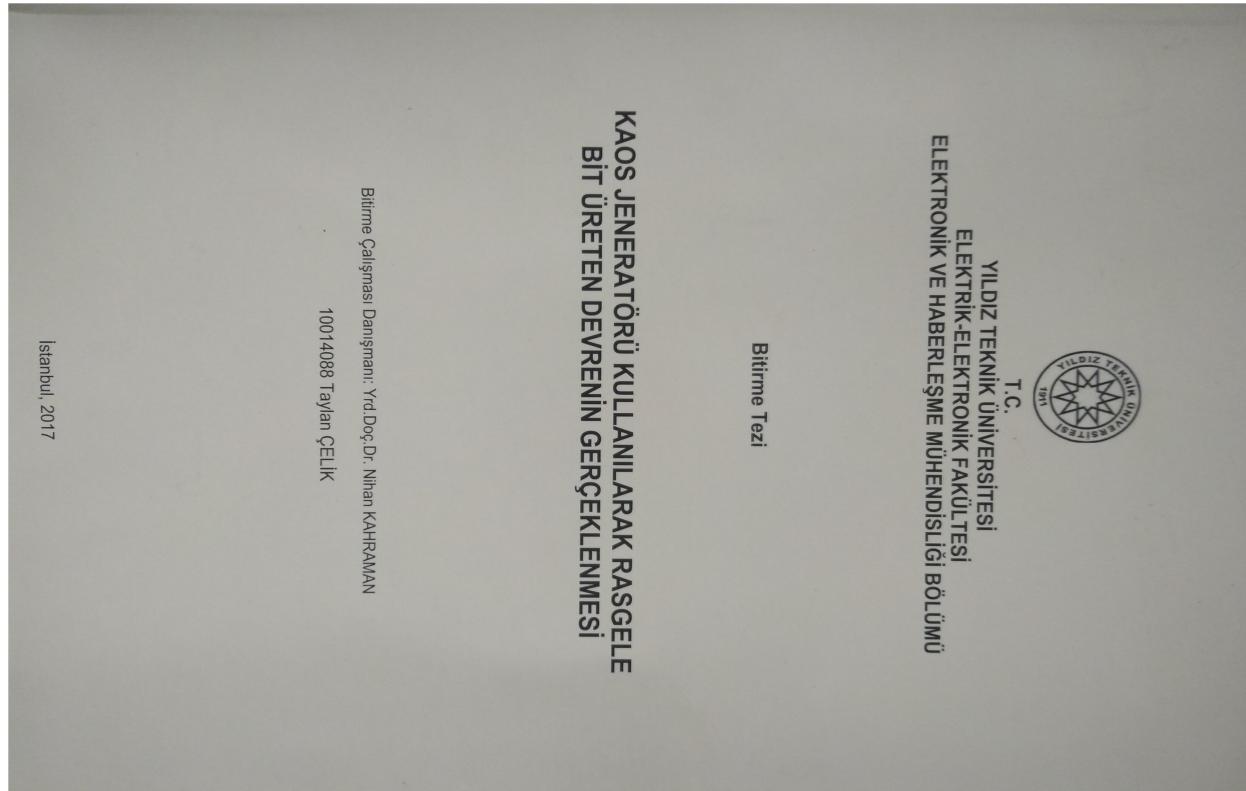


Final Year Project(2017)

Implementation Of Chaos Circuit

In this PDF file you can see some pictures of my final year project.



KİMDEN KİMDEN

	Sayfa
SİNTEZLİ LISTESİ	iv
KISA TİMA LISTESİ	v
ŞEKLİ LISTESİ	vi
ÇİZEL GE LISTESİ	vii
ÖNSÖZ	viii
ÖZET	ix
ABSTRACT	x
1. GIRİŞ	11
1.1 Literatür Özeti	12
1.2 Temin Amacı	12
1.3 Hipotez	12
2. CHUA DEVRESİ VE OSILATÖRÜ	13
2.1 CHUA DEVRESİ	13
2.2 PARAMETRE DEĞERLERİİNİN HESAPLANMASI	16
2.3 DOUBLE SCROLL ATTRACTOR	17
2.4 CHUA OSILATÖRÜ	19
3. SC-CNN MODELİYLE KAOS JENERATÖRÜ DEVRESİ	24
3.1 SC-CNN MODELLİ CHUA DEVRESİNİN SADELEŞTİRİLMESİ	26
3.2 PARAMETRE SEÇİMİ VE JENERATÖR DEVRESİNİN KOMPONENT DEĞERLERİNİN SEÇİLEN PARAMETREYE GÖRE HESAPLANMASI	30
3.3 JENERATOR DEVRESİNİN SIMÜLASYONU	33
3.4 DEVRENİN GERÇEKLENİŞ HALİ	36
3.5 JENERATOR ÇIKIŞINDAKI SINYALI ÖRNEKLENİR HALE GETİRME	38
4. ÖRNEKLEME DEVRESİ	40
4.1 D FLİP-FLOPLAR VE BAĞLANTILARI	41
4.2 CLOCK(SAAT) DEVRESİ	43
4.3 ÖRNEKLEME DEVRESİNİ TOPLU BAKIŞ	44
4.5 SIMÜLASYON SONUCLARI	46
4.6 SIMÜLASYON SONUCLARIN TESTİ	47
4.6.1 TESTLERİN KİTRİRLERİ VE SONUCLARI	49
KAYNAKLAR	54
EKLER	55

Ek 1	Devrenin gerçekleşmesinde kullanılan entegre devrelerin pin uçları	56
Ek 2	Devrenin ard arda ürettiği ve testlere tabi tutulan 84 Byte'lık verinin Hex(16'lık taban) şeklindeki çıktısı	59
ÖZGEÇMİŞ	60

SEKİL LİSTESİ

Sekil 2.1 Chua'nnın devresi.....	13
Sekil 2.2 Chua diyotunun v-i karakteristiği	13
Sekil 2.3 Chua devresi x-y grafiğinden elde edilen double scroll şéki(j(osiloskopta yatay eksen 500mV/div ve dikey eksen 200mV/div).....	13
Sekil 2.4 Chua devresi x-z grafiğinden elde edilen double scroll şéki(j(osiloskopta yatay eksen 1V/div ve dikey eksen 2 V/div)	17
Sekil 2.5 Chua devresi y-z grafiğinden elde edilen double scroll şéki(j(osiloskopta yatay eksen 1V/div ve dikey eksen 200mV/div)	17
Sekil 2.6 Chua devresinde gözlenen DC denge noktaları	18
Sekil 2.7 Chua Osillatörü	20
Sekil 2.8a Chua osillatöründe farklı parametrelerin farklı sarmal yapıları	22
Sekil 2.8b Chua osillatöründe farklı parametrelerin farklı sarmal yapıları	22
Sekil 3.1 Genelleştirilmiş hiperbolik devrenin yapısı(işte) ve komşu hücrelerle kaskad bağlantısı(alta)[1].....	23
Sekil 3.2 Sadelleştirilmiş SC-CNN hücre yapısı[1]	25
Sekil 3.3 SC-CNN modeliyle basitleştirilmiş Chua devresi[1]	27
Sekil 3.4 SC-CNN modeli Jeneratör devresi.....	29
Sekil 3.5 Gerçekleştirilen kaos devresi nin x-t grafiği	33
Sekil 3.6 Gerçekleştirilen kaos devresi nin y-t grafiği	34
Sekil 3.7 Gerçekleştirilen kaos devresi nin z-t grafiği	34
Sekil 3.8 Gerçekleştirilen kaos devresinde y-z grafiğinde gözlenen double scroll	35
Sekil 3.9 Gerçekleştirilen kaos devresi nin x-y grafiğinde gözlenen double scroll	35
Sekil 3.10b Gerçekleştirilen Kaos devresinin y-z çıkışının osiloskopaktaki görüntüsü	37
Sekil 3.10c Yapılan jeneratör devresi	37
Sekil 3.11a Jeneratör ve Örnekleme devresi arasındaki komperatör devresi	38
Sekil 3.11b z sinyalinin Sekil 3.11a'nın çıkışındaki hali	39
Sekil 4.1 D flip-flop uçları	41
Sekil 4.2 Devredeki D-flip-flopların bağlantı	42
Sekil 4.3 Clock Devresi	43
Sekil 4.4 Örnekleme devresi.....	45
Sekil 4.6 Jeneratör ve örnekleme devresinin bir aradaki görüntüyü ve simülasyon sonucundan bir örnek	46
Sekil 4.7 Testlerde kullanılan Random Numbers Analyser Programının Arayüzü	48
Sekil 4.8 Runs Test sonucu	49
Sekil 4.9 Frequency Monobit test sonucu	50
Sekil 4.10 Frequency Test within a Block 8 bitlik bloklar şeklinde yapılan frekans testi)	51
Sekil 4.11 Kümülatif topımlar testi sonucu	51
Sekil 4.12 Ayrık Fourier dönüsümü testi	52
Sekil 4.13 Yapılan örnekleme devresi ile jeneratör devresi bir arada gösterilmiştir	53
Sekil 4.14 Yapılan örnekleme devresi(sağda) ve jeneratör devresini(solda) baskı devreleri	53
Sekil 5.1 74LS273 Register	56
Sekil 5.2 74LS164 Register	56
Sekil 5.3 74LS193 Sayıcı	56
Sekil 5.4 74LS74 D Flip-flop Entegresi	57
Sekil 5.5 74LS86 XOR Entegresi.....	57
Sekil 5.6 74LS14 Schmidt Inverter	57
Sekil 5.7 TL082 Op-amp Entegresi	57
Sekil 5.8 LM7805 Voltaj Regülatörü	58

ÇİZELGE LİSTESİ

Çizelge 3.1 Devrenin gerçekleştirülmesinde kullanılan elementler	36
Çizelge Ek 2 Devreden ard arda üretilen 84 adet 8 bitlik diziler	59

ÖNEMİ

Köns devesi kullanarak rasgele(random) bir tressin konusunu hazırlamamda bana karşı olsa anlayıp ve her türlü yardımlarından dolayı Hocam Yıldız Denizhan Kahraman'a ve Ayşe Arş, Gök, Murat Taşkiran ile Arş Gör Zehra Güllü Çam'a ve her zaman yanında olan aileme teşekkürlerimi sunarım.

Haziran, 2017
Taylan Çelik

1. Giriş

Günümüzde kaos devreleri çok farklı devre topolojileri kullanılarak sentezlenebilmektedir. Farklı devre topolojileri yanında ,kaosun elektronik elementler vasıtasyyla sergilennmesinde binlere farklı parametre veya yine bu parametrelerle göre dizayn edilmiş birkaç jeneratörün birbirlerine bağlanması sonucu çok değişik yöntemler kullanılabilmektedir. Bu çalışmada Chua tarafından tasarlanan ilk model referans almış ve Chua devresine eşdeğer bir model üzerinden(SC-CNN) devre sentezi gerçekleştirmiştir.

Tezin 2. Bölüm'de Chua devresi ve genel denklemleri ve bu denklemlerden parametrelerin eldesi üzerinde durulmuş ve ayrıca ek olarak da Chua osilatöründen bahsedilmiştir. 3.Bölüm'de Chua devresinin SC-CNN eşdeğer modeli açıklanmış ve burdaki modelden harekete jeneratör devresi gerçekleştirmiştir. 4.Bölüm ise jenerator devresinde üretilen sinyalin mikrodenetleyici ya da herhangi bir lojik devre tarafından kullanılabilir formata dönüştürülmesini sağlayan örnekleme devresine ayrılmıştır. Yine 4.Bölümün sonunda gerçekleştirilen devrenin simülasyon sonuçları NIST Test Suite programları kullanılarak test edilmiştir. Sonuçlar değerlendirilmiş, hedefler ve sonuçlar karşılaştırılmış ve daha iyi sonuçların alınabilmesi için nelere dikkat edilmesi gerektiği üzerinde durulmuştur.

Tezin genelinde simülasyonlar Multisim 14 programıyla yapılmış ve devre gerçekleştirmesinde kullanılan bütün elementların bağlantı biçimleri açıklanmıştır. Ayrıca Ek 1'de kullanılan entegrelerin pin uşarına yer verilmiş ve Ek 2 'de ise devrenin aralsız çalıştırılması sonucu ard arda üretilen ve testlerde simanan bitler çizelge şeklinde verilmiştir.

1.1 Literatür Özeti

Chua devresi ve Chua osilatörü'ne ilişkin diferansiyel denklemlerin parametrelerinin eldesini ve bu tür devrelerin tasarım incelemelerine aylanın ve tezin 2.Bölümü'ndeki denklemlerin yazılımasında kullanılan [1], ve benzer şekilde daha farklı yöntemlerle bu tür devrelerin sentez şeklini anlatan [2], [3], [5]; Denklem ve parametre hesaplarla pratik şekilde değerlendir[10], Chua devrelerinin spesifik kullanım alanlarının anlatıldığı(örneğin sinyal kriptolama) ve bunlara ilişkin simülasyonların yapıldığı makaleler [6], [7], [8] ; Örneklemeye ilişkin ve yine Chua devresi kullanmadan rasgele bit üretiminin transistörlerden gürültü üreteme yoluyla yapıldığı [4], ayrıca Rasgelelik Testleri(Randomness Tests) için yararlanılan[12],[13], tezin hazırlanmasında yararlanılan kaynaklar oldu.

1.2 Tezin Amacı

Bu bitirme çalışmasında kaos jeneratorü kullanarak rasgele bit üretebilen bir devre yapımı amaçlanmıştır. Ancak parametre hesabı , Matlab vb... programları kullanarak Chua devresi denklemlerinin parametre çözümü üzerinde durulmamıştır.Tez projesindeki hedef ,sonuç odaklı olup kaos jeneratorü kullanılarak random bitler üretebilen bir devrenin gerçekleşmesi ve bu devreden kullanılabilir bit dizinlerinin örnekleme devresi yoluyla (mikrodenetleyici kullanmadan) elde edilmesi olmuştur. Tezin amacı bu projede yapılan devreyle sinyal kriptolama vb... gibi özel bir amaç taşımadığı için jeneratorün gerçeklemesinde zaten bilinen parametrelerden biri kullanılmış ve bir kaos devresi modelinden hareket edilmiş ve bu devrenin nasıl gerçekleştiği üzerinde durulmuştur.

1.3 Hipotez

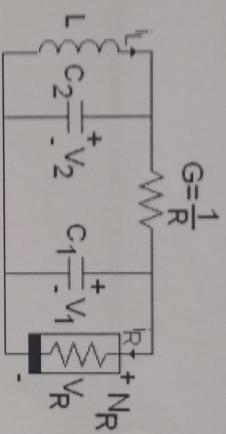
Kaos devreleri gerek karakteristik özellikleri bilinen elementlardan deterministik bir kaosun nasıl üretilibildiğini göstermesi yanı sıra özellikle Kriptografi'de çok önemli bir yere sahiptir.Son kullanıcıya kadar bilgilerin güvenli bir şekilde iletilmesi için sinyal şifrelemede ve bazı yapay zeka alanındaki uygulamalarına kadar öncü uygulama alanlarına sahiptir[8]. Tezde ise gerçekleştirilen devreyle daha basit amaçlarda kullanabilecek bir devrenin yapımı üzerinde çalışılmıştır.

2. CHUA DEVRESİ VE OSİLATÖRÜ

2.1 CHUA DEVRESİ

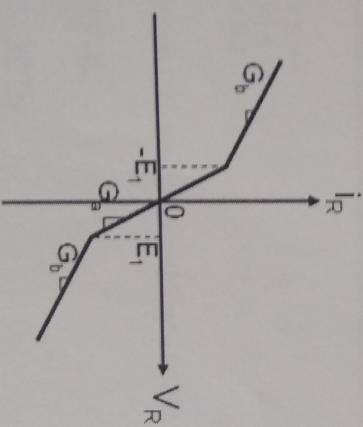
Chua devresi kaosu sergileyen en basit devredir.Şekil 2.1'de gösterildiği gibi üç tane enerji depolayan devre elemanlarından(2 kondansatör ve 1 bobin),bir tane direnç ve bir de Chua diyotu denebilecek olmayan devre elemanından oluşur. Bir elektronik devrenin kaos özelliği gösterememesi için

- en az 3 tane enerji depolayabilen elemana
- en az 1 tane lineer olmayan devre elemanna
- ve en az 1 tane de aktif dirence sahip olmalıdır[1].



Şekil 2.1 Chua'nın devresi

Chua diyotu tek başına son iki şartı sağlamak için yeterlidir.Şekil 2.2'de Chua diyotunun v-i (akım-gerilim) karakteristiği gösterilmiştir.



Şekil 2.2 Chua diyotunun v-i karakteristiği

değişken atamaları yapılfırsa son olarak (2.7)'deki Chua denklemleri elde edilir.

$$\begin{aligned}\dot{x} &= \alpha[y - h(x)] \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y\end{aligned}\tag{2.7}$$

Bu son durumda denklemler Şekil 2.1'deki devreden yola çıkılarak elde edilen parametrik Chua denklemleridir.Denklemlerin bu şekilde yazılışının nedeni çözümlerinin analitik olarak daha basit şekilde ifade edilmesini sağlamaktır.Ve aynı zamanda hangi devreyi kullanırsak kullanalım (SC-CNN,Orijinal Chua devresi veya daha farklı topolojilerden türetilen kaos devreleri vs...) jeneratorun dinamik karakteristığının burda söz edilen α, β, m_0, m_1 parametrelerine belirleneceğidir.Bu parametreler Chua devresinin diferansiyel denklemlerinin çözümüdürler.Matlab programında bu parametreler taratılarak nümerik çözüm bulunamaz sadece R,L,C vs... komponentlerine göre çözüm bulunabilir.Fakat bu parametreler pratik biçimde gözlenebilecek sarmal yapılarının sınırlanılamamasını sağlar.Sonuçta sentezlenenek olan kaos devresindeki α, β, m_0, m_1 gibi parametrelerin, sentezlenen devredeki hangi elemanların çarpmına,bölümüne vs... denk düşüğünün bulunmasını sağlar.Bu ise söz konusu kaotik davranış için gerekli olan direnç,kapasite vs... devre elemanlarının değerlerinin hangi değerlererde seçilmesi gerektiğini bulabilmemizi sağlar.

2.2 PARAMETRE DEĞERLERİ'NİN HESAPLANMASI

1985 yılında Matsumoto tarafından hesaplanan parametre değerleri şu şekildedir:

$$\begin{aligned}\alpha &= 9 \\ \beta &= 14.2886 \\ m_0 &= -1/7 \\ m_1 &= 2/7\end{aligned}\tag{2.8}$$

Bu değerler bulunurken (2.9)'da verilen değerler kullanılmıştır.(2.9)'daki değerlere göre

$$\begin{aligned}C_1 &= 5.5mF \\ C_2 &= 49.5mF \\ L &= 7.07mH \\ R &= 1.428k\Omega \text{ (or } G = 0.7mS) \\ G_a &= -0.8mS \\ G_b &= -0.5mS \\ E &= 1V\end{aligned}\tag{2.9}$$

(2.8)'deki α, β, m_0 ve m_1 parametreleri elde edilmişdir[1]. Bitirme çalışmasında da bu değerler kullanılmıştır. α, β, m_0 ve m_1 değerlerinin devrede neye denk düşüğü (2.3)'te gösterilmiştir.Ayrıca bitirme çalışmasında yapılan jenerator devresine göre bu parametre

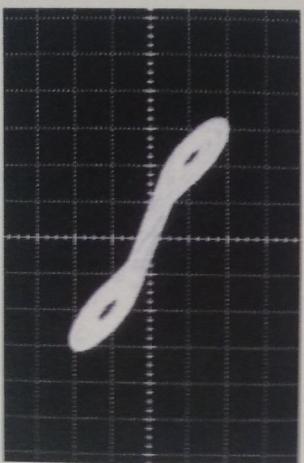
değerlerinin neye denk düşüğü, Bölüm 3.2'de açıklanmıştır. Devre elementleri de bilgisini jeneratörlerin kaotik davranışını bu parametreler belirler.

2.3 DOUBLE SCROLL ATTRACTOR

(2.8)'deki parametre değerlerine göre osiloskoptan elde edilen grafikler Şekil 2.3,Şekil 2.4 ve Şekil 2.5'de gösterilmiştir.Burada x,y,z noktaları Şekil 2.1'deki devrenin sınırları V_x , V_y ve V_z noktalarından alan voltaj değerleridir. Osiloskopta bu voltaj değerlerinin birbirlerine göre değişimleri çizdirilmiştir şekillerde,

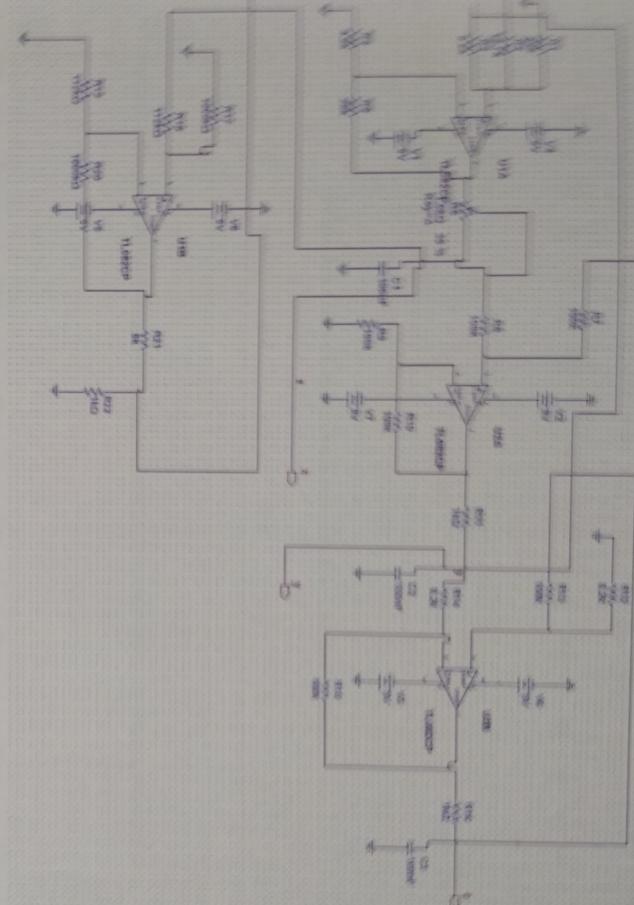


Şekil 2.3 Chua devresi x-y grafiğinden elde edilen double scroll şekli(osiloskopta yatay eksen 500mV/div ve dikey eksen 200mV/div)



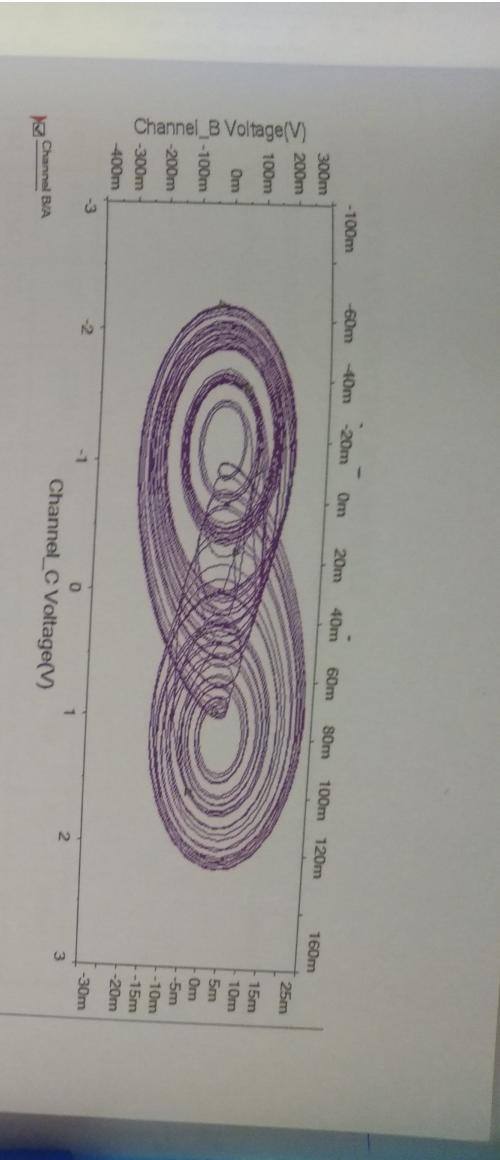
Şekil 2.4 Chua devresi x-z grafiğinden elde edilen double scroll şekli(osiloskopta yatay eksen 1V/div ve dikey eksen 2V/div)

ANÁLISIS DE RESINAS SIMULADAS

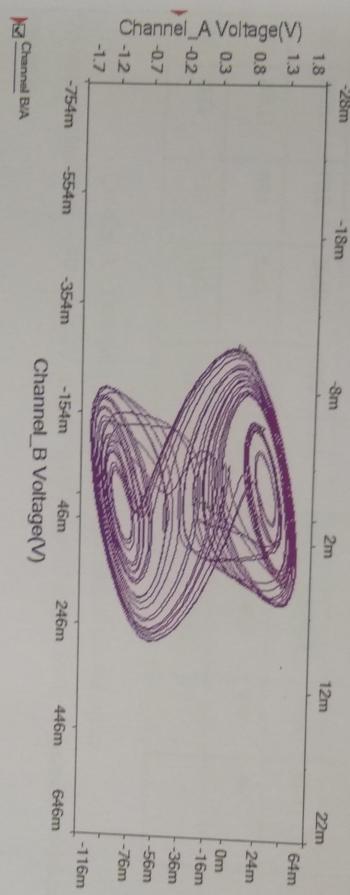


Şekil 3.4 SC-CNN modeli Jeneratör devresi

Sekil 3.4'te projede yapılan jenerator devresi görülmektedir.LM7805 voltaj regülatör ömrüklemeye devresinin beslemesi için kullanılmıştır jenerator devresiyle depuisan bir ligi yoktur.U4A elemanı devreye non-lineer özellik kazandırırken U1A,U2A ve U3A elektranları ise basitleştirilmiş SC-CNN modelindeki B2 bloklarına tekabül etmektedir.U4A ise bu nedenle B1 bloğuna tekabül eder.Simülasyon sonuçları ise sırasıyla sekil 3.5,3.6,3.7,3.8,3.9 da gösterilmiştir.x,y,z çıkışları sırasıyla C1,C2,C3 kapasitelerinin voltaj değerleridir.Sekil 3.8'deki pozitif ve negatif alternanslardaki salının süreleri birbirinden farklıdır ve bu durum kaosun kaynakıdır.Salının ne kadar süre pozitif alternansa veya negatif alternansa devam etkisi belirsizdir.Sekil 3.6 y'ye bağlı değişimini göstermekte olup, SC-CNN modelinde bahsedildiği gibi tamamen bir gürültü kaynağına benzer biçimde çalışmaktadır.Sekil 3.7'de ise 2-4 grafğında z noktasındaki yani C3'ün geriliminin C1'in gerilimiyle zt fazlı olduğunu gösterir.



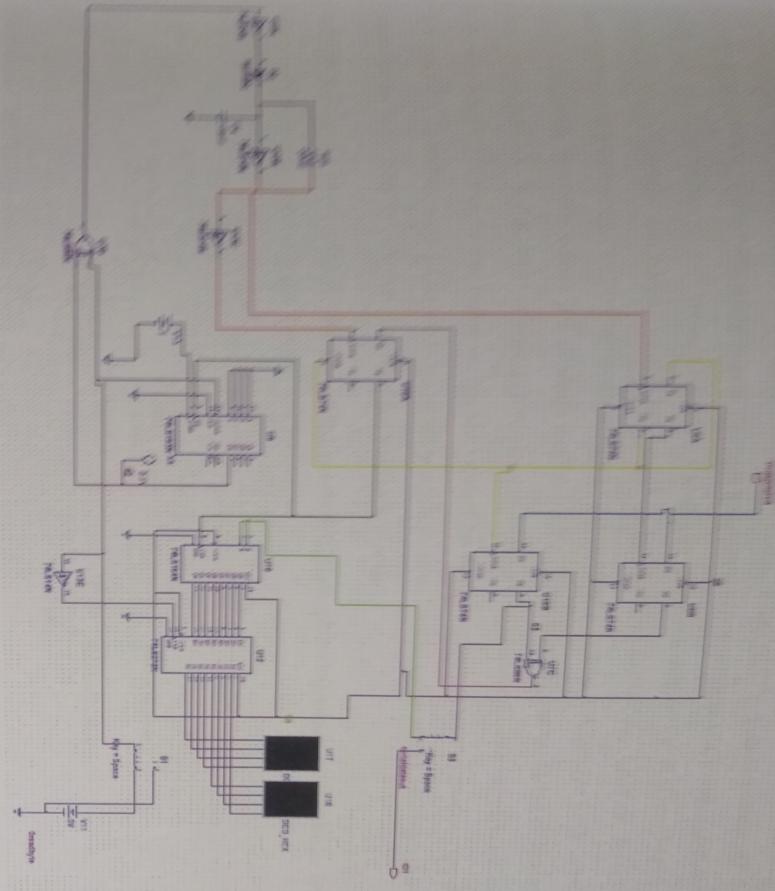
Şekil 3.8 Gerçekleştirilen kaos devresinde y-z grafiğinde gözlenen double scroll



Şekil 3.9 Gerçekleştirilen kaos devresi'nin x-y grafiğinde gözlenen double scroll

Şekil 3.8 ve Şekil 3.9 ise sırasıyla x-y , y-z grafikleridir. Şekil 3.8, C1 kondansatörünün geriliminin C2'ye göre nasıl değiştigini belirtirken Şekil 3.9 ise C2'nin geriliminin C3'e göre nasıl değiştigini gösterir. Double scroll grafiklerine 2.Bölüm'de değinilmiştir.

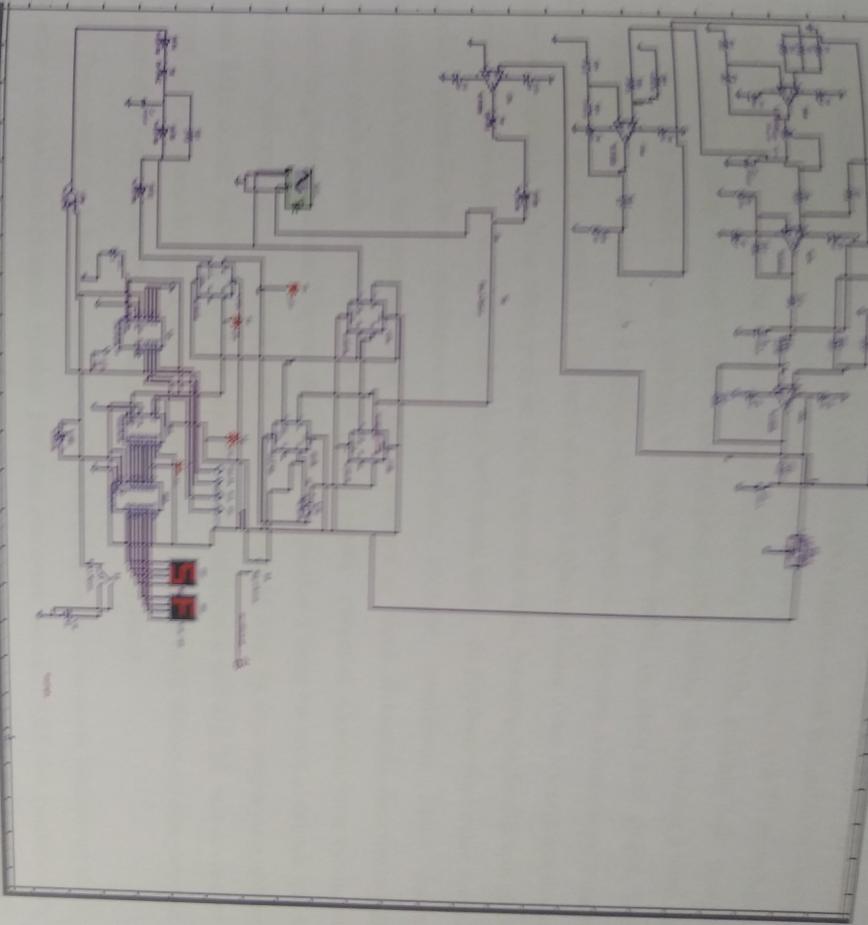
Sonuçta Bölüm 3.2 'de alınan parametrelerle Chua devresindekine benzer sarmal yapı CNN modeliyle elde edilmiş oldu.



Şekil 4.2 Devredeki D-flip-flopların bağlantısı

ve tek pasajde skırgın varsaðığımız bir akışından herhangi iki biti seçmiş bulunuyoruz. Von Neuman metoduna kalımmak için ise U16B ve U6B 'ye kaydettiðimiz iki biti XOR kapısından geçiririz. Yani bu iki bit 00 veya 11 ise XOR çıkış lojik 0 üretecek, eğer 01 veya 10 ise XOR çıkış lojik 1 olacaktır. Duraya kadar Von Neuman metodunu kullanarak XOR kapısı çıkışında rastgele birer birer toplamayı gerçekleştirmiş bulunuyoruz. Bundan sonraki iş ise bu bilgilerden 8 tanesini bir araya getirirken ekstra akırmaktır.

4.5 SIMÜLASYON SONUÇLARI



Sekil 4.6 Jenerator ve Sayıkkene devresinin bir aşaktaki gövdeinden ve simülasyon sonucundan bir örnek

Simülasyon sonuçlama gibi elde edilen 8 bitlik diziler birbirinden farklı olmaktadır ve random bilgilere gibi görünebilir. Elde edilen 8 bitlik sayıları random olmasın da hem yapılan jenerator devresi hemde sayıkkene göre resimde kalıcı olmamış saatin clock frekansı tol oynar. Bu devredeki clock sinyoede yaklaşık 625000 örnek alacak hızdır. Bu frekans veterince yüksek seçilmelidir ki jenerator çıkışından sonra TFT seviyesine vektürgünüz sınıvaldeki(yani zamsampled olarak ekranın birincil çıkış) verilende okunak akan bit açısından çok az sürelik 1'de kalma süreleri de örtüklenmeye çalışıl olsun.

Simülasyon sonucumun testi için önce elde edilen 8 bitlik dizileri bir dosyaya kaydetmeniz ve daha sonra bu dosyaya bir tekton kırılımının gerekerek ne oranda basan olde edildiğini

4.6.1 TESTLERİN KİTERLERİ VE SONUÇLARI

Aşağıdaki test programlarının sonucunda her test içinde ayrı ayrı hesaplanan p değerlerinin(p-value), 0.01 den büyük 1'den küçük olması gereklidir. Bu sonuc elinizdeki bir akıptan random olduğuma dair yeterli koşuldu[13].

Devrenin çalıştırılması sonucu elde edilen veriler Ek 2'de verilmiştir. Burada hatalamak gereklidir ki bilgisayar ortamındaki Simülasyon silresinin çok uzun süremsi nedeniyle Ek 2'de verilen veriler ömeklene frekansı düşürerek elde edilen verilereidir. Normalde saat devresindeki 100 pF'lik kondansatör ile 62.5 kHz'lik frekansa ömeklene yaparıcın devrede simülasyon için 100 nF'lik kapasite değeri seçerek devrenin 62.5 Hz gibi çok düşük bir frekansta çalışırıldığı göz önünde bulunmalıdır. Ömeklene frekansı arturulmaya simülasyon süresinin artacağı ancak testlerden çok daha iyi sonuçları elde edileceğü aşikâtdır.

1-Runs Test

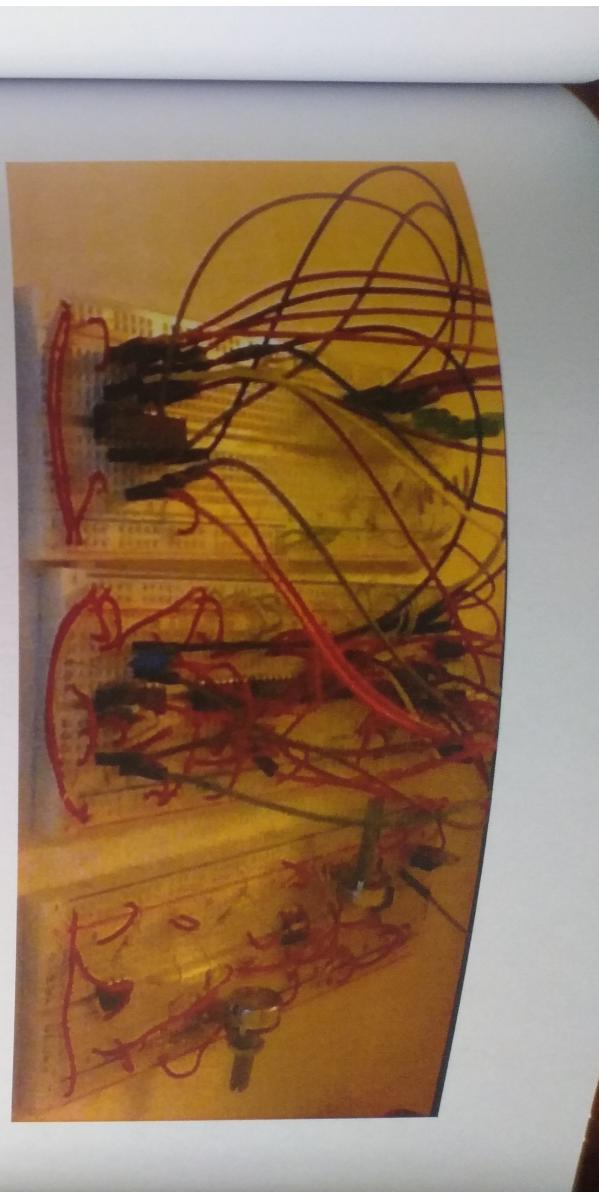
Bu teste bit dizisindeki 0 ve 1'ler arasındaki oslaysyonun çok mu hızlı ya da çok mu yavaş gerçekleştiği kontrol edilir. Bit akışındaki 0 ve 1'lerin uzunluklarının random demek için yeterli olup olmadığı kontrol edilir[12].

Ek 2'de verilen ve devrenin çalıştırılması sonucunda elde edilen bitlerin testi Şekil 4.7'de gösterilmiştir.

Runs Test	
COMPUTATIONAL INFORMATION	
(a) $P_1 = 0.4732/4285714288$	
(b) $V_{N_obs} \text{Total } \# \text{ of } (n=0) = 412$	
(c) $V_{N_obs} - 2\sqrt{P_1} \# \text{ (1=0)} = 289/251 \approx 1142$	
FAILURE	

Şekil 4.8 Runs Test sonucu

Şekil 4.7'de beklenen olmuştur ve test geçilememiştir. Çünkü 0 ve 1 arasındaki uzunluklar ömekleme frekansı çok küçük seçildiğinden yeterince iyi algılanamamıştır. Bu sonucuksi başarısızlık jeneratörden değil ömekleme devresinde seçilen düşük clock frekansının kaynaklamamıştır.



Şekil 4.13 Yapılan örneklemeye devresi ile jeneratör devresi bir arada gösterilmiştir



Şekil 4.14 Yapılan örneklemeye devresi(sağda) ve jeneratör devresinin(solda) baskı devreleri

