T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TAMSAYILI VE KESİRLİ DERECEDEN FARKLI KAOTİK SİSTEMLER İLE RASGELE SAYI ÜRETEÇLERİ VE ARAYÜZ TASARIMI

YÜKSEK LİSANS TEZİ

Coşkun ARSLAN

Enstitü Anabilim Dalı	**:**	**ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Doç. Dr. Akif AKGÜL**

Şubat 2019

T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

TAMSAYILI VE KESİRLİ DERECEDEN FARKLI KAOTİK SİSTEMLER İLE RASGELE SAYI ÜRETEÇLERİ VE ARAYÜZ TASARIMI

YÜKSEK LİSANS TEZİ

Coşkun ARSLAN

Enstitü Anabilim Dalı : ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ

Bu tez 14/02/2019 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Prof. Dr. İhsan PEHLİVAN Jüri Başkanı	Doç. Dr. Akif AKGÜL Üye	Dr. Öğr. Üyesi Abdullah SEVİN Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Coşkun ARSLAN

14.02.2019

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Doç. Dr. Akif AKGÜL'e teşekkürlerimi sunarım.

Ayrıca lisans ve yüksek lisans eğitimim boyunca bilgi ve birikimini benimle paylaşan Elektrik Elektronik Mühendisi Emre Güleryüz'e ve Malzeme Bilimleri Mühendisi Olgun Madak'a teşekkürü bir borç bilirim.

İÇİNDEKİLER

TEŞEKKÜR i
İÇİNDEKİLER ii
SİMGELER VE KISALTMALAR LİSTESİ vi
ŞEKİLLER LİSTESİ ix
TABLOLAR LİSTESİ xiii
ÖZET xiv
SUMMARY xv

BÖLÜM 1.
GİRİŞ 1

BÖLÜM 2.
KAOS VE KAOTİK SİSTEMLER 5
2.1. Kaos ve Temel Kavramlar 8
2.1.1. Kaotik sistemler 9
2.1.1.1. Ayrık zamanlı kaotik sistemler 9
2.1.1.2. Sürekli zamanlı kaotik sistemler 12
2.1.2. Kaotik sistemlerin analiz yöntemleri 13
2.1.2.1. Denge noktaları ve kararlılık analizi 13
2.1.2.2. Faz portreleri (Faz uzayı) 14
2.1.2.3. Zaman serisinde başlangıç değerlerine olan hassas bağımlılık analizi 16
2.1.2.4. Lyapunov üstelleri 17
2.1.2.5. Çatallanma diyagramı 19
2.2. Referans Kaotik Sistemler 21
2.2.1. Chua kaotik sistemi 21
2.2.2. Lorenz kaotik sistemi 23
2.2.3. Rossler kaotik sistemi 25

2.2.4. Van Der Pol kaotik sistemi 26
2.2.5. Aizawa kaotik sistemi 27
2.2.6. Pehlivan kaotik sistemi 29
2.2.7. Chen kaotik sistemi 30
2.2.8. Labyrinth kaotik sistemi 32
2.2.9. Rucklidge kaotik sistemi 33
2.2.10. Rikitake kaotik sistemi 34
2.2.11. Altın oran dengeli kaotik sistem 36

BÖLÜM 3.
RASGELE SAYI ÜRETEÇLERİ (RSÜ) VE TEMEL KAVRAMLAR 38
3.1. İstatistiksel Rasgelelik Testleri 41
3.1.1. FIPS-140-1 testi 42
3.1.1.1. Monobit testi 42
3.1.1.2. Poker testi 42
3.1.1.3. Runs testi 43
3.1.1.4. Long Runs testi 43
3.1.2. NIST-800-22 testi 43
3.1.2.1. Frekans testi (Frequency monobit test) 44
3.1.2.2. Blok frekans testi (Frequency test within a block) 44
3.1.2.3. Yinelemeler (akış) testi (Runs test) 45
3.1.2.4. Blok içinde en uzun bir yinelemesi testi (Tests for the longest-run-ofones in a block test) 45
3.1.2.5. İkili matris rankı testi (Binary matrix rank test) 45
3.1.2.6. Ayrık Fourier dönüşümü testi (Discrete Fourier transform test) 45
3.1.2.7. Örtüşmeyen şablon eşleştirme testi (Non-overlapping template matching test) 46
3.1.2.8. Örtüşen şablon eşleştirme testi (Overlapping template matching test) 46
3.1.2.9. Maurer'in "evrensel istatistik" testi (Maurer's "universal statistical" test) 46
3.1.2.10. Doğrusal karmaşıklık testi (Linear complexity test) 46

3.1.2.11. Seri testi (Serial test) 47
3.1.2.12. Yaklaşık entropi testi (Approximate entropy test) 47
3.1.2.13. Kümülatif (birikimli) toplamlar testi (Cumulative sums test) 47
3.1.2.14. Rasgele gezinimler testi (Random excursions test) 47
3.1.2.15. Rasgele gezinimler değişken testi (Random excursions variant test) 48
3.1.3. ENT testi 48
3.1.3.1. Ki-kare testi 48
3.1.3.2. Aritmetik ortalama 49
3.1.3.3. Pi için monte carlo değeri 49
3.1.3.4. Seri korelasyon katsayısı 50
3.1.4. Diehard testleri 51
3.1.5. PractRand 51

BÖLÜM 4.
TASARLANAN KRSÜ'DE KULLANILAN AYRIK ÇÖZÜM METOTLARI VE SON İŞLEM YÖNTEMLERİ 53
4.1. Sayısal Çözüm Algoritmaları 53
4.2. Kesir Dereceli Türevler (Fractional-Order Systems) 57
4.2.1. L. Euler (1730) tanımı: 61
4.2.2. Riemann-Liouville tanımı: 61
4.2.3. Caputo (1967) tanımı: 61
4.2.4. Grünwald - Letnikov tanımı: 61
4.2.5. Kesir dereceli türevlerin numerik olarak çözülmesi 63
4.3. Kaotik Sistemlerin Kesir Dereceli Türev Modeli ve Analizi 64
4.3.1. Kesir dereceli Lorenz sistemi 64
4.3.2. Kesir dereceli Chen sistemi 66
4.3.3. Kesir dereceli Rössler sistemi 67
4.4. Tez Çalışmasında Kullanılan Yöntemler 69
4.4.1. Yöntem 1 (Kayan noktalı sayı) 70
4.4.2. Yöntem 2 (dec2bin) 71
4.4.3. Yöntem 3 (mod2) 71

BÖLÜM 5.
KESİRLİ TÜREVLİ VE ÇOK FONKSİYONLU KAOTİK RASGELE SAYI ÜRETECİ ARAYÜZ TASARIMI 73
5.1. Matlab GUI ve Arayüz Tasarımı 73
5.2. Kesirli Türev ve Çok Fonksiyonlu Kaotik Rasgele Sayı Üreteci Özellikleri ve Kullanımı 76

BÖLÜM 6.
İSTATİSTİKSEL RASGELELİK TEST SONUÇLARI 89

BÖLÜM 7.
SONUÇ VE ÖNERİLER 97

KAYNAKLAR 99
ÖZGEÇMİŞ 108

SİMGELER VE KISALTMALAR LİSTESİ

a	: Sistem parametresi
b	: Sistem parametresi
C	: Kondansatör
c	: Sistem parametresi
d	: Sistem parametresi
det	: Determinant
E	: Denge Noktası
e	: Sistem parametresi
ENT	: Pseudorandom Number Sequence Test Program
exe	: Windows uygulama dosyası
F	: Frekans
f	: Sistem parametresi
FIPS	: Federal Information Processing Standard
g	: Sistem parametresi
GND	: Ground (Toprak)
GPIO	: General-purpose input/output
GPL	: Copyleft lisansları, GNU Genel Kamu Lisansı
GRSÜ	: Gerçek rasgele sayı üreteci
GUI	: Grafiksel kullanıcı arayüzü
Hz	: Hertz
I	: Akım
IEEE	: Institute of Electrical and Electronics Engineers
IEEE-754	: IEEE Kayan noktalı sayı formatı
i	: İndis
J	: Jakobian matrisi
KCL	: Kirchhoff'un Akım Kanunu

KGRSU : Kaotik gerçek rasgele sayı üreteci

KVL : Kirchhoff'un Gerilim Kanunu

L : Endüktans

LSB : Least significant bit (En düşük anlamlı bit)

M : Bit dizisinde belirli sayıdaki bitlerinden oluşan blok

Matlab : Matrix laboratory

Mbit : Megabit

ms : Milisaniye

n : Bit dizisi uzunluğu

nF : Nanofarad

NIST : National Institute of Standards and Technology

ODE : Ordinary Differential Equation

PHP : İnternet için üretilmiş programlama dili (Personal Home Page)

PRNG : Pseudo random number generator

R : Direnç

r : Yarıçap veya sistem parametresi

rand : Random

RK4 : 4. dereceden Runge-Kutta yöntemi

RK5 : 5. dereceden Runge-Kutta yöntemi

RNG : Random number generator

RSÜ : Rasgele sayı üreteci

SRSÜ : Sözde rasgele sayı üreteci

t : Zaman

TRNG : True Random Number Generator

V : Gerilim

XOR : Exclusive Or (Özel Veya)

Z : Empedans

γ : Sistem parametresi

Δh : Algoritma adım aralığı

λ : Özdeğerler veya Layapunov üsteli

$\chi 2$: Ki-kare dağılımı

Γ : Gama fonksiyonu

L : Laplace

dx : Türev operatörü

p : Probability

q : Türev değr emirleri (kesir derecesi)

x : Durum değişkeni

y : Durum değişkeni

z : Durum değişkeni

β : Sistem parametresi

δ : Sistem parametresi

ζ : Sistem parametresi

$\vec{x}$: Durum vektörü

${}_aD_x^\alpha$: İntegrodiferansiyel operatörü

E_0 : Güç kaynağı gerilim değeri

L_m : Hafıza uzunluğu

N_R : Chua diyotu

R^m : Reel sayılar küme

R_s : Direnç

T_{sim} : Simülasyon zamanı

$V_Ç$: Çıkış gerilimi

V_G : Giriş gerilimi

t_0 : İlk an

x_0 : Durum değişkeninin başlangıç değeri

y_0 : Durum değişkeninin başlangıç değeri

z_0 : Durum değişkeninin başlangıç değeri

μ : Sistem parametresi

ŞEKİLLER LİSTESİ

Şekil 2.1. Kaos durumları ve çeşitleri 6
Şekil 2.2. Van der Pol'un kaos sinyallerini gördüğü neon lamba osilatörü (Chua ve Kennedy, 1986)..... 7
Şekil 2.3. Lojistik haritanın $x0 = 0{,}2$ için, r parametresinin belirli değerlerine göre değişimi: a) r = 2.7, b) r = 3, c) r = 3.5 ve d) r = 4 10
Şekil 2.4. Lojistik harita r=2.5 – 4 arası çatallanma diyagramı 11
Şekil 2.5. Hénon haritanın $x0 = 0,\quad y0 = 0,\quad a = 1{,}4,\quad b = 0{,}3$ için x ve y değişimi 12
Şekil 2.6. Örnek kaotik bir sistemin zamana göre değişimi ve 3 boyutlu faz uzayında yörünge şekli 15
Şekil 2.7. Tigan Sistemi'nin Matlab-Simulink modellemesi, ... 17
Şekil 2.8. Örnek sistemin başlangıç şartlarına olan hassas bağımlılığını gösteren zaman serileri..... 17
Şekil 2.9. Farklı başlangıç şartında iki komşu yörüngenin birbirinden uzaklaşması (Kinsner, 2006) 18
Şekil 2.10. Chua devresi β parametresi değerine göre çatallanma diyagramı 20
Şekil 2.11. Chua Devresi..... 21
Şekil 2.12 Doğrusal olmayan direncin karakteristiği..... 22
Şekil 2.13. Chua x, y, z – zaman grafiği. 22
Şekil 2.14. Chua Sistemi x, y ve z durum değişkenleri faz portreleri..... 23
Şekil 2.15. Chua Sistemi V_1, V_2 ve I_L durum değişkenleri 3 boyut faz portresi..... 23
Şekil 2.16. Lorenz Sistemi x,y,z zaman grafiği..... 24
Şekil 2.17. Lorenz Sistemi 2 boyutlu faz portreleri 24
Şekil 2.18. Lorenz Sistemi 3 Boyutlu faz portresi 25
Şekil 2.19. Rössler Sistemi x,y,z zaman grafiği..... 26
Şekil 2.20. Rössler Sistemi 2 boyutlu faz portreleri..... 26
Şekil 2.21. Rössler Sistemi 3 boyutlu faz portresi 26

Şekil 2.22. Van Der Pol Sistemi x,y zaman grafiği 27
Şekil 2.23. Van Der Pol Sistemi 2 boyutlu faz portreleri 27
Şekil 2.24. Van Der Pol Sistemi x,y,z zaman grafiği 28
Şekil 2.25. Van Der Pol Sistemi 2 boyutlu faz portreleri 28
Şekil 2.26. Van Der Pol Sistemi 3 boyutlu faz portresi 29
Şekil 2.27. Pehlivan G Sistemi x,y,z zaman grafiği 29
Şekil 2.28. Pehlivan G Sistemi 2 boyutlu faz portreleri 30
Şekil 2.29 Pehlivan G Sistemi 3 boyutlu faz portresi 30
Şekil 2.30. Chen Sistemi x,y,z zaman grafiği 31
Şekil 2.31. Chen Sistemi 2 boyutlu faz portreleri 31
Şekil 2.32. Chen Sistemi 3 boyutlu faz portresi 31
Şekil 2.33. Labyrinth Sistemi x,y,z zaman grafiği 32
Şekil 2.34. Labyrinth Sistemi 2 boyutlu faz portreleri 33
Şekil 2.35. Labyrinth Sistemi 3 boyutlu faz portresi 33
Şekil 2.36. Rucklidge Sistemi x,y,z zaman grafiği 34
Şekil 2.37. Rucklidge Sistemi 2 boyutlu faz portreleri 34
Şekil 2.38. Rucklidge Sistemi 3 boyutlu faz portresi 34
Şekil 2.39. Rikitake Sistemi x,y,z zaman grafiği 35
Şekil 2.40. Rikitake Sistemi 2 boyutlu faz portreleri 35
Şekil 2.41. Rikitake Sistemi 3 boyutlu faz portresi 36
Şekil 2.42. Altın oran dengeli sistemin x,y,z zaman grafiği 36
Şekil 2.43. Altın oran dengeli sistemin 2 boyutlu faz portreleri 37
Şekil 2.44. Altın oran dengeli sistemin 3 boyutlu faz portresi 37
Şekil 3.1. Rasgele sayı üreteci genel yapısı 38
Şekil 3.2. RSÜ çeşitleri 39
Şekil 3.3. GRSÜ genel tasarımı 40
Şekil 3.4. Kaotik rasgele sayı üreteci genel tasarımı 41
Şekil 3.5. Bir kare içinde çeyrek daire 49
Şekil 3.6. Rasgele koordinatların dağılımı 50
Şekil 4.1. Reel eksen boyunca gama fonksiyonu 59
Şekil 4.2. f(x) = c fonksiyonun 1 inci ve yarı dereceli türevleri (Korkmaz, 2013) 62
Şekil 4.3. f(x)=x fonksiyonun farklı dereceden türevleri (Korkmaz, 2013) 62

Şekil 4.4. f(x)=x fonksiyonun farklı dereceden integralleri (Korkmaz, 2013) 63
Şekil 4.5. Lorenz kaotik sistemi kesir dereceli faz portreleri: $\sigma = 10,\ \rho = 28,\ \beta = 8/3, q1 = q2 = q3 = 0{,}995$, ve başlangıç şartları $x0, y0, z0 = 0{,}1, 0{,}1, 0{,}1$ 65
Şekil 4.6. Lorenz kaotik sistemi kesir dereceli x-y−z 3 boyut faz portresi: $\sigma = 10,\ \rho = 28,\ \beta = 8/3, q1 = q2 = q3 = 0{,}995$, ve başlangıç şartları $x0, y0, z0 = 0{,}1, 0{,}1, 0{,}1$ 65
Şekil 4.7. Chen kaotik sistemi kesir dereceli faz portreleri: $a = 35,\ b = 3,\ c = 28,\ d = -7$ ve $q1 = q2 = q3 = 0.9$, başlangıç şartları $(x(0), y(0), z(0)) = (-9, -5{,}14)$ 67
Şekil 4.8. Chen kaotik sistemi kesir dereceli x-y-z 3 boyut faz portresi: $a = 35,\ b = 3,\ c = 28,\ d = -7$ ve $q1 = q2 = q3 = 0.9$, başlangıç şartları $(x(0), y(0), z(0)) = (-9, -5{,}14)$ 67
Şekil 4.9. Rössler kaotik sistemi kesir dereceli faz portreleri: $a = 0{,}5,\ b = 0{,}2,\ c = 10,$ ve $q1 = q2 = q3 = 0{,}9$, başlangıç şartları $(x(0), y(0), z(0)) = (0{,}5,\ 1{,}5,\ 0{,}1)$ 69
Şekil 4.10. Rössler kaotik sistemi kesir dereceli x-y-z 3 boyut faz portresi: $a = 0{,}5,\ b = 0{,}2,\ c = 10,$ ve $q1 = q2 = q3 = 0{,}9$, başlangıç şartları $(x(0), y(0), z(0)) = (0{,}5,\ 1{,}5,\ 0{,}1)$ 69
Şekil 4.11. Örnek 0,15625 sayısının IEEE 754 tek duyarlı gösterimi 71
Şekil 5.1 Component Palet a) Nesne İsimleri Var b) Nesne İsimleri Yok 74
Şekil 5.2 GUIDE nesnlerin yerleştirilmesi 75
Şekil 5.3. KGRSU arayüz tasarımı ve nesneleri 78
Şekil 5.4. KGRSU arayüz tasarımı kaotik denklem menüsü 79
Şekil 5.5. “Raspberry” seçeneği seçildikten sonra görünür olan “Çıkış Sinyali” 80
Şekil 5.6. Raspberry Pi donanım için Matlab destek ve kurulum 81
Şekil 5.7. Raspberry Pi donanım için Matlab kurulum ve bağlantı ayarları 82
Şekil 5.8. Raspberry Pi donanım için Matlab kurulum yapılandırma ve test 83
Şekil 5.9. “Onlu” seçeneği seçildikten sonra görünür olan “Onluk için maksimum değer” bölümü 84
Şekil 5.10. Başlat butonu ile çalışan programın akış diyagramı 85
Şekil 5.11. Başlat butonu ile çalışmaya başlayan programda yükleme çubuğu 86

Şekil 5.12. Başlat butonu ile çalışmaya başlayan programda sayı üretildi bildirimi . 86
Şekil 5.13. Kablosuz ağ üzerinden üretilen sayıların Raspberry Pi'ye gönderilmesi 87
Şekil 5.14. Raspberry Pi'den elde edilen sinyalin osilaskop ekranında incelenmesi. 87
Şekil 5.15. Raspberry Pi'den elde edilen sinyalin osilaskop ekran görüntüsü..... 87
Şekil 5.16. Matlab derleyici ile yapılan uygulamanın Windows kurulum dosyası.... 88
Şekil 5.17. Matlab derleyici ile yapılan uygulamanın Windows kurulumu..... 88
Şekil 5.18. Kurulan uygulamanın masaüstü kısayol simgesi..... 88
Şekil 6.1. Binary rasgele sayıların 1000x1000 görselleştirilmesi..... 94
Şekil 6.2. Yakınlaştırılmış görsel..... 94
Şekil 6.3. Üretilen rasgele sayı değerlerinin koordinat olarak işaretlenmesi ve dağılımları..... 95

TABLOLAR LİSTESİ

Tablo 2.2. Lyapunov üstellerinin işaretlerine göre değişimi 19
Tablo 3.1. Runs testi kriterleri 43
Tablo 3.2. Bazı istatistiksel rasgele test programları karşılaştırmaları 52
Tablo 6.1. Lorenz Sistemi NIST800-22 test sonuçları 89
Tablo 6.2. Rössler Sistemi NIST800-22 test sonuçları 90
Tablo 6.3. Chen Sistemi NIST800-22 test sonuçları 90
Tablo 6.4. Kesir dereceli Lorenz Sistemi NIST800-22 test sonuçları 91
Tablo 6.5. Kesir dereceli Rössler Sistemi NIST800-22 test sonuçları 91
Tablo 6.6. Tasarımda bulunan diğer bazı kaotik sistemlerin NIST800-22 test sonuçları (8 Bit LSB) 92
Tablo 6.7. Lorenz'den farklı hassasiyet (LSB) değerlerinde oluşturulan sayıların NIST800-22 test sonuçları 93
Tablo 6.8. Tasarımda bulunan diğer bazı kaotik sistemlerin ENT – Monte Carlo test sonuçları 96

ÖZET

Anahtar kelimeler: Kaos, Kaotik Sistemler, Kesir Dereceden Kaotik Sistemler, Rasgele Sayı Üreteçleri, Arayüz Tasarımı, İstatistiksel Rasgelelik Testleri

Kompleks ve doğrusal olmayan bir davranış olarak nitelendirilerek, "düzensizliğin düzeni" şeklinde tanımlanan kaos ve kaotik sistemler dinamiğine yönelik geçen 15-20 yıllık süreç içerisinde çok büyük bir ilgi olmuştur. Kaos olgusu ve kaotik sistemlerin araştırılmasına dönük ulusal ve uluslararası alanda önemli çalışmalar gerçekleştirilmektedir. Sistem tanıma, optimizasyon algoritmaları, beyin fonksiyonlarını ayırt edebilme, güvenli haberleşme donanımları oluşturma, şifreleme, osilatörler, ikili-kodlu rasgele sayı üreteçleri gibi uygulamalar kaos ve kaotik sinyallerin kullanıldığı bazı uygulama alanlarıdır.

Bu tez çalışmasında kaos tabanlı kesirli ve kesirli dereceden olmayan kaotik sistemler yardımıyla dört farklı yöntem kullanarak kullanıcı dostu bir arayüz ile rasgele sayı üreteç tasarımları yapılarak, mikrobilgisayar tabanlı kullanımı gerçekleştirilmiştir. Rasgele sayıların güvenilirlikleri için uluslararası alanda kabul görmüş NIST-800-22, ENT testleri gibi farklı rasgelelik testleri kullanılarak gerekli test işlemleri yapılmıştır. Gerçekleştirilen çalışma başta kriptoloji olmak üzere, rasgele sayılara ihtiyaç duyulan her alanda kullanılabilecektir.

Tasarlanan arayüz ile, kullanıcılara geniş rasgele sayı üretim seçenekleri sunmak, bunların farklı çıktı yolları ile elde edilmesi ve elde edilen rasgele sayıların mobil olarak kullanımı amaçlanmıştır. Böylece kriptoloji ve güvenli haberleşme sistemleri, istatistiksel örneklemeler, bilgisayar simülasyonları, rasgeleliğe dayalı tasarımlar ve tahmin edilemeyen sonuçlar üreten diğer alanlarda büyük önemi olan rasgele sayı üreteçlerinin farklı yöntemler ile elde edilmesi, kaotik sistemlerin tamsayı (integer) ve kesir dereceli (fractional order) olarak bir arada kullanımı ve bunların uygulanan rasgelelik testlerinde karşılaştırılmaları gerçekleştirilmiştir.

DIFFERENT RANDOM NUMBER GENERATORS AND INTERFACE DESIGN WITH INTEGER AND FRACTIONAL ORDER CHAOTIC SYSTEMS

SUMMARY

Keywords: Chaos, Chaotic Systems, Fractional Order Chaotic Systems, Random Number Generators, Interface Design, Statistical Randomness Tests

There has been a great interest in the chaos and chaotic systems dynamics, which are defined as the order of the disorder, characterized by complex and non-linear behavior. Important studies are carried out in national and international fields for the investigation of chaos and chaotic systems. System recognition, optimization algorithms, distinguishing brain functions, creating secure communication equipment, encryption, oscillators, binary-coded random number generators are some applications where chaos and chaotic signals are used.

In this thesis, by using four different methods with the help of chaos-based fractional and non-fractional chaotic systems, a randomized number generator design was made with a user-friendly interface and microcomputer-based usage was realized. For the reliability of random numbers, necessary tests have been carried out using different randomness tests such as internationally recognized NIST-800-22 and ENT tests. The work performed can be used in all areas where random numbers are needed and especially cryptology.

With the designed interface, it is intended to provide users with large random number production options, their different ways of obtaining and the use of the resulting random numbers as mobile. In this way, it is possible to obtain random number generators with different methods which are of great importance in cryptology and secure communication systems, statistical sampling, computer simulations, randomness-based designs and other fields producing unpredictable results. And they were compared in random tests.

BÖLÜM 1. GİRİŞ

Günümüzde, fiziksel nesnelerin birbirleriyle veya diğer gelişmiş sistemlerle bağlantılı olduğu, ev ve bina otomasyonunda, endüstride, enerji sektöründe, medikal ve sağlık sistemlerinde, ulaşımda, haberleşmede kısaca gündelik hayatın her alanında hayatı kolaylaştıran elektronik sistemlerin ve özellikle de bu sistemlerde iletilen bilginin güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Metin, görüntü, ses gibi birçok bilgiyi içeren dosyalar, dinamik bir şekilde yer kürenin birçok yerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Fakat hayatın külfetli yanlarını kolaylaştıran bu iletişim ağı çok ciddi güvenlik açıklarını da beraberinde getirmiştir. Aralarında haberleşen iki kişi arasındaki iletim bir üçüncül kişi tarafından erişilebilir ve değiştirilebilir hale gelmiştir. Bunu önlemek amacıyla çeşitli koruma aygıtları geliştirilmiş ve yeni teknolojiler ve farklı uygulamaları ortaya çıkmıştır.

Geliştirilen bu teknikler için rasgele sayı üreteçleri önemli bir yer edinmektedir ve önemi de gittikçe artmaktadır. Rasgele sayı üreteçleri şifreleme ve güvenlik uygulamalarının yanında nümerik analiz, oyun teorisi, istatistik, benzetim, eğlence gibi birçok uygulama alanında ihtiyaç duyulan temel bir araçtır.

Kriptoloji ve güvenli haberleşme sistemleri, şans oyunları, istatistiksel örneklemeler, bilgisayar simülasyonları, rasgeleliğe dayalı tasarımlar ve tahmin edilemeyen sonuçlar üreten diğer alanlarda da büyük öneme sahip olan rasgele sayı üreteçlerinin ülkenin gelişen teknoloji ihtiyaçlarına uygun olarak süratli, üretici programın bilgisayar belleğinde az yer kaplaması ve kabul görmüş ileri seviye rasgelelik testlerinden geçmesi gibi ihtiyaçları nedeniyle önemli bir çalışma alanı olmuştur.

Rasgele sayı üreteçleri (RSÜ) herhangi bir biçimden yoksun sayısal veriler veya semboller dizisi meydana getirmek için tasarlanır ve donanımsal (fiziksel) veya hesaplamaya dayalı olarak oluşturulabilir. Günümüzde herhangi bir fiziki donanıma

ihtiyaç duymadan matematiksel yöntemlere dayalı rasgele sayı üreteçlerinin ortaya çıkması kullanıldığı uygulamalar açısından donanım ihtiyacı barındırmama ve daha hızlı çalışma gibi avantajlar sağladı. Fakat bu hesaplamaya dayalı RSÜ'ler çoğunlukla gerçek rasgelelilik hedefinin gerisindedir.

Bu çalışmada, çeşitli bilim dallarında mevcut olan doğrusal olmayan kaotik sistemler ve bu sitemlerin kesir dereceli analizleri de kullanılarak, güvenli haberleşmede alternatif yeni rasgele sayı üreteci yöntemleri ortaya koymak ve bunların kolay anlaşılır ve sade bir arayüz programı ile kullanılabilmesi amaçlanmıştır. Kaotik osilatörlerin tercih edilme sebeplerinden bir tanesi de sinyallerin genlik değerlerinin yüksek olması ve diğer gürültü kaynaklarına göre çevresel koşullardan daha az etkilenmeleridir (Ergün ve Özog, 2007).

Kaos teorisi veya kaos kuramı ise; genel anlamda bir fizik teorisi ya da matematiksel bir tümevarım değil, fiziksel gerçeklik parçalarının bir bütün olarak eğilimini açıklayan bir yöntemdir. Bu teori, temel olarak matematik biliminin içerisinden doğmuştur. Kaos teorisi, hareket ifade eden sistemlerin (fiziksel, ekonomik, matematiksel, biyolojik, felsefi, vs.) başlangıç koşullarına olan bağlılıklarını, zaman serilerinin tahmin edilemez faz uzaylarını ve periyodik olmayan sistem davranışlarını inceleyen bir teoridir.

Karmaşık ve doğrusal olmayan bir davranış olarak nitelendirilip kısaca "düzensizliğin düzeni" şeklinde tanımlanan kaos olayına ve kaotik sistemler dinamiğine yönelik geçen son çeyrek yüzyıl içerisinde çok büyük bir ilgi olmuştur. Bu konuyla ilgili teorik ve simülasyon bazında yapılan çalışmalar deneysel platforma da taşınmıştır. Kaos olgusu ve kaotik sistemlerin araştırılmasına dönük ulusal ve uluslararası alanda önemli çalışmalar gerçekleştirilmektedir. Sistem tanıma, optimizasyon algoritmaları, beyin fonksiyonlarını ayırt edebilme, güvenli haberleşme düzenekleri oluşturma, şifreleme, gürültü üreteçleri, ikili-kodlu rasgele sayı üreteçleri kaos ve kaotik sinyallerin kullanıldığı bazı uygulama alanlarıdır.

Kaosun bilime getirdiği yeni açılımlar çeşitli amaçlarda kullanılmak üzere kaotik işaretler oluşturan osilatörler gelişmesine ya da var olan osilatör devreler üzerinde araştırmaların yapılmasına neden olmuştur. Öyle ki kaos metotları ile evrenin oluşumundan hücre yapılarının tanımlanmasına; haberleşmeden, hava ve deprem olaylarına kadar birçok alanda yararlanılabilir popüler bir bilim dalı haline gelmiştir. Bu konuda kaos ve kaotik işaretlerin bulgularını kendi alanlarında yeni çözümler arayışında olan çalışmaları şu şekilde sıralayabiliriz: Kaos sinyalleri ile şifreleme, nonlineer sistemlerin modellenmesi, nonlineer filtreleme, dinamik bilgi sıkıştırma ve kodlama, haberleşme, kaotik dinamiklerin elektronik, optik ve optoelektronik gerçekleştirilmesi, kaotik titreşimlerin belirlenmesi ve kontrolü, kaotik salınımların yapay üretimi vb. (Kaçar ve ark., 2015).

Bu çalışmada başlangıç şartlarına hassas bağımlı, tahmin edilemez özelliklere ve gürültü benzeri geniş yayılı spektruma sahip olan kaotik sistemler ve bunların rasgele sayı üretimindeki uygulamalarının ortaya konulması; kaotik rasgele sayı üretiminde kullanılan bazı farklı yöntemlerin açıklanması; bu yöntemlerin ve ayarlarının seçilmesi ve kullanılmasının bir arayüz programı aracılığıyla kolaylaştırılması; kullanıcıya geniş bir rasgele sayı üretim seçenekleri sunması ve bunların farklı çıktı yolları ile elde edilmesi; üretilen rassal değerlerin rasgelelik testleri, analizleri ve bunların gerçekleştirilmesi amaçlanmaktadır. Böylece kriptoloji ve güvenli haberleşme sistemleri, istatistiksel örneklemeler, bilgisayar simülasyonları, rasgeleliğe dayalı tasarımlar ve tahmin edilemeyen sonuçlar üreten diğer alanlarda büyük önemi olan rasgele sayı üreteçlerinin farklı yöntemler ile elde edilmesi, kaotik sistemlerin tamsayı (integer) ve kesir dereceli (fractional order) olarak bir arada kullanımı ve bunların uygulanan rasgelelik testlerinde karşılaştırılmaları yapılmıştır. Burada NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından geliştirilen NIST 800-22 istatistiksel testleri ile ENT ve görsel saldırı testleri incelenmiştir.

Bu amaçlar doğrultusunda tezin İkinci Bölüm'ünde kaos ve kaotik sistemler ile ilgili temel kavramlar ve yapılan tasarımda kullanılan kaotik sistemlerin analizleri, üçüncü Bölüm'de ise rasgele sayı üreteçleri, temel kavramları ve uluslararası kabul görmüş istatistiksel rasgelelik testleri anlatılmıştır. Dördüncü Bölüm'de ise yapılan kaotik rasgele sayı üreteci tasarımında kullanılan yöntemler, sayısal çözüm algoritmaları ve kesir dereceli sistemler (fractional-order systems) anlatılmıştır. Burada kesir dereceli kaotik sistemler hakkında L. Euler (1730) tanımı, Riemann-Liouville tanımı, Caputo (1967) tanımı, Grünwald - Letnikov tanımı açıklanmamış ve Grünwald - Letnikov tanımı üzerinden kesir dereceli kaotik sistemlerin numerik analizleri anlatılmıştır.

Beşinci Bölüm'de kesirli türevli ve çok fonksiyonlu kaotik rasgele sayı üreteci tasarımı, özellikleri ve kullanımı, altıncı Bölüm'de yapılan çalışma ve gerçekleştirilen tasarım sonucunda üretilen rasgele sayı dizilerinin uygulandığı uluslararası kabul görmüş istatistiksel rasgelelik testlerinden adlıkları sonuçlar sunularak son bölümde ise sonuçlar ve öneriler verilmiştir.

BÖLÜM 2. KAOS VE KAOTİK SİSTEMLER

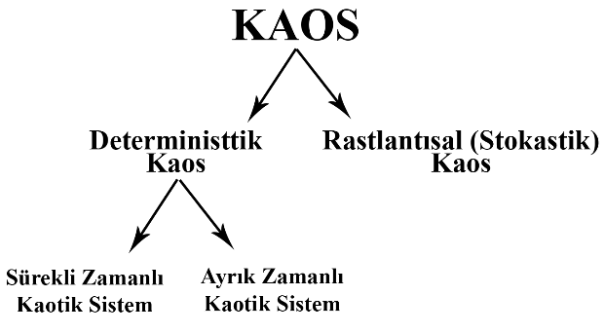
Kelime anlamı olarak kaos: “evrenin düzene girmeden önceki biçimden yoksun, uyumsuz ve karışık durumu” şekliyle tanımlanır. Türk Dil Kurumu Güncel Türkçe Sözlüğü'ndeki bu kelimenin ikinci anlamı “kargaşa” şeklinde verilmiştir. Bilimsel alanda Kaos ise kompleks, doğrusal olmayan ve tahmin edilemeyen olayları inceleyen bir bilim alanı olmuştur.

Kaos, basit bir ifadeyle, düzensiz gibi görünen fakat kendine ait bir düzeni olan ve nonlineer (doğrusal olmayan) olayları açıklamaya yarayan bir bilim alanıdır. Karmaşık, ama kendi iç düzenine ve sınırlarına sahip bir süreçtir. Bir diğer klasik tanım olarak ise dinamik sistemlerde bilinen en karmaşık kararlı hal davranışı “kaos” dur. Kaotik işaretlerin ve kaosun en temel özellikleri; zaman boyutundaki düzensizliği, başlangıç şartlarına olan hassas bağımlılığı, sonsuz denilebilecek sayıda değişik periyodik salınımlar içermesi, gürültü benzeri geniş güç spektrumuna sahip olması, genliğinin ve frekansının tespit edilememesi, ancak sınırlı bir alanda değişken işaretler içermesidir (Pehlivan, 2007).

Doğada meydana gelen olayların çoğu, belirli şartlarda doğrusal davranış gösterirken, bazı şartlarda veya durumlarda doğrusal olmayan (non-lineer) davranış sergilerler. Rüzgârın etkisiyle savrulan yaprak, sigaradan yükselen duman, bir musluktan akan su damlaları, köpüren nehir, kasırgalar vb. bu tür olaylara örnektir (Kurt ve Kasap, 2011; Çiçek, 2016).

Kaos, “deterministtik kaos” ve “rastlantısal (stokastik) kaos” olarak iki durumda incelenebilir. Bilimin daha çok incelediği kısım deterministtik kaos durumudur. Geleneksel çalışmaların ve araştırmaların çoğu elektrik, hareket, yerçekimi veya kimyasal işleyişler gibi tahmin edilebilir olaylarla ilgiliyken, Kaos, türbülans, hava durumu, dilbilim, borsa, zihinsel durumlarımız gibi etkili bir biçimde

öngörülebilirlik dışında bulunan veya kontrol edilemeyen, doğrusal olmayan konuları ele alır.



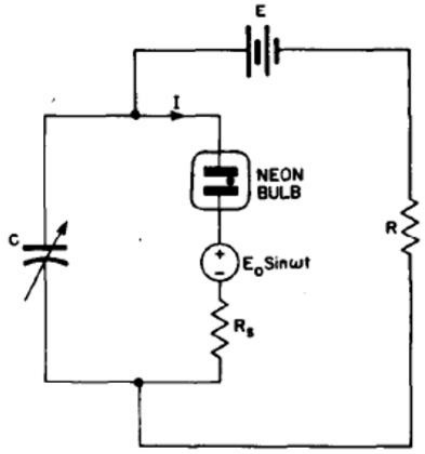
Şekil 2.1. Kaos durumları ve çeşitleri

Bilimsel "kaos" terimi, karmaşık ve rasgele gözüken olayların içinde var olan ve bu olayların nedenini anlamımızı sağlayan bir birbirine bağlılıktan söz eder. Kaos bilimi, karmaşık yapı düzenleri, ince farklar ve tahmin edilemeyenin yeniye nasıl yol açtığına dair bulgular üzerine odaklanır. Kaos, evrende meydana gelen her türlü olay ve yapıların en mikro halinden en makro haline kadar olan hareketleri anlamaya yönelik bir bilim dalıdır.

Kaos bilimi, karmaşıklığın temelinde var olan ve oldukça hassas yapıyı yakalayabilmek için, hem teknoloji kullanımında bazı özel teknikler, hem de bu teknikler ile elde edilen bilgisayar grafikleri ile doğrusal olmayan sistemlerin davranışlarını görselleştirmede çözümler ortaya koymaktadır. Bu yöntemlerle çözümleri ve sistem parametreleri değiştiğinde çözümlerin nasıl değişeceğini de açıklamayı sağlayabilmektedir.

Kaos bilimi bu yönleriyle doğrusal (lineer) olmayan olayları açıklamak için kullanılır. 1892 yılında Fransız matematikçi olan Jules Henri Poincaré, basit dinamik kuralların karmaşık kararlı hal davranışlarına yol açabilir olduğunu keşfetmiştir. Araştırmalarında kaos ihtimalini ortaya koyan ilk bilgindir (Pehlivan, 2007; Holmes, 1990; Gleick, 1997).

Karmaşık ve doğrusal olmayan sistem davranışı bilim tarihi boyunca birçok alanda gözlemlenmiştir. İlk olarak 1920'li yıllarda Hollandalı bir elektrik mühendisi olan Balthazar Van Der Pol, neon lamba osilatörü (Şekil 2.2.) üzerinde yaptığı çalışmalar esnasında o zamanlar bilmese de kaosu gözlemlemiştir. Daha doğrusu dinlemiştir. Van der Pol osilatör frekansının bir frekanstan diğerine atlarken açıklayamadığı düzensiz bir gürültü duymuştur. 1986 yılında M. Peter Kennedy, periyot çoğullama kaosa götürür tanımından faydalanarak Van der Pol'un düzensiz gürültülü olarak tanımlamadığı bu durumun kaos olduğunu göstermiştir (Pol ve Mark, 1927; Chua ve Kennedy, 1986; Gleick, 1997; Wyk ve Steeb, 2013).



Şekil 2.2. Van der Pol'un kaos sinyallerini gördüğü neon lamba osilatörü (Chua ve Kennedy, 1986)

Kaos ve kaotik sistemlere yönelik geçen son yirmi yıl içerisinde çok büyük bir ilgi olmuştur. Elektrik, elektronik, makine, nükleer fizik, katı hal fiziği, lazer optiği, kimya, biyoloji, tıp, ekoloji, astronomi, sosyoloji, ekonomi, uluslararası ilişkiler, tarih, hidrolik, atmosferik, gibi fen ve sosyal bilimlerin çok çeşitli konularında kaos varlığının ortaya konması kaotik sistemlerle ilgili birçok uygulama alanının oluşmasına yol açmıştır. Kaos ve kaotik sistemlerle ilgili oluşan uygulama alanlarına örnek olarak; kaotik paralel dağılımlı işleme, deterministik doğrusal olmayan tahmin, kaotik şifreleme ve steganografi, kimliklendirme ve lineer olmayan sistemlerin modellenmesi, non-lineer filtreleme, biyomedikal ve tıbbi uygulamalar, dinamik bilgi sıkıştırma ve kodlama, rasgele sayı üreteçleri, hassas desen tanıma, kaotik dinamiklerin müzik ve sanat amaçlı kullanımı, kaotik salınımların yapay olarak oluşturulması, kaotik sistemlerin elektronik, optik ve optoelektronik olarak

gerçekleştirilmesi, kaotik titreşim ve salınımların belirlenmesi ve kontrol edilmesi, lazerlerin kontrolü, türbülans kontrolü, vinç ve gemi salınımlarının kontrolü, hava durumu tahmini vb.'leri verilebilir (Kahyaoğlu ve Süleyman, 2015; Arslan ve ark., 2017; Yardım ve Afacan, 2010).

2.1. Kaos ve Temel Kavramlar

Kaos kavramının bilim tarihine girişi çok uzun bir geçmişe sahip değildir. Kaos alanındaki sıçrama yaratan önemli gelişmelerden biri, 1960'lı yılllarda hava akımlarının bir modelini çalışmak üzere bir matematiksel bilgisayar programı yazan Edward Lorenz tarafından yapılmıştır (Kolumbán ve ark., 1998). Lorenz'in araştırdığı modelde kullandığı bu matematik, sonraki yıllarda araştırılmış ve zamanla, kaotik bir sistemin temel özelliği olarak farklı iki başlangıç koşulları arasındaki çok küçük bir farklılığın, sistemde büyük farklara neden olacağı bilinen bir gerçek haline gelmiştir. Bu anlamıyla kaotik sistemler, yalnızca laboratuvar koşullarında üretilebilen sistemler olmadıkları anlaşılmıştır. Hayatımızdaki fiziksel ve doğrusal olmayan yapıların hepsi kaotik bir davranış sergileme potansiyeline sahiptir (Mobayen ve ark., 2018). Kaotik sistemler, "başlangıç şartlarına hassas bağlılık gösteren ve ölçülemeyecek karmaşıklıkta sistemler" olarak da tanımlanabilir (Yardım ve Afacan, 2010). Kaos teorisi, ilk olarak matematik ve fizik olmak üzere birçok bilim dalı literatüründe yerini almıştır (Madan, 1993).

Kaotik sistemler ayrıca elektronik devre çıkışlarının senkronize edilmesinde, kimyasal tepkimelerin osilasyon kontrollerinde, beyin nöron sinyallerinin incelenmesi gibi birçok kullanım alanına sahiptir. (Ditto, ve Pecor, 1993; Uçar ve ark., 2001; Türk ve Ata, 2002; Arslan ve ark., 2017). Bu nedenle birçok bu özelliğe sahip model, kaotik davranışın incelenmesi için önerilmiştir. Bu önerilen modeller, kullanım amaçlarına göre birçok kez revize edilmiş ve birçok varyasyonları literatüre sunulmuştur (Güler ve Kaya, 2016; Hanbay ve ark., 2007).

2.1.1. Kaotik sistemler

Dinamik sistemler ve dolayısıyla kaotik sistemler, bir sistemin zaman içinde ileri doğru gelişimini gösteren deterministik bir matematiksel tarif olarak tanımlanabilir. Bu sistemler, o anki durumu, geçmiş durumlar cinsinden belirten bir kuralla birlikte olası durumların kümesini içerir. Burada zaman, sürekli (continuous) veya ayrık (discrete) bir değişken olabilir. Eğer kural, ayrık zamanlı olarak uygulanırsa, bu ayrık-zamanlı kaotik sistem olarak adlandırılır. Sürekli-zaman dinamik sistemleri durumunda ise genellikle diferansiyel denklem kümeleri ile ifade edilir (Hayes ve ark., 1993; Pehlivan, 2007). Her $x(0)$ giriş durumu için, $t > 0$ iken gelecekteki sistem durumu $x(t)$, elde edilebilir olan sistemler dinamik sistemlerdir. Bu sistemler zamana bağlılığı "otonom olan" ve "otonom olmayan" olmak üzere iki sınıfta incelenebilir. Otonom olmayan kaotik sistemlerde sistemin bir durum değişkeni mutlaka zamana (t) bağlıdır. Otonom kaotik sistemlerde ise sistem zamandan bağımsızdır (Güven, 2006).

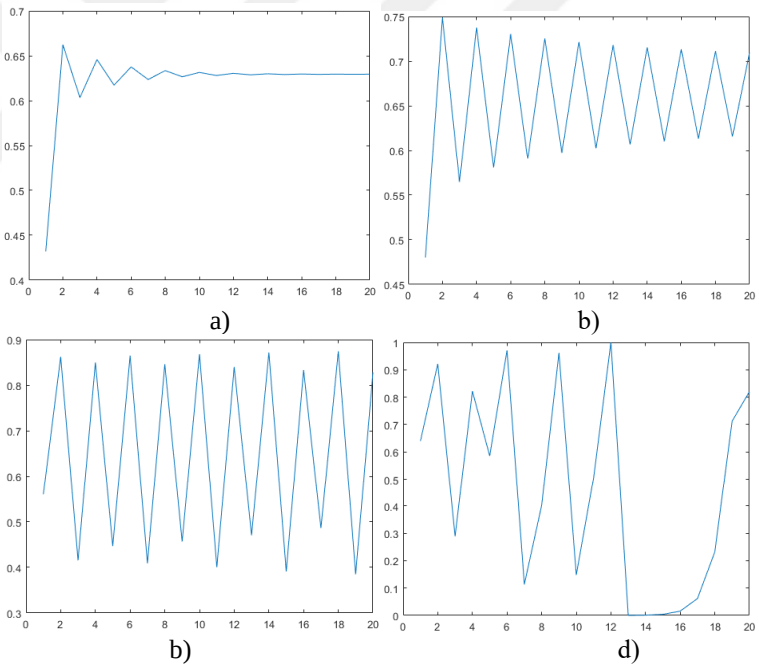
2.1.1.1. Ayrık zamanlı kaotik sistemler

Ayrık zaman kavramı, sürekli olmayan, kesintili ve atlaya atlaya ilerleyen durumlardır. Örneğin bir depodaki doluluğun yıl boyunca değişimini takip etmek için her gün bu ölçüm bir grafiğe işlenirse, sonuçta elde edilen grafiğe ayrık zamanlı grafik denir. Ayrı zamanlarda ölçülüp grafiğe alınan sıcaklık, güç değişimi vs örnek gösterilebilir. Bu tür bir sistemin bir önceki anından faydalanılarak bir sonraki anını veren sistemlere ayrık zamanlı sistemler denir. Bu durum şu şekilde ifade edilir; $\vec{\varphi}: R^m \rightarrow R^m$ bir haritayı ifade eder. $\vec{x}_n$ sisteminin *n.* adımı ve $\vec{x}_{n+1}$ bir sonraki durumu ifade edecek şekilde, $\vec{x}_{n+1} = \vec{\varphi}(\vec{x}_n)$ iterasyon ifadesi ayrık zamanlı bir dinamik sistemi tanımlar. Sonuçta, oluşan $\vec{x}_n$ vektörler dizisi bir yörüngeyi ifade eder. Ayrık zamanlı sistemler tek boyutlu olabildikleri gibi birden fazla boyuta da sahip olabilirler. Bu sistemler içinde tek boyutlu haritaların yapısı oldukça basittir. Bununla beraber, ayrık zamanlı haritaların doğrusal olanları kaotik davranış göstermezler. Doğrusal olmayan haritaların ise kaotik olduğu durumlar vardır.

En çok bilinen tek boyutlu ve nonlineer bir örnek Lojistik haritadır. Kaotik davranış gösteren, basit non-linear denklemlerin kompleksliğine dair ortaya çıkan bu harita, matematiksel biyoloji üzerinde çalışan Robert May tarafından 1976 yılında oluşturulmuştur (May, 1976). Bu tek boyutlu sistem, biyolojik popülasyon dinamiğinin basit bir modeli olan lojistik denklemin ayrıklaştırılmış halidir. Lojistik harita, $0 \leq x \leq 1$ olmak üzere,

$$x_{n+1} = r \cdot x_n(1 - x_n) \tag{2.1}$$

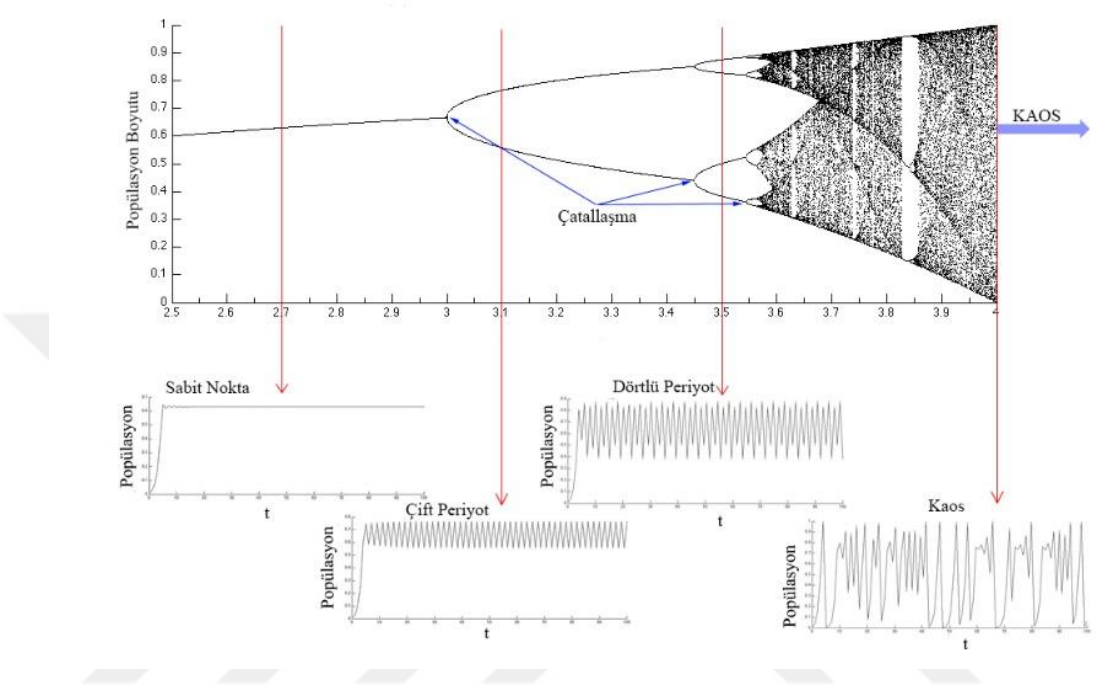
şeklinde tanımlanır. Burada *r* parametresinin sistem davranışı üzerinde büyük etkisi vardır. Şekil 2.3'de, *r* parametresindeki değişimlere göre lojistik haritanın sistem durumları gösterilmiştir.



Şekil 2.3. Lojistik haritanın $x_0 = 0{,}2$ için, *r* parametresinin belirli değerlerine göre değişimi: a) *r = 2.7,* b) *r = 3,* c) *r = 3.5 ve* d) *r = 4*

Şekil 2.3'de görüldüğü gibi lojistik harita, *r* parametresinin değeri 2,7 olduğunda sabit nokta; 3,5 olduğunda dörtlü periyot ve son olarak 4 olduğunda kaotik durum davranış sergilediği görülmüştür.

Lojistik haritanın r'ye bağlı davranışını en açık bir biçimde çatallanma diyagramı (bifurcation diagram) gösterir. Çatallanma diyagramı kaos teorisinde kullanılan analiz yöntemlerinden bir tanesidir. Bununla ilgili kaotik sistemlerin analiz yöntemleri başlığı altında detaylı bilgi verilecektir.



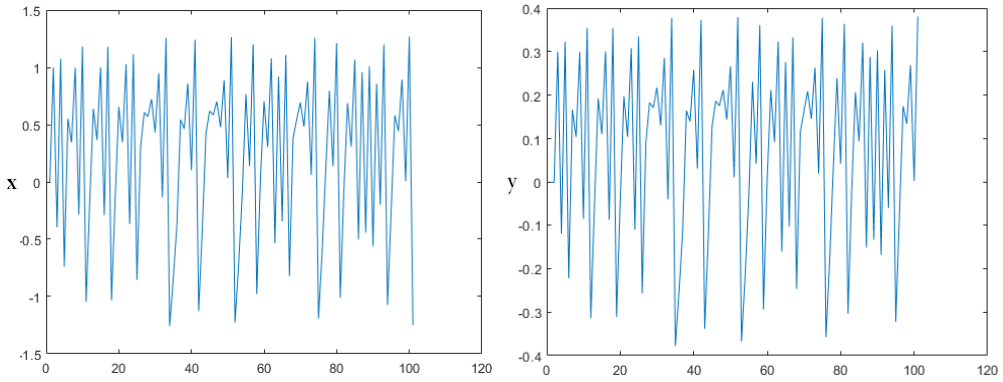
Şekil 2.4. Lojistik harita *r*=2.5 – 4 arası çatallanma diyagramı

Lojistik harita tek boyutlu ayrık zamanlı kaotik haritadır. İki boyutlu ayrık zamanlı kaotik haritaya Hénon haritası örnek verilebilir. Michel Hénon iki boyutlu bir haritanın kaotik olabildiğini göstermiştir (Hénon 1976). Bu iki boyutlu harita aşağıdaki fonksiyon tanımı ile gösterilir.

$$x_{n+1} = y_n + 1 - ax^2{}_n \tag{2.2}$$

$$y_{n+1} = bx_n \tag{2.3}$$

Burada *a* ve *b* değerlerinin durumlarına göre sistem kaotik davranabilmektedir. Hénon makalesinde *a*=1,4 ve *b*=0,3 noktalarının kaotik olduğunu vurgulamıştır.



Şekil 2.5. Hénon haritanın $x_0 = 0,\ \ y_0 = 0,\ \ a = 1{,}4,\ \ b = 0{,}3$ için x ve y değişimi

Lojistik harita dışında literatürde kullanılan tek boyutlu ayrık zamanlı kaotik haritalara; Kübik, Sine, Tent, Gauss, Pinchers ve Spence gibi haritalar örnek gösterilebilir. İki boyutlu ayrık zamanlı kaotik haritalara ise; Hénon, Tinkerball, Kaplan-Yorke, Ikeda, Geciktirmeli Lojistik, Lozi, Holmes kübik, Dissipative Standart, Ayrık Avcı-Av ve Chirikov gibi haritalar örnek olarak verilebilir (Gökyıldırm, 2016).

2.1.1.2. Sürekli zamanlı kaotik sistemler

Sürekli zamanlı bir sistem başlangıç anında yani $\vec{x}(t_0) = \vec{x}_0$ olmak üzere aşağıda verilen denklem (Denklem 2.4) şeklinde tanımlanabilir.

$$\frac{d\vec{x}(t)}{dt} = \vec{F}[\vec{x}(t), t] \tag{2.4}$$

Bu denklemde $\vec{F}: R^m \to R^m$ tanımlı vektör alanını olmak üzere $\vec{x} \in R^m$ durum vektörü, $\vec{x}_0$ başlangıç durum vektörünü, t zamanı ve t_0 başlangıç zamanını göstermektedir. Burada tanımlı vektör alanı zamana bağlı olduğundan otonom olmayan bir sistemdir. Otonom olan yani zamana bağlı olmayan dinamik bir sistemin, başlangıç anında $\vec{x}(t_0) = \vec{x}_0$ olmak üzere şu şekilde tanımlanabilir.

$$\frac{d\vec{x}(t)}{dt} = \vec{F}[\vec{x}(t)] \tag{2.5}$$

Literatürde sıklıkla kullanılmış olan sürekli zamanlı kaotik sistemlere; Lorenz, Rössler, Chua, Duffing-Holmes, Van Der Pol, Chen, Rikikate, Rucklidge, LotkaVolterra, Sprott94, Moore-Spiegel gibi sistemler örnek olarak verilebilir.

2.1.2. Kaotik sistemlerin analiz yöntemleri

Kaotik sistemlerle çalışılabilmesi için öncelikle bu tarz sistemlerin dinamik analizlerinin yapılması ve hangi şartlar altında kaotik olduklarının anlaşılması gerekmektedir. Bir dinamik sistemin kaotik olup olmadığının anlaşılması için çeşitli yöntemler bulunmaktadır. Denge noktaları, zaman serileri, faz portreleri, Lyapunov üstelleri ve çatallanma diyagramı analizleri bunlardan bazılarıdır.

2.1.2.1. Denge noktaları ve kararlılık analizi

Kaotik sistemlerin denge noktaları (equilibrium), doğrusal olmayan (nonlinear) dinamik sistemlerde olduğu gibi o sistemin davranışı hakkında bilgi verir. Sistemin denge noktalarını bulmak için $dx(t)/dt = F[x(t)] = 0$ şeklinde sistem sıfıra eşitlenir. Bu eşitliği sağlayan denge noktaları, yakınlarındaki çözümlerin davranışını da temsil eder. Böylece doğrusal olmayan bir dinamik sistemin davranışı, elde edilen denge noktaları etrafında doğrusal bir sistem gibi yaklaşık olarak incelenebilir (Çiçek, 2016).

Sistemin denklemlerinin çözümü sonucunda elde edilen ifadeler reel sayılar ise sistemin denge noktalarının olduğu söylenebilir. Bununla beraber bazı kaotik sistemlerin reel denge noktaları olmayıp sadece sanal denge noktaları vardır. Bu gibi sistemlere denge noktasız kaotik sistemler denilebilir (Gökyıldırım, 2016).

Dinamik sistemin özdeğerlerinden (eigenvalue) en az biri pozitif ise dinamik sistem kararsızdır. Kaotik sistemler kararsız bir davranış gösterdikleri için sistemin özdeğerlerinin bulunması gerekir. Dinamik sistemin özdeğerlerini bulmak için ilk önce

sistemin Jakobiyen matrisinin bulunması gerekir. Denklem 2.6'da Jakobiyen matrisi ifadesi verilmiştir.

$$J = \begin{bmatrix} {\partial F_1}/{\partial x_1} & {\partial F_1}/{\partial x_2} & \cdots & {\partial F_1}/{\partial x_n} \\ {\partial F_2}/{\partial x_1} & {\partial F_1}/{\partial x_2} & \cdots & {\partial F_2}/{\partial x_n} \\ \vdots & \vdots & \ddots & \vdots \\ {\partial F_n}/{\partial x_1} & {\partial F_n}/{\partial x_2} & \cdots & {\partial F_n}/{\partial x_n} \end{bmatrix} \tag{2.6}$$

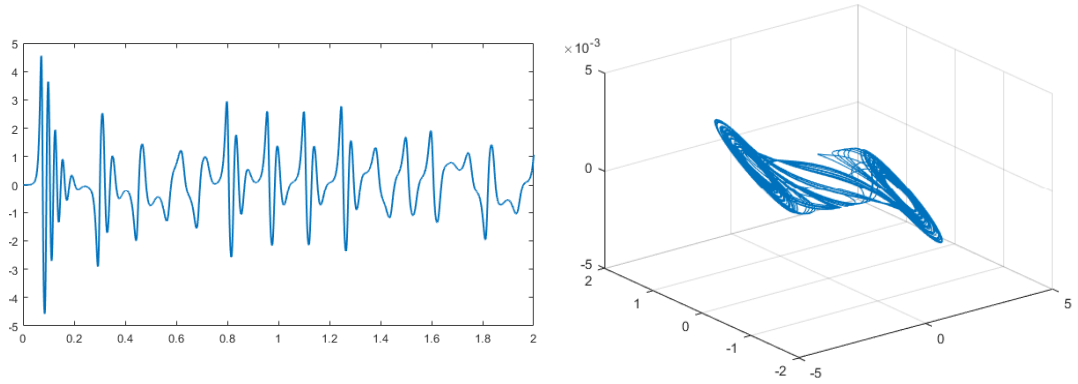
Jakobiyen matrisi kullanılarak Denklem 2.7'de verilen determinant ile özdeğerler (λ) hesaplanır.

$$\det(J - \lambda I) = |J - \lambda I| = 0 \tag{2.7}$$

I, birim matrisi temsil etmektedir. Bulunan bu özdeğerlerden (λ) sistemin kararsızlık durumu, dolayısıyla kaotik olup olmadığı hakkında yorum yapılabilir. Elde edilen özdeğerlerden en az bir tanesinin reel kısmı pozitif ise denge noktası kararsız olup sistem kaotiktir denilebilir. Fakat bulunan bu sonuçlar tek başına ele alındığında sistemin kaotik olup olmadığı konusunda kesin bir kanıya varılamamaktadır. Sistemin kaotikliği konusunda net bir fikir elde edilebilmesi için, daha sonraki kısımlarda anlatılan diğer analizlerin de yapılması gerekmektedir.

2.1.2.2. Faz portreleri (Faz uzayı)

Kaotik sistem durum değişkenlerinin her birinin zamana göre değerleri aperiyodik (periyodik olmayan) bir davranış sergilemesi gereklidir. Bu değişkenlerin zamana göre değişimlerinin grafiği gözlemlendiğinde bu durumun var olup olmadığı anlaşılabilir (Özer, 2005). Şekil 2.6.'da kaotik bir sistemin durum değişkeninin zamana göre çizdirilmiş değerleri verilmiştir.



Şekil 2.6. Örnek kaotik bir sistemin zamana göre değişimi ve 3 boyutlu faz uzayında yörünge şekli

Dinamik bir sistemin durum uzayının yörüngeler ile bölümlenmesi faz portresini (durum uzayını) verir. Dinamik sistemin bir başlangıç noktası ile çözümü sonucu elde edilen durum değişkenleri değerlerinin faz uzayına iz düşümleri dinamik sistemin yörüngesi (trajectory, orbit) olarak tanımlanır. Sürekli zaman dinamik sistemler için yörünge kavramı akış (flow) olarak da ifade edilir. x_0 ilk koşulundan başlayan bir yörünge, x durum uzayının sıralı bir alt kümesidir. Şekil 2.6.'da kaotik bir sistemin üç boyutlu faz uzayında yörünge şekli de verilmiştir.

Kaotik sistemlerin faz uzayı incelendiğinde belli bir sınır içinde karmaşık bir şekil ortaya çıkar. Bu durum sistemin kaotik davranış sergilediğini gösterir (Giannakopoulos ve ark., 2002; Özer, 2005). Sabit bir değerin faz uzayı bir nokta, periyodik bir sinyalin faz uzayı kapalı bir eğri, yarı-periyodik (quasiperiodic) sinyallerin faz uzayı torus şeklinde olur (Özer, 2005; Çiçek, 2016).

Üç boyutlu kaotik bir sistem için üç adet iki boyutlu ve bir adet üç boyut olmak üzere dört farklı şekilde bir sistemin kaotik çekicileri yani faz portrelerine bakılabilir. Matlab odesolve.m programı ile kaotik sistem verileri girilerek program çıktısında istenen faz portreleri kolaylıkla elde edilebilir. Matlab Simulink ve elektronik devre gerçekleme benzetim programlarından osilaskop çıktıları olarak da bu grafikler elde edilebilmektedir.

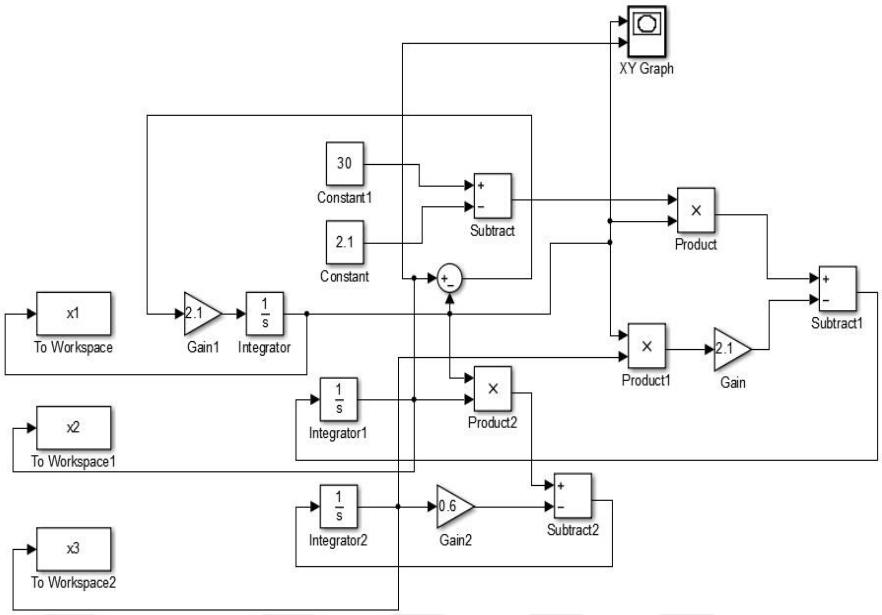
2.1.2.3. Zaman serisinde başlangıç değerlerine hassas bağımlılık analizi

Kaotik sistemler zaman domeninde düzensiz davranış, sınırsız sayıda farklı aperiyodik salınım, gürültü benzeri geniş güç spektrumu başlangıç koşullarına hassas bağımlı pozitif lyapunov üsteli ve sistem boyutunun fraktal olması gibi özellikler gösterir. Bu özelliklerden sadece birinin olması o dinamik sistemin kaotik olduğu hakkında kesin bilgi vermez. Yani bu özelliklerin birkaçının kaotik sistemlerde olması gerek ama yeter şart değildir (Jost, 2005; Kia, 2011; Fraga ve ark., 2012). Bir sistemin kaotik olma şartlarından bir tanesi de başlangıç şartlarına olan hassas bağımlılıktır. Kaotik bir sistemin başlangıç şartlarından herhangi biri değiştirildiğinde, sistemin aynı zaman zarfında farklı kaotik işaretler ürettiği bilenen bir gerçektir.

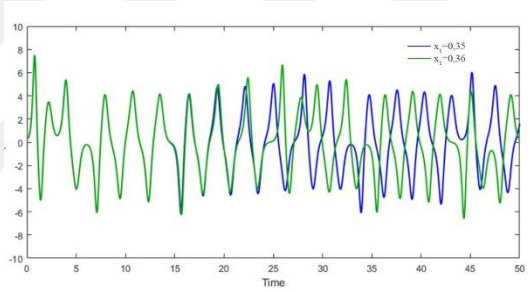
Kaotik bir sistemin değişkenlerinden bir tanesinin iki farklı başlangıç değerinin aynı grafik üzerinden incelenmesi yoluyla sistemin başlangıç şartlarına olan hassas bağımlılığı gözlemlenebilir.

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) \\ \dot{x_2} = (c - a)x_1 - ax_1x_3 \\ \dot{x_3} = -bx_3 + x_1x_2 \end{cases} \tag{2.8}$$

$a = 2.1, b = 0.6, c = 30$ ve başlangıç şartları $x_1 = 0{,}35$, $x_2 = 0$, $x_3 = 3{,}39$ için Matlab-Simulink ile sistem modellendiğinde (Şekil 2.7.) ve x_1 başlangıç şartı 0,35 yerine 0,36 ile başlatıldığında sistemin çıkışındaki değişim grafiği Şekil 2.8.'de verilmiştir.



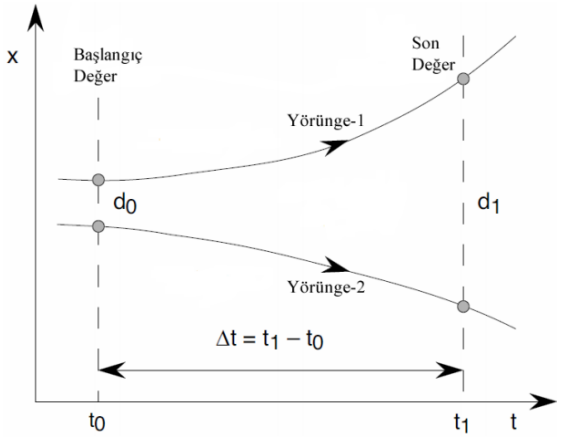
Şekil 2.7. Tigan Sistemi'nin Matlab-Simulink modellemesi,



Şekil 2.8. Örnek sistemin başlangıç şartlarına olan hassas bağımlılığını gösteren zaman serileri

2.1.2.4. Lyapunov üstelleri

Kaotik sistemler başlangıç şartlarına hassas bağımlılık gösteren bir yapıya sahiptir. Faz spektrumunda birbirine çok yakın iki farklı başlangıç noktasındaki hareketlerin zaman içinde birbirinden ortalama bir üstel faktörle uzaklaşıp, ayrılmaları kaotik sistemlerde var olan bir gerçektir. Bu üstel faktör uygulamalı matematik, teorik mekanik ve fizik alanında çalışma yapan Rus matematikçi Aleksandr Mikhailovich Lyapunov'un adı ile anılmıştır. (Yonemoto ve Yanagawa, 2007).



Şekil 2.9. Farklı başlangıç şartında iki komşu yörüngenin birbirinden uzaklaşması (Kinsner, 2006)

Lyapunov üstelleri, deterministtik kaotik sistemin faz uzayının boyut sayısı kadardır ve her bir üstel ayrılma veya yakınlaşmanın ölçüsünü ifade eder. 1980'li yıllarda Lyapunov üstellerinin elde edilmesi Wolf tarafından gerçekleştirilmiştir (Wolf, 1985). İki başlangıç noktası arasındaki uzaklık d_0 olmak üzere, daha sonraki bir zamanda bu uzaklık;

$$d(t) = d_0 e^{\lambda t} \tag{2.9}$$

şeklinde verilir ve birinci Lyapunov üsteli λ;

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})} \tag{2.10}$$

şeklinde hesaplanır (Yardım ve Afacan, 2010, Strogatz, 1994; Kocal ve ark., 2008). Bir dinamik sistem, toplamları sıfırdan küçük olmak üzere, sıfırdan büyük en az bir Lyapunov üsteli içeriyorsa kaotik olarak tanımlanır. Bu özellik tuhaf bir çekiciyi, sürekli hal davranışlarının diğer tiplerinden ayırır (Pehlivan, 2007). Üç boyutlu bir sistemde, Lyapunov üstelleri için tek mümkün durum (+,0,-) tipidir. Bu durumda $\lambda_1>0$, $\lambda_2=0$, ve $\lambda_3<0$, olmaktadır (Bolotin ve ark., 2009; Sandri, 1996). Dinamik sistemlerde Lyapunov üstelleri çekicilerinin tiplerini karakterize etmeye yardımcı olur (Gündüz, 2002). Lyapunov üstelleri (–, –, –) ise sistem kararlı nokta (stable node) veya odak (focus) şeklinde, Lyapunov üstelleri (–, –, 0) ise sistem kararlı limit çevrim (stable limit cycle) şeklinde, Lyapunov üstelleri (–, 0, 0) ise sistem torus şeklinde, Lyapunov

üstelleri (–, 0, +) ise sistem garip çekici (strange attractor) yani kaos durumundadır. Dört boyutlu (higher-dimension) sistemlerde ise üç farklı kaos durumu mevcuttur. Eğer sistemin birden fazla Lyapunov üsteli pozitif ise bu durum hiperkaos (hyperchaos) olarak adlandırılır. Lyapunov üstelleri (+, +, 0, –) ise sistem hiper-kaos (hyper-chaos), Lyapunov üstelleri (+, 0, –, –) ise sistem kaos, Lyapunov üstelleri (+, 0, 0, –) ise sistem torus kaostur.

Tablo 2.2. Lyapunov üstellerinin işaretlerine göre değişimi

Sistem Türü	**Sistem Durumları**	**Lyapunov Üstellerinin İşaretleri**
3 Boyutlu Sistemler	Sabit Nokta	(-, -, -)
	Limit Döngü	(0,-,-)
	Torus	(0,0,-)
	Tuhaf Çekici	(+,0,-)
4 Boyutlu Sistemler	Sabit Nokta	(-,-,-,-)
	Limit Döngü	(0,-,-,-)
	Tuhaf Çekici	(+,0,-,-)
	Hiperkaos	(+,+,0,-)

2.1.2.5. Çatallanma diyagramı

Çatallanma diyagramı kaotik sistemlerin analizlerinde en çok kullanılan yöntemlerden bir tanesidir (Glendinning, 1994; Akgül ve ark.,2016; Tsumoto ve ark., 2012; Kaçar, 2016).

Dinamik sistemlerde ve dolayısıyla kaotik sistemlerde sistemin durum değişkenleri, o sistemin parametrelerine göre farklı değerler alır. Parametre değerlerindeki bu değişiklikler ile bir denge noktası oluşabilmekte veya yok olabilmektedir. Bu tarz değişiklikler sistem kararlılığına etki etmektedir. Dinamik sistemlerde sistemin davranışlarına etki eden parametrelerde oluşan küçük değişikliklerin sistemin denge noktasında ani değişimlere neden olması ya da kararlı denge noktalarının kararsız duruma geçtiği anlarda çatallanma olayı meydana gelir.

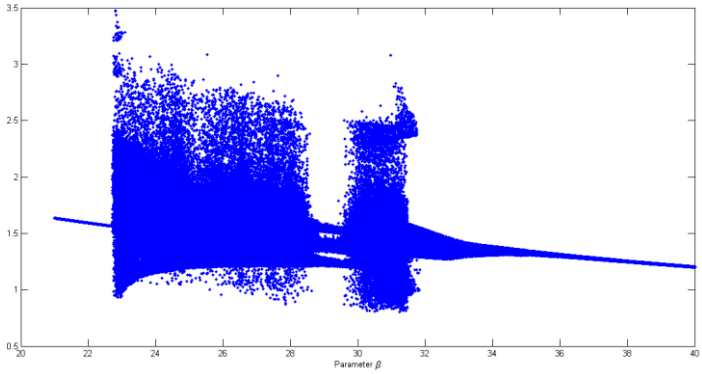
Dinamik sistemin bir parametresinin belli bir aralıktaki sistem durum değişkeninin yerel maksimum değerlerin birbirlerine göre çizdirilmesi ile elde edilen grafik çatallanma diyagramı olarak adlandırılır. Çatallanma diyagramı kullanılarak sistemin kararlılığı, kaotikliği gibi davranışsal özellikleri hakkında yorum yapılabilir.

Şekil 2.10.'da çatallanma olayına ve çatallanma diyagramına bir örnek olarak, en bilinen kaotik sistemlerden birisi olan Chua Kaotik Osilatör sistemine ait çatallanma diyagramı verilmiştir. Bu diyagram Denklem 2.11'de görülen Chua Kaotik Osilatör sistem parametrelerinden β parametresi için elde edilmiştir.

$$\begin{aligned} \dot{x} &= a\left(y - x - g(x)\right) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y \end{aligned} \tag{2.11}$$

Denklem (2.11)'deki "a" ve "β" boyutsuz parametrelerdir. $g(x)$ fonksiyonu denklem (2.12)'de gösterilmiştir. Denklem (2.12)'deki "c" ve "d" ise katsayılardır.

$$g(x) = cx + \frac{1}{2}(d - c)[|x + 1| - |x - 1|] \tag{2.12}$$



Şekil 2.10. Chua devresi β parametresi değerine göre çatallanma diyagramı

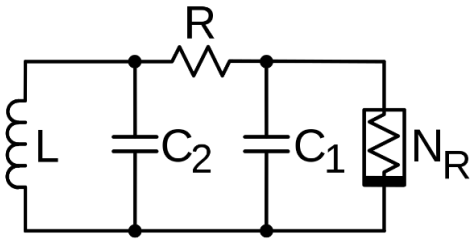
Şekil 2.10'da görüldüğü gibi β, 21-23 ve 33-40 değerleri arasında sistemin kararlı bir davranış sergilediği görülmektedir. Görüldüğü üzere çatallanma diyagramı ile denklem 2.11'daki sistemin dinamik davranışları hakkında yorum yapılabilmektedir.

2.2. Referans Kaotik Sistemler

Yapılan çalışmada kullanılan referans kaotik sistem denklemlerinin, zaman serileri ve faz diyagramları ile birlikte sık kullanılan bazı sistemlerin sayısal ve kaotik analizleri bu başlık altında verilmiştir.

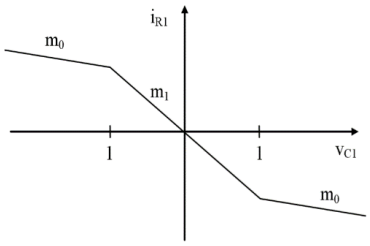
2.2.1. Chua kaotik sistemi

Chua elektronik devresinin sistem yapısı basittir. Dört doğrusal eleman ve bir doğrusal olmayan eleman olan Chua diyotundan oluşmaktadır. Chua diyotu farklı aktif devre yapılarıyla da oluşturulabilir.



Şekil 2.11. Chua Devresi

Chua'nın devresi bir doğrusal indüktans (L), iki doğrusal kapasitör (C_1 ve C_2), bir doğrusal direnç (R) ve Chua diyotu olarak adlandırılan gerilim kontrollü direnç (NR)'den oluşur. Chua devresi ve doğrusal olmayan direncin parça parça lineerleştirilmiş I-V karakteristiği Şekil. 2.12'de görülmektedir. Chua kaotik osilatör devre denklemleri, denklemindeki üç adet adi diferansiyel denklemle tanımlanır.

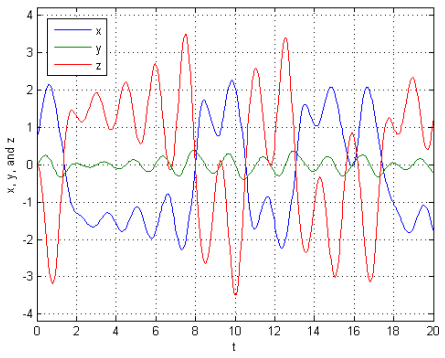


Şekil 2.12 Doğrusal olmayan direncin karakteristiği

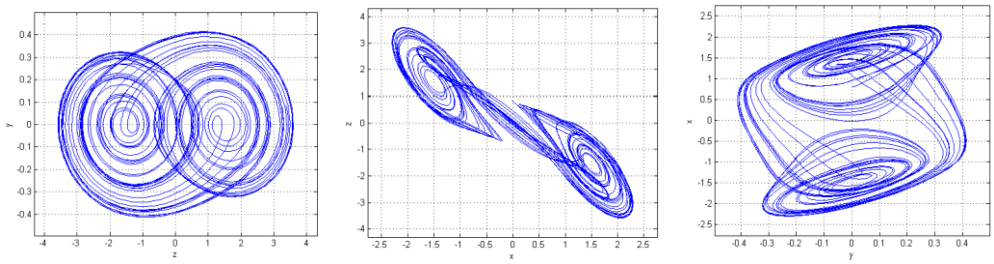
$$C_1\frac{dV_{C_1}}{dt} = G\left(V_{C_2} - V_{C_1}\right) - f(V_{C_1})$$
$$C_2\frac{dV_{C_2}}{dt} = G\left(V_{C_2} - V_{C_1}\right) + i_L \qquad (2.13)$$
$$L\frac{di_L}{dt} = -V_{C_2}$$

Burada, $G = 1/R$ ve doğrusal olmayan elemanın $V_{C_1} - i$ karakteristiği aşağıda tanımlanmaktadır. Chua diyotunun I_R akımı iki kırılma noktasına sahip parça parça doğrusal fonksiyon olan $f(V_{C_1})$ ile ifade edilir. Analitik ifadesi ise denklem 2.14'deki verilmiştir. Burada devre parametreleri $G = 0{,}7$, $m_0 = -5/7$, $m_1 = -8/7$ olup $E = 1$'dir.

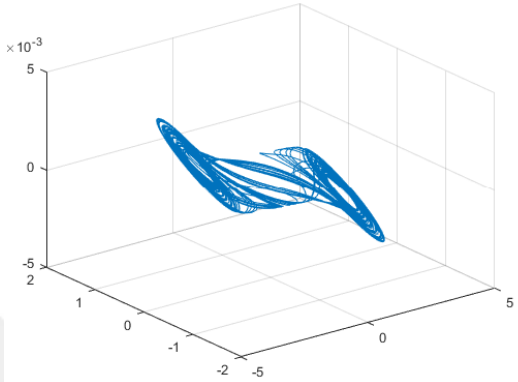
$$f\left(V_{C_1}\right) = m_1 V_{C_1} + \frac{1}{2}(m_0 - m_1)\left(\left|V_{C_1} + E\right| - \left|V_{C_1} - E\right|\right) \qquad (2.14)$$



Şekil 2.13. Chua x, y, z – zaman grafiği.



Şekil 2.14. Chua Sistemi x, y ve z durum değişkenleri faz portreleri



Şekil 2.15. Chua Sistemi V_1, V_2 ve I_L durum değişkenleri 3 boyut faz portresi

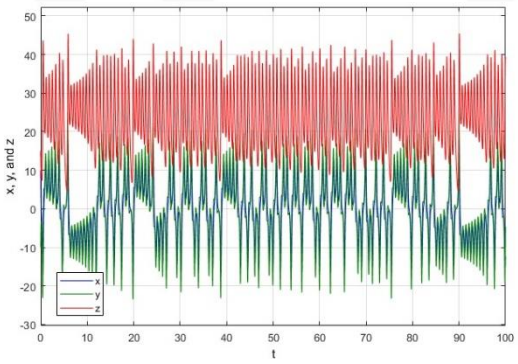
2.2.2. Lorenz kaotik sistemi

1960'lı yılların başlarında hava akımının basit bir modelini oluşturmak üzere matematiksel bilgisayar programı gerçekleştiren Edward Lorenz, hava akımlarının ısınması yoluyla nasıl hareket edeceğine ilişkin bir model üzerinde çalışmıştır (Lorenz, 1963). Edward Lorenz'in tasarladığı bilgisayar sistemi, hava akışını modelleyen matematiksel diferansiyel denklemler içeriyordu. Bilgisayar kodları bütünüyle belirlenimci özellikte olduğundan Lorenz, aynı başlangıç koşulları verildiğinde program sonucu sürekli aynı sonucu almayı bekliyordu. Lorenz, aynı sandığı başlangıç değerlerini çok küçük farklılıklarla girdiği zaman her defasında kökten farklı sonuçlar elde ediyordu. Lorenz'in atmosferi modellemek için kullandığı bu matematiksel sistem 1970'lerden itibaren geniş bir biçimde de araştırma konusu oldu.

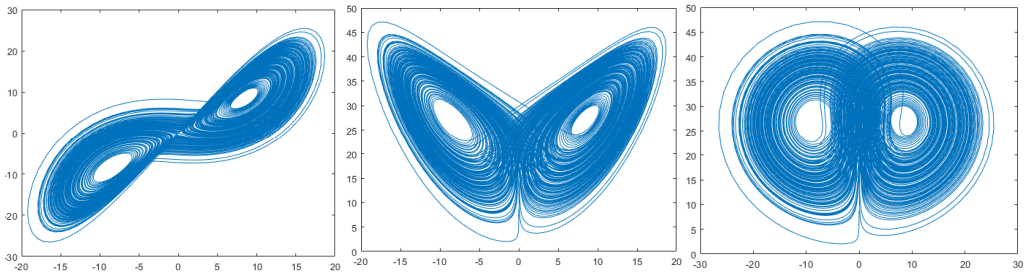
Lorenz'in sunduğu 3 adet non-lineer birinci dereceden olan diferansiyel denklem takımı, epeyce basit olmasının tersine elde edilen davranışlar şaşırtıcı derecede karmaşıktır. Bu denklemler:

$$\begin{cases} \frac{dx}{dt} = a(y - x) \\ \frac{dy}{dt} = rx - y - xz \\ \frac{dz}{dt} = xy - bz \end{cases} \tag{2.15}$$

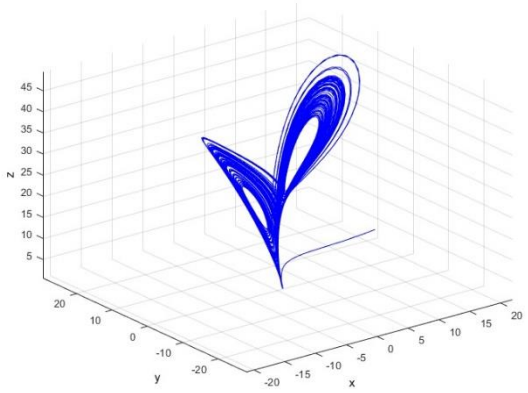
şeklindedir. Denklemlerdeki; a, r ve b denklem parametrelerini ve x, y, z ise durum değişkenleridir. Önerilen çalışma parametreleri ise $a = 10$, $r = 28$ ve $b = 8/3$' tür. Denklemdeki başlangıç şartlarının çok küçük değerlerinde dahi sistemin cevabı oldukça değişmektedir. Uygun parametre değerleri ve başlangıç şartları ile oluşturulan matlab odesolve ile simülasyon sonucu oluşan sistem cevapları ve faz portreleri sırasıyla Şekil 2.16, Şekil 2.17 ve Şekil 2.18'de gösterilmiştir.



Şekil 2.16. Lorenz Sistemi x,y,z zaman grafiği



Şekil 2.17. Lorenz Sistemi 2 boyutlu faz portreleri



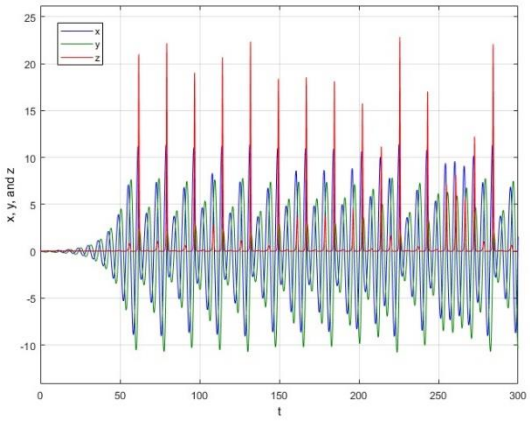
Şekil 2.18. Lorenz Sistemi 3 Boyutlu faz portresi

2.2.3. Rössler kaotik sistemi

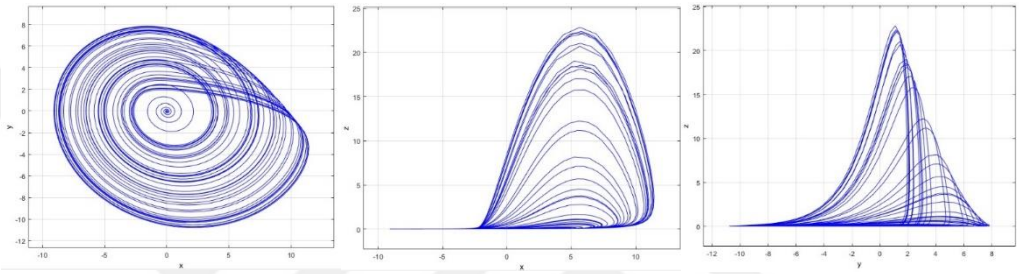
Otto Rössler, Rössler çekicisini 1976 yılında literatüre sunmuştur (Rössler, 1976). Kaotik bir sistem olarak Rössler atraktörü, kimyasal reaksiyonların incelenmesi ile ortaya çıkmıştır. Sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= -(y+z) \\ \dot{y} &= x + ay \\ \dot{z} &= b + z(x-c) \\ a, b, c &> 0 \end{aligned} \tag{2.16}$$

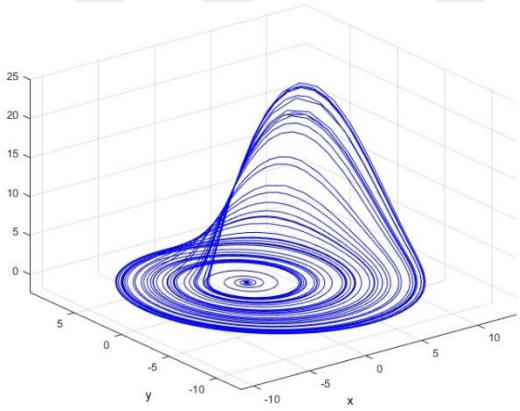
şeklinde ifade edilir. Rössler denklemleri kullanılarak üretilen işaretler de kaotik sistem özelliklerini barındırır. Rössler çekicisine ait $a = 0{,}2$, $b = 0{,}2$ ve $c = 5{,}7$ değerleri için bulunan Rössler faz portreleri ve zaman serisi görüntüleri aşağıdaki şekillerde verilmiştir.



Şekil 2.19. Rössler Sistemi x,y,z zaman grafiği



Şekil 2.20. Rössler Sistemi 2 boyutlu faz portreleri



Şekil 2.21. Rössler Sistemi 3 boyutlu faz portresi

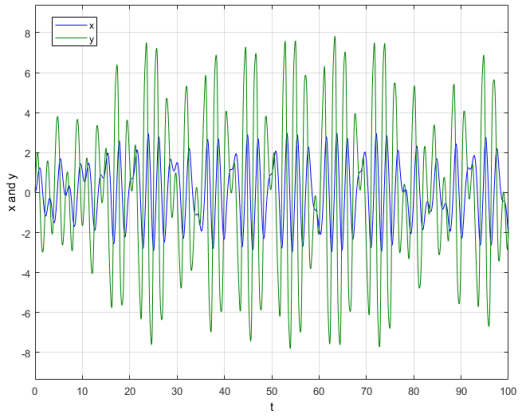
2.2.4. Van Der Pol kaotik sistemi

Kaotik işaret osilatörü olan bir başka dinamik denklem de Van Der Pol kaotik sistemidir. Balthazar Van Der Pol, 1920 ve 1930'larda laboratuvarda modern deneysel dinamikleri başlatan Hollandalı bir elektrik mühendisiydi. Van Der Pol eşitliğinin çözümü, kapalı bir eğri üzerinde bir noktanın hareketidir. Bu hareket sabit genlikli bir

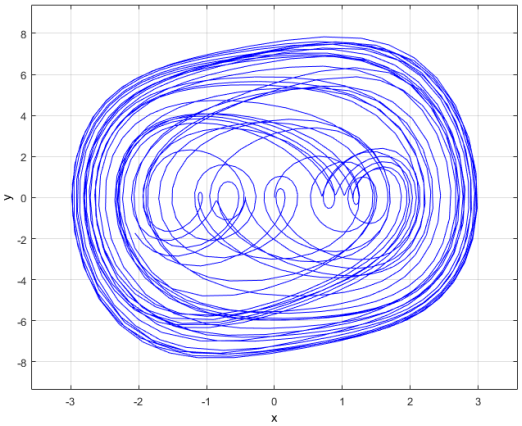
osilasyondur. Van Der Pol eşitliği otonom osilasyonların bir örneğidir (Cartwbight, 1960). Bu çalışmada Denklem 2.17'de verilen eşitlik kullanılmıştır.

$$\dot{x} = y$$
$$\dot{y} = a \cdot (1 - x^2) \cdot y - x^3 + b \cdot \cos(c \cdot t) \qquad (2.17)$$

$x\,(0) = 0,\ y\,(0) = 0$ başlangıç şartları ve $a = 0{,}2, b = 5{,}8\ ve\ c = 3$ parametreleri için elde edilen kaotik zaman serileri ve faz aşağıdaki şekillerde verilmiştir.



Şekil 2.22. Van Der Pol Sistemi x,y zaman grafiği



Şekil 2.23. Van Der Pol Sistemi 2 boyutlu faz portreleri

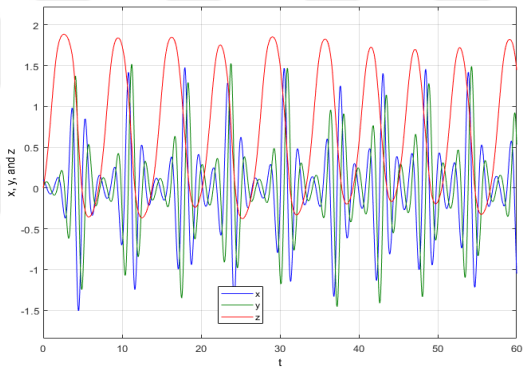
2.2.5. Aizawa kaotik sistemi

Japonya'da yer alan özel bir üniversitede jeoloji ve jeofizik alanında çalışmalar yapan Prof. Yoji Aizawa tarafından bulunan kaotik sistem için denklemler ve parametreler aşağıdaki gibidir.

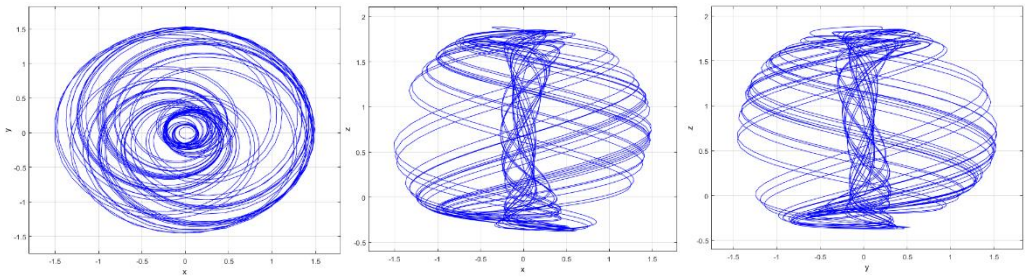
$$\begin{cases} \dot{x} = (z - \beta) \cdot x - \delta \cdot y \\ \dot{y} = (\delta \cdot x) + (z - \beta) \cdot y \\ \dot{z} = \gamma + \alpha \cdot z - \dfrac{z^3}{3} - (x^2 + y^2) \cdot (1 + \varepsilon \cdot z) + (\zeta \cdot z \cdot x^3) \end{cases} \tag{2.18}$$

$$\alpha = 0.95,\ \beta = 0.7,\ \gamma = 0.6,\ \delta = 3.5,\ \varepsilon = 0.25,\ \zeta = 0.1 \tag{2.19}$$

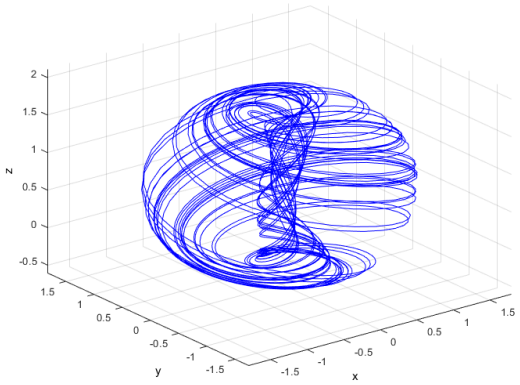
$\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ denklem parametreleri ve x, y, z üç boyutlu koordinatlar olmak üzere Aizawa sistemi aşağıdaki parametreleri ve $x = 0.1,\ y = 0,\ z = 0$ ilk şartları için elde edilen zaman grafikleri Şekil 2.24'de ve kaotik çekiciler şekil 2.25'te, üç boyutlu x-y-z kaotik yörüngesi ise Şekil 2.26.'da verilmiştir.



Şekil 2.24. Van Der Pol Sistemi x,y,z zaman grafiği



Şekil 2.25. Van Der Pol Sistemi 2 boyutlu faz portreleri



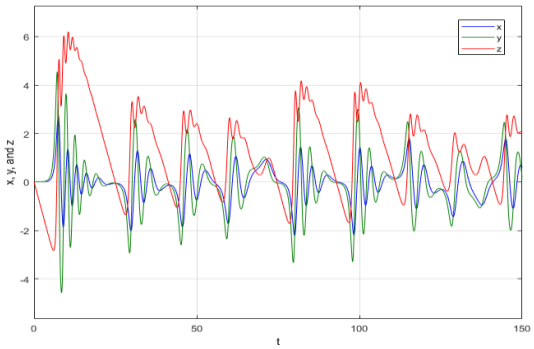
Şekil 2.26. Van Der Pol Sistemi 3 boyutlu faz portresi

2.2.6. Pehlivan kaotik sistemi

Akademisyen İhsan Pehlivan tarafından yapılan bilgisayar simülasyonları ve çalışmalar sonucu, otonom doğrusal olmayan birinci dereceden adi diferansiyel denklemler şeklinde sunulan kaotik sistemlerden yeni kaotik G sistemi olarak adlandırılan kaotik sistem aşağıda verilmiştir.

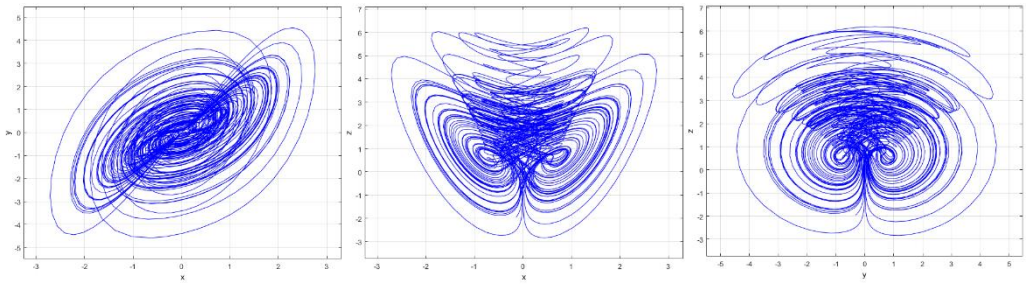
$$\begin{aligned} \dot{x} &= y - x \\ \dot{y} &= ay - xz \\ \dot{z} &= xy - a \end{aligned} \tag{2.20}$$

Bu kaotik sisteminin, $a = 0{,}5$ parametresi, $x_0 = 0{,}001$, $y_0 = 0{,}001$ ve $z_0 = 0$ başlangıç şartları için elde edilen durum değişkenlerinin zamana göre değişimi Şekil 2.27.'de görülmektedir.

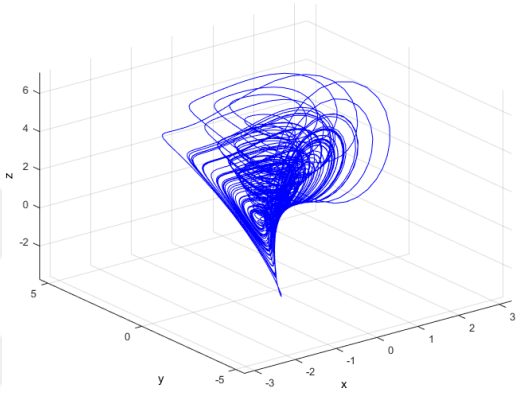


Şekil 2.27. Pehlivan G Sistemi x,y,z zaman grafiği

Aynı parametre ve ilk şartlardaki faz portreleri ise Şekil 2.28.'de verilmiştir.



Şekil 2.28. Pehlivan G Sistemi 2 boyutlu faz portreleri



Şekil 2.29 Pehlivan G Sistemi 3 boyutlu faz portresi

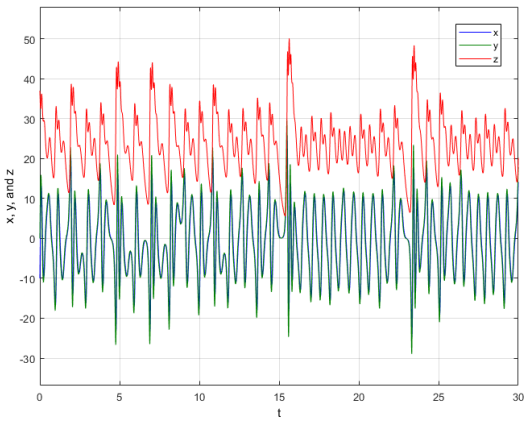
2.2.7. Chen kaotik sistemi

Guanrong Chen ve Ueta tarafından 1999 yılında bulunan (Chen ve Ueta, 1999) aşağıdaki doğrusal olmayan denklem sistemi Chen Sistemi olarak bilinir. Burada a, b ve c reel sabitlerdir.

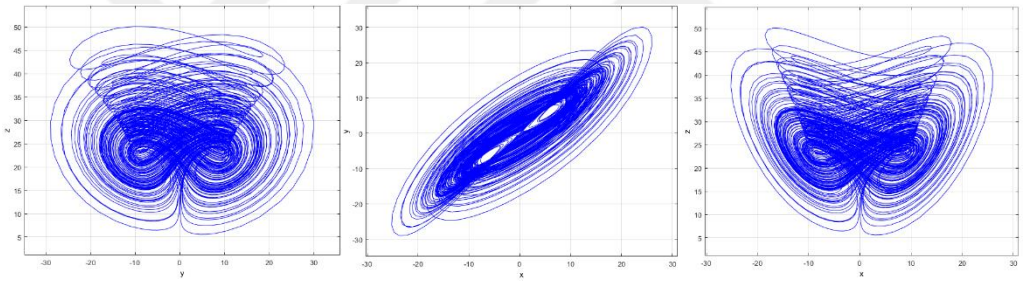
Sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= a(y - x) \\ \dot{y} &= -xz + (c - a)x + cy \\ \dot{z} &= xy - bz \end{aligned} \tag{2.21}$$

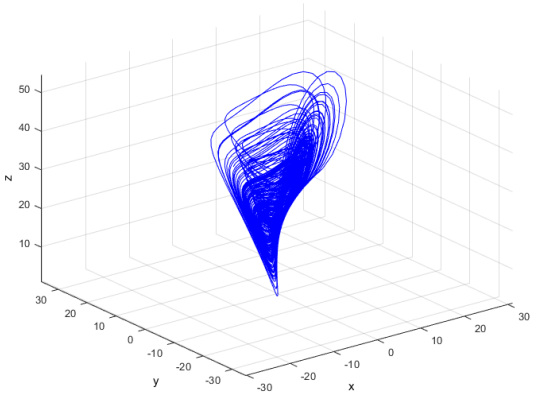
Burada $a = 35$, $b = 3$ ve $c = 28$ parametresi, $x_0 = -10$, $y_0 = 0$ ve $z_0 = 37$ başlangıç şartları için elde edilen x, y, z durum değişkenlerinin zaman grafiği Şekil 2.30.'da, faz portreleri ise Şekil 2.31 ve 2.32'de görülmektedir.



Şekil 2.30. Chen Sistemi x,y,z zaman grafiği



Şekil 2.31. Chen Sistemi 2 boyutlu faz portreleri



Şekil 2.32. Chen Sistemi 3 boyutlu faz portresi

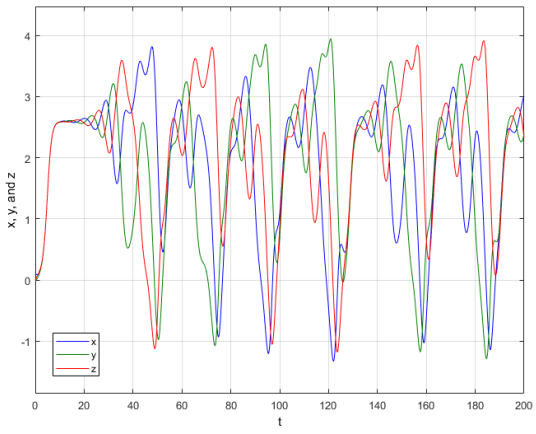
2.2.8. Labyrinth kaotik sistemi

Ren'e Thomas, aşırı dozun bir zaman türevini ifade ettiği, formun özellikle basit ve matematiksel olarak üç boyutlu bir akışını önermiştir (Thomas, 1999). Sistem, kimyasal reaksiyonlar, ekoloji ve evrimde sıkça ortaya çıkan büyük bir otokatalitik model sınıfını temsil etmektedir (Ramussen ve ark., 1990; Deneubourg ve Goss, 1989; Kauffman, 1993). Sistem, b parametresi ile x, y ve z değişkenlerinde döngüsel olarak simetriktir ve bazı harici enerji kaynağı veya başka bir eşdeğer etki altında üç boyutlu bir kafes içinde salınım yapar. Çekicinin tek bir parametre ile (2 ila 3 veya 0 ve 1 aralığında) neredeyse herhangi bir boyuta ayarlanabilen bir kaotik sistemdir (Sprott ve Chlouverakis, 2007).

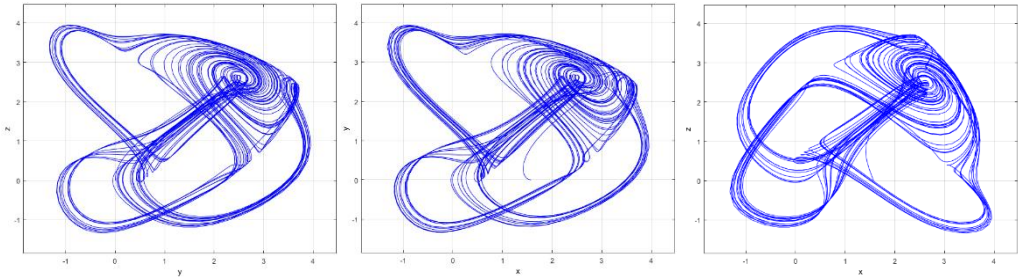
Sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= sin(y) - bx \\ \dot{y} &= sin(z) - by \\ \dot{z} &= sin(x) - bz \end{aligned} \tag{2.22}$$

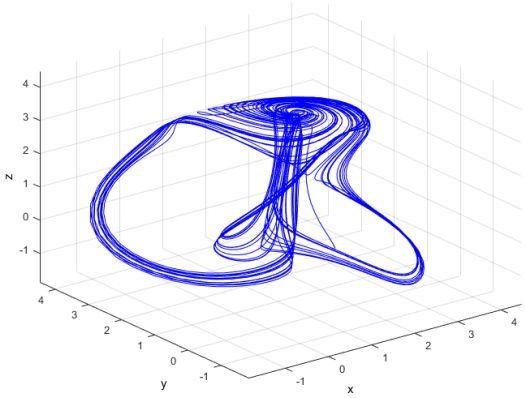
Burada $b = 0{,}2$ parametresi, $x_0 = 0{,}1$, $y_0 = 0$ ve $z_0 = 0$ başalngıç değerleri için elde edilen durum değişkenleri zaman grafiği Şekil 2.33.'de faz portreleri ise Şekil 2.34 ve 2.35'de görülmektedir.



Şekil 2.33. Labyrinth Sistemi x,y,z zaman grafiği



Şekil 2.34. Labyrinth Sistemi 2 boyutlu faz portreleri



Şekil 2.35. Labyrinth Sistemi 3 boyutlu faz portresi

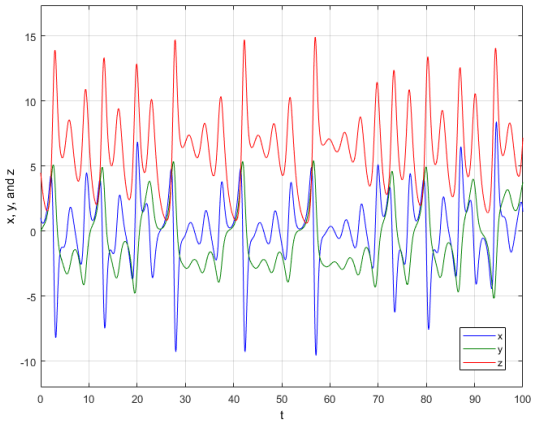
2.2.9. Rucklidge kaotik sistemi

Rucklidge tarafından 1992 yılında sunulan sistem aşağıda verilmiştir (Rucklidge, 1992).

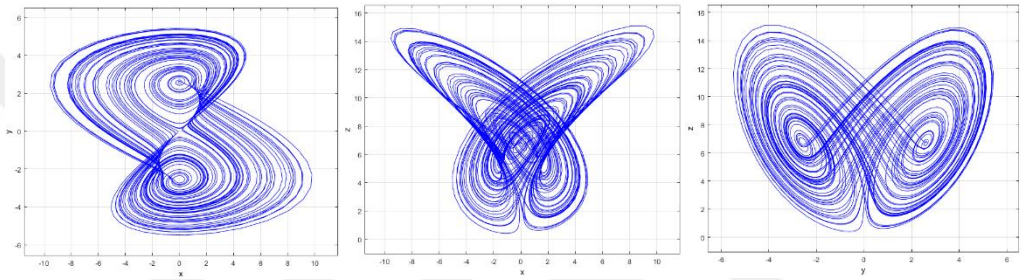
Sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= Kx + Ly - yz \\ \dot{y} &= x \\ \dot{z} &= -z + y^2 \end{aligned} \tag{2.23}$$

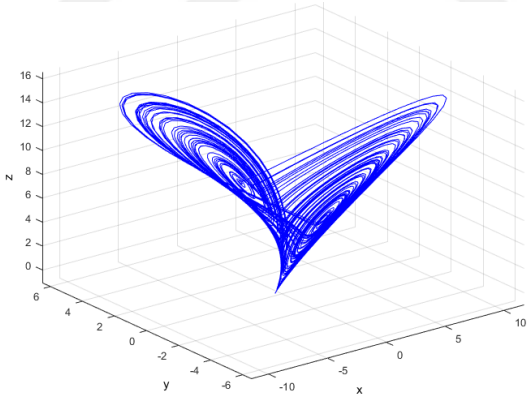
Burada $K = 2$, $L = 6{,}7$ parametreleri, $x_0 = 1, y_0 = 0$ ve $z_0 = 4{,}5$ başalngıç şartları için elde edilen durum değişkenlerini zaman grafiği Şekil 2.36.'da faz portreleri ise Şekil 2.37 ve 2.38'de görülmektedir.



Şekil 2.36. Rucklidge Sistemi x,y,z zaman grafiği



Şekil 2.37. Rucklidge Sistemi 2 boyutlu faz portreleri



Şekil 2.38. Rucklidge Sistemi 3 boyutlu faz portresi

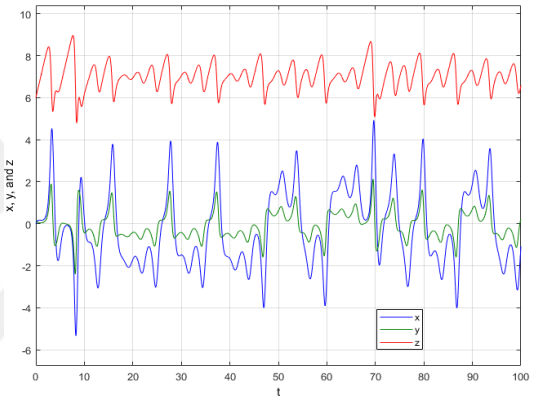
2.2.10. Rikitake kaotik sistemi

Dünyanın jeomanyetik alanınlarının düzensiz polarite anahtarlamasını açıklamaya çalışan bir modeldir bu sistem (Rikitake, 1958; Ito, 1980; Pehlivan ve Uyaroglu, 2007).

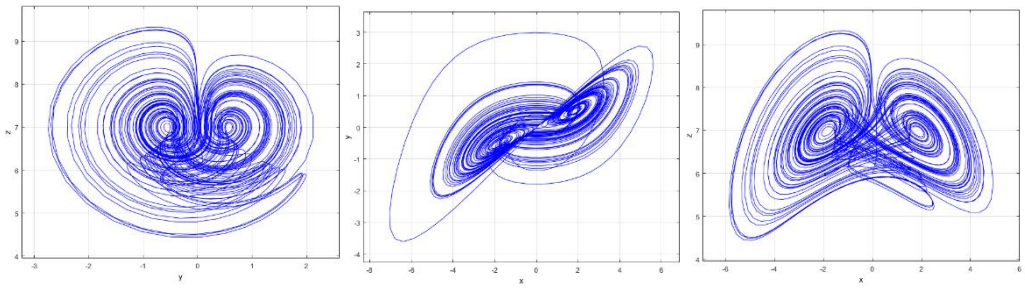
Sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= -\mu x + zy \\ \dot{y} &= -\mu x + (z - a)x \\ \dot{z} &= 1 - xy \end{aligned} \tag{2.24}$$

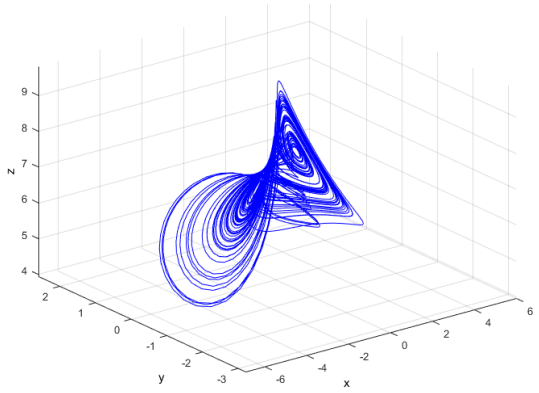
Burada $\mu = 2$, $a = 5$ parametreleri, $x_0 = 0, y_0 = 0{,}1$ ve $z_0 = 0$ başlangıç koşulları için elde edilen durum değişkenleri zaman grafiği Şekil 2.39.'da faz portreleri ise Şekil 2.40 ve 2.41'de görülmektedir.



Şekil 2.39. Rikitake Sistemi x,y,z zaman grafiği



Şekil 2.40. Rikitake Sistemi 2 boyutlu faz portreleri



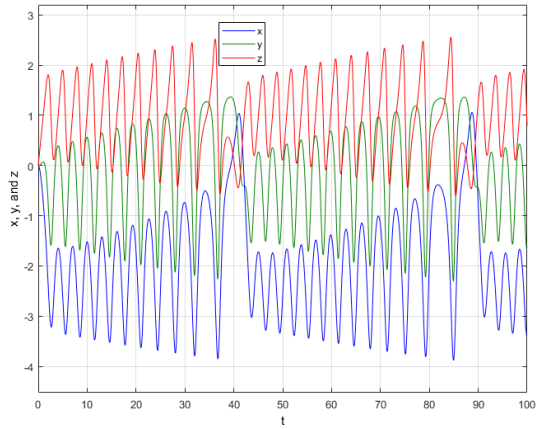
Şekil 2.41. Rikitake Sistemi 3 boyutlu faz portresi

2.2.11. Altın oran dengeli kaotik sistem

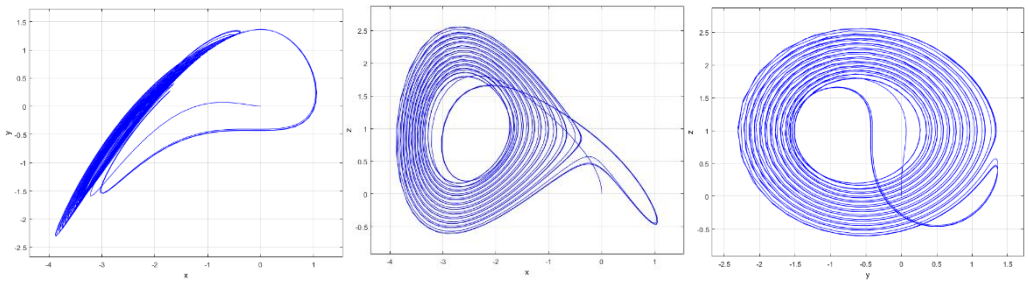
Pehlivan ve Uyaroğlu tarafından 2012 yılında altın oran dengesi ile yeni bir 3 boyutlu kaotik sistem tanıtılmıştır (Pehlivan ve Uyaroğlu, 2012). Bu sistemin dinamik denklemleri;

$$\begin{aligned} \dot{x} &= y - x - az \\ \dot{y} &= xz - x \\ \dot{z} &= -xy - y + b \end{aligned} \tag{2.25}$$

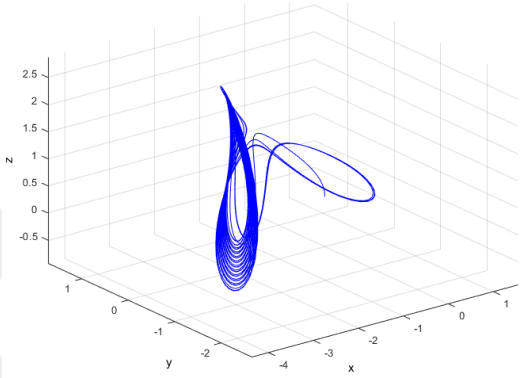
Burada $a = 2$, $b = 1$ parametreleri, $x_0 = 0$, $y_0 = 0$ ve $z_0 = 0$ başlangıç şartları için elde edilen durum değişkenleri zaman grafiği Şekil 2.42.'de faz portreleri ise Şekil 2.43 ve 2.44'de görülmektedir.



Şekil 2.42. Altın oran dengeli sistemin x,y,z zaman grafiği



Şekil 2.43. Altın oran dengeli sistemin 2 boyutlu faz portreleri

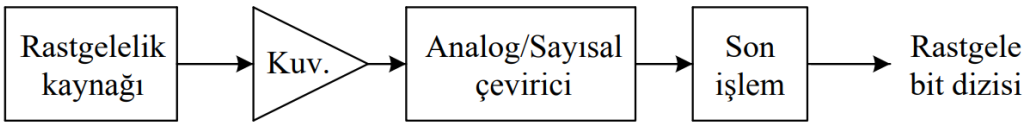


Şekil 2.44. Altın oran dengeli sistemin 3 boyutlu faz portresi

BÖLÜM 3. RASGELE SAYI ÜRETEÇLERİ (RSÜ) VE TEMEL KAVRAMLAR

Rasgele kelimesi; gelişi güzel, düzensiz, nedeni olmayan, öngörülemeyen, tesadüf gibi anlamlara sahiptir. Bir dizi tesadüfi olayın art arda gelmesi rasgele süreçleri oluşturduğu bilinir. Bu durum bilimsel olarak ifade edilmek istenirse, rasgele bir süreçten elde edilen çıktılar arasında determinist ve matematiksel olarak ifade edilebilen, bir irtibat bulunmaz (Viniotis, 1998). Rasgele sayılar ise belirli bir aralık için tanımlanmış, bu aralıkta oluşma olasılıkları eşit ve oluşan rasgele sayılar arasında belirlenebilen bir ilişki olmayan sayılardır.

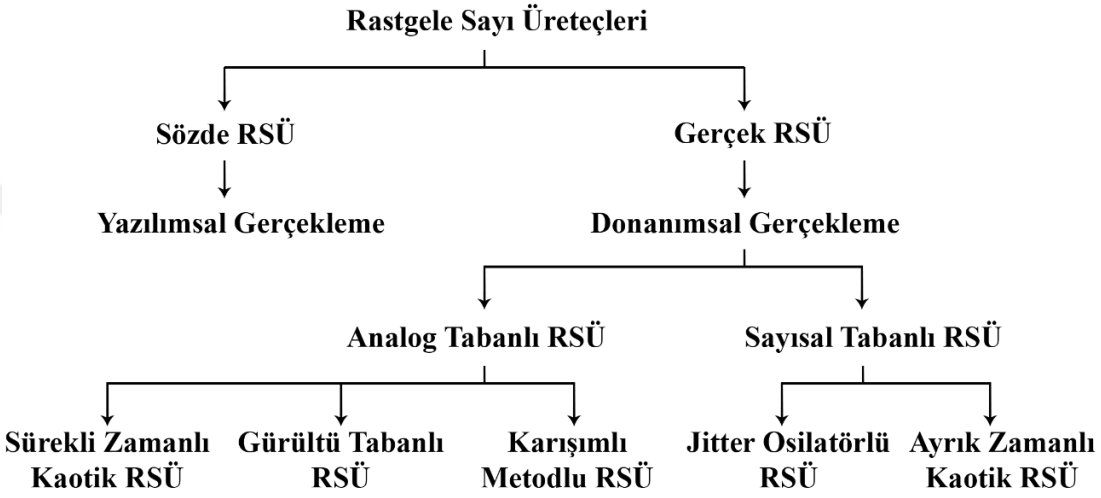
Günümüzde rasgele veriler kullanılarak belirli programlar ve bilgisayar aracılığıyla görüntü, desen ve 3 boyutlu cisimler oluşturulur; içeriği sadece alıcının ve vericinin bilmesi gereken güvenli haberleşme uygulamalarında veya sadece kullanıcı tarafından bilinmesi istenen veri gizleme uygulamalarında rasgele sayılar kullanılır (Daemen ve Rijmen, 2002). İstatistikte örneklerin rasgele seçilmesinde (Robinson ve Dessart, 1998), elektronik tasarım benzetim ortamları oluşturulmasında (Schoukens ve ark., 1988) ve tasarımların test edilmesinde (Rene, 1988), dijital oyunlarda ve bunlara benzer birçok alanda rasgele sayılar kullanılmaktadır.



Şekil 3.1. Rasgele sayı üreteci genel yapısı

Rasgele sayı üreteçleri, gerçek rasgele sayı üreteçleri (True RNG) ve sözde rasgele sayı üreteçleri (Pseudo RNG) olmak üzere ikiye ayrılır. Gerçek rasgele sayı üreteçleri (GRSÜ) rasgele olduğu bilinen fiziksel bir duruma dayanmaktadır. Genellikle gürültü üreten kaynaklar veya doğada hazır bulunan gürültülü kaynaklar bunlara örnek

verilebilir. Başka bir deyişle gerçek RSÜ tam olarak aynı koşullarda iki kere çalıştırılırsa bile birbiriyle ilişkisiz iki rasgele sayı dizisi üretir. Sözde rasgele sayı üreteçleri (SRSÜ), önceden tahmin edilebilen denklemlere dayanan ve bünyesinde rasgele veri bulunduran, sınırlı durumda ve rasgele veri üretimini kendi işlemcisinde hesaplayan sayı üreteçleridir. SRSÜ'nde aynı başlangıç şartlarıyla aynı veri dizisi üretilir (Toyran, 2007).



Şekil 3.2. RSÜ çeşitleri

Sözde rasgele sayı üreteçleri matematiksel formül, algoritma veya önceden tanımlanmış kurallar kullanarak rassal veri dizileri oluşturan üreteçlerdir. Sözde rasgele sayı üreteçleri herhangi bir başlangıç anahtarı ile çalışırlar. Sözde rasgele sayı üreteçlerinin bazı avantajları vardır. Bunlar; diğer yöntemlere göre daha ucuz olması, kolay gerçekleştirilebilir olması, hızlı olması ve donanım ihtiyacına gerek duymamasıdır. Ancak sözde rasgele sayı üreteçlerinde üretilen sayılar başlangıç anahtarı bilindiğinde veya sistemdeki formülasyonlar yeterince karmaşık olmadığı taktirde tahmin edilebilir (Avaroğlu ve Türk, 2013; Sobotka ve Zeman, 2011)

SRSÜ'lere bir örnek olarak lineer eşlenik metodu LEM (LCG) gösterilebilir.

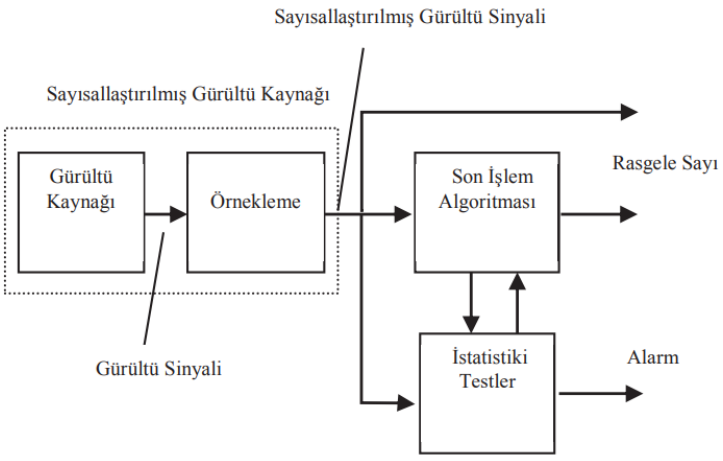
$$X_{n+1} = (aX_n + c) mod\ m \tag{3.1}$$

Burada $m > 0$ şartı, $0 \leq a < m$ şartı ve $0 \leq X_0 < m$ durumlarında rasgele sayı dizisi elde edilir.

$a = 5, c = 1, m = 7\ X_0 = 2$ için sonuç aşağıdaki şekilde olur.
$X = [2, 3, 0, 1, 6, 7, 4, 5, 2, 3, 0, 1, \ldots\ldots]$

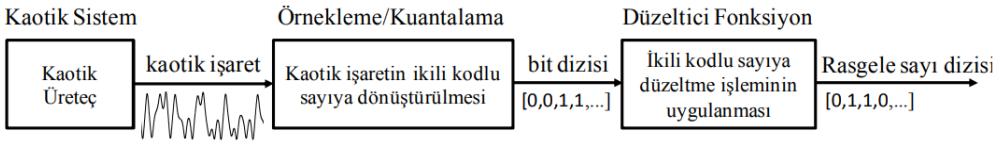
Sözde rasgele sayı üreteçleri genellikle kısa sürede yüksek verimde uzun boyutlu rasgele sayı üretimine ve aynı başlangıç değerlerine ihtiyaç duyulduğunda kullanılmaktadır (Kocarev ve Jakimoski, 2003).

Gerçek rasgele sayı üreteçlerinin genel tasarımı Şekil 3.2'de verilmiştir. GRSÜ tasarımında, gürültü kaynaklarının doğrudan yükseltilmesi ve örneklenmesi, osilatör örnekleme yöntemi ve kaotik sistemler gibi yöntemler kullanılmaktadır (Petrie ve Connelly, 2000). Gürültü kaynaklarının doğrudan yükseltilmesi ve örneklenmesi tabanlı GRSÜ gerçeklemelerinin çeşitli olumsuz yönleri bulunmaktadır. Kullanılan gürültü kaynaklarının ürettiği işaretlerin oldukça düşük güçlü olmaları ve bu nedenle sistemdeki istenmeyen işaretlerden etkilenmeleri ve ayrıca gürültü tabanlı GRSÜ'lerinde gürültü sinyalinin kuvvetlendirilmesi için kullanılacak olan kuvvetlendiricilerin kazancındaki bant sınırlaması sebebiyle, kuvvetlendirici çıkışında gürültü bandının da sınırlı olması, bu olumsuzluklara örnek olarak verilebilir (Özoğuz ve Zeki, 2008).



Şekil 3.3. GRSÜ genel tasarımı

GRSÜ devrelerinin gerçeklemesinde gürültü kaynağı yerine kaotik sistem yapıları da kullanılabilmektedir. Şekil 3.4'te kaos tabanlı RSÜ blok şeması görülmektedir. Bu yapılarda kullanılan kaotik tabanlı üreteçler başlangıç koşullarına ve sistem parametrelerine oldukça hassas bağımlı olup, bu sistemlerin çözümlerinin uzun zaman aralıkları için öngörülmesi mümkün olmamaktadır. Bunun yanında, kaotik işaretlerin periyodik olmamaları nedeniyle, frekans yayılımları geniş ve sürekli olmaktadır (Özoğuz ve Zeki, 2008). Kaotik sistemlerin yukarıda ifade edilen önemli özellikleri sayesinde yüksek bit üretim hızına sahip GRSÜ uygulamalarında kullanılabilirler. Kaotik sistemler, dinamik sistemler olduklarından, osilatör çıkışları zamana göre değişim göstermektedir. Ayrıca bu sistemler, değişken ve periyodik olmayan yapılar olduklarından kendilerini tekrarlamazlar.



Şekil 3.4. Kaotik rasgele sayı üreteci genel tasarımı

3.1. İstatistiksel Rasgelelik Testleri

Rasgele sayı üreteçlerinin ana amacı çıktılarının tahmin edilemez olmasıdır. Yani üretilen veri dizisinden ileride üreteceği veya eski ürettiği verinin tahmin edilememesidir. Bu da mutlaka üretilen veriler arasında bir ilişkininin kurulamamasına bağlıdır. Bundan dolayı rassal olduğu söylenen bir veri dizisinin rassallığı rasgelelik testleri kullanılarak belirlenir. Rassal sayılar belirli bir küme içinde tanımlanmıştır ve bu küme içinde oluşabilme ihtimalleri eşit olmalıdır. Ayrıca bu veri kümesi içinde bulunan rassal sayılar arasında bulunabilen bir ilişki olmamalıdır. Ayrıca rasgele sayı üretecinde üretilen her verinin test edilmesinin zor olmasından dolayı belirli bir verinin istatistiksel anlamlılığına bakılarak RSÜ'nün niteliği üzerine değerlendirme yapılır.

Rasgele sayı üreteçlerinden üretilen bitlerin rasgelelilik derecesini ölçen çeşitli testler vardır. Rasgelelik testleri için en çok kullanılan ve geçerli olan testler FIPS (Federal Information Processing Standards – Federal Bilgi İşleme Standardı) tarafından

belirlenen FIPS 140-1 ve NIST tarafından belirlenen NIST 800-22 testleridir (Demirkol, 2017; Tavas, 2011; Erat, 2008; Yıldırım, 2012).

3.1.1. FIPS-140-1 testi

Rasgele sayı üretecinden elde edilen bilgilerin rasgelelik kalitesini belirlemede kullanılan bir testtir. Veri blok uzunluğu küçük olan veriler için kullanılır. Bu test için rasgele sayı üreteçlerinden oluşturulan 20.000 adet bitlik bir rasgele dizisi monobit, poker, runs ve long runs testi olmak üzere dört adet teste tabi tutulur. Bu testlerden herhangi birinden geçilemediği takdirde rasgele sayı üreteci başarısız kabul edilir (Demirkol, 2017; Erat, 2008; Yıldırım, 2012; Ateş, 2005; Bayram, 2005)

3.1.1.1. Monobit testi

20.000 bitlik rasgele sayı dizisindeki 1'lerin sayısının 9654 ile 10346 arasında olması gerekmektedir (Demirkol, 2017; Erat, 2008; Yıldırım, 2012; Ateş, 2005; Bayram, 2005).

3.1.1.2. Poker testi

Bu test de 20.000 adet bitlik veri (20 Kbit) 4 bitlik olarak 5.000 parçaya bölünür. Bu parçalarda 4 bitin 16 olası durumu sayılır ve kaydedilir. Denklem 3.2'de verilen formül ile X değeri hesaplanır. Denklemde $f(i)$ ifadesi, 16 olası durum değerindeki (i) sayılan sayı değerini ifade eder. Denklem 3.2 ile hesaplanan X değeri $1{,}03 < X \leq 57{,}4$ aralığında ise test başarılı sayılır (Demirkol, 2017; Erat, 2008; Yıldırım, 2012; Ateş, 2005; Bayram, 2005).

$$X = \left(\frac{16}{5000}\right)\left(\sum_{i=0}^{15}[f(i)]^2\right) - 5000 \tag{3.2}$$

3.1.1.3. Runs testi

Üretilen bit dizisinde art arda gelen "1" veya "0" bitlerinden oluşan blokların sayısının Tablo 3.1.'de verilen değer aralıklarında olup olmadığı test edilir. Bu testin amacı "0" ve "1" bitleri arasındaki salınımın çok hızlı veya çok yavaş olup olmadığının belirlenmesidir (Demirkol, 2017; Erat, 2008; Yıldırım, 2012; Ateş, 2005; Bayram, 2005).

Tablo 3.1. Koşu (Runs) testi kriterleri

Blok Uzunluğu	Blok Sayısı Aralığı
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
6+	90-223

3.1.1.4. Long Runs testi

Run testi ile aynıdır. Fakat bu uzun koşu testinin başarılı olabilmesi için üretilen 20000 bitlik bir veri içindeki "1" veya "0" lardan oluşan tüm blokların sayısı 34'ten küçük olmalıdır (Demirkol, 2017; Erat, 2008; Yıldırım, 2012; Ateş, 2005; Bayram, 2005).

3.1.2. NIST-800-22 testi

National Institute of Standarts and Technology (NIST) tarafından geliştirilen NIST 800-22 testi üretilen rasgele sayıların rasgelelik derecesini ölçen bir testtir. NIST 800-

22 testi ile rasgele sayıların testinin yapılabilmesi için en az 1000000 (1 milyon) adet veri önerilmektedir. NIST 800-22 testi kendi içinde 15 ayrı test içerir. NIST 800-22 testi her alt testte bir p değeri (probability) hesaplar. Testlerin başarılı kabul edilmesi için bu p değerinin $0{,}01$'den büyük olması gerekir (Çiçek, 2016; Demirkol, 2017; Avaroğlu, 2014; Rukhin, 2010). Her bir test n boyutlu aynı bit verisine uygulanır ve her test sonucunun p değeri hesaplanır. Teste tabi tutulan verinin başarılı olduğu söylenebilmesi için tüm testlerin başarıyla sonuçlanması gerekmektedir. Sıfır ortalamalı dizilerle çalışmanın kolaylığından dolayı testler $\varepsilon_i = \{0, 1\}$ bit kümesi yerine $X_i = 2\varepsilon_i - 1$ dönüşümüyle $X_i = \{-1, 1\}$ kümesi ile çalışılır (Tavas, 2011).

NIST-800-22 ile FIPS-140-1 testlerine göre hem test sayısı açısından daha fazla test içermekte hem de bit dizileri daha güçlü bir şekilde testlere tabi tutulmaktadır (Koyuncu, 2014).

3.1.2.1. Frekans testi (Frequency monobit test)

Rasgele veri dizisindeki "1" ve "0" bit sayıları takriben aynı olması gerekmektedir. Bu test üretilen bit dizisi içindeki "1" ve "0" bitlerinin sayısının oranını inceler (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.2. Blok frekans testi (Frequency test within a block)

Bu test üretilen bit dizisi içinden seçilen herhangi bir m bitlik bir blok içindeki "1" ve "0" bitlerinin sayısının oranını inceler (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016). Rasgele üretilen m bitlik bloklardaki '1' oranının $m/2$ olması beklenmektedir.

3.1.2.3. Yinelemeler (akış) testi (Runs test)

Bu test üretilen bit dizisi içindeki art arda gelen "1" ve "0" bloklarının sayısını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.4. Blok içinde en uzun bir yinelemesi testi (Tests for the longest-run-ofones in a block test)

Bu test üretilen bit dizisi içindeki art arda gelen en uzun "1" sayısını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016). Test edilecek n bitlik dizi m adet bloğa bölünmekte ve her bir blok içerisindeki en uzun ardışık birlerin akışına bakılmaktadır.

3.1.2.5. İkili matris rankı testi (Binary matrix rank test)

Bu test ile sabit uzunluğa sahip veri blokları kullanılarak, her biri bir satırı belirterek bir matris oluşturulur ve bu matrisin derecesi hesaplanarak bloklar arasındaki doğrusal bağımlılığın olup olmadığı incelenmektedir. (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.6. Ayrık Fourier dönüşümü testi (Discrete Fourier transform test)

Bu test ile üretilen bit dizisinin ayrık Fourier dönüşümü alınarak dizinin periyodikliği incelenir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.7. Örtüşmeyen şablon eşleştirme testi (Non-overlapping template matching test)

Bu testte, rasgele sayı üretecinin ürettiği n bitlik dizideki m bitlik blokların içerisinde, periyodik olmayan önceden belirlenmiş örnek dizinin bulunma sıklığının tespit edilmesi ve incelenmesi amaçlanmaktadır. Seçilen özel blokların tekrar edilmesi durumunda, gözlemlenen bloktan sonraki ilk bitten aramaya devam edilmektedir. Eğer belirlenen m bitlik özel bloklar bulunmaz ise pencere bir bit kaydırılarak arama işlemine devam edilir. Bu test üretilen bit dizisinin içindeki m bitlik bir bloğun dizi içindeki tekrarını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.8. Örtüşen şablon eşleştirme testi (Overlapping template matching test)

Örtüşmeyen şablon eşleştirme testi ile aynıdır. Farkı, eğer bir örüntü (dizi tekrarı) bulunursa pencere bulunan örüntüden sonraki ilk bit yerine sadece o an bulunan pozisyondan bir sonraki bite yeniden konumlanır ve taramaya devam edilir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.9. Maurer'in "evrensel istatistik" testi (Maurer's "universal statistical" test)

Bu test üretilen bit dizisinin veri kaybı olmadan ne kadar sıkıştırılabileceğini inceler (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.10. Doğrusal karmaşıklık testi (Linear complexity test)

Bu test üretilen bit dizisinin karmaşıklığını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.11. Seri testi (Serial test)

Bu test, üretilen bit dizisi içindeki tekrarlanan m bitlik 2^m adet bloğun tekrar sayısının dağılımını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.12. Yaklaşık entropi testi (Approximate entropy test)

Bu test üretilen bit dizisi içindeki iki ardışık bloğun $(m\ ve\ m+1)$ frekansını (entropisini) inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016). Bu testte amaç, seri testinde olduğu gibi tüm muhtemel örtüşen m bitlik örnek dizinin frekansının incelenmesidir. Test, rasgele bir dizi için beklenen frekansın, iki ardışık veya bitişik uzunluktaki örtüşen blokların sıklığını karşılaştırmaktadır.

3.1.2.13. Kümülatif (birikimli) toplamlar testi (Cumulative sums test)

Bu test üretilen bit dizisini ardışık bloklara ayırır ve bu bloklar içindeki "1" ve "0" bitlerinin sayısının oranını (dengesini) belirleyip, bloklar arasındaki bu oranların dengesizliği inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.14. Rasgele gezinimler testi (Random excursions test)

Bu test üretilen bit dizisini ardışık bloklara ayırır ve bu bloklar içindeki "1" ve "0" bitlerinin sayısının oranını (dengesini) belirleyip, bloklar arasındaki bu oranların dengesinin dağılımını inceleyen bir testtir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.2.15. Rasgele gezinimler değişken testi (Random excursions variant test)

Bu test ile üretilen bit dizisi ardışık bloklara ayrılır ve bu bloklar içindeki “1” ve “0” bitlerinin sayısının oranı (dengesi) belirlenip ortalama değerden sapma miktarı belirlenir (Demirkol, 2017; Rukhin, 2010; Erat, 2008; Çiçek, 2016).

3.1.3. ENT testi

ENT testi sözde-rasgele sayı üreteci uygulamaları tarafından üretilen bayt dizilerine çeşitli testler uygulayan John Walker tarafından geliştirilen bir test uygulamasıdır (Walker, 2008). Bu program, dosyalarda saklanan bayt dizilerine çeşitli testler uygular ve bu testlerin sonuçlarını rapor eder. Program, şifreleme ve istatistiksel örnekleme uygulamaları, sıkıştırma algoritmaları ve bir dosyanın bilgi yoğunluğunun ilgilenildiği uygulamaların değerlendirilmesi için kullanışlıdır. Belirlenmiş bir RSÜ algoritması için, bu sınıf aşağıdaki endeksleri hesaplar.

3.1.3.1. Ki-kare testi

Ki-kare testi, verilerin rasgeleliği için en yaygın kullanılan testtir ve sözde-rasgele sayı üreteçlerindeki hatalara son derece duyarlıdır. Ki-kare dağılımı, dosyadaki baytların akışı için hesaplanır ve mutlak bir sayı olarak ifade edilir ve gerçekten rasgele bir dizinin, hesaplanan değerin ne sıklıkta geçeceğini gösterir. Yüzde %99'dan büyük veya %1'den az ise, dizi neredeyse rasgele değildir. %99 ile %95 arasında veya %1 ile %5 arasında ise, dizi şüphelidir. %90 ile %95 ve %5 ile %10 arasındaki oranlar dizinin neredeyse şüpheli olduğunu gösterir (Knuth, 1998).

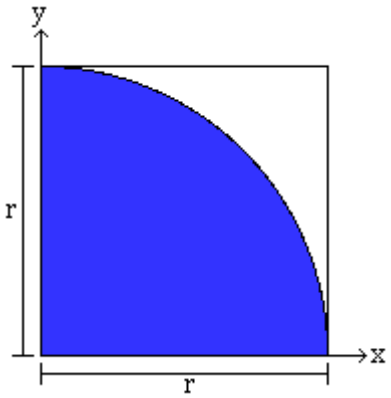
3.1.3.2. Aritmetik ortalama

Bu en basit tabirle dosyadaki tüm (set) bitlerin toplamının dosya uzunluğuna bölünmesi ile bulunur. Veri rasgele ise, bu yaklaşık 0,5 olmalıdır. Bu yanıyla frekans testi mantığıyla aynıdır.

3.1.3.3. Pi için monte carlo değeri

Monte Carlo Metodu, genel olarak istatistiksel simülasyonların yapılması için rasgele sayılardan faydalanılan bir metot olarak tanımlayabiliriz. Bu metot Los Alamos Ulusal Laboratuvarı'ndan Nick Metropolis, Stan Ulam ve John Von Neumann adlarında üç bilim insanı tarafından literatüre sunulmuştur (Metropolis, 1985). Günümüzde bu metot, hücre simülasyonu, borsa modelleri, dağılım fonksiyonları, atom ve molekül fiziği, nükleer fizik modellerini test eden simülasyonlarının hesaplanmalarında kullanılır (Hançerlioğullari, 2006).

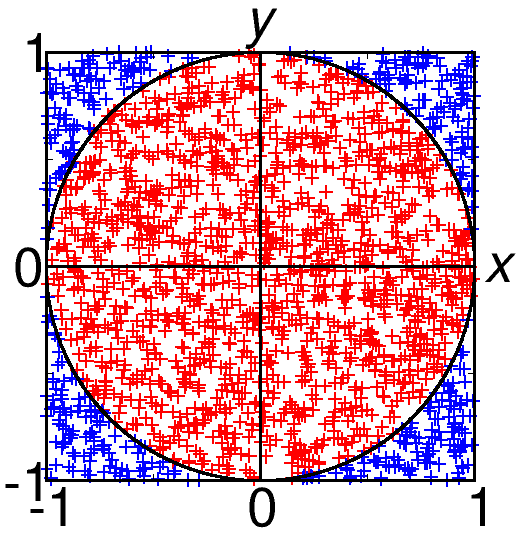
Aşağıda verilen Şekil 3.5'deki gibi bir karenin içine yerleştirilen çeyrek dairenin alanın karenin alanına oranı $\left(\frac{1}{4}\right)\pi$ olacaktır. Kör bir dart oyuncusunun Şekil 3.5'deki gibi bir dart tahtasına atış yaptığını düşünün. Kare içindeki dartların toplam sayısı ile mavi ile taralı olarak gösterilen alana (dairenin dörtte biri) denk gelen dartların sayısının oranı da $\left(\frac{1}{4}\right)\pi$ olmalıdır.



Şekil 3.5. Bir kare içinde çeyrek daire

$$\left(\frac{çember\ içinde\ olma\ olasılığı}{karenin\ içinde\ olma\ olasılığı}\right) = \frac{\pi r^2}{(2r)^2} = \frac{\pi}{4} \tag{3.3}$$

Bu bilgiden yararlanarak üretilen rasgele sayı dizisi test edilebilir. Ardışık her veri, bir kare içinde x ve y koordinatları olarak kullanılır. Rasgele oluşturulmuş noktanın karesi, karenin içine yazılan bir dairenin yarıçapından daha azsa, altı bayt dizisi "vur" olarak kabul edilir. İsabetlerin yüzdesi π'nin değerini vermelidir.



Şekil 3.6. Rasgele koordinatların dağılımı

3.1.3.4. Seri korelasyon katsayısı

Bu miktar, dosyadaki her baytın önceki baytla ne ölçüde bağlı olduğunu ölçer. Rasgele sekanslar için, bu değer (pozitif veya negatif olabilir) sıfıra yakın olmalıdır (Knuth, 1998).

3.1.4. Diehard testleri

Florida'daki Eyalet Üniversitesinde çalışma yapan bilim insanı George Marsaglia tarafından geliştirilen Diehard testleri, rasgele sayı üretecinin kalitesini ölçen aşağıda adları verilen istatistiksel testler bütünüdür (Marsaglia, 2018). Diehard testleri istatistiksel, matematiksel ve çelişkili temellere dayanmaktadır (Tavas, 2011). Diehard test takımı, her biri $[0,1]$ aralığında bir p değeri üreten birkaç istatistiksel testten oluşmaktadır. Bir p değeri 0.01'den düşük veya 0.99'un üzerinde ise, jeneratör testten geçmemiş sayılır (Teh ve ark., 2015).

1. Doğum günü boşlukları testi
2. Çakışan permütasyonlar
3. Matrisler sırası
4. Maymun testleri
5. 1'lerin sayısı
6. Park yeri testi
7. Minimum mesafe testi
8. Rasgele küreler testi Sıkma testi
9. Sıkma testi
10. Çakışan toplamlar testi
11. Koşu testi
12. Craps testi

3.1.5. PractRand

PractRand (Practically Random - Pratik olarak Rasgele), sözde rasgele sayı üreteçleri (PRNG'ler veya sadece RNG'ler) için bir C++ istatistiksel test kütüphanesidir. Diehard geleneğinde standart bir test bataryası içerir. Testler özelleştirilmiş şekillerde çağrılabilir. Test için maksimum dizi uzunluğu sınırlaması yoktur.

Bazı istatistiksel test programları ve karşılaştırmaları aşağıdaki tabloda verilmiştir. Tablo verileri http://pracrand.sourceforge.net/Tests_overview.txt sitesinden alınmıştır.

Tablo 3.2. Bazı istatistiksel rasgele test programları karşılaştırmaları

TESTLER	**Kalite**	**Sunum[1]**	**Açık Kaynak**	**Okuyuculu**
Gjrand http://gjrand.sourceforge.net/	Çok İyi	Uygun	Viral (GPL[2])	Evet
TestU01 http://www.iro.umontreal.ca/~simardr/testu01/tu01.html	İyi	Uygun	Ticari olmayan	Hayır
RaBiGeTe http://cristianopi.altervista.org/RaBiGeTe_MT/	Düşük	Aşırı Karmaşık	Kapalı kaynak	Evet
Dieharder http://www.phy.duke.edu/~rgb/General/dieharder.php	Kötü	Uygun	Viral (GPL)	Evet
NIST STS http://csrc.nist.gov/groups/ST/toolkit/rng/index.html	Standart	Uygun	Kamu	Evet
Diehard http://www.stat.fsu.edu/pub/diehard/	Kötü	Kötü	Kamu	Hayır
ENT http://www.fourmilab.ch/random/	Kötü	Uygun değil	Kamu	Hayır

[1]Sunum, test sonuçlarını anlaşılması kolay ve faydalı olan şekillerde göstermek anlamına gelir.
[2]GPL Copyleft lisansları, GNU Genel Kamu Lisansı

BÖLÜM 4. TASARLANAN KRSÜ'DE KULLANILAN AYRIK ÇÖZÜM METOTLARI VE SON İŞLEM YÖNTEMLERİ

Bu çalışmada rasgele sayı üreteci kaynağı olarak seçilen kaotik sistemler, bu sistemlerin sayısal çözümleri ve çıkışlarında kullanılan farklı son işlem metotları birlikte sunuldu. Geliştirilen arayüz tasarımı ile seçilen kaotik kaynağın ürettiği sinyaller yine arayüzden seçilecek 3 farklı son işlem yöntemi kullanılarak elde edildi. Burada kaotik sistem çözüm algoritmaları kesir dereceli türevler ve kullanılan son işlem yöntemleri bu başlık altında açıklanacaktır.

4.1. Sayısal Çözüm Algoritmaları

Kaotik sistemler ve bu çalışmada kullanılan kaotik sistemler diferansiyel denklemler ile tanımlanmaktadır. Bu kaotik sistemlerin tanımlandığı diferansiyel denklemlerin sayısal tabanlı olarak modellenebilmesi için sayısal analiz yöntemleri kullanılmaktadır. Literatürde bu amaçla çeşitli yöntemler geliştirilmiştir. Bu yöntemlere Euler, Heun, 4. ve 5. dereceden Runge Kutta (RK4 ve RK5) ve Dormand-Prince gibi yöntemler örnek olarak verilebilir.

Matematik ve hesaplama biliminde, Euler yöntemi, belirli bir başlangıç değerine sahip olağan diferansiyel denklemlerin (ODE) çözülmesi için geliştirilen en basit sayısal yöntemlerden biridir. Euler metodu, ismini Leonhard Euler'in yayınladığı (1768–1870) Institutionum Calculi İntegralis'den almıştır (Butcher, 2016; Euler, 1769). Denklem 4.1 ve Denklem 4.2'de euler yöntemi verilmiştir.

$$y'(t) = f\big(t, y(t)\big), \qquad y(t_0) = y_0 \tag{4.1}$$

h adım aralığı olmak üzere $t_n = t_0 + nh$ ve

$$y_{n+1} = y_n + hf(t_n, y_n) \tag{4.2}$$

Heun Metoduna ise Euler metodundaki i'inci noktadaki türev yerine i ve $(i + 1)$'inci noktadaki türevlerin aritmetik ortalaması alınır.

$$y'(t) = f\big(t, y(t)\big), \qquad y(t_0) = y_0 \tag{4.3}$$

$$\bar{y}_{i+1} = y_i + hf(t_i, y_i) \tag{4.4}$$

$$y_{i+1} = y_i + h\frac{f\big(t_i, y_i\big) + f\big(t_{i+1}, \bar{y}_{i+1}\big)}{2} \tag{4.5}$$

Burada h adım aralığı, $t_{i+1} = t_{i,} + h$ olarak verilmiştir.

Literatürde en çok tercih edilen nümerik yöntemlerden birisi de dördüncü dereceden Runge Kutta (RK4) metodudur. Sayısal analizde Runge-Kutta yöntemleri, adi diferansiyel denklemlerin çözüm yaklaşımları için kapalı ve açık yinelemeli yöntemler ailesinin önemli bir tipidir. Bu yöntem 1900'lü yıllarda C. Runge ve M.W. Kutta adlı matematikçiler tarafından geliştirilmiştir. Bu çalışmada geliştirilen numerik çözüm algoritması olarak da RK4 yöntemi seçilmiştir.

Aşağıdaki gibi tanımlanan (Denklem 4.6) bir başlangıç değer problemini ele alalım.

$$y' = f(t, y), \qquad y(t_0) = y_0 \tag{4.6}$$

ve bu problem için RK4 yöntemi aşağıdaki denklemlerle verilir.

$$y_{n+1} = y_n + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4) \tag{4.7}$$

Burada

$$k_1 = hf(t_n, y_n) \tag{4.8}$$

$$k_2 = hf\left(t_n + \frac{h}{2}, y_n + \frac{k_1}{2}\right) \tag{4.9}$$

$$k_3 = hf\left(t_n + \frac{h}{2}, y_n + \frac{k_2}{2}\right) \tag{4.10}$$

$$k_4 = hf(t_n + h, y_n + k_3) \tag{4.11}$$

Böylece bir sonraki y_{n+1} değeri o anki y_n değerine h aralığının büyüklüğüyle tahmini eğimin çarpımının eklenmesiyle elde edilir. Bu eğim, eğimlerin ağırlıklı ortalamasıdır:

- k_1 aralığın başlangıcındaki eğimdir.
- k_2 aralığın orta noktasındaki eğimdir. Bu k_2 eğimi, Euler yöntemi kullanılarak y'nin $t_n + h/2$ noktasındaki değerinden elde edilir.
- k_3 yine orta noktadaki eğimdir. Ama bu sefer *y* değeri k_2 eğiminden elde edilir.
- k_4 aralığın sonundaki eğimdir ve *y* değeri k_3 eğimi kullanılarak bulunur.

Yapılan çalışmada numerik çözüm algoritması olarak RK4 yöntemi kullanılmıştır. Aşağıda kaotik bir sistemin RK4 yöntemiyle çözümü için bir örnek verilmiştir.

$$\begin{aligned} \dot{x} &= f(t,x,y,z), \qquad \dot{x} = a(y-x) \\ \dot{y} &= g(t,x,y,z), \qquad \dot{y} = rx - y - xz \\ \dot{z} &= \delta(t,x,y,z), \qquad \dot{y} = xy - bz \end{aligned} \tag{4.12}$$

Yukarıdaki denklemlerle tanımlı Lorenz kaotik sisteminin RK4 yöntemiyle çözülmesi için k, λ ve σ değerleri aşağıdaki gibi hesaplanır.

$$k_1 = f\big(x(k), y(k), z(k)\big)$$
$$\lambda_1 = g(x(k), y(k), z(k)) \tag{4.13}$$
$$\sigma_1 = \delta(x(k), y(k), z(k))$$

$$k_2 = f\left(x(k) + \frac{1}{2}hk_1, y(k) + \frac{1}{2}h\lambda_1, z(k) + \frac{1}{2}h\sigma_1\right)$$
$$\lambda_2 = g\left(x(k) + \frac{1}{2}hk_1, y(k) + \frac{1}{2}h\lambda_1, z(k) + \frac{1}{2}h\sigma_1\right) \tag{4.14}$$
$$\sigma_2 = \delta\left(x(k) + \frac{1}{2}hk_1, y(k) + \frac{1}{2}h\lambda_1, z(k) + \frac{1}{2}h\sigma_1\right)$$

$$k_3 = f\left(x(k) + \frac{1}{2}hk_2, y(k) + \frac{1}{2}h\lambda_2, z(k) + \frac{1}{2}h\sigma_2\right)$$
$$\lambda_3 = g\left(x(k) + \frac{1}{2}hk_2, y(k) + \frac{1}{2}h\lambda_2, z(k) + \frac{1}{2}h\sigma_2\right) \tag{4.15}$$
$$\sigma_3 = \delta\left(x(k) + \frac{1}{2}hk_2, y(k) + \frac{1}{2}h\lambda_2, z(k) + \frac{1}{2}h\sigma_2\right)$$

$$k_4 = f(x(k) + hk_3, y(k) + h\lambda_3, z(k) + h\sigma_3)$$
$$\lambda_4 = g(x(k) + hk_3, y(k) + h\lambda_3, z(k) + h\sigma_3) \tag{4.16}$$
$$\sigma_4 = \delta(x(k) + hk_3, y(k) + h\lambda_3, z(k) + h\sigma_3)$$

Hesaplanan bu değerler ve değişkenlerin o anki değerleri kullanılarak o değişkenlerin bir sonraki adımdaki değeri aşağıdaki denklemler yardımıyla hesaplanır.

$$x(k+1) = x(k) + \frac{1}{6}h(k_1 + 2k_2 + 2k_3 + k_4)$$
$$y(k+1) = y(k) + \frac{1}{6}h(\lambda_1 + 2\lambda_2 + 2\lambda_3 + \lambda_4) \tag{4.17}$$
$$z(k+1) = z(k) + \frac{1}{6}h(\sigma_1 + 2\sigma_2 + 2\sigma_3 + \sigma_4)$$

Yapılan çalışmada bu yöntem, fonksiyon ve döngüler kullanılarak Matlab ortamında yazılmış ve arayüz tasarında kullanılmıştır.

4.2. Kesir Dereceli Türevler (Fractional-Order Systems)

Fiziksel sistemlerin matematiksel modelinin oluşturulması ve bu sistemlerdeki değişimleri ifade edebilmek için türev kavramına ihtiyaç duyulur. Bu sistemler çoğu zaman kendisinin hâlihazırdaki durumu ve değişimi ile beraber ifade edilebilir. Bu amaçla ilk çalışmalar Newton, L'Hospital, Abel, Euler, Riemann, vb. tarafından yapılmıştır. Kısaca sistemlerin modelini oluşturan fonksiyonların asimptotik davranışlarını incelemek için bağımsız değişkenlerde meydana gelen en küçük değişikliklere fonksiyonun tepkisini incelemişlerdir (Karcı, 2015).

Türev kavram ve konu olarak yaklaşık 300 yıldır üzerinde çalışılan bir konu olagelmiştir. Newton, L'Hospital ve Leibniz türev kavramı ile ilgilenirken türev işleminde dereceyi 1 olarak almışlardır. 1695'te L'Hospital'in (1643-1704) Leibniz'e (1646-1716) sorduğu *"Bir f fonksiyonun n tamsayılı mertebeden türevini tanımladın peki $n = \frac{1}{2}$ olduğunda $\frac{d^n f}{dx^n}$ kavramının bir anlamı var mı?"* sorusu kesirli analizin başlangıcı olarak kabul edilir. Günümüzde kesirli mertebeli türev, integral ve bunları içeren denklemler fizik, kimya, elektrik ve elektronik, termodinamik, kontrol teorisi gibi pek çok alanda kullanılmaktadır. Konunun çeşitli alanlara uygulanabilme potansiyeli ile son kırk yıldır popülerliği ve önemi artmıştır (Kilbas ve ark., 2006; Mathai ve ark., 2009).

Bu konuda çalışma yapan ünlü bazı matematikçiler: Newton, L'Hospital, Leibniz, Euler, Abel, Caputo, Riemann, Grünwald, Miller, Ross, v.b. olmuştur. Yapılan çok sayıda çalışmadan sonra kesir dereceli türev (fractional-order system) kavramı meydana gelmiştir.

Aşağıdaki $f(x)$ fonksiyonunu ve türev tanımını ele alırsak;

$$H^2 f(x) = Df(x) = \frac{d}{dx} f(x) = f'(x) \tag{4.18}$$

$$f(x) = x^k \tag{4.19}$$

İlk türev genel olarak;

$$f'(x) = \frac{d}{dx} f(x) = kx^{k-1} \tag{4.20}$$

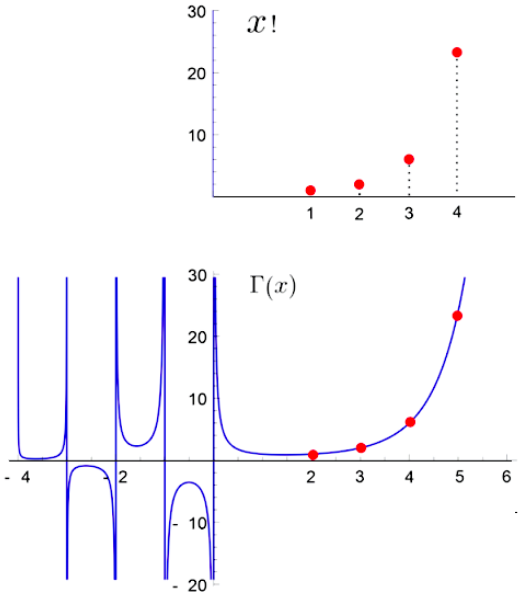
Bu tekrarlama da şu şekilde bir genel sonuç verir.

$$\frac{d^a}{dx^a} x^k = \frac{k!}{(k-a)!} x^{k-a} \tag{4.21}$$

Burada faktöriyel fonksiyonunun karmaşık sayılar ve tam sayı olmayan reel sayılar için aşağıda genellemesi verilen gama fonksiyonu (Γ) kullanılabilir.

$$\begin{aligned} &(n-1)! = \Gamma(n) \\ &\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt \end{aligned} \tag{4.22}$$

Kompleks düzlemde analitik devamlılık için n negatif tam sayı olmamalıdır, pozitif tam sayı olmalıdır.



Şekil 4.1. Reel eksen boyunca gama fonksiyonu

Bu gama fonksiyonu yardımıyla Denklem (4.21) yeniden yazılırsa;

$$\frac{d^a}{dx^a}x^k = \frac{\Gamma(k+1)}{\Gamma(k-a+1)}x^{k-a}, \qquad k \geq 0 \tag{4.23}$$

$k = 1$ ve $a = 1/2$ için;

$$\frac{d^{\frac{1}{2}}}{dx^{\frac{1}{2}}}x = \frac{\Gamma(1+1)}{\Gamma\left(1-\frac{1}{2}+1\right)}x^{1-\frac{1}{2}} = \frac{1!}{\Gamma(\frac{3}{2})}x^{\frac{1}{2}} = \frac{2x^{\frac{1}{2}}}{\sqrt{\pi}} \tag{4.24}$$

olarak x fonksiyonunun yarı türevini elde ederiz.

Yapılan çalışmalar incelendiğinde; kesirli dereceden türevlerle ilgili olarak çok sayıda çalışma yapılmış olduğunu ve çalışmaların günümüzde de yoğun bir şekilde devam ettiğini görebiliriz. Kesirli türevle ilgili 1730'lu yıllardan günümüze kadar farklı şekillerde tanımlar yapılmıştır. Matematiksel tarihi oldukça eski olmasına rağmen kullanımı yeni sayılan bu alan, türev ve integral derecelerinin tam sayı olmayan (reel, irrasyonel, kompleks) değerleri de alabilmesi ile ifade edilebilir. L'Hospital ve Leibniz arasındaki mektuplaşmada yer alan kesirli türev kavramı ile ilgili olarak 1819'da

Lacroix ilk makaleyi yayımlamıştır (Ross, 1975). Daha sonra ise Abel'in çalışması bu hususta önemli bir gelişme sağlamıştır (Cafagna, 2007). Literatürde kesirli türev ve integrallerin ortak gösterimi olarak kullanılan ve D simgesi ile gösterilen "integrodiferansiyel" operatörünün farklı durumları için türev ve integral kavramları tanımlanır. Denklem (4.25)'den görüleceği üzere üs derecesi α'nın farklı durumları için; α negatif değerli ise integral, α pozitif değerli ise türev ifadeleri anlamına gelmektedir (Korkmaz, 2013; Petráš, 2011).

$$ {}_aD_x^{\alpha} = \begin{cases} \dfrac{d^a}{dx^a}, & \alpha > 0 \\ 1, & \alpha = 0 \\ \displaystyle\int_a^x (d\tau)^{-\alpha}, & \alpha < 0 \end{cases} \tag{4.25} $$

Kesirli hesabın tanımları ve kullanımını yapabilmek için bazı matematik tanımlarını bilmek gerekmektedir. Bunlar öncelikle Gama fonksiyonları, Beta fonksiyonları, Laplace dönüşümleri ve Mittag-Leffler fonksiyonlarıdır (Podlubny, 1999, Modanlı, 2018).

Gama fonksiyonunun en basit anlamı faktöriyelin bütün reel sayılar için genelleştirilmesidir. Gama fonksiyonunun tanımı Denklem (4.22)'de verilmiştir. Beta fonksiyonu ise gama fonksiyonunun değerlerinin belirli kombinasyonlarını ifade eder. Gama fonksiyonlarının bu kombinasyonu yerine beta fonksiyonu olarak adlandırılan bir bağıntı kullanmak daha uygundur. Beta fonksiyonu ve yerine kullanıldığı gama fonksiyon kombinasyonu aşağıda (Denklem 4.26) verilmiştir (Küçük, 2014).

$$ B(p,q) = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)} = \int_0^{\infty} \frac{t^{p-1}}{(1+t)^{p+q}}\, dt, \qquad p > 0, \qquad \mathrm{q} > 0 \tag{4.26} $$

Beta fonksiyonu literatürde farklı denklemlerle de gösterilmiştir. Laplace dönüşümü de genel olarak karmaşık denklemlerim çözümünde kullanılan faydalı bir yöntemdir. Laplace dönüşümü ise aşağıdaki denklemle (Denklem 4.27) ifade edilir.

$$L\{f(t)\} = \int_0^{\infty} e^{-st} f(t)dt = F(s) \tag{4.27}$$

Yapılan tanımlar ve yaklaşımlar kısaca aşağıdaki başlıklarda verilmiştir.

4.2.1. L. Euler (1730) tanımı:

$$\frac{d^n x^m}{dx^n} = m(m-1)\dots(m-n+1)x^{m-n}$$
$$\frac{d^n x^m}{dx^n} = \frac{\Gamma(m+1)}{\Gamma(m-n+1)} x^{m-n} \tag{4.28}$$

4.2.2. Riemann-Liouville tanımı:

$${}_aD_x^{\alpha} f(x) = \frac{1}{\Gamma(m-\alpha)} \left(\frac{d}{dx}\right)^m \int_a^x \frac{f(t)}{(x-t)^{\alpha-m+1}} dt \tag{4.29}$$

4.2.3. Caputo (1967) tanımı:

$${}_a^C D_t^{\alpha} f(t) = \frac{1}{\Gamma(\alpha-m)} \int_a^x \frac{f^{(m)}(x)}{(x-t)^{\alpha-m+1}} dt \tag{4.30}$$

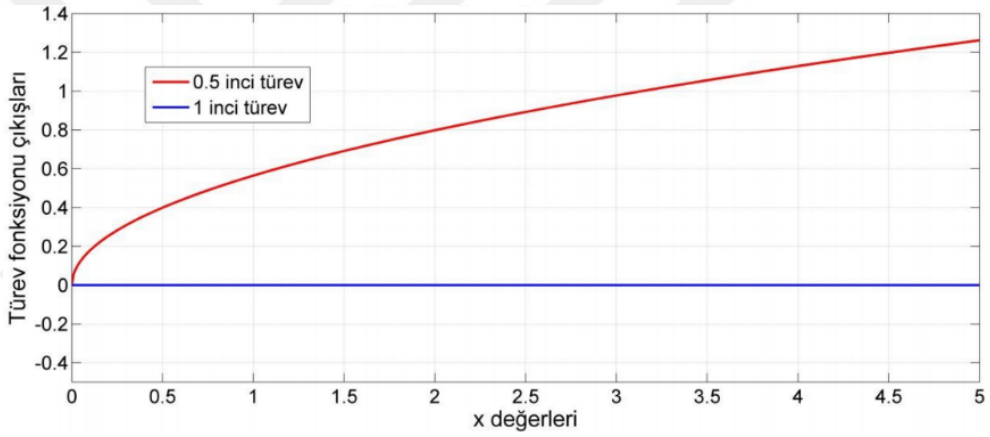
4.2.4. Grünwald - Letnikov tanımı:

$${}_aD_t^{\alpha} f(t) = \lim_{h\to 0} h^{-\alpha} \sum_{j=0}^{\frac{t-a}{h}} (-1)^j \binom{\alpha}{j} f(t-jh) \tag{4.31}$$

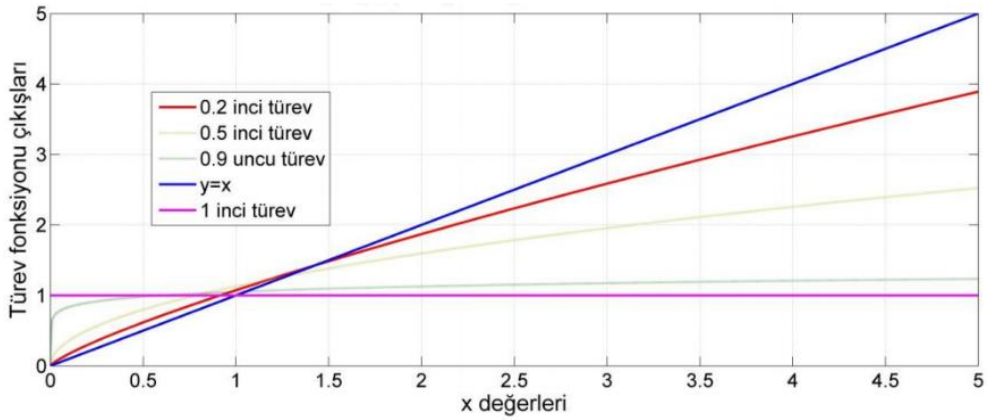
Burada $m-1 < \alpha < m$ şeklinde olmalıdır. Yine Γ ifadesi ise Gama fonksiyonudur. Caputo türevinde kesirli dereceden diferansiyel denklemlerin başlangıç şartları tamsayılı dereceden diferansiyel denklemlerle aynı formdadır. $\binom{\alpha}{j}$ kısmı ise binominal katsayılardır.

$$\binom{\alpha}{j} = \frac{\alpha!}{j!\,(\alpha-j)!} = \frac{\Gamma(\alpha+1)}{\Gamma(j+1)\Gamma(\alpha-j+1)} \tag{4.32}$$

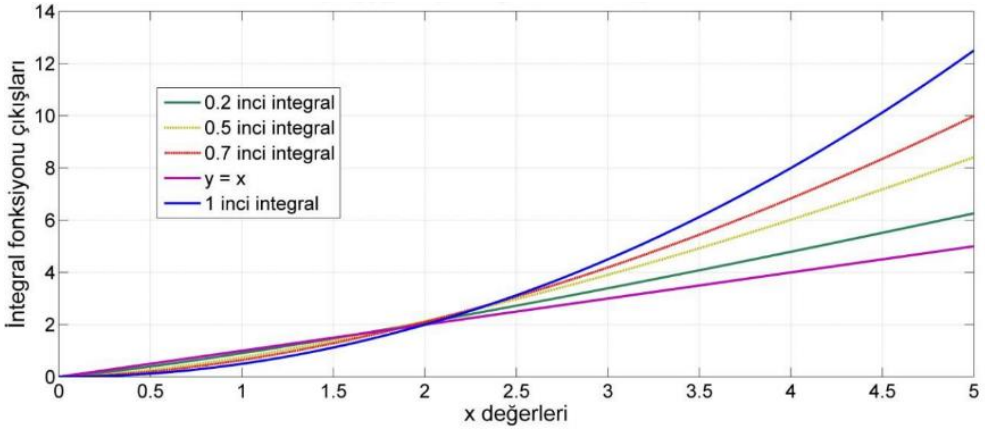
Bazı fonksiyonların kesirli dereceden integral ve türevleri Grünwald-Letnikov tanımı esas alınarak, Şekil 4.2 – 4.4'de görüldüğü gibi elde edilmektedir (Korkmaz, 2013).



Şekil 4.2. f(x) = c fonksiyonun 1 inci ve yarı dereceli türevleri (Korkmaz, 2013)



Şekil 4.3. f(x)=x fonksiyonun farklı dereceden türevleri (Korkmaz, 2013)



Şekil 4.4. f(x)=x fonksiyonun farklı dereceden integralleri (Korkmaz, 2013)

4.2.5. Kesir dereceli türevlerin numerik olarak çözülmesi

Kesir dereceli türevlerin sayısal yani numerik çözümü için Denklem (4.31)'de verilen GL (Grünwald - Letnikov) tanımından yararlanarak aşağıdaki tanımlamayı yapabiliriz.

$$ {}_{k-\frac{L_m}{h}}D_{t_k}^{q} f(t) \approx \lim_{h\to 0} h^{-q} \sum_{j=0}^{\frac{t-a}{h}} (-1)^j \binom{q}{j} f(t_k - j) \tag{4.33} $$

Burada L_m hafıza uzunluğu, $t_k = kh$, h adım aralığı ve $(-1)^j \binom{q}{j}$ binominal katsayıları da $c_j^{(q)}$ $(j = 0,1,2 \ldots)$'dir.

$$ c_0^{(q)} = 1, \qquad c_j^{(q)} = \left(1 - \frac{1+q}{j}\right) c_{j-1}^{(q)} \tag{4.34} $$

Daha sonra, kesirli diferansiyel denklemin genel sayısal çözümü

$$ {}_aD_t^q y(t) = f(y(t), t) \tag{4.35} $$

$$ y(t_k) = f(y(t), t)\, h^q - \sum_{j=v}^{k} c_j^{(q)} y(t_{k-j}) \tag{4.36} $$

şeklinde tanımlanır.

4.3. Kaotik Sistemlerin Kesir Dereceli Türev Modeli ve Analizi

Yapılan çalışmada kullanılan kaotik sistemlerin sayısal analizleri ve çözümü, Grünwald – Letnikov tanımından yararlanılarak geliştirilen kesir dereceli sistemlerin sayısal çözüm yöntemi kullanılarak gerçekleştirilmiştir. Aşağıdaki başlıklarda bazı kaotik sistemlerin kesir dereceli sayısal analizleri verilmiştir.

4.3.1. Kesir dereceli Lorenz sistemi

Lorenz kaotik sistemi Denklem (4.37)'de verilmiştir.

$$\begin{aligned} \frac{dx(t)}{dt} &= \sigma\big(y(t) - x(t)\big) \\ \frac{dy(t)}{dt} &= x(t)\big(\rho - z(t)\big) - y(t) \\ \frac{dz(t)}{dt} &= x(t)y(t) - \beta z(t) \end{aligned} \tag{4.37}$$

Burada σ Prandtl numarası ve ρ Rayleigh numarası olarak adlandırılır (Petráš, 2011). Tüm $\sigma, \rho, \beta > 0$, olmalıdır. Genellikle $\sigma = 10$, $\beta = 8/3$ ve $\rho = 28$ için kaotik davranış sergilediği bilinmektedir.

Kesirli dereceli Lorenz kaotik sistemi şöyle tanımlanır (Li ve Yan, 2007):

$$\begin{aligned} {}_0D_t^{q_1} x(t) &= \sigma\big(y(t) - x(t)\big) \\ {}_0D_t^{q_2} y(t) &= x(t)\big(\rho - z(t)\big) - y(t) \\ {}_0D_t^{q_3} z(t) &= x(t)y(t) - \beta z(t) \end{aligned} \tag{4.38}$$

q_1, q_2 ve q_3 türev kesir dereceleridir. Kesirli dereceli Lorenz kaotik sisteminin sayısal çözümü aşağıdaki gibidir:

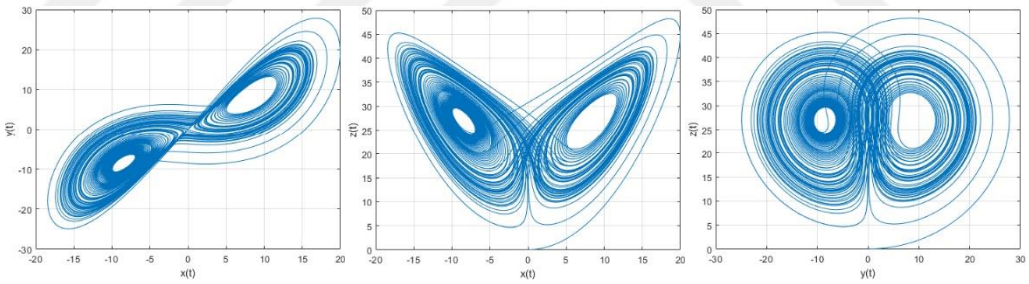
$$x(t_k) = (\sigma(y(t_{k-1}) - x(t_{k-1}))\, h^{q_1} - \sum_{j=v}^{k} c_j^{(q_1)} x(t_{k-j})$$

$$y(t_k) = (x(t_k)(\rho - z(t_{k-1})) - y(t_{k-1}))\, h^{q_2} - \sum_{j=v}^{k} c_j^{(q_2)} y(t_{k-j}) \qquad (4.39)$$

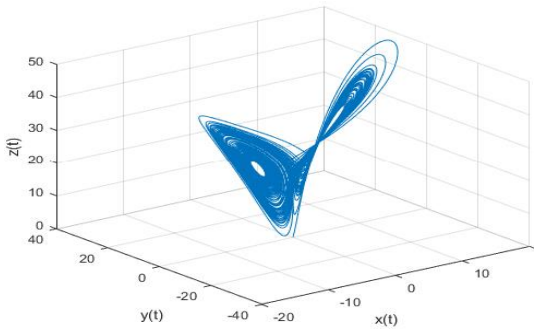
$$z(t_k) = (x(t_k)y(t_k) - \beta z(t_{k-1}))\, h^{q_3} - \sum_{j=v}^{k} c_j^{(q_3)} z(t_{k-j})$$

T_{sim} simülasyon zamanı olmak üzere $k = 1,2,3,\ldots,N$ ve $N = [T_{sim}/h]$'dir. Başlangıç şartları $x(0)$, $y(0)$ ve $z(0)$'dir ve $c_j^{(q_i)}$ binominal katsayıdır ve denklem (4.34)'de tanımı verilmiştir.

Lorenz sisteminin $(\sigma, \rho, \beta) = (10, 28, 8/3)$ parametreleri, $q_1 = q_2 = q_3 = 0.995$ ve başlangıç koşulları $(x\,(0), y\,(0), z\,(0)) = (0{,}1, 0{,}1, 0{,}1)$ seçilerek kesir derece türevli analizi ve faz portreleri Şekil 4.5 ve 4.6'da verilmiştir.



Şekil 4.5. Lorenz kaotik sistemi kesir dereceli faz portreleri: $\sigma = 10,\ \rho = 28,\ \beta = 8/3,\ q_1 = q_2 = q_3 = 0{,}995,$ ve başlangıç şartları $(x(0), y(0), z(0)) = (0{,}1, 0{,}1, 0{,}1)$



Şekil 4.6. Lorenz kaotik sistemi kesir dereceli x-y–z 3 boyut faz portresi: $\sigma = 10,\ \rho = 28,\ \beta = 8/3,\ q_1 = q_2 = q_3 = 0{,}995,$ ve başlangıç şartları $(x(0), y(0), z(0)) = (0{,}1, 0{,}1, 0{,}1)$

4.3.2. Kesir dereceli Chen sistemi

Chen kaotik sistemi Denklem (4.40)'da verilmiştir.

$$\begin{aligned}\frac{dx(t)}{dt} &= a\big(y(t)-x(t)\big)\\ \frac{dy(t)}{dt} &= (c-a)x(t)-x(t)z(t)+cy(t)\\ \frac{dz(t)}{dt} &= x(t)y(t)-bz(t)\end{aligned} \tag{4.40}$$

Burada $(a,b,c)\in R^3$ ve $(a,b,c)=(35,3,28)$ parametreleri için sistem kaotiktir. Kesirli dereceli Chen kaotik sistemi şöyle tanımlanır (Lu ve Chen, 2006):

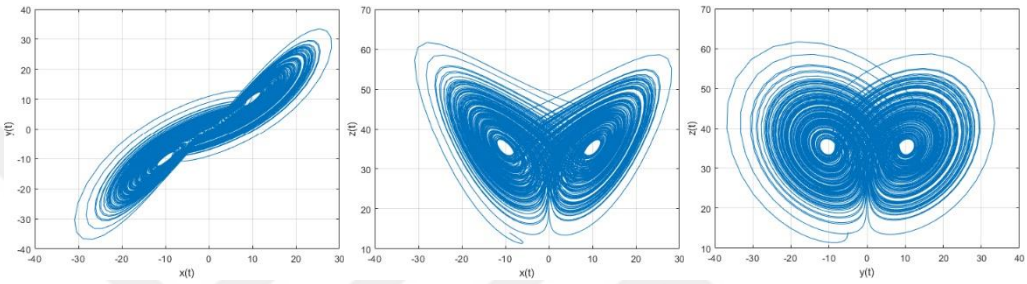
$$\begin{aligned}{}_0D_t^{q_1}x(t) &= a\big(y(t)-x(t)\big)\\ {}_0D_t^{q_2}y(t) &= (c-a)x(t)-x(t)z(t)+cy(t)\\ {}_0D_t^{q_3}z(t) &= x(t)y(t)-bz(t)\end{aligned} \tag{4.41}$$

q_1, q_2 ve q_3 türev kesir dereceleridir. Kesirli dereceli Chen kaotik sisteminin sayısal çözümü aşağıdaki gibidir:

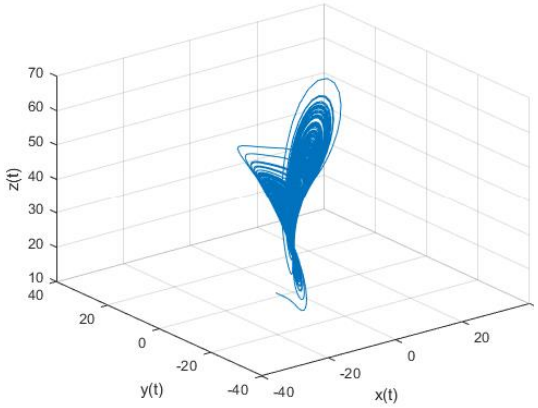
$$\begin{aligned}x(t_k) &= \Big(a\big(y(t_{k-1})-x(t_{k-1})\big)\Big)h^{q_1}-\sum_{j=v}^{k}c_j^{(q_1)}x\big(t_{k-j}\big)\\ y(t_k) &= \big((c-a)x(t)-x(t)z(t_{k-1})+cy(t_{k-1})\big)h^{q_2}-\sum_{j=v}^{k}c_j^{(q_2)}y\big(t_{k-j}\big)\\ z(t_k) &= \big(x(t)y(t)-bz(t_{k-1})\big)h^{q_3}-\sum_{j=v}^{k}c_j^{(q_3)}z\big(t_{k-j}\big)\end{aligned} \tag{4.42}$$

T_{sim} simülasyon zamanı olmak üzere, $k = 1,2,3,\ldots,N$ ve $N = [T_{sim}/h]$'dir. Başlangıç şartları $x(0)$, $y(0)$ ve $z(0)$'dir ve $c_j^{(q_i)}$ binominal katsayıdır ve denklem (4.34)'de tanımı verilmiştir.

Chen sisteminin $(a, b, c, d) = (35, 3,\ 28, -7)$ parametreleri, $q_1 = q_2 = q_3 = 0{,}9$ ve başlangıç koşulları $\big(x\ (0), y\ (0), z\ (0)\big) =\ (-9, -5{,}14)$ seçilerek kesir derece türevli analizi ve faz portreleri Şekil 4.7 ve 4.8'de verilmiştir.



Şekil 4.7. Chen kaotik sistemi kesir dereceli faz portreleri: $a = 35,\ b = 3,\ c = 28,\ d = -7$ ve $q_1 = q_2 = q_3 = 0.9$, başlangıç şartları $(x(0), y(0), z(0)) = (-9, -5{,}14)$



Şekil 4.8. Chen kaotik sistemi kesir dereceli x-y-z 3 boyut faz portresi: $a = 35,\ b = 3,\ c = 28,\ d = -7$ ve $q_1 = q_2 = q_3 = 0.9$, başlangıç şartları $(x(0), y(0), z(0)) = (-9, -5{,}14)$

4.3.3. Kesir dereceli Rössler sistemi

Rössler kaotik sistemi Denklem (4.43)'da verilmiştir.

$$\frac{dx(t)}{dt} = -\big(y(t) + z(t)\big)$$
$$\frac{dy(t)}{dt} = x(t) + ay(t) \tag{4.43}$$
$$\frac{dz(t)}{dt} = b + z(t)(x(t) - c)$$

Burada $a = 0{,}2,\ b = 0{,}2,\ c = 5{,}7$ parametreleri için sistem kaotiktir. Kesirli dereceli Rössler kaotik sistemi şöyle tanımlanır (Li ve Chen, 2004):

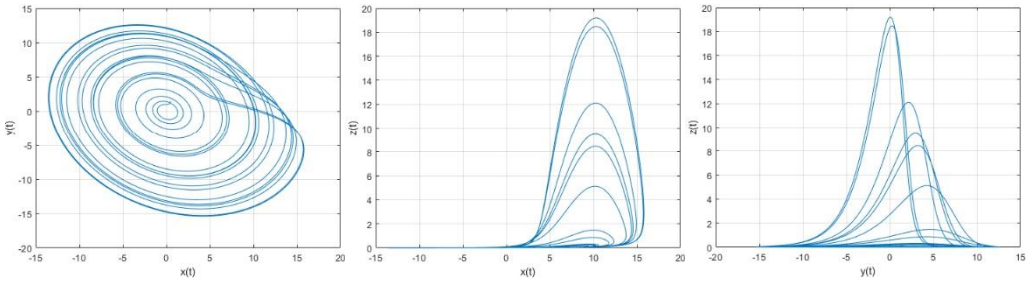
$${}_0D_t^{q_1} x(t) = -\big(y(t) + z(t)\big)$$
$${}_0D_t^{q_2} y(t) = x(t) + ay(t) \tag{4.44}$$
$${}_0D_t^{q_3} z(t) = b + z(t)(x(t) - c)$$

q_1, q_2 ve q_3 türev kesir dereceleridir. Kesirli dereceli Rössler kaotik sisteminin sayısal çözümü aşağıdaki gibidir:

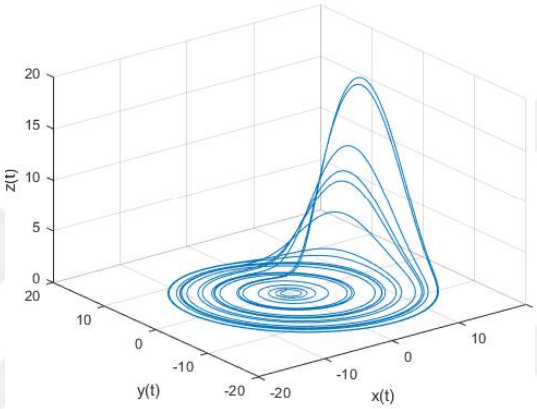
$$x(t_k) = \Big(-\big(y(t_{k-1}) + z(t_{k-1})\big)\Big) h^{q_1} - \sum_{j=v}^{k} c_j^{(q_1)} x\big(t_{k-j}\big)$$
$$y(t_k) = \big(x(t) + ay(t_{k-1})\big) h^{q_2} - \sum_{j=v}^{k} c_j^{(q_2)} y\big(t_{k-j}\big) \tag{4.45}$$
$$z(t_k) = \big(b + z(t_{k-1})(x(t) - c)\big) h^{q_3} - \sum_{j=v}^{k} c_j^{(q_3)} z\big(t_{k-j}\big)$$

T_{sim} simülasyon zamanı olmak üzere, $k = 1{,}2{,}3, \ldots, N$ ve $N = [T_{sim}/h]$'dir. Başlangıç şartları $x(0)$, $y(0)$ ve $z(0)$'dir ve $c_j^{(q_i)}$ binominal katsayıdır ve denklem (4.34)'de tanımı verilmiştir.

Rössler sisteminin $(a, b, c) = (0{,}5,\ 0{,}2, 10)$ parametreleri, $q_1 = q_2 = q_3 = 0{,}9$ $(q > 0{,}839)$ ve başlangıç koşulları $(x\,(0), y\,(0), z\,(0)) = (0{,}5,\ 1{,}5,\ 0{,}1)$ seçilerek kesir derece türevli analizi ve faz portreleri Şekil 4.9 ve 4.10'da verilmiştir.



Şekil 4.9. Rössler kaotik sistemi kesir dereceli faz portreleri: $a = 0{,}5,\ b = 0{,}2,\ c = 10,$ ve $q_1 = q_2 = q_3 = 0{,}9,$ başlangıç şartları $(x(0), y(0), z(0)) = (0{,}5,\ 1{,}5,\ 0{,}1)$



Şekil 4.10. Rössler kaotik sistemi kesir dereceli x-y-z 3 boyut faz portresi: $a = 0{,}5,\ b = 0{,}2,\ c = 10,$ ve $q_1 = q_2 = q_3 = 0{,}9,$ başlangıç şartları $(x(0), y(0), z(0)) = (0{,}5,\ 1{,}5,\ 0{,}1)$

4.4. Tez Çalışmasında Kullanılan Yöntemler

Yapılan çalışmada kullanılan kaotik sistemlerin ürettikleri işaretler sayısal çözüm algoritmaları tarafından elde edilir. Bu elde edilen işaret dizisi pozitif ve negatif sayılar olmak üzere decimal olarak çıktı verir. Yapılan çalışmada bu çıktılar ikili sayıya dönüştürülür ve rasgele dağılımın en çok olduğu en düşük değerlikli bitler (LSB) alınır. Bu başlık altında, yapılan çalışmada kullanılan ikili sayıya dönüştürme ve son işlemleri anlatılacak.

4.4.1. Yöntem 1 (Kayan noktalı sayı)

Yapılan çalışmada ikili sayıya dönüştürmede kullanılan birinci yöntem tek duyarlı (32 bit) IEEE 754 standardına göre düzenlenen ikili sayıya dönüştürme yöntemidir.

IEEE (Institute of Electrical and Electronics Engineers - Elektrik ve Elektronik Mühendisleri Enstitüsü), Kayan Nokta Aritmetiği Standardı kayan noktalı sayıların gösteriminde en çok kullanılan standarttır. İkilik sistemdeki sayılar bilimsel gösterim ile gösterildikten sonra işaret, üst ve anlamlı kısımdan oluşan üç parça şeklinde ifade edilir. Bu gösterime "sonsuz", "sayı değil" ve "sıfır"ın gösterimi de dahildir. IEEE 754 standardına göre sayılar tek duyarlı (32 bit) ve çift duyarlı (64 bit) şekilde gösterilebilirler.

Tek duyarlı gösterimde sayı 32 bitle ifade edilir. Bu bitlerden biri işaret, 8'i üst 23 tanesi ise anlamlı kısmın gösterimi için kullanılır. Tek duyarlı gösterimde üst için kaydırma değeri $2^{8-1} - 1 = 127$ olarak hesaplanır.

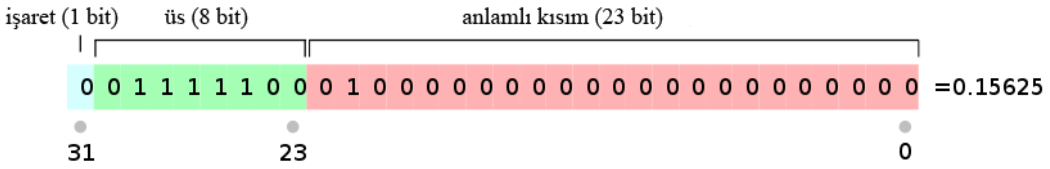
Örnek olarak tek duyarlı gösterimde 6,375 sayısını göstermek istersek;

$$6 = (110)^2 \rightarrow 0{,}375 = (0{,}011)^2 \rightarrow 6{,}375 = (110{,}011)_2$$

Sayıyı olağan duruma getirirsek: $110{,}011 = 1{,}10011x2^2$
Sayı sıfırdan büyük olduğu için işaret biti: 0
Sayının üst değerinin saptırılmış hali: $2 + 127 = 129 \rightarrow 129_{10} = 10000001_2$
Anlamlı kısım: 10011000000000000000

Sayı son olarak; 0 10000001 10011000000000000000 şeklinde ifade edilir.

Başka bir örnek 0,15625 sayısının IEEE 754 tek duyarlı karşılığı aşağıda (Şekil 4.11) verilmiştir.



Şekil 4.11. Örnek 0,15625 sayısının IEEE 754 tek duyarlı gösterimi

4.4.2. Yöntem 2 (dec2bin)

Bu yöntemde üretilen pozitif ve negatif ondalıklı gerçek sayılar önce ötelenerek pozitif sayılara daha sonra bu sayların hassaslığı korunması için de virgülleri kaydırılarak tam sayılara dönüştürülür. Daha sonra da bu tamsayılar ikilik sayıya dönüştürülür. Burada Matlab >>*dec2bin* komutu ile binary sayıya dönüştürme işlemi gerçekleştirilir.

$$(x_k + |min_x|)10^v \tag{4.46}$$

Burada x üretilen diziyi, k dizinin indisini, min_x dizinin en küçük elemanını, v ise kaç basamak virgülün kaydırılacağını belirtir. Bu denklem ile tam sayıya dönüştürülen değer daha sonra binary forma dönüştürülür.

4.4.3. Yöntem 3 (mod2)

Bu yöntemde kaotik sistemden üretilen gerçek sayı dizisinin virgülden sonraki basamaklarına bakılır. Virgülden sonraki basamakların her biri için o sayı çift ise ‘0’, tek ise ‘1’ yazılır. Burada virgülden sonra gelen kaç değerin alınacağını arayüz programından girilen *“Hassasiyet”* değeri belirler.

Örneğin $x_1 = 5{,}78942168125789, x_2 = 4{,}1569223445561, x_3 \ldots$ şeklinde gelen x dizisi için hassaiyet değerimiz 4 olsun.

x_1 için virgülden sonraki 4 basamak → 7894

x_2 için virgülden sonraki 4 basamak → 1569

x_3 ...

alınır. Bu sayıların basamak değerleri için çift ise ‘0’, tek ise ‘1’ olacak şekilde aşağıdaki gibi yazılır.

7894 → 1010

1569 → 1101

…

Bu şekilde oluşturulan binary sayı 10101101 ... şeklinde oluşur.

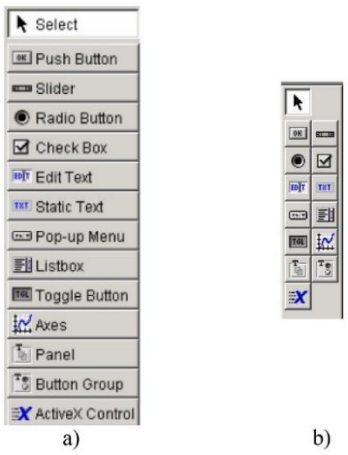
BÖLÜM 5. KESİRLİ TÜREVLİ VE ÇOK FONKSİYONLU KAOTİK RASGELE SAYI ÜRETECİ ARAYÜZ TASARIMI

Önceki bölümlerde anlatılan kaotik sistemler, bunların sayısal çözüm analizleri ve bu sistemlerin ürettiği sayıların ikili (binary) rasgele sayıya dönüştürme yöntemleri hazırlanan bir arayüz programı ile oluşturuldu. Bu arayüz programında seçilen kaotik sistemler, yine arayüz programından seçilen çözüm algoritmaları, seçilen son işlem yöntemleri ve diğer üretim ayarlarıyla birlikte sunuldu. Tasarlanan arayüz programında farklı kaotik sistemlerin bulunması ve eklenebilmesi, başlangıç değerlerinin ve kesir derece değerlerinin girilmesi, farklı çözüm algoritmalarının sunulması, iterasyon sayısı, adım aralığı ve hassasiyet gibi detaylı ayarların ayarlanabilmesi ve üretilen rasgele işaretlerin çıkış yöntemlerinin seçilmesi gibi ayarları bir arada bulundurması açısından kullanımı kolay ve pratik kaotik rasgele sayı üreteci tasarlandı. Bu tasarım ve kullanımı bu bölümde açıklanacaktır.

5.1. Matlab GUI ve Arayüz Tasarımı

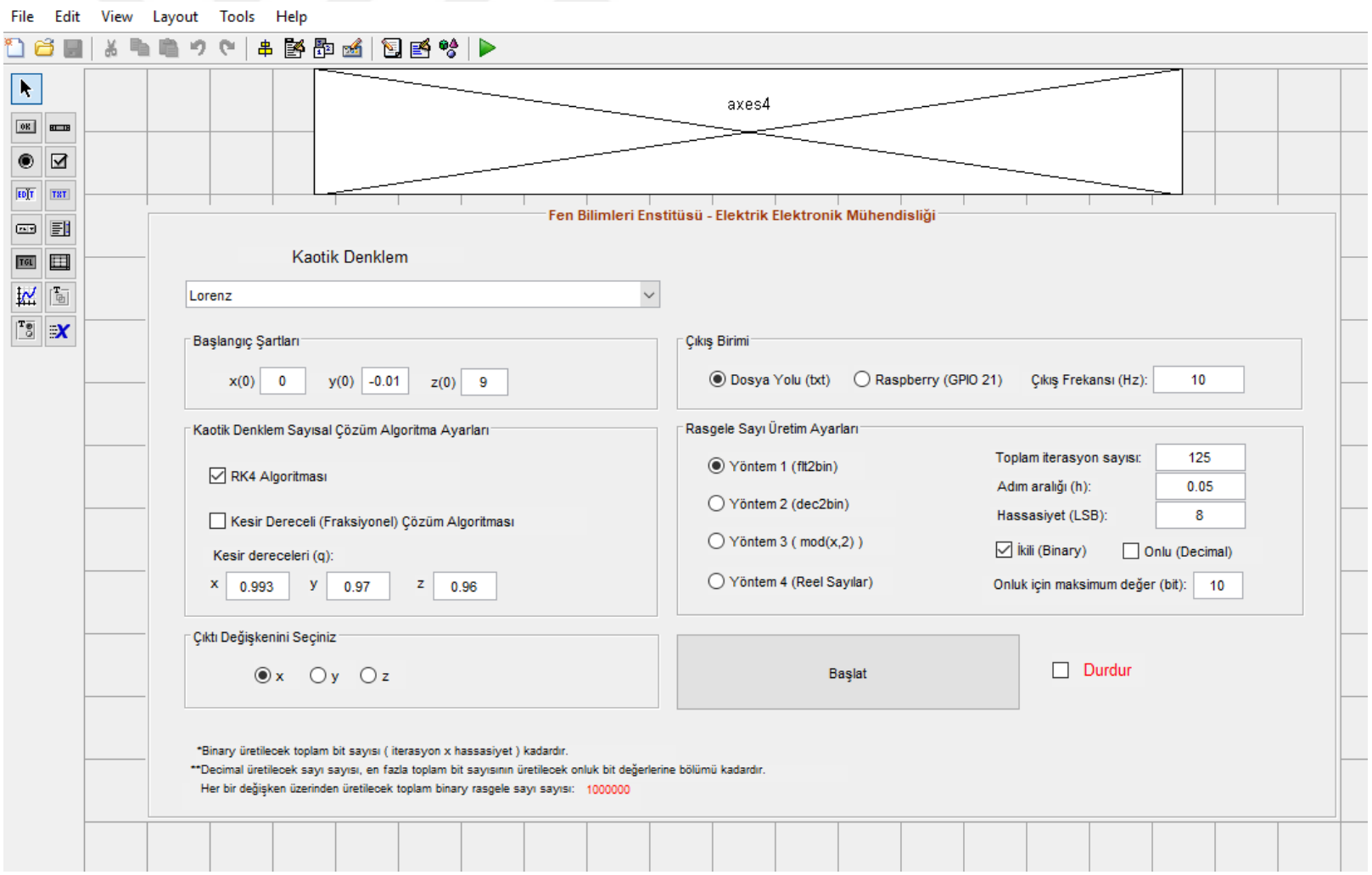
Özellikle GUI tasarımında hızlı arayüzler tasarlamak için MATLAB GUIDE aracının kullanılması büyük bir kolaylık sağlar. Bu araç ile GUI arabirimi kolaylıkla sürükle bırak ve açılan pencerelerde özelliklerin değiştirilmesine dayanan bir yöntem kullanılır. Ayrıca, bu yöntemi kullanmanın ileride var olan bir GUI'nin düzenlenmesi ve değişiklik yapılması bakımından da çok yararlıdır. M-File programlama yönteminde tüm GUI tasarımları ve callback program parçalarının yazılması tamamı ile programlama kodları kullanılarak yapılır.

Kaotik rasgele sayı üreteci uygulamasının grafiksel arayüzü için MATLAB GUIDE kullanılacak araçlar ve nesneler çalışma alanına yerleştirilir ve bu nesnelerin işlev ve fonksiyonları tanımlanması ve yazılmasına hazır hale getirilmiş olur.



Şekil 5.1 Component Palet nesneler a) Nesne İsimleri Var b) Nesne İsimleri Yok

MATLAB GUIDE kullanılan araçları tanıdıktan sonra hazırlanılacak arayüz programı için gerekli nesneler ve bunların tanım ve etiketleri aşağıdaki (Şekil 5.2) gibi hazırlanmıştır.



Şekil 5.2 GUIDE nesnelerin yerleştirilmesi

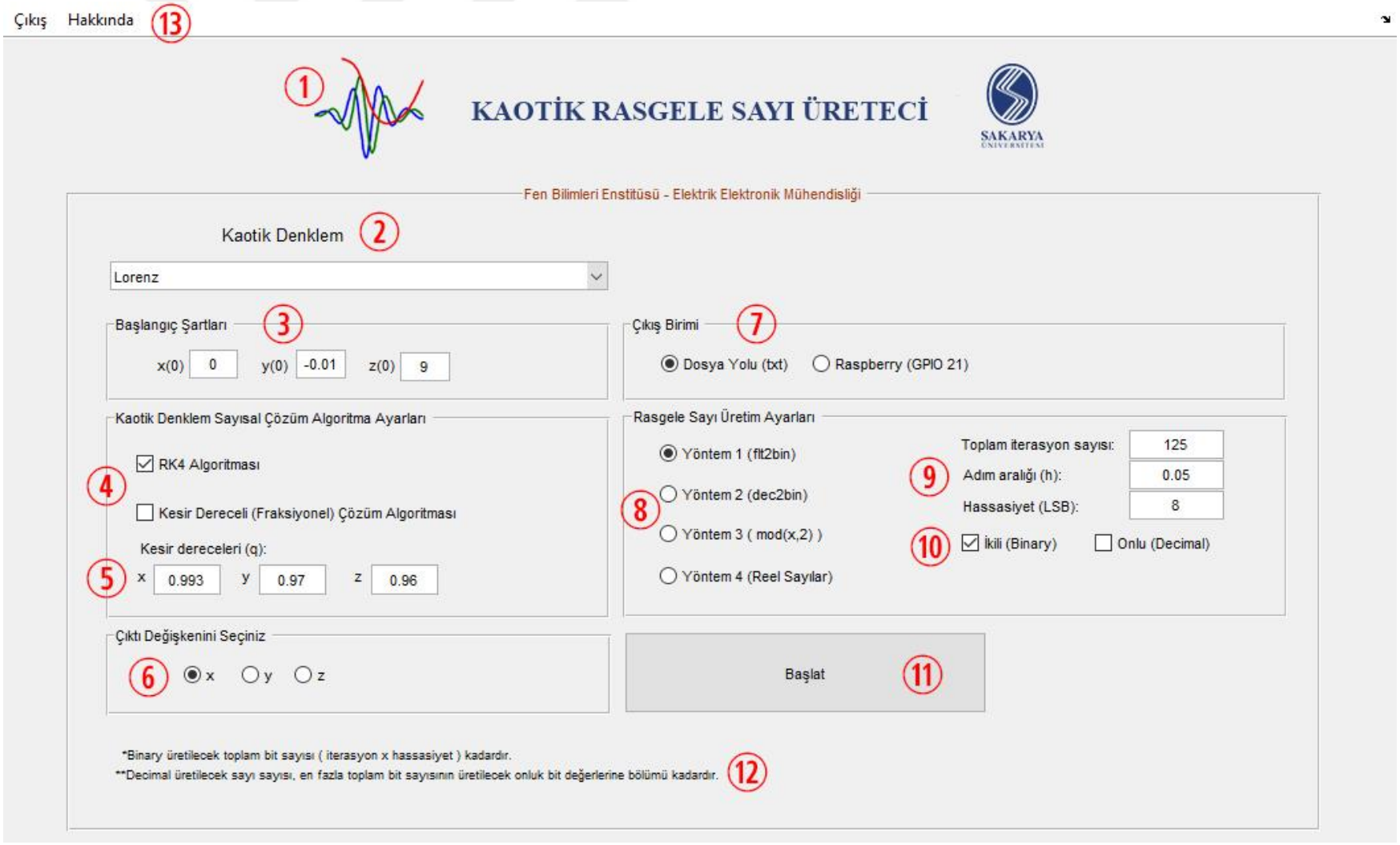
5.2. Kesirli Türev ve Çok Fonksiyonlu Kaotik Rasgele Sayı Üreteci Özellikleri ve Kullanımı

Yukarıdaki (Şekil 5.2) gibi arayüz tasarımında nesneler yerleştirildikten ve tanımlandıktan sonra bu nesneler M-File ortamında programlanır. Şekil 5.3'de program arayüzü verilmiştir. Bu arayüz programının açıklamaları ve tasarımda bulunan nesneler ile yaptıkları işlemler detaylı olarak aşağıda verilmiştir.

Gerçekleştirilen bu çalışmada ve tasarımda, seçilen sürekli kaotik sistem ve başlangıç şartları ile denklem; girilen iterasyon sayısı ve adım aralığı için "RK4" algoritması veya girilen kesir türev emirleri (q_1, q_2, q_3) için "Kesir Dereceli Türevli Kaotik Sistemler Grünwald-Letnikov tanımı" ile çözülür. Burada çözülen sistem için üretilen ayrık değerler gerçek sayı değerleridir. Bu gerçek ondalıklı sayılar, seçilen yöntem türüne göre 32 bit binary sayı formatına dönüştürülür. Tüm bitlerin alınması ideal rasgeleliği sağlamadığı ve testlerden geçemediği için en rasgele dağılıma sahip olan en düşük anlamlı bitler alınır. Burada daha az işlem sayısı ve daha fazla üretilecek sayı için en düşük anlamlı bitlerin kaçının seçileceği de arayüzden girilen "Hassasiyet" değeri ile seçilir. Burada girilen değer, üretilen 32 bit sayısının en düşük anlamlı kaç bitinin alınacağını belirler.

Eğer İkili (Binary) kutusu seçili ise: Çözülen ve 32 bit binary sayıya dönüştürülen değerlerden girilen hassasiyet değerine göre üretilen binary sayılar txt formatında kaydedilir veya girilen frekans değerinde daha önceden tanımlanmış olan Raspberry Pi donanımının dijital çıkış pinine gönderilir. Onlu (Decimal) kutusu seçili ise: Açılan girdi kutusundan girilen değer kadar alınan bit kümeleri decimal formata dönüştürülür ve txt formatında kaydedilir. Burada üretilen bit dizisinden girilen değer kadar alınan bitler decimal formata dönüştürüleceği için decimal üretilecek sayı sayısı, en fazla toplam bit sayısının üretilecek onluk bit değerlerine bölümü kadar olacaktır.

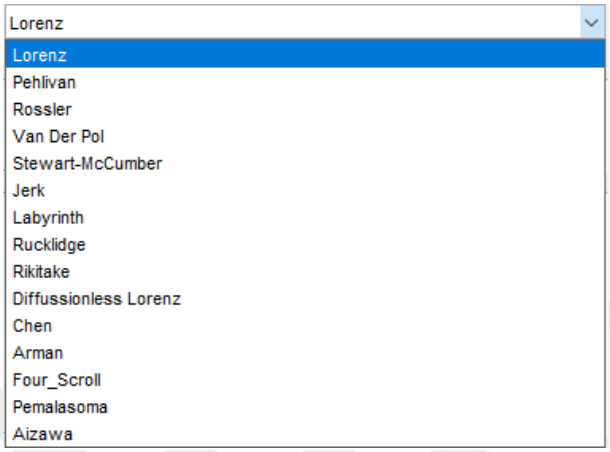
Burada yöntem türleri, üretilen gerçek sayıların binary formata nasıl dönüştürüleceğini belirler. Yöntem 1, üretilen gerçek noktalı sayıları kayan noktalı sayı biçiminde (IEEE 754 Standardı) binary forma dönüştürür. Yöntem 2, üretilen gerçek sayıların virgüllü kısımlarını alacak şekilde çok büyük bir sayı ile çarpıp, tam sayı kısmının mutlak değerini binary forma dönüştürür. Yöntem 3, üretilen gerçek sayıların virgülden sonraki basamak değerlerinin mod2 işleminin alınması ile binary forma dönüştürür. Burada virgülden sonra kaç basamağın bakılacağına arayüz tasarımından girilen "Hassasiyet" değeri belirler. Yöntem 4 ise hiçbir dönüştürme kullanmadan üretilen gerçek sayıları alır.



Şekil 5.3. KGRSU arayüz tasarımı ve nesneleri

(1) Başlık Görseli: Uygulama başlığı ve logoların bulunduğu bölüm.

(2) Kaotik Denklem Menüsü: Kaotik sistem denklemlerinin bulunduğu menü. 15 adet kaotik sistem tasarımda kayıtlıdır.



Şekil 5.4. KGRSU arayüz tasarımı kaotik denklem menüsü

(3) Başlangıç Şartları: Seçilen kaotik sistemin başlangıç şartlarının girildiği bölüm.

(4) Kaotik Denklem Sayısal Çözüm Algoritmaları: Burada seçilen kaotik sistemin hangi yöntem ile çözüleceği belirlenir. 4. dereceden klasik Runge-Kutta Yöntemi için "RK4", Kesir dereceli türevli kaotik sistem sayısal çözüm algoritması için de "Kesir Dereceli Çözüm Algoritması" seçilir.

(5) Kesir Dereceleri (Türev Değer Emirleri): Seçilen "Kesir Dereceli Çözüm Algoritması" için türev değer emirlerinin (q_1, q_3, q_3) girildiği bölüm.

(6) Çıktı Değişkeni: Tasarlanan arayüz programı ile üretilecek rasgele sayı dizisinin kaotik sistemin hangi değişkeninden üretileceğinin seçildiği bölüm.

(7) Çıkış Birimi: Üretilen kaotik sayı dizisinin veya sinyalin çıkış şeklinin seçildiği bölüm. "Dosya Yolu" seçili ise üretilen kaotik sayı dizisi programın çalıştırıldığı klasöre .txt dosyası olarak kaydedilir. "Raspberry" seçili ise üretilen sinyal Matlap'ta tanımlanmış Raspberry kartının GPIO 21 numaralı pininden çıktı verir. Çıkış sinyali

“Raspberry” seçeneği seçildikten sonra görünür olan “Çıkış Sinyali” seçeneğinde girilir.

Şekil 5.5. “Raspberry” seçeneği seçildikten sonra görünür olan “Çıkış Sinyali”

Burada Raspberry donanımının Matlab’a tanıtmak için birkaç farklı yöntem vardır. Raspberry online olarak Matlap programı ile kullanılabilir. Matlab Raspberry destek paketi kurularak kablosuz ağ veya ethernet kablosu ile bağlantı kurulabilir. Aşağıda bu yöntemlerden bazıları açıklanmıştır.

Matlab Online'da Raspberry Pi Donanım Kartına bağlanmak için desteklenen işletim sistemleri Raspbian Jessie veya Raspbian Stretch'dir ve desteklenen anakartlar Raspberry Pi 2 Model B ve Raspberry Pi 3 Model B'dir. Cihazın aynı bilgisayara veya Matlab Online çalışan bilgisayarla aynı ağa bağlı olması gerekmeden herhangi bir internet ağına bağlı olması yeterlidir. Masaüstü ortamı olan bir Raspbian sürümünde yükleme komutlarını girmek gereklidir.

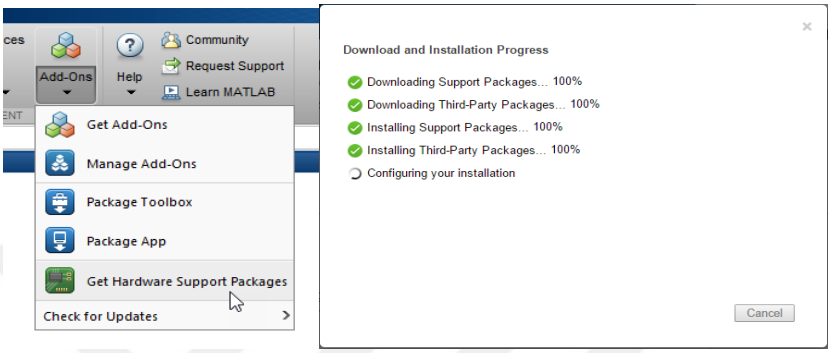
Raspberry Pi komut satırına

```
$sudo apt-get update
$sudo apt-get install matlab-rpi
$sudo matlab-rpi-setup
```

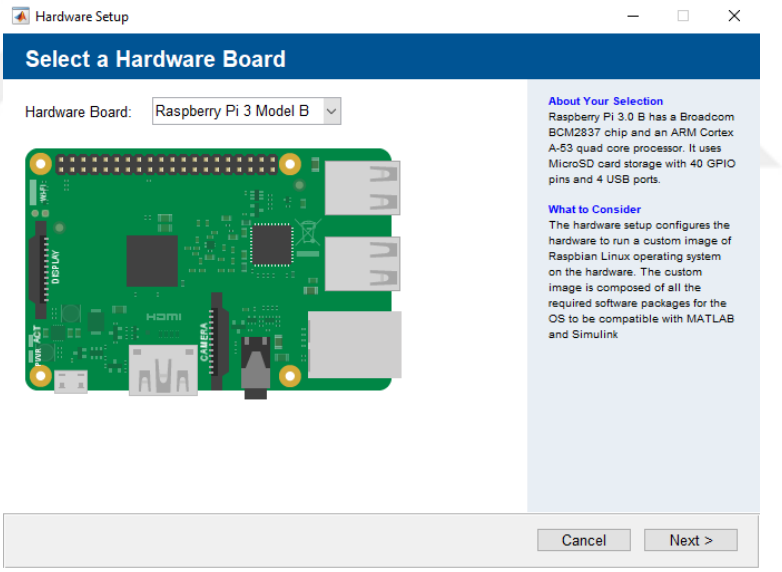
komutları yazılarak kurulum ve diğer tanıtım bilgileri tamamlanır. Burada Matlab Çevrimiçi bağlantısını doğrulamak için MathWorks Hesap bilgilerinin girilmesi istenir. Daha sonra Raspberry donanımı yeniden başlatılarak kullanıma hazır hale gelir. Aynı MathWorks Hesap kimlik bilgileriyle yapılandırılmış Raspberry Pi donanımı Matlab komutlarıyla taranır ve Matlab’da tanıtıldıktan sonra Raspberry Pi ile bağlantı kurulmuş olur.

Matlab destek paketi kurularak Raspberry Pi tanıtılması ve bağlantı kurulması için:

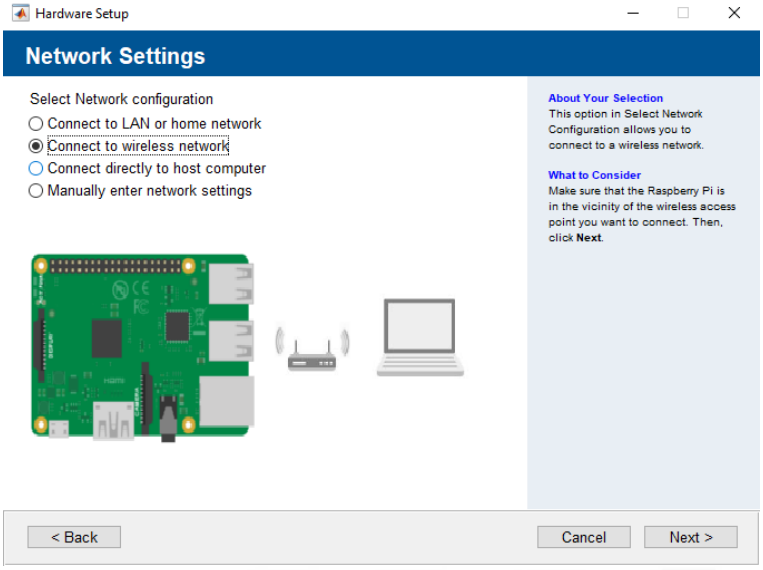
MATLAB Giriş sekmesinde, Ortam bölümünde, Add-Ons > Get Hardware Support Packages seçilir. Açılan ekranda “Matlab Support Package for Raspberry Pi Hardware” paketi seçilir paket kurulumu yapılır.



Şekil 5.6. Raspberry Pi donanım için Matlab destek ve kurulum

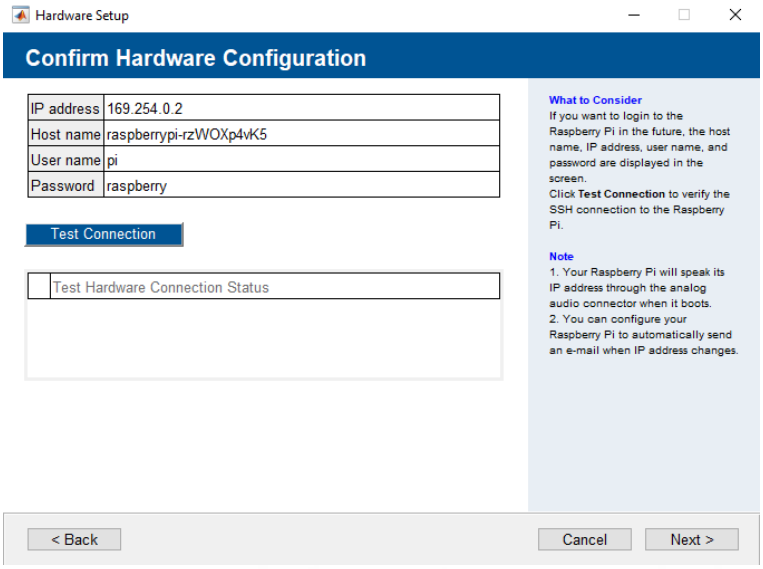


Şekil 5.7. Raspberry Pi donanım seçimi



Şekil 5.8. Raspberry Pi donanım için bağlantı ayarları

Şekil 5.9. Raspberry Pi donanım için hafıza kartına kurulum yapılandırma dosyalarının yüklenmesi

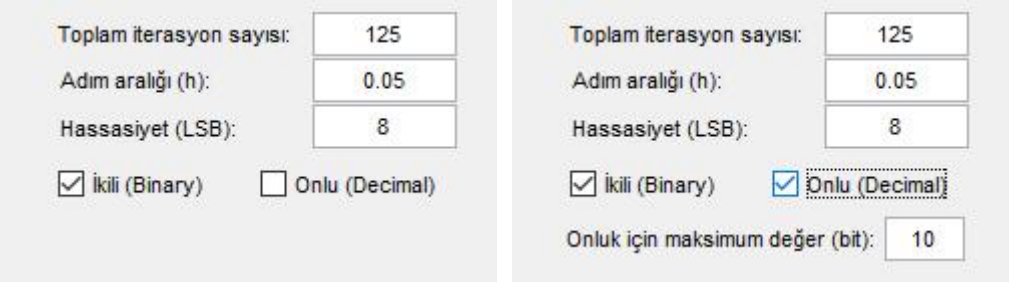


Şekil 5.10. Raspberry Pi donanım için Matlab kurulum yapılandırma ve test

(8) Yöntem Seçenekleri: Burada 4. bölümde anlatılan kaotik işaretin ikili sayıya dönüştürme yöntemleri veya doğrudan reel sayı olarak çıkış seçeneklerinden biri seçilir.

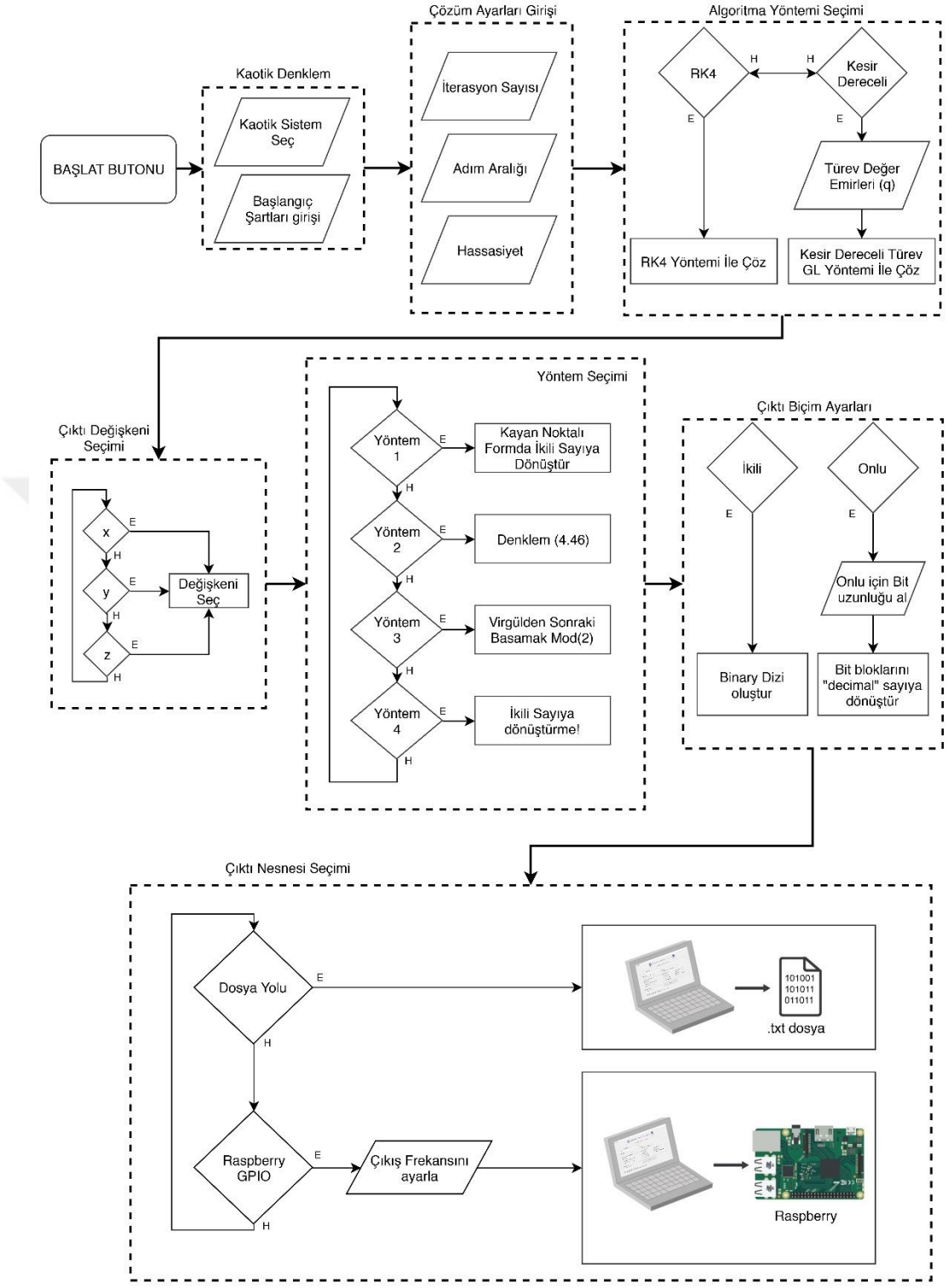
(9) Kaotik Sistemin Sayısal Çözüm Ayarları: Burada kaotik sistemin sayısal çözümü için gerekli "İterasyon Sayısı", "Adım Aralığı" ve ikili sayıya dönüştürmede en hassas kaç bitin seçileceğinin belirleneceği "Hassasiyet" değeri belirlenir.

(10) Rasgele Sayı Çıktı Seçenekleri: Burada üretilen rasgele sayılar "İkili" seçeneği seçili ise binary formda "Onlu" seçeneği seçili ise decimal formda kaydedilir. Onlu forma dönüştürme işlemi üretilen binary rasgele sayılar kullanılarak gerçekleştirilir. "Onlu" seçeneği seçildiğinde üretilen ikili bit dizisinden onlu değere dönüştürme işlemi için alınacak bit bloklarının uzunluğunun girileceği "Onluk için maksimum değer" bölümü görünür olur.



Şekil 5.11 "Onlu" seçeneği seçildikten sonra görünür olan "Onluk için maksimum değer" bölümü

(11) Başlat Butonu: Arayüz tasarımında seçilen seçenekler ve ayarlar için rasgele sayı üretme işlemini başlatma butonu. Seçenek bilgilerinin alındığı ve bu bilgilere rasgele sayı dizisinin üretildiği ve çıktılarının verildiği tüm algoritma ve kodlar bu Matlab M-File dosyasının bu butonun etiketleri (function basla_Callback) altındadır.



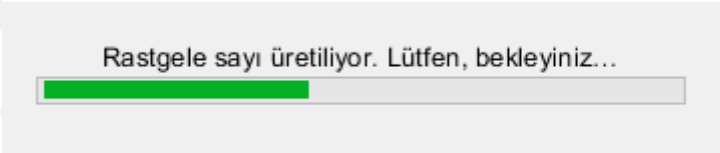
Şekil 5.12. Başlat butonu ile çalışan programın akış diyagramı

Tasarlanan arayüz programında başlat butonu ile birlikte çalışan temel programın akış diyagramı Şekil 5.12'de verilmiştir. Bu program başlat butonu "callback"i altında yer almaktadır. Temel M-File program kodlarında diğer arayüz ve fonksiyonlara ait kodlar da bulunmaktadır.

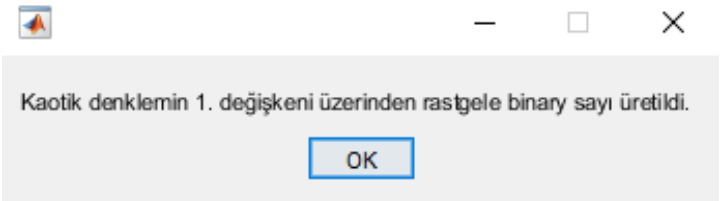
(12) Bilgilendirme: Bu kısımda seçilen ayarlara göre üretilecek rasgele sayılar için bilgiler yer almaktadır.

(13) Menü Çubuğu: Bu kısımda "Çıkış" butonu ve "Hakkında" menüsü vardır. "Hakkında" menüsü altında "Yardım" ve "Bilgi" bölümleri vardır.

Program çalıştırılıp sayı üretilmek istenildiğinde yapılan işlemin ilerlemesi şekil 5.13'de gösterilen yüklem çubuğu ile görselleştirilir.

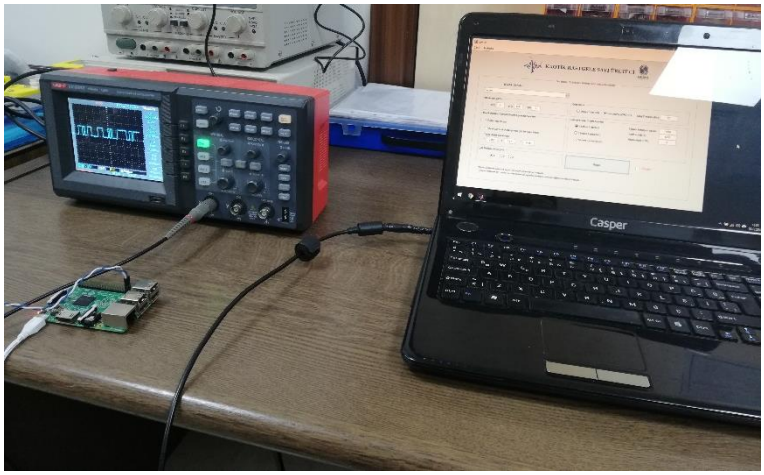


Şekil 5.13. Başlat butonu ile çalışmaya başlayan programda yükleme çubuğu

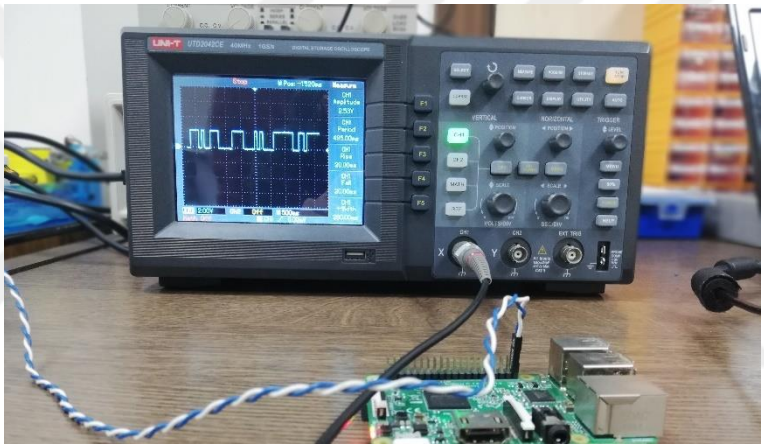


Şekil 5.14. Başlat butonu ile çalışmaya başlayan programda sayı üretildi bildirimi

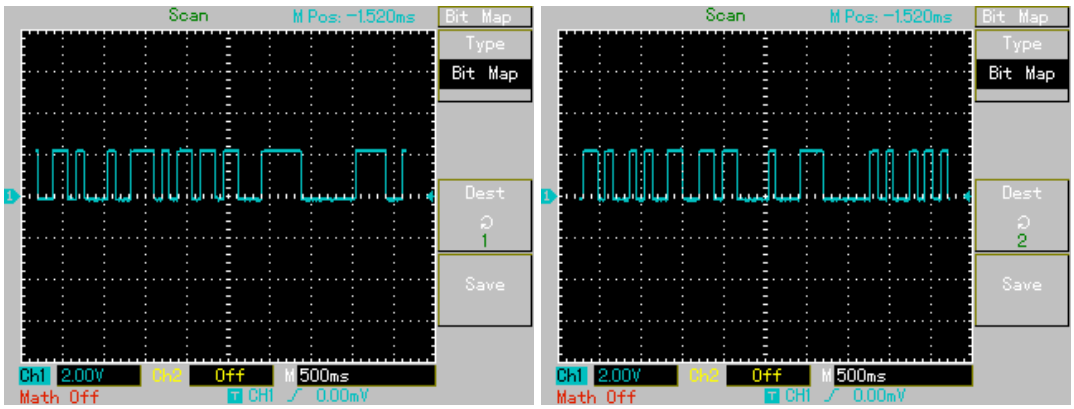
Burada üretilen rasgele sayı dizisi seçilen ayara göre dosya içerisine txt dosyası olarak yazılır veya Raspberry Pi donanımı GPIO21 numaralı pine gönderilmiş olur.



Şekil 5.15. Kablosuz ağ üzerinden üretilen sayıların Raspberry Pi'ye gönderilmesi

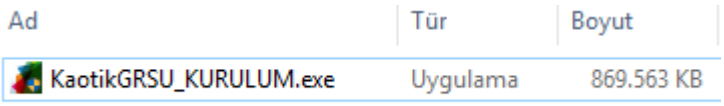


Şekil 5.16. Raspberry Pi'den elde edilen sinyalin osilaskop ekranında incelenmesi



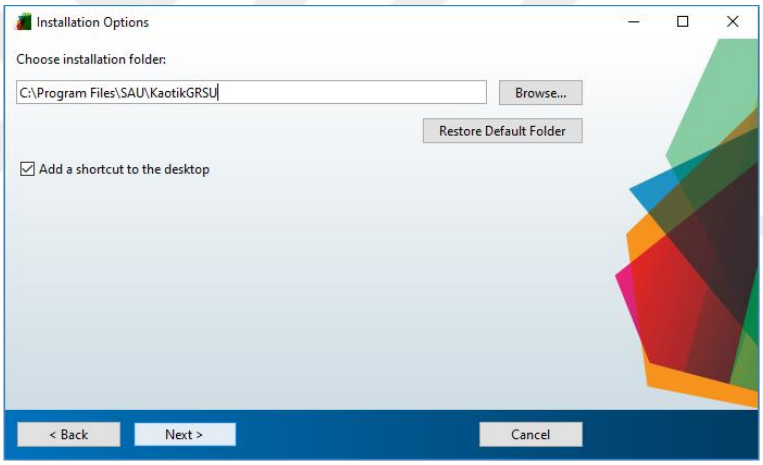
Şekil 5.17. Raspberry Pi'den elde edilen sinyalin osilaskop ekran görüntüsü

Ayrıca Matlab GUIDE ortamında tasarlanan program Windows uygulama dosyası (exe) olarak da derlenmiş ve kurulum dosyası ve kurulu program görselleri aşağıdaki şekillerde verilmiştir.

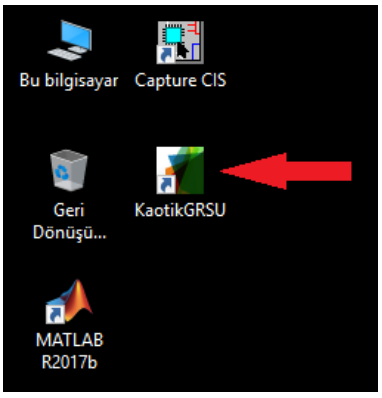


Şekil 5.18. Matlab derleyici ile yapılan uygulamanın Windows kurulum dosyası

Matlab derleyici seçenekleri ile Windows uygulaması olarak kaydedilen program Matlab kurulumuna ihtiyaç duymadan herhangi bir bilgisayar ile de çalıştırılabilir haldedir.



Şekil 5.19. Matlab derleyici ile yapılan uygulamanın Windows kurulumu



Şekil 5.20. Kurulan uygulamanın masaüstü kısayol simgesi

BÖLÜM 6. İSTATİSTİKSEL RASGELELİK TEST SONUÇLARI

Önerilen ve 4. Bölüm'de anlatılan yöntemlerle tasarımı yapılan Kaotik Rasgele Sayı Üreteci'nin ürettiği sayı dizilerinin rasgele olup olmadığını anlamak için rasgelelik testlerini uygulamak gerekmektedir. Literatürde birçok rasgele sayı test programı önerilmiştir. Bunlara FIPS-140-1 testi, NIST-800-22 testi, ENT testi, DIEHARD Testi, PractRand ve RaBiGeTe testleri örnek verilebilir. Tasarımı yapılan programın ürettiği sayıların bazılarının test sonuçları aşağıdaki tablolarda verilmiştir.

Tablo 6.1. Lorenz Sistemi NIST800-22 test sonuçları

Lorenz Sistemi	**Yöntem 1**		**Yöntem 2**		**Yöntem 3**	
İstatistiksel Testler	P-değeri	**Sonuç**	P-değeri	**Sonuç**	P-değeri	**Sonuç**
Frequency (Monobit) Test	0,56732	✓	0,37347	✓	0,9904256	✓
Block-Frequency Test	0,01636	✓	0,88986	✓	0,3661803	✓
Cumulative-Sums Test	0,72051	✓	0,45657	✓	0,7885117	✓
Runs Test	0,61263	✓	0,42209	✓	0,6100516	✓
Longest-Run Test	0,39002	✓	0,09205	✓	0,4176718	✓
Binary Matrix Rank Test	0,3404	✓	0,73107	✓	0,4901672	✓
Discrete Fourier Transform Test	0,93418	✓	0,5147	✓	0,9195958	✓
Non-Overlapping Templates Test	0,46464	✓	0,06464	✓	0,01634	✓
Overlapping Templates Test	0,18705	✓	0,58012	✓	0,473944	✓
Maurer's Universal Statistical Test	0,1921	✓	0,58502	✓	0,7587417	✓
Approximate Entropy Test	0,02435	✓	0,32102	✓	0,6111174	✓
Random-Excursions Test	0,79859	✓	0,60713	✓	0,4888407	✓
Random-Excursions Variant Test	0,48922	✓	0,75212	✓	0,6371215	✓
Serial Test-1	0,24493	✓	0,64047	✓	0,4685653	✓
Serial Test-2	0,24669	✓	0,77561	✓	0,6927195	✓
Linear-Complexity Test	0,34569	✓	0,29519	✓	0,0710091	✓

Tablo 6.2. Rössler Sistemi NIST800-22 test sonuçları

Rössler Sistemi	**Yöntem 1**		**Yöntem 2**		**Yöntem 3**	
İstatistiksel Testler	P-değeri	**Sonuç**	P-değeri	**Sonuç**	P-değeri	**Sonuç**
Frequency (Monobit) Test	0,8587	✓	0,4965	✓	0,0989	✓
Block-Frequency Test	0,8845	✓	0,0821	✓	0,1511	✓
Cumulative-Sums Test	0,5588	✓	0,8883	✓	0,1676	✓
Runs Test	0,2286	✓	0,8772	✓	0,1641	✓
Longest-Run Test	0,5452	✓	0,9623	✓	0,4578	✓
Binary Matrix Rank Test	0,3220	✓	0,9706	✓	0,1823	✓
Discrete Fourier Transform Test	0,9561	✓	0,6009	✓	0,0796	✓
Non-Overlapping Templates Test	0,0118	✓	0,1218	✓	0,1928	✓
Overlapping Templates Test	0,7195	✓	0,9424	✓	0,8178	✓
Maurer's Universal Statistical Test	0,7258	✓	0,2964	✓	0,4460	✓
Approximate Entropy Test	0,8046	✓	0,6067	✓	0,7228	✓
Random-Excursions Test	0,3568	✓	0,4900	✓	0,3034	✓
Random-Excursions Variant Test	0,3234	✓	0,4343	✓	0,3674	✓
Serial Test-1	0,1371	✓	0,1680	✓	0,3798	✓
Serial Test-2	0,7560	✓	0,2006	✓	0,3733	✓
Linear-Complexity Test	0,3854	✓	0,7611	✓	0,26034	✓

Tablo 6.3. Chen Sistemi NIST800-22 test sonuçları

Chen Sistemi	**Yöntem 1**		**Yöntem 2**		**Yöntem 3**	
İstatistiksel Testler	P-değeri	**Sonuç**	P-değeri	**Sonuç**	P-değeri	**Sonuç**
Frequency (Monobit) Test	0,35862	✓	0,83679	✓	0,7520	✓
Block-Frequency Test	0,25588	✓	0,18929	✓	0,23034	✓
Cumulative-Sums Test	0,61647	✓	0,65687	✓	0,48073	✓
Runs Test	0,65332	✓	0,94423	✓	0,03663	✓
Longest-Run Test	0,54472	✓	0,35961	✓	0,23436	✓
Binary Matrix Rank Test	0,20501	✓	0,1806	✓	0,49634	✓
Discrete Fourier Transform Test	0,0325	✓	0,10432	✓	0,18031	✓
Non-Overlapping Templates Test	0,2671	✓	0,0624	✓	0,0332	✓
Overlapping Templates Test	0,57409	✓	0,16621	✓	0,09728	✓
Maurer's Universal Statistical Test	0,42402	✓	0,80093	✓	0,06609	✓
Approximate Entropy Test	0,21038	✓	0,58217	✓	0,66308	✓
Random-Excursions Test	0,9622	✓	0,6624	✓	0,56891	✓
Random-Excursions Variant Test	0,1209	✓	0,49562	✓	0,51515	✓
Serial Test-1	0,19976	✓	0,14742	✓	0,38468	✓
Serial Test-2	0,28172	✓	0,23908	✓	0,85567	✓
Linear-Complexity Test	0,81738	✓	0,42692	✓	0,20124	✓

Tablo 6.4. Kesir dereceli Lorenz Sistemi NIST800-22 test sonuçları

Kesir Dereceli Lorenz Sistemi	**Yöntem 1**		**Yöntem 2**		**Yöntem 3**	
İstatistiksel Testler	P-değeri	**Sonuç**	P-değeri	**Sonuç**	P-değeri	**Sonuç**
Frequency (Monobit) Test	0,54984	✓	0,0268	✓	0,4065	✓
Block-Frequency Test	0,89171	✓	0,6909	✓	0,2070	✓
Cumulative-Sums Test	0,87186	✓	0,0431	✓	0,7784	✓
Runs Test	0,46929	✓	0,0458	✓	0,1120	✓
Longest-Run Test	0,1139	✓	0,6166	✓	0,2374	✓
Binary Matrix Rank Test	0,8626	✓	0,2378	✓	0,5560	✓
Discrete Fourier Transform Test	0,69314	✓	0,1658	✓	0,9415	✓
Non-Overlapping Templates Test	0,02916	✓	0,0646	✓	0,0188	✓
Overlapping Templates Test	0,01659	✓	0,3872	✓	0,6761	✓
Maurer's Universal Statistical Test	0,71419	✓	0,2072	✓	0,7160	✓
Approximate Entropy Test	0,96564	✓	0,2219	✓	0,7425	✓
Random-Excursions Test	0,28161	✓	0,4409	✓	0,3325	✓
Random-Excursions Variant Test	0,37047	✓	0,3560	✓	0,4907	✓
Serial Test-1	0,02469	✓	0,6084	✓	0,8528	✓
Serial Test-2	0,06863	✓	0,4124	✓	0,4675	✓
Linear-Complexity Test	0,99186	✓	0,96811	✓	0,56374	✓

Tablo 6.5. Kesir dereceli Rössler Sistemi NIST800-22 test sonuçları

Kesir Dereceli Rössler Sistemi	**Yöntem 1**		**Yöntem 2**		**Yöntem 3**	
İstatistiksel Testler	P-değeri	**Sonuç**	P-değeri	**Sonuç**	P-değeri	**Sonuç**
Frequency (Monobit) Test	0,3898	✓	0,5823	✓	0,8133	✓
Block-Frequency Test	0,4600	✓	0,5113	✓	0,4710	✓
Cumulative-Sums Test	0,6802	✓	0,2616	✓	0,6457	✓
Runs Test	0,8956	✓	0,2350	✓	0,1056	✓
Longest-Run Test	0,3429	✓	0,5787	✓	0,5032	✓
Binary Matrix Rank Test	0,3906	✓	0,7798	✓	0,2529	✓
Discrete Fourier Transform Test	0,2708	✓	0,8043	✓	0,0344	✓
Non-Overlapping Templates Test	0,0104	✓	0,0614	✓	0,0748	✓
Overlapping Templates Test	0,2135	✓	0,8825	✓	0,6610	✓
Maurer's Universal Statistical Test	0,4410	✓	0,2024	✓	0,2107	✓
Approximate Entropy Test	0,7628	✓	0,2945	✓	0,0066	✓
Random-Excursions Test	0,6028	✓	0,4585	✓	0,5278	✓
Random-Excursions Variant Test	0,6834	✓	0,7227	✓	0,5272	✓
Serial Test-1	0,1590	✓	0,0249	✓	0,5927	✓
Serial Test-2	0,0677	✓	0,0574	✓	0,7718	✓
Linear-Complexity Test	0,6055	✓	0,9978	✓	0,3605	✓

Kaotik Rasgele Sayı Üreteci programı ile üretilen Lorenz, Rössler ve Chen kaotik sistemleri NIST800-22 testine tabi tutulmuştur. Yukarıdaki tablolarda bunların detaylı test sonuçları verilmiştir. Burada bu sistemler standart parametre ve başlangıç şartlarına göre başlatılmış ve en düşük anlamlı (LSB) bitlerin seçileceği blok uzunluğu (hassasiyet) ise 8 ve 16 arasında seçilmiştir. Kesir dereceli ve kesir dereceli olmayan olarak üretilen bu sayılar NIST800-22 testinin 16'sından da başarıyla geçmişlerdir.

Tasarımda bulunan diğer bazı kaotik sistemlerin NIST800-22 test sonuçları da aşağıdaki tablolar da verilmiştir.

Tablo 6.6. Tasarımda bulunan diğer bazı kaotik sistemlerin NIST800-22 test sonuçları (8 Bit LSB)

	Yöntem 1		**Yöntem 2**		**Yöntem 3**	
Kaotik Sistemler	RK4	Kesir Dereceli	RK4	Kesir Dereceli	RK4	Kesir Dereceli
Lorenz	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**
Pehlivan	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	Başarısız[3]	Bşarısız[6]
Rossler	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**
VanDerPol	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	**Başarılı**	Başarısız[3]
Labyrinth	**Başarılı**	Başarısız[1]	**Başarılı**	**Başarılı**	Başarısız[6]	Başarısız[3]
Rucklidge	**Başarılı**	**Başarılı**	Başarısız[1]	**Başarılı**	Başarısız[4]	Başarısız[2]
Rikitake	**Başarılı**	Başarısız[2]	**Başarılı**	Başarısız[2]	Başarısız[4]	Başarısız[6]
Difflorenz	Başarısız[2]	Başarısız[2]	**Başarılı**	**Başarılı**	Başarısız	Başarısız[5]
Chen	**Başarılı**	Başarısız	**Başarılı**	Başarısız	**Başarılı**	Başarısız
Altın Oran D.	**Başarılı**	Başarısız	**Başarılı**	Başarısız	Başarısız[1]	Başarısız
Aizawa	Başarısız[1]	**Başarılı**	**Başarılı**	Başarısız[5]	Başarısız[5]	Başarısız[6]

[1] 16 testte 14 Başarılı
[2] 16 testte 13 Başarılı
[3] 16 testte 12 Başarılı
[4] 16 testte 11 Başarılı
[5] 16 testte 10 Başarılı
[6] 16 testte 8 Başarılı

Yukarıdaki tabloda (Tablo 6.6.) tasarımda bulunan diğer bazı kaotik sistemlerin NIST800-22 test sonuçları verilmiştir. NIST800-22'de bulunan 16 testin tümünden başarılı bir şekilde geçen sistemler "**Başarılı**" olarak, en az bir tanesinden geçemeyenler ise "Başarısız" olarak tabloda sunulmuştur. Burada başarısız olarak sunulan sistemlerin 16 testin kaçından geçtikleri dipnot olarak verilmiştir. Başarısız

olarak verilen sistemlerin büyük çoğunluğu bu 16 testin çok azından geçememiştir. Ayrıca bir yöntem ve çözüm algoritmalarının birinden veya birkaçından geçemeyen sayıların diğer yöntem veya çözüm algoritmaları değiştirildiğinde geçebildiği gözlenmiştir. Yine aynı şekilde tabloda sunulmamış olsa da testten geçemeyen kaotik sistemlerin çıkış değişkenleri değiştirildiğinde testten geçebildiği de gözlemlenmiştir. Örneğin bir kaotik sistemin x değişkeni testlerin birinden veya birkaçından geçemediğinde y veya z değişkenlerinin testlerin tümünden geçebildiği anlaşılmıştır.

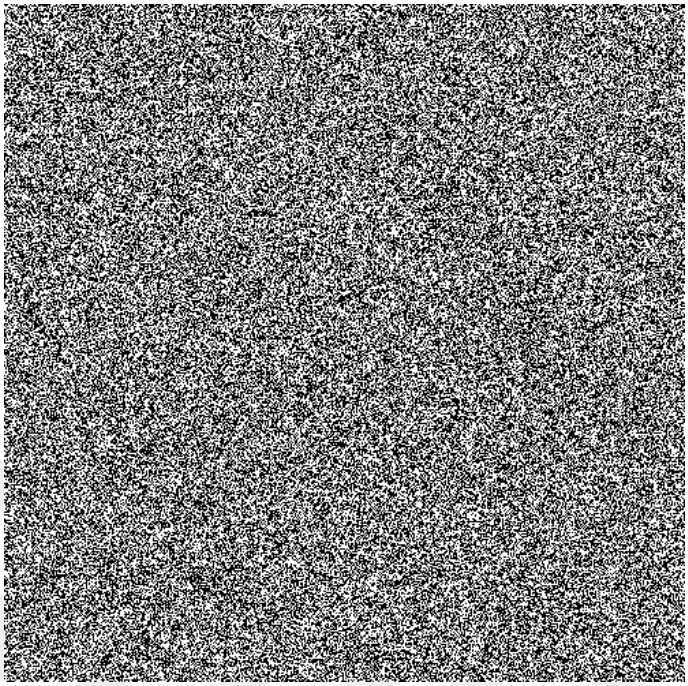
Tablo 6.7. Lorenz'den farklı hassasiyet (LSB) değerlerinde oluşturulan sayıların NIST800-22 test sonuçları

İstatistiksel Testler	**1 Bit**	**4 Bit**	**8 Bit**	**10 Bit**	**12 Bit**	**14 Bit**	**16 Bit**	**20 Bit**	**22 Bit**	**25 Bit**	**28 Bit**	**32 Bit**
Frequency (Monobit) Test	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X	X
Block-Frequency Test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X
Cumulative-Sums Test	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X	X
Runs Test	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X	X
Longest-Run Test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓
Binary Matrix Rank Test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X
Discrete Fourier Transform	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	X	X
Non-Overlapping Temp	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X	X
Overlapping Templates	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X
Maurer's Universal	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X
Approximate Entropy Test	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X
Rad-Exc Test	✓	✓	✓	✓	✓	X	✓	X	X	X	X	X
Rand-Exc Variant Test	✓	✓	✓	✓	✓	X	✓	X	X	X	X	X
Serial Test-1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X
Serial Test-2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Linear-Complexity Test	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X

Ayrıca farklı hassasiyet değerlerine göre oluşturulan rasgele sayı dizilerinin NIST800-22 istatistiksel test sonuçları da yukarıdaki tabloda (Tablo 6.7) verilmiştir. Buna göre en düşük anlamlı ilk 12 bit seçildiği takdirde üretilen sayıların testlerden başarıyla geçtiği, 14-20 bit arasından seçildiğinde testlerden bazen geçebildiği, 20 bit'ten fazlası seçildiğinde ise testlerden geçemediği görülmüştür.

NIST800-22'de bulunan 16 testin birinden veya birkaçından geçemeyen 1 milyon adet binary rasgele sayıların 1000x1000 şeklinde resim olarak görselleştirilmesi aşağıdaki şekillerde verilmiştir. Burada testlerden geçemeyen sayıların dahi sözde rasgele sayı

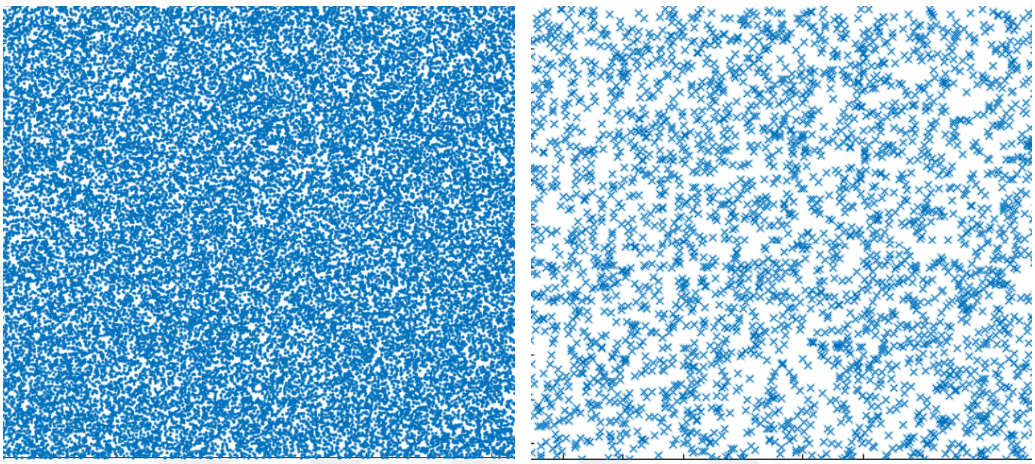
üreteçleri tarafından üretilen sayılara göre daha tahmin edilemez ve tekrarlanmayan sayılardan oluştuğu görülmektedir.



Şekil 6.1. Binary rasgele sayıların 1000x1000 görselleştirilmesi

Şekil 6.2. Yakınlaştırılmış görsel

Tasarlanan kaotik rasgele sayı üreteci program ile üretilen tüm rasgele sayı dizilerinin görsel sonuçları Şekil 6.1'deki gibi olur. Buradaki gibi üretilen bit dizileri resim olarak sunulduğunda veya bu bit dizilerinden elde edilen sayılar koordinat olarak girilip her koordinata bir nokta veya "x" işareti koyulduğunda (Şekil 6.4) ENT testi Pi için Monte Carlo değeri hesaplaması yapılabilir.



Şekil 6.3. Üretilen rasgele sayı değerlerinin koordinat olarak işaretlenmesi ve dağılımları

Kör bir dart oyuncusunun içine tam sığdırılmış bir daire olan kare bir dart tahtasına 1 milyon kez atış yaptığını düşündüğümüzde kare içindeki dartların toplam sayısı ile daire içine denk gelen dartların sayısının oranı $\frac{1}{4}\pi$ olmalıdır. Bu örnekteki gibi üretilen sayılar kullanılarak MxM bir kare alanda dartların saplandığı koordinatlar oluşturulduğunda bu alana saplanan dartların sayısı ile bu alan içine sığdırılmış dairenin içine saplanan dartların sayısı oranları $\frac{1}{4}\pi$ olmalıdır.

Aşağıdaki tabloda (Tablo 6.8) tasarımda kullanılan kaotik sistemlerin farklı yöntemlerle elde edilen rasgele sayı dizilerinin koordinat olarak kullanılmasıyla elde edilen dart görselleri için ENT testi Monte Carlo değerlerinin olması gereken değere oranları verilmiştir.

Tablo 6.8. Tasarımda bulunan diğer bazı kaotik sistemlerin ENT – Monte Carlo test sonuçları

	Yöntem 1		Yöntem 2		Yöntem 3	
Kaotik Sistemler	**RK4**	**Kesir Dereceli**	**RK4**	**Kesir Dereceli**	**RK4**	**Kesir Dereceli**
Lorenz	99,930%	99,999%	99,992%	99,981%	99,988%	99,999%
Pehlivan	99,927%	99,936%	99,985%	99,945%	99,982%	99,947%
Rossler	99,997%	99,969%	99,966%	99,936%	99,928%	99,908%
VanDerPol	99,793%	99,973%	99,980%	99,988%	99,974%	99,977%
Labyrinth	99,963%	99,870%	99,855%	99,964%	99,932%	99,976%
Rucklidge	99,964%	99,951%	99,967%	99,907%	99,944%	99,860%
Rikitake	99,941%	99,915%	99,982%	99,973%	99,952%	99,970%
Difflorenz	99,969%	99,968%	99,988%	99,822%	99,975%	99,933%
Chen	99,942%	99,965%	99,997%	99,966%	99,968%	99,860%
Altın Oran D.	99,974%	98,041%	99,947%	96,724%	99,998%	97,832%
Aizawa	99,982%	99,921%	99,799%	99,936%	99,959%	99,980%

Burada ENT testi Pi için Monte Carlo değerlerinin $\pi/4$ değerine ne kadar yaklaştıklarının oranları sunulmuştur. Bu değere yaklaşıklık 94%'in üzerinde (izin verilen hata %6) olan tüm oranlar için ENT- Pi için Monte Carlo rasgelelik testinden başarıyla geçmiş sayılmaktadır (Walker, 2008). Tabloda tüm değerlerin %94'ün üzerinde olduğu görülmektedir.

BÖLÜM 7. SONUÇ VE ÖNERİLER

Bu tez çalışmasında kaos tabanlı kesirli ve kesirli dereceden olmayan kaotik sistemler yardımıyla ve dört farklı yöntem kullanarak, kullanıcı dostu bir arayüz tasarlanmış ve bu arayüz programı ile rasgele sayı üreteci yapılarak, mikrobilgisayar tabanlı kullanımı gerçekleştirilmiştir. Rasgele sayıların güvenilirlikleri için uluslararası alanda kabul görmüş NIST-800-22, ENT testleri gibi farklı rasgelelik testleri kullanılarak gerekli test işlemleri yapılmıştır.

Çalışmada ayrık ve sürekli zamanlı farklı kaotik sistemlerin kesirli ve kesirli olmayan dereceli türev yöntemleri ile numerik çözümleri, denge noktaları ve kararlılık analizleri, faz uzayları, zaman serisinde başlangıç şartlarına hassas bağımlılık, Lyapunov üstelleri ve çatallanma diyagramları hakkında kapsamlı araştırma ve bunların gerçekleştirmeleri yapılmıştır. Ayrıca literatürde sunulan, rasgele sayı üreteç tasarım yöntemleri ve uluslararası kabul görmüş rasgelelik test yöntemleri incelenmiştir. Kaotik rasgele sayı üretiminde kullanılan bazı farklı yöntemler sunulmuştur. Rasgelelik testleri, analizleri ve bunların gerçekleştirilmesi yapılmıştır. Böylece kriptoloji ve güvenli haberleşme sistemleri, istatistiksel örneklemeler, bilgisayar simülasyonları, rasgeleliğe dayalı tasarımlar ve tahmin edilemeyen sonuçlar üreten diğer alanlarda büyük önemi olan rasgele sayı üreteçlerinin farklı yöntemler ile elde edilmesi ve bunun da tasarlanan kullanıcı arayüz programı ile gerçekleştirilmesi sağlanmıştır.

Tasarlanan arayüz programı, kaotik rasgele sayı üretiminde kullanıcılara birçok kolaylık sağlamıştır. Üretilecek rasgele sayıların elde edilişi, ikili veya onlu olarak txt biçiminde kaydedilmesine veya bir sinyal olarak bir donanıma (Raspberry Pi) gönderilmesine, mobil olarak kullanıma imkân sağlanmıştır. Arayüz programında tanımlanan kaotik sistemlerin, kullanıcı tercihine göre seçilebilmesi veya daha sonra başka sistemlerin de eklenebilmesine izin verilen kolay ve anlaşılır programı sayesinde

birçok farklı rassal sayı üretimi gerçekleştirilmiştir. Yine tasarlanan arayüz programından girilen değerler (başlangıç şartları, kesir dereceleri, iterasyon sayısı, hassasiyet, kaotik çıktı değişkeni) veya seçilen ayarlar sayesinde (yöntem, algoritma, çıktı biçimi ve çıktı birimi) ve kaotik sistemlerin başlangıç şartlarına olan hassas bağımlılık özelliklerinden de yararlanılarak sonsuz çeşitlilikte rasgele sayı üretimi gerçekleştirilebilir olduğu görülmüştür. Böylece, tasarlanan arayüz programı sayesinde istenilen yöntem ve istenilen parametre değerlerinde kaotik sistemler seçilerek kolaylıkla rasgele sayı üretimi gerçekleştirilebilmiştir.

Tasarlanan kaos tabanlı rasgele sayı üreteci ile üretilen sayıların rasgelelikleri incelenmiş, istatistiksel rasgelelik test programlarından test edilmiştir. Bu rasgele sayı dizilerinin NIST 800-22 test sonuçları tablolar halinde gösterilmiştir. Ayrıca üretilen bu sayı dizileri görselleştirilerek dağılımları incelenmiş ve tekrarlanmayan rasgele dağılımlara sahip oldukları görülmüştür.

Bu tez çalışmasında önerilen kaotik sistemler ile, tüm yöntem ve çözüm algoritma ayarlarında rasgele sayı değerleri elde edilebilmiştir. Bunların yanında istatistiksel rasgelelik testlerinin birinden veya birkaçından geçemeyen kaotik sistemler de tasarımda sunulmuştur. Testlerden geçemeyen kaotik sistemlerin testlerden geçebilmesini sağlamak için karıştırıcı son işlemler eklenebilir. Tasarımda üretilen sayı değerleri için XOR veya Von Neumann gibi son işlem metotları yardımı ile üretilen sayı değerlerinin rasgelelikleri artırılabilir. Ayrıca gerçekleştirilen tasarım faklı işlemciler ve faklı dillerle programlanarak bit üretim hızları yükseltilebilir.

KAYNAKLAR

Akgul, A., Moroz, I., Pehlivan, I., & Vaidyanathan, S. (2016). A new four-scroll chaotic attractor and its engineering applications. Optik-International Journal for Light and Electron Optics, 127(13), 5491-5499.

Akram, R. N., Markantonakis, K., & Mayes, K. (2012, May). Pseudorandom number generation in smart cards: an implementation, performance and randomness analysis. In New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on (pp. 1-7). IEEE.

Alani, M. M. (2010). Testing randomness in ciphertext of block-ciphers using DieHard tests. Int. J. Comput. Sci. Netw. Secur, 10(4), 53-57.

Alçın, M., Pehlivan, İ., & Koyuncu, İ. (2016). Hardware design and implementation of a novel ANN-based chaotic generator in FPGA. Optik-International Journal for Light and Electron Optics, 127(13), 5500-5505.

Arslan, C., Pehlivan, İ., Varan, M., & Akgül, A. (2017, September). FitzHugh-Nagumo (FHN) Nöron Modelinin Dinamik Analizleri, Simülasyon ve Analog Devre Gerçeklemesi. In 5th International Symposium on Innovative Technologies in Engineering and Science 29-30 September 2017 (ISITES2017 Baku-Azerbaijan).

Ateş, E. Ö. (2005). Chaotic Oscillator Based Random Bit Generator (Doctoral dissertation).

Avaroğlu, E. (2014). Donanım Tabanlı Rasgele Sayı Üretecinin Gerçekleştilmesi (Doctoral dissertation, Ph. D, Fırat Üniversitesi, Elâzığ, Türkiye).

Avaroğlu, E., & Türk, M. (2013) Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki etkisinin İncelenmesi, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara-Türkiye, 291-294.

Bayam, F. (2005). Chaotic oscillator based random number generator. İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi.

Bolotin, Y., Tur, A., & Yanovsky, V. (2009). Chaos: Concepts, Control and Constructive Use. Springer, 19-34.

Bucci, M., Germani, L., Luzzi, R., Tommasino, P., Trifiletti, A., & Varanonuovo, M. (2003). A high-speed IC random-number source for smartcard

microcontrollers. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 50(11), 1373-1380.

Cafagna, D. (2007). Fractional calculus: A mathematical tool from the past for present engineers [Past and present]. IEEE Industrial Electronics Magazine, 1(2), 35-40.

Cartwbight, M. L. (1960). Balthazar van der Pol. Journal of the London Mathematical Society, 1(3), 367-376.

Chen, G., & Ueta, T. (1999). Yet another chaotic attractor. International Journal of Bifurcation and chaos, 9(07), 1465-1466.

Chua, L. O. (2007). Chua circuit. Scholarpedia, 2(10), 1488. ISO 690

Crawford, J. D. (1991). Introduction to bifurcation theory. Reviews of Modern Physics, 63(4), 991.

Cruz-Hernández, C. (2004). Synchronization of time-delay Chua's oscillator with application to secure communication. Nonlinear Dynamics and Systems Theory, 4(1), 1-13.

Çiçek, S., (2016). Yeni bir kaotik sistem ile FPGA tabanlı bir kaotik haberleşme sistemi tasarımı ve gerçekleştirilmesi. Doktora Tezi, Sakarya Üniversitesi.

Daemen, J., & Rijmen, V. (2013). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

Demirkol, A. Ş. (2007). Kaotik osilatör girişli ADC tabanlı rasgele sayı üreteci. İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Haberleşme Mühendisliği Bölümü, Elektronik Mühendisliği Programı, Yüksek Lisans Tezi.

Deneubourg, J. L., & Goss, S. (1989). Collective patterns and decision-making. Ethology Ecology & Evolution, 1(4), 295-311.

Ditto, W. L., & Pecora, L. M. (1993). Mastering chaos. Scientific American, 269(2), 78-84.

Emiroğlu, S., & Uyaroğlu, Y. (2012). Dynamical analysis and control of chaos in Vilnius chaotic oscillator circuit. ScientiÆc Computing in Electrical Engineering, SCEE2012, Zurich, Switzerland, 151-152.

Erat, M. (2008). FPGA tabanlı, PCI arayüzlü, gerçek zamanlı rasgele sayı üreteci test sistemi tasarımı ve uygulamaları. Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Mühendisliği Bölümü, Doktora Tezi.

Ergün, S., & Özog, S. (2007). Truly random number generators based on a non-autonomous chaotic oscillator. AEU-International Journal of Electronics and Communications, 61(4), 235-242.

Fraga, L. G., Tlelo-Cuautle, E., Carbajal-Gómez, V. H., & Munoz-Pacheco, J. M. (2012). On maximizing positive Lyapunov exponents in a chaotic oscillator with heuristics. Revista mexicana de física, 58(3), 274-281.

Giannakopoulos, K., Deliyannis, T., & Hadjidemetriou, J. (2002). Means for detecting chaos and hyperchaos in nonlinear electronic circuits. In Digital Signal Processing, 2002. DSP 2002. 2002 14th International Conference on (Vol. 2, pp. 951-954). IEEE.

Gleick, J. (1997). Kaos Yeni Bir Bilim Teorisi, (Çev: F. Üçcan). Tübitak Popüler Bilim Kitapları, Ankara.

Glendinning, P. (1994). Stability, instability and chaos: an introduction to the theory of nonlinear differential equations (Vol. 11). Cambridge university press.

Gökyıldırım, A. (2016). Enerji iletim hatlarında geçici olayların z dönüşümü tekniği ile incelenmesi. Doktora Tezi, Sakarya Üniversitesi.

Güler, H., & Kaya, T. (2016). Parça Parça Lineer Memristor Tabanlı Chua Osilatorunun LabVIEW'de Gerçekleştirilmesi.

Gündüz, G., & Gündüz, M. (2002). Kargaşa, kaos ve şekil oluşumları. METU Press.

Güven, P. (2006). Otonom olmayan kaotik sistemlerde rasgele sayı üretiminin incelenmesi. İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Haberleşme Mühendisliği, Yüksek Lisans Tezi

Hanbay, D., Türkoğlu, İ., & Demir, Y. (2007). Chua Devresinin yapay sinir ağı ile modellenmesi. Fırat Üniv. Fen ve Müh. Bil. Dergisi, 19(1), 67-72.

Hançerlioğullari, A. (2006). Monte Carlo Simülasyon Metodu ve MCNP Kod Sistemi. Kastamonu Eğitim Dergisi.

Hayes, S., Grebogi, C., & Ott, E. (1993). Communicating with chaos. Physical review letters, 70(20), 3031.

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. In The Theory of Chaotic Attractors (pp. 94-102). Springer, New York, NY.

Holmes, P. (1990). Poincaré, celestial mechanics, dynamical-systems theory and "chaos". Physics Reports, 193(3), 137-163.

Ito, K. (1980). Chaos in the Rikitake two-disc dynamo system. Earth and Planetary Science Letters, 51(2), 451-456.

Jost, J. (2005). Dynamical Systems: Examples Of Complex Behaviour (Universitext).

Kaçar, S. (2016). Analog circuit and microcontroller based RNG application of a new easy realizable 4D chaotic system. Optik-International Journal for Light and Electron Optics, 127(20), 9551-9561.

Kaçar, S., Akgül, A., Ergüzel, A. T., Öztürk, M. M., & Sevin, A. (2015). Design of a Web Interface for Fractional Chaotic Systems.

Kahyaoğlu, M. B., & Süleyman, İ. Ç. (2015). Kaos Teorisi Çerçevesinde Bireysel Yatırımcı Davranışının Analizi. The Journal Of Business Science, 3(1), 38-51.

KARCI, A. (2015). KESİR DERECELİ TÜREVİN YENİ YAKLAŞIMININ ÖZELLİKLERİ. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 30(3).

Kauffman, S. A. (1993). The Origins of Order Oxford University Press. New York.

Kennedy, M., & Chua, L. (1986). Van der Pol and chaos. IEEE Transactions on Circuits and Systems, 33(10), 974-980.

Kia, B. (2011). Chaos computing: from theory to application. Arizona State University.

Kilbas, A. A., Srivastava, H. M., & Trujillo, J. J. (2006). Theory and applications of fractional differential equations. North-Holland mathematics studies.

Knuth, D. E. (1998). The art of computer programming, 2: seminumerical algorithms, Addision Wesley. Reading, MA.

Kocarev L. ve Jakimoski G. (2003). Pseudorandom Bits Generated by Chaotic Maps, IEEE Trans. Circuits and Systems I, 50, 123-26.

Koçal, O. H., Yuruklu, E., & Avcibas, I. (2008). Chaotic-type features for speech steganalysis. IEEE Transactions on Information Forensics and Security, 3(4), 651-661.

Kolumbán, G., Kennedy, M. P., & Chua, L. O. (1998). The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 45(11), 1129-1140.

Korkmaz, M. (2013). Kesirli dereceden PI D denetleyicilerin, tasarımı, uygulaması ve karşılaştırılması (Doctoral dissertation, Selçuk Üniversitesi Fen Bilimleri Enstitüsü).

Kumar, U., & Shukla, S. K. (1989). Analytical study of inductor simulation circuits. Active and Passive Electronic Components, 13(4), 211-227.

Kurt, E., Kasap, R. (2011). Karmaşanın bilimi kaos. Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti., Ankara, 1-10.

Küçük, G. D. (2014). Kesirli Mertebeden Kısmi Diferansiyel Cebirsel Denklemlerin Farklı Metotlarla Nümerik Çözümü (Doctoral Dissertation).

Li, C., & Chen, G. (2004). Chaos and hyperchaos in the fractional-order Rössler equations. Physica A: Statistical Mechanics and its Applications, 341, 55-61.

Li, C., & Yan, J. (2007). The synchronization of three fractional differential systems. Chaos, Solitons & Fractals, 32(2), 751-757.

Linear Congruential Random Number Generator, (2008). http://www.cse.msu.edu/~nandakum/nrg/Tms/Probability/Probgenera tor.htm

Lorenz, E. N. (1963). Deterministic nonperiodic flow. Journal of the atmospheric sciences, 20(2), 130-141.

Lu, J. G., & Chen, G. (2006). A note on the fractional-order Chen system. Chaos, Solitons & Fractals, 27(3), 685-688.

Lynch, S. (2007). Dynamical systems with applications using Mathematica (pp. 111-123). Boston: Birkhäuser.

Madan, R. N. (Ed.). (1993). Chua's circuit: a paradigm for chaos (Vol. 1). World Scientific

Mamat, M., Sanjaya, M. W. S., & Maulana, D. S. (2013). Numerical simulation chaotic synchronization of Chua circuit and its application for secure communication. Applied Mathematical Sciences, 7(1), 1-10.

Mathai, A. M., Saxena, R. K., & Haubold, H. J. (2009). The H-function: theory and applications. Springer Science & Business Media.

Matsumoto, T., Chua, L., & Komuro, M. (1985). The double scroll. IEEE Transactions on Circuits and Systems, 32(8), 797-818.

May, R. M. (1976). Simple mathematical models with very complicated dynamics. Nature, 261(5560), 459

McKinney, E. H. (1966). Generalized birthday problem. The American Mathematical Monthly, 73(4), 385-387.

Metropolis, N. (1985). Monte Carlo: in the beginning and some great expectations. In Monte-Carlo Methods and Applications in Neutronics, Photonics and Statistical Physics (pp. 62-70). Springer, Berlin, Heidelberg.

Mobayen, S., Volos, C. K., Kaçar, S., & Çavuşoğlu, Ü. (2018). New class of chaotic systems with equilibrium points like a three-leaved clover. Nonlinear Dynamics, 91(2), 939-956.

Modanlı, M. (2018). Kesirli telegraf kısmi diferansiyel denklemlerin fark şeması metodu ile nümerik çözümü. Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi.

National Institute of Standard and Technology, A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications, NIST800-22, (2001). http://csrc.nist.gov/rng/SP800- 22b.pdf

Özer, A. B., (2005). Elektriksel sürücü sistemlerinde doğrusal olmayan olguların kaotik analizi ve yumuşak hesaplama yöntemleri ile denetimi. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Bölümü, Doktora Tezi.

ÖZOĞUZ, S., ZEKİ, A. (2008). Sürekli zamanlı kaotik sistemlerin tümleşik olarak gerçeklenmesi ve rasgele sayı üretiminde kullanılması. Tübitak Projesi Sonuç Raporu (106E093).

Pehlivan, İ., & Uyaroglu, Y. (2007). Rikitake attractor and its synchronization application for secure communication systems. Journal of Applied Sciences, 7(2), 232-236.

Pehlivan, İ., & Uyaroğlu, Y. (2012). A new 3D chaotic system with golden proportion equilibria: Analysis and electronic circuit realization. Computers & Electrical Engineering, 38(6), 1777-1784.

Pehlivan, İ., (2007). Yeni kaotik sistemler: Elektronik devre gerçeklemeleri, senkronizasyon ve güvenli haberleşme uygulamaları. Doktora Tezi, Sakarya Üniversitesi.

Petráš, I. (2011). Fractional-order nonlinear systems: modeling, analysis and simulation. Springer Science & Business Media.

Petrıe, Cs., Connelly, Ja., A. (2000). Noise-Based Ic Rng For Applications İn Cryptography. Ieee Trans. On Circuits And Syst. I: Fundamental Theory And Appl., 47(5):615–621.

Podlubny, I. (1999). Fractional-order systems and PI/sup/spl lambda//D/sup/spl mu//-controllers. IEEE Transactions on automatic control, 44(1), 208-214.

POLKING JC. (2017). Download Odesolve.m, Rice University, http://math.rice.edu/~dfield/, 2017

Rasmussen, S., Knudsen, C., Feldberg, R., & Hindsholm, M. (1990). The coreworld: Emergence and evolution of cooperative structures in a computational chemistry. Physica D: Nonlinear Phenomena, 42(1-3), 111-134.

Rene, D., (1998). Random testing of digital circuits: Theory and application, Dekker Inc., New York.

Rikitake, T. (1958, January). Oscillations of a system of disk dynamos. In Mathematical Proceedings of the Cambridge Philosophical Society (Vol. 54, No. 1, pp. 89-105). Cambridge University Press.

Robert Keim, (2016) “Inductor Out, Op-Amp In: An Introduction to Second-Order Active Filters” https://www.allaboutcircuits.com/technical-articles/inductor-out-op-amp-in-an-introduction-to-second-order-active-filters/

Robinson, S. O. and Dessart, D. J. (1998). Yearbook (National council of teachers of mathematics), pp. 243-50, NCTM, USA.

Ross B. (editor), (1975). Fractional Calculus and Its Applications, Proceedings of the International Conference Held at the University of New Haven, June 1974, Springer Verlag.

Rössler, O. E. (1976). An equation for continuous chaos. Physics Letters A, 57(5), 397-398.

Rucklidge, A. M. (1992). Chaos in models of double convection. Journal of Fluid Mechanics, 237, 209-229.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-Allen and Hamilton Inc Mclean Va.Sandri, M. (1996). Numerical calculation of Lyapunov exponents. Mathematica Journal, 6(3), 78-84.

Schoukens, J., Pintelon, R., van der Ouderaa, E. and Renneboog, J., (1988). Survey of excitation signals for FFT based signal analyzers, IEEE Transactions on Instrumentation and Measurements. Vol. 37, no. 3, pp. 342-352.

Siderskiy, V., & Kapila, V. (2014). Parameter matching using adaptive synchronization of two Chua's oscillators. International Journal of Bifurcation and Chaos, 24(11), 1430032.

Sprott, J. C., & Chlouverakis, K. E. (2007). Labyrinth chaos. International Journal of Bifurcation and Chaos, 17(06), 2097-2108.

Sobotka, J. and Zeman, V. (2011). "Design of the true random numbers generator", Elektrorevue, 2(3):1-6.

Strogatz S. (2000). Non-linear Dynamics and Chaos: With applications to Physics, Biology, Chemistry and Engineering. Perseus Books.

Strogatz, S. H. (2014). Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. Hachette UK.

Sunar, B., Martin, W. J., & Stinson, D. R. (2007). A provably secure true random number generator with built-in tolerance to active attacks. IEEE Transactions on computers, 56(1).

Tamasevicius, A. (2002). Generation of Very High and Ultrahigh Frequency Broadband Chaotic Signals Using Delay Line Oscillators. SEMICONDUCTOR PHYSICS INST VILNIUS (LITHUANIA).

Tavas, V. (2011). Tümleştirmeye uygun rasgele sayı üreteçleri. İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Haberleşme Mühendisliği Bölümü, Elektronik Mühendisliği Programı, Doktora Tezi, 2011.

Thomas, R. (1999). Deterministic chaos seen in terms of feedback circuits: Analysis, synthesis," labyrinth chaos". International Journal of Bifurcation and Chaos, 9(10), 1889-1905.

Toyran, M. (2007, June). Efficient Use of Random Numbers. In Signal Processing and Communications Applications, 2007. SIU 2007. IEEE 15th (pp. 1-4). IEEE.

Tsumoto, K., Ueta, T., Yoshinaga, T., & Kawakami, H. (2012). Bifurcation analyses of nonlinear dynamical systems: From theory to numerical computations. Nonlinear Theory and Its Applications, IEICE, 3(4), 458-476.

Turk, M., & Ata, F. (2002). Performance analysis of adaptive controllers on chaotic parameter modulation and variant channel gain. In Circuits and Systems for Communications, 2002. Proceedings. ICCSC'02. 1st IEEE International Conference on (pp. 283-286). IEEE.

Uçar, A., Türk, M. ve Ata, F. (2001) A Practical Realization of Chaos Synchronization For Transmitting Information‖, The 32nd International Scientific Symposium of the Defense Research Agency, vol.4, Bucharest–Romania, pp.81-88.

Van der Pol, B., & Van Der Mark, J. (1927). Frequency demultiplication. Nature, 120(3019), 363,364.

Van Wyk, M. A., & Steeb, W. H. (2013). Chaos in electronics (Vol. 2). Springer Science & Business Media.

Viniotis, Y. (1998). Probability and random processes for electrical engineers (No. 519.2 V761p Ej. 1 024995). WCB/McGraw-Hill,.

Walker, J. (2008). ENT: a pseudorandom number sequence test program. Software and documentation available at/www. fourmilab. ch/random/S.

Wolf, A., Swift, J. B., Swinney, H. L., & Vastano, J. A. (1985). Determining Lyapunov exponents from a time series. Physica D: Nonlinear Phenomena, 16(3), 285-317.

Yalçın M., Suykens J. ve Vandewalle J. (2004). True Random Bit Generation from a Double Scroll Attractor, IEEE Trans. Circuits Syst. I, 51, 1395-1404.

Yamaçlı, V., Abacı, K., & Köse, E. Chua Devresinin Gerçeklenmesi ve Simülasyonu. In 6th International Advanced Techlogies Symposium, Elazığ-Türkiye (pp. 82-86).

Yang, T., & Chua, L. O. (1996). Secure communication via chaotic parameter modulation. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 43(9), 817-819.

Yardım, F. E., & Afacan, E. (2010). Lorenz-Tabanlı Diferansiyel Kaos Kaydırmalı Anahtarlama (Dcsk) Modeli Kullanılarak Kaotik Bir Haberleşme Sisteminin

Simülasyonu. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 25(1).

Yıldırım, S. (2012). A true random number generator in FPGA for cryptographic applications. Orta Doğu Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik ve Elektronik Mühendisliği, Yüksek Lisans Tezi.

Yıldırım, S., & Bazlamaçcı, C. F. (2012). A True Random Number Generator and Test Platform Built in FPGA. In 5th Internaitonal Conference on Information Security & Cryptology, Ankara/Turkey (pp. 262-267).

Yonemoto, K., & Yanagawa, T. (2007). Estimating the Lyapunov exponent from chaotic time series with dynamic noise. Statistical Methodology, 4(4), 461-480.

Zhun, H., & Hongyi, C. (2001). A truly random number generator based on thermal noise. In ASIC, 2001. Proceedings. 4th International Conference on (pp. 862-864). IEEE.

ÖZGEÇMİŞ

Coşkun Arslan, 25.04.1993'de Tokat/Niksar'da doğdu. İlk, orta ve lise eğitimini Bursa'da tamamladı. 2011 yılında Hürriyet Anadolu Teknik Lisesi'nden mezun oldu. 2011 yılında başladığı Sakarya Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nü 2016 yılında bitirdi. 2016 yılında Sakarya Üniversitesi Elektrik Elektronik Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı. 2017-2018 yılında Hendek Mesleki ve Teknik Anadolu Lisesi'nde Elektrik Elektronik Öğretmeni olarak görev yaptı.