DURUM KONTROLLÜ HÜCRESEL SİNİR AĞI (DK-HSA) DEVRESİ KULLANILARAK GERİBESLEMELİ KAOTİK MASKELEME SİSTEMİNİN TASARLANMASI

Enis GÜNAY **Mustafa ALÇI** **Recai KILIÇ**

Erciyes Üniversitesi Elektronik Mühendisliği Bölümü, 38039, Kayseri
e-posta: egunay@erciyes.edu.tr

Anahtar Sözcükler:Kaotik Maskeleme, Kaos, Hücresel Sinir Ağları.

Abstract

A secure transmission application of State Controlled Cellular Neural Network (SC-CNN)-based circuit is presented. Since SC-CNN-based circuit has feedback connections between the cells, it is very suitable for realizing chaotic masking system with feedback algorithm. Therefore, we have constructed a chaotic masking system with feedback using SC-CNN circuit. The PSpice simulation experiments verify that the proposed SC-CNN-based secure communication system exhibits a good performance over a wide range of amplitude and spectral characteristics of the information signal. The feedback method which had been verified using different chaos generators such as Lorenz system and Chua's circuit in the literature was also verified in this work by using another inductorless chaos generator SC-CNN circuit.

1. Giriş

Son on yıl içerisinde, kaotik devreler ve kaotik devrelerin kullanıldığı güvenilir haberleşme uygulamaları büyük bir ilgi odağı haline gelmiştir. Kaos-tabanlı haberleşme sistemlerinin büyük bir çoğunluğu kaotik senkronizasyonu kullanarak oluşturulmuştur [1-2]. Bu çalışmalara ilaveten son yıllarda kaotik senkronizasyon kullanmayan dijital haberleşme yönelik kaotik sistemler de geliştirilmiştir [3-4]. Kaotik senkronizasyonu kullanan kaos-tabanlı haberleşme sistemlerinde bildiri işareti iletilen kaotik işaret içerisine doğrudan modülasyon, maskeleme ve diğer başka metotlar kullanılarak gömülmektedir. Eğer iki sistem arasında kaotik senkronizasyon sağlanabilirse gürültüye benzeyen bu işaretten bildiri işaretinin tekrar elde edilmesi mümkün olmaktadır. Kaos-tabanlı haberleşme sistemlerinde farklı bir çok kaos üreteçleri kullanılmıştır. Otonom Chua devresi [5] basit bir yapıya sahip olması ve oldukça zengin kaotik davranış sergilemesinden dolayı en çok tercih edilen kaos üreteci konumundadır.

Diğer taraftan, **Hücresel Sinir Ağları** (HSA) lineer olmayan elektronik sistemlerin başka bir sahasını oluşturmaktadır. Chua ve Yang [6] tarafından ilk olarak 1988'de tanıtılmasından itibaren, HSA oldukça ilgi uyandırmış ve HSA ile ilgili bir çok teorik ve deneysel çalışma literatürde yer almıştır. Bu çalışmalar arasında oldukça ilgi çekici olanlardan birisi de, genelleştirilmiş üç HSA hücresinin uygun bir bağlantı ile Chua devresinin dinamiklerinin oluşturulmasında kullanılmasıdır [7]. Özellikle bu çalışmadan sonra Durum Kontrollü Hücresel Sinir Ağı (DK-HSA) tabanlı Chua devresinin kullanıldığı bir çok uygulama literatürde yer almıştır [8]. Yapılan bu çalışmalardaki ana fikir; DK-HSA tabanlı Chua devresinin, HSA-tabanlı güvenli haberleşme uygulamalarında bir kaos üreteci olarak kullanılmasıdır. DK-HSA tabanlı kaotik haberleşme sistemlerinde iletim metodu, anlık senkronizasyon sağlayan ve orijinal bildiri işaretini V-I-V işaret çevrimini kullanarak kaotik olarak şifreleyen bir eşlenik (inverse) sistemi yaklaşımıdır.

Bu çalışmada, DK-HSA-tabanlı devrenin kullanıldığı güvenilir bir haberleşme sistemi sunulmaktadır. DK-HSA-tabanlı devrenin hücreler arasında geribesleme bağlantılılarına sahip olmasından dolayı geribesleme algoritması ile kaotik maskeleme sisteminin gerçekleştirilmesine uygundur. Bu nedenle DK-HSA-tabanlı bir devre kullanılarak bir geribeslemeli kaotik maskeleme sistemi tasarlanmıştır. PSpice simülasyon benzetim sonuçları, önerilen DK-HSA-tabanlı güvenli haberleşme sisteminin, bildiri sinyalini oldukça geniş genlik ve spektral karakteristiklerinde oldukça iyi bir performans sergilediğini göstermiştir. Ayrıca literatürdeki Chua devresi ve Lorenz sistemi gibi farklı kaos üreteçleri kullanılarak doğrulanan geribesleme metodu bir diğer indüktörsüz kaos üreteci olan DK-HSA devresi kullanılarak da doğrulanmıştır.

Bildirinin organizasyonu şu şeklidedir. Bölüm 2'de DK-HSA tabanlı Chua devresi, tanımları ve durum denklemleri ile verilmektedir. Bölüm 3'te ise, önerilen DK-HSA devreleri kullanan geribesleme algoritması ile kaotik maskeleme sistemi tanıtılmaktadır. Bölüm 4' te simülasyon sonuçları verilmekte ve son bölümde de sonuç ve değerlendirme kısımları yer almaktadır.

2.Genelleştirilmiş HSA Hücreleri ve CHUA Devresi

Günümüze kadar kaos-tabanlı güvenilir bir haberleşme sistemi oluşturmak üzere bir çok kaos-tabanlı haberleşme sistemleri ve farklı kaotik devreler geliştirilmiştir. Kaos-tabanlı güvenilir haberleşme sistemlerinin büyük çoğunluğu Chua devresi kullanılarak tasarlanmış ve gerçekleştirilmiştir. Chua devresi Şekil-1(a)' da görüldüğü üzere üç tane enerji depolayan eleman, bir tane doğusal direnç ve bir tane de Chua diyotu olarak adlandırılan doğrusal olmayan direnç N_R içermektedir. Chua devresi aşağıdaki durum denklemleri ile tanımlanmaktadır.

$$\begin{aligned} L\frac{di_L}{dt} &= -V_{C2} - i_L \cdot R_S \\ C_2\frac{dV_{C2}}{dt} &= i_L - \frac{1}{R}\left(V_{C2} - V_{C1}\right) \\ C_1\frac{dV_{C1}}{dt} &= \frac{1}{R}\left(V_{C2} - V_{C1}\right) - f\left(V_R\right) \end{aligned} \qquad (1)$$

Burada, $f(V_R)$, Şekil-1(b)'de görülen parçalineerli bir fonksiyon olup,

$$i_R = f\left(V_R\right) = G_b . V_R + \frac{1}{2}\cdot\left(G_a - G_b\right)\times \left(\left|V_R + B_p\right| - \left|V_R - B_p\right|\right) \qquad (2)$$

Yukarıdaki denklemde G_a ve G_b sırasıyla iç ve dış bölgelerdeki eğimleri göstermektedir. Denklem (1),

$$x = V_{C1}/B_p,\ y = V_{C2}/B_p,\ z = I_L/B_pG,\ \tau = tG/C_2,$$

$$m_0 = \left(G_a/G\right)+1,\ m_1 = \left(G_b/G\right)+1,\ \alpha = C_2/C_1,$$

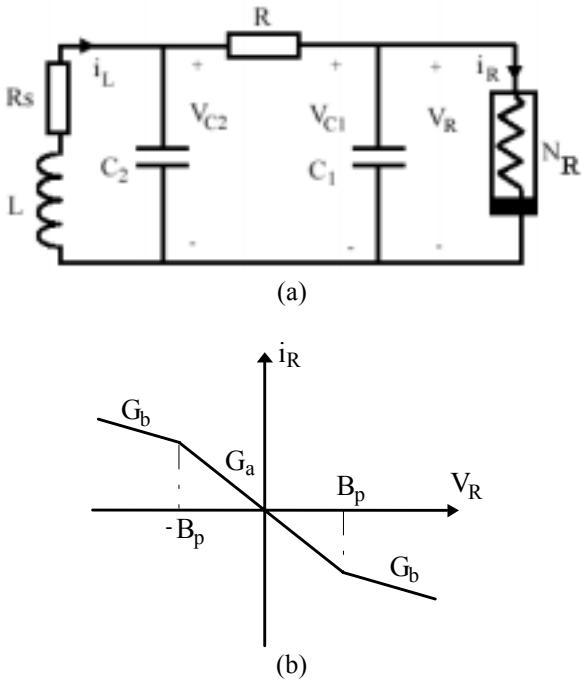
$$\beta = C_2/\left(LG^2\right) \text{ ve } \gamma = \left(C_2R_s\right)/\left(GL\right)$$

dönüşümleri kullanarak Chua devresinin Denklem (3)' deki boyutsuz haline dönüştürülebilir.

$$\begin{aligned} \dot{x} &= \alpha\left[y - h\left(x\right)\right] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta - \gamma z \end{aligned} \qquad (3)$$

Burada,

$$h\left(x\right) = m_1 x + 0.5\cdot\left(m_0 - m_1\right)\times \left(\left|x+1\right| - \left|x-1\right|\right) \qquad (4)$$



Şekil-1. a)Chua devresi b)Chua devresindeki lineer olmayan direncin (N_R) *i-v* karakteristiği.

Diğer taraftan, Arena [7] genelleştirilmiş üç adet hücresel sinir ağı hücresinin uygun bir bağlantısıyla Chua devresinin yeni bir gerçekleştirimini elde etmiştir. Arena oluşturduğu HSA yapısını bir durum kontrollü HSA olarak adlandırmaktadır. Orijinal HSA ile DK-HSA yapıları arasındaki temel fark, komşu hücrelerin dahili durumları arasındaki bağlantıyı temsil eden bir "durum kontrol" şablonunun bulunmasıdır. Bu durum HSA mimarisini daha esnek ve bir çok doğrusal olmayan otonom dinamik devrelerin gerçekleştirilmesinde daha etkili yapmaktadır. Genelleştirilmiş hücre modeli boyutsuz doğrusal olmayan durum denklemleri ile şu şekilde tanımlanmaktadır.

$$\dot{x}_j = -x_j + a_j y_j + G_0 + G_s + i_j \qquad (5)$$

x_j durum değişkenini, a_j sabit bir parametreyi, i_j eşik değerini gösterirken, j ise hücre indeksini göstermektedir. y_j ise aşağıdaki şekilde gösterilmektedir.

$$y_j = 0.5\cdot\left(\left|x_j + 1\right| - \left|x_j - 1\right|\right) \qquad (6)$$

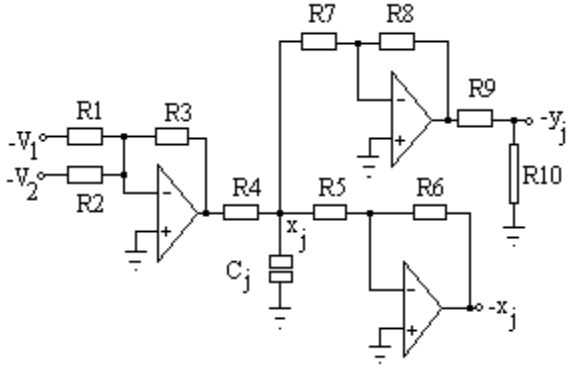
Denklem (5)'teki G_0 ve G_s sırasıyla komşu hücrelerin çıkışlarını ve durum değişkenlerinden yapılan bağlantıları göstermektedir. Önerilen DK-HSA modeli orijinal Chua ve Yang tanımlamasından G_s terimi ile farklılık göstermektedir [6] . Denklem (5)'te verilen durum denkleminden yola çıkılarak üç hücreli bir HSA yapısı aşağıdaki gibi tanımlanmaktadır.

$$\dot{x}_1 = -x_1 + a_1 y_1 + a_{12} y_2 + a_{13} y_3 + \sum_{k=1}^{3} s_{1k} x_k + i_1$$
$$\dot{x}_2 = -x_2 + a_{21} y_1 + a_2 y_2 + a_{23} y_3 + \sum_{k=1}^{3} s_{2k} x_k + i_2 \quad (7)$$
$$\dot{x}_3 = -x_3 + a_{31} y_1 + a_{32} y_2 + a_3 y_3 + \sum_{k=1}^{3} s_{3k} x_k + i_3$$

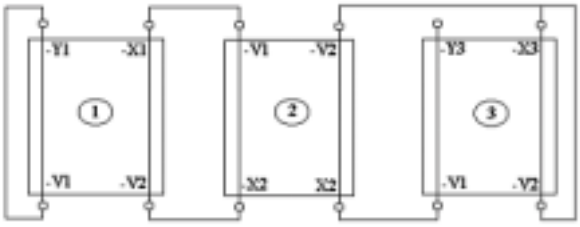
Burada x_1,x_2 ve x_3 durum değişkenlerini y_1, y_2 ve y_3 ise bunlara karşılık gelen çıkışları göstermektedir. $a_{12}= a_{13}= a_2= a_{23}= a_{32}= a_3= a_{21}= a_{31}=0$; $s_{13}= s_{31}= s_{22}=0$; $i_1= i_2= i_3=0$ seçilmek suretiyle Denklem (7) yeniden yazılacak olursa:

$$\begin{aligned} \dot{x}_1 &= -x_1 + a_1 y_1 + s_{11} x_1 + s_{12} x_2 \\ \dot{x}_2 &= -x_2 + s_{21} x_1 + s_{23} x_3 \\ \dot{x}_3 &= -x_3 + s_{32} x_2 + s_{33} x_3 \end{aligned} \quad (8)$$

Dikkat edilirse, Denklem (8)' deki (*a*) ve (*s*) parametreleri $a_1 = \alpha(m_1 - m_0)$; $s_{33} = 1-\gamma$; $s_{21} = s_{23} = 1$; $s_{11} = 1-\alpha \cdot m_1$; $s_{12} = \alpha$; ve $s_{32} = -\beta$ şeklinde belirlenerek ve x_1, x_2 ve x_3 sırasıyla Denklem (3)'teki eş değer boyutsuz durum denklemleri x, y ve z' ye eşit seçilerek, Chua devresinin durum denklemlerini elde etmek mümkün olmaktadır. Arena tarafından önerilen genelleştirilmiş hücre devresi ve hücrelerin bağlantı şeması Şekil-2(a) ve (b)'de sırasıyla verilmektedir.



(a)



(b)

Şekil-2. a) Arena'nın önerdiği tek bir DK-HSA hücresi [7]. b) Chua devresinin Arena'nın önerdiği üç DK-HSA hücresi kullanılarak modellenmesi.

3. DK-HSA Devreleri ile Tasarlanan Geribesleme Algoritmalı Kaotik Maskeleme Sistemi

Bu bölümde DK-HSA hücrelerinin kullanılarak geribeslemeli kaotik maskeleme sisteminin tasarlanabileceği gösterilecektir. Bu amaçla, HSA hücreleri ile modellenmiş Chua devresinin kullanıldığı geribesleme sistemine dayalı kaotik maskeleme sistemi gerçekleştirilmiştir. Önerilen DK-HSA-tabanlı geribeslemeli kaotik maskeleme sistemi Şekil 3'te verilmektedir. Şekil-3'te görüldüğü üzere vericinin ilk hücresi sürücü sistemi ve diğer iki hücre de cevap alt sistemlerini oluşturmaktadır. Birinci hücrenin çıkışından ikinci hücrenin girişine yapılan bağlantı kesilip yerine toplam işareti $m(t)=x_1(t)+s(t)$ uygulandığı durumda verici modül aşağıdaki durum denklemleri ile tanımlanır.

$$\begin{aligned} \dot{x}_1 &= -x_1 + a_1 y_1 + s_{11} x_1 + s_{12} x_2 \\ \dot{x}_2 &= -x_2 + s_{21} m(t) + s_{23} x_3 \\ \dot{x}_3 &= -x_3 + s_{32} x_2 + s_{33} x_3 \end{aligned} \quad (9)$$

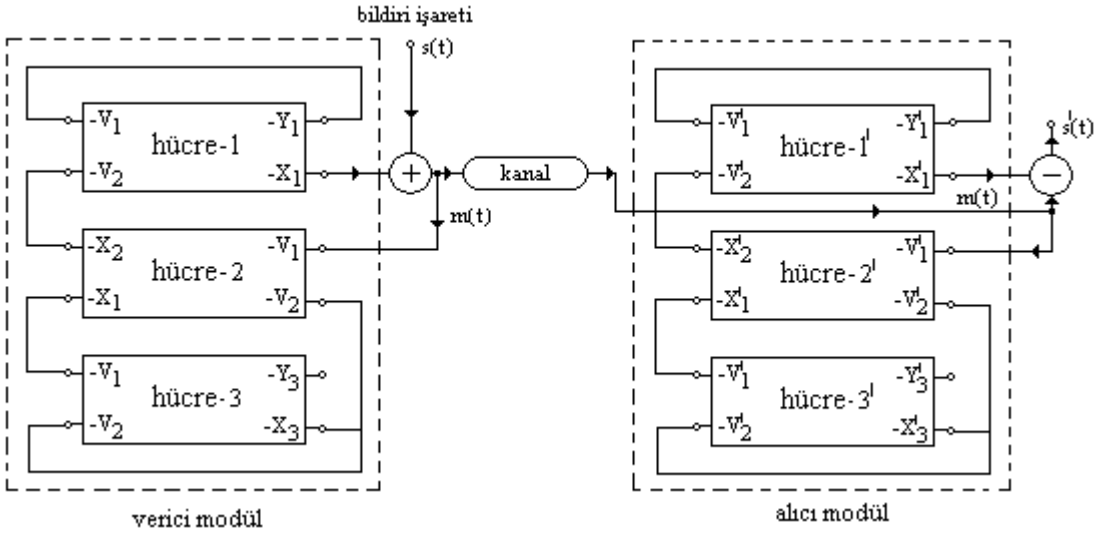
Benzer şekilde alıcı modül de aşağıdaki durum denklemleri ile tanımlanır.

$$\begin{aligned} \dot{x}'_1 &= -x'_1 + a_1 y'_1 + s_{11} x'_1 + s_{12} x'_2 \\ \dot{x}'_2 &= -x'_2 + s_{21} m(t) + s_{23} x'_3 \\ \dot{x}'_3 &= -x'_3 + s_{32} x'_2 + s_{33} x'_3 \end{aligned} \quad (10)$$

Arena, elde edilen bu eşitliklerdeki hücre parametrelerinin, Chua devresindeki $\beta = 14.286$, $\alpha = 9$, $\gamma = 0$, $m_0 = -1/7$ ve $m_1 = 2/7$ parametrelerine bağlı olarak bir kaotik çift-çeker (double-scroll attractor) oluşturması için, $a_1 = \alpha(m_1 - m_0)$; $s_{33} = 1-\gamma$; $s_{21} = s_{23} = 1$; $s_{11} = 1-\alpha \cdot m_1$; $s_{12} = \alpha$; seçmiştir. Buradan hareketle de a_1=3.857, s_{11}= - 1.5714, s_{32} = -14.286, s_{12}=9, $s_{21}= s_{23}= s_{33}$=1 olarak belirlemiştir [7].

Yukarıdaki parametreleri kullanarak tasarlanan, DK-HSA tabanlı alıcı ve verici devrelerden oluşan, geribeslemeli kaotik maskeleme sisteminin blok diyagramı Şekil-4'de ve bu tasarlanan sistemin açık devre şeması ise Şekil-5'te verilmektedir. Şekil-5'teki devrenin eleman değerleri ise:

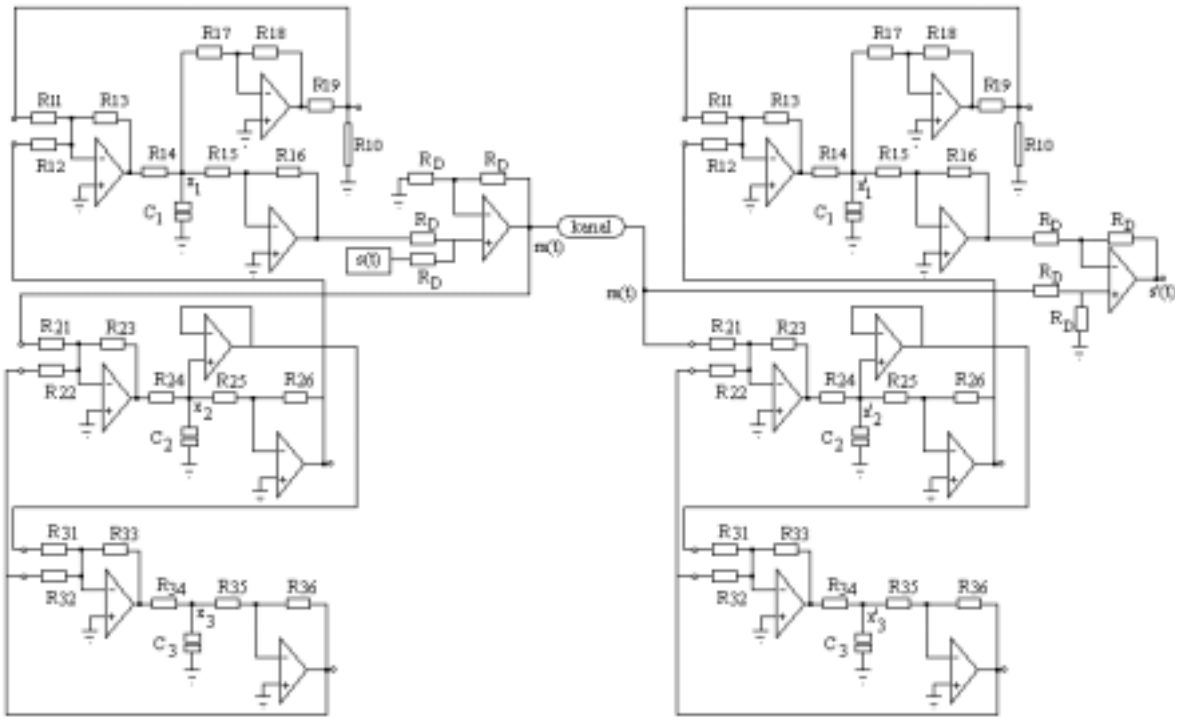
1.Hücre: R_{11}=13.2KΩ;R_{12}=5.7KΩ;R_{13}=20KΩ; R_{14}=390Ω; R_{15}=100KΩ; R_{16}=100KΩ; R_{17}=74.8KΩ; R_{18}=970KΩ; R_{19}=27KΩ ; R_{10}=2.22KΩ; C_1=51nF.
2.Hücre: $R_{21}=R_{22}=R_{23}=R_{25}=R_{26}$=100KΩ;$R_{24}$=1KΩ; C_2=51nF.
3.Hücre: R_{31}=7.8KΩ;$R_{32}=R_{33}=R_{35}=R_{36}$=100KΩ R_{34}=1KΩ; C_3=51nF; R_D=100K'dır.
Güç Kaynakları: V_{CC}= +15V; V_{EE}= -15V'tur.



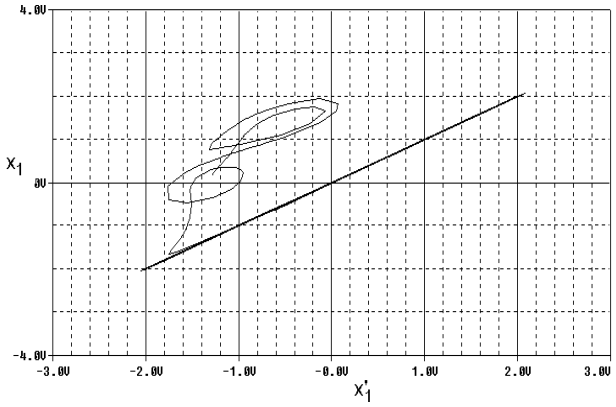
Şekil-3. DK-HSA-tabanlı geribeslemeli kaotik maskeleme sisteminin blok diyagramı.

4. Simülasyon Sonuçları

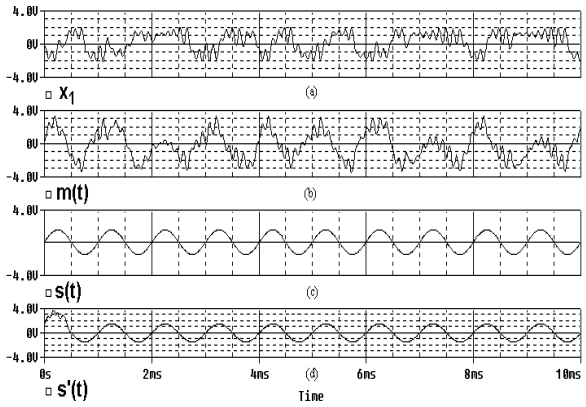
Şekil 4'te verilen geribeslemeli kaotik maskeleme sisteminin performansını göstermek üzere farklı analog işaretler, farklı genlik ve frekanslarda kullanılmışlardır. İlk simülasyon uygulamasında bildiri işareti sinüs ve üçgen dalga formlarında, 1KHz ve 1-2V genlik ile uygulanmaktadır. Yüksek genlikli bildiri işaretlerinin iletiminde kaotik senkronizasyonun bozulmadığını göstermek üzere yüksek-seviyeli bildiri işareti kullanılmıştır. Şekil 5, alıcı ve verici arasındaki senkronizasyon grafiğini göstermektedir. Bu grafikteki 45^0'lik doğru, alıcı devre ile verici devre arasında neredeyse mükemmel bir senkronizasyonun sağlandığını ve korunduğunu göstermektedir. Şekil 6 ve Şekil 7'de ise, DK-HSA tabanlı devrenin kaotik dinamiği, kanaldaki bildiri işareti ile toplanmış iletim işareti, vericideki bildiri ve alıcıda elde edilen bildiri işareti sinüs ve üçgen dalga için sırasıyla verilmektedir. Şekillerden elde edilen simülasyon sonuçları, DK-HSA tabanlı geribeslemeli kaotik maskeleme sisteminin, farklı bildiri işaretleri için mükemmel bir performans sergilediğini göstermektedir.



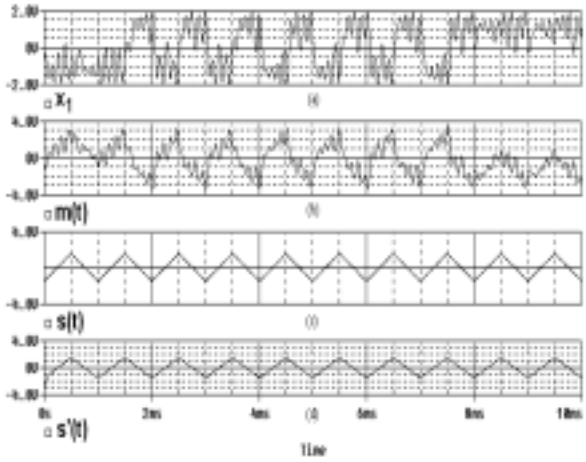
Şekil-4.DK-HSA-tabanlı geribeslemeli kaotik maskeleme sisteminin devre şeması.



Şekil-5. Alıcı verici arasındaki kaotik senkronizasyon.



Şekil-6. Sinüs dalga bildiri işareti için,
a) x_1=DK-HSA tabanlı devrenin kaotik dinamiği.
b) m(t)=kanalda iletilen işaret.
c) s(t)=vericideki bildiri işareti.
d) $s'(t)$= alıcıda elde edilen bildiri işareti.



Şekil-7. Üçgen dalga bildiri işareti için,
a) x_1=DK-HSA tabanlı devrenin kaotik dinamiği.
b) m(t)=kanalda iletilen işaret.
c) s(t)=vericideki bildiri işareti.
d) $s'(t)$= alıcıda elde edilen bildiri işareti.

5. SONUÇ

Bu çalışmada farklı analog sinyaller için DK-HSA tabanlı geribesleme algoritması kullanan bir kaotik maskeleme sistemi önerilmiştir. Önerilen bu yapı ile DK-HSA-tabanlı kaotik devrelerin eşlenik tekniğine dayalı güvenilir iletişim sistemlerine ek olarak, bildiri işaretinin oldukça geniş genlik ve spektral karakteristiklerinde etkili olarak kullanılabilen geribesleme algoritmalı kaotik maskeleme sisteminin gerçeklenmesinde de kullanılabileceği gösterilmiştir. Ayrıca Lorenz sistemi ve Chua devresi gibi farklı kaos üreteçlerinin kullanıldığı geribesleme metodunun aynı zamanda bir diğer kaos üreteci olan DK-HSA-tabanlı kaotik devre kullanılarak da gerçekleştirilebileceği gösterilmiştir.

KAYNAKLAR

[1] Kocarev L., Halle K.S., Eckert K., Chua L.O., Experimental demonstration of secure communication via chaotic synchronization, INT. JOURNAL OF BIFURCATIONS AND CHAOS 2, Vol. 3, pp. 709-713, 1992.

[2] Wu C.W. & Chua L.O., A simple way to synchronize chaotic systems with applications to communications, INT. JOURNAL OF BIFURCATIONS AND CHAOS 3, Vol. 6, pp.1619-1627,1993.

[3] Kolumban G., Kennedy M.P., Chua L.O., The role of synchronization in digital communications using chaos-Part I: Fundamental of digital communications, IEEE TRANS. ON CIRCUITS AND SYSTEMS-I 44, Vol.10, pp. 927-936, 1997.

[4] Kolumban G., Kennedy M.P., Chua, L.O., The role of synchronization in digital communications using chaos-Part II: Chaotic Modulation and Chaotic Synchronization, IEEE TRANS. ON CIRCUITS AND SYSTEMS-I 45, Vol.11, pp.1129-1140, 1998.

[5] Chua L.O., Wu C.W., Huang A., Zhong G.A.,Universal circuit for studying and generating chaos, IEEE TRANS. ON CIRCUITS AND SYSTEMS-I 40, Vol.10, pp.732-745, 1993.

[6] Chua L.O., Yang L., Cellular neural networks: Theory, IEEE TRANS. ON CIRCUITS AND SYSTEMS-I, Vol. 35, pp.732-745, 1988.

[7] Arena P., Baglio S., Fortuna L., Manganaro G., Chua's Circuit Can be Genarated by CNN Cells, IEEE TRAN ON CIRCUITS AND SYSTEMS-I, Vol. 42/2, pp. 123-125, 1995.

[8] Caponetto R., Lavorgna M., Occhipinti L., Cellular neural networks in secure transmission applications, PROC. of CNNA'96, pp. 411-416, 24-26 June, Sevilla, Spain, 1996.