

GÜVENLİ HABERLEŞME İÇİN YENİ BİR KAOTİK SİSTEMİN SENKRONİZASYONU

Bildiri Konusu (3. İletişim Kuramı Ve Teknikleri, Kaotik Sistemler)

İHSAN PEHLİVAN

Sakarya Üniversitesi, Elektrik Elektronik Müh. Bölümü, Esentepe Kampüsü, Sakarya
ihsan333@yahoo.com

Özet: Bu makalede, bilgisayar programları ile yapılan sayısal simülasyonlar ve araştırmalar sonucu bulunan üç boyutlu ikinci dereceden otonom adi diferansiyel denklemler formundaki yeni bir kaotik çekici ve özdeş senkronizasyonu tanıtılmaktadır. Yeni sistemin kaotik elektronik osilatörü tasarlanmış ve deneysel ortamda elektronik devresi kurulmuştur. Matlab-Simulink’ de sayısal olarak, Pspice programı ile de elektronik devre olarak yeni kaotik sistemin senkronize olabileceği gösterilmiştir. Sayısal ve elektronik devre olarak yeni kaotik sistemin senkronize olduğunun görülmesi güvenli haberleşme amaçlı uygulamalarda kullanılabilceğini göstermektedir.

Anahtar kelimeler: Kaotik sistem, Kaotik devre, Kaotik osilatör, Senkronizasyon, Güvenli haberleşme

1. Giriş

E. Lorenz, 1963 yılında atmosferdeki ısı yayılımı üzerinde çalışırken üç boyutlu bir otonom denklem sistemi üzerinde kaosu keşfetti[1]. Rossler 1976’da daha basit bir kaotik model tanıttı[2]. Son 20-30 yıl içerisinde mühendislik sistemlerinde kaos kavramı, örneğin lineer olmayan devreler gibi pratik uygulamalarla, bilimsel bir meraktan çok ümit veren ve gelecek vadeden bir konu olmaya başladı. Amaçlı bir şekilde kaotik işaretler oluşturmanın önemsiz bir iş olmadığı, hem temel araştırmalar hem de mühendislik uygulamaları üzerindeki ilginç etkilerle gösterildi. Bu arayışlarla Chen 1999’da yeni bir kaotik sistem kurdu[3]. Bunu Lü sistemi[4] ve üç ayrı sistemin özel durumlarını birleştiren bir birleştirilmiş sistem[5] takip etti. Yine son zamanlarda Qi Dört-boyutlu bir kaotik sistem kurdu[6]. Kaotik işaretlerin yayılı spektruma sahip olması, mühendisleri bu işaretleri haberleşmede kullanmanın haberleşme açısından güvenli ve gürültüye bağışık kılacağı fikrine itmiştir[7]. Kaotik işaretlerin güvenli haberleşmede kullanılabilceği fikriyle birlikte, haber işaretinin alıcıda tekrar çözülebilmesi için senkronizasyon kavramı ortaya çıkmıştır. Bu sebeple kaotik sistemler arasındaki senkronizasyon ise son yıllarda çok fazla ilgi çeken bir konu olmuştur. Özdeş kaotik sistemlerin kuplağı ve senkronize edilmeleri ile ilgili ilk çalışma Pecora-Carroll[8], [9]’ündür. Kaotik sistemlerin senkronizasyonu ile ilgili çalışmalar, kaotik devre ve dinamikler kullanılarak güvenilir ve gizli haberleşme amaçlı elektronik sistem tasarımı ve gerçekleştirilmesi

ile ilgili çalışmalar için bir dönüm noktası olmuştur. Cuomo ve Oppenheim’ in[10],[11] bir bilgi işaretine kaotik işaret ekleyerek, senkronizasyon kavramının bilgi işaretinin maskelenmesinde nasıl kullanılabilceği ni göstermesi, kaotik haberleşme sistem tasarımında ilk uygulamalar olması açısından önemlidir. Günümüze kadar kaotik sistemlerin senkronizasyonu ve senkronize kaotik sistemlerin güvenilir haberleşme amaçlı kullanımı ile ilgili çok sayıda çalışma yapılmıştır [12-15].

Bu makalenin ikinci bölümünde bulunan yeni kaotik sistem tanıtılacak, üçüncü bölümde yeni kaotik sistemin Matlab-Simulink modellemesi ve elektronik devre gerçekleştirilmesi verilecek, dördüncü bölümde ise yeni kaotik çekicinin senkronizasyonu hem Simulink modeli hem de elektronik devre modeli üzerinde gerçekleştirilecektir. Yeni kaotik sistemin senkronizasyonu için uygulanacak metod Pecora-Carroll (PC) özdeş senkronizasyon metodu olacaktır.

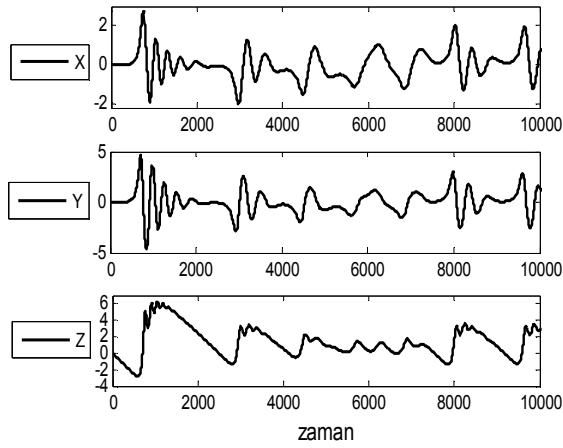
2. Yeni Kaotik Sistem

Bilgisayar programları ile yapılan sayısal simülasyonlar ve araştırmalar sonucu bulunan, otonom doğrusal olmayan birinci dereceden adi diferansiyel denklemler şeklindeki yeni kaotik sistem aşağıda verilmiştir.

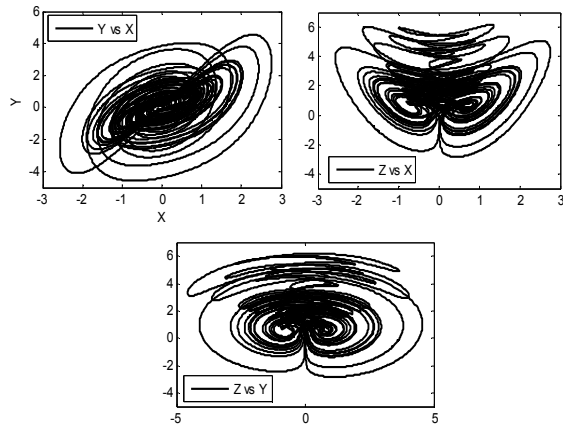
$$\begin{aligned}\dot{x} &= y - x \\ \dot{y} &= a \cdot y - x \cdot z \\ \dot{z} &= x \cdot y - a\end{aligned}\quad (1)$$

Yeni kaotik sisteminin, $a = 0.5$ parametresi, ve $x_0 = 0.001$, $y_0 = 0.001$, $z_0 = 0$ ilk şartları için elde edilen x , y , z kaotik durum değişkenlerinin zamana göre değişimi Şekil 1.’de, x - y , x - z , ve y - z kaotik faz portreleri ise Şekil 2.’de görülmektedir.

Yeni kaotik sistem, dinamik davranış olarak Lorenz tipi kaos gösterir ve kararsız olan simetrik iki kritik nokta etrafındaki kaotik yörüngelerde dolaşır. Lorenz ve Chen sistemlerindeki gibi $(0, 0, 0)$ orijin noktasının kritik nokta olma özelliği bu sistemde yoktur.



Şekil 1. Yeni kaotik sistemin x, y, z kaotik durum değişkenlerinin zamana göre değişimi



Şekil 2. Yeni kaotik sistemin x-y, x-z, ve y-z kaotik faz portreleri

Denge(kritik) noktalarını bulmak için (1) denkleminde $\dot{x} = \dot{y} = \dot{z} = 0$ yapılırsa,

$$\begin{aligned} 0 &= y^* - x^* \\ 0 &= a \cdot y^* - x^* \cdot z^* \\ 0 &= x^* \cdot y^* - a \end{aligned} \quad (2)$$

elde edilir. Bu denklem sistemi x^*, y^*, z^* için çözümlerse denge noktaları $(x^*, y^*, z^*) = (\pm\sqrt{a}, \pm\sqrt{a}, a)$ olarak bulunur. $x, y, z \in \mathbb{R}$ olduğundan, denge noktalarının $a > 0$ için mevcut olduğu anlaşılır.

Denge noktalarının kararsız olup olmadığını anlamak için özdeğerlerin bulunması gerekir. En az bir özdeğerin reel kısmı pozitif olduğu takdirde, denge noktasının kararsızlığına ve kaosa işaret eder. Sistemin Jacobian matrisi aşağıdaki gibidir.

$$J = \begin{bmatrix} -1 & 1 & 0 \\ -z & a & -x \\ y & x & 0 \end{bmatrix} \quad (3)$$

İlk, $(x^*, y^*, z^*) = (\sqrt{a}, \sqrt{a}, a)$ denge noktasında, Jacobian matrisi şu şekilde olur.

$$J = \begin{bmatrix} -1 & 1 & 0 \\ -a & a & -\sqrt{a} \\ \sqrt{a} & \sqrt{a} & 0 \end{bmatrix} \quad (4)$$

$|J - \lambda I| = 0$ karakteristik denkleminin çözümünden özdeğerler bulunur. Karakteristik denklem $-\lambda^3 + a\lambda^2 - \lambda^2 - a\lambda - 2a = 0$ olarak elde edilir. Buradan özdeğerler,

$$\lambda_1 = -1, \quad \lambda_2 = -\frac{\sqrt{a^2 - 8a} - a}{2} \quad \text{ve} \quad \lambda_3 = \frac{\sqrt{a^2 - 8a} + a}{2}$$

olarak bulunur. $a = 0.5$ için

$$\text{özdeğerler, } \lambda_1 = -1, \quad \lambda_2 = -\frac{1.93649 \cdot i - 0.5}{2}$$

$$\text{ve } \lambda_3 = \frac{1.93649 \cdot i + 0.5}{2}, \text{ Buradan}$$

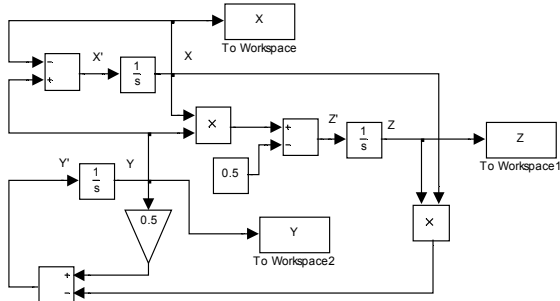
$$\lambda_1 = -1, \quad \lambda_2 = -0.968245 \cdot i - 0.25 \quad \text{ve}$$

$$\lambda_3 = 0.968245 \cdot i + 0.25 \text{ olarak elde edilir.}$$

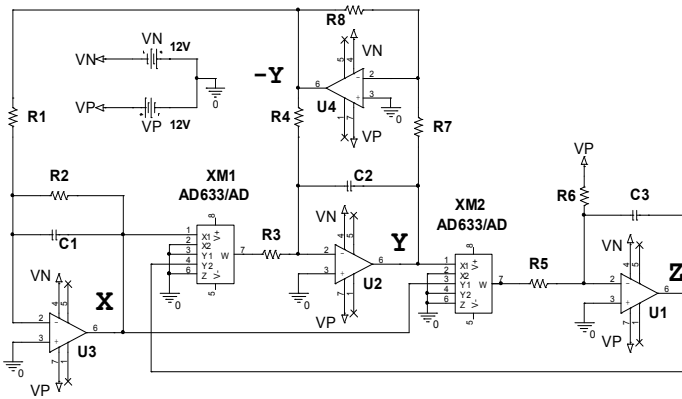
Özdeğerlerden birisinin gerçel kısmı pozitif olduğundan, $(x^*, y^*, z^*) = (\sqrt{a}, \sqrt{a}, a)$ denge noktası kararsızdır. Diğer $(-\sqrt{a}, -\sqrt{a}, a)$ denge noktası için de Jacobian matris elde edilip, $|J - \lambda I| = 0$ karakteristik denkleminin çözümüne bakılırsa aynı özdeğerler bulunacaktır. Demek ki sistem kararsız olan simetrik iki kritik nokta etrafındaki yörüngelerde gezmektedir. Sistemin Lyapunov üstelleri, $\lambda_1 = 0.18717$, $\lambda_2 = 0$ ve $\lambda_3 = -0.68919$ olarak bulunmuştur. Buradan kaotik davranışın oluşması için gereken $(+, 0, -)$ durumunun sağlandığı ve sistemin kaotik olduğu görülmektedir. Yeni çekici, faz portreleri olarak Lorenz ve Chen sistemlerine benzer. Yeni sistem, iki adet ikinci dereceden doğrusal olmayan terim (xz ve xy) olmak üzere toplam altı terim içermekte olduğundan dolayı, Lorenz ve Chen sistemlerinden topolojik olarak daha basittir. Çünkü Lorenz sisteminde yedi terim, Chen sisteminde ise sekiz terim bulunmaktadır. Ayrıca yeni sistemde tek parametre varken, diğerlerinde üçer parametre vardır.

3. Yeni Kaotik Sistemin Simulink Modeli ve Devre Gerçeklemesi

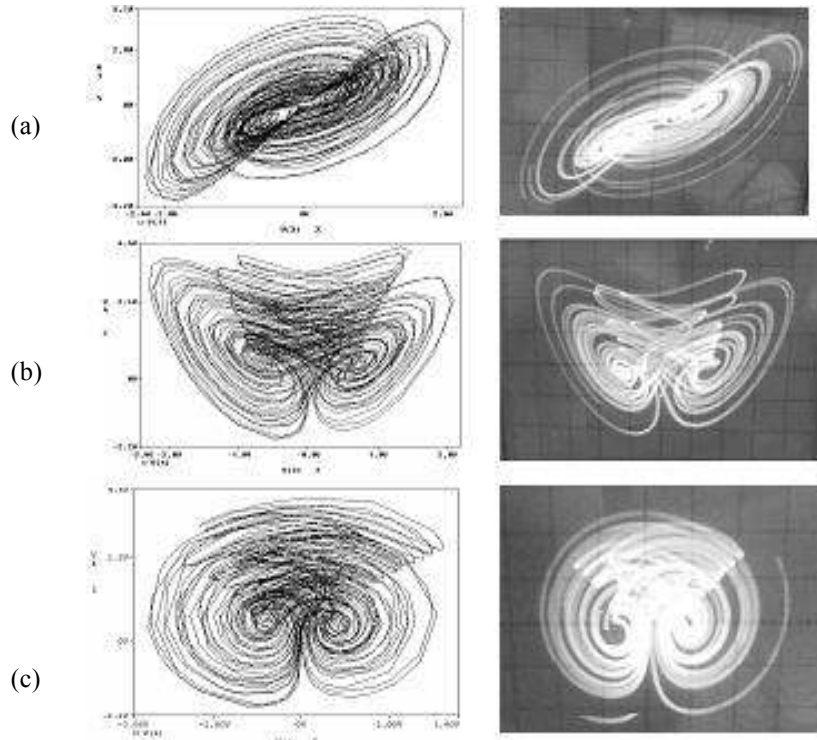
Yeni kaotik sisteminin, Matlab-Simulink'de yapılan blok diyagramları ile modellenmesi Şekil 3.'de verilmiştir.



Şekil 3. Yeni kaotik sisteminin Simulink modeli



Şekil 4. Yeni kaotik sistemin elektronik devre şeması ve elektronik devre gerçekleştirilmesi



Şekil 5. Yeni kaotik devrenin pspice simülasyon sonuçları ve gerçek devresinin osiloskop çıktıları a)x-y, b)x-z, c) y-z kaotik çekicileri

Yeni kaotik sistemi gerçeklemek için $a = 0.5$ parametresi, ve $x_0 = 0.001$, $y_0 = 0.001$, $z_0 = 0$ ilk şartları altında, blok diyagramdan faydalanılarak tasarlanan elektronik devre şeması ve fiziksel gerçekleştirilmesi Şekil 4.'de, Pspice simülasyon sonuçları ile gerçek elektronik devrenin osiloskop çıktıları karşılaştırmalı olarak Şekil 5.'de verilmiştir. Devrede LM741 opamplar, Analog Devices AD633JN analog çarpım entegreleri, uygun değerlerde direnç ve kondansatörler bulunmaktadır. Devre gerçekleştirilmesi ve Pspice simülasyonlarında, $R1=R2 = 400K$, $R3=R5=40K$, $R4 = 800K$, $R6 = 9600K$, $R7 = R8 = 100K$, $C1 = C2 = C3 = 1nF$, $VN = -12V$, $VP = 12V$ alınmıştır. AD633 entegresinin kabul edilebilir giriş değerleri $-10V$ ile $+10V$ arasındadır.

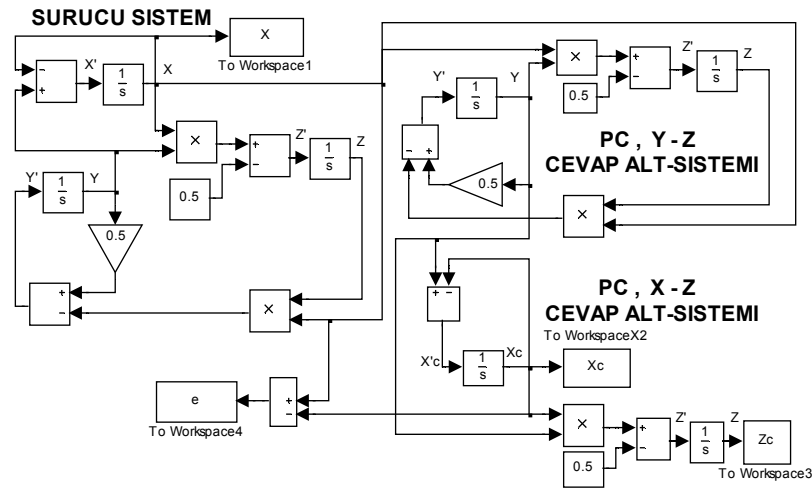
Sayısal simülasyon sonuçları(Şekil 2.), Pspice simülasyon sonuçları(Şekil 5.) ve gerçek devre osiloskop çıkışlarının(Şekil 5.) aynı sonuçları verdiği görülmektedir.

4. Yeni Kaotik Sistemin Senkronizasyon Uygulamaları

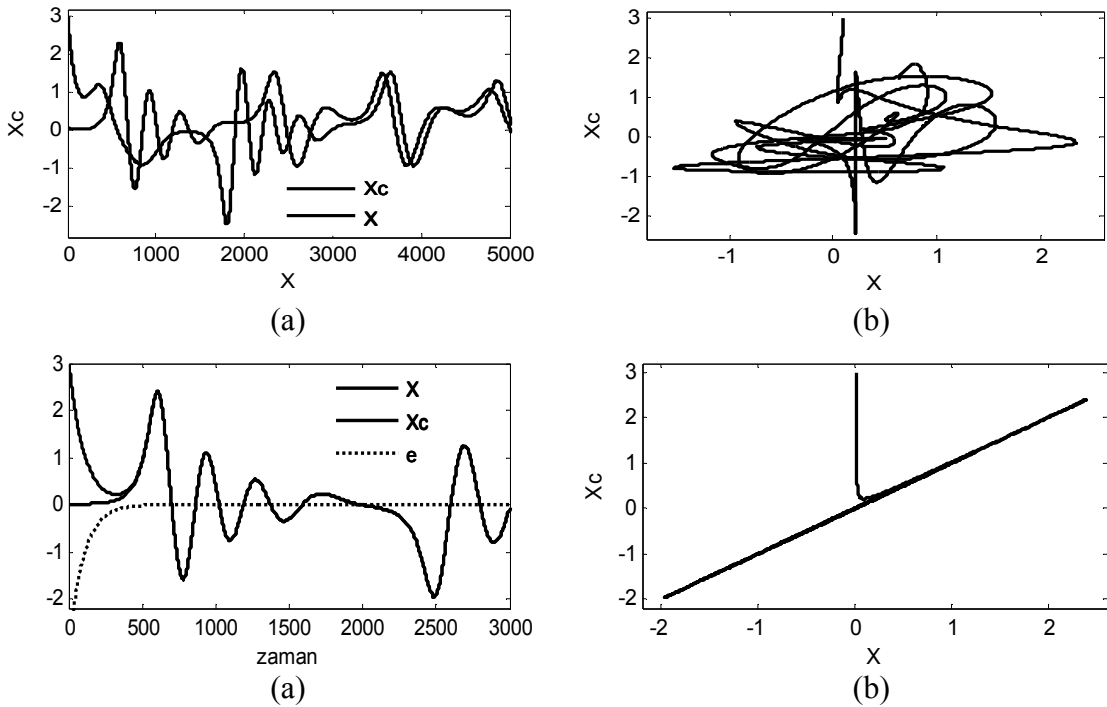
Yeni kaotik sistem, PC yöntemiyle senkronizasyon için; $y_1 = a \cdot y_1 - x \cdot z_1$, $\dot{x}_1 = x \cdot y_1 - a$ şeklinde (y_1, z_1) sürücü olan cevap alt-sistemine,

ve $\dot{y}_c = a \cdot y_1 - x_c \cdot z_c$, $\dot{x}_c = x_c \cdot y_1 - a$

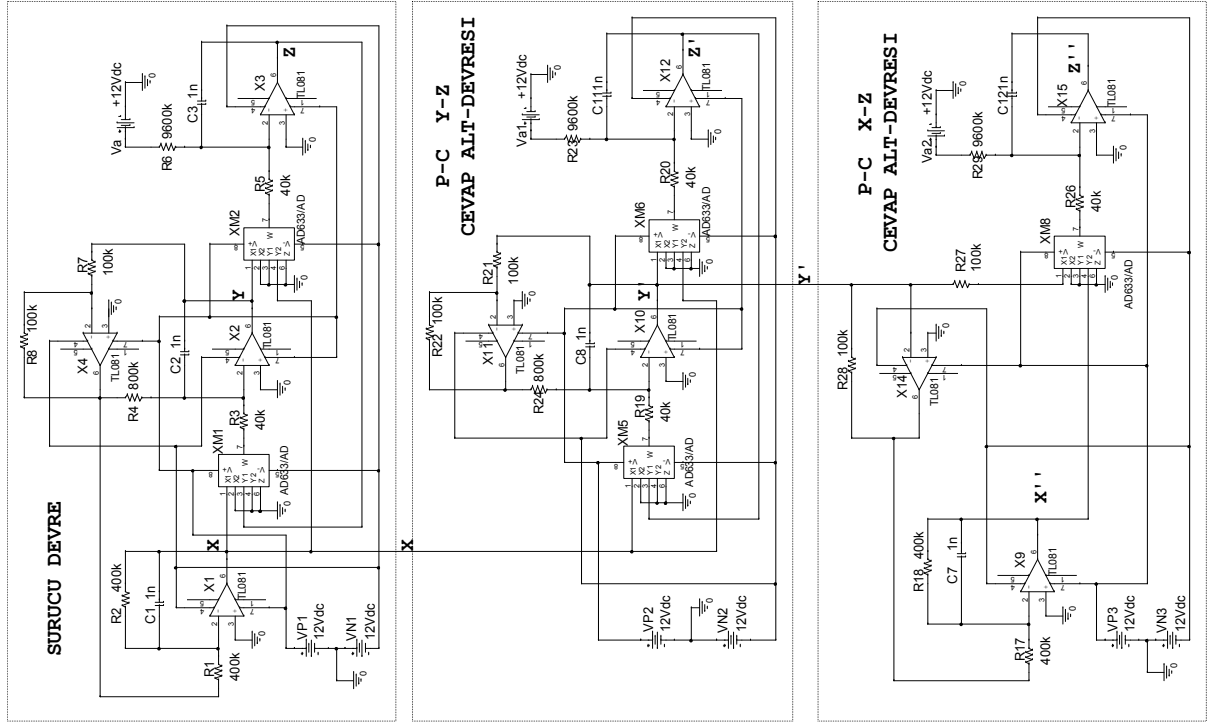
şeklinde (x_c, z_c) kararlı cevap alt-sistemine ayrıştırılabilir. Senkronizasyondan sonra alıcı devrenin x_c sinyali, verici devrenin x sinyaline kısa sürede yaklaşacak ve senkronize olacaktır. Yeni kaotik sistemin PC yöntemi ile Simulink'te yapılan blok diyagramları ile senkronizasyon modellenmesi Şekil 6.'da, simülasyon sonuçları ise Şekil 7.'de verilmiştir. Yeni kaotik çekicinin Pspice PC senkronizasyon devresi Şekil 8.'de, simülasyon sonuçları ise Şekil 9.'da görülmektedir.



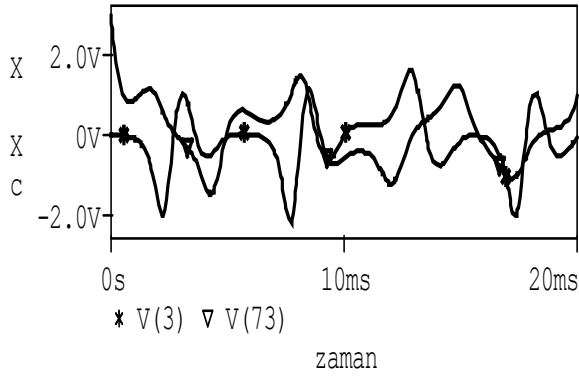
Şekil 6. Yeni kaotik sistemin Simulink PC senkronizasyon modellemesi



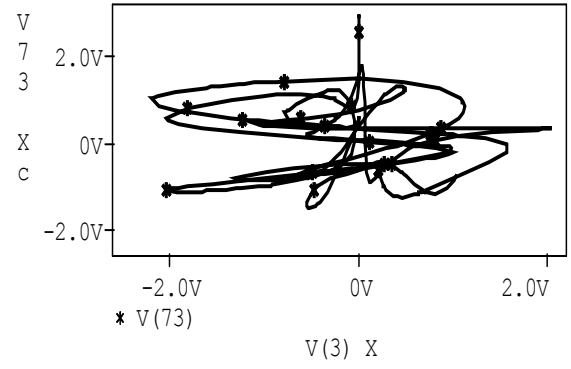
Şekil 7. Yeni kaotik sistemin Simulink senkronizasyon sonuçları (a) Senkronizasyon öncesi Sürücü(X) ve Cevap(Xc) kaotik sinyallerinin zamana göre değişimi (b) X - Xc değişimi (senkronizasyondan önce) (c) Sürücü sinyal(X), cevap sinyali(Xc) ve senkronizasyon hatası(e = X - Xc)'nin zaman göre değişimi (d) X - Xc değişimi (senkronizasyondan sonra)



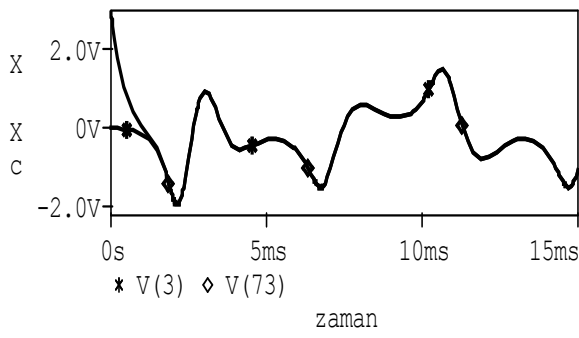
Şekil 8. Yeni kaotik sistemin Pspice PC senkronizasyon devresi



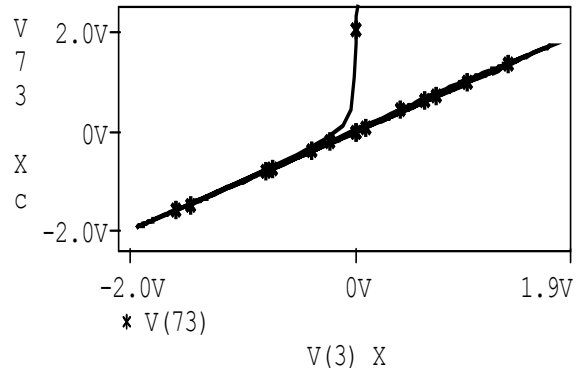
(a)



(b)



(c)



(d)

Şekil 9. Yeni kaotik sistemin Pspice PC senkronizasyon devresi simülasyon sonuçları

(a) Senkronizasyon öncesi Sürücü(X) ve Cevap(Xc) kaotik sinyallerin zamana göre değişimi

(b) Senkronizasyonsuz X-Xc değişimi (c) Sürücü(X) ve Cevap(Xc) kaotik sinyallerinin zamana göre değişimi

(d) X-Xc senkronizasyonu

5.Sonuçlar

Bu makalede, bilgisayar programları ile yapılan sayısal simülasyonlar ve araştırmalar sonucu bulunan üç boyutlu ikinci dereceden otonom adi diferansiyel denklemler formundaki yeni bir kaotik çekici ayrıntılı bir şekilde tanıtılmış, simulink modellemesi ve elektronik osilatörü tasarlanarak gerçek devresi kurulmuş, sayısal simülasyon sonuçları(Şekil 2.), Pspice simülasyon sonuçları (Şekil 5.) ve gerçek devre osiloskop çıkışlarının (Şekil 5.) aynı sonuçları verdiği görülmüştür. Ayrıca Pecora-Carroll metodu ile Matlab-Simulink' de sayısal olarak, Pspice programı ile de elektronik devre olarak yeni kaotik sistemin senkronize olabileceği gösterilmiştir. Sayısal ve elektronik devre olarak yeni kaotik sistemin senkronize olduğunun görülmesi güvenli haberleşme amaçlı uygulamalar için uygun olabileceğini göstermektedir. Özet olarak, güvenli haberleşme sistemleri için kullanılacak yeni bir kaotik sistem tanıtılmış ve kaos senkronizasyon uygulamaları çalışılmıştır,. Simulink ve Pspice simülasyonları ile kausun senkronize edilebileceği yeni bir sistem üzerinde gösterilmiştir.

Kaynaklar

- [1] Lorenz E. N., 1963 , “Deterministic nonperiodic flow”, J. Atmos. Sci., 20:130–141.
- [2] Rossler O. E., 1976, “An equation for continuous chaos”, Phys. Lett. A, 57:397–398.
- [3] Chen G., Ueta T., 1999, “Yet another chaotic attractor”, Int. J. Bifurc. & Chaos, 9:1465-1466.
- [4] Lü J., Chen G., 2002, “A new chaotic attractor coined”, Int. J. Bifurc. & Chaos, 12:659-661.
- [5] Lü J., Chen G, D. Cheng and S. Celikovsky, 2002, “Bridge the gap between the Lorenz system and the Chen system”, Int. J. Bifurcation and Chaos, 12:2917-2926.
- [6] G. Qi, S. Du and G. Chen, 2005, “On a four-dimensional chaotic system”, Chaos, Solitons and Fractals, 23:1671-1682.
- [7] Ogarzalek M. J., 1993, “Taming Chaos Part-I Synchronization”, IEEE Tran. Cir. Sys. CAS I, 40(10):693-699.
- [8] Pecora L. M., Carroll T. L., 1990, “Synchronization in Chaotic Systems”, Phys. Rev. Lett., 64:821-824.
- [9] Pecora L. M., Carroll T. L., 1991, “Driving systems with chaotic signals”, Physical Rev. A , 44:2374-2383
- [10] Cuomo K. M., Oppenheim A. V., 1993, “Circuit Implementation of Synchronized Chaos with applications to Communication”, Phys. Rev. Lett., 71:65-68.
- [11] Cuomo K.M., Oppenheim A.V., Strogatz S.H., 1993, “Synchronization of Lorenz-based chaotic circuits with applications to communications”, IEEE Trans. Circuits Syst., 40(10):626–633.
- [12] Alexeyev A. A., Green M. M., 1997, “Secure Communications Based on Variable Topology of Chaotic Circuits”, Int. J. of Bifurcation and Chaos, 7:2861-2869.
- [13] Itoh M., 1999, “Spread Spectrum Communication via Chaos”, International J. of Bifurcation and Chaos, 9:155-213.
- [14] Pehlivan İ, Uyaroglu Y., 2007, “Rikitake Attractor and its synchronization application for secure communication systems”, Jour. of Applied Sciences, 7(2):232-236
- [15] Pehlivan İ, Uyaroglu Y., (In press), “Simplified Chaotic Diffusionless Lorenz Attractor and its Application to Secure Communication Systems”, IET Communications.