# KAOTİK KODLANMIŞ BİLGİSAYAR DOSYALARI İLE GÜVENLİ VERİ İLETİŞİMİ

**Aydın AKAN[1] Etkin ELVER[2]**

[1,2] Elektronik Mühendisliği Bölümü
Mühendislik Fakültesi
İstanbul Üniversitesi, 34850, Avcılar, İstanbul

[1]e-posta: akan@akasya.istanbul.edu.tr [2]e-posta: etkin@stu.ee.istanbul.edu.tr

Anahtar sözcükler: Kaos, Veri Kodlama, Güvenli İletişim

## ABSTRACT

In this paper we present an alternative method for crypto-coding of streamable computer files using strange attractors, to use in secure communications. Numerical solutions of chaotic attractor equations in state space has a deterministic but unpredictable behavior. A crypto-coding approach using this scheme provides robust secure computer communication when we use the parameters of chaos generator functions and numerical solution method as an authorization certificate for decoding.

## 1.GİRİŞ

Son yıllarda, bilgisayar verilerinin gizlenmesi ve özellikle internet ortamında güvenli iletişimin sağlanması için gelişmiş kodlama yöntemlerinin kullanımı konusunda bir çok çalışma yapılmaktadır. Günümüzde popülerlik kazanan elektronik ekonomi ve para transferlerinin bilgisayarlar aracılığıyla gerçekleştirilmesi, görüntülü ve sesli medyanın sayısal olarak iletilmesine dayalı hizmet sektörü, bu alandaki çalışmaları körüklemektedir.

İdeal kodlama yöntemi; günümüz elektronik ve bilgisayar sistemlerinin işlem gücü açısından kabul edilebilir ve bellek gereksinimi yönünden tutumlu olmalıdır. Özellikle sesli ve görüntülü medya iletişiminde kullanılan akıcı iletilerin, yetkisiz kişiler tarafından, kayıplı da olsa çözülememesi beklenir. İletilen verinin gerçek-zamanlı çözümlemesi sırasında, gelecek veya geçmiş zaman verilerine gereksinimin az olması da istenmektedir.

Bilgisayar verilerinin kodlanmasında kullanılan yöntemlerden bir tanesi, bir dizi kodlayıcı veri oluşturarak kodlanacak bilginin bu verilerle işlem görmesidir. Alıcı taraf kodlanmış veriden gerekli bilgiyi elde edebilmek için, kodlayıcı veriye ya da onu üretebilmesi için gerekli olan ve *sertifika* olarak adlandırılan parametrelere sahip olmalıdır.

Kodlayıcı verilerin alıcı ve verici taraf için önceden tablolanmış bir dizi değerden oluşması gerek bellek tüketimi ve sertifika aktarımını zorlaştırması açısından, gerekse iletilen verinin istatistik olarak incelenmesiyle çözümlenebilmesi yönünden dezavantaj oluşturmaktadır. En çok kullanılan diğer bir yöntem, çeşitli matematiksel fonksiyonları farklı parametrelerle hesaplayarak kodlayıcı verileri elde etmektir. Bu durumda, üretici fonksiyonun matematiksel olarak yakınsanabilmesi, ya da yine istatistiksel analiz ile çözücü verilerin listelenebilmesi olanaklıdır. Bu gibi yöntemlerin günümüz bilgisayarlarının yüksek işlem gücü karşısında bağışıklı olmadığına, ülkemizde görüntülü medyada kullanılan çeşitli şifreli sistemlerin başarısızlığı örnek gösterilebilir.

Bu bildiride, garip çekerler olarak adlandırılan, doğrusal olmayan, karasız dinamik sistemlerin durum uzayındaki davranışının kodlayıcı veri olarak kullanılmasıyla gerçekleştirilen bir yöntem önerilmiştir. Deterministik olan, ancak davranışı önceden kestirilemeyen bu sistemlerin tanım fonksiyonları, başlangıç koşullarına, dolayısıyla sayısal analiz ile çözümünde kullanılan yöntem ve adım aralığına hassas bağlıdır. Önerilen güvenli iletişimde kullanılacak sertifika bu parametrelerden oluşturulacaktır. Yöntemin en önemli özelliği, kaotik fonksiyonların hiçbir anlamda (zaman, frekans) periyodik olmaması ve herhangi bir yakınsama yöntemiyle üretilememesidir, bu da güvenlik açısından yaygın kullanılan bir çok tekniğe karşı daha avantajlı olmasına olanak vermektedir.

## 2.GARİP ÇEKERLER ve SAYISAL ÇÖZÜMLERİ

Yaygın olarak bilinen iki garip çeker, atmosferdeki bir takım hava olaylarının matematik modellemesi için önerilen Lorenz Çekeri [1] ve basit bir, doğrusal olmayan elektronik devre modeli için kullanılan Chua Osilatörü'dür [2]. Lorenz Çekeri aşağıdaki denklem sistemi ile verilmektedir.

$$\frac{dx}{dt} = -\sigma x + \sigma y$$

$$\frac{dy}{dt} = rx - y - xz$$

$$\frac{dz}{dt} = -bz + xy$$

$$\sigma = 10, b = 2.666667, r = 28$$

Diğer taraftan, Chua Osilatörü ise şu diferansiyel denklemler ile tanımlanmaktadır:

$$\frac{dx}{dt} = k\alpha(y - x - f(x))$$

$$\frac{dy}{dt} = k(x - y + z)$$

$$\frac{dz}{dt} = k(-\beta y - \lambda z)$$

$$f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)\{|x+1| - |x-1|\}$$

Her iki diferansiyel denklem sisteminin Runge-Kutta sayısal çözüm yöntemlerini [1] kullanarak çözmeye çalıştığımızda görmekteyiz ki; denklemlerin durum uzayındaki davranışı, çözüm yönteminin derecesine, aynı derece için kullanılan yöntemin seçeneklerine, adım aralığı ve başlangıç koşullarının farklılığına bağlı olarak birbiriyle ilgisizdir. Şekil-1'de, Lorenz çekerinin Örnek-1 için verilen değerlerde ve de $y_1(t)$ fonksiyonunun başlangıç değerini 5.01 olarak değiştirdiğimizde elde ettiğimiz sonuçları görüyoruz. Bu davranışı gösteren sistemler kaotik sistemler olarak adlandırılırlar.

## 3.KODLAMA YÖNTEMİ

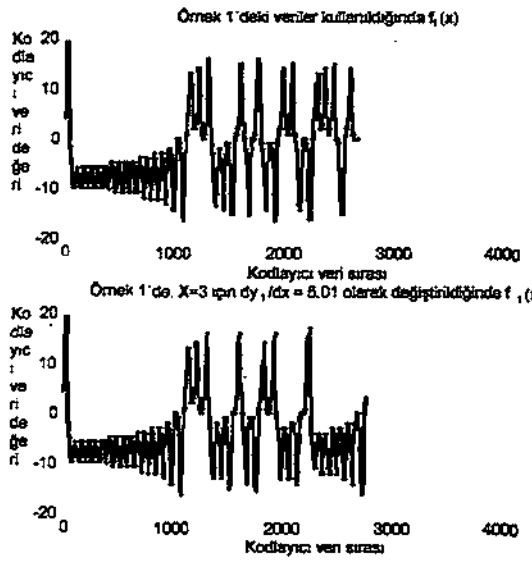
Önerdiğimiz güvenli veri iletimi yönteminde kullanılacak kodlama biçimi için bir sertifika tanımlanır. Tanımlanan sertifikada bulunan farklı kaotik fonksiyonların seçimi için bir indis, denklemlerin başlangıç koşulları, çözüm için kullanılan yöntemin belirlendiği bir indis ve seçilen sayısal çözüm için adım aralığı bilgisi bulunabilir. Sertifika bilgisi bir veri çerçevesi oluşturur ve sistem farklı zamanlarda farklı çerçeveler kullanacak biçimde de tasarlanabilir. Çerçevede kullanılacak veri yoğunlukları da tanımlanır.

**Örnek-1:**
Bir sertifika sistemi tanımlayalım:

*(i) Kullanılacak Kaotik fonksiyonlar olarak,*

1. Lorenz Çekeri'ni
2. Chua Osilatörü'nü temsil etsin

*Kaotik fonksiyon indisi: 1* (1 byte) olsun.




**Şekil-1**

*(ii) Denklemlerin başlangıç koşulları:*

$X$ = 3 (4 byte) için
$dy_1/dx$ = 5 (4 byte)
$dy_2/dx$ = 4 (4 byte)
$dy_3/dx$ = 2 (4 byte) olsun

*(iii) Yöntem indisleri:*

1. 2. Dereceden Runge-Kutta
2. 3. Dereceden Runge-Kutta
3. 4. Dereceden Runge-Kutta'yı temsil etsin

*Çözüm için kullanılan yöntem:* 3 (1 byte) olsun.

*(iv) Çözüm yöntemi için adım aralığı:* 0.01 (4 byte) olsun

Yukarıdaki verilere dayalı bir seçim yaptığımızda *22 byte* veri yoğunluğundaki bir çerçeveyle kodlayıcı sertifika belirlenmiş olur. Bu verilerle kodlanacak bilgi ile aynı uzunlukta üretilecek kodlayıcı değerlerini $y_1(x)$ fonksiyonundan seçelim ve uygun bir veri yoğunluğu ile örnekleyelim. Seçtiğimiz veri yoğunluğu *1 byte* olsun, veri tipi de *işaretli tamsayı* olsun.
Kodlanacak bilginin her byte'ı kodlayıcı veri dizisinin kendisine karşılık gelen byte'ı ile bir işleme girecektir. Seçilecek fonksiyon olarak en uygunlarından birisi bu iki veriyi *EYOR* mantık operatörüyle işleme sokmaktır. Exor işleminin avantajları şöyle sıralanabilir; hızlıdır, her bilgisayarlı sistemde bulunan bir işlemdir, sonucu işleme giren değerlerle aynı veri yoğunluğuna sahiptir, kod çözme işleminde de yine bu işlem kullanılabilir.
(Örnek-2)

**Örnek-2:**
İletilecek bilgi,

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

olsun, bu bilgiye eşleştirilmiş kodlayıcı değeri,

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

ise *ex-or* işlemiyle kodlanmış veri,

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

olur. Kodlanmış veri kodlayıcı değerle tekrar ex-or işlemine uygulandığında iletilen bilgi elde edilir.

Sözkonusu teknik gereksinim duyduğu işlem gücü ve bellek gereksinimi açısından ölçeklendirilebilir olduğu kadar akıcı bilgilerin kodlanması durumunda da ne kendinden önceki ne de kendinden sonraki bilgiye gereksinimi olmadığından avantajlıdır.

## 4.UYGULAMA VE SONUÇ:

Kaotik kodlama tekniği kullanan bir güvenlik yazılımı geliştirilerek çeşitli kelime işlemci, hesap tablosu dosyaları ve düz metin dosyalarda denenmiş ve başarılı olmuştur. Akıcı bilgi niteliği taşıyan *.wav* uzantılı sıkıştırılmamış ses dosyalarında, sertifika parametrelerini tam olarak bilmeyen alıcının iletiye kayıplı da olsa ulaşamayacağı görülmüştür. Sinyal gürültü oranı göz önünde bulundurularak çok küçük parametre farkları da test edilmiştir ve yöntem başarılı olmuştur. Bu durumda MPEG-2 gibi yaygın kullanılan sıkıştırılmış streamable dosyaların sıkıştırma bilgilerine zaten ulaşılamayacağından, yetkisiz uç birimler tarafından çözülemeyeceği ortadadır. Güvenli elektronik posta iletimi için ideal bir yöntemdir.

**REFERENCES**


[1] Chapra S.C., Canale, R.P., Numerical Methods for Engineers

[2] Matsumoto T., Chua L.O., Komuro M., The Double Scroll, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, Vol. CAS-32, No.8, pp. 798-818, 1985

[3] Galleani L., Biey M., Gilli M., Lo Presti L., Analysis of Chaotic Signals in the Time-Frequency Plane

[4] Yang T., Chua L., Secure Communication via Chaotic Parameter Modulation, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, Vol. 43, No.9, pp. 817-819, 1996