

Sıkıştırılmış Videolarda Bilgi Saklama İçin Nicemleme Dizin Modülasyonu ile Yasak Bölgesi Bilgi Saklamasının Karşılaştırılması

Comparison of Quantization Index Modulation and Forbidden Zone Data Hiding for Compressed Domain Video Data Hiding

Ersin Esen^{1,2}, Zafer Doğan¹, Tuğrul K. Ateş^{1,2}, A. Aydın Alatan¹

1. O.D.T.Ü. Elektrik ve Elektronik Mühendisliği Bölümü
e152040@metu.edu.tr, alatan@eee.metu.edu.tr

2. TÜBİTAK UZAY

{ersin.esen, tugrul.ates}@uzay.tubitak.gov.tr

Özetçe

Bilgi saklama, değişik uygulamalar ile günlük hayatımıza girmiştir. Biz de bu çalışmamızda iki farklı bilgi saklama yöntemini, Nicemleme Dizin Modülasyonu ve Yasak Bölgesi Bilgi Saklama, videolara uyarlıyoruz. Genel bir video bilgi saklama çerçevesi içinde iki yöntemin sıkıştırma saldırısına karşı başarımlarını karşılaştırıyoruz. Tipik televizyon verileri ile yapılan deneylerde YBBS'nin özellikle kuvvetli saldırılarda daha iyi sonuç verdiği gözlenmiştir.

Abstract

Data hiding is now a part of daily life through various applications. In this work, we apply two data hiding methods, Quantization Index Modulation and Forbidden Zone Data Hiding, to video applications. We place these methods into a general video data hiding scheme and compare their performance against compression attacks. The results of the experiments with typical TV content indicate the superiority of FZDH, specifically for powerful attacks.

1. Giriş

Bilgi saklama; görünmez damgalama, parmak izi takibi, kopya bulma, kimlik doğrulama ve gizli iletişim gibi pek çok farklı uygulamaları içeren geniş ve son yıllarda ticari ürünler aracılığıyla günlük hayatta yer bulmaya başlayan bir alandır. Uygulama tarzına göre sistem isterleri farklılık gösterse de yapılan işlem temel olarak bilgiyi bir konakçı sinyalin içine algılanamayacak şekilde gömmektir. Konakçı sinyal olarak ses, imge, video, metin olmak üzere farklı sinyal türleri kullanılabilir.

Problem formülasyonu ve çözüm önerilerinde belli bir olgunluğa ulaşılmışsa da ideal limitlere ulaşmayı hedefleyen pratik yöntemler, konakçı sinyaline göre algısal uyarlamalar, güvenlik vb. konularda halen etkin araştırmalar devam etmektedir. Video bilgi saklama konusunda da konakçı sinyalin türünden kaynaklanan ek problemlerin çözümüne yönelik çalışmalar devam etmektedir.

Video bilgi saklama çalışmalarının ilklerinden biri Cox'un [1] yayılı dizge yöntemini video alanına uyarlayan [2]'dur. Bu yöntemde, rasgele bir anahtara bağlı ve

spektrumun tamamına yayılan damga dizisi oluşturulur. Rasgele damga dizisi belirli bir kodlamaya uygun olarak değişik miktarlarda kaydırılır ve toplanarak uzamsal alanda video karesinin ışıklılık kanalına eklenir. Alıcı tarafında Ayrık Fourier Dönüşüm ile hesaplanan ilintinin dorukları arasında bağıntıya göre saklanan bilgi çıkarılır.

Yayıllı dizge yöntemlerinin karşısında nicemleyici tabanlı yöntemlerden bahsedilebilir. Chen [5] tarafından önerilen Nicemleme Dizin Modülasyonu (NDM) çerçevesine göre çeşitli nicemleme tabanlı yöntemler [3, 4] bulunmaktadır. Bu ve benzeri çalışmalarda genel olarak yapılan dönüşüm, katsayılarının NDM kullanılarak nicemlenmesidir. Nicemleme tabanlı yöntemlerinin yayılı izge yöntemlerine göre çeşitli saldırılara karşı gürbüzlüğünün az olmasına rağmen, bilgi saklama kapasitesinin daha yüksek olduğu söylenebilir.

Biz bu çalışmamızda, tipik bir video bilgi saklama altyapısı içerisinde iki farklı bilgi saklama yönteminin sıkıştırma saldırısı karşısındaki başarımlarını karşılaştırıyoruz. İkinci bölümde karşılaştırılan yöntemler kısaca anlatılmaktadır. Video bilgi saklama yöntemi ise üçüncü bölümde verilmektedir. Ardından deneyler ve sonuçlar gelmektedir.

2. Karşılaştırılan Bilgi Saklama Yöntemleri

Bilgi saklama probleminin tanımında s konakçı sinyali, x taşıyıcı sinyali, y alıcıdaki sinyali, m saklanan bilgi bitini temsil etsin. Bu tanımlar doğrultusunda karşılaştırılan iki yöntem aşağıdaki bölümlerde anlatılmaktadır.

2.1. Nicemleme Dizin Modülasyonu (NDM)

Chen [5] tarafından önerilen NDM, nicemleme tabanlı bilgi saklama yöntemlerinin temelini oluşturur. Bu yöntemde, ilk olarak bir nicemleyici kümesi belirlenir ve her bir nicemleyici ile bilgi bitleri arasında ilinti kurulur. Bilgi saklama esasında, konakçı sinyali saklanacak bilgi bitine göre kullanılması gereken nicemleyici ile nicemlenir. Alıcı tarafında, bütün nicemleyiciler tek tek denenir ve en yakın gericiatma noktasma sahip nicemleyicide karar kılınır.

NDM'nin en basit şekli olan Kırpırtı Modülasyonu [5] yönteminin saklayıcı fonksiyonu (1)'deki gibidir.

$$x(s, m) = Q(s + d(m)) - d(m) \quad (1)$$

Burada $Q(\cdot)$, Δ hücre genişliğine sahip birörnek nicemleyiciyi; $d(m)$ bilgi biti ile ilintilendirilmiş kırırtı fonksiyonunu temsil eder. Kırırtı fonksiyonu olarak iki bit saklanacak ise $\pm\Delta/4$ değerleri seçilebilir. Ayrıca, güvenliği artırmak için bu değerler rasgele de seçilebilir. Bunun için $d(0)$, $[-\Delta/2, \Delta/2]$ aralığında rasgele seçilir; $d(1)$ için aynı aralık içine düşen $\Delta/2$ uzaklıktaki nokta alınır.

Alıcı tarafında minimum uzaklık kodçözücüsü (2) kullanılır.

$$\hat{m} = \arg \min_m \|y - (Q(y + d(m)) - d(m))\| \quad (2)$$

2.2. Yasak Bölge Bilgi Saklama (YBBS)

[6]'da önerdiğimiz YBBS, Yasak Bölge (YB) kavramına dayanmaktadır. YB, konakçı sinyalinin değiştirilmeyecek kısmını temsil etmektedir. Saklama işlemi konakçı sinyalinin geri kalan dayanağında gerçekleştirilir. Bunun için nicemleyeciler de kullanılabilir; bu durumda YBBS bir özel durumu olarak NDM'yi de içerir [6].

YBBS'nin tek bir kontrol değişkeni ve nicemleyici kullanılan sürümünün saklama fonksiyonu (3)'te verilmektedir.

$$x = \begin{cases} s, & YB \\ s + e(1 - \frac{r}{|e|}), & IB \end{cases} \quad (3)$$

$$= \begin{cases} s, & YB \\ \frac{r}{|e|}s + (1 - \frac{r}{|e|})Q_m(s), & IB \end{cases}$$

burada

$$e = Q_m(s) - s$$

$$YB = \{s \mid |e| \leq r\} \quad (4)$$

$$IB = \{s \mid |e| > r\}$$

Çıkarıcı fonksiyonu olarak, NDM'deki gibi minimum uzaklık kodçözücüsü kullanılır (5).

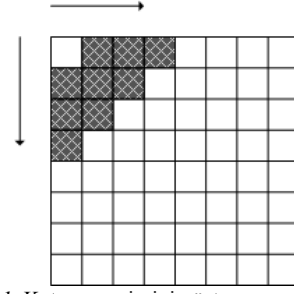
$$\hat{m} = \arg \min_m \|y - y_m\|, \quad (5)$$

Burada y_m , m mesaj biti ile y 'ye (3)'ün uygulanması ile elde edilir.

YBBS'deki temel yaklaşım, konakçı sinyalinin hiç değiştirilmediği YB'yi bir kontrol değişkeni aracılığıyla ayarlayarak istenen gürbüzlük derecesine ulaşmaktır. Bu şekilde saklama bozunumu ve gürbüzlük arasındaki denge tek bir değişkenle kurulur.

3. Video Bilgi Saklama Yöntemi

Videolara bilgi saklamadaki temel yaklaşımımız dönüşüm uzayında seçilen katsayılara ikinci bölümde anlatılan yöntemleri uygulamaktır. Dönüşüm olarak sıkıştırma standartlarında genellikle kullanılan Ayrık Kosinüs Dönüşümü'nü (AKD) kullanıyoruz. Katsayı seçiminde [7]'deki gibi enerji eşikleme gerçekleştirilmektedir.



Şekil 1: Katsayı seçimini gösteren maske.

Yöntemin bilgi saklama aşamasının akış diyagramı Şekil 2'de verilmektedir. Gürbüzlük açısından videonun sadece ışıklılık kanalı işlenmektedir. Her kare, 8×8 'lik örtüşmeyen bloklar halinde ele alınır. İlk olarak, blok AKD'den geçirilerek dönüşüm katsayıları elde edilir. 8×8 'lik dönüşüm katsayılarından Şekil 1'de gösterildiği gibi bir maske (M) içinde tanımlı olan katsayılar enerji denetiminden geçirilir. Bunun için blok ortalama enerjisi ve tek başına katsayı enerjisi, sırasıyla T_1 ve T_2 eşik değerleriyle test edilir. T_1 'i geçen bloklarda T_2 'den büyük enerjili katsayılar bilgi saklama işlemine tabi tutulur. Değiştirilen katsayılar ile ters AKD alınır ve ilgili bloğun ışıklılık kanalındaki veriler yenileri ile değiştirilir. Bu işlem videonun her karesi için gerçekleştirilir. Kareler video kodlayıcısına gönderilir ve belirlenen sıkıştırma hızında bilgi saklı video oluşturulur.

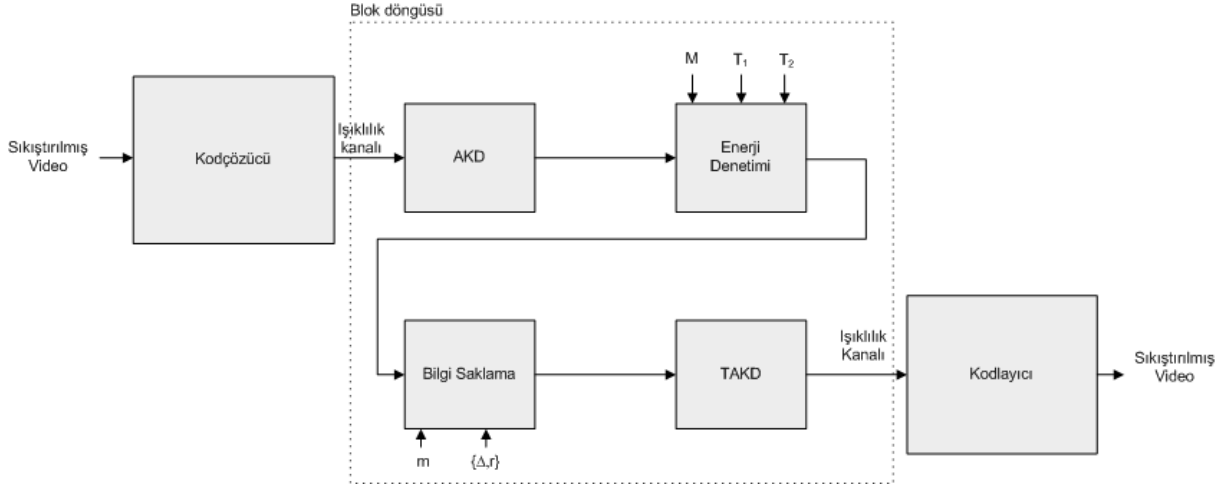
Bilgi çıkarma aşamasında, saklama işleminin simetrisi gerçekleştirilir. Çıkarıcı, saklayıcının değişkenlerini kullanılmalıdır. Bunlar, blok boyutu, M , T_1 , T_2 ve bilgi saklama yöntemine özgü (NDM için Δ , YBBS için Δ ve r) değişkenlerdir. Bilgi çıkarma işleminin akış diyagramı Şekil 3'te verilmektedir. Her karenin ışıklılık kanalı 8×8 'lik bloklar halinde incelenir. AKD katsayıları enerji denetiminden geçirilerek saklama işleminde kullanılmış katsayılar tahmin edilir. Enerji denetiminden geçen katsayılar, ikinci bölümde anlatılan yöntemlerin çıkarıcılarına sokularak saklı bit tahmin edilmektedir.

Bilgi saklama ve saldırılar sebebiyle tam olarak aynı katsayılar tespit edilemeyebilir. Bu yüzden [7]'deki gibi hata düzeltme kodları kullanılabilir. Fakat bu çalışmadaki hedefimiz iki yöntemin başarımını karşılaştırmak olduğundan hata düzeltme kodları olmaksızın bu karşılaştırmayı gerçekleştiriyoruz. Bu amaçla, senkronizasyon problemini aşmak için tüm kareye aynı bilgi bitini saklıyoruz.

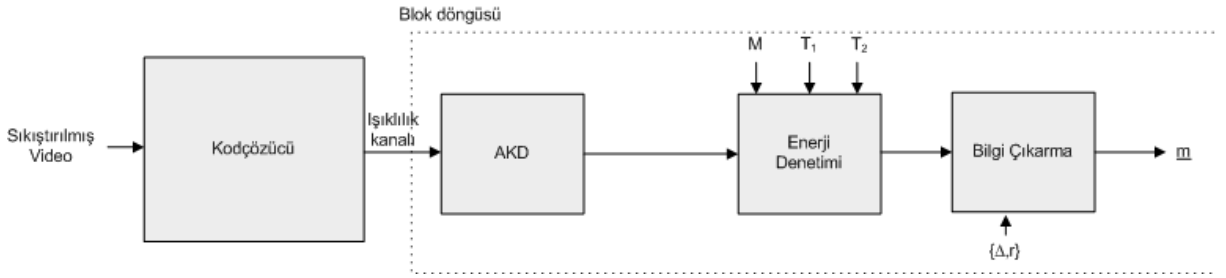
4. Deneyler

YBBS ve NDM'nin sıkıştırma saldırısına karşı başarımları değişik sıkıştırma oranlarında elde edilen bit hataları üzerinden karşılaştırılmaktadır. Bilgi bitleri için hata düzeltme kodları kullanılmaksızın iki yöntemin ham başarımı ölçülmüştür.

Deneylerde sayısal uydu yayınından alınan beş farklı kanaldan değişik program türlerinde toplam bir saatlik MPEG-2 video kümesi kullanılmıştır. Karşılaştırma, her iki yöntemin saklama bozunumunun aynı olduğu değişkenler kullanılarak gerçekleştirilmiştir. Bilgi saklama işleminden sonra elde edilen videolar tekrar MPEG-2 kodlanmıştır. 1Mbps ile 6Mbps arasındaki sıkıştırma oranlarında kodlanan



Şekil 2: Saklayıcı akış diyagramı.



Şekil 3: Çıkarıcı akış diyagramı.

videolardaki saklı bilgi çıkarılarak bit hata oranı ölçülmüştür.

İki farklı saklama bozunumu (kare başına 48 dB ve 51 dB PSNR) için elde edilen sonuçlar Şekil 5'te Intra ve Intra olmayan kareler için ayrı ayrı verilmektedir. 48 dB saklama bozunumu için NDM'de Δ , 30 olarak alınmıştır. YBBS ile aynı saklama bozunumunu verecek farklı $\{\Delta, r\}$ çiftleri olsa da tipik değerler olarak $\{40, 4\}$ alınmıştır. 51 dB saklama bozunumu içinse NDM ve YBBS için sırasıyla $\{15\}$ ve $\{20, 2\}$ değerleri kullanılmıştır. T_1 ve T_2 eşik değerleri için sırasıyla 2000 ve 1000 kullanılmıştır. Katsayı maskesi M , DC hariç zikzak taramadaki ilk dokuz katsayının seçimiyle oluşturulmuştur. YBBS ile elde edilmiş örnek bir sonuç çifti $\{40, 4\}$ çifti ve dört Mbps MPEG-2 sıkıştırma ile) Şekil 4'te gösterilmektedir.

Çift işlemcili (AMD Opteron 248) 2GB RAM'e sahip SUSE 10.0 bir sistemde saklama işlemi video kodçözüme ve yeniden sıkıştırma ile birlikte gerçek zamanın 1,3 katı, çıkarma işlemi ise video kodçözücü ile birlikte 0,6 katı sürede gerçekleşmiştir.

Sonuçlar incelendiğinde düşük sıkıştırma oranları ve düşük saklama bozunumları için YBBS'nin NDM'ye göre daha iyi başarıma sahip olduğu görülmektedir. Bu koşullar düşük WNR (Damga-gürültü oranı) değerlerine karşılık gelmektedir ve [6]'da Gauss kanal gürültüsü için verilen sonuçlarla benzerlik göstermektedir. Intra ve Intra olmayan kareler için sonuçlar yöntem bazında aynı karakteristiğe sahiptir. Fakat, Intra karelerdeki hata oranının diğer duruma göre daha düşük olduğu görülmektedir.

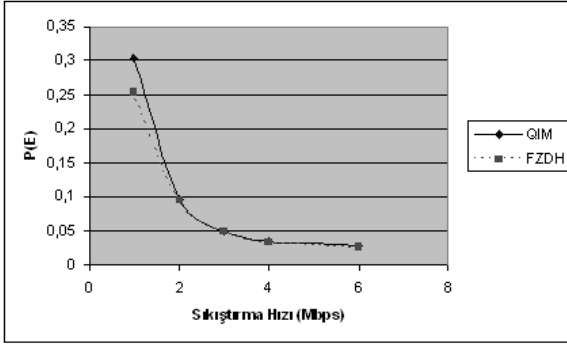


Şekil 4: Konakçı kare (sol) ve YBBS ile elde edilen kare (sağ).

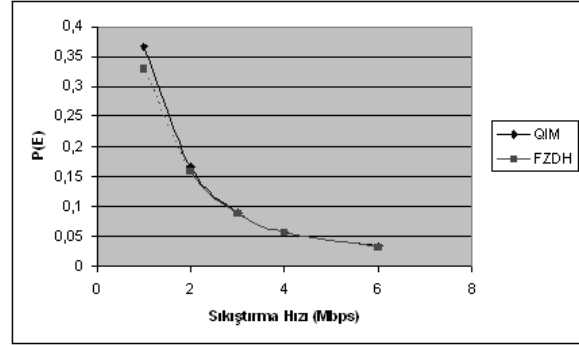
5. Sonuçlar

Farklı iki bilgi saklama yöntemi, NDM ve YBBS, video bilgi saklama uygulamasında kullanılmış ve sıkıştırma saldırısına karşı başarımları karşılaştırılmıştır. Deneyler sonucunda YBBS'nin NDM'den daha iyi sonuç verdiği gözlemlenmiştir. Özellikle düşük WNR değerlerinde bu üstünlük daha belirgin olmaktadır.

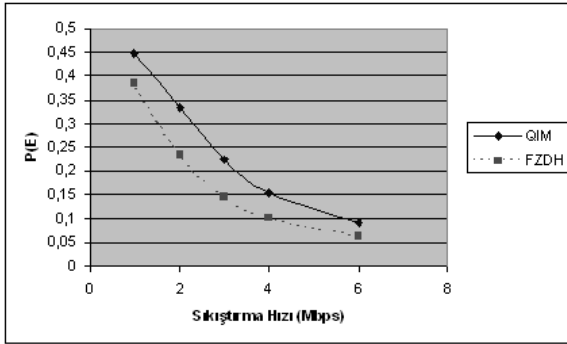
Bundan sonra ilk olarak farklı saldırılar için karşılaştırmalar gerçekleştirilecektir. Daha sonra ise senkronizasyon problemine karşı hata düzeltme kodlarının eklenmesi [7] ve yöntem değişkenlerinin insan görme sistemine göre uyarlanı hale getirilmesi yönünde [8, 9] çalışmalar hedeflenmektedir.



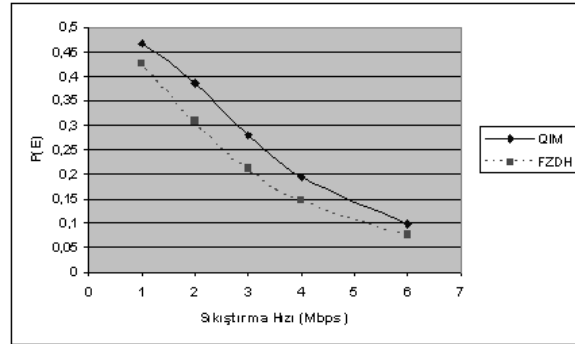
(a)



(b)



(c)



(d)

Şekil 5: YBBS ve NDM başarımları. (a) Intra kareler, 48 dB saklama bozunumu (b) Intra olmayan kareler, 48 dB saklama bozunumu (c) Intra kareler, 51 dB saklama bozunumu (d) Intra olmayan kareler, 51 dB saklama bozunumu

6. Kaynakça

- [1] I. Cox, J. Kilian, F. Leighton, ve T. Shamon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing* 6, pp. 1673 — 1687, Dec. 1997.
- [2] Ton Kalker, Geert Depovere, Jaap Haitzma, ve Maurice J. Maes, "Video watermarking system for broadcast monitoring," *Proc. SPIE*, 1999, 3657, 103.
- [3] Sarkar, A. Madhow, U. Chandrasekaran, S. Manjunath, B. S., "Adaptive MPEG-2 video data hiding scheme," *Proc. SPIE*, 2007, VOL 6505.
- [4] Min Wu; Yu, H.; Bede Liu, "Data hiding in image and video .II. Designs and applications," *Image Processing, IEEE Transactions on*, vol.12, no.6, pp. 696-705, June 2003.
- [5] B. Chen ve G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Trans. Inform. Theory*, vol. 47, no.4, pp.1423-1443, May 2001.
- [6] E. Esen ve A. A. Alatan, "Forbidden Zone Data Hiding", *IEEE ICIP*, 2006, 8-11 October 2006, Atlanta, GA, USA.
- [7] Solanki, K.; Jacobsen, N.; Madhow, U.; Manjunath, B.S.; Chandrasekaran, S., "Robust image-adaptive data hiding using erasure and error correction," *Image Processing, IEEE Transactions on*, vol.13, no.12, pp.1627-1639, Dec. 2004.
- [8] Job C. Oostveen, Ton Kalker, ve Marius Staring, "Adaptive quantization watermarking," *Proc. SPIE*, 2004, 5306, 296
- [9] H Qi, D Zheng, J Zhao, "Human visual system based adaptive digital image watermarking," *Signal Processing Volume 88*, Issue 1, January 2008, Pages 174-188.