

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**OTONOM OLMAYAN KAOTİK SİSTEMLERDE
RASGELE SAYI ÜRETİMİNİN İNCELENMESİ**

YÜKSEK LİSANS TEZİ

Müh. Pınar Güven

Anabilim Dalı: Elektronik ve Haberleşme Mühendisliği

Programı: Elektronik Mühendisliği

Tez Danışmanı: Doç. Dr. Serdar ÖZOĞUZ

HAZİRAN 2006

**OTONOM OLMAYAN KAOTİK SİSTEMLERDE
RASGELE SAYI ÜRETİMİNİN İNCELENMESİ**

YÜKSEK LİSANS TEZİ

Müh. Pınar Güven

504021222

Tezi Enstitüye Verildiği Tarih: 9 Mayıs 2006

Tezin Savunulduğu Tarih: 5 Haziran 2006

Tez Danışmanı: Doç. Dr. Serdar ÖZOĞUZ

Diğer Jüri Üyeleri: Yrd. Doç. Dr. Müştak Erhan YALÇIN

Yrd. Doç. Dr. Osman Kaan EROL

HAZİRAN 2006

ÖNSÖZ

Tez çalışmam sırasında değerli zamanını, önerilerini ve yardımlarını esirgemeyen tez danışmanım Sayın Doç. Dr. Serdar Özoğuz'a, sonsuz anlayışları, destekleriyle her zaman yanımda olan aileme ve cesaretlendirmelerinden dolayı arkadaşlarıma teşekkürü bir borç bilirim.

Haziran 2006

Pınar Güven

İÇİNDEKİLER

KISALTMALAR	iv
TABLO LİSTESİ	v
ŞEKİL LİSTESİ	vi
ÖZET	vii
SUMMARY	ix
1. GİRİŞ	1
1.1 Kaosun Anlamı	1
1.2 Kaotik Sistemler ve Uygulama Alanları	3
1.2.1 Rasgele Sayı Üreteçleri (RSÜ)	3
1.2.2 Yalancı Rastgele Sayı Üreteçleri (YRSÜ)	4
1.2.3 Mesaj Saklama	4
1.2.4 Şifreleme	5
2. KAOTİK SİSTEMLER	7
2.1 Rasgele Sayı Üreteçlerinin Çalışma Prensipleri	7
2.2 Otonom Olmayan Kaotik Sistemlerle Rasgele Sayı Üretimi	8
2.3 Rasgelelik Testleri	15
3. KAOTİK SİSTEMLERDEN RASGELE SAYI ÜRETİMİNİN İNCELENMESİ	17
3.1 Dört Sarmallı Sistemden Rasgele Sayı Üretilmesi	18
3.2 Sekiz Sarmallı Sistemden Rasgele Sayı Üretilmesi	26
3.3 Oniki Sarmallı Sistemden Rasgele Sayı Üretilmesi	33
4. SONUÇLAR	35
EK-1	37
EK-2	38
KAYNAKLAR	39
ÖZGEÇMİŞ	40

KISALTMALAR

ASCII	: American Standard Code for Information Interchange
NIST	: National Institute of Standards and Technology
FIPS	: Federal Information Processing Standards
RSÜ	: Rasgele Sayı Üreteçleri
YRSÜ	:Yalancı Rasgele Sayı Üreteci (Pseudo Random Number Generator)

TABLO LİSTESİ

	<u>Sayfa No</u>
Tablo 1.1. Kaosun keşfedilmesindeki çıkış noktası için örnek iterasyon değerleri.....	2
Tablo 1.2. Kaosun şifrelemedeki uygulaması.....	6
Tablo 2.1. Koşu sayılarının içinde bulunması gerekli aralıklar.....	16

ŞEKİL LİSTESİ

	Sayfa No
Şekil 1.1 : RSÜ blok diyagramı.....	3
Şekil 1.2 : Mesaj Gizleme Yapısı.....	6
Şekil 2.1 : Kaotik rastgele sayı üreten sistemin blok diyagramı	8
Şekil 2.2 : Kaotik osilatör yapısı.....	8
Şekil 2.3 : (a) Otonom Olmayan Kaotik Sistemin nümerik analiz sonuçları (b) Bu sistemin Poincaré kesitinde $c=0$ alınmasıyla oluşan Poincaré kesiti (c) Bu sistemin Poincaré kesitinde $c=0.5$ alınmasıyla oluşan Poincaré kesiti	11
Şekil 2.4 : İkinci kaotik sistemde uygulanan üç basamaklı işaret fonksiyonu	12
Şekil 2.5 : (2.5) denkleminde doğrusal olmayan fonksiyon olarak 3 basamaklı işaret fonksiyonu kullanıldığında (sekiz sarmallı kaotik sistem)($\varepsilon, n, \beta, \varphi$)=(0.05, 1, 0.3, 0.2) parametre değerleri için elde edilen kaotik çekici	13
Şekil 2.6 : Üçüncü kaotik sistemde kullanılan beş basamaklı işaret fonksiyonu.....	13
Şekil 2.7 : (2.5) denkleminde doğrusal olmayan fonksiyon olarak beş basamaklı işaret fonksiyonu kullanıldığında (On iki sarmallı kaotik sistem) ($\varepsilon, n, \beta, \varphi$)=(0.05, 1, 0.3, 0.2) parametre değerleri için elde edilen kaotik çekici	14
Şekil 2.8 : x_k sayı dizisinin saat işaretinin periyodunun belli anlarında örneklenmesi.....	15
Şekil 3.1 : (a) $t = \{t_k \mid \omega t_k \bmod 2\pi = 0\}$ Poincaré kesitinde ($c=0$) ve (b) $t = \{t_k \mid \omega t_k \bmod 2\pi = T/2\}$ Poincaré kesitinde ($c=0.5$) ile ilgili $\{x_k\}$ dizisinin histogram diyagramları.....	19
Şekil 3.2 : (a) $t = \{t_k \mid \omega t_k \bmod 2\pi = 0\}$ ($c=0$) (b) $t = \{t_k \mid \omega t_k \bmod 2\pi = T/2\}$ ($c=0.5$) ile ilgili $\{x_k\}$ dizisinden elde edilen ikili-kodlu sayıların poker testi sonuçlarının eşik ile değişimi.....	19
Şekil 3.3 : Saat işaretinin $t_k = \{t_k \mid \omega t \bmod 2\pi = T/4\}$ anında olası eşik aralığı için poker testi ve entropy sonuçları.....	20
Şekil 3.4 : Dört sarmallı kaotik sistemde a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, için x durum değişkeninin Poincaré kesitindeki dağılımını gösteren histogram diyagramları (140,000 nokta kullanılmıştır)	22
Şekil 3.5 : Dört sarmallı kaotik sistemde g) $c=0.2726$, h) $c=0.3218$, i) $c=0.3525$, j) $c=0.3976$, k) $c=0.4345$, l) $c=0.4680$ için x durum değişkeninin Poincaré kesitindeki dağılımını gösteren histogram diyagramları (140,000 nokta kullanılmıştır).....	23
Şekil 3.6 : a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, anlarındaki entropy testinin sonucunun eşik aralığı ile değişimi	24

Şekil 3.7	: g) $c=0.3525$, h) $c=0.3976$, i) $c=0.4345$, j) $c=0.4680$, k) $c=0.4345$, l) $c=0.4680$ anlarındaki entropy testinin sonucunun eşik aralığı ile değişimi	25
Şekil 3.8	: $c=0.1475$ anında poker testinin sonucunun eşik aralığı ile değişimi	26
Şekil 3.9	: (a) Sekiz sarmallı kaotik sistem kullanılarak Poincaré kesitinde $c=0$ için örneklenerek elde edilen X değerlerinin histogram diyagramı (b) Poker testi sonucu (c) entropy sonucu.....	27
Şekil 3.10	: Sekiz sarmallı kaotik sistemde (a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, anlarında x durum değişkeninin Poincare kesitindeki dağılımını gösteren histogram diyagramları	28
Şekil 3.11	: Sekiz sarmallı kaotik sistemde g) $c=0.3525$, h) $c=0.3976$, i) $c=0.4345$, j) $c=0.4680$, k) $c=0.4345$, l) $c=0.4680$ anlarında x durum değişkeninin Poincare kesitindeki dağılımını gösteren histogram diyagramları	29
Şekil 3.12	: (a) Sekiz sarmallı kaotik sistemde Poincaré kesitinde (a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, anlarındaki entropy testinin sonucunun eşik aralığı ile değişimi.....	31
Şekil 3.13	: g) $c=0.3525$, h) $c=0.3976$, i) $c=0.4345$, j) $c=0.4680$ anlarındaki entropy testinin sonucunun eşik aralığı ile değişimi	32
Şekil 3.14	: (a) On iki sarmallı kaotik sistem kullanıldığında elde edilen histogram diyagramı (b) Poker testi sonucu (c) entropy sonucu.....	34

OTONOM OLMAYAN KAOTİK SİSTEMLERDE RASGELE SAYI ÜRETİMİNİN İNCELENMESİ

ÖZET

Son yıllarda birçok bilim dalında karşılaşılan konulardan biri olan kaos, deterministik bir sistemin ilk koşullara olan aşırı hassasiyetinin sonucunda ortaya çıkan periyodik olmayan uzun zamanlı davranışlardır. Elektronik ve haberleşmenin birçok alanında kaos kullanılmaktadır. Bunun başlıca sebebi, kaotik işaretlerin zamanda düşük özilişki fonksiyonuna sahip olmaları ve geniş bantlı özellikleridir. Bilgisayar teknolojisinin gelişmesiyle de kaos araştırmalarının nümerik analizine büyük katkılar sağlanmış ve bu konuyla ilgili olan araştırmalara hız kazandırmıştır. Bu tezde, otonom olmayan kaotik sistemlerden rasgele sayı üretilmesinde yeni bir parametre sunulmuştur. c parametresi, rasgelelik için yeni bir parametredir. Bu parametreyle rasgele sayı üretiminin karakteristiği artırılabilir.

Bu çalışmanın ilk bölümünde kaos kavramının nasıl ortaya çıktığına, kaosun tanımına, tarihçesine değinilmiş ve kaotik sistemlerin belli başlı uygulama alanlarına örnek sunulmuştur. Ayrıca otonom olmayan kaotik sistemlerinin kullanılmasının sebebi verilmiştir. Bu çalışmada otonom olmayan kaotik osilatörden rasgele sayı üretilmesi inceleneceğinden, ikinci bölümde söz konusu kaotik osilatörler ve bu sistemlerin matematiksel denklemleri tanıtılmıştır. Rasgele sayı üreteçlerinin çalışma prensipleri anlatılmıştır. İkili-kodlu sayı dizilerinin elde edilmesi için bir yöntem verilmiştir. c parametresinden bahsedilmiştir. Dört, sekiz ve oniki sarmallı sistemlerde elde edilen kaotik çekiciler gösterilmiştir. Sayı dizilerinin rasgeleliğini ölçmek için kullanılan rasgelelik testlerine yer verilmiştir. Üçüncü bölümde ise otonom olmayan kaotik sistemlerden elde edilen rasgele sayı dizisinin rasgeleliğini incelemek amacıyla ilk yol olarak olası eşik değerleri için üretilen ikili-kodlu sayılar poker testine tabi tutulmuş, ikinci yol olarak da entropisi hesaplanmıştır. Elde edilen rasgele sayı dizilerinin c parametresinin değişimiyle, kaynak periyodunun hangi aralığında daha nitelikli olduğu incelenmiştir. Ayrıca kaotik çekicinin sarmal sayısının artmasının elde edilecek rasgele sayı dizisinin niteliğini artırıp arttırmadığı incelenmiştir. Son olarak dördüncü bölümde tezle alakalı elde edilen sonuçlar ve öneriler verilmiştir.

RANDOM NUMBER GENERATION AT THE NON-AUTONOMOUS CHAOTIC SYSTEMS

SUMMARY

Chaos which is recently met in many scientific field, is aperiodic complex behaviour occurring by the sensitive behaviour of the deterministic system on the initial conditions. Electronics and telecommunication are the fields whose, in many aspects, benefit from these systems. The main reason is chaotic signals have low correlation functions and wideband futures. Developing computer technology contributes numeric analysis used in chaotic researches which has accelerated in the chaos studies. In this thesis, a new parameter is presented which is used for random numbers are generated from non-otonomous chaotic systems. c parameter is a new parameter for randomness. It might be used to increase characteristic of random number generating. In the first chapter of this thesis, it is explained how the chaos was explored, the definition of the chaos and the main application areas of the chaos. In addition to this, it is explained why non-otonomous chaotic systems are used. Since in this work, the random numbers will be attained from nonotonomous chaotic osilators, in the second chapter the matematical equations of chaotik oscillator and non-otonomous chaotic systems are explained. The operational principals of the random number generators is indicated. There is a method given to form binary number series. It is mentioned about c parameters. Chaotic attractors attained in various systems are shown. There are also randomness tests given. In third chapter, two ways are given to investigate the randomness of the generated numbers from nonotonomous chaotic systems. After this, the poker test is applied to the series as the first way. For the second way, the entropy of the binary numbers is calculated for the potential threshold values. It is tested in which period interval of the source generated random numbers are more qualified by means of c parameter.

In addition, it is given whether the increasing step number of the signal function used as a source has positive effect at generating random numbers. Finally in the fourth chapter, the conclusions and some suggestions of this thesis is given.

1. GİRİŞ

Kaos üzerine yapılan çalışmaların tarihçesi 1890'lı yıllara dayanmaktadır [1]. Henri Poincaré bu tarihlerde, gezegenlerin sürekli kendi yörüngelerinde hareket etmelerine bir açıklama bulmak istemekteydi. Bu nedenle Poincaré yeni bir analitik metot geliştirerek kaosu keşfindeki ilk adımları atmıştır. Poincaré'nin ardından bu düşünce akımını takip edenler arasında matematikçi Andrey Kolmogorov gelmektedir. Çalışmalarında genel olarak dinamik sistemlerin düzensiz (irregular) özelliklerini incelemiştir. 1960 yılında ise matematikçi Stephen Smale dinamik sistemlerin bütün davranışlarını sınıflandıran bir çalışma gerçekleştirmiştir [1].

Teorideki bu çalışmaları takiben kaosu pratikteki uygulamaları ile ilgili ilk çalışmalar David Ruelle ve Floris Takens isimli matematikçiler tarafından gerçekleştirilmiştir. Amerikan fizikçileri Harry Swinney, Jerry Golub ve Fransız fizikçi Albert Libchaber'in çalışmaları da kaos modelleri ve sınıflandırılmaları ile ilgili birçok soruyu gün ışığına çıkarmıştır [1].

Kaos üreten sistemlerin niteliksel davranışları hakkında literatürde birçok çalışma mevcuttur. Bu tür sistemlerin davranışları bilgisayarlar aracılığı ile gerçekleştirilen nümerik analizler ile incelenebilir. Son yıllarda bilgisayar teknolojileri geçirdikleri ilerleme sayesinde kaos araştırmalarına geçmişe oranla çok daha büyük katkılar sağlayabilmektedirler.

Elektronik ve haberleşmenin birçok alanında çeşitli kaos sistemlerine rastlanmaktadır. Bunun başlıca sebebi, kaotik işaretlerin zamanda düşük özilişki fonksiyonuna sahip olmaları ve geniş bantlı yapılarıdır.

1.1 Kaosun Anlamı

Bilgisayar ve benzeri hesaplayıcılarda bir reel sayı sonlu basamakla ifade edilmekte ve bu nedenle kaotik sistemlerin bu araçlarla analizinde büyük hatalar yapılabilmektedir. Gerçekte istenmeyen bu özellik nedeniyle rastgele olmayan (deterministic) sistemlerde bile kaosu olabileceği farkedilmiştir. Meteorolojist

Lorenz bu tezin ilk savunucularından olmuştur. Hava tahminlerinde kullanmış olduğu metotları bilgisayar ile gerçekleğinde elde ettiği benzetim (simulation) sonuçlarının hatalı olduğunu tespit etmiş ve nedenini ondalık sayı basamaklarının yuvarlanması olarak tespit etmiştir. Başta önemsiz sayılabilecek bu hatalar, işlem tekrarlandıkça artmaktadır. Başka bir deyişle, model denklemleri doğru olması durumunda bile uzun zaman aralığında son derece hatalı sonuçlar alınabilmektedir. Örneğin, $p + rp(1 - p) = 0$ ifadeli sistem için $r = 3$, $p_0 = 0.01$ varsayımı altında elde edilen sonuçlar Tablo 1.1’de verilmektedir [1]. Birinci sütun iterasyon sırasını, diğer sütunlar ise sırasıyla bir işlemci yardımı alınmaksızın ve alınarak elde edilen sonuçları göstermektedir.

Tablo 1.1: Kaosun keşfedilmesindeki çıkış noktası için örnek iterasyon değerleri

İterasyon Sırası	İşlemcisiz	İşlemci ile
1	<u>0.0397</u>	<u>0.0397</u>
2	<u>0.15407173</u>	<u>0.15407173</u>
3	<u>0.5450726260</u>	<u>0.5450726260</u>
4	<u>1.288978001</u>	<u>1.288978001</u>
5	<u>0.1715191421</u>	<u>0.1715191421</u>
10	<u>0.7229143012</u>	<u>0.7229143012</u>
10	<u>0.7229143012</u>	<u>0.722</u>
15	<u>1.270261775</u>	<u>1.257214733</u>
20	0.5965292447	1.309731023
25	1.315587846	1.089173907
30	0.3742092321	1.333105032
100	0.7355620299	1.327362739

Onuncu iterasyonda sonuçlar işlemci tarafından yuvarlatılmaya başlandığında görüldüğü üzere, tamamen farklı sonuçlar elde edilmiştir. Bu tabloda basit bir kaotik sistemin ilk koşullara olan yüksek duyarlılığı nedeniyle oluşan farklı davranışları görülebilmekte ve bu özellik kaotik sistemlerin öngörülemezlik özelliği olarak adlandırılmaktadır.

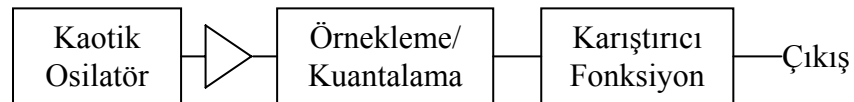
1.2 Kaotik Sistemler ve Uygulama Alanları

Kaotik sistemleri, otonom olan ve otonom olmayan kaotik sistemler olarak iki grupta sınıflandırabiliriz. Bu çalışmada otonom olmayan kaotik sistemler kullanılmıştır. Otonom olan sistemlerde rasgele sayı üreticinin bit üretme hızı sabit değildir. Otonom olmayan kaotik sistemlerde ise saat işareti kaynak olarak kullanılır. Bit üretme hızı sabittir. Bu tezde otonom olmayan kaotik sistemlerden elde edilen rasgele sayı dizilerinin, kullanılan kaotik çekicilerin sarmal sayılarının artmasıyla etkilenmesi incelenmiştir. Burada rasgele sayı üretilirken ikinci bölümde bahsi geçen Poincaré dönüşümünden yararlanılmıştır. Yine ikinci bölümde üzerinde durulan c parametresi, rasgelelik için yeni bir parametre olarak sunulmuştur. Bu parametrenin değişimiyle rasgele sayı üretiminin karakteristik özellikleri incelenebilir ve artırılabilir.

Kaotik sistemlerin uygulama alanları, tekrarlamayan ve kestirilemeyen sayı dizilerine ihtiyaç duyulan her yer yaygın olarak kullanıldıkları alanlardır. Elektronik ve haberleşmede en çok kullanıldıkları uygulama alanlarına örnek olarak rasgele sayı üretimi, mesaj saklama ve şifreleme verilebilir [2-5].

1.2.1 Rastgele Sayı Üreteçleri (RSÜ)

Gün geçtikçe rastgele sayılara, dolayısıyla da rastgele sayı üreteçlerine olan ihtiyaç artmaktadır. Genellikle çekirdek adı verilen bir başlangıç değerine bazı sayısal işlemler uygulanmasıyla rastgele sayılar üretilmektedir. Rastgele sayı üretme işlemi aynı çekirdek kullanıldığında tekrarlanabilir bir hal alır ve çıkışı gerçek anlamda rastgele olmaz.



Şekil 1.1: RSÜ blok diyagramı

Tekrar edilemeyen değerlere ulaşmak için kaotik bir süreçten yararlanmak mümkündür. Şekil 1.1’de bir kaotik osilatörün değerlerinin örneklenmesi ve kuantalanması prensibiyle oluşturulan yapının rasgele sayı üretici olarak

kullanılması gösterilmiştir. Kaotik sürecin mevcut durumunun tahmin edilmesi mümkün olmayacağından çekirdek de aynı şekilde tahmin edilemez olacaktır. Çıkışın gerçek anlamda tekrar-edilemez olmasını her rasgele sayının kendine özel bir çekirdeğe sahip olması ile sağlar. Burada örneklemeyle elde edilen değerlere bir karıştırıcı fonksiyon uygulanmasıyla üretilen bit dizisindeki korelasyonun daha da azaltılmış olması sağlanır. Bütün bunların tek bir kırmık üzerinde üretilmesi, sistem parametrelerinin çok azının dışarıdan gözlemlenebilir olması nedeniyle, güvenliği önemli ölçüde arttıracaktır. Bu kırmığın bir bilgisayarın alt sistemi olarak kullanılması, bilgisayarda yapılacak simülasyonlar için kolayca rasgele sayı üretebilmeyi sağlar.

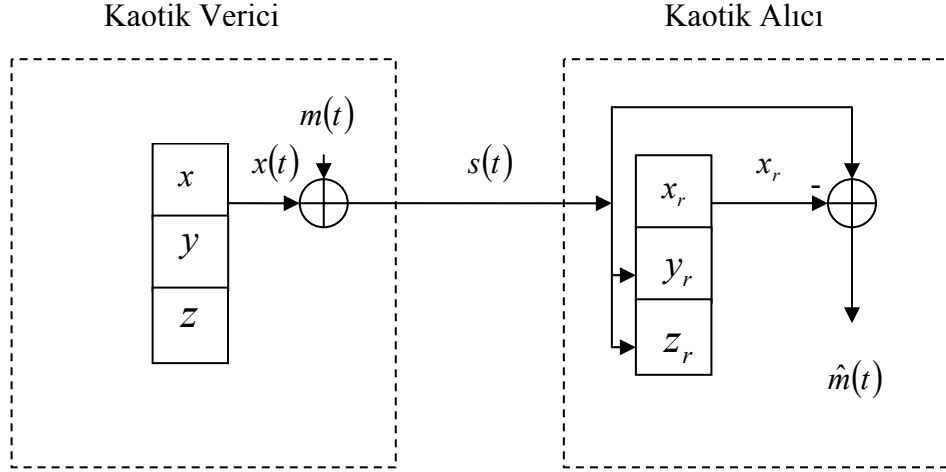
Örnekleme ile elde edilen değerler 1 veya 0 şeklinde kodlanır. Kaotik sürece uygulanan örnekleme işlemi osilatörün temel frekansına göre çok küçükse, örneklerin korelasyonu çok düşük olacaktır. Daha hızlı örneklemeye ise daha yüksek çıkış hızı istendiğinde ihtiyaç duyulur. Bu durumda bile düşük korelasyonlu değerler elde etmek için uygun karıştırıcı fonksiyonlar kullanılabilir. Kuantalama sonrasında ortaya çıkabilecek bitler arası dengesizliğin giderilmesini karıştırıcı fonksiyonlar mümkün kılmaktadır [2].

1.2.2 Yalancı Rastgele Sayı Üreteçleri (YRSÜ)

Gerçekte deterministik sistemler olan YRSÜ'ler sayı üretme işlemine dışarıdan üretece verilen ve üretcin rastgele dizi oluşturmada kullanacağı çekirdek ile başlarlar. Bu çekirdek rastgeleliği sağlayan tek kaynak olmakta ve YRSÜ'nün ürettiği çıkışların rastgeleliği bu çekirdeğin rastgeleliğinden daha yüksek olamamaktadır. YRSÜ'ler sınırlı durum makinelerinde kullanılan algoritmalar olup, basit ve hızlı program rutinlerinde kullanılmaya yatkındırlar. Bu nedenle YRSÜ'lerin çıkışları periyodiktir fakat periyotları çok uzundur [3]. Tamamen rastgele sayı üretmeye yatkın olmadıklarından kısıtlı kullanım alanları vardır. Güvenilirlik açısından RSÜ'lere oranla yetersiz kalırlar.

1.2.3 Mesaj Saklama

Bu bölümde, kaotik sistemlerin eş zamanlama özelliği kullanılarak haberleşmede mesaj işaretlerinin kaotik işaretler içine gizlenmesi incelenecektir. Mesaj saklama yapısı ve bu yapının alıcı-verici alt sistemleri Şekil 1.2'de görülebilir.



Şekil 1.2: Mesaj Saklama Yapısı

Örnek olarak alınan Lorenz Sisteminin ölçeklenmiş durum değişkenleri sırasıyla (1.1) de verilmektedir.

$$\begin{aligned}
 \dot{x} &= \sigma(y - x) & \dot{x}_r &= \sigma(y_r - x_r) \\
 \dot{y} &= rx - y - 20xz & \dot{y}_r &= rx - y_r - 20xz_r \\
 \dot{z} &= 5xy - bz & \dot{z}_r &= 5xy_r - bz_r
 \end{aligned} \tag{1.1}$$

Kaotik vericide iletilen $m(t)$ işaretine gürültüyü andıran maskeleye işareti $x(t)$ eklenir. Böylece, iletilen işaret $s(t) = m(t) + x(t)$ olarak ifade edilir. Alıcı, verici ile eş zamanlı diğer bir deyişle senkronize olmayı başladığında $x_r(t) \cong x(t)$ olur. Alıcı kısımda maskeleye işaretinin toplam işarettten çıkarılmasıyla gönderilen mesaj $\hat{m}(t) = s(t) - x_r(t)$ şeklinde elde edilir.

Bu yöntemin başarılı bir şekilde uygulanabilmesi için mesaj işaretinin güç seviyesinin, $x(t)$ güç seviyesinden önemli derecede küçük olması gerekmektedir [4].

1.2.4 Şifreleme

Bu bölümde bilginin güvenli bir şekilde iletilmesi sırasında kaotik süreçlerden nasıl yararlanıldığı gösterilecektir. Şifrelemede kullanılacak kaotik sistem olarak $x_{n+1} = bx_n(1 - x_n)$ ile verilen lojistik dönüşümünü ele alalım. Örnek olarak iletilen mesajın ASCII karakterlerinden oluştuğunu varsayalım. Bu denklemden elde edilen x değerleri, b parametresinin farklı değerleri için kaotik olmaktadır. Kaotik çekici

$\varepsilon = [V_{\max} - V_{\min}] / S$ genişliğinde S adet bölüme ayrılır. Tablo 1.2 de, S adet ASCII sembol gösterilmektedir. Burada sistemin x_0 başlangıç değerinin tespit edilen x_{n+1} durumuna gelmesi için gereken iterasyon sayısı, n inci sembolün şifrelenmiş halini gösterir. Ayrıca, şifrelenecek her karakter için kullanılacak başlangıç durumu bir önceki karakterin şifrelendiği anda gelinen durumdur. Şu halde şifrenin çözülebilmesi için S aralıkları, x_0 başlangıç değeri ve b kontrol parametresinin bilinmesi gereklidir [5].

Tablo 1.2: Kaosun şifrelemedeki uygulaması

ASCII Sembolü	İterasyon sayısı
*	S
@	S-1
#	S-2
\$	S-3
⋮	⋮
B	4
A	3
/	2
%	1

2. KAOTİK SİSTEMLER

Bu bölümün amacı, bu tezde kullanılacak otonom olmayan kaotik sistemler hakkında bilgi vermek ve bu sistemlerden nasıl rastgele sayı üretilbileceğini açıklamaktır.

Otonom olmayan kaotik osilatörler zamana bağlı periyodik bir kaynak fonksiyonu $f(t)$ içeren lineer olmayan bir diferansiyel denklem sistemi ile modellenenbilmektedir [6]. Doğrusal olmayan ve otonom bir sistemin kaos üretebilmesi için, Poincare-Bendixon Teoremi sonucu olarak sistemin en azından üçüncü dereceden olması gerekmektedir [6]. Otonom olmayan sistemlerde ise diferansiyel denklemin sağ tarafı t zaman değişkenine bağlı olmaktadır. Bu zaman değişkeni fazladan bir durum değişkenine karşı geldiğinden, otonom olmayan sistemlerin kaos üretebilmesi için, bunların en azından ikinci dereceden olmasının gerektiği sonucuna kolaylıkla varılabilir.

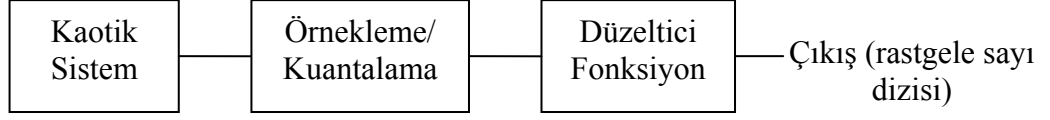
Öte yandan, literatürde incelenen otonom olmayan kaotik sistemlerin önemli bir bölümünde periyodik kaynak olarak sinüzoidal fonksiyonlar kullanılmıştır [6]. Bu fonksiyonun, çözümü $Z(t) = Z(0) \sin \phi t$ olan aşağıdaki lineer otonom sistemin çıkışından elde edildiği düşünelim:

$$\ddot{Z} + \phi^2 Z = 0 \quad (2.1)$$

Bu durumda otonom olmayan sistemlerin tüm durumlarının sınırlı olduğu dördüncü dereceden otonom bir sisteme eşdeğer olduğu görülebilir.

2.1 RSÜ' lerin Çalışma Prensipleri

Literatürde kaotik osilatörlerden rastgele sayı üretilmesi için, Şekil 2.1'de verilmiş temel sistem kullanılmaktadır [7]. Bu sistemde öncelikle osilatör çıkışı belirli bir frekansta örneklenir, çıkış değerleri kuantalanır, daha sonra da elde edilen bit dizisine düzeltici algoritmalar uygulanarak rastgele sayı üretimi sağlanır.



Şekil 2.1: Kaotik rastgele sayı üreten sistemin blok diyagramı

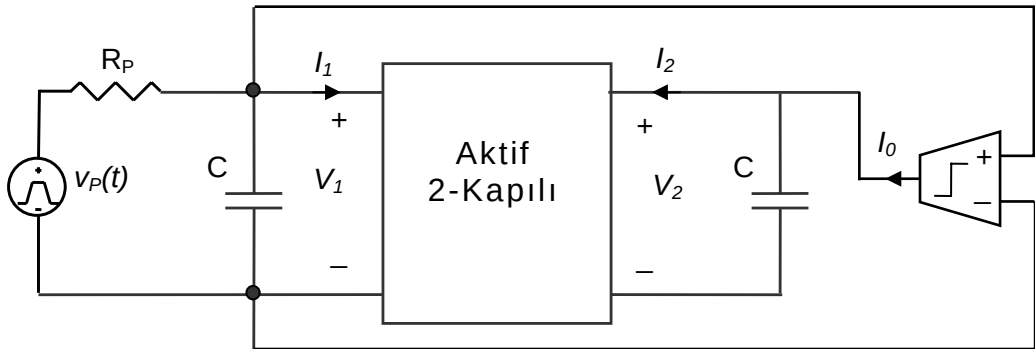
Rastgele olmayan bir kaotik sistemden rastgele sayı üretilebilmesi için sistemin çözümünün özilişki fonksiyonunun düşük değerli olması gerekmektedir. Bilinmektedir ki, kaotik bir sistemin çözümünün

$$r(\tau) = \frac{\int_0^{\infty} x(t)x(t+\tau)dt}{\int_0^{\infty} |x(t)|^2 dt} \quad (2.2)$$

şeklinde tanımlanan özilişki fonksiyonu τ büyüdükçe hızla sıfıra gitmektedir. Bunun nedeni kaotik sistemin başlangıç koşullarına aşırı duyarlı olmasıdır [8]. Bu nedenle kaotik sistemden ikili kodlu sayılı üretirken, üretimlerinin arasında yeterince uzun zaman geçen ikili kodlu sayıların arasındaki ilişki de düşük olacaktır. Ancak bu şekilde elde edilen sayıların düzgün dağılımlı olup olmadığının da kontrol edilmesi gerekmektedir.

2.2 Otonom Olmayan Kaotik Sistemler ile Rastgele Sayı Üretimi

Bu tezde otonom olmayan kaotik osilatörlerin rastgele sayı üretiminde nasıl kullanılacağı inceleneceğinden, söz konusu kaotik osilatörler bu bölümde kısaca tanıtılmıştır.



Şekil 2.2: Kaotik osilatör yapısı

Kısa devre parametreleri $\begin{bmatrix} I_1 \\ I_2 \end{bmatrix} = \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \end{bmatrix}$ şeklinde verilen bir aktif 2-kapılı ile

V_I gerilimi tarafından kontrol edilen, çıkış akımı I_o olan ve doymalı çalışan bir geçiş iletkenliği kuvvetlendiricisi içeren Şekil 2.2'deki devrenin durum denklemleri aşağıdaki gibi kolaylıkla elde edilebilir:

$$\begin{aligned} \dot{V}_{C1} &= \frac{1}{C} \left[- \left(g_{11} + \frac{1}{R_p} \right) V_{C1} - g_{12} V_{C2} \right] + \frac{1}{R_p C} V_p(t) \\ \dot{V}_{C2} &= \frac{1}{C} [-g_{21} V_{C1} - g_{22} V_{C2}] + \frac{I_o}{C} \end{aligned} \quad (2.3)$$

Bu arada $V_p(t) = V_p \operatorname{sgn}(\sin(\omega_p t))$, ω_p ise darbe kaynağının frekansı olmaktadır. I_{sat} geçiş iletkenliği kuvvetlendiricisinin doyma akımı olmak üzere, I_o akımı şu şekilde ifade edilebilir:

$$I_o = I_{sat} \operatorname{sgn}(V_1) = \begin{cases} I_{sat}, & V_1 \geq 0 \\ -I_{sat}, & V_1 < 0. \end{cases} \quad (2.4)$$

$X = -V_{C1} g_{22}^2 / I_{sat} g_{12}$, $Y = V_{C2} g_{22} / I_{sat}$ şeklinde yeni normalize durum değişkenleri tanımlanır ve $\varepsilon = 1 / g_{22} R_p$, $\beta = -V_p g_{22} / I_{sat} g_{12} R_p$, $\phi = \omega_p C / g_{22}$, $\tau = t(g_{22} / C)$, şeklinde tanımlanan parametreler yardımıyla, (2.3)'deki durum denklemleri

$$\begin{aligned} \dot{X} &= (1 - \varepsilon)X + Y + \beta p(\tau) \\ \dot{Y} &= -(1 + n)X - Y + f(X) \\ f(x) &= \operatorname{sgn}(x) \end{aligned} \quad (2.5)$$

şeklinde yazılabilir. Burada $p(\tau) = \operatorname{sgn}(\sin(\Phi\tau))$ olmaktadır. Her ne kadar (2.5) denklemleri, Şekil-2.2'deki devreyi modellese de, farklı $f(x)$ fonksiyonları için de bu denklemler kaotik davranabilmektedir. Bizim bu çalışmada inceleyeceğimiz üç farklı sistem

$f(x) = f_1(x) = \operatorname{sgn}(x)$, (Dört sarmallı kaotik sistem),

$f(x) = f_2(x) = \operatorname{sgn}(x) + \operatorname{sgn}(x+2) + \operatorname{sgn}(x-2)$ (Sekiz sarmallı kaotik sistem), ve

$f(x) = f_3(x) = \operatorname{sgn}(x) + \operatorname{sgn}(x+2) + \operatorname{sgn}(x-2) + \operatorname{sgn}(x-4) + \operatorname{sgn}(x+4)$ (On iki sarmallı kaotik sistem)

şeklinde tanımlanmıştır. Bu yeni sistemleri gerçekleyen devreler Şekil-2.2'deki doymalı geçiş iletkenliği kuvvetlendiricisinin yapısını değiştirerek kolaylıkla elde edilebilir.

Öncelikle tezde incelenen ilk sistemi ele alalım. Bu sistemde $f(x)=f_1(x)=sgn(x)$ alınmıştır. Bu sistem farklı parametre değerleri için farklı kaoslar üretmektedir. Örneğin $n=1.4$, $\varepsilon=0.05$, $\varphi=0.14$, $\beta=0.44$ parametre değerleri için Şekil 2.3a'daki kaotik çekici elde edilmektedir.

Burada eşitlik (2.5)'deki sistemden ikili kodlu sayıların elde edilmesi için bir yöntem verilmiştir. Önce sistem durumları, kaotik sisteme dışarıdan uygulanan periyodik işaretinin belli anlarında örneklenmektedir. Bu işlem, sistem durumlarının aşağıdaki şekilde tanımlanan Poincare kesitindeki izdüşümlerine karşı gelmektedir. Söz konusu Poincare kesiti,

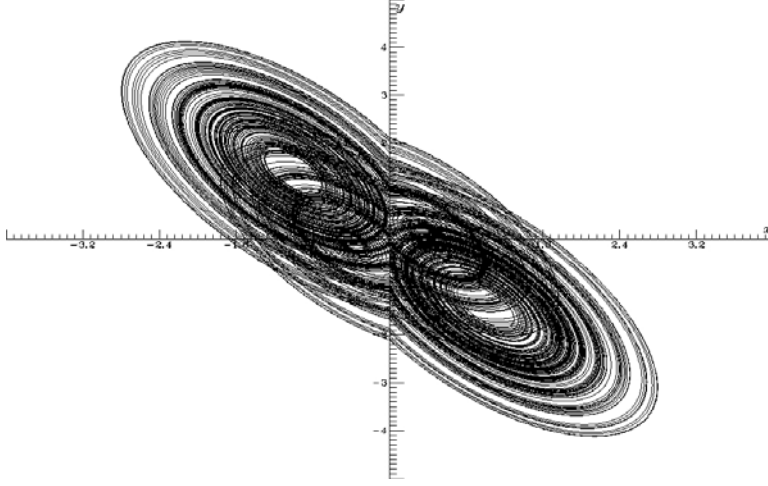
$$\Sigma := \{(x, \eta) \in R^n \times Z^1 : \eta = cT\} \quad (2.6)$$

olarak ifade edilir. Burada $Z^1 := [0, 2\pi)$, $\eta(t) = (\omega t) \bmod 2\pi$ ve $c \in (0, 1)$ olmaktadır. Bu işlem, bir yörüngenin her T saniyede bir örneklenmesi olarak ifade edilebilir. n . dereceden T periyotlu bir sürekli zaman sistemi, Poincaré dönüşümü olan $(n-1)$. derece ayırık zaman sistemine dönüştürülebilir. Sistemin x, y durumlarının (2.6)'da tanımlanan Poincare kesitindeki izdüşümleri Şekil 2.3b'de $c=0$ için, Şekil 2.3c'de ise $c=0.5$ için verilmiştir.

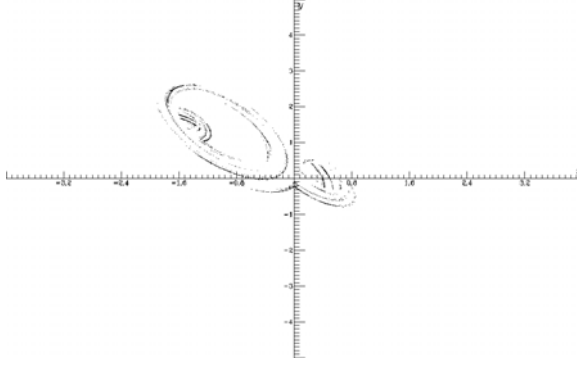
Şekil 2.3'de de görülen bu iki boyutlu izdüşümlerden elde edilen $\{x_k, y_k\}$ sayı dizileri

$$\begin{bmatrix} x_{k+1} \\ y_{k+1} \end{bmatrix} = P \left(\begin{bmatrix} x_k \\ y_k \end{bmatrix} \right) \quad (2.7)$$

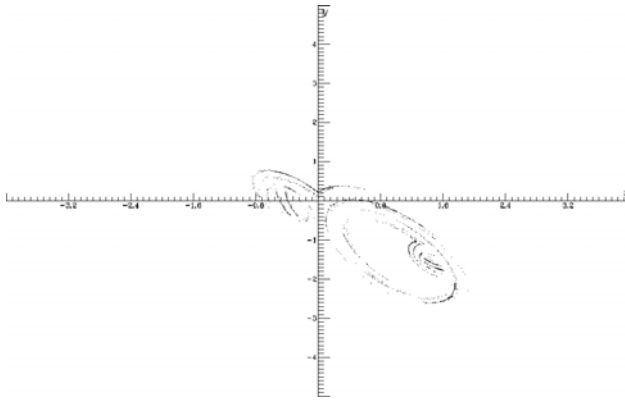
şeklinde tanımlanan bir ayırık dönüşüme karşı geldiğini varsayalım. Stroboskopik Poincare dönüşümü de denilen bu P dönüşümünün (2.5) bağıntısındaki sistemin deterministik olmasının nedeniyle her zaman tersi alınabilmektedir. Dikkat edilirse durum değişkenlerinden sadece biri dikkate alındığında yeni elde edilen dönüşüm tersi alınabilir (tersinir) değildir. Rastgele sayı üreteçlerinde kullanılan dinamik sistemlerin en önemli özelliklerinden birisinin tersinir olmama özelliği [9] olduğu



(a)



(b)



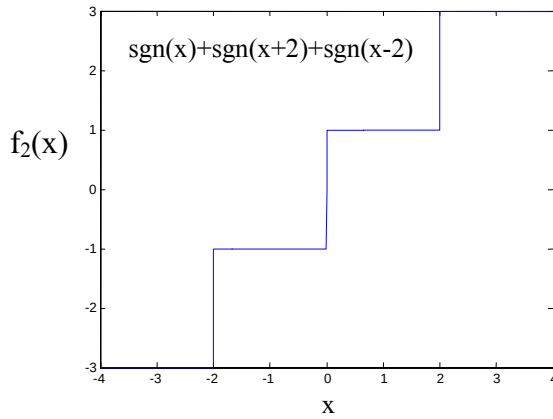
(c)

Şekil 2.3: a) Otonom olmayan kaotik sistemin nümerik analiz sonuçları (b) Bu sistemin Poincaré kesitinde $c=0$ alınarak oluşan Poincaré kesiti (c) Bu sistemin Poincaré kesitinde $c=0.5$ alınarak oluşan Poincaré kesiti

düşünülerek bu tezde kullanılan yöntemde sadece x durum değişkeni dikkate alınmakta ve bir $\{x_k\}$ reel sayı dizisi elde edilmektedir. Daha sonra bu sayı dizisinden $S_i = \text{sgn}(x_i - q)$ denklemleri ile ikili kodlu rastgele sayı S_i üretilmiştir. Burada $\text{sgn}(\cdot)$ signum fonksiyonunu, x_i 'ler Poincaré kesitindeki x değerlerini, q ise yaklaşık olarak seçilmiş eşik değerini göstermektedir.

Ancak elde edilen ikili sayı dizisinin dağılımı düzensizdir. Burada bu düzensizliği önleyebilmek için, sistemimizde literatürde de sıklıkla kullanılan Von Neumann tekniği uygulanmıştır [12]. Bu teknikte 01 bit çifti 0'a, 10 bit çifti ise 1'e dönüştürülür. Geri kalan bit çiftleri ise kullanılmaz. Daha sonra bu elde edilen sayı dizisinin rastgeleliğini kontrol etmek amacıyla, dizi bir sonraki kısımda değinilecek olan standart rastgele sayı testlerine tabi tutulur.

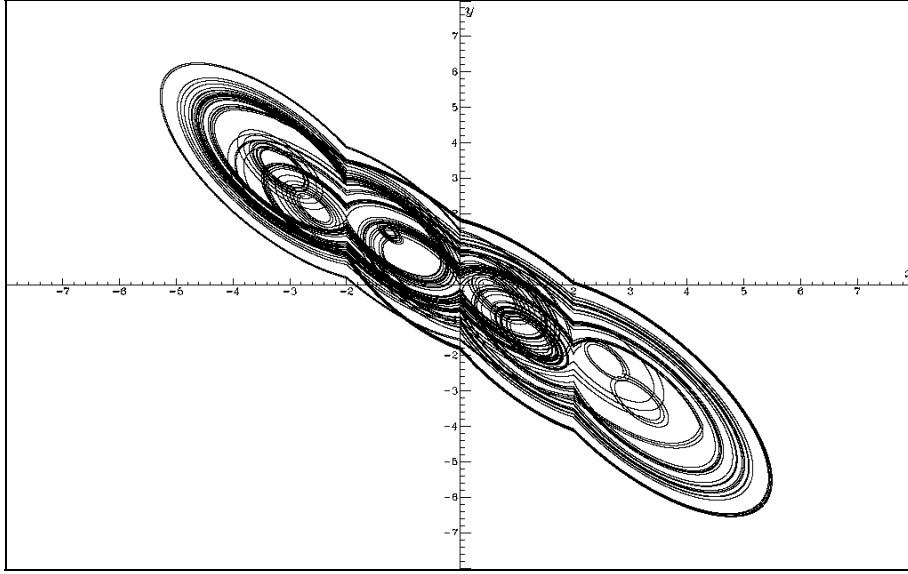
Bu çalışmada incelenen ikinci kaotik sistem olarak (2.5) bağıntısındaki $f(x) = f_2(x) = \text{sgn}(x) + \text{sgn}(x+2) + \text{sgn}(x-2)$ alınmıştır. Bu fonksiyon şekil 2.4'de gösterilmektedir.



Şekil 2.4: İkinci kaotik sistemde uygulanan üç basamaklı işaret fonksiyonu

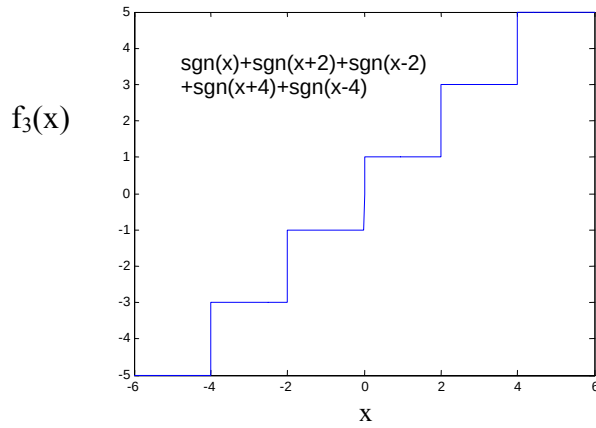
Bu ikinci sistem de farklı parametre değerleri için kaos üretebilmektedir. Örneğin $n=1$, $\varepsilon=0.05$, $\varphi=0.2$, $\beta=0.3$ alınarak, (2.5) denklemleri Şekil 2.5a'da verilen çok sarmallı kaotik çekiciyi üretmektedir.

(2.5) bağıntısıyla modellenen kaotik sistemden ikili kodlu rastgele sayılar daha önce anlatıldığı gibi elde edilebilir.

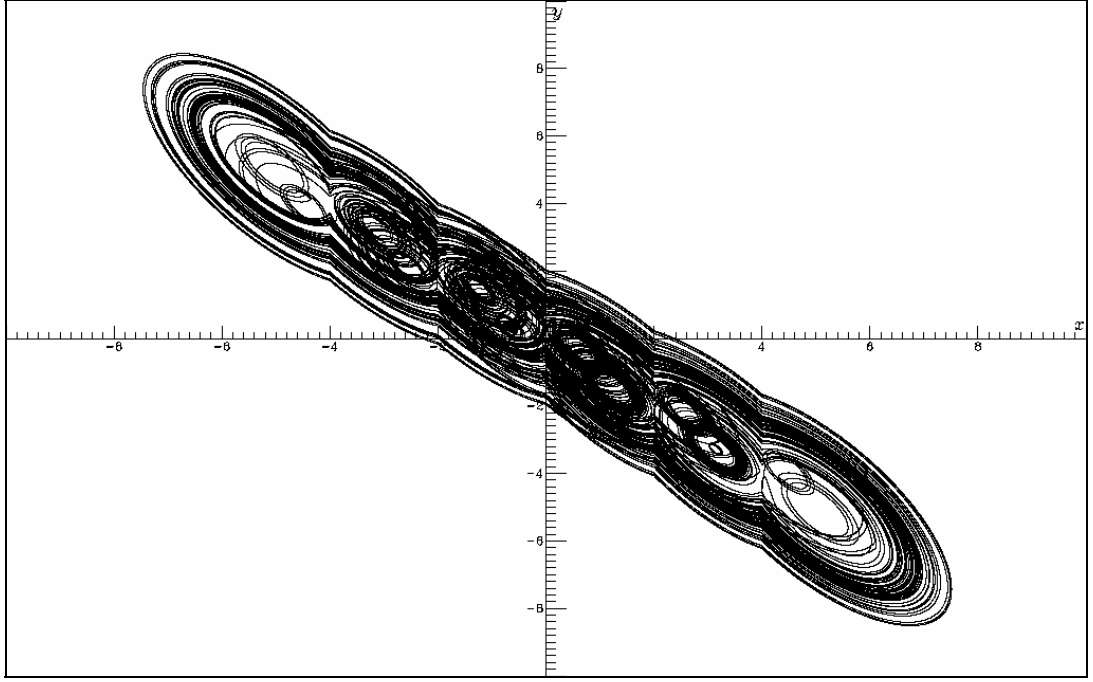


Şekil 2.5 : (2.5) denkleminde doğrusal olmayan fonksiyon olarak 3 basamaklı işaret fonksiyonu kullanıldığında (sekiz sarmallı kaotik sistem) $(\varepsilon, n, \beta, \varphi) = (0.05, 1, 0.3, 0.2)$ parametre değerleri için elde edilen kaotik çekici

Bu tezde incelenecek üçüncü sistem olarak (2.5) bağıntısındaki doğrusal olmayan $f(x) = f_3(x) = \text{sgn}(x) + \text{sgn}(x+2) + \text{sgn}(x-2) + \text{sgn}(x+4) + \text{sgn}(x-4)$ fonksiyonu alınmıştır. $f_3(x)$ çok basamaklı işaret fonksiyonu Şekil 2.6 da verilmiştir.



Şekil 2.6: Üçüncü kaotik sistemde kullanılan beş basamaklı işaret fonksiyonu



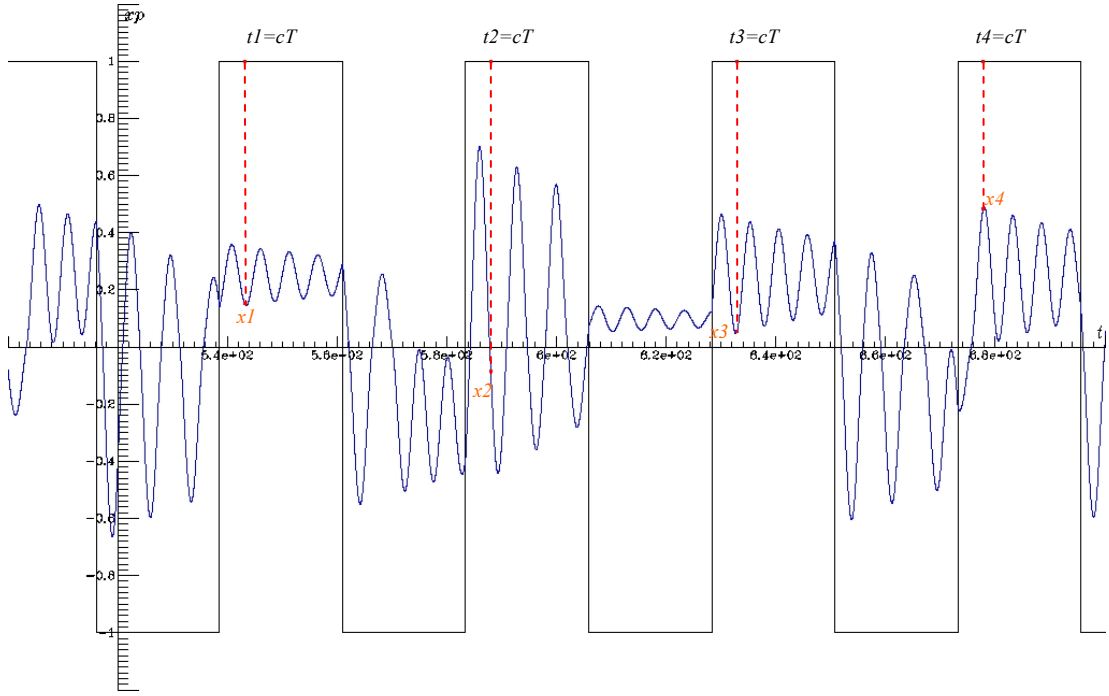
Şekil 2.7 : (2.5) denkleminde doğrusal olmayan fonksiyon olarak beş basamaklı işaret fonksiyonu kullanıldığında (On iki sarmallı kaotik sistem) $(\varepsilon, n, \beta, \varphi)=(0.05, 1, 0.3, 0.2)$ parametre değerleri için elde edilen kaotik çekici

Bu üçüncü sistem de farklı parametre değerleri için kaos üretebilmektedir. Örneğin $n=1$, $\varepsilon=0.05$, $\varphi=0.2$, $\beta=0.3$ için sistem Şekil 2.7’deki kaotik çekiciyi üretmektedir.

Burada da (2.5) bağıntısıyla modellenen kaotik çekiciden ikili kodlu rastgele bitler elde edebilmek için kaotik sistemin stroboskopik Poincaré dönüşümü kullanılmıştır.

İşaret fonksiyonunun daha yüksek katlı şekilde uygulanması Şekil 2.5 ve 2.7’de de görüldüğü gibi, kaotik çekicinin daha çok sayıda sarmal içermesine neden olmaktadır. Bu durumun elde edilecek rastgele sayı dizisinin niteliğini artırıp arttırmadığı bir sonraki bölümde incelenmektedir.

Şekil 2.8’de kaotik çekiciye Poincaré dönüşümü uygulandığında elde edilen x_k sayı dizisinin, sisteme uygulanan saat işaretinin periyodunun belli anlarında örneklenmesi gösterilmektedir.



Şekil 2.8 : x_k sayı dizisinin saat işaretinin periyodunun belli anlarında örneklenmesi

2.3 Rastgelelik Testleri

Sayı dizilerinin rastgeleliğini ölçmek için NIST (Amerikan Ulusal Standart ve Teknoloji Enstitüsü) ve FIPS (Federal Bilgi İşleme Standartları) 140-1’de tavsiye edilen bazı testler bulunmaktadır [10]. Bu bölümde bu testler tanıtılarak, testlerin 20 bin bit uzunluklu sayı dizisi için yazılmış MATLAB kodları verilmektedir.

Tek-Bit Testi (monobit test): Rastgele üretilmiş bit dizisi içerisindeki 1’lerin ve 0’ların yaklaşık olarak aynı sayıda olup olmamasına dayanır. Örneğin, 20 bin bitlik dizi için 1’lerin sayısı X olarak gösterilsin. $9654 < X < 10346$ koşulu sağlanıyorsa bit dizisi testi geçer.

Poker Testi (poker test): 20 bin bitlik dizi 5 bin adet 4 bitlik kümelere ayrılır. Her bir kümenin görülme sıklığı sayılır. $f(i)$, i sayılı kümenin görülme sıklığını göstermek üzere

$$X = (16/5000) \times \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000 \quad (2.8)$$

denkleminde $1.03 < X < 57.4$ sağlanıyorsa test başarılıdır.

Koşu Testleri (runs test): Ardı ardına gelen sıfırların ya da birlerin oluşturduğu dizi, koşu olarak adlandırılır. Test edilen dizideki tüm koşular sayılır ve kaydedilir. 6'dan uzun koşuların sayısı, 6'lık koşuların sayısına eklenir. Koşu sayılarının tümü tabloda verilen aralıklar içerisinde kalırsa dizi testi başarıyla geçer.

Tablo 2.1: Koşu sayılarının içinde bulunması gerekli aralıklar

Koşu Uzunluğu	İstenen Aralık
1	2267-2733
2	1079-1421
3	502-748
4	223-402
5	90-223
6+	90-223

Uzun Koşu Testi (long-run test): 34 veya daha uzun bir koşu tanımlanarak rastgele sayı dizisinde olup olmadığı kontrol edilir. Eğer bu uzun koşu, incelenen sayı dizisinde yoksa test başarılıdır.

Bu tezde ikili-kodlu sayıya dönüştürme, Von Neumann metodu ve poker testi için kullanılan MATLAB kodları Ek-1' de yer almaktadır.

3. KAOTİK SİSTEMLERDEN RASGELE SAYI ÜRETİLMESİNİN İNCELENMESİ

Otonom olmayan kaotik sistemlerden ikili kodlu rasgele sayı dizisi üretmek için incelenen yöntemin bilgisayar benzetimlerinde web'den bedava olarak indirilebilen Dynamics Solver programından yararlanılmıştır [<http://tp.lc.ehu.es/JMA/ds/ds.html>]. Bu program, sürekli ve ayırık sistemlerin alt ve üst sınır değer problemlerinin çözümleri için kullanılmaktadır.

Bölüm 2'de tanıtilan otonom olmayan kaotik sistemlerin matematiksel denklemleri kullandığımız programa uygun olacak şekilde girilmiştir:

$$\begin{aligned}\dot{X} &= (1 - \varepsilon)X + Y + \beta p(\tau) \\ \dot{Y} &= -(1 + n)X - Y + f(x).\end{aligned}\tag{3.1}$$

Burada $f(x)$ fonksiyonu, incelenecek üç sistem için sırasıyla $f(x)=f_1(x)=\text{sgn}(x)$ (Dört sarmallı kaotik sistem), $f(x)=f_2(x)=\text{sgn}(x)+\text{sgn}(x+2)+\text{sgn}(x-2)$ (Sekiz sarmallı kaotik sistem), $f(x)=f_3(x)=\text{sgn}(x)+\text{sgn}(x+2)+\text{sgn}(x-2)+\text{sgn}(x-4)+\text{sgn}(x+4)$ (Oniki sarmallı kaotik sistem) şeklinde alınmıştır. ε , n , β , φ parametre değerleri de sırasıyla birinci sistemde 0.05, 1.4, 0.44, 0.14, ikinci ve üçüncü sistemde 0.05, 1, 0.3, 0.2 şeklinde alınmıştır.

Bu sistemler için x durum değişkeninden $x_k = x(t_k)$, $\{t_k \in \mathbb{R} \mid \omega t_k \bmod 2\pi = 0\}$ şeklinde oluşturulan $\{x_k\}$ reel sayı kümesi dikkate alınır. Uygun bir q eşik değeri belirlendikten sonra bu x_k değerlerinden ikili kodlu sayı dizisi S_k

$$S_k = \begin{cases} 1, & x_k - q > 0 \\ 0, & x_k - q \leq 0 \end{cases}\tag{3.2}$$

şeklinde elde edilmektedir. Buradaki esas problem q eşik değerinin belirlenmesidir. Bu problemin çözümünde iki farklı yol izlenmektedir. İlk olarak, önce $\{x_k\}$ sayılarının dağılımına bakarak uygun eşik değeri için olası bir aralık belirlenir. Daha sonra bu aralıktaki tüm eşik değerleri için ikili kodlu sayılar üretilir ve bunlar FIPS-

140-1 rasgele sayı test dizisindeki önemli testlerden biri olan poker testine tabii tutulur [10]. Poker testi sonucunda elde edilen ve Bölüm 2.3’de açıklanan Xp değerlerinin olağan sınırlar içinde kalmasını sağlayan sayı dizisini üreten eşik aralığı uygun eşik aralığı olarak belirlenir.

İkinci yol ise olası eşik değerleri için üretilen ikili kodlu sayıların entropisini hesaplamak ve ideal rasgele sayı üreticinin entropisi olan $\ln(2)$ ’ye en yakın olan değeri veren eşik değerini belirlemektir.

$O_n = \{b_0, b_1, b_2, \dots, b_{n-1}\}$ n bit uzunluklu diziler, $b_i \in \{0,1\}$ ve $P(O_n)$, O_n dizisinin olasılığı olmak üzere Ortalama Shannon Entropisini (ASE, Average Shannon Entropy)

$$ASE = \lim_{n \rightarrow \infty} -\frac{1}{n} \sum_{O_n} [P(O_n) \ln(P(O_n))] \quad (3.3)$$

$$ASE = \lim_{n \rightarrow \infty} \frac{H_n}{n} \quad (3.4)$$

şeklinde ifade edilir [12].

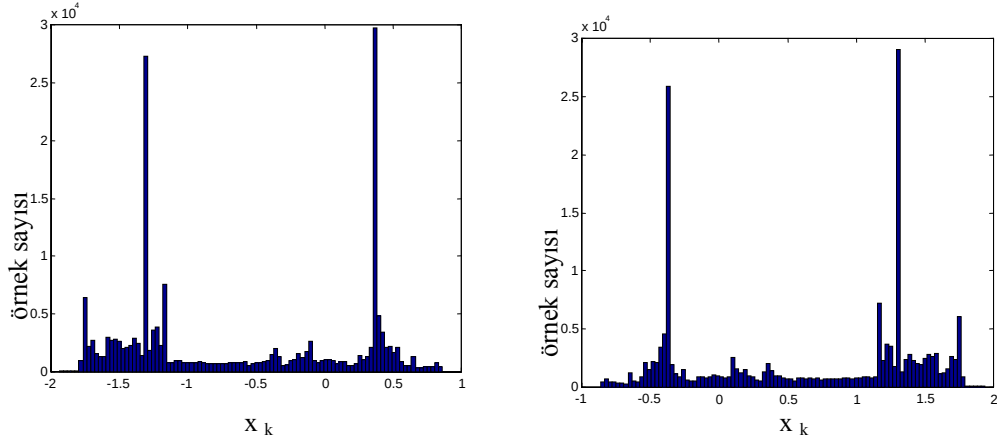
İdeal durumda $P(O_n) = \frac{1}{2^n}$ değerini alır. Bu durumda (3.3) bağıntısında

$P(O_n) = \frac{1}{2^n}$ değerini yerine koyarsak, $\ln 2$ değerini elde ederiz. Bu çalışmada, işlem süresinin uzun olduğu düşünülerek diziler 6 bitlik olarak incelenmiştir. Ek-2’deki Matlab kodu kullanılan sayı dizisinin entropisini hesaplamak amacıyla kullanılmıştır.

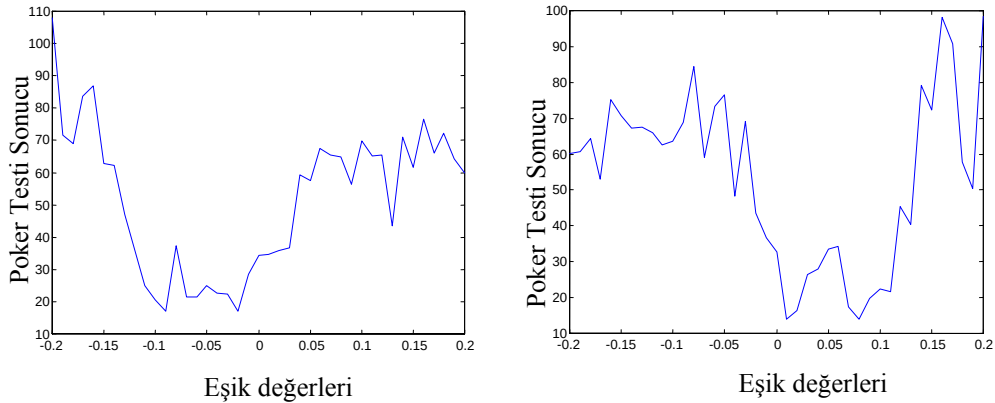
3.1 Dört Sarmallı Sistemden Rasgele Sayı Üretilmesi

Bu kısımda (3.1) bağıntısının $f(x)=f_1(x)$ durumundaki sonuçları verilmiştir. Otonom olmayan dört sarmallı kaotik sistemden rasgele sayı üretmek amacıyla Bölüm 2’de açıklandığı gibi, (3.1)’de verilen denklemlerin nümerik analizi yapılmış ve Poincaré dönüşümü kullanılarak ilk önce $x(t)$ durum değişkeninin $t = \{t_k \in \mathbb{R} \mid \omega t_k \bmod 2\pi = 0\}$ ve $t = \{t_k \in \mathbb{R} \mid \omega t_k \bmod 2\pi = T/2\}$ ayrık zamanlarında 185 bin değeri kaydedilmiştir. Bu x_k değerlerinin MATLAB programı ile histogramları çizdirilmiştir. Şekil 3.1’de x_k değerlerinin Poincaré kesiti $c=0$ ve $c=0.5$ alınarak oluşan dağılımdan elde edilen histogram diyagramları gösterilmektedir.

Bu sistemde birinci durum için Şekil 3.1a' daki diyagram kullanılarak olası eşik aralığı $(-1.5, 0.5)$ arasında seçilmiştir. Bu aralıktaki bütün eşik değerleri için öncelikle ikili-kodlu sayı dizisi üretilmiştir. Sonra bu sayı dizisine Von Neumann Metodu uygulanarak üretilen bitlerin düzgün dağılımlı olması sağlanmıştır. Bu metottan sonra geriye kalan bit sayısı Poincaré kesiti $c=0$ ve $c=0.5$ alındığında 20 bin değerdedir. Daha sonra bu dizinin rasgeleliğini incelemek amacıyla poker testine tabi tutulmuştur.



Şekil 3.1: a) $t = \{t_k \mid \omega t_k \bmod 2\pi = 0\}$ ($c=0$) b) $t = \{t_k \mid \omega t_k \bmod 2\pi = T/2\}$ ($c=0.5$) ile ilgili $\{x_k\}$ dizisinin histogramları (185 bin değer için)

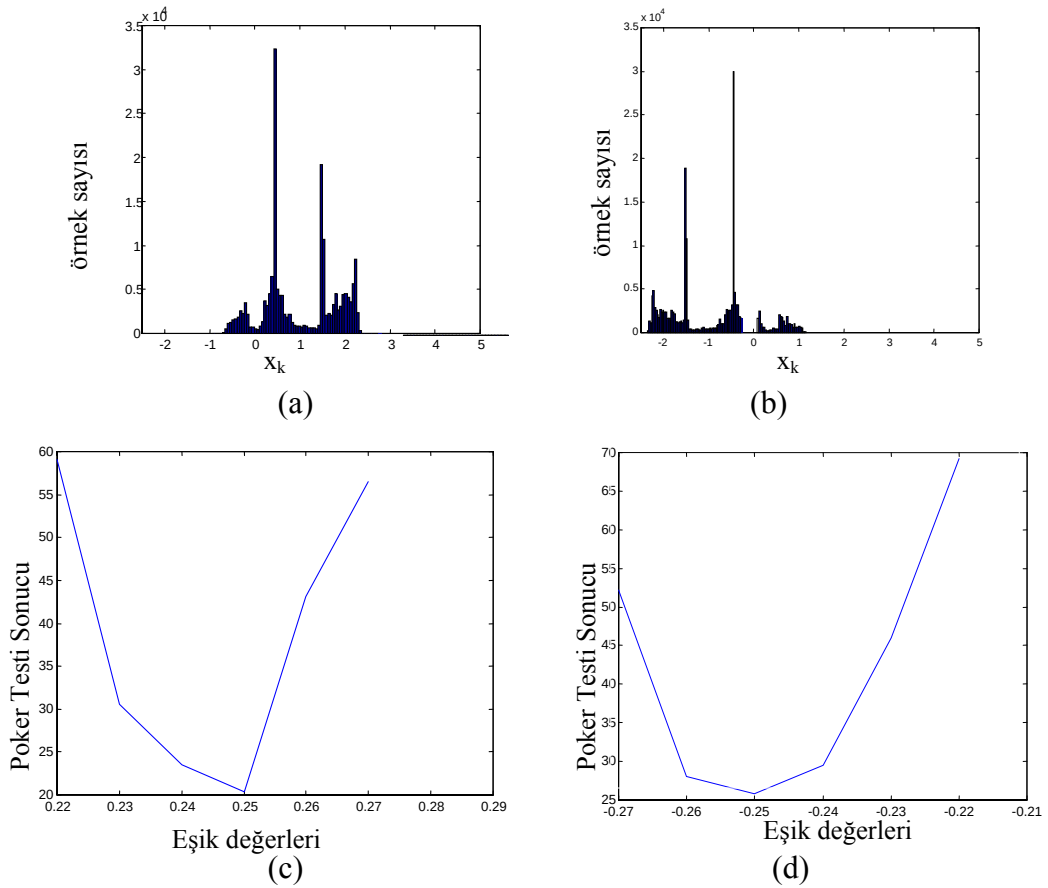


Şekil 3.2: a) $t = \{t_k \mid \omega t_k \bmod 2\pi = 0\}$ ($c=0$) b) $t = \{t_k \mid \omega t_k \bmod 2\pi = T/2\}$ ($c=0.5$) ile ilgili $\{x_k\}$ dizisinden elde edilen ikili-kodlu sayıların poker testi sonuçlarının eşik ile değişimi.

Kullanılan eşik aralığının her iki durum için poker testi sonucuyla olan değişimi Şekil 3.2'de gösterilmiştir. Şekil 3.2(a)'da görüldüğü üzere birinci sistemde q eşik değerini -0.13 ile 0.03 arasında alındığında üretilen ikili-kodlu sayı dizisinin poker testinden geçtiği gözlenmiştir. Öte yandan, Şekil 3.1'deki histogramlar ve Şekil

3.2'deki grafikler incelendiğinde şekillerin birbirinin simetriği olduğu görülmektedir. Farklı başlangıç koşulu için uygulandığında yine aynı histogram diyagramlarına ve entropy grafiklerine ulaşıldığı gözlenmiştir. Bu durum göz önünde bulundurulduğunda sistemin $t = \{t_k \mid \omega t_k \bmod 2\pi = 0\}$ ve $t = \{t_k \mid \omega t_k \bmod 2\pi = T/2\}$ anlarında aynı şekilde davrandığı ve sistemden üretilen ikili-kodlu sayı dizilerinin rasgeleliğinin aynı olduğu sonucuna varılabilir.

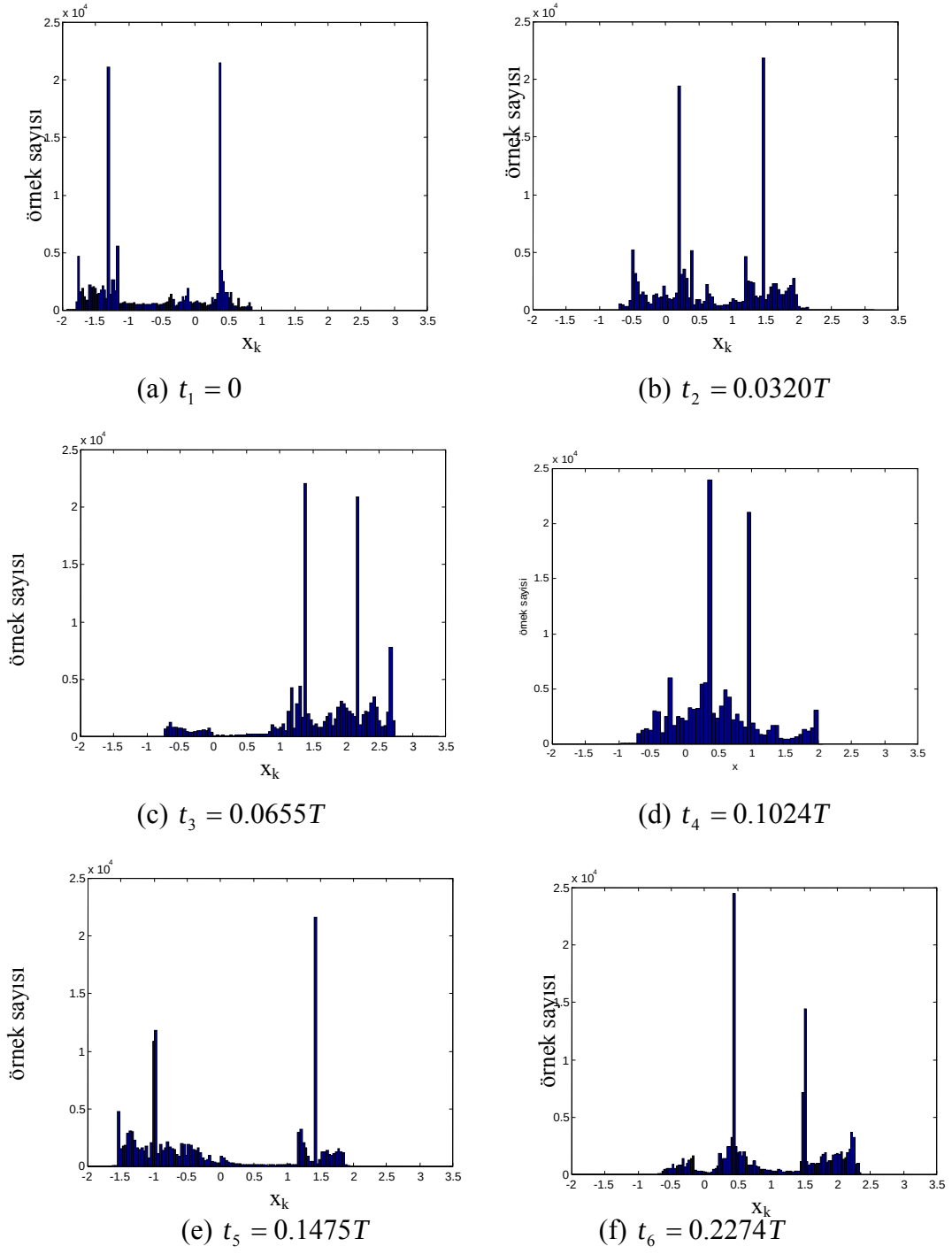
Daha sonra $t = \{t_k \mid \omega t_k \bmod 2\pi = cT\}$ şeklinde tanımlanan Poincare kesitinde $c=1/4$ ve $c=3/4$ alınmış ve her bir durum için x 'in 185 bin değeri kaydedilmiştir. Şekil 3.3a ve b'de her bir durum için histogramlar verilmiştir. Şekil 3.3c ve d'de, üretilen ikili-kodlu sayıların hangi eşik aralıklarında poker testinden geçtikleri görülmektedir.



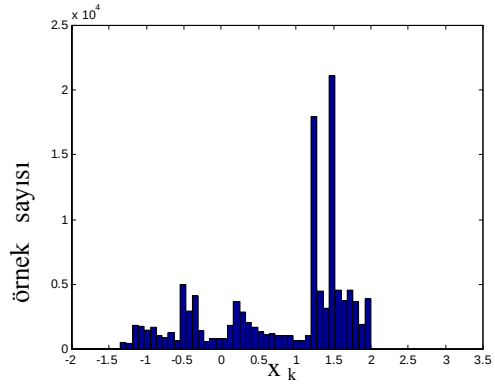
Şekil 3.3: a), c) $t = \{t_k \mid \omega t_k \bmod 2\pi = T/4\}$ b), d) $t = \{t_k \mid \omega t_k \bmod 2\pi = 3T/4\}$ ile ilgili $\{x_k\}$ dizisinden elde edilen ikili-kodlu sayıların poker testi sonuçları

Şekil 3.3'den, $c=1/4$ ve $c=3/4$ için elde edilen histogram ve poker test sonuçları ile ilgili eğrilerin de Şekil 3.1 ve 3.2'de de olduğu gibi birbirlerinin simetriği oldukları açıkça görülmektedir. Bu bilgilerin neticesinde $t = \{t_k \mid \omega t_k \bmod 2\pi = cT\}$ şeklinde tanımlanan Poincare kesitinde $0 < c < 0.5$ ile $0.5 < c < 1$ aralığındaki histogram dağılımları ve poker testi sonuçlarının $x=0$ eksenine göre simetrik çıktığı düşünülebilir. Bu durum Bölüm 2'de açıklanan ve Şekil-2.2'de verilen sistemin Poincare kesitindeki çekicisinin simetri özelliğinin bir sonucudur. Bu nedenle bundan sonraki bölümlerde Poincare kesitindeki c parametresi $0 < c < 0.5$ olarak alınması yeterli olacaktır.

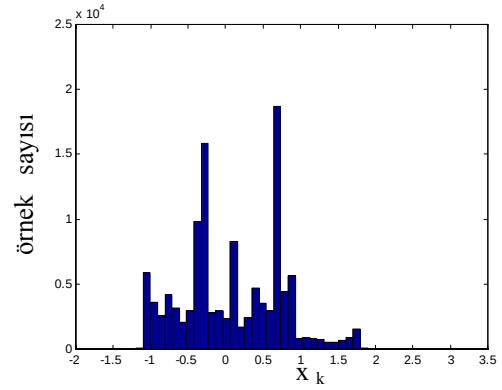
Birinci sistem için Bölüm.2' de bahsi geçen c parametresi, $0 \leq c < 0.5$ arasında değiştirilerek Dynamical Solver programı yardımıyla her durum için nümerik analiz yapılmıştır. Poincaré dönüşümünden faydalanarak $t_1 = 0T$, $t_2 = 0.0320T$, ..., $t_{10} = 0.4680T$ anları için örnekleme yapılmıştır. Her bir durum için elde edilen histogramlar Şekil 3.4 ve 3.5'de gösterilmektedir. Bu diyagramlar incelendiğinde, zamanla birlikte dağılımlarda bir süreklilik gözlenmiştir. Her bir durum için genelde iki tepe noktası gözlenmiştir. İleriki çalışmalarda iki eşik değeri kullanılarak sistemlerin nümerik analizi yapılabilir.



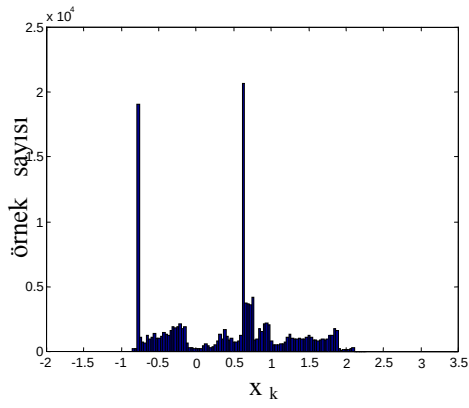
Şekil 3.4: Dört sarmallı kaotik sistemde a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, için x durum değişkeninin Poincaré kesitindeki dağılımını gösteren histogram diyagramları (140,000 nokta kullanılmıştır)



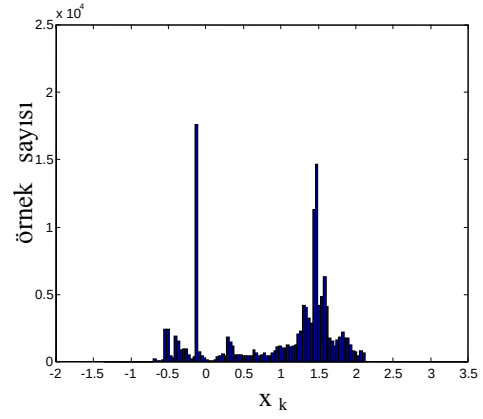
(g) $t_7 = 0.2726T$



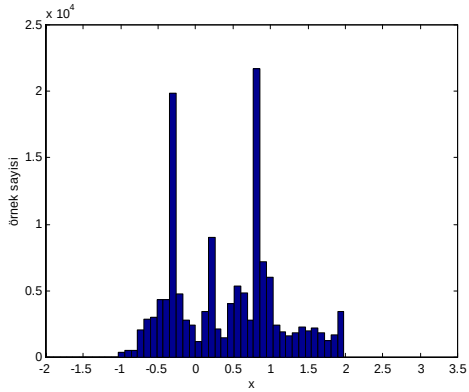
(h) $t_8 = 0.3218T$



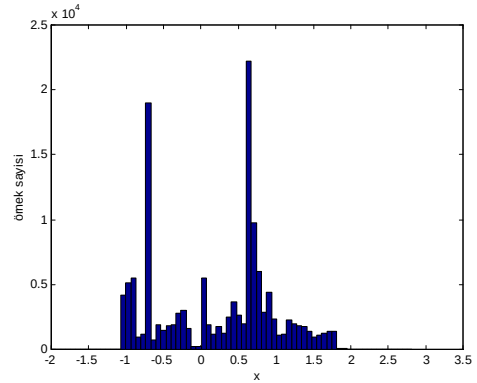
(i) $t_9 = 0.3525T$



(j) $t_8 = 0.3976T$



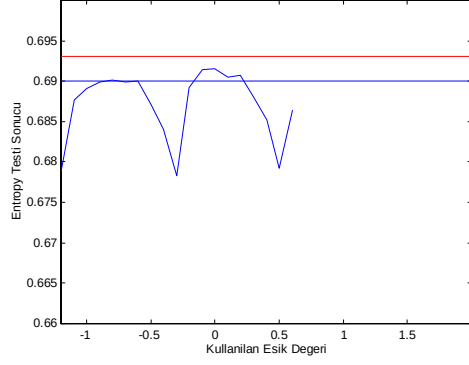
(k) $t_9 = 0.4345T$



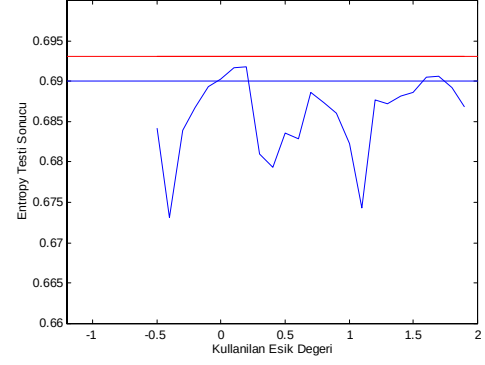
(l) $t_{10} = 0.4680T$

Şekil 3.5: Dört sarmallı kaotik sistemde g) $c=0.2726$, h) $c=0.3218$, i) $c=0.3525$, j) $c=0.3976$, k) $c=0.4345$, l) $c=0.4680$ için x durum değişkeninin Poincaré kesitindeki dağılımını gösteren histogram diyagramları (140,000 nokta kullanılmıştır)

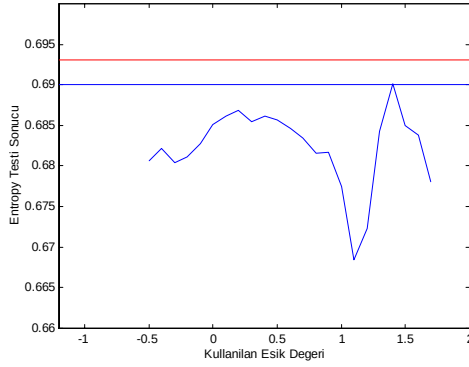
Her durum için üretilen ikili-kodlu sayıların entropileri hesaplanarak Şekil 3.6 ve 3.7’de gösterilmektedir. Bu grafikler incelendiğinde ise $\ln(2)$ ’ ye en yakın değer $t_5 = 0.1475T$ anında Şekil 3.6 (e)’ deki grafikte eşik değeri 1 için 0,6918 olarak bulunmuştur.



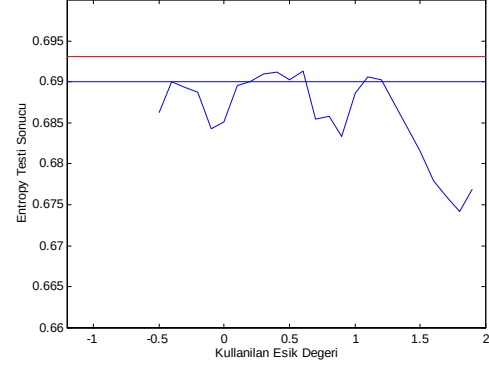
(a) $t_1 = 0$



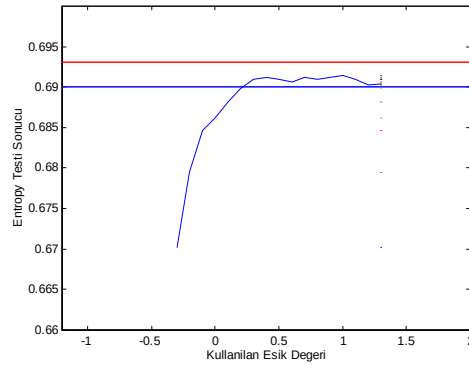
(b) $t_2 = 0.0320T$



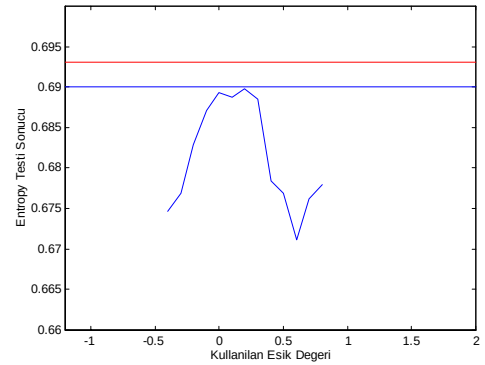
(c) $t_3 = 0.0655T$



(d) $t_4 = 0.1024T$

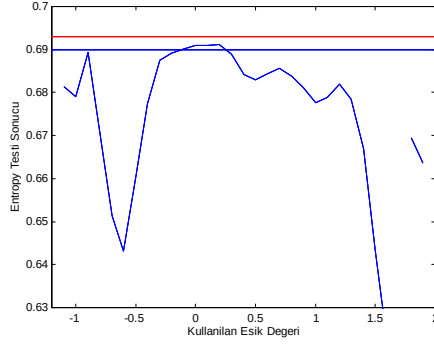


(e) $t_5 = 0.1475T$

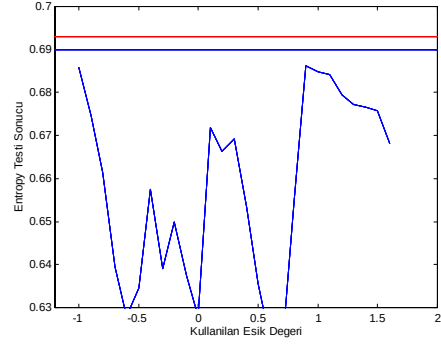


(f) $t_6 = 0.2274T$

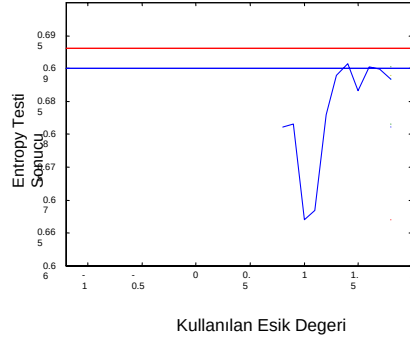
Şekil 3.6: Dört sarmallı kaotik sistemde a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, için entropy testinin sonucunun eşik aralığı ile değişimi (— $=\ln 2$, — $=0.69$)



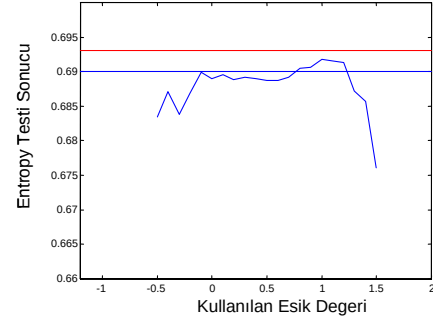
(g) $t_7 = 0.2726T$



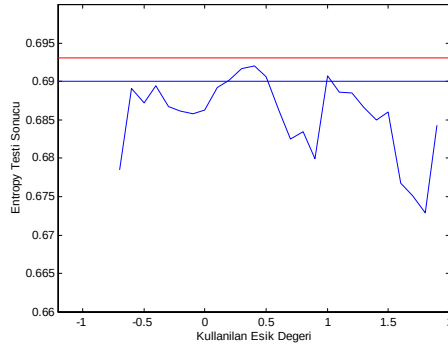
(h) $t_8 = 0.3218T$



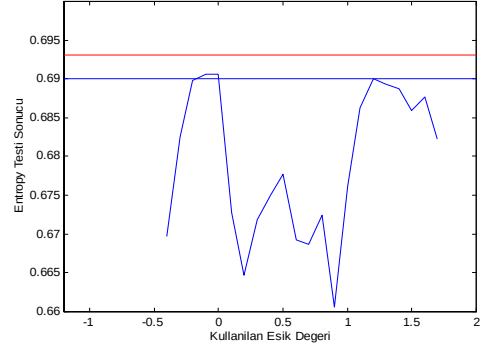
(i) $t_9 = 0.3525T$



(j) $t_{10} = 0.3976T$



(k) $t_{11} = 0.4345T$

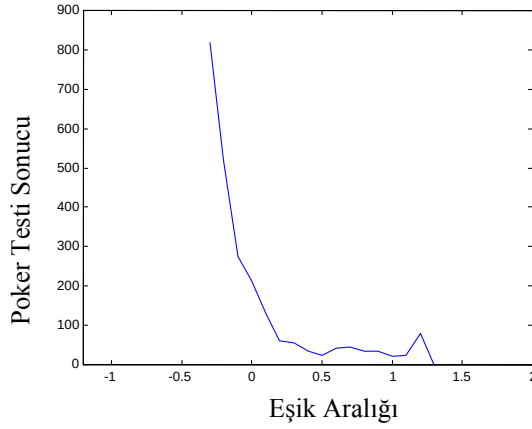


(l) $t_{12} = 0.4680T$

Şekil 3.7: Dört sarmallı kaotik sistemde g) $c=0.2726$, h) $c=0.3218$, i) $c=0.3525$, j) $c=0.3976$, k) $c=0.4345$, l) $c=0.4680$ için entropy testinin sonucunun eşik aralığı ile değişimi (— = $\ln 2$, — =0.69)

Şekil 3.6 ve 3.7'deki grafikler incelendiğinde, $c=0.1475$ için entropinin 0.69 değerinin üzerinde olduğu en geniş aralık elde edilmiştir. Bu örnek için RSÜ'nin çıkışları bir önceki bölümde bahsedilen testlere tabi tutulmuş ve testleri geçtiği gözlenmiştir.

$t_5 = 0.1475T$ için poker testide uygulanmıştır. Şekil 3.8’ da $c=0.1475$ için poker testi sonucu gösterilmektedir.



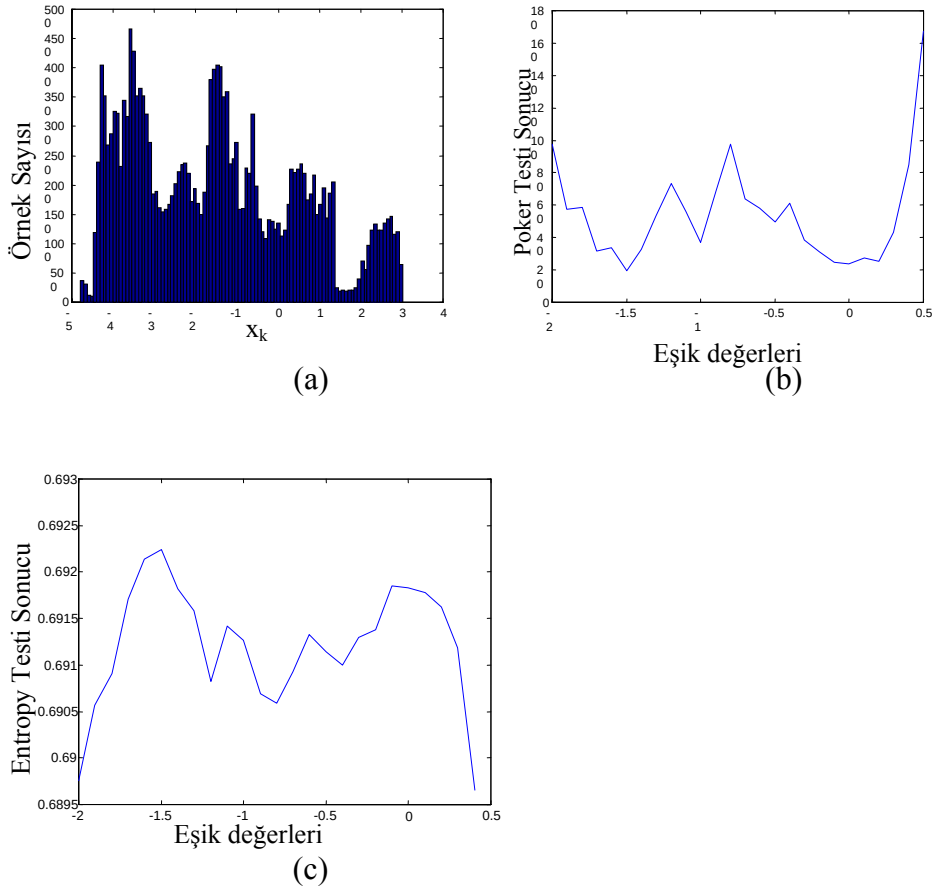
Şekil 3.8: $c=0.1475$ değeri için poker testinin sonucunun eşik aralığı ile değişimi

Bu grafikten 0.3 ile 1.1 arasındaki eşiklerin poker testini geçtiği gözlenmiştir. Bu arada entropi sonuçlarına bakıldığında bu aralıkta 0.69 üzerinde diğer bir deyişle istenilen aralıkta olduğu sonucuna varılmıştır.

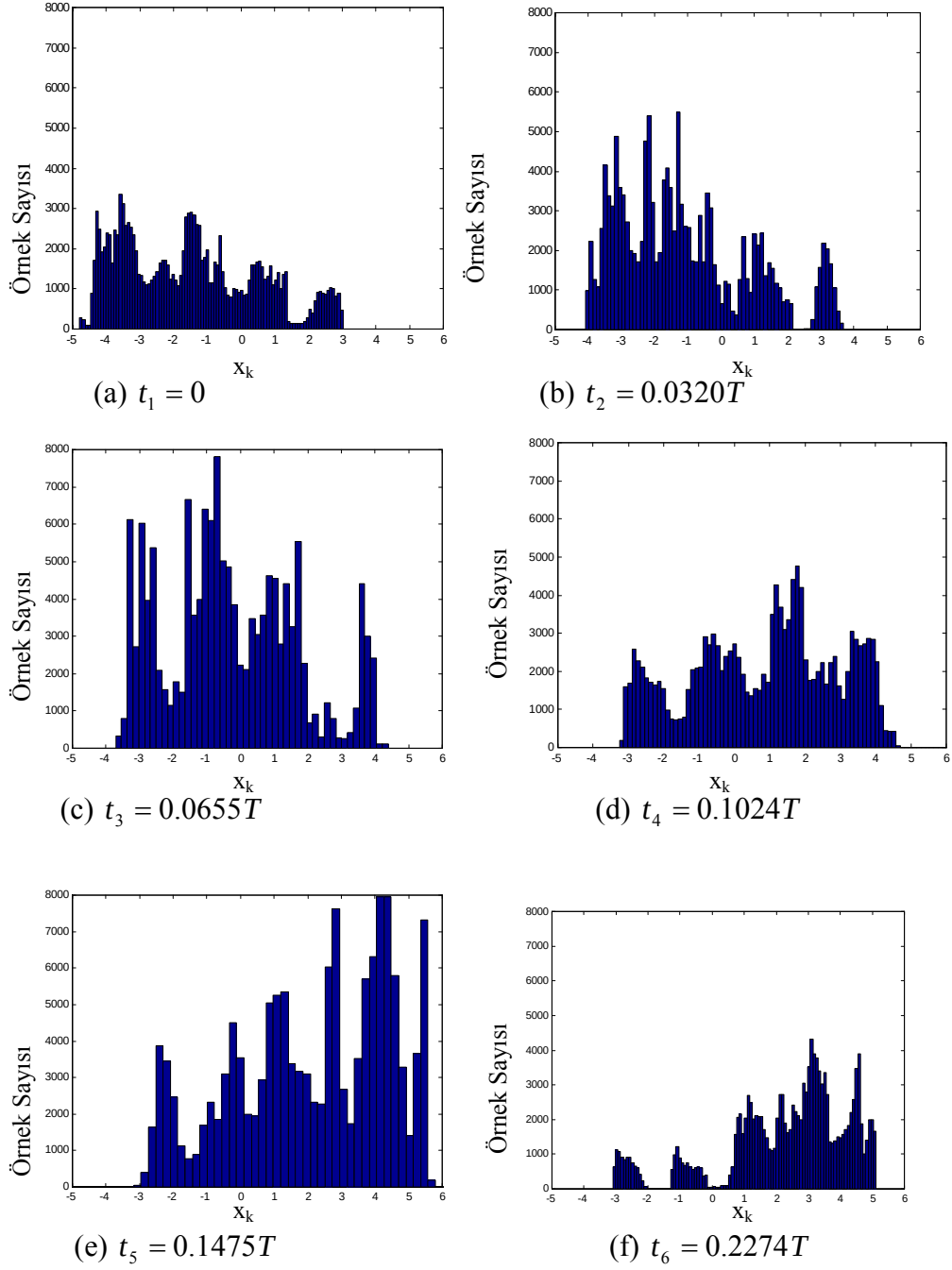
3.2 Sekiz Sarmallı Sistemden Rasgele Sayı Üretilmesi

Bu sistem için lineer olmayan fonksiyon olarak $f(x)=f_2(x)=sgn(x)+sgn(x+2)+sgn(x-2)$ olan sekiz sarmallı kaotik sistem kullanılarak kaos elde edilmiş ve nümerik analizi yapılmıştır. Poincare kesitinde $c=0$ alınmış ve x durum değişkeninin 190 bin değeri kaydedilmiştir. Burada da birinci sistemdeki gibi sadece x değerleri kullanılmış olup, y değerleri alınmamıştır. Bu sistem için 3.1 (a), (b) ve (d)’de verilmiş olan denklemler kullanılarak nümerik analizler gerçekleştirilmiştir. Şekil 3.9(a)’da x_k değerlerinin Poincare kesitinde $c=0$ alınarak örneklenmesinden oluşan dağılımından elde edilen histogram diyagramı gösterilmektedir. Bu diyagram dikkate alındığında birinci sisteme göre eşik aralığının arttığı gözlenmiştir. -5 ile 3 aralığındaki tüm eşik değerleri için önce ikili-kodlu sayı dizisi üretilmiş, sonra sayı dizisinin düzgün dağılımlı olması açısından Von Neumann Metodu uygulanmıştır. Bu sistemden elde edilen dizinin rasgeleliğini test etmek amacıyla önce poker testine tabi tutulmuş, daha sonra bu ikili-kodlu sayıların entropisi hesaplanmıştır. Şekil 3.9(b)-(c)’ de bu sistem için sonuca varılan eşik aralıklarının (-2 ile 0.5 aralığında) poker testiyle ve entropisiyle olan sonuçları gösterilmiştir. Poker testi sonucunda elde edilen minimum değer 19.46 olup, bu değer için kullanılan eşik -1.5’ dur. Bu

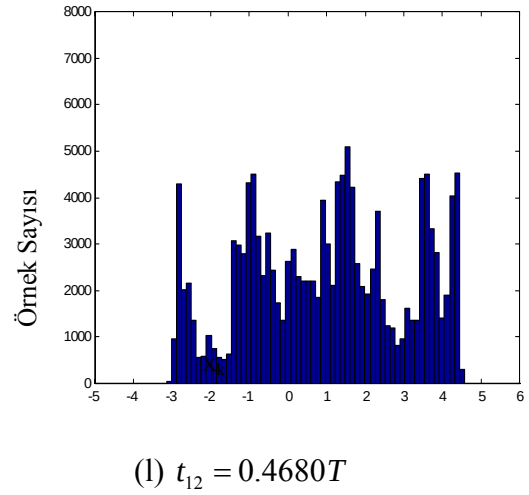
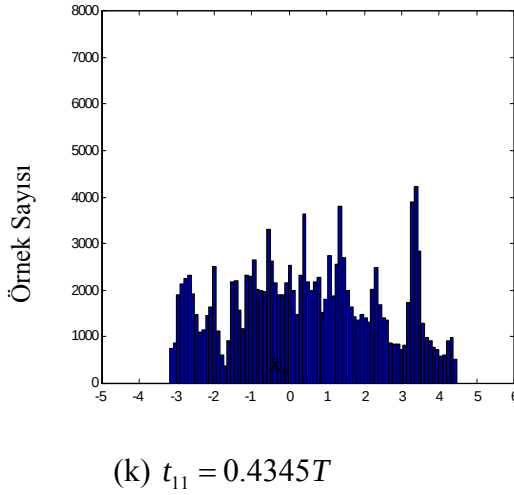
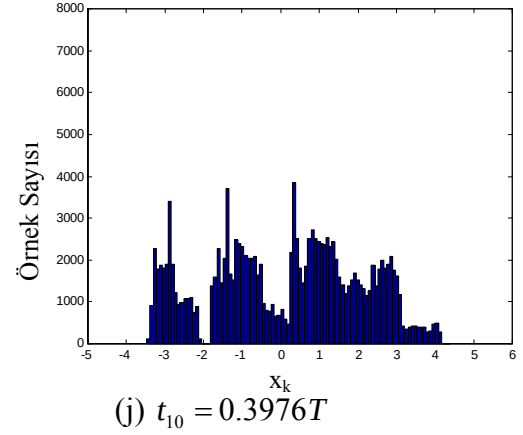
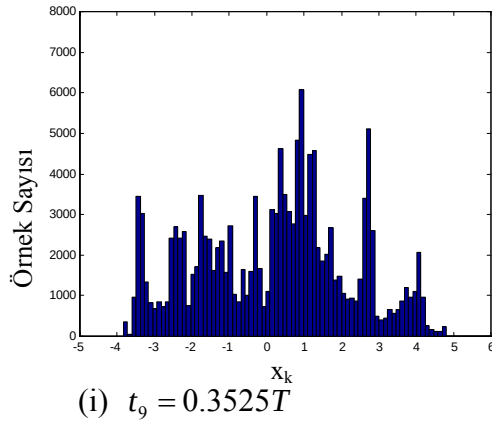
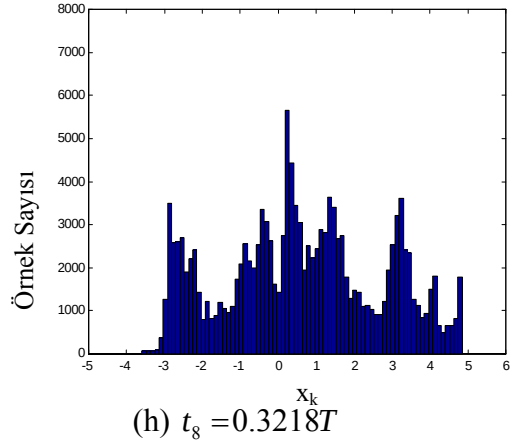
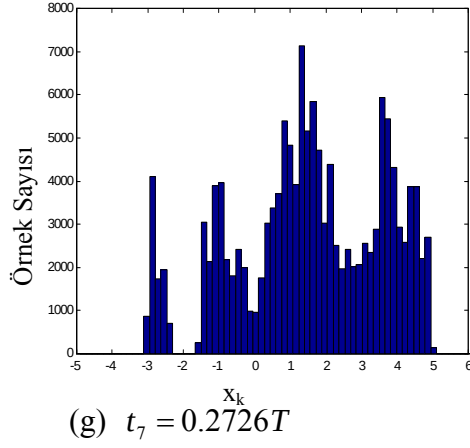
sistemin -1.7 ile -1 ve -0.3 ile 0.3 eşik aralığında poker testini geçtiği gözlenmiştir. Burada entropy sonuçları incelendiğinde $\ln(2)$ ' ye en yakın olan değer, eşik değeri -1.5 için 0.6922 olarak bulunmuştur. Ayrıca -1.9 ile 0.3 eşik aralığında entropy sonuçlarının 0.6900 üzeri olduğu gözlenmiştir.



Şekil 3.9 : (a)Sekiz sarmallı kaotik sistem kullanılarak Poincare kesitinde $c=0$ için örneklenerek elde edilen X değerlerinin histogram diyagramı (b) Poker testi sonucu (c) Entropi sonucu



Şekil 3.10: Sekiz sarmallı kaotik sistem kullanılarak a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$ için x durum değişkeninin Poincare kesitindeki dağılımını gösteren histogram diyagramları

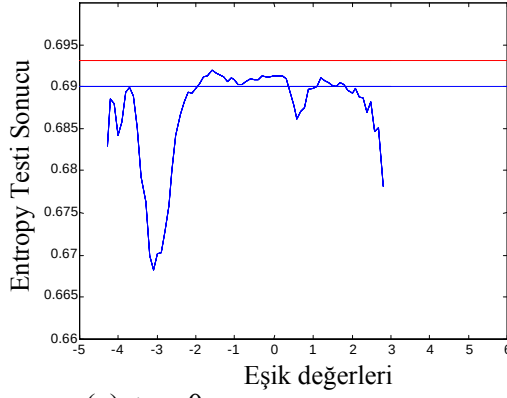


Şekil 3.11: Sekiz sarmallı kaotik sistem kullanılarak g) $c=0.2726$, h) $c=0.3218$, i) $c=0.3525$, j) $c=0.3976$, k) $c=0.4345$, l) $c=0.4680$ için x durum değişkeninin Poincaré kesitindeki dağılımını gösteren histogram diyagramları

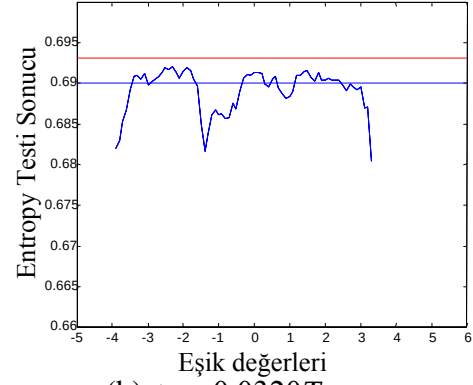
Sekiz sarmallı sistem için c parametresi, $0 \leq c < 0.5$ aralığında Poincaré dönüşümünden faydalanarak $t_1 = 0T$, $t_2 = 0.0320T$, ..., $t_{10} = 0.4680T$ anları için örnekleme yapılmıştır. Her bir durum için elde edilen histogram diyagramları Şekil

3.10 ve 3.11’de gösterilmektedir. Bu diyagramlar incelendiğinde, zamanla birlikte dağılımlarda bir süreklilik gözlenmiştir.

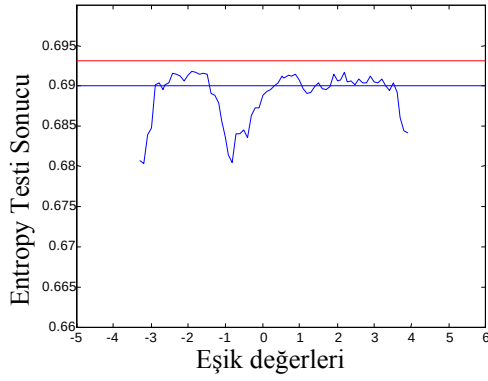
Şekil 3.12 ve 3.13’de ise eşik aralıklarının entropy testiyle olan sonucu gösterilmiştir. Grafikler incelendiğinde, $c=0.35255$ için entropinin 0.69 değerinin üzerinde olduğu en geniş aralık elde edilmiştir. Bu grafikler incelendiğinde sarmal sayısının artmasına bağlı olarak eşik aralığının da artmış olduğu gözlenmiştir. Kaynak olarak kullanılan işaret fonksiyonunun daha yüksek katlı şekilde uygulanmasıyla diğer bir deyişle kaotik çekicinin sarmal sayısının artmasıyla oluşan durumun elde edilen rasgele sayı dizisinin niteliğini ne derecede etkilediği incelenmiş ve sonuç olarak istenen derecede iyi bir artış gözlenememiştir.



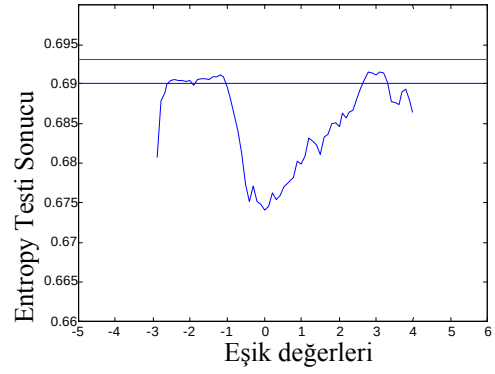
(a) $t_1 = 0$



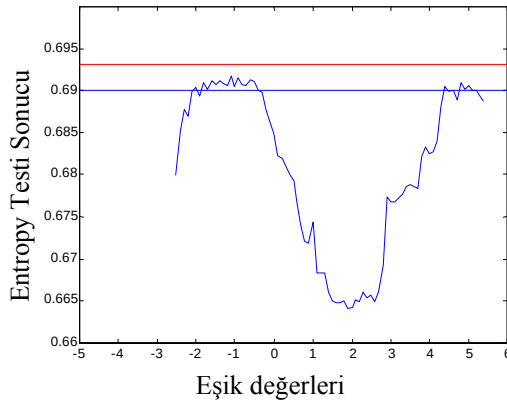
(b) $t_2 = 0.0320T$



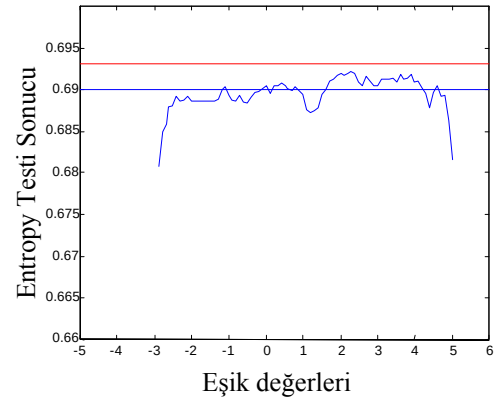
(c) $t_3 = 0.0655T$



(d) $t_4 = 0.1024T$

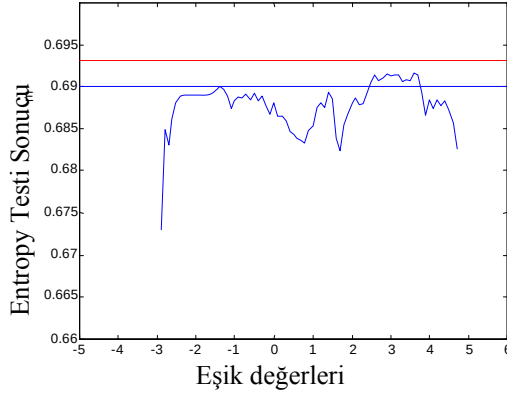


(e) $t_5 = 0.1475T$

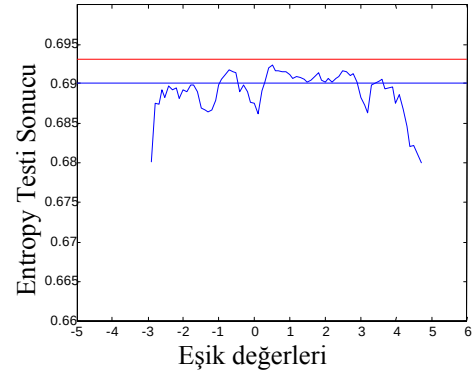


(f) $t_6 = 0.2274T$

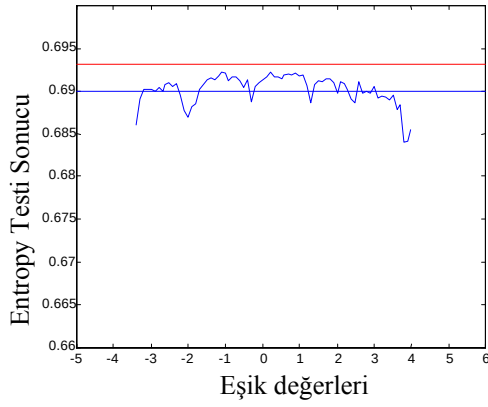
Şekil 3.12: Sekiz sarmallı kaotik sistem kullanılarak a) $c=0$, b) $c=0.032$, c) $c=0.0655$, d) $c=0.1024$, e) $c=0.1475$, f) $c=0.2274$, için entropy testinin sonucunun eşik aralığı ile değişimi (— $=\ln 2$, $0.69 =$ —)



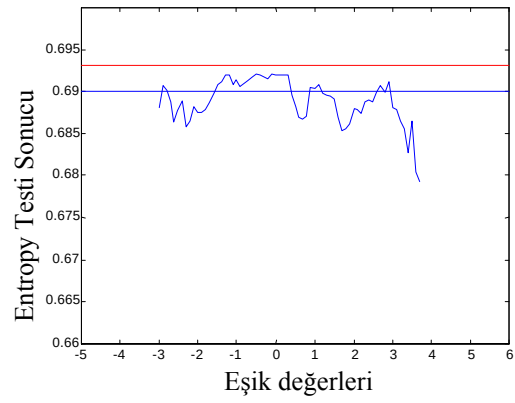
(g) $t_7 = 0.2726T$



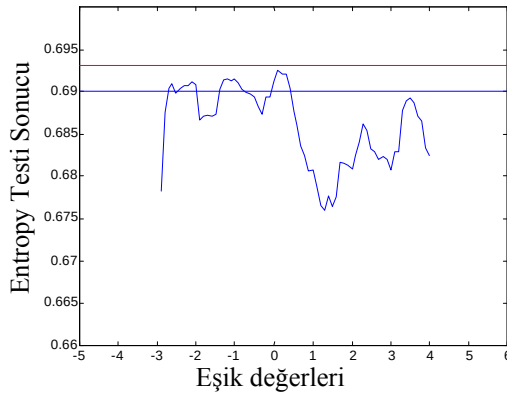
(h) $t_8 = 0.3218T$



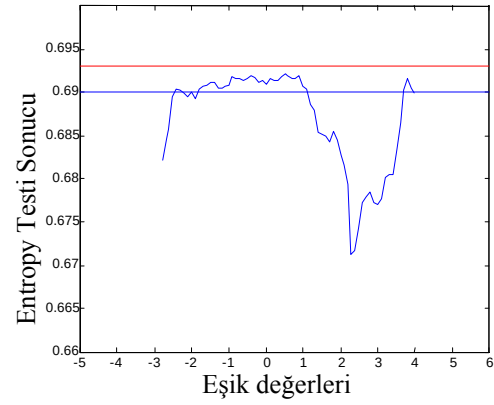
(i) $t_9 = 0.3525T$



(j) $t_{10} = 0.3976T$



(k) $t_{11} = 0.4345T$

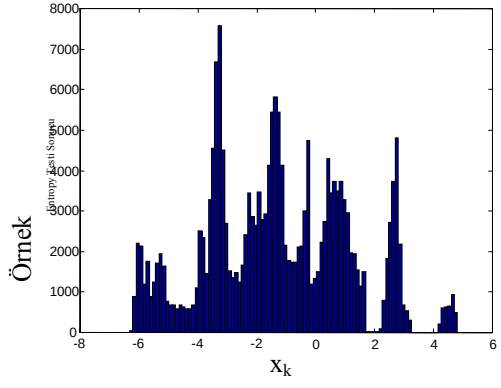


(l) $t_{12} = 0.4680T$

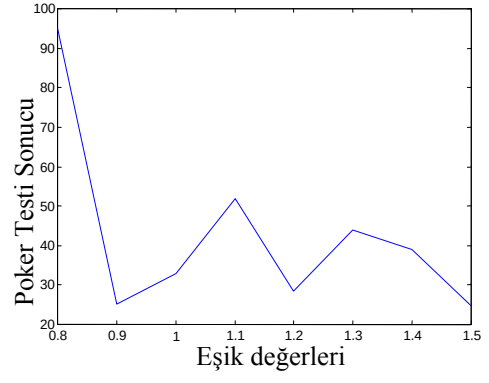
Şekil 3.13: Sekiz sarmallı kaotik sistem kullanılarak g) $c=0.2726$, h) $c=0.3218$, i) $c=0.3525$, j) $c=0.3976$, k) $c=0.4345$, l) $c=0.4680$ için entropy testinin sonucunun eşik aralığı ile değişimi (— = $\ln 2$, 0.69 = —)

3.3 On iki Sarmallı Sistemden Rasgele Sayı Üretilmesi

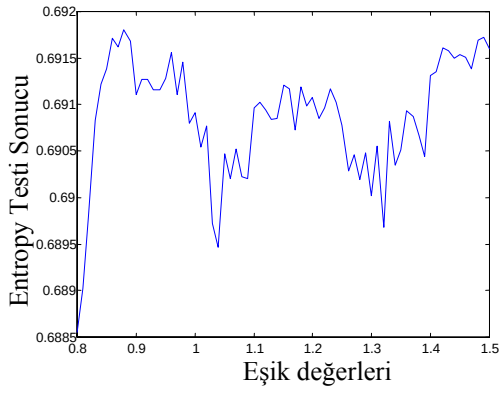
On iki sarmallı kaotik sistem için matematiksel ifadesi 3.1 (a), (b) ve (e)'de verilmiş olan denklemler eşliğinde nümerik analizler yapılmıştır. Bu sistem için de Poincare kesitinde $c=0$ alınmış ve x durum değişkeninin 190 bin değeri kaydedilmiştir. Diğer sistemlerde olduğu gibi burada da sadece x değerleri alınmıştır. Şekil 3.14(a)'da Poincare kesitinde $c=0$ için x durum değişkeninin x_k değerlerinden oluşan dağılımından elde edilen histogram diyagramı gösterilmektedir. Buradaki histogram diyagramı dikkate alındığında ilk iki sisteme göre genliğe bağlı olarak eşik aralığının doğal olarak arttığı gözlenmiştir. Bu sistem için -6 ile 4.5 aralığındaki tüm eşik değerleri için önce ikili-kodlu sayı dizisi üretilmiştir. Sonra oluşan sayı dizisine Von Neumann Metodu düzgün dağılımlı olması açısından uygulanmıştır. Bu sistemden elde edilen dizinin rasgeleliğini incelemek kaydıyla ilk önce poker testine tabi tutulmuş, sonra bu ikili-kodlu sayıların entropisi hesaplanmıştır. Şekil 3.14(b)-(c)' de bu sistem için sonuca varılan eşik aralıklarının (0.8 ile 1.5 aralığında) poker testiyle ve entropisiyle olan sonuçları gösterilmiştir. Poker testi sonucunda elde edilen minimum değer 24.78 olup, bu değer için kullanılan eşik 1.5 dur. Bu sistemin 0.8 ile 1.5 eşik aralığında poker testini geçtiği gözlenmiştir. Burada entropy sonuçları incelendiğinde $\ln(2)$ ' ye en yakın olan değer, eşik değerleri -0.04 ve -1.56 için 0.6918 olarak bulunmuştur. Ayrıca -1.9 ile 0.3 eşik aralığında entropy sonuçlarının 0.6880 üzeri olduğu gözlenmiştir.



(a)



(b)



(c)

Şekil 3.14: (a)On iki sarmallı kaotik sistem kullanılarak Poincare kesitinde $c=0$ alınarak elde edilen X değerlerinin histogramları (b) Poker testi sonucu (c) entropi sonucu

4. SONUÇLAR

Bu tez kaotik sistemlerden rastgele sayı üretilmesi tekniklerinin geliştirilmesi amacıyla yapılmıştır. Bu çalışmada otonom olmayan kaotik sistemden rastgele sayı üretilmesi esnasında, sisteme uygulanan kaynağın periyodunun hangi aralığında elde edilen rastgele sayı dizisinin daha nitelikli olduğu incelenmiştir.

Bilindiği gibi gelişen bilgisayar teknoloji sayesinde kaosu nümerik olarak incelenmesi daha da kolaylaşmış, böylece birçok alanda hizmet verecek olan kaotik sistemlerin incelenmesi de sağlanmıştır.

Bu çalışmada otonom olmayan kaotik sistemlerden üretilen rastgele sayı dizilerinin niteliği ve rastgeleliği incelenmiştir. Öncelikle otonom olmayan kaotik sistemlerden rastgele sayı üretmek amacıyla x durum değişkeninden $x_k = x(t_k)$, $t_k = \{t_k \mid \omega t \bmod 2\pi = 0\}$ şeklinde oluşturulan $\{x_k\}$ reel sayıları dikkate alınmıştır. Sonra bu reel sayı kümesinin histogram diyagramına bakılarak olası eşik aralıkları için ikili-kodlu rastgele sayı üretilmiştir, daha sonra rastgeleliği doğrulamak amacıyla ilk yol olarak olası eşik değerleri için üretilen ikili-kodlu sayılar poker testine tabi tutulmuş, ikinci yol olarak da bu sayı dizilerinin entropisi hesaplanmıştır.

Bu tezde c parametresi rastgelelik için yeni bir parametre olmaktadır. Bu parametreyle rastgele sayı üretiminin karakteristiğini arttırabiliriz. Unutulmaması gereken bir noktada c parametresi değişirken sistemin hep aynı olmasıdır.

$t = \{t_k \mid \omega t_k \bmod 2\pi = cT\}$ şeklinde tanımlanan Poincare kesitinde öncelikle c parametresi $(0,1)$ aralığında alınmıştır. Bu şartlar altında, Poincare kesitinde $0 < c < 0.5$ ile $0.5 < c < 1$ aralığındaki dağılımlar ve poker testi sonuçları $x=0$ eksenine göre simetrik çıkmaktadır. Bu durum, Bölüm 2’de açıklanan ve Şekil-2.2’de verilen sistemin Poincare kesitindeki çekicisinin simetri özelliğinin bir sonucu olarak elde edilmiştir. Bu bağlamda, birinci sistem için Bölüm.2’ de bahsi geçen c parametresi, $0 \leq c < 0.5$ arasında değiştirilerek en iyi eşik aralığı incelenmiştir. Dört sarmallı kaotik sistemin x durum değişkenlerinin Poincare kesitindeki izdüşümleri $c \in (0,1)$ durumu için incelendiğinde, Poincare kesiti $c=0.1475$ iken diğer durumlara göre

rastgele sayı dizisinin daha nitelikli sonuç verdiği gözlenmiştir. Diğer bir deyişle, $c=0.1475$ değeri için en iyi değerin diğer bir deyişle entropisi ideal rastgele sayı üreticinin entropisi olan $\ln(2)$ 'ye yakın olan en geniş aralık olarak bulunmuştur. Bu örnek için, NIST (Amerikan Ulusal Standart ve Teknoloji Enstitüsü) ve FIPS (Federal Bilgi İşleme Standartları) 140-1'de tavsiye edilen testler uygulanmış ve bu eşik alığında tüm testlerden geçtiği gözlenmiştir. Farklı başlangıç koşulu için de uygulandığında yine aynı histogram diyagramlarına ve entropy grafiklerine ulaşıldığı gözlenmiştir.

Sekiz sarmallı kaotik sistemin x durum değişkenlerinin Poincaré kesitindeki izdüşümleri $0 \leq c < 0.5$ aralığında incelendiğinde $c=0.3525$ değeri için entropy testi sonuçları c parametresinin aldığı diğer değerlerdeki durumlarına göre daha iyi sonuç vermiştir. Fakat göz önünde bulundurulması gereken önemli bir noktada sarmal sayısının artmasıyla eşik aralığının artmış olması beklenen bir durumdur. Burada sistemler karşılaştırıldığında, sonuç olarak dört sarmallı sistemde istenen gelişmenin daha iyi gözlenmiş olduğudur. Ayrıca kaynak olarak kullanılan işaret fonksiyonunun daha yüksek katlı şekilde uygulanmasıyla diğer bir deyişle kaotik çekicinin sarmal sayısının artmasıyla oluşan durumun, elde edilen rastgele sayı dizisinin niteliğini ne derecede etkilediği incelenmiş ve sonuç olarak istenen derecede iyi bir artış gözlenememiştir. İleriki çalışmalarda iki eşik değeri kullanılarak bu kaotik sistemlerin nümerik analizi yapılarak rastgele sayı üretilmesinin incelenmesi mümkündür.

EK-1 :

Poker testi için kullanılan Matlab kodlarını içermektedir.

```
clear;load nauto_data.txt -ascii;esik_adimi=0;
for esik=-0.2:0.01:0.3
    esik_adimi=esik_adimi+1;
    ii=1;jj=1;x=[];
    while (ii<length(veri))
        if (veri(ii)==0) & (veri(ii+1)==1)
            x(jj)=0;jj=jj+1;
        elseif (veri(ii)==1) & (veri(ii+1)==0)
            x(jj)=1;jj=jj+1;
        end;
        ii=ii+2;
    end;
    x=x';
    n=length(x);
    if (n>20000)
        x=x(1:20005)';n=length(x);
        n1=0;
        for i=1:n
            n1=n1+x(i);
        end;
        np=[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0];
        i=1;k_4=floor(length(x)/4);
        while (i<n-3)
            b=0;
            for j=0:3
                b=b+2^j*x(i+3-j);
            end;
            np(b+1)=np(b+1)+1;
            i=i+4;
        end;
        X3(esik_adimi)=2^4*np*np/k_4-k_4
        else
            X3(esik_adimi)=0;
        end;
    end;
```

EK-2 :

Entropy testi için kullanılan Matlab kodlarını içermektedir.

```
clear;load nauto_data10.txt -ascii;esik_adimi=0;
for esik=-0.8:0.1:1.7
    esik_adimi=esik_adimi+1;
    veri=0.5*sign(nauto_data10-esik)+0.5;
    ii=1;jj=1;x=[];
    while (ii<length(veri))
        if (veri(ii)==0) & (veri(ii+1)==1)
            x(jj)=0;jj=jj+1;
        elseif (veri(ii)==1) & (veri(ii+1)==0)
            x(jj)=1;jj=jj+1;
        end;
        ii=ii+2;
    end;
    x=x';
    n=length(x);
    n=length(x);
    np=zeros(64,1);
    i=1;
    while (i<=n-5)
        b=0;
        for j=0:5
            b=b+2^j*x(i+j);
        end;
        np(b+1)=np(b+1)+1;
        i=i+6;
    end;
    sum=0;
    for ii=1:64
        sum=sum+np(ii);
    end;
    entropy_=0;pp=0;
    for ii=1:64
        pp=np(ii)/sum;
        entropy_=entropy_-pp*log(pp);
    end;
    entrop(esik_adimi)=entropy_/6
end;
```


KAYNAKLAR

- [1] **Peitgen, H. O., Jürgens, H. and Saupe, D.**, 1992. Chaos and Fractals: New Frontiers of Science, Springer-Verlag, New York.
- [2] **Johansson, A. J. and Floberg, H.**, 1999. Random Number Generation by Chaotic Double Scroll Oscillator on Chip, IEEE International Symposium on Circuits and Systems, **407**
- [3] **Stojanovski T. and Kocarev L.**, 2001. Chaos-Based Random Number Generators, IEEE Transactions on Circuits and Systems-I, **48 (3)**
- [4] **Cuomo, K. M., Oppenheim, A. V.**, 1993. Circuit Implementation of Synchronized Chaos with Applications to Communications, Physical Review Letters,
- [5] **Baptista, M. S.**, 1998. Cryptography with Chaos, Physics Letters A,.
- [6] **Guckenheimer, J. and Holmes, P.**, 1990. Nonlinear Oscillations Dynamical Systems and Bifurcations of Vector Fields, Springer Verlag, New York.
- [7] **Serkan Semiz**, 2005. Otonom Olmayan Bir Kaotik Sistem ve Uygulaması, Yüksek Lisans Tezi , İ.T.Ü. Fen Bilimleri Enstitüsü, İstanbul
- [8] **Abel, A. and Schwarz, W.**, 2002. Chaos Communications–Principles, Schemes, and System Analysis, Proceedings of the IEEE, **90 (5)**
- [9] **Shamir, A.**, 1983. On the Generation of Cryptographically Strong Pseudorandom Segmences – ACM Transactions on Computer Systems, **1 (1)**
- [10] **A. M. Fraser**, 1989. Information and Entropy in Strange Attractors, IEEE Trans. Information Theory, **35(2)**
- [11] **FIPS 140-1**, 1994. Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, United States of America.

ÖZGEÇMİŞ

Pınar Güven, 14.10.1979'da İstanbul'da doğdu. 1997 yılında Cağaloğlu Anadolu Lisesi'nden mezun oldu. Aynı yıl Yıldız Teknik Üniversitesi Elektrik-Elektronik Fakültesi, Elektrik Mühendisliği Bölümünde Lisans öğrenimine başlamıştır. 2002 yılında Elektrik mühendisi ünvanını aldı ve Eylül 2002'de İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Ana Bilim Dalı Elektronik Mühendisliği Yüksek lisans öğrenimine başlamıştır. Mayıs 2004'den itibaren Telsim' de Kalite Mühendisi olarak çalışmış, Şubat 2006'dan bu yana Avrupa Bölge BSS İşletme Bölümü' nde BSS İşletme Mühendisi olarak çalışmaya devam etmektedir.