

**T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**KAOS KAYNAKLI VE ADC TABANLI ÖZGÜN
GERÇEK RASGELE SAYI ÜRETEÇLERİNİN
TASARIM VE GERÇEKLENMESİ**

DOKTORA TEZİ

Selçuk COŞKUN

**Enstitü Anabilim Dalı : ELEKTRONİK VE BİLGİSAYAR
EĞİTİMİ**
Enstitü Bilim Dalı : ELEKTRONİK
Tez Danışmanı : Doç. Dr. İhsan PEHLİVAN

Ocak 2017

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

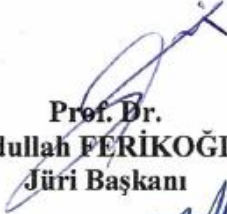
**KAOS KAYNAKLI VE ADC TABANLI ÖZGÜN
GERÇEK RASGELE SAYI ÜRETEÇLERİNİN
TASARIM VE GERÇEKLENMESİ**


DOKTORA TEZİ


Selçuk COŞKUN

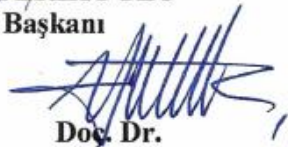
Enstitü Anabilim Dalı : **ELEKTRONİK VE
BİLGİSAYAR EĞİTİMİ**

Bu tez 09/01/2017 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.


Prof. Dr.
Abdullah FERİKOĞLU
Jüri Başkanı


Doç. Dr.
İhsan PEHLİVAN
Üye


Doç. Dr.
Yılmaz UYAROĞLU
Üye


Doç. Dr.
Hayriye KORKMAZ
Üye


Yrd. Doç. Dr.
Mesud KAHRİMAN
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.

Selçuk COŞKUN

09.01.2017

TEŐEKKÜR

Tez alıőması boyunca, bilgi birikimi ve tecrübeleriyle bana yardımcı olan aynı zamanda, maddi ve manevi her türlü desteęi için sayın danışmanım ve deęerli hocam Do. Dr. İhsan PEHLİVAN'a en içten teşekkürlerimi sunarım.

Tez alıőmalarım sırasında, maddi ve manevi desteęi için aileme, benden bir an olsun yardımlarını esirgemeyen kardeşim Sezgin COŐKUN'a, motivasyon kaynaklarım sevgili eşim Betül COŐKUN ve kızım Ela COŐKUN'a teşekkür ederim.

İÇİNDEKİLER

TEŞEKKÜR.....	i
İÇİNDEKİLER.....	ii
SİMGELER VE KISALTMALAR LİSTESİ.....	v
ŞEKİLLER LİSTESİ.....	ix
TABLolar LİSTESİ.....	xii
ÖZET.....	xiii
SUMMARY.....	xiv

BÖLÜM 1.

GİRİŞ.....	1
1.1. Literatür Taraması.....	3
1.2. Tezin Amacı.....	6
1.3. Tezde İzlenecek Yol.....	7

BÖLÜM 2.

TEMEL KAVRAMLAR.....	9
2.1. Rasgele Sayı Üreteçleri (RSÜ).....	9
2.1.1. Sözde rasgele sayı üreteçleri (SRSÜ).....	10
2.1.2. Gerçek rasgele sayı üreteçleri (GRSÜ).....	13
2.1.3. İstatistiksel rasgele sayı testleri.....	15
2.1.4. FIPS 140-1 testi.....	16
2.1.5. NIST 800-22 testi.....	17
2.2. PIC Mikro Denetleyiciler.....	40

BÖLÜM 3.

KAOS VE ENTROPİ KAYNAĞI REFERANS KAOTİK SİSTEMLERİN

ANALİZLERİ.....	43
3.1. Kaotik Sistemler.....	43
3.1.1. Ayrık zamanlı kaotik sistemler	44
3.1.2. Sürekli zamanlı kaotik sistemler	44
3.2. Kaotik Sistem Analiz Yöntemleri	45
3.2.1. Denge nokta analizi	45
3.2.2. Zaman serileri ve başlangıç değerlerine bağımlılık analizi.....	46
3.2.3. Faz portresi analizi.....	48
3.2.4. Lyapunov üstelleri spektrumu analizi.....	49
3.2.5. Poincare haritalama analizi	50
3.2.6. Çatallaşma diyagramı analizi.....	51
3.3. Rucklidge Kaotik Sistemi Analizi.....	52
3.4. Chen Kaotik Sistemi Analizi.....	54
3.5. Zhongtang Kaotik Sistemi Analizi.....	57

BÖLÜM 4.

SZKS'LER İÇİN YENİ BİR KAOTİK DEVRE DENEY SETİ TASARIMI VE

GERÇEKLEMESİ.....	63
4.1. KDDS Kaotik Devre Bloğu Tasarımı	64
4.1.1. İntegral alıcı devre tasarımı	65
4.1.2. Tersleyici devre tasarımı	65
4.1.3. Çarpma devresi tasarımı	66
4.2. KDDS Başlangıç Şartı Gerilim Sürücüsü ve Gerilim Regülatörü Tasarımı.....	67
4.2.1. Başlangıç şartı gerilim regüle devresi tasarımı.....	68
4.2.2. Başlangıç şart gerilim sürücüsü tasarımı	69
4.3. KDDS Kontrol Devresi ve Bilgisayar Programı Tasarımı.....	70
4.3.1. Mikro denetleyici tabanlı kontrol devresi tasarımı.....	70
4.3.2. Bilgisayar programı tasarımı.....	73

BÖLÜM 5.

ENTROPİ KAYNAĞI REFERANS KAOTİK SİSTEMLERİN MODELLENMESİ VE DEVRE GERÇEKLEMELERİ.....	76
5.1. Rucklidge Kaotik Siteminin Modellenmesi ve Devre Gerçeklemesi ...	76
5.2. Chen Kaotik Siteminin Modellenmesi ve Devre Gerçeklemesi	80
5.3. Zhongtang Kaotik Siteminin Modellenmesi ve Devre Gerçeklemesi ..	85

BÖLÜM 6.

GRSÜ TASARIMLARI İÇİN YENİ BİR PLATFORM TASARIMI VE GERÇEKLEMESİ.....	91
6.1. GRSÜ Entropi Kaynakları	91
6.2. ADC 0-5V Seviye Uygunlaştırıcı Devre Tasarımı.....	92
6.3. Mikro Denetleyici Kontrollü Veri Toplama Kartı Tasarımı	94
6.4. Bilgisayar Programı Tasarımı	96

BÖLÜM 7.

KAOS TABANLI YENİ GRSÜ TASARIMLARI VE GERÇEKLEMELERİ.....	99
7.1. Rucklidge Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçeklemesi ...	99
7.2. Chen Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçeklemesi	101
7.3. Zhongtang Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçeklemesi .	103

BÖLÜM 8.

SONUÇLAR VE ÖNERİLER	105
KAYNAKLAR.....	110
EKLER.....	118
ÖZGEÇMİŞ.....	119

SİMGELER VE KISALTMALAR LİSTESİ

AD	: Analog Devices
ADC	: Analog Digital Converter
ApEn(m)	: Aproxiamte Entropy
B	: Örtüşmeyen şablon eşleştirme testinde özel şablon
BMKP	: Bilgisayar ve mikro denetleyici kontrollü platform
CCS	: Custom Computer Services
CMOS	: Complementary Metal Oxide Semiconductor
CCTS	: Chaotic circuits testing set
CTCS	: Continuos time chaotic systems
DGKK	: Doğrusal Geri beslemeli kayan kaydedici
EEPROM	: Electronically Erasable Programmable Read Only Memory
erfc	: The Complementary Error Function
FF	: Flip flop
FIPS	: Federal Information Processing Standard
FPGA	: Field Programmable Gate Array
GRSÜ	: Gerçek rasgele sayı üretici
igamc	: Incomplete Complementary Gamma Function
j	: Kesir bitlerinin sayısı
J	: i. L-bit bloğun onluk sayı sistemindeki değeri
K	: Bağımsızlık katsayısı
KDDS	: Kaotik devre deney seti
Kbit	: Kilobit
Kv	: Tersleyen yükselteç çıkış kazancı
L	: Üniversal testinde her bir bloğun uzunluğu
LED	: Light Emitting Diode
LSB	: Least significant bit

M	: Bit dizisinde belirli sayıdaki bitlerinden oluşan blok
m	: Örtüşen şablon eşleştirme testinde özel blokların bit sayısı
MATLAB	: Matrix laboratory
Mbit	: Megabit
MCCS	: Microcontroller and computer controlled platform
ms	: Mili saniye
n	: Bit dizisinin uzunluğu
N	: İkili matris derece testinde matris sayısı
N_0	: T değerinden daha küçük beklenen değeri
NIST	: National Institute of Standards and Technology
ω_i	: Gözlemlenen frekans
Op-amp	: Operational amplifier
P-değeri	: NIST-800-22 testinde rasgelelik ölçütü
PCB	: Printed circuit board
PEEC	: PMOS Electrical Erasable Cell
PMOS	: P-channel metal oxide semiconductor field effect transistor
PIC	: Peripheral Interface Controller
PLL	: Phase Locked Loop
Q	: İkili matris derece testinde sütun sayısı
R	: Direnç değeri
RF	: Radio frequency
RISC	: Reduced Instruction Set Computing
RSÜ	: Rasgele sayı Üretici
SEA	: Scalable Encryption Algorithm
sign	: İşaret biti
S_n	: Normalizasyon işleminden elde edilen değer
sn	: Saniye
S_{obs}	: Gözlemlenen değer
SRAM	: Static Random Access Memory
SRSÜ	: Sözde rasgele sayı üretici
SZKS	: Sürekli zamanlı kaotik sistemler
t	: Zaman

T	: Tepe yüksekliđi eşik deęeri
T_i	: Daęılımın rasgele deęişkeni
T_j	: Muhtemel L-bit deęerleri
TRNG	: True random number generator
USB	: Universal Serial Bus
V	: Gerilim
$V_{exp(L)}$: Farklı L deęerleri için beklenen deęer
$V(obs)$: Bit osilasyon sayısı
var	: Varyans
VHDL	: VHSI Circuit Hardware Description Language
V_i	: En uzun 1 dizisinin akış frekansı
W_j	: Özel B şablonunun frekansı
XOR	: Exclusive Or (Özel Veya)
α	: Önem seviyesi
γ	: Sistem parametresi
$\Delta^2\Psi_m^2(obs)$: m-bit örneğin beklenen frekansı
Δh	: Algoritma adım miktarı
ε	: Bit dizisi
ε'	: Artırım dizisi
ε_i	: Bit dizisinin i. elemanı
χ^2	: Ki-kare daęılımı
λ	: Öz deęerler
λ_σ	: Algoritma parametreleri
μ	: Beklenen deęer
μs	: Mikro saniye
ξ	: Rasgele yürüyüşlerde ziyaret edilen durumların toplam sayısı
ξ_σ	: Algoritma parametreleri
π	: Bit dizisindeki 1 deęerlerinin sayısı
σ^2	: Varyans
τ	: Test için gerekli parametre şartı
$\varphi^{(m)}$: Blokların ampirik daęılım frekansı
$\Phi(z)$: Olasılık yoğunluk fonksiyonu

$V_{i_1 \dots i_m}$: m bitlik örneklerin frekansı
 y_λ : Algoritma ilk değeri
 $y_{\lambda+1}$: Algoritma sonraki değeri

ŞEKİLLER LİSTESİ

Şekil 2.1. Entropi kaynağının doğrudan yükseltilmesi ve örnekleme tabanlı GRSÜ blok diyagramı	13
Şekil 2.2. Osilatör örnekleme yöntemi tabanlı GRSÜ blok diyagramı.....	14
Şekil 2.3. Kaos tabanlı GRSÜ blok diyagramı [43].....	14
Şekil 2.4. PIC18F4550 giriş/çıkış portlarının fonksiyonları	42
Şekil 3.1. Örnek aynı başlangıç değere sahip kaotik sistemin X1 ve X2 çıkışlarının birbirine göre grafiği.....	47
Şekil 3.2. Örnek farklı başlangıç değerlere sahip aynı sistemin zaman serisi çıkışları	47
Şekil 3.3. Örnek farklı başlangıç değerlere sahip kaotik sistemin X1 ve X2 çıkışlarının birbirine göre grafiği.....	48
Şekil 3.4. Örnek Matlab faz portre çıktısı	48
Şekil 3.5. Örnek OrCAD-PSpice programı faz portre çıktısı.....	49
Şekil 3.6. Örnek osiloskop faz portre çıktısı	49
Şekil 3.7. Örnek Lyapunov üstel grafiği [21]	50
Şekil 3.8. Örnek Poincare haritalama [79]	51
Şekil 3.9. Örnek çatallaşma diyagramı [79].....	51
Şekil 3.10. Rucklidge sistemi Matlab programı X, Y, Z zaman serileri	52
Şekil 3.11. Rucklidge sistemi Matlab programı XY, XZ, YZ, XYZ faz portre çıkışları	53
Şekil 3.12. Rucklidge sistemi a parametresine ait Lyapunov üstel grafiği [21]	54
Şekil 3.13. Chen sistemi Matlab programı X, Y, Z zaman serileri	55
Şekil 3.14. Chen sistemi Matlab programı XY, YZ, XZ, XYZ faz portre çıkışları ...	56
Şekil 3.15. Chen sistemi Y çıkışının başlangıç değerine duyarlılığı.....	56
Şekil 3.16. Chen sistemi a parametresine ait Lyapunov üstelleri spektrumu grafiki ($b=11$ ve $c=28$) [74].....	57

Şekil 3.17. Zhongtang sistemi Matlab programı X, Y, Z zaman serileri	58
Şekil 3.18. Zhongtang sistemi Matlab programı XY, XZ, YZ, XYZ faz portre çıktıları	59
Şekil 3.19. Zhongtang sistemin a ve e parametrelerine ait Lyapunov üstelleri spektrumu grafikleri [79]	60
Şekil 3.20. Zhongtang sistemine ait Poincare haritalama grafikleri (a) $x_0=0$ (b) $y_0=0$ [79]	61
Şekil 3.21. Zhongtang sistemi a ve b parametrelerine ait çatallaşma diyagramları [79].....	62
Şekil 4.1. KDDS blok diyagramı	64
Şekil 4.2. KDDS’de kullanılan modüler integral alıcı devresi.....	65
Şekil 4.3. KDDS’de kullanılan tersleyici devresi	66
Şekil 4.4. KDDS’de kullanılan AD633 fonksiyon diyagramı ve devresi	66
Şekil 4.5. Örnek kaotik sistemin KDDS ile gerçekleştirilmesi.....	67
Şekil 4.6. Başlangıç şart gerilim regülatörü devre şeması	68
Şekil 4.7. Başlangıç şart gerilimini 0V-5V uygunlaştıran devre şeması.....	69
Şekil 4.8. Başlangıç şart gerilim sürücüsü devre şeması	70
Şekil 4.9. Mikro denetleyici tabanlı kontrol devresi	71
Şekil 4.10. PIC18F4550 CCS PIC C Compiler yazılımından bir kesit.....	71
Şekil 4.11. PIC18F4550 yazılımı akış diyagramı	73
Şekil 4.12. KDDS bilgisayar programı arayüzü	74
Şekil 4.13. Bilgisayar ve mikro denetleyici kontrollü KDDS gerçek devresi	75
Şekil 4.14. KDDS ile örnek kaotik devre gerçekleştirilmesi.....	75
Şekil 5.1. Rucklidge kaotik sistemi devre şeması	78
Şekil 5.2. Rucklidge kaotik sistemi X, Y, Z zaman serileri OrCAD-PSpice programı çıktıları	79
Şekil 5.3. Rucklidge kaotik sistemi XZ, YZ, XY faz portreleri OrCAD-PSpice programı çıktıları	79
Şekil 5.4. Rucklidge kaotik sisteminin sırasıyla XZ, XY, YZ faz portrelerine ait osiloskop çıktıları	80
Şekil 5.5. Rucklidge kaotik sistemi devresinin KDDS ile gerçekleştirilmesi	80
Şekil 5.6. Skala edilmiş Chen kaotik sistemi devre şeması	83

Şekil 5.7. Skala edilmiş Chen kaotik sistemi X, Y, Z zaman serileri OrCAD-PSpice programı çıktıları	83
Şekil 5.8. Skala edilmiş Chen kaotik sistemi XY, XZ, YZ faz portreleri OrCAD-PSpice programı çıktıları	84
Şekil 5.9. Chen kaotik sistemi sırasıyla XY, XZ, YZ faz portrelerine ait osiloskop çıktıları.....	85
Şekil 5.10. Skala edilmiş Chen kaotik sistemi devresinin KDDS ile gerçekleştirilmesi ..	85
Şekil 5.11. Skala edilmiş Zhongtang kaotik sistemi devre şeması	88
Şekil 5.12. Skala edilmiş Zhongtang kaotik sistemi X, Y, Z zaman serisi OrCAD-PSpice programı çıktıları.....	88
Şekil 5.13. Skala edilmiş Zhongtang kaotik sistemi XY, XZ, YZ faz portreleri OrCAD-PSpice programı çıktıları.....	89
Şekil 5.14. Skala edilmiş Zhongtang kaotik sistemi sırasıyla XY, XZ, YZ faz portrelerine ait osiloskop çıktıları.....	89
Şekil 5.15. Skala edilmiş Zhongtang kaotik sistemi devresinin KDDS ile gerçekleştirilmesi.....	90
Şekil 6.1. GRSÜ gerçekleştirmek için tasarlanan BMKP'nin blok diyagramı	91
Şekil 6.2. ADC için 0-5V seviye uygunlaştırıcı devre şeması.....	92
Şekil 6.3. Örnek kaotik sinyal	93
Şekil 6.4. ½ oranında küçültülmüş örnek kaotik sinyal	93
Şekil 6.5. 0-5V seviyesine uygunlaştırılmış kaotik sinyal	93
Şekil 6.6. ADC için 0-5V seviye uygunlaştırıcı gerçek devre	94
Şekil 6.7. Mikro denetleyici kontrollü veri toplama kartı devre şeması	94
Şekil 6.8. Mikro denetleyici kontrollü veri toplama kartı	95
Şekil 6.9. PIC18f4550 mikro denetleyicisine ait yazılımın durum diyagramı.....	95
Şekil 6.10. C Sharp programında hazırlanan bilgisayar programı arayüz görüntüsü	96
Şekil 6.11. Geliştirilen BMKP ile örnek GRSÜ gerçekleştirilmesi	98
Şekil 6.12. BMKP ile gerçekleştirilmiş Zhongtang kaotik sistemi tabanlı GRSÜ 1000 bit rasgele bit dizisi	98

TABLolar LİSTESİ

Tablo 2.1. Von Neumann son işlem algoritması doğruluk tablosu.....	15
Tablo 2.2. XOR son işlem algoritması doğruluk tablosu.....	15
Tablo 2.3. Blok uzunluklarına göre run testi koşulları.....	17
Tablo 2.4. Farklı blok değerleri için en uzun birlerin akış frekans değerleri.....	22
Tablo 2.5. Blok uzunluklarına göre K ve N parametre değerleri.....	23
Tablo 2.6. $m=3$ için M1 ve M2 blokları içerisinde B=001 şablonunun incelenmesi.	27
Tablo 2.7. M1 bloğu içerisinde B=11 özel şablonunun bulunma durumları	28
Tablo 2.8. Maurer testi L-bit uzunluktaki blokların bölümleri	30
Tablo 2.9. Dört başlangıç değeri ile oluşturulan muhtemel L-bit değerleri.....	30
Tablo 2.10. Test bölümü için L-bit değerleri	30
Tablo 2.11. L değerleri için $V_{exp}(L)$ ve $var(fn)$ değerleri.....	31
Tablo 2.12. İleri ve geri yönlü metotların uygulanması.....	37
Tablo 2.13. ϵ dizisi için oluşan rasgele gezinti döngü frekansları	38
Tablo 7.1. Rucklidge kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları.....	100
Tablo 7.2. Rucklidge kaotik sistemi XY, YZ, XZ kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları	101
Tablo 7.3. Chen kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları	102
Tablo 7.4. Chen kaotik sistemi XY, YZ, XZ kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları.....	102
Tablo 7.5. Zhongtang kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları.....	103
Tablo 7.6. Zhongtang kaotik sistemi XY, YZ, XZ kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları	104

ÖZET

Anahtar kelimeler: Gerçek Rasgele Sayı Üretici, İstatistiksel Rasgelelik Testleri, NIST Rasgelelik Testi, Kaos, Sürekli Zamanlı Kaotik Sistemler, Mikro denetleyiciler

Bu tezde yapılan çalışmalar üç ana kısımdan oluşmaktadır. Birinci aşamada, sürekli zamanlı kaotik sistemlerin (SZKS) devre gerçeklemelerinin hızlı ve kolay yapılabilmesi için yeni bir bilgisayar ve mikro denetleyici kontrollü kaotik devre deney seti (KDDS) tasarlanmış ve gerçekleştirilmiştir. İkinci aşamada ADC tabanlı gerçek rasgele sayı üretici (GRSÜ) tasarımlarının kolay, hızlı ve esnek yapılabilmesine olanak sağlayan yeni bir bilgisayar ve mikro denetleyici kontrollü bir platform (BMKP) tasarlanmış ve gerçekleştirilmiştir. Son aşamada ise gerçekleştirilen KDDS ve BMKP kullanılarak, uluslararası en üst düzey standart olan NIST800-22 testlerinin tamamından başarıyla geçen yeni GRSÜ tasarım ve gerçeklemeleri yapılmıştır.

Tezin birinci aşamasında ilk olarak; GRSÜ tasarımları için entropi kaynağı olarak kullanılan referans kaotik sistemlerin analizleri yapılmıştır. İkinci olarak; referans alınan kaotik sistemler analog devre elemanları ile modellenerek OrCAD-PSpice programında tasarlanan devrelerin faz portrelerine ait simülasyonlar yapılmıştır. Üçüncü olarak; karmaşık ve uzun zaman alan kaotik devre gerçekleştirme işlemlerinin, kolay, hızlı ve esnek yapılabilmesi amacıyla, yeni bir KDDS tasarlanmış ve gerçekleştirilmiştir. Ardından referans alınan kaotik sistemlerin tasarlanan KDDS ile gerçek devreleri kurulmuş ve elde edilen gerçek devre osiloskop çıktıları, sistemlere ait Matlab, OrCAD-PSpice çıktıları ile karşılaştırılmıştır.

İkinci aşamada; ADC tabanlı olarak yapılacak olan GRSÜ tasarımlarında kullanılacak, yeni bir BMKP tasarlanmış ve gerçekleştirilmiştir. Bu sistemin özgün yönleri; kaotik sistemlerin yanında sıcaklık, RF gibi farklı kaynakları da entropi kaynağı olarak kullanabilmesi, farklı entropi kaynaklarını karıştırarak kullanabilmesi, farklı son işlem algoritmalarının seçilebilmesi olarak sıralanabilir.

Son aşamada, gerçekleştirilen KDDS ve BMKP kullanılarak, Rucklidge, Chen ve Zhongtang kaotik sistemleri tabanlı yeni GRSÜ tasarım ve gerçeklemeleri yapılmıştır. Gerçeklenen GRSÜ'ler, NIST800-22 testlerine tabi tutulmuştur. Chen ve Zhongtang kaotik sistemi tabanlı GRSÜ'ler tüm testlerden başarı ile geçmiştir.

DESIGN AND IMPLEMENTATION OF CHAOS SOURCED AND ADC BASED NOVEL TRUE RANDOM NUMBER GENERATORS

SUMMARY

Keywords: True Random Number Generator, Statistical Randomness Tests, NIST Statistical Tests, Chaos, Continuous-time Chaotic Systems, Microcontroller

The studies in this thesis consists of three main stages. At the first stage, a microcontroller and computer controlled chaotic circuit testing set (CCTS) for fast modelling of continuous-time chaotic systems (CTCS) has been designed and implemented. At the second stage, a microcontroller and computer controlled platform (MCCP) has been designed and implemented to design ADC based true random number generator (TRNG) fast and easily. At the last stage, new TRNGs pass the all of NIST-800-22 statistical tests, which is the highest international standards have been designed and implemented by using CCTS and MCCP for design of TRNG.

At the first stage of the thesis, firstly reference chaotic systems used as entropy source of TRNG have been analyzed. Secondly, reference chaotic systems have been modeled by using analog circuit component and the phase portraits of chaotic electronic circuits modeled have been simulated in OrCAD-PSpice. Thirdly, a CCTS has been designed and implemented to make complex and extremely time-consuming process of chaotic circuit implementation fast and easily. After that, reference chaotic systems has been realized using CCTS and then oscilloscope outputs of real circuits have been compared with Mat lab, OrCAD-PSpice outputs.

At the second stage, a MCCP has been designed and implemented to be used on design of ADC based TRNG fast and easily. The unique aspects of this system come from using chaotic system also different entropy sources such as radio frequency (RF), temperature as an entropy source, using different entropy sources by mixing each other, selecting different last processing algorithm.

At the last stage, Rucklidge, Chen and Zhongtang chaotic systems based TRNGs have been designed and implemented using CCTS and MCCP. TRNGs realized has been subjected to NIST-800-22 statistical tests. Chen and Zhongtang chaotic system based TRNGs have passed successfully to NIST statistical tests.

BÖLÜM 1. GİRİŞ

Teknolojinin geldiği nokta itibariyle, gerek bireysel, gerekse uluslararası güvenlik açısından iletişim güvenliği çok önemli bir hal almıştır. Haberleşme ve iletişim teknolojilerinde veri gizliliğinin sağlanabilmesi için şifreleme teknikleri kullanılmaktadır [1,2]. Şifreleme tekniklerinin temelini rasgele sayılar oluşturur. Sürekli gelişen teknoloji ile kriptolojinin kullanım alanları hızla arttığından, yeni rasgele sayı üreteçlerine olan gereksinim de hızla artmaktadır [2-5].

Rasgele sayı üretici (RSÜ), çıkışı rasgele sayılardan oluşan sanal veya fiziksel bir kaynak kullanılarak üretilmiş sistemlerdir. Rasgele sayı dizileri, aralarında korelasyon bulunmayan birbirinden bağımsız sayılardan oluşur [6-8]. Rasgele sayıların, rasgeleliği istatistiksel testler kullanılarak ispat edilmelidir. RSÜ'ler, kendi aralarında sözde rasgele sayı üreteçleri (SRSÜ) ve gerçek rasgele sayı üreteçleri (GRSÜ) olarak iki temel gruba ayrılır [8,9].

SRSÜ'ler belirli bir algoritma ile üretilmiş deterministik sayı dizilerinden oluşan devrelerdir. Sadece bir periyot boyunca rasgelelik gösterirler ve bu periyotlar birbirini tekrarlar. SRSÜ'ler seçilen bir tohum değeri ile rasgele çıkış üretmeye başlar [8,10,11]. Bundan dolayı seçilen tohum değerinin de rasgele olması gerekir. Kullanılan algoritma bilindiğinde, herhangi bir andaki rasgele çıkış değeri referans alınarak sonraki çıkış değerleri tespit edilebilmektedir. SRSÜ'ler istatistiksel testlerin birçoğundan başarısız olmaktadır. Bu durum SRSÜ'lerin kullanımını kısıtlamaktadır [8,9,11].

GRSÜ'ler, SRSÜ'lerin tersine, tahmin ve kontrol edilemeyen entropi (gürültü) kaynaklarını kullanarak rasgele sayılar üreten sistemlerdir [9,12,13]. GRSÜ'ler donanım ihtiyacının olması ve bit üretim işleminin yavaş olmasına rağmen, tahmin

edilememe özelliğinden dolayı yüksek güvenilirlik istenilen sistemlerde daha çok tercih edilmeye başlanmıştır [9,14,15]. GRSÜ'leri tasarlarken, gürültü kaynaklarının doğrudan yükseltilmesi ve örneklenmesi, osilatör örnekleme yöntemi ve kaotik sistemler yaygın olarak kullanılmaktadır [16-18].

Kaos, düzensizliğin düzeni olarak ifade edilen, doğrusal olmayan olayları açıklamaya yardımcı bir bilim dalıdır. Kaos, karmaşık davranışların yanında kendine has bir iç düzene sahip olmasından dolayı rastlantısal bir olay değildir ve dinamik sistemlerin bilinen en karmaşık hali olarak ifade edilebilir. Kaos, rasgele düşünülen durumların içinde hassas farklardan meydana gelen olayların bir birbiri ile ilişkisine odaklanır. Kaos bilim dalı, gerçek hayatta, bulutların hareketi, sigara dumanı hareketi, köpüren nehir hareketleri, musluktan akan suyun hareketi vb. rasgele davranış gösterdiği düşünülen olayları anlamaya çalışan bilim dalıdır [19-21].

Kaos biliminin temellerini ilk olarak 1892 yılında Fransız matematikçi Henri Poincare, basit dinamik kuralların çok karmaşık kararlı bir davranışa yol açabildiğini keşfederek attı. Poincare kaos biliminin farkına varmadan, kaotik yörünge ve başlangıç şartlarına bağımlılıktan bahsetmiştir [19].

Hollandalı elektrik mühendisi ve fizikçi Van der Pol 1927 yılında Nature Magazine adlı dergide yayınlanan makalesinde, sinüzoidal kaynakla sürülen bir neon lamba osilatörü üzerinde yapılan deneysel çalışmada farkında olmadan kaotik sinyalleri telefon ahizesindeki kulaklık ile dinlemiştir. Kondansatör kapasite değerinin değişimi sırasında, frekanstaki değişimleri bir değerden sonra düzensiz bir gürültü meydana getirdiğini görmüş ve makalesine "Frequency demultiplication" adını vermiştir. 1986 yılında M. Peter Kennedy, Van der Pol'un düzensiz gürültü olarak tanımlamadığı bu olayın kaos olduğunu belirtmiştir [19].

Kaosun matematiksel modeli 1963 yılında ilk olarak Edward Norton Lorenz tarafından ortaya atılmıştır. Bir meteorolog olan Lorenz, hava durumu tahmini yapmak için yaptığı çalışmalar devam ederken, hesaplarda yapılan yuvarlamaların sonuçları çok başka yerlere götürdüğünü görmüştür. Lorenz, hava olayları tahmininde kullanılmak

üzere geliřtirdiđi akıřkan ısı yayınımlı benzetimdeki salınımları tanımlamak için yeni bir model geliřtirmiřtir. Bu model kaotik biliminin ilerlemesinin önünü açmıř ve kaotik olayları açıklamak için en önemli model sistem olmuřtur. Yüksek hızlı bilgisayarların geliřtirilmesi, son yıllarda kaos biliminin ilerlemesi için etkin bir rol oynamıř ve karmařık, çözülemeyen konu olarak görülen kaosa olan ilgiyi arttırmıřtır [19].

Kaotik sistemler, kısaca bařlangıç řartlarına ve denklem parametrelerine ařırı duyarlı dinamik sistemler olarak ifade edilebilir. Kaotik sistemlerin bařlangıç řartlarına ve parametrelere olan hassas duyarlılıđından dolayı, bu deđerlerde yapılacak çok küçük deđiřimler sistemin çıkıřının deđiřmesine sebep olmaktadır. Bu sebepten dolayı, kaotik yapılar deterministik sistemler olmalarına rađmen sadece kısa süreli sistem davranıřı tahmin edilebilmektedir. Daha sonraki iterasyonlarda ise kaotik sistemlerin davranıřları önceden tahmin edilmez bir hal almaktadır [19-21]. Kaotik sistemlerin tahmin edilememe özelliđinden dolayı, GRSÜ için entropi kaynađı olarak kullanılması yaygınlařmaktadır. GRSÜ tasarımlarında kaotik osilatörlerin tercih edilme sebebi, sinyallerin rasgeleliđinin iyi olması ve diđer gürültü kaynaklarına göre çevresel kořullardan daha az etkilenmeleridir [17,18,22].

1.1. Literatür Taraması

Literatürde GRSÜ yapılarının, FPGA çipleri üzerinde modellenmesi, CMOS (Complementary Metal Oxide Semiconductor) teknolojisi ve analog elemanlar ile gerçekleřtirilmesi üzerine çalıřmalar yapılmıřtır. Bunlardan FPGA çipi kullanarak gerçekleřtirilen çalıřmalara örnek olarak ařađıdaki çalıřmalar gösterilebilir.

Danger ve arkadaşları, FPGA kullanarak bit üretim hızı yüksek yeni bir GRSÜ tasarlamıřlardır. Yapılan çalıřmada elde edilen rasgele sayı bitleri NIST testine tabi tutulmuř ve bütün testlerden bařarılı olduđu belirtilmiřtir. Tasarlan GRSÜ'nün bit üretim hızı 20 Mbit/s olarak verilmiřtir [23].

Lozac'h ve arkadaşları, FPGA kullanarak yeni bir GRSÜ tasarlamışlardır. Tasarlanan yapı, Xilinx tarafından üretilen Virtex-5 XC5VLX50T çip ailesinde gerçekleştirilmiştir. Tasarlanan GRSÜ'nün bit üretim hızı 20 Mbit/s olarak belirtilmiştir. Üretilen rasgele sayı bitleri NIST testine tabi tutulmuş ve bütün testlerden geçtiği belirtilmiştir [24].

Wieczorek ve arkadaşları, FPGA üzerinde çift kararlı flip-flop kullanarak GRSÜ tasarlamışlardır. Yapılan çalışma, Spartan3E FPGA çipi kullanarak gerçekleştirilmiştir. Üretilen rasgele diziler rasgelelik testine tabi tutulmuş ve testlerden başarılı olduğu belirtilmiştir. Tasarlanan GRSÜ'nün bit üretim hızı ise 5 Mbit/s olarak belirtilmiştir [25].

Fischer ve arkadaşları, FPGA çipinde PLL tabanlı osilatör kullanarak yeni bir GRSÜ tasarlamışlardır. GRSÜ yapısı VHDL'de tanımlanmış ve Altera firmasının Quartus II programı kullanılarak gerçekleştirilmiştir. GRSÜ'nün rasgele dizi çıkışları NIST testine tabi tutulmuş ve testlerden başarılı olduğu belirtilmiştir. Tasarlanan GRSÜ'nün bit üretim hızı 1 Mbit/s olarak belirtilmiştir [26].

Kaotik osilatörlerin entropi kaynağı olarak kullanıldığı GRSÜ yapılarının, CMOS (Complementary Metal Oxide Semiconductor) teknolojisi ve analog elemanlar ile gerçekleştirilmesi üzerine yapılan çalışmalara aşağıdaki örnekler verilebilir.

Ergün ve Özoğuz, otonom olmayan kaotik sistem ve CMOS teknolojisi kullanarak GRSÜ tasarlamıştır. Tasarlanan GRSÜ'nün bit üretim hızı 10 Mbit/s olarak belirtilmiştir. Tasarlanan GRSÜ ile üretilen rasgele diziler NIST-800-22 testine tabi tutulmuş ve testlerin hepsinden başarılı bir şekilde geçtiği belirtilmiştir [27].

Özoğuz ve arkadaşları, 0.35 µm CMOS teknolojisi ile tümleşik kaotik devre tasarımı yapmış ve yapılan kaotik devreyi entropi kaynağı olarak kullanan GRSÜ tasarlamışlardır. Yapılan kaotik devre, 16 MHz ile 25 MHz arasında kaotik sinyaller üretmektedir. Tasarlanan GRSÜ'nün bit üretim hızı 2 Mbit/s olarak belirtilmiştir. Tasarlanan GRSÜ ile üretilen rasgele diziler FIPS-140-2 ve NIST-800-22 testine tabi tutularak rasgelelikleri ispatlanmıştır [28].

Başka bir çalışmada, Pareschi ve arkadaşları 0.18 μm ve 0.35 μm CMOS teknolojisi ile yeni bir kaos tabanlı GRSÜ gerçekleştirmişlerdir. Tasarlanan GRSÜ ile üretilen rasgele dizilerin NIST testleri yapılarak rasgeleliği ispatlanmıştır. Yapılan testler sonucundan GRSÜ'nün bit üretim hızı 80 Mbit/s olarak verilmiştir [29].

Tavas ve arkadaşları, 0.35 μm CMOS teknolojisi ile sürekli zamanlı bir kaotik sistemi entropi kaynağı olarak kullanan, osilatör örnekleme yöntemi ile yeni bir GRSÜ tasarlamışlardır. Tasarlanan GRSÜ'nün bit üretim hızı 2 Mbit/s olarak verilmiştir. Tasarlanan GRSÜ ile üretilen rasgele dizilerin FIPS-140-1 testi yapılarak rasgeleliği ispatlanmıştır [30].

Drutarovsk'y ve Galajda, kriptolojik uygulamalar için ticari olarak kullanılabilen analog elemanlar ile kaos tabanlı yeni bir GRSÜ tasarlamışlardır. Tasarlanan GRSÜ ile üretilen rasgele dizilerin rasgeleliği, NIST testi ile ispatlanmış ve bit üretim hızınının 60 Kbit/s olduğu belirtilmiştir [31].

Zhang ve arkadaşları, lazer kaotik sinyallerin karşılaştırılmasına dayalı ultra hızlı yeni bir GRSÜ tasarlamışlardır. Tasarlanan sistemde, kaotik lazer kaynaktan gönderilen ışık, foto detektör ile elektrik sinyaline dönüştürülmüş ve elde edilen sinyal karşılaştırıcı ve D tipi FF içeren 1 bit ADC ile örneklenmiştir. Tasarlanan GRSÜ'nün bit üretim hızınının 1.44 Gbit/sn'ye kadar çıkabildiği belirtilmiştir. Tasarlanan GRSÜ ile üretilen rasgele dizilerin NIST ve Diehard testlerine tabi tutularak rasgeleliklerinin ispatlandığı belirtilmiştir [32].

Farklı bir çalışmada, Fabbri ve Callegari, ağ güvenliği için ağ cihazlarına sonradan eklenebilir PIC18f2550 mikro denetleyici kullanarak düşük maliyetli ve ADC tabanlı yeni bir GRSÜ tasarlamış ve gerçekleştirmişlerdir. Gerçeklenen GRSÜ, ürettiği rasgele bitleri USB portu üzerinden bilgisayara aktarmaktadır. Üretilen rasgele bitler NIST 800-22 testine tabi tutulmuş ve testlerin tamamından başarılı olduğu belirtilmiştir. Tasarlanan GRSÜ'nün bit üretim hızı 32 Kbit/sn olarak verilmiştir [33].

Literatürde bulunan çalışmalarda görüldüğü gibi, kaotik sistemleri entropi kaynağı olarak kullanan birçok GRSÜ tasarlanmıştır. Analog elemanlarla gerçekleştirilen GRSÜ'ler için çoğunlukla sürekli zamanlı kaotik sistemler (SZKS) entropi kaynağı olarak kullanılmaktadır. SZKS'lerin devre gerçeklemelerini yaparken 4 önemli sorun ortaya çıkmaktadır:

- SZKS devrelerinin karmaşık yapıya sahip olmasından dolayı breadboard üzerinde kurulmasının zor olması ve PCB gereksinimi duyulması.
- SZKS devrelerinin simetrik devre besleme gerilimi ve başlangıç şart gerilimleri ihtiyacından dolayı çok sayıda farklı simetrik güç kaynağı gerekli olması.
- SZKS devrelerinde standart dışı değerlerde dirençlere ihtiyaç olması.
- SZKS devrelerini çalıştırabilmek için, sistemin yapısı ve yapılan uygulama gereği, başlangıç şartı gerilimlerini uygulayan başlangıç şartı sürücü devresine ihtiyaç duyulmasıdır.

Gerçek rasgele sayı üreticinin kalitesi; ideal bir gürültü kaynağının yanında, kullanılan örnekleme yöntemine ve son işlem algoritmalarına da bağlıdır. İyi bir GRSÜ tasarlamak için en uygun parametreleri seçmek, çok sayıda deneysel çalışma yapmakla mümkün olabilmektedir. Literatürde bulunan çalışmalar incelendiğinde, donanımsal olarak gerçekleştirilen GRSÜ'lerin genel olarak, entropi kaynağı devresi, örnekleme devresi, veri aktarma devresi ve bilgisayar programı kısımlarından oluştuğu görülmektedir.

1.2. Tezin Amacı

Yapılan tezin birinci amacı, SZKS'lerin devre gerçeklemelerinde karşılaşılan zorlukları ortadan kaldıracak, hızlı ve kolay devre kurmayı sağlayacak, mikrodenetleyici ve bilgisayar kontrollü kaotik devre deney seti (KDDS) tasarlamak ve gerçeklemektir.

İkinci amacı, tasarlanan KDDS ile kurulan kaotik osilatörleri ve/veya sıcaklık, RF gibi diğer gürültü kaynaklarını da kaynak olarak kullanabilen, ADC tabanlı GRSÜ tasarımlarının kolay, hızlı ve esnek yapılabilmesine olanak sağlayan bilgisayar ve mikro denetleyici kontrollü bir platform (BMKP) tasarlamak ve gerçekleştirmektir. Bu platform ile istenilen uzunlukta rasgele sayı bitleri üretilebilecek, en uygun örnekleme zamanı, kullanılan ADC bit çıkışı ve son işlem algoritmaları seçilebilecektir.

Üçüncü amacı ise, gerçekleştirilen KDDS ve BMKP kullanılarak, uluslararası en üst düzey standart olan NIST800-22 testlerinin tamamından başarıyla geçen yeni GRSÜ tasarım ve gerçeklemeleri yapmaktır.

1.3. Tezde İzlenecek Yol

Yapılan tez çalışması, SZKS devrelerinin hızlı ve kolay kurulmasını sağlayan KDDS ve ADC tabanlı GRSÜ tasarımları için BMKP tasarlanması ve bu tasarımları kullanarak NIST-800-22 testlerinin hepsinden başarı ile geçen yeni rasgele sayı dizilerinin üretilmesi amacıyla sekiz bölüme ayrılmıştır.

İkinci bölümde, rasgele sayı üreteçleri, FIPS 140-1 ve NIST-800-22 istatistiksel testleri ve tasarlanan sistemlerde kullanılan mikro denetleyiciler gibi temel kavramlar tanıtılacaktır.

Üçüncü bölümde, kaosun tanımı, kaotik sistem çeşitleri, kaotik sistem analiz yöntemleri anlatılacak ve rasgele sayı üreteçleri için entropi kaynağı olarak seçilen örnek kaotik sistemler tanıtılacaktır. Seçilen örnek kaotik sistemlerin dinamik davranışlarını belirlemek amacıyla nümerik benzetim ve analiz programı (Matlab) kullanılarak kaotik sistemin zaman serileri, faz portreleri, denge noktaları ve Lyapunov spektrumu ve Çatallaşma analizleri yapılacaktır.

Dördüncü bölümde, SZKS devre gerçeklemelerinde karşılaşılan zorlukları ortadan kaldıracak, hızlı ve kolay devre kurmayı sağlayacak olan KDDS'nin tasarım adımları bloklar halinde açıklanacaktır.

Beşinci bölümde, GRSÜ için entropi kaynağı olarak kullanılacak kaotik sistemlerin devre modellemeleri yapılacak ve tasarlanan devreler, KDDS ile gerçekleştirilecektir. Ayrıca, devrelerin OrCAD-PSpice programı kullanarak elde edilen faz portre çıktıları, osiloskop faz portre çıktıları ile karşılaştırılacaktır.

Altıncı bölümde, ADC tabanlı GRSÜ tasarımları için BMKP tasarım ve gerçekleştirme aşamaları bloklar halinde açıklanacaktır.

Yedinci bölümde, gerçekleştirilen KDDS ve BMKP kullanılarak üretilen, üç farklı yeni kaos tabanlı GRSÜ tasarımları ve bunlardan elde edilen rasgele sayı dizilerinin NIST800-22 test sonuçlarına ait tablolar sunulacaktır.

Son bölüm de ise, tez çalışmasının sonuçları anlatılacak, istatistiksel test sonuçlarına göre kaotik osilatörlerin hangi parametreler seçildiğinde ideal entropi kaynağı olarak kullanılabilirliği ve hangi kaotik osilatörlerin rasgele sayı üretmek için daha uygun olduğu hakkında inceleme ve değerlendirmeler yapılacaktır. Ayrıca ileride yapılabilecek çalışmalar hakkında öneriler de sunulacaktır.

BÖLÜM 2. TEMEL KAVRAMLAR

Bu bölümde, GRSÜ tasarımları için gerekli bazı genel bilgiler verilmiştir. İlk olarak rasgele sayı üreteçlerinden bahsedilmiştir. Daha sonra, RSÜ'lerden elde edilen bitlerin rasgeleliğini ispat etmek için, en çok kullanılan istatistiksel testlerden ikisi olan FIPS-140-1 ve NIST-800-22 testleri incelenmiştir. Son olarak, SZKS devrelerinin hızlı ve kolay kurulmasını sağlayan KDDS ve GRSÜ tasarlamak için gerçekleştirilen BMKP'de kullanılan mikrodenetleyici hakkında bilgiler verilmiştir.

2.1. Rasgele Sayı Üreteçleri (RSÜ)

Rasgele sayı üretici (RSÜ), çıkışı rasgele sayılardan oluşan sanal veya fiziksel bir kaynak kullanılarak üretilmiş sistemlerdir. Rasgele sayı dizileri, aralarında korelasyon bulunmayan birbirinden bağımsız sayılardan oluşur [6,8,14]. Bu özelliklerinde dolayı, rasgele sayı üreteçlerine istatistiksel analiz, örnekleme, simülasyon ve kriptografi gibi birçok alanda ihtiyaç duyulmuştur. Kriptografinin temelini rasgele sayılar oluşturur. Bir kriptografik sistemin güvenliği, kullanılan sayıların gerçek rasgeleliğine bağlıdır [9,14,15]. Bu sebeple, rasgele sayıların deterministik bir yapıya sahip olmama yani tahmin edilememe, tekrar üretilmeme gibi özelliklere sahip olması gerekir. Rasgele sayıların, rasgeleliği istatistiksel testler kullanılarak ispat edilmelidir. Rasgele sayılara ihtiyaç duyan uygulamaların sayısı arttıkça, farklı rasgele veri üretme teknikleri ihtiyacı doğmuştur. Bu teknikler, rasgele sayının tahmin edilememe kalitesi ve rasgele sayı üretme hızı gibi amaçlar doğrultusunda oluşturulmuştur. RSÜ'leri, kendi aralarında sözde rasgele sayı üreteçleri (SRSÜ) ve gerçek rasgele sayı üreteçleri (GRSÜ) olarak iki temel gruba ayırabiliriz [6,9,34].

2.1.1. Söзде rasgele sayı üreteçleri (SRSÜ)

SRSÜ'ler, belirli bir algoritma ile üretilmiş deterministik sayı dizilerinden oluşan devrelerdir. Sadece bir periyot boyunca rasgelelik gösterirler ve bu periyotlar birbirini tekrarlar. SRSÜ'ler, seçilen bir tohum değeri ile rasgele çıkış üretmeye başlar. Bundan dolayı seçilen tohum değerinin de rasgele olması gerekir [8-10]. Kullanılan algoritma bilindiğinde, herhangi bir andaki rasgele çıkış değeri referans alınarak sonraki çıkış değerleri tespit edilebilmektedir. SRSÜ'ler istatistiksel testlerin birçoğundan başarısız olmaktadır. Bu durum SRSÜ'lerin kullanımını kısıtlamaktadır. Bu sebeplerden dolayı, SRSÜ'ler, yüksek güvenilirlik istenen uygulamalarda tercih edilmemektedir. Bunun yanında, SRSÜ'lerin avantajları, ucuz olması, kolay gerçekleştirilebilir olması, hızlı olması ve donanım ihtiyacına gerek duymamasıdır [8,9,11]. SRSÜ'lerin bilinen en eski yöntemlerinden iki tanesi orta kare tekniği ve lineer eşlikel yöntemidir [34].

Ortakare yöntemi, dikdörtgen dağılıma uygun rasgele sayılar dizisini üretmek için kullanılan ilk aritmetik yöntemlerden biridir. 1916'da Von Neumann ve Metropolis tarafından önerilmiştir. Bu yöntemde, m basamaklı sayının karesi alınır ve elde edilen sayının ortasında yer alan m basamak alınarak, yeni bir sayı üretilir. Orta kare yönteminde ilk olarak, 4 basamaklı bir sayı seçilir ve sayının karesi alınır. 8 basamağı doldurmak için gerekiyorsa sayının sol tarafına sıfır eklenir. Daha sonra, rasgele sayı olarak kullanılmak üzere ortadaki 4 basamak seçilir. İstenildiği kadar sayı elde etmek için aynı işlemler tekrarlanır. Yöntemi açıklamak için ilk sayı olarak $X_0=2152$ seçilirse aşağıdaki dizi elde edilir [35].

$$X_0= 2152 \quad (X_0)^2= 04631104$$

$$X_1= 6311 \quad (X_1)^2= 39828721$$

$$X_2= 8287 \quad (X_2)^2= 68674369$$

$$X_3= 6743 \quad (X_3)^2= 45468049$$

$$X_4= 4680 \quad (X_4)^2= 21902400$$

$$X_5= 9024 \text{ vb.}$$

Bu yöntemi analiz etmek zordur ve istatistik olarak iyi değildir. Örneğin ilk sayı ve dizinin tekrar uzunluğu arasındaki ilişkiyi zamanla tahmin etmek zordur. Çoğu kez tekrar uzunluğu oldukça kısadır. Tekrar uzunluğu kısa olmasa bile örnek rasgele değildir. Örnek verecek olursak ilk sayı olarak 4500 seçilirse istenmeyen aşağıdaki dizi elde edilir.

$$X_0 = 4500 \quad (X_0)^2 = 20250000$$

$$X_1 = 2500 \quad (X_1)^2 = 06250000$$

$$X_2 = 2500 \quad (X_2)^2 = 06250000$$

$$X_3 = 2500 \text{ vb.}$$

Verilen örneğe göre orta kare tekniği pek tercih edilen bir yöntem olmamaktadır.

Lineer eşlikli yöntemi, Lehmer tarafından önerilmiştir. Her biri eşlik ilişkisine dayanan çok sayıda eşlik yöntemi geliştirilmiştir. Bunlardan yaygın olarak bilinenler çarpım, karmaşık ve toplam eşlik yöntemleridir [35,36].

Çarpım eşlik yöntemi, üniform dağılmış sayıların sonlu dizisini üretmek için aritmetik bir yöntemdir. $x_{i+1} = a \cdot x_i \text{ Mod } (m)$ formülü kullanılır. İlk olarak, en az 5 basamaktan oluşan sayı a değeri ile çarpılır ve elde edilen sayı $1/m$ ile çarpılır. 9 haneden daha küçük bir sayı X_0 olarak seçilir. Bu sayı rasgele sayılar tablosundan rasgele olarak seçilebilir. $0 \leq x \leq 1$ olacak şekilde rasgele sayı olarak elde edilen sayının ondalık kısmı seçilir. Daha sonra, oluşan sayıdan rasgele sayı alınır, x tekrar kaynak olarak kullanılır. İstenildiği kadar rasgele sayı üretmek için işlem tekrarlanır [35].

Örnek olarak, $a=37$, $m=100$, $x_0=53$ olarak verilsin. Üretilen rasgele sayı dizisi aşağıdaki gibi olur.

$$x_0 = 53$$

$$x_1 = (37 \cdot 53) \text{ Mod } (100) = (1961) \text{ Mod } (100) = 61$$

$$x_2 = (37 \cdot 61) \text{ Mod } (100) = (2257) \text{ Mod } (100) = 57$$

$$x_3 = (37 \cdot 57) \text{ Mod } (100) = (2109) \text{ Mod } (100) = 09$$

$$x_4 = (37.09) \text{ Mod}(100) = (333) \text{ Mod}(100) = 33$$

Karmaşık eşlik yöntemi Thomson tarafından önerilmiştir. Rasgele sayı üretmek için $x_{i+1} = (a.x_i + c) \text{ Mod}(m)$ formülünü kullanır [35].

Örnek olarak, $a=9$, $m=12$, $c=5$, $x_0=11$ olarak verilirse, üretilen rasgele sayı dizisi aşağıdaki gibi olur.

$$x_0 = 11$$

$$x_1 = (9.11+5) \text{ Mod}(12) = (19) \text{ Mod}(100) = 8$$

$$x_2 = (9.80+5) \text{ Mod}(12) = (77) \text{ Mod}(100) = 5$$

$$x_3 = (9.50+5) \text{ Mod}(12) = (43) \text{ Mod}(100) = 2$$

Toplam karmaşık yöntemi, Green, Smith ve Klem tarafından önerilmiştir. Rasgele sayı üretmek için $x_i = (x_{i-1} + x_{i-k}) \text{ Mod}(m)$ formülünü kullanır [35].

Örnek olarak, $k=5$, $x_1=57$, $x_2=34$, $x_3=89$, $x_4=92$, $x_5=16$, $m = 100$ olarak verilirse, üretilen rasgele sayı dizisi aşağıdaki gibi olur.

$$x_6 = (x_5 + x_1) = (16+57) \text{ mod}(100) = 73$$

$$x_7 = (x_6 + x_2) = (73+34) \text{ mod}(100) = 7$$

$$x_8 = (x_7 + x_3) = (7+89) \text{ mod}(100) = 96$$

$$x_9 = (x_8 + x_4) = (96+92) \text{ mod}(100) = 88$$

$$x_{10} = (x_9 + x_5) = (88+16) \text{ mod}(100) = 4$$

$$x_{11} = (x_{10} + x_6) = (4+73) \text{ mod}(100) = 77$$

$$x_{12} = (x_{11} + x_7) = (77+7) \text{ mod}(100) = 84$$

$$x_{13} = (x_{12} + x_8) = (84+96) \text{ mod}(100) = 80$$

2.1.2. Gerçek rasgele sayı üreteçleri (GRSÜ)

Gerçek rasgele sayı üreteçleri (GRSÜ), SRSÜ'lerin tersine, tahmin ve kontrol edilemeyen entropi (gürültü) kaynaklarını kullanarak rasgele sayılar üreten sistemlerdir. GRSÜ'ler, donanım ihtiyacının olması ve bit üretim işleminin yavaş olmasına rağmen, tahmin edilememe özelliğinden dolayı yüksek güvenilirlik istenen sistemlerde daha çok tercih edilmeye başlanmıştır [13,17,18,37]. GRSÜ tasarlanırken kullanılan yöntemlerden bazıları, gürültü kaynaklarının doğrudan yükseltilmesi ve örnekleme, osilatör örnekleme yöntemi ve kaos kaynaklı sistemlerdir[38]. GRSÜ'ler ile üretilen rasgele sayı dizileri, rasgelelik ve güvenilirliklerinin artırılması amacıyla Von Neumann [39], Xor [9], H fonksiyonu [40] ve resilient fonksiyonu [41] gibi son işlem algoritmalarına tabi tutulurlar.

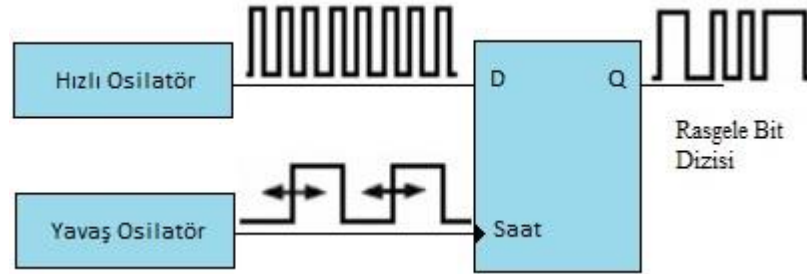
Entropi kaynaklarının doğrudan yükseltilmesi ve örnekleme tabanlı GRSÜ'nün bazı olumsuz yönleri vardır. Kullanılan entropi kaynağının ürettiği sinyalleri çok düşük gerilim seviyelerine sahip olmasından dolayı çevresel kaynaklardan etkilenip periyodik sinyal üretme ihtimalleri, yükseltme ihtiyacı duyması ve yükseltme işlemi yapılırken çıkış frekans bandının düşük olması, bu olumsuzluklara örnek gösterilebilir. Şekil 2.1.'de entropi kaynağının doğrudan yükseltilmesi ve örnekleme tabanlı GRSÜ'nün blok diyagramı verilmiştir [9,38,42].



Şekil 2.1. Entropi kaynağının doğrudan yükseltilmesi ve örnekleme tabanlı GRSÜ blok diyagramı

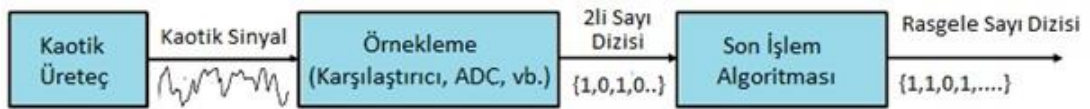
Şekil 2.2.'de şekli verilen osilatör örnekleme yöntemi tabanlı GRSÜ'de rasgelelik, seçirmeli yavaş osilatörün faz gürültüsüne bağlıdır. Bu yöntemde, hızlı osilatör D tipi FF'nin işaret girişine uygulanırken, faz gürültüsüne sahip yavaş osilatör, D tipi FF'nin saat girişine uygulanır ve genellikle yavaş osilatörün yükselen kenarlarında hızlı osilatörün çıkışları örneklenir. Yavaş osilatörün seçirme çıkışının yeterli rasgele dağılımı göstermediği durumlarda, gürültü kaynaklı ya da gerilim kontrollü osilatörler

kullanılarak seçirme seviyesi arttırılmaktadır. Osilatör örnekleme yöntemi, entropi kaynağını doğrudan yükseltilmesi ve örnekleme yönteminde daha az çevresel gürültülerden etkilenmektedir [16].



Şekil 2.2. Osilatör örnekleme yöntemi tabanlı GRSÜ blok diyagramı

Periyodik olmayan yapıları ve başlangıç koşullarına aşırı duyarlı olması sebebiyle kaotik osilatörler GRSÜ için entropi kaynağı olarak kullanılmaktadır. Kaotik osilatörlerin, diğer entropi kaynaklarına göre en büyük avantajı kaotik sinyallerin yükseltilmeye gerek duyulmayacak kadar yüksek genlik seviyesine sahip olması sebebiyle doğrudan entropi kaynağı olarak kullanılabilmesidir [17,22,43]. Şekil 2.3.'te kaos tabanlı GRSÜ blok diyagramı görülmektedir. Kaotik üreteç çıkışı, karşılaştırıcı, FF, ADC, Shimitt Triger gibi yöntemler ile örneklenecek ikili sayı dizisi oluşturulur. Oluşturulan sayı dizisi son işlem algoritmalarına tabi tutularak rasgele sayı dizileri elde edilir. Elde edilen rasgele sayı dizileri istatistiksel testlere tabi tutulur ve testlerden geçinceye kadar sistem üzerinde gerekli ayarlamalar yapılır [9]. Kaotik sistemler, sürekli zamanlı ve ayrık zamanlı kaotik sistemler olarak ikiye ayrılır. Her iki kaotik sistem ile GRSÜ çalışmaları yapılmıştır [44,45].



Şekil 2.3. Kaos tabanlı GRSÜ blok diyagramı [43]

GRSÜ'ler ile üretilen rasgele sayı dizileri, rasgelelik ve güvenilirliklerinin arttırılması amacıyla son işlem algoritmalarına tabi tutulurlar. Von Neumann son işlem

algoritması en eski ve en basit son işlem algoritmasıdır. Bit dizelerindeki düzensizliği giderir. GRSÜ çıkışı (1,0) olduğunda 1 çıkışı verir, (0,1) olduğunda 0 çıkışı verir ve diğer durumlarda çıkış vermez. Tablo 2.1.'de Von Neumann algoritmasına ait doğruluk tablosu görülmektedir. Von Neumann son işlem algoritması (0,0) ve (1,1) bit çiftlerinde çıkış vermediğinden dolayı çıkış bit hızı sabit değildir ve hız entropi kaynağının çıkışına bağlıdır. En büyük dezavantajı Von Neumann çıkış bit hızı, giriş bit hızının $\frac{1}{4}$ 'ü kadardır [39,46].

Tablo 2.1. Von Neumann son işlem algoritması doğruluk tablosu

Girilen Bit Çiftleri	Von Neumann Çıkışı
00	Çıkış yok
01	0
10	1
11	Çıkış yok

XOR son işlem algoritması, GRSÜ'nün ürettiği iki ardışık bitin XOR işlemine tabi tutulduğu yöntemdir. Çıkış bit hızı giriş bit hızının yarısı kadardır. En büyük avantajları, basitliği ve sabit bit çıkış hızıdır. Tablo 2.2.'de XOR son işlem algoritmasına ait doğruluk tablosu görülmektedir [39].

Tablo 2.2. XOR son işlem algoritması doğruluk tablosu

Girilen Bit Çiftleri	XOR Çıkışı
00	0
01	1
10	1
11	0

2.1.3. İstatistiksel rasgele sayı testleri

RSÜ çıkışlarının rasgele olup olmadığı matematiksel olarak kanıtlanamamasına rağmen uluslararası düzeyde kabul görmüş istatistiksel testler ile yorum yapmak mümkündür. İstatistiksel test sonuçları ile RSÜ çıkışlarının rasgeleliği ve kalitesi hakkında yorum yapılabilir. Bir sayı dizisinin rasgele olduğu, tabi tutulan istatistiksel testin bütün testlerinden başarılı olduğu zaman kabul edilir [47-49]. Uluslararası düzeyde kabul görmüş testlerden ikisi, FIPS 140-1 (Federal Information Processing

Standards) [50] ve NIST 800-22 (National Institute of Standards and Technology) [51] testidir. FIPS 140-1 testi blok uzunluğu kısa olan rasgele sayıların testinde kullanılır. NIST 800-22 testi ise uzun bloklardan oluşan rasgele sayıları test etmek için kullanılır. NIST 800-22 testi, FIPS 140-1 testine göre daha çok test içerir ve kriterleri daha zorlayıcıdır. Bu sebeple, bu çalışmada gerçekleştirilen GRSÜ testlerinde NIST 800-22 tercih edilmiştir.

2.1.4. FIPS 140-1 testi

FIPS 140-1 testi, 20k bitlik ikili sayı dizilerinin testi için kullanılan ve 4 ayrı testten oluşmuş uluslararası düzeyde kabul görmüş bir istatistiksel testtir. Bu testler monobit, poker, koşu ve uzun koşu testleridir. Test edilen verilerin rasgele olduğundan bahsedilebilmesi için bu 4 testin tamamından başarı ile geçmiş olması gerekir [42,50].

Monobit testi, ikili sayı dizisindeki 1'lerin sayısını inceler. Test edilen 20k bitlik verinin testi geçebilmesi için dizide bulunan 1'lerin sayısının 9654-10346 aralığında olması gerekmektedir [42,50].

Poker testinde, 'k' bitten oluşan dizi, $k \geq 5 \cdot 2^m$ olacak şekilde, üst üste çakışmayan m-bitlik parçalara bölünür ve i. parça n_i diye isimlendirilir. Teste girilen verilerin rasgeleliğinden bahsetmek için, m bitlik bloklarının hepsi k uzunluklu bir dizide aynı sayıda birbirini tekrar etmelidir. Verilerin testten başarı ile geçmesi için, Denklem (2.1)'de verilen formülle hesaplanan X değeri, $k=20000$ ve $m=4$ için, $1.03 < X < 57.4$ aralığında olmalıdır [48,50].

$$X = \frac{2^m}{k} \left(\sum_i^{2^m} n_i^2 \right) - k \quad (2.1)$$

Koşu testinde, 20k bitlik ikili sayı dizisi içinde art arda gelen 1 ve 0'lardan oluşan çeşitli uzunluktaki blokların sayısının Tablo 2.3.'te gösterildiği gibi olması, test edilen verilerin bu testten başarı ile geçtiği anlamına gelir. 6 bitten daha uzun bloklar 6 bitlik blok olarak kabul edilir [50].

Tablo 2.3. Blok uzunluklarına göre run testi koşulları

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

Uzun koşu testinde, 20k bitlik ikili sayı dizi içerisinde bulunan blok uzunluklarının sayısı, 34'ten küçük olursa, test edilen veriler testi başarı ile geçmiş olur [42].

2.1.5. NIST 800-22 testi

Uluslararası düzeyde kabul görmüş istatistiksel testlerden bir diğeri de NIST-800-22 testidir. NIST-800-22 testi, FIPS-140-1 testine göre daha fazla test içermesinden dolayı ikili sayı dizilerini daha detaylı bir şekilde testlere tabi tutmaktadır. FIPS-140-1 testinden geçen bir ikili bit dizisi NIST-800-22 testinden başarısız olabilir. Bu sebeplerden dolayı NIST-800-22 testi daha güvenilir bir test olarak kabul edilir [43,51]. NIST-800-22 testi 15 farklı test içerir. Teste tabi tutulan ikili sayı dizisinin rasgele olduğu söylenebilmesi için, bütün testlerden başarı ile geçmesi gerekir. NIST-800-22 testinde, test edilecek ikili bit dizisinin bazı parametrelerinin dışarıdan belirlenmesi gerekir. Bu testin en önemli parametrelerden birisi P-değeridir. P-değeri teste tabi tutulan ikili dizilerin rasgeleliğinin bir ölçütü olarak kabul edilmektedir. P-değeri 1'e yakın ise ikili sayı dizisinin rasgele özelliği artarken, 0'a yakın olma durumunda rasgele özelliği azalır [51]. Her istatistiksel test için bir α önem seviyesi vardır. P-değeri $\geq \alpha$ büyükse test edilen veri testten geçmiş olduğu yani verilerin rasgele olduğu anlamına gelir. P-değeri $< \alpha$ ise verilerin rasgele olmadığı anlamına gelir. Yapılan tez çalışmasında $\alpha = 0.001$ olarak alınmıştır. NIST 800-22 testinin içerdiği 15 farklı test aşağıda detaylı bir şekilde açıklanmıştır.

- a. Frekans Testi (The Frequency Test)
 - b. Bir Blok içerisinde Frekans Testi (Frequency Test within a Block)
 - c. Akış Testi (The Runs Test)
 - d. Bir Blok içerisinde En Uzun Birler Akış Testi (Tests for the Longest-Run-of-Ones in a Block)
 - e. İkili Matris Derece Testi (The Binary Matrix Rank Test)
 - f. Ayrık Fourier Dönüşüm Testi (The Discrete Fourier Transform (Spectral) Test)
 - g. Örtüşmeyen Şablon Eşleştirme Testi (The Non-overlapping Template Matching Test)
 - h. Örtüşen Şablon Eşleştirme Testi (The Overlapping Template Matching Test)
 - i. Maurer'in "Evrensel İstatistik" Testi (Maurer's "Universal Statistical" Test)
 - j. Doğrusal Karmaşıklık Testi (The Linear Complexity Test)
 - k. Seri Testi (The Serial Test)
 - l. Yaklaşık Entropi Testi (The Aproximate Entropy Test)
 - m. Birikimli Toplamlar Testi (The Cumulative Sums Test)
 - n. Rasgele Gezinimler Testi (The Random Excursions Test)
 - o. Rasgele Gezinimler Değişken Testi (The Random Excursions Variant Test)
- a. Frekans Testi (The Frequency Test)

Frekans testi, ikili bit dizisindeki 1 ve 0 dengesini inceler. Teste tabi tutulan verilerin testi geçebilmesi için, P-değeri $\geq \alpha$ olması gerekir. P-değeri aşağıda verilen denklemler yardımıyla bulunur.

$$P - \text{value} = \text{erfc}\left(\frac{S_{\text{obs}}}{\sqrt{2}}\right) \quad (2.2)$$

Denklem (2.2)'de bulunan Sobs değerinin bulmak için Denklem (2.3) kullanılır.

$$S_{\text{obs}} = \frac{|S_n|}{\sqrt{n}} \quad (2.3)$$

Denklem (2.3)'de bulunan n değeri dizinin eleman sayısıdır. S_n değerini bulmak için n elemanlı dizinin 0 olan elemanları -1, 1 olan elemanları 1 olarak alınıp toplanır. erf fonksiyon değerini bulmak için Denklem (2.4) kullanılır.

$$\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-u^2} du \quad (2.4)$$

$$\operatorname{erfc}(u) = 1 - \operatorname{erf}(u) \quad (2.5)$$

Örnek, $\varepsilon = 110010010000111111011010101000100010000101101000110000100011010011000100011010011000100110001100011001100010100010111000$ dizisi olsun. Yukarıda verilen denklemler kullanılarak;

$$n = 100$$

$$S_{100} = -16$$

$$S_{\text{obs}} = 1.6$$

P-değeri=0,109599 bulunur. P-değeri=0,109599 \geq 0.001 olduğu için veriler frekans testinden geçmiştir [43,51,53].

b. Blok Frekans Testi (Block Frequency Test)

Blok frekans testi, bit dizisini M bitlik bloklara ayırarak, blok içerisindeki '1' oranını inceler. M değerinin 1 almak frekans testini yapmak anlamına gelir. M bitlik blok içerisindeki 1 sayısının $\frac{1}{2}$ oranında olması istenir. Testin geçerli sonuçlar verebilmesi için veri bit uzunluğu en az n=100 ve blok uzunluğu M=20 olması gerekir. Test istatistiklerinin ve referans dağılımının hesaplamak için, Denklem (2.6)'da verilen ki-kare (χ^2) dağılımı kullanılır.

$$\pi_i = \frac{\sum_{j=1}^M \varepsilon_{(i-1)M+j}}{M} \quad (2.6)$$

χ^2 dağılım istatistiği $\chi^2(\text{obs})$ ise, Denklem (2.7) kullanılarak hesaplanır.

$$\chi^2(\text{obs}) = 4M \sum_{i=1}^N (\pi_i - 1/2) \quad (2.7)$$

$\chi^2(\text{obs})$ değeri, Denklem (2.8)'de yerine yazılarak P-değeri bulunur.

$$P\text{-value} = \text{igamc} \left(\frac{N}{2}, \frac{\chi^2}{2} \right) \quad (2.8)$$

Denklem (2.8)'de bulunan igamc fonksiyonu, a ve x değişkenlerine bağımlı gama fonksiyonudur ve Denklem (2.9) kullanılarak hesaplanır.

$$Q(a, x) \equiv \frac{\Gamma(a, x)}{\Gamma(a)} \equiv \frac{1}{\Gamma(a)} \int_x^{\infty} e^{-t} t^{a-1} dt \quad (2.9)$$

Örnek, $\varepsilon = 1100100100001111110110101010001000100001011010001100001000110100110001001100011001100010100010111000$ dizisi olsun. Yukarıda verilen denklemler kullanılarak;

$$n = 100$$

$$M = 10$$

$$N = 10$$

$$\chi^2 = 7,2$$

P-değeri = 0,706438 bulunur. P-değeri = 0,706438 \geq 0.001 olduğu için veriler blok frekans testinden geçmiştir [43,51,53].

c. Akış Testi (Runs Test)

Bu test, dizideki 1 ve 0 bloklarının akış değişimini inceler ve 0-1 değerleri arasındaki değişimlerin yavaş veya hızlı olması hakkında bilgi verir. Akış testinin yapılabilmesi için, $\tau=2/\sqrt{n}$ olmak üzere Denklem (2.10)'da verilen şartın sağlanması gerekir.

$$\left| \pi - \frac{1}{2} \right| \geq \tau \quad (2.10)$$

Bit akış sayısını bulmak için Denklem (2.11) kullanılır. $V_n(\text{obs})$ değerini hesaplarken, eğer $\varepsilon_k = \varepsilon_{k+1}$ ise $r(k)=0$, diğer durumda ise $r(k)=1$ olarak kabul edilir. ε üretilen bit dizisi, n bit dizisinin uzunluğu, π bit dizisindeki 1 değerlerinin sayısı, $V_n(\text{obs})$ bit akış sayısını gösterir.

$$V_n(\text{obs}) = \sum_{k=1}^{n-1} r(k) + 1 \quad (2.11)$$

$V_n(\text{obs})$ değeri bulunduktan sonra Denklem (2.12) kullanılarak P-değeri hesaplanır.

$$P\text{-value} = \text{erfc} \left(\frac{|V_n(\text{obs}) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi(1-\pi)}} \right) \quad (2.12)$$

Örnek, $\varepsilon = 1100100100001111110110101010001000100001011010001100001000110100110001001100011001100010100010111000$ dizisi olsun. Yukarıda verilen denklemler kullanılarak;

$$n = 100$$

$$\tau = 0.02$$

$$\pi = 0.42$$

$$V_n(\text{obs}) = 52$$

P-değeri= 0,500798 bulunur. P-değeri= 0,500798 \geq 0.001 olduğu için veriler akış testinden geçmiştir [43,51,53].

d. En Uzun Akış Testi (Longest Run Test)

Testin amacı, n bitlik bloklar içerisindeki en uzun ardışık 1 akışını izlemektir. En uzun koşu testi hesaplanırken, referans olarak χ^2 dağılımı kullanılmaktadır. Dizi uzunluğuna göre önerilen M blok uzunluğu değerleri; n=128 için 8, n=6272 için 128, n=750000 için 10000 olmaktadır. Dağılım istatistiği $\chi^2(\text{obs})$ değeri, Denklem (2.13) kullanılarak hesaplanır.

$$\chi^2(\text{obs}) = \sum_{i=0}^K \frac{(V_i - N\pi_i)^2}{N\pi_i} \quad (2.13)$$

Farklı uzunluklardaki bloklar için en uzun birlerin olması gereken akış frekans değerleri (v_i) Tablo 2.4.'te verilmiştir.

Tablo 2.4. Farklı blok değerleri için en uzun birlerin akış frekans değerleri

v_i	M=8	M=128	M=10000
v0	=< 1	=<4	=<10
v1	2	5	11
v2	3	6	12
v3	>=4	7	13
v4		8	14
v5		>=9	15
v6			>=16

Denklem (2.13)'te kullanılan K ve N parametrelerinin değerleri M blok uzunluklarına göre Tablo 2.5.'te gösterilmiştir.

Tablo 2.5. Blok uzunluklarına göre K ve N parametre değerleri

M	K	N
8	3	16
128	5	49
10000	6	75

Bulunan $\chi^2(\text{obs})$ değeri ve K parametresi Denklem (2.14)'de yerine koyularak P-değeri hesaplanır.

$$P\text{-value} = \text{igamc} \left(\frac{K}{2}, \frac{\chi^2(\text{obs})}{2} \right) \quad (2.14)$$

Örnek, $\varepsilon = 1100110000010101011011000100110011100000000001001001101010100010001001111010110100000001101011111001100111001101101100010110010$ dizisi olsun. Yukarıda verilen denklemler kullanılarak ve $K=3$, $M=8$ alınır;

$n = 128$

Alt Bloklar	En uzun Akış	Alt Bloklar	En uzun Akış
11001100	(2)	00010101	(1)
01101100	(2)	01001100	(2)
11100000	(3)	00000010	(1)
01001101	(2)	01010001	(1)
00010011	(2)	11010111	(3)
11001100	(2)	11100110	(3)
11011000	(2)	10110010	(2)

$$v_0 = 4, \quad v_1 = 9, \quad v_2 = 3, \quad v_4 = 0, \quad \chi^2 = 4.882457$$

P-değeri = 0,180609 bulunur. P-değeri= 0.180609 \geq 0.001 olduğu için veriler en uzun akış testinden geçmiştir [43,51,53].

e. İkili Matris Derece Testi (The Binary Matrix Rank Test)

Bu testte, öncelikle dizi bloklara bölünür ve oluşan bloklar ile matrisler oluşturulur. Bu matrisin derecesine bakılarak bloklar arasındaki doğrusal bağımlılığın olup olmadığı incelenir. Matris oluşturulurken, M satır sayısı ve Q sütun sayısını göstermek üzere $M=Q=32$ olarak alınır. Test istatistiği referans dağılımı olarak χ^2 dağılımı kullanılır. Oluşturulacak matris sayısı $N=\lfloor n/MQ \rfloor$ olarak hesaplanır. Oluşturulan matrislerden arda kalan bit sayıları ihmal edilir.

Örnek, 20 elemanlı $\varepsilon=\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{20}=01011001001010101101$ dizisi olsun. $M=Q=3$ ve $N=\lfloor 20/3 \cdot 3 \rfloor=2$ olur. Bir matriste kullanılan bit sayısı $M \cdot Q=3 \cdot 3=9$ bit olur. Test içerisinde 2 matris kullanılacağından $2 \cdot 9=18$ bit kullanılır. Arda kalan 2 bit ihmal edilir.

$$N_1 = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{vmatrix} \text{ ve } N_1 = \begin{vmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{vmatrix} \text{ matrisleri oluşturulur. Daha sonra } P_m, P_{m-1} \text{ ve } P_{m-2}$$

değerleri aşağıda gösterildiği gibi hesaplanır.

$$P_m = \prod_{j=1}^{\infty} \left[1 - \frac{1}{2^j} \right] = 0.2888$$

$$P_{m-1} \approx 2P_m = 2 \cdot 0.2888 = 0.5776$$

$$P_{m-2} \approx \frac{4P_m}{9} = \frac{4 \cdot 0.2888}{9} = 0.1284$$

χ^2 dağılımının hesaplamak için Denklem (2.15) kullanılır.

$$\chi^2(\text{obs}) = \frac{(F_M - P_m \cdot N)^2}{P_m N} + \frac{(F_{M-1} - P_{m-1} \cdot N)^2}{P_{m-1} N} + \frac{(N - F_M - F_{M-1} - P_{m-2} N)^2}{P_{m-2} N} \quad (2.15)$$

Hesaplanan değerler yerine koyulursa, χ^2

$$\chi^2(\text{obs}) = \frac{(1-0.2888 \cdot 2)^2}{0.2888 \cdot 2} + \frac{(1-0.5776 \cdot 2)^2}{0.5776 \cdot 2} + \frac{(2-1-1-0.1336 \cdot 2)^2}{0.1336 \cdot 2} = 0.597$$

olarak bulunur.

P-value = $e^{-\chi^2(\text{obs})/2} = e^{-0.597/2} = 0.742$ olarak hesaplanır. P-değeri= $0.742 \geq 0.001$ olduğu için veriler ikili matris testinden geçmiştir [43,51,53].

f. Ayrık Fourier Dönüşüm Testi (The Discrete Fourier Transform (Spectral) Test)

Bu test, dizinin tepe yüksekliklerine bakarak, dizinin periyodik olup olmadığını inceler. Örnek bir dizi ile ayrık fourier dönüşüm testi aşağıda anlatılmıştır.

Örnek dizi, 10 elamanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{10} = 1001010011$ olsun. İlk olarak (-1,1) dönüşümü yapılarak $X = 1, -1, -1, 1, -1, 1, -1, -1, 1, 1$ elde edilir. Oluşturulan X dizisine ayrık fourier dönüşümü uygulanarak Denklem (2.16)'da verilen formül ile $S = AFD(X)$ hesaplanır.

$$S_j = \sum_{k=1}^n x_k e^{(2\pi_i(k-1)j/n)} \quad (2.16)$$

Daha sonra, S dizisindeki ilk n/2 elemandan oluşan bir alt dizisi olan S' kullanılarak $M = \text{modulus}(S_j')$ fonksiyonu ile dizinin tepe yükseklikleri hesaplanır. Hesaplanan değerler, tepe yüksekliği eşik değerini aşmamalıdır. T değerinden daha küçük tepe yüksekliklerinin beklenen teorik değeri $N_0 = 0.95 \cdot n/2 = 0.95 \cdot 10/2 = 4.75$ olarak hesaplanır. Bu örnek için T'den daha az gerçek gözlemlenen tepe sayısı $N_1 = 4$ 'tür. N_0 ve N_1 değerleri kullanılarak test istatistiği hesaplanır. Bu formülden $d = -2.176$ bulunur. Bulunan d değeri kullanılarak, P-değeri;

$$P - \text{value} = \text{erfc}\left(\frac{|d|}{\sqrt{2}}\right) = \text{erfc}\left(\frac{2.176}{\sqrt{2}}\right) = 0,0129 \text{ olarak bulunur.}$$

P-değeri= 0.029 \geq 0.001 olduğu için veriler ayırık fourier testinden geçmiştir [43,51,53].

g. Örtüşmeyen Şablon Eşleştirme Testi (The Non-overlapping Template Matching Test)

Bu test, n bitlik dizinin m bitlik blokları içerisinde, belirlenen periyodik olmayan örnek bir dizinin bulunma sayısını hesaplayarak inceler. İncelenen bloklar periyodik olması durumunda, incelenen bloktan sonra gelen ilk bitten arama tekrar başlar. Eğer istenen m bitlik blok bulunamaz ise, arama bir bit kaydırılarak devam ettirilir.

Örnek dizi, 20 elemanlı $\varepsilon = 10100100101110010110$ olsun. Dizi eleman sayısı $n=20$, blok sayısı $N=2$ alınırsa, test edilecek alt blok sayısı $M=n/N=20/2=10$ olarak hesaplanır. Blok sayısı 2 olduğu için $M_1 = 1010010010$ ve $M_2 = 1110010110$ olarak iki blok oluşturulur. İstatistiksel testin içerisinde bulunan periyodik olmayan şablon örnekleri B olarak, blok içerisinde m bitlik özel B bloğunun kaç defa bulunduğu W_j olarak ifade edilir. $m=3$ ve $B=001$ örnek şablonu için B şablonunun M_1 ve M_2 blokları içerisindeki sayısı Tablo 2.6.'da gösterilmektedir.

Tablo 2.6. m=3 için M1 ve M2 blokları içerisinde B=001 şablonunun incelenmesi

Bit Pozisyonları	M ₁ Bloğu		M ₂ Bloğu	
	Bitler	W ₁	Bitler	W ₂
1-3	101	0	111	0
2-4	010	0	110	0
3-5	100	0	100	0
4-6	001 (Bulundu)	Arttır 1	001 (Bulundu)	Arttır 1
5-7	Test Edilmedi	1	Test Edilmedi	1
6-8	Test Edilmedi	1	Test Edilmedi	1
7-9	001	Arttır 2	011	1
8-10	010 (Bulundu)	2	110	1

Tablo 2.6.'da görüldüğü gibi, B=001 için W₁=2 ve W₂=1 olarak hesaplanır. Daha sonra, χ^2 dağılımını hesaplamak için,

$$\text{ortalama deęer, } \mu = (M - m + 1)/2^m = (10 - 3 + 1)/2^3 = 1.00,$$

$$\text{varyans deęeri, } \sigma^2 = M(1/2^m - (2m - 1/2^{2m})) = 10(1/2^3 - (2 \cdot 3 - 1/2^{2 \cdot 3})) = 0.468$$

olarak bulunur. Bulunan deęerler yerine koyularak, χ^2 dağılımı,

$$\chi^2(\text{obs}) = \sum_{j=1}^N \frac{(W_j - \mu)^2}{\sigma^2} = \frac{(2-1)^2 + (1-1)^2}{0.468} = 2.133$$

olarak hesaplanır. Bulunan χ^2 dağılımı ve N blok sayısı yerine yazılırsa, P-deęeri;

$$P - \text{value} = \text{igamc} \left(\frac{N}{2}, \frac{\chi^2(\text{obs})}{2} \right) = \text{igamc} \left(\frac{2}{2}, \frac{2.133}{2} \right) = 0.344$$

olarak hesaplanır. P-deęeri= 0.344 \geq 0.001 olduęu için veriler örtüşmeyen şablon eşleřtirme testinden geçmiştir [43,51,53].

h. Örtüşen Şablon Eşleştirme Testi (The Overlapping Template Matching Test)

Bu test, n bitlik dizinin m bitlik blokları içerisinde, belirlenen periyodik olmayan örnek bir dizinin bulunma sayısını hesaplayarak inceler. Örtüşmeyen şablon eşleştirme testinden farklı, örtüşme varsa arama işlemine bir bit sonra devam edilir yoksa pencere bir bit kaydırılarak arama işlemine devam edilir.

Örnek, 50 elemanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{50} = 10111011110010110100011100101110111110000101101001$ dizisi olsun. Örtüşen şablon eşleşme testi için, dizi eleman sayısı $n=50$, bağımsız blok sayısını $N=5$, bağımsızlık katsayısı $K=2$, test edilecek olan ε bitlerinin uzunluğu $M=10$ olarak alınmıştır. 50 elemanlı dizi 10 elemanlı $M_1=1011101111$, $M_2=0010110100$, $M_3=0111001011$, $M_4=1011111000$, $M_5=0101101001$ olmak üzere 5 bloğa bölünmüştür.

Tablo 2.7.'de örnek olarak şablon bit uzunluğu $m=2$ ve $B=11$ olmak üzere M_1 bloğu için B şablonunun bulunma durumları gösterilmiştir.

Tablo 2.7. M_1 bloğu içerisinde $B=11$ özel şablonunun bulunma durumları

Bit Pozisyonları	M_1 Bloğu	
	Bitler	V_i
1-2	10	0
2-3	01	0
3-4	11 (Bulundu)	Arttır 1
4-5	11 (Bulundu)	Arttır 2
5-6	10	2
6-7	01	2
7-8	11 (Bulundu)	Arttır 3
8-9	11 (Bulundu)	Arttır 4
9-10	11 (Bulundu)	Arttır 5

Daha sonra, λ değeri ve η değerleri, $\lambda = (M - m + 1)/2^m = (10 - 2 + 1)/2^2 = 2.25$ ve η değeri, $\eta = \lambda/2 = 2,25/2 = 1.125$ olarak bulunur.

$\chi^2(\text{obs})$ dağılımı değerini hesaplamak için π_i değerleri, $\pi_1=0.3246$, $\pi_2=0.1826$, $\pi_3=0.1426$, $\pi_4=0.1066$, $\pi_5=0.0771$, $\pi_6=0.1662$ olarak bulunur. Bulunan değerler yerine yazılırsa,

$$\chi^2(\text{obs}) = \sum_{j=1}^N \frac{(v_j - N\pi_j)^2}{N\pi_j} = \frac{(0 - 5 \cdot 0.3246)^2}{5 \cdot 0.3246} + \frac{(1 - 5 \cdot 0.1826)^2}{5 \cdot 0.1826} \\ + \frac{(1 - 5 \cdot 0.1426)^2}{5 \cdot 0.1426} + \frac{(1 - 5 \cdot 0.1066)^2}{5 \cdot 0.1066} + \frac{(1 - 5 \cdot 0.0771)^2}{5 \cdot 0.0771} + \frac{(1 - 5 \cdot 0.1662)^2}{5 \cdot 0.1662} = 3.1667$$

değeri bulunur. Hesaplanan $\chi^2(\text{obs})$ ve N değerleri kullanılarak, P-değeri;

$$P\text{-value} = \text{igamc} \left(\frac{N}{2}, \frac{\chi^2}{2} \right) = \text{igamc} \left(\frac{5}{2}, \frac{3.1667}{2} \right) = 0.274$$

olarak hesaplanır. P-değeri= 0.274 \geq 0.001 olduğu için veriler örtüşen şablon eşleştirme testinden geçmiştir [43,51,53].

i. Maurer “Evrensel İstatistik” Testi (Maurer’s “Universal Statistical” Test)

Bu test, rasgele sayı dizilerinin veri kaybı olmadan sıkıştırılıla bilirliğini incelemektedir. Bu test , kriptografik uygulamalarda gizli anahtar kaynağı için bir kalite ölçütü olarak değerlendirilmektedir [43]. Testte bulunan L her bir bloğun uzunluğunu, Q başlangıç bölümü ve $K=[n/L]-Q$ test bölümünü ifade eder.

Örnek, 20 elamanlı $\varepsilon=\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{20}=01011010011101010111$ dizisi olsun. $n=20$, $L=2$ ve $Q=4$ için $K=[20/2]-4=6$ olarak hesaplanır. Başlangıç bloğu $Q=4*2= 8$ bit $Q=01011010$, test bloğu ise $K=6*2=12$ bit $K=011101010111$ elde edilir. Elde edilen verilere göre, Maurer testinin L-bit uzunluktaki bloklarının bölümleri Tablo 2.8.’de gösterilmiştir.

Tablo 2.8. Maurer testi L-bit uzunluktaki blokların bölümleri

Blok	Blok Tipi	İçerik
1		01
2	Başlangıç Bölümü	01
3		10
4		10
5		01
6		11
7	Test Bölümü	01
8		01
9		01
10		11

Başlangıç bölümü için muhtemel L-bit değerleri Tablo 2.9.'da gösterilmektedir. Başlangıç blok değerlerini oluşturmak için, blok içerisindeki muhtemel L-bit ondalık değerleri, başlangıç bloğunda bulunma sayısı ile çarpılır. Tablo 2.10.'da 4 nolu satırda verilen başlangıç bölümü kullanılarak, test bölümündeki L-bit bloklarının aldığı değerler gösterilmiştir. Test bloğunda bulunan her L-bit değeri, başlangıç bloğuyla örtüşürse test bloğu, blok numarası değerini almaktadır.

Tablo 2.9. Dört başlangıç değeri ile oluşturulan muhtemel L-bit değerleri

Muhtemel L-bit Değerleri				
Başlangıç	00	01	10	11
	(T ₀ 'a kayıtlı)	(T ₁ 'e kayıtlı)	(T ₂ 'ye kayıtlı)	(T ₃ 'e kayıtlı)
	0	2	4	0

Tablo 2.10. Test bölümü için L-bit değerleri

Tekrar Bloğu	Muhtemel L-bit Değerleri			
	00	01	10	11
4	0	2	4	0
5	0	5	4	0
6	0	5	4	6
7	0	7	4	6
8	0	8	4	6
9	0	9	4	6
10	0	9	4	10

Test istatistiği Denklem (2.17)'de verilen formül ile hesaplanmaktadır.

$$f_n = \frac{1}{K} \sum_{i=Q+1}^{Q+K} \log(i - T_j) = \frac{1}{6} \sum_{i=4+1}^{10} \log(i - T_j) = \frac{1}{6} \sum_{i=4+1}^{10} \begin{pmatrix} \log(5-2)+ \\ \log(6-0)+ \\ \log(7-5)+ \\ \log(8-7)+ \\ \log(9-8)+ \\ \log(10-6) \end{pmatrix} = \quad (2.17)$$

$$\frac{1}{6} \sum_{i=4+1}^{10} (1.5849 + 4.1699 + 5.1699 + 5.1699 + 5.1699 + 7.1699) = 1.1949$$

Tablo 2.11.'de fonksiyonda beklenen değer $V_{exp}(L)$ ve varyans $var(f_n)$ değerleri verilmiştir.

Tablo 2.11. L değerleri için $V_{exp}(L)$ ve $var(f_n)$ değerleri

L	$V_{exp}(L)$	$Var(f_n)$
6	5,2177052	2,954
7	6,1962507	3,125
8	7,1836656	3,238
9	8,1764248	3,311
10	9,1723243	3,356
11	10,1700320	3,384
12	11,1687650	3,401
13	12,1680700	3,410
14	13,1676930	3,416
15	14,1674880	3,419
16	15,1673790	3,421

Tablo 2.11.'de verilen $V_{exp}(L)$ ve $var(f_n)$ değerleri yerine koyulursa, P-değeri;

$$P - \text{value} = \text{erfc} \left(\left\| \frac{f_n - V_{exp}(L)}{\sqrt{2\text{var}(f_n)}} \right\| \right) = \text{erfc} \left(\left\| \frac{1.1949 - 1.5374}{\sqrt{21.338}} \right\| \right) = 0.767$$

olarak hesaplanır. P-değeri= $0.767 \geq 0.001$ olduğu için veriler Maurer testinden geçmiştir [43,51,53].

j. Doğrusal Karmaşıklık Testi (The Linear Complexity Test)

Bu test, rasgele bit dizisinin doğrusal geri beslemeli kayan kaydedici (DGKK) uzunluğuna bakarak dizinin karmaşıklığını inceler. Karmaşıklığın yüksek olması dizinin rasgelelik kalitesini artırır.

Örnek, 13 elemanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{13} = 1101011110001$ dizisi olsun. Blok içerisindeki bit uzunluğu $M=13$ 'tür. N değeri ise M bit blokların sayısını belirtir ve $n=M*N$ eşitliği ile hesaplanır. N katsayısı, blokların her birinin doğrusal karmaşıklığı polinomun en düşük derecesini bulan Berlekamp-Massey algoritması kullanılarak hesaplanır. Örnek olarak verilen dizi için $N=1$ ve $L_i=4$ olmaktadır. T_i dağılımının rasgele değişkenini hesaplamak için, μ değeri,

$$\mu = \frac{M}{2} + \frac{(9 + (-1)^{M+1})}{36} - \frac{(M/3 + 2/9)}{2^M} =$$

$$\frac{13}{2} + \frac{(9 + (-1)^{13+1})}{36} - \frac{(13/3 + 2/9)}{2^{13}} = 6.7772$$

olarak bulunur. T_i değerini hesaplamak için μ değeri denklemden yerine koyulursa ;

$$T_i = (-1)^M \cdot (L_i - \mu) + 2/9 = (-1)^{13} \cdot (4 - 6.777) + 2/9 = 2.999 \text{ olarak bulunur. } \pi_i$$

değerleri, $\pi_0=0.0104$, $\pi_1=0.03125$, $\pi_2=0.125$, $\pi_3=0.5$, $\pi_4=0.25$, $\pi_5=0.0625$ ve $\pi_6=0.020833$ olarak hesaplanır. Bulunan değerler χ^2 dağılımı formülünde yerine koyulursa, χ^2 dağılımı;

$$\chi^2(\text{obs}) = \sum_{i=1}^K \frac{(v_i - N\pi_i)^2}{N\pi_i} = 47.0008 \text{ olarak bulunur.}$$

Bulunan değerler kullanılarak P-değeri;

$$P\text{-value} = \text{igamc} \left(\frac{K}{2}, \frac{\chi^2(\text{obs})}{2} \right) = \text{igamc} \left(\frac{6}{2}, \frac{47.008}{2} \right) = 0.993 \text{ olarak hesaplanır.}$$

P-değeri= 0.993 \geq 0.001 olduğu için veriler doğrusal karmaşıklık testinden geçmiştir [43,51,53].

k. Seri Testi (The Serial Test)

Bu test, n bit uzunluğundaki diziyi, m bit uzunluğundaki bloklara böler ve elde edilen dizileri, aynı değişimi ve tek düzelelik seviyesini incelemek üzere karşılaştırır. Seri test için m=1 olursa frekans testi gibi işlem yapar. Bu test sonucunda, Pdeğeri1 ve P-değeri2 olmak üzere iki değer elde edilir.

Örnek, 10 elemanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{10} = 0011011101$ dizisi olsun. ε' dizisi, dizinin sonuna 0 biti eklenmesi sonucunda oluşturulan artırım dizisidir. Örnek olarak, m=1 için $\varepsilon' = 0011011101$ (m) iken, m=2 için $\varepsilon' = 00110111010$ (m-1) ve m=3 için $\varepsilon' = 001101110100$ (m-2) gösterilebilir.

Bit dizisinde, m=3 iken, m-1=2 ve m-2=1'dir. 3-bitlik blokların frekansları $v_{000}=0$, $v_{001}=1$, $v_{010}=1$, $v_{011}=2$, $v_{100}=1$, $v_{101}=2$, $v_{110}=2$, $v_{111}=1$, 2-bitlik blokların frekansları $v_{00}=1$, $v_{01}=3$, $v_{10}=3$, $v_{11}=3$ ve 1-bitlik blokların frekansları $v_0=4$, $v_1=6$ olarak hesaplanır. Dizideki, m bit örneğin gözlemlenen frekansının kalitesi $\Delta\Psi_m^2(\text{obs})$ ölçütü ile beklenen frekans kalitesi ise $\Delta^2\Psi_m^2(\text{obs})$ ölçütü ile gösterilir. Ψ_m^2 , Ψ_{m-1}^2 ve Ψ_{m-2}^2 değerleri sırasıyla Denklem (2.18)'de verilen formüller ile hesaplanır.

$$\begin{aligned} \Psi_m^2 &= \frac{2^m}{n} \sum_{i_1 \dots i_m} \left(v_{i_1 \dots i_m}^2 - n \right) & \Psi_{m-1}^2 &= \frac{2^{m-1}}{n} \sum_{i_1 \dots i_{m-1}} \left(v_{i_1 \dots i_{m-1}}^2 - n \right) \\ \Psi_{m-2}^2 &= \frac{2^{m-2}}{n} \sum_{i_1 \dots i_{m-2}} \left(v_{i_1 \dots i_{m-2}}^2 - n \right) \end{aligned} \quad (2.18)$$

Örnek verilen dizi için;

$$\Psi_m^2 = \frac{2^3}{10}(0+1+1+4+1+4+4+1)-10 = 2.8$$

$$\Psi_{m-1}^2 = \frac{2^{3-1}}{10}(1+9+9+9)-10 = 1.2$$

$$\Psi_{m-2}^2 = \frac{2^{3-2}}{10}(16+36)-10 = 0.4$$

Sonuçları elde edilir. Rasgelelik testi için geliştirilmiş seri istatistiklerinin cevabı Denklem (2.19) kullanılarak hesaplanır.

$$\Delta\Psi_m^2 = \Psi_m^2 - \Psi_{m-1}^2 \quad (2.19)$$

$$\Delta^2\Psi_m^2 = \Psi_m^2 - 2\Psi_{m-1}^2 + \Psi_{m-2}^2$$

Yukarıda bulunan değerler yerine koyulduğunda;

$$\Delta\Psi_m^2 = 2.8 - 1.2 = 1.6$$

$$\Delta\Psi_m^2 = 2.8 - 1.2 = 1.6$$

sonuçları elde edilir. P-değeri1 ve P-değeri2 değerlerini bulmak için, elde edilen veriler Denklem (2.20)'de yerine koyulur.

$$P\text{-value } 1 = \text{igamc} \left(2^{m-2}, \nabla\Psi_m^2/2 \right) \quad (2.20)$$

$$P\text{-value } 2 = \text{igamc} \left(2^{m-3}, \nabla^2\Psi_m^2/2 \right)$$

Yapılan işlemler sonucunda, P-değeri1 ve P-değeri2;

$$P\text{-value } 1 = \text{igamc} \left(2^{3-2}, \frac{1.6}{2} \right) = 0.905$$

$$P\text{-value } 2 = \text{igamc} \left(2^{3-3}, \frac{0.8}{2} \right) = 0.880$$

olarak hesaplanır. P-değeri₁ = 0.905 \geq 0.001 ve P-değeri₂ = 0.880 \geq 0.001 olduğu için veriler seri testinden geçmiştir [43,51,53].

1. Yaklaşık Entropi Testi (The Aproximate Entropy Test)

Bu test, muhtemel örtüşen m bitlik örnek dizinin frekansını inceler. Seri testinden farkı, dizi için beklenen frekansın, iki ardışık veya bitişik uzunluktaki örtüşen blokların frekanslarını karşılaştırmasıdır.

Örnek, 10 elemanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{10} = 0100110101$ dizisi olsun. Blok içerisindeki bit uzunluğu $n=10$ ve $m=3$ 'tür. Dizinin sonuna dizinin başından $m-1$ bit eklendiğinde. $m-1=2$ olduğundan yeni dizimiz $\varepsilon = 0100110101$ olarak değişir. Daha sonra, $m=3$ olduğu için oluşturulan dizi ardışık olarak önce m sonra $m+1$ bitlik bloklara bölünür. Sonraki aşamada, m bit blokların değerleri olan i ve muhtemel m bit değerlerin sayısı olan C_i^m , $C_i^m = \#i/n$ formülü kullanılarak hesaplanır. Buradan, $\pi_i = C_j^m$ ve $j = \log_2 i$ olmak üzere m bit uzunluktaki bütün 2^m muhtemel blokların dizi üzerindeki ampirik dağılımın frekansı $\varphi^{(m)}$ Denklem (2.21) kullanılarak hesaplanır.

$$\varphi^{(m)} = \sum_{i=0}^{2^m-1} \pi_i \log \pi_i \quad (2.21)$$

Ki-kare testi için bulunan değerler Denklem (2.22)'de yerine koyularak,

$$\text{ApEn}(m) = \varphi^{(m)} - \varphi^{(m+1)} \quad (2.22)$$

$ApEn(m) = -1.6434 - (-1.8343) = 0.1909$ sonucu elde edilir. Elde edilen sonuç ki-kare sonucunu hesaplamak için Denklem (2.23)'de yerine koyularak,

$$ApEn(m) = \varphi^{(m)} - \varphi^{(m+1)} \quad (2.23)$$

$\chi^2 = 2 * 10(0.6931 - 0.1909) = 0.5021$ sonucu elde edilir. Bulunan ki-kare değerini kullanarak, P-değeri;

$$P - \text{value} = \text{igamc} \left(2^{m-1}, \frac{\chi^2}{2} \right) = \text{igamc} \left(2^{2-1}, \frac{0.5021}{2} \right) = 0.261$$

olarak bulunur. P-değeri = 0.261 \geq 0.001 olduğu için veriler yaklaşık entropi testinden geçmiştir [43,51,53].

m. Birikimli Toplamlar Testi (The Cumulative Sums Test)

Bu test, dizinin birikimli toplamının beklenen davranışı için kısmi alt blokların birikimli toplamının çok büyük veya çok küçük olup olmadığı inceler. İlk olarak bit dizisi, X_i dizisini elde etmek için, $X_i = 2\varepsilon_i - 1$ dönüşümü kullanılarak 0 olan bitlere -1 ve 1 olan bitlere +1 yazılarak normalize edilir. Rasgelelik durumu için sonuç 0'a yakın olmalıdır.

Örnek, 10 elemanlı $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{10} = 1011010111$ dizisi olsun. Dizi normalize edilerek, $X = 1, -1, 1, 1, -1, 1, -1, 1, 1, 1$ dizisi elde edilir. Test ileri ve geri yönlü olmak üzere iki farklı yöntem kullanılarak gerçekleştirilir. Test yapılırken 0 seçilirse ileri yönlü, 1 seçilirse geri yönlü olarak çalışmaktadır. Tablo 2.12.'de ileri ve geri yönlü çalıştırılma gösterilmiştir

Tablo 2.12. İleri ve geri yönlü metotların uygulanması

Metot1=0 (İleri yönlü)	Metot2=1 (Geri yönlü)
$S_1=X_1$	$S_1=X_n$
$S_2=X_1+X_2$	$S_2=X_n+X_{n-1}$
$S_3=X_1+X_2+X_3$	$S_3=X_n+X_{n-1}+X_{n-2}$
:	:
$S_k=X_1+X_2+X_3+\dots+X_k$	$S_k=X_n+X_{n-1}+X_{n-2}+\dots+X_{n-k+1}$
:	:
$S_n=X_1+X_2+X_3+\dots+X_k+\dots+X_n$	$S_n=X_n+X_{n-1}+X_{n-2}+\dots+X_{n-k+1}+\dots+X_1$

Verilen örnekte, uygulama metoduna 0 verilerek ileri yönlü metot seçilmiştir.

$$S1=1$$

$$S2=1+(-1)=0$$

$$S3=1+(-1)+1=1$$

$$S4=1+(-1)+1+1=2$$

$$S5=1+(-1)+1+1+(-1)=1$$

$$S6=1+(-1)+1+1+(-1)+1=2$$

$$S7=1+(-1)+1+1+(-1)+1+(-1)=1$$

$$S8=1+(-1)+1+1+(-1)+1+(-1)+1=2$$

$$S9=1+(-1)+1+1+(-1)+1+(-1)+1+1=3$$

$$S10=1+(-1)+1+1+(-1)+1+(-1)+1+1+1=4$$

Elde edilen sonuçtan, z test istatistik değeri $z=\max_{1 \leq k \leq n} |4| = 4$ olmaktadır. Denklem (2.24) kullanılarak P-değeri hesaplanır.

$$\begin{aligned}
 P - \text{value} = 1 - & \sum_{k=\left(\frac{-n}{z}+1\right)/4}^{\left(\frac{n-1}{z}\right)/4} \left[\Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k-1)z}{\sqrt{n}}\right) \right] + \\
 & \sum_{k=\left(\frac{-n}{z}-3\right)/4}^{\left(\frac{n-1}{z}\right)/4} \left[\Phi\left(\frac{(4k+3)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) \right]
 \end{aligned} \tag{2.24}$$

Elde edilen değerler Denklem (2.24)'te yerlerine koyulduğunda, P-değeri= 0.411 olarak bulunur. P-değeri= 0.411 \geq 0.001 olduğu için veriler birikimli toplamlar testinden geçmiştir [43,51,53].

n. Rasgele Geziniimler Testi (The Random Excursions Test)

Bu test, birikimli toplam rasgele yürüyüşünde K adet döngünün sayısını hesaplar. İlk olarak bit dizisi, X_i dizisini elde etmek için, $X_i=2\epsilon_i-1$ dönüşümü kullanılarak 0 olan bitlere -1 ve 1 olan bitlere +1 yazılarak normalize edilir. Daha sonra, birikimli toplam rasgele yürüyüşü, kısmi toplamlarının hesaplanması ile elde edilir. Bu testte, -4, -3,-2, -1 ve +1, +2, +3, +4 olmak üzere sekiz P-değeri hesaplanır. Örnek, 10 elemanlı $\epsilon_{10}=0110110101$ dizisi olsun. Normalize işlemi yapıldığında X_i dizisi $X=-1, 1, 1, -1, 1, 1, -1, 1, -1, 1$ olur. Birikimli toplamlar testin için metot 0 seçilerek ileri yönlü metot tercih edildiğinde $S_1=-1, S_2=0, S_3=1, S_4=0, S_5=1, S_6=2, S_7=1, S_8=2, S_9=1, S_{10}=2$ değerleri elde edilir ve $S=\{-1, 0, 1, 0, 1, 2, 1, 2, 1, 2\}$ oluşturulur. S' kümesi, S kümesinin başına ve sonuna 0 eklenerek $S'=\{0, -1, 0, 1, 0, 1, 2, 1, 2, 1, 2, 0\}$ oluşturulur. Döngü sayısı dizideki başa ve sona eklenen sıfırlar hariç sıfır sayısıdır ve J ile ifade edilir. $J_1=\{0, -1, 0\}, J_2=\{0, 1, 0\}$ ve $J_3=\{0, 1, 2, 1, 2, 1, 2, 0\}$ olarak 3 tane J döngüsü bulunmaktadır. x durum değerlerinin frekansları, döngüler kullanılarak Tablo 2.13.'te gösterildiği gibi hesaplanır. Döngü içerisindeki her bir durum değerinin frekansı x $-4 \leq x \leq -1$ ve $1 \leq x \leq 4$ değer aralığında hesaplanmaktadır.

Tablo 2.13. ϵ dizisi için oluşan rasgele gezinti döngü frekansları

Durum x	Döngüler (J)		
	Döngü 1 (J_1)	Döngü 2 (J_2)	Döngü 3 (J_3)
-4	0	0	0
-3	0	0	0
-2	0	0	0
-1	1	0	0
1	0	1	3
2	0	0	3
3	0	0	0
4	0	0	0

Daha sonra, döngüler arasında k defa meydana gelen x durumundaki döngünün toplam sayısı $v_k(x)$ hesaplanmaktadır. Bu işlem x değerinin 8 farklı durumu için tekrarlanır ve hesaplamak için Denklem (2.25)'te verilen ki-kare istatistiği kullanılır.

$$\chi^2(\text{obs}) = \sum_{k=0}^5 \frac{(v_k(x) - J\pi_k(x))^2}{J\pi_k(x)} \quad (2.25)$$

x=1 için ki-kare istatistiği hesaplanırsa;

$$\begin{aligned} \chi^2 &= \frac{(1-3(0.5))^2}{3(0.5)} + \frac{(1-3(0.25))^2}{3(0.25)} + \frac{(0-3(0.125))^2}{3(0.125)} \\ &+ \frac{(1-3(0.0625))^2}{3(0.0625)} + \frac{(0-3(0.0312))^2}{3(0.0312)} + \frac{(0-3(0.0312))^2}{3(0.0312)} = 4.3330 \end{aligned}$$

sonucu elde edilir. Elde edilen sonuç P-değeri1 değerini bulmak için yerine yazıldığında P-değeri1= $igamc(5/2, 4.3330/2) = 0.502$ sonucu bulunur. P-değeri1= $0.502 \geq 0.001$ olduğu için sonuç olumludur. Fakat verilerin rasgele gezinimler testinden geçtiğini kabul etmek için x'in diğer değerleri için de P-değerleri hesaplanmalıdır [43,51,53].

o. Rasgele Geziniimler Değişken Testi (The Random Excursions Variant Test)

Bu test, birikimli toplam rasgele yürüyüşte belirli durumların toplam meydana gelme sayısını inceler. İlk olarak bit dizisi, X_i dizisini elde etmek için, $X_i = 2\epsilon_i - 1$ dönüşümü kullanılarak 0 olan bitlere -1 ve 1 olan bitlere +1 yazılarak normalize edilir. Daha sonra, birikimli toplam rasgele yürüyüşü kısmi toplamlarının hesaplanması ile elde edilir. Bu testte, 9, -8, -7, -6, -5, -4, -3, -2, -1 ve +1, +2, +3, +4, +5, +6, +7, +8, +9 olmak üzere on sekiz P-değeri hesaplanır.

Örnek, 10 elemanlı $\epsilon_{10} = 0110110101$ dizisi olsun. Normalize işlemi yapıldığında X_i dizisi $X = -1, 1, 1, -1, 1, 1, -1, 1, -1, 1$ olur. Birikimli toplamlar testin için metot 0

seçilerek ileri yönlü metot tercih edildiğinde $S_1=-1, S_2=0, S_3=1, S_4=0, S_5=1, S_6=2, S_7=1, S_8=2, S_9=1, S_{10}=2$ değerleri elde edilir ve $S=\{-1, 0, 1, 0, 1, 2, 1, 2, 1, 2\}$ oluşturulur. S' kümesi, S kümesinin başına ve sonuna 0 eklenerek $S'=\{0, -1, 0, 1, 0, 1, 2, 1, 2, 1, 2, 0\}$ oluşturulur. Bu testte, J değeri rasgele dizideki döngü sayısını ve ξ bütün rasgele yürüyüşler süresince ziyaret edilen durumların toplam sayısını ifade eder. Örnek dizi için, $\xi(-1)=1, \xi(1)=4, \xi(2)=3$ ve diğerleri $\xi(x)=0$ olmaktadır. Döngü içerisindeki her bir durum değerlerinin frekansları x $-9 \leq x \leq -1$ ve $1 \leq x \leq 9$ değer aralığında hesaplanmaktadır. Her bir $\xi(x)$ değeri için, 18 farklı P-değeri Denklem (2.26) yardımıyla hesaplanmaktadır.

$$P - \text{value} = \text{erfc} \left(\frac{|\xi(x) - J|}{\sqrt{2J(4|x| - 2)}} \right) \quad (2.26)$$

$x=1$ durumu için P-değeri1 hesaplandığında;

$$P - \text{value} = \text{erfc} \left(\frac{|4 - 3|}{\sqrt{23(4|1| - 2)}} \right) = 0.683$$

sonucu bulunur. $P\text{-değeri}1 = 0.683 \geq 0.001$ olduğu için sonuç olumludur. Fakat verilerin rasgele gezinimler değişken testinden geçtiğini kabul etmek için. $\xi(x)$ 'in diğer değerleri için de P-değerleri hesaplanmalıdır [43,51,53].

2.2. PIC Mikro Denetleyiciler

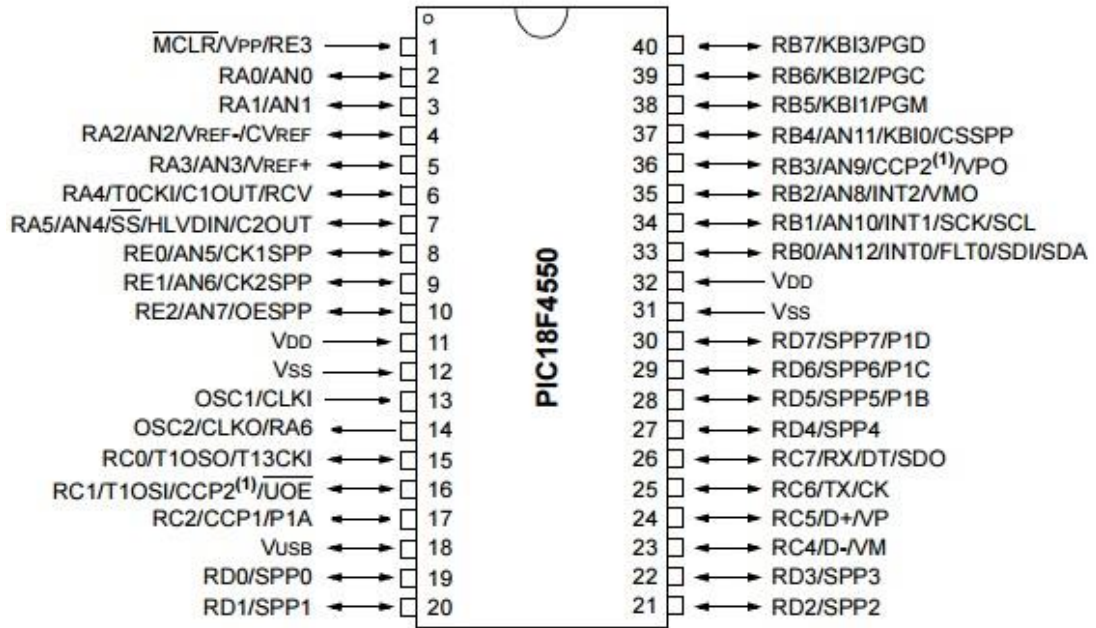
Bir mikro denetleyici, komple bir bilgisayarın tek bir entegre devre üzerinde üretilmiş halidir. Günümüzde mikro denetleyici üreten pek çok firma bulunmaktadır. Bunlara örnek olarak Intel, Motorola, AMD, Philips, Siemens, Texas Instruments, Dallas, Atmel, Microchip, Hitachi, Analog Devices, National gibi firmalar gösterilebilir [54,55].

Microchip Technology firması tarafından üretilen mikro denetleyiciler Çevresel Arabirim Denetleyicisi (PIC) olarak adlandırılmaktadır. PIC mikro denetleyiciler, RISC mimarisi kullanılarak tasarlanmıştır. RISC mimarisinde, program kodları ve veriler ayrı bellek bloklarında tutulurlar. RISC mimarisi kullanılarak tasarlanan işlemcilerde bir komut, 1 dahili saat çevriminde çalıştırılır ve yazılan programların verileri işleme için çok az sayıda komut ihtiyaç vardır. Bu sebeple işlem hızları yüksektir [54-56].

PIC mikro denetleyiciler, güvenilirlik, komut seti, hız, static işlem, yazılım kolaylığı, piyasada bulunabilirliği, fiyatı ve uygulama örnek sayısı gibi özellikleri ile diğer mikro denetleyicilerden daha fazla tercih edilirler [55,56].

PIC18F4550, Microchip Technology firması tarafından üretilen 18F serisi mikro denetleyicilerden biridir. PIC18F4550, USB desteği, çalışma frekans aralığının yüksekliği, yüksek program hafıza boyutu, düşük güç tüketimi, 10 bit A/D çevirici sayısı gibi özelliklere sahiptir.

Ayrıca PIC18f4550, USB 2.0 versiyonu ile uyumludur. Bekleme modunda çekilen akım yaklaşık olarak 6 μ A iken, uyku modunda çekilen akım yaklaşık olarak 0,1 μ A dir. PIC18F4550 bünyesinde, 32 kbayt flash memory, 2 kbayt SRAM ve 256 bayt EEPROM bulundurmaktadır [54,56].



Şekil 2.4. PIC18F4550 giriş/çıkış portlarının fonksiyonları

Şekil 2.4.'te görüldüğü gibi PIC18F4550 birden fazla amaç için kullanılan ve multiplexer ile anahtarlanan 5 adet giriş/çıkış portuna sahiptir [54,56].

BÖLÜM 3. KAOS VE ENTROPİ KAYNAĞI REFERANS KAOTİK SİSTEMLERİN ANALİZLERİ

Kaos, düzensizliğin düzeni olarak ifade edilen, doğrusal olmayan olayları açıklamaya yardımcı bir bilim dalıdır. Kaos, karmaşık davranışların yanında kendine has bir iç düzene sahip olmasından dolayı rastlantısal bir olay değildir. Kaos, dinamik sistemlerin bilinen en karmaşık hali olarak ifade edilebilir. Kaos, rasgele düşünülen durumların içinde hassas farklardan meydana gelen olayların bir birbiri ile ilişkisine odaklanır. Kaos bilim dalı, gerçek hayatta, bulutların hareketi, sigara dumanı hareketi, köpüren nehir hareketleri, musluktan akan suyun hareketi vb. rasgele davranış gösterdiği düşünülen olayları anlamaya çalışan bilim dalıdır [19-21].

Kaos, kısaca başlangıç ve giriş şartlarına aşırı duyarlı dinamik sistemler olarak ifade edilebilir [19,20]. Kaotik sistemlerin başlangıç ve giriş şartlarına olan bu duyarlılığından dolayı bu değerlerde yapılacak küçük değişimler sistemin çıkışının değişmesine sebep olmaktadır. Bu sebepten dolayı, kaotik yapılar deterministik sistemler olmalarına rağmen sadece kısa bir süreliğine sistemin davranışı tahmin edilebilmektedir. Daha sonraki iterasyonlarda ise kaotik sistemlerin davranışları önceden tahmin edilmez bir hal almaktadır [19-21]. Bu özelliklerinden dolayı, kriptoloji, kontrol, görüntü işleme, haberleşme ve yapay sinir ağları gibi bilimsel ve endüstriyel alanlar üzerine yapılan kaotik sistem çalışmalarının sayısı hızla artmaktadır [21,43,57].

3.1. Kaotik Sistemler

Kaotik sistemler ayrık zamanlı ve sürekli zamanlı kaotik sistemler olarak iki grupta incelenebilir. Ayrık zamanlı kaotik sistemler genellikle tek veya çift boyutludur yani

bir veya iki denklemden oluşabilir. Sürekli zamanlı kaotik sistemler ise en az üç boyutludur yani en az üç denklem içerir [21,28,58].

3.1.1. Ayrık zamanlı kaotik sistemler

Ayrık zamanlı kaotik sistemler, uygun bir nonlineer fonksiyonun iterasyonu ile oluşan başka bir deyişle, geri besleme özelliği bulunan kaotik sistemlerdir. Ayrık zamanlı kaotik sistemler dijital ortamlarda, sürekli zamanlı kaotik sistemler gibi ayırıklaştırma algoritmalarına gerek kalmadan doğrudan istenen uygulamalarda kullanılabilir.

Literatürde, tek boyutlu ve çift boyutlu birçok ayrık zamanlı kaotik sistemler bulunmaktadır [21,57,58]. Tek boyutlu ayrık zamanlı kaotik sistemlere, Logistic Map [59], Cubic Map [60], Sine Map [61] ve Tent Map [62] kaotik sistemleri örnek olarak gösterilebilir. Çift boyutlu ayrık zamanlı kaotik sistemlere ise Henon Map [63], Lozi Map [64], Burgers Map [65], Discrete Predator Prey Map [66] ve Arnold's Cat Map [67] örnek olarak gösterilebilir.

3.1.2. Sürekli zamanlı kaotik sistemler

Sürekli zamanlı kaotik sistemler (SZKS) genellikle adi diferansiyel denklemler ile ifade edilmektedir. Sürekli zamanlı n tane birinci dereceden adi diferansiyel denklem sistemi $i=1, 2, 3, \dots, n$ olmak üzere Denklem (3.1) gibi olabilir [21,68].

$$\left. \begin{aligned} dx^{(i)}/dt &= f_1(x^{(i)}, x^{(i+1)}, \dots, x^{(n)}) \\ dx^{(i+1)}/dt &= f_2(x^{(i)}, x^{(i+1)}, \dots, x^{(n)}) \\ &\vdots \\ dx^{(n)}/dt &= f_n(x^{(i)}, x^{(i+1)}, \dots, x^{(n)}) \end{aligned} \right\} \quad (3.1)$$

Yukarıdaki ifadeler düzenlenirse adi diferansiyel denklemler vektörel formda Denklem (3.2)'deki gibi olabilir.

$$\begin{aligned} dx(t)/dt &= F[x(t)] \\ x(t_0) &= x_0 \end{aligned} \tag{3.2}$$

Denklemden verilen x , n boyutlu bir vektördür. Ayrıca $x \in R^n$ durum vektörüdür. x_0 başlangıç durum vektörünü ifade ederken, t ise zamanı ifade etmektedir. Ayrık zamanlı kaotik sistemler, doğrusal olmayan tek boyutlu basit denklemlerle ifade edilirken, sürekli zamanlı kaotik sistemler en az 3 boyutludur. Yani n ifadesi en az üç olmalıdır [21,68].

Literatürde, sürekli zamanlı kaotik sistemlere, Lorenz [69], Rössler [70], Duffing [71], Chua [72], Van Der Pol [73], Chen [74], Rikikate [75], Rucklidge [76,77] kaotik sistemi, hiperkaotik sistemlere ise Arneodo [78], Hindmarsh-Rose [38], Zhongtang [79] kaotik sistemleri örnek olarak gösterilebilir.

3.2. Kaotik Sistem Analiz Yöntemleri

Bir sistemin kaotik olup olmadığını tespit etmek için kullanılan birçok analiz yöntemi vardır. Kaotik bir sistemin belirli bir zaman içerisinde nasıl bir davranış gösterdiği (zaman serileri), kaotik çekicileri (faz portreleri), Lyapunov üstelleri, Çatallaşma diyagramları, Poincare kesiti, sistemin denge noktalarını tespit etmek bunlardan sadece bazılarıdır. Bu yöntemlerden birkaçına bakılarak sistemin kaotik olup olmadığına karar verilebilir [21,57,80].

3.2.1. Denge nokta analizi

Kaotik sistemler basit fonksiyonlara sahip olmadığından, bu sistemler hakkında doğrudan yorum yapmak mümkün değildir. Bundan dolayı doğrusal olmayan dinamik sistem olan kaotik sistemlerin davranışını anlamak için sistemin denge noktaları bulunarak analiz edilmesi gerekmektedir [21].

Denge nokta analizinde; öncelikle sistem denge noktaları bulunur. Denge noktaları, denklemlerin türevleri sıfıra eşitlenerek çözümlenir. Denklemler çözüldükten sonra,

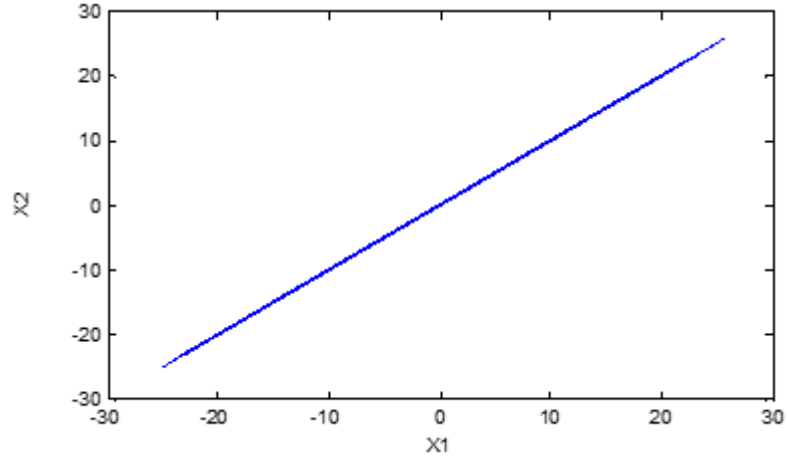
bulunan sonuç reel sayılar ise sistemin denge noktaları mevcuttur denilebilir. Bazı kaotik sistemlerin reel denge noktaları yoktur. Sadece sanal denge noktalarına sahiptir. Bazı sistemlerin ise hiç denge noktası yoktur.

Denge noktaları reel veya sanal olarak bulunduktan sonra sistemin Jacobian matrisine denge noktalarında bulunan sonuçlar yazılır ve karakteristik denge çözümünden öz değerler bulunur [21].

Denge noktalarındaki kararsızlık durumu, öz değerlerden anlaşılabilir. Bulunan öz değerlerden en az birinin reel kısmının pozitif olması, denge noktasının kararsızlığını gösterir ve sistemin kaotik davranışa sahip olduğuna bir işarettir. Fakat kesin olarak kaotik durumun ispatı için Lyapunov veya Çatallaşma analizi gibi analizler yapılmalıdır [21].

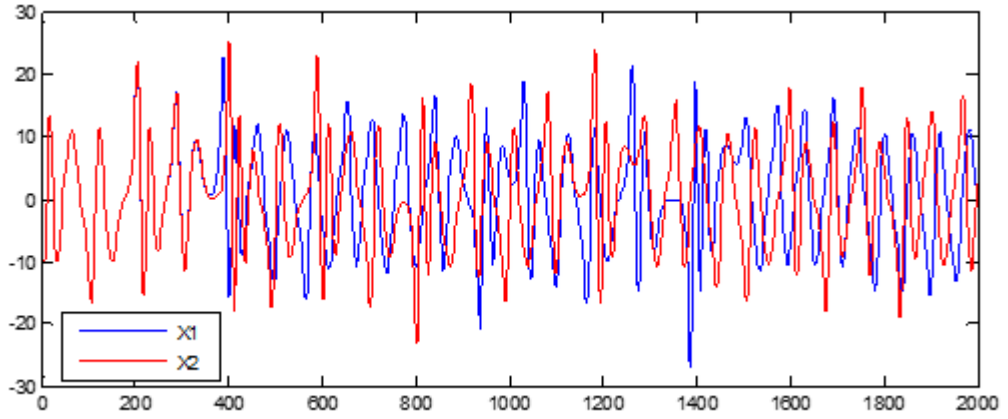
3.2.2. Zaman serileri ve başlangıç değerlerine bağımlılık analizi

Sistemin başlangıç değerlerinde yapılan değişimler sonucunda sistem çıkışlarının değişmesi, sistemin kaotik davranıp davranmadığı noktasında bilgi vermektedir. Bu değişimi anlamamanın en basit yollarında biri, farklı başlangıç değerlerine sahip sistemin aynı ekranda incelenmesidir [21]. Şekil 3.1'de aynı başlangıç değerlerine sahip örnek kaotik sistemin X1 ve X2 çıkış sinyallerinin birbirine göre grafiği görülmektedir.



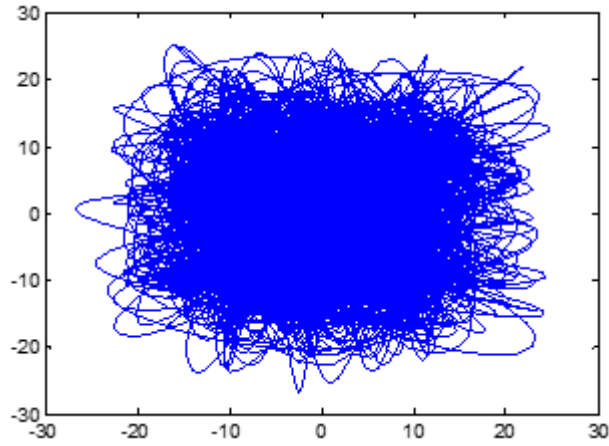
Şekil 3.1. Örnek aynı başlangıç değere sahip kaotik sistemin X1 ve X2 çıkışlarının birbirine göre grafiği

Şekil 3.2.'de örnek kaotik sistemin başlangıç değerinde yapılan çok küçük farklılığın, kaotik sistem çıkışını çok farklı yerlere götürdüğü görülmektedir. X1 sinyali için başlangıç değeri 10V, X2 sinyali için başlangıç değeri 10.0001V alınmıştır.



Şekil 3.2. Örnek farklı başlangıç değerlere sahip aynı sistemin zaman serisi çıktıları

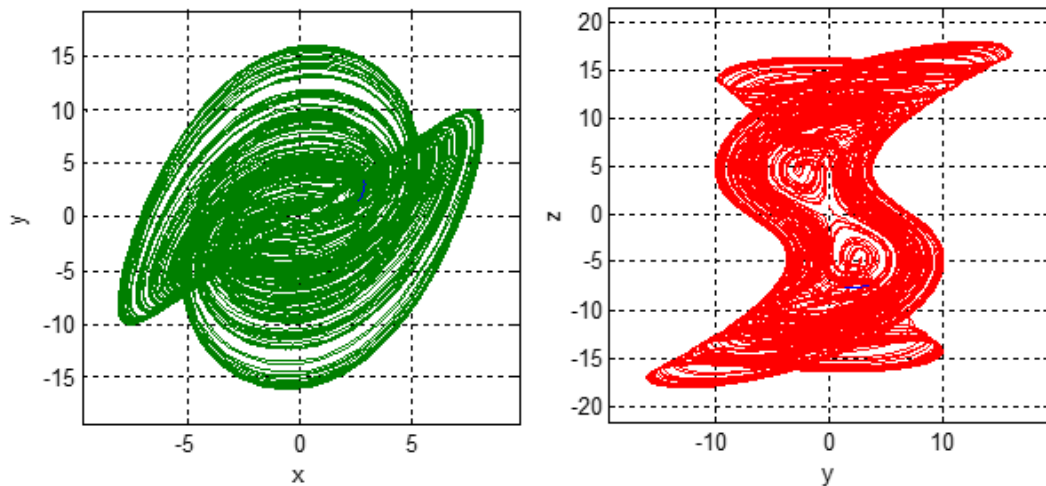
Şekil 3.3.'te farklı başlangıç değerlerine sahip örnek kaotik sistemin X1 ve X2 çıkış sinyallerinin birbirine göre grafiği görülmektedir.



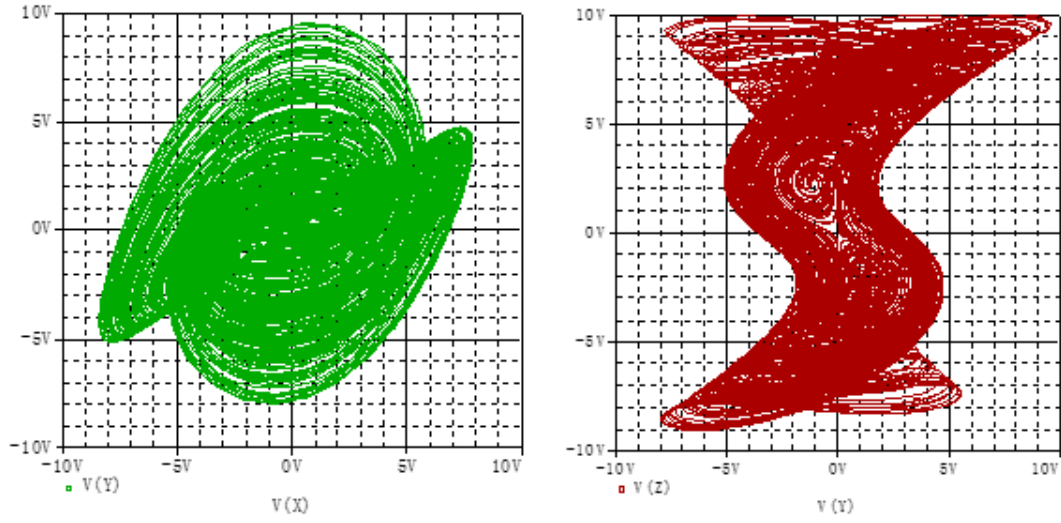
Şekil 3.3. Örnek farklı başlangıç değerlere sahip kaotik sistemin X1 ve X2 çıkışlarının birbirine göre grafiği

3.2.3. Faz portresi analizi

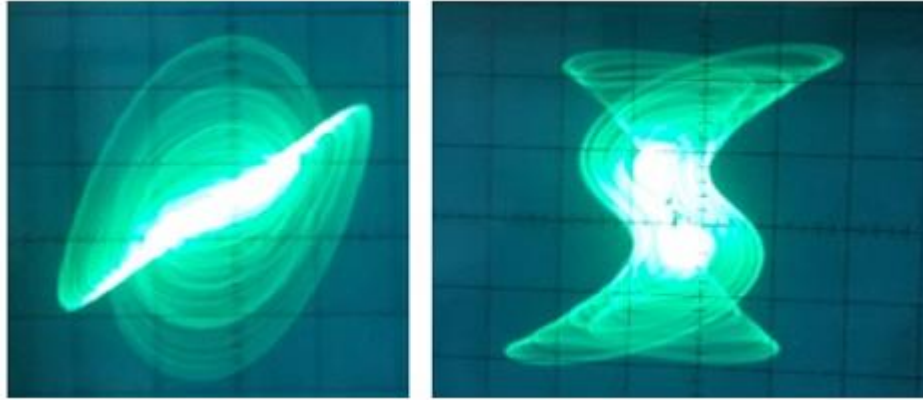
Üç boyutlu bir sistem için XY, YZ, XZ ve XYZ olarak dört farklı şekilde faz portrelerine bakılabilir. Matlab Odesolve programına sistemin denklemleri girilerek sistemin faz portreleri elde edilebilmektedir [21]. Ayrıca, kaotik sistemin elektronik devre gerçekleştirilmesi yapıldıktan sonra simülasyon programları veya yapılan gerçek elektronik devrelerin osiloskop çıktıları ile faz portreleri elde edilebilir [21]. Şekil 3.4.'te Matlab Odesolve, Şekil 3.5.'te OrCAD-PSpice ve Şekil 3.6.'da osiloskop örnek faz portre çıktıları görülmektedir.



Şekil 3.4. Örnek Matlab faz portre çıktısı



Şekil 3.5. Örnek OrCAD-PSpice programı faz portre çıktısı

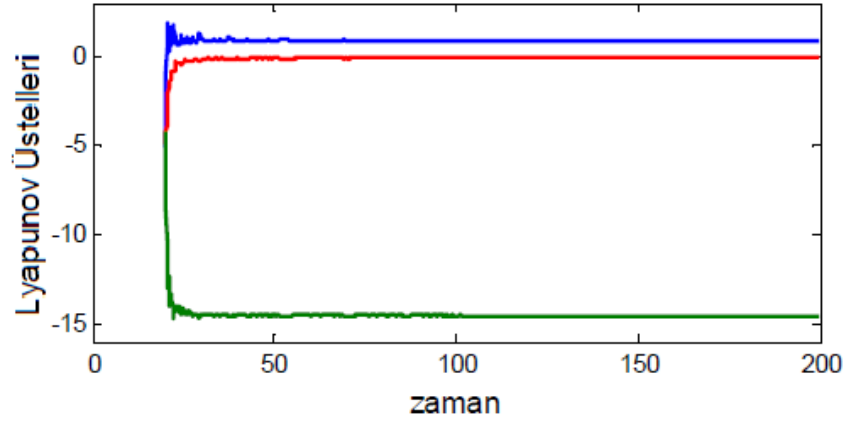


Şekil 3.6. Örnek osiloskop faz portre çıktısı

3.2.4. Lyapunov üstelleri spektrumu analizi

Deterministik sistemlerde kaos, başlangıç koşullarına aşırı duyarlılık gösteren bir yapıya sahiptir. Lyapunov üsteli, bir zaman serisinin kaotik bileşenler içerip içermediğini tespit etmeye yarayan bir analiz yöntemidir. Başka bir deyişle, kaotik sistemin başlangıç şartlarına bağımlı olup olmadığını gösteren bir analizdir. Lyapunov üsteli λ ile gösterilir [21,80]. Kaotik bir sistemden bahsetmek için, sistemin en az bir pozitif Lyapunov üsteline sahip olması gerekir. Herhangi bir sistemde; $\lambda_1 > 0$ ise davranış kaotik, $\lambda_1 < 0$ ise davranış düzenli olarak kabul edilir. Düzenli periyodik hareketler negatif Lyapunov üsteli ile ifade edilir. Çatallaşma noktaları sınırlı düzenli

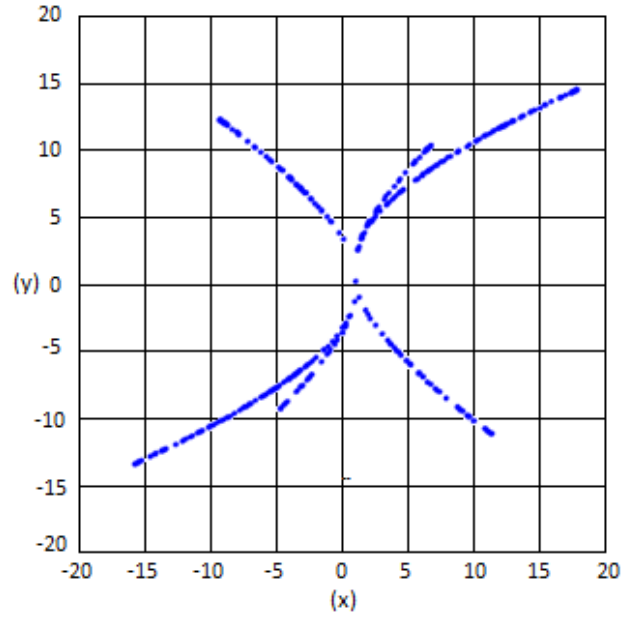
hareketler olarak ifade edilir ve üstel değeri sıfırdır [80]. Üç boyutlu bir kaotik sistemin Lyapunov üstellerine sırasıyla $\lambda_1, \lambda_2, \lambda_3$ dersek; $(-, -, -)$ ise sabit nokta, $(0, -, -)$ ise limit döngü, $(0, 0, -)$ ise torus, $(+, 0, -)$ ise kaotik hareket olarak adlandırılır [21,80]. Şekil 3.7.'de görüldüğü gibi Lyapunov üstelleri, sistemin kaotik olması için gereken durumu $(+, 0, -)$ sağlayacak şekilde $\lambda_1 = 0.9, \lambda_2 = 0, \lambda_3 = -14.5$ olarak bulunmuştur



Şekil 3.7. Örnek Lyapunov üstel grafiği [21]

3.2.5. Poincare haritalama analizi

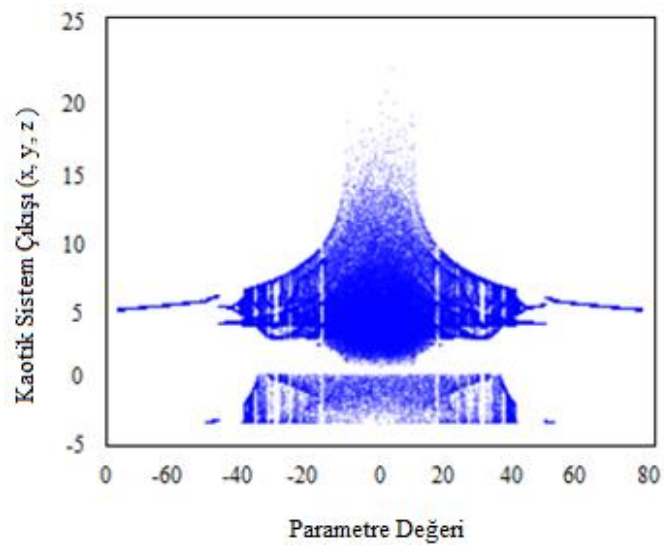
Birçok durumda ayrık zamanlı bir sistemi analiz etmek, sürekli zamanlı bir sistemi analiz etmekten daha kolaydır. Poincare isimli bilim adamı sürekli zamanlı bir sistemi ayrık zamanlı bir sisteme çevirmek için bir yöntem geliştirmiştir [80,81]. Bu sistem ile karmaşık sistemleri daha basit hale getirmek ve kararlılık analizi yapmak mümkündür. Periyodik bir davranış Poincare haritalama yöntemi ile incelenirse, haritada sabit bir nokta oluşur. Çünkü sistemin periyodu ile aynı zaman dilimlerinde örnekler alındığı için hep aynı nokta işaretleneceğinden dolayı tek bir nokta görülür. Sistemin periyodu ise kapalı bir çevrimdir. Fakat sistem kaotik davranış gösteriyor ise, kapalı olmayan, gelişigüzel kapalı bir şekil oluşur. Şekil 3.8.'de örnek Poincare haritalama grafiği verilmiş sistem sabit başlangıç gerilim değerlerinden x, y çıkış değerlerinin geliş güzel yayılım gösterdiği görülmektedir [80,81].



Şekil 3.8. Örnek Poincare haritalama [79]

3.2.6. Çatallaşma diyagramı analizi

Çatallaşma diyagramı, sistemde yapılan anlık parametre değişiklikleri ile sistemin kaotik davranıp davranmadığını tespit etmek için kullanılır. Bir sistemin, kaotik davranış göstermesi için parametrelerindeki küçük değişimler çatallaşmalar meydana getirmelidir. Çatallaşmalar meydana getirmiyorsa sistem periyodik davranış gösteriyordur [21]. Şekil 3.9.'da örnek çatallaşma grafiği gösterilmiştir.



Şekil 3.9. Örnek çatallaşma diyagramı [79]

3.3. Rucklidge Kaotik Sistemi Analizi

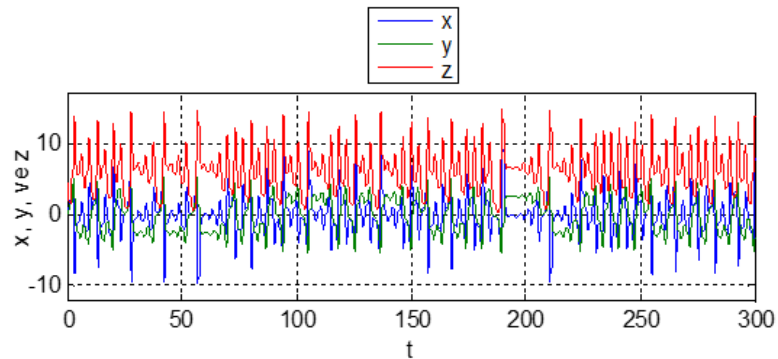
Rucklidge sistemi, sürekli zamanlı üç boyutlu kaotik bir sistemdir. Denklem (3.3)'te görüldüğü gibi 3 farklı diferansiyel denklemden oluşmaktadır.

$$\begin{aligned}\dot{x} &= -ax + by - yz \\ \dot{y} &= x \\ \dot{z} &= -z + y^2\end{aligned}\quad (3.3)$$

Sistemde a, b reel sabitlerdir ve a=2, b=6.7 alınmıştır. Sistemin başlangıç şartları x(0)= 1, y(0)=0, z(0)=4.5 alınmıştır [76,77]. Denklem (3.4)'te sistemin parametrelili hali gösterilmiştir.

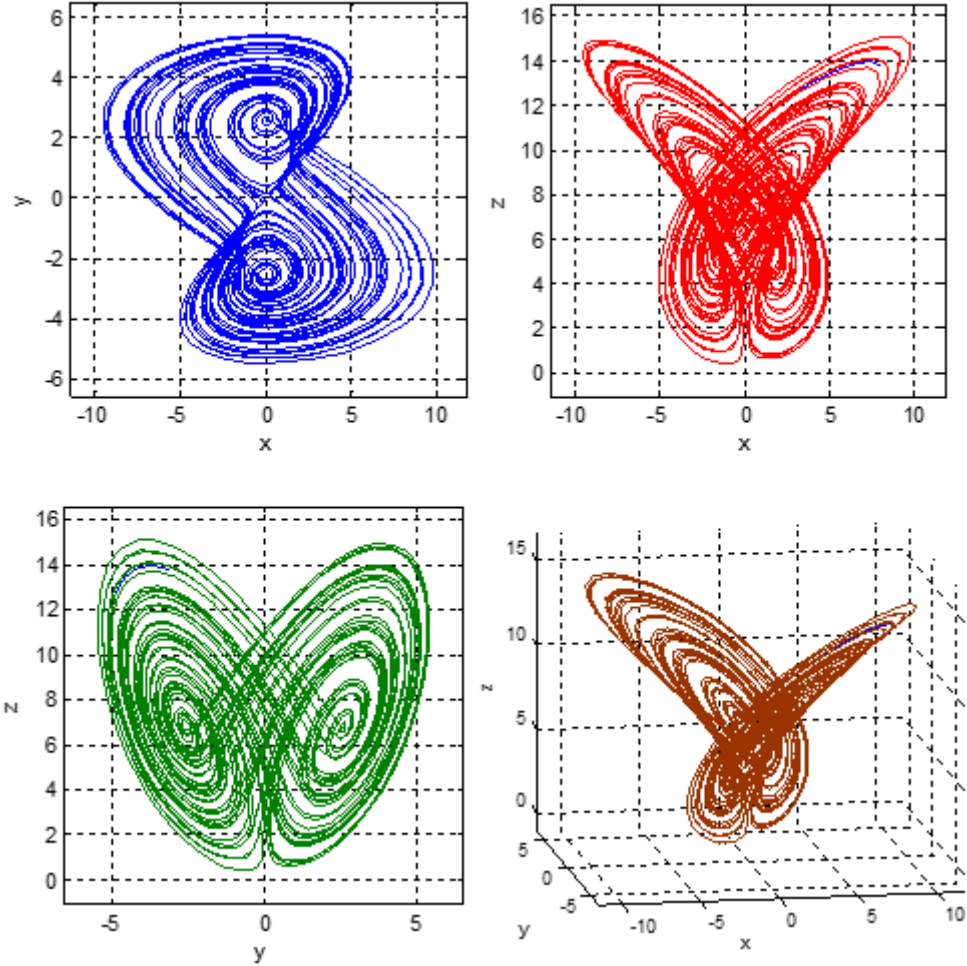
$$\begin{aligned}\dot{x} &= -2x + 6.7y - yz \\ \dot{y} &= x \\ \dot{z} &= -z + y^2\end{aligned}\quad (3.4)$$

Rucklidge sistemi denge nokta analizi hesaplamaları sonucunda bulunan öz değerler $\lambda_1= 0.193$, $\lambda_2=0$, $\lambda_3=-3.193$ 'tür [76,77]. Değerlerden birinin pozitif olması, sistemin kaotik özelliğe sahip olduğunu işaret eder. Sistem, Matlab Odesolve programı kullanılarak analiz edilmiştir. Şekil 3.10.'da Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Rucklidge sistemine ait zaman serileri görülmektedir.



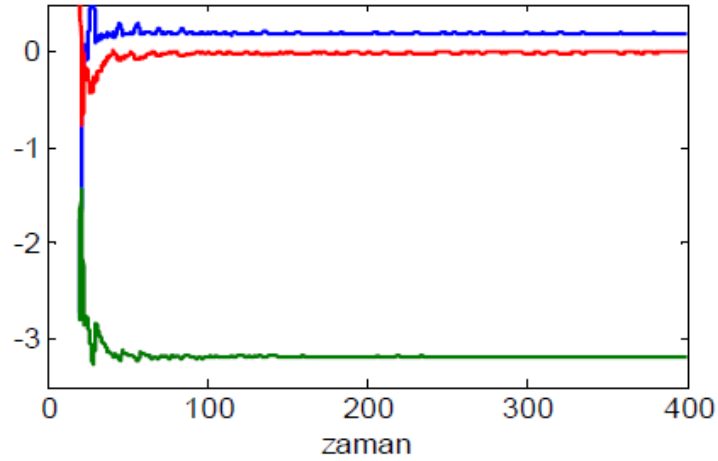
Şekil 3.10. Rucklidge sistemi Matlab programı X, Y, Z zaman serileri

Şekil 3.11.'de Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Rucklidge sistemine ait XY, XZ, YZ, XYZ faz porteleri görülmektedir.



Şekil 3.11. Rucklidge sistemi Matlab programı XY, XZ, YZ, XYZ faz portre çıktıları

Rucklidge sistemi a parametresine ait Lyapunov üstel grafiği Şekil 3.12.'de görülmektedir. Şekil 3.12'de görüldüğü gibi $\lambda_1=0.18$, $\lambda_2=0$, $\lambda_3=-3.2$ Lyapunov üstelleri olarak elde edilmiştir. Elde edilen değerlere göre kaotik davranışın oluşması için gereken (+, 0, -) durumunun sağlandığı için sistemin kaotik olduğu söylenebilir [21,76].



Şekil 3.12. Rucklidge sistemi a parametresine ait Lyapunov üstel grafiği [21]

3.4. Chen Kaotik Sistemi Analizi

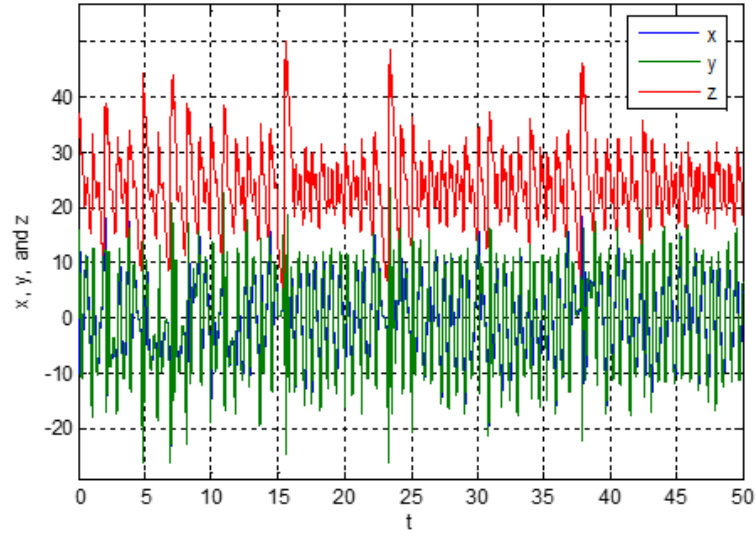
Chen sistemi, sürekli zamanlı üç boyutlu kaotik bir sistemdir. Denklem (3.5)'te görüldüğü gibi 3 farklı diferansiyel denklemden oluşmaktadır. Guanrong Chen ve Ueta tarafından 1999 yılında bulunmuştur.

$$\begin{aligned}
 \dot{x} &= a.(y - x) \\
 \dot{y} &= (c - a).x - x.z + c.y \\
 \dot{z} &= x.y - b.z
 \end{aligned} \tag{3.5}$$

Sistemde a, b, c reel sabitlerdir ve a=35, b=3, c=28 alınmıştır. Sistemin başlangıç şartları $x(0)=-10$, $y(0)=0$, $z(0)=37$ olarak seçilmiştir. Denklem (3.6)'da sistemin parametrelili hali gösterilmiştir [74].

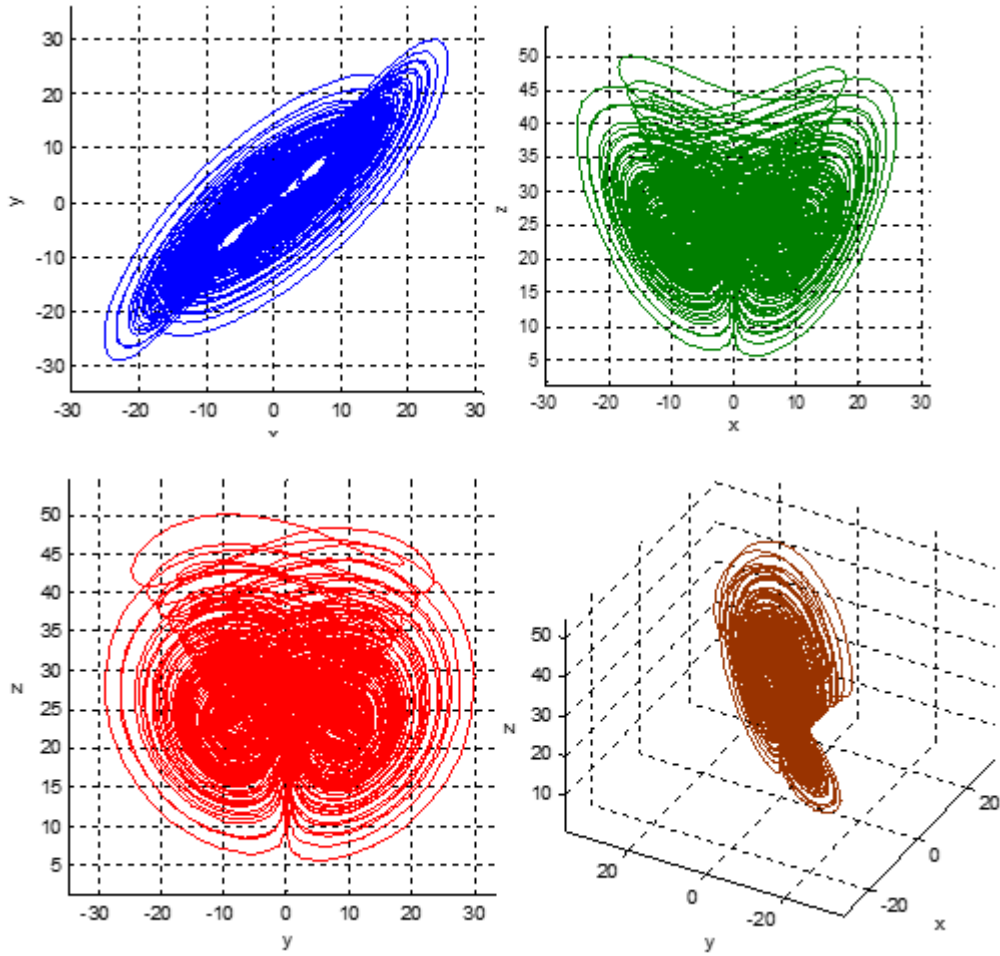
$$\begin{aligned}
 \dot{x} &= 35.(y - x) \\
 \dot{y} &= (-7).x - x.z + 28.y \\
 \dot{z} &= x.y - 3.z
 \end{aligned} \tag{3.6}$$

Chen sistemi denge nokta analizi hesaplamaları sonucunda bulunan öz değerler $\lambda_1=-7.94$, $\lambda_2=-7.94$, $\lambda_3=21$ 'dir.

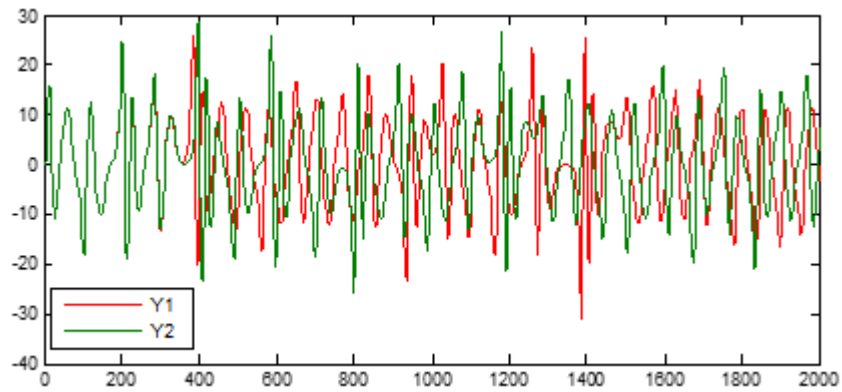


Şekil 3.13. Chen sistemi Matlab programı X, Y, Z zaman serileri

Şekil 3.13.'te Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Chen sistemine ait X, Y, Z zaman serileri görülmektedir. Şekil 3.14.'te ise Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Chen sistemine ait XY, XZ, YZ, XYZ faz portreleri görülmektedir.



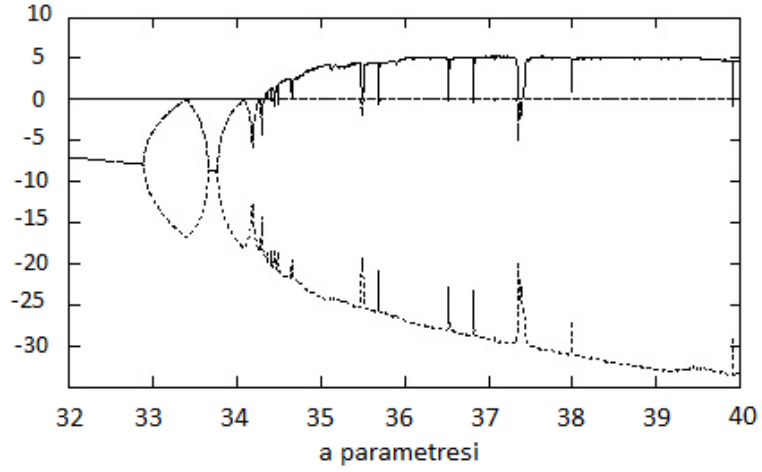
Şekil 3.14. Chen sistemi Matlab programını XY, YZ, XZ, XYZ faz portre çıktıları



Şekil 3.15. Chen sistemi Y çıkışının başlangıç değerine duyarlılığı

Şekil 3.15.'te Chen sistemin başlangıç değerinde yapılan çok küçük farklılığın, kaotik sistem Y çıkışını çok farklı yerlere götürdüğü görülmektedir. Y1 sinyali için başlangıç değeri 0V, Y2 sinyali için başlangıç değeri 0.0001V alınmıştır. Chen sistemin a parametresine ait Lyapunov üstel grafiği Şekil 3.16.'da görülmektedir. Grafik

incelendiğinde b reel sabiti 11, c reel sabiti 28 iken a reel sabiti 34 ve 40 değerleri arasında değiştirildiğinde, sistemin büyük çoğunlukla kaotik davranış gösterdiği görülmektedir [74].



Şekil 3.16. Chen sistemi a parametresine ait Lyapunov üstelleri spektrumu grafiği (b=11 ve c=28) [74]

3.5. Zhongtang Kaotik Sistemi Analizi

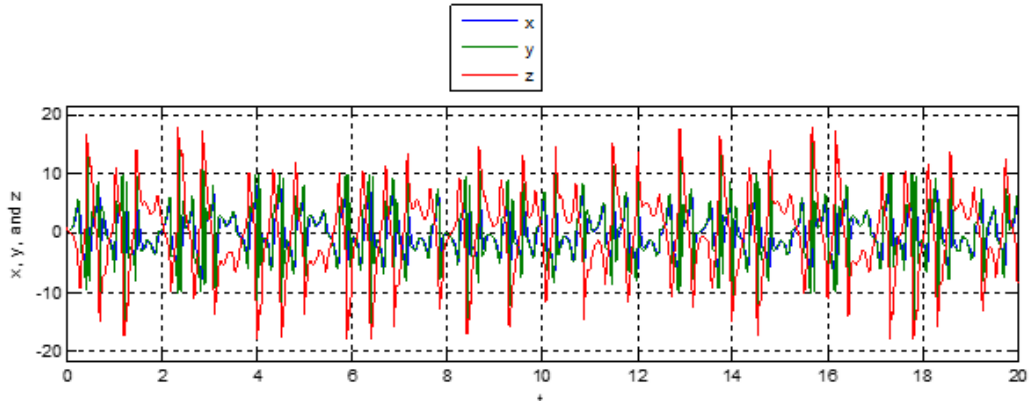
Zhongtang sistemi, sürekli zamanlı üç boyutlu kaotik bir sistemdir. Denklem (3.7)'de görüldüğü gibi 3 adet diferansiyel denklemden oluşmaktadır.

$$\begin{aligned}\dot{x} &= a(y - x) \\ \dot{y} &= b(x + y) - xz^2 \\ \dot{z} &= -ex - cz + x^2\end{aligned}\tag{3.7}$$

Sistemde a, b, c ve e reel sabitlerdir ve a=40, b=10, c=15, e=20 alınmıştır. Sistemin tipik başlangıç şartları $x(0)= 1$, $y(0)=0$, $z(0)=1$ 'dir. Denklem (3.8)'de sistemin parametrelili hali gösterilmiştir.

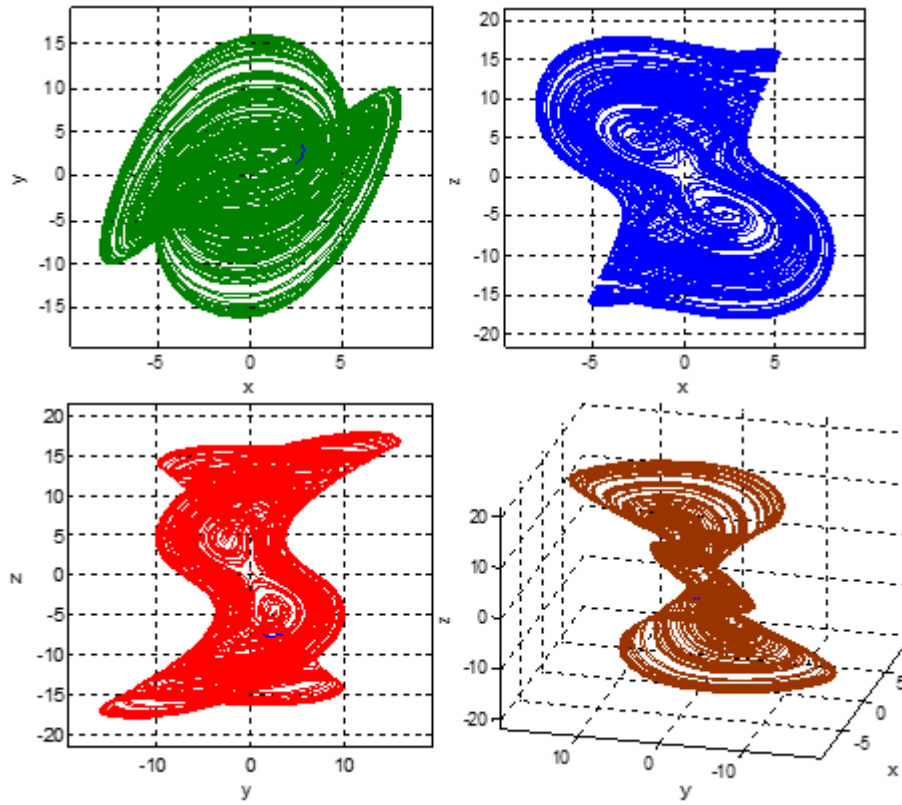
$$\begin{aligned}\dot{x} &= 40(y - x) \\ \dot{y} &= 10(x + y) - xz^2 \\ \dot{z} &= -20x - 15z + x^2z\end{aligned}\tag{3.8}$$

Zhongtang sistemi denge nokta analizi hesaplamaları sonucunda bulunan öz değerler $\lambda_1= 3.7183$, $\lambda_2=0,0266$, $\lambda_3=-38.4310$ 'dur. Değerlerden ikisinin pozitif olması, sistemin hiper kaotik özelliğe sahip olduğunu işaret eder [79]. Şekil 3.17.'de Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Zhongtang sistemine ait X, Y, Z zaman serileri görülmektedir.



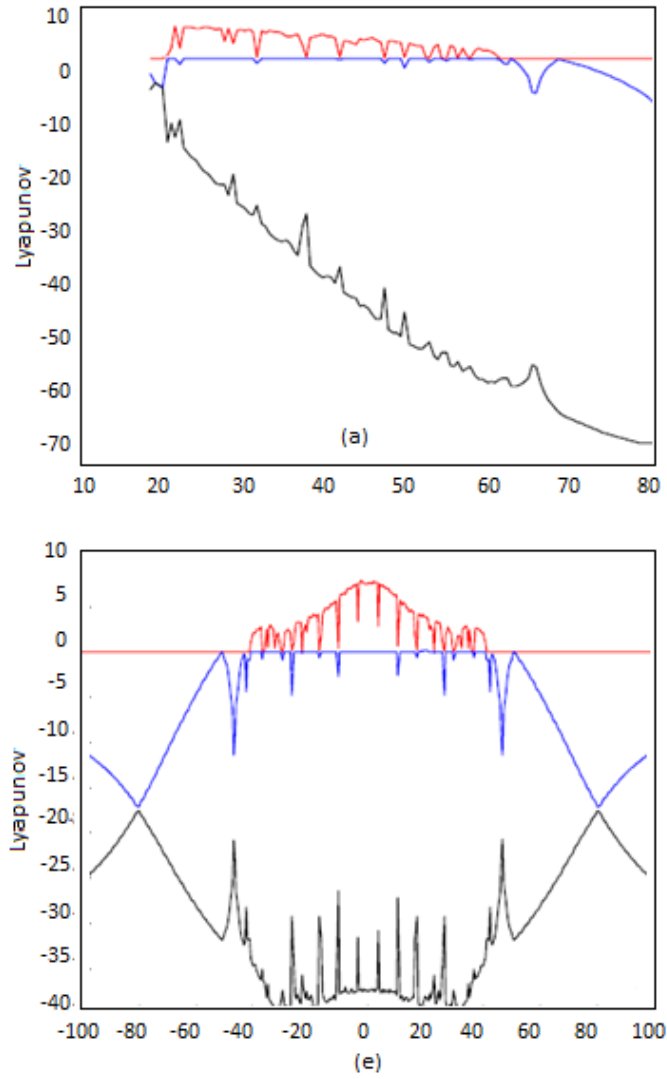
Şekil 3.17. Zhongtang sistemi Matlab programı X, Y, Z zaman serileri

Şekil 3.18.'de Matlab Odesolve programı ile yapılan analiz sonucunda elde edilen Zhongtang sistemine ait XY, XZ, YZ, XYZ faz porteleri görülmektedir.



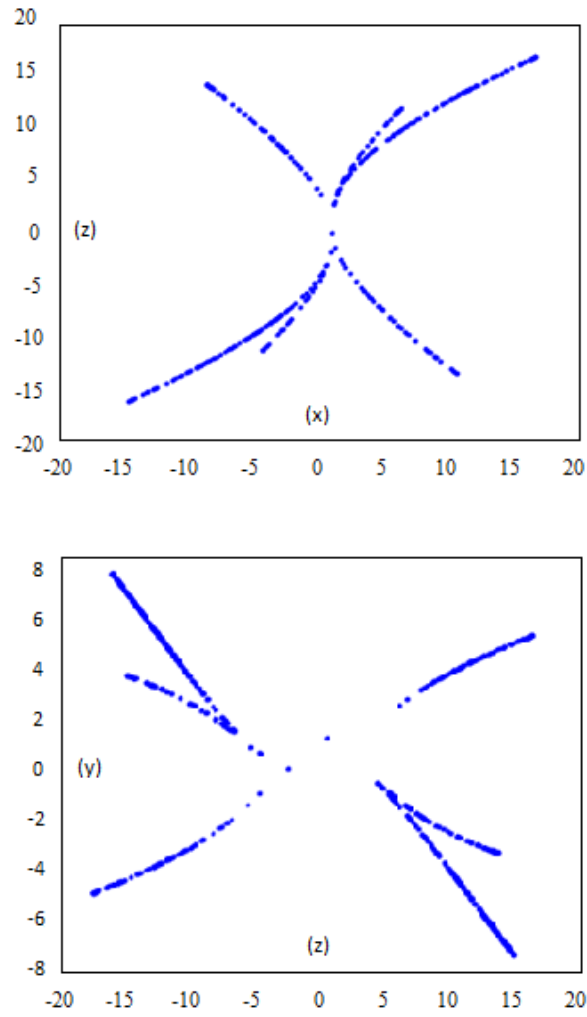
Şekil 3.18. Zhongtang sistemi Matlab programı XY, XZ, YZ, XYZ faz portre çıktıları

Zhongtang sistemine ait Lyapunov üstelleri spektrumu grafikleri Şekil 3.19.'da görülmektedir. Zhongtang kaotik sistemi, a parametresi; 20 ve 60 değerleri arasında, e parametresi ise; -40 ve 40 değerleri arasında olduğunda sistem çoğunlukla kaotik davranış göstermektedir [79].



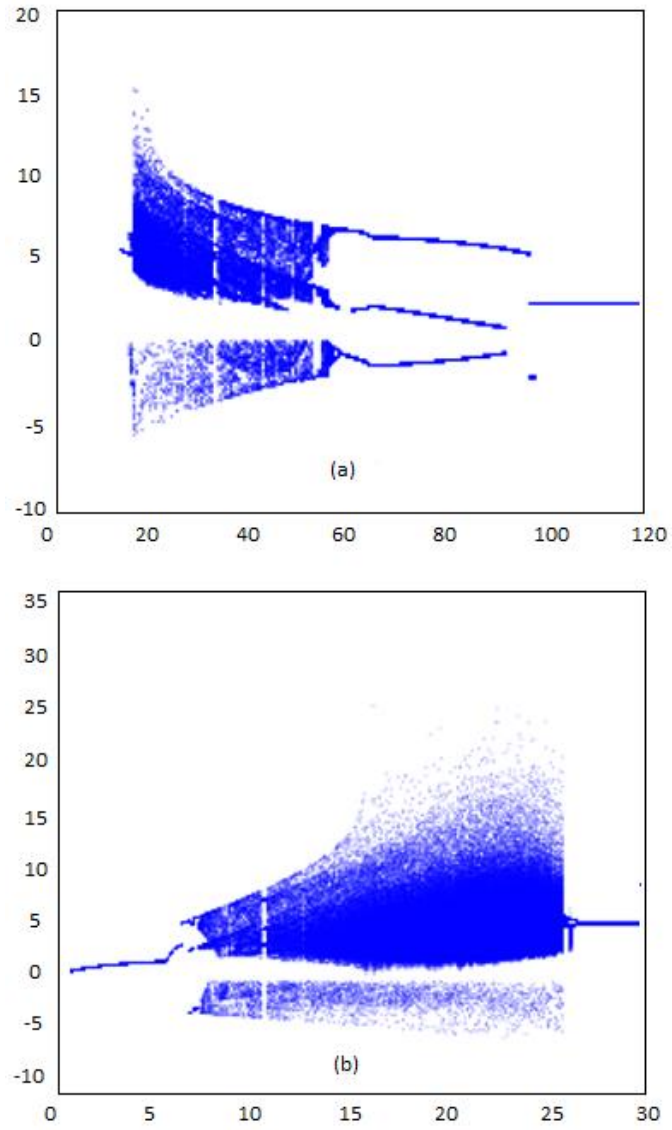
Şekil 3.19. Zhongtang sistemin a ve e parametrelerine ait Lyapunov üstelleri spektrumu grafikleri [79]

Zhongtang sistemine ait Poincare haritalama grafikleri $a=40$, $b=10$, $c=15$, $e=20$ parametreleri, $X_0=0$, $Y_0=0$ başlangıç gerilim değerleri için Şekil 3.20.'de gösterilmiştir. Grafiklerde görüldüğü gibi sabit noktaların oluşmadığı değerlerde sistem kaotik davranış göstermektedir.



Şekil 3.20. Zhongtang sistemine ait Poincare haritalama grafikleri (a) $x_0=0$ (b) $y_0=0$ [79]

Şekil 3.21.'de Zhongtang kaotik sistemi a ve b parametrelerine ait çatallaşma diyagramları görülmektedir. Grafikler incelendiğinde, çatallaşmanın meydana geldiği, a parametresi 20 ile 60, b parametresi 7 ile 25 değerleri arasında değiştirildiğinde, sistem kaotik davranış göstermektedir.



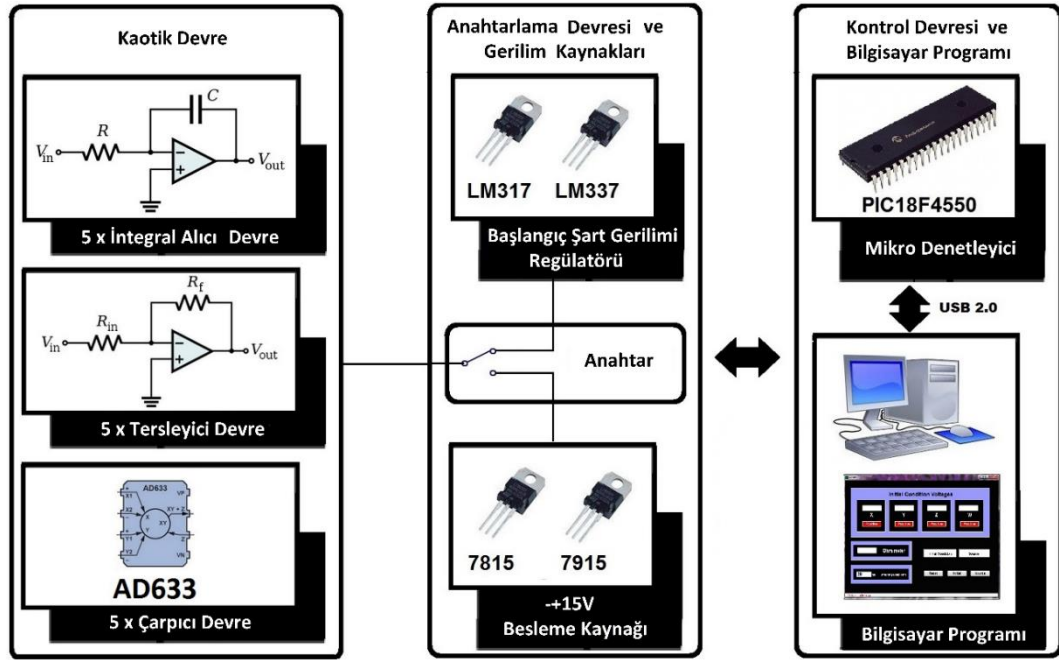
Şekil 3.21. Zhongtang sistemi a ve b parametrelerine ait çatalaşma diyagramları [79]

BÖLÜM 4. SZKS'LER İÇİN YENİ BİR KAOTİK DEVRE DENEY SETİ TASARIMI VE GERÇEKLEMESİ

Gerçek rasgele sayı üreticilerinin rasgeleliği öncelikle doğru seçilmiş bir entropi kaynağına bağlıdır [6,9,18]. Yapılan çalışmada entropi kaynağı olarak SZKS tercih edilmiştir. Günümüzde karmaşık ve farklı dinamik davranışlar gösteren yeni kaotik sistemlerin araştırılması üzerine çalışmalar çok fazladır. Her SZKS, rasgele sayı üretici için kaynak olarak kullanılmaya uygun olmayabilir. Bu sebeple yapılan çalışmada, rasgele sayı üreticisine uygun entropi kaynağı bulmak için çok sayıda SZKS devresi kurma ihtiyacı doğmuştur. Fakat, SZKS devresi kurmak ve çalıştırmak karmaşık yapısı gereği zor ve zaman almaktadır. Ayrıca, kaotik denklemlerin modellenmesine fizik, matematik, elektrik, elektronik, bilgisayar gibi alanlarda çalışan araştırmacı, mühendis ve bilim adamları da ihtiyaç duymaktadır. Bu kişiler çoğunlukla kaotik devre gerçeklemede yeterli elektronik altyapıya sahip olmadıklarından ve kaotik devrelerin yapısı karmaşık olduğundan büyük problemler yaşamaktadırlar. SZKS devresi kurarken karşılaşılan zorluklar;

- SZKS devrelerinin karmaşık yapıya sahip olmasından dolayı breadboard üzerinde kurulmasının zor olması ve PCB gereksinimi duyulması.
- SZKS devrelerinin simetrik devre besleme gerilimi ve başlangıç şart gerilimleri ihtiyacından dolayı çok sayıda farklı simetrik güç kaynağı gerekli olması.
- SZKS devrelerinde standart dışı değerlerde dirençlere ihtiyaç olması.
- SZKS devrelerini çalıştırabilmek için, sistemin yapısı ve yapılan uygulama gereği, başlangıç şartı gerilimlerini uygulayan başlangıç şartı sürücü devresine ihtiyaç duyulmasıdır.

SZKS'lerin devre gerçeklemelerinin hızlı ve kolay yapılabilmesi için yeni bir bilgisayar ve mikro denetleyici kontrollü kaotik devre deney seti (KDDS) tasarlanmış ve gerçekleştirilmiştir. Geliştirilen KDDS, başlangıç şart gerilim sürücüsü ve gerilim kaynakları, kontrol devresi ve bilgisayar programı olmak üzere 3 temel bloktan oluşmaktadır. Şekil 4.1.'de tasarlanan KDDS'nin blok diyagramı gösterilmiştir.



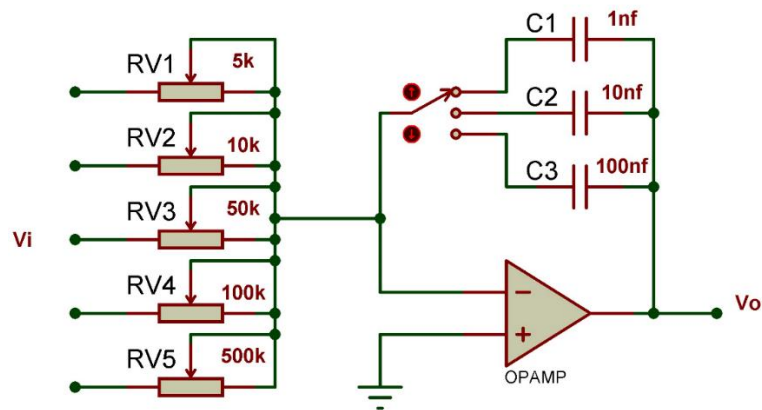
Şekil 4.1. KDDS blok diyagramı

4.1. KDDS Kaotik Devre Bloğu Tasarımı

SZKS devreleri, integral alıcı, tersleyici ve çarpma devrelerinden oluşmaktadır. Kaotik denklemlerin modellenmesi sonucu tasarlanan elektronik devrelerde bulunan standart dışı direnç değerlerini elde etmek için deney setinde çok turlu potansiyometreler kullanılmıştır. Kaotik devre bloğunda, integral alıcı, tersleyici ve çarpma devrelerinden 5'er adet bulunmaktadır. Kaotik devre gerçeklemelerinde kullanılmak istenen bloklara, jumper yardımıyla besleme gerilimleri verilmelidir. Devre gerçekleştirilmesi yapılırken, istenen direnç değerleri için potansiyometre ayarı yapılır ve bloklar arası bağlantılar için jumper kabloları kullanılır.

4.1.1. İntegral alıcı devre tasarımı

İntegral alıcı devre, girişe uygulanan sinyalin integralini alarak çıkışa aktaran devredir. Matematiksel olarak integral, bir eğrinin altında kalan alanı hesaplar. Eğri altında kalan alan, işaret genliği ile zamanın çarpımına eşittir yani işaret giriş eğrisi altında kalan alan zamanla doğru orantılıdır [82]. Deney setinde bulunan integral alıcı bloğu Şekil 4.2.'de görülmektedir.



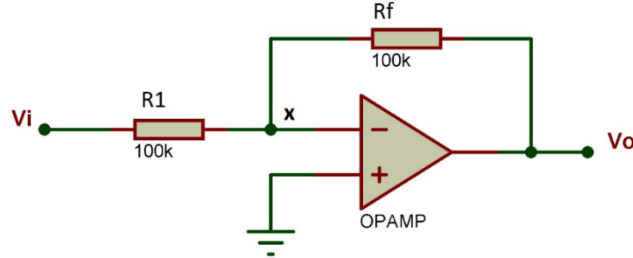
Şekil 4.2. KDDS'de kullanılan modüler integral alıcı devresi

İntegral alıcı, birer adet TL081 opamp, 1nf, 10nf, 100nf kondansatör, 5k, 10k, 50k, 100k, 500k çok turlu potansiyometreden oluşmaktadır. İntegral alıcı bloğunda bulunan 1nf, 10nf ve 100nf kondansatörlerden, istenilen kondansatör jumper ile seçilebilir. Deney setinde integral alıcıdan 5 adet bulunmaktadır. Kullanılmak istenen integral alıcıya jumper ile besleme gerilimi verilmelidir. Çok turlu potansiyometreyi istenilen değere ayarlamak için ölçü aletine gerek yoktur. Deney setinde bulunan probalar potansiyometre uçlarına takılır ayarlanan değer anlık olarak bilgisayar programının ara yüzünden izlenebilir.

4.1.2. Tersleyici devre tasarımı

SZKS devrelerinde kullanılan devrelerden ikincisi tersleyici devreleridir. Şekil 4.3.'te devre şeması verilen tersleyici devrede R1 direnci giriş, Rf direnci ise geri besleme direncidir. Devre tersleyen yükselteç devresidir ve çıkış kazancı $K_v = -(R_f / R_1)$

formülü ile hesaplanır. Formüldeki (-) işareti giriş ile çıkış arasında 180° faz farkı olduğunu gösterir. Tasarlanan devrede, $R1=R_f$ olduğundan çıkış kazancı -1 dir. Yani girişe uygulanan gerilim sadece terslenmiştir [83].

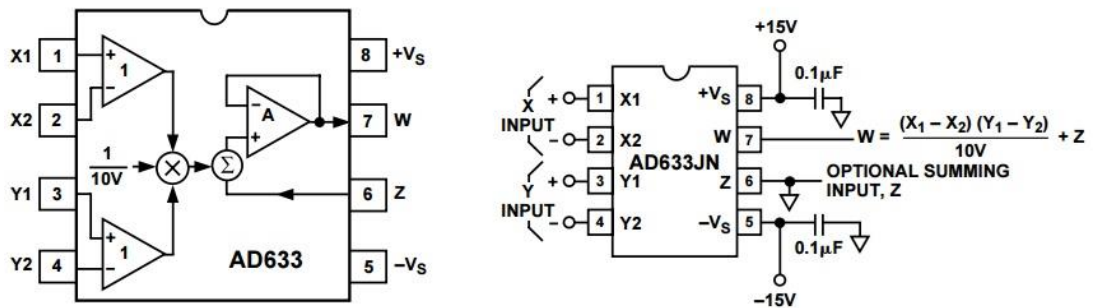


Şekil 4.3. KDDS’de kullanılan tersleyici devresi

Tersleyici devresi, TL081 opamp ve 2 adet 100k dirençten oluşmaktadır. Deney setinde 5 adet tersleyici devre bulunmaktadır. Kullanılmak istenen tersleyici devreye jumper ile besleme gerilimleri verilmelidir.

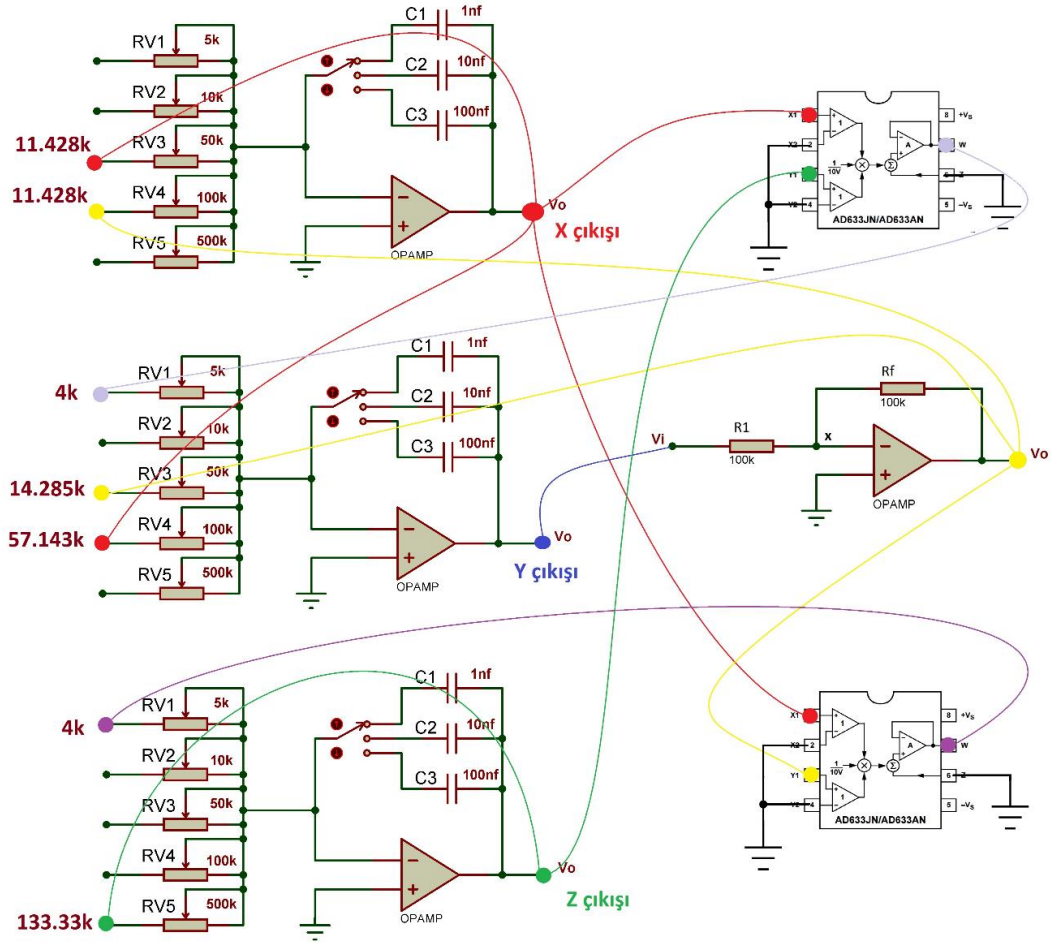
4.1.3. Çarpma devresi tasarımı

SZKS devrelerinde kullanılan devrelerden üçüncüsü AD633 kullanılarak tasarlanmış çarpma devresidir. Şekil 4.4.’te fonksiyon diyagramından da görüldüğü gibi AD633 x giriş farkı ($x1-x2$) ile y giriş farkını ($y1-y2$) çarpımının $1/10$ unu z ile toplayarak w çıkışına aktarır. Yani çıkış formül $w = [(x1-x2)*(y1-y2) / 10] + z$ ’dir. Deney setinde 5 adet çarpma devresi bulunmaktadır. Kullanılmak istenen çarpma devresine jumper ile besleme gerilimi verilmelidir.



Şekil 4.4. KDDS’de kullanılan AD633 fonksiyon diyagramı ve devresi

KDDS kaotik devre bloğu ile gerçekleştirilmiş örnek kaotik osilatör devresi Şekil 4.5.'te gösterilmiştir. İntegral alıcı devrelerde modelleme sonucu hesaplanan direnç değerlerine uygun potansiyometreler seçilerek hassas ayarlamalar yapılır. Bloklar arası bağlantılar jumper kabloları ile yapılır. Düğüm noktaları için aynı renk kablo kullanımı devre takibini kolaylaştırmaktadır.



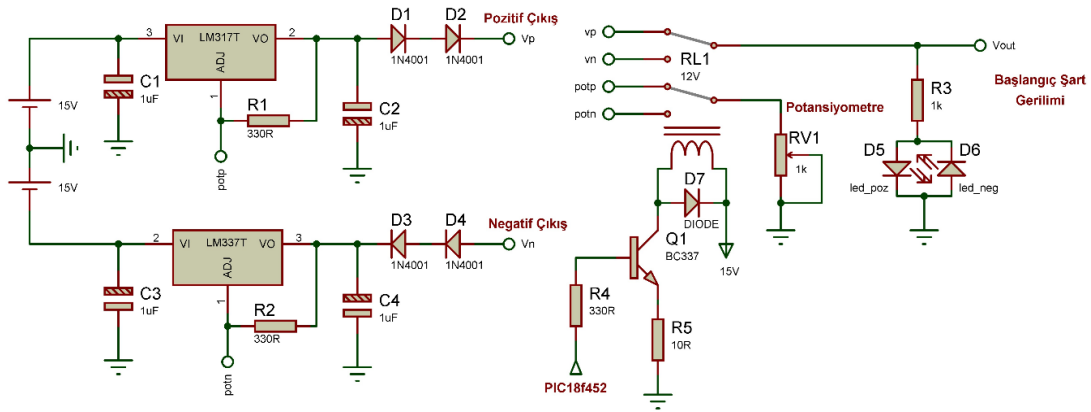
Şekil 4.5. Örnek kaotik sistemin KDDS ile gerçekleştirilmesi

4.2. KDDS Başlangıç Şartı Gerilim Sürücüsü ve Gerilim Regülatörü Tasarımı

Bu blok, SZKS devrelerini sürmek için kullanılan anahtarlama devresi, devre besleme ve başlangıç şart gerilimlerini elde etmek için kullanılan gerilim regülatörlerinden oluşmaktadır.

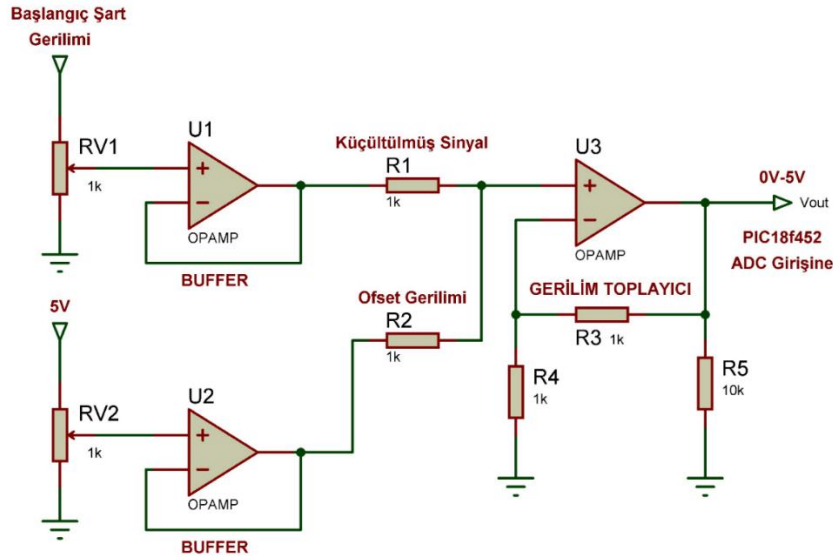
4.2.1. Başlangıç şartı gerilim regüle devresi tasarımı

Şekil 4.6.'da devre şeması görülen devre, kaotik sistemin başlangıç şartlarını -10V ile +10V arasında ayarlayan devredir. Pozitif gerilimler LM317, negatif gerilimler ise LM337 entegreleri kullanılarak regüle edilmiştir. Pozitif ve negatif gerilimi tek bir çıkışta birleştirmek ve bu gerilimleri tek bir potansiyometre ile ayarlayabilmek için çift kontak röle kullanılmıştır. Röle kontaklarından biri çıkış geriliminin polaritesini ayarlamakta diğeri ise kullanılacak regülatörü belirlemektedir.



Şekil 4.6. Başlangıç şart gerilim regülatörü devre şeması

Başlangıç şart gerilimleri PIC18f452 ADC girişi ile ölçülüp USB üzerinde bilgisayar programına aktarılmakta ve gerilim değerleri program arayüzünden anlık izlenebilmektedir. PIC18f452 ADC çalışma aralığı 0-5V'tur. Bu nedenle (-10V)-(+10V) aralığında olan başlangıç şart gerilimlerini, 0-5V aralığına dönüştürmek için Şekil 4.7.'de şeması görülen devre kullanılmıştır. Devre başlangıç şart gerilimini ilk olarak küçültür daha sonra ofset gerilimi ile toplayarak çıkışa aktarır. Devrede kullanılan gerilim izleyiciler (buffer) potansiyometre ile toplayıcı devre arasında empedans uygunlaştırma işini yapar.



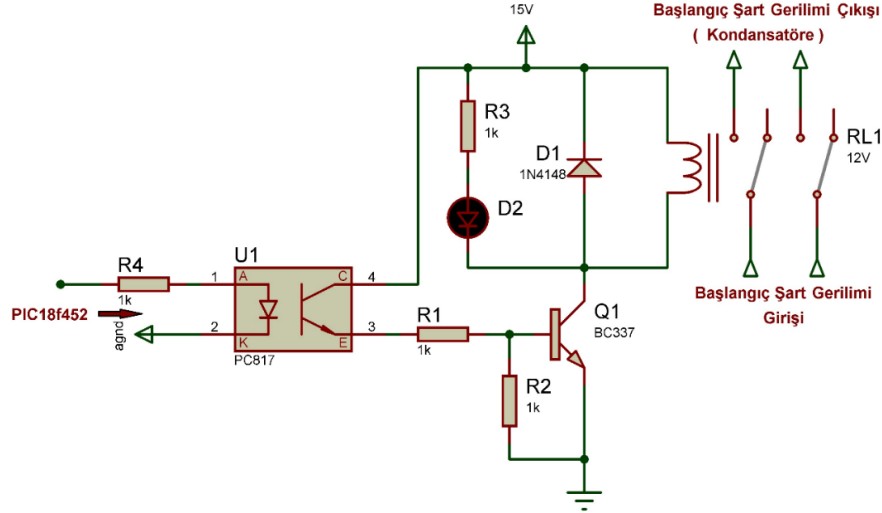
Şekil 4.7. Başlangıç şart gerilimini 0V-5V uygunlaştıran devre şeması

Çıkış geriliminin pozitif veya negatif olması bilgisayar programının ara yüzünden kontrol edilmektedir. Deney setinde X, Y, Z, W çıkışlarının her biri için bir adet olmak üzere toplamda bu devreden 4 adet bulunmaktadır.

4.2.2. Başlangıç şart gerilim sürücüsü tasarımı

Kaotik sitemlerin çalışması için, ilk olarak devreye başlangıç şartları verilmeli daha sonra başlangıç şartları kesilip beslemeler devreye verilmelidir. Şekil 4.8.'de şeması verilen devre başlangıç şart gerilimini anahtarlarmaktadır. Anahtarlama elemanı olarak çift kontaklı röle kullanılmıştır. Yarı iletken anahtarlama elemanı yerine röle kullanılmasının nedeni, analog anahtarlama direncinin 0 değerine çok yakın olmasıdır. X, Y, Z, W başlangıç şartı gerilimleri için anahtarlama devresinden birer adet olmak üzere toplam 4 adet vardır. Bilgisayar arayüzündeki "initial" butonuna basıldığında 4 adet başlangıç şartı kaotik devreye verilir. Bu sırada devrenin besleme gerilimleri yoktur. Devreye başlangıç gerilimleri verildikten sonra, bilgisayar arayüz programındaki "source" butonuna basıldığında, bilgisayar arayüzünde girilen bekleme süresi kadar bekledikten sonra başlangıç şartı gerilimi ile besleme gerilimi aynı anda devreye verilir. Bekleme süresi sonunda başlangıç şartı kesilir. Zaman hesapları

yapılırken rölelerin çekme ve bırakma zamanları hesaba katılmıştır. Rölelerin çekme zamanı 15ms bırakma zamanı 7ms'dir.



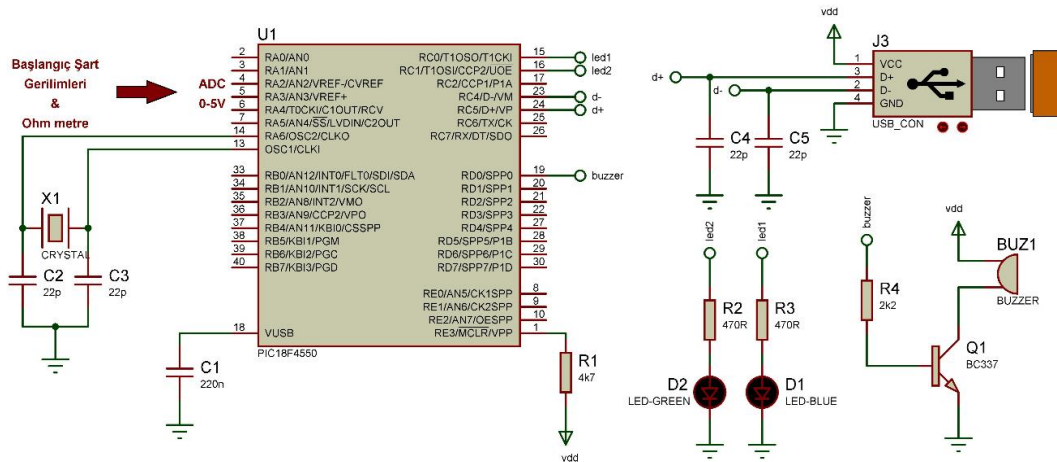
Şekil 4.8. Başlangıç şart gerilim sürücüsü devre şeması

4.3. KDDS Kontrol Devresi ve Bilgisayar Programı Tasarımı

KDDS'ye ait bu blok, mikro denetleyici tabanlı kontrol devresi ve bilgisayar programından oluşmaktadır.

4.3.1. Mikro denetleyici tabanlı kontrol devresi tasarımı

KDDS kontrol devresinde, mikro denetleyici olarak PIC18F4550 kullanılmıştır. PIC18F4550 tercih edilmesinin nedeni dahili 10 bit ADC ve dahili USB 2.0 özelliği bulundurmasıdır. Şekil 4.9.'da mikro denetleyici tabanlı kontrol devresi şeması görülmektedir. Kontrol devresi enerjisini bilgisayarın USB portundan almaktadır. Devre üzerinde yeşil ve sarı renkli iki led ve bir adet buzzer bulunmaktadır. Yeşil renkli led yanıp sönüyor ise bilgisayar programı ile bağlantı olduğunu, yanık kalıyorsa bağlantının koptuğunu göstermektedir. Kullanıcının bilgisayar programının arayüzü yardımı ile gönderdiği her komut için sarı renkli led yanar ve buzzer 50ms çalışır. Kontrol devresi, ADC kullanarak başlangıç şartı gerilimlerini ölçer ve USB ile bilgisayar programına gönderir. Bilgisayar programından USB ile gelen komutlara göre, başlangıç şart ve besleme rölelerini kontrol eder.



Şekil 4.9. Mikro denetleyici tabanlı kontrol devresi

PIC yazılımı, C programlama dilinde yazılmıştır. Derleyici olarak CCS PIC C COMPILER kullanılmıştır. CCS PIC C COMPILER’da yazılmış programdan bir kesit Şekil 4.10.’da görülmektedir.

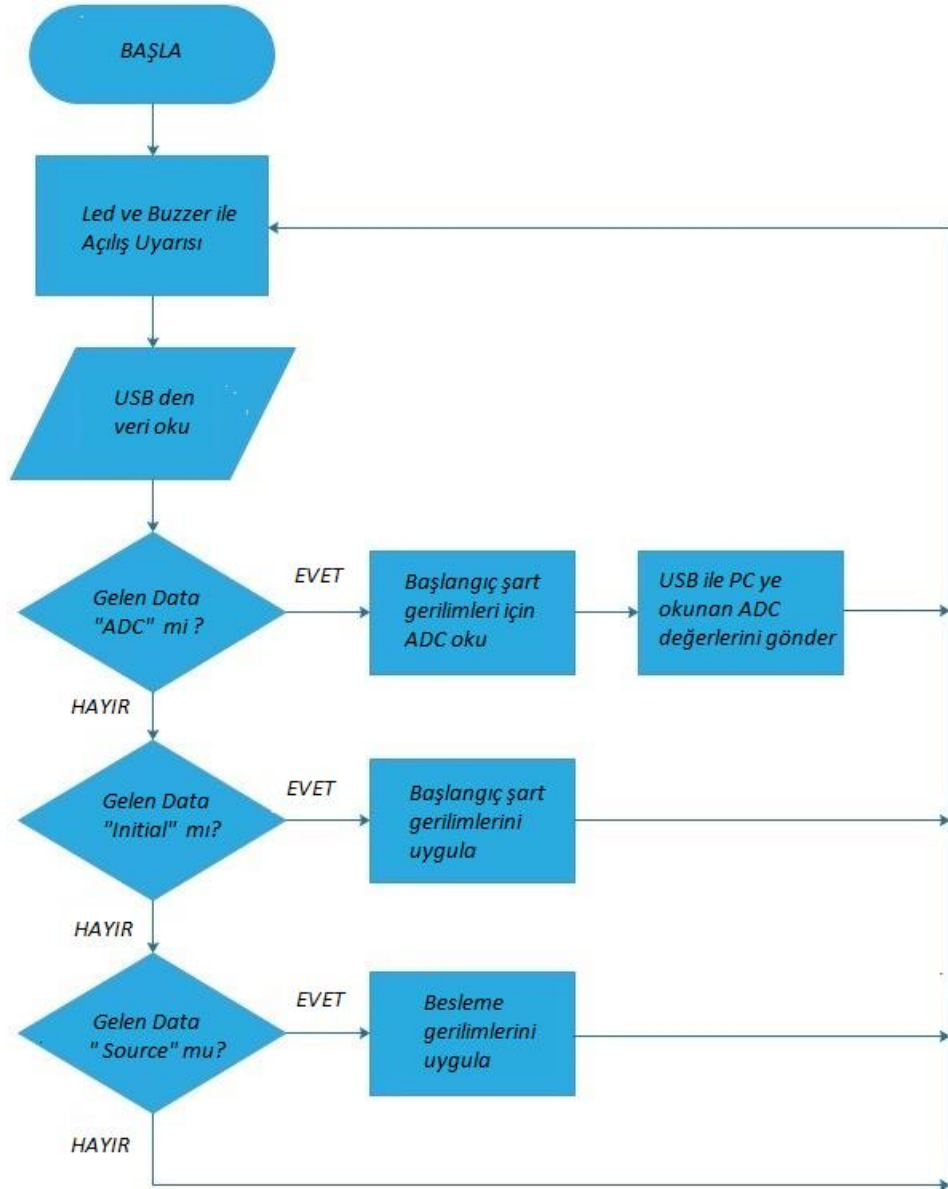
```

PCWHD
Project Edit Search Options Compile View Tools Debug Document User Toolbar
Project PIC Wizard 24 Bit Wizard Create Open All Files Close Project Find Text in Project
Project Options
usb_deny_karti.c
1 ////////////////////////////////////////////////////
2 //Programlayan Selçuk COŞKUN
3 //23.05.2014
4 //coskunselcuk@yahoo.com
5 ////////////////////////////////////////////////////
6 #include <18F4550.h>
7 #device ADC=10
8 //#fuses HSPLL, NOWDT, NOPROTECT, NOLVP, NODEBUG, USBDIV, PLL2, CPUDIV1, VREGEN, NOBROWNOUT // 8MHZ
9 #fuses HSPLL, USBDIV, PLL5, CPUDIV1, VREGEN, NOWDT, NOPROTECT, NOLVP, NODEBUG, NOBROWNOUT // 20 MHZ
10 #use delay (clock=20000000)
11
12 #define USB_HID_DEVICE TRUE
13 #define USB_EP1_TX_ENABLE USB_ENABLE_INTERRUPT //Uçnoktal'de Kesme transferi aktif
14 #define USB_EP1_RX_ENABLE USB_ENABLE_INTERRUPT
15 #define USB_EP1_TX_SIZE 64 //Uçnoktal için maksimum alınacak ve gonderilecek
16 #define USB_EP1_RX_SIZE 64 //veri boyutu (64 byte)
17
18 #include <lcd.c>
19 #include <pic18_usb.h>
20 #include "USB_Konfigurasyon.h" //USB konfigürasyon bilgileri bu dosyadadır.
21 #include <usb.c>
22

```

Şekil 4.10. PIC18F4550 CCS PIC C Compiler yazılımından bir kesit

Mikro denetleyici yazılımının akış diyagramı Şekil 4.11.'de gösterilmiştir. Devreye enerji verildiğinde devre üzerindeki LED'ler ve buzzer açılış uyarısı yapar. Bilgisayar programı ile devre bağlantısı yokken yeşil renkli LED yanar, bağlantı kurulduğunda yeşil renkli LED yanıp söner. Bağlantı kurulduğunda, bilgisayar programı her 50 ms de bir senkronizasyon veri paketi gönderir. Bu veri paketi 3 farklı komut içerir. Gelen veri "ADC" ise başlangıç şart gerilimi, ADC ile okunup bilgisayar programına gönderilir. Gelen veri "Initial" ise devre üzerindeki başlangıç şart gerilimlerini integral alıcı üzerindeki kondansatörlere uygulayan anahtarlama röleleri çekilir. Gelen veri, "Source" ise devreden gönderilen süre kadar beklendikten sonra besleme gerilimi ve başlangıç şart gerilimi aynı anda devreye uygulanır. Daha sonra başlangıç şartlarını anahtarlayan rölelerin enerjisi kesilir.

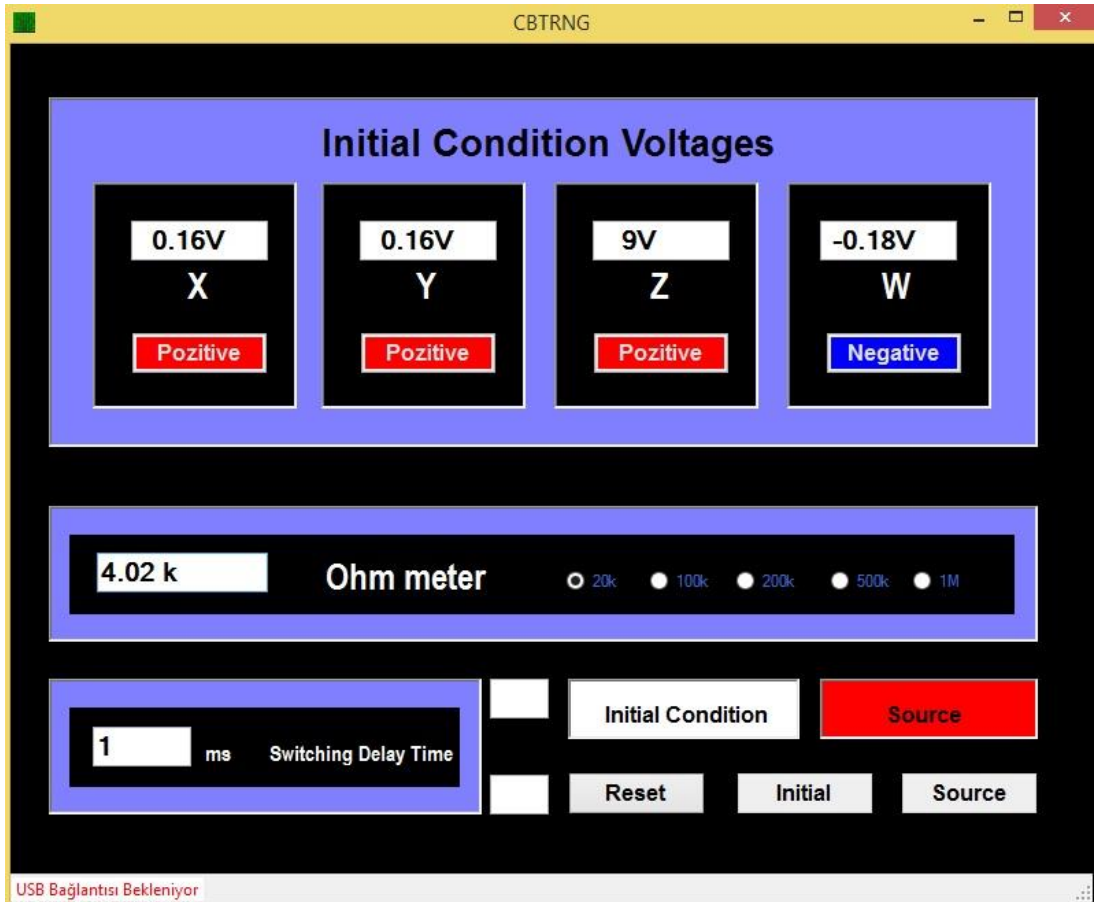


Şekil 4.11. PIC18F4550 yazılımı akış diyagramı

4.3.2. Bilgisayar programı tasarımı

Bilgisayar programı Microsoft Visual Studio C Sharp ile oluşturulmuştur. Bilgisayar programı, mikro denetleyici ile USB portu üzerinden haberleşmektedir. Mikro denetleyicinin ADC ile ölçtüğü değerler USB portu üzerinden bilgisayar programına aktarılır. Ekrandaki değerler 50ms de bir yenilenir. Başlangıç şart gerilimlerinin pozitif veya negatif olacağı programın arayüzündeki butonlar ile seçilir. Değerler ayarlandıktan sonra "Initial" butonuna basılarak kaotik devreye başlangıç şartları

uygulanır. Daha sonra “source” butonuna basılarak, sistemden başlangıç şart gerilimleri çekilir ve besleme gerilimi sisteme verilir. “Source” butonuna basıldığında arayüzden girilen anahtarlama gecikme süresi kadar kaotik sistemde başlangıç şartı ile besleme gerilimi aynı anda kaotik devreye uygulanır. Zaman sonunda başlangıç şart gerilimleri sistemden çekilir. “Reset” butonuna basıldığında sistemden başlangıç şart ve besleme gerilimleri çekilir. Başlangıç şartlarının pozitif veya negatif olması arayüz üzerindeki butonlar ile kontrol edilir. Potansiyometre ayarları yapılırken hassas ölçüm yapabilmek için bilgisayar programının arayüzdeki ohm metre bölümünden maksimum ölçülecek değer seçilmelidir. Yazılan programın arayüzü Şekil 4.12.’de görülmektedir.

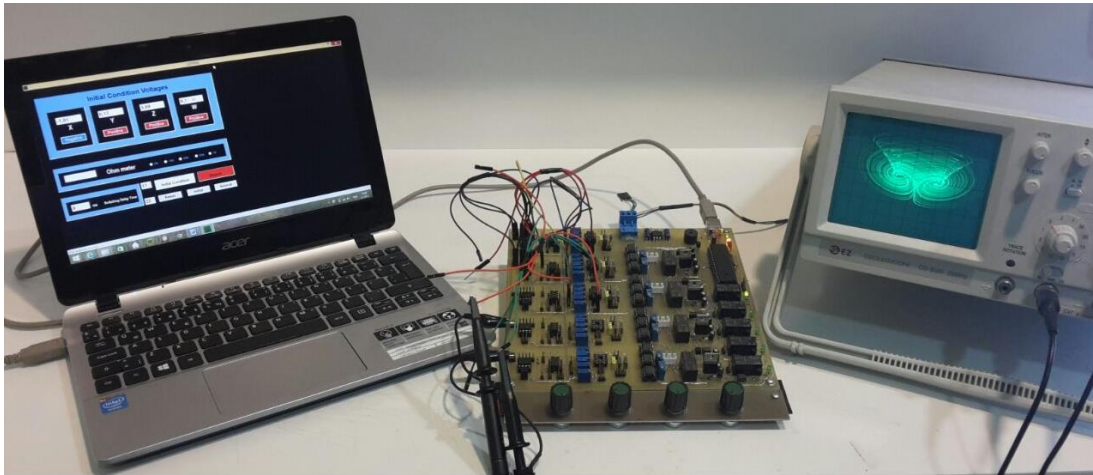


Şekil 4.12. KDDS bilgisayar programı arayüzü

Tasarlanan ve gerçekleştirilen KDDS Şekil 4.13.’te gösterilmiştir. Şekil 4.14.’te KDDS kullanarak gerçekleştirilmiş örnek kaotik devre uygulaması görülmektedir.



Şekil 4.13. Bilgisayar ve mikro denetleyici kontrollü KDDS gerçek devresi



Şekil 4.14. KDDS ile örnek kaotik devre gerçekleştirilmesi

BÖLÜM 5. ENTROPİ KAYNAĞI REFERANS KAOTİK SİSTEMLERİN MODELLENMESİ VE DEVRE GERÇEKLEMELERİ

SZKS'lerin diferansiyel denklemlerini modelleyip elektronik devrelerini oluşturmak için toplama, tersleme, çarpma ve integral alıcı devreler kullanılır [21]. Bu bölümde referans kaotik sistemler modellenerek gerçek devreleri tasarlanmıştır. Tasarlanan kaotik devreler, ilk olarak OrCAD-PSpice programında analiz edilmiş, daha sonra KDDS ile gerçek devreleri kurulmuştur. OrCAD-PSpice programı kullanarak elde edilen faz portreleri ile gerçek devrelerden osiloskop kullanılarak elde edilen faz portreleri karşılaştırılmıştır.

5.1. Rucklidge Kaotik Sisteminin Modellenmesi ve Devre Gerçeklemesi

GRSÜ tasarımı için kaynak olarak kullanılan kaotik sistemlerden ilki Rucklidge kaotik sistemidir. Rucklidge kaotik sistemine ait diferansiyel denklem takımı, Denklem (5.1)'de verildiği gibidir.

$$\begin{aligned}\dot{x} &= -ax + by - yz \\ \dot{y} &= x \\ \dot{z} &= -z + y^2\end{aligned}\tag{5.1}$$

Rucklidge kaotik sisteminin tasarımında parametreler $a = 2$, $b = 6.7$ ve başlangıç değerleri $X_0 = 1V$, $Y_0 = 0V$, $Z_0 = 4.5V$ olarak seçilmiştir [76, 77]. Bu değerler referans alınarak, Rucklidge kaotik sistemi elektronik elemanlar ile modellenmiştir. Rucklidge kaotik devresi elektronik elemanlar ile modellediğinde Denklem (5.2) elde edilir.

$$\begin{aligned}
\dot{x} &= -\frac{1}{R_4 C_1} \cdot x + \frac{1}{R_3 C_1} \cdot y - \frac{1}{R_5 C_1} \cdot yz \\
\dot{y} &= \frac{1}{R_6 C_2} \cdot x \\
\dot{z} &= -\frac{1}{R_7 C_3} \cdot z + \frac{1}{R_8 C_3} \cdot y^2
\end{aligned} \tag{5.2}$$

Elde edilen \dot{x} , \dot{y} , \dot{z} ifadelerinde, kapasitörlerin değerleri devrenin zamanlama skala değerine bağlıdır. Cuomo ve Oppenheim'in yaptıkları çalışmaya [87] göre zamanlama skalası 2505'dir. Bu çalışmada, zamanlama skala değeri $\beta = 2505$ alınmıştır. Denklem (5.2)'de verilen katsayılar eşitlenerek direnç değerleri hesaplanır. AD633 çarpma entegresi çarpım sonuçlarını 10'a böldüğü için bulunan değerler 10 ile bölünmelidir.

$$b = \frac{1}{R_3 C_1 \cdot 2505} \qquad R_3 = \frac{1}{2505 \cdot 10^{-9} \cdot 6,7} = 59,7k\Omega$$

$$a = \frac{1}{R_4 C_6 \cdot 2505} \qquad R_4 = \frac{1}{2505 \cdot 10^{-9} \cdot 2} = 200k\Omega$$

$$R_5 = \frac{1}{2505 \cdot 10^{-9} \cdot 10} = 40k\Omega$$

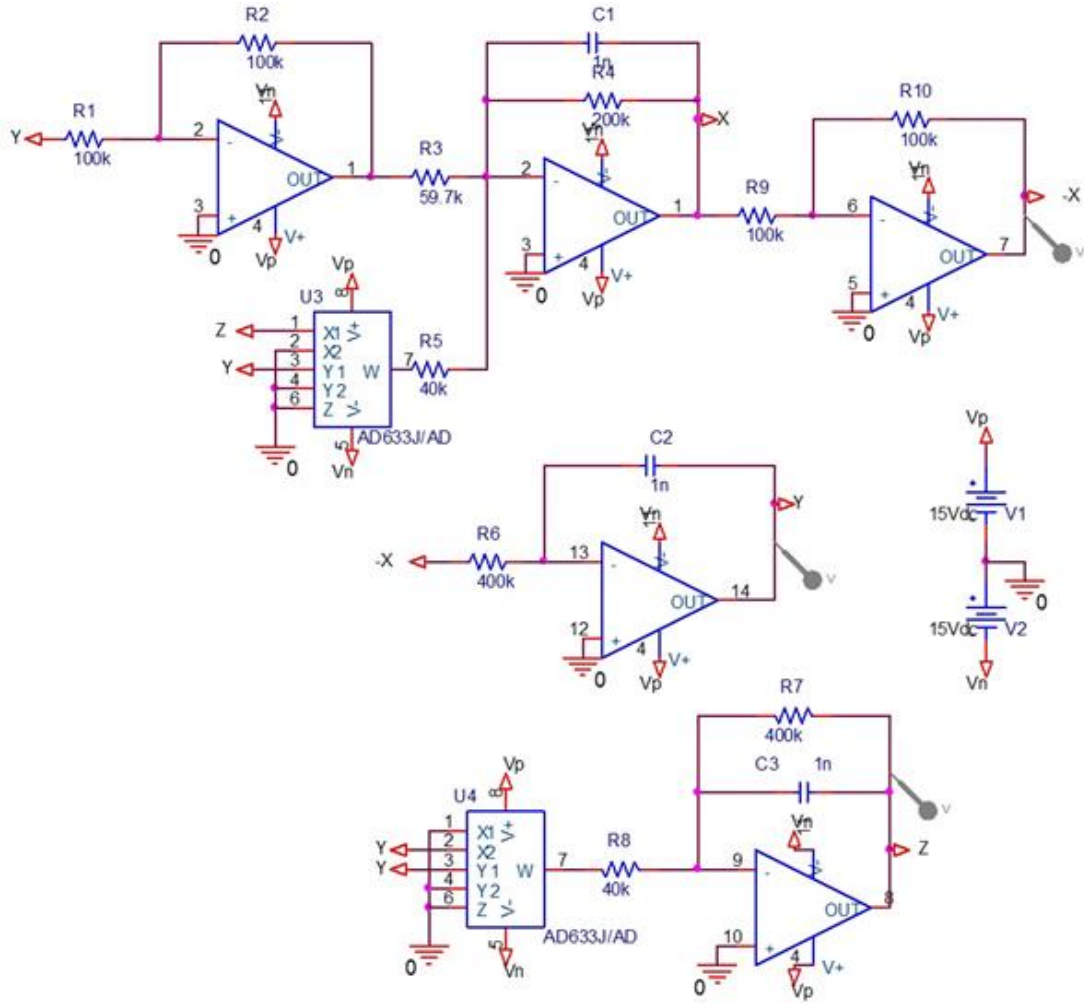
$$R_6 = \frac{1}{2505 \cdot 10^{-9}} = 400k\Omega$$

$$R_7 = \frac{1}{2505 \cdot 10^{-9}} = 400k\Omega$$

$$R_8 = \frac{1}{2505 \cdot 10^{-9} \cdot 10} = 40k\Omega$$

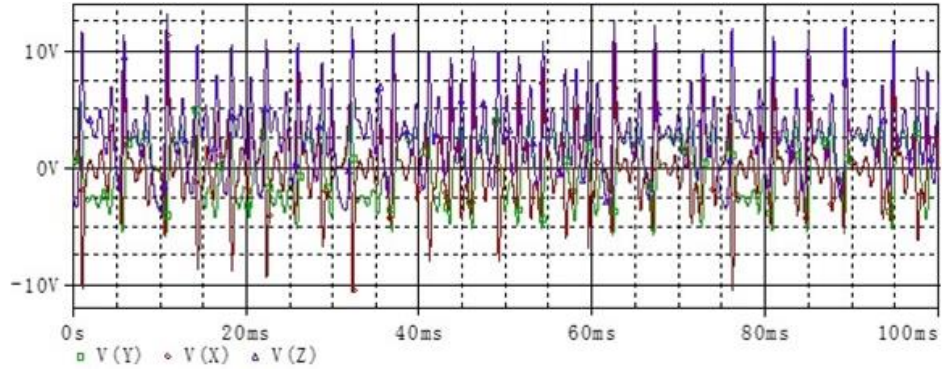
$a=2$, $b=6.7$, parametre değerleri için, elde edilen ifadelerdeki kondansatör değerleri, $C_1, C_2, C_3 = 1nf$ seçilmiş, direnç değerleri $R_3=59k7$, $R_4=200k$, $R_5=R_8=40k$, $R_6=R_7=400k$ ve $R_1=R_2=R_9=R_{10}=100k$ olarak hesaplanmıştır.

Elde edilen değerler ile tasarlanmış Rucklidge sisteminin elektronik devre şeması Şekil 5.1.'de görüldüğü gibidir. Gerçekleştirilen elektronik devre; direnç, opamp, çarpma entegresi, kondansatör gibi temel elektronik elemanlardan meydana gelmektedir. Rucklidge kaotik sistemi elektronik devre gerçekleştirilmesinde, opamp olarak TL081, çarpma entegresi olarak ise AD633 (Analog Devices) kullanılmıştır.

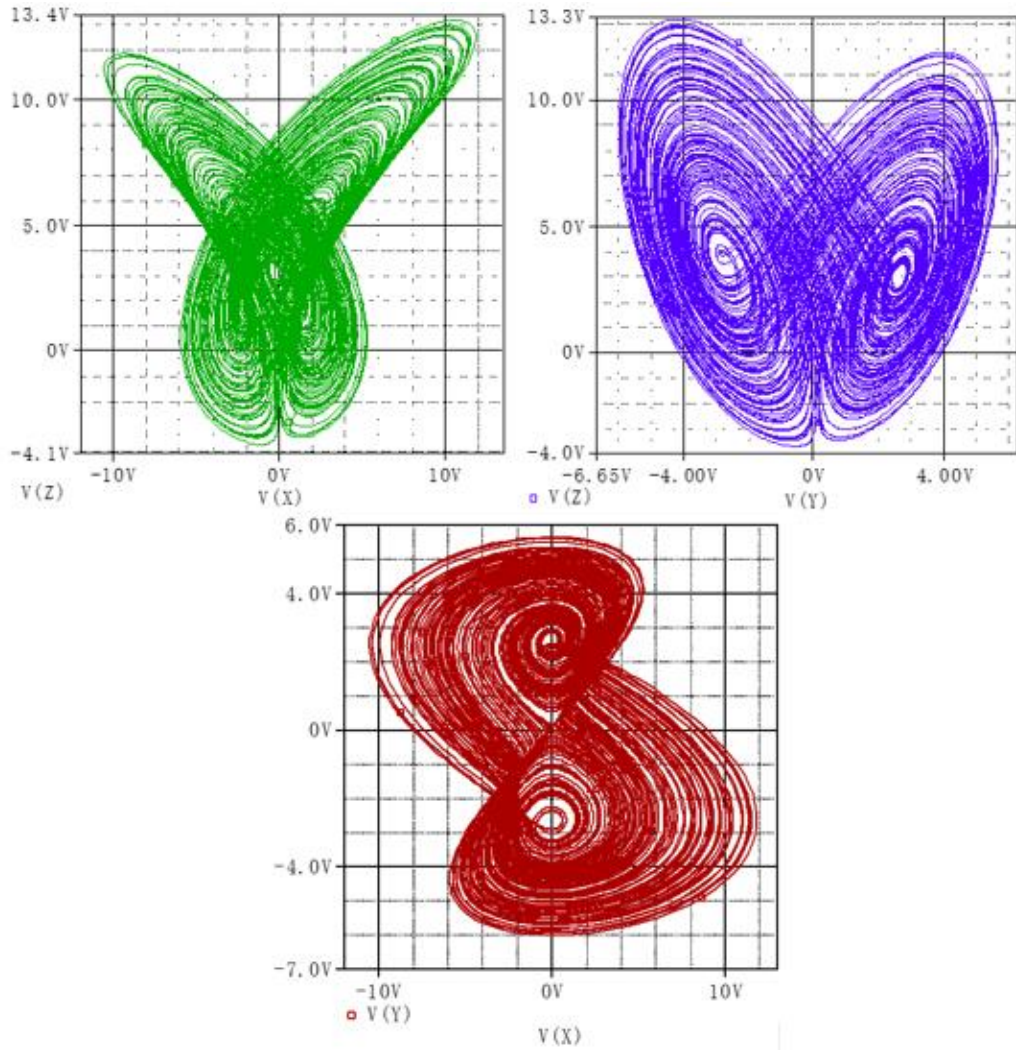


Şekil 5.1. Rucklidge kaotik sistemi devre şeması

Rucklidge sistemi için elektronik devre simülasyonu OrCAD-PSpice programı ile gerçekleştirilmiştir. Rucklidge sistemi için elde edilen x, y, z zaman serisi çıktıları Şekil 5.2.'de, XY, XZ, YZ faz portre çıktıları Şekil 5.3.'te görülmektedir.

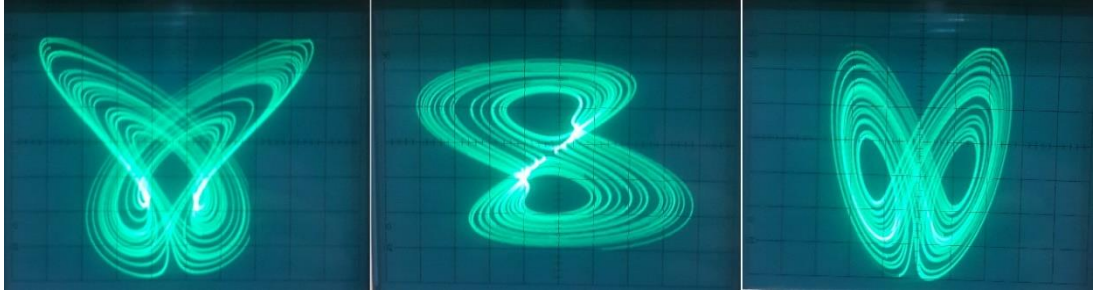


Şekil 5.2. Rucklidge kaotik sistemi X, Y, Z zaman serileri OrCAD-PSpice programı çıktıları



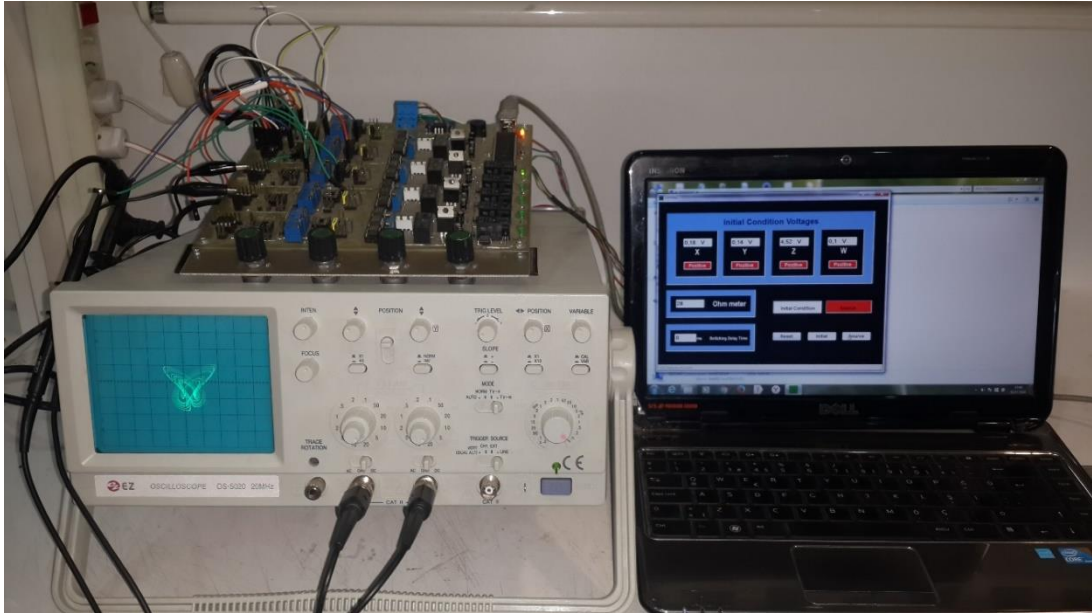
Şekil 5.3. Rucklidge kaotik sistemi XZ, YZ, XY faz portreleri OrCAD-PSpice programı çıktıları

Şekil 5.1’de devre şeması görülen Rucklidge sisteminin gerçek devresini kurmak için tasarlanan KDDS kullanılmıştır [76,77]. Kurulan gerçek devrenin XZ, XY ve YZ osiloskop çıktıları Şekil 5.4.’te görülmektedir.



Şekil 5.4. Rucklidge kaotik sisteminin sırasıyla XZ, XY, YZ faz portelerine ait osiloskop çıktıları

Şekil 5.5.'te Rucklidge kaotik sisteminin tasarlanan KDDS [84] ile gerçekleştirilmesi görülmektedir.



Şekil 5.5. Rucklidge kaotik sistemi devresinin KDDS ile gerçekleştirilmesi

5.2. Chen Kaotik Sisteminin Modellenmesi ve Devre Gerçeklemesi

GRSÜ tasarımı için kaynak olarak kullanılan kaotik sistemlerden ikincisi Chen kaotik sistemidir. Chen kaotik sistemine ait diferansiyel denklem takımı, Denklem (5.3)'de verildiği gibidir.

$$\begin{aligned}
\dot{x} &= a(y - x) \\
\dot{y} &= (c - a)x - xz - cy \\
\dot{z} &= xy - bz
\end{aligned} \tag{5.3}$$

Chen sistemin tipik parametre değerleri $a=35$, $b=3$, $c=28$ başlangıç değerleri ise $x_0= -10V$, $y_0=0V$, $z_0=37V$ 'tur [74]. Sisteminin dinamik sınırları, devredeki Opamp besleme voltaj sınırlarını aştığı için x , y ve z değişkenlerinin skala edilmesi gerekmektedir. Yeni değişkenler $x/10$, $y/10$, ve $z/10$ olarak alınırsa devresi kurulacak Chen sistemi denklemleri Denklem (5.4) gibi olur.

$$\begin{aligned}
\dot{x} &= a(v - u) \\
\dot{y} &= (c - a)u - 10uw - cv \\
\dot{z} &= 10vu - bw
\end{aligned} \tag{5.4}$$

Skala edilmiş Chen sisteminin başlangıç şartları $X_0=0.16V$, $Y_0=0.16V$ ve $Z_0=9V$ seçilmiştir. Rucklidge kaotik devresi elektronik elemanlar ile modellediğinde Denklem (5.5) elde edilir.

$$\begin{aligned}
\dot{x} &= \frac{1}{R_2 C_1} y - \frac{1}{R_1 C_1} x \\
\dot{y} &= \frac{1}{R_4 C_2} x - \frac{1}{R_5 C_2} xz - \frac{1}{R_3 C_2} y \\
\dot{z} &= \frac{1}{R_7 C_3} xy - \frac{1}{R_6 C_3} z
\end{aligned} \tag{5.5}$$

Elde edilen \dot{x} , \dot{y} , \dot{z} ifadelerinde, kapasitörlerin değerleri devrenin zamanlama skala değerine bağlıdır. Bu çalışmada, zamanlama skala değeri $\beta = 2505$ alınmıştır. Denklem (5.5)'te verilen katsayılar eşitlenerek direnç değerleri hesaplanır. AD633 çarpma entegresi çarpım sonuçlarını 10'a böldüğü için bulunan değerler 10 ile bölünmelidir.

$$R_1 = \frac{1}{2505 \cdot 10^{-9} \cdot 35} = 11.40 \text{k}\Omega$$

$$R_2 = \frac{1}{2505 \cdot 10^{-9} \cdot 35} = 11.40 \text{k}\Omega$$

$$R_3 = \frac{1}{2505 \cdot 10^{-9} \cdot 28} = 14.26 \text{k}\Omega$$

$$R_4 = \frac{1}{2505 \cdot 10^{-9} \cdot 7} = 57 \text{k}\Omega$$

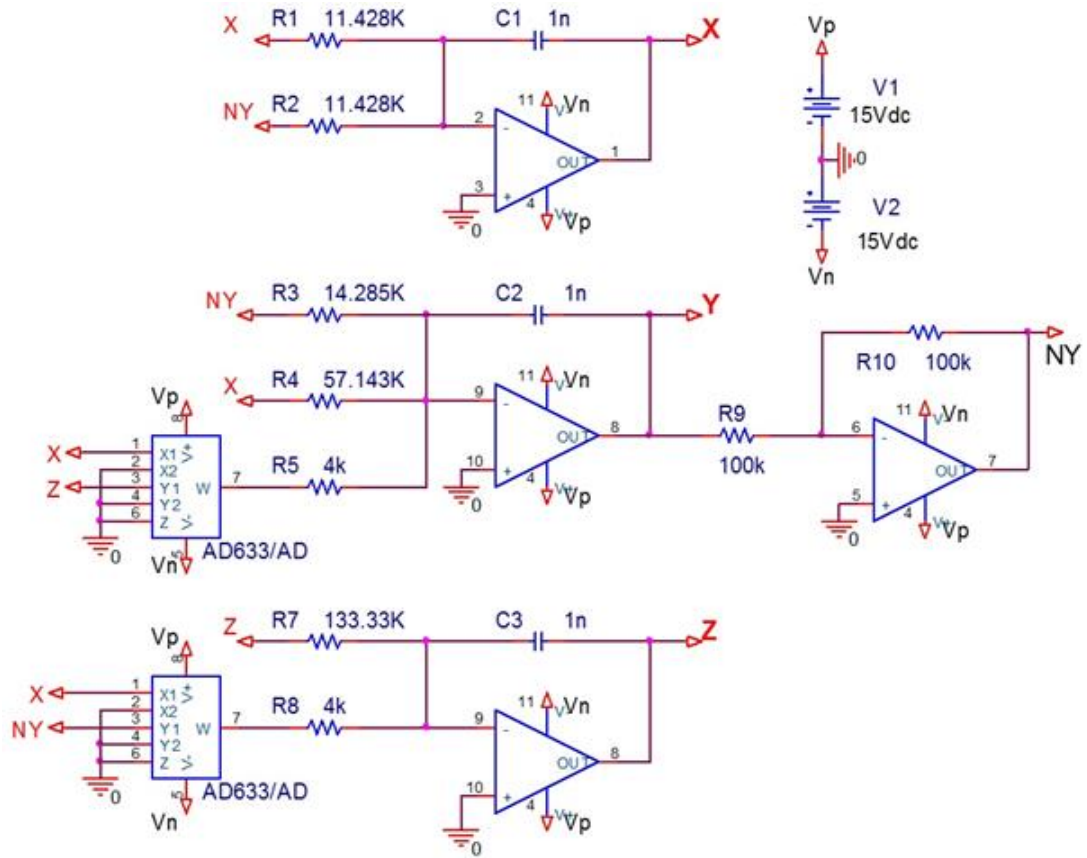
$$R_5 = \frac{1}{2505 \cdot 10^{-9} \cdot 10 \cdot 10} = 4 \text{k}\Omega$$

$$R_6 = \frac{1}{2505 \cdot 10^{-9} \cdot 3} = 133 \text{k}\Omega$$

$$R_7 = \frac{1}{2505 \cdot 10^{-9} \cdot 10 \cdot 10} = 4 \text{k}\Omega$$

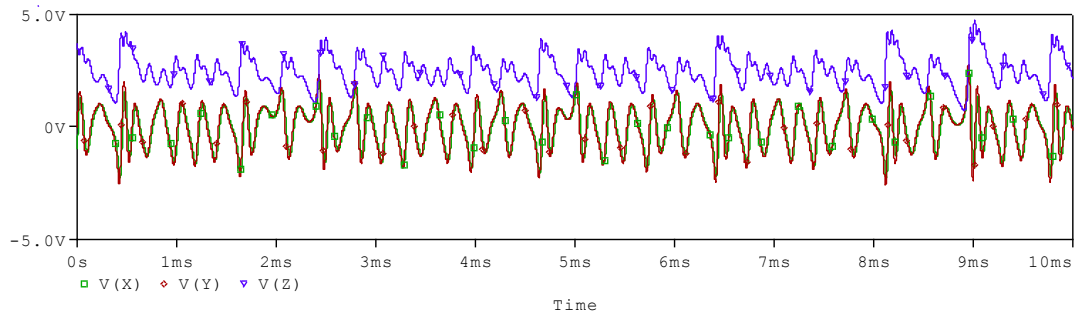
a=35, b=3, c=28 parametre değerleri için, elde edilen ifadelerdeki kondansatör değerleri, $C_1, C_2, C_3 = 1 \text{nf}$ seçilmiş, direnç değerleri $R_1=R_2=11.40 \text{k}$, $R_3=14.26 \text{k}$, $R_4=57 \text{k}$, $R_5=R_8=4 \text{k}$, $R_6=133 \text{k}$, $R_7=4 \text{k}$, $R_9=R_{10}=100 \text{k}$ olarak hesaplanmıştır.

Elde edilen değerler ile tasarlanmış, skala edilmiş Chen sisteminin elektronik devre şeması Şekil 5.6.'da görüldüğü gibidir. Gerçekleştirilen elektronik devre; direnç, opamp, çarpma entegresi, kondansatör gibi temel elektronik elemanlardan meydana gelmektedir. Elektronik devre gerçekleştirilmesinde opamp olarak TL081, çarpma entegresi olarak ise AD633 (Analog Devices) kullanılmıştır.

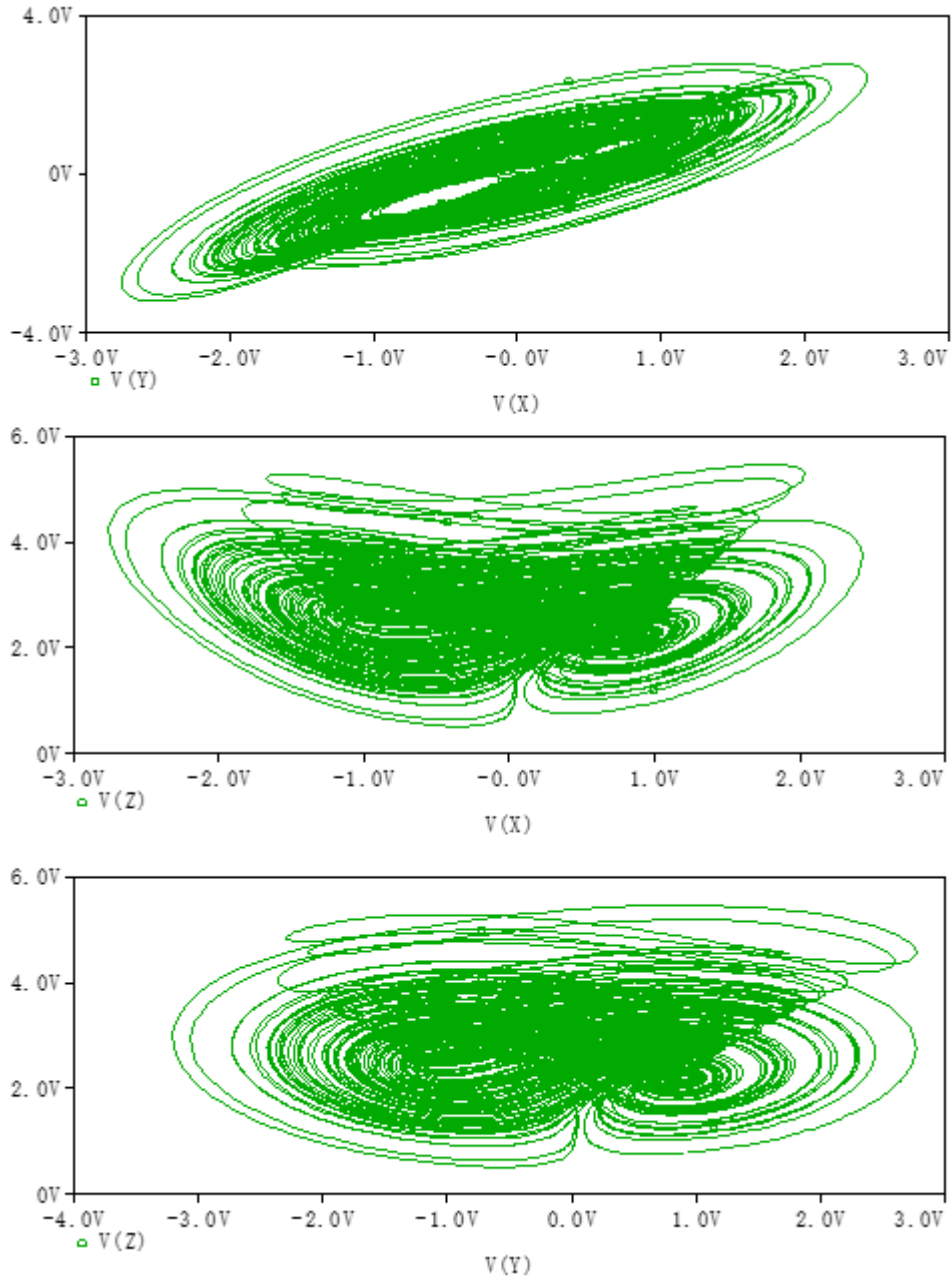


Şekil 5.6. Skala edilmiş Chen kaotik sistemi devre şeması

OrCAD-PSpice programı kullanılarak gerçekleştirilen simülasyon sonucu skala edilmiş Chen sistemi için elde edilen X, Y, Z zaman serisi, Şekil 5.7.'de, XY, XZ, YZ faz portresi çıktıları Şekil 5.8'de gösterilmiştir.

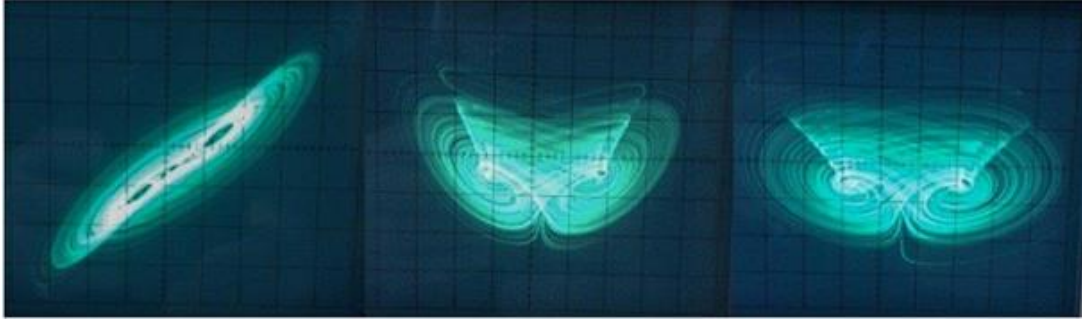


Şekil 5.7. Skala edilmiş Chen kaotik sistemi X, Y, Z zaman serileri OrCAD-PSpice programı çıktıları



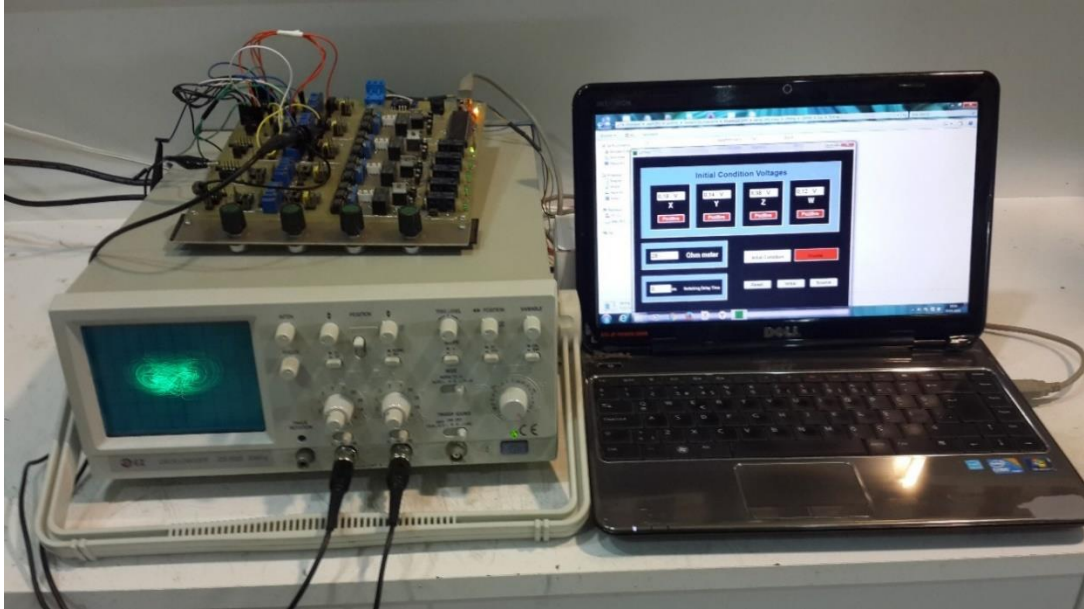
Şekil 5.8. Skala edilmiş Chen kaotik sistemi XY, XZ, YZ faz portreleri OrCAD-PSpice programı çıktıları

Skala edilmiş Chen sisteminin gerçek devresini kurmak için tasarlanan KDDS kullanılmıştır [84]. Kurulan gerçek devrenin XY, XZ, YZ osiloskop çıktıları Şekil 5.9.'da görülmektedir.



Şekil 5.9. Chen kaotik sistemi sırasıyla XY, XZ, YZ faz portrelerine ait osiloskop çıktıları

Şekil 5.10.'da Skala edilmiş Chen kaotik sisteminin tasarlanan KDDS [84] ile gerçekleştirilmesi görülmektedir.



Şekil 5.10. Skala edilmiş Chen kaotik sistemi devresinin KDDS ile gerçekleştirilmesi

5.3. Zhongtang Kaotik Sisteminin Modellenmesi ve Devre Gerçeklemesi

GRSÜ tasarımı için kaynak olarak kullanılan kaotik sistemlerden sonuncusu Zhongtang kaotik sistemidir. Zhongtang kaotik sistemine ait diferansiyel denklem takımı, Denklem (5.6)'da verildiği gibidir.

$$\begin{aligned}
\dot{x} &= a(y - x) \\
\dot{y} &= b(x + y) - xz^2 \\
\dot{z} &= -ex - cz + x^2
\end{aligned} \tag{5.6}$$

Zhongtang sistemin tipik parametre değerleri $a=40$, $b=10$, $c=15$, $e=20$ ve başlangıç değerleri ise $X_0=1V$, $Y_0=0V$, $Z_0=1V$ tur [79]. Sistemin dinamik sınırları, devredeki Opamp besleme voltaj sınırlarını aştığı için x , y ve z değişkenlerinin skala edilmesi gerekmektedir. Yeni değişkenler x , $y/2$ ve $z/2$ olarak alınırsa devresi kurulacak Zhongtang denklemleri Denklem (5.7) gibi olur.

$$\begin{aligned}
\dot{x} &= 80y - 40x \\
\dot{y} &= 5x + 10y - 2xz^2 \\
\dot{z} &= -10x - 15z + x^2
\end{aligned} \tag{5.7}$$

Skala edilmiş Zhongtang sistemin başlangıç şartları $x(0)=1V$, $y(0)=0V$ ve $z(0)=1V$ seçilmiştir. Rucklidge kaotik devresi elektronik elemanlar ile modellediğinde diferansiyel denklem Denklem (5.8) elde edilir.

$$\begin{aligned}
\dot{x} &= \frac{1}{R_1 C_1} \cdot y - \frac{1}{R_2 C_1} \cdot x \\
\dot{y} &= \frac{1}{R_4 C_2} \cdot x + \frac{1}{R_3 C_2} \cdot y - \frac{1}{R_5 C_2} xz^2 \\
\dot{z} &= -\frac{1}{R_7 C_3} x - \frac{1}{R_6 C_3} z + \frac{1}{R_8 C_3} x^2 z
\end{aligned} \tag{5.8}$$

Elde edilen \dot{x} , \dot{y} , \dot{z} ifadelerinde, kapasitörlerin değerleri devrenin zamanlama skala değerine bağlıdır. Bu çalışmada, zamanlama skala değeri $\beta = 2505$ alınmıştır. Denklem (5.8)'de verilen katsayılar eşitlenerek direnç değerleri hesaplanır. AD633 çarpma entegresi çarpım sonuçlarını 10'a böldüğü için bulunan değerler 10 ile bölünmelidir.

$$R_1 = \frac{1}{2505 \cdot 10^{-9} \cdot 80} = 5k\Omega$$

$$R_2 = \frac{1}{2505 \cdot 10^{-9} \cdot 40} = 10k\Omega$$

$$R_3 = \frac{1}{2505 \cdot 10^{-9} \cdot 10} = 40k\Omega$$

$$R_4 = \frac{1}{2505 \cdot 10^{-9} \cdot 5} = 80k\Omega$$

$$R_5 = \frac{1}{2505 \cdot 10^{-9} \cdot 2 \cdot 10 \cdot 10} = 2k\Omega$$

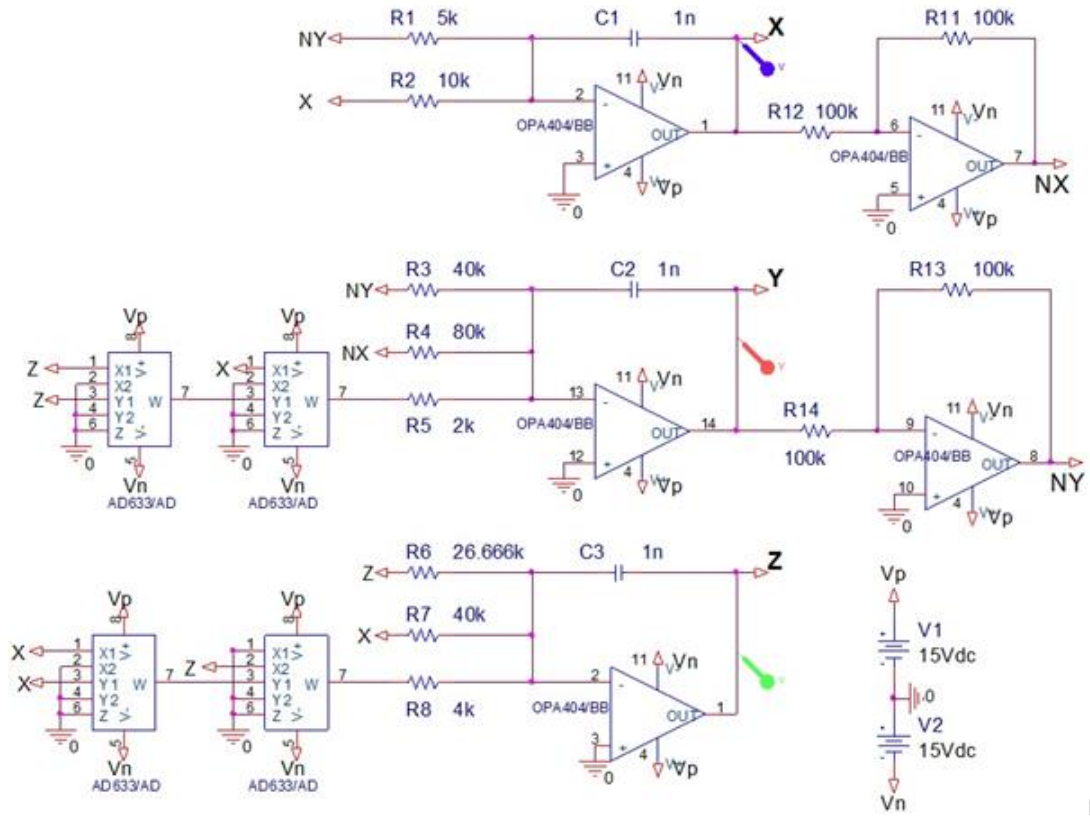
$$R_6 = \frac{1}{2505 \cdot 10^{-9} \cdot 15} = 26,666k\Omega$$

$$R_7 = \frac{1}{2505 \cdot 10^{-9} \cdot 10} = 40k\Omega$$

$$R_8 = \frac{1}{2505 \cdot 10^{-9} \cdot 10 \cdot 10} = 4k\Omega$$

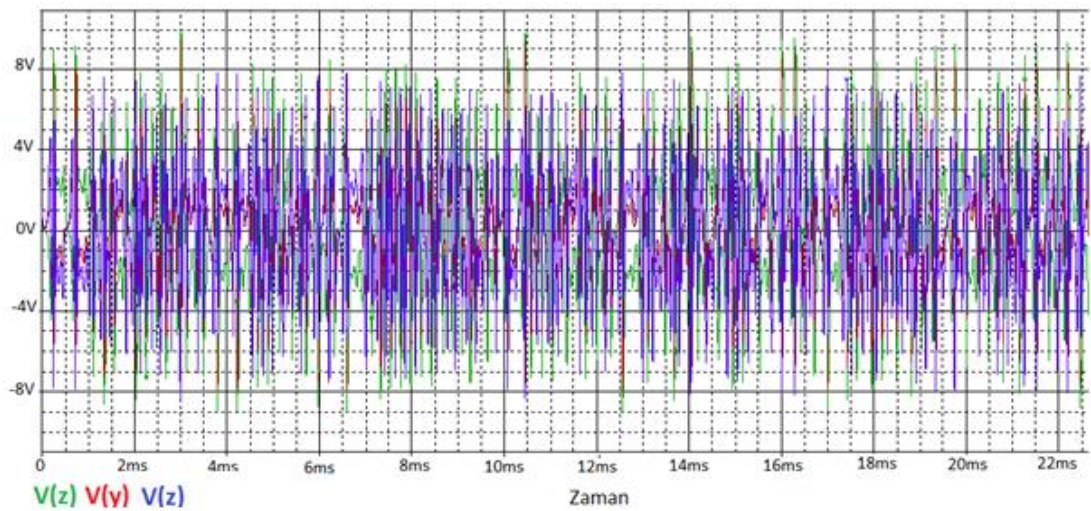
a=40, b=10, c=15, e=20 parametre değerleri için, elde edilen ifadelerdeki kondansatör değerleri, $C_1, C_2, C_3 = 1\text{nf}$ seçilmiş, direnç değerleri $R_1=5K, R_2=10K, R_3=R_7=40K, R_4=80K, R_5=2K, R_6=26,666K, R_8=4K, R_{11}=R_{12}=R_{13}=R_{14}=100K$ olarak hesaplanmıştır.

Elde edilen değerler ile tasarlanmış, skala edilmiş Zhongtang sisteminin elektronik devre şeması Şekil 5.11.'de görüldüğü gibidir. Gerçekleştirilen elektronik devre; direnç, opamp, çarpma entegresi, kondansatör gibi temel elektronik elemanlardan meydana gelmektedir. Elektronik devre gerçekleştirilmesinde opamp olarak TL081, çarpma entegresi olarak ise AD633 (Analog Devices) kullanılmıştır.

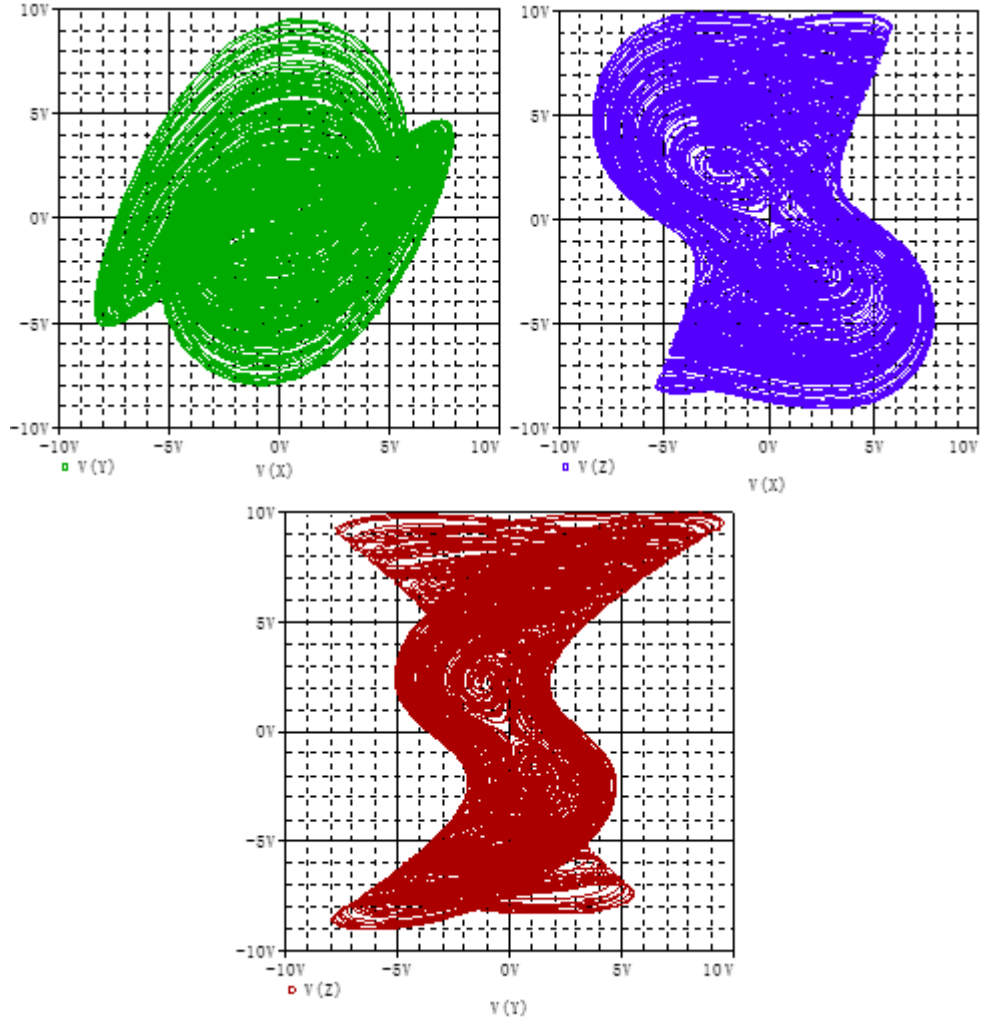


Şekil 5.11. Skala edilmiş Zhongtang kaotik sistemi devre şeması

Gerçekleştirilen simülasyon sonucu skala edilmiş Zhongtang sistemi için elde edilen X, Y, Z zaman serisi çıktıları Şekil 5.12.'de, XY, XZ, YZ faz portre çıktıları Şekil 5.13.'te görüldüğü gibidir.

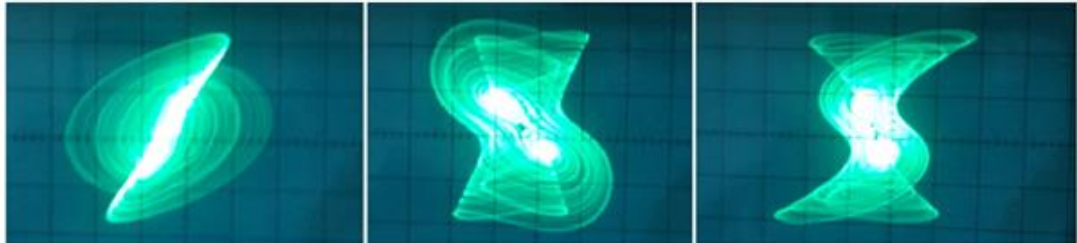


Şekil 5.12. Skala edilmiş Zhongtang kaotik sistemi X, Y, Z zaman serisi OrCAD-PSpice programı çıktıları



Şekil 5.13. Skala edilmiş Zhongtang kaotik sistemi XY, XZ, YZ faz portreleri OrCAD-PSpice programı çıktıları

Skala edilmiş Zhongtang sisteminin gerçek devresini kurmak için tasarlanan KDDS [84] kullanılmıştır. Kurulan gerçek devrenin XY, XZ, YZ osiloskop çıktıları Şekil 5.14.'te görülmektedir.



Şekil 5.14. Skala edilmiş Zhongtang kaotik sistemi sırasıyla XY, XZ, YZ faz portelerine ait osiloskop çıktıları

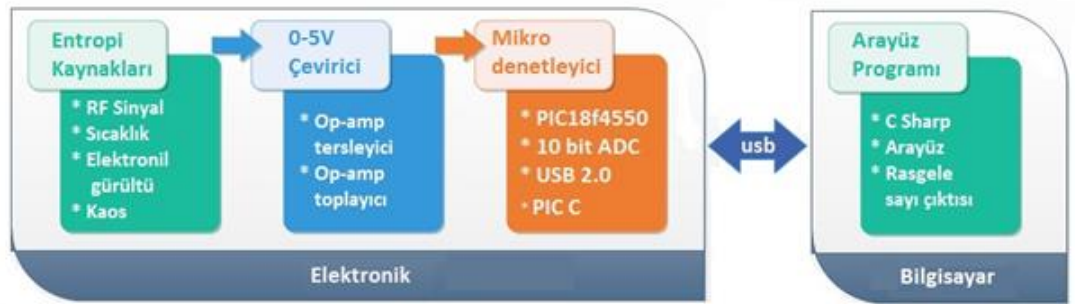
Şekil 5.15.'te Zhongtang kaotik sisteminin tasarlanan KDDS ile gerçekteşmesi görölmektedir.



Şekil 5.15. Skala edilmiş Zhongtang kaotik sistemi devresinin KDDS ile gerçekteşmesi

BÖLÜM 6. GRSÜ TASARIMLARI İÇİN YENİ BİR PLATFORM TASARIMI VE GERÇEKLEMESİ

ADC tabanlı gerçek rasgele sayı üretici çıkışlarının rasgeleliği iyi bir entropi kaynağının yanında, ADC çevrimi için kullanılacak bit örnekleme zamanı, kullanılacak bit sayısı ve son işlem algoritmaları gibi tasarım parametrelerine bağlıdır [9,16,85]. En uygun parametreleri bulmak için devre düzenekleri üzerinde çok sayıda denemelerin yapılması gerekmektedir. ADC tabanlı gerçek rasgele sayı üretici (GRSÜ) tasarımlarının kolay, hızlı ve esnek yapılabilmesine olanak sağlayan yeni bir bilgisayar ve mikro denetleyici kontrollü platform (BMKP) tasarlanmış ve gerçekleştirilmiştir. Tasarlanan platform, Şekil 6.1.'de görüldüğü gibi 4 bölümden oluşmaktadır.



Şekil 6.1. GRSÜ gerçeklemek için tasarlanan BMKP'nin blok diyagramı

6.1. GRSÜ Entropi Kaynakları

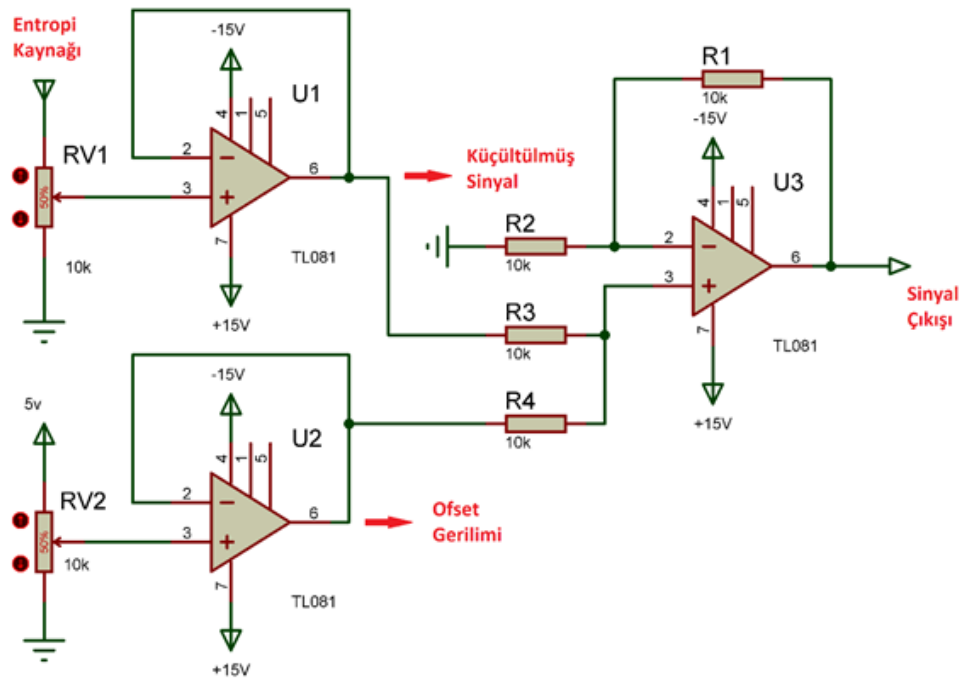
Entropi, en sade ifadeyle bir sistemin düzensizliğinin ölçüsüdür. GRSÜ'nün rasgeleliği öncelikle iyi bir entropi kaynağına bağlıdır. GRSÜ için entropi kaynağı fiziksel rasgelelik kaynağıdır. GRSÜ'lerde kullanılan başlıca gürültü kaynakları;

- RF sinyallerdeki gürültü
- Termal gürültü
- Güneş ışığındaki gürültü
- Elektronik devre elemanlarının yaydığı elektriksel gürültü
- Kaotik osilatörlerdir [16,88,89].

Gerçekleştirilen GRSÜ tasarımında entropi kaynağı olarak kaotik sistemler kullanılmıştır.

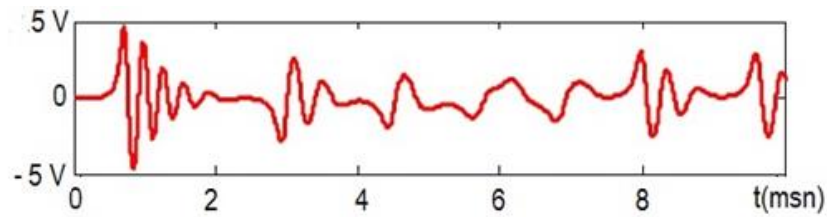
6.2. ADC 0-5V Seviye Uyunlaştırıcı Devre Tasarımı

Rasgele sayı üretmek üzere kullanılan kaotik sistemlere ait sinyaller, tepeden tepeye genlik seviyelerinin büyüklüğü ve negatif voltaj değerlerinden dolayı, direk olarak mikro denetleyici ADC kanalları ile örneklemeğe uygun değildir. Bundan dolayı, bu tip entropi kaynaklarından gelen sinyallerin voltaj seviyelerini, ADC için gerekli olan 0-5V ölçüm aralığına uygunlaştırmak gerekmektedir. Bu amaçla tasarlanan uygunlaştırıcı elektronik devreye ait şema Şekil 6.2.'de görülmektedir.

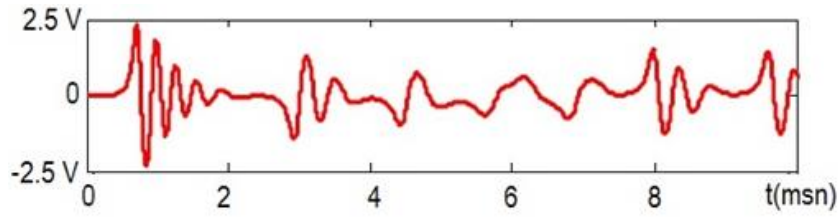


Şekil 6.2. ADC için 0-5V seviye uygunlaştırıcı devre şeması

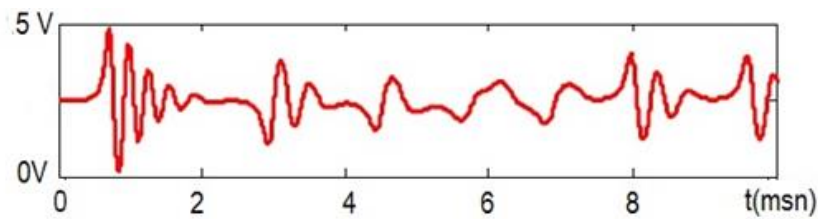
Uygunlaştırıcı devre, ilk olarak girişine uygulanan sinyali tepeden tepeye 5V seviyesine küçültmektedir. Daha sonra, elde edilen küçültülmüş sinyalin sahip olduğu en küçük negatif değer miktarında bir ofset gerilimi ile sinyali toplar. Bu şekilde sinyal, ADC örnekleme işlemi için gerekli olan 0-5 V genlik seviyesine getirilmiş olur. Uygunlaştırıcı devrenin çalışmasının daha iyi anlaşılması için, devre girişine uygulanan örnek bir kaotik sinyal Şekil 6.3.'te, tepeden tepeye 5V seviyesine küçültülmüş kaotik sinyal Şekil 6.4.'te, 0-5 V genlik seviyesine uygunlaştırılmış kaotik sinyal ise Şekil 6.5.'te görülmektedir.



Şekil 6.3. Örnek kaotik sinyal



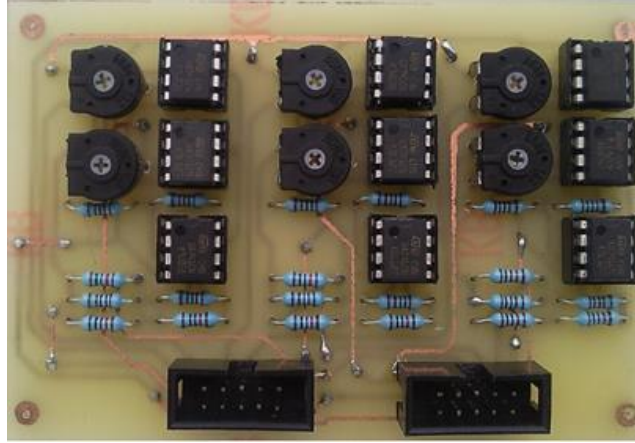
Şekil 6.4. 1/2 oranında küçültülmüş örnek kaotik sinyal



Şekil 6.5. 0-5V seviyesine uygunlaştırılmış kaotik sinyal

Sinyal küçültme ve 0-5V uygunlaştırma işlemleri yapılırken, devreler arası empedans uygunlaştırmak için buffer devreleri kullanılmıştır. Seviye uygunlaştırıcı devre, farklı entropi kaynaklarına ait sinyal çıkışlarının aynı anda kullanılmasına imkan sağlamak üzere üç kanal olarak tasarlanmıştır. Şekil 6.2.'de şeması verilen seviye uygunlaştırıcı devrede, RV1 trimpotu ile sinyaller küçültülmekte, RV2 trimpotu ile ofset gerilimleri

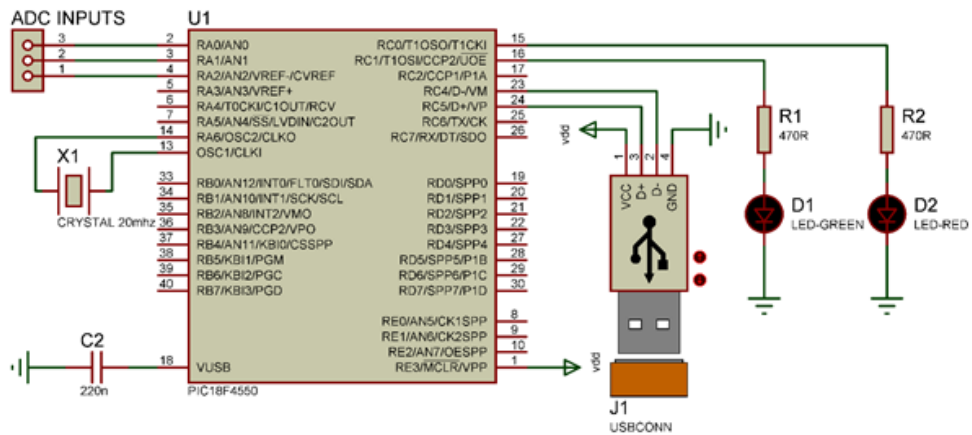
ayarlanmaktadır. Şekil 6.6.'da gerçekleştirilen ADC için 0-5V seviye uygunlaştırıcı gerçek devre görülmektedir.



Şekil 6.6. ADC için 0-5V seviye uygunlaştırıcı gerçek devre

6.3. Mikro Denetleyici Kontrollü Veri Toplama Kartı Tasarımı

Entropi kaynağından elde edilen analog sinyalleri dijital verilere dönüştürmek ve bu verileri yorumlayıp belirli bir formatta USB üzerinden bilgisayara göndermek amacıyla devre şeması Şekil 6.7.'de görülen mikro denetleyici kontrollü veri toplama kartı tasarlanmıştır. Tasarlanan devrede mikro denetleyici olarak yeterli miktarda 10 bit dahili ADC kanalı ve USB 2.0 özelliği bulundurmasından dolayı PIC18f4550 mikro denetleyicisi tercih edilmiştir.



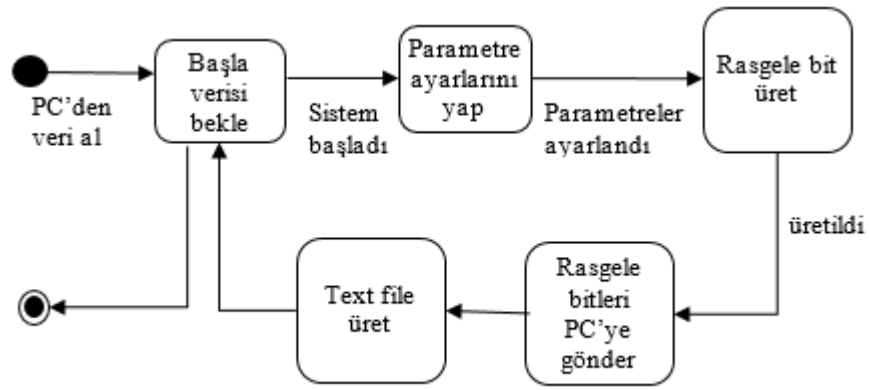
Şekil 6.7. Mikro denetleyici kontrollü veri toplama kartı devre şeması

Şekil 6.8.'de şekli verilen veri toplama kartı, konektör üzerinde üç ayrı kanaldan analog okuma yapabilmektedir. Besleme gerilimini USB üzerinden almaktadır. Kart üzerinde bulunan iki adet LED'ten biri bilgisayar ile haberleşme kurulduğunu diğeri de veri akışının yapıldığını göstermektedir.



Şekil 6.8. Mikro denetleyici kontrollü veri toplama kartı

PIC18f4550 mikro denetleyicisine ait yazılım C programlama dilinde yazılmıştır. Derleyici olarak CCS PIC C COMPILER kullanılmıştır. Yazılan yazılımın durum diyagramı Şekil 6.9.'da görülmektedir.



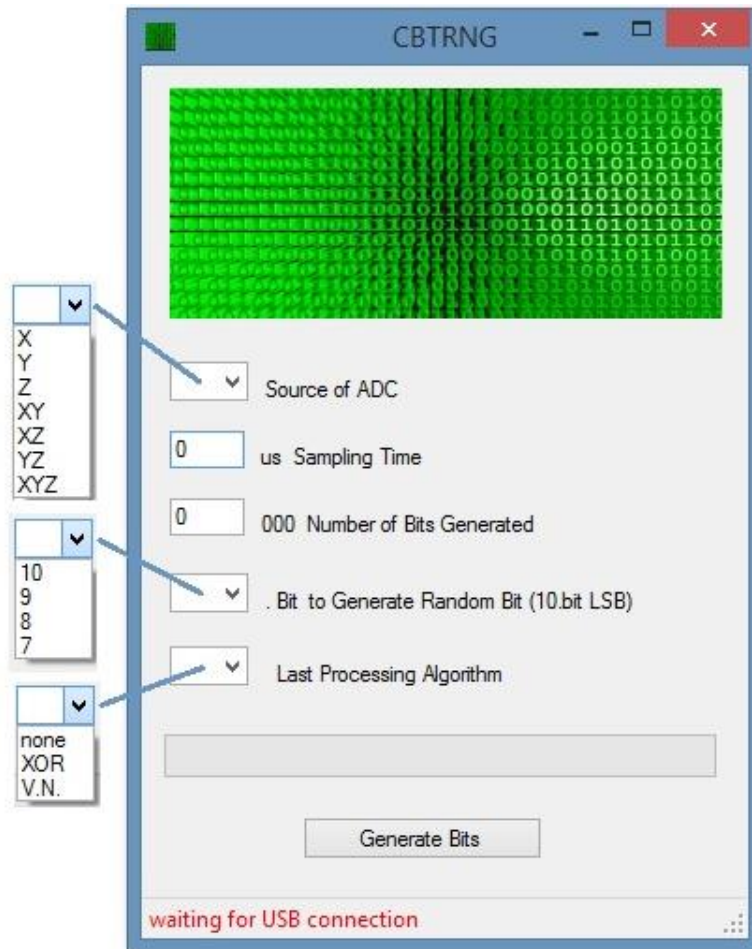
Şekil 6.9. PIC18f4550 mikro denetleyicisine ait yazılımın durum diyagramı

Şekil 6.9.'da verilen durum diyagramından görüldüğü gibi, mikro denetleyici kontrollü veri toplama kartı, USB üzerinden bilgisayar ile bağlantı kurduğunda, kart üzerindeki veri LED'i bağlantının problemsiz yapıldığı anlamına gelen titreme davranışını yapar. Daha sonra, bilgisayar programından "rasgele bitleri üretirken kullanacağı parametreleri ve "Start" komutunu içeren veri paketinin gelmesini bekler. Bu parametreler, ADC örnekleme yapılacak bit, örnekleme zamanı, entropi kaynak

girişi, son işlem algoritması ve üretilecek rasgele bit sayısıdır. Veri paketi geldiğinde, parametre ayarları yapılır ve istenilen sayıda rasgele bit üretme işlemine başlanır. Rasgele bit üretme işleminin devam etme süreci elektronik kart üzerindeki veri LED'İ ile izlenebilir. Üretilen rasgele bitler, anlık olarak, 500 bitlik paketler halinde bilgisayar programına aktarılır.

6.4. Bilgisayar Programı Tasarımı

Rasgele bit üretimi yapılmadan önce, mikro denetleyicinin parametre ayarlarının yapılabilmesi ve rasgele bitlerin belli bir formatta text dosyasına dönüştürülmesi için C Sharp programlama dili ile bir program yazılmıştır. Bilgisayar programı ile mikro denetleyici, USB ile haberleşmektedir. Şekil 6.10.'da yazılan bilgisayar programına ait arayüz görüntüsü görülmektedir.

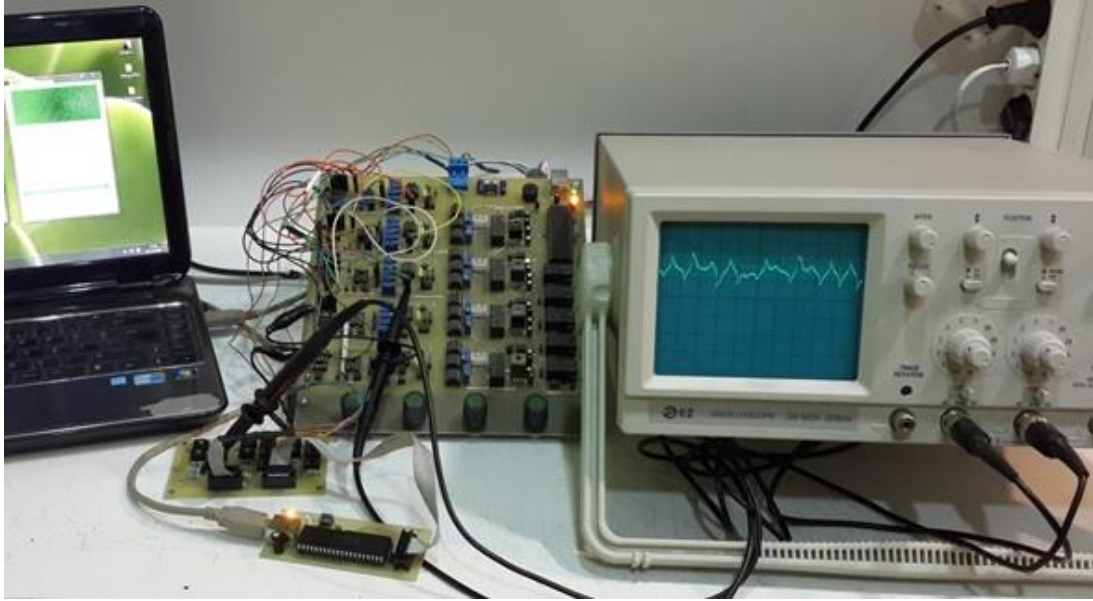


Şekil 6.10. C Sharp programında hazırlanan bilgisayar programı arayüz görüntüsü

Bilgisayar programı açıldığında ilk olarak arayüzün altında bulunan pencerede elektronik kart ile haberleşmenin olup olmadığı gösterilir. Arayüzde bulunan “Source of ADC”, elektronik kart üzerinde bulunan X, Y, Z isimli 3 farklı ADC kanalından hangisinin kullanılacağını belirler. Seçim X, Y, Z, XY, XZ, YZ ve XYZ olmak üzere 7 farklı şekilde gerçekleştirilebilir. XY, XZ, YZ, XYZ seçimlerinde sinyaller XOR işlemine tabi tutulur. “Sampling Time ile ADC” örnekleme zamanı 1 ile 1000 mikro saniye arasında ayarlanır. “Number of Bits Generated” ile üretilmek istenen bit sayısı 1.000 ile 1.000.000 arasında 1.000 bit çözünürlükle yapılır. “Use x. Bit to Generate Random Bit” ile 10 bit dijital veriye çevrilmiş sinyalin kaçınıcı bitini rasgele bit üretmek için kullanılacağı belirlenir. Kaynak olarak, 10. bit LSB olmak üzere 10, 9, 8 ve 7. bitler seçilebilir. “Last Processing Algorithm” ile üretilen bitlerin hangi son işlem algoritmasına tabi olacağı seçilir. Son işlem algoritması olarak XOR işlemi, Von Neumann algoritması veya hiçbiri seçenekleri seçilebilir. Programın kullanım senaryosu aşağıdaki gibidir.

- USB 2.0 kablosunu bilgisayar ve elektronik veri toplama kartına tak.
- Bilgisayar programını çalıştır ve veri toplama kartı ile USB bağlantısını kontrol et.
- ADC örnekleme için kullanılacak kaynağı seç.
- ADC örnekleme zamanını gir.
- Üretilmek istenen bit sayısını gir.
- ADC örnekleme için kullanılacak bit numarasını seç. (LSB 10.bit)
- Son işlem algoritmasını seç.
- Üret butonuna basarak bit üretme işlemini başlat.

Üretilen rasgele bitler, mytextfile isimli text dosyada kök dizine kaydedilir. Şekil 6.11.’de geliştirilen BMKP ile örnek GRSÜ gerçekleştirilmesi görülmektedir.



Şekil 6.11. Geliştirilen BMKP ile örnek GRSÜ gerçekleştirilmesi

Şekil 6.12’de BMKP ile gerçekleştirilen Zhongtang kaotik sistemi entropi kaynağı olarak kullanılan GRSÜ’den elde edilen 1000 bit rasgele sayı dizisi görülmektedir.

```

11110111010010111001111000010110110011111001011011
01110101111011101100011010011100000010100000101000
01000011011101101110110010111011101101000110100100
10000110111111001010100011000111001110111000001110
01010101001001001100100110101100000001011000001001
0100001100010100010100001111111101110001000110011
00001000111110000001001001000101001100000111010011
00110001100100001100101110010010100111011101100110
11011010010100111110111010000110110101111001110001
11000001111100110010100010011000011000011100110101
00001100100101000111110100111100111001101011111001
01001001011011101000000011000011111101000100011110
10010010110100011100110100110110110000011000110111
1010101111111010100011011000001111001000011000000
11000110111011000110001000101101001010111100111110
10001100111010010101100010010001000111111110011101
10101001111011101001010000110101011100101010111110
11111101010000000010111100100001000011001101101111
01101010010010001011101000111001101100100110101000
11001011001111001110111110000111000011100100010010

```

Şekil 6.12. BMKP ile gerçekleştirilmiş Zhongtang kaotik sistemi tabanlı GRSÜ 1000 bit rasgele bit dizisi

BÖLÜM 7. KAOS TABANLI YENİ GRSÜ TASARIMLARI VE GERÇEKLEMELERİ

Son yıllarda, GRSÜ için kaotik osilatörlerin entropi kaynağı olarak kullanılması yaygınlaşmıştır. Kaotik osilatörlerin tercih edilme sebebi, sinyallerin genlik değerlerinin yüksek olması ve diğer gürültü kaynaklarına göre çevresel koşullardan daha az etkilenmeleridir [6,28,86]. Gerçekleştirilen ADC tabanlı rasgele sayı üretimi için entropi kaynağı olarak Rucklidge, Chen ve Zhongtang kaotik sistemleri kullanılmıştır. Gerçekleştirilen kaotik sistemlerin x, y, z çıkışları ayrı ayrı GRSÜ için kaynak olarak kullanılmış ve ADC tabanlı GRSÜ tasarımları için tasarlanan BMKP yardımıyla GRSÜ'leri gerçekleştirilmiştir. Gerçekleştirilen her GRSÜ'den üretilen 1000000 bit, NIST800-22 testlerine tabi tutulmuş ve sonuçlar kullanılan her farklı kaynak için tablolar ile gösterilmiş ve yorumlanmıştır. Üretilen rasgele sayı dizilerinin güvenilirliğini arttırmak için her kaynaktan 10 kez rasgele sayı dizisi üretilmiş ve NIST800-22 testine tabi tutulmuştur.

7.1. Rucklidge Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçeklemesi

GRSÜ için kaynak olarak ilk Rucklidge kaotik osilatörü kullanılmıştır. Kaotik deney seti üzerinde kurulan Rucklidge kaotik osilatörün X, Y, Z sinyal çıkışları ADC ölçümü için 0-5V seviyesine uygunlaştırılmıştır. Daha sonra sistem, gerekli bağlantılar yapılarak rasgele bit üretme deneylerine hazır hale getirilmiştir. Yapılan deneylerde her seferinde 1.000.000 bit rasgele bit üretilmiş ve üretilen rasgele bitler NIST800-22 testlerine tabi tutulmuştur.

Gerçekleştirilen deneyler sonunda, Rucklidge kaotik osilatörün X, Y, Z, XY, YZ, XZ bütün çıkışları için 1 mikro saniye örnekleme zamanı, 10. Bit (LSB) ADC örnekleme biti ve Von Neumann son işlem algoritması parametreleri ile 1.000.000 gerçek rasgele

bit 10 kez üretilmiş ve üretilen rasgele bitler NIST800-22 testine tabi tutulmuştur. En son üretilen rasgele bitlerin NIST800-22 test sonuçları Tablo 7.1. ve Tablo 7.2.'de gösterilmiştir. Tablo 7.1. ve Tablo 7.2.'de görüldüğü gibi sadece Rucklidge kaotik osilatörün X çıkışı, GRSÜ için kaynak olarak kullanıldığında, üretilen 10 farklı rasgele sayı dizisinin tamamı bütün testlerden başarılı olmuştur. Y çıkışı kaynak kullanıldığında, 10 kez gerçekleştirilen GRSÜ'nün sadece bir tanesi testlerinin tamamından başarı olmuştur. Z çıkışı kaynak olarak kullanıldığında 10 kez gerçekleştirilen GRSÜ'lerin hepsi istatistiksel testin tamamından başarısız olmuştur. X çıkışı kaynaklı GRSÜ'nün Von Neumann son işlem algoritması kullanıldığı için rasgele bit üretim hızı sabit değildir. Ortalama rasgele bit üretim hızı 12 kb/sn dir.

Tablo 7.1. Rucklidge kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları

Rucklidge Sistemi	X		Y		Z	
	P-değeri	Sonuç	P-değeri	Sonuç	P-değeri	Sonuç
Frequency (Monobit) Test	0,0551	Başarılı	0,2387	Başarılı		Başarısız
Block-Frequency Test	0,7739	Başarılı	0,4657	Başarılı		Başarısız
Cumulative-Sums Test	0,0551	Başarılı	0,3702	Başarılı		Başarısız
Runs Test	0,0207	Başarılı		Başarısız		Başarısız
Longest-Run Test	0,0436	Başarılı	0,4988	Başarılı		Başarısız
Binary Matrix Rank Test	0,9724	Başarılı	0,2219	Başarılı	0,8114	Başarılı
Discrete Fourier Transform Test	0,6796	Başarılı	0,163	Başarılı		Başarısız
Non-Overlapping Templates Test	0,1496	Başarılı	0,0441	Başarılı		Başarısız
Overlapping Templates Test	0,0599	Başarılı	0,4633	Başarılı		Başarısız
Maurer's Universal Statistical Test	0,037	Başarılı	0,2445	Başarılı		Başarısız
Approximate Entropy Test	0,1255	Başarılı	0,2739	Başarılı		Başarısız
Random-Excursions Test	0,9622	Başarılı	0,2971	Başarılı		Başarısız
Random-Excursions Variant Test	0,1209	Başarılı	0,49	Başarılı		Başarısız
Serial Test-1	0,0859	Başarılı	0,3892	Başarılı		Başarısız
Serial Test-2	0,3037	Başarılı	0,5257	Başarılı	0,2067	Başarılı
Linear-Complexity Test	0,0552	Başarılı	0,2445	Başarılı	0,205	Başarılı
Bit Üretim Hızı / Başarı Oranı	12 kb/sn	10/10	-	1/10	-	0/10

Tablo 7.2.'de görüldüğü gibi kaotik osilatörlerin X ve Y çıkışları XOR işlemine tabi tutularak tasarlanan 10 adet GRSÜ'nün sadece 1 tanesi testlerin tamamından başarılı olmuştur. XZ ve YZ çıkışları XOR işlemine tabi tutularak tasarlanan onar adet GRSÜ'lerin hepsi istatistiksel testin tamamından başarısız olmuştur.

Tablo 7.2. Rucklidge kaotik sistemi XY, YZ, XZ kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları

Rucklidge Sistemi	X \oplus Y		X \oplus Z		Y \oplus Z	
	P-değeri	Sonuç	P-değeri	Sonuç	P-değeri	Sonuç
Frequency (Monobit) Test	0,4939	Başarılı	0,0282	Başarılı	0,2509	Başarılı
Block-Frequency Test	0,496	Başarılı	0,6468	Başarılı	0,5272	Başarılı
Cumulative-Sums Test	0,5832	Başarılı	0,0415	Başarılı	0,3146	Başarılı
Runs Test	0,5349	Başarılı		Başarısız		Başarısız
Longest-Run Test	0,3899	Başarılı	0,4052	Başarılı	0,4363	Başarılı
Binary Matrix Rank Test	0,7946	Başarılı	0,6699	Başarılı	0,3951	Başarılı
Discrete Fourier Transform Test	0,6529	Başarılı	0,5945	Başarılı	0,7972	Başarılı
Non-Overlapping Templates Test	0,8315	Başarılı	0,3702	Başarılı	0,3771	Başarılı
Overlapping Templates Test	0,4432	Başarılı	0,3506	Başarılı		Başarısız
Maurer's Universal Statistical Test	0,886	Başarılı	0,5119	Başarılı	0,9441	Başarılı
Approximate Entropy Test	0,8585	Başarılı	0,1651	Başarılı	0,0274	Başarılı
Random-Excursions Test		Başarısız		Başarısız		Başarısız
Random-Excursions Variant Test		Başarısız		Başarısız		Başarısız
Serial Test-1	0,0589	Başarılı	0,7102	Başarılı	0,8096	Başarılı
Serial Test-2	0,0701	Başarılı	0,4718	Başarılı	0,8034	Başarılı
Linear-Complexity Test	0,7955	Başarılı	0,3811	Başarılı	0,2728	Başarılı
Bit Üretim Hızı / Başarı Oranı	-	1/10	-	0/10	-	0/10

7.2. Chen Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçekleşmesi

GRSÜ için kaynak olarak kullanılan diğer kaotik sistem, Chen kaotik sistemidir. KDDS ile kurulan Chen kaotik sisteminin X, Y, Z sinyal çıkışları ADC ölçümü için 0-5V seviyesine uygunlaştırılmıştır. Daha sonra sistem, gerekli bağlantılar yapılarak rasgele bit üretme deneylerine hazır hale getirilmiştir. Yapılan deneylerde her seferinde 1.000.000 bit rasgele bit üretilmiş ve üretilen rasgele bitler NIST800-22 testlerine tabi tutulmuştur.

Gerçekleştirilen deneyler sonunda, Chen kaotik osilatörün X, Y, Z, XY, YZ, XZ bütün çıkışları için 1 mikro saniye örnekleme zamanı, 10. Bit (LSB) ADC örnekleme biti ve Von Neumann son işlem algoritması parametreleri ile 1.000.000 gerçek rasgele bit 10 kez üretilmiş ve üretilen rasgele bitler NIST800-22 testine tabi tutulmuştur. En son üretilen rasgele bitlerin NIST800-22 test sonuçları Tablo 7.3. ve Tablo 7.4.'te gösterilmiştir. Tablo 7.3. ve Tablo 7.4.'te görüldüğü gibi Chen kaotik osilatörün bütün çıkışları GRSÜ için kaynak olarak kullanıldığında, üretilen 10 farklı rasgele sayı dizisinin tamamı, NIST800-22 testlerinin tamamından başarılı olmuştur. Von

Neumann son işlem algoritması kullanıldığı için rasgele bit üretim hızı sabit değildir. Ortalama rasgele bit üretim hızı 24 kb/sn dir.

Tablo 7.3. Chen kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları

Chen Sistemi	X		Y		Z	
	P-değeri	Sonuç	P-değeri	Sonuç	P-değeri	Sonuç
Frequency (Monobit) Test	0,5431	Başarılı	0,4814	Başarılı	0,8018	Başarılı
Block-Frequency Test	0,2121	Başarılı	0,378	Başarılı	0,1165	Başarılı
Cumulative-Sums Test	0,9313	Başarılı	0,5815	Başarılı	0,9925	Başarılı
Runs Test	0,0425	Başarılı	0,5218	Başarılı	0,0584	Başarılı
Longest-Run Test	0,3058	Başarılı	0,6003	Başarılı	0,9469	Başarılı
Binary Matrix Rank Test	0,8191	Başarılı	0,1581	Başarılı	0,1653	Başarılı
Discrete Fourier Transform Test	0,2257	Başarılı	0,1062	Başarılı	0,9634	Başarılı
Non-Overlapping Templates Test	0,7506	Başarılı	0,4137	Başarılı	0,1975	Başarılı
Overlapping Templates Test	0,8853	Başarılı	0,5142	Başarılı	0,1974	Başarılı
Maurer's Universal Statistical Test	0,7903	Başarılı	0,3798	Başarılı	0,2913	Başarılı
Approximate Entropy Test	0,3763	Başarılı	0,0901	Başarılı	0,111	Başarılı
Random-Excursions Test	0,903	Başarılı	0,3308	Başarılı	0,2438	Başarılı
Random-Excursions Variant Test	0,3549	Başarılı	0,6983	Başarılı	0,2094	Başarılı
Serial Test-1	0,2679	Başarılı	0,5863	Başarılı	0,7798	Başarılı
Serial Test-2	0,128	Başarılı	0,2498	Başarılı	0,9596	Başarılı
Linear-Complexity Test	0,6767	Başarılı	0,1332	Başarılı	0,0859	Başarılı
Bit Üretim Hızı / Başarı Oranı	25 kb/sn	10/10	24 kb/sn	10/10	22 kb/sn	10/10

Tablo 7.4. Chen kaotik sistemi XY, YZ, XZ kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları

Chen Sistemi	X \oplus Y		X \oplus Z		Y \oplus Z	
	P-değeri	Sonuç	P-değeri	Sonuç	P-değeri	Sonuç
Frequency (Monobit) Test	0,4425	Başarılı	0,469	Başarılı	0,8477	Başarılı
Block-Frequency Test	0,2107	Başarılı	0,9255	Başarılı	0,6534	Başarılı
Cumulative-Sums Test	0,3815	Başarılı	0,611	Başarılı	0,7994	Başarılı
Runs Test	0,1655	Başarılı	0,0133	Başarılı	0,4318	Başarılı
Longest-Run Test	0,944	Başarılı	0,6901	Başarılı	0,1919	Başarılı
Binary Matrix Rank Test	0,967	Başarılı	0,5398	Başarılı	0,7392	Başarılı
Discrete Fourier Transform Test	0,7273	Başarılı	0,8185	Başarılı	0,3399	Başarılı
Non-Overlapping Templates Test	0,988	Başarılı	0,0567	Başarılı	0,7665	Başarılı
Overlapping Templates Test	0,7202	Başarılı	0,8639	Başarılı	0,7917	Başarılı
Maurer's Universal Statistical Test	0,281	Başarılı	0,0125	Başarılı	0,1741	Başarılı
Approximate Entropy Test	0,5501	Başarılı	0,2707	Başarılı	0,2715	Başarılı
Random-Excursions Test	0,8294	Başarılı	0,7954	Başarılı	0,7546	Başarılı
Random-Excursions Variant Test	0,847	Başarılı	0,4939	Başarılı	0,8835	Başarılı
Serial Test-1	0,3213	Başarılı	0,4443	Başarılı	0,0516	Başarılı
Serial Test-2	0,3738	Başarılı	0,1034	Başarılı	0,1075	Başarılı
Linear-Complexity Test	0,2819	Başarılı	0,63	Başarılı	0,1861	Başarılı
Bit Üretim Hızı / Başarı Oranı	26 kb/sn	10/10	22 kb/sn	10/10	23 kb/sn	10/10

7.3. Zhongtang Kaotik Sistemi Tabanlı GRSÜ Tasarım ve Gerçekleşmesi

Son olarak, GRSÜ için kaynak olarak Zhongtang kaotik sistemi kullanılmıştır. Kaotik deney seti üzerinde kurulan Zhongtang kaotik sisteminin X, Y, Z sinyal çıkışları ADC ölçümü için 0-5V seviyesine uygunlaştırılmıştır. Daha sonra sistem, gerekli bağlantılar yapılarak rasgele bit üretme deneylerine hazır hale getirilmiştir. Yapılan deneylerde, her seferinde 1.000.000 bit rasgele bit üretilmiş ve üretilen rasgele bitler NIST800-22 testlerine tabi tutulmuştur. Gerçekleştirilen deneyler sonunda, Zhongtang kaotik osilatörün X, Y, Z, XY, YZ, XZ bütün çıkışları için 1 mikro saniye örnekleme zamanı, 10. Bit (LSB) ADC örnekleme biti ve Von Neumann son işlem algoritması parametreleri ile 1.000.000 gerçek rasgele bit 10 kez üretilmiş ve üretilen rasgele bitler NIST800-22 testine tabi tutulmuştur. En son üretilen rasgele bitlerin NIST800-22 test sonuçları Tablo 7.5. ve Tablo 7.6.'da gösterilmiştir. Tablo 7.5. ve Tablo 7.6.'da görüldüğü gibi Zhongtang kaotik osilatörün bütün çıkışları GRSÜ için kaynak olarak kullanıldığında, üretilen 10 farklı rasgele sayı dizisinin tamamı NIST800-22 testlerinin tamamından başarılı olmuştur. Von Neumann son işlem algoritması kullanıldığı için rasgele bit üretim hızı sabit değildir. Ortalama rasgele bit üretim hızı 50 kb/sn dir.

Tablo 7.5. Zhongtang kaotik sistemi X, Y, Z kaynaklı GRSÜ'lerin NIST 800-22 test sonuçları

Zhongtang Sistemi	X		Y		Z	
	P-değeri	Sonuç	P-değeri	Sonuç	P-değeri	Sonuç
Frequency (Monobit) Test	0,876	Başarılı	0,0652	Başarılı	0,1325	Başarılı
Block-Frequency Test	0,2479	Başarılı	0,116	Başarılı	0,821	Başarılı
Cumulative-Sums Test	0,7673	Başarılı	0,0823	Başarılı	0,1918	Başarılı
Runs Test	0,261	Başarılı	0,2242	Başarılı	0,8292	Başarılı
Longest-Run Test	0,0877	Başarılı	0,5386	Başarılı	0,8752	Başarılı
Binary Matrix Rank Test	0,6091	Başarılı	0,7622	Başarılı	0,2606	Başarılı
Discrete Fourier Transform Test	0,5088	Başarılı	0,3084	Başarılı	0,0126	Başarılı
Non-Overlapping Templates Test	0,9846	Başarılı	0,6136	Başarılı	0,8037	Başarılı
Overlapping Templates Test	0,2601	Başarılı	0,7477	Başarılı	0,8837	Başarılı
Maurer's Universal Statistical Test	0,6839	Başarılı	0,0565	Başarılı	0,5993	Başarılı
Approximate Entropy Test	0,3774	Başarılı	0,4431	Başarılı	0,3108	Başarılı
Random-Excursions Test	0,7527	Başarılı	0,7212	Başarılı	0,8133	Başarılı
Random-Excursions Variant Test	0,9239	Başarılı	0,8595	Başarılı	0,9418	Başarılı
Serial Test-1	0,9641	Başarılı	0,4583	Başarılı	0,0309	Başarılı
Serial Test-2	0,9564	Başarılı	0,2149	Başarılı	0,1156	Başarılı
Linear-Complexity Test	0,8377	Başarılı	0,1921	Başarılı	0,8175	Başarılı
Bit Üretim Hızı / Başarı Oranı	46 kb/sn	10/10	50 kb/sn	10/10	52 kb/sn	10/10

Tablo 7.6. Zhongtang kaotik sistemi XY, YZ, XZ kaynaklı GRSÚ'lerin NIST 800-22 test sonuçları

Zhongtang Sistemi	X \oplus Y		X \oplus Z		Y \oplus Z	
	P-deđeri	Sonuç	P-deđeri	Sonuç	P-deđeri	Sonuç
Frequency (Monobit) Test	0,1169	Başarılı	0,6759	Başarılı	0,3821	Başarılı
Block-Frequency Test	0,8434	Başarılı	0,5102	Başarılı	0,311	Başarılı
Cumulative-Sums Test	0,2296	Başarılı	0,545	Başarılı	0,4079	Başarılı
Runs Test	0,2315	Başarılı	0,7458	Başarılı	0,8613	Başarılı
Longest-Run Test	0,3974	Başarılı	0,1382	Başarılı	0,6539	Başarılı
Binary Matrix Rank Test	0,8824	Başarılı	0,3395	Başarılı	0,5513	Başarılı
Discrete Fourier Transform Test	0,3588	Başarılı	0,4408	Başarılı	0,8185	Başarılı
Non-Overlapping Templates Test	0,4852	Başarılı	0,453	Başarılı	0,0224	Başarılı
Overlapping Templates Test	0,7502	Başarılı	0,352	Başarılı	0,4898	Başarılı
Maurer's Universal Statistical Test	0,2907	Başarılı	0,0697	Başarılı	0,0463	Başarılı
Approximate Entropy Test	0,3548	Başarılı	0,2841	Başarılı	0,824	Başarılı
Random-Excursions Test	0,8534	Başarılı	0,1569	Başarılı	0,7559	Başarılı
Random-Excursions Variant Test	0,9565	Başarılı	0,8589	Başarılı	0,8231	Başarılı
Serial Test-1	0,5019	Başarılı	0,3252	Başarılı	0,9941	Başarılı
Serial Test-2	0,3929	Başarılı	0,1739	Başarılı	0,9405	Başarılı
Linear-Complexity Test	0,3965	Başarılı	0,7479	Başarılı	0,8335	Başarılı
Bit Üretim Hızı / Başarı Oranı	50 kb/sn	10/10	51 kb/sn	10/10	53 kb/sn	10/10

BÖLÜM 8.SONUÇLAR VE ÖNERİLER

Sunulan tez çalışmasının birinci aşamasında ilk olarak; GRSÜ tasarımları için entropi kaynağı olarak kullanılan sürekli zamanlı Rucklidge, Chen, Zhongtang referans kaotik sistemlerinin zaman serisi, faz portresi analizleri yapılmış, Lyapunov üstelleri spektrumu ve çatallaşma gibi dinamik analizleri sunulmuştur.

İkinci olarak; referans sistemler, direnç, kondansatör, opamp ve çarpma entegresi gibi analog elektronik elemanlar kullanılarak modellenmiştir. Modellenen referans sistemlerin OrCAD-PSpice programında devreleri kurularak zaman serisi ve faz portrelerine ait simülasyon sonuçları elde edilmiştir (Şekil 5.2., Şekil 5.3., Şekil 5.7., Şekil 5.8., Şekil 5.12., Şekil 5.13.).

Üçüncü olarak; sürekli zamanlı kaotik sistemlerin karmaşık ve uzun zaman alan devre gerçeklemeleri işlemlerinin kolay, hızlı ve esnek bir şekilde yapılabilmesi için bilgisayar ve mikro denetleyici kontrollü kaotik devre deney seti (KDDS) tasarımı ve gerçekleştirilmesi yapılmıştır (Şekil 4.12., Şekil 4.13.). Kaotik sistemlerin elektronik gerçekleştirilmesinde başlangıç şartı uygulanması sistemin yapısı ve yapılan uygulama gereği zorunlu olabilmektedir. Fakat araştırmacıların kullanabileceği bir başlangıç şartı devresi yapmanın zorluğundan dolayı yapılan bilimsel çalışmalar matematiksel analizler ve bilgisayar simülasyonları ile sınırlı kalmaktadır. Geliştirilen deney setinin tasarım aşamasında, özellikle fizik ve matematik gibi alanlarda çalışan ve elektronik altyapısı eksik olan araştırmacıların rahatlıkla kullanabilmesi dikkate alınmıştır.

Birinci aşamada son olarak; referans alınan kaotik sistemlerin, geliştirilen KDDS ile gerçek devreleri kurularak, elde edilen osiloskop görüntüleri sistemlere ait Matlab, OrCAD-PSpice çıktıları ile karşılaştırılmıştır (Şekil 5.4., Şekil 5.9., Şekil 5.14.). Gerçek devre osiloskop çıktıları, elektronik devre simülasyon sonuçları ve Matlab

sayısal simülasyon sonuçlarının birbiriyle örtüştüğü ve geliştirilen KDDS'nin sağlıklı bir şekilde çalıştığı görülmüştür.

Tezin ikinci aşamasında; ADC tabanlı olarak yapılacak olan GRSÜ tasarımlarında kullanılacak, bilgisayar ve mikro denetleyici kontrollü yeni bir platform (BMKP) geliştirilmiştir. Bu sistemin özgün yönleri; kaotik sistemlerin yanında sıcaklık, RF, elektronik devre elemanı gürültüsü, güneş ışınmaları gibi farklı kaynakları da entropi kaynağı olarak kullanabilmesi, farklı entropi kaynaklarını karıştırarak kullanabilmesi, farklı son işlem algoritmalarının seçilebilmesi, istenilen uzunlukta rasgele sayı dizilerinin oluşturulabilmesi olarak sıralanabilir.

Bu yeni sistemi oluşturmak için;

İlk olarak; entropi kaynağından gelen, genlik ve polaritesi ADC ölçümü için uygun olmayan sinyalleri “0-5V Seviyesine Uygunlaştıran bir Devre” (Şekil 6.6.),

İkinci olarak; entropi kaynağından elde edilen analog sinyalleri ikili sayı dizilerine dönüştüren ve bu verileri yorumlayıp belirli bir formatta USB üzerinden bilgisayar programına gönderen “Mikro Denetleyici Kontrollü Veri Toplama Kartı” (Şekil 6.8.),

Üçüncü olarak; rasgele sayı üretimi yapılmadan önce, mikro denetleyicinin parametre ayarlarının yapılabilmesi ve rasgele sayıların özel bir formatta “txt” dosyasına dönüştürülmesi için veri toplama kartı ile USB üzerinden haberleşen C Sharp programlama dili ile yazılan bir “Bilgisayar Programı” (Şekil 6.10.) olmak üzere 3 farklı tasarım ve gerçekleştirilmiştir.

Tezin son aşamasında, gerçekleştirilen KDDS VE BMKP kullanılarak, Rucklidge, Chen ve Zhongtang kaotik sistemleri tabanlı yeni GRSÜ tasarım ve gerçeklemeleri yapılmıştır. Kaotik osilatör sinyallerinin rasgelelik özelliği yanında, daha yüksek genlik değerlerine sahip olması ve diğer gürültü kaynaklarına göre çevresel koşullardan daha az etkilenmelerinden dolayı GRSÜ'ler için entropi kaynağı olarak kullanımı yaygınlaşmaktadır.

Rucklidge, Chen ve Zhongtang kaotik sistemlerinin her birisine ait x, y, z çıkışları önce tek tek ele alınarak, daha sonra ikili x-y, x-z, y-z çıkışları XOR işlemi uygulanarak entropi kaynağı olarak kullanılmıştır. Böylece, her bir kaotik sistemden altı adet olmak üzere toplam 18 farklı entropi kaynağı ile GRSÜ gerçekleştirilmiştir. GRSÜ'lerin güvenilirliğini arttırmak için; 18 farklı GRSÜ'nün her birisinden 10 kez olmak üzere toplam 180 adet, her biri 1 milyon bitlik sayı dizisi üretilmiştir. GRSÜ'lerinden elde edilen 1 milyon bitlik sayı dizileri veri toplama kartı kullanılarak, USB üzerinden bilgisayar programına aktarılmış ve bir dosyaya kaydedilmiştir. Dosyalara kaydedilen 180 adet sayı dizisi, uluslararası en üst düzey standart olan NIST800-22 rasgelelik testlerine tabi tutulmuştur. GRSÜ'lerden en son üretilen rasgele sayı dizilerinin NIST 800-22 test sonuçları, her bir çıkışın test başarı oranları ve rasgele bit üretim hızları tablolar halinde gösterilmiştir (Tablo 7.1.- Tablo 7.6.).

Rucklidge kaotik sistemi entropi kaynağı olarak kullanıldığında, sadece sistemin X çıkışına ait sayı dizisi NIST 800-22 rasgelelik testlerinin tamamından başarılı olmuştur (Tablo 7.1.). Sistemin diğer çıkışlarına ait sayı dizileri, testlerden başarısız olmuştur.

Chen ve Zhongtang kaotik sistemleri entropi kaynağı olarak kullanıldığında, üretilen GRSÜ'lerin tüm çıkışları rasgelelik testlerinden başarı ile geçmiştir. Zhongtang kaotik sistemi entropi kaynağı olarak kullanıldığında, aynı seçim parametre değerlerinde (örnekleme zamanı, son işlem algoritması vb.), Chen kaotik sistemine göre iki kat daha hızlı rasgele sayı ürettiği görülmüştür (Tablo 7.3.-Tablo 7.6.).

Test sonuçları incelendiğinde (Tablo 7.1.-Tablo 7.6.), tasarım seçim parametrelerinin farklı entropi kaynakları için farklılık gösterdiği görülmüştür. ADC kaynak girişlerinin XOR işlemine tabi tutulup karıştırılmasının, rasgele bitlerin testlerden başarılı olmasına ve bit üretim hızına olumlu katkı yaptığı görülmüştür. GRSÜ'den üretilen ikili sayı dizilerine uygulanan son işlem algoritmalarının, ikili dizilerin rasgelelik testlerinden geçmesine olumlu yönde katkı yaptığı, fakat bit üretim hızını düşürdüğü gözlemlenmiştir. Chen ve Zhongtang kaotik sisteminin tüm çıkışlarının entropi kaynağı olarak kullanıldığı GRSÜ'lerden üretilen rasgele sayı dizilerine, XOR işlemi uygulandığında rasgelelik testlerinden geçemediği, Von Neumann son işlem

algoritması uygulandığında ise tüm testlerden başarılı olduğu görülmüştür. Fakat Von Neumann algoritması uygulandığında bit üretim hızı XOR işlemine göre 4 kat düşmektedir. Bunun yanında, XOR işlemi son işlem algoritması olarak seçildiğinde bit üretim hızı sabit, Von Neumann algoritmasında ise değişkendir. Geliştirilen GRSÜ'ler incelendiğinde, kullanılan entropi kaynağının frekansı spektrum aralığı arttıkça ve kullanılan ADC'nin çözünürlüğü arttıkça rasgele bit üretme hızının ve başarı oranının arttığı gözlemlenmiştir.

Yapılan çalışmada, ADC olarak, örneklemede kullanılan mikrodenetleyicinin dahili ADC'si kullanılmıştır. Kullanılan ADC'nin 10 bit çözünürlükte olması, kaotik osilatörlerin frekans spektrum aralıklarının düşük olması ve son işlem algoritma ihtiyacından dolayı, bit üretim hızı ortalama 50 kb/sn seviyelerindedir (Tablo 7.5., Tablo 7.6.). Literatürdeki FPGA ile gerçekleştirilen RSÜ'ler ile karşılaştırıldığında bit üretim hızları düşük gibi görülebilir. Fakat FPGA içerisine programal olarak gömülen kaotik sistemlerin zaman sinyalleri Matlab programında olduğu gibi, Runga-Kutta 4 benzeri, bir sayısal analiz yöntemi ile hesaplatılmakta ve her defasında aynı başlangıç şart değerlerinde aynı rasgele ikili sayı dizileri elde edilmektedir. Bu sebeplerden dolayı; sayısal hesaplama teknikleri ile algoritmik olarak işlem yapan FPGA gibi donanımsal yapılar ile gerçekleştirilen kaos tabanlı RSÜ'lerin "Gerçek" bir "Rasgele Sayı Üretici" olduğu noktasında çok ciddi tereddütler vardır. Buna karşılık tezde geliştirilen GRSÜ'leri üreten sistem, ADC tabanlı gerçek elektronik donanımsal bir yapıda olduğundan, her seferinde aynı başlangıç şartı değerlerinde çalıştırılrsa bile, hiçbir şekilde kendini tekrar etmeyen "Gerçek" rasgele ikili sayı dizileri üretecektir. Dolayısıyla FPGA tabanlı RSÜ'lerin hızlarını kendi kategorisine daha uygun olan Sözcük RSÜ'ler ile karşılaştırmak daha doğru olacaktır.

İlerideki çalışmalarda, geliştirilen BMKP ile daha yüksek frekans spektrum aralıklı kaotik osilatörler araştırılıp seçilerek ve çözünürlüğü daha yüksek harici ADC entegreleri kullanılarak bit üretim hızları yükseltilebilir. Ayrıca, eş zamansız olarak yapılan NIST800-22 testleri bilgisayar programına gömülerek testlerin eş zamanlı olarak yapılması sağlanabilir.

Geliştirilen Zhongtang ve Chen kaotik sistemi tabanlı GRSÜ'ler kriptolojik uygulamalar, haberleşme, savunma sanayi, tıp, endüstriyel sistemler gibi rasgele sayı dizilerinin gerekli olduğu yerlerde güvenle kullanılabilir.

Yeni kaotik devre deney seti ve GRSÜ tasarımları için geliştirilen yeni bilgisayar ve mikro denetleyici kontrollü platform, başta Sakarya Üniversitesi olmak üzere ülkemizdeki lisansüstü eğitim programlarının kaos teorisi ile ilgili derslerinde kullanılarak eğitim kalitesini artırması hedeflenmektedir.

KAYNAKLAR

- [1] Menezes, A.J., Paul, C., Van, O., Scott, A.V., Handbook of applied cryptography. CRC press, 1996.
- [2] Koç, C.K., Cryptographic Engineering, Springer,2009.
- [3] Zhao, L., Liao, X., Xiao, D., Xiang, T., Zhou, Q., Duan, S., TRNG from mobile telephone photo based on chaotic cryptography. Chaos, Solitons & Fract., Elsevier, 42(3), 1692–1699, 2009.
- [4] Kriptografiye giriş ders notları. Uygulamalı Matematik Enstitüsü Kript. Böl., ODTÜ, 2004.
- [5] Hellman, M.E., An overview of public key cryptography. IEEE Communications Magazine, 16(6), 42-49, 2002.
- [6] Ergün, S., Özoğuz, S., TRNGs based on a non-autonomous chaotic oscillator. Int. J. of Electronics and Comm., 61(4), 235–242, 2007.
- [7] Angulo, JAA., Kussenar, E., Barthelemy, H., Duval, B., A new oscillator-based RNG. IEEE Faible Tension Faible Cons., 1–4, June 2012.
- [8] Kocarev L., Jakimoski G., 2003. Pseudorandom Bits Generated by Chaotic Maps, IEEE Trans. Circuits and Systems I, 50, 123-126, 2003.
- [9] Avaroğlu, E., Türk, M., Son işlemin gerçek rasgele sayı üreticileri üzerindeki etkisinin incelenmesi. 6th International Information Security and Cryptology Conference, ISCTURKEY, 290-294, 2013.
- [10] Merah, L., Ali, A., Said, N., Mamat, M., A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation, Applied Mathematical Sciences, 7(55), 2719-2734, 2013.
- [11] Zeng, K., Yang, C., Wei, D., Pseudo-Random Bit Generators in Stream-Cipher Cryptography. Rao University of Southwestern Louisiana, 1991.

- [12] Callegari, S., Rovatti, R., Setti, G., Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos. *IEEE Trans. Signal Process.*, 53, 793-805, 2005.
- [13] Bucci, M., Germani, L., Luzzi, R., Tommasino, P., Trifiletti, A., Varanonuovo, M., A high-speed IC random-number source for smart card microcontrollers. *IEEE Trans. on Circuits and Sys.I: Fundamental Theory and Appl.*, 50(11), 1373–1380, 2003.
- [14] Sobotka, J., Zeman, V., Design of the true random numbers generator. *Elektrorevue*, 2(3), 1-6, 2011.
- [15] Murphy, J.P., Field-programmable true random number generator. *Electronics Letters*, 48(10), 565-566, 2012.
- [16] Wang, L., Meilin, W., Kui, D., Xuecheng, Z., Scalable Truly Random Number Generator. *Proceedings of the World Congress on Engineering*, 1, 2015.
- [17] Yalçın, M., Suyken, J., Vandewalle, J., True random bit generation from a double scroll sstractor. *IEEE Trans. Circuits Syst.*, 51, 1395-1404, 2004.
- [18] Yıldırım, S., Bazlaccı, C., A true random number generator and test platform built in FPGA. *International Information Security and Cryptology Conference, ISCTURKEY 2012*, 262-267, 2012.
- [19] Addison, P.S., *Fractals and Chaos. An illustrated course.* IOP Publishing Limited, 5-7, 1997.
- [20] Hilborn, R.C., *Chaos and Nonlinear Dynamics. An Introduction for Scientists and Engineers.* Oxford University Press, 1994.
- [21] Pehlivan, I., *Yeni kaotik sistemler: Elektronik devre gerçeklemeleri, Senkronizasyon ve Güvenli haberleşme uygulamaları.* Doktora Tezi, Sakarya Üniversitesi, 2007.
- [22] Stojanovski, T., Kocarev, L., Chaos-based random number generators-part I: analysis. *IEEE Trans. on Circuits and Syst. I: Fundamental Theory and Appl.*, 48(3), 281–288, 2001.
- [23] Danger, JL., Guilley, S., Hoogvorst, P., High speed true random number generator based on open loop structures in FPGAs. *Microelectronics J., Elsevier*, 40(11), 1650–1656, 2009.
- [24] Lozach, F., Ben, RM., Graba, T., Danger, JL., FPGA design of an open-loop TRNG. *Euromicro Conf. on Digital Sys. Design*, 615–622, 2013.

- [25] Wieczorek, PZ., Golofit, K., Dual-metastability time-competitive TRNG. *IEEE Trans. on Circuits and Syst.*, 61(1), 134–145, 2014.
- [26] Fischer, V., Drutavosky, M., Simka, M., Bochar, N., High performance TRNG in altera stratix FPLDs. *Field Programmable Logic and App.*, Springer, 3203, 555–564, 2004.
- [27] Ergün, S., Özoğuz, S., Truly RNGs based on non-autonomous continuous-time chaos. *Int. J. of Circuit Theory and App.*, 38(1), 1–24, 2010.
- [28] Özoğuz, S., Zeki, A., Sürekli zamanlı kaotik sistemlerin tümleşik olarak gerçekleştirilmesi ve rasgele sayı üretiminde kullanılması. *Tübitak Projesi Sonuç Raporu (106E093)*, 2008.
- [29] Pareschi, F., Setti, G., Rovatti, R., Implementation and testing of high-speed CMOS TRNGs sased on chaotic systems. *IEEE Trans. On Circuits and Sys.*, 57(12), 3124–3137, 2010.
- [30] Tavas, V., Tümleştirmeye uygun rasgele sayı üreteçleri, *Doktora Tezi, İstanbul Teknik Üniversitesi*, 2011.
- [31] Drutavosky, M., Galajda, P., Chaos based true random number generator embedded in a mixed-signal reconfigurable hardware, *Journal of ELECTRICAL ENGINEERING*, 57(4), 218–225, 2006.
- [32] Zhang, Y., Wang, Y., Liu, M., Xue, L., Li, P., Wang, A., Zhang, M., A robust random number generator based on differential comparison of chaotic laser signals. *OPTICS EXPRESS*, 20(7), 2012.
- [33] Fabbri, M., Callegari, S., Very low cost entropy source based on chaotic dynamics retrofittable on networked devices to prevent RNG attacks. *IEEE 21th International Conference on Electronics*, 175–178, 2014.
- [34] Akram, R., Konstantinos, M., Keith, M., Pseudorandom number generation in smart cards: an implementation, performance and randomness analysis. *2012 5th International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, 1-7, 2012.
- [35] Başlıgil, H., Rasgele sayı üretimi ders notları. *Endüstri Mühendisliği Bölümü, Yıldız Teknik Üniversitesi*, 2011.
- [36] Payne, W., Rabung, J., Bogyo, T, Coding the Lehmer pseudo random number generator. *Communications of the ACM*, 12(2), 86-86, 1969.

- [37] Petrie, CS., Connelly, JA., A noise-based IC RNG for applications in cryptography. *IEEE Trans. on Circuits and Syst. I: Fundamental Theory and Appl.*, 47(5), 615–621, 2000.
- [38] Wang, Z.L., Shi, X.R., Chaotic bursting lag synchronization of Hindmarsh-Rose system via a single controller. *Applied Mathematics and Computation*, 215(3), pp:1091-1097, 2009.
- [39] Von Neumann, J., Various techniques used in connection with random digits, *Applied Math Series, Notes by G. E. Forsythe*, in *National Bureau of Standards*, 12, 6-38, 1951.
- [40] Dichtl, M., Bad and good ways of post-processing biased physical random numbers. *Fast Software Encryption Lecture Notes in Computer Science*, 4593, 137-152, 2007.
- [41] Sunar, B., Martin, W.J., Stinson, D.R., A provably secure true random generator with built-in tolerance to active attacks. *IEEE Transaction on Computers*, 56(1), 2007.
- [42] Demirkol, A., Kaotik osilatör girişli ADC tabanlı rasgele sayı üretici. Yüksek lisans tezi, İstanbul Teknik Üniversitesi, 2007.
- [43] Koyuncu, İ., Kriptolojik uygulamalar için FPGA tabanlı yeni kaotik osilatörlerin ve gerçek rasgele sayı üreticilerinin tasarımı ve gerçekleştirilmesi. Doktora Tezi, Sakarya Üniversitesi, 2014.
- [44] Akizawa Y., Yamazaki, T., Uchida, A., Harayama, T., Sunada, S., Arai, K., Yoshimura, K., Davis, P., Fast RNG with bandwidth-enhanced chaotic semiconductor lasers at 8 times 50Gb/s. *IEEE Photonics Tech. Lett.*, 24(12), 1042–1044, 2012.
- [45] Nien, H., Huang, C., Changchien, S., Shieh, H., Chen, C., Tuan, Y., Digital color image encoding and decoding using a novel chaotic random generator. *Chaos, Solitons & Fract.*, 32(3), 1070–1080, 2007.
- [46] Suresh, V.B., Burlison, W.P., Entropy extraction in metastability-based TRNG. *Hardware-Oriented Security and Trust, 2010 IEEE International Symposium on*, 135-140, 2010.
- [47] Avaroğlu, E., Türk, M., RNG using multi-mode chaotic attractor. *IEEE Signal Processing and Comm. Appl. Conf.*, 1–4, April 2013.
- [48] Güven, P., Otonom olmayan kaotik sistemlerde rasgele sayı üretiminin incelenmesi. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, 2006.

- [49] Yılmaz, R., Kriptolojik Uygulamalarda Bazı İstatistik Testler. Yüksek Lisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü İstatistik Anabilim Dalı, 2010.
- [50] Federal information processing standards publication, Security requirements for cryptographic modules. FIPS PUB 140-1, 1994. <http://csrc.nist.gov/publications/fips/fips1401.htm>, Erişim Tarihi: 06.06.2014.
- [51] A statistical test suite for random and pseudo RNGs for cryptographic applications. National institute of stand. and tech., NIST-800-22, 2001. <http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf>, Erişim Tarihi: 07.02.2016.
- [52] Yayık, A., Kutlu, Y., Improving PNRG using artificial neural networks. IEEE 21st Signal Processing and Comm. App. Conf., pp:1-4, 2013.
- [53] Avaroğlu, E., Donanım tabanlı rasgele sayı üreticinin gerçekleştirilmesi. Doktora Tezi, Fırat Üniversitesi, 2014.
- [54] Kazan, F.A., Terzioğlu, H., Ağaayak, A.C., The design of a test & development board for the training of PIC18F4550 microcontroller, 2nd International Conference on Information Science and Control Engineering, 951-955, 2015.
- [55] Coşkun, S., Mikrodenetleyici tabanlı sesli bilgilendirme sistemi OTOGÖZ, Yüksek Lisans Tezi, Marmara Üniversitesi, 2008.
- [56] Kiremitçi, A.F., PIC18F4550 mikrodenetleyicisi ile USB-PC veri aktarım arabirimi gerçekleştirilmesi. Yüksek Lisans Tezi, Atatürk Üniversitesi, 2007.
- [57] Akgül, A., Yeni kaotik sistemler ile rasgele sayı üretici tasarımı ve çoklu-ortam verilerinin yüksek güvenli şifrelenmesi. Doktora Tezi, Sakarya Üniversitesi, 2015.
- [58] Özdemir, K., Sürekli zamanlı kaos ile rasgele sayı üretici tasarımı, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, 2008.
- [59] Pareek, N.K., Patidar, V., Sud, K.K., Image encryption using chaotic logistic map. Image and Vision Computing, 24(9), 926-934, 2006.
- [60] Udawadia, F.E., Guttalu, R.S., Chaotic Dynamics of a piecewise cubic map. The American Physical Society, 40(7), 4032-4044, 1989.

- [61] Saha, B., Malasani, S.T., Seventline, J.B., Application of modified chaotic Sine Map in secure communication. *International Journal of Computer Applications*, 113(13), 9-13, 2015.
- [62] Vladi, A., Luca, A., Hodea, O., Tataaru, R., Generating chaotic secure sequence using tent map and running-key approach. *The Publishing House of The Romanian Academy*, 14, 295-302, 2013.
- [63] Vajargah, B.F., Asghari, R., A pseudo random number generator based on chaotic henon map (CHCG). *International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)*, 5(15), 2120-2129, 2015.
- [64] Aziz Alaoui, M.A., Robert, K., Grebogi, C., Dynamics of a Henon-Lozi-type map. *Pergamon Chaos Solitons and Fractals*, 12, 2323-2341, 2001.
- [65] Senkerik, R., Zelinka, I., Pluhacek, M., Oplatkova, Z.K., Evolutionary control of chaotic burgers map by means of chaos enhanced differential evolution. *International Journal of Mathematics and Computers in Simulation*, 8, 39-45, 2014.
- [66] Sohel Rana, SM., Chaotic dynamics in a discrete-time predator-prey food chain. *Computational Ecology and Software*, 5(1), 28-47, 2015.
- [67] Mishra, M., Routray, A.R., Kumar, S., High security image steganography with modified Arnold's cat map. *International Journal of Computer Applications*, 37(9), 16-20, 2012.
- [68] Butcher, J.C., *Numerical methods for ordinary differential equations*. John Wiley & Sons, 2008.
- [69] Zhang, W., Gui, Z., Wang, K., Impulsive control for synchronization of Lorenz chaotic system. *Journal of Software Engineering and Applications*, 5(12), 23-25, 2013.
- [70] Precup, R.E., Tomescu, M.L., Dragos, C.A., Stabilization of Rössler chaotic dynamical system using fuzzy logic control algorithm. *International Journal of General Systems*, 43(5), 413-433, 2014.
- [71] Sheu, L.J., Chen, H.K., Chen, J.H., Tam, L.M., Chaotic dynamics of the fractionally damped Duffing equation. *Chaos, Solitons & Fractals*, 32, 1459-1468, 2007.
- [72] Kuetche, M., Fotsin, E.S., Kengne, H.B., Wofo, P., Parameters estimation based adaptive GPS of chaotic Chua's circuit with application to chaos communication by parametric modulation. *Chaos, Solitons & Fract.*, Elsevier, 61, 27-37, 2014.

- [73] Sundarapandian, V., Global chaos synchronization of the forced Van der Pol chaotic oscillators via adaptive control method. *International Journal of PharmTech Research*, 8(6), 156-166, 2015.
- [74] Chen, G., Ueta, T., *Chaos in Circuits and Systems*. World Scientific Pub. Co. Singapore, 2002.
- [75] Vembarasan, V., Balasubramaniam, P., Chaotic synchronization of Rikitake system based on TS fuzzy control techniques. *Nonlinear Dynamics*, 74(1-2), 31-44, 2013.
- [76] Rucklidge, A.M., Chaos in models of double convection. *Journal of Fluid Mechanics*, 237, 209-229, 1992.
- [77] Sundarapandian, V., Global chaos synchronization of Rucklidge chaotic systems for double convection via sliding mode control. *International Journal of ChemTech Research*, 8(8), 61-72, 2015.
- [78] Sundarapandian, V., Output regulation of the Arneodo chaotic system. *International Journal on Computer Science and Engineering (IJCSSE)*, 2(5), 1601-1608, 2010.
- [79] Zhongtang, W., Wang, M., Jianxiu, J., Jiuchap, F., A Novel Strange Attractor and its Dynamic Analysis, *JOURNAL OF MULTIMEDIA*, 9(3), 408-415, 2014.
- [80] Pamuk, N., Dinamik Sistemlerde Kaotik Zaman Dizilerinin Tespiti. *BAÜ Fen Bilimleri Enstitüsü Dergisi*, 15(1), 77-91, 2013.
- [81] Özer, S., Zorlu, H., Doğrusal olmayan par sistemler kullanılarak kaotik zaman serisi kestirimi. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 27(2), 323-331, 2012.
- [82] Tapashetti, P., Gupta, A., Mithlesh, C., Umesh, AS., Design and simulation of Op Amp integrator and its applications. *International Journal of Engineering and Advanced Technology (IJEAT)*, 1(3), 12-19, 2012.
- [83] İşlemsel yükselteçler ders notları. *Elektronik Haberleşme Mühendisliği, Kocaeli Üniversitesi*, 2014.
- [84] Coşkun, S., Tuncel, S., Pehlivan, İ., Akgül, A., Microcontroller-controlled electronic circuit for fast modelling of chaotic circuits. *Electronics World*, 121(1947), 24-25, 2015.
- [85] Özkaynak, F., Cryptographically secure random number generator with chaotic additional input. *Nonlinear Dynamics*, 78, 2015-2020, 2014.

- [86] Pareshi, F., Setti, G., Rovatti, R., A fast chaos-based true random number generator for cryptographic applications. ESSCIRC 2006, Proceedings of the 32nd European Solid-State Circuits Conference, 130-133, 2006.
- [87] Cuomo K.M., Oppenheim, A.V., Circuit Implementation of Synchronized Chaos with applications to Communication. Phys. Rev. Lett., 71, 65-68, 1997.
- [88] Holman, W.T., Connelly, J.A., Dowlatabadi, A.B., An integrated analog/digital random noise source. IEEE Transactions on Circuits and Systems I: Fundemantal Theory and Applications, 44, 521-528, 1997.
- [89] Zhun, H., Hongyi, C. "A truly random number generator based on thermal noise. IEEE Proceedings: 4th International Convergence on ASIC, 862-864, 2001.

EKLER

EK A: Doktora Tez Kapsamında Yapılan Bilimsel Çalışmalar

Doktora tez kapsamında yapılan bilimsel yayınlar aşağıda verilmiştir.

- [1] COSKUN, S., TUNCEL, S., PEHLIVAN, I., AKGUL, A., Microcontroller-Controlled electronic circuit for fast modelling of chaotic equations, Electronics World, 121(1947):24–25, 2015.

ÖZGEÇMİŞ

Selçuk COŞKUN, 02.11.1981 tarihinde Sakarya'da doğdu. İlköğrenimini Sakarya'da tamamladı. 2000 yılında Sakarya Fatih Anadolu Teknik Lisesi'nden mezun oldu. 2000 yılında başladığı Marmara Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Haberleşme Öğretmenliği Bölümü'nü 2005 yılında tamamladı. 2008 yılında Marmara Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Bilgisayar Eğitimi Anabilim Dalı'ndaki yüksek lisansını bitirdi. 2008 Şubat ayında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Elektronik-Bilgisayar Eğitimi Anabilim Dalı'nda doktora eğitimine başladı. Şubat 2006 yılından beri, Sakarya İMKB Mesleki ve Teknik lisesinde Elektronik öğretmeni olarak görev yapmaktadır.