

YÜKSEK KAPASİTELİ BİR ALINDISIZ VİDEO SIRÖRTME YÖNTEMİ

Özdemir Çetin^{1,2}, Ahmet T. Özcerit¹, Barış Boru¹

Sakarya Üniversitesi, Teknik Eğitim Fakültesi Elektronik-Bilgisayar Bölümü¹

University of New Mexico, Electrical&Computer Engineering Dept.²

{ocetin, aozcerit, barisb}@sakarya.edu.tr

ABSTRACT

In this paper, we have proposed a novel method for hiding secret data into digital video files. The proposed method requires two steps to complete the entire process: appropriate pixels for embedding procedures in the carrier video streams are determined first and then the secret data are mapped into those pixels using a special coding mechanism. The appropriate pixels in the video stream are resolved by a histogram method which utilizes the color and motion changes in the successive frames. The histogram weights of each pixel are calculated individually against a specified reference value and proper pixels are tagged accordingly. A data hiding coding technique is then applied to embed secret data into video frames.

The perceptibility of the hidden data in the modified video stream (stego-video) is evaluated by the PSNR (Peak Signal to Noise Ratio) parameter. The main motivation of this study is to obtain lower PSNR values while to maintain higher hidden data rates.

Keywords: Steganography, Data Hiding, Data Embedding, Histogram

1. GİRİŞ

İnternetin zaman ve mesafe kavramını ortadan kaldırması, sayısal medya ortamlarının da son yıllarda büyük bir gelişme göstermesiyle toplumlar arasındaki bilgi alışverişi ve haberleşme de inanılmaz boyutlara ulaşmış ve birçok avantaja sahip olmuştur. Örneğin, popüler bir müzik parçasının veya sinema filminin yasal olarak bir İnternet sitesinden elde edilebilmesi mümkündür ve büyük bir zaman tasarrufu, kolaylık sağladığı da açıktır. Ancak bu üstünlüklerin yanında ortaya çıkan güvenlik zafiyeti, bazı tekniklerin geliştirilmesini de zorunlu kılmıştır. Paylaşım kanalı açık sayısal verilerin damgalanması (watermarking) veya sırörtme (steganography) bu tekniklerden sadece bir kaçıdır.

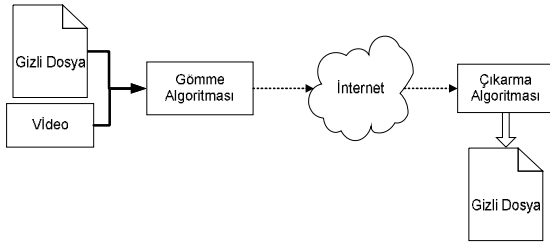
Sayısal medyanın gizli haberleşmede kullanılmaya başlanmasından önce yazılı metinler üzerinde birtakım işlemler yapılarak gizli haberleşme sağlanırdı. Bu gizli haberleşme yöntemine şifreleme

(cryptography) denir. Şifreleme işleminde yazılı metinler anlaşılması imkânsız olan biçimlere dönüştürülür ve bu şekilde haberleşme yapılır. Buradaki en büyük sorun, yetkisiz kişilerin haberleşmenin içeriğini bilmeseler bile ortada bir gizli haberleşme olduğunu anlayabilmeleridir. Sayısal medyanın gelişmesi ile gizli haberleşmede bu ortamların kullanılması ile sayısal damgalama, sırörtme gibi veri gizleme için değişik yöntemler geliştirilmiştir. Sayısal damgalama ve sırörtmede kullanılan yöntemler benzerlik gösterse de kullanım amaçları itibarıyla farklılıklara sahiptirler. Bir sayısal ortamın (sinema filmi, müzik parçası vb.) korunması ve yasadışı yollarla paylaşılmasını önlemek için sayısal damgalama kullanılır. Farklı coğrafi bölgelerde bulunan insanlar aralarında gizli haberleşme (askeri istihbarat vb.) yapmak için ise sırörtmeyi kullanırlar. Sayısal damgalama bilinen popüler bir medya dosyası üzerinde yapıldığından karşılaştığı saldırılar sırörtmeden farklılık gösterir. Çünkü sırörtmede kullanılan dosya, bilinmeyen herhangi bir dosya olacaktır ve saldırıya maruz kalması çok düşük bir ihtimaldir. Her iki yöntemde de en önemli nokta algılanabilirliğin neredeyse imkânsız olmasıdır. Gizli haberleşme teknikleri ilk olarak hareketsiz görüntüler üzerinde uygulanmıştır. Daha sonraki araştırmalarda ise geniş uygulama alanı ve büyük kapasiteye sahip olmasından dolayı hareketli görüntü üzerinde durulmuştur [1]. Hareketli görüntü üzerinde yapılan damgalama çalışmaları da kullanılan videoya göre Sıkıştırılmamış-Video Damgalama (Raw-Video Watermarking) ve Sıkıştırılmış-Video Damgalama (Bit-Stream Watermarking) olarak iki ana sınıfa ayrılmaktadır [2]. Sıkıştırılmamış Video Damgalama ile ilgili olarak Hartung ve Girod'un çalışmasını [3] ilk yapılan çalışmalardan biri olarak zikredebiliriz. Araştırmacılar çalışmalarında yayılı-izge (spread-spectrum) haberleşmesinden esinlenmişlerdir. Bir başka çalışmada ise Hsu ve Wu videonun bloklar halinde ayrık kosinüs dönüşümünden (DCT) faydalanarak damgalama işlemini gerçekleştirmişlerdir [4]. Sıkıştırılmamış video damgalama ile ilgili bir başka çalışma ise Swanson tarafından sunulmuştur [5]. Araştırmacı çalışmasında video'nun zamansal dalgalık dönüşümleri ile üretilen durağan ve dinamik zamansal bileşenlerine damgayı yerleştirmeyi önermektedir. Bu çalışmanın bir sakıncası damganın

geri elde edilmesi işleminde özgün videoya ihtiyaç duyulmasıdır.

Bu çalışmada, yapılmış önceki çalışmalardan farklı olarak bilgi gömme (iletişim amaçlı) ve damga ekleme (güvenlik amaçlı) problemleri [6] birbirlerinden ayrılarak sadece bilgi gömme üzerinde durulmuştur. Burada amacımız, şifreli video ile özgün video arasında en az bozulmayla bilginin gizlenmesini sağlayabilmektir. Böylece gizli haberleşme, dışarıdan gelebilecek harici saldırılara maruz kalmayacaktır.

Bu makalede sayısal videoların içerisine haberleşme bilgisinin gizlenebilmesi için geliştirilen yeni veri gizleme algoritmaları sunulmuştur. Gizli mesaj, taşıyıcı video ile bağlantılı değil gömülü olmalıdır.



Şekil 1. Veri gizleme (gömme) ve geri elde etme genel blok diyagramı.

Bütün veri gizleme teknikleri, gömme algoritması ve bir detektör fonksiyonundan meydana gelmektedir. Gömme algoritması haberleşme bilgisini taşıyıcı video (cover video) dosyası içerisine gömmek için kullanılır. Gömme süreci, bir anahtar kelime tarafından korunmaktadır. Bu yüzden yalnızca yetkili kişiler gizli anahtar kelime ile gömülü mesaja erişebilirler. Detektör fonksiyonunun taşıyıcı videoya uygulanması ile gizli mesaj geri elde edilir.

2. SAYISAL VIDEO ve HİSTOGRAM KAVRAMLARI

Bir sayısal video, hareketsiz sayısal görüntülerin (resimlerin) ard arda saniyede 25 veya üzerinde görüntülenmesi ile oluşmaktadır. Bu işlemin sonucunda, insan gözü resimleri hareketli bir görüntüsü olarak algılamaktadır. Sayısal videoyu oluşturan her bir resmin en küçük yapı taşları piksel hücreleri olarak isimlendirilir. Bir piksel, Kırmızı (Red), Yeşil (Green) ve Mavi (Blue) renklerinin birleşmesinden oluşmaktadır. Bu üç ana rengin belirli oranlarda karışımı ile diğer ara renkler elde edilmektedir. Her bir ana renk 8-bit (1 Bayt) olarak gösterilir. Bu durumda her bir piksel toplam 24 bite (3-Bayt) karşılık gelmektedir.

Histogram kavramı, bir resmi oluşturan piksellerin sahip oldukları renk bileşenlerinin koyuluk bilgilerine göre dağılımlarını gösteren değerler dizisidir. Histogram tipik olarak 256 elemanlı

pozitif tam sayılar dizisidir. Bir resmin histogramı alındığında sıfırdan farklı olan değerler ne kadar fazla ise o resim için çok fazla renk ve ton içerdiği söylenebilir. Eğer alınan histogramda sıfırdan farklı olan değerler ardışık olarak bir aralığa dizilmişse, o resmin neredeyse düz bir renk olduğu söylenebilir.

3. SIRÖRTME YÖNTEMİ

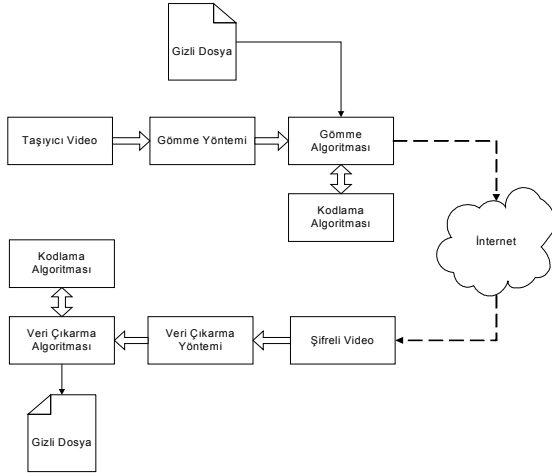
Haberleşme bilgilerinin anlamsız karakter ya da dizilerden oluşturulmasını esas alan yöntem şifrelemedir. Şifrelemedeki en büyük sorun, verilerin gözlemlenmesi sonucunda haberleşmenin şifreli olduğunun anlaşılmasıdır. Haberleşmenin de gizli olarak yapılmasının gerektiği durumlarda ise haberleşme bilgilerinin maskelenmesi yoluna gidilir. Aynı zamanda bu yöntem, sırörtme (masum nesne içerisine veri gizleme) olarak da bilinir. Bu yöntemde, şifrelemenin sakıncası olan şifreli haberleşme bilgilerinin izlenerek fark edilmesinin önüne geçilmeye çalışılır. Sırörtme yöntemleri, gizli bilgilerin masum görünümü taşıyıcılar ile gönderilmesi kurallarını kapsamaktadır. Bahsedilen taşıyıcılar resim, ses, video, metin veya diğer sayısal olarak sunulan kod veya yayımlar olabilir. Görüntü dosyaları üzerinde bilgi gizlemek için çeşitli sırörtme yöntemleri geliştirilmiştir. Bunlar üç başlık altında sınıflandırılabilir;

- ◇ En önemsiz bite ekleme (LSB)
- ◇ Maskeleye ve filtreleme
- ◇ Algoritmalar ve dönüşümler [7].

4. ÖNERİLEN VERİ GÖMME ALGORİTMALARI

Literatür çalışmalarında sayısal damgalama olarak da bilinen nesne içerisine veri gizleme ile ilgili olarak son yıllarda yapılan çalışmaların büyük çoğunluğu sadece uzay boyutundan faydalanarak yapılmış, hareketsiz görüntüler (resim) içerisine veri gizleme işini hem uzay boyutunda hem de zaman boyutunda ele almaktadır. Bu makalede, bir görüntü içerisine hem uzay boyutunda hem de zaman boyutunda veri gizlemek için yeni yöntemler önerilmektedir. Çalışmamızda; öncelikle veri gömülebilecek uygun pikseller belirlenir. Bu işlem için histogram hesaplama yöntemi kullanılmıştır. İlk önerdiğimiz yöntemde veri gömme işlemi uygun pikselleri içeren karenin tamamına yapıldığından algılanabilirliğin fazla olduğunu düşünerek, ikinci yöntemde bu sakıncayı ortadan kaldırmak için her bir karedeki uygun piksellerin bulunduğu bölgeler tespit edildikten sonra veri gömme işlemi tespit edilen bölgeler üzerinde yapılmıştır. Üçüncü ve sonuncu yöntemde ise; gizli bilgi kapasitesini daha fazla artırabilmek için her bir video karesinin histogramları birbirinden bağımsız şekilde değerlendirilerek veri gizleme işlemi yapılmıştır.

Şekil 2’ de yapılan çalışmayı gösteren bir blok diyagram görülmektedir.



Şekil 2. Geliştirilen sıvırtme yöntemlerinin blok diyagramı

4.1 HİSTOGRAMLAR YÖNTEMİ

Çalışmamızda; öncelikle içerisine veri gizlenecek görüntüyü oluşturan en küçük birimler yani kareler elde edilir. Elde edilen her bir görüntü karesinin histogram değerleri hesaplanır ve daha sonra ardışık gelen video kareleri arasındaki histogram farkları her bir renk bileşeni (R, G, B) için ayrı ayrı elde edilir. Bu işlemi takiben, bileşenlerin ortalaması alınarak ardışık gelen video karelerindeki renk ve hareket geçişlerini değerlendirme imkânı sağlayan bir değer elde edilir. Bu değerın büyük olması iki kare arasında renk ve hareket değişimlerinin fazla olduğunu, küçük olması ise sahne içeriğinin hemen hemen hiç değişmediğini ve renk değişiminin önemsiz olduğunu gösterir. Bu yaklaşım, aynı zamanda literatürde video bölümlendirme (video segmentation) olarak bilinen çalışmalarda da kullanılmaktadır [8]. Ardışık video kareleri arasındaki renk ve hareket geçişleri bir eşik değeri ile algılanır. Eşik değeri, ardışık kareler arasında bir değişim veya benzerlik algılaması için kullanılan kullanıcı tanımlı bir algılama kıstasıdır. Bu bilgiler ışığında ardışık video karelerinin histogram farkları eşik değeri ile kıyaslanarak veri gizlenecek pikseller belirlenir. Eşik değerinin üzerinde kalan bileşenler seçilirse, ardışık video karelerinin renk bakımından karışık bir yapıya sahip olduğu anlaşılır ki buna farklı histogramlar yöntemi adı verilmiştir. Eşik değerinin altında kalan bileşenlerin seçilmesi durumunda ise ardışık video karelerinin renk bakımından tekdüze olduğu anlaşılır ki buna da benzer histogramlar yöntemi adı verilmiştir.

Veri gömmeye uygun pikseller iki farklı yöntemle belirlenir;

I. Blok tabanlı yöntemde öncelikle video kareleri uygun matematiksel ifadelerle bloklara bölünür.

Ardışık video karelerinde birbirlerine karşılık gelen blokların histogram değerlerinin karşılaştırılması ile veri gömülebilecek uygun pikselleri içeren bloklar belirlenir.

II. Kare tabanlı yöntemde ise ardışık video kareleri bir bütün olarak değerlendirilir. Sahne içeriğinin tümünün değiştiği veya değişmediği (kullanılan veri gömme yöntemine göre) ardışık video karelerinin tamamına veri gömme yapılır.

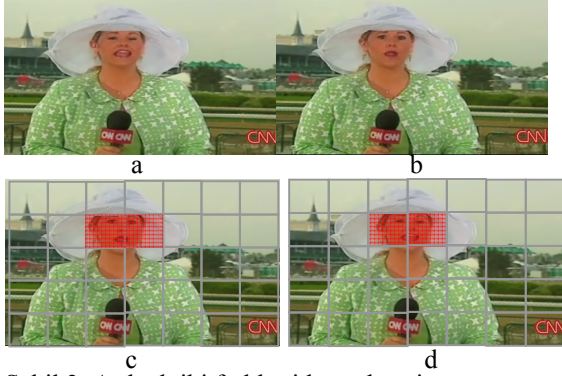
4.1.1 FARKLI HİSTOGRAMLAR YÖNTEMİ

Farklı histogramlar yöntemi ile hedeflenen; video kareleri arasındaki uzamsal algılanabilirliğin önlenmesinin yanında, literatürde titreşim sorunu olarak da bilinen zamansal algılanabilirlik sorununa da bir çözüm getirmektir. Bu yöntemde, ardışık video kareleri arasındaki insan görme sisteminin (İGS) algılayamadığı renk ve hareket geçişlerinin belirlenerek veri gömmeye kullanılmaları sağlanmaktadır. Ardışık video kareleri arasındaki geçiş anları veya video karesinin içerisindeki hareket geçiş noktaları veri gömmeye kullanılan alanlardır. Örneğin bir haber programında kare tabanlı farklı histogram yöntemi kullanılırsa, Şekil 3.a ve 3.b’de görüldüğü gibi değişik histogram değerlerine sahip ardışık her bir haber sahnesine veri gömülecektir. Şekillerde görüldüğü gibi gerçekte histogram değişimleri sunucunun yüz bölgesindeki hareketlerden kaynaklanmaktadır. Örnek video için bu yöntemin kullanılmasının bir sakınca doğuracağı açıktır. Bu örnek için blok tabanlı farklı histogram yönteminin (Şekil 3.c ve 3.d) kullanılmasıyla hareket ve renk anlamında değişim olan sunucunun yüz bölgesi ve ellerinin bulunduğu (kırmızı bölgeler) bölgelere veri gömülerek bir önceki yöntemde söz konusu olan sakınca ortadan kaldırılır. Böylelikle uzamsal ve zamansal boyutta gizli bilginin İGS tarafından algılanması önlenmiş olur.

4.1.2 BENZER HİSTOGRAMLAR YÖNTEMİ

Benzer histogramlar yönteminde video içerisindeki ardışık video karelerinin renk ve hareket bakımından değişmeyen bölgelerine veri gizlemenin yapılması önerilmektedir. Örneğin karelerde renk ve hareket bakımından değişmeyen bir arka plana sahip videolar veri gizleme için daha uygundur. Bu yöntemin kullanılması ile veri gizleme kapasitesi artırılmış buna karşın güvenlik seviyesi ise indirgenmiş olur. Bunun sebebi, sabit veya durağan bölgelerdeki renk değişimlerinin İGS tarafından daha rahat algılanabilmesidir. Örneğin blok tabanlı benzer histogramlar yöntemi kullanılarak Şekil 3’de

verilen örnek videoda veri gömülecek bölgeler sunucunun arkasında kalan hareketsiz alan olacaktır.



Şekil 3. Ardışık iki farklı video sahnesi.

4.2 BÖLGESEL HİSTOGRAMLAR OPTİMİZASYONU

Video karelerine yapılan veri gömme işlemi renk bakımından düz olan bölgelere yapıldığında uzamsal ve zamansal algılanabilirlik artmaktadır. Bu problemi ortadan kaldırmak amacıyla geliştirilen bölgesel histogram optimizasyonu yönteminde ardışık video kareleri matematiksel ifadelerle belirlenen uygun bloklara bölünür. Blokların renk içerikleri hakkında bilgi sahibi olabilmek için her bir blok histogram değeri incelenir. Blok histogram dağılımı bir eşik değerinin altındaysa blok içinde farklı renkler olmadığı düz renk ihtiva ettiği ve veri gömme için uygun olmadığı anlaşılır. Blok histogram dağılımının eşik değerinin üzerinde olması durumunda ise blok içerisinde farklı renklerin olduğu ve veri gömme için uygun olduğu anlamına gelir. Örneğin düz bir renge sahip zemin önünde bir nesne bulunan video karesinde veri gömme işlemi, nesnenin kenarlarının bulunduğu ve nesne üzerindeki renk dağılımlarının yoğun olduğu bölgelere yapılır. Bu yöntemi önerdiğimiz diğer yöntemlerimizden ayıran en önemli özellik; veri gömülecek alanlar ardışık video karelerinin birbirleriyle değil, video karelerindeki blokların birbirleriyle değerlendirilmesi sonucunda bulunmasıdır. Böylece bu farklılık, videoda algılanabilirliği arttıracak gereksiz piksel bozulmalarını önlemektedir.

5. ÖNERİLEN VERİ GÖMME KODLAMA TEKNİĞİ

Görüntüde enaz bozulma ile beraber en fazla veri gizleme, sırtörme yöntemlerinde aranan en temel kıstaslardandır. İstenilen bu kıstasları sağlamak amacıyla RGB ağırlıklı kodlama tekniği geliştirilmiştir [9].

RGB: (89,143,240) olarak üç ana renk dağılımına sahip olan bir pikselin R=89, G=143, B=240

ağırlıklarına sahip olduğu söylenebilir. RGB ağırlıklarına sahip bu pikselin içerisine “s” harfinin ASCII karşılığı olan “115” sayısının gömülme işlemi şu şekilde olacaktır; öncelikle RGB değerinin son rakamları sıfırlanır. Buna göre elimizde R=80, G=140, B=240 değerleri olur. Bir sonraki aşamada “s” karakterinin ASCII karşılığı her basamak değeri 10 sayısından çıkarılır (10-1=9, 10-1=9, 10-5=5). Elde edilen rakamlar her bir RGB değerlerinin son basamaklarına yerleştirilir. Son durumda ise elimizde R=89, G=149, B=245 olan bir RGB değeri bulunur. Gizli bilginin elde edilmesi aşamasında ise; pikselin sahip olduğu RGB değerinin son rakamları alınır (9, 9, 5). Bu rakamlar 10 sayısından (10-9=1, 10-9=1, 10-5=5) çıkarılarak tekrar “s” harfinin ASCII kodları elde edilmiş olur.

6. DENEYSEL SONUÇLAR

Önerdiğimiz yöntemin deneysel sonuçlarına bakıldığında getirdiği üstünlükler daha iyi görülmektedir. Tablo 1 ve Tablo 2’de elde edilen sonuçlar için taşıyıcı video dosyası olarak “Foreman.avi”, “Miss.avi” ve “Vipmen.avi”; gizli dosya olarak da kendi oluşturduğumuz “hello.rar” isimli sıkıştırılmış dosya kullanılmıştır. Önerilen yöntemde gizli dosya olarak “rar”, “jpg”, “doc”, “xls”, “txt” uzantılı dosyalar kullanmak mümkündür. Günümüzde en iyi dosya sıkıştırma formatlarından biri olarak kabul edilen “rar” sıkıştırma formatını kullanarak gizli bilginin maksimum şekilde sıkıştırılabilmesine imkân verilebilmektedir. Ayrıca “rar” sıkıştırma formatının sıkıştırma esnasında dosyaların şifrelenmesine imkân vermesi de güvenlik için büyük bir avantaj olarak göz önüne alınmalıdır.

Tablo 1’de verilen PSNR değerlerine bakıldığında her bir örnek video için özellikle 2. karelerde önerdiğimiz yöntemin üstünlüğü fark edilmektedir. Tablo 2’de görülen değerlerden ise, önerilen yöntemdeki piksel bozulması var olan yöntemdeki piksel bozulmasının yaklaşık olarak sadece %37’si kadardır. Diğer bir deyişle, önerilen yöntemle bozulması önlenmiş piksel sayısı 122’dir. Bu sonuç doğal olarak doğrudan algılanabilirliği etkilemektedir.

Tablo 1. Veri gömülen video karelerinin algılanabilirlik değerleri.

Taşıyıcı Video (avi)	PSNR (db)			
	LSB kodlama		RGB kodlama	
	1. Kare	2. Kare	1. Kare	2. Kare
Foreman	69.714	61.035	69.616	61.035
Miss	67.698	58.178	67.692	61.035
Vipmen	67.968	58.178	67.968	61.035

Tablo 2. Taşıyıcı video da bozulan piksel sayıları.

Gizli Dosya Boyutu	Değişen Piksel Sayısı	
	LSB kodlama	RGB kodlama
584 bit – (73 bayt)	195 piksel	73 piksel

7. SONUÇLAR

Bu makalede sunulan araştırmanın amacı, internet gibi güvenli olmayan ortamlarda güvenli haberleşme sağlayabilmek, haberleşme bilgilerinin veya verilerinin korunması için yeni birtakım veri gizleme tekniklerini ortaya koymak ve gerçekleştirmektir.

Araştırmada gizli bilginin video karelerinin veri gömmeye uygun pikselleri içerisine yerleştirilmesinde daha önceden yapılmış benzer çalışmalarda rastlanılmayan histogramlar yöntemi kullanılmıştır.

Bu çalışmada sunulan yöntemleri literatürdeki çalışmalardan ayıran en önemli özellik, video karesinin tümü yerine veri gömülebilecek uygun bölgelerin ve piksellerin belirlenerek gömme işleminin gerçekleştirilmesidir. Video karelerinin bloklara ayrılarak gerçekleştirilen veri gömme işlemi bölgesel histogram optimizasyonu, blok tabanlı farklı histogramlar ve blok tabanlı benzer histogramlar yöntemlerinde kullanılmaktadır. Bu yöntemlerde video içerisindeki en uygun alanlara gömme yapılı ve böylece algılanabilirlik daha da zayıflatılmış olur.

Geliştirilen yöntemlerden benzer histogramlar yöntemi yüksek gizli bilgi kapasitesi sunmasına karşın düşük güvenlik seviyesine sahiptir. Gizli bilgi kapasitenin düşük, güvenliğin yüksek olduğu durum ise farklı histogramlar yöntemiyle elde edilebilmektedir.

Ayrıca araştırmamızda yeni bir RGB ağırlıklı kodlama tekniği üzerinde durulmuştur. Bu kodlama tekniği ile video görüntüsünde enaz bozulma hedeflenerek gizli bilgi kapasitesi artırılmaya çalışılmıştır.

KAYNAKLAR

- [1] Alper Koz, Aydın Alatan, “Oblivious Video Watermarking Using Temporal Sensitivity of HVS”, Proceedings of the 2005 International Conference on Image Processing (ICIP 2005), Genoa, Italy, September 11-14, 2005, IEEE.
- [2] M.Barni, F. Bartolini, N. Checcacci, “Watermarking of MPEG-4 Video Objects”, IEEE Transactions On Multimedia, Vol. 7, No. 1, February 2005.
- [3] F. Hartung and B. Girod, “Digital watermarking of raw and compressed video,” in Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication, Berlin, Germany, Oct. 1996, pp. 205–213.

[4] C. Hsu and J. Wu, “Digital watermarking for video,” in Proc. IEEE Int. Conf. Digital Signal Processing, vol. 1, Jul. 1997, pp. 217–220.

[5] M. D. Swanson, B. Zhu, and A. H. Tewfik, “Multiresolution scene-based video watermarking using perceptual models,” IEEE J. Select. Areas Commun., vol. 16, pp. 540–550, May 1998.

[6] M. Kıvınc Mıhçak, “Watermarking via Optimization Algorithms for Quantizing Randomized Image Characteristics”, Microsoft Research, Cryptography and Anti-Piracy Group WA, USA.

[7] Sellars D., “An Introduction to Steganography”, Student Papers, 1999.

<http://cs.uct.ac.za/courses/CS400/NIS04/papers99/dsellars>.

[8] I.Koprinska and S.Carrato, “Temporal Video Segmentation: A Survey Signal Processing Image Communication”, Elsevier Science, 2001.

[9] Feyzi Akar, H. Selçuk Varol, “A New RGB Weighted Encoding Technique for Efficient Information Hiding in Images” Journal of Naval Science and Engineering Number 2 Volume 2 July 2004.