http://fbe.trakya.edu.tr/tujs
Trakya Univ J Sci, 8(2): 73–79, 2007
ISSN 1305–6468
DIC: 235DTET820712070108

**Araştırma Makalesi / Research Article**

# MPEG AKIMINI GEÇİCİ REFERANS NUMARALARINI KULLANARAK ŞİFRELEME

Deniz TAŞKIN, Nurşen SUÇSUZ, Cem TAŞKIN
Trakya Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü 22100 EDİRNE, Tel: 0544 336 4938, e-posta: deniztaskin@trakya.edu.tr

Alınış: 28 Haziran 2007
Kabul Ediliş: 26 ekim 2007

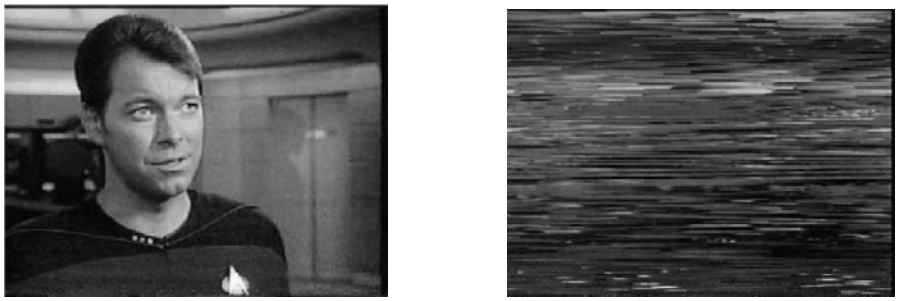
***Özet:*** *Bu çalışmanın amacı, sıkıştırılmış video verisinin güvenlik ihtiyaçlarını karşılayan düşük sistem gereksinimi gerektiren bir yöntem geliştirmektir. Video akımın sıkıştırılması ve açılması aşamaları sistem kaynaklarını kullandığından, şifreleme işlemi için kullanılan ağır algoritmalar, video verisinin gerçek zamanlılık gereksinimini karşılayamamaktadır. Önerilen yöntem, düşük sistem kaynak ihtiyacı ve karmaşıklık seviyesine karşılık sıkıştırılmış video akımına özel şifreleme, taşınabilirlik ve hız sağlamaktadır. Bunlara ilaveten şifrelenen veri miktarını düşürmekte ve şifrelenmiş akımın gerçek zamanlı olarak izlenebilmesine olanak vermektedir.*
***Anahtar Kelimeler:*** *MPEG, Şifreleme, Video kodlama, Video güvenliği*

## *Encrypting Mpeg Stream Using Temporal Referance Numbers*

***Abstract:*** *The aim of this study is to develop a method which meets the security needs of the compressed video and needs low system requirements. Since the compress of video stream and the opening process uses the system sources, heavy algorithms that are used for encryption aren't able to deal with the real time necessity of the video data. Proposed method provides special encryption for compressed video stream, mobility and speed for lower system requirements and complexity. Beside this, method reduces encrypted data mount and allows encrypted data to be watched real time.*
***Keywords:*** *MPEG, Encrypting, Video coding, Video security*

**Giriş**

Video verisi, miktar olarak çok fazla yer kaplamaktadır ve gerçek zamanlılık gibi gereksinimleri bulunmaktadır. Bu yüzden video verisinin şifrelenmesi için genellikle görsel bozulmalara dayanan basit şifreleme metotları kullanılmaktadır. Görsel bozulmaya dayalı şifreleme sistemleri video verisini şifreledikten sonra, görüntü bozuk olarak gösterildiğinden şekil.1'de olduğu gibi bozuk izlenmektedir.



**Şekil1**. Görsel şifreleme

Görsel olarak bozulmuş video verisi izleyiciye ulaştığında, görüntüyü çözmeye yarayan özel kod çözücü cihazlar yardımıyla görüntü tekrar izlenebilir hale gelmektedir. Görsel bozulmaya dayalı şifreleme sistemleri analog video verisine uygulanmaktadır.

Video verisinin kapladığı alanın büyük olması ve bant genişliği gereksinimlerinden dolayı sıkıştırılması gerekmektedir. MPEG video sıkıştırma yöntemi, günümüz video depolama ve iletiminin temelini teşkil etmektedir. Benzersiz ve yüksek sıkıştırma oranları MPEG video sıkıştırmasını vazgeçilmez kılmıştır. MPEG, büyük miktarda görsel veri içeren ve eşsiz bir yapıya sahip olan videonun özelliklerini kullanarak yüksek sıkıştırma oranlarını yakalamaktadır. Video dosyası sıkıştırıldıktan sonra açıldığında görüntüde fark edilemeyecek düzeyde bir kayıp söz konusudur. MPEG sıkıştırma yöntemi izleyici tarafından fark edilemeyecek alanlarda kaliteyi düşürerek sıkıştırılmış sinyalin kalitesini yüksek tutmaktadır. MPEG basitçe özetlendiğinde birbirini izleyen video çerçevelerinde büyük

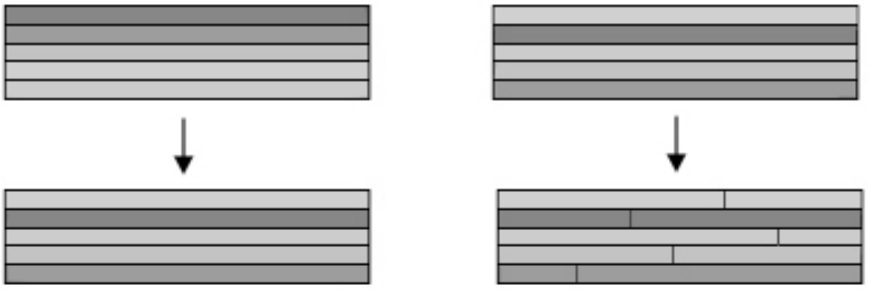
oranda tekrar eden benzerlikleri ve insan gözünün algılayamayacağı düzeydeki detayları yok sayarak yüksek oranda sıkıştırma sağlamaktadır (Mitchell, J.L. ve Ark. 1996).

Görsel bozulmalara dayalı şifreleme sistemleri (Nagravision,…) video verisinin görsel özelliklerini bozmaktadır. Görsel bozulmaya dayalı klasik şifreleme yöntemleri MPEG sıkıştırma yöntemi ile verimli sıkıştırılamazlar. Görsel özellikleri bozulmuş bir video akımı sıkıştırıldığında sıkıştırma oranı çok düşük olmaktadır. MPEG sıkıştırma yöntemi kayıplı bir sıkıştırma yöntemi olduğundan şifrelenmiş bir görüntünün sıkıştırıldıktan sonra şifresinin çözülmesi durumunda görüntüde büyük oranda bozulmalar görülmektedir.

Bu çalışma, video verisinin güvenlik gereksinimlerini karşılama için gerçek zamanlı ve sıkıştırma oranlarını düşürmeden çalışabilecek düzeyde yeni bir yöntemi öne sürmektedir. Geleneksel görsel bozulmaya dayalı şifreleme metodu ve kırılması Bölüm 2'de anlatıldıktan sonra Bölüm 3'te Mpeg video sıkıştırma metodundan bahsedilecektir. Ardından Bölüm 4'te Mpeg video çerçevelerinin özellikleri incelenecektir ve alternatif yöntem Bölüm 5'te anlatılacaktır. Çalışma, sonuçların Bölüm 6'da açıklanacaktır.

**Görsel Bozulmaya Dayalı Şifreleme**

Video verisi, miktar olarak çok fazla yer kaplamaktadır. Bu yüzden güvenliğinin sağlanmasında basit şifreleme metotları kullanılmaktadır. Buna örnek olarak, yakın bir zamana kadar üyelerine yayınlarını ücretli olarak sunmak için Nagravision sistemini kullanan ulusal bir televizyon kanalı verilebilir. Nagra Kudelski tarafından geliştirilen Nagravision sistemi analog video verisi üzerinde çalışmaktadır ve PAL televizyon yayınlarında kullanılmaktadır. Şekil.2 Nagravision şifreleme aşamalarını göstermektedir.



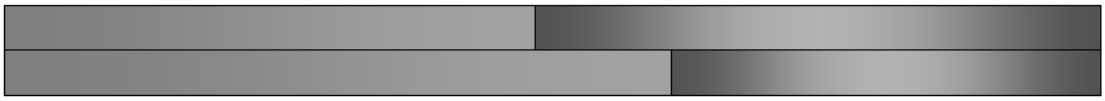
**a)** Blok karıştırma **b)** Yatay konumların değiştirilmesi

**Şekil 2**. Nagravision şifreleme aşamaları

Nagravision şifreleme metodu, görüntüyü satırlara ayırmakta ve yerlerini bloklar halinde karıştırmaktadır. Bu karıştırma işlemi video görüntüsünü oluşturan her bir kareye aynı şekilde uygulanmaktadır.

Şifreyi kırmak isteyen saldırgan blok karıştırma sırasını bir kez çözdüğü takdirde, bu sıra hiç değişmediğinden sistemi kolayca etkisiz hale getirebilmektedirler. Bu yüzden Nagravision şifreleme sisteminden sonra ikinci bir şifreleme aşaması kullanılmaktadır. İzleyiciye üyelik sistemi tarafından sağlanan akıllı kart üzerinde bulunan ikinci bir şifreleme algoritması, blokların yatay konumlarını 256 farklı kesim noktasından birisini kullanarak değiştirmektedir. Saldırgan için tamamen rastlantısal sayılabilecek olan bu kesim noktaları akıllı kart olmadan belirlenememektedir.

Bu şifreleme sistemi günümüzde teknolojinin gelişmesi ile; uygun şifre çözücü cihaz ve akıllı kart kullanılmadan yazılım ile gerçek zamanlı kırılabilmektedir. Çok fazla karmaşıklık içermeyen şifreleme sistemi yine 2 adımda kırılmaktadır. Yerleri değiştirilen blokların yer değiştirilme sırasının sabit olması, sistemin en zayıf olduğu noktasıdır. Deneme yolu ile bu sabit dizilimi belirlemek mümkündür. Şekil.3 blokların örnek parlaklık değerlerini göstermektedir.



**Şekil 3**. Örnek blok parlaklık değerleri

Akıllı kart tarafından ise sistemin ikinci adımında gerçekleştirilen blokların kendi arasında yatay konumlarının kesilerek değiştirilmesi gerçekleştirilmektedir. Saldırgan, elinde akıllı kart olmadan 256 farklı değerden birisini tespit etmek için bloğun parlaklık değerlerini bir üst bloğun parlaklık değerleriyle karşılaştırmaktadır. Birbirine çok yakın parlaklık değerleri elde edildiğinde blokların yatay konumları kolaylıkla belirlenmektedir.

Nagravision şifreleme sistemi, görsel bozulmaya dayanan ve çıktığı yıllarda son derece güvenli sayılan fakat son

yıllarda resim işleme metotları kullanılarak anahtar bilgisi olmadan kırılabilen bir şifreleme sistemi olarak anılmaktadır.

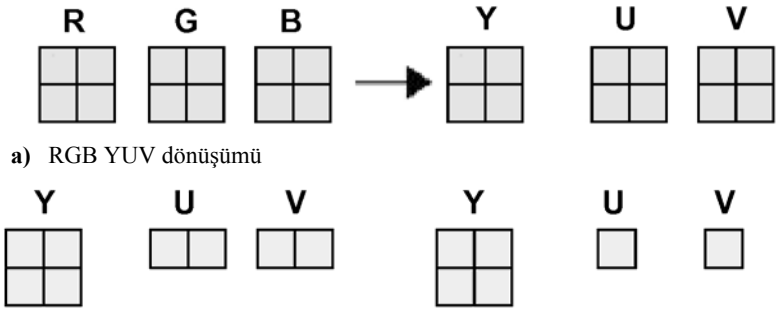
**MPEG Video Sıkıştırma Metodu**

MPEG sıkıştırma metodu, verideki fazla ve gerekli olmayan görüntü bilgisini yok ederek hareketli resim dizilerini kaydetmek için gerekli olan bellek miktarını önemli derecede azaltmaktadır. Saklama hacmi olarak toplamda daha az bit kullanılması hareketli resimlerin çok daha hızlı bir şekilde transfer edilmesi anlamına gelmektedir. Böylece pahalı haberleşme hatların ve depolama cihazları bu yeni hareketli resim uygulamalarında daha verimli kullanılmaktadır. MPEG sıkıştırma metodu, kullandığı birçok yöntem sayesinde yüksek sıkıştırma oranları yakalamaktadır.

Bir hareketli resim dizisindeki iki komşu çerçeve genellikle birbirlerine çok benzerler. Resmin bazı kısımları çerçeveler arasında çok küçük miktarda yer değiştirmektedir. MPEG sıkıştırma metodu her yeni çerçeveyi uygun bir şekilde bölümlere ayırıp, bu bölümlerin nereden geldiğini belirlemek için bir önceki çerçeveyi araştırarak meydana gelmiş olan zamansal fazlalıkları atmaktadır. Bir çerçevenin içeriğinin çoğu bir önceki çerçevede de bulunuyorsa, o çerçevenin tekrardan gönderilmesi depolama ve aktarım kaybı yaratmaktadır. Bütün çerçeveyi göndermek yerine, bir önceki çerçeve referans alınarak farklılıkların gönderilmesi akım hacmini düşürmektedir.

Tek bir çerçeve içindeki, gökyüzü ya da duvar bölgeleri gibi birçok parça tamamıyla aynı renktedir. MPEG sıkıştırma, görüntüyü uygun bir şekilde bölümlere ayırarak ve gökyüzü, duvar gibi parçaları tek bir renge indirgeyerek fazlalıkları atmaktadır.

İnsan gözü, bir noktadaki parlaklık değişikliğini renk değişikliğine göre daha çok fark etmektedir. MPEG sıkıştırma metodu, RGB renk uzayını YUV renk uzayına dönüştürerek UV ile temsil edilen renkleri daha az yer kaplayacak şekilde daraltmaktadır. Y ile temsil edilen parlaklık değerleri ise insan gözünün parlaklık değişikliklerine olan yüksek hassasiyetinden dolayı değiştirilmemektedir. Şekil.4 RGB renk uzayından YUV renk uzayına dönüşümü ve sıkıştırma işlemini göstermektedir.




**a)** RGB YUV dönüşümü

**b)** 4:2:2 sıkıştırma **c)** 4:2:0 sıkıştırma

**Şekil 4**. Renk uzayı dönüşümleri ve sıkıştırma

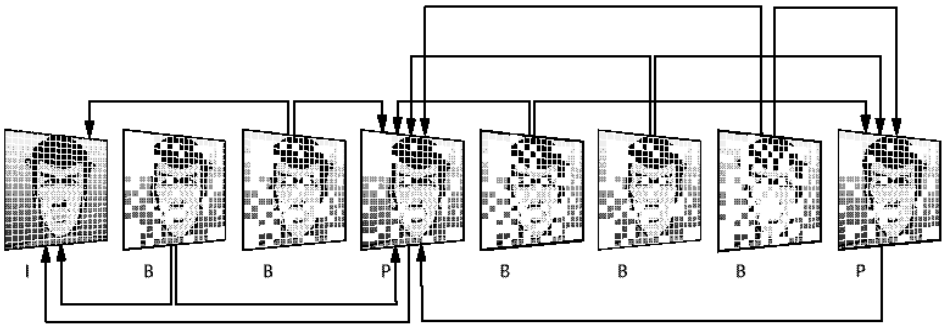
**Ara çerçeve tahmini**

Sıkıştırılmamış video dosyalarının aksine MPEG yöntemi ile sıkıştırılmış video dosyalarında 3 farklı çerçeve tipi vardır. Birbirini takip eden çerçeveler arasında az bir görsel fark olduğunda çerçevenin tamamı dosyaya aktarılmaz. Ara çerçeve tahmini, ardıl çerçevelerdeki benzerlikleri avantaj olarak kullanmaktadır. 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 kullanılmaktadır. Şekil.5'te bu çerçeveler ve aralarındaki ilişkiler gösterilmektedir.

**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 I çerçevesine ihtiyaç duymaktadır. B çerçevesinden daha fazla yer kaplamaktadır.

**c)** B çerçevesi: Bir önceki yada daha sonraki çerçevedeki farklılıkları kodlamaktadır. I çerçevesindeki verinin en az %25ini içermektedir. Gösterilebilmesi için bir önceki ya da sonraki P çerçevesine ihtiyaç duymaktadır.




**Şekil 5.** Mpeg Çerçeve Tipleri

**MPEG Video Çerçeveleri**

MPEG video akımında görüntüyü izlenebilir hale getiren birime, kod çözücü denilmektedir. Kod çözücü birim, bir uygulama yazılımı olabildiği gibi akıma özel tasarlanmış bir donanım da olabilmektedir. Bu birimin MPEG sıkıştırma yönteminde kullanılan tüm sıkıştırma aşamalarını eksiksiz olarak yerine getirmesi gerekmektedir. Şekil.6'da örnek bir video akımında çerçeve tiplerine göre sıralanışı gösterilmektedir.

| Sıra | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10I | 11 | 12 | 13 | 14B | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Çerçeve Tipi | I | B | B | P | B | B | B | B | B | | B | B | P | | B | P |

**Şekil 6.** Örnek Video Akımı

Video akımının izlenebilir olması için aşılması gereken sorunlardan biri, MPEG video çerçevelerinin sıralanması işlemidir. MPEG akımında 3 tip çerçeve bulunmakta, B ve P tipi çerçevelerinin gösterilebilmesi için referans çerçevelere ihtiyaç duyulmaktadır. Şekil.6'da yer alan 2. çerçeve olan B çerçevesinin gösterilebilmesi için 4. çerçeve olan P çerçevesine ihtiyaç duyulmaktadır. Kod çözücü birimin 2. çerçeveyi gösterirken 4. çerçeveye ait bilgilere de kullanmak zorundadır. Sıralar ardıl olmadığından bu sorunun aşılması için; MPEG video akımında çerçevelerin gösterim sırası ile akım içindeki sıraları farklı tutulmaktadır. Şekil.7'de örnek bir video akımında bu sıralar gösterilmektedir.

| Sıra | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10I | 11 | 12 | 13P | 14 | 15 | 16P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Çerçeve Tipi | I | B | B | P | B | B | P | B | B | | B | B | | B | B | |

**a)** Gösterim sırası

| Sıra | 1 | 4 | 2 | 3 | 7 | 5 | 6 | 10I | 8 | 9 | 13P | 11 | 12 | 16P | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Çerçeve Tipi | I | P | B | B | P | B | B | | B | B | | B | B | | B | B |

**b)** Akım sırası

**Şekil 7.** Video gösterim ve akım sıraları

Mpeg dosyalarında kod çözücü birimin gösterim sıralarını tespit edebilmesi için, *geçici referans numarası* adı verilen 10 bitlik bir numara ve 3 bitlik çerçeve tipi ile ilgili bir bilgi şekil.8'de olduğu gibi, çerçevenin içeriğinden önce ikili kodlanmış akıma dâhil edilmektedir.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 9 | 10 | | | | | | |
| Geçici Referans Numarası | | | | | | | |
| | | 11 | 12 | 13 | | | |
| Çerçeve Tipi<br>001=I Çerçevesi<br>010=P Çerçevesi<br>011=B Çerçevesi | | | | | | | |

**Şekil 8.** Geçici referans numarası ve çerçeve tipi bit dağılımı

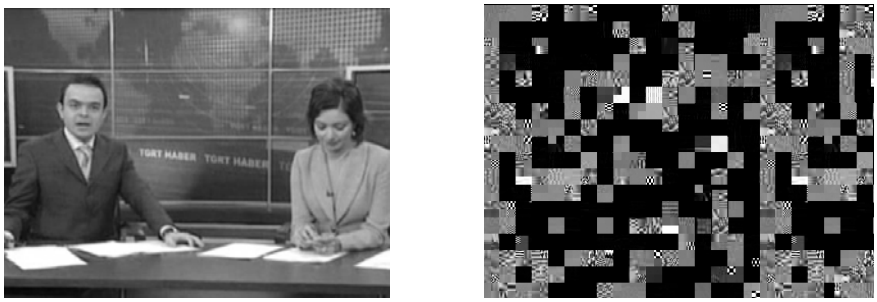
**MPEG Akımının Şifrelenmesi**

MPEG akımında görsel bozulmaya dayalı şifreleme işlemi yapmak kayıplı bir sıkıştırma metodu olduğundan uygun değildir. Ayrıca görsel bozulmaya dayalı şifreleme sistemlerinin video işleme metotları kullanarak kırılabileceği yukarıda açıklanmıştır. Bu yüzden, görsel bozulmaya dayalı bir şifreleme algoritması kadar basit ve düşük maliyetli bir şifreleme için MPEG sıkıştırma algoritmasına uyumlu bir metot geliştirilmelidir.

Sıkıştırılmış video akımının şifrelenmesi için Taşkın ve Ark. (2007) tarafından yapılan bir çalışma akımın tamamının şifrelenmesi durumunda ortaya çıkan güvenlik zaaflarını açıkça göstermektedir. Kendine has bir yapısı olan Video verisinin düz metin gibi şifrelenmesi, şifreyi çözmek isteyen saldırgana açık noktalar bırakmaktadır. Çalışma, akımın bütününün yerine belli bir kısmının şifrelenmesinin daha fazla güvenlik sağlayacağını açıkça göstermektedir.

MPEG akımını şifrelemek için geliştirilen diğer bir yaklaşımda, akımın gösterilebilmesi için hayati önem taşıyan başlık bilgilerinin akımdan çıkartılması şeklindedir. Akımın yaklaşık %1'ini içeren başlık bilgileri akımdan çıkartılıp başka bir dosyada tutulmaktadır. Başlık bilgilerinin akımdan çıkartılması akımı bozmakta ve kod çözücü birim için anlamsız bir dosya haline getirmektedir. Kod çözücü birim yapısı bozulmuş akımı işleyememekte ve akımda hata olduğunu kullanıcıya iletmektedir. Bu yöntemin dezavantajı da, akımın yapısı tamamen bozulmakta ve başlık bilgilerini tutacak ikinci bir dosyaya ihtiyaç duyulmaktadır (Taşkın ve Ark. 2007).

MPEG video akımının doğru olarak gösterilebilmesi için geçici referans numaraları çok önemlidir. Bir MPEG video akımında her bir çerçevenin geçici referans numarası bulunmaktadır. Saniyede 30 çerçeve gösterim oranına sahip bir akımda, bir dakikalık görüntüde yaklaşık 2KB yer kaplayan 1800 adet geçici referans numarası vardır. Geçici referans numarası bilinçli şekilde bozulmuş bir video akımının şifreli olduğu kod çözücü birim tarafından fark edilememektedir. Kod çözücü birim hatalı referans numaralarını kullanarak akımın kodunu çözdüğünde görsel olarak bozuk bir görüntü elde edilmektedir. Şekil.9'da kod çözücünün şifreli görüntüyü nasıl gösterdiği görülmektedir.



**a)** Orijinal görüntü **b)** Şifrelenmiş görüntü

**Şekil 9.** Orijinal görüntü ve bit kaydırma işlemi sonrası izlenebilen görüntü

Referans numaralarının bilinçli şekilde bozulması için bit kaydırma işlemi gerçekleştirilmiştir. Geliştirilen metotta referans numarası içeren 10 bitlik veri bir sonraki 10 bitlik veri ile yer değiştirilmektedir. Bit bazında, akım çözülmeden yer değiştirme işlemi yapıldığından yöntemin kaynak ihtiyacı çok düşük olmaktadır.

```
C7 00 F7 D5 82 D8 00 00  01 00 00 D7 38 03 80 00
00 01 B5 81 1F F3 51 80  00 00 01 01 4A 27 0A 0D
7F F6 71 04 7A 49 23 DC  78 AA 91 01 74 78 E9 85
B6 17 6A 0A 0C 60 03 05  E8 00 7F 1C 2E A8 27 13
C5 41 60 3E 89 E1 78 07  93 80 6F 1C 2E D5 00 2E
8F 60 39 00 BC 44 B0 1F  F1 D1 C3 BD E8 3C 8E 64
```

**a)** Resim başlangıç kodu

**00 D7 38**

0000 0000 1101 0111 0011 1000
0101 1100 1110 0000 0000 0011

**5C E0 03**

**b)** Byte akımının şifrelenmesi

```
C7 00 F7 D5 82 D8 00 00  01 00 5C E0 03 03 80 00
00 01 B5 81 1F F3 51 80  00 00 01 01 4A 27 0A 0D
7F F6 71 04 7A 49 23 DC  78 AA 91 01 74 78 E9 85
B6 17 6A 0A 0C 60 03 05  E8 00 7F 1C 2E A8 27 13
C5 41 60 3E 89 E1 78 07  93 80 6F 1C 2E D5 00 2E
8F 60 39 00 BC 44 B0 1F  F1 D1 C3 BD E8 3C 8E 64
```

**c)** Şifrelenmiş akım

**Şekil 10.** Bit kaydırma işlemi ile şifrelenmiş akım

Akımın tümünün geleneksel şifreleme metotlarıyla şifrelenmesi video verisinin gerçek zamanlılık ihtiyacından dolayı mümkün olmamaktadır. Güvenliği daha da yüksek tutmak için bit değişim işlemi dışında, geçici referans numaralarını bozabilecek geleneksel şifreleme yöntemi kullanılabilmektedir. Bu sayede akımın belli bir kısmı geleneksel şifreleme algoritmalarıyla şifrelenmekte ve zaman kayıpları en düşük düzeyde tutulmaktadır.

**Sonuçlar**

Burada önerilen yöntem ve diğer şifreleme yöntemleri aynı dosyaya uygulanmış ve elde edilen sonuçlar aşağıda tablo.1'de gösterilmiştir.

**Tablo 1**. MPEG dosyalarında şifreleme yöntemlerinin hızları

| **Yöntem** | **Yöntem Türü** | **Dosya Boyutu** | **Şifreleme Zamanı(sn)** | **Hız (Mbit/s)** |
|---|---|---|---|---|
| RSA (8 Bit anahtar) | Geleneksel | 309MB | 47.23 | 52 |
| MPEG akımında başlık şifreleme | Kısmi | 309MB | 27.89 | 89 |
| MPEG akımında operatör işlemleri-nin kısıtlanması yoluyla içerik koruma | Kısmi | 309MB | 26.50 | 93 |
| Başlık dışında şifreleme | Geleneksel + Kısmi | 309MB | 46.82 | 52 |
| Seçimli XOR işlemi ile MPEG video akımını koruma | Kısmi | 309MB | 27.71 | 89 |
| Byte dağılımını değiştirerek MPEG video akımını koruma | Kısmi | 309MB | 26.22 | 94 |
| Sıkıştırılmış video akımının düzensiz haritalar ve başlangıç kodlarına dayalı şifrelenmesi | Kısmi | 309MB | 30.60 | 81 |
| Önerilen Yöntem | Kısmi | 309MB | 26.40 | 93 |

Sonuç olarak önerilen yöntem, geleneksel yöntemin yaklaşık iki katı şifreleme hızına ulaşmaktadır. Gerçek zamanlı uygulamalar için yöntemin hızı yeterli seviyededir.

**Tartışma**

Bu çalışmada MPEG video akımının şifrelenmesi üzerine yeni bir yaklaşım önerilmektedir. Yeni geliştirilen yöntem, MPEG kodlama yapısına özel geliştirildiğinden, veri bütünün şifrelenmesi gereken kısımlarını kendisi belirlemektedir. Video akımının tamamı şifrelenmediğinden ve akımın kodu çözülmeden bit düzeyinde işlemler içerdiğinden önerilen yöntemin kaynak ihtiyacı çok düşük olmaktadır. Geçici referans numaralarının şifrelenmesi MPEG akımının yapısını bozmamakta ve şifrelenmiş akım kod çözücü birim tarafından bozuk şekilde de olsa gösterilebilmektedir. Görsel olarak şifrelenmemesine rağmen kodu çözüldüğünde görsel olarak bozukluk yaratan yöntem, şifreyi kırmaya çalışan saldırganları da yanıltmaktadır.

**Kaynaklar**

Kuhn, M. G., Analysis of the nagravision video scrambling method, 1998

Taşkın, D., Sucsuz, N. ve Taşkın, C., Sıkıştırılmış video güvenliği, *e-Journal of New World Sciences Academy*, Volume: 2, Number:3 (Basımda), 2007

Taşkın, D., ve Suçsuz, N., Sıkıştırılmış ortamda çerçeve tipine dayalı gerçek zamanlı sahne değişimi belirleme, IV. Bilgi teknolojileri Kongresi, Denizli, 2006

Taşkın, D., Taşkın, C., and Suçsuz, N., MPEG akımında başlık şifreleme, Akademik Bilişim, Kütahya, 2007

Taşkın, D., Taşkın, C., and Suçsuz, N., MPEG akımında operatör işlemlerinin kısıtlanması yoluyla içerik koruma, Akademik Bilişim, Kütahya, 2007

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

Chang, S., Compressed Domain Techiques for Image/Video Indexing and Manipulation, IEEE Conference On Image Processing, 1995

Gilvarry, J., Extraction of Motion Vectors from an MPEG Stream, 1999

Meng, J., and Chang, S., Tools for Compressed Domain Video Indexing and Editing, SPIE Conference on Storage and Retrieval, 1995

Patel, N., and Sethi, I., Compressed Video Processing for Cut Detection, 1995

Rivest, R., Shamir, A., and Adleman, L., A method for optaining digital signatures and public-key cryptosystems, Communications of ACM, 1978

Coppersmith, D., The data encryption Standard (DES) and its strenght against attacks, IBM journal of research and development, 1994

RSA Laboratories, Frequently asked questions about today's cryptography, 2000