Yerel İkili Örüntü Tabanli Veri Gizleme Algoritmasi: LBP-LSB

Local Binary Pattern Based Data Hiding Algorithm: LBP-LSB

Türker TUNCER[1], Engin AVCI[2]
[1]Adli Bilişim Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ, Türkiye
[2]Yazılım Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ, Türkiye
{turkertuncer, enginavci}@firat.edu.tr

Öz

Bir Steganografik metodun değerlendirme kriterlerinden biri de dayanıklılıktır. Bu çalışmada, iletim hattı boyunca örtü verinin uğrayabileceği saldırılara karşı gizlenmiş veriyi korumak hedeflenmiştir. Resmin parlaklık değişimlerine karşı gizlenmiş mesajı korumak için yerel ikili örüntü (LBP) operatörünün kullanılması önerilmiştir. Daha önceden damgalama tekniklerinde kullanılan bu metodun, daha farklı bir yaklaşımla steganografide kullanılması önerilmiştir. Resme LBP operatörü uygulandıktan sonra LBP haritasının üzerinde, LSB metodu kullanılarak veri gizlenecektir. Önerilen algoritmanın saldırılara karşı dayanıklılığı, kapasitesi ve taşıyıcıdaki değişim ölçülecektir.

Anahtar Kelimeler — Veri gizleme; Bilgi güvenliği; Görüntü steganografi; Görüntü İşleme.

Abstract

One of evaluation criterias of a steganographic method is durability. In this study, it is aimed to protect hidden data against attacks throughout transmission line. It is proposed to use Local Binary Pattern (LBP) operator in order to save secret message against to changes in brightness of the image. This method, which earlier have been used in watermarking techniques, is now proposed to be used in steganography with a different approach. After applying LBP operator on image, data will be hidden by using LSB method on LBP map. Durability of the proposed algorithm against to attacks, capacity of the algorithm and changes in carrier will be measured**.**

Keywords — Data hiding; Information security; Image Steganography; Image processing.

1. Giriş

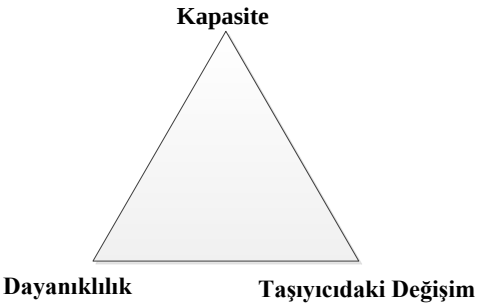
Veri gizleme yöntemleri antik çağlardan günümüze kadar kullanılan bilgi güvenliği yöntemleridir [1,2]. Bilgilerin sayısal ortama aktarılmasıyla birlikte bilgi güvenliğinin önemi de artmıştır ve modern veri gizleme yöntemleri geliştirilmeye devam etmektedir [1,3]. Veri gizlemenin en önemli alt dalları sayısal damgalama ve steganografidir. Steganografinin en önemli özelliği, gizli veriyi örtü nesnesi kullanarak saldırganlardan gizlenmektir. [4-6]. Bir örtü nesnesinde gizli mesajın varlığını analiz eden bilim dalına ise steganaliz denmektedir [7, 8].

Bir steganografik yöntemi değerlendirmek için 3 temel kriter kullanılmaktadır. Bunlar veri gizleme kapasitesi, saldırılara karşı dayanıklılık ve taşıyıcıdaki değişimi ölçen görsel/işitsel kalite metrikleridir [9]. Steganografik yöntemlerin değerlendirme kriterleri Şekil 1'deki üçgende gösterilmektedir. Bu üçgene sihirli üçgen denilmektedir.

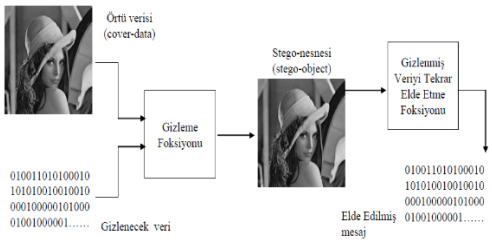
Genel olarak Steganografik yöntemlerin başarımlarının ölçülmesi için yukarıdaki üçgen referans alınmaktadır. Ancak farklı Steganografik yöntemlerin analizleri farklı şekilde yapılmaktadır [10,11].

Genel olarak Steganografik yöntemlerin başarımlarının ölçülmesi için yukarıdaki üçgen referans alınmaktadır. Ancak farklı Steganografik yöntemlerin analizleri farklı şekilde yapılmaktadır [10,11].

Gönderim ve kabul tarihi : 11.11.2016 - 22.07.2017



Şekil 1. Bir Steganografik Sistemin Değerlendirme Kriterleri



Şekil 2. Görüntü Steganografinin Blok Diyagramı

Bu çalışmada, LBP-LSB veri gizleme yönteminden bahsedilecektir. Bu çalışmanın temel amacı, örtü verisindeki oluşacak parlaklık değişimlerine karşı gizli mesajı korumak ve yöntemin dayanıklılığını arttırmaktır. Çalışmanın ikinci bölümünde görüntü steganografi, üçüncü bölümde LSB metodu, dördüncü bölümünde LBP operatörü, beşinci bölümünde LBP-LSB algoritması, altıncı bölümde deneysel sonuçlar ve yedinci bölümde ise sonuç ve öneriler kısmına yer verilecektir.

2. Görüntü Stenografi

Sayısal imgeler, steganografinin en sık kullanıldığı ve literatürde en çok örneği olan medyalarıdır. Günümüzde sosyal medya kullanımı ve mobil cihazların kullanımının artmasıyla birlikte sayısal görüntülerin dağıtımı hızla yaygınlaşmıştır [11].

Görüntülere veri gizlemek için ön şart görüntü dosyaların sayısal forma dönüştürülmesidir. Görüntü dosyası sayısallaştırılıp piksel değerleri elde edildikten sonra amaca uygun veri gizleme fonksiyonu kullanılarak veri gizleme işlemi gerçekleştirilir. Gizli mesajın güvenilirliği sağlamak için anahtar kullanılmaktadır. Anahtar kullanılarak gizli verinin gömülme noktaları tespit edilir. Anahtarın bir diğer kullanım şekli ise şifreleme amaçlıdır [11,12].

Bir Steganografik yöntemin başarılı olabilmesi için yüksek veri gizleme kapasitesine sahip olması, dayanıklı olması ve veri gizlendikten sonra bozulmanın az olması istenmektedir [13]. Veri gizleme kapasitesinin hesaplanmasıyla ilgili denklemler Denklem 1-3'te verilmiştir [11].

$$S = m \cdot n \cdot k \quad (1)$$

$$B = 8 \cdot b \quad (2)$$

$$K = S/8 \quad (3)$$

S görüntünün piksel sayısını, m görüntünün genişliğini, n uzunluğunu, k katman sayısını, b biti, B baytı, K ise kapasiteyi sembolize etmektedir. Denklem 3'teki kapasite piksel başına 1 bitlik kapasite (bpp) için hesaplanmıştır. Bu denklem veri gizleme fonksiyonunun özelliğine göre değişebilmektedir [9].

Muhteşem bir steganografi yönteminin elde edilmesi için Şekil 1'de gösterilen 3 başarım ölçütünün de sağlanması gerekmektedir. Ancak görsel/işitsel kalite ve kapasite ters orantılıdır. Kapasite arttıkça görsel/işitsel kalite azalmaktadır. Dayanıklı bir Steganografik yöntemin oluşturulması için de sayısal dönüşümler kullanılmaktadır. Dönüşüm tabanlı veri gizleme yöntemleri hem görsel kaliteyi hemde kapasiteyi olumsuz yönde etkilememektedir [14]. Görüntü steganografide en sık kullanılan metotlar ise aşağıda verilmiştir

- En önemsiz bite ekleme
- Filtre ve maskeleme tabanlı yöntemler
- Sayısal dönüşümler ve algoritmik yöntemler

[11].

3. En Önemsiz Bite Ekleme Yöntemi (LSB)

Bu yöntem en basit ve uygulaması en kolay yöntemdir. LSB yöntemi kullanılarak yüksek görsel kalite ve yüksek veri gizleme kapasiteleri elde edilmektedir. Bu yöntemin en büyük dezavantajı ise saldırılara karşı dayanıksız olmasıdır. Yöntem hem saldırılara karşı dayanıksız hem de imge kimliklendirmek için yeterli derecede kırılgan

olmamasıdır. Ayrıca bu yöntemin steganalizi için birçok yöntem geliştirilmiştir [15,16].

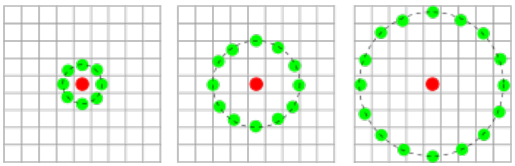
LSB yöntemi kullanılarak veri gizlemek için her piksel en anlamsız bitleri değiştirilir. Veri gizlendikten sonra en anlamsız bit veya bitlerde gizli mesaj barındırılmaktadır [17,18]. LSB yöntemi kullanılarak veri gizleme örneği Tablo 1'de verilmiştir.

Tablo 1. LSB yöntemiyle veri gömülmesi

	Pikselin Renk Değeri	**Renk Değerinin İkilik Sistemdeki Karşılığı**
Orijinal Piksel	158	1001110
Veri gömülmüş Piksel	159	1001111

4. Yerel İkili Örüntüler Operatörü (LBP)

LBP operatörü, gri seviyeden bağımsız bir doku ölçümü yöntemidir. LBP operatörü görüntünün her pikseli için bir etiket oluşturmaktadır ve bu etiketler birler ve sıfırlardan oluşmaktadır. Bu etiketler merkez pikselin NxN komşuluğundaki piksellerin karşılaştırılmasıyla oluşturulmaktadır. Genel olarak LBPP,R üç farklı dairesel komşulukla tanımlanabilir. P komşu sayını, R ise örnekleme yarıçapını temsil etmektedir. Şekil 3' te çeşitli LBP operatörleri gösterilmektedir[19].



P=8 R=1 P=12 R=2.5 P=16 R=4

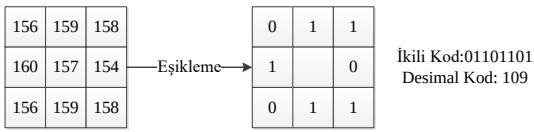
Şekil 3. Çeşitli dairesel $LBP_{P,R}$ Operatörleri

Bu çalışmada $LBP_{8,1}$ operatörü kullanılacaktır. Yani 3 x 3' lük matrisler kullanılarak komşuluk analizleri yapılacaktır.

$$LBP_{8,1}(x_c) = \sum_{p=0}^{p-1} u(x_p - x_c)\, 2^p \quad (4)$$

$$u(y) = \begin{cases} 1 & y \geq 0 \\ 0 & y < 0 \end{cases} \quad (5)$$

Burada y, merkez pikselle komşu piksel arasındaki farkı, xc LBP etiketi üretilen merkez pikseli, xp merkez pikselin komşuları, u(y) ise LBP operatörü sonucu üretilen bitleri ifade etmektedir. Şekil 4' te LBP operatörüyle piksellerin etiketlenmesine ilişkin bir örnek verilmiştir [20].



Şekil 4. $LBP_{8,1}$ Operatörünün uygulanması

LBP operatörünün en önemli özelliği ise parlaklık değişimlerine karşı dayanıklı olmasıdır. Aşağıdaki örnekte "cameraman" adlı resmin parlaklığı arttırılıp azaltıldığı halde LBP histogramının değişmediği gösterilmiştir.

(a) (b) (c)

Şekil 5. (a) Orijinal Resim (b) Parlaklığı arttırılmış resim (c) Parlaklığı azaltılmış resim

5. LBP-LSB Veri Gizleme Şeması

Bölüm 4' te de bahsedildiği gibi LBP operatörü kullanılarak parlaklık saldırılarına (gürültülerine) karşı dayanıklı metotlar oluşturulabilir. Genelde dokusal imge tanıma ve yüz tanıma da kullanılan LBP operatörünü veri gizleme şemalarında kullanmakta mümkündür. Bu yöntemi görüntü steganografide en sık kullanılan LSB metoduyla birlikte kullanarak parlaklık saldırılarına (gürültüsüne) daha dayanıklı yeni bir gizleme şeması elde etmek mümkün

olacaktır. Geliştirilen veri gömme şemasının algoritması aşağıdaki gibidir:

Adım 1: Örtü verisi alınır. Eğer örtü verisi renkli ise katmanlarına ayrılır.

Adım 2: Gizlenecek mesaj ikili forma çevrilerek hide_data adında bir diziye atılır.

Adım 3: Örtü verisine $LBP_{8,1}$ operatörü uygulanarak resmin ikili LBP haritası çıkarılır ve buradan elde edilen 8. Bitler lbplsb adlı diziye atılır.

Adım 4: 3x3 boyutunda matrislerle örtü verisi gezilir ve fark=|CI(i+1,j+1)-CI(i+1,j)| olarak hesaplanır.

Adım 5: Eğer lbplsb(i)=0 ve data(i)=1 ise SI(i+1,j)=SI(i+1,j)+fark işlemi yapılır. Eğer lbplsb(i)=1 ve data(i)=0 ise SI(i+1,j)=SI(i+1,j)-fark işlemi yapılarak yeni bir LBP haritası oluşturulur.

Adım 6: Data dizisinin uzunluğuna dek adım 4 ve 5 tekrarlanır ardından SI elde edilir.

Yukarıdaki algoritma CI örtü resim ve SI ise stego resim'i temsil etmektedir.

Veri çıkarma şeması ise aşağıdaki algoritmada verilmiştir.

Adım 1: SI alınır ve LBP8,1 operatörü uygulanarak resmin LBP haritası çıkarılır.

Adım 2: LBP haritasındaki son bitler (8. Bitler bu işlemi yapabilmek için mod 8 işlemi de kullanılabilir.) ilbplsb adında bir diziye atılır.

Adım 3: ilbplsb dizisinde ki elemanları kullanılan anahtarda ki bilgiler ışığında istenilen forma çevrilir. Eğer gömülen mesaj metin formatındaysa, ilbplsb dizisindeki değerler desimale çevrilerek ASCII kodlar elde edilir ve bu kodlar istenilen forma çevrilir. Görüntü için ise ilbplsb dizisindeki değerler piksel değerlerine çevrilir ve anahtarda ki boyut bilgilerine istinaden, gömülmüş veri resim haline dönüştürülür.

6. Deneysel Sonuçlar

Önerilen algoritmayla Şekil 5.a'daki 256x256 boyutlu resme 6800 bitlik metin formatında veri gizlenmiştir. Ardından resmin, önce Şekil 5.b'deki gibi parlaklığı arttırılmıştır ve veri çıkarma işlemi gerçekleştirilmiştir. Veri doğru ve tam olarak çıkarılmıştır. Ardından Şekil 5.c'deki gibi parlaklığı azaltılıp veri çıkarma işlemi uygulanmıştır ve gizli veri başarıyla çıkarılmıştır.

Bu algoritmaya göre 3x3' lük bir matrise tek bit gömülebileceği için kapasite 0.11 bpp (bit per pixel) olarak bulunmuştur. Kapasiteyi arttırmak için çok seviyeli model önerilebilir ve seviye sayısı aşağıdaki formülle hesaplanır [21].

$$l = log_{b^2} m.n.k \tag{5}$$

$$c = \sum_{n=1}^{l} \frac{mxnxk}{b^{2^n}} \tag{6}$$

Denklem 6 ve 7 kullanılarak çok katmanlı algoritmanın katmanlı uygulamasının kapasitesi hesaplanmıştır. l seviye sayısını, m resmin satır sayısını, n sütun sayısını, k katman sayısını, b ise kullanılan matrisin boyutunu ifade etmektedir. Örneğin LBP operatörüyle eşikleme işlemi yapabilmek için 3x3 matris kullanılıyorsa b değeri 3 alınacaktır.

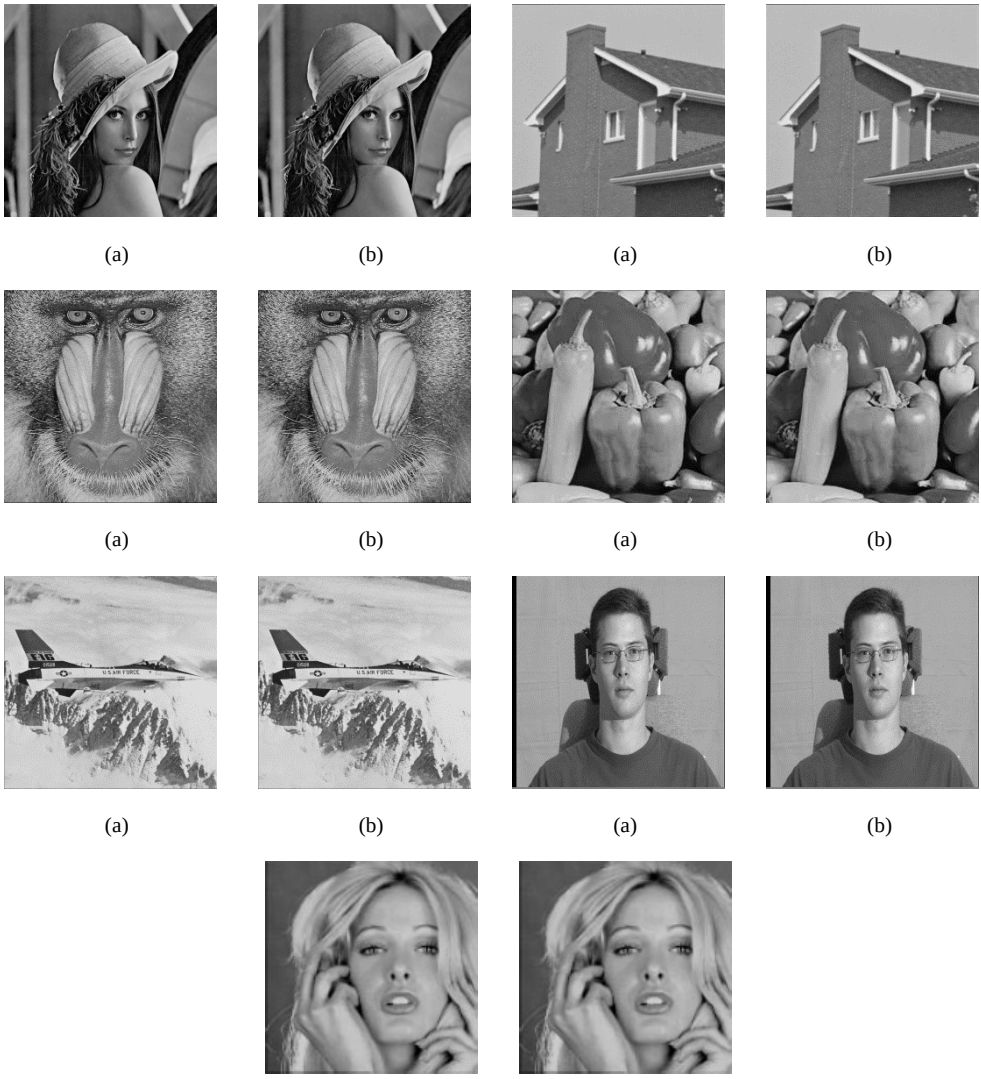
Örneğin 512x512 boyutlu renkli bir resme maksimum 6 seviyeye uygulanabilir ve bu 6 seviye ardından kapasite yaklaşık 0.17 bpp' ye çıkacaktır. Şayet matris resim üzerinde üçer üçer değil de ikişer ikişer gezdirilirse kapasite 0.25 bpp'ye, tek tek gezdirilirse olursak kapasite 0.44' e çıkacaktır. Eğer ikişerli gezintiye ve tek tek gezintiye sırasıyla 6 level önerilen algoritma uygulanırsa kapasite 0.31 ve 0.65 bpp' ye kadar çıkacaktır. Ancak deneyler sonucu tek tek gezinti yerine diğer gezintiler önerilmektedir. Ayrıca LBP' nin 2 biti 3 biti veya 4 biti kullanılacak olursa kapasite kullanılan bit sayısı katına çıkacaktır.

Taşıyıcıdaki değişimi test etmek için ise resimlerin bozulma oranları hesaplanmaktandadır. Eğer bir resim ne kadar fazla bozulmuşsa, taşıyıcıdaki değişimi o kadar artmakta ve daha fazla dikkat çekmektedir. Resimlerin bozulma oranı MSE ve PSNR metrikleriyle hesaplanmaktadır ve bu metriklerin formülleri aşağıdaki gibidir [22].

$$MSE = \frac{1}{mn} \sum_{i,j} (CI_{i,j} - SI_{i,j})^2 \tag{7}$$

$$PSNR = 10 \log \frac{Max(CI_{i,j}^2)}{MSE} \tag{8}$$

Test uygulamalarında 512 x 512 boyutunda resimler kullanılmıştır ve bu resimlere önerilen algoritmayla maksimum gizlenebilecek metin verisi gizlenmiştir. Bu verinin boyutu 28896 bittir. Test resimleri olarak sırasıyla "lena", "house", "baboon", "pepper", "jet", "boy" ve "tiffany" adlı resimler seçilmiştir.



(a) (b) (a) (b)

(a) (b) (a) (b)

(a) (b) (a) (b)

(a) (b)

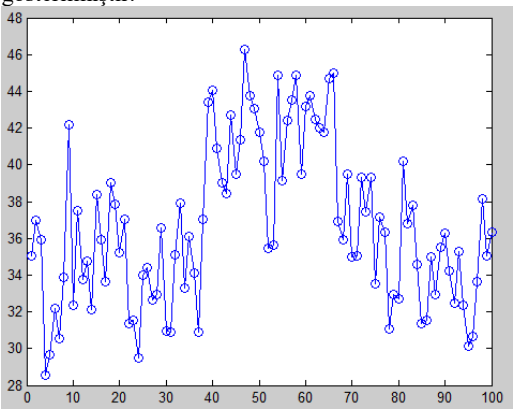
Şekil 7. Test resimleri için (a) Orjinal resim (b) Stego Resim

Şekil 7' de verilen test imajların PSNR değerleri Tablo 2'de verilmiştir.

Tablo 2. Test Resimlerinin PSNR Sonuçları

Test Resimleri	PSNR (dB)
Lena	39.84
House	45.30
Baboon	39.78
Pepper	43.56
Jet	38.28
Boy	44.29
Tiffany	47.29

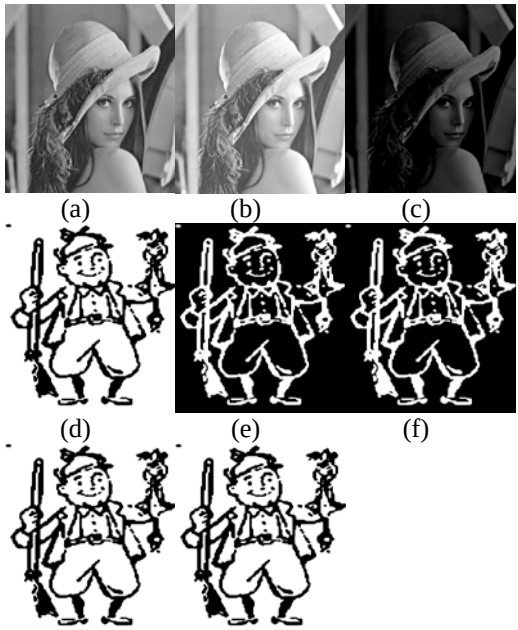
Ucid image database (v2)' den rastgele 100 adet resim seçilmiştir. Bu resimlere alabilecekleri maksimum sayıda bit gömülerek PSNR değerleri ölçülmüştür. Ölçülen PSNR değer grafiği Şekil 8' de gösterilmiştir.



Şekil 8. UCID veri tabanındaki 100 resmin PSNR sonuçları

Önerilen şema UCID-Image Database (v2) kullanılarak test edilmiştir. UCID-Image Database birbirinden farklı 1338 resimden oluşmaktadır. Bu veri tabanından rastgele seçilen 100 resme, önerilen gizleme şeması uygulanarak PSNR değerleri ölçülmüştür. Test sonucunda en düşük PSNR değeri 28.55, en yüksek PSNR değeri 46.28 ve ortalama PSNR değeri ise 36,67 olarak bulunmuştur.
Testler MATLAB2013a programında Windows 8 işletim sistemine sahip olan 4 GB ram ve Pentium Core i5 4300u işlemcili bir dizüstü bilgisayarda gerçekleştirilmiştir. Testlerde 512 x 512 boyutundaki resimlere 28896 bit veri gömülmüştür ve şemanın çalışma süresi 0.96 saniyedir.

Önerilen yöntemin LSB yöntemine göre daha dayanıklı olduğu 4. Bölümde gösterilmiştir. Şekil 9'da parlaklık ataklarına karşı her iki yöntemin dayanıklılığı verilmiştir.



Şekil 9. LSB ile LBP-LSB yönteminin karşılaştırılması. (a) Örtü imge (b) parlaklığı arttırılmış imge (c) parlaklığı azaltılmış imge (d) gizli veri (e) LSB kullanılarak (b)'den çıkarılan gizli veri (f) LSB kullanılarak (c)'den çıkarılan gizli veri (g) LBP-LSB kullanılarak (b)'den çıkarılan gizli veri (h) LBP-LSB kullanılarak (b)'den çıkarılan gizli veri.

7. Sonuçlar

Veri gizlemede daha önceden damgalama uygulamalarında önerilen LBP operatörü, bu çalışmada steganografik açıdan ilk kez ele alınmıştır. LBP operatörü steganografide en sık kullanılan LSB metoduyla birleştirilip yeni bir gizleme şeması ortaya konmuştur. Bu gizleme şeması parlaklık ve zıtlık değişimlerine karşı dayanıklıdır.

Önerilen gizleme şeması dayanıklılık, kapasite ve Taşıyıcıdaki değişim açısından ele alınmıştır. Çok katmanlı yöntemler kullanılarak kapasitenin ve dayanıklılığın daha fazla arttırılabileceği ortaya konmuştur. Şemanın dayanıklı olduğu LBP histogramları gösterilerek ispat edilmiş ve kapasite matematiksel olarak ortaya konmuştur. Ayrıca taşıyıcıdaki değişim ile ilgili birçok resim

kullanılarak PSNR sonuçları elde edilmiştir ve sonuçlar başarılı bulunmuştur.

Bu çalışmanın temel amacı özellikle tarama sonucunda oluşan parlaklık gürültülerinden korumaktır ve testler sonucunda şema başarılı olmuştur.

İlerleyen çalışmalarda şemanın kapasitesini ve dayanıklılığını arttırmaya yönelik çalışmalar yapılacaktır ve bahsedilen metot spatial domain' de uygulanacaktır.

Teşekkür

Bu çalışma TUBITAK 2130120 numaralı proje tarafından desteklenmektedir.

Kaynakça

[1] SHEN, S. Y., HUANG, L. H., "A DATA HİDİNG SCHEME USİNG PİXEL VALUE DİFFERENCİNG AND İMPROVİNG EXPLOİTİNG MODİFİCATİON DİRECTİONS", COMPUTERS & SECURİTY, CİLT 48, 131-141, 2015.

[2] Lin, C. C., Liu, X. L., Yuan, S. M., "Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping", Information Sciences, Cilt 293, 314-326, 2015.

[3] Lu, T. C., Tseng, C. Y., Deng, K. M., "Reversible data hiding using local edge sensing prediction methods and adaptive thresholds", Signal Processing, Cilt 104, 152-166, 2014.

[4] S. U. Maheswari, S. U., Hemanth, D. J., "Frequency domain QR code based image steganography using Fresnelet transform", AEU - International Journal of Electronics and Communications, Cilt 69, No 2, 539-544, 2015.

[5] Roy, S., Venkateswaran, P., "A Text based Steganography Technique with Indian Root", Procedia Technology, Cilt 10,167-171, 2013.

[6] Dasgupta, K., Mondal, J. K., Dutta P., "Optimized Video Steganography Using Genetic Algorithm (GA)", Procedia Technology, Cilt 10,131-137, 2013.

[7] Mali, S. N., Patil, P. M., Jalnekar, R. M., "Robust and secured image-adaptive data hiding", Digital Signal Processing, Cilt 22, No 2, 314-323, 2012.

[8] Yan, D., Wang, R., Yu, X., Zhu J., "Steganalysis for MP3Stego using differential statistics of quantization step", Digital Signal Processing, Cilt 23, No 4, 1181-1185, 2013.

[9] Tang, M., Hu, J., Song W., "A high capacity image steganography using multi-layer embedding", Optik - International Journal for Light and Electron Optics, Cilt 125, No 15, 3972-3976, 2014.

[10] Wu, M. Y., Ho, Y. K., Lee J., H., "An iterative method of palette-based image steganography", Pattern Recognition Letters, Cilt 25, No 3, 301-309, 2004.

[11] Şahin Mesut A., Mesut A.,Saklı M.T., "Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri", III Ağ ve Bilgi Güvenliği Sempozyumu, Ankara-Türkiye, 2010.

[12] Chen, W. Y., "Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques", Applied Mathematics and Computation, Cilt 196, No 1, 40-54, 2008.

[13] Ioannidou, A., Halkidis, S. T., Stephanides, G., "A novel technique for image steganography based on a high payload method and edge detection", Expert Systems with Applications, Cilt 39, No 14, 11517-11524, 2012.

[14] Elshoura, S. M., Megherbi, D. B., "A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments", Signal Processing: Image Communication, Cilt 28, No 5, 531-552, 2013.

[15] Yang, C. H., "Inverted pattern approach to improve image quality of information hiding by LSB substitution", Pattern Recognition, Cilt 41, No 8, 2674-2683, 2008.

[16] Chen, S. K., "A module-based LSB substitution method with lossless secret data compression", Computer Standards & Interfaces, Cilt 33, No 4, 367-371, 2011.

[17] Chang, C.C., Hsiao, J.Y., Chen, C.S., "Finding optimal Least-Significant-Bit substitutionin image hiding by dynamic programming strategy", Pattern Recognition, Cilt 36, 1583–1595, 2003.

[18] Chan, C. K., Cheng, L. M., "Improved hiding data in images by optimal moderately significant-bit replacement", IEE Electron. Lett., Cilt 37, No 16, 1017–1018, 2001.

[19] Yang, B., Chen, S., "A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image", Neurocomputing, Cilt 120, 365-379, 2013.

[20] Luo, Y., Wu, C. M., Zhang, Y., "Facial expression feature extraction using hybrid PCA and LBP", The Journal of China Universities of Posts and Telecommunications, Cilt 20, No 2, 120-124, 2013.

[21] Nanni, L., Lumini, A., Brahnam, S., "Survey on LBP based texture descriptors for image classification", Expert Systems with Applications, Cilt 39, No 3, 3634-3641, 2012.

[22] Kanan, H. R., Nazeri B., "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm", Expert Systems with Applications, Cilt 41, No 14, 6123-6130, 2014.