KISMİ MPEG AKIMININ XOR İŞLEMİ İLE ŞİFRELENMESİ

Nurşen SUÇSUZ
Trakya Üniversitesi
nursen@trakya.edu.tr

Deniz TAŞKIN
Trakya Üniversitesi
deniztaskin@trakya.edu.tr

Cem TAŞKIN
Trakya Üniversitesi
cemtaskin@trakya.edu.tr

ABSTRACT

MPEG compression is the most popular video compression technique today. Biggest problem of digital world is protecting content. In this work selective encryption is used for developing a new method to cover security needs. As developed method is specially designed for encrypting MPEG stream, it is harder to break. Encrypted piece is so small that encryption-decryption cost is decreased.

Key words: MPEG, compression, encryption, selective encryption

1. GİRİŞ

Medya ortamlarının günümüzde paylaşılır olması iş imkânları ve gelişim için oldukça önemlidir. Yüksek kalitede video ve ses dosyaları artık kolaylıkla internette paylaşılmakta ve ayrıca PC'lerin özellikleri de bunları desteklemektedir.

Milyonlarca kullanıcı ses ve video dosyalarını rahatlıkla indirip saklayabilmekteler. Kullanıcılar, indirilen bu sayısal içeriklerle ilgili olarak ciddi bir tehditle karşı karşıya kalmaktadırlar. Bu tehlikelerden kurtulmak için videoların bir yerden başka bir yere taşınırken şifrelenmeleri gerekmektedir.

2. AKAN MEDYA NEDİR?

Akan veriler sunucu uygulamaları tarafından taşınırlar ve eş zamanlı olarak istemci uygulamalar tarafından alınır ve görüntülenirler. Bu uygulamalar videoları göstermeye başlayabilir veya sesleri yeteri kadar alınan veri oranında çalabilirler. Server medyayı ağ boyunca taşırken paketlere ayırır. Böylece istemci tarafından yeniden bağlantı kurulur ve medya indiği kadarıyla oynatılır. Aslında istemci gerçekte dosyayı indirmiş olmaz, paketleri yeniden toplar, çalar ve bırakır.

Tüm dijital medya tipleri akabiliyor olmalıdır. Örneğin; yazı, resim, ses, görüntü, yazılım ve üç boyutlu veri akımlarının tamamı akabiliyor olmalıdır.

3. AKAN MEDYA SİSTEMİ

Talep geldiği anda şifreleme, depolama sistemi arşivlenmekte ve istemci talep ettiğinde istemciye ulaşmaktadır. Akım anında akan medya kodlanır, paketlenir ve eş zamanlı olarak istemciye akar.

Bir akan medya sistemi aşağıdaki temel bileşenleri içermelidir:

- Medyanın talep edilmesi
- Kodlama (Sıkıştırma)
- Paketleme
- Paketlerin taşınması
- Paketlerin akım oranı
- Hata kontrolü
- Yeniden kurma
- Çözme (açma)
- İstemcinin akımı çalması

Güvenlik gerektiğinde ise kimlik tanımlama, şifreleme ve anahtar yönetimi gibi ek bileşenlerin olması gerekmektedir.

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

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

4. MEDYA ŞİFRELEME

Multimedya verilerinin boyut olarak büyük olması, akan medyanın sürekli oynatılabilmesi için zaman kısıtlanmasının bulunması ve istemci makinesinde şifrelenmiş medyaları çözmek için meydana çıkan potansiyel masraflar, akan medya şifrelemesini birçok uygulamada kullanmak için zorunlu hale getirmektedir.

Zaman açısından önemli olan büyük boyuttaki verileri (video gibi) transfer ederken, en temel ilke güvenlik özelliklerini uygularken minimum gürültü ve zaman kaybıyla bu işlemin gerçekleştirilmelidir. Bu sebeple yeni şifreleme metotları, ihtiyaçları zamanında karşılamak için daha hızlıdır.

4.1. Gerçek Zaman Sınırlaması

Gerçek zaman kısıtlaması sorununu çözebilmek için *kısmi şifreleme algoritmaları* uygulanmaktadır. Bu algoritmalarda komple bit akışının tamamı yerine bazı bölümleri şifrelenmektedir. Örneğin videonun I çerçeveleri veya P ve B çerçevelerindeki bazı bloklar şifrelenir.

4.2. Potansiyel Maliyet Artırımı

Önceden kredi kartı bilgileri gibi boyut olarak ufak bilgiler şifrelenip transfer ediliyordu. Şu an internet bağlantı hızlarının artması ile birlikte sunucu ve istemciler arasında boyutları megabyteları aşan ses ve görüntü dosyaları transfer edilmektedir. Tabi ki bu transferlerde güvenliği sağlamak, kredi kartı gibi ufak bilgilere nazaran daha maliyetli bir hal almaktadır. Bu büyük boyuttaki veriler çevrimiçi olarak şifrelenmekte ve bu sebeple şifreleme işlemini gerçekleştirmek için daha güçlü makinelere ihtiyaç duyulmaktadır. Aynı şekilde şifrelenmiş verilerin istemci tarafında da çözümlenebilmesi için daha güçlü makineler gerekmektedir ve dolayısıyla ihtiyaçlar maliyeti oldukça arttırmaktadır. Bu maliyetleri düşürebilmek için özel seçilmiş ve boyut olarak yük getirmeyecek daha hafif şifreleme algoritma şemaları uygulanmalıdır.

5. KISMİ ŞİFRELEME

Kısmi şifreleme veri bütününün bir kısmını değiştirerek veri bütününün tamamının güvende olmasını sağlamaktadır. Kısmi şifrelemede, şekil 1'de görüldüğü gibi boyut olarak küçük fakat videonun izlenebilirliği için önemli olan parçalar şifrelenmekte, geriye kalan kısım ise şifrelenmemektedir.

Gerek gerçek zaman sınırlamaları, gerekse potansiyel maliyet artımı gibi sebeplerden akan video görüntüleri kısmi olarak şifrelenmelidir.

Kısmi şifrelemenin en hassas noktası, şifrelenecek olan önemli alanların belirlenmesi işlemidir.

Örnex olarxk Türxçe bix cümlx için xer beşixci haxfin şxfrelxnmesx çok exkin bxr yönxem dexildix.

Yukarıdaki örnek cümlede %20'lik bir tahribat olmasına rağmen cümle hala anlaşılabilir düzeydedir. Kısmi şifreleme yapılırken en düşük düzeyde bozulma ile en yüksek düzeyde güvenlik hedeflenmektedir. Bu örnek yöntem göstermektedir ki kısmi şifreleme, şifrelenecek olan verinin tipine özel olmalıdır.

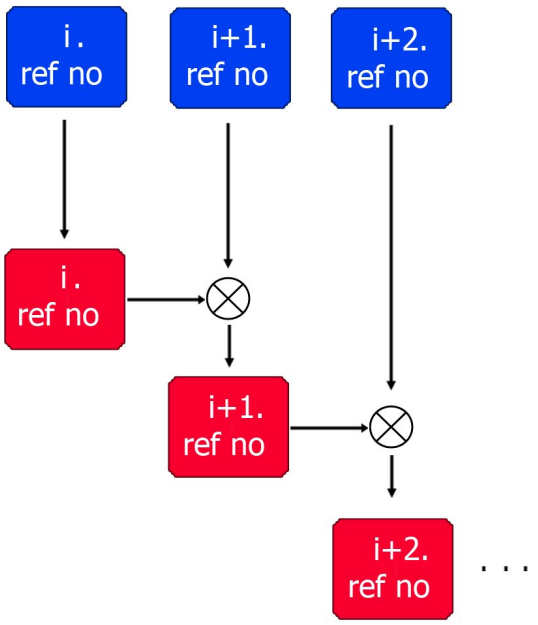
Gerçekleştirilen şifreleme algoritmasında, video akımında bulunan geçici referans numaraları şifrelenecek alan olarak belirlenmektedir. Şekil 2'de gösterildiği gibi geçici referans numaraları, sıkıştırılmış video akımın depolanması ile gösterilmesi arasındaki sıralama farklılıklarını kodlamaktadır.

a) Gösterim sırası

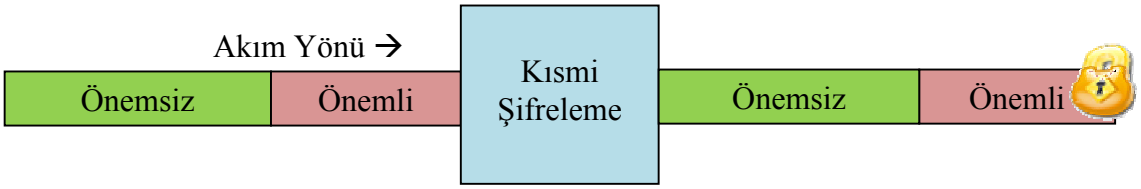
b) Depolama sırası

Şekil 2. Gösterim ve depolama sıraları

Geçici referans numaralarını şifrelemek için geçici referans numarası ile bir önceki referans numarasının değeri şekil 3'te olduğu gibi XOR işlemine tabi tutulmaktadır.



Şekil 3. Referans numaralarının şifrelenmesi



Şekil 1. Kısmi Şifreleme

```
fs.Read(data, 0, (int)stream_size);
fs.Close();long i = 0;tmp = 0;
while (i < stream_size)
{if (i < (stream_size - 3)) if (data[i] == 0 & data[i + 1] == 0
                                & data[i + 2] == 1 & (data[i + 3] == 0))
        {
            if (tmp==0)
                tmp = data[i + 5];
            else
            {

                data[i + 5] ^= tmp;
                data[i + 6] ^= tmp;
                tmp = data[i + 5];
             }

        }
      i++;
}
  i = 0;

while (i < stream_size)
  {
      bw.Write(data[i]);
      i++; }
  bw.Close();
```

Şekil 4. Yöntemin C# kodu

Şekil 4'teki program kodu yöntemin C#'ta kodlanmasını göstermektedir.

Referans numaralarının şifrelenmesi ile gösterim sırası bozulmuş çerçeveler elde edilmektedir. Yapılan şifreleme sonucunda video akımında 1/15.000 oranında çok düşük bir şifreleme alanı ile akımda izlenemeyecek oranda bozulma elde edilmiştir.

Şekil 5, şifrelenecek görüntüyü ve aynı görüntünün şifrelendikten sonraki durumunu göstermektedir.

a) Orijinal video

b) Şifrelenmiş video

Şekil 5. Video görüntüsü

6. SONUÇLAR

Şifreleme işleminin sonucunda referans numaraları tahrip edilmiş bir video akımı elde edilmektedir ve hatalı referanslara sahip hareket vektörleri ortaya çıkmaktadır. Benzer yöntemler MPEG video katmanları dikkate alındığında hareket vektörlerinin ve işaretlerinin değiştirilebilmesi için akımı blok seviyesine kadar çözmektedir. Bu da akımın neredeyse tamamının elden geçmesi anlamına gelmektedir. Geliştirilen yöntem, akımı resim katmanına kadar incelemekte ve hareket vektörlerinin şifrelenmesi işlemini, hatalı referanslar yaratarak temelden çözmektedir.

Çizelge 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
Önerilen Yöntem	26.32	93

Çizelge 1, 309 MB boyutundaki örnek video dosyasının tamamının şifrelenmesi işlemi için önerilen yöntemin diğer yöntemler ile karşılaştırmasını göstermektedir.

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

[7] Chang, S., Compressed Domain Techiques 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 optaining 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