

## MPEG AKIMIMINDA BAŞLIK ŞİFRELEME

Deniz TAŞKIN\*, Cem TAŞKIN\*\* ve Nursen SUÇSUZ\*

(\*) Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, 22030, EDİRNE

(\*\*) Trakya Üniversitesi, Kırklareli Teknik Bilimler MYO, BTP Programı, 39100, KIRKLARELİ  
[deniztaskin@trakya.edu.tr](mailto:deniztaskin@trakya.edu.tr), [cemtaskin@trakya.edu.tr](mailto:cemtaskin@trakya.edu.tr), [nursen@trakya.edu.tr](mailto:nursen@trakya.edu.tr)

### ÖZET

Günümüzde, sayısallaştırılmış video dosyalarının büyük bir çoğunluğu sıkıştırılmış olarak depolanmakta ve dağıtılmaktadır. Sıkıştırılmış ortamda saklanan video dosyalarının güvenliği için güncel şifreleme algoritmaları kullanılmaktadır. Kullanılan algoritmaların gücü arttıkça bunları çözmek için gereken sistem kaynaklarında da artış olmaktadır. Geliştirilen yöntem sayesinde sıkıştırılmış bir video akımının tamamı yerine %1'lik bir kısmının şifrenmesi ile video akımının aynı seviyede güvenliği sağlanmıştır. Geliştirilen yöntem sayesinde artan güvenlik ihtiyaçları daha düşük bir maliyet ile karşılanmaktadır.

**Anahtar Kelimeler:** Mpeg akımı, Şifreleme, Mpeg başlıkları

### HEADER CRYPTING IN MPEG STREAM

#### ABSTRACT

Nowadays most of the digital video files are stored and distributed in compressed domain. For security of video files which are stored in compressed domain, current crypto algorithms are used. While strength of algorithms increases, system resources to resolve these algorithms will also increase. Despite of full stream, one percent of video stream cryption will provide same security level by using developed method. In assistance of given method, increasing security requirements will be covered by lower costs.

**Keywords:** Mpeg Stream, Crypting, Mpeg headers.

### 1. GİRİŞ

Sayısal video görüntüsü kullanımına paralel olarak artan depolama ve bant genişliği ihtiyaçları yüzünden video dosyaların çok büyük bir çoğunluğu sıkıştırılmaktadır. Sıkıştırılmış video görüntüleri düşük miktarda yer kaplarken, iletimde de kolaylıklar sağlamaktadır. Yüksek sıkıştırma ve görüntü kalitesi sağlayan Mpeg yöntemi çoğu kullanıcı ve yayıncı tarafından tercih edilmektedir.

Sayısal ortamda saklanan video dosyalarının şifrenmesi için özel olarak kullanılan algoritmalar bulunmazken, mevcut şifreleme algoritmalarının yayıncı kuruluşlar tarafından sayısal uydu yayınlarını şifrelemek amacıyla kullandıkları Cryptoworks, Nagravision, Viaccess gibi özelleştirilmiş sürümleri bulunmaktadır.

İster depolanmış video verisini ister canlı video verisini şifrelemek için tasarlanmışlar, kullanılan bütün şifreleme algoritmaları verinin bütününe şifreleyerek güvenlik altına almak zorundadırlar. Bu yüzden dosya boyutlarındaki ve kullanılan şifreleme anahtarlarının uzunluğundaki artış ile birlikte artan sistem maliyetleri olmaktadır.

Bu gerçekleştirilen çalışmada Mpeg yöntemi ile sıkıştırılmış video dosyalarına özel bir şifreleme yaklaşımı geliştirilmiştir. Video bütününe ait -yüzde bir gibi- çok düşük miktardaki verinin mevcut şifreleme metotları kullanılarak şifrenmesi sonucunda video bütününe tamamının güvenliği sağlanmıştır.

### 2. MPEG SIKIŞTIRMA YÖNTEMİ

Bir video akımının Mpeg sıkıştırma yöntemiyle sıkıştırılması hazır çorbaya benzetilebilir. Çorba paketlenirken taşıma ve

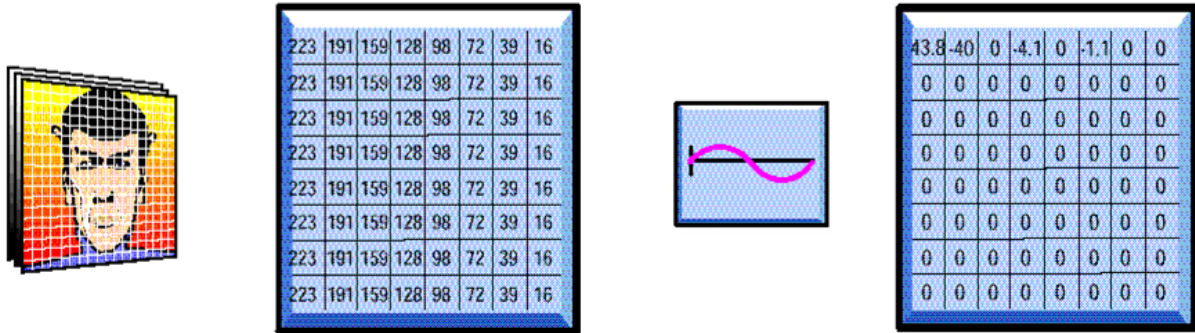
saklamayı daha etkin yapmak için tüm su buharlaştırılarak ayrıştırılır. Kurutulmuş hazır çorba paketi müşteriye ulaştığında karışıma su eklenerek çorba yeniden oluşturulmaktadır. Mpeg sıkıştırma yöntemi ses ve görüntü akımından gereksiz bilgileri çıkartarak sinyali orijinal boyutundan 180 kez daha küçük hale getirir. Gösterim sırasında sıkıştırılmış veriden orijinal görüntü elde edilir. [2]

Video verisi sayısallaştırıldığında sıkıştırma işlemi başlar. Mpeg yöntemi kendi içerisinde birden çok sıkıştırma metodu ve iyileştirme işlemi kapsamaktadır. Video sıkıştırması kullanılarak resim kalitesinde kabul edilebilir bir düşüş ile birlikte orijinal sinyalin %98'i atılabilir.

Mpeg video sıkıştırması iki temel sıkıştırma yöntemi içermektedir: uzaysal kodlama ve geçici kodlama. [4] Uzaysal kodlama video çerçevesindeki ardışık piksellerdeki, fazlalığı yok eder, geçici kodlama ise video akımındaki çerçeveler arasındaki fazlalığı en aza indirir.

## 2.1. Uzaysal Kodlama

Uzaysal kodlama bir resmin düz alanlarındaki piksel gruplarındaki benzerlikleri temel alır. Örnek olarak mavi gökyüzü arka planına sahip bir sahne birçok benzer renk değerine sahip sütunlardan oluşacaktır. Uzaysal kodlama bu piksel grubundan sadece bir tanesini kodlar ve ardından diğerlerinin buna benzer olduklarını belirtir. Böylece bit akımından fazla veri atılır.



Şekil 1. Ayrık kosinüs dönüşümü

Uzaysal kodlama işlemi aşağıdaki adımlardan oluşur.

- 1- Ayrı kosinüs dönüşüm
- 2- Nicelendirme
- 3- Ağırlıklandırma
- 4- Tarama
- 5- Entropi Kodlama

## 2.2. Geçici Kodlama

Geçici kodlama video akımındaki sıralı çerçevelerdeki fazlalıkları yok eder. Örnek olarak futbol oyununu gösteren bir video verilebilir. Oyuncular çerçeveden çerçeveye hareket ederken, arka plan sahnesi değişmez. Geçici kodlama birbiri ardına gelen çerçevelerdeki benzerlikleri değerlendirir ve çerçeveler arasındaki farklılıkları kodlar. Bu kodlama iki farklı şekilde gerçekleşmektedir: ara çerçeve tahmini ve hareket tahmini.

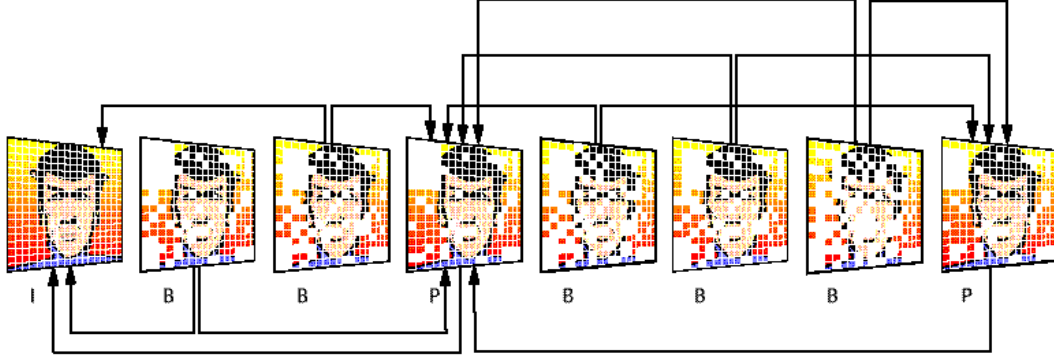
### 2.2.1. Ara çerçeve tahmini

Sıkıştırılmamış video dosyalarının aksine Mpeg yöntemi ile sıkıştırılmış video dosyalarında 3 farklı çerçeve tipi vardır. Bu sayede birbirini takip eden çerçeveler arasında az bir görsel fark olması durumunda çerçevenin tamamı dosyaya aktarılmaz. Ara çerçeve tahmini ardıl çerçevelerdeki benzerlikleri avantaj olarak kullanır. Öncelikle tam bir referans çerçeve seçilmekte ve ardından takip eden çerçeveler bu referans çerçeve ile olan farklılıklar kodlanmak suretiyle ifade edilmektedir. Referans çerçeveye ara kodlanmış çerçeve ya da "I-çerçevesi" denilmektedir. I-çerçevesi P ve B tipi çerçeveleri tahmin etmek için kullanılırlar.

a) I çerçevesi: Tam bir video resmidir. Gösterilebilmesi için başka bir resme ihtiyaç yoktur. En çok veriyi kapsamaktadır.

b) P çerçevesi: Bir önceki çerçevedeki farklılıkları şifrelemektedir. Gösterilebilmesi için bir önceki çerçeveye ihtiyaç duyar. B çerçevesinden daha fazla yer kaplamaktadır.

c) B çerçevesi: Bir önceki yada daha sonraki çerçevedeki farklılıkları şifrelemektedir. I çerçevesindeki verinin en az %25ini içerir. Gösterilebilmesi için bir önceki ya da sonraki çerçeveye ihtiyaç duyar.[5]

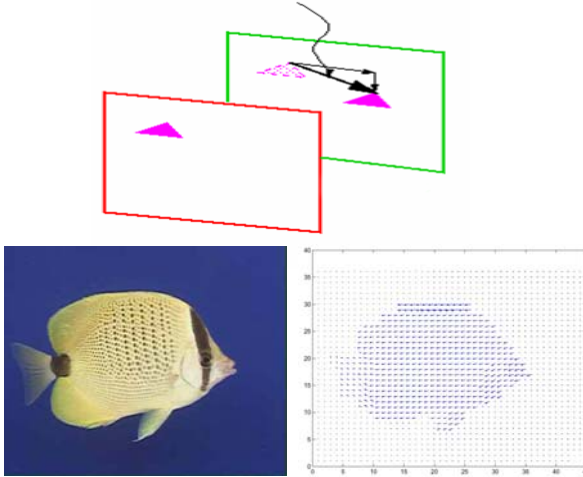


Şekil 2. Mpeg Çerçeve Tipleri

### 2.2.2. Hareket tahmini

Nesnelerin ekrandaki konumları değişirken genellikle görünümünde bir değişiklik olmamaktadır. Hareket tahmini bu benzerliğin avantajını, nesnenin kendisini kodlamak yerine hareketini kodlamak suretiyle kullanmaktadır. Tipik olarak hareket, birden çok çerçeve arasında devam eder bu sayede nesnenin sürekli yeniden kodlanması gerekmemektedir. [2]

parçacıkları oluşturulabilir ve yine bunların izlenebilmesi için ana video bütününe ihtiyaç duyulmaz. Esnek dosyalama yapısını Mpeg başlıkları sağlamaktadır. Bütün başlangıç kodları yirmi üç adet 0 ve bir adet 1'den oluşan 3 byte'lık bir öne ek alırlar. Bunun ardından gelen son byte farklı başlangıç kodlarının kimliğini belirler. Mpeg akımında başlangıç kodları dışında buna benzer bir dizilime izin verilmez. Tablo 1'de bazı başlangıç kodları verilmiştir. [6]



Şekil 3. Hareket vektörü, örnek nesne ve hareket vektörleri

### 3. MPEG AKIMININ ÇÖZÜLMESİ

Etkin bir sıkıştırma yöntemi olması dışında Mpeg sıkıştırma yöntemi aynı zamandan dosya deseni bakımından esnektir. Bir video bütününden kopartılan belli bir sürelik video parçasığı kendi başına izlenebilir. Bu video parçacıkları birleştirilerek daha büyük video

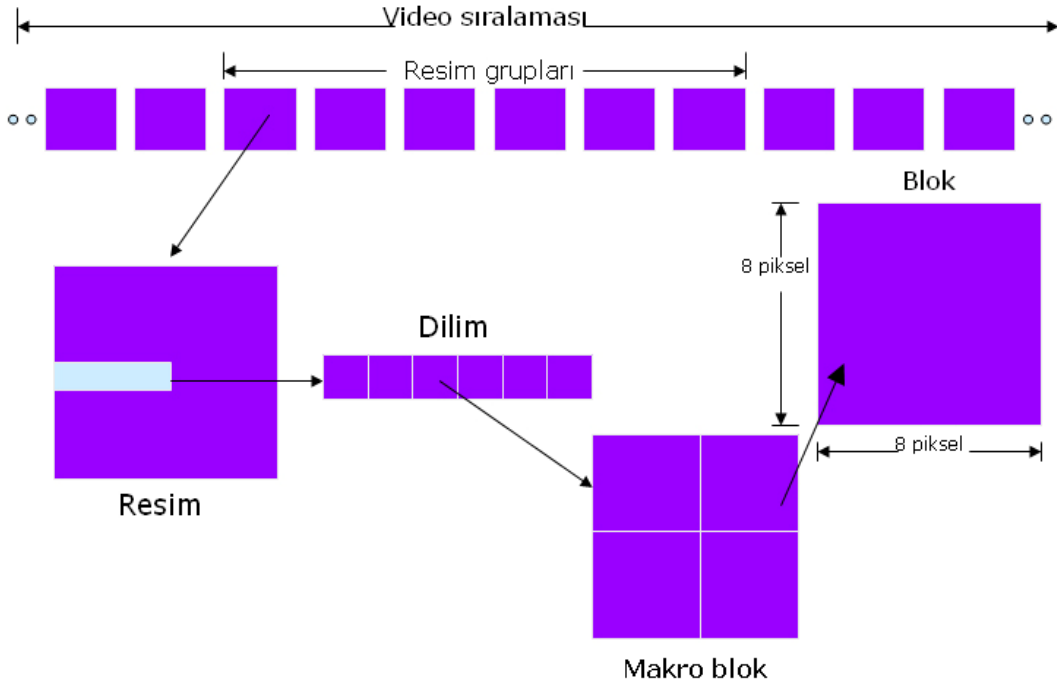
Tablo 1. Mpeg video başlıkları

Kod Adı	Değeri (Hex)
Resim grubu	0 0 1 B8
Resim	0 0 1 0
Sıralama bitişi	0 0 1 B7
Sıralama hatası	0 0 1 B4
Sıralama başlangıcı	0 0 1 B3
Dilim 1-	0 0 1 1 -
Dilim 175	0 0 1 AF
Kullanıcı verisi	0 0 1 B2

Bir video akımının çözülebilmesi için sıralama başlangıç kodunun bulunması gerekmektedir. Bunun ardından resim grubu başlangıç kodu aranmaktadır. Resim grubu başlangıç kodu bulunduktan sonra resimlerin çözülmesi işlemine başlanır. Resimleri belirlemek için "0 0 1 0" hex değeri, akım içinde aranır. Resmi oluşturan verilerin bulunduğu konum bu başlık değeri sayesinde belirlenir. Videoyu oluşturan resimlerin yeniden izlenebilir hale gelebilmesi için

öncelikle dilimler, ardından makro bloklar ve blokların çözülmesi gerekmektedir. Bunların çözülebilmesi için yine başlık bilgilerine

ihtiyaç duyulmaktadır. Şekil 4.'te sıkıştırılmış videoyu oluşturan katmanlar görülmektedir. [3]



Şekil 4. Mpeg video katman yapısı

#### 4. MPEG AKIMININ ŞİFRELENMESİ

Mpeg olarak sıkıştırılmış bir video akımı mevcut şifreleme algoritmaları kullanarak şifrelenebilir. Mevcut güvenliğin artırılması amacıyla şifreleme ve açma anahtar uzunlukları büyütülebilmektedir. Fakat bu işlem şifreleme ve çözme işlemlerinin maliyetini arttırmaktadır.

Mpeg akımının çözülmesi işleminin adımları incelendiğinde videonun tekrardan izlenebilir hale gelebilmesi için, Mpeg başlıklarının ne kadar hayati bir önem taşıdığı görülmektedir. Aşağıda bir resme ait bir dilim başlangıcı ve dilime ait bazı kodlar verilmiştir.

00	00	01	01	4A	BB	D1	40	04	E0	0F	50
10	FF	E4	60	22	80	27	40	9A	00	6D	F1
C7	11	45	EB	9D	4D	3F	32	9D	83	60	43
7E	98	C6	F8	11	1A	AF	B0	AA	3F	8C	21
36	9A	16	D1	1A	B7	80	00	72	24	02	50
08	30	90	C4	00	E4	48	04	BE	98	48	6D
EC	CD	6A	1A	D6	DF	34	00	E4	48	04	BE

Şekil 4. 1 numaralı dilim

Dikkat edilecek olunursa “00 00 01 01” byte dizisi 1 numaralı dilimin başlangıcını belirtmektedir. Bu başlık değeri dışında bu verinin birinci dilime ait olduğu gösteren başka bir işaret bulunmamaktadır. Eğer bu başlık değeri akımdan çıkartılır ise veya başlık değeri kasıtlı biçimde bozulursa video akımının yeniden izlenebilir hale getirilmesi imkânsızdır.

00	00	01	01	4A	BB	D1	40	04	E0	0F	50
W	X	Y	Z	4A	BB	D1	40	04	E0	0F	50

Şekil 5. Orijinal ve şifrelenmiş Mpeg akımları

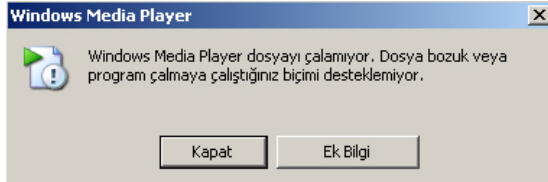
Geliştirilen yöntemde şifreleyici bir yazılım yardımıyla izlenebilir Mpeg akımındaki tüm başlık değerleri rastlantısal değerlerle değiştirilir. Şifreleme işlemi sonucunda akımın orijinal başlıkları farklı bir anahtar dosya içine kaydedilmektedir. Anahtar dosya olmaksızın şifrelenmiş video akımını izlemek hiçbir şekilde mümkün değildir.

Şifre çözücü yazılım kısmında, anahtar dosyada bulunan başlık değerleri kullanılarak şifresi çözülmüş video akımı yeniden oluşturulur.

## 5. SONUÇ

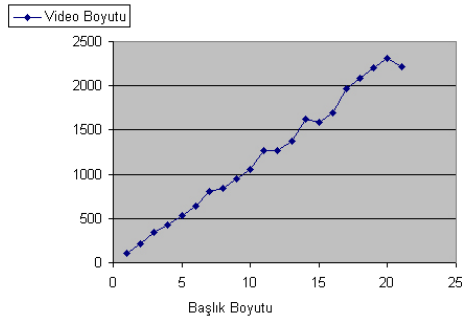
Başlık verileri tahrip edilmiş bir Mpeg dosyasının izlenmesi mümkün değildir. Başlıkları bozulmuş bir video akımını izlenebilir kılan henüz bir metot geliştirilmemiştir. Bu avantajları kullanarak yöntem çok küçük bir veriyi şifreleyerek bir veri bütününe anahtar dosya olmadan, anlamsız ve kullanılamaz hale getirmiştir.

Anahtar dosya mevcut şifreleme metotları kullanılarak şifrelendiğinde güvenlik son derece sağlam hale gelmektedir. Anahtar dosya şifrelenmediği durumda dahi anahtar dosyanın deseni bilinmediğinden dolayı şifre çözme işlemi gerçekleştirilemeyecektir.



Şekil 6. Şifrelenmiş akım izleme hatası

Şekil 7.de videoların kapladıkları dosya boyularına göre sistem başlıklarının kapladıkları alan verilmiştir.



Şekil 7. Video boyutuna göre toplam boşluk boyutları

Video boyutuna bağlı olarak başlıkların kapladığı toplam boyut da artmaktadır. Bu şifrelenecek veri miktarında da artışa neden olmaktadır. Buna rağmen başlık boyutları toplam video boyutunun yaklaşık yüzde birine eşdeğerdir.

## 9. KAYNAKLAR

- [1].CHANG, S., ‘Compressed Domain Techiques for Image/Video Indexing and Manipulation’, IEEE Conference On Image Processing, 1995

- [2].J. GILVARRY, ‘Extraction of Motion Vectors from an MPEG Stream’, 1999.

- [3].MENG, J., CHANG, S., ‘Tools for Compressed Domain Video Indexing and Editing’, SPIE Conference on Storage and Retrieval, 1995.

- [4].Mitchell, J.L., Pennebaker, W.B., Fogg, C.E. ve Legal, D.J., *Mpeg Video Compression Standard*, Chapman and Hall, 1996.

- [5].PATEL, N., SETHI, I., ‘Compressed Video Processing for Cut Detection’, 1996

- [6].Taşkın, D., Suçsuz, N., “Sıkıştırılmış ortamda çerçeve tipine dayalı gerçek zamanlı sahne değişimi belirleme”, IV. Bilgi teknolojileri Kongresi, 9-11 Şubat 2006, Pamukkale Üni.