

Sayısal Görüntülerdeki Yerel Parlaklık Değişimine Dayalı Adaptif Steganografi

M. Ulutaş IEEE Üyesi, V.V. Nabiyev, G. Ulutaş

Özet - Veri güvenliğinin sağlanmasındaki yöntemlerden biri de eski çağlardan beri kullanılmakta olan Steganografi tekniğidir. En bilinen teknik olan LSB'ye gömmeden farklı olarak kodlanacak bit miktarının yan bilgiler aracılığıyla belirlenmesi, adaptif steganografi olarak adlandırılır. Çalışmada, sayısal görüntü içerisindeki piksel grupları üzerinde, yerel parlaklık değişimleri hesaplanmış ve bu doğrultuda kodlanacak bit sayısı belirlenmiştir. Yerel değişimlerin hesaplanmasında standart sapma fonksiyonundan faydalanılmıştır. Görüntüdeki değişimlere göre kodlanacak bit sayısını belirleyen yöntem, gömülebilir veri içeriğini görüntünün karmaşıklığı ile orantılı olarak artırmıştır. Oluşturulan stego görüntüdeki parlaklık değişiminin gözle görülemeyecek ölçüde olduğu gösterilmiştir. Görüntünün ayrıntı düzeyi ile PSNR değerleri ters orantılı olarak değişirken taşıma kapasitesinin doğru orantılı olarak değiştiği görülmüştür.

Anahtar Sözcükler – Adaptif Steganografi, Steganografi

I. GİRİŞ

Günümüzün vazgeçilemez iletişim araçlarından birisi ve belki de en önemlisi internet'tir. Güncel bilgiye olan ihtiyacın giderek artacağı göz önüne alındığında internetin iletişim amacı ile kullanımının önemi açıkça ortaya çıkmaktadır. Gelişmiş ülkelerde yapılan işlemlerin çoğu artık elektronik ortamda da yapılabilir hale gelmiştir. Askeri birim veya devlet kurumları arasındaki haberleşme, elektronik ve mobil ticaret, online banka işlemleri, öğrenci not girişi gibi güvenlik gerektiren işlemlerin internet üzerinden yapıldığı göz önüne alındığında, veri güvenliğinin sağlanmasının gerekliliği açıkça görülmektedir.

Veri güvenliğinin sağlanmasında kullanılan yöntemlerden biri şifrelemedir. Taraflarca bilinen şifreleme algoritmasının uygulanması sonucu oluşan kodlanmış veri, kötü amaçlı kişilerin hedefi haline gelecektir. Veri gizlemede kullanılan diğer bir yöntem olan Steganografi'de, iletilmek istenen veri başka bir ortamın içerisine saklanır [1,2]. Kodlanmış bilginin görünür olmayışı, verinin dikkat çekmeden iletilmesini sağlayacaktır. Saklama için kullanılan ortam görüntü, video klip, ses veya metin dosyası olabilir. Bunların içerisinde veri saklamada en yaygın olarak kullanılanı, veri saklama kapasitesi büyük olup sayısal biçimde iletilen görüntü dosyalarıdır.

Aktarılmak istenen bilginin, örten görüntü (cover image) içerisine saklanmasından sonra oluşan ortama stego görüntü adı verilir. Stego görüntüyü oluşturan steganografik sistemden beklenen bazı gereksinimler vardır. (i) yüksek kapasitede veri saklayabilme (ii) saklama sonucu oluşan stego görüntüdeki verinin gözle fark edilememesi (iii) iletişim kanalından kaynaklanan bozulmalara karşı dayanıklı olması. Fakat bu gereksinimlerin hepsini aynı anda karşılamak zordur. [3]

Verinin görüntü içerisine saklanmasında kullanılan steganografik teknikleri şu şekilde özetleyebiliriz [3,4]

LSB'ye gömme: Bilinen ilk steganografik veri saklama yöntemidir. Resme ait piksel değerlerinin en az anlamlı bit hanelerine, verinin yerleştirilmesiyle gerçekleştirilir. Uygulama açısından basit olan bu yöntemde kullanılan bit sayısı depolama kapasitesini ve resmin bozulma oranını belirler.

İz düşürme yöntemi (Mapping Method): Gönderen tarafça seçilen matematiksel fonksiyon ile veri gömülmesi gerçekleştirilir. Tarafların kullanılan matematiksel fonksiyonu önceden bilmesi zorunludur. Diğer yöntemlerle karşılaştırıldığında düşük veri depolama özelliğine sahiptir.

Frekans Domenine Gömme (Frequency Domain Embedding): Sayısal görüntü DCT, FFT ya da wavelet fonksiyonlarının yardımıyla frekans domenine dönüştürülür. Saklanacak olan veri, en anlamsız frekans katsayılarına gömülür ve ardından görüntü yeniden uzaysal domene dönüştürülür.

Sıçramalı Tayfa Gömme (Spread Spectrum Embedding): Geniş frekans bandına, rasgele olarak verinin dağıtılması işlemidir.

Yayının geri kalan kısmında, bölüm 2'de adaptif steganografi'de yapılmış olan bazı çalışmalardan bahsedilirken, bölüm 3'de önerilen yöntem detayları ile anlatılacaktır. Yöntemin sonuçlarına ilişkin veri ve değerlendirmeler bölüm 4'de ve yapılabilecek öneriler bölüm 5'de yer almaktadır.

II. BENZER ÇALIŞMALAR

Uygulama kolaylığı açısından kullanılan en genel steganografik yöntem olarak LSB'ye gömme gösterilebilir. Piksellere veri saklamada kullanılan bit sayısının, görüntüdeki niteliklere göre belirleniyor olmaması, yapılan değişimin insan gözü tarafından ayırt edilebileceği gerçeğini beraberinde getirir. Oysa her pikselin saklayabileceği olduğu bit sayısı gerek komşu piksellerdeki değişime, gerekse kendisinin genel tablo içerisinde taşıdığı özneliğe bağlı olarak değişir. Parlaklık değişiminin düşük olduğu bölgelerde saklanan bilgi insan gözü ile kolayca fark edilebilirken, değişimin yüksek olduğu bölgelerde daha fazla bilgi kodlansa dahi görme sisteminin algılaması neredeyse imkansızdır [5]. Bu nedenle yapılan bazı çalışmalarda farklı piksellere, kullanılan yöntemin belirlediği sayıda bit kodlanarak adaptif steganografik yöntemler önerilmiştir [5,6,7,8].

Yaklaşımlardan birinde, kodlanacak pikselin komşuluklarındaki iki, üç veya dört pikselin parlaklık değerlerinin ortalaması alınarak yan bilgi oluşturulur [5]. Pikselin çevresindeki parlaklık değişimi hakkında bilgi veren bu değer, kodlanacak olan bit sayısını belirlemede kullanılır. Yöntemde depolama kapasitesi

artırılırken, aynı zamanda görüntüdeki bozulmanın olabildiğince azaltıldığı söylenmektedir. Alıcı tarafta bilginin çıkartılması esnasında fazladan herhangi bir bilgiye ya da resmin aslına ihtiyaç duyulmamaktadır.

Görüntüdeki örtüşmeyen ikili piksel grupları farklarının, parlaklık değişimini temsil ettiği düşünülen çalışmada, fark değerleri sayısal aralıklara karşı düşürülür [6]. Aralığın genişliğinden kodlanacak olan bit miktarı belirlenir. İki piksel arasındaki fark değerinden yeni fark değeri elde edilmesi esnasında, aynı aralık içerisinde kalınmasına dikkat edilir. Oluşan yeni fark değerini temsil edecek ve aynı zamanda kodlanacak bilgiyi içerecek şekilde, piksel değerleri kullanılan matematiksel bir fonksiyon yardımıyla değiştirilir. Yöntemin RS Diyagramları tarafından analiz edilemeyeceği de gösterilmiştir.

AdMod olarak da bilinen diğer çalışmada, gömme fonksiyonu Dither maskesine göre seçilmiştir. Amaç kullanılan adaptif steganografik yöntemi histogram analizlerine karşı dirençli hale getirmektir. [7]

Gri seviyeleri, çalışmada belirtilen algoritma uyarınca belirlenen şekilde, farklı genişlikte olabilen dört aralığa bölünür. İşlem görmekte olan pikselin hangi aralığa düştüğünün belirlenmesi, ilgili piksele gömülebilecek bit miktarını verir. Çalışmada görüntüde oluşabilecek bozulmaları engelleyebilmek amacıyla bir piksele en fazla dört bit veri kodlanabileceği varsayımı yapılmıştır [8]. Alıcı tarafta verinin stego ortamdan çıkarılabilmesi için asıl görüntü içerisine, gönderen tarafta en fazla 3 byte uzunluğunda veri yerleştirilmektedir.

III. ÖNERİLEN YÖNTEM

Önerilen yöntem, seçilen bölge içindeki piksellere kodlanabilecek bit sayısını parlaklık değişiminin bir fonksiyonu olarak hesaplamaktadır. Örtüşmeyen 3x3 boyutlarındaki piksel grupları içindeki merkez piksele göre kuzey, güney, doğu ve batı yönlerindeki komşu piksel parlaklık değerleri kullanılarak grubun parlaklık değişimi hesaplanmaktadır. Değişimin hesaplanmasında kullanılan ifade, (1) de hesaplanan standart sapma fonksiyonudur.

$$x = \frac{1}{N} \sum_{i=1}^N x_i = \frac{x_1 + x_2 + \dots + x_N}{N} \quad (1)$$

$$s = \sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - x)^2}$$

Standart sapma fonksiyonu, her biri aslında küçük bir görüntü olan yerel bölgelerdeki içerik hakkında bilgi vermektedir. Piksel grubunun temsil ettiği görüntü parçasının içerisinde köşe gibi sert geçişlerin mi olduğunun ya da değişmeyen özellik gösteren görüntümü barındırdığının belirlenmesinin matematiksel yoludur.

Parlaklık değerleri g_u , g_d , g_r ve g_l olan dört piksele ait standart sapma değeri (2) de elde edilmektedir.

$$a = \frac{(g_u + g_d + g_r + g_l)}{4}$$

$$s = \sqrt{\frac{(g_u - a)^2 + (g_d - a)^2 + (g_r - a)^2 + (g_l - a)^2}{4}} \quad (2)$$

Dört komşu piksel üzerinde yapılan standart sapma işlemi sonucu elde edilen değer iki tabanına göre logaritması alınarak, kodlanabilecek bit sayısı (3)'deki şekilde elde edilir.

$$n = \log_2 s, \quad s \geq 2 \quad (3)$$

Bulunan bu değer, piksel grubunun standart sapma hesabında kullanılmayan diğer beş pikselin her birine kaç bit kodlanacağını gösterir. Gömülecek olan mesajın n biti çıkartılır. Veri gömme işlemi esnasında 7 elemanlı bir dizi kullanılmaktadır. Bu dizinin hangi elemanının kullanılacağına ilişkin indeks değerini n değeri referanslamaktadır. Maske olarak adlandırılan dizinin onaltılık düzendeki elemanları tablo 1'de verilmektedir.

Tablo 1. Maske dizisinin elemanları

Maske	[1]	[2]	[3]	[4]	[5]	[6]	[7]
	FE	FC	F8	F0	E0	C0	80

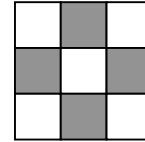
N bitlik verinin Şekil 1'de beyaz ile gösterilen piksellerden birine kodlanması esnasında gerçekleştirilen işlemler (4)'de verilmektedir. Kodlama yapılacak piksel değeri g ve kodlanacak n bitlik veri b ile gösterilirse

$$g = g \wedge Maske[n] \quad (4)$$

$$g = g \vee b$$

(4) ile gösterilen işlem Şekil 1'de beyaz ile temsil edilen piksellere uygulanır. Her piksel için farklı n bitlik veri grupları işlem görecektir. İlgili piksellere belirlenen sayıda bit yerleştirilerek stego görüntü oluşturulur. Şekil 1'de gri ile temsil edilen bölgeler standart sapma hesabında kullanılan pikselleri temsil ederken, beyazla gösterilen pikseller veri saklamada kullanılanlardır.

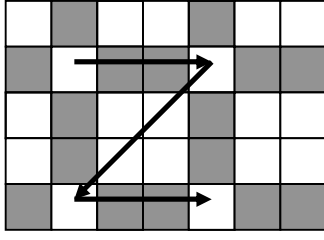
Veri kodlama esnasında görüntü raster-scan yöntemi ile taranır. Tarama işlemi ikinci satır ikinci sütunundan başlarken, son sütundan bir önceye kadar devam eder. Yatay ve düşey eksenlerde üç birimlik atlamalarla ilerlenmektedir.



Şekil 1. Kullanılan 3x3 lük yerel piksel grupları

Böyle bir tarama yönteminin kullanılmasındaki neden, standart sapma hesabında kullanılacak olan piksel değerlerinin değiştirilmemesi gerektiğidir. Kodlama esnasında kullanılan tarama yöntemi şekil 2'de gösterilmektedir.

Alıcı tarafta kodlanmış piksellerin kaç bitinin veri taşımada kullanıldığını belirleyebilmek için, standart sapma hesabında kullanılan piksel değerlerinin değiştirilmemesi gerekmektedir. Diğer bir deyişle standart sapma hesabında kullanılan dört pik-



Şekil 2. Kullanılan tarama yönteminin örnek görüntüsü

sel, veri kodlamada kullanılmayacaktır. Kullanılan pikseller 5/9 oranında olsa dahi, yöntemin adaptifliği sayesinde resmin taşıma kapasitesi sonuçlar bölümünde de görüldüğü gibi yeterince büyüktür. Gömülü olan verinin çıkartılması için gereken işlemler gönderen tarafındaki ile aynıdır. Standart sapma hesabı 3x3'lük bloklar üzerinde gerçekleştirilecek ve elde edilen bit değeri, veri çıkarmada kullanılacaktır.

Denklem (1)'den yola çıkarak karşılaşılabilecek en büyük standart sapma değeri, hesapta kullanılan dört pikselin değerlerinin birbirine en uzak olduğu durumda ortaya çıkar. Diğer bir deyişle en büyük standart sapma dört pikselin ikisi siyah, ikisi beyazken gerçekleşir. Söylenilen durumun oluşması sonucu hesaplanan ve üste yuvarlanan değer 128 olur. Önerilen yöntem gereği, hesaplanan standart sapmanın 2 tabanına göre logaritması alındığında 7 değeri elde edilir.

Piksel grupları üzerinde yapılan standart sapma hesabının sonuçlarının 0 ile 128 arasında olacağı açıktır. Bu aralık, kodlanacak bit sayısını verecek şekilde, iki tabanına göre logaritma alınarak 1 ile 7 arasına iz düşürülür. Kodlanabilecek asgari bit miktarı kullanıcı tanımlıdır. İstenildiği takdirde piksel başına kodlanabilecek asgari bit sayısı düşürülebilmektedir. Bit sayısının düşürülmesi PSNR değerini iyileştirirken, kodlanacak veri miktarını azaltacaktır. Standart sapma sonucu çıkan değerlerin ikiden küçük olması durumunda, ilgili piksel grubundaki parlaklık değişiminin az olduğu anlaşılır ve kodlama yapılmaz.

IV. SONUÇLAR

Yapılan deneyler 512x512 boyutlarındaki, Lena, Pepper, Baboon, Jet isimli dört sayısal görüntü üzerinde gerçekleştirilmiştir. Gri seviyesi ile temsil edilen görüntüdeki parlaklık değerleri [0-255] aralığındadır. Kullanılan görüntülerden ikisi Şekil 3'de gösterilmiştir.

Yapılan testlerde, örnek görüntüler içerisine rasgele oluşturulan bit dizisi gömülmüştür. Şekil 4'de gömme işleminin sonucu oluşan stego görüntüler verilmektedir. Oluşan stego görüntülerde insan gözüyle fark edilebilen herhangi bir değişikliğe rastlanmamaktadır.

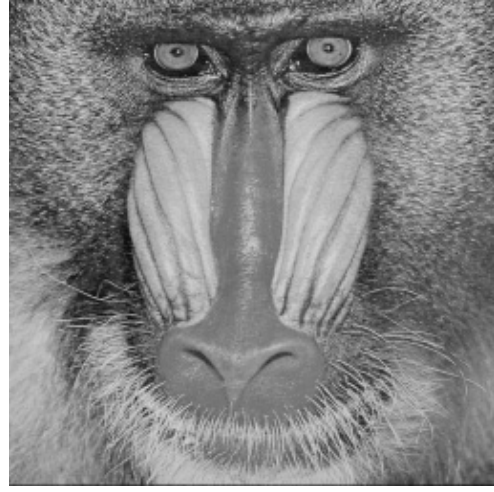
Gömme işleminin resmin neresinde ne kadar bozulmaya neden olduğunu görebilmek amacıyla fark görüntüleri elde edilmiştir. Görüntünün elde edilebilmesi için, stego görüntüler ile asıl görüntülerin parlaklık değerlerinin farkı alınmıştır. Oluşan yeni sayısal görüntülere bakarak, veri gömme işleminin daha çok resmin hangi bölgelerinde gerçekleştiği gözlemlenebilmektedir. Bu görüntüler üzerinde iyileştirmeler yapılarak (piksel parlaklık değerlerinin beş kat artırılması) belirgin hale gelmeleri sağlanmıştır. Şekil 5'de ilgili fark görüntüleri gösterilmektedir.

Görüntülerdeki bozulmanın daha çok parlaklık seviyesinin hızla değiştiği kenar bölgelerinde gerçekleştiği fark görüntülerine bakarak rahatlıkla söylenebilir. Bozulmanın daha çok bu bölgelerde olması, yöntemin sonucunun insan gözü tarafından ayırt edilmesinin güç olduğunu gösterir. Çünkü parlaklık seviyesinin hızla değiştiği kenarlardaki bozulmalar, insan gözü tarafından ayırt edilemez.

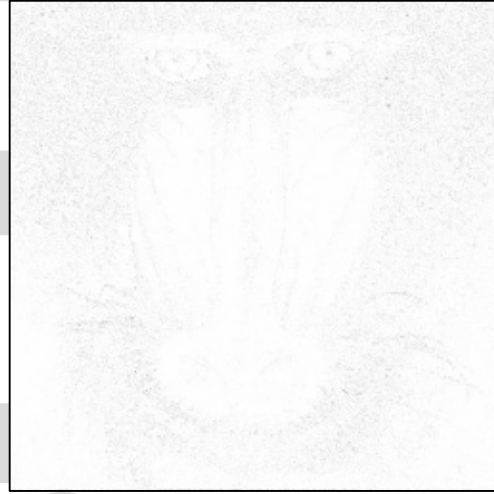
Yöntemin performansını ölçebilmek amacıyla uygulanan diğer bir yöntem, oluşan stego görüntü üzerinde PSNR (Peaks of the signal to noise), RMSE (Root Mean Square Error) ve taşıma kapasitesi değerlerinin hesaplanmasıdır. Elde edilen sonuçlar Tablo 2'de verilmiştir.



Şekil 3. 512x512 boyutlarındaki örten görüntüler (a) Lena (b) Baboon



Şekil 4. Veri gömme sonucu oluşan stego görüntüler



Şekil 5. Lena ve Baboon'a ait fark görüntüleri

Tablo 2. Stego görüntülerdeki PSNR, RMSE ve taşıma kapasitesi değerleri

	PSNR	RMSE	Taşıma Kapasitesi
Lena	47.148	1.119	141300
Jet	45.067	1.422	168710
Peppers	46.104	1.262	133710
Baboon	41.179	2.226	299605

PSNR değerinin yüksek olması görüntüdeki daha az bozulmanın bir işaretçisidir. En fazla bozulmanın, en düşük PSNR'ye sahip olmasının gereği olarak Baboon resminde olduğu söylenebilir. Oysa Şekil 4'den görülebileceği gibi, görüntüde fark edilebilir hiçbir bozulma oluşmamıştır. Baboon'da kodlanan veri miktarının fazlalığından dolayı oluşan düşük PSNR, taşıma kapasitesinin artması ile sonuçlanmıştır. Önerilen yöntemde de bahsedildiği üzere, parlaklık değişiminin fazla olduğu yerlerde, kodlanacak bit miktarı, standart sapma fonksiyonunun sonucundan dolayı fazla olacaktır.

Baboon resminin diğerlerine kıyasla daha fazla veri barındırıyor olması, yöntemin çalıştığı bir ispatıdır. Lena'ya bakıldığında PSNR değerinin daha yüksek, bunun karşılığında taşıma kapasitesinin düşük olduğu görülmektedir. Resmin genelindeki parlaklık değişimlerinin Baboon'a kıyasla daha az oluşu, gömülecek veri miktarını da düşürmüştür. Değişimin azlığı standart sapma fonksiyonu sonucu oluşan değerlerin Baboon'a kıyasla daha küçük oluşuna, dolayısıyla daha az bit kodlanmasına sebep olacaktır.

Yöntem, standart sapma fonksiyonunu, işlem gören piksel grubundaki piksellere kaç bit veri kodlanacağını bulabilmek amacıyla kullanır. Tüm piksellere sabit sayıda bit kodlamak-tansa, pikselin bulunduğu bölgedeki parlaklık değişimi göz önüne alınarak değişken sayıda bit kodlaması gerçekleştirilmiştir. Sonuçta oluşan görüntülerde görülebilir herhangi bir etki ile karşılaşılma-mış, resmin karmaşıklığıyla orantılı miktarda veri gömme işlemi gerçekleştirilmiştir. Aynı zamanda verinin, daha çok görüntünün parlaklık değerlerinin hızla değiştiği kenar kısımlarını içeren bölgelerine kodlandığı fark görüntülerinden izlenmiştir.

V. DEĞERLENDİRME

Parlaklık değişimlerini kullanılan matematiksel fonksiyon aracılığıyla belirleyen, resmin geneli üzerinde değişen sayılarda bit kodlayan yeni ve etkin bir yöntem önerilmiştir. Yöntemin sonuçları göz önüne alındığında, taşıma kapasitesi açısından, ayrıntı ile uyumlu bir artım gözlemlenmiştir. Aynı zamanda oluşan stego görüntüler üzerinde insan gözünün ayırt edileceği herhangi bir kötü etki ile karşılaşılma-mıştır. Gerek güvenlik açısından gerekse görsel etkisi açısından LSB kodlamaya nazaran çok daha etkin bir yöntemdir. Verinin alıcı tarafta elde edilmesi esnasında asıl görüntüye ya da asıl görüntü içerisine eklenecek herhangi bir bilgiye ihtiyaç duyulmamaktadır. İlerleyen çalışmalarda yöntemin istatistiksel ataklara karşı analizi yapılabileceği gibi, 3x3 lük kareler halinde seçilen piksel gruplarının büyütülmesinin taşıma kapasitesi ve PSNR açısından nasıl sonuçlar vereceği gözlemlenebilir.

KAYNAKÇA

- [1] Anderson, R.J., Petitcolas, F.A.P., "On the limits of steganography", IEEE J. Select. Area Commun., vol. 16, pp. 474-481, 1998.
- [2] Katzenbeisser, S., Petitcolas, F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Inc., Boston, 2000.
- [3] K.B. Raja, Sidaraju S, K.R. Venugopal, L.M. Patnaik, "Secure Image steganography Using Color Palette Decomposition", International Conference on Intelligent Sensing, Anna University, Chennai, February 2007.
- [4] Shirali-Shahreza, M., Shirali-Shahreza, S., "Collage Steganography", 5th IEEE/ACIS International Conference on Computer and Information Science, pp. 316-321, July 2006.
- [5] Chang, C.C., Tseng, H.W., "A steganographic method for digital images using side match", No. 12, pp. 1431-1437, September 2004.
- [6] Wu, D.C., Tsai, W.H., "A steganographic method for images by pixel-value differencing", No. 9-10, pp. 1613-1626, June 2003.
- [7] Franz, E. and Schneidewind, "Adaptive steganography based on dithering", In Proceedings of the 2004 Workshop on Multimedia and Security, Germany, September 20 - 21, 2004.
- [8] Wen-Nung L., Li Chun Chang, "Data hiding in images with adaptive numbers of least significant bits based on the human visual system", ICIP99, 286-290 pp, vol.1, 1999.