmektedir ve kanal seçim yöntemi olarak Yöntem_1 kullanılması halinde, bu piksel verinin gizleneceği piksel olarak seçilmiştir. Bu blok matrisinde 1.satır ve 1.sütunundaki indiste yer alan piksel değerinin 164 olduğu görülmektedir ve kanal seçim yöntemi olarak Yöntem_2 kullanılması halinde, bu piksel verinin gizleneceği piksel olarak seçilmiştir. Hangi kanala verinin gizleneceği belirlendikten sonra, görüntünün en az anlamlı bitlerine gizli mesajın bitleri sırası ile gizlenmektedir. 1-lsb için kapak görüntü pikselinin en az anlamlı bir biti ile mesajın bir biti, 2-lsb için pikselin en az anlamlı son iki bitine gizli mesajın iki biti ve son olarak 3-lsb için seçilen pikselin son üç bitine gizli mesajın üç biti gizlenmektedir.

3.2.2 Veri Çıkarma

Alıcı taraf internet üzerinden stego görüntüyü elde ettiğinde yapması gereken işlemler, görüntüyü birbiri ile örtüşmeyen 4x4 bloklara bölmek ve her blok için gradyan hesaplamaktır. En yüksek gradyan değerine sahip pikselin son bitlerinden çıkarma işlemi yaptığında alıcı veriyi eksiksiz ve kayıpsız olarak alabilmektedir.

4. Deneysel Sonuçlar ve Analiz

Bu bölümde, önerilen yöntemin performansını göstermek için elde edilen deneysel sonuçlar sunulmaktadır. Kapak görüntüleri için dijital görüntülerin koleksiyonundan oluşan, USC-SIPI görüntü veri tabanı kullanılmıştır.

Gizlenecek mesaj rasgele üretilerek elde edilmiştir. Her iki yöntem için de gizlenecek olan mesajlar aynıdır. Stego görüntünün başarı performansını belirlemek için tepe sinyal gürültü oranı (PSNR), ortalama karesel hata (MSE) ve yapısal benzerlik oranı (SSIM) metrikleri kullanılmıştır.

$$PSNR = 10log10(\frac{255^2}{MSE}) \quad (2)$$

Genellikle desibel (dB) cinsinden logaritmik olarak ifade edilen PSNR değerinin, yüksek kaliteli stego görüntüye sahip olabilmek adına 40 db değerinin altına inmemesi önerilir.

$$MSE = \frac{1}{\boldsymbol{satırxsutun}} \sum_{i=1}^{satır} \sum_{j=1}^{sutun} (K_{i,j} - S_{i,j})^2 \quad (3)$$

Denklem 3'te verilen ortalama karesel hata denkleminde satır, sutun değerleri matrisin satır ve sütun sayısıdır. $K_{i,j}$ kapak görüntü bitlerini, $S_{i,j}$ ise stego görüntü bitleridir.

Yapısal benzerlik oranı (SSIM) değeri, veri gizleme ve veri çıkarma işlemlerinden kaynaklı görüntünün kalitesindeki bozulma oranını ölçmeye yarayan hesaplamadır; 0-1 aralığında değerler üretir ve 1 iki görüntünün aynı olduğunu belirtirken 0 görüntülerin birbirinden tamamen farklı olduğunu belirtir (Çataltaş, 2017). Çalışmalarda bu değerin 1'e yakın olması hedeflenmektedir. Tablo 1'de, çalışmamızın deneysel sonuçları referans seçilen üç görüntü için verilmiştir.

Çıkarılan verilerin kayıpsız olduğunu göstermek için BER değerlendirme parametresi Denklem 4'teki gibi uygulanmıştır. BER değeri 0 ve 1 aralığında bir sonuç üretir. 0 verilerin kayıpsız alındığını ifade eder.

Denklem 4'te verilen; n değeri gizlenen mesajın uzunluğu, M değeri gizlenen mesaj, C değeri çıkarılan mesajı vermektedir. Gizlenen mesaj ile çıkarılan mesaj XOR ($\oplus$) mantıksal işleminden geçirilerek, gizlenen verinin ne kadarının geri alınabildiğini göstermektedir.

Tablo 1. Önerilen yaklaşımın PSNR, MSE, SSIM değerleri

Payload		Yöntem_1				Yöntem_2			Resim 512x512
	PSNR	SSIM	MSE	Gizleme Süresi (sn)	PSNR	SSIM	MSE	Gizleme Süresi (sn)	
0.007	63.2475	0.9999	0.0313	0.101	63.2351	0.9999	0.0315	0.116	*Baboon*
0.015	56.9130	0.9996	0.1324	0.419	56.8668	0.9996	0.1318	0.440	
0.031	50.4573	0.9984	0.5853	0.411	50.4983	0.9984	0.5798	0.412	
0.007	63.1929	0.9998	0.0313	0.149	63.2297	0.9998	0.0311	0.111	*Peppers*
0.015	56.7597	0.9991	0.1371	0.504	56.7573	0.9991	0.1372	0.440	
0.031	50.4978	0.9964	0.5798	0.502	50.5367	0.9964	0.5747	0.408	
0.007	63.2046	0.9997	0.0313	0.106	63.2582	0.9997	0.0314	0.105	*Female*
0.015	56.8784	0.9986	0.1334	0.425	56.9472	0.9986	0.1313	0.476	
0.031	50.5212	0.9939	0.5767	0.422	50.4983	0.9938	0.5804	0.459	

Çalışmamızda hesaplanan BER değerleri 0 (sıfır) bulunmuştur. Bu da bize verinin kayıpsız geri alınabildiğini göstermektedir.

Şekil 4 (a)'da verilmiş olan kapak görüntüsüne Yöntem_1 kullanılarak, 2 bit lsb veri gizlenmekte ve (b)'deki stego görüntü elde edilmektedir. Aynı şekilde Şekil 5'te de Yöntem_2 kullanılarak 3 bit lsb yöntemi ile veri gizlenmektedir.

(a) *(b)*

Şekil 4. (a) Kapak Görüntü Kırmızı Renk Kanalı, (b) Stego Görüntü Kırmızı Renk Kanalı

(a) *(b)*

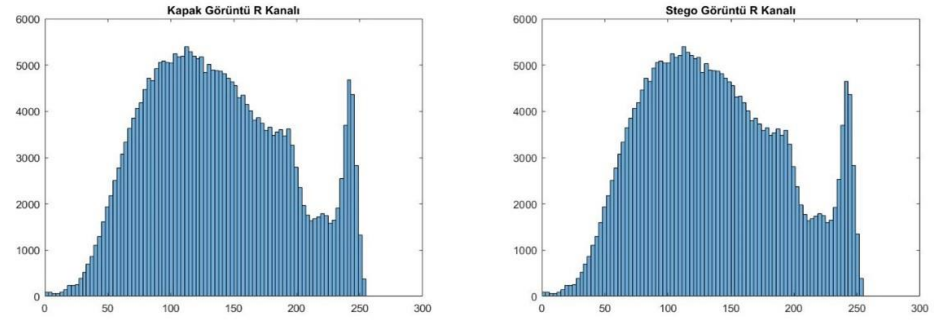
Şekil 5. (a) Kapak Görüntü Kırmızı Renk Kanalı, (b) Stego Görüntü Kırmızı Renk Kanalı

Şekil 6 ve Şekil 7'de verilen grafikleri Yöntem_1 ve Yöntem_2 ile veri gizleme işlemleri yapıldıktan sonra, kapak görüntü ile stego görüntüdeki histogram grafikleridir. Her iki yöntemde de 1 bit LSB ile veri gizlendiğinde histogramlarda belirgin bozulmaların olmadığı, ancak 3 bit lsb ile veri gizlendiğinde histogramlardaki değişimlerin ayırt edilecek şekilde olduğu görülmektedir.

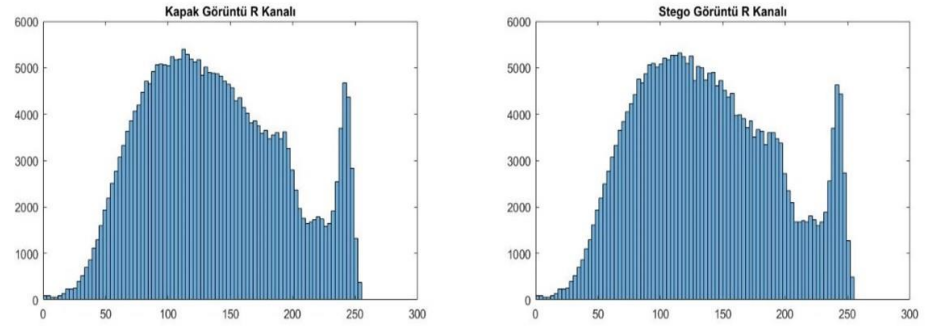
4. Sonuçlar

Bu çalışmada, gizli mesaj bitlerini gömmek için, görüntüdeki keskin kenar geçişlerinin olduğu pikselleri seçmek için kanal seçim kuralına dayalı iki yöntem önerilmiştir. Her iki yöntemde de PSNR ve SSIM değerlerinin birbirlerine yakın olduğu tespit edilmiştir. Üretilen stego görüntülerin 1-lsb için ortalama PSNR değeri 63.2631 ve bpp değeri 0,007, 2-lsb için PSNR değeri 56.8598 ve bpp değeri 0.015, 3-lsb için PSNR değeri 50.5023 ve bpp değeri 0.03 bulunmuştur, bu değerlerin oldukça başarılı olduğu görülmüştür. Sonuçlar önerilen kanal seçim kurallarının gri tonlamalı resimlerde, veri gömmeden kaynaklanan gürültüleri azaltmak için kullanılabilir olduğunu göstermektedir. Bu, saldırılara karşı stego görüntünün daha da güçlenmesini sağlamaktadır.

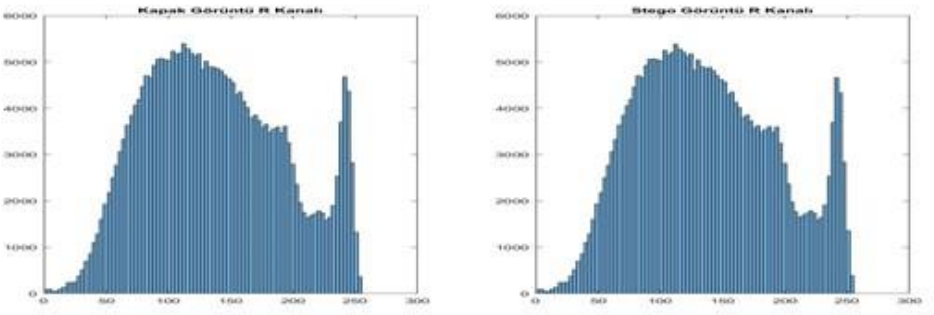
Elde edilen deneysel sonuçların, önerilen şema ile veri gizleme işleminden sonra stego görüntülerinin görsel kalitesini koruduğunu göstermektedir. Gelecekteki araştırmalarımızda, stego görüntülerin güvenliğini arttırmak ve tepe sinyal gürültü oranı değerlerini koruyarak, gizleme kapasitesini arttırmak hedeflenmektedir.



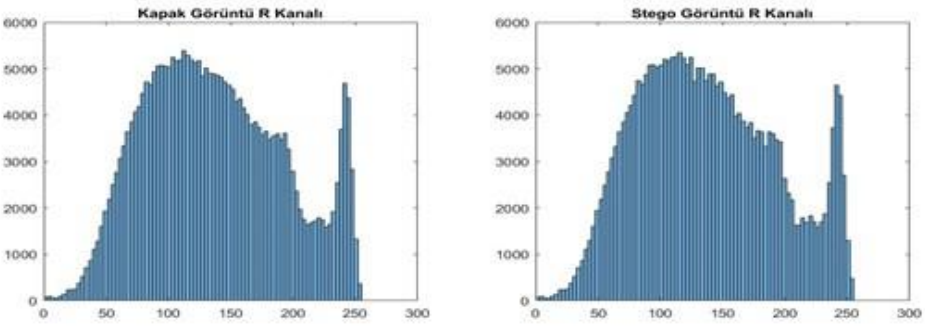
(a)



(b)



(c)



(d)

Şekil 6. (a) Yöntem_1 Baboon görüntüsü 1 bit lsb veri gizleme görüntü histogramı, (b) Yöntem_1 Baboon görütnüsü 3 bit lsb veri gizleme görüntü histogramı, (c) Yöntem_2 Baboon görütnüsü 1 bit lsb veri gizleme görüntü histogramı, (d) Yöntem_2 Baboon görütnüsü 3 bit lsb veri gizleme görüntü histogramı

Kaynakça

Cheddad, A., Condell, J., Curran K. ve Kevitt, P.M. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*, 727-752.

Chen, J., Zhu, Y., Shen Y. ve Zhang, W. (2010). Efficient Matrix Embedding Based on Random Linear Codes. *2010 International Conference on Multimedia Information Networking and Security*, 879-883.

Crandall, R. (1998). Some Notes on Steganography.

Çataltaş, Ö. ve Tütüncü, K. (2017). Improvement of lsb based image steganography, *International Journal Of Electrical, Electronics And Data Communication, 5*.

Fridrich, J. ve Soukal, D. (2006). Matrix embedding for large payloads. *IEEE Transactions on Information Forensics and Security*, *1*, 390-395.

Kanan, H. R. ve Nazeri, B. (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on genetic algorithm. *Expert Systems with Applications, 41*, 6123-6130.

Nguyen, T. D., Arch-int, S. ve Arch-int, N. (2015). A novel secure channel selection rule for spatial image steganography. *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 230-23.

Nguyen, T. D., Arch-int, S. ve Arch-int, N. (2015). New Channel Selection Criterionfor Spatial Domain Steganography. *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, 230, 2015.

Sabeti V., Samavi, S. ve Shirani, S. (2013). An adaptive LSB matching steganography based on octonary complexity measure. *Multimed Tools Appl*, *64*,777-793.

Shah, P. D. ve Bichkar, R.S. (2021). Secret data modification based image steganography technique usng genetic algorithm having a flexible chromosome structure. *Engineering Science and Technology, an International Journal, 24*, 782-94.

Zhong, Y., Huang, F. ve Zhang, D. (2013). New Channel Selection Criterion for Spatial Domain Steganography. *Digital Forensics and Watermaking, Berlin, Heidelberg:Springer Berlin Heidelberg, 7809*, 1-7.