Sözde Rastsal Sayı Üretecinin Yapay Sinir Ağları ile Güçlendirilmesi

Improving Pseudo Random Number Generator Using Artificial Neural Networks

Apdullah Yayık
Enformatik Ana Bilim Dalı
Mustafa Kemal Üniversitesi
Hatay, Türkiye
apdullahyayik@gmail.com

Yakup Kutlu
Bilgisayar Mühendisliği Bölümü
Mustafa Kemal Üniversitesi
Hatay, Türkiye
ykutlu@mku.edu.tr

***Özetçe*— Sözde rastsal sayı üreteçleri ürettiği sayılar dizisi arasında ilişki kurulamayacak algoritma türleridir. Rastsal sayı üretimi fiziksel ve istatistiksel çalışmalardan kriptoloji başta olmak üzere birçok bilimsel çalışmada kullanılmaktadır. Bu çalışmada Çok Katmanlı yapay sinir ağları kullanılarak Mevcut rastsal sayı üreteçleri ile üretilen sayıların rastsallığı arttırılmaya çalışılmıştır. Çalışmanın sonunda MATLAB programlama dilinde üretilen sıradan sözde rastsal sayılar ile yapay sinir ağı ile güçlendirilmiş sözde rastsal sayılar, rastsallık testlerine tabii tutulmuştur. Sonuç olarak yapay sinir ağlarının rastsal sayı üretiminde etkili bir yöntem olduğu tespit edilmiştir.**

Anahtar Kelimeler — Çok Katmanlı Yapay Sinir Ağı; Sözde Rastsal Sayı Üreteçleri.

Abstract*— Pseudo-random number generators generate sequent of digits that cannot be expected before. Random number generators are used in lots of studies especially physical and statical implementations. In this paper; by using Multi-Layer Perceptron Neural Network, a traditional random number generator is strengthened. In the end of the study; both of random number generators are tested by some randomness tests of National Institute of Standard Technology test suite. As a result, it is learned that Neural Networks can generate good random numbers.

Keywords — Multi-Layer Perceptron; Neural Networks; Pseudo Random Number Generators.

I. GİRİŞ

Rastsal sayı üreteçleri özellikle kriptolojide anahtar üretiminin güvenirliliğinin sağlanması maksadıyla hayati önem taşımaktadır. Bir kripto-sisteminde üretilen anahtarların tahmin edilemez olması güvenirlilik açısından gerekmektedir. Yani üretilen anahtar dizinde kripto analist tarafından ele geçirilen bir anahtar kullanılarak, geçmişte üretilen anahtar ile gelecekte üretilecek olan anahtarın tahmin edilemez olması gerekmektedir. Kripto-sisteminde; üretilen anahtarlar arasında hiçbir ilgileşim olmaması sistemi kullanan kişi ve kurumları birçok bilgisayar korsanından, siber teröristlerden, yazılım hırsızlarından ve sosyal medya casuslarından koruyacaktır.

Sözde rastsal sayı üretecin (Pseudo-random number generators**,** PRNG) geliştirilmesinin uzun tarihsel süreci vardır. 1971 yılında, Vernam rastsal olarak sıralanan sayı dizisi ile tek zamanlı şifrelemeyi bulmuştur [1]. PRNG kullanılarak tasarlanan kripto sistemlerinin güvenlilik ölçüsü, PRNG' nın gerçek rastsal sıralı sayı dizisinden ayırt edilemeyeceği varsayımına dayanmaktadır. PRNG kripto uygulamalarının güvenilirliğinde hayati önem taşımaktadır.

Bir sayı dizisi eğer rastsallık testlerini başarı ile geçiyorsa, sayı dizisinde bir sonraki rakamın ne olacağını hesaplamanın imkânsız olduğu değerlendirilmektedir. Üretilen sayıları bu şekilde olan üreteç, Sözde rastsal sayı (Pseudo-random number, PRN) olma şartını sağlıyor demektir ve kripto sisteminde kullanılması doğru bir karardır.

Bugüne kadar haberleşmede kullanmak maksadıyla güçlü kripto sistemi geliştirmek için birçok çalışma yapılmıştır. Yakın geçmişe dikkatle bakıldığında yapay sinir ağları ile şifreleme teknikleri sıklıkla kullanılmakta olduğunu görmekteyiz. Yapay sinir ağlarının kriptolojide kullanma fikri ilk kez Francesco E.Lauria tarafından 1990 yılında ortaya atılmıştır [2]. Tanrıverdi H. tarafından 1993 yılında yapay sinir ağlarının ağırlıkları kriptolojide anahtar olarak kullanılmıştır [3]. 1994 yılında nöral kriptoloji uygulamaları D.Pointcheval tarafından yapılmıştır [4]. Yapay sinir ağlarının kaotik davranmalarına dayanan kripto modeli 1999 yılında D.Guo tarafından geliştirilmiştir [5]. 2003 yılında, D.A. Karras; IDEA ve ANS X.9 gibi 3DES algoritmasına dayanan klasik kripto sistemlerini Sözde rastsal sayı üreteçleri tabanlı yapay sinir ağları ile güçlendirmiştir [6]. 2005 yılında, T.Godhavari senkronize olan iki yapay sinir ağının ağırlıklarını DES algoritmasında gizli anahtar olarak kullanmıştır [7]. 2006 yılında, Andreas TUTTON ağaç paritesi yapılı iki yapay sinir ağının herbian öğrenme kuramı ile ortak çıkış değerinde senkronize olmasını sağlayarak, ağırlıkları ortak gizli anahtar üretmeyi başarmıştır [8]. M.Arvandi

tarafından yapay sinir ağı tabanlı simetrik şifreleme sistemi dizayn edilmiştir [9]. 2007 yılında, Ş.Sağıroğlu DELPHİ ile geliştirdiği yapay sinir ağının bazı verilerini gizli anahtar olarak kullanan algoritma ile elektronik haberleşmede yapay sinir ağı güvenliğini tanıtmıştır [10]. Ayrıca, şifrelemenin herhangi bir kurala dayanmadan yapıldığında, yapay sinir ağlarının öğrenme özelliği ile deşifre edilebileceğinin mümkün olduğu iddia etmiştir [11]. 2010 yılında, D.İlker kaotik kriptolojiyi güçlendirmek için MATLAB da yapay sinir ağı tabanlı kaotik sayı üreteci tasarlamıştır. 2011 yılında, Karam M.Z.Othman MATLAB ile yapay sinir ağı kullanarak Sözde rastsal sayı üreteci yazılımı ve FPGA kullanarak gerekli donanımı geliştirmiştir [12].

Bu çalışmada Çok Katmanlı yapay sinir ağları kullanılarak Mevcut rastsal sayı üreteçleri ile üretilen sayıların rastsallığı arttırılmaya çalışılmıştır.

Çalışmanın 2'inci bölümünde yapay sinir ağları, 3'üncü bölümde sözde rastsal sayı üreteçleri ve yapay sinir ağı tabanlı rastsal sayı üreteçleri ve 4'üncü bölümünde rastsallık testleri anlatılmıştır. 5'inci bölümde ise sıradan rastsal sayılara ve yapay sinir ağı tabanlı rastsal sayılara uygulanan rastsallık testlerinin sonuçları yorumlanmıştır.

II. YAPAY SINIR AĞLARI

İnsan vücudu, sinir sistemi sayesinde yaşadığı olaylardan meydana gelen her türlü fiziksel, biyolojik ve kimyasal değişim karşısında, değişimlere alışabilmek maksadıyla kendisini yenilemekte ve çeşitli reaksiyonlar üretmektedir. Bütün sistemleri uyumlu çalışan bu sistem birçok araştırmacıya çalışmalarında esin kaynağı olmuştur. Bugün dahi insan beyninin yetenekleri, kapasitesi ve sınırları hala tam anlamıyla çözülememiştir.

Yapay sinir ağları yapay nöronların ağırlıklandırılmış grafiğidir. Yapay sinir ağlarının avantajlarından bazıları; bilinen durumlardaki sonuçları kullanarak bilinmeyen durumlar hakkında karar verilebilmesi, işletiminde hızlı tepki verilebilmesi ve güvenilirlik ile verimlilik derecesinin yüksek olmasıdır.

Çok katmanlı Perceptron (Multi Layer Perceptron, MLP) ağları ileri beslemeli bir ağ modelidir. Çok sayıda öğrenme algoritması kullanılarak eğitilebilen bu ağ yapısında; giriş, çıkış ve ara katlarda bulunan nöron sayısı problemin karmaşıklığı ile ilgili olup bu sayı tecrübeye dayalı olarak belirlenir [13].

A. Yapay Sinir Ağının Tasarlanması

Dört katmanlı olarak belirlenen yapay sinir ağının giriş katmanında 1 nöron diğer katmanlarında ise 25'er nöron bulunmaktadır. Yapay sinir ağının giriş verisi olarak Modified Subtract with Borrow üreteci ile üretilen sayılar kullanılmaktadır. Katmanların transfer fonksiyonları ise sırasıyla; tansig, tansig, hardlim, satlins transfer fonksiyonlarıdır. Yapay sinir ağı ile eğitim yapmadan başlangıç ağırlık verileri kullanılarak çıkış verileri elde edilmiştir.

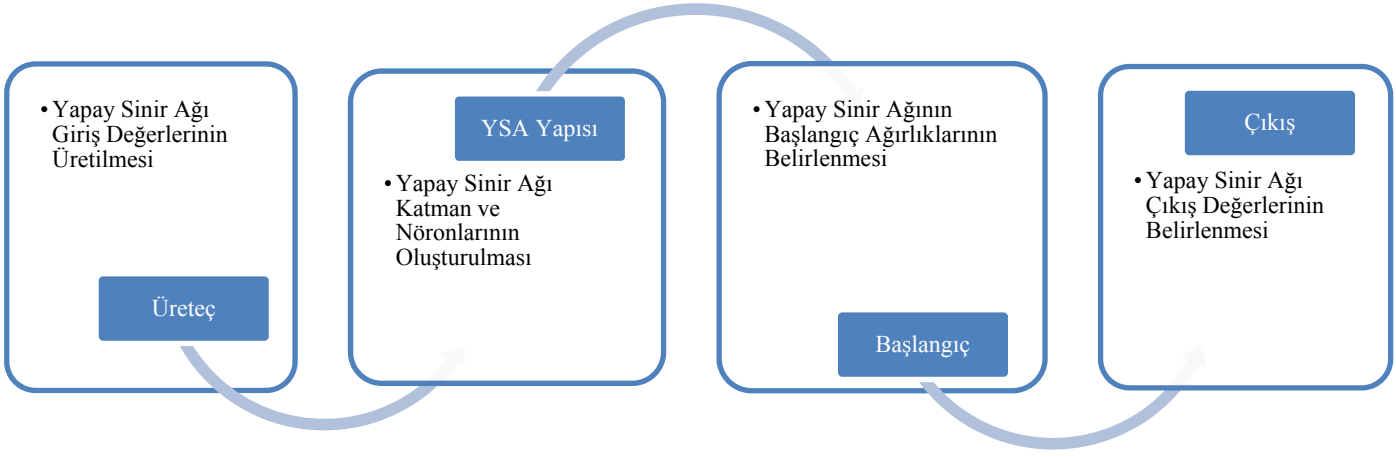
III. SÖZDE RASTSAL SAYILAR

Bir sayı dizisi eğer rastsallık testlerini başarı ile geçiyorsa, sayı dizisinde bir sonraki rakamın ne olacağını hesaplamanın imkânsız olduğu değerlendirilmektedir. Üretilen sayıları bu şekilde olan üreteç, Sözde rastsal sayı (Pseudo-Random Number, PRN) olma şartını sağlıyor demektir ve kripto sisteminde kullanılması doğru bir karardır.

Çalışmada Matlab paket programı kullanılmıştır. MATLAB paket programda beş farklı PRN üreten algoritma vardır [14]. Bunlardan Modified subtract with borrow algoritması kullanılarak PRN üretilmiştir. Bu algoritma, Fibonacci rastsal sayı üretecine benzer ve 2^{1376} bitlik uzun periyoda sahiptir [20]. Rastsal başlangıç ağırlıkları ile işlem yapan yapay sinir ağlarında Modified subtract with borrow üreteci ile üretilen sayılar giriş değerleri olarak kullanılırsa, çıkış değerlerinin rastsallık ölçüsü sıradan rastsal dizilere göre çok daha güçlü olacağı düşünülmüştür.

A. Yapay Sinir Ağı Tabanlı Rastsal Sayılar

Yapay sinir ağlarının ile üretilen başlangıç ağırlıklarına dayalı veriler kullanılarak rastsal üretilen rastsal sayılara yapay sinir ağı tabanlı rastsal sayılar denilmektedir. Bu sayıların üretilmesi blok şeması Şekil 1' de gösterilmiştir.



Şekil 1. Yapay Sinir Ağı Tabanlı Rastsal Sayı Üretimi

978-1-4673-5563-6/13/$31.00 ©2013 IEEE

IV. RASTSALLIK TESTLERİ

Rastsallık Testleri

Kriptolojide kullanılan rastsal sayı üreteçlerinin güçlü olması şifrelemenin güvenilirliği açısından son derece önemli bir hususdur. Bu sebeple, rastgeleliği ölçen ve değerlendiren istatistik testler kriptolojiye önemli hizmet etmektedir. Birkaç paket test yazılımları mevcuttur.

A. •Frekans Testi

Testin faaliyet merkezi, parçalanmamış sıra (Kriptolojide devamlı olarak kullanılan sembollerin (harfler, rakamlar v.s.) sıralanmış terkibidir [18]. Bu testin amacı, bir sırada bulunan sıfır ve birlerin miktarının tamamen rastgele bir sıra için beklenen ile yaklaşık olarak aynı olup olmadığının belirlenmesidir.

B. • Runs Testi

Bu testin amacı; farklı uzunluklardaki 0 ve 1'lerin tekrarının rastgele bir dizi için beklendiği gibi olup olmadığının belirlenmesidir. Özellikle, bu test 0 ve 1'ler arasındaki değişimin çok hızlı veya çok yavaş olup olmadığını belirler [18].

C. • Rank Testi

Rank Testi: Testin faaliyet merkezi, parçalanmamış sıranın alt matrislerinin sıralı ranklarıdır. Bu testin amacı, orjinal sıranın alt sıralarının sabit uzunlukları arasındaki lineer bağımlılığını kontrol etmektir. Test içerisinde sıra M x M-bitlik matrisler halinde parçalanır ve oluşturulan her bir matrisin rankı hesaplanır. Sıradan oluşturulan matrislerin ranklarının frekansları hesaplanır, beklenen frekansla kıyaslanır ve ciddi bir sapma olup olmadığı kontrol edilir.

D. • Bloktaki En Uzun Birler Testi

Testin faaliyet merkezi, M-bit bloklarda birlerin en uzun tekrar sayısıdır. M-bitlik bloklarda bulunan en uzun birler grubu üzerinde odaklaşır. Bu testin amacı, test edilen sıradaki birlerin en uzun tekrar sayısı ile rastgele bir sıradaki birlerin beklenen en uzun tekrar sayısının uyumlu olup olmadığını belirlemektir.

E. • Kümülatif Toplamlar Testi

Bu testin amacı; dizinin değişik parçalarının kümülatif toplamın beklenen değerlere göre ne kadar farklılık gösterdiğinin belirlenmesidir. Kümülatif toplamlar da rastsal bir ilişki içerisinde olabilirler. Bu test sonucunda dizinin rastsal kabul edilebilmesi için kümülatif toplamının 0 (sıfır) ' a yakın olması gerekmektedir.

F. • Ayrık Fourier Dönüşüm Testi

Bu testin faaliyet merkezi sıranın Ayrık Fourier Dönüşümündeki tepe noktalarıdır. Bu testin amacı rastgelelik varsayımından bir sapma gösteren, test edilen sıradaki periyodik özellikleri (yani, birbirine yakın olan tekrarlı kalıpları)tespit etmektir. Bu amaç, %95 barajını önemli ölçüde %5 den farklı olarak aşan tepelerin sayısını tespit etmek içindir.

G. • Blok Frekans Testi

Blok Frekans Testi: Testin faaliyet merkezi, M-bit blokları içindeki birlerin oranıdır. Verilen bir sırada bulunan 0 ve 1'lerin oranını M bitlik bloklar içinde kontrol eder. Her bir bloktaki 1'lerin beklenen oranı M/2'dir. Bu testin amacı, bir M-bit bloktaki birlerin frekansının bir rastgelelik varsayımı altında beklenen gibi yaklaşık olarak M/2 olup olmadığının belirlenmesidir. Blok uzunluğu M=1 olarak alındığında blok frekans testi, frekans testine dönüşür.

V. RASTSALLIK TESTLERI SONUÇLARI

NIST [19] istatistiksel test yazılımlarından biridir. Bu test paketleri Frekans testi, Runs test, örüntü testi gibi ortak testleri içerirler. Bu çalışmada Frekans Testi, Runs Testi, Rank Testi, Bloktaki En Uzun Birler Testi, Kümülatif Toplamlar Testi, Ayrık Fourier Dönüşüm Testi ve Blok Frekans Testi yapılarak test sonuçları Tablo 1 ve Tablo 2' de sunulmuştur. Modified subtract with borrow üreteci ile üretilen sayılar için elde edilen test sonuçları Tablo 1 ve Yapay Sinir ağı tabanlı üretilen sayılar için elde edilen test sonuçları ise Tablo 2 verilmektedir.

İstatistiksel çıkarım yapmak için istatistiksel hipotez testleri kullanılır. Bu testlerde bir hipotez (yokluk hipotezi, H0) öne sürülür, bu hipotezin tersi de alternatif hipotez, Ha olarak kabul edilir. İstatistiksel test sonucunda varılabilecek iki farklı temel karar vardır: - H0' ı reddet. - H0' ı reddetme. Birinci karar, H0 aleyhine güçlü bir kanıt elde edildiğinde verilir. Bu güçlü kanıt bulunamadığında ise ikinci karar verilir.

Bütün istatistiksel testlerde kaçınılmaz hata yapma payı vardır. Test sonucunda iki farklı hata, birinci tip (alfa) ve ikinci tip (beta) yapılabilir. Birinci tip hata hipotezimiz doğruyken, kararımız H0'ı reddetmek olarak gerçekleşir. İkinci tip hata ise hipotezimiz yanlışken, kararımız H0'ı reddetme olduğunda gerçekleşir. Hipotez testinde birinci tip hata yapma olasılığını sınırlamak gerekir. Test sonucunda birinci tip hata yapma olasılığımız, testimizin anlam seviyesini verir. Bu değer genellikle 0.01- 0.05 olarak seçilir. İstatistiksel bir testin gücü, ikinci tip hatayı yapmama olasılığına eşittir. Testin gücü daha çok örneklem ile artırılabilir.

İstatistiksel bir test yapılacağında ilk olarak, H0 ve Ha belirlenir. Daha sonar testin anlam seviyesine karar verilir. Kitleden alınan rastgele örneklemden test istatistiğinin ve teste ilişkin ret bölgesinin olasılığı olan p-değeri elde edilir. P değeri, birinci tip hata yapma olasılığını kontrol etmek yerine, H0'ın doğru olduğu varsayımı altında test istatistiğinin değeri veya daha uç bir değer olması olasılığına karşılık gelir. Bu tanıma uygun olarak hesaplanan olasılık p-değerini verir. Eğer bu değer seçilen anlamlılık değerinden küçükse H0 hipotezi reddedilir.

Eğer p-değeri<0.01 olarak hesaplandıysa, karar, sıranın rastgele olmadığı şeklindedir. Aksi takdirde, karar sıranın rastgele olduğu şeklindedir [18]

Tablo 1.Yapay Sinir Ağı Tabanlı Rastsal Sayıların Test Sonuçları.

	p Değeri	SONUÇ
Frekans Testi	0.14986	Başarılı
Blok Frekans Testi	0.911733	Başarılı
Runs Testi	0.85160	Başarılı
Bloktaki En Uzun Birler Testi	0.093350	Başarılı
Kümülatif Toplamlar Testi	0.911733	Başarılı
Ayrık Fourier Dönüşüm Testi	0.646355	Başarılı
Rank Testi	0.741908	Başarılı

Tablo 2. Modified Subtract with Borrow ile Üretilen Sözde Rastsal Sayıların Test Sonuçları.

	p Değeri	SONUÇ
Frekans Testi	0.000233	**Başarısız**
Blok Frekans Testi	0.234600	Başarılı
Runs Testi	0.000212	**Başarısız**
Bloktaki En Uzun Birler Testi	0.000001	**Başarısız**
Kümülatif Toplamlar Testi	0.000368	**Başarısız**
Ayrık Fourier Dönüşüm Testi	0.408863	Başarılı
Rank Testi	0.741908	Başarılı

VI. SONUÇ

Günümüzde kripto sistemlerinin güvenirliğinin ileriye taşınması için mutlaka bilimin gelişen dallarından destek alınmalıdır. Kuantum mekaniği, yapay sinir ağları, kaotik sistemler bunlarda birkaçıdır. Yapay sinir ağları kaotik başlatıcı, sözde rastsal sayı üreteci, S-kutusu gibi kriptolojinin pek çok alanında kullanılan bir araçtır. Bu çalışmada; yapay sinir ağları ile sözde rastsal sayı üreteçlerinin rastsallıklarını güçlendirmek için yeni bir yol çizilmeye çalışılmıştır. Çalışmada sıradan bir rastsal sayı üretiminden sonra dört katmanlı yapay sinir ağı oluşturularak elde edilen rastsal sayılar ağın parametreleri olarak kullanılmakta ve ağın sonuçlar yeni rastsal sayıları oluşturmaktadır. Böylece sıradan rastsal sayı üreteçlerini yapay sinir ağı ile güçlendirilerek daha güçlü sözde rastsal sayı üreteci elde edilmiş olmaktadır. Bu durum testlerden de anlaşılmaktadır. Sıradan sözde rastsal sayı üreteci ile 7 adet testin yalnızca 3 adedinde başarılı sonuçlar alınırken; yapay sinir ağı ile güçlendirilmiş rastsal sayı üreteci ile tamamında başarılı sonuçlar alındığı görülmüştür.

BİLGİLENDİRME

Bu araştırma Mustafa Kemal Üniversitesi 8702 nolu Bilimsel Araştırma Projesi ile desteklenmektedir.

KAYNAKÇA

[1] Zeng, K., Yang, C. and Wei, D. Rao University of Southwestern Louisiana "Pseudo-Random Bit Generators in Stream-Cipher Cryptography", 1991

[2] E.Lauria, F., "On Neural cryptology" Parallel Architectures and Neural Networks. Third Italian workshop [A]. World Scientic [C]. Singapore, 1990, 337- 343

[3] Tanrıverdi H., "Yapay Sinir Ağlarının Kriptolojide Uygulanması", Msc Thesis, Middle East Technical University, Turkey, 1993

[4] Pointcheval, D. , "Neural Networks and Their Cryptographic Applications," in Proc. of Euro code, pp. 183–193, 1994.

[5] Guo, D., Cheng, L.M. and Cheng, L.L. "A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks," Applied Intelligence, vol. 10, no. 1,pp. 71–84, 1999.

[6] Karras, D.A. and Zorkadis, V., "On Neural Network techniques in Secure Management of Communication Systems Through improving and Quality Assessing Sözde rastsal Stream Generators", Journal of Pergamum, 2003.

[7] Godhavari, T.N., Alamelu, R. and Soundararjan, R., "Cryptography Using Neural Network" in IEEE Indicon 2005 Conference, Chennai, India 11-13 December 2005

[8] TUTTON, A. "Neural Synchronization and Cryptography", PhD Thesis, Bayerischen Julius-Maximilians Universty, Germany, 2006

[9] Arvandi, M., Wu, S., Sadeghian, A., Melek, W. and Woungang, I.," Symmetric Chipper Design Using Recurrent Neural Networks", International Joint Conference on Neural Networks, Sheraton Vancouer Wall Hotel, Vancouer, BC, Canada, July 2006

[10] Sağıroğlu, Ş., Özkaya, N.," Neural Solutions For Information Security", Journal of Polytechnic Vol: 10 No: 1 pp.21-25 Gazi University, Turkey 2007.

[11] Muukur, R. and Gnanam, V.," Neural Network Based Decryption for Random Encryption Algorithms", Department of Electronics and Communication Engineering PSG College of Technology, India 2007.

[12] Othman, K.M.Z. and Jammas, M.H.Al., "Implementation of Neural –Cryptographic System Using FPGA", Journal of Engineering Science and Technology Vol: 6 No: 4 pp: 411-428, 2011

[13] Dalkıran, İ., Yapay Zeka Tekniği Kullanan Bilgisayar Tabanlı Yüksek Hassasiyetli Sıcaklık Ölçme Birimi Tasarımı, Yüksek Lisans Tezi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, Kayseri, 2003.

[14] www.mathworks.com

[15] Hughes, J.M., "Pseudo-random Number Generation Using Binary Recurrent Neural Networks", A Technical Report submitted to Kalamazoo College 2007.

[16] Abdi, H., "A neural network primer", Journal of Biological Systems, 1994.

[17] Walker, J., ENT Test suite. www.fourmilab.ch/random/, Oct., 1998.

[18] YILMAZ, R., "Kriptolojik Uygulamalarda Bazı İstatistik Testler" Yüksek Lisans Tezi, 2007

[19] Andrew, R., Soto, J., Nechvata, J., Barker, M.S.E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., "Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", Special Publication 800-22 National Institute Standart Technology April2010

[20] Marsagilla G. and Zaman A. "The New Class Random Number Generators" Annals of Applied Probablity 1991,Vol.1 Number 3 462-480