

MPEG AKIMINDA I ÇERÇEVELERİNİN ŞİFRELENMESİ

Deniz TAŞKIN

Trakya Üniversitesi
deniztaskin@trakya.edu.tr

Cem TAŞKIN

Trakya Üniversitesi
cemtaskin@trakya.edu.tr

Nurşen SUÇSUZ

Trakya Üniversitesi
nursen@trakya.edu.tr

ABSTRACT

Encrypting video stream is an important problem of digital word. Encryption weight and encryption level change by user requirements, bandwidth and system limits. Situation requires higher security level, requires heavy algorithm that means higher processing costs also. Selective encryption will provide higher security levels by appropriate costs. In this work, *I frame* the most valuable part of compressed stream is encrypted.

Key words: MPEG, compression, encryption, selective encryption

1. GİRİŞ

Teknolojinin gelişmesi ve görselliğin ön plana çıkması ile 1990'lı yılların ortalarından itibaren internet ses ve görüntü akımı pazarı hızla gelişmeye başlamıştır. Başlangıçta tasarlanan şifreleme sistemleri, ses ve görüntü gibi büyük veriler içeren ortamlar için amaçlanmamıştır.

Genel güvenli bir akıcı medya servisi aşağıdaki maddelerden bazılarını ya da hepsine ihtiyaç duymaktadır.

- Kullanıcı ve sunucu kimlik doğrulaması
- Medya şifreleme
- Hak yönetimi
- Anahtar dağılımı

Günümüzde en çok kullanılan video sıkıştırma yöntemi MPEG video sıkıştırma yöntemidir. MPEG sıkıştırma metotları dosya boyutlarını maksimum sıkıştırma oranları 240:1 ile sıkıştırılmaktadır[13]. Normal görüntü üzerinde şifreleme yapmak yerine sıkıştırılmış veri üzerinde şifreleme yapmak bu açıdan çok avantajlıdır.

2. MPEG ŞİFRELEME

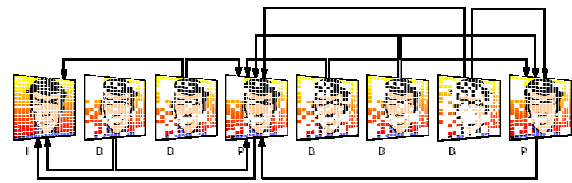
MPEG akımının şifrenmesi için birçok yöntem önerilmektedir. Bu yöntemler farklı güvenlik seviyeleri sağlamaktadırlar. Video çok büyük miktarda veri içerdiğinden şifrenmesi işlemi, normal verilerin şifrenmesinden daha fazla gereksinime ihtiyaç duymaktadır. Kullanım alanına göre şifreleme için gereksinimler de değişmektedir. Örneğin depolama amacıyla saklanan video dosyalarının şifrenmesi için ağır ve zaman

gerektiren algoritmalar kullanılabilirken, gerçek zamanlı video görüntülerinin şifrenmesi için hafif algoritmalar tercih edilmektedir. Video görüntüleri şifrelendikten sonra sıkıştırıldığında, şifre çözme işlemi mümkün olmamaktadır. Bu yüzden şifreleme algoritmaları sıkıştırılmış domain'de çalışmak zorundadır.

Bu çalışmada gerçekleştirilen yöntem sıkıştırılmış domain'de I çerçevelerinin şifrenmesine dayanmaktadır. Kullanıcının tercihini sağlıklı yapabilmesi açısından çalışma sonuçlarında algoritmanın diğer yöntemler ile karşılaştırmaları verilmiştir.

3. MPEG ÇERÇEVE TİPLERİ

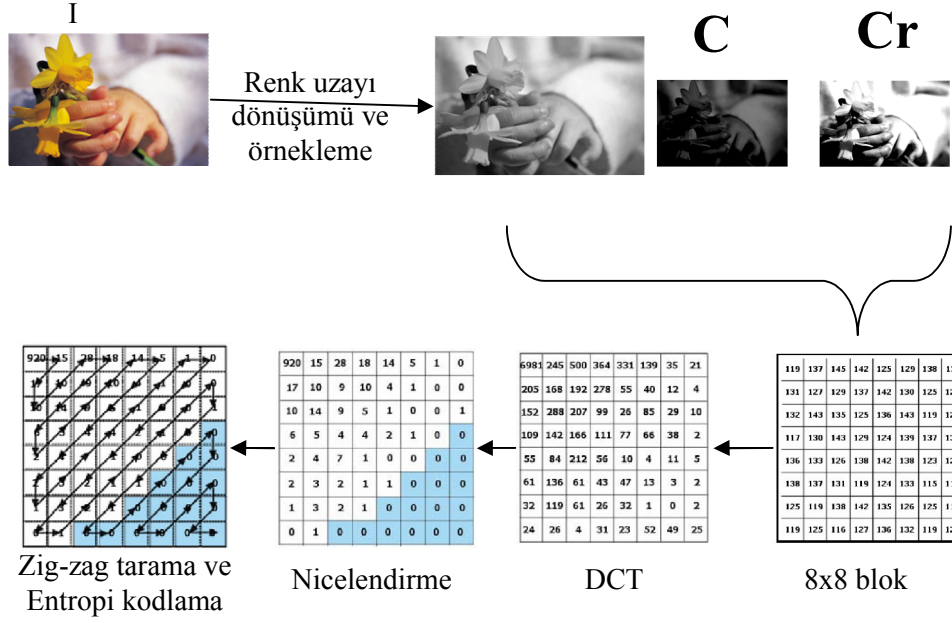
Sıkıştırılmamış video akımının aksine, MPEG sıkıştırma yöntemi ile sıkıştırılmış video akımında 3 farklı çerçeve tipi vardır. Bu sayede birbirini takip eden çerçeveler arasında az bir görsel fark olması durumunda çerçevenin tamamı akıma aktarılmaz. Tam bir referans çerçeve seçilerek ardından gelen çerçeveler bu referans çerçeve ile olan farklılıklar kodlanmak suretiyle ifade edilmektedir. Referans çerçeveye *iç-kodlanmış çerçeve* ya da *I çerçevesi* denmektedir. I çerçevesi P ve B tipi çerçeveleri tahmin etmek için kullanılmaktadır. Şekil 1, MPEG çerçeve tipleri ve çerçeveler arasındaki ilişkiyi göstermektedir.



Şekil 1. MPEG akımında çerçeve tipleri

4. I ÇERÇEVESİ ŞİFRELEME

I çerçevesi, gösterilebilmesi için başka resme ihtiyaç duyulmayan tam bir video resmidir. Bu yüzden I çerçeveleri MPEG akımında en çok bilgiyi tutan alanlardır. Diğer çerçevelerden bağımsız olduğu için ayrı bir resim gibi düşünülebilir. I çerçevesi bir önceki çerçeve ile çok fazla farklılıkların olduğu durumlarda kullanılmaktadır. Bu çerçeve tipi, renk uzayı dönüşümü, örnekleme ve iç-çerçeve sıkıştırma metodu kullanılarak kodlanmaktadır. Şekil 1



Şekil 2. I çerçevesi sıkıştırma aşamaları

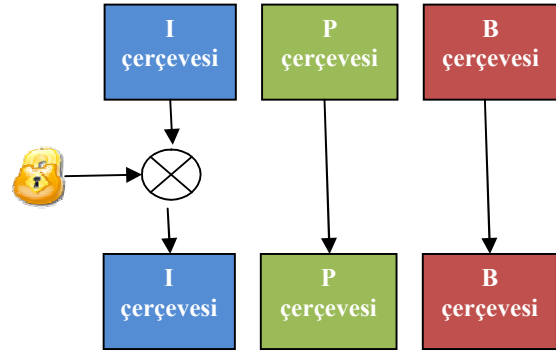
çerçevesinin sıkıştırılması sırasında kullanılan yöntemleri göstermektedir.

Akım içindeki I çerçevesinin şifrenmesi ile yüksek oranda güvenlik sağlanabilir. Fakat MPEG akımında sabit konumlu bir dosya yapısı olmadığından şifrelenecek kısımların tespit edilmesinde başlık bilgilerinden yararlanılır. MPEG akımı değişken uzunlukta kodlama yapısına sahiptir ve video katmanları başlık adı verilen özel bit dağılımlarıyla belirlenmektedir. Şekilde 3'te de görüldüğü gibi 0 referans numaralı I çerçevesi için 00000000 – 00000000 – 00000001 – 00000000 - 0000000000 - 001 bit diziliminin akımında bulunması gerekmektedir.

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	Değeri
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0	0
Resim								
0	0	0	0	0	0	0	0	
0	0							
Geçici referans numarası								
		0	0	1				1
Çerçeve tipi 001=I çerçevesi								

Şekil 3. I çerçevesi akım başlangıç kodları

I çerçevesinin konumu belirlendikten sonra çerçevenin tamamı 128 bitlik bir anahtar ile XOR işlemine tabi tutularak şifrenlenmektedir.



Şekil 4. I çerçevesi şifreleme

Şekil 4'te görüldüğü gibi diğer çerçeve tiplerindeki veriler şifrenmemektedir. B ve P tipi çerçeveler şifrenmediği halde referans olarak kullandıkları I çerçeveleri, şifreleri olduğundan akımın izlenebilmesi mümkün değildir.

5. SONUÇLAR

Çizelge 1'de görüldüğü gibi, I çerçevelerinin şifrenmesi diğer kısmı şifreleme algoritmaları ile karşılaştırıldığında daha yüksek oranda veriyi şifrelediğinden daha düşük bir hıza sahiptir. Fakat geleneksel yöntemler ile karşılaştırıldığında anahtar uzunluğu daha büyük olmasına rağmen daha uygun sonuçlar yakalamaktadır. Yüksek güvenliğin gerektiği durumlarda I çerçevelerinin şifrenmesi tercih edilebilir. Kısmi şifreleme algoritmaları kullanılarak şifrelenen video akımları, görsel olarak büyük bir kısmı bozuk da olsa izlenme şansına sahiptir. Bu yöntemde şifrenmiş akım hiçbir şekilde izlenebilirliğe sahip değildir.

Cizelge 1. Şifreleme Zamanları

Yöntem	Şifreleme Zamanı (s)	Hız (mbit /s)
RSA (8 Bit anahtar)	47.23	52
MPEG akımında başlık şifreleme	27.89	89
MPEG akımında operatör işlemlerinin kısıtlanması yoluyla içerik koruma	26.50	93
Başlık dışında şifreleme	46.82	52
Seçimli XOR işlemi ile MPEG video akımını koruma	27.71	89
Byte dağılımını değiştirerek MPEG video akımını koruma	26.22	94
Sıkıştırılmış video akımının düzensiz haritalar ve başlangıç kodlarına dayalı şifrelenmesi	30.60	81
MPEG akımını geçici referans numaralarını kullanarak şifreleme	26.40	93
I Çerçevelerini şifreleme	40.83	63

[7] Chang, S., Compressed Domain Techniques for Image/Video Indexing and Manipulation, IEEE Conference On Image Processing, 1995

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

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

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

[11] Rivest, R., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, Communications of ACM, ss:120-126, 1978

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

[13]<http://www.arslanguvenlik.com/digitalguvenlik.asp>

KAYNAKLAR

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

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

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

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

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

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