itüdergisi/***d***
mühendislik
Cilt:2, Sayı:1, 13-22
Şubat 2003

Görsel bozulmaya dayalı sayısal video şifreleme

Vadi DİPÇİN, Melih PAZARCI*
İTÜ Elektrik-Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği Bölümü, 34469, Ayazağa, İstanbul

Özet

Bu çalışmada, sayısal şifreli yayıncılık ortamında kullanılan "bit dizilerinin şifrelenmesi" yöntemine alternatif olarak resimde görsel bozukluk oluşturan bir yöntem önerilmektedir. Böylece izleyicinin içeriğe kısıtlı erişimi ve mevcut sistemlerde ek güvenlik sağlanmış olmaktadır. Algoritma resim içeriğini altbloklara bölerek, beneklerin RGB bileşenlerini değiştirmekte ve şifrenin çözümü için gerekli tüm veriyi resim içinde saklamaktadır. Böylece yöntem var olan tüm sistemlerle kullanılabilir, tüm standartlarla uyumludur. Bunun tek önkoşulu MPEG ile uyumluluktur. Görsel bozulmaya dayalı klasik şifreli yayın yöntemleri MPEG ile verimli kodlanamaz.Bu çalışmada önerilen yöntem, bu probleme özgün bir çözüm içermektedir. Resim içinde veri taşınması önemli bir güvenlik avantajı sunar.
Anahtar Kelimeler: *MPEG, sayısal televizyon, şifreli yayıncılık, telif hakları.*

Picture scrambler for digital video

Abstract

The current conditional access techniques for digital TV systems depend on encrypting MPEG-2 data packets at the bitstream level. Known methods, using visual distortion, can not be used in digital systems because they produce video sequences which can not be encoded with MPEG-2 efficiently. This paper examines the conditions of scrambling systems using visual distortion for MPEG-2 compliance and then proposes a solution which fulfills them. In order to obtain usability with existing systems, the proposed method must be independent of all the parameters in digital broadcasting systems such as channel, bit-rate, modulation etc. This is possible if the method is MPEG-2 transparent. The algoritm works in any case where an MPEG-2 video can be transmitted and displayed.The main condition of this is to carry the related information within the video sequence. This is realised by using the subblock boundaries which are created by the scrambling and the TV logo which exists in all broadcasts. Transmission of scrambling parameters in images enables a high degree of security and flexibility.The main concept to modify the pixel values of the original content enables also various applications for copyright protection in other digital distribution channels like VoD, DVD, PVR etc.
Keywords: *MPEG-2, digital TV, scrambled broadcast, copyright protection.*

*Yazışmaların yapılacağı yazar: Melih PAZARCI. eepazarc@ehb.itu.edu.tr; Tel: (212) 285 35 04.
Bu makale, birinci yazar tarafından İTÜ Elektrik-Elektronik Fakültesi'nde tamamlanmış "Görsel bozulmaya dayalı sayısal video şifreleme" adlı doktora tezinden hazırlanmıştır. Makale metni 14.06.2002 tarihinde dergiye ulaşmış, 28.11.2002 tarihinde basım kararı alınmıştır. Makale ile ilgili tartışmalar 31.05.2003 tarihine kadar dergiye gönderilmelidir.

Giriş

Sayısal şifreli yayın sistemlerinde içeriğe erişimin engellenmesi için kullanılan teknik, MPEG (ISO/IEC 13818, 1996; Mitchell v. diğ., 1996) veri paketlerinin bitler seviyesinde şifrelenmesine dayanır. İzleyicinin yetkisi olması durumunda alıcı kutu, yollanan anahtarları kullanarak şifreyi çözer ve yayının seyredilmesini sağlar. Aksi halde izleyici ekranda erişim hakkı olmadığına dair bir mesaj görür. Oluşturulan standartlara uyumlu olan ve üreticilerin özgün matematiksel modellerine dayanan bu şifreleme sistemleri büyük oranda kırılmıştır. Özellikle yayın izleme yetkisi, sistemlerde standart olarak yer alan akıllı kartlarla oynanarak değiştirilmektedir. Bu nedenle alternatif bir yöntemle, yeni uygulamalar sağlayacak ve ek güvenlik getirecek bir yöntem işlevsel öneme sahip olacaktır.

Analog yayınlarda şifrelemenin temel iki yönteminden biri görsel bozulmaya dayanır. Bu yöntemler sayısal ortamda kullanılamazlar çünkü MPEG-2 ile verimli bir şekilde kodlanamazlar. Görsel bozulmaya dayalı bir yöntemin sayısal ortamda kullanılması, içeriğe sınırlı erişim ve özendirme, ek güvenlik, içeriği farklı ortamlarda farklılaştırarak dağıtmak gibi işlevleri sağlayacaktır. Bu nedenle bu makalede görsel bozulmaya dayalı ve MPEG-2 uyumlu bir şifreli yayın sistemi tasarımı ele alınmaktadır.

Öncelikle olarak MPEG-2 uyumluluğu için gerekli koşullar tesbit edilmiştir. Buna dayanarak, beneklerin renk ve parlaklık özelliklerini bozan ve oransal çıkartma işlemine dayanan bir yöntem önerilmektedir. Resimler MPEG-2 makroblok boyutlarının katlarındaki büyüklüklerde olan altbloklara bölünerek, RGB bileşenlerine ayrı parametrelerle bu işlem uygulanır. MPEG kodlama veriminin sağlanması açısından parametre değişimi MPEG GOP yapısı ile eşzamanlı olmalıdır.

Algoritmanın MPEG-2 hariç tüm sayısal yayın parametrelerinden bağımsız olması gerekir. Aksi halde mevcut sistemlerde kullanılamaz. Bunun temel koşulu, şifre çözümü için gerekli verinin resim içinde gömülü olarak taşınmasıdır. Resim içinde veri taşıma amaçlı olarak iki ana yöntem tanıtılmaktadır. Bunlardan birincisi, her yayında yer alan TV logosunu kullanmaktadır. İkinci yöntem ise, şifreleme ile oluşan altblokların sınırlarında süreklilik kontrolü yapılmasına dayanmaktadır.

Şifreleme, verici tarafta MPEG kodlamasının hemen öncesinde gerçekleşir. Alıcı taraftaki kodçözümü ise MPEG kodçözümünün ardından yapılır. Algoritma, tanımlandığı şekliyle, herhangi bir MPEG-2 video dizisinin yayınlanıp gösterilebildiği herhangi bir sisteme uyumludur. Kanal (uydu, kablo, karasal), modülasyon (QAM, COFDM vb.), sıkıştırma oranı, standartlar (DVB, ATSC) gibi tüm değişkenlerden bağımsızdır. Ayrıca içeriğin orjinal yapısının değiştirilmesine dayandığından farklı dağıtım kanallarında (DVD, PVR, VoD vb.) telif haklarının korunmasına destek olacak etkin uygulamalara da yol açmaktadır.

Şifreleme

Koşullar

Görsel bozulmayı sağlayacak şifreleme işlemi temel olarak

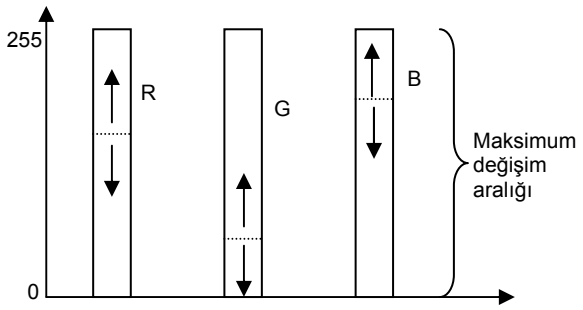
- rastgele parametrelere bağlılık,
- MPEG uyumluluğu,
- düşük işlem yükü,
- düşük bellek gereksinimi

koşullarını sağlamak durumundadır. MPEG uyumluluğunun sağlanması için resim içi ve ardışıl resimler arası ilişkilerin bozulmaması ya da en az belli bölgelerde korunması gerekir. Bu nedenle şifreleme işlemi, en az belli sayıda benek için, aynı parametrelerle uygulanmalıdır ve uygulanan işlem orjinal durumda benzer olan benek değerlerini yine yakın değerlere ötelemelidir. Görsel bozulmanın etkisini kuvvetlendirmek için resimler altbloklara ayrılmaktadır. MPEG kodlayıcıların hareket vektörlerini arama yöntemleri nedeniyle altblok boyutları MPEG makroblok boyutlarının (16*16) katlarında olmalıdır. MPEG kodlayıcının verimli kodlama yapabilmesi için şifreleme parametreleri bir GOP içinde

değişmemelidir. Bunun sağlanması amacıyla şifreleme sisteminin parametre değişimi MPEG kodlayıcının GOP yapısı ile eşzamanlı olmalıdır. Rastgele parametre ile değişim koşulu, RGB renk uzayını en uygun seçim kılmaktadır. YcrCb uzayında uygulanacak rastgele ötelemeler RGB uzayına geri dönüldüğünde fiziksel karşılığı olmayan koordinatlara karşı düşebilmektedir.

Şifreleme işlemi

Şifreleme işlemi, iki ayrı işlevi içerir. Birinci ve temel işlev, beneklerin RGB bileşenlerinin rastgele parametrelere bağlı bir işlem ile değer aralıkları içinde rastgele ötelenmeleridir. Bu amaçla incelenen metodlar arasında en uygununun oransal çıkartma işlemi olduğu görülmüştür, çünkü uyarlamalı bir yöntem olduğu için rastgele parametrelerle uygulandığında RGB değerlerininin sınır değerleri aşmamasını garanti eder. İşlem orjinal değerlerden belli bir yüzdenin çıkartılmasına dayanır. Bu şekilde benek değerleri azaltılır. Değerlerin arttırılması için ise negatif resimde değer azaltma işlemi uygulanır. Sistemin yapısı Şekil 1'de verilmiştir.



Şekil 1. Şifreleme işleminde öteleme

Yüzde oranlı öteleme işlevi f, α yüzde oranı, B her bir bileşen için bit çözünürlüğü, X ise herhangi bir bileşenin orjinal değeri olmak üzere şöyle tanımlanır:

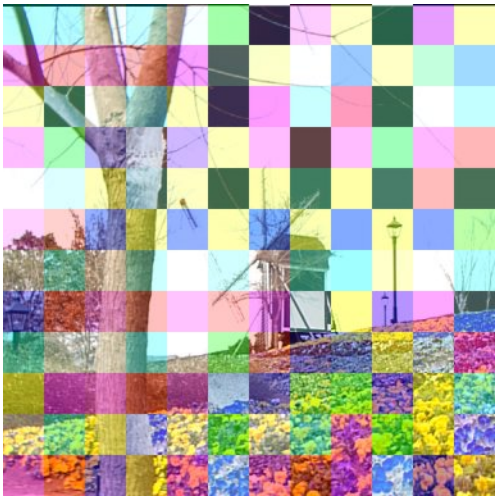
$$f(\alpha, X) = \begin{cases} \alpha X & , azalma \\ (2^B - 1) - \alpha(2^B - 1 - X) & , artma \end{cases} \quad (1)$$

Bu işlem, M*N boyutundaki video dizisi en genel halde K*L boyutundaki dikdörtgensel altbloklara bölünmesi ve her bir altblokta RGB bileşenleri için ayrı ayrı ve rastgele belirlenen α parametreleri ile uygulanır. MPEG makrobloklarının karesel olmaları nedeniyle ve altbloklarının boyutlarının makroblok boyutlarının tam katlarında olması koşuluna dayanarak K=L=32 seçilmiştir. Karşılaştırma için K=L=64 değeri de kullanılmıştır. Ayrıca resim kalitesinin yüksek tutulması için α parametreleri [50,90] aralığında kullanılmıştır. Çünkü daha yüksek yüzde oranı, orjinal bilginin daha iyi korunması demektir. Yüzdeli şifreleme işlemini belirleyecek iki parametre bulunmaktadır. α parametreleri ve yönü belirleyen D matrisi. D matrisi her bir altblok için $[D_R\ D_G\ D_B]$ vektörünü içerir, ki elemanları {0,1}'dir (0 azaltma işlemi, 1 arttırma işlemi).

Görsel bozulmayı sağlayan ikinci işlem, negatife çevirme işlemidir. Her bir altblok için RGB bileşenlerine ortak olarak uygulanan bu işlemi belirleyen N matrisi de {0,1} elemanlarından oluşur (0 değişim yok, 1 negatif al). Buna göre negatif alma işlemi:

$$N(X) = \begin{cases} X & , N = 0 \\ 2^B - 1 - X & , N = 1 \end{cases} \quad (2)$$

olarak tanımlanır. Negatif alma işlemi, görsel bozulma etkisini güçlendirmek amacıyla, RGB bileşenlerinin üçünün de azaltılması durumunda ($[D_R\ D_G\ D_B]=[0\ 0\ 0]$) uygulanmaktadır. Şekil 2'de algoritma ile bozulmuş örnek bir resim yer almaktadır.



Şekil 2. Flowers dizisinden şifreli bir kare

MPEG kodlamasında verimliliğin sağlanması amacıyla, şifreleme parametreleri olan α yüzde oranları, Y matrisi ve N matrisi bir GOP boyunca sabit kalmalıdır. Parametrelerin daha yüksek frekanslı değişimi görsel bozukluk etkisini kuvvetlendirecektir. Diğer yandan bu GOP uzunluğunun kısalması, MPEG kodlama veriminin düşmesi anlamına gelmektedir. Yayınlarda genellikle 12 uzunluklu GOP yapıları kullanılır. Bu da, PAL yayınlar(25fps) için saniyede yaklaşık 2Hz'lik bir değişim frekansı anlamına gelir. Gözün parlaklık değişimine zaman boyutunda olan duyarlığı ise 8Hz mertebesinde en üst düzeye çıkar. Bu veriler göz önünde tutularak GOP uzunluğu ve parametre değişim peryodunun 6 kare olması uygun bir seçim olmaktadır.

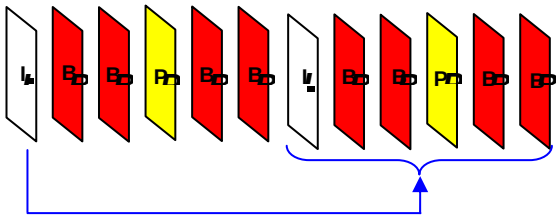
Verilerin taşınması

Genel yapı

Şifre çözümü için gerekli tüm parametreler, güvenlik ve mevcut sistemlerle uyumluluk koşulları nedeniyle, içeriği oluşturan resim dizisinin içinde taşınmaktadır. Böyle bir yapı algoritmayı mevcut tüm standart ve sistemlerden bağımsız kılar. Resim içinde veri taşıma çözümlerinde en öncelikli prensip, her yöntemin şifreleme için kullanılan yüzde oranlı değişim kuralına uyumlu olmasıdır. Bunun iki büyük avantajı vardır:

1. Veriler, resimlerin şifreli durumdaki bozuk yapısının doğasında saklanır. Verilere bağlı hiç bir değişim ya da farklılık gözlenemez. Yüksek seviyede güvenlik sağlanır.
2. Şifreleme yapıldığında, şifreyi çözmek için gerekli veri resme yazılmış olur. Bunun için ayrıca kaynak kullanmak gerekmez.

Veri taşıma ile ilgili diğer bir temel unsur her bir GOP'a ait tüm parametrelerin bir önceki GOP'un I-Karesi'nde taşınmasıdır. Böylece hata olması durumunda kaybedilecek resim adedi ve kanal değiştirmede bekleme süresi azalır. Bu yapı Şekil 3'te gösterilmiştir.



Şekil 3. Bir önceki GOP'un I-Karesi bir sonraki GOP'a ait tüm şifreleme parametrelerini taşır.

Resim içinde veri taşınması temel olarak iki ayrı yöntemle gerçekleştirilmiştir. Birinci yöntem, her TV yayınında var olan TV logosunu kullanmaya dayanır. Böylece içeriğin sabit olan ve alıcı tarafta ne olduğu bilinen bir parçası kullanılmış olur. Diğer yöntem ise resmin kalan bölümünü yani izlenecek içeriği kullanır. Bu içerik önceden bilinemez ya da kontrol edilemez.

Logonun kullanımı

TV logosunun veri taşıma amaçlı kullanımı temel olarak sabit içeriği olmasına dayanır. Bu özelliği yüzde oranlı değişim kuralı ile uyumlu bir şekilde kullanmak ve taşınan bilgiyi MPEG kodlamasındaki kayıplardan korumak için logoda seçilen uygun bölgelerin DC değerlerini kullanmak gerekir. Çünkü DC değerler MPEG kodlamasından en az etkilenen bilgilerdir. Yöntem prensip olarak seçilen bölgenin önceden belli ve sınırlı sayıda α parametresinden biri ile şifrelenmesine dayanır. Logo sabit olduğundan, her bir α parametresi için DC değerin öteleneceği yeni değer bellidir ve alıcı tarafta bilinebilir. Sözkonusu bölgede taşınması gereken bit miktarına göre α parametresinin değişim aralığının bölünmesi ile dönüşüm kuralı belirlenir ve alıcı buna göre kestirimi yapar. Bu kural her logo ile kullanılabilir. Bunun tek önkoşulu logoların analiz edilerek uygun bölgelerinde DC değerlerinin belirlenmesidir.

Testlerde kullanılan örnek sistemde logoda şifreye giriş/çıkış bilgisi taşınmaktadır. Böylece alıcı ne zaman şifre çözme işlemini yapacağını, ne zaman bu süreçten çıkacağını bilir.

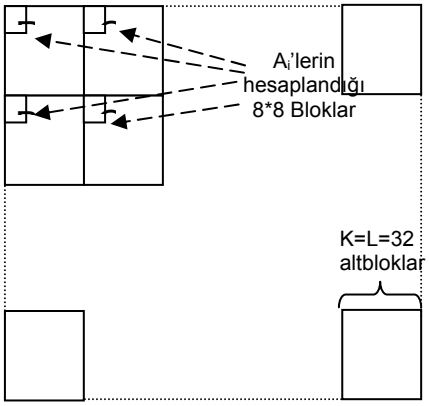
α parametrelerinin iletilmesi

Belirtildiği gibi α parametreleri [50,90] aralığında kullanılmaktadır. Şifreleme ve şifre çözümü sırasında her bir bileşen için hem bu aralıktaki değerin hem de Y matrisinin ilgili bileşeninin bilinmesi gerekir. Tasarlanan algoritma, Y matrisini α parametrelerinin içinde taşıyacak bir yöntem içermektedir. Yöntem α parametrelerinin [50,90] aralığında olmasından yararlanır. α parametrelerini rastgele üretecek olan işlem [0,40] aralığında rastgele sayılar üretir ve hem verici hem de alıcı tarfta bilinen rastgele bir karar mekanizmasına dayanarak bu sayıyı bir δ büyüklüğü ile toplayarak [5,45] ya da [50,90] aralığına öteler. Eğer nihai olarak hesaplanan α parametresi [50,90] aralığındaysa, olduğu haliyle azaltma yönünde kullanılır (Y_x=0). Aksi halde, yani α parametresi [5,45] aralığında ise, bu değer 45 ile toplanarak elde edilen değer arttırma işlemi için kullanılır (Y_x=1). Böylece α parametresi bilindiğinde Y matrisinin ilgili elemanları da bilinmiş olur. α parametrelerinin verici ve alıcı tarafta hesaplandığı formül şu şekildedir:

$$\alpha_X = 9A_i + A_j + \delta \qquad (3)$$

Burada X, her bir altblok için RGB bileşenlerinden biri, A_i ile A_j resim içinde konumları, büyüklükleri ve adetleri rastgele seçilebilecek dikdörtgensel bölgelerin DC değerlerinin en anlamlı bitlerinden elde edilen değerler (i,j=0,1,2,..,T-1. T:bölge adedi) ve δ (δ=5,45) ise rastgele belirlenen öteleme bileşenidir.

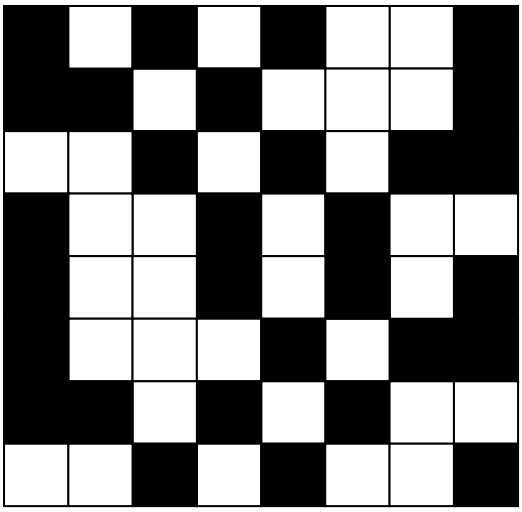
(3)'te α parametrelerinin resim içinde taşınan veri ile elde edilmesini ve iletilmesini temel olarak sağlayan bileşenler A_i'lerdir. Bu büyüklükler, her bir altblok için seçilen belli dikdörtgensel bölgelere ait DC değerlerinin en anlamlı bitlerinden üretilir. Testlerde örnek olarak her 2*2 altblok dörtlüsü için T=4 adet karesel (8*8) bölge kullanılmıştır (Şekil 4). Elde edilen ortalama değerler 64'e bölünerek en anlamlı 2 bit mertebesinde kullanılmıştır. Bu nedenle A_i'lerin aldığı değerler [0,4) aralığındadır. Yuvarlama hatalarından oluşan hataları engellemek amacıyla A_i'ler ondalıklı sayı olarak kullanılır. Bu yöntem ile resmin doğal yapısı içinde yer alan veri, şifreleme parametrelerini elde etmek için kullanılmış olur. Alıcı tarafta da aynı veri var olduğundan, şifre çözümü için gerekli parametreler taşınmış olur ve bu verinin resim içindeki yerine dair hiç bir ipucu, şifreli yayının gözlenmesi ya da matematiksel analizi ile elde edilemez. Sözkonusu bölgelerin yerleri ve büyüklükleri değiştirilebilmesi de güvenlik açısından önemli bir ek avantaj sağlar.



Şekil 4. A_i'lerin hesaplandığı karesel blokların örneği. Her 4 altblok için 4 adet blok kullanılmıştır.

Bağımsız veri taşınması

α parametrelerinin taşınması, şifre çözümü için gerekli şifreleme parametrelerinin taşınmasıdır. Bunun standart şifreleme sistemlerindeki karşılığı ECM'dir (Entitlement Control Message). Bir şifreleme sisteminde ayrıca ikinci bir verinin taşınması da gerekir. Bu veri izleyicilerin içeriğe ulaşma yetkilerini belirler ve EMM (Entitlement Management Message) adını taşır. Söz konusu veri içerikten ve kod kelimelerinden (şifreleme parametreleri) tamamen bağımsızdır. Bu çalışmada önerilen şifreleme sisteminin kullanılabilmesi için bu tür bağımsız bir veriyi de resim dizisi içinde iletebilmesi gerekir. Algoritmanın veri taşıma sisteminin temel ilkesi olan "yüzde oranlı değişim kuralına uyumluluk" gereğince, bu verinin, şifrelemenin ortaya çıkardığı altblok sınırlarındaki sürekliliğin modüle edilmesi yöntemi ile taşınması uygun bir çözümdür (Şekil 5).



Şekil 5. Bağımsız verinin altblok sınırlarında taşınması. Karar kuralı, süreklilik "0", süreksizlik "1" şeklinde tasarlanmıştır. örn. üst sıradaki mesaj "1111101"

Buna göre, her bir altblok satırı boyunca sınırlarda süreklilik kontrol edilerek alınan bit dizisinin belirlenmesi için kestirim yapılabilir. Karar fonksiyonu g:

$$g = \begin{cases} 0 & ,süreklilik \\ 1 & ,süreksizlik \end{cases} \quad (4)$$

şeklinde tanımlıdır. Sürekliliğin verinin resme yazılması sırasındaki kontrolü şu şekilde sağlanır. İşlenmekte olan I-Karede bir sonraki GOP'ta kullanılacak olan α parametreleri bir önceki bölümde belirtilen kurallar çerçevesinde belirlenir. Ardından gönderilecek olan bit dizisine göre α parametre matrisi yeniden yazılır. Öyle ki, sıradaki altblok sınırına yazılacak bilgiye göre sağdaki altbloğun α parametresi α_{i+1}, soldaki altbloğa ait olan α_i ile ilişkilendirilir:

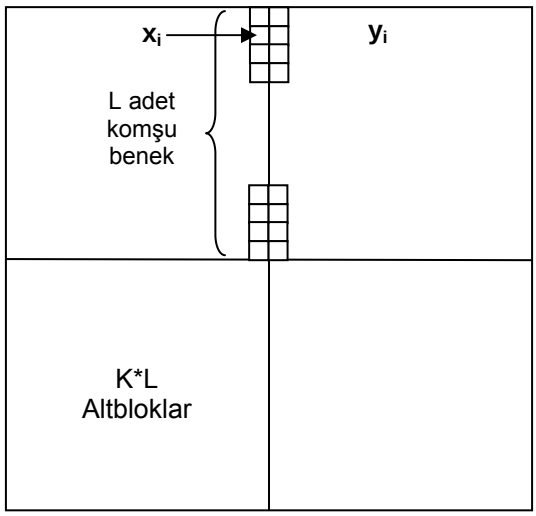
$$\alpha_{i+1} = \begin{cases} \alpha_i & ,veri = 0 \\ \alpha_i \pm 45 & ,veri = 1 \end{cases} \quad (5)$$

+/-45'lik öteleme, (3)'teki ifadede yer alan δ'nın işlevini yerine getirmektir. Yani iletilecek verinin "0" olması durumunda komşu altblokların seçilen renk bileşenleri aynı α parametresi ile aynı yönde, "1" olması durumunda ise aynı α parametresi zıt yönde şifrelenirler. Böylece belli bir miktar süreksizlik yaratılması garantilenmiş olur.

Bu kural gereğince resme yazılan verinin alıcı tarafta kestirilmesi şu şekilde gerçeklenir. Alıcı tarafta, belirlenen altblok sınırları boyunca süreklilik/süreksizlik kararı verilmelidir. Bu işlem, sınır boyunca uzanan komşu beneklerin farklarının ortalaması incelenerek yapılır. Bu fark:

$$F = \frac{1}{L}\sum_{i=1}^{L}(x_i - y_i) \quad (6)$$

ile ifade edilir. Burada, x_i ve y_i altblok sınırları boyunca yer alan beneklerin seçilen bileşenlerine ait parlaklık değerleridir (Şekil 6). Hataların ortalaması alındığından, F sadece iki benek arasındaki bir fark değer mertebesinde ve karakteristik bir büyüklük olacaktır.



Şekil 6. Altblok sınırlarında sürekliliğin kontrol edilmesi

Bu kestirim kuralının matematiksel analizi şu şekildedir. Doğal görüntülerde komşu benekler (x_i,y_i) birbirlerine çok benzerler ve aralarındaki fark küçüktür. Bu nedenle aynı α parametresi ile şifrelendiklerinde yine çok benzer olmaları beklenir.

Söz konusu bileşenlerin kırmızı (R) oldukları varsayımıyla bu durum:

$x_i = R,\ y_i = R+dR$ (7)

ile gösterilebilir.

Buna göre, iletilen verinin "1" olması durumunda 8 bitlik benekler için:

$x_i' = \alpha * R,\ y_i' = 255 - \alpha\,(255-R-dR)$ (8)

olur. Bu durumda komşu iki benek arasında oluşacak fark F:

$$F(1) = y_i' - x_i' = [255 - \alpha\,(255-R-dR)] - \alpha R = 255 + \alpha\,(dR-255) \quad (9)$$

bulunur. Görüldüğü gibi alıcıda gözlenecek F fark değeri ilk değerden (R) bağımsızdır, α parametresine ve dR'ye bağlıdır. İletilen verinin "0" olması durumunda ise fark değeri:

$$F(0) = \alpha * dR \quad (10)$$

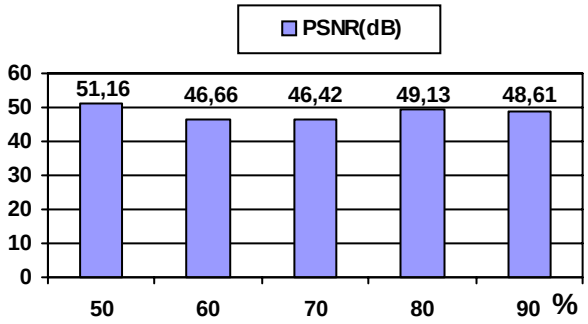
olur. Alıcı, ilgili altbloklar için α parametresini biliyor olacaktır. F fark değerini ise (6) uyarınca hesaplayabilir. Kestirim kuralı, belirtildiği gibi dR'nin doğal resimlerde büyük olasılıkla küçük değerli olmasına dayanmaktadır. Buna göre (9) ve (10) denklemleri dR'ye göre açılarak her iki denkleme α ve F değerleri konur ve "0" ve "1" durumları için iki dR hesaplanır. Hangi denklemin verdiği dR küçükse, o veri lehine kestirim yapılır.

Testler ve sonuçlar

Test sonuçlarında iki temel konunun ortaya konması gerekmektedir. Birincisi şifrelenmiş ve alıcıda yeniden şifresi çözülmüş video dizisinin yeterli görüntü kalitesine sahip olması, ikincisi ise iletilen bilginin güvenilirliğinin belirlenmesidir.

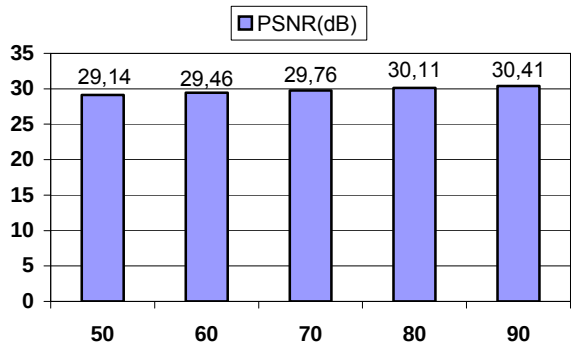
Resim kalitesi

Şekil 7'de sadece şifreleme uygulanan resim dizisinde oluşan PSNR değerleri görünmektedir. Testlerde kullanılan [50,90] yüzde aralığı için iyi sonuçlar alındığı görülmektedir. Yüzde oranı yükseldikçe, orjinal bilgi daha iyi korunmuş olduğundan resim kalitesi genel eğilim olarak yükselmektedir. Bununla birlikte %50 için daha iyi bir sonuç alınmaktadır. Bunun nedeni bu yüzde değerinin pratikte ikiye bölme işlemi olması ve bu işlemin ikili düzende hesap yapan işlemcilerde daha küçük hataya neden olmasıdır.



Şekil 7. Sadece şifreleme uygulanan video dizisinde PSNR'nin α parametresine göre değişimi

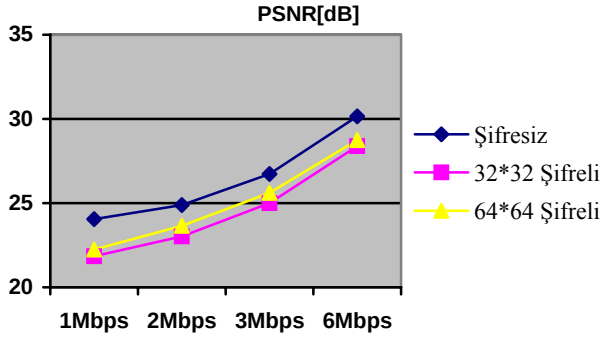
Şifrelemenin MPEG kodlaması ile birlikte uygulanması durumunda PSNR'nin α parametresine göre değişimi de Şekil 8'de yer almaktadır. İki işlemin birden uygulanması ile PSNR'nin α parametresine göre değişimi hemen hemen doğrusal bir ilişki oluşturmaktadır.



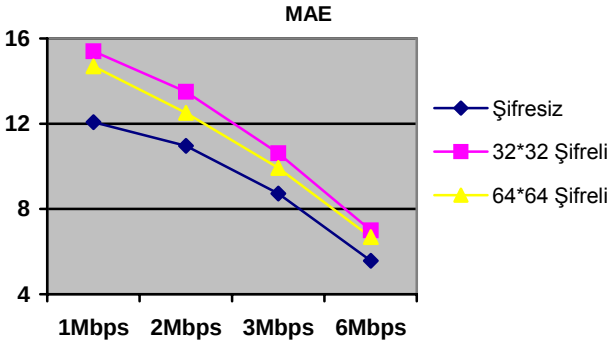
Şekil 8. Hem şifreleme hem MPEG kodlama uygulanması durumunda PSNR'nin α parametresine göre değişimi.

Resim kalitesinin rastgele α değerleriyle şifrelenmiş video dizilerinde MPEG bit hızına göre değişimi ise Şekil 9 ve Şekil 10'da yer almaktadır. Burada görülen iki sonuç, şifrelemeden kaynaklanan ek hatanın

MPEG'den kaynaklanan hataya göre küçük olduğu ve MPEG'deki kodlama kalitesi yükseldikçe düştüğüdür. Şifrelemeden dolayı eklenen hata, benek değerleri bazında 2-3 mertebesindedir. MPEG kodlamasından kaynaklanan hata baskın bileşeni oluşturur. Gerçekten de, resim kalitesi MPEG kodlayıcının şifresiz durumda verdiği kalite ile yakından ilişkili olmaktadır. MPEG kodlayıcının kaliteli video ürettiği sıkıştırma parametreleri için şifreli video da kalitelidir.



Şekil 9. Şifreli ve şifresiz durumda video dizisinin PSNR'sinin MPEG bit hızına göre değişimi



Şekil 10. Şifreli ve şifresiz durumda video dizisinin MAE'sinin MPEG bit hızına göre değişimi

Şekil 9 ve 10'da yer alan 32*32 ile 64*64 ifadeleri altblok boyutlarını (K*L) göstermektedir. İki ayrı altblok boyutu kullanmanın amacı şifreleme nedeniyle kaybedilen hareket vektörlerinin etkisini tesbit etmektir. Görüldüğü gibi 64*64 boyutlu altblok kullanıldığında görüntü kalitesi biraz daha iyi olmaktadır. Ayrıca yapılan bir analizle altbloklara bölünmeden dolayı kaybedilen hareket vektörlerinin oranı saptanmıştır. Test dizisinde, 32*32'lik altbloklar için orjinal durumda var olan hareket vektörlerinin %18.43'ü yok olmaktadır. Aynı sayı 64*64'lük altbloklar için %10.96'dır.

Sonuç olarak bu veriler, algoritmanın yayın kalitesinde görüntü sağlayabildiğini, MPEG ile verimli bir şekilde kodlanabildiğini göstermektedir. Dolayısıyla, hedeflenen MPEG uyumlu ve görsel bozulmaya dayalı bir şifreli TV sistemi bu açıdan elde edilmiştir.

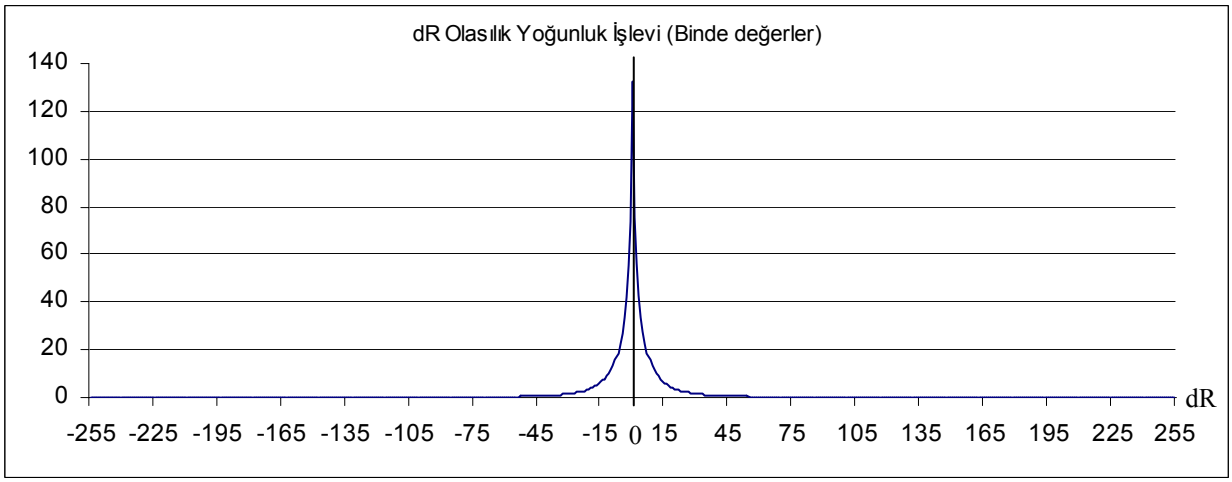
Veri taşıma

Algoritmada iletilen ve alıcı tarafta kestirimi yapılan iki tür veri bulunmaktadır. α parametreleri ve altblok sınırlarında taşınan bağımsız bit dizileri.

α parametrelerinin kestirimi ile ilgili yapılan testlerin sonuçları, alıcı tarafta α parametrelerinin %78.3'ünün hatasız, %21.7'sinin ise 1 hata ile kestirilebildiğini göstermektedir. α parametreleri, resim içindeki çeşitli bölgelerin DC değerleri kullanılarak, MPEG'in getirdiği kayıplara rağmen çok başarılı bir şekilde alıcıda oluşturulabilmektedir. α parametresinin bir yüzde değeri olduğu düşünülürse bundan kaynaklanacak yöntem hatasının 8 bitlik renk bileşenleri için en fazla 2.5 (255/100) mertebesinde olacağı görülür. Böylece neden şifrelemeden dolayı MAE'de büyük bir yöntem hatası gözlenmediği de açıklanmış olur. Şifreleme parametrelerinin alıcıda bu kadar doğru bir şekilde kestirilebilmesi önemli bir avantajdır.

Bağımsız bit dizisinin iletiminde ise dR'lerin doğal resimlerdeki olasılık dağılımına bağlı bir hata oluşması kaçınılmazdır. Çünkü kestirim kuralı daima daha küçük dR'yi veren denkleme ait biti doğru kabul etmektedir.

Bu kestirim kuralının hata yapma olasılığının analizinin yapılması amacıyla örnek resimlerden alınan verilerle düzenlenen dR dağılım işlevi Şekil 11'de yer almaktadır.



Şekil 11. dR fark değerlerinin olasılık yoğunluk işlevi

Bu dağılım, normal dağılım yapısına çok benzemektedir. dR'lerin şifresiz durumda bu şekilde olan dağılımının ortalama değeri ve varyansı şifreleme ile birlikte değişmektedir. Öyle ki iletilen veri "0" ise ortalama değişmeyerek sıfırda kalır fakat varyans, α ile çarpım ve genel olarak C adet benek boyunca alınan ortalama nedeniyle değişir. "1" verisi gönderildiğinde ise hem ortalama hem de varyans değişir. Her iki durum için elde edilecek normal dağılımın parametreleri:

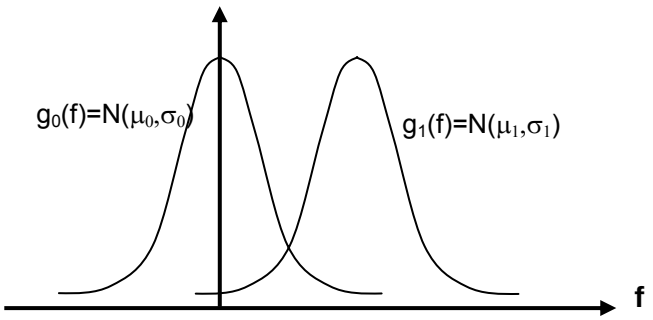
$\mu_0=0$ (11)

$\sigma_0= \alpha\sigma/(C)^{1/2}$ (12)

$\mu_1=255(1-\alpha)$ (13)

$\sigma_1= \alpha\sigma/(C)^{1/2}$ (14)

olur ve iki dağılım Şekil 12'deki gibi görünürler.



Şekil 12. Fark değerlerin şifrelemeden sonraki dağılımı

Buna göre karar kuralının hata yapacağı bölge, her iki dağılımın kesiştiği bölgededir. Hata oranının hesaplanacağı formül ise,

$$p_h = \frac{1}{2}\int_{255(1-\alpha)+\alpha dR_{\min}}^{255(1-\alpha)/2} g_1(f)\,df + \frac{1}{2}\int_{255(1-\alpha)/2}^{\alpha dR_{\max}} g_0(f)\,df \quad (15)$$

olur. Hata olasılığı görüldüğü gibi belli bir resim kümesi için α'ya göre değişmektedir. α'nın tezde kullanılan aralıktaki değerleri için bu formülden elde edilen örnek hata olasılıkları Tablo 1'de yer almaktadır. Bu tablodaki veriler, dR'lerin, σ=15 gibi çok yüksek sapmalı bir dağılım göstermesi durumu için doğrudur ki, bu değer hata üst sınırını belirlemek için yeterince toleranslıdır.

Tablo 1. Örnek hata olasılıkları

α	**50**	**60**	**70**	**80**	**90**
P_h (C=1)	$4*10^{-14}$	$2*10^{-7}$	$8*10^{-4}$	0,033	0,208
P_h (C=16)	0	0	0	$1*10^{-13}$	$5*10^{-4}$
P_h (C=32)	0	0	0	0	$2*10^{-6}$

C'nin anlamı altblok sınırı boyunca kaç benek çiftinin farkının ortalamasının alındığıdır. C=1 tek bir benek çiftinin farkının doğrudan

kullanıldığını gösterir. C=16 ise altblok sınırı boyunca 16 benek çiftinin farklarının ortalaması ile karar alındığını göstermektedir. Algoritmanın gerçek bir sistemde kullanımında, şifreleme için kullanılan α parametre aralığının ve C değerinin üreteceği hata olasılıklarına göre uygun bir hata düzeltme algoritması kullanılabilir.

Bu yöntemi kullanarak taşınabilecek veri miktarı şöyle hesaplanabilir. Yatayda veri saklanabilecek altblok sınır adedi:

$$S_y = INT(0,5+M/K) \quad (16)$$

ve altblokların oluşturduğu satır adedi ise:

$$S_d = INT(0,5+N/L) \quad (17)$$

olur. (16) ve (17)'nin çarpımı bir GOP'ta ve bir renk bileşeninde oluşan altblok sınırı adedini verir. GOP uzunluğu 6 kare olduğundan dolayı, f_t kullanılan yayın sisteminde saniyedeki resim karesi frekansını göstermek üzere, 3 renk bileşeninin birden kullanılması durumunda saniyedeki bit hızı:

$$b = 3*S_y*S_d*f_t/6 \quad (18)$$

ifadesi ile hesaplanır. PAL TV için (M,N)=(720,576) ve f_t=25 tir. Buna göre testlerde kullanılan altblok boyutu K=L=32 için veri hızı:

$$b = 4950bps \quad (19)$$

olarak bulunur. Bu, altblokları kullanan yöntem ile iletilebilecek maksimum veri hızıdır. Analizi verilen hata olasılıkları gereği bir hata düzeltme yönteminin kullanılması gerekir.

Sonuç

Çalışmada, sayısal TV yayınlarında kullanılmak üzere tasarlanmış, görsel bozulmaya dayalı bir şifreli yayın sitemi tanıtılmıştır. Algoritma, sayısal TV ortamı için görsel bozulmaya dayalı bir yöntem olması açısından özgün bir işlevi yerine getirmektedir. Yaratılan görsel bozulma, rastgele olması ve içerikteki görsel özellikleri değiştirmesine rağmen MPEG ile verimli bir şekilde kodlanabilir resim dizileri üretebilmektedir. Bu anlamda temel hedefe ulaşılmıştır.

Elde edilen görüntülerin analizi, video kalitesi açısından tatmin edici sonuçlar vermiştir. Yöntem hatası olarak ortaya çıkan etki, MPEG kodlamasından kaynaklanan hataya göre daha küçüktür. MPEG kodlayıcının şifresiz durumda kaliteli görüntü verdiği parametreler için, şifreli durumda da kaliteli video dizileri elde edilmiştir.

Algoritmanın en önemli özelliklerinden biri, şifre çözümü için gerekli parametreleri içinde taşımasıdır. Temel olarak resim içinde seçilen bölgelerin ortalama parlaklık değerlerini kullanan parametre oluşturma ve iletme algoritması, MPEG kodlamasından kaynaklanan hatalara rağmen, alıcı tarafta şifreleme parametrelerini başarıyla kestirmektedir. Ayrıca altblok sınırlarında taşınabilen bağımsız bit dizileri ile, sisteme ait izleme yetkisi ve ek işlevler sağlayacak komutların taşınması mümkün kılınmıştır. Bu veri çok düşük hata olasılıkları ile taşınabilmektedir.

Sonuç olarak algoritma kendinden beklenen iki temel işlevi de başarı ile yerine getirmiştir. TV yayıncılığının yanısıra, MPEG kodlamasına dayanan farklı multimedya kanalları (DVD, VoD, PVR vb.) için de kullanılması mümkündür. Kişisel kopyaların farklılaştırılmasına yönelik kullanılarak telif haklarının etkin bir şekilde korunmasını sağlayacak uygulamalar geliştirmeye açıktır.

Kaynaklar

ISO/IEC 13818, (1996). Coding of Moving Pictures and Associated Audio (MPEG-2); Part 1: Systems, Part 2: Video.

Mitchell J. L., Pennebaker W. B., Fogg C. E., LeGall D. J., (1996). *MPEG Video Compression Standard*, Chapman&Hall.