FPGA Üzerinde Yeni Bir Kaotik Üretecin Gerçek Zamanlı Gerçekleştirilmesi

Real Time Implementation of A Novel Chaotic Generator on FPGA

Murat Tuna
Elektrik Teknolojisi
Kırklareli Üniversitesi
Kırklareli, Türkiye
murat.tuna@klu.edu.tr

İsmail Koyuncu
Kontrol ve Otomas. Tekn.
Düzce Üniversitesi
Düzce, Türkiye
ismailkoyuncu@duzce.edu.tr

Can Bülent Fidan
Mekatronik Mühendisliği
Karabük Üniversitesi
Karabük, Türkiye
cbfidan@karabuk.edu.tr

İhsan Pehlivan
Elektrik-Elektronik Müh.
Sakarya Üniversitesi
Sakarya, Türkiye
ipehlivan@sakarya.edu.tr

***Özetçe*—Bu çalışmada, literatüre sürekli zamanlı yeni bir otonom kaotik sistem sunulmuş ve FPGA üzerinde sayısal olarak gerçeklenmiştir. Sunulan yeni kaotik sistem, FPGA üzerinde IEEE 754-1985 kayan noktalı sayı formatında, Heun algoritması kullanılarak VHDL dili ile gerçekleştirilmiştir. Tasarlanan sistem Xilinx Virtex-6 FPGA çipinde sentezlenmiş ve test edilmiştir. Test sonuçlarına göre FPGA-tabanlı yeni kaotik işaret üretecinin çalışma frekansı 390 MHz olarak belirlenmiş ve çip istatistikleri ile performans sonuçları verilmiştir. Ayrıca, FPGA-tabanlı yeni kaotik işaret üretecinden elde edilen sonuçlar ile Matlab-tabanlı nümerik sonuçlar karşılaştırılmış ve başarılı sonuçlar elde edildiği görülmüştür. Geliştirilen FPGA tabanlı kaotik sistem modeli kullanılarak, rasgele sayı üretimi ve güvenli haberleşme gibi kaos tabanlı çeşitli mühendislik uygulamaları gerçekleştirilebilir.**

Anahtar Kelimeler*—*Kaos; Kaotik sistemler; Heun; FPGA; VHDL.

***Abstract*—In this study, a new continuous-time autonomous chaotic system has been presented and implemented on FPGA. Presented a new chaotic system has been designed using the IEEE 754-1985 floating-point format and implemented using Heun algorithm with VHDL language. The designed system has been synthesized and tested on Xilinx Virtex-6 FPGA chip. According to the test results, operation frequency of the FPGA-based a new chaotic signal generator is certain as 390 MHz and performance results have been given with chip statistics. In addition, the results obtained from FPGA-based new chaotic generator have been compared with the Matlab-based numerical results and it has been observed that obtained results are successful. By the developed FPGA-based novel chaotic system model, chaos-based various engineering applications such as true random number generation and secure communication system can be performed.**

Keywords*—*Chaos; Chaotic systems; Heun; FPGA; VHDL.

I. GİRİŞ

Günümüzde üzerinde pek çok araştırma ve çalışmalar yapılan doğrusal olmayan sistemler alanından birisi de kaos bilimi veya kaotik sistemlerdir. Kaotik çekerler başlangıç koşullarına hassas bağlı, karmaşık ve düzensiz görünümlü olmakla birlikte bu çekerler deterministik doğrusal olmayan zamanla değişen sürekli ve ayrık sistemlerde ortaya çıkarlar [1]. Kaotik sistemlerin araştırılması ve uygulanmasına yönelik bilimsel ve endüstriyel alanlarda önemli çalışmalar gerçekleştirilmektedir. Mühendisliğin pek çok alanında kaotik sistemlerin varlığının ortaya çıkarılması, bu konuda yapılan yoğun çalışmalar ve yaşanan gelişmeler kaotik sistemlerin birçok uygulama alanında kullanılabileceğini göstermiştir. Bu uygulama alanlarına kriptografi, güvenli haberleşme, biyomedikal, kuantum elektroniği, görüntü işleme, optik elektronik, kontrol, optimizasyon, yapay sinir ağları gibi alanlar örnek olarak verilebilir [2-4]. Kaotik işaretlerin elektronik mühendisliğindeki önemli araştırma ve uygulama alanları arasında güvenli haberleşme düzenekleri oluşturma, şifreleme, gürültü üreteçleri, ikili-kodlu rasgele sayı üreteçleri bulunmaktadır. Bu nedenle son zamanlarda yeni ve farklı özelliklere sahip kaotik işaret üreteçlerinin literatüre kazandırılması gerekliliği de her zaman önem arz etmektedir [5-8]. Kaotik sistemler ayrık zamanda kaotik sistemler ve sürekli zamanda kaotik sistemler olmak üzere ikiye ayrılır [9]. Sürekli zamanlı kaotik sistemler donanımsal olarak analog veya sayısal tabanlı olmak üzere iki farklı şekilde gerçekleştirilmektedir. Analog Bütünleyici Yarı İletken Metal Oksit (Complementary Metal Oxide Semiconductor (CMOS)) devre tabanlı kaotik osilatör yapılarının uygulamadaki sıcaklık ve zamanla değişen devre parametreleri gibi bazı zorluklarını ortadan kaldırmak için son yıllarda sürekli zamanlı kaotik sistemlerin sayısal tabanlı uygulama çalışmaları artış göstermiştir [10-11]. En iyi çözüm kaotik işaret üreteçlerin

978-1-4673-7386-9/15/$31.00 ©2015 IEEE

Sayısal İşaret İşlemciler (Digital Signal Processors (DSPs)), Uygulamaya Özel Tümleşik Devreler (Application Specific Integrated Circuits (ASIC)) ve Sahada Programlanabilir Kapı Dizileri (Field Programmable Gate Array (FPGA)) gibi entegre içerisinde sayısal devre tabanlı gerçekleştirilmesidir [12]. FPGA bu problemin üstesinden gelmekle birlikte aynı zamanda bu işlemleri yüksek frekanslarda da gerçekleştirebilmektedir. FPGA çipleri yüksek hız ve kapasiteleri nedeniyle özellikle yüksek performans ve işlemci gücü gerektiren kriptoloji ve güvenli haberleşme gibi uygulamalarda bilgi güvenliği kapasitesini iyileştirmekte önemli bir potansiyele sahiptir [13]. Kaotik osilatörlerin sayısal FPGA tabanlı modellenmesine yönelik çalışmalara literatürde oldukça fazla önem verilmektedir [1, 5, 12, 14-15]. Bazı sürekli zaman kaotik yapılar, $x(t)$ bir vektör olmak üzere,

$$\frac{d\,(x(t))}{dt} = f\,(x(t)) \qquad (1)$$

denklem (1) verilen adi diferansiyel denklemler ile ifade edilirler. Literatürdeki çalışmalar incelendiğinde sürekli zamanlı kaotik bir sistem oluşturmak için basit yapıda üçüncü dereceden diferansiyel bir denklem takımı ve nonlineer bir yapı çoğu zaman yeterli olmaktadır [16].

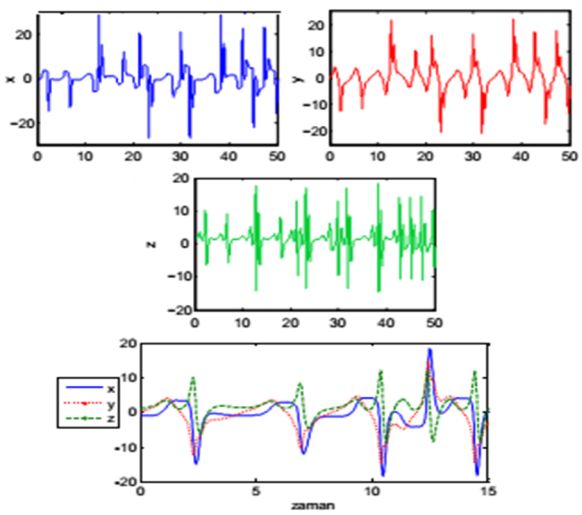
Bu çalışmada ikinci bölümde literatüre yeni sunulan kaotik sisteminin matematiksel modeli verilerek nümerik analiz ile zaman serileri ve faz porteleri elde edilmiştir. Üçüncü bölümde yeni kaotik çekerin FPGA tabanlı modeli sunularak çip üzerinden alınan test ve analiz sonuçları verilmiştir. Son bölümde bu çalışma kapsamında elde edilen sonuçlar değerlendirilmiştir.

II. YENİ KAOTİK SİSTEMİN MODELİ

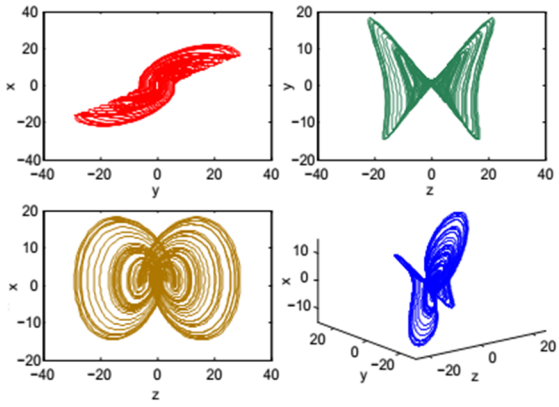
Adi diferansiyel denklemler şeklinde denklem (2)' de matematiksel olarak ifade edilen yeni kaotik sistemde x, y ve z kaotik durum değişkenleri ρ ve σ ise sistem parametreleridir.

$$\begin{cases} \dfrac{dx}{dt} = y\cdot(z-\rho) \\ \dfrac{dy}{dt} = y\cdot(z-\rho) - x\cdot(z+\rho) \\ \dfrac{dz}{dt} = -y\cdot(\rho\cdot x - y) - \sigma\cdot(z-\rho) \end{cases} \qquad (2)$$

Yeni kaotik çekerin sistem parametreleri ρ=1.3, σ=4 ve başlangıç şartları x0=-1, y0=0, z0=1 olarak alınmıştır. Doğrusal olmayan diferansiyel denklem sisteminin çözümü özellikle başlangıç şartlarına ve sistem parametrelerine bağladır. Bu sistemin nümerik olarak çözümünde Heun (iyileştirilmiş Euler) algoritması kullanılmıştır. Matlab programında nümerik analiz sonucunda Şekil 1'de yeni kaotik sistemin zaman serileri ve Şekil 2'te faz portreleri ile üç boyutlu çekici verilmiştir.



Şekil 1. Yeni kaotik sisteminin; **a)** x sinyali **b)** y sinyali **c)** z sinyali **d)** x, y ve z sinyali zaman serileri



Şekil 2. Yeni kaotik sisteminin Matlab nümerik modelleme sonuçları; **a)** x-y, **b)** y-z, **c)** x-z faz portreleri ve **d)** 3 boyutlu (x, y, z) kaotik çekici

III. FPGA TABANLI TEST SONUÇLARI

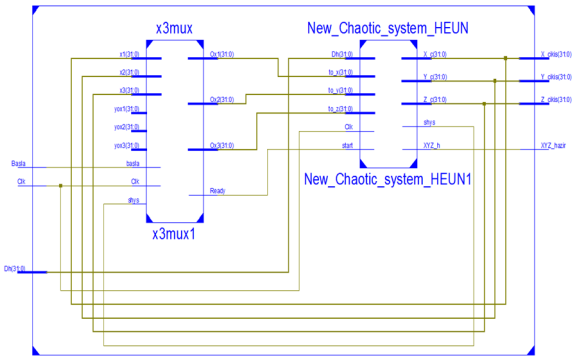
Diferansiyel denklemlerin nümerik çözümleri için literatürde çeşitli algoritmalar (Euler, Heun, RK-4 ve RK-5 Butcher) kullanılmaktadır. Tüm bu yöntemler diferansiyel denklemlerin sayısal olarak ayrıklaştırılmasında kullanılmaktadır. Bu yöntemlerden algoritma olarak en basit olanı Euler olmasına rağmen çok hassas çözümler üretememektedir [15]. Bu çalışmada kaotik sistemin FPGA tabanlı sayısal modelinin oluşturulması için Heun algoritması kullanılmıştır. Heun algoritması diferansiyel denklemin çözümünde Euler algoritmasından daha hassas, çözümler üretebilmekte ve Runge Kutta algoritmasına göre ise daha az çip donanımı kullanmaktadır. Bu yönteme ait denklemler (3) verilmiştir.

$$y(x_0) = y_i = y_0$$
$$y^0{}_{\lambda+1} = y_\lambda + f(y_\lambda) * \Delta h \quad (3)$$
$$y_{\lambda+1} = y_\lambda + \frac{f(y_\lambda) + y^0{}_{\lambda+1}}{2} * \Delta h$$

Bu denklemde y_0 kaotik sistemin başlangıç şartlarını ve Δh ise algoritmanın adım aralığını belirtmektedir. Heun algoritması iki adımdan oluşmaktadır. Birinci adımda $f(y^0{}_{\lambda+1})$ değeri hesaplanmaktadır. İkinci adımda hesaplanan $f(y^0{}_{\lambda+1})$ değeri ile y_λ değerleri kullanılarak sistemin bir sonraki değeri $f(y_{\lambda+1})$ hesaplanmaktadır. Heun algoritması, Euler algoritmasına göre daha hassas sonuçlar üretmesine rağmen yüksek frekanslı fonksiyonların eğimini yakalayamamaktadır. Heun tabanlı ayrıklaştırılmış Yeni kaotik sistemin matematiksel modeli denklem (4) verilmiştir. Bu denklemde $x(k)$, $y(k)$ ve $z(k)$ değerleri kullanılarak sırasıyla $x(k^0+1)$, $y(k^0+1)$ ve $z(k^0+1)$ ara değerleri hesaplanmaktadır. Daha sonra bu ara değerler kullanılarak diferansiyel denklemin $x(k+1)$, $y(k+1)$ ve $z(k+1)$ olan Δh adımı kadar sonraki ilk değerleri hesaplanmaktadır.

$$x(k^0+1) = x(k) + \Delta h.(\alpha.(y(k) - x(k)))$$
$$x(k+1) = x(k) + \Delta h \cdot \frac{(\alpha.(y(k) - x(k))) + x(k^0+1)}{2}$$
$$y(k^0+1) = y(k) + \Delta h.(-z \cdot x(k) + c \cdot y(k))$$
$$y(k+1) = y(k) + \Delta h \cdot \frac{(-z \cdot x(k) + c \cdot y(k)) + y(k^0+1)}{2} \quad (4)$$
$$z(k^0+1) = z(k) + \Delta h.(x(k) \cdot y(k) - b \cdot z(k))$$
$$z(k+1) = z(k) + \Delta h \cdot \frac{(x(k) \cdot y(k) - b \cdot z(k)) + z(k^0+1)}{2}$$

Denklem (4)' te verilen yeni kaotik sistemin modellenmesinde nümerik Heun algoritmasının adım aralığı $\Delta h = 0.005$ olarak alınmıştır. Kaotik sistemin Heun algoritması ile FPGA tabanlı olarak modellenmesinde donanım tanımlama dili olarak VHDL (**V**ery High Speed Integrated Circuit **H**ardware **D**escription **L**anguage (Çok Yüksek Hızlı Tümleşik Devre Donanım Tanımlama Dili)) kullanılmıştır. Heun algoritması kullanılarak VHDL dilinde FPGA-tabanlı gerçeklenen yeni kaotik sinyal üreteci için Xilinx ISE 14.1 tasarım programından elde edilen modelleme Şekil 3'te verilmiştir. Kaotik işaret üreteci MUX ve Yeni_Kaotik_Sistem olmak üzere iki kısımdan meydana gelmektedir. MUX ünitesi, sistemin başlangıç şartlarının sağlanması amacıyla kullanılmaktadır. Yeni_Kaotik_Sistem ise kaotik sinyalleri üreten bölümdür. Sistem, Basla sinyalini aldığında ilk başlangıç koşulu değerleri üreteç içerisinde tanımlanan değerlerden almaktadır. Kaotik işaret üreteci ilk değerini ürettiğinde ise shys sinyali '1' olmakta ve kaotik işaret üreteci başlangıç şartlarını üretecin çıkışından aldığı sinyallerden sağlamaktadır. Tasarlanan sistemin çıkışında 3 tane 32-bit kayan noktalı sayı standardında X_cikis, Y_cikis ve Z_cikis sinyalleri ile bu sinyallerin çıkışa aktarıldığını gösteren XYZ_hazir kontrol sinyali bulunmaktadır.



Şekil 3. FPGA-tabanlı yeni kaotik sistem en üst seviye blok diyagramı

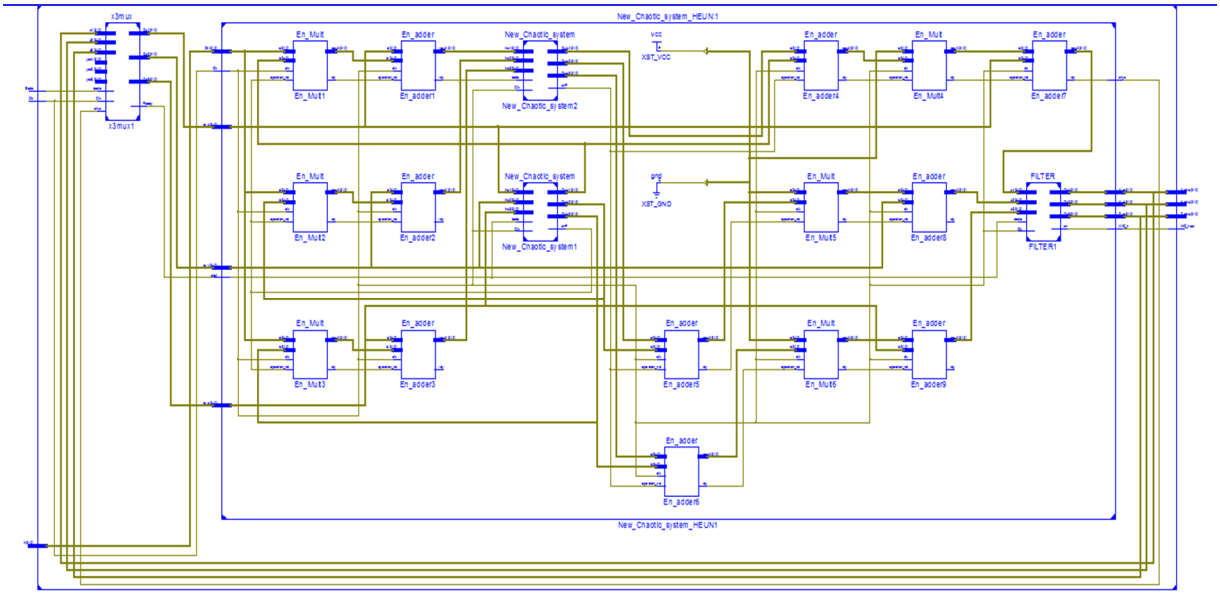
Kaotik işaret üretecin ikinci seviye blok diyagramı Şekil 4'te verilmiştir. Tasarlanan sistem içerisindeki kayan noktalı sayı formatındaki çarpma, toplama, çıkarma ve diğer modüller Xilinx firmasının geliştirdiği IP Core Generator kullanılarak oluşturulmuştur. Filter ünitesi ise istenmeyen sinyallerin çıkışa aktarılmasını engellemektedir. Şekil 5'te FPGA-tabanlı kaotik üretecin gerçeklenmesinden elde edilen Xilinx ISE simülasyon sonuçları verilmiştir. Ünite pipeline olarak çalışmakta ve ilk sonuçlarını 54 saat darbesi sonucunda üretmektedir. Bundan sonra her 54 saat darbesinde yeni sonuçlar üretilmektedir. Gerçeklenen kaotik işaret üreteci Xilinx firmasının ürettiği Virtex-6 ailesinin XC6VLX75T-3FF785 çipine yüklenerek test edilmiştir. Yerleştirme ve bağlama (Place-Route) işleminin ardından elde edilen çip istatistikleri Tablo 1'de verilmiştir. Tasarlanan ünitenin minimum çalışma periyodu 2,56 ns' dir.

Lojik Kullanım	Slice Reg. Sayısı	LUT Sayısı	Occupied Slice Sayısı	IOB Sayısı	Çalışma Frekans (MHz)
Kullanılan	21,499	20,333	6,283	131	390.076
Kul. Oranı	23%	43%	53%	15%	

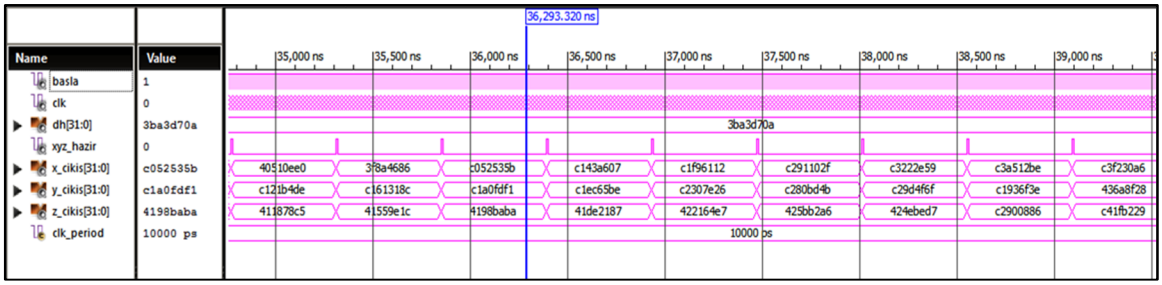
Tablo 1. FPGA-tabanlı yeni Kaotik işaret üreteç ünitesi için Xilinx Virtex-6 çip istatistikleri

IV. SONUÇLAR

Bu çalışmada, literatüre yeni sunulan kaotik sistemin zaman serileri ve faz portreleri incelenmiştir. Ayrıca sunulan bu yeni kaotik sistem FPGA üzerinde VHDL dilinde IEEE 754-1985 kayan noktalı sayı standardına uygun bir biçimde tasarlanmış ve tasarımın çalışma frekansı 390 MHz olarak elde edilmiştir. Bu çalışma ile literatüre ilk defa sunulan kaotik sistemin FPGA üzerinde tasarımının gerçekleştirilmesi ile rasgele sayı üretimi ve güvenli haberleşme sistemi gibi kaos tabanlı mühendislik uygulamalarında kullanılabileceği gösterilmiştir.



Şekil 4. FPGA-tabanlı yeni kaotik işaret üreteci ikinci seviye blok diyagramı



Şekil 5. FPGA-tabanlı yeni kaotik işaret üreteci Xilinx ISE simülasyon sonuçları

KAYNAKÇA

[1] Merah, L., Pacha, A. A., Said, N. H., Mamat, M., "A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation", Applied Mathematical Sciences, 7(55): 2719-2734, 2013.

[2] Banerjee, S., Kurths, J., "Chaos and Cryptography: A new Dimension in Secure Communications", The European Physical Journal Special Topics, 223(8): 1441-1445, 2014.

[3] Lawande, Q. V., Ivan, B. R., and Dhodapkar, S. D., "Chaos Based Cryptography: A New Approach to Secure Communications", Barc Newsletter, *Vol.* 258, 2005.

[4] Xiong, A., Zhao, X., Han, J., Liu, G., "Application of the Chaos Theory in the Analysis of EMG on Patients with Facial Paralysis", In Robot Intelligence Tech. and App., Springer, 274: 805-819, 2014.

[5] Koyuncu, İ., Özcerit, A. T., Pehlivan, I., "Implementation of FPGA-based Real Time Novel Chaotic Oscillator", Nonlinear Dyn., Springer, 75(1-2): 49-59, 2014.

[6] Deng, K., Li, J., Yu, S., "Dynamics Analysis and Synchronization of A New Chaotic Attractor", Elsevier Optik, *Vol.*125: 3071-3075, 2014.

[7] Abooee, A., Yaghini-Bonabi, H. A., Jahed-Motlagh, M. R., "Analysis and Circuitry Realization of A Novel Three-Dimensional Chaotic System", Commun Nonlinear Sci Numer Simulation, 18: 1235-1245, 2013.

[8] Pehlivan, İ., Wei, Z., "Analysis, Nonlinear Control, and Chaos Generator Circuit of Another Strange Chaotic System", Turk J Elec Eng & Comp Sci, 20(2):1229-1239, 2012.

[9] Uyaroğlu, Y., "Kaotik Lorenz Sisteminin Yarı-Ayna Yapısı", Journal of İstanbul Kultur University, *Vol.* 3, 141-146, 2006.

[10] Pande, A., Zambreno, J., "Design and hardware implementation of a chaotic encryption scheme for real-time embedded systems", Int. Conf. on Signal Processing and Comm., 1-5, 2010.

[11] Eroğlu, C., "Implementation of synchronized chaotic systems by FPGA", Graduate Sch. of Eng. and Sci. of Izmir Inst. of Tech., Izmir, Turkey, 2007.

[12] Azzaz, M. S., Tanougast, C., Sadoudi, S., Fellah, R., Dandache, A., "A New Auto-Swiched Chaotic System and Its FPGA Implementation", Comm. In Nonlinear Sci. and Numerical Sim., Elsevier, 18(7): 1792-1804, 2013.

[13] Sadoudi, S., Azzaz, M. S., Tanougast, C., Dandache, A., "Real Time Hardware Implementation of A New Duffing's Chaotic Attractor", 16th IEEE International Conference on Electronics, Circuits, and Systems, 559-562, 2009.

[14] Koyuncu, İ., Özcerit A. T., Pehlivan, İ., "An Analog Circuit Design and FPGA-Based Implementation of the Burke-Shaw Chaotic System", Optoelectronics and Advanced Materials–Rapid Communications, *Vol.* 7: 635-638, 2013.

[15] Koyuncu, İ., Özcerit, A. T., Pehlivan, İ., "FPGA-Based A Chaotic Oscillator Design and Implementation", 1st International Symposium on Innovative Technologies in Engineering and Science, 873-879, 2013.

[16] Chua, L., Wu, W., Huang, A., Zhong, G., "A Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos", IEEE Trans. Circuits and Systems I, 40: 732-744, 1993.