T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MİKROBİLGİSAYAR TABANLI YENİ BİR RASGELE SAYI ÜRETECİ TASARIMI VE ŞİFRELEME UYGULAMASI

YÜKSEK LİSANS TEZİ

Bilal GÜREVİN

Enstitü Anabilim Dalı : MEKATRONİK MÜHENDİSLİĞİ

Tez Danışmanı : Doç. Dr. Akif AKGÜL

Haziran 2019

T.C.
SAKARYA UYGULAMALI BİLİMLER ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

MİKROBİLGİSAYAR TABANLI YENİ BİR RASGELE SAYI ÜRETECİ TASARIMI VE ŞİFRELEME UYGULAMASI

YÜKSEK LİSANS TEZİ

Bilal GÜREVİN

Enstitü Anabilim Dalı : MEKATRONİK MÜHENDİSLİĞİ

Bu tez 13/06/2019 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

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

Bilal GÜREVİN
13.06.2019

TEŞEKKÜR

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

Laboratuvar olanakları konusunda anlayış ve yardımlarını esirgemeyen Sakarya Uygulamalı Bilimler Üniversitesi Elektrik-Elektronik Mühendisliği Bölüm Başkanı Prof. Dr. İhsan PEHLİVAN'a ve bilgi ve deneyimlerinden yararlandığım sayın hocam Doç. Dr. Sezgin KAÇAR ve elektrik-elektronik mühendisi Emre GÜLERYÜZ'e teşekkür ederim.

Ayrıca bu çalışmanın maddi açıdan desteklenmesine olanak sağlayan Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (Proje No: 117E284) teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

E_x	: x'in matematiksel beklentisi
d_1	: Sistem parametresi
d_2	: Sistem parametresi
d_3	: Sistem parametresi
$\dot{x}$	: x Türev
x_0	: Durum değişkeninin başlangıç değeri
$\dot{y}$	: y Türev
y_0	: Durum değişkeninin başlangıç değeri
$\dot{z}$	: z Türev
z_0	: Durum değişkeninin başlangıç değeri
ARM	: Advanced RISC Machine
bin	: Binary
cov	: Koveryans
D(x)	: x'in Tahmini Değeri
det	: Determinant
E	: Denge Noktası
ENT	: Pseudorandom Number Sequence Test Program
F	: Frekans
f (i)	: Farklı Bit Durumları
F[x(t)]	: Durum Değişken Fonksiyonu
FFT	: Fast Fourier Transform
FIPS	: Federal Information Processing Standard
GB	: Giga Byte
GHz	: Giga Hertz
GPIO	: General-purpose input/output
h	: Adım aralığı

H(s) : Kaynak Entropi Değeri
HDMI : Hight Definition Multimedia İnterface
Hz : Hertz
I : Birim Matris
K : Sistem parametresi
Kbit : Kilo bit
L : Sistem parametresi
Labview : Laboratuary Virtul İnstrument For Engineering Workbench
LFSR : Linear Feedback Shift Register
LSB : Least significant bit (En düşük anlamlı bit)
m : Blok Uzunluğu
M : Bit dizisinde belirli sayıdaki bitlerinden oluşan blok
Matlab : Matrix laboratory
Mbit : Megabit
MÖ. : Milattan önce
ms : Milisaniye
n : Bit Uzunluğu
NIST : National Institute of Standards and Technology
NPCR : Number Of Pixel Change Rate
ODE : Ordinary Differential Equation
Pspice : Personel Simulation Program With İntegrated Circuit Emphasis
r : Sistem parametresi
RK4 : 4. dereceden Runge-Kutta yöntemi
RSÜ : Rasgele sayı üreteci
s : LSB biti
UACI : Unified Average Changing İntensity
USB : Universal Serial Bus
X : Poker Testi Sonuç Değeri
XOR : Exclusive Or (Özel Veya)
γ : Sistem parametresi
J : Jakobian matrisi
a : Sistem parametresi

b : Sistem parametresi

c : Sistem parametresi

d : Sistem parametresi

dx : Türev operatörü

e : Sistem parametresi

f : Sistem parametresi

i : İndis

n : Bit dizisi uzunluğu

p : Probability (olasılık)

q : Türev değer emirleri (kesir derecesi)

t : Zaman veya sistem parametresi

x : Durum değişkeni

y : Durum değişkeni

z : Durum değişkeni

β : Sistem parametresi

λ : Özdeğerler veya Layapunov üsteli

σ : Sistem parametresi

τ : Sistem parametresi

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

MİKROBİLGİSAYAR TABANLI YENİ BİR RASGELE SAYI ÜRETECİ TASARIMI VE ŞİFRELEME UYGULAMASI

ÖZET

Bu tez çalışmasında doğrusal olmayan bir kaotik sistem ile mikrobilgisayar tabanlı rasgele sayı üreteci (RSÜ) tasarımı yapılarak resim şifreleme uygulaması gerçekleştirilmiştir. Üretilen sayıların rasgeleliği NIST 800-22 ve FIPS 140-1 istatistiksel testleri ile ölçülürken, şifreli resmin güvenilirliği de histogram analizi, korelasyon katsayısı, entropi katsayısı, korelasyon haritası, UACI, NPCR gibi güvenlik analizleri ile ölçülmüştür.

Tezin ilk bölümünde; kaos ve kaotik sistemler hakkında literatür taraması yapılarak günümüze kadar hangi alanlarda ne tür çalışmalar yapıldığı hakkında bilgi verilmiştir. İkinci bölümde; bir sistemin kaotik davranışlarını incelemek için yapılan dinamik analiz yöntemleri anlatılmıştır. Üçüncü bölümde; RSÜ'ler, istatistiksel rasgelelik testleri, görüntü şifreleme ve şifreli görüntünün güvenlik analizleri hakkında bilgi verilmiştir. Dördüncü bölümde; yeni kaotik sistemin Matlab programı yardımı ile zaman serileri ve faz portreleri çizdirilmiş, Lyapunov boyutu hesaplatılmış, parametre değişimine göre Lyapunov üstel spektrumu ve çatallanma diyagramı çizdirilmiş, FFT ve Poincare kesit analizleri yapılmıştır. Beşinci bölümde; Mobil RSÜ tasarımı için entropi kaynağı olarak seçilen yeni kaotik sistemden Runge Kutta-4 çözüm metodu ile Raspberry Pi 3 Model B mikrobilgisayarında Spyder arayüzünde Python dili kullanılarak rasgele sayılar elde edilmiş ve çıkan değerler NIST 800-22 ve FIPS 140-1 testlerinden başarı ile geçirilmiştir. Altıncı bölümde; testleri başarı ile geçen rasgele sayı dizileri kullanılarak bir görüntü şifreleme uygulaması gerçekleştirilmiştir. Şifrelenen görüntünün histogram analizi, korelasyon haritaları, korelasyon ve entropi katsayıları, UACI, NPCR gibi güvenlik analizleri gerçekleştirilmiştir. Tez çalışmasının son bölümünde; sonuç ve önerilere yer verilmiştir.

Anahtar kelimeler: Kaotik Sistemler, Şifreleme, Analiz, Güvenlik, Rasgele Sayı Üreteci, Raspberry Pi 3 Model B, Matlab, Spyder, Runge Kutta-4

NEW RANDOM NUMBER GENERATOR DESIGN BASED ON MICROCOMPUTER AND ENCRYPTION APPLICATION

SUMMARY

In this thesis, microcomputer based random number generator (RNG) with a non-linear chaotic system was designed and image encryption was implemented. The randomness of the generated numbers was measured by NIST 800-22 and FIPS 140-1 statistical tests and the reliability of the encrypted image was measured by histogram analysis, correlation coefficient, entropy coefficient, correlation map, UACI, NPCR.

In the first chapter of the thesis; literature on chaos and chaotic systems were searched and information were given about what kind of studies have been carried out. In the second part; dynamic analysis methods used to examine the chaotic behavior of a system were explained. In the third chapter; information were given about RNG, statistical randomness tests, image encryption and security analysis of the encrypted image. In the fourth chapter; time series and phase portraits of the new chaotic system were drawn with the help of Matlab program, Lyapunov dimension was calculated, Lyapunov exponential spectrum and bifurcation diagram was drawn according to the change of parameter, FFT and Poincare section analysis were performed. In the fifth chapter; random numbers based on the new chaotic system, which is selected as the entropy source for the mobile RNG design, were obtained by employing Runge Kutta-4 solution method and by using Spyder interface on the Raspberry Pi 3 Model B microcomputer and the resulting values were successfully passed from NIST 800-22 and FIPS 140-1 tests. In the sixth chapter; an image encryption application was performed using random number sequences that passed the tests successfully. Security analysis such as histogram analysis, correlation maps, correlation and entropy coefficients, UACI, NPCR of the encrypted image were performed. Finally, in the last part of the thesis; results and recommendations are given.

Keywords: Chaotic Systems, Encryption, Analysis, Security, Random Number Generator, Raspberry Pi 3 Model B, Matlab, Spyder, Runge Kutta-4

BÖLÜM 1. GİRİŞ

Günümüzde Endüstri 4.0'ın da hayatımıza girmesiyle beraber fiziksel nesnelerin gerek kendileri arasında gerekse diğer sistemler arasında olan iletişimi oldukça önemli bir yer edinmiştir. Ev otomasyonu sistemlerinden kredi kartlarına, endüstriden akıllı tarım sistemlerine kadar hayatın birçok alanında devamlı bir veri alışverişi gerçekleşmektedir. Sürekli olarak iletim halinde olan bu verilerin istenmeyen kişiler tarafından elde edilmesi her ne kadar önlenmeye çalışılsa da tam olarak sağlanamamaktadır. İstenilmeyen bu duruma karşı, yetkisiz kişiler tarafından elde edilen verilerin korunması önemli bir alan teşkil etmektedir. Bu hususta veri güvenliğinin sağlanması amacıyla kriptolama teknikleri geliştirilmiştir. Şifrelenecek veri dosyası kullanılan cihazlara göre ses, video, metin veya bir görüntüden oluşabilmektedir. Veriyi şifreleme ve çözme işlemi bir anahtar yardımı ile yapılır. Şifrelenmiş verinin çözülmesi ancak doğru anahtarın kullanılmasıyla mümkündür.

Şifreleme insanlık tarihinin başlarına kadar uzanmaktadır. Şifrelemenin tarihteki ilk belirgin örneği MÖ. 60-50 yıllarında Julius Caesar tarafından verilmektedir. Roma alfabesinde harflerin yerlerini belli bir metoda göre değiştirerek oluşturduğu şifreleme yöntemini devletin haberleşme ağında kullanmıştır. MÖ. 7. yy.'da ise Yunan şair Archilochus tarafından bir başka şifreleme yöntemi gerçekleştirilmiştir. Bu metoda göre belirli bir çaptaki çubuğa üzerinde harfler bulunan bir bez sarılmakta ve böylece yan yana gelen harfler anlamlı kelimeler oluşturmaktadır. Çubuğun çapı şifrenin anahtarı vazifesini görmektedir. Şifrelemede asıl önemli gelişmeler 2. Dünya Savaşı dönemlerinde gerçekleşmiştir. William Frederick Friedman'nın Japonların yaptığı şifreleme tekniğini çözmesi Amerika Birleşik Devletleri'nin menfaatine olmuştur. Aynı şekilde yine o dönemde İngiliz Alan Turing ve ekibinin Alman ordusunun şifreleme sistemini çözmesi İngilizlere üstünlük sağlamıştır (Kaşkaloğlu, t.y.). Günümüze gelindiğinde ise online bir şekilde herkesin interneti kullanmasından dolayı şifrelemeye askeri alandan ziyade sağlık

hizmetleri, özel sektör, finans gibi alanlarda da ihtiyaç duyulmaya başlanmıştır (Yerlikaya, Gençoğlu, Emir, Çankaya ve Buluş, 2011).

Güvenli veri alışverişinin sağlanabilmesi için gizlilik, bütünlük, doğrulama gibi temel etkenler bulunmaktadır. Gizlilik; verinin sadece yetkili kullanıcılar tarafından görüntülenmesi, bütünlük; verinin sadece gönderici tarafından değiştirilmesi, doğrulama; mesajın bozulmamış olması anlamlarını ifade eder. Şifreleme sistemlerinin karmaşık bir yapıda olması bu yapıları ekarte edebilmektedir (Akgül, 2015). Veriyi şifreleme ve çözme işlemi bir anahtar yardımı ile yapılır. Şifrelenmiş verinin çözülmesi ancak doğru anahtarın kullanılmasıyla mümkündür. Veriyi şifreleme ve çözme işleminde anahtarın üretilmesi önemli bir problemdir. Günümüzde karmaşık dinamik özelliklerinden dolayı kaotik sistemlerden üretilen rasgele sayıların anahtar olarak kullanılması bu alanda ilgi çeken bir çalışma konusu olmuştur.

Kaos bilimi ilk olarak 1963'te Edward Lorenz'in hava olaylarının tahmini üzerine yaptığı bir takım çalışmalar ile ortaya çıkmıştır (Munmuangsaen ve Srisuchinwong, 2018; Özdemir, 2008). Başlangıç şartlarına aşırı duyarlı olan kaotik sistemlerin çok küçük bir parametre değişimi sonucunda tahmin edilebilirliği imkânsızlaşmaktadır (Pamuk, 2016). Rasgele gibi gözüken olayların temeldeki birbirine bağlılığından bahseden kaos kısaca düzensizliğin düzeni olarak da ifade edilebilir (Pehlivan, 2010; Tuna ve Fidan, 2018). Kaos ve kaotik sistemler ile evrenin oluşumundan biyolojik canlı yapılarının tanımlanmasına, veri güvenliğinden doğa olaylarının tahminine kadar birçok alanda yararlanılmaktadır. Her sistem kaotik bir davranış sergilemeyebilir. Literatürde, bir sistemin kaotik davranış gösterip göstermediğini analiz etmede kullanılan birçok yöntem bulunmaktadır. Lyapunov üstelleri, çatallanma diyagramları, faz portreleri, Poincare kesiti, denge noktalarının incelenmesi bu analiz yöntemlerinden bazılarıdır (Akgül, 2015; Lai, Akgul, Varan, Kengne ve Erguzel, 2018; Su, 2015; Xian, Xia, Guo, Fu ve Xu, 2018; Yang ve Qi, 2019). Kaotik sinyallerin gürültü benzeri davranışlar göstermesi, parametrelerine ve başlangıç şartlarına hassas bir şekilde duyarlı olması özellikle güvenli haberleşmede kaos tabanlı rasgele sayı üreteçlerini ön plana çıkarmaktadır.

Rasgele sayı üreteci (RSÜ); donanımsal veya yazılımsal yöntemler kullanılarak istatistiksel olarak birbirinden bağımsız sayılar üreten ve çıkışında korelasyon bulundurmayan sistemlere denir. Bu üreteçler sayesinde bir önceki veri kullanılarak, öngörülemeyecek seviyede rasgele çıkış üretilebilmektedir (Özdemir, 2008). Bu gibi özelliklerinden dolayı rasgele sayı üreteçleri günümüzde şans oyunları, simülasyon, modelleme, rasgele örnekleme, genetik algoritma, şifreleme, damgalama, gizli yazı gibi alanlarda kullanılan güncel bir çalışma konusu olmuştur. Üretilen rasgele sayıların güvenlik açısından tahmin edilebilirliğinin çok düşük olması istenmektedir. Bu amaçla üretilen rasgele sayıların literatürde kabul görmüş olan NIST-800-22 ve FIPS-140-1 gibi bazı istatistiksel testlere tabi tutulması gerekmektedir.

Literatür taraması yapıldığında bu alanda yapılan birçok çalışma ile karşılaşılmaktadır. Su yaptığı çalışmada bir kaotik sistemin dinamik analizlerini incelemiştir (Su, 2015). Xian ve arkadaşları geniş aralıkta çekerlere sahip kaotik sistemin dinamik analizlerini bir FPGA uygulaması kullanarak gerçekleştirmişlerdir (Xian vd., 2018). Zhu ve arkadaşları gözdeki irisin benzersiz rasgeleliğini kullanarak bir kaotik sistem geliştirmiş ve rasgele sayı üretimini gerçekleştirmişlerdir (Zhu, Zhao, Zhang ve Yang, 2013).

Toyran yaptığı bir çalışmada rasgele sayıların verimli kullanımını incelemiştir (Toyran, 2007). Yaptığı çalışmalarla rasgele sayıların hangi durumlarda daha verimli ve daha verimsiz olduğunu göstermiştir. Avaroğlu ve Türk yaptığı bir çalışmada doğal gürültü kaynağı olarak kaotik sarmalları kullanarak bir RSÜ tasarımı gerçekleştirmişlerdir (Avaroğlu ve Türk, 2013). Şahin, yaptığı bit çalışmada modern blok şifreleme algoritmalarını incelemiştir. Blok şifrelerin gücünün analizini yapmıştır (Şahin, 2015). Özdemir ve arkadaşları tarafından gerçekleştirilen bir çalışmada altın oran dengesine sahip bir kaotik sistem kullanılanılarak RSÜ tasarımı yapılmıştır (Ozdemir, Pehlivan, Akgul ve Guleryuz, 2018). Özkaynak yaptığı bir çalışmada kriptolojik uygulamalarda kullanılmak amacıyla RSÜ'lerin mimari yapıları üzerinde bir çalışma yapmışlardır (Özkaynak, 2016).

Güvenoğlu ve Esin resim şifreleme üzerine kullanımı kolay, etkin ve güçlü olan bir çalışma yapmışlardır. Bunu gerçekleştirirken Knutt / Durstenfeld Shuffle Algoritmasını

kullanmışlardır (Güvenoğlu ve Esin, 2009). Milani ve arkadaşları yaptıkları bir çalışmada Henon kaotik sistemlerini ve logistik harita kullanarak hızlı bir görüntü şifreleme algoritması geliştirmişlerdir (Milani, Pehlivan ve Pour, 2013). Çavuşoğlu ve arkadaşları Lorenz kaotik sistemini kullanarak sinyal gizleme uygulaması gerçekleştirmişlerdir (Çavuşoğlu, Uyaroğlu ve Pehlivan, 2014).

Bu tez çalışmasında ise; doğrusal olmayan bir sistemin kaotik davranışlarını analiz etmek için Lyapunov üstel spektrum ve boyut analizi, çatallanma diyagramları, faz portreleri Poincare kesiti, denge nokta analizi ve başlangıç koşullarına hassas duyarlı olma gibi kaotik sistem analiz yöntemlerinin incelenmesi; yeni elde edilen bir kaotik sistemin Matlab programı yardımıyla kaotiklik analizleri yapıldıktan sonra, geliştirilen algoritma ile Raspberry Pi 3 Model B mikrobilgisayarı üzerinde, Spyder programında Phyton programlama dili ile bir mobil RSÜ tasarımı gerçekleştirilmesi; elde edilen rasgele sayıların rasgeleliğini test etmek için NIST 800-22, FIPS 140-1 (Akhshani, Akhavan, Mobaraki, Lim ve Hassan, 2014; Çavuşoğlu, Akgül, Zengin ve Pehlivan, 2017; Barış Karakaya, Gülten ve Frasca, 2019; Koyuncu ve Özcerit, 2017; Zhu vd., 2013) istatistiksel testleri kullanılarak güvenli bir şekilde kullanılabileceğinin gösterilmesi; üretilen rasgele sayıların Raspberry Pi 3 Model B milrobilgisayarı üzerinde bir resim şifreleme uygulamasında kullanılması; son olarak da şifrelenmiş resmin Matlab programı yardımıyla histogram analizi, korelasyon ve entropi katsayıları, korelasyon haritası, NPCR, UACI (Alawida, Samsudin, Teh ve Alkhawaldeh, 2019; Fahd, Afzal, Abbas, Iqbal ve Waheed, 2018; Hua, Zhou ve Huang, 2019; Kandar, Chaudhuri, Bhattacharjee ve Dhara, 2019; Su, Wo ve Han, 2019) gibi güvenlik testlerine sokularak şifreleme algoritmasının güvenilirliğinin ölçülmesi amaçlanmıştır.

BÖLÜM 2. KAOS VE KAOTİK SİSTEMLER

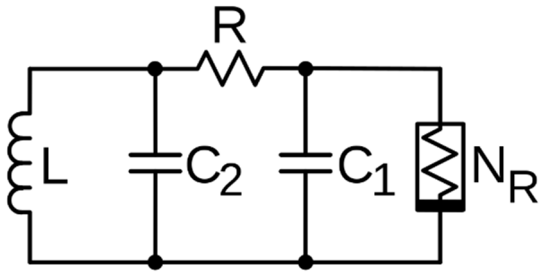
2.1. Kaotik Sistemler

Kaos 1963 yılında Amerikalı bir meteorolog bir bilim adamı olan Edward Norton Lorenz'in hava olaylarındaki küçük değişimlerin neticede büyük değişimlere yol açtığının farkına varmasıyla bilim dünyasına girmiştir (Yardım ve Afacan, 2010; Yerlikaya vd., 2011). Kelime anlamı olarak kaos; "evrenin düzene girmeden önceki biçimden yoksun, uyumsuz ve karmaşık durumu" şeklinde tanımlanmaktadır. Kaotik sistem, başlangıç şartlarına aşırı derecede hassas bağımlı ve ölçülemeyecek kadar karmaşıkdır olan sistemler olarak da tanımlanmaktadır (Ağır, 2010). Kaos teorisi matematiksel bir teori olmakla birlikte aynı zamanda evrenin oluşumu, evrim, tıp, nüfus bilimi, coğrafya, biyoloji, finans gibi konularda da yer edinmektedir. Gündelik hayatımıza bakacak olursak yapılan bir davranışın ya da alınan bir kararın hangi neticeleri doğuracağı tam olarak kestirilemediği için kaosa yaşamımızın her noktasında rastlamak mümkündür.

Kaos teorisi günümüzde karmaşık, doğrusal olmayan olayları inceleyen bir bilim dalı haline gelmiştir. Yerçekimi, fizik, elektriksel veya kimyasal tepkimeler gibi geleneksel bilimlerin aksine kaos teorisi hava tahmini, türbülans, borsa, zihinsel durumlar gibi öngörülebilirliği çok zor olan veya kontrol edilemeyen konuları ele almaktadır (Tufan, 2017).

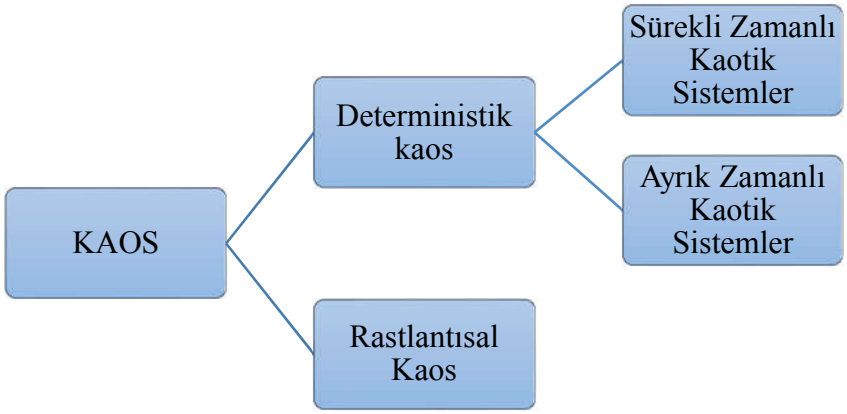
Kaos dinamik sistemlerdeki en karmaşık kararlı hal davranışıdır. Genlik ve frekansının tespit edilememesi, zaman boyutunda meydana gelen düzensiz salınımlar, başlangıç şartlarına olan hassas duyarlılık, gürültü benzeri geniş güç spektrumlarına sahip olma, limit kümesinin fraktal yapıda olması ve sınırlı bir alan içersinde tahmin edilemez bir şekilde değişen işaretler içermesi kaosun başlıca önemli özelliklerindendir (Pehlivan, 2010).

Bir kaotik sistemin gerçek hayata uyarlanabilmesi için genellikle yazılımsal veya elektronik olarak gerçeklenebilmesi gerekmektedir. Leon Ong Chua tarafından elektronik devre elemanları kullanılarak 1983'te bir kaotik sistemin modellenmesi gerçekleştirilmiştir. Tasarımcısının ismini alan Chua devresinin (Şekil 2.1) tasarımı ve anlaşılması kolay olduğu için birçok defa üzerinde uygulamalar gerçekleştirilmiş ve günümüz çalışmalarına da yol göstermiştir (Özdemir, 2008).



Şekil 2.1. Chua devresi (Martínez-Guerra, Pérez-Pinacho ve Gómez-Cortés, 2015)

Kaos teorisi kaos kelimesinin zıttına düzenli bir yapıdan ziyade karmaşa gibi gözüken bir yapının içerisindeki düzeni ortaya koymakla ilgilenmektedir. Kaos terorisi; "deterministik kaos" ve "rastlantısal kaos" olmak üzere iki ayrı başlıkda incelenmektedir. Bilim daha çok deterministik kaos ile ilgilenmektedir. Şekil 2.2.'de kaos bilimi ve alt başlıkları verilmiştir.



Şekil 2.2. Kaos bilimi alt başlıkları

Meydana gelen olaylar zaman parametresine bağlı olarak sürekli veya ayrık zamanlı olmak üzere iki şekilde karşımıza çıkmaktadır. Devamlı olarak zamana bağlı bir şekilde ölçümleri gerçekleştirilebilen sistemler sürekli zamanlı sistemler adını alır. Diğer yandan ayrık zamanlı değişimler gösteren sistemler de ayrık zamanlı sistemler olarak tanımlanmaktadır (Pamuk, 2016).

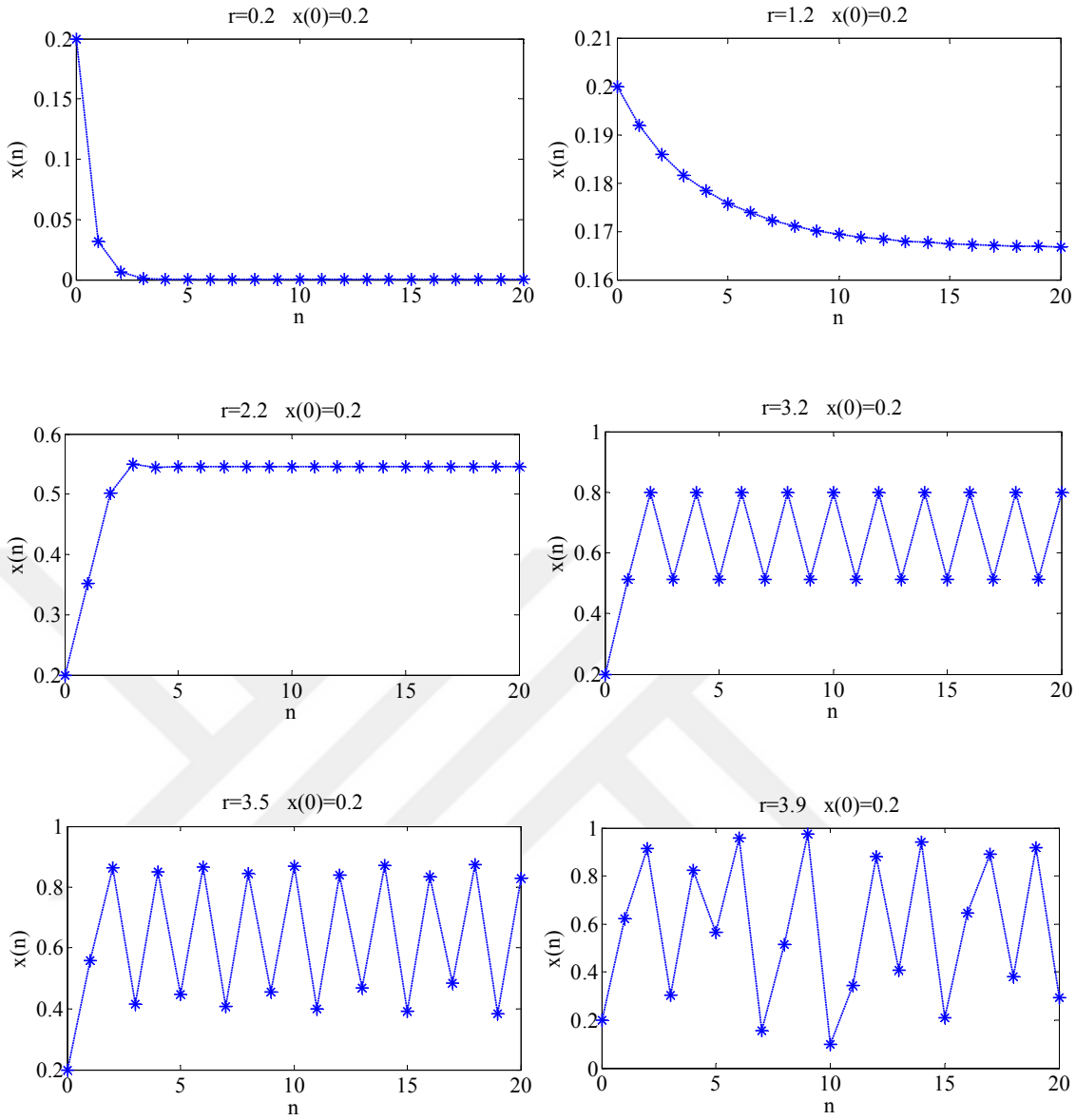
2.1.1. Ayrık zamanlı kaotik sistemler

Ayrık işaretler olarak incelenen bir kaotik sistem ayrık zamanlı dinamik sistem olarak adlandırılmaktadır. Ayrık zamanlı kaotik sistemler en az üç boyuttan meydana gelen sürekli zamanlı kaotik sistemlerin aksine, bir boyuttan da oluşabilmektedir. Logistic Map, Cubic Map, Sine Map, Tent Map, Gauss Map, Cusp Map, Gaussian White Chaotic Map, Pinchers Map gibi bazı tek boyutlu ayrık zamanlı kaotik sistemler literatürde sunulan sistemlere örnek olarak verilebilir (Akgül, 2015).

Literatürde en sık çalışılan tek boyutlu ayrık zamanlı kaotik sistemlerden biri olan Logistic map; memeliler, kuşlar vb. gibi biyolojik nüfus dağılımının basit bir modeli olan lojistik denklemin ayrıklaştırılmış şeklidir (Pehlivan, 2010). Logistic map ilk olarak 1976 tarihli bir makalede biyolog Robert May tarafından literature tanıtılmıştır (G.-C. Wu ve Baleanu, 2014). Denklem 2.1'de logistic map denklemi gösterilmektedir.

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

Burada x değeri sistem değişkenini, n ise tekrarlama sayısını ifade etmektedir. Sistem parametresi olarak ise sadece r değeri verilmiştir. Sistemde başlangıç değeri olarak da x_0 verilmiştir. Şekil 2.3.'te de görüldüğü üzere x_0 başlangıç değeri olarak 0.2 sabit bir değer verildiğinde r parametresi için 3.2'den büyük değerlerde sistem kaosa girmektedir.



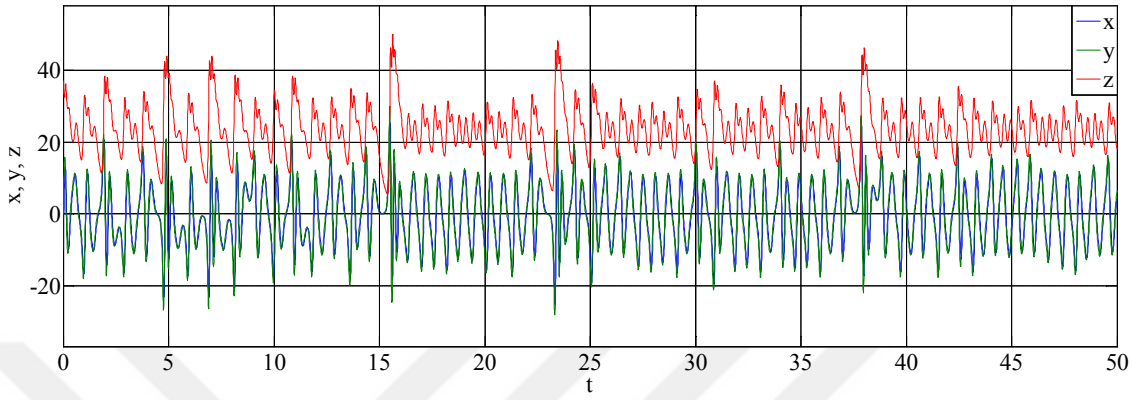
Şekil 2.3. 'r' parametresindeki değişime göre Logistic Map değişim grafiği

2.1.2. Sürekli zamanlı kaotik sistemler

Ayrık zamanlı kaotik sistemler tek bir denklemden meydana gelebilirken, sürekli zamanlı kaotik sistemler ise en az üç denklem içeren kaotik sistemlerdir (Akgül, 2015). Sürekli zamanlı sistemler genelde diferansiyel denklemlerle ifade edilirler.

Günümüze kadar gelmiş ve literatürde sunulan bir çok sürekli zamanlı kaotik sistemler mevcuttur. Lorenz, Rössler, Chua, Chen, Van Der Pol, Duffing, Rikikate, Rucklidge, Arneodo, Aizawa, Moore Spiegel, Sundarapandian-Pehlivan sistemleri bunlardan

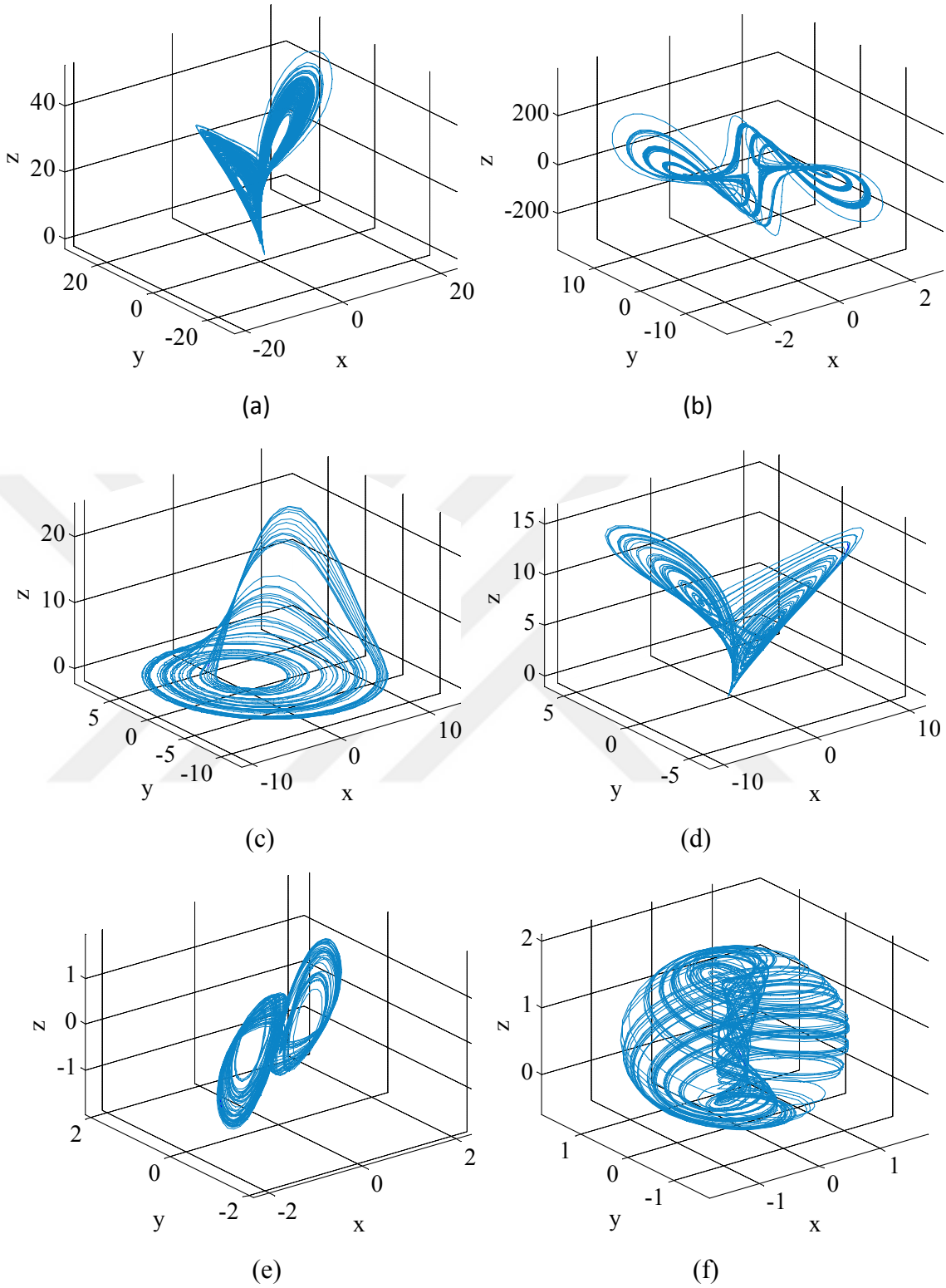
bazılarıdır (Akgül, 2015; Almali ve Dikici, 2016; Dursun ve Kaşifoğlu, 2018; Baris Karakaya, Turk, Turk ve Gulten, 2018; Koyuncu, 2014; Özyapici, 2017; Yeşil ve Babacan, 2019).



Şekil 2.4. Sürekli zamanlı bir kaotik sistemin zaman x, y, z fazlarının zaman serileri

2.2. Kaotik Sistemlerin Analiz Yöntemleri

Her diferansiyel denklem bir kaotik sistemi ifade etmez. Bir nonlineer dinamik sistemin kaotik özellik gösterip göstermediğini ya da hangi aralıklarda kaosa girip, hangi aralıklarda kaosdan çıktığını yorumlayabilmek için yapılan bazı analiz yöntemleri ve istenen şartlar bulunmaktadır. Bu şartların en önemlisi sistemde kesinlikle en az bir doğrusal olmayan terim bulunmalıdır ve sistem sürekli zamanlı ise en az üçüncü dereceden olmalıdır. Ayrık zamanlı sistemlerde böyle bir zorunluluk yoktur. Bu şartlar sağlanıyorsa sistemin kaotik analizleri yapılabilir (Koyuncu, 2014). Denge noktalarının, Lyapunov üstel spektrum ve boyutunun, faz portrelerinin, çatallanma diyagramlarının, zaman serilerinde başlangıç noktalarına olan hassasiyetlerin analizi gibi birçok analiz yöntemleri literatürde kullanılmaktadır (Lai vd., 2018; Pamuk, 2016; Su, 2015; Xian vd., 2018). Literatürde sunulan birçok kaotik sistem bulunmaktadır. Bu kaotik sistemlerden bazılarının 3D faz portreleri Şekil 2.5'te örnek olarak gösterilmiştir.



Şekil 2.5. Lorenz (a), Moore Spiegel (b), Rössler (c), Rucklidge (d), Sundaparandian Pehlivan (e), Aizawa (f) kaotik sistemlerinin 3D faz portreleri

Bu bölümde de bir sistemin kaotik davranışlarını incelerken yapılması gereken bazı analiz yöntemlerinden bahsedilmiştir. Bu analiz yöntemlerinin sonuçlarına bakılarak sistemin nasıl yorumlanması gerektiği anlatılmıştır.

2.2.1. Denge noktaları ve kararlılık analizi

Bir sistemin kaotik özellik gösterebilmesi için kararsız bir davranış sergilemesi gerekmektedir. Eğer sistem en az bir pozitif özdeğere sahipse kararsız yapıda olduğu söylenebilir (Çiçek, Ferikoğlu ve Pehlivan, 2016). Sistemin denge noktalarını bulmak için her bir durum değişkenlerinin türevi sıfıra eşitlenir (Denklem 2.2). Denklemler çözülerek denge noktaları elde edilir. Burada $dx(t)/dt$ durum değişkeninin türevini ve $F[x(t)]$ vektör alanını ifade eder.

$$\frac{dx(t)}{dt} = F[x(t)] = 0 \tag{2.2}$$

Her kaotik sistem reel denge noktalarına sahip değildir. Elde edilen denge noktaları reel sayılardan oluşuyor ise sistem reel denge noktalarına sahiptir denir. Sonuçlar sadece sanal değerlerden oluşuyorsa bu sistemler sanal denge noktalı kaotik sistemler diye adlandırılır.

$$J = \begin{bmatrix} \partial F_1/\partial x_1 & \partial F_1/\partial x_2 & \cdots & \partial F_1/\partial x_n \\ \partial F_2/\partial x_1 & \partial F_2/\partial x_2 & \cdots & \partial F_2/\partial x_n \\ \vdots & \vdots & \ddots & \vdots \\ \partial F_n/\partial x_1 & \partial F_n/\partial x_2 & \cdots & \partial F_n/\partial x_n \end{bmatrix} \tag{2.3}$$

Burada J jacobian matrisini ifade eder. Elde edilen denge noktaları Denklem 2.3'teki gibi Jacobian matrisinde yerine yazılarak $\det(J - \lambda I) = |J - \lambda I| = 0$ denkleminden özdeğerler (λ) elde edilir. Burada I birim matrisi temsil eder. Denge noktarındaki kararsızlık özdeğerlerden anlaşılabilir. Elde edilen özdeğerlerden en az birinin reel kısmının pozitif

olması denge noktasının kararsız olduğunu ifade eder ve sistemin kaotik olduğuna bir işaret olabilir.

Örnek olarak Denklem 2.4'teki x, y, z sistem değişkenlerini kullanan Lorenz sistemininin denge noktalarını inceleyecek olursak;

$$\begin{aligned} \dot{x} &= 10.(y - x) \\ \dot{y} &= -x.z + 28.x - y \\ \dot{z} &= x.y - (8/3).z \end{aligned} \tag{2.4}$$

İlk olarak türevler sıfıra eşitlendiğinde (Denklem 2.5) denge noktaları aşağıdaki gibi elde edilir.

$$\begin{aligned} 0 &= 10.(y - x) \\ 0 &= -x.z + 28.x - y \\ 0 &= x.y - (8/3).z \end{aligned} \tag{2.5}$$

E_1 = -8.5373 + 0.0000i, -8.4373 + 0.0000i, 27.0117 - 0.0000i
E_2 = 8.4336 - 0.0000i, 8.5336 - 0.0000i, 26.9881 + 0.0000i
E_3 = 0.0037 - 0.0000i, 0.1037 - 0.0000i, 1.4403e-04

Burada E_1, E_2, E_3 denge noktalarını ifade eder.

Bulunan denge noktalarının kararsız olup olmadıkları özdeğerlerinin bulunması ile anlaşılabilir. Özdeğerlerin bulunması için sistemin Jacobian matrisi alınır. Elde edilen Jacobian matrisinin sistem parametreleri ile yazılımı Denklem 2.6'daki gibidir.

$$J = \begin{bmatrix} -10 & 10 & 0 \\ 28 - z & -1 & -x \\ y & x & -8/3 \end{bmatrix} \tag{2.6}$$

Elde edilen denge noktaları Jacobian matrisinde yerlerine sırasıyla yazılırsa E_1 denge noktası için;

$$J(E_1) = \begin{bmatrix} -10 & 10 & 0 \\ 0.9883 & -1 & 8.5373 \\ -8.4373 & -8.5373 & -8/3 \end{bmatrix} \quad (2.7)$$

elde edilir.

$|\lambda I - J(E_1)| = 0$ denkleminin çözümünden E_1 denge noktası için karakteristik denkleminin özdeğerleri aşağıdaki gibi elde edilir.

$\lambda_1 = -13.8398 - 0.0000i$
$\lambda_2 = 0.0866 + 10.2335i$
$\lambda_3 = 0.0866 - 10.2335i$

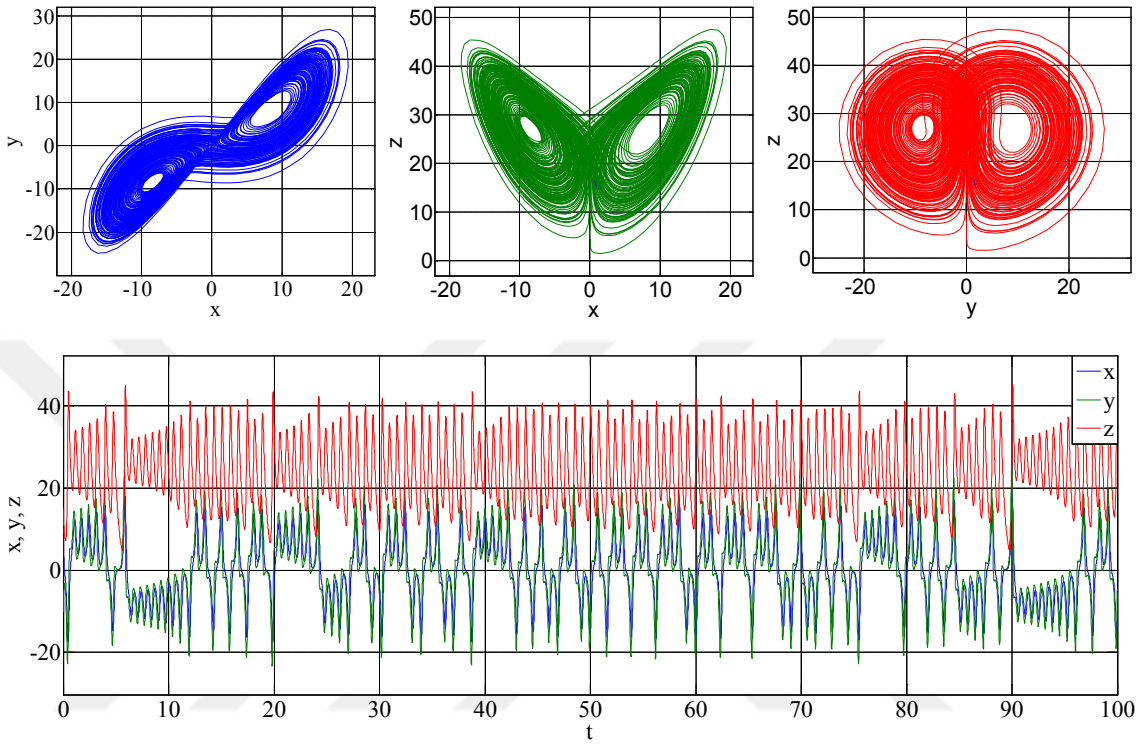
Görüldüğü üzere E_1 denge noktası için elde edilen özdeğerlere bakıldığında λ_2 ve λ_3 için reel kısımların pozitif olduğu görülmektedir. Bu sistemin kararsız olduğunu gösterir ve bir kaotik davranış sergilediğine işaret eder. Aynı şekilde E_2 ve E_3 denge noktalarının da kaotik davranışları hakkında yorum yapılabilmesi için özdeğerlerinin incelenmesi yapılmalıdır.

2.2.2. Faz portreleri (faz uzayı) ve zaman serileri

Nonlineer dinamik sistem analizlerinden biri de faz portrelerinin ve zaman serilerinin analizidir. Bir sistemin kaotik çekerleri ve zaman serilerinin dağılımı bize sistemin kaotikliği hakkında bilgi vermektedir. Faz portrelerindeki dinamik davranışın belli sınırlar içersinde ama karmaşık bir dağılımda olması ve zaman serilerindeki dağılımın periyodik olmayan bir davranış göstermesi gerekmektedir (Liu, Liu, Liu ve Liu, 2004). Günümüzde gelişen teknoloji ile üç boyutlu bir sistemin x-y, x-z, y-z faz portreleri Matlab, Labview, Pcpise gibi programlarla kolaylıkla elde edilebilmektedir.

Aşağıda Matlab programı kullanılarak elde edilen bazı sürekli zamanlı kaotik sistemlerin faz portleri, diferansiyel denklem ifadeleri ve başlangıç şartları gösterilmektedir.

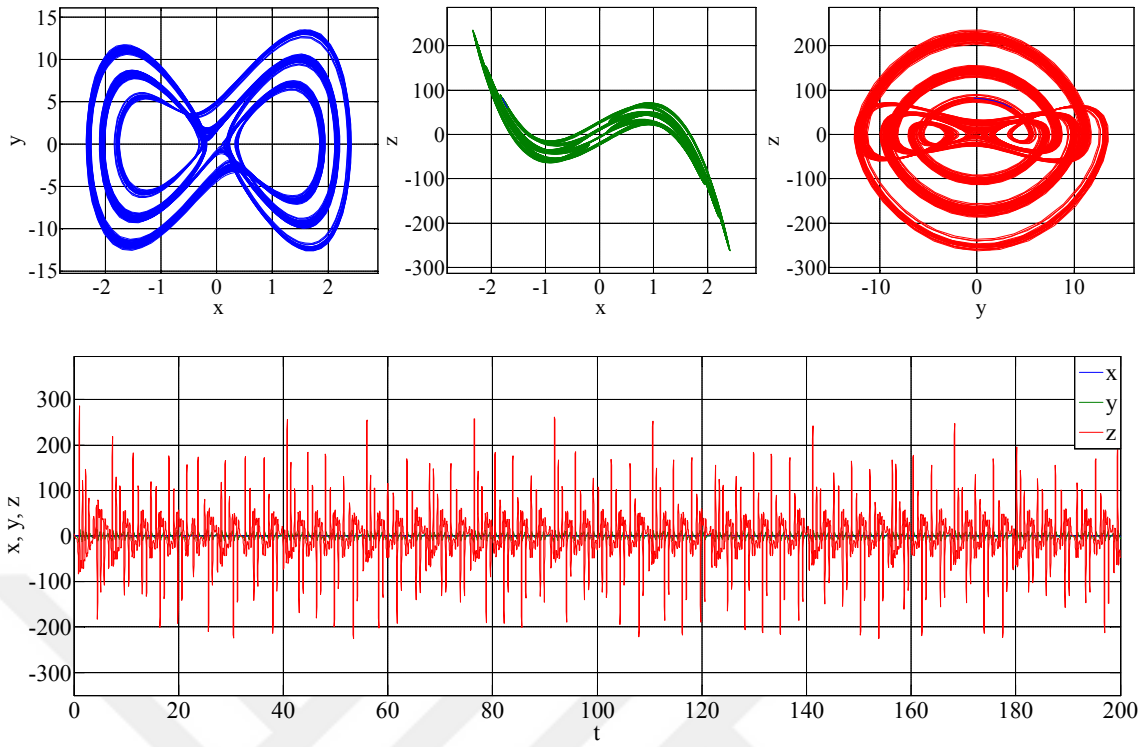
Lorenz kaotik sistemi, Denklem 2.8 kullanılarak; $\sigma = 10$, $r = 28$, $b = 8/3$ parametreleri ve $x_0 = 0{,}1$, $y_0 = -0{,}1$, $z_0 = 9$ başlangıç şartları sağlandığında, Şekil 2.6'daki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.



Şekil 2.6. Lorenz sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

$$\begin{aligned} \dot{x} &= \sigma.(y - x) \\ \dot{y} &= -x.z + r.x - y \\ \dot{z} &= x.y - b.z \end{aligned} \qquad (2.8)$$

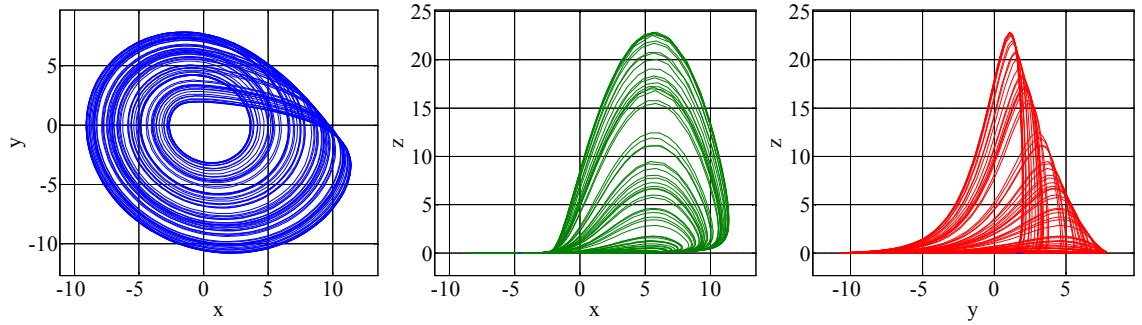
Moore Spiegel kaotik sistemi, Denklem 2.9 kullanılarak; $t = 26$, $\tau = 100$ parametreleri ve $x_0 = 0{,}1$, $y_0 = 0$, $z_0 = 0$ başlangıç şartları sağlandığında, Şekil 2.7'deki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.



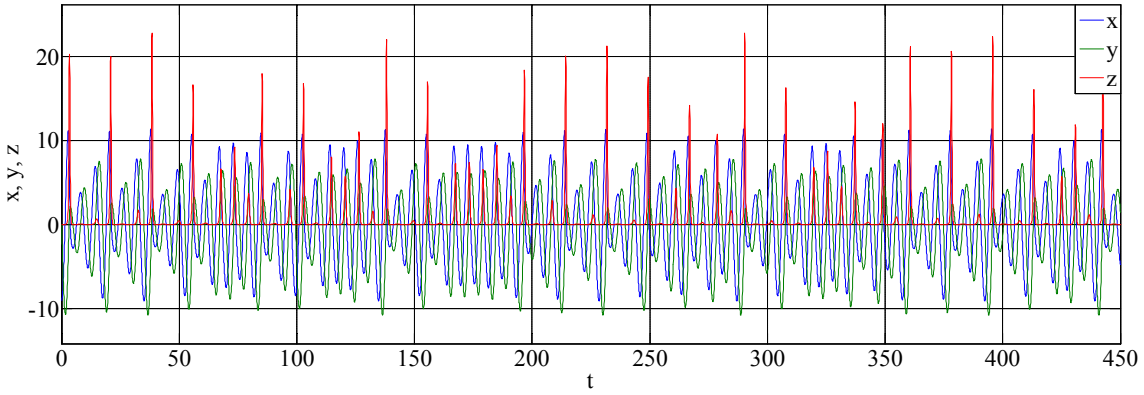
Şekil 2.7. Moore Spiegel sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= -z-(t-\tau+\tau.x^2).y-t.x \end{aligned} \tag{2.9}$$

Rössler kaotik sistemi, Denklem 2.10 kullanılarak; $a=0,2$, $b=0,2$, $c=5,7$ parametreleri ve $x_0=-9$, $y_0=0$, $z_0=0$ başlangıç şartları sağlandığında, Şekil 2.8'deki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.



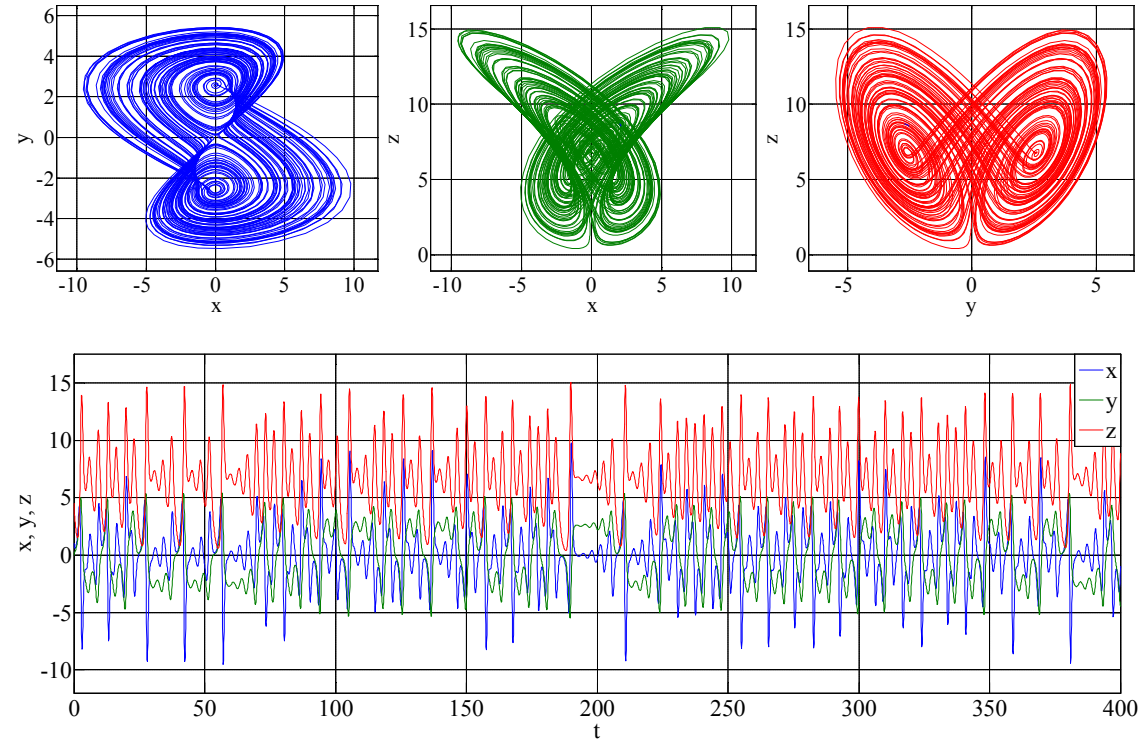
Şekil 2.8. Rössler sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri



Şekil 2.8. (devam) Rössler sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

$$\begin{aligned} \dot{x} &= -y - z \\ \dot{y} &= x + a.y \\ \dot{z} &= b + z.(x - c) \end{aligned} \tag{2.10}$$

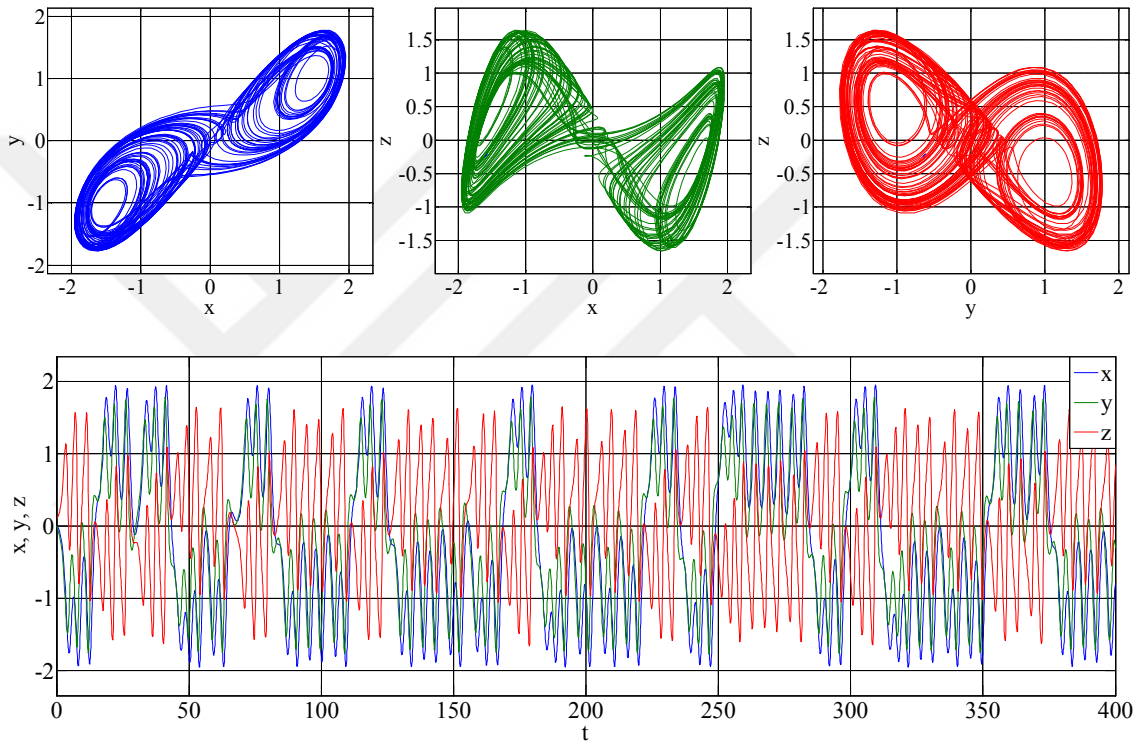
Rucklidge kaotik sistemi, Denklem 2.11 kullanılarak; $K = 2$, $L = 6,7$ parametreleri ve $x_0 = 1$, $y_0 = 0$, $z_0 = 4,5$ başlangıç şartları sağlandığında, Şekil 2.9'daki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.



Şekil 2.9. Rucklidge sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

$$\dot{x} = -K.x + L.y - y.z$$
$$\dot{y} = x \qquad (2.11)$$
$$\dot{z} = -z + y^2$$

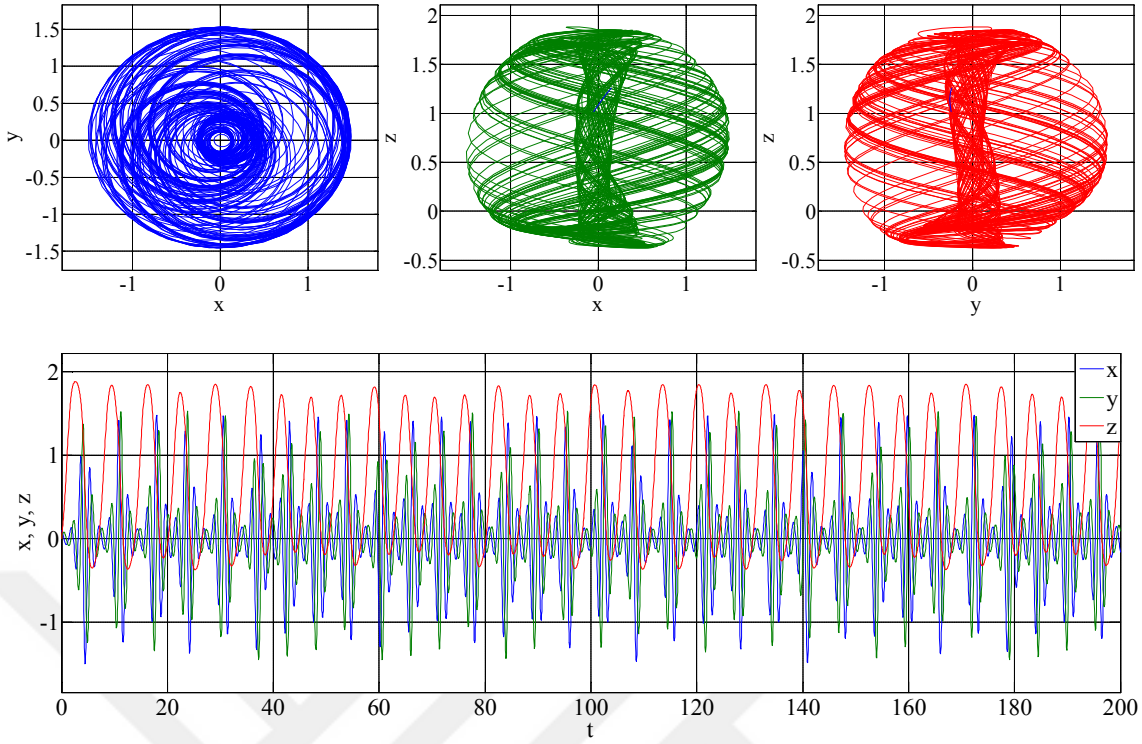
Sundarapandian-Pehlivan kaotik sistemi, Denklem 2.12 kullanılarak; $a = 1,5$, $\beta = 0,4$, $\gamma = 0,4$ parametreleri ve $x_0 = 0$, $y_0 = 0$, $z_0 = 0,1$ başlangıç şartları sağlandığında, Şekil 2.10'daki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.



Şekil 2.10. Sundarapandian-Pehlivan sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

$$\dot{x} = a.y - x$$
$$\dot{y} = -\beta.x - z \qquad (2.12)$$
$$\dot{z} = \gamma.z + x.y^2 - x$$

Aizawa kaotik sistemi, Denklem 2.13 kullanılarak; $a = 0,95$, $b = 0,7$, $c = 0,6$, $d = 3,5$, $e = 0,25$, $f = 0,1$ parametreleri ve $x_0 = 0,1$, $y_0 = 0$, $z_0 = 0$ başlangıç şartları sağlandığında, Şekil 2.11'deki kaotik faz portreleri ve zaman serilerini meydana getirmektedir.

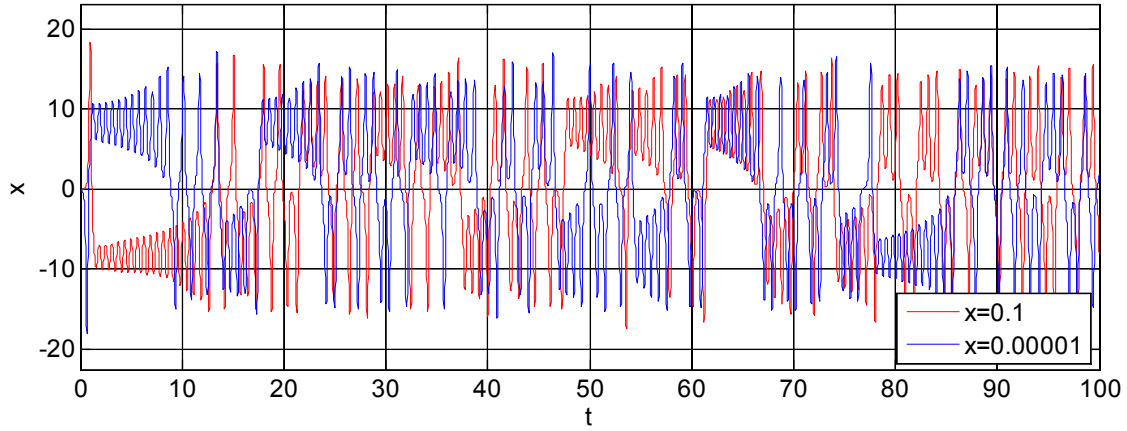


Şekil 2.11. Aizawa sistemi kaotik faz portreleri (x-y), (x-z), (y-z) ve zaman serileri

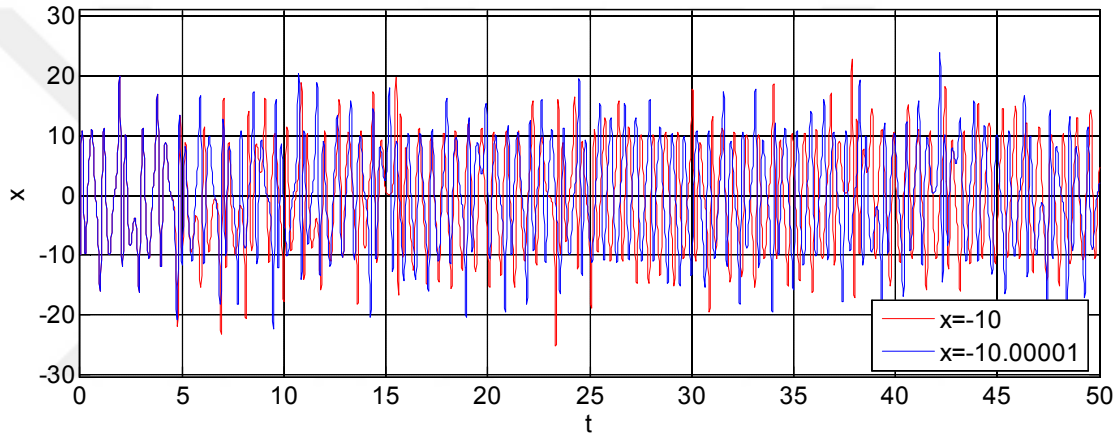
$$\begin{aligned}\dot{x} &= (z-b).x - d.y \\ \dot{y} &= d.x + (z-b).y \\ \dot{z} &= c + a.z - \frac{z^3}{3} - (x^2+y^2).(1+e.z) + f.z.x^3\end{aligned} \tag{2.13}$$

2.2.3. Zaman serisinde başlangıç şartlarına hassas bağımlılık

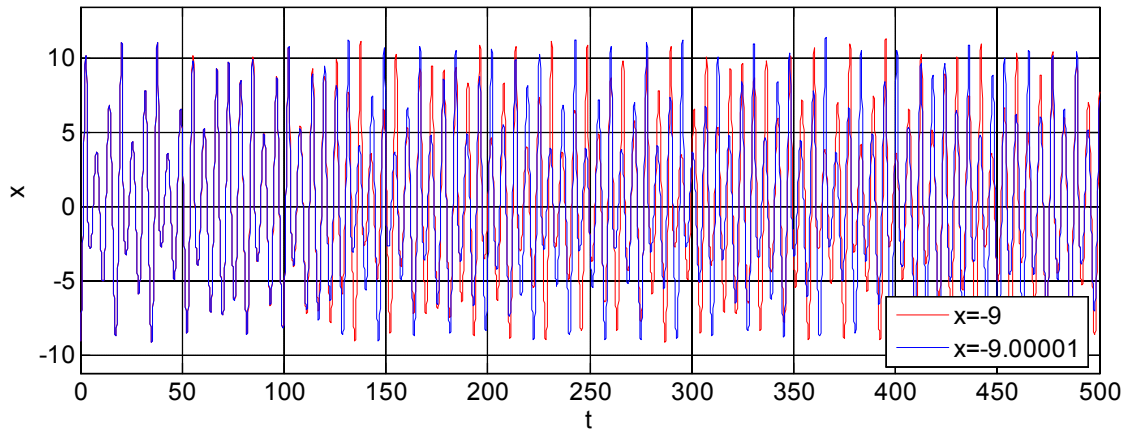
Nonlineer bir sistemin kaotik özellik göstermesi için gerekli olan bir diğer özellik de başlangıç şartlarına karşı son derece hassas bir yapıda olmasıdır. Başlangıç koşullarındaki hassas bir değişim sonraki aşamalarda öngörülemez bir şekilde büyük değişimlere yol açmaktadır. Bunun en kolay bir şekilde görülebilmesi için zaman serilerine bakmak yeterli olacaktır. Aşağıda Matlab programı kullanılarak elde edilen Şekil 2.12, Şekil 2.13 ve Şekil 2.14'te bazı kaotik sistemlerin başlangıç şartlarında yapılan hassas değişimlerin neticesinde meydana gelen zaman serilerindeki değişimler gösterilmiştir.



Şekil 2.12. Lorenz kaotik sistemi başlangıç şartlarına hassas bağımlılığın gösterimi



Şekil 2.13. Chen kaotik sistemi başlangıç şartlarına hassas bağımlılığın gösterimi



Şekil 2.14. Rössler kaotik sistemi başlangıç şartlarına hassas bağımlılığın gösterimi

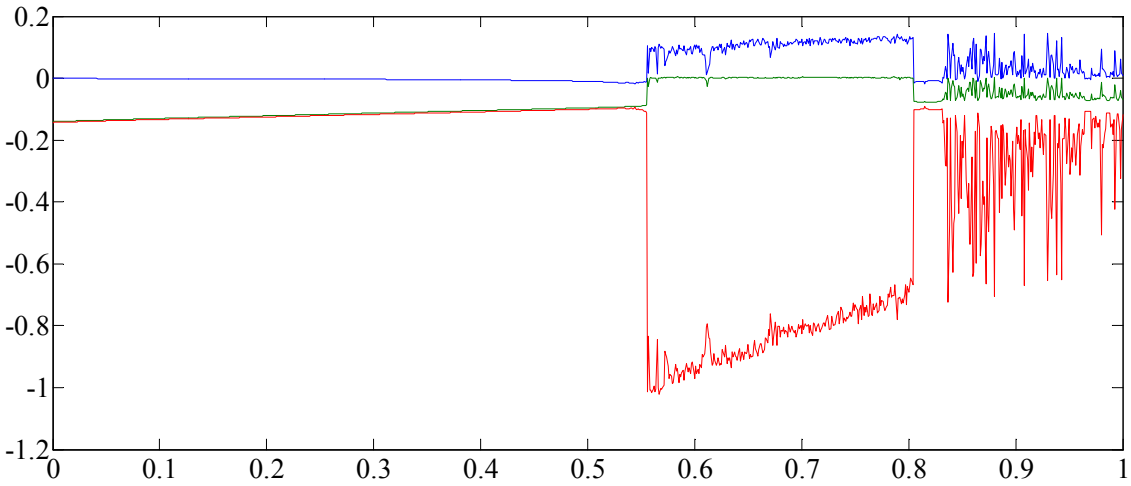
2.2.4. Lyapunov üstelleri ve boyut analizi

Lyapunov üstelleri bir sistemin dinamik davranışının belirlenmesinde çok önemli bir ölçüt olarak kullanılmaktadır. Lyapunov üstelleri sayesinde sistemin karakteristiği ve aynı zamanda kaotik davranışı hakkında bilgi edinilir. Rus matematikçi Aleksandr Mikhailovich Lyapunov tarafından bulunan Lyapunov üstelleri yöntemi ile bir zaman serisinin hangi aralıklarda kaotik bileşenler içerip içermediğinin tespiti yapılabilmektedir.

Kaotik sistemlerde her biz faz uzayı eğrisi neredeyse aynı başlangıç şartlarında farklı üstel artışlar gösterir. Bu yüzden kaotik sistemler periyodik olmayan dinamik davranışlar sergiler (Fell, Röschke ve Beckmann, 1993). Başlangıç şartlarına hassaslık olarak adlandırılan bu durumun hassasiyeti olan Lyapunov üsteli (λ), faz uzayındaki eğrilerin ayrılma açılarının ortalamasıdır. λ 'nın durumuna göre sistemin kaotikliğinin yorumu yapılır. λ negatif ise farklı başlangıç koşulları aynı sonuçlar vereceğinden sistem kaotik olmayacaktır. Diğer yandan λ pozitif olduğundan farklı başlangıç şartları farklı sonuçlar vereceğinden sistem kaotik bir davranış sergileyecektir (Munmuangsaen ve Srisuchinwong, 2018; Yılmaz ve Güler, 2006). Üç boyutlu sistemlerde Lyapunov üstelleri sadece (+, 0, -) durumunda kaotik özellik göstermektedir. Yani Lyapunov üstelleri $\lambda_1 > 0$, $\lambda_2 = 0$, $\lambda_3 < 0$ şeklinde olmaktadır. Diğer durumlar ise Tablo 2.1'de gösterildiği gibidir (Akgül, 2015; Pamuk, 2016). Temsili bir Lyapunov üstel spektrum grafiği ise Şekil 2.15'te gösterildiği gibidir.

Tablo 2.1. Lyapunov üstellerinin işaretlerine göre değişimi

Lyapunov Üstelleri	**Sistem Durumu**
(0,0,0)	İki-Torus
(-,-,-)	Sabit Nokta
(0,-,-)	Limit Döngü
(0,0,-)	Torus
(+,0,-)	Kaotik



Şekil 2.15. Temsili bir Lyapunov üstel spektrum grafiği

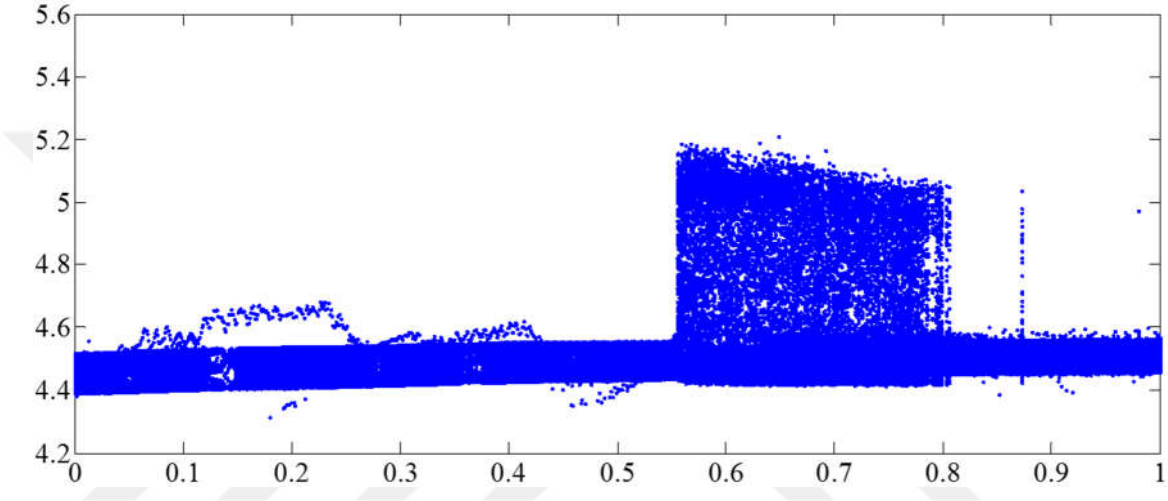
Bir dinamik sistemin diğer bir ifade ile Kaplan-Yorke boyutu olarak da bilinen Lyapunov boyutunun hesabı ile kaotik olup olmadığının yorumu yapılabilir. Sistemin kaotikliğinden bahsedilebilmesi için sırası ile pozitif, sıfır ve negatif değerde Lyapunov üstellerine sahip olması ve Lyapunov boyutunun da $2 < D < 3$ şartını sağlaması gerekmektedir. Denklem 2.14'te Layapunov boyutunun nasıl hesaplanacağı gösterilmiştir (Hamamci, Göğebakan ve Işık, 2015). Denklem 2.14'te j sistemin durum değişken sayısı, λ_i de Lyapunov üstelleri için kullanılmaktadır.

$$D = (j-1) + \frac{\sum_{i=1}^{j-1} \lambda_i}{|\lambda_j|} = 2 + \frac{\lambda_1 + \lambda_2}{|\lambda_j|} \tag{2.14}$$

2.2.5. Çatallanma diyagramı

Dinamik sistemlerde en sık kullanılan ve giderek önemi artan bir diğer analiz yöntemi de çatallanma diyagramlarıdır (Bayani vd., 2019; Kim ve Kim, 2019; Wei, Zhu, Yang, Perc ve Slavinec, 2019). Çatallanma diyagramları ile sistemin başlangıç değerlerine duyarlılığı analiz edilebildiği gibi sistemin hangi noktalarda periyodik durumdan kaotik duruma geçtiği rahatlıkla görülebilir (Min, Li, Zhang ve Li, 2019; Wang, Li, Zhong ve Hou, 2019).

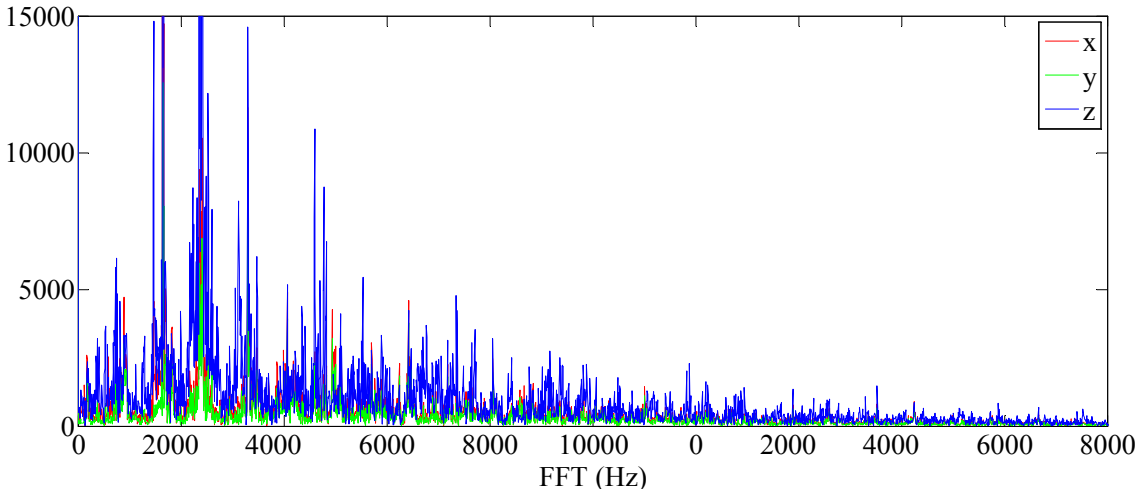
Kaotik bir sistemde durum değişkenleri, sistemin parametrelerine göre değişir. Bu değişiklikler sistemin kararlı bir hale girmesine ve aynı şekilde kaosa girmesine neden olur. Parametrelerindeki ufak değişimler faz uzayında çatallanma olayını meydana getirir. Kaotik bir sistemin herhangi bir parametresinin belli aralığında durum değişkeninin birbirlerine göre çizdirilmesi ile çatallanma grafiği elde edilir. Bu grafikler üzerinden sistemin kaotikliği analiz edilebilir. Temsili bir çatallanma grafiği ise Şekil 2.16'da gösterildiği gibidir.



Şekil 2.16. Temsili bir çatallanma grafiği

2.2.6. FFT (Fast Fourier Tranform) analizi

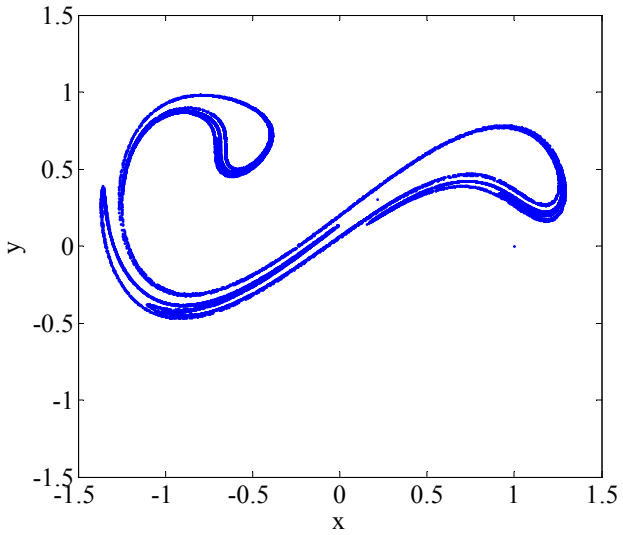
FFT yöntemi çıkış sinyalinin rasgele ve gürültülü bir yapıda olduğunu görmek için kullanılan bir analiz yöntemidir (Abdirash, Dolzhikova ve James, 2018). Sinyal çıkışları çok sayıda farklı frekanslardan oluşmaktadır. FFT ile farklı genlik, faz ve frekanslardaki bir sinyal, sinus ve cosinus bileşenlerinin toplamını ifade eder. Hangi frekansta ve genlikte sinyaller olduğu FFT işlemi yapılarak grafiğe aktarılır. Zaman boyutunda bulunan sinyaller, frekans boyutuna aktarılırak ifade edilir. Frekans bileşenlerininin artmasıyla çıkış sinyallerinin karmaşıklığı da artmaktadır. Bununla birlikte kaotik sistemler rasgele çıkışlar ürettiği için periyodik bir sinyal çıkışı üretmesi beklenemez. Temsili bir FFT grafiği ise Şekil 2.17'de gösterildiği gibidir.



Şekil 2.17. Temsili bir FFT analiz grafiği gösterimi

2.2.7. Poincare kesiti

Kaotik sistemlerde kullanılan bir diğer analiz yöntemi de Poincare kesitinin incelenmesidir (Kim ve Kim, 2019). Faz portreleri karışık yapıda olan kaotik sistemlerin gözlemlenmesi zor olabilir. Bu karmaşık yapıya Poincare kesiti ile bakmak daha belirginlik sağlamaktadır. Poincare yöntemi ile kaotik sistemin faz portrelerinden kesit alınarak görüntüler elde edilir. Poincare haritasındaki noktasal dağılımların yorumlanması ile kaotiklik hakkında sonuca varılır. Sistemin kaotikliğinden bahsedebilmek için noktasal dağılımın belirli yerlerde yoğunlaşması gerekir (Şekil 2.18). (Akgül, 2015).



Şekil 2.18. Temsili bir Poincare grafiği gösterimi

BÖLÜM 3. RASGELE SAYI ÜRETEÇLERİ, İSTATİSTİKSEL TESTLER VE GÜVENLİK ANALİZLERİ

Tezin bu bölümünde, Raspberry Pi 3 Model B tabanlı kaotik osilatörlerin ve sözde rasgele sayı üreteçlerinin tasarımı için bazı literatür çalışmalarına değinilmiştir. İlk olarak tasarımın gerçekleştirileceği Raspberry Pi 3 Model B mikrobilgisayarı hakkında bilgi verilmiştir. Daha sonra üretilen rasgele sayıların güvenli bir şekilde kullanılması için literatürde kabul görmüş olan rasgelelilik testlerinden bahsedilmiştir. Son olarak da resim şifreleme uygulaması ve şifrelenen resmin güvenlik analizleri hakkında bilgi verilmiştir.

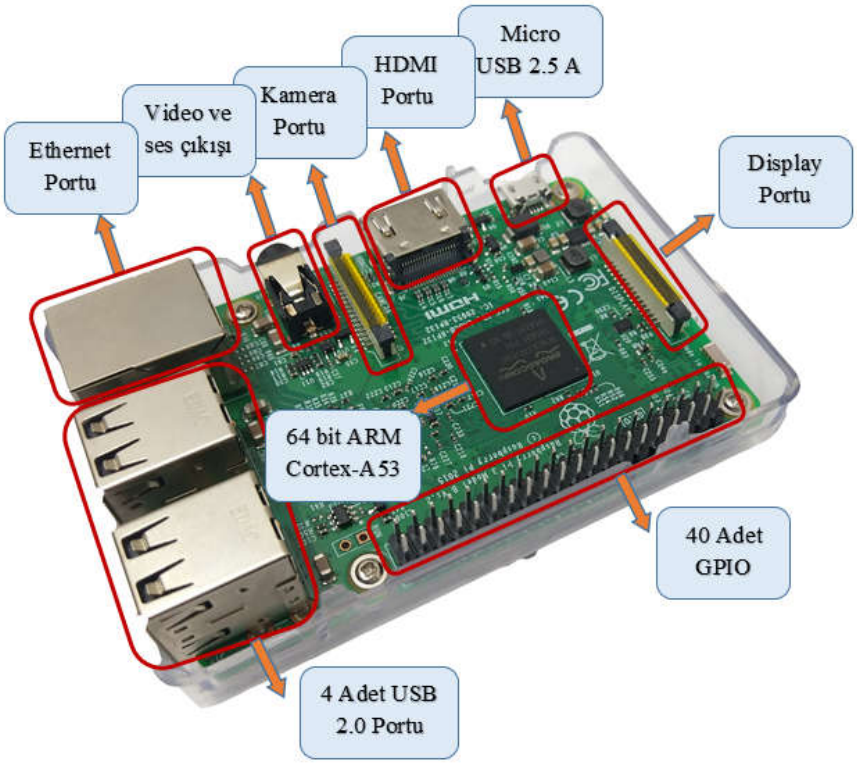
3.1. Raspberry Pi 3 Model B

Bu tez çalışmasında mikrobilgisayar olarak kullanılması düşünülen Raspberry Pi 3 Model B şimdiye kadar çıkmış en güçlü mikrobilgisayarlardan birisidir. Kart üzerinde Broadcom tarafından üretilen BCM2837 SoC (system-on-chip), 1,2 GHz 64-bit 4 çekirdekli ARM Cortex-A53 işlemci bulunmaktadır. Bilgisayarda yapılabilen her işlemin yapılabilmesi ve düşük maliyeti sayesinde günümüzde oldukça rağbet görmektedir (Hatun, 2018). Raspberry Pi 3 Model B'ye ait genel görünüm Şekil 3.1'de verildiği gibidir.

Raspberry Pi 3 Model B'ye ait teknik özellikler ise aşağıda verildiği gibidir ("Raspberry Pi Foundation - About Us", t.y.).

- Broadcom BCM2837 SoC
- 1.2 GHz 4 çekirdekli 64-bit ARM Cortex-A53 işlemci
- 2 çekirdekli Videocore IV® Multimedia işlemcisi
- 1 GB bellek
- Dahili WiFi
- Bluetooth 4.1

- 10/100 Mbit Ethernet portu
- HDMI portu (HDMI 1.4 destekli)
- Ses ve video çıkışı için 3.5 mm konektör
- 4 adet USB 2.0 portu
- Diğer Raspberry Pi modelleri ile uyumlu olan 40 adet GPIO
- WiFi / Bluetooth için dahili çip anten
- DSI (ekran) ve CSI (kamera) girişi
- Mikro SD kart yuvası
- 85 x 56 x 17 mm boyutlarında

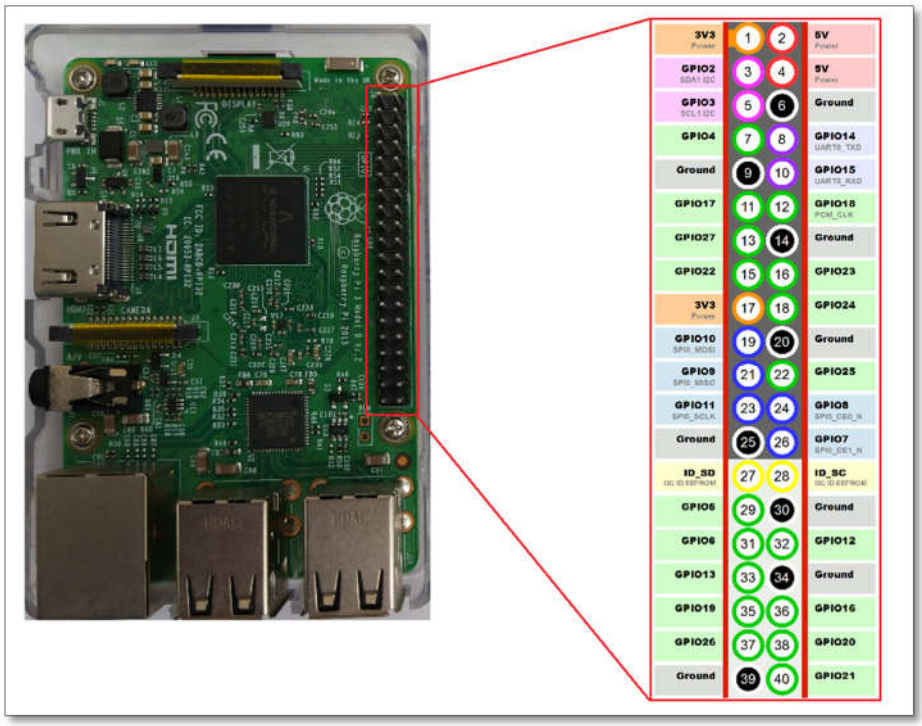


Şekil 3.1. Raspberry Pi 3 Model B genel görünüm

Raspberry'ye bağlantı VNC, SSH, TTL gibi uzaktan bağlantı yöntemleri ile gerçekleştirilebildiği gibi doğrudan HDMI bağlantısı ile LCD ekran ya da display portu ile dokunmatik ekran üzerinden masaüstüne erişim sağlanabilmektedir. Raspberry Pi 3 Model B üzerinde elektronik sistemlerle haberleşmeyi ve kontrolü sağlamak amacıyla oluşturulmuş 40 adet GPIO (General Purpose Input/Output) pini bulunmaktadır:

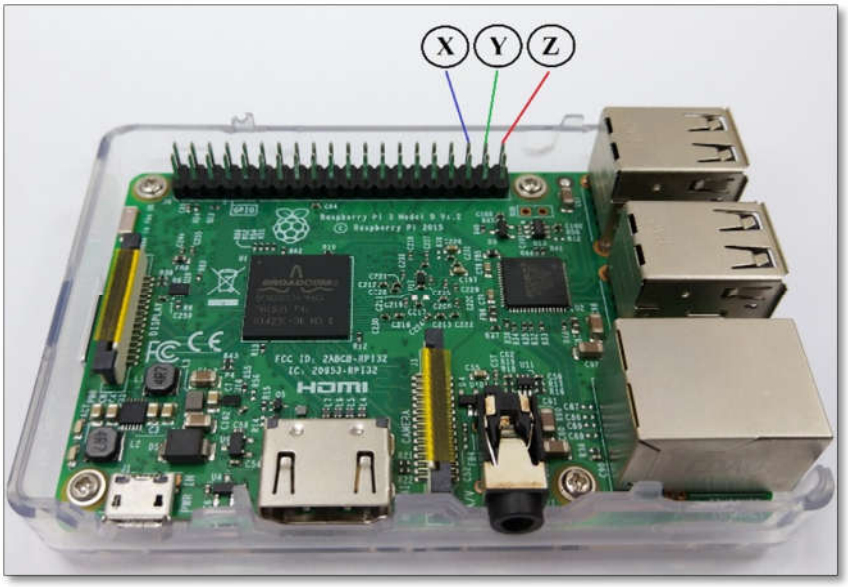
- Genel amaçlı giriş / çıkış için kullanabileceğimiz GPIO pinleri
- I2C haberleşme portu (GPIO2 ve GPIO3 pinleri)
- SPI haberleşme portu (GPIO10, GIPO09 ve GPIO11 pinleri)
- Seri haberleşme portu - UART (GPIO14 ve GPIO15 pinleri)
- 5V çıkış portu (2 ve 4 nolu pin)
- GND (6, 9, 14, 20, 25, 30, 34, 39 pinleri)

Şekil 3.2'de bu pinlerin yerleri ayrıntılı bir şekilde gösterilmiştir.



Şekil 3.2. Raspberry Pi 3 Model B GPIO pinleri

Raspberry Pi 3 Model B ile tasarlanan ve gerçeklenen mikrobilgisayar tabanlı mobil RSÜ sayesinde Raspberry Pi 3'ün GPIO pinlerinden rasgele sayılar çıkış olarak alınabilecektir. Şekil 3.3'te örnek olarak çıkış alınabilecek GPIO pinler gösterilmiştir. Kaotik sistem 3 boyutlu bir sistem olduğu için x, y ve z olarak 3 farklı çıkıştan rasgele sayılar elde edilebilir.

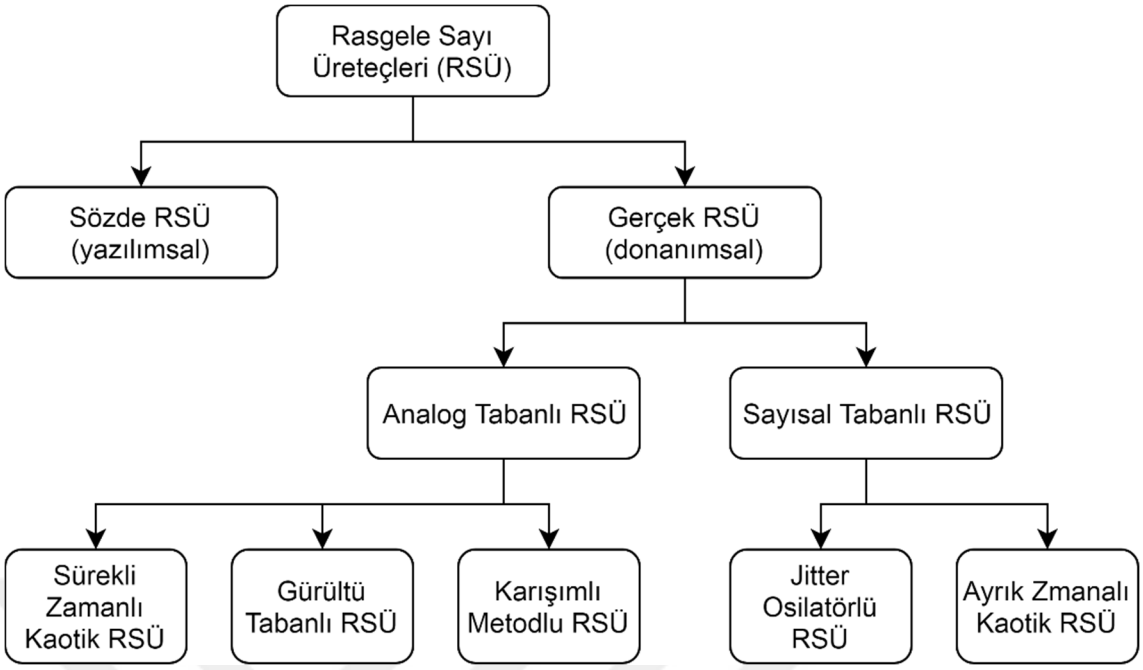


Şekil 3.3. Raspberry Pi 3 x-y-z pin çıkışları

3.2. Rasgele Sayı Üreteçleri

Rasgele sayılar belirli bir aralık içersinde oluşturulan ve aralarında herhangi bir bağlantı olmayan sayılardır (Toyran, 2007). Rasgelelik günümüzde birçok uygulamada kullanılan bir kavram haline gelmiştir. İstatistik, nümerik analiz, şans oyunları gibi birçok alanın yanısıra kriptolojik uygulamaların çoğunluğunda rasgele sayılardan faydalanılmaktadır. İletilecek veya alınacak verinin sadece alıcı ve iletici tarafından bilinmesi gereken güvenli haberleşme uygulamalarında rasgele sayılardan yararlanılır. Bankamatik kullanıcı erişimi, oturum erişimi, kimlik doğrulama vb. kullanılan bazı şifreleme alanlarından birkaçıdır (Akkaya, Pehlivan, Akgül ve Varan, 2018; Avaroğlu ve Türk, 2013; Özkaynak, 2016).

RSÜ'ler Şekil 3.4'te görüldüğü gibi Sözde RSÜ (SRSÜ - Pseudo random number generator) ve Gerçek RSÜ (GRSÜ - True random number generator) olmak üzere iki ana başlıkdan oluşmaktadır. GRSÜ'lerin tasarımı donanımsal olarak gereçekleştirilirken, SRSÜ'lerin tasarımı yazılımsal olarak gerçekleştirilmektedir. Önceki bölümlerde bahsedilen sürekli zamanlı sitemler (analog sistemler) ve ayrık zamanlı sistemler (sayısal sistemler) ise Gerçek RSÜ'lerin alt başlıklarını oluşturmaktadır (Akgül, 2015).



Şekil 3.4. Rasgele sayı üreteçleri alt dalları

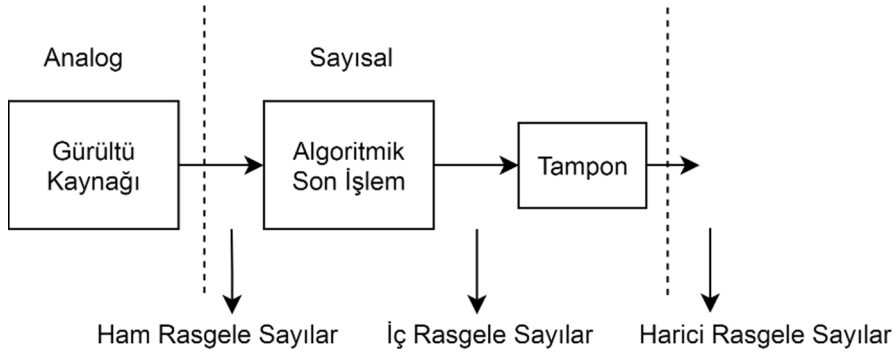
3.2.1. Sözde rasgele sayı üreteçleri

SRSÜ'lerinde entropi kaynağı olarak belli bir algoritma, matematiksel denklem ya da önceden belirlenmiş tablolar kullanılmaktadır. GRSÜ'lerin aksine SRSÜ'leri ile aynı başlangıç şartları ile aynı rasgele sayılar elde edilebilmektedir. GRSÜ'lerinde olduğu gibi SRSÜ'leri donanımsal bir alt yapı gerektirmediği için gerçekleme işleminin kolaylığı ve maliyetinin uygun olması gibi avantajlara sahiptir (Özdemir, 2008).

3.2.2. Gerçek rasgele sayı üreteçleri

Entropi kaynağı olarak GRSÜ'lerinde deterministik olmayan doğadaki fiziksel durumlardan yararlanılır. Termal gürültü, fotoelektrik etkisi, ısıl gürültü gibi doğal gürültü kaynakları GRSÜ için kullanılan entropi kaynaklarına örnek olarak verilebilir. Yüksek güvenliğin ön planda olduğu şifreleme gibi işlemlerde GRSÜ'ler kullanılmaktadır (Özdemir, 2008). İşlemin temelinde genellikle analog verinin dijital veriye dönüşümü yatmaktadır (Erdinç Avaroğlu ve Türk, 2013). GRSÜ'ler çıkışında tamamen rasgele diziden oluşan sayılar üretilmektedir. Aynı koşullarda iki kere çalıştırılan bir GRSÜ'de tamamen farklı bir dizide rasgele sayı üretimi gerçekleştirilir

(Toyran, 2007). Şekil 3.5'te genel olarak bir GRSÜ'nün mimari yapısı gösterilmektedir. Gürültü kaynağı olarak elektronik devreler ya da fiziksel deneyler kullanılır. Gürültü kaynağından üretilen sürekli zamanlı sinyaller binary değerlere dönüştürülür. Karşılaşılabilecek zayıflıkları indirgemek için son işlem uygulanır. Ancak güçlü gürültü kaynakları kullanılarak son işleme gerek kalmadan iç rasgele sayıları çıktı olarak da kullanılabilir (Özkaynak, 2016).



Şekil 3.5. GRSÜ genel mimarisi (Özkaynak, 2016)

3.3. İstatistiksel Rasgelelik Testleri

Rasgele sayıların üretiminde en önemli nokta rasgeleliğin tahmin edilemez olmasıdır. Kaotik sistemler periyodik olmayan davranışları, önceden tahmin edilemez yapıları ve gürültü benzeri sinyalleri sayesinde rasgele sayı üretiminde önemli bir yer edinmiştir. Kaotik sistelerden elde edilen rasgele sayıların güvenli bir şekilde uygulanabilmesi için literatürde kullanılan bazı rasgelelik testleri bulunmaktadır. Federal Information Processing Standards (FIPS) 140-1, National Institute of Standards and Technology (NIST) 800-22, Ent, DieHard, Practrand testleri bunlardan bazılarıdır (Akhshani, Behnia, Akhavan, Hassan ve Hassan, 2010; Camara, Peris-Lopez, Martín ve Aldalaien, 2018; Ergün ve Tanrıseven, 2018; Vaidyanathan, Akgul, Kaçar ve Çavuşoğlu, 2018). Tablo 3.1'de rasgele sayı üretimi ve istatistiksel testlere tabi tutulmasının algoritması gösterilmiştir.

Tablo 3.1. RSÜ sözde kodu

Algoritma: Rasgele Sayı Üretimi
Input: Kaotik sistem
Output: Rasgele sayılar
1: START Kaotik sistemim girilmesi
2: Kaotik işaretlerin binary sayı formatına dönüştürülmesi
3: Binary sayıların RSÜ için işleme tabi tutulması
4: Rasgele sayılar
5: IF (İstatistiksel testler) **THEN**
6: Başarılı
7: Adım 10'a git
8: ELSE (test results == false)
9: Adım 3'e git
10: END
11: EXIT

3.3.1. NIST-800-22 testi

NIST tarafından geliştirilen NIST 800-22 testi uluslararası standartlarda kabul görmüş olup on beş farklı aşamadan oluşan bir testtir. Teste tabi tutulacak sayının bit uzunluğu en az 1000000 bit uzunluğuna sahip olması gerekmektedir. Testin başarılı sayılabilmesi için her aşamada ürettiği P değerinin $P \geq 0,001$ şartını sağlaması gerekir (Koyuncu, 2014). Test tek bir aşamada bile geçemezse rasgele sayı üretimi başarısız sayılmaktadır. Aşağıdaki bölümlerde NIST 800-22 testinin alt basamakları ve P değerinin nasıl hesaplandığı hakkında bilgi verilmiştir.

Frekans testi: Bu tetstin amacı rasgele veri dizisi içersindeki 0 ve 1 sayılarının oranını incelemektir. Bu oranın hemen hemen aynı olması gerekir. Sonraki tüm testler bu testin geçmesine bağlıdır (Koyuncu, 2014).

Blok frekans testi: Tüm bit dizisini inceleyen Frekans testinin aksine Blok Frekans tetinde rasgele alınan m bitlik blok uzunluğuna sahip dizi içersindeki 0 ve 1 sayıları incelenmektedir. Teste tabi tutulacak dizinin blok uzunluğu n=20 ve bit uzunluğu en az

m=100 olarak alınması gerekmektedir. m bit uzunluğa sahip bir blok içersinde m / 2 oranında 1 bulunması gerekir (Koyuncu, 2014).

Akış testi: Bu test ile test edilen bit dizisi içersindeki ardışık 0 ve 1 bloklarına bakılır. 0 ve 1 değerlerinin yavaş veya hızlı bir şekilde gerçekleşen değişimleri değerlendirilir (Koyuncu, 2014).

Blok içinde en uzun bit yinelemesi testi: Bu testte ele alınan bloklar içersindeki ardışık bulunan en uzun 1 değerlerine bakılır. n bitlik bir dizi uzunluğu için seçilecek olan m blok uzunluğu, Tablo 3.2'de gösterildiği gibi olmalıdır (Koyuncu, 2014).

Tablo 3.2. Dizi uzunluğuna uygun önerilen blok uzunluğu

Minimum n	m
128	8
6272	128
750.000	100000

İkili matris rank testi: Bu teste orijinal rasgele sayı dizisi ile bu dizinin sabit uzunluktaki alt dizileri arasındaki doğrusal bağımlılığı kontrol edilir (Koyuncu, 2014).

Ayrık fourier dönüşümü testi: Bu testte rasgele sayı dizisinin ayrık fourier dönüşümündeki tepe noktaları incelenir. Amaç % 95 eşik noktasını geçen tepe sayısının % 5'ten ne oranda farklı olup olmadığını belirlemektir (Koyuncu, 2014).

Örtüşmeyen şablon eşleştirme testi: Bu testteki amaç; n bitlik veri uzunluğuna sahip rasgele sayı dizisindeki seçilen m bitlik bloklar içersinde, önceden belirlenen aperiyodik örnek dizilerin bulunma sıklığının incelenmesidir. Örnek dizi bloklarının tekrarı durumunda bir sonraki bloğun ilk bitinden devam edilir. Eğer örnek dizi bloklarına rastlanmazsa pencere bir bit ötelenerek arama devam ettirilir (Koyuncu, 2014).

Örtüşen şablon eşleştirme testi: Bu test de aynı bir önceki test ile aynı şekilde gerçekleştirilmektedir. Örtüşmeyan şablon eşleştirme testinden farklı olarak örnek dizi blokları tespit edilirse bir bit öteleme yapılarak arama devam eder (Koyuncu, 2014).

Maurer'in evrensel istatistik testi: Bu testte eşleşen modeller arasındaki bit sayısına bakılır. Testin amacı, bilgi kaybı olmadan dizinin önemli ölçüde sıkıştırılıp sıkıştırılamayacağını tespit etmektir. Önemli ölçüde sıkıştırılabilir bir dizinin rasgele olmadığı kabul edilir (Koyuncu, 2014).

Doğrusal karmaşıklık testi: Bu testte doğrusal geri besleme kaydırma yazmacının (LFSR) uzunluğuna bakılır. Amaç; dizinin rasgele olarak kabul edilebilecek kadar karmaşık olup olmadığını belirlemektir. Rasgele diziler daha uzun LFSR'ler ile karakterize edilir. Çok kısa olan bir LFSR rasgele olmama anlamına gelir (Koyuncu, 2014).

Seri testi: Bu testte rasgele sayı dizisi içersindeki herbir m bitlik örneğin diğer m bitlik örnekler ile benzerlik seviyesini incelemektir. Diğer testlerden farklı olarak bu testte iki farklı P değeri elde edilir (Koyuncu, 2014).

Yaklaşık entropi testi: Bu testte bir önceki test gibi tüm dizideki örtüşen m bitlik örneklerin frekansına (entropi) bakılır. İki ardışık blok (m ve m+1) frekansı ile rasgele sayı dizisi için beklenen frekans karşılaştırılır (Koyuncu, 2014).

Kümülatif (birikimli) toplamlar testi: Bu testdeki amaç, teste sokulan dizide meydana gelen kısmi dizilerin kümülatif toplamının, rasgele diziler için bu kümülatif toplamın beklenen davranışa göre çok büyük veya çok küçük olup olmadığını saptamaktır. Bu kümülatif toplam rasgele bir değişim olarak kabul edilebilir. Rasgele bir sıra için, rasgele değişimin sapmaları sıfıra yakın olmalıdır (Koyuncu, 2014).

Rasgele gezinimler testi: Bu testte rasgele bit dizisindeki ardışık bloklar içersindeki 0 ve 1 oranı belirlenir. Daha sonra bloklar arasındaki bu oranın dağılımına bakılır (Koyuncu, 2014).

Rasgele gezinimler değişken testi: Bu testte de bir önceki test gibi ardışık bloklar içersindeki 0 ve 1 oranı belirlenir. Bu oranın ortalama değerden sapma miktarına bakılır (Koyuncu, 2014).

3.3.2. FIPS 140-1 testi

FIPS 140-1 testi; monobit, poker, runs, long runs testleri olmak üzere dört aşamadan oluşmaktadır. Üretilen rasgele sayıların başarılı sayılabilmesi için bu dört testten de başarılı bir şekilde geçmesi gerekmektedir (Tuna ve Fidan, 2018; Uğur, 2005). FIPS 140-1 testi genellikle 20 Kbit gibi küçük boyutlu blok uzunluğuna sahip bit dizilerinin testinde kullanılmaktadır (Koyuncu, 2014).

Monobit testi: RSÜ tarafından üretilen 20 Kbit'lik bit dizisinin içerdiği 0 ve 1 değerlerinin dağılımına bakar. Dizinin içerdiği 1 değeri n ile ifade edilecek olursa, testin başarılı sayılabilmesi için $9654 < n < 10346$ şartının sağlanması gerekmektedir. Aksi durumda monobit testi geçersiz sayılır (Akgül, 2015; Sakallı, 2011).

Poker testi: Üretilen 20 Kbit'lik bit dizisi 5000 eşit parçaya bölünerek 4 bitlik değerler elde edilir. Bu 4 bit değerlerinin 16 farklı durumlarının değerleri tutulur. Denklem 3.1 ile X değeri elde edilir. $f(i)$, 4 bitin 16 farklı durumunu ifade eder. $1,03 < X \leq 57,4$ şartının sağlanmasıyla test sonucunun geçerli olduğu Kabul edilmektedir. Aksi durumda test geçersiz sayılacaktır (Özdemir, 2008).

$$X = \frac{16}{5000}\left(\sum_{i=0}^{15}\left[f(i)\right]^2\right) - 5000 \tag{3.1}$$

Runs testi: RSÜ'den elde edilen rasgele sayıların Runs testinden geçebilmesi için bit dizisi içersindeki ard arda gelen 0 ve 1 değerilerden oluşan farklı uzunluktaki bit değerlerinin belirli aralıklar içersinde olması gerekmektedir. Örneğin Tablo 3.3'te gösterildiği gibi blok uzunluğu 4 olursa $223 \leq x \leq 402$ şartının sağlanması gerekir. Burada bit dizisinin uzunluğu "x" ile ifade edilmektedir (Akgül, 2015; Sakallı, 2011).

Tablo 3.3. Run tetsi için blok uzunluklarına göre blok sayıları

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

Long Runs testi: Run test ile aynı olan bu testin tek farkı 20 Kbit'lik bit serisindeki 0 ve 1 lerden oluşan blokların toplam sayısı 34'ten küçük olmalıdır. Aksi taktirde test başarısız sayılacaktır.

3.4. Güvenlik Analizleri

Güvenlik analizlerini başarı ile geçen rasgele sayılar şifreleme işleminde kullanılmak için hazır hale gelir. Ancak bir verinin şifrelenme işleminde başarılı bir sonuç elde edilmesi sadece rasgele sayıların güvenilirliğine bağlı değildir. Aynı zamanda iyi bir şifrelme algoritmasına da ihtiyaç duyulmaktadır. Tablo 3.4'te bu tezde kullanılan görüntü şifreleme algoritmasının sözde kodu verilmiştir. Bu kod taslağına göre görüntünün şifrelenemesi Bölüm 5'te daha ayrıntılı bir şekilde anlatılacaktır.

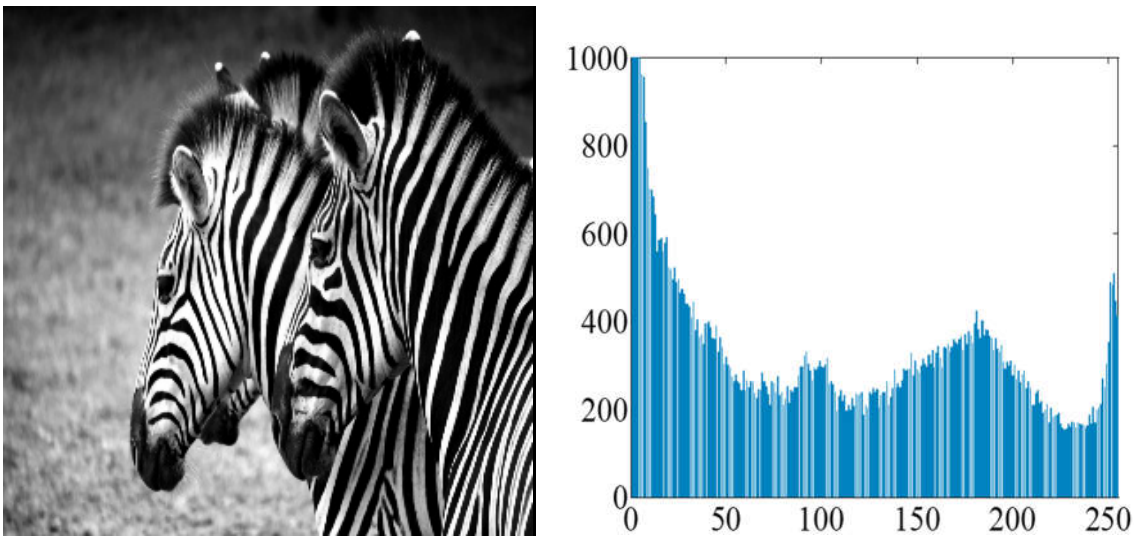
Tablo 3.4. Görüntü şifreleme sözde kodu

Algoritma: Görüntü şifreleme
Input: Kaynak görüntü
Output: Şifreli görüntü
1: START Resim ve rasgele sayıların girilmesi
2: Resmin boyutlarının belirlenmesi
3: Resmin piksel değerlerinin binary formata dönüştürülmesi
4: Rasgele sayılar ile resmin binary değerlerinin XOR işlemine tabi tutulması
5: Şifreli görüntünün elde edilmesi
6: EXIT

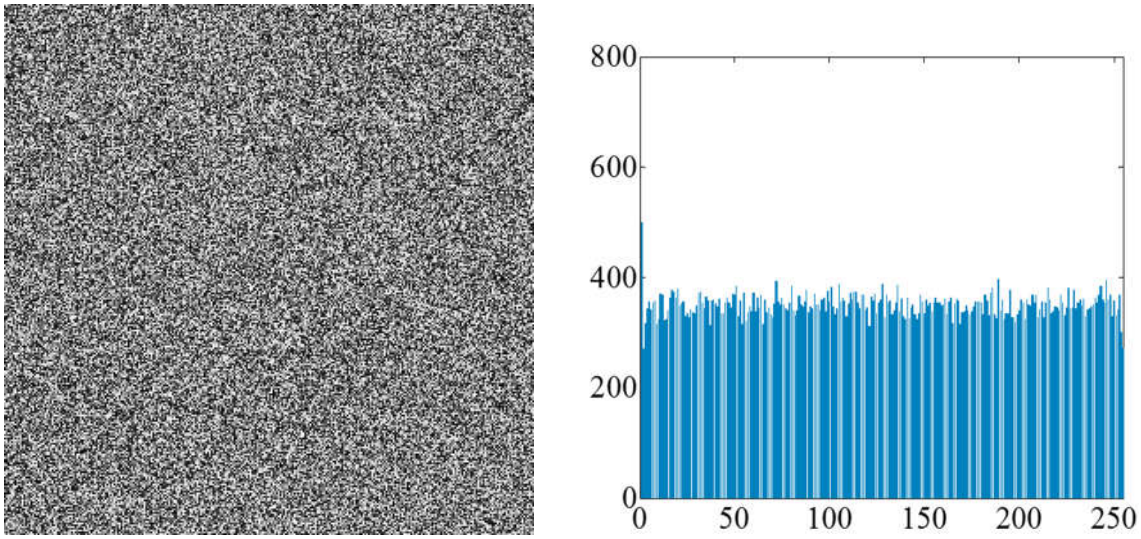
İyi bir şifreleme prosedürü her türlü kriptanalitik, istatistiksel ve güvenlik saldırılarına karşı dayanıklı olmalıdır. Bunun için literatürde görüntü şifreleme üzerine sunulan bazı güvenlik analiz yöntemleri vardır. Histogram analizi, korelasyon ve entropi hesabı, korelasyon haritaları, NPCR ve UACI analiz yöntemleri bunlardan birkaçıdır. (Kandar vd., 2019; Y. Liu, Tang, Liu, Zhang ve Ma, 2018; Sivakumar ve Li, 2019).

3.4.1. Histogram analizi

Histogram analizinde tekrarlı sayılardan oluşan bir veri dizisi içersinde hangi sayı değerlerinden kaç adet bulunduğu hakkında bilgi sahibi olunur. Histogram analizi birçok alanda kullanılabilmektedir. Şifrelemede ise şifreleme algoritmasının kalitesini değerlendirmede histogram analizlerinden yararlanılır. Şifreli bir görüntüden elde edilen veriler histogram grafiğinde birbirine ne kadar yakın olursa deşifre etme işlemi o kadar zorlaşacaktır (Akgül, 2015). Şekil 3.6'da bir resmin histogram analizi gösterilmiştir. Burada resmin histogramının çok düzensiz ve istatistiksel saldırılara karşı daha zayıf olduğu görülebilir. Diğer yandan Şekil 3.7'de gösterildiği gibi şifreli görüntünün histogramı oldukça düzgündür ve orijinal görüntünün ilgili histogramlarından önemli ölçüde farklıdır ve bu nedenle saldırganlara istatistiksel saldırı için herhangi bir ipucu sağlamaz (Mondal, Singh ve Kumar, 2019).



Şekil 3.6. Kaynak resim ve histogram analizi



Şekil 3.7. Şifreli resim ve histogram analizi

3.4.2. Entropi katsayısı

Entropi Ludwing Boltzmann tarafından tanımlanan, bir sistemin düzensizliğinin ölçüsüdür (Group, 2016). Entropi, rastlantısallığın en olağanüstü özelliğidir. Teori 1949'da Claude E. Shannon tarafından kurulan matematiksel bir veri iletişim ve depolama teorisidir (Akhshani vd., 2010). Entropi katsayısı Denklem 3.2'deki gibi hesaplanmaktadır. Burada H(s) kaynağın entropisini ifade eder. N bit değerini ifade eder. Örneğin 8 bitlik bir görüntü üzerinde çalışılıyorsa $2^8 - 1 = 255$ değerine kadar işlem yapılır. $P(s_i)$ ise s_i 'nin veri dizisi içersindeki olasılığını ifade eder. Literatürde şifreli resim için elde edilen en uygun entropi değeri 8 olarak kabul edilmektedir (Yavuz, Yazıcı, Kasapbaşi ve Yamaç, 2014)

$$H(s) = \sum_{i=0}^{2^N-1} P(S_i) \log_2 \frac{1}{P(S_i)} \tag{3.2}$$

3.4.3. Korelasyon katsayısı ve korelasyon haritaları

Bir görüntünün pikselleri arasında içsel özellik denilen yüksek bir korelasyon vardır. İstatistiksel saldırılar kriptanaliz gerçekleştirmede bu özellikden faydalanırlar. Bu yüzden güvenli bir şifreleme algoritması istatistiksel analize karşı direnci arttırmak için

korelasyonu kaldırmalıdır. Yani korelasyon değerinin mümkün olduğunca 0 değerine yakın çıkması istenmektedir (Akhshani vd., 2010). Yatayda, dikeyde ve diagonalde olmak üzere üç farklı şekilde bitişik pikseller arasında korelasyon hesabı yapılabilir. Aşağıdaki denklemlerde korelasyon katsayısının nasıl hesaplandığı gösterilmektedir. Denklem 3.3, Denklem 3.4 ve Denklem 3.5'teki x_i ve y_i gri scala formundaki resmin ardışık piksel değerlerini ifade etmektedir. Denklem 3.3'teki E_x, x'in matematiksel olasılıklarının ve Denklem 3.4'teki $D(x)$, x varyansının tahmini değerini ifade eder. Denklem 3.5'teki $cov(x, y)$, x ve y arasındaki kovaryansın tahmini değeridir. Denklem 3.6'daki r_{xy} değeri de korelasyon katsayısını ifade eder.

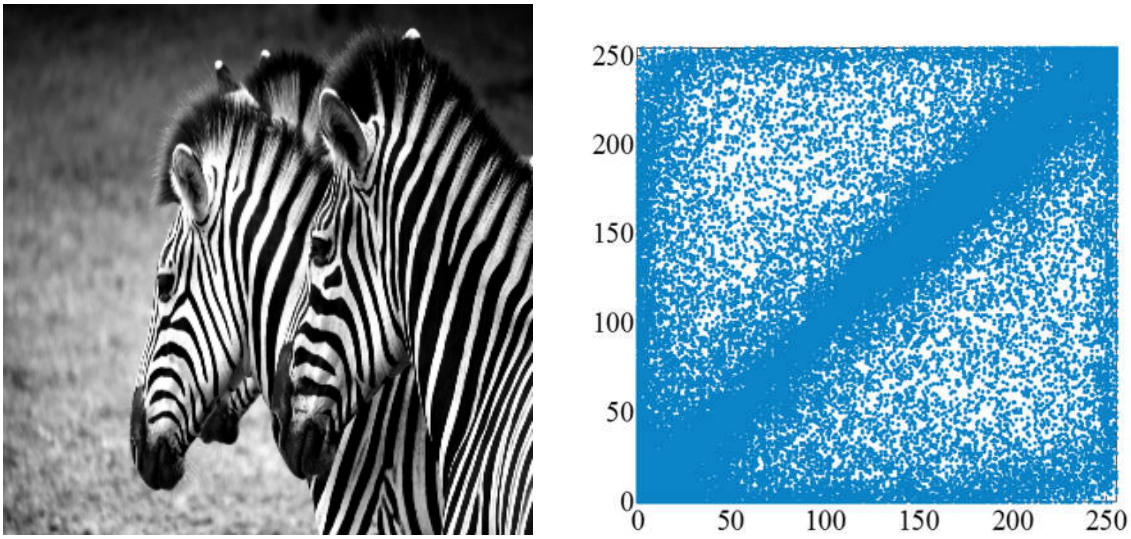
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{3.3}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{3.4}$$

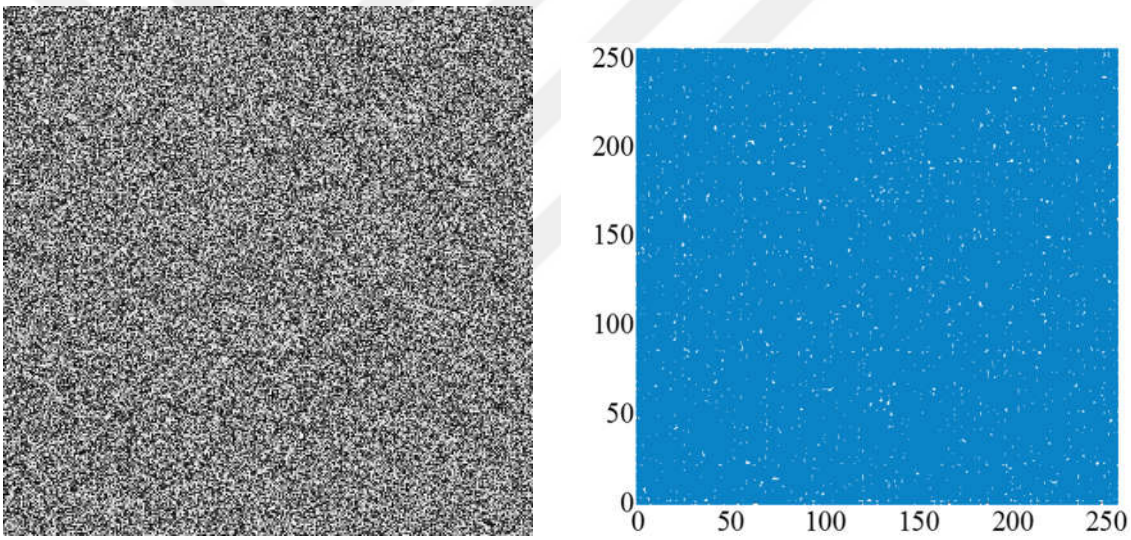
$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{3.5}$$

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D)(y)}} \tag{3.6}$$

Korelasyon haritaları dikey, yatay ve diagonal olmak üzere Bölüm 3.4.3'teki korelasyon katsayıları gibi üç farklı şekilde hasaplanabilmektedir. Her seferinde bir adım ötelenerek iki piksel değeri karşılaştırılır. Karşılaştırılan piksellerin kesim noktası korelasyon haritasında işaretlenir. Bu şekilde tüm pikseller taranarak korelasyon haritası ortaya çıkartılır. Şekil 3.8'deki gibi şifrelenmemiş bir görüntünün korelasyon haritasına baktığımızda diaogonalde bir yoğunlaşma görülürken Şekil 3.9'daki gibi şifreli bir görüntünün korelasyon haritasına baktığımızda homojen bir dağılım gözlemlenir (Sivakumar ve Li, 2019).



Şekil 3.8. Kaynak resim ve korelasyon haritası



Şekil 3.9. Şifreli resim ve korelasyon haritası

3.4.4. NPCR ve UACI analizleri

Değişen piksel oranını ifade eden NPCR (Number of pixel change rate) ve birleşik ortalama değiştirilmiş yoğunluğu ifade eden UACI (Unified average changing intensity) sayısı, diferansiyel ataklara göre görüntü şifreleme algoritmalarının ve şifrelerinin gücünü değerlendirmek için kullanılan en yaygın iki istatistiktir. Bir diğer ifade ile NPCR tüm piksellerin % kaçının değiştiğini ifade ederken, UACI değeri ise piksellerin % kaç oranında değiştiğini göstermektedir. Yüksek bir NPCR ve UACI değeri, genellikle diferansiyel ataklara karşı yüksek direnç olarak yorumlanır. Bununla birlikte, NPCR ve

UACI'nın her zaman yüksek olması, doğrudan görüntü şifresinin gerçekten de yüksek bir güvenlik seviyesine sahip olduğu hakkında net bir bilgi vermeyebilir (Kandar vd., 2019; Wu ve Agaian, 2011). Önceki çalışmalara bakıldığında NPCR'nin %99,6'dan büyük UACI değerinin ise %30'a yakın ya da büyük bir değerde olması şifreleme işleminin başarılı bir şekilde gerçekleştiğinin göstergesi olarak kabul edilmektedir (Praveenkumar, Amirtharajan, Thenmozhi ve Rayappan, 2015).

Aşağıdaki denklemlerde UACI ve NPCR değerlerini hesaplamada kullanılan formüller verilmiştir (Chen, Zhu, Fu, Yu ve Zhang, 2015). Denklem 3.7 ve Denklem 3.9'daki M kaynak görüntünün toplam satır sayısını, N kaynak görüntünün toplam sütun sayısını, Denklem 3.8'deki C_1 kaynak görüntünün piksel değerini, C_2 şifreli görüntünün piksel değerini ifade eder.

$$NPCR = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} Dif(i,j) \times 100\% \tag{3.7}$$

$$Dif(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, C_1(i,j) = C_2(i,j) \end{cases} \tag{3.8}$$

$$UACI = \frac{1}{MN}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |C_1(i,j) - C_2(i,j)|}{255} \times 100\% \tag{3.9}$$

BÖLÜM 4. YENİ KAOTİK SİSTEM TASARIMI VE DİNAMİK ANALİZLERİ

4.1. Yeni Kaotik Sistem Tasarımı

Bu bölümde yeni bir kaotik sistem elde edilmiş ve bu sistemin dinamik analizleri Matlab programı yardımıyla yapılmıştır. Denklem 4.2'de gösterilen yeni kaotik sistemin türetilmesinde Denklem 4.1'de (Jafari vd., 2017) bulunan kaotik sistemden faydalanılmıştır.

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= -x + y.z \\ \dot{z} &= -x - 15.x.y - x.z \end{aligned} \tag{4.1}$$

$$\begin{aligned} \dot{x} &= a.y \\ \dot{y} &= -x + b.y.z \\ \dot{z} &= -x - c.x.y - d.x.z \end{aligned} \tag{4.2}$$

Yeni üretilen kaotik sistemin başlangıç şartları $x_0 = 0,4$, $y_0 = 0,1$, $z_0 = 0$ ve parametre değerleri $a = 1,9$, $b = 1,1$, $c = 11,5$, $d = 0,7$ olarak seçilmiştir. Sonraki bölümlerde yeni kaotik sistemin dinamik analizleri yapılmıştır.

4.2. Yeni Kaotik Sistem Dinamik Analizleri

Bu bölümde yeni tasarlanan kaotik sistemin kaotik davranışlarını analiz etmek için; denge noktaları, faz portreleri, zaman serileri, Lyapunov üstelleri ve boyutu, çatallanma diyagramı, FFT ve Poincare kesiti gibi bazı dinamik analizleri incelenmiştir.

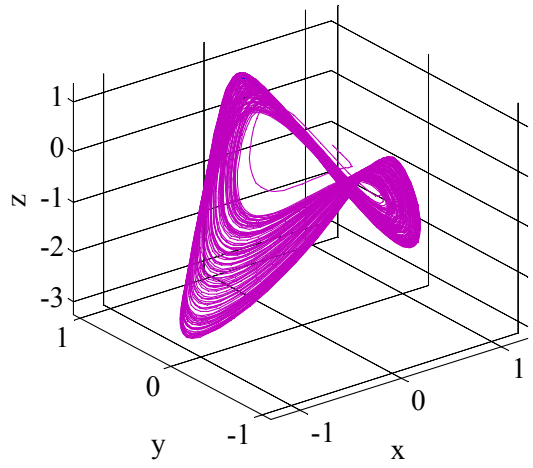
4.2.1. Denge noktaları ve kararlılık analizi

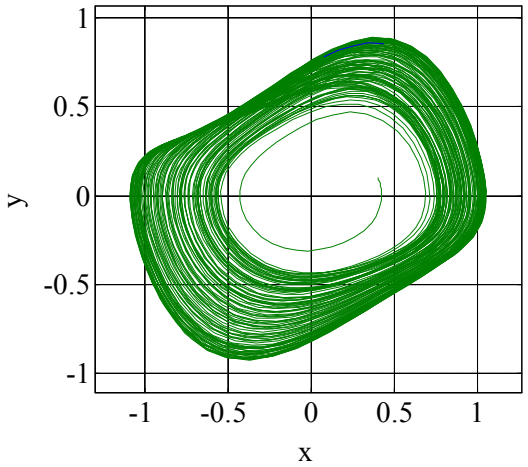
Denklem 4.2'deki yeni kaotik sistemin türevi sıfıra eşitlenerek çözdürüldüğünde (Denklem 4.3) kesin bir çözüm sonucu elde edilememektedir. Bu yüzden sistem denge noktasız bir sistemdir ve Şekil 4.1'de gösterilen kaotik çekerler gizli kaotik çekerler olarak adlandırılmaktadır (Wang, Hu, Han ve Cang, 2016).

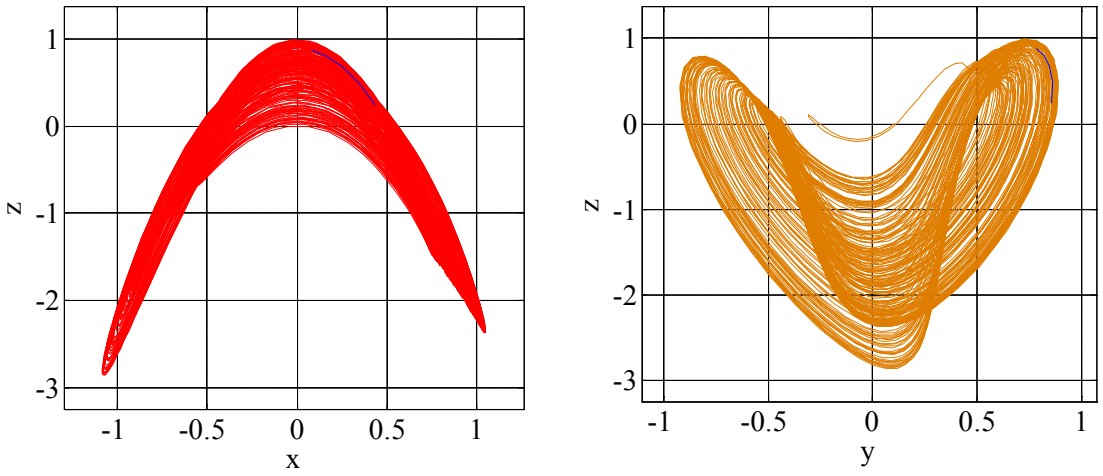
$$\begin{aligned} 0 &= 1,9y \\ 0 &= -x + 1,1yz \\ 0 &= -x - 11,5xy - 0,7xz \end{aligned} \tag{4.3}$$

4.2.2. Faz portreleri (Faz uzayı) ve zaman serileri

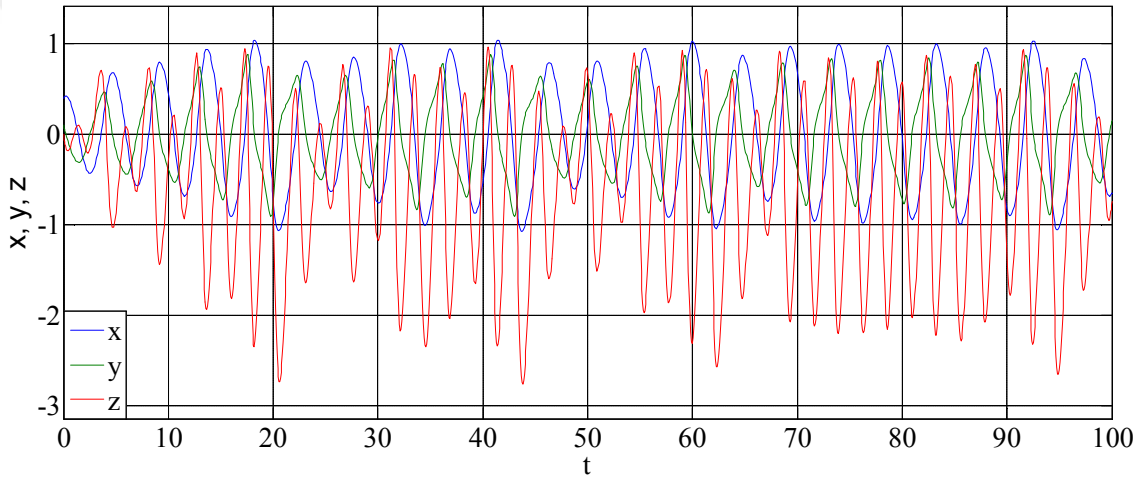
Yeni üretilen kaotik sistemin başlangıç şartları $x_0 = 0,4$, $y_0 = 0,1$, $z_0 = 0$ ve parametre değerleri $a = 1,9$, $b = 1,1$, $c = 11,5$, $d = 0,7$ olarak seçildiğinde Matlab programı yardımıyla Şekil 4.1'deki x-y-z, x-y, x-z, y-z faz portreleri ve Şekil 4.2'deki x-y-z zaman serileri elde edilmiştir. Şekillerden de görüldüğü üzere yeni kaotik sistem zengin dinamik davranışlar sergilemektedir. Bu sebeple faz portrelerine bakıldığında sistemin kaotik olduğu söylenebilir. Ancak kaotiklik hakkında kesin bir kanıya varmak için gelecek bölümlerdeki analiz yöntemlerine de bakılmasında fayda vardır.







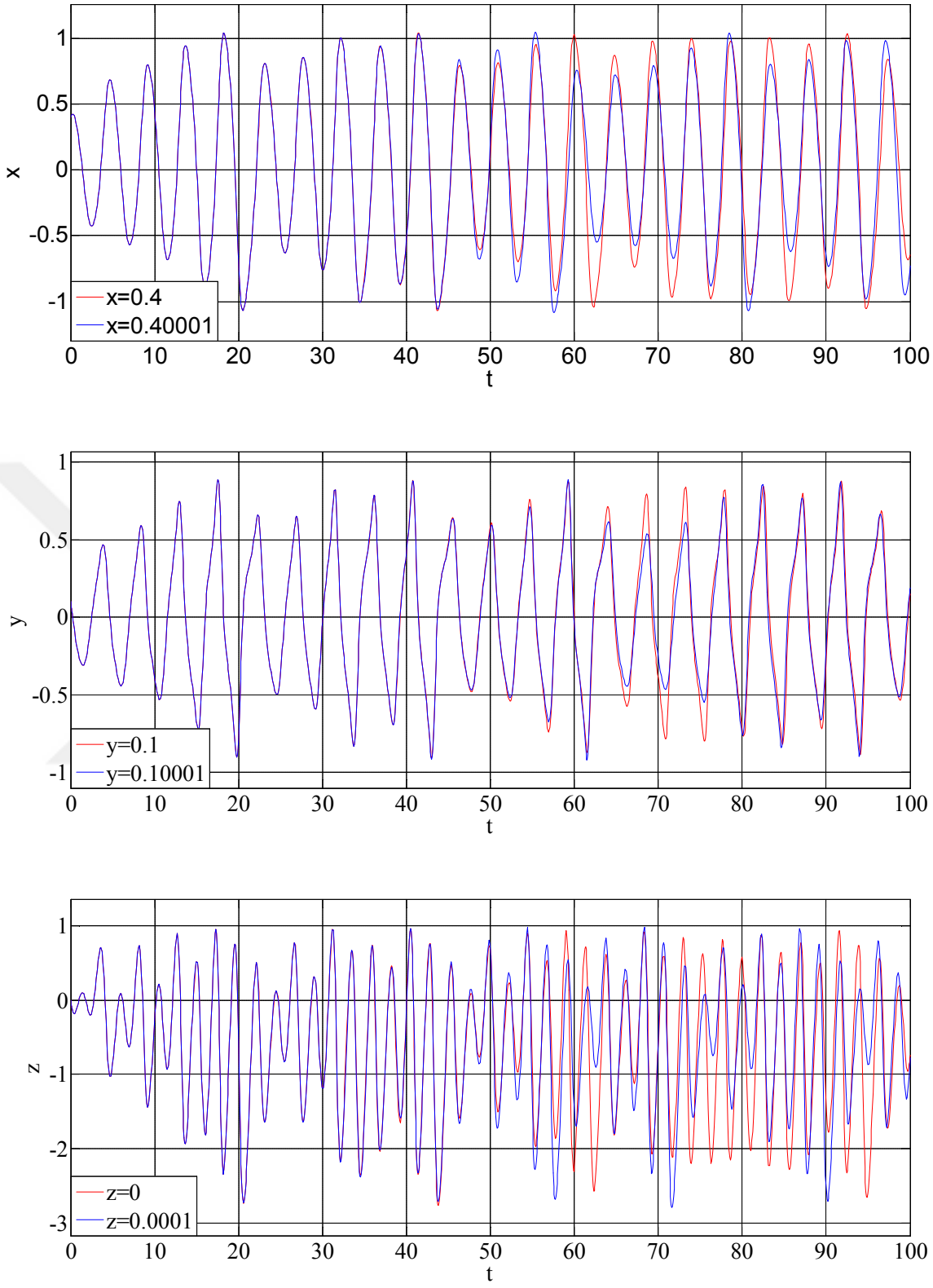
Şekil 4.1. Yeni kaotik sistemin faz diyagramları



Şekil 4.2. Yeni kaotik sistemin zaman serileri

4.2.3. Zaman serisinde başlangıç şartlarına hassas bağımlılık

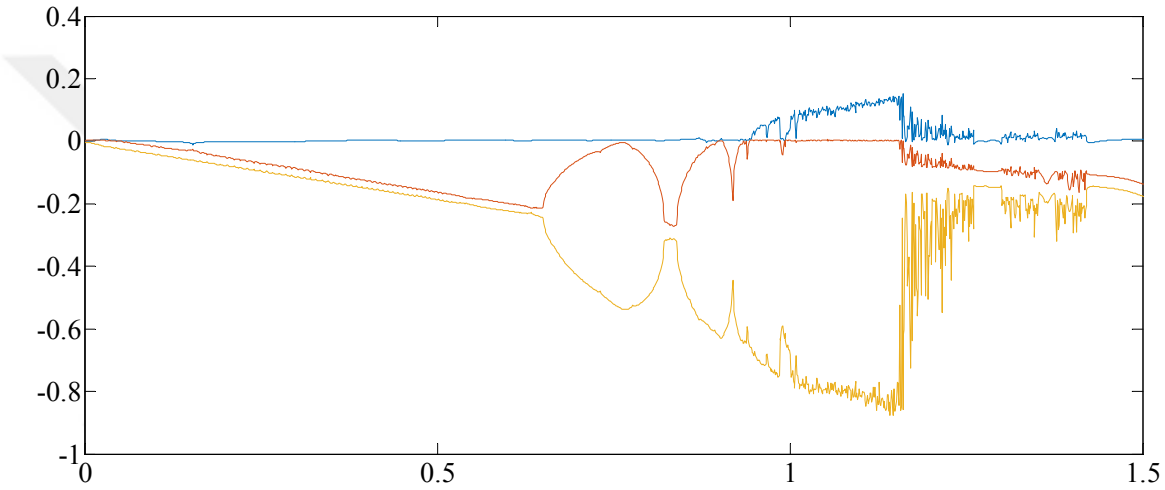
Bir sistemin başlangıç şartlarına karşı hassas bir şekilde bağımlı olması kaotiklik hakkında bilgi vermektedir. Şekil 4.3'te yeni sistemin x-y-z fazlarının herbiri ayrı ayrı incelenerek başlangıç şartlarına bağımlılıkları incelenmiştir. Şekillerden de görüldüğü üzere başlangıç şartlarındaki 1/100000'lik bir değişim sistemin çıktısında farklılıklara yol açmaktadır. Örneğin Şekil 4.3 (a)'da x fazının başlangıç değerine karşı olan hassas bağımlılığı Matlab ile çizilen bir grafik ile gösterilmiştir. t = 40'dan itibaren sistemin zaman serilerinde farklılaşmalar görülmeye başlamıştır. Buradan da sistemin kaotik bir davranış sergilediği anlaşılmaktadır.



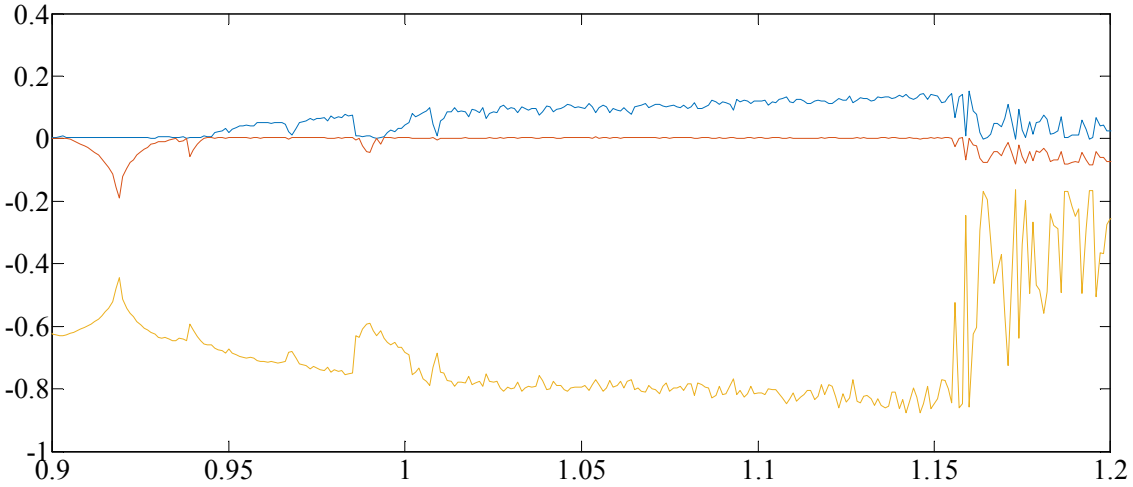
Şekil 4.3. Yeni kaotik sistemin sırası ile x, y, z fazlarındaki başlangıç şartlarına olan hassas bağımlılık

4.2.4. Lyapunov üstelleri ve boyut analizi

Şekil 4.4'teki Lyapunov üstellerinin incelendiği grafiğe bakıldığında yeni sitemin kaotik bir hal sergilediği görülmektedir. Burada "b" parametresine göre $0-1,5$ aralığında Lyapunov üstel spektrum analizi yapılmıştır. Sistemin kaotikliği Lyapunov üstellerine göre incelendiğinde kaotik olabilmesi için değerlerin $+, 0, -$ şeklinde olması gerekmektedir. Şekil 4.5'te daha da detaylı bakıldığında sistemin yaklaşık olarak $0,95-1,15$ aralığında kaotik bir davranış sergilediği görülmektedir.



Şekil 4.4. Yeni kaotik sistemin 'b' parametresine göre yapılan Lyapunov spaektrum analizi (0-1.5)



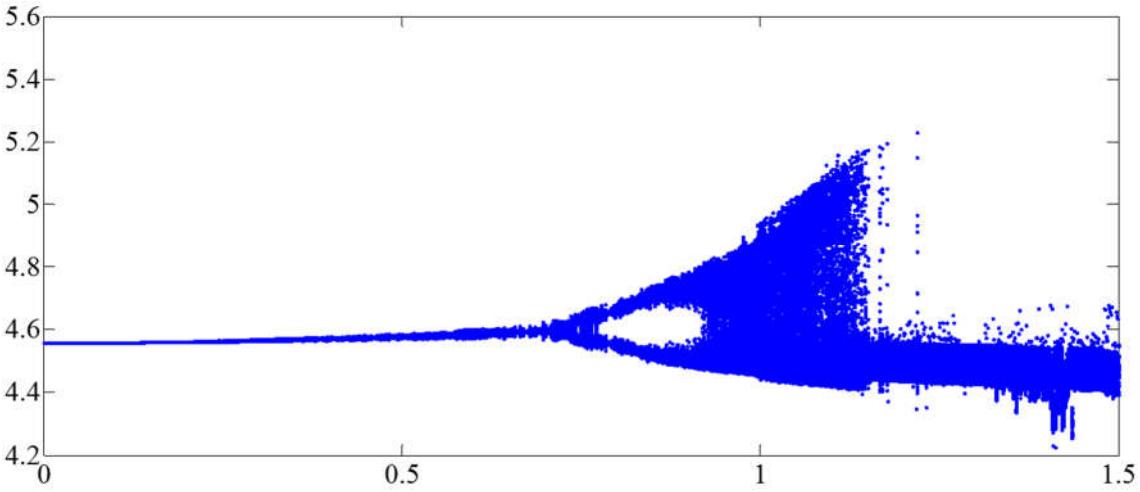
Şekil 4.5. Yeni kaotik sistemin 'b' parametresine göre yapılan Lyapunov analizi (0-1.5)

Yeni türetilen denklem 4.2'deki kaotik sistemin Lyapunov üstelleri sırası ile $\lambda_1 = 0{,}12448$, $\lambda_2 = -0{,}00014555$, $\lambda_3 = -0.82275$ olarak elde edilmiştir. Denklem 4.4'te Lyapunov değerleri yerine yazıldığında Lyapunov boyutu $D = 2{,}1511$ olarak elde edilmektedir. $2 < D < 3$ şartı sağlandığından dolayı Lyapunov boyutuna bakarak sistemin kaotik olduğu söylenebilmektedir.

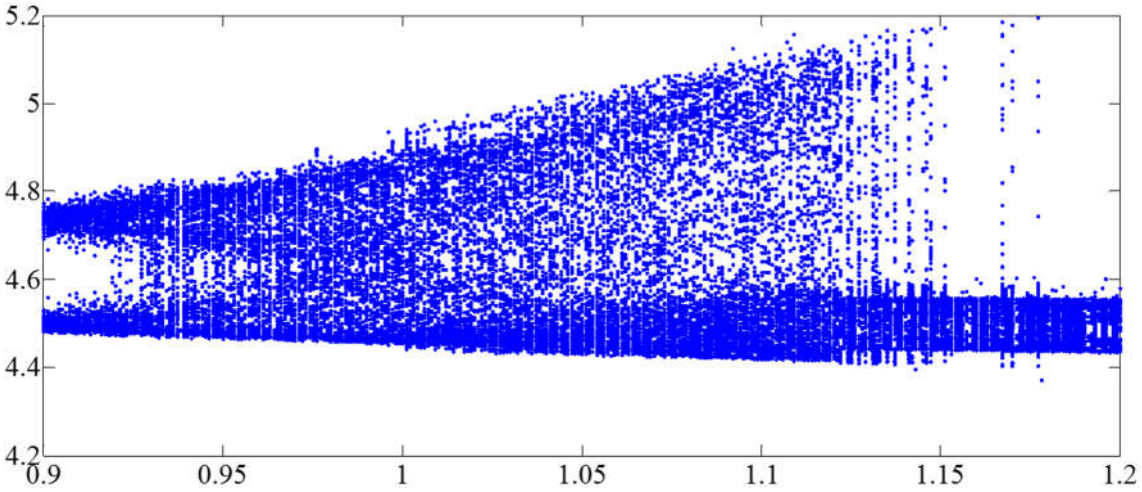
$$D = 2 + \frac{\lambda_1 + \lambda_2}{|\lambda_3|} \tag{4.4}$$

4.2.5. Çatallanma diyagramı

Çatallanma analizi ve (Çavuşoğlu vd., 2017) Lyapunov spektrum analizlerinden elde edilen grafiklerde kaotiklikden bahsedebilmemiz için aynı aralıklarda aynı sonuçlar elde edilmelidir. Şekil 4.6'da sistemin $0-1{,}5$ aralığında çatallanma grafiği gösterilmiştir. Bölüm 4.2.4.'te yapılan Lyapunov analizleri ile Şekil 4.6'da elde edilen çatallanma sonuçları aynı aralıklar içersinde uyuşmaktadır. Şekil 4.7'de $0{,}95-1{,}15$ aralığında ayrıntılı inceleme yapıldığında bu daha da net görülebilmektedir.



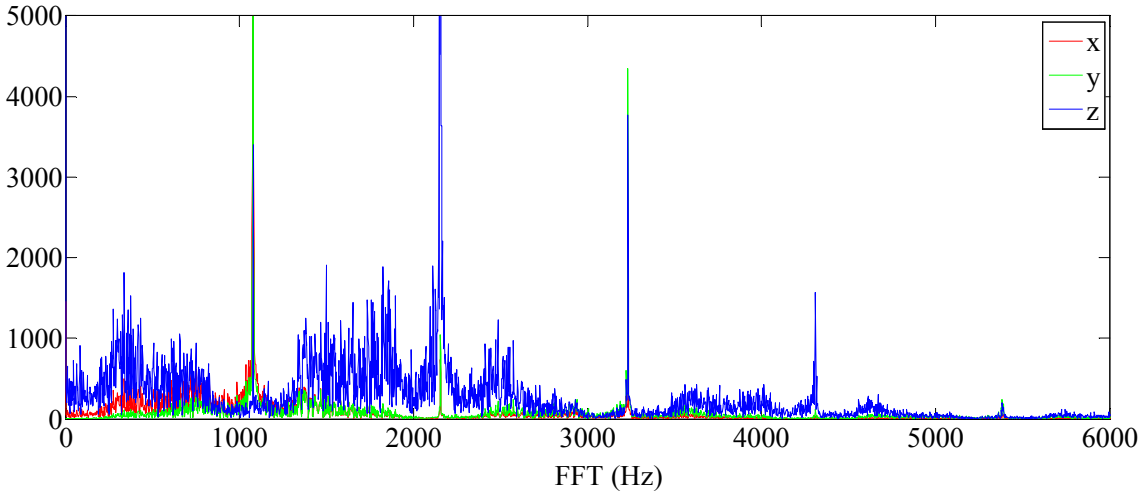
Şekil 4.6. Yeni kaotik sistemin 'b' parametresine göre yapılan çatallanma analizi (0-1.5)



Şekil 4.7. Yeni kaotik sistemin 'b' parametresine göre yapılan çatallanma analizi (0.8-1.3)

4.2.6. FFT (Fast Fourier Tranform) analizi

FFT analizinde sistemin çıkış sinyalleri incelenmektedir. Şekil 4.8'de yeni kaotik sistemin FFT analizleri gösterilmiştir. Şekil 4.8'de görüldüğü üzere görüldüğü üzere sistem 3 KHz'den fazla frekans spektrumuna sahiptir. Ve ayrıca bant genişliği yüksek olduğundan rasgelelik ve karmaşıklığı da yüksekdir. Böylece sistem kaotiktir denilebilir.

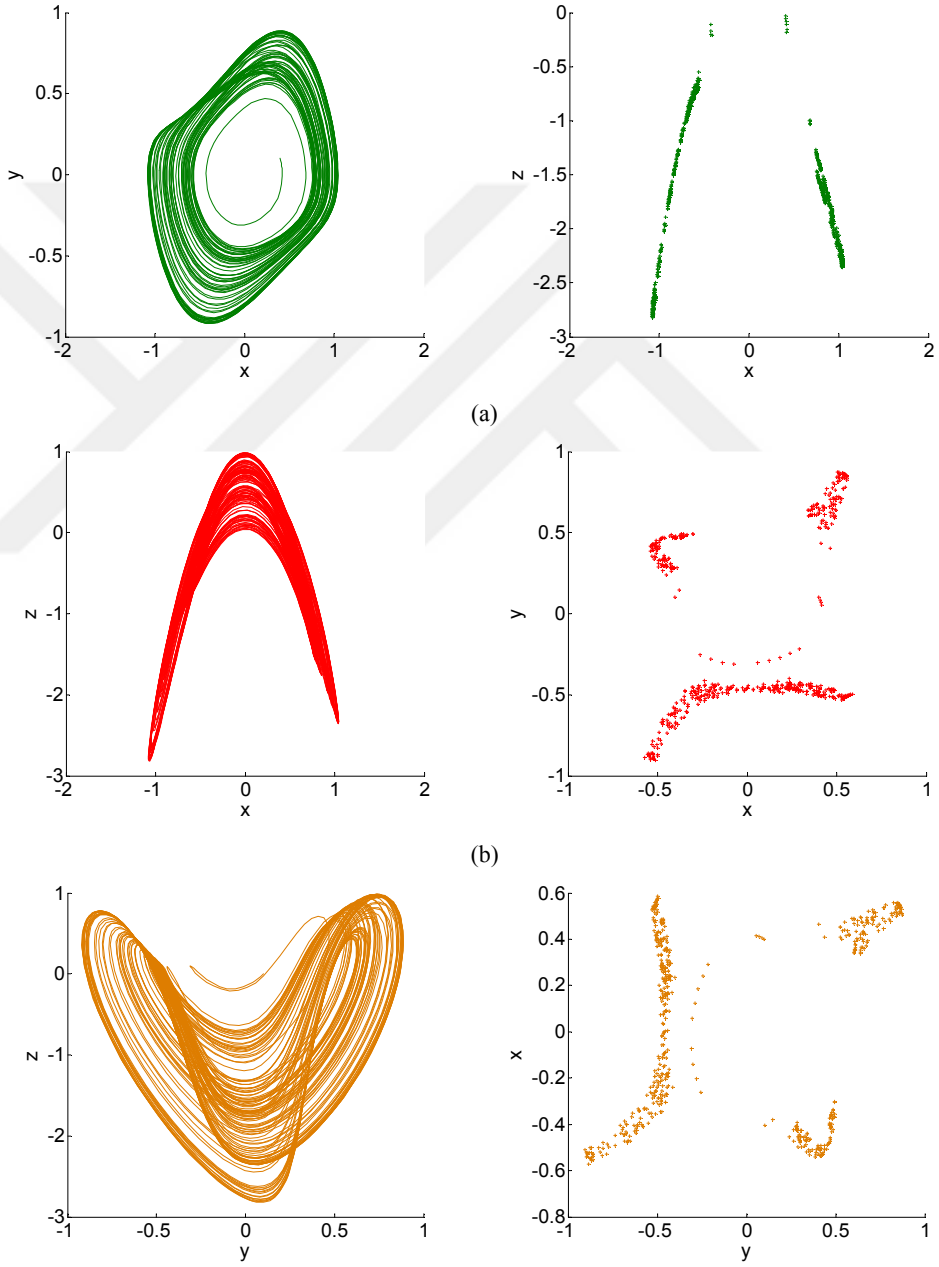


Şekil 4.8. Yeni kaotik sistemin x, y, z değişkenlerinin FFT analizi

4.2.7. Poincare kesiti

Poincare kesit analiz yöntemi ile kaotik sistemin faz portrelerinden kesit alınarak görüntüler elde edilmiştir. Poincare kesitlerindeki noktasal dağılımın belirli sınırlar

içersinde yoğunlaşması sistemin kaotikliğinden bahsedebilmemizi sağlamaktadır. Şekil 4.9'da görüldüğü üzere x-y, x-z ve y-z faz portrelerinden alınan kesitlerde aynı faz portreleri sınırları içersinde noktasal yoğunluk görülmektedir. Bu sistemin kaotik olduğunun bir kanıtıdır. Örneğin x-y faz portresinde y boyutundan x boyutuna paralel olarak bir kesit alıp bu kesite x-z izdüşümünden baktığımızda oluşacak görüntü hemen yanındaki x-z Poincare kesiti gibi olacaktır.

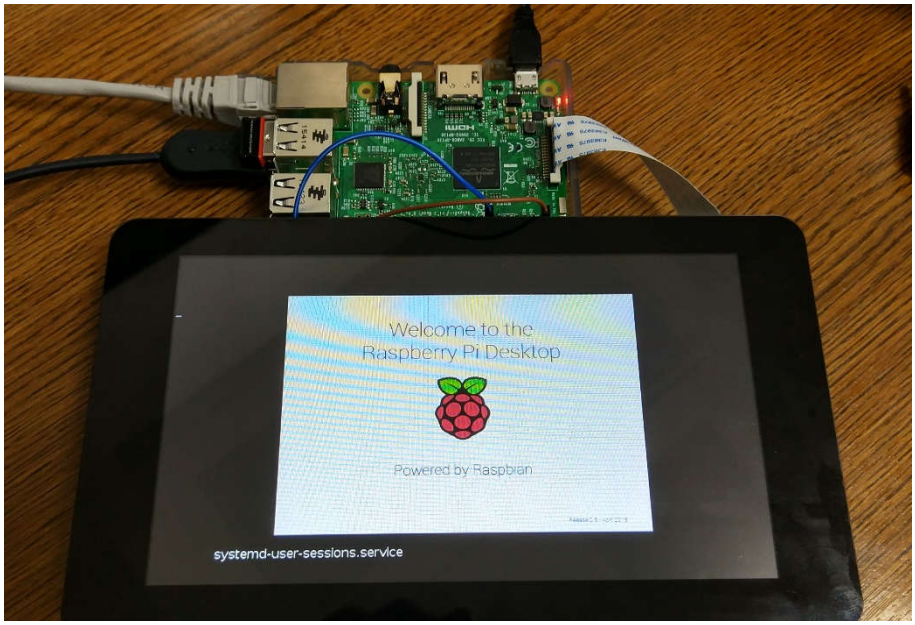


Şekil 4.9. Yeni kaotik sistemin sırası ile x-y (a), x-z (b), y-z (c) çekerlerinin Poincare kesitleri

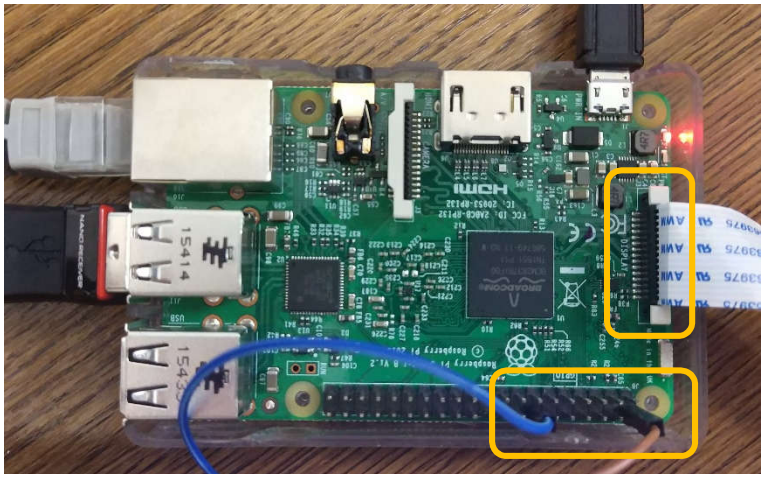
BÖLÜM 5. MOBİL RASGELE SAYI ÜRETEÇ TASARIMI VE İSTATİSTİKSEL TESTLER

5.1. Mobil Rasgele Sayı Üreteç Tasarımı

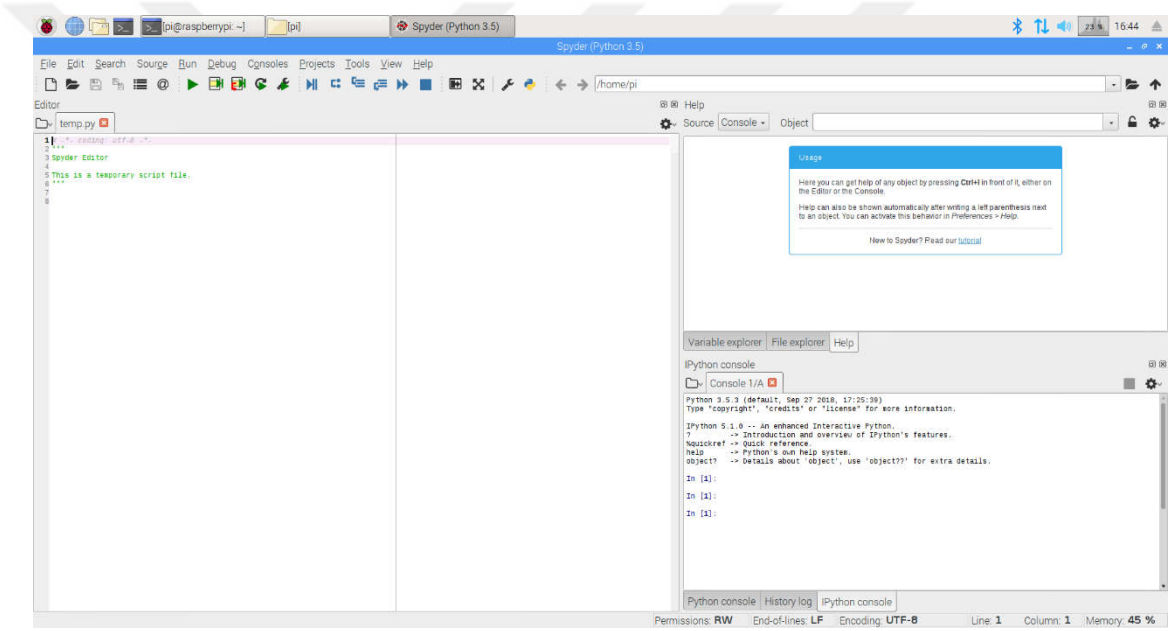
Bu bölümde tezde yapılan RSÜ tasarımından bahsedilmiştir. Rasgele sayı üretiminde tüm işlemlerde mikrobilgisayar olarak Raspberry Pi 3 Model B kullanılmıştır. Şekil 5.1'de görüldüğü üzere Raspberry Pi 3 Model B'nin masaüstüne erişim doğrudan dokunmatik ekran aracılığıyla sağlanmıştır. Dokunmatik ekranın +5V ve GND uçları Raspberry pinlerinden beslenerek ve dokunmatik ekranın kablosu Raspberry üzerinde ayrılmış olan ekran soketine girişi yapılarak kolay bir şekilde dokunmatik ekran bağlantısı yapılmış olur (Şekil 5.2). İlave bir yazılımsal ayar gerektirmez. Programlama dili olarak Python dili kullanılırken, programlama arayüzü olarak da kullanıcıya sağladığı imkânlardan dolayı da Spyder programından yararlanılmıştır (Şekil 5.3).



Şekil 5.1. Raspberyy Pi 3 Model B masaüstü erişimi



Şekil 5.2. Raspberyy Pi 3 Model B dokunmatik ekran bağlantı



Şekil 5.3. Spyder programı arayüzü

Şekil 5.7'de RSÜ tasarımında izlenen yolun blok diyagramı gösterilmiştir. Algoritmayı inceleyecek olursak ilk olarak yeni kaotik sistem belirlendikden sonra başlangıç şartları ve sistem parametreleri girilir (Şekil 5.4). Sonrasında Runge Kutta-4 (RK4) çözüm metodu (Şekil 5.5) için gerekli olan adım aralığı girildikden sonra sistem x-y-z fazlarında ayrık zamanlı hale getirilerek float değerler elde edilir. Float değerler 32 bit binary forma getirilir ve bu 32 bitlik sayıların hangi LSB (Least significant bit) bitinde işlem yapılacağı seçilir. Şekil 5.6'daki 32 bitlik sayılara bakacak olursak 0. bit değerine doğru gidildikçe değerler aynı çıkmaya başlamaktadır. Sonlara doğru ise birbirinden bağımsız daha farklı değerler çıktığı görülmektedir. Bu yüzden bit seçiminin son bitlerden yapılması daha

yararlı olmaktadır. Ancak seçimin çok küçük, örneğin son 4 bit seçimi yapmak diğer taraftan süreyi uzatacaktır. Bu sebeple burada s = 8 (LSB) bit olarak seçilmiştir. Her bir fazdan elde edilen 8 bit değerler birleştirilerek 1.000.000 bit uzunluğuna sahip bir rasgele sayı dizisi elde edilmiştir. Son işlem olarak da bu veri dizisi NIST ve FIPS testlerine tabi tutulmuşlardır. Eğer başarılı sonuçlar elde edilmezse seçilen LSB bitlerinde değişim yapılarak işlem tekrarlanır.

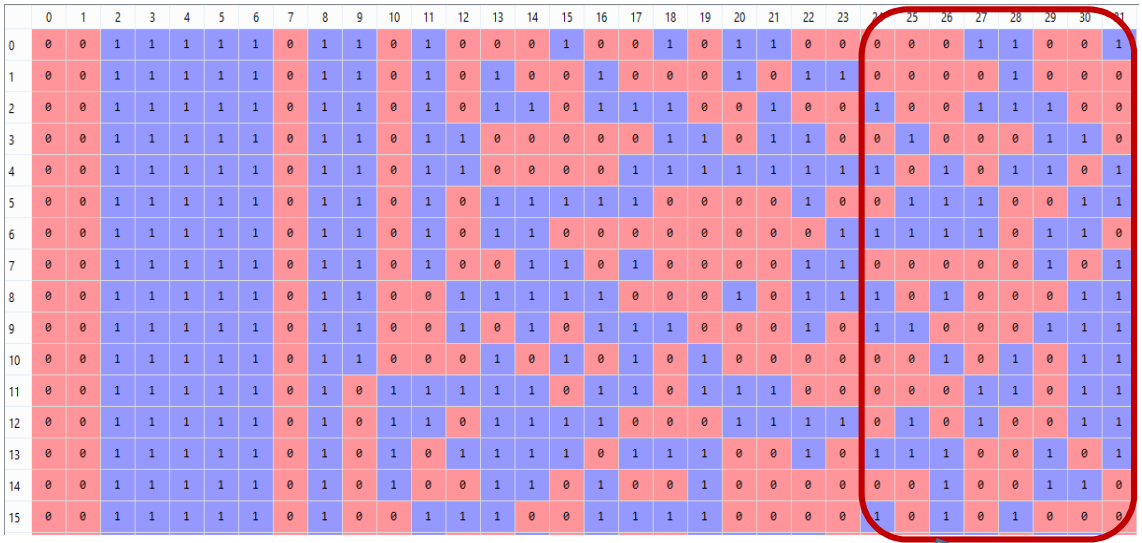
```
def kaos (t,y):
    yp= 1.9*y[1],-y[0]+1.1*y[1]*y[2],-y[0]-11.5*y[0]*y[1]-0.7*y[0]*y[2]
    return yp

y0 = [0.4,0.1,0];
adim_sayisi=100000;
bit = 8;
```

Şekil 5.4. Kaotik denklem program kesiti

```
for time in range(0,adim_sayisi, 1):
    print(time)
    ye = y0
    k1 = kaos(time, y0);
    k2=  kaos(time+0.5*h, y0+0.5*np.inner(k1,h));
    k3=  kaos(time+0.5*h, y0+0.5*np.inner(k2,h));
    k4=  kaos(time+h,y0+np.inner(k3,h));
    ys = y0 + (1/6)*np.inner(k1,h) + (1/3)*np.inner(k2,h)+(1/3)*np.inner(k3,h)+(1/6)*np.inner(k4,h)
    y0 = list(ys);
```

Şekil 5.5. RK4 program kesiti

x-y-z fazlarından elde edilen rasgele sayıların dönüşümü Şekil 5.6'da daha ayrıntılı bir şekilde incelenmiştir. Şekil 5.6 (b)'de x fazından RK4 çözümü ile elde edilen float değerlerin ilk 15 değeri gösterilmiştir. Daha sonra tüm bu değerler Şekil 5.6 (a)'da gösterildiği gibi 32 bitlik binary formata dönüştürülmektedir. LSB biti olarak s daha hassas olacağı düşünüldüğünden 8 bit olarak seçildiği için her bir 32 bitlik binary değerlerin son 8 biti alınarak Şekil 5.6 (c)'de görüldüğü gibi 8 bitlik verilerden oluşan ayrı bir dizi oluşturulur. Oluşturulan bu 8 bitlik verilerin her biri art arda eklenerek toplamda 1000000 bit uzunluğa sahip bir rasgele sayı elde edilmiş olur.



(a)

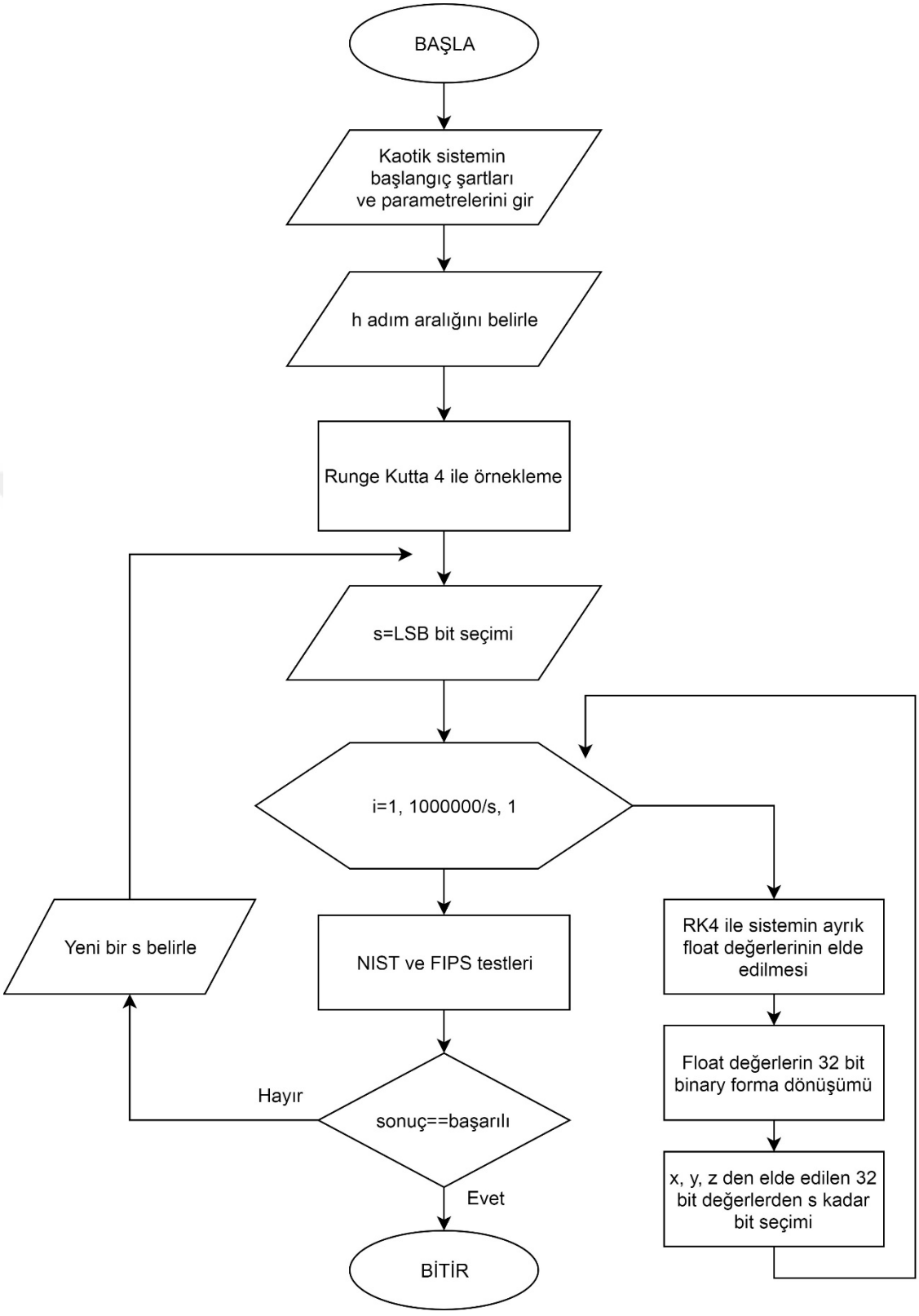
	0
0	0.40854
1	0.415123
2	0.419713
3	0.422289
4	0.422849
5	0.421405
6	0.417984
7	0.412621
8	0.405362
9	0.396261
10	0.385377
11	0.372773
12	0.358515
13	0.342673
14	0.325319
15	0.306524

(b)

	0	1	2	3	4	5	6	7
0	0	0	0	1	1	0	0	1
1	0	0	0	0	1	0	0	0
2	1	0	0	1	1	1	0	0
3	0	1	0	0	0	1	1	0
4	1	0	1	0	1	1	0	1
5	0	1	1	1	0	0	1	1
6	1	1	1	1	0	1	1	0
7	0	0	0	0	0	1	0	1
8	1	0	1	0	0	0	1	1
9	1	1	0	0	0	1	1	1
10	0	0	1	0	1	0	1	1
11	0	0	0	1	1	0	1	1
12	0	1	0	1	0	0	1	1
13	1	1	1	0	0	1	0	1
14	0	0	1	0	0	1	1	0
15	1	0	1	0	1	0	0	0

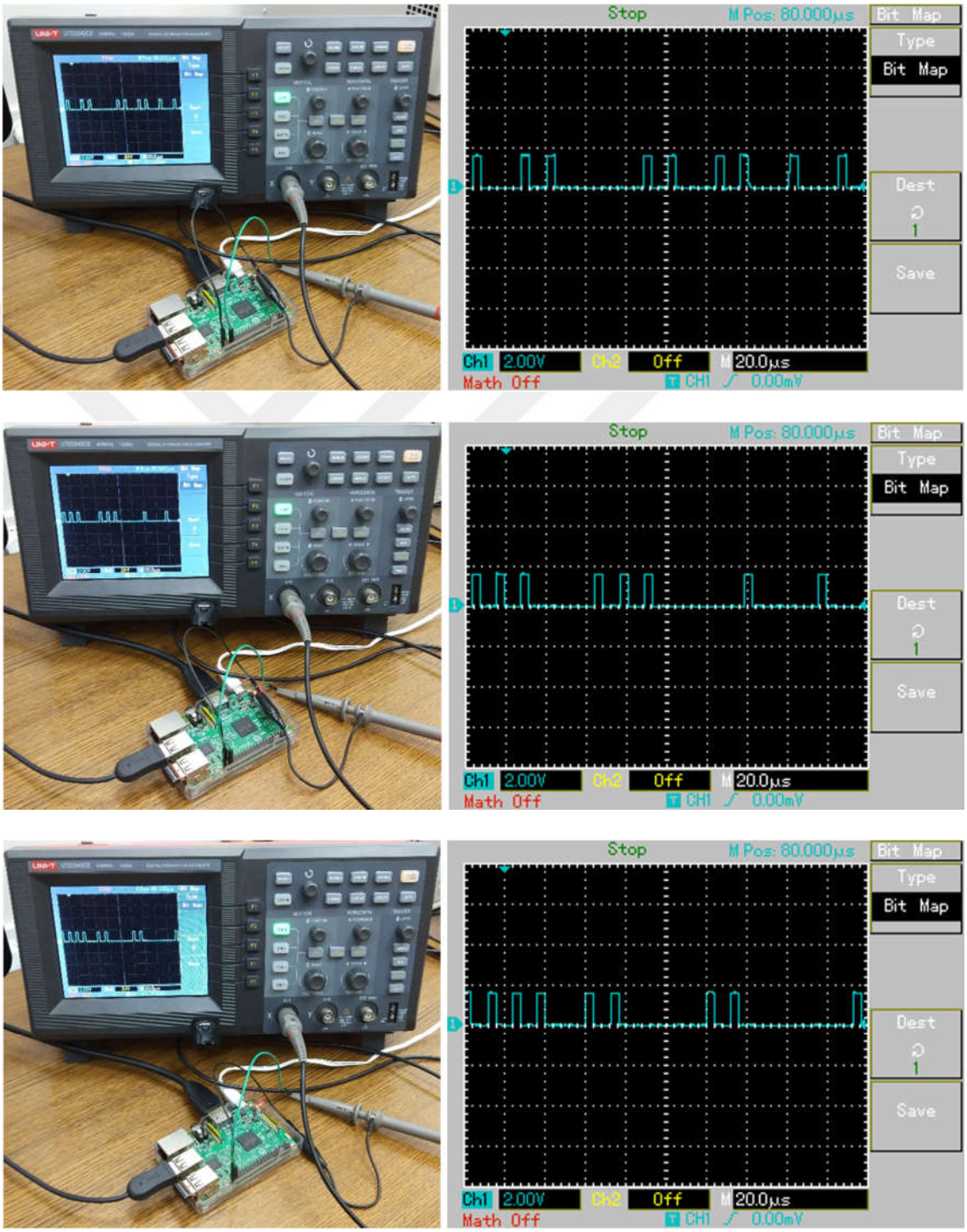
(c)

Şekil 5.6. x boyutundan çözümlenen float sayıların binary sayı formatına dönüşümü



Şekil 5.7. Yeni kaotik sistem RSÜ algoritması

Şekil 5.8'de x-y-z fazlarından elde edilen rasgele sayıların gerçek hayatta herhangi bir uygulamada kullanılabileceğini göstermek adına Raspberry Pi 3 Model B kullanılarak elde edilen osilaskop görüntüleri verilmiştir.



Şekil 5.8. Sırası ile x-y-z fazlarından elde edilen rasgele sayıların osilaskop çıktıları

5.2. RSÜ İstatistiksel Testleri

5.2.1. NIST 800-22 testi

NIST 800-22 testi ulusal düzeyde kabul gören bir rasgele sayı test edicisidir. Kendi içersinde 16 farklı testten oluşur ve sayının rasgeleliğinden söz edebilmek için bu 16 testin hepsinden başarılı bir şekilde geçmesi gerekir. Her bir aşamada test sonuçları P çıktısına göre değerlendirilir. Her bir test aşamasında $P \geq 0,001$ şartı sağlandığı sürece test sonucu başarı sayılır. Tablo 5.1'de yeni kaotik sistemin x-y-z (8 bit) fazlarından elde edilen rasgele sayıların NIST 800-22 testinden başarılı bir şekilde geçtiği P değerlerinden anlaşılmaktadır.

Tablo 5.1. x, y ve z'den elde edile rasgele sayıların NIST-800-22 test sonuçları

İstatistiksel Testler	P-değeri (X_8bit)	P-değeri (Y_8bit)	P-değeri (Z_8bit)	Sonuç
Frequency (Monobit) Test	0,1835	0,5619	0,9028	Başarılı
Block-Frequency Test	0,9886	0,4733	0,5049	Başarılı
Cumulative-Sums Test	0,1415	0,7570	0,7477	Başarılı
Runs Test	0,7370	0,0596	0,1096	Başarılı
Longest-Run Test	0,6039	0,7461	0,3937	Başarılı
Binary Matrix Rank Test	0,3413	0,3521	0,7038	Başarılı
Discrete Fourier Transform Test	0,2513	0,0454	0,4246	Başarılı
Non-Overlapping Templates Test	10,103	0,0051	0,0506	Başarılı
Overlapping Templates Test	0,4714	0,6056	0,8564	Başarılı
Maurer's Universal Statistical Test	0,9012	0,4438	0,5287	Başarılı
Approximate Entropy Test	0,6074	0,2596	0,5061	Başarılı
Random-Excursions Test (x = -4)	0,5684	0,1659	0,2135	Başarılı
Random-Excursions Variant Test (x = -9)	0,6490	0,4958	0,1828	Başarılı
Serial Test-1	0,7416	0,5162	0,5991	Başarılı
Serial Test-2	0,9123	0,2447	0,9363	Başarılı
Linear-Complexity Test	0,1100	0,3270	0,3663	Başarılı

5.2.2. FIPS 400-1 testi

Bu bölümde RSÜ'den elde edilen rasgele sayı dizisinin FIPS 140-1 test analizleri yapılmıştır. Tablo 5.2'de x-y-zboyutlarının her birinin 8 bitlik verilerinden elde edilen rasgele sayı dizilerinin FIPS 140-1 testi sonuç değerleri gösterilmiştir. Başarı kriteri bölümü ile kıyaslandığında testlerin her birinin olumlu bir şekilde geçtiği görülmektedir.

Tablo 5.2. x, y ve z'den elde edile rasgele sayıların FIPS 400-1 test sonuçları

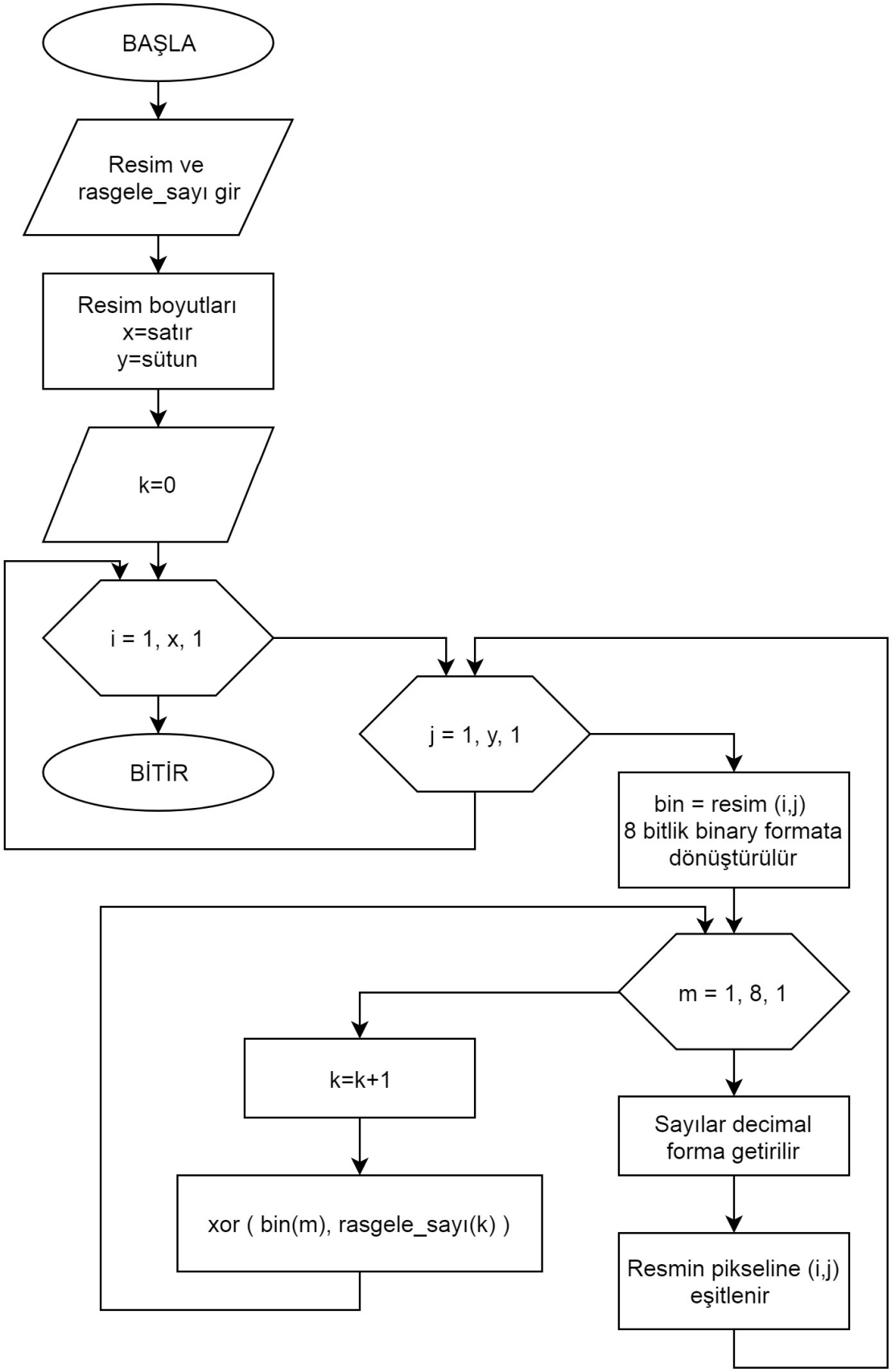
FIPS 140-1 Testleri	**Başarı Kriteri**	**Sonuç değeri**			**Sonuç**
		x	y	z	
Monobit Testi	$9654 < n < 10346$	10014	9929	10071	Başarılı
Poker Testi	$1.03 < X < 57.4$	8.3264	14.5024	8.6464	Başarılı
Run Testi (blok uzunluğu 1)	$2267 \leq x \leq 2733$	2567	2545	2491	Başarılı
Run Testi (blok uzunluğu 2)	$1079 \leq x \leq 1421$	1267	1206	1264	Başarılı
Run Testi (blok uzunluğu 3)	$502 \leq x \leq 748$	615	658	617	Başarılı
Run Testi (blok uzunluğu 4)	$223 \leq x \leq 402$	338	296	316	Başarılı
Run Testi (blok uzunluğu 5)	$90 \leq x \leq 223$	129	165	151	Başarılı
Long Run Testi	$34 >$ Koşu	13	12	13	Başarılı

BÖLÜM 6. ŞİFRELEME UYGULAMASI VE GÜVENLİK ANALİZLERİ

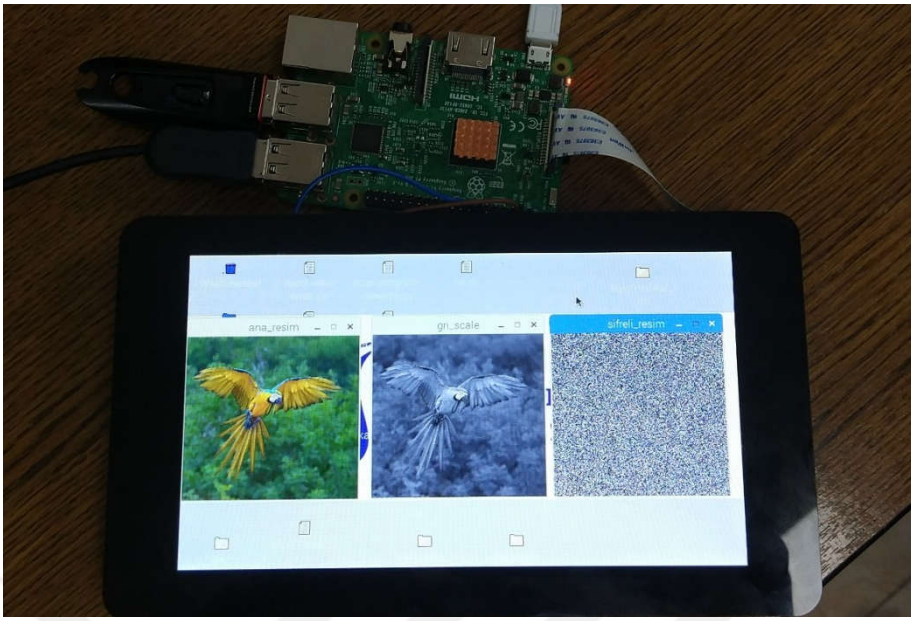
Bu bölümde yeni kaotik sistemin x, y, z fazlarının Runge Kutta-4 çözüm metodu ile ayrıklaştırılmasıyla elde edilen değerler kullanılarak bir resmin şifreleme uygulaması Spyder (Python 3.7) programı aracılığı ile gerçekleştirilmiştir. Daha sonra ise şifreleme algoritmasının kalitesini ve şifrelenen resmin güvenliğini ölçmek adına şifrelenmiş resim üzerinde Matlab programı kullanılarak güvenlik analizleri gerçekleştirilmiştir.

6.1. Şifreleme Uygulaması

Bu bölümde yeni kaotik sistemin x-y-z fazlarından üretilen rasgele sayılar ile bir resmin mobil olarak Raspberry Pi 3 Model B ile şifrelenme uygulaması gerçekleştirilmiştir (Şekil 6.2). Şekil 6.1'de şifreleme esnasında izlenen teknik, akış diyagramı olarak gösterilmiştir. Bu algoritmaya göre ilk olarak şifrelenecek resim programa tanıtılır. Gri scala forma dönüştürülen resmin boyutları (satır = x, sütun = y) hesaplandıktan sonra bir k = 0 index değeri tanımlanır. Tüm satır ve sütun değerlerinde işlem yapabilmek için satır (x) ve sütun (y) şeklinde iki ayrı for döngüsü yapılır. Her bir satır ve sütun değeri 8 bitlik binary formata dönüştürülür. Girilen rasgele sayılardan (x, y, z fazlarından biri) alınan 8 bitlik diziler ile resmin 8 bitlik değerleri XOR işlemine tabi tutlur. Resmin tüm matris yapısı bu işlemden geiçirilir. XOR işleminin sonucunda elde edilen değerler decimal forma dönüştürülür. Bu şekilde görüntünün şifreleme işlemi gerçekleştirilmiş olur. Şekil 6.3'te resmin şifrelenmeden önceki ve Şekil 6.4'te şifrelenmeden sonraki matris değerleri gösterilmiştir.



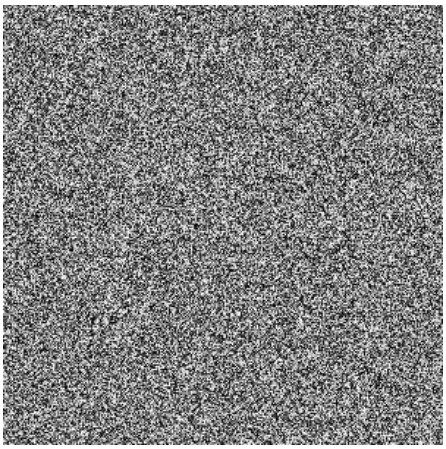
Şekil 6.1. Görüntü şifreleme algoritması



Şekil 6.2. Mobil şifreleme uygulaması (8 bitlik görüntü)

	0	1	2	3	4
0	144	142	132	133	131
1	144	143	134	134	128
2	145	143	138	133	131
3	142	140	135	132	125
4	141	138	138	129	128
5	136	132	130	124	127
6	134	135	129	126	122
7	133	131	127	124	121
8	132	129	127	119	118
9	127	128	125	118	114
10	126	123	122	119	116
11	128	123	118	117	115

Şekil 6.3. Resmin şifreleme öncesi matris değerleri



	0	1	2	3	4
0	149	186	216	218	79
1	83	129	35	6	197
2	23	74	27	22	49
3	135	112	50	105	3
4	186	211	62	35	238
5	10	83	50	161	41
6	97	127	19	119	23
7	160	122	209	220	104
8	42	50	199	63	99
9	60	1	165	120	88
10	170	176	191	119	95
11	239	85	136	245	180

Şekil 6.4. Resmin şifreleme sonrası matris değerleri

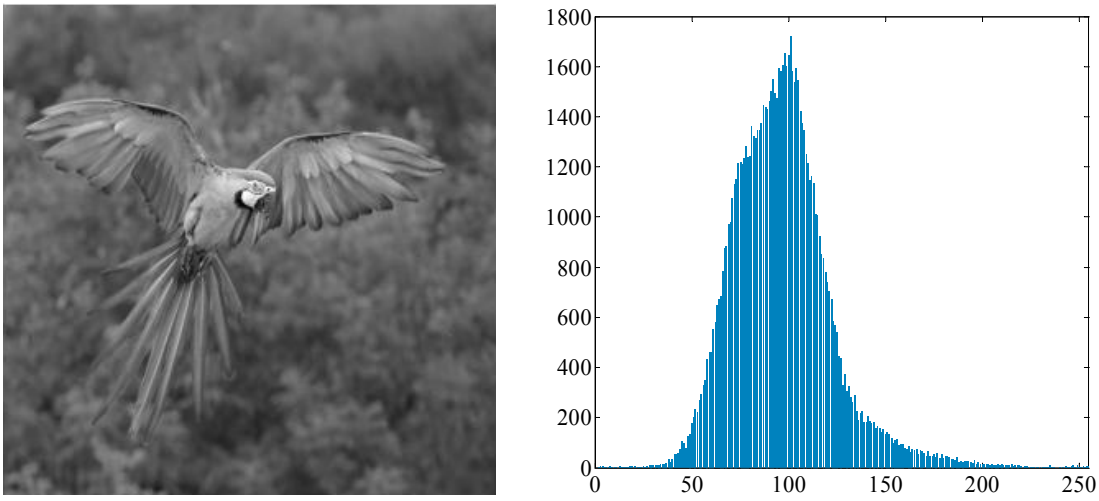
Gelecek bölümlerde şifreleme işleminin kalitesini ve güvenilirliğini ölçmek adına yapılan analiz yöntemlerinden bahsedilecektir.

6.2. Güvenlik Analizleri

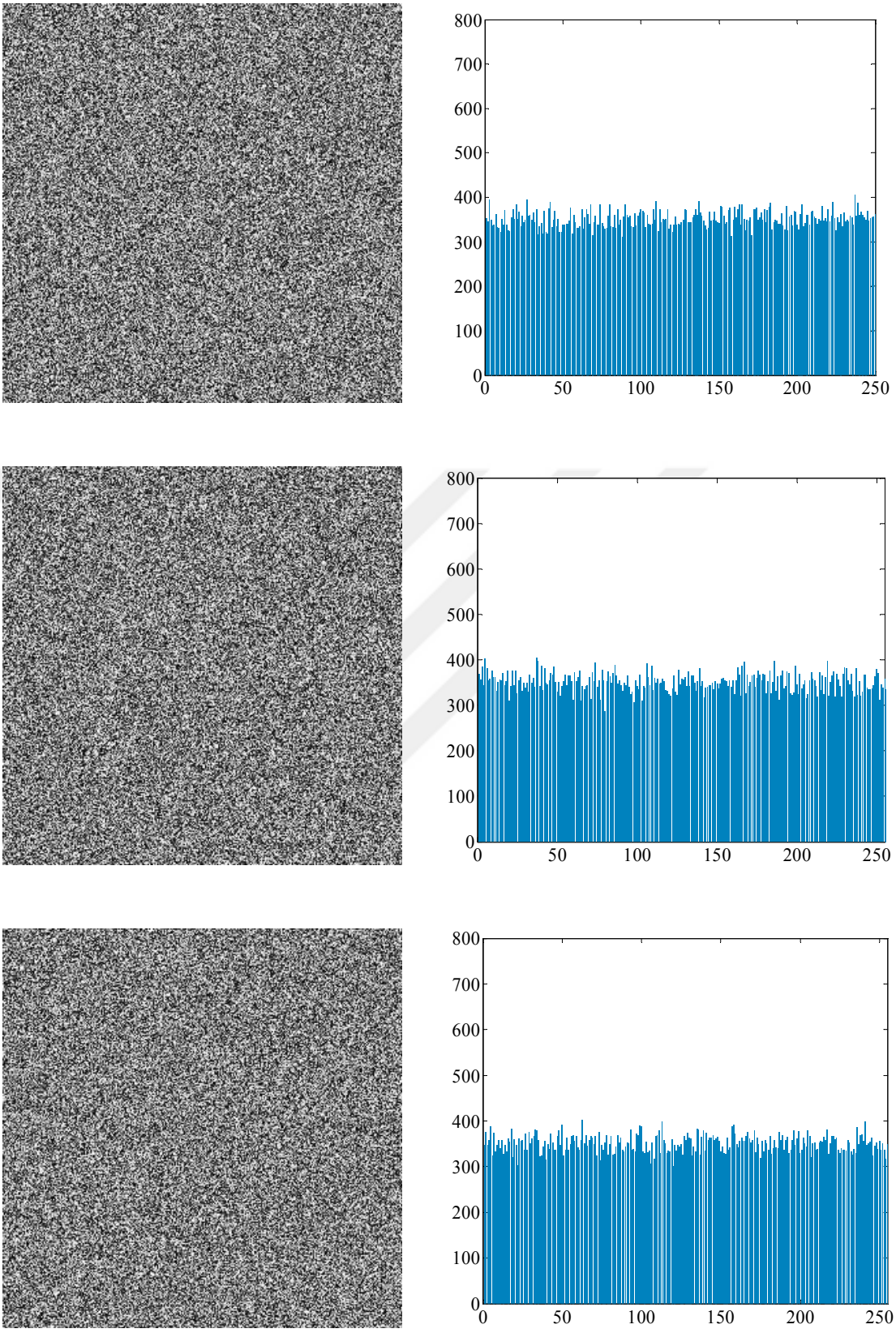
Bu bölümde şifreleme işlemi gerçekleştirilen görüntü üzerinde şifrelemenin güvenilirliğini ve kalitesini ölçmek adına yapılana histogram analizi, korelasyon ve entropi katasıyı, korelasyon haritaları gibi bazı testler üzerine uygulamalar gerçeklelştirilmiştir.

6.2.1. Histogram analizi

Bu bölümde kaynak görüntü ve x, y, z fazlarının her biri ile şifreleme işlemi yapılan görüntünün histogram analizleri gerçekleştirilmiştir. Şekil 6.5'e bakıldığında kaynak görüntünün histogram görüntüsü dağınık bir yapıda iken Şekil 6.6'daki x-y-z fazlarından elde edilen rasgele sayılar ile şifrelenen şifreli görüntülerin histogram analizleri yakın değerleri göstermektedir. Bu şifreleme işleminin başarılı olarak gerçekleştiğinin bir göstergesi olarak kabul edilir.



Şekil 6.5. Kaynak resim histogram analizi



Şekil 6.6. Sırası ile x fazından, y fazından, z fazından elde edilen rasgele sayılar kullanılarak 8 bitlik şifrelenmiş görüntüler ve histogram analizleri

6.2.2. Korelasyon ve entropi katsayıları

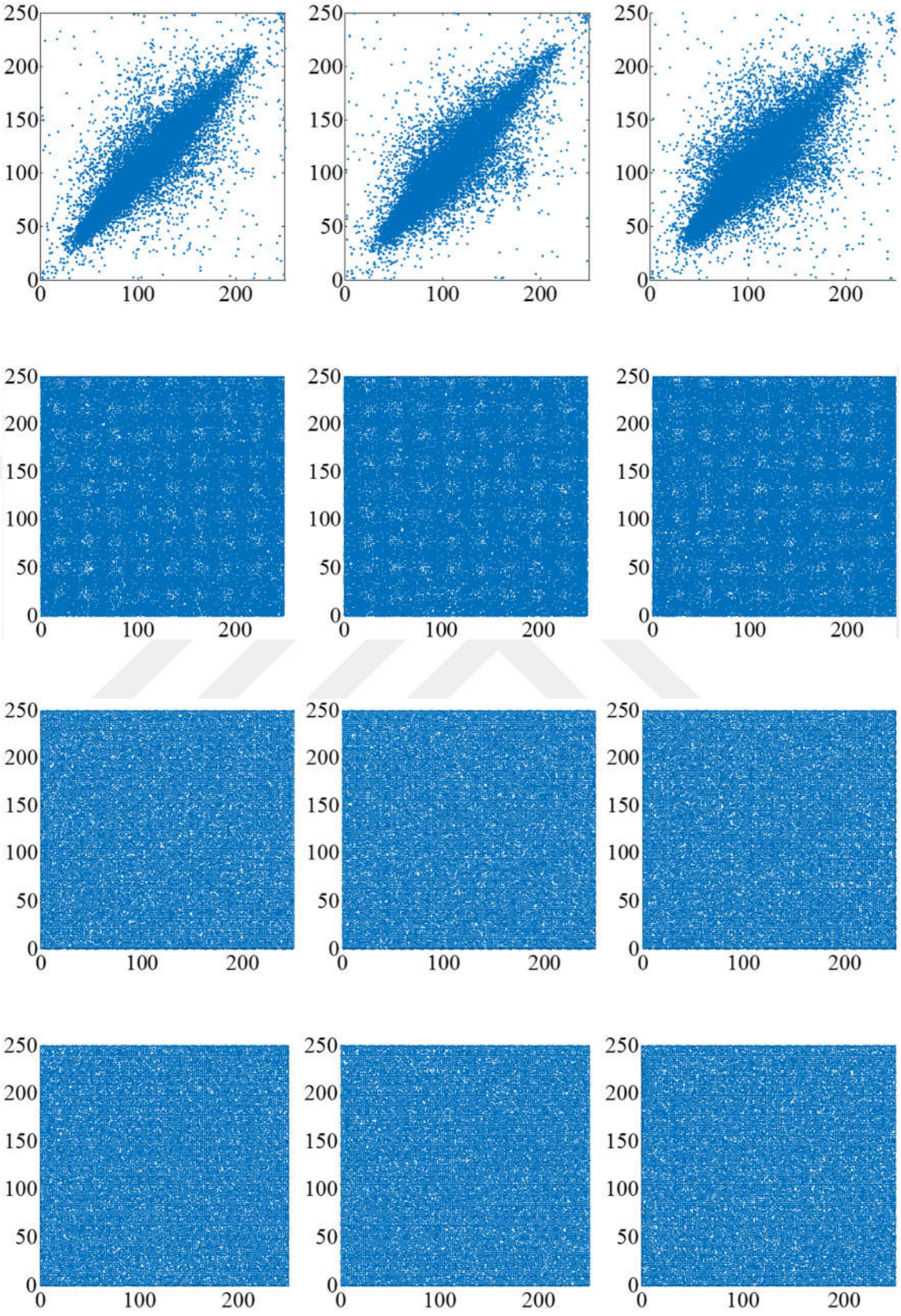
Bu bölümde entropi ve korelasyon katsayılarının incelemesi yapılmıştır. Şifreli görüntü içersinde rasgele dağılımın kalitesinden ve dolayısıyla başarılı bir şifrelemeden sözedilebilmesi için entropi değerinin 8 ve korelasyon değerinin de 0 değerine çok yakın olması gerekmektedir. Tablo 6.1'de şifreli resmin entropi ve korelasyon katsayılarının sonuçları gösterilmektedir. Kaynak resmin korelasyon değerleri yaklaşık 1 civarında iken x, y, z fazlarının her biri ile ayrı ayrı şifrelenen görüntülerin korelasyon değerleri 0'a çok yakın çıkmıştır. Aynı şekilde şifreli görüntünün entropi değerinin de 8'e çok yakın çıkması saldırılara karşı başarılı bir şifrelemenin gerçekleştirildiğini göstermektedir.

Tablo 6.1. Kaynak resmin ve x-y-z fazları ile şifrelenmiş görüntülerin korelasyon ve entropi katsayıları

Görüntü	Dikey Korelasyon	Yatay Korelasyon	Entropi
Ana resim	0,91209	0,88927	6,6297
Şifreli resim (x fazı)	-0,005053	0,00025276	7,9981
Şifreli resim (y fazı)	0,0032142	0,0017896	7,9976
Şifreli resim (z fazı)	-0,00056856	-0,0042772	7,998

6.2.3. Korelasyon haritaları

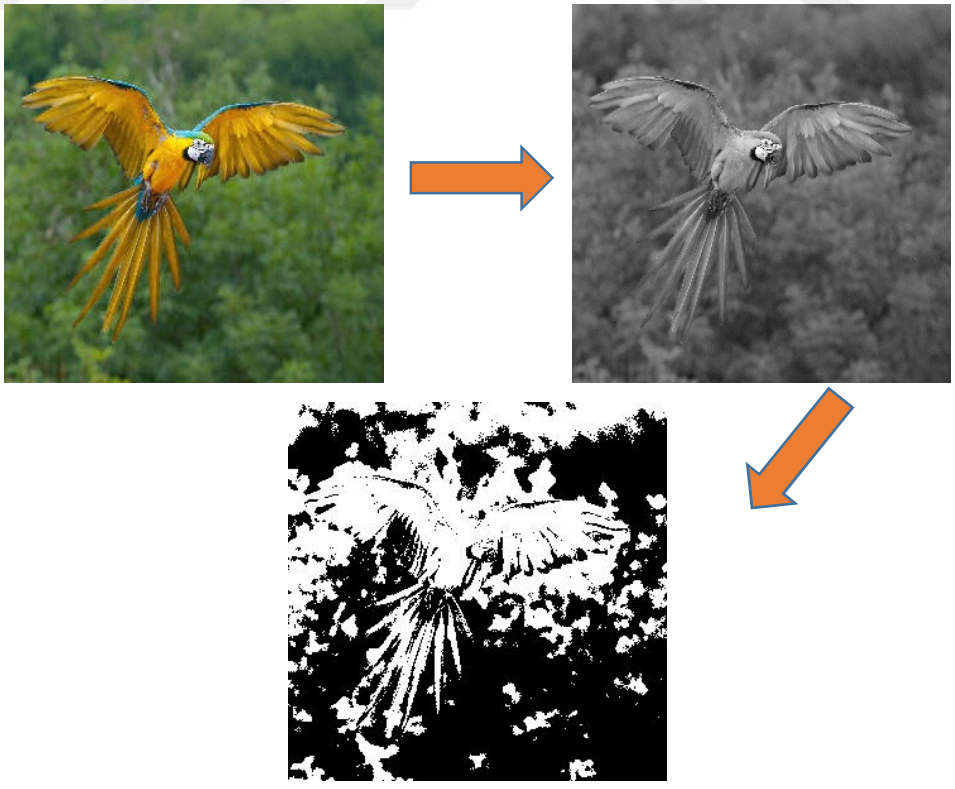
Bu bölümde kaynak görüntü ve şifreleme işlemi gerçekleştirilmiş olan görüntülerin korelasyon haritaları incelenmiştir. Şekil 6.7'de sırası ile orjinal görüntünün, x fazında şifrelenmiş görüntünün, y fazında şifrelenmiş görüntünün ve z fazında şifrelenmiş görüntünün korelasyon haritaları gösterilmektedir. Şifreleme yapılmayan kaynak görüntünün satır, sütun ve diagonal korelasyon haritaları diagonalde yoğunlaşırken, şifreli görüntülerin korelasyon dağılımları oldukça homojen bir dağılımda olduğu görülmektedir. Bu homojen dağılım şifreleme sonucu elde edilen görüntülerin oldukça rasgele bir dağılımda olduğunu göstermektedir.



Şekil 6.7. Yukarıdan aşağıya sırası ile orjinal görüntünün, x fazında şifrelenmiş görüntünün, y fazında şifrelenmiş görüntünün, z fazında şifrelenmiş görüntünün korelasyon haritaları

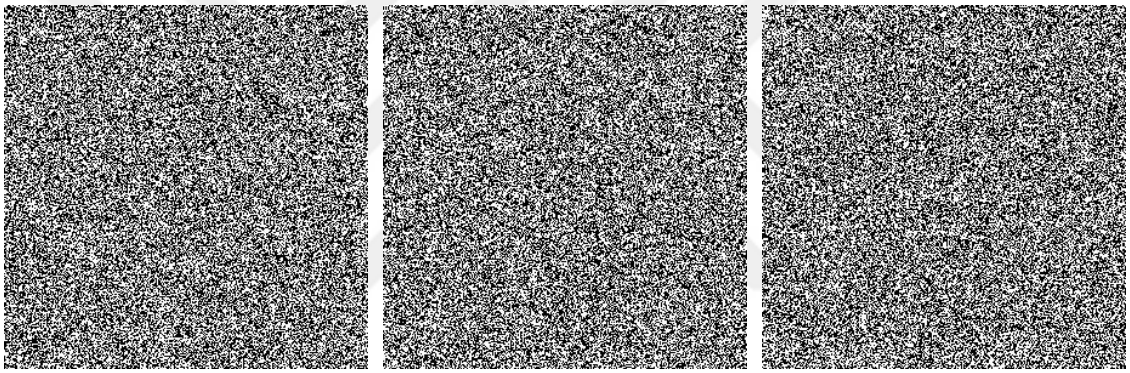
6.2.4. NPCR ve UACI

Bu bölümde mobil olarak şifrelenen (Şekil 6.9) 8 bit ve 1 bit şifreli görüntüler karşılaştırılarak NPCR ve UACI değerleri incelenmiştir. NPCR tüm piksellerin % kaçının değiştiğini ifade ederken, UACI değeri ise piksellerin % kaç oranında değiştiğini göstermektedir. 1 bit görüntünün şifreleme işleminin yapılabilmesi için ilk olarak kaynak görüntü üzerinde threshold işlemi uygulanarak Şekil 6.8'de görüldüğü üzere 1 bit değerlerden oluşan görüntü verisi elde edilmiştir. Sonrasında her bir piksel değeri x, y, z fazlarından elde edilen rasgele sayılar ile XOR edilerek Şekil 6.10'daki şifreli görüntüler elde edilmiştir. 8 bit ve 1 bitte yapılan şifrelemeleri karşılaştıracak olursak; şifreli 1 bit görüntünün toplam değişen piksel sayısı ile değişen piksellerin ortalaması eşit çıkmaktadır. Tablo 6.2'de x, y, z fazlarında şifrelenen 1 bit ve 8 bit görüntülerin NPCR ve UACI değerleri gösterilmektedir. Örneğin x fazında 8 bit şifrelenen görüntünün pikselleri % 99,60 oranında değişirken, piksellerin genel olarak önceki değerlerine göre değişim oranı % 27,68 olarak gösterilmektedir. Ancak 1 bit şifrelenen görüntünün NPCR ve UACI değerleri aynı çıkmıştır.



Şekil 6.8. Kaynak görüntünün 1 bit görüntüye dönüşümü

Şekil 6.9. Mobil şifreleme uygulaması (1 bitlik görüntü)



(a) (b) (c)

Şekil 6.10. a) 1 bit görüntünün x fazı ile şifrelenmesi, b) 1 bit görüntünün y fazı ile şifrelenmesi, c) 1 bit görüntünün z fazı ile şifrelenmesi

Tablo 6.2. x-y-z fazları ile şifrelenmiş görüntülerin NPCR ve UACI analizleri

Görüntüler	NPCR	UACI
x fazında şifreli resim (8 bit)	99,60	27,68
x fazında şifreli resim (1 bit)	50,13	50,13
y fazında şifreli resim (8 bit)	99,62	27,62
y fazında şifreli resim (1 bit)	49,88	49,88
z fazında şifreli resim (8 bit)	99,62	27,54
z fazında şifreli resim (1 bit)	50,21	50,21

BÖLÜM 7. SONUÇ VE ÖNERİLER

Yapılan tez çalışmasında doğrusal olmayan bir kaotik sistem kullanılarak mikrobilgisayar tabanlı mobil RSÜ tasarımı gerçekleştirilmiştir. Üretilen rasgele sayıların güvenli bir şekilde kullanılabileceği NIST 800-22 ve FIPS 140-1 istatistiksel testleri ile doğrulandıktan sonra bu sayılar kullanılarak resim şifreleme uygulaması yapılmıştır. Şifreleme algoritmasının kalitesi ve şifrelenen resmin güvenilirliğinin ölçülmesinde histogram analizi, korelasyon ve entropi katsayısı, korelasyon haritası, UACI, NPCR gibi güvenlik analizlerinden yararlanılmıştır.

Tez çalışmasının ilk aşamasında; kaotik sistemler, RSÜ tasarımı ve görüntü şifreleme alanında kapsamlı bir literatür araştırmasının ardından ilk olarak önceden literatürde sunulmuş olan bir kaotik sistemden yeni bir kaotik sistem türetilerek kaotiklik analizleri yapılmıştır. Kaotik analizlerinin yapımında faz portreleri, layapunov üstelleri, laypunov boyutu, zaman serileri, başlangıç şartlarına hassas bağımlılık, çatallanma grafiği, FFT analizi gibi kaotiklik hakkında bilgi sağlayan bazı analiz yöntemleri Matlab programı yardımı ile gerçekleştirilmiştir.

İkinci aşamada; kaotiklik analizlerinden başarı ile geçen yeni kaotik sistem entropi kaynağı olarak kullanılarak Raspberry Pi 3 Model B mikrobilgisayarı üzerinde Spyder programı yardımı ile bir mobil RSÜ tasarımı gerçekleştirilmiştir. RSÜ tasarımı genel olarak; yeni kaotik sistemin RK4 metodu kullanılarak ayrıştırılması ve binary forma getirilmesi prensibi ile gerçekleştirilmiştir. 1000000 bit gibi uzun bir veri dizisine sahip olan ve x-y-z fazlarının her birinden elde edilen binary formattaki rasgele sayılar NIST-800-22 ve FIPS-140-1 testlerinden başarı ile geçmesi sağlanmıştır.

Bu tez çalışmasının son aşamasında testleri başarı ile geçen rasgele sayılardan bir görüntü verisi üzerinde Raspberry Pi 3 Model B mikrobilgisayarında Spyder programı

kullanılarak şifreleme uygulaması gerçekleştirilmiştir. Piksellerine ayrıştırılan görüntünün her bir piksel değeri rasgele sayılar ile aynı şekilde binary forma dönüştürülmüş ve binary sayı formatına dönüşen resmin her bir piksel değeri tek tek 1000000 bit uzunluğundaki rasgele sayılardan alınan 8 bit verilerle XOR işlemine tabi tutulmuştur. Çıkan sonuçlar decimal sayı formatına döştürülerek şifrelenmiş görüntünün elde edilmesi sağlanmıştır. Şifreli görüntünün daha doğrusu şifreleme algoritmasının saldırılara karşı güvenilirliğini test etmek için bazı testler uygulanmıştır. Histogram analizi, korelasyon haritaları, UACI, NPCR, entropi katsayısı gibi uygulanan güvenlik analizlerinin gerçekleştirilmesinde yine Matlab programı kullanılmıştır.

Yapılan tüm bu araştırma ve çalışmaların sonucunda kaotik sistemlerin analiz yöntemleri, kaos tabanlı mobil rasgele sayı üretimi, rasgelelik testleri, görüntü şifreleme, şifreli görüntünün güvenlik analizleri gibi alanlarda yapılan çalışmalara toplu bir bilgi kaynağı sağlanmıştır. Veri güvenliğine önem verilen şifreleme, damgalama, gizli yazı gibi yapılan çalışmalarda kolaylıkla kullanılabilecek bir mobil RSÜ tasarımı gerçekleştirilmiştir.

Yapılan çalışmalara ek olarak rasgele sayı üretiminde yeni ve farklı algoritmalar sunularak rasgele sayıların rasgelelik testlerinden geçmeleri kolaylaştırılabilir. Yeni şifreleme algoritmaları geliştirilerek resim üzerinde olduğu gibi metin, ses ve video verileri üzerinde de uygulanabilir. Ayrıca yapılan tüm bu işlemler bir arayüzde toplanarak kullanıcı kolaylığı sağlanabilir.

KAYNAKLAR

Abdirash, M., Dolzhikova, I., & James, A. P. (2018). Brief Tutorial On Hp Memristor-Based Chua's Chaotic Oscillator. 2018 International Conference On Computing And Network Communications (Coconet), 122-129. Https://Doi.Org/10.1109/Coconet.2018.8476908

Ağır, E. (2010, Ağustos 8). Kaotik Sistemler. Geliş Tarihi 24 Mart 2019, Gönderen Okyanusum.Com Website: Http://Okyanusum.Com/Makale/Kaotik-Sistemler/0000000000

Akgül, A. (2015). Yeni Kaotik Sistemler İle Rasgele Sayi Üreteci Tasarımı Ve Çoklu-Ortam Verilerinin Yüksek Güvenlikli Şifrelenmesi (Phd Thesis). Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya.

Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C., & Hassan, Z. (2014). Pseudo Random Number Generator Based On Quantum Chaotic Map. Communications In Nonlinear Science And Numerical Simulation, 19(1), 101-111. Https://Doi.Org/10.1016/J.Cnsns.2013.06.017

Akhshani, A., Behnia, S., Akhavan, A., Hassan, H. A., & Hassan, Z. (2010). A Novel Scheme For Image Encryption Based On 2d Piecewise Chaotic Maps. Optics Communications, 283(17), 3259-3266. Https://Doi.Org/10.1016/J.Optcom.2010.04.056

Akkaya, S., Pehlivan, İ., Akgül, A., & Varan, M. (2018). Yeni Bir Kaos Tabanlı Rasgele Sayı Üreteci Kullanan Banka Şifrematik Cihazı Tasarımı Ve Uygulaması. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 2018(2018). Https://Doi.Org/10.17341/Gazimmfd.416418

Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A New Hybrid Digital Chaotic System With Applications In Image Encryption. Signal Processing, 160, 45-58. Https://Doi.Org/10.1016/J.Sigpro.2019.02.016

Almali, M. N., & DiKiCi, Z. (2016). The Simulation Of Sound Signal Masking With Different Chaotic Oscillations And Its Circuit Application. Turkish Journal Of Electrical Engineering & Computer Sciences, 24(5), 4284-4293.

Avaroğlu, E., & Türk, M. (2013). Random Number Generation Using Multi-Mode Chaotic Attractor. 2013 21st Signal Processing And Communications Applications Conference (Siu), 1-4. Https://Doi.Org/10.1109/Siu.2013.6531520

Avaroğlu, Erdinç, & Türk, M. (2013). Son Işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki Etkisinin İncelenmesi, 6. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı, Ankara-Türkiye, 291–294.

Bayani, A., Rajagopal, K., Khalaf, A. J. M., Jafari, S., Leutcho, G. D., & Kengne, J. (2019). Dynamical Analysis Of A New Multistable Chaotic System With Hidden Attractor: Antimonotonicity, Coexisting Multiple Attractors, And Offset Boosting. Physics Letters A. Https://Doi.Org/10.1016/J.Physleta.2019.02.005

Camara, C., Peris-Lopez, P., Martín, H., & Aldalaien, M. (2018). Ecg-Rng: A Random Number Generator Based On Ecg Signals And Suitable For Securing Wireless Sensor Networks. Sensors, 18(9), 2747. Https://Doi.Org/10.3390/S18092747

Chen, J., Zhu, Z., Fu, C., Yu, H., & Zhang, L. (2015). A Fast Chaos-Based Image Encryption Scheme With A Dynamic State Variables Selection Mechanism. Communications In Nonlinear Science And Numerical Simulation, 20(3), 846-860. Https://Doi.Org/10.1016/J.Cnsns.2014.06.032

Çavuşoğlu, Ü., Akgül, A., Zengin, A., & Pehlivan, I. (2017). The Design And Implementation Of Hybrid Rsa Algorithm Using A Novel Chaos Based Rng. Chaos, Solitons & Fractals, 104, 655-667. Https://Doi.Org/10.1016/J.Chaos.2017.09.025

Çavuşoğlu, Ü., Uyaroğlu, Y., & Pehlivan, İ. (2014). Sürekli Zamanlı Otonom Kaotik Devre Tasarımı Ve Sinyal Gizleme Uygulaması. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 29(1).

Çiçek, S., Ferikoğlu, A., & Pehlivan, İ. (2016). A New 3d Chaotic System: Dynamical Analysis, Electronic Circuit Design, Active Control Synchronization And Chaotic Masking Communication Application. Optik, 127(8), 4024-4030. Https://Doi.Org/10.1016/J.Ijleo.2016.01.069

Dursun, M., & Kaşifoğlu, E. (2018). Design And Implementation Of The Fpga-Based Chaotic Van Der Pol Oscillator. 6.

Ergün, S., & Tanrıseven, S. (2018). Random Number Generation Using Dual Oscillator Architecture And Discrete-Time Chaos. 2018 International Symposium On Electronics And Smart Devices (Isesd), 1-4. Https://Doi.Org/10.1109/Isesd.2018.8605452

Fahd, S., Afzal, M., Abbas, H., Iqbal, W., & Waheed, S. (2018). Correlation Power Analysis Of Modes Of Encryption In Aes And Its Countermeasures. Future Generation Computer Systems, 83, 496-509. Https://Doi.Org/10.1016/J.Future.2017.06.004

Fell, J., Röschke, J., & Beckmann, P. (1993). Deterministic Chaos And The First Positive Lyapunov Exponent: A Nonlinear Analysis Of The Human

Electroencephalogram During Sleep. Biological Cybernetics, 69(2), 139-146. Https://Doi.Org/10.1007/Bf00226197

Group, Webders. (2016). Entropi - Webders.Net. Geliş Tarihi 24 Mart 2019, Gönderen Http://Www.Webders.Net/256/Entropi.Html

Güvenoğlu, E., & Esin, E. M. (2009). Knutt/Durstenfeld Shuffle Algoritmasının Resim Şifreleme Amacıyla Kullanılması. Politeknik Dergisi, 12(3), 151–155.

Hamamci, S. E., Göğebakan, V., & Işık, İ. (2015). A New Chaotic System With Chaos Entanglement. 2015 23nd Signal Processing And Communications Applications Conference (Siu), 2597-2600. Https://Doi.Org/10.1109/Siu.2015.7130417

Hatun, E. (2018). Raspberry Pi Üzerinde Gerçeklenmiş Rsa Algoritmasina Yan Kanal Analizi. 93.

Hua, Z., Zhou, Y., & Huang, H. (2019). Cosine-Transform-Based Chaotic System For Image Encryption. Information Sciences, 480, 403-419. Https://Doi.Org/10.1016/J.Ins.2018.12.048

Jafari, M. A., Mliki, E., Akgul, A., Pham, V.-T., Kingni, S. T., Wang, X., & Jafari, S. (2017). Chameleon: The Most Hidden Chaotic Flow. Nonlinear Dynamics, 88(3), 2303-2317. Https://Doi.Org/10.1007/S11071-017-3378-4

Kandar, S., Chaudhuri, D., Bhattacharjee, A., & Dhara, B. C. (2019). Image Encryption Using Sequence Generated By Cyclic Group. Journal Of Information Security And Applications, 44, 117-129. Https://Doi.Org/10.1016/J.Jisa.2018.12.003

Karakaya, Barış, Gülten, A., & Frasca, M. (2019). A True Random Bit Generator Based On A Memristive Chaotic Circuit: Analysis, Design And Fpga Implementation. Chaos, Solitons & Fractals, 119, 143-149. Https://Doi.Org/10.1016/J.Chaos.2018.12.021

Karakaya, Baris, Turk, M. A., Turk, M., & Gulten, A. (2018). Selection Of Optimal Numerical Method For Implementation Of Lorenz Chaotic System On Fpga. 6.

Kaşkaloğlu, D. K., & Üniversitesi, A. (T.Y.). Geçmişten Günümüze Kriptoloji: Şifrelerin Bilimi. 6.

Kim, Y.-S., & Kim, J.-C. (2019). Analysis Of Chaotic Vibration Of Shilnikov-Type In Rotor With Asymmetric And Non-Linear Stiffness. International Journal Of Non-Linear Mechanics, 109, 132-139. Https://Doi.Org/10.1016/J.Ijnonlinmec.2018.12.002

Koyuncu, İ. (2014). Kriptolojik Uygulamalar Için Fpga Tabanlı Yeni Kaotik Osilatörlerin Ve Gerçek Rasgele Sayı Üreteçlerinin Tasarımı Ve Gerçeklenmesi (Phd Thesis). Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü.

Koyuncu, İ., & Turan Özcerit, A. (2017). The Design And Realization Of A New High Speed Fpga-Based Chaotic True Random Number Generator. Computers & Electrical Engineering, 58, 203-214. Https://Doi.Org/10.1016/J.Compeleceng.2016.07.005

Lai, Q., Akgul, A., Varan, M., Kengne, J., & Turan Erguzel, A. (2018). Dynamic Analysis And Synchronization Control Of An Unusual Chaotic System With Exponential Term And Coexisting Attractors. Chinese Journal Of Physics, 56(6), 2837-2851. Https://Doi.Org/10.1016/J.Cjph.2018.09.015

Liu, C., Liu, T., Liu, L., & Liu, K. (2004). A New Chaotic Attractor. Chaos, Solitons & Fractals, 22(5), 1031-1038. Https://Doi.Org/10.1016/J.Chaos.2004.02.060

Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure And Robust Digital Image Watermarking Scheme Using Logistic And Rsa Encryption. Expert Systems With Applications, 97, 95-105. Https://Doi.Org/10.1016/J.Eswa.2017.12.003

Martínez-Guerra, R., Pérez-Pinacho, C. A., & Gómez-Cortés, G. C. (2015). Synchronization Of Integral And Fractional Order Chaotic Systems: A Differential Algebraic And Differential Geometric Approach With Selected Applications In Real-Time (Ss. 135-151). Https://Doi.Org/10.1007/978-3-319-15284-4_8

Milani, M. M. R. A., Pehlivan, H., & Pour, S. H. (2013). Kaos Tabanlı Bir Şifreleme Yöntemi Ve Analizi. Akademik Bilisim, 487–493.

Min, F., Li, C., Zhang, L., & Li, C. (2019). Initial Value-Related Dynamical Analysis Of The Memristor-Based System With Reduced Dimensions And Its Chaotic Synchronization Via Adaptive Sliding Mode Control Method. Chinese Journal Of Physics, 58, 117-131. Https://Doi.Org/10.1016/J.Cjph.2018.12.020

Mondal, B., Singh, S., & Kumar, P. (2019). A Secure Image Encryption Scheme Based On Cellular Automata And Chaotic Skew Tent Map. Journal Of Information Security And Applications, 45, 117-130. Https://Doi.Org/10.1016/J.Jisa.2019.01.010

Munmuangsaen, B., & Srisuchinwong, B. (2018). A Hidden Chaotic Attractor In The Classical Lorenz System. Chaos, Solitons & Fractals, 107, 61-66. Https://Doi.Org/10.1016/J.Chaos.2017.12.017

Ozdemir, A., Pehlivan, I., Akgul, A., & Guleryuz, E. (2018). A Strange Novel Chaotic System With Fully Golden Proportion Equilibria And Its Mobile Microcomputer-Based Rng Application. Chinese Journal Of Physics, 56(6), 2852–2864.

Özdemir, K. (2008). Sürekli-Zamanlı Kaos İle Rastgele Sayı Üreteci Tasarımı (Thesis, Fen Bilimleri Enstitüsü). Geliş Tarihi Gönderen Https://Polen.Itu.Edu.Tr/Handle/11527/1110

Özkaynak, F. (2016). Kriptolojik Rasgele Sayı Üreteçleri. Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi, 8(2), 37-45.

Özyapici, A. (2017). Generalized Trial Equation Method And Its Applications To Duffing And Poisson-Boltzmann Equations. Turkish Journal Of Mathematics, 41(3), 686-693.

Pamuk, N. (2016). Dinamik Sistemlerde Kaotik Zaman Dizilerinin Tespiti. Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 15(1), 78-92.

Pehlivan, İ. (2010). Yeni Kaotik Sistemler: Elektronik Devre Gerçeklemeleri, Senkronizasyon Ve Güvenli Haberleşme Uygulamaları. Doktora Tezi, Fen Bilimleri Enstitüsü, Sakarya Üniversitesi.

Praveenkumar, P., Amirtharajan, R., Thenmozhi, K., & Rayappan, J. B. B. (2015). Pixel Scattering Matrix Formalism For Image Encryption—A Key Scheduled Substitution And Diffusion Approach. Aeu - International Journal Of Electronics And Communications, 69(2), 562-572. Https://Doi.Org/10.1016/J.Aeue.2014.11.010

Raspberry Pi Foundation - About Us. (T.Y.). Geliş Tarihi 24 Mart 2019, Gönderen Raspberry Pi Website: Https://Www.Raspberrypi.Org/About/

Sakallı, F. B. (2011). Akış Şifrelerin Tasarım Teknikleri Ve Güç Analizi. Geliş Tarihi Gönderen Http://Dspace.Trakya.Edu.Tr/Xmlui/Handle/1/1111

Sivakumar, T., & Li, P. (2019). A Secure Image Encryption Method Using Scan Pattern And Random Key Stream Derived From Laser Chaos. Optics & Laser Technology, 111, 196-204. Https://Doi.Org/10.1016/J.Optlastec.2018.09.048

Su, K. (2015). Dynamic Analysis Of A Chaotic System. Optik, 126(24), 4880-4886. Https://Doi.Org/10.1016/J.Ijleo.2015.09.052

Su, Y., Wo, Y., & Han, G. (2019). Reversible Cellular Automata Image Encryption For Similarity Search. Signal Processing: Image Communication, 72, 134-147. Https://Doi.Org/10.1016/J.Image.2018.12.008

Şahin, F. (2015). Modern Blok Şifreleme Algoritmaları. İstanbul Aydın Üniversitesi Dergisi, 7(26), 23–40.

Toyran, M. (2007). Efficient Use Of Random Numbers. 2007 Ieee 15th Signal Processing And Communications Applications, 1-4. Https://Doi.Org/10.1109/Siu.2007.4298567

Tufan, T. (2017, Eylül 24). Kaos Teorisi Nedir? - Tarkan Tufan. Geliş Tarihi 24 Mart 2019, Gönderen Https://Www.Gazeteduvar.Com.Tr/Dunya-Forum/2017/09/24/Dunya-Forum-Tanimsizligin-Formulleri-Kaos-Teorisi-Nedir/

Tuna, M., & Fidan, C. B. (2018). A Study On The Importance Of Chaotic Oscillators Based On Fpga For True Random Number Generating (Trng) And Chaotic Systems. Journal Of The Faculty Of Engineering And Architecture Of Gazi University, 33(2), 469–486.

Uğur, A. (2005). Uzaktan Erişimli Kriptografik Güvenli Haberleşme Protokolü. Geliş Tarihi Gönderen Http://Acikerisim.Pau.Edu.Tr:8080/Xmlui/Handle/11499/1171

Vaidyanathan, S., Akgul, A., Kaçar, S., & Çavuşoğlu, U. (2018). A New 4-D Chaotic Hyperjerk System, Its Synchronization, Circuit Design And Applications In Rng, Image Encryption And Chaos-Based Steganography. The European Physical Journal Plus, 133(2), 46. Https://Doi.Org/10.1140/Epjp/I2018-11872-8

Wang, C., Hu, C., Han, J., & Cang, S. (2016). A New No-Equilibrium Chaotic System And Its Topological Horseshoe Chaos [Research Article]. Https://Doi.Org/10.1155/2016/3142068

Wang, J., Li, Y., Zhong, S., & Hou, X. (2019). Analysis Of Bifurcation, Chaos And Pattern Formation In A Discrete Time And Space Gierer Meinhardt System. Chaos, Solitons & Fractals, 118, 1-17. Https://Doi.Org/10.1016/J.Chaos.2018.11.013

Wei, Z., Zhu, B., Yang, J., Perc, M., & Slavinec, M. (2019). Bifurcation Analysis Of Two Disc Dynamos With Viscous Friction And Multiple Time Delays. Applied Mathematics And Computation, 347, 265-281. Https://Doi.Org/10.1016/J.Amc.2018.10.090

Wu, G.-C., & Baleanu, D. (2014). Discrete Fractional Logistic Map And Its Chaos. Nonlinear Dynamics, 75(1), 283-287. Https://Doi.Org/10.1007/S11071-013-1065-7

Wu, Y., & Agaian, S. (2011). Npcr And Uaci Randomness Tests For Image Encryption. 9.

Xian, Y., Xia, C., Guo, T., Fu, K., & Xu, C. (2018). Dynamical Analysis And Fpga Implementation Of A Large Range Chaotic System With Coexisting Attractors. Results In Physics, 11, 368-376. Https://Doi.Org/10.1016/J.Rinp.2018.06.022

Yang, Y., & Qi, G. (2019). Comparing Mechanical Analysis With Generalized-Competitive-Mode Analysis For The Plasma Chaotic System. Physics Letters A, 383(4), 318-327. Https://Doi.Org/10.1016/J.Physleta.2018.10.046

Yardım, F. E., & Afacan, E. (2010). Lorenz-Tabanli Diferansiyel Kaos Kaydirmali Anahtarlama (Dcsk) Modeli Kullanilarak Kaotik Bir Haberleşme Sisteminin Simülasyonu. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 25(1).

Yavuz, E., Yazıcı, R., Kasapbaşi, M. C., & Yamaç, E. (2014). Enhanced Chaotic Key-Based Algorithm For Low-Entropy Image Encryption. 2014 22nd Signal Processing And Communications Applications Conference (Siu), 385-388. Https://Doi.Org/10.1109/Siu.2014.6830246

YerliKaya, T., Gençoğlu, H., EmiR, M. K., Çankaya, M., & Buluş, E. (2011). Rsa Şifreleme Algoritmasi Ve Aritmetik Modül Uygulamasi. İstanbul Aydın Üniversitesi Dergisi, 3(9), 95-104.

Yeşil, A., & Babacan, Y. (2019). Elektronik Olarak Ayarlanabilir Memristör Tabanlı Chua Devresinin Gerçeklenmesi. Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9(1), 121–129.

Yılmaz, D., & Güler, N. F. (2006). Kaotik Zaman Serisinin Analizi Üzerine Bir Araştırma. Gazi Üniversitesi Mühendislik Ve Mimarlık Fakültesi Dergisi, 21(4), 759–779.

Zhu, H., Zhao, C., Zhang, X., & Yang, L. (2013). A Novel Iris And Chaos-Based Random Number Generator. Computers & Security, 36, 40-48. Https://Doi.Org/10.1016/J.Cose.2013.02.003

ÖZGEÇMİŞ

Bilal Gürevin, 23.05.1993'te Bursa'da doğdu. İlk, orta ve lise eğitimini Bursa'da tamamladı. 2011 yılında Mehmet Kemal Coşkunöz Anadolu Teknik Lisesi'nden mezun oldu. 2011 yılında başladığı Sakarya Üniversitesi Mekatronik Mühendisliği Bölümü'nü 2016 yılında tamamladı. 2017 yılında Sakarya Üniversitesi Mekatronik Mühendisliği Bölümü'nde yüksek lisans eğitimine başladı. Yüksek lisans eğitimine Sakarya Uygulamalı Bilimler Üniversitesi Mekatronik Mühendisliği Bölümü'nde devam etti. Aynı zamanda Nisan-2018 ve Nisan-2019 tarihleri arasında Sakarya Uygulamalı Bilimler Üniversitesi'nde Tübitak projesinde bursiyer olarak görev aldı.