DOĞRUSAL OLMAYAN KAOTİK ŞİFRELEME ALGORİTMASININ MPEG DOSYA İÇERSİNDE YER ALAN SES VERİSİNE UYGULANMASI

Cem TAŞKIN
Trakya Üniversitesi
cemtaskin@trakya.edu.tr

Nurşen SUÇSUZ
Trakya Üniversitesi
nursen@trakya.edu.tr

Deniz TAŞKIN
Trakya Üniversitesi
deniztaskin@trakya.edu.tr

ABSTRACT

Nowadays, parallel to enhancement of accessing digital information, the amount of stored or queried information increased and a lot of studies about data security prepared. The algorithms that previously developed for securing text data are not sufficiently qualified for securing multimedia data. Especially, the large data size of multimedia files extends encryption and decryption duration. In this study, we use non linear chaotic encryption algorithm that was previously used on image files for securing audio data in multimedia files.

Key words: Mpeg Video Encryption, Audio in Mpeg Files, Chaotic Algorithm

1. GİRİŞ

Günümüzde sayısal bilgiye ulaşım imkânlarının gelişmesine paralel olarak, sayısal ortamlarda saklanan ve sorgulanan bilgi miktarı da artmıştır. Bu artış bilgi güvenliği konusunda çalışmalar yapılmasını zorunlu kılmıştır. Daha önceden metin dosyaları üzerinde kullanılmış olan veri şifreleme teknikleri, video dosyaları üzerinde etkin olarak kullanılamamaktadır. Özellikle çoklu ortam video dosyaları içersinde, metin dosyalara göre çok daha fazla bilgi miktarı bulunması, şifreleme ve şifreli dosyaların çözülmesi işlemlerinin çok uzun sürmesine sebep olmaktadır. Bu sebeple, video dosyalarının şifrelenmesi için, sıkıştırılmış video yapısına uygun algoritmalar geliştirilmiş ve uygulanmıştır. Şifreleme işlemi dosya içersindeki veriye kısmi olarak uygulanmaktadır.

2. SIKIŞTIRILMIŞ VİDEO DOSYALARININ YAPISI

Sıkıştırılmış video dosyaları içersinde, görüntü ve ses verileri birbirini takip eden bit akımı olarak yer almaktadır. Bit akımı içersinde yer alan bu bilgilerin birbirinden ayırt edilmesi ve senkronizasyonun sağlanabilmesi için başlık bilgileri kullanılmaktadır. Video dosyaları içersinde yer alan görüntü verisi, görüntü başlık bilgilerinden, ses verisi de ses başlık bilgisinden sonra gelmektedir. Görüntü ve ses başlık bilgileri 4 byte yani toplam 32 bitten oluşmaktadır.

GÖRÜNTÜ BAŞLIĞI			
BYTE	BYTE	BYTE	BYTE
0	0	1	0
00000000	00000000	00000001	00000000

Şekil 1. Görüntü Başlığı

Şekil 1'de gözlenebilen görüntü başlığını tespit etmek için birbirini takip eden 4 byte'ın 0,0,1,0 şartının sağlanması gerekirken, ses başlığında durum daha farklıdır. Şekil 2'de yer alan ses başlığında senkronizasyonu sağlamak için 32 bitlik başlık bilgisinin ilk 11 biti kullanılırken, kalan 21 bit ise sıkıştırılmış ses verisi ile ilgili format bilgilerini belirlemek için kullanılır.

SES BAŞLIĞI			
BYTE	BYTE	BYTE	BYTE
1	111xxxxx	X	X
11111111	111xxxxx	xxxxxxxx	xxxxxxxx

Şekil 2. Ses Başlığı

2.1. Ses Başlık Bilgisi

Sıkıştırılmış video dosyaları içersinde yer alan 32 bitlik ses başlık bilgisinin ilk 11 biti 1, diğer 21 bit ise sıkıştırılmış ses verisinin formatı ile ilgili bilgileri içermektedir. Bu bilgiler:

- Sıkıştırma için kullanılan algoritma (2 bit)
- Katman Türü (2 bit)
- Kontrol Biti (1 bit)
- Bit Hızı (4 bit)
- Örnekleme Hızı (2 bit)
- Ekleme Biti (1 bit)
- Özel Bit (1 bit)
- Kanal Modu (2 bit)
- Mod Eklentisi (2 bit)
- Lisans Hakkı Biti (1 bit)
- Orijinal Biti (1 bit)
- Ses Vurgusu Bitleri (2 bit)

olarak sıralanmaktadır.

Bugüne kadar yapılmış olan birçok çalışmada, sadece görüntü bilgisinin bir kısmı şifrelenirken[3,4], ses verisine dokunulmamıştır. Bu çalışmada ise, doğrusal olmayan kaotik şifreleme algoritması[5] kullanılarak video akımı içersinde yer alan ses verisi şifrelenmektedir.

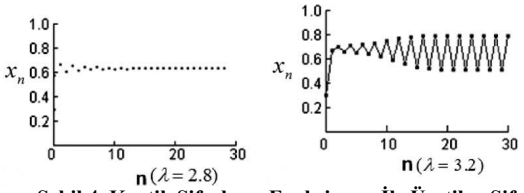
3. DOĞRUSAL OLMAYAN KAOTİK ŞİFRELEME ALGORİTMASI

Kaotik şifreleme algoritmalarını diğer algoritmalardan güçlü kılan özelliklerin başında şifreleme ve şifre çözme işlemleri için kullanıcıdan parametre alması ve şifreleme anahtarının her bir şifreleme adımında değişmesi sayılabilir. Şifreleme için kullanılmış olan kullanıcı parametresinin aynısı şifre çözme için kullanılmazsa çözme işlemi doğru olarak yapılamamaktadır.

$$x_{n+1} = \lambda \times x_n \times (1 - x_n)$$

Şekil 3. Kaotik Şifreleme Fonksiyonu

İlk olarak ortaya atılmış olan kaotik şifreleme fonksiyonu Şekil 3'te görülmektedir. Bu fonksiyon, her bir şifreleme adımında yeni anahtar değer üretmek için kullanılmaktadır. Kullanıcıdan parametre olarak da x_0 başlangıç değeri ve □ değeri alınmaktadır. Kaotik algoritmalar için her bir şifremle adımında üretilen anahtar değerin öncekilerden farklı olması şifreleme algoritmasının gücünü arttırmaktadır.



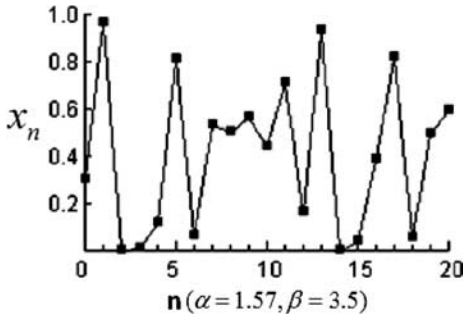
Şekil 4. Kaotik Şifreleme Fonksiyonu İle Üretilen Şifre Değerleri

Şekil 4'te kaotik şifreleme fonksiyonu kullanılarak elde edilmiş değerler görülmektedir. Görüldüğü üzere, elde edilen anahtar değerler sürekli tekrar etmektedir. Algoritmanın şifreleme gücünü arttırmak için, fonksiyon üzerinde değişiklik yapılarak Doğrusal Olmayan Kaotik Şifreleme Algoritması [5] geliştirilmiştir.

$$x_{n+1} = (1 - \beta^{-4}) \cdot \operatorname{ctg}\left(\frac{\alpha}{1+\beta}\right) \cdot \left(1 + \frac{1}{\beta}\right)^{\beta} \cdot \operatorname{tg}(\alpha x_n) \cdot (1 - x_n)^{\beta}$$

Şekil 5. Doğrusal Olmayan Koatik Şifreleme Fonksiyonu

Doğrusal Olmayan Kaotik Şifreleme Algoritması kullanıcıdan 3 parametre almakta ve tekrarsız anahtar değerleri üretmektedir.



Şekil 6. Doğrusal Olmayan Kaotik Şifreleme Fonksiyonun Ürettiği Anahtar Değerler

Şekil 6'da da gözlenebildiği gibi üretilen anahtar değerler tekrarsızdır ve bu algoritmanın gücünü arttırmaktadır.

4.SES VERİSİNİN DOĞRUSAL OLMAYAN KAOTİK ŞİFRELEME ALGORİTMASI İLE ŞİFRELENMESİ

Güçlü bir şifreleme algoritması olan doğrusal olmayan kaotik şifreleme algoritması kullanarak, video dosyaları içersinde yer alan ses verisi şifrelenerek olumlu sonuçlar alınmıştır. Şifreleme için aşağıdaki adımlar izlenmiştir.

- Video akımı içersinde yer alan ses başlıkları sayılır
- Ses başlığı sayısı kadar, doğrusal olmayan kaotik şifreleme algoritması kullanılarak anahtar değerler üretilir
- Anahtar değerler ile ses verisi XOR işlemine tabi tutularak şifrelenir ve şifreli dosyaya yazılır
- Ses verisi dışında kalan bilgiler herhangi bir işleme tabi tutulmadan şifreli dosyaya yazılır

Şifre üretmek için C# dili kullanılarak bir fonksiyon yazılmıştır.

```
double sifre(double x, double alfa, double beta)
{

    double a = 1 - Math.Pow(beta, -4.0);
    double b1 = alfa / (1 + beta);
    double b = 1 / Math.Tan(b1);
    double c1 = 1 + (1 / beta);
    double c = Math.Pow(c1, beta);
    double d = Math.Tan(alfa * x);
    double e1 = 1 - x;
    double e = Math.Pow(e1, beta);

    return a * b * c * d * e;

}
```

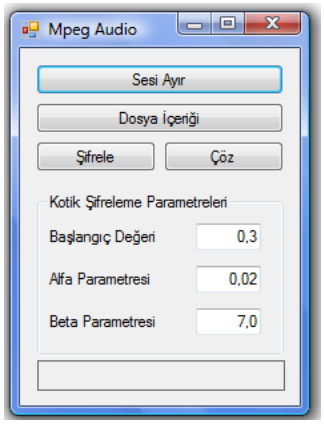
Şekil 7. C# dili kullanılarak hazırlanmış şifreleme fonksiyonu

Bu fonksiyon video akımı içersinde yer alan ses başlığı sayısı kadar çalıştırılarak şifreleme için gerekli olan anahtar değerler üretilmektedir. Üretilen anahtar değerler, ses başlığı ile görüntü başlığı arasında kalan ses verirsine XOR operatörü kullanılarak uygulanmaktadır.

```
while (i < boyut - 4)
{

    if (veri[i] == 255 & veri[i + 1] == 253 & veri[i + 2] == 176 & veri[i+3]==0)
    {
        bw.Write(veri[i]);
        bw.Write(veri[i + 1]);
        bw.Write(veri[i + 2]);
        bw.Write(veri[i + 3]);

        j = i + 4;

        while (j < boyut - 4)
        {

            if (veri[j] == 0 & veri[j + 1] == 0 & veri[j + 2] == 1)
            {
                i = j;
                s++;
                break;
            }

            veri[j] ^= anahtar[s];
            bw.Write(veri[j]);
            j++;
        }
    }

    bw.Write(veri[i]);
    i++;
}
```

Şekil 8. Şifreleme İşlemi Yapan Kod Parçası

Şekil 8'de şifreleme işlemi yapan kod parçası görülmektedir. İlk while döngüsü, video dosyasının içeriğini byte byte okuyabilmek için kurulmuştur. Şayet okuma işlemi yapılırken, birbirini takip eden 4 byte 255, 253, 176 ve 0 değerlerine sahip ise, ses başlığı bulunmuştur. Ses başlığından hemen sonra şifreleme işlemi başlamaktadır ve görüntü başlığı ile karşılaşılana kadar devam etmektedir.



Şekil 9. Şifreleme Programı Arayüzü

Şekil 9'da C# programlama dili kullanılarak hazırlanmış olan şifreleme programı arayüzü görülmektedir. Program şifreleme ve şifre çözme için kullanıcıdan parametreler almaktadır.

5. SONUÇLAR

Hazırlanmış olan ve doğrusal kaotik şifreleme algoritmasını kullanan şifreleme programı video akımı içersimde sadece ses verisini şifrelemekte ve görüntü şifreli dosya içersinde hatasız olarak izlenebilmekte, ses anlaşılır olarak dinlenememektedir. Program 295 MB boyutundaki bir MPEG dosyasının içersinde yer alan ve yaklaşık 29.8 MB boyutundaki ses verisini, 40.32 sn gibi kısa bir sürede şifrelemekte, şifrelenmiş olan dosyayı ise, 37.06 sn 'de çözebilmektedir.

KAYNAKLAR

[1] Tsueike M, Ueta T, Nishio Y. An application of two-dimensional chaos cryptosystem. Tech. Rep. of IEICE, NLP96-19, May 1996.

[2] Analyses and New Designs of Digital Chaotic Ciphers, Ph. D. Thesis, Dissertation of Xi'an Jiaotong University, TN918, N93, 2003
[3] Mutimedia Security And Copyright Protection, Ph. D. Thesis, University of Illinois at Urbana Champaign, IEEE,1998
[4] Changgui S., Bharat B., An Efficient MPEG Video Encryption Algorithm, 1998
[5] Haojiang G., Yisheng Z., Shuyun L., Dequn L. A new chaotic algorithm for image encryption, Chaos, Solitons and Fractals 29, 393–399, Agu 2006
[6] Taşkın, D., Sucsuz, N. ve Taşkın, C., Sıkıştırılmış video güvenliği, e-Journal of New World Sciences Academy, Volume: 2, Number:3 (Basımda), 2007
[7] Taşkın, D., ve Suçsuz, N., Sıkıştırılmış ortamda çerçeve tipine dayalı gerçek zamanlı sahne değişimi belirleme, IV. Bilgi teknolojileri Kongresi, Denizli, 2006
[8] Mitchell, J.L., Pennebaker, W.B., Fogg, C.E. ve Legal, D.J., Mpeg Video Compression Standard, Chapman and Hall, 1996
[9] Rivest, R., Shamir, A., and Adleman, L., A method for optaining digital signatures and public-key cryptosystems, Communications of ACM, ss:120-126, 1978