MPEG2 UYUMLU SAYISAL TV ŞİFRELEME YÖNTEMİ

Doç.Dr.Melih Pazarcı[1], Vadi Dipçin[2]
[1]İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi
80626 Maslak, İstanbul, eepazarc@ehb.itu.edu.tr
[2]Turkcell İletişim Hizmetleri A.Ş. Turkcell Plaza Meşrutiyet Cad. No:153
80050 Tepebaşı, İstanbul, vadi.dipcin@turkcell.com.tr

Özet

Ücretli sayısal TV uygulamalarında içeriğe erişimin kısıtlanması ve denetimi için kullanılan mevcut şifreleme yöntemleri, MPEG bit dizisinin şifrelenmesine dayanmaktadır. Analog uygulamalarda kullanılan ve görüntünün içeriğini bozan yöntemlerle MPEG ile verimli bir kodlama sağlanamamaktadır. Oysa görüntünün bozulmasını sağlayan bir algoritma, hem içeriğe kısıtlı erişimi sağlayarak hizmete özendirici rol oynayabilecek hem de ek bir güvenlik katmanı oluşturacaktır. Bu çalışmada MPEG'in kodlama prensipleri göz önünde bulundurularak görüntünün bozulmasına dayanan bir şifreli TV sistemi tasarlanmıştır. İmge içi ve imgeler arası benzerlikler MPEG'in kısıtları dikkate alınarak bozulmuş ve içeriğin serbestçe izlenmesi engellenmiştir. Burada en önemli hedef, yöntemin tamamen MPEG uyumlu olması, diğer tüm yayın parametrelerinden (yayın ortamı, modülasyon vb.) bağımsız olması ve bu nedenle şifre çözümü için gerekli bilgiyi de video dizisinin kendi içinde taşımasıdır. Bu makalenin kapsamı, MPEG uyumlu bu tür bir algoritmanın tanımlanması ve çalıştırılabileceğinin gösterilmesi ile sınırlıdır.

Anahtar kelimeler: mpeg, video, şifreleme

1 Giriş

Günümüzde hızla büyüyen bir pazara hitap eden sayısal TV yayıncılığı, ağırlıklı olarak şifreli yayın modeli üzerine kurulmuştur. Böylece hem ayrıcalı içerik olarak kabul edilen değerli içerik ürünleri bir bedel karşılığında pazarlanmakta, hem de sayısal ortamda kayıpsız kopyalanma işlemine karşı korunma sağlanmaktadır. Bu nedenle, içeriğe serbest erişimi engelleyen Koşullu Erişim (Conditional Access) sistemleri kullanılmaktadır. Bu sistemler içeriğe ait verinin şifrelenmesi, müşteri veritabanının yönetilmesi, İzle ve Öde (Pay Per View) türü servislerin verilmesi ve faturalama gibi işlevleri yerine getirirler.

Koşullu erişimin vaz geçilmez öğesi ise şifrelemedir. Çünkü içeriğe istenmeyen kişilerin erişiminin engellenmesini mümkün kılan teknoloji odur. Analog TV yayınlarında iki çeşit şifreleme yöntemi kullanılmaktaydı:

- Analog işaretin yapısını bozan yöntemler
- Resim içeriğini bozan yöntemler

Sayısal ortamda ise yaygın olan, MPEG kodlanmış haldeki bit dizisinin şifrelenmesidir [1]. Böylece şifreli bitleri alan herhangi bir MPEG kod çözücü bu bilgiyi kullanarak resim ve ses bilgisini elde edemeyecektir. Analog yayınlar için kullanılan resim içeriğinin bozulması türü yöntemler ise MPEG ile verimli kodlanması mümkün olmayan imgeler yarattığından sayısal yayınlarda kullanılmaya uygun değildir. Örneğin Nagravision'a [2] ait "Satır Karıştırma"ya dayanan yöntemde video dizisine ait her karedeki imgenin satırlarının yeri rasgele bir yöntemle yer değiştirir. Bu durumda hem resim içi ilişkiler hem de resimler arası ilişkiler tamamen bozulduğundan şifreleme uygulanınca MPEG ile verimli kodlanamaz bir video dizisi üretilir.

Bu çalışmanın amacı, rasgele değişimlere dayanan ve görsel bozulma sağlayan ama aynı zamanda MPEG ile kodlanabilir, işlem ve bellek gereksinimi düşük, ve hızlı bir algoritma oluşturmaktır. Makalede önce bu özellikleri gerektiren koşullar anlatılmakta, ardından algoritmanın tanımı yapılmakta ve sonuçlar değerlendirilmektedir.

2 Kısıtlar

İstenen türde bir algoritmanın oluşturulabilmesi için gerekli şartlar iki başlık altında ele alınabilir:

Algoritmanın sağlaması gereken işlevsel kısıtlar:

- Gerçek zamanda ucuz maliyetle uygulanabilme (düşük işlem yükü ve bellek geresinimi)
- Rasgele ve sürekli değişen parametrelerin kullanılması (güvenlik nedeniyle)
- Şifrelenen imgelerin MPEG ile kodlandıklarında farkedilir bir kalite kaybı veya bit hızı artışına neden olmaması
- Şifre çözümü için gerekli bilginin imge içinde taşınması
- İstenen bozulma seviyesinde görüntü elde edilmesi

MPEG ile verimli kodlanabilme kısıtları:

- İmge içi ilişkilerin mümkün olduğunca az bozulması
- İmgeler arası ilişkilerin mümkün olduğunca az bozulması.

Belirlenmesi gereken bir diğer konu da şifreleme işleminin hangi renk uzayında gerçekleştirileceğidir. Üç Renk teorisi [3] uyarınca, tanımlanan tüm sistemler 3 bileşenlidir. Çalışma için göz önünde bulundurulup incelenmiş olan 3 adet renk uzayı bulunmaktadır:

- **RGB Uzayı:** Kırmızı, Mavi, Yeşil renklerden oluşan toplamsal küme
- **YCrCb Uzayı:** [4,5]: JPEG ve MPEG'de kullanılan, parlaklık ve iki renk bileşenine dayanan küme
- **HSI Uzayı:** [6] H(renk), S(doyma), I(şiddet-parlaklık) kümesi

Bu üç uzayın temel özellikleri incelendiğinde RGB uzayının en uygun yöntem olduğu görülür. Çünkü YCrCb uzayı rasgele değişimlerin uygulanmasına uygun değildir. Bu uzayın bileşenlerine yapılacak rasgele değer atamaları, esas gösterim için kullanılacak olan RGB uzayında fiziksel-matematiksel anlamda karşılığı olmayan noktalara gidebilmektedir. HSI uzayında ise sadece H bileşeninin dönüşümü kullanılır özellikler yansıtmaktadır. Fakat gerek işlem yükü gerekse sadece renk bileşenini değiştirmenin istenen görsel rahatsızlığı yaratmaması nedeniyle HSI uzayı da tercih edilmemiştir. Sonuç olarak görüntünün kayıt sırasında kamerada ve ekranda gösterilirken işlendiği, dolayısıyla MPEG kodlayıcının girişindeki ve MPEG kodçözücünün çıkışındaki uzay olan RGB uzayı seçilmiştir.

3 Algoritma

Söz konusu koşulları sağlayan ve RGB uzayında benekleri değiştirecek olan dönüşüm algoritması, R, G, B bileşenlerinin değerlerinin seçilen belli yüzdelere göre arttırılması ya da azaltılmasıdır. Yüzde orana dayalı değer değişimi ile, RGB değerlerinin tanımlı oldukları [0-255] aralığında kalmaları da garanti altına alınmaktadır. Yüzde değerleri (α parametreleri) R, G, ve B bileşenleri için ayrı ayrı belirlenir. Böylece görsel bozulmanın etkisi artar. α parametresinin bir beneğe uygulanması iki şekilde yapılır:

- **Benek değerini azaltma:** Orijinal değer α parametresi ile çarpılır.
- **Benek değerini arttırma:** Orijinal değer 255'ten çıkarılır. Elde edilen fark α parametresi ile çarpılarak küçültülür, ve bu sonuç yeniden 255'ten çıkartılır.

Bu mekanizma ile α parametresinin [0-100] aralığındaki değerleri için RGB bileşenleri [0,255] aralığında tanımlı oldukları tüm değerlere atanabilirler. Böylece resimdeki parlaklık, renk ve kontrast bilgisi serbestçe değiştirilebilmektedir ve resimde yer alan içeriğin görsel özellikleri bozulmuş olur. Ayrıca ek bir işlem olarak negatife çevirme uygulanabilir. Bu haliyle algoritma kayıplı bir algoritmadır.

Bu algoritmanın uygulanması sırasında MPEG ile kodlama koşulları gereği belli sayıda komşu beneğin aynı α parametresi ile dönüştürülmesi gerekmektedir. Böylece imge içi ilişki mümkün olduğunca korunmuş olacaktır. Bu durum iki ana kriter göz önüne alındığında şu koşulları ortaya koyar. MPEG imge içi kodlama süreçleri 8*8 resim bloklarına AKD [7] (Ayrık Kosinüs Dönüşümü, DCT) uygulanmasını içermektedir. Bu nedenle aynı α parametresi ile kodlanacak benek blokları en az 8*8 boyutunda olmalıdır. İkinci kriter olan hareket vektörleri göz önüne alındığında ise makroblok boyutunun [8] katlarına çıkılması gerekmektedir. Bu durumda en az 32*32'lik blokların kullanılması gerekir. Video dizisine ait resimlerin 32*32'lik alt bloklara bölünerek, her altblokta farklı α parametreleri kullanılması, görsel bozulma açısından çok etkin bir sonuç yaratmaktadır. Negatife çevirme işlemi de her bir altblokta bağımsız ya da uyarlamalı uygulanabilir.

Görsel bozulma etkisinin zamana yayılması ve algoritmanın kırılmaması için α parametreleri zaman içinde de değiştirilir. MPEG kodlamasının verimli olması açısından ideal çözüm, bu değişimin GOP uzunluğuna bağlı yapılmasıdır. Gözün zaman boyutunda frekans duyarlığı 8Hz civarında en üst düzeydedir [9]. Yüksek frekanslara çıkıldıkça (70Hz üstü) hassasiyet iyice azalarak tamamen yok olmaktadır. PAL TV sisteminde saniyedeki resim adedi 25, NTSC'de ise 30'dur. Şifreleme ile gözün mümkün olduğunca rahatsız edilmesi için 8Hz esas alınırsa 3-4 karelik GOP yapılarının kullanılması gerektiği görülür. Günümüzde çoğu yayıncı 12 karelik GOP'lar kullanır ve GOP uzunluğu arttıkça (belli sınırlar içinde kalmak koşuluyla) MPEG kodlamanın verimi artar. Bu nedenle çok kısa GOP yapıları tercih edilmez. Fakat, bu algoritma ile 12 karelik GOP yapıları için elde edilen zamansal görsel rahatsızlık da yeterli olmaktadır. Bu çalışmada, α parametrelerinin aynı kaldığı kare sayısı ve dolayısıyla GOP uzunluğu 6 kare olarak seçilmiştir. Bu rakam MPEG verimi ve görsel bozukluk yaratma açısından ortada, ideal bir ölçü olmaktadır. Şekil 1'de çalışma sırasında kullanılan iki video dizisinin ilk kareleri orjinal halde ve şifrelenmiş olarak verilmiştir.

4 Test Koşulları

Algoritmanın test edilmesi amacıyla ellişer karelik iki adet video dizisi kullanılmıştır. Birinci dizi Heinrich Herz Ensititüsü'nün [10] kataloğunda yer alan Harbour isimli dizidir; 4:2:2 örnekleme ile 50Mbps'de kodlanmış olan bir dizidir (*testler açısından kayıpsız bir kaynak olarak değerlendirilebilir*). Testler için, orijinal boyutundan 384*320 boyutuna indirgenmiştir.

İkinci dizi ise algoritmanın olası kusurlarını ortaya çıkarabilecek şekilde tasarlanmış özgün bir dizidir. Özel bir yazılımla orjinal olarak üretildiğinden hiç bir kayıp ya da gürültü söz konusu değildir. Bu ikinci dizinin imge boyutu 384*384'tür. İmge boyutlarının 3.Bölüm'de anlatılan koşulların test edilebilmesi amacıyla 64'ün katı olmasına dikkat edilmiştir. Böylece 32*32'lik ve hatta 64*64'lük altblok kullanımındaki sonuçlar incelenmiştir. Ayrıca genel uygulamalar çerçevesinde resimlerin RGB değerleri [25,225] aralığına normalize edilmiştir. Bu iki dizinin ilk kareleri Şekil 1'de yer almaktadır.

Görsel izlenebilirliği tamamen yok etmemek söz konusu olduğundan yöntem hatalarını küçük tutmak amacıyla α parametreleri [50-90] aralığında kullanılmıştır. MPEG2 kodlayıcısı olarak MPEG Organizasyonu'nun web sitesinde [11] bulunan MPEG Software Simulation Group'a ait 1.1 versiyon yazılım kullanılmıştır. Tüm kodlamalar 4:2:0 örnekleme ile gerçekleştirilmiştir.

1 a

1 b

1 c

1 d

Şekil 1. Testlerde kullanılan iki video dizisinin ilk kareleri rasgele parametrelerle şifrelenmiş ve şifresiz durumda; a ve c: Harbour, b ve d: özel hazırlanmış resim dizisinden.

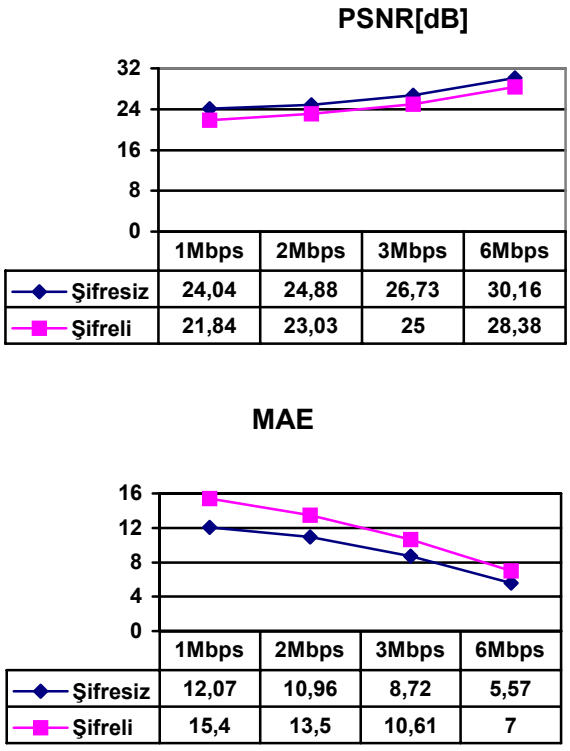
5 Testler ve Sonuçlar

Algoritmanın sağlaması gereken temel şart alıcıda yayın kalitesinde görüntünün elde edilmesidir. Bu nedenle ilk incelenmesi gereken özellik MPEG kodlamasının uygulandığı ve uygulanmadığı durumlardaki kalite ölçütleridir. Tablo 1'de MPEG kodlamasız durum için şifre çözücü çıkışında elde edilen kalite ölçütleri α parametresine bağlı olarak verilmiştir. Buradaki sonuçlar, MPEG kodlama kayıpları olmaksızın sadece şifreleme algoritmasından kaynaklanan kayıpların çok küçük olduğunu ortaya koymaktadır. Kayıplar göz açısından algılanamayacak mertebededir.

Tablo 1.
α değerine göre şifrelemeden kaynaklanan hata.

α (%)	50	60	70	80	90
MAE	0,4	0,8	0,88	0,64	0,72
PSNR(dB)	52,1	47,62	47,33	50	49,54

Önemli olan, algoritmanın, MPEG kodlaması ile birlikte uygulanması sonucu, MPEG'in oluşturacağı kayıplara ek olarak ne kadar ek kayıp oluşturacağıdır. Sonuçlar bu kaybın küçük mertebede olduğunu, ve en önemlisi MPEG ile kodlama kalitesi arttıkça küçüldüğünü göstermektedir. Yani MPEG kodlamasının resim kalitesi ne kadar iyiyse, şifrelemenin getirdiği kalite kaybı o kadar küçüktür. Bu durum, algoritmanın doğası gereğidir. Şekil 2'de şifrelemenin uygulandığı ve uygulanmadığı durumlarda MPEG kodlanmış diziye ait kalite ölçütleri yer almaktadır. Görüldüğü gibi, MPEG kodlama kalitesi arttıkça şifrelemeden dolayı olan hata küçülmektedir**.**

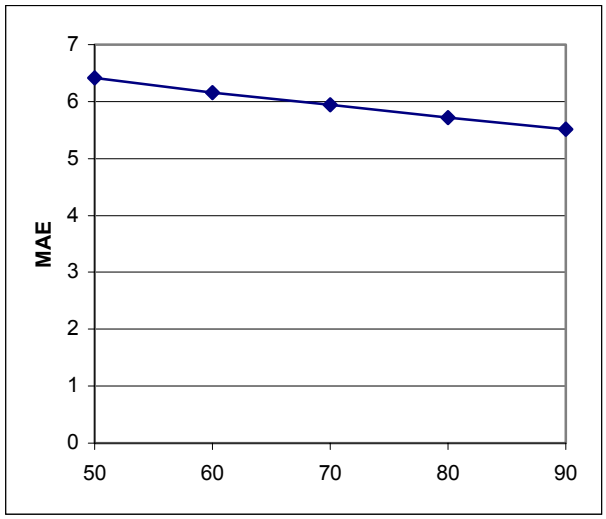


Şekil 2. Şifreleme varken ve yokken MPEG kodlanmış dizinin farklı bit hızları için kalite ölçütleri *(α parametrelerinin rasgele ve bağımsız değiştiği şifreleme durumunda*). MAE, 8-bit için 255 tam ölçek üzerinden.

Elde edilen performans, algoritmanın, görsel bozulmaya dayalı bir yöntem olarak sayısal yayıncılık için kullanılabileceğini görüntü kalitesi açısından göstermektedir. Kullanılan MPEG kodlayıcıda 4-6Mbps arası değerlerde yayın kalitesinde kabul edilebilir videolar elde edilebilmektedir. Bu seviyede şifrelemeden dolayı gelen ek hata MAE bazında 2'den küçüktür. Bu hata görüntüye bir çeşit beyaz gürültü gibi rasgele ve dağılmış olarak eklenmektedir. Çünkü kaybın temeli yüzde alma işlemi sırasında oluşan sayısal yuvarlama hatalarıdır. Bu hatalar MPEG kodlamasının ardından α parametresine bağlı olarak düzgün şekilde değişen bir özellik göstermektedir. Bu durum Şekil 3'te görülmektedir. 4Mbps ile kodlanmış dizide elde edilen MAE değerlerinin değişimi α parametresine bağlı olarak verilmiştir. Bu dizinin, şifrelenmeden 4Mbps için sadece MPEG kodlandığında, sahip olduğu MAE 4.74'tür. Şekilde artan α ile MAE değişiminin şifresiz haldeki 4.74 değerine doğru yakınsadığı görülmektedir. PSNR için de değişim tamamen aynı karakterdedir. Görüldüğü gibi α parametresi büyüdükçe, yani orijinal bilginin daha büyük bir kısmı korundukça MAE doğrusal bir karakterde azalmaktadır.

Algoritmanın MPEG kodlamasının performansını etkileyecek farklı özellikleri ile ilgili ayrıntılı testler yapılmıştır. Yukarıda örnekleri verilen test çıktılarının analizinden elde edilen bazı sonuçlar şunlardır:

- 6 ve 12 uzunluklu GOP yapısı ve şifreleme peryodu kullanıldığında elde edilen kalite değerleri çok yakındır. Aradaki fark, MAE bazında 0.2'den, PSNR bazında ise 0.2dB'den küçüktür. Bu durumda daha sık şifre değişimini sağlamak için 6'lı GOP yapısının kullanılması MPEG kodlamasının verimini çok etkilememektedir.
- Resmin bloklar halinde şifrelenmesi, beklendiği gibi hareket vektörlerinin bir kısmının yok olmasına neden olmaktadır. Hareket vektörleri adedi bakımından bu kayıp, şifre blok boyutunun 32*32 olması durumunda %18, 64*64 olması durumunda ise %11mertebesinde gerçekleşmektedir. Diğer yandan blok boyutlarının 32*32 ve 64*64 seçilmesi durumları arasındaki kalite farkları MAE bazında 1'in altında, PSNR bazında ise 0,8dB'in altında kalmaktadır. Bu nedenle algoritmanın son halinde 32*32'lik blok kullanılmasına karar verilmiştir.



Şekil 3. Aynı dizinin 5 ayrı α (%) değeri için 4Mbps ile MPEG kodlanmış halinde elde edilen MAE değerleri (*8-bit pikseller ve tam sapma 255 hesabıyla*). Dizinin, şifrelenmeden sadece MPEG kodlandığında, elde edilen MAE 4.74'tür

6 Sonuç

Tasarlanan algoritma amaca uygun şekilde çalıştırılarak, elde edilen sonuçlarla, algoritmanın sayısal yayıncılık için uygulanabilir olduğu gösterilmiştir. Şifrelemenin uygulanmasından dolayı oluşan ek hata düşük ve kabul edilebilir düzeyde kalmaktadır. Oluşturulan görsel bozulma hem içeriğin

normal izlenmesini engelleyecek hem de kısıtlı izlemeyi sağlayacak düzeydedir. α parametrelerinin izin verilen değişim aralığını GOPlar için zamanda sırayla daraltarak (veya genişleterek) elde edilen görsel bozulmanın miktarı kontrol edilebilir. Örneğin, şifrelemeye önce %100 bölgesine yakın ve dar bir α değer aralığı için az bozulmuş bir görsel etki ile başlayarak, zamanla bu aralığı aşağıya doğru genişleterek görsel bozulma arttırılarak belli bir süre sonra arzulanan seviyede bozulmuş bir görüntüye gidilebilir. Şifrelemeye böyle bir yumuşak geçişin, halen uygulanmakta olan keskin geçişlere göre ticari bakımdan daha cazip olacağı beklenmektedir. Çalışmanın takip eden aşamasında, şifre çözümü için gerekli parametrelerin (α parametreleri gibi) ve sistemin yönetimi için gerekli komutların resim içinde aktarılması üzerinde durulmaktadır [12].

Kaynaklar

[1] Support for use of Scrambling and Conditional Access within Digital Broadcasting Systems-DVB Document A007, Şubat 1997

[2] www.nagravision.com

[3] Jain A.K., Fundementals of Digital Image Processing, Prentice Hall, 1989

[4] Pennebaker W.B., Mitchell J.L., JPEG Still Image Data Compression Standard. J.LVan Nostrand Reinhold, 1993.

[5] Mitchell J.L., Pennebaker W.B., Fogg C.E., LeGall D.J., MPEG Video Compression Standard, Chapman&Hall, 1996

[6] R.C.Gonzalez, R.E.Woods, Digital Image Processing., Addison-Wesley Publishing Company 1993

[7] Rao K.R., Yip P., Discrete Cosine Transform, Academic Press Inc., 1990

[8] ISO/IEC 13818-2. Information Technology-Generic coding of moving pictures and associated audio information: Video

[9] Hutson G.H., Shepherd P. J., Brice W.S.J., Colour Television, McGraw Hill, 1989

[10] www.hhi.de

[11] www.mpeg.org

[12] Pazarcı, M, Dipçin. V., A MPEG2-Transparent Scrambling Technique, IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, Mayıs 2002.