FPGA Tabanlı Kaotik Osilatör Tasarımı ve Gerçeklenmesi

*[1]Ismail Koyuncu, [2]Ahmet Turan Ozcerit and [3]Ihsan Pehlivan
*[1]Control and Automation Technology Program, Duzce Vocational High School, Duzce University, Turkey
[2]Faculty of Technology, Department of Computer Engineering, Sakarya University, Turkey
[3]Faculty of Technology, Electrical and Electronics Engineering Department, Sakarya University, Turkey

Özet

Günümüzde kriptoloji ve güvenli haberleşme alanlarında kaotik sistemler ve kaos tabanlı uygulamalar yaygın bir şekilde kullanılmaya başlanmıştır. Özellikle kaos tabanlı kriptolojik uygulamalarda kullanılan en temel yapılardan birisi de kaotik sinyali üreten bir kaos üretecidir. Bu çalışmada, yeni bir kaotik sistem PC üzerinde nümerik olarak modellenmiş ve faz portresi yönteminden yararlanılarak sistemin kaos analizi yapılmıştır. Kaotik sistem ayrıca FPGA üzerinde Heun metodu kullanılarak modellenmiştir. Tasarlanan sistem, Virtex-6 FPGA çipi için sentezlenmiş ve test edilmiştir. Test sonuçlarına göre tasarlanan kaotik sistemin çalışma frekansı 390.076MHz'dir. Ayrıca FPGA tabanlı kaotik osilatör bir milyon veriyi 0.151s'de üretebilmektedir. Bu çalışmada sunulan FPGA tabanlı kaotik sistem modeli kullanılarak, kriptoloji ve güvenli haberleşme alanlarında çeşitli uygulamalar gerçekleştirilebilir.

Anahtar Kelimeler: Kaos, kaotik osilatör, VHDL, FPGA, Heun

FPGA-Based A Chaotic Oscillator Design and Implementation

Abstract

Chaotic systems and chaos-based applications have begun widely to be used in the field of cryptography and security communication nowadays. Especially one of the most significant structures used in chaos-based applications is chaotic signal generator. In this paper, a novel chaotic system on PC numerically has been modeled and the chaos analysis of the system has been realized using phase portraits method. Also, the chaotic system has been modelled using Heun method on FPGA. Designed system has been synthesized and tested for Virtex-6 FPGA chip. According to the test results, operating frequency of designed chaotic system is 390.076MHz. In this case, FPGA-based chaotic system is able to generate a million data set at 0.151s. Using the FPGA-based chaotic system model proposed in this paper can be performed various applications in field of encryption and secure communication.

Key words: Chaos, chaotic oscillator, VHDL, FPGA, Heun

1. Giriş

Kaos ve kaotik sistemlerin araştırılması ve mühendislik alanlarında uygulanmasına yönelik bilimsel ve endüstriyel alanlarda önemli çalışmalar gerçekleştirilmektedir. Bu çalışma alanlarına kriptoloji [1], haberleşme [2], görüntü işleme [3], yapay sinir ağları [4] ve kontrol [5] örnek

*Corresponding author: Address: Control and Automation Technology Program of Duzce Vocational High School, Duzce University, Uzunmustafa Mah. 81010 Düzce/Turkey. E-mail address: ismailkoyuncu@duzce.edu.tr, Phone: (+90)-380-524-0098, Fax: (+90)-380-524-0097

olarak verilebilir. Kaotik tabanlı mühendislik uygulamalarında kullanılması gereken en temel yapılardan birisi kaotik işareti üreten bir kaos üretecidir. Kaos üreteçleri, donanımsal olarak analog veya sayısal tabanlı olmak üzere iki farklı şekilde gerçekleştirilebilmektedir. Sayısal devre tabanlı kaotik üreteçler literatürde sayısal işaret işlemciler (Digital Signal Processing (DSP)) [6], uygulamaya özel tümleşik devreler (Application Specific Integrated Circuits (ASIC)) [7], ve alanda programlanabilir kapı dizileri (Field Programmable Gate Array (FPGA)) [8] gibi farklı yapılarla gerçeklenebilmektedir. ASIC tabanlı kaotik üreteçlerden diğer sayısal tabanlı eşdeğerlerine göre daha yüksek performans elde edilmektedir. Ancak ASIC tabanlı uygulamalar esnek bir yapıya sahip olmamakla birlikte bu sistemlerin ilk tasarım ve test maliyeti oldukça yüksektir. Ayrıca ASIC ile yapılan tasarımların maliyetinin düşürülmesi için önemli miktarda üretim yapılmalıdır. ASIC tabanlı seri üretim aşamalarında yapılacak bir hata oldukça yüksek maliyet ve uzun zaman kaybına da neden olmaktadır. DSP çipleri, işlemleri sıralı (sequential) olarak gerçekleştirmektedir. Sürekli zamanlı kaotik sistemler genel olarak en az iki veya üç diferansiyel denklemden oluşmakta ve çıkış sayısı da buna göre değişmektedir. Çıkış sinyali değerlerinin mikroişlemci veya DSP tabanlı sistemler tarafından sıralı bir şekilde hesaplanması uzun zaman almakta ve çalışma frekansları düşük kalmaktadır. FPGA çipleri paralel işlem yapabilmekle birlikte oldukça esnek bir yapıya sahiptirler. FPGA çiplerinin tasarım ve test maliyetleri de düşüktür. Ayrıca sayısal tabanlı olmaları, tekrar programlanabilme özellikleri sayesinde FPGA tabanlı kaotik sistemler ve bu sistemlerin kullanıldığı uygulamalar daha esnek olmaktadır. Kaotik devre modelleri tekrar programlanabilir veya yeniden yapılandırılabilir sistemler içerisinde gerçeklemeye uygundur. Bu sayede kaotik sistemler parametre değişimlerine göre farklı formda işaret üretebilmektedir. Ayrıca ilgili kaotik sistemin farklı doğrusal olmayan fonksiyonlarla alternatifli olarak gerçekleştirilmesi söz konusu olmaktadır. Bu özelliklere sahip kaotik devre modelleri, tekrar yapılandırılabilir bir şekilde esnek ve donanım karmaşası olmadan tasarlanabilirler.

Bu çalışmada, ikinci bölümde seçilen kaotik sistemin nümerik modeli ve faz portreleri sunulmuştur. Üçüncü bölümde, kaotik sistemin FPGA tabanlı modeli tanıtılmıştır. Dördüncü bölümde, FPGA tabanlı kaotik modelin test sonuçları verilmiştir. Son bölümde ise elde edilen sonuçlar yorumlanmıştır.

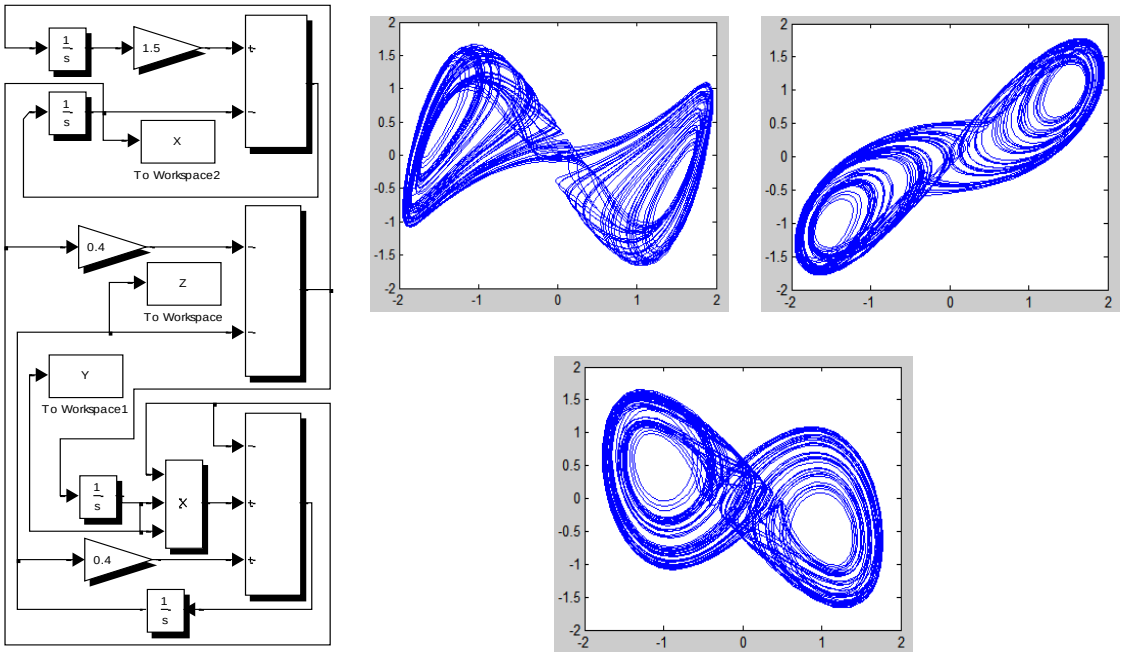
2. Kaotik Sistem Nümerik Modeli

Kaotik sistemler genellikle diferansiyel denklemler ile ifade edilmektedir. Aşağıda bir kaotik sisteme ait diferansiyel denklemler (1) verilmiştir [9].

$$\begin{aligned} dx/dt &= \alpha.y - x \\ dy/dt &= -\beta.x - z \\ dz/dt &= \gamma.z + x.y^2 - x \end{aligned} \tag{1}$$

Burada sistem parametreleri α=1.5, β=0.4 ve γ=0.4 ve başlangıç şartları x_0=0, y_0=0, z_0=0.1 olarak alınmıştır. Sistem parametreleri ve başlangıç şartları sistem dinamik davranışını çok büyük oranda değiştirebilmektedir. Hatta sistem parametrelerinin değişimi sistemin kararlı veya kararsız

dinamik davranışını belirleyebilmektedir. Sürekli zamanlı nonlineer dinamik bir sistemin kaotik davranış gösterebilmesi için sistemde en az bir nonlineer terim bulunmalı ve sistem en az üç değişken içermelidir. Bir sistem bu iki şartı sağlıyorsa, sistemin kaos analizleri yapılabilir. Bununla beraber, sistem ayrık zamanlı ise bu iki şartın bulunmasına gerek yoktur. Bir veya iki boyutlu ayrık denklemlerde kaotik davranış ortaya çıkabilmektedir. Bir sistemin kaos analizinin yapılabilmesi için geliştirilmiş çeşitli yöntemler bulunmaktadır. Bu yöntemlerden bazıları şunlardır: Sistemin faz uzayının incelenmesi, yörüngenin izlenmesi, Poincare haritalama, güç spektrumu, çatallaşma diyagramı ve Lyapunov üstelleri spektrumu. Yukarıda diferansiyel denklem takımları verilmiş olan kaotik sistem Matlab-Simulink program kullanılarak modellenmiş ve şekil 1.(a)'da kaotik sistemin modeli sunulmuştur. Bu çalışma da kaos analizi için faz portresi yönteminden yararlanılmış ve sonuçlar şekil 1.(b)'de verilmiştir. Şekilden görüldüğü gibi sistem değişkenleri *x, y* ve *z* sürekli olarak değişmekte ancak bu değişim belirli aralıklar içerisinde sınırlı kalmaktadır.



Şekil 1. (a) Kaotik sistemin Matlab-Simulink modeli (b) x-z, x-y ve y-z sinyalleri faz portreleri

3. Kaotik Sistemin FPGA Tabanlı Gerçeklenmesi

Literatürde diferansiyel denklemlerin nümerik çözümlerinin gerçekleştirilebilmesi amacıyla çeşitli yöntemler geliştirilmiştir. Bu yöntemlerden en basit olanı Euler algoritmasıdır. Ancak Euler algoritması genel olarak çok hassas çözümler üretememektedir. Ayrıca kaotik sistemler başlangıç şartlarına çok hassas bağımlı olduklarından başlangıç şartlarındaki az bir değişim sistemin dinamik davranışını oldukça değiştirmektedir. Bu nedenle sistemin FPGA tabanlı sayısal modeli oluşturulurken daha hassas sonuçlar üreten ve Euler algoritmasının daha gelişmiş hali olan Heun algoritması kullanılmıştır. Aşağıda y_0 kaotik sistemin başlangıç şartlarını ve $\tau=0.05$

algoritmanın adım sayısını belirtmek üzere Heun algoritmasına ait denklemler (2) verilmiştir.

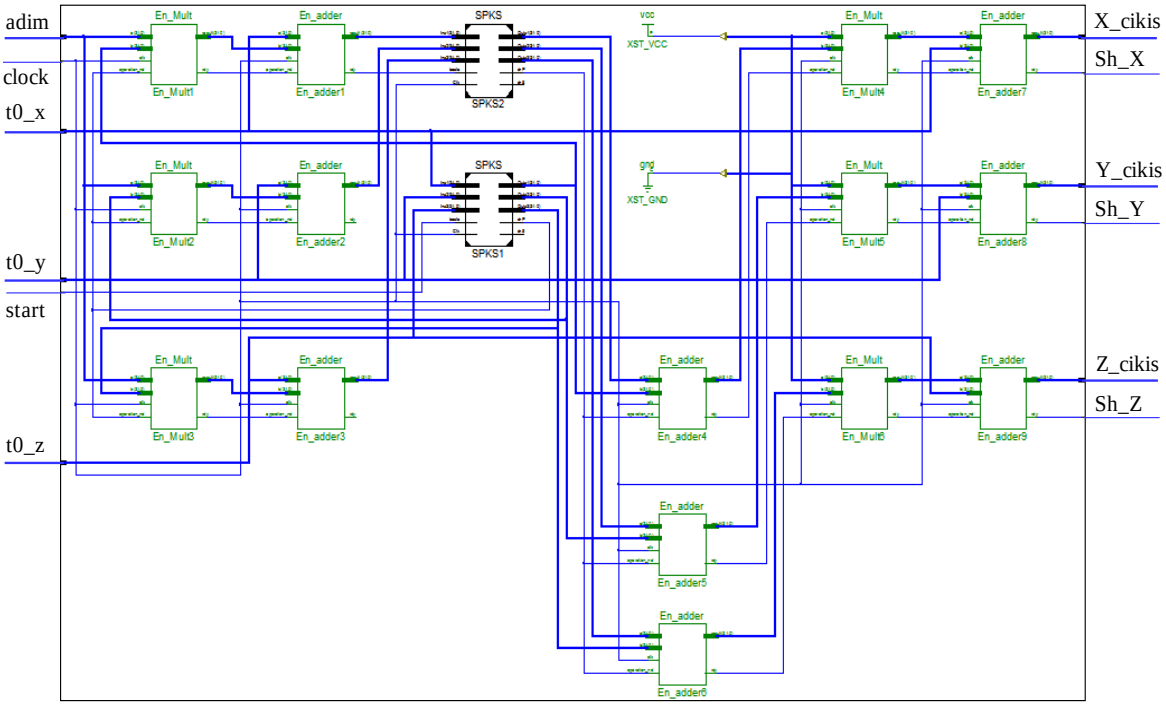
$$
\begin{aligned}
&y(x_0) = y_i = y_0 \\
&f(y^0{}_{\lambda+1}) = y_\lambda + f(y_\lambda)\tau \\
&f(y_{\lambda+1}) = y_\lambda + \frac{f(y_\lambda) + f(y^0{}_{\lambda+1})}{2}\tau
\end{aligned}
\tag{2}
$$

Örnek kaotik sistemin sayısal olarak çözümlenebilmesi amacıyla kullanılan algoritma iki aşamadan oluşmaktadır. Bu yaklaşım kullanılarak diferansiyel denklemler hesaplanırken ilk aşamada $f(y^0{}_{\lambda+1})$ değeri hesaplanmaktadır. Bu değer hesaplandıktan sonra $f(y_{\lambda+1})$ ifadesinde yerine konularak diferansiyel denklemin üreteceği değer elde edilmiş olur. Heun algoritması kullanılarak kaotik sistemin ayrıklaştırılmış matematiksel modeli eşitlik (3)'te verilmiştir. Bu denklemlerdeki $x(k^0+1)$, $y(k^0+1)$ ve $z(k^0+1)$ değerleri Heun algoritmasında diferansiyel denklemin sonuçlarının elde edilmesi için gerekli olan ara değerleri ifade etmektedir. Matematiksel modeldeki *x(k), y(k)* ve *z(k)*'nın başlangıç değerleri olan $x(t_0)=x(k)=0.0$, $y(t_0)=y(k)=0.0$ *ve* $z(t_0)=z(k)=0.1$ olarak alınmıştır.

$$
\begin{aligned}
&x(k^0+1) = x(k) + \tau\left(\alpha.y(k) - x(k)\right) \\
&x(k+1) = x(k) + \tau\left(\left(\alpha.y(k) - x(k)\right) + x(k^0+1)\right)/2 \\
&y(k^0+1) = y(k) + \tau\left(-\beta.x(k) - z(k)\right) \\
&y(k+1) = y(k) + \tau\left(\left(-\beta.x(k) - z(k)\right) + y(k^0+1)\right)/2 \\
&z(k^0+1) = z(k) + \tau\left(\gamma.z(k) + x(k).y(k)^2 - x(k)\right) \\
&z(k+1) = z(k) + \tau\left(\left(\gamma.z(k) + x(k).y(k)^2 - x(k)\right) + z(k^0+1)\right)/2
\end{aligned}
\tag{3}
$$

Bu çalışmada örnek kaotik sistemin Heun algoritması ile FPGA tabanlı olarak modellenebilmesi için 32-bit IEEE 754-1985 kayan noktalı sayı standardı kullanılmış ve örnek kaotik sistem bir donanım tanımlama dili olan VHDL kullanılarak kodlanmıştır. Tasarlanan ünite içerisinde kullanılan kayan noktalı sayı standardındaki çarpma, toplama ve çıkarma modülleri, Xilinx IP CORE Generator kullanılarak oluşturulmuştur. Şekil 2'de örnek sisteme ait tasarlanan kaotik osilatörün blok diyagramı görülmektedir. Ünite girişinde bulunan 32-bitlik *to_x, to_y* ve *to_z* sinyalleri sistemin ilk çalışması anında ihtiyaç duyduğu başlangıç şartlarını sağlamaktadır. Tasarlanan Heun tabanlı kaotik osilatörde 3 adet 32-bit'lik *X_cikis, Y_cikis* ve *Z_cikis* çıkış sinyalleri ve bu çıkış sinyallerinin hazır olduğunu göstermek amacıyla kullanılan 1-bitlik *Sh_X, Sh_Y* ve *Sh_Z* sinyalleri bulunmaktadır. Örnek kaotik osilatöre *Clock* sinyali ve başlangıç şartları

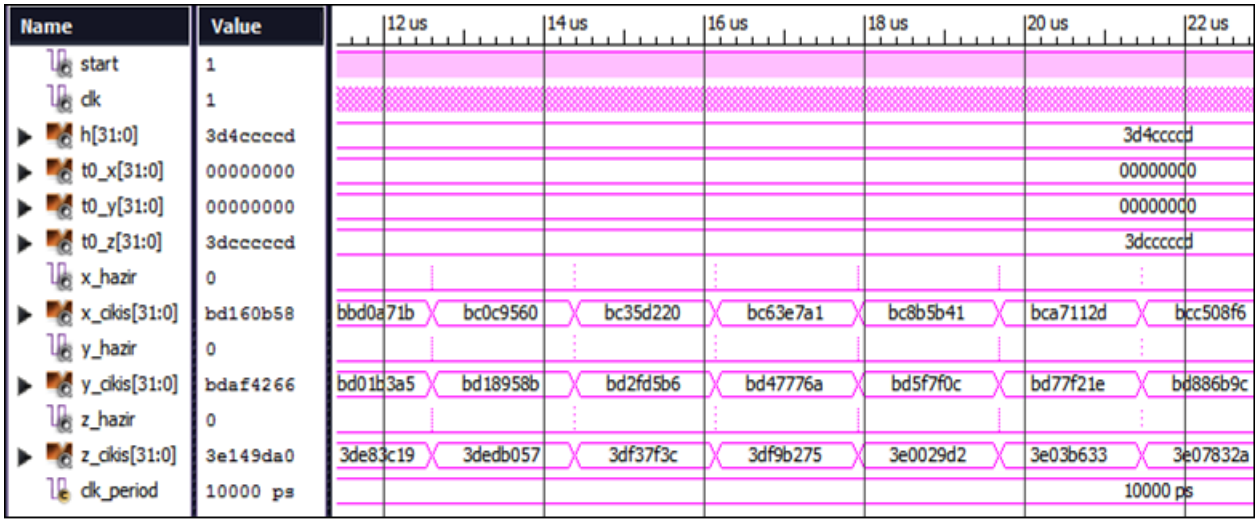
uygulandığı andan itibaren sistem 132 saat periyodu boyunca çalışmakta ve bunun sonunda sonuçları *X_cikis*, *Y_cikis* ve *Z_cikis* çıkış sinyallerine iletmektedir. Ayrıca sistem *X_cikis*, *Y_cikis* ve *Z_cikis* sinyallerini ürettiğinde, *Sh_X*, *Sh_Y* ve *Sh_Z* kontrol sinyalleri çıkışları '1' olmakta ve bu şekilde sisteme bağlanabilecek diğer ünitelerle senkron bir şekilde çalışması sağlanmaktadır.



Şekil 2. Örnek kaotik sistemin FPGA tabanlı modeli

4. FPGA Test Sonuçları

Heun tabanlı kaotik osilatör ünitesi, Xilinx Virtex-6 ailesi XC6VCX75T çipi için sentezlenerek, FPGA kaynak kullanımına ve saat hızlarına ait parametrelerin istatistikleri incelenmiştir. Ünitenin belirlenen veriyi işleme süresi, Xilinx ISE Design Tools 14.2 simülasyon programı kullanılarak elde edilmiştir. Şekil 3'te Xilinx ISE Simülatöründe osilatör ünitesinin FPGA'de gerçeklenmesinden elde edilen *x*, *y* ve *z* sinyallerine karşılık gelen *X_cikis*, *Y_cikis* ve *Z_cikis* sinyallerinin zaman serilerine ait değerler görülmektedir. Osilatörün FPGA'de gerçeklenmesinden elde edilen *X_cikis*, *Y_cikis* ve *Z_cikis* sinyallerinin zaman serilerine ait değerler 32-bit kayan noktalı sayı formatında olduğu için osilatör çıkışlarının doğrudan gözlenmesi oldukça zor olmaktadır. Bu nedenle elde edilen *X_cikis*, *Y_cikis* ve *Z_cikis* değerlerinin ISE simülasyon ekranında daha rahat bir biçimde incelenmesini sağlamak amacıyla sinyal çıkışları *onaltılık* sayı formatında verilmiştir. Ünite 132 saat darbesi sonunda ilk sonuçları üretmektedir. Bu süreden önce osilatör ünitesinin çıkışlarından herhangi bir veri alınamamaktadır. Bundan sonra her 132 saat darbesinde modül çıkışlarından istenilen değerler alınabilmekte ve modül pipeline olarak çalışabilmektedir.



Şekil 3. Xilinx ISE Design Tools Simülatörü tarafından üretilen kaotik osilatör çıkışları

Tablo 1'de sentezleme işleminin ardından yapılan place & route sonrasında elde edilen FPGA çip istatistikleri verilmiştir. Ünitenin minimum darbe periyodu 2.564ns'dir. Bu sentez sonuçları Xilinx Virtex-6 ailesi XC6VCX75T çipi için elde edilmiştir. Simülasyonda kullanılan FPGA çipi Virtex-6 ailesinin en küçük çiplerinden birisidir. Eğer aynı çip ailesinden daha büyük kaynaklara sahip farklı bir çip kullanılırsa çip kaynak kullanım oranları düşecektir.

Tablo 1. Tasarlanan kaotik osilatör için kullanılan FPGA kaynakları

FPGA Çipi	Slice Reg. Sayısı / %	LUTs Sayısı / %	Occupied Slices Sayısı / %	Bounded IOBs Sayısı / %	Min. Clock Periyodu (ns)
Virtex-6	18,491 / 19	17,007 / 36	5,656 / 48	229 / 63	2.564

5. Sonuçlar

Bu çalışmada sunulan kaotik sistem, Matlab-Simulink'te modellenmiş ve elde edilen verilerle sistemin faz portresi çıkartılmıştır. İkinci olarak örnek kaotik sistem, Heun algoritması kullanılarak VHDL dilinde kodlanmış, Xilinx ISE 14.2 tasarım ortamında Virtex-6 FPGA çipi için sentezlenmiş ve test edilmiştir. Elde edilen test sonuçlarına göre FPGA tabanlı kaotik osilatörün çalışma frekansı 390.076MHz'dir. FPGA tabanlı tasarım bir milyon veriyi 0.151s gibi çok kısa bir sürede hesaplayabilmektedir. Örnek kaotik sistemin FPGA tabanlı modelinden elde edilen başarılı sonuçlar bu yeni kaotik osilatörün kriptoloji ve güvenli haberleşme uygulamalarında kullanılabileceğini göstermiştir. İleride FPGA tabanlı yeni kaotik osilatör kullanılarak senkronizasyon, bilgi gizleme ve rasgele sayı üretimi gibi çeşitli uygulamalar gerçekleştirilebilir.

Kaynaklar

[1] Bakhache B, Ghazal JM, Assad SE. Improvement of the security of zigbee by a new chaotic algorithm. Systems Journal, IEEE, 2013; doi: 10.1109/JSYST.2013.2246011.
[2] Jia-Gui W, Zheng-Mao W, Yu-Ran L, Li F, Xi T, Guang-Qiong X. Simulation of bidirectional long-distance chaos communication performance in a novel fiber-optic chaos synchronization system. Lightwave Technology Journal of, 2013; 31:3-461.
[3] Azhar H, Amer A. Classification of surveillance video objects using chaotic series. Image Processing, IET, 2012; 6:7919.
[4] Decai Li, Min Han, Jun Wang. Chaotic time series prediction based on a novel robust echo state network. Neural Networks and Learning Systems, IEEE Transactions on, 2012; 23:5-787.
[5] Zhen Z, Chau KT, Zheng W. Chaotic speed synchronization control of multiple induction motors using stator flux regulation. Magnetics, IEEE Transactions on, 2012; 48:11-4487.
[6] Kharel R, Busawon K, Aggoune W, Ghassemlooy Z. Implementation of a secure digital chaotic communication scheme on a DSP board. Communication systems networks and digital signal processing (CSNDSP), 7th International Symposium on, 2010; 212.
[7] Yiwei Z, Zexiang L, Xinjian Z. A chaos-based image encryption ASIC using reconfigurable logic. Circuits and Systems, IEEE Asia Pacific Conference on, 2008; 1782.
[8] Azzaz MS, Tanougast C, Sadoudi S, Fellah R, Dandache A. A new auto-swiched chaotic system and its FPGA implementation. Communications in Nonlinear Science and Numerical Simulation, 2012; 1007.
[9] Sundarapandian V, Pehlivan I. Analysis, control, synchronization, and circuit design of a novel chaotic system. Mathematical and Computer Modelling, 2012; 55:7-1904.