

# Histogramlar Optimizasyonu ile Alındısız Sırörtme Yaklaşımı

Özdemir Çetin, Fevzi Akar

**ÖZET** — Video stenografi uygulamalarında dikkat edilmesi gereken en önemli noktalardan birisi veri gömme yapılacak uygun pikselin bulunmasıdır. Uygun pikselin atanamaması durumunda video çerçevelerinde veri gömme yapılmış noktalar dalgalanma etkisi yaparak gizli veriyi ele verirler. Bu çalışmada dalgalanma etkisini ortadan kaldıracak yeni bir stenografi yaklaşımı geliştirilmiştir. Sunulan stenografi yaklaşımında uygun pikseller videonun histogram değerlerine göre belirlenerek dalgalanma etkisi yok edilmiştir.

**Anahtar Kelimeler:** Veri Gömme, Alındısız Sırörtme, Sayısal Video, Histogram

## I. GİRİŞ

Son yıllarda büyük bir gelişme kaydeden Internet gibi bilgi paylaşım platformları sayısal bilgiyi kalitesini bozmadan paylaşabilme imkânı sunar. Bu durumun teorik olarak düşünüldüğü zaman insanlara inanılmaz bir kolaylık ve fayda sağladığı söylenebilir. Bununla birlikte bu devasa büyüklükteki sanal dünyanın güvenlik zafiyetleri beraberinde birçok sorunu da getirmektedir. Örneğin maddi değeri olan sayısal medyanın yasadışı dağıtımı yüzünden büyük bir ekonomik kayba yol açtığı tartışmasız bir gerçektir [1]. Maddi kayıpların yanında diğer bir önemli sorun ise, insanların haberleşme mahremiyetlerinin ihlal edilmesidir. Gerek ekonomik anlamda gerekse de güvenlik anlamında meydana gelen bu tür olumsuzluklar sayısal medyanın korunması ve güvenli haberleşme gerekliliklerini ortaya çıkarmaktadır.

Bu gereksinimleri gidermek için yapılan çalışmalar, Çoklu ortam dosyalarının telif hakkını korumayı amaçlayan sayısal damgalama ve gizli haberleşme yapmaya imkân sağlayan stenografi olarak iki kategoride toplanabilir [2,3]. Her iki uygulamada da kullanılan yöntemler benzerlik gösterse de kullanım amaçları itibariyle teknikler birbirlerinden ayrılmaktadırlar. Sayısal damgalama bir sayısal medyanın (film, müzik dosyaları vb.) illegal yollarla paylaşılmasını önlemek için kullanılırken, stenografi, dünyanın farklı coğrafi bölgelerinde bulunan bireylerin gizli haberleşme yapmalarına olanak sağlamak için tercih edilen uygulamalardır [3,4].

Özdemir Çetin is with the Department of Computer Systems, Sakarya University, Sakarya, 54188, Turkey  
(e-mail: ocerin@sakarya.edu.tr)

Fevzi Akar is with the Department of Electrical&Electronic Engineering, Turkish Naval Academy, İstanbul, 34940, Turkey  
(e-mail: fezyiakar@dho.edu.tr)

Telif hakkı koruma için geliştirilmiş sayısal damgalama teknikleri gizli haberleşme için geliştirilmiş olan stenografi tekniklerine göre saldırılara karşı daha dayanıklı olmak zorundadır. Çünkü gizli haberleşme esnasında kullanılacak taşıyıcı dosya herkes tarafından bilinen bir dosya olmak zorunda değildir. Bu yüzden de bu taşıyıcının bir saldırıya maruz kalma ihtimali de daha düşük olacaktır.

Video Stenografi teknikleri sıkıştırılmış ve sıkıştırılmamış videolar için iki sınıfa ayrılmıştır. Sıkıştırılmamış videoya uygulanan ilk stenografi çalışmasında spread-spectrum yöntemi kullanılmıştır. Burada gizli bilgi taşıyıcı dosyanın uzunluğuna sahip olan ikili sayı dizileri olarak temsil edilmiştir. Gizli bilginin geri alınması korelasyon metodu ile olmaktadır ve video çerçevelerinden biri veya birkaçının zarar görmesi durumunda gizli bilgiye ulaşılamamaktadır [5]. Bir başka çalışmada, araştırmacılar resim kırpma saldırılarına karşı bir stenografi yöntemi geliştirmişlerdir. Araştırmacılar amaçlarını gerçekleştirebilmek için taşıyıcı resmi alt guruplara bölmüşler ve gizli bilgiyi sıkıştırıp şifreleyerek bunların içerisine yerleştirmişlerdir. Lagrange Interpolating Polynomial yöntemi kullanılarak gizli bilgi geri elde edilmektedir. Bir diğer çalışmamızda ise, histogram yöntemini kullanarak gizli verinin taşıyıcı video içerisine yerleştirilmesini önermiştik. Bunun için her bir çerçeve alt guruplara bölünerek histogram değerleri hesaplanmış ve İGS'nin (İnsan Görme Sistemi) algı sınırının altında olan bölgeler belirlenerek veri gizleme gerçekleştirilmiştir [2,6].

Veri gizleme/gömme çalışmalarında birbirleriyle yakından ilişkili olan kritik parametreler: güvenlik, güvenilirlik, görünmezlik, karmaşıklık ve veri gömme kapasitesidir [7]. Haberleşme amaçlı veri gizleme/gömme işlemi hedeflendiğinde gizli veri kapasitesinin mümkün olduğunca yüksek olması istenir. Böyle uygulamalarda sıkıştırılmış video kullanmak gizli veri kapasitesini olumsuz yönde etkileyecektir. Telif hakkı koruma amaçlı veri gizleme/gömme gerçekleştirilecek ise burada gizli veri kapasitesi küçük boyutlarda olacağından bu tür uygulamalarda sıkıştırılmış video kullanılabilir.

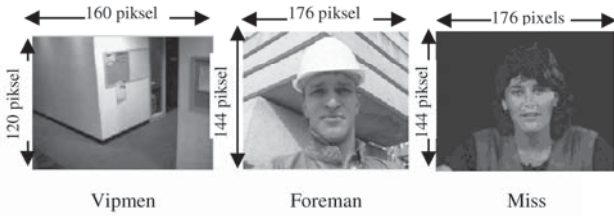
Bu makalede, önceki çalışmalardan farklı olarak taşıyıcı video içindeki veri gömmeye uygun pikseller video çerçevelerinin histogram değerlerine göre belirlenmiştir. Gizli haberleşme süresince taşıyıcı videonun dışarıdan gelebilecek saldırılara maruz kalmaması için gizli bilgi algılanabilirliğinin en düşük seviyelerde tutulması çalışmanın temel amacıdır.

## II. TEMEL KAVRAMLAR

Bir sayısal video, çerçeve olarak isimlendirilen hareketsiz sayısal görüntülerin İGS'nin fark edemeyeceği bir hızda ardı sıra oynatılması ile elde edilen hareketli görüntü olarak tanımlanabilir.

Veri gizleme uygulamalarında kullanılan video türleri arasında en yaygın olanı AVI (Audio-Video Interleave) formatıdır. Bu formattaki videolar BMP formatındaki resim dosyalarının ardı sıra eklenmesi ile oluşturulur. Deneysel çalışmalar süresince 'vipmen.avi', 'foreman.avi' ve 'miss.avi' videoları kullanılmıştır. Şekil 1'de bu videoların boyutları verilmiştir.

Histogram sayısal bir görüntüyü oluşturan piksellerin sahip oldukları renk bileşenlerinin koyuluk bilgilerine göre dağılımlarını gösteren değerler dizisidir. Bu değerler dizisine bakılarak sayısal görüntünün keskinlik durumu ya da tonları hakkında bilgi sahibi olunabilir.



Şekil-1. Deneysel çalışmalarda kullanılan video çerçeveleri.

## III. BÖLGESEL HİSTOGRAMLAR OPTİMİZASYON YÖNTEMİ

Veri gizleme alanında son yıllarda yapılan çalışmalarda araştırmacılar uyarlanabilir stenografiye yönelmişler ve İGS tabanlı teknikler geliştirmişlerdir. Uyarlanabilir stenografide amaç gizli bilginin taşıyıcı içerisine gömülmesinde İGS kriterlerinin ön planda olmasıdır. Böylece gizli bilginin yetkisiz kişiler tarafından algılanması neredeyse imkânsız hale gelmektedir. Bu tekniklerde kullanılan yöntemlerden biri histogramlar yaklaşımıdır [6].

Histogramlar yaklaşımında taşıyıcı videonun her bir çerçevesine ait histogram değerleri elde edilerek yorumlanır. Histogram değerinin büyük olması renk ve hareket değişimlerinin fazla olduğunu, küçük olması ise sahne içeriğinin hemen hemen hiç değişmediğini belirtir.

Video çerçevelerindeki renk ve hareket geçişlerini algılamak için eşik değeri olarak adlandırılan sayısal bir değer kullanılır. Eşik değeri, çerçevelerin içeriğinde bir değişim veya benzerlik algılanmasında kullanılan, maksimum alabileceği değer video çerçevelerinin boyutu (MxN) ile ifade edilen piksel sayısıdır.

Veri gömme işlemi histogram farkının düşük olduğu çerçevelere yani renk bakımından tekdüze olan bölgelere yapıldığında uzamsal ve zamansal algılanabilirlik arttığı için veri gizleme işlemi başarısız olmaktadır. Bölgesel histogramlar optimizasyonu bu soruna çözüm getirmek amacıyla geliştirilmiş bir yöntemdir. Bu yöntemde veri gömülecek çerçeveler video boyutuna göre bloklara bölünür.

Çerçevelerdeki her bir bloğun histogram değeri

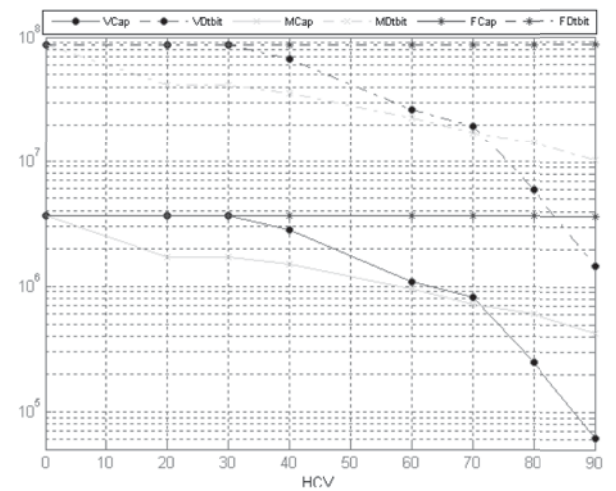
belirlenen eşik değeri ile karşılaştırılır. Bloğun histogram dağılımının belirlenen eşik değerinin üzerinde olması durumunda blok içerisinde farklı renklerin olduğu ve veri gömme için uygun olduğu söylenir.

Bu yöntemle veri gömme kapasitesinin artırılması amaçlanırken algılanabilirliğin ise düşürülmesi hedeflenmiştir. Her çerçeveye veri gömülmesine imkân verilerek kapasite artırılırken, çerçevedeki bütün pikseller yerine renk değişiminin en çok olduğu piksellere veri gömülerek de algılanabilirlik düşürülmüştür.

## IV. DENEYSEL SONUÇLAR

Çalışmanın bu bölümünde 'vipmen.avi', 'foreman.avi' ve 'miss.avi' videoları kullanılarak önerilen yöntemin deneysel sonuçları elde edilmiştir.

Şekil 2'de her üç videonun HCV (Histogram sabiti), gizli bilgi kapasitesi ve bozulan bit sayısına göre değerlendirildiği bir grafik görülmektedir. Grafikteki VCap; Vipmen videosunun kapasitesini, VDbt; Vipmen videosundaki bozulan bitleri belirtmektedir. Diğer videolar içinde aynı durum söz konusudur. Grafikte görüldüğü gibi HCV değerinin artması algılanabilirliğin azalmasına yani haberleşmenin güvenliğinin artması anlamına gelmektedir. Grafiğe göre deneysel çalışmada kullanılan her HCV değerinde de üç videodan gizli bilgi kapasitesi en yüksek olan Foreman videosudur. Bu durumda yüksek gizli bilgi kapasitesi gerektiren buna karşılık düşük güvenlik seviye haberleşmesinde Foreman videosunun kullanılması uygundur. Grafiğe göre HCV değerinin büyümesi ile Vipmen videosunun gizli veri kapasitesinin düştüğü görülmektedir. Bunun anlamı, yüksek güvenlik seviyesi gerektiren haberleşmede Vipmen videosu bölgesel histogramlar yöntemi için en ideal videodur.



Şekil-2. HCV parametresine göre bölgesel histogramlar optimizasyonu yönteminin analizi.

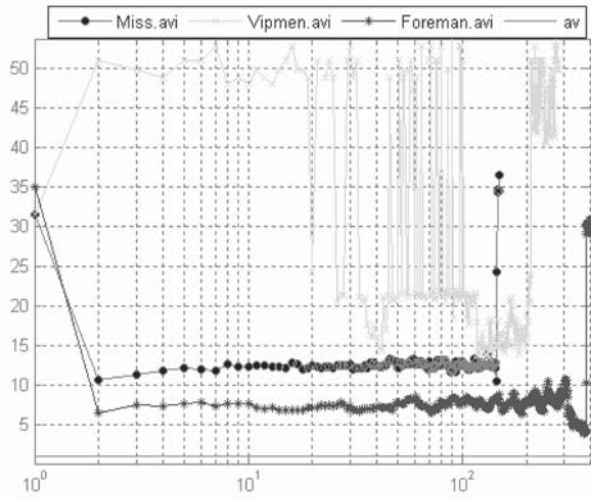
Ayrıca çalışmada elde edilen her bir sırlı videoya istatistiksel yöntemler uygulanarak görüntülerdeki bozulmalara ilişkin PSNR değerleri bulunmuştur. Her bir videoya ait PSNR analizleri Şekil 3 ve Şekil 4'de

verilmiştir. Elde edilen bu PSNR değerleri mevcut çalışmalara ait PSNR değerleri ile karşılaştırıldığında önerilen yöntemin iyi sonuç verdiği görülmektedir. Değiştirilmiş bir görüntünün PSNR değerleri 30dB ile 50dB arasında ise bu görüntüdeki bozulmalar önemsenmeyecek seviyede olduğu söylenebilir [8,9].

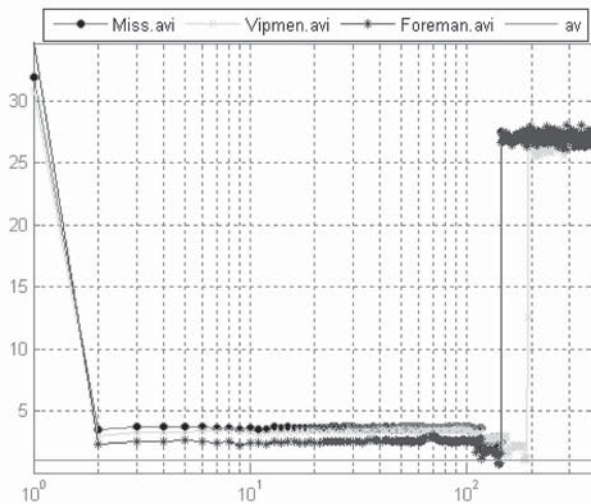
Şekil 3'de en yüksek HCV değerinde her bir videoya ait PSNR değerleri, Şekil 4'de ise en düşük HCV değerinde her bir videoya ait PSNR değerleri gösterilmektedir. Ayrıca grafikler kabul edilmiş 40dB PSNR değerinde normalize edilmiştir. Normalize işlemi av çizgisi ile gösterilmektedir.

Şekil 3'deki grafiğin sonucuna göre HCV değerinin en yüksek olduğu durumda bölgesel histogramlar yöntemi Vipmen videosu için en iyi sonucu vermektedir.

Şekil 4'deki grafiğin sonucuna bakıldığında en düşük HCV değerinde bölgesel histogramlar yöntemi Miss videosu için en iyi sonucu vermektedir.



Şekil-3. En yüksek HCV değerinde videolara ait PSNR değerleri.



Şekil-4. En düşük HCV değerinde videolara ait PSNR değerleri.

## V. SONUÇLAR

Bu çalışmanın amacı, güvenli olmayan haberleşme kanallarında haberleşme güvenliğini en üst seviyeye çıkarabilmek için yeni bir veri gizleme tekniği geliştirmek ve gerçekleştirmektir.

Stenografi uygulamalarının en kritik parametresi olan algılanamazlığı sağlamak için, uyarlanabilir stenografide kullanılan yaklaşımlardan biri histogramlar yaklaşımıdır. Histogram kriteri İGS hassasiyeti olan görsel bir kriter olması nedeniyle algılanabilirlikte önemli rol oynamaktadır. Bu çalışmada taşıyıcı videonun her bir çerçevesi bloklara bölünerek histogram değerlerinin elde edilmesi ile gizli veri gömülecek alanlar belirlenmektedir. Böylece çerçevelerdeki gereksiz bozulmaların önüne geçilerek algılanamazlık artmaktadır.

## KAYNAKLAR

- [1] Alattar, A.M., Lin, E.T., Celik, M.U., Digital Watermarking of Low Bit-Rate Advanced Simple Profile MPEG-4 Compressed Video, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 8, 2003.
- [2] O. Cetin, "A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach" Ph.D. dissertation, Dept. Elect. Eng., Sakarya Uni., Sakarya, Turkey, 2008.
- [3] O. Cetin, "A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Sakarya Uni., Sakarya, Turkey, 2008.
- [4] O. Cetin, A.T. Ozcerit, "A Novel Video-Stego Method Based On HVS (İGS Tabanlı Yeni Bir Video-Sırtörme Yöntemi)" 3rd Information Security&Cryptology Conference with International Participation, Ankara, Turkey, pp.84-88,December,2008.
- [5] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information Hiding a Survey, Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.
- [6] Ozdemir Cetin, A.Turan Ozcerit, "A new steganography algorithm based on color histograms for data embedding into raw video streams", Computers & Security, Volume 28, Issue 7, Pages 670-682, October 2009.
- [7] Wang H, Wang S. Cyber warfare:steganography vs.steganalysis. Communications of the ACM 2004,47(10).
- [8] A.N. Netravali, B.G. Haskell, "Digital Pictures: Representation, Compression, and Standards (2nd Ed)", Plenum Press, New York, NY 1995.
- [9] M. Rabbani, P.W. Jones, "Digital Image Compression Techniques", Vol TT7, SPIE Optical Engineering Press, Bellvue, Washington 1991.